Print
Back to Docs Hub

TrueNAS SCALE

TrueNAS SCALE is the latest member of the TrueNAS family and provides Open Source HyperConverged Infrastructure (HCI) including Linux containers and VMs. TrueNAS SCALE includes the ability to cluster systems and provide scale-out storage with capacities of up to hundreds of Petabytes. Just like TrueNAS CORE, TrueNAS SCALE is designed to be the most secure and efficient solution to managing and sharing data over a network, from smaller home networks “scaled” up to massive business environments.

The Linux base of SCALE allows for a similar, but slightly different feature set that will appeal to an audience that is more familiar with Linux applications and workflows while TrueNAS CORE continues to provide the known and heavily tested performance and features from the FreeBSD operating system. SCALE is an acronym that represents the core features of the software:

Scaled-Out ZFS
Converged
Active-Active
Linux Containers
Easy to Manage

Unlike other HCI platforms, a user can get started with TrueNAS SCALE on a single node and incrementally scale up and scale out to over 100 storage nodes with many additional compute-only nodes. TrueNAS SCALE is true Disaggregated HCI, meaning storage and compute can be scaled independently. Each node can support Virtual Machines (with the KVM hypervisor) as well as Docker containers by using native Kubernetes.

Free to download and use, TrueNAS SCALE welcomes developers and testers to contribute to its Open Source development model.
OpenZFS and Gluster combine to enable scale-out ZFS capabilities with excellent stability and very efficient compression and snapshots.
Deploy a single hyperconverged node in a home/office or a cluster with hundreds of compute and storage nodes in a datacenter.
With support for KVM VMs, Kubernetes, and Docker containers, it’s easy to add applications to suit your every need.

Documentation Sections

TrueNAS SCALE documentation is divided into several sections or books:

- The Getting Started Guide provides the first steps for your experience with TrueNAS SCALE:
  - Software Licensing information.
  - Recommendations and considerations when selecting hardware.
  - Installation tutorials.
  - First-time software configuration instructions.
- Configuration Tutorials have many community and iXsystems -provided procedural how-tos for specific software use-cases.
- The UI Reference Guide describes each section of the SCALE web interface, including descriptions for each configuration option.

- API Reference describes how to access the API documentation on a live system and includes a static copy of the API documentation.

- SCALE Security Reports links to the TrueNAS Security Hub and also contains any additional security-related notices.

Ready to get started? Choose a topic or article from the left-side **Navigation** pane. Click the **<** symbol to expand the menu to show the topics under this section.

1 - SCALE 22.02 Angelfish Release Notes

Software Lifecycle

TrueNAS Quality Lifecycle

Release Stage	Completed QA Cycles	Typical Use	Description
NIGHTLY	0	Developers	Incomplete
ALPHA	1	Testers	Not much field testing
BETA	2	Enthusiasts	Major Feature Complete, but expect some bugs
RC	4	Home Users	Suitable for non-critical deployments
RELEASE	6	General Use	Suitable for less complex deployments
U1	7	Business Use	Suitable for more complex deployments
U2+	8	Larger Systems	Suitable for higher uptime deployments

> The Software Status page shows the latest recommendations for using the various TrueNAS software releases.

SCALE Schedule

> All release dates listed are **tentative and are subject to change**. The items in this list might not show every deadline or testing cycle that iXsystems uses to manage internal effort.

The progress and specific work is being tracked through tickets opened in Jira. If you have a feature suggestion or bug report, create a Jira account and file a ticket in the TrueNAS or TrueCommand projects. TrueNAS SCALE tickets are also tracked in the TrueNAS Jira Project.

Version	Checkpoint	Scheduled Date
TBD		

Obtaining the Release

To download an .iso file for installing SCALE Angelfish, go to https://www.truenas.com/truenas-scale/ and click **Download**. Manual update files are also available at this location.

To upgrade an existing SCALE install, log in to your SCALE web interface and go to **System Settings > Update**.

> SCALE is developed as an appliance that uses specific Linux packages with each release. Attempting to update SCALE with `apt` or methods other than the SCALE web interface can result in a nonfunctional system.

22.02.4

Septemeber 27, 2022

iXsystems is excited to announce the release of TrueNAS SCALE 22.02.4!

New Feature

- NAS-117827 New cloud sync provider: “Storj iX” (13 and Angelfish)
- NAS-104367 Add NVDIMM HA mirroring to TrueNAS SCALE
- NAS-102791 No support for Netgroups from LDAP

Improvement

- NAS-118216 Record midclt enclosure.query in debug (Core/Enterprise/Scale)
- NAS-118061 CLONE - Expose ZFS dataset case sensitivity setting via sb_opts
- NAS-117828 Add Storj as Cloud Sync service (13 and Angelfish)
- NAS-117802 Use truenas tls endpoint for usage stats
- NAS-117699 add tests for copy_file_range (server-side copy) for NFSv4.2
- NAS-117618 Review pickle module usage in middlewared
- NAS-117528 ctdb.public.ips.interface_choices require interfaces with an IP
- NAS-117422 Remove `retrieve_versions` from `catalog.query`
- NAS-117398 Add Storj as Cloud Sync service
- NAS-117394 type object ‘FailoverService’ has no attribute ‘LAST_DISABLED_REASONS’
- NAS-117233 New Google Cloud Storage task field: bucket_policy_only
- NAS-116556 netbios fields should be disabled when AD is enabled
- NAS-113922 gluster volume deletion integration tests

Bug

- NAS-118288 fix behavioral change in api_key.create
- NAS-118268 Add `.angular/cache` to `.gitignore`
- NAS-118240 Branchout for 22.02.4
- NAS-118239 Remove redundant debian-security mirror
- NAS-118178 fix typo in failover_/event.py
- NAS-118149 Removed log_py_exceptions from middlewared.test.integration.utils.client
- NAS-118140 Do not use `undefined` from `middlewared.utils` in integration tests
- NAS-118135 fix crash in nginx.get_remote_addr_port
- NAS-118131 fix ctdb shared volume teardown integration test
- NAS-118123 Alert in TrueNAS Scale won’t go away even after clicking on “dismiss”
- NAS-118117 move gluster fuse mounts to root cgroups
- NAS-118110 move fenced process to root cgroup
- NAS-118102 Support `--log-cli-level` for `runtest.py`
- NAS-118093 Dont block event look in check_permission hook
- NAS-118092 Properly terminate Web Shell and it’s children
- NAS-118091 Forbid using download token for websocket authentication
- NAS-118083 fix AttributeError crash in ha_permission hook
- NAS-118074 (SCALE) Plugins HPE MicroServer Gen8 not working with more, than 4 Drives
- NAS-118064 cache failover.hardware.detect
- NAS-118059 fix blank graphs when UPSBase plugin crashes
- NAS-118019 Prohibit trailing spaces in ZFS dataset names
- NAS-118014 fix failover.get_ips
- NAS-118013 Improve `core.bulk` documentation
- NAS-117972 No error message when trying to delete snapshot with hold
- NAS-117970 Mini customers report pools sometimes not importing at boot on Scale 22.02.3
- NAS-117955 Can not delete old boot environments
- NAS-117952 * [Apps] App logs dropdown, doesn’t allow selecting initcontainer
- NAS-117933 remove migrate call in make reinstall_container
- NAS-117931 Using HTTP Basic Auth will bypass 2FA
- NAS-117921 add `reinstall_container` make argument
- NAS-117911 Samba Share ACL resets to Everyone when disabled and re-enabled
- NAS-117895 CRITICAL ERROR ON UPDATE TrueNAS-22.02.0.1 -> TrueNAS-22.02.3
- NAS-117885 Shift winbindd_cache.tdb path in middleware
- NAS-117877 Improve KDC detection during domain join
- NAS-117865 Fix timeout during idmap updates
- NAS-117858 relax zfs_space VFS object validation
- NAS-117853 UI should not specify path attribute when zvol is being created for disk based vm devices
- NAS-117852 Fix path behaviour when disk type vm device is created
- NAS-117829 fix failover.disabled.reasons….again

- NAS-117825 Remove python nslcd client
- NAS-117801 Add some explicit tests for firstboot
- NAS-117800 Systemd Services fail
- NAS-117794 /etc/resolv.conf in Live ISO's filesystem.squash contains development information
- NAS-117777 Unable to join active directory if SMB is not started first
- NAS-117755 [SCALE] Downloading Logs from VMs is not working
- NAS-117747 vm.stop services do not stop
- NAS-117736 Installed chart in TrueNAS SCALE gives Middleware error
- NAS-117735 Only break out of fuse mount loop early on success
- NAS-117728 Shift timeouts to a single dict for cluster tests
- NAS-117725 Deleting cluster does not wipe the ctdb_shared_vol brick / dataset causing many issues on new create
- NAS-117713 Change how API keys are created
- NAS-117702 Applications Advanced settings menu does nothing
- NAS-117695 use asterisk to explicitly indicate full API access
- NAS-117691 Minimum memory field is not applicable for angelfish based vms
- NAS-117688 Cannot Edit VMs
- NAS-117684 Separately test basic NFS ops for version 3 and version 4
- NAS-117675 Add basic tests for ctdb managed services
- NAS-117674 Pool import fails randomly
- NAS-117673 enforce minimum zfs passphrase length
- NAS-117661 Minor bug fix for vm plugin
- NAS-117658 TrueNAS-SCALE-22.02.4-MASTER-20220805-041141 can't start VMs after importing old config or upgrading from 22.02.3 or earlier
- NAS-117655 Active Directory gets disabled on reboot
- NAS-117639 TrueNAS Scale update from TrueNAS-22.02.1 -> TrueNAS-22.02.3 fails with 'Devlinks'
- NAS-117636 Fix account test assets
- NAS-117627 `zfs.dataset.query_for_quota_alert` returns only top-level datasets
- NAS-117622 Add SMB client failover test for cluster
- NAS-117620 HA issue on M30 after loading SCALE Bluefin, ntb device problem
- NAS-117619 Same app mountpoint cannot be added even after app is (re)created
- NAS-117607 Breadcrumb for SMB Edit Filesystem ACL function is Incorrect
- NAS-117604 Node is unable to rejoin cluster after power off/on of 1/4 nodes
- NAS-117601 system.general.get_ui_urls blocks main event loop
- NAS-117592 24h clock in tasks
- NAS-117589 Cluster Cold Start Fails
- NAS-117587 Fix regression in getgrnam for gid 0
- NAS-117584 fix Makefile MWPATH
- NAS-117581 Launch Docker Image button only works on Available Applications tab
- NAS-117577 Applications fail to launch
- NAS-117557 Improvements to ctdb.public.ips APIs
- NAS-117556 fix IndexError in failover.vip.get_states
- NAS-117551 Fix `ftp_server_with_user_account` asset
- NAS-117526 Restore set netbios for angelfish stable tests
- NAS-117525 Remove silent from starting service in custer test
- NAS-117524 huge optimization to query_for_quota_alert
- NAS-117504 Reporting page won't load
- NAS-117501 disk_resize: Don't trigger udev events for NVMe
- NAS-117500 call install-dev-tools before setup_test.py
- NAS-117495 fix and improve middlewared Makefile
- NAS-117479 Skipping RAW device to be created
- NAS-117476 bucket_policy_only: Field was not expected when expanding folders in Cloudsync task
- NAS-117471 Improve AD health checks
- NAS-117467 Reuse tdb / ctdb handles
- NAS-117455 Reporting graph bug
- NAS-117449 credentials.verify doesn't timeout on incorrect SFTP credentials
- NAS-117443 Fix clustered SMB service management events
- NAS-117442 fix test_cluster_path_snapshot test
- NAS-117441 Added better support for python virtual environment
- NAS-117436 stop running file IO in main event loop
- NAS-117424 freenas-debug: Restore ZFS kstat capture
- NAS-117420 Initialize cluster so that all nodes have all public IPs
- NAS-117400 Fix activedirectory join in cluster
- NAS-117395 iscsi_/extents.py blocks main event loop in many places
- NAS-117391 Remove redundant dataset.query
- NAS-117382 Handle case of non-existent path during smbconf generation
- NAS-117378 Bump up timeout values for permissions tests on cluster
- NAS-117377 Fix clustered filesystem test
- NAS-117375 Problems upgrading certain applications
- NAS-117362 improve ntp alert verbiage
- NAS-117360 disk_resize: Don't wait 15 seconds for SAS flash
- NAS-117357 fix typo in disabled_reasons
- NAS-117353 Fix Failover_disks alert typo
- NAS-117352 Bump config version
- NAS-117330 vfs_fruit can write invalid timestamp as BTIME to user.DOSATTRIB xattr
- NAS-117328 Fixes an empty line in SMB share presets
- NAS-117307 Invesitgate/fix ix-volumes being migrated on apps migration
- NAS-117273 sedutil-cli fails to identify SAS SED drives on Linux
- NAS-117230 A pool scrub shows up twice in task manager
- NAS-117180 ZFS scrubs can cause very long pool import times
- NAS-117167 UPS reporting not working SCALE 22.02.2.1

- NAS-117144 Swagger documentation line on API Keys screen incorrect if default port has been changed
- NAS-117126 UI “Next Run” time is incorrect when Web client is in different time zone to TrueNas server.
- NAS-117123 After upgrade from TrueNAS-SCALE-22.02.2 to TrueNAS-SCALE-22.02.2.1 ZFS Volumes will no longer mount
- NAS-117118 Invalid update image file when trying to update nightlies
- NAS-117073 Pool Managers' dev type doesn’t initially match the Estimated raw capacity
- NAS-116975 Replication job fails to open docker-related dataset
- NAS-116875 TrueNAS Scale kubernetes Error
- NAS-116839 Hostname not set in /etc/hosts
- NAS-116823 UPS report completely empty
- NAS-116794 Official nextcloud app gets stuck during deployment
- NAS-116513 pmem on SCALE doesn’t report serial information
- NAS-116380 Trivial: On Network, Scale is displaying 2 default Gateways
- NAS-116295 Free RAM reported mismatch
- NAS-116098 nmbd breaks system dataset migration
- NAS-116071 On Angelfish Nightly after pressing Failover at the login it display “Failover is in an error state.”
- NAS-115992 NFSv4 not configured properly when active directory domain name != server subdomain
- NAS-115981 store cython-generated c files when making builds
- NAS-115869 NTP service broken when DHCP provides NTP servers.
- NAS-115817 Active Directory Middleware User / Group cache not initialized properly on boot.
- NAS-115737 Space in Pool Name / Path to Zlog kills iSCSI
- NAS-115649 Middleware crashing
- NAS-115625 Panic in encrypted ZFS receive
- NAS-114971 Intel X540-T2 no longer negotiates at 10G
- NAS-114707 SCALE Nightlies - SMB Time Machine Avahi is still not working
- NAS-114657 L2ARC size increases after reboot
- NAS-113895 Running zpool clear while a scrub is running effectively locks up entire system
- NAS-112995 Alert reads “…replication from scratch…” but entry is called differently in GUI

Notice

MinIO has removed backwards compatibility with version 2022-10-24_1.6.58.

MinIO fails to deploy if you update your version 2022-10-24_1.6.58 Minio app to 2022-10-29_1.6.59 or later using the TrueNAS web UI. Use the app roll back function and return to 2022-10-24_1.6.58 to make your MinIO app functional again. See the MinIO Migration documentation to manually update your MinIO app to the latest version without losing functionality.

22.02.3

22.02.3

August 9, 2022

iXsystems is excited to announce the release of TrueNAS SCALE 22.02.3!

Improvement

- NAS-117528 ctdb.public.ips.interface_choices require interfaces with an IP
- NAS-117394 type object ‘FailoverService’ has no attribute ‘LAST_DISABLED_REASONS’
- NAS-117269 failover.disabled_reasons returns a new NO_FENCED that webUI needs to account for
- NAS-117072 Include nftables ruleset in network debug dump
- NAS-117009 Only enable wsdd on recovery master when clustered
- NAS-116991 Add python ctdb client
- NAS-116981 Merge truenas/zfs-2.1-release into stable/angelfish
- NAS-116979 Don’t activate LVM volume groups before importing boot pool
- NAS-116976 improve boot time on SCALE enterprise hardware
- NAS-116857 Merge zfs 2.1.5
- NAS-116836 Force BSD semantics for group ownership if NFSV4ACL
- NAS-116819 Add ability for xattr handler to “strip” NFSv4 ACL
- NAS-116769 expose snapshot count via stat(2) of .zfs/snapshot
- NAS-116708 Under System Settings > General > Support add photo of system platform (R Series)
- NAS-116685 Add file size to manifest.json
- NAS-111488 Implement disk_resize equivalent in SCALE

Epic

- NAS-116239 Enclosure Management for SCALE

Bug

- NAS-117467 Reuse tdb / ctdb handles
- NAS-117443 Fix clustered SMB service management events
- NAS-117441 Added better support for python virtual environment
- NAS-117400 Fix activedirectory join in cluster
- NAS-117377 Fix clustered filesystem test
- NAS-117357 fix typo in disabled_reasons
- NAS-117351 Update 22.02.3 manifest to use 22.02.3 mirrors

- NAS-117329 Branch out for 22.02.3
- NAS-117313 Active Directory randomly automatically getting disabled during server reboot
- NAS-117306 Fix ctdb jobs on pnn 0
- NAS-117293 Deprecate legacy behavior to allow empty homes path
- NAS-117283 Key error when querying for filesystem.acltemplate.by_path on a dataset with an NFS acl type
- NAS-117276 migrate shells from core to scale properly
- NAS-117267 Fix multiple issues with failover.disabled_reasons
- NAS-117264 Updater size estimates seem quite off
- NAS-117263 Add test for disabling ACL auto-inheritance via SMB
- NAS-117245 Running rsync crashes middleware
- NAS-117231 Add CTDB event integration
- NAS-117217 CORE 12.0-U8 to SCALE 22.02.2.1 upgrade: middleware crash loop
- NAS-117209 smb.status parse blocking event loop
- NAS-117207 Submitting a ticket does not work
- NAS-117197 Kerberos: Slave KDC name is not provided as separate config line in /etc/krb5.conf
- NAS-117185 Snapshots Not Deleted After Specified Lifetime Expires
- NAS-117181 Allow setting UID 0 for new users
- NAS-117175 unable to flash chelsio cards on SCALE
- NAS-117174 /usr/local/bin/chelsio_adapter_config is FreeBSD specific
- NAS-117170 Unable to manual upgrade due to version comparison (downgrade error)
- NAS-117155 Fix bug in `ensure_builtins` option for ACL templates
- NAS-117149 Fix test mail subject
- NAS-117141 Fix `reporting.setup`
- NAS-117135 Add comment field to ACL templates
- NAS-117113 Report S.M.A.R.T. test in progress if there is a `Self test in progre…
- NAS-117097 regression in cluster api integration tests
- NAS-117085 Cloud Sync doesn't work with Google Cloud Storage buckets which use uniform access
- NAS-117081 Fix regression in clustered timeinfo
- NAS-117061 netif.list_interfaces() leaks small amount of memory on scale stable
- NAS-117058 Include "df -T" for SMB share paths in debug output
- NAS-117049 improve getting zfs arcstats
- NAS-117044 Do not expose user certificate's keys in debug
- NAS-117039 Failed to check for alert ZpoolCapacity
- NAS-117038 Upgrade pool menu item is not visible
- NAS-117032 No limit on collectd memory cache
- NAS-117014 Replace subprocess calls for clustered tdb backend
- NAS-117010 Provide more detailed ctdb status
- NAS-116990 Fix `etc/initramfs-tools/conf.d/noresume.conf` not being installed
- NAS-116988 Fix `"device": "pmem0p2", "disk": "pmem0p"` in pool topology
- NAS-116984 Switch to using ctdb client python bindings
- NAS-116978 Improve logging for when we disable a directory service
- NAS-116955 SCALE - Official apps' catalog stopped working
- NAS-116953 middleware/asyncio_loop memory and cpu leak
- NAS-116936 Remove unnecessary debug statements
- NAS-116924 Pool Offline
- NAS-116919 Constant alert.process_alerts in Task Manager
- NAS-116913 Cannot Delete Zvol
- NAS-116911 Using netgroups on NFS share exports broke in SCALE 22.02.2
- NAS-116910 Directory Service is sometimes not starting
- NAS-116909 LDAP fails with START_TLS and Validate certificates.
- NAS-116908 BootPoolStatus Alert
- NAS-116904 rate limit disk.temperatures endpoint
- NAS-116900 Verify that child mounts under SMB path are consistent
- NAS-116897 Process 3569743 (smartctl) of user 0 dumped core
- NAS-116881 stop doing file I/O on main event loop
- NAS-116879 zectl snapshot dumps core
- NAS-116876 Reduce some etc-file related log spam
- NAS-116875 TrueNAS Scale kubernetes Error
- NAS-116867 Add filesystem plugin method to get mount_info
- NAS-116865 Also install `pytest-timeout` in `install-dev-tools`
- NAS-116850 zfs.pool_events hook traceback
- NAS-116837 Launch Docker Image Button disabled and other UI bugs
- NAS-116835 add ipv6 flags to interfaces
- NAS-116834 Fix regression in s3 attachment
- NAS-116832 Fix setting up reporting database
- NAS-116826 smartd can't start
- NAS-116821 BUG: kernel NULL pointer dereference after SCALE 22.02.2 upgrade
- NAS-116820 Avaliable applications keeps populating and depopulating post 22.02.2 update
- NAS-116816 use statx to retrieve btime for files in filesystem.stat output
- NAS-116815 Going to Catalog Summary produces following error affter 22.02.2 update
- NAS-116814 Catalogs double listed after upgrade to 22.02.2
- NAS-116812 minor improvement to interface.sync
- NAS-116810 Place mako module directory under /run
- NAS-116808 Improve IPMI password validation
- NAS-116802 K3S fail to start cause by SSL issue. APPs module is not available.
- NAS-116794 Official nextcloud app gets stuck during deployment
- NAS-116776 Unable to upgrade from CORE 12.0-U8 to SCALE 22.02.1
- NAS-116767 Add test coverage for SMB ACL "map modify" behavior
- NAS-116763 Can't delete old certificate
- NAS-116751 Expose pool-wide space counters

- NAS-116750 NVIDIA Drivers update to 470.x.x
- NAS-116749 Expose used stats through pool.dataset
- NAS-116734 py-libzfs exceptions missing error action
- NAS-116728 Unable to backup Lightroom Classic Catalog directly to mapped drive on Truenas Scale
- NAS-116706 Core files error on TrueNAS SCALE
- NAS-116704 Fix debug size
- NAS-116701 VM RAW file support does not work because it configures the domain wrong
- NAS-116691 Re-enable rsync task fails
- NAS-116683 Add new helper function to convert mountinfo to dict
- NAS-116681 Remove host path validations temporarily on charts
- NAS-116680 Fix validation error naming schema for chart releases
- NAS-116677 Fix KeyError while collecting coredump info
- NAS-116676 PVC not getting migrated
- NAS-116612 UPS config not working
- NAS-116559 Application / container name validation error message is confusing and lacks helptext
- NAS-116547 Timezones on App (docker) creation are not ordered
- NAS-116507 Ensure all official apps have host path validation
- NAS-116492 Bonded interface names are not updated on upgrade from core to scale
- NAS-116455 TrueNAS ignores SMB Path Suffix when “Use as Home Share” is enabled
- NAS-116422 cpu and ram usage on dashboard fails on TrueNAS Scale
- NAS-116364 Pool name with spaces produces an error when creating a VM or attempting to start one
- NAS-116332 Upload ISO fails with wrong error when dataset is encrypted
- NAS-116212 SMART tests do not start
- NAS-116205 After reboot SMB will not start automatically
- NAS-116071 On Angelfish Nightly after pressing Failover at the login it display “Failover is in an error state.”
- NAS-115994 Idmap issue with “OWNER RIGHTS” SID
- NAS-115759 Do not allow immutable fields to be modified in UI
- NAS-115670 Cannot disable SMB share if “directory does not exist” (this *is* a bug, believe me!)
- NAS-113895 Running zpool clear while a scrub is running effectively locks up entire system
- NAS-113829 SCALE: Creating a second time machine share kills mDNS
- NAS-113136 Add check for SMB service being initialized

Security

- SCALE 22.02.3 Security Report

22.02.2

22.02.2

22.02.2.1 Hotpatch

July 7, 2022

iXsystems is excited to announce the release of TrueNAS SCALE 22.02.2.1! This is a small hotpatch meant to address a few bugs found after release, primarily with Enclosure Management, memory usage, and the Launch Docker button.

Bug

- NAS-117061 - netif.list_interfaces() leaks small amount of memory on scale stable
- NAS-117044 - Do not expose user certificate’s keys in debug
- NAS-117038 - Upgrade pool menu item is not visible
- NAS-116909 - LDAP fails with START_TLS and Validate certificates.
- NAS-116837 - Launch Docker Image Button disabled and other UI bugs
- NAS-116821 - BUG: kernel NULL pointer dereference after SCALE 22.02.2 upgrade

22.02.2

June 21, 2022

iXsystems is excited to announce the release of TrueNAS SCALE 22.02.2!

Enclosure Management

As TrueNAS SCALE continues to progress, so has Enclosure view functionality. With this release, the Enclosure view is available on the following TrueNAS platforms:

- R10
- R20
- R20B
- R40
- R50B
- Mini 3.0 X
- Mini 3.0 X+
- Mini 3.0 XL+
- Mini 3.0 E

- Mini 3.0 E+
- M50

Functionality is still improving for these platforms and we are working to add additional platforms in future releases.

Improvement

- [NAS-110523] - When ZFS dedup is enabled on a pool, use SHA512 as the checksum algorithm
- [NAS-111673] - ZFS debuginfo RPM conversion to DEB
- [NAS-112058] - [SCALE] Multiple containers cannot use the same intel GPU
- [NAS-113866] - create trunas-devel metapackage SCALE
- [NAS-114918] - Help dialog under System/Certificates/Add mostly quite useless
- [NAS-115659] - Set ZFS module parameter spl_panic_halt
- [NAS-115713] - new api endpoint to be used for recordsize choices for webUI
- [NAS-115720] - Azure Custom Endpoint
- [NAS-115740] - Azure Custom Endpoint
- [NAS-116049] - cache dmidecode -t0 data in dmidecode plugin
- [NAS-116053] - cache truenas.get_chassis_hardware results
- [NAS-116154] - Improve error message when quota cannot be set on user/group
- [NAS-116203] - TrueNAS Capacity Monitoring via Proactive Support
- [NAS-116248] - Cannot restore a PUSH replication
- [NAS-116265] - Merge truenas/zfs-2.1-release into stable/angelfish
- [NAS-116269] - Validate that all groups / users in a proposed ACL can chdir into the path prior to actually setting it
- [NAS-116387] - Remove unused trueview.stats event
- [NAS-116388] - Allow custom reporting.realtime time
- [NAS-116475] - better exceptions in py-nvme/py-sgio (get errno) on SCALE
- [NAS-116484] - optimize disk.sync_all on SCALE
- [NAS-116566] - using glob.glob in disk code on SCALE is painful
- [NAS-116624] - update scst with upstream
- [NAS-116637] - Build Core samba vfs modules on SCALE
- [NAS-116641] - Merge truenas/zfs-2.1.5-release into stable/angelfish

New Feature

- [NAS-114311] - ImageInspectError for all pods in kube-system namespace
- [NAS-115707] - Expose info about gluster network interface
- [NAS-116303] - add r50b nvme rear drive bays mapping support
- [NAS-116304] - add r50 nvme rear drive bays mapping support
- [NAS-116447] - "Proactive support" checkbox for "Alert Settings"
- [NAS-116670] - Branch out for 22.02.2

Bug

- [NAS-106532] - M50 and M60 rear nvme drive bay mapping
- [NAS-112562] - Attempt to add third SSD to mirrored pool fails
- [NAS-113532] - Cannot re-import zpool from GUI
- [NAS-114143] - Dashboard: Interface names cut off
- [NAS-114235] - Need better Linux kernel config procedure
- [NAS-114924] - Import CSR errors out on passphrase
- [NAS-114942] - Rclone fails with Scaleway S3 storage due to incorrect region
- [NAS-114960] - Long SMART Extended Self Test stuck at 90% for more than 48 hours
- [NAS-114984] - Core files for the following executables were found
- [NAS-114987] - Can not create pool
- [NAS-115025] - UPS Shutdown occurs when Power Off UPS is not set
- [NAS-115050] - Unhandled exception in dataset size observer
- [NAS-115094] - Allow /cluster locations to be used for CloudSync Tasks
- [NAS-115102] - SMB stops when changes to the LDAP configuration are made
- [NAS-115176] - SNMP Monitoring of the pools fail
- [NAS-115306] - NextCloud hits the SQL connection limit
- [NAS-115334] - CPU widget reporting Hottest CPU wrong when there are 2 CPUs
- [NAS-115394] - Apps : Search field default text gets outside the field when not selected
- [NAS-115425] - Rebooting Cluster Node does not restart smbd properly
- [NAS-115426] - Active Directory doesn't allow saving or warn when NetBIOS name > 15 characters
- [NAS-115435] - Falls off LDAP
- [NAS-115478] - SMB_ASSERT() on failure to get ZFS dataset information
- [NAS-115541] - adding description to an interface causes unhandled exception
- [NAS-115544] - adjusting lagg/bond membership excludes existing members 22.02.0.1
- [NAS-115578] - Rebooting TrueNAS Scale does not cleanly shut down VMs
- [NAS-115602] - Cannot remove netbios alias when updating AD config
- [NAS-115611] - Server does not boot in degraded state after loosing one boot-pool drive
- [NAS-115616] - CPU usage is wrong
- [NAS-115628] - Device list in iSCSI Extents is empty
- [NAS-115633] - Network graph: incorrect legend units
- [NAS-115639] - scale - zfs recordsize artificially capped at 1M. Should be tunable to 16M
- [NAS-115663] - in Sharing / SMB / Edit Share ACL, first entry cannot be deleted even if multiple present
- [NAS-115675] - Dashboard does not provide storage widget for pool named "temp"
- [NAS-115689] - Corrupted zpool may cause smbd service to crash
- [NAS-115738] - No "overview" information in "Interface" widget in dashboard, Chinese, Germen language are affected.
- [NAS-115770] - Fix `pool.dataset.processes_using_paths` for datasets that have nested zvols

- [NAS-115783] - Generated dhclient.conf files in BlueFIN nightlies are broken
- [NAS-115787] - After configuring LAGG, dashboard UI is broken and apps don't show
- [NAS-115796] - [SCALE] UI becomes unresponsive when installing some apps
- [NAS-115798] - Nextcloud missing configuration to prevent locks
- [NAS-115802] - TrueNAS Scale doesn't automatically use new LetsEncrypt certificate
- [NAS-115812] - When using Kubernetes GUI slows down to a crawl after a few minutes
- [NAS-115833] - VM clone of a clone zvol name length issue
- [NAS-115850] - 22.12 - Mapping loginShell to /bin/sh enables nologin users to log in
- [NAS-115854] - Can't change SMB admin group due to typo
- [NAS-115856] - [CLI] print created API key
- [NAS-115860] - Failed Upgrade to SCALE 22.02.0.1 - Zpool Wont Import
- [NAS-115865] - `middleware.block_hooks`
- [NAS-115872] - `zfs send -V` prints a per-second report of how much data has been sent (like `-v` does)
- [NAS-115887] - No System Dataset Option
- [NAS-115902] - [SCALE] Quota critical/warning alert cannot be 0
- [NAS-115913] - Secure temporary dir with `generate_ssh_key_pair`
- [NAS-115915] - Reduce the vulnerability to timing attacks
- [NAS-115935] - Fix unit tests
- [NAS-115938] - Tryinto replicate ix-systems
- [NAS-115942] - Port NAS-115110 to Scale
- [NAS-115952] - Update samba to 4.15.7
- [NAS-115954] - GeckoMain filling /var/db/system/cores (Container/App core!?)
- [NAS-115956] - SMBD Core Dump after transfer of huge data volume (time machine backup 800GB)
- [NAS-115964] - Fix integration tests
- [NAS-115969] - Permit case-insensitive renames in Samba 4.15
- [NAS-115975] - Unable to connect to KMIP server
- [NAS-115976] - Add tests for renames over SMB protocol
- [NAS-115977] - Add `ReplicationContext.remove_dataset` so we don't forget to update …
- [NAS-115980] - add ctdb.shared.volume.teardown method
- [NAS-115981] - store cython-generated c files when making builds
- [NAS-115983] - missing f in f-string
- [NAS-116017] - Syncthing host paths are not mounted
- [NAS-116029] - smb.sharesec.query returns list index out of range
- [NAS-116030] - `truenas-devel` package is not available on the apt
- [NAS-116033] - Fix unlocking readonly datasets
- [NAS-116063] - optimize system_is_enterprise_ix_hardware calls
- [NAS-116068] - Pod/Application logs do not display
- [NAS-116072] - `middlewared.utils.functools.cache`
- [NAS-116074] - Maintain equal `--ignore` option for both flake8 invocations
- [NAS-116082] - Sysctl "Variable" tooltip is outdated
- [NAS-116092] - System dataset update validation errors are not displayed
- [NAS-116093] - k3s uses system configured proxy for internal/localhost calls
- [NAS-116094] - [SCALE] UPS Reporting is empty
- [NAS-116097] - Bettet diagnostics for system dataset umount failures
- [NAS-116099] - Fix `pool.dataset.processes` returning bogus paths for locked datasets
- [NAS-116105] - The process asyncio_loop occupies the CPU for a long time
- [NAS-116108] - crash during session teardown after failure to create recycle bin
- [NAS-116116] - Kubernetes service is not running
- [NAS-116118] - Include lsblk -f output in Hardware debug
- [NAS-116119] - zv exists but no pv/pvc linked impossible to delete
- [NAS-116121] - Apps can't create PVC and stuck on deploying
- [NAS-116128] - Include rpc-statd and rpc-gssd status in debug output
- [NAS-116130] - Plex (official) doesn't start automatically after reboot
- [NAS-116134] - Device list in iSCSI Extents UX issues
- [NAS-116135] - fix changing hostname on standby node on HA
- [NAS-116140] - iSCSI wizard breaks down when middleware returns errors
- [NAS-116157] - Fix system_/dmi.py comparing a list to an int
- [NAS-116163] - SCALE: multiple machines get the same MAC address for LACP interfaces
- [NAS-116170] - retry git commands on failure
- [NAS-116207] - smbd crash due to SMB_ASSERT() being triggered in vfs_recycle
- [NAS-116208] - i225 FW1.79 support issues in Core and Scale, fixes in Freebsd 14 and Ubuntu 22.05
- [NAS-116220] - Cannot update dataset options in UI
- [NAS-116225] - Smart can't load
- [NAS-116231] - after Update 22.02.1 My app can not gpu passthrough anymore
- [NAS-116233] - Fix alternate code path for SMB connection rename in tests
- [NAS-116242] - Add initial Windows SD conversion regression tests
- [NAS-116244] - Reporting shows null data
- [NAS-116252] - Blacklist wide links related parameters
- [NAS-116253] - Remove crossrename from vfs objects when recycle enabled (#8967)
- [NAS-116264] - fix NO_VIP check on SCALE HA
- [NAS-116266] - Disable vfs_shadow_copy_zfs if snapdir is visible
- [NAS-116273] - remove nonexistent entry point for middlewared
- [NAS-116279] - Only the first selected dataset obey snapshot retention policy on replication
- [NAS-116283] - fix pool.is_upgraded_by_name
- [NAS-116288] - Use /proc/spl/kstat/zfs for quick zpool checks
- [NAS-116289] - [EFAULT] Unable to define domain for cloud: operation failed: domain 'xxx is already defined with uuid
- [NAS-116300] - Long replication output runs off of the screen and can't be scrolled
- [NAS-116310] - Remove automatic quota on TM preset
- [NAS-116324] - filesystem.can_access_as_user is broken. May be impacting vm plugin access checks
- [NAS-116326] - Significantly increase maxPods per node

- [NAS-116346] - Not able to retrieve logs for a successful cloud sync task
- [NAS-116349] - Do not send events for transient jobs
- [NAS-116350] - `pool.is_upgraded` minor performance improvements and tests
- [NAS-116351] - Reporting/rrd loging issues with .zfs snapshot set as visible
- [NAS-116362] - iptables-restore fails do to unquoted comments
- [NAS-116365] - Exception while calling periodic task (smb.sharesec.synchronize_acls)
- [NAS-116373] - include file type in filesystem.stat output
- [NAS-116379] - kernel bug at startup (ntb_hw_plx)
- [NAS-116424] - Clean up created replication tasks after replication test
- [NAS-116425] - Do not crash `zettarepl_schedule` if `begin` or `end` are not specified
- [NAS-116433] - device.get_disks() optimizations
- [NAS-116454] - Add mount flags to filesystem.statfs() output
- [NAS-116470] - Ensure disk_choices methods don't show in-use zvols
- [NAS-116480] - Fix migrations
- [NAS-116486] - Simplify process of adding NFS SPNs
- [NAS-116490] - Raise validation errors on ZFS ctldir and snapdir
- [NAS-116496] - Raise validation error on permissions changes to .zfs
- [NAS-116500] - Remove widelinks from list of sample aux params for CI
- [NAS-116518] - Upgrade from Core 12.0-U8.1 to Scale 22.02.1 - NFS & iSCSI Fail
- [NAS-116520] - Allow setting gid 0 on new groups
- [NAS-116522] - remove sockstat dependency
- [NAS-116530] - Do not allow port forwarding in ix-chart/minio app with hostnetworking
- [NAS-116531] - Fix AD debug script
- [NAS-116532] - Remove FreeBSD debug scripts
- [NAS-116540] - disk.get_unused traceback
- [NAS-116545] - Add key to SMB share presets to indicate cluster-safety
- [NAS-116546] - SCST rotational config option is 0 or 1
- [NAS-116567] - Fix `rmtree_one_filesystem` error reporting
- [NAS-116568] - fix typo causing exorbitant memory usage
- [NAS-116569] - Fix typo in SMB presets
- [NAS-116575] - Expose ZFS dosmodes in filesystem plugin
- [NAS-116584] - Add initial bunch of returns decorators to DS-related plugins
- [NAS-116586] - Libvirt guests are not gracefully terminating at shutdown
- [NAS-116596] - fix AttributeError in disabled_reasons
- [NAS-116600] - Fix mseries nvme mapping
- [NAS-116602] - catch proper pyudev exception
- [NAS-116613] - Fix async path validator
- [NAS-116630] - fix disk serial detection when SCALE is installed on bhyve
- [NAS-116631] - `wait_to_hang_and_dump_core` script
- [NAS-116646] - ctdb teardown method to resync interfaces
- [NAS-116650] - fix NO_VIP check when bond iface is empty
- [NAS-116651] - Improve error messages for invalid AD accounts
- [NAS-116652] - fix SCALE HA detection on BHYVE VMs
- [NAS-116657] - Fix `EventSource` error handling
- [NAS-116658] - resolve uid -1 and gid -1 prior to perm_check
- [NAS-116659] - Fix iSCSI disk tests
- [NAS-116660] - Ensure that SMB service stays running after AD stop
- [NAS-116671] - optimize ctdb.general.healthy

22.02.1

22.02.1

May 3, 2022

iXsystems is pleased to announce the release of TrueNAS SCALE 22.02.1!

Improvement

- [NAS-111197] - Document return type(s) of public endpoints of gluster plugin
- [NAS-113826] - add ability to enable/disable STP on bridge interfaces SCALE
- [NAS-114564] - Increase default number of NFS servers in TrueNAS 13 and SCALE
- [NAS-115010] - Disable the docker-compose binary
- [NAS-115057] - Provide indication that SED password was set
- [NAS-115066] - Debug should show if connected to truecommand
- [NAS-115194] - Update SCALE V5.10 to latest upstream release
- [NAS-115214] - umount FUSE mountpoint before stopping gluster volume
- [NAS-115244] - optimization in network common_validation
- [NAS-115465] - Expose additional flags via acl_flags in NFS4 ACL struct
- [NAS-115467] - nfs4xdr-acl-tools optimize determination of whether ACL is trivial
- [NAS-115468] - parallelize the git checkout portion of the scale build
- [NAS-115479] - Get usage stats of docker images being used by ix-chart
- [NAS-115618] - Have bullseye backports mirror for angelfish
- [NAS-115690] - Update Polish Translation (pool)

New Feature

- [NAS-104368] - NTB investigation/implementation in Linux
- [NAS-113617] - Update iconik plugin
- [NAS-114424] - Add netdata application
- [NAS-114881] - Remove Disable Hardware Offload checkbox from webUI
- [NAS-114929] - add truenas/py-nvme to scale-build
- [NAS-115932] - Branch out for 22.02.1

Bug Fixes

- [NAS-112105] - Domain name included in hostname twice in DHCP registration
- [NAS-113532] - Cannot re-import zpool from GUI
- [NAS-114013] - CLI Menu: memory leak and thread utilization
- [NAS-114315] - No apps starting after unexpected restart
- [NAS-114327] - Add notice-level alert for NTLMv1 auth attempts (maybe daily report)
- [NAS-114336] - No foreign console keyboard map possible
- [NAS-114435] - Fix `IoThreadPool`
- [NAS-114436] - cannot provide blank domain in networking config
- [NAS-114514] - After removing GPU from system, GPU still shows up in Apps/Chart config
- [NAS-114519] - Kubernetes unusable after adding 2nd network bridge to Scale
- [NAS-114536] - truecommand.poll_api_for_status jobs can queue up
- [NAS-114547] - Fix aptly local repository not being able to update
- [NAS-114594] - After update to 12.0-U8 S3 fails to start
- [NAS-114601] - Push replication issue from TrueNAS to FreeBSD 13.0 offsite server
- [NAS-114620] - Unable to create intermediate CA in UI
- [NAS-114652] - Support upload max file size
- [NAS-114653] - Show a warning when debug file was too large to upload
- [NAS-114667] - SCALE Nightlies - Failed to start kubernetes cluster for Applications
- [NAS-114674] - 22.02 / allow variables for portal path
- [NAS-114676] - Dry run action fails in Cloud Sync Task edit mode
- [NAS-114689] - Add a $ref for hostPath schema validation
- [NAS-114702] - "mail_html" not in sys.module error
- [NAS-114705] - make some ctdb plugins accessible via cli program
- [NAS-114715] - Update nvidia device plugin tag
- [NAS-114717] - Dropbox API tokens auto-expire
- [NAS-114721] - Type-safer job progress defaults
- [NAS-114722] - Safer reporting of job progress
- [NAS-114723] - TrueNAS SCALE - Missing sdparm command
- [NAS-114727] - Minio broken by default in recent scale (missing setcap)
- [NAS-114732] - Fix `disk_entry` schema
- [NAS-114733] - Fix serial console test when checking enabled serial
- [NAS-114741] - Have consistent plex friendly name
- [NAS-114742] - Allow multiple bind ips for NFS server
- [NAS-114751] - TrueNas Scale Cloud Sync Remote folder reset to /
- [NAS-114753] - Add tests for NFS share parameters
- [NAS-114754] - Incorrect ECC certificate ciphers available
- [NAS-114760] - Set log level of pyroute.netlink to critical
- [NAS-114769] - Changing Kerberos Principal from nothing to "---" breaks AD form
- [NAS-114771] - S3 service access key validation error
- [NAS-114781] - Reporting database used size 1.13 GiB is larger than 1.13 GiB.
- [NAS-114790] - Add regression tests for NFS subtree behavior
- [NAS-114792] - check=false for track_processes api test
- [NAS-114794] - Replication failed, None Command failed with code 1..
- [NAS-114795] - Fix behavior for allow_nonroot
- [NAS-114800] - Scale > Cannot create app using PVCs, stuck deplying.
- [NAS-114802] - Scale > Cannot remove zvol without breaking the running system
- [NAS-114807] - Restart NFS service on configuration update
- [NAS-114808] - fix acltype logic in sysdataset plugin
- [NAS-114809] - Add test for NFS "allow nonroot"
- [NAS-114811] - Expose "allow_nonroot" in Services > NFS in webui
- [NAS-114815] - Add regression tests for NFS server config
- [NAS-114819] - More `can_update` tests
- [NAS-114821] - Fix `zettarepl.annotate_snapshots` deadlock
- [NAS-114825] - Expose ability to query active NFSv3 and NFSv4 clients
- [NAS-114829] - Add regression tests for endpoints to get NFSv3 and NFSv4 clients
- [NAS-114833] - Error when disabling Hardware Offloading on physical interface
- [NAS-114834] - [SCALE] Apps fail to start after an update
- [NAS-114837] - VLAN with multiple IP address not working from GUI when boot system
- [NAS-114839] - SCALE missing UPS reporting
- [NAS-114850] - /etc/default/locale missing in TrueNas Scale
- [NAS-114853] - The following system core files were found: /usr/bin/udevadm
- [NAS-114854] - Add regression tests for ACLs over NFS protocol
- [NAS-114860] - fix failover_critical.py alert on SCALE HA
- [NAS-114867] - remove copyright/cleanup failover_disks.py alert
- [NAS-114869] - remove unnecessary SCALE HA alert
- [NAS-114873] - fix failover.py alert on SCALE HA
- [NAS-114874] - fix license alert verbiage
- [NAS-114877] - make sata dom alert run on SCALE HA
- [NAS-114898] - Fix `hold_pending_snapshots` feature allowing for incremental base to…
- [NAS-114899] - Fix unit tests
- [NAS-114900] - Allow getting / setting NFS-related debug levels at runtime

- [NAS-114904] - Improve `zfs.snapshot.query` `{"count": True}` performance.
- [NAS-114907] - Expand stats collected for nfsd in SCALE
- [NAS-114909] - less verbosity of logs in disk.sync
- [NAS-114910] - Remove contrib/non-free components
- [NAS-114912] - Add regression tests for NFS debug API
- [NAS-114915] - Option to global set SED password missing from Advanced
- [NAS-114919] - Extend nfsd stats to include threadpool info
- [NAS-114920] - Add private API to get / set NFSD threadpool mode
- [NAS-114922] - FusionIO Card (PCI Passthru to underlying VM) Blocks Automatic Update in Web GUI
- [NAS-114923] - Add regression tests for get/set threadpool mode
- [NAS-114938] - VM's uuid changes after every (system) reboot
- [NAS-114945] - Expand warning for shell modifications
- [NAS-114956] - CLI percent downloading and extracting significant digits
- [NAS-114974] - Cannot Export/Disconnect zpool
- [NAS-114977] - Error: [EFAULT] The uploaded file is not valid: no such table: django_migrations close
- [NAS-114978] - Default to enabling SA-based xattrs
- [NAS-114980] - Excutable found in /usr/sbin/apache2 alerts annoying
- [NAS-114986] - Replication fails with: can't compare offset-naive and offset-aware datetimes
- [NAS-115001] - Dataset name with spaces Produces error when creating a new VM
- [NAS-115019] - Missing qlogic Firmware
- [NAS-115027] - Local User creation taking over 4-5 minutes to Save
- [NAS-115037] - Web UI not working after sideloading
- [NAS-115039] - CTDB is unhealthy due to old nodes still present
- [NAS-115041] - Upgrading from 22.02-RC.2 to RELEASE failing
- [NAS-115049] - macOS cannot mount NFS shares with default options
- [NAS-115054] - Cutting from a SMB Share results in error
- [NAS-115058] - Exception disable_offload_capabilities when configuring network interface from CLI
- [NAS-115061] - k3s fails to restart after system reboot
- [NAS-115069] - Upgrade From CORE 12.0-U8 to SCALE 22.02 RELEASE Fails - freenas-boot/grub Dataset Exists
- [NAS-115077] - Google Sync Task Dry Run causes permanent task
- [NAS-115080] - SED drives do not work on SCALE
- [NAS-115083] - Add link state of interfaces for reporting realtime event source
- [NAS-115095] - CRITICAL: Web UI HTTPS certificate setup failed.
- [NAS-115101] - NSCD not running
- [NAS-115104] - iftop no longer available
- [NAS-115111] - KeyError 'nodePort'
- [NAS-115113] - Fix validation for raw uids / gids in pool.dataset.set_quota
- [NAS-115119] - Convert SSH etc group to use common render_ctx
- [NAS-115121] - Convert PAM etc group to use a render_ctx
- [NAS-115126] - Avoid pwd and grp lookups in etc file generation
- [NAS-115128] - Remove FreeBSD checks from etc plugin in SCALE
- [NAS-115130] - Pool created and Working but showing as "N/A" under disk tab
- [NAS-115133] - Core files for /usr/sbin/proftpd were found
- [NAS-115135] - Improve webdav validation and disable deprecated TLS versions
- [NAS-115137] - use new webdav.cert_choices to determine which certificate options to present users for webdav + https
- [NAS-115140] - Convert webdav etc group to use render_ctx
- [NAS-115166] - Fix iSCSI extents with whitespace in zvol names
- [NAS-115171] - Assignment of qcow2 image to a VM fails
- [NAS-115185] - SCALE: UPS Reporting Graphs Blank
- [NAS-115191] - "Network / Global Configuration / Host Name Database" is inconvenient
- [NAS-115195] - Fix updating `22.02.0` to `CUSTOM`
- [NAS-115196] - Use opener in ssh etc file generation
- [NAS-115198] - Reuse fd in etc file generation and run unlink in thread
- [NAS-115203] - Improve permissions handling in temporary keytab files
- [NAS-115207] - Fix middleware not starting
- [NAS-115211] - Remove legacy LDAP truenas_cacerts.pem file
- [NAS-115215] - Remove pwd and grp lookups from minio etc file
- [NAS-115218] - Avoid writing pool secrets to temp file and use fchmod where possible
- [NAS-115231] - Middleware does not detect when disks are used by a pool
- [NAS-115232] - Improve net global
- [NAS-115237] - Add better handling for NFS hosts that don't resolve
- [NAS-115240] - Job leak in middlewared
- [NAS-115243] - Dashboard Pool Widget not seeing new pool
- [NAS-115246] - GUI form cannot be saved on a fresh install
- [NAS-115249] - Fix regression in clusterjobs
- [NAS-115251] - add junit_family=xunit2
- [NAS-115256] - Dashboard widget is broken after pool is removed
- [NAS-115258] - Make `network_alias` `alias_address` and `alias_interface_id` NOT NULL
- [NAS-115268] - Fix id used for user-related config file regression tests
- [NAS-115272] - Merge migrations
- [NAS-115273] - Employ `flake8-import-order` to ensure correct import orders accordin…
- [NAS-115277] - Fix `replication.list_datasets` crashing when `SSH+NETCAT` transport is used
- [NAS-115284] - Disk Pool not updated after replace
- [NAS-115291] - unable to unlock encrypted dataset using gui
- [NAS-115294] - lldp was removed so remove from api tests
- [NAS-115295] - add system.product_type API test
- [NAS-115298] - stop test_022_catalog completely on HA
- [NAS-115299] - OpenSSL CVE
- [NAS-115300] - fix dissapear typos
- [NAS-115302] - fix regression in dns.sync

- [NAS-115309] - No error is shown if update servers cannot be reached
- [NAS-115310] - simplify and fix test_003_network.py
- [NAS-115327] - swagger API execution does not work when redirect to HTTPS is enabled
- [NAS-115352] - Memory leak in zettarepl
- [NAS-115355] - fix test_400_service.py
- [NAS-115356] - Disable root squashing in export config on demand
- [NAS-115359] - Aborting cloud sync task did not close the progress window
- [NAS-115367] - fix test_400_enable_disable_services on HA
- [NAS-115369] - Fix test_003_network.py on HA
- [NAS-115370] - Allow SYS security for NFSv3
- [NAS-115374] - [Scale] Cores files found (/opt/bitnami/redis/bin/redis-cli)
- [NAS-115378] - Ensure that rpc-statd service is enabled / started when NFS is started
- [NAS-115383] - prevent sharenfs parameter from breaking NFS exports
- [NAS-115397] - fix network regression on HA
- [NAS-115399] - Test NFS bindip separately from NFS server
- [NAS-115405] - `from middlewared.test.integration.assets.pool import pool` to test p…
- [NAS-115408] - Add option to enable shares on pool import
- [NAS-115411] - Fix test failure
- [NAS-115412] - improve disk.get_dev_size
- [NAS-115414] - better test_disk_get_dev_size tests
- [NAS-115415] - No installed apps shown after upgrade to SCALE 22.02.0.1
- [NAS-115420] - The dashboard displays "Updates available" when no updates are available.
- [NAS-115426] - Active Directory doesn't allow saving or warn when NetBIOS name > 15 characters
- [NAS-115430] - Root Email Will Not Save - TrueNAS Scale
- [NAS-115432] - net.inet.tcp.recvbuf_inc was removed in 13
- [NAS-115434] - fix test_disk_get_dev_size api test
- [NAS-115439] - [SCALE] Apps do not use the newer cert
- [NAS-115446] - [SCALE] debug file not attached
- [NAS-115448] - Expand maproot tests
- [NAS-115450] - Remove anonuid / anongid if user sets uid 0 / gid 0 as maproot
- [NAS-115456] - Fix logic for ms-account validation
- [NAS-115469] - Optimize acl_is_trivial
- [NAS-115471] - Remove LEGACY HA mode for SMB on SCALE
- [NAS-115482] - Don't set posixacl acltype on freenas-boot pool
- [NAS-115485] - Certificate authority generates invalid certificates on SCALE
- [NAS-115486] - Fix api docs not respecting port properly when redirecting
- [NAS-115496] - Add check that systemdataset pool is valid
- [NAS-115498] - Fix typo in filesystem.listdir and add optimization
- [NAS-115511] - SMB GUI for Recycle Bin Advising Bad Config
- [NAS-115521] - return stp info in interface.query
- [NAS-115545] - filesystem.setperm isn't properly handling cases where acltype = off
- [NAS-115552] - sqlite3.IntegrityError UNIQUE constraint failed when signing a csr
- [NAS-115557] - Upstream avahi master has NULL deref fix, bring into our repo
- [NAS-115561] - Provide `sensors -j` output in debug
- [NAS-115572] - Remove `/var/log/btmp` and `/var/log/wtmp` from debug
- [NAS-115601] - Fix FileExistsError: [Errno 17] File exists: '/var/db/collectd/rrd/localhost > '/var/db/collectd/rrd/test91.test91.nb.ixsystems.com'
- [NAS-115604] - connecting to TC is broken on 13 (potentially stable/master too)
- [NAS-115605] - Fix ValueError crashes
- [NAS-115606] - add rsync to depends in README.md
- [NAS-115616] - CPU usage is wrong
- [NAS-115619] - Don't write to same log file during parallel checkout in builder
- [NAS-115628] - Device list in iSCSI Extents is empty
- [NAS-115647] - Log branch override
- [NAS-115678] - fix NameError crash in exports.mako
- [NAS-115681] - nginx fixes
- [NAS-115688] - Fix `system.info` schema
- [NAS-115697] - Alert if the total number of snapshots is too large
- [NAS-115705] - Update codeowners
- [NAS-115719] - Fix job state reporting
- [NAS-115752] - set netbios name in cluster api tests
- [NAS-115766] - Fix NUT user group for 22.02.1
- [NAS-115793] - Allow netbiosname changes through AD plugin when clustered
- [NAS-115801] - Try to persist uids and gids across builds
- [NAS-115845] - Prevent integration tests to interfere with each other
- [NAS-115854] - Can't change SMB admin group due to typo
- [NAS-115887] - No System Dataset Option
- [NAS-115935] - Fix unit tests

22.02.0.1

22.02.0.1

March 22, 2022

iXsystems is pleased to announce the release of TrueNAS SCALE 22.02.0.1! This is a small update to SCALE 22.02.0 to address multiple security issues.

Security Hotpatch

The 22.02.0.1 security hotpatch implements security measures in response to these security vulnerabilities:

- CVE-2022-0847
- CVE-2022-0001
- CVE-2022-0002
- CVE-2022-0778

Improvement

- [NAS-115214] - umount FUSE mountpoint before stopping gluster volume

Bug

- [NAS-115202] - Fix CVE-2022-0847 vulnerability
- [NAS-115245] - Intel CVE-2022-0001 & CVE-2022-0002
- [NAS-115299] - OpenSSL CVE

22.02.0

22.02.0

February 22, 2022

iXsystems is pleased to announce the release of TrueNAS SCALE 22.02.0!

Improvement

- [NAS-105865] - Display parent dataset name in GUI in the "Add Dataset" form
- [NAS-109278] - Allow specifying properties for ix volumes
- [NAS-109638] - send signals to fenced based on zpool events
- [NAS-110488] - Review allowedCommonJsDependencies
- [NAS-110533] - Improve experience when reloading page
- [NAS-111045] - SCALE: Want CI for truenas/linux repo
- [NAS-111100] - Add bulk alternate datastream modification utility
- [NAS-111419] - Investigate automatically forcing xattr_fallback=on so it can be off by default
- [NAS-111842] - Sync improvements for Data Protection Dashboard
- [NAS-111872] - Use toggle slider to control share status
- [NAS-111964] - Enable fullTemplateTypeCheck
- [NAS-112096] - Angelfish splash screen
- [NAS-112767] - Better implementation of IxUserCombobox using IxCombobox
- [NAS-112919] - Refactor JIRA form to new ix-forms
- [NAS-112945] - Add ix-file-upload to new ix forms
- [NAS-113296] - Add support for expandable rows
- [NAS-113433] - ignore AttributeError in get_remote_os_version()
- [NAS-113575] - Refactor NFS service form to new ix forms
- [NAS-113649] - Investigate running waagent only in azure
- [NAS-113671] - Remove support for showing console on loading indicator
- [NAS-113679] - Remove unnecessary password checks
- [NAS-113689] - remove osc from pool plugin
- [NAS-113702] - improve pool.import_pool on SCALE
- [NAS-113716] - Host needs to be a dropdown in TFTP service configuration form
- [NAS-113734] - Rename Adjust priority button
- [NAS-113793] - remove int_pass column from SCALE HA db
- [NAS-113821] - Refactor LLDP form to new ix-forms
- [NAS-113847] - declutter network plugin
- [NAS-113855] - add zstd package to SCALE (to unpack core dumps)
- [NAS-113914] - Add Minio to Enterprise Plugin Repository
- [NAS-113915] - Merge OpenZFS 2.1.2 and a few other commits
- [NAS-114011] - PlexPass Version of Plex for SCALE
- [NAS-114028] - Add an input field for "tls_server_uri" into in S3 configuration form
- [NAS-114043] - Expose TTY into UI for TrueNAS Catalog Apps
- [NAS-114137] - Add an input field "console_bindport" into in S3 configuration form
- [NAS-114297] - Add link to docs from Update page
- [NAS-114379] - Improve vm.query performance after middleware restart
- [NAS-114448] - Refactor Export/Disconnect dialog into a separate component
- [NAS-114492] - Merge Linux v5.10.93
- [NAS-114500] - micro optimization in snmp-agent.py get_Kstat on SCALE
- [NAS-114531] - Pull from debian upstream
- [NAS-114638] - Skip duplicate action runs on TrueNAS/Linux CI
- [NAS-114697] - SCALE update files in build artifacts should be named with version string
- [NAS-114773] - Make xattr_compat a tunable, zfs_xattr_compat

New Feature

- [NAS-105932] - Add a few more ACMD DNS Authenticators

- [NAS-108574] - Add TLS support for Minio chart
- [NAS-108575] - Allow disabling docker image updates
- [NAS-108577] - Take backup of postgres in nextcloud chart
- [NAS-108689] - Chart release events on chart release resource changes
- [NAS-108691] - Ability to retrieve next unused port in middleware for Apps
- [NAS-108692] - Ability to retrieve k8s pods logs in middleware
- [NAS-109470] - Allow setting security privileges in ix-chart
- [NAS-111274] - Nextcloud server app not configurable due to volume persistency
- [NAS-112591] - Alert for large number of snapshots
- [NAS-112741] - Help Widget for TrueNAS dashboard
- [NAS-113095] - Machinaris Chart v0.6.x (new arch requires multiple containers)
- [NAS-113455] - Please document how our systemd preset works
- [NAS-113675] - Allow dashboard widgets to be reordered
- [NAS-113759] - New FTP option: timeout_notransfer
- [NAS-114241] - Replication configuration
- [NAS-114454] - Add unit/api tests for crypto plugin
- [NAS-114619] - Branch out build for 22.02

Epic

- [NAS-108382] - Mount locally joined Gluster Volumes
- [NAS-109636] - Add ability to make fenced reserve disks based off detected zpool
- [NAS-111870] - Additional middleware changes to support Democratic CSI use of native API
- [NAS-111907] - bugclerk visibility into OS Services repos

Bug Fixes

«ul>

- [NAS-108202] - bad signature because OCSP stapling not activated in the nginx config file
- [NAS-108333] - create ctdb plugin for gluster smb integration
- [NAS-108334] - create gluster shared volume for ctdb recovery db
- [NAS-108939] - Dashboard Memory legend changes colour
- [NAS-109118] - Use library chart for official catalog items
- [NAS-109138] - fix up ctdb.shared.volume and gluster.volume/peer CRUD APIs
- [NAS-109194] - handles k3s and VMs on SCALE HA appropriately
- [NAS-109206] - add interface validation in ctdb.public.ip.create
- [NAS-109304] - zfs.dataset.create set xattr=sa by default like pool.dataset.create
- [NAS-109322] - typo in reset_keys() in fenced on SCALE
- [NAS-109325] - fix check_path_resides_within_volume wrt to gluster paths
- [NAS-109451] - fix ctdb.general.ips
- [NAS-109456] - deprecate internal uses of system.is_freenas
- [NAS-109491] - cache if a system is licensed for HA (failover.licensed)
- [NAS-109497] - change cluster_events API to mount all gluster volumes based on events
- [NAS-109498] - add gluster FUSE api
- [NAS-109597] - FailoverService HA_MODE/HA_LICENSED not working
- [NAS-109599] - traceback in jail_freebsd
- [NAS-109602] - traceback in libvirt event_loop_connection
- [NAS-109617] - improvements to gluster.peer.status API
- [NAS-110853] - Export keys from dataset does not render json output
- [NAS-111581] - Upstream xattr compat
- [NAS-111680] - Support form will not work correctly if user is required to enter captcha
- [NAS-111800] - Replication failed: cannot receive resume stream: space quota exceeded.
- [NAS-111810] - Fixes #116 by swapping MINIO_ACCESS_KEY and MINIO_SECRET_KEY
- [NAS-111814] - Do not report coredumps generated by apps in containers
- [NAS-111851] - TrueNAS Scale Manual Page URLs are incorrect and/or out-of-date
- [NAS-111858] - TrueNAS-12.0-U4.1 alert email set for 'warning' and 'immediately' but for failed SSH logins is sending the alert daily (at midnight)
- [NAS-111989] - loading the dashboard calls to our update servers
- [NAS-111998] - CLI: network interface setup is very non-intuitive
- [NAS-112122] - Cloud sync task ignores configured subfolder
- [NAS-112189] - No Scrollbar For Selecting SSL Certs For K8S Ingress
- [NAS-112307] - CPU Reports in Dashboard broken, when using a proxy host
- [NAS-112334] - Applications add route - default route - truenas scale
- [NAS-112371] - Misleading and ambiguous description for creating a new pool with encryption
- [NAS-112667] - Core was generated by python3.9: middlewared (zettarepl)
- [NAS-112912] - Lost WebUI and SSH access on SCALE
- [NAS-113041] - FTP Timeout not honoured
- [NAS-113212] - System freezing/not restarting after kernel bugs
- [NAS-113277] - SCALE reproducible virtualization system crash / boot loop
- [NAS-113314] - CPU Usage Reports Incorrectly in GUI on Dual Socket EPYC System
- [NAS-113406] - Truenas scale - info messages show that it is based on Freebsd.
- [NAS-113441] - Replication with dedicated user broken TrueNAS Core -> TrueNAS Scale /usr/sbin is not in PATH
- [NAS-113453] - system continually does an orderly shutdown if browser tab is left open
- [NAS-113490] - [SCALE] Downloading certificates is not working correctly
- [NAS-113492] - Plugin install impossible
- [NAS-113494] - Disk wipe very slow on some disks
- [NAS-113520] - Core files for the following executables were found: smartctl
- [NAS-113527] - TFTP failed to start

- [NAS-113560] - Changing tab in the job list do not update the table.
- [NAS-113564] - Installer doesn't UEFI boot
- [NAS-113568] - Network UPS Tools missing SNMP driver
- [NAS-113570] - SCALE - swap partiton on boot-pool is newer used
- [NAS-113583] - Unable to expand pool
- [NAS-113588] - Password is NOT a required FTP credential field
- [NAS-113590] - It's unclear how to edit a cloud sync task
- [NAS-113609] - M60 has traceback alerts for "SATADOMWear" but system doesn't have SATADOMs
- [NAS-113615] - Add implmentation of configuring immutable flag via ioctl
- [NAS-113630] - Kubernetes will not start on fresh install
- [NAS-113641] - Bind IP address ignored when clicking 'Display' button
- [NAS-113642] - TrueNAS Scale UPS service fails to start
- [NAS-113651] - Fix credential button doesn't do anything
- [NAS-113652] - Container_images error when opening an app
- [NAS-113664] - Add required parameters for fsrvp in SCALE
- [NAS-113682] - Update common library
- [NAS-113687] - Document Boot CD and Python packages
- [NAS-113700] - Apps are not working, chart jobs never complete
- [NAS-113706] - Cloud Sync Tasks: null credentials is not allowed
- [NAS-113708] - Fix autocomplete on search field
- [NAS-113709] - TrueNAS logo do not fit the box on Reboot page
- [NAS-113720] - SMB Service is not listed alphabetically
- [NAS-113727] - Web gui unresponsive after a few days
- [NAS-113733] - Properly report if vm device fails to delete in the UI
- [NAS-113740] - mail.send task fails. Cannot find offending email address
- [NAS-113753] - Fix nested `Dict` validation error attribute name
- [NAS-113754] - Remove unnecessary usage of parametrize in filesystem api test
- [NAS-113756] - Fix form-chip
- [NAS-113757] - LetsEncrypt Certificate not showing in Application Charts
- [NAS-113758] - Bug fix for encryption summary of dataset
- [NAS-113760] - Export keys from dataset does not render json output
- [NAS-113772] - Virtualization: SPICE doesn't support display resize due to missing agent support
- [NAS-113781] - TrueNAS Scale - iftop is taking huge CPU load
- [NAS-113785] - SCALE NIGHTLY: Cannot create debug
- [NAS-113789] - Allow enabling multichannel SMB through API validation
- [NAS-113790] - "Mixing disks of different sizes in a vdev is not allowed."
- [NAS-113791] - Allow empty fromemail
- [NAS-113798] - Fix machinaris configs update + Add additional env variables (base for workers setup)
- [NAS-113811] - TrueNAS can offer to use HDDs of one zpool in creating another!
- [NAS-113812] - NFS large file transfers never finish with sec=krb5p or krb5i
- [NAS-113816] - Fix wsdd configuration generation
- [NAS-113817] - Errors in EntityJobComponent cannot be closed
- [NAS-113838] - Cloud sync dry run websocket performance improvements
- [NAS-113848] - VMs cannot start with ISO attached
- [NAS-113853] - VDEV Removal Error - Failed to wipe disks: 2) sdi: [ESERVICESTARTFAILURE] The smartd service failed to start
- [NAS-113856] - SQLAlchemy 1.4 does not use `default=` when adding a column through alembic
- [NAS-113861] - SQLAlchemy 1.4 compatibility
- [NAS-113867] - Unit tests should not be making real network requests
- [NAS-113890] - Fix KeyError: 'naming-schema'
- [NAS-113892] - GUI nvme manual smart test ValidationErrors
- [NAS-113903] - Input type="number" validation in Firefox
- [NAS-113907] - Build with Ganesha v4.0
- [NAS-113912] - Buttons has different fonts
- [NAS-113918] - TrueNAS Scale Upgrade Installation Fails
- [NAS-113921] - Optionally expand get_user_obj output to include grouplist
- [NAS-113937] - Improve executing commands with a user context implementation
- [NAS-113943] - [SCALE RC2] WebUI Prevents Loading in I-frame
- [NAS-113953] - When locale is not "English (en)" reports other than CPU cannot be accessed, as they redirect to the dashboard
- [NAS-113961] - Database used size 1.07 GiB is larger than 1.01 GiB
- [NAS-113967] - Update TrueNAS failed
- [NAS-113970] - Disk report specific dropdowns don't show content
- [NAS-113987] - "Installed Applications" Screen Takes Longer to Load
- [NAS-113995] - Failing to create a ticket with large debug file
- [NAS-113999] - Apps create directories on path of locked dataset, preventing it from mounting
- [NAS-114005] - VM with PCI-Passthrough won't boot
- [NAS-114012] - Core to Scale upgrade, very minor networking bug (DHCP)
- [NAS-114013] - CLI Menu: memory leak and thread utilization
- [NAS-114015] - Export/Disconnect fails: PoolDataset does not exist
- [NAS-114020] - Despite NAS-110600 being marked as resolved, the same bug continues to prevent me from disconnecting two outdated pools.
- [NAS-114022] - [SCALE] WebUI keeps "Unlocking Datasets" even though It's already done
- [NAS-114024] - Properly validate empty/malformed chart/questions yaml files
- [NAS-114025] - Disable apt by default
- [NAS-114026] - VM delete fails due to non existing PCI device
- [NAS-114029] - Print full name of the plugin being initialized
- [NAS-114031] - Nextcloud update never ends
- [NAS-114032] - Entity empty should be centered
- [NAS-114034] - Installing Nextcloud as a plugin leads to php error

- [NAS-114045] - Truenas Scale PCIe Passthru issue - Raid card not visible
- [NAS-114047] - core file found
- [NAS-114058] - Duplicate drives in pool creation
- [NAS-114074] - Hostname Database regression in SCALE 22.02-RC.2
- [NAS-114076] - Pool shows up as unhealthy when replacing drive in pool
- [NAS-114084] - ZFS metadata corruption - Pool state green in dashboard
- [NAS-114087] - VM - RAW file type broken/unable to run VM
- [NAS-114088] - Cloud Sync Tasks - WebUI broken
- [NAS-114092] - Delete dataset with childs - lsof at 100%
- [NAS-114113] - Memory leak in zettarepl
- [NAS-114116] - Make minio console port configurable
- [NAS-114122] - SCALE Nightlies - Upgrade Apps Screen is Still Slow to Load
- [NAS-114130] - Correctly recognize wg/macvtap interfaces as cloned interfaces
- [NAS-114135] - Correctly raise assertion error in api tests
- [NAS-114144] - No login shell for SSH after upgrade for user root
- [NAS-114146] - "Create Pool" dialog improvements
- [NAS-114149] - Impossible to install SCALE on SSD "size partition table entries is 0 bytes"
- [NAS-114159] - Fix building docs
- [NAS-114170] - Properly check catalog dataset is locked
- [NAS-114171] - Scale and Core: "Serial Shell" French translation
- [NAS-114176] - Cloud Sync Fail with snapshots enabled and existing Zvol
- [NAS-114187] - Add allow interfaces directive to avahi config
- [NAS-114189] - Fix a few schema errors discovered when performing integration tests …
- [NAS-114207] - Ability to mount extras in read-only mode
- [NAS-114208] - Kubernetes/Docker Environment Variable With Value of "y" Becomes "true"
- [NAS-114212] - Reportsdashboard doesn't work
- [NAS-114214] - Deleting a dataset causes the deletion of a replication task
- [NAS-114215] - [SCALE] Disk Report not showing the correct drives in a pool
- [NAS-114223] - Do not take snapshot of docker dataset when making a backup of apps
- [NAS-114224] - APPS: Fix Launch Docker Image and Settings dropdown
- [NAS-114226] - Do not enable waagent automatically
- [NAS-114228] - zettarepl.create_recursive_snapshot_with_exclude
- [NAS-114248] - Selectively handle auth header in docker client
- [NAS-114279] - Reduce pyroute logs footprint in middleware logs
- [NAS-114280] - Set certain sysctl(s) to configure system behavior appropriately
- [NAS-114302] - Only log once that no enclosures were found
- [NAS-114306] - Delete app while smb share open through windows
- [NAS-114338] - Warning not showing up for isolating Passthrough devices
- [NAS-114347] - Virtual Machines list don't update when starting or stopping a VM
- [NAS-114353] - Do not run `disk.sync_all` on zvol creation/deletion
- [NAS-114356] - Make sure we close opened snapshot handle
- [NAS-114358] - Wrong timezone in various timestamps throughout the UI + CLI
- [NAS-114359] - Provide `exclude_mountpoint_property` for `replication.run_onetime` f…
- [NAS-114360] - Correctly retrieve bus attribute for disk
- [NAS-114375] - Static routes are not added after reboot
- [NAS-114378] - Investigate always adding a no-execute taint on kubernetes on start
- [NAS-114381] - Increate acme.client logging level
- [NAS-114391] - randomly erorrs during replication: "Timeout in head()"
- [NAS-114393] - App Catalog Sync is Too Slow
- [NAS-114394] - Unable to update gui https cert
- [NAS-114404] - Move crypto plugin to separate service parts
- [NAS-114405] - [SCALE] Dataloss: PVC's getting destroyed when backup is restored
- [NAS-114410] - Custom cron job modal is cut off on smaller screens
- [NAS-114417] - Do not modify original create properties dict
- [NAS-114420] - Cloud Sync Task UI does not keep Directory/Files checkbox checked
- [NAS-114428] - Validation Error Traceback from unsetting Include Dataset Properties
- [NAS-114431] - VM performance improvements
- [NAS-114435] - Fix `IoThreadPool`
- [NAS-114444] - Add Shibgreen support for Machinaris
- [NAS-114481] - Fix xattr compat fallback handling on Linux
- [NAS-114501] - services/nfs - convert to kernel NFS server
- [NAS-114503] - Free memory for snapshot mountpoint
- [NAS-114506] - Can not delete a virtual machine with not present GPU
- [NAS-114513] - Fix 13.0 freenas/webui in nightlies build
- [NAS-114519] - Kubernetes unusable after adding 2nd network bridge to Scale
- [NAS-114529] - Fix memory leak in py-libzfs iterators
- [NAS-114533] - Replication no longer works on nightly build
- [NAS-114541] - NFS Path with "spaces" never shows up
- [NAS-114546] - Some tables in the UI have left aligned empty and loading states
- [NAS-114555] - Ensure that zpool handles are freed in iterator
- [NAS-114567] - Remove py-bonjour dependency
- [NAS-114569] - Remove unused packages
- [NAS-114573] - fix process pool deadlock
- [NAS-114581] - fix exorbitant middlewared service memory usage
- [NAS-114594] - After update to 12.0-U8 S3 fails to start
- [NAS-114596] - Eliminate extra call to cache.get for SMB_HA_MODE
- [NAS-114601] - Push replication issue from TrueNAS to FreeBSD 13.0 offsite server
- [NAS-114620] - Unable to create intermediate CA in UI
- [NAS-114622] - Fix UI verbiage to say CSR's when importing certs
- [NAS-114623] - fix get_smartd_schedule_pieces

- [NAS-114632] - Fix websocket regression
- [NAS-114635] - Fix `Unable to downgrade from 22.02-MASTER-20211206-192929 to 22.02-C…
- [NAS-114655] - nfsv4 acltype doesn't work for NFS 4 clients
- [NAS-114667] - SCALE Nightlies - Failed to start kubernetes cluster for Applications
- [NAS-114689] - Add a $ref for hostPath schema validation
- [NAS-114702] - "mail_html" not in sys.module error
- [NAS-114704] - [SCALE] nfs service not startable. (/etc/exports not being generated at least)
- [NAS-114710] - Error: Unable to downgrade from 22.02-MASTER-20220207-112927 to 22.02.1-MASTER-20220208-034252
- [NAS-114721] - Type-safer job progress defaults
- [NAS-114722] - Safer reporting of job progress
- [NAS-114723] - TrueNAS SCALE - Missing sdparm command
- [NAS-114732] - Fix `disk_entry` schema
- [NAS-114733] - Fix serial console test when checking enabled serial
- [NAS-114734] - Fix ACL checks for NFS kernel server
- [NAS-114784] - Disable subtree checking if NFS export is a mountpoint
- [NAS-114795] - Fix behavior for allow_nonroot
- [NAS-114807] - Restart NFS service on configuration update

22.02-RC.2

22.02-RC.2

December 22, 2021

iXsystems is pleased to announce the release of TrueNAS SCALE 22.02-RC.2!

Improvement

- [NAS-110081] - Investigate/fix Sentry integration for webui
- [NAS-112309] - Make an example of user combobox
- [NAS-112525] - Standartize IP validation
- [NAS-112555] - Add ChangeDetection.OnPush to new ix-form components
- [NAS-112556] - Solve input text formatting
- [NAS-112571] - Add tooltips to explain dataset lock icons
- [NAS-112586] - Add test harnesses to new ix-form components
- [NAS-112617] - Implement new form checkbox
- [NAS-112655] - Move inline styles to associated files
- [NAS-112660] - Update apt mirrors preparing for next Angelfish RC
- [NAS-112663] - Add titles to pages
- [NAS-112689] - Improve i18n support
- [NAS-112713] - Replace T-marker with translate.instant
- [NAS-112724] - Network Metrics: Octets != MB/s
- [NAS-112739] - Enable prefer-as-const
- [NAS-112769] - Add tests to localization form
- [NAS-112770] - Refactor any simple form to new ix-forms
- [NAS-112771] - Refactor any simple form to new ix-forms
- [NAS-112772] - Refactor any simple form to new ix-forms
- [NAS-112777] - Add "multiple" support for ix-select
- [NAS-112781] - Create pools with atime disabled by default
- [NAS-112793] - W42 - Improving type safety
- [NAS-112803] - cleanup unused failover code on SCALE
- [NAS-112804] - create new failover endpoint for triggering failover event on SCALE
- [NAS-112818] - When GMail mail is configured, hide "fromemail" and "fromname" fields from UI and send them as empty strings
- [NAS-112821] - clean up interface/configure.py
- [NAS-112848] - Refactor NTP form on System Settings to new ix-forms
- [NAS-112851] - The "Unlock Children" box unchecked doesn't indicate that inherited child datasets will be unlocked as well
- [NAS-112880] - Refactor SysctlFormComponent
- [NAS-112889] - W42 - Type safety improvements
- [NAS-112896] - Enable no-nested-ternary linter rule
- [NAS-112901] - Redesign error handling in ix-forms
- [NAS-112908] - Show job arguments in webui task manager
- [NAS-112914] - Remove unused theme editor
- [NAS-112925] - Refactor remaining bootenv forms to ix-forms
- [NAS-112938] - Refactor ssh key pair form
- [NAS-112949] - Standartize progress indication in new ix-forms
- [NAS-112968] - capture stderr on ssh_test
- [NAS-112969] - Display human-readable values on Network widget charts
- [NAS-112987] - Add app metadata for helm subcharts in app operations
- [NAS-112989] - W43 - Type safety improvement
- [NAS-112990] - use filterable_returns in dns.query
- [NAS-113023] - Refactor Console and Static Route forms
- [NAS-113027] - Refactor Isolated GPU PCI Ids form to new ix forms
- [NAS-113037] - Refactor some of Kerberos forms
- [NAS-113050] - Enable implicit-arrow-linebreak and other rules
- [NAS-113061] - change cluster API tests to use new cluster IPs

- [NAS-113062] - update ixsystems/releng to use new cluster ip env vars
- [NAS-113069] - add ldap/ad env vars to cluster tests pipeline
- [NAS-113104] - remove multipath related api calls from webUI on SCALE
- [NAS-113116] - Refactor ServiceWebdavComponent to use new ix forms
- [NAS-113117] - Refactor SyslogFormComponent to use new ix forms
- [NAS-113130] - Add endpoint to retrieve valid choices for syslog tls certificate
- [NAS-113152] - Refactor Add Init/Shutdown Script form
- [NAS-113184] - Refactor BootEnvReplaceForm and BootEnvAttachForm to new ix forms
- [NAS-113186] - Switch from debug builds to production builds of ZFS
- [NAS-113204] - Refactor SMART service form to ix-forms
- [NAS-113205] - Refactor SystemDatasetPool to new forms
- [NAS-113217] - Refactor resilver config form to new forms
- [NAS-113219] - Enclosure UI should provide more disk details like disk model
- [NAS-113267] - Refactor Catalog and Pull Image forms to new ix-forms
- [NAS-113286] - flag primary interface on active-backup bonds
- [NAS-113289] - webui to preserve order for bond members
- [NAS-113294] - Build an example of basic ix-table
- [NAS-113298] - Add examples and utilities to test pages using ix-table
- [NAS-113299] - Enable linter rule to force camelCase for local variables
- [NAS-113319] - Enable strict templates in Angular
- [NAS-113322] - Allow closing slide-in forms with Escape key
- [NAS-113363] - Enforce camelCase on function params
- [NAS-113377] - Refactor Rsync form to new ix forms
- [NAS-113378] - Refactor license form to new ix forms
- [NAS-113379] - Refactor S3 settings form to new ix forms
- [NAS-113382] - up the gluster.localevents.send timeout parameter
- [NAS-113390] - Refactor service ssh form
- [NAS-113421] - Enforce proper naming convention of class members
- [NAS-113430] - W47: Improving type safety
- [NAS-113451] - Refactor Dashboard Configuration to use new ix forms
- [NAS-113467] - Refactor ServiceDDNSComponent component to new ix forms
- [NAS-113493] - Add unit tests for Services table
- [NAS-113569] - Merge Linux v5.10.81
- [NAS-113604] - Keep sidenav state in user preferences
- [NAS-113606] - improve fenced logging SCALE HA

New Feature

- [NAS-111019] - Allow disabling builtin load balancer in k8s
- [NAS-111274] - Nextcloud server app not configurable due to volume persistency
- [NAS-112132] - Support: Use OAuth flow instead of username/password
- [NAS-112168] - Add collabora official application
- [NAS-112754] - Improve process of updating apt mirrors
- [NAS-112865] - Please add custom mount point to host data access for minio app
- [NAS-112936] - Mirror debian-debug repo
- [NAS-113095] - Machinaris Chart v0.6.x (new arch requires multiple containers)
- [NAS-113125] - Should we display WAITING jobs in Task manager
- [NAS-113153] - Allow setting capabilities for workloads deployed with ix-chart
- [NAS-113455] - Please document how our systemd preset works

Epic

- [NAS-103664] - Add support for NFSv4.X ACLs on Linux
- [NAS-111888] - Clustered SMB: Initial Delivery Requirements

Bug Fixes

- [NAS-111694] - Dataset keyfile upload not working, manually entered key works
- [NAS-111863] - IPMI Identify is not working
- [NAS-112060] - [SCALE] Rollback should use dropdown instead of textfield
- [NAS-112102] - Can't Upgrade TrueNAS Core 12.0-U3 to TrueNAS Scale 21.08
- [NAS-112122] - Cloud sync task ignores configured subfolder
- [NAS-112238] - Application events order changes order on every button or mouse click
- [NAS-112347] - TrueNAS Scale Quote Exceeded on Dataset - Daily
- [NAS-112351] - Error: "Disk 10336936891386576613 is FAULTED" - What is 10336936891386576613?
- [NAS-112427] - ACL view in "Storage" shows "-" instead of the group
- [NAS-112430] - core dump after migrating from TrueNAS Core 12.0-U5 to TrueNAS SCALE Beta 21.08
- [NAS-112481] - Booting on a network without a DHCP server results in a funky console.
- [NAS-112490] - Failed to access Homes Directory for Domain Users
- [NAS-112543] - Freenas_default expired
- [NAS-112569] - pbkdf2iters value is not correctly shown
- [NAS-112594] - R40: first enclosure element is unclickable
- [NAS-112629] - TrueNAS SCALE Enterprise login window says "TrueNAS SCALE_ENTERPRISE ® © 2021"
- [NAS-112633] - Fix colors for Directory Services Monitor popup
- [NAS-112643] - Fix job width on Task Manager
- [NAS-112645] - Unable to Startup Windows VM
- [NAS-112666] - WebUI was all blank except the menu on the left
- [NAS-112676] - Add initial cluster tests for sharing.smb
- [NAS-112682] - Add basic filesystem API tests for clustered filesytem

- [NAS-112684] - Fix empty state on entity table
- [NAS-112700] - Fix regex for branchout in scale build repo
- [NAS-112706] - Columns "Frequency" and "Next Run" in "Rsync Tasks" list wrong values
- [NAS-112743] - reporting broken after changing system dataset
- [NAS-112751] - Add initial clustered activedirectory tests
- [NAS-112752] - NVIDIA Tesla P4 not recognized by K3S
- [NAS-112760] - Correctly specify nightlies version
- [NAS-112761] - FTP fails to start when Enable TLS is checked
- [NAS-112765] - Apply Pending Updates prompt is shown twice when configuration is saved
- [NAS-112766] - Add last 1000 lines of k3s logs to debug
- [NAS-112768] - middleware cannot parse UPS driver list correctly
- [NAS-112773] - azurelinuxagent tries to run and fails on local Hyper-V VM
- [NAS-112780] - Migration from CORE to SCALE results in a corrupted install of SCALE
- [NAS-112783] - [ix-input] the clear button invisible on form init
- [NAS-112788] - Split AD service into parts and add DNS client plugin
- [NAS-112797] - storage widget is capitalizing zpool names
- [NAS-112798] - standby controller widget on dashboard doesnt work
- [NAS-112814] - The "From Name" isn't used in an email sent that was configured in Alerts -> Email
- [NAS-112823] - shutdown -r now races and breaks scale HA
- [NAS-112835] - Attach Debug fails with: Error: [EFBIG] Debug too large to attach
- [NAS-112844] - WARNING Domain validation failed with error: [ENOMETHOD] Method 'get_n_working_srvers' not found in 'activedirectory'
- [NAS-112853] - journal_ha thread being started on non-HA systems
- [NAS-112856] - ACL editor stuck on "please wait"
- [NAS-112857] - CPU Temperature not appearing in Reporting
- [NAS-112887] - openebs not starting correctly
- [NAS-112900] - Prevent users from disabling mDNS if time machine is enabled
- [NAS-112903] - vrrp_fifo_listen thread not running on initial setup
- [NAS-112904] - failover.status taking forever on initial failover
- [NAS-112907] - Ensure that samba internal directories are owned by root
- [NAS-112912] - Lost WebUI and SSH access on SCALE
- [NAS-112913] - JIRA categories can not be retrieved using oauth token
- [NAS-112920] - "The reporting database is broken" message appears for irrelevant errors
- [NAS-112922] - fix service restart on SCALE HA
- [NAS-112924] - Investigate improving restore functionality of k8s cluster
- [NAS-112939] - Fix cluster tests
- [NAS-112947] - Investigate failures with support.attach_ticket endpoint
- [NAS-112950] - Allow booting TrueNAS CORE from GRUB menu
- [NAS-112953] - remove __nfsv4link from sysdataset plugin
- [NAS-112960] - Convert ldap start stop to job
- [NAS-112961] - failover.force_master broken on SCALE HA
- [NAS-112967] - Add basic set of clustered LDAP tests
- [NAS-112971] - user.update ignores missing home directory
- [NAS-112976] - Webui submits invalid alert policy when "IMMEDIATELY" is selected
- [NAS-112978] - Add ability to query ntp peers
- [NAS-112981] - Update webui to follow job_id returned by ldap.update() in master
- [NAS-112982] - Add method to get cluster-wide time info
- [NAS-112993] - [SCALE] Syslog lvl "Is Debug" not working
- [NAS-112998] - Make sure we don't iterate over none object
- [NAS-113003] - NextCloud PHP memory limit set to 2 MB for CLI commands
- [NAS-113006] - Improve ad idmap validation
- [NAS-113008] - Unable to promote dataset/zvol clones in SCALE 21.08-BETA.2
- [NAS-113009] - Update machinaris to correctly configure worker address
- [NAS-113013] - Bug fix for correctly retrieving k8s secret after creation
- [NAS-113025] - remove unused code and clean-up info_linux.py
- [NAS-113026] - remove unused code and clean-up lag_linux.py
- [NAS-113028] - remove used code and clean-up type_linux.py
- [NAS-113032] - more validaiton to failover.events.validate()
- [NAS-113034] - less verbose about sql related logs in journal_ha
- [NAS-113048] - SCALE - Apps - Sometimes show as nothing installed after updating an app
- [NAS-113052] - Can't update TrueNAS Scale 21.08 Beta 2 to 22.02 RC1. Stuck on ZFS import.
- [NAS-113053] - Add Cron Job, but schedule is lost upon save
- [NAS-113054] - Add basic auto-configuration for non-OpenLDAP LDAP servers
- [NAS-113056] - Kubernetes won't start after upgrade to 22.02-RC.1
- [NAS-113058] - Core files for the following executables were found: /usr/sbin/smbd
- [NAS-113059] - Re-initialize docker dataset on k8s cluster restore
- [NAS-113060] - Allow mocking methods in integration tests
- [NAS-113064] - UPS Service crashes with repeated errors in console log
- [NAS-113070] - Bug fix for running tests in CI
- [NAS-113071] - Installer does not activate legacy boot partition
- [NAS-113073] - Bypass validation in OROperator if value matches default
- [NAS-113075] - Only adjust "ldap ssl" parameter in idmap backend if AD enabled
- [NAS-113076] - 22.02-RC.1 fresh install not working (middleware doesn't start)
- [NAS-113083] - Unable to upgrade from 21.08-BETA.2 to 22.02-RC.1
- [NAS-113084] - macOS Safari TrueNAS FavIcon/TouchIcons
- [NAS-113089] - Fix WebUI CI
- [NAS-113092] - Default idmap options to empty dict
- [NAS-113093] - zectl activate randomly fails the first time it's called (2nd time works)
- [NAS-113094] - remove hdd standby force radio box in SCALE webUI
- [NAS-113098] - Remove FreeBSD lsiget util

- [NAS-113107] - Use valid data for test_230
- [NAS-113115] - Hover in enclosure UI / disks not clickable on some resolutions
- [NAS-113126] - No jobs are available. Please be patient...
- [NAS-113127] - Task Manager → Active → Shows only 10 jobs
- [NAS-113129] - Unable to rename boot environments
- [NAS-113133] - Allow updating anything to MASTER release
- [NAS-113134] - Allow call("pool.query", [], {"extra": {"is_upgraded": true}}) to avo…
- [NAS-113135] - Storage page: Do not call pool.is_upgraded in a loop
- [NAS-113138] - GUI does not allow bond interfaces to be members of a bond (works on command line)
- [NAS-113144] - Stuck on boot. middleware not running
- [NAS-113157] - Fix ordering of crossrename and recycle.
- [NAS-113158] - SMBD Core File
- [NAS-113175] - Remove chart context added when doing validation
- [NAS-113180] - Blacklist `interfaces` global parameter in SMB config
- [NAS-113182] - Inputs on login page look weird when password is saved
- [NAS-113189] - Fix TrueNAS ZFS CI workflow
- [NAS-113190] - Allow checking out all repos by providing an override
- [NAS-113194] - usb-devices not implemented in freenas-debug for SCALE
- [NAS-113196] - Dashboard Memory and CPU Widgets stop updating and show "spinners"
- [NAS-113207] - Failed to parse IPMI
- [NAS-113214] - Kubernetes won't start after upgrade to 22.02-RC.1-1
- [NAS-113223] - cluster.utils.resolve_hostnames TypeError crash
- [NAS-113237] - add more unit tests for dmi parsing
- [NAS-113244] - Disks being listed are suffering from weird caching issues?
- [NAS-113246] - Time Machine SMB share not accessible
- [NAS-113249] - GUI does not show configured network interface MTU
- [NAS-113251] - middlewared to core dump
- [NAS-113252] - Show correct choices for ups ports
- [NAS-113257] - Unable to deploy Plex App on TrueNAS Scale -taint {ix-svc-start: }
- [NAS-113258] - Unable to continue after replication task fails
- [NAS-113268] - Mark macvtapX as an internal interface
- [NAS-113272] - Do not repeatedly log same error
- [NAS-113275] - [SMB 22.02.RC.1-1] - TimeMachine cannot find backup disk even after restarting avahi
- [NAS-113276] - TrueNAS ISO Image does not boot in UEFI mode when written with Rufus
- [NAS-113280] - `{"ha_sync": False}` option for queries that should not be synchroniz…
- [NAS-113281] - dont run ssh.save_keys if nothing changed
- [NAS-113282] - Locked ZFS Encrypted Dataset visible on network and can be written to creating data leak
- [NAS-113283] - Provide iso chroot env with custom built packages
- [NAS-113287] - Fix `Attribute` constructor arguments typos and fix the bug that made…
- [NAS-113288] - Fix a couple of incorrect schemas
- [NAS-113292] - Datasets disappear when encrypted options are opened
- [NAS-113304] - VM loses internet connectivity
- [NAS-113305] - Do not check for an updated docker tag if tag is using digest
- [NAS-113308] - netif.create_interface races with netif.list_interfaces
- [NAS-113312] - fix smb cluster api tests
- [NAS-113316] - fix event that is sent when gluster vol is deleted
- [NAS-113327] - fix cluster smb api tests (round 2)
- [NAS-113338] - Some groups and users created by the user are not displayed in the ACL permissions setting interface
- [NAS-113348] - Drag and drop sometimes breaks on group members list
- [NAS-113352] - Make sure SED disks are unlocked on HA systems
- [NAS-113359] - Minio service deletes bucket metadata on startup
- [NAS-113365] - Update payload for catalog.items job in api tests
- [NAS-113370] - [SCALE] Add return button on the "Unlock Datasets" popup
- [NAS-113375] - SCALE - Disks - Name Tooltip incorrect
- [NAS-113396] - smbd dumps core whed accessing manualy mounted fs
- [NAS-113397] - Partially received snapshot is saved
- [NAS-113400] - timeout ix-zfs.service after 15mins at boot time
- [NAS-113418] - [SCALE] Dashboard statistics don't load fully
- [NAS-113420] - simplify SCALE HA duplicate failover event logging
- [NAS-113427] - missing f-string formatter in cluster.localevents
- [NAS-113443] - system.is_stable
- [NAS-113447] - Apps can't access files after fresh install and import of pool
- [NAS-113452] - filesystem.statfs incorrectly identifies filesystem types
- [NAS-113468] - Only run nscd when LDAP is enabled
- [NAS-113473] - Add acls to debug
- [NAS-113474] - First time update UI doesn't allow apply updates and reboot checkbox
- [NAS-113475] - Error activating BE
- [NAS-113487] - Have humanized app version for history of chart releases
- [NAS-113518] - mDNS stops working when specifying SMB interface bindings
- [NAS-113561] - fix fstype parsing in filesystem.statfs
- [NAS-113564] - Installer doesn't UEFI boot
- [NAS-113568] - Network UPS Tools missing SNMP driver
- [NAS-113574] - Skip statfs check on SMB path if it does not exist
- [NAS-113576] - use PAM in sshd_config when AD is configured to allow PAM
- [NAS-113577] - Fix handling of partially replicated snapshots
- [NAS-113589] - Selecting single source directory for cloud sync behaves incorrectly
- [NAS-113592] - Generate new user `uid` before chowning his home directory to that uid
- [NAS-113607] - Cloud Sync Tasks can't be loaded on Data Protection dashboard
- [NAS-113608] - Fix job progress statement for ctdb plugin
- [NAS-113631] - Fix bug in initializing hwm in winbindd_idmap.tdb

- [NAS-113632] - Ensure rid value consistency between user/group name changes
- [NAS-113662] - Add debian debug mirror to nightlies apt soruces
- [NAS-113758] - Bug fix for encryption summary of dataset
- [NAS-113791] - Allow empty fromemail
- [NAS-113890] - Fix KeyError: 'naming-schema'

22.02-RC.1-2

22.02-RC.1-2

November 23, 2021

iXsystems is pleased to announce the availability of TrueNAS SCALE 22.02-RC.1-2! This is a maintenance release that includes Samba security updates, WebUI form improvements and fixes a regression with TrueCommand clustering.

Improvement

- [NAS-113322] - Allow closing slide-in forms with Escape key
- [NAS-113195] - Jira Ticket for Samba 4.15.2 and 4.13.14 Security Releases
- [CVE 2021-25717] - TrueNAS Security Notice for Samba CVE
- [CVE 2020-23192] - TrueNAS Security Notice for Samba CVE
- [CVE 2020-2124] - TrueNAS Security Notice for Samba CVE

Bug Fixes

- [NAS-113417] - fix event that is sent when gluster vol is deleted
- [NAS-113223] - cluster.utils.resolve_hostnames TypeError crash
- [NAS-113144] - Stuck on boot. middleware not running

22.02-RC.1-1

22.02-RC.1-1

November 4, 2021

iXsystems is pleased to announce the availability of TrueNAS SCALE 22.02-RC.1-1! This is a maintenance release that fixes ZFS pool import issues.

Bug Fixes

- [NAS-113052] - Can't update TrueNAS Scale 21.08 Beta 2 to 22.02 RC1. Stuck on ZFS import.

22.02-RC.1

22.02-RC.1

October 26, 2021

TrueNAS SCALE reached an important milestone today when TrueNAS SCALE 22.02-RC1 was released after 12 months of Alpha and Beta testing by over 4,000 TrueNAS Community members. This release includes scale-out file and object (S3) storage services as well as a wide range of containerized applications, supported on a Kubernetes platform.

TrueNAS SCALE is an Open Source Hyperconverged Infrastructure (HCI) project that began its journey as an Alpha release in October 2020 with the now-delivered promise of:

- Scale-out ZFS
- Converged Compute and Storage
- Active-Active Reliability
- Linux Containers (Kubernetes) & VMs (KVM)
- Ease of Deployment and Operation

The scale-out capabilities extend to both file (clustered SMB, Glusterfs) and object storage (S3 API with Minio) and do not force users to choose between file and object storage. After 12 months of enthusiastic development and testing, it is now being deployed in many applications and has about 100 PB under management. The Release Candidate (RC) phase is the start of more widespread deployment which will grow as further updates are provided.

We appreciate the community feedback and bug reports and hope to get all those features to RELEASE quality faster. A special thanks also goes to the large number of awesome community members who joined the development and test team. We've really appreciated your contributions and teamwork and it has greatly contributed to the accelerated development process.

Improvements

- [NAS-104564] - Add smbtorture regression tests for ix-developed SMB VFS modules
- [NAS-110194] - Strings with variables are untranslatable
- [NAS-110196] - Add an HTML linter
- [NAS-110406] - Improve yarn.lock workflow
- [NAS-110472] - Lint commit messages
- [NAS-110498] - Enable another 2 linter rules
- [NAS-110838] - Start designing better ways of working with forms or tables
- [NAS-111064] - Refactor tooltips in webui
- [NAS-111091] - Refactor any small form to reflect new coding practices
- [NAS-111179] - improve system.dmidecode_info
- [NAS-111196] - Document return type(s) of public endpoints of filesystem plugin
- [NAS-111290] - Red service status on share dashboard with no shares
- [NAS-111447] - Update filesystem.default_acl_choices to accept path
- [NAS-111466] - Add tests to Acl Editor
- [NAS-111467] - Add tests to Task Manager
- [NAS-111537] - Allow job dialog to collapsed
- [NAS-111567] - Change Patch object to reflect name correctly in schema
- [NAS-111574] - Real-time updates on the Storage widget
- [NAS-111590] - Validate gateway specified for kubernetes
- [NAS-111625] - Add ensure_display_device field in the UI for vms
- [NAS-111638] - Upgrade to Angular 11
- [NAS-111639] - Improve type safety in Apps
- [NAS-111640] - Split FieldConfig into separate interfaces
- [NAS-111641] - Type EntityWizard configuration
- [NAS-111643] - Standartize terminal components
- [NAS-111644] - Add type information to failover endpoints
- [NAS-111645] - Correct some of the template errors
- [NAS-111662] - W32 - Improving type safety
- [NAS-111717] - Layout improvements for Shares dashboard
- [NAS-111746] - Upgrade catalog_update vm to 21.04 ubuntu
- [NAS-111842] - Sync improvements for Data Protection Dashboard
- [NAS-111852] - Improvements to retrieving catalog(s)
- [NAS-111875] - W34 - Improving type safety
- [NAS-111882] - SCALE: Merge Linux v5.10.58
- [NAS-111905] - Update text on submit button
- [NAS-111919] - Improvements for disabled checkbox
- [NAS-111943] - Huge titles on Reports
- [NAS-111949] - Add rsync modules to usage stats plugin
- [NAS-111964] - Enable fullTemplateTypeCheck
- [NAS-112000] - OpenZFS 2.1.1 patch set
- [NAS-112006] - Improve type safety of core events
- [NAS-112010] - Improve type checking in templates
- [NAS-112011] - Update to Angular 12
- [NAS-112080] - Remove non-common properties from BaseFieldConfig
- [NAS-112081] - Do not send lots of "removed" messages when moving apps pool
- [NAS-112094] - Impossible to delete a vm if something happened to its dataset
- [NAS-112095] - W36 - Improving type safety
- [NAS-112108] - Do not show vms in the UI if system does not support virtualization
- [NAS-112119] - deprecate custom "options" for interfaces on scale
- [NAS-112128] - Template and dialog service calls cleanup
- [NAS-112138] - Remove `services_restart` from `pool.dataset.unlock` call
- [NAS-112144] - M30 support in Enclosure UI
- [NAS-112156] - add more unit tests for dmidecode
- [NAS-112199] - Fix some of untranslatable messages
- [NAS-112205] - Simplify ModalService
- [NAS-112239] - Add support in UI for R20B
- [NAS-112247] - add init_gluster to cluster API pipeline
- [NAS-112248] - setup pytest for cluster API unit tests
- [NAS-112249] - update license alert to detect M30
- [NAS-112271] - W37 - Improving type safety
- [NAS-112292] - change ixsystems/releng to call --initialize-gluster flag
- [NAS-112295] - call pytest instead of pytest-3 in cluster API tests
- [NAS-112308] - Finish refactoring of localization form
- [NAS-112309] - Make an example of user combobox
- [NAS-112341] - remove osc related code in network plugin
- [NAS-112359] - MTU validation is too restrictive
- [NAS-112382] - CLI Shortcut (Network): Create Bridged interface
- [NAS-112399] - Sync styles for Network and Storage widgets
- [NAS-112400] - midcli doesn't flush systemd messages logged on console
- [NAS-112405] - remove the "Options" field in the network settings in webUI
- [NAS-112407] - W38 - Improving type safety
- [NAS-112409] - lagg member validation broken on SCALE
- [NAS-112414] - Enable no-for-in-array linter rule
- [NAS-112416] - Enable additional linter rules
- [NAS-112431] - Enable @typescript-eslint/no-this-alias linter rule
- [NAS-112432] - Enable @typescript-eslint/no-unused-expressions linter rule
- [NAS-112433] - Enable no-restricted-globals linter rule
- [NAS-112437] - remove scan_vrrp from network.py
- [NAS-112440] - clean up disk.get_reserved on SCALE
- [NAS-112442] - bridge and lagg member choices methods are wrong on SCALE

- [NAS-112446] - rewrite core dump handling on SCALE
- [NAS-112485] - Remove some of unused code
- [NAS-112524] - Do not allow user to navigate to next step if current has errors in Apps
- [NAS-112537] - W39 - Improving type safety
- [NAS-112557] - Should we provide a kind of "shortcuts" in new CLI
- [NAS-112570] - Make "Dismiss all alerts" easier to find
- [NAS-112572] - Enable additional linter rules
- [NAS-112573] - Add tests for FormatDateTimePipe
- [NAS-112586] - Add test harnesses to new ix-form components
- [NAS-112587] - Remove support for legacy encryption from webui
- [NAS-112612] - Enable @typescript-eslint/prefer-for-of
- [NAS-112613] - Enable @typescript-eslint/prefer-includes
- [NAS-112617] - Implement new form checkbox
- [NAS-112627] - DiskStats does not scale
- [NAS-112657] - use casefold() for hostname validation in gluster API tests
- [NAS-112674] - Expose Chia node port for the app
- [NAS-112689] - Improve i18n support
- [NAS-112722] - SCALE: Merge Linux v5.10.70

New Feature

- [NAS-107006] - Display job description in task manager
- [NAS-111632] - SCALE 21.06 BETA: KVM change machine type
- [NAS-111692] - Add application for guydavis/machinaris
- [NAS-111896] - setup QE infrastructure for testing SCALE cluster
- [NAS-112123] - create "run-cluster-tests.py"
- [NAS-112161] - Request to include python3-pip
- [NAS-112246] - change ixsystems/releng repo to call run-cluster-tests.py in pipeline
- [NAS-112602] - create systemd.link file to rename ntb network device
- [NAS-112603] - fix internal heartbeat code for m-series ntb device on SCALE

Epic

- [NAS-112342] - remove complexity of network API on SCALE
- [NAS-112600] - ntb driver is written for SCALE so need to plumb in middleware code

Bug Fixes

- [NAS-109873] - Empty graphs in Reporting: CPU, Disk, Memory, System, ZFS
- [NAS-110483] - Interface allows creation of child dataset on read-only dataset
- [NAS-110863] - Fix scrollbar on Shares Dashboard
- [NAS-110864] - UI issues on Advanced Settings for Isolated PCI Ids
- [NAS-111123] - Not an integer when trying to generate a private key for a ssh connections
- [NAS-111276] - VMware Snapshot Not Being Removed from vSphere 7
- [NAS-111289] - reporting.realtime updates are received on all pages
- [NAS-111393] - pool health UI shows both green and red checkmarks while resilvering and removing mirror
- [NAS-111397] - untilDestroyed bugs on DiskListComponent
- [NAS-111420] - SCALE 21.06 BETA: Cirrus video device in libvirt xml when removing all emulated displays
- [NAS-111445] - Exceptions are not handled when using folder selector
- [NAS-111491] - ARC size tunable set incorrectly
- [NAS-111499] - "Next Run" in Cloud Sync Tasks does not sort properly
- [NAS-111526] - [SCALE] timemachine and samba issues
- [NAS-111529] - Imported CA Certificates not trusted by system
- [NAS-111540] - cron jobs for CloudSync tasks with encrypted destinations are not created after dataset is unlocked
- [NAS-111621] - No usable error when trying to add smb idmap
- [NAS-111627] - Change text of update dialog of apps
- [NAS-111634] - Syslog TLS misconfigured
- [NAS-111702] - SMB acces problem
- [NAS-111711] - Replication says finished, but actually has error
- [NAS-111716] - Fix dataset delete dialog
- [NAS-111718] - [SCALE 21.08 Nightly - Launch Docker Image] DNS Policy dropdown should show full description
- [NAS-111719] - Error loading module '/usr/lib/x86_64-linux-gnu/samba/vfs/zfsacl.so'
- [NAS-111731] - Locked cloud sync and rsync tasks are displayed as PENDING
- [NAS-111733] - Locked shares are displayed normally
- [NAS-111751] - Not showing that we are retrieving catalog data in UI
- [NAS-111782] - Replication says finished, but actually has error - cannot receive incremental stream
- [NAS-111823] - SCALE Can't delete boot environment
- [NAS-111835] - duplicate webUI entries on 21.06-BETA.1
- [NAS-111838] - Move LDAP client code into explicit service plugin
- [NAS-111858] - TrueNAS-12.0-U4.1 alert email set for 'warning' and 'immediately' but for failed SSH logins is sending the alert daily (at midnight)
- [NAS-111869] - Add configurable ACL templates
- [NAS-111877] - Infinite loading when switching to Rsync Module
- [NAS-111878] - TextLimiter directive prevent values from change detection updates
- [NAS-111881] - catch NoSuchDevice in ethtool
- [NAS-111884] - Fix unnecessary re-rendering on Sharing dashboard
- [NAS-111885] - /auth/check_user always returns false
- [NAS-111899] - Export compile_name_regex to be used in TrueNAS middleware
- [NAS-111902] - Remove dependency on samba3 loadparm context

- [NAS-111910] - Remove invalid auxiliary parameter from test payload
- [NAS-111917] - Avoid generating invalid krb5.conf
- [NAS-111920] - Run corefile alert every 6 hours instead of every 5 minutes
- [NAS-111921] - Add validation to ensure that packages only build from truenas organisation
- [NAS-111922] - Fix displaying percent value
- [NAS-111924] - Investigate why table header and rows gets huge
- [NAS-111925] - Fix regression in kerberos config generation
- [NAS-111927] - Update preferred trains default value for catalog
- [NAS-111934] - Move loglevel mapping conversion to compress method
- [NAS-111935] - Do not retrieve old catalog.items jobs when querying up catalogs
- [NAS-111938] - Create idmap service to wrap around winbind
- [NAS-111940] - [SCALE] Storage > Apply Permissions Recursively checkbox Is not getting checked & applied
- [NAS-111944] - Unrecoverable crash when upgrading from CORE to SCALE
- [NAS-111947] - Remove additional unused mDNS service types
- [NAS-111954] - Fix GMail thread safety
- [NAS-111958] - Properly retrieve snapshots in bootenv plugin
- [NAS-111966] - Disk I/O Performance is Null
- [NAS-111968] - Impossible to remove all permissions in trivial permissions editor
- [NAS-111970] - Remove unnecessary validation for SMB password
- [NAS-111971] - Linted files are not added to the same commit
- [NAS-111973] - Can't delete dataset(s)
- [NAS-111975] - [SCALE] Can't convert POSIX Dataset into NFSv4 Dataset
- [NAS-111983] - Some tables don't have left margin anymore
- [NAS-111984] - typos in task error messages
- [NAS-111988] - Fresh TrueNAS SCALE boot: samba-related middleware exceptions
- [NAS-111990] - Wait for permissions job to finish during dataset creation
- [NAS-111992] - Log parameter lookup failures due to missing config file
- [NAS-111993] - Shift wsdd setup to post_init
- [NAS-111994] - Do not allow host networking to be enabled when external interfaces are supplied
- [NAS-111995] - Fix out of order operations in applying smb config
- [NAS-111997] - Properly retrieve registry config and ACLs in SMB debug
- [NAS-112001] - Deprecate heimdal portion of kerberos plugin
- [NAS-112003] - All application data lost when changing pools
- [NAS-112004] - [SCALE] Can't save changes to VMs general settings because the UI wants a GPU to be selected
- [NAS-112005] - Sync catalogs before trying to validate them
- [NAS-112007] - Fix system dataset setup
- [NAS-112008] - Remove unused code in vm plugin
- [NAS-112009] - Update nvidia device plugin tag
- [NAS-112012] - It is possible to start a manual S.M.A.R.T. test for disk that does not support tests
- [NAS-112013] - Storage Widget on Dashboard Reporting Incorrect Values
- [NAS-112017] - Unable to use GPU in apps/charts
- [NAS-112018] - Fix pool export
- [NAS-112019] - Issues when migrating system dataset
- [NAS-112020] - Copies must be a string when it is
- [NAS-112022] - Artifacts when scrolling reporting graphs
- [NAS-112029] - Performance drop is sometimes blocked by top menu bar
- [NAS-112032] - Fix check for whether advanced flags are inherited
- [NAS-112033] - Remove clear button from disabled inputs
- [NAS-112034] - Add smb data to account plugin
- [NAS-112035] - Fix unit tests
- [NAS-112036] - Schema unit tests are failing
- [NAS-112037] - Chart releases unit test is failing
- [NAS-112038] - media user issues (duplicate entry, wrong uid/gid)
- [NAS-112039] - Wait for sync job to complete
- [NAS-112040] - [SCALE] Can't unlock encrypted pool
- [NAS-112049] - Properly initialize service announcements on boot
- [NAS-112082] - Sidebar is not scrollable on a small screen
- [NAS-112083] - Fix infinite restart on main CLI when middleware is not running
- [NAS-112089] - Add returns to filesystem acl
- [NAS-112090] - Add dump endpoint for or-operator schema
- [NAS-112097] - fix filesystem.statfs (round 2)
- [NAS-112101] - Add regression tests for ACL templates
- [NAS-112107] - Add endpoint clarifying why virtualization is not supported
- [NAS-112109] - Handling broken reporting database
- [NAS-112111] - Update group api tests to use 'additional_information'
- [NAS-112112] - query SMB information through user plugin in tests
- [NAS-112117] - .zshrc missing on SCALE
- [NAS-112118] - Clearing reporting database should not be offered when "Report CPU usage in percent" is changed
- [NAS-112130] - Allow using OROperator directly in accepts
- [NAS-112133] - Build custom collectd
- [NAS-112136] - Add returns decorator to kerberos methods
- [NAS-112137] - SHM Arguments for Containers
- [NAS-112140] - Nextcloud upgrade failed
- [NAS-112141] - smb.configure fails
- [NAS-112148] - Add test for complex groupmap behavior
- [NAS-112154] - SCALE: Applications startup even when host path volume is on locked encrypted dataset
- [NAS-112157] - Properly check if system supports virtualization
- [NAS-112158] - [SCALE] NFSv4 permissions are not applied recursively
- [NAS-112159] - Fix activedirectory idmap cache generation
- [NAS-112163] - Properly apply default SMB acl on dataset creation

- [NAS-112164] - Correctly generate nut.conf
- [NAS-112166] - Snapshot UI Hangs forever
- [NAS-112167] - Do not generate username map unless required
- [NAS-112169] - Check for SMB share registry entry before cleanup in delete
- [NAS-112170] - Fix validation for MS account
- [NAS-112181] - Pi-Hole on TrueNAS-21.08-BETA.1
- [NAS-112186] - [SCALE] App Stop "stuck", doesn't register when using Loadbalancer
- [NAS-112192] - ClusterFirst DNS not connecting to external addresses.
- [NAS-112197] - Update iX apt mirrors to not reference "unstable"
- [NAS-112225] - SMART disabled for disks behind SATL
- [NAS-112228] - Slide-in forms do not fit mobile device display
- [NAS-112229] - Add handling for ZFS cmd returning '-' for quota / used
- [NAS-112236] - Fix validation of auxiliary parameters for SMB shares
- [NAS-112238] - Application events order changes order on every button or mouse click
- [NAS-112240] - App fails to deploy because of failing nvidia-device-plugin
- [NAS-112257] - Fix issue unix tokens for local users
- [NAS-112263] - LACP bond does not activate (works using command line)
- [NAS-112264] - MTU (jumbo frame) settings from GUI ignored; works on command line
- [NAS-112269] - [SCALE] (2) Can't save changes to VMs general settings because the UI wants a GPU to be selected
- [NAS-112272] - definitions/nodeIP not working
- [NAS-112273] - UPS email configuration reports "Field was not expected"
- [NAS-112274] - GUI configuration for UPS description requires explicit quotes
- [NAS-112280] - smbd throws core dump
- [NAS-112282] - "Create Snapshot" GUI "recursive" checkbox text label missing
- [NAS-112283] - Console MOTD Banner field not wrapping text
- [NAS-112284] - Disabling (rather than deleting) a Time Machine SMB share does not stop its MDNS announcement.
- [NAS-112289] - "attach" or "expand" does not show in storage options
- [NAS-112290] - Recently changed boot drive, network stats no longer show
- [NAS-112291] - remove item_method decorator from gluster volume plugin
- [NAS-112293] - fix cluster tests (missed local commit)
- [NAS-112294] - Add LDAP_DN attribute for middleware schema
- [NAS-112296] - GRUB install: error: filesystem 'zfs' doesn't support blocklists
- [NAS-112298] - Reboot Link
- [NAS-112300] - zilstat not functional on SCALE
- [NAS-112312] - [SCALE] App Upgrade Changelog field very small on bigger screens
- [NAS-112314] - Prevent permissions changes to contents of ix-applications
- [NAS-112317] - Upgrade rclone to 1.56.0 to resolve Google API issue
- [NAS-112319] - Fix External PR Docker Build on GitHub
- [NAS-112329] - Preferences not being saved and potentially other bugs
- [NAS-112336] - WebUI and middleware use different range checks for VLAN tags
- [NAS-112340] - Quick fix the first time notice popup issue
- [NAS-112352] - Broadcast address zero for network interfaces
- [NAS-112357] - smart.test.disk_choices returns disks that do not support smart tests
- [NAS-112363] - webUI needs to send ip address type information
- [NAS-112373] - fix address/mixin.py typo
- [NAS-112378] - Services page is broken
- [NAS-112383] - Reboot as part of Scale Nightly Upgrade always results in Unscheduled Reboot Warning
- [NAS-112397] - Python script failure during Cloud Sync Task with Microsoft Onedrive, error: "InvalidAuthenticationToken: Unable to initialize RPS"
- [NAS-112398] - Shadow copies not visible via SMB
- [NAS-112410] - Fix full groupmap test
- [NAS-112420] - middleware prevents valid bridge configuration on SCALE
- [NAS-112423] - Cloud Sync Form is broken
- [NAS-112424] - Fix delete message on Shares
- [NAS-112425] - Cloud Sync Tasks should show "Disabled" instead of a "Next Run" time if task is disabled
- [NAS-112428] - Disable Hardware Offloading shows TrueNAS Core text
- [NAS-112429] - Deleting snapshots is not reflected in GUI when search is performed
- [NAS-112430] - core dump after migrating from TrueNAS Core 12.0-U5 to TrueNAS SCALE Beta 21.08
- [NAS-112434] - Fix abort button on job item component
- [NAS-112435] - Poor looking cloud sync error dialog
- [NAS-112468] - Update middleware for samba changes in 4.15
- [NAS-112470] - Build with Samba 4.15
- [NAS-112481] - Booting on a network without a DHCP server results in a funky console.
- [NAS-112482] - Failed login SSH using Domain Admin account
- [NAS-112489] - Remove osc from plugins/reporting/update.py
- [NAS-112490] - Failed to access Homes Directory for Domain Users
- [NAS-112518] - Dump errors to stderr in noninteractive mode and exit with code 1 on …
- [NAS-112519] - Send proper ClientException for a job exception
- [NAS-112520] - Improve factory reset speed and display progress
- [NAS-112521] - Remove SSH keys
- [NAS-112522] - KeyError in coredump.py plugin
- [NAS-112526] - EntityJobComponent regression
- [NAS-112531] - Alter behavior of restrict_pam key for AD plugin
- [NAS-112533] - Fix automatic home directory creation
- [NAS-112535] - Display nice error in YAML error dialog
- [NAS-112536] - Print nicer job progress
- [NAS-112546] - IPv6 has incorrect http port on CLI
- [NAS-112554] - Unable to Create OpenVPN Server/Client Certificate
- [NAS-112560] - Preserve whitespaces for traceback output
- [NAS-112567] - Raise error if SMB client connection fails for shadow copy test

- [NAS-112577] - hook_setup_ha endless loop
- [NAS-112581] - SCALE won't boot "Failed to start `Save SSH keys`"
- [NAS-112583] - "MirrorEstimated raw capacity"
- [NAS-112584] - Fix logic for path_suffix removal
- [NAS-112588] - Add clear button on the search field
- [NAS-112596] - SCALE Can't clear UPS Alerts (critical and info)
- [NAS-112597] - The system returned the following error - [object Object]
- [NAS-112598] - Only run interactive editor if we requested so explicitly
- [NAS-112605] - Ensure we have clean state for SMB VSS tests
- [NAS-112608] - systemdataset.setup is broken on scale HA
- [NAS-112628] - Adjust site-specific kerberos info for API usage change
- [NAS-112629] - TrueNAS SCALE Enterprise login window says "TrueNAS SCALE_ENTERPRISE ® © 2021"
- [NAS-112631] - APPS: Mismatch colors on charts badge
- [NAS-112632] - Start / stop idmap service when clearing idmap cache
- [NAS-112633] - Fix colors for Directory Services Monitor popup
- [NAS-112634] - Same SMB SIDs are assigned twice
- [NAS-112640] - NFS-Ganesha fails on alias change
- [NAS-112643] - Fix job width on Task Manager
- [NAS-112669] - Fix SMB config generation issues when clustered
- [NAS-112686] - Do not wipe host address bits when setting network interface alias
- [NAS-112687] - Unable to create CSR in the UI
- [NAS-112688] - Expose current interface addresses in `network interface query`
- [NAS-112701] - Address issues in ctdb public ip generation
- [NAS-112703] - Expand usage of ads domain info
- [NAS-112719] - Unable to verify or use mega.nz cloud creds
- [NAS-112721] - Add API call to create directories
- [NAS-112725] - SCALE: Remove feature@xattr_compat
- [NAS-112746] - Use specified smartd polling `interval`
- [NAS-112747] - Address multiple issues with clustered active directory
- [NAS-112748] - Safely consume state key in vm event
- [NAS-112749] - ethtool.from_netlink log spam
- [NAS-112780] - Migration from CORE to SCALE results in a corrupted install of SCALE
- [NAS-112786] - remove the `Alias` dialog box in nfs sharing form
- [NAS-112799] - rrdcached plugin spamming logs on SCALE
- [NAS-112873] - Add validation to internal kerberos.get_cred method
- [NAS-112920] - "The reporting database is broken" message appears for irrelevant errors

21.08-BETA.2

21.08-BETA.2

October 8, 2021

TrueNAS SCALE 21.08-BETA.2 has been released! This is a maintenance release that includes an undisclosed security update and improvements for SMB/NFSv4 protocols while development looks ahead to the upcoming SCALE 22.02-RC.1 release later this month.

We appreciate the community feedback and bug reports and hope to get all those features to RELEASE quality faster. A special thanks also goes to the large number of awesome community members who joined the development and test team. We've really appreciated your contributions and teamwork and it has greatly contributed to the accelerated development process.

Bug Fixes

- [NAS-112141] - smb.configure fails
- [NAS-112158] - [SCALE] NFSv4 permissions are not applied recursively

21.08-BETA.1

21.08-BETA.1

August 31, 2021

TrueNAS SCALE 21.08-BETA.1 has been released and includes clustered SMB (aka Windows storage) and a much improved Windows-style ACL (Access Control List) editor, building on the major iXsystems innovation of Windows-style (aka NFSv4) ACLs on Linux ZFS. With these new features, the first release ("Angelfish") of TrueNAS SCALE is largely feature complete and scheduled to go through the RC and RELEASE process in Q4 of 2021.

TrueNAS SCALE 21.06-BETA.1 had the largest community of BETA users of any previous TrueNAS or FreeNAS release with over 3,000 deployed systems and a lot of field testing. Many thanks to the thousands of community developers and testers who have contributed to the effort.

Commercial BETA trials have started for a limited number of users and are also going well. The TrueNAS R-Series platforms are the first platforms available with TrueNAS SCALE support.

TrueNAS SCALE 21.08-BETA.1 includes over 500 new features, improvements and bug fixes along with major new capabilities including:

- **Windows-style ACL Editor**: TrueNAS CORE and Enterprise support Windows-style file system ACLs (aka NFSv4 ACLs), based on OpenZFS with FreeBSD-compatible extended attributes. TrueNAS SCALE includes iXsystems enhancements to Linux which also allow importing of TrueNAS CORE & Enterprise pools while keeping the same extended attributes. With 21.08, the ACL editor in the WebUI received a large improvement in ease of use, while still supporting advanced ACL configurations. This makes it much easier for storage administrators to set up and manage ACLs in an immediately familiar way with a much smaller learning curve for new users.
- **Scale-Out SMB**: TrueCommand 2.0 provides a WebUI for TrueNAS SCALE which enables ZFS datasets to be pooled together as cluster volumes which span multiple nodes. Clustered SMB access to those clustered volumes is previewed on TrueNAS SCALE 21.08 via APIs, and will be WebUI configurable with an upcoming TrueCommand version update. This allows scale-out capacity and bandwidth as well as fault tolerance.
- **Improved System and Sharing Dashboards**: The main dashboard and the sharing dashboards have been significantly improved. The overall goal is to simplify setup and administration by reducing the steps required.
- **Enclosure Management**: Enclosure management provides visual control of specific iXsystems platforms such as the TrueNAS R-Series, with support for the Minis, M-Series, and X-Series coming soon.
- **OpenZFS 2.1**: 21.08-BETA.1 includes an updated version of OpenZFS which lays the groundwork for future file-system feature enhancements. iXsystems contributed code for better scaling of worker processes with processor cores which makes tasks such as scrubbing and resilvering behave more reliably.
- **Container Storage Interface (CSI)**: The Democratic CSI is now supported and has been improved to be all API based. This will enable more robust deployments of TrueNAS storage for kubernetes systems.
- **Application Catalog Improvement**: Third-party applications can be deployed as single (Docker) containers or “pods” of containers described with customizable Helm charts. These applications can be downloaded via catalogs like TrueCharts, which also provides a process for users to build and customize their own catalogs. The syncing and managing of catalogs has been improved and is now snappier and more robust.

The WebUI, while similar to TrueNAS CORE, has also been vastly improved with new UX enhancements which enable configuration and management of a system with far greater ease than ever before. Users will find much more relevant and important information readily available with less need to navigate through multiple pages in the interface. TrueNAS SCALE documentation has also improved significantly and includes instructions on how to sidegrade from TrueNAS CORE to SCALE. In addition, there are Developer Notes and Release Notes.

We appreciate the community feedback and bug reports and hope to get all those features to RELEASE quality faster. A special thanks also goes to the large number of awesome community members who joined the development and test team. We’ve really appreciated your contributions and teamwork and it has greatly contributed to the accelerated development process.

Epic

- [NAS-107149] - UX Improvements for SCALE
- [NAS-108215] - Integrate Gluster into Samba
- [NAS-108347] - Storage section improvements
- [NAS-108383] - Add ACLs to API keys
- [NAS-109669] - UI dependency audit
- [NAS-110668] - Sharing dashboard
- [NAS-110942] - remove lxml from SCALE

New Feature

- [NAS-100829] - Checkbox for restart services during unlock
- [NAS-107006] - Display job description in task manager
- [NAS-108291] - Investigate using SPICE instead of VNC
- [NAS-108842] - SCALE: Allow custom App catalogs
- [NAS-108922] - UI should update chart release status based on chart release events
- [NAS-110126] - Allow selecting multiple source directories for cloud sync
- [NAS-110368] - Show upgrade summary when trying to upgrade a chart release
- [NAS-110519] - New cloud sync remote: Google Photos
- [NAS-110531] - Log websocket messages in debug file
- [NAS-110543] - New replication task field: name_regex
- [NAS-110673] - Move WebDAV share form to sidebar
- [NAS-110732] - Investigate automating app versions with new upstream images
- [NAS-110764] - Implement Redesigned permissions/ACL forms
- [NAS-110938] - Network traffic chart
- [NAS-110964] - Storage Widget for Dashboard
- [NAS-110966] - Network Widget for Dashboard
- [NAS-110967] - View Permissions sidebar
- [NAS-110983] - Document best practices for chart devs
- [NAS-110984] - Document return type of events generated by middleware
- [NAS-111266] - add 2 drop-downs to network interface section
- [NAS-111267] - add endpoint for retrieving xmit_hash_policy and lacpdu_rate
- [NAS-111288] - Support R-series enclosure UI on SCALE
- [NAS-111291] - Job log page
- [NAS-111292] - Improvements for Task Manager

- [NAS-111316] - Add chelsio_adapter_config_v4 to scale
- [NAS-111331] - Use our custom chia docker image for official app
- [NAS-111340] - Allow updating stable train from test train with catalog_update
- [NAS-111395] - Add support for policy based routing for kubernetes
- [NAS-111410] - Automatically update official catalog items
- [NAS-111632] - SCALE 21.06 BETA: KVM change machine type
- [NAS-111708] - DemoCSI: Add functionality to allow deletion of all snapshots of a dataset

Improvement

- [NAS-101423] - Display available memory in VM wizard
- [NAS-106051] - Redesign Task Manager
- [NAS-108602] - Gracefully abort jobs
- [NAS-108604] - Make restarting/reloading locked attachments optional
- [NAS-108779] - Add tooltip for tips on webshell page
- [NAS-109432] - CLONE - Gracefully abort jobs
- [NAS-109677] - Update information in WebUI repo
- [NAS-110075] - Standartize how subscriptions are handled in webui
- [NAS-110116] - Improve documentation of backend endpoints
- [NAS-110264] - Remove AFP sharing (backend)
- [NAS-110275] - Bugclerk: try to set assignee for tickets created from github
- [NAS-110285] - Add interfaces to at least 5 API endpoints
- [NAS-110320] - Update welcome image
- [NAS-110383] - Various issues with new webui implementation of directory services
- [NAS-110514] - UI should show that it failed to retrieve catalogs data
- [NAS-110583] - Render ix-chart dynamically in the UI
- [NAS-110642] - zfs snapshot API - ability to update properties after snapshot creation
- [NAS-110712] - add --trace-malloc arg to middlewared
- [NAS-110798] - Investigate stopping database pods before taking snapshot during app upgrade
- [NAS-110806] - Linter: ban unused imports
- [NAS-110807] - Bugclerk should set ticket status to In review on PR
- [NAS-110808] - Linter: ban console.log
- [NAS-110820] - Allow specifying extra arguments in get_instance
- [NAS-110824] - Auto refresh application list when new Catalog is added
- [NAS-110827] - Linter: add max-len linter rule
- [NAS-110828] - Clean up entity-table
- [NAS-110835] - Remove Rest and Jails related code
- [NAS-110836] - Remove or make a plan to remove moment.js
- [NAS-110837] - Add 3 linter rules
- [NAS-110839] - Setup unit test infrastructure
- [NAS-110840] - Add typing to EntityWizard configuration
- [NAS-110841] - Make volumes-list.component.ts less bad
- [NAS-110843] - Reduce amount of `any`s in webui code
- [NAS-110848] - Allow using a specific existing snapshot for one time replication
- [NAS-110879] - Modernize webui build process
- [NAS-110887] - Enable bridge STP/RSTP on SCALE
- [NAS-110943] - remove lxml from vm/utils on SCALE
- [NAS-110944] - remove lxml from vm/supervisor/supervisor_base on SCALE
- [NAS-110945] - remove lxml from vm/pci_linux on SCALE
- [NAS-110946] - remove lxml from vm/info_linux on SCALE
- [NAS-110947] - remove python3-lxml build dependency on SCALE
- [NAS-110950] - remove unused files that reference lxml on SCALE
- [NAS-110982] - Improve error logging in case py-libzfs fails to retrieve dataset handle
- [NAS-110987] - Expose `checksum` for public APIs of ZFS info
- [NAS-110989] - UI should consume catalog.create as a job
- [NAS-111014] - Add JSON input / output support for batch net_groupmap operations
- [NAS-111036] - Intelligently set defaults for 'acl_mode'based on 'acl_type'
- [NAS-111056] - SCALE: Want system performance analysis tools
- [NAS-111058] - Add commonly used upgrade strategy versioning patterns
- [NAS-111067] - Linter: ban boxed types
- [NAS-111068] - Linter: angular-eslint
- [NAS-111079] - Improving type safety.
- [NAS-111089] - Improve type safety of resourceTransformIncomingRestData and ws jobs
- [NAS-111102] - Improve huge catalog(s) handling edge cases
- [NAS-111113] - Add option to replication run onetime to fail if target already exists
- [NAS-111114] - snapshot data in GET dataset to mimic GET snapshot structure
- [NAS-111136] - Enforce Finnish notation for observables
- [NAS-111143] - too many calls to system.info unnecessarily
- [NAS-111170] - W26 - Improving type safety
- [NAS-111173] - add a private system.hostname endpoint
- [NAS-111175] - Add ability to select common options for bond interfaces
- [NAS-111176] - traceback in unscheduled_reboot_alert on SCALE HA
- [NAS-111178] - consistent use of quotes in dmidecode_info
- [NAS-111193] - Allow upgrading CI helm chart values when using catalog update tool
- [NAS-111194] - Document return type(s) of failover plugin
- [NAS-111195] - Document return type(s) of public endpoints of replication plugin
- [NAS-111200] - Catalog sync endpoint is a job now and UI should treat it as such
- [NAS-111204] - Make chart.release.scale a job to wait for pods to be scaled up/down
- [NAS-111205] - Treat start/stop action for apps as a job in UI
- [NAS-111218] - Update SCALE to Samba 4.14.5

- [NAS-111234] - Add unit tests for EntityUtils.parseSchemaFieldConfig
- [NAS-111235] - Refactor and add unit tests to compare-validation.ts
- [NAS-111236] - Add unit tests to password-validation.ts
- [NAS-111261] - W27 - Improving type safety
- [NAS-111263] - interface return type is broken
- [NAS-111270] - Document how valid_char regex works for chart devs
- [NAS-111272] - Re-install scale-build if there are manual edits
- [NAS-111284] - Don't allow root dataset permissions to be edited
- [NAS-111290] - Red service status on share dashboard with no shares
- [NAS-111303] - CLONE - Render ix-chart dynamically in the UI
- [NAS-111312] - Removing barrel files
- [NAS-111314] - add filterable "ctdb getdbmap" to API
- [NAS-111315] - Renaming files to match naming convention
- [NAS-111328] - Merge zfs-2.1.0
- [NAS-111347] - W29 - Improving type safety
- [NAS-111386] - xattr compat cleanup
- [NAS-111414] - Treat removing vdev in the UI as a job
- [NAS-111428] - Add an alert/warning for users when they change cidr of k8s cluster in UI
- [NAS-111442] - Hard to find how to run Cron jobs manually
- [NAS-111446] - Layout improvements for Storage widget
- [NAS-111447] - Update filesystem.default_acl_choices to accept path
- [NAS-111463] - improve truenas.get_chassis_hardware on SCALE
- [NAS-111468] - New POSIX ACL editor
- [NAS-111469] - Add support for horizontal radio buttons on ACL Editor
- [NAS-111470] - Support checkbox groups for redesigned ACL editor
- [NAS-111517] - graceful addition/removal of ctdb public ip addresses
- [NAS-111528] - W30 - Improving type safety
- [NAS-111541] - W31 - Improving type safety
- [NAS-111590] - Validate gateway specified for kubernetes
- [NAS-111593] - More user-friendly CLI for network operations
- [NAS-111594] - improve wipe_disk/delete_partitions
- [NAS-111623] - Layout improvements for Network widget
- [NAS-111641] - Type EntityWizard configuration
- [NAS-111656] - KeyError in network.py on SCALE
- [NAS-111662] - W32 - Improving type safety
- [NAS-111773] - SCALE build broken after upstream packages update
- [NAS-111836] - Branch out feature in build system
- [NAS-112081] - Do not send lots of "removed" messages when moving apps pool

Bug Fixes

- [NAS-100503] - Avoid N event subscriptions to run the same code
- [NAS-102855] - ZoL user namespace xattrs are incompatible with FreeBSD and vice-versa
- [NAS-108044] - Unable to generate debug file
- [NAS-108200] - SCALE fails to import boot pool when HBA is attached
- [NAS-108277] - Truenas Scale : Installation failed if no disc is selected in menu
- [NAS-108560] - Pool status will not update unless system is restarted/system panics
- [NAS-108792] - [SCALE] Fix VNC Input
- [NAS-109021] - Dashboard widget template error
- [NAS-109165] - icons on the dashboard are not aligned
- [NAS-109335] - SCALE - samba auto-generated datasets aren't getting correct permissions
- [NAS-109476] - Full filesystem replication doesn't work incrementally
- [NAS-109485] - pam_krb5(sudo:auth): parse_name failed
- [NAS-109720] - Interrupted full replications are silently failing to resume
- [NAS-109820] - SCALE Samba group write permissions do not work
- [NAS-109976] - Changes in debug generation process
- [NAS-110008] - rsync task ceases to work after 11.3-U5 -> 12.0-U2.1 upgrade, rsync command returned 12
- [NAS-110024] - SCALE: lagg name bond0
- [NAS-110166] - Winbind does not start on boot
- [NAS-110391] - Can't mirror boot-pool
- [NAS-110404] - Main menu may disappear when resizing window
- [NAS-110405] - Impossible to open a secondary menu on mobile
- [NAS-110428] - UI in Virtualization page incorrectly reporting available system memory
- [NAS-110515] - Threadripper 1950X incorrect temperature shown
- [NAS-110575] - Wireguard Tunnel remains on passive node of HA system after failover.
- [NAS-110582] - Properly show summary of selected options in application's wizard
- [NAS-110616] - Make it more obvious how to get to Console Setup menu in Scale
- [NAS-110651] - Encryption options are not shown/set correctly after canceling "Add dataset" with passphrase encryption
- [NAS-110665] - OpenStack Swift auth_version Invalid Version
- [NAS-110671] - Middlewared is leaking enourmous amounts of memory (high CPU usage as well)
- [NAS-110703] - Many invalid opcodes reported by Kernel
- [NAS-110754] - rsync task configuration corrupted
- [NAS-110760] - Entity table multiselect doesn't respect filters or pages
- [NAS-110773] - Fix kerberos error
- [NAS-110775] - [SCALE] UI Freeze/slowdown when displaying catalog info with a lot of Apps
- [NAS-110797] - Plex providing CODEC error with transcoding
- [NAS-110802] - Double-click on Launch Docker Wizard breaks wizard
- [NAS-110812] - Issues when selecting disk during Scale installation
- [NAS-110816] - Grub config is not updated on FreeBSD bootenv activation
- [NAS-110825] - Refresh All apps job progress gets to 100% too quickly

- [NAS-110826] - inadyn is ancient and appears to be broken in Scale
- [NAS-110832] - Telegram & Email Notification Not Working
- [NAS-110833] - CertificateChecks traceback
- [NAS-110842] - openebs does not run
- [NAS-110844] - Allow retrieving snapshot(s) of dataset(s) from pool.dataset
- [NAS-110863] - Fix scrollbar on Shares Dashboard
- [NAS-110877] - Create storage class before doing helm action
- [NAS-110883] - Remove legacy FreeBSD files
- [NAS-110884] - Replication Task Wizard UI issues
- [NAS-110894] - Reinitialize udev monitor on udev polling error
- [NAS-110914] - SCALE smartd (smart | S.M.A.R.T.) not starting on Virtual Machine's
- [NAS-110927] - No UI option to change the readonly state of a ZVOL.
- [NAS-110929] - Allow retrieving catalog data partially
- [NAS-110930] - Improvements to kubernetes lifecycle
- [NAS-110931] - Raise multus log level
- [NAS-110932] - Do not attempt to query chart releases if no pool is set
- [NAS-110934] - Allow specifying environment variables independently
- [NAS-110948] - Compile errors related to @types/d3-array
- [NAS-110949] - Improve retrieving installed application(s) performance
- [NAS-110952] - Clean supervisor_freebsd reference
- [NAS-110953] - Removing ports folder
- [NAS-110955] - Add regression tests for AFP/SMB migration param
- [NAS-110957] - Out of sync data on Sharing Dashboard
- [NAS-110958] - Start libvirt before probing for cpu model choices
- [NAS-110969] - Increase verbosity of range-related idmap verrors
- [NAS-110972] - Add latest_human_version key in catalog items
- [NAS-110974] - Always update container image(s) during app upgrade
- [NAS-110976] - Print full shell pipe commands in the debug instead of obfuscated and…
- [NAS-110979] - fix 'NoneType' object has no attribute 'call_sync'
- [NAS-110980] - Make catalog.create endpoint a job
- [NAS-110981] - Volume List header misaligned after click Import button
- [NAS-110986] - Middleware in some cases unable to retrieve vm status
- [NAS-110988] - Enabling additional linter rules
- [NAS-110998] - ACL Manager shows empty page, other issues
- [NAS-111000] - S3 secret key cannot be shown (button show/hide doesn't work)
- [NAS-111006] - Submit Button for Charts Broken in 20210610 builds
- [NAS-111010] - Correctly validate root uid when retrieving user object
- [NAS-111011] - [EFAULT] Failed to wipe disks error with vdev removal
- [NAS-111012] - Perform chown() when setting POSIX1E ACL non-recursively
- [NAS-111015] - cloudsync.onedrive_list_drives called for unrelated cloud credentials
- [NAS-111016] - Document return type(s) for pool plugin
- [NAS-111017] - Allow acltype to change through middleware
- [NAS-111022] - Add validation related to legacy AFP shares
- [NAS-111025] - Unable to change Web Interface HTTP/HTTPS Port
- [NAS-111027] - Is the email field under Services/UPS superfluous?
- [NAS-111029] - GSSAPI authentication is not usable for LDAP bind
- [NAS-111038] - Fix parsing error for POSIX1E getfacl output
- [NAS-111039] - Remove strict check for path existence in AFP validation
- [NAS-111041] - SCALE: Missing cxgbetool for Chelsio NICs
- [NAS-111046] - Middleware/UI not giving optimal volblocksize for 5 wide raidz1 layout
- [NAS-111050] - Incorrect group tag when adding a mask ACL
- [NAS-111051] - Retrieve created at property for datasets/volumes
- [NAS-111060] - disk.get_unused results in an error on API Incremental CI plan
- [NAS-111063] - Document return types of ups plugin
- [NAS-111065] - Use correct API endpoint for disabling ACL on update
- [NAS-111070] - Document return type(s) of webdav plugin
- [NAS-111071] - Document return type(s) of vpn plugin
- [NAS-111073] - Fix MIT kerberos keytab handling
- [NAS-111080] - Fix Enclosure Mapping for early version Mini X 3.0 Systems
- [NAS-111081] - Fix setting default SMB ACL on dataset creation
- [NAS-111087] - Do not read/validate all catalog item versions
- [NAS-111092] - [SCALE] NFS Service settings page broken - "Field was not expected"
- [NAS-111094] - [SCALE] Add NFS share missing local groups in dropdown list
- [NAS-111096] - Synchronously sync catalog on creation
- [NAS-111098] - Manual update stuck at 0 percent from core to scale
- [NAS-111099] - Replication progress says "total 11.12 TiB of 11.04 TiB"
- [NAS-111103] - [SCALE] k3s agent fatal error
- [NAS-111118] - incorrect help dialog box on SCALE
- [NAS-111123] - Not an integer when trying to generate a private key for a ssh connections
- [NAS-111130] - Can't create Google Photos credentials
- [NAS-111132] - Fix r10 enclosures
- [NAS-111140] - SCALE 21.06 BETA: Error after imported pool from CORE
- [NAS-111144] - CLI: python exception while typing storage subcommand
- [NAS-111145] - CLI: python exception when unknown binary specified in EDITOR env var
- [NAS-111163] - Unable to revoke certificate from OpenVPN Server Service access
- [NAS-111164] - CLI: Query of Account -> Group does not show 'group' as viable option
- [NAS-111165] - CPU dashboard widget layout buggy with 128 thread CPU
- [NAS-111174] - Fix api tests for catalog
- [NAS-111188] - UI Debug failing to complete
- [NAS-111192] - Remove cached content of a catalog after deleting it

- [NAS-111201] - Treat openebs/zfs-driver image as system internal image
- [NAS-111202] - Properly show which image(s) would be upgraded in UI on app upgrade
- [NAS-111203] - Error(s) are not rasied by UI on app upgrade and is stuck on loop
- [NAS-111210] - Improvements to revoking a certificate/ca
- [NAS-111215] - Bug fix for validating acltype when parent ds does not exist
- [NAS-111217] - Disable containerd in systemd preset file
- [NAS-111223] - Fix R40 to comply with enclosure management nep specified single mapped enclosure to UI.
- [NAS-111226] - Mark login password as private
- [NAS-111227] - After upgrading app UI does not show newer app version in tile
- [NAS-111228] - SMBd startup fails when connecting to Active Directory
- [NAS-111229] - After rollback app UI does not show rollbacked app version in tile
- [NAS-111240] - Add `who` string to ACL output
- [NAS-111243] - Remove netatalk from build
- [NAS-111246] - Error when trying to save NFS Acl
- [NAS-111247] - Add WDS support for Win10 clients, so they can discover SCALE hosts
- [NAS-111248] - Convert JSON validation errors ValidationErrors
- [NAS-111254] - Remove API test for MULTIPROTOCOL_AFP
- [NAS-111259] - Fix R20 to comply to enclosure management NEP
- [NAS-111264] - Some themes do not display all text
- [NAS-111273] - Fix R50 to comply with enclosure NEP
- [NAS-111283] - Error when creating ubuntu vm in Scale
- [NAS-111286] - Boot environment -> Add is broken
- [NAS-111287] - Boot environment -> Clone is broken
- [NAS-111289] - reporting.realtime updates are received on all pages
- [NAS-111295] - [SCALE] hubernetes hostnames periodically become unreachable/unresponsive
- [NAS-111296] - Update certificate/ca return type entry
- [NAS-111305] - Reporting database size (1.08 GB) is larger than 1 GiB.
- [NAS-111309] - [scale]BUG with app version control
- [NAS-111317] - traceback when creating failover type bond on SCALE
- [NAS-111324] - traceback when setting default route on SCALE
- [NAS-111325] - properly handle internal interfaces when configuring default route on SCALE
- [NAS-111333] - Pool operations (creation or deletion) cause critical alerts on NVMe drives
- [NAS-111334] - CoreService Tests
- [NAS-111337] - dhclient is stopped for random interfaces
- [NAS-111339] - Add iptables rules with counters to debug
- [NAS-111342] - Unable to edit email alert service in UI
- [NAS-111343] - Additional Enclosure Fixes
- [NAS-111344] - Log error(s) if we fail to add/remove iptable rules for k8s
- [NAS-111348] - CallError from k8s when k8s isn't used
- [NAS-111350] - only log pyroute2.NDB errors
- [NAS-111353] - fix pyroute2.NDB typo
- [NAS-111360] - Add ipsets to debug
- [NAS-111368] - Bug fix for syslog log level
- [NAS-111369] - Bug fix for chart release api tests
- [NAS-111371] - Merge multiple calls for creating an SSH connection into one
- [NAS-111376] - can't disable VM autostart in GUI in 21.07-MASTER-20210703-212917
- [NAS-111390] - Enclosure Management fix for R20A.
- [NAS-111391] - View permissions sidebar doesn't appear on long lists
- [NAS-111392] - Smart Tests page does not show anything
- [NAS-111397] - untilDestroyed bugs on DiskListComponent
- [NAS-111399] - fix NDB() instantiation
- [NAS-111402] - Fix api tests for ups plugin
- [NAS-111406] - Fix for mini-3.0-xl+ 2.5 inch drive bays being swapped.
- [NAS-111415] - Update chart.release.scale api tests
- [NAS-111416] - Updated to latest nightly, TrueNAS-SCALE-21.07-MASTER-20210715-052922
- [NAS-111420] - SCALE 21.06 BETA: Cirrus video device in libvirt xml when removing all emulated displays
- [NAS-111424] - Bug fix for retrieving catalog item versions in api tests
- [NAS-111427] - Bug fix for catalog item migration handling
- [NAS-111429] - crash in ha_permission()
- [NAS-111430] - Allow running update-grub even if vdev is DEGRADED (too many errors)
- [NAS-111433] - Adding no-implicit this to introduce stricter checks.
- [NAS-111435] - NFS under "Reporting" does not show data
- [NAS-111436] - 500 on /api/docs in CI
- [NAS-111443] - mc works poorly in the Shell
- [NAS-111444] - Middleware takes up a lot of CPU
- [NAS-111460] - webUI is showing incorrect information
- [NAS-111461] - [SCALE] Tunables settings error - UI missing tunable type dropdown, defaults to 'loader'
- [NAS-111465] - User is not redirected to ACL editor after SMB home share is created
- [NAS-111482] - Add configuration entries for SMB multichannel
- [NAS-111483] - Nothing happens after testing network interface configuration changes
- [NAS-111485] - Disabling Cloud Sync tasks throws error about PoolScrub
- [NAS-111494] - deprecation warning for middleware test/api2/runtest.py
- [NAS-111496] - fix and improve webdav api tests
- [NAS-111500] - ACL type mismatch when stripping POSIX ACL
- [NAS-111505] - Add support for fuse-mounted paths to filesystem plugin
- [NAS-111511] - automatic configuration of ctdb clustering daemon
- [NAS-111531] - make sure xmit hash and lacpdu rate are reported
- [NAS-111532] - fix xmit-hash and lacpdu rate on iface update
- [NAS-111536] - Reporting database continues to grow
- [NAS-111538] - raise CallError on cluster api events

- [NAS-111542] - Traceback starting up middlewared
- [NAS-111543] - Replace netcli with new CLI
- [NAS-111556] - Bug fix for iptables getting out of sync
- [NAS-111557] - Can't Create Link Aggregation Latest Nightly TrueNAS-SCALE-21.07-MASTER-20210727-152922
- [NAS-111558] - Prevent boot installation into installation media itself
- [NAS-111560] - UI bug when going to Alerts -> Settings Cog -> Email page
- [NAS-111561] - Html appears as text in Slack alerts
- [NAS-111564] - Correct vm.query event payload to match vm_entry schema
- [NAS-111565] - UI should update vm event handling logic
- [NAS-111568] - Bug fix for collectd configuration generation
- [NAS-111570] - Wait when adding/removing iptables rules
- [NAS-111571] - Make acltype=nfsv4 the default on Linux
- [NAS-111572] - SCALE POSTINIT scripts aren't executing
- [NAS-111575] - Fix label on the Network widget
- [NAS-111576] - [scale/apps] Specific field in charts are not remembered on edit.
- [NAS-111578] - Clear cached chart releases when stopping k8s
- [NAS-111582] - Swap size should consider boot drive size
- [NAS-111583] - No Reportng Data Latest TrueNAS SCALE
- [NAS-111597] - Retrieve more useful information for app upgrade summary
- [NAS-111603] - Fix quota alert for dataset owner
- [NAS-111605] - TrueNAS SCALE MinIO App - GUI does not work
- [NAS-111613] - Improving naming convention
- [NAS-111617] - Alignment for radio buttons in Alerts > Email
- [NAS-111620] - Cannot rename boot environment
- [NAS-111621] - No usable error when trying to add smb idmap
- [NAS-111628] - Failed to check for alert CoreFilesArePresent
- [NAS-111631] - fuse mount gluster volumes with acl support
- [NAS-111633] - Bug fix for creating a zvol
- [NAS-111655] - Fix check for passdb backend type
- [NAS-111668] - Fix free space on storage widget
- [NAS-111670] - Fix DS_TYPE_LDAP idmap generation
- [NAS-111671] - Fix foreign groupmap alias removal
- [NAS-111674] - only eventsd.delete if glustereventsd is running
- [NAS-111682] - Excessive smartctl usage
- [NAS-111683] - Fix smb plugin issues causing test_435_smb_registry failures
- [NAS-111689] - Fixes for test_425_smb_protocol
- [NAS-111690] - call enclosure.query once in disk.sync_all
- [NAS-111693] - fix enclosure.sync_zpool
- [NAS-111695] - Upload config: File is bigger than 10MiB
- [NAS-111697] - Fix idmap create / delete methods
- [NAS-111703] - Add bpfcc-tools
- [NAS-111706] - Fixes for base SMB regression tests
- [NAS-111707] - DemoCSI: Allow setting refreservation and refquota properties simultaneously
- [NAS-111710] - Fix groupmap tests
- [NAS-111712] - zettarepl logs are being truncated, hindering investigation of errors.
- [NAS-111714] - Enable SMB2/3 aapl extensions prior to AFP compat tests
- [NAS-111715] - Add global parameter handling for guest access
- [NAS-111716] - Fix dataset delete dialog
- [NAS-111722] - SQL foreign key error when trying to delete a cloudsync credential
- [NAS-111726] - Chart is broken on Network widget
- [NAS-111727] - Shares tables collapse and show nothing on smaller screens
- [NAS-111734] - When a dataset is deleted, underlying resources are silently deleted too
- [NAS-111738] - Directory services FAULTED when expected DISABLED
- [NAS-111740] - Bug fix for specifying env variables for minio app
- [NAS-111741] - Stop containerd explicitly after stopping docker
- [NAS-111742] - iSCSI Targets table doesn't automatically refresh when new item is added
- [NAS-111744] - Fix SSHd IPV6 link local ListenAddress
- [NAS-111747] - Cannot add Google Drive in Backup Credentials
- [NAS-111749] - Fix IP Addresses on Network widget
- [NAS-111758] - fix IndexError in network.py
- [NAS-111762] - Remove Samba passdb binding from middleware
- [NAS-111763] - Fix homedir copy on SCALE
- [NAS-111767] - UI gets stuck when error occurs trying to create new SSH Connection
- [NAS-111768] - `replication.count_eligible_manual_snapshots gives 'index out of range' error
- [NAS-111770] - Adapt Minio app to conform to upstream configuration for TLS
- [NAS-111771] - Expose machinaris api port for workers usage
- [NAS-111772] - Fix multiple issues with krb nfs4 config in SCALE
- [NAS-111785] - Fix tdb directory setup
- [NAS-111789] - Perform direct smb config write when updating with AD domain name
- [NAS-111792] - Allow setting permissions on /root/.ssh
- [NAS-111794] - Move static nsswitch.conf to base install
- [NAS-111795] - Error when updating Alpha to Beta
- [NAS-111796] - Fix lazy initialization of directory services cache
- [NAS-111799] - Fix scale installer
- [NAS-111806] - Add tests for directory services user/group cache
- [NAS-111810] - Fixes #116 by swapping MINIO_ACCESS_KEY and MINIO_SECRET_KEY
- [NAS-111811] - Current rest-api only returns `text/plain` responses
- [NAS-111813] - Remove check for privatedir path in passdb_list
- [NAS-111816] - Improve acltype retrieval based on path
- [NAS-111819] - Fix taking vmware-aware manual snapshots

- [NAS-111820] - Setting id on USER_OBJ or GROUP_OBJ creates another USER ace
- [NAS-111822] - Stripping acl produces inconsistent permissions
- [NAS-111825] - grub2 failing to build
- [NAS-111828] - Fix regression on network chart
- [NAS-111832] - Ban ViewEncapsulation.None
- [NAS-111837] - Make sure we start nfs when user requests it
- [NAS-111843] - Fix typo in _strip_acl_posix1e call
- [NAS-111846] - Bug fix for string initialization in cython
- [NAS-111847] - Enforce global configuration reload on share guest access change
- [NAS-111848] - Improve share enumeration test
- [NAS-111849] - Fix typo in smb.py
- [NAS-111854] - [SCALE] SMB only works after reloading a Share
- [NAS-111877] - Infinite loading when switching to Rsync Module
- [NAS-111938] - Create idmap service to wrap around winbind
- [NAS-111940] - [SCALE] Storage > Apply Permissions Recursively checkbox Is not getting checked & applied
- [NAS-111951] - Fix update dialog
- [NAS-111954] - Fix GMail thread safety
- [NAS-111958] - Properly retrieve snapshots in bootenv plugin
- [NAS-111975] - [SCALE] Can't convert POSIX Dataset into NFSv4 Dataset
- [NAS-111997] - Properly retrieve registry config and ACLs in SMB debug
- [NAS-112004] - [SCALE] Can't save changes to VMs general settings because the UI wants a GPU to be selected
- [NAS-112013] - Storage Widget on Dashboard Reporting Incorrect Values
- [NAS-112020] - Copies must be a string when it is

21.06-BETA.1

21.06-BETA.1

June 22, 2021

After a very successful ALPHA cycle with thousands of deployed and tested systems, iXsystems is excited to announce the release of TrueNAS SCALE 21.06, which marks the official beginning of BETA. SCALE is now being tested for general NAS usage, scale-out, and application deployment. Many thanks to the thousands of community developers and testers who have contributed to the effort.

As our initial community post and blog indicated, TrueNAS SCALE is defined by its acronym:

Scale-Out ZFS: Capacity & Performance
Converged compute and storage
Active-Active reliability
Linux containers & virtualization: Docker, K8s, and KVM
Easy Setup & Management

With TrueNAS SCALE 21.06 and the recent release of TrueCommand 2.0, every element in the acronym has been delivered and is ready for BETA testing on the path to RELEASE later this year. The major new capabilities of TrueNAS SCALE 21.06 include:

- **SMB ACLs**: TrueNAS CORE supports NFSv4 and SMB ACLs, based on OpenZFS with FreeBSD-compatible extended attributes. TrueNAS SCALE includes an iXsystems enhancement to Linux which also allows importing of TrueNAS pools while keeping the same extended attributes functional. This is the final piece which allows migration of storage from TrueNAS CORE to SCALE.
- **Applications**: Third-party applications can now be deployed as single (Docker) containers or “pods” of containers using Helm charts with dynamic, customizable configurations. TrueNAS SCALE 21.06 also includes the ability to use one or more community-provided application repositories. One of our community members (Ornias) has built an extensive library of applications called TrueCharts, which also provides a process for users to build and customize their own libraries.
- **Scale-Out ZFS**: TrueCommand 2.0 provides a cluster volumes interface for TrueNAS SCALE systems. This enables ZFS datasets to be pooled together as cluster volumes which span multiple nodes. Cluster volumes can have a variety of redundancy properties including 3-way Mirrors, N+1, and N+2. Each cluster volume can then be shared with GlusterFS natively. Support for clustered SMB access will be available in August with SCALE 21.08.

TrueNAS SCALE documentation has also reached its BETA phase. It is based on the greatly improved documentation of TrueNAS CORE. In addition, there are Developer Notes (retired) and Release Notes. Even if you aren’t ready to make the leap, please review the docs and let us know if you have any questions.

We appreciate the community feedback and bug reports and hope to get all those features to RELEASE quality faster. A special thanks also goes to the large number of awesome community members who joined the development and test team. We’ve really appreciated your contributions and teamwork and it has greatly contributed to the accelerated development process.

21.04-ALPHA.1

21.04-ALPHA.1

April 22, 2021

After a very successful development cycle with thousands of downloads and deployments, iXsystems is pleased to announce TrueNAS SCALE 21.04 is now available! This release is planned to be the last ALPHA version on the path toward BETA. TrueNAS SCALE 21.04 is based on Debian “Bullseye” Linux and includes:

> **KVM Virtualization**: Mature Hypervisor with good reliability, Guest OS support, and enterprise features. This hypervisor is performing well in the field with our early adopters. In a future version, we plan to integrate it with Kubernetes so that VMs and containers can be deployed from a common user interface and API.
> **Kubernetes**: 3rd Party Applications can now be deployed as a single (docker) image or “pods” of containers. Using Helm Charts, complex applications can now be easily deployed with dynamic charts, giving users fine-grained control and flexibility. TrueNAS SCALE 21.04 now includes the ability to utilize community-provided catalogs, including TrueCharts.
> **GPU Passthrough**: SCALE 21.02 introduced Intel QuickSync GPU passthrough to containers. 21.04 improves this support by bringing NVIDIA GPU/CUDA passthrough to the UI and containers as well. Now containers which have GPU offload capabilities, such as Plex, can take advantage of a wider-range of GPU hardware. The sharing of GPU resources across multiple containers simultaneously is also supported.
> **Scale-out ZFS**: Cluster volumes which span multiple nodes and ZFS pools can be created to provide scalable and robust data stores. The web UI for these is included in TrueCommand 2.0 which is available as a nightly image.

The UI, while similar to TrueNAS CORE, has also been improved with some new UX enhancements across the ‘Data Protection’ and ’Sharing’ sub-sections. Further UX improvements are expected to arrive in version 21.06.

In the 21.02 version, we also introduced the new TrueNAS CLI that uses the API and persists all changes. This CLI will make it easier to script the set-up and configuration of TrueNAS. Feedback on the CLI has been very positive and provided much help in us rapidly maturing it for field-use.

In March, the TrueNAS CORE documentation received a major facelift which greatly improved navigation and ease of use. TrueNAS SCALE documentation is taking shape as a clone of TrueNAS CORE. TrueNAS SCALE documentation is minimal at the moment and relies on its similarity to TrueNAS CORE in addition to the Developer Notes (retired) and Release Notes.

We appreciate the community feedback and bug reports and hope to get SCALE to production quality faster. A special thanks also goes to the large number of community members who joined the development and test team. We’ve really enjoyed your contributions and teamwork and it has greatly contributed to the accelerated development process.

Software Features

Verified

Verified Features are generally working in SCALE. Minor bugs could be present.

- Pool Management
- SMB Shares
- iSCSI Shares
- NFS Shares
- S3 Shares
- AFP Shares
- AD / LDAP Directory Services
- Online / Offline updating
- Virtual Machines (Using KVM)
- WebDAV
- Monitoring, Alerting and Reporting
- POSIX 1e support
- Boot Environments
- SSH Credentials
- ZFS Encryption
- Cloud Sync
- Replication
- TrueCommand Cloud connections
- Applications UI

Provisional

These features have been added, but have known issues or are not fully feature-complete. Please use only with caution.

- Command Line Interface. To access, log in to the web interface and click **System Settings > Shell**. Enter `cli` to activate the interface and `help` to see a list of options.
- Tasks:
  - Cron
  - Init/Shutdown Scripts
  - S.M.A.R.T. testing
  - Resilver prioritization
  - Periodic Snapshots
  - Rsync
  - Scrub
- Docker Images deployed as Helm Charts with Kubernetes NVIDIA / Intel Quicksync GPU passthrough (CLI)
- Wireguard (CLI)
- Networking and Settings UX Refresh
- OpenVPN Client and Server
- Two-factor authentication

- Certificate Management

Experimental

These features are still in early development and will be landing in Nightly images of SCALE in the near future.

- Clustered Datasets API support for TrueCommand
- TrueCommand Clustering UI for SCALE
- NFSv4 ACL support

New Feature

- [NAS-104330] - Remove NIS support for SCALE
- [NAS-105932] - Add a few more ACMD DNS Authenticators
- [NAS-107219] - Allow no password sudo with commands (API)
- [NAS-108291] - Investigate using SPICE instead of VNC
- [NAS-108322] - Applications UI implementation
- [NAS-108574] - Add TLS support for Minio chart
- [NAS-108692] - Ability to retrieve k8s pods logs in middleware
- [NAS-108957] - Show chart release events in the UI
- [NAS-109169] - Config upload / factory reset for TN HA
- [NAS-109303] - Introduce concept of changelog for chart release upgrades
- [NAS-109315] - Push openzfs/catalog validation docker images on master update
- [NAS-109316] - Custom Catalogs Support in UI
- [NAS-109381] - Report installation and first boot versions on TrueNAS
- [NAS-109446] - Show pod logs in UI
- [NAS-109458] - Need "-d sat" on RI-SSD drives in debug/SMART
- [NAS-109537] - Have readable/better ACME authenticator field names
- [NAS-109538] - Detach used PCI devices automatically

Improvement

- [NAS-108602] - Gracefully abort jobs
- [NAS-109029] - Allow user to configure GPU in Launch Docker image wizard in UI
- [NAS-109153] - Implement entity-empty on entity-table
- [NAS-109154] - Implement Entity-empty on Dashboard
- [NAS-109159] - Update rendering for a list
- [NAS-109172] - System Advanced Dashboard
- [NAS-109202] - Data Protection Dashboard
- [NAS-109240] - Have a spinner while loading chart releases
- [NAS-109256] - Move Email link to Alerts Menu
- [NAS-109257] - Move Guide link to topbar
- [NAS-109258] - Remove Misc page from UI
- [NAS-109271] - We should allow selecting apps from app tiles for bulk actions
- [NAS-109278] - Allow specifying properties for ix volumes
- [NAS-109280] - Retrieve only desired properties when loading storage page in UI
- [NAS-109305] - Allow chart devs to have more control on values for helm release
- [NAS-109312] - Chart Release creation should be a wizard like "launch docker image"
- [NAS-109314] - Allow saving preferred train of a catalog for the user
- [NAS-109326] - Show warning when adding sysctls
- [NAS-109345] - Add validation for $ref types in catalog_validation
- [NAS-109442] - Investigate cleaning up challenges similar to how certbot does for ACME
- [NAS-109468] - Investigate having a sane version for applications
- [NAS-109469] - Investigate using PV/PVC for storage in Apps
- [NAS-109479] - Implement entity-empty on credentials/certificates cards
- [NAS-109559] - Allow setting a container to be privileged in the UI for ix-chart
- [NAS-109591] - Implement entity-empty on the Storage page
- [NAS-109601] - Expose consolemsg property in System General
- [NAS-109638] - send signals to fenced based on zpool events
- [NAS-109677] - Update information in WebUI repo
- [NAS-109804] - Scale: Implement column sorting in entity-tree-table
- [NAS-109859] - remove incorrect verbiage for iscsi
- [NAS-109914] - FUSE mnt/umnt gluster volumes when the volume is started/stopped/deleted
- [NAS-109990] - improve nfs debug section for SCALE
- [NAS-109999] - gluster.localevents.send is not a job
- [NAS-110023] - Remove custom scrollbar implementation
- [NAS-110029] - make public api endpoint for retrieving unique system hash
- [NAS-110053] - fix nvme drive detection on SCALE

Bug Fixes

- [NAS-100503] - Avoid N event subscriptions to run the same code
- [NAS-107243] - Unable to passthrough GPU pci devices in SCALE
- [NAS-107508] - Unable to install TrueNAS Scale in UEFI mode
- [NAS-108154] - Limit number of simultaneous replications
- [NAS-108202] - bad signature because OCSP stapling not activated in the nginx config file
- [NAS-108421] - Missing stats in virtual memory (psutil)
- [NAS-108560] - Pool status will not update unless system is restarted/system panics
- [NAS-108599] - SMB shares not accessible after reboot until avahi (mDNS) is restarted

- [NAS-108630] - Bad key labels for the UPS battery statistics and time remaining graphs
- [NAS-108737] - TNSCALE - Upgrading via a new ISO wipes the initial image
- [NAS-108799] - 20.12 TrueNAS SCALE USB ISO unknown filesystem
- [NAS-108854] - Mandatory field SAN when creating new CA Certificate
- [NAS-108879] - Scale - grub.cfg changes for console boot
- [NAS-108921] - Allow users to disable container image updates in the UI
- [NAS-108924] - Edit ZVOL → wrong compression property selected by default
- [NAS-108938] - SCALE - If network bridge is set, kube-bridge make WebUI unreachable
- [NAS-108956] - Can not resume "import disk" after reboot
- [NAS-108975] - Boot Pool Status in GUI is empty
- [NAS-108990] - Aborted disk import job is displayed as completed
- [NAS-109005] - Shell does not display Greek characters
- [NAS-109014] - SMART not reporting properly on SAS drives since r5022. Was working in r4883
- [NAS-109020] - SSH service failed to start - After Upgrade from Freenas - Hostkey missing
- [NAS-109034] - Emailing alerts sometimes happens before the network interface is online (and fails)
- [NAS-109041] - Overlapping icons
- [NAS-109042] - Entity-form checkboxes breaking field alignment
- [NAS-109052] - Idmap GUI issue after adding trusted domain.
- [NAS-109074] - Add user form template display error
- [NAS-109077] - Editing disk device of VM does not show up already selected zvol
- [NAS-109087] - UI dashboard takes very long to show up
- [NAS-109102] - SCALE TFTP does not affect config
- [NAS-109134] - CLONE - Fix the year displayed in Display System Processes and the Shell
- [NAS-109173] - middleware job - re-raise existing CallError
- [NAS-109177] - Clean up LDAP error messages and fix call to set ldap passwd
- [NAS-109183] - Disk usage sorting is alphaneumeric, not by actual space used
- [NAS-109192] - TrueNAS Scale and plex Hardware accleration adding support
- [NAS-109193] - Bring kdump-tools back in TN Scale
- [NAS-109197] - traceback in CLI system->boot->get_disks
- [NAS-109206] - add interface validation in ctdb.public.ip.create
- [NAS-109220] - Installing TrueNAS Scale Nightly 02. Febuary fails with "no space left on volume /dev/sda" on a 300GB SAS drive
- [NAS-109232] - UI allows modifying boolean checkbox when editable is false
- [NAS-109237] - Cannot create ACME Certificate
- [NAS-109261] - After adding CSR, page needs to be refreshed to see the new CSR
- [NAS-109269] - We have some unexpected text remaining after certificate deletion in UI
- [NAS-109270] - Inconsistent extension form while creating CSR
- [NAS-109273] - SMB share is unavailable because it uses a locked dataset
- [NAS-109281] - Application names cannot be modified once installed
- [NAS-109289] - Test - SCALE-21.02- ALPHA (Angelfish) Sprint 1
- [NAS-109300] - Truenas Scale installer install disk selection does not list drives past sdz i.e. sdaa...
- [NAS-109307] - Restart services dependent on acme certs when they renew
- [NAS-109310] - New Firmware for EOL E16 Shelf validated
- [NAS-109311] - OpenStack Swift auth_version verification fails
- [NAS-109313] - Add validation for app train names
- [NAS-109321] - Add basic pseudo service for directory services cache
- [NAS-109325] - fix check_path_resides_within_volume wrt to gluster paths
- [NAS-109327] - Remove temporary wrapper to start kubernetes service
- [NAS-109328] - Register events of services as private which are private themselves
- [NAS-109336] - Delete snapshots in descendant filesystems as well on chart release upgrade
- [NAS-109341] - VM libvirtError - internal error: client socket is closed
- [NAS-109344] - Keep track of catalog repo/branches for installed chart releases
- [NAS-109350] - CLONE - Bad key labels for the UPS battery statistics and time remaining graphs
- [NAS-109351] - systemd-sysv-generator - console warning for missing native systemd unit file
- [NAS-109370] - Column for Disk Serial number
- [NAS-109371] - Can't delete VM without deleting snaps first
- [NAS-109388] - disk.get_unused isn't returning a complete list
- [NAS-109398] - Replication of ZVOLs stopped working after upgrade from 11.3-U5 to 12.0-U2
- [NAS-109403] - Replication task prograss is showing wrong units
- [NAS-109405] - Trying to add a cloud sync job complains about no folder attribute defined
- [NAS-109408] - LSI3008 firmware image not found
- [NAS-109411] - Add encryption summary for pools in debug
- [NAS-109412] - CPU Usage graph: 'idle' is always pegged at 100%
- [NAS-109417] - Set zvol_volmode to 2 in SCALE
- [NAS-109418] - Properly set error code if dataset is busy on deletion
- [NAS-109420] - libvirtd.core on upgrade to 12.0-U2
- [NAS-109428] - UI displays an ACME certificate as a CSR
- [NAS-109429] - UI incorrectly displays certificate type value when creating CSR
- [NAS-109430] - Improve error handling for directory services
- [NAS-109431] - UI does not show null selected entry in enum for chart release edit/create form
- [NAS-109434] - Resolve issues with joining Active Directory Domains
- [NAS-109435] - API Call systemGeneralUiRestartGet gives no response
- [NAS-109440] - Fix migration revision id
- [NAS-109441] - Properly send events for event sources when arguments are specified
- [NAS-109443] - UI should retrieve ACME DNS authenticator choices from middleware
- [NAS-109448] - Properly reload/restart services dependent on ACME certs
- [NAS-109449] - TrueNAS Scale: cannot select UPS driver
- [NAS-109451] - fix ctdb.general.ips
- [NAS-109452] - disk.query doesn't fire event on removal
- [NAS-109454] - Improve handling for corefile alerts

- [NAS-109456] - deprecate internal uses of system.is_freenas
- [NAS-109462] - [SCALE] Can't unlock encrypted zfs pool
- [NAS-109467] - SCALE 21.02 - certificate import not working
- [NAS-109472] - DIsable pagination on services page
- [NAS-109473] - "File Ticket" form link to JIRA is indistinguishable from the rest of the text
- [NAS-109474] - Reconfigure zettarepl_file logger on system dataset reconfiguration
- [NAS-109480] - unify failover.** api calls to a single entity
- [NAS-109481] - coredns container keeps restarting since install
- [NAS-109483] - Telegram Notification Not Formatting HTML
- [NAS-109484] - Upgrade of Truenas Scale from nightly 2021-02-06 to 2021-02-18 breaks users
- [NAS-109487] - nslcd.service failed
- [NAS-109490] - Use the correct verbiage when Applying Pending Updates for HA
- [NAS-109491] - cache if a system is licensed for HA (failover.licensed)
- [NAS-109495] - General Settings broken after page reload
- [NAS-109497] - change cluster_events API to mount all gluster volumes based on events
- [NAS-109498] - add gluster FUSE api
- [NAS-109509] - Replication says finished, but actually has error "cannot receive org.truenas:managedby property"
- [NAS-109510] - Destination dataset already exists and is it's own encryption root.
- [NAS-109513] - TrueNAS Scale: UPS shutdown command is incorrect
- [NAS-109520] - TrueNAS Scale: UPS (NUT) service fails to start correctly
- [NAS-109522] - Can't reconfigure S3 AkSk on the same dataset
- [NAS-109523] - S3 listen only to https
- [NAS-109526] - Use get_instance endpoint when using middleware call
- [NAS-109528] - ignore `docs` folder for train validation
- [NAS-109531] - pool.dataset.query should not return the boot pool
- [NAS-109532] - ix-applications content (folders) not moved when pools changed
- [NAS-109533] - Use colon to concatenate repository and tag for ix-chart
- [NAS-109534] - Fix service query
- [NAS-109545] - Slow (iSCSI) api
- [NAS-109548] - Snapshots can't be deleted from gui
- [NAS-109549] - Add human version for catalog items
- [NAS-109550] - Export Key option visible when using passphrase encryption
- [NAS-109552] - Add ability to change "System Dataset Pool" option
- [NAS-109553] - Add "Show Console Messages" to GUI on General Settings
- [NAS-109555] - Add endpoint to retrieve valid system dataset pool choices
- [NAS-109560] - Retrieve timestamps for each pod log entry
- [NAS-109564] - Setting Plex to "Require" secure connection prevents docker container from properly deploying
- [NAS-109581] - products filter in alert not working
- [NAS-109582] - Improve UI error handling - [object Object] while taking a debug
- [NAS-109584] - Kubernetes/dump.txt is 193MB
- [NAS-109585] - Give proper replication and periodic snapshot task debug
- [NAS-109597] - FailoverService HA_MODE/HA_LICENSED not working
- [NAS-109598] - Vulenribilty found in Web UI
- [NAS-109599] - traceback in jail_freebsd
- [NAS-109602] - traceback in libvirt event_loop_connection
- [NAS-109605] - Validate certificate while creating/updating idmap
- [NAS-109606] - Replication Task cannot be created through UI due to SSH check even for LOCAL
- [NAS-109610] - HA systems only deliver debug for active node when a proxy is configured
- [NAS-109617] - improvements to gluster.peer.status API
- [NAS-109627] - Error: [EFAULT] Kubernetes service is not running.
- [NAS-109642] - Roll Back breaks the page
- [NAS-109643] - Adjust default NFSv4 ACL for new datasets
- [NAS-109648] - Retrieve chart release history on chart.release.query event
- [NAS-109652] - Wrong san value in the payload of "certificate.create" when creating a CSR
- [NAS-109656] - replication does not work after upgrade to 12.0-U2.1
- [NAS-109659] - Change wording to "Unselect All" when all apps are selected
- [NAS-109665] - UI should show readable names of popular ACME servers
- [NAS-109668] - Fix resolving patch for certificate service
- [NAS-109682] - Page needs to be refreshed to see newly created VM
- [NAS-109686] - [Charts/Apps] "show_if" only working on "type: dict"
- [NAS-109687] - R20 doesn't recognize its own enclosure
- [NAS-109692] - New SSH connection form hides errors
- [NAS-109694] - Initial protocol testing for SMB using pylibsmb
- [NAS-109696] - Cloud Sync Task Dropbox never completes, stuck at 100%
- [NAS-109700] - Support mailcfg[fromname]
- [NAS-109702] - Retrieve build time without authentication
- [NAS-109705] - All replication hangs until system is rebooted after getting SSHException
- [NAS-109710] - Remove chart release update alert if chart release is deleted
- [NAS-109712] - Use updated endpoints to manipulate VM display/vnc devices
- [NAS-109713] - Do not use "vm.create" for adding VM devices in the UI
- [NAS-109714] - Unexpected asterik in VM delete dialog
- [NAS-109715] - Unable to launch a docker image from UI
- [NAS-109718] - Add throttle for build_time endpoint
- [NAS-109720] - Interrupted full replications are silently failing to resume
- [NAS-109722] - no doc.txz in 12.0 -- jail creation failure
- [NAS-109724] - allow failover.status in rest api
- [NAS-109727] - middlewared (zettarepl) zombie process
- [NAS-109728] - Dynamic DNS service not starting
- [NAS-109729] - Unable to modify/edit a chart release based on ix-chart
- [NAS-109731] - fix failover.in_progress on SCALE

- [NAS-109732] - Clear various AD-related caches when service explicitly stopped
- [NAS-109734] - Fix RcloneVerboseLogCutter
- [NAS-109739] - Snapshots deletion confirmation page does not display snapshot names
- [NAS-109741] - Allow better progress report for core.bulk
- [NAS-109743] - Explicitly set tdbsam as passdb backend when stopping ldap
- [NAS-109749] - Fix SMB share ids in smb_registry tests
- [NAS-109752] - Do not wait for completed job pods to be deleted
- [NAS-109754] - [Charts/Apps] Lists-in-Lists broken on latest build
- [NAS-109757] - SCALE: Failed to start kubernetes cluster - Unable to find "ix-truenas" node.
- [NAS-109762] - remove ability to share raw disks via iscsi on SCALE
- [NAS-109769] - HA journal EOFError pickle.load()
- [NAS-109777] - Retrieve app_readme at item level for UI
- [NAS-109780] - [Certificates] Creating ACME certificate fails stating missing "root email adress"
- [NAS-109782] - Bridged NIC adapter always set to DOWN state
- [NAS-109790] - Add initial tests for alternate datastream support
- [NAS-109797] - "Bucket is required" when setting up Google Drive cloud sync task
- [NAS-109799] - Some Text In UI (Storage>Pools>Edit>ACL) don't show up in the .PO file
- [NAS-109801] - Some LDAP configuration fields are empty after upgrading
- [NAS-109805] - Add regression tests for domain sid modifications
- [NAS-109808] - Fix typo in nis.get_cache
- [NAS-109810] - fix various issues in CtdbSharedVolumeService
- [NAS-109816] - Restarting the middlewared service leaves you with no dhclient
- [NAS-109819] - Traceback trying edit disk on pool status page
- [NAS-109820] - SCALE Samba group write permissions do not work
- [NAS-109824] - Ensure aclmode set to DISCARD if not using NFSv4 ACLs on SCALE
- [NAS-109826] - All encryption indicators and menu options missing in Storage tree table
- [NAS-109827] - Retrieve k8s backup name after completing backup
- [NAS-109831] - Task manager shows vmware.periodic_snapshot_task_begin every 10 minutes
- [NAS-109847] - Cannot create docker containers without some fields.
- [NAS-109855] - [certificates] ACME crashes with valid credentials and wildcard domain
- [NAS-109858] - Recursively destroy backup snapshot
- [NAS-109861] - Always add encryption properties while retrieving datasets
- [NAS-109865] - Add dependencies to SMB SID tests
- [NAS-109867] - Chart release summary dialog styling issue
- [NAS-109884] - [SCALE] Some VMs don't have network access after Update
- [NAS-109893] - Opening openVPN server settings takes you back to the dashboard
- [NAS-109898] - PoolDatasetService.do_create: skip children lookups on parent datasets
- [NAS-109903] - Wrong openapi schema on {id} endpoints
- [NAS-109905] - SCALE Init scripts are not executed
- [NAS-109907] - TrueCommand Cloud cannot access added systems if they have the Listen Interface customized
- [NAS-109911] - CRUDService.query: handle force_sql_filters
- [NAS-109919] - Bug fix for validation acme authenticator schemas
- [NAS-109921] - Correctly display CertBot validation errors
- [NAS-109926] - Increase permitted SMB stream size
- [NAS-109927] - Do not have catalog query fail
- [NAS-109928] - Replication failed (ZFS snap) after last upgrade
- [NAS-109930] - Set graphic console charmap to utf-8 so CLI can be used normally
- [NAS-109932] - Properly show error messages for invalid client cert
- [NAS-109944] - Allow specifying default identifier field for tables
- [NAS-109947] - TrueNAS Scale 20.02 A1 doesn't recognize LSI 9201-16e even with latest Firmware
- [NAS-109959] - Fix AD cache fill with alternate character sets
- [NAS-109961] - `reporting.get_data` returns null arrays for data and aggregation
- [NAS-109968] - Allow retrieving parsed image tags for container images
- [NAS-109974] - Fix entity-empty text color on light themes
- [NAS-109975] - ACME Domain list messed up
- [NAS-109981] - Fix using sql filters in rest api
- [NAS-109983] - Mark zfs-localpv and nvidia images as internal system images
- [NAS-109984] - Do not traceback when adding misconfigured catalog
- [NAS-109986] - Add endpoint to retrieve gpu pci ids choices
- [NAS-109993] - Fix spacing and border color on dark themes
- [NAS-110009] - use correct logrorate size
- [NAS-110013] - Creating a new Open VPN Client fails with OpenSSL.crypto.Error
- [NAS-110039] - Ignore encoding errors in stdout/stderr
- [NAS-110044] - null_value in ISCSI extent Device field
- [NAS-110046] - udev not working
- [NAS-110047] - Fix TypeError: sync_interface() missing 1 required positional argumen…
- [NAS-110067] - Normalise docker data-root path
- [NAS-110071] - SCALE: UI auth_token login handling breaks server (500 Internal Server Error)
- [NAS-110095] - Make sure we correctly retrieve active containers status
- [NAS-110099] - Make sure required crds are setup before considering k8s node to be ready
- [NAS-110102] - Fix failing tests
- [NAS-110120] - No way to know cloud sync task progress or why it failed
- [NAS-110128] - use failover.sendfile in failover.sync_to_peer
- [NAS-110133] - Do not show a successful status for cloud sync that was not executed …
- [NAS-110163] - CLONE - Fix TrueNASMOldBIOSVersionAlertSource
- [NAS-110191] - Retrieve display device id with each display uri
- [NAS-110192] - Add normalized vm pci id to device.get_gpus
- [NAS-110251] - Handle case where active_media_subtype can be none

21.02-ALPHA.1

21.02-ALPHA.1

February 16, 2021

iXsystems is pleased to release the next Alpha version of TrueNAS SCALE! SCALE is the newest member of the TrueNAS family. When complete, SCALE will have all major TrueNAS CORE storage and sharing features and web interface based on Debian GNU/Linux. There will also be additional SCALE-specific features that are derived from the application's Linux base. The major features of SCALE are represented in the application acronym:

Scaled-Out ZFS
Converged
Active-Active
Linux Containers
Easy to Manage

Initial developer's notes (retired) for TrueNAS SCALE are available in the TrueNAS Documentation Hub. Note that because SCALE shares a similar user interface as the FreeBSD-based TrueNAS CORE, many of the current documentation articles also apply to SCALE. SCALE feature-specific articles will be added to the SCALE section as the software approaches its first full release.

Code-named Angelfish, TrueNAS SCALE ALPHA follows a *year.month-ALPHA.#* scheme for versioned releases. Because this is an ALPHA release of the software, not all planned features are present. The status of major features are listed here, along with the full changelog of bug fixes that are part of the SCALE 21.02-ALPHA.1 release.

Software Features

Verified

Verified Features are generally working in SCALE. Minor bugs could be present.

- Pool Management
- SMB Shares
- iSCSI Shares
- NFS Shares
- S3 Shares
- AFP Shares
- AD / LDAP Directory Services
- Online / Offline updating
- Virtual Machines (Using KVM)
- WebDAV
- Monitoring, Alerting and Reporting
- POSIX 1e support
- Boot Environments
- SSH Credentials
- ZFS Encryption
- Cloud Sync
- Replication
- TrueCommand Cloud connections
- Applications UI

Provisional

These features have been added, but have known issues or are not fully feature-complete. Please use only with caution.

- Command Line Interface. To access, log in to the web interface and click **System Settings > Shell**. Enter `cli` to activate the interface and `help` to see a list of options.
- Tasks:
  - Cron
  - Init/Shutdown Scripts
  - S.M.A.R.T. testing
  - Resilver prioritization
  - Periodic Snapshots
  - Rsync
  - Scrub
- Docker Images deployed as Helm Charts with Kubernetes NVIDIA / Intel Quicksync GPU passthrough (CLI)
- Wireguard (CLI)
- Networking and Settings UX Refresh
- OpenVPN Client and Server
- Two-factor authentication
- Certificate Management

Experimental

These features are still in early development and will be landing in Nightly images of SCALE in the near future.

- Clustered Datasets API support for TrueCommand

- TrueCommand Clustering UI for SCALE
- NFSv4 ACL support

21.02-ALPHA.1 Changelog

New Feature

- [NAS-100018] - S.M.A.R.T tests not sticky when disk is replaced
- [NAS-100207] - In smart tests table, add enable/disabled columns
- [NAS-107146] - Migrate from 12.x to SCALE (Backend / Framework)
- [NAS-108271] - New alert service: Telegram
- [NAS-108575] - Allow disabling docker image updates
- [NAS-108688] - Allow access to pod console from UI
- [NAS-108689] - Chart release events on chart release resource changes
- [NAS-108690] - Dynamically create chart release form in UI
- [NAS-108691] - Ability to retrieve next unused port in middleware for Apps
- [NAS-108693] - Have ability to search chart releases in UI and have bulk options
- [NAS-108842] - SCALE: Allow custom App catalogs
- [NAS-108922] - UI should update chart release status based on chart release events
- [NAS-108991] - Add ability to update container images in use in a chart release

Improvement

- [NAS-100562] - Remove custom themes feature
- [NAS-100629] - The text in the Shell appears to wrap prematurely even on a sufficiently wide display/screen
- [NAS-102006] - Improve Alert Settings page
- [NAS-104469] - Shell does not select text accurately
- [NAS-105062] - WebUI forces to choose bridge members upon its definition
- [NAS-106588] - Can't log in to GUI with <enter> when credentials are saved
- [NAS-107898] - Improve display of Service > UPS driver options
- [NAS-108143] - [SCALE] Removing all NFS exports requires manual restart of NFS service
- [NAS-108154] - Limit number of simultaneous replications
- [NAS-108333] - create ctdb plugin for gluster smb integration
- [NAS-108444] - lagg interface member menu proposes a vlan interface
- [NAS-108452] - Restore background cpu dashboard widget updating
- [NAS-108464] - Dashboard CPU widget does not clear out the old values
- [NAS-108479] - Mystery Error 3221225867
- [NAS-108512] - GELI unlock very slow
- [NAS-108519] - Do not re-use IDs for the various assets in the DB
- [NAS-108525] - unable to create a jail that has partly the name of another
- [NAS-108535] - Use smart.test.disk_choices
- [NAS-108548] - Creating a passphrase for a dataset in UI accepts different passphrases
- [NAS-108557] - [SCALE] Unable to create a debug
- [NAS-108571] - Big samba log files in /var/log/samba4 on SCALE
- [NAS-108586] - Can't remove offline pool
- [NAS-108600] - Still no Reporting graphs afer 12.0-U1
- [NAS-108624] - Traceback ISCSIPortalIP
- [NAS-108625] - Unable to update configuration for FTP service
- [NAS-108629] - Bad labels for key in NFS Stats (Bytes) graph
- [NAS-108639] - Cannot configure MTU < 1492
- [NAS-108640] - Save configuration exports encryption keys regardless of checkbox
- [NAS-108648] - SMB Home Share not creating user folder
- [NAS-108655] - cannot exclude an irelevant dataset
- [NAS-108657] - Not allowed to set schedule for PUSH replication linked to snapshot task
- [NAS-108660] - SMART test error pre-format is not respected
- [NAS-108665] - TrueNAS 12.0 U1 email outgoing mail server and port missing
- [NAS-108666] - netcli operation hangs on uniq
- [NAS-108675] - Cannot toggle boot flag after pluggin creation
- [NAS-108685] - Traceback when trying to export an offline pool
- [NAS-108686] - Bug fix while editing plex chart release form
- [NAS-108695] - Hide static IP fields when DHCP is set in launch docker image form
- [NAS-108715] - Reporting graphs aren't functions
- [NAS-108716] - Inconsistent dialog action button colors
- [NAS-108721] - Entity Table UX Improvements
- [NAS-108726] - htop -s segfaults
- [NAS-108737] - TNSCALE - Upgrading via a new ISO wipes the initial image
- [NAS-108744] - Launch Docker Image buttion brings up wrong menu screen
- [NAS-108746] - Saving debug fails (two pools)
- [NAS-108749] - HTML in text/plain part of the alert email
- [NAS-108753] - Panic on special_small_blocks > 128KB
- [NAS-108762] - run time error when configuring ip address on vlan1350 interface from webUI
- [NAS-108776] - Docker application exposes network as mgmt interface
- [NAS-108777] - replication allows mountroot to be set to /
- [NAS-108778] - /run/lock is too small in SCALE
- [NAS-108786] - 12.0-U1 - Interface reports use inconsistent units
- [NAS-108792] - [SCALE] Fix VNC Input
- [NAS-108794] - vlan interface creation wizard : 'parent interface' dropdown menu proposes physical interfaces that are already members of a lagg
- [NAS-108796] - SMB Error with push replicaton

- [NAS-108806] - SSH login accepts password although password login is disabled globally when user home is on encrypted volume
- [NAS-108809] - Installation script does not remove ZFS headers from partition before creating new partition table
- [NAS-108814] - SMB Service stops responding afer some time. Needs a service restart or system restart to reset
- [NAS-108816] - Missing network interfaces in SCALE 20.12
- [NAS-108821] - Network config from dashboard
- [NAS-108834] - Pod console connection is killed right after it is connected successfully
- [NAS-108835] - Group members view navigates to dashboard
- [NAS-108839] - SCALE: Nvidia driver incompatibility in 20.12
- [NAS-108853] - Missing hover effect on table rows
- [NAS-108855] - Duplicated enties in the dropdown list of certificates
- [NAS-108871] - Reporting Disks does not show temperature. HDD Standby is already set to always on.
- [NAS-108882] - openebs-zfs-plugin zfs-driver uses wrong lib versions
- [NAS-108883] - Apps page gives Docker Service Error
- [NAS-108889] - middleware AD health checks can contend with winbindd netlogon connection NT_STATUS_RPC_SEC_PKG_ERROR
- [NAS-108895] - Cannot save debug
- [NAS-108906] - Private key should be a mandatory field in the UI when importing CSR
- [NAS-108907] - Invalid call to disk.query
- [NAS-108909] - Allow unsetting a pool for Applications in UI
- [NAS-108916] - Change replication task schedule logic
- [NAS-108920] - Error when trying to send test email
- [NAS-108931] - TrueNAS SCALE fails to boot from USB
- [NAS-108932] - Sending email always causes a broken pipe error
- [NAS-108952] - Storage tree table missing some columns
- [NAS-108974] - FreeNAS Certified systems show empty space instead of logo
- [NAS-108985] - Huge freenas-debug, preventing debug
- [NAS-108986] - SCALE: unable to change Restart Policy for Apps
- [NAS-109005] - Shell does not display Greek characters
- [NAS-109021] - Dashboard widget template error
- [NAS-109030] - Cannot add iscsi user
- [NAS-109031] - Default update train is missing in 12.0 U1.1
- [NAS-109033] - Error while importing certificates
- [NAS-109038] - Combobox broken
- [NAS-109039] - After Failover during Manual Update from 11.3-U5 to TrueNAS-12.0-INTERNAL-125 HA failed
- [NAS-109040] - NTP Server Settings form field size issue
- [NAS-109041] - Overlapping icons
- [NAS-109043] - Clean up svg imports in app component
- [NAS-109045] - CallError - [EFAULT] Failed to set NT password for XXXXXX: Username not found!
- [NAS-109050] - Fix the year displayed in Display System Processes and the Shell
- [NAS-109064] - Allow to not retrieve children of a dataset
- [NAS-109066] - Switch middleware rsync plugin to "new compression"
- [NAS-109067] - Update image cache after pulling docker image
- [NAS-109072] - Cannot create second VM on SCALE
- [NAS-109074] - Add user form template display error
- [NAS-109076] - UI does not refresh pool status after clicking on refresh
- [NAS-109079] - Error exporting/disconnecting pools on TrueNAS 12.0
- [NAS-109080] - Retrieve chart release schema for installed chart releases
- [NAS-109081] - Optimize retrieval for a single chart release
- [NAS-109082] - exclude "sr" devices on fenced in SCALE
- [NAS-109087] - UI dashboard takes very long to show up
- [NAS-109088] - Make GPU label more descriptive
- [NAS-109089] - Cog icon overused
- [NAS-109090] - traceback in libsgio for get_rotation_rate
- [NAS-109091] - py-sgio doesn't propagate exceptions to caller
- [NAS-109093] - Don't show clear icon on readonly input fields
- [NAS-109098] - Minio process does not start with encrypted pool
- [NAS-109101] - Fetch datastores connecting to vCenter (6.7U3) does not get remote datastores
- [NAS-109102] - SCALE TFTP does not affect config
- [NAS-109107] - Build SCALE with Samba 4.14
- [NAS-109115] - dmidecode error on Disk Testing and Pool Creation
- [NAS-109136] - Isolate kubernetes cluster
- [NAS-109138] - fix up ctdb.shared.volume and gluster.volume/peer CRUD APIs
- [NAS-109142] - SCALE - logging doesn't persist across middleware restarts
- [NAS-109164] - dont traceback in ctdb.general.healthy
- [NAS-109170] - start/stop ctdbd service with glusterd
- [NAS-109176] - add ctdb shared vol validation to gluster.volume CRUD API
- [NAS-109185] - no smbusers file can not map accounts to email for microsoft accounts
- [NAS-109194] - handles k3s and VMs on SCALE HA appropriately
- [NAS-109204] - traceback in ctdb.public.ips.query
- [NAS-109219] - System not showing alerts for degraded pool, alert email not sent/received
- [NAS-109228] - Allow running a migration for chart release upgrades
- [NAS-109230] - zettarepl.datasets_have_encryption
- [NAS-109231] - Schema changes chart releases
- [NAS-109233] - Fix lack of whitespace in dialog box
- [NAS-109234] - Fix potential division-by-zero error
- [NAS-109237] - Cannot create ACME Certificate
- [NAS-109238] - CSS regression on input fields.
- [NAS-109242] - Fix List() schema with multiple dict "items"
- [NAS-109250] - Fix enclosure.sync_zpool KeyError

- [NAS-109251] - Fix coroutine never awaited
- [NAS-109261] - After adding CSR, page needs to be refreshed to see the new CSR
- [NAS-109262] - Certificate/CSR creation is a job and UI should show errors raised by the job
- [NAS-109267] - After upgrading chart release UI does not show updated version of app
- [NAS-109268] - Please wait dialog stays after failing to delete a certificate
- [NAS-109279] - Allow consumer to specify which properties to retrieve for datasets
- [NAS-109281] - Application names cannot be modified once installed
- [NAS-109285] - Send a changed event after chart release upgrade completes
- [NAS-109286] - Validation error in LibDefaults section for option default_cc_type on Kerberos settings ui page
- [NAS-109291] - Add validation for catalog label
- [NAS-109292] - Bug fix for chart release name regex
- [NAS-109304] - zfs.dataset.create set xattr=sa by default like pool.dataset.create
- [NAS-109318] - TureNAS SCALE: Applications, Error getting pool data after adding new disk
- [NAS-109321] - Add basic pseudo service for directory services cache
- [NAS-109327] - Remove temporary wrapper to start kubernetes service
- [NAS-109328] - Register events of services as private which are private themselves
- [NAS-109329] - Unable to create zvol from UI - TrueNAS Scale Nightly
- [NAS-109336] - Delete snapshots in descendant filesystems as well on chart release upgrade
- [NAS-109344] - Keep track of catalog repo/branches for installed chart releases

Bug Fixes

- [NAS-103140] - Don't encapsulate xterm in a mat-card
- [NAS-103316] - System/Reporting should be embedded into ReportsDashboard
- [NAS-103438] - Use a better monospaced font in the shell section of webui
- [NAS-105823] - Move Alert settings to Alert Bar
- [NAS-107574] - Scale: virtualization - when adding new disk to existing VM, have option to create new zvol
- [NAS-107663] - New Hosts API for iSCSI
- [NAS-108151] - UX improvements for System/General global actions
- [NAS-108324] - Convert Certificate and CA forms to wizards
- [NAS-108481] - zvol zfs encryption settings missing from UI
- [NAS-108495] - Missing ix-auto in -> and + button in Sharing/iSCSI/Initiators/Add on 12.0
- [NAS-108604] - Make restarting/reloading locked attachments optional
- [NAS-108681] - Use id filter for retrieving root dataset information on UI dashboard
- [NAS-108725] - Make first column of table data always sticky
- [NAS-108779] - Add tooltip for tips on webshell page
- [NAS-108781] - Better UX for entity-wizard
- [NAS-108782] - Slide out forms should fill viewport height
- [NAS-108840] - Add session-id filter optimization to smbstatus
- [NAS-108894] - Display warning if user selects FULL or DEBUG log level for SMB
- [NAS-108918] - Tooltip for ACL in SMB share GUI form is wrong
- [NAS-108949] - Better flex rules for global actions
- [NAS-108950] - Better text input field UX
- [NAS-108961] - Unbalanced field layout in Edit Disks form
- [NAS-108968] - Convert services page to entity-table
- [NAS-108973] - Wasted space in System/Advanced
- [NAS-109022] - Properly show if there are no installed apps in UI
- [NAS-109153] - Implement entity-empty on entity-table
- [NAS-109154] - Implement Entity-empty on Dashboard
- [NAS-109159] - Update rendering for a list
- [NAS-109172] - System Advanced Dashboard
- [NAS-109236] - Do not render variables which have "hide=True" in schema for Apps
- [NAS-109240] - Have a spinner while loading chart releases
- [NAS-109256] - Move Email link to Alerts Menu
- [NAS-109257] - Move Guide link to topbar

20.12-ALPHA

20.12-ALPHA

December 18, 2020

iXsystems is pleased to release the next Alpha version of TrueNAS SCALE! SCALE is the newest member of the TrueNAS family. When complete, SCALE will have all major TrueNAS CORE storage and sharing features and web interface based on Debian GNU/Linux. There will also be additional SCALE-specific features that are derived from the application's Linux base. The major features of SCALE are represented in the application acronym:

Scaled-Out ZFS
Converged
Active-Active
Linux Containers
Easy to Manage

Initial developer's notes (retired) for TrueNAS SCALE are available on the TrueNAS Documentation Hub. Note that because SCALE shares a similar user interface as the FreeBSD-based TrueNAS CORE, many of the current documentation articles also apply to SCALE. SCALE feature-specific articles will be added to the SCALE section as the software approaches its first full release.

Code-named Angelfish, TrueNAS SCALE-ALPHA follows a year.month scheme for versioned releases. Because this is an ALPHA release of the software, not all planned features are present. The status of major features are listed here, along with the full changelog of bug fixes that are part of the SCALE 20.12-ALPHA release.

Software Features

Verified

Verified Features are generally working in SCALE. Minor bugs could be present.

- Pool Management
- SMB Shares
- iSCSI Shares
- NFS Shares
- S3 Shares
- AFP Shares
- AD / LDAP Directory Services
- Online / Offline updating
- Virtual Machines (Using KVM)
- WebDAV
- Monitoring, Alerting and Reporting
- POSIX 1e support
- Boot Environments
- SSH Credentials
- ZFS Encryption
- Cloud Sync
- Replication
- TrueCommand Cloud connections

Provisional

These features have been added, but have known issues or are not fully feature-complete. Please use only with caution.

- Applications UI
- Tasks:
  - Cron
  - Init/Shutdown Scripts
  - S.M.A.R.T. testing
  - Resilver prioritization
  - Periodic Snapshots
  - Rsync
  - Scrub
- Docker Images deployed as Helm Charts with Kubernetes NVIDIA / Intel Quicksync GPU passthrough (CLI)
- Wireguard (CLI)
- Networking and Settings UX Refresh
- OpenVPN Client and Server
- Two-factor authentication
- Certificate Management

Experimental

These features are still in early development and will be landing in Nightly images of SCALE in the near future.

- Clustered Datasets API support for TrueCommand
- TrueCommand Clustering UI for SCALE
- NFSv4 ACL support

Change Log

New Feature

- [NAS-100018] - S.M.A.R.T tests not sticky when disk is replaced
- [NAS-104324] - Platform dependent IPMI plugin
- [NAS-104374] - Google requiring oauth for sending mail starting June 2020
- [NAS-105082] - Allow hiding network interfaces from dashboard.
- [NAS-107305] - TrueNAS User Performance Monitoring
- [NAS-107619] - Tuneables for M-Series Gen3
- [NAS-107628] - Support IPv6 for HA
- [NAS-107864] - GMail OAuth when configuring e-mail
- [NAS-107923] - TrueCommand Icon: un-grey it
- [NAS-108039] - Kubernetes Catalog Support
- [NAS-108068] - Add iftop option for SNMP service
- [NAS-108070] - Add properties_override replication option
- [NAS-108074] - Bind services to 0.0.0.0 when removing IP address from interface configuration
- [NAS-108166] - R-Series support in enclosure API
- [NAS-108271] - New alert service: Telegram
- [NAS-108322] - Applications UI implementation
- [NAS-108323] - Add cloud credentials pCloud "hostname" field

- [NAS-108329] - R-Series Dashboard widget product images

Improvement

- [NAS-102208] - Disable the ability to create pools, etc on an HA system with mismatched TN versions
- [NAS-105947] - Add regression testing for netwait
- [NAS-107463] - Allow creating encrypted dataset on receiving side
- [NAS-107495] - Assign new Extent to existing Target
- [NAS-107498] - iSCSI filter by FC/iSCSI/BOTH
- [NAS-107507] - Prompt user to add Kerberos keytab entries as needed in NFS form.
- [NAS-107534] - Create dashboard for Backup Credentials
- [NAS-107651] - Metadata (Special) Small Block Size
- [NAS-107661] - Rename Initiators in iSCSI
- [NAS-107694] - Expose option to enable / disable TRIM in Advanced Menu
- [NAS-107706] - Make a global titlebar component with optional breadcrumbs
- [NAS-107735] - Create Dashboard for Certificates
- [NAS-107751] - Make Save Config easier to find
- [NAS-107788] - Add extra ZFS ARC stats to reporting.realtime
- [NAS-107789] - Current bandwidth % per interface on reporting.realtime
- [NAS-107790] - Add pool.query event
- [NAS-107791] - Add pool.dataset.query event
- [NAS-107793] - Add *.query event
- [NAS-107819] - 12 interfaces to SCALE
- [NAS-107823] - Proxy collectd graphite stream
- [NAS-107829] - Overall system disks stats in reporting.realtime
- [NAS-107830] - Add call to return non-idle processes
- [NAS-107902] - Turbostat In TrueNAS Scale
- [NAS-107905] - When usage collection is disabled - Only report the total capacity
- [NAS-107929] - zfs/snpashot endpoint only returns "false" on failure
- [NAS-107944] - Use new TrueCommand logo
- [NAS-107994] - Gluster Config does not persist Upgrades
- [NAS-108108] - Python with debug and no optimizations
- [NAS-108156] - Redundant forms on Network Page
- [NAS-108173] - Increase vCore limit for KVM under SCALE
- [NAS-108189] - Add HA platform detection for bhyve
- [NAS-108213] - Iconic template icon does not work on white background
- [NAS-108348] - Slide out dataset options form
- [NAS-108349] - Slide out zvol create/edit form
- [NAS-108359] - No ix-auto in Test Changes, Revert Changes changes button
- [NAS-108360] - Fix ix-auto directives on Storage page Global Actions
- [NAS-108391] - Slide out pool import wizard
- [NAS-108495] - Missing ix-auto in -> and + button in Sharing/iSCSI/Initiators/Add on 12.0

Bugs

- [NAS-102006] - Improve Alert Settings page
- [NAS-104668] - Make SED disks handling platform dependent
- [NAS-105156] - Upgraded to 11.3, Cloud Sync to B2 rclone failing
- [NAS-106351] - remove code related to hardware older than z-series
- [NAS-106424] - Add support for Xen/XCP-ng xe-guest-utilities
- [NAS-107187] - Disks page does not show Pool affiliation in Pool column
- [NAS-107317] - Replication progress % Incorrect
- [NAS-107318] - replication target as non-root cannot mount
- [NAS-107354] - Package remote-pdb in SCALE
- [NAS-107384] - 2FA for SSH plus LDAP ignores 2FA
- [NAS-107419] - Replicated datasets of encrypted pools to another encrypted pool is inaccessible
- [NAS-107527] - allow creation of failover lagg from netcli
- [NAS-107577] - Tunables regex prevents editing/creation of valid tunables
- [NAS-107590] - mDNS not starting? Server not visible to macOS clients
- [NAS-107600] - iSCSI target deletion via 12rc1 GUI does not remove connection
- [NAS-107609] - Alerts for NFS services could not bind to specific IP addresses, using 0.0.0.0.
- [NAS-107638] - Deleting mountpoint of a jail doesn't update UI
- [NAS-107643] - glusterd service api
- [NAS-107644] - glusterd-events service api
- [NAS-107646] - GUI shouldn't allow IPv6 to be attempted on HA
- [NAS-107647] - ZFS dataset creation can fail with UTF decode error
- [NAS-107677] - ensure glusterd related services are started after zpool import service
- [NAS-107678] - hide vhid option on SCALE HA webUI
- [NAS-107697] - WebUI makes firefox 80.0.1 hang
- [NAS-107702] - Misleading validation in EDIT IDMAP dialogue
- [NAS-107713] - Saving ACLs aborted on click
- [NAS-107737] - IP address cannot be modified
- [NAS-107753] - Ldap Messages for root and operator
- [NAS-107784] - nfs alias issues on SCALE
- [NAS-107800] - SCALE HA webUI side-bar issues
- [NAS-107808] - "File ticket" form fields are not aligned
- [NAS-107809] - Attaching screenshots to "File ticket" form has no visual feedback
- [NAS-107832] - Network activity does not seem to be behaving properly on dashboard
- [NAS-107840] - Broken ACL editor shown after creating home share

- [NAS-107845] - fix device.get_disks on SCALE HA
- [NAS-107851] - Make dns_domain_name optional in idmap form
- [NAS-107857] - replace lshw in ixdiagnose with alternative
- [NAS-107860] - replace lshw in device.get_info GPU with alternative
- [NAS-107873] - SCALE: Adding Static Route does not show up on Summary page
- [NAS-107884] - "Network connectivity will be interrupted." message is incorrect
- [NAS-107888] - change "FreeNAS" to "TrueNAS" in vmware plugin
- [NAS-107892] - Cloud sync task "Advance options" should probably be "Advanced options"
- [NAS-107907] - add better validation to update.manual API
- [NAS-107914] - TrueNAS alerted me to a NextCloud update, but the updater says it was already up to date
- [NAS-107918] - sas2flash segmentation fault
- [NAS-107927] - NFS cannot bind IP
- [NAS-107928] - CLONE - CPU temperature graph always has a drop to zero at the end
- [NAS-107933] - Periodic snapshot task calendar is broken
- [NAS-107948] - [User error] Ability to delete System Dataset is too easy - UI suggestions.
- [NAS-107955] - Internal services classes showing up in API docs
- [NAS-107957] - middlewared crashing too many files no login
- [NAS-107987] - [SCALE] Fails to change nginx HTTP listen port for WebUI
- [NAS-107988] - Can't delete newly created user on SCALE
- [NAS-107992] - proftpd starts in SCALE after pool import
- [NAS-108005] - Replication Task: divide by zero
- [NAS-108010] - ntb0 broken on upgrade to 12.0-RELEASE
- [NAS-108020] - iSCSI CHAP passwords incorrect after upgrade to 12.0-RELEASE
- [NAS-108023] - email save throws an error
- [NAS-108024] - Add GUI deprecation warning for samba_schema in LDAP plugin
- [NAS-108031] - Retry download of update
- [NAS-108047] - make sure HA SCALE accounts for IPv6
- [NAS-108048] - investigate link-local IPv6 address removal on SCALE
- [NAS-108050] - SNMP consuming 100% CPU and becomes unavailable
- [NAS-108056] - Ignore/reset zfs mountpoint property on ZFS replication task
- [NAS-108059] - Only submit usage stats from the MASTER node if failover licensed
- [NAS-108064] - only ask for subnet mask once on HA systems
- [NAS-108065] - change verbiage in network section for HA systems
- [NAS-108067] - Kerberos Ticket not refreshed (regression)
- [NAS-108071] - typo in EUI64 ipv6 link-local generation and only generate if one doesn't exist
- [NAS-108072] - keepalived.conf indentation issue
- [NAS-108075] - FreeNAS fails to create alert for failed power supply that IPMI does detect as failed
- [NAS-108085] - Pool disk details duplicated on other pool's frame in dashboard
- [NAS-108087] - Bad GPTID label text
- [NAS-108089] - CPU widget temperature legend color doesn't match bar color
- [NAS-108097] - Time Machine not advertised after unlocking dataset until SMB is manually restarted
- [NAS-108102] - Fix routing from pool manager to storage page
- [NAS-108110] - Exporting pool(s) on TrueNAS 12.0-RELEASE
- [NAS-108117] - Replication task fails when created with a throttle
- [NAS-108120] - API v2 regression broke user creation
- [NAS-108124] - Periodic Snapshot Task Creation allows use of inappropriate characters (i.e. forward slash "/") in snapshot name
- [NAS-108129] - Truenas SCALE UI broken for VM creation
- [NAS-108140] - make sure ix-postinit runs as one of the last services in startup
- [NAS-108141] - [SCALE] Shares cannot support both NFS and SMB
- [NAS-108144] - UPS connection lost after failover
- [NAS-108155] - Missing global action buttons for network dashboard
- [NAS-108171] - stripe option is deprecated in gluster
- [NAS-108183] - UPS shutdown leaves passive up on HA system
- [NAS-108185] - Pull replication fails - ps command has wrong (missing) flags
- [NAS-108204] - [SCALE] nfsv4 shares do not export properly
- [NAS-108209] - Add delete call to VMWare Snapshot in SCALE
- [NAS-108210] - Remove unneeded first step for Import Pool wizard for SCALE
- [NAS-108220] - Replication failed: cannot send <snapshot name>: encrypted dataset may not be sent with properties without the raw flag
- [NAS-108222] - pull replication seems ummount replicated dataset
- [NAS-108223] - hide ".glusterfs" from pool.dataset.query
- [NAS-108235] - sysctl rc script is running twice on boot breaking carp.allow
- [NAS-108240] - I cannot change the LAGG protocol type in the aggregation setting in WebUI
- [NAS-108273] - Traceback printed on VM operations
- [NAS-108278] - add ability to set quota on gluster volumes
- [NAS-108279] - Truenas Scale : UPS monitor password is mandatory but it is not shown and error message is unclear
- [NAS-108282] - return verbose information from gluster.volume.status by default
- [NAS-108286] - Can't connect to pCloud
- [NAS-108288] - duplicate shell entries local users
- [NAS-108292] - SCALE Shows "Unknown CPU"
- [NAS-108294] - HA network validation isn't working
- [NAS-108302] - Actions button disappeared from the pool status page
- [NAS-108308] - Cant add google cloud service account
- [NAS-108313] - failover.control and failover.update are broken on HA systems
- [NAS-108330] - Snapshot expirations fail when there are too many of them at once
- [NAS-108331] - plumb the gluster related config into smb plugin API
- [NAS-108335] - Remove Mirror is not working
- [NAS-108343] - Error when deleting target in use
- [NAS-108345] - Cron jobs are blocking each other from running

- [NAS-108351] - Error (traceback) when editing unrelated properties on dataset with certain zstd (zstandard) compression levels
- [NAS-108353] - Math error in pool creation dialog
- [NAS-108354] - unable to delete VM due to XML error
- [NAS-108371] - UI says replication failed..but it worked
- [NAS-108376] - Fix console error for tables
- [NAS-108396] - Linked release notes are to wrong version (11.3U5 -> 12)
- [NAS-108405] - netatalk is broken on SCALE
- [NAS-108413] - Make truenas.set_production a job
- [NAS-108416] - Convert Pool Status Disk Edit to slide out form
- [NAS-108417] - Make Settings > Change Password into a Dialog
- [NAS-108423] - Dashboard for CPU & memory do not show values, also reporting is missing
- [NAS-108473] - '>' not supported between instances of 'str' and 'Version'
- [NAS-108475] - CLONE - Error (traceback) when editing unrelated properties on dataset with certain zstd (zstandard) compression levels
- [NAS-108485] - Repliaction tasks, key-format validation on edit, incorrectly setting all-caps?
- [NAS-108499] - Remove red border around cron picker
- [NAS-108504] - Popup on dashboard will not go away
- [NAS-108520] - high concurrency api requests result in invalid responses
- [NAS-108529] - [SCALE] Unable to create a debug
- [NAS-108539] - Reporting graphs missing / rrdcached errors spamming log
- [NAS-108553] - Degraded pool alert not received in UI or Email
- [NAS-108560] - Pool status will not update unless system is restarted/system panics
- [NAS-108562] - Unable to access FTP using "Allow Root Login" option
- [NAS-108578] - zettarepl failing to pull-replicate a dataset with canmount=noauto (12.0-U1 regression)

20.10-ALPHA

20.10-ALPHA

October 16, 2020

iXsystems is pleased to release the first Alpha version of TrueNAS SCALE! SCALE is the newest member of the TrueNAS software family. When complete, SCALE will have all major TrueNAS CORE storage and sharing features and web interface based on Debian GNU/Linux. There will also be additional SCALE-specific features that are derived from the application's Linux base. The major features of SCALE are represented in the application acronym:

Scaled-Out ZFS
Converged
Active-Active
Linux Containers
Easy to Manage

Initial developer's notes for TrueNAS SCALE are available on the TrueNAS Documentation Hub. (developer's notes are now retired, please see the SCALE documentation content instead.) Note that because SCALE shares the same UI as the FreeBSD-based TrueNAS CORE, many of the current documentation articles also apply to SCALE. SCALE feature-specific articles will be added to the TrueNAS SCALE page as the software approaches its first full release.

Code-named Angelfish, TrueNAS SCALE-ALPHA will be following a **year.month** scheme for versioned releases. Because this is an ALPHA release of the software, not all planned features are present. The status of major features are listed here, along with the full changelog of bug fixes that are part of the SCALE 20.10-ALPHA release.

Features

Verified

Verified Features are generally working in SCALE. Minor bugs could be present.

- Pool Management
- SMB Shares
- iSCSI Shares
- NFS Shares
- S3 Shares
- AFP Shares
- Online / Offline updating
- Virtual Machines (Using KVM)
- WebDAV
- Monitoring, Alerting and Reporting

Provisional

These features have been added, but have known issues or are not fully feature-complete. Please use only with caution.

- Cloud Sync Tasks
- Docker with Kubernetes (CLI)
- Docker with NVIDIA gpu passthrough flags (CLI)
- AD / LDAP Directory Services

- Wireguard (CLI)
- Networking and Settings UX Refresh

Experimental

These features are still in early development and will be landing in Nightly images of SCALE in the near future.

- Applications UI
- Clustered Datasets API support for TrueCommand
- TrueCommand Clustering UI for SCALE
- POSIX 1e / NFSv4 ACL support

Cautions

As the root user, it is possible to load additional software via the apt package manager commands. This is useful for developers on experimental systems who are trying new features or diagnosing issues. Installing the wrong packages could render a system non-functional and caution should be taken.

Packages downloaded via apt are not persistent. They will not survive an upgrade and may negatively impact normal operation. Users of operational systems should not use the apt command unless advised by the developers. For persistence between upgrades, users should deploy custom packages as containers.

Bug Fixes

Key	Summary	Component/s
NAS-107933	Periodic snapshot task calendar is broken	WebUI
NAS-107931	Selecting a certificate for LDAP	
NAS-107907	add better validation to update.manual API	Middleware
NAS-107886	CPU temperature graph always has a drop to zero at the end	Reporting
NAS-107879	Traceback on interface pre sync	Middleware
NAS-107872	build syslog-ng with debug symbols	OS
NAS-107859	SCALE - Networking Changes aren't fully applied on reboot	
NAS-107842	Failure to approve acme cert	Certificates
NAS-107837	Can't change security setting for NFS share	WebUI
NAS-107836	internal interface on SCALE HA are not being configured on boot	Middleware
NAS-107831	fix failover on SCALE HA	Middleware
NAS-107809	Attaching screenshots to "File ticket" form has no visual feedback	
NAS-107802	traceback in hactl along with flake8 fixes	Middleware
NAS-107784	nfs alias issues on SCALE	WebUI
NAS-107779	SCALE HA code running on non-enterprise hardware	Middleware
NAS-107770	fix failover.vip.check_states logic on SCALE HA	Middleware
NAS-107764	iface.up() on SCALE HA internal heartbeat interface	Middleware
NAS-107763	Method 'force' not found in 'failover.fenced'	Middleware
NAS-107738	fenced is not panic'ing on SCALE HA	Middleware
NAS-107736	reporting.realtime Event: Network rates wrong	Middleware

Key	Summary	Component/s
NAS-107724	traceback in vrrp_hook_license_update	Middleware
NAS-107723	traceback in failover.sync_from_peer	Middleware
NAS-107720	multiple issues with netcli	Middleware
NAS-107707	plumb in fenced into failover plugin on SCALE HA	Middleware
NAS-107704	add py-sgpersist to scale build	Middleware
NAS-107703	add py-fenced to scale build	Middleware
NAS-107686	trailing slash breaks NFS permanently?	NFS
NAS-107678	hide vhid option on SCALE HA webUI	Middleware
NAS-107674	middleware, Traceback issue at iddle	Middleware
NAS-107664	Update bug renders SCALE non bootable	Middleware
NAS-107655	JS console error complaining that model property is missing	WebUI
NAS-107644	glusterd-events service api	Middleware
NAS-107643	glusterd service api	Middleware
NAS-107617	FreeNAS 11.3 upgrade to TrueNAS 12.0RC1 does not migrate user passwords	Upgrades
NAS-107603	Replication that worked in 11.3-U4 and 12.0-Beta2 fails in 12.0-RC1	Replication
NAS-107587	SSH Keypair input validation issue Again	WebUI
NAS-107552	Timezone mismatch in reporiting graphs	Reporting
NAS-107545	CloudSync Dryrun isn't dry	Middleware
NAS-107531	Comment and restrict change of large blocks support in replication	Replication
NAS-107529	Snapshot option missing for Zvol's in contextual menu on pools UI	Snapshot, WebUI
NAS-107526	Failed Error when clicking Expand Pool	
NAS-107516	S3 Sync Task Part number must be an integer between	Tasks
NAS-107506	Additional Domains don't show up on save	Middleware, WebUI
NAS-107502	NetBIOS Alias value is not saved after Server reboot	Services
NAS-107483	SCALE SMB Shares Unusable	
NAS-107479	SMART Service Fails to Start	SMART
NAS-107436	Elements in "Title Bar" no longer Clickable	WebUI
NAS-107417	NVME disks are listed twice AMD	
NAS-107413	replication failures	Replication

Key	Summary	Component/s
NAS-107411	No Task Manager Progress is shown	Replication
NAS-107409	nfs shares can be created outside zpool path	Middleware
NAS-107407	Default uid for new users may be less than 1000	Middleware
NAS-107402	Migration of SMB "show hidden files" option is backwards	
NAS-107401	Disable autocomplete for 2FA code on login page	WebUI
NAS-107400	Inconsistency if root pw is required for DL of encryption key	System
NAS-107387	traceback in peer and volume gluster plugin	Middleware
NAS-107361	Truenas Scale: Empty create smb share	
NAS-107354	Package remote-pdb in SCALE	Middleware
NAS-107353	Traceback on available memory for VM	Middleware
NAS-107350	Can't import pools from CORE to SCALE	ZFS
NAS-107348	high cpu usage by middleware...slow performance	Middleware
NAS-107346	Problems with listing and deleting jails and plugins	Middleware
NAS-107332	Issue with 2FA in TrueNAS Core 12 Beta2	System
NAS-107328	ACL editor does not reflect preselected template	WebUI
NAS-107315	middlewared memory leak	Middleware
NAS-107314	Replicated dataset is not set to read-only	Replication
NAS-107302	Inappropriate message / incorrect handling, when an old config references datasets/vols that no longer exist.	WebUI
NAS-107273	tracebacks in smb plugin on SCALE	Middleware
NAS-107263	When running a scrub from the pools manual it shows a GUI bug	Console
NAS-107260	Date columns do not sort correctly	WebUI
NAS-107257	WebUI Pool Status empty	WebUI
NAS-107256	Cluster of service fails and middleware connections fails, 12-beta2	
NAS-107248	Snapshot Extra column "Used", incorrect sorting	
NAS-107238	Cancel doesn't work during install of TrueNAS SCALE	Boot Environments
NAS-107235	Error when updating a Jail 11.3-RELEASE-p6 to 11.3-RELEASE-p612	Middleware
NAS-107229	Virtual Machine Next Button and Breadcrumbs Broken	WebUI
NAS-107226	middlewared_truenas/plugins/enclosure_/map.py TypeError line 66	Middleware
NAS-107217	Theming issues after merge of WIP	

Key	Summary	Component/s
NAS-107213	SMB Service Save - TypeError occurs	SMB
NAS-107165	Cannot add cache disk to existing pool	
NAS-107164	Jails not mounting after update to 12.0BETA2	
NAS-107158	Unable to upload config file in 12.0 BETA2	
NAS-107154	Fix issue with smb share generation	
NAS-107148	Generate a random default serial extent	
NAS-107143	Ensure groupmap entries are properly added / deleted on group.update	
NAS-107142	Add tests for SMB groupmaps	
NAS-107141	remove excess logging info when syncing disks	
NAS-107140	Expand api tests for user	
NAS-107135	SMB status change does not update passdb/groupmap	
NAS-107130	Add test to verify builtin users are not smb users	
NAS-107129	SMART test results doesn't handle 0 results	
NAS-107123	Add catia mappings for special Apple characters	
NAS-107121	`failover_aliases` and `failover_virtual_aliases` are being overwritten as empty arrays	WebUI
NAS-107120	change failover_vhid to type `select` instead of `input`	WebUI
NAS-107116	allow editing empty interfaces	
NAS-107115	Newly created builtin users should not default to 'smb'	
NAS-107112	Strip newline from plugin-properties	
NAS-107107	Clear any potential stale state after leaving AD domain	
NAS-107104	ACME DNS renewals don't work	Certificates
NAS-107102	Report HA in usage statistics	Middleware
NAS-107101	Top bar "resilvering" shows 0% constantly when it's 60% done.	
NAS-107100	Do not run check_available in a tight loop in case an exception happens	
NAS-107099	Do not display previous replication task status after deleting it and…	
NAS-107085	Disable fruit:locking on time machine shares	
NAS-107076	Expand regression tests for user api	
NAS-107074	Permissions are incorrect on home directory move	
NAS-107073	Dashboard interface cards show impossible throughput values	

Key	Summary	Component/s
NAS-107069	Symlink /usr/share/skel to /etc/skel in FreeBSD	
NAS-107067	Fix chown of skel directory contents for new local users	
NAS-107060	NFS statistics GUI are wrong.	
NAS-107053	Pool in dashboard omits special vdevs from count and status	WebUI
NAS-107052	Cannot replicate encrypted datasets	
NAS-107050	Jails not auto-started after unlocking encrypted iocage dataset	
NAS-107046	Cannot seem to delete network interfaces	WebUI
NAS-107035	Swap size setting not honored on 4k sector disks	WebUI
NAS-107032	Unable to upload 8TB file to backblaze.	Middleware
NAS-107031	OpenVPN autostart not working	
NAS-107029	Unable to configure UPS on TrueNAS 12	WebUI
NAS-107027	Add JRA async DNS patches to samba	
NAS-107023	Expand list of error strings that should trigger an AD rejoin	
NAS-107021	Make failover faster by not doing failover.status_refresh when it's not necessary	
NAS-107013	Leftover debug message for acltype	
NAS-107012	Omit debug botocore module log	
NAS-107011	Add idmap regression tests for AD environments	
NAS-107009	System generated SSH host key does not persist through reboot	OS
NAS-107007	OpenVPN Service : Additional parameter need to be textarea	Services
NAS-106999	Human-readable error for deleting used cloud credential	
NAS-106998	middlewared_truenas/plugins/enclosure.py AttributeError line 342	Middleware
NAS-106995	24h clock not shown on dashboard	WebUI
NAS-106994	OpenVPN Service : Could not determine IPv4/IPv6 protocol	
NAS-106993	Reassign sys.{stdout,stderr} after log rollover	
NAS-106991	Reduce SMB-related log entries	
NAS-106988	Attempting to export/offline share while in use causes crash/exception	
NAS-106986	Add regression tests for SMB registry configuration	
NAS-106984	"jls" hostname does not reflect modified hostname	
NAS-106981	Changing Default ACL Options resetting user changes	

Key	Summary	Component/s
NAS-106978	Add regression tests for AD machine account keytab generation	
NAS-106973	kbdmap_choices in SCALE	Middleware
NAS-106972	AFP not running on SCALE	Middleware
NAS-106966	collectd: blank warning emails	
NAS-106965	qBittorrent Plugin Not Installing	Plugins
NAS-106964	Overlapping tooltips	WebUI
NAS-106962	Update zettarepl port	
NAS-106961	Fix bug	
NAS-106955	Clarify reboot instructions in installer	Installation
NAS-106953	Improve validation for SMB service and shares	
NAS-106948	Recycle bin versioning not enabled	Middleware
NAS-106946	AD faulted, no error	Directory Services
NAS-106941	Incorrect parent check when unlocking encrypted dateset	Middleware
NAS-106936	Handle ZoL error messages	
NAS-106928	zettarepl middlewared file descriptor leak	Middleware
NAS-106923	traceback in ready_system_sync_keys	Middleware
NAS-106921	Expand ACL testing regimen	
NAS-106912	Make sure ix-shutdown is not stopped after middlewared	
NAS-106902	VM libvirt connection improvements	
NAS-106901	Clear out bootready file on boot	
NAS-106894	webUI no longer allows login on SCALE HA	WebUI
NAS-106893	run LicenseStatus on ENTERPRISE and SCALE_ENTERPRISE	
NAS-106891	fix LicenseStatus alert on SCALE	
NAS-106889	traceback in failover event plugin	Middleware
NAS-106875	Add directory services to usage stats	Middleware
NAS-106874	WebDAV service tests failing	Middleware
NAS-106872	Update py-libzfs port	
NAS-106871	Fix migrations state	
NAS-106866	Proper/better errno for failed authentication	Middleware

Key	Summary	Component/s
NAS-106864	SED doesn't work for nvme	Middleware
NAS-106858	Clarify bootloader options to be more verbose	
NAS-106854	plugin boot checkbox re-enables itself	WebUI
NAS-106851	Truenas Scale - Incorrect CPU temperature displayed in Dashboard Widget	Dashboard, WebUI
NAS-106850	Correctly split on cases where there are multiple '='	
NAS-106847	Detaching device from boot mirror but not physically removing from the system can cause boot loader confusion	Middleware
NAS-106844	KMIP is a TrueNAS Enterprise feature	WebUI
NAS-106842	Setting IPMI to DHCP should gray-out IP addresses	WebUI
NAS-106840	setting invalid VHID value fails silently.	HA, WebUI
NAS-106833	Scale SMB - override build options for statedir and private dir	
NAS-106827	Remove extra debug statements from directory service refresh	
NAS-106826	fix hardware detection for M and X on SCALE	Middleware
NAS-106825	Update zettarepl port	
NAS-106822	Use path to determine plugin version	
NAS-106821	Fix handling recoverable errors	
NAS-106818	When replicating without a Periodic Snapshot task, Recursive is not working.	Replication
NAS-106812	TrueNAS CORE 12.0 -- Import of certificates is impossible.	Certificates, System
NAS-106808	Ensure monpwd/monuser fields are provided for UPS service	
NAS-106807	Cover rm -rfx usages in scale to use --one-file-system	
NAS-106806	Unknown CARP state None	Middleware
NAS-106800	Retrieve plugins version data from packagesite.txz	
NAS-106798	api context /services/iscsi/targettoextent does not allow null value for iscsi_lunid	API, iSCSI
NAS-106797	Periodic Snapshot Tasks - "Enabled" checkboxes are not unique inputs	Snapshot, Tasks
NAS-106796	Unlock encrypted datasets when initialising KMIP keys	
NAS-106795	Modify migration to simplified SMB configuration setup	
NAS-106794	write_if_changed may block the event loop as it does sync file ops	
NAS-106789	Unable to open UI on recent SCALE ISO	WebUI
NAS-106787	iSCSI webUI columns COMPLETELY break when edited	iSCSI, WebUI
NAS-106783	Change default hostname to truenas	

Key	Summary	Component/s
NAS-106780	Treat most of the paramiko errors (e.g. SSH banner errors) as recover…	
NAS-106773	Host guest configuration for KVM guests	
NAS-106770	iocage upgrade of existing jail not functional	Middleware
NAS-106768	fix HA API tests	API
NAS-106764	SNMP FREENAS-MIB not working	Services
NAS-106763	New Replication tasks fail on SCALE	Middleware
NAS-106751	Disk power management is FreeBSD specific	Middleware
NAS-106750	Traceback syncing routes	Middleware
NAS-106748	Traceback on user creation	Middleware
NAS-106747	User page doing invalid sharing.smb.query call	WebUI
NAS-106740	Error when entering email address in UPS setup.	WebUI
NAS-106735	Add support for nested VM's in SCALE	
NAS-106734	fix SCALE API for configuring network	Middleware
NAS-106732	adding or deleting alias on HA systems cause DISAGREE_CARP alert	Middleware
NAS-106730	Update Samba to 4.12.5	
NAS-106729	Samba s3:smbd - add acl_brand to struct connection_struct	
NAS-106728	Fixes for pkg in latest 12-stable	
NAS-106726	Donot collect jails/plugins usage in SCALE	
NAS-106723	traceback when configuring an alias on HA systems	Middleware
NAS-106722	Update zettarepl port	
NAS-106721	deleting interface on HA system does not remove info from standby	Middleware
NAS-106719	service middlewared restart leaves orphaned processes behind	Middleware
NAS-106716	Update migrate113 port	
NAS-106714	critical interfaces are being marked as non-critical	Middleware
NAS-106713	Cron job still runs despite being deactivated and then deleted	Tasks
NAS-106707	falover -> failover	
NAS-106703	Ensure that permissions for tmp are correct during smb.configure	
NAS-106702	SMB shares mounted in Windows cannot set the sparse flag	
NAS-106697	We'll have to replicate system dataset if we want full replication	

Key	Summary	Component/s
NAS-106694	Samba:s3:modules:aio_fbsd - remove extra calloc()/free()	
NAS-106693	Only map partitions which have valid partition uuid	
NAS-106692	Fix VM console command	
NAS-106691	Update zettarepl port	
NAS-106690	Can't clear Kerberos Principal from GUI	WebUI
NAS-106688	Fix validation check for user quotas	
NAS-106683	Use correct rsync path for SCALE	
NAS-106682	Validation Error on creation of Manual SSH Connection for Replication Task	Replication
NAS-106681	Fix stdout read	
NAS-106673	Cannot export pool with system dataset on	Middleware
NAS-106672	resilver progress not updated	Dashboard
NAS-106671	Inconsistency in pool health widgets	Dashboard
NAS-106665	Browser cache issues cause tables to malfunction	WebUI
NAS-106653	System → Advanced lacks syslog options	WebUI
NAS-106648	Make registry configuration aware of locked datasets	
NAS-106642	Fix TN HA NFS config validation	
NAS-106641	VM Console should use shell endpoint in middleware	WebUI
NAS-106640	Do not update grub on first boot when system is ready	
NAS-106639	Fix traceback in ldap.conf generation script when AD enabled	
NAS-106638	Fix regression in winacl's chown()	
NAS-106634	Do not check ABI difference on upgrades	
NAS-106632	Unable to list or manage plugins in UI	Plugins
NAS-106626	Update zettarepl port	
NAS-106625	Cannot add/apply network interface option	
NAS-106620	Prevent users from setting user / group quota on id 0	
NAS-106616	Delete BE option not visible in SCALE	WebUI
NAS-106613	Always add server auth extension to default certificate created	
NAS-106612	CLONE - OpenVPN Service configuration issues	Certificates, Networking, Services
NAS-106611	Don't log libvirt connection failure if there are no vm's	

Key	Summary	Component/s
NAS-106610	Move plugins from official plugins list to community plugins	
NAS-106599	Add timeout for ix-etc service	
NAS-106598	iscsi portal IP traceback in webUI	Middleware
NAS-106589	fix(midclt): properly handle job call to show progress and not rewind	
NAS-106587	disabling wsdd causes traceback	Middleware
NAS-106584	Unable to access serial console for VM's	WebUI
NAS-106583	FreeNAS disks forget their assigned pool	ZFS
NAS-106582	unable to upgrade from master to internal	Middleware
NAS-106581	Traceback in interface.query	Middleware
NAS-106579	Remove deprecated AD parameters	
NAS-106577	SMB using LDAP will not start when restoring a configuration on new system	Directory Services, SMB, System
NAS-106575	Fix 12 config upload	
NAS-106574	Remove exra wait argument from dhclient start	
NAS-106571	Make sure we move uploaded config to tn db location in scale	
NAS-106570	Error creating user "File not found error" "/usr/share/skel"	System
NAS-106569	Static Route API not working	Middleware
NAS-106568	Empty attributes in interface.query	Middleware
NAS-106563	update-grub error on API tests	Middleware
NAS-106547	Changing DHCP to static with BPF enabled doesn't clear IP config completely.	Plugins
NAS-106546	Move radarr/sonarr to community repo	Plugins
NAS-106545	All passwords are visible while unlocking datasets	WebUI
NAS-106541	Cloud Sync to Backblaze B2 fails	Tasks
NAS-106538	Expose method to retrieve list of all systemd units	
NAS-106537	Form submission does not lead back to listing extents	WebUI
NAS-106535	Make sure netcli features work in SCALE	Middleware
NAS-106531	Get rid of swapsize on TrueNAS for data disks	Middleware, WebUI
NAS-106530	Donot create swap partition for TN enterprise on pool creation	
NAS-106528	Order datasets alphabetically in Storage screen	WebUI
NAS-106527	Change wording when we create zfs encrypted pools	WebUI

Key	Summary	Component/s
NAS-106520	Fix product type on VM's	Middleware
NAS-106518	Detach option not appearing in pool manager (needed to promote a spare)	WebUI
NAS-106517	Replication tasks - entire dataset keeps being resent	Replication
NAS-106497	Recursive Replication via GUI not possible	Replication
NAS-106486	Custom update server for SCALE	Middleware
NAS-106483	Label "Overview" translate does not work in some widgets	
NAS-106482	NVMe reservation in fenced	Middleware
NAS-106480	Investigating having zinject in zfs package	Middleware
NAS-106479	Query middleware to determine types of tunables to be exposed in UI	WebUI
NAS-106473	Unable to use Active Directory Account for new Rsync Module	WebUI
NAS-106469	Trivial Screen Display Bug	Dashboard
NAS-106455	OpenVPN Service configuration issues	Certificates, Networking, Services
NAS-106442	locked dataset exported via nfs	NFS
NAS-106435	ZFS replicate recursive fails: No such file or directory	Console, Replication, ZFS
NAS-106430	failover.force_master is freebsd specific	Middleware
NAS-106417	status method in failover plugin calls freeBSD specific methods	Middleware
NAS-106405	enclosure detection traceback	Middleware
NAS-106390	SSH error messages filling up console during ZFS replication	Middleware
NAS-106381	get rid of /tmp/failover.json	Middleware
NAS-106380	carp related methods in failover plugin are freebsd specific	Middleware
NAS-106343	syslog-ng not working on SCALE	Middleware
NAS-106342	netcli doesnt work on SCALE	Middleware
NAS-106338	internal_interfaces method is freeBSD specific	Middleware
NAS-106333	sync_internal_ip method is freeBSD/CARP specific	Middleware
NAS-106325	generic method for random string generation	Middleware
NAS-106324	fix wsclient on SCALE	Middleware
NAS-106323	make hactl work on SCALE	Middleware
NAS-106181	avahi-daemon spams logs on TN HA systems	OS
NAS-106177	Package minio	Middleware

Key	Summary	Component/s
NAS-106110	UPS ups is on battery power alerts since upgrade to 11.3	Middleware
NAS-106087	Setup iSNS server(s) in the lab	iSCSI
NAS-106004	SED disks not unlocking at boot	WebUI
NAS-105645	zfs-stats -a shows unknown oids and divide by 0	OS
NAS-105511	vfs.zfs.arc.max at 16GiB if not set manually on 32GiB system, nightly 12.0	OS
NAS-105156	Upgraded to 11.3, Cloud Sync to B2 rclone failing	Middleware
NAS-105099	Periodic Snapshot are missing the lifetime in its name	
NAS-104906	Rsync tasks view shows incorrect remote path	Tasks
NAS-104837	Investigate usgae of pyudevd to simplify disk retrieval code	
NAS-104665	Investigate automatic builds for TN Scale packages	Build system
NAS-104615	Create a dump on disk for linux	Middleware
NAS-102808	Running Cloud Sync tasks keep on running after deletion in GUI	Cloud Credentials, Middleware
NAS-101008	iSCSI extents on all-flash pool should have option serseq set to "off"	iSCSI, Middleware

Known Issues

Seen In	Key	Summary	Workaround	Resolved In
22.02.4		Upgrading from 22.02.4 to 22.12-BETA.1 is known to not work.	Workaround is to either upgrade from a version before 22.02.4 or to upgrade to 22.12-BETA.2 when it is released.	Targeted 22.12-BETA.2
22.02.4	N/A	UPS Reports Disabled	Support for UPS reporting page is temporarily disabled due to an upstream issue with the upstream Debian package.	Unknown
22.02.3	NAS-117581	Launch Docker Image button is disabled.	On the **Apps** page, select the **Available Applications** tab before trying to click the button.	22.02.3.1
22.02.1	NAS-116473	Large Drive Count Issues	iX is investigating isuses with booting SCALE on systems with more than 100 Disks.	22.12-RC.1
22.02.0	NAS-115238	Removed drive from pool does not degrade pool status (SCALE).	Issue is being investigated and a fix provided in a future release	Targeted 22.02.4
22.02.0-RC.2		Cosmetic issue with update trains when updating from SCALE 22.02.0-RC.2.	After updating from 22.02.0-RC.2, the previous update train might show in **System Settings > Update**. This is a cosmetic issue only and can be ignored.	
		Unable to mount an NFS export after migrating from CORE > SCALE or updating to 22.02.0.	The /etc/exports file is no longer generated when the NFS configuration contains *mapall* or *maproot* entries for unknown users or groups. This can impact users who previously had a mapping group set to *wheel*, which does not exist in SCALE. If you are unable to mount an NFS export, review your NFS share configuration and change any *wheel* entries to something specific for your environment or *root*.	
		ZFS feature flag has been removed.	See ZFS Feature Flag Removal for more information.	
		SCALE Gluster/Cluster.	Gluster/Cluster features are still in testing. Administrators should use caution when deploying and avoid use with critical data.	
	NAS-110263	AFP sharing is removed from TrueNAS SCALE. The	TrueNAS SCALE automatically migrates any existing AFP shares into an SMB configuration that is preset to function	21.06-BETA.1

Seen In	Key	Summary	Workaround	Resolved In
		protocol is deprecated and no longer receives development effort or security fixes.	like an AFP share.	
21.06-BETA.1	NAS-111547	ZFS shouldn't count vdev IO errors on hotplug removal	Pool status isn't being updated immediately on disk exchange events.	Targeted 22.12

ZFS Feature Flag Removal

Executive Summary

- ZFS `xattr_compat` feature flag removed

How to tell if I'm impacted by this change

- Users who created or upgraded a pool using a TrueNAS SCALE nightly build dated between June 29, 2021 and July 15, 2021 are impacted by this change.
- Users who have manually set `xattr_compat=all` on a dataset and written an xattr are impacted by this change.
- If unsure, you can verify a pool's status of the `xattr_compat` feature flag. If the flag is in the active state, you are impacted by this change.

```
root@truenas[~]# zpool get feature@xattr_compat my_pool
NAME      PROPERTY               VALUE       SOURCE
my_pool   feature@xattr_compat   active      local
root@truenas[~]#
```

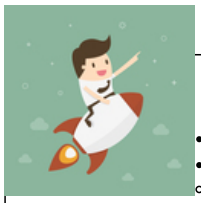
How to resolve this if I am impacted

- Any pool that has had the feature active, must be backed up and restored into a pool created on a version of ZFS without the feature. For details on how to perform data protection procedures, please refer to the TrueNAS SCALE Data Protection documentation.

Technical details behind the change

See the ZFS Feature Flags Removal article for more information.

2 - Getting Started with SCALE



This section guides you through installing and accessing TrueNAS SCALE, storing, backing up, and sharing data, and expanding TrueNAS with different applications solutions.

Table of Contents (click to expand)

SCALE Documentation Sections

For more detailed interface reference articles, configuration instructions, and tuning recommendations, see the remaining sections in this topic.

TrueNAS SCALE documentation is divided into several sections or books:

- The Getting Started Guide provides the first steps for your experience with TrueNAS SCALE:
  - Software Licensing information.
  - Recommendations and considerations when selecting hardware.
  - Installation tutorials.
  - First-time software configuration instructions.
- Configuration Tutorials have many community and iXsystems -provided procedural how-tos for specific software use-cases.
- The UI Reference Guide describes each section of the SCALE web interface, including descriptions for each configuration option.
- API Reference describes how to access the API documentation on a live system and includes a static copy of the API documentation.
- SCALE Security Reports links to the TrueNAS Security Hub and also contains any additional security-related notices.

Ready to get started? Choose a topic or article from the left-side **Navigation** pane. Click the **<** symbol to expand the menu to show the topics under this section.

2.1 - User Agreements

2.1.1 - TrueNAS SCALE EULA

TrueNAS SCALE End User License Agreement

Important - Please Read This EULA Carefully

PLEASE CAREFULLY READ THIS END USER LICENSE AGREEMENT (EULA) BEFORE CLICKING THE AGREE BUTTON. THIS AGREEMENT SERVES AS A LEGALLY BINDING DOCUMENT BETWEEN YOU AND IXSYSTEMS, INC. BY CLICKING THE AGREE BUTTON, DOWNLOADING, INSTALLING, OR OTHERWISE USING TRUENAS SCALE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT). IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS IN THIS AGREEMENT, DO NOT USE OR INSTALL TRUENAS SCALE SOFTWARE.

This agreement is provided in accordance with the Commercial Arbitration Rules of the American Arbitration Association (the “AAA Rules”) under confidential binding arbitration held in Santa Clara County, California. To the fullest extent permitted by applicable law, no arbitration under this EULA will be joined to an arbitration involving any other party subject to this EULA, whether through class arbitration proceedings or otherwise. Any litigation relating to this EULA shall be subject to the jurisdiction of the Federal Courts of the Northern District of California and the state courts of the State of California, with venue lying in Santa Clara County, California. All matters arising out of or relating to this agreement shall be governed by and construed in accordance with the internal laws of the State of California without giving effect to any choice or conflict of law provision or rule.

1.0 Definitions

1.1 “Company”, “iXsystems” and “iX” means iXsystems, Inc., on behalf of themselves, subsidiaries, and affiliates under common control.

1.2 “TrueNAS SCALE Software” means the TrueNAS SCALE storage management software.

1.3 “TrueNAS Device” means the TrueNAS storage appliances and peripheral equipment provided by iXsystems or a third party.

1.4 “Product” means, individually and collectively, the TrueNAS SCALE Software and the TrueNAS Device provided by iXsystems.

1.5 “Open Source Software” means various open source software components licensed under the terms of applicable open source license agreements, each of which has its own copyright and its own applicable license terms.

1.6 “Licensee”, “You” and “Your” refers to the person, organization, or entity that has agreed to be bound by this EULA including any employees, affiliates, and third party contractors that provide services to You.

1.7 “Agreement” refers to this document, the TrueNAS End User License Agreement.

2.0 License

Subject to the terms set forth in this Agreement, iXsystems grants You a non-exclusive, non-transferable, perpetual, limited license without the option to sublicense, to use TrueNAS SCALE Software on Your TrueNAS Device(s). This use includes but is not limited to using or viewing the instructions, specifications, and documentation provided with the Product.

TrueNAS SCALE software is made available as Open Source Software, subject to the license conditions contained within that Open Source Software.

3.0 License Restrictions

TrueNAS SCALE Software is authorized for use on any TrueNAS Device. TrueNAS Devices can include hardware provided by iXsystems or third parties. TrueNAS Devices may also include virtual machines and cloud instances. TrueNAS SCALE software may not be commercially distributed or sold without an addendum license agreement and express written consent from iXsystems. .

The TrueNAS SCALE Software is protected by copyright laws and international treaties, as well as other intellectual property laws, statutes, and treaties. The TrueNAS SCALE Software is licensed, not sold to You, the end user. You do not acquire any ownership interest in the TrueNAS SCALE Software, or any other rights to the TrueNAS SCALE Software, other than to use the TrueNAS SCALE Software in accordance with the license granted under this Agreement, subject to all terms, conditions, and restrictions. iXsystems reserves and shall retain its entire right, title, and interest in and to the TrueNAS SCALE Software, and all intellectual property rights arising out of or relating to the TrueNAS SCALE Software, subject to the license expressly granted to You in this Agreement.

The TrueNAS SCALE Software may contain iXsystems’ proprietary trademarks and collateral. By agreeing to this license agreement for TrueNAS SCALE, You agree to use reasonable efforts to safeguard iXsystems’ intellectual property and hereby agree to not use or distribute iXsystems’ proprietary intellectual property and collateral commercially without the express written consent of iXsystems. Official iXsystems Channel Partners are authorized to use and distribute iXsystems’ intellectual property through an addendum to this license agreement. By accepting this Agreement, You are responsible and liable for all uses of the Product through access thereto provided by You, directly or indirectly.

The TrueNAS SCALE software includes Open Source components and some proprietary extensions which are available through additional licences You agree to not alter the source code to take advantage of the proprietary extensions without a license to those proprietary extensions, including the TrueNAS Enterprise features sets.

4.0 General

4.1 Entire Agreement - This Agreement, together with any associated purchase order, service level agreement, and all other documents and policies referenced herein, constitutes the entire and only agreement between You and iXsystems for use of the TrueNAS SCALE Software and all other prior negotiations, representations, agreements, and understandings are superseded hereby. No agreements altering or supplementing the terms hereof may be made except by means of a written document signed by Your duly authorized representatives and those of iXsystems.

4.2 Waiver and Modification - No failure of either party to exercise or enforce any of its rights under this EULA will act as a waiver of those rights. This EULA may only be modified, or any rights under it waived, by a written document executed by the party against which it is asserted.

4.3. Severability - If any provision of this EULA is found illegal or unenforceable, it will be enforced to the maximum extent permissible, and the legality and enforceability of the other provisions of this EULA will not be affected.

4.4 United States Government End Users - For any TrueNAS SCALE Software licensed directly or indirectly on behalf of a unit or agency of the United States Government, this paragraph applies. Company's proprietary software embodied in the Product: (a) was developed at private expense and is in all respects Company's proprietary information; (b) was not developed with government funds; (c) is Company's trade secret for all purposes of the Freedom of Information Act; (d) is a commercial item and thus, pursuant to Section 12.212 of the Federal Acquisition Regulations (FAR) and DFAR Supplement Section 227.7202, Government's use, duplication or disclosure of such software is subject to the restrictions set forth by the Company and Licensee shall receive only those rights with respect to the Product as are granted to all other end users.

4.5 Title - iXsystems retains all rights, titles, and interest in TrueNAS SCALE Software and all related copyrights, trade secrets, patents, trademarks, and any other intellectual and industrial property and proprietary rights, including registrations, applications, registration keys, renewals, and extensions of such rights. Contact Information - If You have any questions about this Agreement, or if You want to contact iXsystems for any reason, please email legal@ixsystems.com.

4.6 Maintenance and Support - You may be entitled to support services from iXsystems after purchasing a Product or a support contract. iXsystems will provide these support services based on the length of time of the purchased support contract. This maintenance and support is only valid for the length of time that You have purchased with Your Product. iXsystems may from time to time and at their sole discretion vary the terms and conditions of the maintenance and support agreement based on different business environmental and personnel factors. Any variations will be notified via email and the support portal. For more information on our Maintenance and Support contract, refer to https://www.ixsystems.com/support/.

4.7 Force Majeure - iXsystems will not be deemed to be in default of any of the provisions of this Agreement or be liable for any delay or failure in performance due to Force Majeure, which shall include without limitation acts of God, earthquake, weather conditions, labor disputes, changes in law, regulation or government policy, riots, war, fire, epidemics, acts or omissions of vendors or suppliers, equipment failures, transportation difficulties, malicious or criminal acts of third parties, or other occurrences which are beyond iXsystems' reasonable control.

4.8 Termination - iXsystems may cease any and all support, services, or maintenance under this Agreement without prior notice, or liability, and for any reason whatsoever, without limitation, if any of the terms and conditions of this Agreement are breached. Other provisions of this Agreement will survive termination including, without limitation, ownership provisions, warranty disclaimers, indemnity, and limitations of liability.

4.9 Open Source Software Components - iXsystems uses Open Source Software components in the development of the TrueNAS SCALE Software. Open Source Software components that are used in the TrueNAS SCALE Software are composed of separate components each having their own trademarks, copyrights, and license conditions.

4.10 Assignment - Licensee shall not assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance, under this Agreement, in each case whether voluntarily, involuntarily, by operation of law, or otherwise, without iXsystems' prior written consent. No delegation or other transfer will relieve Licensee of any of its obligations or performance under this Agreement. Any purported assignment, delegation, or transfer in violation of this Section is void. iXsystems may freely assign or otherwise transfer all or any of its rights, or delegate or otherwise transfer all or any of its obligations or performance, under this Agreement without Licensee's consent. This Agreement is binding upon and inures to the benefit of the parties hereto and their respective permitted successors and assigns.

5.0 Export Control Regulations

"The Product may be subject to export control laws. You shall not, directly or indirectly, export, re-export, or release the Product to, or make the Product accessible from, any jurisdiction or country to which export, re-export, or release is prohibited by law, rule, or regulation. You shall comply with all applicable laws, regulations, and rules, and complete all required undertakings (including obtaining any necessary export license or other governmental approval)."

6.0 Data Collection and Privacy

TrueNAS SCALE Software may collect non-sensitive system information relating to Your use of the Product, including information that has been provided directly or indirectly through automated means. Usage of TrueNAS SCALE Software, device status and system configuration are allowed according to iXsystems' privacy policy.

TrueNAS SCALE Software will not collect sensitive User information including email addresses, names of systems, pools, datasets, folders, files, credentials.

By accepting this Agreement and continuing to use the Product, you agree that iXsystems may use any information provided through direct or indirect means in accordance with our privacy policy and as permitted by applicable law, for purposes relating to management, compliance, marketing, support, security, update delivery, and product improvement.

7.0 Limitation of Liability and Disclaimer of Warranty

THE PRODUCT IS PROVIDED “AS IS” AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, IXSYSTEMS, ON ITS OWN BEHALF AND ON BEHALF OF ITS AFFILIATES AND ITS AND THEIR RESPECTIVE LICENSORS AND SERVICE PROVIDERS, EXPRESSLY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THE PRODUCT, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND WARRANTIES THAT MAY ARISE OUT OF COURSE OF DEALING, COURSE OF PERFORMANCE, USAGE, OR TRADE PRACTICE. WITHOUT LIMITATION TO THE FOREGOING, IXSYSTEMS PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE PRODUCT WILL MEET THE LICENSEE’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE, OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS, OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE, OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

TO THE FULLEST EXTENT PERMITTED UNDER APPLICABLE LAW: (A) IN NO EVENT WILL IXSYSTEMS OR ITS AFFILIATES, OR ANY OF ITS OR THEIR RESPECTIVE LICENSORS OR SERVICE PROVIDERS, BE LIABLE TO LICENSEE, LICENSEE’S AFFILIATES, OR ANY THIRD PARTY FOR ANY USE, INTERRUPTION, DELAY, OR INABILITY TO USE THE PRODUCT; LOST REVENUES OR PROFITS; DELAYS, INTERRUPTION, OR LOSS OF SERVICES, BUSINESS, OR GOODWILL; LOSS OR CORRUPTION OF DATA; LOSS RESULTING FROM SYSTEM OR SYSTEM SERVICE FAILURE, MALFUNCTION, OR SHUTDOWN; FAILURE TO ACCURATELY TRANSFER, READ, OR TRANSMIT INFORMATION; FAILURE TO UPDATE OR PROVIDE CORRECT INFORMATION; SYSTEM INCOMPATIBILITY OR PROVISION OF INCORRECT COMPATIBILITY INFORMATION; OR BREACHES IN SYSTEM SECURITY; OR FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, OR PUNITIVE DAMAGES, WHETHER ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE AND WHETHER OR NOT IXSYSTEMS WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; (B) IN NO EVENT WILL IXSYSTEMS’ AND ITS AFFILIATES', INCLUDING ANY OF ITS OR THEIR RESPECTIVE LICENSORS' AND SERVICE PROVIDERS', COLLECTIVE AGGREGATE LIABILITY UNDER OR IN CONNECTION WITH THIS AGREEMENT OR ITS SUBJECT MATTER, UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE, EXCEED THE TOTAL AMOUNT PAID TO IXSYSTEMS PURSUANT TO THIS AGREEMENT FOR THE PRODUCT THAT IS THE SUBJECT OF THE CLAIM; (C) THE LIMITATIONS SET FORTH IN THIS SECTION SHALL APPLY EVEN IF THE LICENSEE’S REMEDIES UNDER THIS AGREEMENT FAIL OF THEIR ESSENTIAL PURPOSE.

You hereby acknowledge that you have read and understand this Agreement and voluntarily accept the duties and obligations set forth herein by clicking accept on this Agreement.

2.1.2 - Software Development Life Cycle

The TrueNAS Software Development Life Cycle (SDLC) is the process of planning, creating, testing, deploying, and maintaining TrueNAS releases.

Requirement Analysis
Determine the objectives, nature, and scope of future versions of the software. Requirement Analysis involves gathering feedback and interpreting customer needs and requirements, diagnosing existing problems, and weighing the pros and cons of potential solutions. The end result is a list of recommended improvements to be integrated into future versions of TrueNAS.
Design and Development
Required and planned changes are investigated in detail and development steps are determined. Proposed alterations are reviewed by peers for completeness, correctness, and proper coding style. TrueNAS developers then begin altering the software to include new features, resolve software bugs, or implement security improvements.
Testing and Evaluation
Code is integrated into the existing TrueNAS source tree, then built and tested by the Release Engineering (RE) department. RE verifies that all requirements and objectives are properly met and the updated software is reliable and fault-tolerant according to the determined requirements. If issues are found, code is reworked to meet the development requirements. Simultaneously, a security evaluation of the TrueNAS code is completed, with any discovered issues sent to the engineering team for resolution.
Documentation
The Validation and Documentation Team audits all development changes to the software and resolves any inconsistencies with the current software documentation. This is to verify that end user documentation is as accurate as possible. Any security notices, errata, or best practices are also drafted for inclusion on the TrueNAS Security website.
Maintenance
The new release of TrueNAS is evaluated to determine further feature development, bug fixes, or security vulnerability patches. During this stage, security patches and software erratum are corrected, updated versions of existing branches are pushed, and feedback is solicited for future versions of the software.

SDLC Application

The TrueNAS SDLC applies to the latest two release branches. As new releases are created for TrueNAS, the oldest TrueNAS release branch is dropped out of the SDLC and labeled as End of Life (EoL). For example, TrueNAS/FreeNAS 11.3 and TrueNAS 12.0 were in active development under the SDLC in August 2020. In early 2021, TrueNAS Core/Enterprise 12.0 and 13.0 branches were in active development under the SDLC. These versions of the software are in active development and maintenance. We encourage users to actively keep their software updated to an active development version to continue to receive security patches and other software improvements.

> The Software Status page shows the latest recommendations for using the various TrueNAS software releases.

TrueNAS Quality Lifecycle

TrueNAS releases follow a general adoption guideline for their lifetime. Starting with the NIGHTLY builds, each stage of a major release incorporates more testing cycles and bug fixes that represent a maturation of the release. With each version release stage, users are encouraged to install, upgrade, or otherwise begin using the major version, depending on the specific TrueNAS deployment and use case:

Release Stage	Completed QA Cycles	Typical Use-case	Description
NIGHTLY	0	Developers	Incomplete
ALPHA	1	Testers	Not much field testing
BETA	2	Enthusiasts	Major Feature Complete, but expect some bugs
RC	3	Home Users	Suitable for non-critical deployments
RELEASE	4	General Use	Suitable for less complex deployments
U1	5	Business Use	Suitable for more complex deployments
U2+	6+	Mission Critical	Suitable for critical uptime deployments

---

2.1.3 - TrueNAS Data Collection Statement

TrueNAS collects non-sensitive system data and relays the data to a collector managed by iXsystems. This system data collection is enabled by default and can be disabled in the web interface under **System Settings > General > GUI Settings > Usage collection**.

When disabled, no information about system configuration and usage is collected. The system capacity and software version is still collected.

The protocol for system data collection uses the same TCP ports as HTTPS (*443*) and passes through most firewalls as an outgoing web connection. If a firewall blocks the data collection or the data collection is disabled, there is no adverse impact to the TrueNAS system.

Non-sensitive system data is used to identify the quality and operational trends in the fleet of TrueNAS systems used by the entire community. The collected data helps iXsystems identify issues, plan for new features, and determine where to invest resources for future software enhancements.

The non-sensitive system data collected is clearly differentiated from sensitive user data that is explicitly not collected by TrueNAS. This table describes the differences:

	Sensitive User Data (NOT COLLECTED)	Non-Sensitive System Data (Optionally Collected)
Description	Any data that includes user identity or business information	Data that only includes information about the TrueNAS system and its operation
Frequency	NEVER	Daily
Examples	Usernames, passwords, email addresses	Anonymous hardware inventory, faults, statistics, Pool configuration
	User-created System and dataset names	Software versions, firmware versions
	Directory, files names, user data	Services and features enabled, Usage and Performance statistics

2.2 - SCALE Hardware Guide

This article provides information on system hardware and system minimum requirements. Included information covers CPUs, storage considerations and solutions, media and controllers, device sizing and cooling, SAS expanders, and system memory.

From repurposed systems to highly-custom builds, the fundamental freedom of TrueNAS is the ability to run it on almost any x86 computer.

Minimum Hardware Requirements

The recommended system requirements to install TrueNAS:

Processor	Memory	Boot Device	Storage
2-Core Intel 64-Bit or AMD x86_64 processor	8 GB Memory	16 GB SSD boot device	Two identically-sized devices for a single storage pool

The TrueNAS installer recommends 8 GB of RAM. TrueNAS installs, runs, operates jails, hosts SMB shares, and replicates TBs of data with less. iXsystems recommends the above for better performance and fewer issues.

You do not need an SSD boot device, but we discourage using a spinner or a USB stick for obvious reasons. We do not recommend installing TrueNAS on a single disk or striped pool unless you have a good reason to do so. You can install and run TrueNAS without any data device, but we strongly discourage it.

TrueNAS does not require two cores, as most halfway-modern 64-bit CPUs likely already have at least two.

For help building a system according to your unique performance, storage, and networking requirements, read on!

Storage Considerations

The heart of any storage system is the symbiotic pairing of its file system and physical storage devices. The ZFS file system in TrueNAS provides the best available data protection of any file system at any cost and makes very effective use of both spinning-disk and all-flash storage or a mix of the two. ZFS is prepared for the eventual failure of storage devices. It is highly configurable to achieve the perfect balance of redundancy and performance to meet any storage goal. A properly-configured TrueNAS system can tolerate the failure of multiple storage devices and even recreate its boot media with a copy of the configuration file.

Storage Device Quantities

TrueNAS is capable of managing large quantities of storage devices as part of a single storage array. The community-focused TrueNAS SCALE Angelfish release can manage as many as 400 drives in a single storage array; a significant level of flexibility for home users to larger business deployments. With more Enterprise-level tuning in the mature 13.0 release and similar tuning in the upcoming SCALE Bluefin release, TrueNAS can expand even further and manage as many as 1,250 drives in a single storage array!

Storage Media

Choosing storage media is the first step in designing the storage system to meet immediate objectives and prepare for future capacity expansion.

Spinning Disks
Until the next scientific breakthrough in storage media, spinning hard disks are here to stay thanks to their balance of capacity and cost. The arrival of double-digit terabyte consumer and enterprise drives provides more choices to TrueNAS users than

ever. TrueNAS Mini systems ship with Western Digital NAS and NL-SAS for good reason. Understanding the alternatives explains this decision.

SATA NAS Disks

Serial Advanced Technology Attachment (SATA) is still the de facto standard disk interface found in many desktop/laptop computers, servers, and some non-enterprise storage arrays. SATA disks first arrived offering double-digit gigabyte capacities and are now produced to meet many capacity, reliability, and performance goals. While consumer desktop SATA disks do not have the problematic overall reliability issues they once had, they are still not designed or warrantied for continuous operation or use in RAID groups. Enterprise SATA disks address the always-on factor, vibration tolerance, and drive error handling required in storage systems. However, the price gap between desktop and enterprise SATA drives is vast enough that it forces users to push their consumer drives into 24/7 service to pursue cost savings.

Drive vendors, likely tired of honoring warranties for failed desktop drives used in incorrect applications, responded to this gap in the market by producing NAS drives. NAS drives achieved fame from the original Western Digital (WD) Red™ drives with CMR/PMR technology (now called WD Red Plus). Western Digital Designed the WD Red™ Plus NAS drives (non-SMR) for systems with up to 8 hard drives, the WD Red™ Pro for systems with up to 16 drives, and the WD UltraStar™ for systems beyond 16 drives.

The iXsystems Community Forum regards WD drives as the preferred hard drives for TrueNAS builds due to their exceptional quality and reliability. All TrueNAS Minis ship with WD Red™ Plus drives unless requested otherwise.

Nearline SAS Disks

Nearline SAS (NL-SAS) disks are 7200 RPM enterprise SATA disks with the industry-standard SAS interface found in most enterprise storage systems. SAS stands for **Serial Attached SCSI**, with the traditional SCSI disk interface in serial form. SAS systems, designed for data center storage applications, have accurate, verbose error handling, predictable failure behavior, reliable hot swapping, and the added feature of multipath support. Multipath access means that each drive has two interfaces and can connect to two storage controllers or one controller over two cables. This redundancy protects against cable, controller card, or complete system failure in the case of the TrueNAS high-availability architecture in which each controller is an independent server that accesses the same set of NL-SAS drives. NL-SAS drives are also robust enough to handle the rigors of systems with more than 16 disks. So, capacity-oriented TrueNAS systems ship with Western Digital UltraStar NL-SAS disks thanks to the all-around perfect balance of capacity, reliability, performance, and flexibility that NL-SAS drives offer.

SAS Disks

Enterprise SAS disks, built for the maximum performance and reliability that a spinning platter can provide, are the traditional heavy-lifters of the enterprise storage industry. SAS disk capacities are low compared to NL-SAS or NAS drives due to the speed at which the platters spin, reaching as high as 15,000 RPMs. While SAS drives may sound like the ultimate answer for high-performance storage, many consumer and enterprise flash-based options have come onto the market and significantly reduced the competitiveness of SAS drives. For example, enterprise SAS drives discontinued from the TrueNAS product lines were almost completely replaced by flash drives (SSDs or NVMe) in 2016 due to their superior performance/cost ratio.

SATA & SAS Flash Storage SSDs

Flash storage technology has progressed significantly in recent years, leading to a revolution in mobile devices and the rise of flash storage in general-purpose PCs and servers. Unlike hard disks, flash storage is not sensitive to vibration and can be much faster with comparable reliability. Flash storage remains more expensive per gigabyte, but is becoming more common in TrueNAS systems as the price gap narrows.

The shortest path for introducing flash storage into the mainstream market was for vendors to use standard SATA/SAS hard disk interfaces and form factors that emulate standard hard disks but without moving parts. For this reason, flash storage Solid State Disks (SSDs) have SATA interfaces and are the size of 2.5" laptop hard disks, allowing them to be drop-in replacements for traditional hard disks. Flash storage SSDs can replace HDDs for primary storage on a TrueNAS system, resulting in a faster, though either a smaller or more expensive storage solution. If you plan to go all-flash, buy the highest-quality flash storage SSDs your budget allows with a focus on power, safety, and write endurance that matches your expected write workload.

NVMe

While SSDs pretending to be HDDs made sense for rapid adoption, the Non-Volatile Memory Express (NVMe) standard is a native flash protocol that takes full advantage of the flash storage non-linear, parallel nature.

The main advantage of NVMe is generally its low-latency performance, and it is becoming a mainstream option for boot and other tasks. At first, NVMe was limited to expansion-card form factors such as PCIe and M.2. The new U.2 interface offers a universal solution that includes the 2.5" drive form factor and an externally accessible (but generally not hot-swappable) NVMe interface.

Note: NVMe devices can run quite hot and may need dedicated heat sinks.

> Manual S.M.A.R.T. tests on NVMe devices is currently not supported.

USB Hard Disks

Avoid using USB-connected hard disks for primary storage with TrueNAS. You can use USB Hard Disks for very basic backups in a pinch. While TrueNAS does not automate this process, you can connect a USB HDD, replicate at the command line, and then take it off-site for safekeeping.

> **Warning:** USB-connected media (including SSDs) may report their serial numbers inaccurately, making them indistinguishable from each other.

These storage device media arrange together to create powerful storage solutions.

Storage Solutions

Hybrid Storage & Flash Cache (SLOG/ZIL/L2ARC)

With hard disks providing double-digit terabyte capacities and flash-based options providing even higher performance, a best of both worlds option is available. With TrueNAS and OpenZFS, you can merge both flash and disk to create hybrid storage that makes the most of both storage types. Hybrid setups use high-capacity spinning disks to store data while DRAM and flash perform hyper-fast read and write caching. The technologies work together with a flash-based separate write log (SLOG). Think of it as a write cache keeping the ZFS-intent log (ZIL) used to speed up writes. On the read side, flash is a level two adaptive replacement (read) cache (L2ARC) to keep the hottest data sets on the faster flash media. Workloads with synchronous writes such as NFS and databases benefit from SLOG devices, while workloads with frequently-accessed data might benefit from an L2ARC device. An L2ARC device is not always the best choice because the level one ARC in RAM always provide a faster cache, and the L2ARC table uses some RAM.

SLOG devices do not need to be large, since they only need to service five seconds of data writes delivered by the network or a local application. A high-endurance, low-latency device between 8 GB and 32 GB in size is adequate for most modern networks, and you can strip or mirror several devices for either performance or redundancy. Pay attention to the published endurance claims for the device since a SLOG acts as the funnel point for most of the writes made to the system.

SLOG devices also need power protection. The purpose of the ZFS intent log (ZIL), and thus the SLOG, is to keep sync writes safe during a crash or power failure. If the SLOG is not power-protected and loses data after a power failure, it defeats the purpose of using a SLOG in the first place. Check the manufacturer specifications for the device to ensure the SLOG device is power-safe or has power loss/failure protection.

The most important quality to look for in an L2ARC device is random read performance. The device needs to support more IOPS than the primary storage media it caches. For example, using a single SSD as an L2ARC is ineffective in front of a pool of 40 SSDs, as the 40 SSDs can handle far more IOPS than the single L2ARC drive. As for capacity, 5x to 20x larger than RAM size is a good guideline. High-end TrueNAS systems can have NVMe-based L2ARC in double-digit terabyte sizes.

Keep in mind that for every data block in the L2ARC, the primary ARC needs an 88-byte entry. Poorly-designed systems can cause an unexpected fill-up in the ARC and reduce performance in a p. For example, a 480 GB L2ARC filled with 4KiB blocks needs more than 10GiB of metadata storage in the primary ARC.

Self Encrypting Drives
TrueNAS supports two forms of data encryption at rest to achieve privacy and compliance objectives: Native ZFS encryption and Self Encrypting Drives (SEDs). SEDs do not experience the performance overhead introduced by software partition encryption but are not as readily available as non-SED drives (and thus can cost a little more).
Boot Devices

Booting legacy FreeNAS systems from 8 GB or larger USB flash drives was once very popular. We recommend looking at other options since USB drive quality varies widely and modern TrueNAS versions perform increased drive writes to the boot pool. For this reason, all pre-built TrueNAS Systems ship with either M.2 drives or SATA DOMs.

SATA DOMs, or disk-on-modules, offer reliability close to that of consumer 2.5" SSDs with a smaller form factor that mounts to an internal SATA port and does not use a drive bay. Because SATA DOMs and motherboards with m.2 slots are not as common as the other storage devices mentioned here, users often boot TrueNAS systems from 2.5" SSDs and HDDs (often mirrored for added redundancy). The recommended size for the TrueNAS boot volume is 8 GB, but using 16 or 32 GB (or a 120 GB 2.5" SATA SSD) provides room for more boot environments.

Hot Swapability
TrueNAS systems come in all shapes and sizes. Many users want to have external access to all storage devices for efficient replacement if issues occur. Most hot-swap drive bays need a proprietary drive tray into which you install each drive. These bay and tray combinations often include convenient features like activity and identification lights to visualize activity and illuminate a failed drive with sesutil(8) (https://www.freebsd.org/cgi/man.cgi?query=sesutil&sektion=8 for CORE, https://manpages.debian.org/testing/sg3-utils/sg3_utils.8.en.html for SCALE). TrueNAS Mini systems ship with four or more hot-swap bays. TrueNAS R-Series systems can support dozens of drives in their head units and external expansion shelves. Pre-owned or repurposed hardware is popular among TrueNAS users.
Pay attention to the maximum performance offered by the hot-swap backplanes of a given system. Aim for at least 6 Gbps SATA III support. Note that hot-swapping PCIe NVMe devices is not currently supported.

Storage Device Sizing

Zpool layout (the organization of LUNs and volumes, in TrueNAS/ZFS parlance) is outside of the scope of this guide. The availability of double-digit terabyte drives raises a question TrueNAS users now have the luxury of asking: How many drives should I use to achieve my desired capacity? You can mirror two 16TB drives to achieve 16TB of available capacity, but that does not mean you should. Mirroring two large drives offers the advantage of redundancy and balancing reads between the two devices, which could lower power draw, but little else. The write performance of two large drives, at most, is that of a single drive. By contrast, an array of eight 4TB drives offers a wide range of configurations to optimize performance and redundancy at a lower cost. If configured as striped mirrors, eight drives could yield four times greater write performance with a similar total capacity. You might also consider adding a hot-spare drive with any zpool configuration, which lets the zpool automatically rebuild itself if one of its primary drives fails.

Storage Device Burn-In

Spinning disk hard drives have moving parts that are highly sensitive to shock and vibration and wear out with use. Consider pre-flighting every storage device before putting it into production, paying attention to:

- Start a long HDD self-test (`smartctl -t long /dev/`), and after the test completes (could take 12+ hrs)
- Check the results (`smartctl -a /dev/`)
- Check pending sector reallocations (`smartctl -a /dev/ | grep Current_Pending_Sector`)
- Check reallocated sector count (`smartctl -a /dev/ | grep Reallocated_Sector_Ct`)
- Check the UDMA CRC errors (`smartctl -a /dev/ | grep UDMA_CRC_Error_Count`)

- Check HDD and SSD write latency consistency (`diskinfo -wS `) *Unformatted drives only!*
- Check HDD and SSD hours (`smartctl -a /dev/ | grep Power_On_Hours`)
- Check NVMe percentage used (`nvmecontrol logpage -p 2 nvme0 | grep "Percentage used"`)

Take time to create a pool before deploying the system. Subject it to as close to a real-world workload as possible to reveal individual drive issues and help determine if an alternative pool layout is better suited to that workload. Be cautious of used drives as vendors may not be honest or informed about their age and health. Check the number of hours on all new drives using `smartctl(8)` to verify they are not recertified. A drive vendor could also zero the hours of a drive during recertification, masking its true age. iXsystems tests all storage devices it sells for at least 48 hours before shipment.

Storage Controllers

The uncontested most popular storage controllers used with TrueNAS are the 6 and 12 Gbps (Gigabits per second, sometimes expressed as Gb/s) Broadcom (formerly Avago, formerly LSI) SAS host bus adapters (HBA). Controllers ship embedded on some motherboards but are generally PCIe cards with four or more internal or external SATA/SAS ports. The 6 Gbps LSI 9211 and its rebranded siblings that also use the LSI SAS2008 chip, such as the IBM M1015 and Dell H200, are legendary among TrueNAS users who build systems using parts from the second-hand market. Flash using the latest IT or Target Mode firmware to disable the optional RAID functionality found in the IR firmware on Broadcom controllers. For those with the budget, newer models like the Broadcom 9300/9400 series give 12 Gbps SAS capabilities and even NVMe to SAS translation abilities with the 9400 series. TrueNAS includes the `sas2flash`, `sas3flash`, and `storcli` commands to flash or perform re-flashing operations on 9200, 9300, and 9400 series cards.

Onboard SATA controllers are popular with smaller builds, but motherboard vendors are better at catering to the needs of NAS users by including more than the traditional four SATA interfaces. Be aware that many motherboards ship with a mix of 3 Gbps and 6 Gbps onboard SATA interfaces and that choosing the wrong one could impact performance. If a motherboard includes hardware RAID functionality, do not use or configure it, but note that disabling it in the BIOS might remove some SATA functionality depending on the motherboard. Most SATA compatibility-related issues are immediately apparent.

There are countless warnings against using hardware RAID cards with TrueNAS. ZFS and TrueNAS provide a built-in RAID that protects your data better than any hardware RAID card. You can use a hardware RAID card if it is all you have, but there are limitations. First and most importantly, do not use their RAID facility if your hardware RAID card supports HBA mode, also known as passthrough or JBOD mode (there is one caveat in the bullets below). When used, it allows it to perform indistinguishably from a standard HBA. If your RAID card does not have this mode, you can configure a RAID0 for every single disk in your system. While not the ideal setup, it works in a pinch. If repurposing hardware RAID cards with TrueNAS, be aware that some hardware RAID cards:

- Could mask disk serial number and S.M.A.R.T. health information
- Could perform slower than their HBA equivalents
- Could cause data loss if using a write cache with a dead battery backup unit (BBU))

SAS Expanders

A direct-attached system, where every disk connects to an interface on the controller card, is optimal but not always possible. A SAS expander (a port multiplier or splitter) enables each SAS port on a controller card to service many disks. You find SAS expanders only on the drive backplane of servers or JBODs with more than twelve drive bays. For example, a TrueNAS JBOD that eclipses 90 drives in only four rack units of space is not possible without SAS expanders. Imagine how many eight-port HBAs you would need to access 90 drives without SAS expanders.

While SAS expanders, designed for SAS disks, can often support SATA disks via the SATA Tunneling Protocol or STP, we still prefer SAS disks for reasons mentioned in the NL-SAS section above (SATA disks function on a SAS-based backplane). Note that the opposite is not true: you cannot use a SAS drive in a port designed for SATA drives.

Storage Device Cooling

A much-cited study floating around the Internet asserts that drive temperature has little impact on drive reliability. The study makes for a great headline or conversation starter, but carefully reading the report indicates that the drives were tested under optimal environmental conditions. The average temperature that a well-cooled spinning hard disk reaches in production is around 28 °C, and one study found that disks experience twice the number of failures for every 12 °C increase in temperature. Before adding drive cooling that often comes with added noise (especially on older systems), know that you risk throwing money away by running a server in a data center or closet without noticing that the internal cooling fans are set to their lowest setting. Pay close attention to drive temperature in any chassis that supports 16 or more drives, especially if they are exotic, high-density designs. Every chassis has certain areas that are warmer for whatever reason. Watch for fan failures and the tendency for some models of 8TB drives to run hotter than other drive capacities. In general, try to keep drive temperatures below the drive specification provided by vendor.

Memory, CPU, and Network Considerations

Memory Sizing

TrueNAS has higher memory requirements than many Network Attached Storage solutions for good reason: it shares dynamic random-access memory (DRAM or simply RAM) between sharing services, add-on plugins, jails, and virtual machines, and sophisticated read caching. RAM rarely goes unused on a TrueNAS system and enough RAM is key to maintaining peak performance. You should have at least 8 GB of RAM for basic TrueNAS operations with up to eight drives. Other use cases each have distinct RAM requirements:

- Add 1 GB for each drive added after eight to benefit most use cases.
- Add extra RAM (in general) if more clients will connect to the TrueNAS system. A 20 TB pool backing lots of high-performance VMs over iSCSI might need more RAM than a 200 TB pool storing archival data. If using iSCSI to back VMs, plan to use at least 16 GB of RAM for reasonable performance and 32 GB or more for optimal performance.

- Add 2 GB of RAM for directory services for the winbind internal cache.
- Add more RAM as required for plugins and jails as each has specific application RAM requirements.
- Add more RAM for virtual machines with a guest operating system and application RAM requirements.
- Add the suggested 5 GB per TB of storage for deduplication that depends on an in-RAM deduplication table.
- Add approximately 1 GB of RAM (conservative estimate) for every 50 GB of L2ARC in your pool. Attaching an L2ARC drive to a pool uses some RAM, too. ZFS needs metadata in ARC to know what data is in L2ARC.

Error Correcting Code Memory

Electrical or magnetic interference inside a computer system can cause a spontaneous flip of a single bit of RAM to the opposite state, resulting in a memory error. Memory errors can cause security vulnerabilities, crashes, transcription errors, lost transactions, and corrupted or lost data. So RAM, the temporary data storage location, is one of the most vital areas for preventing data loss.

Error-correcting code or ECC RAM detects and corrects in-memory bit errors as they occur. If errors are severe enough to be uncorrectable, ECC memory causes the system to hang (become unresponsive) rather than continue with errored bits. For ZFS and TrueNAS, this behavior virtually eliminates any chances that RAM errors pass to the drives to cause corruption of the ZFS pools or file errors.

The lengthy, Internet-wide debate on whether to use error-correcting code (ECC) system memory with OpenZFS and TrueNAS summarizes as:

- ECC RAM is *strongly* recommended as another data integrity defense

However:

- Some CPUs or motherboards support ECC RAM but not all
- Many TrueNAS systems operate every day without ECC RAM
- RAM of any type or grade can fail and cause data loss
- RAM is most likely to fail in the first three months so test all RAM before deployment.

Central Processing Unit (CPU) Selection

Choosing ECC RAM limits your CPU and motherboard options, but that can be a good thing. Intel® makes a point of limiting ECC RAM support to their lowest and highest-end CPUs, cutting out the mid-range i5 and i7 models.

Which CPU to choose can come down to a short list of factors:

- An underpowered CPU can create a performance bottleneck because of how OpenZFS does checksums, and compresses and (optional) encrypts data.
- A higher-frequency CPU with fewer cores usually performs best for SMB only workloads because of Samba, the lightly-threaded TrueNAS SMB daemon.
- A higher-core-count CPU is better suited for parallel encryption and virtualization.
- A CPU with AES-NI encryption acceleration support improves the speed of the file system and network encryption.
- A server-class CPU is recommended for its power and ECC memory support.
- A Xeon E5 CPU (or similar) is recommended for software-encrypted pools.
- An Intel Ivy Bridge CPU or later recommended for virtual machine use.

Watch for VT-d/AMD-Vi device virtualization support on the CPU and motherboard to pass PCIe devices to virtual machines. Be aware if a given CPU contains a GPU or requires an external one. Also, note that many server motherboards include a BMC chip with a built-in GPU. See below for more details on BMCs.

AMD CPUs are making a comeback thanks to the Ryzen and EPYC (Naples/Rome) lines. Support for these platforms is limited on FreeBSD and, by extension, TrueNAS CORE. However, Linux has significant support, and TrueNAS SCALE should work with AMD CPUs without issue.

Remote Management: IPMI

As a courtesy to further limit the motherboard choices, consider the Intelligent Platform Management Interface or IPMI (a.k.a. baseboard management controller, BMC, iLo, iDrac, and other names depending on the vendor) if you need:

- Remote power control and monitoring of remote systems
- Remote console shell access for configuration or data recovery
- Remote virtual media for TrueNAS installation or reinstallation

TrueNAS relies on its web-based user interface (UI), but you might occasionally need console access to make network configuration changes. TrueNAS administration and sharing default to a single network interface, which can be challenging when you need to upgrade features like LACP aggregated networking. The ideal solution is to have a dedicated subnet to access the TrueNAS web UI, but not all users have this luxury. The occasional visit to the hardware console is necessary for global configuration and even for system recovery. The latest TrueNAS Mini and R-Series systems ship with full-featured, HTML5-based IPMI support on a dedicated gigabit network interface.

Power Supply Units

The top criteria to consider for a power supply unit (or PSU) on a TrueNAS system are its:

- Power capacity (in watts) for the motherboard and number of drives it must support
- Reliability
- Efficiency rating
- Relative noise

- Optional redundancy to keep important systems running if one power supply fails

Select a PSU rated for the initial and a future load placed on it. Have a PSU with adequate power to migrate from a large-capacity chassis to a fully-populated chassis. Also, consider a hot-swappable redundant PSU to help guarantee uptime. Users on a budget can keep a cold spare PSU to limit their potential downtime to hours rather than days. A good, modern PSU is efficient and completely integrates into the IPMI management system to provide real-time fan, temperature, and load information.

Most power supplies carry a certified efficiency rating known as an 80 Plus rating. The 80 plus rating indicates the power drawn from the wall is lost as heat, noise, and vibration, instead of doing useful work like powering your components. If a power supply needs to draw 600 watts from the wall to provide 500 watts of power to your components, it is operating at 500/600 = ~83% efficiency. The other 100 watts get lost as heat, noise, and vibration. Power supplies with higher ratings are more efficient but also far more expensive. Do some return-on-investment calculations if you are unsure what efficiency to buy. For example, if an 80 Plus Platinum PSU costs $50 more than the comparable 80 Plus Gold, it should save you at least $10 per year on your power bill for that investment to pay off over five years. You can read more about 80 Plus ratings in this post.

Uninterruptible Power Supplies

TrueNAS provides the ability to communicate with a battery-backed, uninterruptible power supply (UPS) over a traditional serial or USB connection to coordinate a graceful shutdown in the case of power loss. TrueNAS works well with APC brand UPSs, followed by CyberPower. Consider budgeting for a UPS with pure sine wave output. Some models of SSD can experience data corruption on power loss. If several SSDs experience simultaneous power loss, it could cause total pool failure, making a UPS a critical investment.

Ethernet Networking

The network in Network Attached Storage is as important as storage, but the topic reduces to a few key points:

- Simplicity - Simplicity is often the secret to reliability with network configurations.
- Individual interfaces - Faster individual interfaces such as 10/25/40/100GbE are preferable to aggregating slower interfaces.
- Interface support - Intel and Chelsio interfaces are the best-supported options.
- Packet fragmentation - Only consider a *jumbo frames* MTU with dedicated connections such as between servers or video editors and TrueNAS that are unlikely to experience packet fragmentation.
- LRO/LSO offload features - Interfaces with LRO and LSO offload features generally alleviates the need for jumbo frames and their use can result in lower CPU overhead.

High-Speed Interconnects

Higher band hardware is becoming more accessible as the hardware development pace increases and enterprises upgrade more quickly. Home labs can now deploy and use 40 GB and higher networking components. Home users are now discovering the same issues and problems with these higher speeds found by Enterprise customers.

iXsystems recommends using optical fiber over *direct attached copper* (DAC) cables for the high speed interconnects listed below:

- 10Gb NICs: SFP+ connectors
- 25Gb NICs: SFP28 connectors
- 40Gb NICs: QSFP+ connectors
- 100Gb NICs: QSFP28 connectors
- 200Gb NICs: QSFP56 connectors
- 400Gb NICs: QSFP-DD connectors

iXsystems also recommends using optical fiber for any transceiver form factors mentioned when using fiber channels. Direct attached copper (DAC) cables could create interoperability issues between the NIC, cable, and switch.

Virtualized TrueNAS CORE

Finally, the ultimate TrueNAS hardware question is whether to use actual hardware or choose a virtualization solution. TrueNAS developers virtualize TrueNAS every day as part of their work, and cloud services are popular among users of all sizes. At the heart of the TrueNAS design is OpenZFS. The design from day one works with physical storage devices. It is aware of their strengths and compensates for their weaknesses. When the need arises to virtualize TrueNAS:

- Pass hardware disks or the entire storage controller to the TrueNAS VM if possible (requires VT-d/AMD-Vi support).
- Disable automatic scrub pools on virtualized storage such as VMFS, and never scrub a pool while also running storage repair tasks on another layer.
- Use a least three vdevs to provide adequate metadata redundancy, even with a striped pool.
- Provide one or more 8 GB or larger boot devices.
- Provide the TrueNAS VM with adequate RAM per its usual requirements.
- Consider jumbo frame networking if all devices support it.
- Understand that the guest tools in FreeBSD might lack features found in other guest operating systems.
- Enable MAC address spoofing on virtual interfaces and enable promiscuous mode to use VNET jail and plugins.

2.3 - Installation Instructions

This section provides instructions for users that are installing TrueNAS SCALE for the first time on their own system hardware and for users that need to do a clean install of SCALE.

The installation process covers installing SCALE using an iso, and then using the Console setup menu to configure their primary network interface. TrueNAS SCALE uses DHCP to provide the system IP address. It also describes configuring the rest of the network settings, storage pools, data sharing and data storage backup solutions in the web UI. Finally, it covers backing up the system configuration to a file.

If you plan to use this TrueNAS SCALE system as part of a cluster, complete the configuration process and then save the system configuration file.

Installation Articles

- Installing SCALE

  This article provides SCALE installation instructions for both physical hardware and virtual machines using an iso file. It also describes the iso verification process using and OpenPGP encryption application.

- Console Setup Menu Configuration

  This article provides instructions on configuration network settings using the Console setup menu after you install TrueNAS SCALE from the iso file.

- Setting Up Storage

  This article provides basic instructions for setting up your first storage pool, and also provides storage requirement information.

- Setting Up Data Sharing

  This article provides general information on setting up basci data sharing on TrueNAS SCALE.

- Backing Up TrueNAS

  This article provides general information and instructions on setting up storage data backup solutions and saving the system configuration file in TrueNAS SCALE.

2.3.1 - Installing SCALE

This article provides SCALE installation instructions for both physical hardware and virtual machines using an iso file. It also describes the iso verification process using and OpenPGP encryption application.

After you download the .iso file, you can start installing TrueNAS SCALE!

This article describes verifying the .iso file and installing SCALE using that file, and selecting the type of installation as either on physical hardware or a virtual machine (VM).

ISO Verification

The iXsystems Security Team cryptographically signs TrueNAS .iso files so that users can verify the integrity of their downloaded file. This section demonstrates how to verify an .iso file using the Pretty Good Privacy (PGP) and SHA256 methods.

PGP ISO Verification

You need an OpenPGP encryption application for this method of ISO verification.

Click here for the verification process.

1. Obtain an OpenPGP encryption application to used. There are many different free applications available, but the OpenPGP group provides a list of available software for different operating systems at https://www.openpgp.org/software/. The examples in this section show verifying the TrueNAS .iso using gnupg2 in a command prompt, but Gpg4win is also a good option for Windows users.

2. To verify the .iso source, go to https://www.truenas.com/download-tn-scale/, expand the **Security** option, and click **PGP Signature** to download the Gnu Privacy Guard signature file. This file may be a (.gpg) or a (.sig) file. Open the PGP Public key link and note the address in your browser and **Search results for** string.

3. Use one of the OpenPGP encryption tools mentioned above to import the public key and verify the PGP signature.

   Go to the .iso and the .iso.gpg or .iso.sig download location and import the public key using the keyserver address and search results string:

   ```
   user@ubuntu /tmp> gpg --keyserver keys.gnupg.net --recv-keys 0xc8d62def767c1db0dff4e6ec358eaa9112cf7946
   gpg: DBG: Using CREATE_BREAKAWAY_FROM_JOB flag
   gpg: key 358EAA9112CF7946: public key "IX SecTeam <security-officer@ixsystems.com>" imported
   gpg: DBG: Using CREATE_BREAKAWAY_FROM_JOB flag
   gpg: Total number processed: 1
   gpg:               imported: 1
   user@ubuntu /tmp>
   ```

   Use `gpg --verify` to compare the .iso and the .iso.gpg or .iso.sig files:

   ```
   user@ubuntu /tmp>  gpg --verify TrueNAS-SCALE-21.04-ALPHA.1.iso
   gpg: Signature made Thu May 27 10:49:02 2021 EDT using RSA key ID 12CF7946
   gpg: Good signature from "IX SecTeam <security-officer@ixsystems.com>"
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg:          There is no indication that the signature belongs to the owner.
   Primary key fingerprint: C8D6 2DEF 767C 1DB0 DFF4  E6EC 358E AA91 12CF 7946
   user@ubuntu /tmp>
   ```

   This response means the signature is correct but still untrusted.

4. Go back to the browser page that has the **PGP Public key**. Open and manually confirm that the key is issued for `IX SecTeam <security-officer@ixsystems.com>` (iX Security Team) on October 15, 2019 and is signed by an iXsystems account.

SHA256 Verification

SHA256 verification uses the checksum to validate/verify the file.

Click here for the verification process.

The command to verify the checksum varies by operating system:

- BSD use command `sha256 isofile`
- Linux use command `sha256sum isofile`
- Mac use command `shasum -a 256 isofile`

Windows or Mac users can install additional utilities like HashCalc or HashTab.

The value produced by running the command must match the value shown in the sha256.txt file. Different checksum values indicate a corrupted installer file that you should not use.

Installing SCALE

You can install SCALE on either physical hardware or a virtual machine.

Installing on Physical Hardware

TrueNAS SCALE is very flexible and can run on any x86_64 compatible (Intel or AMD) processor. SCALE requires at least 8GB of RAM (more is better) and a 20GB Boot Device.

Preparing the Install File

Physical hardware requires burning the TrueNAS SCALE installer to a device, typically a CD or removable USB device. This device is temporarily attached to the system to install TrueNAS SCALE to the system permanent boot device.

Write TrueNAS installer to a USB stick on Linux

To write the TrueNAS installer to a USB stick on Linux, plug the USB stick into the system and open a terminal.

Start by making sure the USB stick connection path is correct. There are many ways to do this in Linux, but a quick option is to enter the command `lsblk -po +vendor,model` and note the path to the USB stick. This shows in the **NAME** column of the `lsblk` output.

Next, use command `dd` to write the installer to the USB stick.

> Be very careful when using dd, as choosing the wrong *of=* device path can result in irretrievable data loss!

Enter command `dd status=progress if=path/to/.iso of=path/to/USB` in the CLI.

If this results in a permission denied error, use command `sudo dd` with the same parameters and enter the administrator password.

Installing on Physical Hardware From Device Media

Before you begin:

- Locate the hotkey defined by the manufacturer of your motherboard to uses in this process.
- Disable SecureBoot if your system supports it so or set it to **Other OS** so you can boot to the install media.

With the installer added to a device (CD or USB), you can now install TrueNAS SCALE onto the desired system.

Physical Hardware Install Instructions

Insert the install media and reboot or boot the system. At the motherboard splash screen, use the hotkey defined by your motherboard manufacturer to boot into the motherboard UEFI/BIOS.

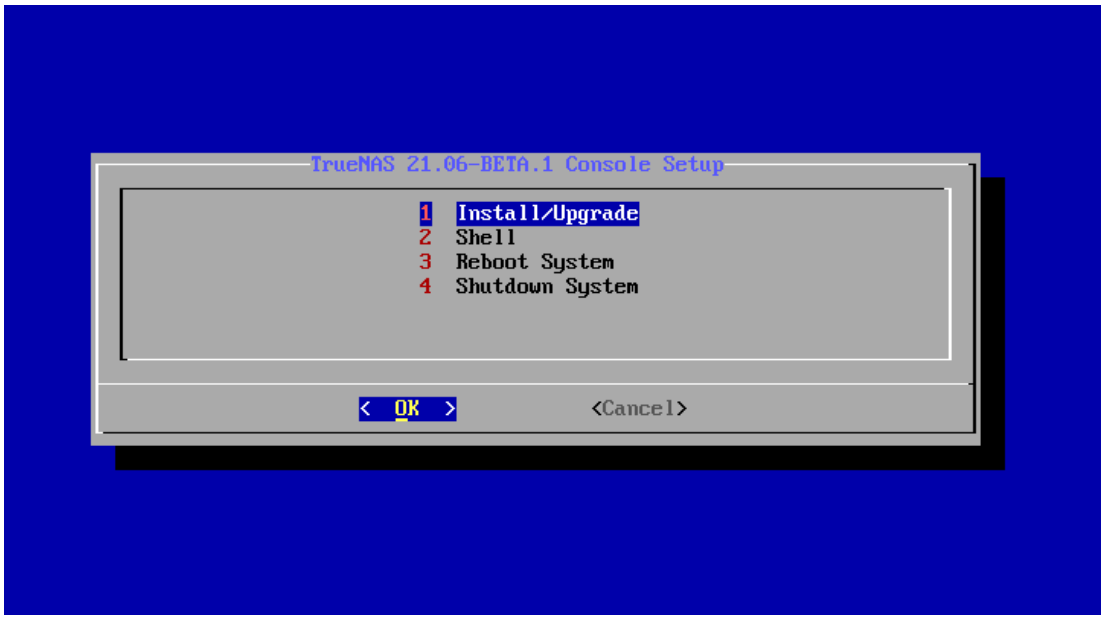
Choose to boot in **UEFI mode** or **legacy CSM/BIOS mode**. When installing TrueNAS, make the matching choice for the installation. For Intel chipsets manufactured in 2020 or later, UEFI is likely the only option.

If your system supports SecureBoot, and you haven't disable it or set it to **Other OS**, do it now so you can boot the install media.

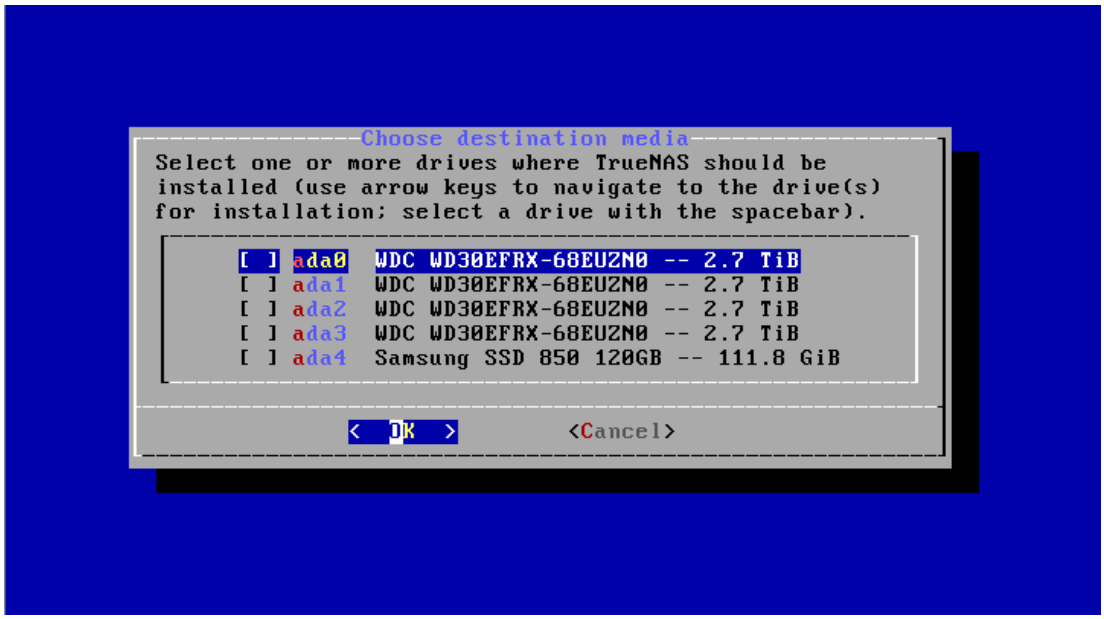
Select the install device as the boot drive, exit, and reboot the system. If the USB stick is not shown as a boot option, try a different USB slot. Which slots are available for boot differs by hardware.

After the system boots into the installer, follow these steps.

1. Select **Install/Upgrade**.



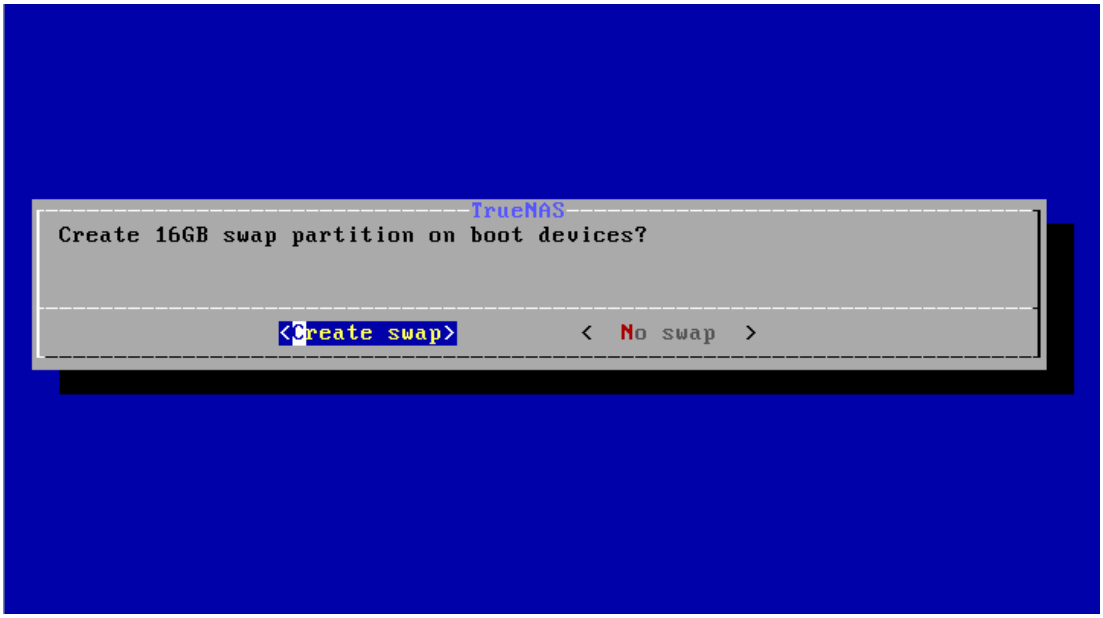
2. Select the desired install drive.



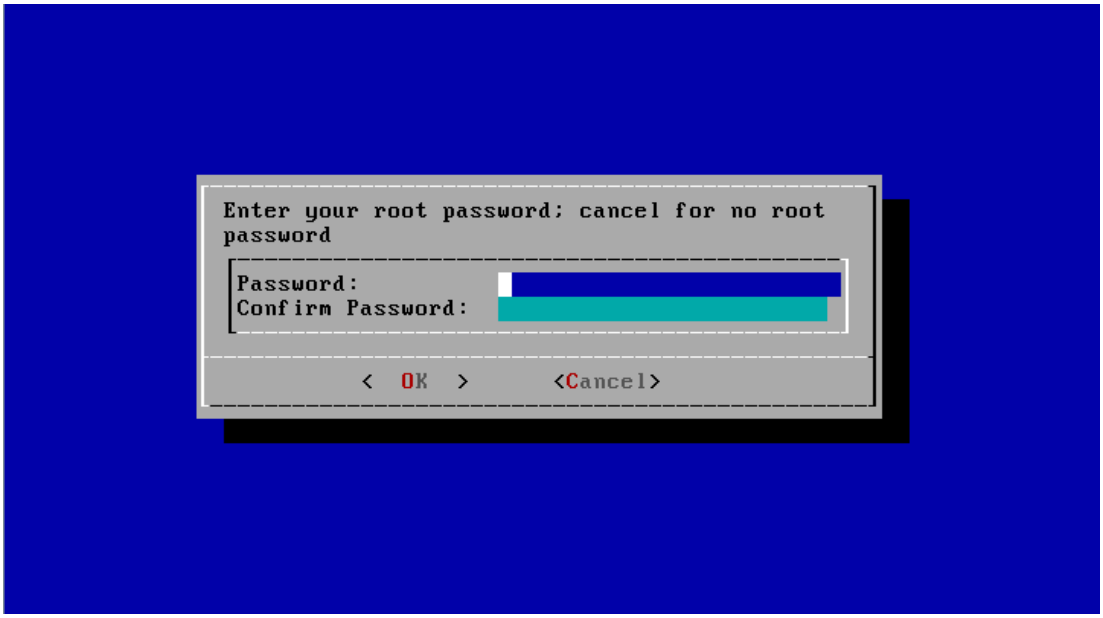
Select **Yes**.

3. Select **Fresh Install** to do a clean install of the downloaded version of TrueNAS SCALE. This erases the contents of the selected drive!

When the operating system device has enough additional space, you can choose to allocate some space for a swap partition to improve performance.



4. Next, set a password for the TrueNAS administrative account, named `root` by default. This account has full control over TrueNAS and is used to log in to the web interface. Set a strong password and protect it.



5. After following the steps to install, reboot the system and remove the install media.

Troubleshooting

If the system does not boot into TrueNAS SCALE, there are several things you can check to resolve the situation:

- Check the system BIOS and see if there is an option to change the **USB emulation** from **CD/DVD/floppy** to **hard drive**. If it still does not boot, check to see if the card/drive is UDMA compliant.
- Check to see if the system BIOS supports **EFI with BIOS emulation**, if not, see if it has an option to boot using **legacy BIOS mode**.
- If the system starts to boot but hangs with this repeated error message: `run_interrupt_driven_hooks: still waiting after 60 seconds for xpt_config`, go into the system BIOS and look for an onboard device configuration for a `1394 Controller`. If present, disable that device and try booting again.
- If the burned image fails to boot and the image was burned using a Windows system, wipe the USB stick before trying a second burn using a utility such as Active@ KillDisk. Otherwise, the second burn attempt fails as Windows does not understand the partition that was written from the image file. Be very careful to specify the correct USB stick when using a wipe utility!

Installing on a Virtual Machine

Installation Tutorial Video

Because TrueNAS SCALE is built and provided as an .iso file, it works on all virtual machine solutions (VMware, VirtualBox, Citrix Hypervisor, etc). This section describes installing on a VM using VMware Workstation Player on Windows.

Minimum Virtual Machine Settings

Regardless of virtualization application, use these minimum settings:

- RAM: at least 8192MB (8GB)
- DISKS: two virtual disks with at least 16GB, one for the operating system and boot environments and at least one additional virtual disk to use as data storage.
- NETWORK: Use NAT, bridged, or host-only depending on your host network configuration.

Networking Checks for VMWare

When installing TrueNAS in a VMWare VM, double check the virtual switch and VMWare port group. A misconfigured virtual switch or VMWare port group can cause network connection errors for plugins or jails inside the TrueNAS VM. Enable **MAC spoofing** and **promiscuous mode** on the switch first, and then the port group the VM is using.

Jail Networking

If you have installed TrueNAS in VMware, you need functional networking to create a jail.

For the jail to have functional networking, you have to change the VMware settings to allow Promiscuous, MAC address changes, and Forged Transmits.

Setting	Description
Promiscuous Mode	When enabled at the virtual switch level, objects defined within all portgroups can receive all incoming traffic on the vSwitch.
MAC Address Changes	When set to **Accept**, ESXi accepts requests to change the effective MAC address to a different address than the initial MAC address.
Forged Transmits	When set to **Accept**, ESXi does not compare source and effective MAC addresses.

Installing on a Generic Virtual Machine

For most hypervisors, the procedure for creating a TrueNAS VM is the same.

Genic VM Install Instructions

1. Create a new virtual machine as usual, taking note of the following settings.
   - The virtual hardware has a bootable CD/DVD device pointed to the TrueNAS SCALE installer image (this is usually an .iso).
   - The virtual network card configuration allows your network to reach it. **bridged** mode is optimal as this treats the network card as one plugged into a simple switch on the existing network.
   - Some products require you identify the OS you plan to install on the VM. The ideal option is **Debian 11 64 bit**. If this is not available, try options like **Debian 11**, **Debian 64 bit**, **64 bit OS**, or **Other**. *Do not* choose a Windows, Mac or BSD related OS type!
   - For VMWare hypervisors, install in BIOS mode.
   - Ensure the VM has sufficient memory and disk space. For TrueNAS set to at least **8 GB** RAM and **20 GB** disk space. Not all hypervisors allocate enough memory by default.
2. Boot the VM and install TrueNAS as usual.
3. When installation completes, shut down the VM instead of rebooting, and disconnect the CD/DVD from the VM before rebooting the VM.
4. After rebooting into TrueNAS, install VM tools if applicable for your VM, and if they exist for Debian 11, or ensure they loaded on boot.

Example VMWare Player 15.5 Installation

This example describes installing TrueNAS SCALE using VMWare Player 15.5.

Click here for more information.

Open VMware Player and click **Create a New Virtual Machine** to enter the New Virtual Machine Wizard.

1. Install disk image file.

   Select the **Installer disk image file (.iso)** option, click **Browse…**, and upload the TrueNAS SCALE .iso downloaded earlier.

2. Name the virtual machine.

   In this step, you can change the virtual machine name and location.

3. Specify the disk capacity.

   Specify the maximum disk size for the initial disk. The default *20GB* is enough for TrueNAS.

   Next, select **Store virtual disk as a single file**.

4. Review the virtual machine.

   Review the virtual machine configuration before proceeding. By default, VMware Player does not set enough RAM for the virtual machine.

   Click **Customize Hardware…** > **Memory**. Drag the slider up to 8GB and click **Ok**.

5. Power on the machine after creation if desired. Select **Power on this virtual machine after creation**.

Add Virtual Disks

After installing SCALE on a virtual machine (VM), add virtual disks to the VM. You need a minimum of two disks, 16 GB each. One disk is for the boot environment the other for data storage.

Adding Virtual Disks

1. After creating the virtual machine, select it from the virtual machine list and click **Edit virtual machine settings**.
2. Click **Add…** and select **Hard Disk**. Select **SCSI** as the virtual disk type.
3. Select **Create a new virtual disk**. Specify the maximum size of this additional virtual disk. This disk stores data in TrueNAS. If desired, allocate the disk space immediately by setting **Allocate all disk space now**.
4. Select **Store virtual disk as single file**.
5. Name and chose a location for the new virtual disk.

Repeat this process until enough disks are available for TrueNAS to create ideal storage pools. This depends on your specific TrueNAS use case. See Pool Creation for descriptions of the various pool (“vdev”) types and layouts.

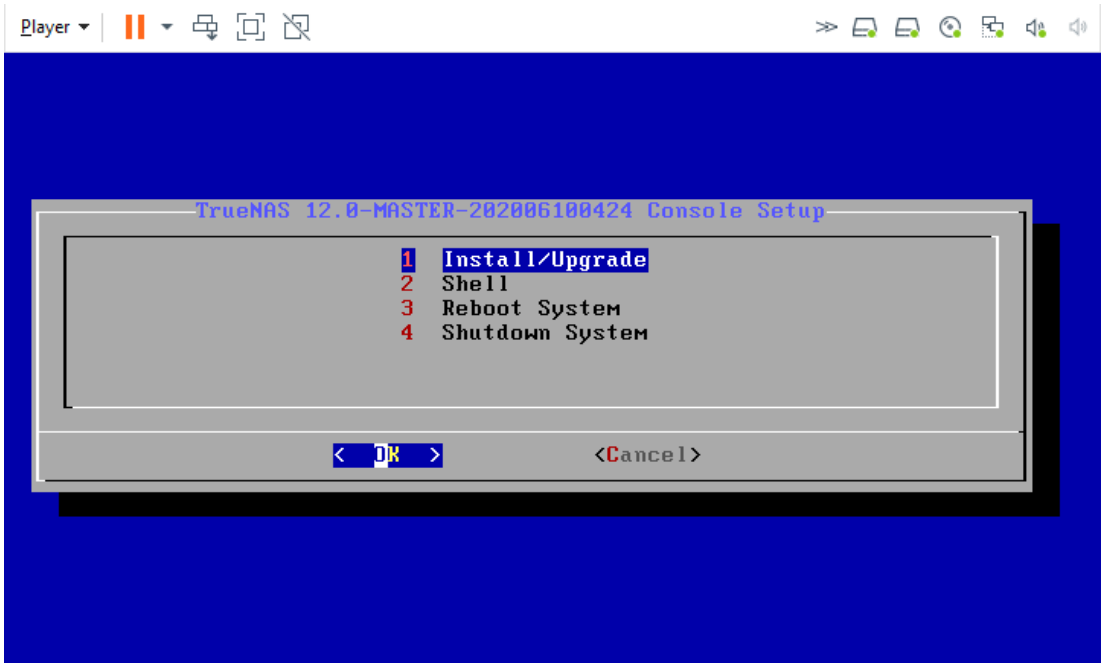
Using the TrueNAS Installer

Just as with installing SCALE on physical hardware, you complete the install in the VM by booting into the TrueNAS installer.

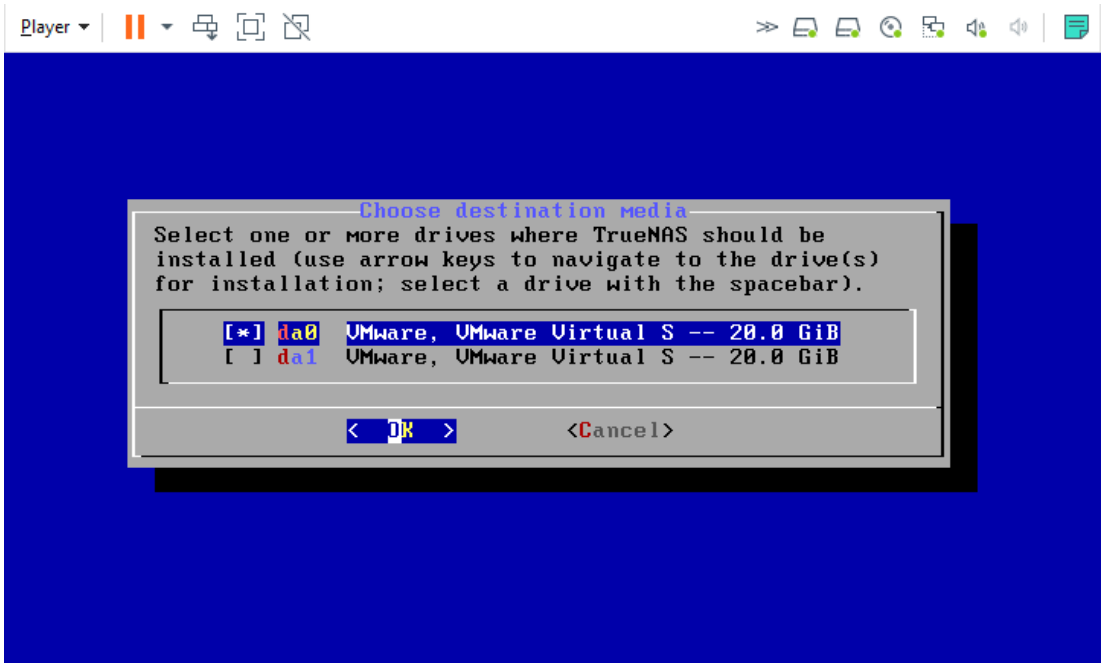
Using the TrueNAS Installer in a Virtual Machine

Select the virtual machine from the list and click **Play virtual machine**. The machine starts and boots into the TrueNAS installer.

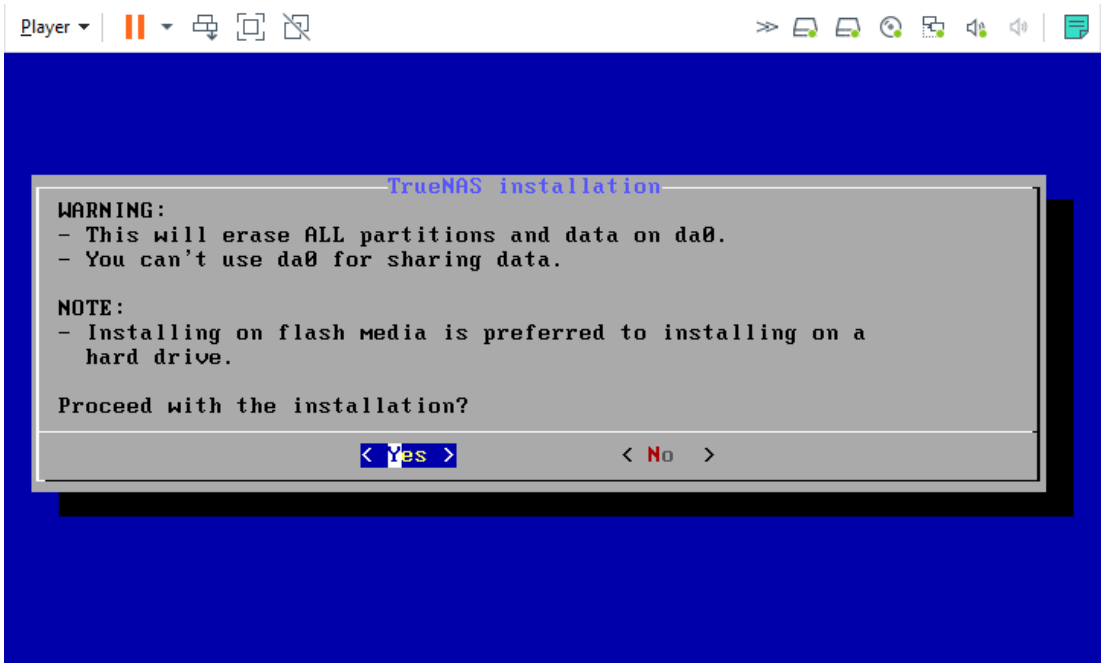
1. Select **Install/Upgrade**.



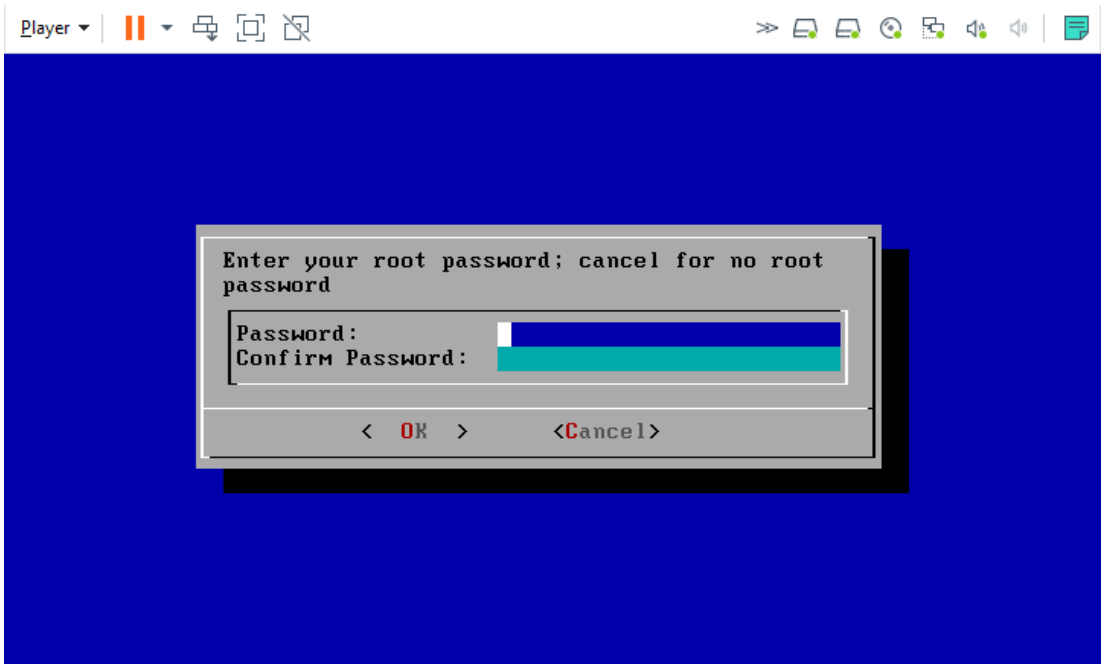
2. Select the desired disk for the boot environments.



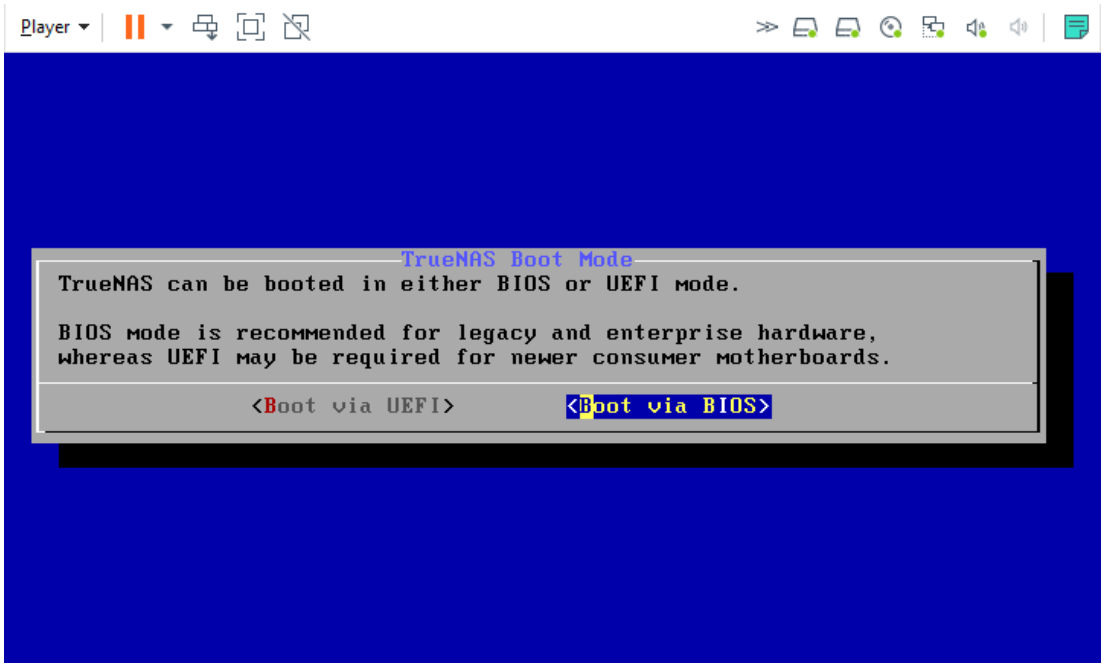
3. Select **Yes**. This erases all contents on the disk!



4. Next, set a password for the TrueNAS administrative account, named `root` by default. This account has full control over TrueNAS and is used to log in to the web interface. Set a strong password and protect it.



5. Select **Boot via BIOS**.



After the TrueNAS SCALE installation completes, reboot the system. The Console Setup Menu displays when the system boots successfully.

Congratulations, TrueNAS SCALE is now installed!

The next step is to boot up the system and configure SCALE network and general settings with the [Console Setup Menu]](/scale/gettingstarted/install/consolesetupmenuscale/) so you can log into the web UI.

Related Content

- Adding Network Settings
- Console Setup Menu Configuration
- Migrating from TrueNAS CORE
- Setting Up Storage
- Creating Storage Pools
- Importing Storage Pools
- First Time Login
- Setting Up Data Sharing
- Backing Up TrueNAS

Related Update Articles

- Update Screens
- Updating SCALE

Related Virtual Machine Articles

- Adding and Managing VMs
- Accessing NAS From a VM
- Virtualization Screens

2.3.2 - Console Setup Menu Configuration

This article provides instructions on configuration network settings using the Console setup menu after you install TrueNAS SCALE from the iso file.

The Console setup menu (CSM) displays at the end of the boot process. If the TrueNAS system has a keyboard and monitor, you can use this menu to administer the system.

By default, TrueNAS does not display the Console setup menu when you connect via SSH or the web shell. The root user or another user with root permissions can start the Console setup menu by entering the `/etc/netcli` command.

The menu provides these options:

- **1) Configure network interfaces** which provides options to set up network interfaces. These display in the **Global Configuration** widget on the **Network** screen in the web UI.
- **2) Configure network settings** which provides options to set up the network default gateway, host name, domain, IPv4 gateway and the DNS name servers.
- **3) Configure static routes** which provides options to setup static routes. Not required as part of the initial configuration setup.
- **4) Reset root password** which resets the root user password. This is the password for the `root` user in the CLI and the root user login password for the web UI.
- **5) Reset configuration to defaults** which resets the system configuration settings back to defaults.
- **6) Open TrueNAS CLI shell** which starts a shell for running TrueNAS commands. Type `exit` to leave the shell.
- **7) Open Linux shell** which starts a shell window for running Linux CLI commands. Type `exit` to leave the shell.
- **8) Reboot** which reboots the system.
- **9) Shut down** which shuts down the system.

Console setup menu options can change with software updates, service agreements, etc.

> During boot, TrueNAS attempts to connect to a DHCP server from all live interfaces. If it receives an IP address, the Console setup menu displays it under **The web user interface is at:** so you can access the Web UI.

You might be able to access the web UI using a `hostname.domain` command at the prompt (default is `truenas.local`) if your system:

- Does not have a monitor.
- Is on a network that supports Multicast DNS (mDNS).

Configuring Network Settings

You can use the Console setup menu to configure your primary network interface and any other interfaces you want to uses such as a link aggregate (LAGG) or virtual LAN (VLAN). You can also use the Console setup menu to configure other network settings such as the default gateway, host name, domain, and the DNS name servers, or add static routes.

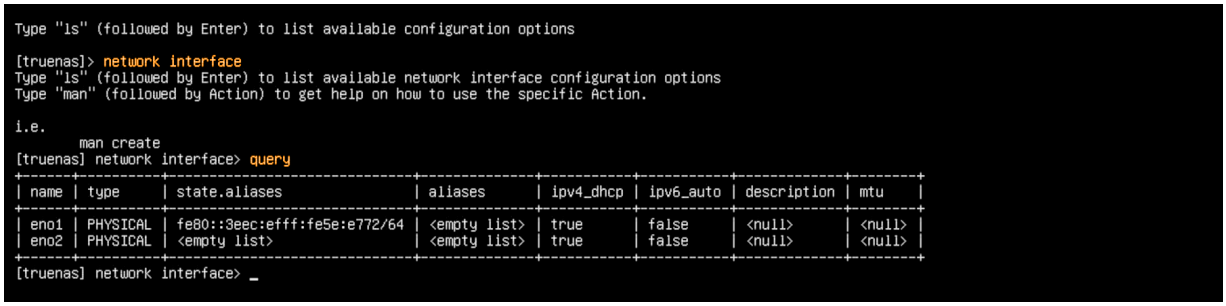
Enter `1` to display the **Configure Network Interfaces** screen where you can select the interface settings. If you want to use commands, enter `7` to open a Linux shell and then enter commands.

Enter `2` to display the Network Settings screen where you set up the host name, domain, default gateway and name servers.

Enter `3` to display the Static Route Settings screen where you can set up any static routes. You can also add static routes in the web UI.

Configuring Required Network Settings

First, configure your primary network interface. The IP address assigned by DHCP displays in the Console setup menu screen. You can configure the default gateway, host name, domain and DNS name severs using the Console setup menu but you should use the web UI to configure these settings. Go the **Network** screen.



To use the CSM, type **1** to display the **Configure Network Interfaces** screen. Select the interface to use as your primary network interface and the settings to use. Use `Tab` to select **Save** and then press `Enter`.

Next, open a browser window and enter the IP address DHCP assigned to your TrueNAS. The web UI should display, verifying you can access it. If it does not, return to the Console setup menu and re-enter the correct IP address as the primary interface address.

Log into the web UI as root with the default password set up during step 4 of the TrueNAS Installer process in Installing Scale.

After configuring the interface, you can use the CSM to configure the rest of your network settings, but this procedure describes using the web UI to configure the rest of the network settings.

To enter the remaining network settings in the web UI, go to **Network > Global Configuration** and click **Settings**. Enter the values in the appropriate fields and click **Save**.

For home users, use 8.8.8.8 as the DNS nameserver address. This allows you to access the internet using TrueNAS SCALE.

Changing the Root Password

Type **2** while in the Console setup menu. Type the new root user password and then re-enter the new password.

> Changing the root password disables 2FA (Two-Factor Authentication).

Resetting the System Configuration

> **Caution!** Resetting the configuration deletes all settings and reverts TrueNAS to default settings. Before resetting the system, back up all data and encryption keys/passphrases! After the system resets and reboots, you can go to **Storage** and click **Import** to re-import pools.

Enter **5** in the Console setup menu, then enter y to reset the system configuration. The system reboots and reverts to default settings.

Completing your System Setup

After setting up network requirements in the web UI, complete your system setup by:

- Setting up storage
- Setting up sharing
- Backing Up your Configuration

Related Content

- Adding Network Settings
- Installing SCALE
- Migrating from TrueNAS CORE

- Setting Up Storage
- Creating Storage Pools
- Importing Storage Pools
- First Time Login
- Setting Up Data Sharing
- Backing Up TrueNAS

Related Network Articles

- Dashboard
- Network Interface Screens
- Adding Network Settings
- Managing Interfaces
- Global Configuration Screens
- Managing Network Global Configurations
- Setting Up a Network Bridge
- Static Route Screens
- Setting Up a Link Aggregation

2.3.3 - Setting Up Storage

This article provides basic instructions for setting up your first storage pool, and also provides storage requirement information.

Now that you are logged in to the web interface, it is time to set up TrueNAS storage. These instructions describe a simple *mirrored* pool setup, where one disk is for storage and the other for data protection. However, there are a vast number of configuration possibilities for your storage environment! You can read more about these options in the in-depth Creating Storage Pools.

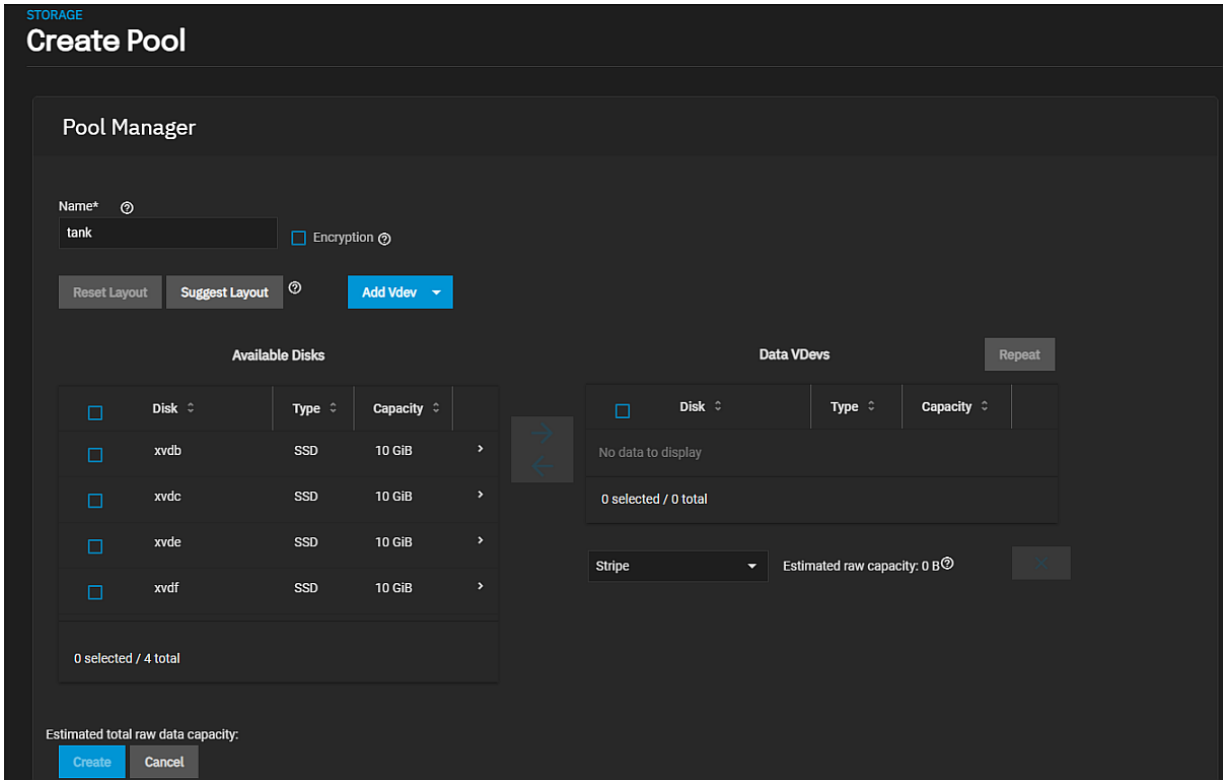
Minimum Storage Requirements

At minimum, the system needs at least two disks of identical size to create a mirrored storage pool. While a single-disk pool is technically allowed, it is not recommended. The disk used for the TrueNAS installation does not count toward this limit.

You can configure data backups in several ways and have different requirements. Backing data up in the cloud requires a 3rd party cloud storage provider account. Backing up with replication requires you to have additional storage on the TrueNAS system or (ideally) another TrueNAS system in a different location.

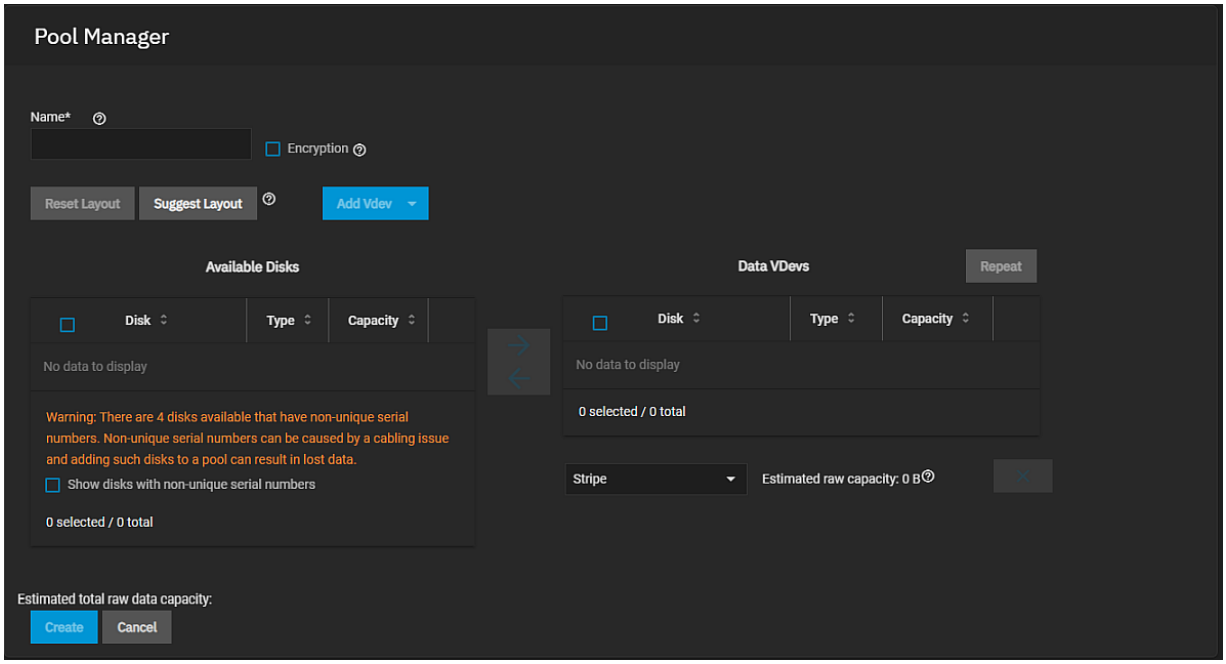
Setting Up Storage

Go to **Storage > Pools** and click **Add**. Select **Create a new pool** and click **Create Pool**



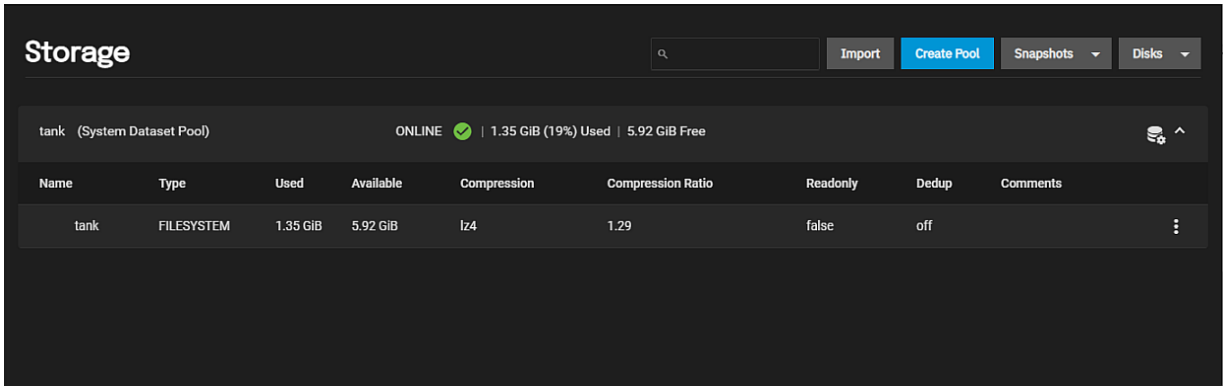
Enter a name for your first storage pool in **Name**. For example, *tank* or any other preferred name. Select two disks listed under the **Available Disks** section and then click the → to move them to the **Data VDevs** area.

> If the disks used have non-unique serial numbers a warning message displays. To populate the **Available Disks** section with these disk, select the **Show disk with non-unique serial numbers** checkbox.



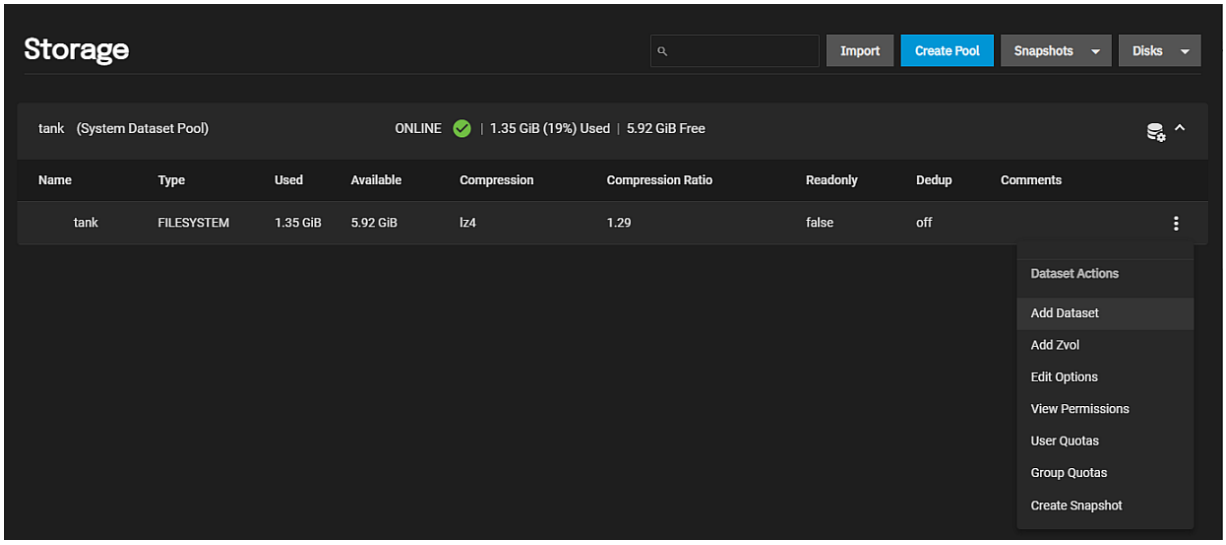
TrueNAS automatically suggests **Mirror** as the ideal layout for maximized data storage and protection.

Review the **Estimated raw capacity** to the right of the Data Vdev type dropdown list to make sure you have the storage capacity you need, and then click **Create**. A warning dialog displays. Click **Confirm** to activate the **CREATE POOL** button. After you click **CREATE POOL** the system displays a fetching-data dialog and then a status dialog.
TrueNAS wipes the disks and adds your pool (*tank* is the example used) to the **Storage > Pools** list.



Adding Datasets or Zvols

New pools have a root dataset that allows further division into new datasets or zvols. A *dataset* is a file system that stores data and has specific permissions. A *zvol* is a virtual block device that has a predefined storage size. To create either one, go to **Storage > Pools**, click ⋮, and select **Add Dataset** or **Add Zvol**.



The two fields that you cannot change after you click **Save** are the dataset **Name** and **Share Type**. **Name** is a required field but **Share Type** is optional. The default setting for **Share Type** is **Generic** which works for any share type you create or you can select **SMB** if you know you want to create an SMB share. A dataset with a **Share Type** set to **SMB** optimizes that dataset for the Windows sharing protocol.

Organize the pool with as many datasets or zvols you need according to your access and data sharing requirements before moving any data into the pool.

If you want to create additional pools with other disks not assigned to a pool, you can do that now or as you have a need for them.

When you finish building and organizing your TrueNAS pools, move on to configuring how the system shares data

Related Content

- Adding Network Settings
- Installing SCALE
- Console Setup Menu Configuration
- Migrating from TrueNAS CORE
- Creating Storage Pools
- Importing Storage Pools
- First Time Login
- Setting Up Data Sharing
- Backing Up TrueNAS

Related Storage Articles

- Storage Screens
- Snapshots Screens
- Zvol Screens
- Creating Storage Pools
- Edit ACL Screens
- Importing Storage Pools
- Adding and Managing Datasets
- Installing and Managing Self-Encrypting Drives
- Adding and Managing Zvols

2.3.4 - Setting Up Data Sharing

This article provides general information on setting up basci data sharing on TrueNAS SCALE.

After setting up storage on your TrueNAS, it is time to begin sharing data! There are several sharing solutions available on SCALE, but in this article we discuss the most common.

Sharing Data Methods

TrueNAS SCALE provides four types of sharing methods, but this article only discusses three:

- SMB for Windows
- NFS for Unix-like sharing
- ISCSi block shares

Setting UP SMB for Windows

To set up SMB sharing:

1. Create a dataset with **Share Type** set to **SMB**. Go to **Storage > Pools**

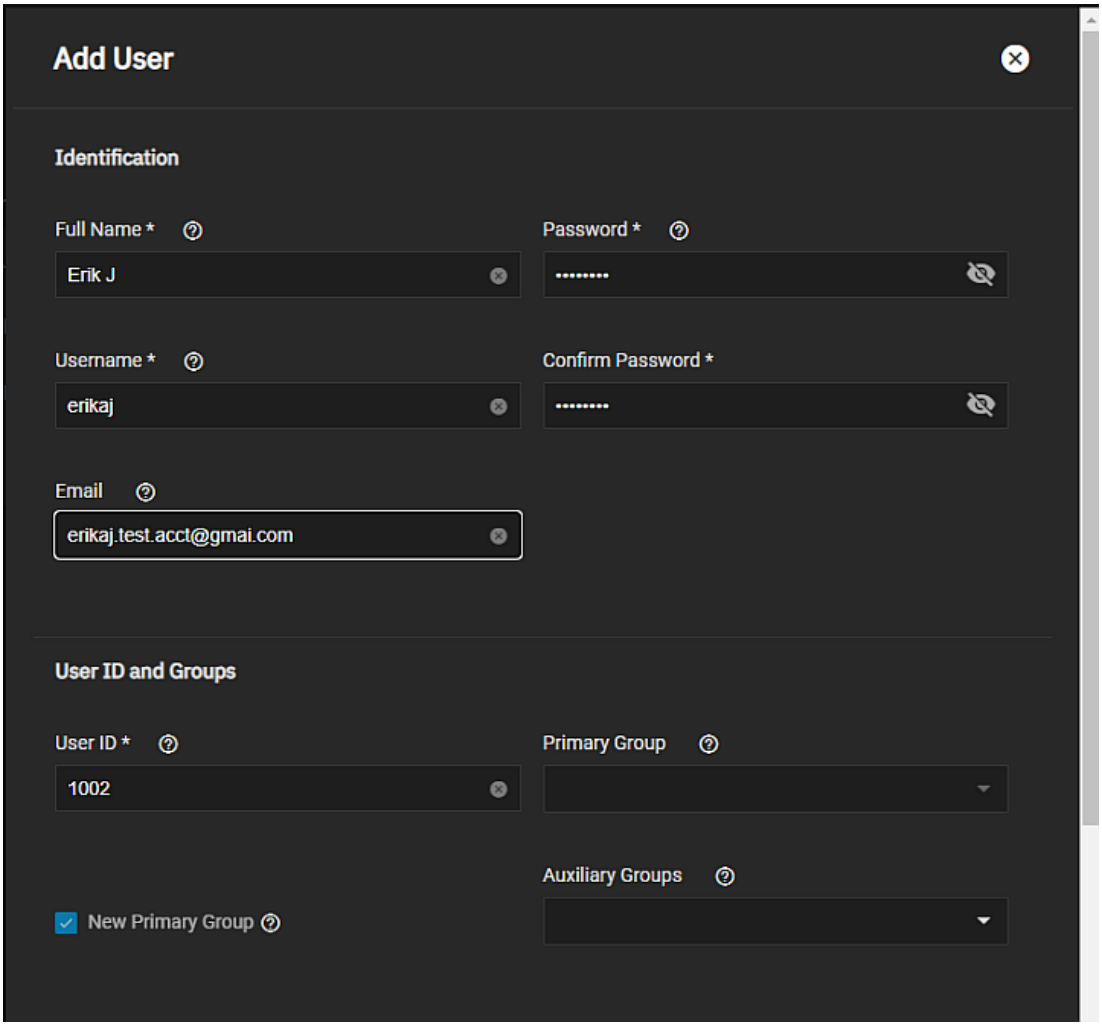
   a. Go to **Storage > Pools** and click on the ⋮ and click **Add Dataset**.

   b. Enter a name and select **SMB** in the **Share Type** field.

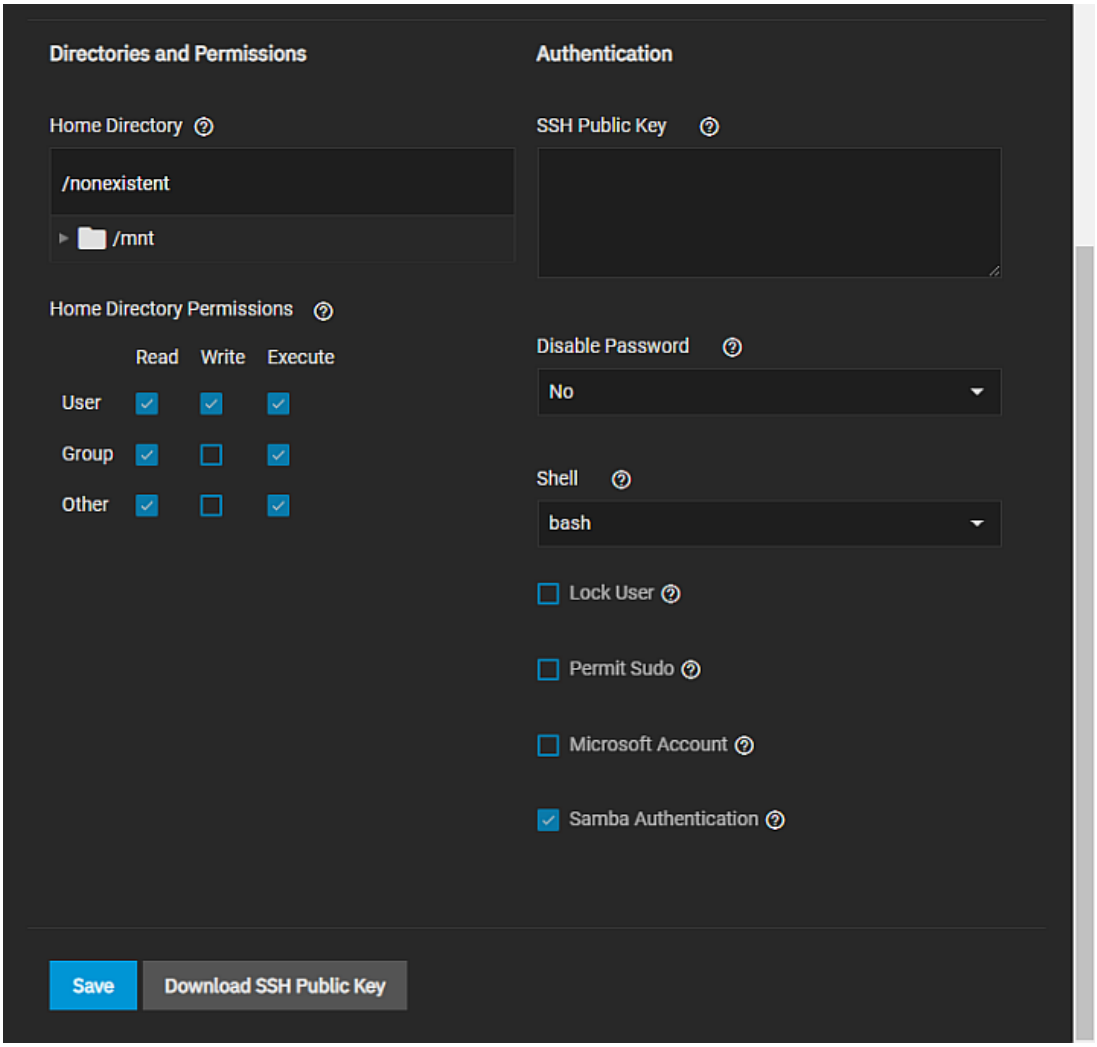
   c. Click **Save**.

2. Create the TrueNAS user accounts with **Samba Authentication** set.

   a. Go to **Credentials > Local Users** and click **Add** to create users.



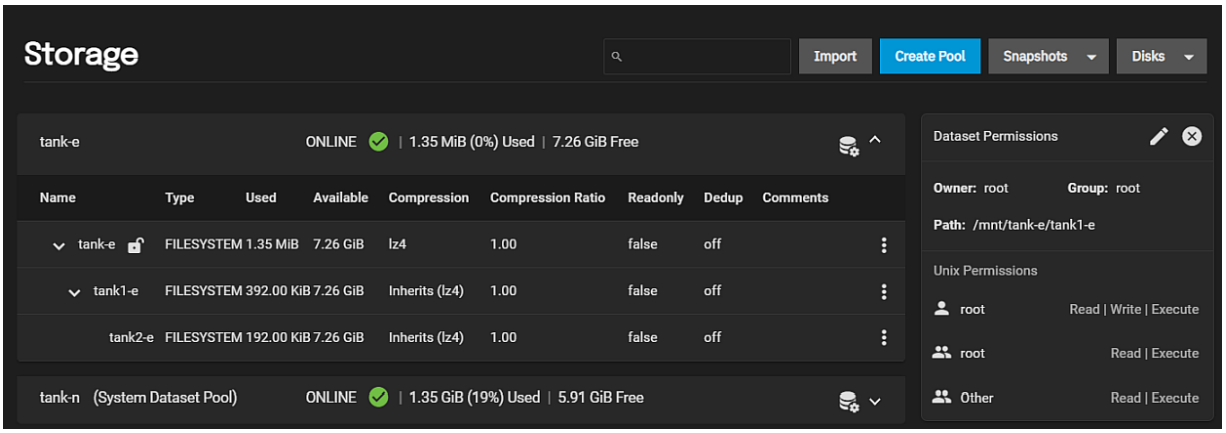
b. Enter the values in each required field, and then verify the checkmark for **Samba Authentication** exists.



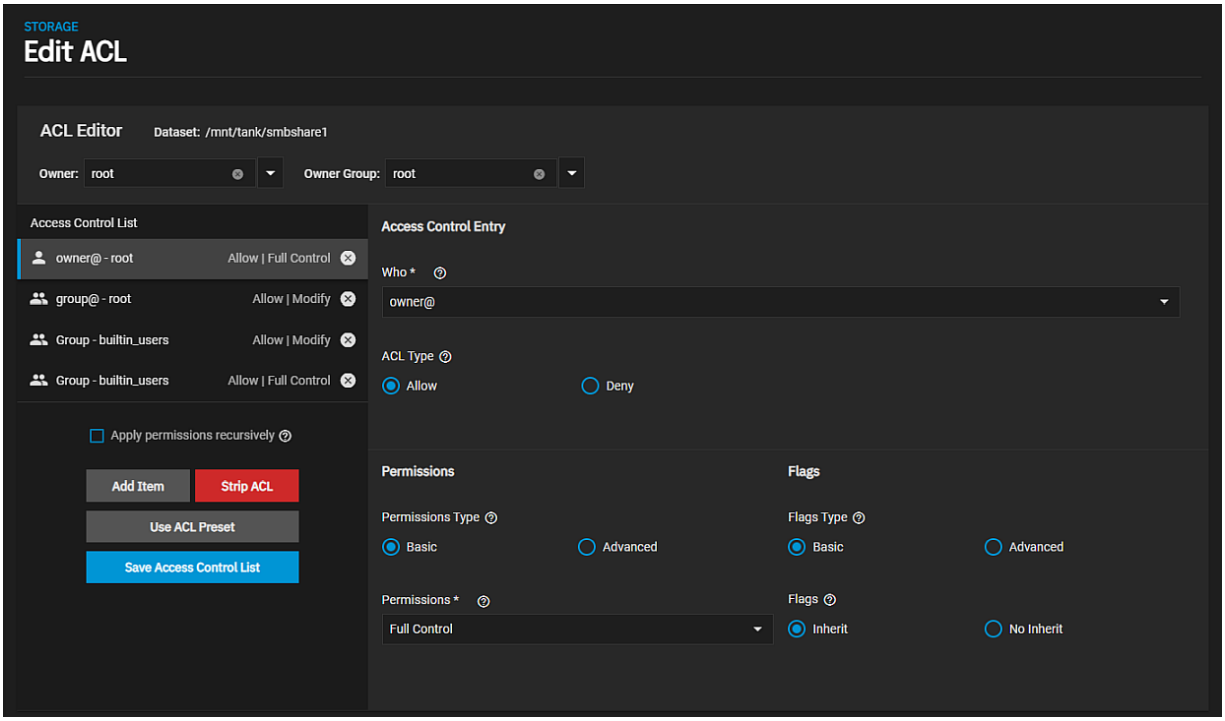
c. Click **Save**.

3. Edit the dataset permissions to set the **Select an ACL Preset** to **Open**.

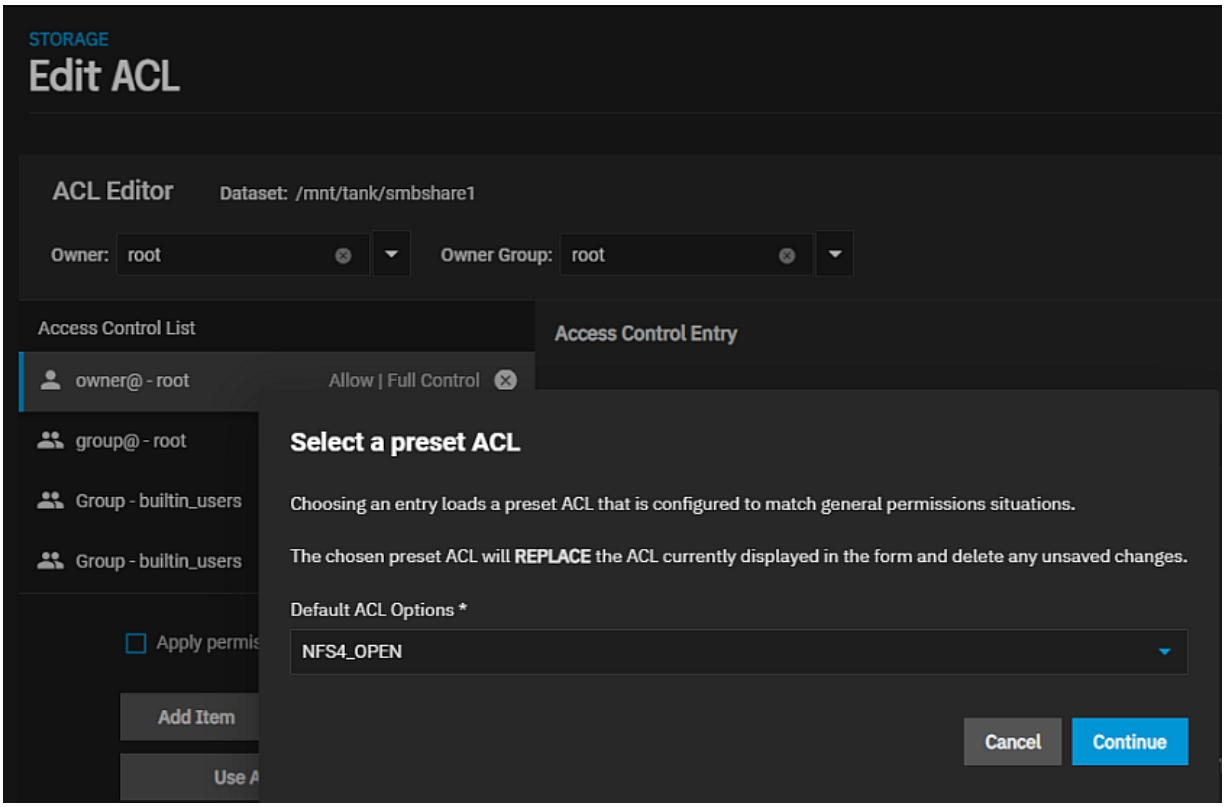
a. Go to **Storage > Pools** and click on the ⋮ for the dataset, and select **View Permissions**. The **View Permissions** widget for the selected dataset displays on the right side of the screen.



b. Click on the ✎ edit icon to display the **Edit ACL** screen.



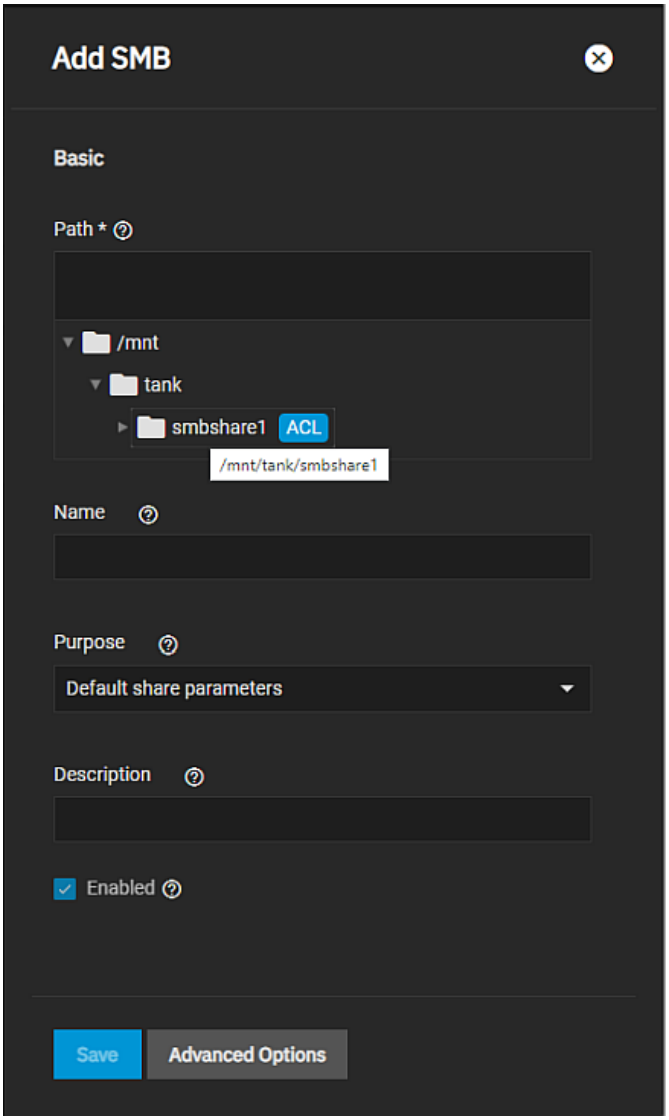
c. Select **Use ACL Preset**. The **Select a preset ACL** dialog displays. Select **NFS4_OPEN** from the dropdown list and then click **Continue**.



d. Click **Save Access Control List**.

4. Create the new SMB share. Go to **Shares > Windows (SMB) Shares** and click **Add**.

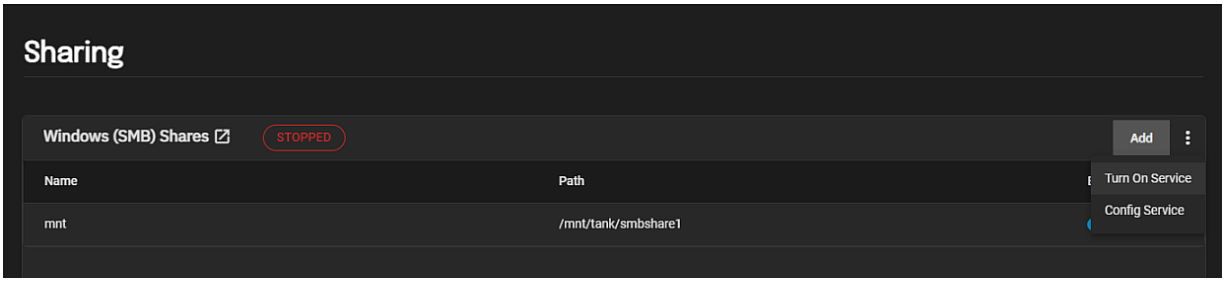
   a. Select the dataset you created for the share in the **Path** field. You can click on the ▸ to the left of **mnt**, and then at the pool to expand the options, and then click on the dataset to populate the field with the full path.



b. Enter a name for the share.

c. Click **Save**.

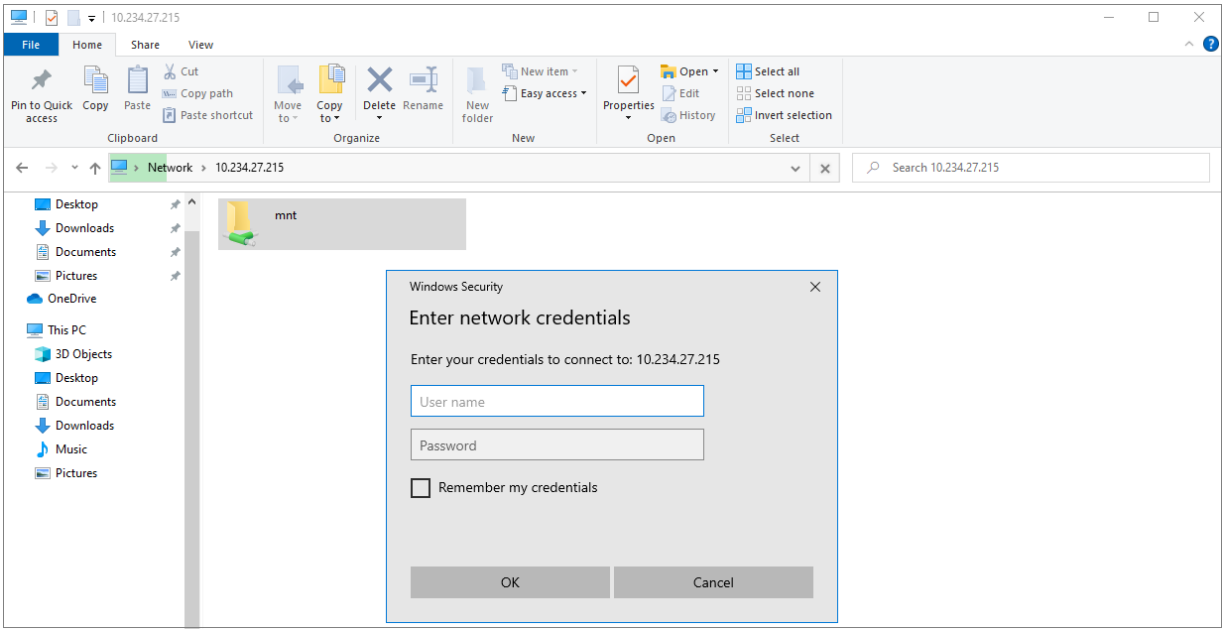
5. Turn the SMB service on. Click the ⋮ for the share and select **Turn On Service** from the **Sharing** screen.



6. Connect to the share. On a Windows 10 system, open the **File Browsers** and then:

a. In the navigation bar, enter \\ and the TruNAS system name or IP address. A login or credentials dialog displays.

b. Enter the TrueNAS user account credentials you created on the TrueNAS system.



c. Begin browsing the dataset.

Setting UP NFS for Unix-Like Share

To set up NFS sharing:

1. Create a dataset with **Share Type** set to **Generic**. Go to **Storage > Pools**

   a. Go to **Storage > Pools** and click on the ⋮ and click **Add Dataset**.

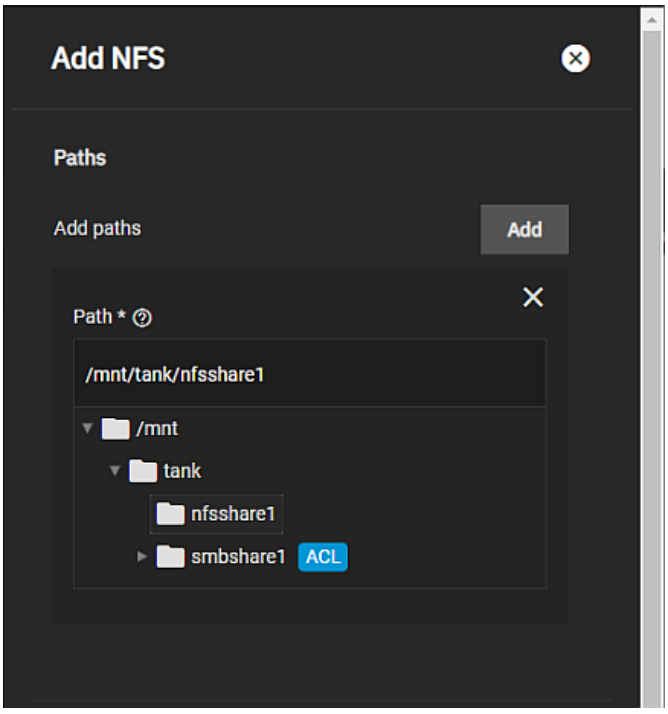
   b. Enter a name and select **Generic** in the **Share Type** field.

   c. Click **Save**.

2. Add additional packages like `nfs-common` to any client systems that require them.

3. Create the NFS share. Go to **Shares > UNIX (NFS) Share Targets** and click **Add**. The **Add NFS** configuration form displays.

   a. Select the dataset you created for the share in the **Path** field. You can click on the ▸ to the left of **mnt**, and then at the pool to expand the options, and then click on the dataset to populate the field with the full path.



b. Click **Save**.

4. Access the dataset. On a Unix-like system, open a command line and enter command `showmount -e *IPADDRESS*` where *IPADDRESS`* is your TrueNAS system address.

   ```
   tmoore@ChimaeraPrime:~$ showmount -e 10.238.15.194
   Export list for 10.238.15.194:
   /mnt/pool1/testds (everyone)
   ```

5. Make a local directory for the NFS mount. Enter command `sudo mkdir nfstemp/`

   ```
   tmoore@ChimaeraPrime:~$ sudo mkdir nfstemp/
   ```

6. Mount the shared directory. Enter command `sudo mount -t nfs *IPADDRESS:dataset path* where *IPADDRESS* is your system IP address and *:dataset path`* is the full path displayed in step 3.a. above.

   ```
   tmoore@ChimaeraPrime:~$ sudo mount -t nfs 10.238.15.194:/mnt/pool1/testds nfstemp/
   ```

7. From here, `cd` into the local directory and view or modify the files as needed.

Setting Up an ISCSi Block Share

Setting up block sharing is a complicated scenario that requires detailed configuration steps and knowledge of your network environment. A simple configuration is beyond the scop of this getting started guide, but detailed articles are available in the UI Reference section under Shares.

With simple sharing now set up, you can back up your configuration and set up data backup.

Related Content

- Adding Network Settings
- Installing SCALE
- Console Setup Menu Configuration
- Migrating from TrueNAS CORE
- Setting Up Storage
- Creating Storage Pools
- Importing Storage Pools
- First Time Login
- Backing Up TrueNAS

Related Shares Articles

- Adding SMB Shares
- SMB Shares Screens
- Managing SMB Shares
- Adding iSCSI Block Shares
- Block (iSCSI) Share Target Screens
- Using SMB Shadow Copy
- AFP Migration
- Configuring WebDAV Shares
- Setting Up SMB Home Shares
- Using an iSCSI Share

2.3.5 - Backing Up TrueNAS

This article provides general information and instructions on setting up storage data backup solutions and saving the system configuration file in TrueNAS SCALE.

After configuration your TrueNAS storage and data sharing, it is time to ensure effective back up of your data using the backup options TrueNAS provides. You should also download and save your system configuration file to protect your system configuration information.

Backing Up TrueNAS Storage Data

TrueNAS provides for data backup through cloud sync or replication.

Using Cloud Sync for Data Backup

> Cloud sync requires an account with a cloud storage provider and a storage location created with that provider, like Amazon S3 bucket. SCALE support major providers like Amazon S3, Google Cloud, Box and Microsoft Azure, along with a variety of other vendors. These providers can charge fees for data transfer and storage, so please review the polices of your cloud storage provider before transferring your data.

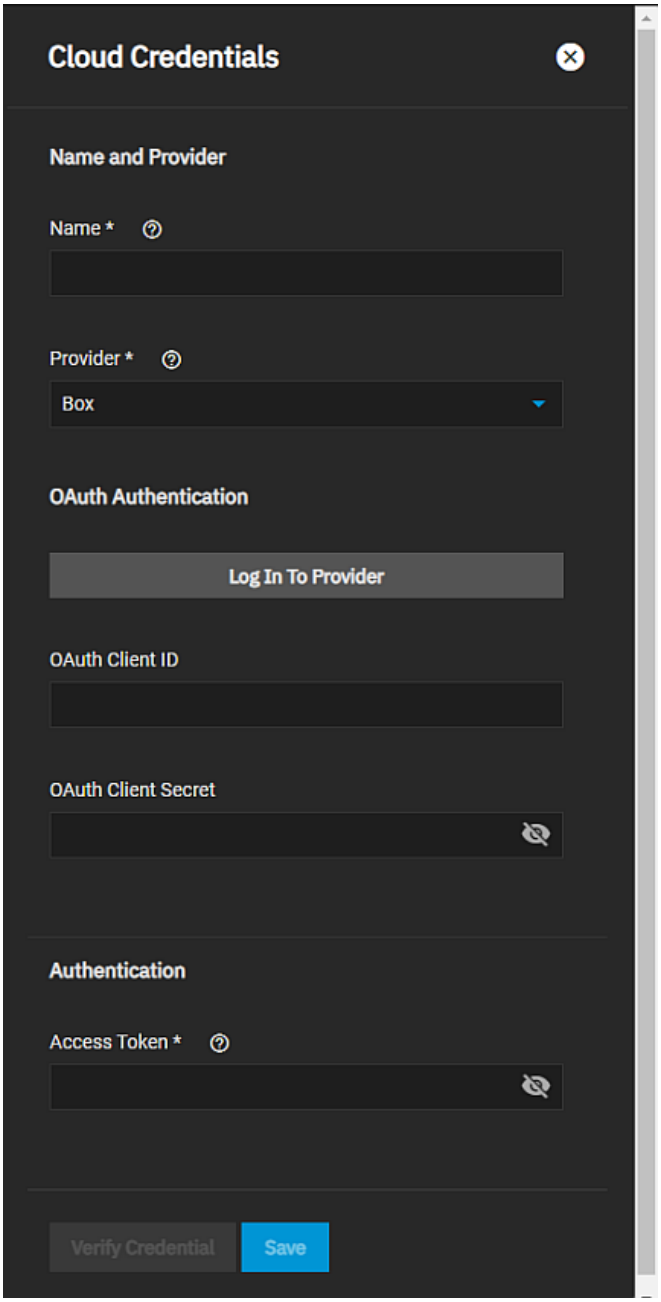
You can configure TrueNAS to send, receive, or synchronize data with a cloud storage provider. To set up cloud sync:

1. Add your cloud storage credentials to TrueNAS.

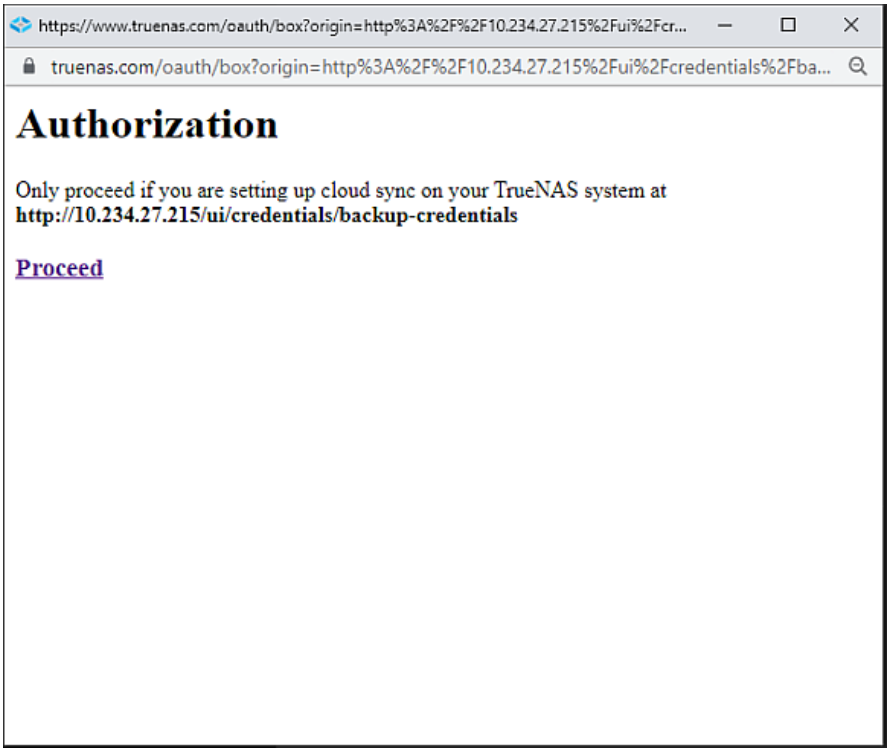
   Go to **Credentials > Backup Credentials** and click **Add**. The **Cloud Credentials** configuration panel displays.

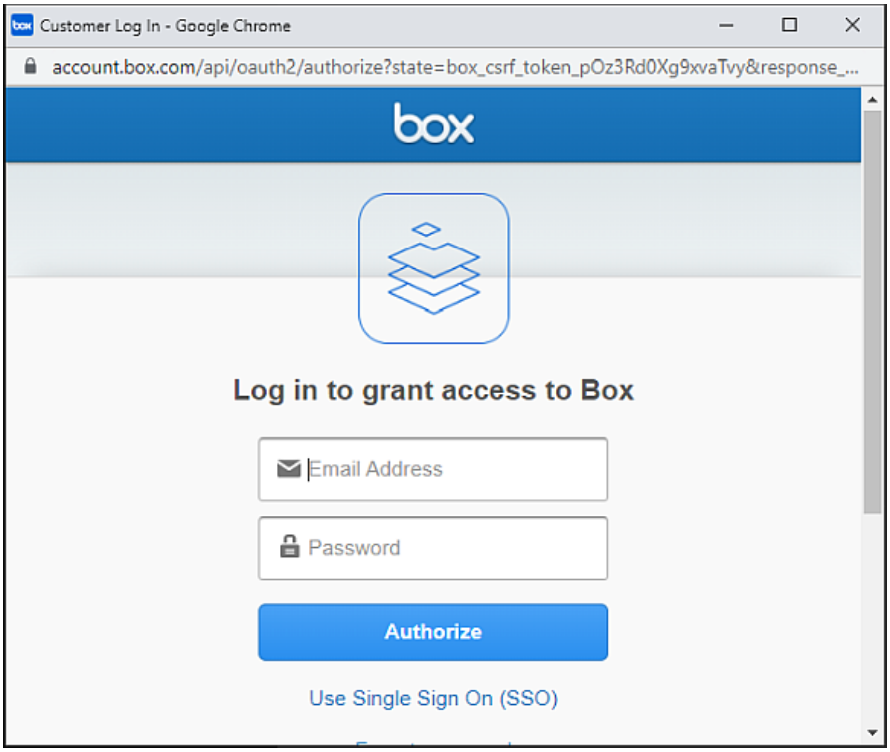
   Some cloud storage providers, like Amazon S3, require you log into your cloud account to generate additional information like an access key. TrueNAS requires you to enter the Amazon S3 credentials you generate on their **Security Credentials > Access Keys** page before you can save and add the cloud credentials. Check with your cloud storage provider to see what credentials they require TrueNAS to provide to complete data transfers.

   Some cloud storage providers, like Box, can automatically populate the required **Authentication** fields if you log into your account.



To automatically configure this credential, click **Log In To Provider**. An Authorization screen displays where you click **Proceed** to continue to the login screen for that service.



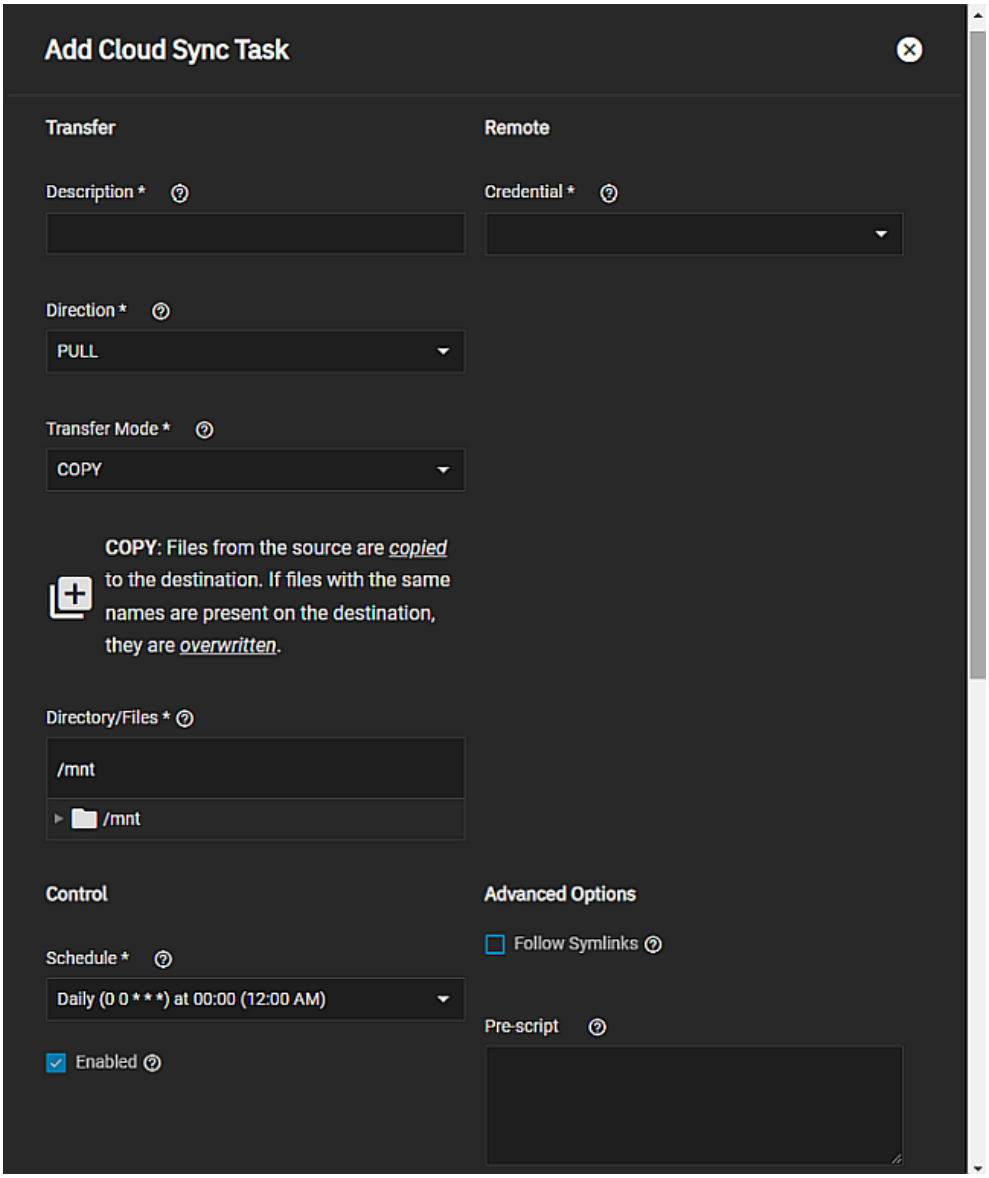


After you enter your cloud account login and password, the TrueNAS Cloud Credential authentication fields auto-populate with the required information. Click **Save** to complete the process of adding your cloud credentials.

We recommend you verify the credential before saving it if you do not log into your cloud storage provider as part of the process.

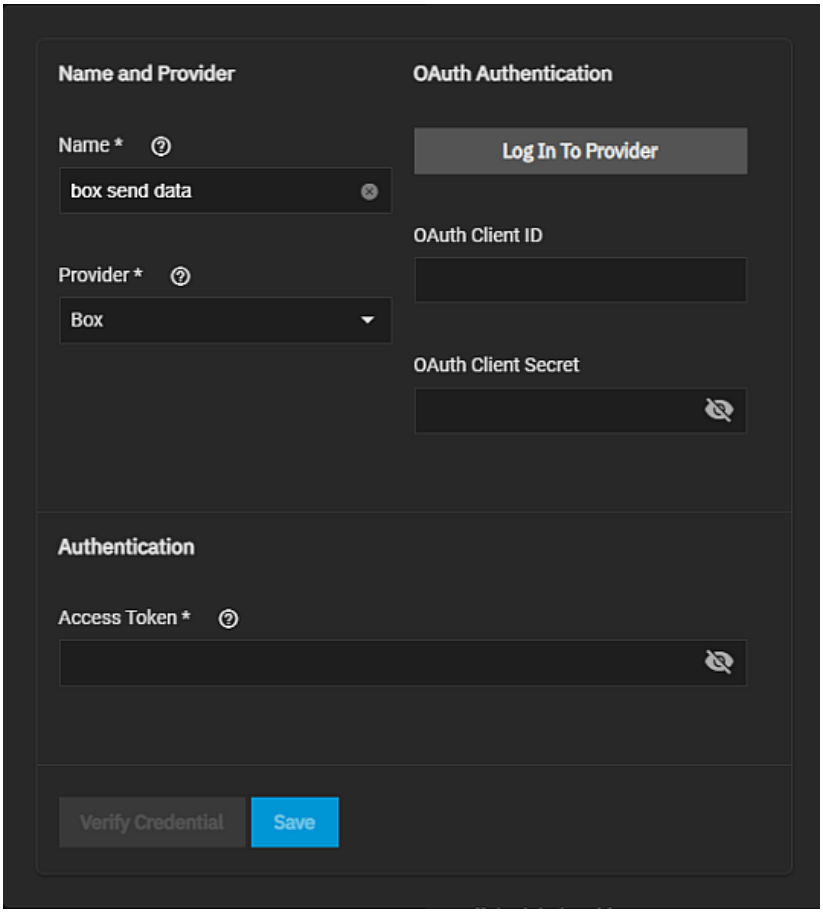
2. Create a data transfer task.

   Go to **Data Protection > Cloud Sync Tasks** and click **Add**. The **Add Cloud Sync Task** configuration panel displays.



Type a memorable name for this in **Name**, select the **Direction** as either **Push** to send data to the cloud service or **Pull** to get data from the cloud service. You can set up a cloud sync task to send data to and another task to get data from the cloud storage provider. Select the **Transfer Mode** as **Copy**, **Move** or **Sync**.

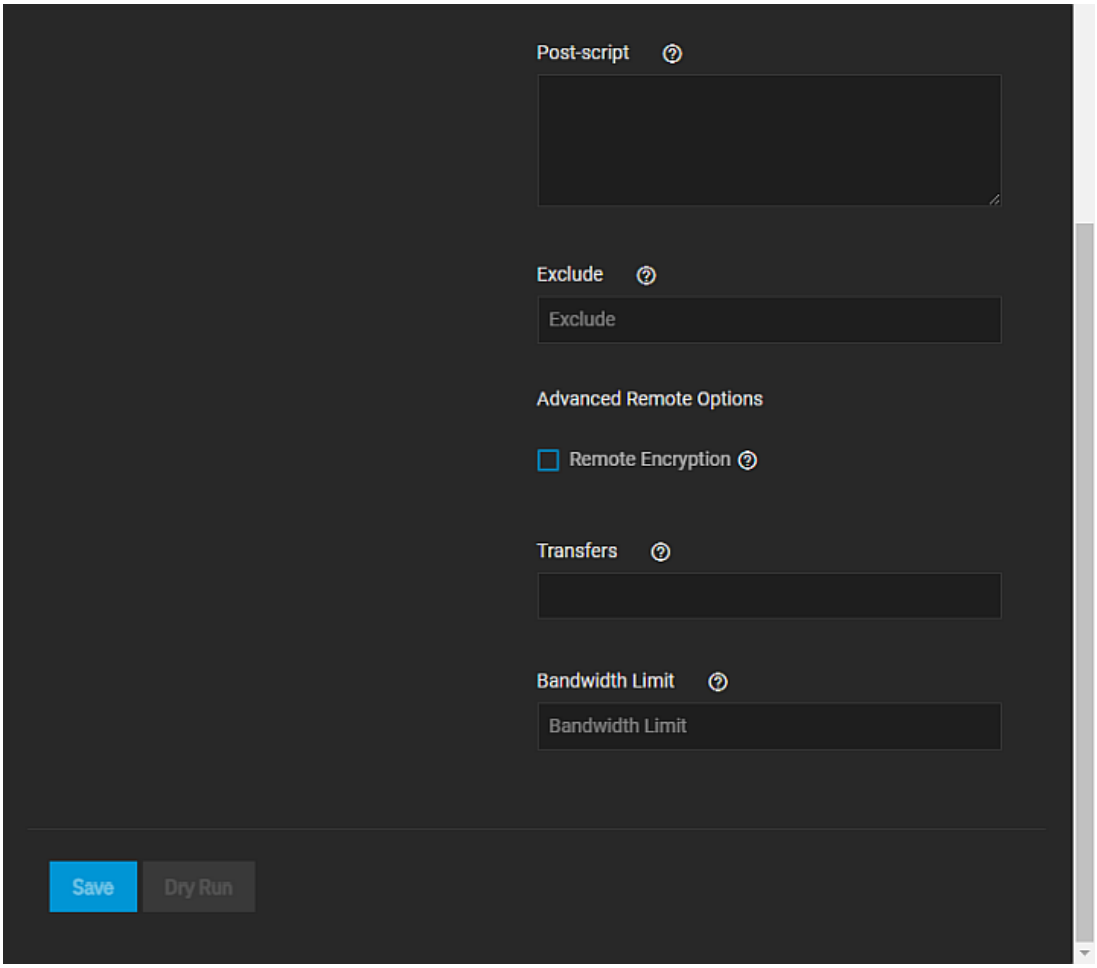
Click in the **Credential** dropdown field to select **Add a backup credential**. This displays a new form where you select and configure your cloud storage provider credentials. Amazon S3 is the default provider when the form opens. The example shown uses *box send data* as the name and **Box** as the **Provider**.



Box provides a way to auto-populate the authentication credentials when you click **Log In To Provider**. An **Authorization** window displays. Click **Proceed** and then the Box login window displays. Enter your Box cloud credentials. After the TrueNAS cloud storage provider authentication details populate the form, click **Verify Credential** and after verified, click **Save**. This form closes and returns you to the **Add Cloud Sync Task** configuration panel to complete the set up.

Either type the path into the **Directory/Files** field or click on the ▸ to the left of **mnt**, and then at the pool to expand the dataset options, and then click on the dataset, and then file if you want to narrow backup down that far, to populate the field with the full path.

Next when you want this task to run using the **Schedule** dropdown list to select the frequency.



Clear the **Enable** checkmark to make the configuration available without allowing the specified schedule to run the task.

To test the sync task, click **Dry Run**.

To manually activate a saved task, go to **Data Protection > Cloud Synch Tasks** click the ▸ for the cloud sync task you want to run. Select **Run Now** to start the cloud sync operation.

Using Replication for Data Backup

Replication is the process of taking a moment-in-time *snapshot* of the data and copying that snapshot to another location. Snapshots typically use less storage than full file backups and have more management options. This instruction shows using the TrueNAS replication wizard to create a simple replication task.

1. Create the replication task.

   Go to **Data Protection > Replication** and click **Add**. The **Replication Task Wizard** displays the **What and Where** configuration screen. Select both the **Source Location** and **Destination Location** using the dropdown list options. You can back up your data on the same system or a different system. If you select **A different system** you must have SSH connection, destination and source information ready.

   Next enter the **Source** and **Destination** paths. You can either type the full path to the data you want to back up or click on the ▸ to the left of **mnt**, and then at the pool to expand the dataset options, and then click on the dataset, and then file if you want to narrow backup down that far, to populate the field with the full path.

   The task a name populates from the values in **Source** and **Destination**. Click **Next**.

2. Define when you want this task to occur.

   Select the radio button for **Run On a Schedule** and select the schedule you want to use. Or select **Run Once** to run the task manually.

   Select the radio button to specify how long the destination snapshot lifetime.

3. Click **START REPLICATION**

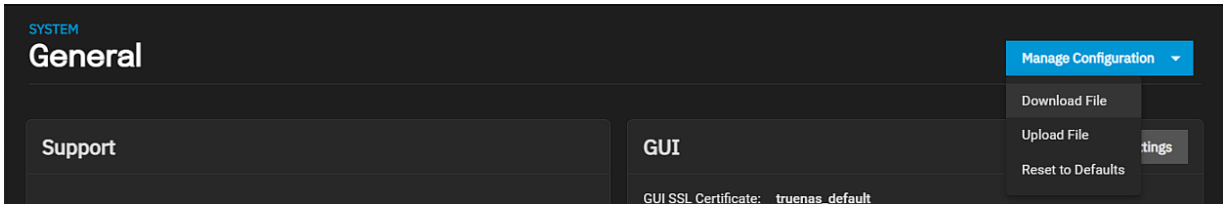
To confirm replication created your snapshot, go to **Storage > Snapshots**.

Backing Up the System Configuration

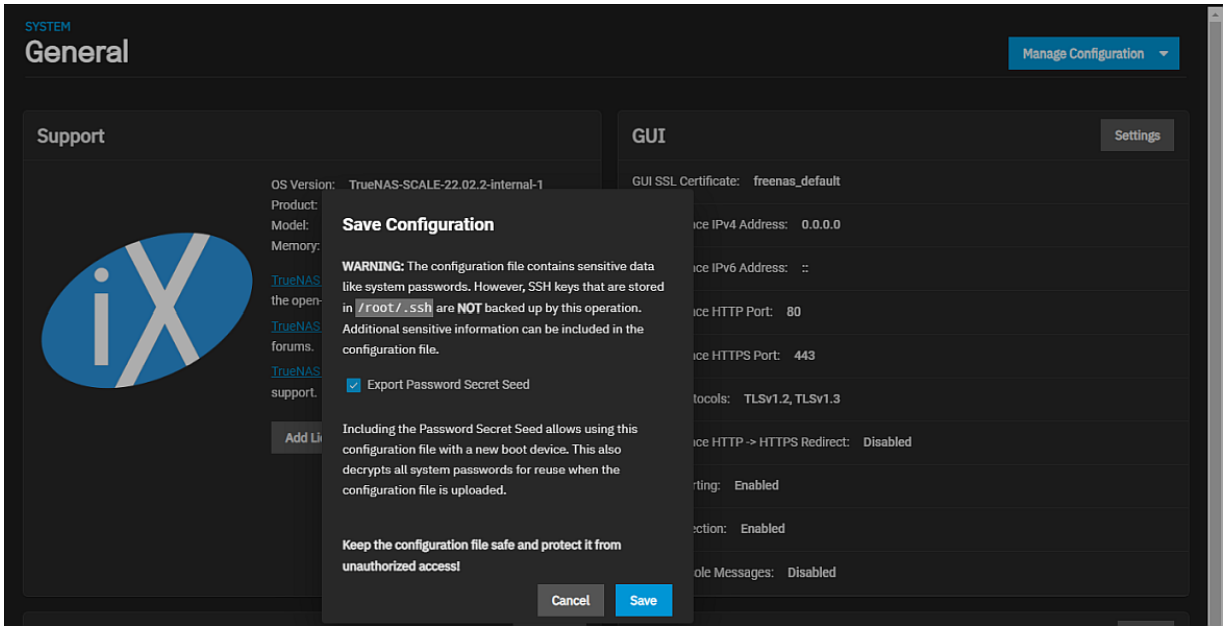
Now that you configured your system network, storage and any data shares you wanted, and you have set up your data back up solution it is time to back up your system configuration.

If you plan to set up a cluster that includes this TrueNAS scale, wait to download your system configuration file until the cluster is set up and working.

Go to System **Settings > General** and click on **Manage Configuration**. Select **Download File**.



The **Save Configuration** dialog displays.



Click **Export Password Secret Seed** and then click **Save**. The system downloads the system configuration. Save this file in a safe location on your network where files are regularly backed up.

Anytime you change your system configuration, download the system configuration file again and keep it safe.

Related Content

- Adding Network Settings
- Installing SCALE
- Console Setup Menu Configuration
- Migrating from TrueNAS CORE
- Setting Up Storage
- Creating Storage Pools
- Importing Storage Pools
- First Time Login
- Setting Up Data Sharing

Related Backup Articles

- Adding Cloud Credentials
- Adding Cloud Sync Tasks
- Adding Replication Tasks
- Backing Up Google Drive to TrueNAS SCALE
- Cloud Credentials Screens
- Managing the System Configuration
- Cloud Sync Tasks Screens
- Setting Up a Local Replication Task
- Setting Up Advanced Replication Tasks
- Backup Credentials

Related Cluster Articles

2.4 - Migrating Instructions

This section provides information for CORE users migrating to SCALE.

Linux treats device names differently than FreeBSD so please read Component Naming for more information.

The ZFS flag feature merged into the TrueNAS fork of OpenZFS for developers to test and integrage with other parts of the system on June 29,2021 is also removed. Please read ZFS Feature Flags Removed for details on this change.

Migration Articles

- Migrating from TrueNAS CORE

  This article provides instructions on migrating from TrueNAS CORE to SCALE. Migration methods include using an ISO file or a manual update file.

- Component Naming

  This article provides information on disk and interface naming changes related to the change from FreeBSD storage and sharing in CORE to Linux in TrueNAS SCALE.

- ZFS Feature Flags Removed

  This article provides information on the removal of the ZFS feature flag merged into OpenZFS in June 29, 2021.

2.4.1 - Migrating from TrueNAS CORE

This article provides instructions on migrating from TrueNAS CORE to SCALE. Migration methods include using an ISO file or a manual update file.

Migration Notes

> Migrating TrueNAS from CORE to SCALE is a one-way operation. Attempting to activate or roll back to a CORE boot environment can break the system. You cannot upgrade CORE systems with High Availability enabled (HA) to SCALE HA.

TrueNAS systems on 12.0x or lower should update to the latest CORE 13.0 release (e.g 13.0-U2) prior to migrating to SCALE.

TrueNAS SCALE is Linux based, so it does not support FreeBSD GELI encryption. If you have GELI-encrypted pools on your system that you plan to import into SCALE, you must migrate your data from the GELI pool to a non-GELI encrypted pool *before* migrating to SCALE.

TrueNAS SCALE validates the system certificates when a CORE system migrates to SCALE. When a malformed certificate is found, SCALE generates a new self-signed certificate to ensure system accessibility.

Migration Methods

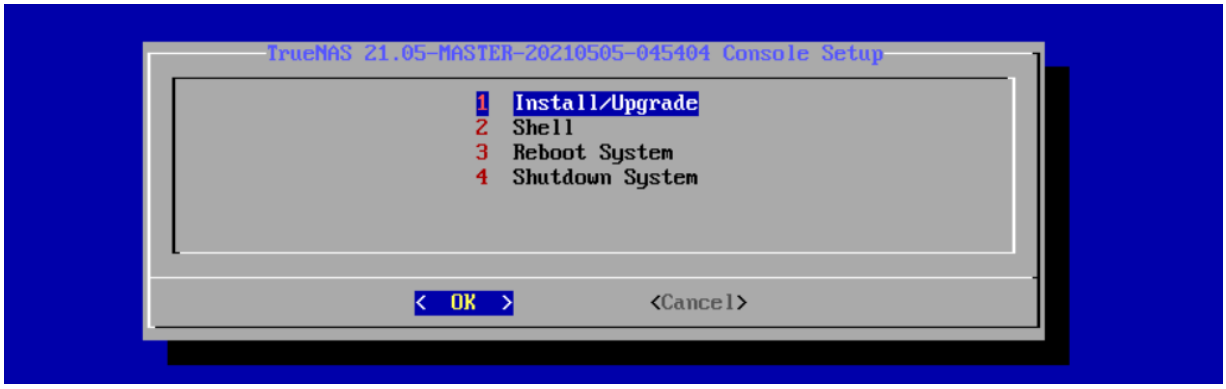
You can migrate from CORE to SCALE using an iso file or a manual update file.

ISO File Method

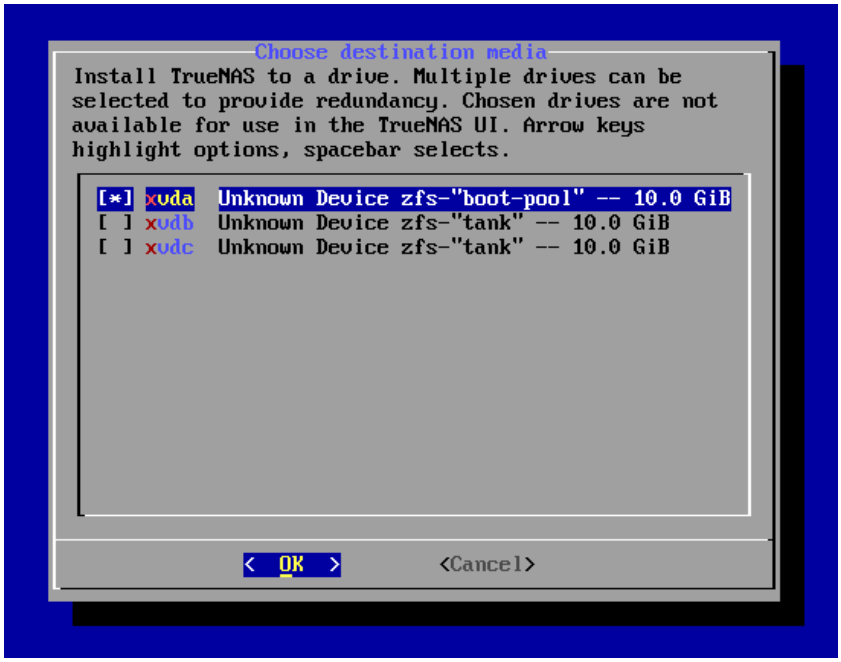
Start by saving the SCALE ISO file to a USB drive (see the **Physical Hardware tab** in Installing SCALE). Plug the USB drive into the CORE system that you want to sidegrade and boot or reboot the system.

At the motherboard splash screen, use the hotkey defined by your motherboard manufacturer to select a boot device, then select the USB drive with the SCALE .iso.

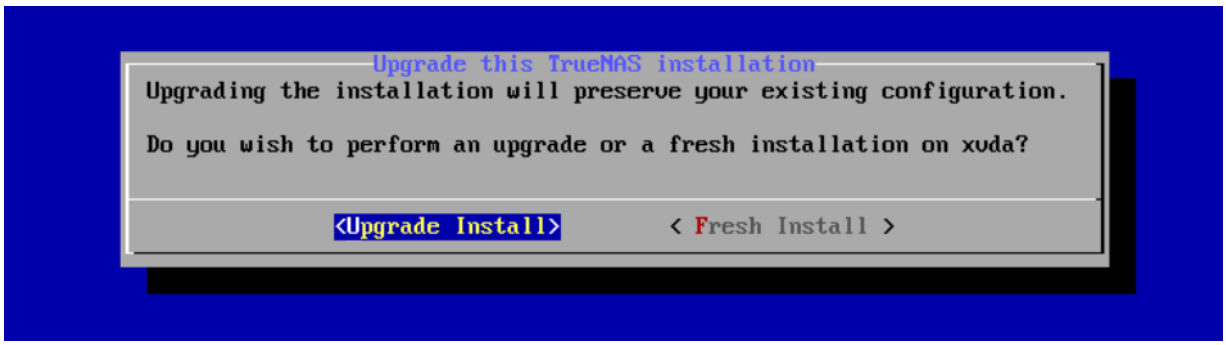
When the SCALE console setup screen appears, select **Install/Upgrade**.

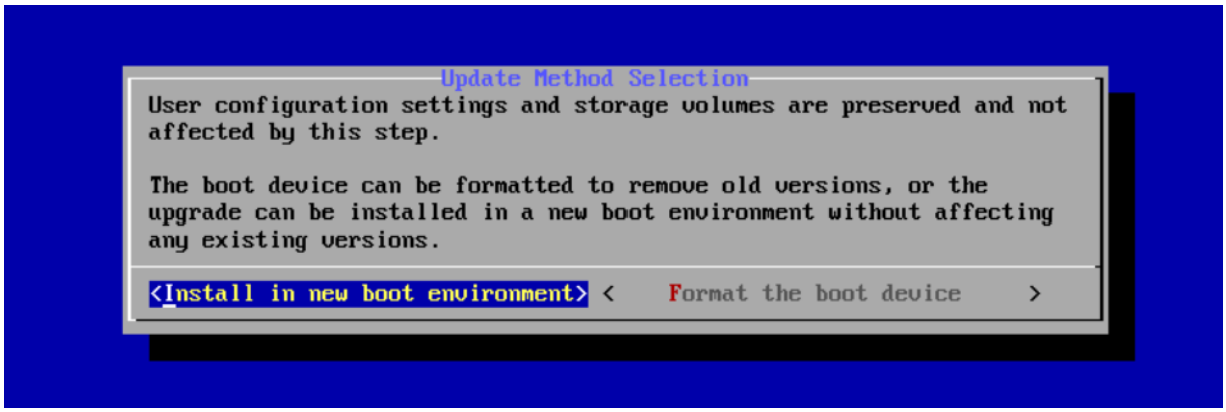


Select your TrueNAS boot disk



The installer asks if you want to preserve your existing configuration or start with a fresh installation. We recommend selecting **Upgrade Install** when migrating from CORE to SCALE to keep your configuration data. Then select **Install in new boot environment**.





> Although TrueNAS attempts to keep most of your CORE configuration data when upgrading to SCALE, some CORE-specific items do not transfer. GELI encrypted pools, NIS data, jails, tunables, and boot environments do not migrate from CORE to SCALE. VM storage and its basic configuration is transferred over during a migration. You need to double-check the VM configuration and the network interface settings specifically before starting the VM. AFP shares also do not transfer, but you can migrate them into an SMB share with AFP compatibility enabled. Init/shutdown scripts transfer, but can break. Review them before use. The CORE netcli utility is also swapped for a new CLI utility to use for the Console Setup Menu and other commands issued in a CLI.

After choosing to install in new boot environment, the installer warns that SCALE installs into the boot pool previously used for CORE. Select **Yes**.

Once the installation completes, reboot the system and remove the USB with the SCALE .iso file.

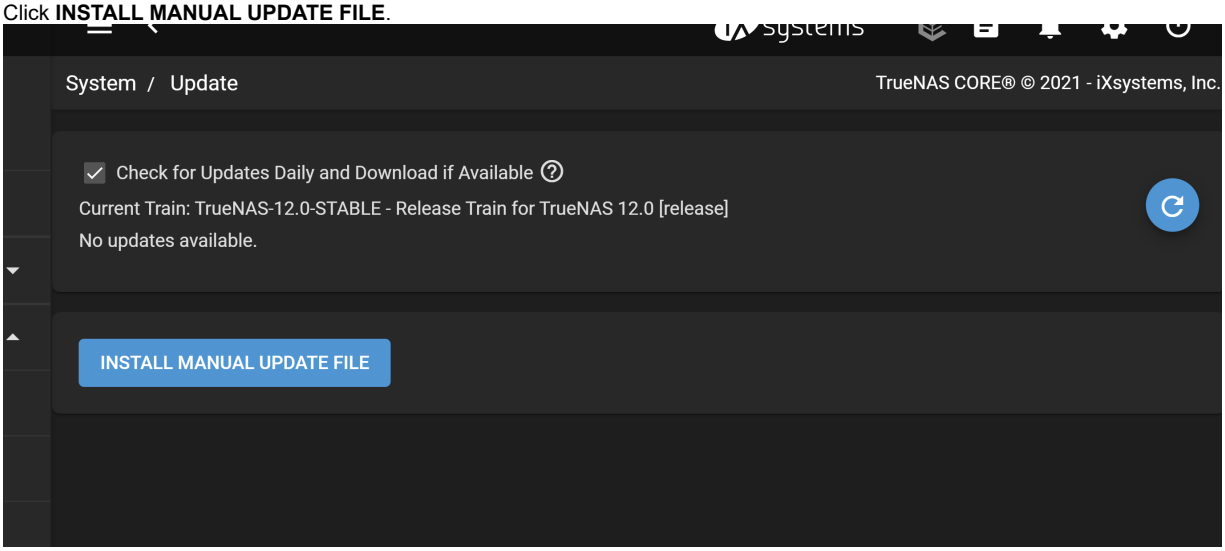
When TrueNAS SCALE boots, you might need to use the Shell to configure networking interfaces to enable GUI accessibility.

Manual Update File Method

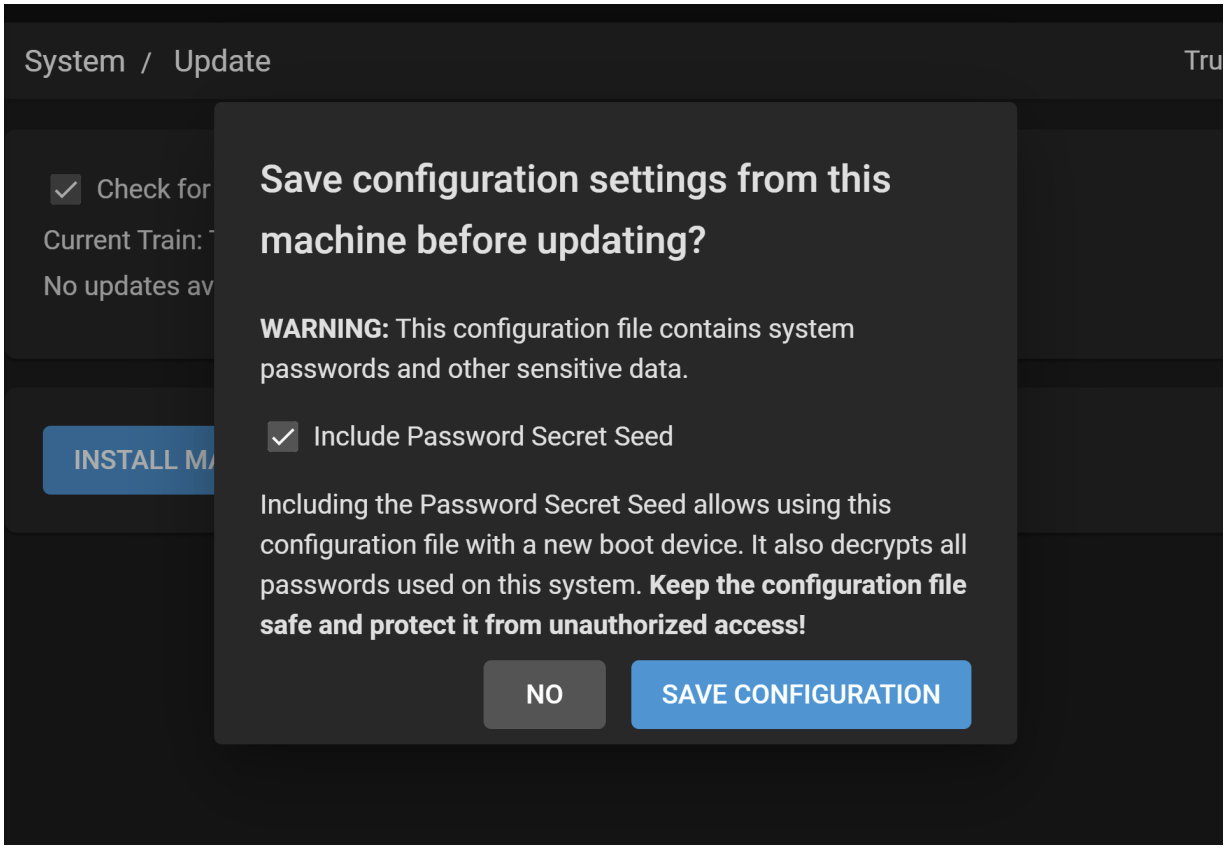
Start by downloading the SCALE manual update file. Confirm that the TrueNAS system is on the latest public release, 13.0-U2 or better.

Click **CHECK FOR UPDATES** in the **System Information** card on the **Dashboard** or go to **System > Update**.

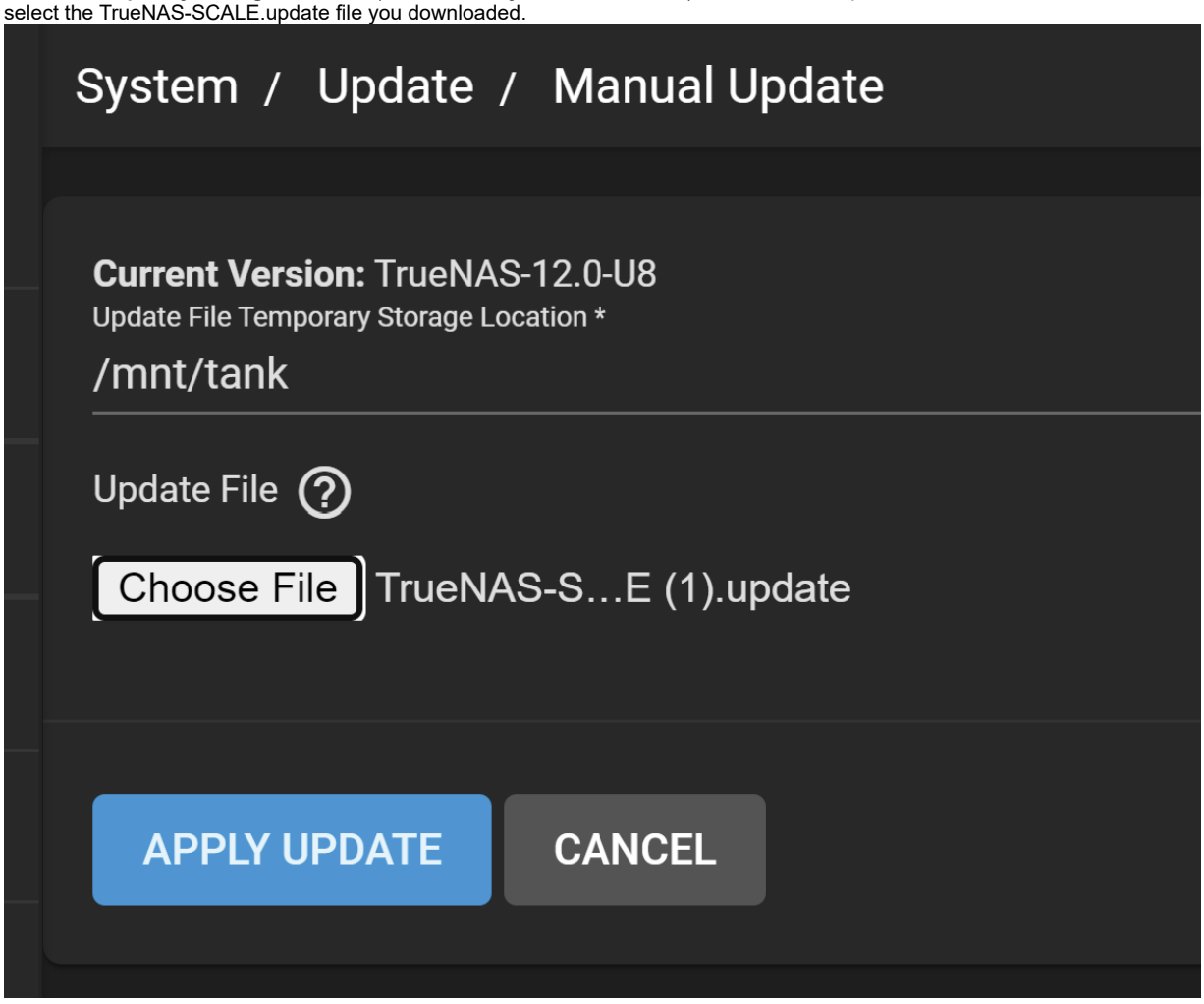
Click **INSTALL MANUAL UPDATE FILE**.



Click **SAVE CONFIGURATION** to download a backup file that can restore the system configuration in the event something goes wrong with the migration. This is recommended but it not required.

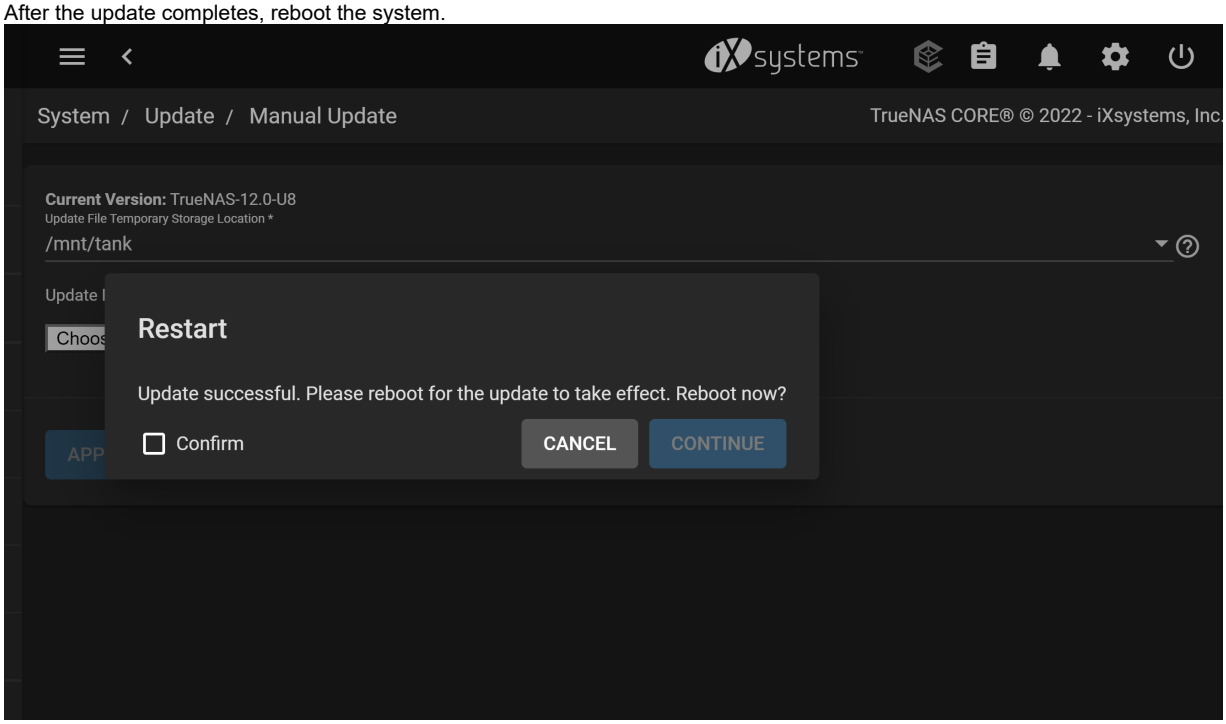


Select a **Temporary Storage Location** (either **Memory Device** or a **Pool**) for the manual update file. Click **Choose File** and select the TrueNAS-SCALE.update file you downloaded.



Then click **APPLY UPDATE**.

After the update completes, reboot the system.



Parallel SCALE CLI Commands

The following CLI commands are available after migrating from CORE to SCALE. The CORE equivalent CLI commands are for reference. These commands are for diagnostic use. Making configuration changes using the SCALE OS CLI is not recommended.

CORE CLI Comand	SCALE CLI Command	Description
camcontrol devlist	lshw -class disk -short sfdisk -l	Use `lshw -class disk -short sfdisk -l` to get detailed information on hardware (disk) configuration that includes memory, mainboard and cache cofiguration, firmware version, CPU version and speed.
geom disk list	lsblk, hdparm	Use `lsblk` to lists block devices or `hwparm` to get or set SATA/IDE device parameters.
glabel status	blkid	Use `blkid` to locate or print block device attributes.
gstat -pods	iostat iostat -dtx	Use `iostat -dtx` to display the device utiilization report with the time for each report displayed and includes extended statistics.
ifconfig ifconfig -l	ip addr ifconfig -s lshw -class network -short ethtool *devname*	Use `ip addr` to show or manipulate routing, devices, or policy routing and tunnels. Use `ifconfig -s` cofigure a network interface. Use `lshw -class network -short` to display a network device tree showing hardware paths. Use `ethtool *devnam*` to query or control network driver and hardware settings.
netstat -i	ifstat -i	Use `ifstat -i` to get interface statisitcs on a list of interfaces to monitor.
nvmecontrol devlist	nvme list	Use `nvme list` to identify the list of NVMe devices on your system.
pmcstat	profile-bpfcc	Use `profile-bpfcc` to get a CPU usage profile obtaine by sampling stack traces.
systat -ifstat	iftop netstat	Use `iftop` to display interface bandwidth usage by host and `netstat` to print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.
top -SHIzP	top -Hi	Use `top -Hi` to display Linux tasks for all individual threads and starts with the last remembered *i* state reversed.
vmstat -P	sar -P ALL	Use `sar -P ALL` to get reports with statistics for each individual processor and global statistics among all processors.

Related Content

- Migrating to TrueNAS
- Component Naming
- AFP Migration
- ZFS Feature Flags Removed
- Importing Storage Pools

- First Time Login
- Setting Up Data Sharing
- Backing Up TrueNAS

Related Installation Articles

- Adding Network Settings
- Installing SCALE
- Console Setup Menu Configuration
- Setting Up Storage
- Creating Storage Pools
- Importing Storage Pools
- First Time Login
- Setting Up Data Sharing
- Backing Up TrueNAS

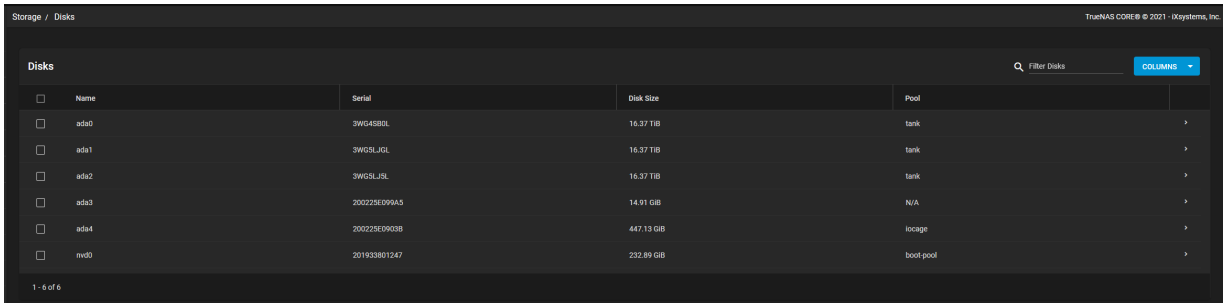
2.4.2 - Component Naming

This article provides information on disk and interface naming changes related to the change from FreeBSD storage and sharing in CORE to Linux in TrueNAS SCALE.

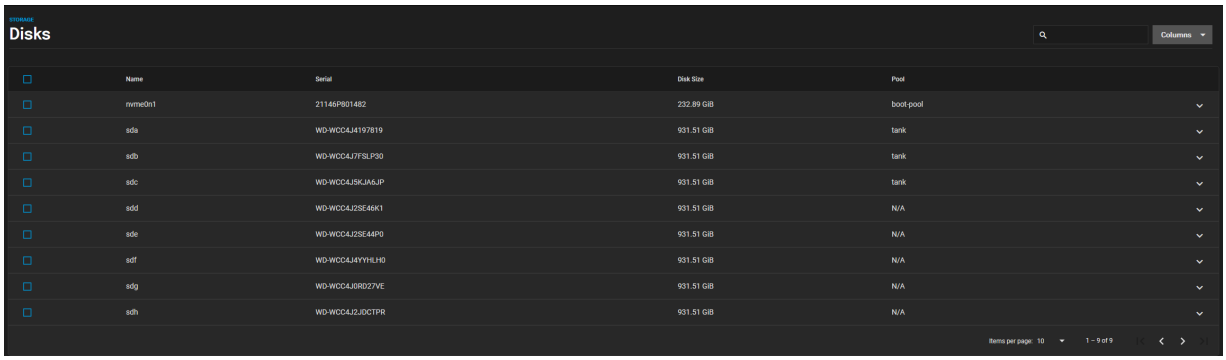
TrueNAS SCALE incorporates all the major TrueNAS CORE storage and sharing features with a web interface based on Debian GNU/Linux. Because SCALE shares the same UI as the FreeBSD-based TrueNAS CORE, users might notice there are similarities. However, SCALE does incorporate some differences, primarily in component naming.

Disks

TrueNAS Core utilizes a numerical listing of drives in a system.



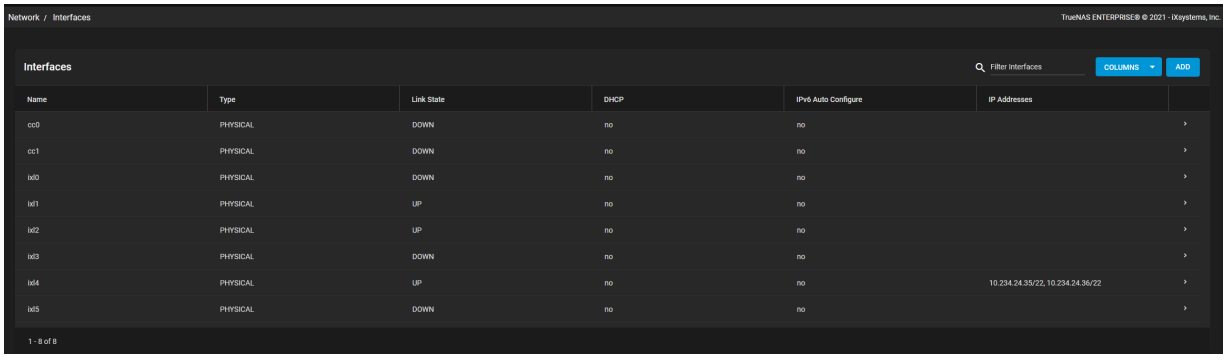
TrueNAS SCALE uses a lettered format for drive identification.



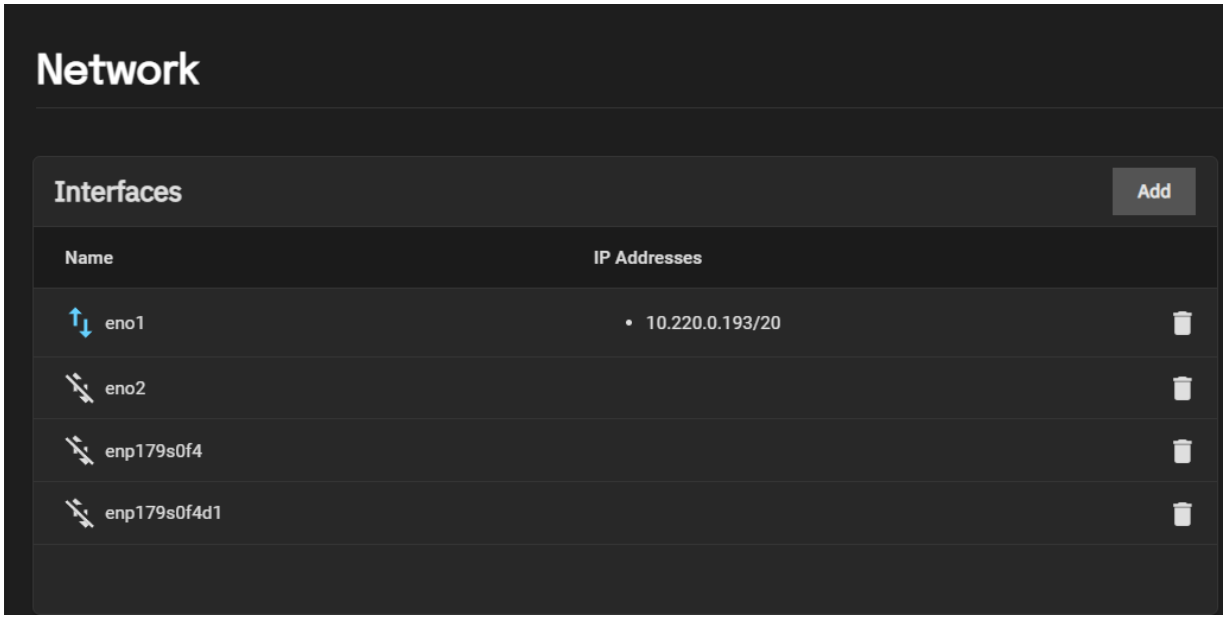
> SCALE still labels NVMe drives with a numeric value.

Interfaces

TrueNAS CORE utilizes driver information and enumeration to assign an interface name.



TrueNAS SCALE uses PCI location to assign an interface name.



See the TrueNAS Systems section for lists of the default port names for each platform.

Related Content

2.4.3 - ZFS Feature Flags Removed

This article provides information on the removal of the ZFS feature flag merged into OpenZFS in June 29, 2021.

Early testers of TrueNAS SCALE are advised:

On June 29, 2021, a new feature was merged into the TrueNAS fork of OpenZFS[1] for developers to test and integrate with other parts of the system. This feature included a new pool feature flag to signify an on-disk format change to how xattr names are encoded on Linux. This original version of the feature was easily activated by a default pool configuration. We quickly decided that the default configuration should not activate this feature until it is available in upstream OpenZFS, and on July 15 we merged changes[2] which make the defaults prevent activation of the new feature.

[1]: https://github.com/truenas/zfs/pull/8
[2]: https://github.com/truenas/zfs/pull/16

The new feature fixes a long standing issue in ZFS on Linux, which had from its start encoded xattr names in a way that is incompatible with ZFS implementations for every other platform. As one of the planned features of TrueNAS SCALE is the easy migration of pools from TrueNAS CORE, we have been developing this and other missing features to improve feature parity and compatibility across all platforms in OpenZFS. A pull request[3] for the xattr compatibility feature was opened with a request for comments in OpenZFS on April 20, 2021.

[3]: https://github.com/openzfs/zfs/pull/11919

On October 6, 2021, we received feedback that the feature flag will not be needed, as a bump to the ZFS POSIX Layer version number should be sufficient. As a result, we have removed the feature flag in question from TrueNAS SCALE to prevent the feature from being enabled moving forward in the release cycle. This is an unfortunate time to receive this insight, as nightly and now beta users of SCALE will have pools created or upgrade with this flag. The impact for most users is negligible, as the pool is still fully operational with the feature flag enabled, as long as it is not active. These users will merely see the unsupported feature is present but inactive:

```
root@truenas[~]# zpool status storage
  pool: storage
 state: ONLINE
  scan: resilvered 860K in 00:00:00 with 0 errors on Mon Oct  4 10:54:52 2021
config:

        NAME                                      STATE     READ WRITE CKSUM
        storage                                   ONLINE       0     0     0
          raidz2-0                                ONLINE       0     0     0
            99bfba03-cf73-44d4-8418-71b770be1a88  ONLINE       0     0     0
            5c219c07-b29f-45fd-84e8-8e0438dc91c6  ONLINE       0     0     0
            93e7106c-b988-45f4-8437-981b085bcbb2  ONLINE       0     0     0
            71de1ea8-5cab-45dd-aefb-1b19e24ed4b2  ONLINE       0     0     0
            7e75c4d0-c865-40ab-b927-cd13de92fbeb  ONLINE       0     0     0
            c601b128-65e7-4958-884b-235f739d9986  ONLINE       0     0     0

errors: No known data errors
root@truenas[~]# zpool get all storage | grep xattr_compat
storage  unsupported@com.ixsystems:xattr_compat  inactive                       local
root@truenas[~]#
```

Users who created or upgraded a pool using a TrueNAS SCALE build from between June 29 and July 15 2021 or who have manually set `xattr_compat=all` on a dataset and written an xattr will have activated the feature. Once activated, the feature cannot be deactivated until all datasets (including snapshots) that have ever utilized the feature (writing an xattr with `xattr_compat=all` on Linux) have been destroyed. This can be hard to determine, as there is currently no way of checking the feature activation status of a dataset. Most people who did unwittingly activate the feature will merely see the new default value of `xattr_compat=linux` when checking the property.

The feature was marked as read-only compatible, so pools with the feature active are able to be imported read-only on versions of ZFS that do not support the feature. Users are advised to check if their pool has the feature active, and if so, the pool must be backed up and recreated on a version of ZFS without the feature. Builds of SCALE as of October 9, 2021 have the feature removed.

This pool has `feature@xattr_compat` enabled but not active, and can continue to be used on newer versions of TrueNAS SCALE and other ZFS systems:

```
root@truenas[~]# zfs get feature@xattr_compat p0
NAME  PROPERTY             VALUE                SOURCE
p0    feature@xattr_compat  enabled              local
```

Changing the `xattr_compat` property and writing an xattr in the user namespace activates the feature, preventing the pool from being used on TrueNAS SCALE and other ZFS systems moving forward. The feature is only activated by writing an xattr in the user namespace with `xattr_compat=all` on Linux. Once activated, it stays active even if `xattr_compat=linux` is restored and the file removed:

```
root@truenas[~]# sudo zfs set xattr_compat=all p0
root@truenas[~]# zpool get feature@xattr_compat p0
NAME  PROPERTY              VALUE                 SOURCE
p0    feature@xattr_compat  enabled               local

root@truenas[~]# sudo touch /p0/somefile
root@truenas[~]# zpool get feature@xattr_compat p0
NAME  PROPERTY              VALUE                 SOURCE
p0    feature@xattr_compat  enabled               local

root@truenas[~]# sudo attr -s someattr -V someval /p0/somefile
Attribute "someattr" set to a 7 byte value for /p0/somefile:
someval

root@truenas[~]# zpool get feature@xattr_compat p0
NAME  PROPERTY              VALUE                 SOURCE
p0    feature@xattr_compat  active                local
root@truenas[~]# sudo zfs set xattr_compat=linux p0
root@truenas[~]# sudo rm /p0/somefile
root@truenas[~]# zpool get feature@xattr_compat p0
NAME  PROPERTY              VALUE                 SOURCE
p0    feature@xattr_compat  active                local
```

Creating a new pool with the feature explicitly disabled and replicating the desired datasets is one workaround if your pool has the feature active:

```
root@truenas[~]# sudo zpool create -o feature@xattr_compat=disabled p1 ~/d1
root@truenas[~]# zpool get all p1 | grep xattr_compat
p1    feature@xattr_compat          disabled                       local

root@truenas[~]# sudo zfs snap p0@snap
root@truenas[~]# sudo zfs send p0@snap | sudo zfs recv -F p1
root@truenas[~]# zpool get all p1 | grep xattr_compat
p1    feature@xattr_compat          disabled                       local
root@truenas[~]# zfs get xattr_compat p1
NAME  PROPERTY      VALUE         SOURCE
p1    xattr_compat  linux         default
```

Please keep in mind these are simplified, contrived examples. If you aren't sure of how to replicate your pool yourself, seek help on the TrueNAS forums.

After upgrade to 22.02-RC.1, the only visible artifact of the feature is that the unsupported flag is present in `zpool get all`:

```
root@truenas[~]# zpool get all storage | grep xattr_compat
storage unsupported@com.ixsystems:xattr_compat inactive         local
```

The unsupported feature will not presented by `zpool status`.

> It is not possible to disable the feature once it is enabled; however, having the feature in the enabled state, should not cause a problem. The problem arises when the feature is active. There is currently no practical way to tell which datasets or snapshots are keeping the feature active, so while destroying all traces of it should in theory return the feature from active back to enabled, in practice it is hard to know you won't have to end up destroying the whole pool anyway. For information on how to perform data protection procedures, please refer to the TrueNAS SCALE Data Protection documentation.

Related Content

2.5 - First Time Login

Now that you have installed and configured TrueNAS SCALE, you can log in to the web interface and begin managing data!

Can I configure TrueNAS SCALE using a CLI?

After installing TrueNAS, you can configure and use the system through the web interface.

> Important! Use only the web interface to make configuration changes to the system.

By default, using the command-line interface (CLI) to modify the system *does not* modify the settings database. The system reverts to the original database settings when it restarts and wipes any user-made command line changes. TrueNAS automatically creates several ways to access the web interface, but you might need to adjust the default settings for your network environment.

Web Interface Access

By default, fresh installs of TrueNAS SCALE provide a default address for logging in to the web interface. To view the web interface IP address or reconfigure web interface access, connect a monitor and keyboard to your TrueNAS system or connect with IPMI for out-of-band system management.

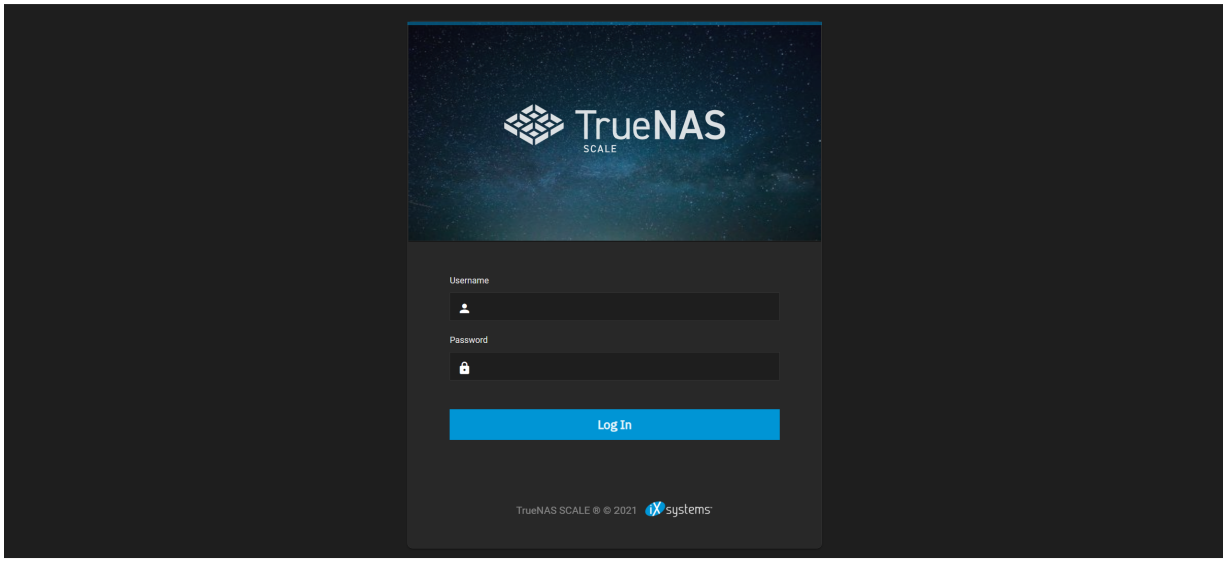
When powering on a TrueNAS system, the system attempts to connect to a DHCP server from all live interfaces to access the web UI. On networks that support Multicast Domain Name Services (mDNS), the system can use a host name and domain to access the TrueNAS web interface. By default, TrueNAS uses the host name and domain truenas.local. To change the host name and domain in the web interface, go to **Network** and click **Settings** in the **Global Configuration** card.

To access the web interface using an IP address, use the one that the Console Setup Menu generated after installing SCALE, or use the one you configured in the Post-install Configuration article if you upgraded from CORE.

Logging In

On a computer with access to the same network as the TrueNAS system, enter the host name and domain or IP address in a web browser to connect to the web interface.

> The quality of your user experience can be impacted by the browser that you use. We generally recommend using Firefox, Edge, or Chrome.



Use the administrative account credentials to log in. The default administrator username is `root` and the password is created when installing TrueNAS.

Troubleshooting

If the user interface is not accessible by IP address from a browser, check these things:

- If the browser configuration has proxy settings enabled, disable them and try connecting again.
- If the page does not load, ensure a `ping` reaches the TrueNAS system IP address. If the IP address is in a private range, you must access it from within that private network.

If the web interface displays but seems unresponsive or incomplete:

- Make sure the browser allows cookies, Javascript, and custom fonts from the TrueNAS system.
- Try a different browser. We recommend Firefox.

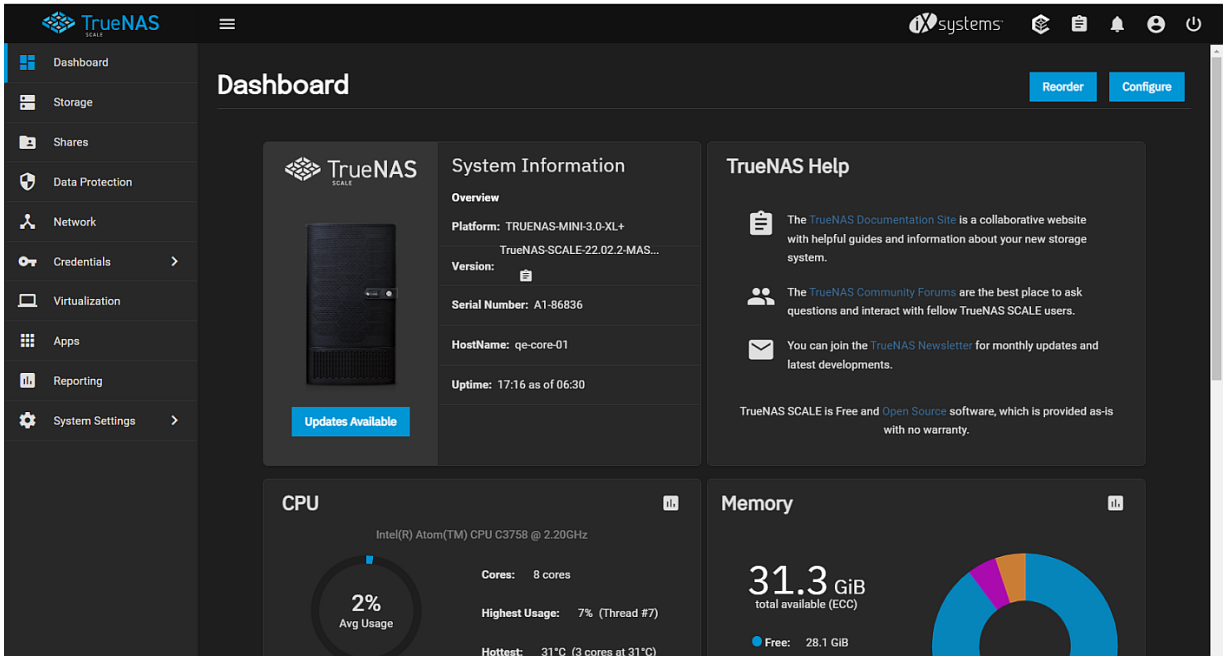
If the UI becomes unresponsive after an upgrade or other system operation, clear the site data and refresh the browser (`Shift+F5`).

If I cannot remember the administrator password to log in to the web interface, connect a keyboard and mouse to the TrueNAS system and open the console setup menu to reset the `root` account password.

Dashboard

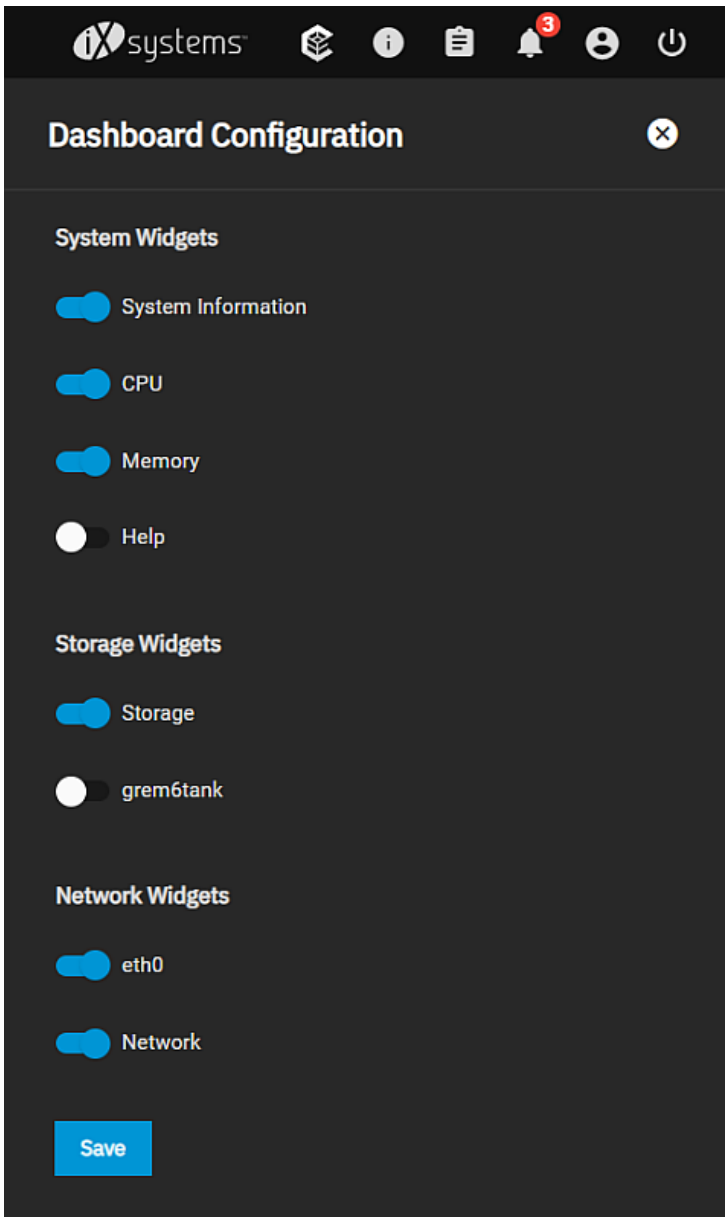
Dashboard Video Tutoral

After logging in, you see the system **Dashboard** screen. **Dashboard** displays basic information about the installed version, systems component usage, and network traffic. For users with compatible TrueNAS hardware, clicking the system image takes you to the **System Settings > Enclosure** page.



The **Dashboard** provides access to all TrueNAS management options. The top row has links to outside resources and buttons to control the system. The left-hand column lets users navigate to the various TrueNAS Configuration screens.

You can reorder dashboard widgets by clicking **Reorder** and then dragging them into your preferred order. You can also choose which widgets appear on the dashboard by clicking **Configure**.



Top Bar Menu

The icon buttons in the top toolbar menu link to the iXsystems site, display the status of TrueCommand and directory servers, and show system processes, and configuration menus. You can also collapse and expand the main function menu on the left side of the screen.

Top Toolbar Icons

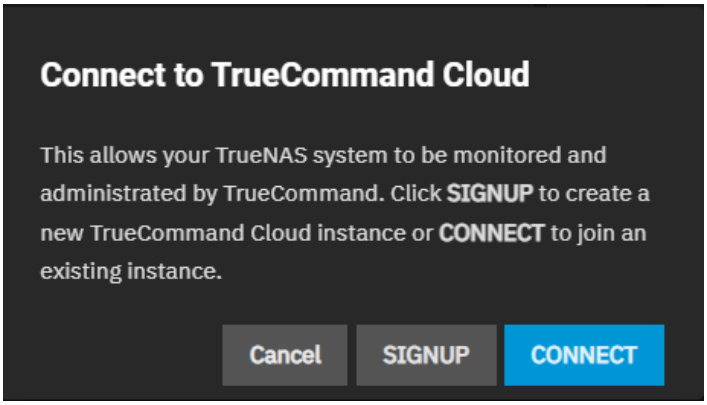
iXsystems

The iXsystems logo opens the iXsystems home page. There, users can find information about storage and server systems.

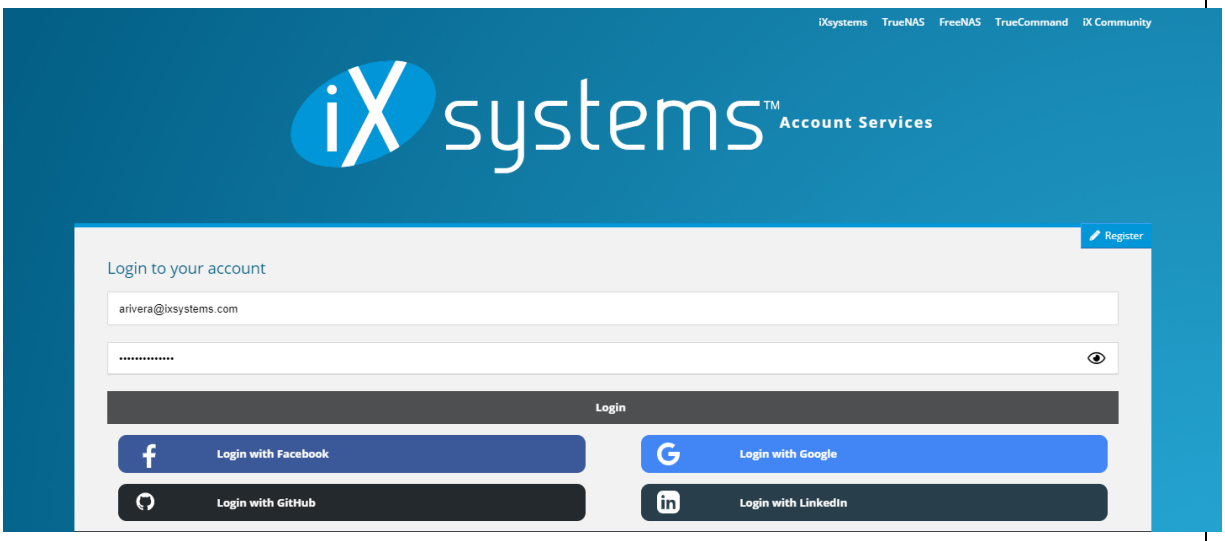
Users can also use the iXsystems home page to access their customer portal and community section for support.

Status of TrueCommand

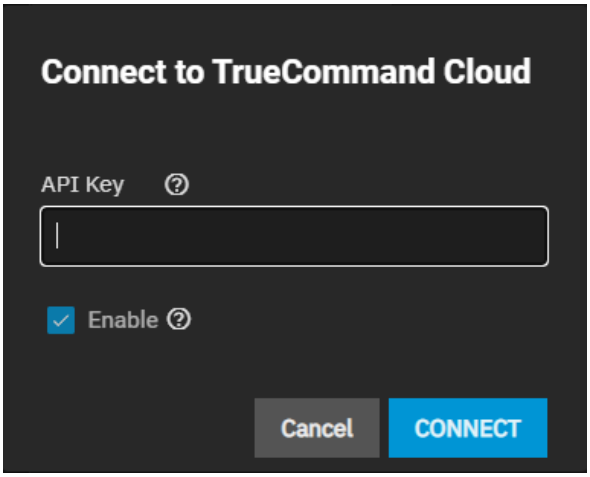
The **Status of TrueCommand** icon lets users sign up with and connect to TrueCommand Cloud.



Clicking **SIGNUP** opens the TrueCommand sign-up page in a new tab.



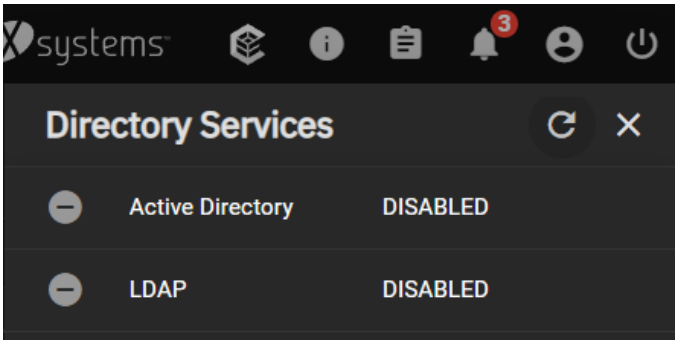
After users sign up, they can click the **CONNECT** button and enter their API key to connect SCALE to TrueCommand Cloud.



See Connecting TrueNAS for more information on configuring a TrueCommand cloud account and getting an API key.

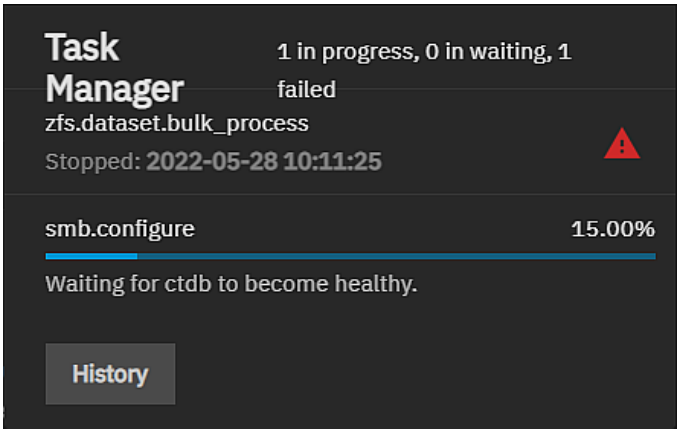
Directory Services Monitor

The **Directory Services Monitor** icon button displays the status of Active Directory and LDAP services. Clicking on either takes you to their respective configuration screens.



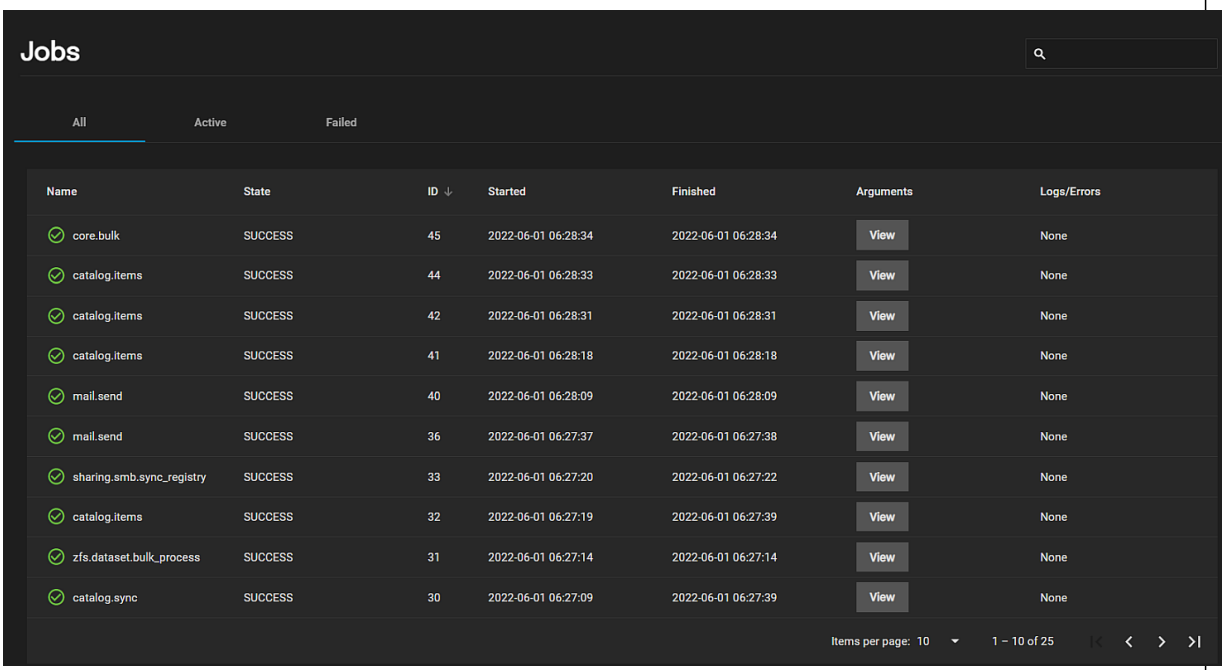
Task Manager

The **Task Manager** icon button displays all running and failed jobs/processes. Minimized jobs/processes can be accessed here.



Click on a running task to display the dialog window for that running task.

Click the **History** button to open the **Jobs** screen. **Jobs** lists all successful, active, and failed jobs. Users can also click **View Log** next to a failed process to view its log information and error message.

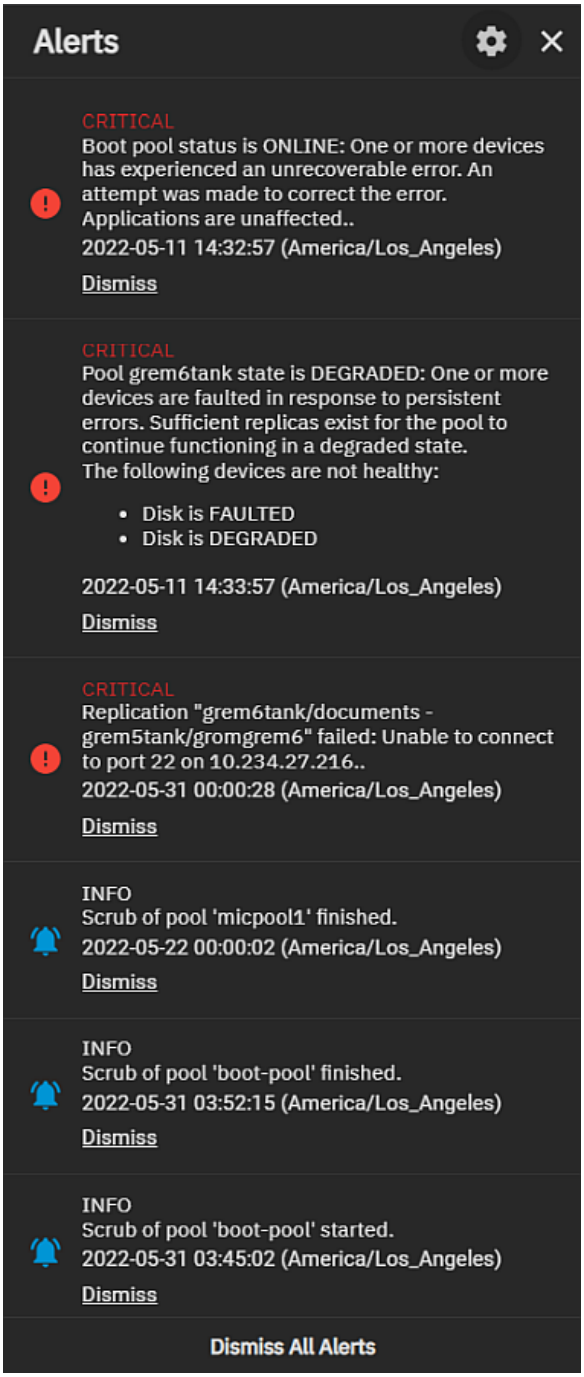


For more information see the **Jobs Screens** article.

Alerts

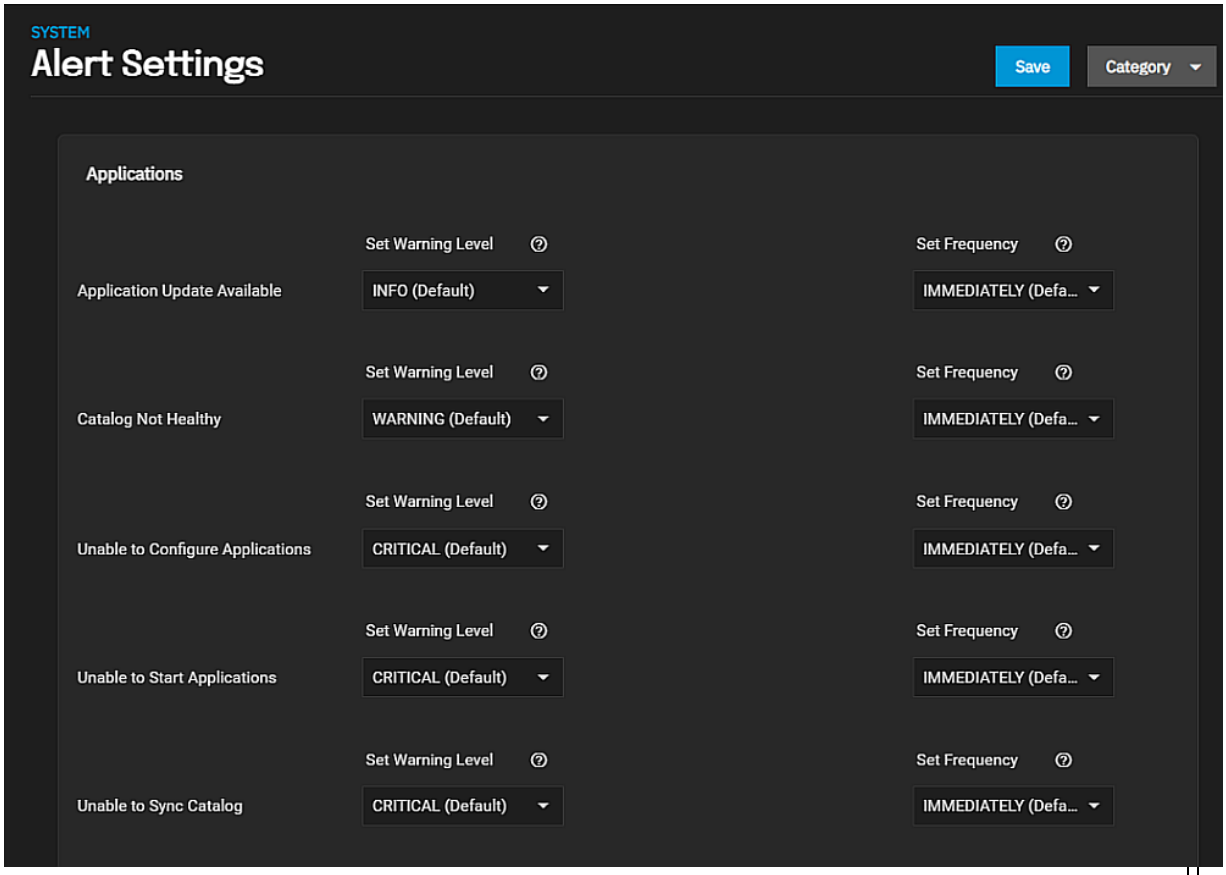
The **Alerts** icon button displays a list of current alerts for your TrueNAS system. Users can dismiss them one at a time or all at once.

It also provides an **Alerts** menu you access by clicking the icon. From this menu users can configure **Alert Settings**, **Alert Services**, and **Email**.



Alert Settings

The **Alert Settings** screen has options for setting the warning level and frequency for alerts specific to application actions.



Use the **Set Warning Level** dropdown list options to customize alert importance. Each warning level has an icon and color to express the level of urgency.

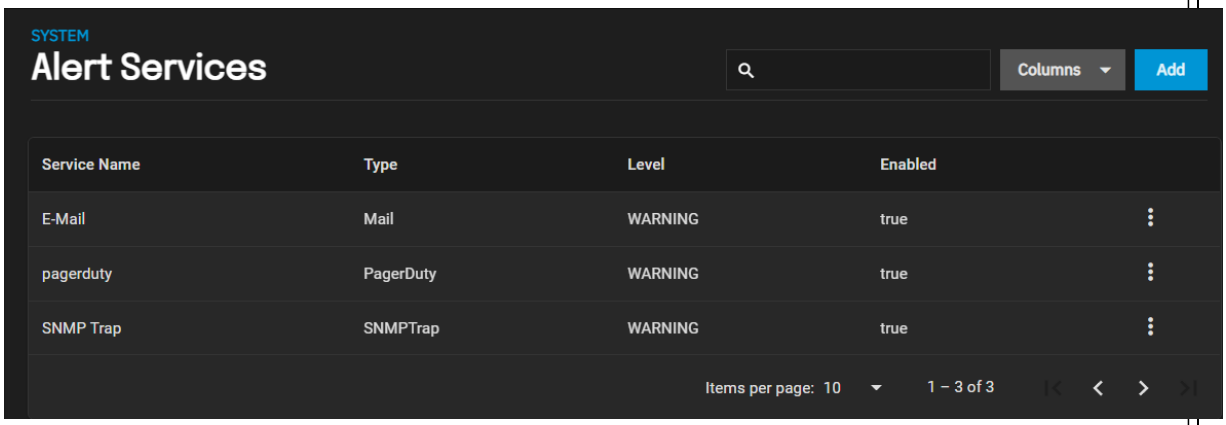
Use the **Set Frequency** dropdown list options adjust how often the system sends alert notifications. Setting the **Frequency** to **NEVER** prevents that alert from appearing in the **Alerts** list, but it still pops up in the UI if triggered.

Each warning level has a different icon and color to express its urgency. To make the system email you when alerts with a specific warning level trigger, set up an email alert service with that warning level.

See Alert Settings Screen for more information on settings.

Alert Services

The **Alert Services** screen has options to create and edit alert services. It also displays existing services in a list that users can filter by **Type**, **Level**, and **Enabled**.



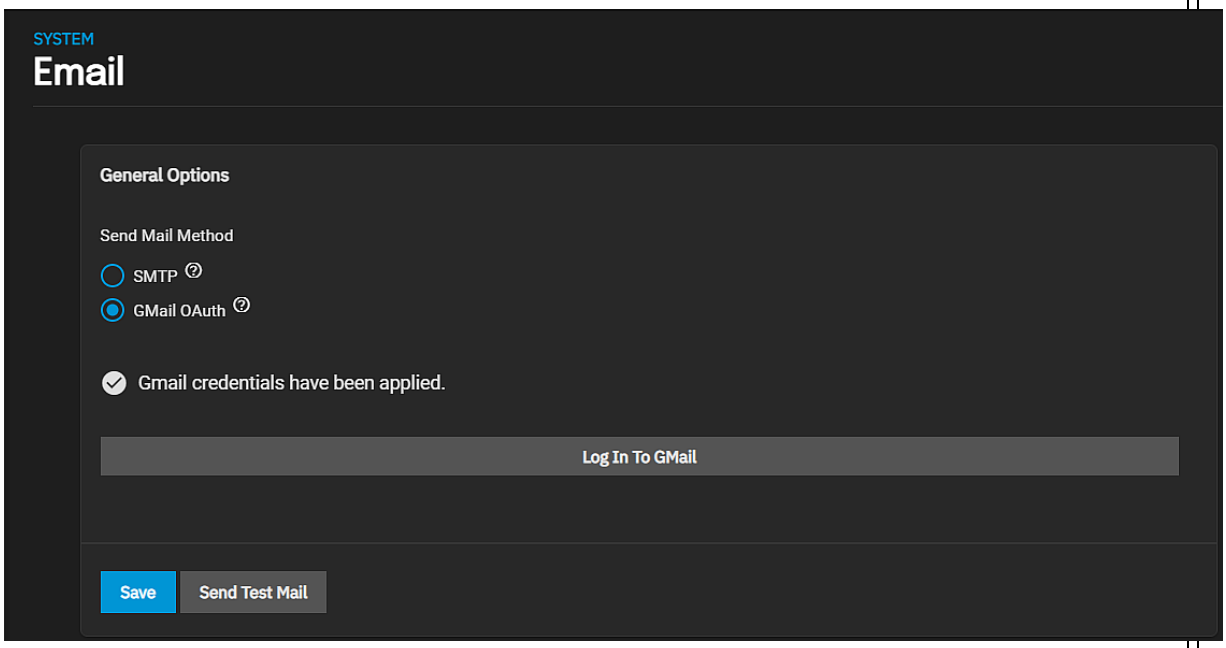
To create a new alert service, click **Add** and fill out the form, then click **Save**.

Click **SEND TEST ALERT** to generate a test alert to confirm the alert service works.

See Alert Services Screen for more information on settings.

Email

The **Email** screen lets you set up a system email address.



Click on **Send Test Mail** to generate a test email to confirm the system email works.

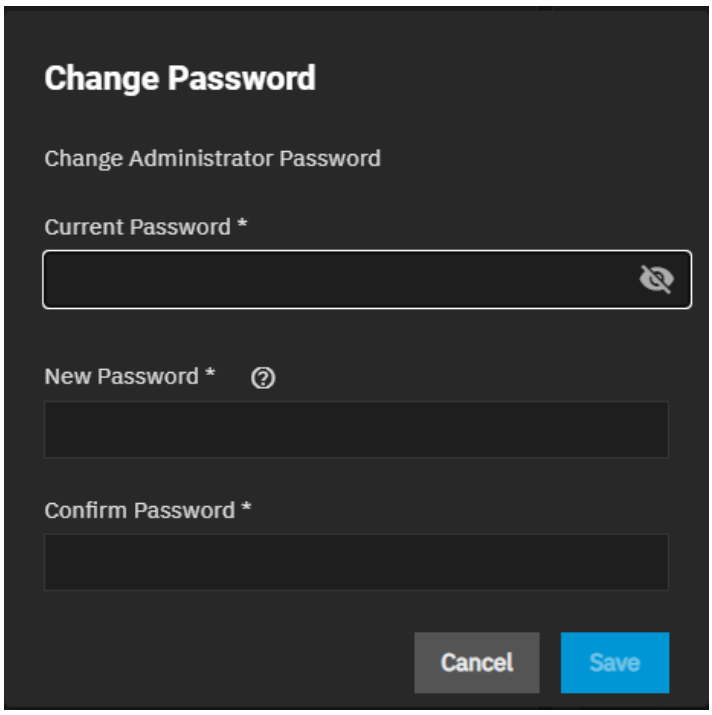
See Email Screens for information on email settings.

Settings

The **Settings** icon button has options for passwords, web interface preferences, API Keys, and TrueNAS information.

Change Password

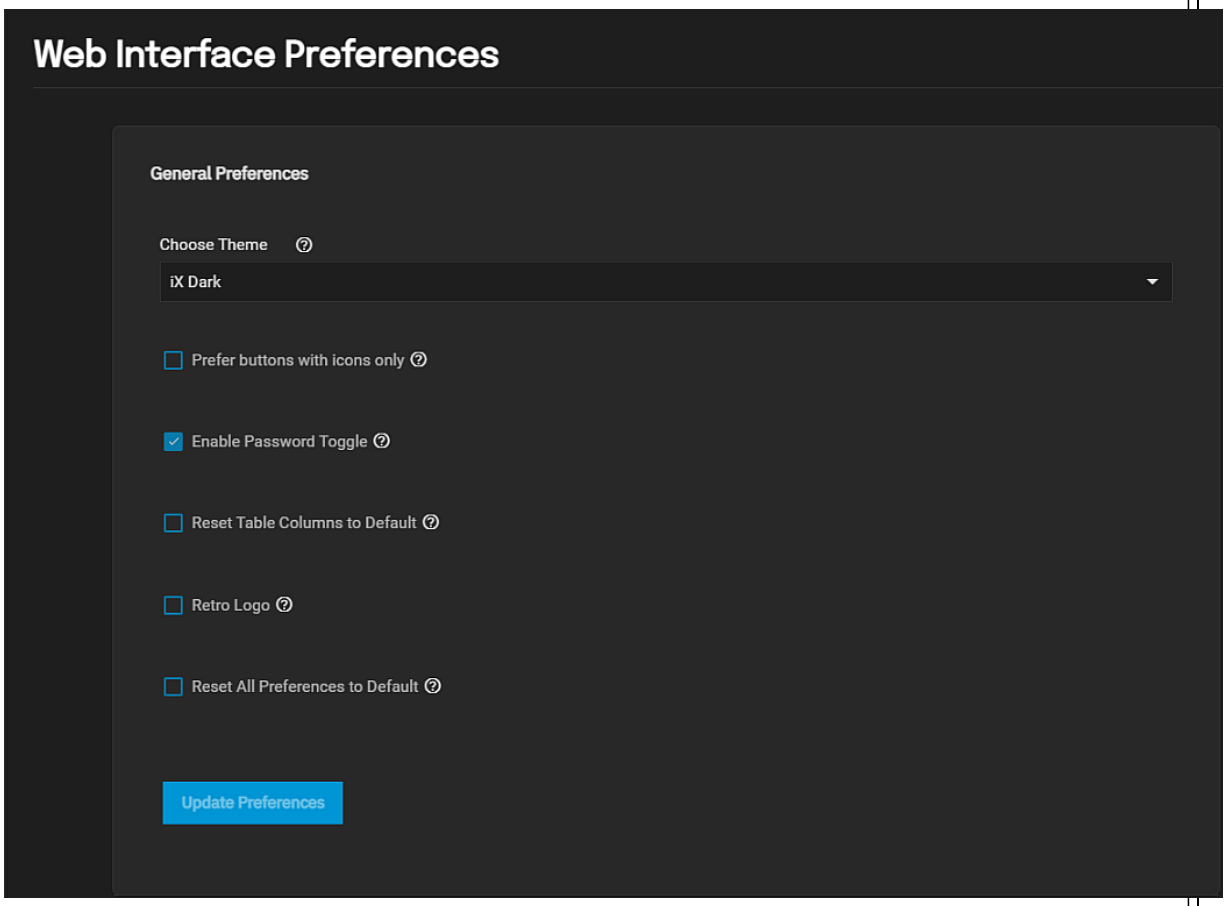
Click on the **Change Password** icon button to display the change password dialog where you can change the currently logged-in user password.



Click on the icon to display the password entered. To stop displaying the password, click on the icon.

Preferences

Click on **Preferences** to select general preferences for the system that include changing the display color theme and other display options.



See Web Interface Preferences Screen for more information on settings.

API Keys

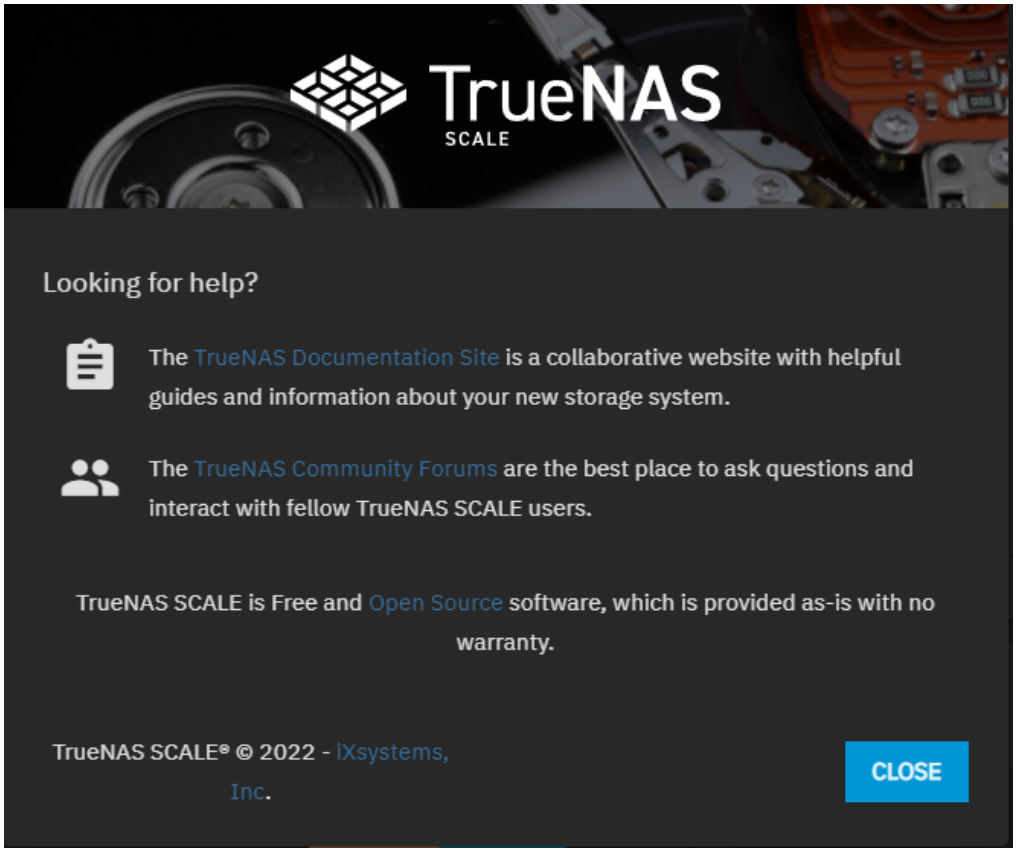
Click on **API Keys** to add API keys that identify outside resources and applications without a principal. Users can also click **DOCS** to access their system API documentation.

See API Keys for more information on adding or managing API keys.

Guide and About

Click on **Guide** to open the TrueNAS Documentation Hub in a new tab.

Click on **About** to display the information window with links to the TrueNAS Documentation Hub, TrueNAS Community Forums, FreeNAS Open Source Storage Appliance GitHub repository, and iXsystems home page.



Power Options

Click the **Power** icon button to either log out of, restart, or shut down the system.

Storing Data

Now that you can access the TrueNAS web interface and see all the management options, you can begin storing data!

Related Installation Articles

- Adding Network Settings
- Installing SCALE
- Console Setup Menu Configuration
- Migrating from TrueNAS CORE
- Setting Up Storage
- Creating Storage Pools
- Importing Storage Pools
- Setting Up Data Sharing
- Backing Up TrueNAS

Related Migration Articles

- Migrating to TrueNAS
- Migrating from TrueNAS CORE
- Component Naming
- AFP Migration
- ZFS Feature Flags Removed
- Importing Storage Pools
- Setting Up Data Sharing
- Backing Up TrueNAS

2.6 - Preparing for Clustering

Initial setup procedures to prepare a system for clustering

One unique capability of TrueNAS SCALE is ability to cluster groups of systems together. These clusters can then create new volumes within the existing SCALE storage pools. Data stored in a clustered volume is shared between the clustered systems and can add additional redundancy or performance to the environment. Currently, data stored in a clustered volume is shareable using Active Directory (AD) and the SMB protocol.

> Clustering is considered experimental and should not be used in a production environment or for handling critical data!

Warnings and Restrictions

Clustering is a back-end feature in TrueNAS SCALE and should only be configured using the TrueCommand web interface. Attempting to configure or manage clustering from within the TrueNAS SCALE UI or Shell can result in cluster failures and permanent data loss.

Using the clustering feature on a SCALE system adds some restrictions to that system:

- Any existing non-clustered SMB shares present no longer function.
- New SMB shares cannot be created separately from the clustering settings.
- When added, the system cannot be added to a different cluster.
- Removing single systems from one cluster and migrating to another is currently unsupported. Removing a system from a cluster requires deleting the entire cluster.

Requirements

To set up clustering with TrueNAS SCALE, you need:

- 3-20 TrueNAS SCALE systems (version 22.02.2 or later) on the same network. Each SCALE system must have:
  - Two network interfaces and subnets. The primary network interface and subnet is used for client access to the SCALE system The secondary interface and subnet is dedicated for cluster traffic. This interface must use static IP addresses.
  - Disks available or Storage pools already created and available for use.
- A TrueCommand 2.2 or later environment that is on the same network as the SCALE systems.
- A Microsoft Active Directory environment must be available and connected to the same network as the SCALE systems and TrueCommand environment. Reverse DNS must be configured to allow the SCALE cluster systems to communicate back and forth with the AD environment.

Setting up the Environment

TrueNAS SCALE Systems

Follow this procedure for each TrueNAS SCALE system that is to be connected to TrueCommand and used in the cluster.

1. Log in to the SCALE UI and go the the **Storage** page. Ensure a storage pool is available for use in the cluster. If not, click **Create Pool** and make a new pool using any of the available disks.

2. Go to the **Network** page and look at the **Interfaces** card. a. Ensure two interfaces are available and note which is the primary interface that allows SCALE web interface access and access between SCALE systems, TrueCommand, and Active Directory environments. This allows connecting the SCALE systems to Active Directory and using TrueCommand to create and manage the cluster. b. Ensure the second interface is configured with a static IP address on a different network/subnet that connects all the SCALE systems. This interface securely handles all the data sharing traffic between the clustered systems.

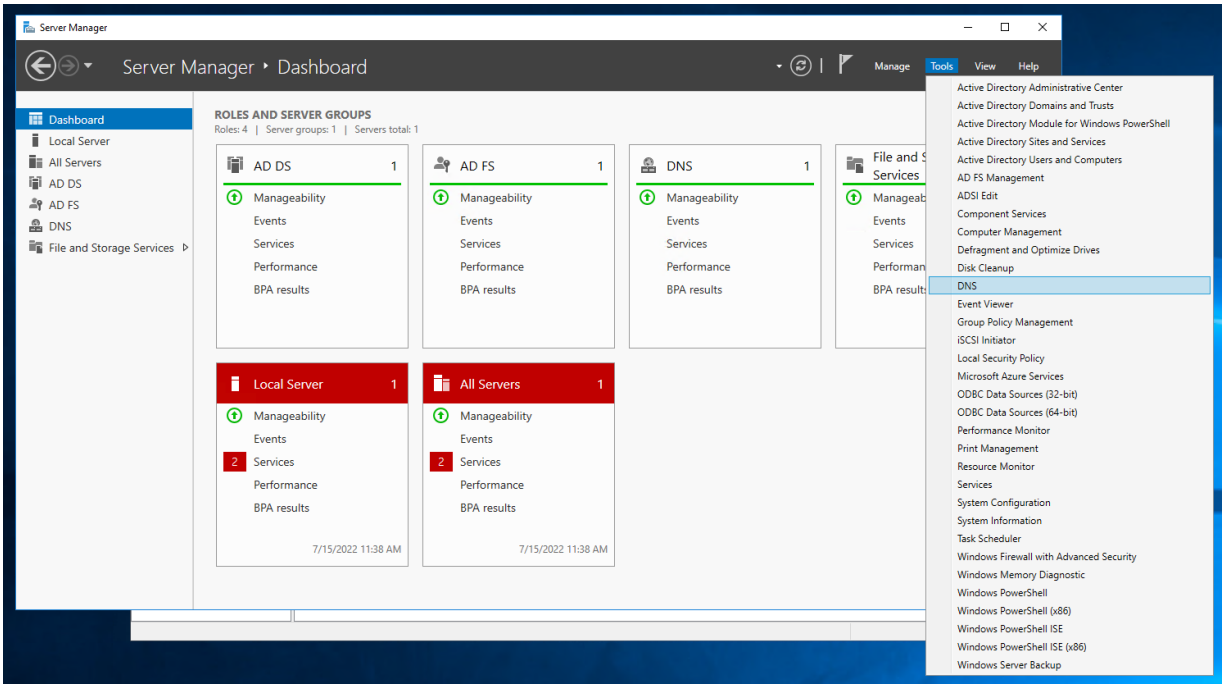
3. Go to the **Shares** page and look at the **Windows (SMB) Shares** section. Note if there are any critical shares and take steps to ensure that disabling those shares isn't disruptive.

Repeat this procedure for each SCALE system to be clustered.

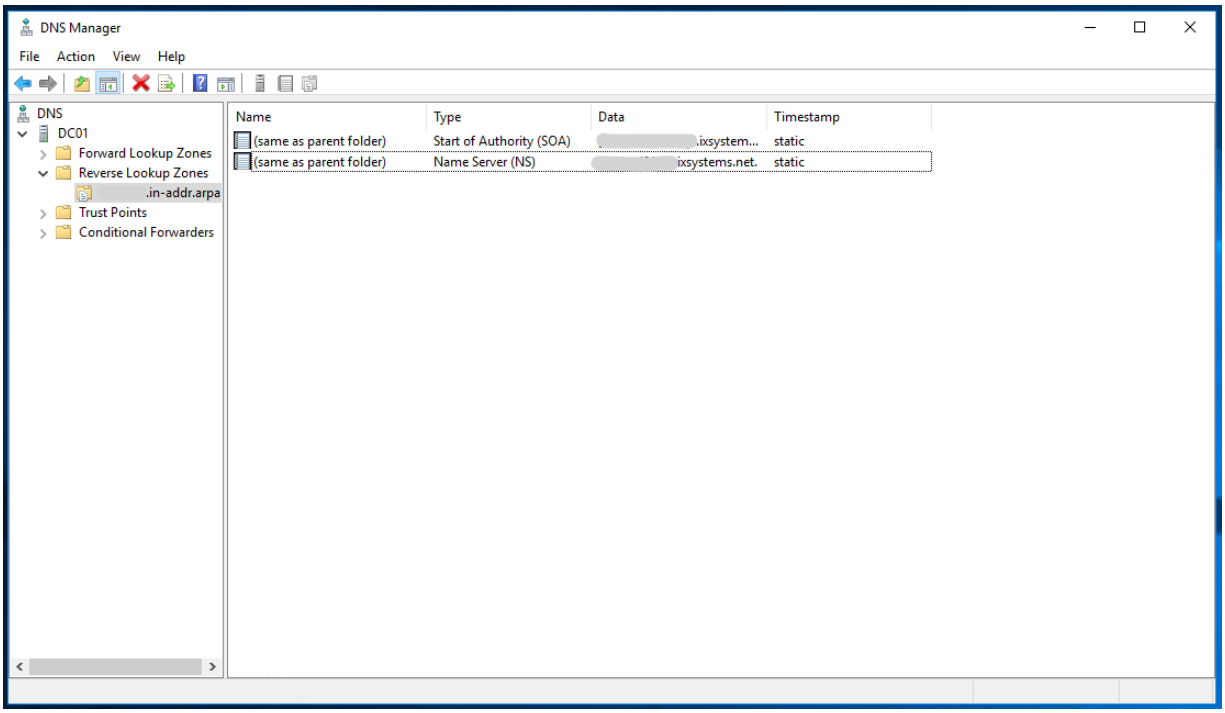
Microsoft Active Directory

1. Verify that the Active Directory (AD) environment to pair with the cluster is available and administratively accessible on the same network as the TrueCommand and TrueNAS SCALE systems.

2. Log in to the Windows Server system and open the **Server Manager**. Click **Tools** > **DNS** to open the **DNS Manager**.

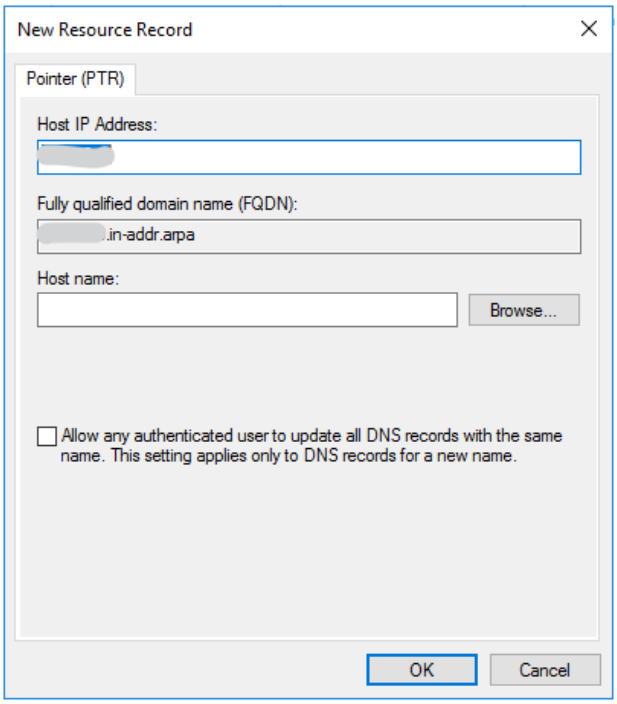


3. In the left side menu, expand **Reverse Lookup Zones** and select the **Active Directory-Integrated Primary** zone to use for the cluster.

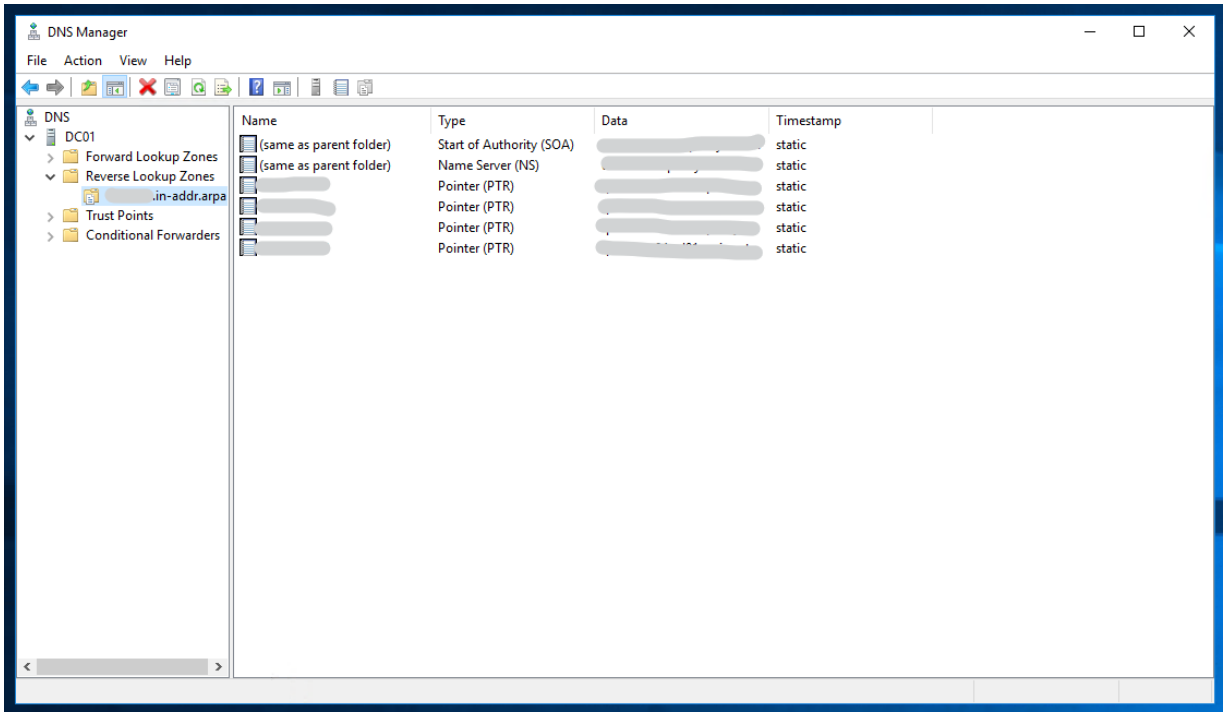


If no zone exists, see Microsoft's guide for creating DNS Zones.

4. Click **Action** > **New Pointer (PTR…)** and configure the **New Resource Record**. Enter the SCALE system IP address, host name, and click **OK**.



Repeat this process for each system intended for clustering. The new records appear inside the zone as they are saved.



TrueCommand Container

1. If not already completed, deploy TrueCommand 2.2 or later in a Docker container. The system used for the TrueCommand container cannot be any of the TrueNAS SCALE systems intended for the cluster.
2. In a browser, enter the TrueCommand IP address and create the first user. Log in with these user credentials to see the **Dashboard**.
3. Click **New System** and add the credentials for the first SCALE system. Use the SCALE **root** account password. When ready, click **ADD AND CONTINUE** and repeat the process for each SCALE system intended for the cluster. When complete, each SCALE system has a card on the TrueCommand **Dashboard** and is actively displaying system statistics.

> A good practice is to backup the SCALE system configuration before creating the cluster. In the TrueCommand **Dashboard**, click on the name of a connected system. This opens a detailed view of that system. Click **Config Backups** and **CREATE BACKUP** to store the SCALE configuration file with TrueCommand. This allows quickly restoring the system configuration to the initial working state, should something go wrong.

See Also

- Clustering and Sharing SCALE Volumes with TrueCommand
- Clusters Screen
- Network Screen

3 - SCALE Tutorials

Welcome to TrueNAS tutorials!

This guide collects various how-tos for both simple and complex tasks using primarily the TrueNAS web interface. It is loosely organized by topic and is continuously being updated with new or replacement tutorials.

To display all tutorials in a linear HTML format, export it to PDF, or physically print it, please select **Download or Print**.

If you are interested in writing a TrueNAS tutorial, see the Contributing section for some guidance!

Table of Contents (click to expand)

- Using the TrueNAS CLI Shell
- Community Tutorials
  - Hardened Backup Repository for Veeam
  - Spotlight Support on a SCALE SMB Share

SCALE Documentation Sections

TrueNAS SCALE documentation is divided into several sections or books:

- The Getting Started Guide provides the first steps for your experience with TrueNAS SCALE:
  - Software Licensing information.
  - Recommendations and considerations when selecting hardware.
  - Installation tutorials.
  - First-time software configuration instructions.
- Configuration Tutorials have many community and iXsystems -provided procedural how-tos for specific software use-cases.
- The UI Reference Guide describes each section of the SCALE web interface, including descriptions for each configuration option.
- API Reference describes how to access the API documentation on a live system and includes a static copy of the API documentation.
- SCALE Security Reports links to the TrueNAS Security Hub and also contains any additional security-related notices.

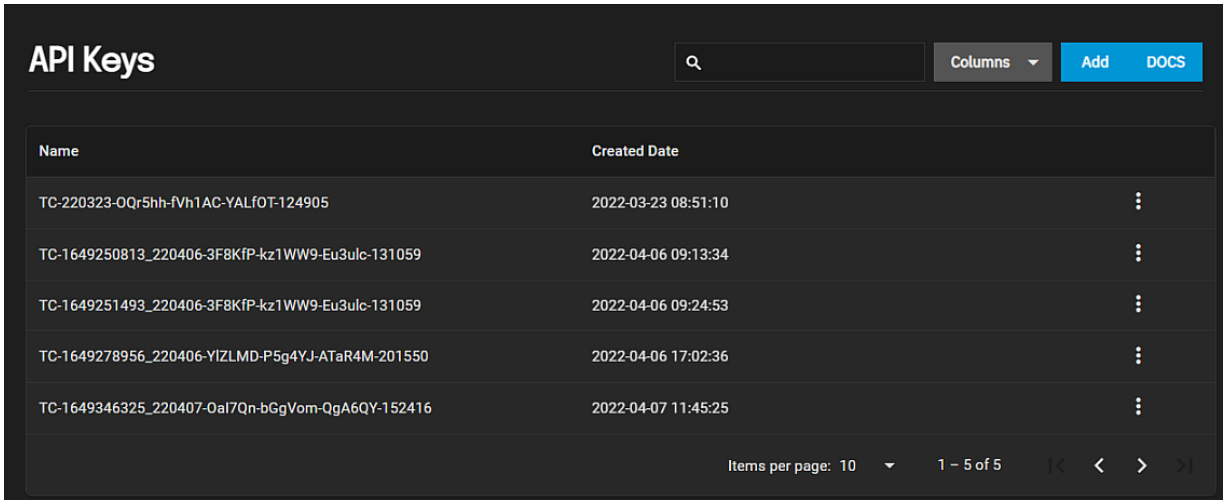
Ready to get started? Choose a topic or article from the left-side **Navigation** pane. Click the **<** symbol to expand the menu to show the topics under this section.

3.1 - Top Toolbar

- Managing API Keys
- Setting Up System Email

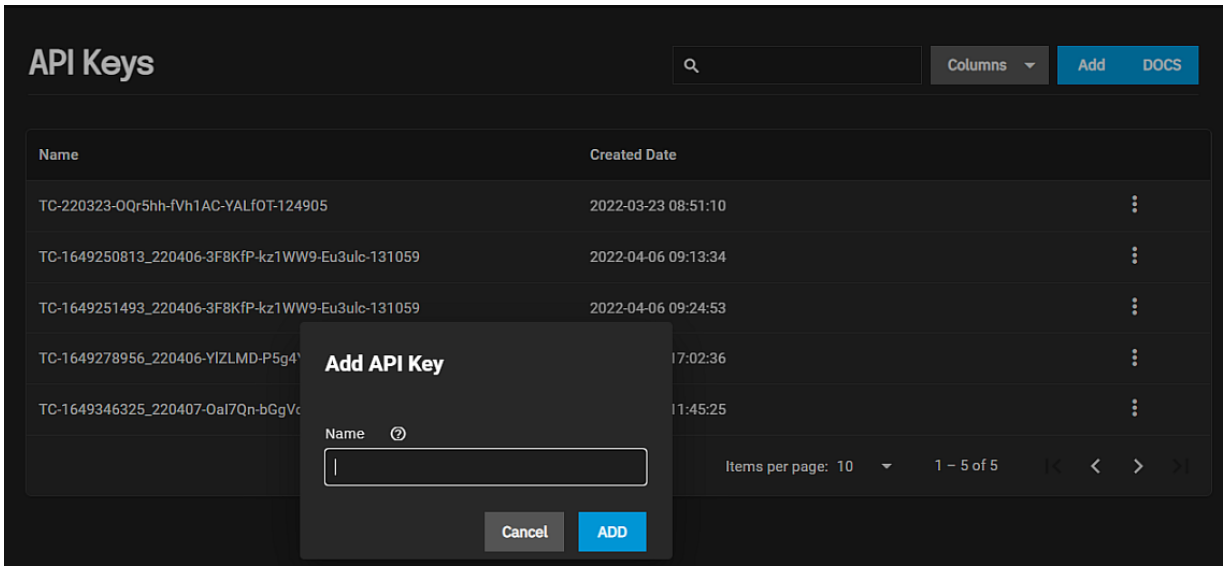
3.1.1 - Managing API Keys

The **API Keys** option on the top toolbar **Settings** dropdown menu displays the **API Keys** screen. This screen displays a list of API keys added to your TrueNAS.



Adding an API Key

Click **Add** to display a dialog window that lets users add a new API key. API keys identify outside resources and applications without a principal.



Type a descriptive name and click **Add**. The system displays a confirmation dialog and adds a new API key to the list.

Creating API Keys in the Shell

TrueNAS SCALE supports creating API keys in the **Shell** with an allow list of permissions for the keys.

Go to **System Settings > Shell** and enter `midclt call api_key.create '{"name":"KEYNAME", "allowlist": [{"method": "HTTPMETHOD", "resource": "METHODNAME"}]}'` using your desired `allowlist` parameters.

Example of a Call

```
midclt call api_key.create '{"name":"api key 1", "allowlist": [{"method": "SUBSCRIBE", "resource": "certificate.query"}]}'
```

In this case, the HTTP `method` is `SUBSCRIBE`, which is a websocket API event subscription. The `resource` is `certificate.query`, which is the event name.

Example of a Wildcard Call

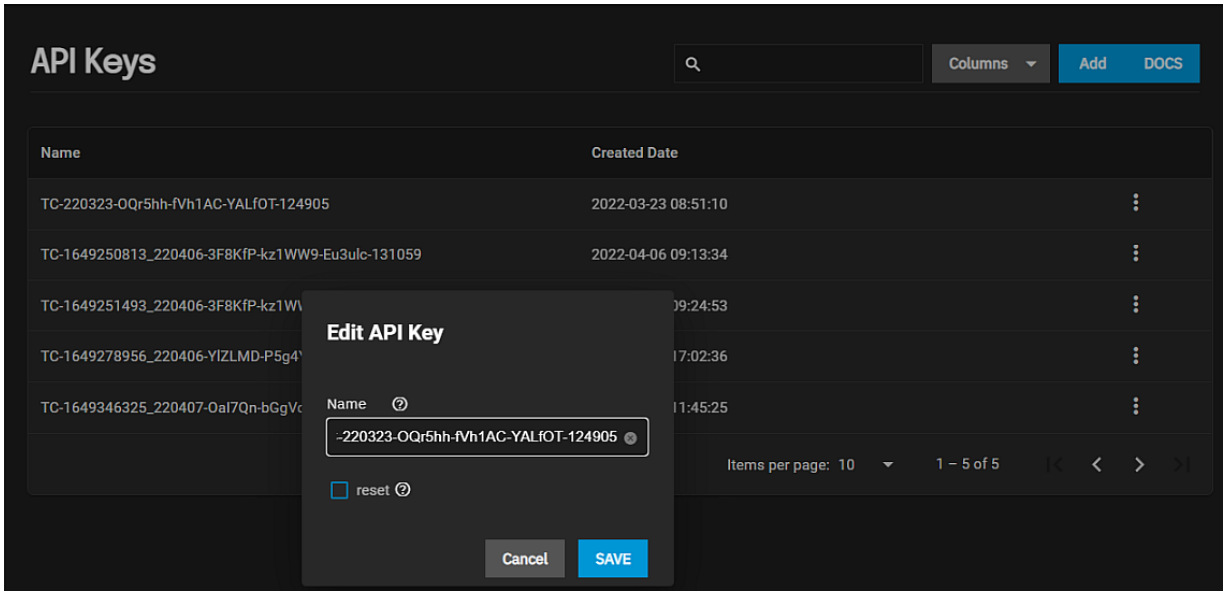
```
midclt call api_key.create '{"name":"api key 2", "allowlist": [{"method": "CALL", "resource": "zfs.snapshot.*"}]}'
```

In this case, the HTTP `method` is `CALL`, which is a websocket API method call. The `resource` is `zfs.snapshot.*`, which is the method name wildcard.

After you enter the command, the **Shell** displays the API Key in the output.

Editing or Deleting an API Key

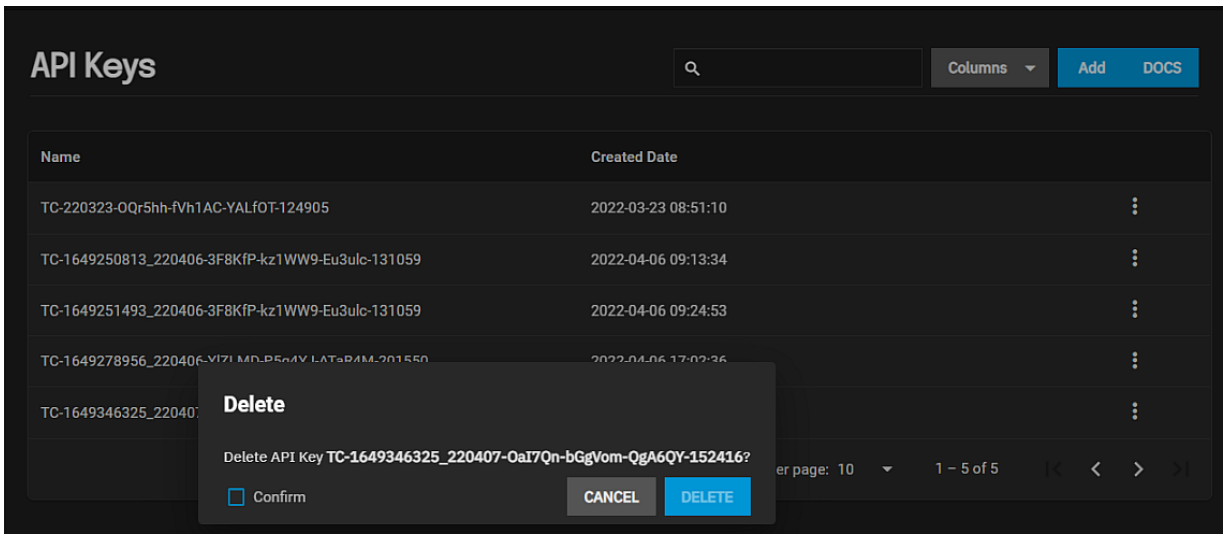
Select the icon for any API key on the list to display options to manage that API key. Options are **Edit** or **Delete**.



Select the **Reset** to remove the existing API key and generate a new random key. The dialog displays the new key and the **Copy to Clipboard** option to copy the key to the clipboard.

> Always back up and secure keys. The key string displays only one time, at creation!

To delete, select **Confirm** on the delete dialog to activate the **Delete** button.



API Key Documentation

Click **DOCS** to access API documentation for your system.

Related Content

- API Keys Screen

3.1.2 - Setting Up System Email

An automatic script sends a nightly email to the administrator root account containing important information such as the health of the disks. Alert events are also emailed to the root user account. Configure the system to send these emails to the administrator remote email account for fast awareness and resolution of any critical issues.

> Scrub Task issues and S.M.A.R.T. reports are mailed separately to the address configured in those services.

Setting up User Accounts

Configure the email address for the system root user as part of your initial system setup. You can also configure email addresses for additional user accounts as needed.

Configuring the Root User Email Address

Before configuring anything else, set the root account email address.

Click here for instructions

Go to **Credentials > Local Users**, select the click ⌄ to expand the root user information. Select **Edit** to display the **Edit User** configuration screen. In the **Email** field, enter a remote email address that the system administrator regularly monitors (like *admin@example.com*) and click **Save**.

Configuring User Email

Just as with the root user, you can add new users as an admin or non-administrative account, and set up email for that user. Follow the directions in Configuring the Root User Email Address for an existing user or in Setting Up User Accounts to add email service for a new user.

Configuring System Email

After setting up the root user email address you need to set up the send method for email service.

Click the **Alerts** icon in the top right of the UI, then click the gear icon and select **Email** to open the **Email** configuration screen.

The **Send Mail Method** shows two different options:

- **SMTP**
- **GMail OAuth**

The **Email** screen configuration options change based on the selected option.

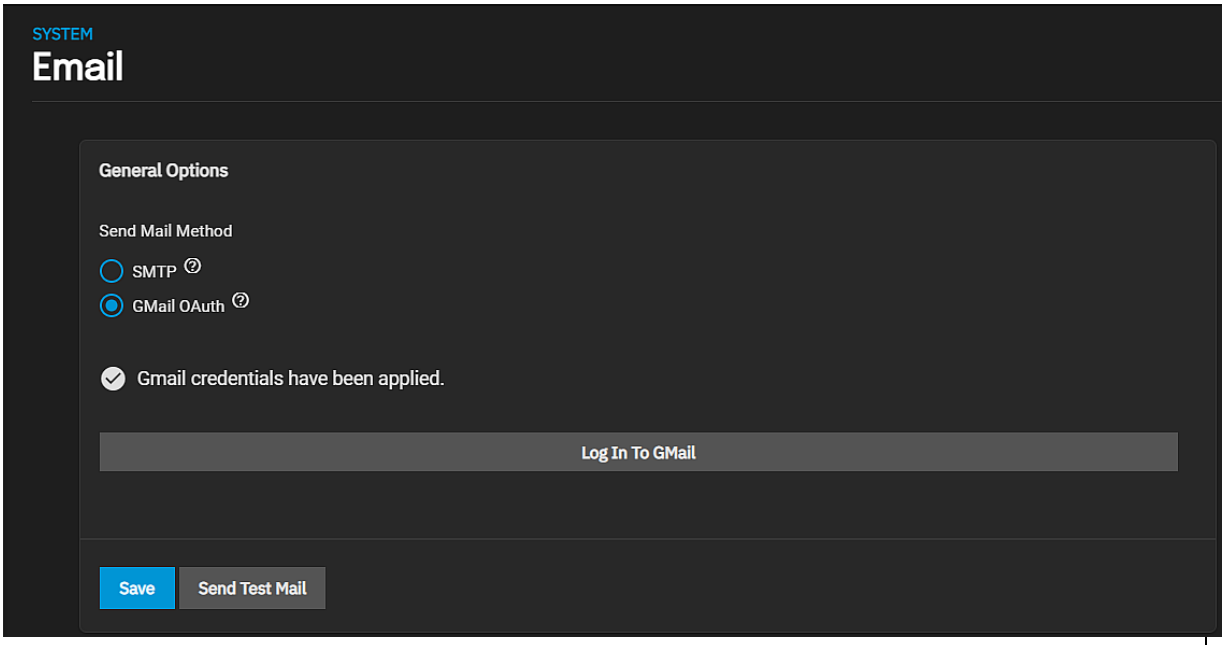
After configuring the send method, click **Send Test Mail** to verify the configured email settings are working. If the test email fails, verify that the root user **Email** field is correctly configured for the root user. Return to **Credentials > Users** to select the root user.

Setting Up Email Using GMail OAuth

The **Email** screen displays with **GMail OAuth** preselected as the default send method.

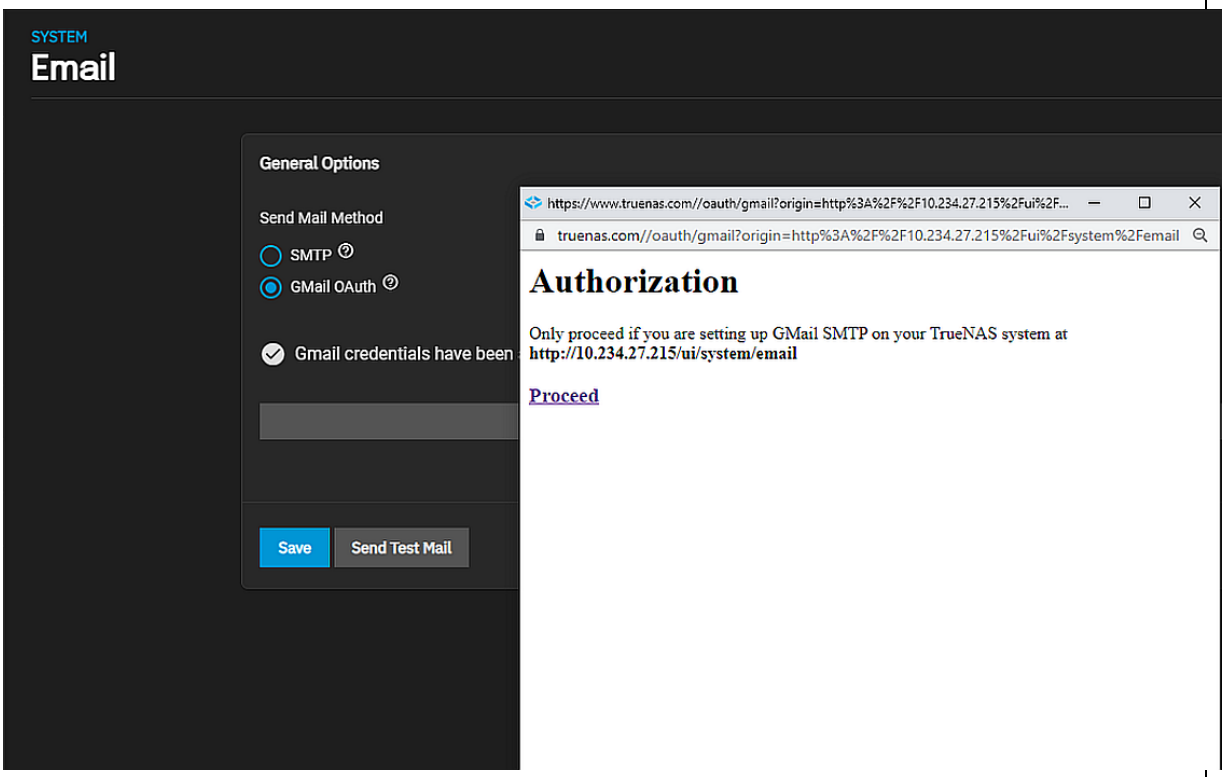
Click here for more information

To use the **GMail OAuth** send method:

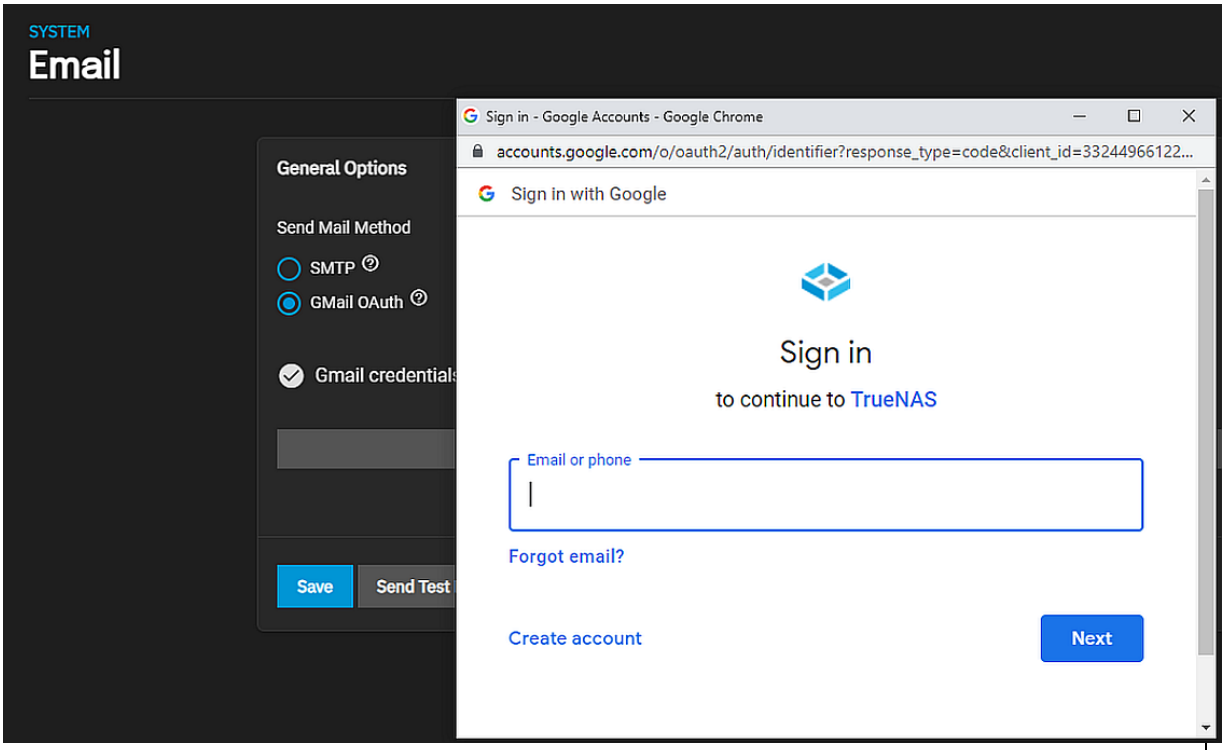


Click on **Log In To GMail**.

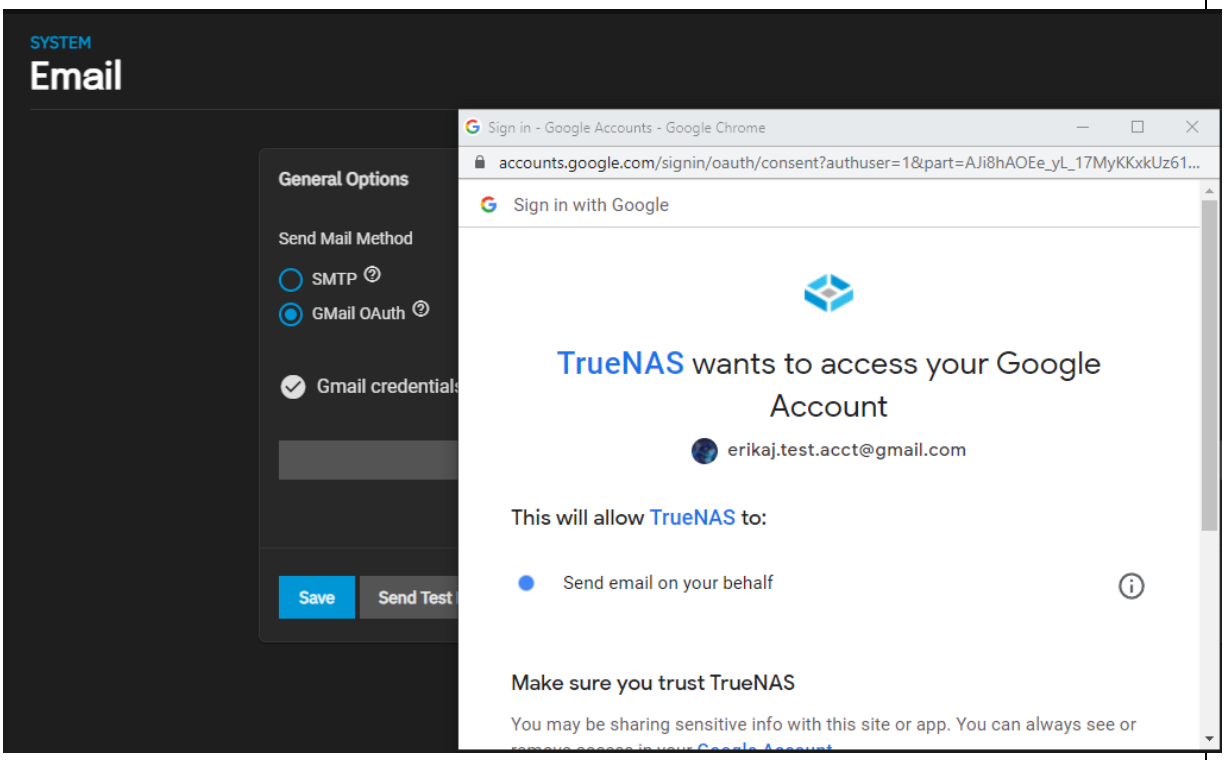
The GMail **Authorization** window displays.

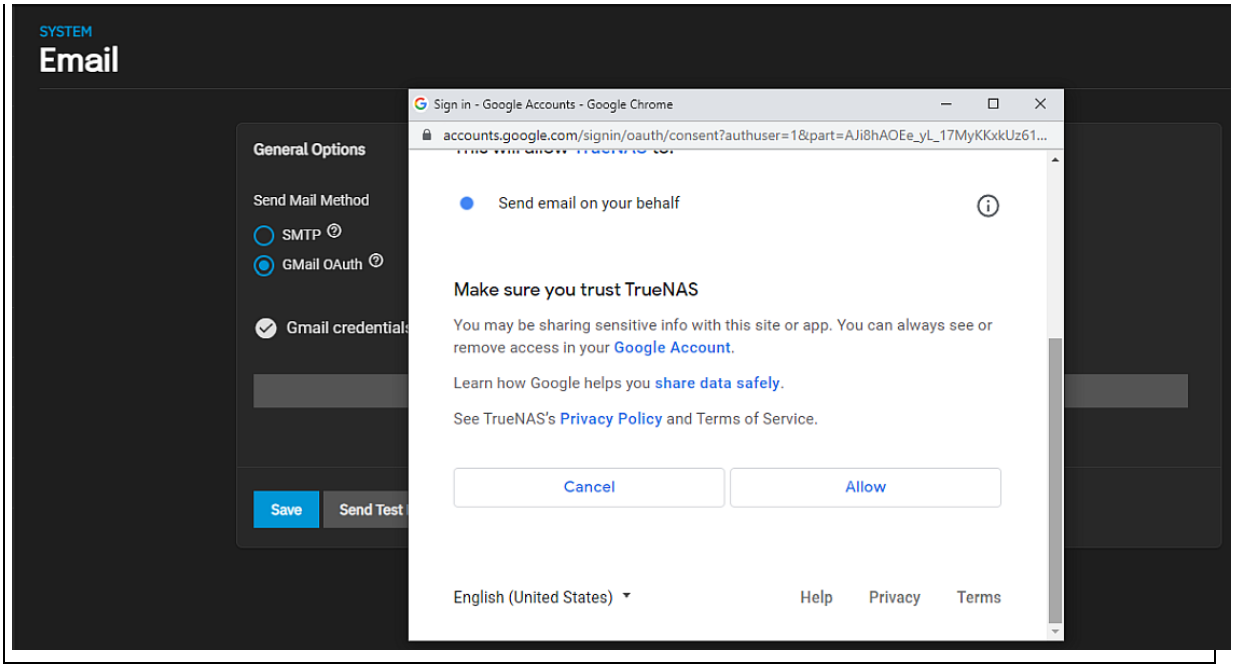


Click **Proceed** to display the **Sign in with Google** window.



Enter the Gmail account credentials. Type in the GMail account to use and click **Next**. Enter the password for the GMail account you entered. When the **TrueNAS wants to access your Google Account** window displays, scroll down and click **Allow** to complete the set up or **Cancel** to exit set up and close the window.



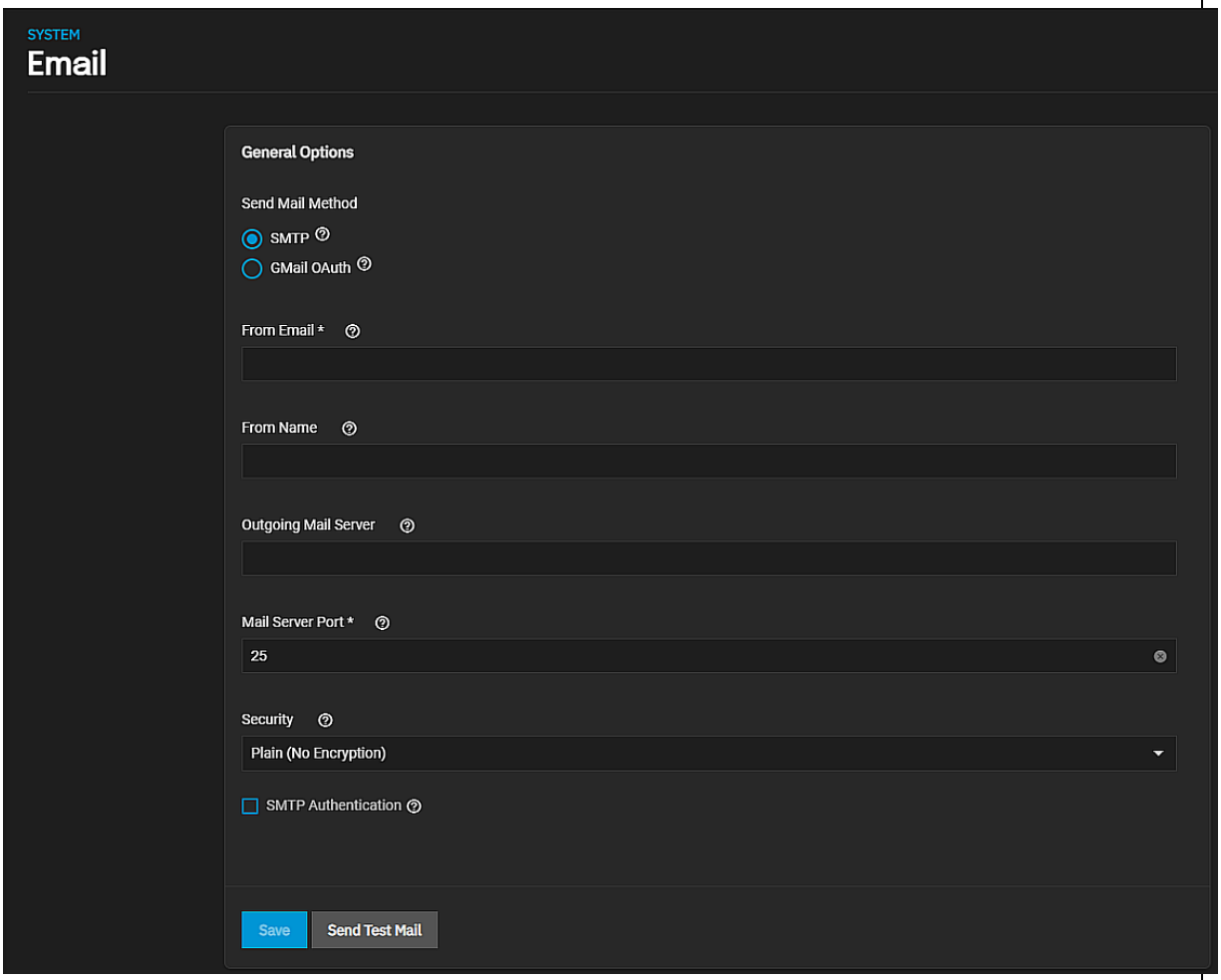


Setting Up Email Using SMTP

To setup up SMTP service for the system email send method you need the outgoing mail server and port number for the email you entered.

Click here for more information

Enter the email you want to use in **From Email** and the name in **From Name**. This is the email that sends the alerts and the name associated with the email.



Enter the host name or IP address of SMTP server sending email. Enter the SMTP port number. Typically 25/465 (secure SMTP), or 587 (submission).

Select the level of security from the **Security** dropdown list. Options are **Plain (No Encryption)**, **SSL (Implicit TLS)**, or **TLS (STARTTLS)**.

Select **SMTP Authentication** if you use the SMTP server uses authentication credentials and enter those credentials.

Click **Save**.

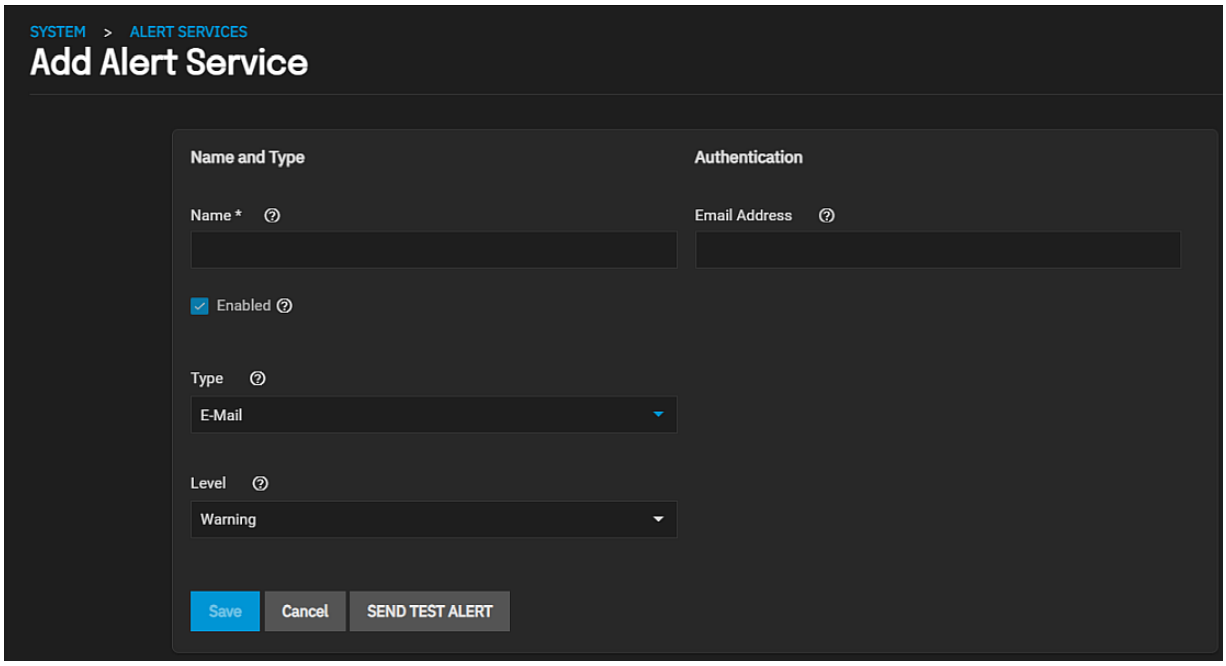
Click **Send Test Email** to verify you receive an email.

Setting up the Email Alert Service

The system email account is sent a system health email every night/morning, if it is configured. You can also add/configure the **Email Alert Service** to send timely email warnings, when the system hits a specific state that is listed in Alert Settings, to the email specified in the alert service.

From the **Alerts** panel, select the ⚙ icon and then **Alert Services**.

Change the **Type** field to **Email** and then populate the **Add Alert Service** form.



Add the system email address in the **Email Address** field.

Use **SEND TEST ALERT** to generate a test alert and confirm the email address and alert service works.

Related Content

- Email Screens

3.2 - Network

- Interface Configurations

  Managing Interfaces This article describes how to add, edit, and delete a network interface. Setting Up a Network Bridge This article provides instructions on setting up a network bridge interface. Setting Up a Link Aggregation This article provides instructions on setting up a network link aggregation (LAGG) interface. Setting Up a Network VLAN This article provides instructions on setting up a network VLAN interface.

  - Managing Interfaces

    This article describes how to add, edit, and delete a network interface.

  - Setting Up a Network Bridge

    This article provides instructions on setting up a network bridge interface.

  - Setting Up a Link Aggregation

    This article provides instructions on setting up a network link aggregation (LAGG) interface.

  - Setting Up a Network VLAN

    This article provides instructions on setting up a network VLAN interface.

  - Setting Up Static IPs

    This article provides instructions on setting up a network interface static IP address.

- Adding Network Settings

  This article provides instructions on adding network settings during initial SCALE installation or after a clean install of SCALE.

- Managing Network Global Configurations

  This article provides instructions on configuring or managing global configuration settings.

- Configuring Static Routes

  This article provides instructions on configuring a static route using the SCALE web UI.

- Setting Up IPMI

  This article guides you through setting up Intelligent Platform Management Interface (IPMI) on TrueNAS SCALE.

3.2.1 - Interface Configurations

- Managing Interfaces

  This article describes how to add, edit, and delete a network interface.

- Setting Up a Network Bridge

  This article provides instructions on setting up a network bridge interface.

- Setting Up a Link Aggregation

  This article provides instructions on setting up a network link aggregation (LAGG) interface.

- Setting Up a Network VLAN

  This article provides instructions on setting up a network VLAN interface.

- Setting Up Static IPs

  This article provides instructions on setting up a network interface static IP address.

3.2.1.1 - Managing Interfaces

This article describes how to add, edit, and delete a network interface.

You can add new or edit existing network interfaces on the **Network** screen.

Why should I use different interface types?

LAGG (Link Aggregation)

You should use LAGG if you want to optimize multi-user performance, balance network traffic, or have network failover protection.

For example, Failover LAGG prevents a network outage by dynamically reassigning traffic to another interface when one physical link (a cable or NIC) fails.

Network Bridge

You should use a Bridge if you want to enable communication between two networks and provide a way for them to work as a single network.

For example, bridges can serve IPs to multiple VMs on one interface, which allows your VMs to be on the same network as the host.

Adding an Interface

> You can only use DHCP to provide the IP address for one network interface and this is most likely for your primary network interface configured during the installation process.
>
> To add another network interface leave the **DHCP** checkbox clear and click the **Add** button near the bottom of the **Add Interface** configuration panel so you can enter a static IP address for the interface.

Click **Add** on the **Interfaces** widget to display the **Add Interface** panel.

You must specify the type of interface you want to create. The **Type** field provides three options: **Bridge**, **Link Aggregation** or LAGG, and **VLAN*** or virtual LAN. You cannot edit the interface type after you click **Save**.

Each interface type displays new fields on the **Add Interface** panel. Links with more information on adding these specific types of interfaces are at the bottom of this article.

Editing an Interface

Click on an existing interface in the **Interfaces** widget to display the **Edit Interface** configuration panel. The fields on the **Edit Interface** and **Add Interface** configuration panel fields are identical except for the **Type** and **Name** fields. Both of these fields are editable only on the **Add Interface** panel before you click **Save**. The **Type** field only appears on the **Add Interface** configuration panel.

Because you cannot edit the interface type or name after you click **Save**, if you make a mistake with either field you can only delete that interface and create a new one with the desired type.

If you want to change from DHCP to a static IP, you must also add the new default gateway and DNS nameservers that work with the new IP address. See Setting Up a Static IP for more information.

> If you delete the primary network interface you can lose your TrueNAS connection and the ability to communicate with the TrueNAS through the web interface!
>
> You might need command line knowledge or physical access to the TrueNAS system to fix misconfigured network settings.

Deleting an Interface

Click the icon next to the interface. The delete interface confirmation dialog displays.

> Do not delete the primary network interface!

> If you delete the primary network interface you lose your TrueNAS connection and the ability to communicate with the TrueNAS through the web interface! You might need command line knowledge or physical access to the TrueNAS system to fix misconfigured network settings.

Related Content

- Network Interface Screens
- Console Setup Menu Configuration
- Setting Up a Network Bridge
- Setting Up a Link Aggregation
- Setting Up a Network VLAN
- Configuring Static Routes
- Setting Up Static IPs

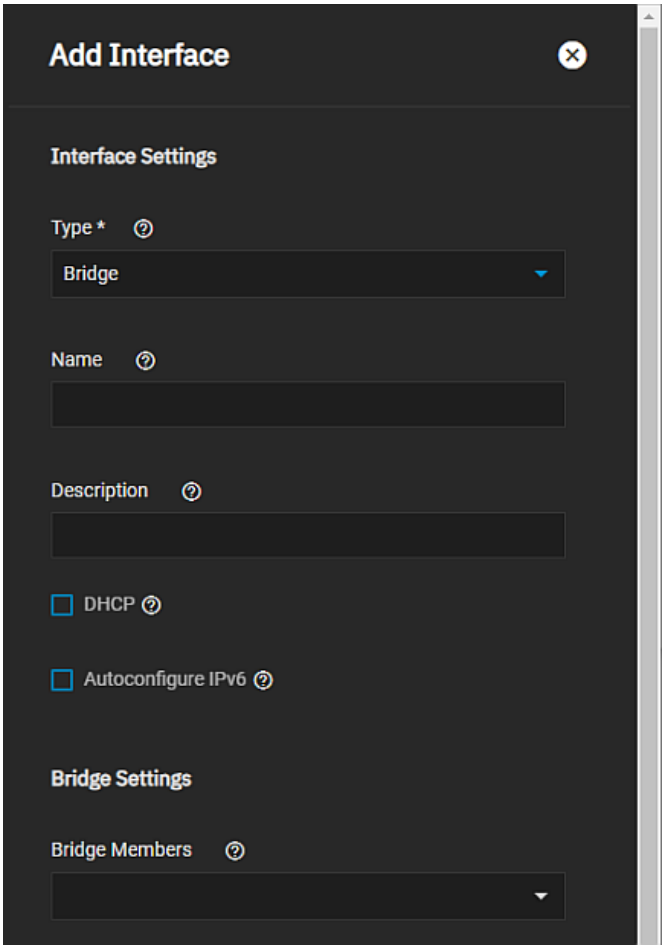
3.2.1.2 - Setting Up a Network Bridge

This article provides instructions on setting up a network bridge interface.

In general, a bridge refers to various methods of combining (aggregating) multiple network connections into a single aggregate network. TrueNAS uses bridge(4) as the kernel bridge driver. Bridge(8) is a command for configuring the kernal bridge in Linux. While the examples focus on the deprecated brctl(8) from the bridge-utilities package, we use ip(8) and bridge(8) from iproute2 instead. Refer to the FAQ section that covers bridging topics more generally.

To set up a bridge interface, from the **Network** screen:

1. Click **Add** in the **Interfaces** widget. The **Add Interface** configuration screen displays.



2. Select **Bridge** from the **Type** dropdown list. You cannot change the **Type** field value after you click **Apply**.
3. Enter a name for the interface using the format *bridgex* where *x* is a number representing a non-parent interface. You cannot change the **Name** of the interface after you click **Apply**.
4. (Optional but recommended) Enter any notes or reminders about this particular bridge in the **Description** field.
5. Select the interfaces on the **Bridge Members** dropdown list.
6. (Optional) Click **Add** to enter another IP address if desired for this bridge interface. Click **Add** to display an IP address field for each IP address you want to add.
7. Click **Apply** when finished.

Related Content

- Network Interface Screens
- Managing Interfaces
- Console Setup Menu Configuration
- Setting Up a Link Aggregation
- Setting Up a Network VLAN
- Configuring Static Routes
- Setting Up Static IPs

Related Network Articles

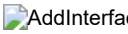
3.2.1.3 - Setting Up a Link Aggregation

This article provides instructions on setting up a network link aggregation (LAGG) interface.

In general, a link aggregation (LAGG) a general method of combining (aggregating) multiple network connections in parallel to provide additional bandwidth or redundancy for critical networking situations. TrueNAS uses lagg(4) to manage LAGGs.

To set up a LAGG interface, from the **Network** screen:

1. Click **Add** in the **Interfaces** widget. The **Add Interface** configuration screen displays.

    AddInterfaceLinkAggregationTypes

2. Select **Link Aggregation** from the **Type** dropdown list. You cannot change the **Type** field value after you click **Apply**.

3. Enter a name for the interface using the format *laggX* where *X* is a number representing a non-parent interface. You cannot change the **Name** of the interface after you click **Apply**.

4. (Optional but recommended) Enter any notes or reminders about this particular LAGG interface in the **Description** field.

5. Select the **Link Aggregation Settings** for this interface.

   a. Select the **Link Aggregation Protocol** from the dropdown list of options. There are three protocol options, **LACP**, **FAILOVER** and **LOADBALANCE**. Additional fields display based on the LAGG protocol you select.

   Select **LACP** to use the most common protocol for LAGG interfaces based on IEEE specification 802.3ad. In LACP mode, negotiation is performed with the network switch to form a group of ports that are all active at the same time. The network switch must support LACP for this option to function.

   Select **FAILOVER** to have traffic sent through the primary interface of the group. If the primary interface failes, traffic diverts to the next available interface in the LAGG.

   Select **LOADBALANCE** to accept traffic on any port of the LAGG group and balance the outgoing traffic on the active ports in the LAGG group. This is a static setup that does not monitor the link state nor does it negotiate with the switch.

   b. Select the LAGG interfaces from the **Link Aggregation Interfaces**.

   c. If the protocol selected is **LACP** or **LOADBALANCE**, select the **Transmit Hash Policy** option from the dropdown list. **LAYER2+3** is the default selection.

   d. If the protocol selected is **LACP**, select the **LACPDU Rate** to used. Select **SLOW** to set the heartbeat request to every second and the timeout to a three-consecutive heartbeat loss that is three seconds (default is SLOW). Select **FAST** to set the timeout rate at one per second even after synchronization. Using **FAST** allows for rapid detection of faults.

6. (Optional) Click **Add** to enter another IP address if desired for this LAGG interface. Click **Add** to display an IP address field for each IP address you want to add.

7. Click **Apply** when finished.

Related Content

- Network Interface Screens
- Managing Interfaces
- Console Setup Menu Configuration
- Setting Up a Network Bridge
- Setting Up a Network VLAN
- Configuring Static Routes
- Setting Up Static IPs

Related Network Articles

- Dashboard
- Network Interface Screens
- Adding Network Settings
- Managing Interfaces
- Console Setup Menu Configuration
- Global Configuration Screens
- Managing Network Global Configurations
- Setting Up a Network Bridge
- Static Route Screens

3.2.1.4 - Setting Up a Network VLAN

This article provides instructions on setting up a network VLAN interface.

A virtual LAN (VLAN) is a partitioned and isolated domain in a computer network at the data link layer (OSI layer 2). Click here for more information on VLANs. TrueNAS uses vlan(4) to manage VLANs.

Before you begin, make sure you have an Ethernet card connected to a switch port and already configured for your VLAN. Also that you have preconfigured the VLAN tag in the switched network.

To set up a VLAN interface, from the **Network** screen:

1. Click **Add** in the **Interfaces** widget. The **Add Interface** configuration screen displays.

2. Select **VLAN** from the **Type** dropdown list. You cannot change the **Type** field value after you click **Apply**.
3. Enter a name for the interface using the format *vlanX* where *X* is a number representing a non-parent interface. You cannot change the **Name** of the interface after you click **Apply**.
4. (Optional but recommended) Enter any notes or reminders about this particular VLAN in the **Description** field.
5. Select the interface in the **Parent Interface** dropdown list. This is typically an Ethernet card connected to a switch port already configured for the VLAN.
6. Enter the numeric tag for the interface in the **Vlan Tab** field. This is typically preconfigured in the switched network.
7. Select the VLAN Class of Service from the **Priority Code Point** dropdown list.
8. (Optional) Click **Add** to enter another IP address if desired for this bridge interface. Click **Add** to display an IP address field for each IP address you want to add.
9. Click **Apply** when finished.

Related Content

- Network Interface Screens
- Managing Interfaces
- Console Setup Menu Configuration
- Setting Up a Network Bridge
- Setting Up a Link Aggregation
- Configuring Static Routes
- Setting Up Static IPs

Related Network Articles

- Dashboard
- Network Interface Screens
- Adding Network Settings
- Managing Interfaces
- Console Setup Menu Configuration
- Global Configuration Screens
- Managing Network Global Configurations
- Setting Up a Network Bridge
- Static Route Screens
- Setting Up a Link Aggregation

3.2.1.5 - Setting Up Static IPs

This article provides instructions on setting up a network interface static IP address.

This article provides instructions on setting up a network interface with a static IP address or changing the main interface from a DHCP-assigned to a manually-entered static IP address. You must know the DNS name server and default gateway addresses for your IP address.

> **Disruptive Change!**
>
> You can lose your TrueNAS connection if you change the network interface that the web interface uses!
> You might need command line knowledge or physical access to the TrueNAS system to fix misconfigured network settings.

Before you Begin

Have the DNS name server addresses and the default gateway for the new IP address, and the new static IP address on hand to prevent lost communication with the server. You have only 60 seconds to change and test these network settings before they revert back to the current settings, for example back to DHCP assigned if moving from DHCP to a static IP.

Back up your system to preserve your data and system settings.

As a precaution, grab a screenshot of your current settings in the **Global Configuration** widget.

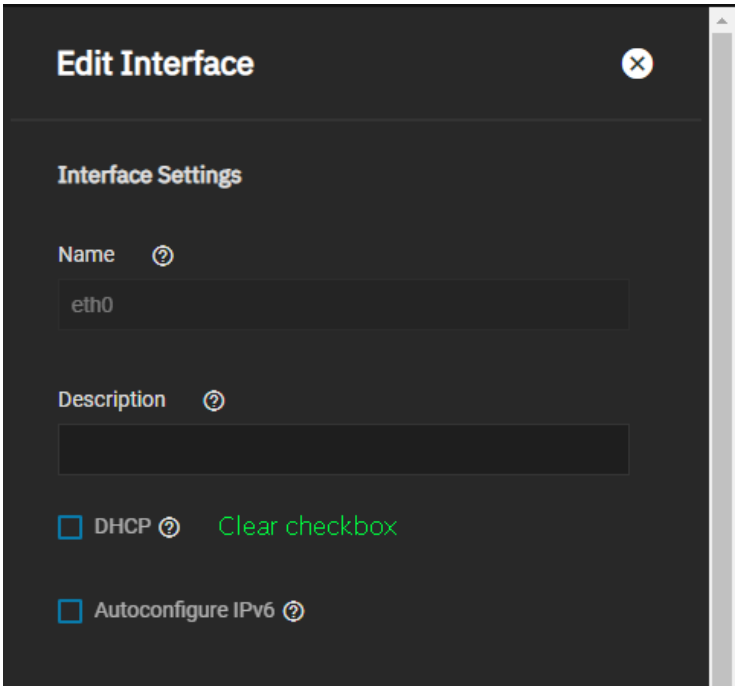
If your network changes result in lost communication with the network and you need to return to the DHCP configuration you had before, you can refer to this information to restore communication with your server. Lost communicatation could require you to reconfigure your network settings using the Console Setup Menu.

Changing the Interface to a Static IP Address

To view a demonstration of this procedure see the tutorial video in the Managing Global Configuration article.

To change an interface from using DHCP to a static IP address:

1. Select the interface on the **Interfaces** widget to open the **Edit Interface** configuration screen to turn off **DHCP** and add the new static IP. Click **Apply**.



Click here for more help with this.

a. Clear the checkmark from the **DHCP** checkbox.

b. Click **Add** in the **IP Addresses** section of the form and then enter the new static IP address into the field displayed. Select the CIDR number from the dropdown list.

```
![EditInterfaceAddStaticIP](/images/SCALE/22.02/EditInterfaceAddStaticIP.png "Add IP Addresses")
```

c. Click **Apply**. The **Network** screen displays with a new widget where you can select to either **Test Changes** or **Revert Changes**.

```
![NetworkTestChangesWidget](/images/SCALE/22.02/NetworkTestChangesWidget.png "Test Change Widget")
```

2. Check the name servers and default router information in the **Global Information** card. If the current settings are not on the same network click **Settings** and modify each as needed to allow the static IP to communicate over the network.

For home users, use **8.8.8.8** for a DNS name sever address so you can communicate with external networks.

Click here for more help with this.

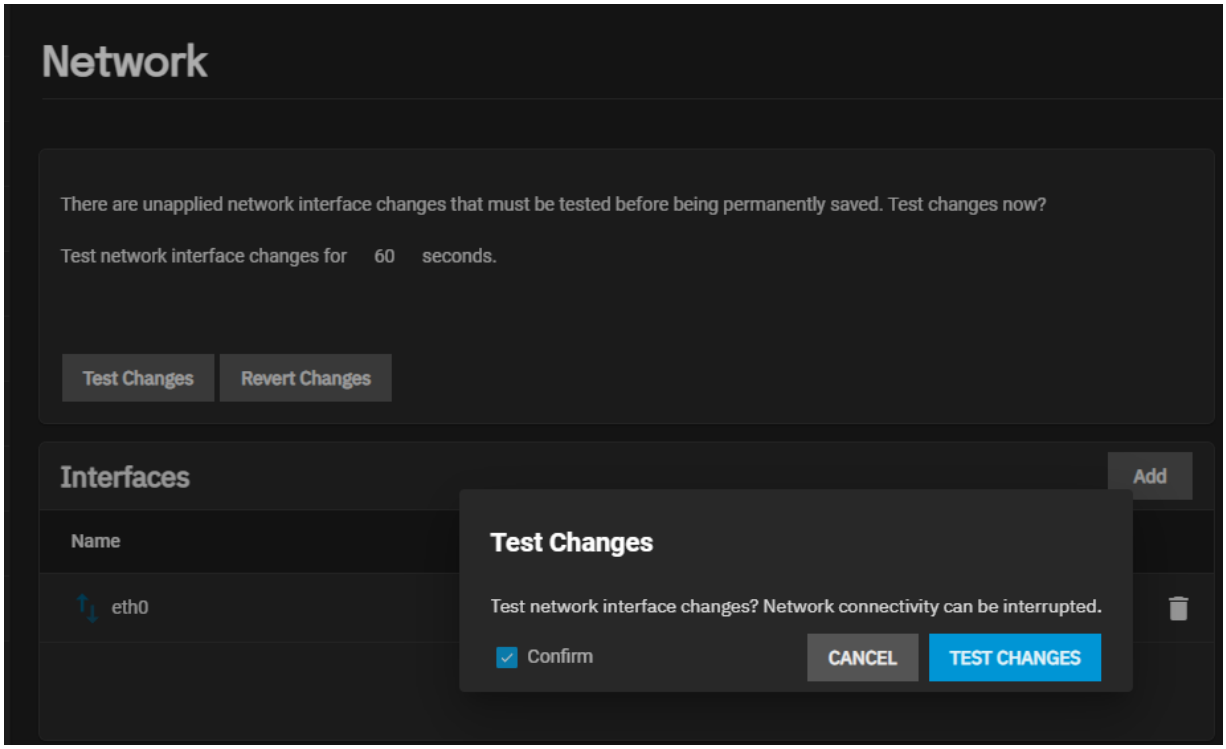
a. Add the IP addresses for the DNS name servers in the **Nameserver 1**, **Nameserver2**, and **Nameserver3** fields.

```
![EditGlobalConfiguration](/images/SCALE/22.02/EditGlobalConfiguration.png "Add Nameserver and Default Gateway")
```

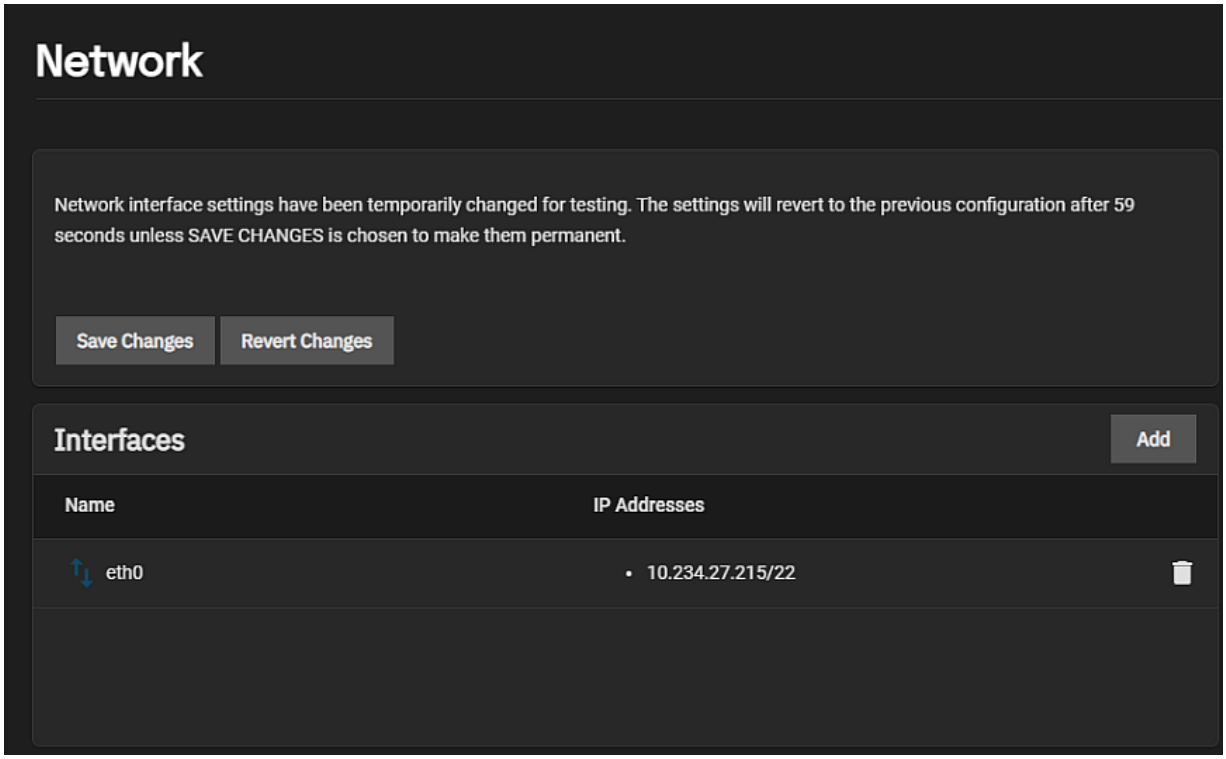
b. Add the IP address for the default gateway in the appropriate field. If the static network is IPv4 enter the gateway in **IPv4 Default Gateway**, if the static network is IPv6 use **IPv6 Default Gateway**.

c. Click **Save**.

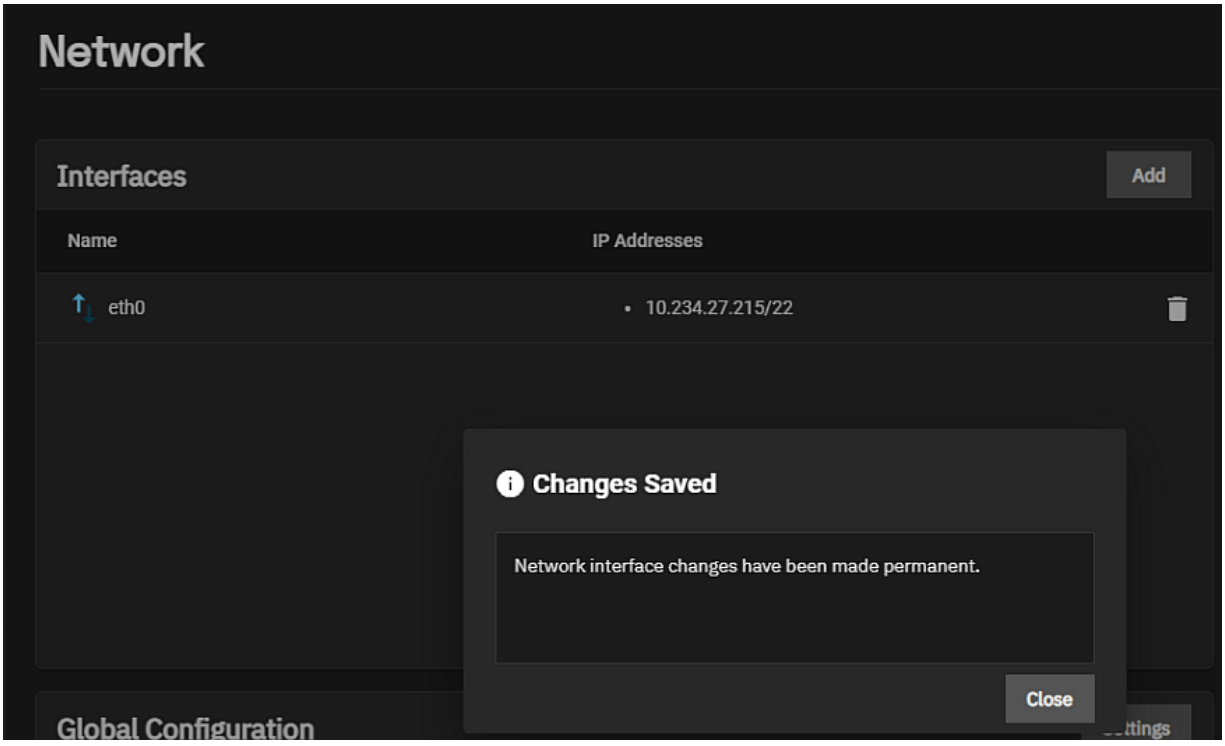
5. Test the network changes. Click **Test Changes**. Select **Confirm** to activate **Test Changes** button. Click the button and then click **Save** on the **Save Changes** dialog.



The system attempts to connect to the new static IP address. If successful the **Save Changes** widget displays.



6. Click **Save Changes** to make the change to the static IP address permanent or click **Revert Changes** to discard changes and return to your previous settings. The **Save Changes** confirmation dialog displays. Click **SAVE**. The system displays a final confirmation that the change is in effect.



Changing from Static IP to DHCP

Only one interface can use DHCP to assign the IP address and that is likely the primary network interface. If you do not have a existing network interface set to use DHCP you can use it to convert from static IP to DHCP.

To return to using DHCP:

1. Click **Settings** on the **Global Configuration** widget.
2. Clear the name server fields and the default gateway, and then click **Save**.
3. Click on the interface to display the **Edit Interface** screen.

4. Select **DHCP**.
5. Remove the static IP address from the **IP Address** field.
6. Click **Apply**.
7. Click **Settings** to display the **Global Configuration** configuration form and enter name server and default gateway addresses for the new DHCP-provided IP address. Home user can enter 8.8.8.8 in the **Nameserver 1** field.
8. Click **Test Change**. If the network settings are correct, the screen displays the **Save Changes** widget. Click **Save Changes**.

   If the test network operation fails or the system times out, your system returns to the network settings before you attempted the change. Verify the name server and default gateway information to try again.

Related Content

- Network Interface Screens
- Managing Interfaces
- Console Setup Menu Configuration
- Setting Up a Network Bridge
- Setting Up a Link Aggregation
- Setting Up a Network VLAN
- Configuring Static Routes

Related Network Articles

- Dashboard
- Network Interface Screens
- Adding Network Settings
- Managing Interfaces
- Console Setup Menu Configuration
- Global Configuration Screens
- Managing Network Global Configurations
- Setting Up a Network Bridge
- Static Route Screens
- Setting Up a Link Aggregation

3.2.2 - Adding Network Settings

This article provides instructions on adding network settings during initial SCALE installation or after a clean install of SCALE.

Use the **Global Configuration Settings** screen to add general network settings like the default gateway, DNS name servers to allow external communication.

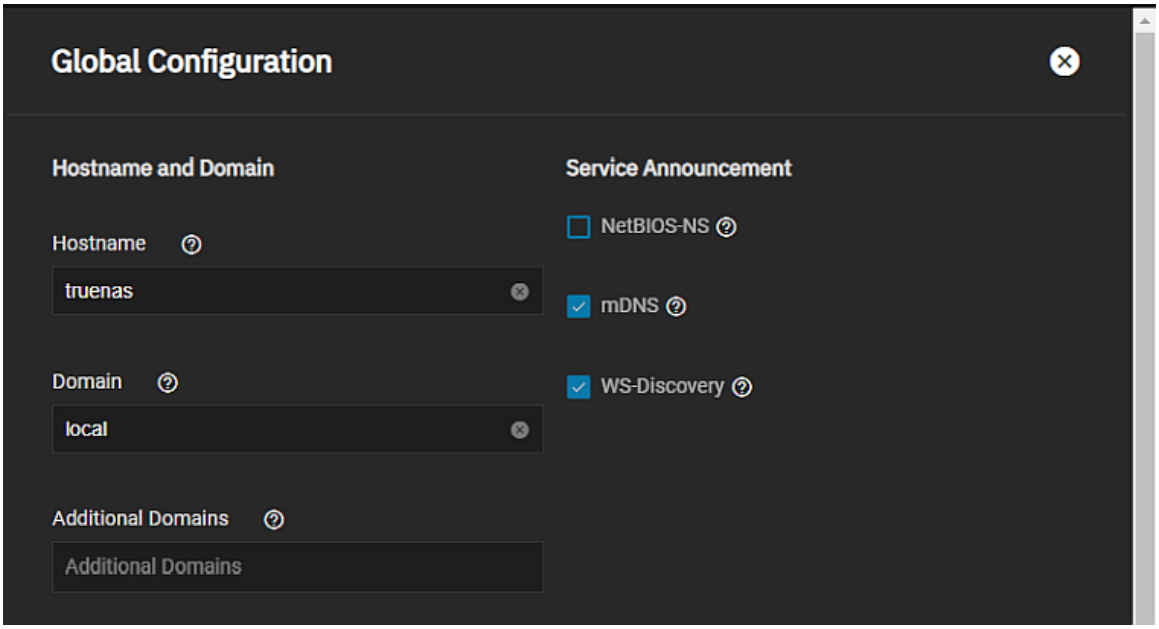
To add new or change existing network interfaces see Managing Interfaces.

> **Disruptive Change**
>
> You can lose your TrueNAS connection if you change the network interface that the web interface uses!
> You might need command line knowledge or physical access to the TrueNAS system to fix misconfigured network settings.

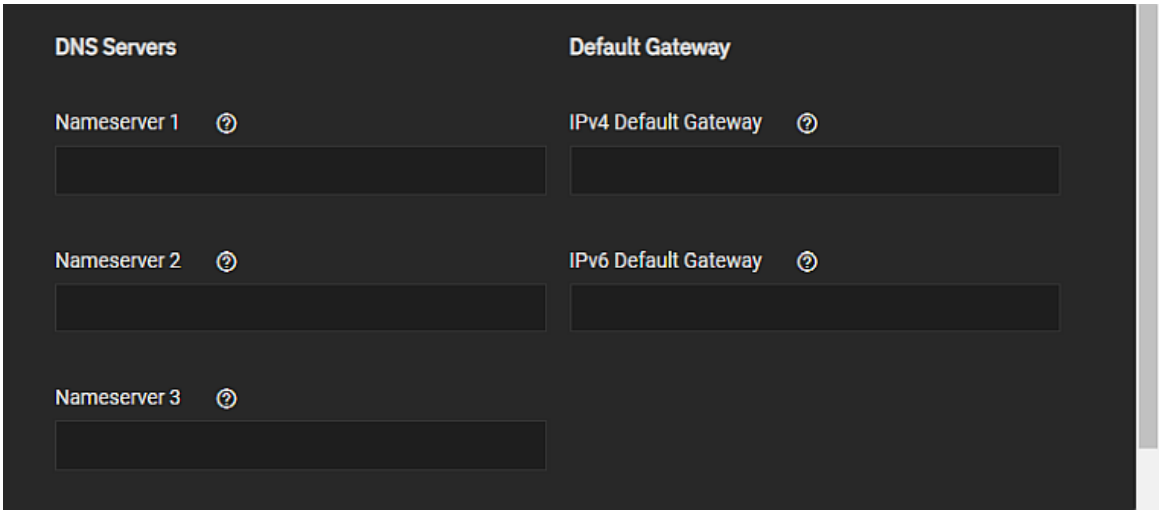
Adding Network Settings

From the **Network > Global Configuration** screen click **Settings** to display the **Global Configuration** configuration form and then:

1. Enter the host name for your TrueNAS in **Hostname**. For example, *truenas*.

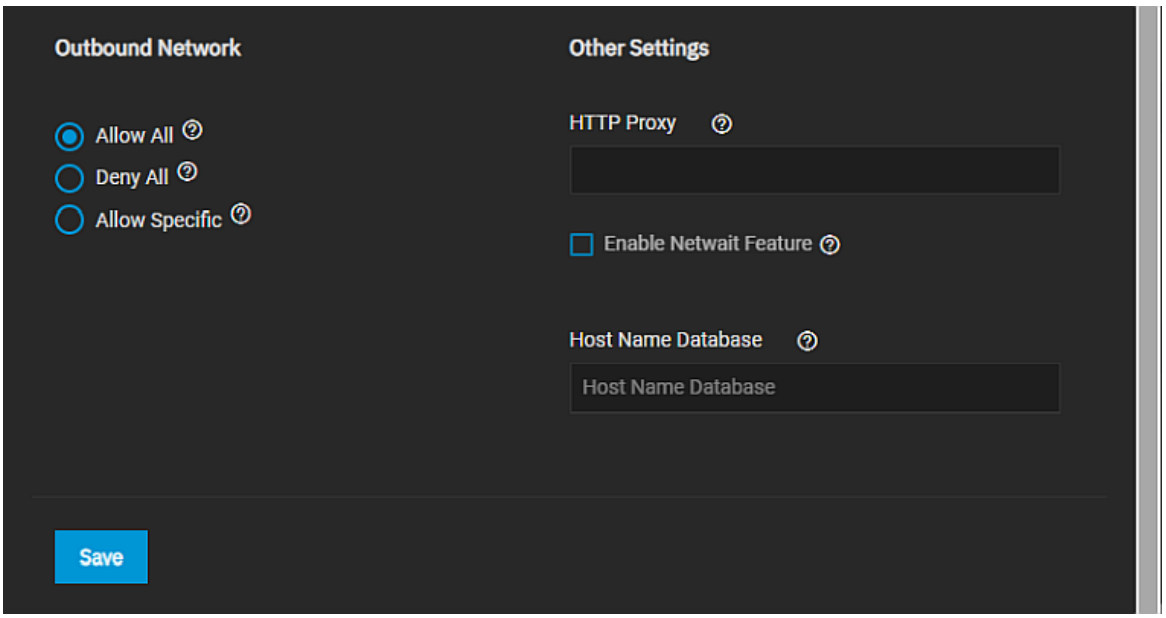


2. Enter the system domain name in **Domain**. For example, *mycompanyname.com*.
3. Enter the IP addresses for your DNS name servers in the **Nameserver 1**, **Nameserver 2**, and/or **Nameserver 3** fields. For home users, enter **8.8.8.8** in the **Nameserver 1** field so your TrueNAS SCALE can communicate externally with the Internet.

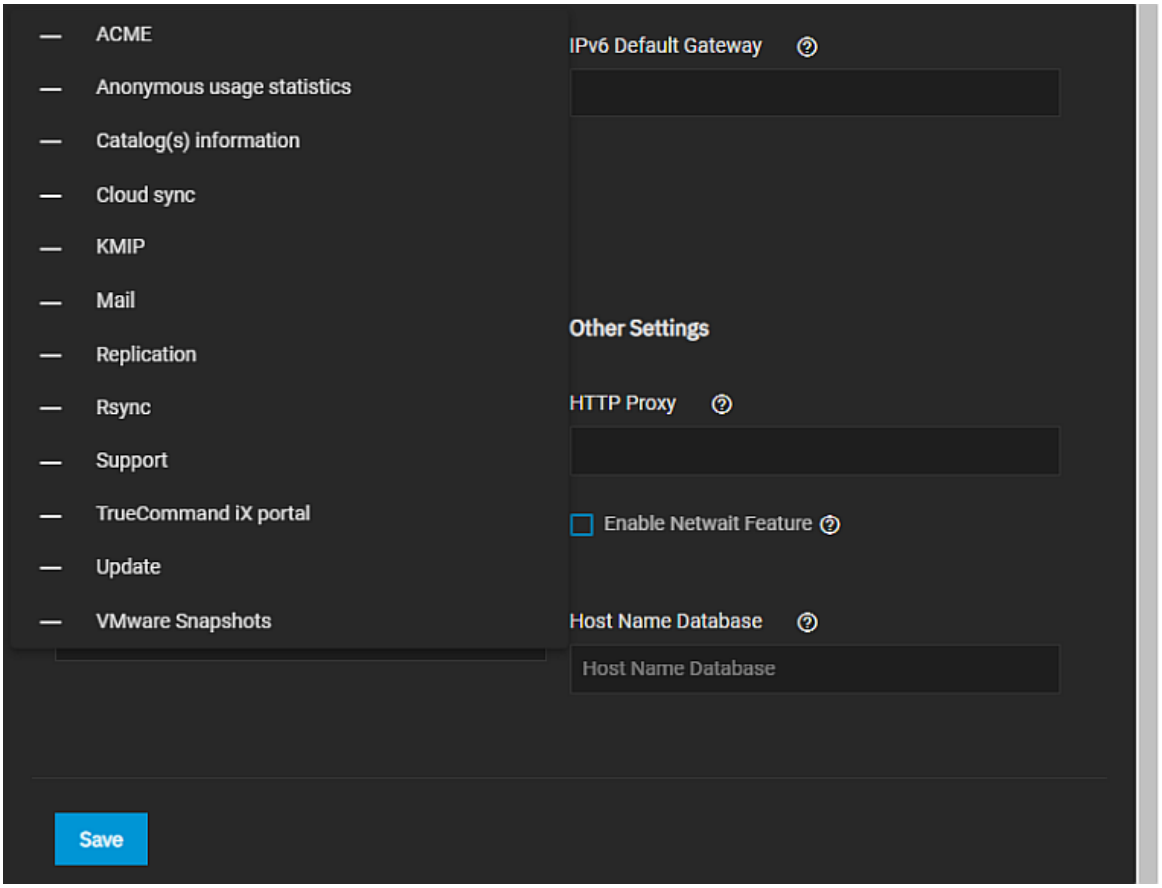


4. Enter the IP address for your default gateway into the **IPv4 Defalut Gateway** if you are using IPv4 IP addresses. Enter the IP address in the **IPv6 Default Gateway** if you are using IPv6 addresses.

5. Select the **Outbound Network** radio button for outbound service capability.



Select **Allow All** to permit all TrueNAS SCALE services that need external communication to do that or select **Deny All** to prevent that external communication. Select **Allow Specific** and then use the dropdown list to pick the services you want to allow to communicate externally.



Click on as many services as you want to permit external communications for. Unchecked services cannot communication externally.

6. Click **Save**. The **Global Configuration** widget on the **Network** screen update to show the new settings.

Related Content

- Dashboard

- Network Interface Screens
- Managing Interfaces
- Console Setup Menu Configuration
- Global Configuration Screens
- Managing Network Global Configurations
- Setting Up a Network Bridge
- Static Route Screens
- Setting Up a Link Aggregation

3.2.3 - Managing Network Global Configurations

This article provides instructions on configuring or managing global configuration settings.

Use the **Global Configuration Settings** screen to manage existing general network settings like the default gateway, DNS servers, set DHCP to assign the IP address or to set a static IP address, add IP address aliases, and set up services to allow external communication.

> **Disruptive Change**
>
> You can lose your TrueNAS connection if you change the network interface that the web interface uses!
> You might need command line knowledge or physical access to the TrueNAS system to fix misconfigured network settings.

Tutorial Video

Can I configure these options elsewhere?
Users can configure many of these interface, DNS, and gateway options in the Console setup menu. Be sure to check both locations when troubleshooting network connectivity issues.

Setting Up External Communication for Services

Use the **Global Configuration Outbound Network** radio buttons to set up services to have external communication capability.

Services that use external communication are:

- ACME DNS-Authenticators
- Anonymous usage statistics
- Catalog(s) information exchanges
- Cloud sync
- KMIP
- Mail (email service)
- Replication
- Rsync
- Support
- TrueCommand iX porta
- Updates
- VMWare snapshots

Select the **Allow All** to permit all the above services to externally communicate. This is the default setting.

Select the **Deny All** to prevent all the above services from externally communicating.

Select the **Allow Specific** to permit external communication for the services you specify. Selecting **Allow Specific** displays a dropdown list field with the list of services you can select from. Select all that apply. A checkmark displays next to each selected service. Selected services display in the field separated by a (,).

Click **Save** when finished.

Setting Up Netwait

Use Netwait to prevent starting all network services until the network is ready. Netwait sends a ping to each of the IP addresses you specify until one responds, and after receiving the response then services can start.

To set up Netwait, from the **Network** screen:

1. Click on **Settings** in the **Global Configuration** widget. The **Global Configuration** screen displays.
2. Select the **Enable Netwait Feature** checkbox. The **Netwait IP List** field displays.
3. Enter your list of IP addresses to ping. Press `Enter` after entering each IP address.

Related Content

- Dashboard
- Network Interface Screens
- Adding Network Settings
- Managing Interfaces

- Console Setup Menu Configuration
- Global Configuration Screens
- Setting Up a Network Bridge
- Static Route Screens
- Setting Up a Link Aggregation

3.2.4 - Configuring Static Routes

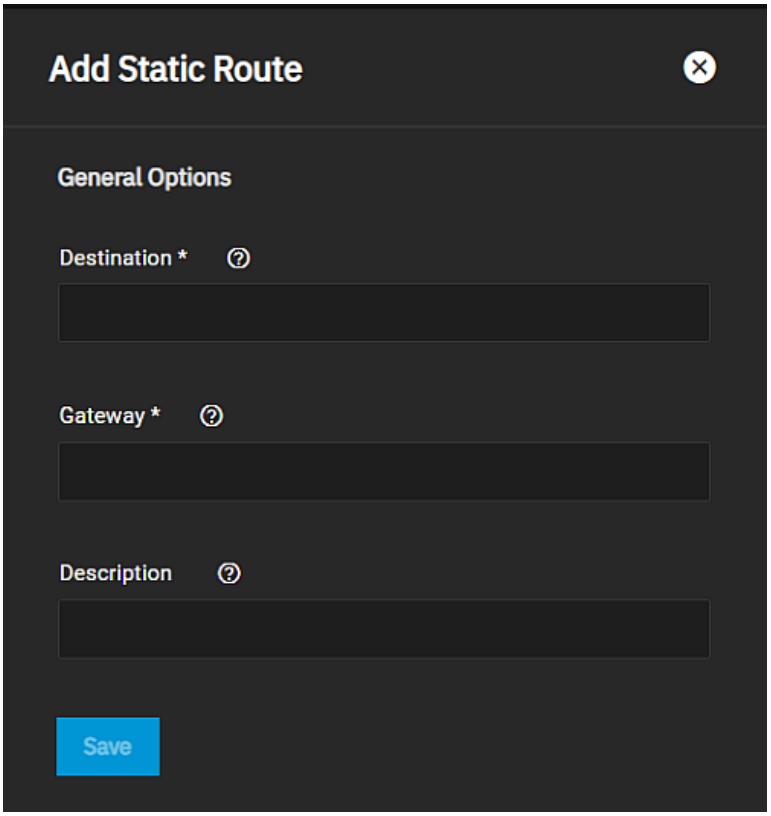
This article provides instructions on configuring a static route using the SCALE web UI.

TrueNAS does not have defined static routes by default but TrueNAS administrators can use the **Static Routes** widget on the **Network** screen to manually enter routes so the router can send packets to a destination network.

> If you have a monitor and keyboard connected to the system you can use the Console setup menu to configure static routes during the installation process, but we recommend using the web UI for all configuration tasks.

If you need a static route to reach portions of the network, from the **Network** screen:

1. Click **Add** in the **Static Routes** widget. The **Add Static Route** configuration screen displays.



2. Enter a value in **Destination**. Enter the destination IP address and CIDR mask in the format *A.B.C.D/E* where *E* is the CIDR mask.
3. Enter the gateway IP address for the destination address in **Gateway**.
4. (Optional) Enter a brief description for this static route, such as the part of the network it reaches.
5. Click **Save**.

Related Content

- Dashboard
- Network Interface Screens
- Adding Network Settings
- Managing Interfaces
- Console Setup Menu Configuration
- Global Configuration Screens
- Managing Network Global Configurations
- Setting Up a Network Bridge
- Static Route Screens
- Setting Up a Link Aggregation

3.2.5 - Setting Up IPMI

This article guides you through setting up Intelligent Platform Management Interface (IPMI) on TrueNAS SCALE.

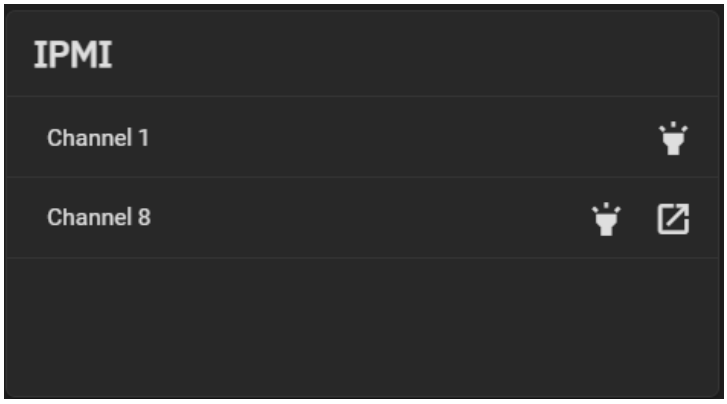
> IPMI requires compatible hardware! Refer to your hardware documentation to determine if the TrueNAS web interface has IPMI options.

Many TrueNAS Storage Arrays have a built-in out-of-band management port that provides side-band management should the system become unavailable through the web interface.

Intelligent Platform Management Interface (IPMI) allows users to check the log, access the BIOS setup, and boot the system without physical access. IPMI also enables users to remotely access the system to assist with configuration or troubleshooting issues.

> Some IPMI implementations require updates to work with newer versions of Java. See here for more information.

IPMI is configured in **Network > IPMI**. The IPMI configuration screen provides a shortcut to the most basic IPMI configuration.



IPMI Options

We recommend setting a strong IPMI password. IPMI passwords must include at least one upper case letter, one lower case letter, one digit, and one special character (punctuation, e.g. ! # $ %, etc.). It must also be 8-16 characters long. Document your password in a secure way!

After saving the configuration, users can access the IPMI interface using a web browser and the IP address specified in **Network > IPMI**. The management interface prompts for login credentials. Refer to your IPMI device documentation to learn the default administrator account credentials.

After logging in to the management interface, users can change the default administrative user name and create additional IPMI users. IPMI utility appearance and available functions vary by hardware.

Related Content

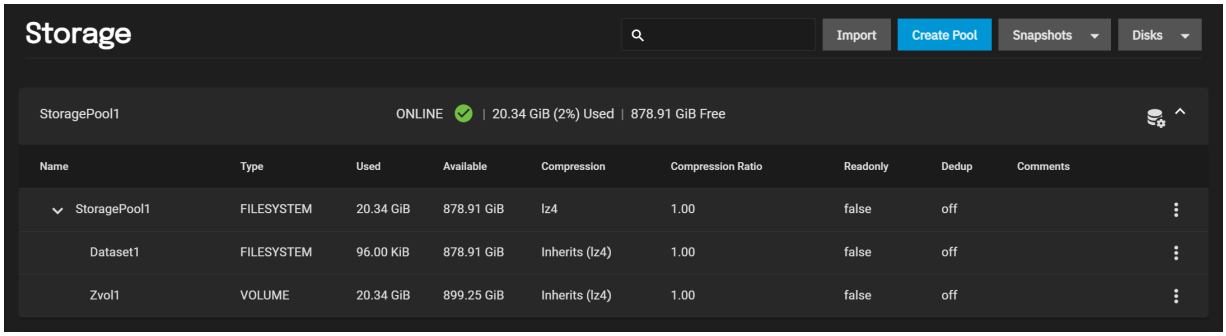
- SCALE Hardware Guide
- IPMI Screens

3.3 - Storage

The SCALE Storage section has controls for pool, snapshot, and disk management. The storage section also has options for datasets, zvols, and permissions.

For guidance on clustering storage across multiple SCALE systems, see (Clustering and Sharing SCALE Volumes with TrueCommand)[/solutions/integrations/smbclustering/].

Storage Overview



The top row of the SCALE storage screen lets users search for existing pools, datasets, and zvols.

The *Import* button lets users reconnect pools exported/disconnected from the current system or created on another system. The import button also reconnects pools after users reinstall or upgrade the TrueNAS system.

The *Create Pool* button creates ZFS data storage “pools” with physical disks to efficiently store and protect data.

The *Snapshots* drop-down creates snapshots, which provide read-only point-in-time copies of a file system, volume, or a running virtual machine.

The *Disks* drop-down lets users manage, wipe, and import storage disks that TrueNAS will use for ZFS data storage.

The Storage screen displays the pools, datasets, and zvols users have created on the system. Users may perform actions to root pools or specific datasets using the *Pool Actions* and *Dataset Actions* menus.

Ready to get started? Choose a topic or article from the left-side **Navigation** pane. Click the **<** symbol to expand the menu to show the topics under this section.

Storage Article Summaries

- Pools

  TrueNAS uses ZFS data storage pools to efficiently store and protect data. What is a pool? expand Storage pools are attached drives organized into virtual devices (vdevs). ZFS and TrueNAS periodically review and heal when discovering a bad block in a pool. Drives are arranged inside vdevs to provide varying amounts of redundancy and performance. Combined, ZFS and vdevs combined create high-performance pools, pools that maximize data lifetime, and all situations in between.

  - Creating Storage Pools

    This article provides information on creating storage pools and using Vdev layout options in TrueNAS SCALE.

  - Importing Storage Pools

    This article provides information on ZFS importing for storage pools in TrueNAS SCALE. It also addresses GELI-encrypted pools.

  - Managing Pools

    This article provides instructions on managing storage pools in TrueNAS SCALE.

  - Adding and Managing Datasets

    This article provides instructions on creating and managing datasets.

  - Adding and Managing Zvols

    This article provides instructions on how to create zvols.

  - Setting Up Permissions

This article provides instructions on viewing and edting ACL permissions, using the ACL editor screens, and general information on ACLs.

- Storage Encryption

  This article provides information on SCALE storage encryption for pools, datasets and zvols.

- Managing User or Group Quotas

  This article provides information on managing user and group quotas.

- SLOG Over-Provisioning

  This article provides information on the disk_resize command in SCALE.

- Fusion Pools

  Fusion Pools are also known as ZFS allocation classes, ZFS special vdevs, and metadata vdevs (Metadata vdev type on the Pool Manager screen.). What's a special vdev? expand A special vdev can store meta data such as file locations and allocation tables. The allocations in the special class are dedicated to specific block types. By default, this includes all metadata, the indirect blocks of user data, and any deduplication tables.

- Disks

  This section provides articles with instructions for importing, replacing, wiping disks. Disk Article Summaries Managing Disks This article provides information on managing disks, performing manual testing and S.M.A.R.T. test results. Importing Disks This article provides instructions for importing a disk and monitoring the import progress. Replacing Disks This article provides disk replacement instructions that includes offlining the failed disk and onlining the replacement disk.

  - Managing Disks

    This article provides information on managing disks, performing manual testing and S.M.A.R.T. test results.

  - Importing Disks

    This article provides instructions for importing a disk and monitoring the import progress.

  - Replacing Disks

    This article provides disk replacement instructions that includes offlining the failed disk and onlining the replacement disk.

  - Wiping a Disk

    This article provides instructions for wiping a disk.

- Creating and Managing Snapshots

  This article provides instructions on managing ZFS snapshots in TrueNAS Scale.

- Disks

  The Disks page displays the names, serial numbers, sizes, and pools of all the system’s physical drives. Users can customize disk columns using the Columns drop-down*. Clicking the the chevron_right in a disk’s row will expand it to show the traits specific to that disk. Managing Disks Managing Disks To manage disks, go to Storage and click Disks, then select Disks. The Disks page lets users edit disks, perform manual tests, and view S.

- Creating VMWare Snapshots

  This article provides instructions for creating ZFS snapshots when using TrueNAS as a VMWare datastore.

- Installing and Managing Self-Encrypting Drives

  This article covers self-encrypting drives, including supported specifications, implementing and managing SEDs in TrueNAS, and managing SED passwords and data.

3.3.1 - Pools

TruenAS uses ZFS data storage *pools* to efficiently store and protect data.

What is a pool?
Storage pools are attached drives organized into virtual devices (*vdevs*). ZFS and TrueNAS periodically review and *heal* when discovering a bad block in a pool. Drives are arranged inside vdevs to provide varying amounts of redundancy and performance. Combined, ZFS and vdevs combined create high-performance pools, pools that maximize data lifetime, and all situations in between.

Review Storage Needs

We strongly recommend users review the available system resources and plan the storage use case before creating a storage pool.

- Allocating more drives to a pool increases redundancy when storing critical information.
- Maximizing total available storage at the expense of redundancy or performance entails allocating large-volume disks and configuring a pool for minimal redundancy.
- Maximizing pool performance entails installing and allocating high-speed SSD drives to a pool.

Determining your specific storage requirements is a critical step before creating a pool.

Pool Article Summaries

The articles in this section provide information on setting up system storage, which includes adding, importing or mananging pools, adding or managing datasets and zvols.

Storage Articles

- Creating Storage Pools

  This article provides information on creating storage pools and using Vdev layout options in TrueNAS SCALE.

- Importing Storage Pools

  This article provides information on ZFS importing for storage pools in TrueNAS SCALE. It also addresses GELI-encrypted pools.

- Managing Pools

  This article provides instructions on managing storage pools in TrueNAS SCALE.

- Adding and Managing Datasets

  This article provides instructions on creating and managing datasets.

- Adding and Managing Zvols

  This article provides instructions on how to create zvols.

- Setting Up Permissions

  This article provides instructions on viewing and edting ACL permissions, using the ACL editor screens, and general information on ACLs.

- Storage Encryption

  This article provides information on SCALE storage encryption for pools, datasets and zvols.

- Managing User or Group Quotas

  This article provides information on managing user and group quotas.

- SLOG Over-Provisioning

  This article provides information on the disk_resize command in SCALE.

- Fusion Pools

  Fusion Pools are also known as ZFS allocation classes, ZFS special vdevs, and metadata vdevs (Metadata vdev type on the Pool Manager screen.). What's a special vdev? expand A special vdev can store meta data such as file locations and allocation tables. The allocations in the special class are dedicated to specific block types. By default, this includes all metadata, the indirect blocks of user data, and any deduplication tables.

3.3.1.1 - Creating Storage Pools

This article provides information on creating storage pools and using Vdev layout options in TrueNAS SCALE.

TrueNAS uses ZFS data storage *pools* to efficiently store and protect data.

What's a pool?
Storage pools attach drives organized into virtual devices called *vdevs*. ZFS and TrueNAS periodically review and *heal* when discovering a bad block in a pool. Drives arranged inside vdevs provide varying amounts of redundancy and performance. Combined, ZFS and vdevs combined create high-performance pools, pools that maximize data lifetime, and all situations in between.

Review Storage Needs

It is strongly recommend that you review the available system resources and plan the storage use case before creating a storage pool.

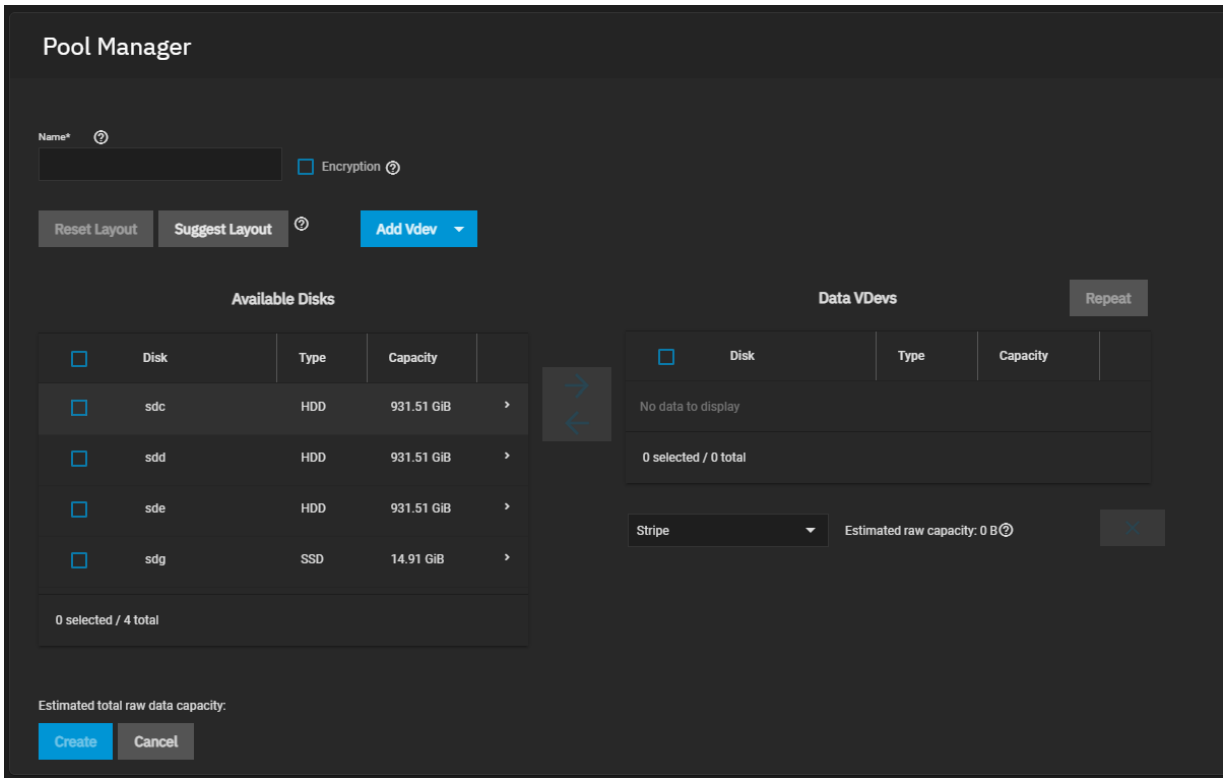
- Allocating more drives to a pool increases redundancy when storing critical information.
- Maximizing total available storage at the expense of redundancy or performance entails allocating large-volume disks and configuring a pool for minimal redundancy.
- Maximizing pool performance entails installing and allocating high-speed SSD drives to a pool.

Determining your specific storage requirements is a critical step before creating a pool.

Creating a Pool

Creating a Pool Tutorial

To create a new pool, go to **Storage** and click **Create Pool**.



First, enter a pool name.

Encryption?

TrueNAS offers several encryption algorithms to maximize security. However, encryption also complicates data retrieval and risks permanent data loss! Refer to the Encryption article for more details and decide if encryption is necessary for your use case before setting any **Encryption** option.

Next, configure the virtual devices (vdevs) that make up the pool.

> If the disks used have non-unique serial numbers, they do not populate the **Available Disks** section until you select the **Show disk with non-unique serial numbers** checkbox.

Suggested Layout

Clicking **Suggest Layout** allows TrueNAS to review all available disks and populate the primary **Data VDevs** with identically sized drives in a configuration balanced between storage capacity and data redundancy. Click **Reset Layout** to clear the suggestion.

To manually configure the pool, add vdevs according to your use case. Select the **Disk** checkboxes and click the ➔ to move the disks into a vdev.

> **Warning:** USB-connected disks might report their serial numbers inaccurately, making them indistinguishable from each other.

Vdev Types

Pools offer several vdev types. Vdevs store data or enable unique features for the pool.

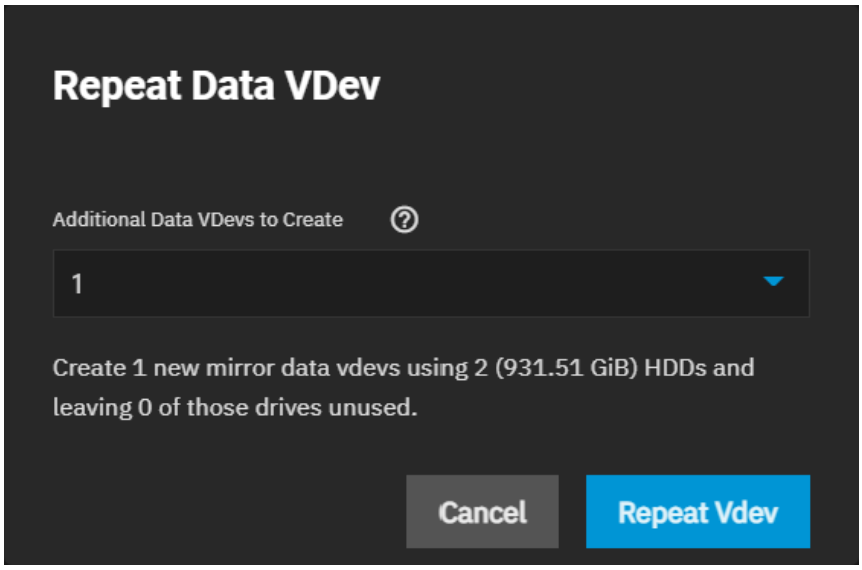
These store data or enable unique features for the pool:

Data

Standard vdev for primary storage operations. Each storage pool requires at least one data vdev. **Data** vdev configuration typically affects how the other kinds of vdevs get configured.

Duplicating a Data vdev

A **Data VDev** with disks is duplicated by clicking **REPEAT**. When more disks are available and equal in size, the **REPEAT** button creates another vdev with an identical configuration called a *mirror* of vdevs.



When even more same-size disks are available, you can create multiple copies of the original vdev.

> Don't have multiple data vdevs with different numbers of disks in each vdev. This complicates and limits the pool capabilities.

Cache

ZFS L2ARC read-cache used with fast devices to accelerate read operations. You can add or remove this after creating the pool.

Log
ZFS LOG device that improves synchronous write speeds. You can add or remove this after creating the pool.

Hot Spare

Hot Spare are drives reserved to insert into **Data** vdevs when an active drive fails. Hot spares are temporarily used as replacements for failed drives to prevent larger pool and data loss scenarios.

When you replace a failed drive with a new drive, the hot spare reverts to an inactive state and is available again as a hot spare.

If you only detach the failed drive from the pool, the temporary hot spare gets promoted to a full data vdev member and is no longer available as a hot spare.

Metadata
Special Allocation class used to create Fusion Pools for increased metadata and small block I/O performance.

Dedup
Dedup vdevs store ZFS de-duplication. Requires allocating *X* GiB for every *X* TiB of general storage. For example, 1 GiB of Dedup vdev capacity for every 1 TiB of Data vdev availability.

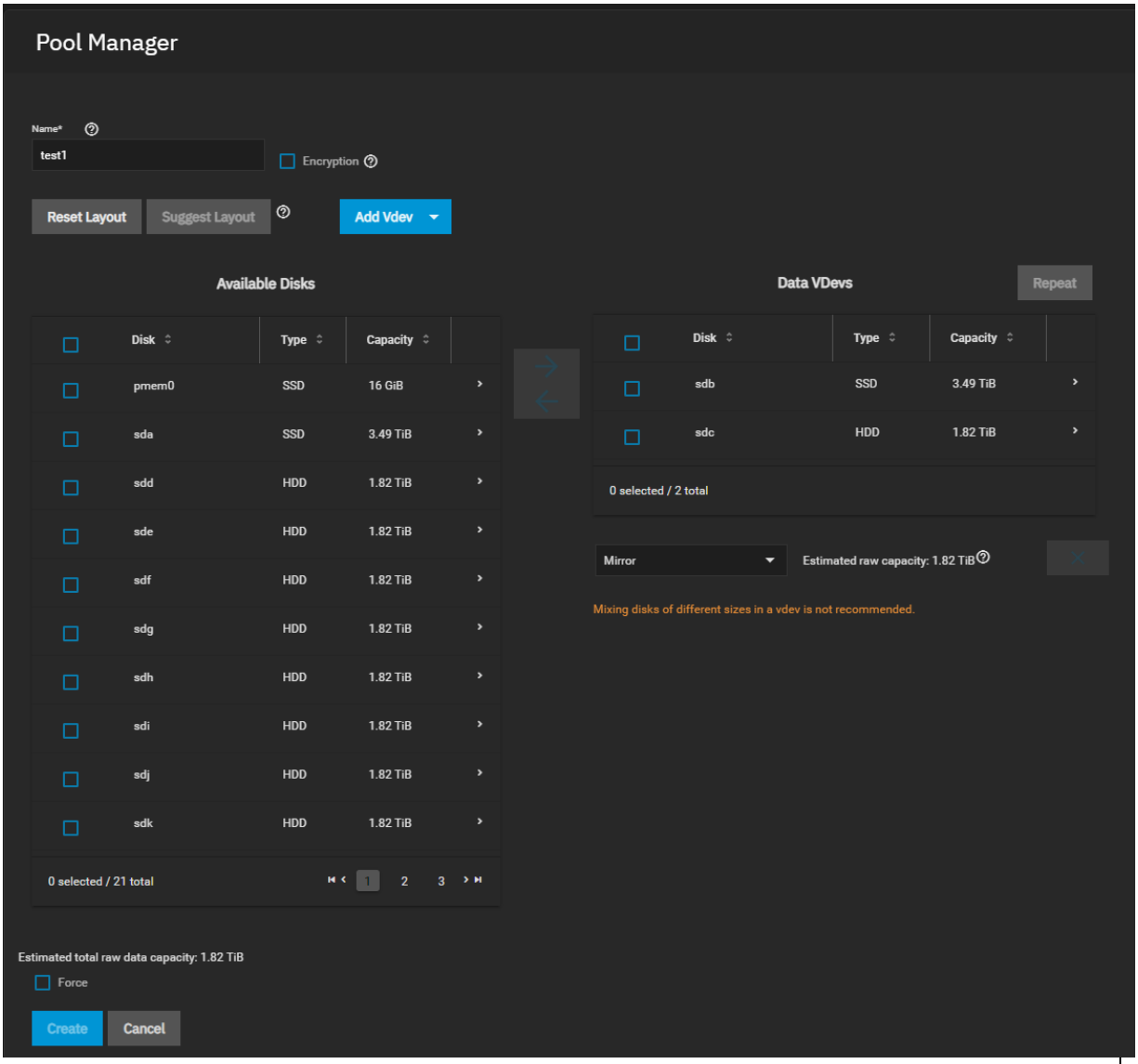
To add a vdev type during pool creation, click **Add Vdev** and select the type. Select disks from **Available Disks** and use the ➔ (right arrow) next to the new VDev to add it to that section.

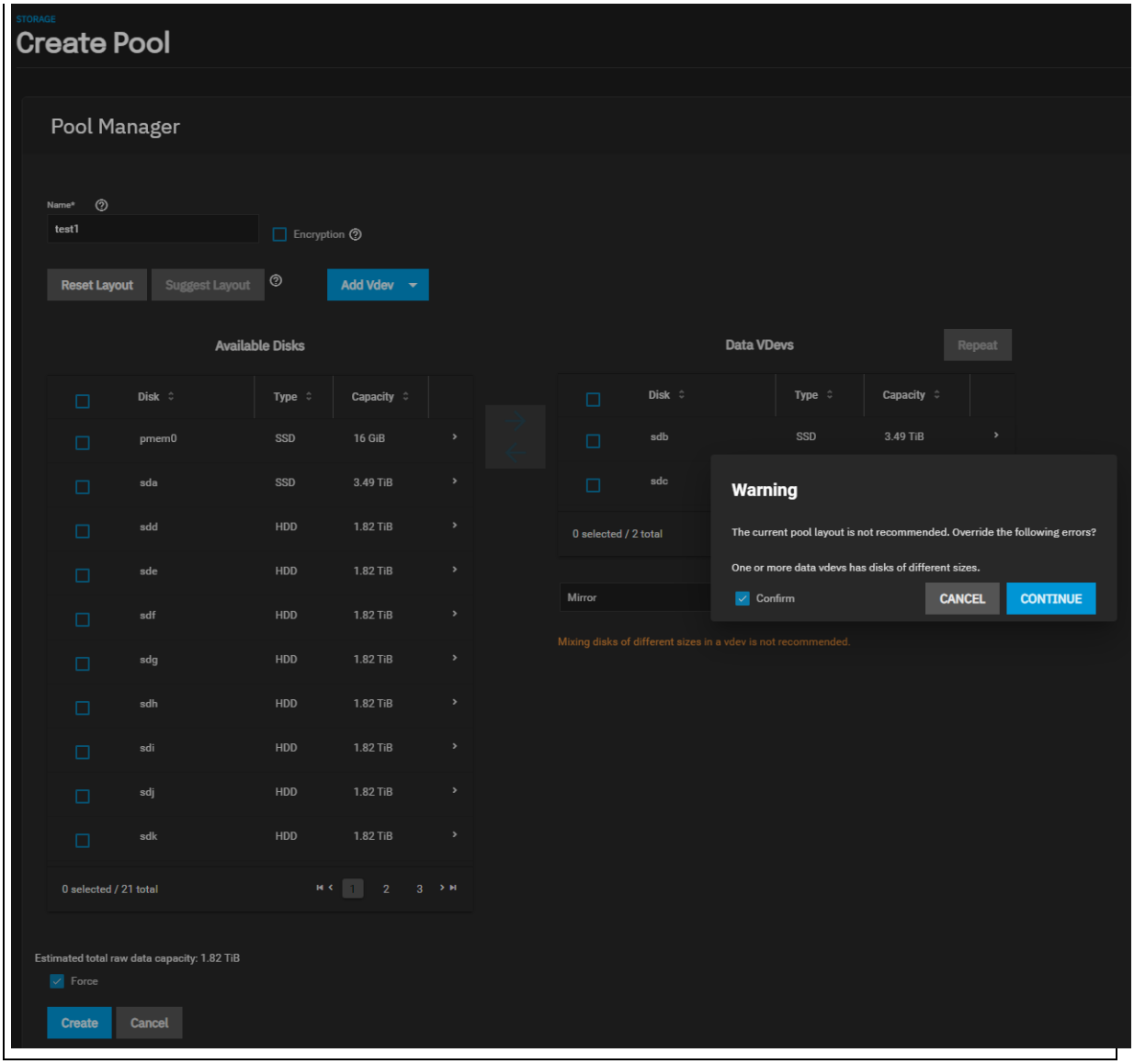
Vdev Layouts

Disks added to a vdev arrange in different layouts, according to the specific pool use case.

Can I use different-sized disks when creating a pool?

We do not recommend mixing disks of different sizes in a vdev. If you do, you must **Force** the action and override the **One or more data vdevs has disks of different sizes** error.


Pool Manager
Name*
test1
Encryption
Reset Layout
Suggest Layout
Add Vdev
Available Disks
Data VDevs
Repeat
Disk
Type
Capacity
pmem0 SSD 16 GiB
sda SSD 3.49 TiB
sdd HDD 1.82 TiB
sde HDD 1.82 TiB
sdf HDD 1.82 TiB
sdg HDD 1.82 TiB
sdh HDD 1.82 TiB
sdi HDD 1.82 TiB
sdj HDD 1.82 TiB
sdk HDD 1.82 TiB
0 selected / 21 total
1 2 3
sdb SSD 3.49 TiB
sdc HDD 1.82 TiB
0 selected / 2 total
Mirror
Estimated raw capacity: 1.82 TiB
Mixing disks of different sizes in a vdev is not recommended.
Estimated total raw data capacity: 1.82 TiB
Force
Create
Cancel



Can I create vdevs with different layouts in one pool?
TrueNAS SCALE does not support adding multiple vdevs with different layouts to a pool. Create a new pool when a different vdev layout is required. For example, *pool1* has a data vdev in a *mirror* layout, so create *pool2* for any *raid-z* vdevs.

Stripe

Each disk stores data. Requires at least one disk and has no data redundancy.

> Never use a **Stripe** type vdev to store critical data! A single disk failure results in losing all data in the vdev.

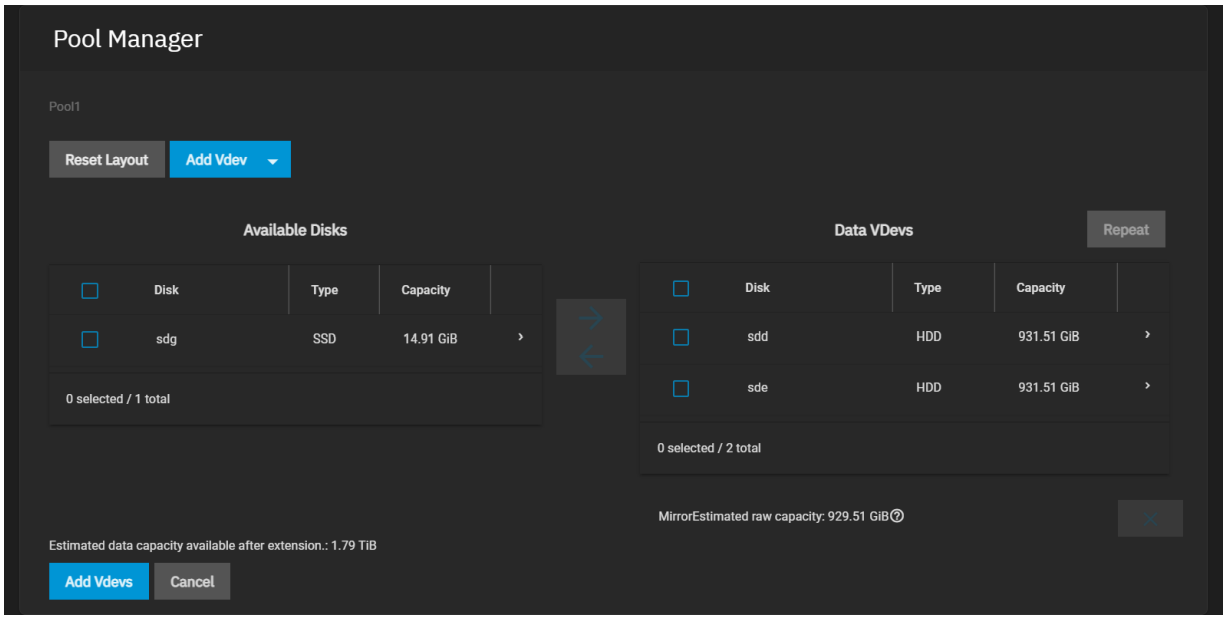
Mirror
Data is identical in each disk. Requires at least two disks, has the most redundancy, and the least capacity.

RAIDZ1
Uses one disk for parity while all other disks store data. Requires at least three disks.

RAIDZ2
Uses two disks for parity while all other disks store data. Requires at least four disks.

RAIDZ3
Uses three disks for parity while all other disks store data. Requires at least five disks.

The **Pool Manager** suggests a vdev layout from the number of disks added to the vdev. For example, if you add two disks, TrueNAS automatically configures the vdev as a Mirror. The total available storage is the size of one added disk while the other disk provides redundancy.



To change the vdev layout, open the **Data VDevs** list and select the desired layout.

Related Content

- Importing Storage Pools

Related Storage Articles

- Storage Screens
- Snapshots Screens
- Setting Up Storage
- Zvol Screens
- Edit ACL Screens
- Importing Storage Pools
- Adding and Managing Datasets
- Installing and Managing Self-Encrypting Drives
- Adding and Managing Zvols

3.3.1.2 - Importing Storage Pools

This article provides information on ZFS importing for storage pools in TrueNAS SCALE. It also addresses GELI-encrypted pools.

ZFS pool importing works for pools that are exported or disconnected from the current system, those created on another system, and for pools you reconnect after reinstalling or upgrading the TrueNAS system.

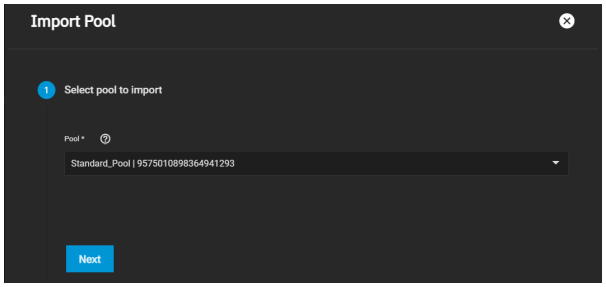
> The import procedure only applies to disks with a ZFS storage pool. To import disks with different file systems, see the SCALE Disks article.

Do I need to do anything different with disks installed on a different system?
When physically installing ZFS pool disks from another system, use the `zpool export poolname` command in the command line or a web interface equivalent to export the pool on that system. Shut that system down and move the drives to the TrueNAS system. Shutting down the original system prevents an **in use by another machine** error during the TrueNAS import.

To import a pool, go to **Storage** and click **Import**.

TrueNAS detects any pools that are present but unconnected.

Select a pool from the **Pool** dropdown list and click **Next**.



Review the Pool Import Summary and click **Import**.

Can I import GELI-encrypted pools?
Since GELI encryption is specific to FreeBSD, TrueNAS SCALE cannot import GELI-encrypted pools. See the **Migrating GELI-encrypted Pools to SCALE** section in the Installing SCALE article.

Related Content

- Creating Storage Pools

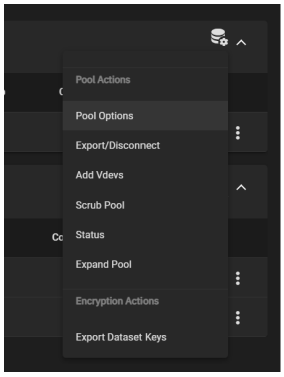
Related Storage Articles

- Storage Screens
- Snapshots Screens
- Setting Up Storage
- Zvol Screens
- Creating Storage Pools
- Edit ACL Screens
- Adding and Managing Datasets
- Installing and Managing Self-Encrypting Drives
- Adding and Managing Zvols

3.3.1.3 - Managing Pools

This article provides instructions on managing storage pools in TrueNAS SCALE.

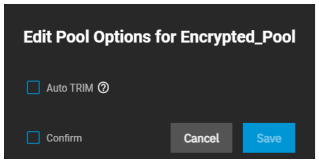
Use the **Pool Operations** icon button to manage a pool. Click to display the **Pool Actions** dropdown list.



The options on the **Pool Actions** dropdown list vary based on the pool setup. Only pools with encryption include the **Encryption Actions Export Dataset Keys** option.

Setting Up Auto TRIM

Select **Pool Options** to display the **Edit Pool Options** dialog for the selected pool.



Select **Auto TRIM**.

Select **Confirm** and then **Save**.

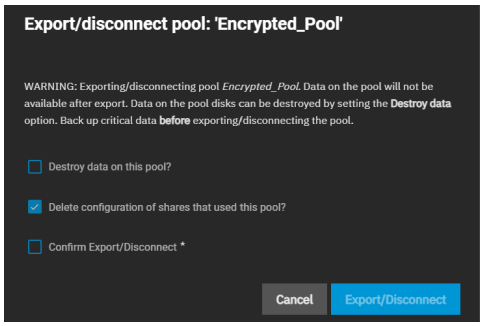
With **Auto TRIM** selected and active, TrueNAS periodically checks the pool disks for storage blocks it can reclaim. Auto TRIM can impact pool performance, so the default setting is disabled.

For more details about TRIM in ZFS, see the `autotrim` property description in zpool.8.

Exporting or Disconnecting a Pool

The **Export/Disconnect** option disconnects the pool to transfer drives to a new system where you can import the pool. Also use to completely delete the pool and any data stored on it.

Select **Export/Disconnect** on the **Pool Actions** dropdown list for the selected pool.



A dialog box displays with any system services affected by exporting the pool listed in the dialog.

Select **Destroy data on this pool?** to erase all data on the pool.

Click **Delete configuration of shares that used this pool?** to delete shares connected to the pool.

Adding Vdevs

ZFS supports adding vdevs to an existing ZFS pool to increase the capacity of the pool. Use **Add Vdevs** to expand the storage of an existing vdev. After creating a vdev, you cannot add more drives to that vdev but you can stripe a new vdev with another of the same type to increase the overall pool size. To extend a pool, you must add a vdev that is the same type as existing vdevs.

Vdevs extending examples:

- To make a striped mirror, add the same number of drives to extend a ZFS mirror. For example, you start with ten available drives. Begin by creating a mirror of two drives, and then extending the mirror by adding another mirror of two drives. Repeat this three more times until you add all ten drives.
- To make a stripe of two RAIDZ1 vdevs (similar to RAID 50 on a hardware controller), add another three drives to extend the three-drive RAIDZ1.
- To make a stripe of RAIDZ2 vdevs (similar to RAID 60 on a hardware controller), add another four drives to extend the four-drive RAIDZ2.
- To make a hot spare for a vdev, add a disk to the pool using **Hot Spare**.

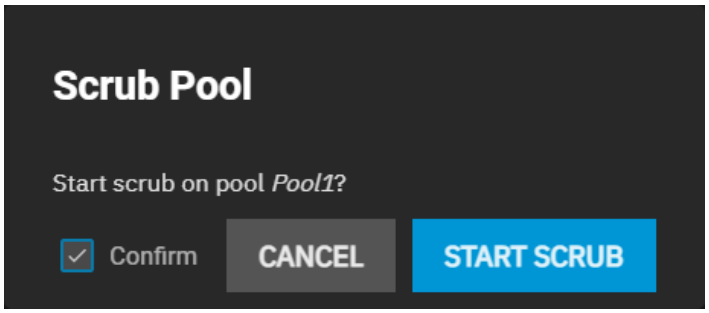
The **Add Vdevs** button opens the **Pool Manager** in the **Add Vdevs to Pool** screen.

> You cannot change the original encryption or data Vdev configuration.

TrueNAS selects data vdevs by default. To add different Vdev types to a pool, select one from the **Add Vdev** dropdown.

Using Scrub Pool

Use **Scrub Pool** to start a pool data integrity check.



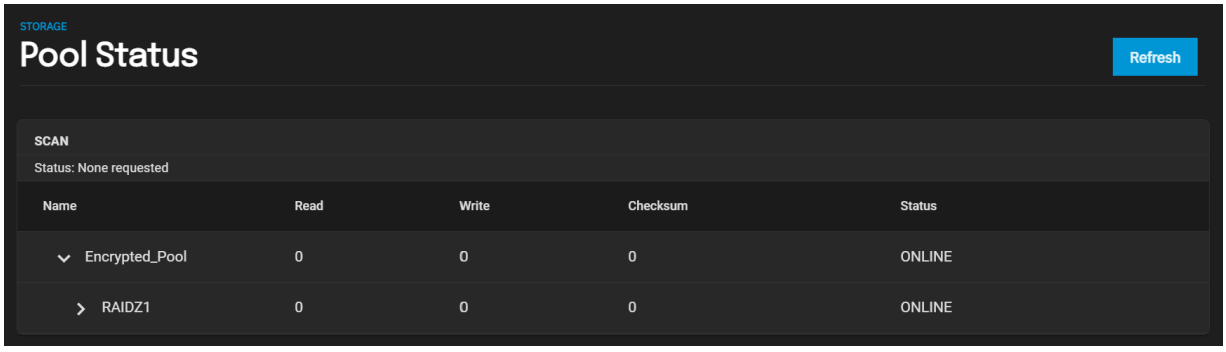
If TrueNAS detects problems during the scrub operation, it either corrects them or generates an alert in the web interface.

By default, TrueNAS automatically checks every pool on a reoccurring scrub schedule.

To check the state of the last scrub or disks in the pool, use **Status**.

Extending a Vdev

Click **Status** to open the **Pool Status** screen.



Use the ⋮ to display the options for a selected vdev. Click **Extend** to display the **Extend Vdev** dialog.

Select the disk from the dropdown list and click **Extend**.

Managing Pool Disks

The **Pool Status** screen disks also have disk management options.

See Replacing Disks for more information on the **Offline**, **Replace** and **Online** options.

Expand Pool

Click **Expand Pool** to increase the pool size to match all available disk space. An example is expanding a pool when resizing virtual disks apart from TrueNAS.

Related Content

- Dashboard
- Managing Advanced Settings
- Advanced Settings Screen
- View Enclosure Screen
- Setting Up Permissions
- Storage Encryption
- SLOG Over-Provisioning
- Fusion Pools

Related Storage Articles

- Storage Screens
- Snapshots Screens
- Setting Up Storage
- Zvol Screens
- Creating Storage Pools
- Edit ACL Screens
- Importing Storage Pools
- Adding and Managing Datasets
- Installing and Managing Self-Encrypting Drives
- Adding and Managing Zvols

3.3.1.4 - Adding and Managing Datasets

This article provides instructions on creating and managing datasets.

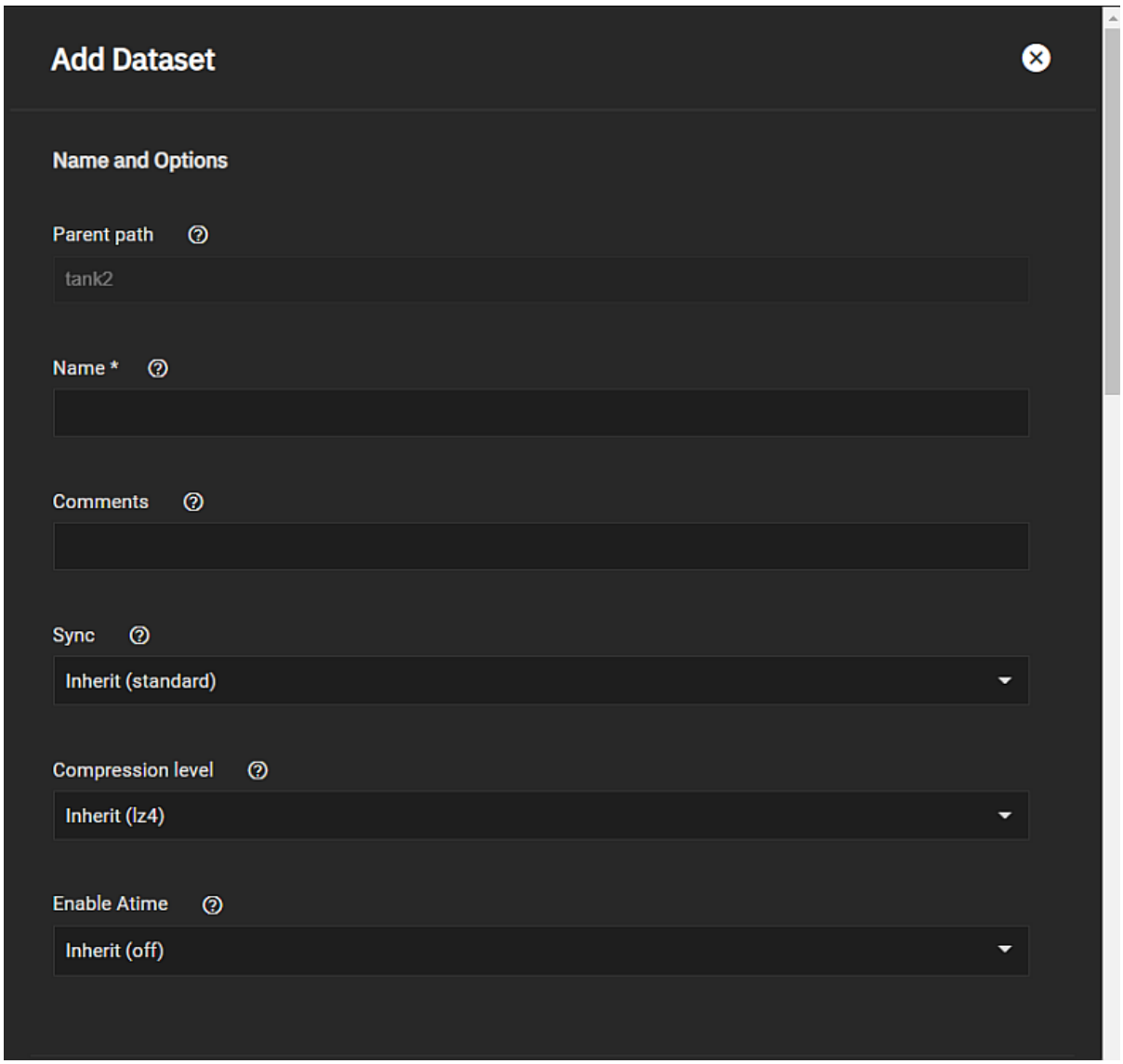
A TrueNAS dataset is a file system within a data storage pool. Datasets can contain files, directories (child datasets), and have individual permissions or flags. Datasets can also be encrypted, either using the encryption created with the pool or with a separate encryption configuration.

We recommend organizing your pool with datasets before configuring data sharing, as this allows for more fine-tuning of access permissions and using different sharing protocols.

Creating a Generic Dataset

To create a dataset using the default settings, go to **Storage**. Default settings includes settings datasets inherit from the parent dataset.

Select a dataset, pool (root) dataset or a child dataset, click the ⋮ and then select **Add Dataset**.



Enter a name and click **Save**.

Creating Custom Datasets

You can create datasets optimized for SMB shares or with customized settings for your dataset use cases.

> Review the **Share Type** and **Case Sensitivity** options on the configuration screen before clicking **Save**. You cannot change these settings and the **Name** setting after clicking **Save**.

Setting Dataset Compression Levels

Compression encodes information in less space than the original data occupies. We recommended you choose a compression algorithm that balances disk performance with the amount of saved space.

Select the compression algorithm that best suits your needs from the **Compression** dropdown list of options.

LZ4 maximizes performance and dynamically identifies the best files to compress. LZ4 provides lightning-fast compression/decompression speeds and comes coupled with a high-speed decoder. This makes it one of the best Linux compression tools for enterprise customers.

ZSTD offers highly configurable compression speeds, with a very fast decoder.

Gzip is a standard UNIX compression tool widely used for Linux. It is compatible with every GNU software which makes it a good tool for remote engineers and seasoned Linux users. It offers the maximum compression with the greatest performance impact. The higher the compression level implemented the greater the impact on CPU usage levels. Use with caution especially at higher levels.

ZLE or Zero Length Encoding, leaves normal data alone but only compresses continuous runs of zeros.

LZJB compresses crash dumps and data in ZFS. LZJB is optimized for performance while providing decent compression. LZ4 compresses roughly 50% faster than LZJB when operating on compressible data, and is greater than three times faster for uncompressible data. LZJB was the original algorithm used by ZFS but it is now deprecated.

Setting Dataset Quotas

Click **Advanced Options** to see the dataset quota management tools.

Setting a quota defines the maximum allowed space for the dataset. You can also reserve a defined amount of pool space to prevent automatically generated data like system logs from consuming all of the dataset space. You can configure quotas for only the new dataset or include all child datasets.

Define the maximum allowed space for the dataset in either the **Quota for this dataset**. Enter **0** to disable quotas.

Dataset quota alerts are based on the percentage of used storage. To set up a quota warning alert, enter a percentage value in **Quota warning alert at, %**. When consumed space reaches the defined percentage it sends the alert. To change the setting from the parent dataset warning level, clear the **Inherit** checkbox and then change the value.

To set up the quota critical level alerts, enter the percentage value in **Quota critical alert at, %**. Clear the **Inherit** checkbox to change this value to something other than using the parent alert setting.

When setting quotas or changing the alert percentages for both the parent dataset and all child datasets, use the fields under **This Dataset and Child Datasets**.

Enter a value in **Reserved space for this dataset** to set aside additional space for datasets that contain logs which could eventually take all available free space. Enter **0** for unlimited.

For more information on quotas, see Managing User or Group Quotas.

Changing Dataset Inherited Values

By default, many of dataset options inherit their values from the parent dataset. When the **Inherit** checkbox is selected, whatever setting has this checkbox selected uses the settings from the parent dataset. For example, the Storage Encryption settings.

To change any setting that can inherit the parent setting, clear the checkmark and then enter the desired setting values for the child dataset you are configuring.

Setting Datasets Access Controls

There are two **Add Dataset** or **Edit Dataset** screen ACL settings in the **Advanced Options** settings that you need to configure to use ACLs, **ACL Type** and **ACL Mode**.

You must select **NFSv4** in **ACL Type** before you can change the **ACL Mode** setting. The system changes the **ACL Mode** setting if you select **POSIX** in **ACL Type**.

Leave the **ACL Type Inherit** checkbox selected to preserve the ACL type from the parent dataset. For SCALE, which is based on Linux, use either **NFSv4** or **POSIX**. Warning dialogs display after selecting either setting. NFSv4 is richer than POSIX and is used to losslessly migrate Windows-style ACLs across Active Directory domains (or stand-alone servers). POSIX ACLs are a Linux-specific ZFS feature, used when an organization data backup target does not support native NFSv4 ACLs. Since the Linux

platform used POSIX for a long time, many backup products that access the server outside the SMB protocol cannot understand or preserve native NFSv4 ACLs.

> All datasets within an SMB share path must have identical ACL types

The **ACL Mode** setting determines how chmod behaves when adjusting file ACLs. See the zfs(8) `aclmode` property. When **ACL Type** is set to **NFSv4** you can select **Passthrough** to only update ACL entries related to the file or directory mode or **Restricted** which does not allow chmod to make changes to files or directories with a non-trivial ACL. An ACL is trivial if it can be fully expressed as a file mode without losing any access rules. When set to **Restricted** it optimizes a dataset for SMB sharing, but it can also require further optimizations. For example, configuring an rsync task with this dataset could require adding `--no-perms` in the task **Auxiliary Parameters** field.

For a more in-depth explanation of ACLs and configurations in TrueNAS SCALE, see our ACL Primer.

For more information on ACL settings see Setting Up Permissions.

Creating a Dataset for a Fusion Pool

Use the **Metadata (Special) Small Block Size** setting to set a threshold block size for including small file blocks into the special allocation class (fusion pools). Blocks smaller than or equal to this value are assigned to the special allocation class while greater blocks are assigned to the regular class. Valid values are zero or a power of two from 512B up to 1M. The default size **0** means no small file blocks are allocated in the special class. Before setting this property, you must add a special class vdev to the pool.

Managing Datasets

After creating a dataset, users can manage additional options by going to **Storage** and clicking the dataset ⋮ icon to display the **Dataset Actions** list. Each option is described in detail in the Storage Screens article.

Editing a Dataset

Select **Edit Options** to change the dataset configuration settings. You can change all settings except **Name**, **Case Sensitivity**, or **Share Type**.

The **Edit Dataset** screen settings are identical to the **Add Dataset** screen.

Editing Dataset Permissions

Select **View Permissions** on the **Dataset Actions** list of options to open the **Dataset Permissions** widget. Click ✎ to display the **Edit Permissions** screen with the **Unix Permissions Editor** you use to configure ACLs. For more information, see the permissions article.

Deleting a Dataset

Select **Delete Dataset** to remove the dataset, all stored data, and any snapshots from TrueNAS.

> Deleting datasets can result in unrecoverable data loss! Move or obsolete any critical data off the dataset before performing the delete operation.

Related Datasets Articles

- Advanced Settings Screen
- Edit ACL Screens
- User and Group Quota Screens
- Setting Up Permissions
- Storage Encryption
- Managing User or Group Quotas

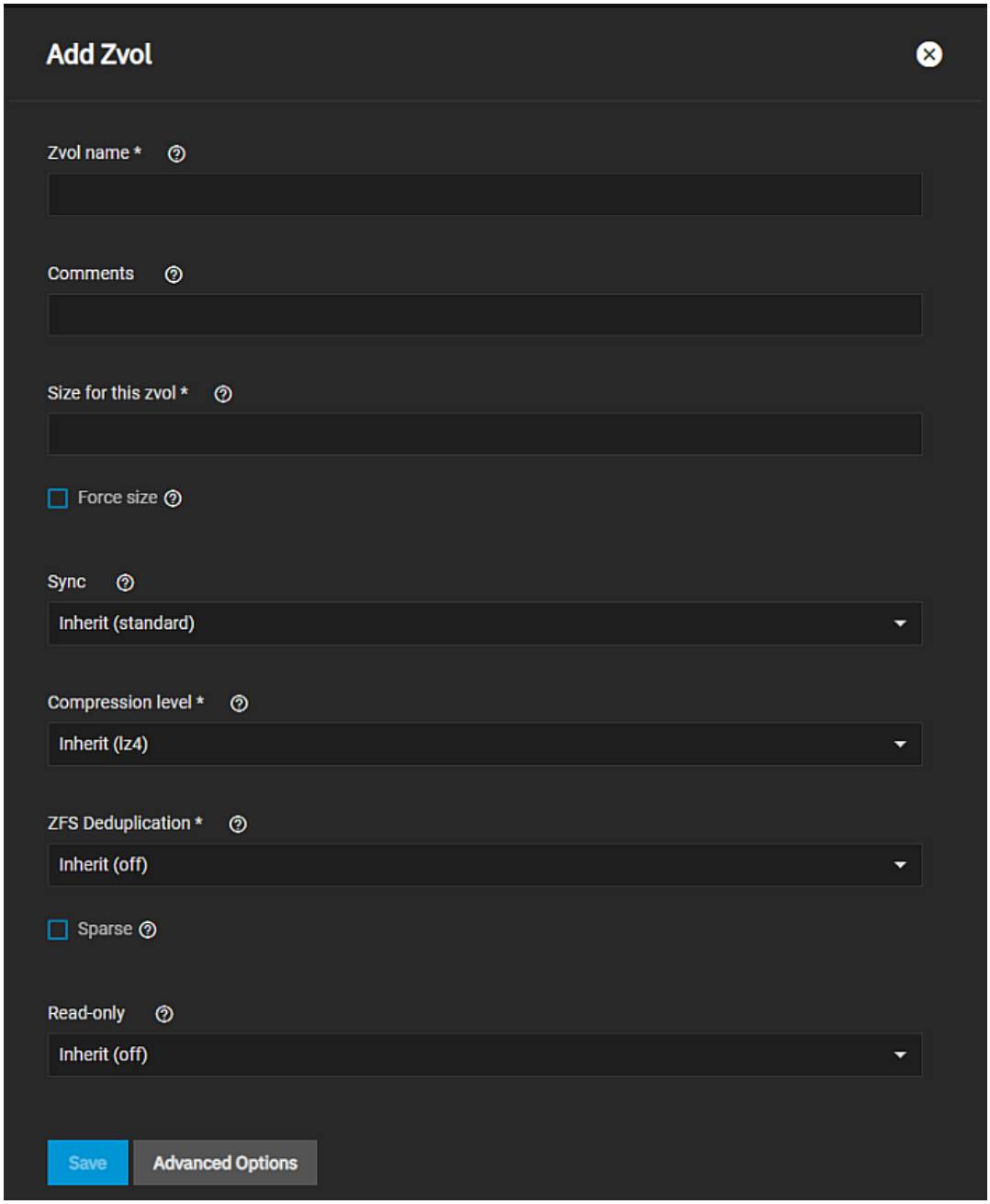
3.3.1.5 - Adding and Managing Zvols

This article provides instructions on how to create zvols.

A ZFS Volume (zvol) is a dataset that represents a block device. TrueNAS requires a zvol when configuring iSCSI Shares.

Adding a Zvol

To create a zvol in a pool, go to **Storage** and click ⋮ on a pool root dataset or child dataset, then select **Add Zvol**.



To create a zvol with default options, enter a name and size for the zvol and click **Save**.

Managing Zvols

To see zvol options, click ⋮ next to the desired zvol listed on the **Storage** screen:

- **Delete Zvol** removes the zvol from TrueNAS. Deleting a zvol also deletes all snapshots of that zvol.

> Deleting zvols can result in unrecoverable data loss! Remove critical data from the zvol or verify it is obsolete before deleting a zvol.

- **Edit Zvol** opens the **Edit Zvol** screen where you can change the saved settings. **Name** is read-only and you cannot change it.
- **Create Snapshot** opens a dialog where you can take a single, current point-in-time snapshot image of the zvol and saves it to the **Snapshots** screen. TrueNAS suggest a name and provides the option to include any child zvols of the selected zvol by selecting **Recursive**.

Cloning a Zvol from a Snapshot

If you clone a zvol from an existing snapshot, the cloned zvol that displays on the **Storage** screen includes the option to **Promote Dataset** on the **Zvol Actions** dropdown list. Click to promote the clone. A confirmation dialog displays.

After promoting a clone, the original volume becomes a clone of the promoted clone. Promoting a clone allows users to delete the volume that created the clone. Otherwise, you cannot delete a clone while the original volume exists.

When a zvol is the child of an encrypted dataset, TrueNAS offers additional **Encryption Actions**.

Related Content

- Zvol Screens

3.3.1.6 - Setting Up Permissions

This article provides instructions on viewing and edting ACL permissions, using the ACL editor screens, and general information on ACLs.

TrueNAS SCALE provides basic permissions settings and a full Access Control List (ACL) editor to define dataset permissions. ACL permissions control the actions users can perform on dataset contents.

> An Access Control List (ACL) is a set of account permissions associated with a dataset and applied to directories or files within that dataset. TrueNAS uses ACLs to manage user interactions with shared datasets and creates them when users add a dataset to a pool.

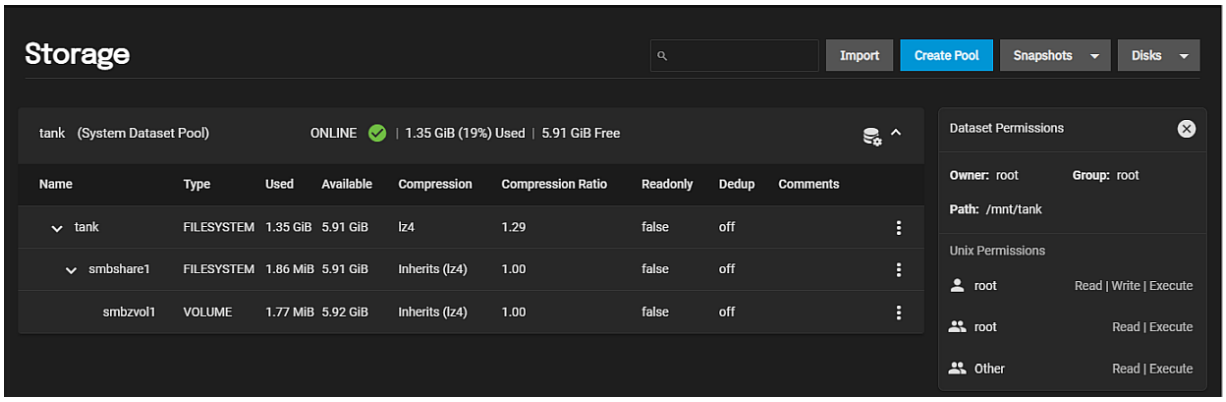
ACL Types in SCALE

TrueNAS SCALE offers two ACL types: POSIX which is the SCALE default, and NFSv4. For a more in-depth explanation of ACLs and configurations in TrueNAS SCALE, see our ACL Primer.

Viewing Permissions

Basic ACL permissions are viewable and configurable on both the **Add Dataset** and **Edit Dataset** screens. Click **Advanced Options** to access the **ACL Type** and **ACL Mode** settings.

Advanced ACL permissions are viewable on the **Dataset Permissions** widget, but only editable for non-root datasets.



Editing Basic ACL Settings

Click the ⋮ icon to display the **Dataset Actions** list of options, and then click **Add Dataset** to open the **Add Dataset** configuration screen, or click **Edit Options** to open the **Edit Dataset** configuration screen.

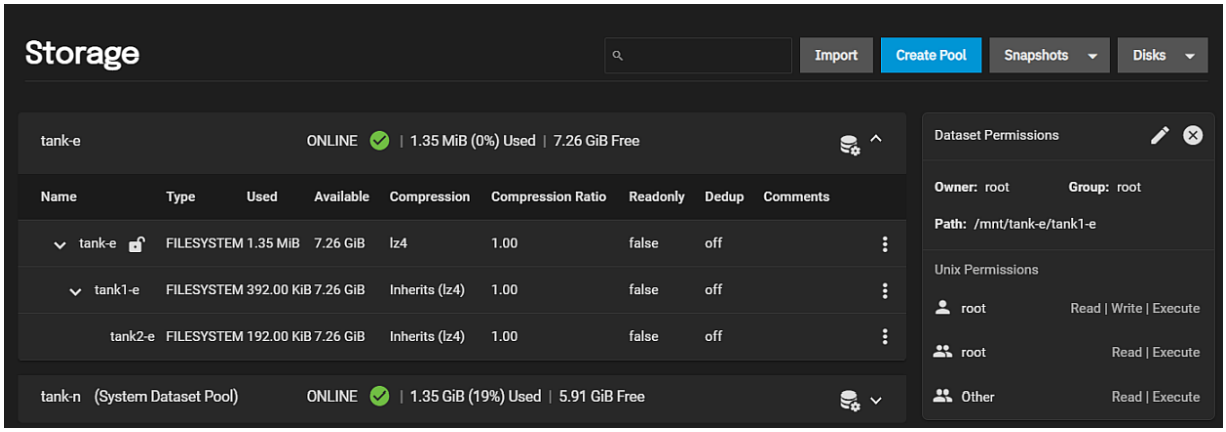
Click **Advanced Options** and scroll down to the **ACL Type** and **ACL Mode** settings.

First, select the **ACL Type** from the dropdown list. The option selected changes the **ACL Mode** setting.

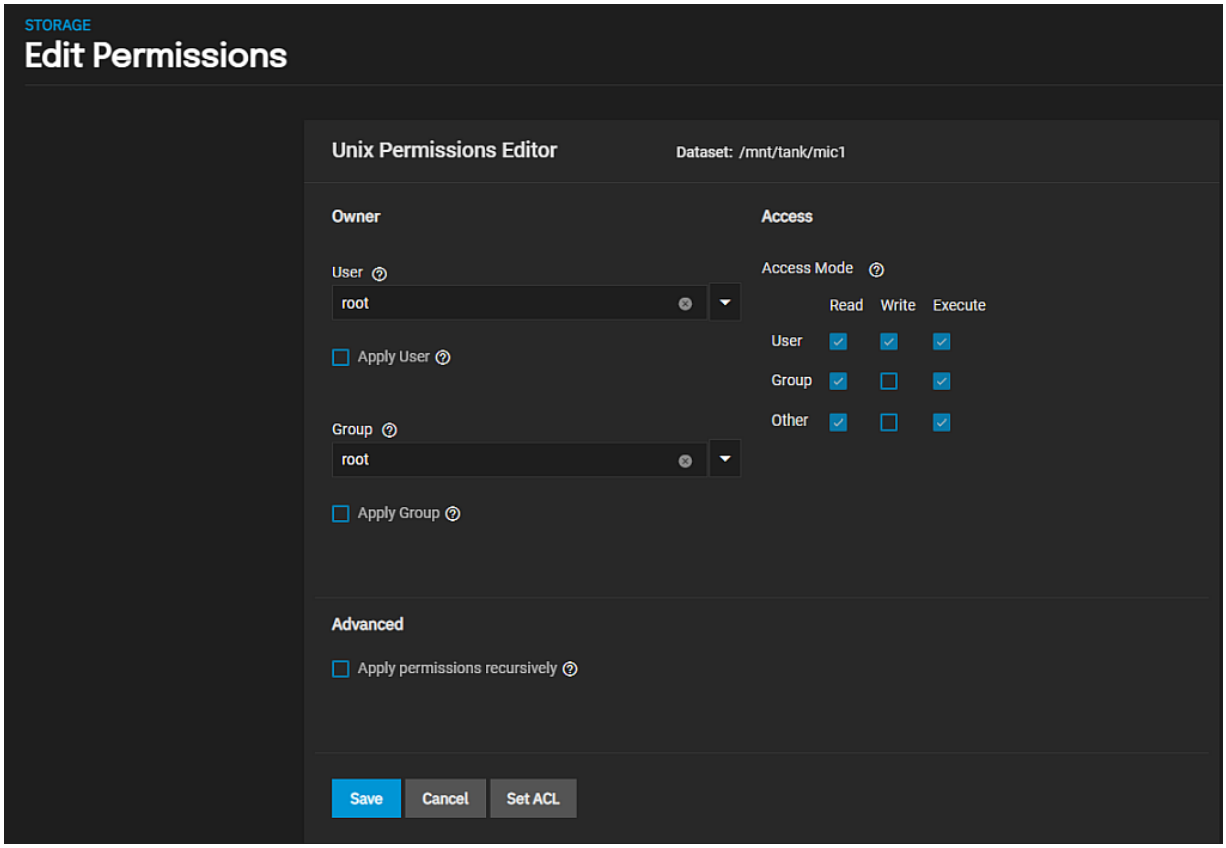
Editing ACL Permissions

> You can view permissions for any dataset but the edit option only displays on the **Dataset Permissions** widget for non-root datasets.
>
> Configuring advanced permissions overrides basic permissions configured on the add and edit dataset screens.

Click the ⋮ icon to display the **Dataset Actions** list of options for a non-root dataset, and then click **View Permissions**.



Click the **Edit** icon. The **Edit Permissions** screen displays with the **Unix Permissions Editor** configuration settings.



Enter or select the user from the dropdown list, set the read/write/execute permissions, and then select **Apply User**. The options include users created manually or imported from a directory service. Click **Apply User** to confirm changes. To prevent errors, TrueNAS only submits changes when selected.

> A common misconfiguration is removing the **Execute** permission from a dataset that is a parent to other child datasets. Removing this permission results lost access to the path.

Next enter or select the group from the dropdown list, set the read/write/execute permissions, and then select **Apply Group**. The options include groups created manually or imported from a directory service. Click **Apply Group** to confirm changes. To prevent errors, TrueNAS only submits changes when selected.

If you want to apply these settings to all child datasets, select **Apply permissions recursively**.

Click **Save** if you do not want to use an ACL preset.

Configuring an ACL Preset (NFSv4 ACL)

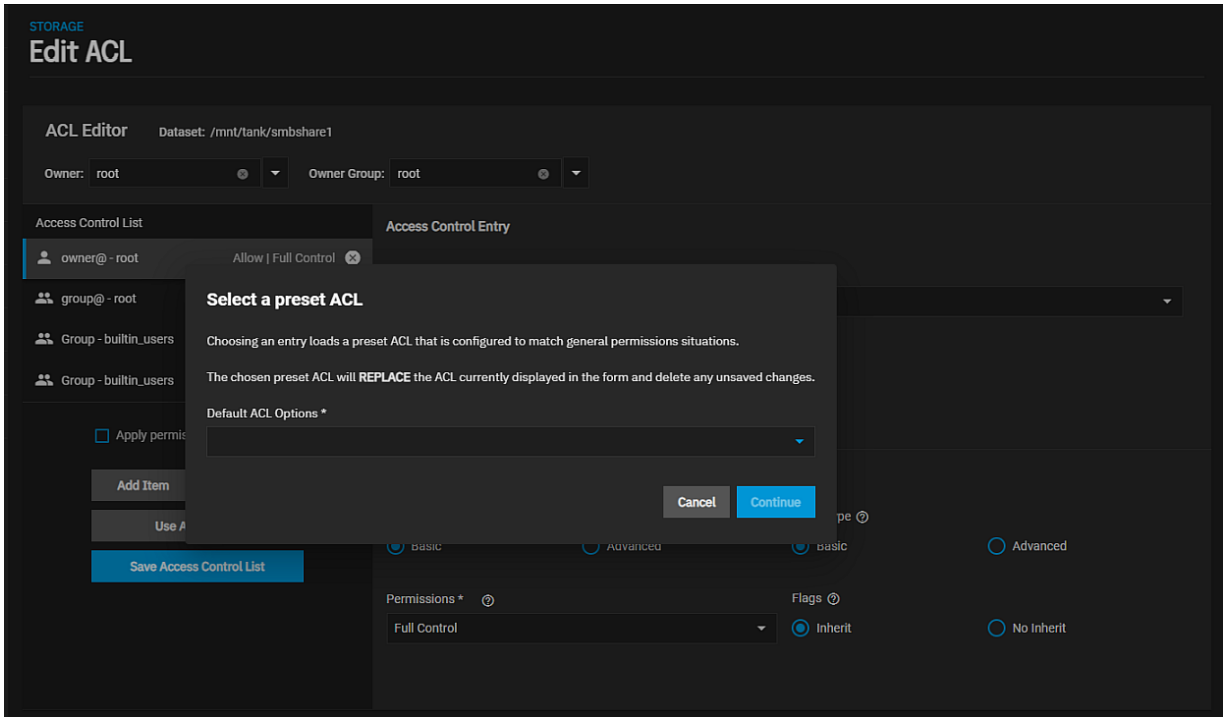
> WARNING: Changing the ACL type affects how TrueNAS writes and reads on-disk ZFS ACL.
>
> When the ACL type changes from POSIX to NFSv4, internal ZFS ACLs do not migrate by default, and access ACLs encoded in posix1e extended attributes convert to native ZFS ACLs.

> When the ACL type changes from NFSv4 to POSIX, native ZFS ACLs do not convert to posix1e extended attributes, but ZFS will use the native ACL for access checks.
>
> To prevent unexpected permissions behavior, you must manually set new dataset ACLs recursively after changing the ACL type.
>
> Setting new ACLs recursively is destructive. We suggest creating a ZFS snapshot of the dataset before changing the ACL type or modifying permissions.

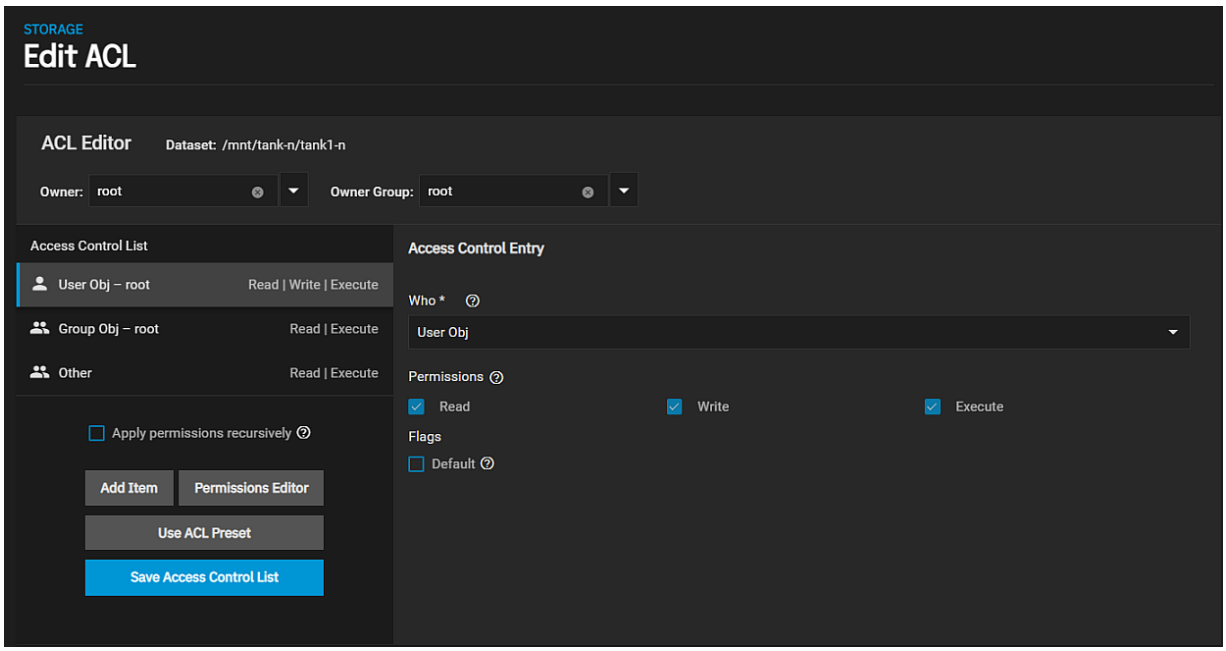
An ACL preset loads NFS4 pre-configured permissions to match general permissions situations.

From the **Unix Permissions Editor** configuration screen, click **Set ACL** to configure advanced NFS4 permissions. The If you want to use an ACL preset, click **Set ACL**. The **Edit ACL** screen displays with the **Select a preset ACL** dialog as the first step.

Click the **Select a present ACL** radio button to use a pre-configured set of permissions, and then select the preset you want to use from the **Default ACL Options** dropdown list, or click **Create a custom ACL** to configure your own set of permissions. Click **Continue**.



Each default preset loads different permissions to the **Edit ACL** screen. The **Create a custom preset** opens the **Edit ACL** screen with no default permission settings.



First select or type the name of the user in **Owner**. The owner controls which TrueNAS user and group has full control of this dataset.

Next select or type the name of the group in **Owner Group**.

Select the **Who** ACE value from the dropdown list and then select the **Permissions**. If you select **User** or **Group** you then select the name from **User** or **Group**. See nfs4_setfacl(1) NFSv4 ACL ENTRIES. Whatever you select in **Who** highlights the **Access Control List** entry on the left side of the screen.

Select **Flags** to specify how this ACE applies to newly created directories and files within the dataset. Basic flags enable or disable ACE inheritance. Advanced flags allow further control of how the ACE applies to files and directories in the dataset.

If you want to apply this preset to all child datasets select **Apply permissions recursively**.

To add another item to your ACL, click **Add Item**. To display the ACL presets window, click **Use ACL Preset**.

Click **Save Access Control List** when you finish configuring settings for the user or group in the **Who** field.

ACL Details from Shell

To view ACL information from the console, go to **System Settings > Shell** and enter:

```
getfacl /mnt/path/to/dataset
```

Related Content

- Managing SMB Shares
- Edit ACL Screens
- Adding and Managing Datasets

Related Dataset Articles

- Advanced Settings Screen
- Edit ACL Screens
- User and Group Quota Screens
- Adding and Managing Datasets
- Storage Encryption
- Managing User or Group Quotas

3.3.1.7 - Storage Encryption

This article provides information on SCALE storage encryption for pools, datasets and zvols.

TrueNAS SCALE offers ZFS encryption for your sensitive data in pools and datasets or zvols.

> Users are responsible for backing up and securing encryption keys and passphrases! Losing the ability to decrypt data is similar to a catastrophic data loss.

Data-at-rest encryption is available with:

- Self Encrypting Drives (SEDs) using OPAL or FIPS 140.2 (Both AES 256)
- Encryption of specific datasets (AES-256-GCM)

The local TrueNAS system manages keys for data-at-rest. Users are responsible for storing and securing their keys. TrueNAS SCALE includes the Key Management Interface Protocol (KMIP).

Pool Manager Encryption

> Encryption is for users storing sensitive data. Pool-level encryption does *NOT* apply to the storage pool or the disks in the pool. It only applies to the root dataset that shares the same name as the pool. Child datasets, or zvols, inherit encryption from the parent dataset unless you overwrite encryption when creating the child datasets or zvols.

Every pool has a root dataset automatically created when you create the pool. This root dataset indicates the encryption status for the pool. If you select the **Encryption** option on the it forces encryption for all datasets, zvols, and all data contained in that pool because encryption is inherited from the parent. You cannot add unencrypted datasets to an encrypted pool or root dataset for an encrypted pool.

If you leave the **Encryption** option clear on the **Pool Create > Pool Manager** screen that pool and the root dataset are not encrypted. You have the option to add an encrypted dataset under an unencrypted root dataset if you need to protect data with encryption. If you choose to add an encrypted dataset under an unencrypted root dataset, that new encrypted dataset becomes a “parent” for encryption for any dataset created from it. All child datasets, zvols, and all data in that storage branch inherits the encryption from that parent. The other datasets created from the unencrypted root dataset remain unencrypted unless you choose to add it again.

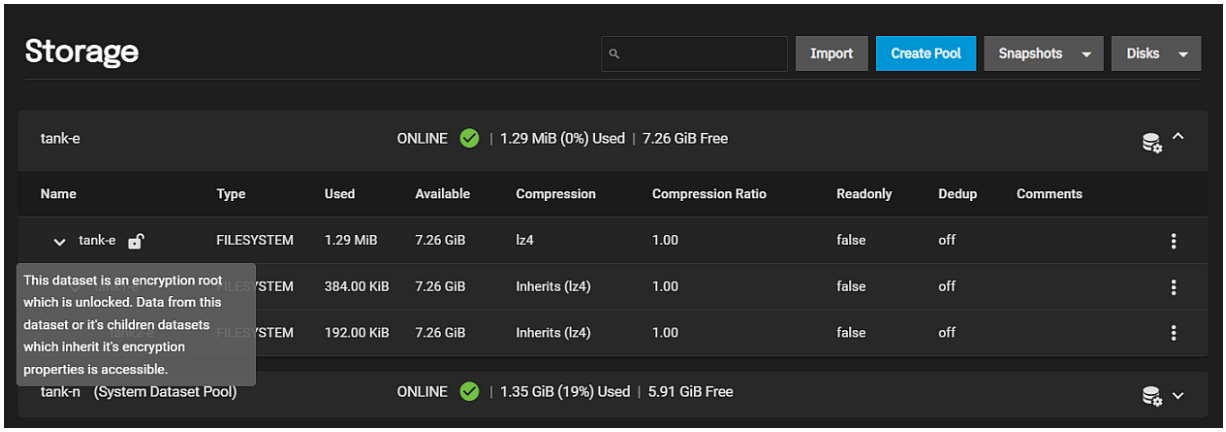
> You can only mix an encrypted dataset with an unencrypted dataset in a pool created without encryption at the pool level.

Encryption Visual Cues

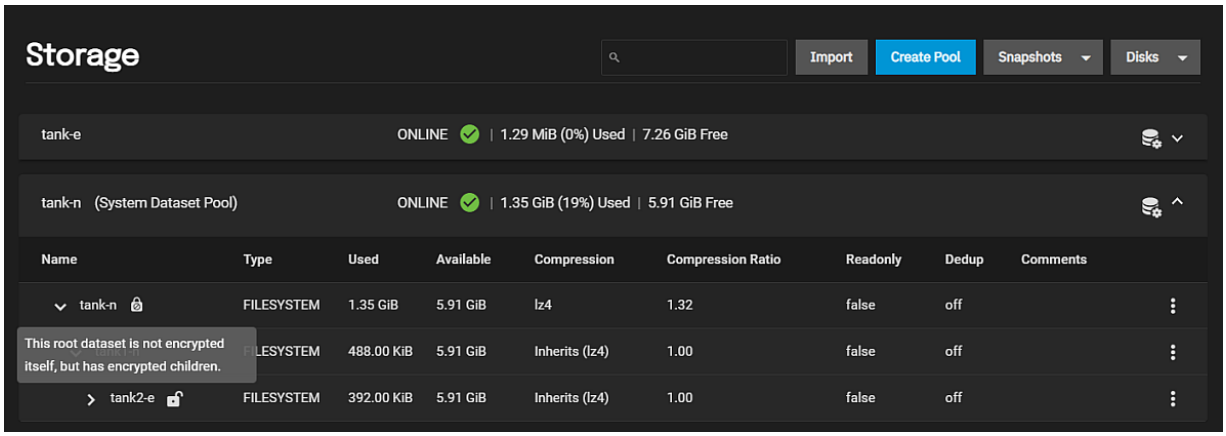
Pool and dataset encryption can be visually confusing in SCALE. SCALE uses three different lock-type icons that indicate the encryption state of a root or parent dataset and the pool. Each of these icons display text dialogs that explain the state of the dataset when you hover the mouse over it.

Lock Icon	Description
	Unlocked icon
	Locked icon
	No lock icon

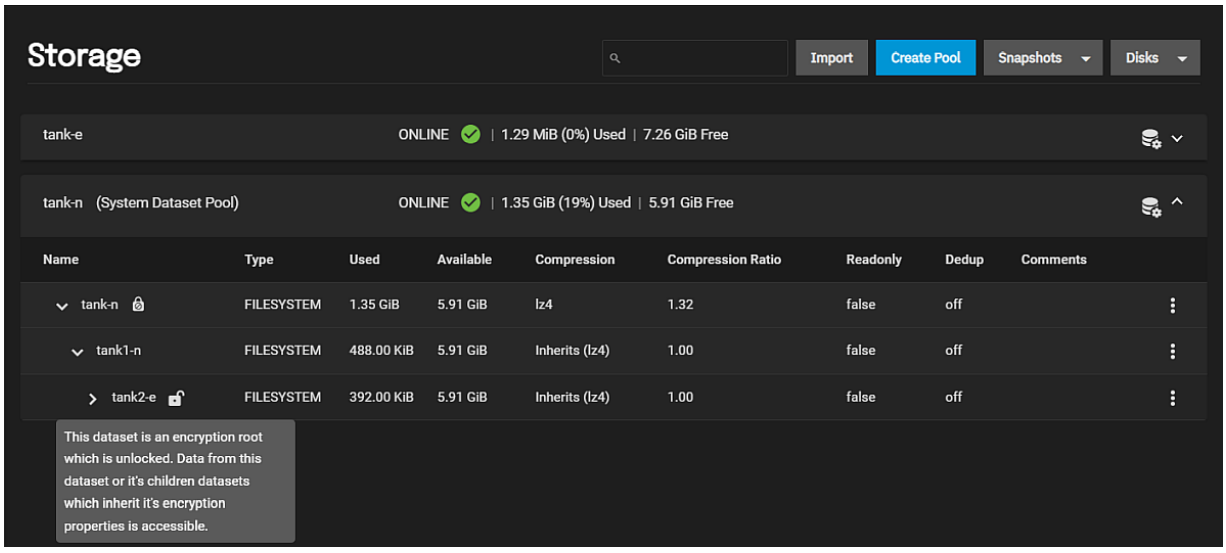
Because the root dataset inherits encryption from its parent, in this case the pool, the root dataset displays the lock icon that applies. Child datasets of the parent do not display a lock icon, so on the **Storage** screen you must look to the parent or root dataset to determine if the child is encrypted.



If the pool and root dataset are not encrypted they do not display a lock icon unless you create a new child dataset you encrypt. In this case, the root dataset displays the no-lock icon, the new encrypted child dataset displays the unlock icon.



This encrypted child dataset becomes a parent for all datasets created from it and those child datasets inherit the encryption the encrypted parent.



The encryption icon only displays on the root or for a child dataset that becomes parent-root dataset for encryption.

The dataset encryption state is unlocked until you lock it using the **Data Actions > Lock** option, and then the icon changes to the locked version.

Implementing Encryption

Before creating a pool with encryption make sure you want to encrypt all datasets and data stored on the pool.

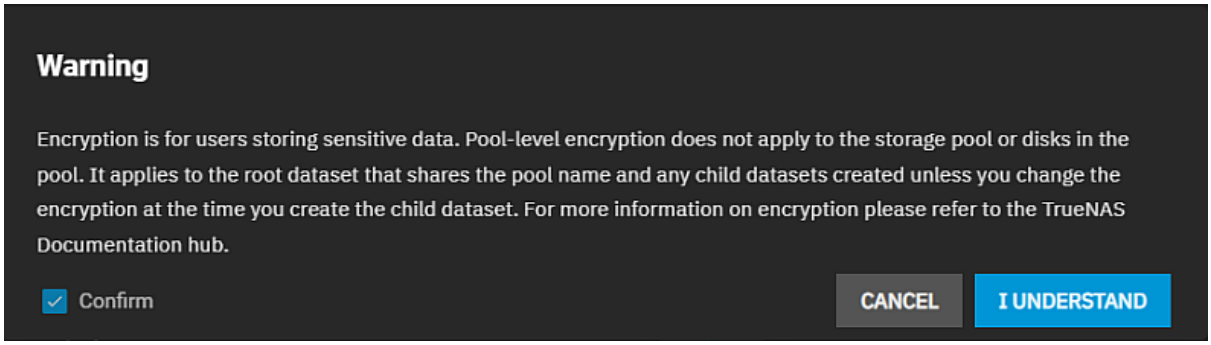
> You cannot change a pool from an encrypted to a non-encrypted, you can only change the encryption type for the datasets in the encrypted pool.

If your system does not have enough disks to allow you to create a second storage pool, it is recommend you not use encryption at the pool level. If you want to mix encrypted and unencrypted datasets, do no implement encryption at the pool level.

> All datasets created in an encrypted pool have encryption. You cannot create an unencrypted dataset in an encrypted pool.
>
> All pool-level encryption is key-based encryption. You cannot use passphrase encryption at the pool/root level.

Select **Encryption** on the **Create Pool > Pool Manager** screen.

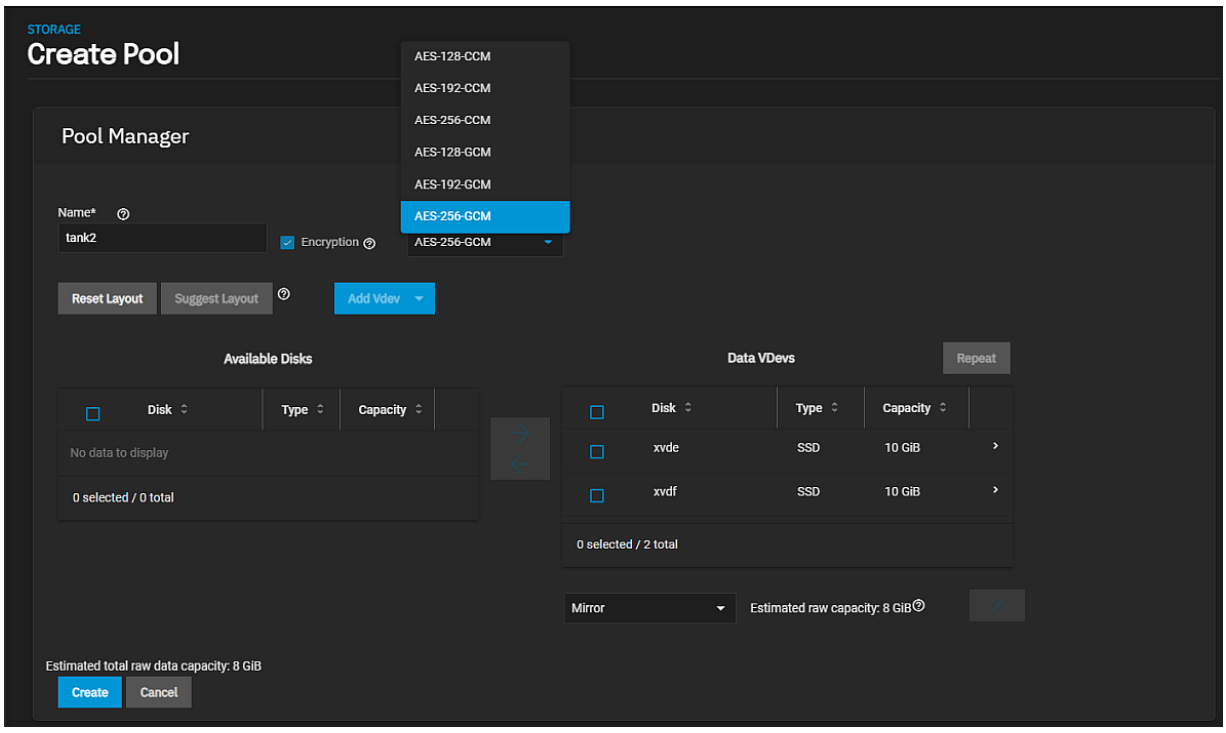
A warning dialog displays.



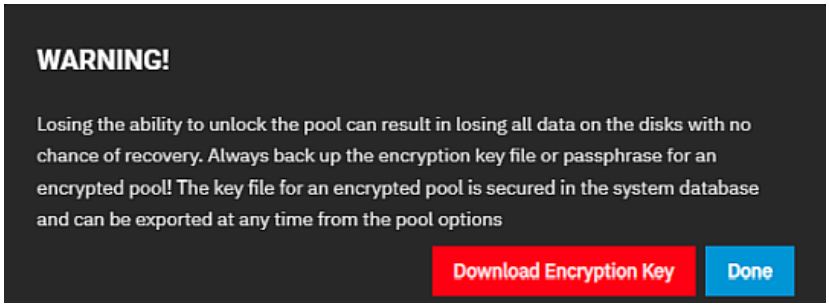
Read the warning, select **Confirm**, and then click **I UNDERSTAND**.

Select the encryption algorithm to use from the **Encryption Standard** dropdown list of options. Leave the default selection if you do not have a particular encryption standard you want use.

What are these options?
TrueNAS supports AES Galois Counter Mode (GCM) and Counter with CBC-MAC (CCM) algorithms for encryption. These algorithms provide authenticated encryption with block ciphers.



After clicking **Create**. The download encryption keys warning dialog displays. Click **Download Encryption Key** and then click **Done**. The root dataset on the **Storage** screen displays the unlocked encryption icon.



Move the downloaded key to safe location where you perform regular backups.

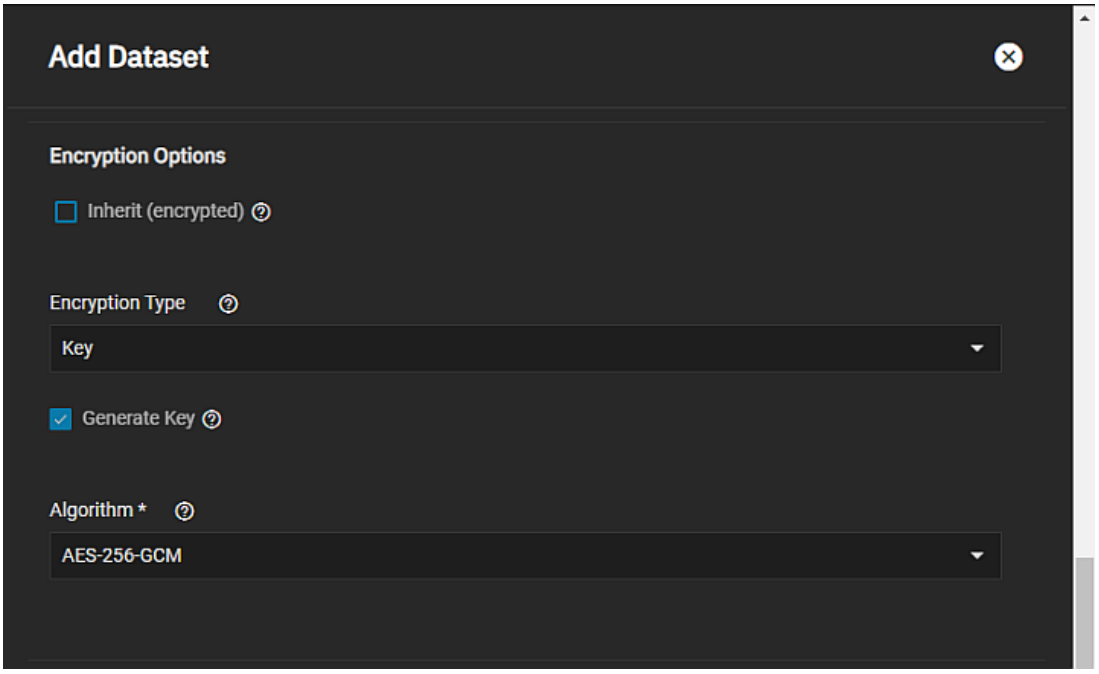
> Keep encryption keys and/or passphrases safeguarded in a secure and protected place. Losing encryption keys or passphrases can result in permanent data loss!

Adding an Encrypted Dataset to an Encrypted Pool

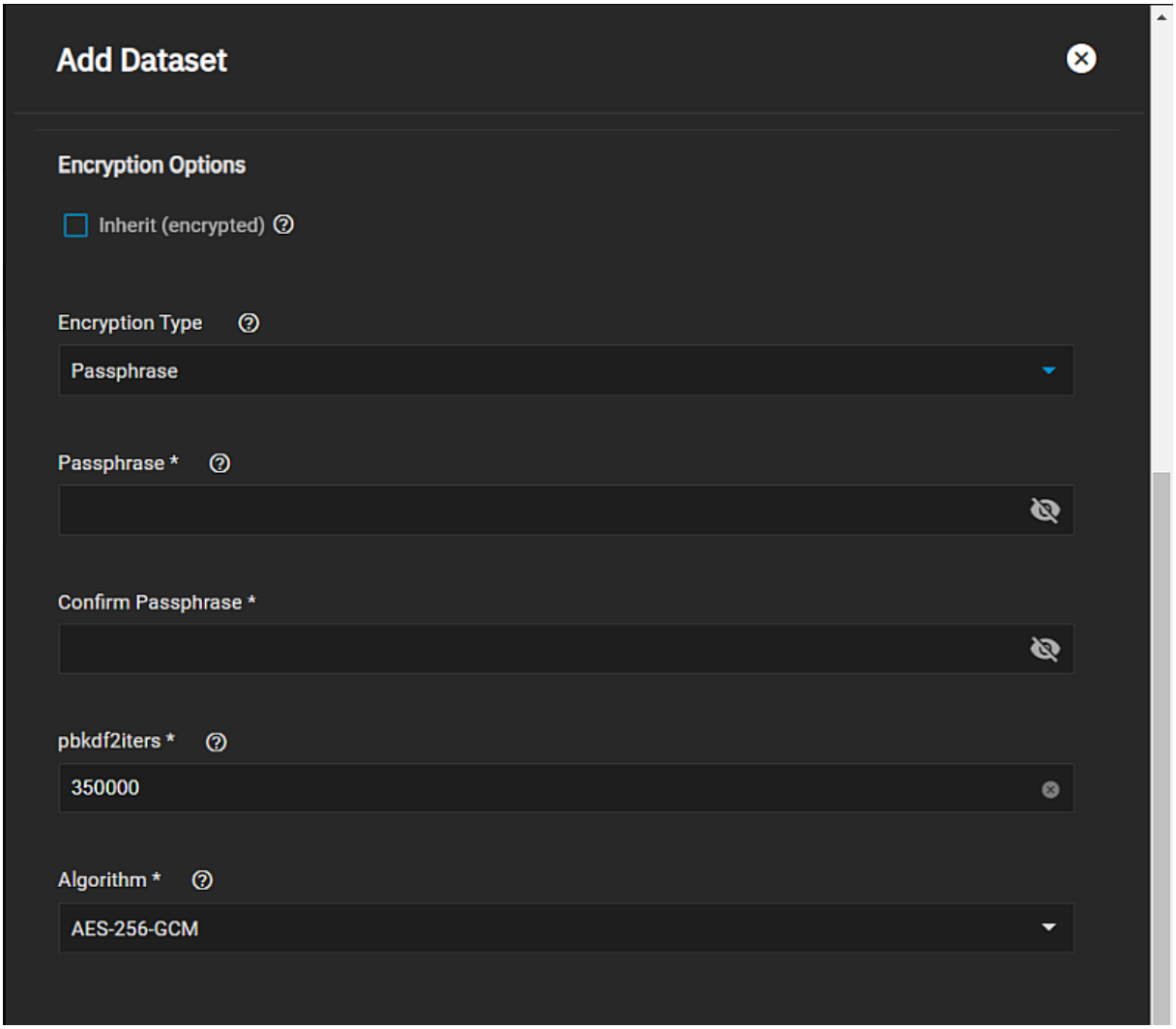
You can add a dataset to an encrypted root dataset on and encrypted pool using either key or passphrase-type encryption. The default is key-type encryption.

To create a child dataset with passphrase encryption:

1. Select the dataset ⋮ icon for where you want to create the new dataset. Click **Add Dataset**.
2. Enter a name for the dataset, scroll down to **Encryption Options** and clear the **Inherit (encryption)** checkmark. The **Encryption Options** displays the **Encryption Type** with **Key** as the option, the **Generate Key** selected and the **Algorithm** selected when you created the pool.



3. Select **Passphrase** from the **Encryption Type** dropdown list of options. The fields change to passphrase type encryption fields.



Enter the passphrase twice. Use a complex passphrase that is not easy to guess. Store in a secure location subject to regular backups.

> If you only want to change the encryption key and not change to a passphrase, clear the **Generate key** checkbox, and then enter the new key into the **Key** field.

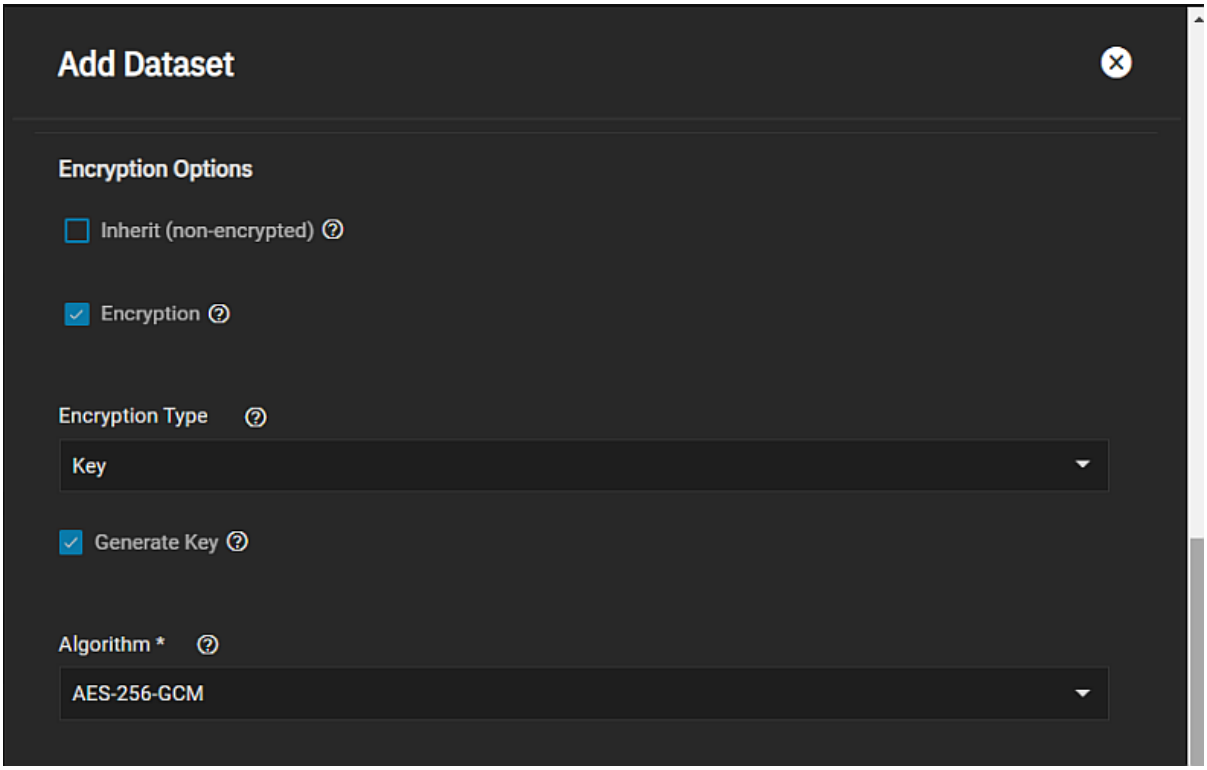
Adding an Encrypted Dataset to an Unencrypted Pool

You can mix encrypted datasets with unencrypted datasets if the pool is not encrypted. You can add an encrypted dataset from the root dataset, or you can add an encrypted dataset from dataset that is a child of the root dataset.

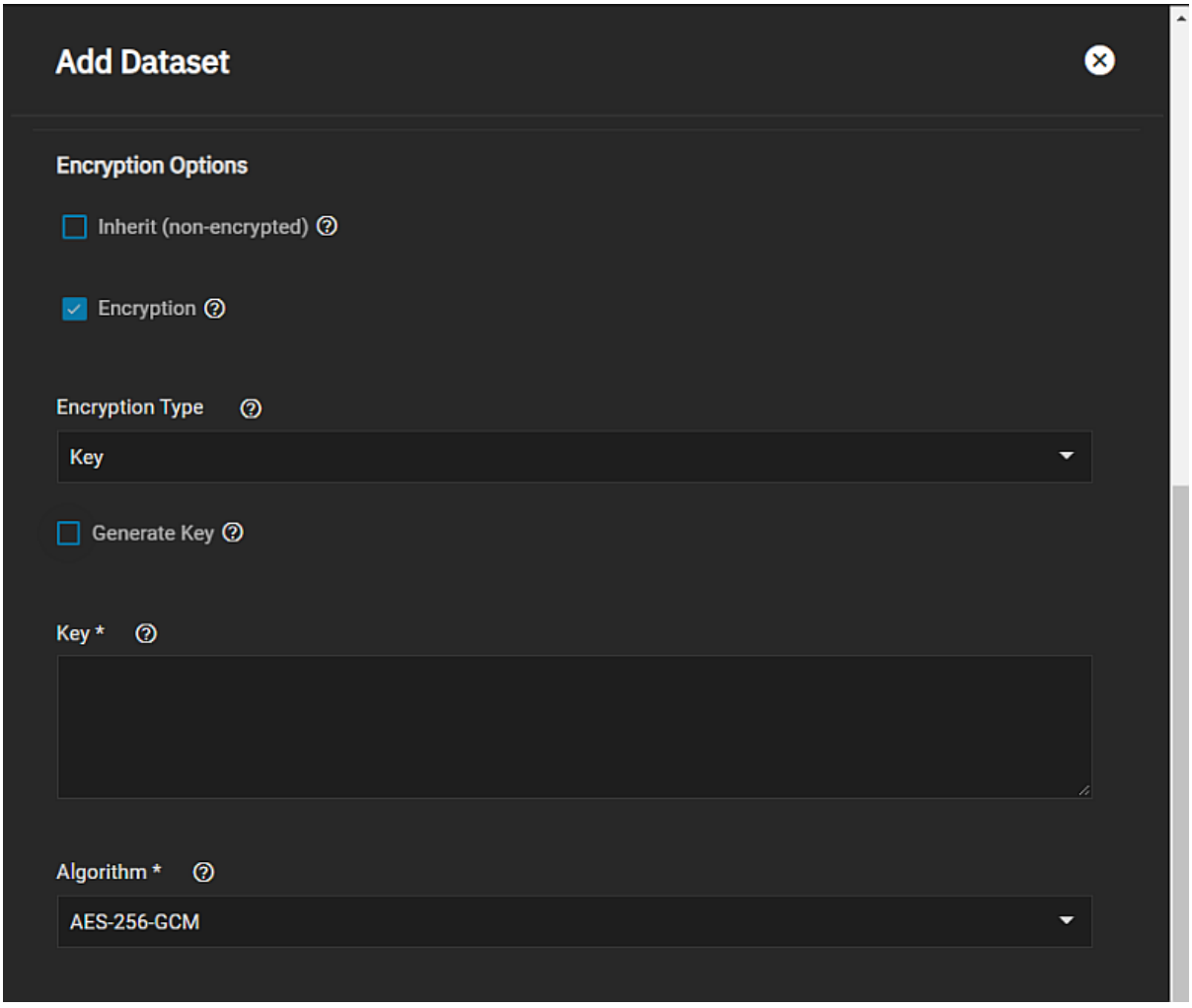
To add an encrypted dataset from an unencrypted dataset:

1. Select the dataset ⋮ icon for where you want to create the new dataset. Click **Add Dataset**.
2. Enter a name for the dataset, configure the settings you need, and scroll down to **Encryption Options**.
3. Clear the **Inherit (non-encryption)** checkbox.

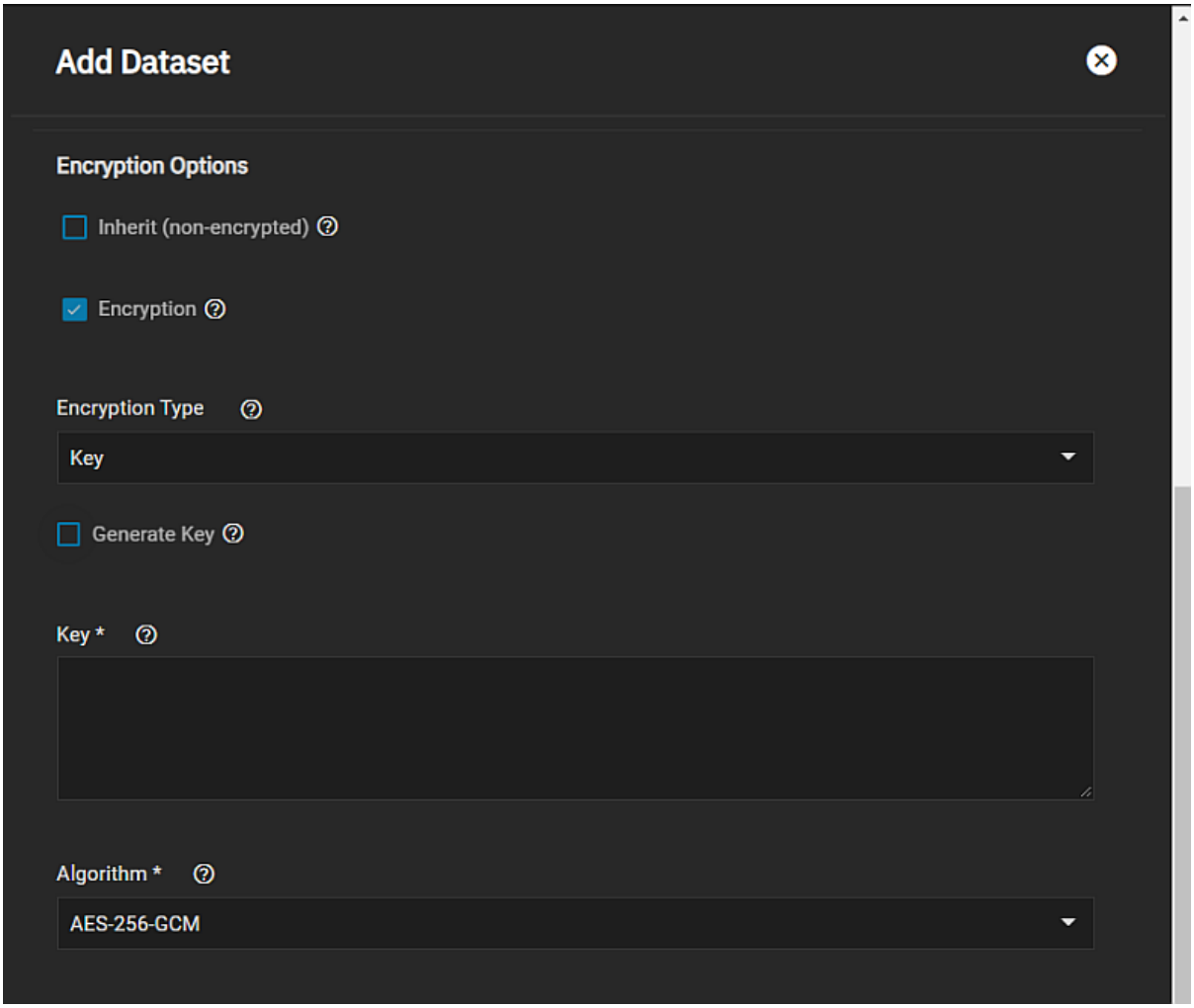
   The **Encryption Type** fields for **Key** display with **Generate Key** selected and the **Algorithm** populated with the default.



(Optional) Clear the **Generate Key** checkbox to enter the encryption key of your choice in the **Key** field.



(Optional) Select **Passphrase** in **Encryption Type** to use a passphrase instead of a key. Choose a complex passphrase not easily guessed and enter it twice.



4. (Optional) Select a new encryption standard from the **Algorithm** dropdown list or use the default iXsystems value provided.
5. Configure the other settings you want or need for your dataset and then click **Save**

The **Storage** screen displays the dataset with the unlocked encryption icon and adds the no encryption icon to the root dataset. This indicates the pool and root dataset do not have encryption. See the image for adding an encrypted dataset to an unencrypted pool in Encryption Visual Cues above.

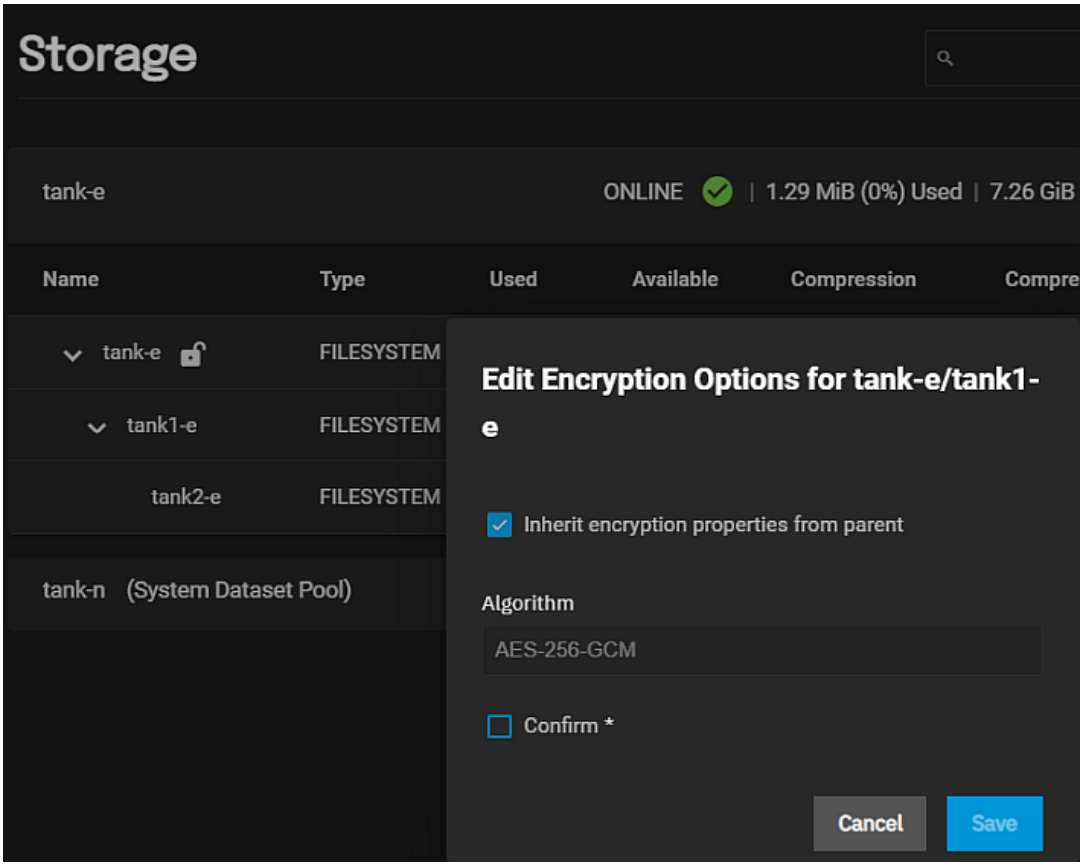
Changing Dataset-Level Encryption

A dataset created from an encrypted root dataset on and encrypted pool has key-type encryption by default. The root dataset for the pool is created with key-type encryption. Use this procedure to change from key-type encryption to passphrase-type, or from a system-generated key to one you enter . If you add a dataset to a non-encrypted pool and want to change the encryption type, you can also use this procedure to change the encryption type.

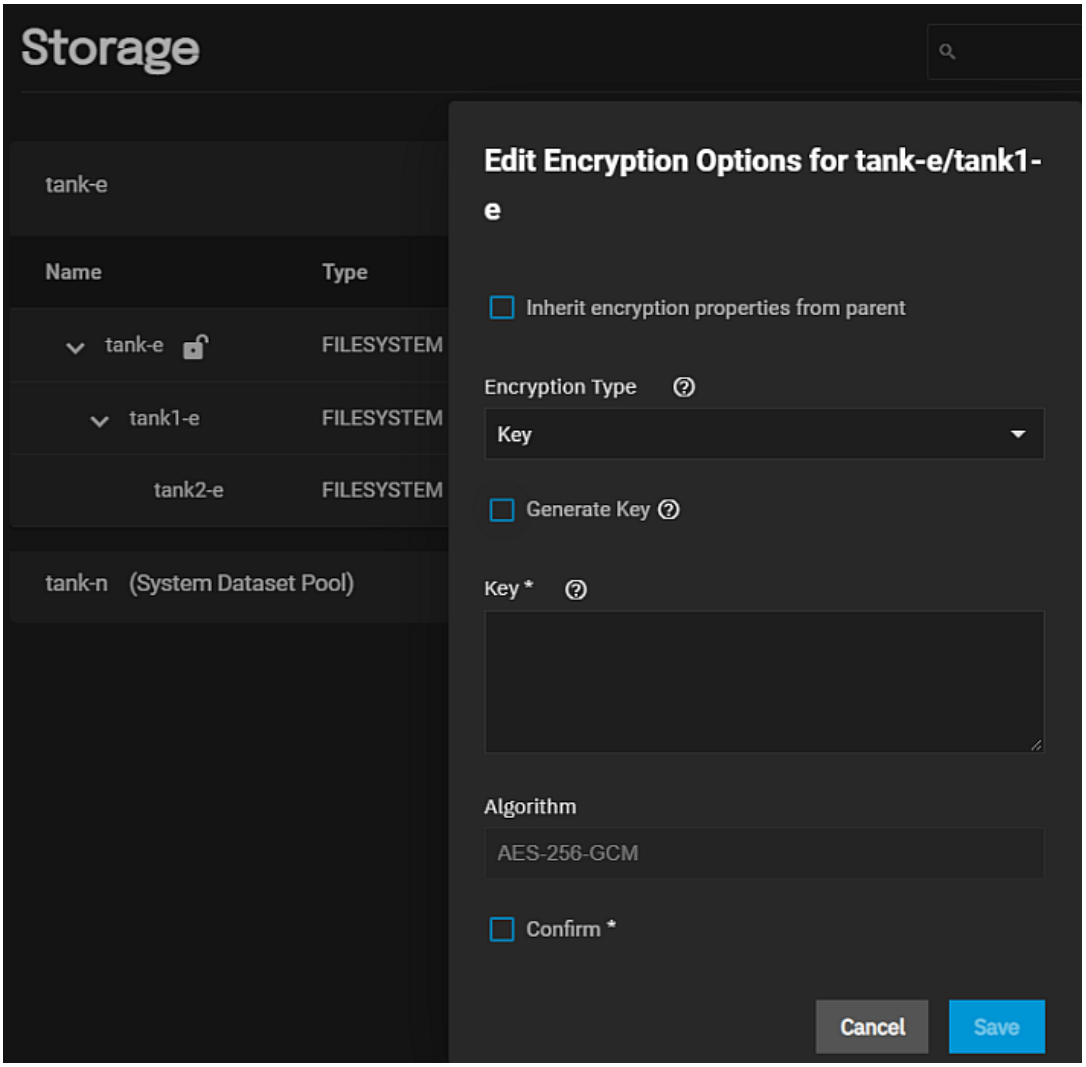
> Save any change to the encryption key or passphrase, and update your saved passcodes and keys file, and then back up that file.

To change the encryption type:

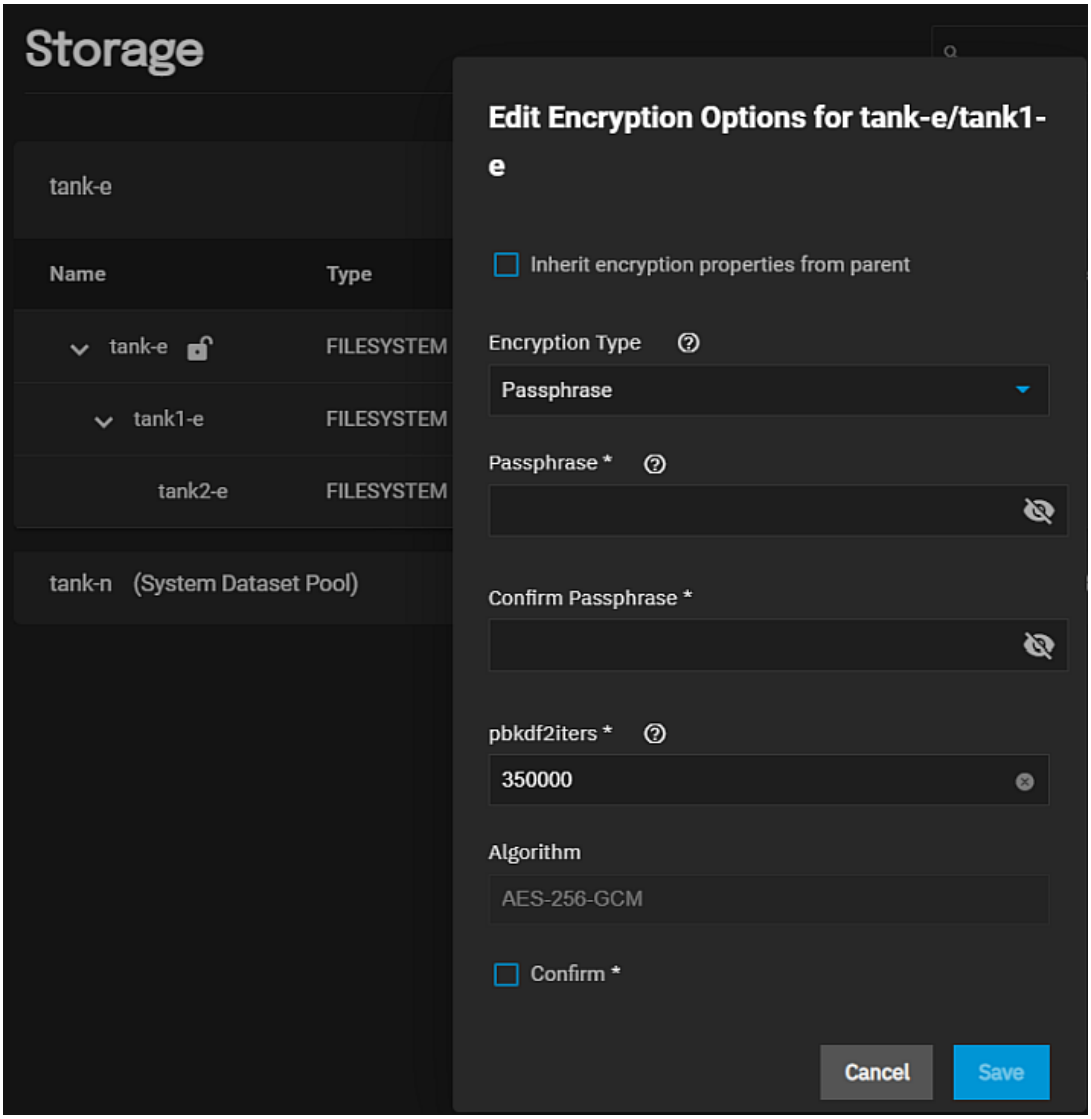
1. Select the dataset ⋮ icon for where you want to create the new dataset. Click **Edit Options**. The **Edit Encryption Options** dialog for the selected dataset (with encryption) displays.



2. Clear the **Inherit encryption properties from parent** checkmark. The dialog displays **Key** as the **Encryption Type** with the **Generate Key** and the **Algorithm** options used when you created the pool.



3. Select **Passphrase** from the **Encryption Type** dropdown list of options. The fields change to passphrase type encryption fields.



Enter the passphrase twice. Use a complex passphrase that is not easy to guess. Store in a secure location subject to regular backups.

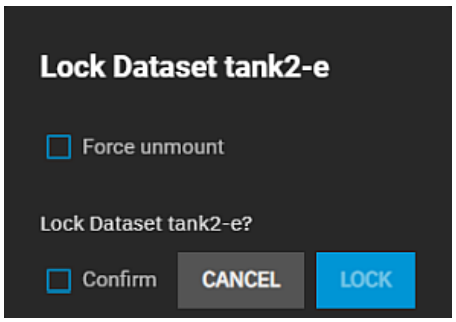
If you only want to change the encryption key to one of your choosing, clear the **Generate key** checkbox and then either the new key into the **Key** field.

Locking and Unlocking Datasets

You can only lock and unlock an encrypted dataset if it is secured with a passphrase instead of a key file. Before locking a dataset, verify that it is not currently in use.

Locking a Dataset

Click the dataset ⋮ icon to display the **Dataset Actions** option list and then click **Lock**. The **Lock Dataset** dialog displays with the dataset full path name.

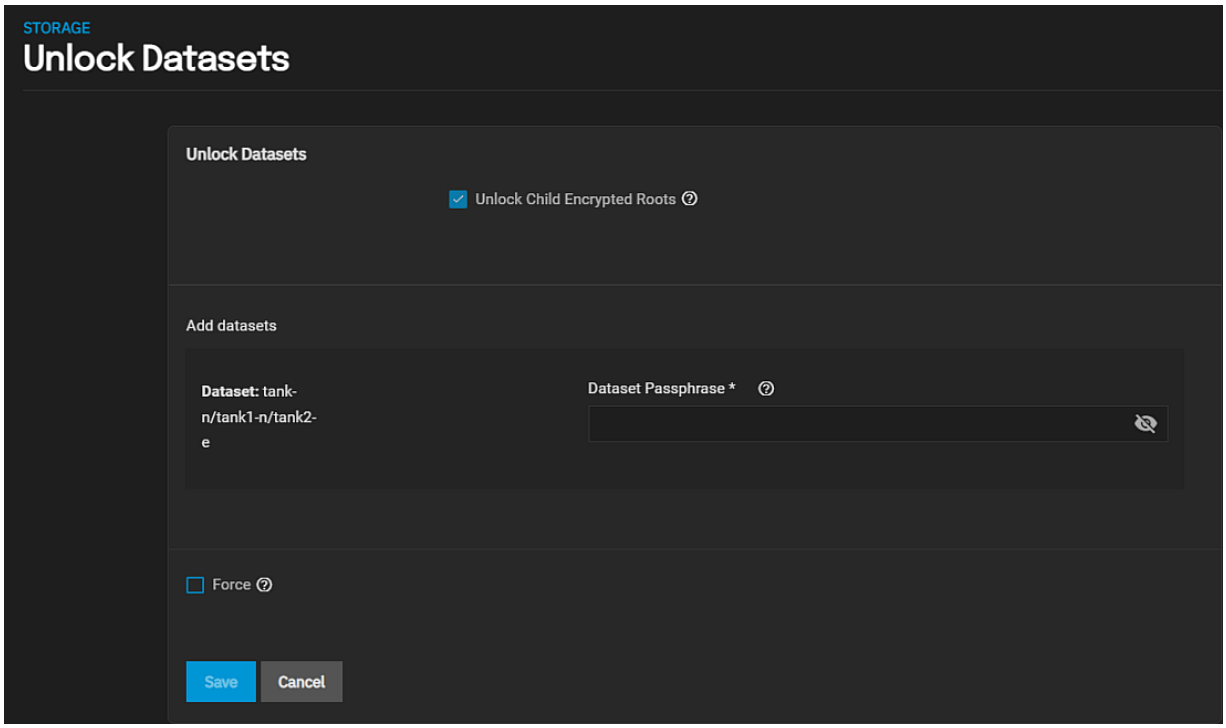


Use the **Force unmount** option only if you are certain no one is currently accessing the dataset. Click **Confirm**to activate **LOCK**, and then click **LOCK**.

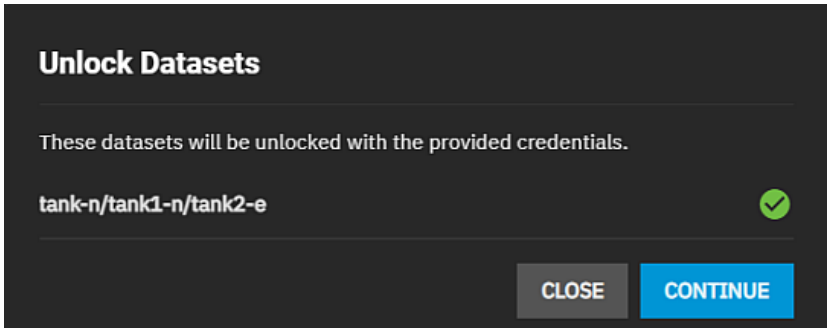
> You *cannot* use locked datasets.

Unlocking a Dataset

To unlock a dataset, click on the ⋮ icon to display the **Dataset Actions** option list and then click **Unlock**.



Type the passphrase into **Dataset Passphrase** and click **Save**. Select **Unlock Child Encrypted Roots** to unlock all locked child datasets if they use the same passphrase. Select **Force** if the path where the dataset mounts exists but is not empty. When this happens the unlock operation fails. The **Force** option allows the system to rename the existing directory and file where the dataset should mount. This prevents the mount operation from failing. A confirmation dialog displays.



Click **CONTINUE** to confirm you want to unlock the datasets or **CLOSE** to exit and keep the datasets locked. A second confirmation window displays confirming the datasets unlocked. Click **CLOSE**. TrueNAS displays the dataset with the unlocked icon.

Encrypting a Zvol

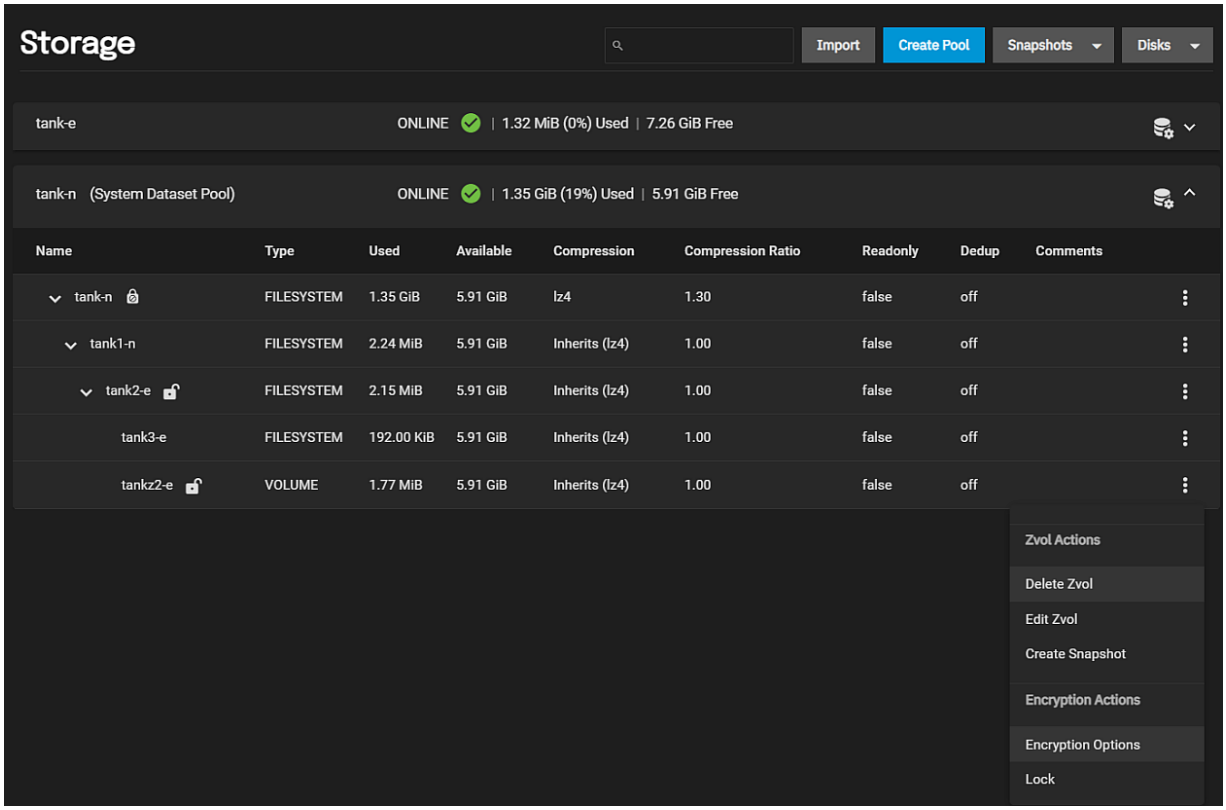
Encryption is for securing sensitive data.

> You can only encrypting a zvol if you create the zvol from a dataset with encryption.

> Users are responsible for backing up and securing encryption keys and passphrases! Losing the ability to decrypt data is similar to a catastrophic data loss.

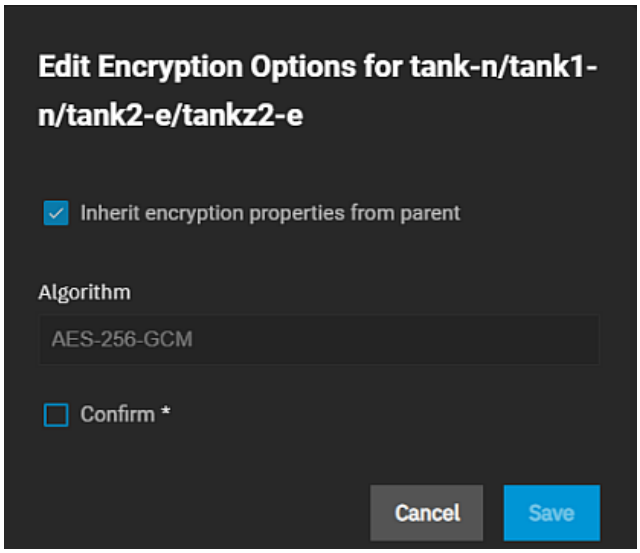
Zvols inherit encryption settings from the parent dataset.

To encrypt a zvol, select a dataset configured with encryption and then create a new zvol. Next, click the ⋮ icon to display the **Zvol Actions** options list and then click **Encryption Options**.



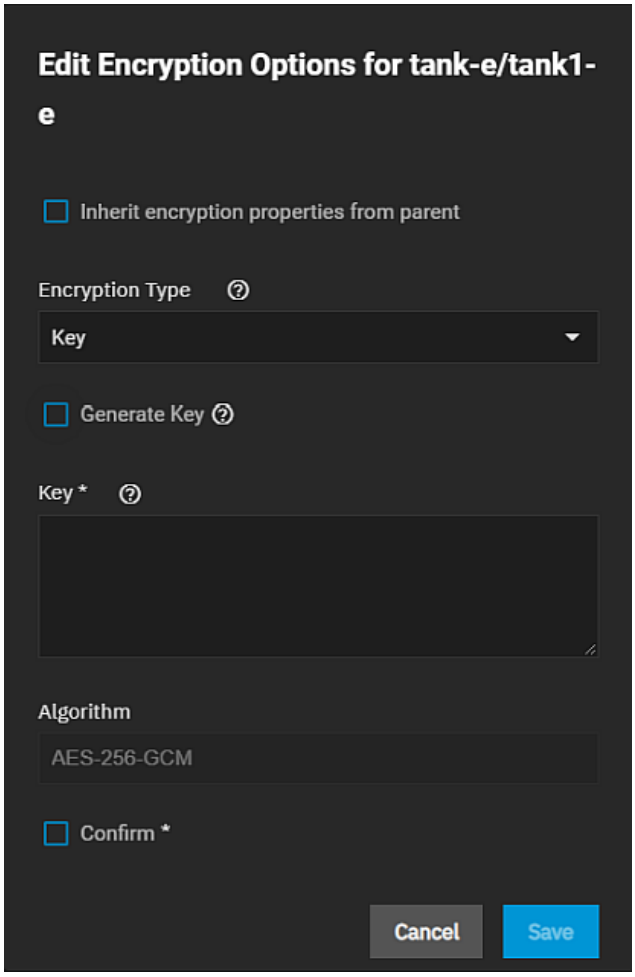
If you do not see **Encryption Options** on the **Zvol Action**s option list you created the zvol from an unencrypted dataset. Delete the zvol and start over.

Click **Encryption Options**. The **Edit Encryption Options** dialog for the Zvol displays with **Inherit encryption properties from parent** selected.



If not making changes, click **Confirm**, and then click **Save**. The zvol is encrypted with settings inherited from its parent.

To change inherited encryption properties, clear the **Inherit encryption properties from parent** checkbox. The current encryption settings display. You can change from key to passphrase or change from a system-generated key to one of your choosing.



If **Encryption Type** is set to**Key**, type an encryption key into the **Key** field or select **Generate Key**. If using **Passphrase**, it should be at least eight characters long. Use a passphrase complex enough to not easily guess. After making any changes, select **Confirm**, and then click **Save**.

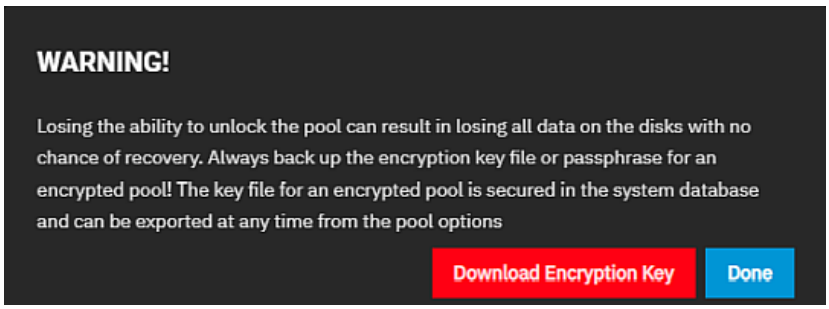
> Save any change to the encryption key or passphrase, update your saved passcodes and keys file, and back up the file.

Managing Encryption Credentials

There are two ways to manage the encryption credentials, with a key file or passphrase.

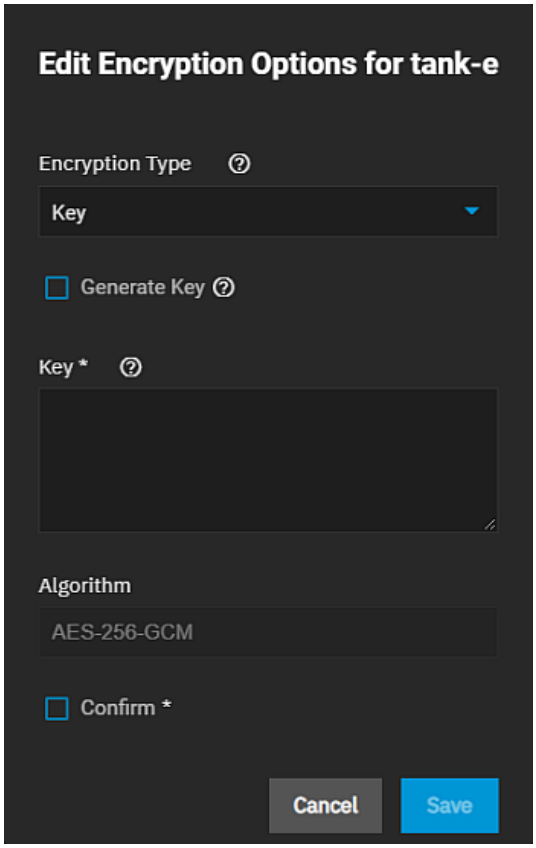
Creating a new encrypted pool automatically generates a new key file and prompts users to download it.

> Always back up the key file to a safe and secure location.



To manually back up a root dataset key file, click the icon to display the **Pool Actions** list of options, and select **Export Dataset Keys**. The keys download to your system.

To change the key, click ⋮ for the dataset, and then click **Encryption Options**.



See Changing Dataset-Level Encryption for more information on changing encryption settings.

A passphrase is a user-defined string at least eight characters long that is required to decrypt the dataset.

The **pbkdf2iters** is the number of password-based key derivation function 2 (PBKDF2) iterations to use for reducing vulnerability to brute-force attacks. Users must enter a number greater than *100000*.

Unlocking a Replicated Encrypted Dataset or Zvol Without a Passphrase

TrueNAS SCALE users should either replicate the dataset/Zvol without properties to disable encryption at the remote end or construct a special json manifest to unlock each child dataset/zvol with a unique key.

Method 1: Construct JSON Manifest.

1. Replicate every encrypted dataset you want to replicate with properties.
2. Export key for every child dataset that has a unique key.
3. For each child dataset construct a proper json with poolname/datasetname of the destination system and key from the source system like this: `{"tank/share01": "57112db4be777d93fa7b76138a68b790d46d6858569bf9d13e32eb9fda72146b"}`
4. Save this file with the extension .json.
5. On the remote system, unlock the dataset(s) using properly constructed json files.

Method 2: Replicate Encrypted Dataset/zvol Without Properties.

Uncheck properties when replicating so that the destination dataset is not encrypted on the remote side and does not require a key to unlock.

1. Go to **Data Protection** and click **ADD** in the **Replication Tasks** window.
2. Click **Advanced Replication Creation**.
3. Fill out the form as needed and make sure **Include Dataset Properties** is *NOT* checked.
4. Click **Save**.

Method 3: Replicate Key Encrypted Dataset/zvol.

1. Go to **Storage -> pool/root dataset** on the replication system. Click ⋮ and select **Export Key**.

2. Apply the key file or key code to the dataset. Either download the key file, open that file and change the *pool name/dataset* to the receiving *pool name/dataset*, or copy the key code provided in the **Key** window.

3. On the receiving pool/dataset: Click ⋮ next to pool/dataset and select **Unlock**.

4. Unlock the dataset. Either clear the **Unlock with Key file** checkbox, paste the Key Code into **Dataset Key** field (if there is a space character at the end of the key, delete the space), or select the downloaded Key file that was edited.

5. Click **Save**.

6. Click **Continue**.

3.3.1.8 - Managing User or Group Quotas

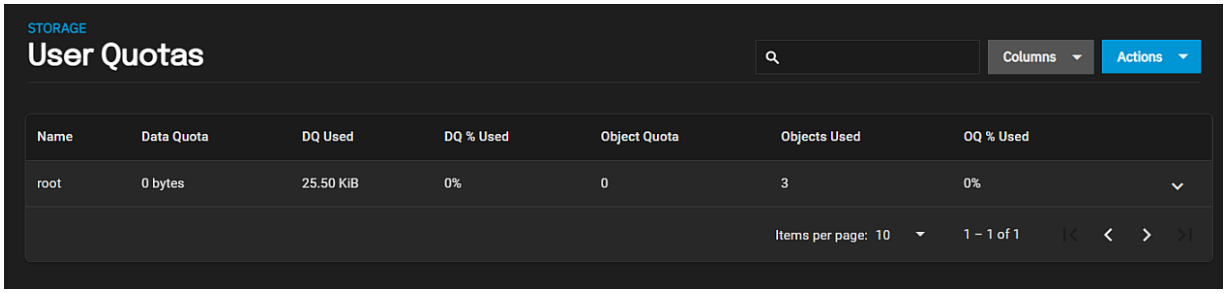
This article provides information on managing user and group quotas.

TrueNAS allows setting data or object quotas for user accounts and groups cached on or connected to the system. You can use the quota settings on the **Add Dataset** or **Edit Dataset** configuration screens in the **Advanced Options** settings to set up alarms and set aside more space in a dataset. See Adding and Managing Datasets for more information.

Configuring User Quotas

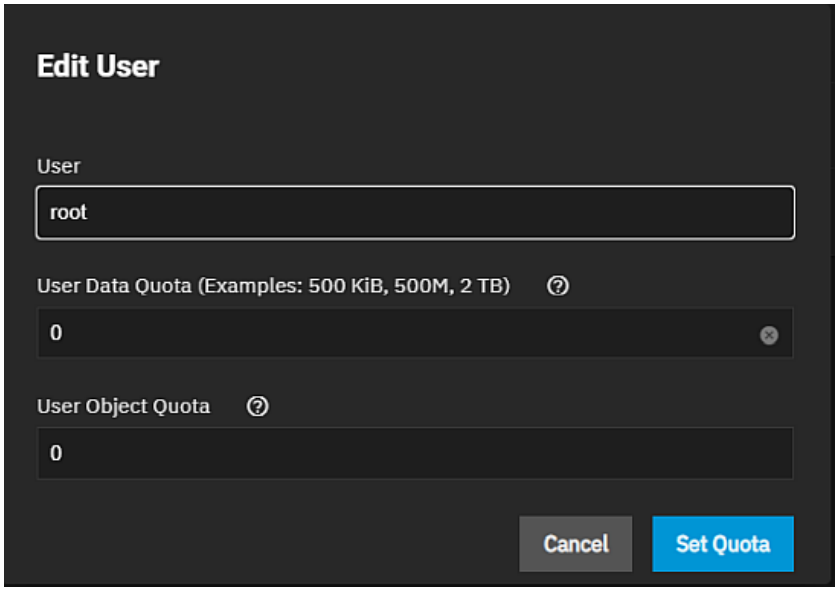
Select **User Quotas** to set data or object quotas for user accounts cached on or connected to the system.

To view and edit user quotas, go to **Storage** and click ⋮ next to a dataset to open the **Dataset Actions** menu, then select **User Quotas**.



The **User Quotas** page displays the names and quota data of any user accounts cached on or connected to the system.

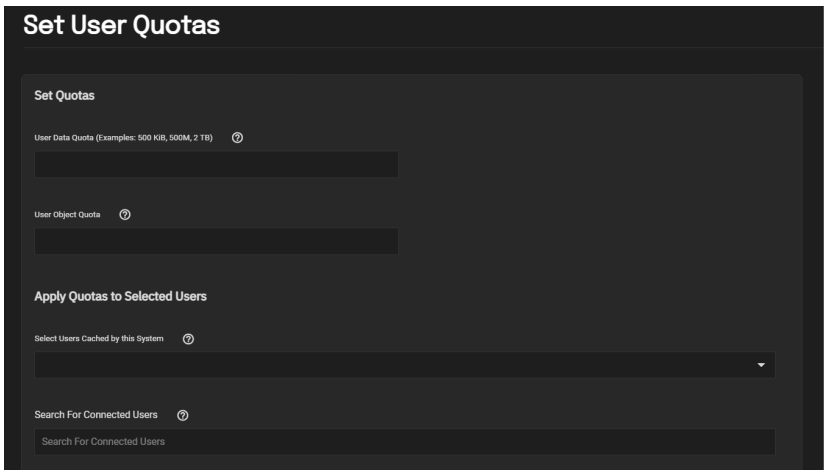
To edit individual user quotas, go to the user row and click the ⌄ icon to display a detailed individual user quota screen. Click ✎ **Edit**.



The **Edit User** window lets users edit the **User Data Quota** and **User Object Quota** values.

User Data Quota is the amount of disk space that selected users can use. **User Object Quota** is the number of objects selected users can own.

To edit user quotas in bulk, click **Actions** and select **Set Quotas (Bulk)**.

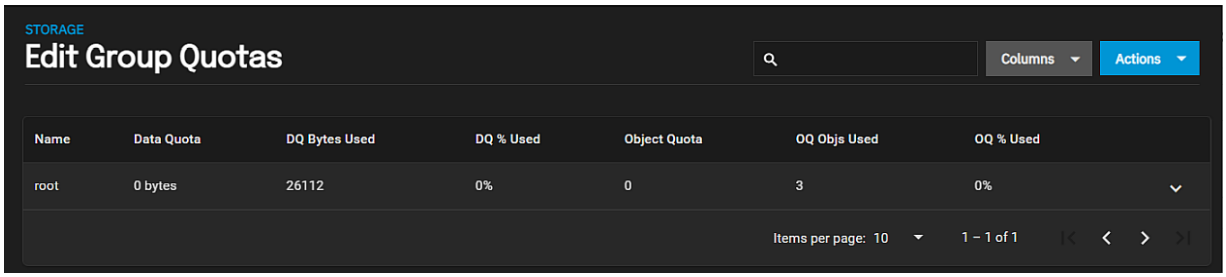


The **Set Quotas** window lets you edit user data and object quotas after selecting any cached or connected users.

Configuring Group Quotas

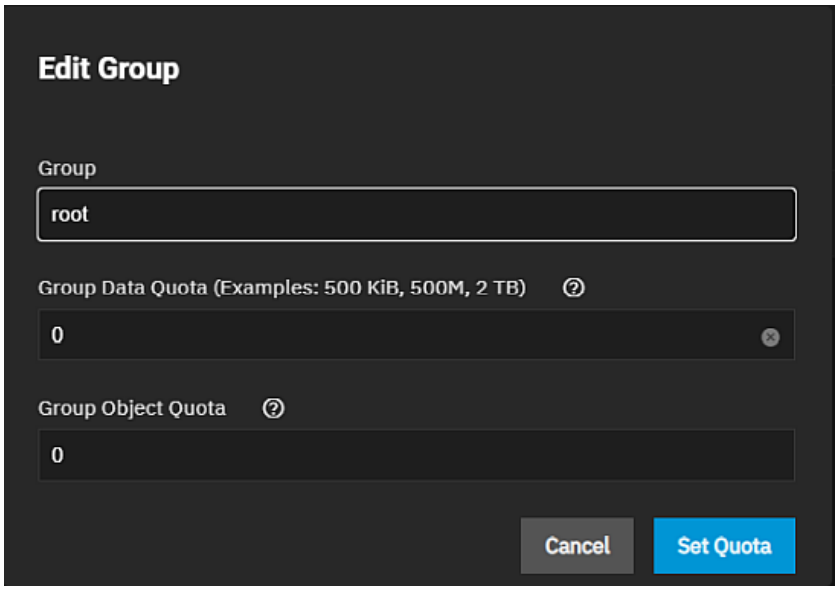
Select **Group Quotas** to set data or object quotas for user groups cached on or connected to the system.

Go to **Storage** and click ⋮ next to a dataset to open the **Dataset Actions** menu, then select **Group Quotas**.



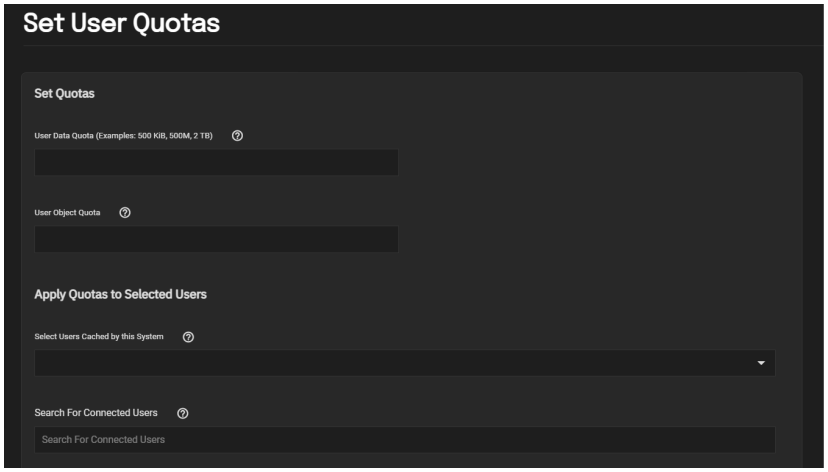
The **Group Quotas** page displays the names and quota data of any groups cached on or connected to the system.

To edit individual group quotas, go to the group row and click ⌄ icon, then click ✎ **Edit**.



The **Edit Group** window lets users edit the **Group Data Quota** and **Group Object Quota** values.

To edit group quotas in bulk, click **Actions** and select **Set Quotas (Bulk)**.



TrueNAS presents the same options for single groups and lets users choose groups for the new quota rules.

Related Content

- User and Group Quota Screens
- Adding and Managing Datasets

3.3.1.9 - SLOG Over-Provisioning

This article provides information on the disk_resize command in SCALE.

Over-provisioning SLOG SSDs is useful for different scenarios. The most useful benefit of over-provisioning is greatly extending SSD life. Over-provisioning an SSD distributes the total number of writes and erases across more flash blocks on the drive.

Seagate provides a thoughtful investigation into over-provisioning SSDs here: https://www.seagate.com/tech-insights/ssd-over-provisioning-benefits-master-ti/.

> Some SATA devices are limited to one resize per power cycle. Some BIOS can block resize during boot and require a live power cycle.

Over-Provision with Disk_Resize

SCALE uses the `disk_resize` command to change the size of a device. The SCALE UI does not have a UI function for this command yet.

Go to **System Settings > Shell** to enter the command and resize or over-provision a device.

`disk_resize sda 32GB` where *sda* is the device and *32GIB* is the new size for the device.

When no size is specified, it reverts the provision back the full size of the device.

The `disk_resize` command supports SAS, SATA, SAT (interposer) and NVMe drives. Power cycle SATA drives before a second resize

Related Content

- Advanced Settings Screen
- Disks Screens
- Managing Disks
- Importing Disks
- Managing SEDs
- Replacing Disks
- View Enclosure Screen
- Wiping a Disk

3.3.1.10 - Fusion Pools

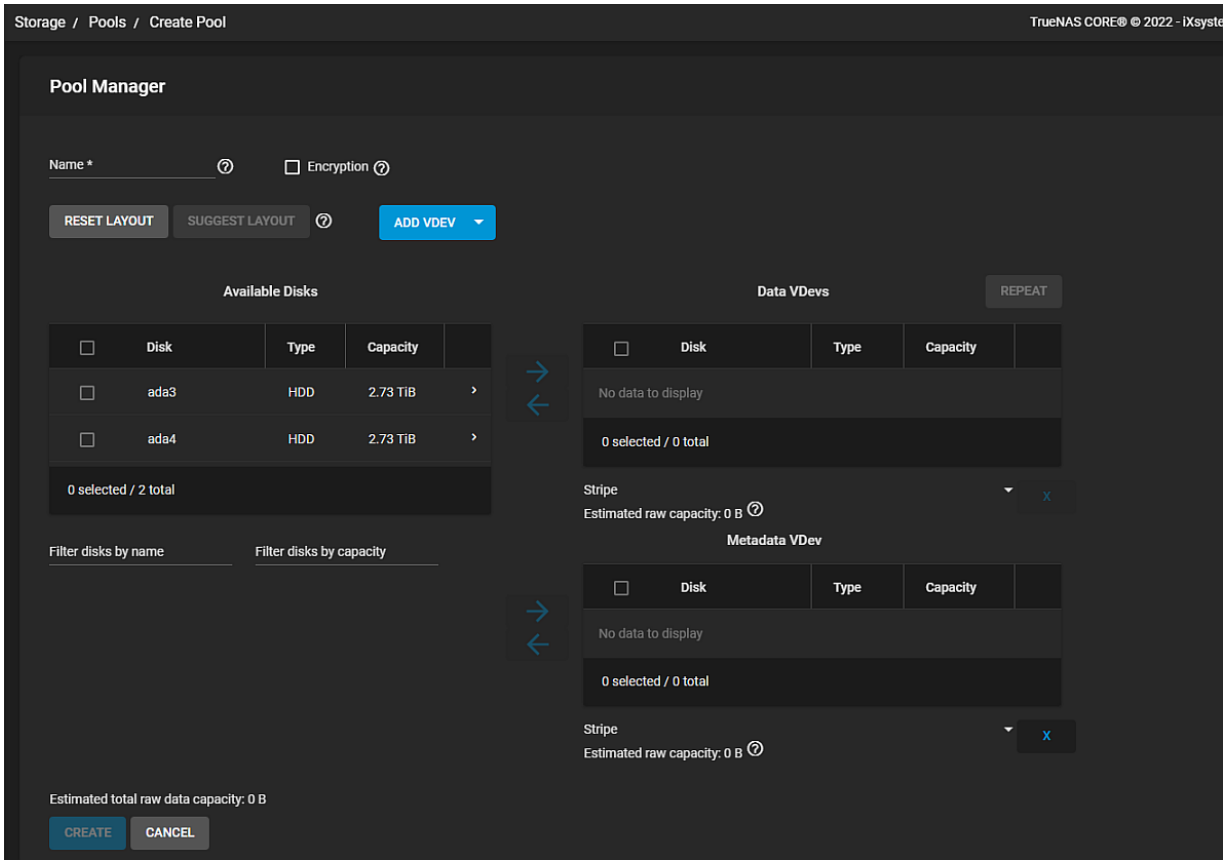
Fusion Pools are also known as ZFS allocation classes, ZFS special vdevs, and metadata vdevs (**Metadata** vdev type on the **Pool Manager** screen.).

What's a special vdev?
A special vdev can store meta data such as file locations and allocation tables. The allocations in the special class are dedicated to specific block types. By default, this includes all metadata, the indirect blocks of user data, and any deduplication tables. The class can also be provisioned to accept small file blocks. This is a great use case for high performance but smaller sized solid-state storage. Using a special vdev drastically speeds up random I/O and cuts the average spinning-disk I/Os needed to find and access a file by up to half.

Creating a Fusion Pool

Go to **Storage > Pools**, click **ADD**, and select **Create new pool**.

A pool must always have one normal (non-dedup/special) vdev before other devices can be assigned to the special class. Configure the **Data VDevs**, then click **ADD VDEV** and select **Metadata**.



Add SSDs to the new **Metadata VDev** and select the same layout as the **Data VDevs**.

> The metadata special vdev is critical for pool operation and data integrity, so you must protect it with hot spare(s).

UPS Recommendation
When using SSDs with an internal cache, add uninterruptible power supply (UPS) to the system to help minimize the risk from power loss.

Using special vdevs identical to the data vdevs (so they can use the same hot spares) is recommended, but for performance reasons you can make a different type of vdev (like a mirror of SSDs). In that case you must provide hot spare(s) for that drive type as well. Otherwise, if the special vdev fails and there is no redundancy, the pool becomes corrupted and prevents access to stored data.

> Drives added to a metadata vdev cannot be removed from the pool.

When more than one metadata vdev is created, then allocations are load-balanced between all these devices. If the special class becomes full, then allocations spill back into the normal class.

After the fusion pool is created, the **Status** shows a **Special** section with the metadata SSDs.

Related Pools Articles

- Dashboard
- Managing Advanced Settings
- Advanced Settings Screen
- View Enclosure Screen
- Setting Up Permissions
- Storage Encryption
- SLOG Over-Provisioning

3.3.2 - Disks

This section provides articles with instructions for importing, replacing, wiping disks.

Disk Article Summaries

- Managing Disks

  This article provides information on managing disks, performing manual testing and S.M.A.R.T. test results.

- Importing Disks

  This article provides instructions for importing a disk and monitoring the import progress.

- Replacing Disks

  This article provides disk replacement instructions that includes offlining the failed disk and onlining the replacement disk.

- Wiping a Disk

  This article provides instructions for wiping a disk.

3.3.2.1 - Managing Disks

This article provides information on managing disks, performing manual testing and S.M.A.R.T. test results.

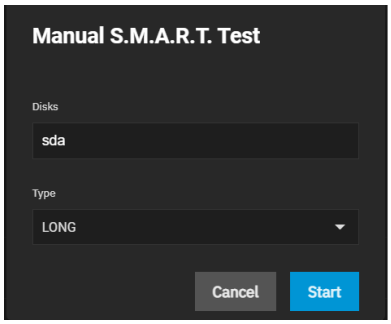
To manage disks, go to **Storage** and click **Disks** on the top right of the screen to display the **Storage Disks** screen.

Select the disk on the list, then select **Edit**.

The **Disks** page lets users edit disks, perform manual tests, and view S.M.A.R.T. test results. Users may also delete obsolete data off an unused disk.

Performing Manual Testing

Select the disk(s) you want to perform a S.M.A.R.T. test on and click **Manual Test**.



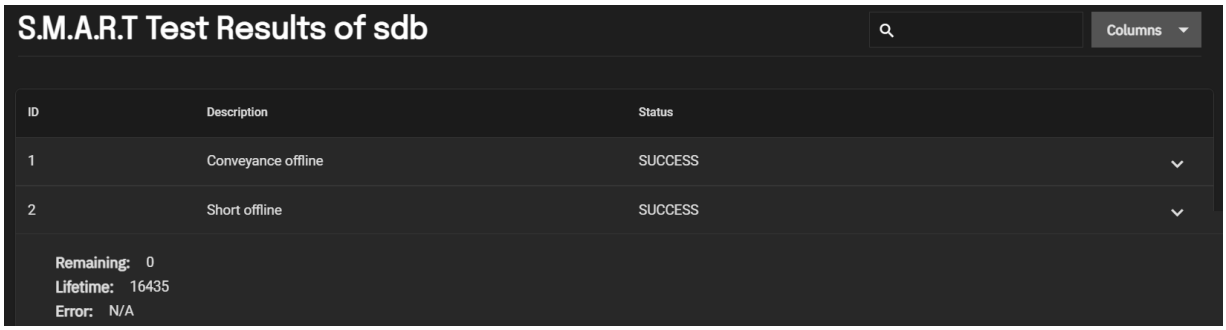
- **Long** runs SMART Extended Self Test. This scans the entire disk surface and can take many hours on large-volume disks.
- **Short** runs SMART Short Self Test (usually under ten minutes). These are basic disk tests that vary by manufacturer.
- **Conveyance** runs a SMART Conveyance Self Test. This self-test routine is intended to identify damage incurred during transporting of the device. This self-test routine requires only minutes to complete.
- **Offline** runs SMART Immediate Offline Test. The effects of this test are visible only in that it updates the SMART Attribute values, and if the test finds errors, they appear in the SMART error log.

Click **Start** to begin the test. Depending on the test type you choose, the test can take some time to complete. TrueNAS generates alerts when tests discover issues.

For information on automated S.M.A.R.T. testing, see the S.M.A.R.T. tests article.

S.M.A.R.T. Test Results

To review test results, expand the disk and click **S.M.A.R.T. Test Results**.



Users can also view S.M.A.R.T. Test Results in **Shell** using the `smartctl` command and the name of the drive. For example, `smartctl -l selftest /dev/sdb`.

Related Content

- Advanced Settings Screen
- Disks Screens
- Importing Disks
- Managing SEDs
- Replacing Disks
- View Enclosure Screen
- Wiping a Disk
- SLOG Over-Provisioning

Related Storage Articles

- Storage Screens
- Snapshots Screens
- Setting Up Storage
- Zvol Screens
- Creating Storage Pools
- Edit ACL Screens
- Importing Storage Pools
- Adding and Managing Datasets
- Installing and Managing Self-Encrypting Drives
- Adding and Managing Zvols

3.3.2.2 - Importing Disks

This article provides instructions for importing a disk and monitoring the import progress.

Importing is a one-time procedure that copies the data from that disk into a TrueNAS dataset. TrueNAS can only import one disk at a time, and you must install or physically connect it to the TrueNAS system.

You can use the import function to integrate UFS (BSD Unix), NTFS (Windows), MSDOS (FAT), or EXT2 (Linux) formatted disks into TrueNAS.

What about EXT3 or EXT4 file systems?

Importing an EXT3 or EXT4 filesystem is possible in some cases, although neither is fully supported. EXT3 journaling is not supported, so those file systems must have an external `fsck` utility, like the one provided by E2fsprogs utilities, run on them before import.

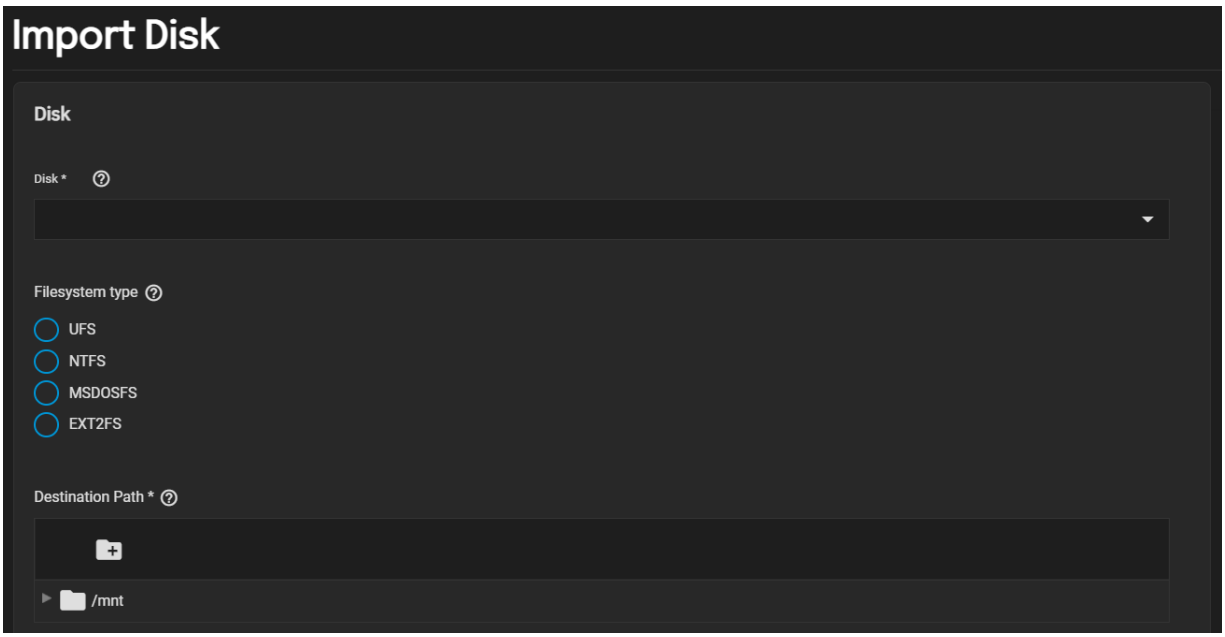
EXT4 file systems with extended attributes or i-nodes greater than 128 bytes are not supported. EXT4 file systems with EXT3 journaling must have an `fsck` run on them before import, as described above.

Importing a Disk

You can only import one disk at a time.

To import a disk:

1. Go to **Storage** and click **Disks** at the top right of the screen.
2. Select **Import Disk** to display the **Import Disk** screen.



3. Use the **Disk** dropdown list to select the disk you want to import.

   TrueNAS attempts to detect and select the file system type. If not already selected by the system, click a radio button for a file system type to use from the on-screen options.

   Selecting the MSDOSFS file system displays the **MSDOSFS locale** dropdown field. Use this option to select the locale when non-ASCII characters are present on the disk.

4. Select the ZFS dataset you want to hold the copied data in **Destination Path**.
5. Click **Save**. The disk mounts and copies its contents to the specified dataset you entered in **Destination Path**.

The import was interrupted!
Use the same import procedure to restart the task. Choose the same dataset in **Destination Path** as the interrupted import for TrueNAS to scan the destination for previously imported files and resume importing any remaining files.

Monitoring a Disk Import

To monitor an in-progress import, open the **Task Manager** by clicking the  in top toolbar. The disk unmounts after the copy operation completes. A dialog allows viewing or downloading the disk import log.

Related Content

- Advanced Settings Screen
- Disks Screens
- Managing Disks
- Managing SEDs
- Replacing Disks
- View Enclosure Screen
- Wiping a Disk
- SLOG Over-Provisioning

Related Storage Articles

- Storage Screens
- Snapshots Screens
- Setting Up Storage
- Zvol Screens
- Creating Storage Pools
- Edit ACL Screens
- Importing Storage Pools
- Adding and Managing Datasets
- Installing and Managing Self-Encrypting Drives
- Adding and Managing Zvols

3.3.2.3 - Replacing Disks

This article provides disk replacement instructions that includes offlining the failed disk and onlining the replacement disk.

Hard drives and solid-state drives (SSDs) have a finite lifetime and can fail unexpectedly. When a disk fails in a Stripe (RAID0) pool, you must to recreate the entire pool and restore all data backups. We always recommend creating non-stripe storage pools that have disk redundancy.

To prevent further redundancy loss or eventual data loss, always replace a failed disk as soon as possible! TrueNAS integrates new disks into a pool to restore it to full functionality.

> TrueNAS requires you to replace a disk with another disk of the same or greater capacity as a failed disk. You must install the disk install in the TrueNAS system and it should not be part of an existing storage pool. TrueNAS wipes the data on the replacement disk as part of the process.

Replacing a Failed Disk

A SCALE **Pool** widget, or the **Storage** widget if you are not displaying individual pool widgets, on the **Dashboard** shows when a disk failure degrades that pool.

Click the on the pool card to go to the **Pool Status** screen. You can also select **Storage** on the function main menu on the left side of the screen. The pool status displays for each pool listed on the screen. Click the icon for the degraded pool to display the **Pool Actions** dropdown list and then click **Status** to display the **Pool Status** screen to locate the failed disk.

To replace a failed disk:

1. Offline the disk.
2. Pull the disk from your system and replace with a disk of at lease the same or greater capacity as the failed disk.
3. Online the new disk.

Off-lining a Failed Disk

We recommend users off-line a disk before starting the physical disk replacement. Off-lining a disk removes the device from the pool and can prevent swap issues.

Can I use a disk that is failing but still active?

There are situations where you can leave a disk that has not completely failed online to provide additional redundancy during the replacement procedure.

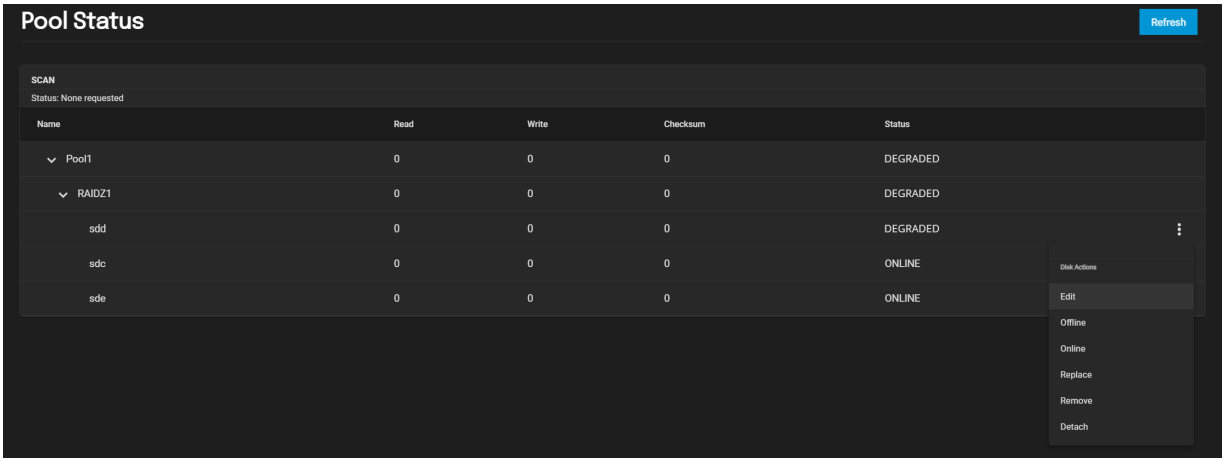
> We do not recommend leaving failed disks online unless you know the exact condition of the failing disk.

Attempting to replace a heavily degraded disk without off-lining it significantly slows down the replacement process.

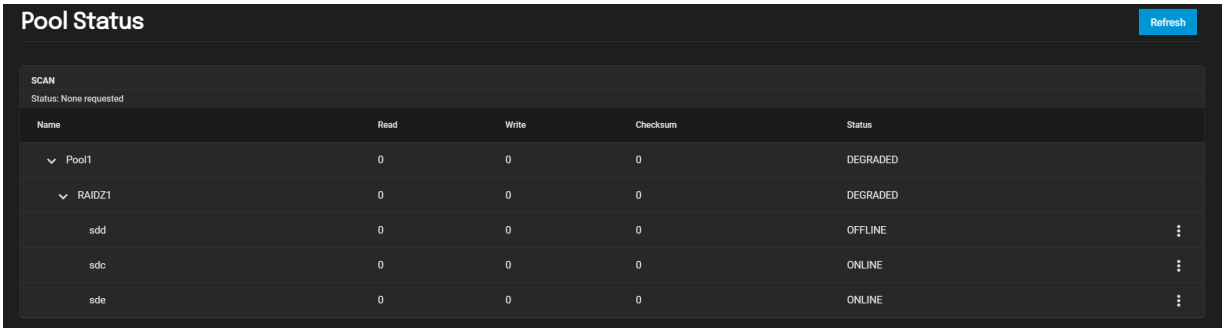
The offline failed?

If the off-line operation fails with a **"Disk offline failed - no valid replicas"** message, go to **Storage**, click the ⚙ for the degraded pool, and select **Scrub Pool**. When the scrub operation finishes, reopen the **Pool Status** screen and try to off-line the disk again.

1. Click ⋮ next to the failed disk to display the **Disk Actions** dropdown menu of options.
2. Click **Offline**. A confirmation dialog displays. Click **Confirm** and then **Offline**. The system begins the process to take the disk offline. When complete, the list of disks displays the status of the failed disk as **Offline**.



3. You can physically remove the disk from the system when the disk status is **Offline**.



4. If the replacement disk is not already physically installed in the system, do it now.

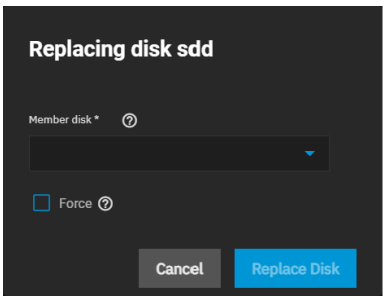
Next, bring the new disk online.

On-lining a New Disk

The new disk must have the same or greater capacity as the disk you are replacing.

On **Pool Status** screen click the ⋮ next to the offline disk to display the **Disk Actions** dropdown menu of options.

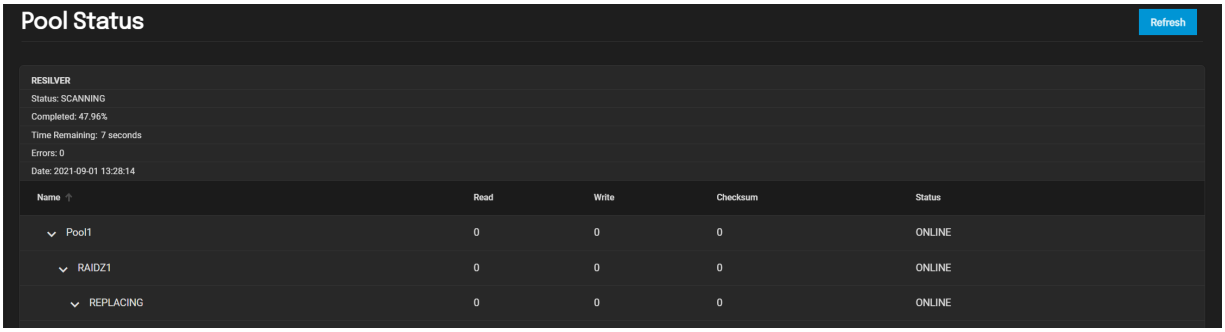
1. Click **Replace**.



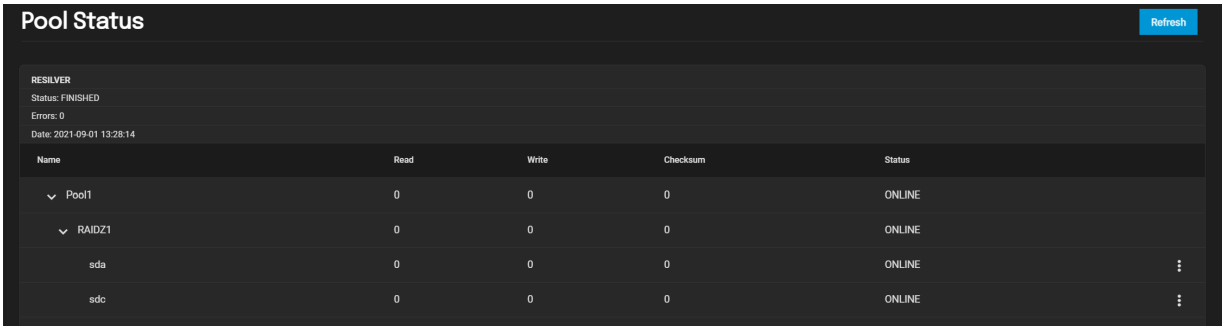
2. Select a new member disk and click **Replace Disk**.

   Disk replacement fails when the selected disk has partitions or data present. To destroy any data on the replacement disk and allow the replacement to continue, select the **Force** option.

   When the disk wipe completes, TrueNAS starts replacing the failed disk. A status spinner displays over the **Pool Status** screen to show progress of the proceess.



TrueNAS resilvers the pool during the replacement process. For pools with large amounts of data, this can take a long time. When the resilver process completes, the pool status returns to **Online** status on the **Disks** screen.



Related Content

- Advanced Settings Screen
- Disks Screens
- Managing Disks
- Importing Disks
- Managing SEDs
- View Enclosure Screen
- Wiping a Disk
- SLOG Over-Provisioning

Related Storage Articles

- Storage Screens
- Snapshots Screens
- Setting Up Storage
- Zvol Screens
- Creating Storage Pools
- Edit ACL Screens
- Importing Storage Pools
- Adding and Managing Datasets
- Installing and Managing Self-Encrypting Drives
- Adding and Managing Zvols

3.3.2.4 - Wiping a Disk

This article provides instructions for wiping a disk.

The disk wipe option deletes obsolete data from an unused disk.

> Wipe is a destructive action and results in permanent data loss! Back up any critical data before wiping a disk.

TrueNAS only shows the **Wipe** option for unused disks.

> Ensure you have backed-up all data and are no longer using the disk. Triple check that you have selected the correct disk for the wipe. Recovering data from a wiped disk is usually impossible.

Click **Wipe** to open a dialog with additional options:

- **Quick** erases only the partitioning information on a disk without clearing other old data, making it easy to reuse. Quick wipes take only a few seconds.
- **Full with zeros** oerwrites the entire disk with zeros and can take several hours to complete.
- **Full with random** overwrites the entire disk with random binary code and takes even longer than the **Full with zeros** operation to complete.

After selecting the appropriate method, click **Wipe** and confirm the action.

Verify the name to ensure you have chosen the correct disk. When satisfied you can wipe the disk, set **Confirm** and click **Continue**.

Related Content

- Advanced Settings Screen
- Disks Screens
- Managing Disks
- Importing Disks
- Managing SEDs
- Replacing Disks
- View Enclosure Screen
- SLOG Over-Provisioning

Related Storage Articles

- Storage Screens
- Snapshots Screens
- Setting Up Storage
- Zvol Screens
- Creating Storage Pools
- Edit ACL Screens
- Importing Storage Pools
- Adding and Managing Datasets
- Installing and Managing Self-Encrypting Drives
- Adding and Managing Zvols

3.3.3 - Creating and Managing Snapshots

This article provides instructions on managing ZFS snapshots in TrueNAS Scale.

Snapshots are one of the most powerful features of ZFS. A *snapshot* provides a read only point-in-time copy of a file system or volume. This copy does not consume extra space in the ZFS pool. The snapshot only records the differences between storage block references whenever the data is modified.

Why do I want to keep snapshots?
Snapshots keep a history of files and provide a way to recover an older or even deleted files. For this reason, many administrators take regular snapshots, store them for some time, and copy them to a different system. This strategy allows an administrator to roll the system data back to a specific point in time. In the event of catastrophic system or disk failure, off-site snapshots can restore data up to the most recent snapshot.

Taking snapshots requires the system have all pools, datasets, and zvols already configured.

Creating a Snapshot

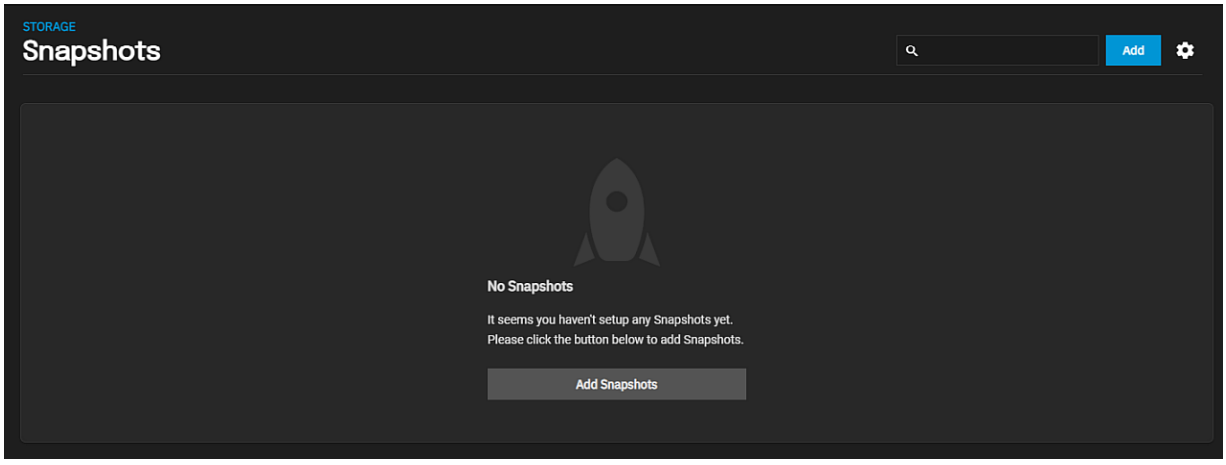
> Consider making a Periodic Snapshot Task to save time and create regular, fresh snapshots.

Video Tutorial

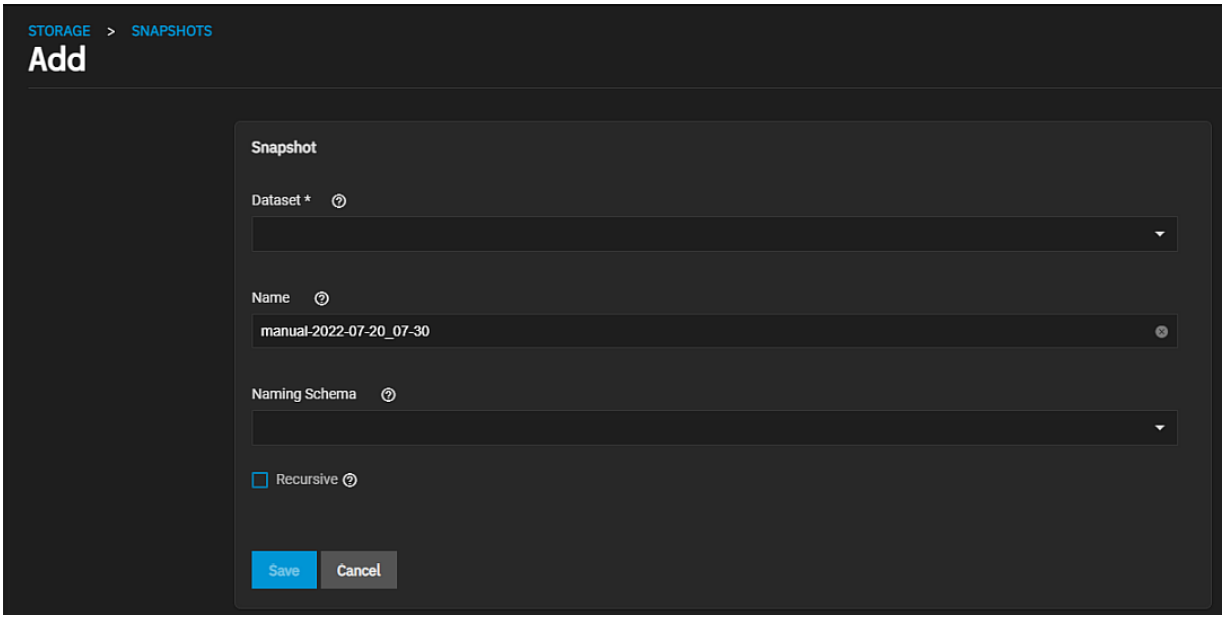
This short video demonstrates manually adding a snapshot

From the **Storage** screen you can either and click **Snapshots** on the top right corner of the screen. Select **Snapshots** to display the **Snapshots** screen, or click on the ⋮ for the dataset on the **Pool Manager** screen and select **Create Snapshot** to take a one-time snapshot of that dataset.

If you don't have snapshots created, the **Snapshots** screen displays the **Add Snapshots** option in the center of the screen.



1. Click either **Add Snapshots** or **ADD** at the top right of the screen to open the **Add Snapshot** screen.

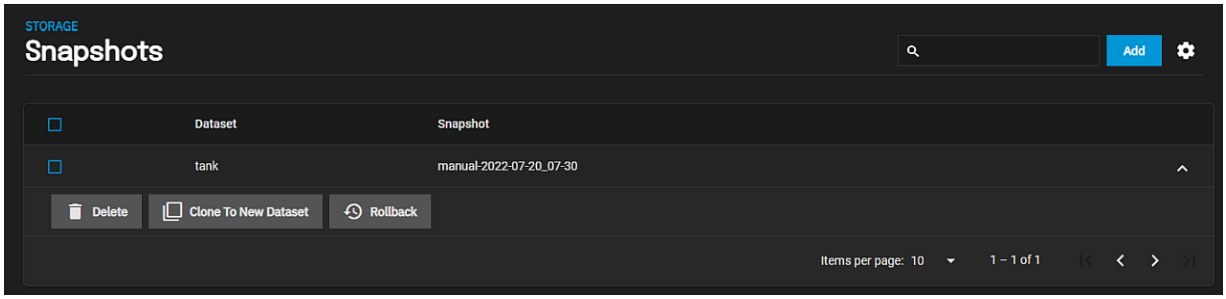


2. Select an existing ZFS pool, dataset, or zvol to snapshot option from the **Dataset** dropdown list.
3. Accept the name suggested by the TrueNAS software in the **Name** field ore enter any custom string to override the suggested name.
4. (Optional) Select an option from the **Naming Schema** dropdown list that the TrueNAS software populated with existing periodic snapshot task schemas.
   If you select an option, TrueNAS generates a name for the snapshot using that naming schema from the selected Periodic Snapshot and replicates that snapshot.

   You cannot enter a value in **Naming Schema** and in **Name** as selecting or entering a value in **Naming Schema** populates the other field.
5. (Optional) Select **Recursive** to include child datasets with the snapshot.
6. Click **Save** to create the snapshot.

Managing Snapshots

The **Snapshots** screen lists all snapshots created on the system. To manage snapshots, click the ⌄ icon to expand the snapshot and display the options for managing that snapshot.



You can display more information in that table by clicking the ⚙ icon. Click **Show** to display extra columns in the table. To hide the added columns, click the span class=“material-icons”>settings icon again and then click **Hide**.

Each snapshot entry in the list includes the dataset and snapshot names. Entries also display the snapshot numbers, the space they use, the date the system created them, and the amount of data the dataset can access.

Click ⌄ to view snapshot options.

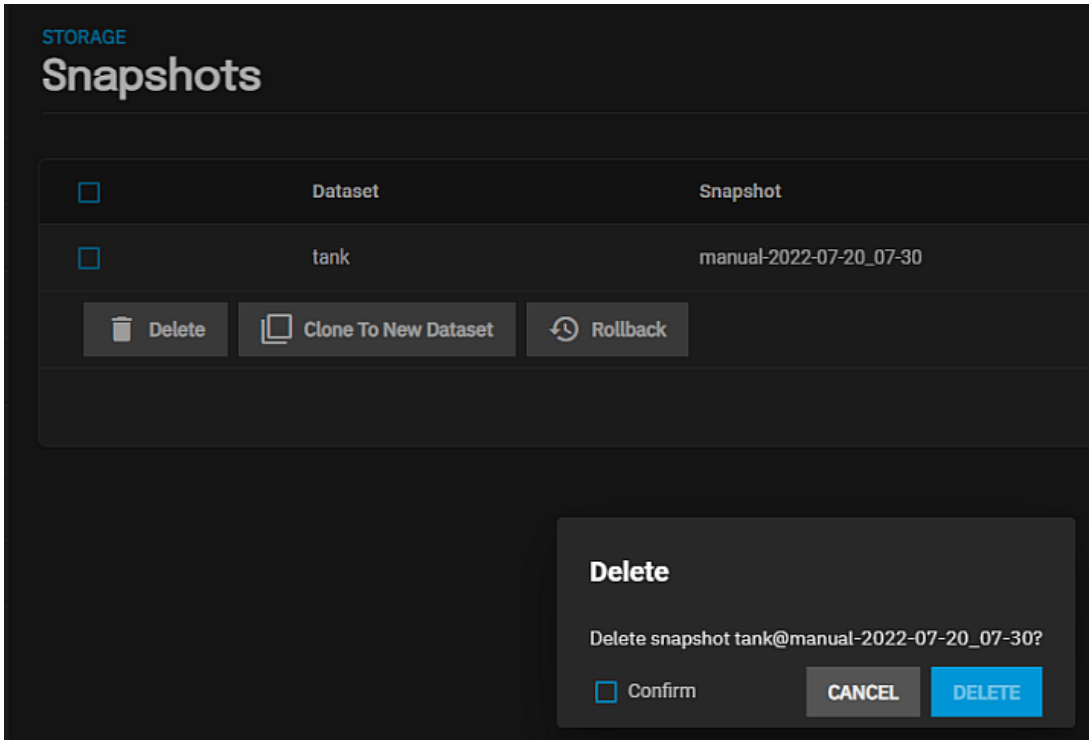
> File Explorer he number of snapshots Windows presents to users. If TrueNAS responds with more than the File Explorer limit, File Explorer shows no available snapshots. TrueNAS displays a dialog stating the dataset snapshot count has more snapshots than recommended, and states performance or functionality might degrade.

Deleting a Snapshot

The **Delete** option destroys the snapshot. You must delete child clones before you can delete their parent snapshot. While creating a snapshot is instantaneous, deleting one is I/O intensive and can take a long time, especially when deduplication is

enabled.

Why?
ZFS has to review all allocated blocks before deletion to see if another process is using that block. If not used, the ZFS can free that block.



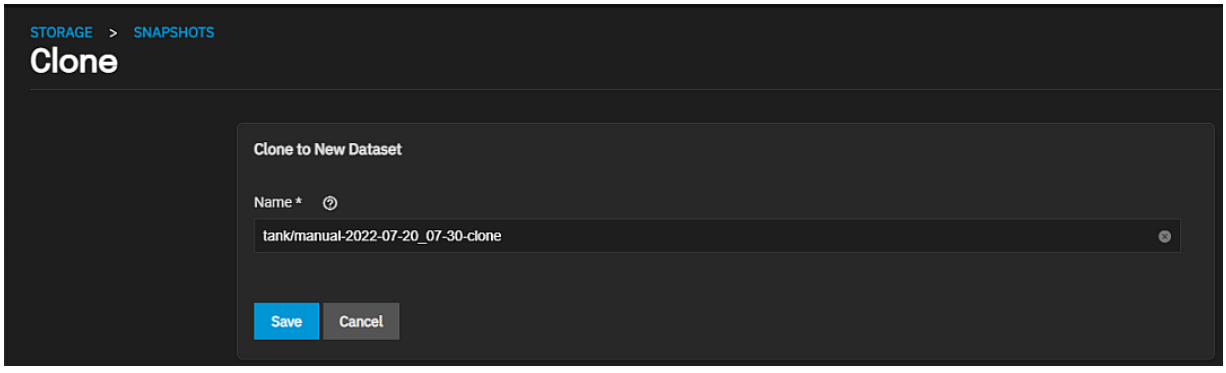
Click the **Delete** button. A confirmation dialog displays. Select **Confirm** to activate the **Delete** button.

Cloning to a New Dataset

The **Clone to New Dataset** option creates a new snapshot *clone* (dataset) from the snapshot contents.

What is a clone?
A **clone** is a writable copy of the snapshot. Because a clone is a mountable dataset, it appears in the **Storage** screen rather than the **Snapshots** screen. By default, TrueNAS adds **-clone** to the new snapshot name when creating the clone.

A dialog prompts for the new dataset name. The suggested name derives from the snapshot name.



Rollback

The **Rollback** option reverts the dataset back to the point in time saved by the snapshot.

> Rollback is a dangerous operation that causes any configured replication tasks to fail.

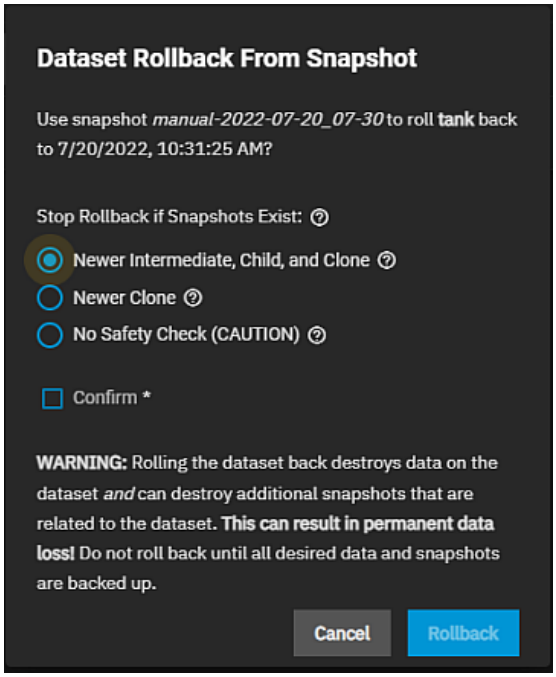
Replications use the existing snapshot when doing an incremental backup, and rolling back can put the snapshots out-of-order. To restore the data within a snapshot, the recommended steps are:

1. Clone the desired snapshot.
2. Share the clone with the share type or service running on the TrueNAS system.

3. Allow users to recover their needed data.
4. Delete the clone from **Storage**.

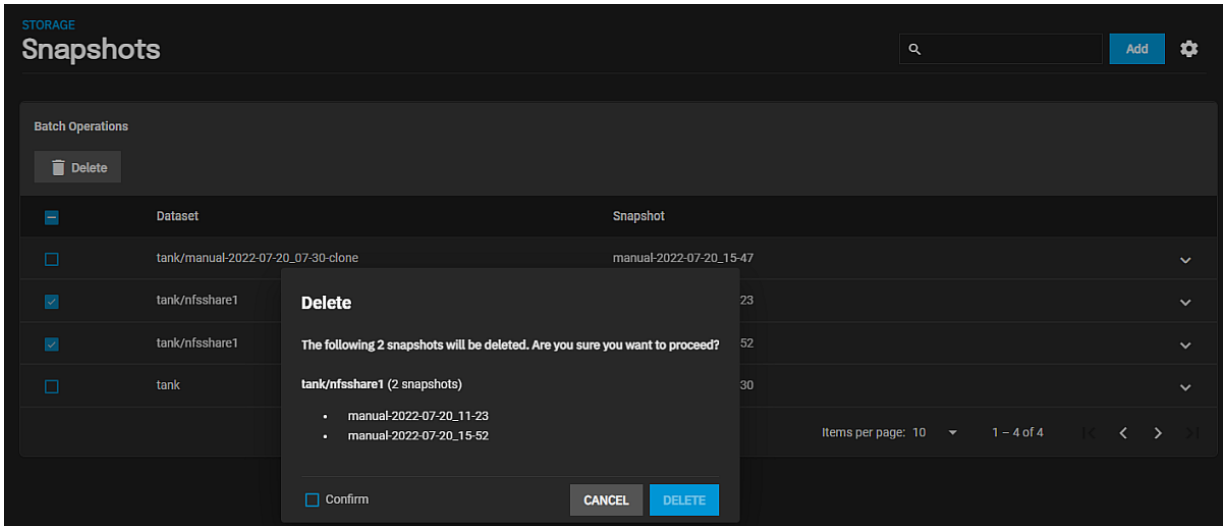
This approach does not destroy any on-disk data or impact replication.

TrueNAS asks for confirmation before rolling back to the chosen snapshot state. Select the radio button for how you want the rollback to operate.



Click **Confirm** to activate the **Rollback** button.

Deleting with Batch Operations



To delete multiple snapshots, select the left column box for each snapshot to include. Click the **Delete** button that displays.

To search through the snapshots list by name, type a matching criteria into the **Filter Snapshots** text field. The list now displays only the snapshot names that match the filter text.

Browsing a Snapshot Collection

> Browsing a snapshot collection is an advanced capability that requires ZFS and command-line experience.

All dataset snapshots are accessible as an ordinary hierarchical file system, accessed from a hidden .zfs located at the root of every dataset.

> A snapshot and any files it contains are not accessible or searchable if the snapshot mount path is longer than 88

> characters. The data within the snapshot is safe but to make the snapshot accessible again shorten the mount path.

A user with permission to access the hidden file can view and explore all snapshots for a dataset from the **Shell** or the **Shares** screen using services like **SMB**, **NFS**, and **SFTP**.

In summary, the main required changes to settings are:

- In dataset properties, change the ZFS properties to enable snapshot visibility.
- In the Samba auxiliary settings, change the `veto files` command to not hide the .zfs, and add the setting `zfsacl:expose_snapdir=true`.

The effect is that any user who can access the dataset contents can view the list of snapshots by going to the dataset .zfs directory. Users can browse and search any files they have permission to access throughout the entire dataset snapshot collection.

When creating a snapshot, permissions or ACLs set on files within that snapshot might limit access to the files.

Snapshots are read-only, so users do not have permission to modify a snapshot or its files, even if they had write permissions when creating the snapshot.

The `zfs diff` ZFS command, which can run in the **Shell**, lists all changed files between any two snapshot versions within a dataset, or between any snapshot and the current data.

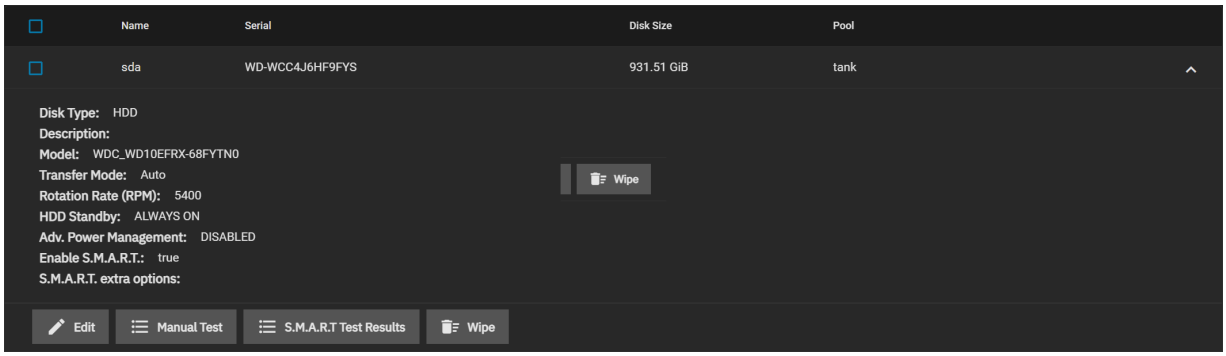
Related Content

- Snapshots Screens
- Creating VMWare Snapshots
- VMWare Snapshots Screen
- Periodic Snapshot Tasks Screens

3.3.4 - Disks

The *Disks* page displays the names, serial numbers, sizes, and pools of all the system's physical drives. Users can customize disk columns using the *Columns* drop-down*.

Clicking the the › in a disk's row will expand it to show the traits specific to that disk.



Managing Disks

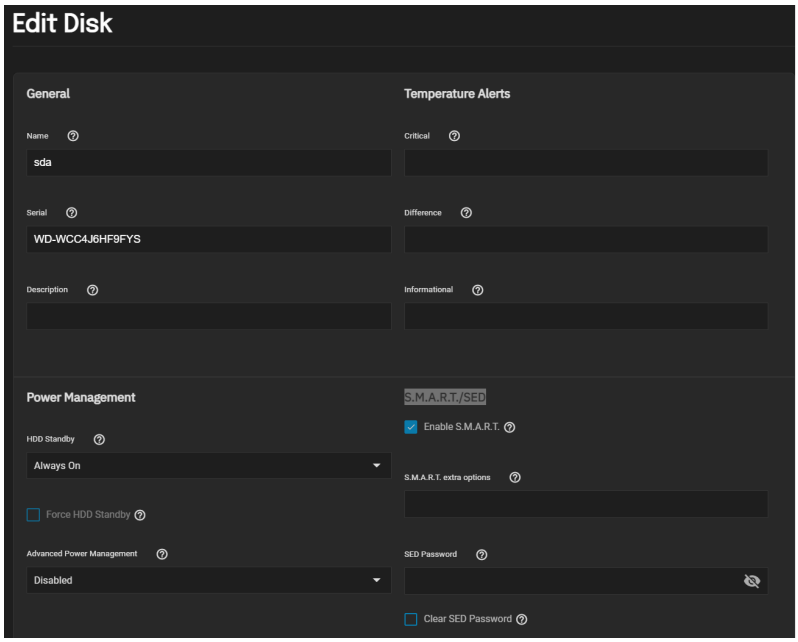
Managing Disks

To manage disks, go to **Storage** and click *Disks*, then select *Disks*.

The *Disks* page lets users edit disks, perform manual tests, and view S.M.A.R.T. test results. Users may also delete obsolete data off an unused disk.

Editing Disks

Clicking *Edit* allows users to configure general disk settings, as well as power management, temperature alerts, and S.M.A.R.T./SED settings.



General

Setting	Description
Name	Linux disk device name.
Serial	Serial number for this disk.
Description	Notes about this disk.

Power Management

Setting	Description
HDD Standby	Minutes of inactivity before the drive enters standby mode. This forum post describes identifying spun down drives. Temperature monitoring is disabled for standby disks.
Force HDD Standby	Allows the drive to enter standby, even when non-physical S.M.A.R.T. operations could prevent the drive from sleeping.
Advanced Power Management	Select a power management profile from the menu.

Temperature Alerts

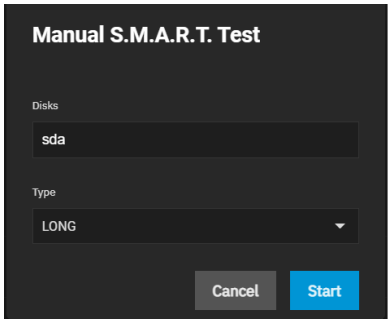
Setting	Description
Critical	Threshold temperature in Celsius. If the drive temperature is higher than this value, a LOG_CRIT level log entry is created and an email is sent. 0 disables this check.
Difference	Report if the temperature of a drive has changed by this many degrees Celsius since the last report. 0 disables the report.
Informational	Report if drive temperature is at or above this temperature in Celsius. 0 disables the report.

S.M.A.R.T./SED

Setting	Description
Enable S.M.A.R.T.	Enabling allows the system to conduct periodic S.M.A.R.T. tests.
S.M.A.R.T. extra options	Additional smartctl(8) options.
SED Password	Set or change the password of this SED. This password is used instead of the global SED password.
Clear SED Password	Clear the SED password for this disk.

Manual Testing

Select the disk(s) you want to perform a S.M.A.R.T. test on and click *Manual Test*.



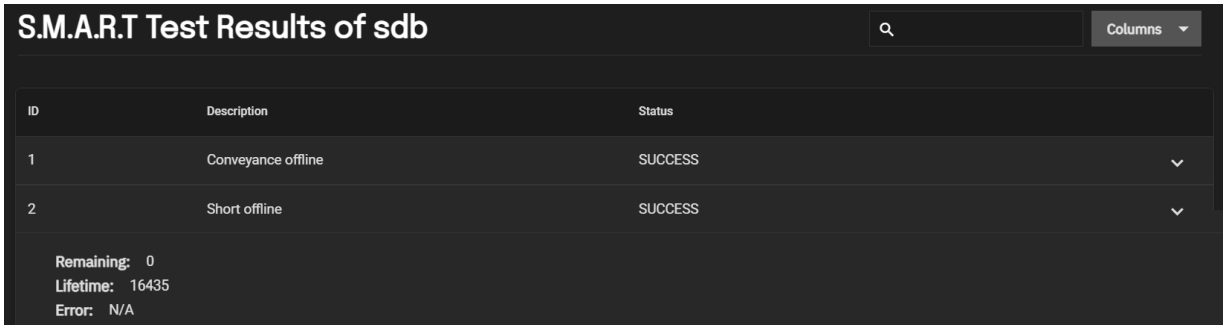
- *Long* - runs SMART Extended Self Test. This will scan the entire disk surface and can take many hours on large-volume disks.
- *Short* - runs SMART Short Self Test (usually under ten minutes). These are basic disk tests that vary by manufacturer.
- *Conveyance* - runs a SMART Conveyance Self Test. This self-test routine is intended to identify damage incurred during transporting of the device. This self-test routine requires only minutes to complete.
- *Offline* - runs SMART Immediate Offline Test. The effects of this test are visible only in that it updates the SMART Attribute values, and if the test finds errors, they appear in the SMART error log.

Click *Start* to begin the test. Depending on the test type you choose, the test can take some time to complete. TrueNAS generates alerts when tests discover issues.

For information on automated S.M.A.R.T. testing, see the S.M.A.R.T. tests SCALE article.

S.M.A.R.T. Test Results

To review test results, expand the disk and click *S.M.A.R.T. Test Results*.



Users can also view S.M.A.R.T. Test Results in **Shell** using `smartctl` and the name of the drive: `smartctl -l selftest /dev/sdb`.

Wipe

The *Wipe* option deletes obsolete data off an unused disk.

> Wipe is a destructive action and results in permanent data loss! Back up any critical data before wiping a disk.

TrueNAS only shows the *Wipe* option for unused disks. Click *Wipe* to open a dialog with additional options:

- *Quick* - Erases only the partitioning information on a disk without clearing other old data, making it easy to reuse. Quick wipes take only a few seconds.
- *Full with zeros* - Overwrites the entire disk with zeros and can take several hours to complete.
- *Full with random* - Overwrites the entire disk with random binary code and takes even longer than *Full with zeros* to complete.

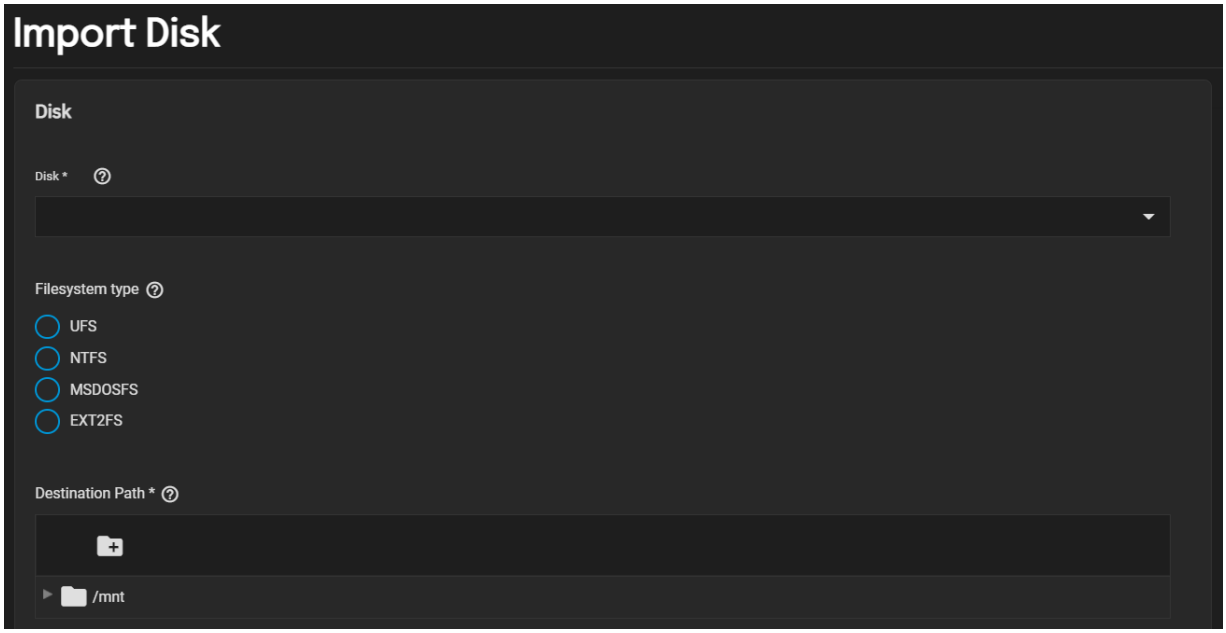
> Ensure you have backed-up all data and are no longer using the disk. Triple check that you have selected the correct disk for the wipe. Recovering data from a wiped disk is usually impossible.

After choosing the appropriate method, click *Wipe* and confirm the action.

Verify the name to ensure you have chosen the correct disk. When satisfied the disk can be wiped, set *Confirm* and click *Continue*.
Importing Disks

Go to **Storage** and click *Disks*, then select *Import Disk* to integrate UFS (BSD Unix), NTFS (Windows), MSDOS (FAT), or EXT2 (Linux) formatted disks into TrueNAS. Importing is a one-time procedure that copies the data from that disk into a TrueNAS dataset. TrueNAS can only import one disk at a time, and it must be installed or physically connected to the TrueNAS system.

What about EXT3 or EXT4 filesystems?
Importing an EXT3 or EXT4 filesystem is possible in some cases, although neither is fully supported. EXT3 journaling is not supported, so those filesystems must have an external `fsck` utility, like the one provided by E2fsprogs utilities, run on them before import. EXT4 filesystems with extended attributes or inodes greater than 128 bytes are not supported. EXT4 filesystems with EXT3 journaling must have an `fsck` run on them before import, as described above.



Use the drop-down menu to select the *Disk* to import.

TrueNAS attempts to detect and select the *Filesystem type*. Selecting the MSDOSFS filesystem shows an additional *MSDOSFS locale* drop-down menu. Use this option to select the locale when non-ASCII characters are present on the disk.

Finally, select the ZFS dataset you want to hold the copied data in *Destination Path*.

After clicking *Save*, the chosen *Disk* mounts and copies its contents to the specified dataset at the end of the *Destination Path*.

To monitor an in-progress import, open the Task Manager by clicking the in the interface top bar. The disk unmounts after the copy operation completes. A dialog allows viewing or downloading the disk import log.

The import was interrupted!
Use the same import procedure to restart the task. Choose the same *Destination Path* as the interrupted import for TrueNAS to scan the destination for previously imported files and resume importing any remaining files.

Replacing Disks

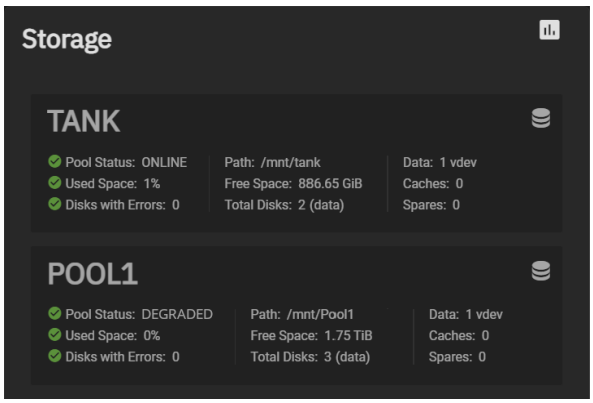
Hard drives and solid-state drives (SSDs) have a finite lifetime and can fail unexpectedly. When a disk fails in a Stripe (RAID0) pool, must to recreate the entire pool and restore all data backups. We always recommend creating non-stripe storage pools that have disk redundancy.

To prevent further redundancy loss or eventual data loss, always replace a failed disk as soon as possible! TrueNAS integrates new disks into a pool to restore it to full functionality.

Replacing a Disk

TrueNAS requires another disk of the same or greater capacity to replace a failed disk. The disk must be installed in the TrueNAS system and not part of an existing storage pool. TrueNAS wipes any data on the replacement disk as part of the process.

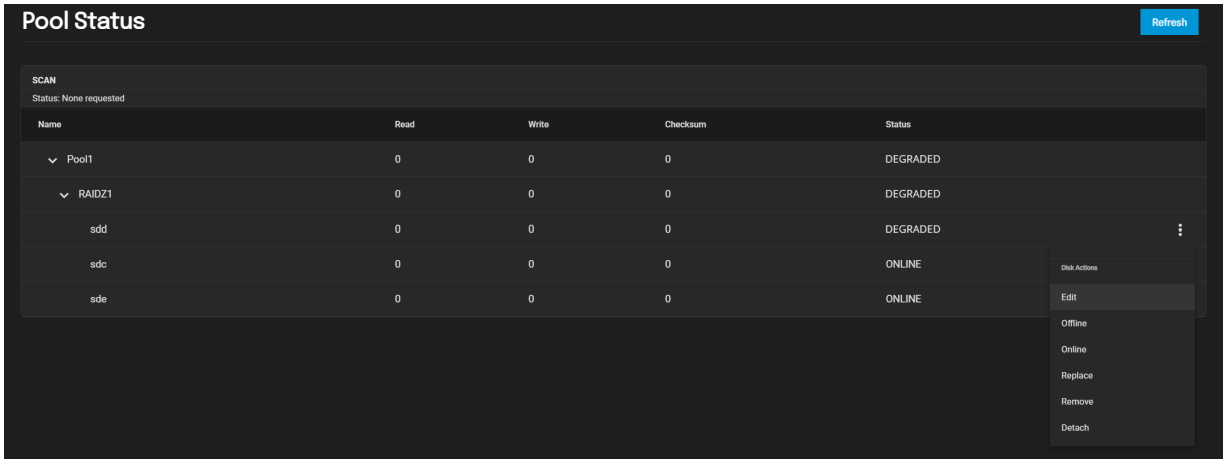
The TrueNAS **Dashboard** shows when a disk failure degrades a pool.



Click the on the pool card to go to the *Pool Status* screen and locate the failed disk.

Offline the Failed Disk

Clicking ⋮ next to the failed disk shows additional operations.



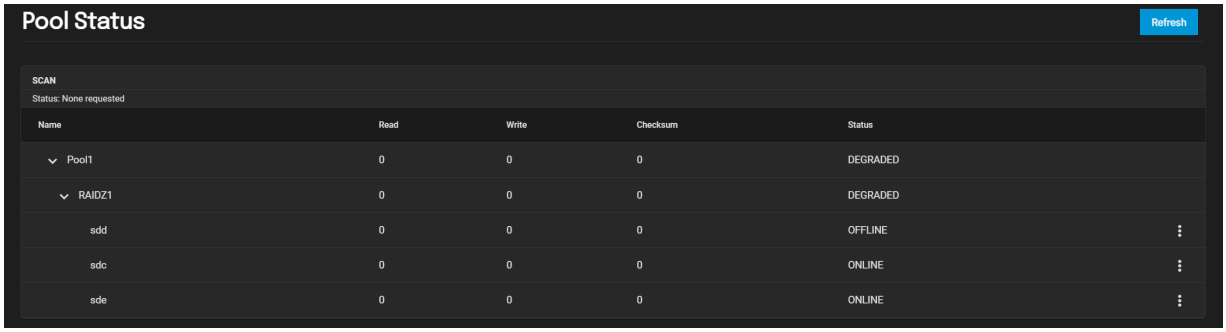
We recommend users *Offline* the disk before starting the replacement. Doing so removes the device from the pool and can prevent swap issues.

Can I use a disk that is failing but still active?
There are situations where a disk that has not completely failed can be left online to provide additional redundancy during the replacement procedure. **We do not recommend leaving failed disks online unless you know the exact condition of the failing disk.** Attempting to replace a heavily degraded disk without offlining it will significantly slow down the replacement process.

The offline failed?

If the *Offline* operation fails with a “Disk offline failed - no valid replicas” message, go to **Storage**, click the ⚙ for the degraded pool, and select *Scrub Pool*. When the scrub operation finishes, reopen the pool *Status* and try to *Offline* the disk again.

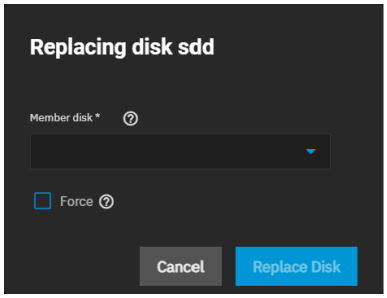
You can physically remove the disk from the system when the disk status is *Offline*.



If the replacement disk is not already physically added to the system, add it now.

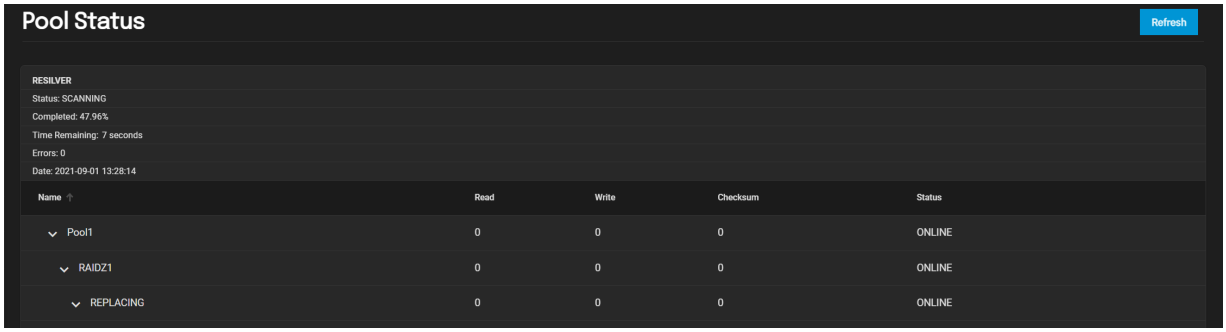
Online the New Disk

In *Pool Status*, open the options for the *Offline* disk and click *Replace*.

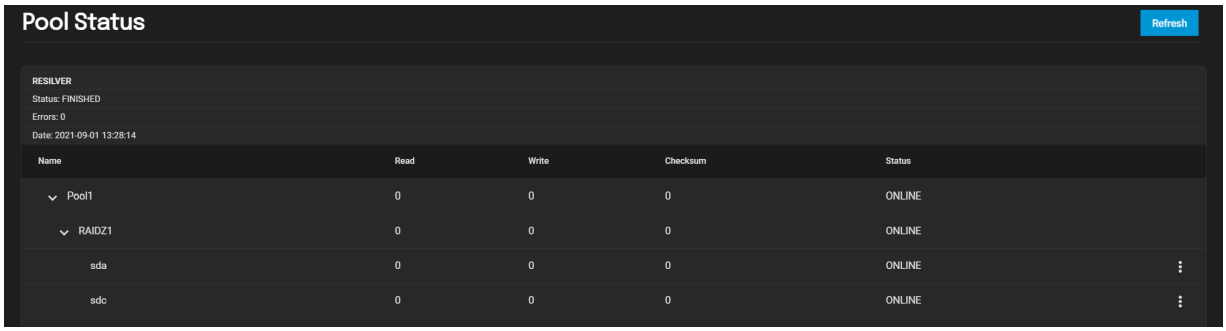


Select a new member disk and click *Replace Disk*. The new disk must have the same or greater capacity as the disk you are replacing. The replacement fails when the chosen disk has partitions or data present. To **destroy** any data on the replacement disk and allow the replacement to continue, set the *Force* option.

When the disk wipe completes, TrueNAS will start replacing the failed disk. *Pool Status* updates to show the in-progress replacement.



TrueNAS resilvers the pool during the replacement process. For pools with large amounts of data, this can take a long time. When the resilver is complete, the pool status returns to **Online** shows the new disk.



3.3.5 - Creating VMWare Snapshots

This article provides instructions for creating ZFS snapshots when using TrueNAS as a VMWare datastore.

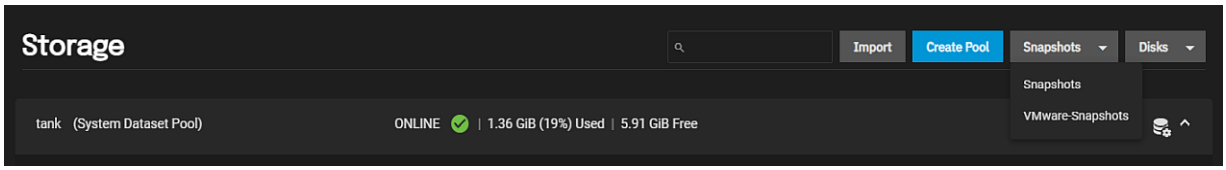
You must power on virtual machines for TrueNAS to copy snapshots to VMware. The temporary VMware snapshots deleted on the VMware side still exist in the ZFS snapshot and are available as stable restore points. These coordinated snapshots go in the **Snapshots** list.

Use this procedure to create ZFS snapshots when using TrueNAS SCALE as a VMWare datastore. VMware-Snapshots coordinate ZFS snapshots when using TrueNAS as a VMware datastore. When creating a ZFS snapshot, TrueNAS SCALE automatically takes a snapshot of any running VMWare virtual machine before taking a scheduled or manual ZFS snapshot of the data or zvol backing that VMWare datastore.

> You must have a paid-edition for VMWare ESXi to use the TrueNAS SCALE VMWare-snapshots feature. If you try to use them with the free-edition of VMware ESXi, you see this error message: “Error, Can’t create snapshot, current license or ESXi version prohibits execution of the requested operation.” ESXi free has a locked (read-only) API that prevents using TrueNAS SCALE VMWare-snapshots. The cheapest ESXi edition that is compatible with TrueNAS VMware-shapshots is VMWare vSphere Essentials Kit.

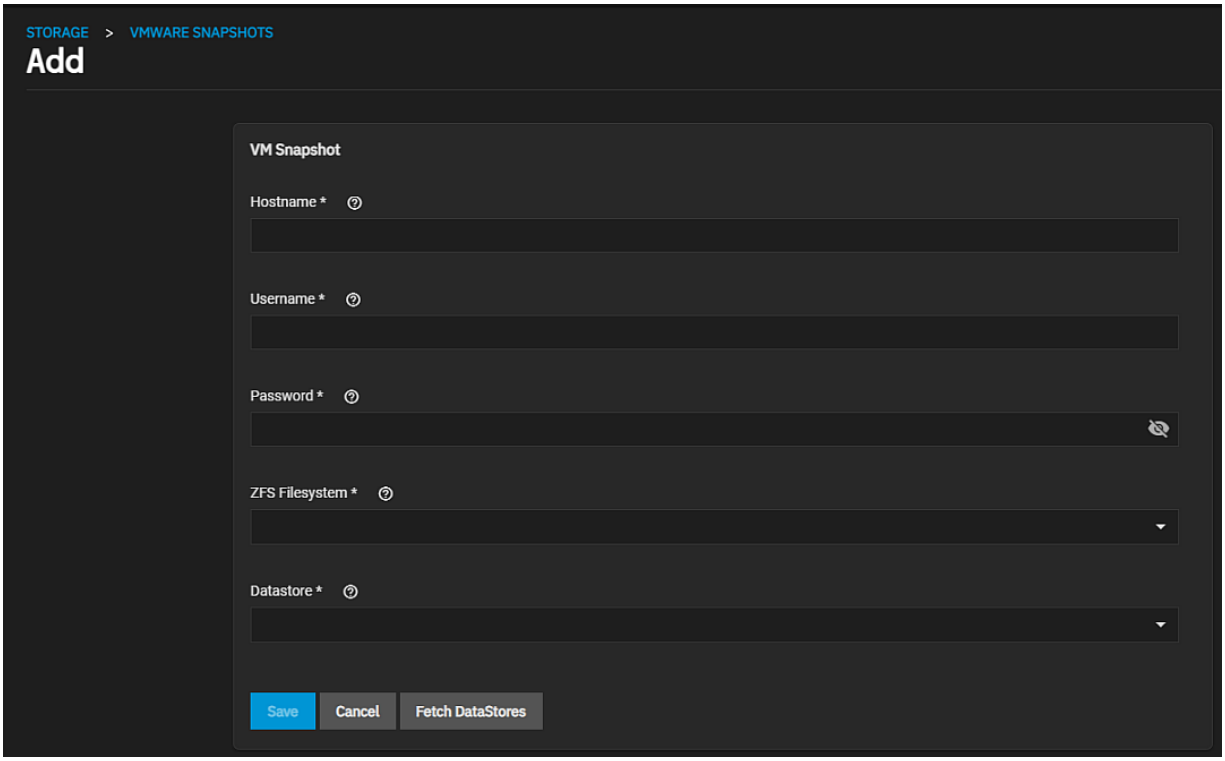
Creating a VMWare Snapshot

Go to **Storage** and click the **Snapshots** button at the top right of the screen. Select **VMware-Snapshots** on the dropdown list.



> You must follow the exact sequence to add the VMware snapshot or the **ZFS Filesystem** and **Datastore** fields do not populate with options available on your system. If you click in *ZFS Filestore** or **Datastores** before you click **Fetch Datastores** the creation process fails, the two fields do not populate with the information from the VMWare host and you must exit the add form or click **Cancel** and start again.

1. Enter the IP address or host name for your VMWare system in **Hostname**.



2. Enter the user on the VMware host with permission to snapshot virtual machine for VMWare in **Username** and the the password for that account in **Password**.
3. Click **Fetch Datastores**. This connects TrueNAS SCALE to the VMWare host and populates the **ZFS Filesystem** and **Datastore** dropdown fields with the host response.

4. Select the file system from the **ZFS Filesystem** dropdown list of options.
5. Select the datastore from the **Datastore** dropdown list of options.
6. Click **Save**.

Copying TrueNAS SCALE Snapshots to VMWare

You must power on virtual machines before you can copy TrueNAS SCALE snapshots to VMWare.

The temporary VMWare snapshots deleted on the VMWare side still exist in the ZFS snapshot and are available as stable restore points. Thes coordinated snapshots go on the list found on the **Storage > Snapshots** screen.

Related Content

- Snapshots Screens
- VMWare Snapshots Screen
- Periodic Snapshot Tasks Screens

Related VMWare Articles

- VMWare Snapshots Screen

3.3.6 - Installing and Managing Self-Encrypting Drives

This article covers self-encrypting drives, including supported specifications, implementing and managing SEDs in TrueNAS, and managing SED passwords and data.

Supported Specifications

- Legacy interface for older ATA devices (Not recommended for security-critical environments!)
- TCG Opal 1 legacy specification
- TCG OPAL 2 standard for newer consumer-grade devices
- TCG Opalite which is a reduced form of OPAL 2
- TCG Pyrite Version 1 and Version 2 are similar to Opalite, but with hardware encryption removed Pyrite provides a logical equivalent of the legacy ATA security for non-ATA devices. Only the drive firmware protects the device.

  > Pyrite Version 1 SEDs do not have PSID support and can become unusable if the password is lost.

- TCG Enterprise designed for systems with many data disks These SEDs cannot unlock before the operating system boots.

See this Trusted Computing Group and NVM Express® joint white paper for more details about these specifications.

TrueNAS Implementation

TrueNAS implements the security capabilities of camcontrol for legacy devices and sedutil-cli for TCG devices. When managing a SED from the command line, it is recommended to use the `sedhelper` wrapper script for `sedutil-cli` to ease SED administration and unlock the full capabilities of the device. See provided examples of using these commands to identify and deploy SEDs below.

You can configure a SED before or after assigning the device to a pool.

By default, SEDs are not locked until the administrator takes ownership of them. Ownership is taken by explicitly configuring a global or per-device password in the web interface and adding the password to the SEDs. Adding SED passwords in the web interface also allows TrueNAS to automatically unlock SEDs.

A password-protected SED protects the data stored on the device when the device is physically removed from the system. This allows secure disposal of the device without having to first wipe the contents. Repurposing a SED on another system requires the SED password.

> For TrueNAS High Availability (HA) systems, SED drives only unlock on the active controller!

Deploying SEDs

Enter command `sedutil-cli --scan` in the **Shell** to detect and list devices. The second column of the results identifies the drive type:

Character	Standard
no	non-SED device
1	Opal V1
2	Opal V2
E	Enterprise
L	Opalite
p	Pyrite V1
P	Pyrite V2
r	Ruby

Example:

```
root@truenas1:~ # sedutil-cli --scan
Scanning for Opal compliant disks
```

```
/dev/ada0  No  32GB SATA Flash Drive SFDK003L
/dev/ada1  No  32GB SATA Flash Drive SFDK003L
/dev/da0   No  HGST    HUS726020AL4210  A7J0
/dev/da1   No  HGST    HUS726020AL4210  A7J0
/dev/da10    E WDC     WUSTR1519ASS201  B925
/dev/da11    E WDC     WUSTR1519ASS201  B925
```

TrueNAS supports setting a global password for all detected SEDs or setting individual passwords for each SED. Using a global password for all SEDs is strongly recommended to simplify deployment and avoid maintaining separate passwords for each SED.

Setting a Global Password for SEDs

Go to **System Settings > Advanced > Self-Encrypting Drive** and click **Configure**. A warning displays stating **Changing Advanced settings can be dangerous when done incorrectly. Please use caution before saving.** Click **Close** to display the settings form. Enter the password in **SED Password** and **Confirm SED Password** and click **Save**.

> Record this password and store it in a safe place!

Now configure the SEDs with this password. Go to the **Shell** and enter command `sedhelper setup <password>`, where `<password>` is the global password entered in **System > Advanced > SED Password**.

`sedhelper` ensures that all detected SEDs are properly configured to use the provided password:

```
root@truenas1:~ # sedhelper setup abcd1234
da9                 [OK]
da10                [OK]
da11                [OK]
```

Rerun command `sedhelper setup <password>` every time a new SED is placed in the system to apply the global password to the new SED.

Creating Separate Passwords for Each SED

Go to **Storage** click the **Disks** dropdown in the top right of the screen and select **Disks**. From the **Disks** screen, click the ⌄ for the confirmed SED, then **Edit**. Enter and confirm the password in the **SED Password** fields to override the global SED password.

You must configure the SED to use the new password. Go to the **Shell** and enter command `sedhelper setup --disk <da1> <password>`, where `<da1>` is the SED to configure and `<password>` is the created password from **Storage > Disks > Edit Disks > SED Password**.

Repeat this process for each SED and any SEDs added to the system in the future.

> Remember SED passwords! If you lose the SED password, you cannot unlock SEDs or access their data. After configuring or modifying SED passwords, always record and store them in a secure place!

Check SED Functionality

When SED devices are detected during system boot, TrueNAS checks for configured global and device-specific passwords.

Unlocking SEDs allows a pool to contain a mix of SED and non-SED devices. Devices with individual passwords are unlocked with their password. Devices without a device-specific password are unlocked using the global password.

To verify SED locking is working correctly, go to the **Shell**. Enter command `sedutil-cli --listLockingRange 0 <password> <dev/da1>`, where `<dev/da1>` is the SED and `<password>` is the global or individual password for that SED. The command returns `ReadLockEnabled: 1`, `WriteLockEnabled: 1`, and `LockOnReset: 1` for drives with locking enabled:

```
root@truenas1:~ # sedutil-cli --listLockingRange 0 abcd1234 /dev/da9
Band[0]:
    Name:            Global_Range
    CommonName:      Locking
    RangeStart:      0
    RangeLength:     0
    ReadLockEnabled: 1
    WriteLockEnabled:1
    ReadLocked:      0
    WriteLocked:     0
    LockOnReset:     1
```

Managing SED Passwords and Data

This section contains command line instructions to manage SED passwords and data. The command used is sedutil-cli(8). Most SEDs are TCG-E (Enterprise) or TCG-Opal (Opal v2.0). Commands are different for the different drive types, so the first step is to identify the type in use.

> These commands can be destructive to data and passwords. Keep backups and use the commands with caution.

Check SED version on a single drive, */dev/da0* in this example:

```
root@truenas:~ # sedutil-cli --isValidSED /dev/da0
/dev/da0 SED --E--- Micron_5N/A U402
```

To check all connected disks at once:

```
root@truenas:~ # sedutil-cli --scan
Scanning for Opal compliant disks
/dev/ada0 No 32GB SATA Flash Drive SFDK003L
/dev/ada1 No 32GB SATA Flash Drive SFDK003L
/dev/da0 E Micron_5N/A U402
/dev/da1 E Micron_5N/A U402
/dev/da12 E SEAGATE XS3840TE70014 0103
/dev/da13 E SEAGATE XS3840TE70014 0103
/dev/da14 E SEAGATE XS3840TE70014 0103
/dev/da2 E Micron_5N/A U402
/dev/da3 E Micron_5N/A U402
/dev/da4 E Micron_5N/A U402
/dev/da5 E Micron_5N/A U402
/dev/da6 E Micron_5N/A U402
/dev/da9 E Micron_5N/A U402
No more disks present ending scan
root@truenas:~ #
```

Instructions for Specific Drives

TCG-Opal Instructions

Reset the password without losing data with command:

```
sedutil-cli --revertNoErase <oldpassword> </dev/device>
```

Use **both** of these commands to change the password without destroying data:

```
sedutil-cli --setSIDPassword <oldpassword> <newpassword> </dev/device>
sedutil-cli --setPassword <oldpassword> Admin1 <newpassword> </dev/device>
```

Wipe data and reset password to default MSID with this command:

```
sedutil-cli --revertTPer <oldpassword> </dev/device>
```

Wipe data and reset password using the PSID with this command:

`sedutil-cli --yesIreallywanttoERASEALLmydatausingthePSID <PSINODASHED> </dev/device>` where is the PSID located on the pysical drive with no dashes (-).

TCG-E Instructions

Changing or Resetting the Password without Destroying Data

Run these commands for every *LockingRange* or *band* on the drive. To determine the number of bands on a drive, use command `sedutil-cli -v --listLockingRanges </dev/device>`. Increment the `BandMaster` number and rerun the command with `--setPassword` for every band that exists.

Use **all** of these commands to reset the password without losing data:

```
sedutil-cli --setSIDPassword <oldpassword> "" </dev/device>
sedutil-cli --setPassword <oldpassword> EraseMaster "" </dev/device>
sedutil-cli --setPassword <oldpassword> BandMaster0 "" </dev/device>
sedutil-cli --setPassword <oldpassword> BandMaster1 "" </dev/device>
```

Use **all** of these commands to change the password without destroying data:

```
sedutil-cli --setSIDPassword <oldpassword* newpassword */dev/device*
sedutil-cli --setPassword <oldpassword> EraseMaster <newpassword> </dev/device>
sedutil-cli --setPassword <oldpassword> BandMaster0 <newpassword> </dev/device>
sedutil-cli --setPassword <oldpassword> BandMaster1 <newpassword> </dev/device>
```

Resetting Password and Wiping Data

Reset to default MSID:

```
sedutil-cli --eraseLockingRange 0 <password> </dev/device>
sedutil-cli --setSIDPassword <oldpassword> "" </dev/device>
sedutil-cli --setPassword <oldpassword> EraseMaster "" </dev/device>
```

Reset using the PSID:

```
sedutil-cli --PSIDrevertAdminSP <PSIDNODASHS> /dev/<device>
```

If it fails use:

```
sedutil-cli --PSIDrevert <PSIDNODASHS> /dev/<device>
```

Related Content

- Advanced Settings Screen
- Managing SEDs

3.4 - Data Protection

The Data Protection section allows users to set up multiple reduntant tasks that will protect and/or backup data in case of drive failure.

Scrub Tasks and S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) Tests can provide early disk failure alerts by identifying data integrity problems and detecting various indicators of drive reliability.

Cloud Sync, Periodic Snapshot, Rsync, and Replication Tasks, provide backup storage for data and allow users to revert the system to a previous configuration or point in time.

Ready to get started? Choose a topic or article from the left-side **Navigation** pane. Click the **<** symbol to expand the menu to show the topics under this section.

3.4.1 - Adding Replication Tasks

To streamline creating simple replication tasks use the **Replication Wizard**. The wizard assists with creating a new SSH connection and automatically creates a periodic snapshot task for sources that have no existing snapshots.

Before You Begin

Configure SSH in TrueNAS before creating a remote replication task. This ensures that new snapshots are regularly available for replication.

Setting Up Simple Replications

Process Summary

- **Data Protection > Replication Tasks**
  - Choose sources for snapshot replication.
    - Remote sources require an SSH connection.
    - TrueNAS shows the number of snapshots available to replicate.
- Define the snapshot destination.
  - A remote destination requires an SSH connection.
  - Choose a destination or define it manually by typing a path.
    - Adding a new name at the end of the path creates a new dataset.
- Choose replication security.
  - iXsystems always recommend replication with encryption.
  - Disabling encryption is only meant for absolutely secure and trusted destinations.
- Schedule the replication.
  - You can schedule standardized presets or a custom-defined schedule.
  - Running once runs the replication immediately after creation.
    - Task is still saved and you can rerun or edit it.
- Choose how long to keep the replicated snapshots.

This video tutorial presents a simple example of setting up replication:

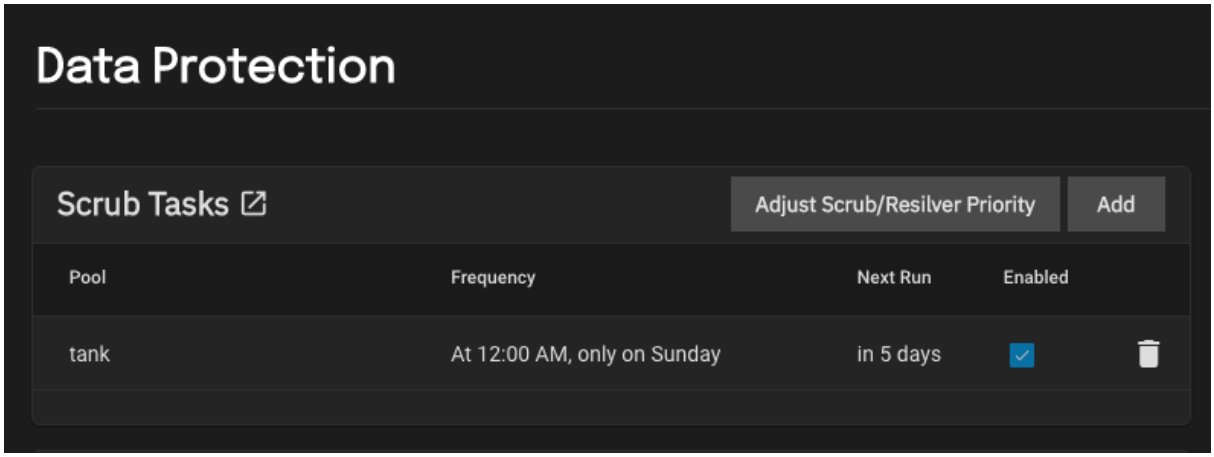
3.4.2 - Managing Scrub Tasks

This article provides instruction on running scrub and resilver tasks.

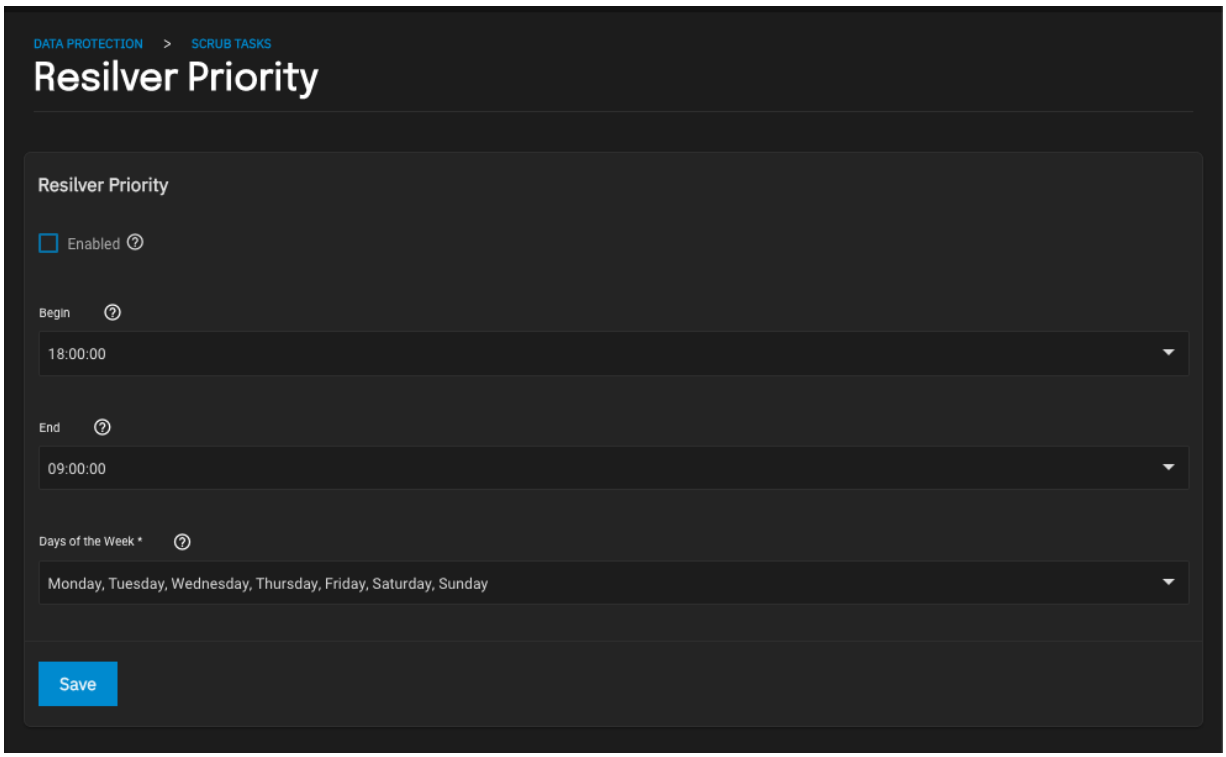
When TrueNAS performs a scrub, ZFS scans the data on a pool. Scrubs identify data integrity problems, detect silent data corruptions caused by transient hardware issues, and provide early disk failure alerts.

Default Scrub Tasks

TrueNAS generates a default scrub task when you create a new pool and sets it to run every Sunday at 12:00 AM.



Adjust Scrub/Resilver Priority



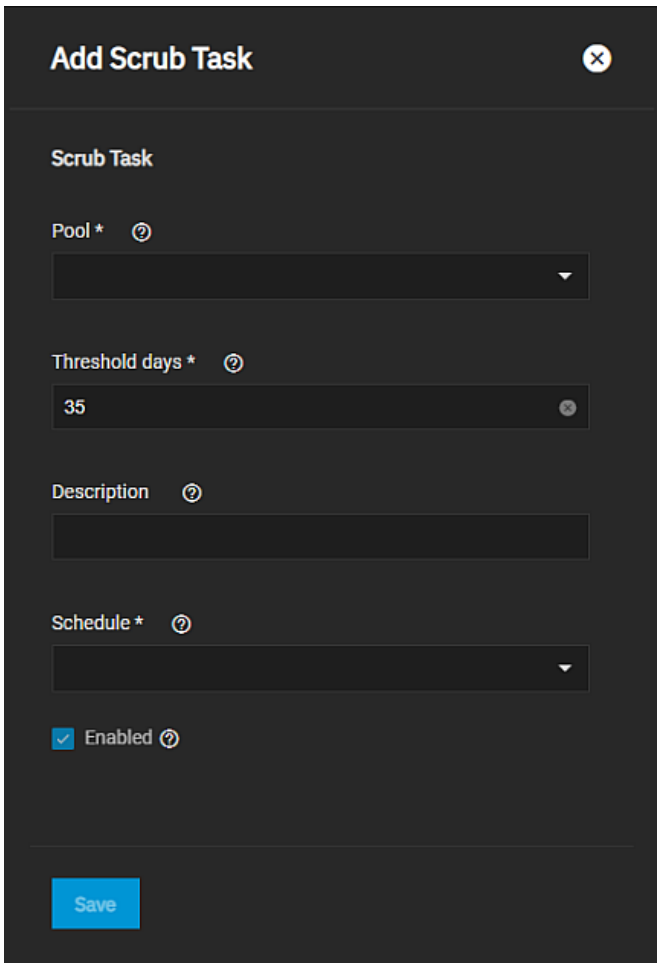
To schedule a new resilver task to run at a higher priority, select the hour and minutes from the **Begin** dropdown list.

To schedule a new resilver task to run at a lower priority to other processes, select the hour and minutes from the **End** dropdown list. Running at a lower priority is a slower process and takes longer to complete. Schedule this for times when your server is at its lowest demand level.

Creating New Scrub Tasks

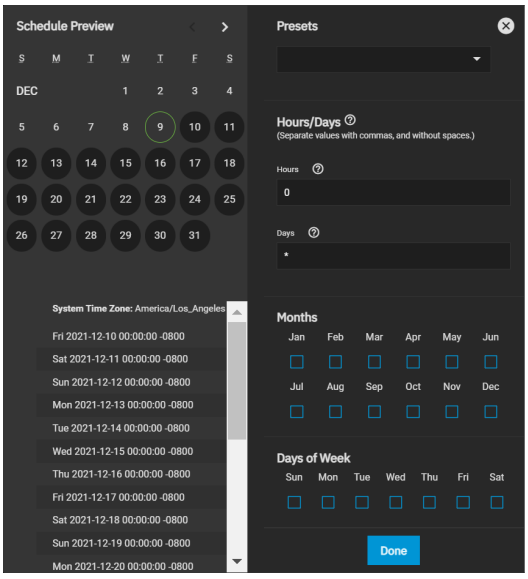
TrueNAS needs at least one data pool to create scrub task.

To create a scrub task for a pool, go to **Data Protection** and click **ADD** in the **Scrub Tasks** window.



Select a preset schedule from the dropdown list or click **Custom** to create a new schedule for when to run a scrub task. **Custom** opens the **Advanced Scheduler** window.

Advanced Scheduler



Choosing a **Presets** option populatess in the rest of the fields. To customize a schedule, enter crontab values for the `Minutes/Hours/Days`.

These fields accept standard cron values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering *10* means that the job runs when the time is ten minutes past the hour.

An asterisk (*) means match all values.

You can set specific time ranges by entering hyphenated number values. For example, entering *30-35* in the **Minutes** field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.

You can also enter lists of values. Enter individual values separated by a comma (`,`). For example, entering *1,14* in the **Hours** field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).

A slash (`/`) designates a step value. For example, entering `*` in **Days** runs the task every day of the month. Entering `*/2` runs it every other day.

Combining the above examples creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

TrueNAS has an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days in addition to any listed days. For example, entering *1* in **Days** and setting *Wed* for **Days of Week** creates a schedule that starts a task on the first day of the month *and* every Wednesday of the month.

The **Schedule Preview** dipslays when the current settings mean the task runs.

Examples of CRON syntax

Syntax	Meaning	Examples
*	Every item.	* (minutes) = every minute of the hour. * (days) = every day.
*/N	Every N^{th} item.	*/15 (minutes) = every 15th minute of the hour. */3 (days) = every 3rd day. */3 (months) = every 3rd month.
Comma and hyphen/dash	Each stated item (comma) Each item in a range (hyphen/dash).	1,31 (minutes) = on the 1st and 31st minute of the hour. 1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour. mon-fri (days) = every Monday to Friday inclusive (every weekday). mar,jun,sep,dec (months) = every March, June, September, December.

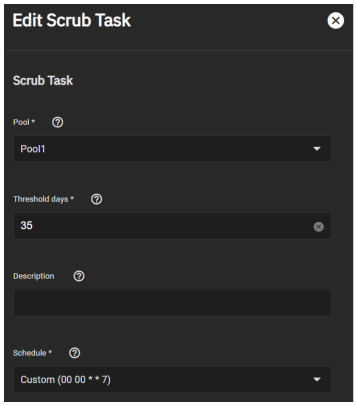
You can specify days of the month or days of the week.

TrueNAS lets users create flexible schedules using the available options. The table below has some examples:

Desired schedule	Values to enter
3 times a day (at midnight, 08:00 and 16:00)	months=*; days=*; hours=0/8 or 0,8,16; minutes=0 (Meaning: every day of every month, when hours=0/8/16 and minutes=0)
Every Monday/Wednesday/Friday, at 8.30 pm	months=*; days=mon,wed,fri; hours=20; minutes=30
1st and 15th day of the month, during October to June, at 00:01 am	months=oct-dec,jan-jun; days=1,15; hours=0; minutes=1
Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday	Note that this requires two tasks to achieve: (1) months=*; days=mon-fri; hours=8-18; minutes=*/15 (2) months=*; days=mon-fri; hours=19; minutes=0 We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00.

Editing Scrub Tasks

To edit a scrub, go to **Data Protection** and click the scrub task you want to edit.



Related Content

- Scrub Tasks Screens

3.4.3 - Cloud Sync Tasks

Article Summaries

- Adding Cloud Sync Tasks

  This article provides instructions to add a cloud sync task, configure environment variables, run an unscheduled sync task, create a copy of a task with a reversed transfer mode, and troubleshoot common issues with some cloud storage providers.

- Backing Up Google Drive to TrueNAS SCALE

  This article provides instructions on adding Google Drives cloud credentials using **Add Cloud Credentials** and **Add Cloud Sync Task** screens. It also provides information on working with Google-created content.

3.4.3.1 - Adding Cloud Sync Tasks

This article provides instructions to add a cloud sync task, configure environment variables, run an unscheduled sync task, create a copy of a task with a reversed transfer mode, and troubleshoot common issues with some cloud storage providers.

TrueNAS can send, receive, or synchronize data with a cloud storage provider. Cloud sync tasks allow for single-time transfers or recurring transfers on a schedule. They are an effective method to back up data to a remote location.

> Using the cloud means data can go to a third-party commercial vendor not directly affiliated with iXsystems. You should fully understand vendor pricing policies and services before using them for cloud sync tasks.
>
> iXsystems is not responsible for any charges incurred from using third-party vendors with the cloud sync feature.

TrueNAS supports major providers like Amazon S3, Google Cloud, and Microsoft Azure. It also supports many other vendors. To see the full list of supported vendors, go to **Credentials > Backup Credentials > Cloud Credentials** click **Add** and open the **Provider** dropdown list.

Cloud Sync Task Requirements

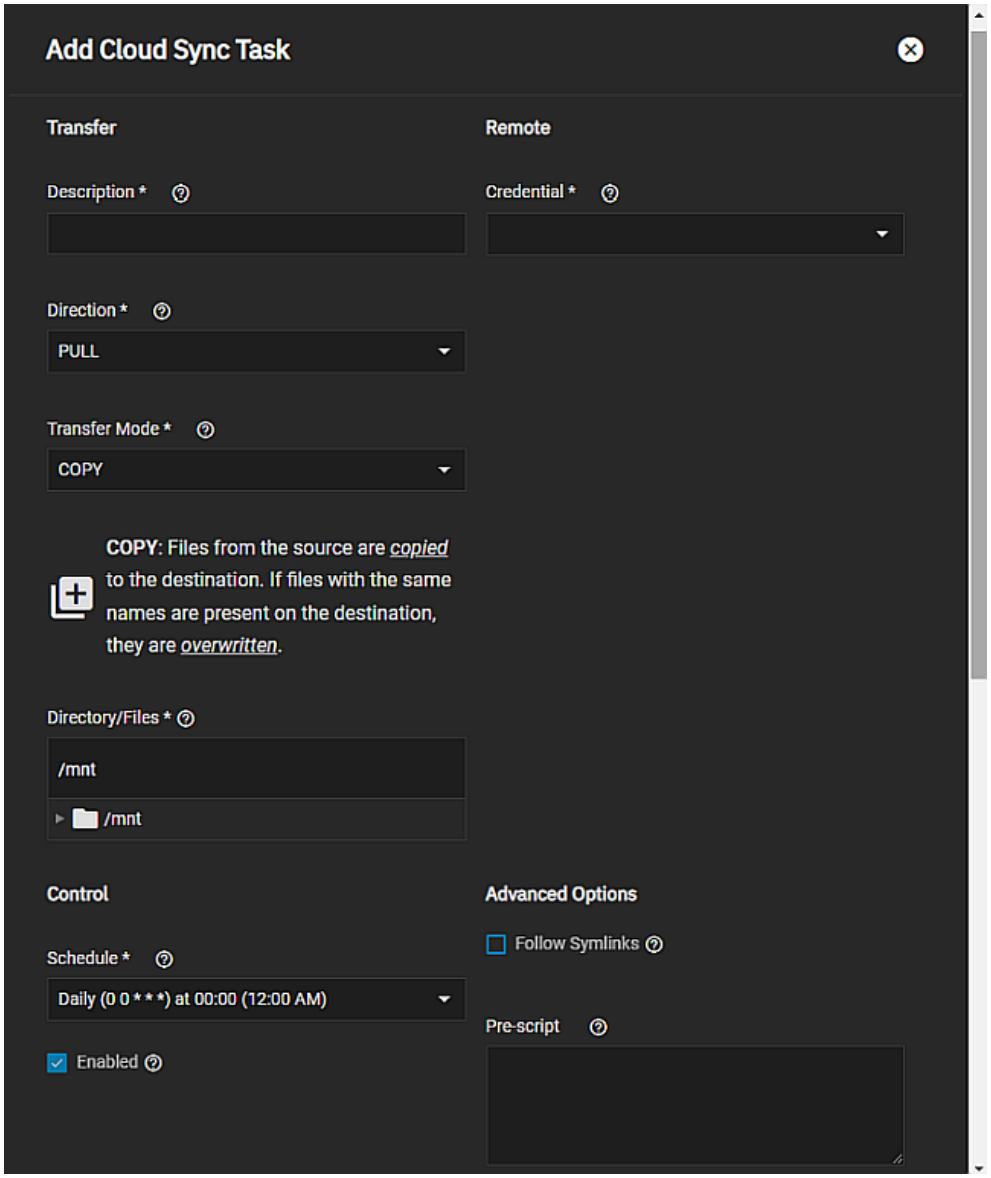
- You must have all system storage configured and ready to receive or send data.
- You must have a cloud storage provider account and location (like an Amazon S3 bucket).

You can create the cloud storage account credentials using **Credentials > Backup Credentials > Cloud Credentials** before creating the sync task or add it at the time you create the cloud sync task on **Data Protection > Cloud Sync Task > Add Cloud Sync Task**. See the Cloud Credentials article for instructions on adding a backup credential using cloud credentials.

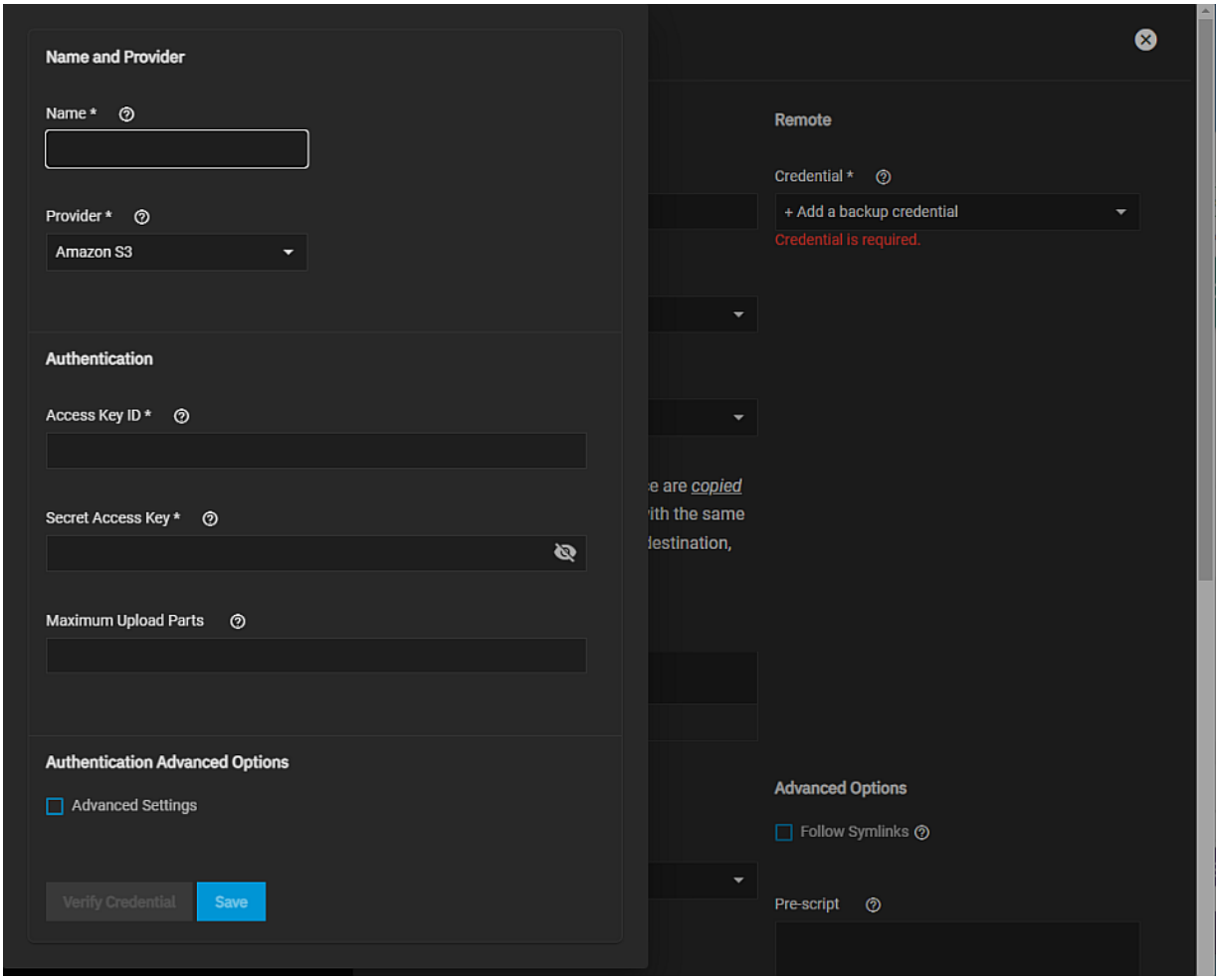
Creating a Cloud Sync Task

Adding Cloud Sync Tutorial Video ↧

To add a cloud sync task, go to **Data Protection > Cloud Sync Tasks** and click **Add**. The **Add Cloud Sync Task** configuration screen opens.



1. (Required) Type a memorable task description in **Description**.
2. Select an existing backup credential from the **Credential** dropdown list or select **+ Add a backup credential** to add a new backup credential. **+ Add a backup credential** opens a backup credential configuration window.



a. (Required) Enter a name for the backup credential.

b. Select the cloud storage provider from the **Provider** dropdown list. The authentication fields displayed vary by provider. See Adding Cloud Credentials for more information on authentication settings for each provider.

c. Enter the authentication credentials for the selected provider.

d. Click **Verify Credentials**. TrueNAS attempts to connect to the selected provider with the authentication settings entered.

e. Click **Save**. The backup credentials window closes and the **Credentials** field displays the newly created backup credential. The **Bucket** field displays if using S3 to connect.

3. Select the direction for the sync task. **PULL** brings files from the cloud storage provider to the location specified in **Directory/Files** (this is the location on TrueNAS SCALE). **PUSH** sends files from the location in **Directory/Files** to the cloud storage provider location you specify in **Folder**.

4. Select the transfer method from the **Transfer Mode** dropdown list. **Sync** keeps files identical on both TrueNAS SCALE and the remote cloud provider server. If the sync encounters an error, destination server files are not deleted. **Copy** duplicates files on both the TrueNAS SCALE and remote cloud provider server. **Move** transfer the files to the destination server and then deleted the copy on server that transferred the files. It also overwrites files with the same names on the destination.

5. Enter or browse to the dataset or folder directory using the ▸ arrow to the left of 🗀/ under the **Directory/Files** and **Folder** fields. Select the TrueNAS SCALE dataset path in **Directory/Files** and the Google Drive path in **Folder**. If **PUSH** is the selected **Direction**, this is where on TrueNAS SCALE the files you want to copy, sync or move transfer to the provider. If **Direction** is set to **PULL** this is the location where on TrueNAS SCALE you want to copy, sync or move files to.

   Click the ▸ to the left of 🗀/ to collapse the folder tree.

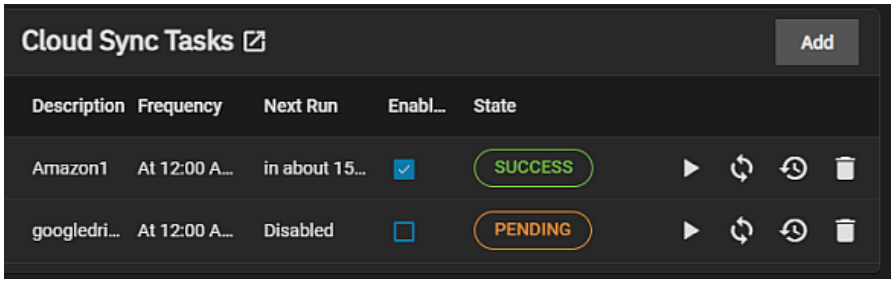
6. Select the preset from the **Schedule** dropdown that defines when the task runs. For a specific schedule, select **Custom** and use the **Advanced Scheduler**. Clear the **Enable** checkbox to make the configuration available without allowing the specified schedule to run the task.

   To manually activate a saved task, go to **Data Protection > Cloud Sync Tasks**, click ▶ for the cloud sync task you want to run. Click **CONTINUE** or **CANCEL** for the **Run Now** operation.

7. (Optional) Set any advanced option you want or need for your use case or define environment variables in either the **Pre-script** or **Post-script** fields. These fields are for advanced users.

8. Click then click **Dry Run** to test your settings before you click **Save**. TrueNAS connects to the cloud storage provider and simulates a file transfer but does not send or receive data.

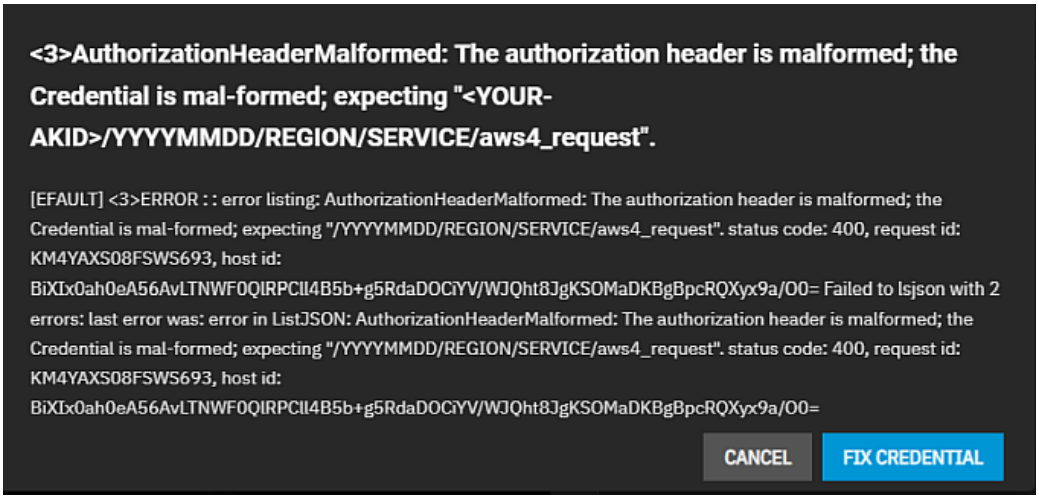
The new cloud sync task displays on the **Cloud Sync Tasks** widget with the status of **PENDING** until it completes. If the task completes without issue the status becomes **SUCCESS**.



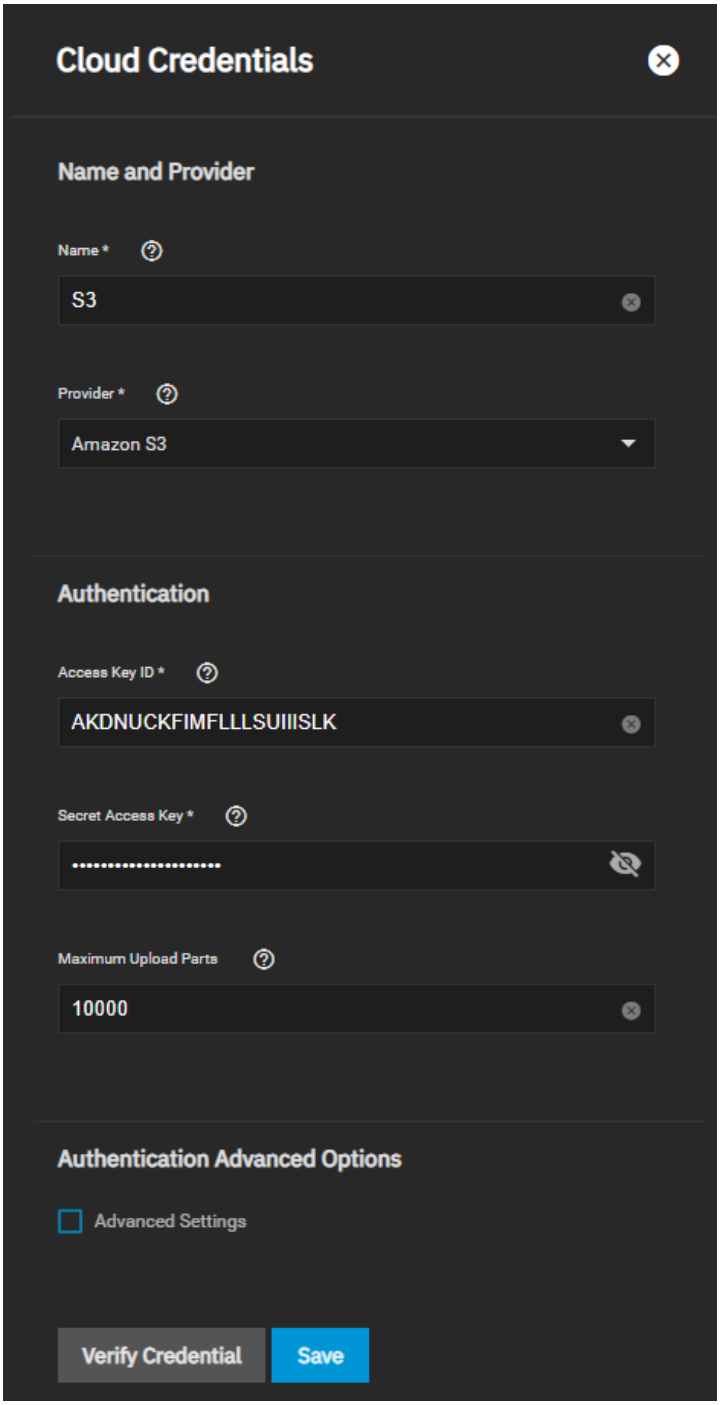
See **Using Scripting and Environment Variables** for more information on environment variables.

What happens if my cloud sync credentials are invalid?

After you choose a cloud credential from the dropdown list, TrueNAS automatically validates access to that cloud sync provider. Invalid credentials results in the following alert:



Click **FIX CREDENTIAL** opens the **Credentials > Cloud Credentials > Edit Cloud Credentials** screen for the cloud service selected in **Credentials**.



Check your provider credentials and update the applicable authentication fields on the **Edit Cloud Credentials** screen, and then click **Verify Credential**. If TrueNAS successfully accesses the provider the system displays the **The Credential is valid** dialog. Click **Save** and then return to **Data Protection > Cloud Sync Tasks > Add** to try again.

Troubleshooting Transfer Mode Problems

Sync keeps all the files identical between the two storage locations. If the sync encounters an error, it does not delete files in the destination.

Dropbox Issues

One common error occurs when the Dropbox copyright detector flags a file as copyrighted.

BackBlaze B2 Issues

Syncing to a Backblaze B2 bucket does not delete files from the bucket, even when you deleted those files locally. Instead, files are tagged with a version number or moved to a hidden state. To automatically delete old or unwanted files from the bucket, adjust the Backblaze B2 Lifecycle Rules.

Amazon S3 Issues

Sync cannot delete files stored in Amazon S3 Glacier or S3 Glacier Deep Archive. First restore these files by another means, like the Amazon S3 console.

Using Scripting and Environment Variables

Advanced users can write scripts that run immediately before or after the cloud sync task. Using either the **Add Cloud Sync Task** or **Edit Cloud Sync Task** screens, enter environment variables to either the **Pre-script** or **Post-script** fields. The **Post-script** field only runs when the cloud sync task succeeds.

Click here for Environment Variables

General Environment Variables

- `CLOUD_SYNC_ID`
- `CLOUD_SYNC_DESCRIPTION`
- `CLOUD_SYNC_DIRECTION`
- `CLOUD_SYNC_TRANSFER_MODE`
- `CLOUD_SYNC_ENCRYPTION`
- `CLOUD_SYNC_FILENAME_ENCRYPTION`
- `CLOUD_SYNC_ENCRYPTION_PASSWORD`
- `CLOUD_SYNC_ENCRYPTION_SALT`
- `CLOUD_SYNC_SNAPSHOT`

Provider-Specific Variables

There also are provider-specific variables like CLOUD_SYNC_CLIENT_ID or CLOUD_SYNC_TOKEN or CLOUD_SYNC_CHUNK_SIZE.

Remote storage settings:

- `CLOUD_SYNC_BUCKET`
- `CLOUD_SYNC_FOLDER`

Local storage settings:

- `CLOUD_SYNC_PATH`

Running an Unscheduled Cloud Sync Task

Saved tasks activate according to their schedule or you can use the **Run Now** option the **Cloud Sync Task** widget.
To run the sync task before the saved schedule for the task, click on the cloud sync task to open the edit configuration screen for that task. If not already cleared, select **Enable** below the **Schedule** field to clear the checkbox, and then click **Save**.

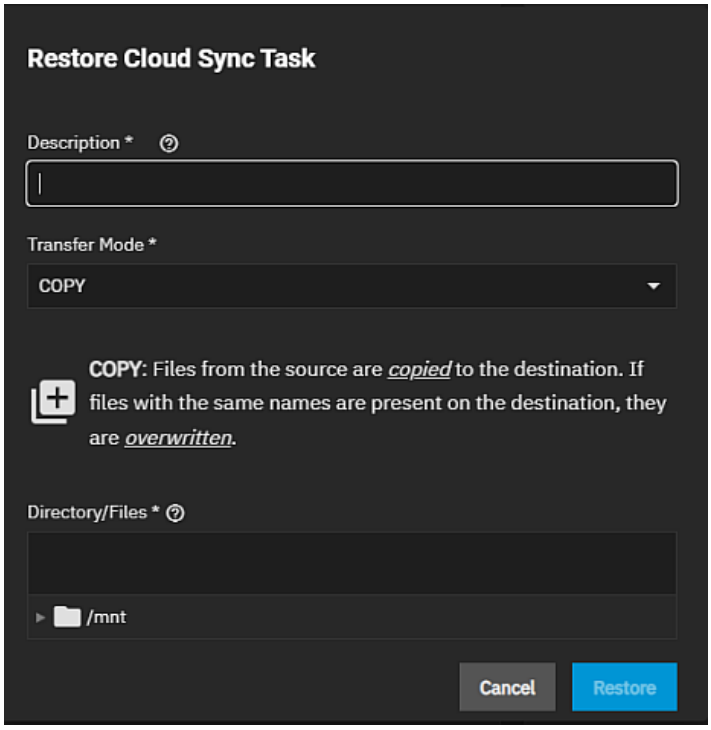
On the **Cloud Sync Task** widget, click the **Run Now** ▶ button.

An in-progress cloud sync must finish before another can begin. Stopping an in-progress task cancels the file transfer and requires starting the file transfer over.

To view logs about a running task, or its most recent run, click **State**.

Using Cloud Sync Task Restore

To create a new cloud sync task that uses the same options but reverses the data transfer, select for an existing cloud sync on the **Data Protection** page. The **Restore Cloud Sync Task** window opens.



Enter a name in **Description** for this reversed task.

Select the **Transfer Mode** and then define the path for a storage location on TrueNAS scale for the transferred data.

Click **Restore**.

TrueNAS saves the restored cloud sync as another entry in **Data protection > Cloud Sync Tasks**.

If you set the restore destination to the source dataset, TrueNAS may alter ownership of the restored files to **root**. If root did not create the original files and you need them to have a different owner, you can recursively reset their ACL permissions through the GUI or run `chown` from the CLI.

Related Content

- Adding Cloud Credentials
- Backing Up Google Drive to TrueNAS SCALE
- Cloud Credentials Screens
- Cloud Sync Tasks
- Cloud Sync Tasks Screens

3.4.3.2 - Backing Up Google Drive to TrueNAS SCALE

This article provides instructions on adding Google Drives cloud credentials using **Add Cloud Credentials** and **Add Cloud Sync Task** screens. It also provides information on working with Google-created content.

Google Drive and G Suite are widely used tools for creating and sharing documents, spreadsheets, and presentations with team members. While cloud-based tools have inherent backups and replications included by the cloud provider, certain users might require additional backup or archive capabilities. For example, companies using G Suite for important work might be required to keep records for years, potentially beyond the scope of the G Suite subscription. TrueNAS offers the ability to easily back up Google Drive by using the built-in cloud sync.

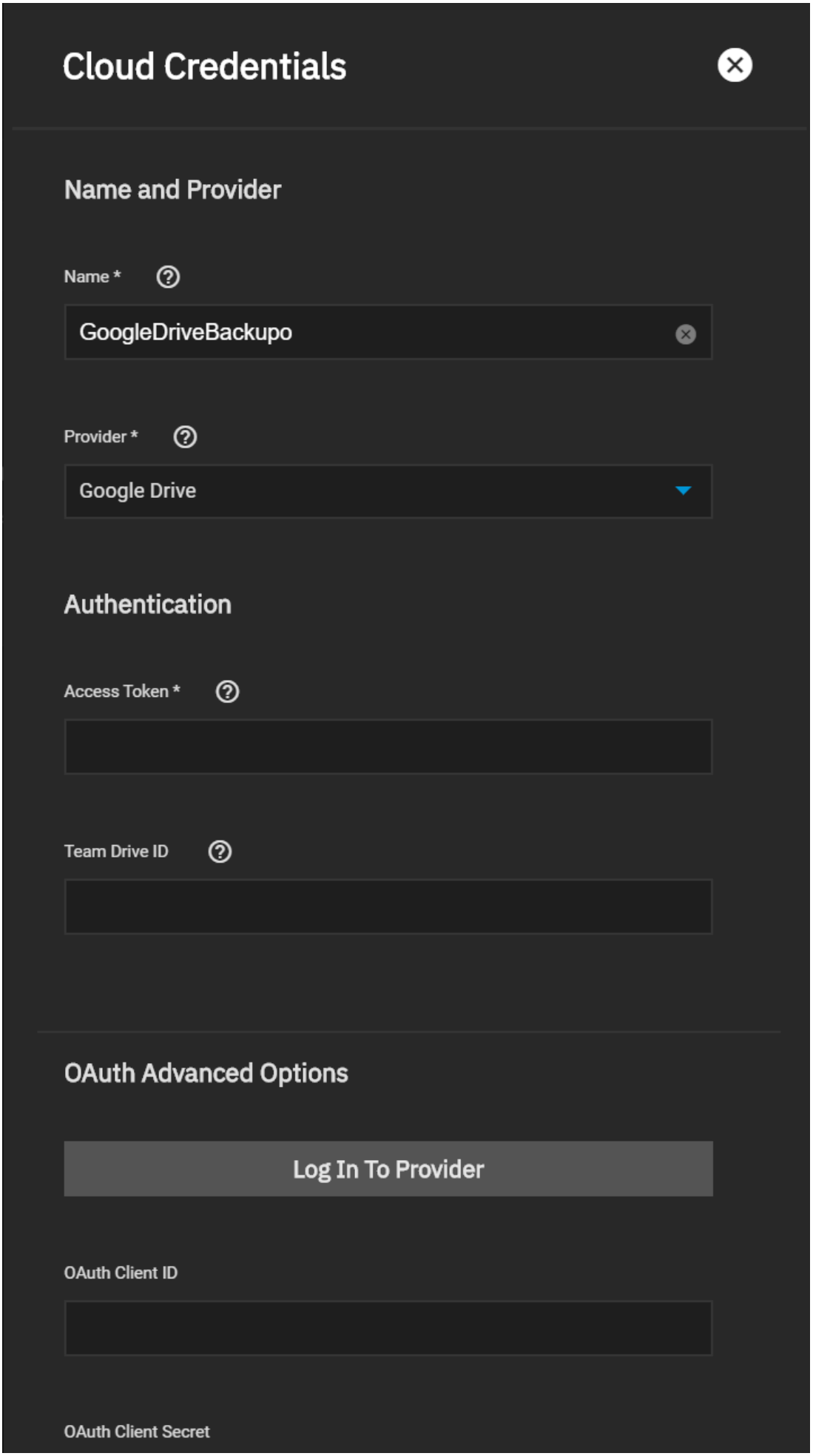
Setting up Google Drive Credentials

You can add Google Drive credentials using the **Add Cloud Credentials** screen accessed from the **Credentials > Backup Credentials > Cloud Credentials** screen, or you can add them when you create a cloud sync task using the **Add Cloud Sync Task** screen accessed from the **Data Protection > Cloud Sycn Task** screen.

Adding Google Drive Credentials Using Cloud Credentials

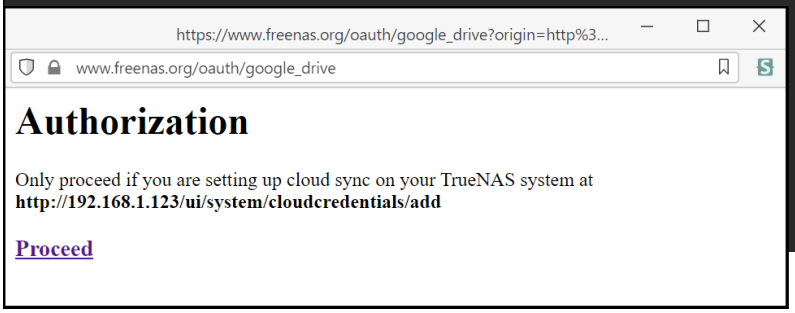
To set up a cloud credential, go to **Credentials > Backup Credentials** and click **Add** in the **Cloud Credentials** widget.

1. Enter a credential name.
2. Select **Google Drive** on the **Provider** dropdown list. The Google Drive authentication settings display on the screen.
3. Enter the Google Drive authentication settings.

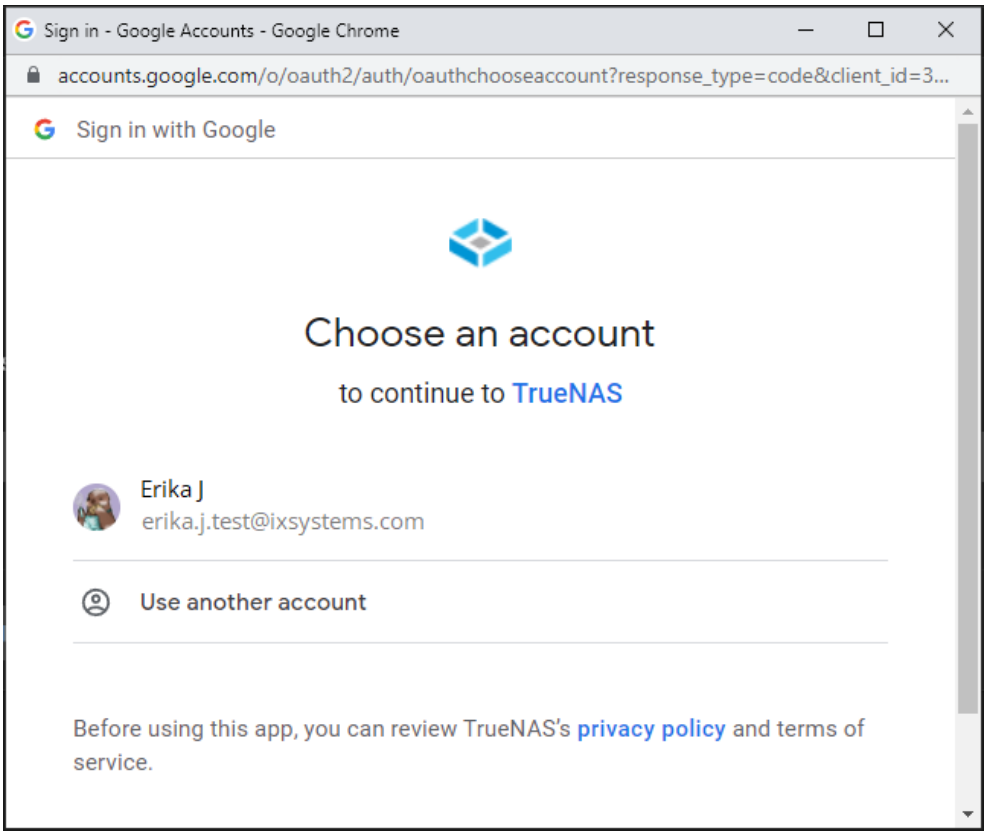

Cloud Credentials
Name and Provider
Name *
GoogleDriveBackupo
Provider *
Google Drive
Authentication
Access Token *
Team Drive ID
OAuth Advanced Options
Log In To Provider
OAuth Client ID
OAuth Client Secret

a. Enter the Google Drive user name and password.

b. Click **Log In To Provider**. The Google **Authentication** window opens.

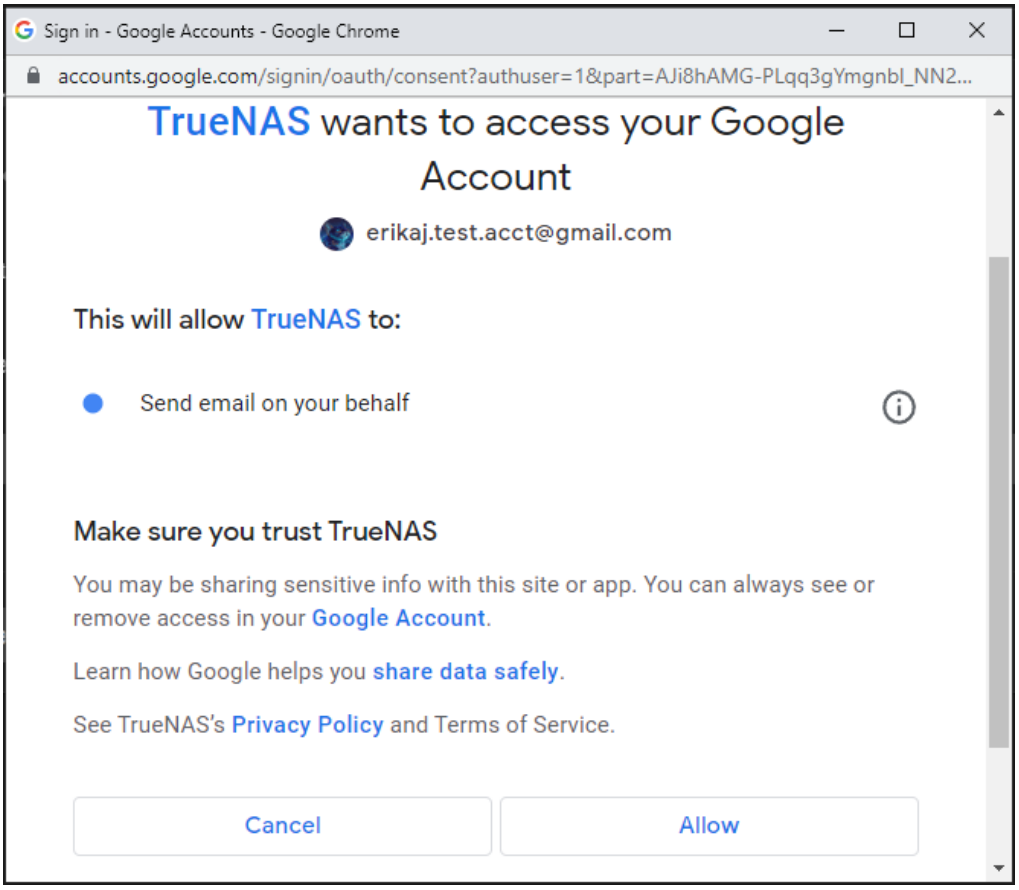


c. Click **Proceed** to open the **Choose an Account** window.



d. Select the email account to use. Google displays the **Sign In** window. Enter the password and click **Next** to enter the password. Click **Next** again. Google might display a **Verify it's you** window. Enter a phone number where Google can text an verification code, or you can click **Try another way**.

e. Click **Allow** on the **TrueNAS wants to access your Google Account** window. TrueNAS populates **Access Token** with the token Google provides.

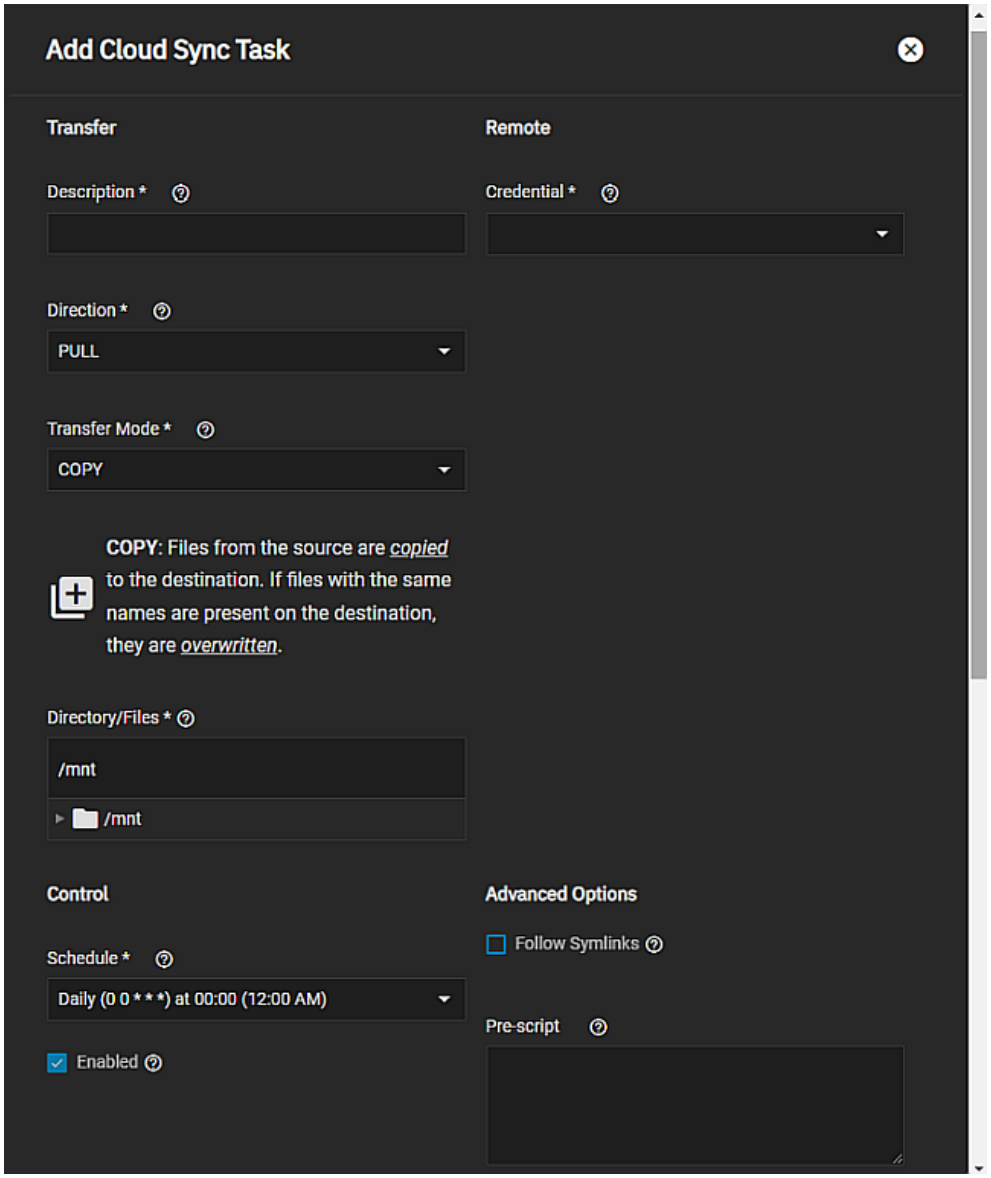


4. Click **Verify Credentials** and wait for TrueNAS to display the verification dialog with verified status. Close the dialog.
5. Click **Save**. The **Cloud Credentials** widget displays the new credentials. These are also available for cloud sync tasks to use.

Adding Cloud Credentials Using Cloud Sync Task

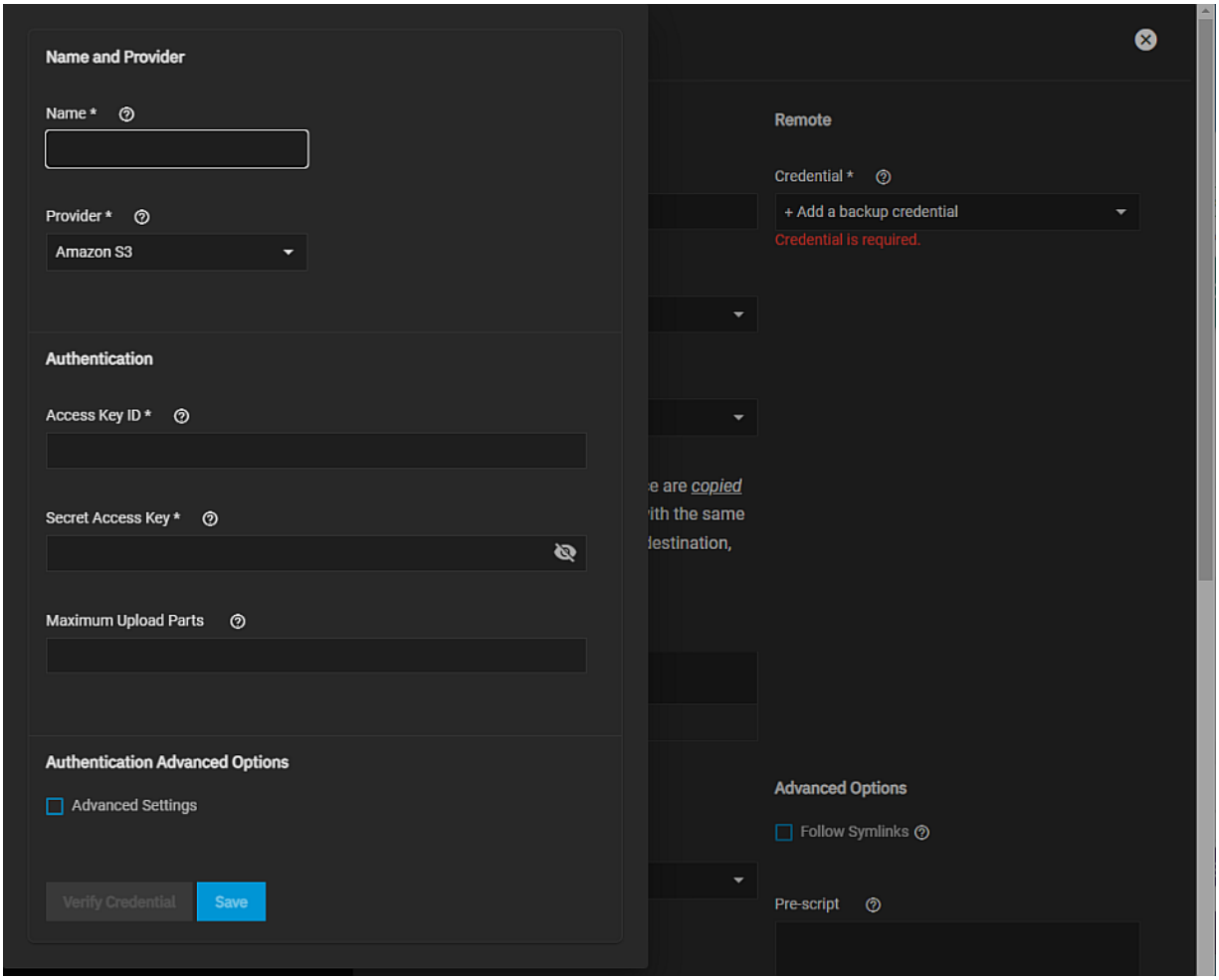
You can add a new cloud credential on the **Add Cloud Sync Task** screen.

To add a cloud sync task, go to **Data Protection > Cloud Sync Tasks** and click **Add**. The **Add Cloud Sync Task** configuration screen opens.



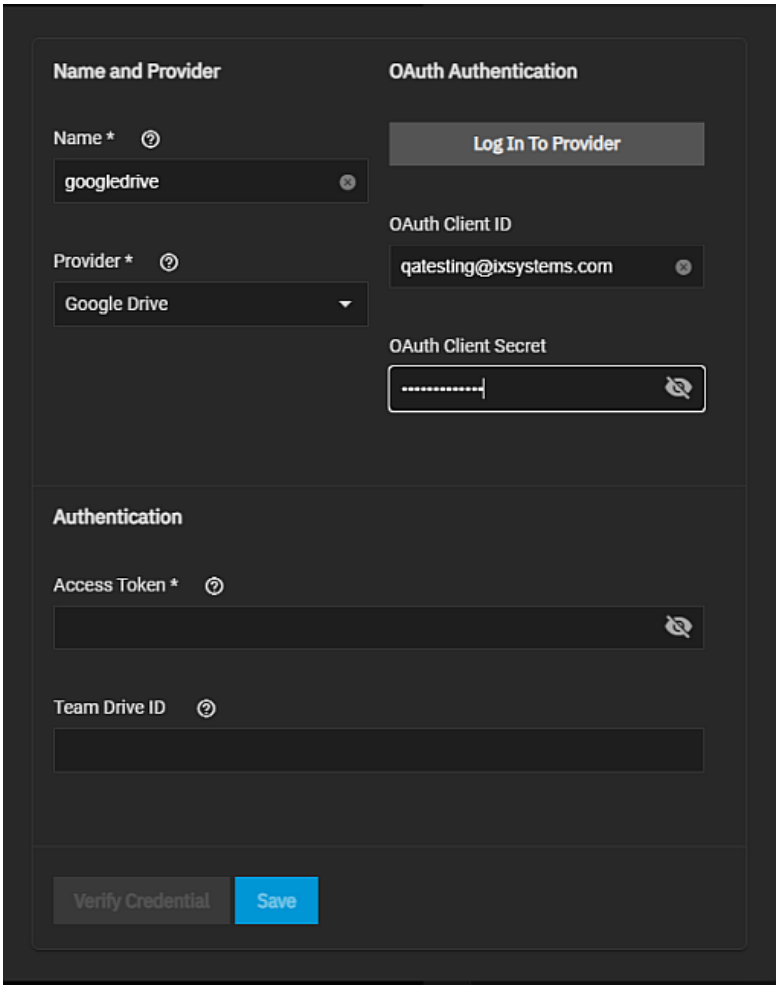
1. (Required) Type a memorable task description in **Description**. For example, *googledrivepush* to represent the provider name and transfer direction.

2. Select **+ Add a backup credential** from the **Credential** dropdown list to add a new backup credential. **+ Add a backup credential** opens a backup credential configuration window.



a. (Required) Enter a name for the backup credential. For example, *googledrive*.

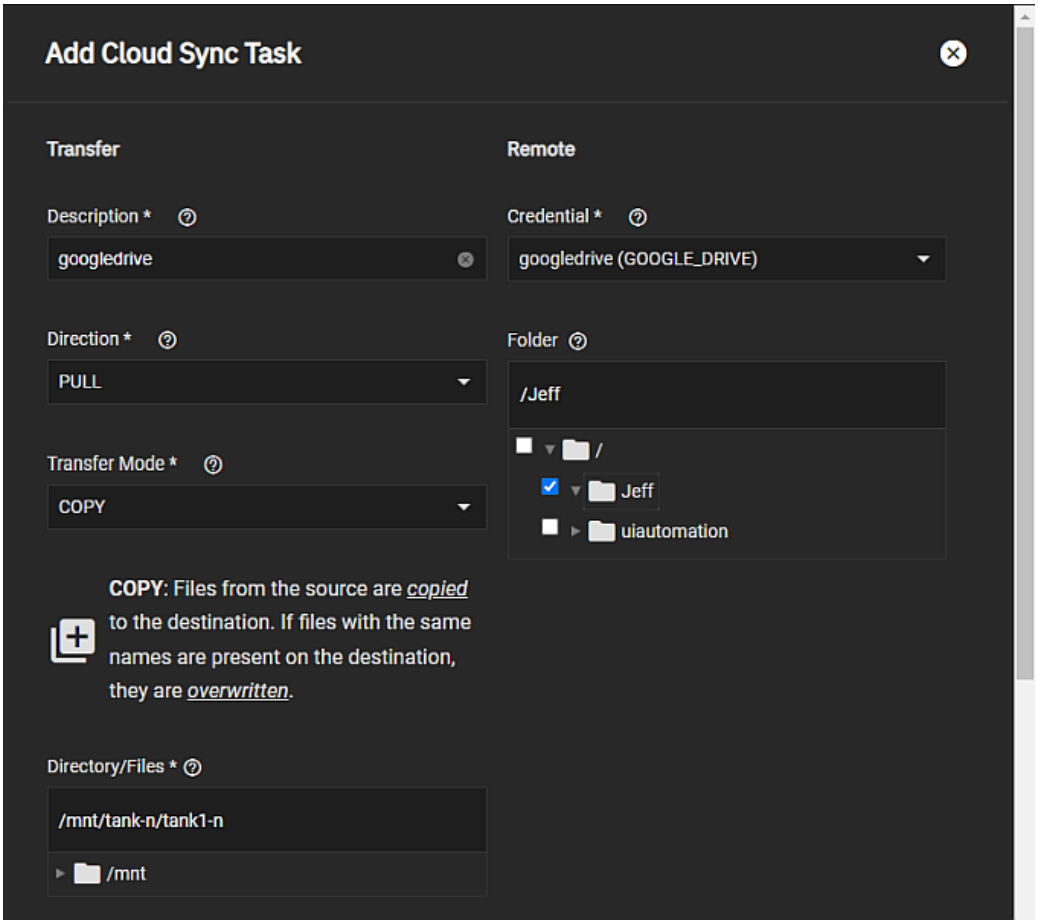
b. Select the **Google Drive** from the **Provider** dropdown list. The Google Drive authentication fields display. See Adding Cloud Credentials for more information on authentication settings for each provider.



c. Enter the Google Drive account email and password, then click **Log In To Provider**. Google displays the authentication windows just as in the process described in step 3 in the cloud credentials procedure above.

d. Click **Verify Credentials**. TrueNAS attempts to connect to the selected provider with the authentication settings entered.

e. Click **Save**. The backup credentials window closes and the **Credentials** field displays the newly created backup credential.



3. Select the direction for the sync task. **PULL** brings files from the cloud storage provider to the location specified in **Directory/Files** (this is the location on TrueNAS SCALE). **PUSH** sends files from the location in **Directory/Files** to the cloud storage provider location you specify in **Folder**.

4. Select the transfer method from the **Transfer Mode** dropdown list. **Sync** keeps files identical on both TrueNAS SCALE and the remote cloud provider server. If the sync encounters an error, destination server files are not deleted. **Copy** duplicates files on both the TrueNAS SCALE and remote cloud provider server. **Move** transfer the files to the destination server and then deleted the copy on server that transferred the files. It also overwrites files with the same names on the destination.

5. Enter or browse to the dataset or folder directory using the ▸ arrow to the left of 🗀/ under the **Directory/Files** and **Folder** fields. Select the TrueNAS SCALE dataset path in **Directory/Files** and the Google Drive path in **Folder**. If **PUSH** is the selected **Direction**, this is where on TrueNAS SCALE the files you want to copy, sync or move transfer to the provider. If **Direction** is set to **PULL** this is the location where on TrueNAS SCALE you want to copy, sync or move files to.

   Click the ▸ to the left of 🗀/ to collapse the folder tree.

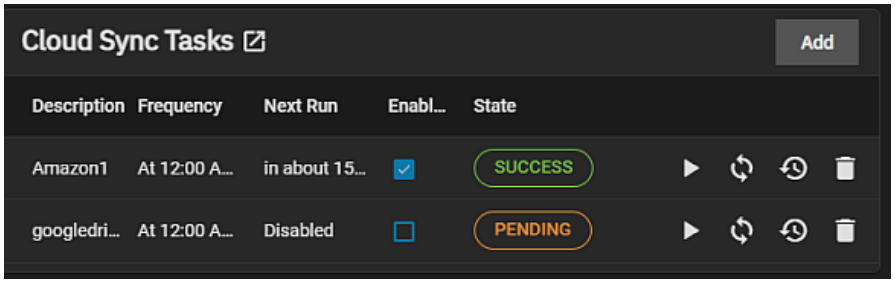
6. Select the preset from the **Schedule** dropdown that defines when the task runs. For a specific schedule, select **Custom** and use the **Advanced Scheduler**. Clear the **Enable** checkbox to make the configuration available without allowing the specified schedule to run the task.

   To manually activate a saved task, go to **Data Protection > Cloud Sync Tasks**, click ▶ for the cloud sync task you want to run. Click **CONTINUE** or **CANCEL** for the **Run Now** operation.

7. (Optional) Set any advanced option you want or need for your use case or define environment variables in either the **Pre-script** or **Post-script** fields. These fields are for advanced users.

8. Click then click **Dry Run** to test your settings before you click **Save**. TrueNAS connects to the cloud storage provider and simulates a file transfer but does not send or receive data.

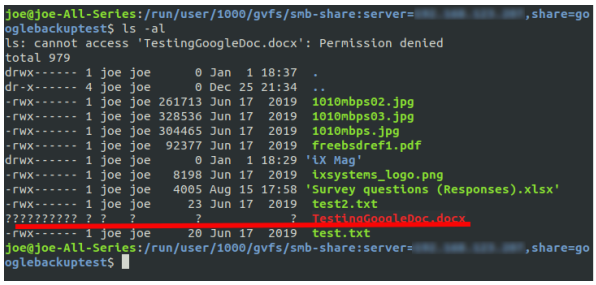
The new cloud sync task displays on the **Cloud Sync Tasks** widget with the status of **PENDING** until it completes. If the task completes without issue the status becomes **SUCCESS**.



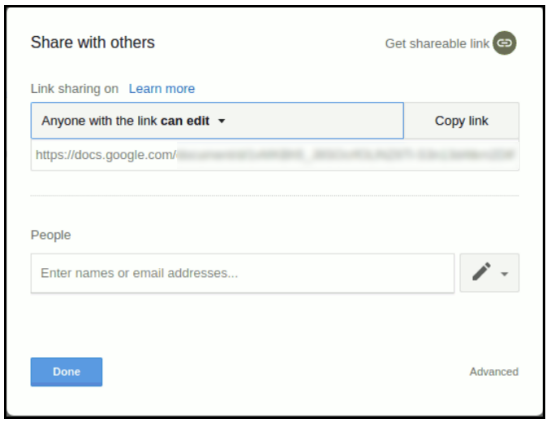
See **Using Scripting and Environment Variables** for more information on environment variables.

Working with Google Created Content

One caveat is that Google Docs and other files created with Google tools have their own proprietary set of permissions and their read/write characteristics unknown to the system over a standard file share. Files are unreadable as a result.



To allow Google-created files to become readable, allow link sharing to access the files before the backup. Doing so ensures that other users can open the files with read access, make changes, and then save them as another file if further edits are needed. Note that this is only necessary if the file was created using Google Docs, Google Sheets, or Google Slides; other files should not require modification of their share settings.



TrueNAS is perfect for storing content, including cloud-based content, for the long term. Not only is it simple to sync and backup from the cloud, but users can rest assured that their data is safe, with snapshots, copy-on-write, and built-in replication functionality.

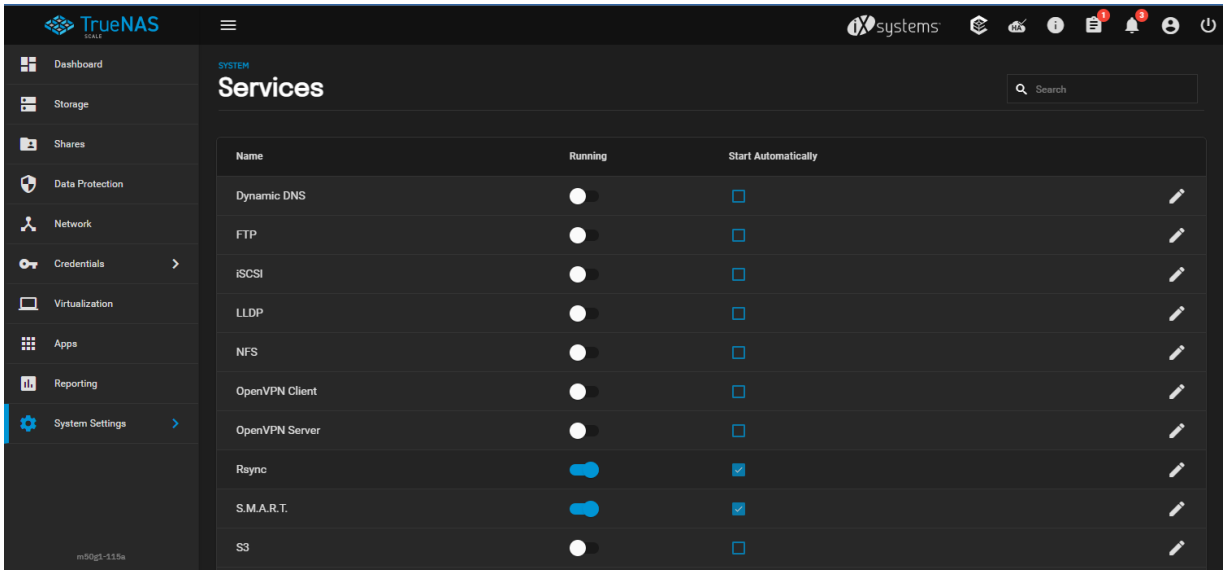
3.4.4 - Configuring Rsync Tasks

This article provides instructions on adding rsync tasks using either of two methods, one using an rsync module created in TrueNAS and the other using an SSH connection.

You often need to copy data to another system for backup or when migrating to a new system. A fast and secure way of doing this is by using rsync. These instructions assume that both sides of the rsync task, host and remote, use a TrueNAS systems.

Rsync Service and Modules

The rsync task does not work unless the related system service is turned on. To turn the rsync service on, go to **System > Services** and toggle the **Rsync** on. To activate the service whenever TrueNAS boots, select the **Start Automatically** checkbox.



Click the ✎ to configure the service on the **Services > RSYNC > Rsync** screen. There are two tabs for rsync configuration: basic **Configure** options and **Rsync Module** creation and management.

Rsync Basic Requirements

For an remote synch (rsync) task to work you need to first:

- Create a dataset on both the TrueNAS and know the host and path to the data on the remote system you plan to sync with.
- Create at least one rsync module in TrueNAS SCALE in **Services > Rsync > Rsync Module**

  or

  Create an SSH connection in **Credentials > Backup Credentials > SSH Connections**.
- Turn on the rsync service on both the TrueNAS and in the remote server.

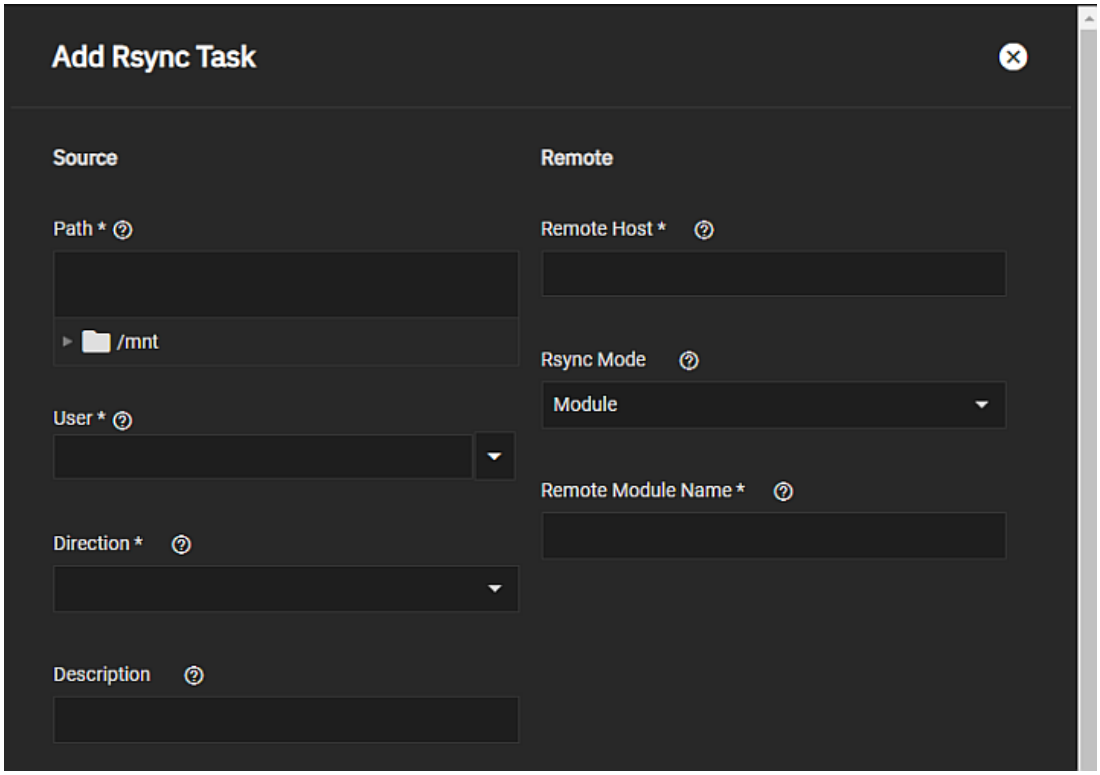
Rsync provides the ability to either push or pull data. The **Rsync Tasks** task push function copies data from the TrueNAS host system to a remote system. The **Rsync Tasks** task pull function moves or copies data from a remote system and puts on the TrueNAS host system.

> The remote system must have the rsync service activated.

Creating an Rsync Task

Tutorial Video ↧

Go to **Data Protection > Rsync Tasks** and click **Add** to open the **Add Rsync Task** configuration screen.



Enter or use the ▸ to the left of **/mnt** to browse to the path to copy.

Begin typing the user into the **User** field or select the user from the dropdown list. The user must have permissions to run an rsync on the remote server.

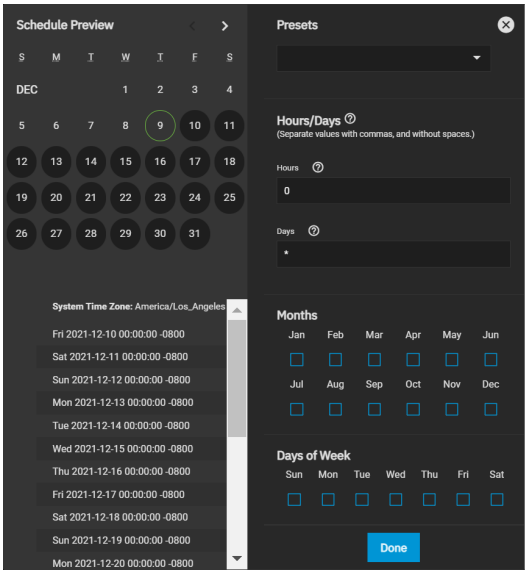
Select the direction. Select **Pull** to copy from the remote server to the TrueNAS SCALE server location, or **Push** to copy from the TrueNAS to the remote server.

Enter the remote host name or IP in **Remote Host**. You need to have the remote server rsync service configured and turned on.

Select the connection mode from the **Rsync Mode** dropdown. Each mode option displays settings for the selected type. You need to have either a rsync module configured or an SSH connection for the remote server already configured.

Set the schedule for when to run this task, and any other options you want to use. If you need a custom schedule, select **Custom** to open the advanced scheduler window.

Advanced Scheduler



Choosing a **Presets** option populatess in the rest of the fields. To customize a schedule, enter crontab values for the `Minutes/Hours/Days`.

These fields accept standard cron values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering *10* means that the job runs when the time is ten minutes past the hour.

An asterisk (*) means match all values.

You can set specific time ranges by entering hyphenated number values. For example, entering *30-35* in the **Minutes** field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.

You can also enter lists of values. Enter individual values separated by a comma (`,`). For example, entering *1,14* in the **Hours** field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).

A slash (`/`) designates a step value. For example, entering `*` in **Days** runs the task every day of the month. Entering `*/2` runs it every other day.

Combining the above examples creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

TrueNAS has an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days in addition to any listed days. For example, entering *1* in **Days** and setting *Wed* for **Days of Week** creates a schedule that starts a task on the first day of the month *and* every Wednesday of the month.

The **Schedule Preview** dipslays when the current settings mean the task runs.

Examples of CRON syntax

Syntax	Meaning	Examples
*	Every item.	* (minutes) = every minute of the hour. * (days) = every day.
*/N	Every N^{th} item.	*/15 (minutes) = every 15th minute of the hour. */3 (days) = every 3rd day. */3 (months) = every 3rd month.
Comma and hyphen/dash	Each stated item (comma) Each item in a range (hyphen/dash).	1,31 (minutes) = on the 1st and 31st minute of the hour. 1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour. mon-fri (days) = every Monday to Friday inclusive (every weekday). mar,jun,sep,dec (months) = every March, June, September, December.

You can specify days of the month or days of the week.

TrueNAS lets users create flexible schedules using the available options. The table below has some examples:

Desired schedule	Values to enter
3 times a day (at midnight, 08:00 and 16:00)	months=*; days=*; hours=0/8 or 0,8,16; minutes=0 (Meaning: every day of every month, when hours=0/8/16 and minutes=0)
Every Monday/Wednesday/Friday, at 8.30 pm	months=*; days=mon,wed,fri; hours=20; minutes=30
1st and 15th day of the month, during October to June, at 00:01 am	months=oct-dec,jan-jun; days=1,15; hours=0; minutes=1
Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday	Note that this requires two tasks to achieve: (1) months=*; days=mon-fri; hours=8-18; minutes=*/15 (2) months=*; days=mon-fri; hours=19; minutes=0 We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00.

Click **Save.**

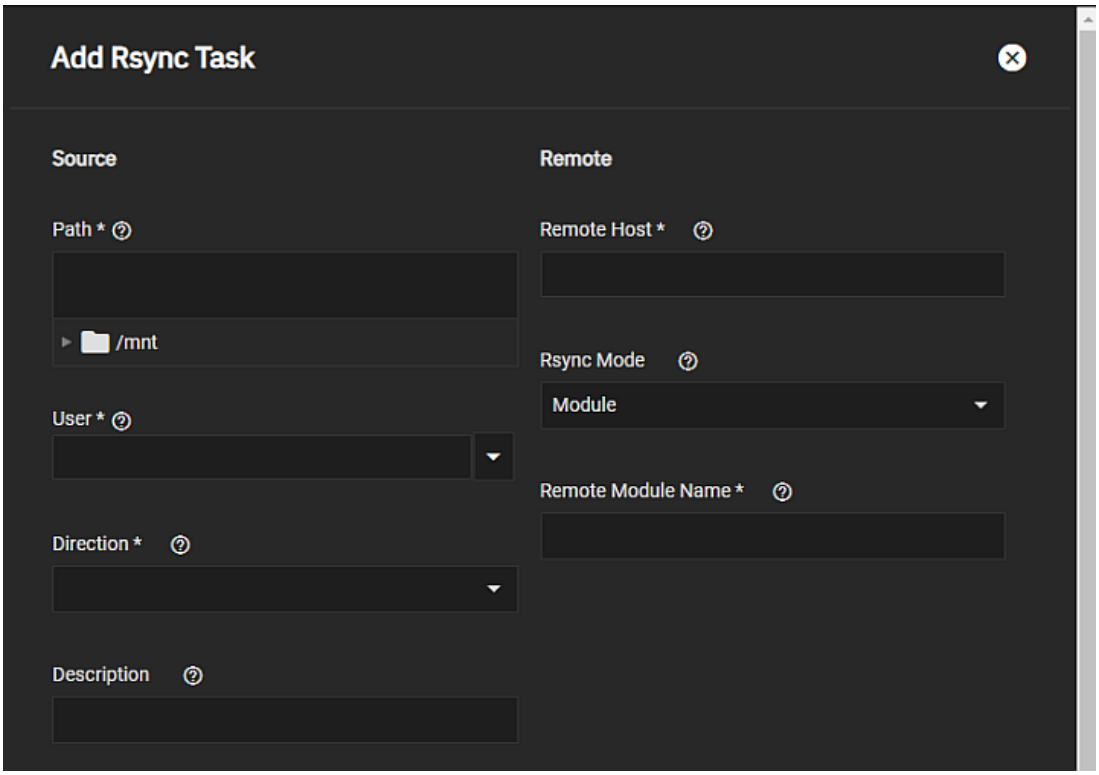
Creating an Rsync Task Using Module Mode

Before you create an rsync task on the host system, you must create a module on the remote system. You must define at least one module in rsyncd.conf(5) of the rsync server or in the rsync modules of another system. When TrueNAS is the remote system, create a module in **System Settings > Services > Rsync** on the **Rsync Modules** screen. See Configuring an Rsync Module for more information.

Click Here for More Information

After adding the rsync module, go to **Data Protection > Rsync Tasks**, and click **Add** to open the **Add Rsync Task** configuration screen.

Enter the required information as described in Creating an Rsync Task above.



Select the direction for the rsync task.

Next, enter the **Remote Host** IP address or hostname. Use the format *username@remote_host* when the username differs from the host entered into the **Remote Host** field.

Now select **Module** from the **Rsync Mode** dropdown list, and then enter either the remote system host name or IP address exactly as it appears on the remote system in **Remote Module Name**.

Select a schedule for the rsync task.

Configure the remaining options according to your specific needs.

If you leave the **Enable** checkbox cleared it disables the task schedule, but you can still save and run the rsync task manually.

Click **Save**.

Creating an Rsync Task Using SSH Mode

First, enable SSH on the remote system. Next enable SSH in TrueNAS. Go to **System > Services** and toggle **SSH** on.

Now set up an SSH connection to the remote server. You can do this in **Credentials > Backup Credentials** using **SSH Connections** and **SSH Keypairs**, or using **System Settings > Shell** and TrueNAS CLI commands. To use the UI, see Adding SSH connections. Populate the **SSH Connections** configuration fields as follows:

Select **Semi-automatic** as the **Setup Method** Select **Private Key** to **Generate New**

Creating an SSH Connection Using CLI in Shell

You can use **System Settings > Shell** and TrueNAS command-line to set up an SSH connection.

Click Here for More Information

To use a command line, go to the **Shell** on the host system. Enter `su - {USERNAME}`, where *{USERNAME}* is the TrueNAS user account that runs the rsync task. Enter `ssh-keygen -t rsa` to create the key pair. When prompted for a password, press `Enter` without setting a password (a password breaks the automated task). Here is an example of running the command:

```
truenas# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification is saved in /root/.ssh/id_rsa.
Your public key is saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:NZMgbuPvTHeEqi3SA/U5wW8un6AWrx8ZsRQdbJJHmR4 tester@truenas.local
The key randomart image is:
+---[RSA 2048]----+
|       . o=o+    |
|      . .ooE.    |
|       +.o==.    |
|      o.oo+.+    |
|      ...S+. .   |
|     . ..++o.    |
|      o oB+. .   |
|     . =Bo+.o    |
|      o+==oo     |
+----[SHA256]-----+
```

The default public key location is ~/.ssh/id_rsa.pub. Enter `cat ~/.ssh/id_rsa.pub` to see the key and copy the file contents.

Copy it to the corresponding user account on the remote system in **Credentials > Users**. By default, SCALE only displays the root user and prompts you to display hidden users. Follow the directions to locate the **sshd** user account. Click on the **sshd** user and then on **Edit**. Paste the key in **SSH Public Key**.

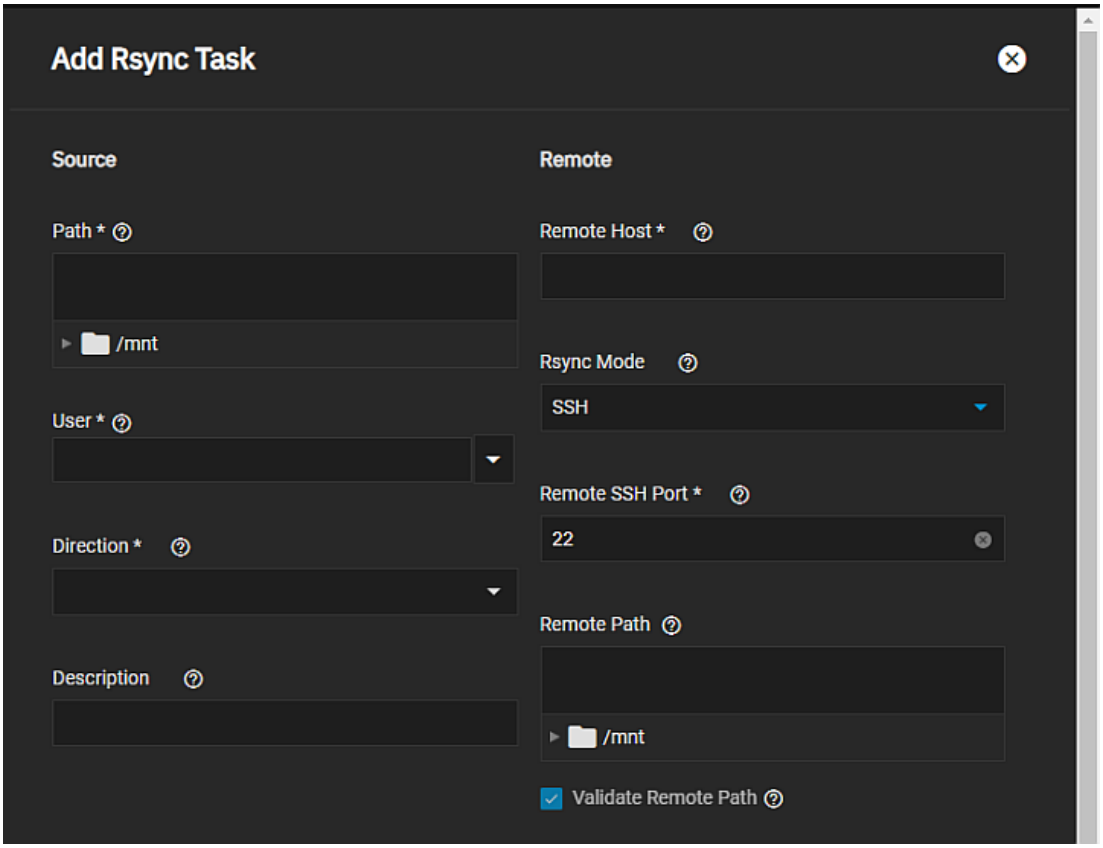
Next, copy the host key from the remote system to the host system user .ssh/known_hosts directory, using `ssh-keyscan`.

On the host system, open the **Shell** and enter `ssh-keyscan -t rsa {remoteIPaddress} >> {userknown_hostsDir}` where *{remoteIPaddress}* is the remote system IP address and *{userknown_hostsDir}* is the known_hosts directory on the host system. Example: `ssh-keyscan -t rsa 192.168.2.6 >> /root/.ssh/known_hosts`.

After establishing the SSH connection, add the rsync task.

Click Here for More Information

Go to **Data Protection > Rsync Tasks** and click **Add** to open the **Add Rsync Task** configuration screen.



Enter the required information as described in Creating an Rsync Task above.

Select a **User** account that matches the SSH connection **Username** entry in the **SSH Connections** you set up.

Choose a **Direction** for the rsync task as either **Push** or **Pull** and then define the task **Schedule**.

Next, enter the **Remote Host** IP address or hostname. Use the format *username@remote_host* if the username differs on the remote host.

Select **SSH** in **Rsync Mode**. The SSH settings fields display.

Enter the SSH port number in **Remote SSH Port**. By default, **22** is reserved in TrueNAS.

Enter or browse to the location on the remote server where you either copy information from or to in **Remote Path**. Maximum path length is *255* characters.

Select **Validate Remote Path** if the remote path location does not exist to create and define it in **Remote Path**.

Select the schedule to use and configure the remaining options according to your specific needs.

Additional options for the **SSH Rsync Mode**:

Clear the **Enabled** checkbox to disable the task schedule without deleting the configuration. You can still run the rsync task by going to **Data Protection > Rsync Tasks** and clicking ❯ then the **Run Now** ▶ icon.

Click **Save**.

Related Content

- Adding SSH Credentials
- Rsync Tasks Screens
- Configuring Rsync Modules
- Rsync Services Screen

3.4.5 - Adding Periodic Snapshot Tasks

A periodic snapshot task allows scheduling the creation of read only versions of pools and datasets at a given point in time.

How should I use snapshots?

Snapshots do not make not copies of the data so creating one is quick and if little data changed, they take very little space. It is common to take frequent snapshots as soon as every 15 minutes, even for large and active pools. A snapshot where no files changed takes no storage space, but as files changes happen, the snapshot size changes to reflect the size of the changes. In the same way as all pool data, after deleting the last reference to the data you recover the space.

Snapshots keep a history of files, providing a way to recover an older copy or even a deleted file. For this reason, many administrators take snapshots often, store them for a period of time, and store them on another system, typically using the **Replication Tasks** function. Such a strategy allows the administrator to roll the system back to a specific point in time. If there is a catastrophic loss, an off-site snapshot can restore data up to the time of the last snapshot.

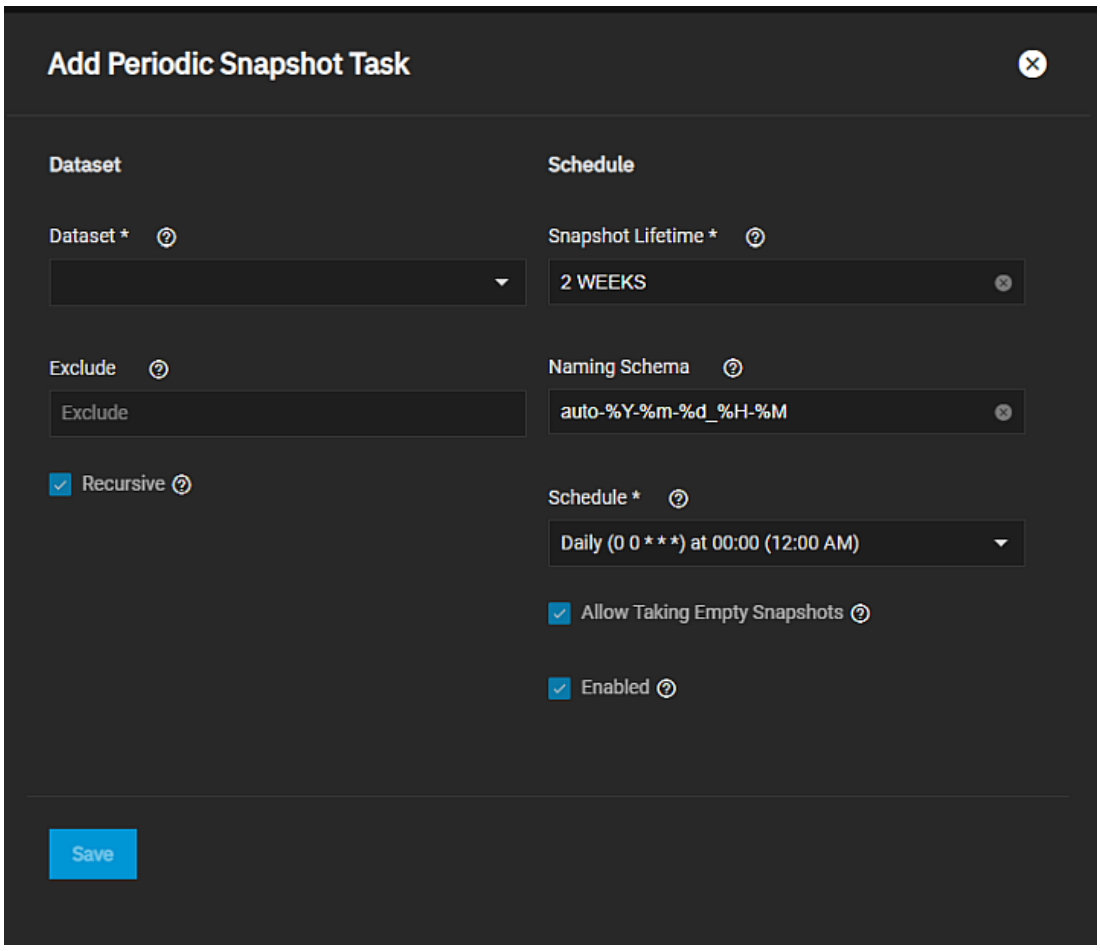
Creating a Periodic Snapshot Task

Create the required datasets or zvols before creating a snapshot task.

Video Tutorial

This short video demonstrates adding a periodic snapshot task

Go to **Data Protection > Periodic Snapshot Tasks** and click **Add**.



First, choose the dataset (or zvol) to schedule as a regular backup with snapshots, and how long to store the snapshots.

Next, define the task **Schedule**. If you need a specific schedule, choose **Custom** and use the Advanced Scheduler section below.

Configure the remaining options for your use case. For help with naming schema and lifetime settings refer to the sections below.

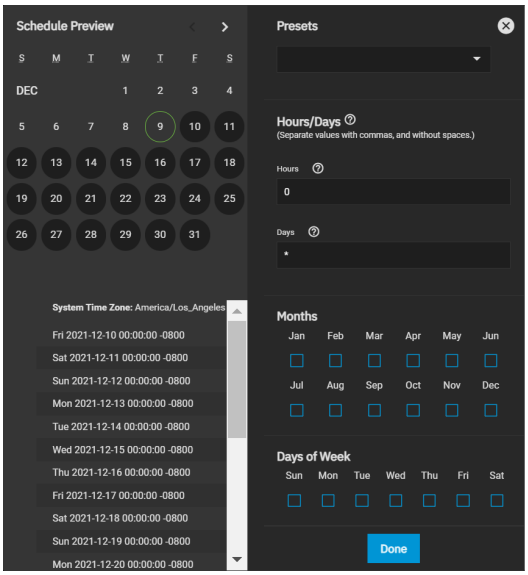
Click **Save** to save this task and add it to the list in **Data Protection > Periodic Snapshot Tasks**.

You can find any snapshots taken using this task in **Storage > Snapshots**.

To check the log for a saved snapshot schedule, go to **Data Protection > Periodic Snapshot Tasks** and click on the task. The **Edit Periodic Snapshot Tasks** screen displays where you can modify any settings for the task.

Using the Advanced Scheduler

Advanced Scheduler



Choosing a **Presets** option populatess in the rest of the fields. To customize a schedule, enter crontab values for the `Minutes/Hours/Days`.

These fields accept standard cron values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering *10* means that the job runs when the time is ten minutes past the hour.

An asterisk (*) means match all values.

You can set specific time ranges by entering hyphenated number values. For example, entering *30-35* in the **Minutes** field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.

You can also enter lists of values. Enter individual values separated by a comma (`,`). For example, entering *1,14* in the **Hours** field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).

A slash (`/`) designates a step value. For example, entering `*` in **Days** runs the task every day of the month. Entering `*/2` runs it every other day.

Combining the above examples creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

TrueNAS has an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days in addition to any listed days. For example, entering *1* in **Days** and setting *Wed* for **Days of Week** creates a schedule that starts a task on the first day of the month *and* every Wednesday of the month.

The **Schedule Preview** dipslays when the current settings mean the task runs.

Examples of CRON syntax

Syntax	Meaning	Examples
*	Every item.	* (minutes) = every minute of the hour. * (days) = every day.
*/N	Every N^{th} item.	*/15 (minutes) = every 15th minute of the hour. */3 (days) = every 3rd day.

Syntax	Meaning	Examples
		*/3 (months) = every 3rd month.
Comma and hyphen/dash	Each stated item (comma) Each item in a range (hyphen/dash).	1,31 (minutes) = on the 1st and 31st minute of the hour. 1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour. mon-fri (days) = every Monday to Friday inclusive (every weekday). mar,jun,sep,dec (months) = every March, June, September, December.

You can specify days of the month or days of the week.

TrueNAS lets users create flexible schedules using the available options. The table below has some examples:

Desired schedule	Values to enter
3 times a day (at midnight, 08:00 and 16:00)	months=*; days=*; hours=0/8 or 0,8,16; minutes=0 (Meaning: every day of every month, when hours=0/8/16 and minutes=0)
Every Monday/Wednesday/Friday, at 8.30 pm	months=*; days=mon,wed,fri; hours=20; minutes=30
1st and 15th day of the month, during October to June, at 00:01 am	months=oct-dec,jan-jun; days=1,15; hours=0; minutes=1
Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday	Note that this requires two tasks to achieve: (1) months=*; days=mon-fri; hours=8-18; minutes=*/15 (2) months=*; days=mon-fri; hours=19; minutes=0 We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00.

Using Naming Schemas

The **Naming Schema** determines how automated snapshot names generate. A valid schema requires the *%Y* (year), *%m* (month), *%d* (day), *%H* (hour), and *%M* (minute) time strings, but you can add more identifiers to the schema too, using any identifiers from the Python strptime function.

> For **Periodic Snapshot Tasks** used to set up a replication task with the **Replication Task** function:
>
> You can use custom naming schema for full backup replication tasks. If you are going to use the snapshot for an incremental replication task, use the default naming schema. Go to Using a Custom Schema for additional information.

This uses some letters differently from POSIX (Unix) time functions. For example, including %z (time zone) ensures that snapshots do not have naming conflicts when daylight time starts and ends, and *%S* (second) adds finer time granularity.

Examples:

Naming Scheme	Snapshot Names Look Like
replicationsnaps-1wklife-%Y%m%d_%H:%M	`replicationsnaps-1wklife-20210120_00:00`, `replicationsnaps-1wklife-20210120_06:00`
autosnap_%Y.%m.%d-%H.%M.%S-%z	`autosnap_2021.01.20-00.00.00-EST`, `autosnap_2021.01.20-06.00.00-EST`

> When referencing snapshots from a Windows computer, avoid using characters like colon (:) that are invalid in a Windows file path. Some applications limit filename or path length, and there might be limitations related to spaces and other characters. Always consider future uses and ensure the name given to a periodic snapshot is acceptable.

Setting Snapshot Lifetimes

TrueNAS deletes snapshots when they reach the end of their life and preserves snapshots when at least one periodic task requires it. For example, you have two schedules created where one schedule takes a snapshot every hour and keeps them for a week, and the other takes a snapshot every day and keeps them for 3 years. Each has an hourly snapshot taken. After a week, snapshots created at *01.00* through *23.00* get deleted, but you keep snapshots timed at *00.00* because they are necessary for the second periodic task. These snapshots get destroyed at the end of 3 years.

Related Content

- Snapshots Screens
- Creating VMWare Snapshots
- VMWare Snapshots Screen
- Periodic Snapshot Tasks Screens

3.4.6 - Managing S.M.A.R.T. Tests

This article provides instructions on running S.M.A.R.T. tests manually or automatically, using Shell to view the list of tests, and configuring the S.M.A.R.T. test service.

S.M.A.R.T. or Self-Monitoring, Analysis and Reporting Technology is a standard for disk monitoring and testing. You can monitor disks for problems using different kinds of self-tests. TrueNAS can adjust when it issues S.M.A.R.T. alerts. When S.M.A.R.T. monitoring reports a disk issue, we recommend you replace that disk. Most modern ATA, IDE, and SCSI-3 hard drives support S.M.A.R.T. Refer to your respective drive documentation for confirmation.

TrueNAS runs S.M.A.R.T. tests on disks. Running tests can reduce drive performance, so we recommend scheduling tests when the system is in a low-usage state. Avoid scheduling disk-intensive tests at the same time! For example, do not schedule S.M.A.R.T. tests on the same day as a disk scrub or other data protection task.

How do I check or change S.M.A.R.T. testing for a disk?

Go to **Storage**, then click **Disks** dropdown and select **Disks**.

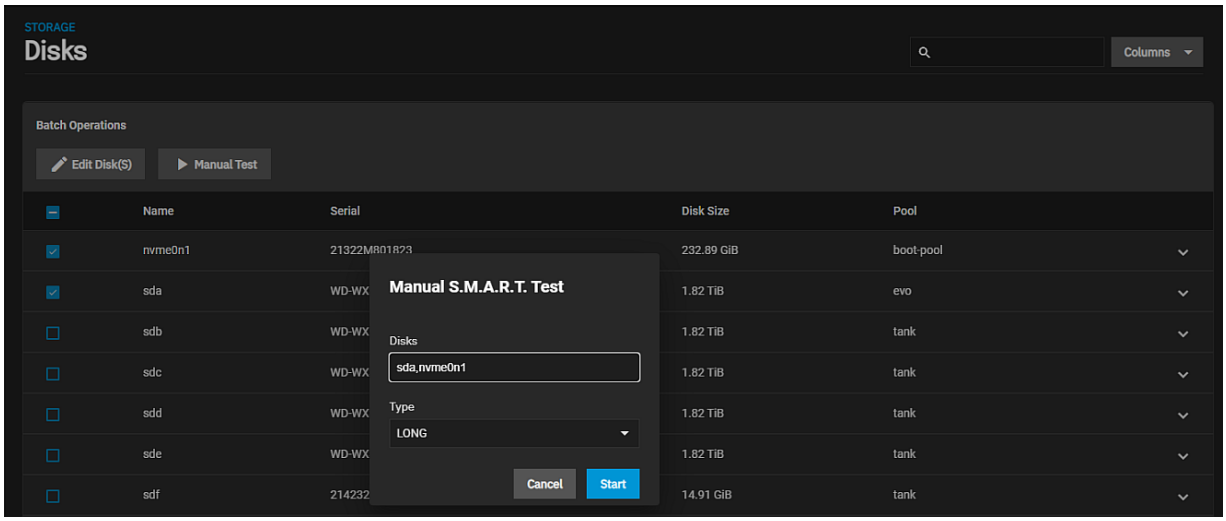
Click the ⌄ to the right of the disk row to expand it. **Enable S.M.A.R.T.** shows as **true** or **false**.

To enable or disable testing, click **EDIT** and find the **Enable S.M.A.R.T.** option.

Running a Manual S.M.A.R.T. Test

To test one or more disk for errors, go to **Storage**, select **Disks** and then select the disks you want to test to display the **Batch Operations** options.

Click **Manual Test**. The **Manual S.M.A.R.T. Test** dialog displays.



Next, select the test type from the **Type** dropdown and then click **Start**.

Test types differ based on the drive connection, ATA or SCSI. Test duration varies based on the test type you chose. TrueNAS generates alerts when tests discover issues.

> Manual S.M.A.R.T. tests on NVMe devices is currently not supported.

ATA Drive Connection Test Types

The ATA drive connection test type options are:

- **Long** runs a S.M.A.R.T. Extended Self Test that scans the entire disk surface, which may take hours on large-volume disks.
- **Short** runs a basic S.M.A.R.T. Short Self Test (usually under ten minutes) that varies by manufacturer.
- **Conveyance** runs a S.M.A.R.T. Conveyance Self Test (usually only minutes) that identifies damage incurred while transporting the device.

- **Offline** runs a S.M.A.R.T. Immediate Offline Test that updates the S.M.A.R.T. Attribute values. Errors will appear in the S.M.A.R.T. error log.

SCSI Drive Connection Test Type

- **Long** runs the “Background long” self-test.
- **Short** runs the “Background short” self-test.
- **Offline** runs the default self-test in the foreground, but doesn’t place an entry in the self-test log.

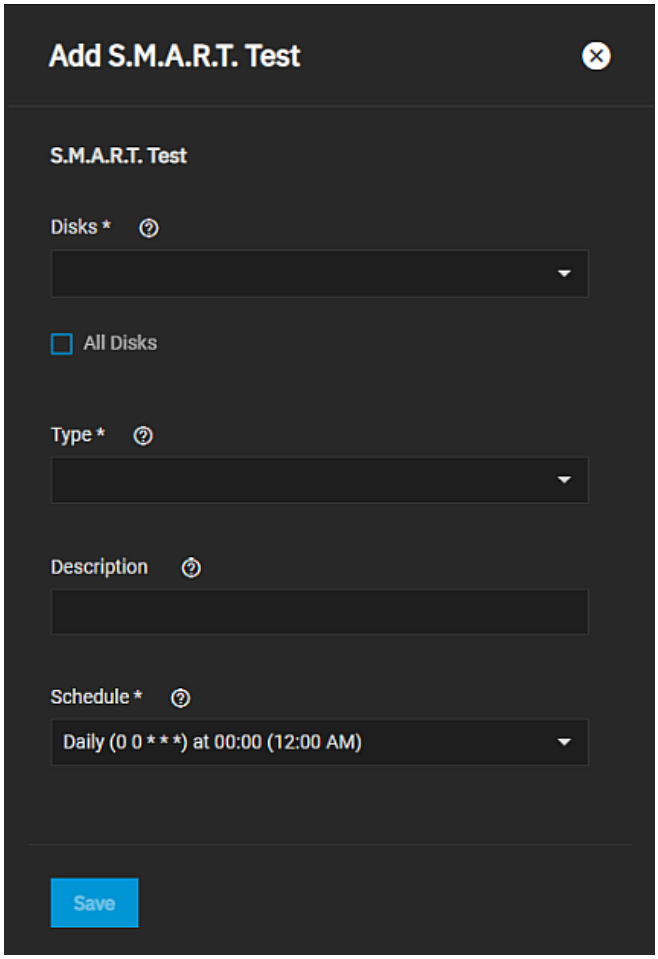
For more information, refer to smartctl(8).

Where can I view the test results?

Click the ⌄ in a disk’s row to expand it, then click **S.M.A.R.T. TEST RESULTS**. You can also see results in the **Shell** using `smartctl` and the name of the drive: `smartctl -l selftest /dev/ada0`.

Running Automatic S.M.A.R.T. Tests

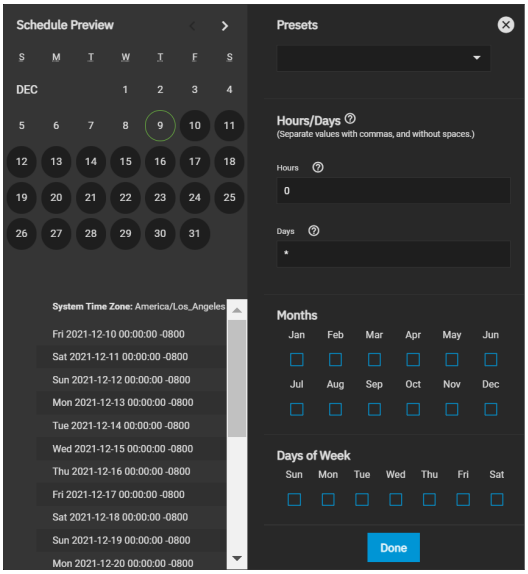
To schedule recurring S.M.A.R.T. tests, go to **Data Protection** and click **ADD** in the **S.M.A.R.T. Tests** widget.



Select the disks to test from the **Disks** dropdown list, and then select the test type to run from the **Type** dropdown list.

Next select a preset from the **Schedule** dropdown. To create a custom schedule select **Custom** to open the advanced scheduler window where you can define the schedule parameters you want to use.

Advanced Scheduler



Choosing a **Presets** option populatess in the rest of the fields. To customize a schedule, enter crontab values for the `Minutes/Hours/Days`.

These fields accept standard cron values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering *10* means that the job runs when the time is ten minutes past the hour.

An asterisk (*) means match all values.

You can set specific time ranges by entering hyphenated number values. For example, entering *30-35* in the **Minutes** field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.

You can also enter lists of values. Enter individual values separated by a comma (`,`). For example, entering *1,14* in the **Hours** field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).

A slash (`/`) designates a step value. For example, entering * in **Days** runs the task every day of the month. Entering `*/2` runs it every other day.

Combining the above examples creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

TrueNAS has an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days in addition to any listed days. For example, entering *1* in **Days** and setting *Wed* for **Days of Week** creates a schedule that starts a task on the first day of the month *and* every Wednesday of the month.

The **Schedule Preview** dipslays when the current settings mean the task runs.

Examples of CRON syntax

Syntax	Meaning	Examples
*	Every item.	* (minutes) = every minute of the hour. * (days) = every day.
*/N	Every N^{th} item.	*/15 (minutes) = every 15th minute of the hour. */3 (days) = every 3rd day. */3 (months) = every 3rd month.
Comma and hyphen/dash	Each stated item (comma) Each item in a range (hyphen/dash).	1,31 (minutes) = on the 1st and 31st minute of the hour. 1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour. mon-fri (days) = every Monday to Friday inclusive (every weekday). mar,jun,sep,dec (months) = every March, June, September, December.

You can specify days of the month or days of the week.

TrueNAS lets users create flexible schedules using the available options. The table below has some examples:

Desired schedule	Values to enter
3 times a day (at midnight, 08:00 and 16:00)	months=*; days=*; hours=0/8 or 0,8,16; minutes=0 (Meaning: every day of every month, when hours=0/8/16 and minutes=0)

Desired schedule	Values to enter
Every Monday/Wednesday/Friday, at 8.30 pm	months=*; days=mon,wed,fri; hours=20; minutes=30
1st and 15th day of the month, during October to June, at 00:01 am	months=oct-dec,jan-jun; days=1,15; hours=0; minutes=1
Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday	Note that this requires two tasks to achieve: (1) months=*; days=mon-fri; hours=8-18; minutes=*/15 (2) months=*; days=mon-fri; hours=19; minutes=0 We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00.

Saved schedules appear in the **S.M.A.R.T. Tests** window.

> S.M.A.R.T. tests can offline disks! Avoid scheduling S.M.A.R.T. tests simultaneously with scrub or other data protection tasks.

Start the S.M.A.R.T. service. Go to **System Settings > Services** and scroll down to the **S.M.A.R.T.** service. If not running, click the toggle to turn the service on. Select **Start Automatically** to have this service start after after the system reboots.

If you have not configured the S.M.A.R.T. service yet, while the service is stopped, click  to open the service configuration form. See Services S.M.A.R.T. Screen for more information on service settings. Click **Save** to save settings and return to the **Services** screen.

RAID controllers?
Disable the S.M.A.R.T. service when a RAID controller controls the disks. The controller monitors S.M.A.R.T. separately and marks disks as a **Predictive Failure** on a test failure.

Using Shell to View Scheduled Tests

CLI
To verify the schedule is saved, you can open the shell and enter `smartd -q showtests`.

Related Content

- Configuring S.M.A.R.T. Service
- S.M.A.R.T. Service Screen
- S.M.A.R.T. Tests Screens

3.4.7 - Replication Tasks

Article Summaries

- Setting Up a Local Replication Task

  This article provides instructions on adding a replication task on the same TrueNAS system.

- Setting Up Advanced Replication Tasks

  This article provides instruction on using the advanced replication task creation screen to add a replication task.

- Setting Up a Remote Replication Task

  This article provides instructions on adding a replication task with a remote system (TrueNAS or other).

- Unlocking a Replication Encrypted Dataset or Zvol

  This article provides information on three methods of unlocking replicated encrypted datasets or zvols without a passphrase.

3.4.7.1 - Setting Up a Local Replication Task

This article provides instructions on adding a replication task on the same TrueNAS system.

Local Replication

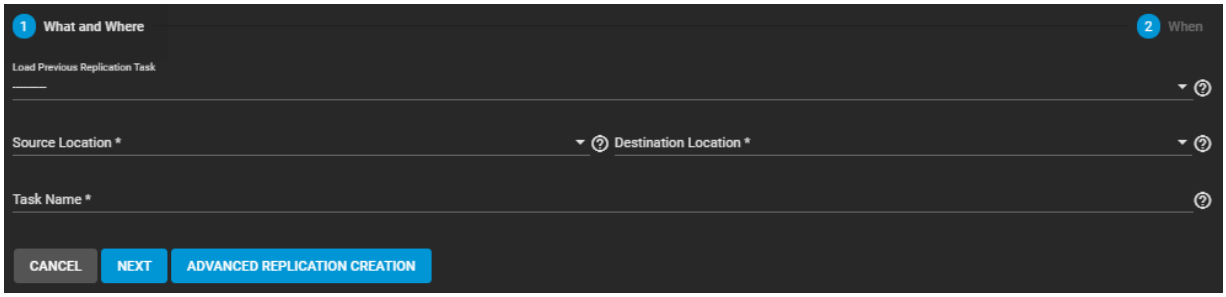
Process Summary

Process Summary

- Requirements: Storage pools and datasets created in **Storage > Pools**.
- Go to **Data Protection > Replication Tasks** and click **ADD**
  - Choose **Sources**
    - Set the source location to the local system
    - Use the file browser or type paths to the sources
  - Define a **Destination** path
    - Set the destination location to the local system
    - Select or manually define a path to the single destination location for the snapshot copies.
  - Set the **Replication schedule** to run once
  - Define how long the snapshots are stored in the **Destination**
  - Clicking **START REPLICATION** immediately snapshots the chosen sources and copies those snapshots to the destination
    - Dialog might ask to delete existing snapshots from the destination. Be sure that all important data is protected before deleting anything.
- Clicking the task **State** shows the logs for that replication task.

Quick Local Backups with the Replication Wizard

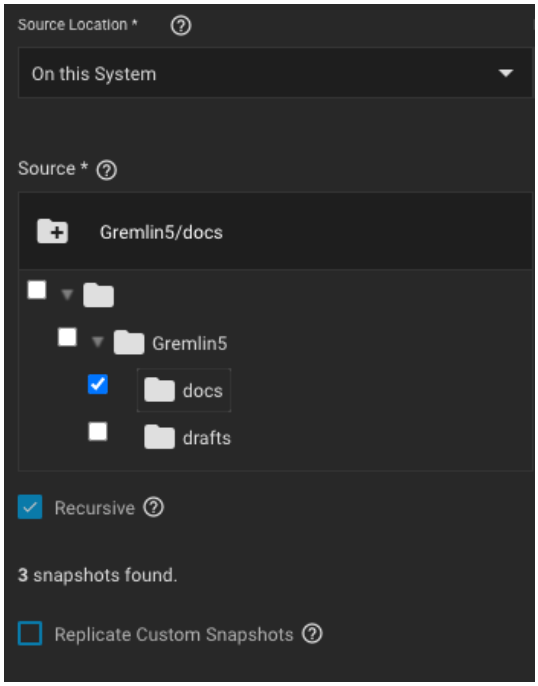
TrueNAS provides a wizard for quickly configuring different simple replication scenarios.



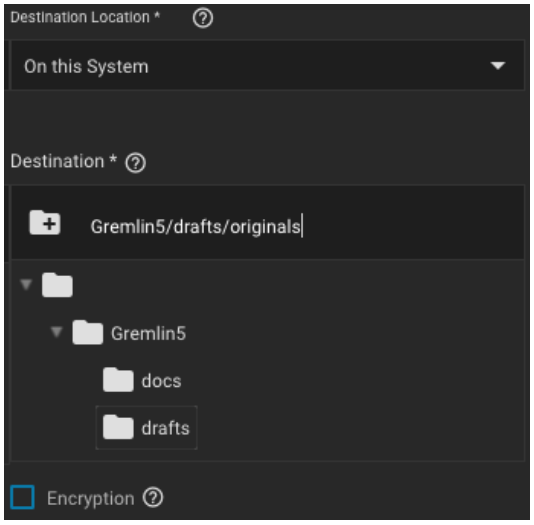
While we recommend regularly scheduled replications to a remote location as the optimal backup scenario, the wizard can very quickly create and copy ZFS snapshots to another location on the same system. This is useful when no remote backup locations are available, or when a disk is in immediate danger of failure.

The only things you need before creating a quick local replication are datasets or zvols in a storage pool to use as the replication source and (preferably) a second storage pool to use for storing replicated snapshots. You can set up the local replication entirely in the **Replication Wizard**.

To open the **Replication Wizard**, go to **Data Protection > Replication Tasks** and click **ADD**. Set the source location to the local system and pick which datasets to snapshot. The wizard takes new snapshots of the sources when no existing source snapshots are found.
Enabling **Recursive** replicates all snapshots contained within the selected source dataset snapshots. Local sources can also use a naming schema to identify any custom snapshots to include in the replication. A naming schema is a collection of strftime time and date strings and any identifiers that a user might have added to the snapshot name.



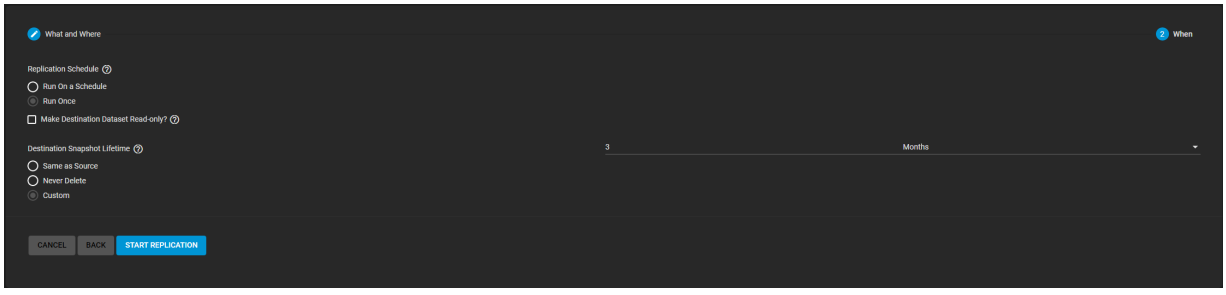
Set the destination to the local system and define the path to the storage location for replicated snapshots. When manually defining the destination, be sure to type the full path to the destination location.



TrueNAS suggests a default name for the task based on the selected source and destination locations, but you can type your own name for the replication. You can load any saved replication task into the wizard to make creating new replication schedules even easier.

You can define a specific schedule for this replication or choose to run it immediately after saving the new task. TrueNAS saves unscheduled tasks in the replication task list. You can run saved tasks manually or edit them later to add a schedule.

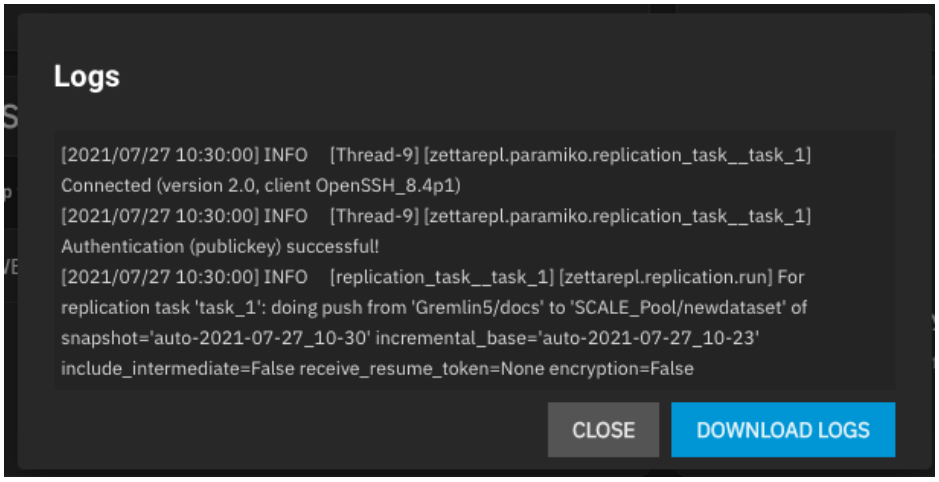
The destination lifetime is how long copied snapshots are stored in the destination before they are deleted. We usually recommend defining a snapshot lifetime to prevent storage issues. Choosing to keep snapshots indefinitely can require you to manually clean old snapshots from the system if or when the destination fills to capacity.



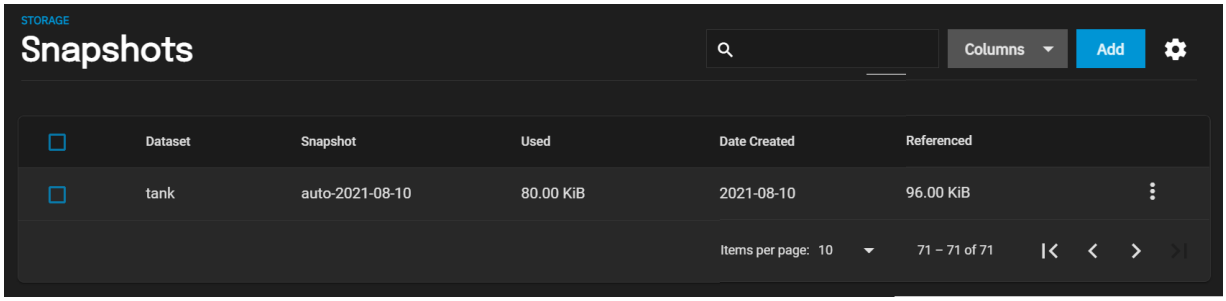
Clicking **START REPLICATION** saves the new task and immediately attempts to replicate snapshots to the destination. When TrueNAS detects that the destination already has unrelated snapshots, it asks to delete the unrelated snapshots and do a full

copy of the new snapshots. This can delete important data, so ensure you can delete any existing snapshots or back them up in another location.

TrueNAS adds the simple replication to the replication task list and shows that it is currently running. Clicking the task state shows the replication log with an option to download the log to your local system.



To confirm that snapshots are replicated, go to **Storage > Snapshots > Snapshots** and verify the destination dataset has new snapshots with correct timestamps.



Related Content

- Adding Replication Tasks
- Managing Advanced Settings
- Advanced Settings Screen
- Setting Up Advanced Replication Tasks
- Periodic Snapshot Tasks Screens
- Setting Up a Remote Replication Task
- Unlocking a Replication Encrypted Dataset or Zvol
- Replication Task Screens

3.4.7.2 - Setting Up Advanced Replication Tasks

This article provides instruction on using the advanced replication task creation screen to add a replication task.

Advanced Replication

Requirements:

- Storage pools with datasets and data to snapshot.
- SSH configured with a connection to the remote system saved in **Credentials > Backup Credentials > SSH Connections**.
- Dataset snapshot task saved in **Data Protection > Periodic Snapshot Tasks**.

Process Summary

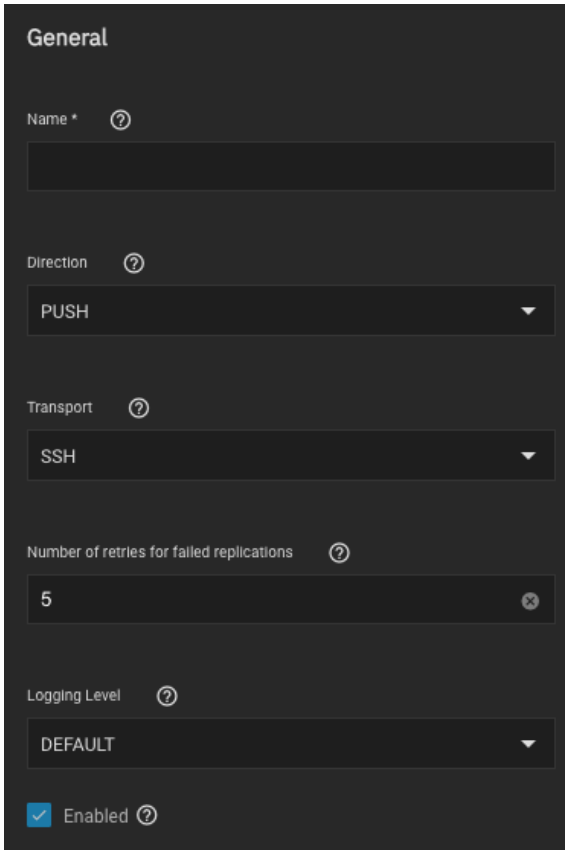
Process Summary

Go to **Data Protection > Replication Tasks** and click **ADD**, then select **ADVANCED REPLICATION CREATION**.

- General Options:
  - Name the task.
  - Select **Push** or **Pull** for the local system.
  - Select a replication transport method.
    - SSH is recommended.
    - SSH+Netcat is used for secured networks.
    - Local is for in-system replication.
- Configure the replication transport method:
  - Remote options require a preconfigured SSH connection.
  - SSH+Netcat requires defining netcat ports and addresses.
- Sources:
  - Select sources for replication.
  - Choose a preconfigured periodic snapshot task as the source of snapshots to replicate.
  - Remote sources require defining a snapshot naming schema.
- Destination:
  - Remote destination requires an SSH connection.
  - Select a destination or type a path in the field.
  - Define how long to keep snapshots in the destination.
- Scheduling:
  - Run automatically starts the replication after a related periodic snapshot task completes.
  - To automate the task according to its own schedule, set the *schedule* option and define a schedule for the replication task.

To use the advanced editor to create a replication task, go to **Data Protection > Replication Tasks**, click **Add** to open the wizard, then click the **Advanced Replication Creation** button.

Options are grouped together by category. Options can appear, disappear, or be disabled depending on the configuration choices you make. Start by configuring the **General** options first, then the **Transport** options before configuring replication **Source**, **Destination**, and **Replication Schedule**.



Type a name for the task in **Name**. Each task name must be unique, and we recommend you name it in a way that makes it easy to remember what the task is doing.

Direction allows you to choose whether the local system is sending (**Push**) or receiving data (**Pull**).

Decide what **Transport** method (**SSH**, **SSH+NETCAT**, or **LOCAL**) to use for the replication before configuring the other sections.

Set the **Number of retries for failed replications** before stopping and marking the task as failed (the default is 5).

Use the **Logging Level** to set the message verbosity level in the replication task log.

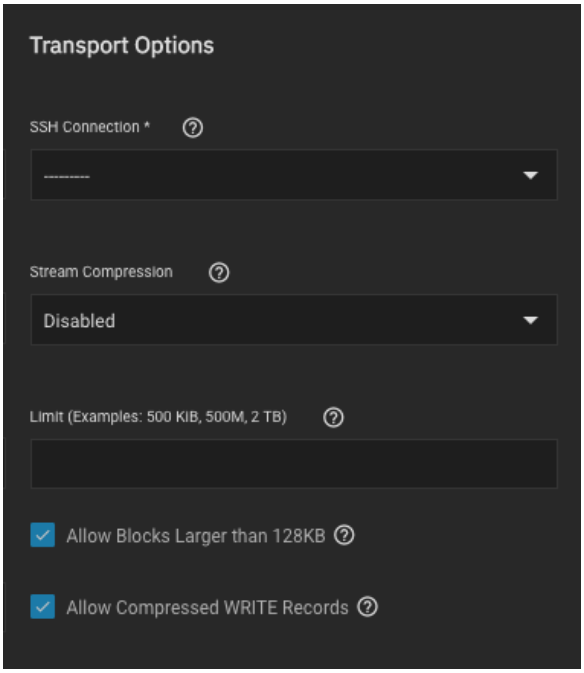
To ensure the replication task is active, check the **Enabled** box.

Transport Options

Transport Options

The **Transport** selector determines the method to use for the replication: **SSH** is the standard option for sending or receiving data from a remote system, but **SSH+NETCAT** is available as a faster option for replications that take place within completely secure networks. **Local** is only used for replicating data to another location on the same system.

With SSH-based replications, configure the transport method by selecting the **SSH Connection** to the remote system that sends or receives snapshots. Options for compressing data, adding a bandwidth limit, or other data stream customizations are available. **Stream Compression** options are only available when using SSH. Before enabling **Compressed WRITE Records**, verify that the destination system also supports compressed WRITE records.



For SSH+NETCAT replications, you must define the addresses and ports to use for the Netcat connection.

> **Allow Blocks Larger than 128KB** is a one-way toggle. Replication tasks using large block replication only continue to work as long as this option remains enabled.

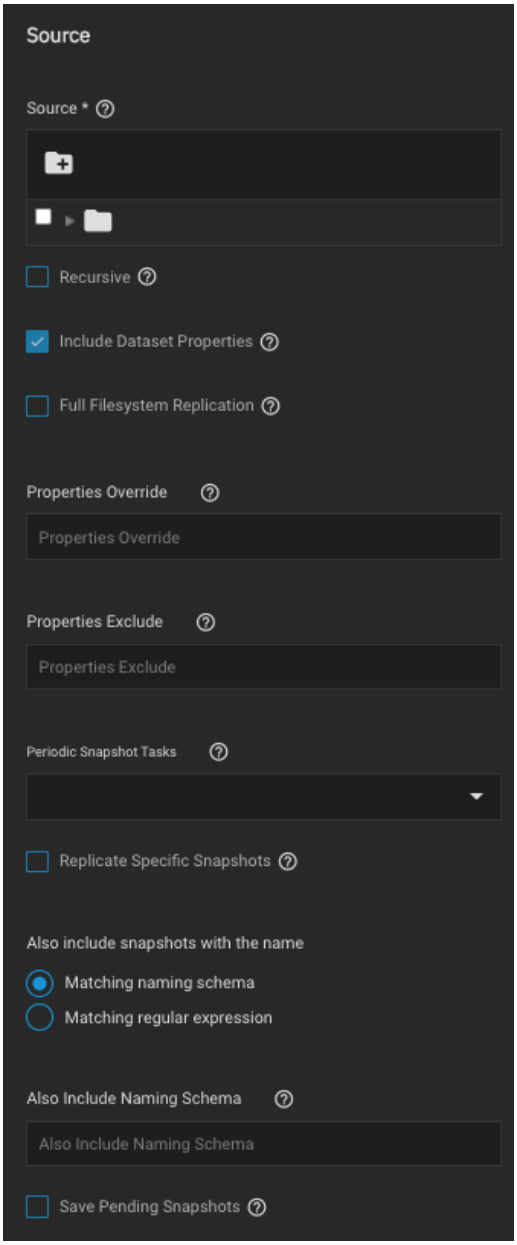
Configure the Source

Source

The replication **Source** is the datasets or zvols to use for replication. Select the sources to use for this replication task by opening the file browser or entering dataset names in the field. Pulling snapshots from a remote source requires a valid **SSH Connection** before the file browser can show any directories.

If the file browser shows a connection error after selecting the correct **SSH Connection**, you might need to log in to the remote system and configure it to allow SSH connections.

In TrueNAS, do this by going to the **System Settings > Services** screen, checking the **SSH** service configuration, and starting the service.



By default, the replication task uses snapshots to quickly transfer data to the receiving system. When **Full Filesystem Replication** is set, the task completely replicates the chosen **Source**, including all dataset properties, snapshots, child datasets, and clones. When choosing this option, we recommended allocating additional time for the replication task to run.

Leaving **Full Filesystem Replication** unset but setting **Include Dataset Properties** includes just the dataset properties in the snapshots to be replicated.

Checking the **Recursive** check box allows you to recursively replicate child dataset snapshots or exclude specific child datasets or properties from the replication.

Enter newly defined properties in the **Properties Override** field to replace existing dataset properties with the newly defined properties in the replicated files.

List any existing dataset properties to remove from the replicated files in the **Properties Exclude** field.

Local sources are replicated by snapshots that were generated from a periodic snapshot task and/or from a defined naming schema that matches manually created snapshots.

Select a previously configured periodic snapshot task for this replication task in the **Periodic Snapshot Tasks** drop-down list. The replication task selected must have the same values in **Recursive** and **Exclude Child Datasets** as the chosen periodic snapshot task. Selecting a periodic snapshot schedule removes the **Schedule** field.

To define specific snapshots from the periodic task to use for the replication, set **Replicate Specific Snapshots** and enter a schedule. The only periodically generated snapshots included in the replication task are those that match your defined schedule.

Remote sources require entering a snapshot naming schema to identify the snapshots to replicate. A naming schema is a collection of strftime time and date strings and any identifiers that a user might have added to the snapshot name. For

example, entering the naming schema `custom-%Y-%m-%d_%H-%M` finds and replicates snapshots like `custom-2020-03-25_09-15`. Multiple schemas can be entered by pressing `Enter` to separate each schema.

Alternately, you can use your **Replication Schedule** to determine which snapshots are replicated by setting **Run Automatically**, **Only Replicate Snapshots Matching Schedule**, and defining when the replication task runs.

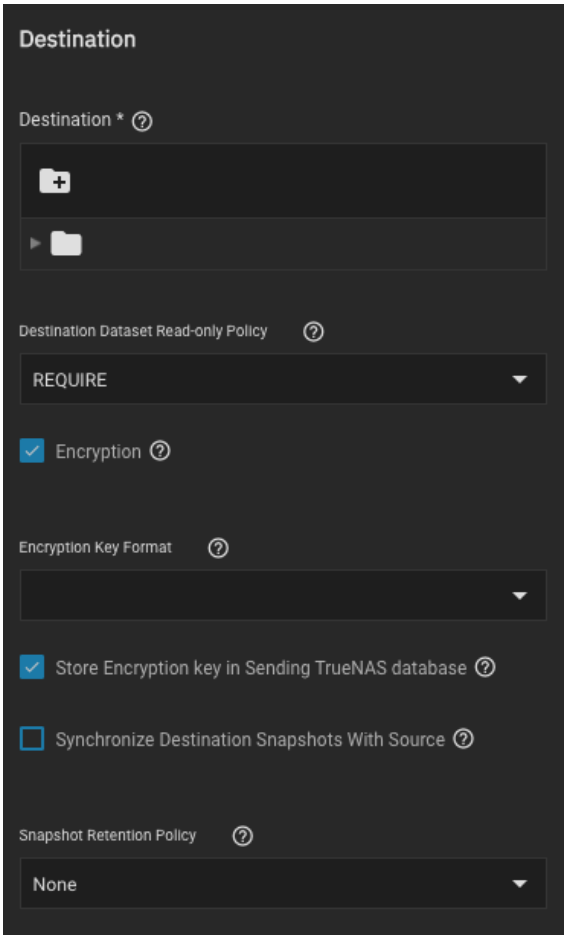
When a replication task is having difficulty completing, it is a good idea to set **Save Pending Snapshots**. This prevents the source TrueNAS from automatically deleting any snapshots that failed to replicate to the destination system.

Set up the Destination

Destination

Use **Destination** to specify where replicated data is stored. Choosing a remote destination requires an *SSH Connection to that system. Expanding the file browser shows the current datasets that are available on the destination system. You can click a destination or manually type a path in the field. Adding a name to the end of the path creates a new dataset in that location.

> *DO NOT* use zvols as remote destinations.



By default, the destination dataset is set to be *read-only* after the replication is complete. You can change the **Destination Dataset Read-only Policy** to only start replication when the destination is read-only (**REQUIRE**) or to disable checking the dataset's read-only state (**IGNORE**).

The **Encryption** checkbox adds another layer of security to replicated data by encrypting the data before transfer and decrypting it on the destination system.

- Setting the checkbox adds more options to choose between using a **HEX** key or defining your own encryption **PASSPHRASE**.
- You can store the encryption key either in the TrueNAS system database or in a custom-defined location.

> **Synchronizing Destination Snapshots With Source** *destroys* any snapshots in the destination that do not match the source snapshots. TrueNAS also does a full replication of the source snapshots as if the replication task had never been run before, which can lead to excessive bandwidth consumption.
>
> This can be a very destructive option. Make sure that any snapshots deleted from the destination are obsolete or otherwise backed up in a different location.

Defining the **Snapshot Retention Policy** is generally recommended to prevent cluttering the system with obsolete snapshots. Choosing **Same as Source** keeps the snapshots on the destination system for the same amount of time as the defined **Snapshot Lifetime** from the source system periodic snapshot task.

You can use **Custom** to define your own lifetime for snapshots on the destination system.

Schedule the Task

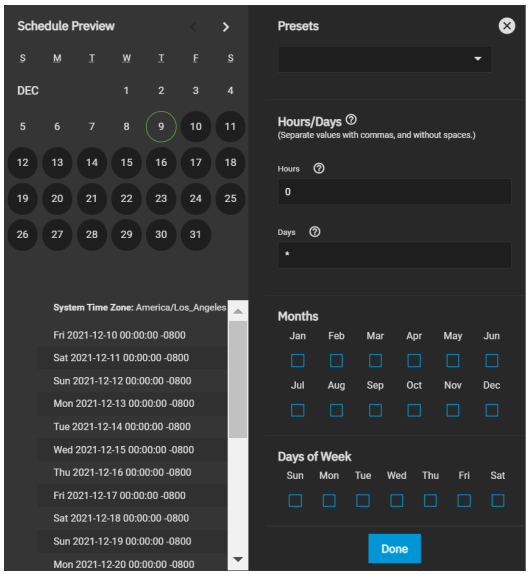
Schedule

By default, setting the task to **Run Automatically** starts the replication immediately after the related periodic snapshot task is complete.

Setting the **Schedule** checkbox allows scheduling the replication to run at a separate time.

- Defining a specific time for the replication task to run is a must-do.
- Choose a time frame that both gives the replication task enough time to finish and is during a time of day when network traffic for both source and destination systems is minimal.
- Use the custom scheduler (recommended) when you need to fine-tune an exact time or day for the replication.

Advanced Scheduler



Choosing a **Presets** option populatess in the rest of the fields. To customize a schedule, enter crontab values for the `Minutes/Hours/Days`.

These fields accept standard cron values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering *10* means that the job runs when the time is ten minutes past the hour.

An asterisk (`*`) means match all values.

You can set specific time ranges by entering hyphenated number values. For example, entering *30-35* in the **Minutes** field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.

You can also enter lists of values. Enter individual values separated by a comma (`,`). For example, entering *1,14* in the **Hours** field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).

A slash (`/`) designates a step value. For example, entering `*` in **Days** runs the task every day of the month. Entering `*/2` runs it every other day.

Combining the above examples creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

TrueNAS has an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days in addition to any listed days. For example, entering *1* in **Days** and setting *Wed* for **Days of Week** creates a schedule that starts a task on the first day of the month *and* every Wednesday of the month.

The **Schedule Preview** dipslays when the current settings mean the task runs.

Examples of CRON syntax

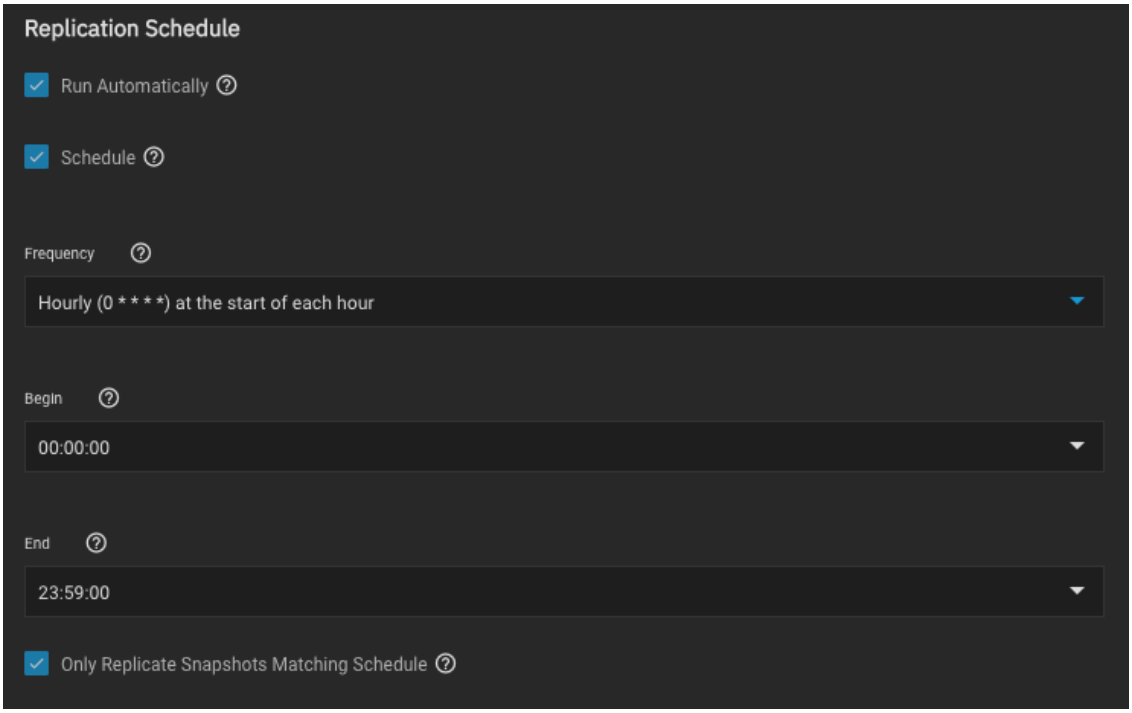
Syntax	Meaning	Examples
*	Every item.	* (minutes) = every minute of the hour. * (days) = every day.
*/N	Every Nth item.	*/15 (minutes) = every 15th minute of the hour. */3 (days) = every 3rd day. */3 (months) = every 3rd month.
Comma and hyphen/dash	Each stated item (comma) Each item in a range (hyphen/dash).	1,31 (minutes) = on the 1st and 31st minute of the hour. 1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour. mon-fri (days) = every Monday to Friday inclusive (every weekday). mar,jun,sep,dec (months) = every March, June, September, December.

You can specify days of the month or days of the week.

TrueNAS lets users create flexible schedules using the available options. The table below has some examples:

Desired schedule	Values to enter
3 times a day (at midnight, 08:00 and 16:00)	months=*; days=*; hours=0/8 or 0,8,16; minutes=0 (Meaning: every day of every month, when hours=0/8/16 and minutes=0)
Every Monday/Wednesday/Friday, at 8.30 pm	months=*; days=mon,wed,fri; hours=20; minutes=30
1st and 15th day of the month, during October to June, at 00:01 am	months=oct-dec,jan-jun; days=1,15; hours=0; minutes=1
Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday	Note that this requires two tasks to achieve: (1) months=*; days=mon-fri; hours=8-18; minutes=*/15 (2) months=*; days=mon-fri; hours=19; minutes=0 We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00.

Setting **Only Replicate Snapshots Matching Schedule** restricts the replication to only replicate those snapshots created at the same time as the replication schedule.



Related Content

- Adding Replication Tasks
- Managing Advanced Settings
- Setting Up a Local Replication Task
- Advanced Settings Screen
- Periodic Snapshot Tasks Screens
- Setting Up a Remote Replication Task

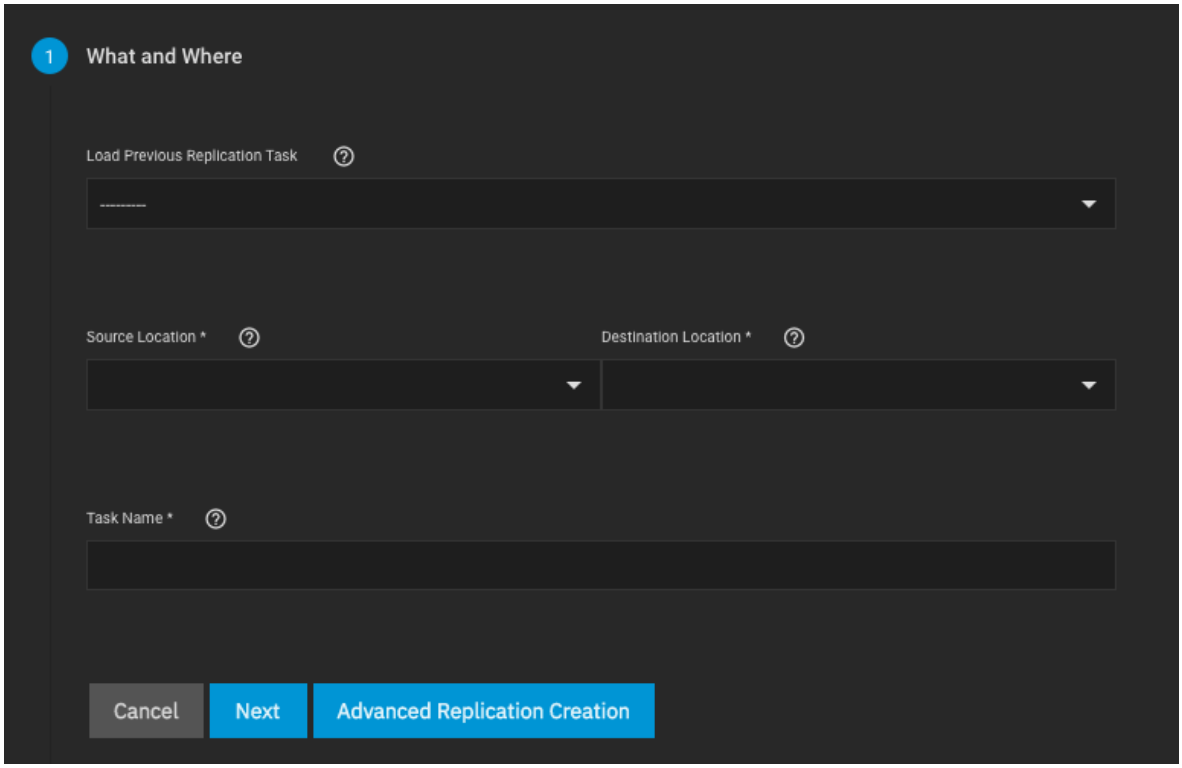
- Unlocking a Replication Encrypted Dataset or Zvol
- Replication Task Screens

3.4.7.3 - Setting Up a Remote Replication Task

This article provides instructions on adding a replication task with a remote system (TrueNAS or other).

Creating a Remote Replication Task

To create a new replication, go to **Data Protection > Replication Tasks** and click **ADD**.



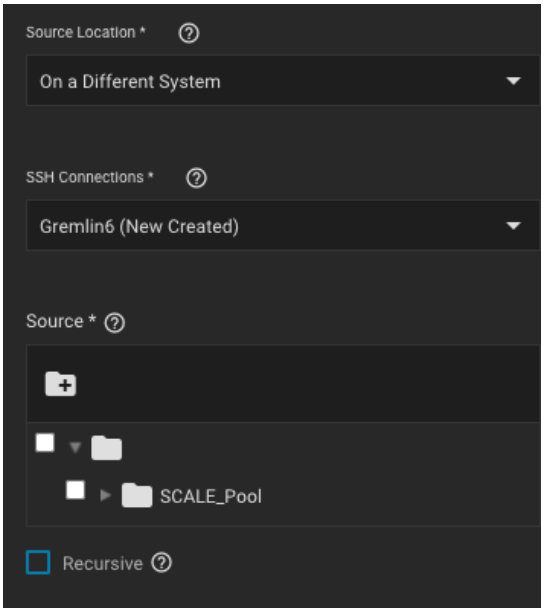
You can load any saved replication to prepopulate the wizard with that configuration. Saving changes to the configuration creates a new replication task without altering the task you loaded into the wizard. This saves some time when creating multiple replication tasks between the same two systems.

Set up the Sources

Source

Start by configuring the replication sources. Sources are the datasets or zvols with snapshots to use for replication. Choosing a remote source requires selecting an SSH connection to that system. Expanding the directory browser shows the current datasets or zvols that are available for replication. You can select multiple sources or manually type the names into the field.

TrueNAS shows how many snapshots are available for replication. We recommend you manually snapshot the sources or create a periodic snapshot task *before* creating the replication task. However, when the sources are on the local system and don't have any existing snapshots, TrueNAS can create a basic periodic snapshot task and snapshot the sources immediately before starting the replication. Enabling **Recursive** replicates all snapshots contained within the selected source dataset snapshots.

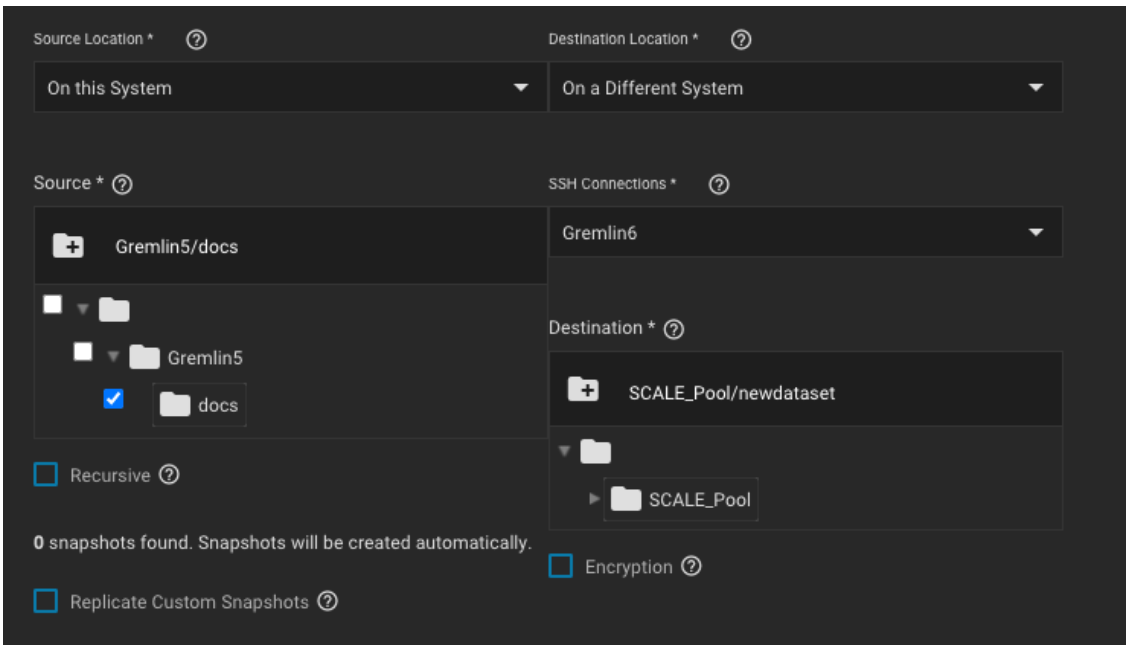


Local sources can also use a naming schema to identify any custom snapshots to include in the replication. Remote sources require entering a *snapshot naming schema* to identify the snapshots to replicate. A naming schema is a collection of strftime time and date strings and any identifiers that a user might have added to the snapshot name.

Configure the Destination

Destination

The destination is where replicated snapshots are stored. Choosing a remote destination requires an SSH connection to that system. Expanding the directory browser shows the current datasets that are available for replication. You can select a destination dataset or manually type a path in the field. You cannot use zvols as a remote replication destination. Adding a name to the end of the path creates a new dataset in that location.



To use encryption when replicating data click the **Encryption** box. After selecting the box these additional encryption options become available:

- **Encryption Key Format** allows the user to choose between a hex (base 16 numeral) or passphrase (alphanumeric) style encryption key.
- **Store Encryption key in Sending TrueNAS database** allows the user to either store the encryption key in the sending TrueNAS database (box checked) or choose a temporary location for the encryption key that decrypts replicated data (box unchecked)

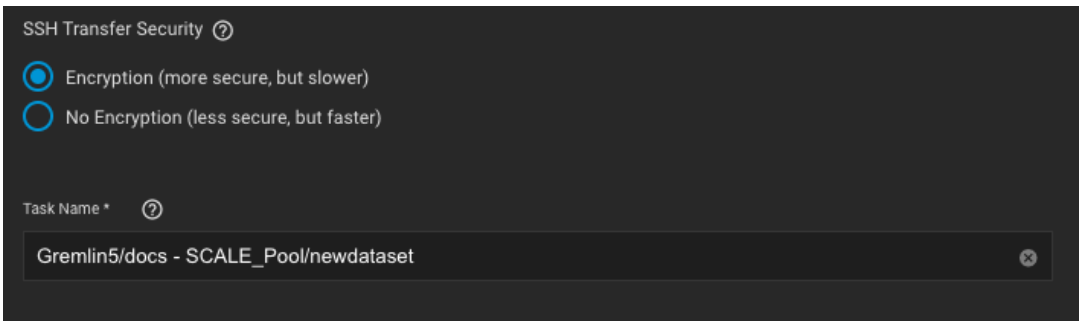
Security and Task Name

Security and Task Name

> Using encryption for SSH transfer security is always recommended.

In situations where two systems within an absolutely secure network are used for replication, disabling encryption speeds up the transfer. However, the data is completely unprotected from eavesdropping.

Choosing **no encryption** for the task is less secure but faster. This method uses common port settings but these can be overridden by switching to the advanced options screen or editing the task after creation.



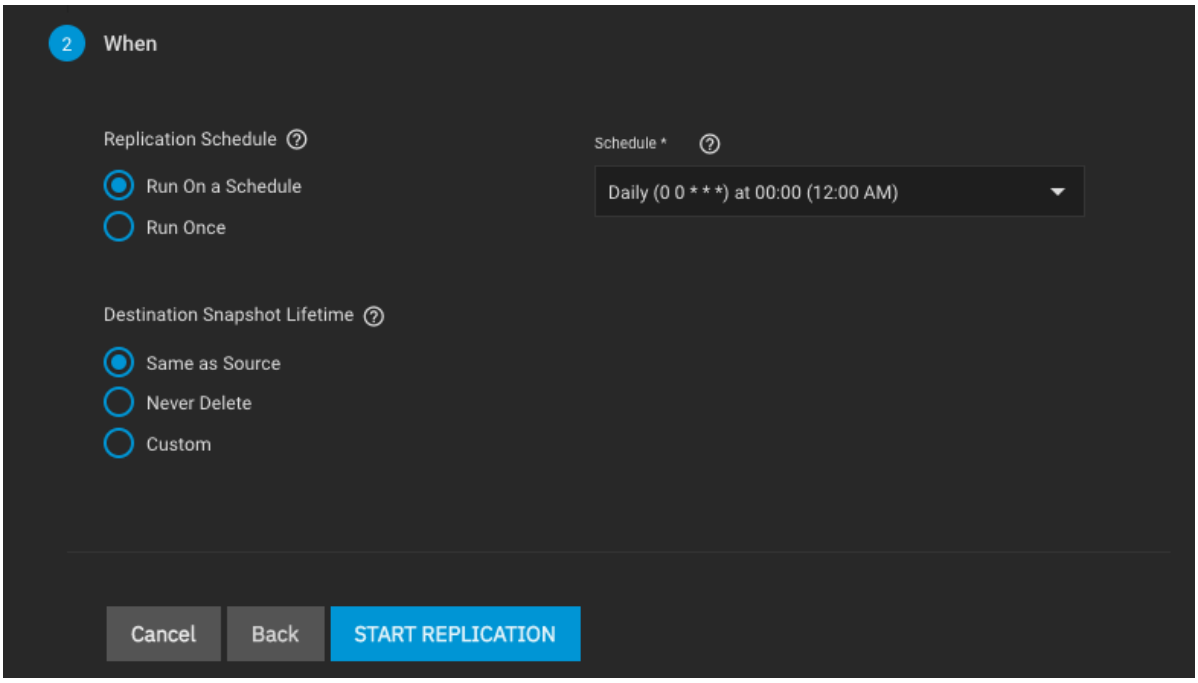
TrueNAS suggests a name based off the selected sources and destination, but this can be overwritten with a custom name.

Define a Schedule and Snapshot Lifetime

Schedule and Lifetime

Adding a schedule automates the task to run according to your chosen times. You can choose between a number of preset schedules or create a custom schedule for when the replication runs. Choosing to run the replication once runs the replication immediately after saving the task, but you must manually trigger any additional replications.

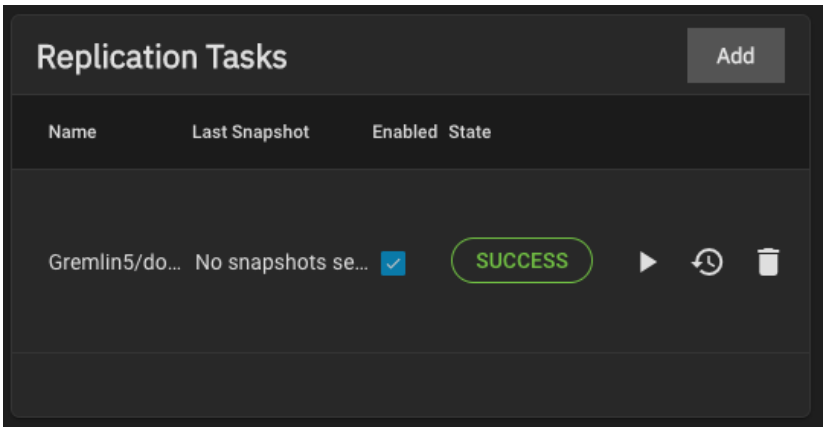
Finally, define how long you want to keep snapshots on the destination system. We generally recommend defining snapshot lifetime to prevent cluttering the system with obsolete snapshots.



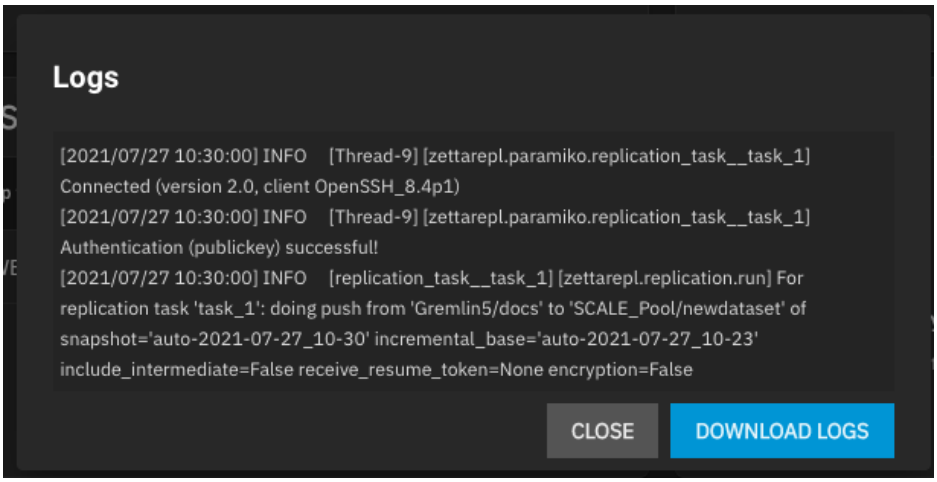
Starting the Replication

Starting the Replication

Start Replication* saves the new replication task. New tasks are enabled by default and activate according to their schedule or immediately when no schedule is chosen. The first time a replication task runs, it takes longer because the snapshots must be copied entirely fresh to the destination.



Later replications run faster since the task only replicates subsequent changes to snapshots. Clicking the task state opens the log for that task.



Related Content

- Adding Replication Tasks
- Managing Advanced Settings
- Setting Up a Local Replication Task
- Advanced Settings Screen
- Setting Up Advanced Replication Tasks
- Periodic Snapshot Tasks Screens
- Unlocking a Replication Encrypted Dataset or Zvol
- Replication Task Screens

3.4.7.4 - Unlocking a Replication Encrypted Dataset or Zvol

This article provides information on three methods of unlocking replicated encrypted datasets or zvols without a passphrase.

Unlocking a Replicated Encrypted Dataset or Zvol Without a Passphrase

TrueNAS SCALE users should either replicate the dataset/Zvol without properties to disable encryption at the remote end or construct a special JSON manifest to unlock each child dataset/zvol with a unique key.

Method 1: Construct JSON Manifest.

1. Replicate every encrypted dataset you want to replicate with properties.
2. Export key for every child dataset that has a unique key.
3. For each child dataset construct a proper json with poolname/datasetname of the destination system and key from the source system like this: `{"tank/share01": "57112db4be777d93fa7b76138a68b790d46d6858569bf9d13e32eb9fda72146b"}`
4. Save this file with the extension .json.
5. On the remote system, unlock the dataset(s) using properly constructed json files.

Method 2: Replicate Encrypted Dataset/zvol Without Properties.

Uncheck properties when replicating so that the destination dataset is not encrypted on the remote side and does not require a key to unlock.

1. Go to **Data Protection** and click **ADD** in the **Replication Tasks** window.
2. Click **Advanced Replication Creation**.
3. Fill out the form as needed and make sure **Include Dataset Properties** is *NOT* checked.
4. Click **Save**.

Method 3: Replicate Key Encrypted Dataset/zvol.

1. Go to **Storage -> pool/root dataset** on the replication system. Click ⋮ and select **Export Key**.
2. Apply the key file or key code to the dataset. Either download the key file, open that file and change the *pool name/dataset* to the receiving *pool name/dataset*, or copy the key code provided in the **Key** window.
3. On the receiving pool/dataset: Click ⋮ next to pool/dataset and select **Unlock**.
4. Unlock the dataset. Either clear the **Unlock with Key file** checkbox, paste the Key Code into **Dataset Key** field (if there is a space character at the end of the key, delete the space), or select the downloaded Key file that was edited.
5. Click **Save**.
6. Click **Continue**.

Related Content

- Adding Replication Tasks
- Managing Advanced Settings
- Setting Up a Local Replication Task
- Advanced Settings Screen
- Setting Up Advanced Replication Tasks
- Periodic Snapshot Tasks Screens
- Setting Up a Remote Replication Task
- Replication Task Screens

3.5 - Credentials

SCALE Credential options are collected in this section of the UI and organized into a few different screens:

- **Local Users** allows those with permissions to add, configure, and delete users on the system. There are options to search for keywords in usernames, display or hide user characteristics, and toggle whether the system shows built-in users.
- **Local Groups** allows those with permissions to add, configure, and delete user groups on the system. There are options to search for keywords in group names, display or hide group characteristics, and toggle whether the system shows built-in groups.
- **Directory Services** contains options to edit directory domain and account settings, set up Idmapping, and configure access and authentication protocols. Specific options include configuring Kerberos realms and key tables (keytab), as well as setting up LDAP validation.
- **Backup Credentials** stores credentials for cloud backup services, SSH Connections, and SSH Keypairs. Users can set up backup credentials with cloud and SSH clients to back up data in case of drive failure.
- **Certificates** contains all the information for certificates, certificate signing requests, certificate authorities, and DNS-authenticators. TrueNAS comes equipped with an internal, self-signed certificate that enables encrypted access to the web interface, but users can make custom certificates for authentication and validation while sharing data.
- **2FA** allows users to set up Two-Factor Authentication for their system. Users can set up 2FA, then link the system to an authenticator app (such as Google Authenticator, LastPass Authenticator, etc.) on a mobile device.

Ready to get started? Choose a topic or article from the left-side **Navigation** pane. Click the **<** symbol to expand the menu to show the topics under this section.

3.5.1 - Managing Users

This article provides instructions on adding and managing local user accounts.

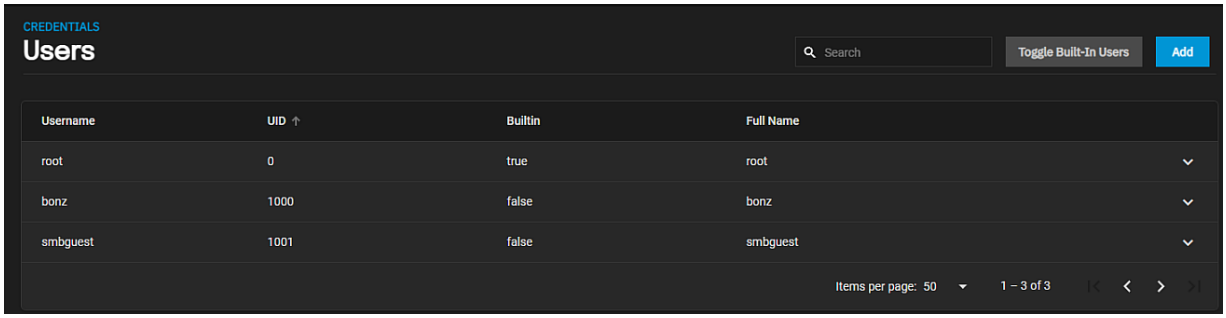
In TrueNAS, user accounts allow flexibility for accessing shared data. Typically, administrators create users and assign them to groups. Doing so makes tuning permissions for large numbers of users more efficient.

> Only the **root** user account can log in to the TrueNAS web interface until the root user creates an admin user with the same permissions.
>
> As part of security hardening and to comply with Federal Information Processing standards (FIPS), iXsystems plans to completely disable root login in a future release. When this occurs, the sign-in screen prompts first-time users to create a new administration account they used in place of the root user. System administrators should create and begin using a new root-level user before this function goes away.

When the network uses a directory service, import the existing account information using the instructions in Directory Services.

Using Active Directory requires setting Windows user passwords in Windows.

To see user accounts, go to **Credentials > Local Users**.



TrueNAS hides all built-in users (except root) by default. Click **Toggle Built-In Users**, then click **SHOW** to see all built-in users.

Creating User Accounts

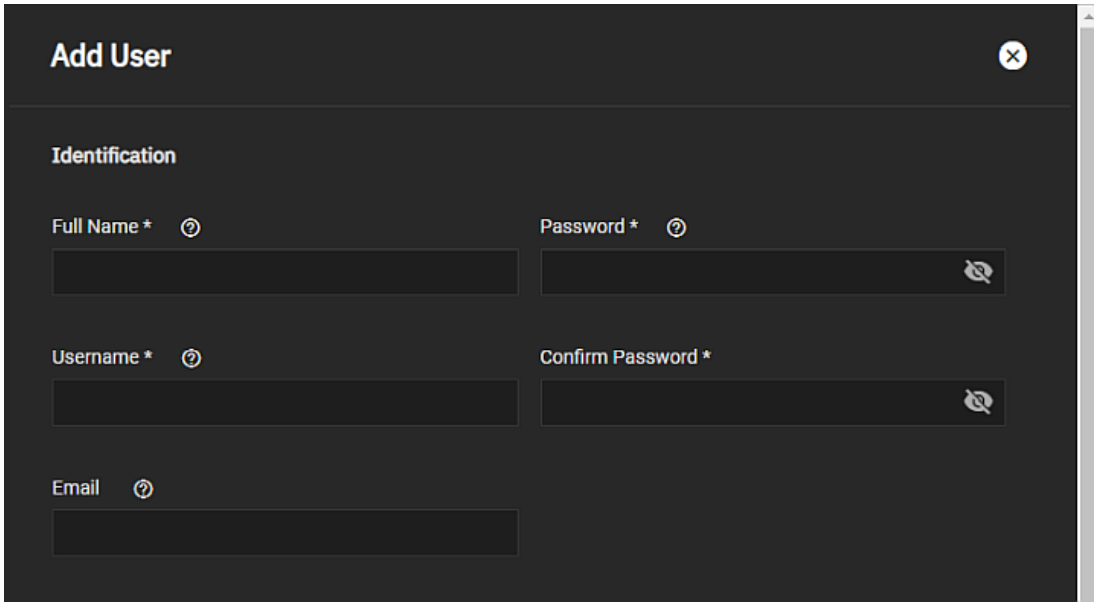
Tutorial Video

This short video demonstrates adding a local user.

To create a new user, click **Add**.

TrueNAS lets users configure four different user account traits (settings).

Configuring User Identification Settings

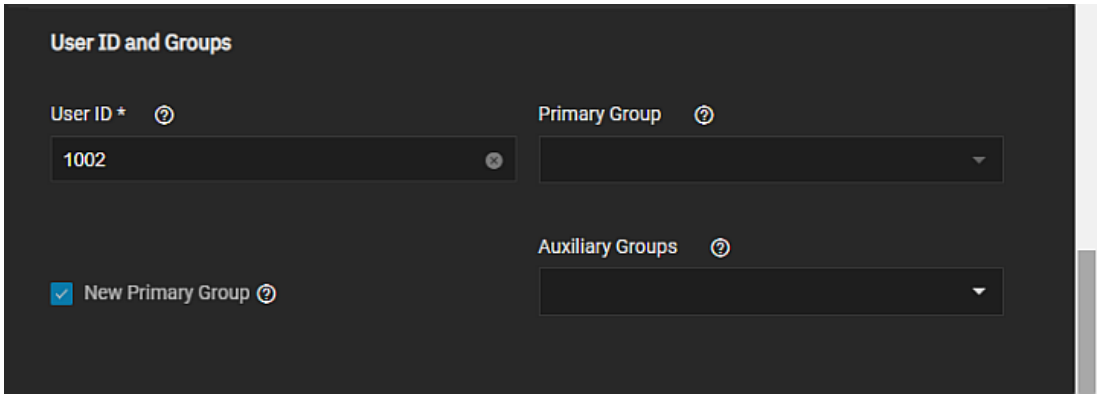


Enter the user full name in **Full Name**. TrueNAS suggests a simplified name in **Username** derived from the **Full Name**, but you can override it with your own choice.

You can also assign a user account email address in the **Email** field.

Set and confirm a password.

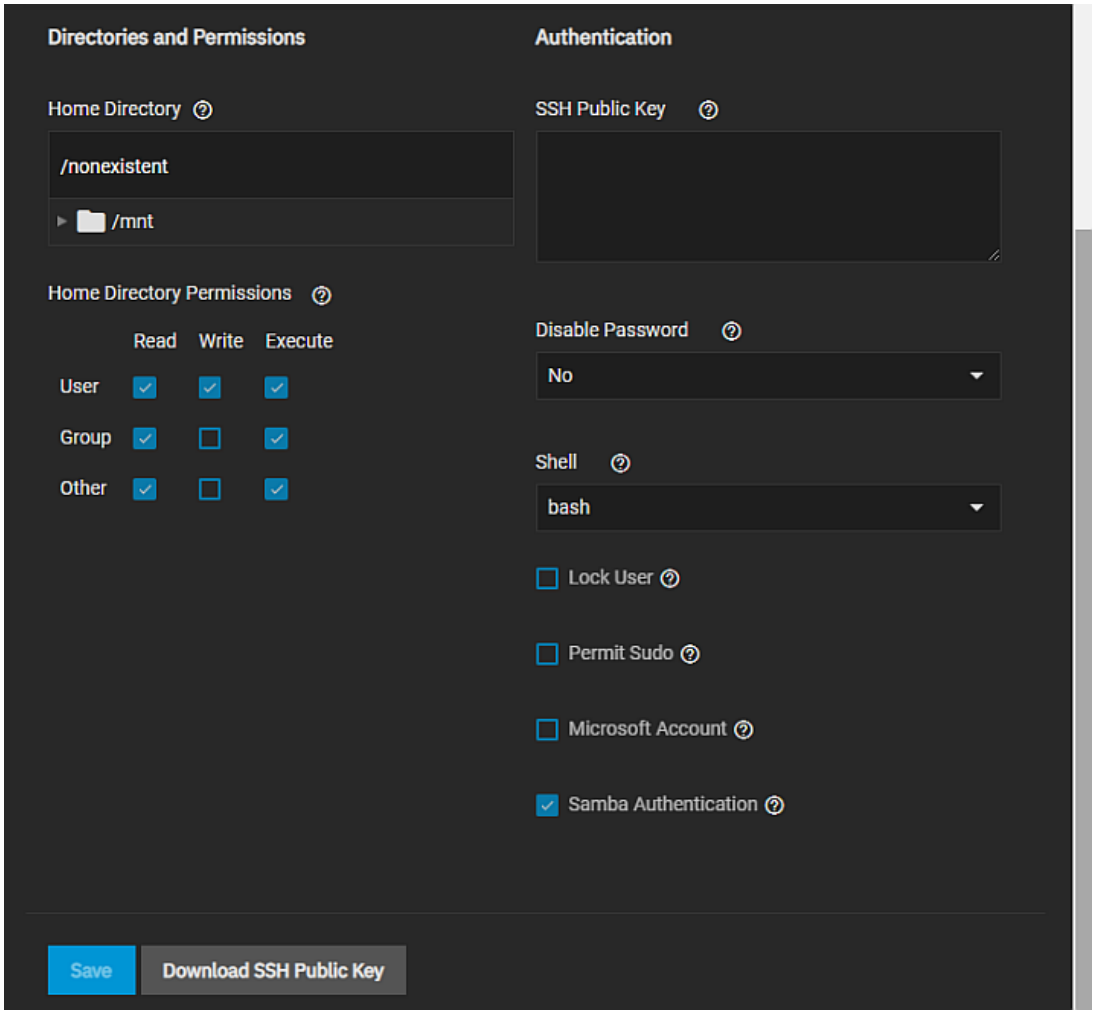
Configuring User ID and Groups Settings



Next, you must set a user ID (UID). TrueNAS suggests a user ID starting at **1000**, but you can change it if you wish. We recommend using an ID of 1000 or greater for non-built-in users. New users can be created with a UID of **0**.

By default, TrueNAS creates a new primary group with the same name as the user. To add the user to an existing primary group instead, clear the **New Primary Group** checkbox and select a group from the **Primary Group** drop-down list. You can add the user to more groups using the **Auxiliary Groups** drop-down list.

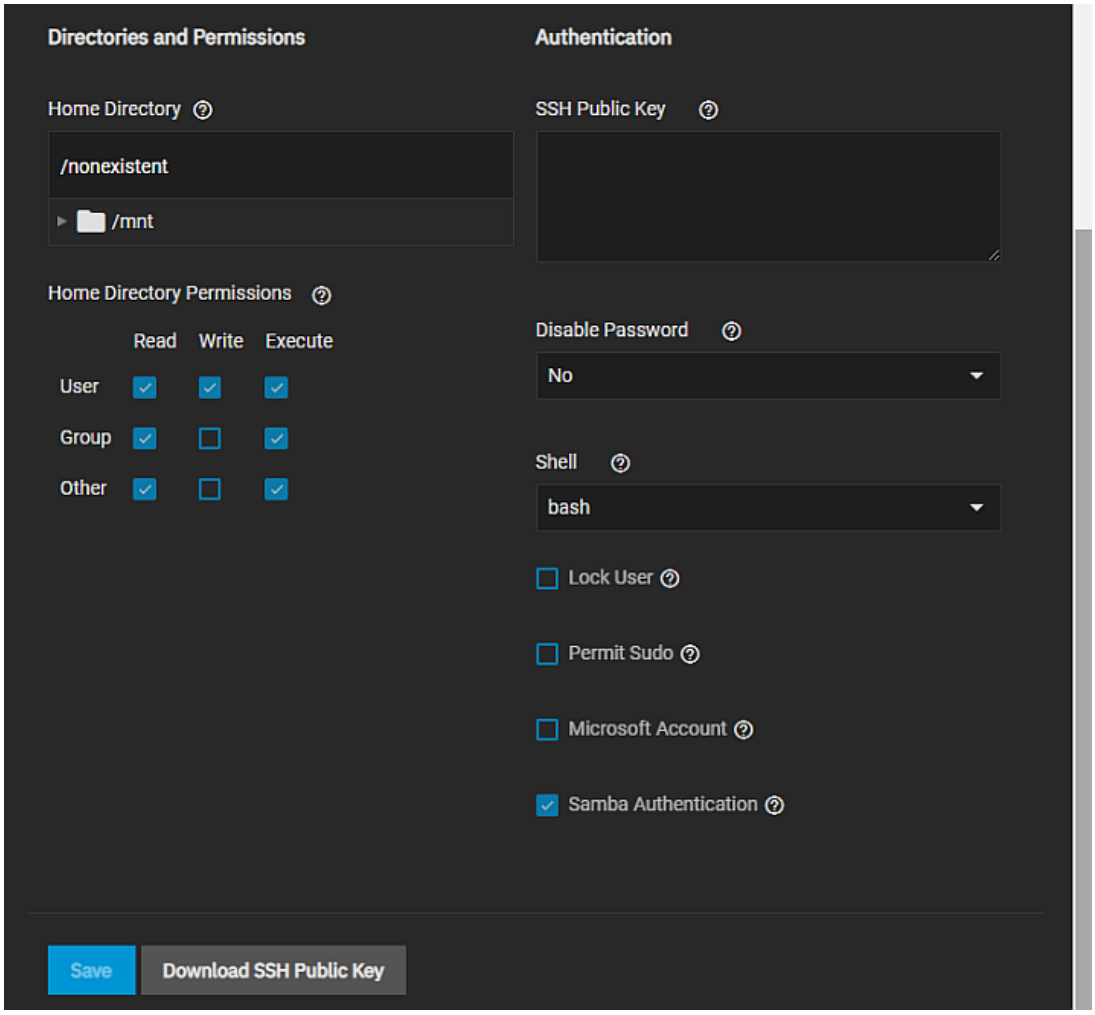
Configuring Directories and Permissions Settings



When creating a user, the home directory path is set to /nonexistent, which does not create a home directory for the user. To set a user home directory, select a path using the file browser. If the directory exists and matches the user name, TrueNAS sets it as the user home directory. When the path does not end with a sub-directory matching the user name, TrueNAS creates a new sub-directory. TrueNAS shows the path to the user home directory when editing a user.

You can set the home directory permissions directly under the file browser. You cannot change TrueNAS default user account permissions.

Configuring Authentication Settings



You can assign a public SSH key to a user for key-based authentication by pasting the *public* key into the **SSH Public Key** field. If you are using an SSH public key, always keep a backup of the key. Click **Download SSH Public Key** to download the pasted key as a .txt file.

By default, **Disable Password** is **No**.

Setting **Disable Password** to **Yes** disables several options:

- The **Password** field becomes unavailable, and TrueNAS removes any existing password from the account.
- The **Lock User** and **Permit Sudo** options disappear.
- The account is restricted from password-based logins for services like SMB shares and SSH sessions.

You can set a specific shell for the user from the **Shell** dropdown options:

Shell	Description
bash	Bourne Again shell for the GNU operating system.
rbash	Restricted bash
dash	Debian Almquist shell
sh	Bourne shell
zsh	Z shell
tmux	terminal multiplexer
nologin	Use when creating a system account or to create a user account that can authenticate with shares but that cannot log in to the TrueNAS system using `ssh`.

Selecting **Lock User** disables all password-based functionality for the account until you clear the checkbox.

Permit Sudo allows the account to act as the system administrator using the `sudo` command. Leave it disabled for better security.

If the user accesses TrueNAS data using Windows 8 or newer, select **Microsoft Account** to enable those systems' additional authentication methods.

By default, **Samba Authentication** is enabled. This allows using the account credentials to access data shared with SMB.

Editing User Accounts

To edit an existing user account, go to **Credentials > Local Users**, expand the user entry, and click **Edit** to open the **Edit User** configuration screen. See Local User Screens for details on all settings.

Related Content

- Local Users Screens

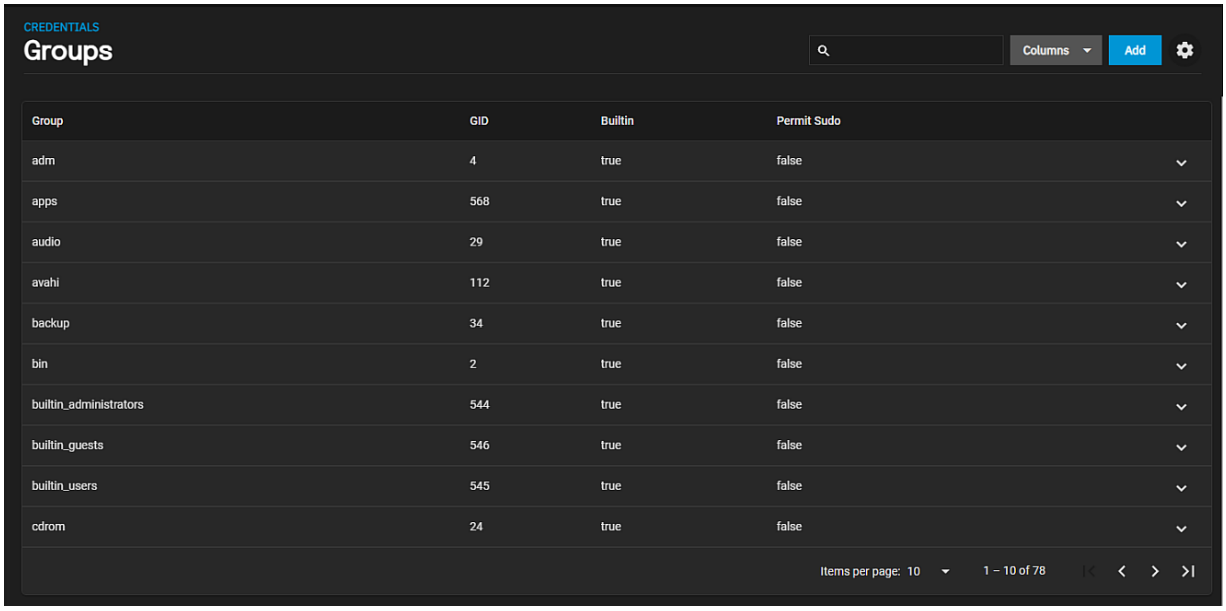
3.5.2 - Managing Local Groups

This article provides instructions to manage local groups.

TrueNAS offers groups as an efficient way to manage permissions for many similar user accounts. See Users for managing users. The interface lets you manage UNIX-style groups. If the network uses a directory service, import the existing account information using the instructions in Active Directory.

View Existing Groups

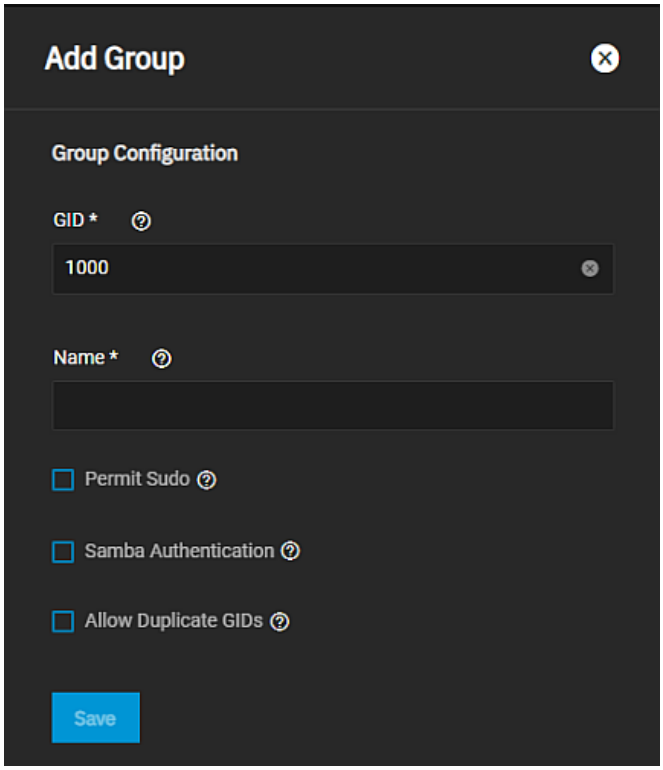
To see saved groups, go to **Credentials > Local Groups**.



By default, TruNAS hides the system built-in groups. To see built-in groups, click **Toggle Built-In Groups** icon. The **Show Built-In Groups** dialog opens. Click **Show**. Click **Toggle Built-In Groups** icon again to open the **Hide Built-In Groups** dialog. Click **Hide** to show only non-built-in groups on the system.

Adding a New Group

To create a group, go to **Credentials > Local Groups** and click **Add**.



Enter a unique number for the group ID in **GID** that TrueNAS uses to identify a Unix group. Enter a number above 1000 for a group with user accounts or for a system service enter the default port number for the service as the GID. Enter a name for the group. The group name cannot begin with a hyphen (-) or contain a space, tab, or any of these characters: colon (:), plus (+), ampersand (&), hash (#), percent (%), carat (^), open or close parentheses ( ), exclamation mark (!), at symbol (@), tilde (~), asterisk (*), question mark (?) greater or less than (<) (>), equal). You can only use the dollar sign ($) as the last character in a user name.

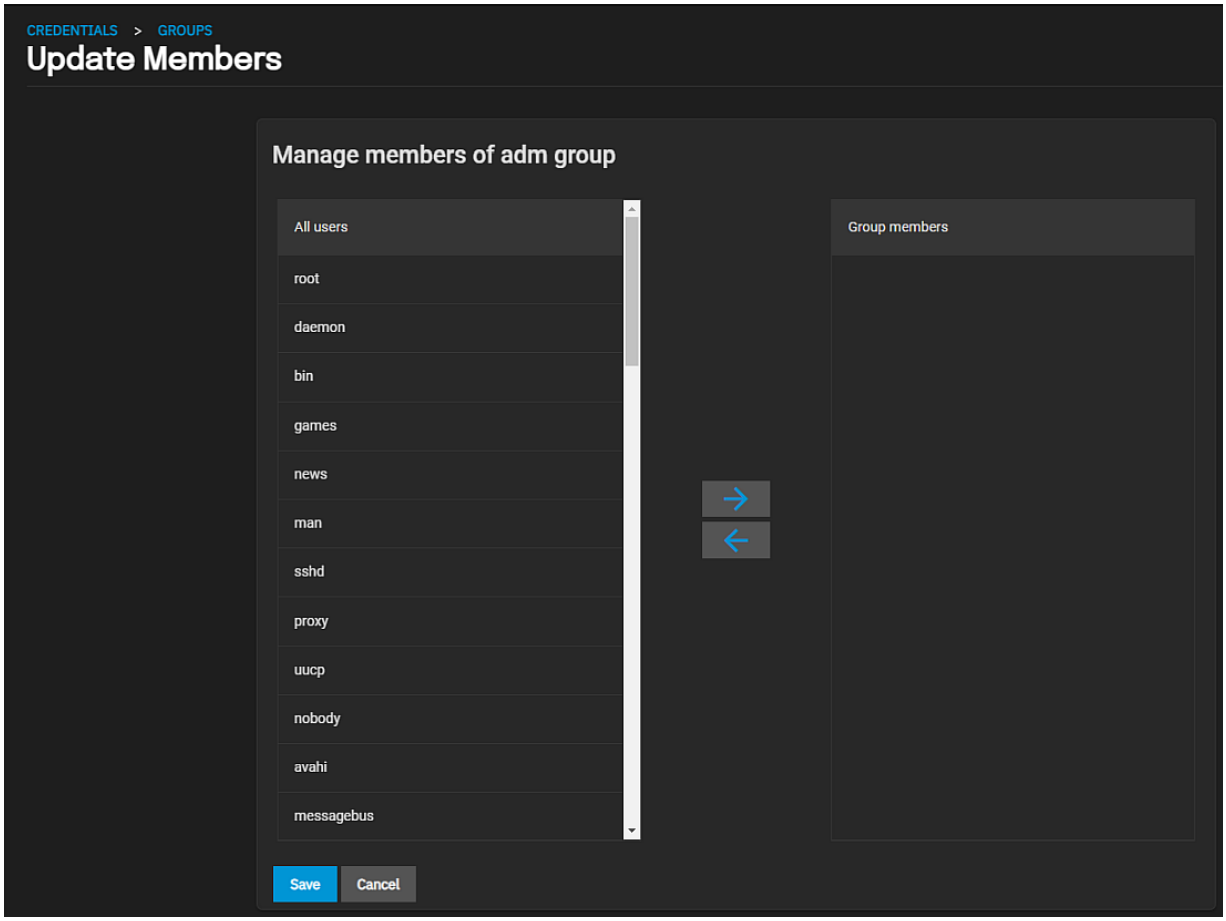
If giving this group administration permissions, select **Permit Sudo**.

To allow Samba permissions and authentication to use this group, select **Samba Authentication**.

To allow more than one group to have the same group ID (not recommended), select **Allow Duplicate GIDs**.

Managing Group Members

To manage group membership, go to **Credentials > Local Groups**, expand the group entry, and click **Members** to open the **Update Members** screen.



To add user accounts to the group, select users and then click ➔. Select **All Users** to move all users to the selected group, or select multiple users by holding `Ctrl` while clicking each entry.

Related Content

- Local Groups Screens

3.5.3 - Setting Up Directory Services

The SCALE Directory Services section contains options to edit directory domain and account settings, set up Idmapping, and configure authentication and authorization services in TrueNAS SCALE.

Choosing Active Directory or LDAP

When setting up directory services in TrueNAS, you can connect TrueNAS to either an Active Directory or an LDAP server.

Configuring Active Directory In TrueNAS

The Active Directory (AD) service shares resources in a Windows network. AD provides authentication and authorization services for the users in a network, eliminating the need to recreate the user accounts on TrueNAS.

Once joined to an AD domain, you can use domain users and groups in local ACLs on files and directories. You can also set up shares to act as a file server.

Joining an AD domain also configures the Privileged Access Manager (PAM) to let domain users log on via SSH or authenticate to local services.

Users can configure AD services on Windows or Unix-like operating systems using Samba version 4.

To configure an AD connection, you must know the AD controller domain and the AD system account credentials.

Preparation

Users can take a few steps before configuring Active Directory to ensure the connection process goes smoothly.

Verify Name Resolution

To confirm that name resolution is functioning, go to **System Settings > Shell** and use `ping` to check the connection to the AD domain controller.

```
truenas# ping ad02.lab.ixsystems.com
ping: ad02.lab.ixsystems.com (10.215.5.200): 56 data bytes
64 bytes from 10.215.5.200: icmp_seq=0 ttl=126 time=0.800 ms
64 bytes from 10.215.5.200: icmp_seq=1 ttl=126 time=0.933 ms
^C
--- ad02.lab.ixsystems.com ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.800/0.933 ms
truenas#
```

When TrueNAS sends and receives packets without loss, the connection is verified. Press `Ctrl + C` to cancel the `ping`.

Another option is to use `host -t srv _ldap._tcp.domainname.com` to check the network SRV records and verify DNS resolution.

The ping failed!
If the ping fails, go to **Network** and click **Settings** in the **Global Configuration** window. Update the **DNS Servers** and **Default Gateway** settings so the connection to your Active Directory Domain Controller can start. Use more than one **Nameserver** for the AD domain controllers so DNS queries for requisite SRV records can succeed. Using more than one Nameserver helps maintain the AD connection whenever a domain controller becomes unavailable.

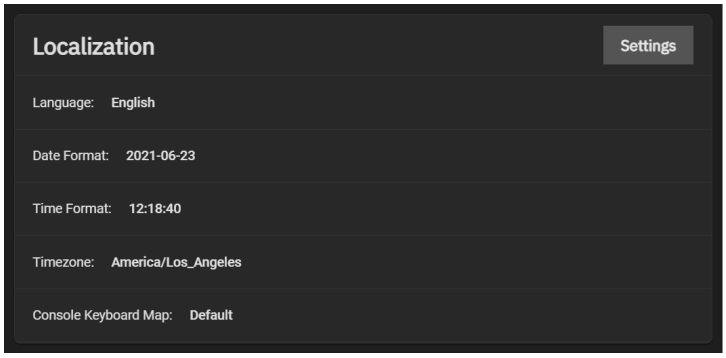
Time Synchronization

Active Directory relies on the time-sensitive Kerberos protocol. TrueNAS adds the AD domain controller with the PDC Emulator FSMO Role as the preferred NTP server during the domain join process. If your environment requires something different, go to **System Settings > General** and add or edit a server in the **NTP Servers** window.

The local system time cannot be out of sync by more than **five (5) minutes** with the AD domain controller time in a default AD environment. Use an external time source when configuring a virtualized domain controller. TrueNAS generates alerts if the system time gets out-of-sync with the AD domain controller time.

TrueNAS has a few options to ensure both systems are synchronized:

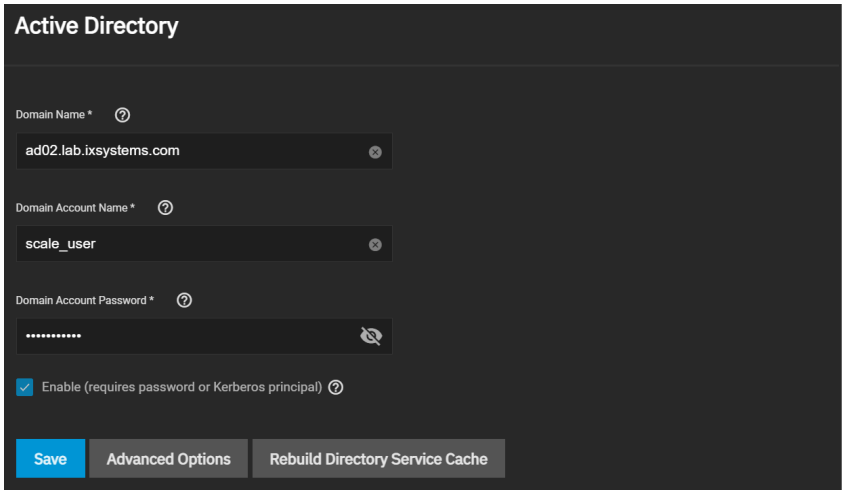
1. Go to **System Settings > General** and click **Settings** in the **Localization** window to ensure the **Timezone** matches the AD Domain Controller.



2. Set either local time or universal time in the system BIOS.

Connect to the Active Directory Domain

To connect to Active Directory, click **Settings** in the **Active Directory** window and enter the AD **Domain Name** and account credentials. Set *Enable* to attempt to join the AD domain immediately after saving the configuration.



TrueNAS offers advanced options for fine-tuning the AD configuration, but the preconfigured defaults are generally suitable.

I don't see any AD information!
TrueNAS can take a few minutes to populate the Active Directory information after configuration. To check the AD join progress, open the **Task Manager** in the upper-right corner. TrueNAS displays any errors during the join process in the **Task Manager**.

When the import is complete, AD users and groups become available while configuring basic dataset permissions or an ACL with TrueNAS cache enabled (enabled by default).

Joining AD also adds default Kerberos realms and generates a default `AD_MACHINE_ACCOUNT` keytab. TrueNAS automatically begins using this default keytab and removes any administrator credentials stored in the TrueNAS configuration file.

Troubleshooting

Resync the Cache

If the cache becomes out of sync or fewer users than expected are available in the permissions editors, resync it by clicking **Settings** in the **Active Directory** window and selecting **Rebuild Directory Service Cache**.

If you are using Windows Server with 2008 R2 or older, try creating a **Computer** entry on the Windows server Organizational Unit (OU).

When creating the entry, enter the TrueNAS hostname in the name field and make sure it matches the:

- *Hostname*: Go to **Network** and find **Hostname** in the **Global Configuration** window.
- *NetBIOS alias*: Go to **Credentials > Directory Services** and click **Settings** in the **Active Directory** window. Click **Advanced Options** and find the **NetBIOS alias**.

Shell Commands

You can go to **System Settings > Shell** and enter various commands to get more details about the AD connection and users:

AD current state: `midclt call activedirectory.get_state`.

Connected LDAP server details: `midclt call activedirectory.domain_info | jq`. For example:

```
truenas# midclt call activedirectory.domain_info | jq
{
  "LDAP server": "192.168.1.125",
  "LDAP server name": "DC01.HOMEDOM.FUN",
  "Realm": "HOMEDOM.FUN",
  "Bind Path": "dc=HOMEDOM,dc=FUN",
  "LDAP port": 389,
  "Server time": 1593026080,
  "KDC server": "192.168.1.125",
  "Server time offset": 5,
  "Last machine account password change": 1592423446
}
```

View AD users: `wbinfo -u`.

- Enter `getent passwd DOMAIN\\<user>` to see more user details (`<user>` = desired user name).
- If `wbinfo -u` shows more users than are available when configuring permissions and the TrueNAS cache is enabled, go to **Directory Services**, click *Settings* in the *Active Directory* window, and increase the *AD Timeout* value.

View AD groups: `wbinfo -g`. Enter `getent group DOMAIN\\domain\ users` to see more details.

View domains: `wbinfo -m`.

Test AD connection: `wbinfo -t`.

- A successful test shows a message like `checking the trust secret for domain YOURDOMAIN via RPC calls succeeded`.

Test user connection to SMB share: `smbclient '//0.0.0.0/smbshare -U AD.DOMAIN.COM\user`

- `0.0.0.0` is the server address
- `smbshare` is the SMB share name
- `AD.DOMAIN.COM` is the trusted domain
- `user` is the user account name to authenticate.

Clean Up Active Directory

TrueNAS SCALE requires users to cleanly leave an Active Directory using the **Leave Domain** button under **Advanced Settings** to remove the AD object.

If the AD server moves or shuts down without you using **Leave Domain**, TrueNAS won't remove the AD object, and you will have to clean up the Active Directory.

Go to **Credentials > Directory Services** and click **Show** next to **Advanced Settings**

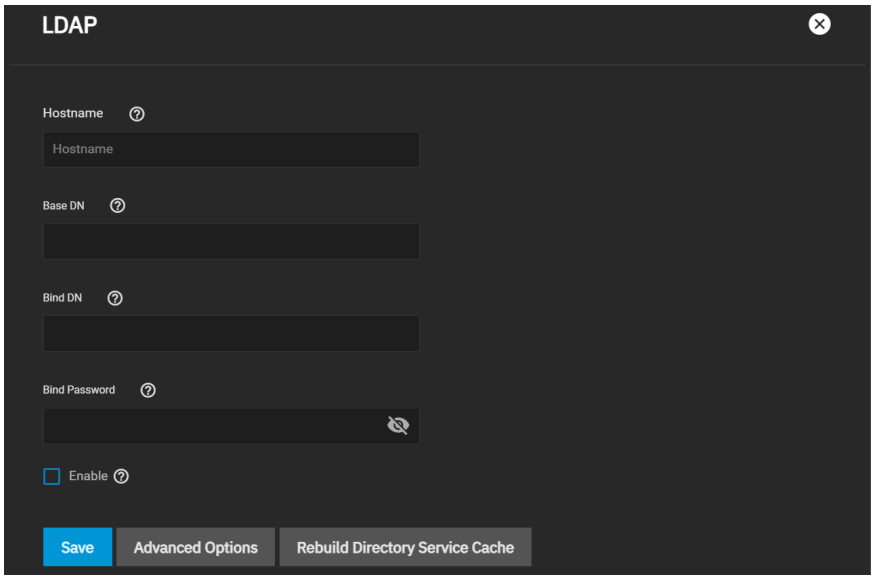
1. Clean out Kerberos settings by clicking **Settings** in the **Kerberos Settings** window and clearing the **Appdefaults Auxiliary Parameters** and **Libdefaults Auxiliary Parameters** boxes. You may also need to clear out leftover Kerberos Realms and Keytabs by clicking the next to the remaining entries.
2. Click the *Idmap Active Directory - Primary Domain* entry and clear out the Active Directory settings, then click **CONTINUE** to clear the Idmap cache.
3. Go to **Network** and click *Settings* in the *Global Configuration* window. Remove the Active Directory Nameserver and enter a new one.
4. Ensure all other network settings are correct.
5. Go to **System Settings > Services** and change the workgroup to "WORKGROUP".
6. Go to **Credentials> Directory Services** and edit the Active Directory config to the new domain.
7. Make sure the Kerberos settings and Idmap are correct and SMB is running.

Configuring LDAP In TrueNAS

TrueNAS has an Open LDAP client for accessing the information on an LDAP server. An LDAP server provides directory services for finding network resources like users and their associated permissions.

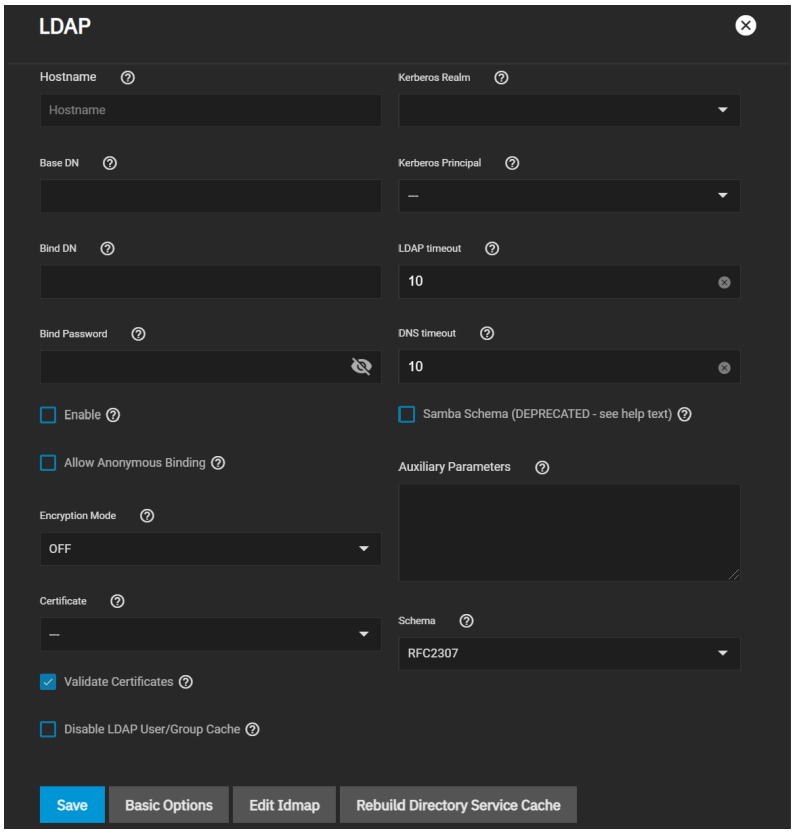
Does LDAP work with SMB?
LDAP authentication for SMB shares is disabled unless you have configured and populated the LDAP directory with Samba attributes. The most popular script for performing this task is `smbldap-tools`. The LDAP server must support SSL/TLS, and you must import the certificate for the LDAP server CA. TrueNAS does not support non-CA certificates.

Go to **Credentials > Directory Services** and click **Configure LDAP**.



Enter your LDAP server hostname, then enter your LDAP server Base and Bind domain names and the bind password. Check the **Enable** box to activate the server, then click **Save**.

To further modify the LDAP configuration, click **Advanced Options**. See the LDAP UI Reference article for details about advanced settings.



Troubleshooting Directory Services

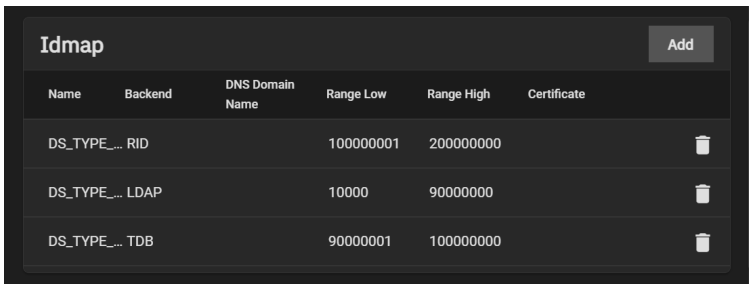
If the AD or LDAP cache becomes out of sync or fewer users than expected are available in the permissions editors, resync the cache using the *Rebuild Directory Service Cache*.

Advanced Settings

To view Idmap and Kerberos Services, click **Show** next to **Advanced Settings**.

Idmap

The **Idmap** directory service lets users configure and select a backend to map Windows security identifiers (SIDs) to UNIX UIDs and GIDs. Users must enable the **Active Directory** service to configure and use Identity Mapping (Idmap).



Users can click **Add** in the **Idmap** window to configure backends or click on an already existing Idmap to edit it.

TrueNAS automatically generates an Idmap after you configure AD or LDAP.

Kerberos

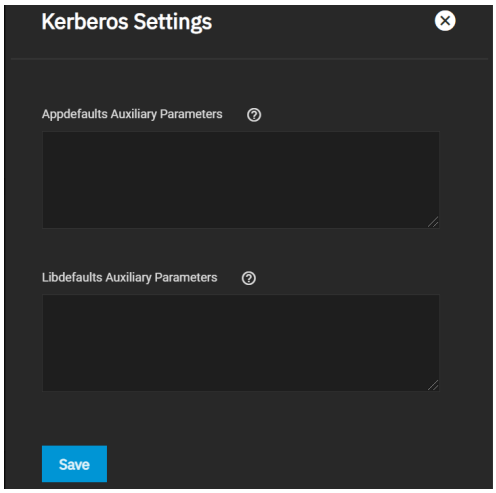
Kerberos is a web authentication protocol that uses strong cryptography to prove the identity of both client and server over an insecure network connection.

Kerberos uses “realms” and “keytabs” to authenticate clients and servers. A Kerberos realm is an authorized domain that a Kerberos server can use to authenticate a client. By default, TrueNAS creates a Kerberos realm for the local system. A keytab (“key table”) is a file that stores encryption keys for authentication.

TrueNAS SCALE allows users to configure general Kerberos settings, as well as realms and keytabs.

Kerberos Settings

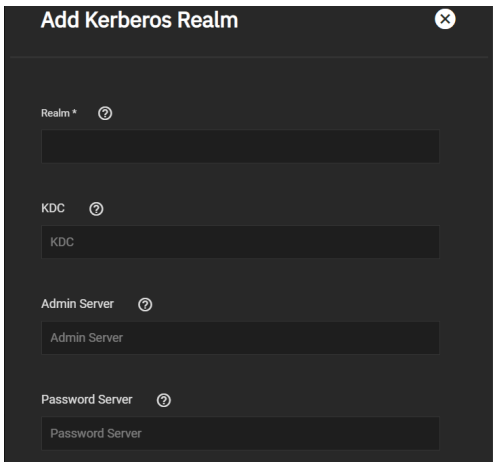
Users can configure Kerberos settings by navigating to **Directory Services** and clicking **Settings** in the **Kerberos Settings** window.



Field	Description
Appdefaults Auxiliary Parameters	Additional Kerberos application settings. See [appdefaults] in krb.conf(5) for settings and usage syntax.
Libdefaults Auxiliary Parameters	Additional Kerberos library settings. See [libdefaults] in krb.conf(5) for settings and usage syntax.

Kerberos Realms

Users can configure Kerberos realms by navigating to **Directory Services** and clicking **Add** in the **Kerberos Realms** window.



Enter the Realm and Key Distribution (KDC) names, then define the Admin and Password servers for the Realm.

TrueNAS automatically generates a Realm after you configure AD or LDAP.

Kerberos Keytabs

Kerberos keytabs let you join an Active Directory or LDAP server without a password.

TrueNAS automatically generates a Keytab after you configure AD or LDAP.

Since TrueNAS does not save the Active Directory or LDAP administrator account password in the system database, keytabs can be a security risk in some environments.

> When using a keytab, create and use a less-privileged account to perform queries. TrueNAS will store that account's password in the system database.

Create a Keytab on Windows

To create a keytab on a Windows system, use the ktpass command:

```
ktpass.exe /out file.keytab /princ http/user@EXAMPLE.COM /mapuser user /ptype KRB5_NT_PRINCIPAL /crypto
ALL /pass userpass
```

- `file.keytab` is the file to upload to the TrueNAS server.
- `user` is the user account name for the TrueNAS server generated in Active Directory Users and Computers.
- `http/user@EXAMPLE.COM` is the principal name written in the format `host/user.account@KERBEROS.REALM`. The Kerberos realm is usually in all caps, but be sure to match the Kerberos Realm case with the realm name. See this note about using `/princ` for more details.
- `userpass` is the `user`'s password.
- `/crypto` is the cryptographic type.

Setting `/crypto` to *ALL* allows using all supported cryptographic types. You can use specific keys instead of using *ALL*:

- *DES-CBC-CRC* is backward compatible.
- *DES-CBC-MD5* adheres more closely to the MIT implementation and is backward compatible.
- *RC4-HMAC-NT* uses 128-bit encryption.
- *AES256-SHA1* uses AES256-CTS-HMAC-SHA1-96 encryption.
- *AES128-SHA1* uses AES128-CTS-HMAC-SHA1-96 encryption.

Add the Windows Keytab to TrueNAS

After generating the keytab, go back to **Directory Services** in TrueNAS and click **Add** in the **Kerberos Keytab** window to add it to TrueNAS.

To make AD use the keytab, click **Settings** in the **Active Directory** window and select it using the **Kerberos Principal** drop-down.

When using a keytab with AD, ensure the keytab *username* and *userpass* match the *Domain Account Name* and *Domain Account Password*.

To make LDAP use a keytab principal, click **Settings** in the **LDAP** window and select the keytab using the **Kerberos Principal** drop-down.

3.5.4 - Backup Credentials

This article provides infomation on backup credential tutorials on integrating TrueNAS SCLE with cloud storage providers by setting up SSH connections and keypairs.

TrueNAS backup credentials store cloud backup services credentials, SSH connections, and SSH keypairs. Users can set up backup credentials with cloud and SSH clients to back up data in case of drive failure.

Article Summaries

- Adding Cloud Credentials

  This article provides basic instructions on how to add backup cloud credentials, and more detailed instructions for some cloud storage providers.

- Adding SSH Credentials

  This article provides information on adding SSH connections, generating SSH keypairs, and adding the SSH public key to the root user.

3.5.4.1 - Adding Cloud Credentials

This article provides basic instructions on how to add backup cloud credentials, and more detailed instructions for some cloud storage providers.

The **Cloud Credentials** widget on the **Backup Credentials** screen allows users to integrate TrueNAS with cloud storage providers.

Is this secure?
To maximize security, TrueNAS encrypts cloud credentials when saving them. However, this means that to restore any cloud credentials from a TrueNAS configuration file, you must enable **Export Password Secret Seed** when generating that configuration backup. Remember to protect any downloaded TrueNAS configuration files.

TrueNAS SCALE supports linking to 18 cloud storage providers. Authentication methods for each provider could differ based on the provider security requirements. You can add credentials for many of the supported cloud storage providers from the information on the Cloud Credentials Screens. This article provides instructions for the more involved providers.

Before You Begin

We recommend users open another browser tab to open and log into the cloud storage provider account you intend to link with TrueNAS.

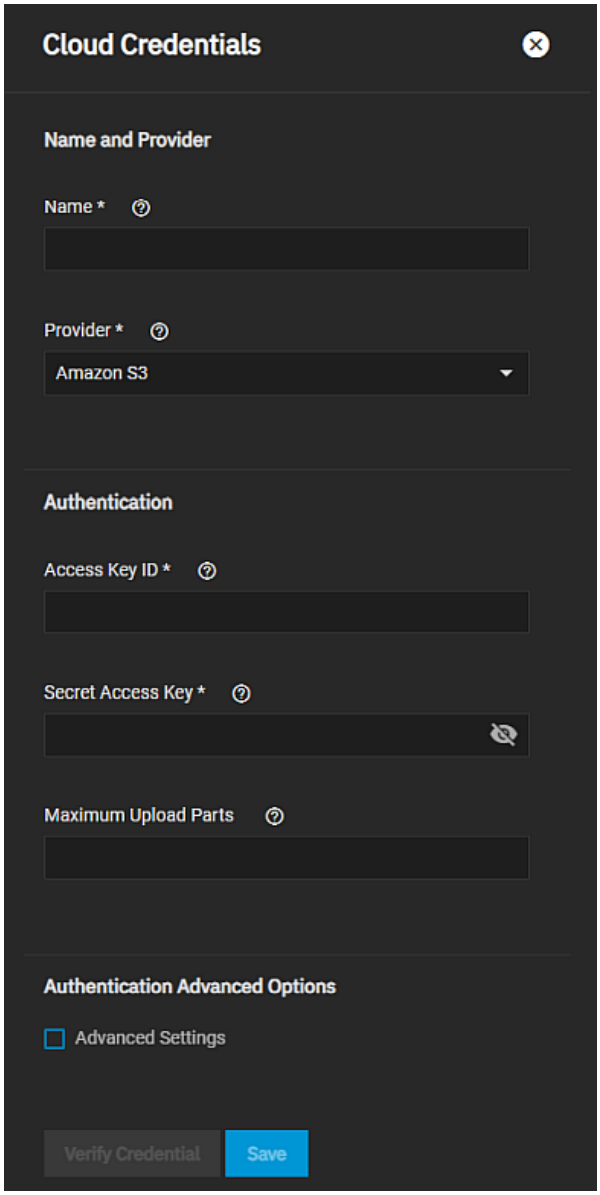
Some providers require additional information that they generate on the storage provider account page. For example, saving an Amazon S3 credential on TrueNAS could require logging in to the S3 account and generating an access key pair found on the **Security Credentials > Access Keys** page.

Have any authentication information your cloud storage provider requires on-hand to make the process easier. Authentication information could include but are not limited to user credentials, access tokens, and access and security keys.

Adding Cloud Credentials

To set up a cloud credential, go to **Credentials > Backup Credentials** and click **Add** in the **Cloud Credentials** widget.

1. Enter a credential name.



2. Select the cloud service from the **Provider** dropdown list. The provider required authentication option settings display.

   For details on each provider authentication settings see Cloud Credentials Screens.

3. Click **Verify Credentials** to test the entered credentials and verify they work.

4. Click **Save**.

Adding Amazon S3 Cloud Credentials

If adding an Amazon S3 cloud credential, you can use the default authentication settings or use advanced settings if you want to include endpoint settings.

Click here for more information

After entering a name and leaving **Amazon S3** as the **Provider** setting:

1. Open a web browser tab to Amazon AWS.

2. Navigate to **My account > Security Credentials > Access Keys** to obtain the Amazon S3 secret access key ID. Access keys are alphanumeric and between 5 and 20 characters.

   If you cannot find or remember the secret access key, go to **My Account > Security Credentials > Access Keys** and create a new key pair.

3. Enter or copy/paste the access key into **Access Key ID**.

4. Enter or copy/paste the Amazon Web Services alphanumeric password that is between 8 and 40 characters into **Secret Access Key**

5. (Optional) Enter a value to define the maximum number of chunks for a multipart upload in **Maximum Upload Ports**. Setting a maximum is necessary if a service does not support the 10,000 chunk AWS S3 specification.
6. (Optional) Select **Advanced Settings** to display the endpoint settings.

   a. Enter the S3 API endpoint URL in **Endpoint URL**.

   To use the default endpoint for the region and automatically fetch available buckets leave this field blank. For more information refer to the AWS Documentation for a list of Simple Storage Service Website Endpoints.

   b. Enter an AWS resources in a geographic area in **Region**.

   To detect the correct public region for the selected bucket leave the field blank. Entering a private region name allows interacting with Amazon buckets created in that region.

   c. (Optional) Configure a custom endpoint URL. Select **Disable Endpoint Region**.

   d. (Optional) Select **User Signature Version 2** to force using signature version 2 with the custom endpoint URL. For more information on using this to sign API requests see Signature Version 2.
7. Click **Verify Credentials** to check your credentials for any issues.
8. Click **Save**

Adding Cloud Credentials that Authenticate with OAuth

Cloud storage providers using OAuth as an authentication method are Box, Dropbox, Google Drive, Google Photo, pCloud and Yandex.

Click here for more information

After logging into the provider with the OAuth credentials, the provider provides the access token. Google Drive and pCloud use one more setting to authenticate credentials.

1. Enter the name and select the cloud storage provider from the **Provider** dropdown list.
2. Enter the provider account email in **OAuth Client ID** and the password for that user account in **OAuth Client Secret**.
3. Click **Log In To Provider**. The **Authentication** window opens. Click **Proceed** to open the OAuth credential account sign in window.

   Yandex displays a cookies message you must accept before you can enter credentials.

   Enter the provider account user name and password to verify the credentials.
4. (Optional) Enter the value for any additional authentication method. For pCloud, enter the pCloud host name for the host you connect to in **Hostname**. For Google Drive when connecting to **Team Drive**, enter the Google Drive top-level folder ID.
5. If not populated by the provider after OAuth authentication, enter the access token from the provider. Obtaining the access token varies by provider.

Provider	Access Token
Box	For more information the user acess token for Box click here. An access token enables Box to verify a request belongs to an authorized session. Example token: T9cE5asGnuyYCCqIZFoWjFHvNbvVqHjl.
Dropbox	Create an access token from the Dropbox account.
Google Drive	The authentication process creates the token for Google Drive and populates the **Access Token** field automatically. Access tokens expire periodically, so you must refresh them.
Google Photo	does not used an access token.
pCloud	Create the pCloud access token here. These tokens can expire and require an extension.
Yandex	Create the Yandex access token here.

6. Click **Verify Credentials** to make sure you can connect with the entered credentials.
7. Click **Save**.

Adding BackBlaze B2 Cloud Credentials

BackBlaze B2 uses an application key and key ID to authenticate credentials.

Click here for more information

From the **Cloud Credentials** widget, click **Add** and then:

1. Enter the name and select **BackBlaze B2** from the **Provider** dropdown list.
2. Log into the BackBlaze account, go to **App Keys** page and add a new application key. Copy and past this into **Key ID**.
3. Generate a new application key on the BackBlaze B2 website. From the **App Keys** page, add a new application key. Copy the application Key string **Application Key**.
4. Click **Verify Credentials**.
5. Click **Save**.

Adding Google Cloud Storage Credentials

Google Cloud Storage uses a service account json file to authenticate credentials.

Click here for more information

From the **Cloud Credentials** widget, click **Add** and then:

1. Enter the name and select **Google Cloud Storage** from the **Provider** dropdown list.
2. Go to your Google Cloud Storage website to download this file to the TrueNAS SCALE server. The Google Cloud Platform Console creates the file.
3. Upload the json file to **Preview JSON Service Account Key** using **Choose File** to browse the server to locate the downloaded file.
   For help uploading a Google Service Account credential file click here.
4. Click **Verify Credentials**.
5. Click **Save**.

Adding Microsoft OneDrive Cloud Credentials

Microsoft OneDrive Cloud uses OAuth authentication, an access token, and Drives list, account type and IDs to authenticate credentials.

Click here for more information

From the **Cloud Credentials** widget, click **Add** and then:

1. Enter the name and select **Google Cloud Storage** from the **Provider** dropdown list.
2. Enter your account credentials in **OAuth Client ID** and **OAuth Client Secret**. Click **Log In To Provider**. Click **Proceed** on the **Authentication** window, and then enter your user credentials on the sign in screen.
3. Enter the token generated by the Microsoft OneDrive website through the OAuth authentication in **Access Token** if not populated by this process. For help with the authentication token click Microsoft Onedrive Access Token.
4. Enter the Microsoft OneDrive drive information.

   a. Select the drive(s) from the **Drives List** dropdown options of drives and IDs registered to the Microsoft account. This should populate **Drive ID**.

   b. Select the Microsoft account type from the **Drive Account Type** dropdown options.

   c. Enter the unique drive identifier in **Drive ID** if not already populated by selecting the drive(s) in **Drives List**. If necessary to add valid drive IDs, from your Microsoft account and choose a drive from the **Drives List** dropdown list.
5. Click **Verify Credentials**.
6. Click **Save**.

Adding OpenStack Swift Cloud Credentials

OpenStack Swift authentication credentials change based on selections made in **AuthVersion**. All options use the user name, API key or password and authentication URL, and can use the optional endpoint settings.

Click here for more information

For more information on OpenStack Swift settings see rclone documentation.

From the **Cloud Credentials** widget, click **Add** and then:

1. Enter the name and select **OpenStack Swift** from the **Provider** dropdown list.

2. Enter your OpenStack OS_USERNAME from an OpenStack credentials file in **User Name**.
3. Enter the OS_PASSWORD from an OpenStack credentials file in **API Key or Password**.
4. (Optional) Select the version from the **AuthVersion**. For more information see rclone documentation. If set to **v3** the **Advanced Options** settings display.

   a. (Optional) Enter the user ID to log into OpenStack. Leave blank to log into most Swift systems. (Optional) Enter the **User Domain**.

   b. (Required) Enter the OS_TENANT_NAME from an OpenStack credentials file in **Tenant Name**.

   c. Enter the ID in **Tenant ID**. Required for **v2** and **v3**. (Optional) Enter a **Tenant Domain**.

   d. (Optional) Enter the alternative authentication token in **Auth Token**.
5. (Optional) Enter endpoint settings.

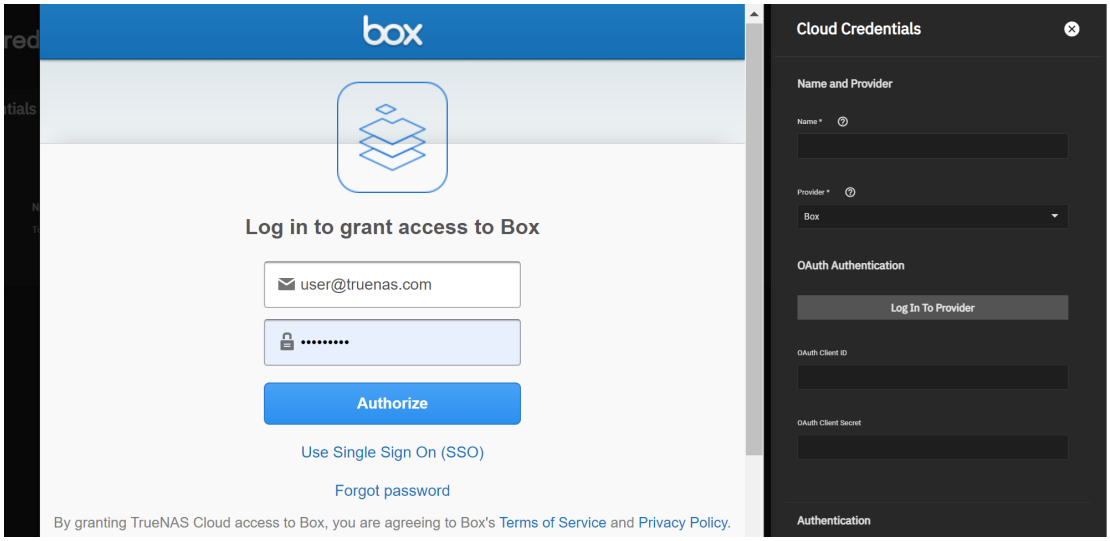
   a. Enter a region name in **Region Name**

   b. (Optional) Enter the URL in **Storage URL**.

   c. (Optional) Select service catalogue option from the **Endpoint Type** dropdown. Options are **Public**, **Internal** and **Admin**. **Public** is recommended.
6. Click **Verify Credentials**.
7. Click **Save**.

Using Automatic Authentication

Some providers can automatically populate the required authentication strings by logging in to the account. To automatically configure the credential, click **Login to Provider** and entering your account user name and password.



We recommend verifying the credential before saving it.

Related Content

- Adding Cloud Sync Tasks
- Backing Up Google Drive to TrueNAS SCALE
- Cloud Credentials Screens
- Cloud Sync Tasks
- Cloud Sync Tasks Screens

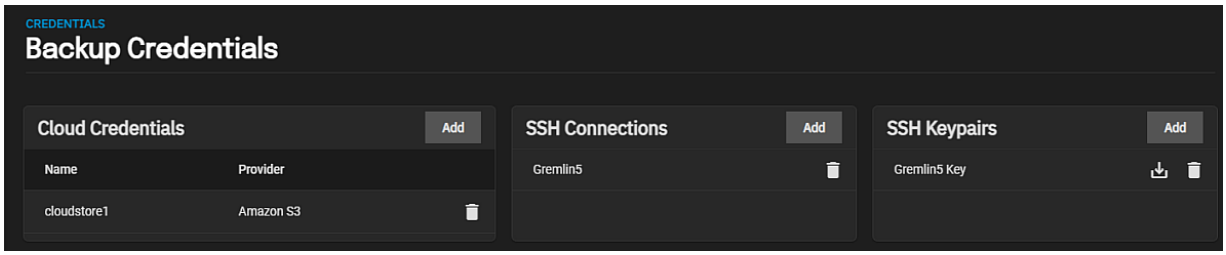
Related Backup Articles

- Adding Cloud Sync Tasks
- Adding Replication Tasks
- Backing Up Google Drive to TrueNAS SCALE
- Cloud Credentials Screens
- Managing the System Configuration
- Cloud Sync Tasks Screens
- Setting Up a Local Replication Task
- Setting Up Advanced Replication Tasks
- Backup Credentials

3.5.4.2 - Adding SSH Credentials

This article provides information on adding SSH connections, generating SSH keypairs, and adding the SSH public key to the root user.

The **SSH Connections** and **SSH Keypairs** widgets on the **Backup Credentials** screen display a list of SSH connections and keypairs configured on the system. Using these widgets, users can establish Secure Socket Shell (SSH) connections.



To begin setting up an SSH connection, go to **Credentials > Backup Credentials** and click the **Add** button on the **SSH Connections** widget.

Creating an SSH Connection

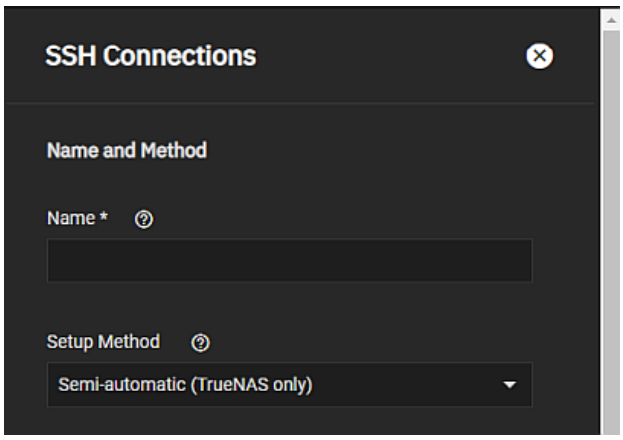
This procedure uses the semi-automatic setup method for creating an SSH connection with other TrueNAS or FreeNAS systems.

Click here for more information

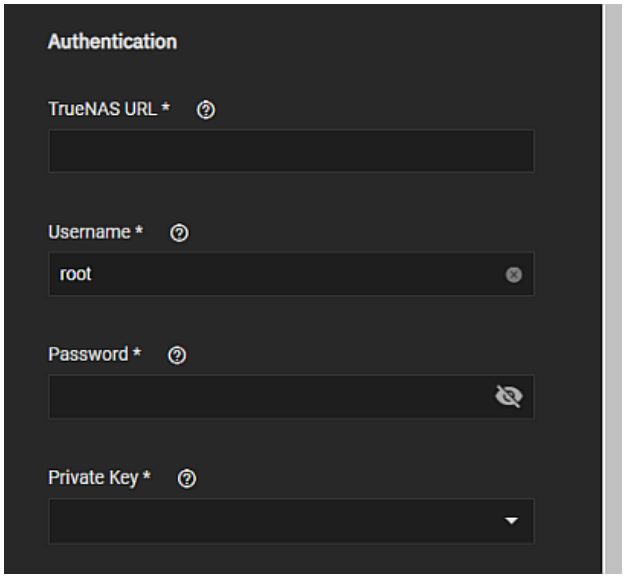
Semi-automatic simplifies setting up an SSH connection with another FreeNAS or TrueNAS system without logging in to that system to transfer SSH keys. This requires an SSH keypair on the local system and administrator account credentials for the remote TrueNAS. You must configure the remote system to allow root access with SSH. You can generate the keypair as part of the semiautomatic configuration or a manually created one using **SSH Keypairs**.

Using the **SSH Connections** configuration screen:

1. Enter a name and select the **Setup Method**. If establishing an SSH connection to another TrueNAS server use the default **Semi-automatic (TrueNAS only)** option. If connecting to a non-TrueNAS server select **Manual** from the dropdown list.



2. Enter the authentication settings.

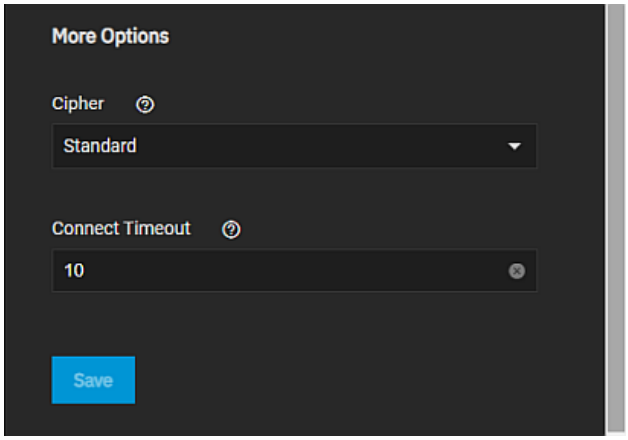


a. Enter a valid URL scheme for the remote TrueNAS URL in **TrueNAS URL**. This is a required field.

b. Enter a user name or leave **Username** set to the default **root** user and enter the user password **Password**.

c. Enter or import the private key from a previously created SSH keypair, or create a new one using the **SSH Keypair** widget.

3. (Optional) Select a security option from the **Cipher** dropdown list. Select **Standard** for the most secure option, but this has the greatest impact on connection speed. Select **Fast** for a less secure option than **Standard** but it can give reasonable transfer rates for devices with limited cryptographic speed. Select **Disabled** to remove all security and maximize connection speed, but only disable security when using this connection within a secure, trusted network.



4. (Optional) Enter the number of seconds you want to have SCALE wait for the remote TrueNAS/FreeNAS system to connect in **Connect Timeout**.

5. Click **Save**. Saving a new connection automatically opens a connection to the remote TrueNAS and exchanges SSH keys. The new SSH connection displays on the **SSH Connection** widget. To edit it, click on the name to open the **SSH Connections** configuration screen populated with the saved settings.

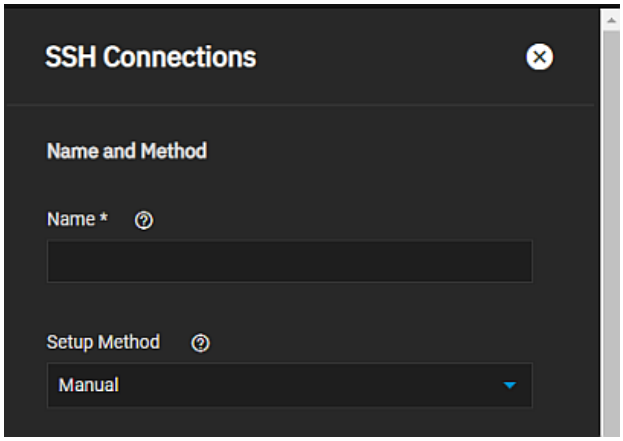
Manually Configuring an SSH Connection

This procedure provides instructions on setting up an SSH connection to a non-TruNAS or non-FreeNAS system. To manually set up an SSH connection, you must copy a public encryption key from the local system to the remote system. A manual setup allows a secure connection without a password prompt.

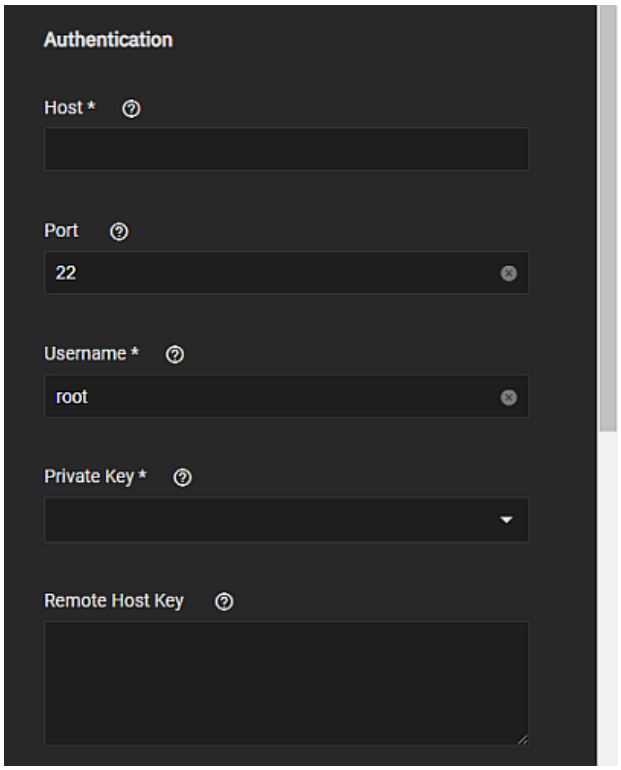
Manual

Using the **SSH Connections** configuration screen:

1. Enter a name and select **Manual** from the **Setup Method** dropdown list.



2. Enter the authentication settings.



a. Enter a host name or host IP address for the remote non-TruNAS/FreeNAS system as a valid URL. An IP address example is *https://10.231.3.76*. This is a required field.

b. Enter the port number of the remote system to use for the SSH connection.

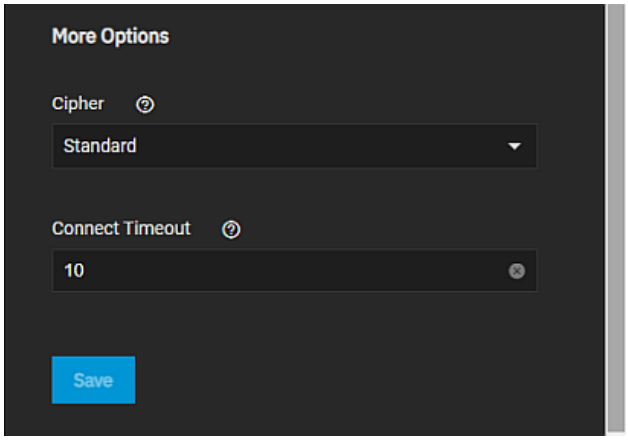
c. Enter a user name for logging into the remote system in **Username**.

c. Select the private key from the SSH keypair that you used to transfer the public key on the remote NAS from the **Private Key** dropdown.

d. Enter the remote system SSH key for this TrueNAS SCALE system in **Remote Host Key** to authenticate the connection.

e. Click **Discover Remote Host Key** after properly configuring all other fields to connect to the remote system and attempt to copy the key string to the related SCALE field.

3. (Optional) Select a security option from the **Cipher** dropdown list. Select **Standard** for the most secure option, but this has the greatest impact on connection speed. Select **Fast** for a less secure option than **Standard** but it can give reasonable transfer rates for devices with limited cryptographic speed. Select **Disabled** to remove all security in favor of maximizing connection speed, but only disable security when usisg this connection within a secure, trusted network.



4. (Optional) Enter the number of seconds you want to have SCALE wait for the remote TrueNAS/FreeNAS system to connect in **Connect Timeout**.
5. Click **Save**. Saving a new connection automatically opens a connection to the remote TrueNAS and exchanges SSH keys. The new SSH connection displays on the **SSH Connection** widget. To edit it, click on the name to open the **SSH Connections** configuration screen populated with the saved settings.

Adding a Public SSH Key to the TrueNAS Root Account

This procedure covers adding a public SSH key to the root user account on the TrueNAS SCALE system and generating a new SSH Keypair to add to the remote system (TrueNAS or other).

Click here for more information

1. Copy the SSH public key text or download it to a text file.

   Log into the TrueNAS system that generated the SSH keypair and go to **Credentials > Backup Credentials**.

   Click on the name of the keypair on the **SSH Keypairs** widget to open the keypair for the SSH connection.

   Copy the text of the public SSH key or download the public key as a text file.

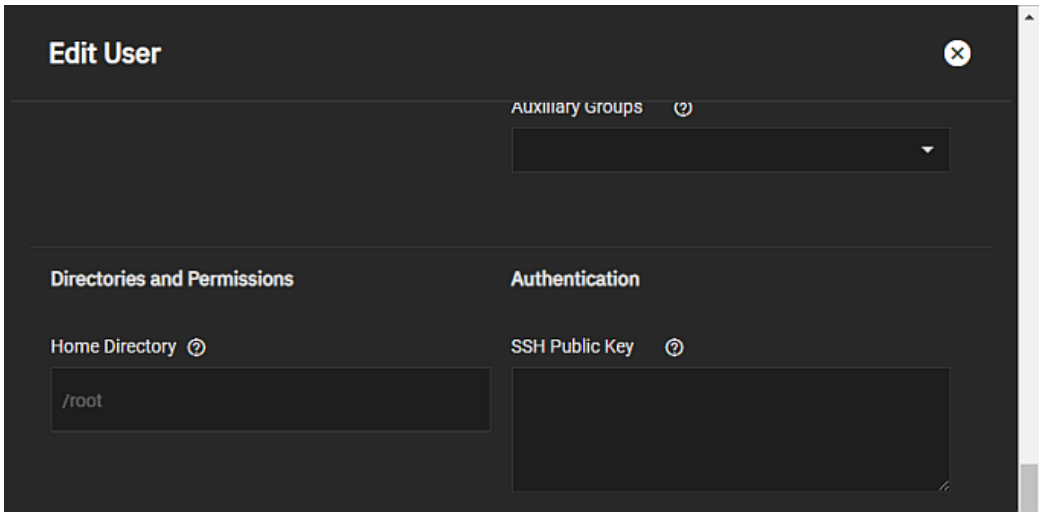
2. Add the public key to the **root** user account on the system where you want to register the public key.

   Log into the TrueNAS system that you want to register the public key on and go to **Credentials > Local Users**.

   Edit the **root** user account. Click on the icon and then click **Edit** to open the **Edit User** screen.

   Paste the SSH public key text into the **SSH Public Key** field on the **Edit User** configuration screen in the **Authentication** settings.

   Click **Save**.



3. Add a new public SSH key to the remote system.

   Generate a new SSH keypair in **Credentials > Backup Credentials**. Click **Add** on the **SSH Keypairs** widget and select **Generate New**.

   Copy or download the value for the new public key.

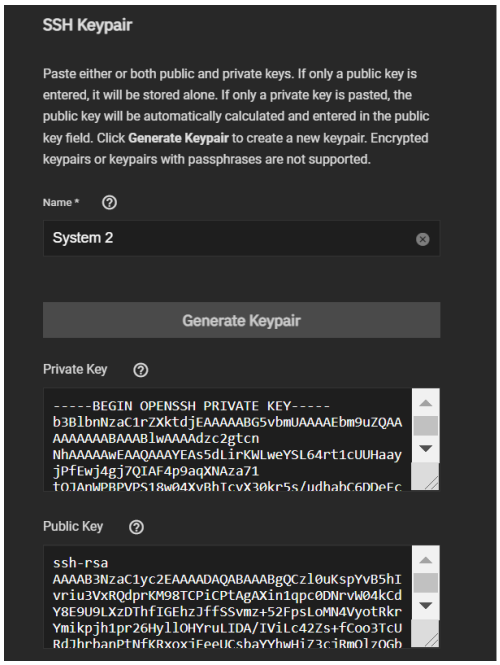
Add the public key to the remote NAS.

If the remote NAS is not a TrueNAS system, refer to the documentation for that system, and find their instructions on adding a public SSH key.

Generating SSH Keypairs

TrueNAS generates and stores RSA-encrypted SSH public and private keypairs on the **SSH Keypairs** widget found on the **Credentials > Backup Credentials** screen. Keypairs are generally used when configuring **SSH Connections** or SFTP **Cloud Credentials**. TrueNAS does not support encrypted keypairs or keypairs with passphrases.

TrueNAS automatically generates keypairs as needed when creating new **SSH Connections** or **Replication** tasks. To manually create a new keypair, click **Add** on the **SSH Keypairs** widget. Click **Generate New** on the **SSH Keypairs** screen. Give the new keypair a unique name and click **Save**. The keypair displays on the **SSH Keypairs** widget.



Use the download icon or click the ⋮ at the bottom of the **SSH Keypairs** configuration screen to download these strings as text files for later use.

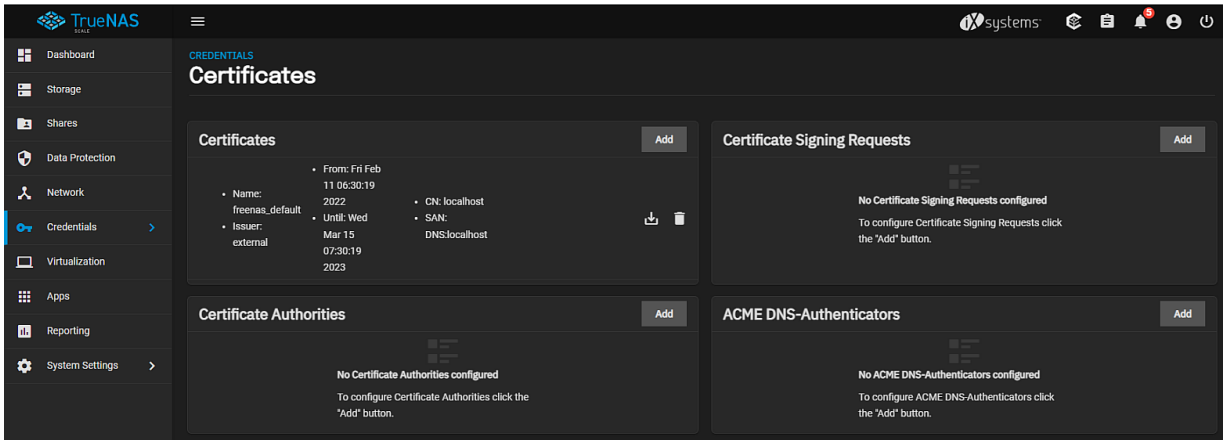
Related Content

- SSH Screens
- Configuring Rsync Tasks
- Rsync Tasks Screens
- Security Recommendations
- Configuring SSH Service
- SSH Service Screen
- Using 2FA (Two-Factor Authentication)

3.5.5 - Certificates

This article provides general information about articles that add or manage certificates, CSRs, CAs and ACME DNS-Authenticators in SCALE.

Use the **Credentials > Certificates** screen **Certificates**, **Certificate Signing Requests** (CSRs), **Certificate Authorities** (CA), and **ACME DNS-Authenticators** widgets to manage certificates, certificate signing requests (CSRs), certificate authorities (CA), and ACME DNS-authenticators.



Each TrueNAS comes equipped with an internal, self-signed certificate that enables encrypted access to the web interface, but users can make custom certificates for authentication and validation while sharing data.

Article Summaries

- Managing Certificates

  This article provides information on adding or managing SCALE certificates.

- Managing Certificate Authorities

  This article provides basic instructions on adding and managing SCALE certificate authorities (CAs).

- Managing Certificate Signing Requests

  This article provides basic instructions on adding and managing SCALE certificate signing requests (CSRs).

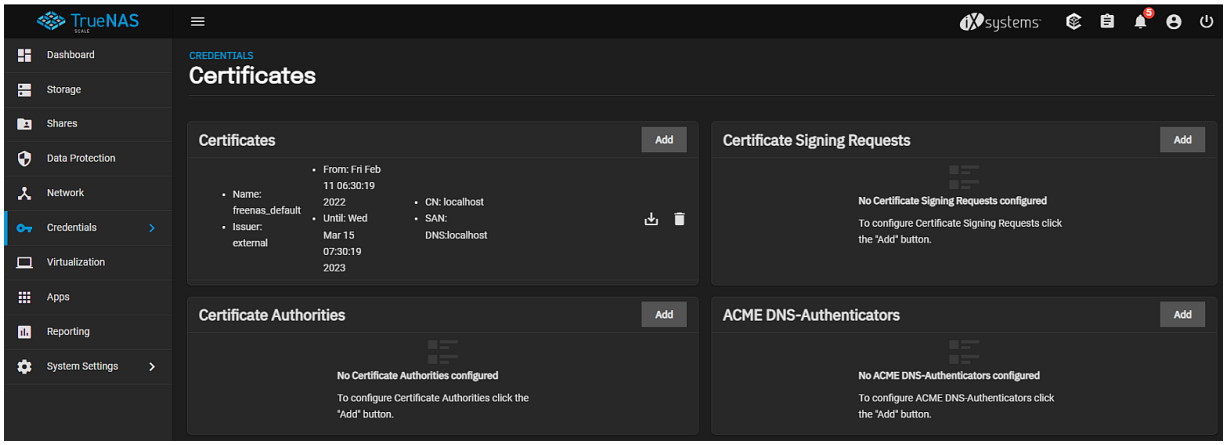
- Adding ACME DNS-Authenticators

  This article provides basic instructions on adding and managing SCALE ACME DNS-authenticators.

3.5.5.1 - Managing Certificates

This article provides information on adding or managing SCALE certificates.

The **Certificates** screen widgets display information for certificates, certificate signing requests (CSRs), certificate authorities(CAs), and ACME DNS-authenticators configured on the system, and provide the ability to add new ones. TrueNAS comes equipped with an internal, self-signed certificate that enables encrypted access to the web interface, but users can make custom certificates for authentication and validation while sharing data.



Adding Certificates

By default, TrueNAS comes equipped with an internal, self-signed certificate that enables encrypted access to the web interface, but users can import and create more certificates by clicking **Add** in the **Certificates** window.

To add a new certificate:

Click **Add** on the **Certificates** widget to open the **Add Certficates** wizard.

First, enter a name as certificate identifier and select the type. The **Identifier and Type** step lets users name the certificate and choose whether to use it for internal or local systems, or import an existing certificate.
Users can also select a predefined certificate extension from the **Profiles** dropdown list.

Next, specify the certificate options. Select the **Key Type** as this selection changes the settings displayed. The **Certificate Options** step provides options for choosing the signing certificate authority (CSR), the type of private key type to use (as well as the number of bits in the key used by the cryptographic algorithm), the cryptographic algorithm the certificate uses, and how many days the certificate authority lasts.

Now enter the certificate location and basic information. The **Certificate Subject** step lets users define the location, name, and email for the organization using the certificate.
Users can also enter the system fully-qualified hostname (FQDN) and any additional domains for multi-domain support.

Lastly, select any extension types you want to apply. Selecting **Extended Key** displays settings for **Key Usage** settings as well. Select any extra constraints you need for your scenario. The **Extra Constraints** step contains certificate extension options.

- **Basic Constraints** when enabled this limits the path length for a certificate chain.
- **Authority Key Identifier** when enabled provides a means of identifying the public key corresponding to the private key used to sign a certificate.
- **Key Usage** when enabled defines the purpose of the public key contained in a certificate.
- **Extended Key Usage** when enabled it further refines key usage extensions.

Review the certificate options. If you want to change something Click **Back** to reach the screen with the setting option you want to change, then click **Next** to advance to the **Confirm Options** step.

Click **Save** to add the certificate.

Importing a Certificate

To import a certificate, first select **Import Certificate** as the **Type** and name the certificate.

Next, if the CSR exists on your SCALE system, select **CSR exists on this system** and then select the CSR.

Copy/paste the certificate and private Keys into their fields, and enter and confirm the passphrase for the certificate if one exists.

Review the options, and then click **Save**.

Related Content

- Certificates Screens
- Certificates Authorities Screens
- Managing Certificate Authorities
- Certificate Signing Requests Screens
- Managing Certificate Signing Requests
- ACME DNS-Authenticators Screens
- Adding ACME DNS-Authenticators
- Certificates
- Certificates

3.5.5.2 - Managing Certificate Authorities

This article provides basic instructions on adding and managing SCALE certificate authorities (CAs).

The **Certificate Authorities** widget lets users set up a certificate authority (CA) that certifies the ownership of a public key by the named subject of the certificate.

To add a new CA:

First, add the name and select the type of CA. The **Identifier and Type** step lets users name the CA and choose whether to create a new CA or import an existing CA.
Users can also select a predefined certificate extension from the **Profiles** drop-down list.

Next, enter the certificate options. Select the key type. The **Key Type** selection changes the settings displayed. The **Certificate Options** step provides options for choosing what type of private key to use (as well as the number of bits in the key used by the cryptographic algorithm), the cryptographic algorithm the CA uses, and how many days the CA lasts.

Now enter the certificate subject information. The **Certificate Subject** step lets users define the location, name, and email for the organization using the certificate.
Users can also enter the system fully-qualified hostname (FQDN) and any additional domains for multi-domain support.

Lastly, enter any extra constraints you need for your scenario. The **Extra Constraints** step contains certificate extension options.

- **Basic Constraints** when enabled this limits the path length for a certificate chain.
- **Authority Key Identifier** when enable provides a means of identifying the public key corresponding to the private key used to sign a certificate.
- **Key Usage** when enabled defines the purpose of the public key contained in a certificate.
- **Extended Key Usage** when enabled it further refines key usage extensions.

Review the CA options. If you want to change something Click **Back** to reach the screen with the setting option you want to change, then click **Next** to advance to the **Confirm Options** step.

Click **Save** to add the CA.

Related Content

- Certificates Screens
- Managing Certificates
- Certificates Authorities Screens
- Certificate Signing Requests Screens
- Managing Certificate Signing Requests
- Adding ACME DNS-Authenticators

3.5.5.3 - Managing Certificate Signing Requests

This article provides basic instructions on adding and managing SCALE certificate signing requests (CSRs).

The **Certificate Signing Requests** widget allows users configure the message(s) the system sends to a registration authority of the public key infrastructure to apply for a digital identity certificate.

To add a new CSR:

First enter the name and select the CSR type. The **Identifier and Type** step lets users name the certificate signing request (CSR) and choose whether to create a new CSR or import an existing CSR.
Users can also select a predefined certificate extension from the **Profiles** drop-down list.

Next, select the certficate options for the CSR you selected. The **Certificate Options** step provides options for choosing what type of private key type to use, the number of bits in the key used by the cryptographic algorithm, and the cryptographic algorithm the CSR uses.

Now enter the information about the certificate. The **Certificate Subject** step lets users define the location, name, and email for the organization using the certificate.
Users can also enter the system fully-qualified hostname (FQDN) and any additional domains for multi-domain support.

Lastly, enter any extra constraints you need for your scenario. The **Extra Constraints** step contains certificate extension options.

- **Basic Constraints** when enabled this limits the path length for a certificate chain.
- **Authority Key Identifier** when enable provides a means of identifying the public key corresponding to the private key used to sign a certificate.
- **Key Usage** when enabled defines the purpose of the public key contained in a certificate.
- **Extended Key Usage** when enabled it further refines key usage extensions.

Review the certificate options. If you want to change something Click **Back** to reach the screen with the setting option you want to change, then click **Next** to advance to the **Confirm Options** step.

Click **Save** to add the CSR.

Related Content

- Certificates Screens
- Managing Certificates
- Certificates Authorities Screens
- Managing Certificate Authorities
- Certificate Signing Requests Screens
- Adding ACME DNS-Authenticators

3.5.5.4 - Adding ACME DNS-Authenticators

This article provides basic instructions on adding and managing SCALE ACME DNS-authenticators.

Automatic Certificate Management Environment (ACME) DNS authenticators allows users to automate certificate issuing and renewal. The user must verify ownership of the domain before certificate automation is allowed.

The system requires an ACME DNS Authenticator and CSR to configure ACME certificate automation.

To add an authenticator,

Click **Add** on the **ACME DNS-Authenticator** widget to open the **Add DNS Authenticator** screen.

Enter a name, and select the authenticator you want to configure. The selection changes the screen settings.

If you select **Cloudflare** as the authenticator, you must enter your Cloudflare account email address, API key, and API token.

If you select **Route53** as the authenticator, you must enter you Route53 Access key ID and secret access key.

Click **Save** to add the authenticator.

Related Content

- ACME DNS-Authenticators Screens

3.5.6 - Using 2FA (Two-Factor Authentication)

This article provides information on SCALE two-factor authentication, setting it up and logging in with it enabled.

Two-factor authentication (2FA) is great for increasing security.

TrueNAS offers 2FA to ensure that entities cannot use a compromised administrator root password to access the administrator interface.

About SCALE 2FA

To use 2FA, you need a mobile device with the current time and date, and that has Google Authenticator installed. Other authenticator applications can be used, but you will need to confirm the settings and QR codes generated in TrueNAS are compatible with your particular app before permanently activating 2FA.

> Two-factor authentication is time-based and requires a correct system time setting. Make sure Network Time Protocol (NTP) is functional before enabling is strongly recommended!

What is 2FA and why should I enable it?
2FA adds an extra layer of security to your system to prevent someone from logging in, even if they have your password. 2FA requires you to verify your identity using a randomized 6-digit code that regenerates every 30 seconds (unless modified) to use when you log in.

Benefits of 2FA

Unauthorized users cannot log in since they do not have the randomized 6-digit code.

Authorized employees can securely access systems from any device or location without jeopardizing sensitive information.

Internet access on the TrueNAS system is not required to use 2FA.

Drawbacks of 2FA

2FA requires an app to generate the 2FA code.

If the 2FA code is not working or users cannot get it, the system is inaccessible through the UI and SSH (if enabled). You can bypass or unlock 2FA using the CLI.

Enabling 2FA

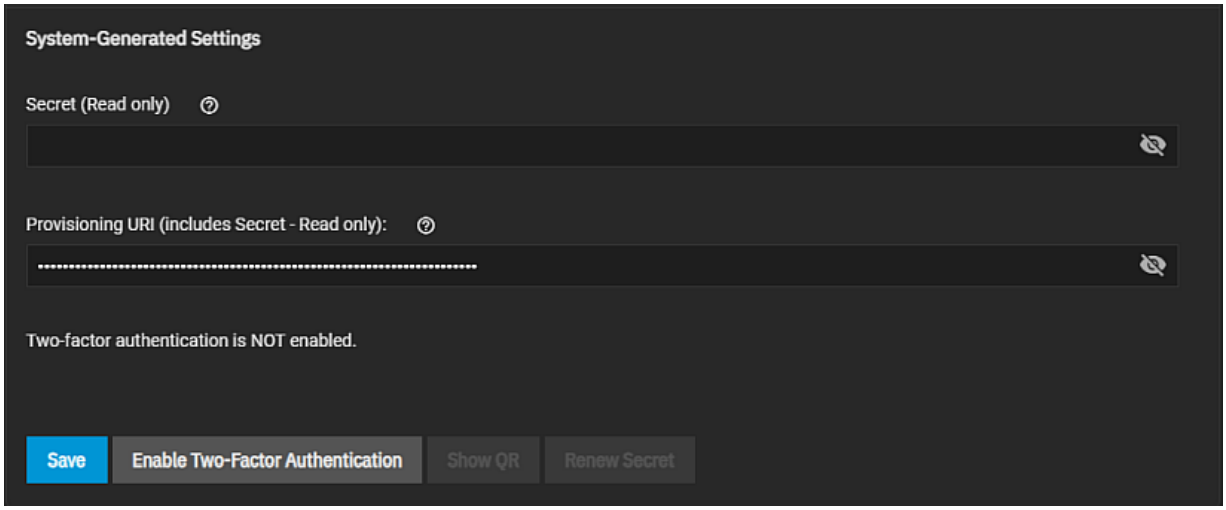
Video Tutorial

This short video demonstrates adding 2FA.

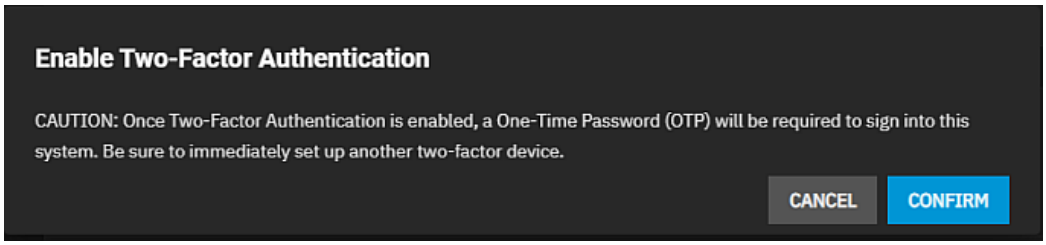
> Set up a second 2FA device as a backup before proceeding.

Before you begin, download Google Authenticator to your mobile device.

1 Go to **Credentials > 2FA** to open the **Two-Factor Auth** screen and scroll down to the bottom.



2 Click **Enable Two Factor Authentication**. The **Enable Two-Factor Authentication** confirmation dialog opens. Click **Confirm**.



Disable Two-Factor Authentication displays next to **Save** to turn 2FA off.

3 Click **Show QR**. A QR code dialog opens.

4 Start Google Authenticator on the mobile device and scan the QR code. After scanning the code click **Close** to close the dialog on the **Two-Factor Auth** screen.

Disabling or Bypassing 2FA

Go to **Credentials > 2FA** to open the **Two-Factor Auth** screen and scroll down to the bottom. Click **Disable Two-Factor Authentication**.

> If the device with the 2FA app is not available, you can use the system CLI to bypass 2FA with administrative IPMI or by physically accessing the system.
>
> To unlock 2FA in the CLI, enter: `midclt call auth.twofactor.update '{ "enabled":false }'`

Reactivating 2FA

After disabling 2FA, if you want to enable it again at some point in the future, go to **Credentials > 2FA** to open the **Two-Factor Auth** screen and scroll down to the bottom. Click **Enable Two-Factor Authentication**.

To change the system-generated **Secret** and **Provisioning URI** values, click **Renew Secret**. If you want to save these values in a text file, click the icon in the field to display the alphanumeric string and either enter or copy/paste the value into a text file. Keep all login codes in protected and backed up location.

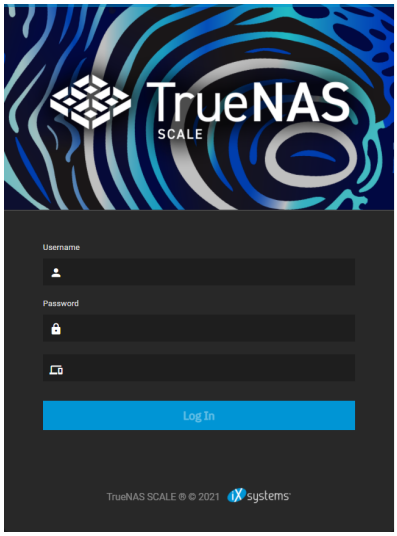
Using 2FA to Log in to TrueNAS

Enabling 2FA changes the login process for both the TrueNAS web interface and SSH logins.

Logging In Using the Web Interface

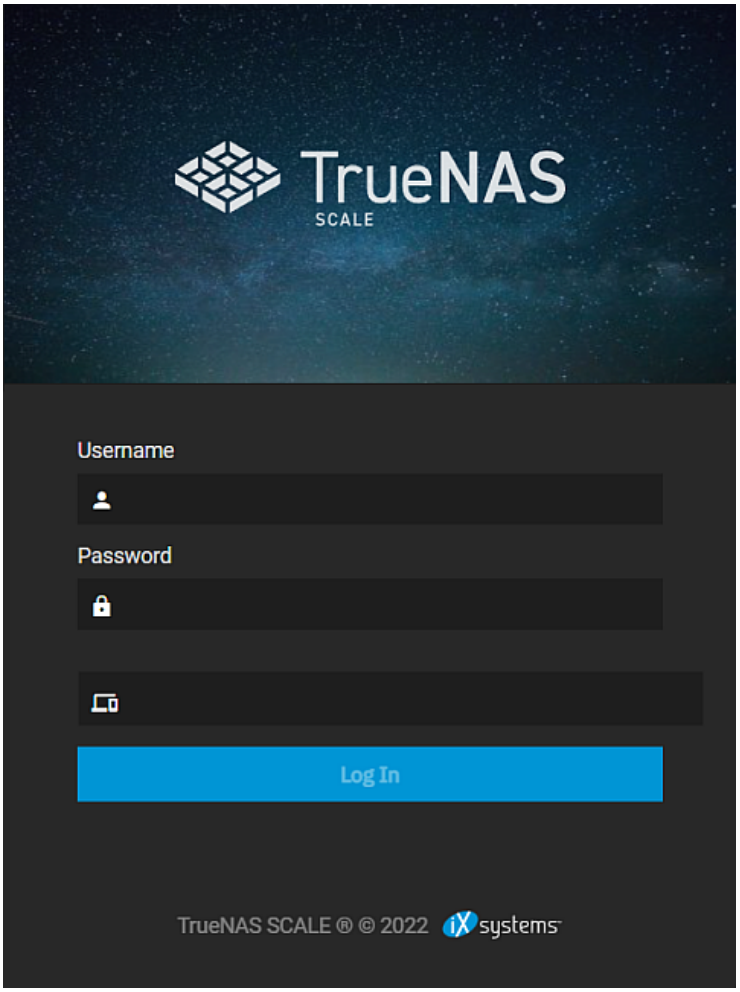
The login screen adds another field for the randomized authenticator code. If this field is not immediately visible, try refreshing the browser.

Enter the code from the mobile device (without the space) in the login window and use the root User name and password.



Logging In Using SSH

1. Confirm that you set **Enable Two-Factor Auth for SSH** in **Credentials > 2FA**.
2. Go to **System Settings > Services** and edit the **SSH** service.
   a. Set **Log in as Root with Password**, then click **Save**.
   b. Click the **SSH** toggle and wait for the service status to show that it is running.
3. Open the Google Authentication app on your mobile device.
4. Open a terminal and SSH into the system using its host name or IP address, the root account user name and password, and the 2FA code.



Related Content

- Two-Factor Auth Screen

3.6 - Virtualization Tutorials

The Virtualization section allows users to set up Virtual Machines (VMs) to run alongside TrueNAS. Delegating processes to VMs reduces the load on the physical system, which means users can utilize additional hardware resources. Users can customize six different segments of a VM when creating one in TrueNAS SCALE.

What system resources do VMs require?

TrueNAS assigns a portion of system RAM and a new zvol to each VM. While a VM is running, these resources are not available to the host computer or other VMs.

TrueNAS VMs use the KVM virtual machine software. This type of virtualization requires an x86 machine running a recent Linux kernel on an Intel processor with VT (virtualization technology) extensions or an AMD processor with SVM extensions (also called AMD-V). Users cannot create VMs unless the host system supports these features.

To verify that you have Intel VT or AMD-V, open the **Shell** and run `egrep '^flags.*(vmx|svm)' /proc/cpuinfo`. If device information appears, your system has VT. You can also check the processor model name (in `/proc/cpuinfo`) on the vendor's website.

Ready to get started? Choose a topic or article from the left-side **Navigation** pane. Click the **<** symbol to expand the menu to show the topics under this section.

Article Summaries

- Adding and Managing VMs

  This article provides instructions on how to add or manage a virtual machine and installing an operating system in the VM.

- Accessing NAS From a VM

  This article provides instructions on how to create a bridge interface for the VM and provides a Linux and Windows example.

3.6.1 - Adding and Managing VMs

This article provides instructions on how to add or manage a virtual machine and installing an operating system in the VM.

A Virtual Machine (VM) is an environment on a host computer that you can use as if it were a separate, physical computer. Users can use VMs to run multiple operating systems simultaneously on a single computer. Operating systems running inside a VM see emulated virtual hardware rather than the host computer physical hardware. VMs provide more isolation than Jails but also consumes more system resources.

What system resources do VMs require?

TrueNAS assigns a portion of system RAM and a new zvol to each VM. While a VM is running, these resources are not available to the host computer or other VMs.

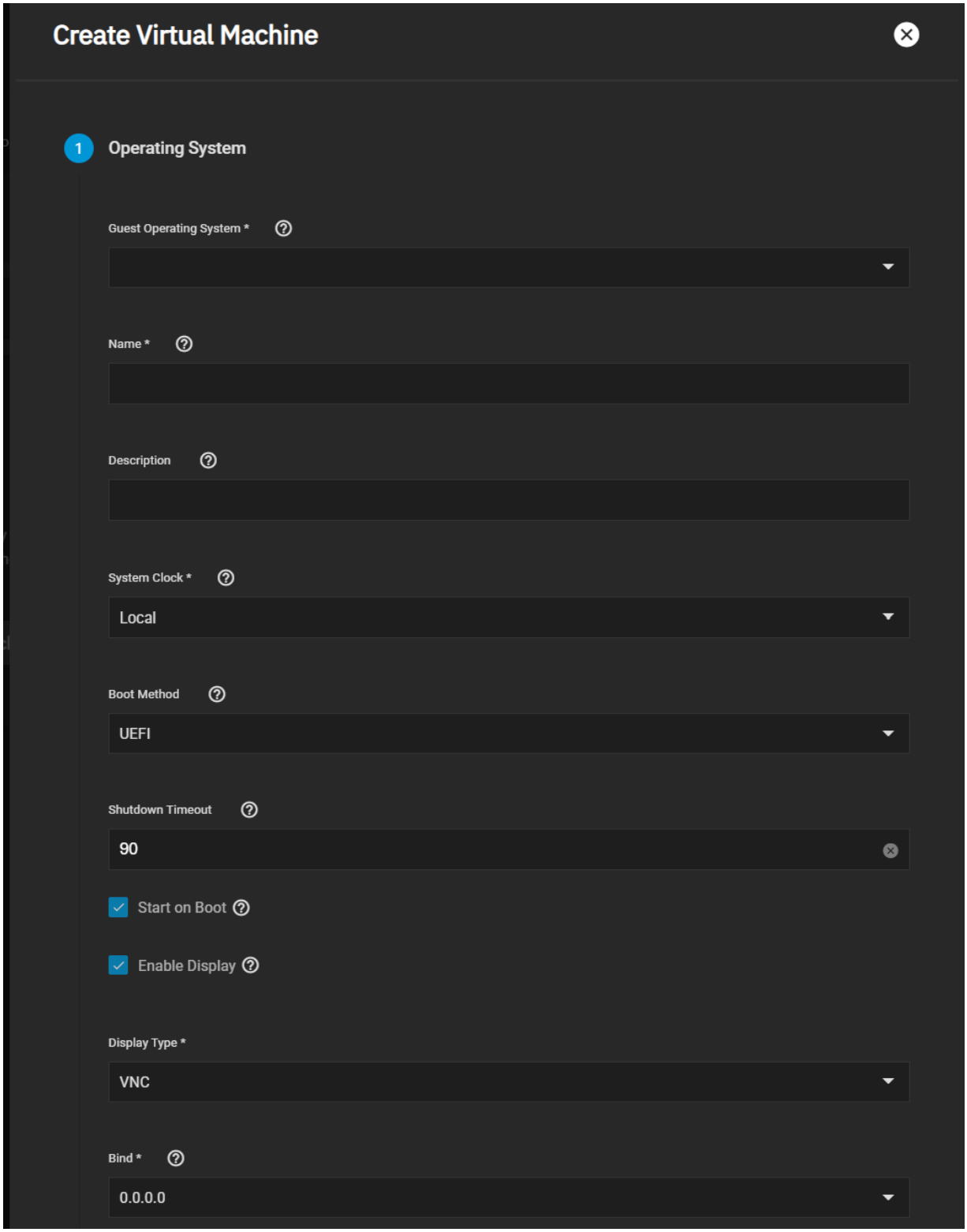
TrueNAS VMs use the KVM virtual machine software. This type of virtualization requires an x86 machine running a recent Linux kernel on an Intel processor with VT (virtualization technology) extensions or an AMD processor with SVM extensions (also called AMD-V). Users cannot create VMs unless the host system supports these features.

To verify that you have Intel VT or AMD-V, open the **Shell** and run `egrep '^flags.*(vmx|svm)' /proc/cpuinfo`. If device information appears, your system has VT. You can also check the processor model name (in `/proc/cpuinfo`) on the vendor's website.

Creating a Virtual Machine

Before creating a virtual machine, you need an installer .iso or image file for the OS you intend to install, and a storage pool available for both the virtual disk and OS install file.

To create a new VM, go to **Virtualization** and click **Add** or **Add Virtual Machines** if you have not yet added a virtual machine to your system. Configure each category of the VM according to your specifications, starting with the **Operating System**.



For more information see Virtualization Screens for more information on virtual machine screen settings.

Additional notes:

Compare the recommended specifications for your guest operating system with the available host system resources when allocating virtual CPUs, cores, threads, and memory size.

Do not allocate too much memory to a VM. Activating a VM with all available memory allocated to it can slow the host system or prevent other VMs from starting.

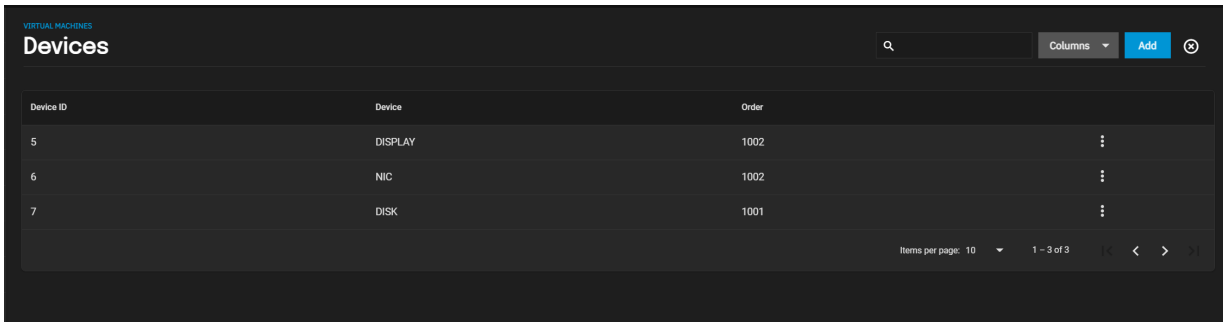
We recommend using **AHCI** as the **Disk Type** for Windows VMs.

The **VirtIO** network interface requires a guest OS that supports VirtIO paravirtualized network drivers.

> iXsystems does not have a list of approved GPUs at this time but does have drivers and basic support for the list of nvidia Supported Products.

Adding and Removing Devices

After creating the VM, add and remove virtual devices by expanding the VM entry on the **Virtual Machines** screen and clicking **Devices**.

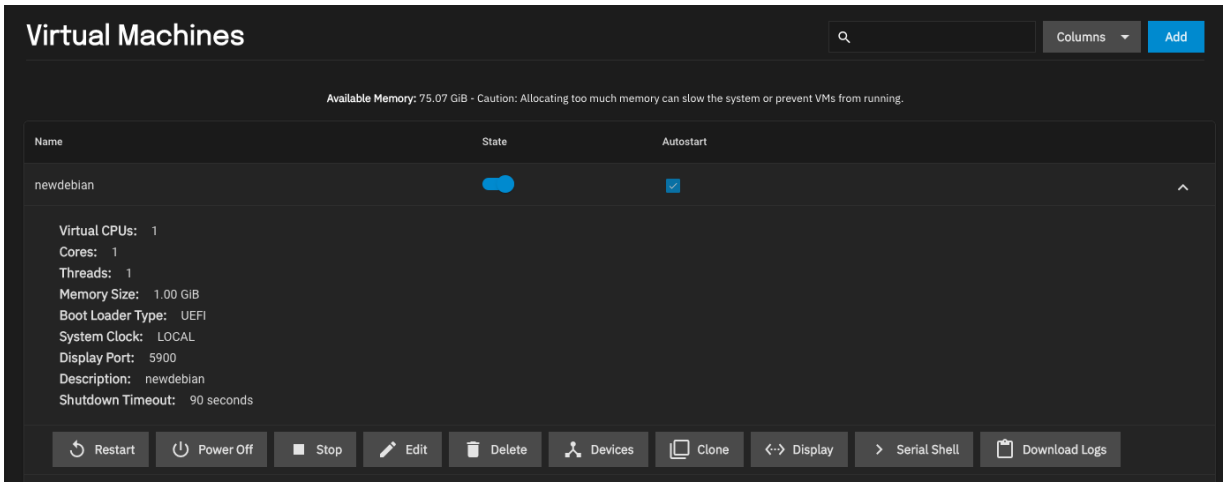


Device notes:

- A virtual machine attempts to boot from devices according to the **Device Order**, starting with **1000**, then ascending.
- A **CD-ROM** device allow booting a VM from a CD-ROM image like an installation CD. The CD image must be available in the system storage.

Managing a Virtual Machine

After creating the VM and configuring devices for it, manage the VM by expanding the entry on the **Virtual Machines** screen.



An active VM displays options for **Display** and **Serial Shell** connections.

If the display connection screen appears distorted, try adjusting the display device resolution.

Use the **State** toggle or click **Stop** to follow a standard procedure to do a clean shutdown of the running VM. Click **Power Off** to halt and deactivate the VM, which is similar to unplugging a computer.

> If the VM you created has no Guest OS installed, The VM **State** toggle and **Stop** button might not function as expected. The **State** toggle and **Stop** button send an ACPI power down command to the VM operating system, but since an OS is not installed, these commands time out. Use the **Power Off** button instead.

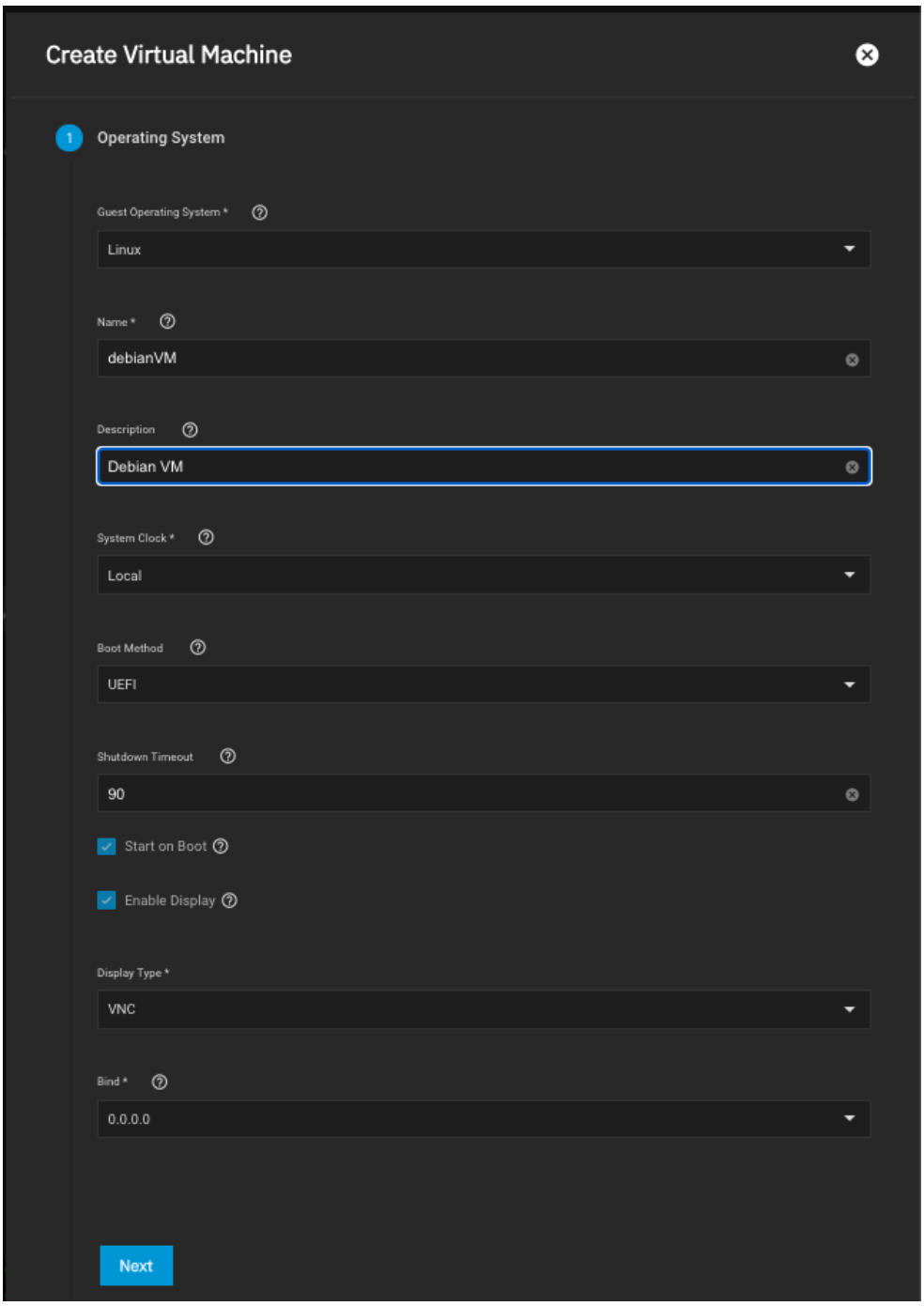
Installing an OS

When the VM is configured in TrueNAS and has an OS .iso, file attached, you can start the VM and begin installing the operating system.

> Some operating systems can require specific settings to function properly in a virtual machine. For example, vanilla Debian can require advanced partitioning when installing the OS. Refer to the documentation for your chosen operating system for tips and configuration instructions.

Here is an example of installing a Debian OS in a TrueNAS VM. The Debian .iso is uploaded to the TrueNAS system and attached to the VM as a CD-ROM device.

1. Click on the **Virtualization** menu then click **ADD** to start the VM creation process using the wizard.



VM Values Entered for the Debian Example

Operating System:

- Guest Operating System: Linux
- Name: debianVM
- Description: Debian VM

CPU and Memory:

- Change the memory size to 1024 MiB.

Disks:

- Select **Create new disk image**.
- Select the Zvol Location.
- Change the size to 30 GiB.

Network Interface:

- Attach NIC: Select the physical interface to associate with the VM.

Installation Media:

- In this case the installation ISO is uploaded to `/mnt/tank2/isostorage/`. Click on the installation ISO, *debian-11.0.0-amd64-netinst.iso*.
- If the ISO is or was not uploaded, you need to set **Upload an installer image file**. Select a dataset to store the ISO, click **Choose file**, then click **Upload**. Wait for the upload to complete (this can take some time).

GPU:

- Leave the default values.

Confirm Options

- Verify the information is correct and then click **Save**.

2. After the VM is created, start it by expanding the VM entry (select the down-pointing arrow to the right of the VM name) and click **Start**.

3. Click **Display** to open a virtual monitor to the VM and see the Debian Graphical Installation screens.

Debian Install Example

Debian Graphical Install

- Press `Return` to start the Debian Graphical Install.
- Language: English
- Location: United States
- Keymap: American English

Installation begins

- Continue if the network configuration fails.
- Do not configure the network at this time.
- Enter a name in **Hostname**.
- Enter the root password and re-enter the root password.
- Enter a name in **New User**.
- Select the username for your account (it should already be filled in).
- Enter and re-enter the password for the user account.
- Choose the time zone, *Eastern* in this case.

Disk detection should begin

- Partition disks: select **Guided - use entire disk**.
- Select the available disk.
- Select **All files in one partition** (recommended for new users).
- Select **Finish partitioning and write changes to disk**.
- Select **Yes** to **Write the changes to disks?**.

Installing the base system

- Select **No** to the question **Scan extra installation media**.
- Select **Yes** when asked **Continue without a network mirror**.

Installing software

- Select **No** when asked **Participate in the package usage survey**.
- Select **Standard** system utilities.
- Click **Continue** when the installation finishes.

After the Debian installation finishes, close the display window.

4. Remove the device. In the expanded section for the VM, click **Power Off** to stop the new VM.

   a. Click **Devices**.

   b. Remove the CD-ROM from the devices by clicking the ⋮ and selecting **Delete**. Click **Delete Device**.

5. Return to the **Virtual Machines** screen and expand the new VM again.

6. Click **Start**.

7. Click **Display**.

What if the grub file does not run after starting the VM?

The grub file does not run when you start the VM, you can do this manually after each start. At the shell prompt:

1. Type `FS0: Return`.
2. Type `cd EFI Return`.
3. Type `cd Debian Return`.
4. Type `grubx64.efi Return`.

To ensure it starts automatically, you create the startup.nsh file at the root directory on the vm. To create the file:

1. Go to the **Shell**.
2. At the shell prompt type `edit startup.nsh`.
3. In the editor type:

- Type `FS0: Return`.
- Type `cd EFI Return`.
- Type `cd Debian Return`.
- Type `grubx64.efi Return`.
- Use the `Control+s` keys (Command+s for Mac OS) then `Return`.
- Use the `Control+q` keys to quit.

4. Close the display window
5. To test if it now boots up on startup:
    - Power off the VM.
    - Click **Start**.
    - Click **Display**.
    - Log into your Debian VM.

Related Content

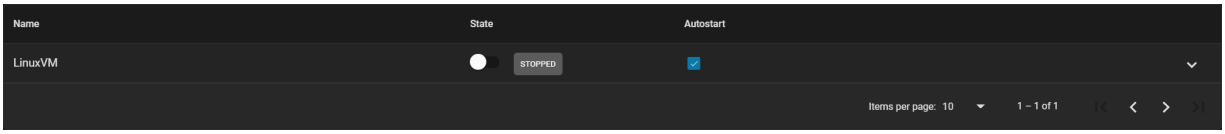
- Installing SCALE
- Accessing NAS From a VM
- Virtualization Screens

3.6.2 - Accessing NAS From a VM

This article provides instructions on how to create a bridge interface for the VM and provides a Linux and Windows example.

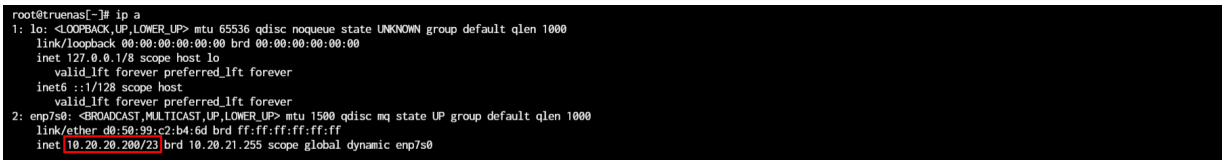
If you want to access your TrueNAS SCALE directories from a VM, you must create a bridge interface for the VM to use.

Go to **Virtualization**, find the VM you want to use to access TrueNAS storage, and toggle it off.

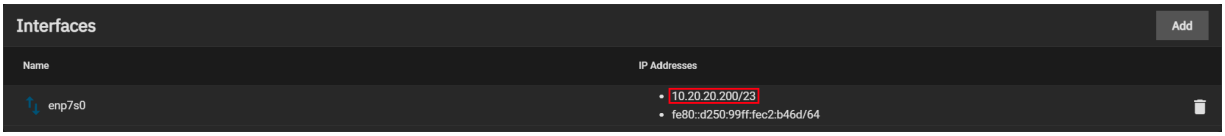


Go to **Network** and find the active interface you used as the VM parent interface. Note the interface IP Address and subnet mask.

> You can also get the IP address and subnet mask by going to **Shell** and entering `ip a`.

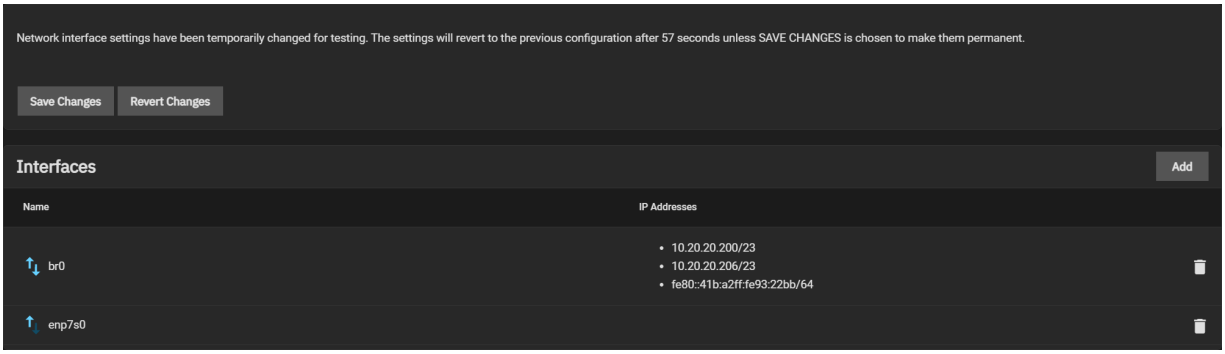


Click the interface. If selected, clear the **DHCP** checkbox, then click **Apply**.



Click **Add** in the **Interfaces** widget. Select **Bridge** for the **Type** and give it a name (must be in *brX* format). If selected, clear the **DHCP** checkbox, then select the active interface on the **Bridge Members** dropdown list. Click **Add** under **IP Addresses** and enter the active interface IP and subnet mask.

Click **Apply**, then click **Test Changes**. Once TrueNAS finishes testing the interface, click **Save Changes**.



Go to **Virtualization**, expand the VM you want to use to access TrueNAS storage, and click **Devices**. Click ⋮ in the **NIC** row and select **Edit**. Select the new bridge interface from the **Nic to attach:** dropdown list, then click **Save**.

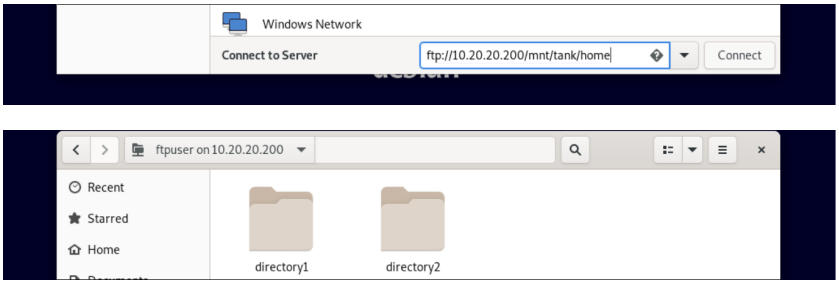
You can now access your TrueNAS storage from the VM. You might have to set up shares or users with home directories to access certain files.

Examples

Linux Example

Linux VMs can access TrueNAS storage using FTP, SMB, and NFS.

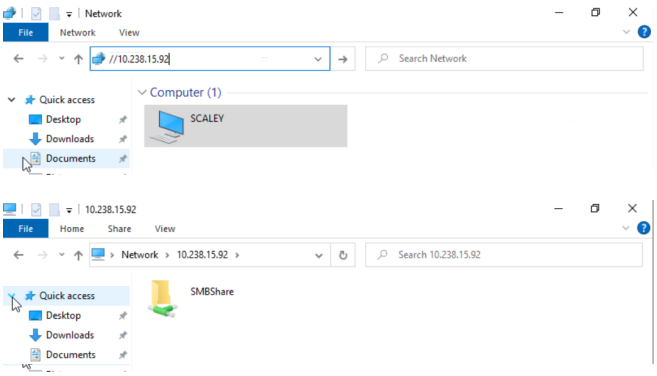
In the example below, the Linux VM is using FTP to access a home directory for a user on TrueNAS.



Windows Example

Windows VMs can access TrueNAS storage using FTP and SMB.

In the example below, the Windows VM accessing an SMB share on TrueNAS.



Related Content

- Adding and Managing VMs
- Installing SCALE
- Virtualization Screens

3.7 - Apps

Article Summaries

- Using Apps

  This article provides information on deploying official apps in TrueNAS SCALE.

- Using SCALE Catalogs

  This article provides basic information on adding or managing application catalogs in SCALE.

- Using Docker Image

  This article provides information on using the Docker image wizard to configure third-party applications in TrueNAS SCALE.

- Installing Nextcloud on SCALE

  This article provides instructions for a basic Nextcloud installation on TrueNAS SCALE.

- Adding NextCloud for Media Previews

  This article provides instructions to configure TrueNAS SCALE and install NextCloud to support hosting a wider variety of media file previews such as HEIC, Mp4 and MOV files.

- Configuring the Chia App

  This article provides basic installation instruction for the Chia application using both the TrueNAS webUI and CLI commands.

- Collabora App

  This article provides basic configuration instructions for adding the Collabora app using the TrueNAS webUI.

- MinIO Clusters

  This article provides information on configuring MinIO using the Docker image or the official application widget for MinIO.

  - Updating MinIO from 1.6.58

    This article provides information on updating MinIO from 1.6.58 to newer versions.

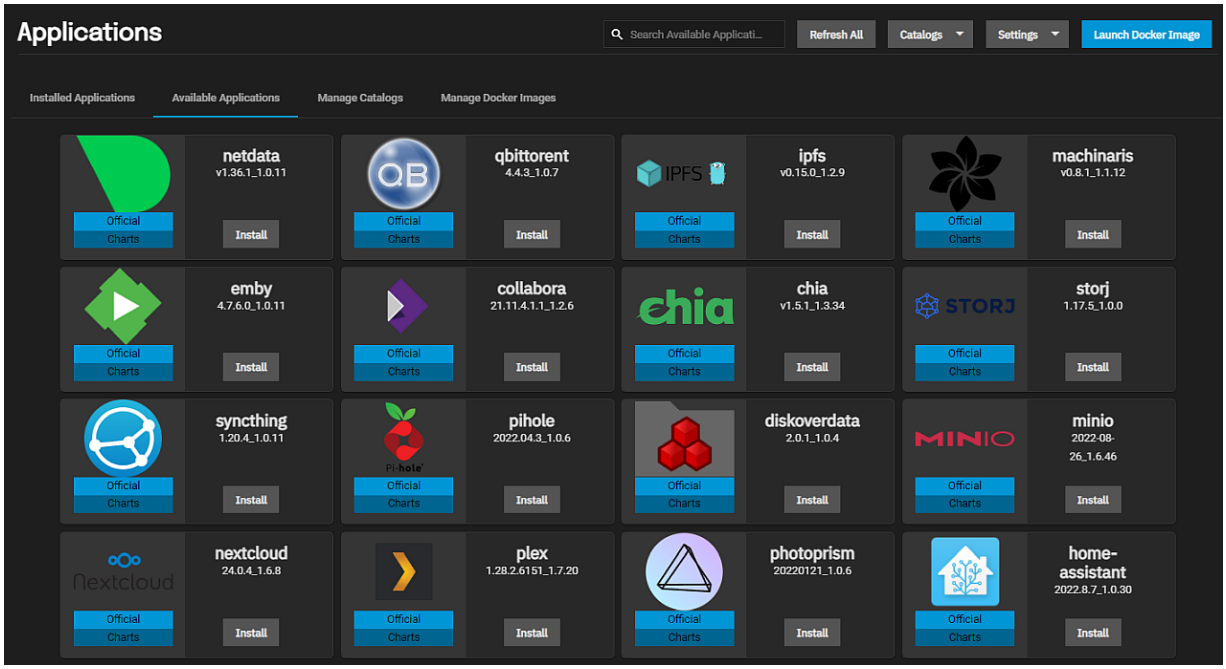
- Adding Pi-Hole Using Docker Image

  This article provides information on using the Docker image wizard to configure third-party applications like Pi-Hole in TrueNAS SCALE.

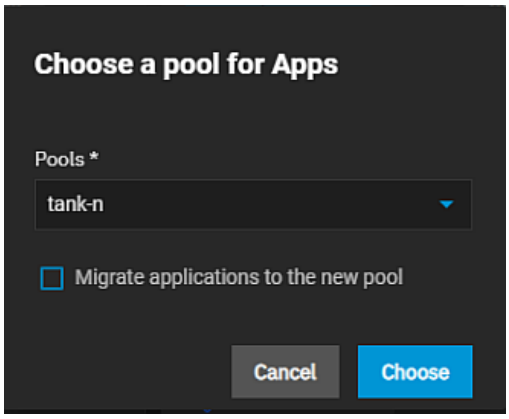
3.7.1 - Using Apps

This article provides information on deploying official apps in TrueNAS SCALE.

Both pre-built official containers and custom application containers can be deployed using the **Applications** page in the SCALE web interface.

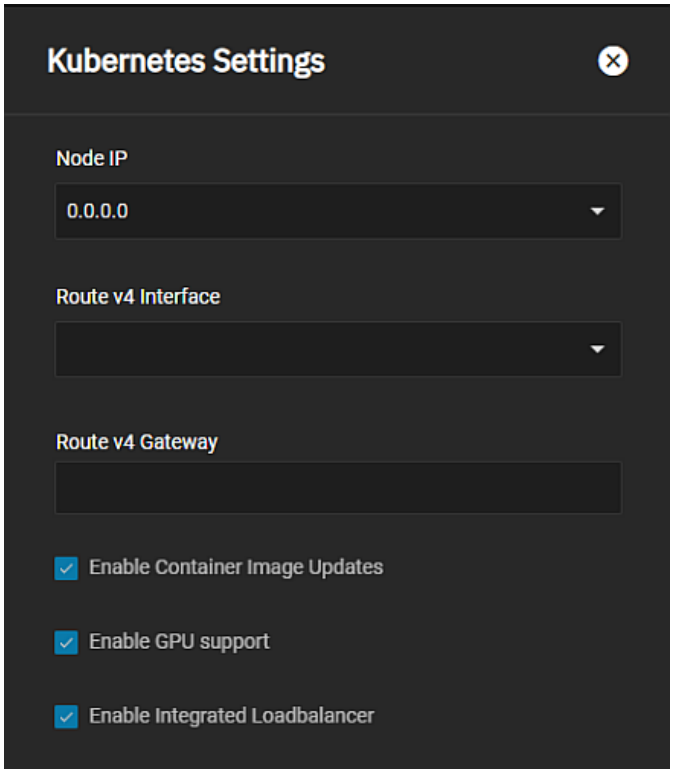


The UI asks to use a storage pool for applications.



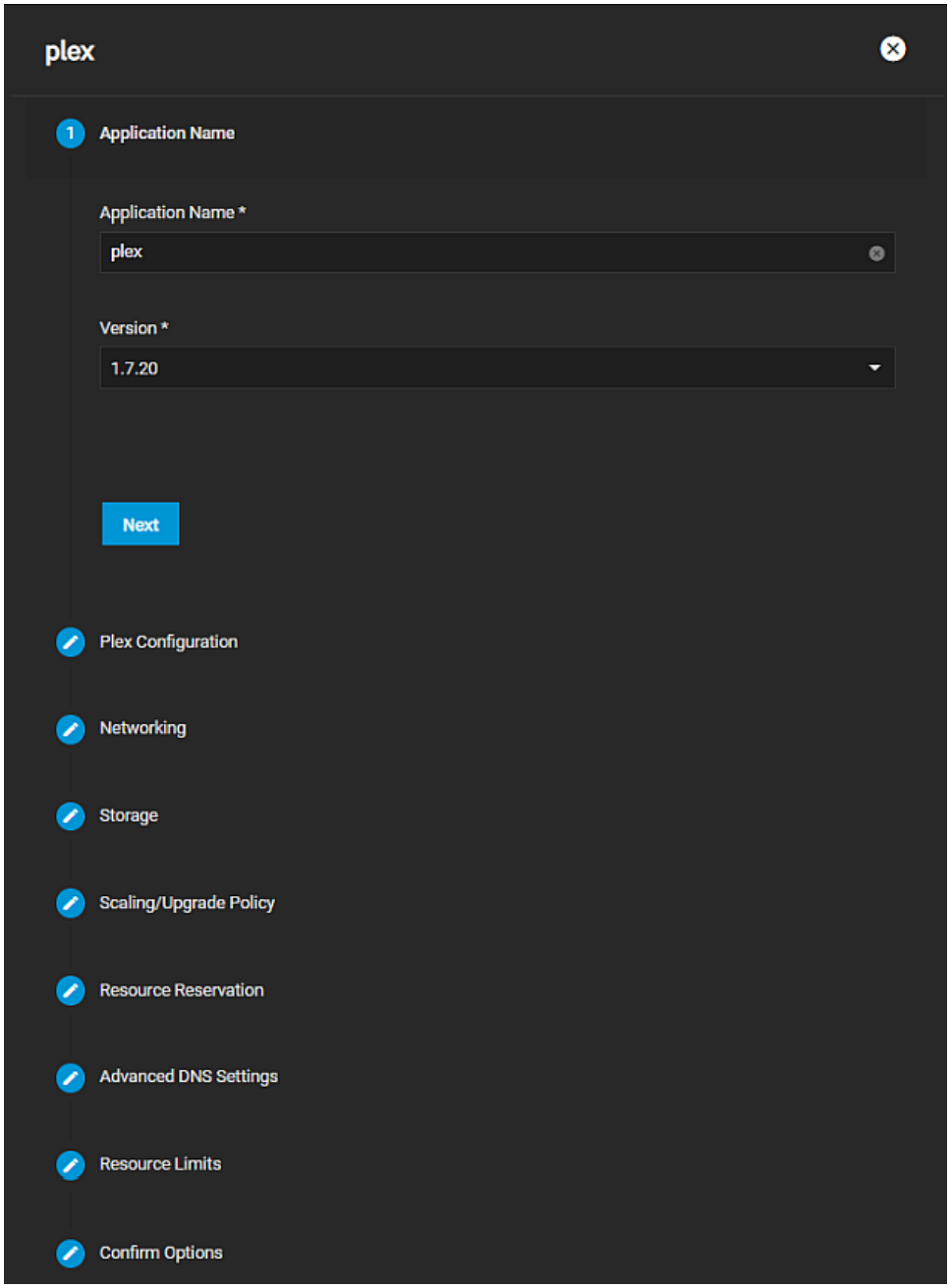
We recommend users keep the container use case in mind when choosing a pool. Select a pool that has enough space for all the application containers you intend to use. TrueNAS creates an *ix-applications* dataset on the chosen pool and uses it to store all container-related data.

You can find additional options for configuring general network interfaces and IP addresses for application containers in **Apps > Settings > Advanced Settings**.

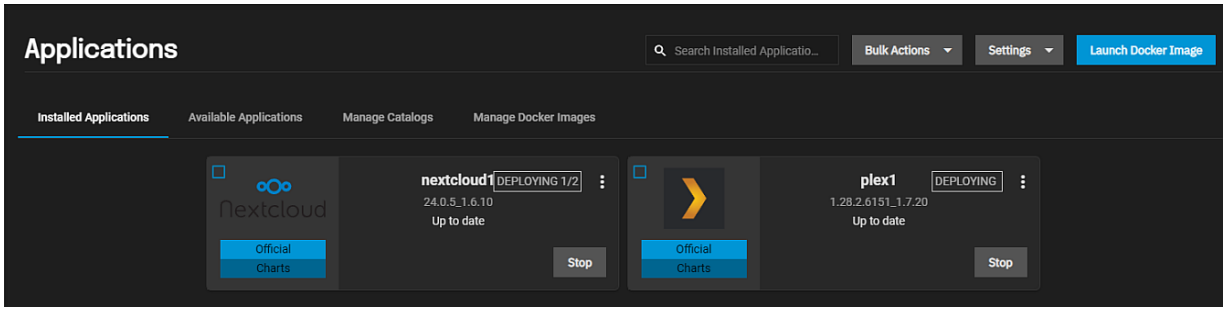


Official Applications

Official containers are pre-configured to only require a name during deployment.



A button to open the application web interface displays when the container is deployed and active.



Users can adjust the container settings by editing a deployed official container. Saving any changes redeploys the container.

Custom Applications

To deploy a custom application container in the Scale web interface, go to **Apps** and click **Launch Docker Image** for more on the Docker image wizard screens and settings..

Related Content

- Applications Screens
- Updating MinIO from 1.6.58
- Using SCALE Catalogs
- Launch Docker Image Screens
- Using Docker Image
- Adding NextCloud for Media Previews
- Configuring the Chia App
- Collabora App
- MinIO Clusters

3.7.2 - Using SCALE Catalogs

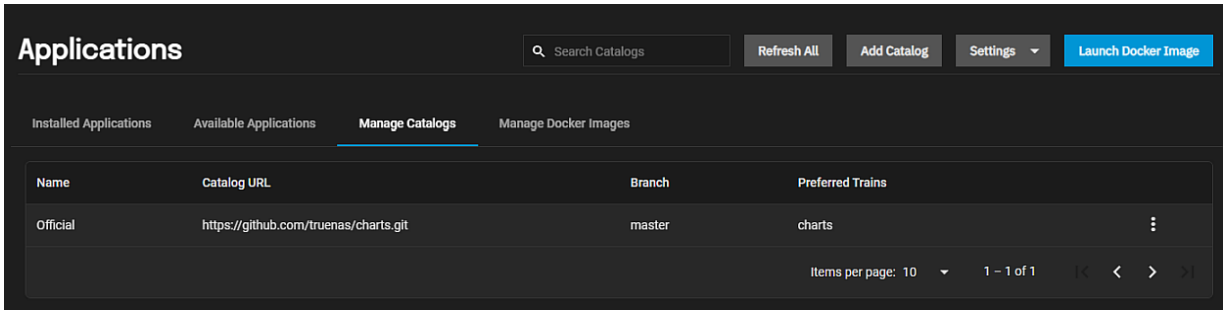
This article provides basic information on adding or managing application catalogs in SCALE.

TrueNAS SCALE comes with a pre-built official catalog of iXsystems-approved Docker apps that includes Plex, MinIO, Nextcloud, Chia, and IPFS.

Users can also configure custom apps catalogs, although iXsystems does not directly support any non-official apps in a custom catalog.

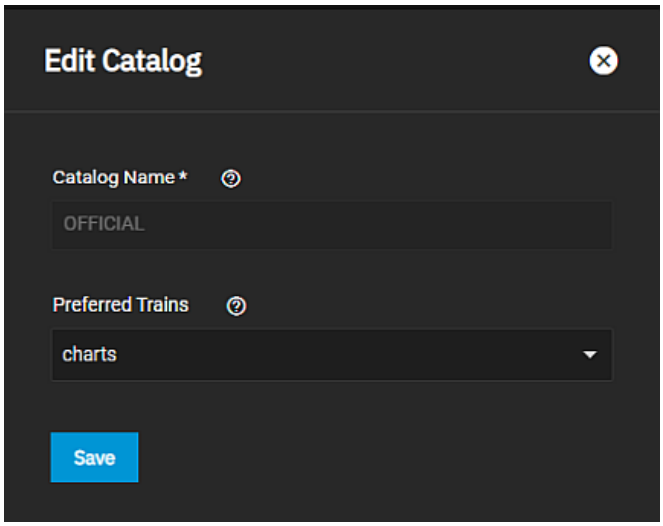
Managing Catalogs

To manage and add catalogs, click on the **Manage Catalogs** tab on the **Applications** screen.



Users can edit, refresh, delete, and view the summary of a catalog by clicking the ⋮ button next to the intended catalog.

Edit opens the **Edit Catalog** screen where users can change the name TrueNAS uses to look up the catalog or change the trains from which the UI should retrieve available applications for the catalog.

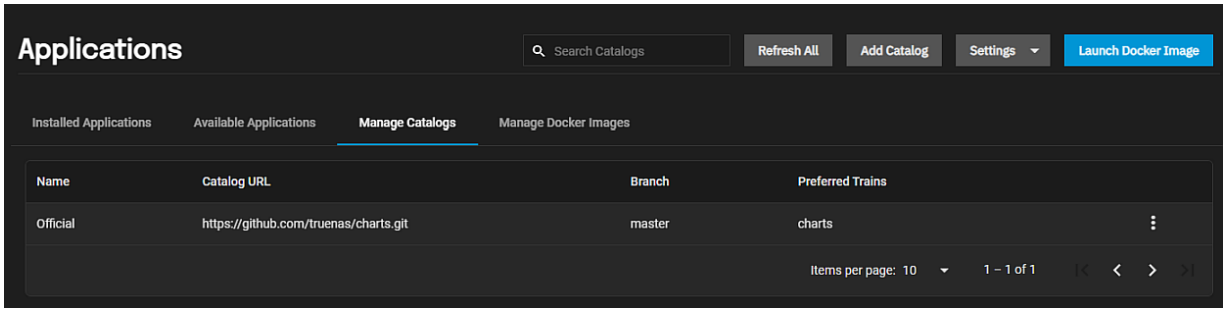


Refresh re-pulls the catalog from its repository and applies any updates.

Delete allows users to remove a catalog from the system. Users cannot delete the default Official catalog.

Summary lists all apps in the catalog and sorts them train, app, and version.

Users can filter the list by **Train** type (**All**, **charts**, or **test**), and by **Status** (**All**, **Healthy**, or **Unhealthy**).



Adding Catalogs

To add a catalog, click the **Add Catalog** button at the top right of on the **Manage Catalogs** tab. Fill out the **Add Catalog** form. As an example, the data below to add the Truecharts catalog to SCALE.

Enter the name in **Catalog Name**, for example, type *truecharts*.

Leave the **Force Create** checkbox clear.

Select a valid git repository in **Repository**. For example, *https://github.com/truecharts/catalog* for TrueCharts.

Now select the train TrueNAS should use to retrieve available application information of the catalog. For example, select *stable* or *incubator* for the TrueCharts example.

Finially, enter the git repository branch TrueNAS should use for the catalog in **Branch**. For example, for TrueCharts, enter *main*.

Click **Save**.

Related Content

- Applications Screens
- Updating MinIO from 1.6.58
- Using Apps
- Launch Docker Image Screens
- Using Docker Image
- Adding NextCloud for Media Previews
- Configuring the Chia App
- Collabora App
- MinIO Clusters

3.7.3 - Using Docker Image

This article provides information on using the Docker image wizard to configure third-party applications in TrueNAS SCALE.

SCALE includes the ability to run Docker containers using Kubernetes.

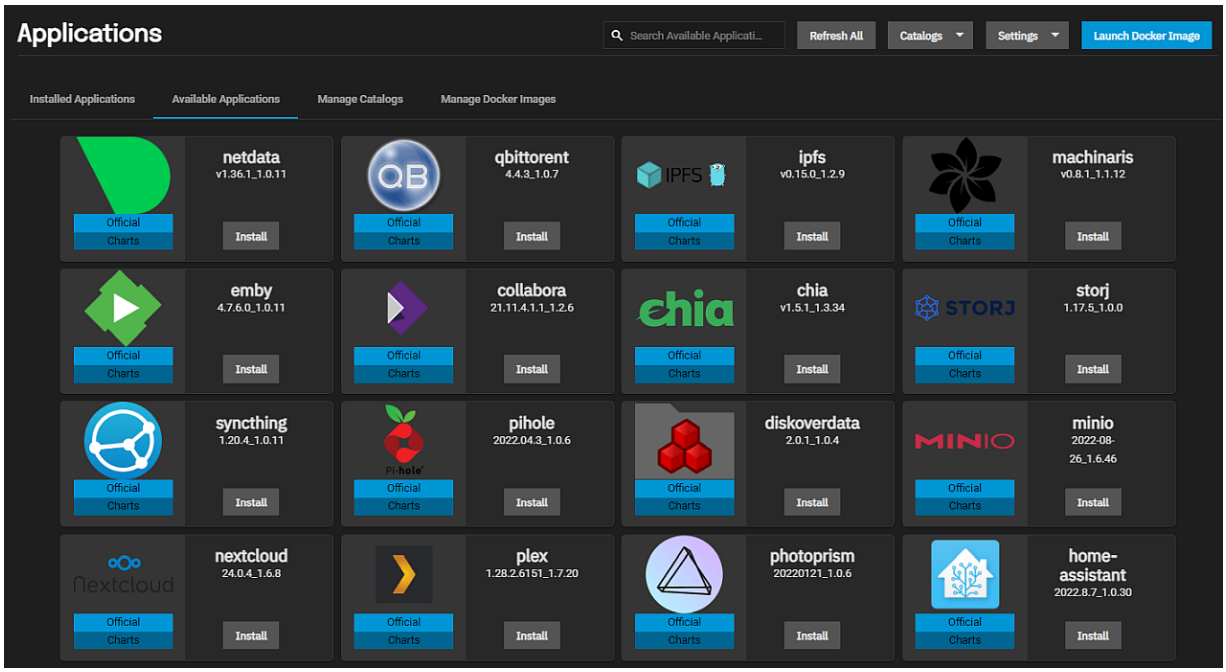
What is Docker?
Docker is an open platform for developing, shipping, and running applications. Docker enables the separation of applications from infrastructure through OS-level virtualization to deliver software in containers.

What is Kubernetes?
Kubernetes is a portable, extensible, open-source container-orchestration system for automating computer application deployment, scaling, and management with declarative configuration and automation.

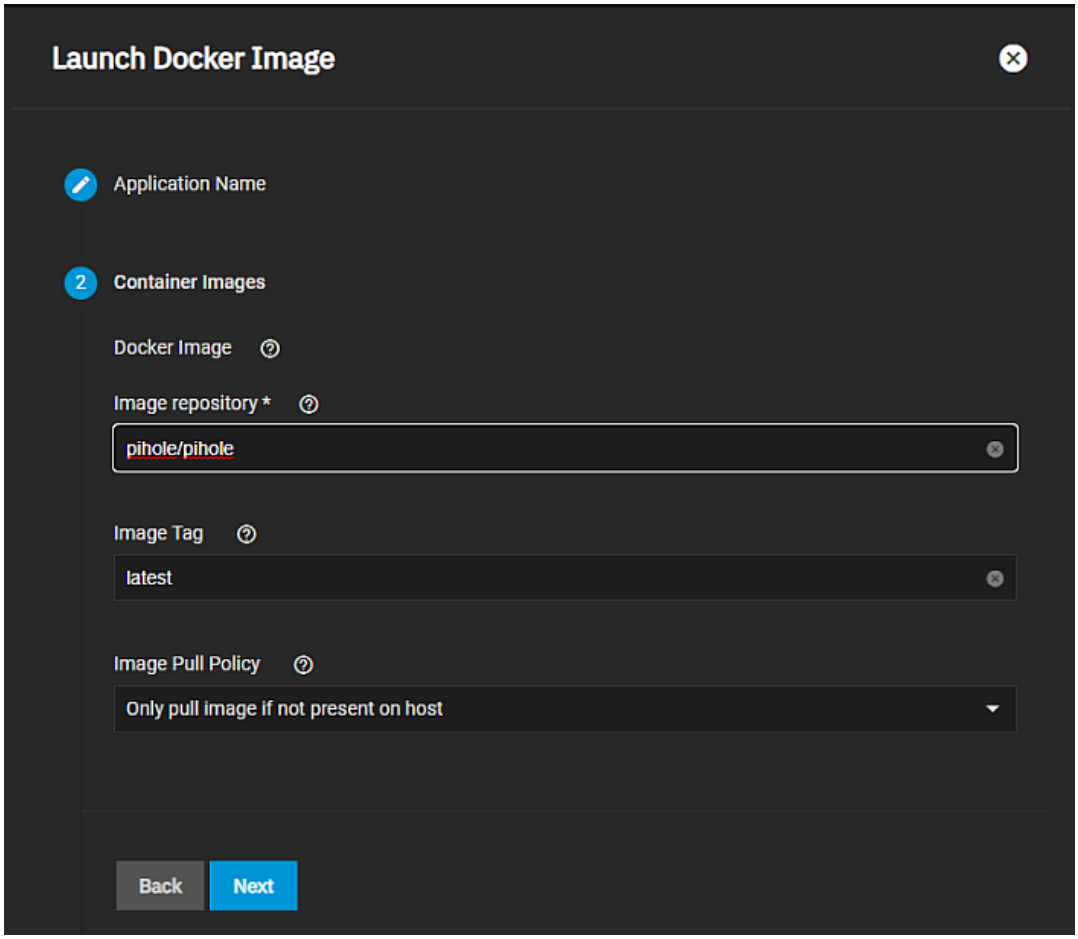
Always read through the Docker Hub page for the container you are considering installing so that you know all of the settings that you need to configure. To set up a Docker image, first determine if you want the container to use its own dataset. If yes, create a dataset for host volume paths before you click **Launch Docker Image**.

Adding Custom Applications

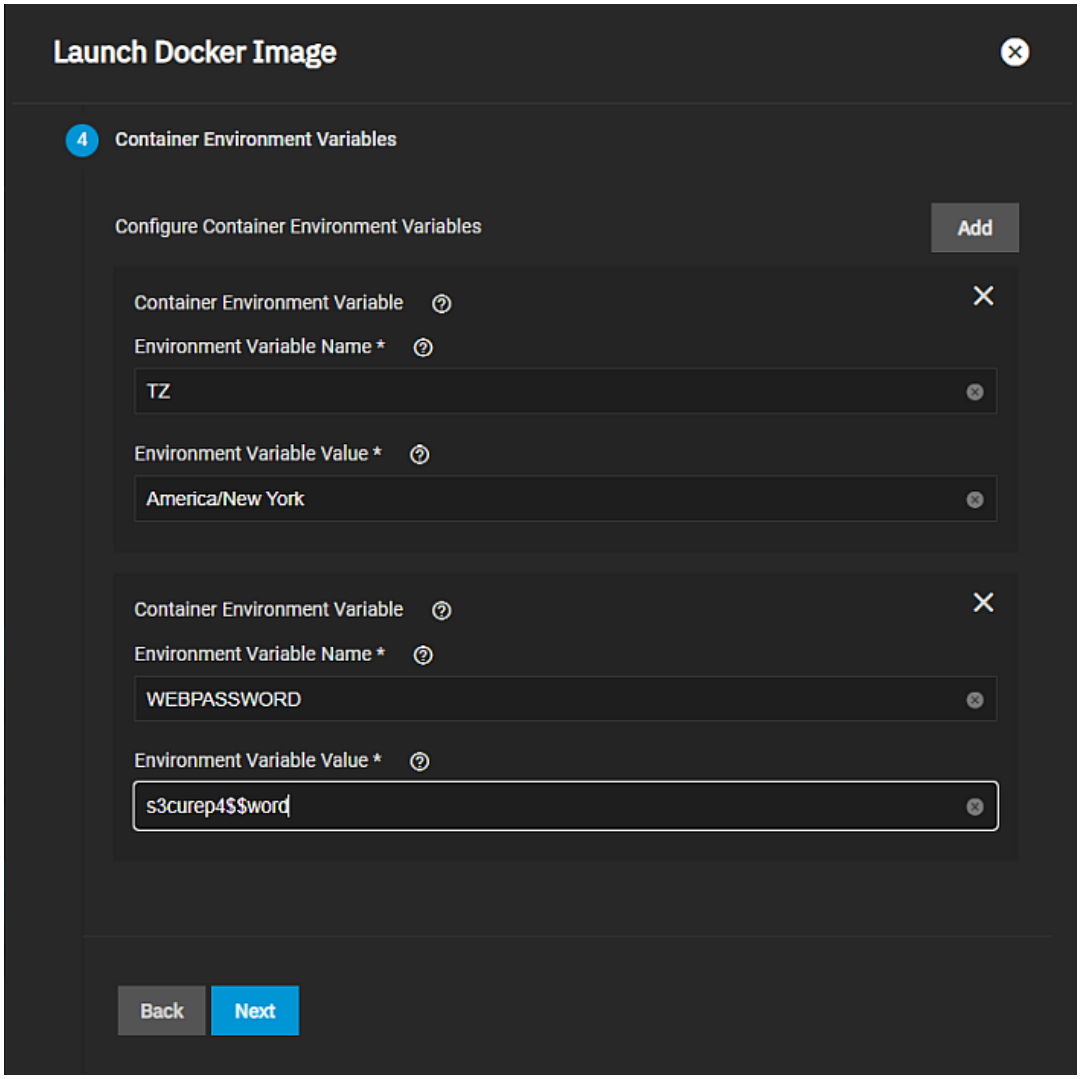
When you are ready to create a container, open the **APPS** page, select the **Available Applications** tab, and then click **Launch Docker Image**.



Fill in the **Application Name** and click **Next**. Add the github repository URL in **Image Repository** for the docker container are setting up. For example, to add Pi-Hole in **Launch Docker Image** wizard, enter **pihole/pihole** as the PiHole project image repository on the **Container Image** configuration screen.

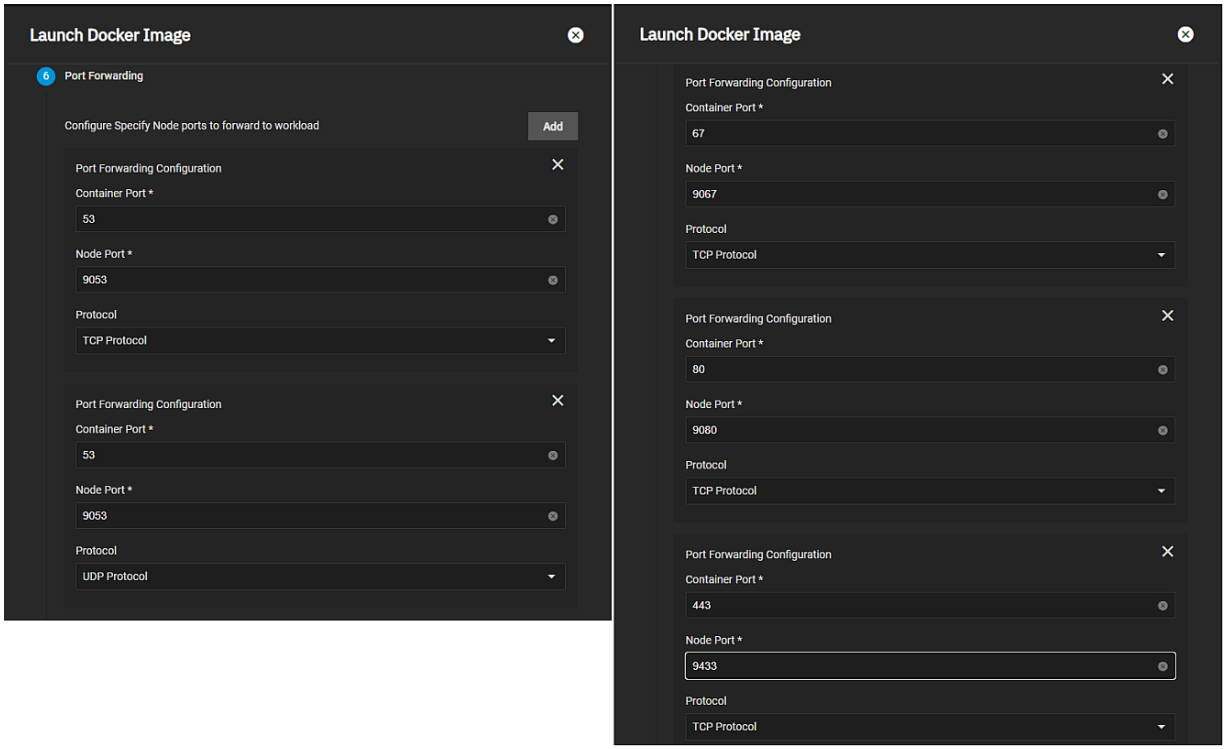


Click **Next** to move to the **Container Environment Variables**. Not all applications use environment variables. Check the Docker Hub for details on the application you want to install to verify which variables are required for that particular application. For Pi-Hole, click **Add** then enter **TZ** for timezone, and then **America/NewYork** for the value. And click **Add** again to enter the second required variable **WEBPASSWORD** with a secure password like the exaple used, *s3curep4$$word*.



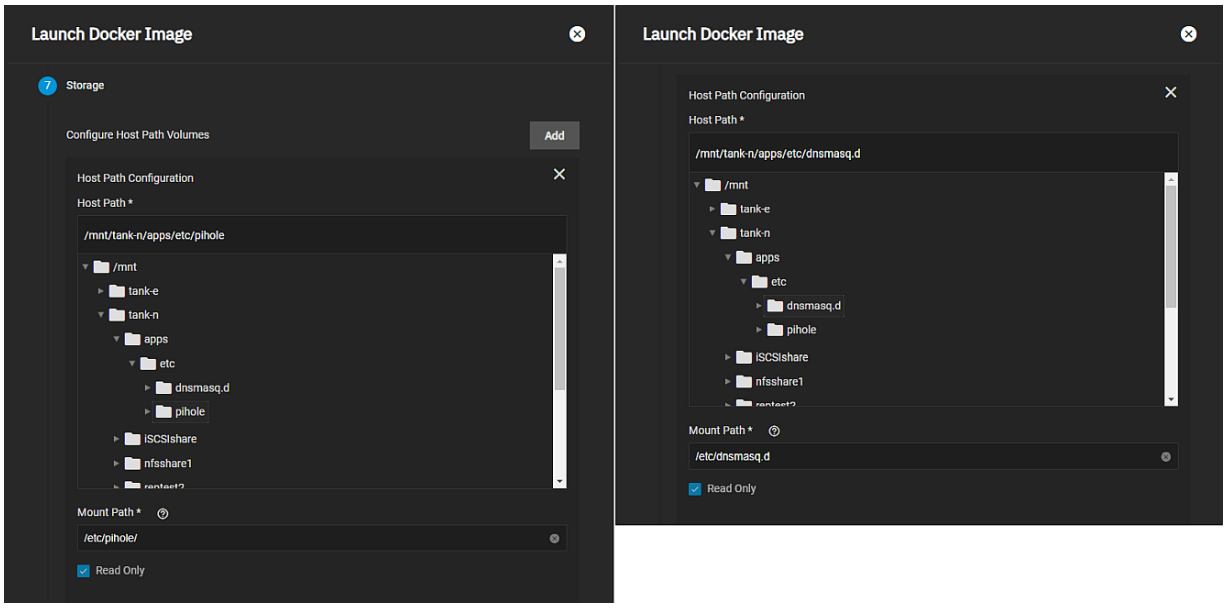
Click **Next** to advance to each of the **Launch Docker Image** configuration screens. Enter information required for the application you are adding on each screen that requires input.

When you reach **Networking**, if the container needs special networking configuration, enter it here. Click **Next** to open **Port Forwarding** to add ports. Click **Add** for each port you need to enter. The PiHole Docker Hub page lists a set of four ports and the node port you need to set. Adjust these values if your system configuration requires changes. TrueNAS SCALE requires setting all **Node Ports** above 9000.



Click **Next** after configuring all the ports to open **Storage**. Click **Add** for each host path you need to enter for the application. Pi-Hole uses two blocks of host path settings.

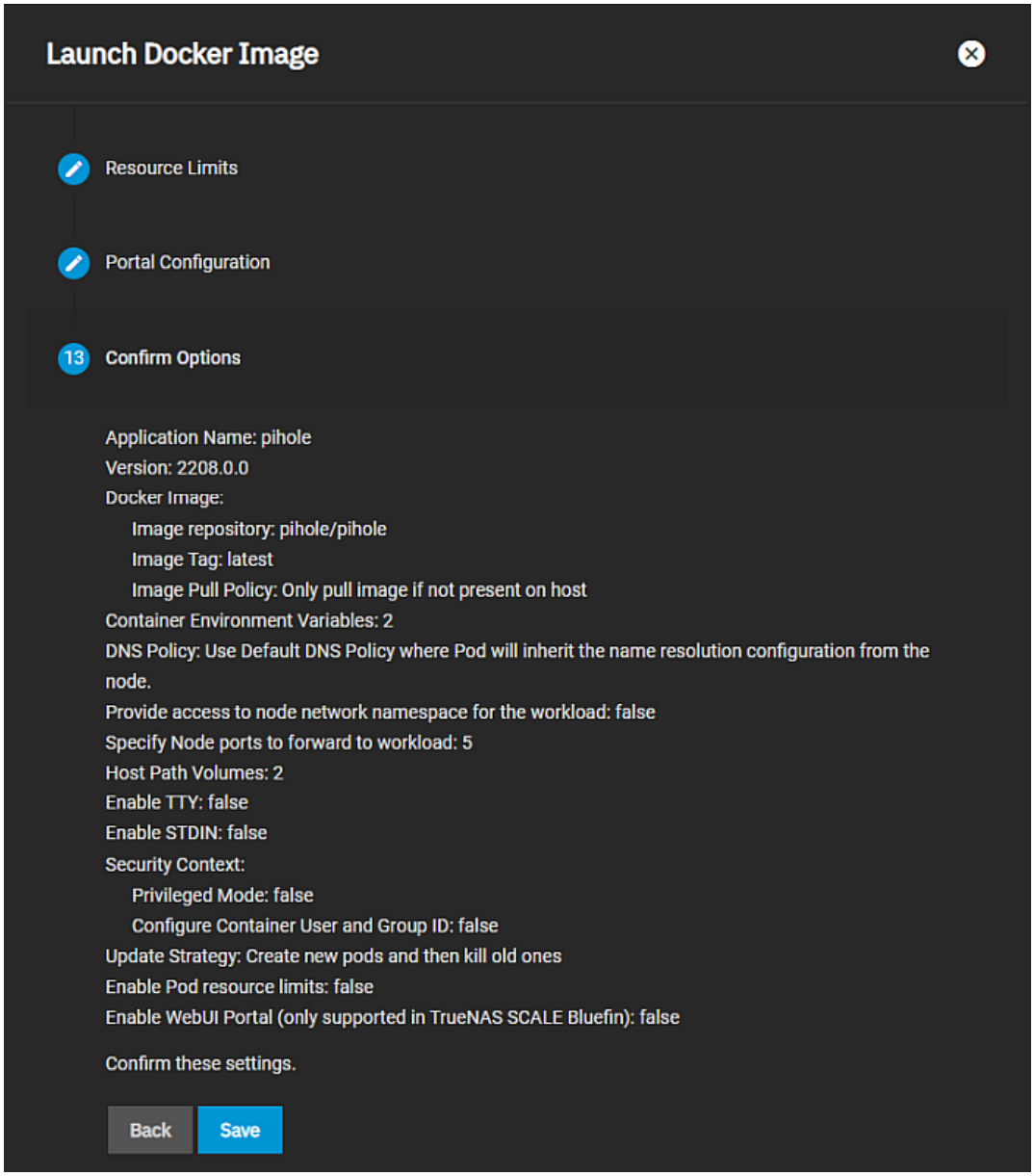
> If your application requires directory paths, specific dataset, or storage arrangements, configure these before you starting the **Launch Docker Image** wizard. You cannot interrupt the configuration wizard and save settings to leave and go create data storage or directories in the middle of the process. You need to create these directories in a dataset on SCALE using **System Settings > Shell** before you begin installing this container.



You can add more volumes to the container later if they are needed.

Click **Next** to move through the configuration screens, entering settings where required for your application.

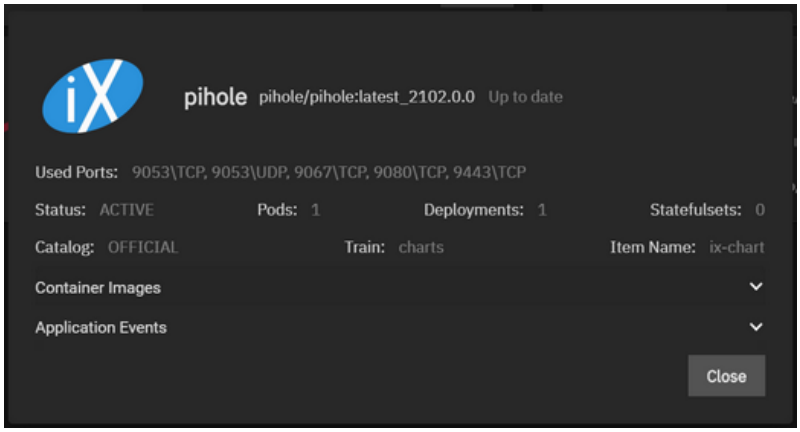
When you reach **Confirm Options**. Verify the the information on the screen and click **Save**.



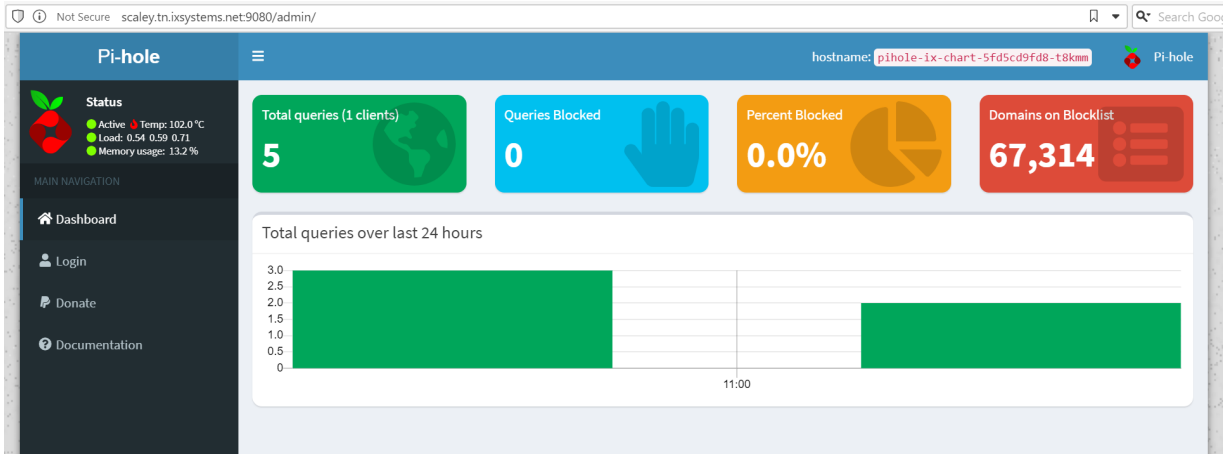
TrueNAS SCALE deploys the container. If correctly configured, the application widget displays on the **Installed Applications** screen.

When the deployment is completed the container becomes active. If the container does not autostart, click **Start** on the widget.

Clicking on the App card reveals details.



With PiHole as our example we navigate to the IP of our TrueNAS system with the port and directory address `:9080/admin/`.



Defining Container Settings

Define any commands and arguments to use for the image. These can override any existing commands stored in the image.

You can also define additional environment variables for the container. Some Docker images can require additional environment variables. Be sure to check the documentation for the image you're trying to deploy and add any required variables here.

Defining Networking

To use the system IP address for the container, set *Host Networking*. The container is not given a separate IP address and the container port number is appended to the end of the system IP address. See the Docker documentation for more details.

Users can create additional network interfaces for the container if needed. Users can also give static IP addresses and routes to new interface.

By default, containers use the DNS settings from the host system. You can change the DNS policy and define separate nameservers and search domains. See the Docker DNS services documentation for more details.

Defining Port Forwarding List

Choose the protocol and enter port numbers for both the container and node. Multiple port forwards can be defined. The node port number must be over *9000*. Make sure no other containers or system services are using the same port number.

Defining Host Path Volumes

Scale storage locations can be mounted inside the container. To mount Scale storage, define the path to the system storage and the container internal path for the system storage location to appear. You can also mount the storage as read-only to prevent the container from being used to change any stored data. For more details, see the Kubernetes hostPath documentation.

Defining Other Volumes

Users can create additional Persistent Volumes (PVs) for storage within the container. PVs consume space from the pool chosen for Application management. You need to name each new dataset and define a path where that dataset appears inside the container.

To view created container datasets, go to **Storage** and expand the pool used for applications. Expand **/ix-applications/releases//volumes/ix-volumes/**.

Setting Up Persistent Volume Access

Users developing applications should be mindful that if an application uses Persistent Volume Claims (PVC), those datasets won't be mounted on the host, and therefore are not accessible within a file browser. This is upstream zfs-localpv behavior which is being used for managing PVC(s)

If you want to consume or have file browser access to data that is present on the host, set up your custom application to use host path volumes.

Alternatively, you can use the network to copy directories and files to and from the pod using `k3s kubectl` commands.

To copy from a pod in a specific container: `k3s kubectl cp <file-spec-src> <file-spec-dest> -c <specific-container>`

To copy a local file to the remote pod: `k3s kubectl cp /tmp/foo <some-namespace>/<some-pod>:/tmp/bar`

To copy a remote pod file locally: `k3s kubectl cp <some-namespace>/<some-pod>:/tmp/foo /tmp/bar`

Accessing the Shell in an Active Container

To access the shell in an active container, first identify the namespace and pod for the container. In the Scale UI, go to **System Settings > Shell** to begin entering commands:

To view container namespaces: `k3s kubectl get namespaces`. To view pods by namespace: `k3s kubectl get -n <NAMESPACE> pods`. To access container shell: `k3s kubectl exec -n <NAMESPACE> --stdin --tty <POD> -- /bin/bash`.

Additional Container Commands

- View details about all containers: `k3s kubectl get pods,svc,daemonsets,deployments,statefulset,sc,pvc,ns,job --all-namespaces -o wide`.
- Get container status: `k3s kubectl describe -n <CONTAINER NAMESPACE> <POD-ID>`.

Related Content

- Updating MinIO from 1.6.58
- Using SCALE Catalogs
- Launch Docker Image Screens
- MinIO Clusters
- Adding Pi-Hole Using Docker Image

Related Apps Articles

- Applications Screens
- Updating MinIO from 1.6.58
- Using Apps
- Using SCALE Catalogs
- Launch Docker Image Screens
- Adding NextCloud for Media Previews
- Configuring the Chia App
- Collabora App
- MinIO Clusters

3.7.4 - Installing Nextcloud on SCALE

This article provides instructions for a basic Nextcloud installation on TrueNAS SCALE.

Nextcloud provides a suite of client-server software for creating and using file hosting services. TrueNAS SCALE includes Nextcloud in the catalog of available applications you can install on your system.

Before You Begin

Before using SCALE to install the Nextcloud application you need to configure TrueNAS SCALE storage for Nextcloud application to use.

Set up an account with Nextcloud if you don't already have one.

Installing Nextcloud

This procedure includes setting up the pool storage for Nextcloud and the basic installation and configuration of the application.

Adding Nextcloud Storage

Nextcloud needs a primary dataset for the application. You can add as many child datasets as your use case requires such as a primary data volume, a postgres data volume (db) and a postgres backup volume (dbbackup), or for extra mount path volume (opt).

You can either create these datasets under an existing dataset you use for applications (apps), or if you have enough disks on your TrueNAS system and want to create a new pool to use just for media files, create a new pool and then add the Nextcloud datasets as child datasets to the root dataset.

To create a new pool, go to **Storage** and click **Create Pool** to add a new pool.

To add under an existing dataset, click the ⋮ for the dataset where you want to add the Nextcloud datasets, and then select **Add Dataset**. In our Nextcloud example we use pool *tank*, parent dataset *apps** and then created the *nextcloud* dataset.

Next, select the **nextcloud** dataset, click ⋮ and select **Add Dataset** to add the child dataset **data** and click **Save**.

Installing Nextcloud

> **Official Applications**
>
> Official applications listed on **Available Applications** are pre-configured to only require a name during deployment.

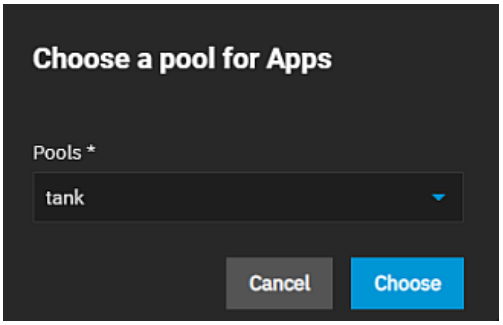
Installing Nextcloud in SCALE

This procedure installs Nextcloud with basic settings and only one dataset.

Go to **Apps** to open the **Applications** screen and then click on the **Available Applications** tab.

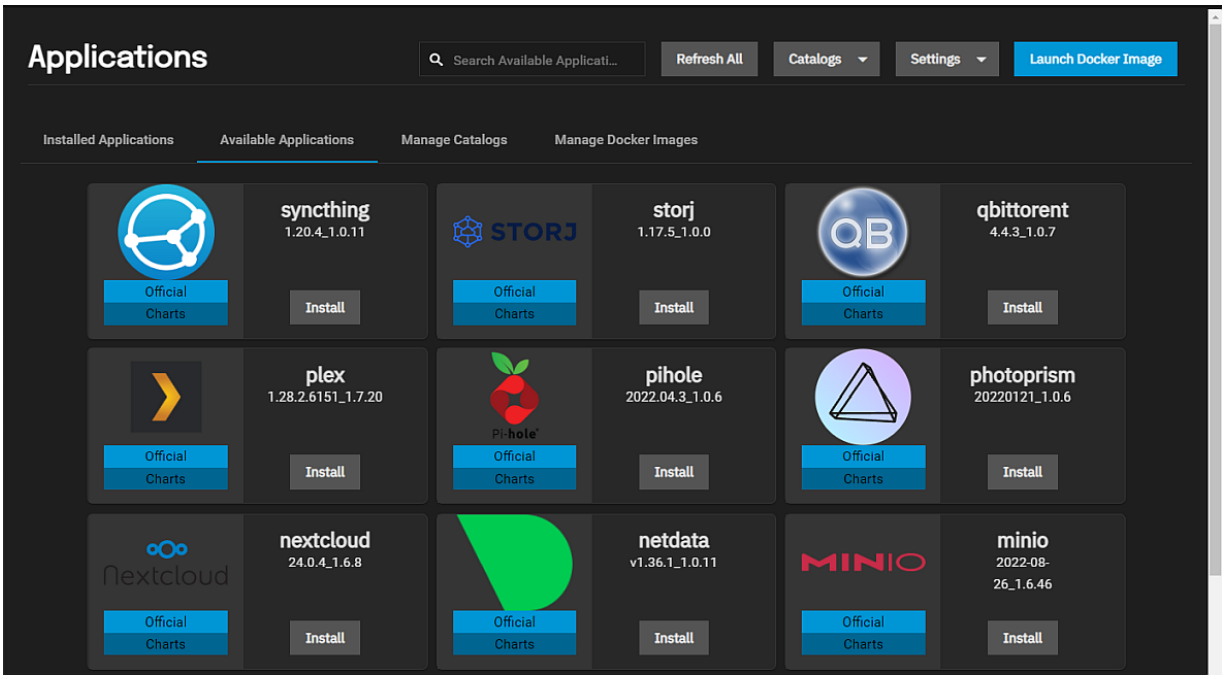
1. Set the pool SCALE applications use.

   If you have not installed an application yet, SCALE opens the **Choose a pool for Apps** dialog. Select the pool where you created the Nextcloud dataset from the **Pools** dropdown list and then click **Choose** to set the pool for all applications.

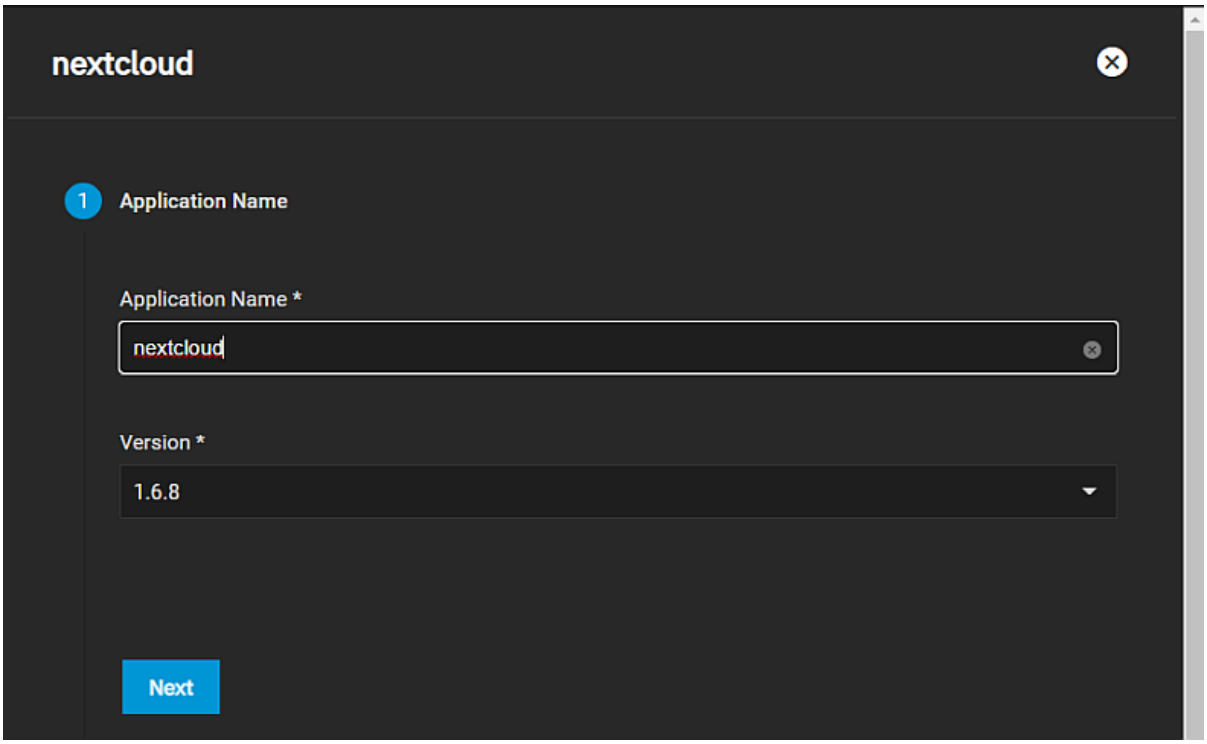
   

   After SCALE finishes configuring the system to use this pool, a confirmation dialog displays. Click **Close**

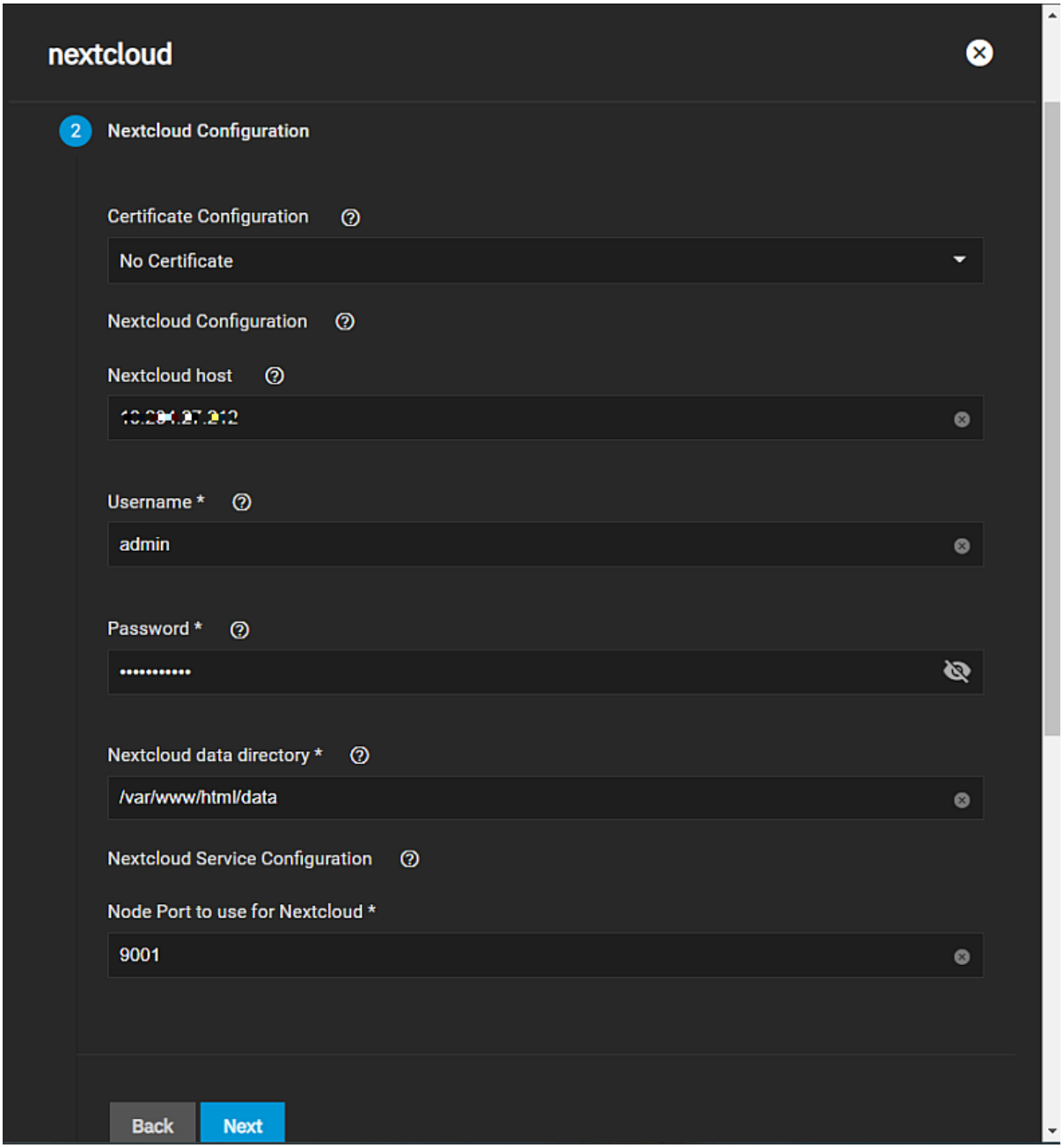
2. Locate the **nextcloud** widget and then click **Install** to open the **Nextcloud** configuration wizard.



3. Enter a name for the app in **Application Name** and then click **Next**. This example uses *nextcloud*.

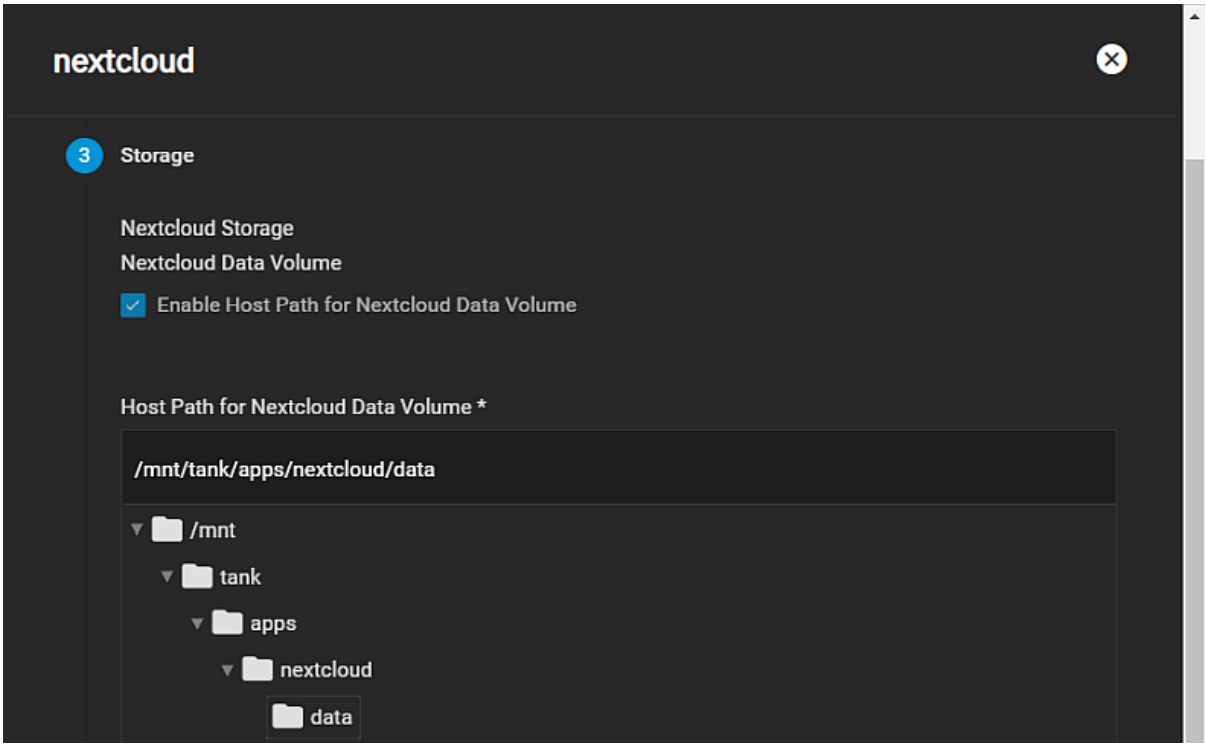


4. Enter a user name and password to use as a Nextcloud login on the **Nextcloud Configuration** settings screen, and then click **Next**. For a basic installation you can leave the default values in all settings except **Username** and **Password**. This example uses *admin* as the user. TrueNAS populates **Nextcloud host** with the IP address for your server, **Nextcloud data directory** with the correct path, and **Node Port to use for Nextcloud** with the correct port number.



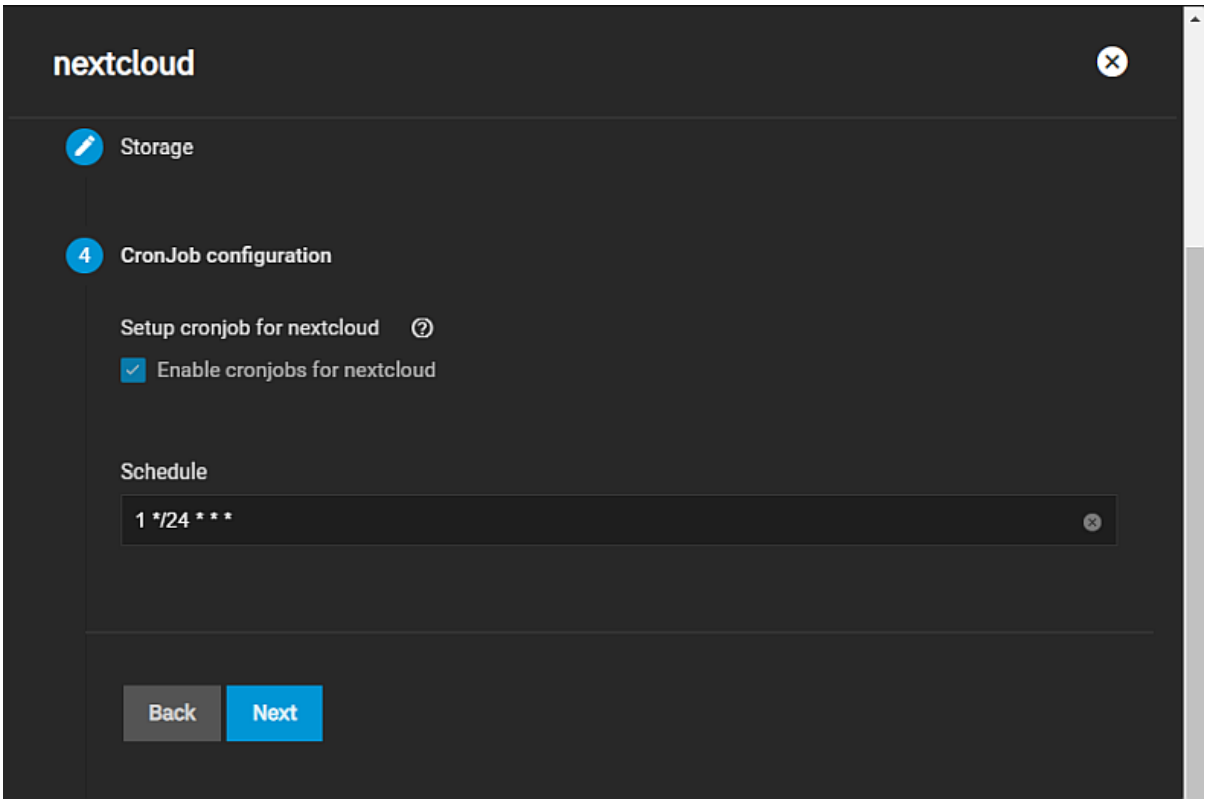
5. Enter the storage settings for the Nextcloud dataset.

   Enter or browse to the location where you created the nextcloud/data dataset in **Host Path for Nextcloud Data Volume**. This example uses the */mnt/tank/apps***/nextcloud/data*** path.

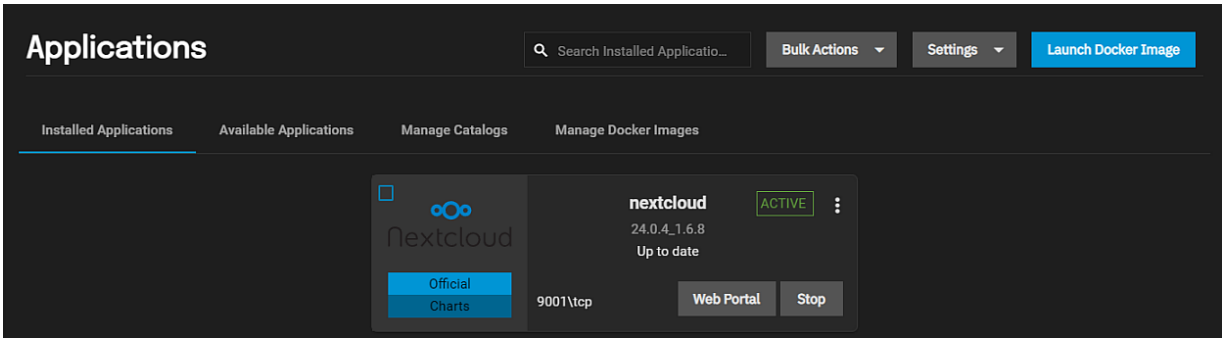


To collapse the directory tree, click the arrow to the left of /mnt. Do not click on /mnt as this changes the path and you have to reselect your dataset This completes the basic storage setup for Nextcloud. Click **Next**.

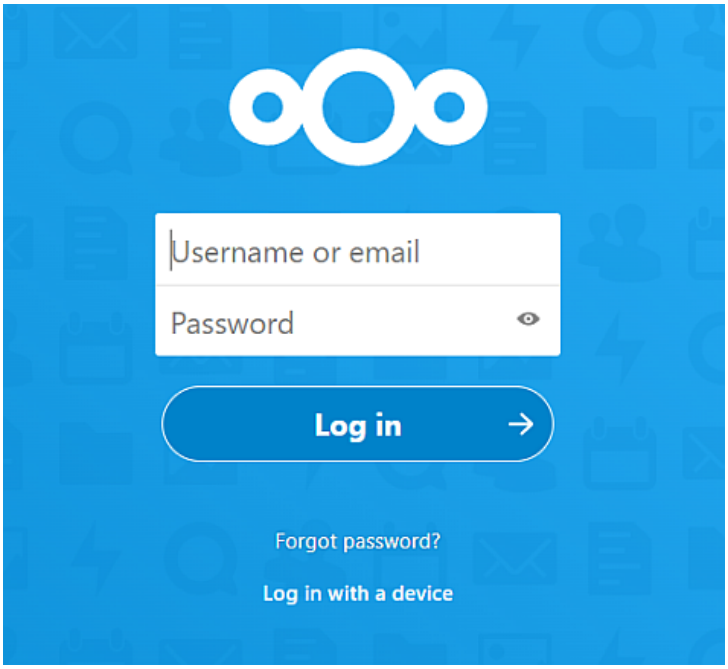
6. (Optional) Select **Enable cronjobs for nextcloud** on the **CronJob configuration** screen, and then click **Next**.



7. Accept the remaining setting defaults and click **Next** on the **Scaling/Upgrade Policy** and **Advanced DNS Settings** screens.
8. Review the configuration settings and then click **Back** to fix any errors or **Save** to complete the installation.
9. Click on the **Installed Applications** tab to see the **nextcloud** widget.



When the **nextcloud** widget displays **ACTIVE**, click **Web Portal** to open the Nextcloud sign in screen in a new browser window.



Refer to the Nextcloud documentation for details about using the Nextcloud platform:

- Administrators Manual
- Users Manual
- Nextcloud Developer Documentation

Related Nextcloud Articles

- Adding Cloud Credentials
- Cloud Credentials Screens
- Using SCALE Catalogs
- Adding NextCloud for Media Previews

3.7.5 - Adding NextCloud for Media Previews

This article provides instructions to configure TrueNAS SCALE and install NextCloud to support hosting a wider variety of media file previews such as HEIC, Mp4 and MOV files.

NextCloud is a drop-in replacement for many popular cloud services, including file sharing, calendar, groupware and more. One of its more common uses for the home environment is serving as a media backup, and organizing and sharing service. This procedure demonstrates how to set up NextCloud on TrueNAS SCALE, and configure it to support hosting a wider variety of media file previews, including High Efficiency Image Fromat (HEIC), MP4 and MOV files. The instructions in this article apply to SCALE 22.02.3 and later.

Before You Begin

Before using SCALE to install the NextCloud application you need to configure TrueNAS SCALE storage for NextCloud application to use. You also use the SCALE Shell to set the ffmpg binary before you begin the NextCloud installation and configuration.

Set up an account with NextCloud if you don't already have one.

Installing NextCloud on SCALE

In this procedure you:

1. Add the storage NextCloud uses
2. Set up the ffmpg binary
3. Install the NextCloud app in SCALE

Adding NextCloud Storage

NextCloud needs a primary dataset for the application, and four datasets it uses for the primary data volume, a postgres data volume (db) and one as a postgres backup volume (dbbackup), and an one for extra mount path volume (opt).

You can either create these datasets under an existing dataset you use for applications (apps), or if you have enough disks on your TrueNAS system and want to create a new pool to use just for media files, create a new pool and then add the NextCloud datasets as child datasets to the root dataset.

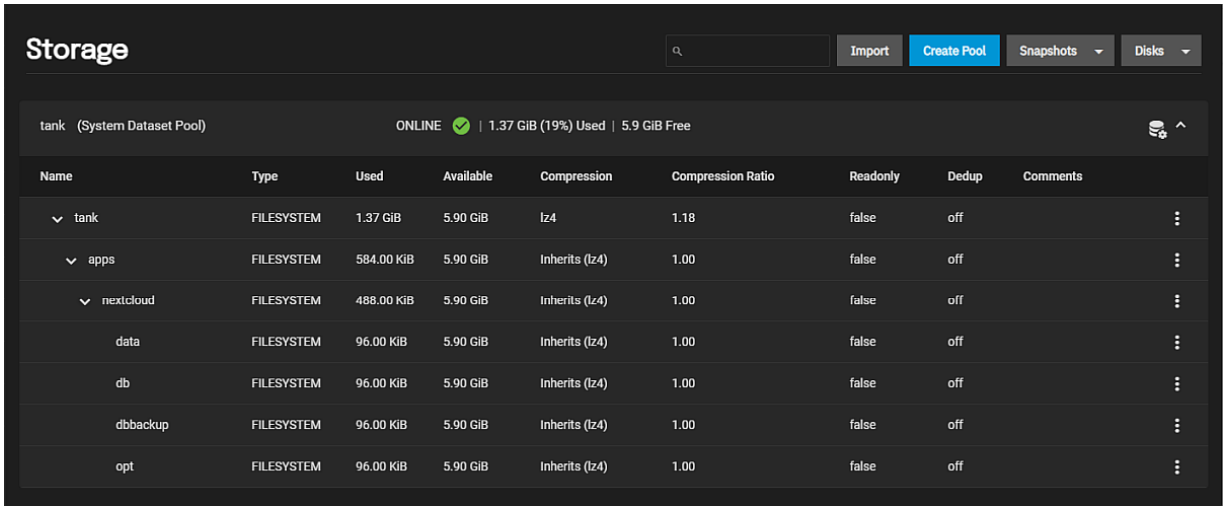
To create a new pool, go to **Storage** and click **Create Pool** to add a new pool.

To add under an existing dataset, click the ⋮ for the dataset where you want to add the NextCloud datasets, and then select **Add Dataset**. In our Nextcloud example we use pool *tank*, parent dataset *apps** and then created the *nextcloud* dataset.

Next, select the **nextcloud** dataset, click ⋮ and select **Add Dataset** to add a child dataset. Enter **data** in **Name** and click **Save**. Repeat this step three more times to add the three child datasets to the **nextcloud** dataset, one named **db**, the next **dbbackup**, and then finally **opt**.

When finished you should have the *nextcloud* parent dataset with four child datasets under it. Our example paths are:

- */mnt/tank/apps/nextcloud/data*
- */mnt/tank/apps/nextcloud/db*
- */mnt/tank/apps/nextcloud/dbbackup*
- */mnt/tank/apps/nextcloud/opt*



Set Up the ffmpg Binary

Go to **System > Shell** and enter these six commands:

```
cd /mnt/tank/apps/nextcloud/opt

wget https://johnvansickle.com/ffmpeg/releases/ffmpeg-release-amd64-static.tar.xz

tar xvf ffmpeg-release-amd64-static.tar.xz --wildcards \*static/ffmpeg

rm ffmpeg-release-amd64-static.tar.xz

mv ffmpeg-*-static/ bin/

chown root:root bin/ffmpeg
```

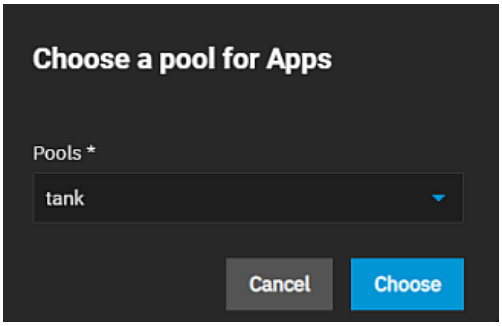
With the ffmpeg binary set you can now install NextCloud on your TrueNAS SCALE.

Installing NextCloud in SCALE

Go to **Apps** to open the **Applications** screen and then click on the **Available Applications** tab.

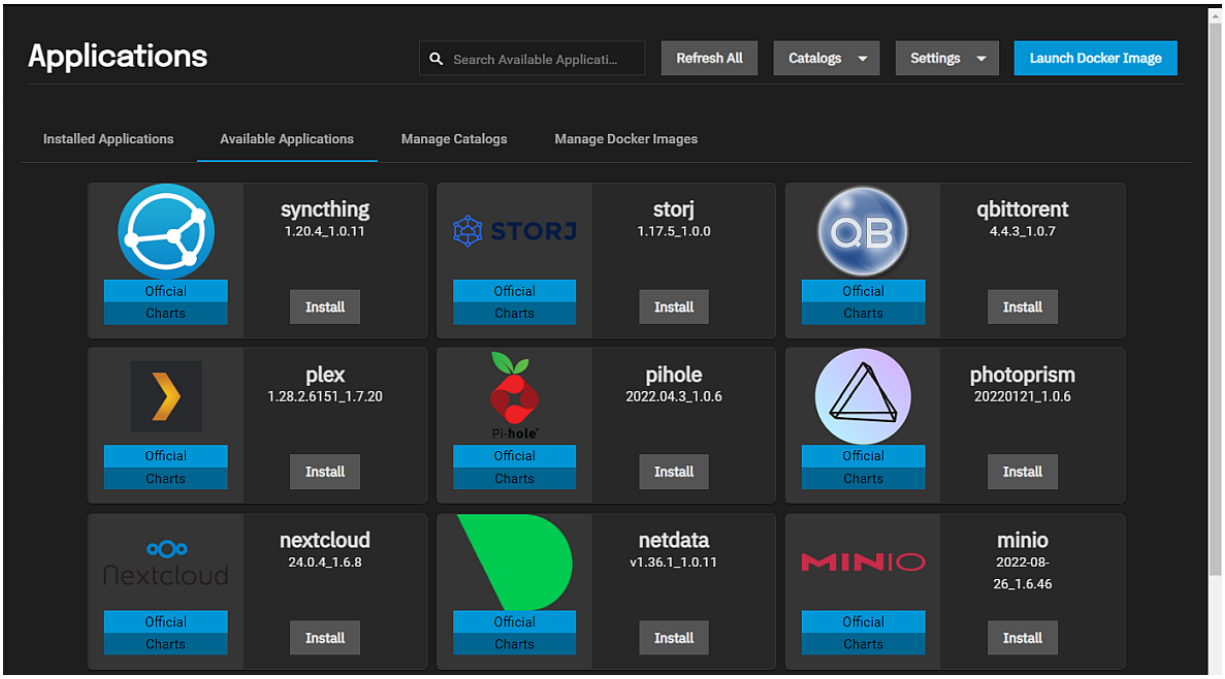
1. Set the pool SCALE applications use.

   If you have not installed an application yet, SCALE opens the **Choose a pool for Apps** dialog. Select the pool where you created the NextCloud datasets from the **Pools** dropdown list and then click **Choose** to set the pool for all applications.

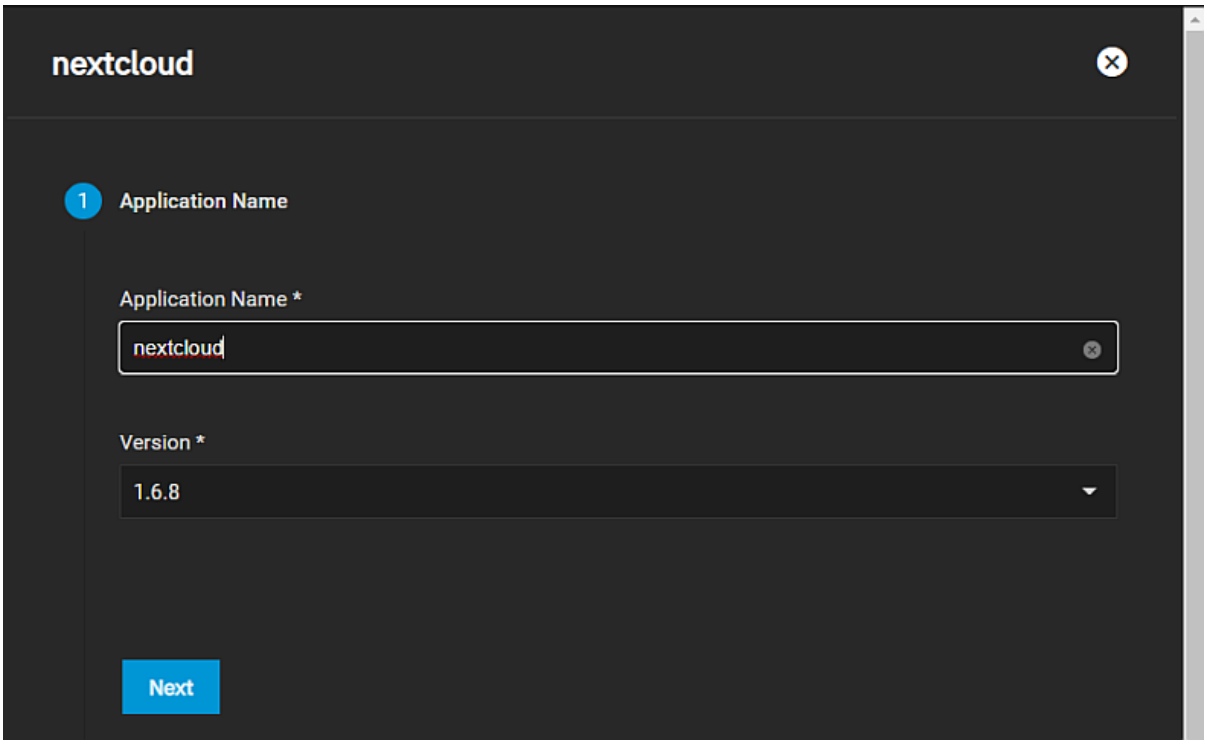
   

   After SCALE finishes configuring the system to use this pool, a confirmation dialog displays. Click **Close**

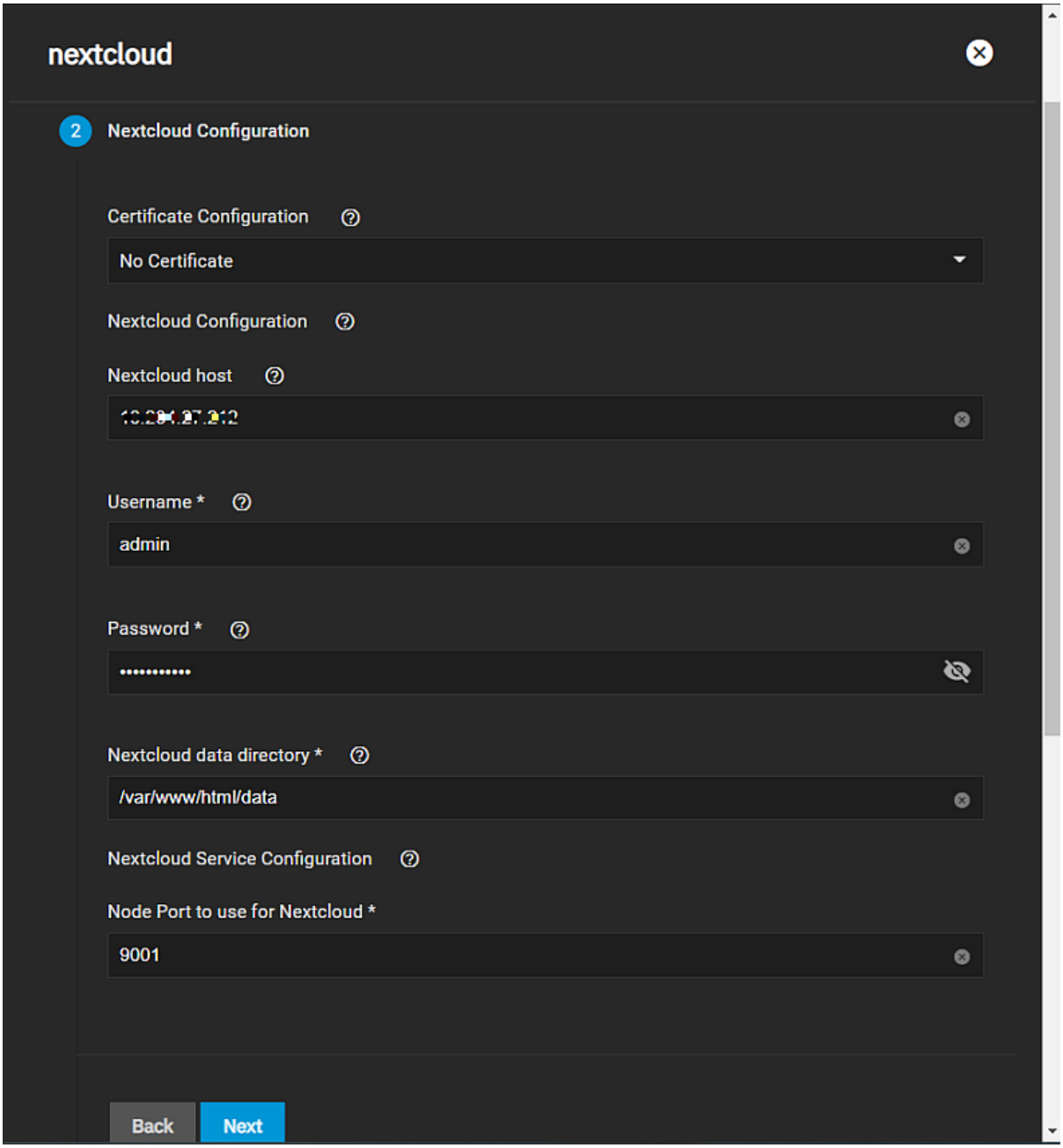
2. Locate the **nextcloud** widget and then click **Install** to open the **Nextcloud** configuration wizard.



3. Enter a name for the app in **Application Name** and then click **Next**. This example uses *nextcloud*.

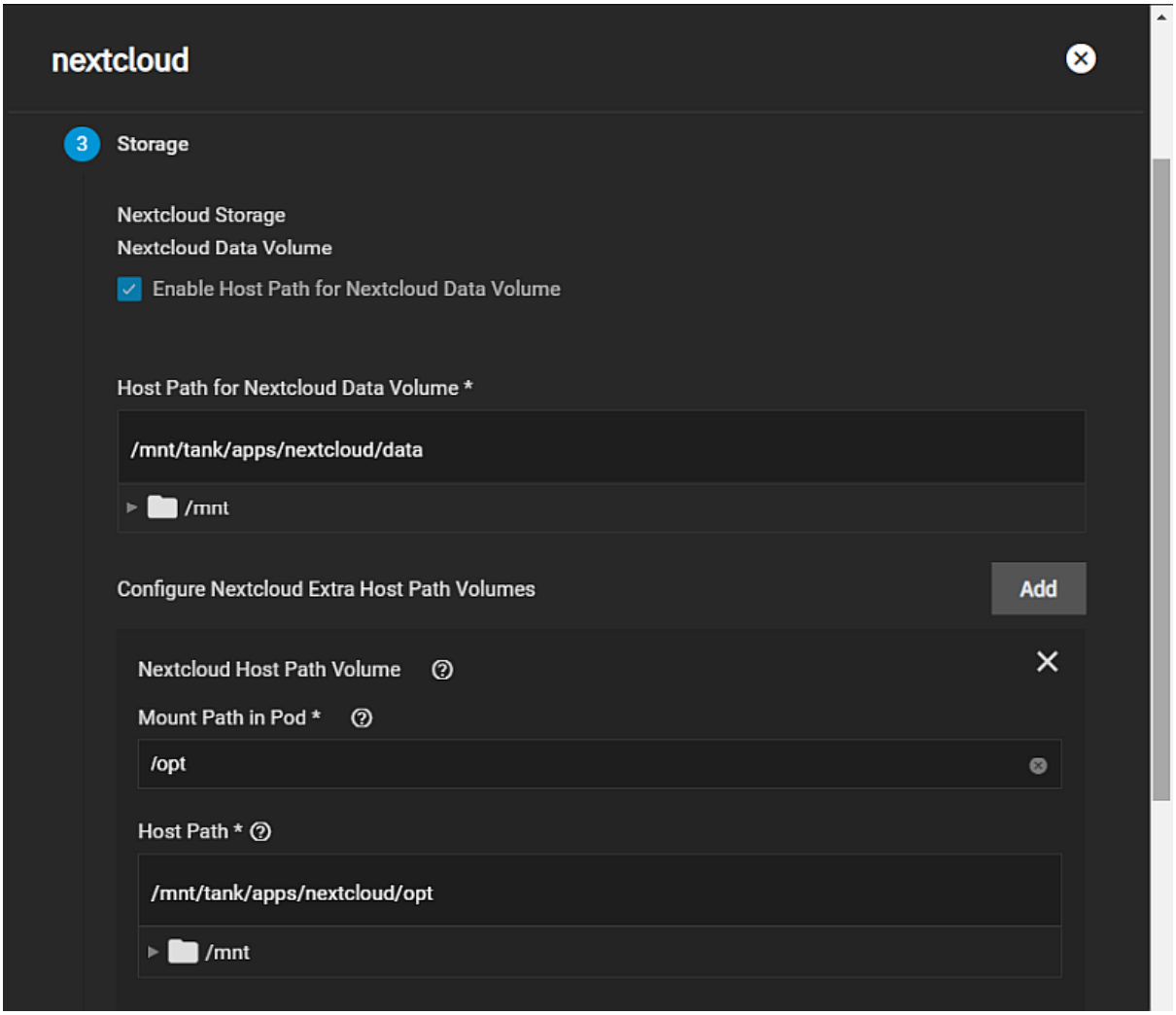


4. Enter a user name and password to use as a NextCloud login on the **Nextcloud Configuration** settings screen, and then click **Next**. For a basic installation you can leave the default values in all settings except **Username** and **Password**. This example uses *admin* as the user. TrueNAS populates **Nextcloud host** with the IP address for your server, **Nextcloud data directory** with the correct path, and **Node Port to use for Nextcloud** with the correct port number.



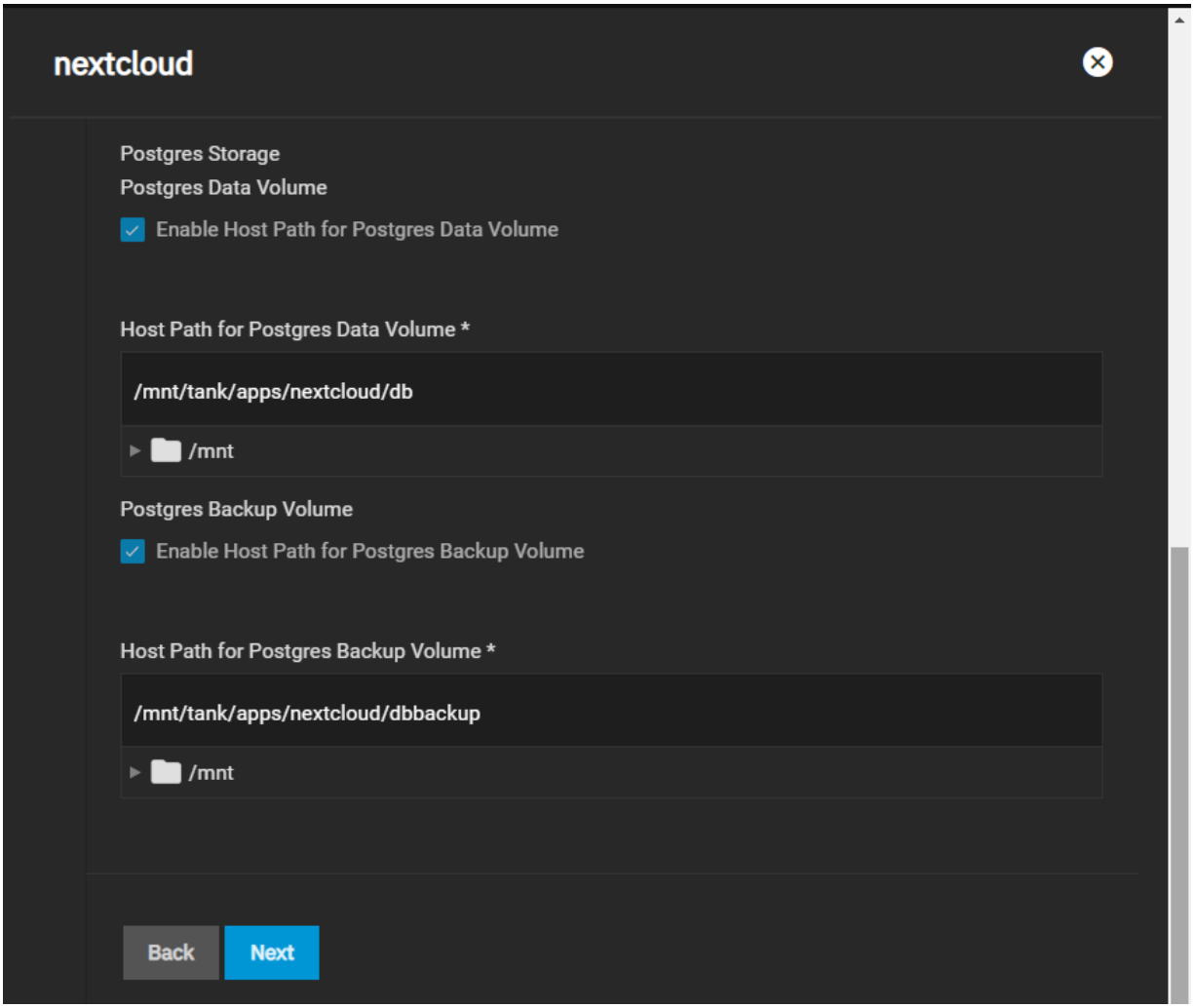
5. Enter the storage settings for each of the four datasets created for NextCloud.

   Enter or browse to the location where you created the nextcloud/data dataset in **Host Path for Nextcloud Data Volume**. This example uses the */mnt/tank/apps***/nextcloud/data*** path.



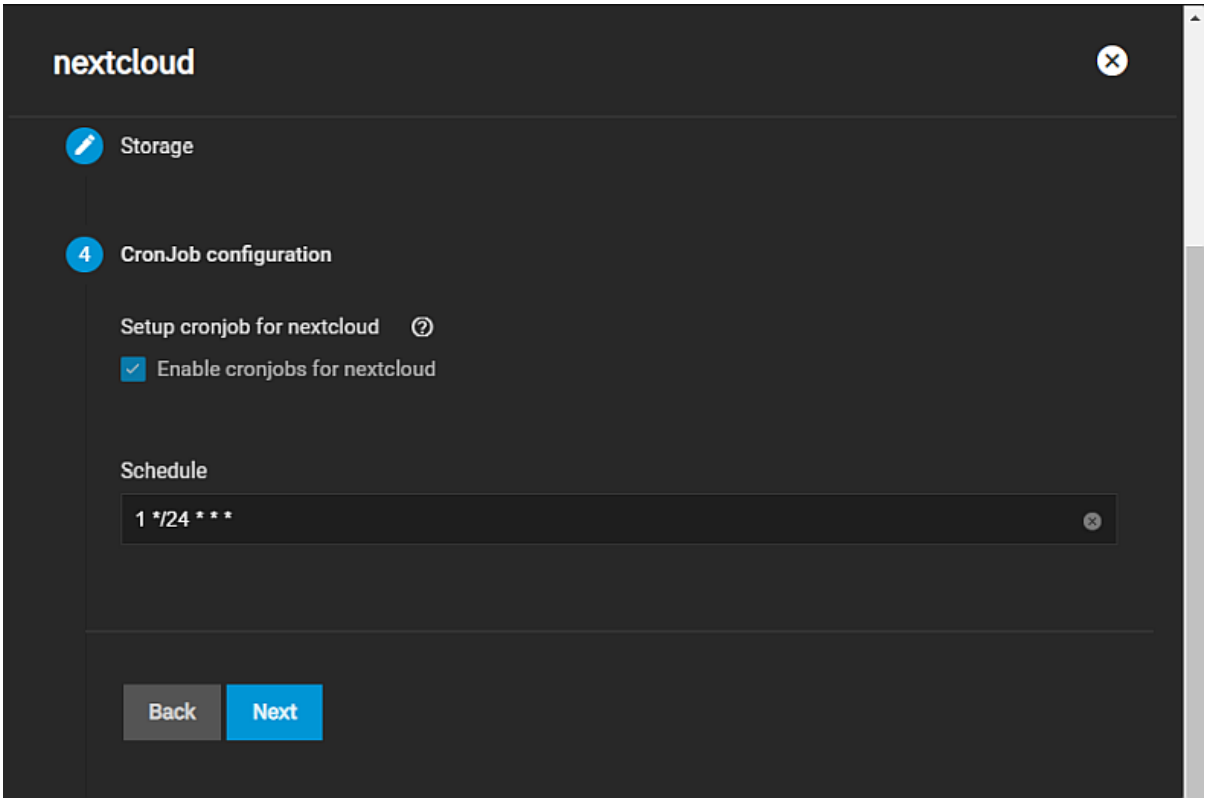
Click **Add** to display the **Mount Path in Pod** and **Host Path** fields. Enter **/opt** in **Mount Path in Pod**, and then either enter or browse to the location where you created the **nextcloud/opt** dataset in **Host Path**. This example uses the */mnt/tank/apps***/nextcloud/opt*** path.

Select **Enable Host Path for Postgres Data Volume**, and then enter or browse to the location where you created the **nextcloud/db** dataset in **Host Path for Postgres Data Volume**.

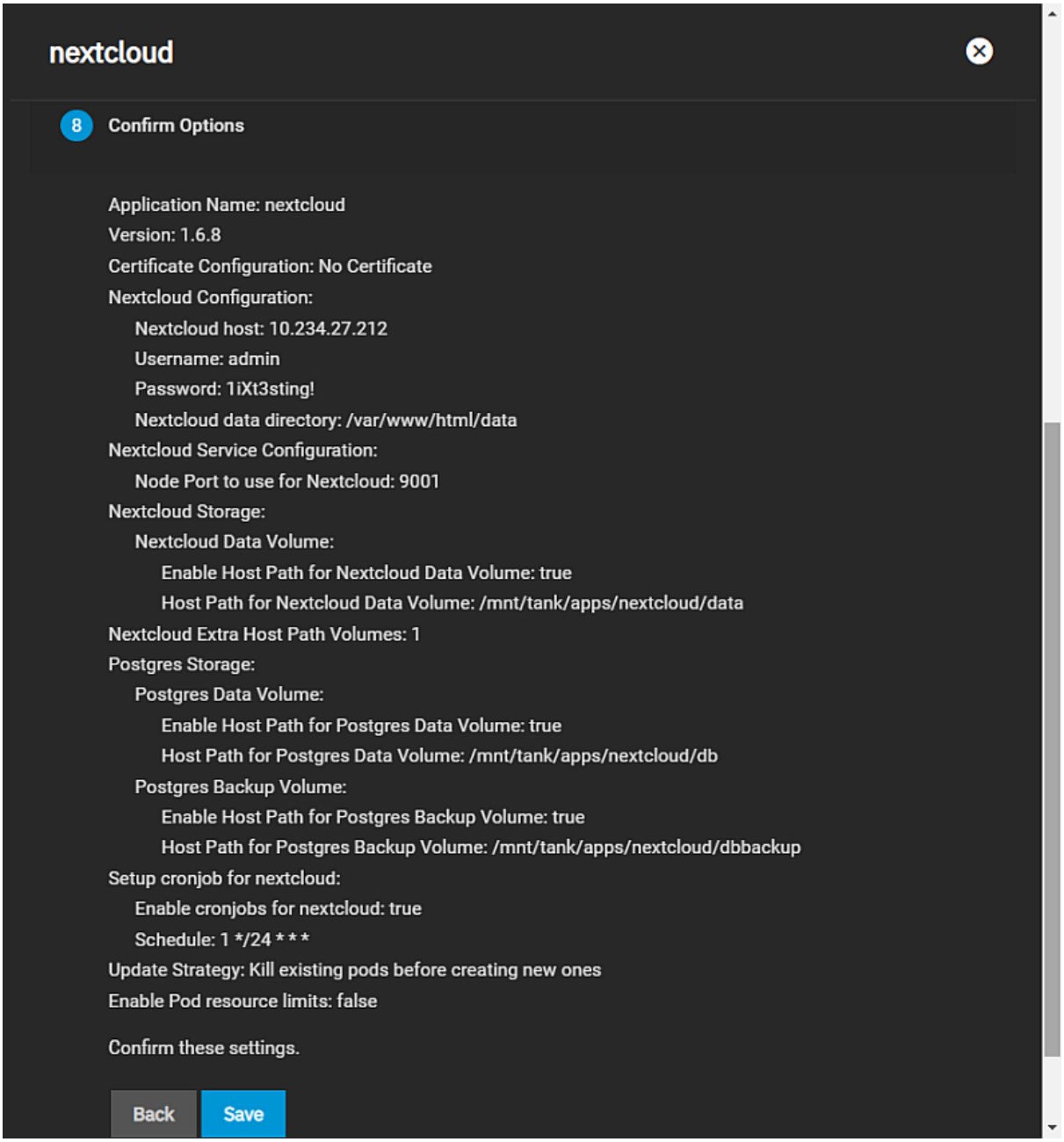


Select **Enable Host Path for Postgres Backup Volume**, and then enter or browse to the location where you created the **nextcloud/dbbackup** dataset in the **Host Path for Progres Backup Volume**. This completes the storage setup for NextCloud. Click **Next**.

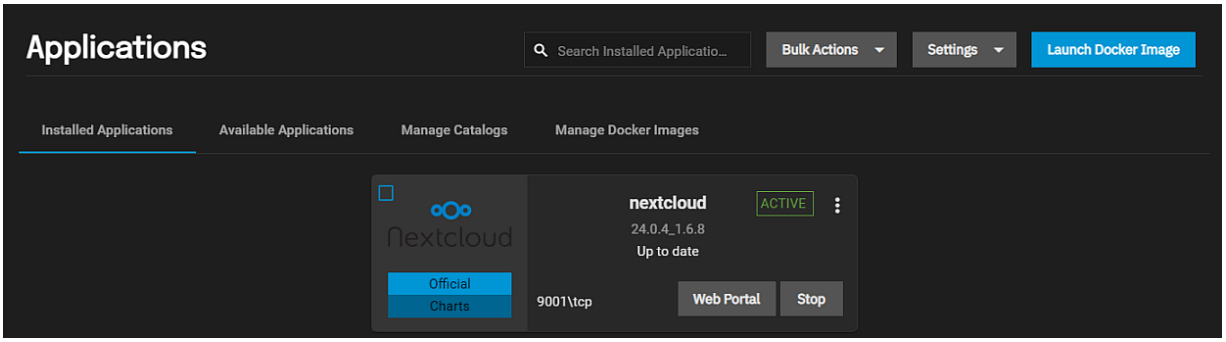
6. Select **Enable cronjobs for nextcloud** on the **CronJob configuration** screen, and then click **Next**.



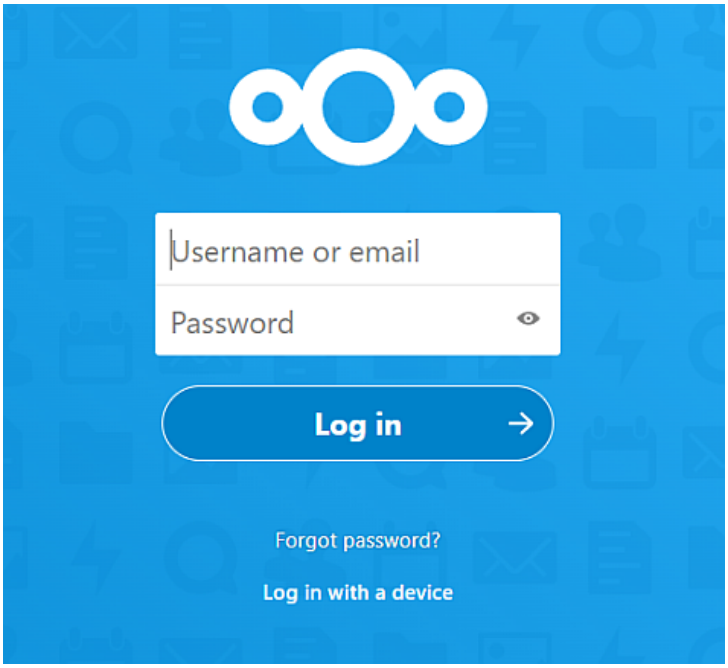
7. Accept the remaining setting defaults and click **Next** on the **Scaling/Upgrade Policy** and **Advanced DNS Settings** screens.
8. Review the configuration settings and then click **Back** to fix any errors or **Save** to complete the installation.



9. Click on the **Installed Applications** tab to see the **nextcloud** widget.



When the **nextcloud** widget displays **ACTIVE**, click **Web Portal** to open the NextCloud sign in screen in a new browser window.



Related NextCloud Articles

- Adding Cloud Credentials
- Cloud Credentials Screens
- Using SCALE Catalogs
- Installing Nextcloud on SCALE

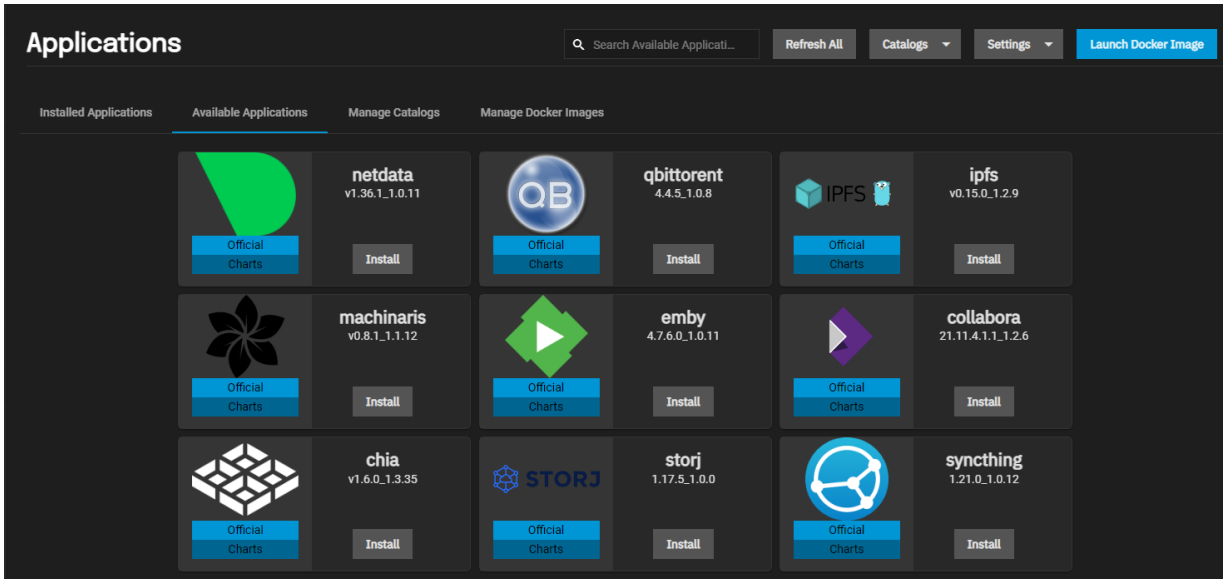
3.7.6 - Configuring the Chia App

This article provides basic installation instruction for the Chia application using both the TrueNAS webUI and CLI commands.

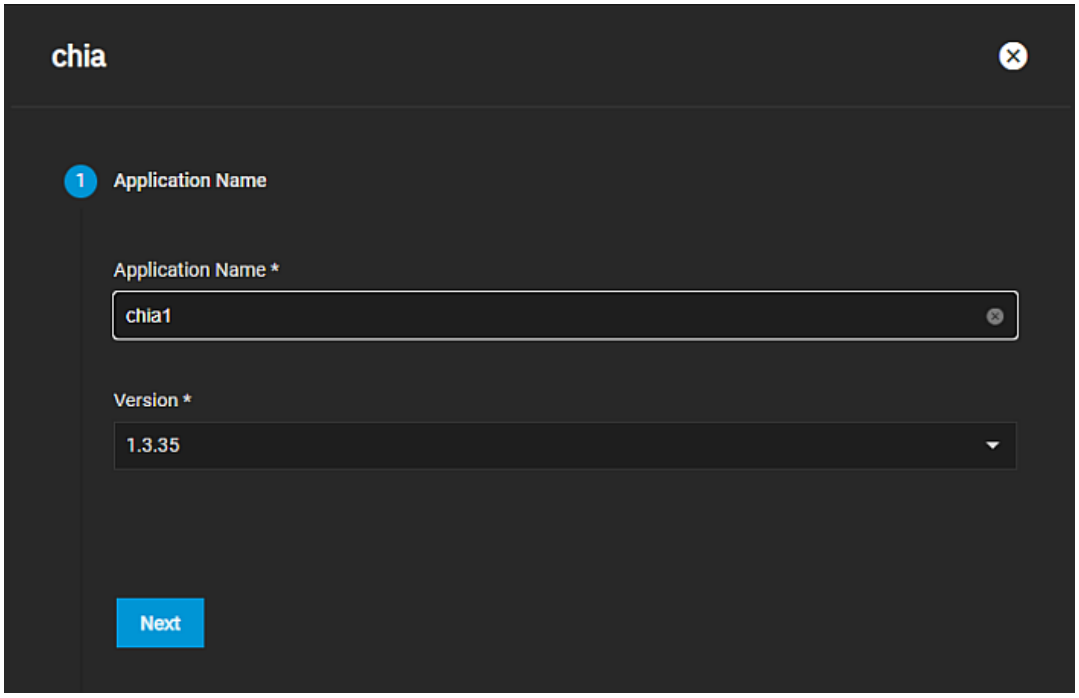
SCALE includes Chia in its Official Apps catalog. Chia Blockchain is a new cryptocurrency that uses Proof of Space and Time. Instead of using expensive hardware that consumes exorbitant amounts of electricity to mine cryptos, it leverages existing empty hard disk space on your computer(s) to farm cryptos with minimal resources, such as electricity.

Install the Chia App

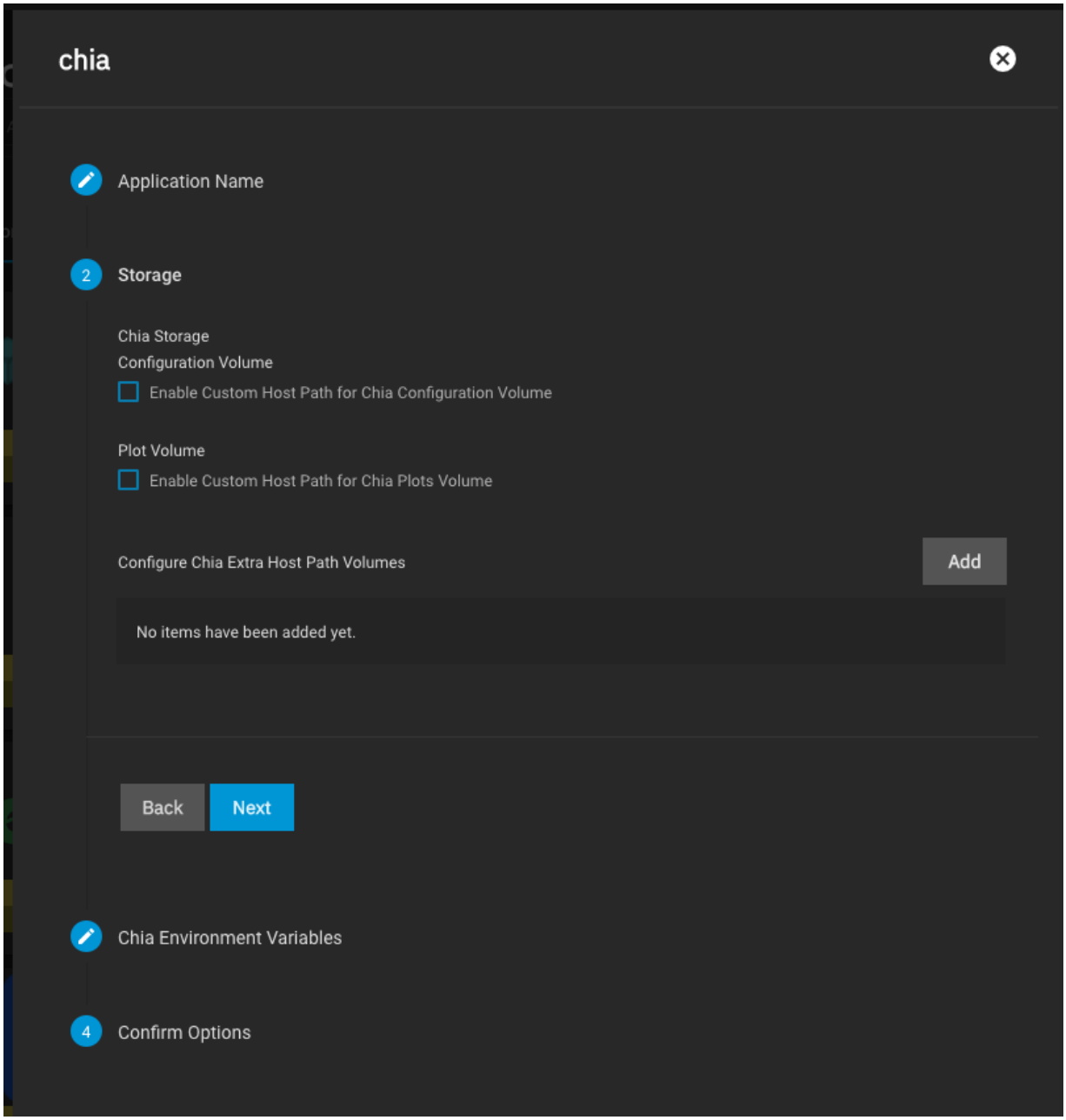
Click on the Chia app **Install** button in the **Available Applications** list.



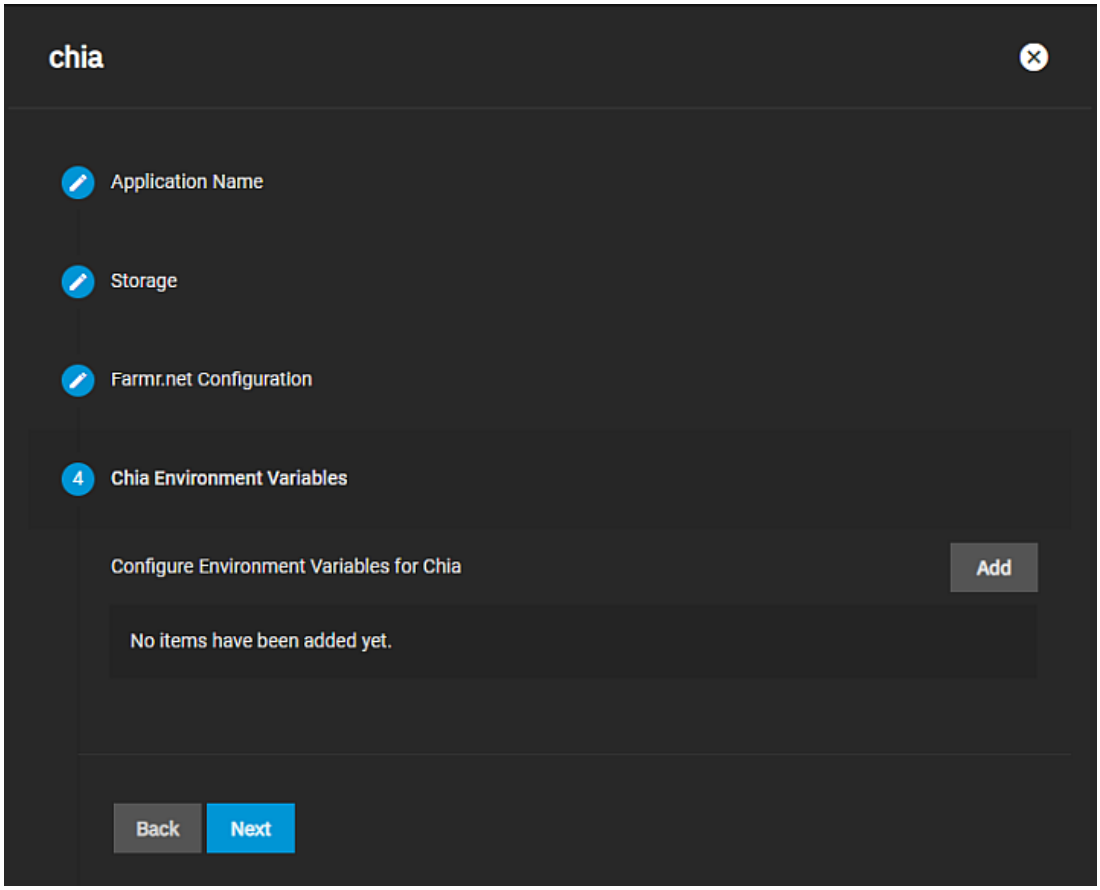
Name your App and click **Next**. In this example, the name is *chia1*.



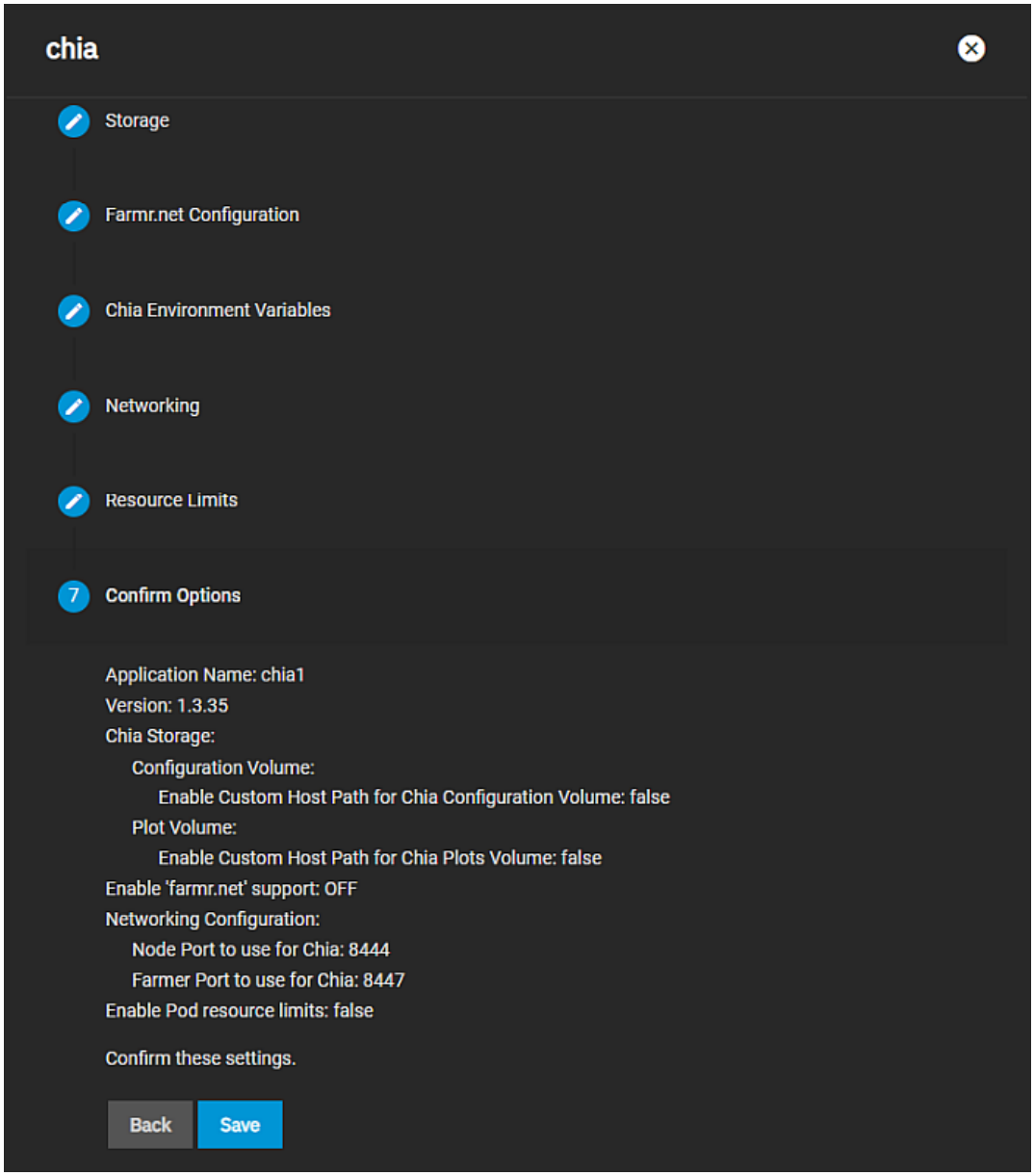
Leave **Enable Custom Host Path for Chia Configuration Volume** and **Enable Custom Host Path for Chia Plots Volume** unchecked and click **Next**.



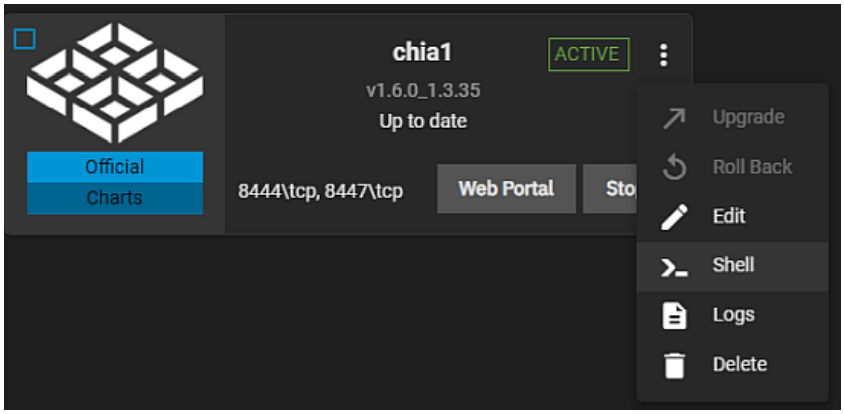
Click **Next** in the Chia Environment Variables screen. You add one later.



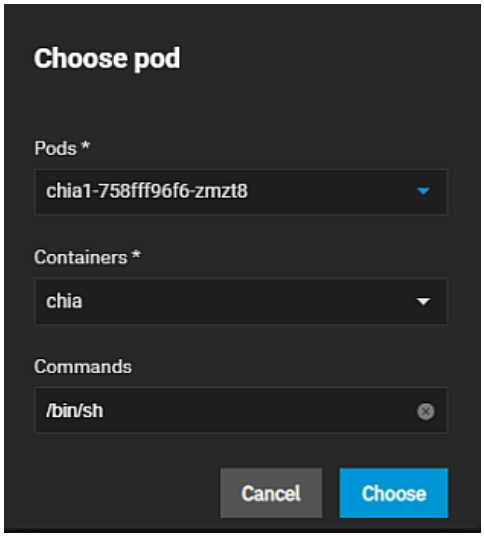
Confirm the options and click **Submit**.



Continue through the wizard and create the new application. After a minute or two the new Chia container starts and shows ACTIVE status. Click the three-dot menu on the top-right and launch the Shell.

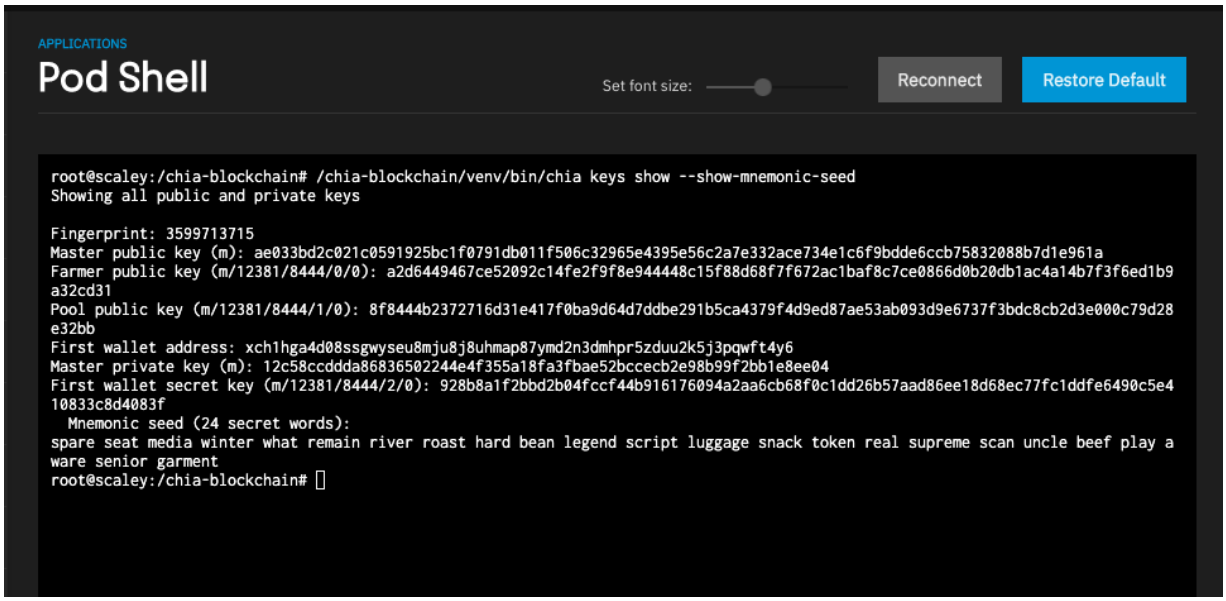


Leave the defaults for the pod (there is only one) and use the selected /bin/bash shell.



The first time Chia launches, it automatically creates a new private key set (for plotting purposes) and wallet. However, the private key set is not preserved across container restarts. To make sure your keys and wallet persist, save the Mnemonic Seed that was created and make sure it gets used at each container initialization. To do this, start by displaying the current key information by running the following shell command:

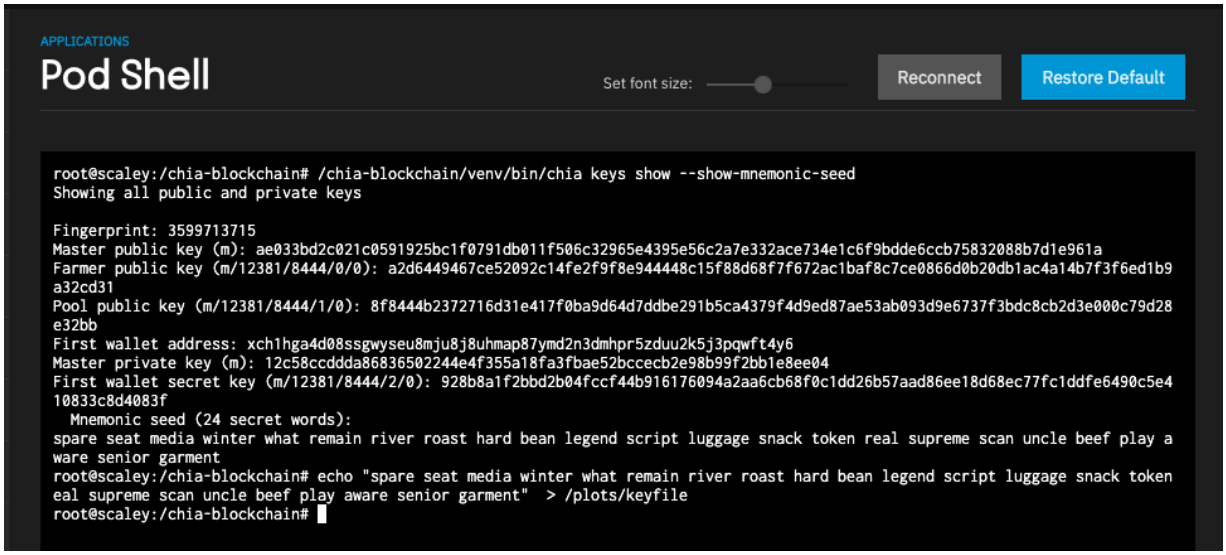
```
/chia-blockchain/venv/bin/chia keys show --show-mnemonic-seed
```



We suggest you make a backup copy of the information provided here for your reference in case you lose the keyfile. To make sure the same key is used for this container going forward, you save the mnemonic-seed phrase to one of your host volumes on TrueNAS.

Copy and paste the 24 secret words of the mnemonic seed into a new shell command:

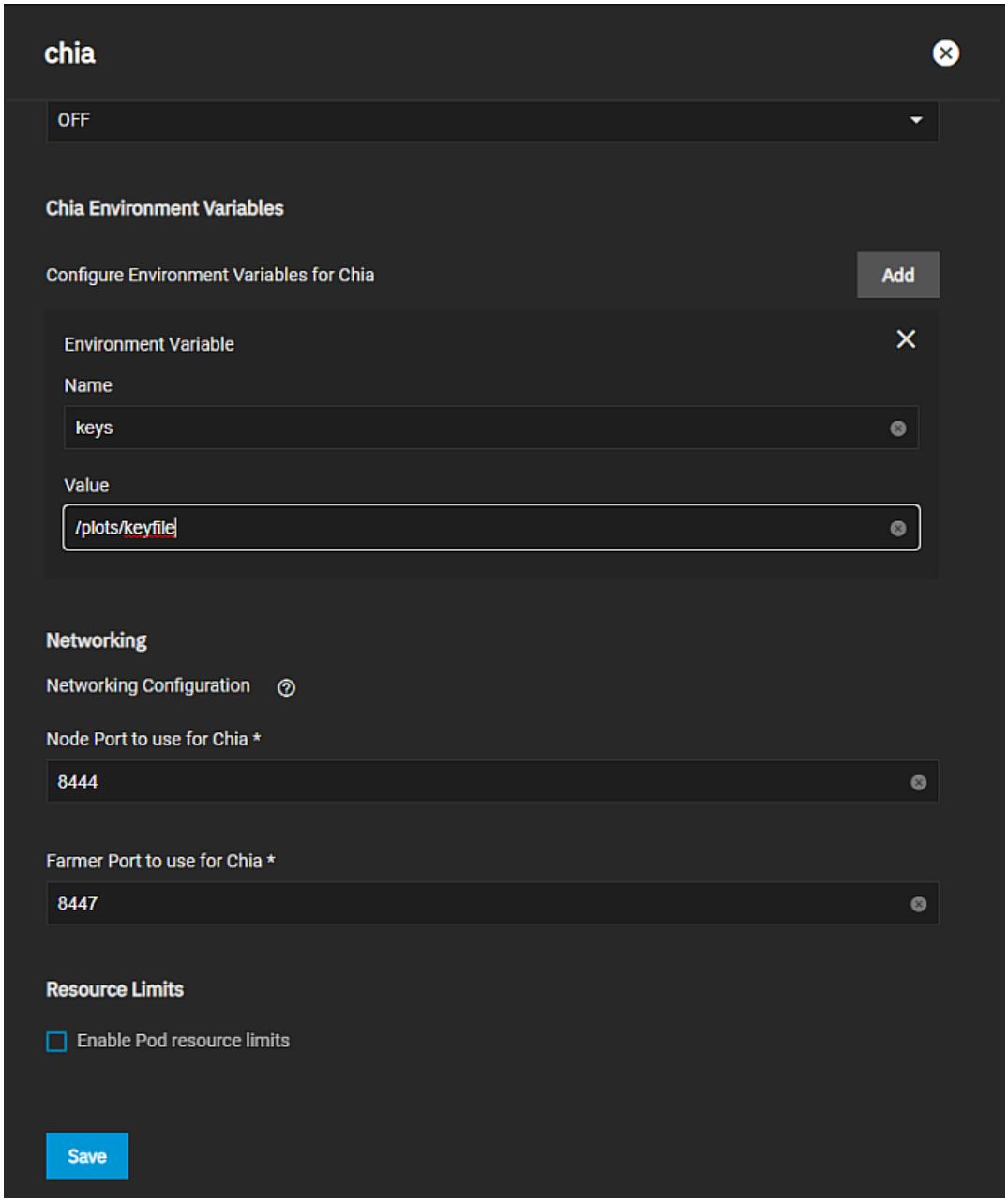
```
echo "my unique 24 secret words here" > /plots/keyfile
```



Now exit the shell and go back to the **Installed Apps** page. Click **Edit** on your Chia container.

Scroll down until you find the **Container Environment Variables** section and add a new variable as shown below:

- Environment Variable Name: keys
- Environment Variable Value: /plots/keyfile



If you entered the command correctly, you should see some output that looks like the screenshot.

Save the change, and the chia container should restart automatically. To confirm your changes have persisted you can log into the containers shell again and run the same `/chia-blockchain/venv/bin/chia keys show --show-mnemonic-seed` command to show your keys. If the keys are identical to what you previously recorded, then you are done! This Chia container persists across reboots, upgrades, and re-deployments.

At this point, you are ready to begin farming Chia. This is a CLI process and beyond the scope of this quick how-to, but we recommend you start by reading up on their CLI reference materials, Quick Start guide and other documentation.

Related Content

- Using SCALE Catalogs

Related Apps Articles

- Applications Screens
- Updating MinIO from 1.6.58
- Using Apps
- Using SCALE Catalogs
- Launch Docker Image Screens
- Using Docker Image
- Adding NextCloud for Media Previews
- Collabora App
- MinIO Clusters

3.7.7 - Collabora App

This article provides basic configuration instructions for adding the Collabora app using the TrueNAS webUI.

The SCALE **Apps** catalogue now includes Collabora from the developers of Nextcloud.

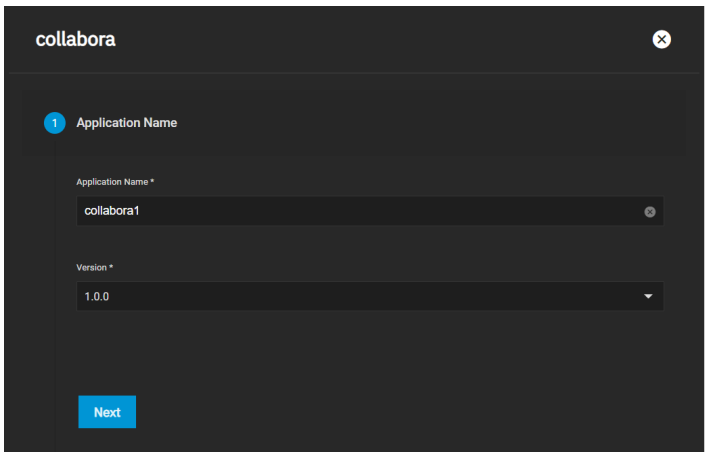
With Collabora, you can host your online office suite at home.

> To integrate Collabora correctly, you must have a Nextcloud account with Collabora added.

Install the Collabora App

Click on the Collabora app **Install** button in the **Available Applications** list.

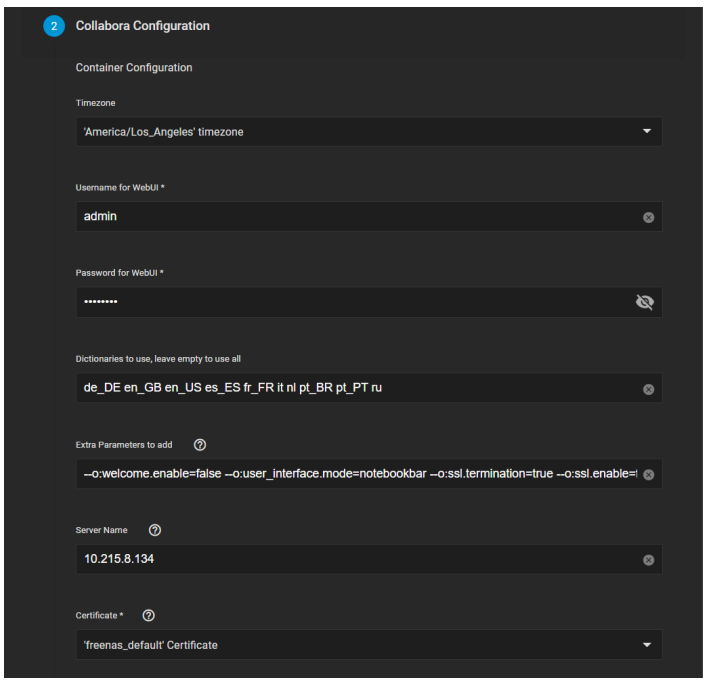
Name your app and click **Next**. In this example, the name is *collabora1*.



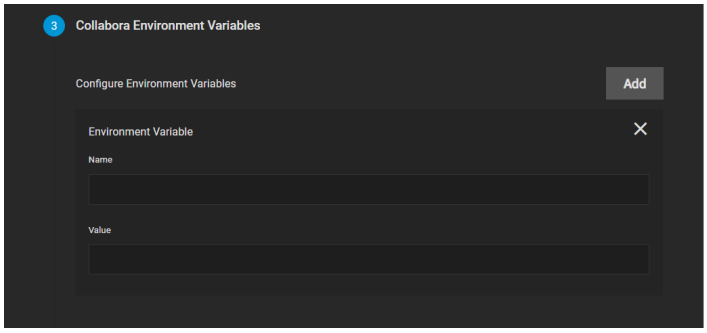
Select a **Timezone** and, if you wish, enter a custom **Username** and **Password**.

You can also add extra parameters to your container as you see fit. See The LibreOffice GitHub Parameters page for more.

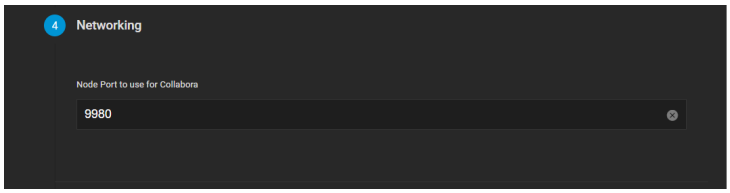
After you select your container settings, choose a **Certificate** and click **Next**.



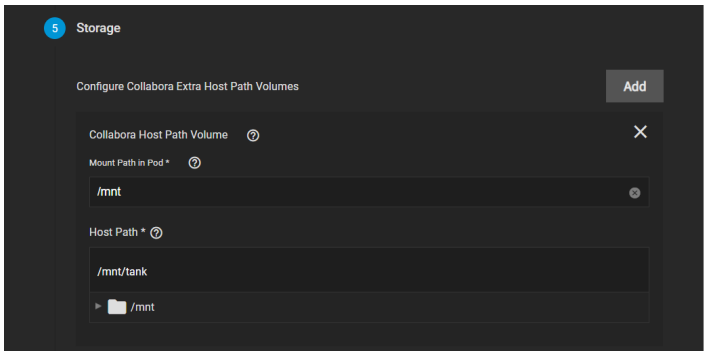
Enter **Environmental Variables** as needed, then click **Next**.



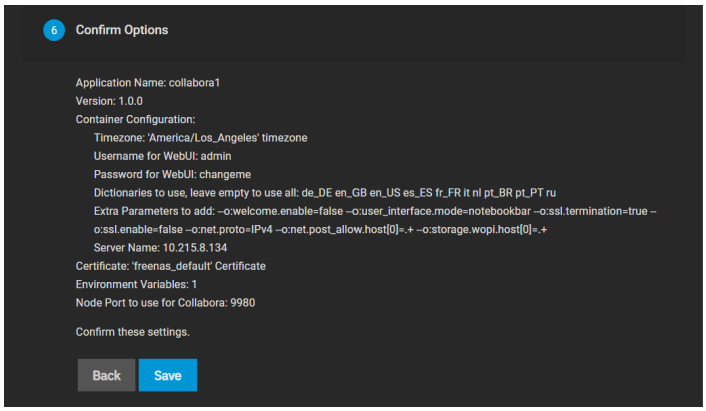
Choose a node port to use for Collabora (we recommend the default), then click **Next**.



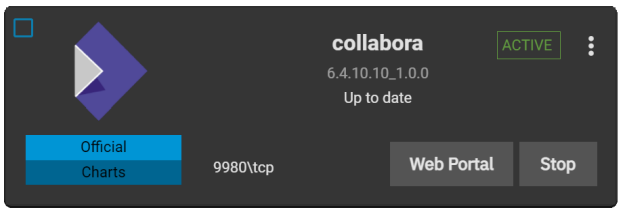
Configure extra host path volumes for Collabora as you see fit, then click **Next**.



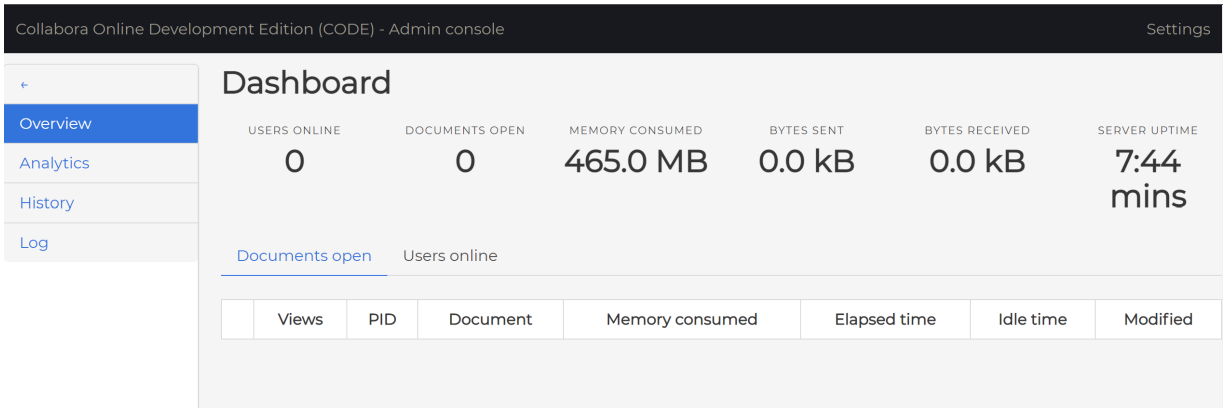
Confirm your Collabora container options and click **Save** to complete setup.



After a few minutes, the Collabora container displays as **ACTIVE**.



After it does, you can click **Web Portal** to access the admin console.



Related Content

Related Apps Articles

- Using SCALE Catalogs
- Configuring the Chia App

3.7.8 - MinIO Clusters

This article provides information on configuring MinIO using the Docker image or the official application widget for MinIO.

On TrueNAS SCALE 20.12-ALPHA and later, users can create a MinIO S3 distributed instance to scale out and handle individual node failures. A node refers to a single TrueNAS storage system in a cluster.

In the images below, we used four TrueNAS systems to create a distributed cluster. For more information on MinIO distributed setups, refer to the MinIO documentation.

First Steps

Before you configure MinIO, you must create a dataset and shared directory for the persistent MinIO data. Go to **Storage > Pools** and select the pool you want to place the dataset in. You can use an existing pool or create a new one.

After creating the dataset, go to **System > Shell** and create the directory MinIO stores information the application uses. MinIO uses **/data** but allows users to replace this with the directory of their choice. Change to the */pool/dataset* directory and then use the `mkdir /mnt/data` command to create the **/data** directory.

For a distributed configuration, repeat this on all system nodes in advance.

Note the system (node) IP addresses or hostnames and have them ready for configuration. Also, have your S3 username and password ready for later.

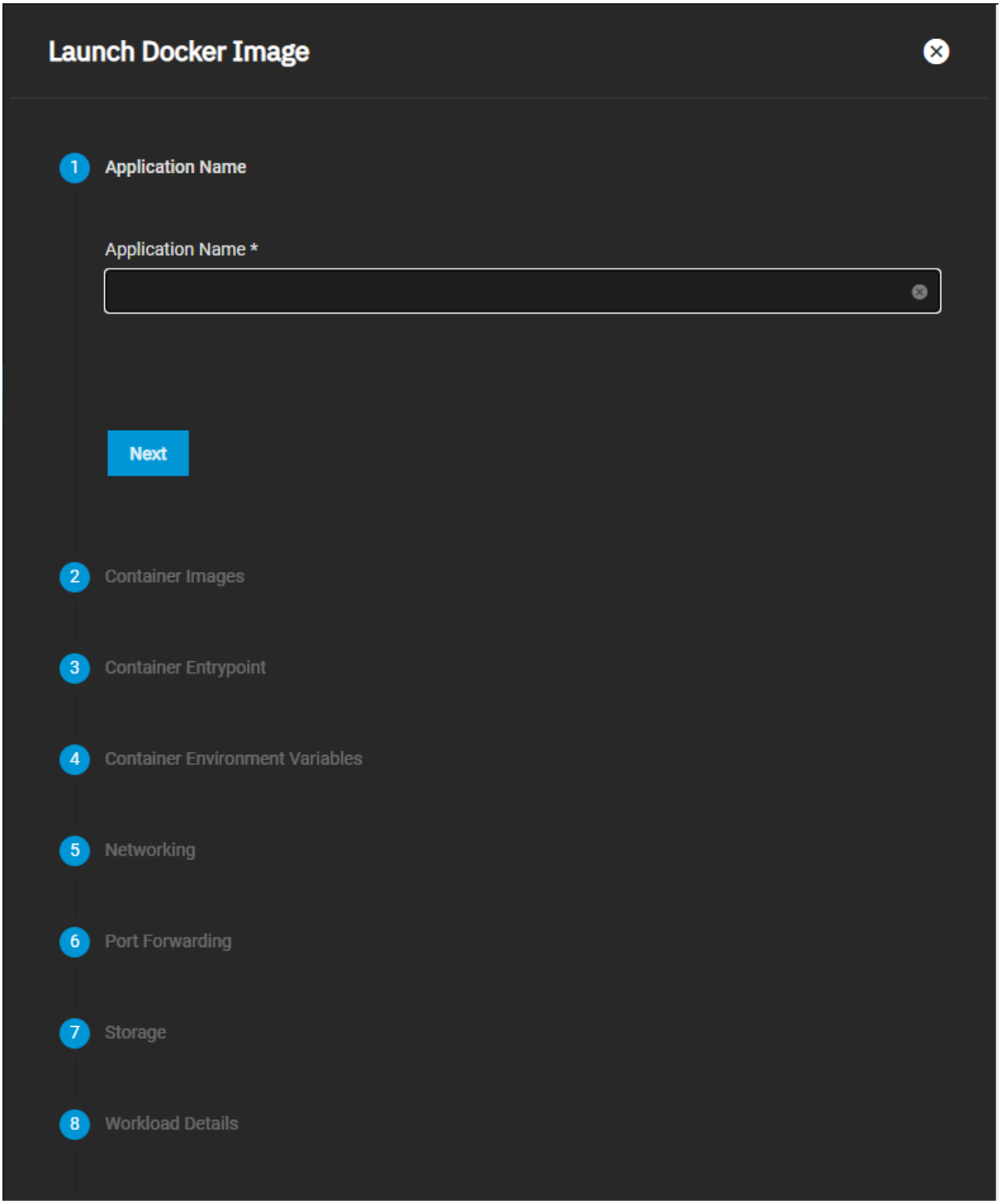
Configuring MinIO

You can configure the MinIO application using either the **Launch Docker Image** button or the **Install** button on the MinIO application card on the **Available Applications** tab.

Setting Up Using Launch Docker Image

Click Here for More Information

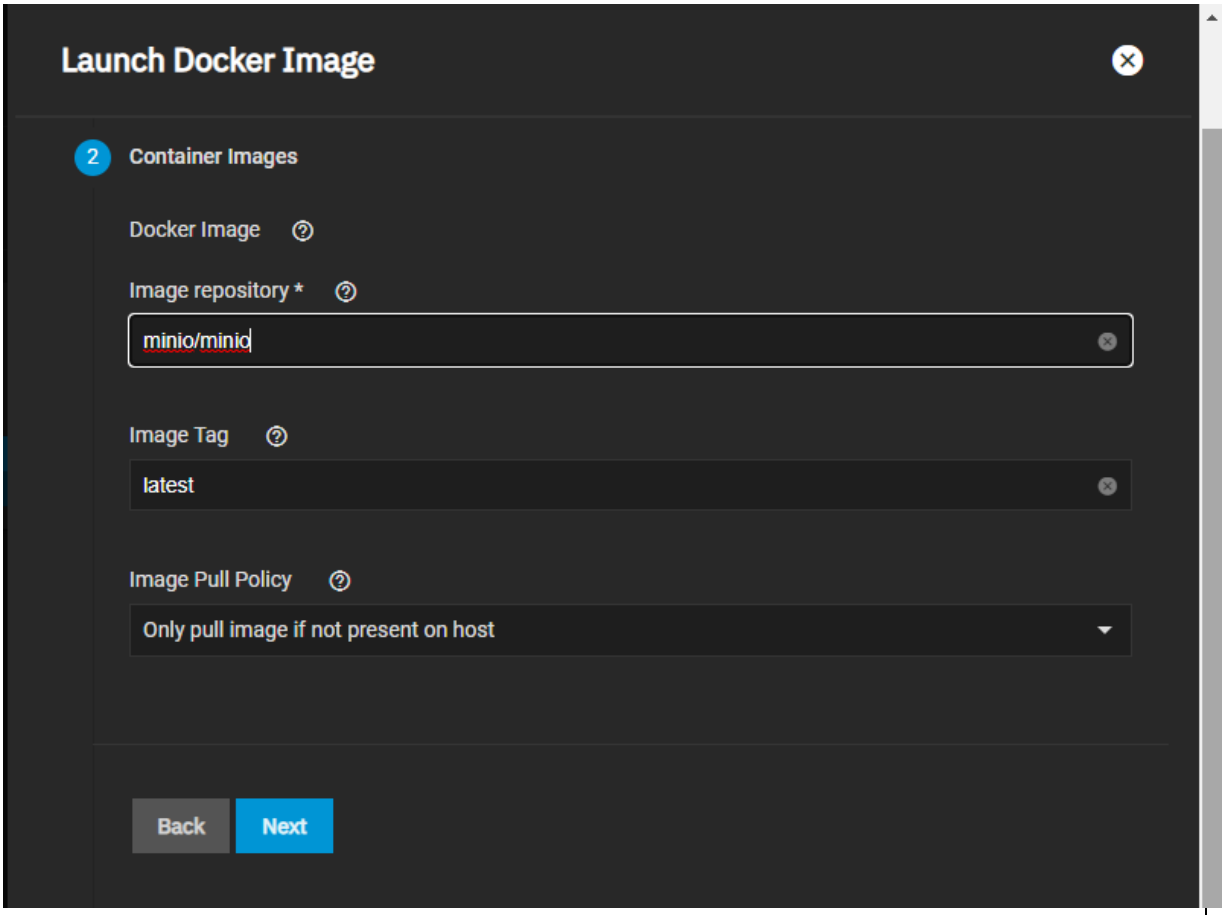
On your first node, go to **Apps** and click **Launch Docker Image**.



First, enter a name in **Application Name** (for example, *minio* for a normal configuration or *minio-distributed* for a distributed MinIO configuration). A MinIO in distributed mode allows you to pool multiple drives (even if they are different machines) into a single object storage server for better data protection in the event of single or multiple node failures because MinIO distributes the drives across several nodes. For more information, see the [Distributed MinIO Quickstart Guide (https://docs.min.io/docs/distributed-minio-quickstart-guide).

Click **Next** to continue after completing each section of the configuration form.

Enter **minio/minio** as the image name under **Image Repository**. Click **Next**.

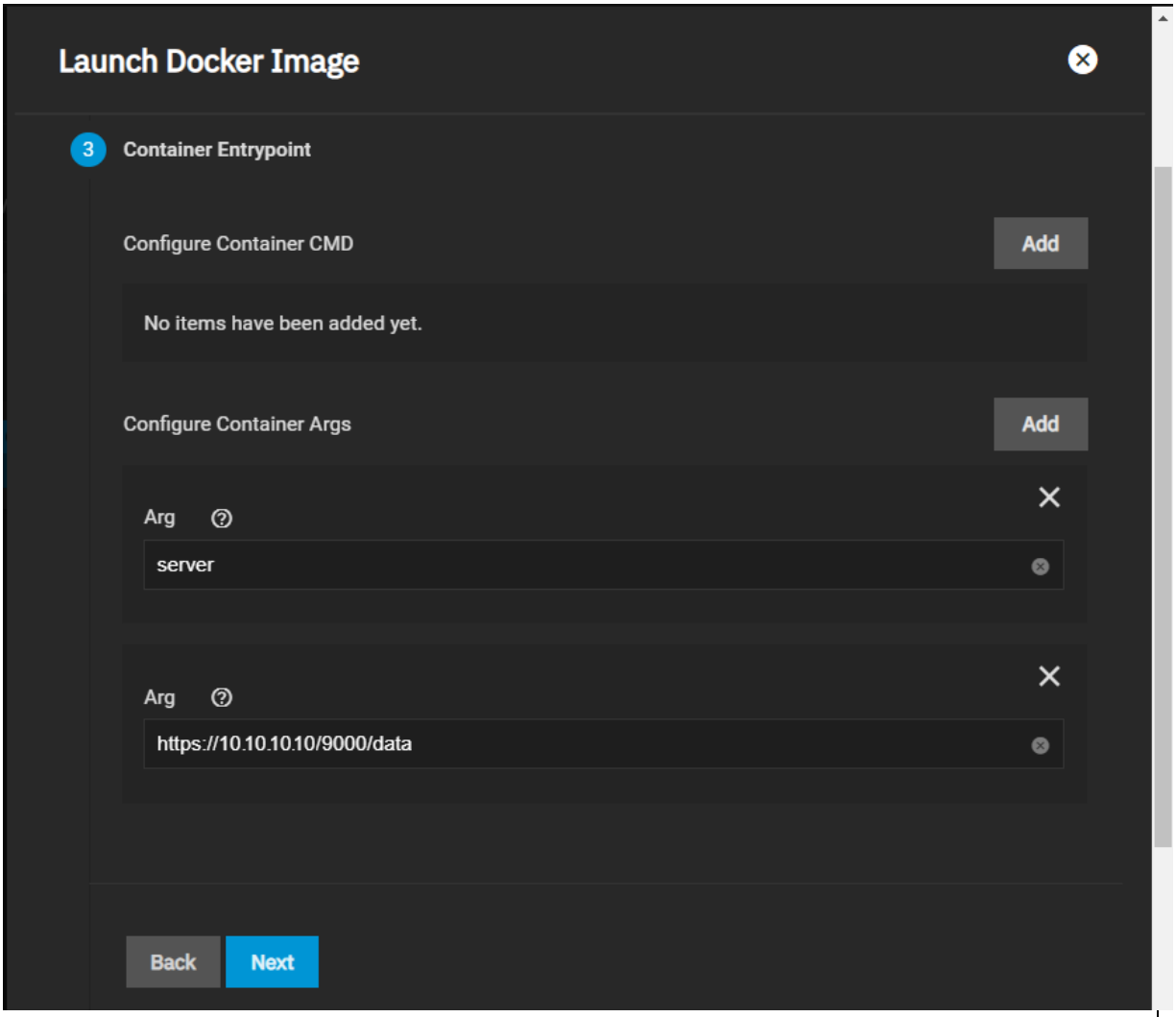


Configure the **Container Entrypoint** arguments. Click the **Add** button to the right of **Configure Container Args** twice to add two **Arg** fields. In the first **Arg** field type **server**. In the second **Arg** field, type the valid IP or hostname of each TrueNAS system on the network, the MinIO port number, and the directory you created for MinIO. Use this format: **http://*0.0.0.0*/9000/data**.

For a distributed cluster, add the valid TrueNAS system (node) IP addresses/hostnames. The order is important, so use the same order across all the nodes.

MinIO containers use server port 9000. The MinIO Console communicates using port 9001.

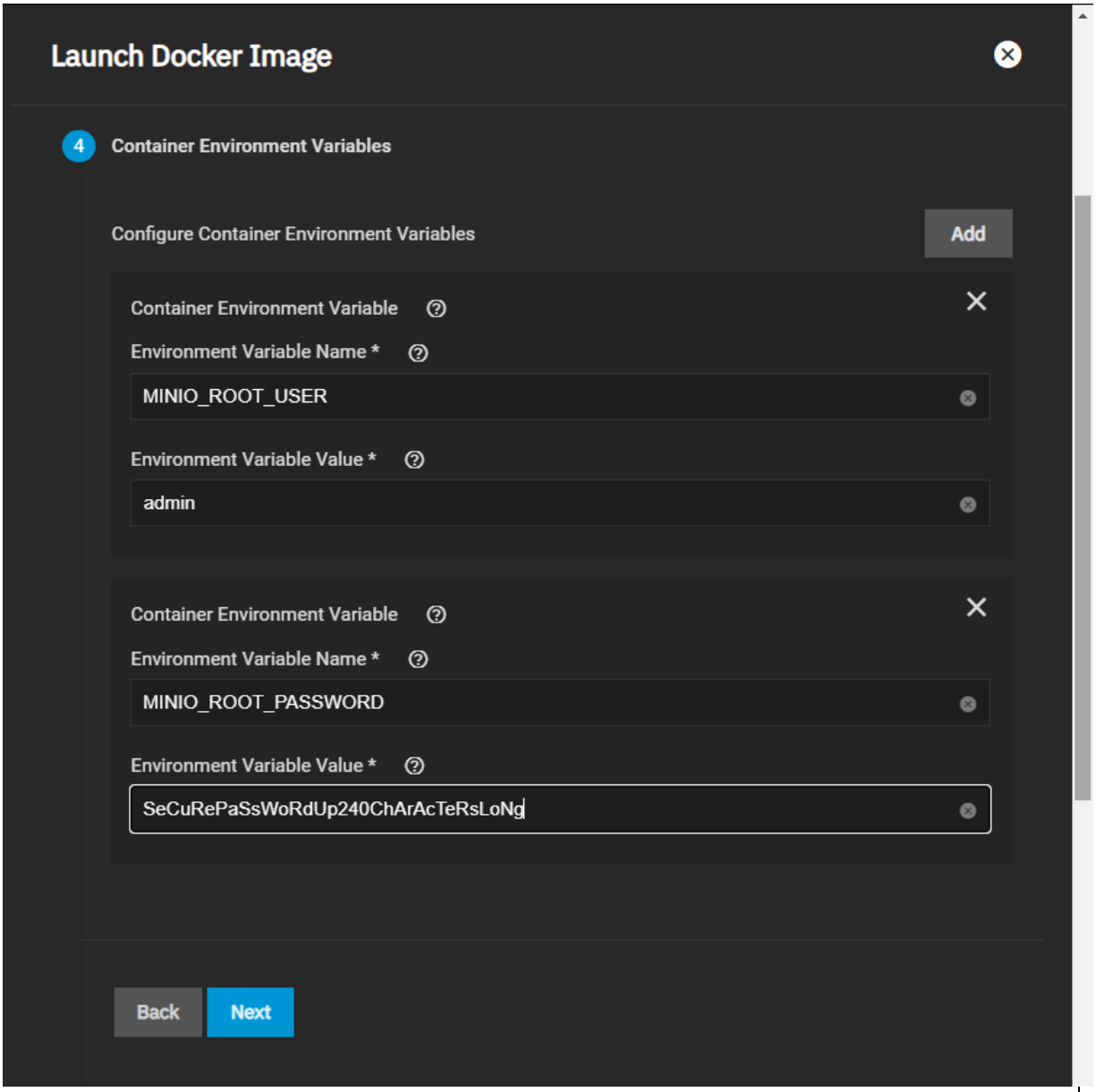
Use the /data path which is set up in the next steps.



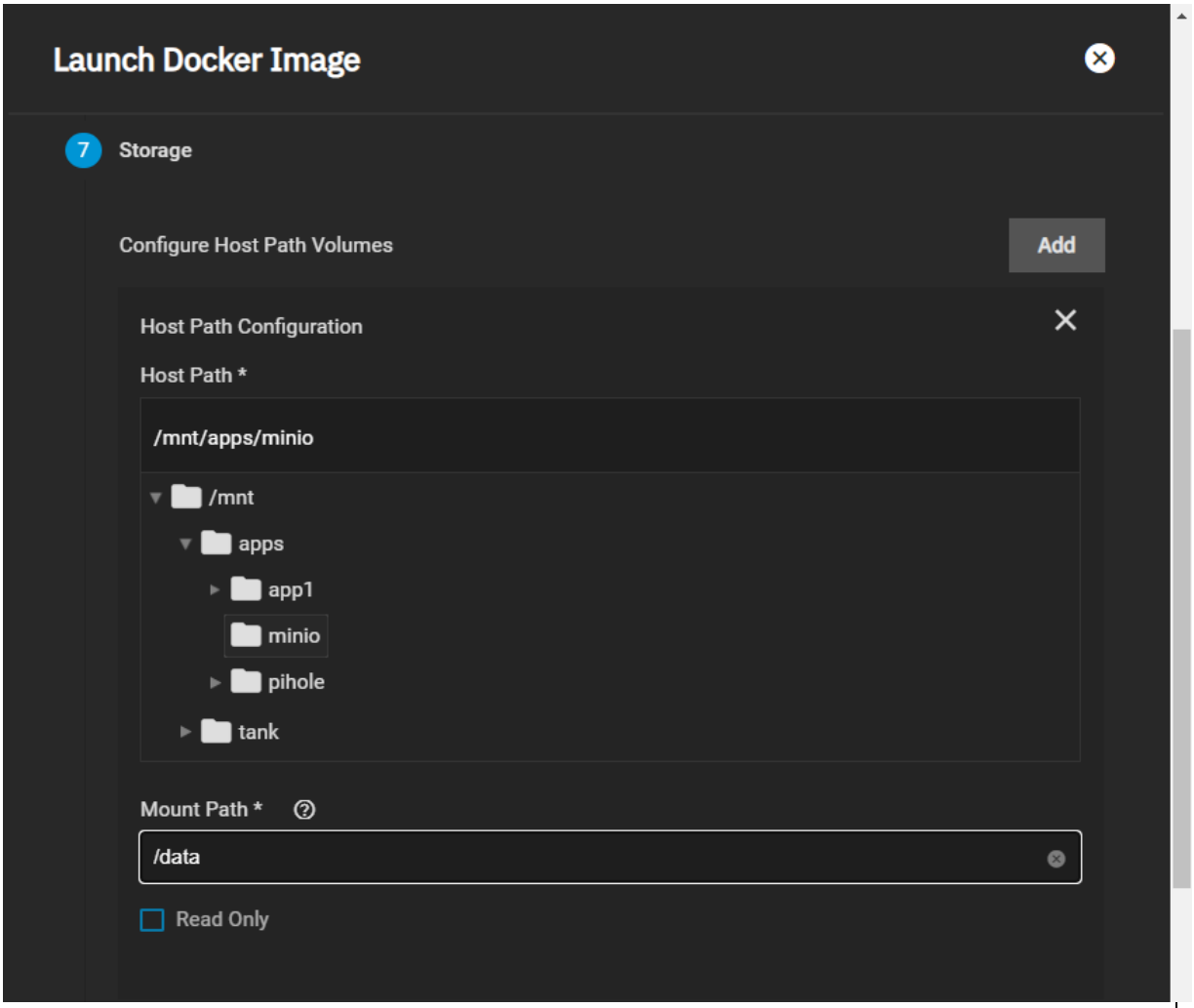
Next, create the **Container Environment Variables** and define the **MINIO_ROOT USER** and **MINIO_ROOT_PASSWORD** arguments and their values. For the **ROOT_USER** value, use a name up to 20 characters. For the **ROOT_PASSWORD**, use a string of 8 to 40 randomized characters. MinIO recommends using a long password string of unique random characters. Refer to MinIO User Management for more information.

> Keep all passwords and credentials secured and backed up.

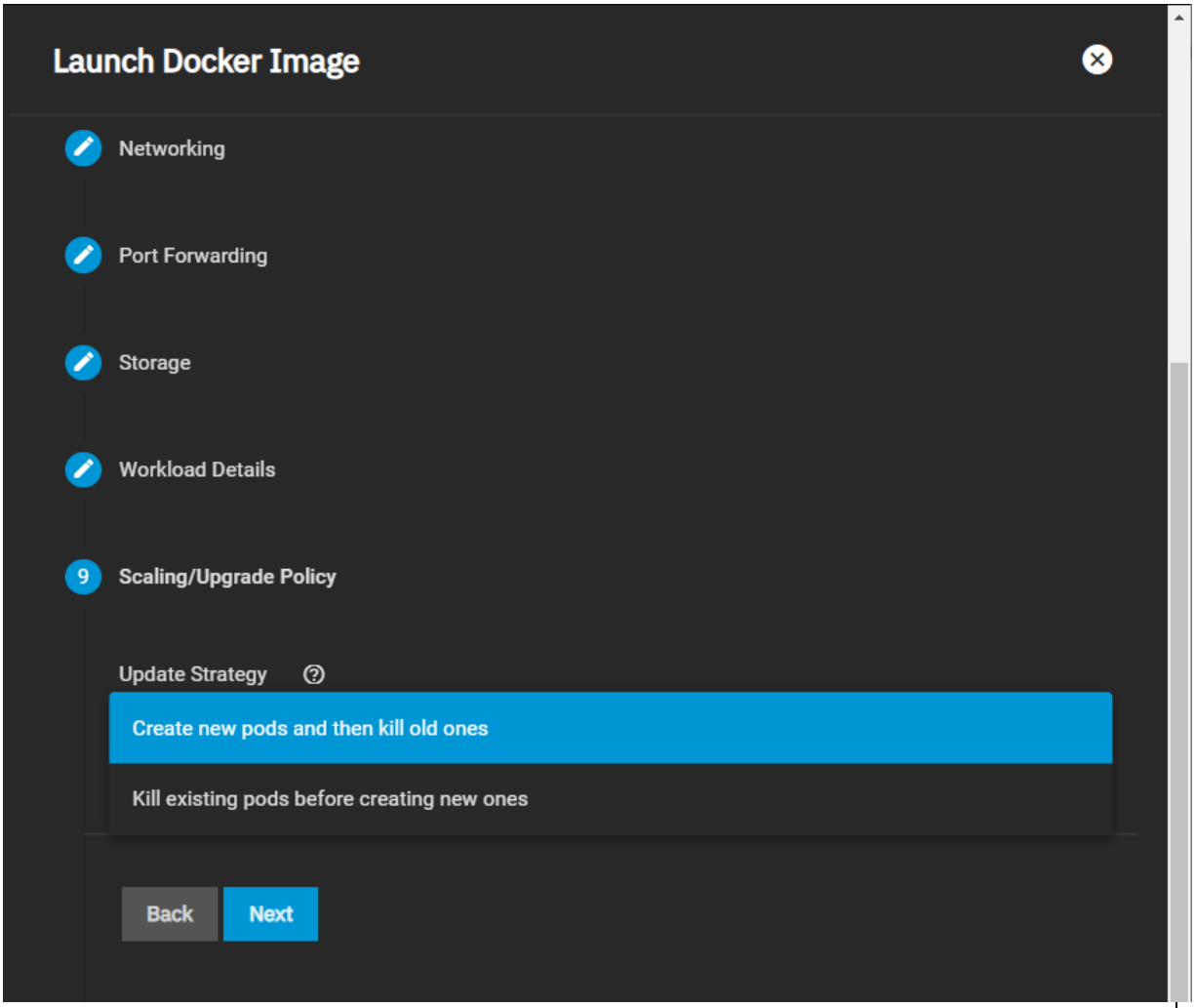
For a distributed cluster, ensure the values are identical between nodes and fill the **Environment Variable Value** with proper random credentials.



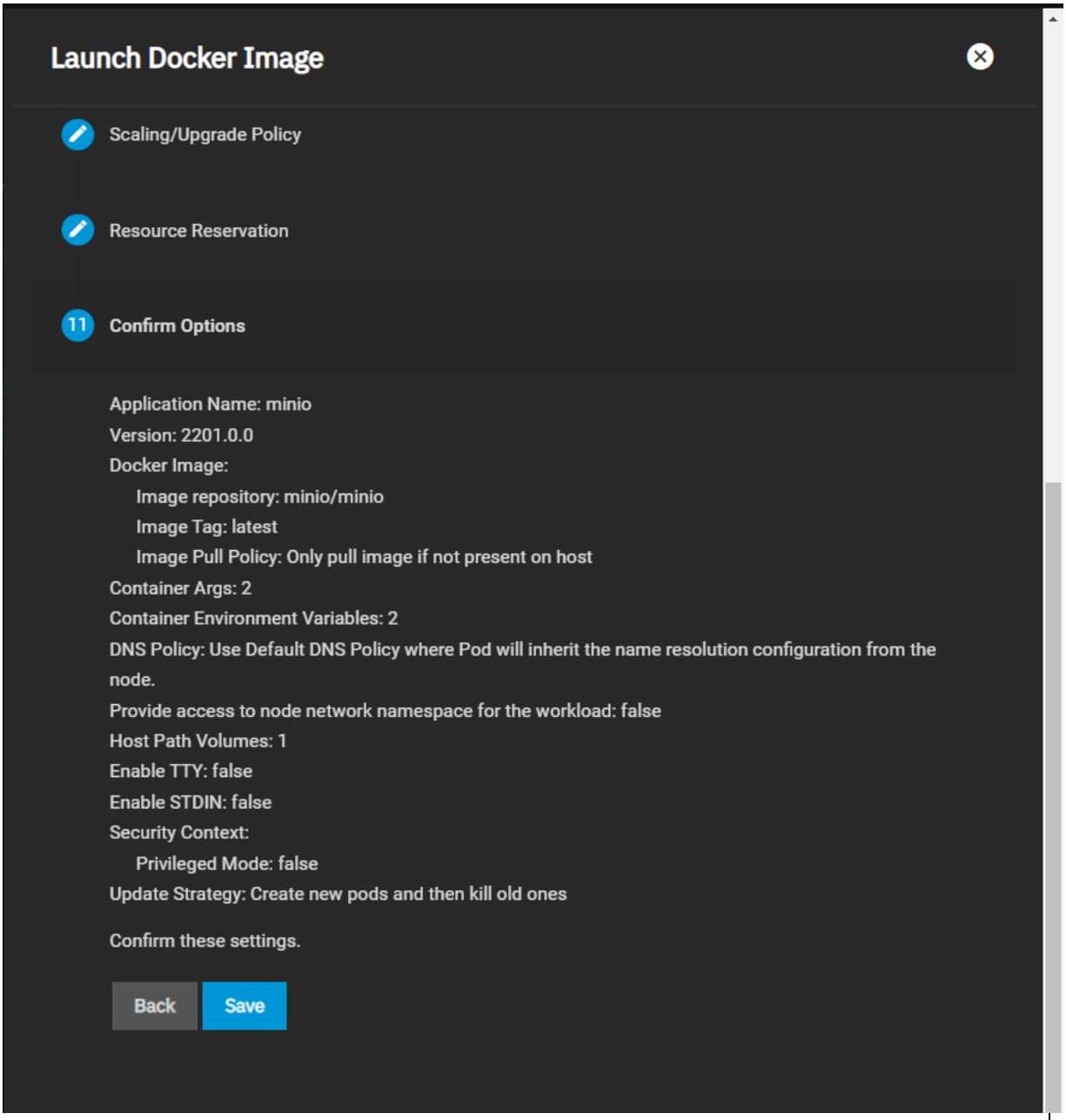
Click **Next** until the **Storage** section displays. Select the dataset you created for the MinIO container for the **Host Path** and enter the **/data** directory under **Mount Path**, then click **Next**.



Click **Next** until you reach the **Scaling/Upgrade Policy** screen. Select the **Update Strategy** option you want to deploy. Use **Kill existing pods before creating new ones** to recreate the container or **Create new pods and then kill old ones** if you want rolling upgrades. Click **Next**.



Confirm your options, then click **Save** to complete the first node.



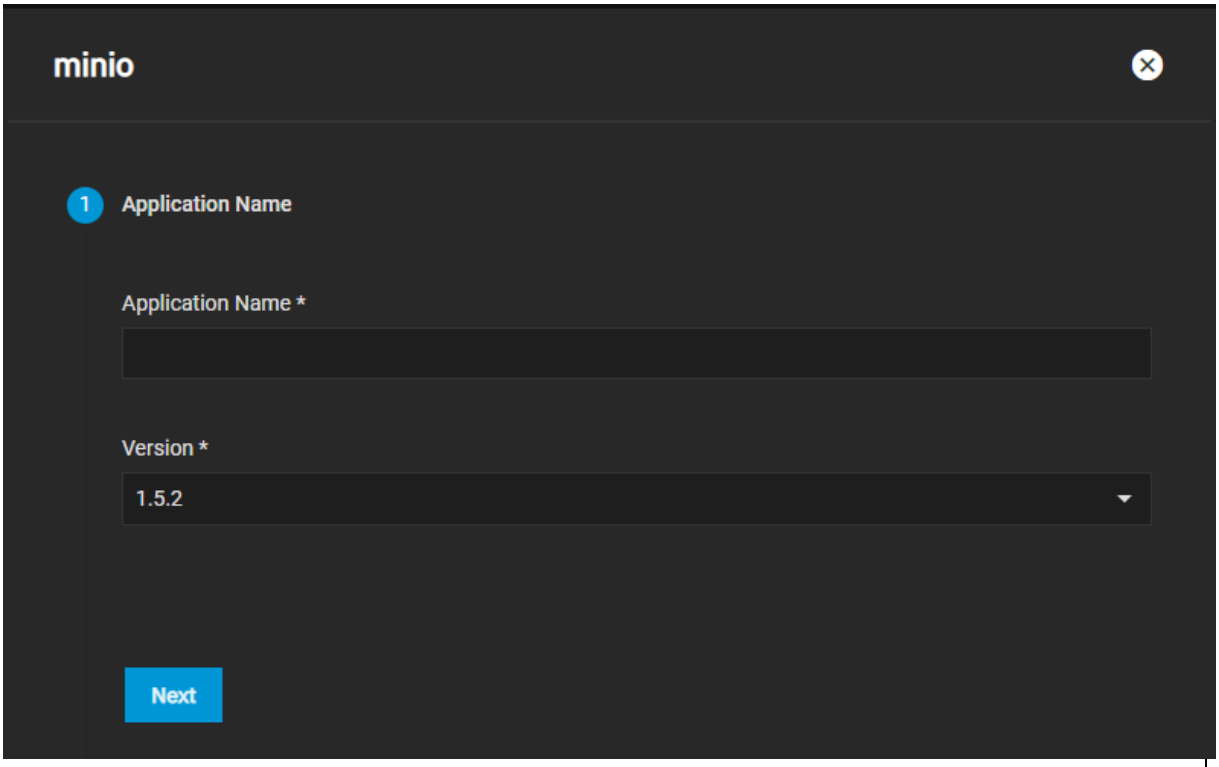
Now that the first node is complete, you can configure any remaining nodes (including datasets and directories).

Setting Up Using MinIO Install

Setting Up Using MinIO Install

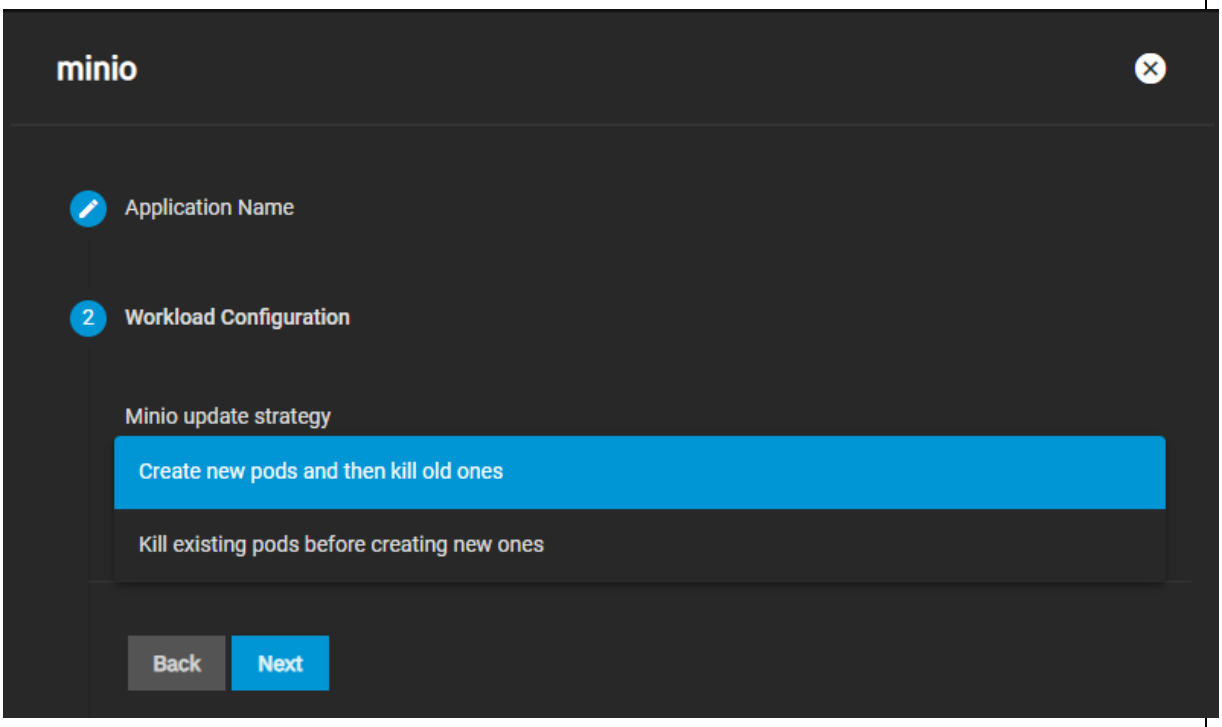
Go to **Apps** and select the **Available Applications** tab to display the MinIO application card. Click **Install** on the MinIO card to open the MinIO configuration wizard.

First, enter a name for the MinIO cluster. Click **Next**. Type the name in all lowercase.



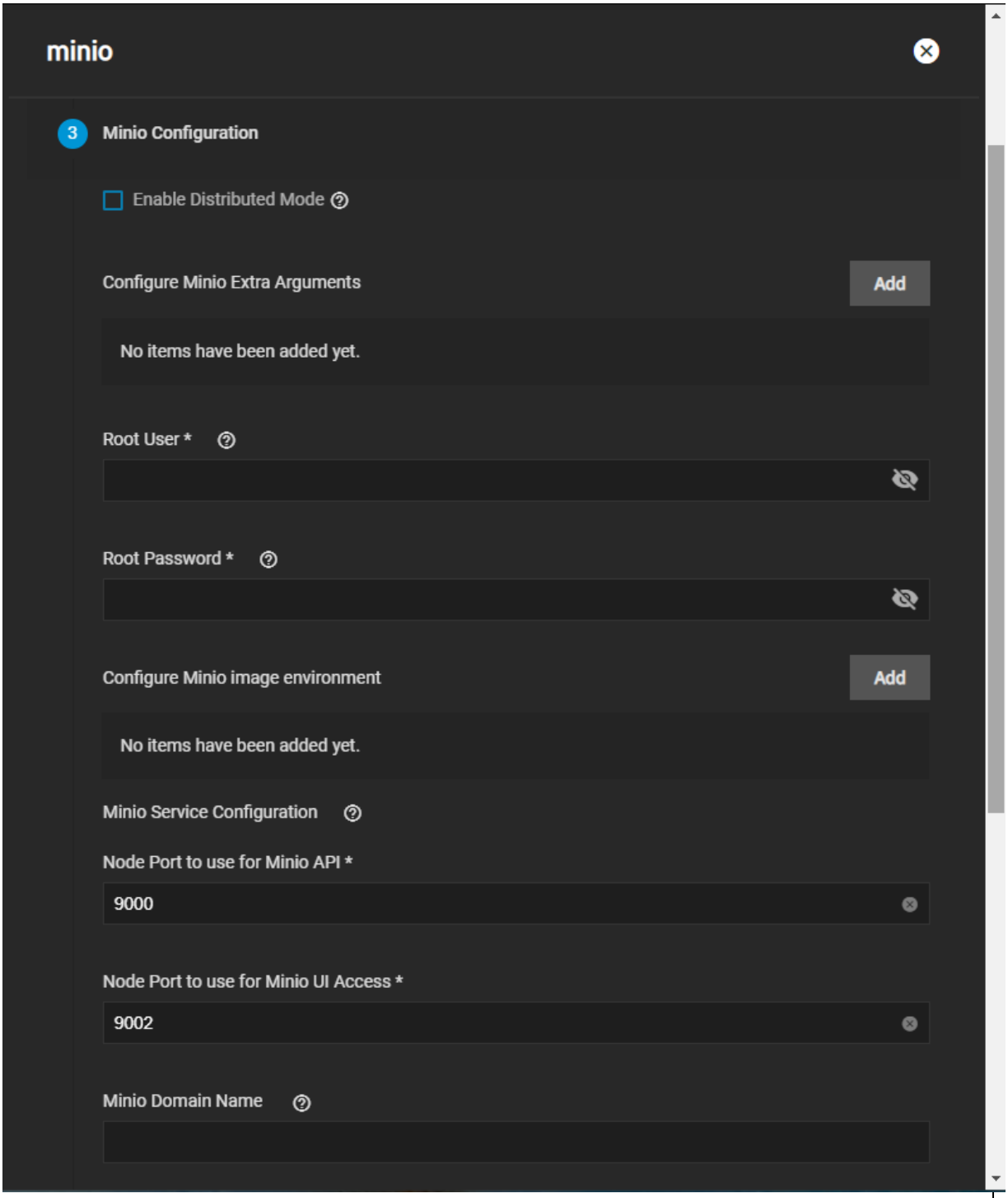
Next, add the **Workload Configuration** settings.

Select an update strategy. Use **Kill existing pods before creating new ones** to recreate the container or **Create new pods and then kill old ones** if you want rolling upgrades. We recommend **Kill existing pods before creating new ones**. Click **Next**.



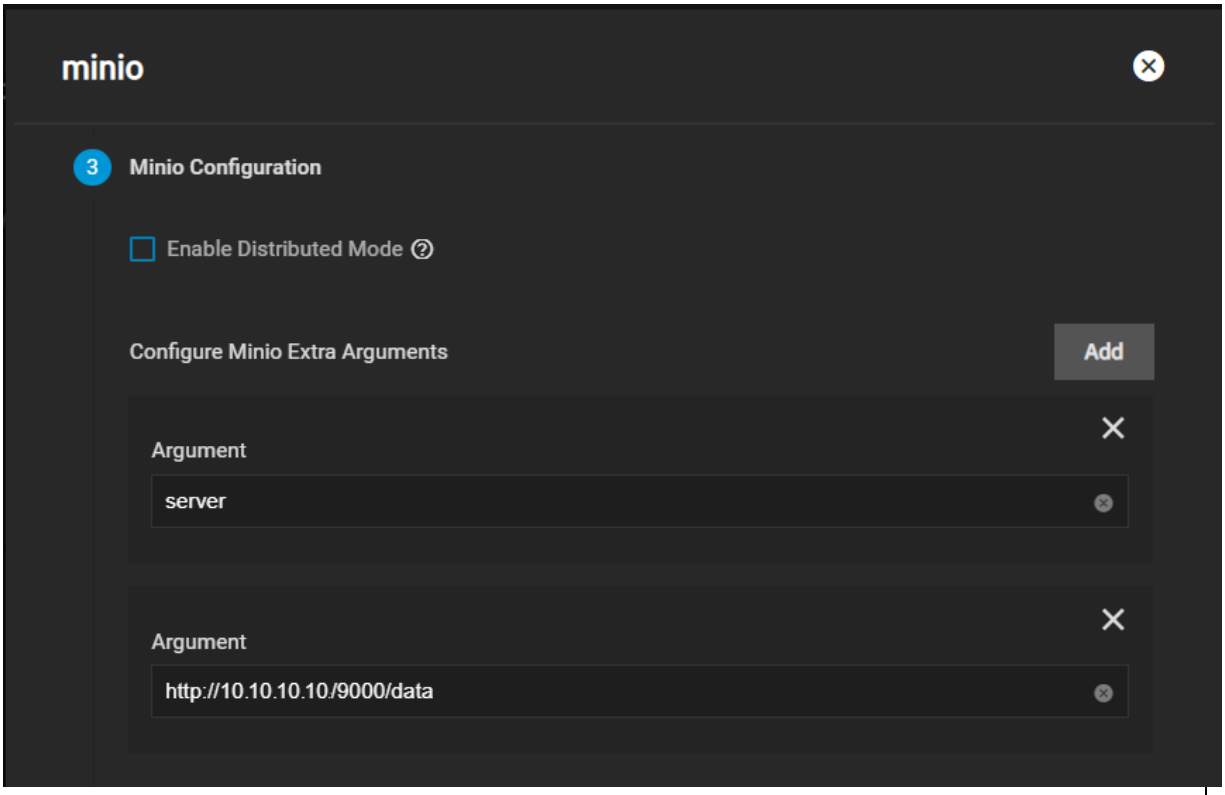
Now enter the **MinIO Configuration** settings.

If you want to run your MinIO instance to connect to a distributed MinIO cluster, set **Enable Distributed Mode** and input your Distributed Minio Instance URI. See the Distributed MinIO Quickstart Guide for more information.



Click the **Add** button to the right of **Configure MinIO Extra Arguments** twice to display two **Arg** fields. In the first **Arg** field type **server**. In the second **Arg** field type the valid IP or hostname of each TrueNAS systems on the network, the MinIO port number, and the directory you created for MinIO. Use this format, **http://*0.0.0.0*/9000/data**.

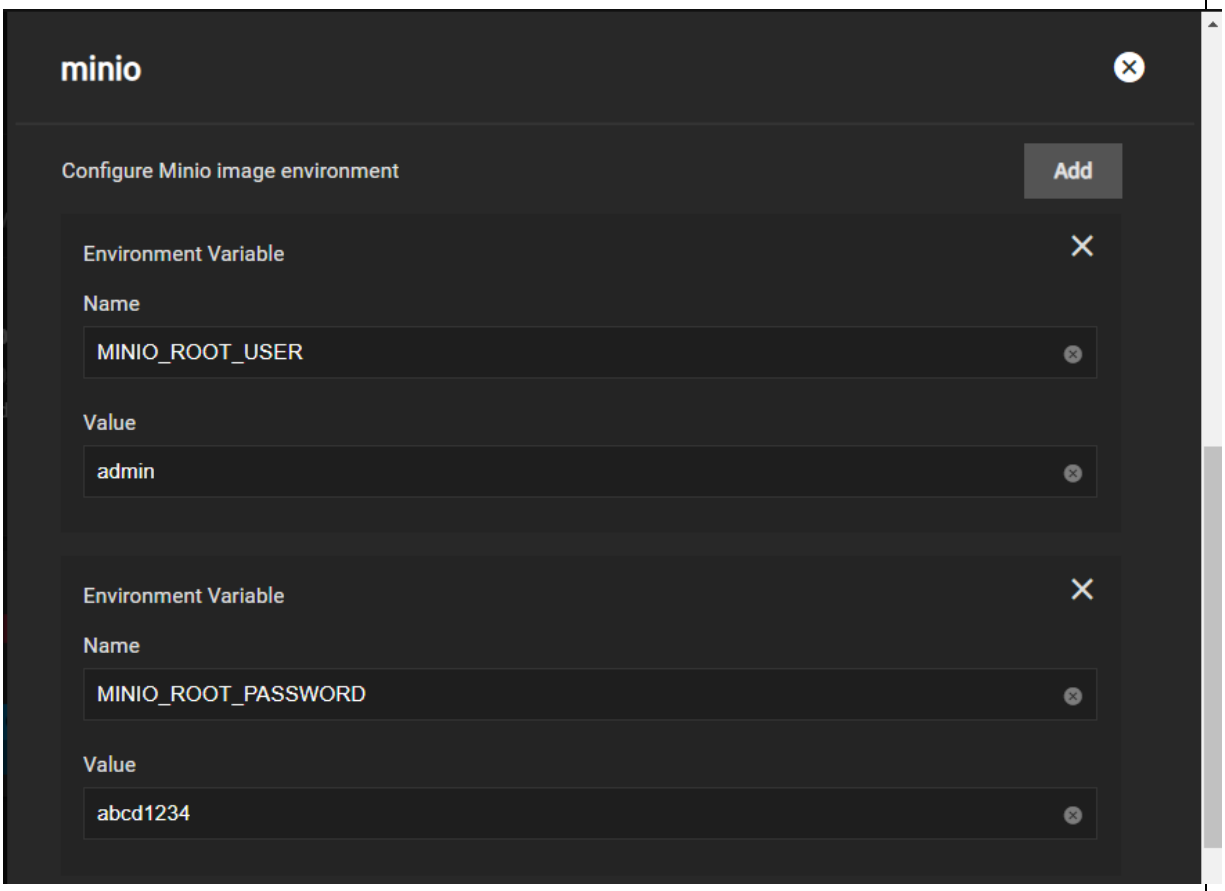
Add the other valid TrueNAS system IP addresses/hostnames of your various nodes. The order is important, so use the same order across all the nodes. MinIO containers use server port 9000. The MinIO UI communicates using port 9002.



Enter the S3 root user in **Root User** and the S3 password in the **Root Password** fields.

Click the **Add** button to the right of **Container Environment Variables** and enter the **MINIO_ROOT_USER** and **MINIO_ROOT_PASSWORD** arguments and values. For the **ROOT_USER** value, use a name up to 20 characters. For the **ROOT_PASSWORD**, use 8 to 40 randomized characters. MinIO recommends using a long password string of unique random characters. Refer to MinIO User Management for more information.

> Keep all passwords and credentials secured and backed up.

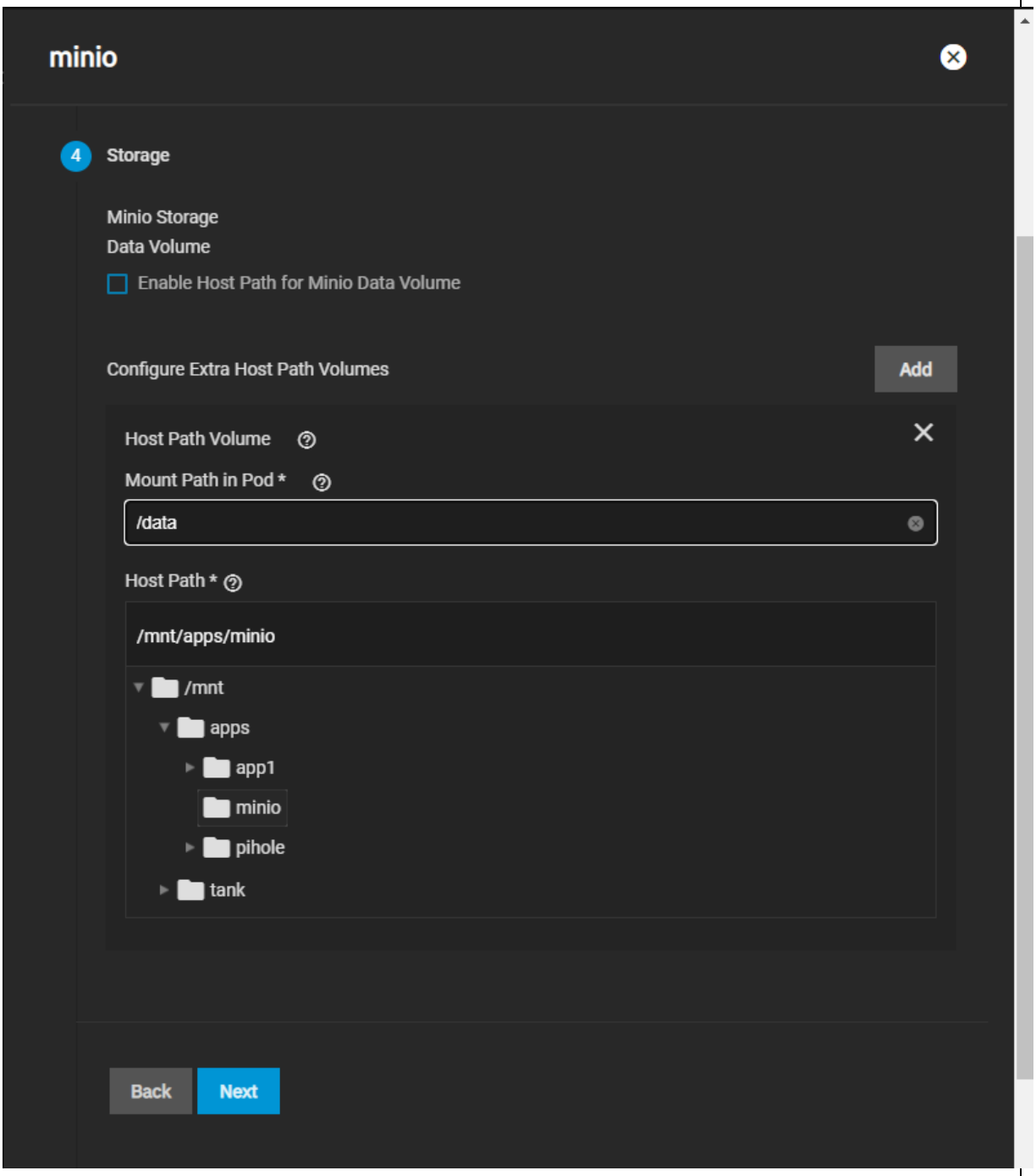


You can configure the API and UI access node ports and the MinIO domain name if you have TLS configured for MinIO. You can also configure a MinIO certificate if you wish.

Now enter the **Storage** settings.

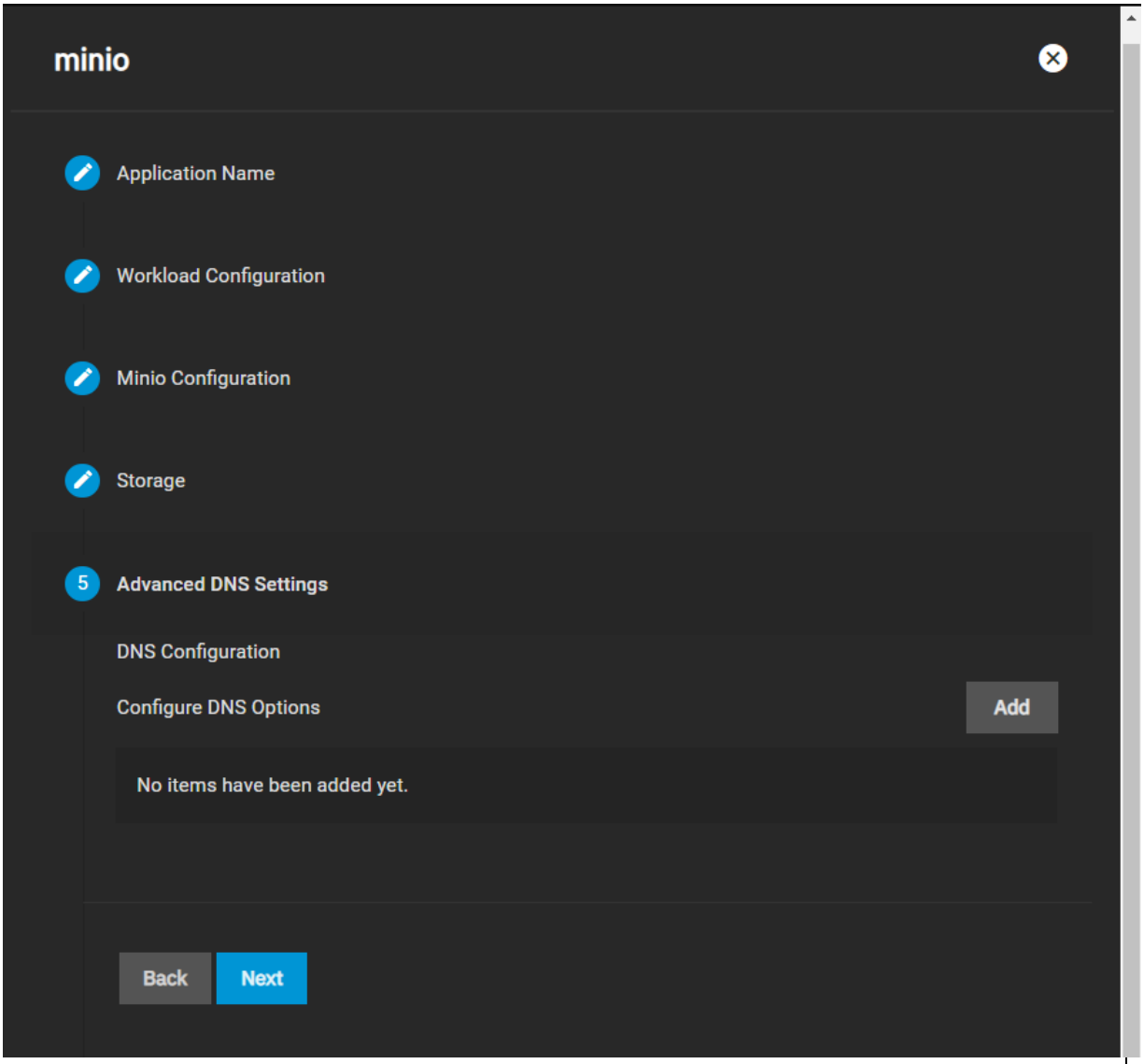
If you want to use a host path to store your MinIO data volume, select the **Enable Host Path for MinIO Data Volume** checkbox and select a path.

Under **Configure Extra Host Path Volumes**, enter the /data directory under **Mount Path in Pod**, then select the directory or dataset you created earlier and click **Next**.



Add the **Advanced DNS Settings** next.

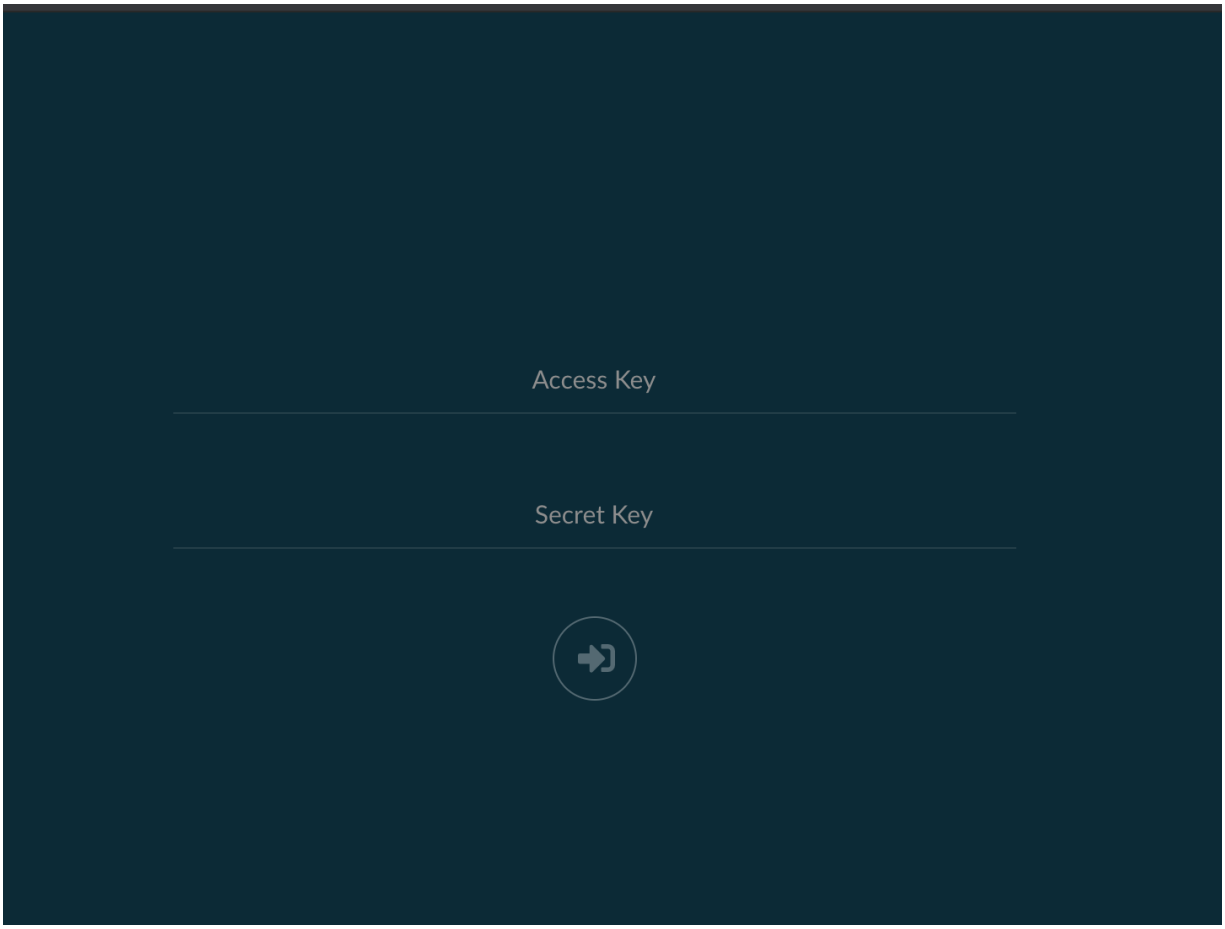
You can configure additional DNS options in Advanced DNS Settings. Click **Add** to add more DNS option entries. Click **Next**.



Finally, confirm options. Make sure the configuration summary meets your needs, then click **Save**.

Accessing the Minio Setup

Once you're done creating datasets, you can navigate to the TrueNAS address at port **:9000** to see the MinIO UI. If you created a distributed setup, you can see all your TrueNAS addresses. Log in with the **ROOT_USER** and **ROOT_PASSWORD** keys you created as Container Environment Variables.



Related Content

- Updating MinIO from 1.6.58
- Using SCALE Catalogs
- Configuring S3 Service
- S3 Service Screen

Related Apps Articles

- Applications Screens
- Updating MinIO from 1.6.58
- Using Apps
- Using SCALE Catalogs
- Launch Docker Image Screens
- Using Docker Image
- Adding NextCloud for Media Previews
- Configuring the Chia App
- Collabora App

3.7.8.1 - Updating MinIO from 1.6.58

This article provides information on updating MinIO from 1.6.58 to newer versions.

Overview

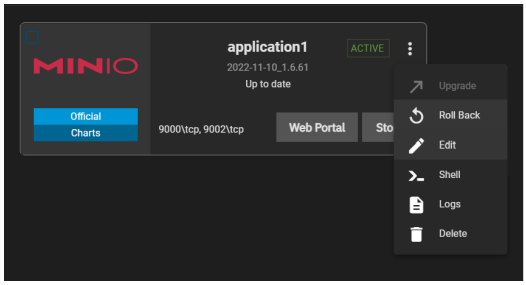
MinIO fails to deploy if you update your version 2022-10-24_1.6.58 Minio app to 2022-10-29_1.6.59 or later using the TrueNAS web UI.

Your app logs display an error similar to the following:

```
ERROR Unable to use the drive /export: Drive /export: found backend type fs, expected xl or xl-single: Invalid arguments specified.
```

If you get this error after upgrading your MinIO app, use the app **Roll Back** function and return to 2022-10-24_1.6.58 to make your MinIO app functional again.

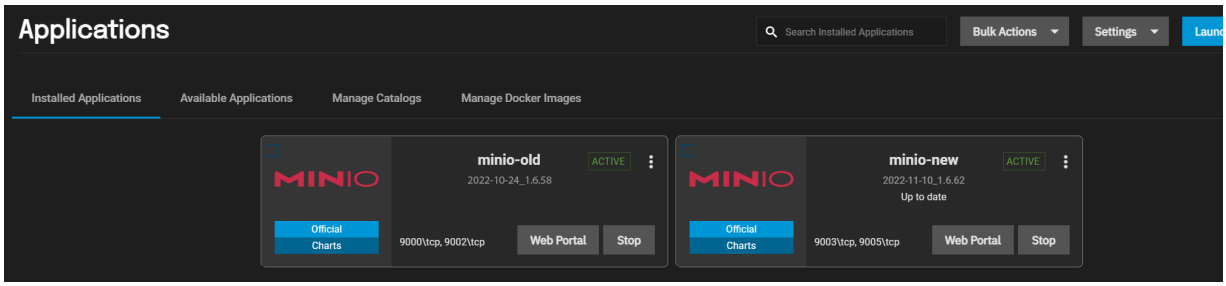
You will need WSL2 (Windows Subsystem for Linux) if you are using a Windows computer.



Manual Update Process

Create a New MinIO Deployment

Follow the instructions here to make a new, up-to-date MinIO deployment in TrueNAS. Make sure it is version 2022-10-29_1.6.59 or later.



Download MinIO Client

Download the MinIO Client here for your OS and follow the installation instructions. The MinIO Client (mc) lets you create and manage MinIO deployments via your system command prompt.

Add both TrueNAS MinIO Deployments to MC

Open a terminal or CLI.

If you are on a Windows computer, open PowerShell and enter `wsl` to switch to the Linux subsystem.

Change directories to the folder that contains mc.exe.

Add your old deployment to mc by entering: `./mc alias set old-deployment-name http://IPaddress:port/ rootuser rootpassword`.

Example

`old-deployment-name` is your old MinIO app name in TrueNAS.

`http://IPaddress:port/` is the IP address and port number the app uses.

`rootuser` is the root username.

`rootpassword` is the root password.

```
root@01-USER:/mnt/c/Users/User/Downloads# ./mc.exe alias set minio-old http://10.220.1.163:9000/ rootuser rootpass
Added `minio-old` successfully.
```

Add your new deployment to mc using the same command with the new alias: `./mc alias set new-deployment-name http://IPaddress:port/ rootuser rootpassword`.

Example

`new-deployment-name` is your new MinIO app name in TrueNAS.

`http://IPaddress:port/` is the IP address and port number the app uses.

`rootuser` is the root username.

`rootpassword` is the root password.

```
root@01-USER:/mnt/c/Users/User/Downloads# ./mc.exe alias set minio-new http://10.220.1.163:9003/ rootuser rootpass
Added `minio-new` successfully.
```

Port the configurations from the old MinIO deployment into the new one.

Export your old MinIO app configurations by entering `./mc.exe admin config export old-deployment-name > config.txt`.

MinIO Client exports the config file to the current directory path.

Example

`old-deployment-name` is your old MinIO app name in TrueNAS.

```
root@01-USER:/mnt/c/Users/User/Downloads# ./mc.exe admin config export minio-old > config.txt
```

In this case, the config file exports to the User Downloads folder.

Import the old app config file into the new app by entering: `./mc.exe admin config import old-deployment-name < config.txt`.

Example

`new-deployment-name` is your new MinIO app name in TrueNAS.

`config.txt` is the config file name.

```
root@01-USER:/mnt/c/Users/User/Downloads# ./mc.exe admin config import minio-new < config.txt
Setting new key has been successful.
Please restart your server with `mc admin service restart minio-new`.
```

Restart the MinIO service

Restart the new MinIO app to apply the configuration changes.

`./mc.exe admin service restart new-minio-deployment`

Example

`new-deployment-name` is your new MinIO app name in TrueNAS.

```
root@01-USER:/mnt/c/Users/User/Downloads# ./mc.exe admin service restart minio-new
Restart command successfully sent to `minio-new`. Type Ctrl-C to quit or wait to follow the status of the restart process.
...
Restarted `minio-new` successfully in 1 seconds
```

Port bucket data from the old deployment into the new one.

Export the old app bucket metadata by entering `./mc.exe admin cluster bucket export old-minio-deployment`.

Import the metadata into the new app with `./mc.exe admin cluster bucket import new-minio-deployment cluster-metadata.zip`

Example

`old-deployment-name` is your old MinIO app name in TrueNAS.

`new-deployment-name` is your new MinIO app name in TrueNAS.

`cluster-metadata.zip` is the metadata zip file name.

```
root@01-USER:/mnt/c/Users/User/Downloads# ./mc.exe admin cluster bucket export minio-old
mc.exe: Bucket metadata successfully downloaded as cluster-metadata.zip
```

```
root@01-USER:/mnt/c/Users/User/Downloads# ./mc.exe admin cluster bucket import minio-new cluster-metadata.zip

1/1 buckets were imported successfully.
```

Port Identity and Access Management (IAM) Settings

Export the old app IAM settings by entering `./mc.exe admin cluster iam export old-minio-deployment`.

Import the IAM settings into the new app with `./mc.exe admin cluster iam import new-minio-deployment alias-iam-info.zip`.

Example

`old-deployment-name` is your old MinIO app name in TrueNAS.

`new-deployment-name` is your new MinIO app name in TrueNAS.

`alias-iam-info.zip` is the IAM settings zip file name.

```
root@01-USER:/mnt/c/Users/User/Downloads# ./mc.exe admin cluster bucket export minio-old
mc.exe: Bucket metadata successfully downloaded as cluster-metadata.zip
```

```
root@01-USER:/mnt/c/Users/User/Downloads# ./mc.exe admin cluster iam import minio-new minio-old-iam-info.zip
mc.exe: IAM info imported to minio-new from minio-old-iam-info.zip
```

Move Objects and Data

Create buckets in your new MinIO app to move data and objects to.

Move the objects and data from your old MinIO app to your new one using `./mc.exe mirror --preserve --watch source/bucket target/bucket`.

Repeat for every bucket you intend to move.

Example

`source/bucket` is your old MinIO app name in TrueNAS and one of its buckets.

`target/bucket` is your new MinIO app name in TrueNAS and one of its buckets.

```
root@01-USER:/mnt/c/Users/User/Downloads# ./mc.exe mirror --preserve --watch minio-old/bucket1 minio-new/bucket1
...bucket1/Migration.txt: 398 B / 398 B [=============================================================================================================] 1 B/s
```

Delete Old App

After you have moved all data from the old app to the new one, return to the TrueNAS UI **Apps** screen and stop both Minio apps.

Delete the old MinIO app. Edit the new one and change the API and UI Access Node Ports to match the old MinIO app.

Restart the new app to finish migrating.

Related Content

- Using SCALE Catalogs
- MinIO Clusters
- Configuring S3 Service
- S3 Service Screen

3.7.9 - Adding Pi-Hole Using Docker Image

This article provides information on using the Docker image wizard to configure third-party applications like Pi-Hole in TrueNAS SCALE.

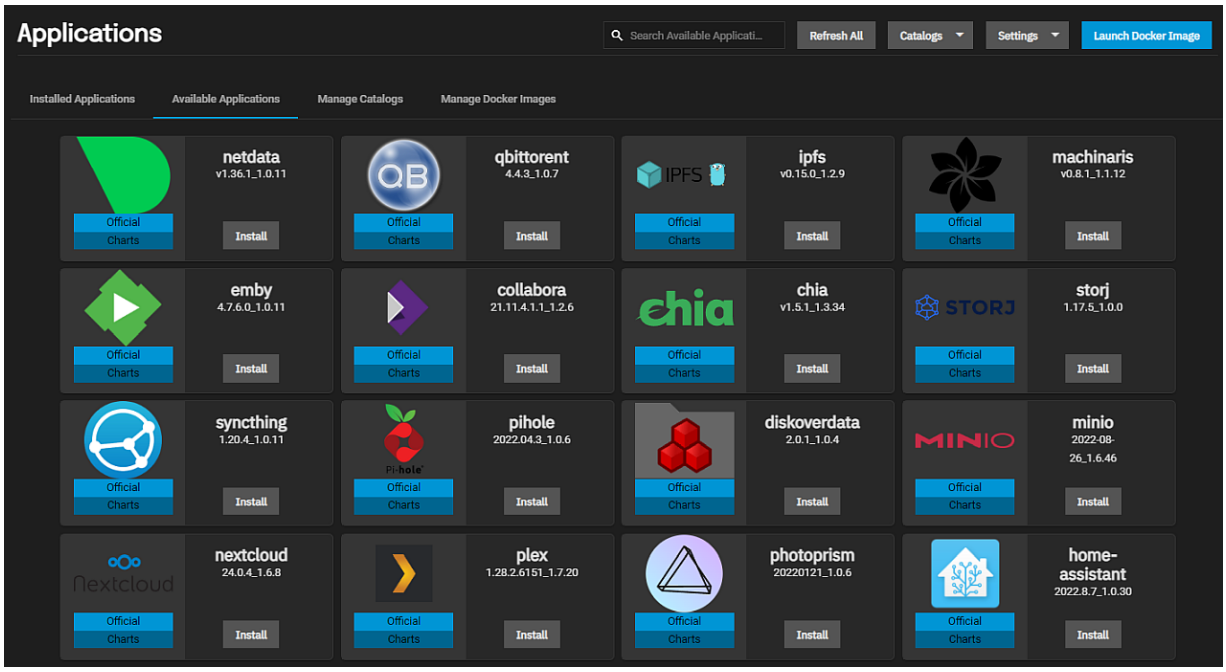
SCALE includes the ability to run Docker containers using Kubernetes.

What is Docker?
Docker is an open platform for developing, shipping, and running applications. Docker enables the separation of applications from infrastructure through OS-level virtualization to deliver software in containers.

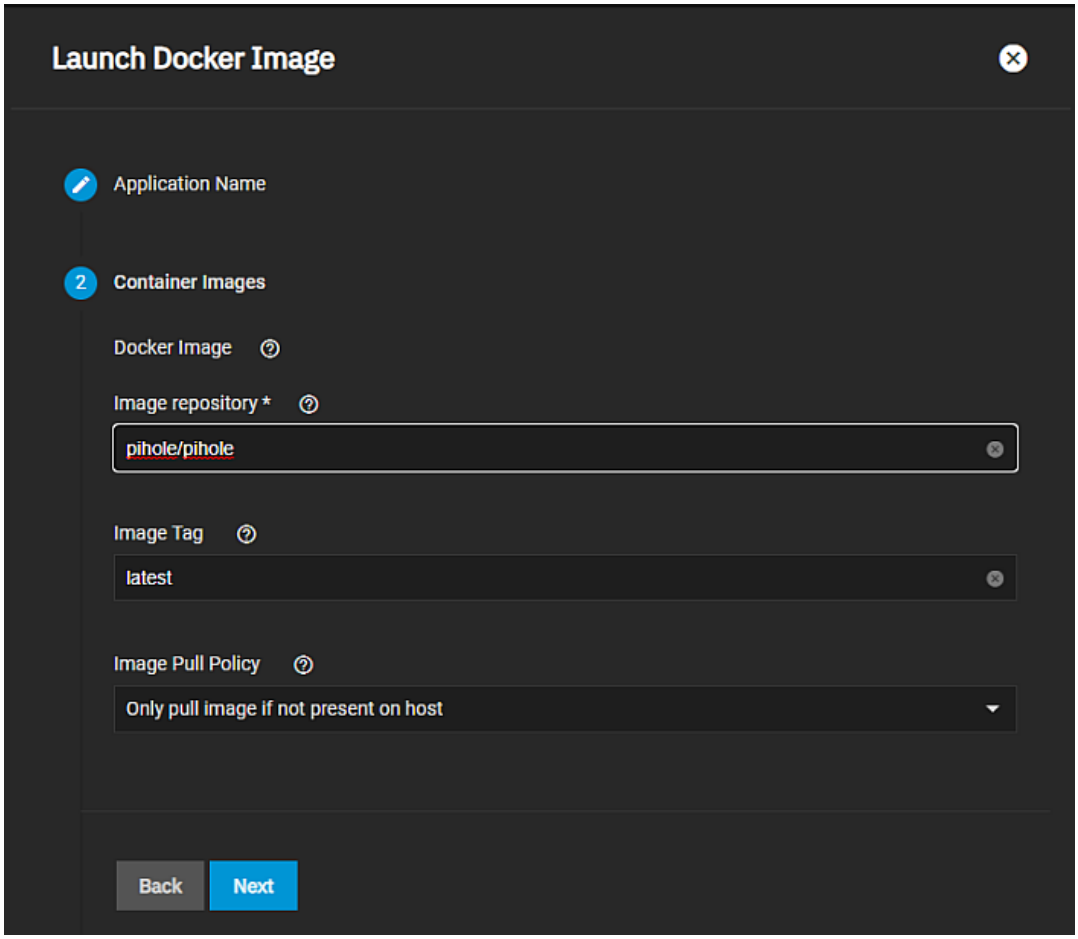
What is Kubernetes?
Kubernetes is a portable, extensible, open-source container-orchestration system for automating computer application deployment, scaling, and management with declarative configuration and automation.

Always read through the Docker Hub page for the container you are considering installing so that you know all of the settings that you need to configure. To set up a Docker image, first determine if you want the container to use its own dataset. If yes, create a dataset for host volume paths before you click **Launch Docker Image**.

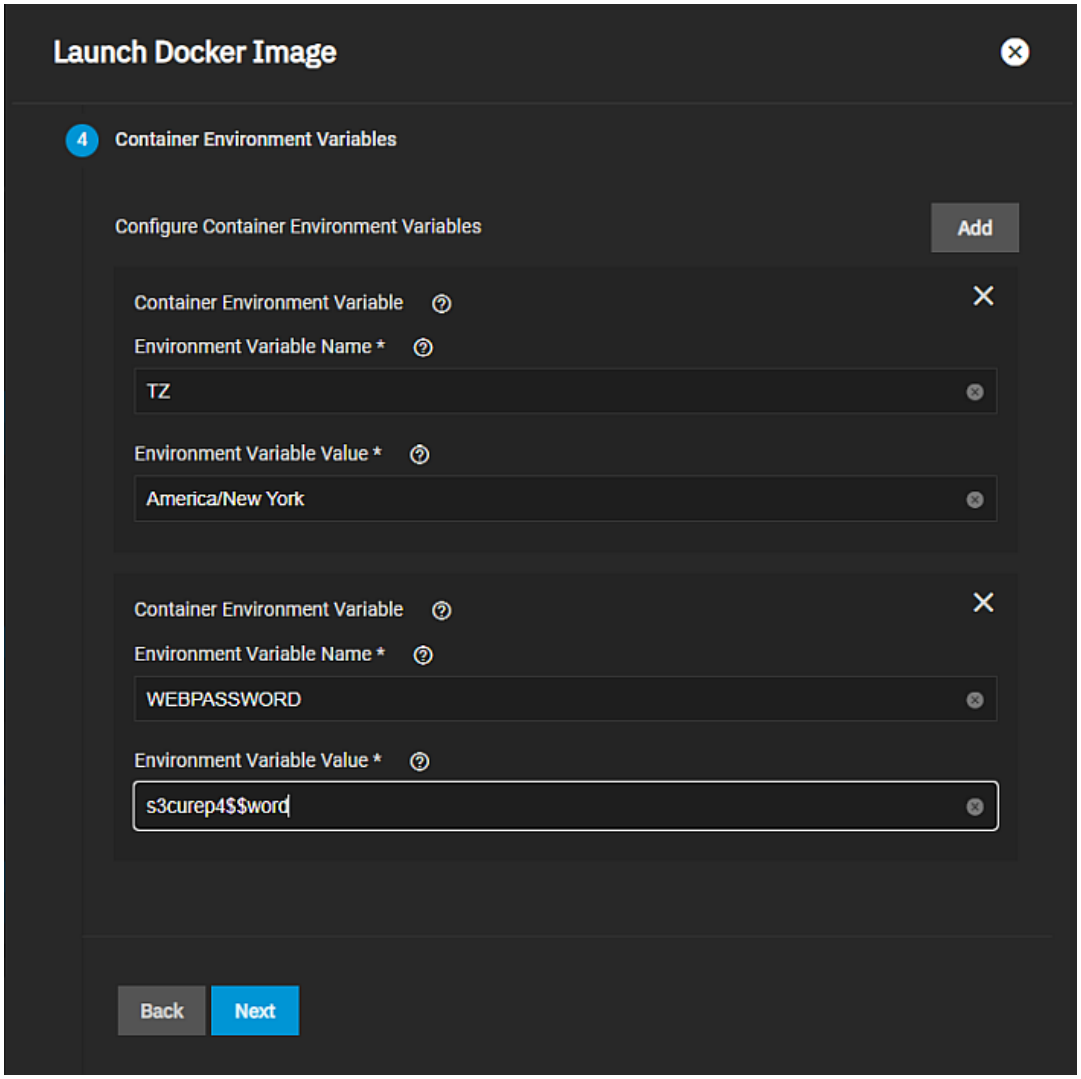
When you are ready to create a container, open the **APPS** page and click **Launch Docker Image**.



Fill in the **Application Name** and click **Next**. Add the github repository URL in **Image Repository** for the docker container are setting up. For the PiHole project enter **pihole/pihole**.

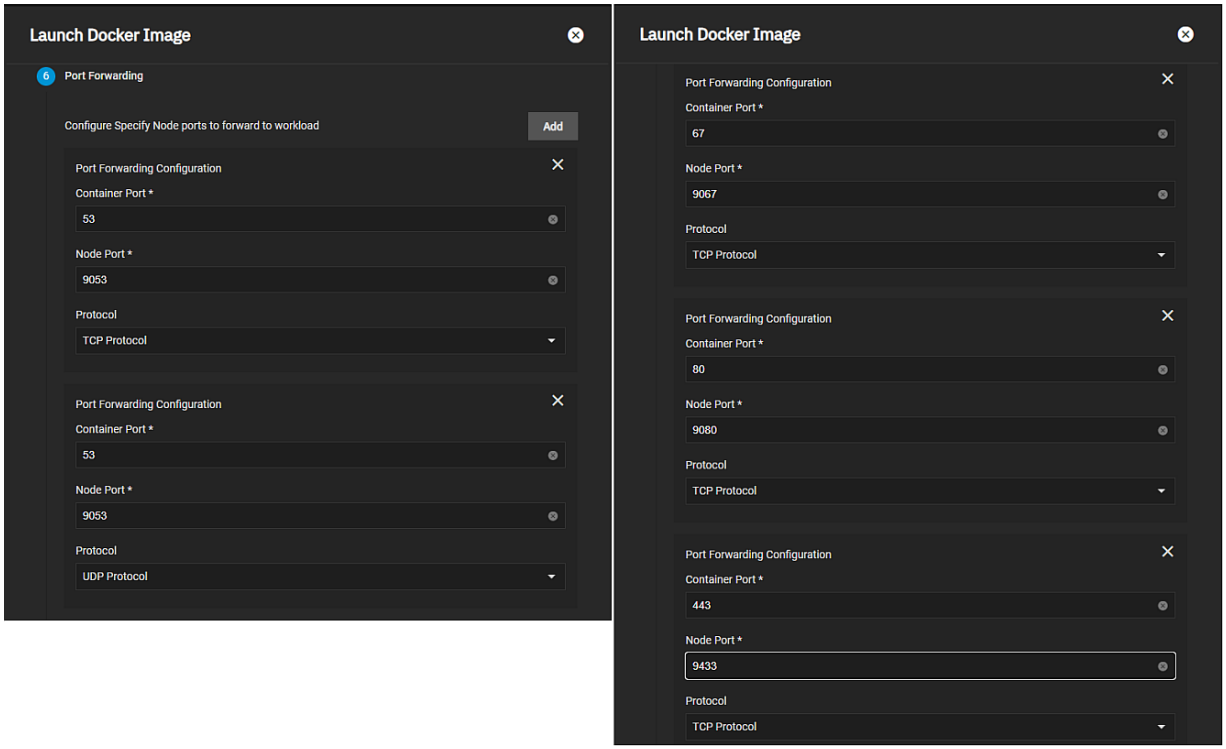


Click **Next** to move to the **Container Environment Variables**. For Pi-Hole, click **Add** then enter **TZ** for timezone, and then **America/NewYork** for the value. Click **Add** again and enter **WEBPASSWORD** and then a secure password like the example used, *s3curep4$$word*. Always refer to the docker hub page for information on what the docker container requires.



Click **Next** to open **Networking**. If the container needs special networking configuration, enter it here. Click **Next** to open **Port Forwarding** to add the Pi-Hole ports.

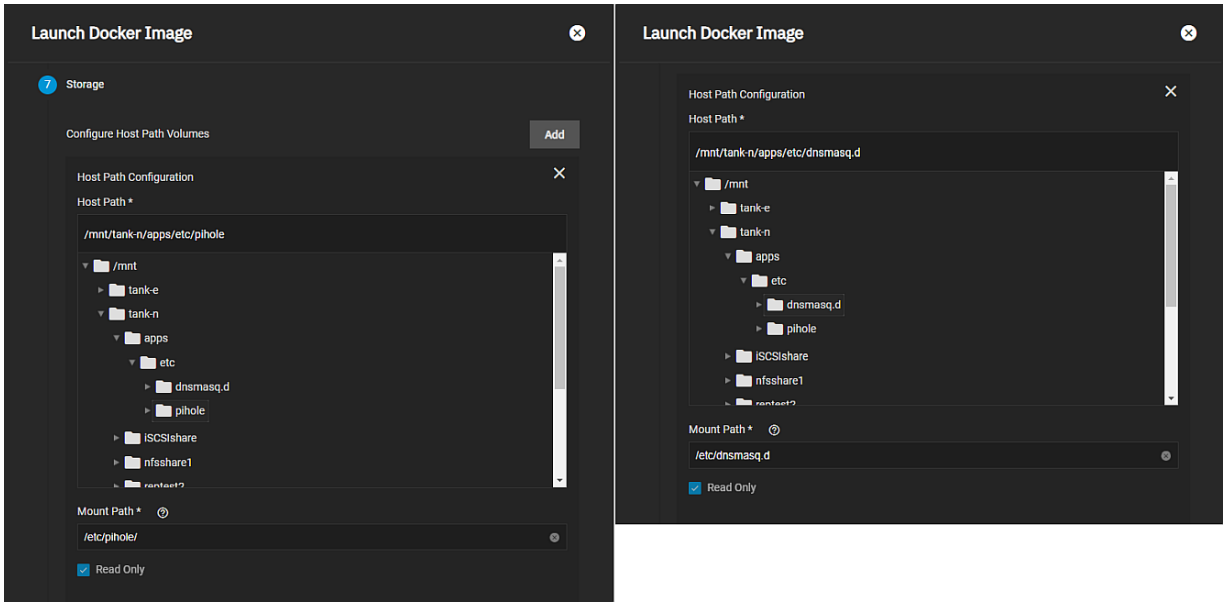
The PiHole Docker Hub page lists a set of four ports and the node port you need to set. Adjust these values if your system configuration requires changes. TrueNAS SCALE requires setting all **Node Ports** above 9000.



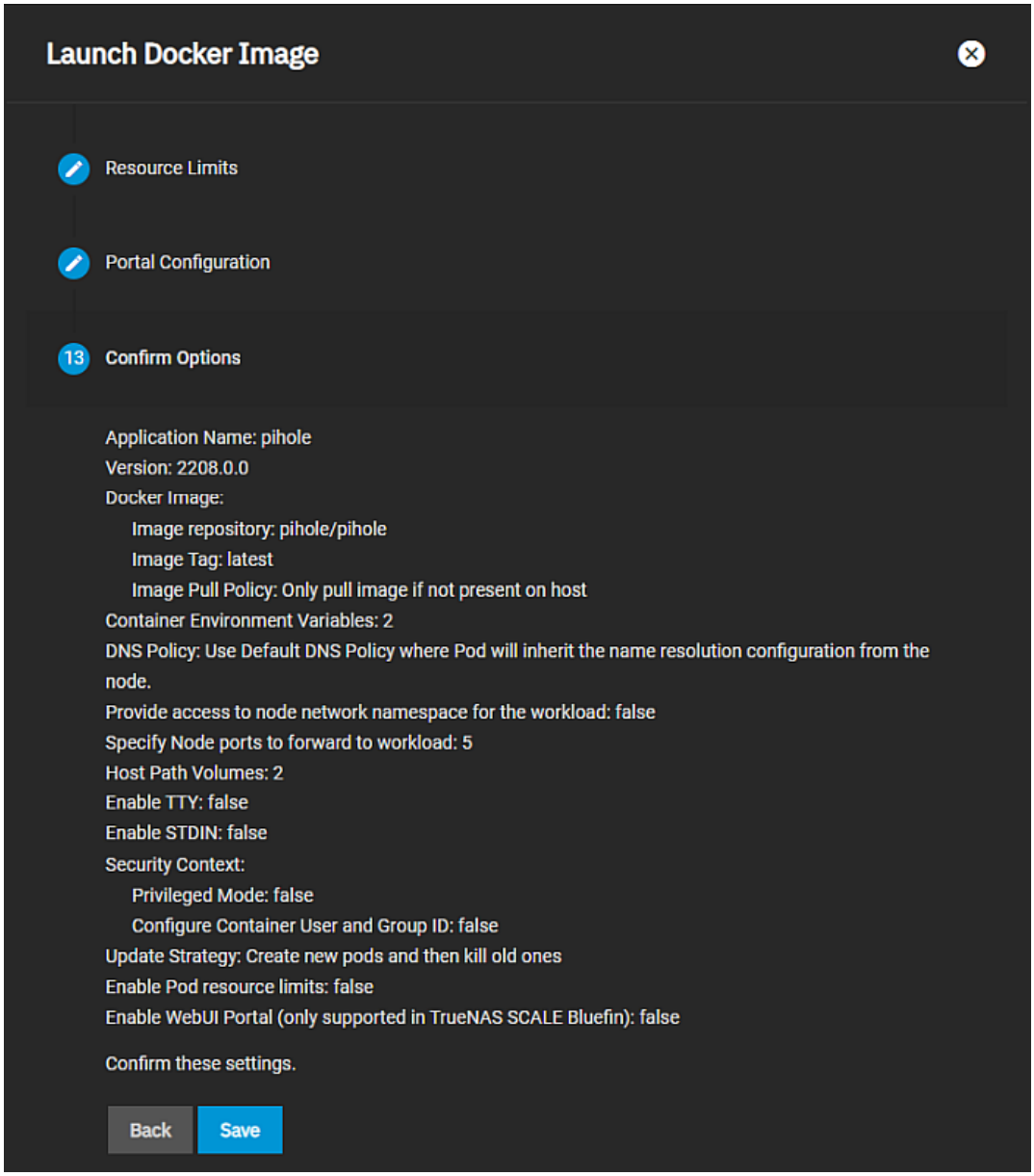
Click **Next** after configuring all the ports to open **Storage**.

Click **Add** twice to add two blocks of host path settings. Browse to the dataset and directory paths you created before beginning the container deployment. PiHole uses volumes store your data between container upgrades.

> You need to create these directories in a dataset on SCALE using **System Settings > Shell** before you begin installing this container.



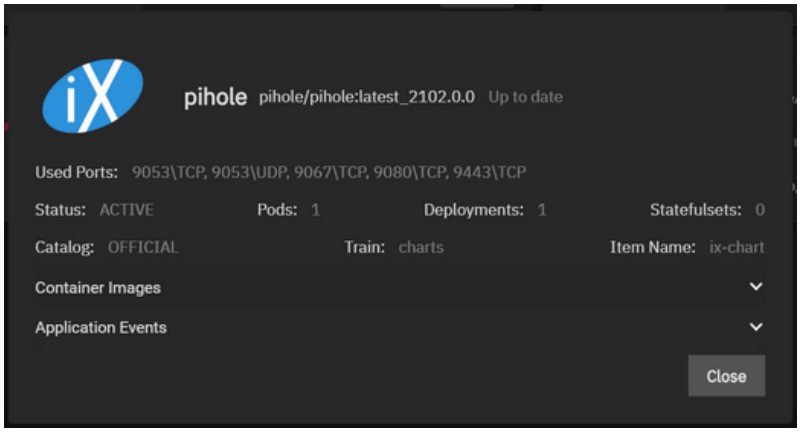
You can add more volumes to the container if needed. When all the settings are entered, click **Next** until you reach **Confirm Options**. Verify the the information on the screen and click **Save**.



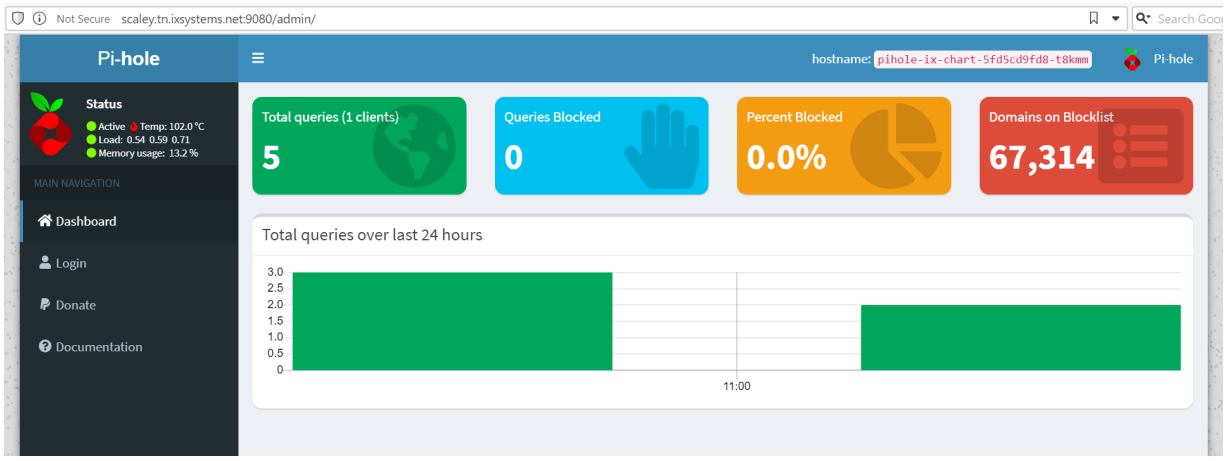
TrueNAS SCALE deploys the container. If correctly configured, the Pi-Hole widget displays on the **Installed Applications** screen.

When the deployment is completed the container becomes active. If the container does not autostart, click **Start** on the widget.

Clicking on the App card reveals details.



With PiHole as our example we navigate to the IP of our TrueNAS system with the port and directory address `:9080/admin/`.



Related Content

- Updating MinIO from 1.6.58
- Using SCALE Catalogs
- Launch Docker Image Screens
- Using Docker Image
- MinIO Clusters

Related Apps Articles

- Applications Screens
- Updating MinIO from 1.6.58
- Using Apps
- Using SCALE Catalogs
- Launch Docker Image Screens
- Using Docker Image
- Adding NextCloud for Media Previews
- Configuring the Chia App
- Collabora App
- MinIO Clusters

3.8 - Reporting

Article Summaries

- Configuring Reporting

  This article provides information on changing settings that control how TrueNAS displays report graphs, interacting with graphs, and the TrueCommand Enhancement option.

3.8.1 - Configuring Reporting

This article provides information on changing settings that control how TrueNAS displays report graphs, interacting with graphs, and the TrueCommand Enhancement option.

TrueNAS has a built-in reporting engine that provides helpful graphs and information about the system.

What does TrueNAS use for reporting?

TrueNAS uses Graphite to gather metrics and create visualizations.

TrueNAS uses collectd to provide reporting statistics.

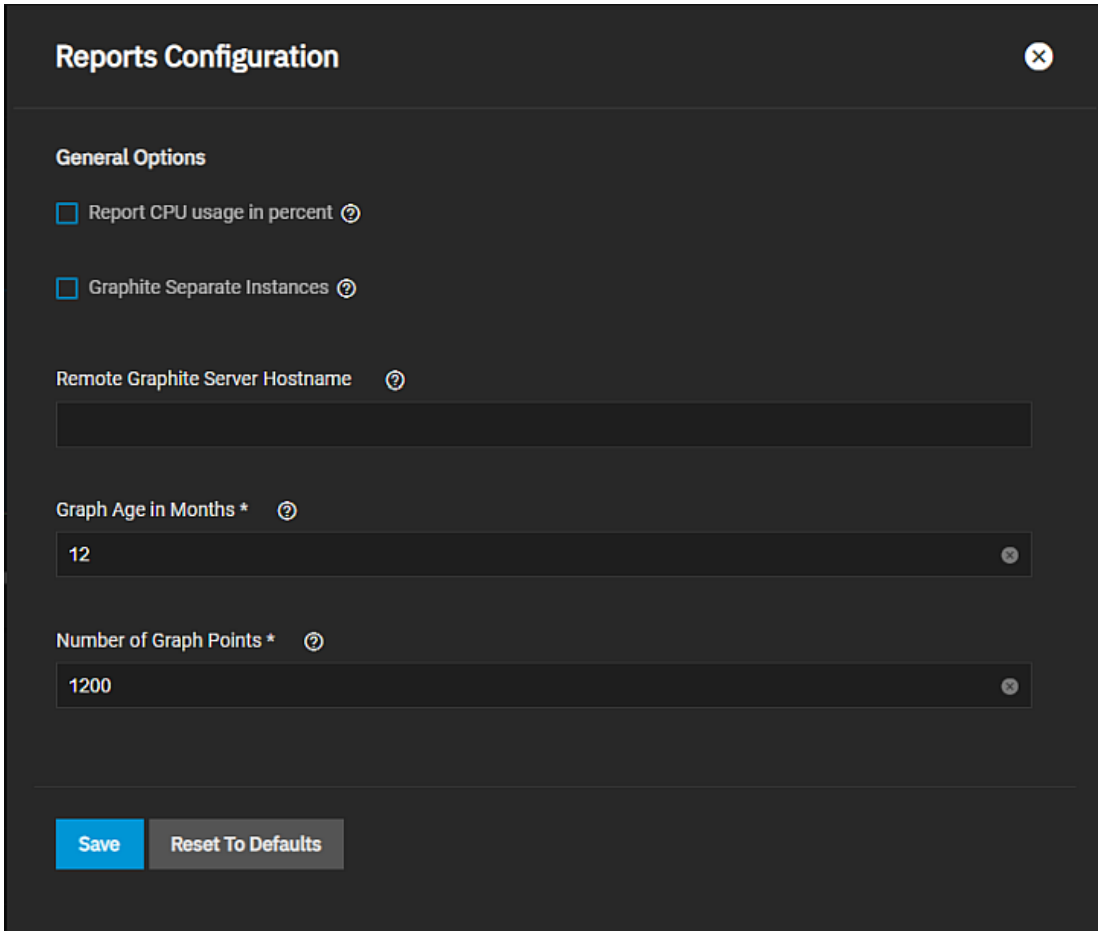
Reporting data is saved to permit viewing and monitoring usage trends over time. This data is preserved across system upgrades and restarts.

> Because reporting data is written frequently do not store it on the boot pool or operating system device.
>
> TrueNAS clears the report history when you change the report CPU, graph age, or graph points options.

Data files are saved in /var/db/collectd/rrd/.

Configuring Report Settings

Click the ⚙ to open the **Reports Configuration** configuration screen where you control how TrueNAS displays the graphs.



Select the general options you want to use in your TrueNAS.

Specify either the host name or IP address of the Graphite server you want to use.

Click **Save**.

TrueCommand Enhancement

To increase TrueNAS reporting functionality connect it to our TrueCommand multi-system management software.

TrueCommand Reports offer enhanced features like creating custom graphs and comparing utilization across multiple systems.

Interacting with Graphs

Click on and drag a certain range of the graph to expand the information displayed in that selected area in the Graph. Click on the icon to zoom in on the graph. Click on the icon to zoom out on the graph. Click the to move the graph forward. Click the to move the graph backward.

Related Content

- Reporting Screens

3.9 - Shares

File sharing is one of the primary benefits of a NAS. TrueNAS helps foster collaboration between users through network shares. TrueNAS SCALE allows users to create and configure block (iSCSI) shares targets, Windows SMB shares, Unix (NFS) shares, and WebDAV shares.

> When creating zvols for shares, avoid giving them names with capital letters or spaces since they can cause problems and failures with iSCSI and NFS shares.

Article Summaries

- Apple Shares (AFP)
  - AFP Migration

    This article provides information on migrating AFP shares from CORE to SCALE.
- Block Shares (iSCSI)

  About Block (iSCSI) Shares Targets Internet Small Computer Systems Interface (iSCSI) represents standards for using Internet-based protocols for linking binary data storage device aggregations. IBM and Cisco submitted the draft standards in March 2000. Since then, iSCSI has seen widespread adoption into enterprise IT environments. iSCSI functions through encapsulation. The Open Systems Interconnection Model (OSI) encapsulates SCSI commands and storage data within the session stack. The OSI further encapsulates the session stack within the transport stack, the transport stack within the network stack, and the network stack within the data stack.
  - Adding iSCSI Block Shares

    This article provides instructions on setting up iSCSI block shares manually or using the wizard and starting the service.
  - Using an iSCSI Share

    This article provides information on setting up a Linux or Windows system to use a TrueNAS-configured iSCSI block share.
  - Increasing iSCSI Available Storage

    This article provides information on increasing available storage in zvols and file LUNs for iSCSI block shares.
- Unix Shares (NFS)

  Article Summaries Adding NFS Shares This article provides instructions on adding NFS shares, starting NFS service and accessing the share.
  - Adding NFS Shares

    This article provides instructions on adding NFS shares, starting NFS service and accessing the share.
- WebDAV Shares

  Article Summaries Configuring WebDAV Shares This article provides instructions on adding a WebDAV share, configuring and starting the WebDAV service, and then connecting to it with a web browser.
  - Configuring WebDAV Shares

    This article provides instructions on adding a WebDAV share, configuring and starting the WebDAV service, and then connecting to it with a web browser.
- Windows Shares (SMB)

  Article Summaries Adding SMB Shares This article provides instructions to add an SMB share, starting the service, and mounting the share. Managing SMB Shares This article provides instructions on managing existing SMB shares, adding share ACLs, and managing file system ACLs Using SMB Shadow Copy This article provides information on SMB share shadow copies, enbling shadow copies, and resolving an issue with Microsoft Windows 10 v2004 release.
  - Adding SMB Shares

    This article provides instructions to add an SMB share, starting the service, and mounting the share.
  - Managing SMB Shares

    This article provides instructions on managing existing SMB shares, adding share ACLs, and managing file system ACLs
  - Using SMB Shadow Copy

    This article provides information on SMB share shadow copies, enbling shadow copies, and resolving an issue with Microsoft Windows 10 v2004 release.

- Setting Up SMB Home Shares

  This article provides instructions to set up SMB home shares.

3.9.1 - Apple Shares (AFP)

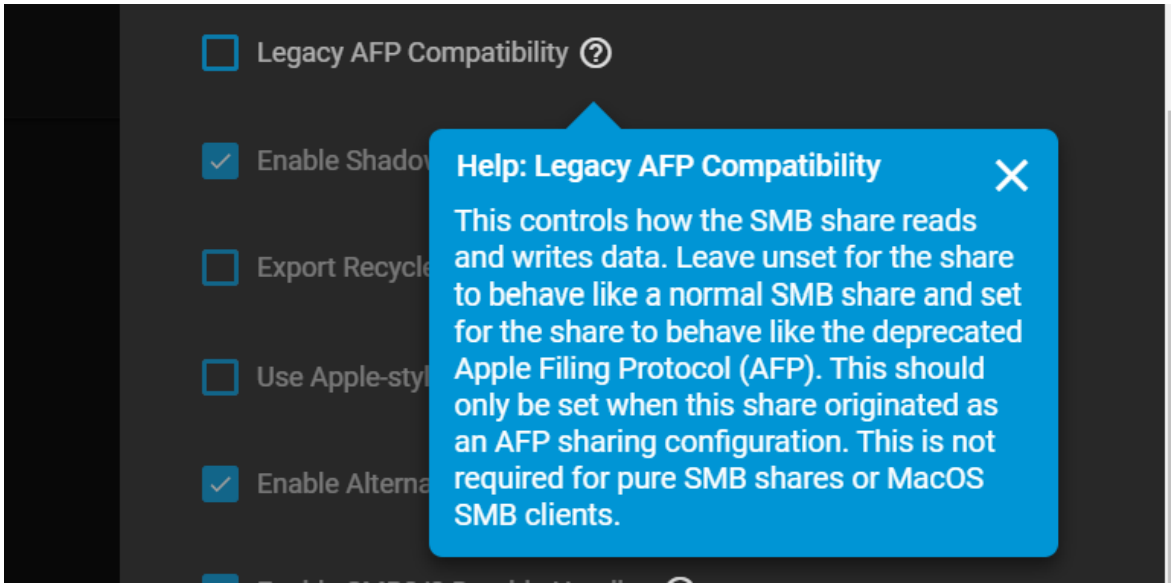
3.9.1.1 - AFP Migration

This article provides information on migrating AFP shares from CORE to SCALE.

Since the Apple Filing Protocol (AFP) for shares is deprecated and no longer receives updates, it is not included in TrueNAS SCALE.

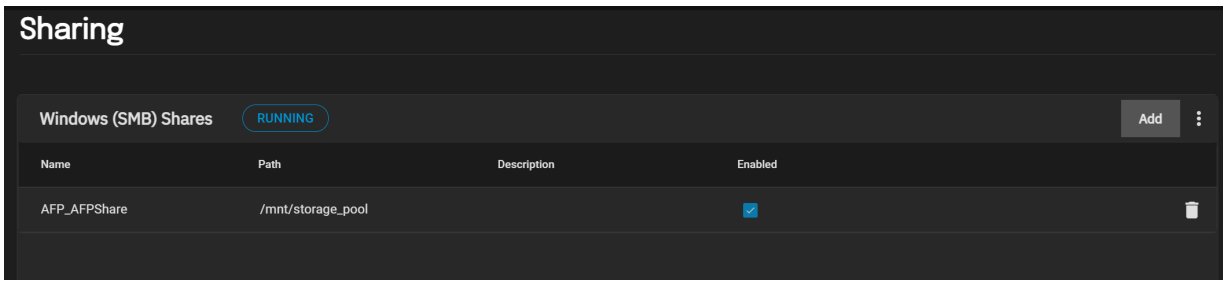
However, users can sidegrade a TrueNAS CORE configuration into SCALE, so TrueNAS SCALE migrates previously-saved AFP configurations into SMB configurations.

To prevent data corruption that could result from the sidegrade operation, in SCALE go to **Windows (SMB) Shares** select the ⋮ for the share, and then select **Edit** to open the **Edit SMB** screen. Click **Advanced Options** and scroll down to the **Other Options** section. Select **Legacy AFP Compatibility** to enable compatibility for AFP shares migrated to SMB shares. Do not select this option if you want a pure SMB share with no AFP relation.



> Netatalk service was removed in SCALE version 21.06. AFP shares are automatically migrated to SMB shares with the **Legacy AFP Compatibility** option selected. Do not clear the **Legacy AFP Compatibility** checkbox as it impacts how data is written to and read from shares. Any other shares created to access these paths after the migration must also have **Legacy AFP Compatibility** selected.

Once you have sidegraded from CORE to SCALE, you can find your migrated AFP configuration in **Shares > Windows Shares (SMB)** with the prefix **AFP_**. To make the migrated AFP share accessible, start the SMB service.



Related Content

- Adding SMB Shares
- SMB Shares Screens
- Managing SMB Shares
- Using SMB Shadow Copy
- Setting Up SMB Home Shares
- Configuring SMB Service
- SMB Service Screen
- Spotlight Support on a SCALE SMB Share

Related Migration Articles

- Migrating to TrueNAS
- Migrating from TrueNAS CORE
- Component Naming
- ZFS Feature Flags Removed
- Importing Storage Pools
- First Time Login
- Setting Up Data Sharing
- Backing Up TrueNAS

3.9.2 - Block Shares (iSCSI)

About Block (iSCSI) Shares Targets

Internet Small Computer Systems Interface (iSCSI) represents standards for using Internet-based protocols for linking binary data storage device aggregations. IBM and Cisco submitted the draft standards in March 2000. Since then, iSCSI has seen widespread adoption into enterprise IT environments.

iSCSI functions through encapsulation. The *Open Systems Interconnection Model* (OSI) encapsulates SCSI commands and storage data within the session stack. The OSI further encapsulates the session stack within the transport stack, the transport stack within the network stack, and the network stack within the data stack. Transmitting data this way permits block-level access to storage devices over LANs, WANs, and even the Internet itself (although performance may suffer if your data traffic is traversing the Internet).

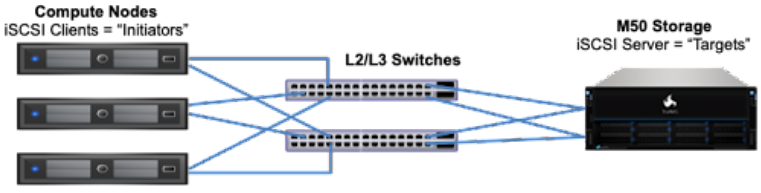
The table below shows where iSCSI sits in the OSI network stack:

OSI Layer Number	OSI Layer Name	Activity as it relates to iSCSI
7	Application	An application tells the CPU that it needs to write data to non-volatile storage.
6	Presentation	OSI creates a SCSI command, SCSI response, or SCSI data payload to hold the application data and communicate it to non-volatile storage.
5	Session	Communication between the source and the destination devices begins. This communication establishes when the conversation starts, what it talks about, and when the conversion ends. This entire dialogue represents the session. OSI encapsulates the SCSI command, SCSI response, or SCSI data payload containing the application data within an iSCSI Protocol Data Unit (PDU).
4	Transport	OSI encapsulates the iSCSI PDU within a TCP segment.
3	Network	OSI encapsulates the TCP segment within an IP packet.
2	Data	OSI encapsulates the IP packet within the Ethernet frame.
1	Physical	The Ethernet frame transmits as bits (zeros and ones).

Unlike other sharing protocols on TrueNAS, an iSCSI share allows block sharing *and* file sharing. Block sharing provides the benefit of block-level access to data on the TrueNAS. iSCSI exports disk devices (zvols on TrueNAS) over a network that other iSCSI clients (initiators) can attach and mount.

iSCSI Terminology

- **Challenge-Handshake Authentication Protocol (CHAP)**: an authentication method that uses a shared secret and three-way authentication to determine if a system is authorized to access the storage device. It also periodically confirms that the session has not been hijacked by another system. In iSCSI, the client (initiator) performs the CHAP authentication.
- **Mutual CHAP**: a CHAP type in which both ends of the communication authenticate to each other.
- **Internet Storage Name Service (iSNS)**: protocol for the automated discovery of iSCSI devices on a TCP/IP network.
- **Extent**: the storage unit to be shared. It can either be a file or a device.
- **Portal**: indicates which IP addresses and ports to listen on for connection requests.
- **Initiators and Targets**: iSCSI introduces the concept of *initiators* and *targets* which act as sources and destinations respectively. iSCSI initiators and targets follow a client/server model. Below is a diagram of a typical iSCSI network. The TrueNAS storage array acts as the iSCSI target and can be accessed by many of the different iSCSI initiator types, including software and hardware-accelerated initiators.



  The iSCSI protocol standards require that iSCSI initiators and targets is represented as iSCSI nodes. It also requires that each node is given a unique iSCSI name. To represent these unique nodes via their names, iSCSI requires the use of one of two naming conventions and formats, IQN or EUI. iSCSI also allows the use of iSCSI aliases which are not required to be unique and can help manage nodes.

- **Logical Unit Number (LUN)**: LUN represents a logical SCSI device. An initiator negotiates with a target to establish connectivity to a LUN. The result is an iSCSI connection that emulates a connection to a SCSI hard disk. Initiators treat iSCSI LUNs as if they were a raw SCSI or SATA hard drive. Rather than mounting remote directories, initiators format and directly manage filesystems on iSCSI LUNs. When configuring multiple iSCSI LUNs, create a new target for each

LUN. Since iSCSI multiplexes a target with multiple LUNs over the same TCP connection, there can be TCP contention when more than one target accesses the same LUN. TrueNAS supports up to 1024 LUNs.

- **Jumbo Frames**: Jumbo frames are the name given to Ethernet frames that exceed the default 1500 byte size. This parameter is typically referenced by the nomenclature as a maximum transmission unit (MTU). A MTU that exceeds the default 1500 bytes necessitates that all devices transmitting Ethernet frames between the source and destination support the specific jumbo frame MTU setting, which means that NICs, dependent hardware iSCSI, independent hardware iSCSI cards, ingress and egress Ethernet switch ports, and the NICs of the storage array must all support the same jumbo frame MTU value. So, how does one decide if they should use jumbo frames?

  Administrative time is consumed configuring jumbo frames and troubleshooting if/when things go sideways. Some network switches might also have ASICs optimized for processing MTU 1500 frames while others might be optimized for larger frames. Systems administrators should also account for the impact on host CPU utilization. Although jumbo frames are designed to increase data throughput, it may measurably increase latency (as is the case with some un-optimized switch ASICs); latency is typically more important than throughput in a VMware environment. Some iSCSI applications might see a net benefit running jumbo frames despite possible increased latency. Systems administrators should test jumbo frames on their workload with lab infrastructure as much as possible before updating the MTU on their production network.

TrueNAS Enterprise Feature:

- **Asymmetric Logical Unit Access (ALUA)**: ALUA allows a client computer to discover the best path to the storage on a TrueNAS system. HA storage clusters can provide multiple paths to the same storage. For example, the disks are directly connected to the primary computer and provide high speed and bandwidth when accessed through that primary computer. The same disks are also available through the secondary computer, but speed and bandwidth are restricted. With ALUA, clients automatically ask for and use the best path to the storage. If one of the TrueNAS HA computers becomes inaccessible, the clients automatically switch to the next best alternate path to the storage. When a better path becomes available, as when the primary host becomes available again, the clients automatically switch back to that better path to the storage.

Do not enable ALUA on TrueNAS unless it is also supported by and enabled on the client computers. ALUA only works when enabled on both the client and server.

iSCSI Configuration Methods

There are a few different approaches for configuring and managing iSCSI-shared data:

- TrueNAS CORE web interface: the TrueNAS web interface is fully capable of configuring iSCSI shares. This requires creating and populating zvol block devices with data, then setting up the iSCSI Share. TrueNAS Enterprise licensed customers also have additional options to configure the share with Fibre Channel.
- TrueNAS SCALE web interface: TrueNAS SCALE offers a similar experience to TrueNAS CORE for managing data with iSCSI; create and populate the block storage, then configure the iSCSI share.
- TrueCommand instances that have many TrueNAS systems connected can manage iSCSI Volumes from the TrueCommand web interface. TrueCommand allows creating block devices and configuring iSCSI Targets and Initiators from one central location.
- TrueNAS Enterprise customers that use vCenter to manage their systems can use the TrueNAS vCenter Plugin to connect their TrueNAS systems to vCenter and create and share iSCSI datastores. This is all managed through the vCenter web interface.

Article Summaries

- Adding iSCSI Block Shares

  This article provides instructions on setting up iSCSI block shares manually or using the wizard and starting the service.

- Using an iSCSI Share

  This article provides information on setting up a Linux or Windows system to use a TrueNAS-configured iSCSI block share.

- Increasing iSCSI Available Storage

  This article provides information on increasing available storage in zvols and file LUNs for iSCSI block shares.

3.9.2.1 - Adding iSCSI Block Shares

This article provides instructions on setting up iSCSI block shares manually or using the wizard and starting the service.

To get started with iSCSI shares, make sure you have already created a zvol or a dataset with at least one file to share.

Go to **Shares** and click **Configure** in the **Block (iSCSI) Shares Targets** window. You can either use the creation wizard or set one up manually.

Configuring an iSCSI Share Tutorial Video

Tutorial Video

This short tutorial video demonstrates basic steps to set up an iSCSI share configuration.

Adding an iSCSI Block Share

TrueNAS SCALE offers two methods to add an iSCSI block share: the setup wizard or the manual steps using the screen tabs. Both methods cover the same basic steps but have some differences.

The setup wizard requires you to enter some settings before you can move on to the next screen or step in the setup process. It is designed to ensure you configure the iSCSI share completely so it can be used immediately.

The manual process has more configuration screens over the wizard and allows you to configure the block share in any order. Use this process to customize your share for special uses cases. It is designed to give you additional flexibility to build or tune a share to your exact requirements.

Before you Begin

Have the following ready before you begin adding your iSCSI block share:

- Storage pool and dataset.

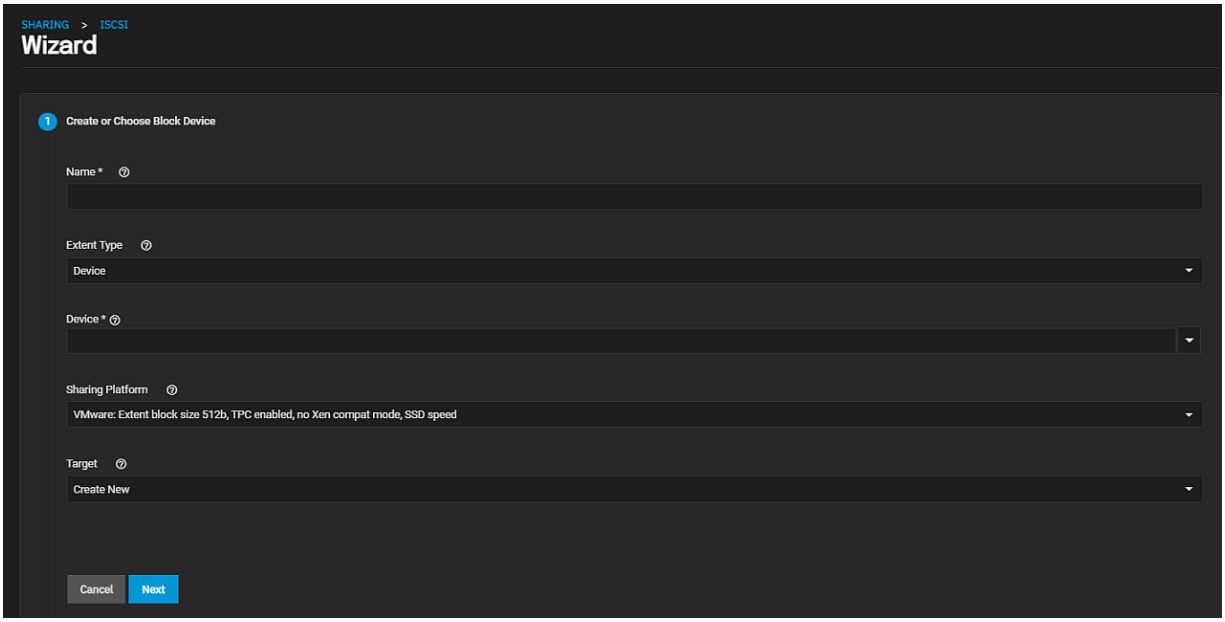
iSCSI Wizard

This section walks you through the setup process using the wizard screens.

To use the setup wizard,

1. Add the block device.

   a. Enter a name using all lowercase alphanumeric characters plus a dot (.), dash (-), or colon (:). We recommend keeping it short or at most 63 characters.



b. Choose the **Extent Type**. You can select either **Device** or **File**.

If you select **Device**, select the zvol to share from the **Device** dropdown list.

If you select **File**, file settings display. Browse to the location of the file to populate the path, and then enter the size in **Filesize**.

c. Select the type of platform using the share. For example, if you use an updated Linux OS, choose **Modern OS**.

d. Click **Next**.

2. Add the portal

Now you either create a new portal or select an existing one from the dropdown list.

If you create a new portal, select a **Discovery Authentication Method** from the dropdown list.

If you select **None**, you can leave **Discovery Authentication Group** empty.

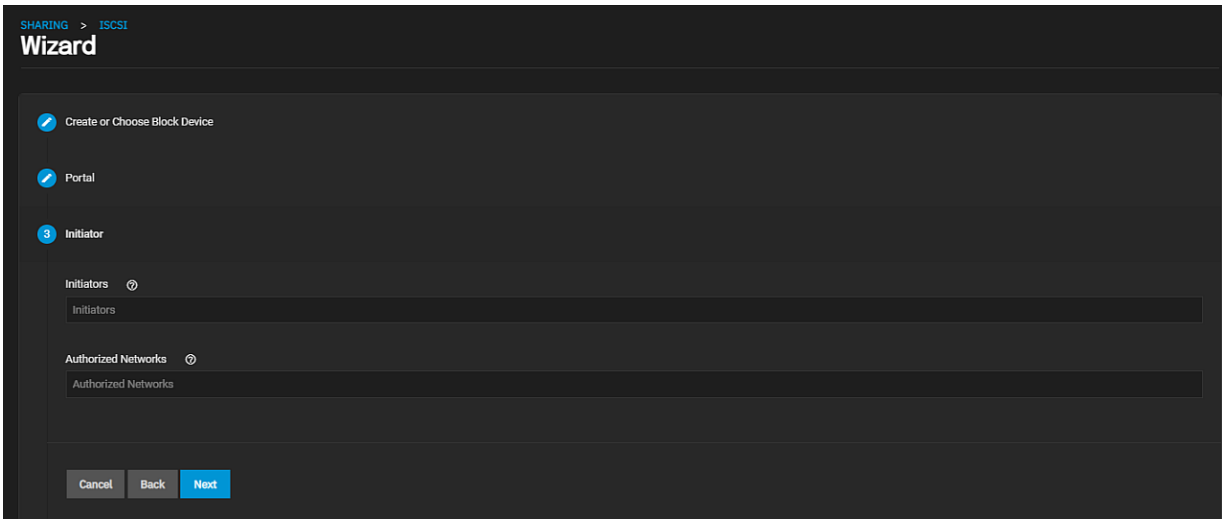
If you select either **CHAP** or **MUTUAL CHAP**, you must also to select a **Discovery Authentication Group** from the dropdown list. If no group exists, click **Create New** and enter a value in **Group ID**, **User**, and **Secret**.

Select **0.0.0.0** or **::** from the **IP Address** dropdown list. **0.0.0.0** listens on all IPv4 addresses and **::** listens on all IPv6 addresses.

Click **NEXT**

3. Add the Initiator. After adding the portal set up the initiator or networks that use the iSCSI share.

   Decide which initiators or networks can use the iSCSI share. Leave the list empty to allow all initiators or networks, or add entries to the list to limit access to those systems.



4. Confirm the iSCSI setup. Review your settings. If you need or want to change any setting click **Back** until you reach the wizard screen with the setting.

5. click **Save**.

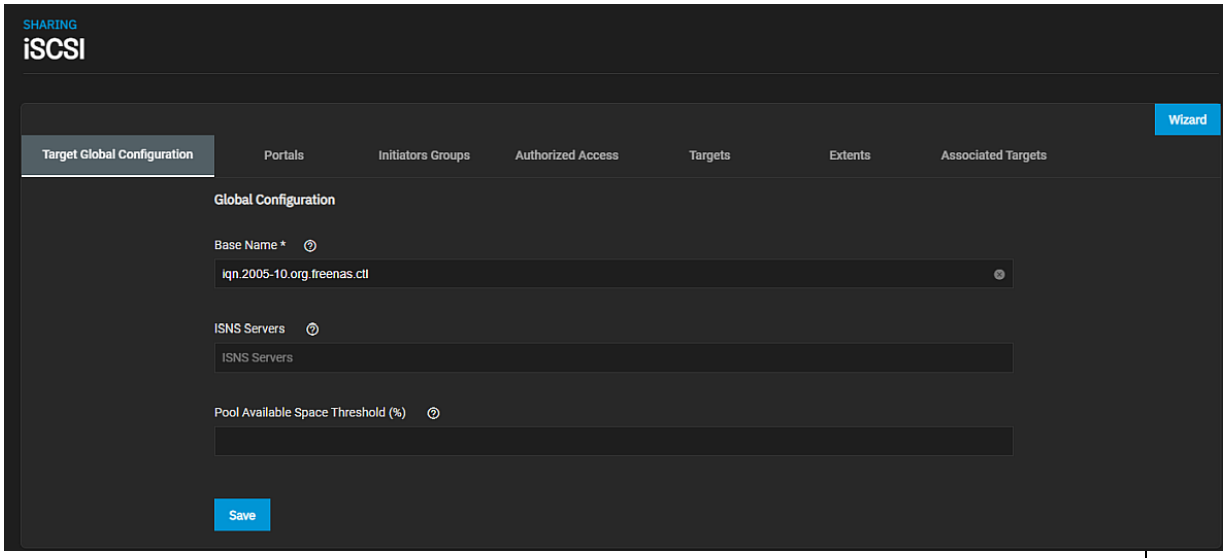
iSCSI Manual Setup

This procedure walks you through adding each configuration setting on the seven configuration tab screens. While the procedure places each tab screen in order, you can select the tab screen to add settings in any order.

Click here for more information

1. Configure share settings that apply to all iSCSI shares.

   a. Click **Configure** on the main **Block (iSCSI) Share Targets** widget. The **Target Global Configuration** tab screen opens.

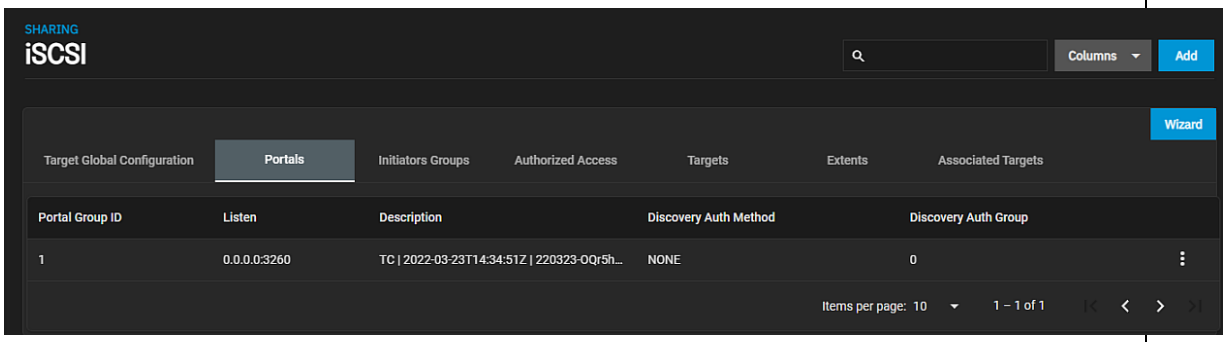


b. Enter a name using lowercase alphanumeric characters plus dot (.), dash (-), and colon (:) in **Base Name**. Use the iqn.format for the name. See the “Constructing iSCSI names using the iqn.format” section of RFC3721.

c. Enter the host names or IP address of the ISNS servers to register with the iSCSI targets and portals of the system. Separate entries by pressing `Enter`.

d. Click **Save**.

2. Add portals. Click **Portals** to open the screen.



a. Click **Add** at the top of the screen to open the **Sharing > iSCSI > Portals > Add** screen.

SharingiSCSIPortalsAddScreen

b. (Optional) Enter a description. Portals are automatically assigned a numeric group.

c. Select the **Discovery Authentication Method** from the dropdown list.

None alows anonymous discovery and does not require you to select a **Discovery Authentication Group**.

CHAP and **Mutual CHAP** require authentication and you to select a group ID in **Discovery Authentication Group**.

d. (Optional) Based on your **Discovery Authentication Method**, select a group in **Discovery Authentication Group**.

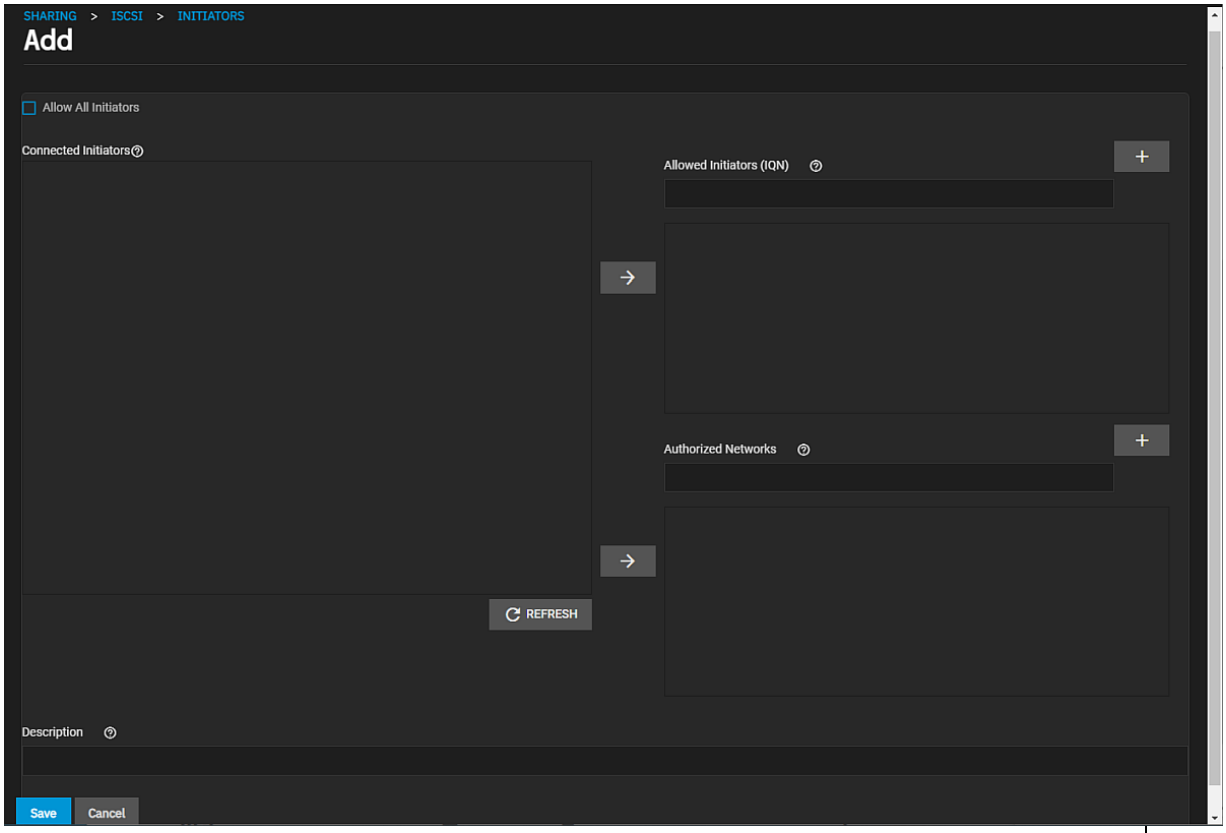
e. Click **Add** to display the **IP Address** and **Port** fields. Click **Add** for each network IP address and port.

Add the IP address. **0.0.0.0** listens on all IPv4 addresses and **::** listens on all IPv6 addresses.

Add the TCP port used to access the iSCSI target. Default is **3260**.

f. Click **Save**.

3. Add initiators groups to create authorized access client groups. Click on the **Initiators Groups** tab to open the screen.



a. Click **Add** to open the **Sharing > iSCSI > Initiators > Add** screen.

b. Select **Allow All Initiators** or configure your own allowed initiators and authorized networks.

Enter the iSCSI Qualified Name (IQN) in **Allowed Initiators (IQN)** and click **+** to add it to the list. Example: *iqn.1994-09.org.freebsd:freenas.local*.

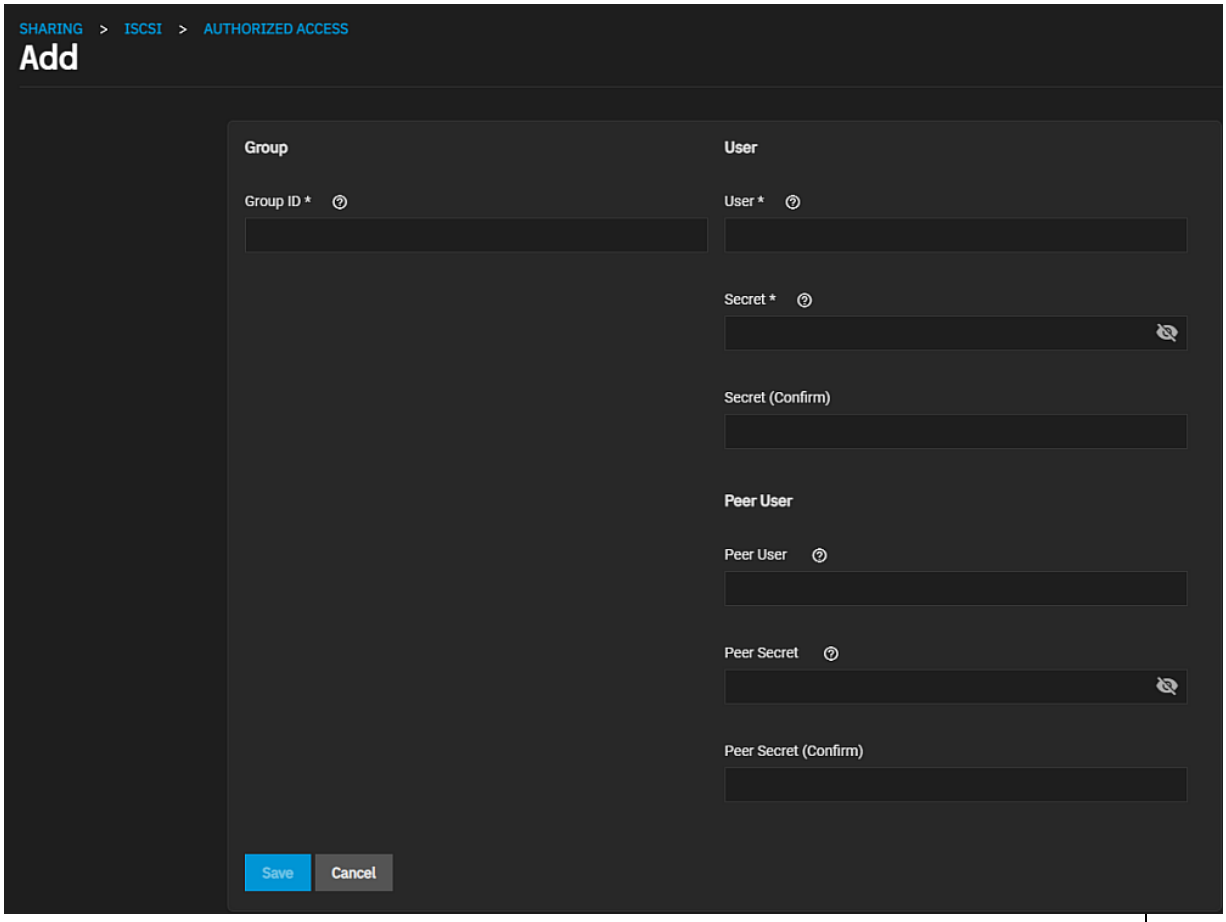
Enter network addresses allowed to use this initiator in **Authorized Networks** and click **+** to add it to the list. Each address can include an optional CIDR netmask. Click **+** to add the network address to the list. Example: *192.168.2.0/24*.

c. Click **Save**.

4. Add network authorized access. Click on the **Authorized Access** tab to open the screen.

If this is the first iSCSI share, the **No Authorized Access** screen opens.

a. Click **Add Authorized Access** in the center of the screen. To add another network click **Add** at the top of the screen to open the **Sharing > iSCSI > Authorized Access > Add** screen.



b. Enter a number in **Group ID**. Each group ID allows configuring different groups with different authentication profiles. Example: all users with a group ID of *1* inherits the authentication profile associated with *Group 1*.

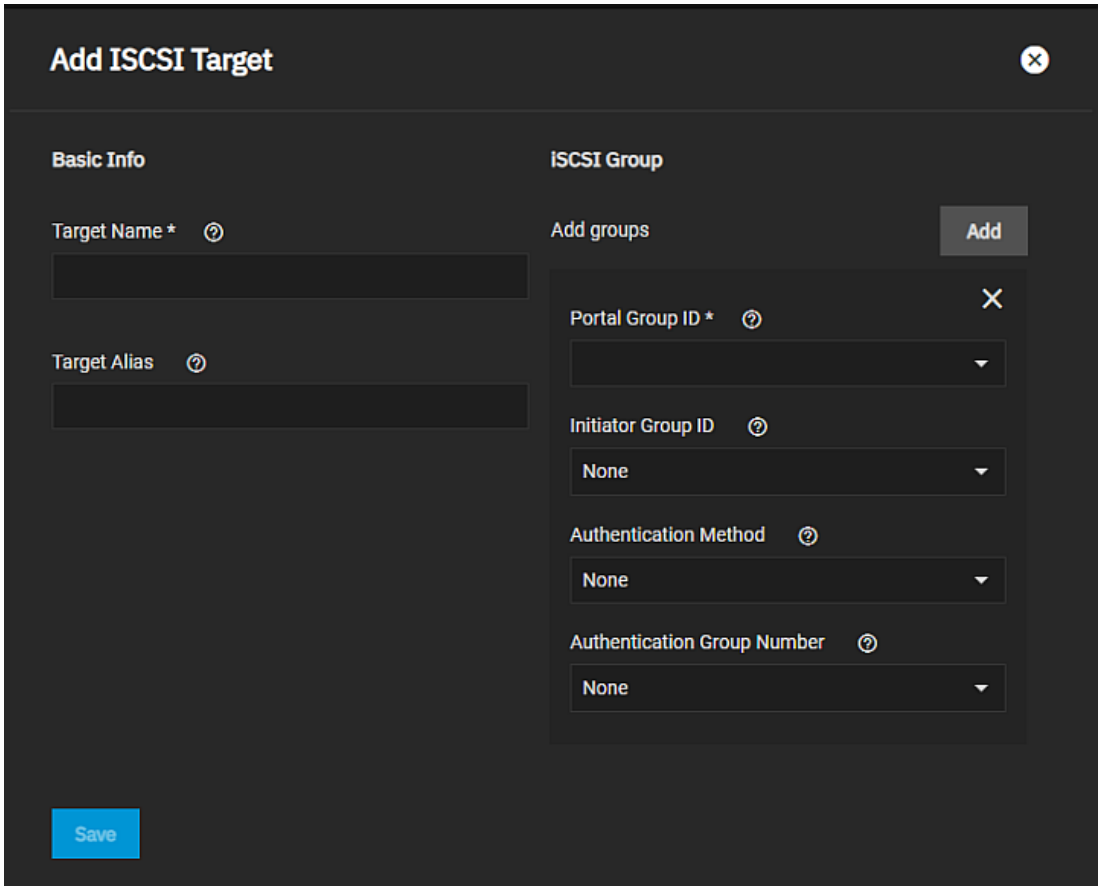
c. Enter a user around to create for CHAP authentication with the user on the remote system. Consider using the initiator name as the user name.

d. Enter the user password of at least 12 to no more than 16 characters long in **Secret** and **Secret (Confirm)**.

e. (Optional) Enter peer user details in **Peer User** and **Peer Secret** and **Peer Secret (Confirm)**. Peer user is only entered when configuring mutual CHAP and is usually the same value as **User**. The password must be different from the one entered in **Secret**.

f. Click **Save**.

5. Create storage resources. Click **Targets** tab to open the screen.



a. Click **Add** at the top of the screen to open the **Add iSCSI Target** screen.

b. Enter a name using lowercase alphanumeric characters plus dot (.), dash (-), and colon (:) in the iqn.format. See the “Constructing iSCSI names using the iqn.format” section of RFC3721.

c. (Optional) Enter a user-friendly name.

d. Click **Add** under **iSCSI Group** to display the group settings.

e. Select the group ID from the **Portal Group ID** dropdown.

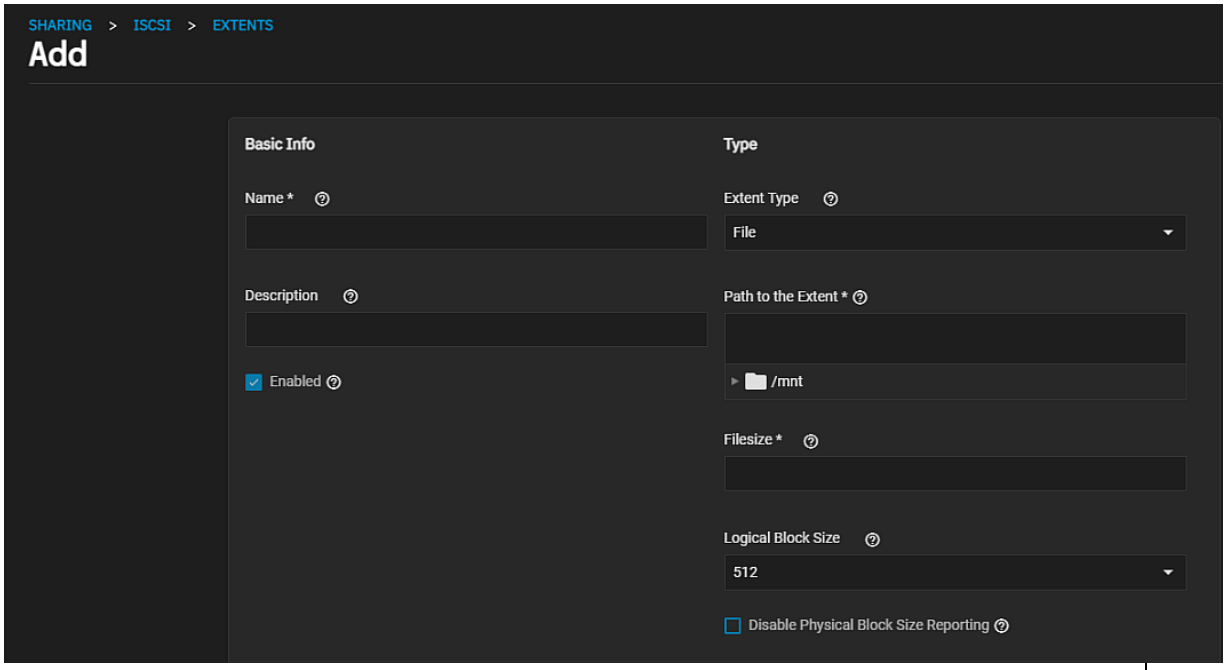
f. (Optional) Slect the group ID in **Initiator Group ID** or leave it set to **None**.

g. (Optional) Select the **Authentication Method** from the dropdown list of options.

h. (Optional) Select the **Authentication Group Number** from the dropdown list. Leave at **None** or enter an integer to represent the number of existing authorized access.

i. Click **Save**.

6. Add new share storage units (extents). Click **Extents** to open the **Sharing > iSCSI > Extents > Add** screen.

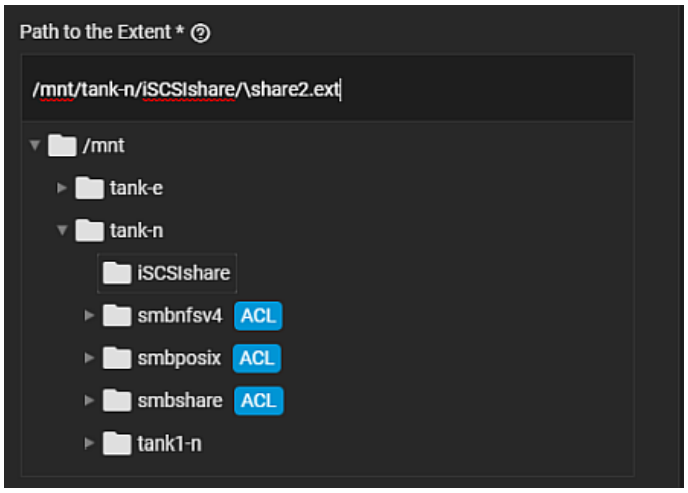


a. Enter a name for the extent. If the extent size is not **0**, it cannot be an existing file within the pool or dataset.

b. Leave **Enable** selected.

c. Select the extent type from the **Extent Type** dropdown. **Device** provides virtual storage access to zvols, zvol snapshots, or physical devices. **File** provides virtual storage access to a single file.

d. (Optional) Select the option from the **Device** dropdown. This field only displays when **Extent Type** is set to **Device**. Select the path when **Extent Type** is set to **File**. Browse to the location. Create a new file by browsing to a dataset and appending /{filename.ext} to the path. And Enter the size in **Filesize**.



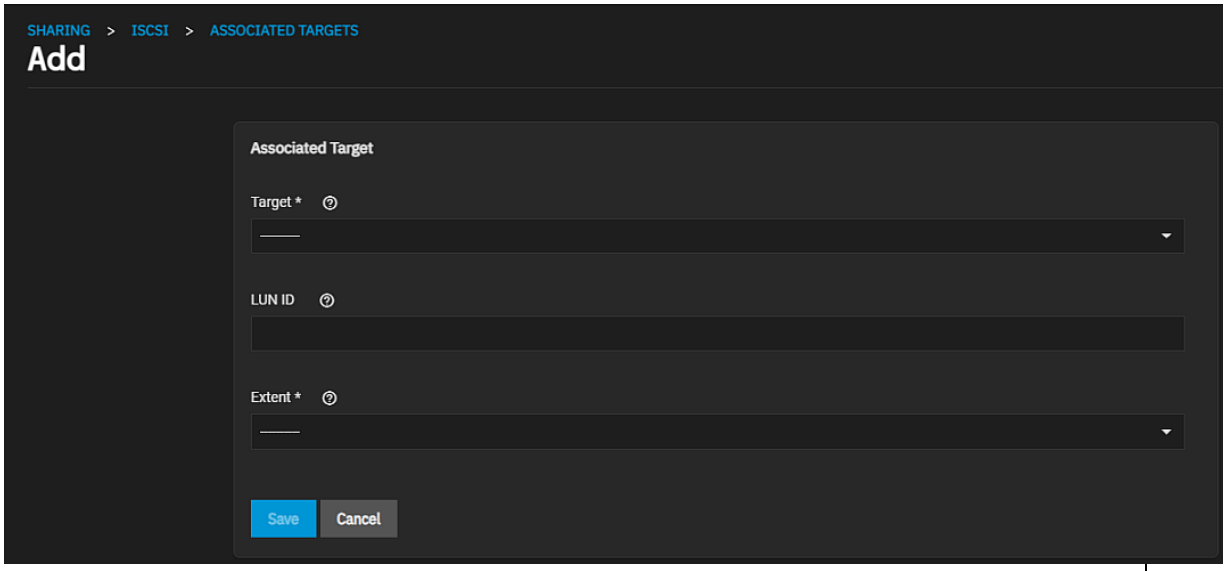
e. Select **Disable Physical Block Size Reporting** if the initiator does not support physical block size values over 4K (MS SQL).

f. (Optional) Select the compatibility settings that apply to your extent. See iSCSI Share Screens for more information.

g. Click **Save**.

7. Add associated storage resources. Click **Associate Targets** tab to open the screen.

a. Click **Add** to open the **Sharing > iSCSI > Associated Targets > Add** screen.



b. Select the target from the **Target** dropdown list.

c. Select the value or enter a value 0 and 1023. Some initiators expect a value below 256. Leave blank to automatically assign the next available ID.

d. Select the option from the **Extent** dropdown.

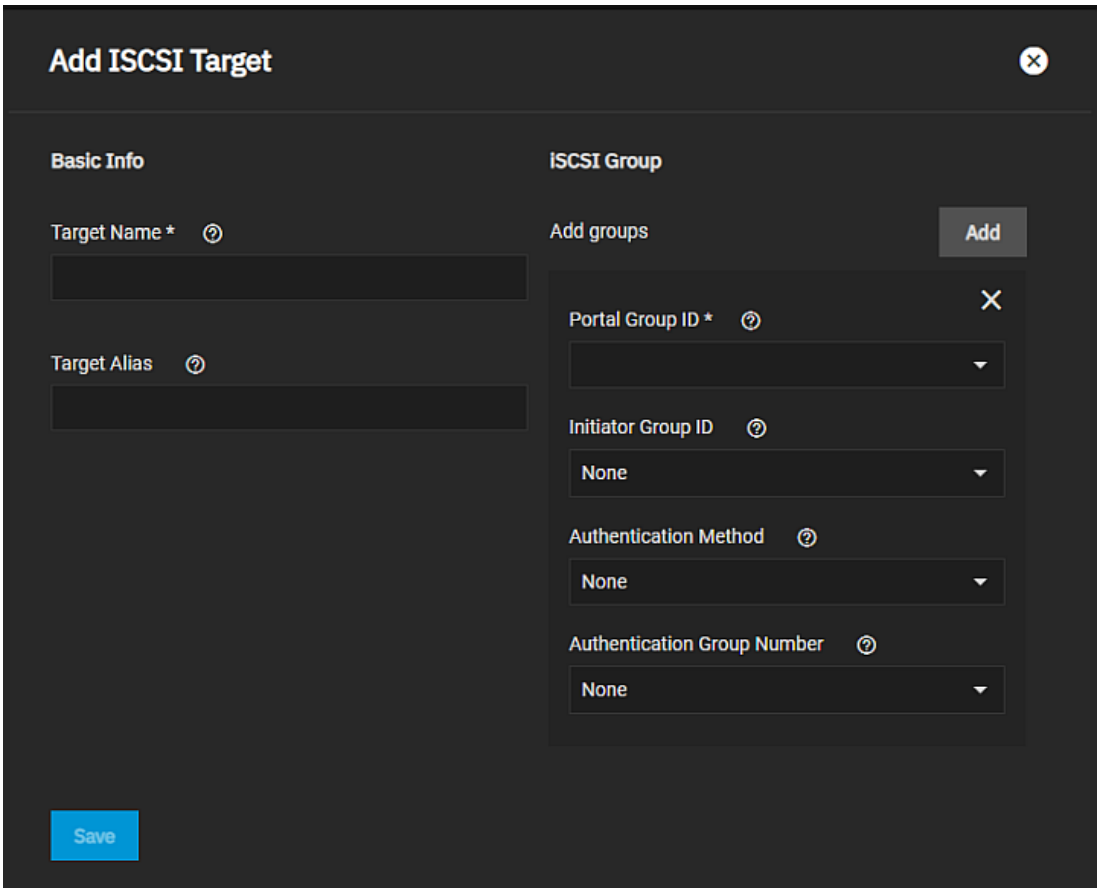
e. Click **Save**

Creating a Quick iSCSI Target

TrueNAS SCALE allows users to add iSCSI targets without having to set up another share.

Click here for more information

Go to **Shares** and click **Add** in the **Block (iSCSI) Shares Targets** widget.

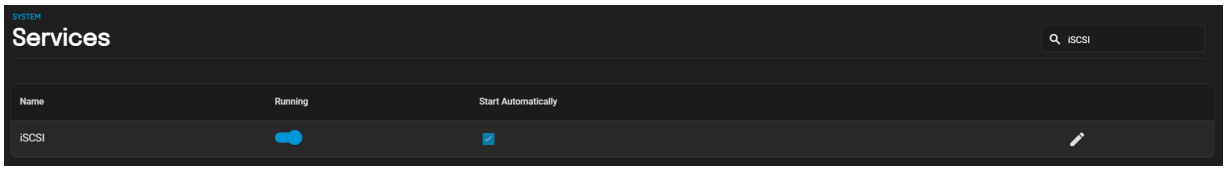


1. Enter a name using lowercase alphanumeric characters plus dot (.), dash (-), and colon (:) in the iqn.format. See the “Constructing iSCSI names using the iqn.format” section of RFC3721.
2. (Optional) Enter a user-friendly name in **Target Alias**.
3. Click **Add** under **iSCSI Group** to display the group settings.
4. Select the group ID from the **Portal Group ID** dropdown.
5. (Optional) Select the group ID in **Initiator Group ID** or leave it set to **None**.
6. (Optional) Select the **Authentication Method** from the dropdown list of options.
7. (Optional) Select the **Authentication Group Number** from the dropdown list. Leave at **None** or enter an integer to represent the number of existing authorized access.
8. Click **Save**.

Starting the iSCSI Service

To turn on the iSCSI service, from the **Block (iSCSI) Shares Targets** widget click the ⋮ and select **Turn On Service**. You can also go to **System Settings > Services** and locate **iSCSI** on the list and click the **Running** toggle to start the service.

Set iSCSI to start when TrueNAS boots up, go to **System Settings > Services** and locate **iSCSI** on the list. Select **Start Automatically**.



Clicking the ✎ returns to the options in **Shares > Block (iSCSI) Shares Targets**.

Related Content

- Block (iSCSI) Share Target Screens
- Using an iSCSI Share
- Increasing iSCSI Available Storage

3.9.2.2 - Using an iSCSI Share

This article provides information on setting up a Linux or Windows system to use a TrueNAS-configured iSCSI block share.

Connecting to and using an iSCSI share can differ between operating systems.

This article provides instructions on setting up a Linux and Windows system to use the TrueNAS iSCSI block share.

Using Linux iSCSI Utilities and Service

This section describes preparing your system to start the iSCSI service, log in to the share and obtian the basename and target TrueNAS configured. It provides information on partitioning the iSCSI disk, making a file system for the share, mounting it, and sharing data.

Click here for more information

Before you begin, open the command line and ensure you have installed the `open-iscsi` utility. To install the utility on an Ubuntu/Debian distribution, enter command `sudo apt update && sudo apt install open-iscsi`. After the installation completes, ensure the **iscsid** service is running using the `sudo service iscsid start` command.

First, with the **iscsid** service started, run the `iscsiadm` command with the discovery arguments and get the necessary information to connect to the share.

```
truenas@LinuxMachine:~$ sudo apt update && sudo apt install open-iscsi
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:1 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:1 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:1 http://us.archive.ubuntu.com/ubuntu focal-security InRelease
Reading package lists... Done
```

Next, discover and log into the iSCSI share.

1. Run the command `sudo iscsiadm \--mode discovery \--type sendtargets \--portal {IPADDRESS}`. The output provides the basename and target name that TrueNAS configured.

   ```
   truenas@LinuxMachine:~$ sudo iscsiadm \--mode discovery \--type sendtargets \--portal 10.10.10.
   10.238.15.118:3260,-1 iqn.2005-10.org.freenas.ctl:iscsishare
   10.238.15.118:3260,-1 iqn.2005-10.org.freenas.ctl:iscsishare2
   10.238.15.118:3260,-1 iqn.2005-10.org.freenas.ctl:iscsifile
   truenas@LinuxMachine:~$
   ```

   Alternatively, enter `sudo iscsiadm -m discovery -t st -p {IPADDRESS}` to get the same output. Note the basename and target name given in the output. You need them to log in to the iSCSI share.

   When a Portal Discovery Authentication Method is CHAP, add the three following lines to /etc/iscsi/iscsid.conf.

   ```
   discovery.sendtargets.auth.authmethod = CHAP
   discovery.sendtargets.auth.username = user
   discovery.sendtargets.auth.password = secret
   ```

   The user for `discovery.sendtargets.auth.username` is set in the **Authorized Access** used by the iSCSI share **Portal**. Likewise, the password to use for `discovery.sendtargets.auth.password` is the **Authorized Access** secret. Without those lines, the iscsiadm does not discover the portal with the CHAP authentication method.

2. Enter comand `sudo iscsiadm \--mode node \--targetname {BASENAME}:{TARGETNAME} \--portal {IPADDRESS} \--login`, where *{BASENAME}* and *{TARGETNAME}* is the discovery command information.

   ```
   truenas@LinuxMachine:~$ sudo iscsiadm \--mode discovery \--type sendtargets \--portal freenas.local
   freenas.local:3260,-1 iqn.2005-10.org.freenas.ctl:iscsi.share
   truenas@LinuxMachine:~$ sudo iscsiadm \--mode node \--targetname iqn.2005-10.org.freenas.ctl:iscsi.
   share \--portal freenas.local \--login
   Loggin in to [iface: default, target: iqn.2005-10.org.freenas.ctl:iscsi.share, portal: freenas.loca
   l,3260] (multiple)
   Login to [iface: default, target: iqn.2005-10.org.freenas.ctl:iscsi.share, portal: freenas.local,32
   60] successful.
   truenas@LinuxMachine:~$
   ```

Now you partition an iSCSI disk.

When the iSCSI share login succeeds, the device shared through iSCSI shows on the Linux system as an **iSCSI Disk**. To view a list of connected disks in Linux, enter command `sudo fdisk -l`.

```
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/sda: 476.96 GiB, 512110190592 bytes, 1000215216 sectors
Disk model: SAMSUNG MZNLN512
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: B7D9E3B0-EBED-4CEA-9CC6-08F2918A54FB

Device       Start        End   Sectors   Size Type
/dev/sda1     2048    1050623   1048576   512M EFI System
/dev/sda2  1050624 1000214527 999163904 476.4G Linux filesystem


Disk /dev/loop8: 240.82 MiB, 252493824 bytes, 493152 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/loop9: 29.84 MiB, 31272960 bytes, 61080 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/sdb: 10 GiB, 10737434624 bytes, 2621444 sectors
Disk model: iSCSI Disk
Units: sectors of 1 * 4096 = 4096 bytes
Sector size (logical/physical): 4096 bytes / 16384 bytes
I/O size (minimum/optimal): 16384 bytes / 1048576 bytes
truenas@LinuxMachine:~$
```

Because the connected iSCSI disk is raw, you must partition it. Identify the iSCSI device in the list and enter `sudo fdisk {/PATH/TO/iSCSIDEVICE}`.

```
truenas@LinuxMachine:~$ sudo fdisk /dev/sdb

Welcome to fdisk (util-linux 2.34).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.


Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1):
First sector (256-2621443, default 256):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (256-2621443, default 2621443):

Created a new partition 1 of type 'Linux' and of size 10 GiB.

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

truenas@LinuxMachine:~$
```

Shell lists the iSCSI device path in the `sudo fdisk -l` output. Use the `fdisk` command defaults when partitioning the disk.

> Remember to type `w` when finished partitioning the disk. The `w` command tells `fdisk` to save any changes before quitting.

```
truenas@LinuxMachine:~$ sudo mkfs /dev/sdb1
mke2fs 1.45.5 (07-Jan-2020)
Discarding device blocks: done
Creating filesystem with 2621188 4k blocks and 655360 inodes
Filesystem UUID: 1b38f07a-bb23-40ab-b1eb-255480e4dbbc
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done

truenas@LinuxMachine:~$
```

After creating the partition on the iSCSI disk, a partition slice displays on the device name. For example, /dev/sdb1. Enter `fdisk -l` to see the new partition slice.

Next, make a file system on the iSCSI disk.

Finally, use `mkfs` to make a file system on the new partition slice. To create the default file system (ext2), enter `sudo mkfs {/PATH/TO/iSCSIDEVICEPARTITIONSLICE}`.


```
truenas@LinuxMachine:~$ sudo mkfs /dev/sdb1
mke2fs 1.45.5 (07-Jan-2020)
Discarding device blocks: done
Creating filesystem with 2621188 4k blocks and 655360 inodes
Filesystem UUID: 1b38f07a-bb23-40ab-b1eb-255480e4dbbc
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done
```


Mount the iSCSI device and share the data.

Enter `sudo mount {/PATH/TO/iSCSIDEVICEPARTITIONSLICE}`. For example, `sudo mount /dev/sdb1 /mnt` mounts the iSCSI device */dev/sdb1* to file */mnt*.

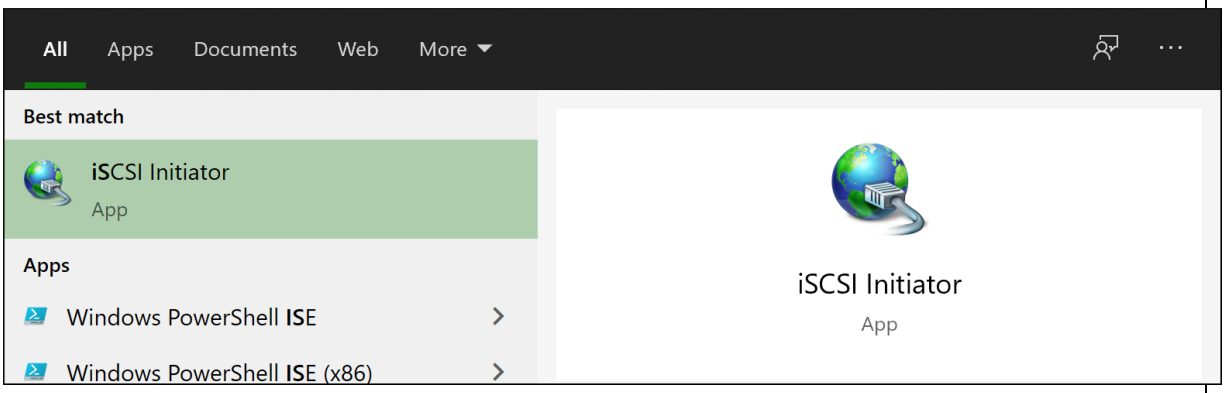
Using the iSCSI Share with Windows

This section provides instructions on setting up Windows iSCSI Initiator Client to work with TrueNAS iSCSI shares.

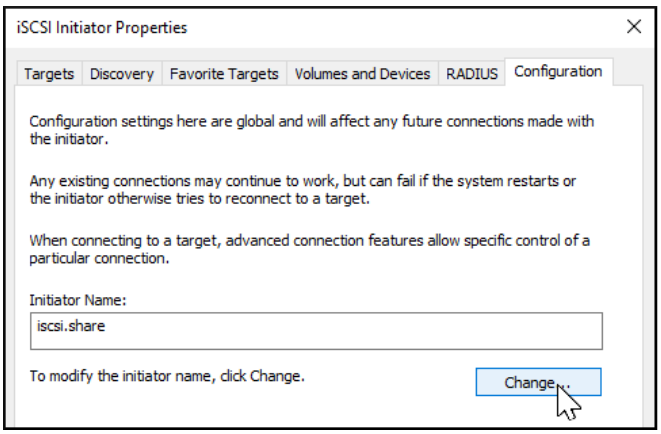
Click here for more information

To access the data on the iSCSI share, clients need to use iSCSI Initiator software. An iSCSI Initiator client is pre-installed in Windows 7 to 10 Pro, and Windows Server 2008, 2012, and 2019. Windows Professional Edition is usually required.

First, click the **Start Menu** and search for the **iSCSI Initiator** application.



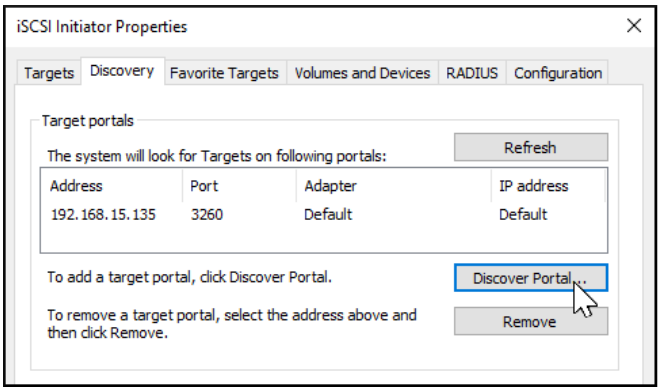
Next, go to the **Configuration** tab and click **Change** to replace the iSCSI initiator with the name created earlier. Click **OK**.



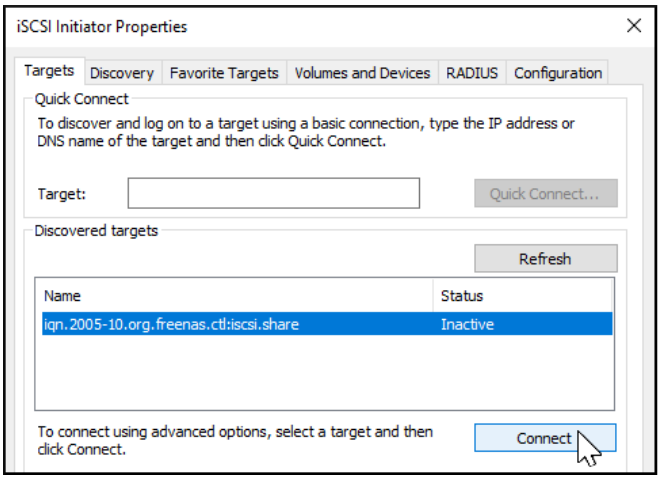
Next, switch to the **Discovery Tab**, click **Discover Portal**, and type in the TrueNAS IP address.

- If TrueNAS changed the port number from the default **3260**, enter the new port number.
- If you set up CHAP when creating the iSCSI share, click **Advanced…**, set **Enable CHAP log on**, and enter the initiator name and the same target/secret set earlier in TrueNAS.

Click **OK**.

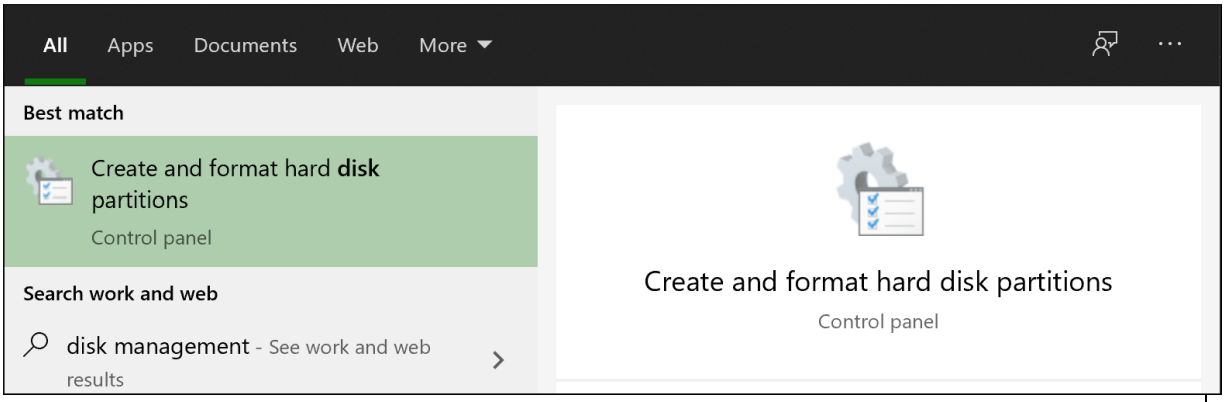


Go to the **Targets** tab, highlight the iSCSI target, and click **Connect**.

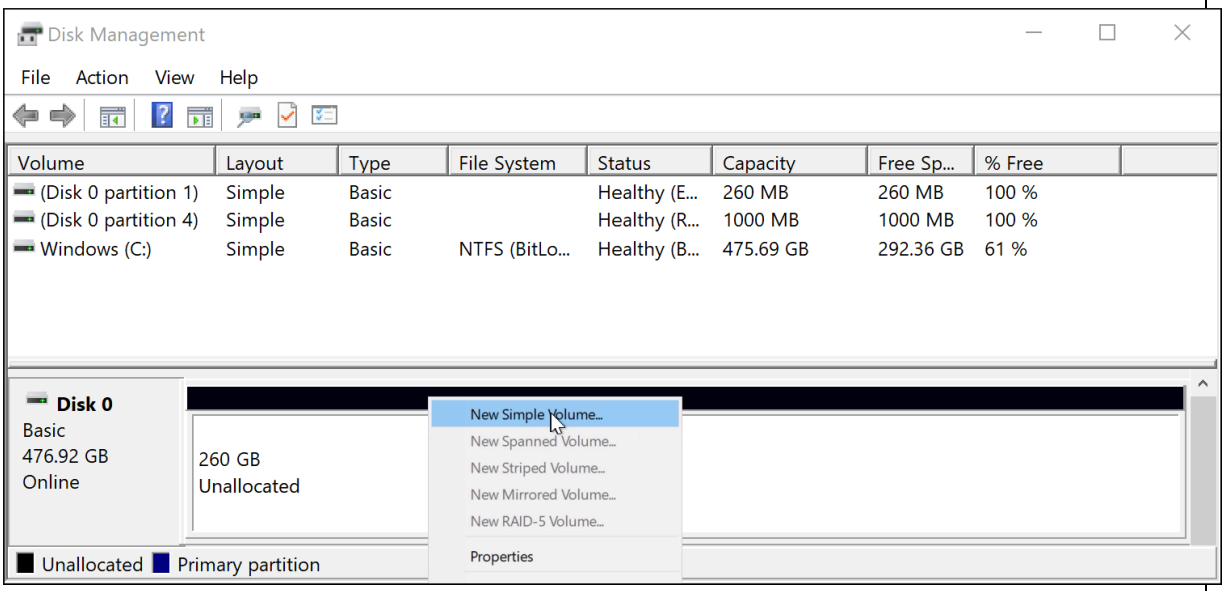


After Windows connects to the iSCSI target, you can partition the drive.

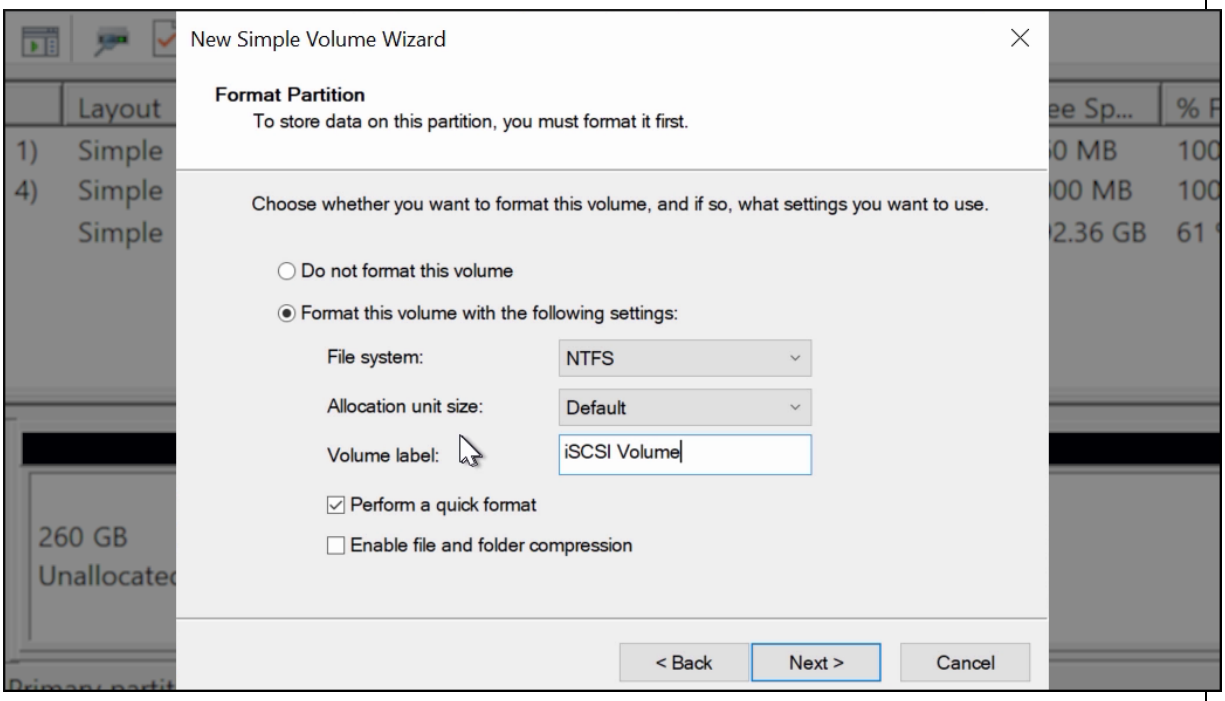
Search for and open the **Disk Management** app.



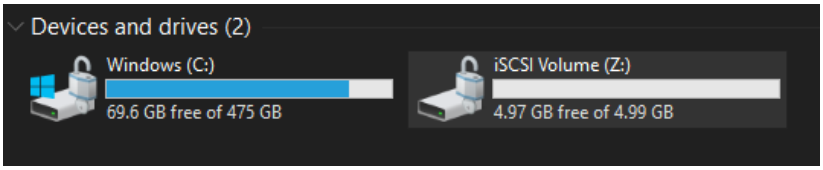
The current state of your drive should be **unallocated**. Right-click the drive and click **New Simple Volume…**.



Complete the wizard to format the drive and assign a drive letter and name.



Finally, go to **This PC** or **My Computer** in **File Explorer**. The new iSCSI volume should display under the list of drives. You should now be able to add, delete, and modify files and folders on your iSCSI drive.



Related Content

- Adding iSCSI Block Shares
- Block (iSCSI) Share Target Screens
- Increasing iSCSI Available Storage

3.9.2.3 - Increasing iSCSI Available Storage

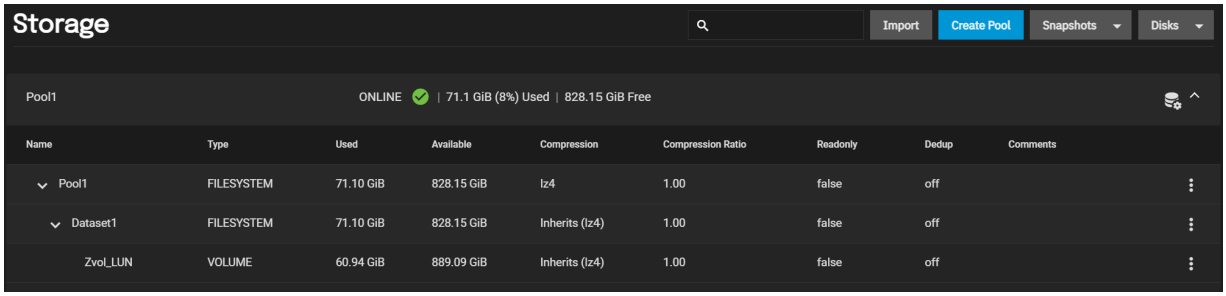
This article provides information on increasing available storage in zvols and file LUNs for iSCSI block shares.

Expanding LUNs

TrueNAS lets users expand Zvol and file-based LUNs to increase the available storage that the iSCSI shares.

Zvol LUNs

To expand a Zvol LUN, go to **Storage** and click the ⋮ next to the Zvol LUN, then select **Edit Zvol**.



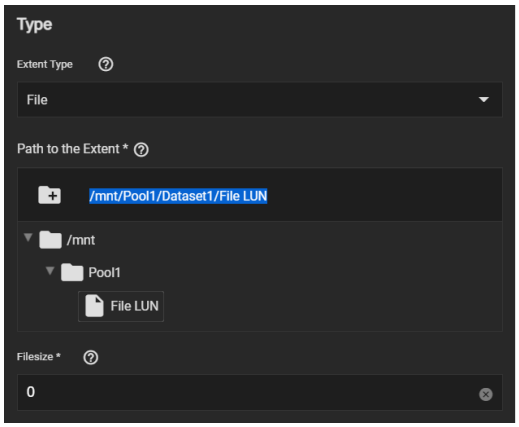
Enter a new size in **Size for this zvol**, then click **SAVE**.

> TrueNAS prevents data loss by not allowing users to reduce the Zvol size. TrueNAS also does not allow users to increase the Zvol size past 80% of the pool size.

File LUNs

You need to know the path to the file to expand a file-based LUN. Go to **Shares** and click **Configure** in the **Block (iSCSI) Shares Targets** window, then select the **Extents** tab.

Click the ⋮ next to the file-based LUN and select **Edit**.



Highlight and copy the path, then click **Cancel**.

Go to **Shell** and input `truncate -s +[size] [path to file]`, then press `Enter`.

Where *[size]* is how much space you want to grow the file by, and *[path to file]* is the file path you copied earlier.

```
Linux truenas.scale.local 5.10.42+truenas #1 SMP Mon Aug 30 21:54:59 UTC 2021 x86_64

        TrueNAS (c) 2009-2021, iXsystems, Inc.
        All rights reserved.
        TrueNAS code is released under the modified BSD license with some files copyrighted by (c) iXsystems, Inc.

        For more information, documentation, help or support, go here: http://truenas.com
Welcome to TrueNAS
Last login: Fri Sep 17 06:52:53 PDT 2021 on pts/2
root@truenas# truncate -s +2g /mnt/Pool1/Dataset1/File LUN
```

An example command could look like this: `truncate -s +2g /mnt/Pool1/Dataset1/File LUN`

Lastly, go back to the extent in **Shares > Block (iSCSI) Shares Targets** and make sure the **Filesize** is set to **0** so that the share uses the actual file size.

Related Content

- Adding iSCSI Block Shares
- Block (iSCSI) Share Target Screens
- Using an iSCSI Share

3.9.3 - Unix Shares (NFS)

Article Summaries

- Adding NFS Shares

  This article provides instructions on adding NFS shares, starting NFS service and accessing the share.

3.9.3.1 - Adding NFS Shares

This article provides instructions on adding NFS shares, starting NFS service and accessing the share.

About UNIX (NFS) Shares

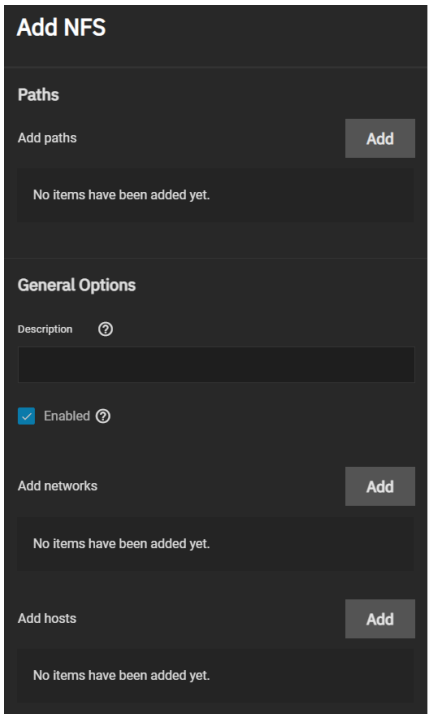
Creating a Network File System (NFS) share on TrueNAS makes a lot of data available for anyone with share access. Depending on the share configuration, it can restrict users to read or write privileges.

To create a new share, make sure a dataset is available with all the data for sharing.

Creating an NFS Share Tutorial Video

Creating an NFS Share

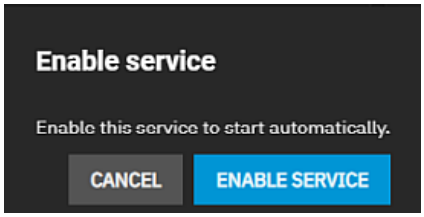
Go to **Shares > Unix (NFS) Shares** and click **Add** to open the **Add NFS** configuration screen.



Click **Add** to display **Add paths** settings, and then enter the path or use the ▸ icon to the left of **/mnt** to locate the dataset and populate the path.

You can enter an optional text to help identify the share in **Description**. Click **Save** to create the share.

After adding the first NFS share, the system opens an enable service dialog.



Enable Service turns the NFS service on and changes the toolbar status to **Running**. If you wish to create the share but not immediately enable it, select **Cancel**.

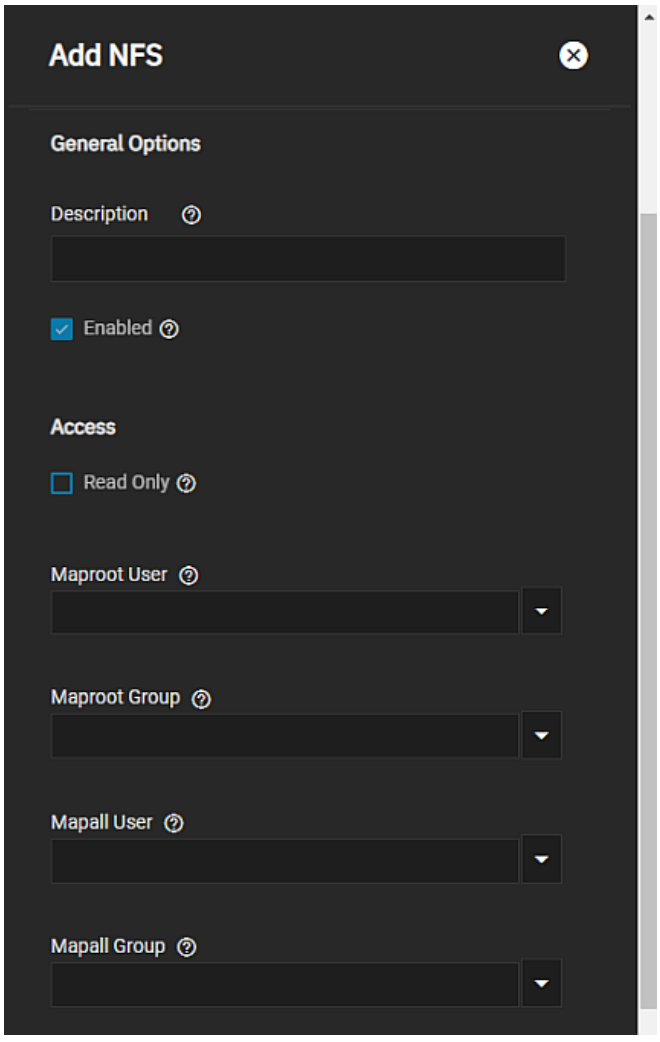
Adding NFS Share Network and Hosts

If you want to enter allowed networks, click **Add** to the right of **Add Networks**. Enter an IP address in the **Authorized Networks** field and select the mask CIDR notation. Click **Add** for each network address and CIDR you want to define as an authorized network. Defining an authorized network restricts access to all other networks. Leave empty to allow all networks.

If you want to enter allowed systems, click **Add** to the right of **Add hosts**. Enter a host name or IP address to allow that system access to the NFS share. Click **Add** for each allowed system you want to define. Defining authorized systems restricts access to all other systems. Leave the field empty to allow all systems access to the share.

Adjusting Access Permissions

If you want to tune the NFS share access permissions or define authorized networks, click **Advanced Options**.



Select **Read Only** to prohibit writing to the share.

To map user permissions to the *root* user, enter a string or select the user from the **Maproot User** dropdown list. To map the user permissions to all clients, enter a string or select the user from the **Mapall User** dropdown list.

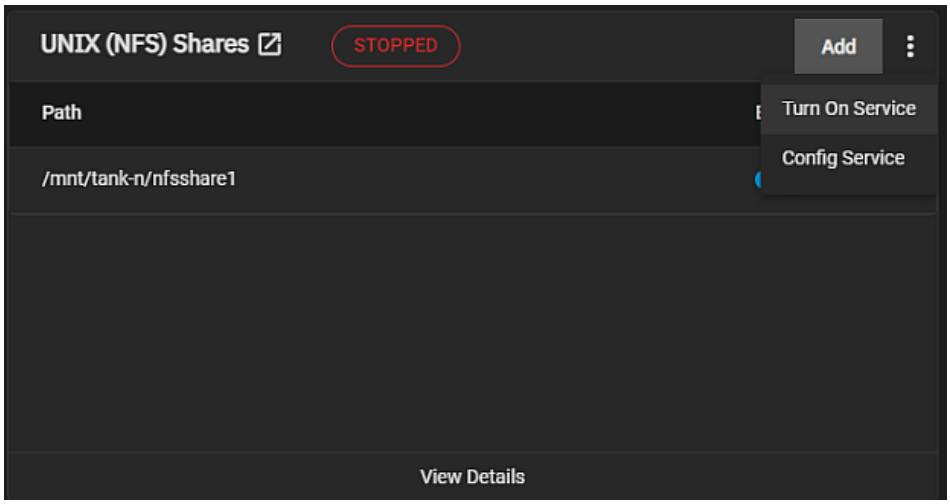
To map group permissions to the *root* user, enter a string or select the group from the **Maproot Group** dropdown list. To map the group permissions to all clients, enter a string or select the group from the **Mapall Group** dropdown list.

Editing an NFS Share

To edit an existing NFS share, go to **Shares > Unix Shares (NFS)** and click the share you want to edit. The **Edit NFS** screen settings are identical to the share creation options.

Starting the NFS Service

To begin sharing, click the ⋮ on the toolbar displays options turn the NFS service on or off. **Turn Off Service** displays if the service is running or **Turn On Service** if the service is stopped.



Or you can go to **System Settings > Services**, locate **NFS** and click the toggle to running. Select **Start Automatically** if you want NFS to activate when TrueNAS boots.

Configuring NFS Service

To configure NFS service settings click ✎ on the **System Settings > Services** screen.

Unless you need a specific setting, we recommend using the default NFS settings.

When TrueNAS is already connected to Active Directory, setting **NFSv4** and **Require Kerberos for NFSv4** also requires a Kerberos Keytab.

Connecting to the NFS Share

Although you can connect to an NFS share with various operating systems, it is recommended to use a Linux/Unix operating system.

First, download the `nfs-common` kernel module. You can do this using the installed distribution package manager. For example, on Ubuntu/Debian, enter command `sudo apt-get install nfs-common` in the terminal.

After installing the module, connect to an NFS share by entering command `sudo mount -t nfs {IPaddressOfTrueNASsystem}:{path/to/nfsShare} {localMountPoint}`. Where *{IPaddressOfTrueNASsystem}* is the remote TrueNAS system IP address that contains the NFS share, *{path/to/nfsShare}* is the path to the NFS share on the TrueNAS system, and *{localMountPoint}* is a local directory on the host system configured for the mounted NFS share. For example, `sudo mount -t nfs 10.239.15.110:/mnt/Pool1/NFS_Share /mnt` mounts the NFS share *NFS_Share* to the local directory */mnt*.

You can also use the linux `nconnect` function to let your NFS mount to support multiple TCP connections. To enable `nconnect`, enter command `sudo mount -t nfs -o rw,nconnect=16 {IPaddressOfTrueNASsystem}:{path/to/nfsShare} {localMountPoint}`. Where *{IPaddressOfTrueNASsystem}*, *{path/to/nfsShare}*, and *{localMountPoint}* are the same you used when connecting to the share. For example, `sudo mount -t nfs -o rw,nconnect=16 10.239.15.110:/mnt/Pool1/NFS_Share /mnt`.

By default, anyone that connects to the NFS share only has read permission. To change the default permissions, edit the share, open the **Advanced Options**, and change the **Access** settings.

> ESXI 6.7 or later is required for read/write functionality with NFSv4 shares.

Related Content

- Configuring NFS Service
- NFS Services Screen
- NFS Shares Screens

3.9.4 - WebDAV Shares

Article Summaries

- Configuring WebDAV Shares

  This article provides instructions on adding a WebDAV share, configuring and starting the WebDAV service, and then connecting to it with a web browser.

3.9.4.1 - Configuring WebDAV Shares

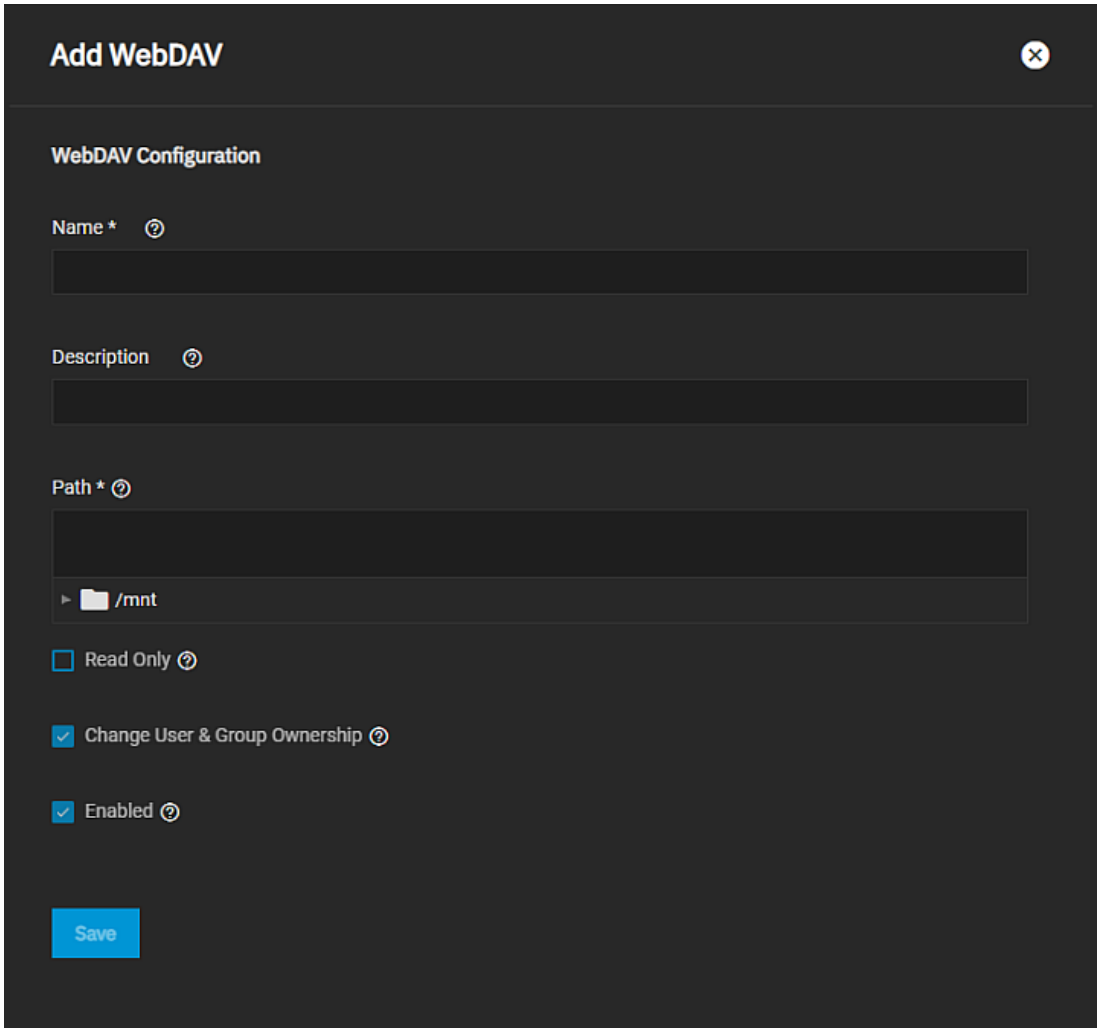
This article provides instructions on adding a WebDAV share, configuring and starting the WebDAV service, and then connecting to it with a web browser.

A Web-based Distributed Authoring and Versioning (WebDAV) share makes it easy to share a TrueNAS dataset and its contents over the web.

To create a new share, make sure a dataset is available with all the data for sharing.

Configuring a WebDAV Share

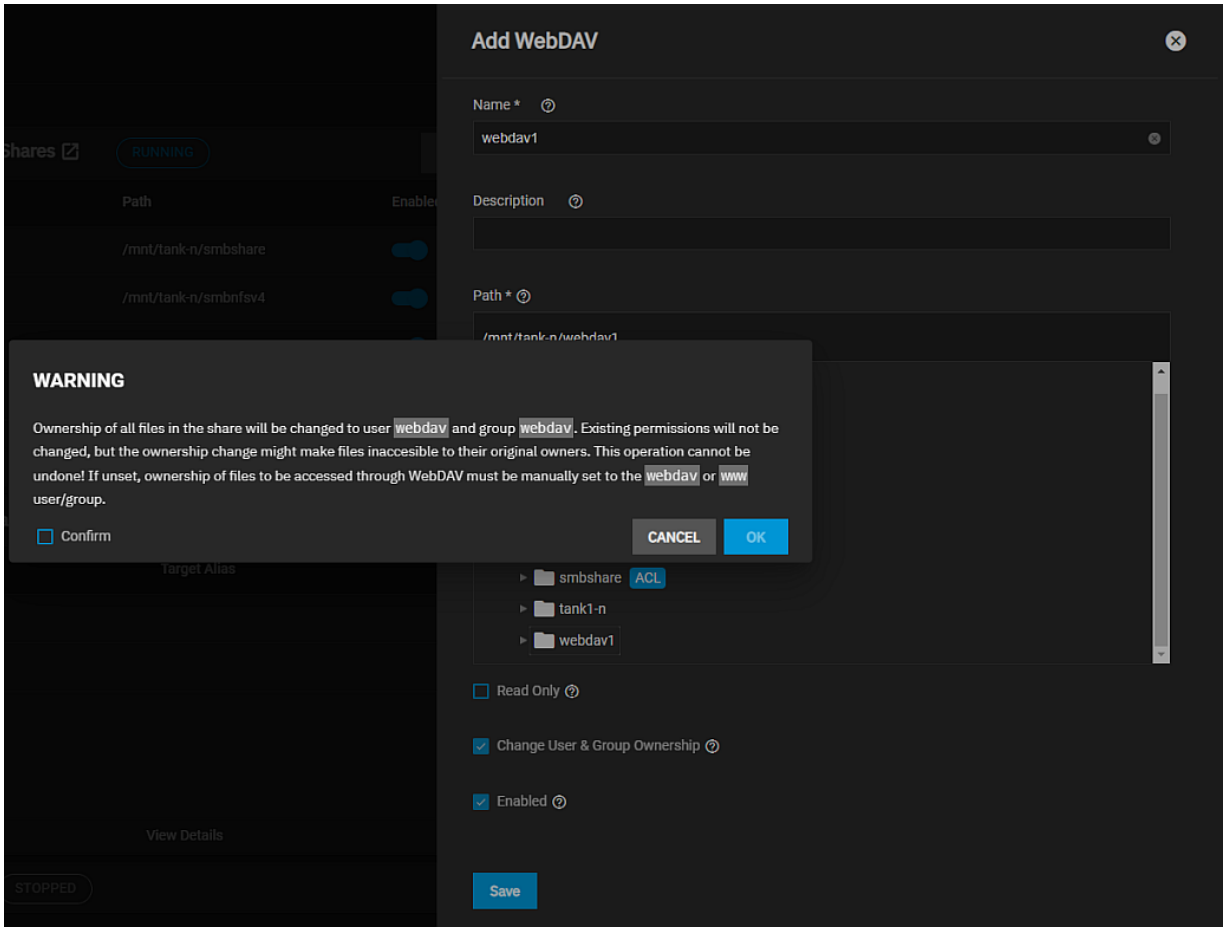
Go to **Shares** and click on **Add** on the **WebDAV** widget. The first WebDAV share added to your system opens the **No WebDAV** screen. Click **Add WebDAV** to open the **Add WebDAV** configuration screen.



Enter a share **Name**.

Add the path to the pool or dataset in **Path**. Enter or use the icon to the left of **/mnt** to browse to the dataset and populate the path. An optional **Description** helps to identify the share. To prevent user accounts from modifying the shared data, set **Read Only**.

To change existing ownership of all files in the share to the **webdav** user and group accounts leave **Change User & Group Ownership** selected. This default simplifies WebDAV share permission, but is unexpected, so the web interface displays a warning:



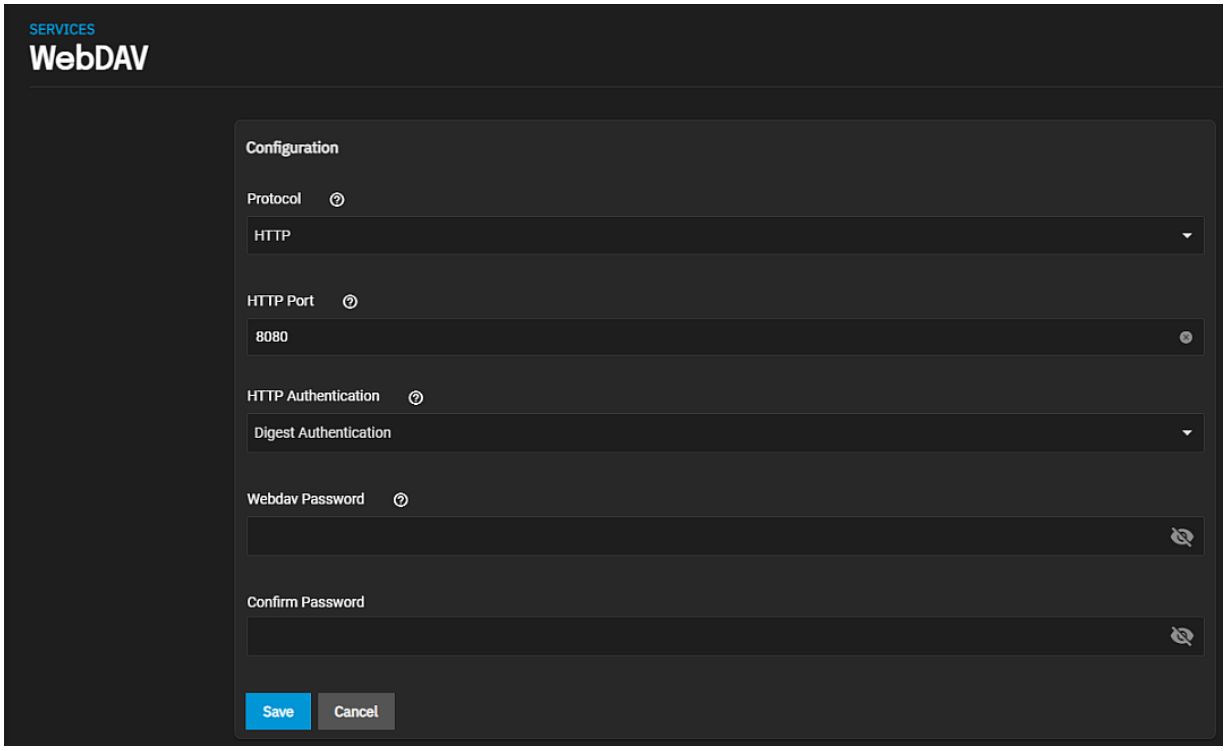
If you clear the **Change User & Group Ownership** checkbox this warning does not display and you must manually set shared file ownership to the **webdav** or **www** user and group accounts.

Click **Save** to add the share. The **Enable service** dialog opens. Click **Enable Service** to start the service or click **Cancel** to start the service at a later time.

Configuring WebDAV Service

To automatically start the service when TrueNAS boots, select **Start Automatically**.

Click to change the service settings.



For better data security, set **Protocol** to **HTTPS**. If you require it, you must choose an SSL certificate (*freenas_default* is always available). Define a number in the **Port** field. But do not use the default **8080** or reuse the same port number. Make sure the network is not already using the WebDAV service port.

To prevent unauthorized access to the shared data, set **HTTP Authentication** to either **Basic** or **Digest** and create a new **Webdav Password**. Do not use the default password **davtest** as it is a known password.

TrueNAS requires a username and password when setting the **Authentication** WebDAV service option to **Basic** or **Digest**. Enter the user name **webdav** and the password defined in the WebDAV service.

Click **Save** after making changes.

Activating the WebDAV Service

Creating a share allows users to activate the WebDAV service.

You can enable the serivce from the **Sharing** screen **Enable Service** dialog or from the **WebDAV** widget toolbar option.

Click ⋮ and then click **Turn On Service**. Or you can go to **System Settings > Services** and scroll down to **WebDAV** and click the toggle to **Start**.

Connecting to the WebDAV Share

WebDAV shared data is accessible from a web browser. To see the shared data, open a new browser tab and enter `{PROTOCOL}://{TRUENASIP}:{PORT}/{SHAREPATH}` where the elements in curly brackets {} are variables to replace with your chosen WebDAV share and service settings. For example: *https://10.2.1.1:8081/newdataset*

Related Content

- Adding Cloud Credentials
- Cloud Credentials Screens
- WebDAV Shares Screens
- Configuring WebDAV Service
- WebDAV Service Screen

3.9.5 - Windows Shares (SMB)

Article Summaries

- Adding SMB Shares

  This article provides instructions to add an SMB share, starting the service, and mounting the share.

- Managing SMB Shares

  This article provides instructions on managing existing SMB shares, adding share ACLs, and managing file system ACLs

- Using SMB Shadow Copy

  This article provides information on SMB share shadow copies, enbling shadow copies, and resolving an issue with Microsoft Windows 10 v2004 release.

- Setting Up SMB Home Shares

  This article provides instructions to set up SMB home shares.

3.9.5.1 - Adding SMB Shares

This article provides instructions to add an SMB share, starting the service, and mounting the share.

About Windows (SMB) Shares

SMB (also known as CIFS) is the native file sharing system in Windows. SMB shares can connect to most operating systems, including Windows, MacOS, and Linux. TrueNAS can use SMB to share files among single or multiple users or devices.

SMB supports a wide range of permissions, security settings, and advanced permissions (ACLs) on Windows and other systems, as well as Windows Alternate Streams and Extended Metadata. SMB is suitable for managing and administering large or small pools of data.

TrueNAS uses Samba to provide SMB services. The SMB protocol has multiple versions. An SMB client typically negotiates the highest supported SMB protocol during SMB session negotiation. Industry-wide, SMB1 protocol (sometimes referred to as NT1) usage is being deprecated for security reasons. However, most SMB clients support SMB 2 or 3 protocols, even when they are not default.

> Legacy SMB clients rely on NetBIOS name resolution to discover SMB servers on a network. TrueNAS disables the NetBIOS Name Server (nmbd) by default. Enabled in **Network** if you require its functionality.
>
> MacOS clients use mDNS to discover SMB servers present on the network. TrueNAS enables the mDNS server (avahi) by default.
>
> Windows clients use WS-Discovery to discover the presence of SMB servers, but network discovery can be disabled by default depending on the Windows client version.
>
> Discoverability through broadcast protocols is a convenience feature and not required to access an SMB server.

Adding SMB Shares Video Tutorial

Adding an SMB Share

Adding an SMB share to your system involves several steps to add the share and get it working.

First you set up the storage for your new share.

Next you create local user accounts. It is also possible to use Directory Services to provide additional user accounts.

After adding or modifying local users, modify the dataset ACL.

Now you create the SMB share. You can create a basic SMB share or for more specific share types or feature requirements, use the Advanced Options instructions before you save the share.

After adding the share you start the service and mount it to your other system.

Adding an SMB Share Dataset

Before creating the SMB share, first add the dataset the share uses for data storage.

We recommend creating a new dataset with the **Share Type** set to **SMB** for the new SMB share.

What does this do?

TrueNAS creates the ZFS dataset with these settings:

- **ACL Mode** set to **Restricted** The **ACL Type** influences the **ACL Mode** setting. When **ACL Type** is set to **Inherit** or **POSIX**, you cannot change the **ACL Mode** setting. When **ACL Type** is set to **NFSv4** you can change the **ACL Mode** setting to **Restricted**.
- **Case Sensitivity** set to **Insensitive**

TrueNAS also applies a default access control list to the dataset. This default ACL is restrictive and only allows access to the dataset owner and group. You can modify the ACL later according to your use case.

Creating Local User Accounts

Use **Credentials > Local Users** to add new users to your TrueNAS.

By default, all new local users are members of a built-in SMB group called **builtin_users**.

Click here for more information
For more information on the **builtin_users** group, go to **Credentials > Local Users** and click the **Toggle Built-In Users** button at the top right of the screen. Scroll down to the **smbguest** user and click on the name. Click **Edit** to view the **Edit User** screen. The **Auxiliary Group** field displays the **builtin_user** group.

You can use the group to grant access to all local users on the server or add more groups to fine-tune permissions to large numbers of users.

> You cannot access SMB shares with the root user, or user accounts built-in to TrueNAS or those without the **smb** flag.

Why not just allow anonymous access to the share?
Anonymous or guest access to the share is possible, but it is a security vulnerability. Major SMB client vendors are deprecating it, partly because signing and encryption are not possible for guest sessions.

What about LDAP users?

If you want LDAP server users to access the SMB share, go to **Credentials > Directory Services**. If an LDAP server is configured, select the server and click **Edit** to display the **LDAP** configuration screen. If not configured, click **Configure LDAP** to display the **LDAP** configuration screen. Click **Advanced Options** and select **Samba Schema (DEPRECATED - see help text**.

> Only set LDAP authenication for SMB share is required and the LDAP server is already configured with Samba attributes. Support for **Samba Schema** is officially deprecated in Samba 4.13. This feature will be removed after Samba 4.14. Users should begin upgrading legacy Samba domains to Samba AD domains.

Local TrueNAS user accounts no longer have access to the share.

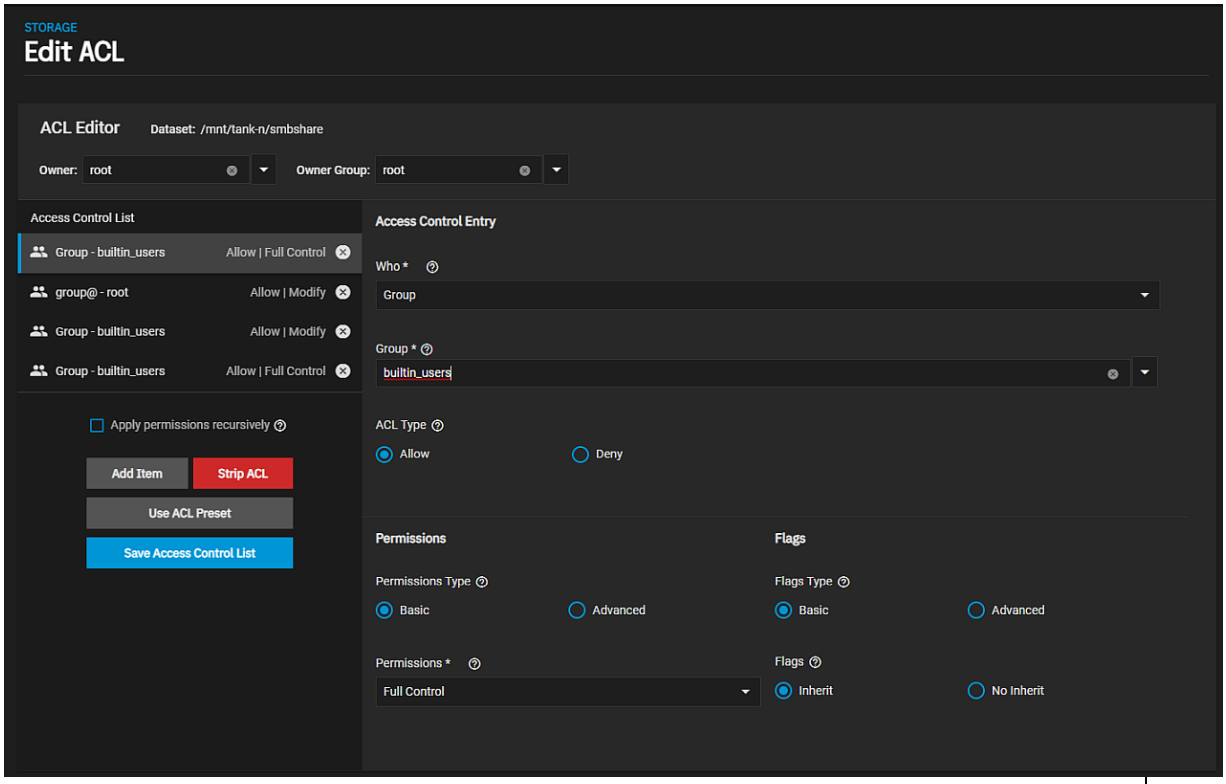
Tuning the Dataset ACL

After creating a dataset and accounts, you need to investigate your access requirements and adjust the dataset ACL to match. Many home users typically add a new ACL entry that grants **FULL_CONTROL** to the **builtin_users** group with the flags set to **INHERIT**.

Click here for instructions

To change or add permissions for the **builtin_users** group, go to **Storage**,

1. Click the ⋮ for your SMB dataset and then click on **View Permissions**.
2. Click the pencil icon. The **Edit ACL** screen for the dataset displays.
3. Check the **Access Control List** to see if this user is on the list and has the correct permissions. If not add this ACE item.



a. Enter **Group** in the **Who** field or use the dropdown list to select **Group**.

b. Begin typing **builtin_users** in the **Group** field to display a filtered list of groups you can select from and then select **builtin_users**.

c. Verify **Full Control** displays in **Permissions**. If not, select it from the dropdown list.

d. Click **Save Access Control List** to add the ACE item.

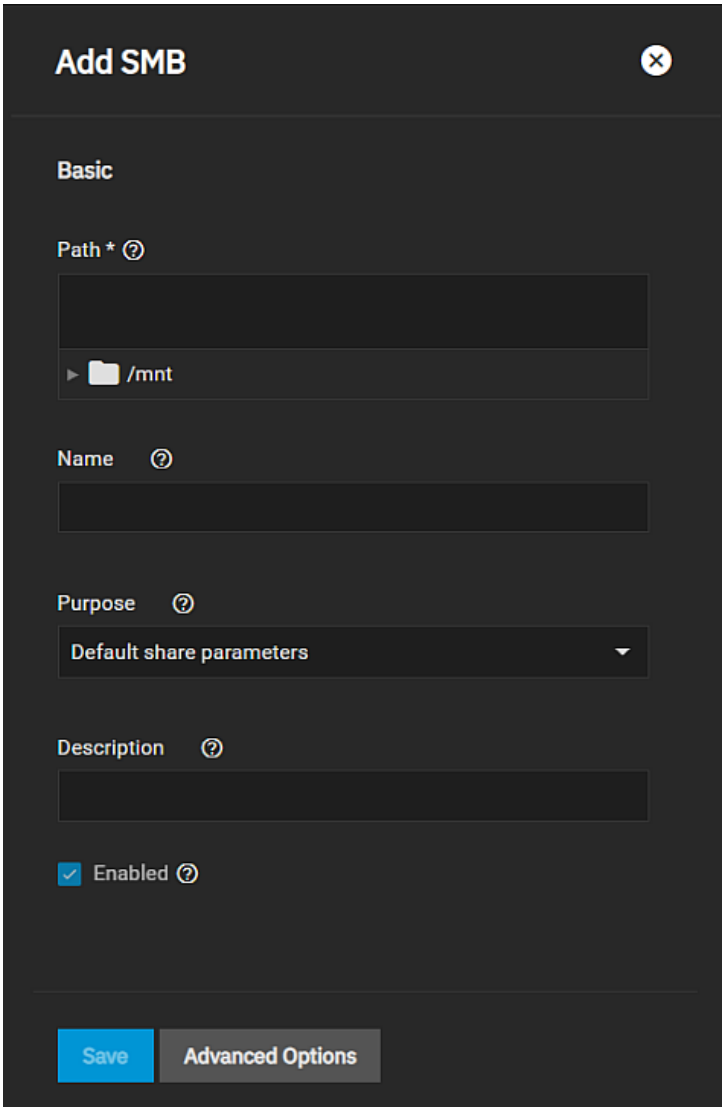
See Permissions for more information on editing dataset permissions.

> You cannot access SMB shares with the root user. Always change SMB dataset ownership to the intended SMB user.

Creating the SMB Share

To create a basic Windows SMB share, go to **Shares**.

1. Click on **Windows Shares (SMB)** to select it and then click **Add**. The **Add SMB** configuration screen displays the **Basic Options** settings.



2. Enter the SMB share **Path** and **Name**.

   The **Path** is the directory tree on the local file system that TrueNAS exports over the SMB protocol.

   The **Name** is the SMB share name, which forms part of the full share pathname when SMB clients perform an SMB tree connect. Because of how the SMB protocol uses the name, it must be less than or equal to 80 characters and it cannot have any invalid characters as specified in Microsoft documentation MS-FSCC section 2.1.6. If you do not enter a name the share name becomes the last component of the path.

3. (Optional) Select a preset from the **Purpose** dropdown list to apply and lock or unlock pre-determined **Advanced Options** settings for the share. To retain control over all the share **Advanced Options** settings, select **No presets**.

4. (Optional) Enter a **Description** to help explain the share purpose.

5. Select **Enabled** to allow sharing of this path when the SMB service is activated. Leave it cleared if you want to disable but not delete the share configuration.

6. Click **Save** to create the share and add it to the **Shares > Windows (SMB) Shares** list.

You can also choose to enable the SMB service at this time.

Configuring Share Advanced Options Settings

For a basic SMB share you do not need to use the **Advanced Options** settings, but if you set **Purpose** to **No Presets**, click **Advanced Options** to finish customizing the SMB share for your use case.

The following are possible use cases, but for all settings see SMB Shares Screens.

Enabling ACL Support

To add ACL support to the share, select **Enable ACL**, and then see Managing SMB Shares for more on configuring permissions for the share and the file system.

Setting Up Guest Access

If you want to allow guest access to the share, select **Allow Guest Access**.

Click here for more information

The privileges are the same as the guest account. Guest access is disabled by default in Windows 10 version 1709 and Windows Server version 1903. Additional client-side configuration is required to provide guest access to these clients.

- **MacOS clients**: Attempting to connect as a user that does not exist in FreeNAS *does not* automatically connect as the guest account.
- **Connect As: Guest** Specifically choose this option in macOS to log in as the guest account. See the Apple documentation for more details.

Setting Up Read or Write Access

To prohibit writes to the share, select **Export Read Only**.

To restrict share visibility to users with read or write access to the share, select **Access Based Share Enumeration**. See the smb.conf manual page.

Setting Up Host Allow and Host Deny

To control allowed or denied host names or IP addresses, use the **Host Allow** and **Host Deny** options.

Click here for more information

Use the **Hosts Allow** field to enter a list of allowed hostnames or IP addresses. Separate entries by pressing `Enter`. You can find a more detailed description with examples here. Use the **Hosts Deny** field to enter a list of denied hostnames or IP addresses. Separate entries by pressing `Enter`.

The **Hosts Allow** and **Hosts Deny** fields work together to produce different situations:

- If neither **Hosts Allow** or **Hosts Deny** contains an entry, then SMB share access is allowed for any host.
- If there is a **Hosts Allow** list but no **Hosts Deny** list, then only allow hosts on the **Hosts Allow** list.
- If there is a **Hosts Deny** list but no **Hosts Allow** list, then allow all hosts on the **Hosts Deny** list.
- If there is both a **Hosts Allow** and **Hosts Deny** list, then allow all hosts on the **Hosts Allow** list. If there is a host not on the **Hosts Allow** and not on the **Hosts Deny** list, then allow it.

Approving Apple Software Compatibility

AFP shares are deprecated and not available in SCALE. To customize your SMB share to work with a migraged AFP share or with your MacOS, use the **Advanced Options** settings provided for these uses cases.

Click here for more information

Time Machine enables Apple Time Machine backups on this share.

Legacy AFP Compatibility controls how the SMB share reads and writes data. Leave unset for the share to behave like a normal SMB share and set for the share to behave like the deprecated Apple Filing Protocol (AFP). Only set this when this share originated as an AFP sharing configuration. This is not required for pure SMB shares or macOS SMB clients.

Use Apple-style Character Encoding converts NTFS illegal characters in the same manner as MacOS SMB clients. By default, Samba uses a hashing algorithm for NTFS illegal characters.

Starting the SMB Service

To connect to an SMB share you must start the related system service. You can start the service from the **Windows SMB Share** header on the **Sharing** screen or on the **System Settings > Services** screen.

Starting the Service Using the Windows SMB Share

From the main **Sharing** screen, click on the **Windows (SMB) Shares** ⋮ to display the service options which are **Turn Off Service** if the service is running or **Turn On Service** if the service is stopped.

Each SMB share on the list also has a toggle you can use to enable or disable the service for that share.

Starting the Service Using the System Settings

To make SMB share available on the network, go to **System Settings > Services** and click the toggle to running for **SMB**. Set **Start Automatically** if you want the service to activate when TrueNAS boots.

Service Configuration

Configure the SMB service by clicking . Unless you need a specific setting or are configuring a unique network environment, we recommend the default settings.

Mounting the SMB Share

The instructions in this section cover mounting the SMB share on system with the following operating systems.

Mounting on Linux System

Verify that your Linux distribution has the required CIFS packages installed.

Click here for more information

Create a mount point: `sudo mkdir /mnt/smb_share`.

Mount the volume. `sudo mount -t cifs //computer_name/share_name /mnt/smb_share`.

If your share requires user credentials, add the switch `-o username=` with your username after `cifs` and before the share address.

Mounting on Windows System

Have the information on the Windows drive letter, computer name and share name ready before you start.

Click here for more information

To mount the SMB share to a drive letter on Windows, open the command line and run the following command with the appropriate drive letter, computer name, and share name.

```
net use Z: \\computer_name\share_name /PERSISTENT:YES
```

Mounting on Apple System

Have the user name and password for the user assigned to pool or for the guest if the share has guest access ready before you begin.

Click here for more information

Open **Finder > Go > Connect To Server** Enter the SMB address: `smb://192.168.1.111`.

Input the username and password for the user assigned to that pool or guest if the share has guest access.

Mounting on FreeBSD System

Mounting on a FreeBSD system involves creating the mount point and then mounting the volume.

Click here for more information

Create a mount point: `sudo mkdir /mnt/smb_share`.

Mount the volume. `sudo mount_smbfs -I computer_name\share_name /mnt/smb_share`.

Related Content

- SMB Shares Screens
- Managing SMB Shares
- Using SMB Shadow Copy
- Setting Up SMB Home Shares
- Configuring SMB Service
- SMB Service Screen
- Spotlight Support on a SCALE SMB Share

Releated AFP Articles

- SMB Shares Screens
- Managing SMB Shares
- AFP Migration

3.9.5.2 - Managing SMB Shares

This article provides instructions on managing existing SMB shares, adding share ACLs, and managing file system ACLs

---

To access SMB share management options from the **Sharing > Windows (SMB) Shares** screen you need to access the **Sharing >SMB** screen that lists all SMB shares on the system. To access this, after going to **Shares**, click the **Windows (SMB) Shares** launch icon.

Managing SMB Shares

To manage an SMB share use the **Sharing > SMB** details screen. Click the ⋮ for the share you want to manage.

Click on the dropdown list option for the operation you want to perform.

- Click **Edit** to open the **Edit SMB** screen where you can change any setting for the share.
- Click **Edit Share ACL** to open the **Sharing > SMB > Share ACL** screen where you can add or edit ACL entries.
- Click **Edit Filesystem ACL** to open the **Storage > Edit *POSIX.1e* ACL** screen where you can edit the SMB dataset permissions. The SMB dataset ACL options you set determine the **ACL Editor** screen displayed.
- Click **Delete** to open a delete confirmation dialog where you delete the share and remove it from the system. Delete does not affect shared data.

Modifying ACL Permissions for SMB Shares

You have two options that modify ACL permissions for SMB shares:

- To modify SMB share ACL permissions that apply to the users and groups and permissions of the entire SMB share use **Edit Share ACL**.
- To modify ACL permissions at the dataset level for the users and groups that own or have specific permissions to the shared dataset.

See both the Permissions article for more details on configuring ACLs and Edit ACL Screen article for more information on the ACL editor screens and setting options.

Also see Tuning the Dataset ACL for an example of modifying ACL permissions for an SMB share.

Configuring SMB Share ACL

To configure an Access Control List (ACL) entry for an SMB share use the **Edit Share ACL** option. This opens the **SMB> Share ACL** screen. This screen is separate from file system permissions and applies at the entire SMB share level. Changes made to permissions on this screen for the selected SMB share do not apply to other file sharing protocol clients or other SMB shares that export the same share **Path**.

> You cannot access SMB shares with the root user. Always change SMB dataset ownership to the intended SMB user.

This ACL determines the browse list if you enable **Access Based Share Enumeration**. See SMB Share Screens for more information on settings.

Open is the default.

From the main **Sharing** screen, click on either **Windows (SMB) Share** or **View Details** to open the **Sharing > SMB** details screen. Click the ⋮ icon for the SMB share you want to edit ACL permissions for and then click **Edit Share ACL**.

Either select new values for the ACL entry or click **Add** to add a new block of **Add share_ACL** settings. Click **Save** when you finish your changes.

Configuring Dataset File System ACL

To configure an Access Control List (ACL) entry for the SMB share the path (defined in **Path**) at the dataset level, use the **Edit Filesystem ACL** option.

The ACL type setting on the **Add Dataset** or **Edit Dataset** configuration screen, in **Advanced Options**, determines the ACL editor screen or windows you see when you click **Edit Filesystem ACL**.

- If you set the dataset **ACL Type** to **POSIX**, the **Select a preset ACL** window displays first. After you select a preset and click **Continue** a POSIX type **ACL Editor** screen displays.
- If you set the dataset **ACL Type** to **NFSv4**, the NFSv4 type **ACL Editor** displays.

Since SCALE gives users the option to use either POSIX or NFSv4 share ACL types, the **ACL Editor** screen differs depending on which ACL type the file system uses.

Both the POSIX and NFSv4 **ACL Editors** allow you to define ACL user accounts or groups that own or have specific permissions to the shared dataset. The **User** and **Group** values show which accounts own or have full permissions to the dataset. Change the default settings to your preferred primary account and group and select **Apply permissions recursively** before saving any changes.

To define permissions for a specific user account or group for this SMB share at the dataset level, click **Add Item**. Select a **User** or **Group** from the **Who** dropdown list, then select a specific user or group account. Define how the settings apply to the account, then specify the permissions to apply. For example, to only allow the *newuser* user permission to view dataset contents but not make changes, set the **ACL Type** to **Allow** and **Permissions** to **Read**.

See both the Permissions for more details on configuring ACLs and Edit ACL Screen for information on the ACL editor screens and setting options.

Using Preset ACL Entries (ACEs) on an NFSv4 ACL Editor

To rewrite the current ACL with a standardized preset, click **Use ACL Preset** and select an option:

NFS4_OPEN to give the owner and group full dataset control. All other accounts can modify the dataset contents. **NFS4_RESTRICTED** to give the owner full dataset control. Group can modify the dataset contents. **NFS4_HOME** to give the owner full dataset control. Group can modify the dataset contents. All other accounts can navigate the dataset.

When finished, click **Save Access Control List** to add this to the **Access Control List**.

Using ACL Entries (ACEs) on a POSIX ACL Editor

If the file system uses a POSIX ACL, the first option presented is to select a preset.

To rewrite the current ACL with a standardized preset, click **Use ACL Preset** and select an option:

POSIX_OPEN to give owner and group full dataset control. All other accounts can modify the dataset contents. **POSIX_RESTRICTED** to give owner full dataset control. Group can modify the dataset contents. **POSIX_HOME** to give owner full dataset control. Group can modify the dataset contents. All other accounts can navigate the dataset.

Related Content

- Adding SMB Shares
- SMB Shares Screens
- Using SMB Shadow Copy
- Setting Up SMB Home Shares
- Configuring SMB Service
- SMB Service Screen
- Spotlight Support on a SCALE SMB Share

Releated AFP Articles

- Adding SMB Shares
- SMB Shares Screens
- AFP Migration

3.9.5.3 - Using SMB Shadow Copy

This article provides information on SMB share shadow copies, enbling shadow copies, and resolving an issue with Microsoft Windows 10 v2004 release.

Enable Shadow Copies exports ZFS snapshots as Shadow Copies for Microsoft Volume Shadow Copy Service (VSS) clients.

About SMB Shadow Copies

Shadow Copies, also known as the Volume Shadow Copy Service (VSS) or Previous Versions, is a Microsoft service for creating volume snapshots. You can use shadow copies to restore previous versions of files from within Windows Explorer.

By default, all ZFS snapshots for a dataset underlying an SMB share path are presented to SMB clients through the volume shadow copy service or are accessible directly with SMB when the hidden ZFS snapshot directory is within the SMB share path.

Before you activate Shadow Copies in TrueNAS, there are a few caveats:

- Shadow Copies might not work if the Windows system is not patched to the latest service pack. If previous versions of files to restore are not visible, use Windows Update to ensure the system is fully up-to-date.
- Shadow Copies support only works for ZFS pools or datasets.
- SMB share dataset or pool permissions must be configured appropriately.

Enabling Shadow Copies

To enable shadow copies, go to **Shares > Windows (SMB) Shares** and click **Windows (SMB) Shares** launch icon to display the list view **Sharing > SMB** screen.

1. Click the ⋮ for the share you want to change, and then click **Edit**. The **Edit SMB** screen displays.
2. Scroll down to the bottom and click **Advanced Options**.
3. Scroll down to **Other Options** and select **Enable Shadow Copies**.
4. Click **Save**

Windows 10 v2004 Issue

Some users might experience issues in the Windows 10 v2004 release where they cannot access network shares. The problem appears to come from a bug in gpedit.msc, the Local Group Policy Editor. Unfortunately, setting the **Allow insecure guest logon** flag value to **Enabled** in **Computer Configuration > Administrative Templates > Network > Lanman Workstation** in the Windows appears to have no effect on the configuration.

To work around this issue, edit the Windows registry. Use **Regedit** and go to **HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters**. The **DWORD AllowInsecureGuestAuth** is an incorrect value: *0x00000000*. Change this value to **0x00000001** (Hexadecimal 1) to allow adjusting the settings in gpedit.msc. You can use a Group Policy Update to apply this to a fleet of Windows machines.

Deleting Shadow Copies

Users with an SMB client cannot delete Shadow copies. Instead, the administrator uses the TrueNAS web interface to remove snapshots.

Disable shadow copies for an SMB share by clearing the **Enable shadow copies** checkbox on the **Edit SMB** screen for the SMB share. Disabling does not prevent access to the hidden .zfs/snapshot directory for a ZFS dataset when the directory is located within the path for an SMB share.

Related Content

- Adding SMB Shares
- SMB Shares Screens
- Managing SMB Shares
- Setting Up SMB Home Shares
- Configuring SMB Service
- SMB Service Screen
- Spotlight Support on a SCALE SMB Share

3.9.5.4 - Setting Up SMB Home Shares

This article provides instructions to set up SMB home shares.

Setting Up SMB Home Shares

TrueNAS offers the **Use as Home Share** option for organizations or SMEs that want to use a single SMB share to provide a personal directory to every user account. Each user is given a personal home directory when connecting to the share. These home directories are not accessible by other users. Only one share can be used as the home share, but other non-home shares can be created.

Creating an SMB home share requires configuring the system storage and joining Active Directory.

Create a Pool and Join Active Directory

First, go to **Storage** and create a pool.

Next, set up the Active Directory that you want to share resources with over your network.

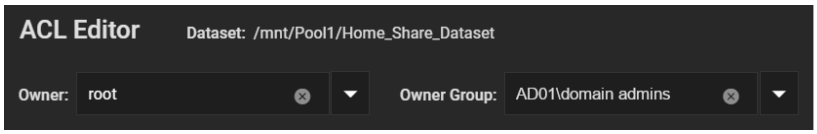
Prepare a Dataset

Go to **Storage** and open the ⋮ next to the root dataset in the pool you just created, then click **Add Dataset**.

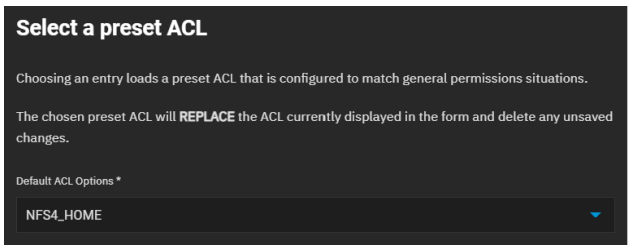
Name the dataset and set **Share Type** to **SMB**.

After creating the dataset, go to **Storage** and open ⋮ next to the new dataset. Select **View Permissions**, then click ✎.

Click the **Group** dropdown list and change the owning group to your Active Directory domain admins.



Click **Use an ACL Preset** and choose **NFS4_HOME**. Then, click **Continue**.



Create the Share

Go to **Shares > Windows (SMB) Shares** and click **Add**.

Set the **Path** to the prepared dataset.

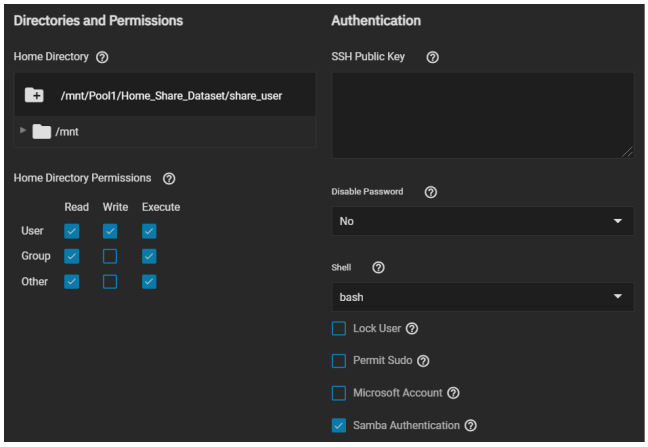
The **Name** automatically becomes identical to the dataset. Leave this as the default.

Set the **Purpose** to **No presets**, then click **Advanced Options** and set **Use as Home Share**. Click **Save**.

Enable the **SMB** service in **System Settings > Services** to make the share is available on your network.

Add Users

Go to **Credentials > Local Users** and click **Add**. Create a new user name and password. By default, the user **Home Directory** title comes from the user account name and is added as a new subdirectory of **Home_Share_Dataset**.



If existing users require access to the home share, go to **Credentials > Local Users** and edit an existing account.

Adjust the user home directory to the appropriate dataset and give it a name to create their own directory.

After adding the user accounts and configuring permissions, users can log in to the share and see a folder matching their user name.

Related Content

- Adding SMB Shares
- SMB Shares Screens
- Managing SMB Shares
- Using SMB Shadow Copy
- Configuring SMB Service
- SMB Service Screen
- Spotlight Support on a SCALE SMB Share

3.10 - System Settings

SCALE system management options are collected in this section of the UI and organized into a few different screens:

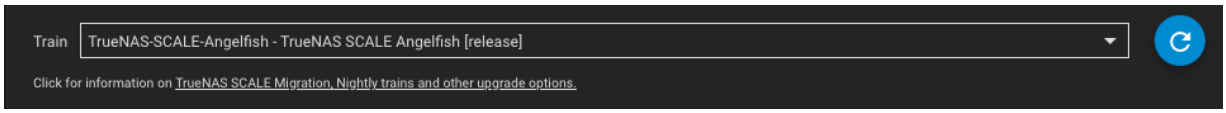
- **Update** controls when the system applies a new version. There are options to download and install an update, have the system check daily and stage updates, or apply a manual update file to the system.
- **General** shows system details and has basic, less intrusive management options, including web interface access, localization, and NTP server connections. This is also where users can input an Enterprise license or create a software bug ticket.
- **Advanced** contains options that are more central to the system configuration or meant for advanced users. Specific options include configuring the system console, log, and dataset pool, adding custom system controls, kernel-level settings, scheduled scripting or commands, and determining any isolated GPU devices. *Warning*: Advanced settings can be disruptive to system function if misconfigured.
- **Boot** lists each ZFS boot environment stored on the system. These restore the system to a previous version or specific point in time.
- **Services** displays each system component that runs continuously in the background. These typically control data sharing or other external access to the system. Individual services have their own configuration screens and activation toggles, and can be set to run automatically.
- **Shell** allows users to enter commands directly into the TrueNAS Operating System. Shell accepts Unix-like commands, and there is an experimental TrueNAS-specific command-line interface (CLI) for configuring the system separately from the web interface.
- **Enclosure** appears when the system is attached to compatible SCALE hardware. This is a visual representation of the system with additional details about disks and other physical hardware components.

Ready to get started? Choose a topic or article from the left-side **Navigation** pane. Click the **<** symbol to expand the menu to show the topics under this section.

3.10.1 - Updating SCALE

TrueNAS has several software branches (linear update paths) known as trains. SCALE is currently a Prerelease Train. Prerelease Trains have various preview/early build releases of the software.

SCALE has several trains available for updates. However, the web interface only displays trains you can select as an upgrade. To view a list of the available trains, click on the arrow to the right of your current train.



For more information on other available trains, see TrueNAS Upgrades.

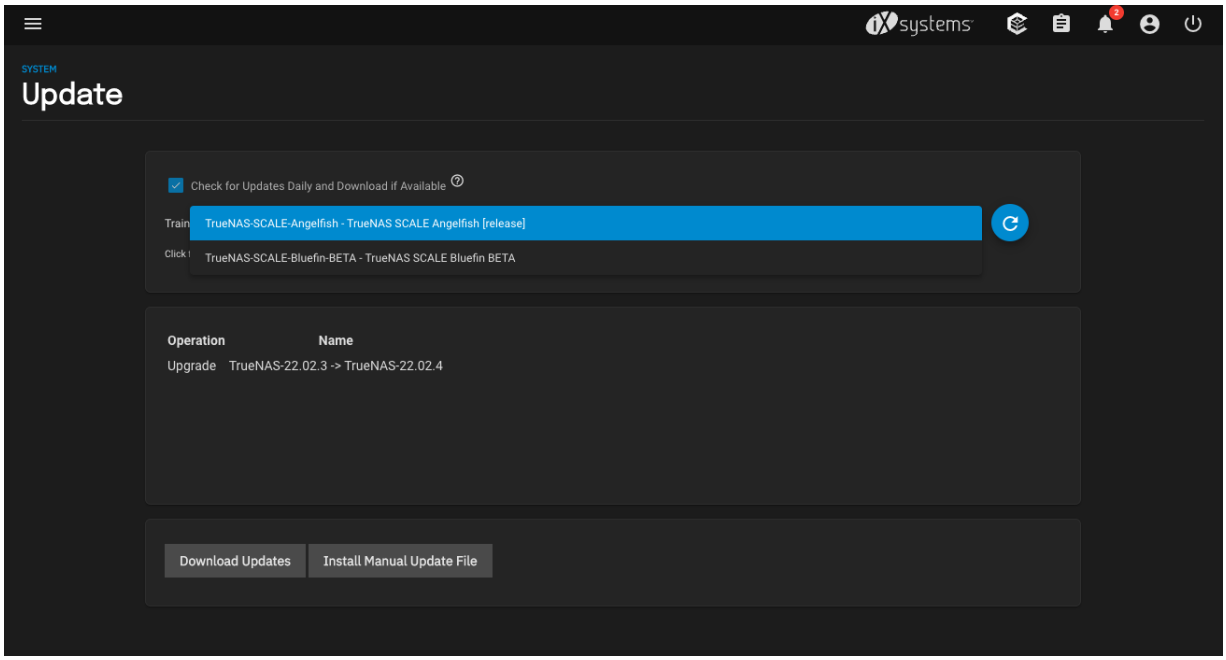
> See the Software Status page for the latest recommendations for software usage. Bluefin and Nightlies are non-production trains. If you are using a non-production train, be prepared to experience bugs or problems. Testers are encouraged to submit bug reports and debug files at https://jira.ixsystems.com.

The TrueNAS SCALE **Update** screen lets users update their system using two different methods: manual or automatic.

We recommend updating TrueNAS when the system is idle (no clients connected, no disk activity, etc). Most updates require a system reboot.

Update during scheduled maintenance times to avoid disrupting user activities.

> All auxiliary parameters are subject to change between major versions of TrueNAS due to security and development issues. We recommend removing all auxiliary parameters from TrueNAS configurations before upgrading.



Automatic

Select the **Check for Updates Daily and Download if Available** option to automatically download updates.

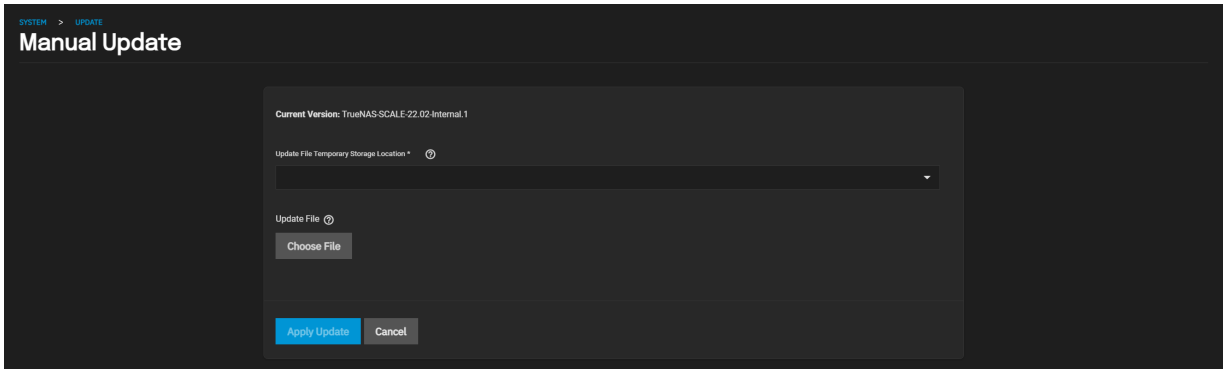
If an update is available, click **Apply Pending Update** to install it.

Manual

To do a manual update, click **Download Updates** and wait for the file to download to your system.

Download the SCALE Manual Update File.

To manually update TrueNAS, click **Install Manual Update File** and save your configuration.



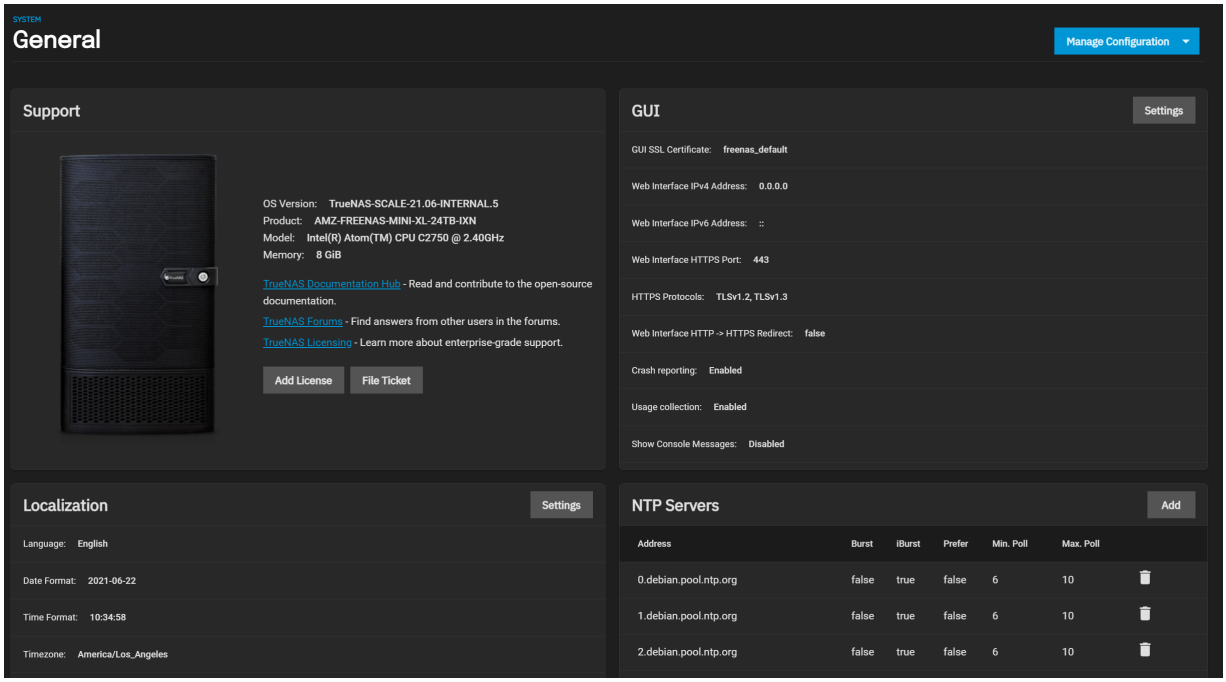
Select a temporary location to store the update file and click **Choose File**. Select the .iso you want to upgrade to and click **Apply Update**.

Related Content

- Update Screens
- Installing SCALE

3.10.2 - General Settings

The TrueNAS SCALE General Settings section provides settings options for support, graphic user interface, localization, NTP servers, and system configuration.



Article Summaries

- Getting Support

  This article provides instructions for SCALE users to access TrueNAS Community and Social Media, get system support, report problems, and find system license information.

- Managing the System Configuration

  This article provides information on downloading your TrueNAS configuration to back up system settings, or uploading a new configuration file, and resetting back to default settings.

- Managing General Settings

  This article provides information on the WebUI settings for your local region language, adding an NTP server, and configuring other web interface settings.

3.10.2.1 - Getting Support

This article provides instructions for SCALE users to access TrueNAS Community and Social Media, get system support, report problems, and find system license information.

There are several options to get support for your TrueNAS installation. TrueNAS SCALE users can engage with the TrueNAS community to answer questions and resolve issues. TrueNAS Enterprise hardware customers can also access the fast and effective support directly provided by iXsystems.

TrueNAS SCALE users are welcome to report bugs and vote for or suggest new TrueNAS features in the project Jira instance. Have questions? We recommend searching through the software documentation and community resources for answers.

Using the TrueNAS Community

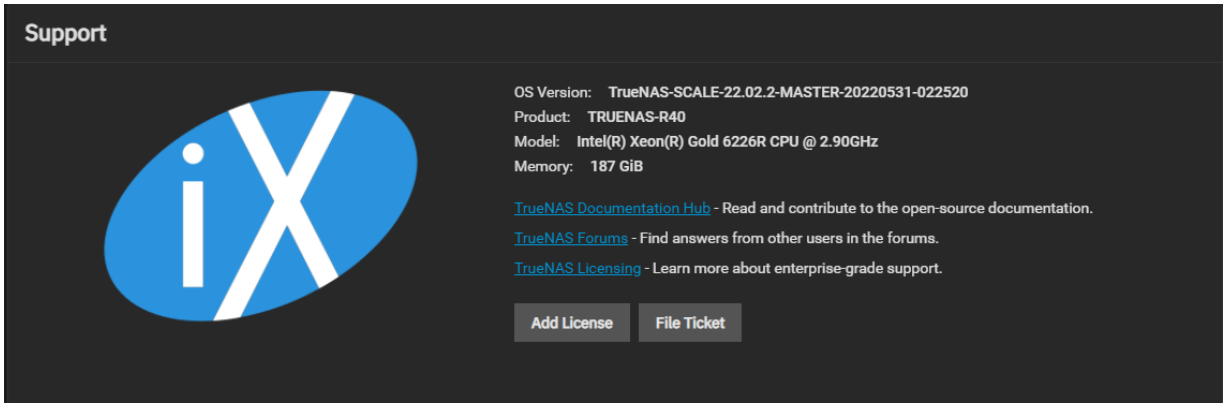
The TrueNAS Community is an active online resource for asking questions, troubleshooting issues, and sharing information with other TrueNAS users. You must register to post. We encourage new users to briefly introduce themselves and review the forum rules before posting.

Community Resources are user-contributed articles about every facet of using TrueNAS. They are organized into broad categories and incorporate a community rating system to better highlight content that the whole community has found helpful.

Using TrueNAS Social Media

You are always welcome to network with other TrueNAS users using the various social media platforms!

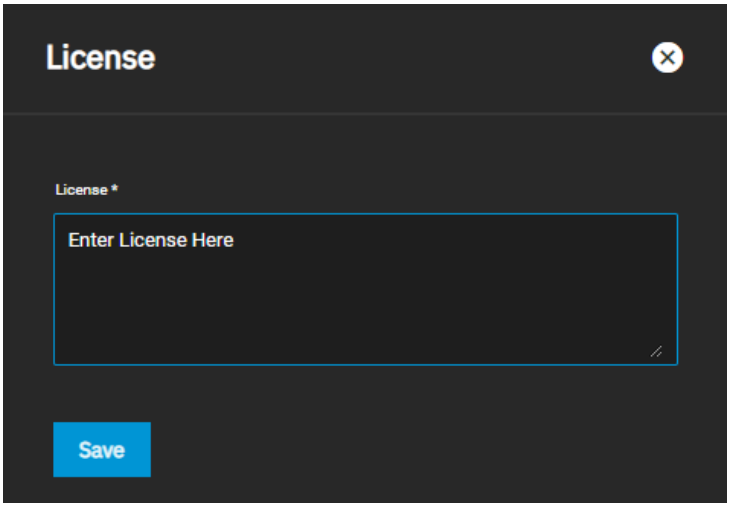
- Reddit
- Twitter
- LinkedIn
- Facebook



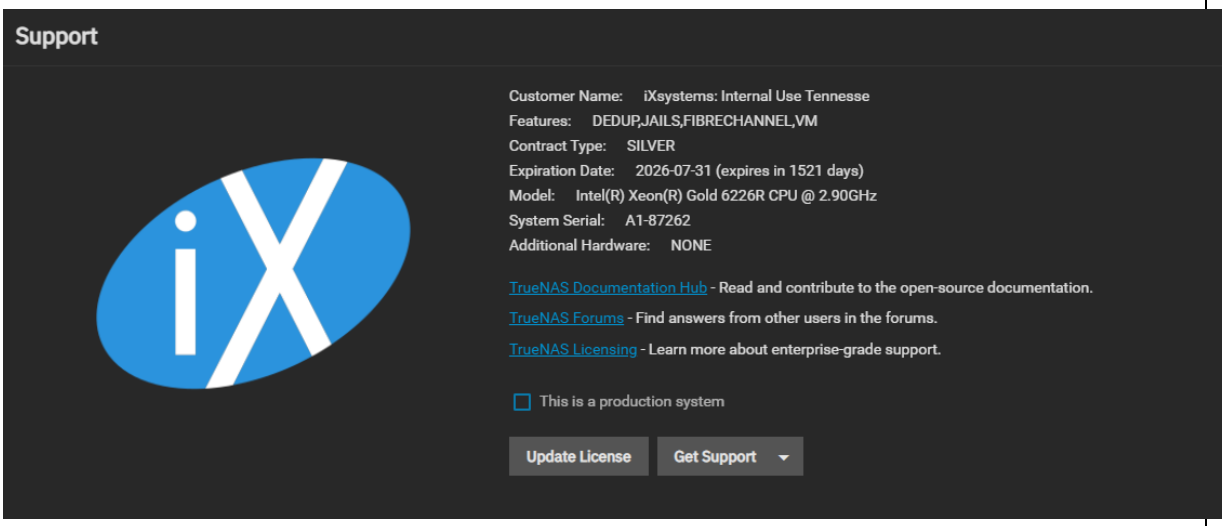
Adding a License

For users with a valid TrueNAS license, click **Add License**. Copy your license into the box and click **Save**.

Click Here for More Information



You are prompted to reload the page for the license to take effect, click **RELOAD NOW**. Log back into the WebUI where the **End User License Agreement (EULA)** displays. Read it thoroughly and completely. After you finish, click **I AGREE**. The system information updates to reflect the licensing specifics for the system.



Silver and Gold level Support customers can also enable Proactive Support on their hardware to automatically notify iXsystems if an issue occurs. To find more details about the different Warranty and Service Level Agreement (SLA) options available, see iXsystems Support.

When the system is ready to be in production, update the status by selecting **This is a production system** and then click the **Proceed** button. This sends an email to iXsystems declaring that the system is in production.

While not required for declaring the system is in production, TrueNAS has an option to include a initial debug with the email that can assist support in the future.

Filing a Ticket

TrueNAS SCALE users are encouraged to report bugs and to vote for or suggest new TrueNAS features in the project Jira instance. Have questions? We recommend searching through the software documentation and community resources for answers.

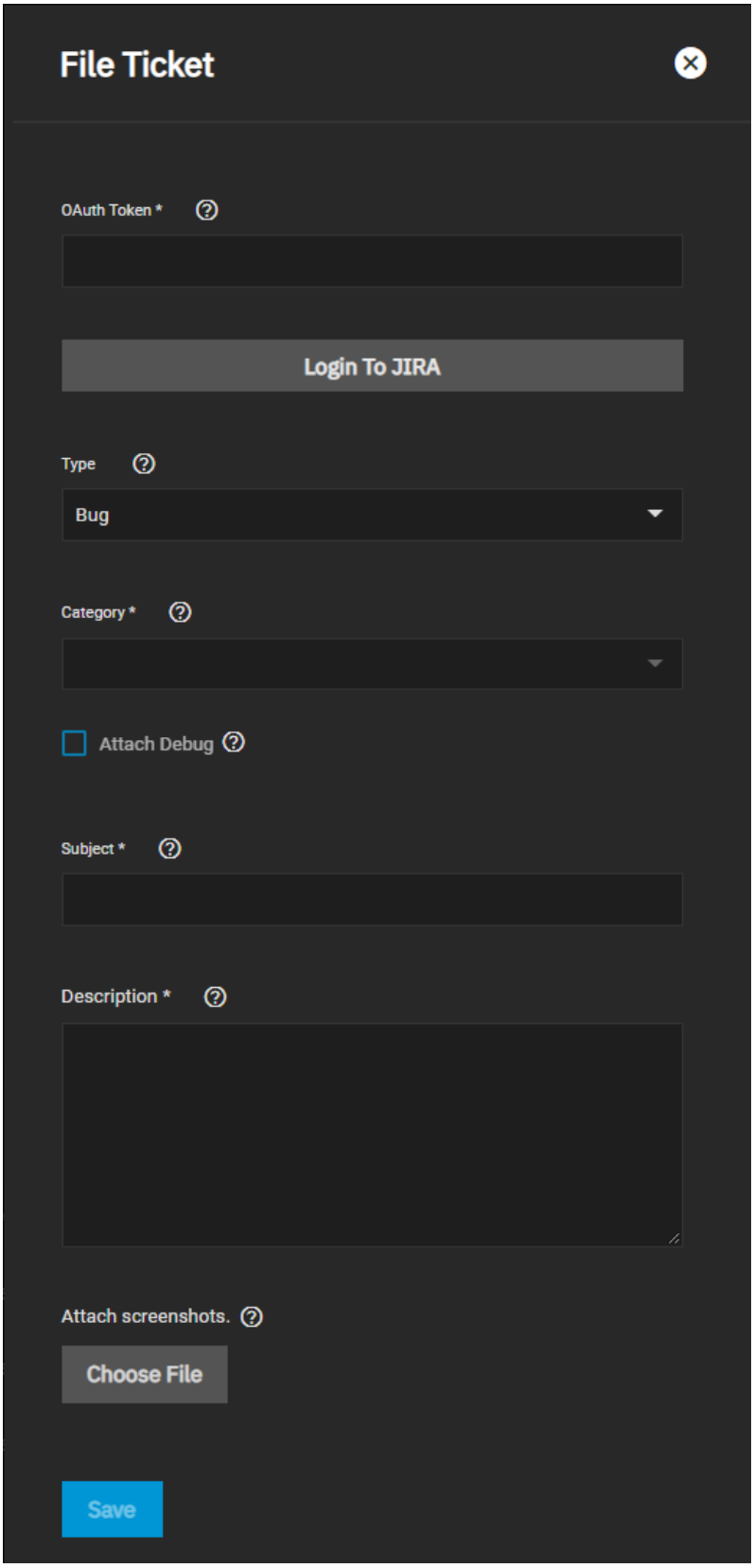
If you encounter a bug or other issue while using TrueNAS SCALE, use the **File Ticket** option on the **System Settings > General** screen to create a bug report in the TrueNAS Jira Project. The web interface provides a form to report issues without logging out and that prompts you to provide the information and attachments we need to assist users.

> At present, all Jira tickets are marked as **iX Private** to safeguard user personal and private data, so it is not possible to search the project first to see if another user already reported the issue.

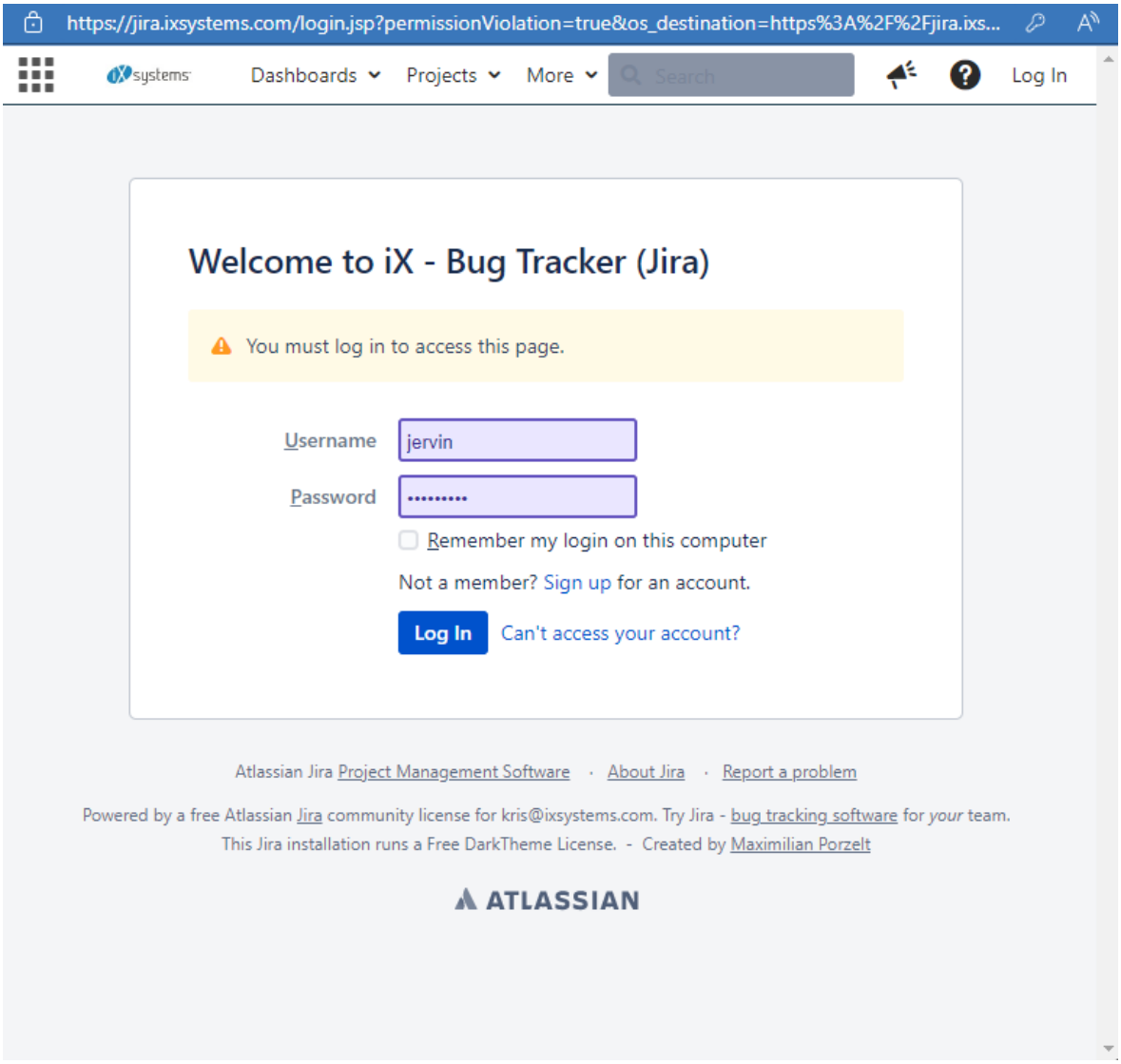
You must have a Jira account to create a bug ticket.

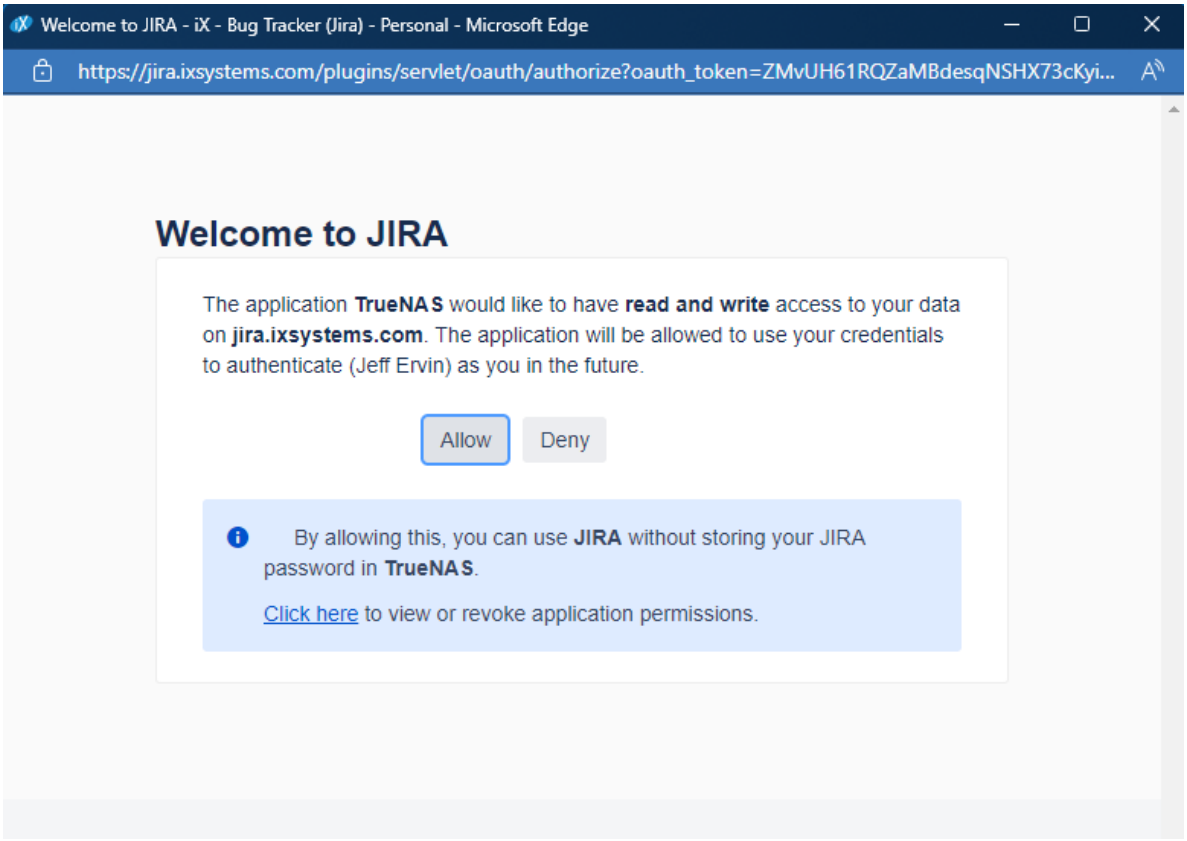
Filing Issue Tickets

To report an issue using the web interface, go to **System Settings > General** and click **File Ticket** to open the **File Ticket** form.



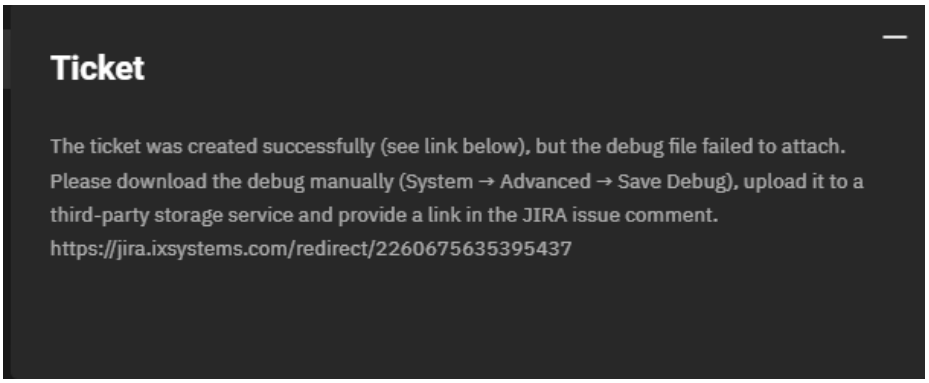
Click **Login to JIRA** and enter your credentials in the fields provided. After logging in, select **Allow** to give TrueNAS read and write access to your data on the Jira site. A token is added to the OAuth section of this form.


https://jira.ixsystems.com/login.jsp?permissionViolation=true&os_destination=https%3A%2F%2Fjira.ixs...
Dashboards
Projects
More
Search
Log In
Welcome to iX - Bug Tracker (Jira)
You must log in to access this page.
Username
jervin
Password
Remember my login on this computer
Not a member? Sign up for an account.
Log In
Can't access your account?
Atlassian Jira Project Management Software · About Jira · Report a problem
Powered by a free Atlassian Jira community license for kris@ixsystems.com. Try Jira - bug tracking software for your team.
This Jira installation runs a Free DarkTheme License. - Created by Maximilian Porzelt
ATLASSIAN

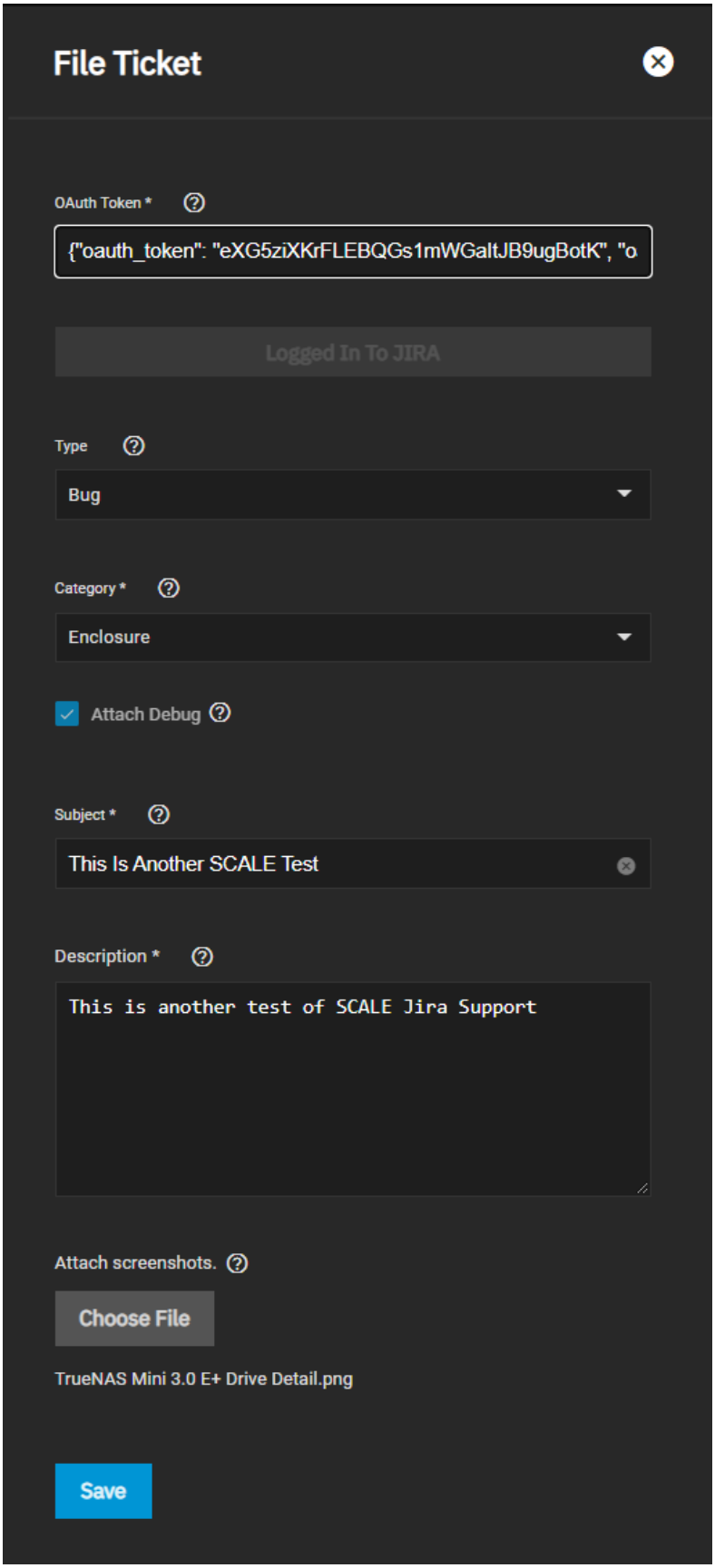


After logging into Jira, select either **Bug** or **Feature** as the **Type** of ticket to create, then choose the appropriate **Category** for your request.

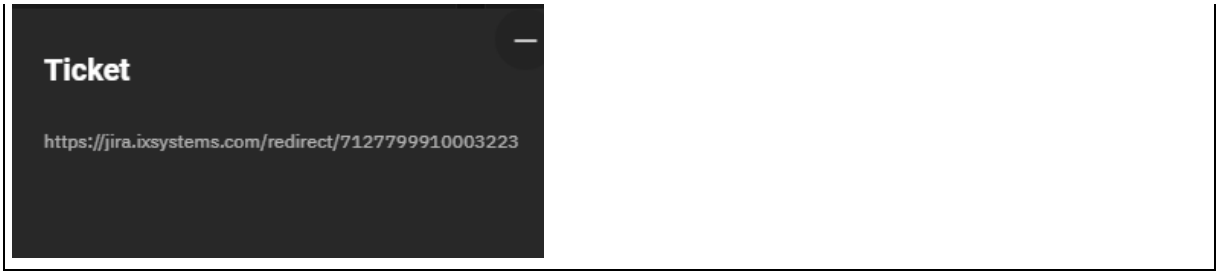
Attach a debug file to all bug tickets. Click **Attach Debug** to give the TrueNAS Team pertinent information about the system and what could be causing any issues. If the debug file is too large to attach to your ticket, the following displays:



Provide a brief summary of the issue in **Subject**. Enter much details about the issue as possible as the reason for submitting the ticket in the **Description** field. Attach any applicable screenshots and click **Save**.



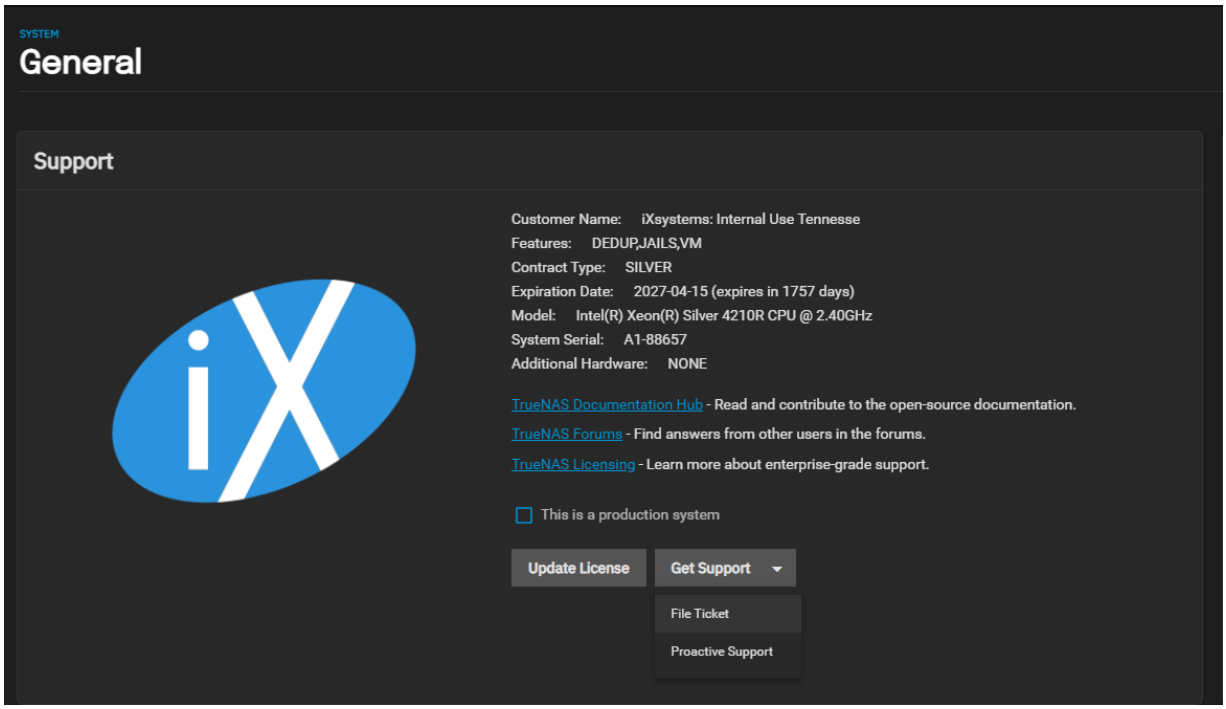
After the ticket generates, you can view it by clicking the link provided in the WebUI.



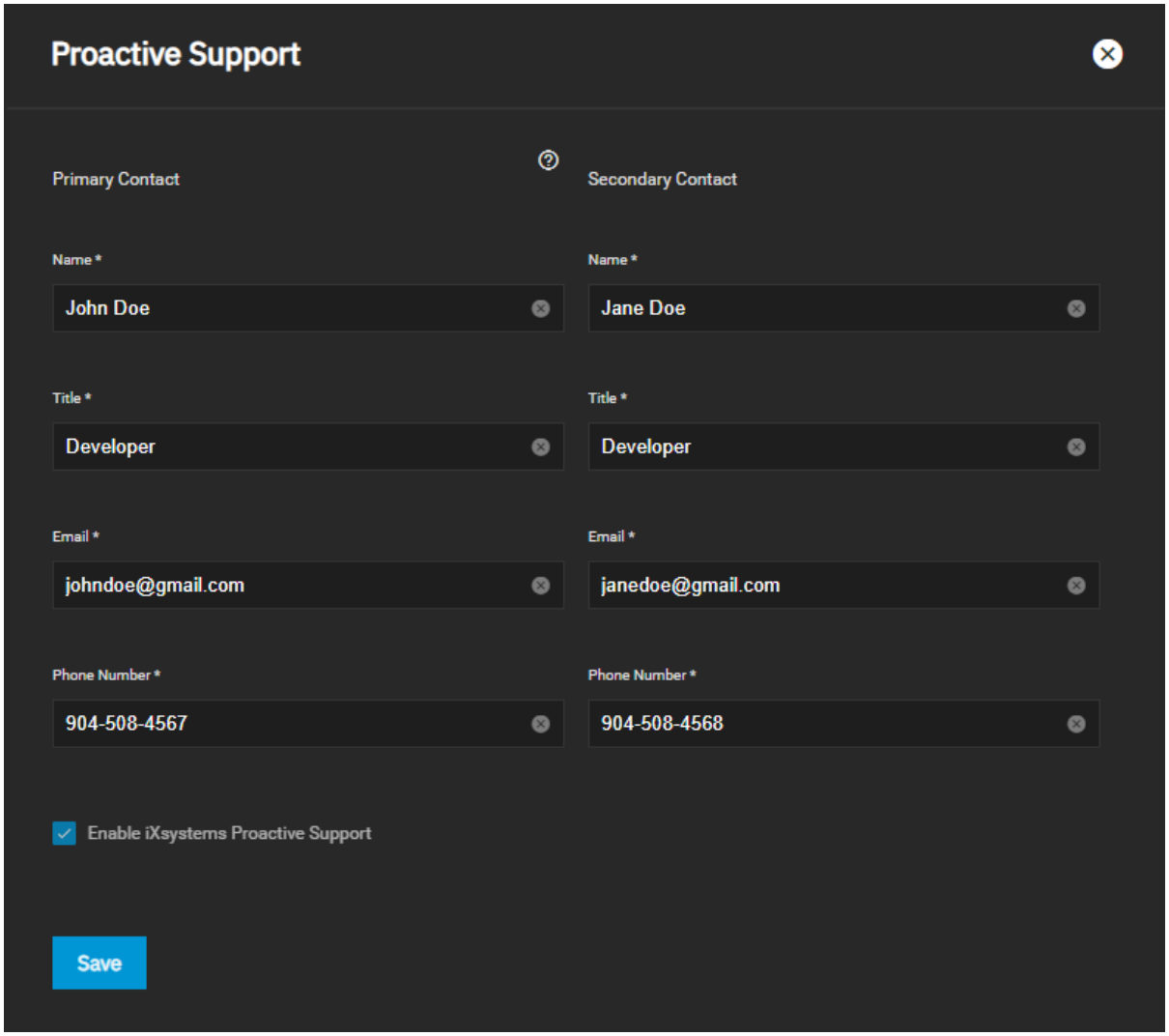
Using Proactive Support

Silver/Gold Coverage Customers can enable iXsystems Proactive Support. This feature automatically emails iXsystems when certain conditions occur in a TrueNAS system.

To configure Proactive Support, click the **Get Support** dropdown and select **Proactive Support**.



Complete all available fields and select **Enable iXsystems Proactive Support** if it is not check-marked, then click **Save**.



Contacting iXsystems Support

Customers who purchase iXystems hardware or that want additional support must have a support contract to use iXystems Support Services. The TrueNAS Community forums provides free support for users without an iXsystems Support contract.

Contact Method	Contact Options
Web	https://support.ixsystems.com
Email	support@ixsystems.com
Telephone	Monday - Friday, 6:00AM to 6:00PM Pacific Standard Time: US-only toll-free: 1-855-473-7449 option 2 Local and international: 1-408-943-4100 option 2
Telephone	After Hours (24x7 Gold Level Support only): US-only toll-free: 1-855-499-5131 International: 1-408-878-3140 (international calling rates apply)

Related Content

3.10.2.2 - Managing the System Configuration

This article provides information on downloading your TrueNAS configuration to back up system settings, or uploading a new configuration file, and resetting back to default settings.

TrueNAS SCALE allows users to manage the system configuration by uploading or downloading configurations, or by resetting the system to the default configuration.

System Configuration Options

The **Manage Configuration** option on the **system Settings > General** screen provides three options:

- **Download File** that downloads your system configuration settings to a file on your system.
- **Upload File** that allows you to upload a replacement configuration file.
- **Reset to Defaults** that resets system configuration settings back to factory settings.

Downloading the File

The **Download File** option downloads your TrueNAS SCALE current configuration to the local machine.

When you download the configuration file, you have the option to **Export Password Secret Seed**, which includes encrypted passwords in the configuration file. This allows you to restore the configuration file to a different operating system device where the decryption seed is not already present. Users must physically secure configuration backups containing the seed to prevent unauthorized access or password decryption.

We recommend backing up the system configuration regularly. Doing so preserves settings when migrating, restoring, or fixing the system if it runs into any issues. Save the configuration file each time the system configuration changes.

Uploading the File

The **Upload File** option gives users the ability to replace the current system configuration with any previously saved TrueNAS SCALE configuration file.

> All passwords are reset if the uploaded configuration file was saved without the selecting **Save Password Secret Seed**.

Resetting to Defaults

The **Reset to Defaults** option resets the system configuration to factory settings. After the configuration resets, the system restarts and users must set a new login password.

> Save the system current configuration with the **Download File** option before resetting the configuration to default settings!
>
> If you do not save the system configuration before resetting it, you could lose data that was not backed up, and you cannot revert to the previous configuration.

Related Content

- Settings Options
- Web Interface Preference Screen
- Getting Support
- Managing Advanced Settings
- Managing Cron Jobs
- Managing the Console Setup Menu
- General Settings Screen
- Managing General Settings
- Managing System Logging

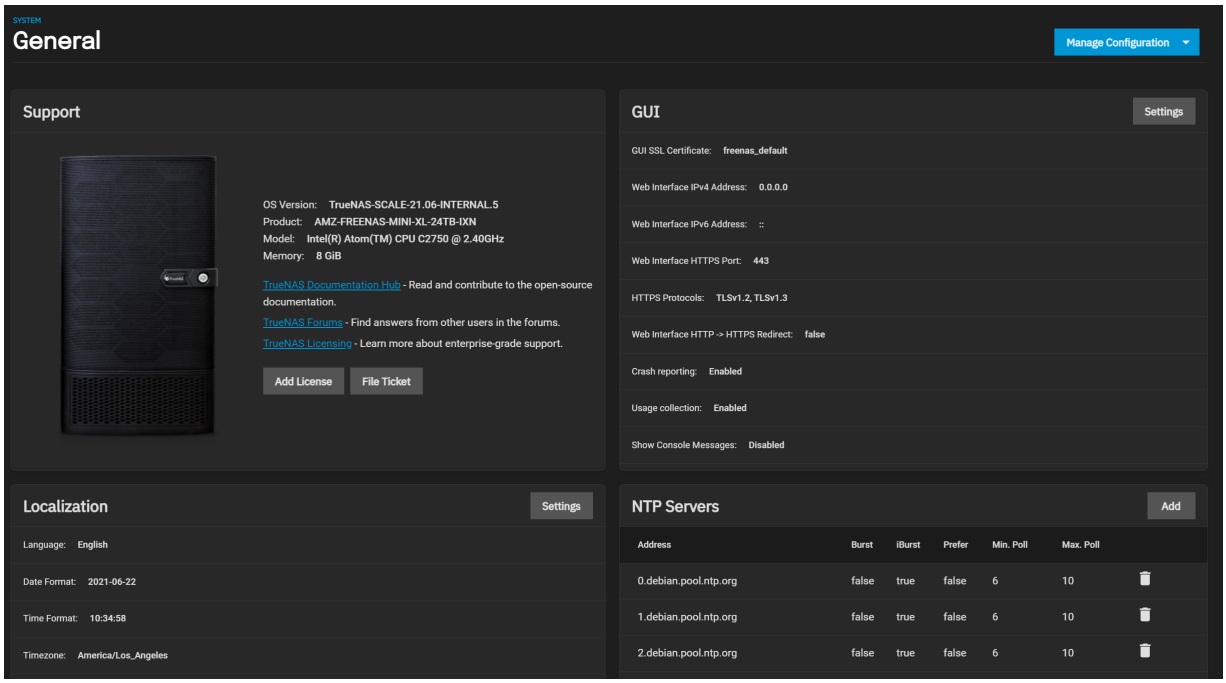
Related Backup Articles

- Adding Cloud Credentials
- Adding Cloud Sync Tasks
- Adding Replication Tasks
- Backing Up Google Drive to TrueNAS SCALE
- Cloud Credentials Screens
- Cloud Sync Tasks Screens
- Setting Up a Local Replication Task
- Setting Up Advanced Replication Tasks
- Backup Credentials

3.10.2.3 - Managing General Settings

This article provides information on the WebUI settings for your local region language, adding an NTP server, and configuring other web interface settings.

The TrueNAS SCALE General Settings section provides settings options for support, graphic user interface, localization, NTP servers, and system configuration.



Configuring GUI Options

The **GUI** widget allows users to configure the TrueNAS SCALE web interface address. Click **Settings** to open the **GUI Settings** configuration screen.

Changing the GUI SSL Certificate

The system uses a self-signed certificate to enable encrypted web interface connections. To change the default certificate, select a different certificate that was created or imported in the **Certificates** section from the **GUI SSL Certificate** dropdown list.

Setting the Web Interface IP Address

To set the WebUI IP address, if using IPv4 addresses, select a recent IP address from the **Web Interface IPv4 Address** dropdown list. This limits the usage when accessing the administrative GUI. The built-in HTTP server binds to the wildcard address of 0.0.0.0 (any address) and issues an alert if the specified address becomes unavailable. If using an IPv6 address, select a recent IP address from the **Web Interface IPv6 Address** dropdown list.

Configuring HTTPS Options

To allow configuring a non-standard port to access the GUI over HTTPS, enter a port number in the **Web Interface HTTPS Port** field.

Select the cryptographic protocols for securing client/server connections from the **HTTPS Protocols** dropdown list. Select the Transport Layer Security (TLS) versions TrueNAS SCALE can use for connection security.

To redirect HTTP connections to HTTPS, select **Web Interface HTTP -> HTTPS Redirect**. A GUI SSL Certificate is required for HTTPS. Activating this also sets the HTTP Strict Transport Security (HSTS) maximum age to 31536000 seconds (one year). This means that after a browser connects to the web interface for the first time, the browser continues to use HTTPS and renews this setting every year. A warning displays when setting this function. Setting HTTPS redirects can have unintended

consequences if an app does not support secure connections. If this occurs, to reset, clear this option and click **Save**. Then clear the browser cache before trying to connect to the app again.

To send failed HTTP request data which can include client and server IP addresses, failed method call tracebacks, and middleware log file contents to iXsystems, select **Crash Reporting**.

Sending Usage Statistics to iXsystems

To send anonymous usage statistics to iXsystems, select the **Usage Collection** option.

Showing Console Messages

To display console messages in real time at the bottom of the browser, select the **Show Console Messages** option.

Localizing TrueNAS SCALE

To change the WebUI on-screen language and set the keyboard to work with the selected language, click **Settings** on the **System Settings > General > Localization** widget. The **Localization Settings** configuration screen opens.

Select the language from the **Language** dropdown list, and then the keyboard layout in **Console Keyboard Map**.

Enter the time zone in **Timezone** and then select the local date and time formats to use.

Click **Save**.

Adding NTP Servers

The **NTP Servers** widget allows users to configure Network Time Protocol (NTP) servers. These sync the local system time with an accurate external reference. By default, new installations use several existing NTP servers. TrueNAS SCALE supports adding custom NTP servers.

Related Content

- Settings Options
- Web Interface Preference Screen
- Getting Support
- Managing Advanced Settings
- Managing Cron Jobs
- Managing the Console Setup Menu
- Managing the System Configuration
- General Settings Screen
- Managing System Logging

3.10.3 - Advanced Settings

Article Summaries

- Managing Advanced Settings

  This article provides information on adding sysctl variables, setting the system dataset pool, and setting the number of simultaneous replication tasks the system can run.

- Managing Cron Jobs

  This article provides information on adding or modifying cron jobs in SCALE.

- Managing the Console Setup Menu

  This article provides information on setting up or changing the Console setup menu port, port speed, the banner users see, and determine whether it requires a password to use.

- Managing System Logging

  This article provides information on setting up or changing the syslog server, the level of logging and the information included in the logs, and using TLS as the transport protocol.

- Managing Init/Shutdown Scripts

  This article provides information on adding or modifying init/shutdown scripts in SCALE.

- Managing SEDs

  This article provides information on adding or modifying self-encrypting drive (SED) user and global passwords in SCALE.

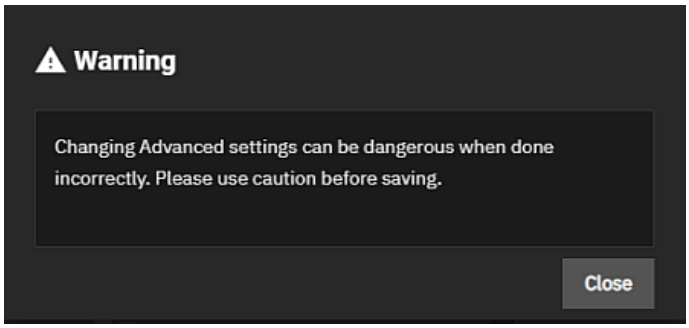
- Managing GPUs

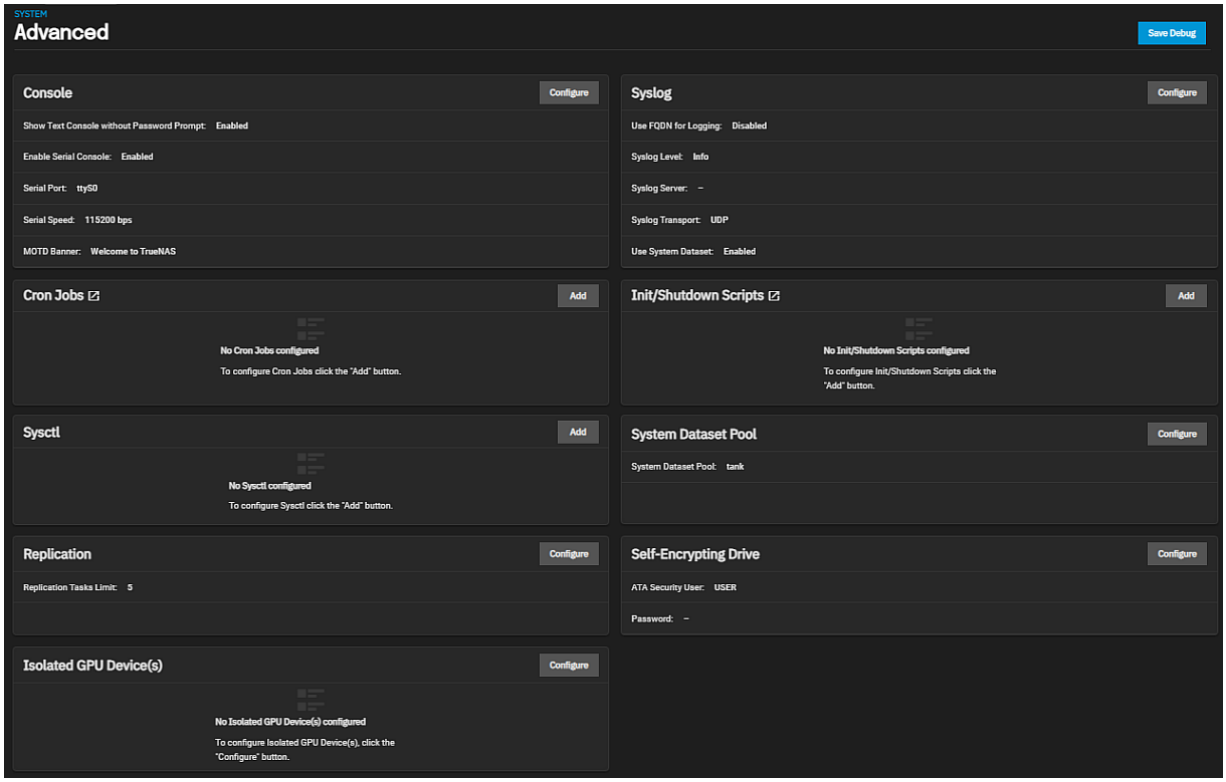
  This article provides information on isolating Graphic Processing Units (GPUs) installed in your system for use by a VM in SCALE.

3.10.3.1 - Managing Advanced Settings

This article provides information on adding sysctl variables, setting the system dataset pool, and setting the number of simultaneous replication tasks the system can run.

TrueNAS SCALE advanced settings screen provides configuration options for the console, syslog, sysctl, replication, cron jobs, init/shutdown scripts, system dataset pool, isolated GPU device(s), and self-encrypting drives.

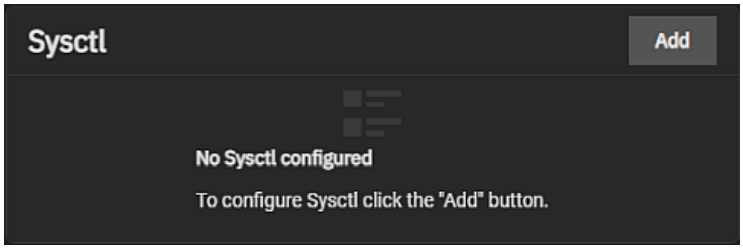
> Advanced settings have reasonable defaults in place. A warning message displays for some settings advising of the dangers making changes. Changing advanced settings can be dangerous when done incorrectly. Use caution before saving changes.
>
> 
>
>
> Make sure you are comfortable with ZFS, Linux, and system configuration backup and restoration before making any changes.



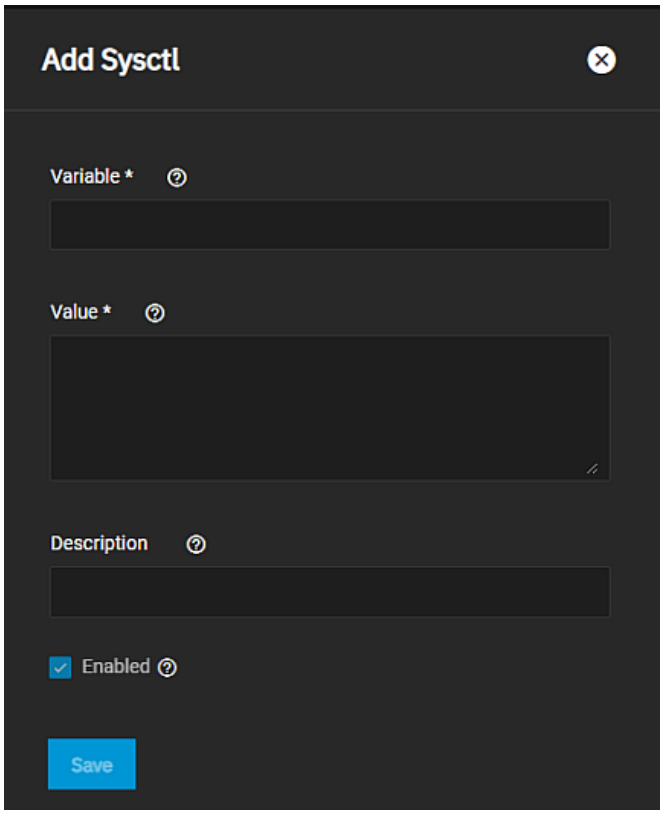
This article provides information on sysctl, system dataset pool and setting the maximum number of simultaneous replication tasks the system can perform.

Managing Sysctl Variables

Use **ADD** on the **Sysctl** widget to add a tunable that configures a kernel module parameter at runtime.



The **Add Sysctl** or **Edit Sysctl** configuration screens display the settings.



Enter the sysctl variable name in **Variable**. Sysctl tunables are used to configure kernel module parameters while the system is running and generally take effect immediately.

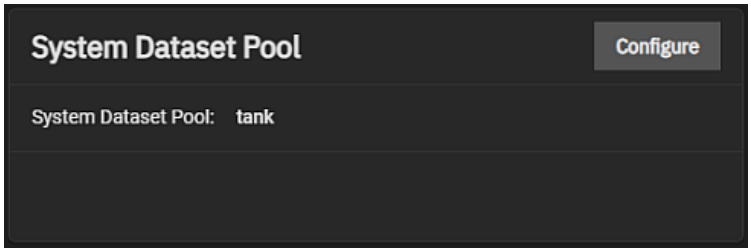
Enter a sysctl value to use for the loader in **Value**.

Enter a description and then select **Enable**. To disable but not delete the variable, clear the **Enable** checkbox.

Click **Save**.

Managing the System Dataset Pool

System Dataset Pool widget displays the pool configured as the system dataset pool. The widget allows users to select the storage pool they want to hold the system dataset. The system dataset stores debugging core files, encryption keys for encrypted pools, and Samba4 metadata, such as the user and group cache and share level permissions.



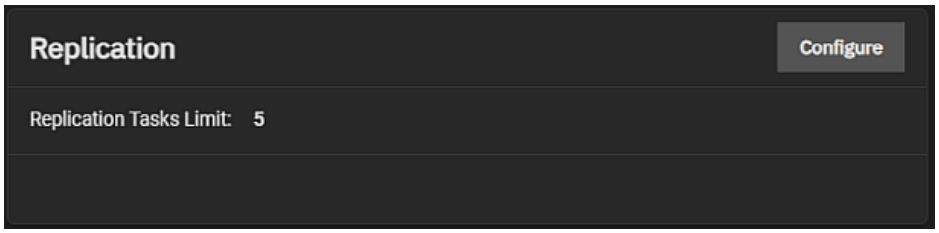
Click **Configure** to open the **System Dataset Pool** configuration screen. Select a pool from the dropdown list and click **Save**.

If the system has one pool, TrueNAS configures that pool as the system dataset pool. If your system has more than one pool, you can select the system dataset pool from the dropdown list of available pools. Users can move the system dataset to unencrypted pools or encrypted pools without passphrases.

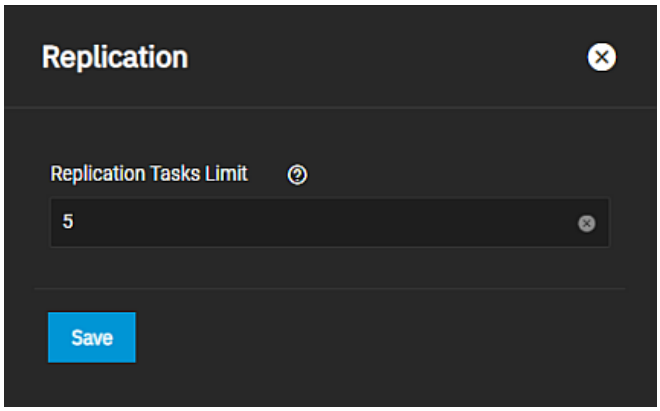
Users can move the system dataset to a key-encrypted pool, but cannot change the pool encryption type afterward. If the encrypted pool already has a passphrase set, you cannot move the system dataset to that pool.

Setting the Number of Replication Tasks

The **Replication** widget displays the number of replication tasks that can execute simultaneously configured on the system. It allows users to adjust the maximum number of replication tasks the system can execute simultaneously.



Click **Configure** to open the **Replication** configuration screen.



Enter a number for the maximum number of simultaneous replication tasks you want to allow the system to process and click **Save**.

Related Content

- Settings Options
- Web Interface Preference Screen
- Getting Support
- Managing Cron Jobs
- Managing the Console Setup Menu
- Managing the System Configuration
- General Settings Screen
- Managing General Settings
- Managing System Logging

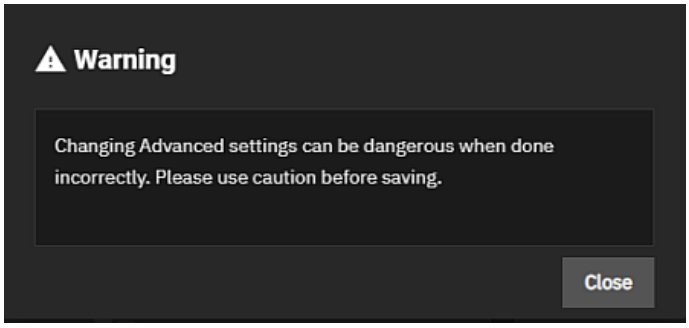
Related Replication Articles

- Adding Replication Tasks
- Setting Up a Local Replication Task
- Advanced Settings Screen
- Setting Up Advanced Replication Tasks
- Periodic Snapshot Tasks Screens
- Setting Up a Remote Replication Task
- Unlocking a Replication Encrypted Dataset or Zvol
- Replication Task Screens

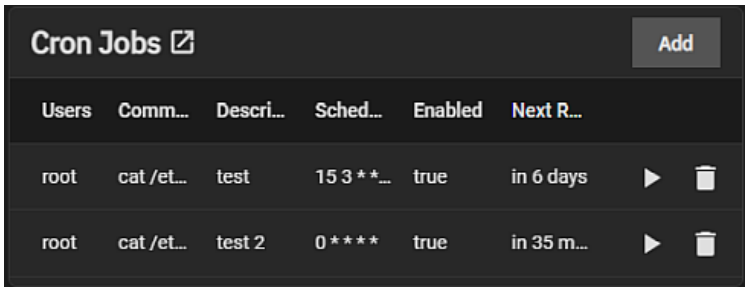
3.10.3.2 - Managing Cron Jobs

This article provides information on adding or modifying cron jobs in SCALE.

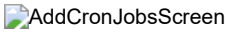
Cron jobs allow users to configure jobs that run specific commands or scripts on a regular schedule using cron(8). Cron Jobs help users run repetitive tasks.

> Advanced settings have reasonable defaults in place. A warning message displays for some settings advising of the dangers making changes. Changing advanced settings can be dangerous when done incorrectly. Use caution before saving changes.
>
> 
>
>
> Make sure you are comfortable with ZFS, Linux, and system configuration backup and restoration before making any changes.

The **Cron Jobs** widget on the **System > Advanced** screen displays **No Cron Jobs configured** until you add a cron job, and then it displays information on cron job(s) configured on the system.



Click **Add** to open the **Add Cron Job** configuration screen to create a new cron job, or if you want to modify an existing job, click anywhere on the item to open the **Edit Cron Jobs** configuration screen populated with the settings for that cron job. The **Add Cron Job** and **Edit Cron Job** configuration screens display the same settings.


AddCronJobsScreen

Enter a description for the cron job.

Next, enter the full path to the command or script to run in **Command**. For example, a command string to create a list of users on the system and write that list to a file enter `cat /etc/passwd > users_$(date +%F).txt`.

Select a user account to run the command from the **Run As User** dropdown list. The user must have permissions allowing them to run the command or script.

Select a schedule preset or choose **Custom** to open the advanced scheduler. Note that an in-progress cron task postpones any later scheduled instance of the same task until the running task is complete.

If you want to hide standard output (stdout) from the command, select **Hide Standard Output**. If left cleared, TrueNAS emails any standard output to the user account cron that ran the command.

To hide error output (stderr) from the command, select **Hide Standard Error**. If left cleared, TrueNAS emails any error output to the user account cron that ran the command.

Select **Enabled** to enable this cron job. If you leave this checkbox cleared it disables the cron job without deleting it.

Click **Save**.

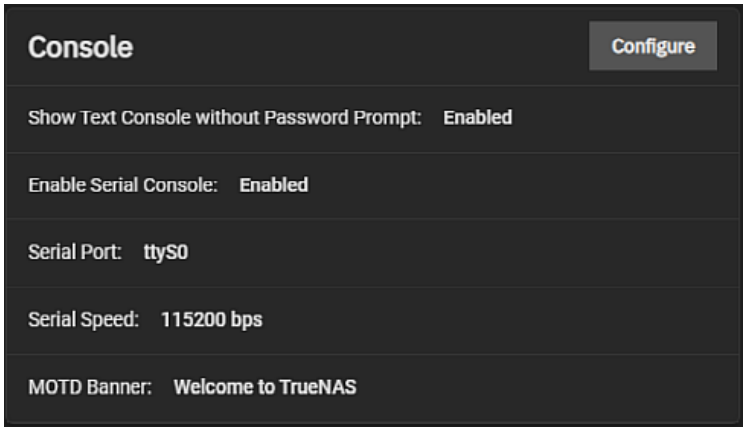
Related Content

- Advanced Settings Screen

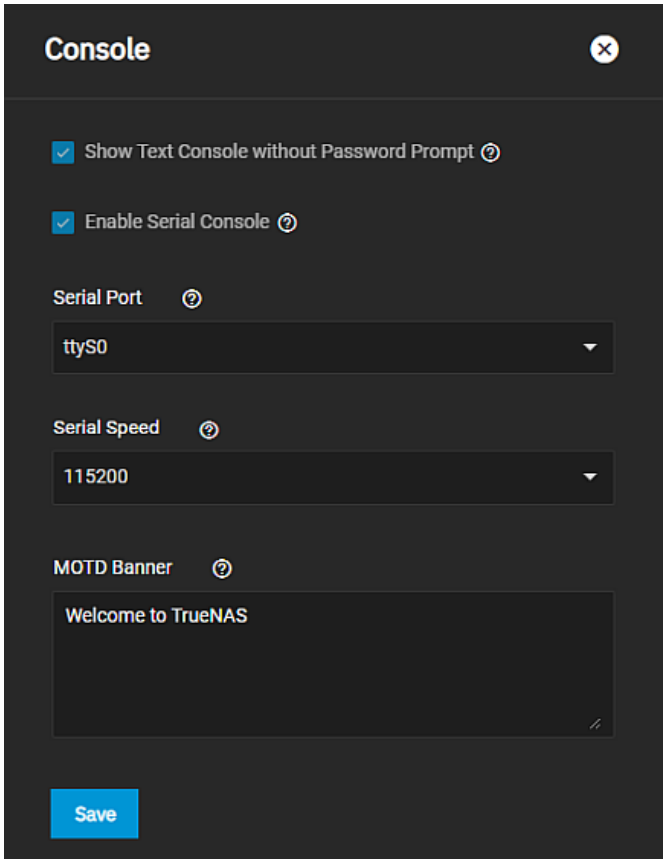
3.10.3.3 - Managing the Console Setup Menu

This article provides information on setting up or changing the Console setup menu port, port speed, the banner users see, and determine whether it requires a password to use.

The **Console** widget on the **System Setting > Advanced** screen displays current console settings for TrueNAS.



Click **Configure** to open the **Console** configuration screen. The **Console** configuration settings determine how the Console setup menu displays, the serial port it uses and the speed of the port, and the banner users see when it is accessed.



To display the console without being prompted to enter a password, select **Show Text Console without Password Prompt**. Leave it clear to add a login prompt to the system before showing the console menu.

Select **Enable Serial Console** to enable the serial console but do not select this if the serial port is disabled.

Enter the serial console port address in **Serial Port** and set the speed (in bits per second) from the **Serial Speed** dropdown list. Options are 9600, 19200, 38400, 57600 or 115200.

Finally, enter the message you want to display when a user logs in with SSH in **MOTD Banner**.

Click **Save**

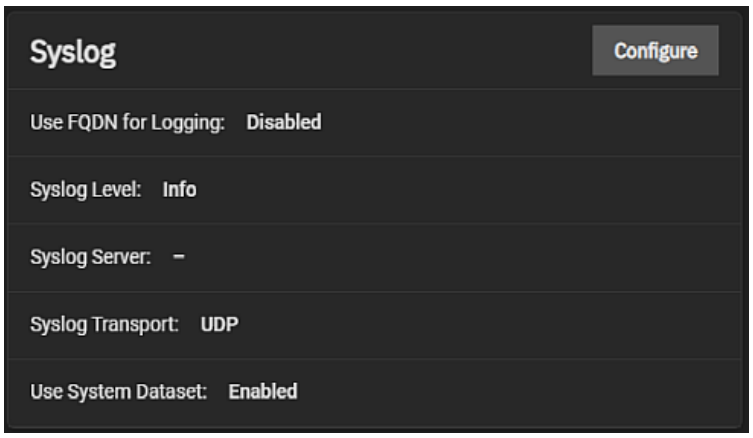
Related Content

- Console Setup Menu Configuration
- General Settings Screen
- Advanced Settings Screen

3.10.3.4 - Managing System Logging

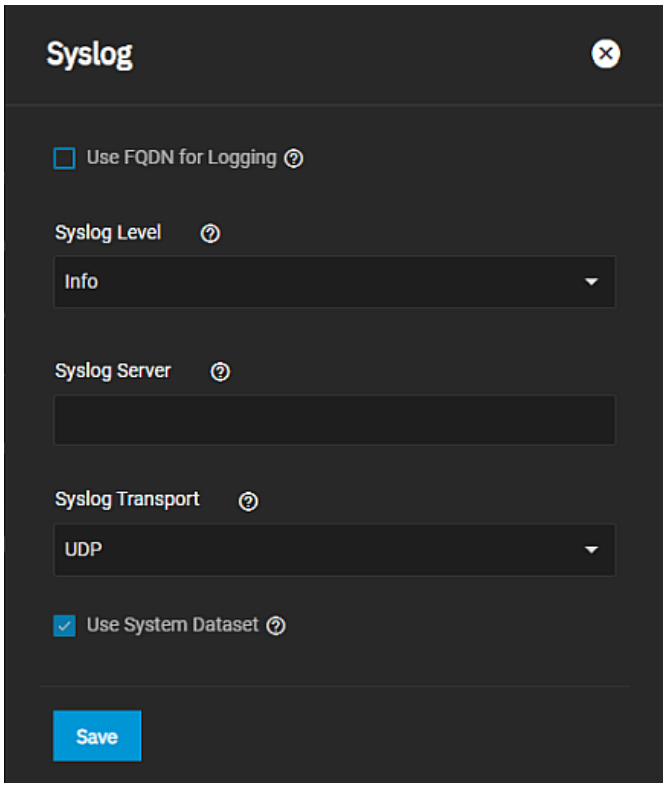
This article provides information on setting up or changing the syslog server, the level of logging and the information included in the logs, and using TLS as the transport protocol.

The **Syslog** widget on the **System > Advanced** screen allows users determine how and when the system sends log messages to the syslog server. The **Syslog** widget displays the existing system logging settings.



> Before configuring your syslog server to use TLS as the **Syslog Transport** method, first make sure you add a certificate and certificate authority (CA) to the TrueNAS system. Go to **Credentials > Certificates** and use the **Certificate Authority (CA)** and **Certificates** widgets to verify you have the required certificates or to add them.

Click **Configure** to open the **Syslog** configuration screen. The **Syslog** configuration screen settings specify the logging level the system uses to record system events, the syslog server DNS host name or IP, the transport protocol it uses, and if using TLS, the certificate and certificate authority (CA) for that server, and finally if it uses the system dataset to store the logs.



Enter the remote syslog server DNS host name or IP address in **Syslog Server**. To use non-standard port numbers like *mysyslogserver:1928*, add a colon and the port number to the host name. Log entries are written to local logs and sent to the remote syslog server.

Enter the transport protocol for the remote system log server connection in **Syslog Transport**. Selecting Transport Layer Security (TLS) displays the **Syslog TLS Certificate** and **Syslog TSL Certificate Authority** fields.

Next, select the transport protocol for the remote system log server TLS certificate from the **Syslog TLS Certificate** dropdown list, and select the TLS CA for the TLS server from the **Syslog TLS Certificate Authority** dropdown list.

Select **Use FQDN for Logging** to include the fully-qualified domain name (FQDN) in logs to precisely identify systems with similar host names.

Select the logging level the syslog server uses when creating system logs from **Syslog Level** the dropdown list. The system only sends logs matching this level.

Select **Use System Dataset** to store system logs on the system dataset. Leave clear to store system logs in `/var/` on the operating system device.

Click **Save**.

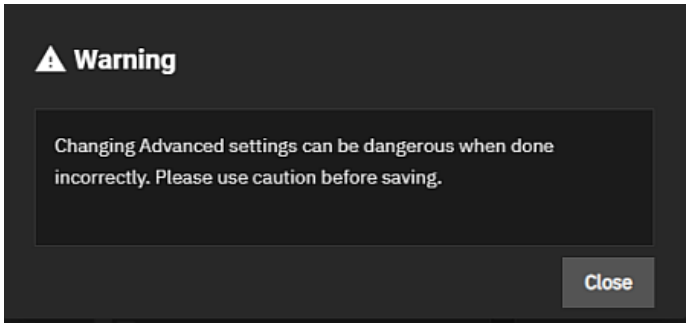
Related Content

- Settings Options
- Web Interface Preference Screen
- Getting Support
- Managing Advanced Settings
- Managing Cron Jobs
- Managing the Console Setup Menu
- Managing the System Configuration
- General Settings Screen
- Managing General Settings

3.10.3.5 - Managing Init/Shutdown Scripts

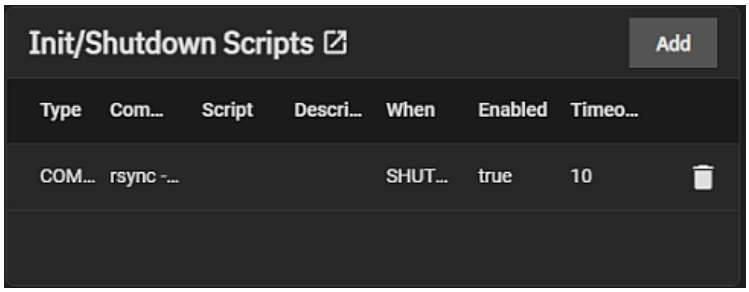
This article provides information on adding or modifying init/shutdown scripts in SCALE.

The **Init/Shutdown Scripts** widget on the **System > Advanced** screen allows you to add scripts to run before or after initialization (start-up), or at shutdown. For example, creating a script to backup your system or run a systemd command before exiting and shutting down the system.

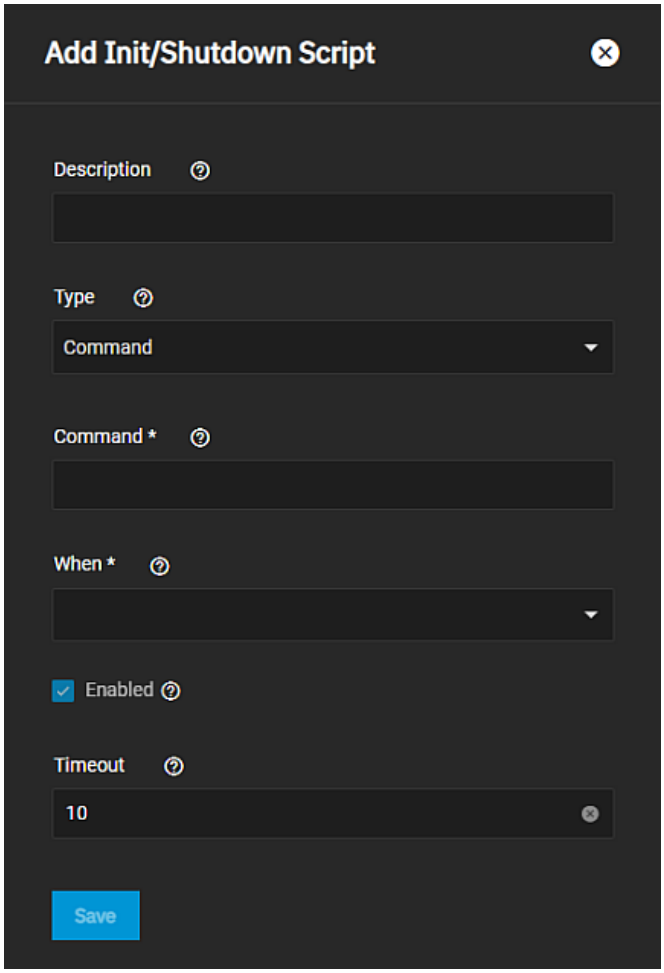
> Advanced settings have reasonable defaults in place. A warning message displays for some settings advising of the dangers making changes. Changing advanced settings can be dangerous when done incorrectly. Use caution before saving changes.
>
> 
>
>
> Make sure you are comfortable with ZFS, Linux, and system configuration backup and restoration before making any changes.

Adding an Init/Shutdown Script

The **Init/Shutdown Scripts** widget displays **No Init/Shutdown Scripts configured** until you add either a command or script, and then the widget lists the scripts configured on the system.



Click **Add** to open the **Add Init/Shutdown Script** configuration screen.



Enter a description and then select **Command** or **Script** from the **Type** dropdown list. Selecting **Script** displays additional options.

Enter the command string in **Command**, or if using a script, enter or use the browse to the path in **Script**. The script runs using dash(1).

Select the option from the **When** dropdown list for the time this command or script runs.

Enter the number of seconds after the script runs that the command should stop in **Timeout**.

Select **Enable** to enable the script. Leave clear to disable but not delete the script.

Click **Save**.

Editing an Init/Shutdown Script

Click a script listed on the **Init/Shutdown Scripts** widget to open the **Edit Inti/Shutdown Script** configuration screen populated with the settings for that script.

You can change from a command to a script, modify the script or command as needed.

To disable but not delete the command or script, clear the **Enabled** checkbox.

Click **Save**.

Related Content

- Advanced Settings Screen

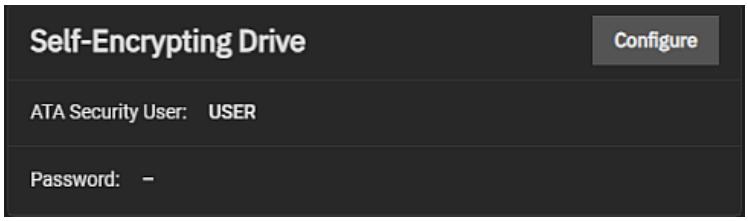
3.10.3.6 - Managing SEDs

This article provides information on adding or modifying self-encrypting drive (SED) user and global passwords in SCALE.

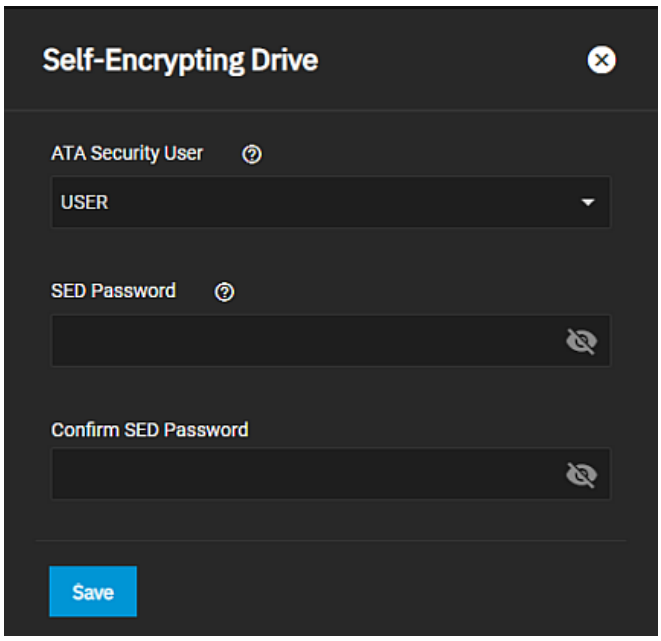
The **Self-Encrypting Drive(s)** widget on the **System > Advanced** screen allows you set the user and global SED password in SCALE.

Managing Self-Encrypting Drives

The **Self-Encrypting Drive** (SED) widget displays the ATA security user and password configured on the system.



Click **Configure** to open the **Self-Encrypting Drive** configuration screen. The **Self-Encrypting Drive** configuration screen allows users set the ATA security user and create a SED global password.



Select the user passed to *camcontrol security -u* to unlock SEDs from the **ATA Security User** dropdown list. Options are **USER** or **MASTER**.

Enter the global password to unlock SEDs in **SED Password** and in **Confirm SED Password**.

Click **Save**.

Related Content

- Advanced Settings Screen

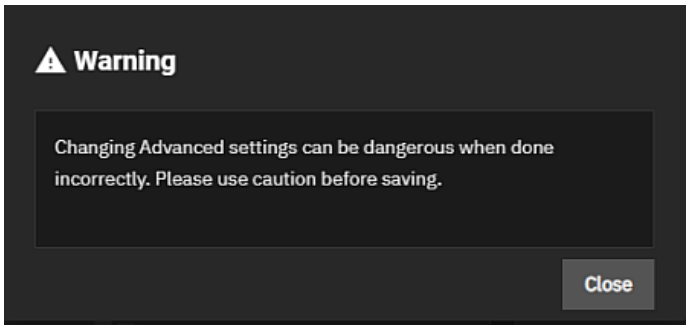
Related Disks Articles

- Advanced Settings Screen
- Disks Screens
- Managing Disks
- Importing Disks
- Replacing Disks
- View Enclosure Screen
- Wiping a Disk
- SLOG Over-Provisioning

3.10.3.7 - Managing GPUs

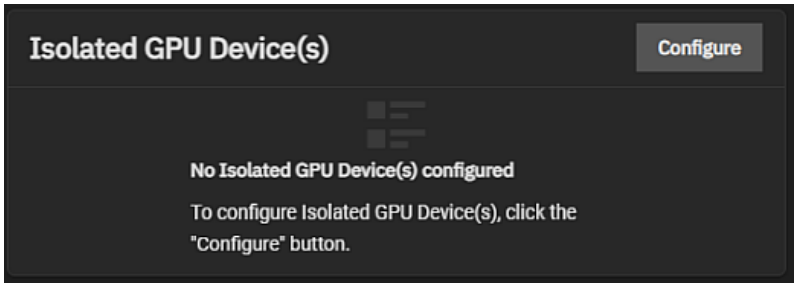
This article provides information on isolating Graphic Processing Units (GPUs) installed in your system for use by a VM in SCALE.

The **Isolate GPU PCI's ID** widget on the **System > Advanced** screen allows you to isolate a GPU installed in your system for use by a virtual machine (VM).

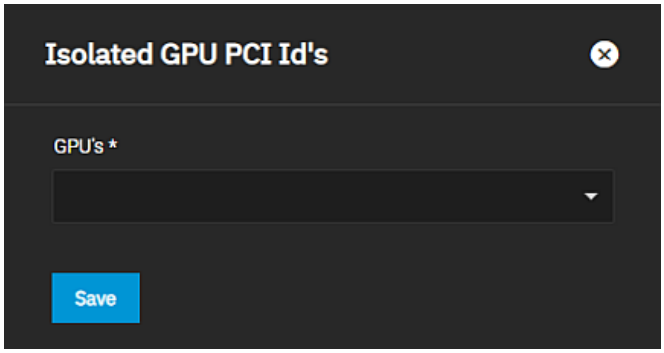
> Advanced settings have reasonable defaults in place. A warning message displays for some settings advising of the dangers making changes. Changing advanced settings can be dangerous when done incorrectly. Use caution before saving changes.
>
> 
>
>
> Make sure you are comfortable with ZFS, Linux, and system configuration backup and restoration before making any changes.

Isolated GPU Device(s)

The **Isolated GPU Device(s)** widget displays an graphics processing unit (GPU) device(s) configured on your system.



Click **Configure** to open the **Isolate GPU PCI's ID** screen where you can select a GPU to isolate it for GPU passthrough. GPU passthrough allows the TrueNAS SCALE kernel to directly present an internal PCI GPU to a virtual machine (VM).



The GPU device acts like the VM is driving it, and the VM detects the GPU as if it is physically connected. Select the GPU device ID from the dropdown list. To isolate a GPU you must have at least two in your system; one allocated to the host system for system functions and the other available to isolate for use by a VM or application. Isolating the GPU prevents apps and the system from accessing it.

Click **Save**.

Related Content

- Adding and Managing VMs

- Virtualization Screens
- Advanced Settings Screen

3.10.4 - Managing Boot Environments

This article provides instructions on managing TrueNAS boot environments.

TrueNAS supports a ZFS feature known as boot environments. These are snapshot clones that TrueNAS can boot into. Only one boot environment can be used for booting.

How does this help me?
A boot environment allows rebooting into a specific point in time and greatly simplifies recovering from system misconfigurations or other potential system failures. With multiple boot environments, the process of updating the operating system becomes a low-risk operation. The updater automatically creates a snapshot of the current boot environment and adds it to the boot menu before applying the update. If anything goes wrong during the update, the system administrator can boot TrueNAS into the previous environment to restore system functionality.

Managing Boot Environments

To view the list of boot environments on the system, go to **System Settings > Boot**. Each boot environment entry contains this information:

- **Name**: the name of the boot entry as it appears in the boot menu.
- **Active**: indicates which entry boots by default if a boot environment is not active.
- **Created**: indicates the boot environment creation date and time.
- **Space**: shows boot environment size.
- **Keep**: indicates whether or not TrueNAS deletes this boot environment when a system update does not have enough space to proceed.

To access more options for a boot environment, click ⋮ to display the list of options.

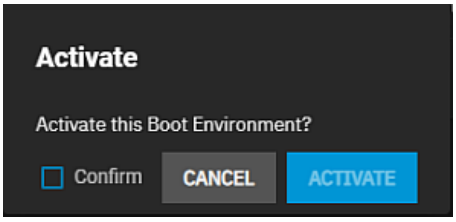
Activating a Boot Environment

The option to activate a boot environment only displays for boot entries not set to **Active**

Click Here for More Information

Activating an environment means the system boots into the point of time saved in that environment the next time it is started.

Click the ⋮ for an inactive boot environment, and then select **Activate** to open the **Activate** dialog.



Click **Confirm**, and then click **Activate**.

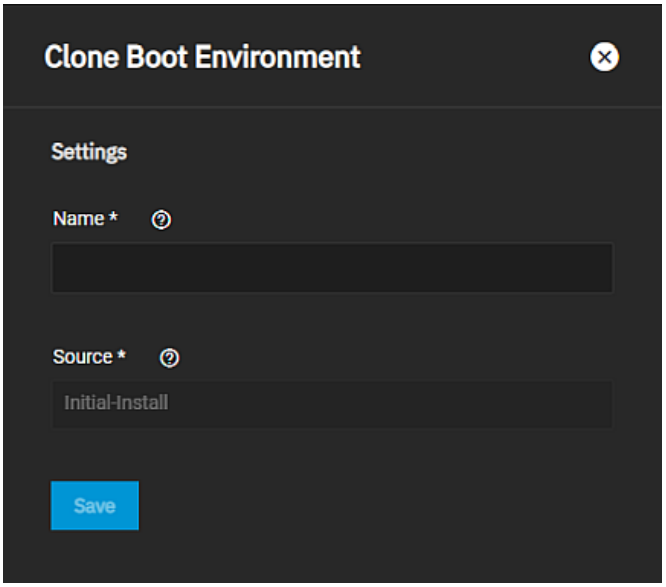
The **System Boot** screen status changes to **Reboot** and the current **Active** entry changes from **Now/Reboot** to **Now**, indicating that it is the current boot environment but is not used on next boot.

Cloning a Boot Environment

Cloning copies the selected boot environment into a new entry.

Click Here for More Information

Click the ⋮ for a boot environment, and then select **Clone** to open the **Clone Boot Environment** window.



Enter a new name using only alphanumeric characters, and/or the allowed dashes (-), underscores (_), and periods (.) characters.

The **Source** field displays the boot environment you are cloning. If the displayed name is incorrect, close the window and select the correct boot environment to clone.

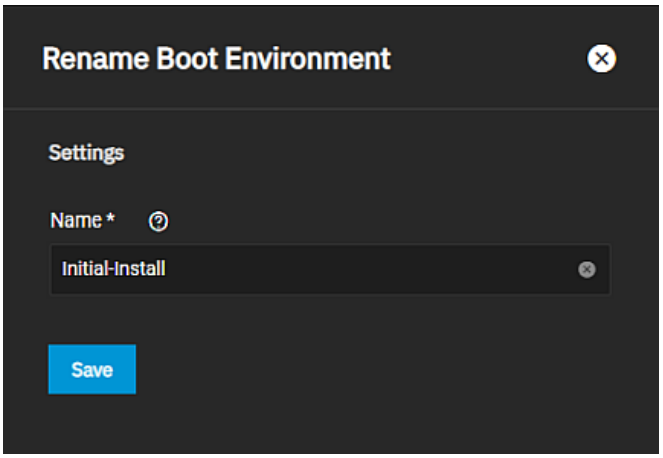
Click **Save**.

Renaming a Boot Environment

You can change the name of any boot environment on the **System > Boot** screen.

Click Here for More Information

Click the ⋮ for a boot environment, and then select **Rename** to open the **Rename Boot Environment** window.



Enter a new name using only alphanumeric characters, and/or the allowed dashes (-), underscores (_), and periods (.) characters.

Verify the boot environment in **Name** is the one you want to rename.

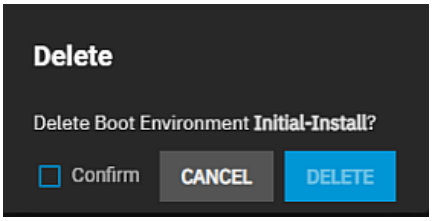
Click **Save**.

Deleting a Boot Environment

Deleting a boot environment removes it from the **System > Boot** screen and from the boot menu.

Click Here for More Information

Click the ⋮ for a boot environment, and then select **Delete** to open the **Delete** dialog. Select **Confirm** and then click **Delete**.



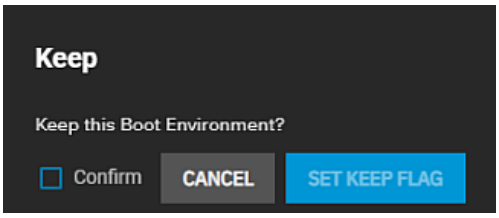
You cannot delete the default and any active entries. Because you cannot delete an activated boot entry, this option does not display for activated boot environments To delete the active boot environment, first activate another entry and then delete the environment you want to remove.

Keeping a Boot Environment

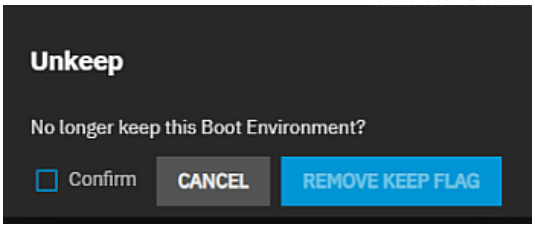
Keep toggles with the **Unkeep** option, and they determine whether the TrueNAS updater can automatically delete this boot environment if there is not enough space to proceed with an update.

Click Here for More Information

Click the ⋮ for a boot environment, and then select **Keep** to open the **Keep** dialog. Select **Confirm** and then click **Keep Flag**.



The boot environment action list removes the **Keep** option and adds **Unkeep**.



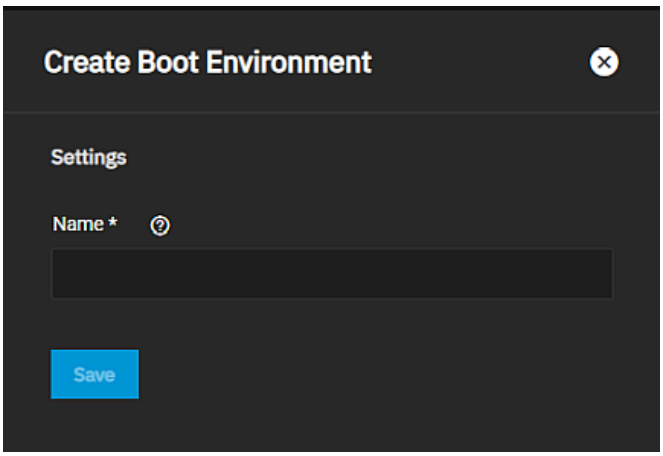
This makes the boot environment subject to automatic deletion if the TrueNAS updater needs space for an update.

Adding a Boot Environment

You can make a new boot environment to your TrueNAS.

Click Here for More Information

To add a new boot environment, click **Actions** at the top right of the **System > Boot** screen and click **add** to open the **Create Boot Environment** window.



Enter a new name using only alphanumeric characters, and/or the allowed dashes (-), underscores (_), and periods (.) characters.

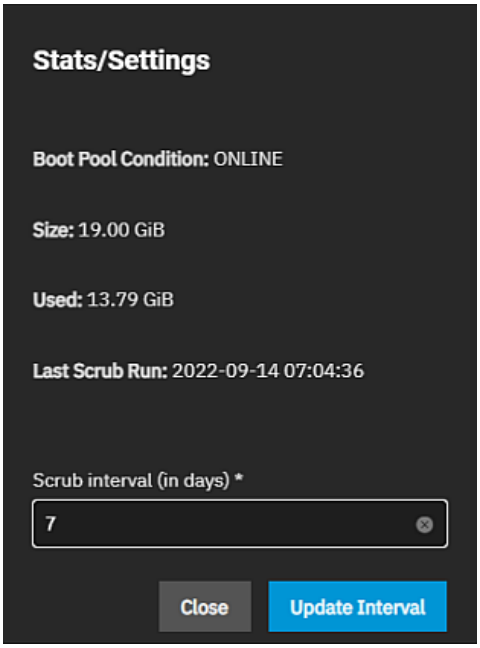
Click **Save**.

Changing the Scrub Interval

The **Stats/Settings** option displays current system statistics and provides the option to change the scrub interval, or how often the system runs a data integrity check on the operating system device.

Click Here for More Information

Click **Actions** at the top right of the **System > Boot** screen and click **Stats/Settings**. The **Stats/Settings** window displays statistics for the operating system device: **Boot pool Condition** as **ONLINE** or **OFFLINE**, **Size** in GiB and the space in use in **Used**, and **Last Scrub Run** with the date and time of the scrub. By default, the operating system device is scrubbed every 7 days.



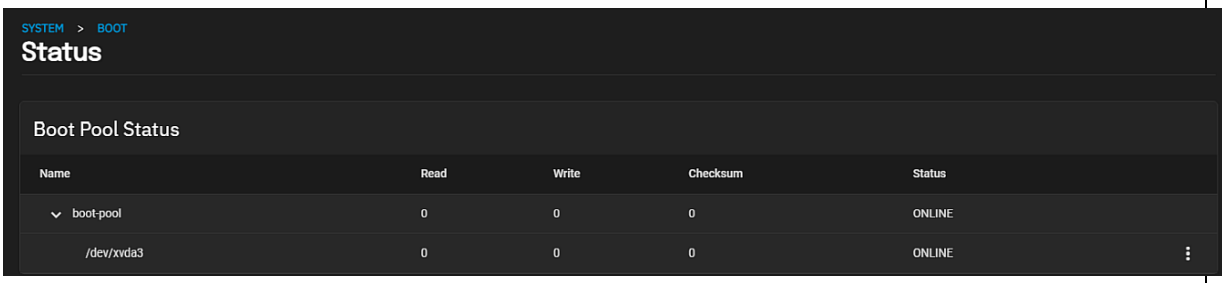
To change the default scrub interval, input a different number in **Scrub interval (in days)** and click **Update Interval**.

Checking Boot Pool Status

You an attach or replace the boot environment.

Click Here for More Information

Click **Actions** at the top right of the **System > Boot** screen and click **Boot Pool Status** to open the **Boot Pool Status** screen that shows current operating system device (boot pool), the path for the pool, and the read, write, or checksum errors for the device.



Click the ⋮ to open the **Actions** options. Click **Attach** to select a device from the **Member Disk** dropdown.

Select **Use all disk space** to use the entire capacity of the new device.

Click **Save**.

If you want to replace the device, click **Replace**, select the device from the **Member Disk** dropdown, and then click **Save**.

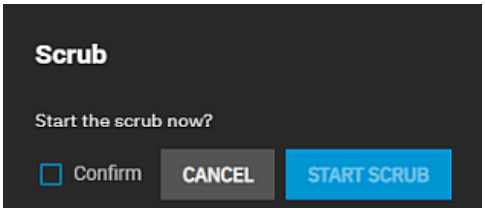
To return to the **System > Boot** screen, click **Boot** in the breadcrumb header.

Scrubbing a Boot Pool

You can perform a manual data integrity check (scrub) of the operating system device at any time.

Click Here for More Information

Click **Actions** at the top right of the **System > Boot** screen and click **Scrub Boot Pool** to open the **Scrub** dialog.



Click **Confirm** and then **Start Scrub**.

Changing Boot Environments

Sometimes, rolling back to an older boot environment can be useful. For example, if an update process does not go as planned, it is easy to roll back to a previous boot environment. TrueNAS automatically creates a boot environment when the system updates.

Use the **Activate** option on the ⋮ for the desired boot environment.

This changes the **Active** column to **Reboot** for the boot environment, and means the boot environment becomes active on the next system boot. The system configuration also changes to the state it was in when the boot environment was created.

Related Content

- System Boot Screens

3.10.5 - Services

This article provides general information on the TrueNAS services, and a summary of each indiviual service article in the Services area.

System Settings > Services displays each system component that runs continuously in the background. These typically control data-sharing or other external access to the system. Individual services have configuration screens and activation toggles, and you can set them to run automatically.

Documented services related to data sharing or automated tasks are in their respective Shares and Tasks articles.

Article Summaries

- Configuring Dynamic DNS Service

  This article provides instructions on how to configure dynamic DNS service in TrueNAS SCALE.

- Configuring FTP Service

  This article provides instructions on configuring the storage, user, and access permissions FTP service uses, and configuring the FTP service.

- Configuring LLDP Services

  This article provides instuctions on configuring the Link Layer Discovery Protocol (LLDP) service.

- Configuring NFS Service

  This article provides information on configuring NFS service in SCALE.

- Configuring OpenVPN Service

  This article provides configuration information for OpenVPN Client and Server services.

- Configuring Rsync Modules

  This article provides information on configuring an rsync module and TCP port to use as an alternative to SSH when communicating with a TrueNAS as a remote rsync server.

- Configuring S.M.A.R.T. Service

  This article provides information on S.M.A.R.T. service screen settings.

- Configuring S3 Service

  This article provides information on configuring S3 service in SCALE.

- Configuring SMB Service

  This article provides instructions on configuring the SMB service in SCALE.

- Configuring SNMP Service

  This article provides information on configuring SNMP service on SCALE.

- Configuring SSH Service

  This article provides information on configuring the SSH service in SCALE, and using an SFTP connection.

- Configuring TFTP Services

  This article provides instructions on configuring TFTP service in SCALE.

- Configuring UPS Service

  This article provides information on configuring UPS service in SCALE.

- Configuring WebDAV Service

  This article provides information on configuring the WebDAV service.

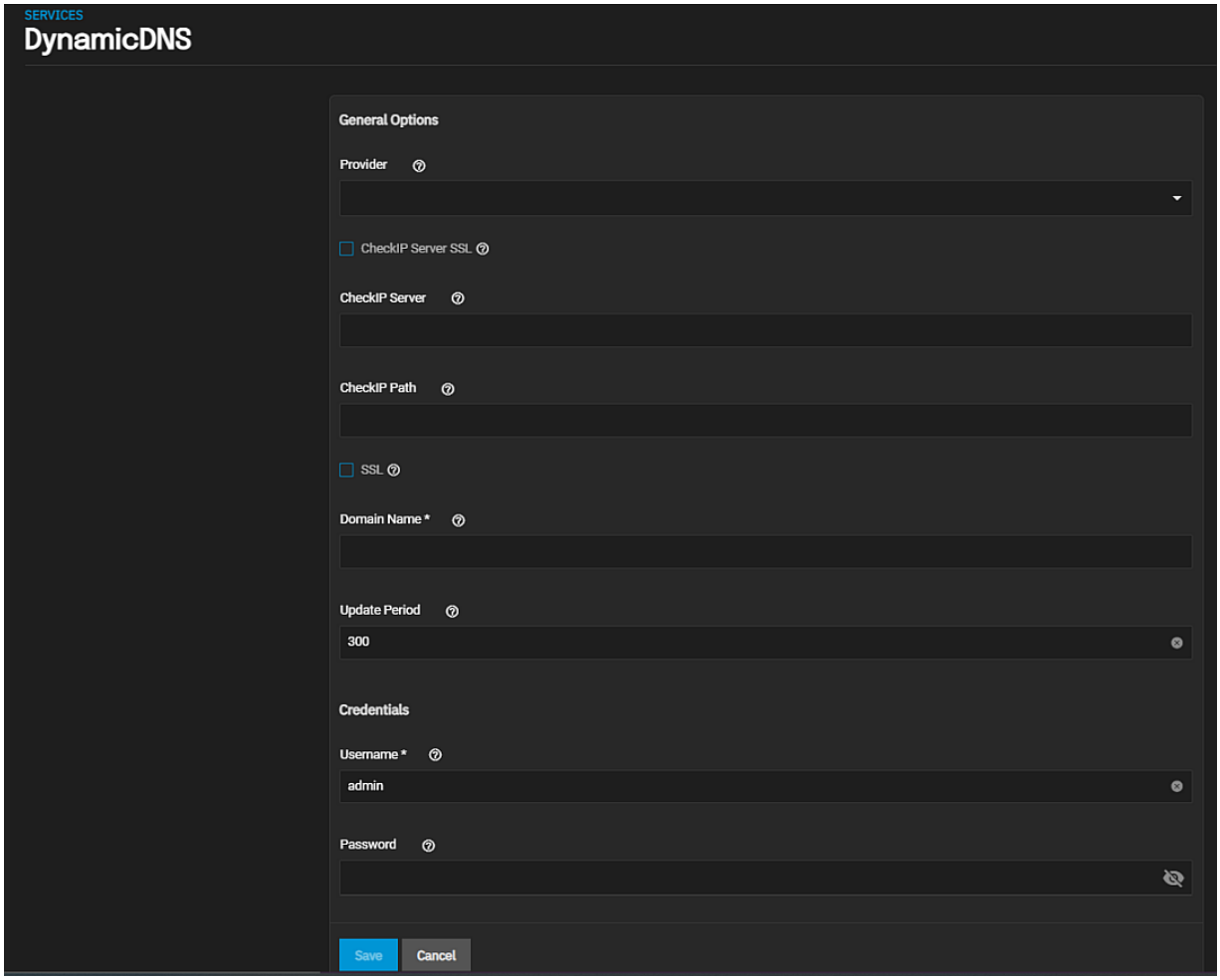
3.10.5.1 - Configuring Dynamic DNS Service

This article provides instructions on how to configure dynamic DNS service in TrueNAS SCALE.

Dynamic Domain Name Service (DDNS) is useful when you connect TrueNAS to an Internet service provider (ISP) that periodically changes the system's IP address. With Dynamic DNS, the system automatically associates its current IP address with a domain name and continues to provide access to TrueNAS even if the system IP address changes.

Configuring Dynamic DNS

DDNS requires registration with a DDNS service such as DynDNS before configuring TrueNAS. Have the DDNS service settings available or open in another browser tab when configuring TrueNAS. Log in to the TrueNAS web interface and go to **System Settings > Services > Dynamic DNS**.



Select the provider from the dropdown list, or if not listed, select **Custom Provider**. If you select **Custom Provider** also enter the DynmicDNS server name in **Custom Server** and the path to the server obtained from that provider in **Custom Path**.

Select **CheckIP Server SSL** if you want to use HTTPS to connect to the CheckIP server, and then enter the name and port number of the server that reports the external IP addresses and the path to the CheckIP server.

Select **SSL** if you want to use HTTPS to connect o the server that updates the DNS record.

Enter the fully qualified domain name of the host with the dynamic IP address in **Domain Name**.

Enter the number of seconds for how often you want to check the IP address in **Update Period**.

Click **Save**.

Start the DDNS service after choosing your **Provider** options and saving the settings.

Related Content

- Dynamic DNS Service Screen

3.10.5.2 - Configuring FTP Service

This article provides instructions on configuring the storage, user, and access permissions FTP service uses, and configuring the FTP service.

The File Transfer Protocol (FTP) is a simple option for data transfers. The SSH and Trivial FTP options provide secure or simple config file transfer methods respectively.

Options for configuring **FTP**, **SSH**, and **TFTP** are in **System Settings > Services**. Click the ✎ to configure the related service.

Configuring FTP Services Storage

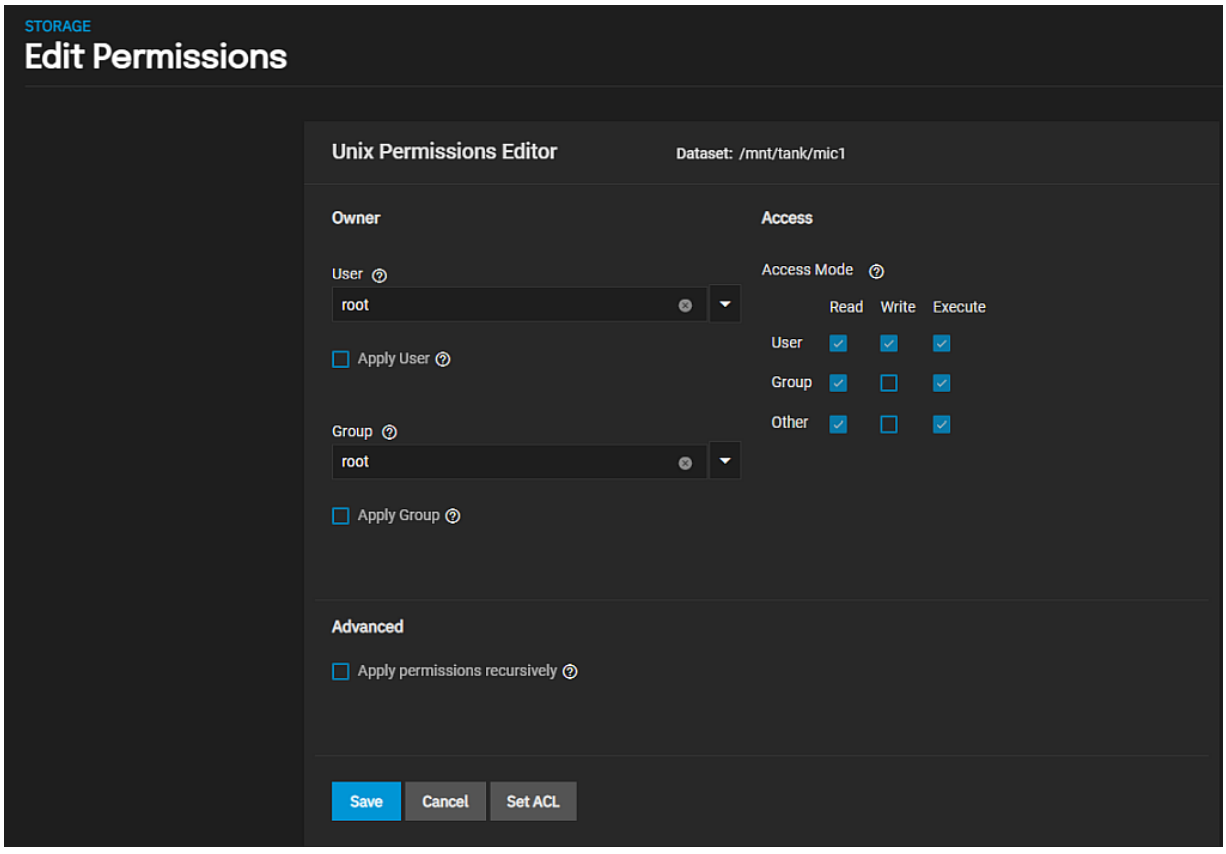
FTP requires a new dataset and a local user account.

Go to **Storage** to add a new dataset to use as storage for files.

Next, add a new user. Go to **Credentials > Local Users** and click **Add** to create a local user on the TrueNAS.

Assign a user name and password, and link the newly created FTP dataset as the user home directory. You can do this for every user, or create a global account for FTP (for example, *OurOrgFTPaccnt*).

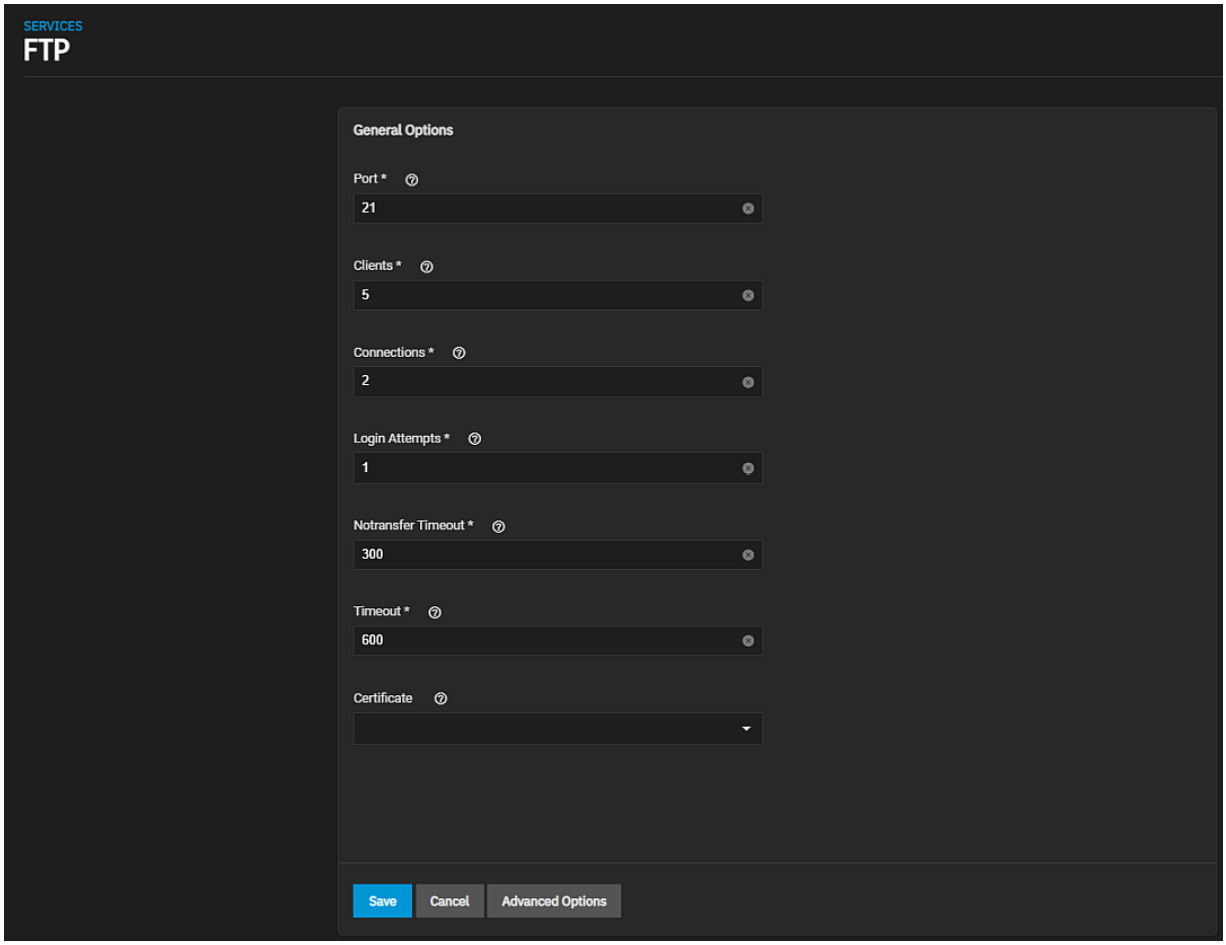
Edit the file permissions for the new dataset.



Return to **Storage**, locate the new dataset, click ⋮, and then select **View Permissions**. Next click ✎. Enter or select the new user account in the **User** and **Group** fields. Select **Apply User** and **Apply Group**. Select the **Read**, **Write** and **Execute** for **User**, **Group** and **Other** that you want to apply. Click **Save**.

Configuring FTP Service

To configure FTP, go to **System Settings > Services** and find **FTP**, then click ✎ to open the **Services > FTP** screen.



Configure the options according to your environment and security considerations. Click **Advanced Settings** to display more options.

To confine FTP sessions to the home directory of a local user, select both **chroot** and **Allow Local User Login*.

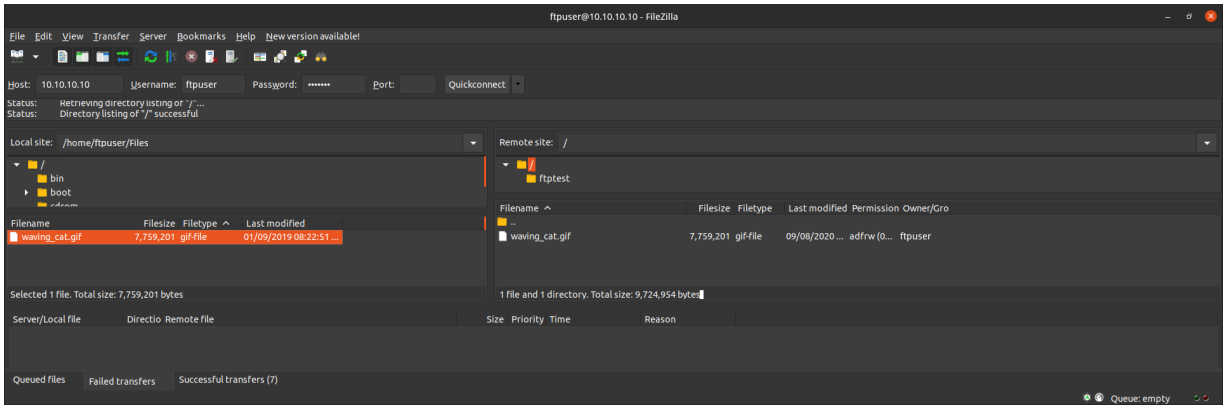
Do *not* allow anonymous or root access unless it is necessary. For better security, enable TLS when possible (especially when exposing FTP to a WAN). TLS effectively makes this FTPS.

Click **Save** and then start the FTP service.

Connecting with FTP

Use a browser or FTP client to connect to the TrueNAS FTP share. The images below use FileZilla, a free option.

The user name and password are those of the local user account on the TrueNAS. The default directory is the same as the user home directory. After connecting, you can create directories and upload or download files.



Related Content

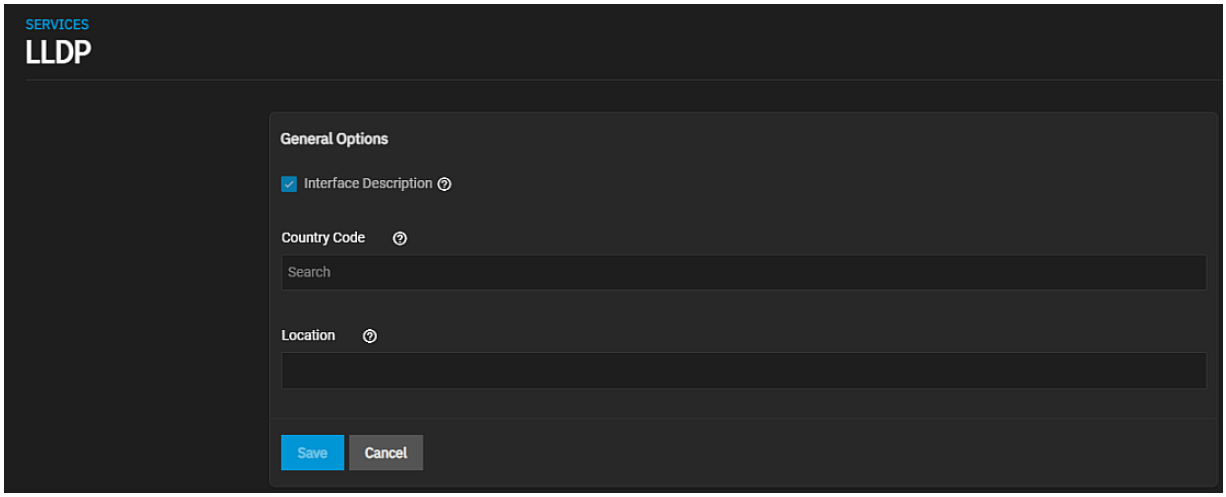
- Configuring TFTP Services

3.10.5.3 - Configuring LLDP Services

This article provides instuctions on configuring the Link Layer Discovery Protocol (LLDP) service.

Network devices use the Link Layer Discovery Protocol (LLDP) to advertise their identity, capabilities, and neighbors on an Ethernet network. TrueNAS uses the ladvd LLDP implementation. When the local network contains managed switches, configuring and starting LLDP tells TrueNAS to advertise itself on the network.

To configure LLDP, go to **System Settings > Services**, find **LLDP** and click the .



Enter the two-letter country code as found in ISO 3166-1 alpha-2 used to enable LLDP location support.

Enter the physical location of the host in **Interface Description**.

To save any peer information received, select **Interface Description**.

Click **Save**.

Start the service.

Related Content

- LLDP Services Screen

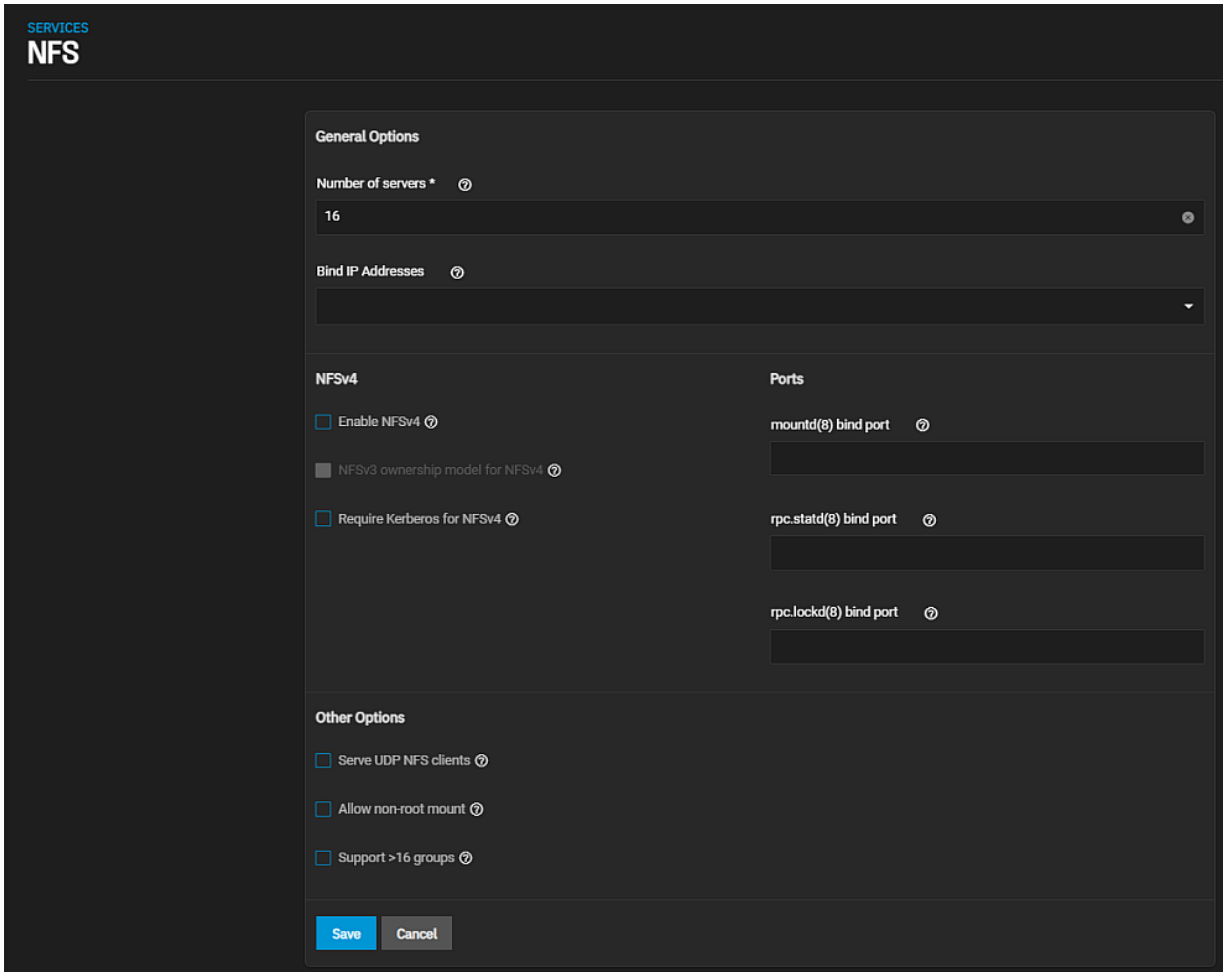
3.10.5.4 - Configuring NFS Service

This article provides information on configuring NFS service in SCALE.

The **Services > NFS** configuration screen displays settings to customize the TrueNAS NFS service.

You can access it from **System Settings > Services** screen. Locate **NFS** and click  to open the screen, or use the **Config Service** option on the **Unix (NFS) Share** widget options menu found on the main **Sharing** screen.

Select **Start Automatically** to activate NFS service when TrueNAS boots.



Configuring NFS Service

Unless a specific setting is required, we recommend using the default NFS settings.

First enter the number of servers you want to create in **Number of servers**.

Select the IP addressed from the **Bind IP Addresses** dropdown list if you want to use a specific static IP address, or to list on all available addresses leave this blank.

If you are using NFSv4 select **Enable NFSv4**. **NFSv3 ownership model for NFSv4** clears, allowing you to select or leave it clear.

If you want to force NFS shares to fail if the Kerberos ticket is unavailable, select **Require Kerberos for NFSv4**.

Next enter a port to bind to in the field that applies:

- Enter a port to bind mountd(8) in **mountd(8) bind port**.
- Enter a port to bind rpc.stad(8)in **rpc.statd(8) bind port**.
- Enter a port to bind rpc.lockd(8) in **rpc.lockd(8) bind port**.

Select **Allow non-root mount** only if required by the NFS client to allow serving non-root mount requests.

Click **Save**.

Start the NFS service.

When TrueNAS is already connected to Active Directory, setting **NFSv4** and **Require Kerberos for NFSv4** also requires a Kerberos Keytab.

Related Content

- NFS Services Screen
- NFS Shares Screens
- Adding NFS Shares

3.10.5.5 - Configuring OpenVPN Service

This article provides configuration information for OpenVPN Client and Server services.

A virtual private network (VPN) is an extension of a private network over public resources. It lets clients securely connect to a private network even when remotely using a public network. TrueNAS provides OpenVPN as a system-level service to provide VPN server or client functionality. TrueNAS can act as a primary VPN server that allows remote clients to access system data using a single TCP or UDP port. Alternatively, TrueNAS can integrate into a private network, even when the system is in a separate physical location or only has access to publicly visible networks.

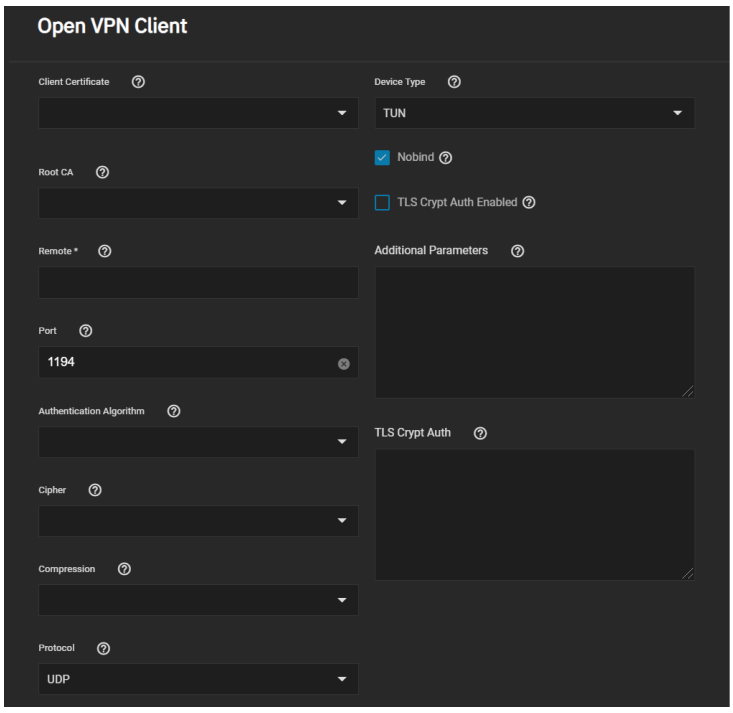
Before configuring TrueNAS as either an OpenVPN server or client, you need an existing public key infrastructure (PKI) with Certificates and Certificate Authorities created in or imported to TrueNAS.

What does this do?
Certificates allow TrueNAS to authenticate with clients or servers by confirming a valid master Certificate Authority (CA) signed the network credentials. To read more about the required PKI for OpenVPN, see the OpenVPN PKI Overview.

In general, configuring TrueNAS OpenVPN (server or client) includes selecting networking credentials, setting connection details, and choosing additional security or protocol options.

OpenVPN Client

Go to **System Settings > Services** and find **OpenVPN Client**. Click the pencil to configure the service.



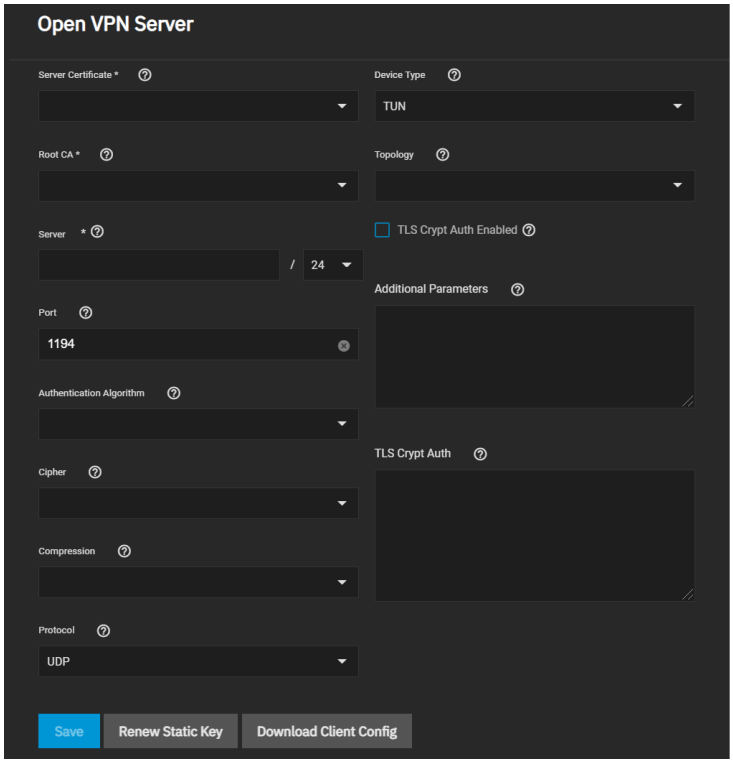
Choose the certificate to use as an OpenVPN client. The certificate must exist in TrueNAS and be active (unrevoked). Enter the **Remote** OpenVPN server's hostname or IP address.

Continue to review and choose any other Connection Settings that fit your network environment and performance requirements. The **Device Type** must match the OpenVPN server **Device Type**. **Nobind** prevents using a fixed port for the client and is enabled by default so the OpenVPN client and server run concurrently.

Finally, review the Security Options and ensure they meet your network security requirements. If the OpenVPN server uses TLS Encryption, copy the static TLS encryption key and paste it into the **TLS Crypt Auth** field.

OpenVPN Server

Go to **System Settings > Services** and find **OpenVPN Server**. Click the pencil to configure the service.



Choose a **Server Certificate** for the OpenVPN server. The certificate must exist in TrueNAS and be active (unrevoked).

Now define an IP address and netmask for the OpenVPN **Server**. Select the remaining Connection Settings that fit your network environment and performance requirements. If using a **TUN Device Type**, you can choose a virtual addressing topology for the server in **Topology**:

- **NET30**: Use one */30* subnet per client in a point-to-point topology. Use when connecting clients are Windows systems.
- **P2P**: Point-to-point topology that points the local server and remote client endpoints to each other. Each client gets one IP address. Use when none of the clients are Windows systems.
- **SUBNET**: The interface uses an IP address and subnet. Each client gets one IP address. Windows clients require the **TAP-Win32 driver** version 8.2 or newer. **TAP** devices always use the **SUBNET Topology**.

TrueNAS applies the **Topology** selection to any connected clients.

When **TLS Crypt Auth Enabled** is selected, TrueNAS generates a static key for the **TLS Crypt Auth** field after saving the options. To change this key, click **Renew Static Key**. Clients connecting to the server require the key. TrueNAS stores keys in the system database and includes them in client config files. We recommend always backing up keys in a secure location.

Finally, review the Security Options and choose settings that meet your network security requirements.

After configuring and saving your OpenVPN Server, generate client configuration files to import to any OpenVPN client systems connecting to this server. You need the certificate from the client system already imported into TrueNAS. To generate the configuration file, click **Download Client Config** and select the **Client Certificate**.

Common Options (Client or Server)

Many OpenVPN server or client configuration fields are identical. This section covers these fields and lists specific configuration options in the Server and Client sections.

The **Additional Parameters** field manually sets any core OpenVPN config file options. See the OpenVPN Reference Manual for descriptions of each option.

Connection Settings

Setting	Description
Root CA	The Certificate Authority (CA) must be the root CA you used to sign the client and server certificates.
Port	The port that the OpenVPN connection is to use.
Compression	Choose a compression algorithm for traffic. Leave empty to send data uncompressed. **LZO** is a standard compression algorithm that is backward compatible with previous (pre-2.4) versions of OpenVPN. **LZ4** is newer and typically faster and requires fewer system resources.
Protocol	Choose between **UDP** or **TCP** OpenVPN protocols. **UDP** sends packets in a continuous stream. **TCP** sends packets sequentially.

Setting	Description
	UDP is usually faster and less strict about dropped packets than TCP. To force the connection to be IPv4 or IPv6, choose one of the `4` or `6` UDP or TCP options.
Device Type	Use a **TUN** or **TAP** virtual networking device and layer with OpenVPN. The device must be identical between the OpenVPN server and clients.

Security Options

OpenVPN includes several security options since using a VPN involves connecting to a private network while sending data over less secure public resources. Security options are not required, but they help protect data users send over the private network.

Setting	Description
Authentication Algorithm	Validates packets sent over the network connection. Your network environment might require a specific algorithm. If not, **SHA1 HMAC** is a reliable algorithm to use.
Cipher	Encrypts data packets sent through the connection. Ciphers aren't required but can increase connection security. You might need to verify which ciphers your networking environment requires. If there are no specific cipher requirements, AES-256-GCM is a good default choice.
TLS Encryption	When **TLS Crypt Auth Enabled** is selected, OpenVPN adds another layer of security by encrypting all TLS handshake messages. This setting requires sharing a static key between the OpenVPN server and clients.

Service Activation

Click **Save** after configuring the server or client service. Start the service by clicking the related toggle in **System Settings > Services**. Hover over the toggle to check the service current state.

Selecting **Start Automatically** starts the service whenever TrueNAS completes booting.

Related Content

- OpenVPN Screens

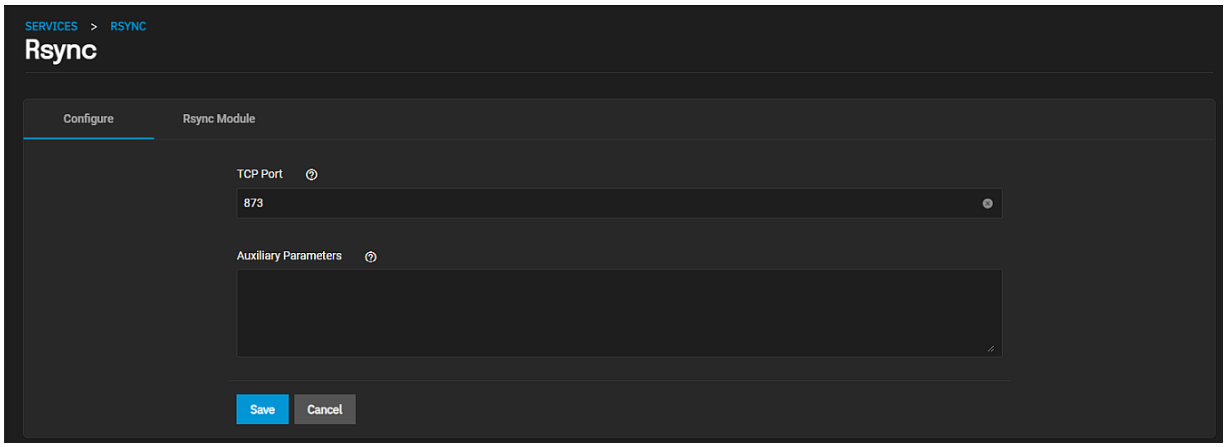
3.10.5.6 - Configuring Rsync Modules

This article provides information on configuring an rsync module and TCP port to use as an alternative to SSH when communicating with a TrueNAS as a remote rsync server.

Rsync is a utility that copies data across a network. The **Services > Rsync** screen has two tabs: **Configure** and **Rsync Module**. Use the **Configure** screen to add the TCP port number for the rsync service. Port 22 is reserved for TrueNAS. Use the **Rsync Module** screen to configure an rsync module on a TrueNAS system. You must configure at least one rsync module. This module is used as the communication mode when you set up a data protection rsyc task.

Adding an Rsync Module TCP Port

Go to **Services** and click the **Configure** icon for **Rsync** to open the **Configure** screen.



Enter a new port number if not the default in **TCP Port**. This is the port the rsync server listens on.

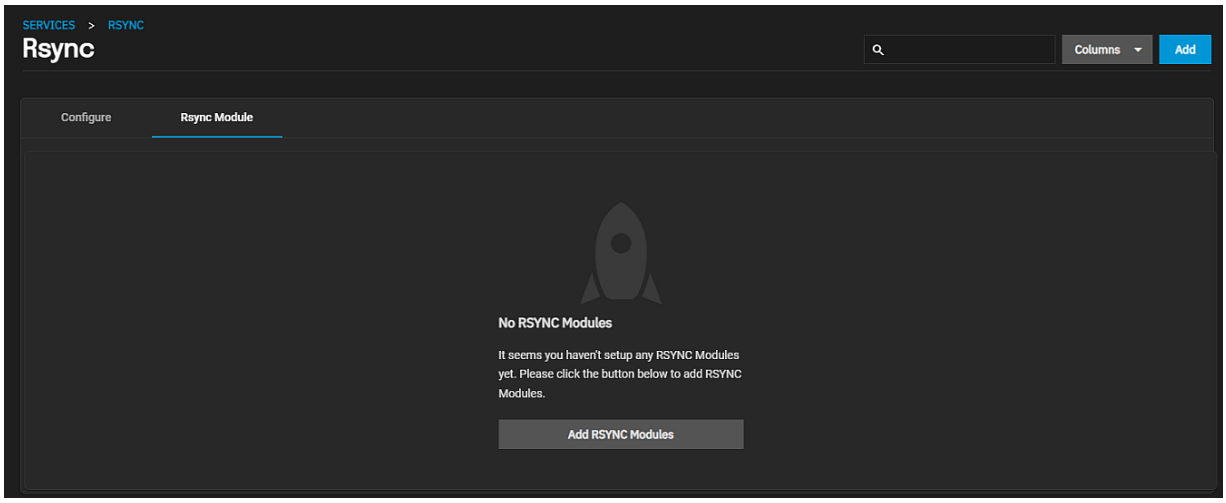
Enter any additional parameters from rsyncd.conf(5) you want to use in **Auxiliary Parameters**.

Click **Save**.

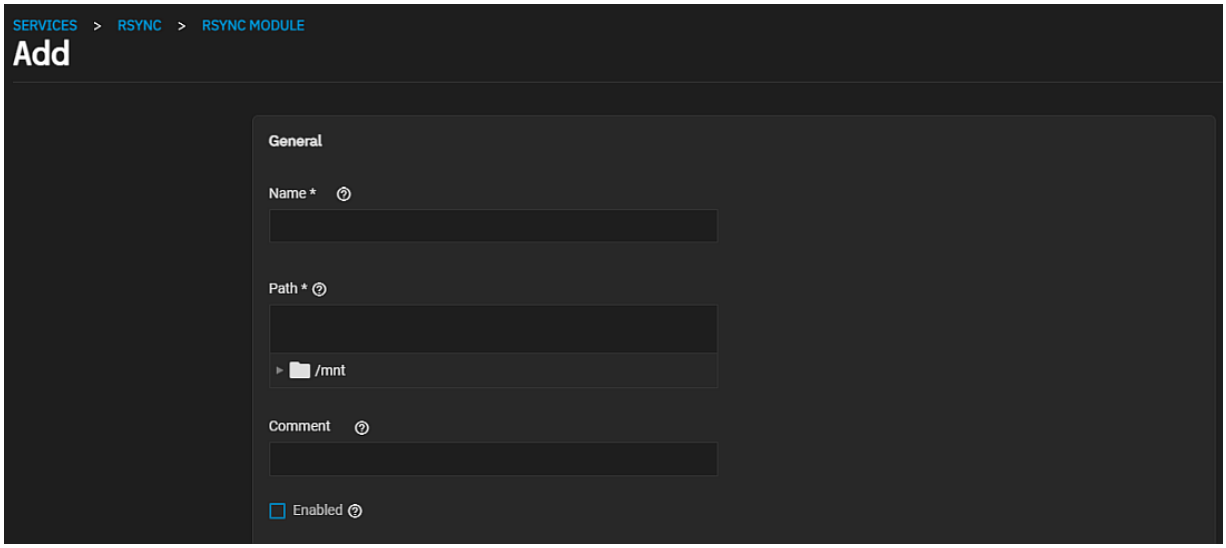
Adding an Rsync Module

When you set up an rsync task on the **Data Protection** screen, you can use either **Module** or **SSH** as the rsync mode. If you select **Module** in **Rsync Mode** on the **Add Rsync Task** screen, it uses the rysnc module set up in the rsync service as a custom-defined remote module of the rsync server.

To configure an rsync module click **Add** or **Add Rsync Modules** on the **Services > Rsync > Rsync Module** screen.



Click either **Add RSYNC Modules** if a remote module does not exist, or **Add** to open the **Add Rsync** screen to configure a module to use as the mode.



Enter a name, and then either enter the path or use the ▸ to the left of **/mnt** to browse to the pool or dataset to store received data. Click on the dataset or zvol name to populate the path field. To collapse the dataset tree, click the ▸ to the left of **/mnt** again.

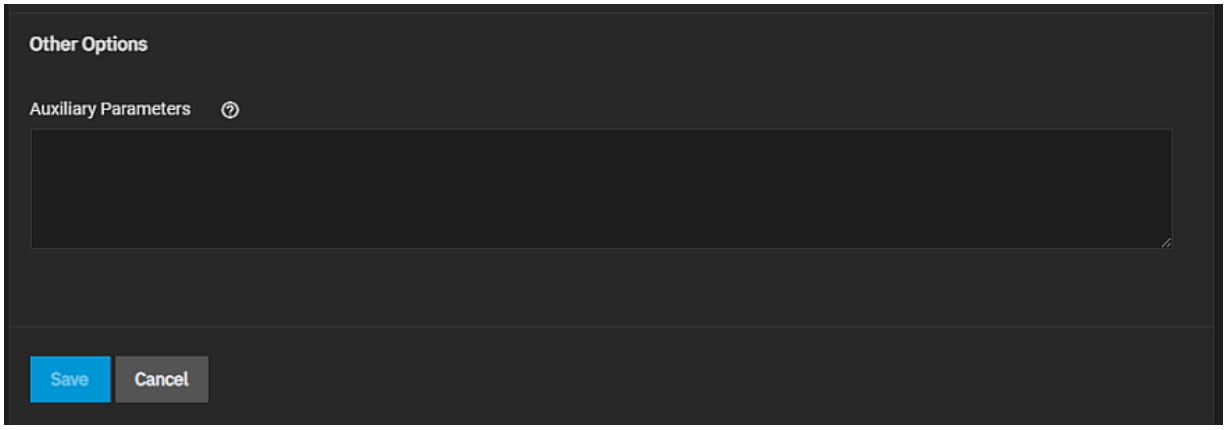
Select **Enable** to activate the module for use with rsync.

Select the permission access level in **Access Mode**.

Select the user and group that runs the rsync command during file transfer to and from this module.

Enter any allow and or deny hosts. Separate multiple entries by pressing `Enter` after each entry in **Hosts Allow** and/or **Hosts Deny**.

> When a **Hosts Allow** list is defined, *only* the IPs and hostnames on the list are able to connect to the module.



Enter any additional rsync configuration parameters from rsyncd.conf(5) in **Auxilliary Parameters**.

Click **Save**.

You can now configure an rsync task that uses **Module** in **Rsync Mode** on the **Add Rsync Task** screen, or change an existing rsync task from **SSH** to **Module**.

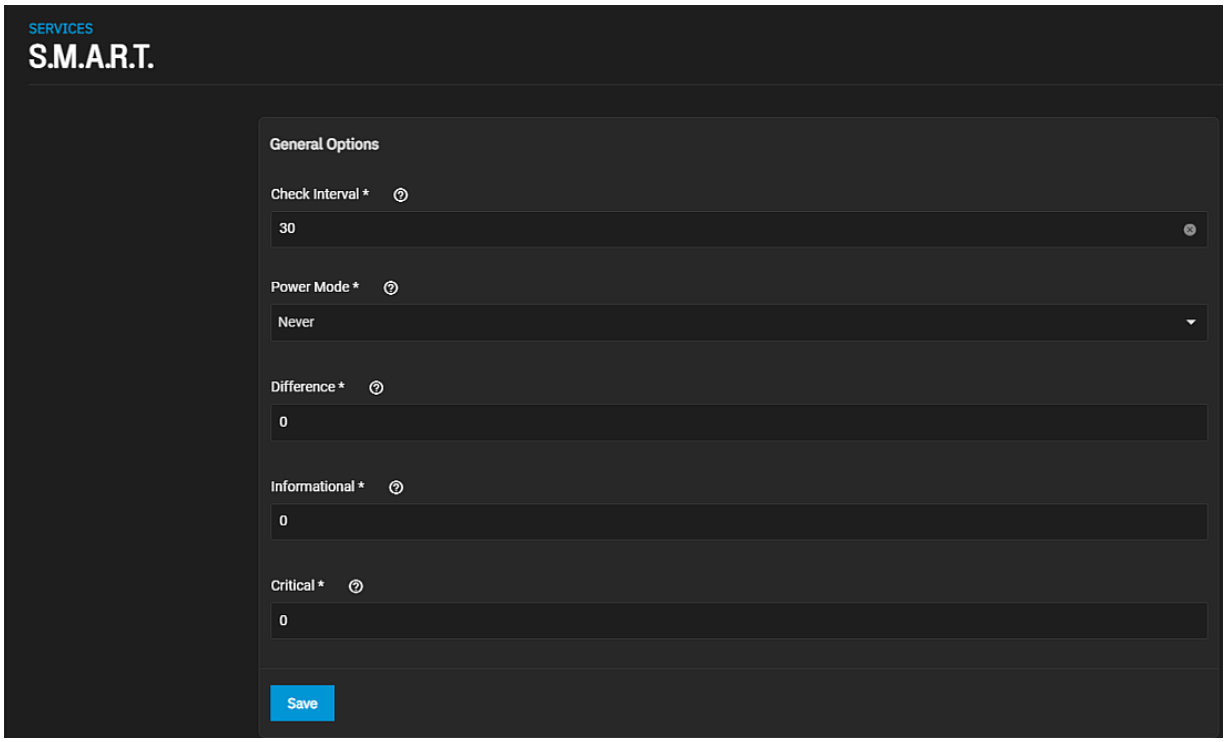
Related Content

- Adding SSH Credentials
- Configuring Rsync Tasks
- Rsync Tasks Screens
- Rsync Services Screen

3.10.5.7 - Configuring S.M.A.R.T. Service

This article provides information on S.M.A.R.T. service screen settings.

Use the **Services > S.M.A.R.T.** screen to configure when S.M.A.R.T. tests run and when to trigger alert warnings and send emails.



Click the **Configure** icon to open the screen.

Enter the time in minutes smartd to wake up and check if any tests are configured to run in **Check Interval**.

Select the power mode.

Set the temperatures that trigger alerts in **Difference**, **Informational** and **Critical**.

Click **Save** after changing any settings.

Start the service.

Related Content

- S.M.A.R.T. Service Screen
- Managing S.M.A.R.T. Tests
- S.M.A.R.T. Tests Screens

3.10.5.8 - Configuring S3 Service

This article provides information on configuring S3 service in SCALE.

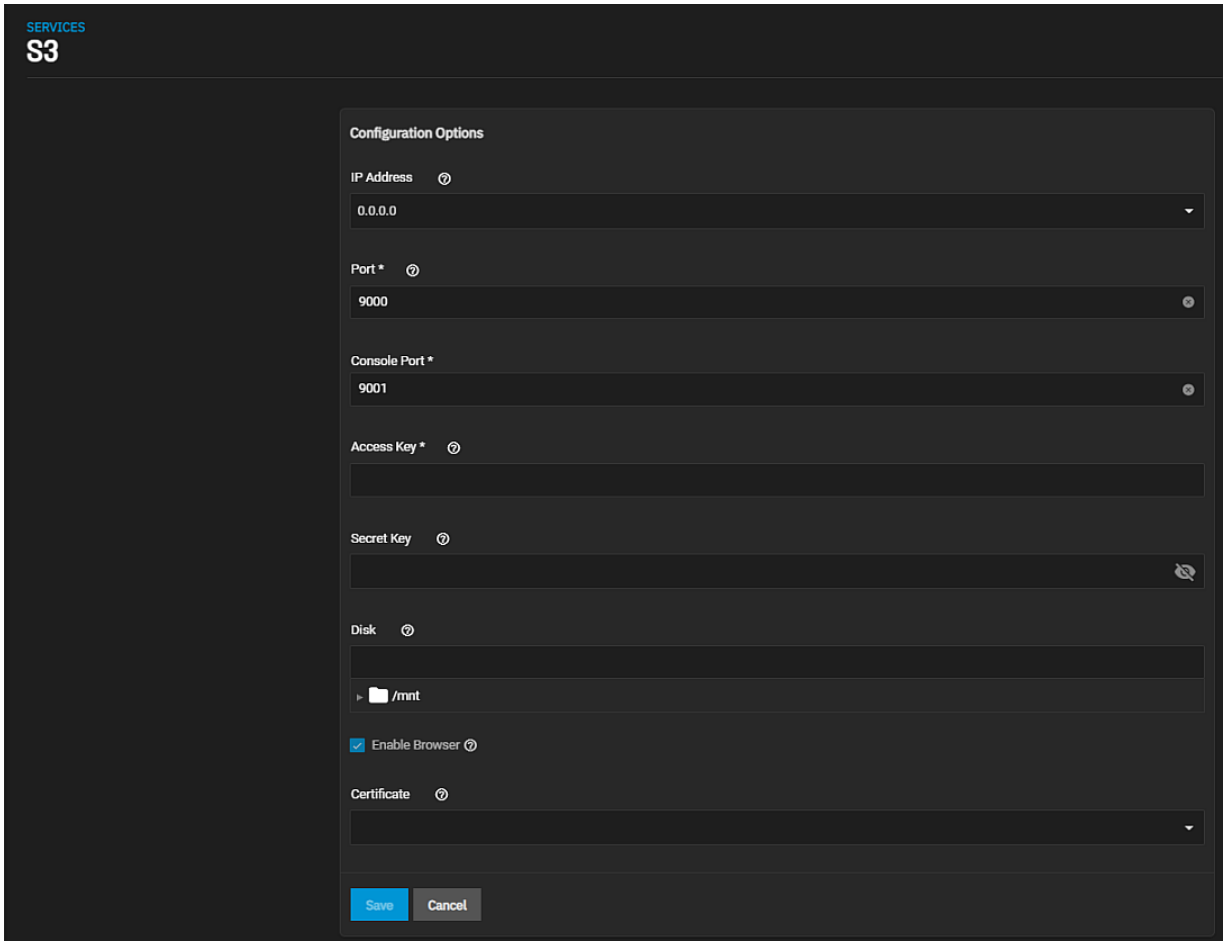
S3 allows you to connect to TrueNAS from a networked client system with the MinIO browser, s3cmd, or S3 browser.

Background
S3 is an object storage protocol that many major cloud providers like Amazon Web Services™ use. On TrueNAS, the service is another way to store files and can be viewed with a web browser. Because S3 is the de facto standard for cloud-based storage, setting up an S3 service allows organizations or online application developers to use TrueNAS to replace or archive expensive cloud storage.

Setting up the S3 service

> Having large numbers of files (>100K for instance) in a single bucket with no sub-directories can harm performance and cause stability issues.

Go to the **System Settings > Services** and find **S3**, then click to open the **Services > S3** screen to configure the service.



First, select a clean dataset, one that does not have existing data files. If you do not have a clean dataset, create a dataset. MinIO manages files as objects that you *cannot* mix with other dataset files.

Configure the remaining options as needed in your environment and start the service after saving any changes.

Making MinIO Connections

When **Enable Browser** is selected, test the MinIO browser access by opening a web browser and typing the TrueNAS IP address with the TCP port. You must allow the port entered in the **Services > S3** screen **Port** through the network firewall to

permit creating buckets and uploading files. Example: `https://192.168.0.3:9000`.

MinIO supports two different connection methods.

Using s3cmd

Linux or macOS users must have the s3cmd service installed before beginning this setup. On Windows, users can also refer to S3Express for a similar command-line experience.

> Ubuntu or other Linux distributions can access the configuration by running `s3cmd --configure` to walk through critical settings.

Enter the specified access key and the secret key. Enter the TrueNAS IP address followed by TCP port under `S3 Endpoint`, and reply `N` to the DNS-style bucket+hostname.

Save the file. On Linux, the default is in the home directory ~/.s3cfg.

If the connection has issues, open .s3cfg again to troubleshoot. In Ubuntu, use `nano .s3cfg` or `vi .s3cfg` or `gedit .s3cfg` depending on the preferred text editor. For other operating systems, .s3cfg file location and editing tools might vary.

Scroll down to the host_bucket area and ensure the configuration removed the `%(bucket)s.` portion and the address points to the *IP_address:TCP_port* for the system.

Correct Example

```
host_base = `192.168.123.207:9000`
host_bucket = `192.168.123.207:9000`
```

Incorrect Example

```
host_base = `192.168.123.207`
host_bucket = `%(bucket)s.192.168.123.207`
```

Poll the buckets using `s3cmd ls` to see the buckets created with the MinIO browser.

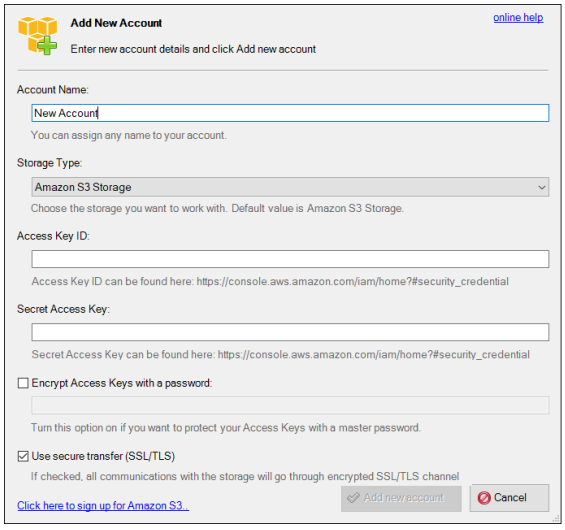
For more information on using MinIO with `s3cmd`, see https://docs.minio.io/docs/s3cmd-with-minio.html and https://s3tools.org/s3cmd.

Using S3 Browser (Windows)

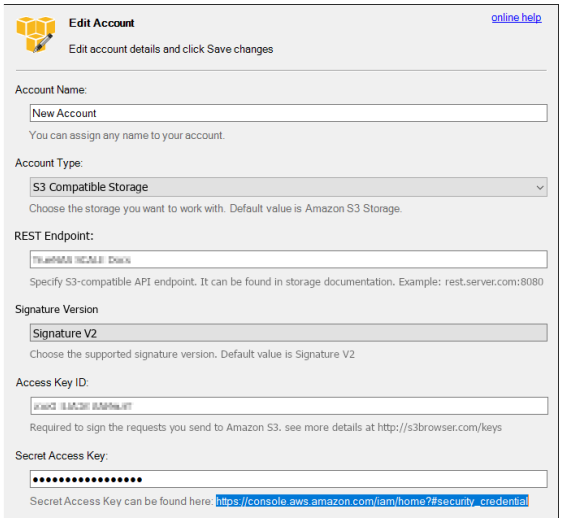
The Windows PC S3 browser is another convenient way to connect to the MinIO S3 from TrueNAS.

To set it up, first install the S3 browser.

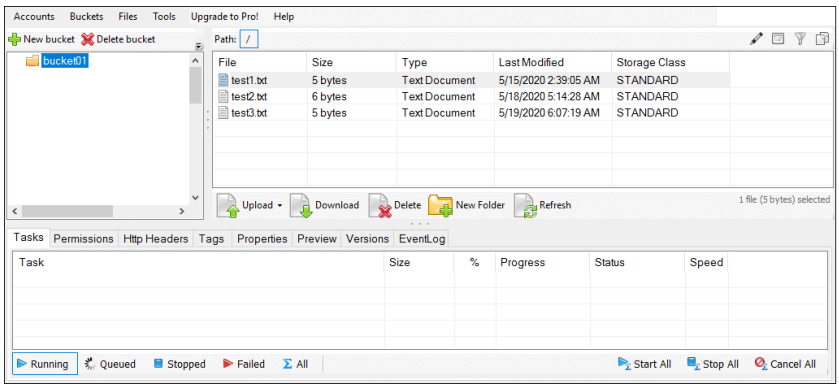
After installation completes, add a new account.



In the settings, select **S3 Compatible Storage** as the **Account Type**, then enter the MinIO access point similar to the `s3cmd` setup (TrueNAS_IP_address:9000 or other port if set differently). Select the SSL settings appropriate for the particular setup. The S3 browser assumes SSL by default, but it can be unset for a LAN attached session.



It is possible to access, create new buckets, or upload files to created buckets.



Related Content

- Adding Cloud Credentials
- Cloud Credentials Screens
- S3 Service Screen

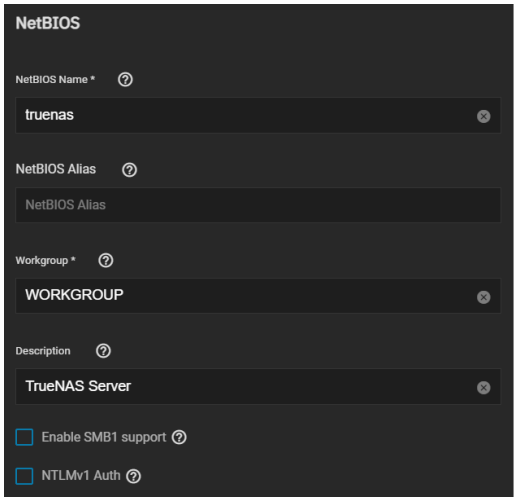
3.10.5.9 - Configuring SMB Service

This article provides instructions on configuring the SMB service in SCALE.

The **Services > SMB** screen displays after going to the **Shares** screen, finding the **Windows (SMB) Shares** section, and clicking ⋮ + **Config Service**. Alternately, you can go to **System Settings > Services** and click the ✎ edit icon for the SMB service.

Configuring SMB Service

The **SMB Services** screen displays setting options to configure TrueNAS SMB settings to fit your use case. In most cases you can set the required fields and accept the rest of the setting defaults. If you have specific needs for your uses case, click **Advanced Options**. This displays more settings



Enter the name of the TrueNAS host system if not the default displayed in **NetBIOS Name**. This name is limited to 15 characters and cannot be the **Workgroup** name.

Enter any alias name or names that do not exceed 15 characters in **NetBIOS Alias**. Separate alias names with a space between them.

Enter a name that matches the Windows workgroup name in **Workgroup**. When unconfigured and Active Directory or LDAP is active, TrueNAS detects and sets the correct workgroup from these services.

If using SMB1 clients, select **Enable SMB1 support** to allow legacy SMB1 clients to connect to the server. Note: SMB1 is being deprecated. We advise you to upgrade clients to operating system versions that support modern SMB protocol versions.

If you plan to use the insecure and vulnerable NTLMv1 encryption, select **NTLMv1 Auth** to allow smbd attempts to authenticate users. This setting allows backward compatibility with older versions of Windows, but is not recommended. Do not use on untrusted networks.

Enter any notes about the service configuration in **Description**

For more advanced setting see SMB Services Screen.

Use **Auxiliary Parameters** to enter additional smb.conf options, or to log more details when a client attempts to authenticate to the share, add `log level = 1, auth_audit:5`. Refer to the [Samba Guide]9http://www.oreilly.com/openbook/samba/book/appb_02.html) for more information on these settings.

Click **Save**.

Start the **SMB** service.

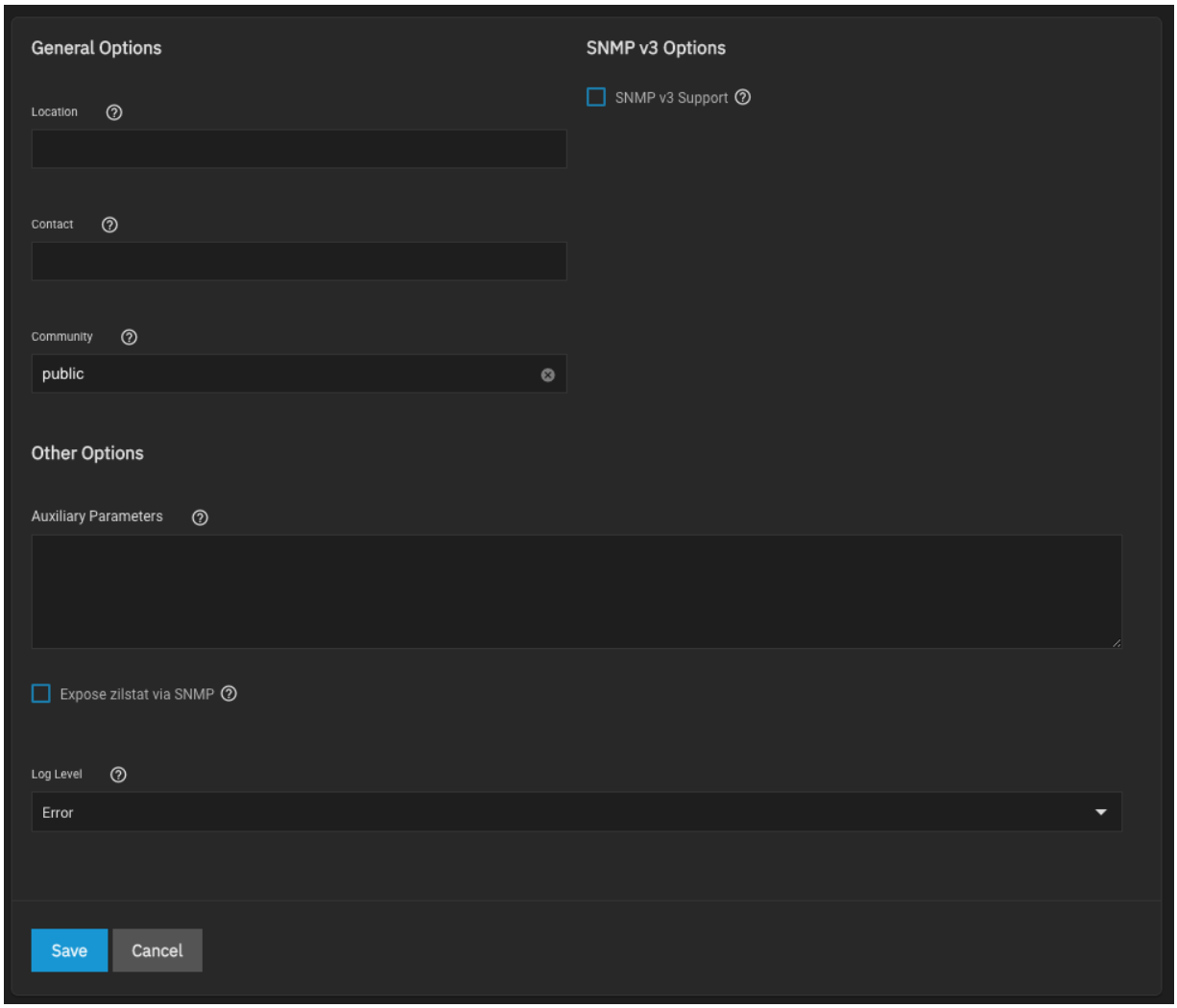
Releated SMB Articles

- Adding SMB Shares
- SMB Shares Screens
- Managing SMB Shares
- Using SMB Shadow Copy
- Setting Up SMB Home Shares
- SMB Service Screen
- Spotlight Support on a SCALE SMB Share

3.10.5.10 - Configuring SNMP Service

This article provides information on configuring SNMP service on SCALE.

SNMP (Simple Network Management Protocol) monitors network-attached devices for conditions that warrant administrative attention. TrueNAS uses Net-SNMP to provide SNMP. To configure SNMP, go to **System Settings > Services** page, find **SNMP**, and click the ✎.

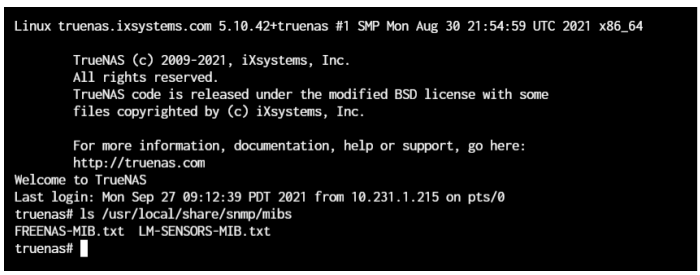


See SNMP Service Screen for setting information.

Port **UDP 161** listens for SNMP requests when starting the SNMP service.

Management Information Bases (MIBs)

Available Management Information Bases (MIBs) are located in /usr/local/share/snmp/mibs. This directory contains many files routinely added or removed from the directory. Check the directory on your system by going to **System Settings > Shell** and entering `ls /usr/local/share/snmp/mibs`. Here is a sample of the directory contents:



Related Content

- SNMP Service Screen

3.10.5.11 - Configuring SSH Service

This article provides information on configuring the SSH service in SCALE, and using an SFTP connection.

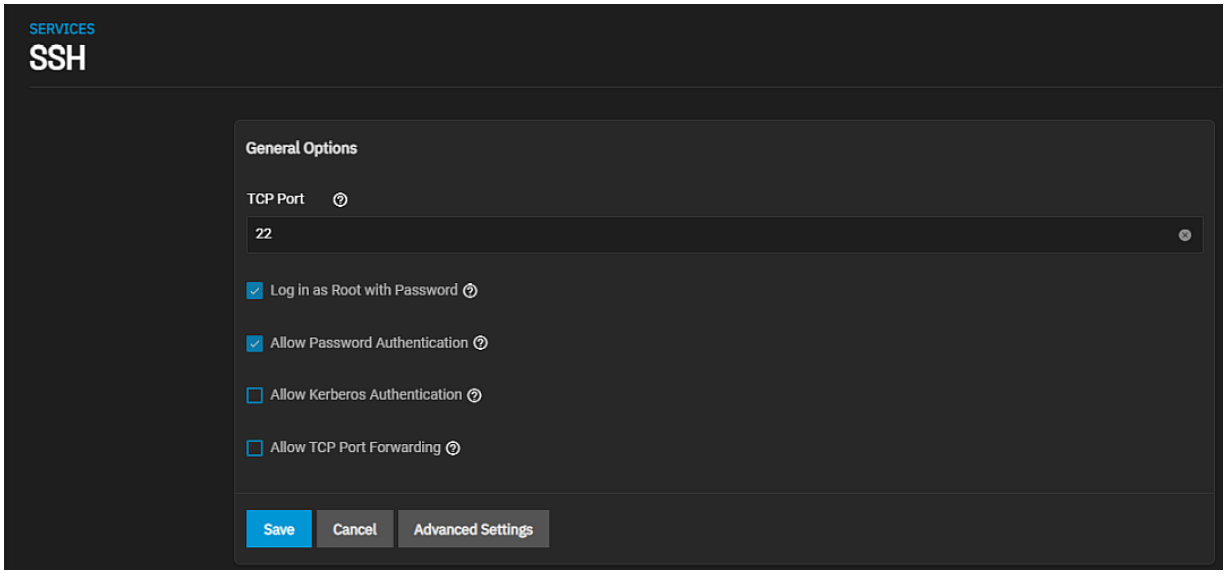
The SSH service lets users connect to TrueNAS with the Secure SHell Transport Layer Protocol. When using TrueNAS as an SSH server, the users in the network must use SSH client software to transfer files with SSH.

> Allowing external connections to TrueNAS is a security vulnerability! Do not enable SSH unless you require external connections. See Security Recommendations for more security considerations when using SSH.

SSH Tutorial Video

Configuring SSH Service

To configure SSH go to **System Settings > Services**, find **SSH**, and click to open the basic settings **General Options** configuration screen.



Configure the options as needed to match your network environment.

We recommend you add these SSH service options in **Auxiliary Parameters**:

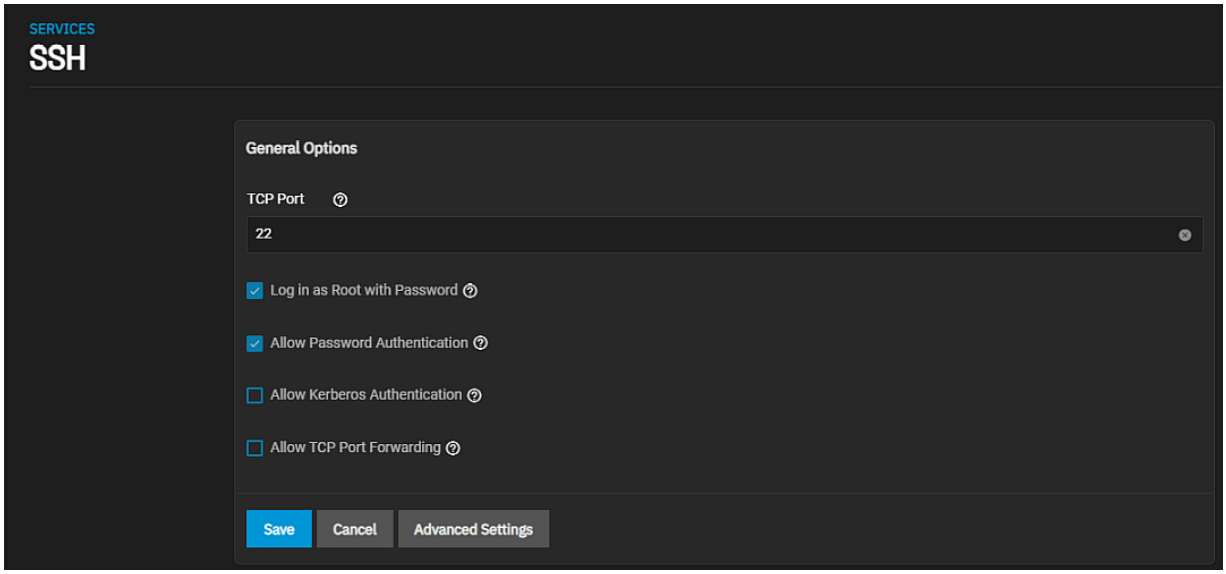
- Add `NoneEnabled no` to disable the insecure **none** cipher.
- Increase the `ClientAliveInterval` if SSH connections tend to drop.
- Increase the `ClientMaxStartup` value (**10** is default) when you need more concurrent SSH connections.

Remember to enable the SSH service in **System Settings > Services** after making changes. To create and store specific SSH connections and keypairs, go to **Credentials > Backup Credentials**.

Using SSH File Transfer Protocol (SFTP)

SFTP (SSH File Transfer Protocol) is available by enabling SSH remote access to the TrueNAS system. SFTP is more secure than standard FTP as it applies SSL encryption on all transfers by default.

Go to **System Settings > Services**, find the **SSH** entry, and click the to open the **Services > SSH** basic settings configuration screen.



Select **Allow Password Authentication** and decide if you need **Log in as Root with Password**.

> SSH with root is a security vulnerability. It allows users to fully control the NAS remotely with a terminal instead of providing SFTP transfer access.

Review the remaining options and configure them according to your environment or security needs.

Using SFTP Connections

Open an FTP client (like FileZilla) or command line. This article shows using FileZilla as an example.

Using FileZilla, enter `SFTP://{TrueNAS IP} {username} {password} {port 22}`. Where {TrueNAS IP} is the IP address for your TrueNAS system, {username} is the administrator login user name, and {password} is the adminstrator password, and {port 22} to connect.

> SFTP does not offer chroot locking. While chroot is not 100% secure, lacking chroot lets users move up to the root directory and view internal system information. If this level of access is a concern, FTP with TLS might be the more secure choice.

Related Content

- Adding SSH Credentials
- SSH Screens
- Configuring Rsync Tasks
- Rsync Tasks Screens
- Security Recommendations
- SSH Service Screen
- Using 2FA (Two-Factor Authentication)

3.10.5.12 - Configuring TFTP Services

This article provides instructions on configuring TFTP service in SCALE.

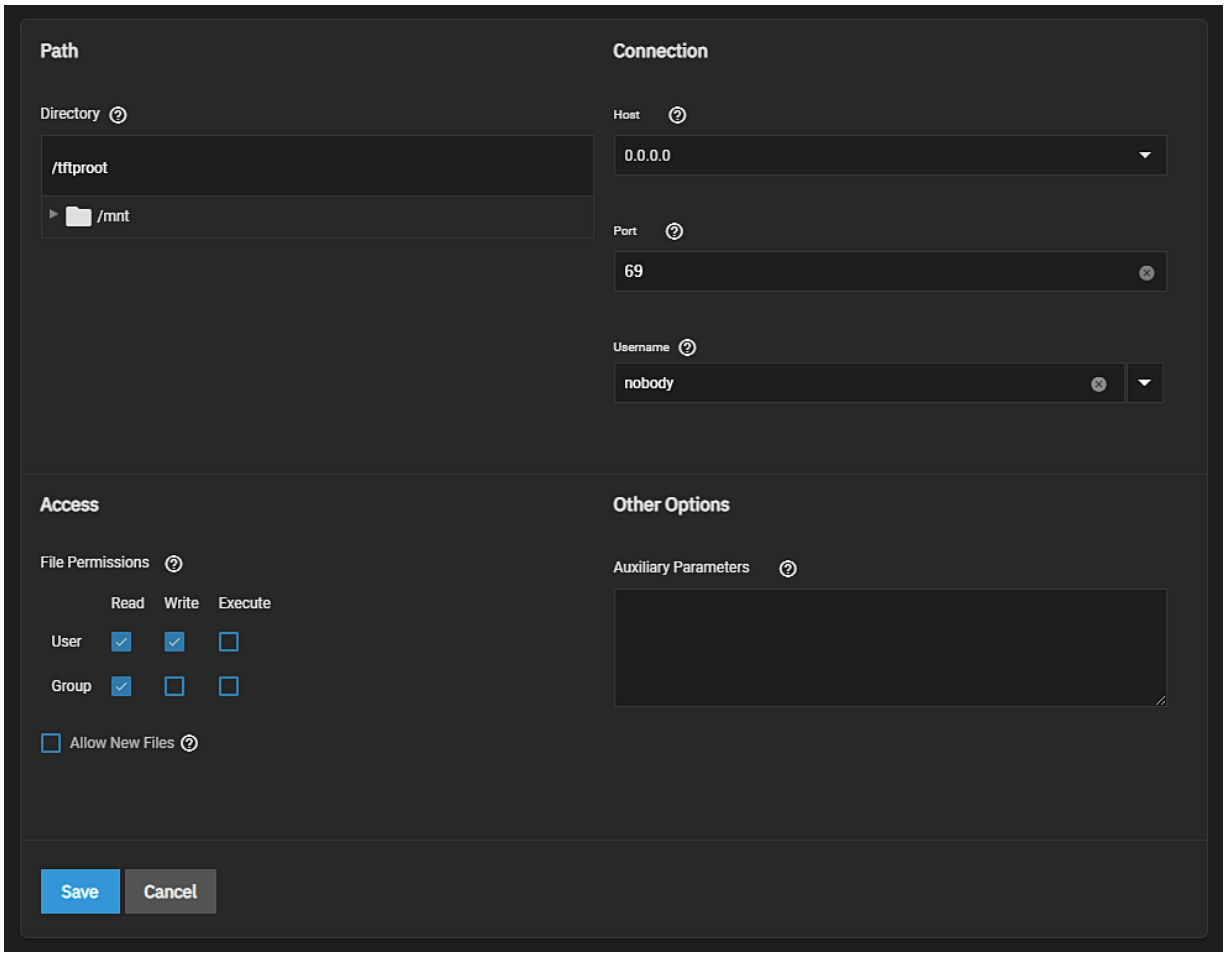
The File Transfer Protocol (FTP) is a simple option for data transfers. The SSH and Trivial FTP options provide secure or simple config file transfer methods respectively.

Options for configuring **FTP**, **SSH**, and **TFTP** are in **System Settings > Services**. Click the ✎ to configure the related service.

TFTP Service

The Trivial File Transfer Protocol (TFTP) is a lightweight version of FTP typically used to transfer configuration or boot files between machines, such as routers, in a local environment. TFTP provides a limited set of commands and provides no authentication.

If TrueNAS is only storing images and configuration files for network devices, configure and start the TFTP service. Starting the TFTP service opens UDP port **69**.



Select the path to where you want to store files, and then select the file access permissions for both user and group. If you want to allow new file transfers select **Allow new Files**.

Add the host and port connection settings and select the user that can access TFTP services.

Enter any additional TFTP settings in the **Auxiliary Parameters** field.

Click **Save** and then start the service.

Related Content

- Configuring FTP Service
- FTP Service Screen
- TFTP Services Screen

3.10.5.13 - Configuring UPS Service

This article provides information on configuring UPS service in SCALE.

TrueNAS uses Network UPS Tools NUT to provide UPS support. After connecting the TrueNAS system UPS device, configure the UPS service by going to **System settings > Services**, finding **UPS**, and clicking .

See [UPS Service Screen]({{ relref “UPSServicesScreenSCALE.md” }}) for details on the UPS service settings.

Some UPS models are unresponsive with the default polling frequency (default is two seconds). TrueNAS displays the issue in logs as a recurring error like **libusb_get_interrupt: Unknown error**. If you get an error, decrease the polling frequency by adding an entry to **Auxiliary Parameters (ups.conf)**: `pollinterval = 10`.

upsc(8) can get status variables like the current charge and input voltage from the UPS daemon. Run this in **System Settings > Shell** using the syntax `upsc ups@localhost`. The upsc(8) manual page has other usage examples.

upscmd(8) can send commands directly to the UPS, assuming the hardware supports it. Only users with administrative rights can use this command. You can create them in the **Extra Users** field.

How do I find a device name?
For USB devices, the easiest way to determine the correct device name is to set **Show console messages** in **System Settings > Advanced**. Plug in the USB device and look for a /dev/ugen or /dev/uhid device name in the console messages.

Can I attach Multiple Computers to One UPS?
A UPS with adequate capacity can power multiple computers. One computer connects to the UPS data port with a serial or USB cable. This primary system makes UPS status available on the network for other computers. The UPS powers the secondary computers, and they receive UPS status data from the primary system. See the NUT User Manual and NUT User Manual Pages.

Related Content

- SCALE Hardware Guide
- UPS Services Screen

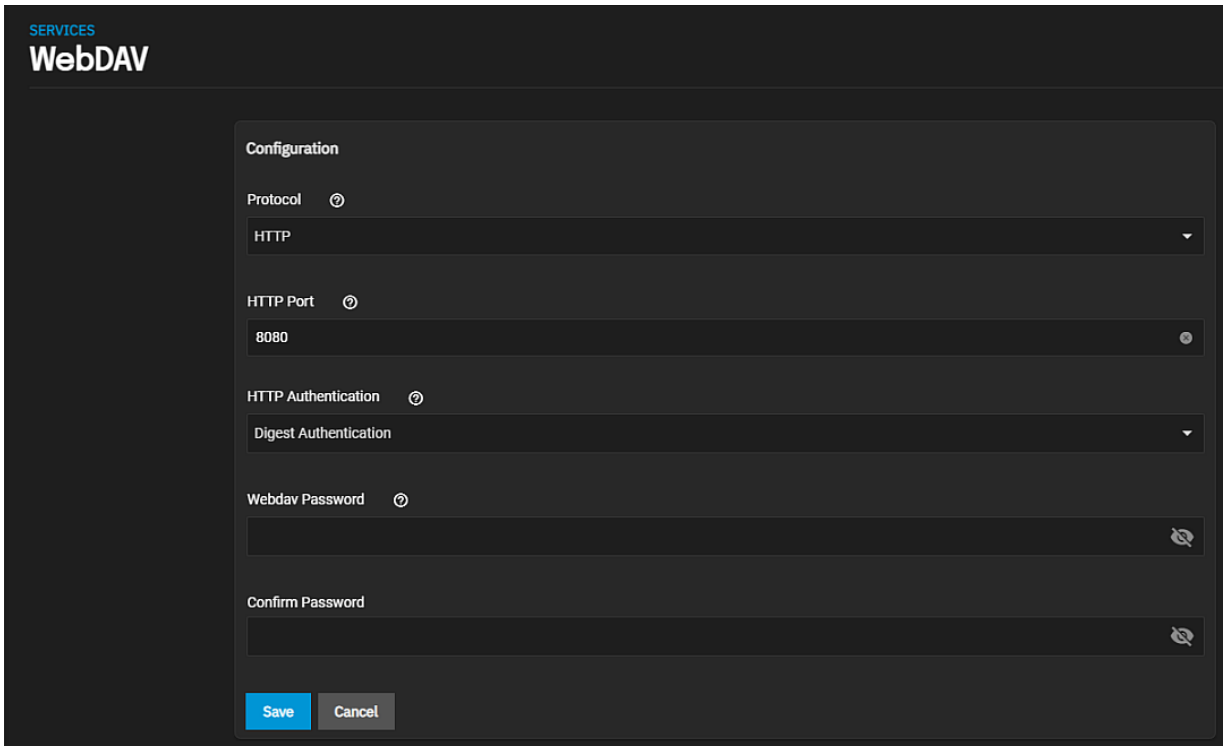
3.10.5.14 - Configuring WebDAV Service

This article provides information on configuring the WebDAV service.

The **Services > WebDAV** configuration screen displays settings to customize the TrueNAS WebDAV service.

You can access it from **System Settings > Services** screen. Locate **WebDAV** and click to open the screen, or use the **Config Service** option on the **WebDAV** widget options menu found on the main **Sharing** screen.

Select **Start Automatically** to activate the service when TrueNAS boots.



If you require it, you must choose an SSL certificate (*freenas_default* is always available). All **Protocol** options require you to define a number in the **Port** field. Make sure the network is not already using the WebDAV service port.

Select the protocol option from the **Protocol** dropdown list. For better security, select **HTTPS**.

Enter a port number for unencrypted connections in **HTTP Port**. The default **8080** is not recommended. Do not reuse a port number.

Select the authentication method from the **HTTP Authentication** dropdown list. Select **Basic Authentication** for unencrypted or **Digest Authentication** for encrypted. **No Authentication** to not use any authentication method. To prevent unauthorized access to the shared data, set the **HTTP Authentication** to either **Basic** or **Digest** and create a new **Webdav Password**.

Enter and then confirm a password but do not use the know default **davtest** password.

Click **Save**.

Start the service.

Related WebDAV Articles

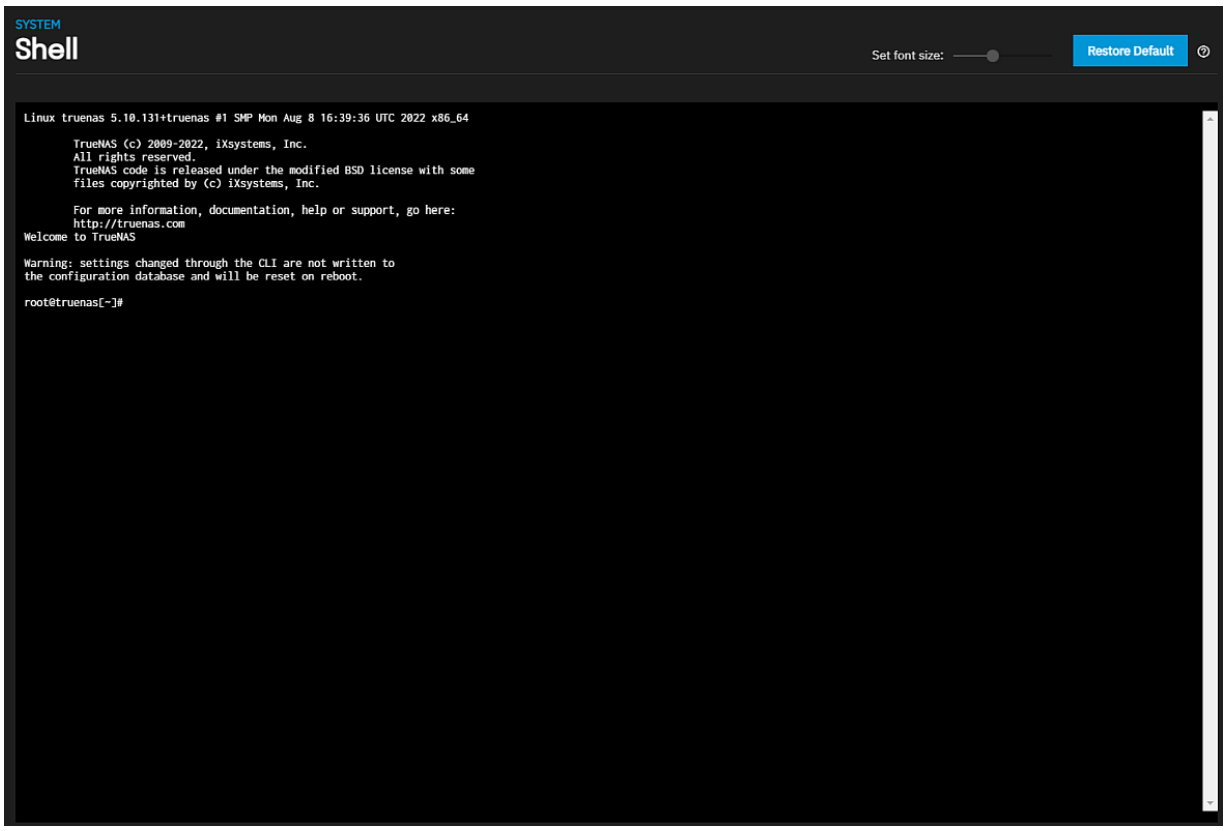
- Adding Cloud Credentials
- Cloud Credentials Screens
- Configuring WebDAV Shares
- WebDAV Shares Screens
- WebDAV Service Screen

3.10.6 - Using Shell

This article provides information on using SCALE **Shell**.

The SCALE **Shell** is convenient for running command lines tools, configuring different system settings, or finding log files and debug information. The **Shell** screen opens with the root user logged in.

> Warning! The supported mechanisms for making configuration changes are the TrueNAS WebUI, CLI, and API exclusively. All other are not supported and result in undefined behavior that can result in system failure!



The **Set font size** slider adjusts the **Shell** displayed text size. **Restore Default** resets the font size to default.

The **Shell** stores the command history for the current session.

Leaving the **Shell** screen clears the command history.

Click **Reconnect** to start a new session.

Navigating In Shell

This section provides keyboard navigation shortcuts you can uses in Shell.

Click Here for More Information

Action	Keyboard/ Command	Description
Scroll up	Up arrow ^	Scroll up through previous commands.
Scroll down	Down arrow v	Scroll down through following commands.
Re-enter command	`Enter`	After entering a command, press `Enter` to re-enter the command.
	`Home`	Moves the cursor to the top of the screen entries and results.
	`End`	Moves the cursor to the bottom of the screen command entries and results.
	`Delete`	Deletes what you highlight.

Action	Keyboard/ Command	Description
	`Tab`	Type a few letters and press `Tab` to complete a command name or filename in the current directory.
right-click		Right-clicking in the terminal window displays a reminder about using `Command+c` and `Command+v` or `Ctrl+Insert` and `Shift+Insert` for copy and paste operations.
	`exit`	Entering `exit` leaves the session.
	`Ctrl+Insert`	Enter `Ctrl+Insert` to copy highlighted text in Shell.
	`Shift+Insert`	Enter `Shift+Insert` to paste copied text in Shell.
	`Ctrl+c`	Enter `Ctrl+c` to kill a process running in Shell. For example, the `ping` command.

Changing the Default Shell

Clicking other web interface menus closes the shell session and stops commands running in the **Shell** screen.

zsh is the default **Shell**, but you can change this by editing the **root** user. Go to **Credentials > Local Users** and expand the **root** user. Click **Edit** to open the **Edit User** screen. Scroll down to **Shell** and select a different option from the dropdown list. Most Linux command-line utilities are available in the **Shell**. Click **Save**.

Tmux allows you to detach sessions in **Shell** and then reattach them later. Commands continue to run in a detached session.

Experimental CLI

The experimental SCALE command-line interface (CLI) lets you directly configure SCALE features.

> SCALE CLI is experimental and still in active development. We are not accepting bug reports or feature requests at this time.

To switch to the experimental CLI, enter `cli`.

Basic commands

Command	Description
`..`	up one level
`exit`	exit the CLI
`ls`	list the available directories and commands
`?` or `help`	list the built-in commands

The CLI features an auto-suggest mechanism for commands. When you begin typing a command, the CLI shows a list of all matching commands.

We intend the CLI to be an alternative method for configuring TrueNAS features. Because of the variety of available features and configurations, we include CLI-specific instructions in their respective UI documentation sections.

Related Content

- Shell Screen

3.11 - Using the TrueNAS CLI Shell

This article describes how to use the SCALE CLI Shell for basic networking, updating, and storage management.

The TrueNAS CLI Shell functions like a text-based version of the web UI. Users can enter commands to “navigate” to different menus within SCALE and perform actions. This article covers basic operations like setting up networking, performing updates, and listing storage pools/datasets.

Launch the TrueNAS CLI Shell

To open the TrueNAS CLI Shell, go to the Console Setup Menu and enter `6`.

To close the TrueNAS CLI Shell, enter `quit`.

Basic Networking

Interfaces

This section covers assigning an IP address to a network interface.

Enter `network interface`.

If you don’t already know the interface you want to configure, enter `query` to display a list of all physical network interfaces.

To edit the interface, enter `update interfacename aliases=["ipaddress/subnetmask"] ipv4_dhcp=false`

The CLI displays the message: “You have pending network interface changes. Please run ‘network interface commit’ to apply them.”

Enter `commit` to apply the changes, then enter `checkin` to make them permanent.

```
[truenas] network interface> update ens33 aliases=["192.168.230.129/24"] ipv4_dhcp=false
You have pending network interface changes. Please run `network interface commit`
to apply them.
[truenas] network interface> commit
<null>
Network interface changes have been applied. Please run `network interface checkin`
if the network is still operational or they will be rolled back in 51 seconds.
[truenas] network interface> checkin
<null>
[truenas] network interface>
```

Enter `query` to make sure the Truenas applies the changes successfully.

Enter `..` to exit `interface` and go up one level to the `network` menu.

Global Configuration

This section covers configuring the default gateway.

Enter `configuration` (or `network configuration` if you just opened the CLI Shell).

Enter `update ipv4gateway="ipaddress"`

If entered properly, your system networking is now configured.

Performing Manual Updates

To perform a manual update via the TrueNAS CLI Shell, you will first have to upload a manual update file onto the system.

Connect to your system with your choice of FTP program (such as WinSCP) and place the manual update file in **/var/tmp/firmware**.

Once it finishes uploading, go to the console setup menu and launch the TrueNAS CLI Shell.

Enter `system update manual path="/var/tmp/firmware/updatefilename"`

```
[truenas]> system update manual path="/var/tmp/firmware/TrueNAS-SCALE-22.02.4.update"
[50%] Reading update file...
[  771.327098] loop: module loaded
[  771.379238] squashfs: version 4.0 (2009/01/31) Phillip Lougher
[50%] Verifying rootfs.squashfs...
[50%] Verifying truenas_install/__main__.py...
[50%] Verifying truenas_install/__init__.py...
[50%] Creating dataset...
[50%] Extracting...
[51%] Extracting...
[56%] Extracting...
[71%] Extracting...
[72%] Extracting...
[73%] Extracting...
[78%] Extracting...
[95%] Extracting...
[95%] Performing post-install tasks...
[95%] Cleaning up...
[100%] Cleaning up...
<null>
```

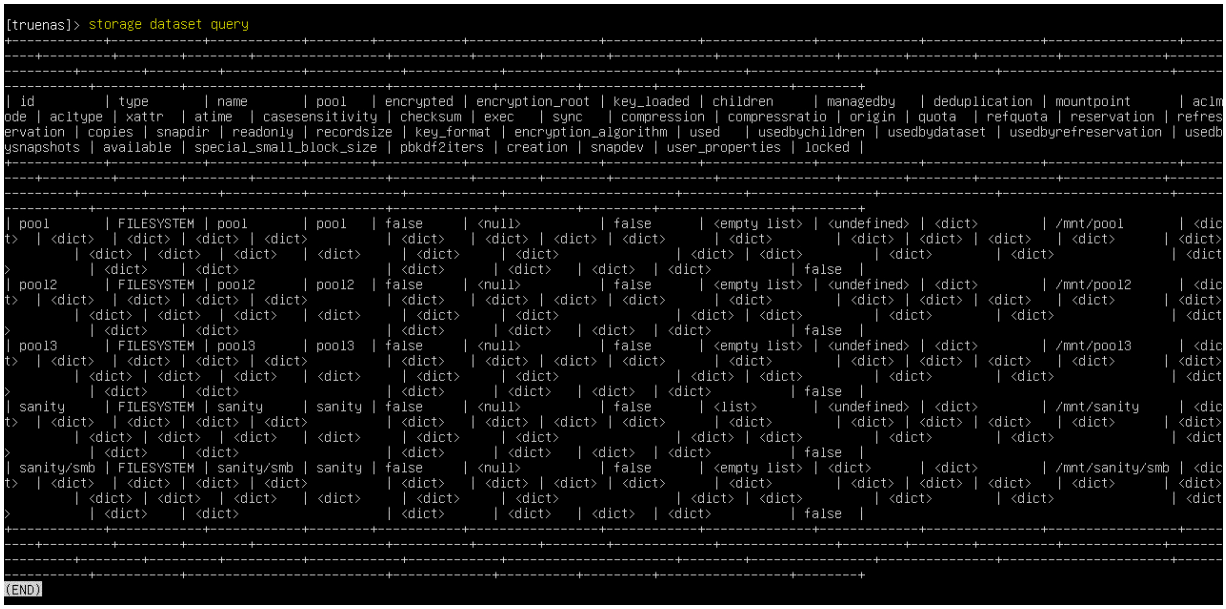
Listing Storage Pools and Datasets

To list all configured storage pools, enter `storage pool query`.

```
[truenas]> storage pool query
+----+-------+------------------+--------+-----------+------------+-------+-------+----------+---------+---------+---------------+-------------+-------------+
| id | name  | guid             | encrypt | encryptkey | path       | status | scan  | topology | healthy | warning | status_detail | size        | allocated | free        | freeing | fragmentation | size_str    | allocated_str | free_str    | freeing_str | autotrim | encryptkey_path | is_decrypted |
+----+-------+------------------+--------+-----------+------------+-------+-------+----------+---------+---------+---------------+-------------+-------------+
| 1  | sanity | 4612590513058318053 | 0      |           | /mnt/sanity | ONLINE | <dict> | <dict>   | true    | false   | <null>        | 996432412672 | 854657436 | 987885838336 | 0       | 0             | 996432412672 | 8546574336  | 987885838336 | 0           | <dict>   | <null>          | true         |
| 2  | pool  | 8377915652589342099 | 0      |           | /mnt/pool  | ONLINE | <dict> | <dict>   | true    | false   | <null>        | 996432412672 | 552960    | 996431859712 | 0       | 0             | 996432412672 | 552960      | 996431859712 | 0           | <dict>   | <null>          | true         |
| 3  | pool2 | 627576972228238739 | 0      |           | /mnt/pool2 | ONLINE | <dict> | <dict>   | true    | false   | <null>        | 996432412672 | 540672    | 996431872000 | 0       | 0             | 996432412672 | 540672      | 996431872000 | 0           | <dict>   | <null>          | true         |
| 4  | pool3 | 6548424125891600913 | 0      |           | /mnt/pool3 | ONLINE | <dict> | <dict>   | true    | false   | <null>        | 996432412672 | 565248    | 996431847424 | 0       | 0             | 996432412672 | 565248      | 996431847424 | 0           | <dict>   | <null>          | true         |
+----+-------+------------------+--------+-----------+------------+-------+-------+----------+---------+---------+---------------+-------------+-------------+
(END)
```

Enter `q` to exit the query.

To list all configured datasets, enter `storage dataset query`.



Enter q to exit the query.

3.12 - Community Tutorials

Because TrueNAS is both Open Source and complicated, the massive user community often creates tutorials for very specific hardware or use cases. User-created tutorials are available in this location, but be aware these are provided “as-is” and are not officially supported by iXsystems, Inc.

Article Summaries

- Hardened Backup Repository for Veeam

  Abstract This guide explains in details how to create a Hardened Backup Repository for VeeamBackup with TrueNAS Scale that means a repository that will survive to any remote attack. The main idea of this guide is the disabling of the webUI with an inititialisation script and a cron job to prevent remote deletion of the ZFS snapshots that guarantee data immutability. The key points are: Rely on ZFS snapshots to guarantee data immutability Reduce the surface of attack to the minimum When the setup is finished, disable all remote management interfaces Remote deletion of snapshots is impossible even if all the credentials are stolen.

- Spotlight Support on a SCALE SMB Share

  This article describes how to configure a SCALE SMB (Samba) share to support the Spotlight search API

3.12.1 - Hardened Backup Repository for Veeam

Abstract

This guide explains in details how to create **a Hardened Backup Repository** for VeeamBackup with **TrueNAS Scale** that means a repository that will survive to **any remote attack**.

The main idea of this guide is **the disabling of the webUI** with an inititialisation script and a cron job **to prevent remote deletion of the ZFS snapshots** that guarantee data immutability.

The key points are:

- Rely on ZFS snapshots to **guarantee data immutability**
- Reduce the surface of attack to the minimum
- When the setup is finished, disable **all remote management interfaces**
- Remote deletion of snapshots is impossible **even if all the credentials are stolen**.
- The only way to delete the snapshot is having **physically access to the TrueNAS Server Console**.

> This article targets specifically *TrueNAS Scale* and *Veeam Backup*, but it may also apply to some extent to TrueNAS Core and/or other backup software.

Installation

Install *TrueNAS Scale 22.02* on a **physical** machine.

- If possible the computer should have at least 2 network interfaces:
  - one dedicated network interface for the management
  - the other one for the data sharing

> A *virtualized* TrueNAS server is not suitable for a hardened backup repository because a malware can easily take the control of TrueNAS server and destroy its data after compromising the hypervisor.

Create a ZFS pool

Go to *Storage* | *Create Pool*

- *Name*: **tank1**

  > Even if you can use any pool name, the guide is easier to follow if you use **tank1** as pool name.

- Click on *SUGGEST LAYOUT* to let TrueNAS guessing the best layout for you. In most situations, it will just work very well.
- Review the proposed layout, then click on *CREATE*

  > For a backup repository, the following layouts will provide a good balance between IOPS, available space and level of redundancy:
  >
  > - 2 to 4 disks: Stripe of mirrors
  > - 6 disks: RaidZ2
  > - 8 to 11 disks: RaidZ3
  > - 12 disks and more: Stripe of Raidz2/Raidz3

Configure SMART Tests

> SMART (*Self-Monitoring, Analysis and Reporting Technology*) is a monitoring system included in hard disk drives to anticipate imminent hardware failures.

Go to *Data Protection* | *S.M.A.R.T Test* | *Add*

- All Disks
- *Type*: **LONG**
- *Description*: **Long SMART test**
- *Schedule*: **Monthly (0 0 1 * *) on the first day of the month at 00:00 (12:00 AM)**
- *SAVE*

Configure the network

> For a hardened repository, it is better to use a **fixed IP address** than a DHCP configuration, because a compromised DHCP server can provide malicious DNS settings.

Global Network Configuration

Go to *Network* | *Global Configuration*

- *Hostname and Domain*
  - Configure **Hostname** and **Domain**
- *Service Annoucement*
  - NetBIOS-NS
  - mDNS
  - WS-Discovery

> For a hardened repository it is preferable to disable any service annoucement

- *DNS Servers*
  - *Nameserver 1*: **1.1.1.1**
  - *Nameserver 2*: **8.8.8.8**

    > For a hardened server, it is preferable to use the IP addresses of very well known and secure public DNS than your own internal DNS server.
    >
    > - Cloudflare: 1.1.1.1
    > - Google: 8.8.8.8

- *Default Gateway*
  - Setup *IPv4 (or IPv6) Default Gateway* according to your network
- *Outbound Network*
  - **(o) Allow Specific**
    - Enable **Mail** and **Update**
- Other Settings
  - *HTTP Proxy*: stay empty

    > Connecting to Internet through a proxy is a good security practice because it prevents malwares to communicate easily with their control and command servers, but it is out of the scope of this guide.

- *SAVE*

Network Interfaces Configuration

Go to *Network* | *Interfaces*

- Click on the first interface and configure it as the management interface
  - Management interface
    - *Description*: **management**
    - DHCP
    - Autoconfigure IPv6
    - *Other Settings*
      - Disable Hardware Offloading
      - *MTU*: **1500**

        > For a hardened repository, it is preferable to keep the default value (1500) for the MTU, because using jumbo frame makes the network configuration more complex to manage.

      - *IP Addresses*
        - Add the IP address of the management interface
    - *APPLY*
    - *TEST CHANGES*

      > When you are testing the new network settings, you have 60 seconds to confirm that it works by clicking on *SAVE CHANGES*, otherwise the system automatically rolls back to the previous network configuration to avoid kicking you out of the network.

  - Data interface
    - Management interface
      - *Description*: **data sharing**
      - DHCP
      - Autoconfigure IPv6
      - *Other Settings*
        - Disable Hardware Offloading
        - *MTU*: **1500**
        - *IP Addresses*
          - Add the IP address of the data sharing interface

- *APPLY*
- *TEST CHANGES*
- *SAVE CHANGES*

Configure the user accounts

Setup root account

Go to *Credentials* | *Local Users*

- Edit the *root* user
  - Fill the *Email* field

    > System notification are sent by email to the **root** user, so this email address is very important.

  - If you wish to use SSH for management, fill also *SSH Public Key*

> SSH is more convenient than the web shell interface to enter commands that are missing from the web user interface.

Create a account for Veeam

Go to *Credentials* | *Local Groups* | *Add*

- *GID*: **10000**
- *Name*: **veeam**
- Permit Sudo
- Samba Authentication
- Allow Duplicated GIDs
- *SAVE*

Go to *Credentials* | *Local Users* | *Add*

- *Full Name*: **Veeam Backup**
- *Username*: **veeam**
- *Password*: **use a very long and strong password**
- *Password confirmation*:
- *Email*: stay empty
- *User ID and Groups*
  - *User ID*: **10000**
  - New Primary Group
  - *Primary Group*: **veeam**
  - *Auxiliary group*: stay empty
- *Directories and Permissions*
  - *Home Directory*: **/nonexistent**
  - *Home Directory Permission*: **clear all permissions, except user permissions**
  - *SSH Public Key*: stay empty
  - *Disable password*: **no**
  - *Shell*: **nologin**
  - Lock User
  - Permit Sudo
  - Microsoft Account
  - Samba Authentication
- *SAVE*

Configure SSH

Go to *System Settings* | *Services* | *SSH* and click on the pencil (✎)

- Click **ADVANCED SETTINGS**
  - *TCP Port*: **22**
  - Log in As Root with Password
  - Allow Password Authentication
  - Allow Kerberos Authentication
  - Allow TCP Port Forwarding
  - *Bind Interfaces*: **use the management network interface**
  - Compress Connections
  - SFTP Log Level: stay blank
  - SFTP Log Facility: stay blank
  - Weak Ciphers: **None, AES128-CBC**
  - Auxiliary Parameters: **AllowUsers root@192.168.0.10**
    - where 192.168.0.10 is the IP address of your desktop computer you use to manage the TrueNAS server.
- *SAVE*
- Toggle the running button to start the SSH service **but do not start automatically SSH**

> Do not start automatically SSH because we will disable the SSH service later to harden the repository.

Configure the mail notification

> Configuring the mail notification is very important, because it will be the only way to know that happens (for example if a disk is dying) after disabling the web management interface to harden the repository.

Edit mail notification

- Click on the **bell** 🔔 icon on the top right corner
- Click on the **gear** ⚙ icon
- Select **Email**
- Fill the web form according to your email provider
- *Send Test Mail*
- Check that you receive the testing email
- *SAVE*

Create a dataset for Veeam

Go to *System Settings* | *Shell* (or connect with SSH)

```
zfs create tank1/veeam
zfs set org.freenas:description="veeam hardened repo" tank1/veeam
zfs set compression=off tank1/veeam
chown veeam:veeam /mnt/tank1/veeam
chmod 700 /mnt/tank1/veeam
```

> Description of shell commands
>
> 1. Create a dataset name **tank1/veeam**
> 2. Set dataset description (“veeam hardened repo”)
> 3. Set compression level to **off** because Veeam backup are already compressed
> 4. Set ownership of user **veeam** and group **veeam** on directory **/mnt/tank1/veeam**
> 5. Set restrictive user permissions on **/mnt/tank1/veeam**

If you really following this guide from scratch, then the dataset **tank1/veeam** is empty, then you can create an **empty snapshot** and **lock it** to prevent deleting by mistake the dataset from the web user interface or with the command `zfs destroy`

```
zfs snap tank1/veeam@LOCKED
zfs hold LOCKED tank1/veeam@LOCKED
```

> Description of shell commands
>
> 1. Create a snapshot named **LOCKED** on **tank1/veeam**.
> 2. Hold a lock named **LOCKED** on the snapshot. Indeed the name of the snapshot and the name of the lock can be different, but it is easier to use twice the same name.

> More information about ZFS locked snapshot
>
> - To lock a snapshot use `zfs hold LOCK_NAME SNAPSHOT_NAME`
> - Snapshot can have multiple locks, each lock must have a different name
> - A locked snapshot cannot be deleted
> - To unlock a snapshot, use `zfs release LOCK_NAME SNAPSHOT_NAME`
> - To list the lock names of a particular snapshot, use `zfs holds SNAPSHOT_NAME`
> - A dataset with a locked snapshot cannot be deleted neither with the webui nor with the `zfs destroy` command, so it avoid human errors.

Configure ZFS periodic snapshots

Create 3 periodic (hourly, daily and weekly) ZFS snapshots to recover the data if they are deleted or modified.

Hourly snapshots

Go to **Data Protection | Periodic Snapshot Tasks**

- *Dataset* **tank1**
- *Exclude*: stay empty

- Recursive
- *Snapshot lifetime*: **1 day**
- *Naming Schema*: **auto-%Y%m%d_%H%M-hourly**
- *Schedule*: **Hourly (0 * * * *) at the start of each hour**
- *Begin*: **00:00:00**
- *End*: **23:59:00**
- Allow Taking Empty Snapshots
- Enabled
- *SAVE*

> It is easier to setup the periodic snapshot at the root dataset and to enable *recursive* snapshot.

Daily snapshots

Go to **Data Protection | Periodic Snapshot Tasks**

- *Dataset* **tank1**
- *Exclude*: stay empty
- Recursive
- *Snapshot lifetime*: **1 week**
- *Naming Schema*: **auto-%Y%m%d_%H%M-daily**
- *Schedule*: **Daily (0 0 * * *) at 00:00 (12:00 AM)**
- Allow Taking Empty Snapshots
- Enabled
- *SAVE*

Weekly snapshots

Go to **Data Protection | Periodic Snapshot Tasks**

- *Dataset* **tank1**
- *Exclude*: stay empty
- Recursive
- *Snapshot lifetime*: **1 month**
- *Naming Schema*: **auto-%Y%m%d_%H%M-weekly**
- *Schedule*: **Weekly (0 0 * * sun) on Sundays at 00:00 (12:00 AM)**
- Allow Taking Empty Snapshots
- Enabled
- *SAVE*

> If you have enough disk space, you can use longer retention time. The longer the snapshot are kept, the better your safety is.

Configure Samba Service

Go to *System Settings* | *Services* | *SMB* and click on the pencil (✎)

- Click **ADVANCED SETTINGS**
  - *NetBIOS Name*: **strongbox** (you can use any name here)
  - *NetBIOS Alias*: stay empty
  - *Workgroup*: **WORKGROUP**
  - *Description*: **Hardened TrueNAS**
  - Enable SMB1 support
  - NTLMv1 Auth
  - *UNIX Charset*: **UTF-8**
  - *Log Level*: **Minimum**
  - Use Syslog Only
  - Local Master
  - Enable Apple SMB2/3 Protocol Extensions
  - *Administrators Group*: stay empty
  - *Guest Account*: **nobody**
  - *File Mask*: **0600**
  - *Directory Mask*: **0700**
  - *Bind IP Address*: bind on the IP address of the data network interface
  - *Auxiliary Parameters*: stay empty
  - *SAVE*
- Toggle the running button to start the SMB service
- Start Automatically SMB

Configure Samba share for Veeam

Go to *Shares* | *Windows (SMB) Shares* | *ADD*

- Click on **ADVANCED OPTIONS**
  - *Basic*
    - *Path*: **/mnt/tank1/veeam**

        - *Name*: veeam
        - *Purpose*: **Multi-protocol (NFSv3/SMB) shares**
        - *Description*: **hardened veeam repository**
        - Enabled
    - *Access*
        - Enable ACL
        - Export Read Only
        - Browseable to Network client
        - Allow guest access
        - Allow based shared enumeration
        - *Host Allow*: *put the IP of the Veeam Software server here*
        - *Host Deny*: stay empty
    - *Other Options*
        - Use as home share
        - Timemachine
        - Legacy AFP compatibility
        - Enable shadow copy
        - Export Recycle bin
        - Use Apple-Style Character Encoding
        - Enable alternate data streams
        - Enable SMB2/3 Durable handles
        - Enable FSRVP
        - *Path suffix*: **stay empty, very important**
        - *Auxiliary parameters:* stay empty
    - *SAVE*

Add this repository to Veeam Software

See the documentation of Veeam Backup to add this SAMBA share as a backup target.

In the Veeam wizard select

- **Network attached storage**
- **SMB Share**
- For the credentials, use the veeam account creates on the hardened backup resporitory (see above)

Hardened the repository

To hardened the backup repository, just remove any possibility to remotely destroy the ZFS snapshots.

Enable password for console access

Go to *System Settings* | *Advanced* | *Console* | *Configure*

- Show Text Conosle wihout Password Prompt
- *SAVE*

Disconnect IPMI

If your server has a IPMI interface, **physically disconnect the network cable**.

> - If a malware takes the control of your management computer, it can use the IPMI interface to destroy your backups.
> - Be cautious and just disconnect the cable.

Check that NTP works as expected

- Go to *System Settings* | *General* | *NTP Servers*

By default TrueNAS Scale comes with the following NTP servers

- 0.debian.pool.ntp.org
- 1.debian.pool.ntp.org
- 2.debian.pool.ntp.org

Open a shell

- Go to *System Settings* | *Shell*
- Enter the command `ntpq -p`
- The output will look like

```
# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*ntppub.darksky. 172.18.1.20      2 u  326 1024  377   11.447   +0.475   0.531
+ip139.ip-5-196- 145.238.203.14   2 u  208 1024  377   11.484   -0.249   0.279
+ns2.euskill.com 193.107.56.120   4 u   33 1024  377   22.541   +0.167   0.538
```

> Do not worry if you have different remote hostnames or IP addresses for NTP servers, it is normal because domain names of **ntp.org** point to a pool of servers.

Configure HTTPS

Create an Internal Certificat Authority

Go to *Credentials* | *Certificates* | *Certificates Authorities* | *Add*

- *Identifier and Type*
  - *Name*: **hardened-truenas-scale-ca**
  - *Type*: **Internal CA**
  - *Profiles*: **CA**
- *Certificate Options*
  - *Key Type*: **RSA**
  - *Key Length*: **4096**
  - *Digest Algorithm*: **SHA512**
  - *Lifetime*: **3650**
- *Certificate Subject*
  - *Country*: **United States**
  - *State*: **California**
  - *Locality*: **San Francisco**
  - *Organization*: **The Name of My Company**
  - *Organization Unit*: **Backup Department**
  - *Email*: **firstname.surname@the-name-of-my-company.com**
  - *Common Name*: **hardened-truenas-scale-ca**
  - *Subject Alternate Names*: **hardened-truenas-scale-ca**
- *Extra Constraints*
  - Basic Constraints
  - Authority Key Identifier
  - Extended Key Usage
  - Key Usage
- *Confirm Options*
  - *SAVE*

Create a certificate for HTTPS

Go to *Credentials* | *Certificates* | *Certificates* | *Add*

- *Identifier and Type*
  - *Name*: **hardened-truenas-scale-cert**
  - *Type*: **Internal Certificate**
  - *Profiles*: **———**
- *Certificate Options*
  - *Signing Certificate Authority*: **hardened-truenas-scale-ca**
  - *Key Type*: **RSA**
  - *Key Length*: **4096**
  - *Digest Algorithm*: **SHA512**
  - *Lifetime*: **3650** (10 years)
- *Certificate Subject*
  - *Country*: **United States**
  - *State*: **California**
  - *Locality*: **San Francisco**
  - *Organization*: **The Name of My Company**
  - *Organization Unit*: **Backup Department**
  - *Email*: **firstname.surname@the-name-of-my-company.com**
  - *Common Name*: **hardened.mydomainname.com** (the full qualified domain name)
  - *Subject Alternate Names*: **hardened.mydomainname.com** (the full qualified domain name)
- *Extra Constraints*
  - Basic Constraints
  - Authority Key Identifier
  - Extended Key Usage
  - Key Usage
- *Confirm Options*
  - *SAVE*

Apply the new HTTPS certificate

Go to *System Settings* | *General* | *GUI* | *Settings*

- *GUI*
  - *GUI SSL Certificate* : **hardened-truenas-scale-cert**
  - *Web Interface IPv4 Address*: **select the management interface**
  - *Web Interface IPv6 Address*: **::**
  - *Web Interface HTTP Port*: **80**
  - *Web Interface HTTPS Port*: **443**
  - *HTTPS Protocols*: **TLSv1.3**
  - Web Interface HTTP -> HTTPS Redirect

- *Other Options*
  - Crash reporting
  - Usage collection
  - Show Console Messages
- *SAVE*

Restart Web Service: *CONFIRM*, *CONTINUE*

Enable Two-Factor Authentication (2FA)

> Two-Factor Authentication is time-based, and requires that the system time is set correctly, so check before that NTP works.

- Install an application on your smartphone to generate an One-Time-Password from a QR-Code. For example FreeOTP Authenticator
- Go to *Credentials* | *2FA*
- Keep the default
  - *One-Time Password (OTP) Digits*: 6
  - *Interval*: 30
  - *Window*: 0
  - Enable Two-Factor Auth for SSH
- Click on *Enable Two-Factor Authentication*
- *SHOW QR*
- Use *FreeOTP* to capture the QR code
- Log out the web interface
- Test Two-Factor Authentication
- If something goes wrong you can disable the 2FA from the console

```
midclt call auth.twofactor.update '{"enabled": false}'
```

Disable SSH for normal operations

> Letting SSH service running is dangerous: if someone steals your SSH private key and passphrase, he can remotely connect to the backup repository and destroy the data.

Check SSH does not automatically start

Go to *System Settings* | *Services*

- Check that SSH does not start automatically

Stop SSH service on boot

Add a startup script to stop the SSH service in case it has been enabled by mistake

Go to *System Settings* | *Advanced* | *Init/Shutdown Scripts* | *Add*

- *Description*: **Stop SSH at startup**
- *Type*: **Command**
- *Command*: **/usr/bin/systemctl stop ssh**
- *When*: **Post Init**
- Enabled
- *Timeout*: **10**
- *SAVE*

Stop SSH service at midnight

To avoid the SSH service stays enabled forever, stop it automatically at midnight

Go to *System Settings* | *Advanded* | *Cron Job* | *Add*

- *Description*: **stop ssh at midnight**
- *Command*: **/usr/bin/systemctl stop ssh**
- *Run as user*: **root**
- *Schedule*: **daily (0 0 * *) at 00:00 (12:AM)*
- hide standard output
- hide standard error
- Enabled
- SAVE

Disable Web User Interface for normal operations

Stop WebUI on boot

Go to *System Settings* | *Advanced* | *Init/Shutdown Scripts* | *Add*

- *Description*: **Stop webUI at startup**
- *Type*: **Command**
- *Command*: **/usr/bin/systemctl stop nginx**
- *When*: **Post Init**
- Enabled
- *Timeout*: **10**
- *SAVE*

Stop WebUI at midnight

To avoid the WebUI stays enabled forever, stop it automatically at midnight

Go to *System Settings* | *Advanded* | *Cron Job* | *Add*

- *Description*: **stop webUI at midnight**
- *Command*: **/usr/bin/systemctl stop nginx**
- *Run as user*: **root**
- *Schedule*: **daily (0 0 * *) at 00:00 (12:AM)*
- hide standard output
- hide standard error
- Enabled
- SAVE

Change the message of the day

Go to *System Settings* | *Advanced* | *Console* | *Configure*

- MOTD Banner: **Hardened repository without remote management, to enable temporary the web interface type "systemctl start nginx"**
- *SAVE*

Backup the server configuration

Go to *System Settings* | *General* | *Manage Configuration*

- *DOWNLOAD FILE*

Test the setup

Reboot the server to check that the web interface is disabled when the computer boots

Daily management

You can temporary enable the web interface to change the configuration

Enable the web interface

Connect to the console and type:

```
systemctl start nginx
```

> If you forgot to stop the webUI when you have finished your work, the cron job will do if for you at midnight

Disable the web interface

To immediately disable the web interface connect to the console and type:

```
systemctl stop nginx
```

Recover data after an attack

If your Veeam backup files have been altered it means that the password to access the SAMBA share has been compromised, so you have to change it immediately.

Change the password for the veeam account

Go to *Credentials* | *Local Users* | *veeam*

- Unroll the options, click **EDIT**
- Change *Password*
- *SAVE*

Lock the snapshot to preserve the data

It may take few day to audit your system after an attack, therefore it is a good idea to lock all snapshots to avoid they are automatically deleted when they reached their end of life.

Run the following command in the shell

```
for s in `zfs list -r -t snap -H -o name tank1/veeam`; do zfs hold LOCKED $s ; done
```

Clone the healthy snapshot

Go to *Storage* | *Snapshots*

- Pick the healthy snapshot
- Unroll the option
- Click *CLONE TO NEW DATASET*
  - *Name*: **tank1/veeam-snap-clone**
  - **SAVE**

Create a new Samba Share to export the cloned dataset

- Use the above instruction to share **tank1/veeam-snap-clone** with SAMBA.
- Reinstall Veeam on a new server
- Connect to the new SAMBA share
- Restore your data.

> - The guide for a hardened repository is finished
> - Enjoy your hardened repository, and sleep more peacefully at night.

3.12.2 - Spotlight Support on a SCALE SMB Share

This article describes how to configure a SCALE SMB (Samba) share to support the Spotlight search API

This is a fast spun up tutorial to demonstrate how to have a Samba share on TrueNAS SCALE (in short: TNS) supporting macOS' Spotlight search API. My goal was to have my scans saved inside a network folder being indexed and spotlight enabled. So I write this tutorial for my "scans" share. For having this to work we will install an ElasticSearch engine, a script called fscrawler and tesseract libraries and will also show you how you could configure each part of the toolchain to make this work. We will heavily rely on docker images, as I don't want to spin up an extra VM within my VM ;)

ElasticSearch

or in short within this tutorial only "ES" (Elastic LINK) is an engine that enables you to process searches in an "elastic" way. That means after querying it the search hits will be returned immediately and not after the search was completed. So results will shown may increase after some time, depending on the database ES utilizes. We will use ES 8.4.3 with our docker image

FS Crawler

is the script that builds the index in the ES database. It can be optimized to index specific values of your files and folders, according to your needs. For example if you prefer to search for titles it may be better for you to not have a fulltext search enabled. Someone else likes to keep an eye only on the size of the files and wants to search for file and folder size only. If you need more details, feel free to dive deeper into this topic with the fscrawler documentation (FS Crawler LINK). We will use FS Crawler 2.10-SNAPSHOT.

FS Crawler alternative: fs2es-indexer

Tesserract

is an ocr engine. ocr is the abbreviation for "optical character recognition". fscrawler can be configured to hand over picture and pdf files to an ocr engine to have it searching for characters. This enables fscrawler not only to build an index of filenames and metadata but also for written content within binary files. Because ocr works with an engine that compares objects found in an image, for example, with existing similar objects from installed fonts, it needs a lot of space for its Docker image.

optional: kibana

is a tool to manually query ES via webUI.

fancy bread crumbs

If I use the stylish symbols "-" and ">" in combination "->" it means I want you to click on something, enter some text or change a value or entry somewhere.

Prerequisites

As this tutorial will not cover the basic installation of a TNS I assume you have

1. TNS already running
2. at least one storage pool
3. already configured a place for additional Apps

let's get it on

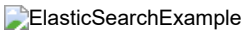
Install ES

Now, to get our hands dirty, we install ES as a docker image. Sadly neither TreuNAS SCALE offical repo nor the elastic one provides a docker we can use. So I googled all night and found this beautiful blog (Heavy Setup LINK). To sum up what we need

do: -> Add a new catalog (TrueCHARTS, https://github.com/truecharts/charts.git) -> leave everything on default and -> save. Now you could grab yourself a cup of coffee as this process takes some time (it took about half an hour with my setup).

After the charts (i.e. Community Apps) are indexed, you will find A LOT of additional apps ready to install. But not our most wanted one.

-> So get to the catalog view again -> go to the settings of the new imported catalog and edit it -> select “Incubator” -> switch to apps -> search for “tubearchivist-es” -> install it! (you may follow the instructions from the blog linked above (Heavy Setup LINK)) If you now click on open you should be asked for user:password (elastic:verysecret) and then get the presented something similar to this:


ElasticSearchExample

You might change the user name and password (elastic:verysecret), you find the how to here (LINK)

install FS Crawler (and OCR)

Luckily there is a docker image that already combines fscrawler and ocr:

`dadoonet/fscrawler`

For those who don’t want to use ocr and feel 1.2GB+ is too heavy for their docker space can deploy a docker image without ocr:

`dadoonet/fscrawler:noocr`

As it is offered by hub.docker.com you can simply deploy it via one of the commands above. Don’t forget to add access to your directory(/ies) you want to index.


SpotlightBackend


SpotlightStorage

We will configure everything else from the shell TNS has built in, so this is all we have to do here.

After that start your docker image. Open a shell and double check your files accessibility. I have mounted my scans folder under /media/scans, so I do a `ls -lah /media/scans/` and get something like this:


SpotlightBackendPermissions

Now we will need to create an initial fscrawler configuration, so execute the following command (you may adjust the name of the crawler instance, IMPORTANT! Only use lowercase characters, as upper case is not allowed!) `bin/fscrawler instancename` That creates a yaml config file under: `/root/.fscrawler/instancename/_settings.yaml` We want to edit this and so we need an editor. So let’s install one: `apt-get update | apt-get install nano` and now edit the file: `nano /root/.fscrawler/instancename/_settings.yaml`

Mine looks like this:

```yaml
---
name: "instancename"
fs:
  url: "/path/to/your/target/folder"
  update_rate: "1m"
  excludes:
  - "*/~*"
  json_support: false
  filename_as_id: false
  add_filesize: true
  remove_deleted: true
  add_as_inner_object: false
  store_source: false
  index_content: true
  attributes_support: false
  raw_metadata: false
  xm1_ support: false
  index_folders: true
  lang_detect: false
  continue_on_error: false
  ocr:
    language: "eng"
```

```
    enabled: true
    pdf_strategy: "or_and_text"
    follow_symlinks: false
  elasticsearch:
    nodes:
    - uri: "http://[ip or dn of your SCALE]:9200"
    bulk_size: 100
    flush_interval: "5s"
    byte_size: "10mb"
    ssl_verification: true
    username: "elastic"
    password: "verysecret"
```

I adjusted everything to my needs, so yours will differ… Most important are the settings under elasticsearch as this will impact the connection to the ES docker.

Save and exit via ‘ctrl + x’ and ‘y’. Start fscrawler again with the above command. It should immediately start scanning your directory.

Samba configuration

We need to tell Samba, that it is now capable to utilize an elasticsearch engine.

SMB server preparation

We do this in the advanced settings of the samba server: -> System Settings -> Services -> SMB settings (pencil) -> Advanced Options -> Auxiliary Parameters:

```
spotlight backend = elasticsearch
elasticsearch:address = [ip or dn of your SCALE]
elasticsearch:port = 9200
```

SMB share preparation

-> Shares -> [select the share you want to enable spotlight on] -> Advanced Options -> Auxiliary Parameters:

```
spotlight = yes
```

Final words

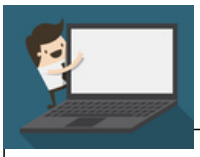
Now you’re ready to go. After a couple of minutes my spotlight search was working and ES responses were shown in my finder.

As I prefer a TL;DR approach there are still a lot of things to optimize within this How To that I or maybe someone else might add.

Definitely open todos:

- autostart fscrawler script when docker image was started

4 - UI Reference Guide



Welcome to this Web Interface (UI) Reference Guide! This document shows and describes each screen and configurable option contained within the TrueNAS web interface. The document is arranged in a **parallel** manner to the UI, beginning with the top panel and then descending through each option in the left side menu. To display this document in a linear HTML format, export it to PDF, or physically print it, please select **Download or Print**.

Table of Contents (click to expand)

SCALE Documentation Sections

TrueNAS SCALE documentation is divided into several sections or books:

- The Getting Started Guide provides the first steps for your experience with TrueNAS SCALE:
  - Software Licensing information.
  - Recommendations and considerations when selecting hardware.
  - Installation tutorials.
  - First-time software configuration instructions.
- Configuration Tutorials have many community and iXsystems -provided procedural how-tos for specific software use-cases.

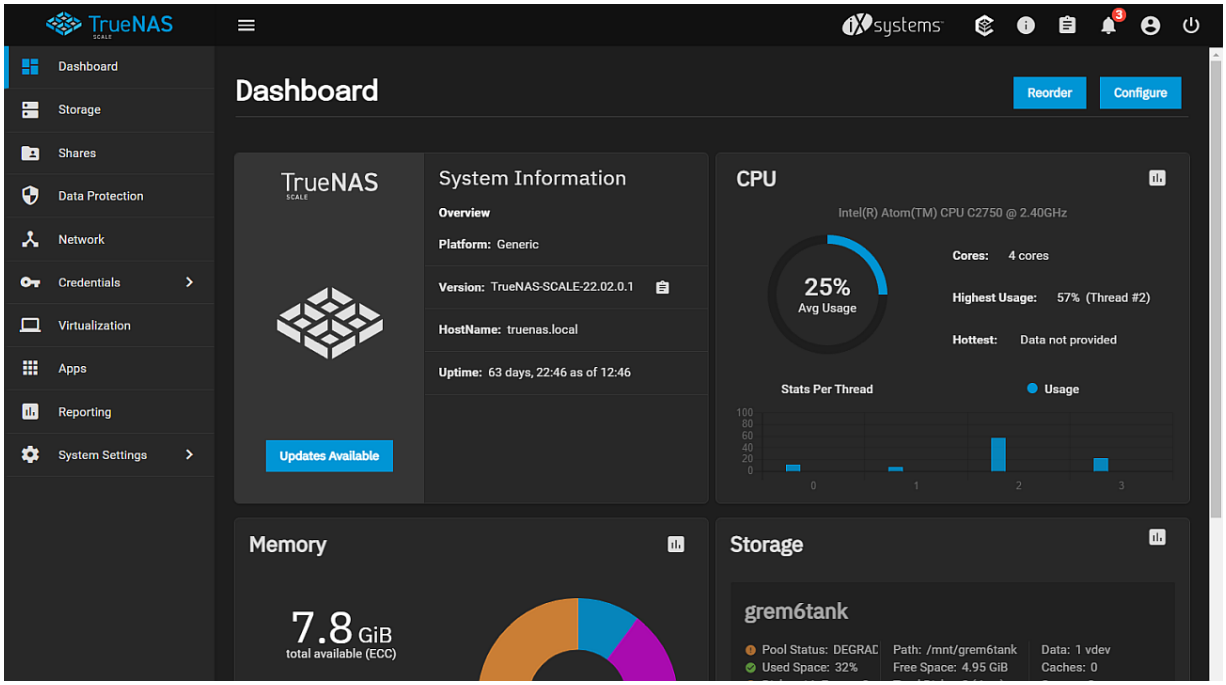
- The UI Reference Guide describes each section of the SCALE web interface, including descriptions for each configuration option.
- API Reference describes how to access the API documentation on a live system and includes a static copy of the API documentation.
- SCALE Security Reports links to the TrueNAS Security Hub and also contains any additional security-related notices.

Ready to get started? Choose a topic or article from the left-side **Navigation** pane. Click the **<** symbol to expand the menu to show the topics under this section.

4.1 - Dashboard

This article provides information on the information cards (widgets) on the **Dashboard** screen and how to customize the display by moving, adding or removing the widgets.

The **Dashboard** screen displays the first time you log into the SCALE web interface. To display the **Dashboard** screen again click **Dashboard** on the left side panel.



Tutorial Video

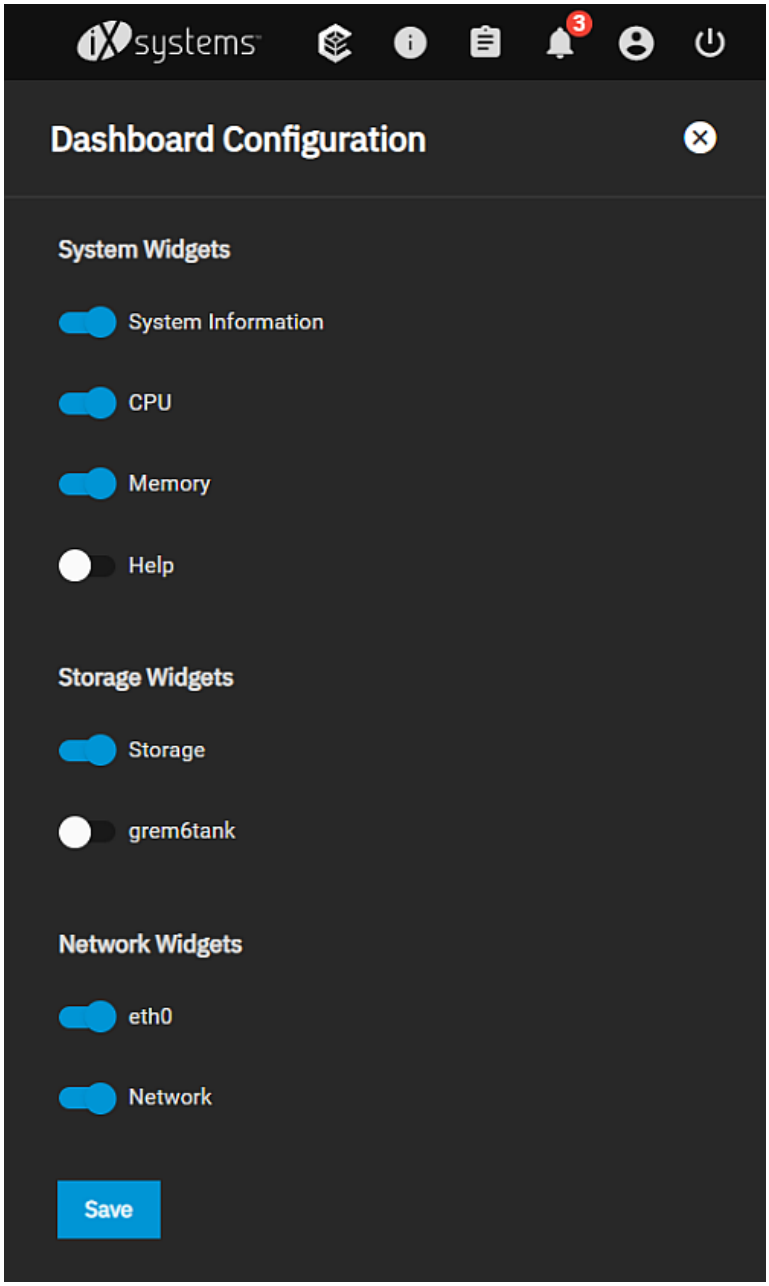
The **Dashboard** displays basic information about your TrueNAS system in widgets or information cards that group information about your TrueNAS by type. For example, CPU information in the CPU widget. These widgets display in a default layout that you can change.

Use the **Reorder** button to change the layout of the various widgets to suit your preference.

Use **Configure** turn the widget display on or off. When on the widget displays on the dashboard.

Dashboard Configuration Panel

The **Dashboard Configuration** panel allows you to turn widget displays on or off. There are three widget group types, **System Widgets**, **Storage Widgets** and **Network Widgets**. Storage and network widgets vary based on the pools and network interfaces configured on your TrueNAS.



Click on the slider to turn the information display on or off.

System Widgets control the display of the **System Information**, **CPU**, **Memory** and **Help** widgets.

Storage Widgets control the display of the **Storage** widget and individual widgets for each pool configured on your TrueNAS.

Network Widgets control the display of the **Network** widget and any individual interfaces configured on your TruNAS.

Use **Save** to retain any setting changes you make. Click on the **X** or on any part of the UI screen away from the **Dashboard Configuration** panel to close it without saving changes.

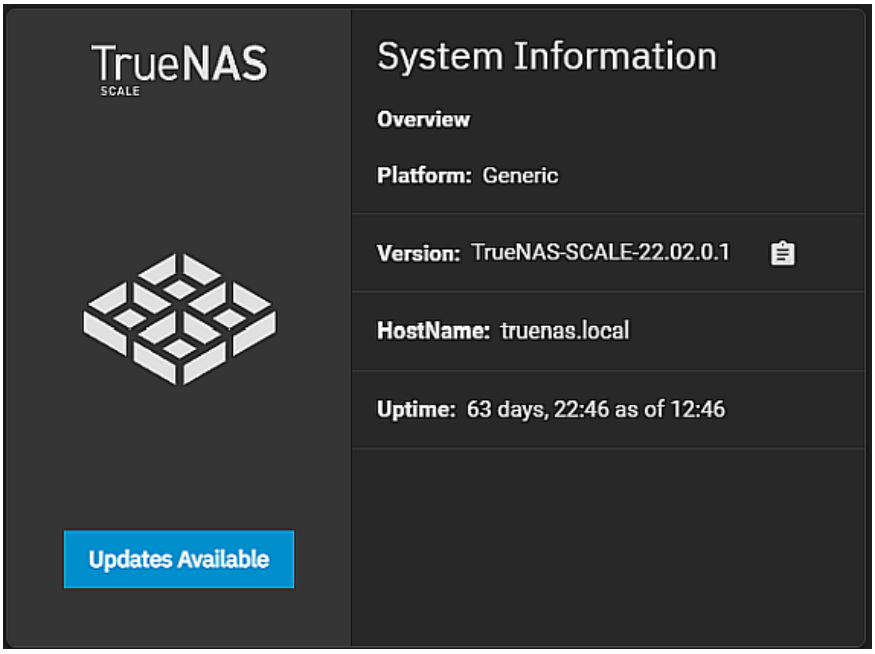
Click on the icon to display the report screen that corresponds to that widget. For example, clicking the assessment icon on the **CPU** widget opens the **Reports > CPU** screen.

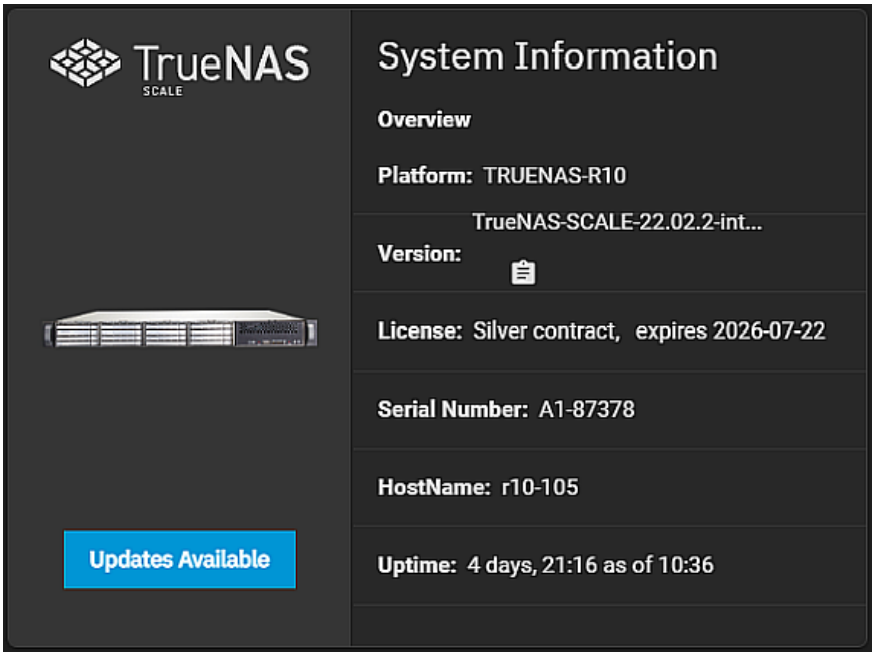
System Information Widget

The **System Information** widget displays general information on the SCALE system.

Click here for more information

If installed on customer-provided servers the widget displays a generic TrueNAS image. If installed on iXsystems-provided hardware, a picture of the iXsystems hardware displays on the card above the **Updates Available** button. Click on the image to display the **System Enclosure** screen.





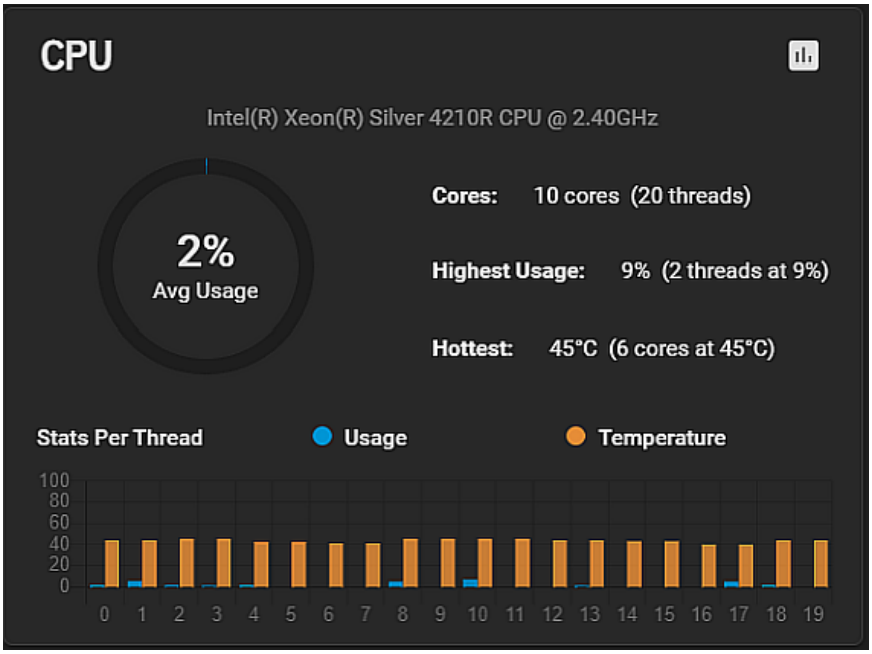
Field	Description
Platform	Displays **Generic** for customer-provided server and hardware, and a TrueNAS logo displays to the left of the **System Information** fields. Displays the TrueNAS model number for the iXsystems-provided server and hardware, and a picture of the server displays in the area to the left of the fields.
Version	Displays the currently-installed software release of TrueNAS SCALE. Use the clipboard assignment icon to display the full name of the release installed and to copy the version to the clipboard.
HostName	Displays the host name for the TrueNAS system. Configure the host name i on the **Network > Global Configuration** screen.
Uptime	Displays the number of consecutive days and the number of hours and minutes the system has run since the last reboot.
Updates Available	Click to display the **System Update** screen. You can also display the **System Update** screen by selecting **System > Updates** on the main menu panel on the left side of the screen.

CPU Widget

The **CPU** widget displays information on the system CPU.

Click here for more information

The widget includes an **Avg Usage** dynamic spinner that displays the percentage of usage at that moment on the CPU. The **Stats Per Thread** bar graph displays **Usage** in blue and **Temperature** in orange with the x axis with the number threads and the y axis the percent usage in 20 increment counts. It also details the number **Cores** as ***x* cores (*y* threads)**, the **Highest Usage** as ***x*% (*y* threads at *x*%)**, and the **Hottest** temperature as ***x*°C (*y* cores at *x*°C)**.

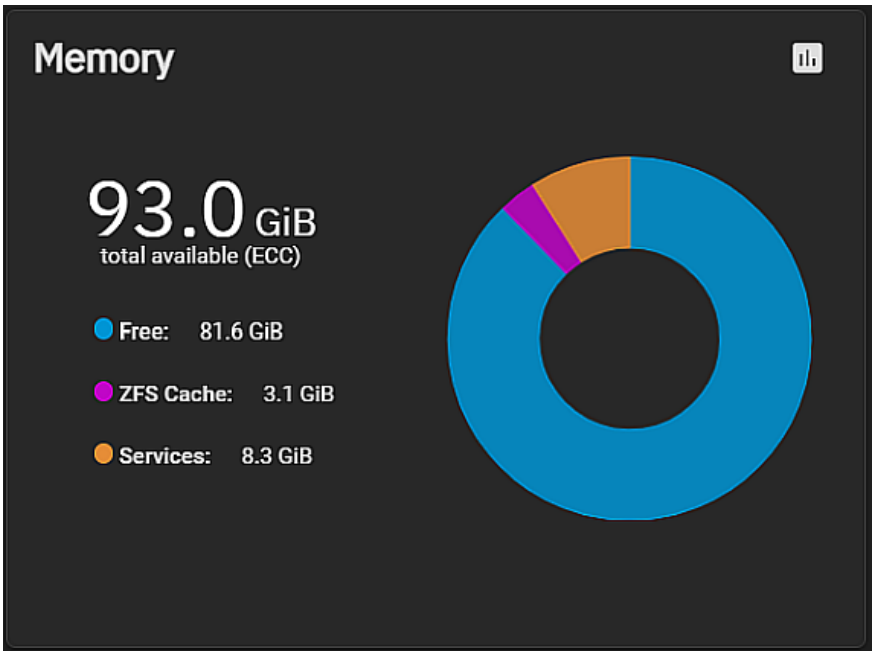


Memory Widget

The **Memory** widget displays information on the system memory.

Click here for more information

The widget displays a spinner showing the GiB **Free** in blue, **ZFS Cache** in fuchia pink, and **Services** in orange.

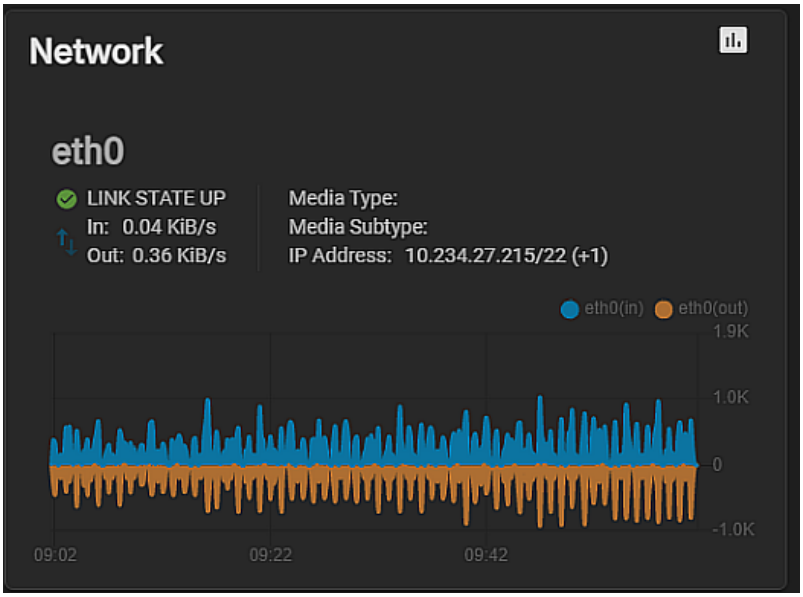


Network and Interface Widgets

The **Network** widget displays network the status of the system interfaces, I/O stats, link status and the system IP address and port number.

Click here for more information

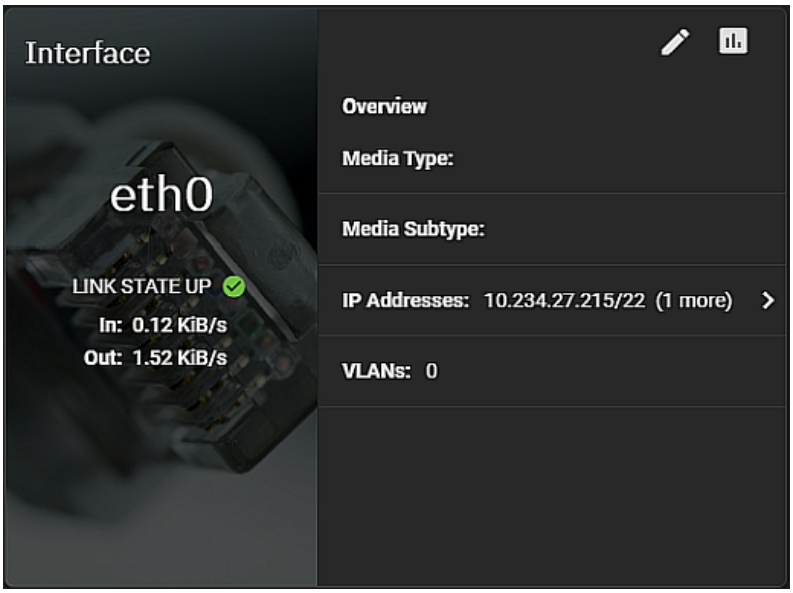
The **Network** widget displays a dynamic graph of input (blue) and output (orange) I/O activity over the primary system interface.



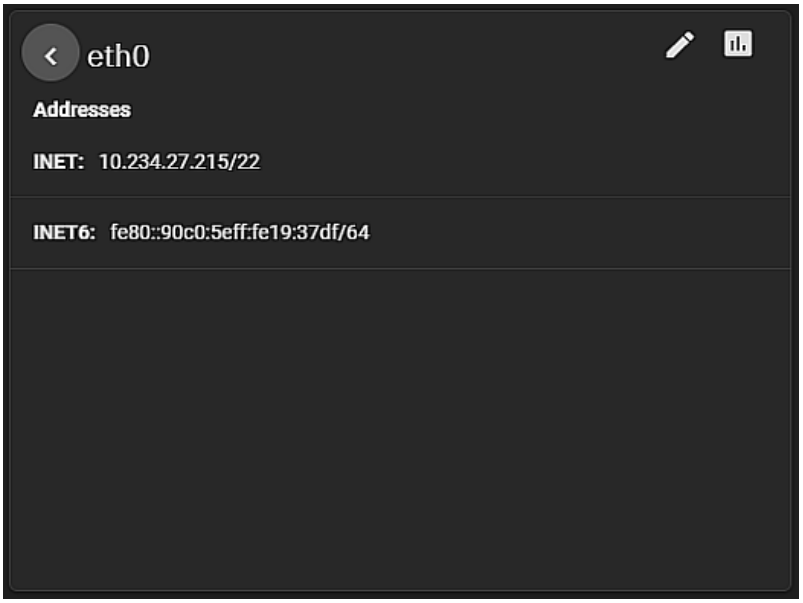
The **Interface** widgets display I/O stats and link status, and provides more information on that interface media type and subtype, any VLANS and the IP Address and port number.

Click here for more information

If more than one interface is configured on your TrueNAS you can use the **Dashboard Configuration** panel to add an interface widget for each interface. The **Interface** card displays the information for that interface.



Click on the arrow_forward_ios to display the **Addresses** widget for that interface.



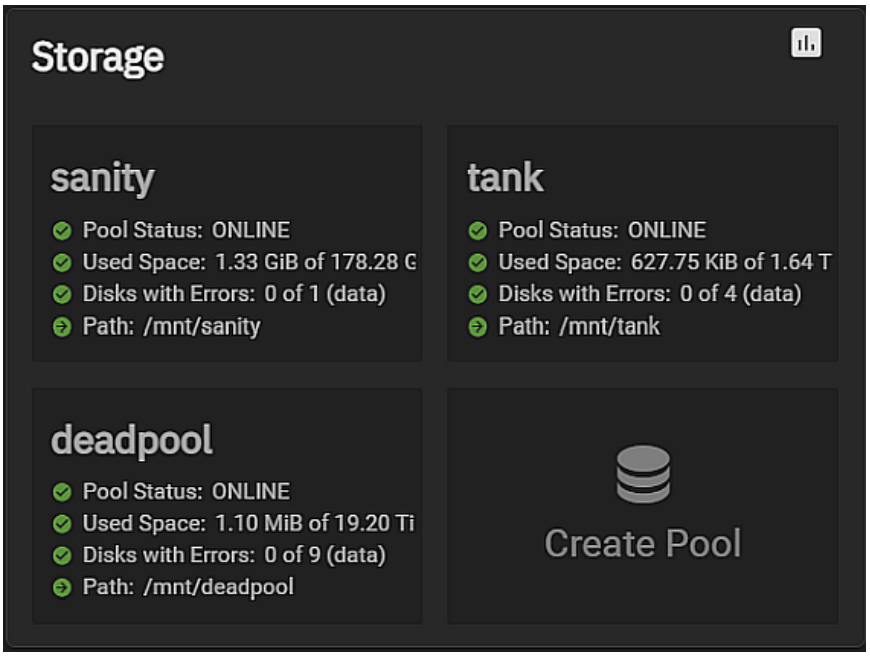
Click the edit to display the **Network** screen where you can select the interface to open the **Edit Interface** panel.

Storage and Pool Widgets

The **Storage** widget displays information on the root and other storage pools configured on your system.

Click here for more information

The **Storage** widget displays the root pool status, path, and the number of vdevs configured. It also displays the percentage of space it uses, is free and any caches. It also reports on the number disks with errors, the total number of disks the root pool uses and if a spare exists.

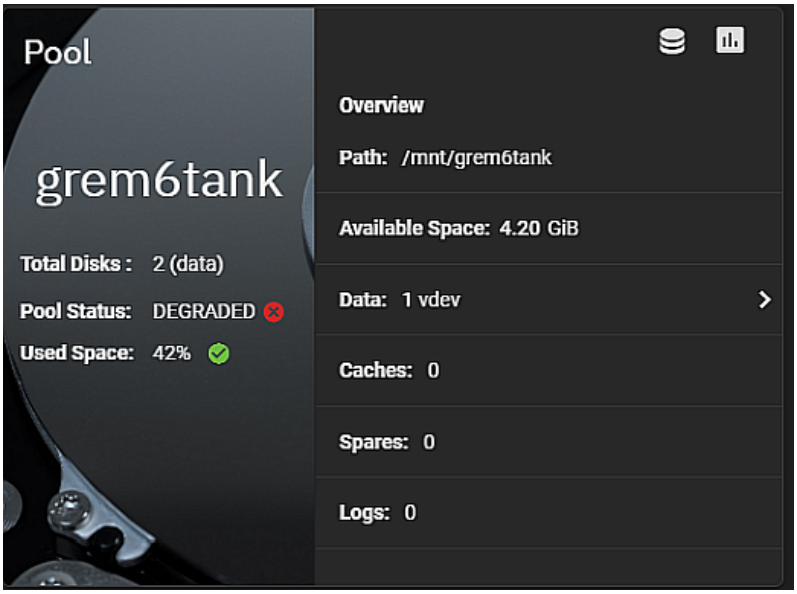


The individual pool information displayed in this widget includes the same information as the root pool.

The **Pool** widget displays information on a single storage pool.

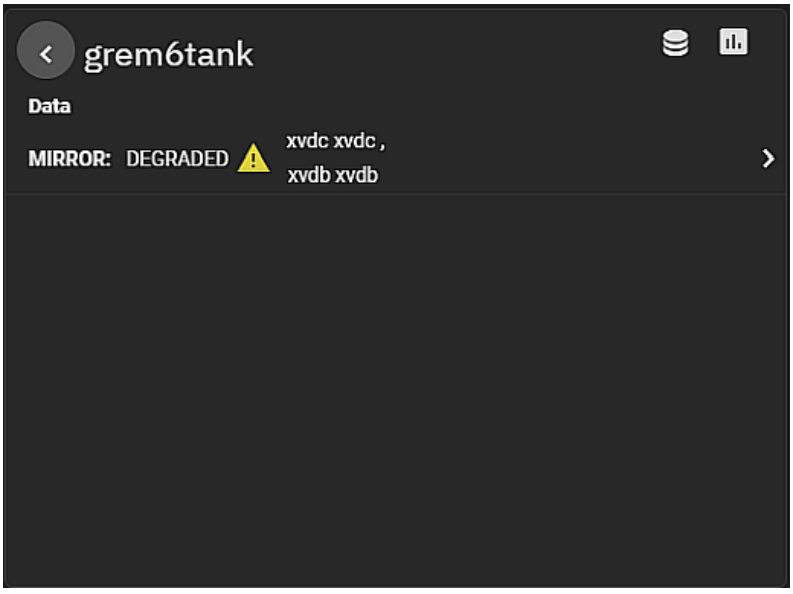
Click here for more information

You can use the **Dashboard Configuration** panel to add a pool widget for each pool you want to include on the **Dashboard**. The **Pool** widget displays the total number of disks, pool status and space used by the pool this widget reports on. It also provides the mount path, available space, number of data vdevs, caches, spares and logs configured for this pool.



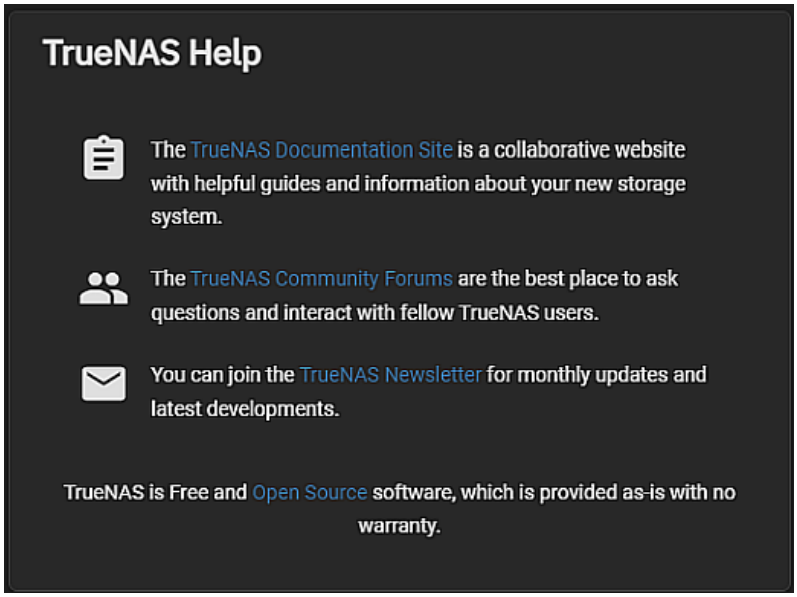
Click on the icon to display the **Storage > Pool Status** screen.

Click on the arrow_forward_ios to display the details on the vdevs.



Help Widget

The **TrueNAS Help** widget displays links to the TrueNAS Documentation Site and community forums, as well as a link to where users can sign up for the TrueNAS Newsletter and a link to the Github web page for TrueNAS open source software.



Click on each link to open it in a new browser tab.

Related Pools Articles

Related Network Articles

4.2 - Top Toolbar Options

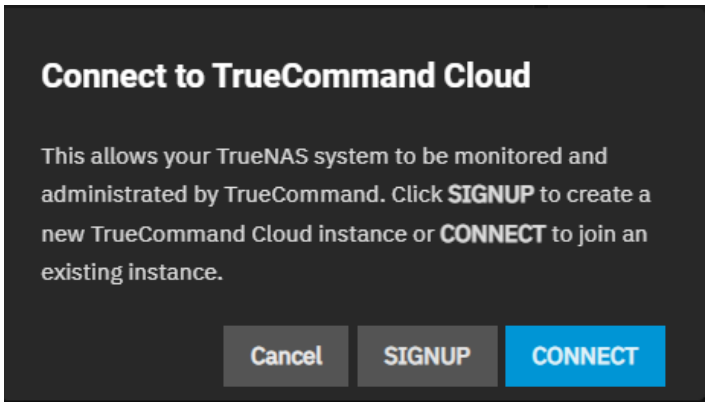
The top toolbar icon buttons provide access to the iXsystems website, displays the status of TrueCommand and directory services configured on your system, and displays other configuration menu options.

Toolbar Icons

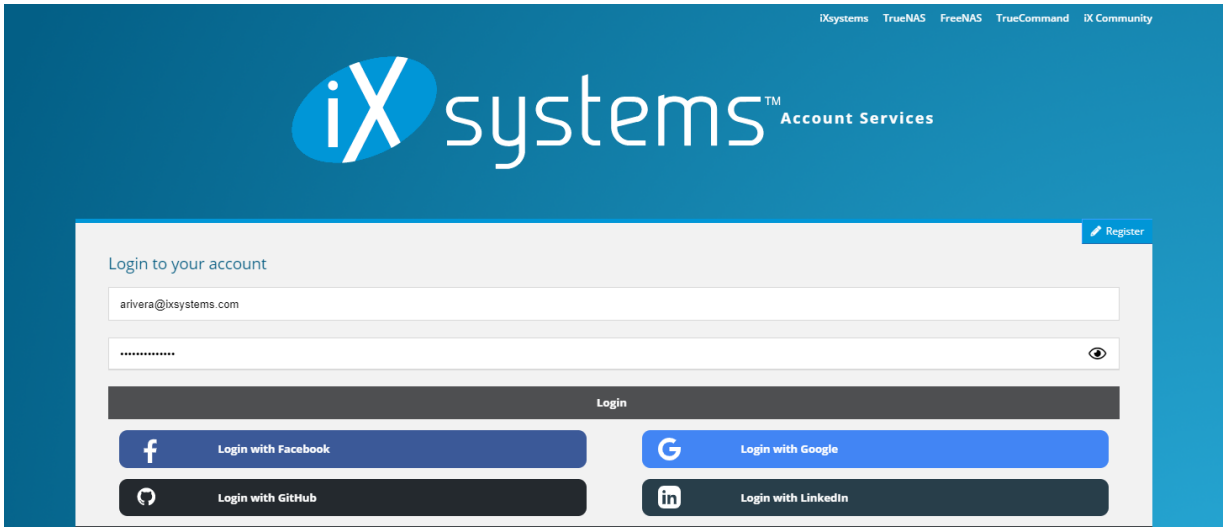
Icon	Name	Description
	Toggle collapse	Click to expand or collapse the main menu panel on the left side of the screen.
	iXsystems Website	Opens the iXsystems home page website where users can find information about storage and server systems. Users can also use the iXsystems home page to access their customer portal and community section for support.
	TrueCommand status	Displays either the status of a TrueCommand cloud connection or a dialog that allows users to sign up for a new TrueCommand cloud connection. Instructions are found in the **Cloud Deployment** section.
	Directory Services status	Displays a dialog with the status of Active Directory and LDAP directory servers configured on the TrueNAS.
	Task Manager	Displays the Task Manager dialog. Click the **History** button to display the **Jobs** screen with a list of **All**, **Active** or **Failed** jobs or processes.
	Alerts	Displays a list of system alerts and a dropdown list the alert options **Alert Settings**, **Alert Services** and **Email**.
	Settings	Displays a dropdown menu of setting options **Change Password**, **Preferences**, **API Keys**, **Guide** and **About**.
	Power options	Displays the power related options **Log Out**, **Restart** or **Shut Down**.

Status of TrueCommand

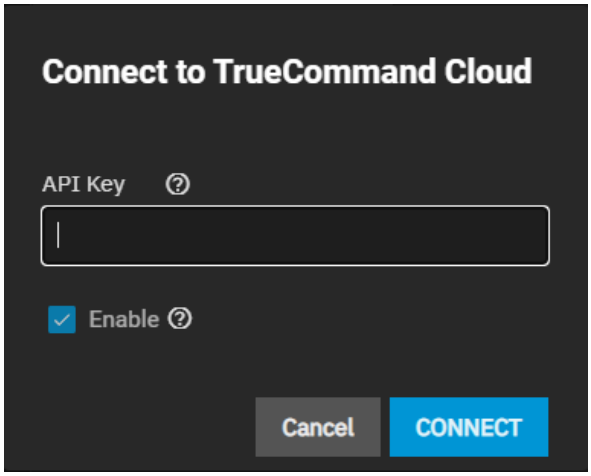
The **Status of TrueCommand** icon lets users sign up with and connect to TrueCommand Cloud.



Clicking **SIGNUP** opens the TrueCommand sign-up page in a new tab.



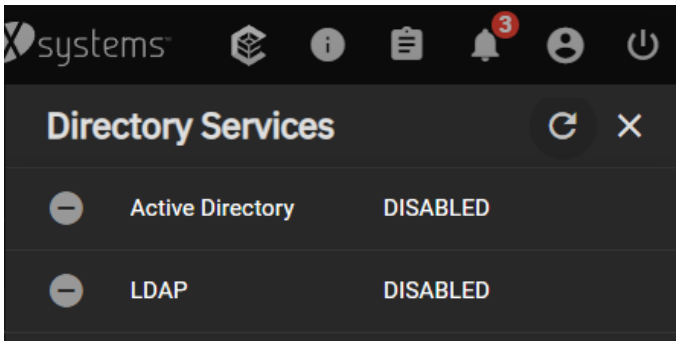
After users sign up, they can click the **CONNECT** button and enter their API key to connect SCALE to TrueCommand Cloud.



See Connecting TrueNAS for more information on configuring a TrueCommand cloud account and getting an API key.

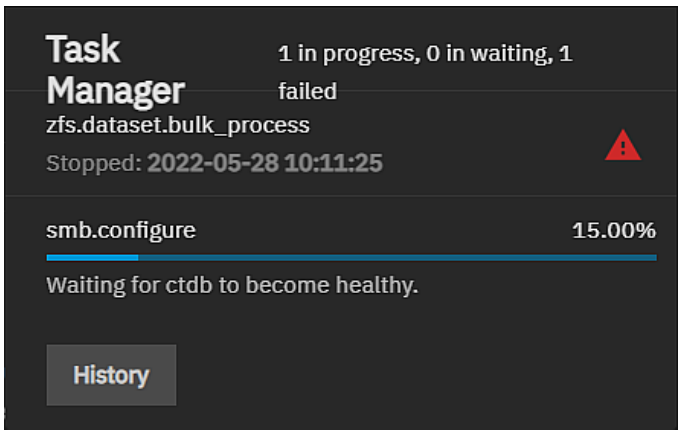
Directory Services Monitor

The **Directory Services Monitor** icon button displays the status of Active Directory and LDAP services. Clicking on either takes you to their respective configuration screens.



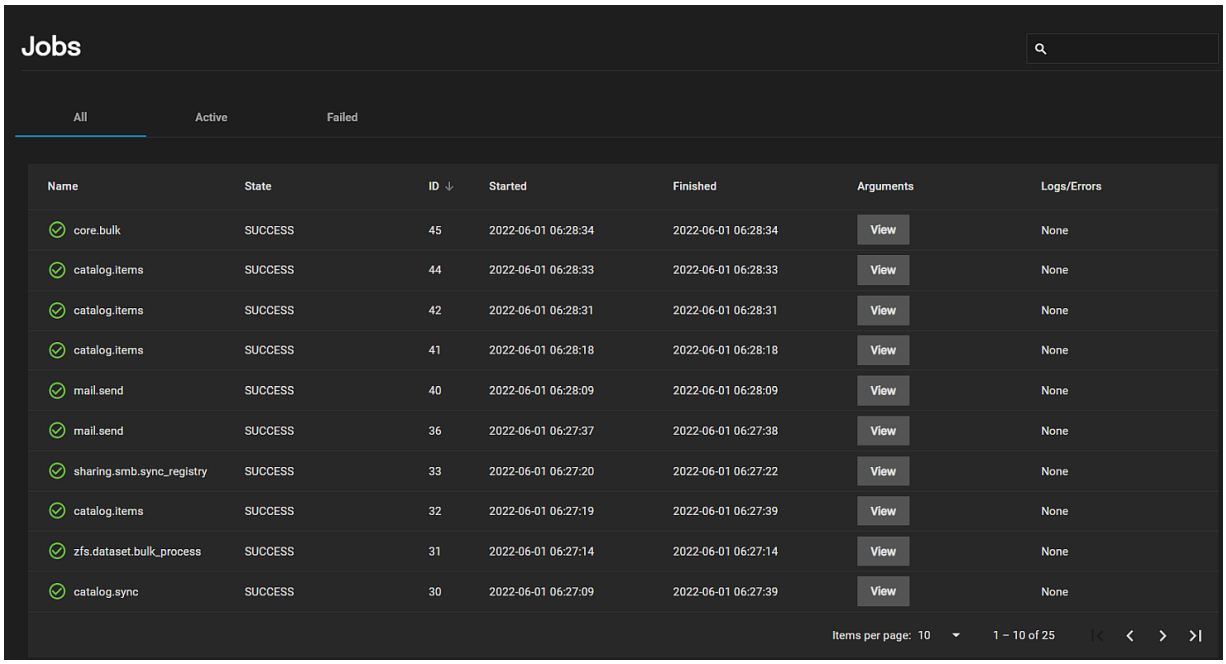
Task Manager

The **Task Manager** icon button displays all running and failed jobs/processes. Minimized jobs/processes can be accessed here.



Click on a running task to display the dialog window for that running task.

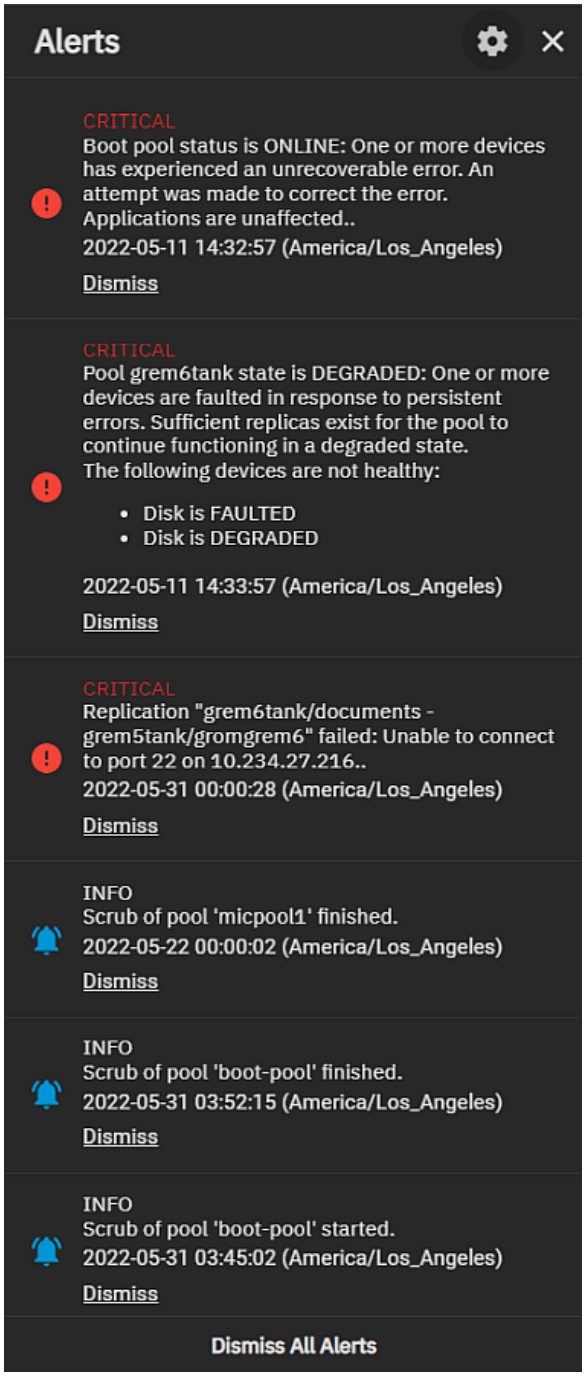
Click the **History** button to open the **Jobs** screen. **Jobs** lists all successful, active, and failed jobs. Users can also click **View Log** next to a failed process to view its log information and error message.



For more information see the **Jobs Screens** article.

Alerts

The **Alerts** icon button displays a list of current alert notifications. To remove an alert notification click **Dismiss** below it or use **Dismiss All Alerts** to remove all notifications from the list.



Use the icon to display the **Alerts** dropdown list with three options **Alert Settings**, **Alert Services** and **Email**.

Select **Alert Settings** to configure alert options such as the warning level and frequency and how the system notifies you. See Alerts Settings Screens for more information on **Alert Settings** screens and settings.

Select **Alert Services** to add or edit existing system alert services. See Alerts Services Screen for more information on **Alert Services** screens and settings.

Select **Email** to configure the email service and account to receive alerts from the TrueNAS. See Email Screens for information on **Email** screens and settings, or see Setting Up System Email for general information about setting up the system email.

Settings

The **Settings** icon button displays a menu of general system settings options. The options are **Change Password**, **Preferences**, **API Keys**, **Guide** and **About**.

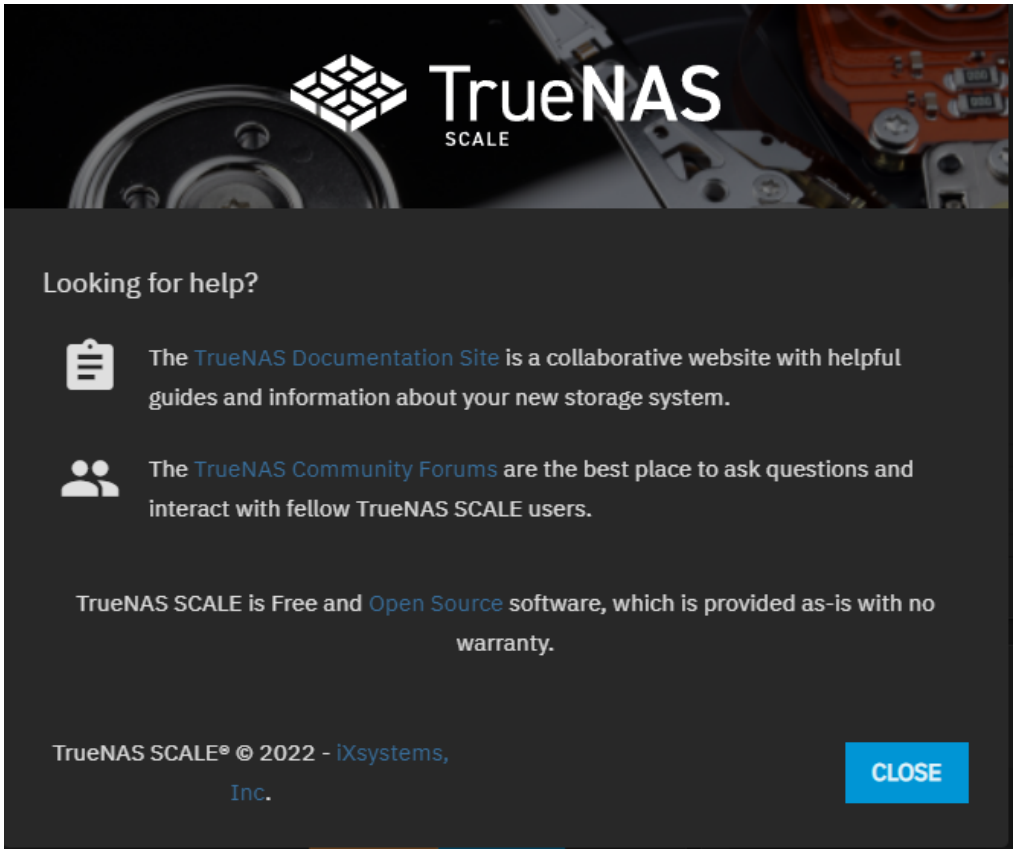
The **Change Password** icon button displays a dialog where you can change the login password for the currently logged-in administrator password.

The **Preferences** icon button displays the Web Interface Preferences screen where you can select general preferences for the system, such as a color theme.

The **API Keys** icon button displays the API Keys screen that lists current API keys and where you can add or manage API keys that identify outside resources and applications without a principal.

The **Guide** icon button opens the TrueNAS Documentation Hub website in a new tab.

The info **About** icon button displays a window with links to the TrueNAS Documentation Hub, the TrueNAS Community Forums, the FreeNAS Open Source Storage Appliance GitHub repository, and the iXsystems hom page. Use the **Close** button to close the window.



Power

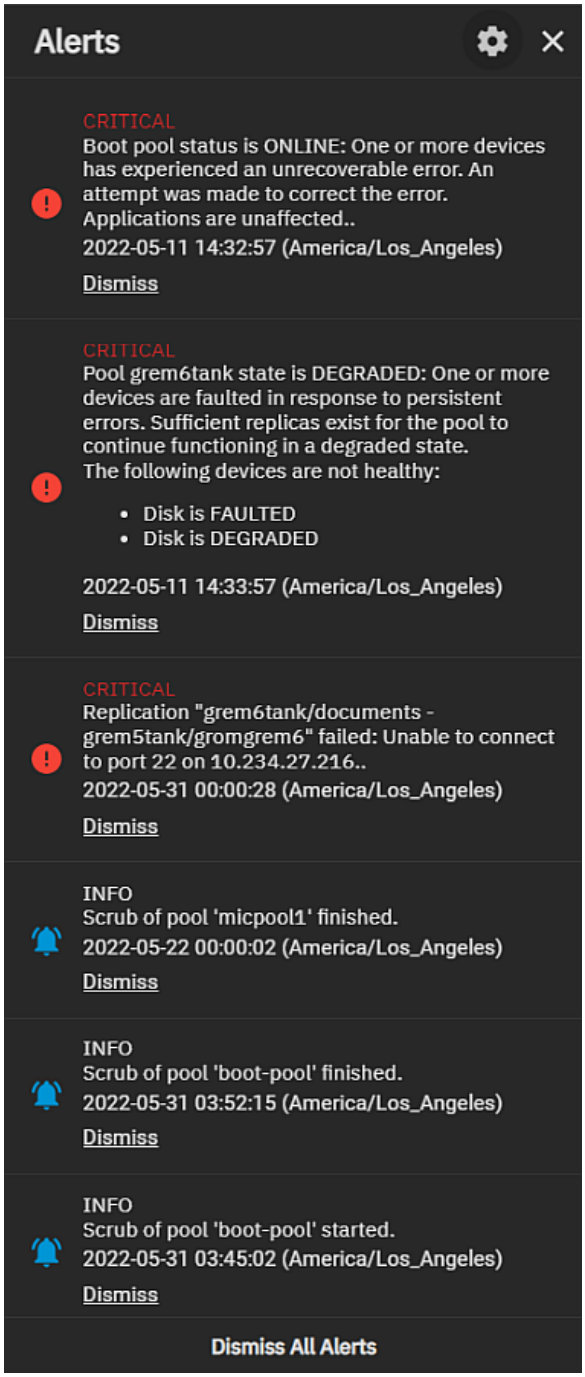
The **Power** button provides three options that lets the user log out of the web UI, restart, or shut down their TrueNAS system.

Related Information

- Alerts
  - Alert Settings Screens
  - Alert Services Screens
  - Email Screens
- Settings Options
  - Web Interface Preference Screen
  - API Keys Screen
- Jobs Screens

4.2.1 - Alerts

The **Alerts** icon button displays a list of current alert notifications. To remove an alert notification click **Dismiss** below it or use **Dismiss All Alerts** to remove all notifications from the list.



Use the icon to display the **Alerts** dropdown list with three options **Alert Settings**, **Alert Services** and **Email**.

Select **Alert Settings** to configure alert options such as the warning level and frequency and how the system notifies you. See Alerts Settings Screens for more information on **Alert Settings** screens and settings.

Select **Alert Services** to add or edit existing system alert services. See Alerts Services Screen for more information on **Alert Services** screens and settings.

Select **Email** to configure the email service and account to receive alerts from the TrueNAS. See Email Screens for information on **Email** screens and settings, or see Setting Up System Email for general information about setting up the system email.

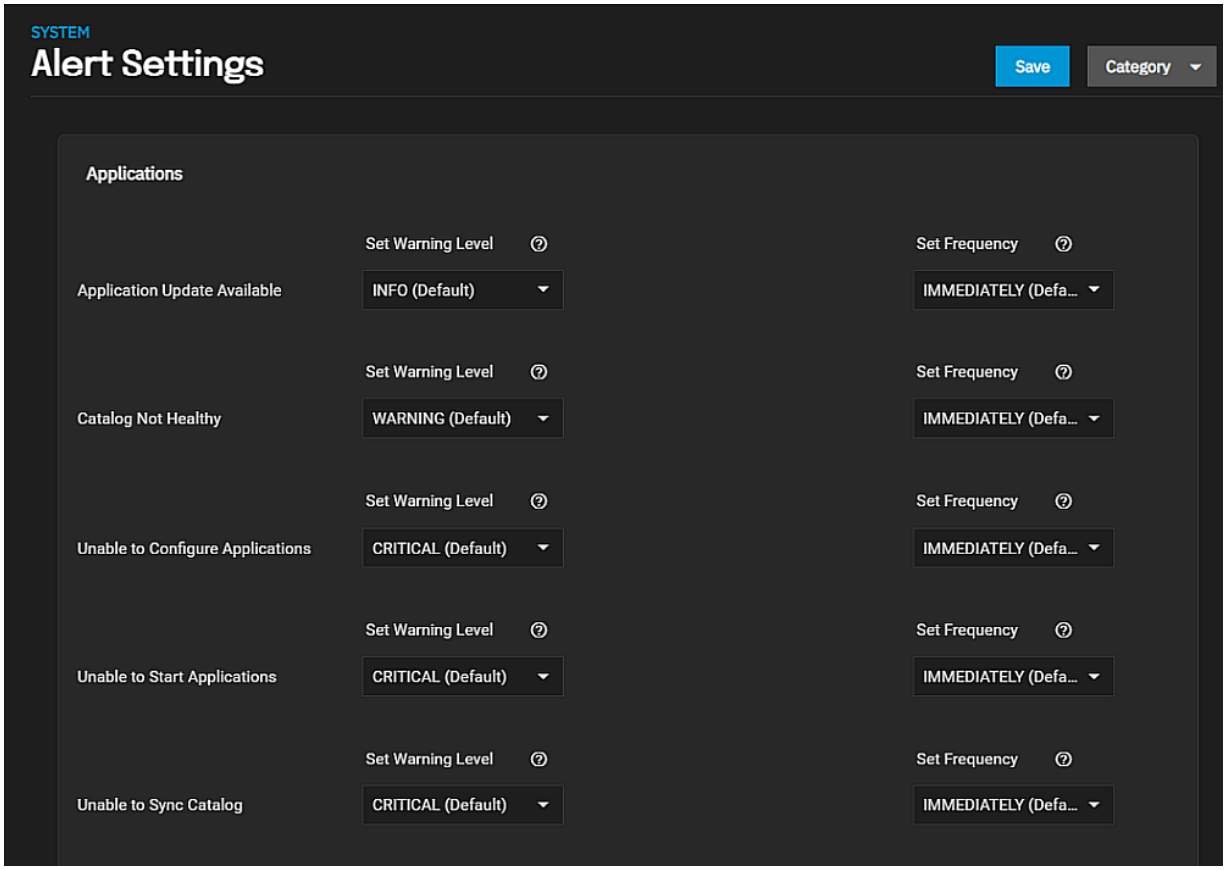
Related Articles

- Alert Settings Screens

- Alert Services Screens
- Email Screens

4.2.1.1 - Alert Settings Screens

The **Alert Settings** screen displays options to set the warning level and frequency.



To access this screen, click the icon, and then click the icon and select **Alert Settings** on the dropdown list.

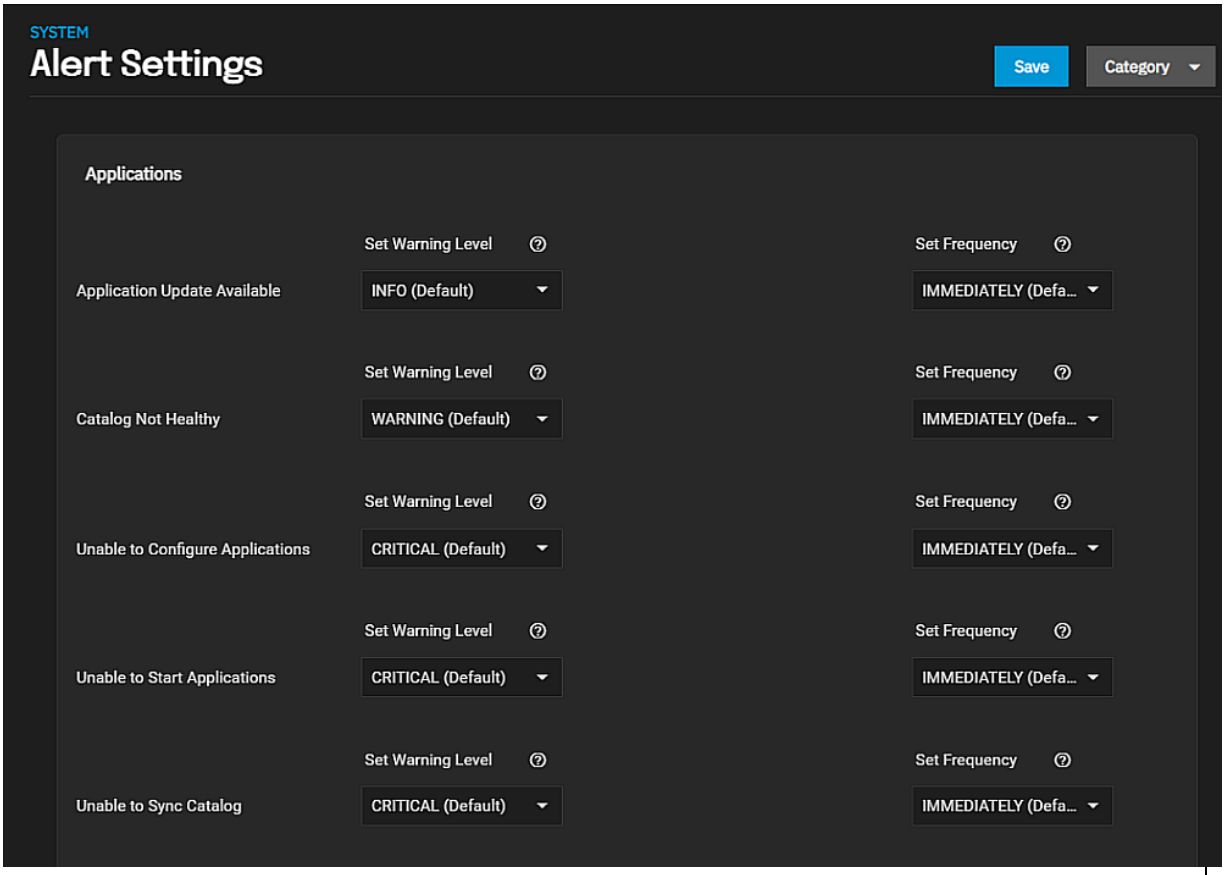
Alert Categories

Use the **Category** dropdown list to displays alert settings for each category. Select from:

Application Alert Settings

Applications alert settings display by default. These alerts apply to the third-party applications you deploy on your TrueNAS.

Click here for more information

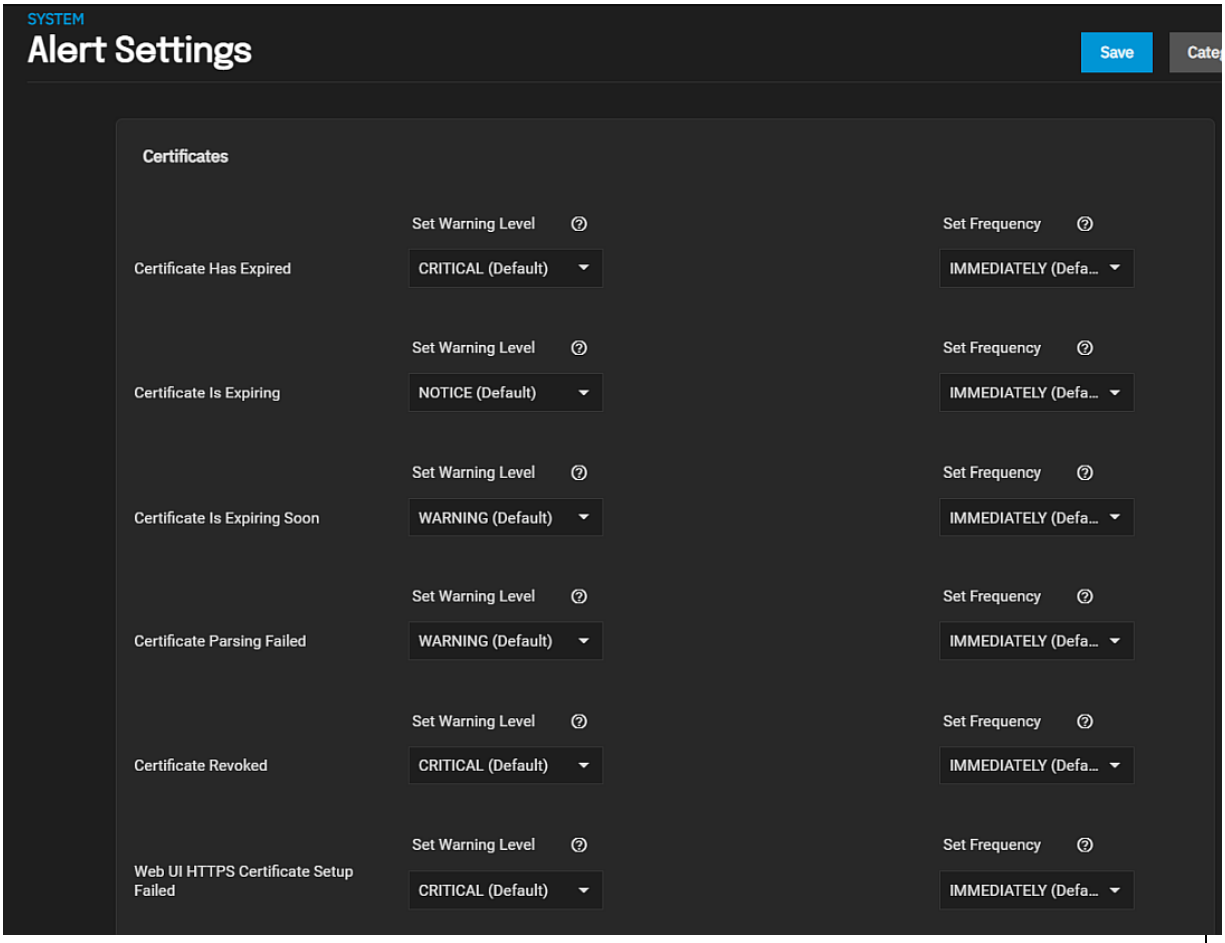


Options cover available updates, health of the catalog, ability to configure or start applications, and ability to sync the catalog.

Certificate Alert Settings

Certificates alert settings apply to certificates you add through the **Credentials > Certificates** screen.

Click here for more information

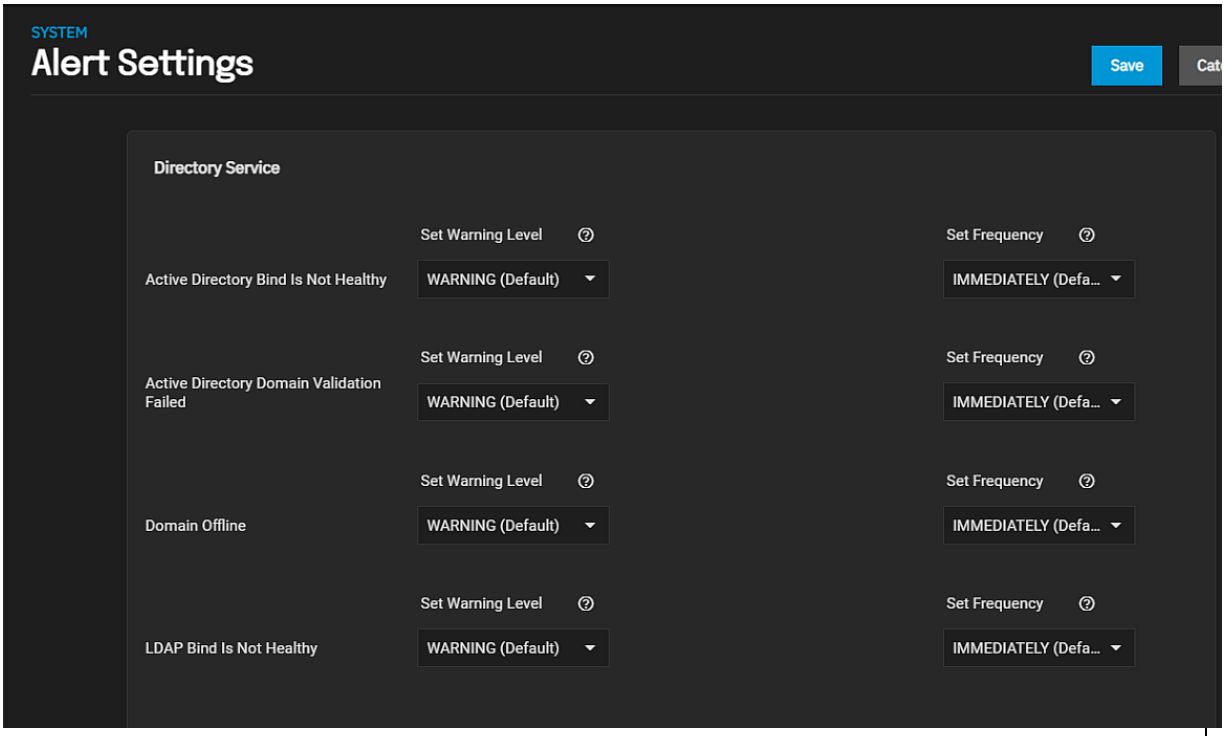


Options cover certificate expiration, parsing, and revoke status> Status cover expired, expiring or expiring soon, revoked, parsing failed and web UI HTTPS certificate setup failed.

Directory Services Alert Settings

Directory Services alert settings apply to the Active Directory and LDAP servers configured on your TrueNAS.

Click here for more information

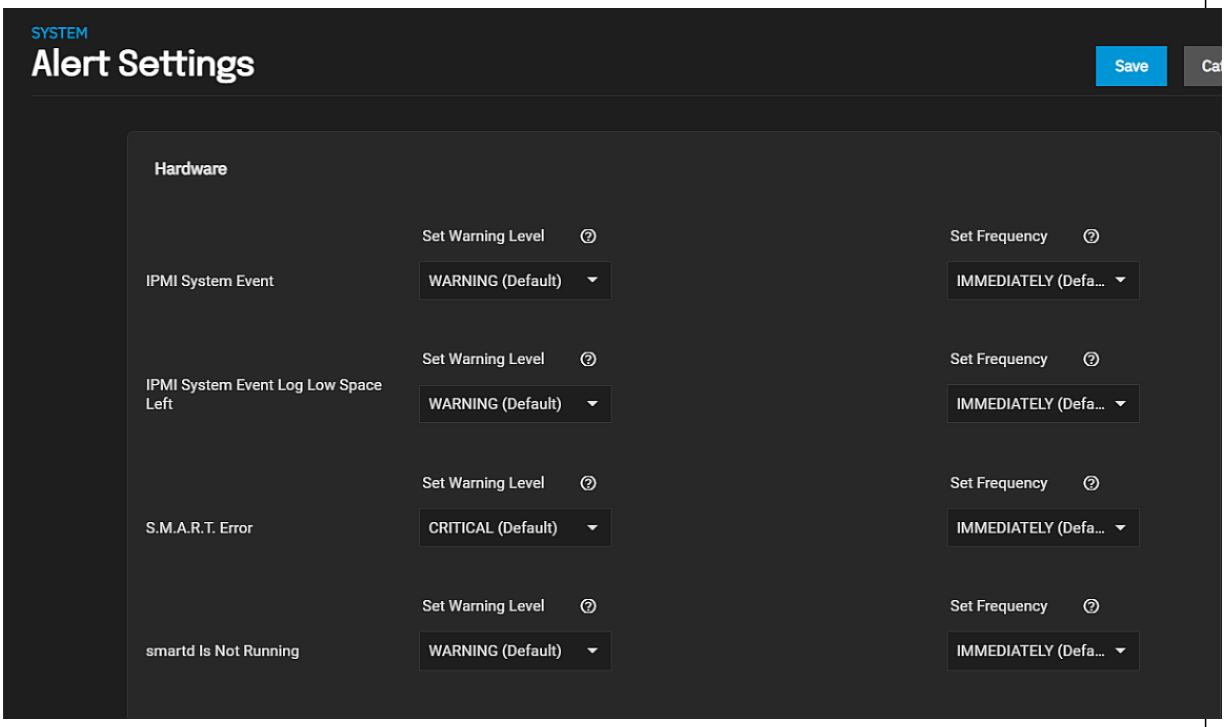


Options cover the health of Active Directory bind, if Active Directory domain validation failed, or the domain is offline, and the health of LDAP bind.

Hardware Alert Settings

Hardware alert settings apply to the IPMI network connections, and S.M.A.R.T. and smartd that monitors the hard drives installed on your TrueNAS system.

Click here for more information

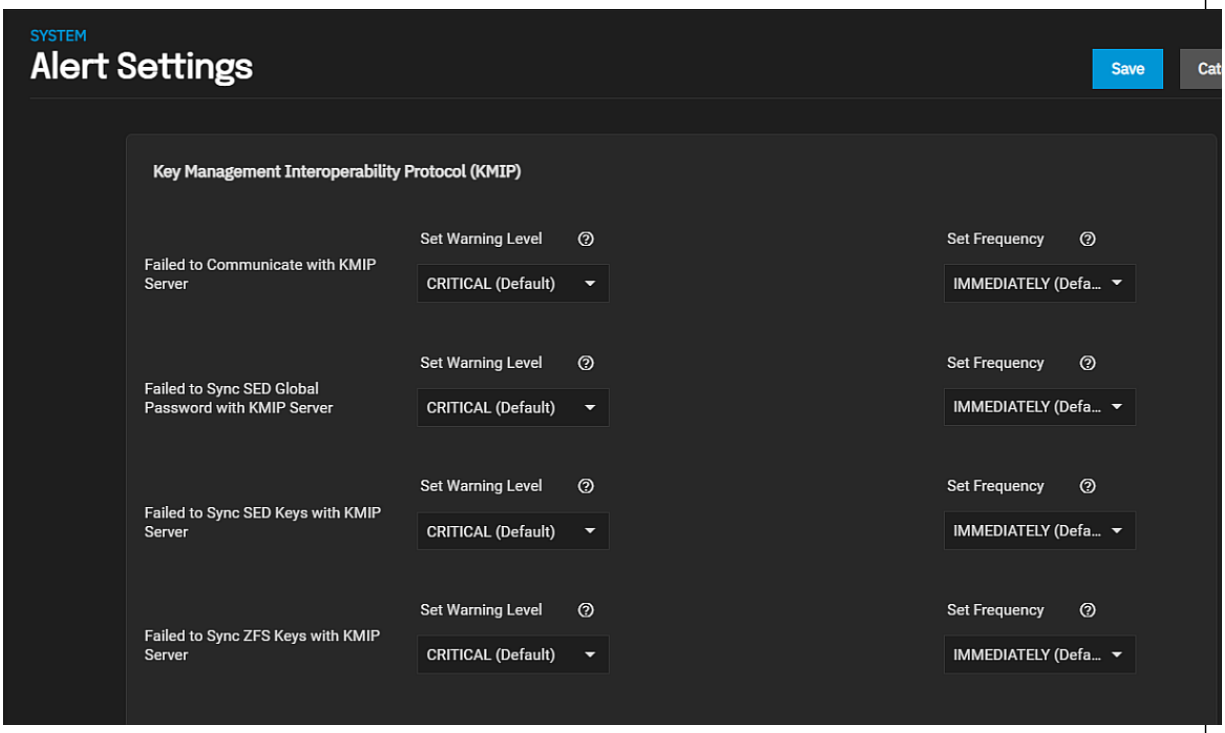


Setting cover IPMI system events, system event log space, S.M.A.R.T. error and smartd running status.

Key Management Interoperability Protocol (KMIP) Alert Settings

Key Management Interoperability Protocol (KMIP) alert settings only apply to KMIP configured on a TrueNAS Enterprise system.

Click here for more information

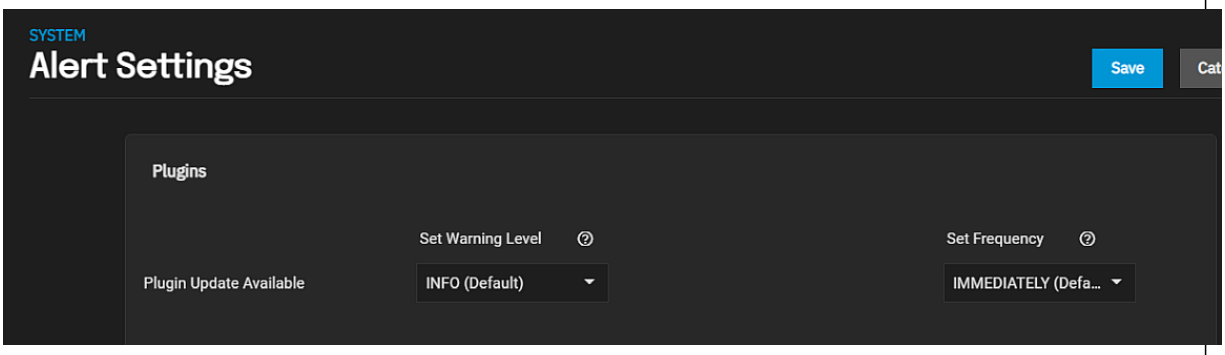


Options cover communication failures with KMIP server, failure to sync SED Global Password, keys, and ZFS with the KMIP server.

Plugins Alert Settings

Plugins alert settings apply to plugins installed on your TrueNAS.

Click here for more information

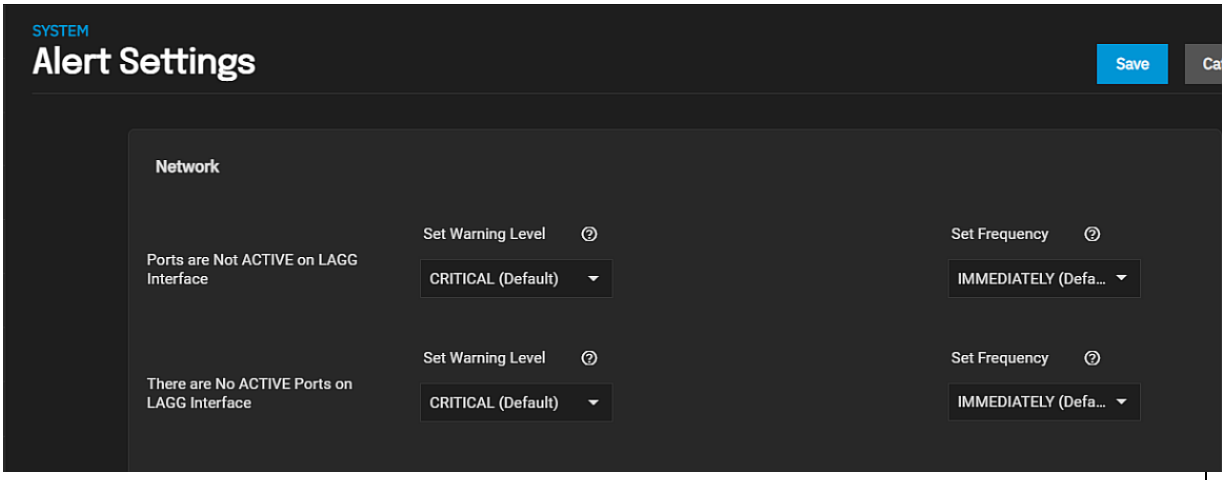


Option is **Plugin Update Available**.

Network Alert Settings

Network alert settings applies to network interfaces configured on your TrueNAS.

Click here for more information

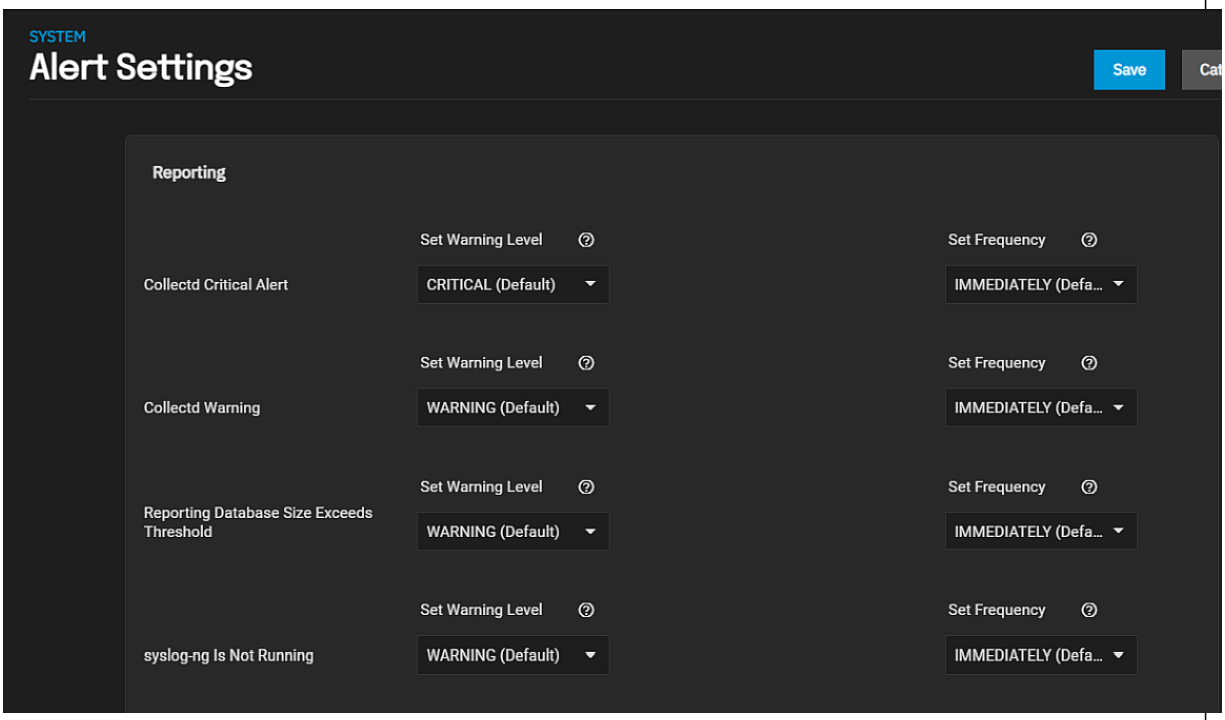


Options cover LAGG interface ports status.

Reporting Alert Settings

Reporting alert settings apply to collectd, reporting database and syslog processes on your TrueNAS.

Click here for more information

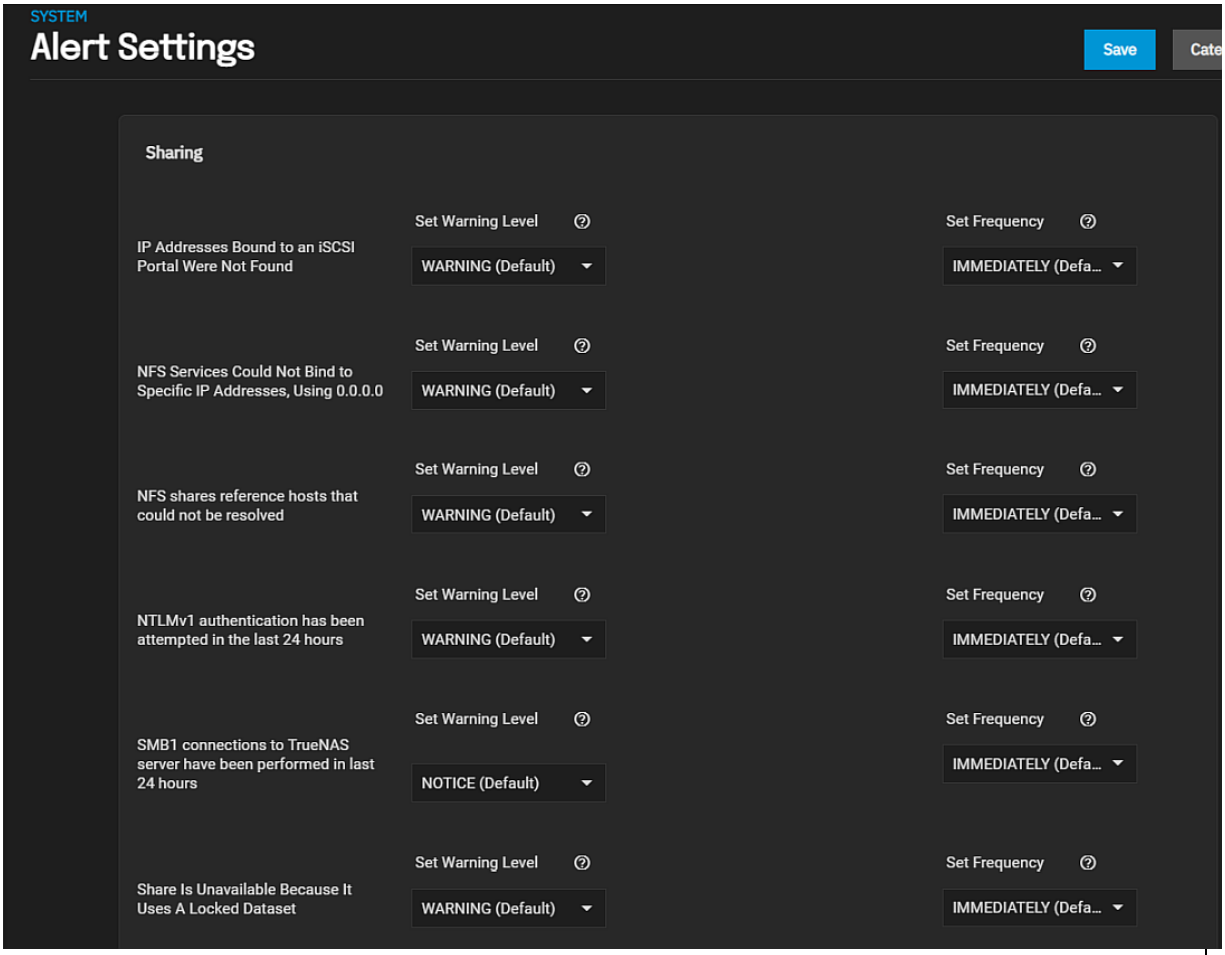


Options cover collectd critical alerts and warnings, reporting database size threshold exceeded and syslog-ng is not running.

Sharing Alert Settings

Sharing alert settings apply to iSCSI, NFS or SMB shares and connections configured on your TrueNAS.

Click here for more information

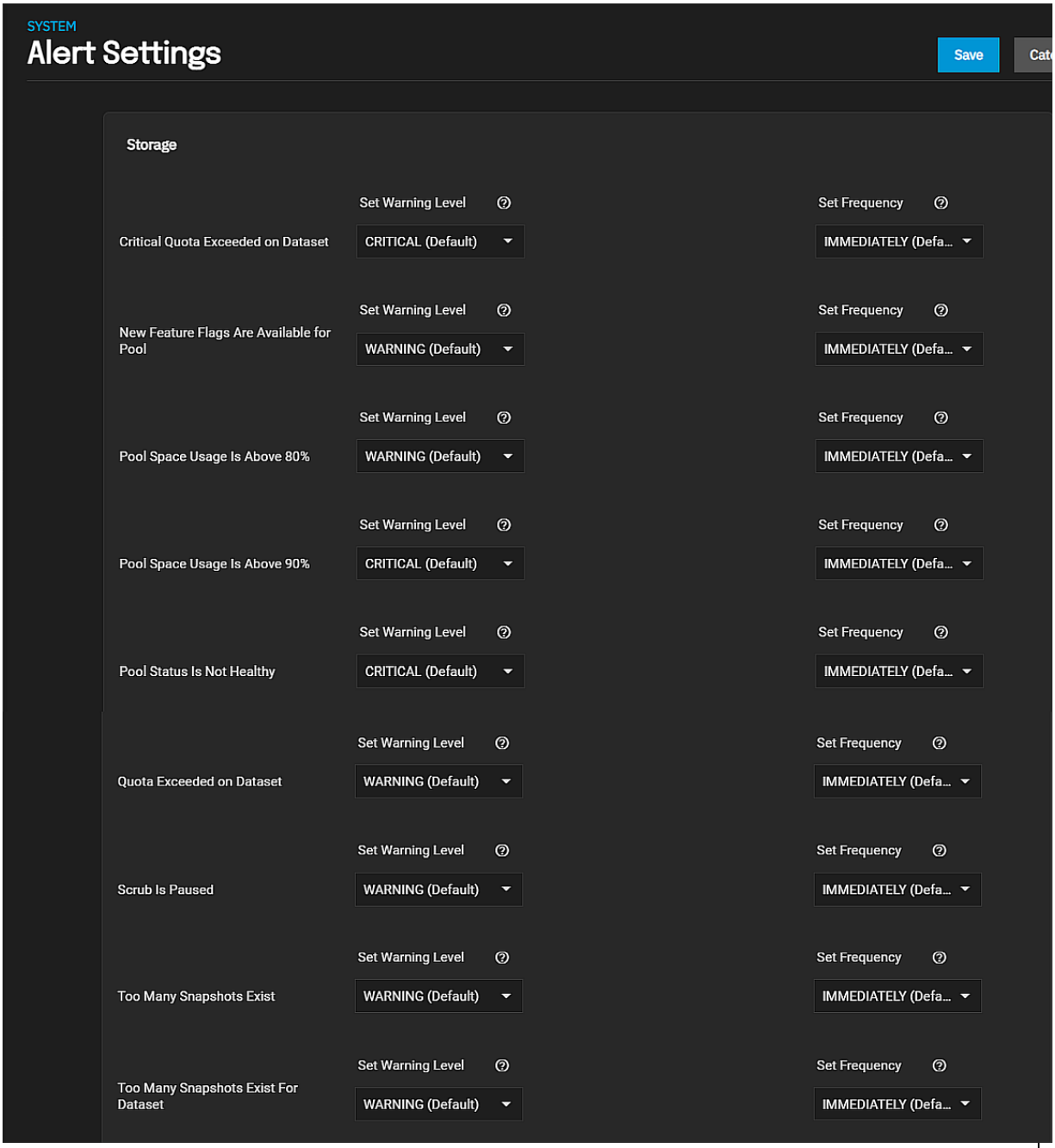


Options cover IP addresses bound to an iSCSI ports not found, NFS services not bound to specific IP addresses using 0.0.0.0, NFS share references hosts that cannot b resolved, NTLMv1 authentication attempted in the last 24hours, SMB1 connections to TrueNAS server performed in last 24 hous and share unavailable because it uses a locked dataset.

Storage Alert Settings

Storage alert settings apply to quotas, pools, snapshots, and scrub processes on your TrueNAS.

Click here for more information

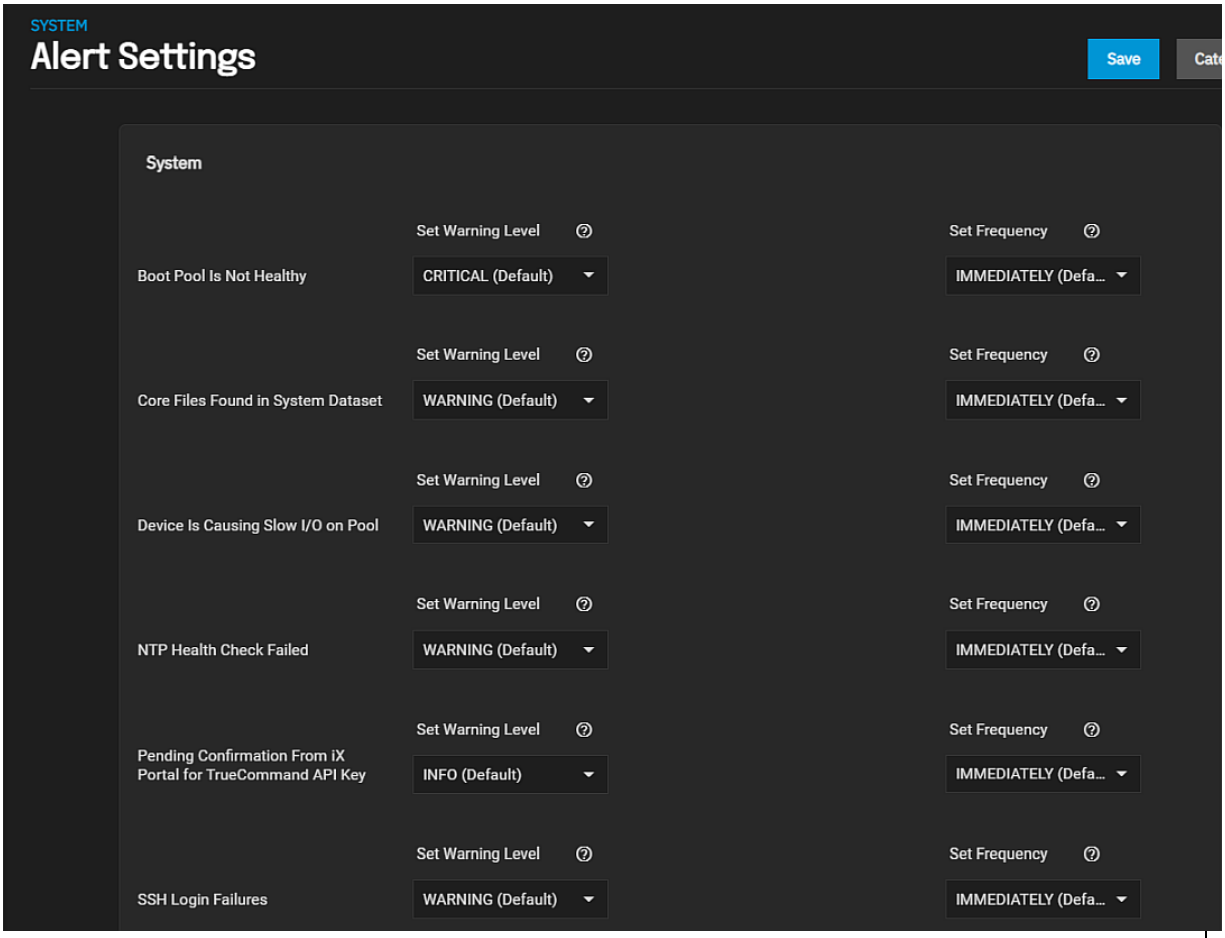


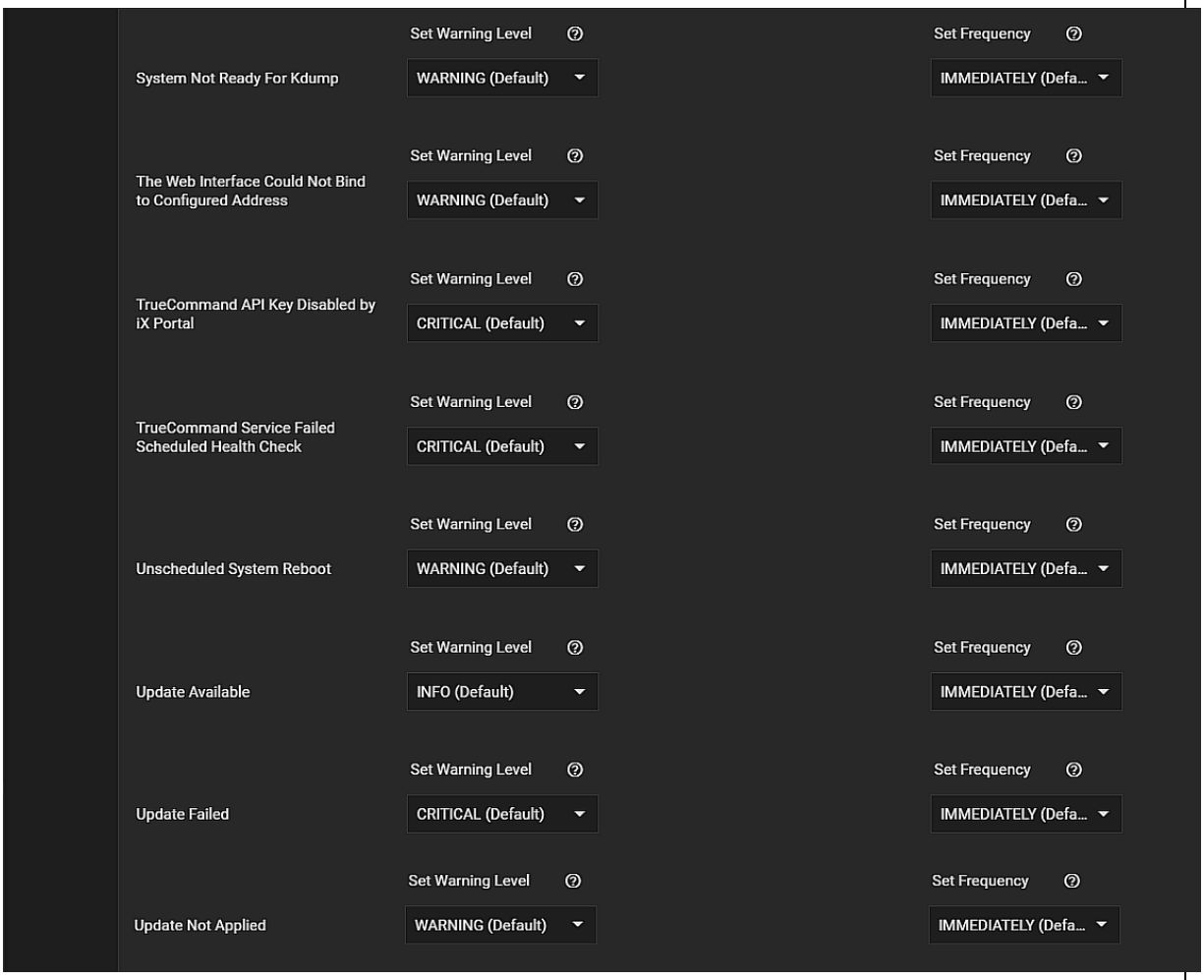
Options cover critical quota exceeded on dataset, new feature flags available for pools, pool space usage above 80% or 90%, pool status not healthy, quota exceeded on dataset, paused scrub, too many snapshots exist and too many snapshots exist for dataset.

System Alert Settings

System alert settings apply to system processes, system dataset, TrueCommand API Key, SSH logins, system reboots, updates and the web interface.

Click here for more information


SYSTEM
Alert Settings
Save
Cate
System
Set Warning Level
Set Frequency
Boot Pool Is Not Healthy
CRITICAL (Default)
IMMEDIATELY (Defa...
Core Files Found in System Dataset
WARNING (Default)
Device Is Causing Slow I/O on Pool
NTP Health Check Failed
Pending Confirmation From iX Portal for TrueCommand API Key
INFO (Default)
SSH Login Failures

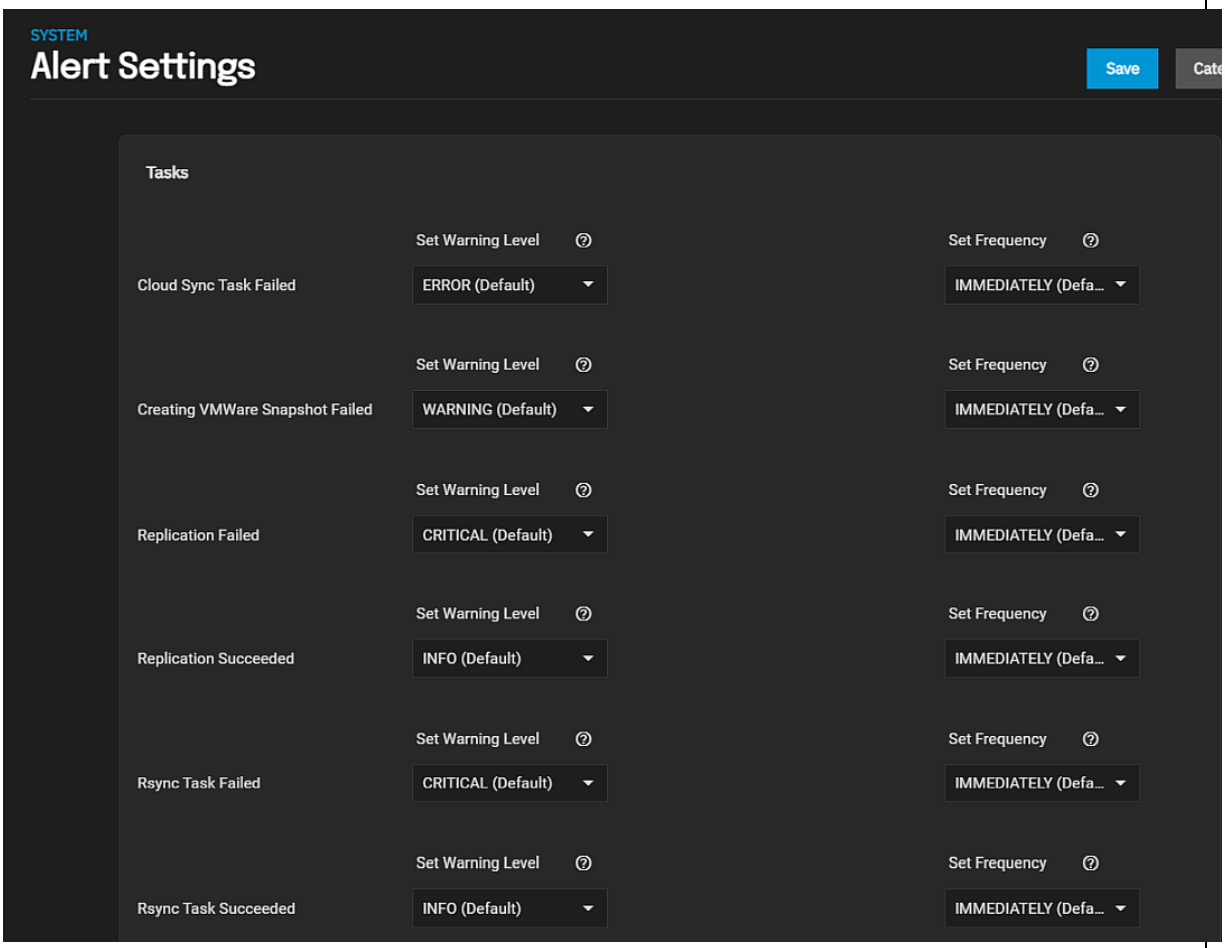

System Not Ready For Kdump
WARNING (Default)
IMMEDIATELY (Defa...
The Web Interface Could Not Bind to Configured Address
TrueCommand API Key Disabled by iX Portal
CRITICAL (Default)
TrueCommand Service Failed Scheduled Health Check
Unscheduled System Reboot
Update Available
INFO (Default)
Update Failed
CRITICAL (Default)
Update Not Applied
WARNING (Default)

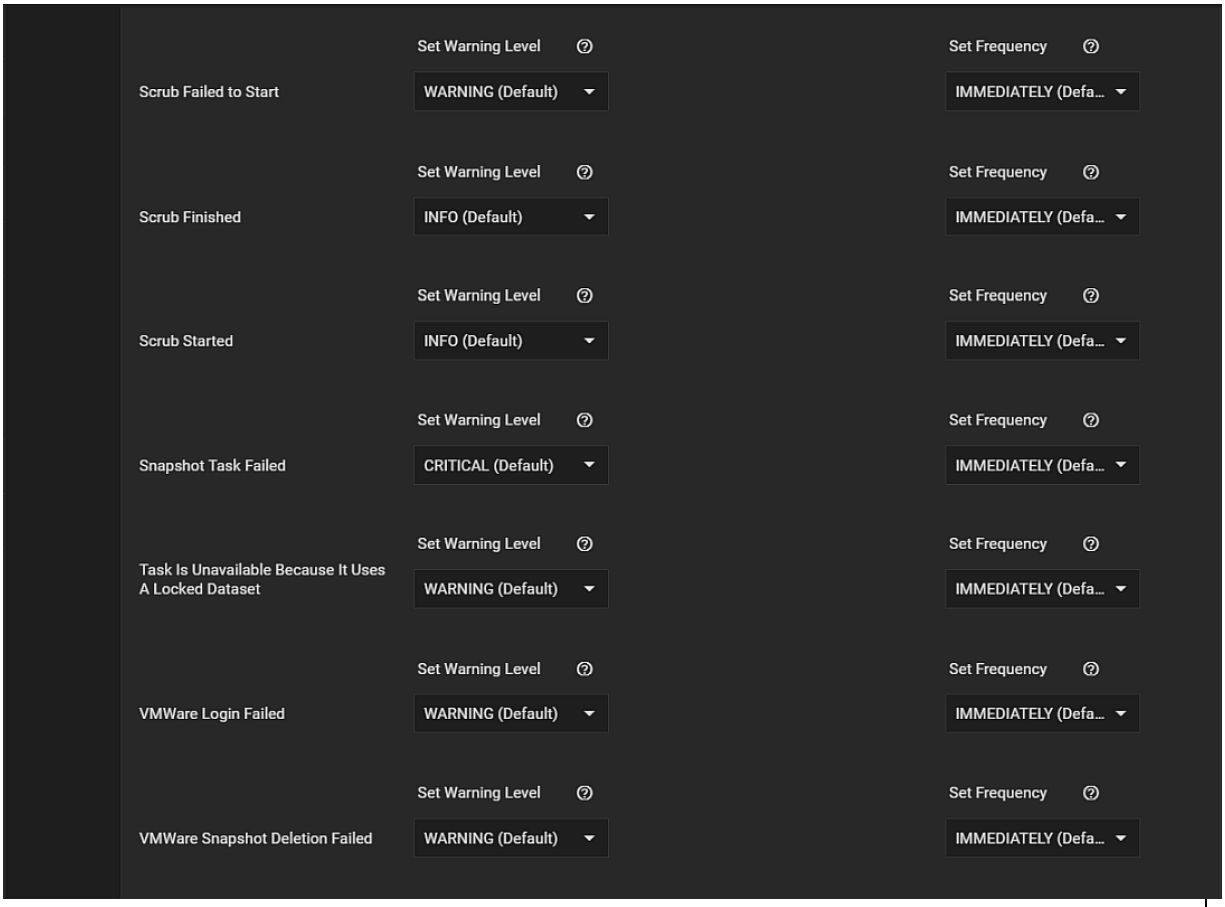
Options cover boot pool health, core files found in system dataset, device causing slow I/O on pool, failed NTP health checks, SSH login failures, system not ready for Kdump, web interface bind to configured address, TrueCommand API key disabled by iX portal, TrueCommand service failed scheduled health check, unscheduled system reboot, update available and failed and update not applied.

Task Alert Settings

Task alert settings apply to cloud sync, VMWare snapshots, replication, rsync, scrub and snapshot tasks scheduled on your TrueNAS.

Click here for more information



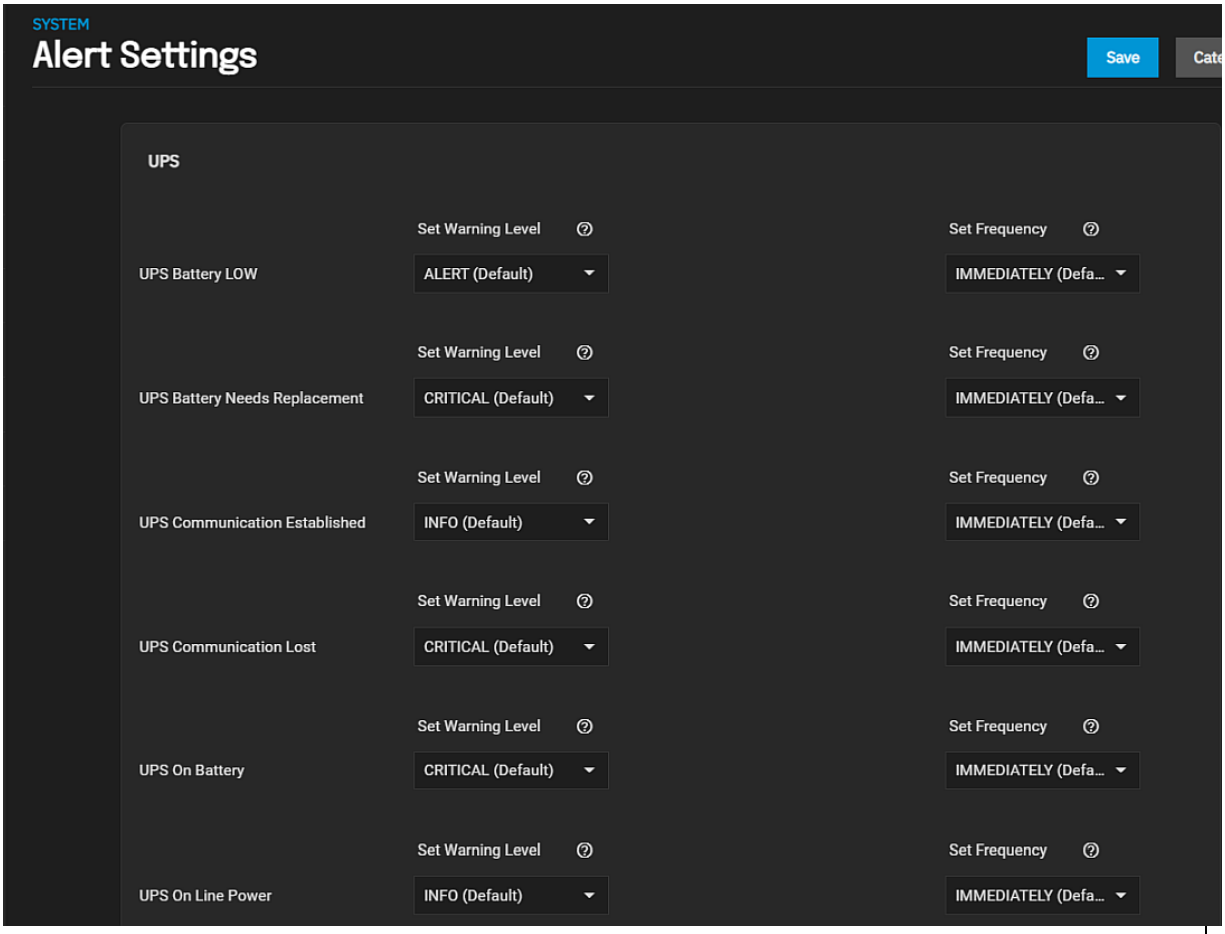


Options cover failed cloud sync, creating VMWare snapshot, replication, rsync, scrub and snapshot tasks, replication, rsync tasks succeeded, scrub task failed to start, it started or finished, a task is unavailable because it uses a locked dataset, VMWare login failed and VMWare snapshot deletion failed.

UPS Alert Settings

UPS alert settings apply to a UPS connected to your TrueNAS.

Click here for more information



Options cover UPS battery low, needs replacement, or that it is on batter power or line power, and lost or established UPS communication status.

Alert Warning Levels

Use the **Set Warning Level** dropdown list to customize alert importance. Each warning level has an icon and color to express the level of urgency.

To make the system email you when alerts with a specific warning level trigger, set up an email alert service with that warning level.

Level	Icon	Alert Notification?
INFO		No
NOTICE		Yes
WARNING		Yes
ERROR		Yes
CRITICAL		Yes
ALERT		Yes
EMERGENCY		Yes

Alert Frequency

Use the **Set Frequency** dropdown list to adjust how often the system sends or displays alert notifications.

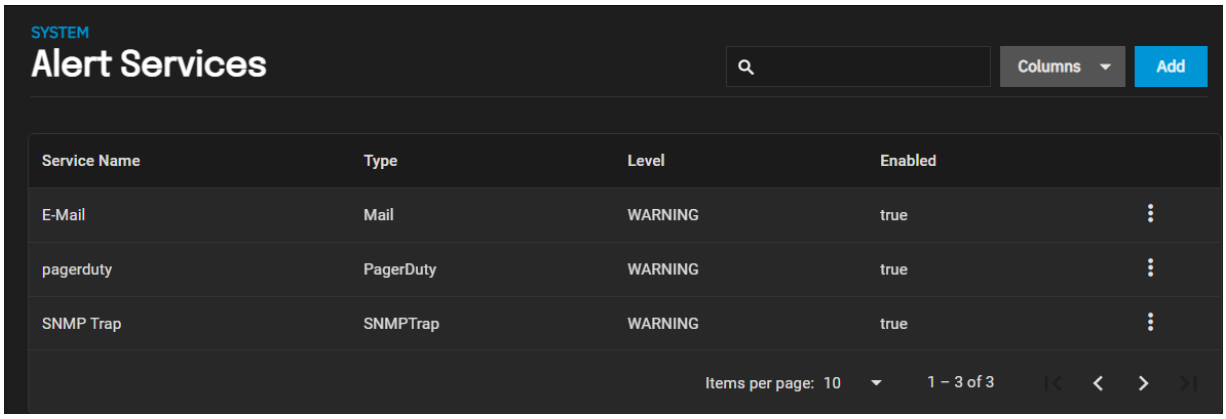
Alert frequencies options are **Immediately (Default)**, **Hourly**, **Daily** or **Never**. Setting the **Frequency** to **Never** prevents that alert from displaying in the **Alerts Notification** dialog, but it still pops up in the UI if triggered.

Related Content

- Alert Services Screens

4.2.1.2 - Alert Services Screens

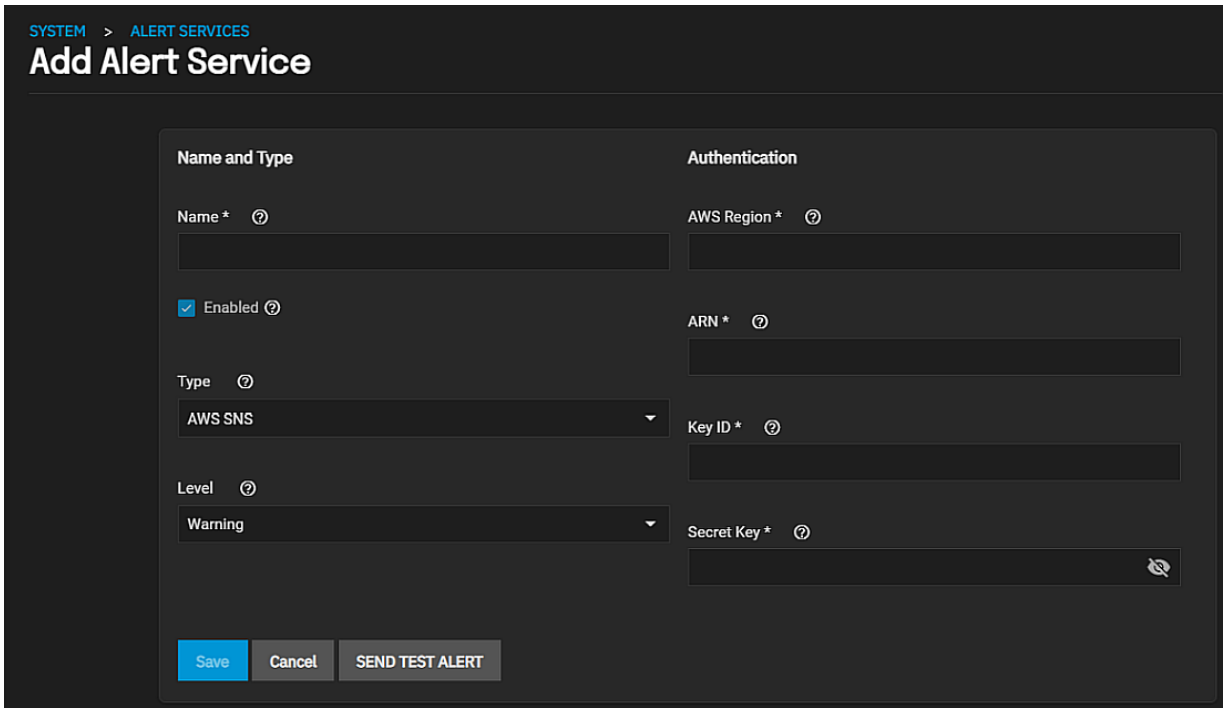
The **Alert Services** screen has options to create and edit alert services.



Use **Columns** to change the information displayed in the list of alert services. Options are **Unselect All**, **Type**, **Level**, **Enabled** and **Reset to Defaults**.

Add Alert Service Screen

Use **Add** to create a new alert service using the **Add Alert Service** screen. The **Type** settings for **AWS SNS** display by default. To add an alert service for another option, use the **Type** dropdown list. Only the **Authentication Settings** change for each option.



Name and Type Settings

Setting	Description
Name	Enter a name for the new alert service.
Enabled	Clear the checkmark to disable this service without deleting it.
Type	Select an option from the dropdown list for an alert service to display options for that service. Options are **AWS SNS** which is the default type displayed, **E-Mail**, **InfluxDB**, **Mattermost**, **OpsGenie**, **PagerDuty**, **Slack**, **SNMP Trap**, **Telegram** or **VictorOPS**.
Level	Select the level of severity from the dropdown list. Options are **Info**, **Notice**, **Warning**, **Error**, **Critical**, **Alert** or **Emergency**.

AWS SNS Authentication Settings

Setting	Description
AWS Region	Enter the AWS account region.
ARN	Topic Amazon Resource Name (ARN) for publishing. For example, *arn:aws:sns:us-west-2:111122223333:MyTopic*.
Key ID	Enter the access key ID for the linked AWS account.
Secret Key	Secret access key for the linked AWS account.

Use **SEND TEST ALERT** to generate a test alert to confirm the alert service works.

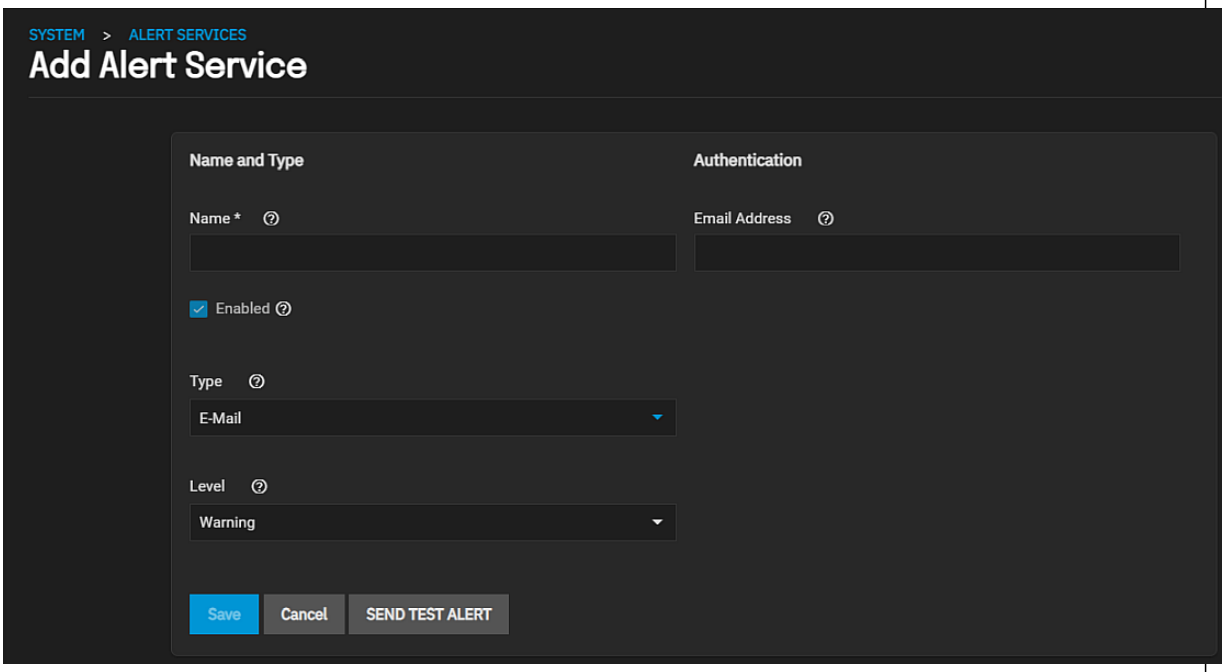
Cancel exist to the **Alert Services** screen without saving.

Use **Save** to add the new service with the settings you specify to the list of alert services.

Email Authentication Settings

Click here for more information

Select **Email** from the **Type** dropdown list to display email authentication settings.



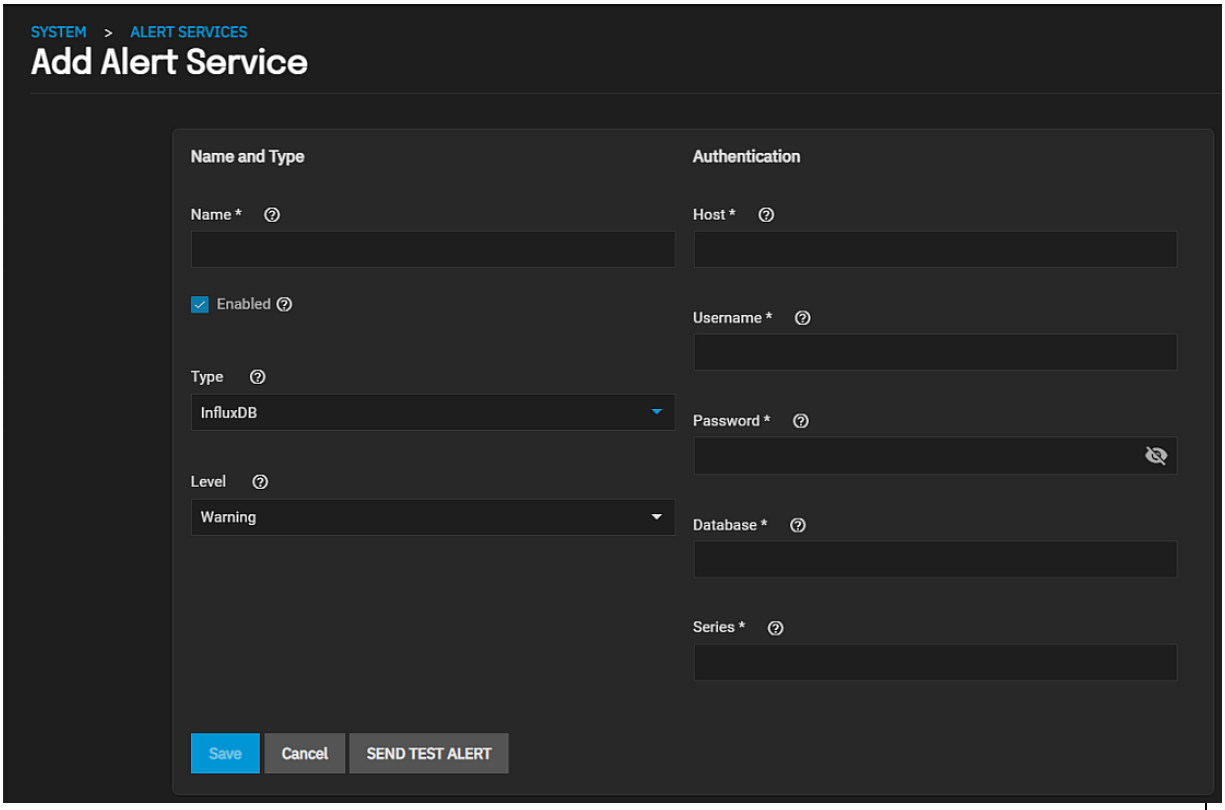
Authentication Settings

Setting	Description
Email Address	Enter the a valid email address to receive alerts from this TrueNAS system.

InfluxDB Authentication Settings

Click here for more information

Select **InfluxDB** from the **Type** dropdown list to display InfluxDB authentication settings.



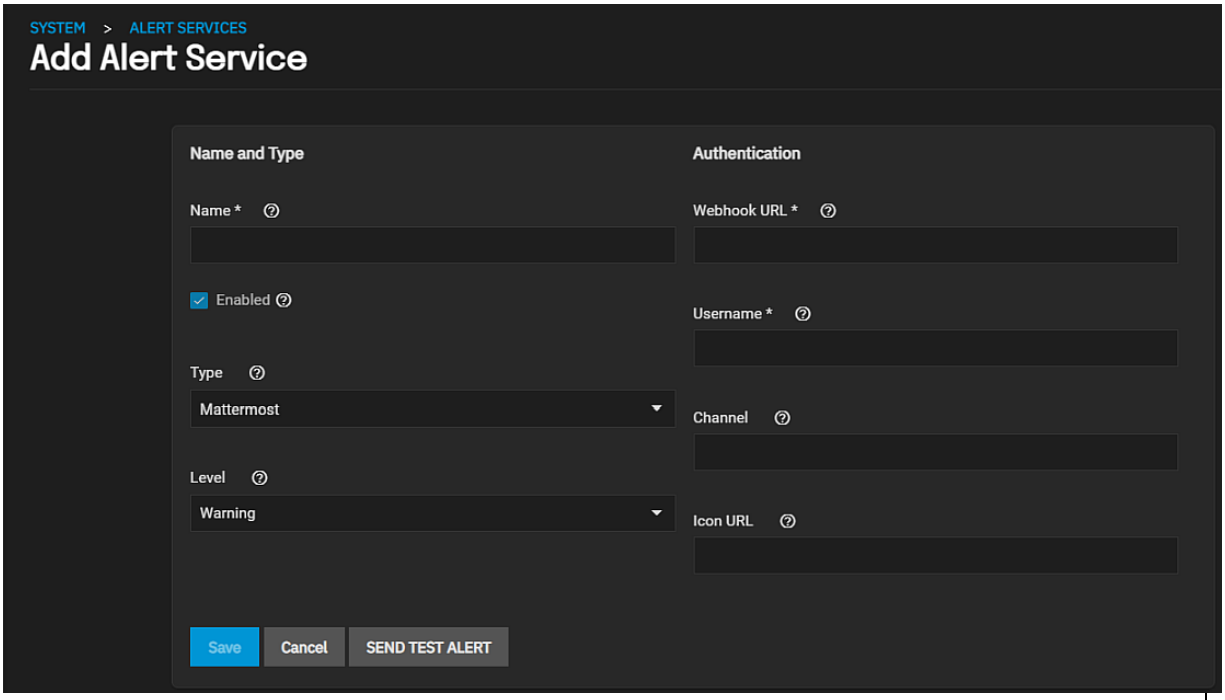
Authentication Settings

Setting	Description
Host	Enter the InfluxDB host name.
Username	Enter the user name for this service.
Password	Enter the password for the user on this service
Database	Enter the name of the InfluxDB database.
Series	Enter the name for the InfluxDB time series name for collected points.

MatterMost Authentication Settings

Click here for more information

Select **Mattermost** from the **Type** dropdown list to display Mattermost authentication settings.



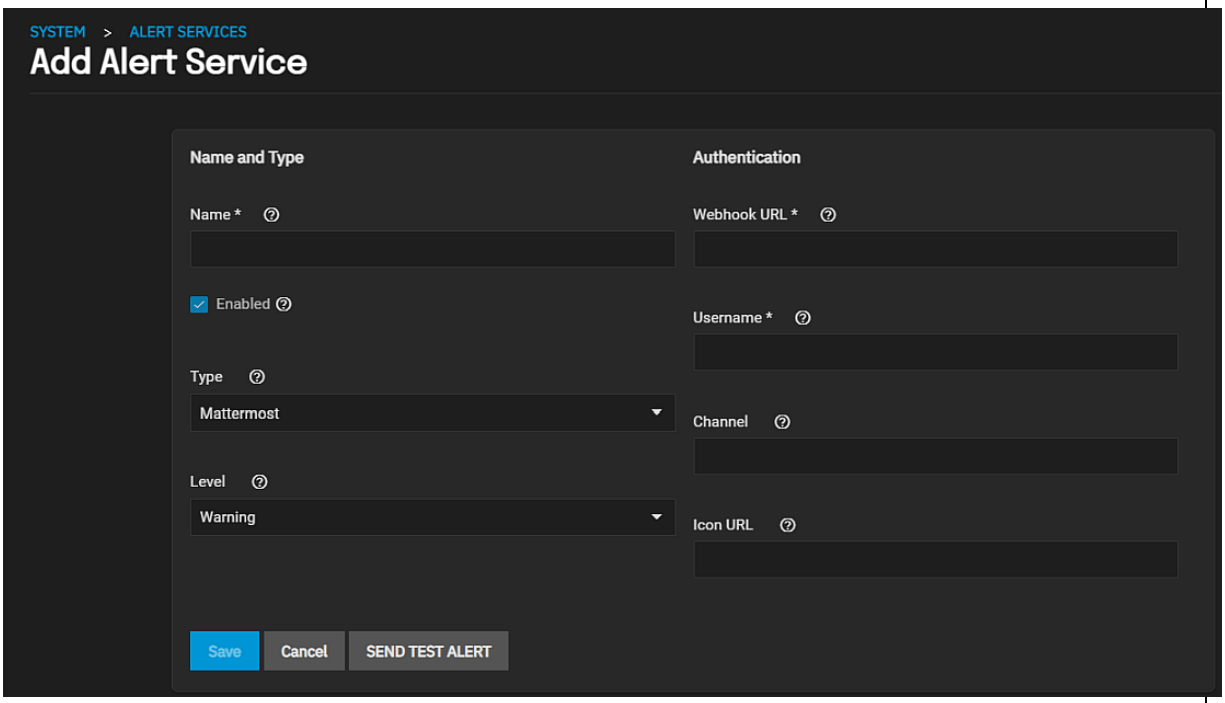
Authentication Settings

Setting	Description
Webhoot URL	Enter or past the incoming webhook URL assoicated with this service.
Username	Enter the Mattermost user name.
Channel	Enter the name of the channel to receive notifications. This overrides the default channel in the incoming webhot settings.
Icon URL	Enter the icon file to use as the profile picture for new messages. For example, *https://mattermost.org/wp-content/uploads/2016/04/icon.png*. Requires configuring Mattermost to override profile picture icons.

OpsGenie Authentication Settings

Click here for more information

Select **OpsGenie** from the **Type** dropdown list to display OpsGenie authentication settings.



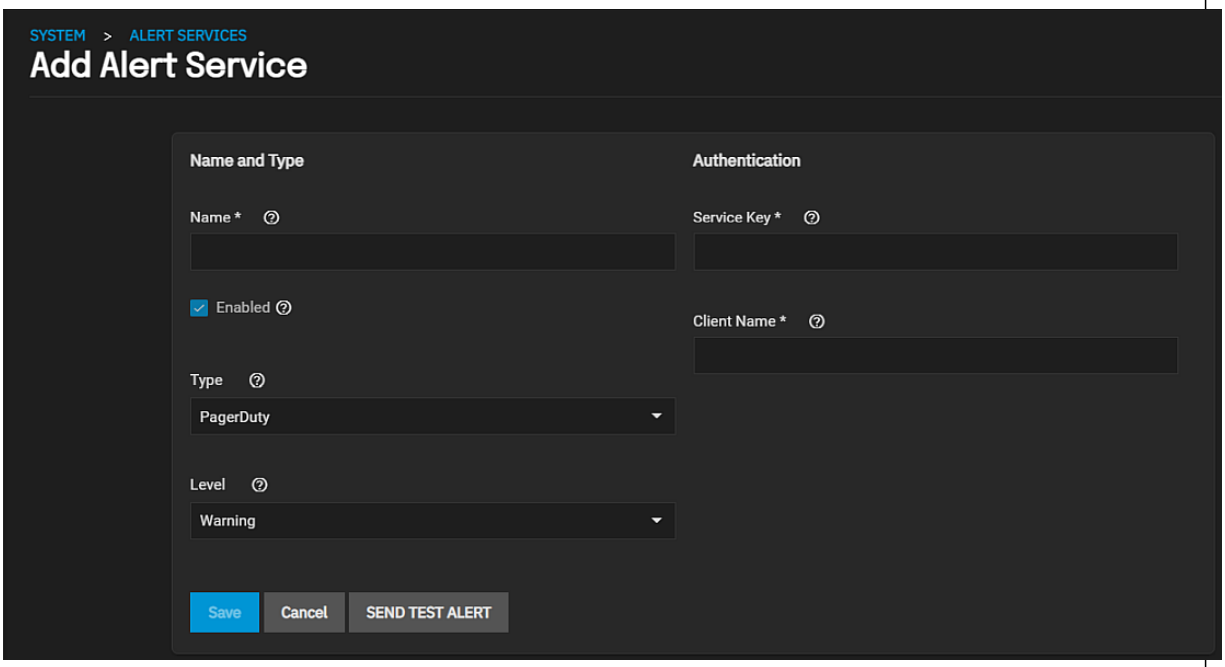
Authentication Settings

Setting	Description
API Key	Enter the API key. Find the API key by signing into the OpsGenie web interface and going to **Integrations/Configured Integrations**. Click the desired integration, **Settings**, and read the **API Key** field.
API URL	Leave empty for default (OpsGenie API).

PagerDuty Authentication Settings

Click here for more information

Select **PagerDuty** from the **Type** dropdown list to display PagerDuty authentication settings.



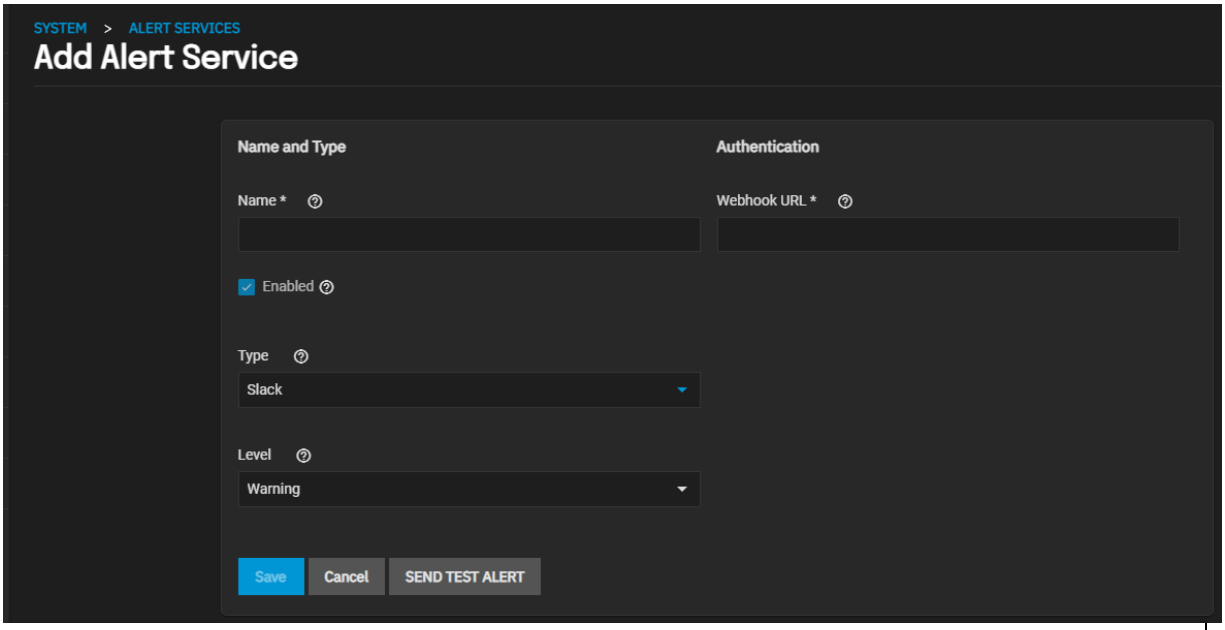
Authentication Settings

Setting	Description
Service Key	Enter or paste the **integration/service** key for this system to access the PagerDuty API.
Client Name	Enter the PagerDuty client name.

Slack Authentication Settings

Click here for more information

Select **Slack** from the **Type** dropdown list to display Slack authentication settings.



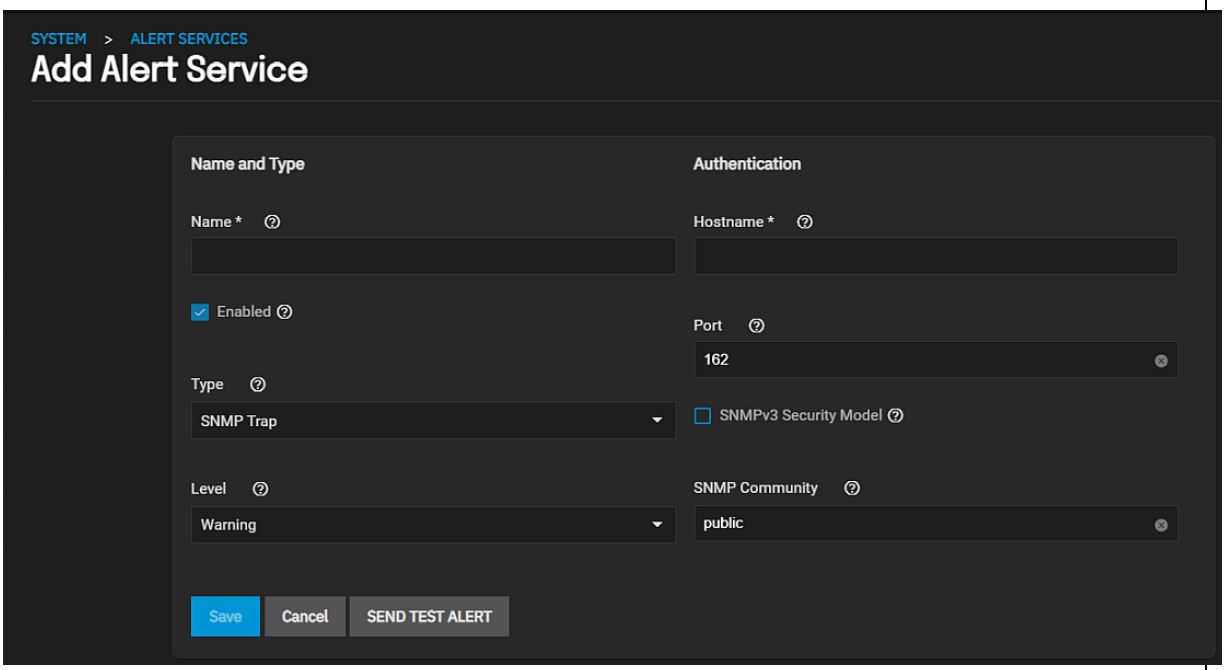
Authentication Settings

Setting	Description
Webhook URL	Paste the incoming webhook URL assoicated with this service.

SNMP Trap Authentication Settings

Click here for more information

Select **SNMP Trap** from the **Type** dropdown list to display SNMP trap authentication settings.



Authentication Settings

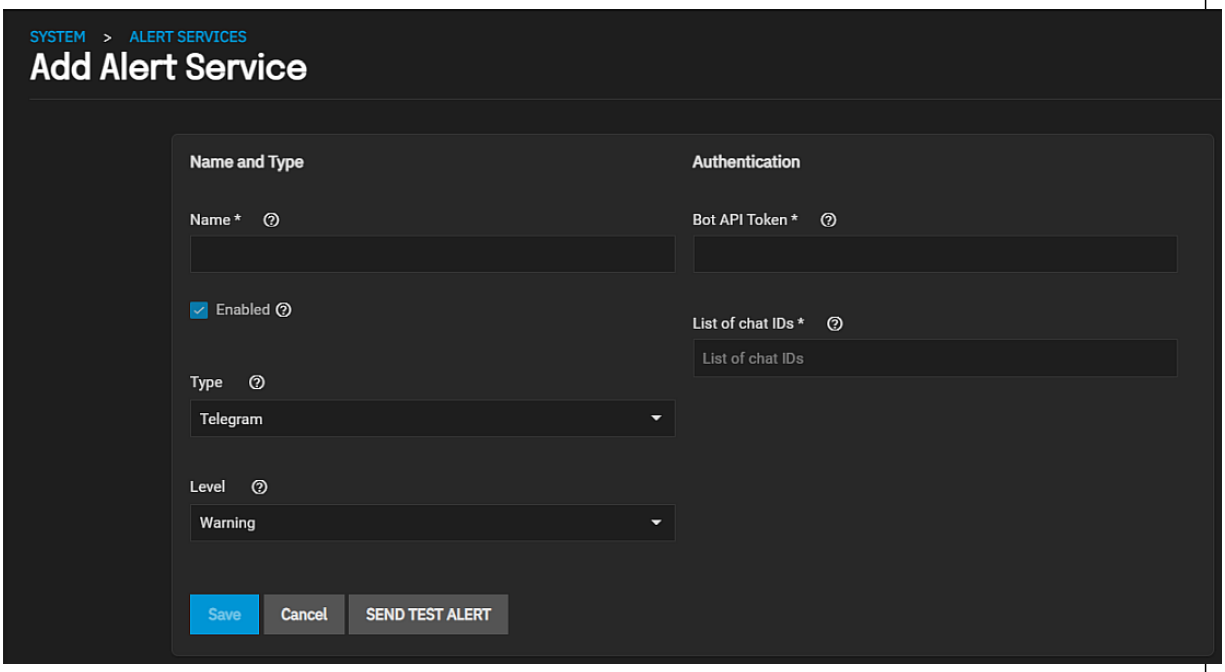
Setting	Description
Hostname	Enter the host name or IP address of the system to receive SNMP trap notifications.
Port	Enter the UDP port number on the system receiving SNMP trap notifications. The default is **162**.
SNMPv3 Security Model	Select to enable the SNMPv3 security model.
SNMP Community	Enter the network community string. The community string acts like a user ID or password. A user with the correct community string has access to network information. the default is *public*. For more

Setting	Description
	information, see What is an SNMP Community String?.

Telegram Authentication Settings

Click here for more information

Select **Telegram** from the **Type** dropdown list to display Telegram authentication settings.



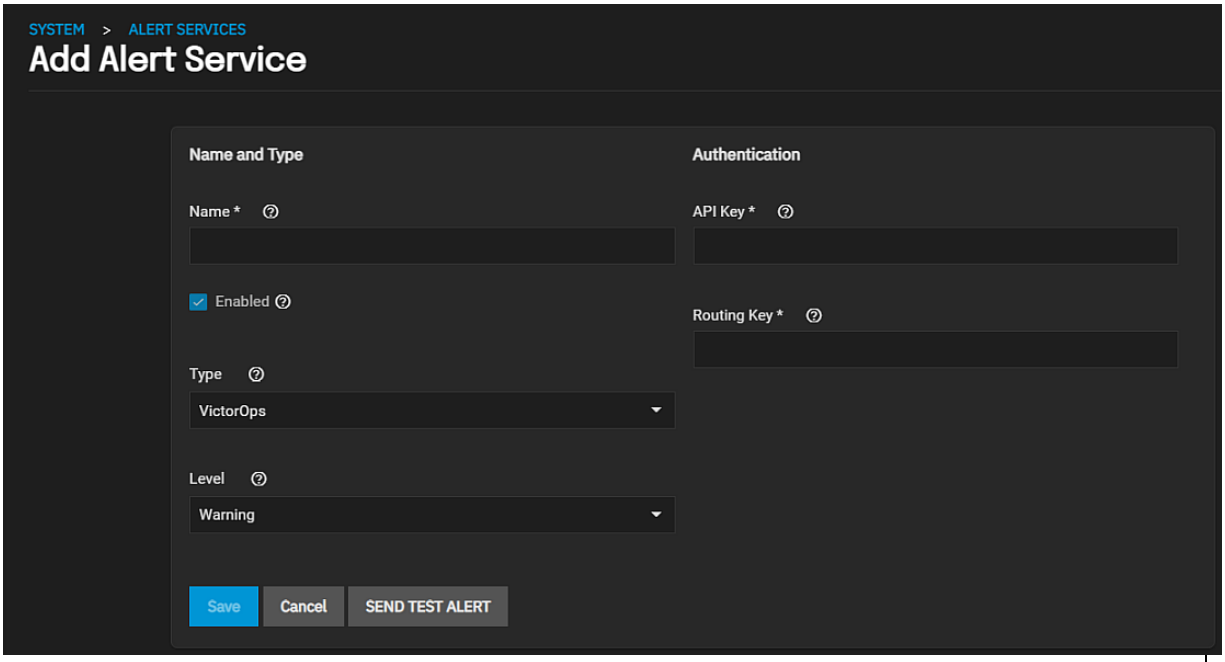
Authentication Settings

Setting	Description
Bot API Token	Enter the Telegram Bot API Token How to create a Telegram Bot.
List of chat IDs	Enter a list of chat IDs separated by space ( ), comma (,) or semicolon (;). To find your chat ID send a message to the bot, group or channel and visit https://core.telegram.org/bots/api#getting-updates.

VictorOPS Authentication Settings

Click here for more information

Select **VictorOps** from the **Type** dropdown list to display VictorOps authentication settings.

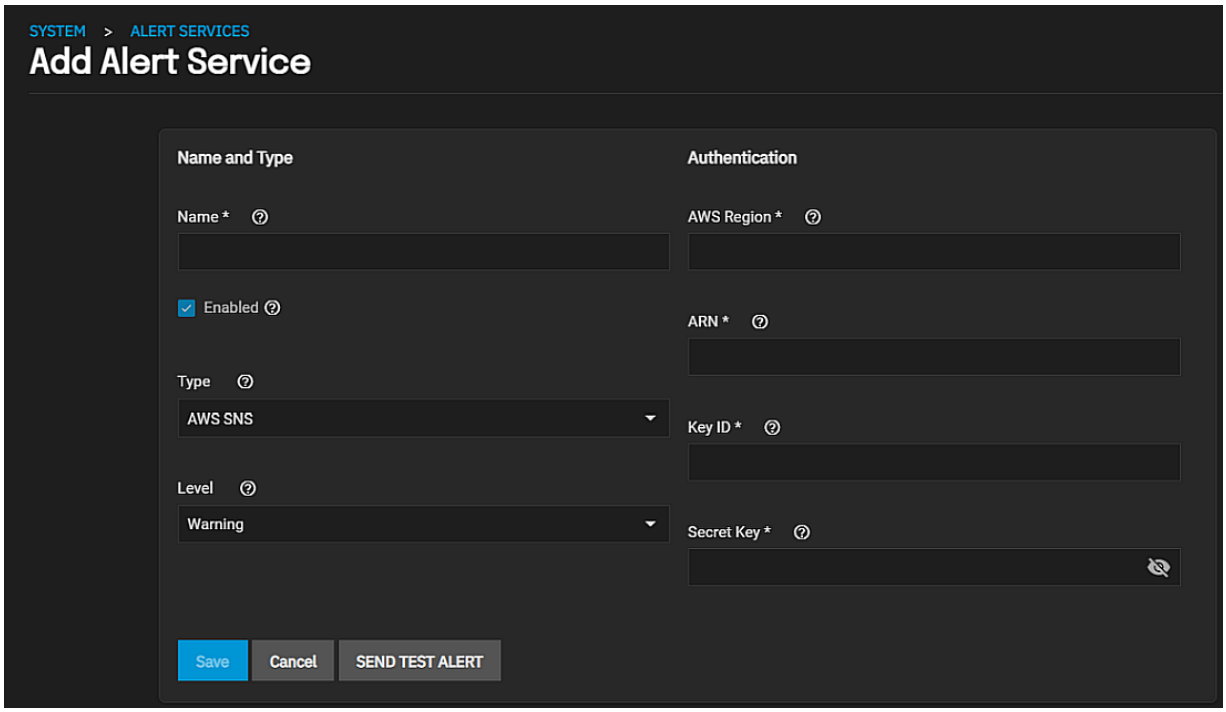


Authentication Settings

Setting	Description
API Key	Enter or paste the VictorOps API key.
Routing Key	Enter or past the VictorOps routing key.

Edit Alert Service Screen

Use the **Edit Alert Service** screen to modify settings for a service. Select the ⋮ icon for the service, and then click **Edit** to display the **Edit Alert Service** screen.



Name and Type Settings

Setting	Description
Name	Enter a name for the new alert service.
Enabled	Clear the checkmark to disable this service without deleting it.

Setting	Description
Type	Select an option from the drop down list for an alert service to display options for that service. Options are **AWS SNS**, **E-Mail**, **InfluxDB**, **Mattermost**, **OpsGenie**, **PagerDuty**, **Slack**, **SNMP Trap**, **Telegram** or **VictorOPS**.
Level	Select the level of severity from the dropdown list. Options are **Info**, **Notice**, **Warning**, **Error**, **Critical**, **Alert** or **Emergency**.

Authentication Settings

Setting	Description
Email Address	Enter a valid email address to receive alerts from this system.

Use **SEND TEST ALERT** to generate a test alert to confirm the alert service works.

Cancel exist to the **Alert Services** screen without saving.

Use **Save** to keep any changes made.

Related Content

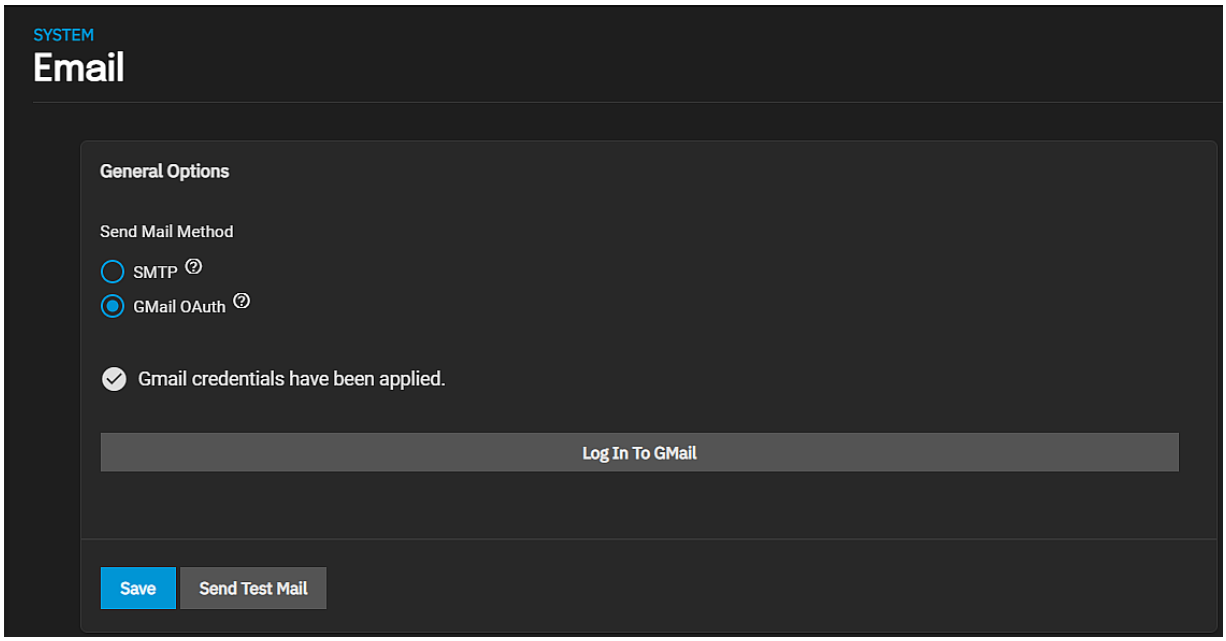
- Alert Settings Screens

4.2.1.3 - Email Screens

The **Email** screens lets you set up a system email address using one of two options to set up email. Select either an **SMTP** or **GMail OAuth** setup. The screen changes based on the selected radio button. **Gmail OAutH** is the default screen and option.

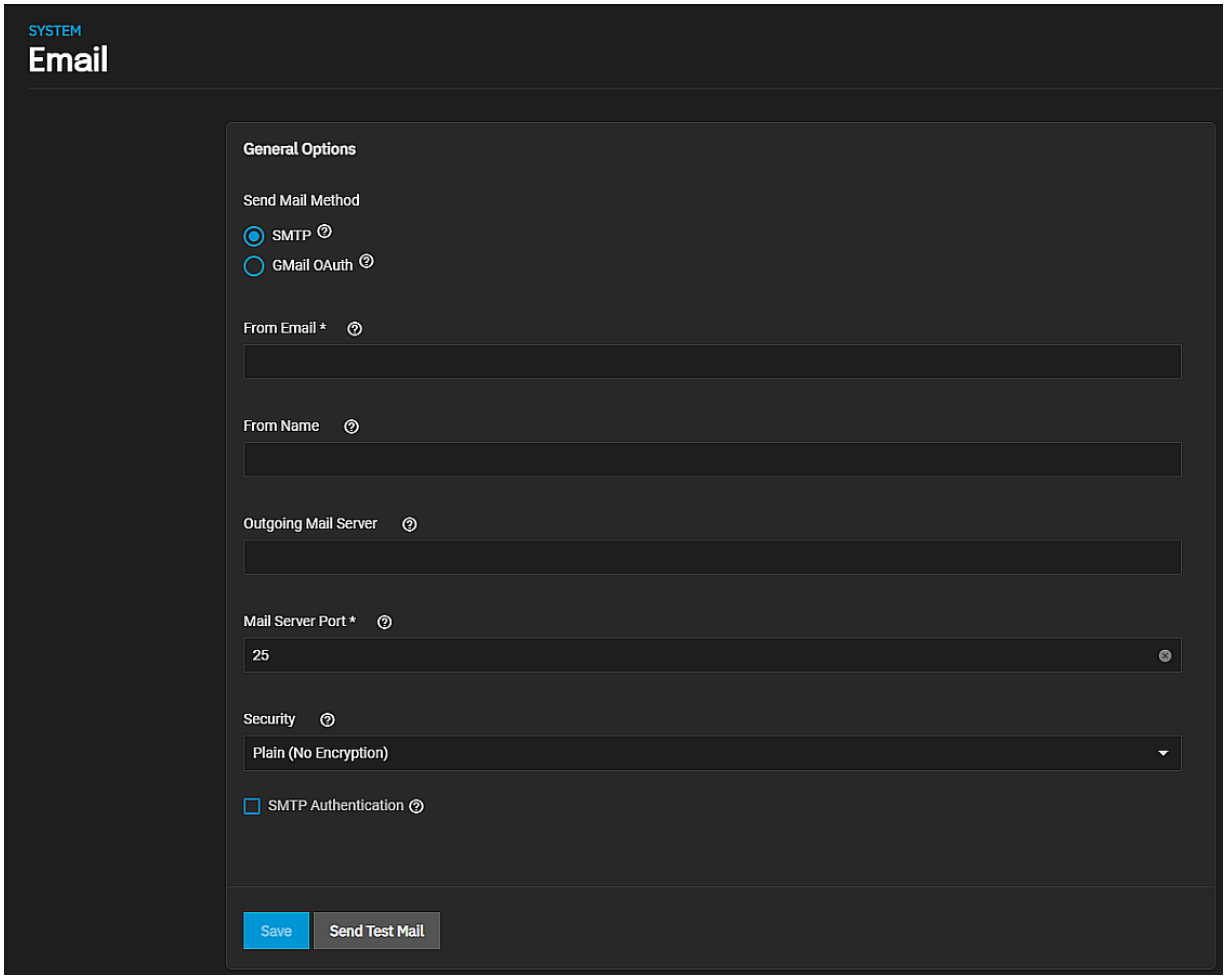
Email GMail OAuth Screen

The default **GMail OAuth** screen display changes after you select **Login In To GMail** and complete the authentication process for Gmail.



The **Send Test Mail** button generates a test email to confirm the system email works correctly.

Email SMTP Screen



Setting	Description
From Email	The user account Email address to use for the envelope From email address. You must configure the user account email first in **Accounts > Users > Edit**.
From Name	The friendly name to show in front of the sending email address. Example: *Storage System 01it@example.com*
Outgoing Mail Server	Host name or IP address of SMTP server to use for sending this email.
Mail Server Port	MTP port number. Typically 25,465 (secure SMTP), or 587 (submission).
Security	Select the security option from the dropdown list. Options are **Plain (No Encryption)**, **SSL (Implicit TLS)**, or **TLS (STARTTLS)**. See email encryption for more information on types.
SMTP Authentication	Select to enable SMTP AUTH using PLAIN SASL. Requires a valid user name and password.

Related Content

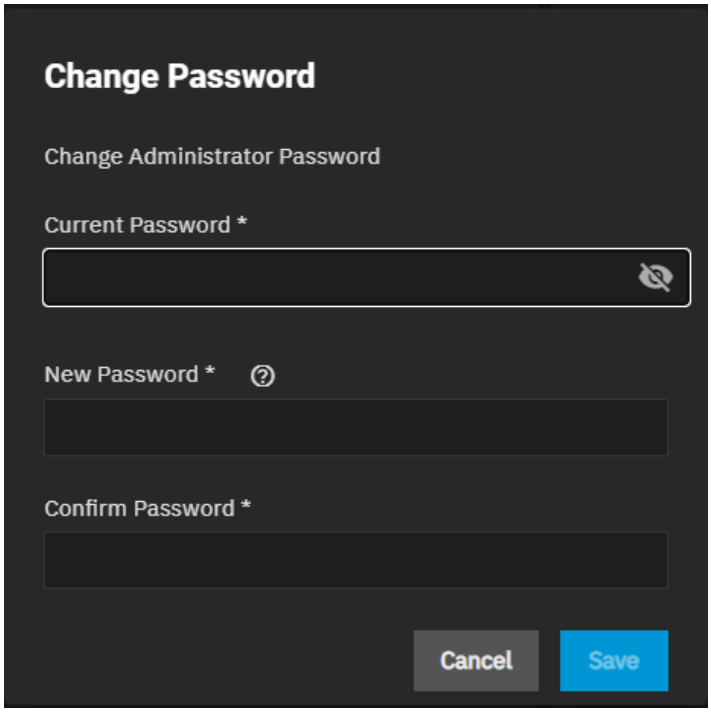
- Setting Up System Email

4.2.2 - Settings Options

The **Settings** icon button displays a menu of general system settings options. The options are **Change Password**, **Preferences**, **API Keys**, **Guide** and **About**.

Change Password

Click on the **Change Password** icon button to display the change password dialog where you can change the currently logged-in user password.



Click on the icon to display the password entered. To stop displaying the password, click on the icon.

Preferences

Click on **Preferences** to dispaly the **Web Interface Preferneces** screen where you can change general system settings such as the color theme.

API Keys

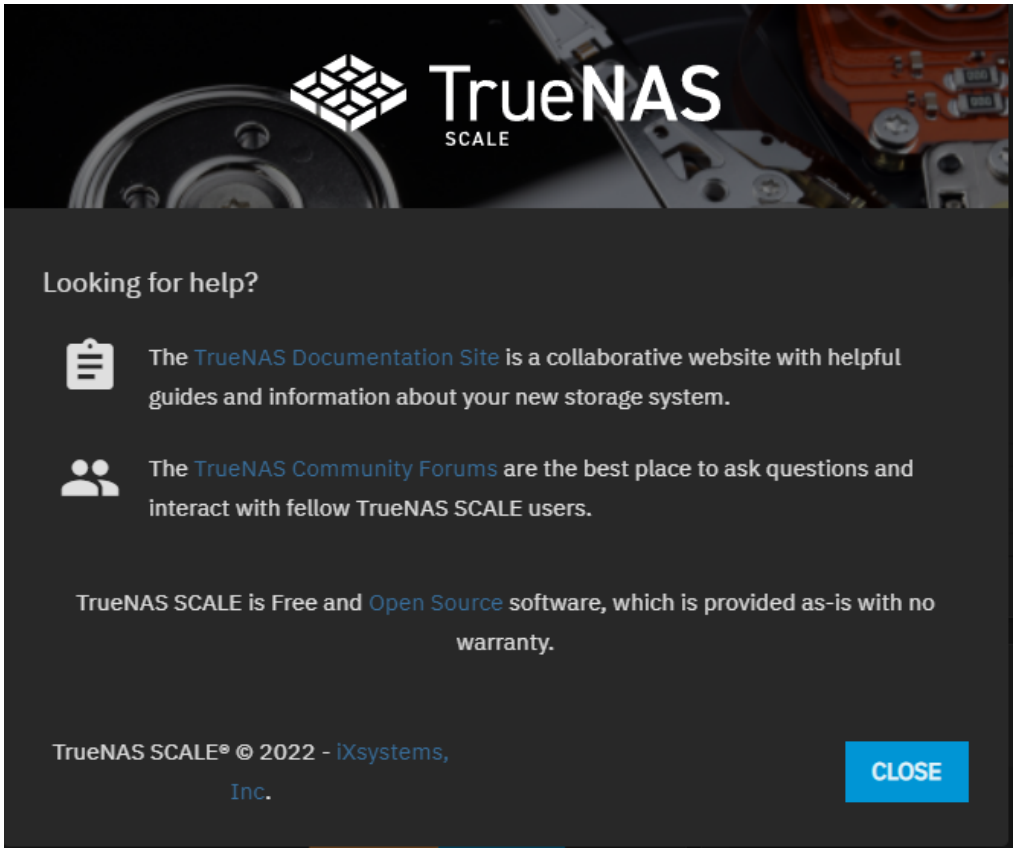
Click on **API Keys** to display the **API Keys** screen where you can add new or manage existing API keys on your system.

Guide

Click on **Guide** to display the TrueNAS Documentation Hub in a new tab.

About

Click on **About** to display the information window links to the TrueNAS Documentation Hub, TrueNAS Community Forums, FreeNAS Open Source Storage Appliance GitHub repository, and iXsystems home page.

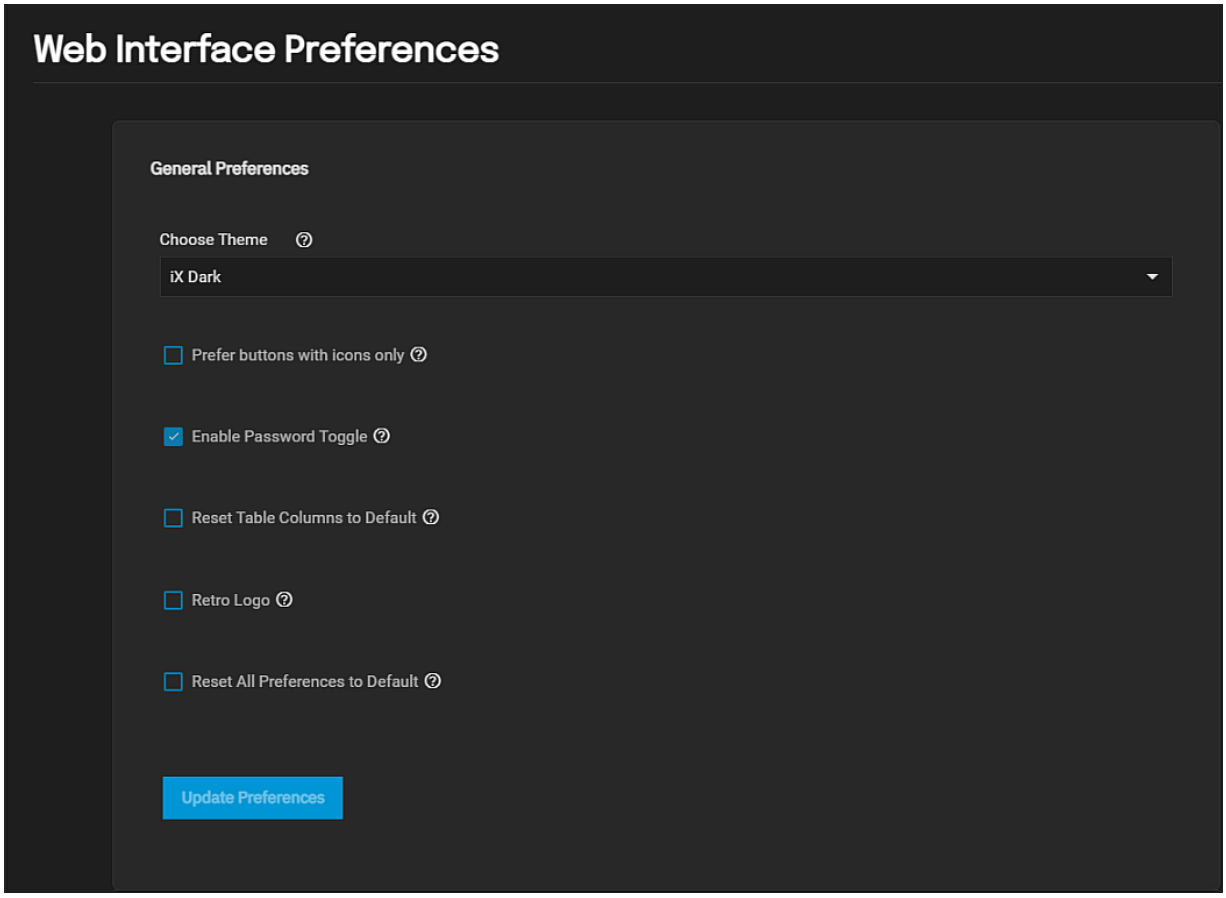


Related Information

- Web Interface Preference Screen
- API Keys Screen

4.2.2.1 - Web Interface Preference Screen

Use the **Web Interface Preferences** screen, accessed from the top toolbar **Settings** menu, to select general system preferences for your TrueNAS system.



Setting	Description
Choose Theme	Select a preferred color theme from the dropdown list of eight options.
Prefer buttons with icons only	Select to preserve screen space by displaying icons and tooltips instead of text labels.
Enable Password Toggle	Select to display an eye icon next to password fields. Click the icon to reveal the password.
Reset Table Columns to Default	Select to reset all tables to display default columns.
Retro Logo	Select to change the UI TrueNAS branding to FreeNAS.
Reset All Preferences to Default	Select to reset all user preferences to their default values (custom themes are preserved).

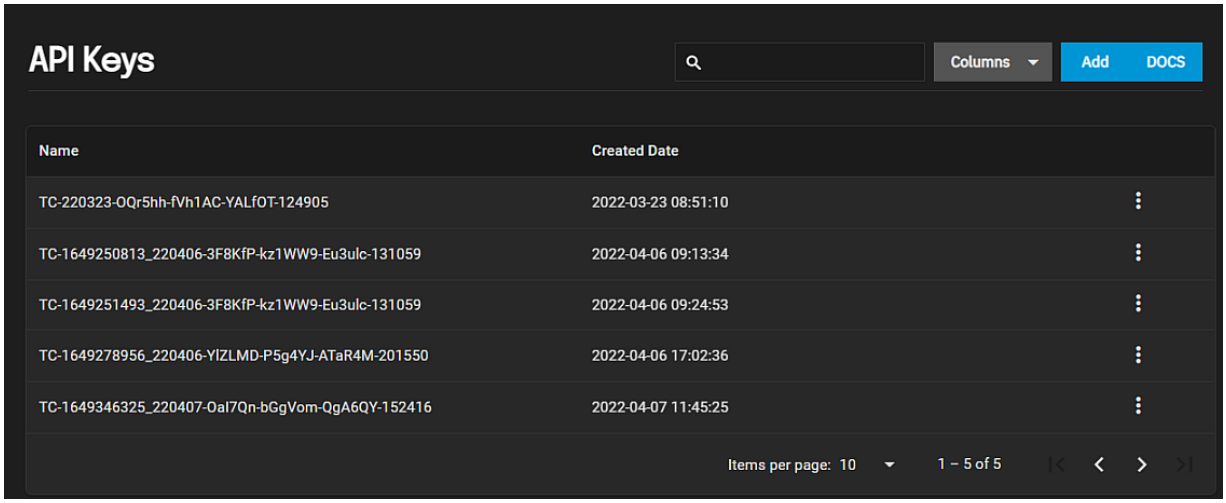
Use **Update Preferences** to save changes. A green circle with a checkmark briefly displays to validate the changes made are saved and implemented.

Related Content

- Settings Options
- Getting Support
- Managing Advanced Settings
- Managing Cron Jobs
- Managing the Console Setup Menu
- Managing the System Configuration
- General Settings Screen
- Managing General Settings
- Managing System Logging

4.2.2.2 - API Keys Screen

The **API Keys** option on the top toolbar **Settings** dropdown menu displays the **API Keys** screen. This screen displays a list of API keys added to your TrueNAS.



Use the **Column** button to display options to customize information in the list of API keys. Options are **Unselect All**, **Created Date** and **Reset to Defaults**.

Click the icon to the right of an API key to display options for that key. API key options are **Edit** and **Delete**.

Use **Add** to add a new API key to your TrueNAS.

> Always back up and secure keys. The key string displays only one time, at creation!

API Key Documentation

Click **DOCS** to access API documentation for your system.

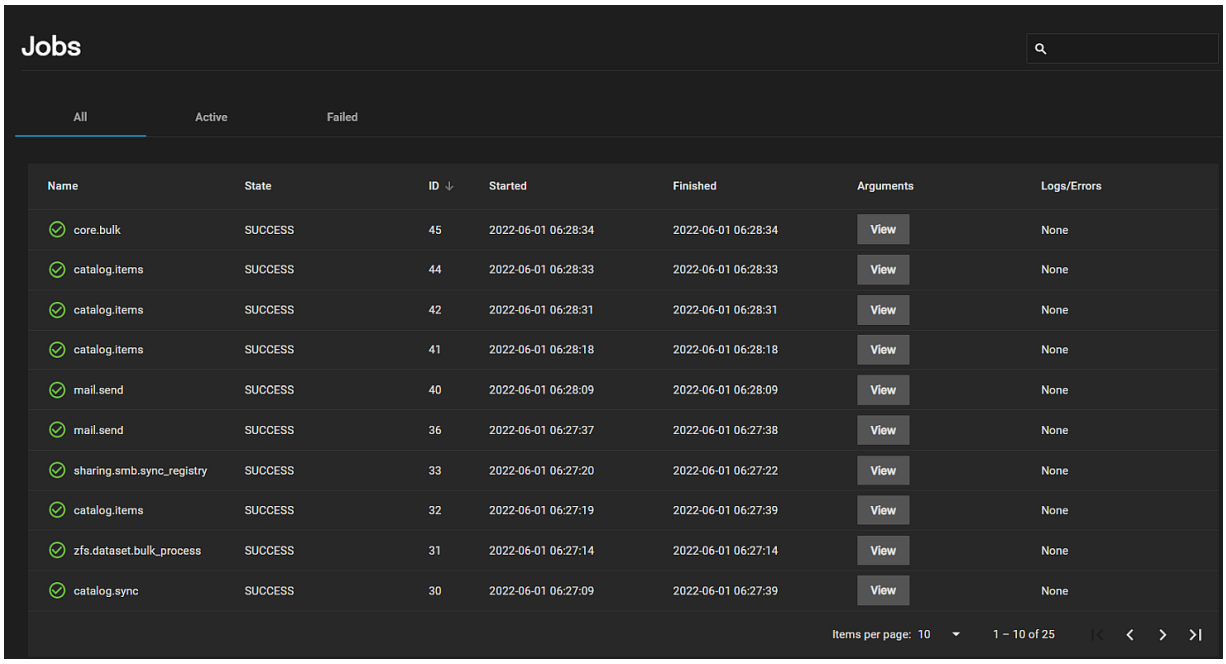
Related Content

- Managing API Keys

4.2.3 - Jobs Screens

The **Jobs** screens, accessed from the **Task Manager** after clicking **History**, displays all jobs executed on the system.

There are three tab views, **All**, **Active** and **Failed**. **All** displays by default.



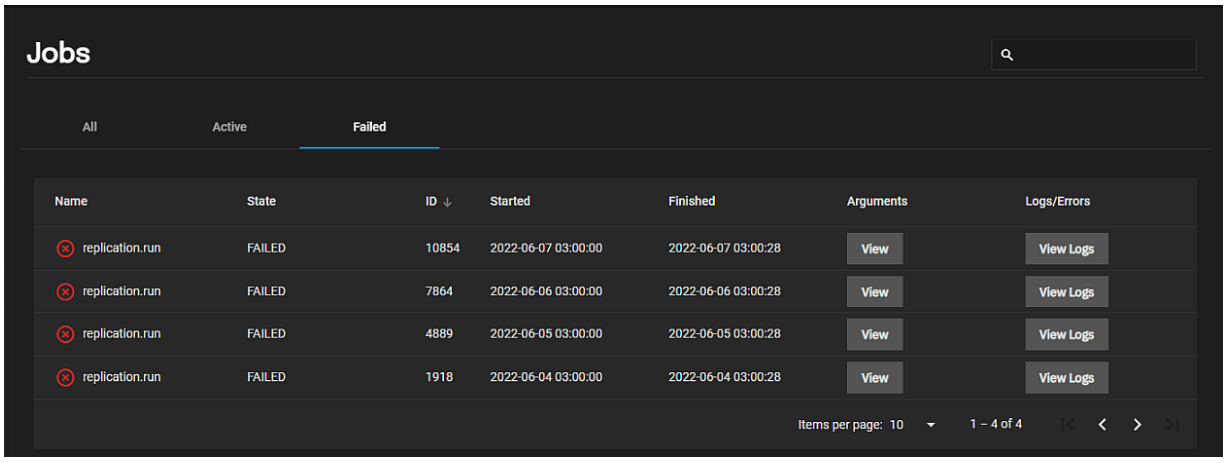
Use the arrow display options to change the number of jobs per screen. Options are the default **10**, **50** or **100**.

Click **View** to display the argument passed for the selected job.

Use the north arrow beside the **State** or **ID** header to change the display order, or the south arrow to return to the top down display order.

Failed Jobs Screen

The **Failed** screen displays the list of failed jobs.



Use the **View Logs** button to display the task log. The system error for this failed job displays at the bottom of the log file.

Related Content

- Top Toolbar
- Top Toolbar Options

4.3 - Storage

The SCALE Storage section has controls for pool, snapshot, and disk management.

The storage section also has options for datasets, Zvols, and permissions.

SCALE supports clustering storage across multiple systems. See TrueCommand Clustering for more details.

Ready to get started? Choose a topic or article from the left-side **Navigation** pane. Click the **<** symbol to expand the menu to show the topics under this section.

Storage Article Summaries

4.3.1 - Pools

TruenAS uses ZFS data storage *pools* to efficiently store and protect data.

What is a pool?
Storage pools are attached drives organized into virtual devices (*vdevs*). ZFS and TrueNAS periodically review and *heal* when discovering a bad block in a pool. Drives are arranged inside vdevs to provide varying amounts of redundancy and performance. Combined, ZFS and vdevs combined create high-performance pools, pools that maximize data lifetime, and all situations in between.

Review Storage Needs

We strongly recommend users review the available system resources and plan the storage use case before creating a storage pool.

- Allocating more drives to a pool increases redundancy when storing critical information.
- Maximizing total available storage at the expense of redundancy or performance entails allocating large-volume disks and configuring a pool for minimal redundancy.
- Maximizing pool performance entails installing and allocating high-speed SSD drives to a pool.

Determining your specific storage requirements is a critical step before creating a pool.

Pool Article Summaries

- Pool Screens

  This article provides information on Pool screens, settings and functions.

- Datasets Screens

  This article provides information on Datasets screens, settings and functions.

- Zvol Screens

  This article provides information on Zvol screen settings and functions.

- Edit ACL Screens

  This article describes the ACL permissions screens and settings for POSIX and NFSv4 ACLs, and the conditions that result in addition setting options.

- User and Group Quota Screens

  This article provides information on User and Group Quota screen settings and functions.

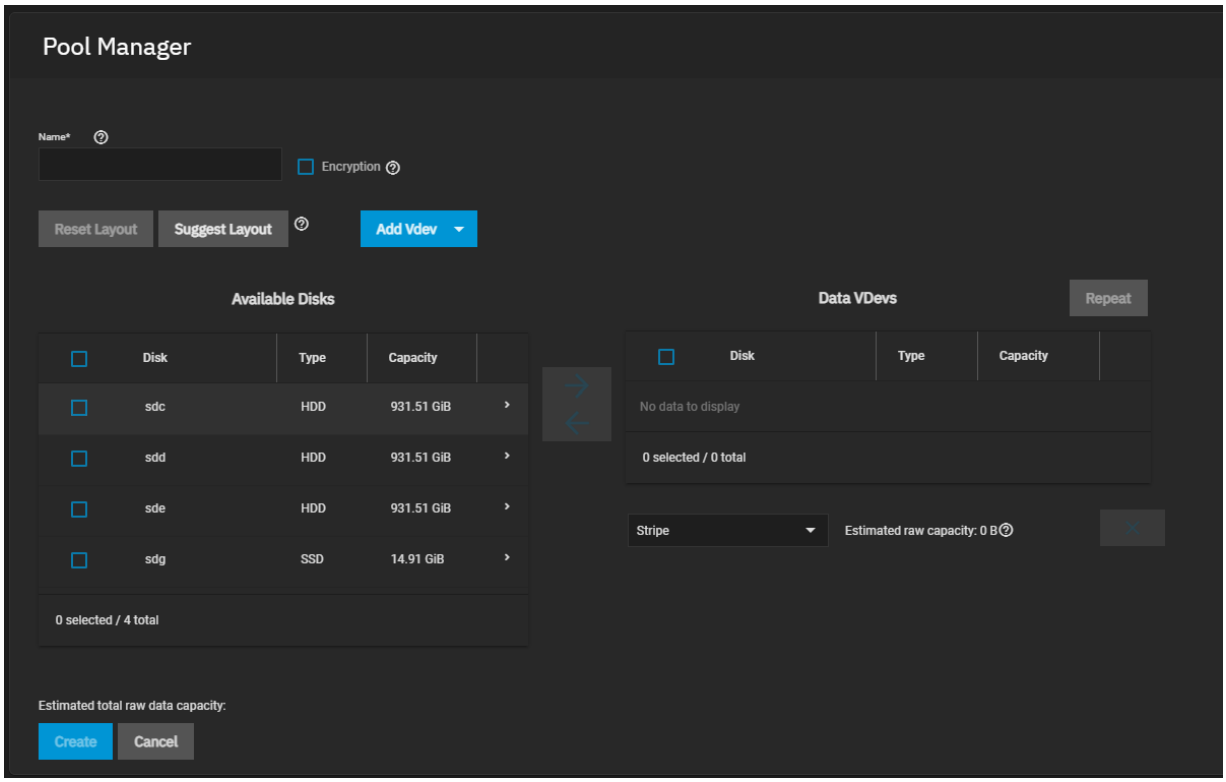
4.3.1.1 - Pool Screens

This article provides information on Pool screens, settings and functions.

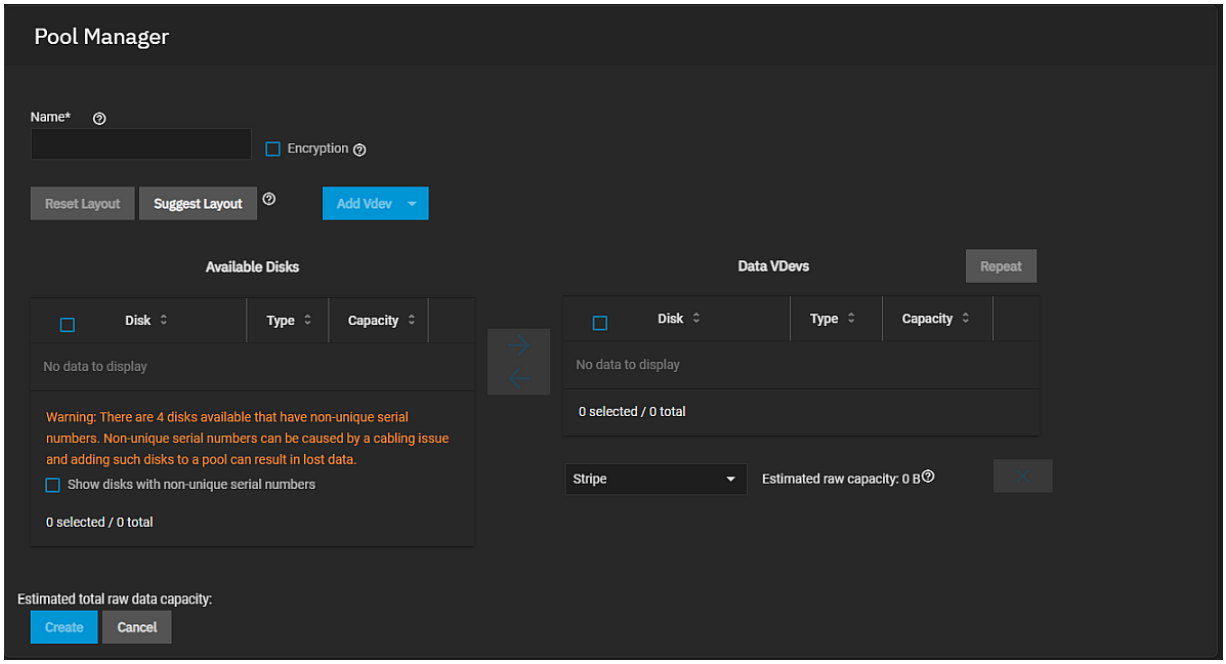
The **Storage** screen displays a list of all the pools and datasets or zvols configured in your TrueNAS.

Pool Manager Screen

To access the **Pool Manager** screen to create a new pool click **Create Pool**. To access **Pool Manager** to modify an existing pool, click the icon button for the pool and select **Add Vdevs**.



If your system disks do not have unique serial numbers, the **Pool Manager** screen displays a warning message and the **Show disks with non-unique serial numbers** option.



Select **Show disks with non-unique serial numbers** to display the system disks. The **0 selected/ # total** below the **Available Disks** displays a count of the number of disks selected to the total number of disks available on your system. This counter keeps track of the total number of available disk in the system when disks span across several screen pages.

Settings	Description
Name	Enter the name you want to use for the pool. Choose something that helps you identify this pool and the type of data it stores. This helps with locating data in systems with pages or hundreds of storage pools configured on the system.
Encryption	Select to enable encryption for this pool, the root dataset and if desired, child datasets and zvols in this pool. See Storage Encryption for more information on using SCALE storage encryption.
Reset Layout	Click to clear a suggested layout after you click **Suggest Layout**.
Suggested Layout	Click to have TrueNAS review all available disks and populate the primary **Data VDev** list with identically-sized drives in a configuration balanced between storage capacity and data redundancy. **Reset Layout** clears the suggested layout.
Add Vdev	Click to display the dropdown list of vdev options in the section below.
Available Disks	Displays the list of disks on your system. Click the › expand icon to see the disk serial number and model number and where it is on the **Enclosure** screen (the position in the server if using iXsystems-provided hardware).
Data VDevs	Default vdev type on the **Pool Manager** screen. After selecting a vdev type from the **Add Vdev** a new list displays under the **Data VDevs** list.
Repeat	Click to create another vdev of the same type and configuration below the exiting **Data VDevs** list.
Vdev type	The vdev type dropdown list below the **Data Vdevs** list displays **Stripe** but then changes to **Mirror** after you select two disks and move them to the **Data Vdevs** list. If you select more than two disk you can select different types from this list based on the number of disks moved.
Estimated raw capacity	Displays the raw storage capacity of the disks for the **Data VDev** type. For a mirror, this is the storage of one disk with the other disk provides redundancy.
Estimated total raw data capacity Estimated data capacity available after extension	The total estimated raw capacity of the disks in the vdev. **Estimated total raw data capacity** changes to **Estimated data capacity available after extension** on the **Add Vdevs to Pool** version of **Pool Manager**.

Vdev Layout Options

Settings	Description
Data	Data is the standard vdev for primary storage operations. Each storage pool requires at least one Data vdev. Data vdev configuration typically affects how users can configure other types of vdevs.
Cache	A cache vdevs is a ZFS L2ARC read-cache used with fast devices to accelerate read operations. Users can add or remove cache vdevs after creating the pool.

Settings	Description
Log	A log vdev is a ZFS LOG device that improves synchronous write speeds. Users can add or remove log vdevs after creating the pool.
Hot Spare	A Hot Spare vdev is a drive or drives reserved for inserting into data vdevs when an active drive fails. The system uses hot spares as temporary replacements for failed drives to prevent larger pool and data loss scenarios. When a user replaces a failed drive with a new one, the hot spare reverts to an inactive state and becomes available again as a hot spare. If a user detaches the failed drive from the pool without adding a new one, the system promotes the temporary hot spare to a full data vdev member.
Metadata	A metadata vdev is a special allocation class used to create fusion pools for increased metadata and small block I/O performance.
Dedup	A dedup vdev stores ZFS de-duplication metadata. Requires allocating X GiB of metadata for every X TiB of general storage. Example: *1 GiB* of dedup metadata vdev capacity for every *1 TiB* of data vdev availability.

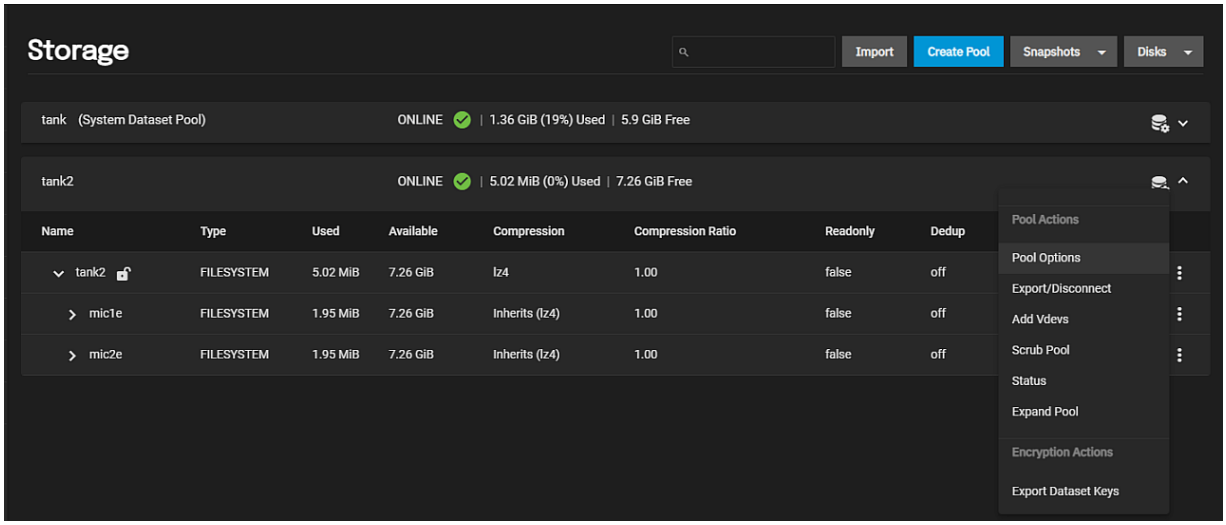
Vdev Options

Settings	Description
Stripe	Each disk stores data. A Stripe requires at least one disk and has no data redundancy.
Mirror	Data is identical in each disk. A Mirror requires at least two disks, provides the most redundancy, and has the least capacity.
RAIDZ1	Uses one disk for parity while all other disks store data. RAIDZ1 requires at least three disks.
RAIDZ2	Uses two disks for parity while all other disks store data. RAIDZ2 requires at least four disks.
RAIDZ3	Uses three disks for parity while all other disks store data. RAIDZ3 requires at least five disks.

Pool Actions List Options

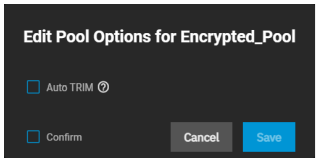
The **Pool Actions** dropdown list displays options to expand the pool, check the status of disks in the pool, implement ZFS TRIM, perform an integrity check on the pool, and export or disconnect the pool. If the pool is configured to use encryption, the option to export dataset keys also displays on the **Pool Actions** dropdown list.

To access options for pools listed on the **Storage** screen click on the icon button to display the **Pool Actions** dropdown list of options.



Pool Options Dialog

Select **Pool Options** to display the **Edit Pool Options** dialog.



Select **Auto TRIM** to enable TrueNAS to periodically review data blocks to identify empty obsolete blocks it can delete. If left clear (default), TrueNAS incorporates day-block overwrites when a device write starts.

Click here for more Auto TRIM information

When enabled, TrueNAS to periodically reviews data blocks tp identify the blocks it can reclaim. Auto TRIM is disabled because it can impact pool performance.

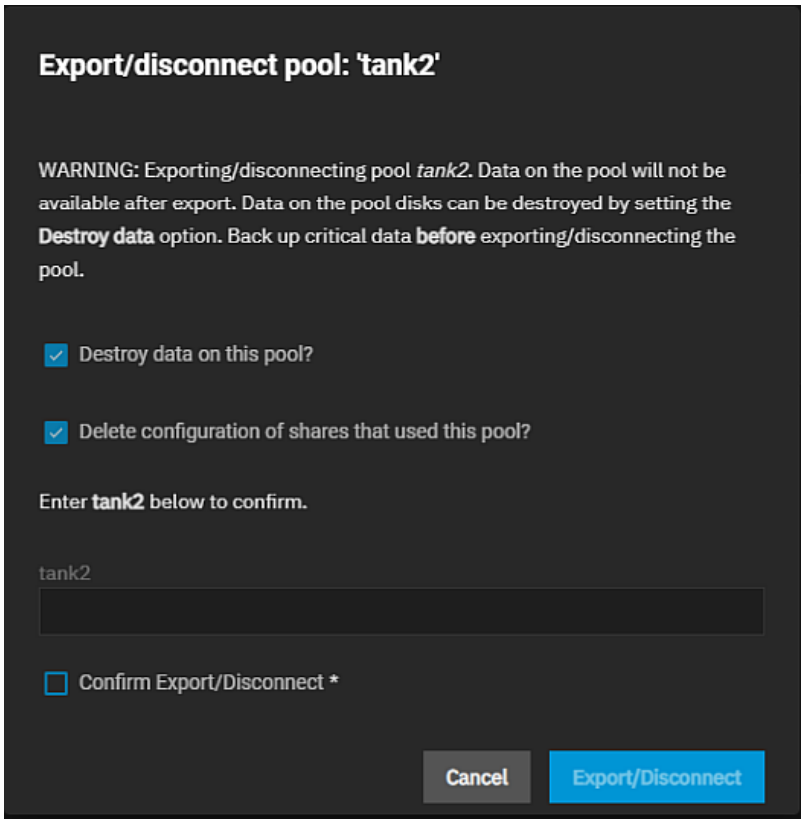
For more details about TRIM in ZFS, see the `autotrim` property description in zpool.8.

Select **Confirm** to activate **Save**.

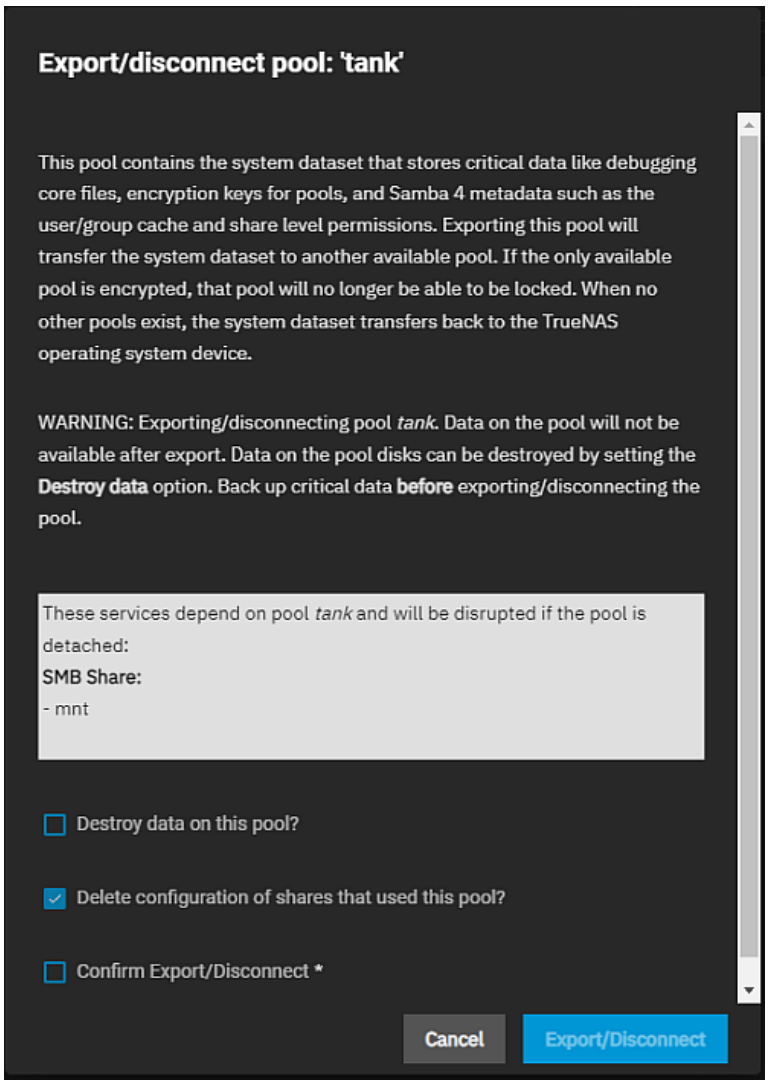
Export/Disconnect Window

Select **Export/Disconnect** to display the **Export/disconnect pool: *poolname*** window. **Export/Disconnect** allows users to export, disconnect, or delete a pool. Disks in the pool become available to use in a new pool. A warning displays stating data becomes unavailble after an export and that selecting **Destroy Data on this pool** destroys data on the pool disks.

> This can be a destructive process! Back up all data before performing this operation. You might not be able to recover data lost though this operation.



If a share uses the pool this window displays the share type (for example, SMB share, etc.) affected by the export/disconnect operation.

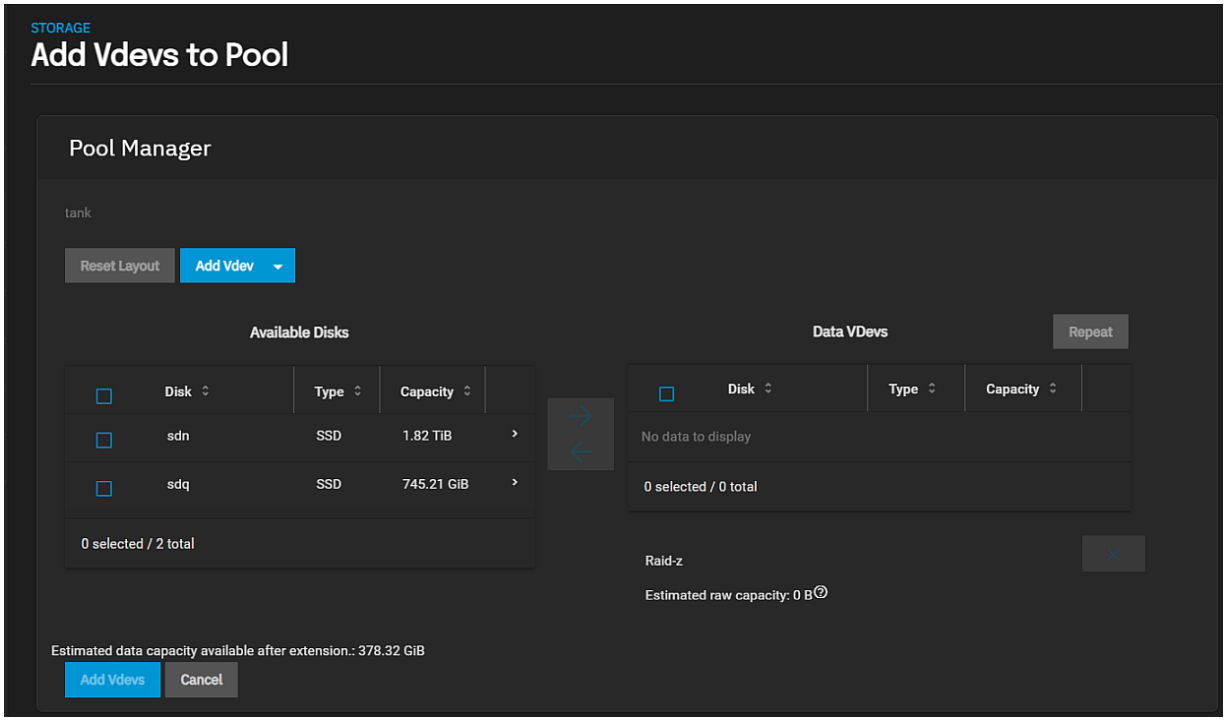


Setting	Description
Destroy data on this pool?	Select to erase all data on the pool. When selected the **Confirm Export/Disconnect** checkbox disappears.
Delete configuration of shares that sued this pool?	Enabled by default to remove the share connection to this pool. Exporting or disconnecting the pool deletes the configuration of shares using this pool. You must reconfigure the shares affected by this operation.
Confirm Export/Disconnect	Required option. Select to confirm this operation and accept the warnings displayed. Activates the **Export/Disconnect** button.

Click **Export/Disconnect** to execute the process and begin the pool export or disconnect. A status window displays with progress. When complete, a final dialog displays stating the export/disconnect completed successfully.

Add Vdevs Screen

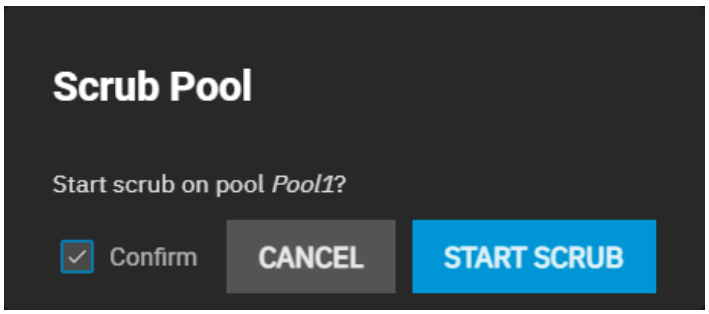
Displays the **Add Vdev to Pool** screen with **Pool Manager** showing the selected pool. You cannot rename the pool or change the vdev type.



The screen settings are described in the Pool Manager section above.

Scrub Pool Dialog

Select **Scrub Pool** to display the start pool scrub dialog. Select **Confirm** to activate the **Start Scrub** button.

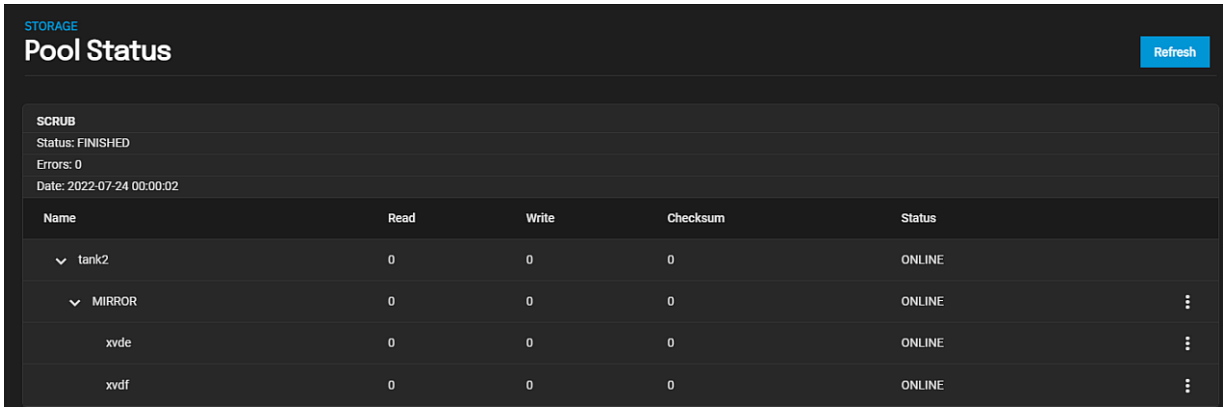


Scrub Pool initiates a check on pool data integrity. If TrueNAS detects any problems during the scrub, it either corrects them automatically or generates an alert in the web interface.

By default, TrueNAS automatically checks every pool to verify it is on a reoccurring scrub schedule.

Status Screen

Select **Status** to display the **Pool Status** screen that lists the pool, vdev type, and drives in the pool.



Pool Status screen displays the status of any scrub operation, errors encountered and the date of the scrub operation.

The list displays the number of reads, writes and checksums, and the status of each root dataset, vdev for the root dataset, and disks in the vdev.

Use **Refresh** to update the screen after making a change.

Click the ⋮ for the pool vdev to display the vdev type actions dropdown list if the type is **Mirror**. Options are **Extend** or **Remove**.

Click the ⋮ for a disk to display **Disk Actions** dropdown list. Options are **Edit**, **Offline**, **Online**, **Replace**, **Remove** and **Detach**. See Disk Screen for more information on these options.

Expand Pool

Select **Expand Pool** to increase the pool size to match all available disk space. Users with pools using virtual disks use this otpion to resize these virtual disks apart from TrueNAS.

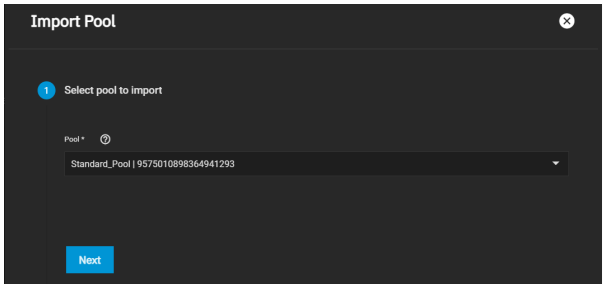
Export Dataset Keys Dialog

Select **Export Dataset Keys** to obtain the encryption keys for the dataset. Displays the exported json file at the bottom of the screen. Click the expand icon and select the desired option for the downloaded file.

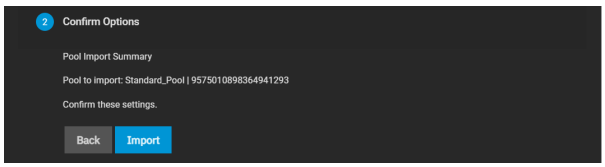
> Keep exported encryption files in a safe and secure location!
>
> Always back up encryption keys. Losing an encryption key could result in permanently locked, or lost, data!

Import Pool Screens

Click **Import** to view the **Import Pool** wizard screens.



Use the **Pool Import Summary** dropdown to select the pool to import. Click **Next** to advance to the **Confirm Options** screen



Click **Import** to begin the pool import process.

Related Pools Articles

- Dashboard
- Managing Advanced Settings
- Advanced Settings Screen
- View Enclosure Screen
- Setting Up Permissions
- Storage Encryption
- SLOG Over-Provisioning
- Fusion Pools

Related Storage Articles

- Storage Screens
- Snapshots Screens
- Setting Up Storage
- Zvol Screens
- Creating Storage Pools
- Edit ACL Screens
- Importing Storage Pools
- Adding and Managing Datasets

- Installing and Managing Self-Encrypting Drives
- Adding and Managing Zvols

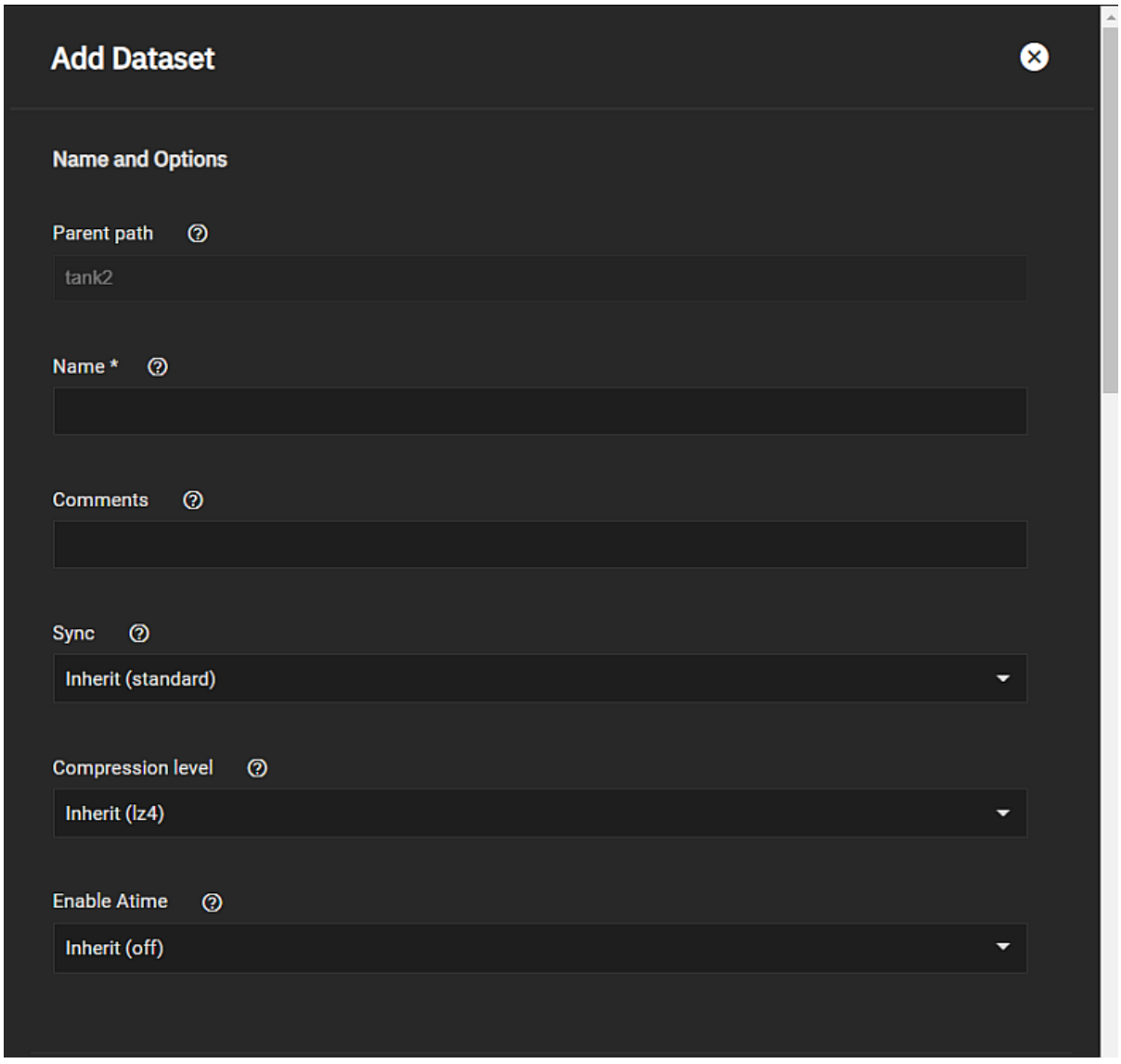
4.3.1.2 - Datasets Screens

This article provides information on Datasets screens, settings and functions.

The **Datasets** screens, accessed from datasets on the **Storage** screen, display the configuration settings for datasets. Click the ⋮ and select **Add Dataset** to display the **Add Dataset** screen or click **Edit Options** to display the **Edit Dataset** screen.

Both the add and edit dataset screens display **Basic Options** settings to set up a simple dataset. Click **Advanced Options** to display more settings to further customize datasets.

Dataset Basic Options



Name and Options Settings

Setting	Description
Parent path	Read-only field that displays the dataset path for the dataset. The root dataset path includes the only the name of the root dataset. Child datasets created from a child of root include the root dataset/parent dataset in the path.
Name	Enter a unique identifier for the dataset. You cannot change the dataset name after clicking **Save**.
Comments	Enter notes about the dataset.
Sync	Select the sync setting option from the dropdown list. **Standard** uses the sync settings requested by the client software. **Always** waits for data writes to complete, and **Disabled** never waits for writes to complete.
Compression level	Select the compression algorithm to use from the dropdown list. Options encode information in less space than the original data occupies. It is recommended to choose a compression algorithm that balances disk performance with the amount of saved space. **LZ4** is generally recommended as it maximizes performance and dynamically identifies the best files to compress. **ZSTD** is the Zstandard compression algorithm with several options for balancing speed and compression. **Gzip** options range from **1** for least compression with best performance, through **9** for maximum compression with greatest performance impact. **ZLE** is a fast algorithm that only eliminates runs of zeroes. **LZJB** is a legacy algorithm that is not recommended for use.
Enable Atime	Select the access time for files option from the dropdown list. Access time can result in significant performance gains. **Inherit** uses the access time setting of the parent or the root dataset. **On** updates the access time for files when they are read. **Off** disables creating log traffic when reading files to maximize performance.

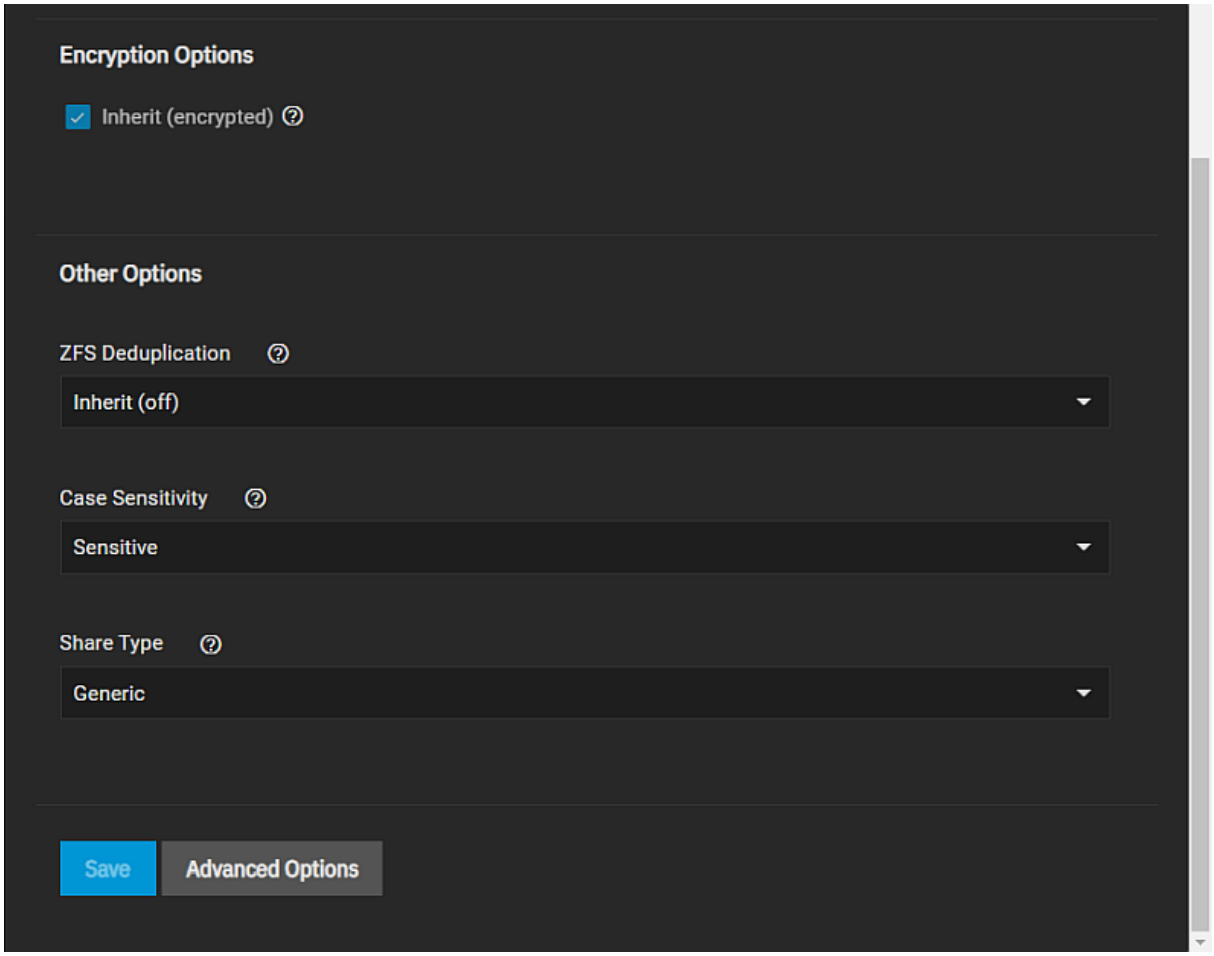
Encryption Options Settings

The default is **Inherit** selected. Clearing the checkbox displays more options. Selections in the **Encryption Type** field also displays additional setting options. See Storage Encryption for more information on encryption.

Setting	Description
Inherit	Select to use the encryption setting of the parent or root dataset (selected by default).
Encryption Type	Select the option for the type of encryption to secure the dataset from the dropdown list. Select **Key** to use key-based encryption. Displays the **Generate Key** option. Creating a new key file invalidates any previously downloaded key file for this dataset. Delete any previous key file backups and back up the new key file. Select **Passphrase** to enter a user-defined passphrase to secure the dataset. This displays two additional **Passphrase** fields to enter and confirm the passphrase and the **pbkdf2iters** field.
Generate key	Selected by default to have the system randomly generate an encryption key for securing this dataset. Clearing the checkbox displays the **Key** field and requires you to enter an encryption key you define. Warning! The encryption key is the only means to decrypt the information stored in this dataset. Store encryption keys in a secure location!
Key	Enter or paste a string to use as the encryption key for this dataset.
Algorithm	Displays for both key and passphrase encryption types. Select the mathematical instruction set that determines how plaintext converts into ciphertext from the dropdown list of options. See Advanced Encryption Standard (AES) for more details.
pbkdf2iters	Enter the number of password-based key deviation function 2 (PBKDF2) iterations to use for reducing vulnerability to brute-force attacks. Entering a number larger than 100000 is required. See PBKDF2 for more details.

Other Options Settings

The **Other Options** settings help tune the dataset for specific data sharing protocols.



Setting	Description
ZFS Deduplication	Select the option from the dropdown list to transparently reuse a single copy of duplicated data to save space. Options are **Inherit** to use the parent or root dataset settings. **On** to use deduplication. **Off** to not use deduplication, or **Verify** to do a byte-to-byte comparison when two blocks have the same signature to verify the block contents are identical. Deduplication can improve storage capacity, but is RAM intensive. Compressing data is recommended before using deduplication. Deduplicating data is a one-way process. *Deduplicated data cannot be undeduplicated!*
Case Sensitivity	Select the option from the dropdown list. **Sensitive** assumes file names are case sensitive. **Insensitive** assumes file names are not case sensitive. **Mixed** understands both types of file names. You cannot change case sensitivity after the saving the dataset.
Share Type	Select the option from the dropdown list to define the type of data sharing the dataset uses to optimize the dataset for that sharing protocol. Select **SMB** if using with an SMB share. Select **Generic** for all other share types. You cannot change this setting after the saving dataset.

Data Compression Algorithms

Select the compression algorithm that best suits your needs from the **Compression** dropdown list of options.

LZ4 maximizes performance and dynamically identifies the best files to compress. LZ4 provides lightning-fast compression/decompression speeds and comes coupled with a high-speed decoder. This makes it one of the best Linux compression tools for enterprise customers.

ZSTD offers highly configurable compression speeds, with a very fast decoder.

Gzip is a standard UNIX compression tool widely used for Linux. It is compatible with every GNU software which makes it a good tool for remote engineers and seasoned Linux users. It offers the maximum compression with the greatest performance impact. The higher the compression level implemented the greater the impact on CPU usage levels. Use with caution especially at higher levels.

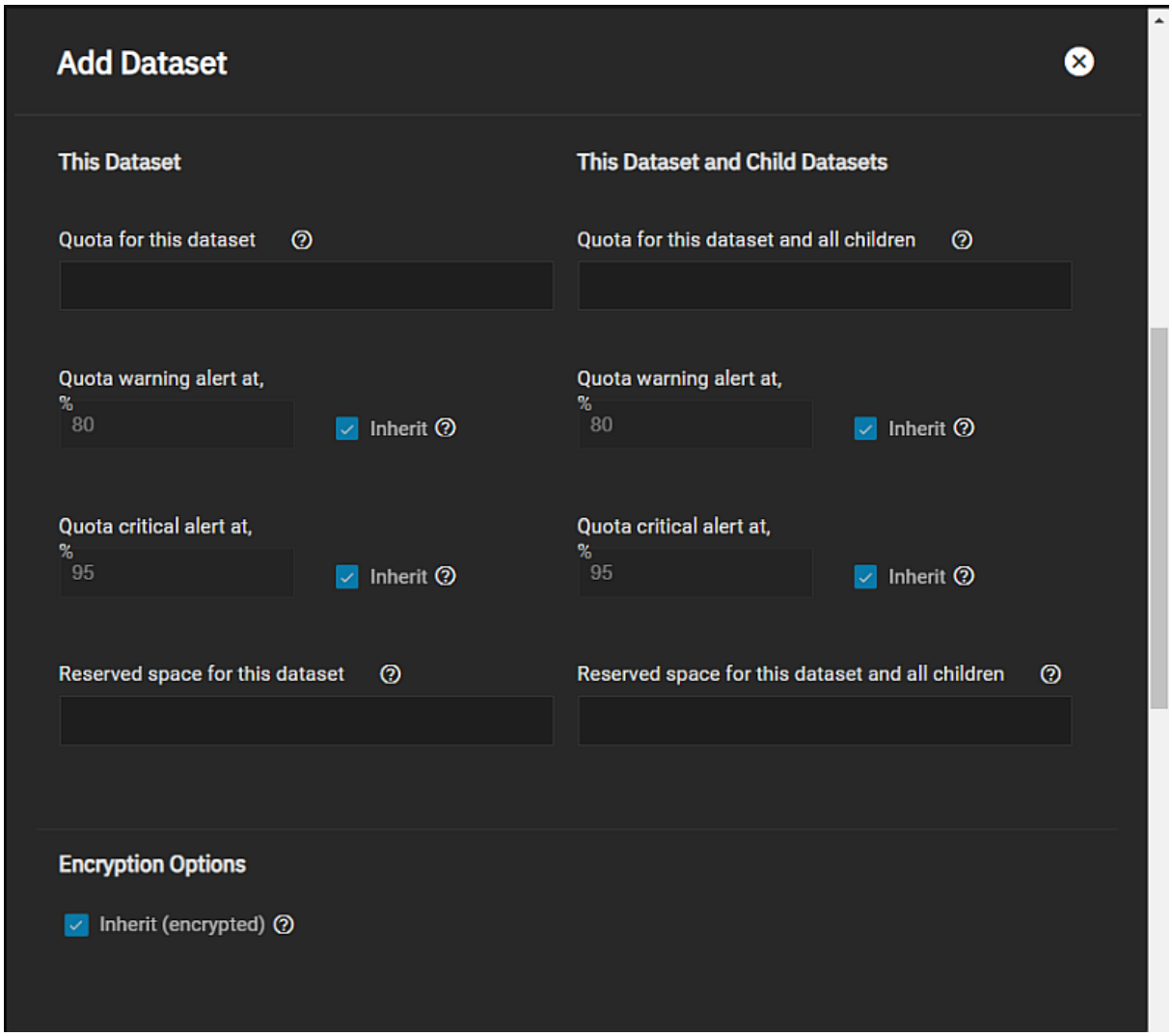
ZLE or Zero Length Encoding, leaves normal data alone but only compresses continuous runs of zeros.

LZJB compresses crash dumps and data in ZFS. LZJB is optimized for performance while providing decent compression. LZ4 compresses roughly 50% faster than LZJB when operating on compressible data, and is greater than three times faster for uncompressible data. LZJB was the original algorithm used by ZFS but it is now deprecated.

Advanced Options Settings

Advanced Options adds dataset quota management tools and more fields to the **Other Options** settings.

Dataset Quota Settings

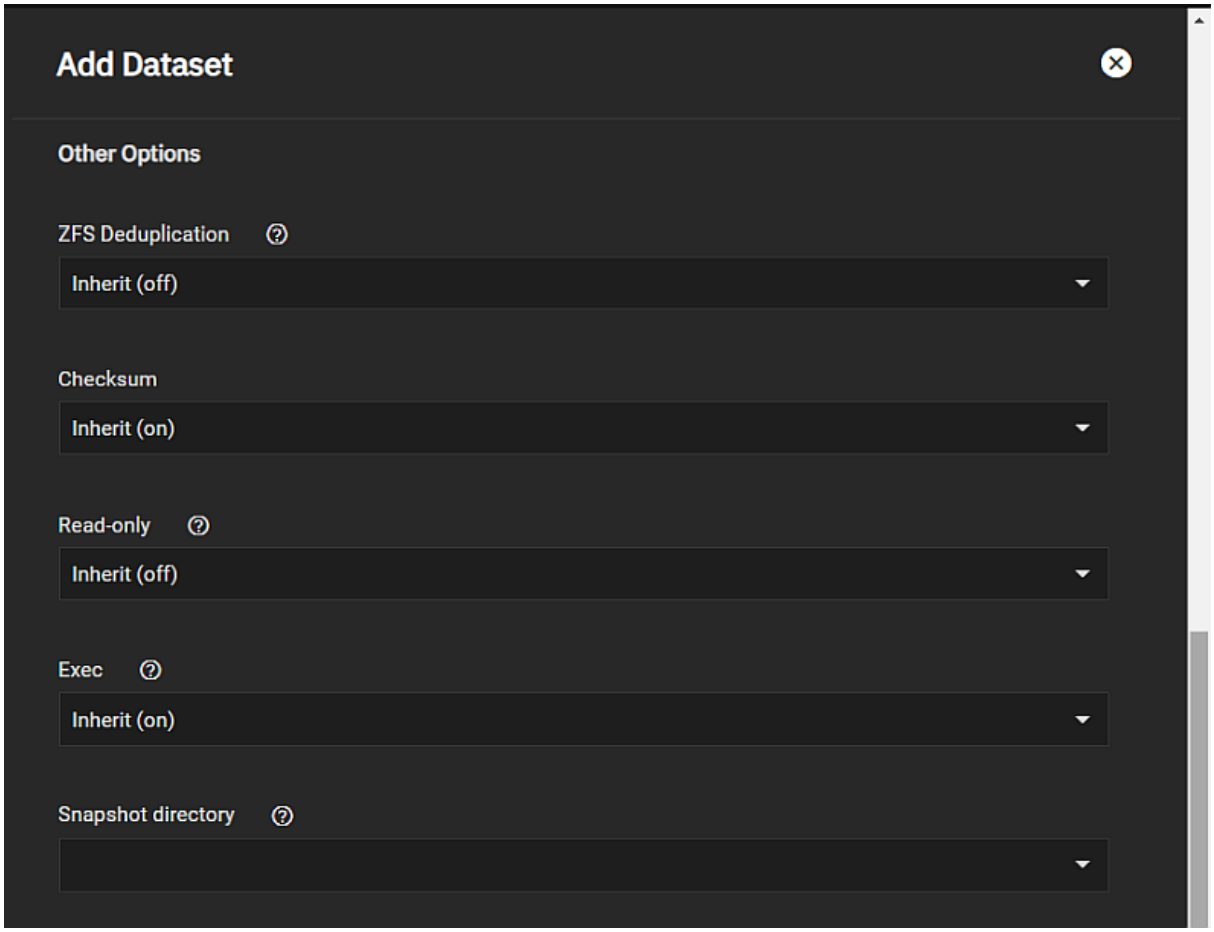


Setting a quota defines the maximum allowed space for the dataset or the dataset and child datasets. You can also reserve a defined amount of pool space to prevent automatically generated data like system logs from consuming all of the dataset space. You can configure quotas for only the new dataset or include all child datasets.

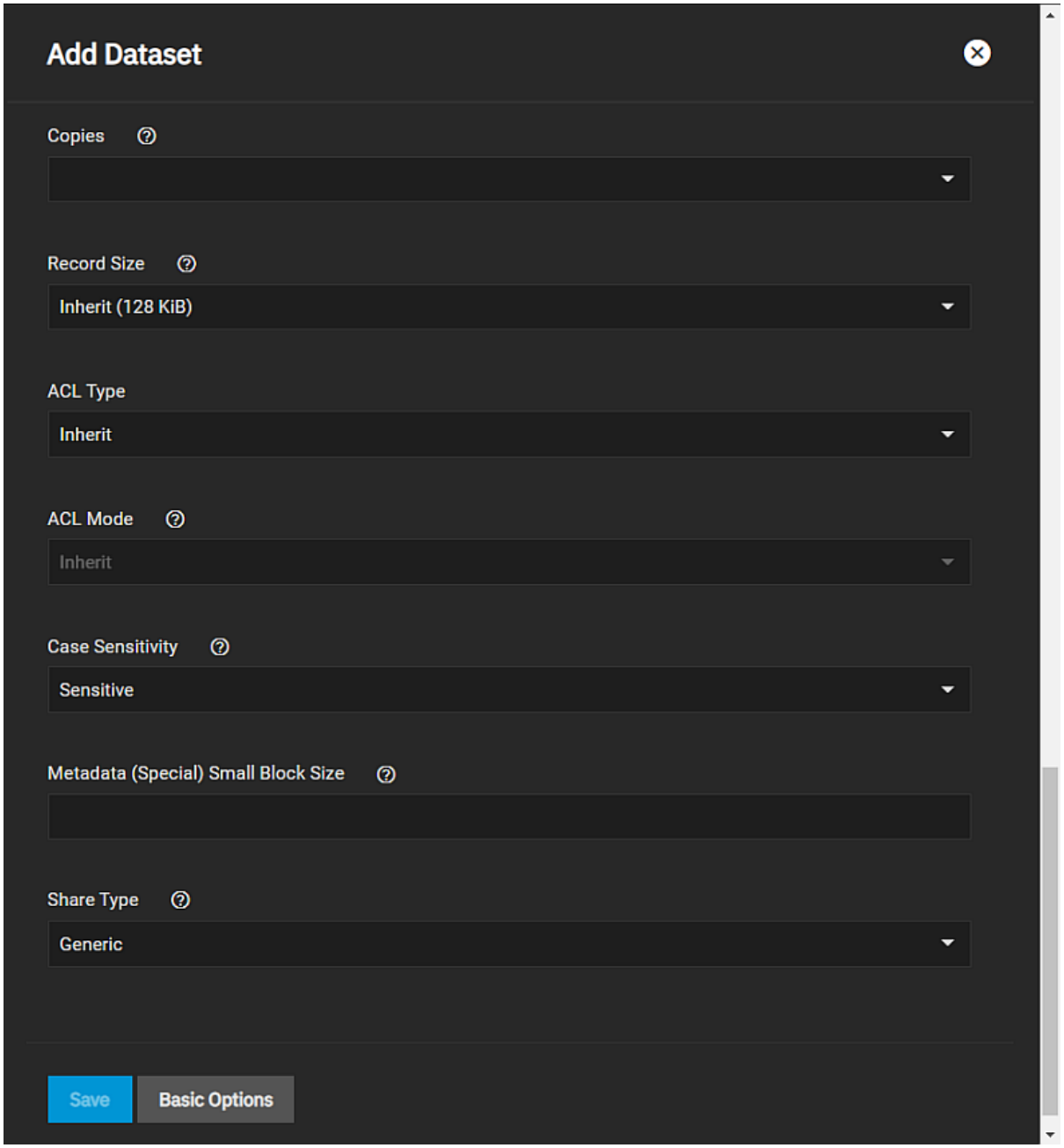
Setting	Description
Quota for this dataset **Quota for this dataset and all children**	Enter a value to define the maximum allowed space for the dataset. **0** disables quotas.
Quota warning alert at, %	Enter a percentage value to generate a warning level alert when consumed space reaches the defined level. By default, the dataset inherits this value from the parent dataset. Clear the **Inherit** checkbox to change the value.
Quota critical alert at, %	Enter a percentage value to generate a critical level alert when consumed space reaches the defined level. By default, the dataset inherits this value from the parent dataset. Clear the **Inherit** checkbox to change the value.
Reserved space for this dataset **Reserved space for this dataset and all children**	Enter a value to reserve additional space for datasets that contain logs which could eventually take up all the available free space. **0** is unlimited.

Advanced Other Option Settings

Many of the **Other Options** settings inherit their values from the parent dataset.



Setting	Description
Checksum	Select the checksum option from the dropdown list. Select **Inherit** to use the parent setting; **On** to use checksum without specifying the variant; **FLETCHER2** (deprecated) or **FLETCHER4** to use a position-dependent checksum that uses two checksums to determine single-bit errors in messages transmitted over network channels or ZFS streams; **SHA256** (default for dedupted datasets) or **SHA512** to use a sequence of numbers and letters to check the copy of a downloaded update file is identical to the original; **SKEIN** which is not supported for a file system on boot pools; or **EDNOR** which is not supported for file systems on boot pools and Edon-R requires verification when used with dedup so it automatically uses `verify`.
Read-only	Select the option to allow or prevent dataset modification from the dropdown list. **On** prevents modifying the dataset. **Off** allows users accessing the dataset to modify its contents.
Exec	Select the option for executing processes from within the dataset from the dropdown list. **On** allows executing processes from within this dataset. **Off** prevents executing processes from with the dataset. We recommend setting it to **On**.
Snapshot directory	Select the option to controls visibility of the .zfs directory on the dataset from the dropdown list. Select either **Visible** or **Invisible**.



Setting	Description
Copies	Select the number of duplicate of ZFS user data stored on this dataset from the dropdown list. Select between **1**, **2**, or **3** redundant data copies. This can improve data protection and retention, but is not a substitute for storage pools with disk redundancy.
Record Size	Select the logical block size in the dataset from the dropdown list of options. Matching the fixed size of data, as in a database, can result in better performance.
ACL Type	Select the access control list type from the dropdown list of options. **Inherit** preserves ACL type from the parent dataset. **Off** to use neither NFSv4 or POSIX protocols. **NFSv4** is used to losslessly migrate Windows-style ACLs across Active Directory domains (or stand-alone servers) that use ACL models richer than POSIX. Since POSIX ACLs are a Linux-specific ZFS feature, administrators should use NFSv4 to maintain compatibility with TrueNAS Core, FreeBSD, or other non-Linux ZFS implementations. **POSIX** use when an organization data backup target does not support native NFSv4 ACLs. Since the Linux platform used POSIX for a long time, many backup products that access the server outside the SMB protocol cannot understand or preserve native NFSv4 ACLs. All datasets within an SMB share path must have identical ACL types. For a more in-depth explanation of ACLs and configurations in TrueNAS SCALE, see our ACL Primer.
ACL Mode	Select the option that determines how chmod behaves when adjusting file ACLs from the dropdown list. See the zfs(8) `aclmode` property. **Passthrough** only updates ACL entries that are related to the file or directory mode. **Restricted** does not allow chmod to make changes to files or directories with a non-trivial ACL. An ACL is trivial if it can be fully expressed as a file mode without losing any access rules. Set the ACL Mode to

Setting	Description
	restricted to optimize a dataset for SMB sharing, but it can require further optimizations. For example, configuring an rsync task with this dataset could require adding `--no-perms` in the task **Auxiliary Parameters** field.
Metadata (Special) Small Block Size	Enter a threshold block size for including small file blocks into the special allocation class (fusion pools). Blocks smaller than or equal to this value are assigned to the special allocation class while greater blocks are assigned to the regular class. Valid values are zero or a power of two from 512B up to 1M. The default size **0** means no small file blocks are allocated in the special class. Before setting this property, you must add a special class vdev to the pool.

Edit Dataset Screens

Click **Edit Options** on the **Dataset Actions** list of options to access the **Edit Dataset** screens.

The fields and settings on the **Edit Dataset** screens are the same as the **Add Dataset** screens but you cannot edit the **Name**, **Case Sensitivity** or **Share Type** fields on the Basic and Advanced Options screens.

Dataset Actions List

The **Dataset Actions** dropdown list options for child datasets are the same but also include **Delete Dataset**.

Add Dataset

The **Add Dataset** option displays the **Add Dataset** configuration screen where you can create a child dataset to the root dataset or to another child dataset.

Add Zvol

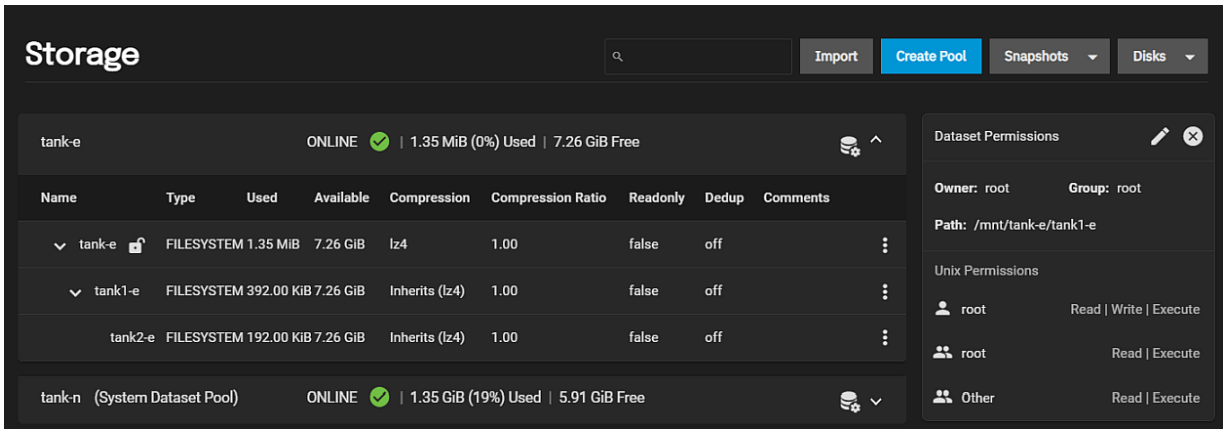
Add Zvol displays the **Add Zvol** where you can create zvols for a root or child dataset.

Edit Options

Edit Options displays the **Edit Dataset** screen where you can edit the settings for the selected dataset.

View Permissions

View Permissions displays the **Dataset Permissions** widget to the right of the root dataset on the **Storage**screen. The **Dataset Permissions** widget is read-only.



Settings	Description
Owner	Displays the name of the owner, which is **root** for both the root dataset and the child datasets of root.
Group	Displays the name of the group, which is **root** for both the root dataset and the child datasets of root..
Path	Displays the path for the selected dataset.
Unix Permissions	Displays three levels of permissions, **Read

User Quotas

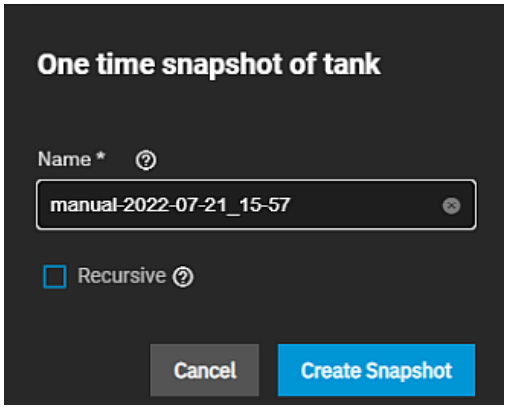
User Quotas displays the **Set User Qutoas** screen.

Group Quotas

Group Quotas displays the **Set Group Qutoas** screen.

Create Snapshot

Create Snapshot displays the **One time snapshot of *datasetname*** dialog where you can create a manual snapshot of the selected dataset. The dialog *datasetname* changes based on the name of the selected dataset (or zvol).



Name displays the system-created name for the snapshot.

Select **Recursive** to include child datasets or zvols in the snapshot of the parent or root dataset.

Click **Create Snapshot** to create the manual snapshot.

Related Datasets Articles

- Advanced Settings Screen
- Edit ACL Screens
- User and Group Quota Screens
- Adding and Managing Datasets
- Setting Up Permissions
- Storage Encryption
- Managing User or Group Quotas

4.3.1.3 - Zvol Screens

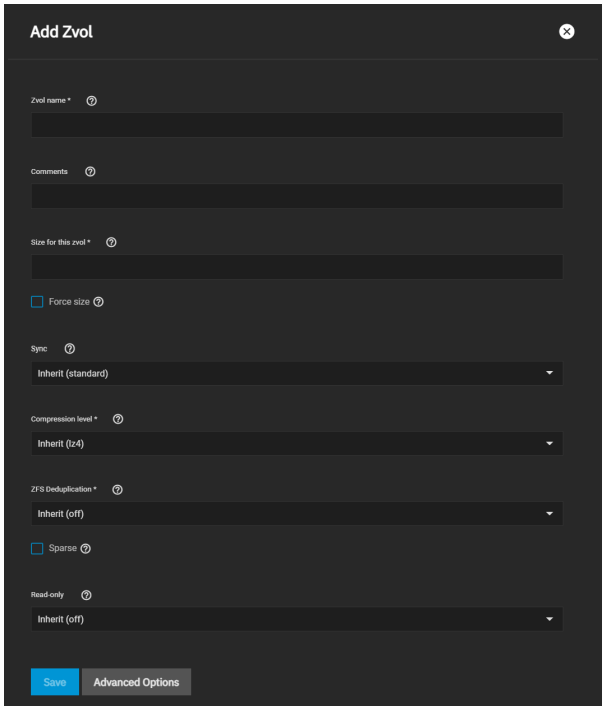
This article provides information on Zvol screen settings and functions.

To access the Zvol screens, from the **Storage** screen click the ⋮ for a pool or dataset, then click **Add Zvol** to display the **Add Zvol** screen. To edit a zvol, click the ⋮ for a zvol, then click **Edit Zvol** to display the **Edit Zvol** screen.

Add Zvol Screen

The **Add Zvol** has two screens, basic options and advanced options. The basic options display by default. Click **Advanced Options** to expand the settings that includes block size.

Basic Options Settings

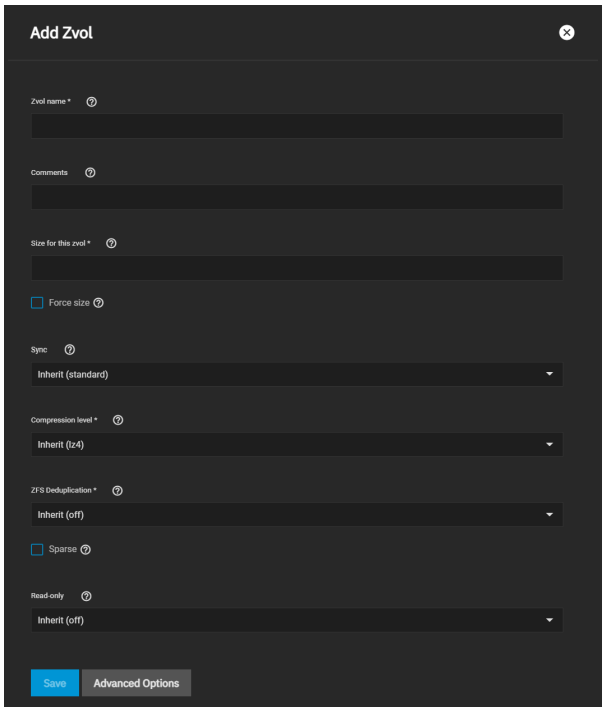


Setting	Description
Zvol name	Required setting. Enter a short name for the zvol. Using a zvol name longer than 63-characters can prevent accessing zvols as devices. For example, you cannot use a zvol with a 70-character file name or path as an iSCSI extent.
Comments	Enter any notes about this zvol.
Size for this zvol	Specify size and value. You can include units like **t** as in TiB, and **G**. You can increase the size of the zvol later, but you cannot reduce size. If the size is more than 80% of the available capacity, the creation fails with an out-of-space error unless you select **Force size**.
Force size	Select to enable the system to create a zvol where the size is over 80% capacity. By default, the system does not create a zvol of this size. While not recommended, enabling this option forces the creation of the zvol.
Sync	Select the data write synchronization option from the dropdown list. **Inherit** gets the sync settings from the parent dataset. **Standard** uses the sync settings requested by the client software. **Always** waits for data writes to complete. **Disabled** never waits for writes to complete.
Compression level	Select the option from the dropdown list for the type of data compression to use or encoding information in less space than the original data occupies. Select the algorithm that balances disk performance with the amount space saved. See below for the options.

Setting	Description
ZFS Deduplication	Do not change this setting unless instructed to do so by your iXsystems support engineer. Select to transparently reuse a single copy of duplicated data to save space. Deduplication can improve storage capacity, but it is RAM intensive. Compressing data is recommended before using deduplication. Deduplicating data is a one-way process. You cannot un-deduplicate deduplicated data!
Sparse	Used to provide thin provisioning. Use with caution as writes fail when space is low on a pool.
Read-only	Select the option to use to prevent modifying the zvol. Options are **Inherit (off)**, **On** or **Off**.

Encryption options do not display unless you create the zvol from dataset using encryption.

Advanced Options Settings



Setting	Description
Block size	Select the size option from the dropdown list. The default is **Inherit**, other options include, **4KiB**, **8KiB**, **16KiB**, **32KiB**, **64KiB**, **128KiB**.

TrueNAS recommends a space-efficient block size for new zvols. This table shows the minimum recommended volume block size values by configuration (mirror or RAIDz type). Use this table to change the **Block size** value.

Configuration	Number of Drives	Optimal Block Size
Mirror	N/A	16k
Raidz-1	3	16k
Raidz-1	4/5	32k
Raidz-1	6/7/8/9	64k
Raidz-1	10+	128k
Raidz-2	4	16k
Raidz-2	5/6	32k
Raidz-2	7/8/9/10	64k
Raidz-2	11+	128k
Raidz-3	5	16k
Raidz-3	6/7	32k
Raidz-3	8/9/10/11	64k
Raidz-3	12+	128k

Depending on their workload, zvols can require additional tuning for optimal performance. See the OpenZFS handbook workload tuning chapter for more information.

Data Compression Algorithms

Select the compression algorithm that best suits your needs from the **Compression** dropdown list of options.

LZ4 maximizes performance and dynamically identifies the best files to compress. LZ4 provides lightning-fast compression/decompression speeds and comes coupled with a high-speed decoder. This makes it one of the best Linux compression tools for enterprise customers.

ZSTD offers highly configurable compression speeds, with a very fast decoder.

Gzip is a standard UNIX compression tool widely used for Linux. It is compatible with every GNU software which makes it a good tool for remote engineers and seasoned Linux users. It offers the maximum compression with the greatest performance impact. The higher the compression level implemented the greater the impact on CPU usage levels. Use with caution especially at higher levels.

ZLE or Zero Length Encoding, leaves normal data alone but only compresses continuous runs of zeros.

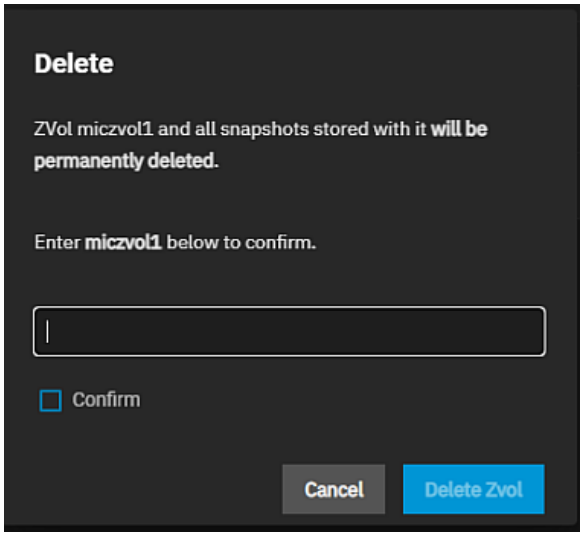
LZJB compresses crash dumps and data in ZFS. LZJB is optimized for performance while providing decent compression. LZ4 compresses roughly 50% faster than LZJB when operating on compressible data, and is greater than three times faster for uncompressible data. LZJB was the original algorithm used by ZFS but it is now deprecated.

Zvol Actions List

Click the ⋮ for a dataset to display the **Zvol Actions** dropdown list. The options for the selected zvol are **Delete Zvol**, **Edit Zvol** and **Create Snapshot**.

Delete Zvol Dialog

Delete Zvol displays a confirmation dialog where you enter the name of the zvol and select **Confirm** to activate the **Delete Zvol** button.



Edit Zvol Option

Edit Zvol displays the **Edit Zvol** screen where you can modify current settings.

Create Snapshot Dialog

Create Snapshot displays a **One time snapshot *zvol*** dialog where you can create a manual snapshot of the selected zvol.

Related Content

- Adding and Managing Zvols

4.3.1.4 - Edit ACL Screens

This article describes the ACL permissions screens and settings for POSIX and NFSv4 ACLs, and the conditions that result in addition setting options.

TrueNAS SCALE offers two ACL types: POSIX (the SCALE default) and NFSv4. For a more in-depth explanation of ACLs and configurations in TrueNAS SCALE, see our ACL Primer.

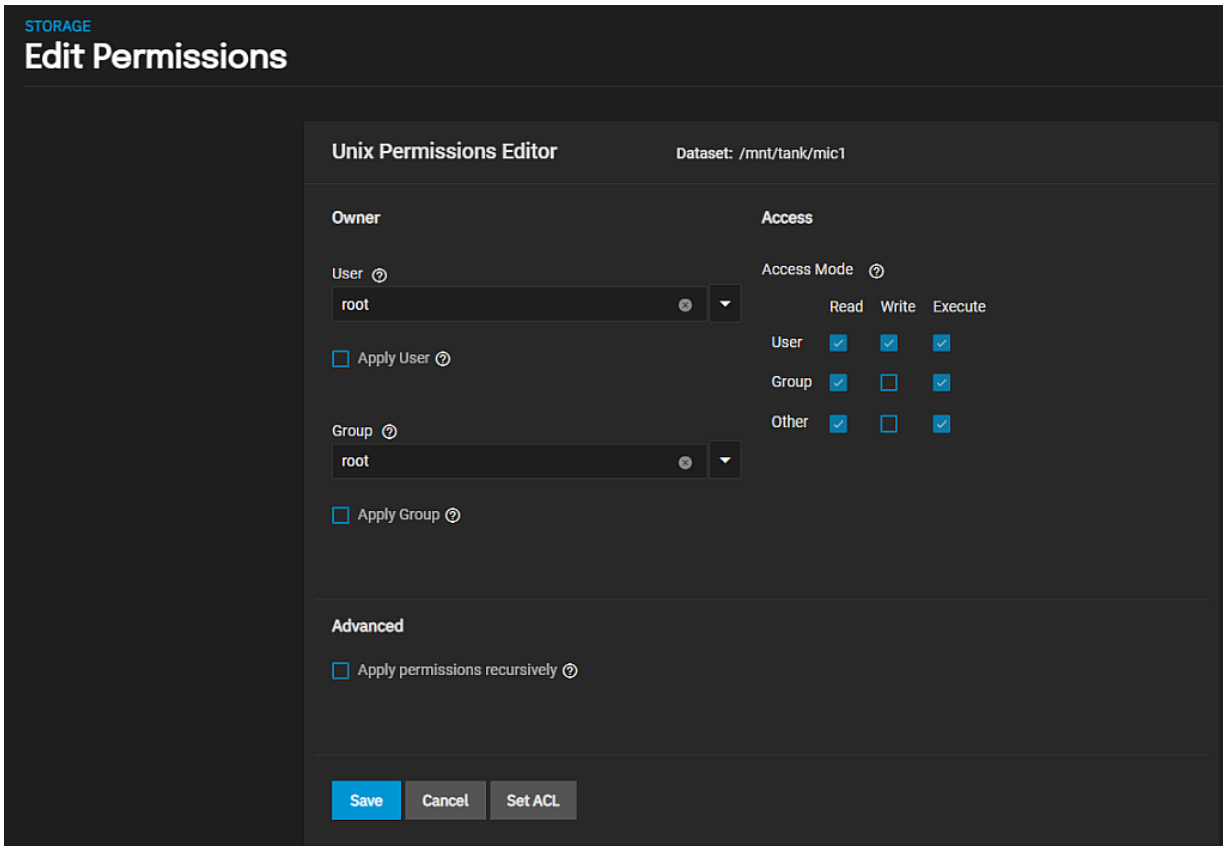
The **ACL Type** setting, found in the **Advanced Options** of both the **Add Dataset** and **Edit Dataset** screens, determines the ACL presets available on the **Select a preset ACL** window and also determines which permissions editor screens you see after you click the edit icon on the **Dataset Permissions** widget.

If **ACL Type** is set to **NSFv4**, you can select the **ACL Mode** you want to use.

> NFSv4 is a type of access control list (ACL) that is not related to the type of share you might use (SMB or NFS).

Unix Permissions Editor Screen

If you selected **POSIX** or **Inherit** as your ACL type, the first screen you see after you click edit on the **Dataset Permissions** widget is the **Storage > Edit Permissions** screen with the **Unix Permissions Editor** basic ACL configuration settings.



Use the settings on this screen to configure basic ACL permissions.

Owner Settings

The **Owner** section controls which TrueNAS user and group has full control of this dataset.

Click here for details

Setting	Description
User	Enter or select a user to control the dataset. Users created manually or imported from a directory service appear in the menu.
Apply User	Select to confirm user changes. To prevent errors, TrueNAS only submits changes only after you select this option.
Group	Enter or select the group to control the dataset. Groups created manually or imported from a directory service appear in the menu.
Apply Group	Select to confirm group changes. To prevent errors, TrueNAS only submits changes only after you select this option.

Access Settings

The **Access** section lets users define the basic **Read**, **Write**, and **Execute** permissions for the **User**, **Group**, and **Other** accounts that might access this dataset.

> A common misconfiguration is removing the **Execute** permission from a dataset that is a parent to other child datasets. Removing this permission results in lost access to the path.

Advanced Settings

The **Advanced** section lets users **Apply Permissions Recursively** to all directories, files, and child datasets within the current dataset.

To access advanced POSIX ACL settings, click **Add ACL** on the **Unix Permissions Editor**. The **Select a preset ACL** window displays with two radio buttons.

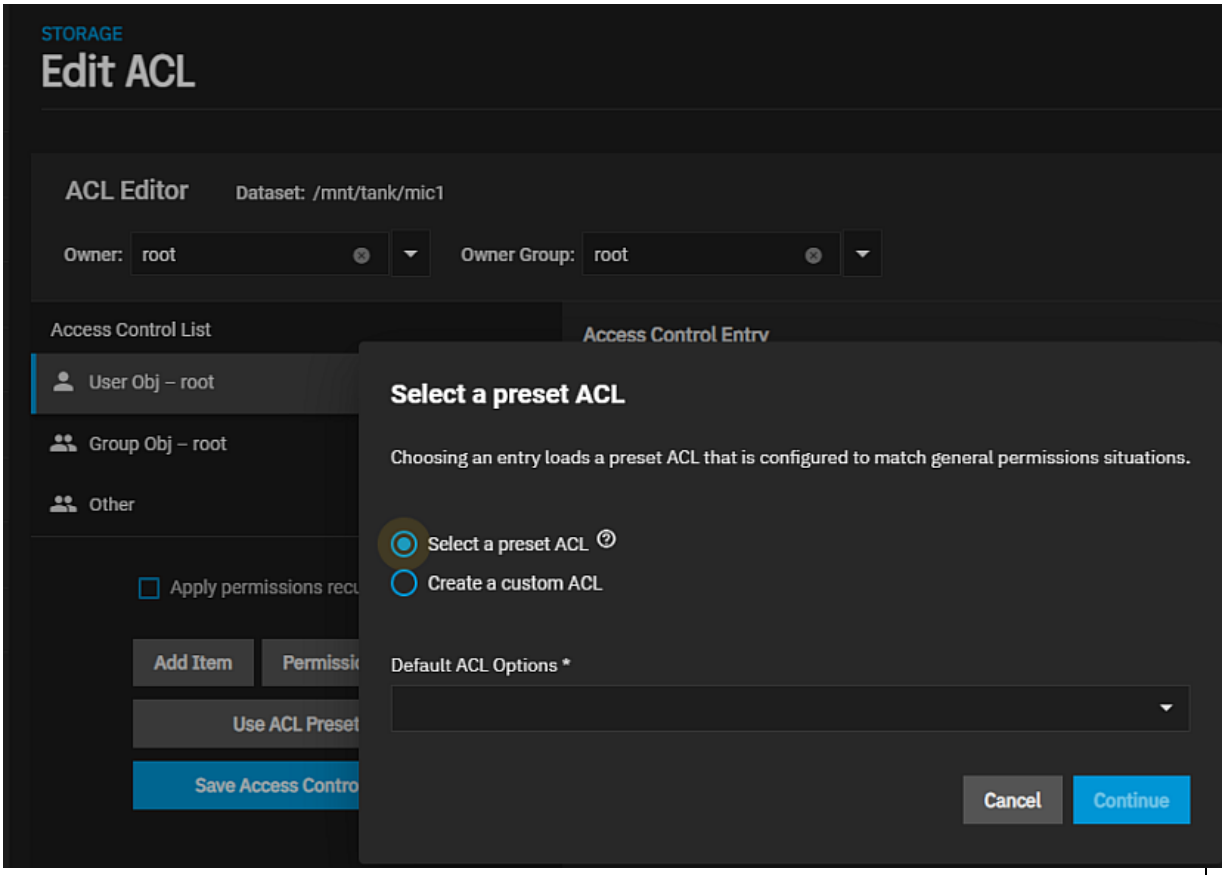
Select A Preset ACL

> Selecting a preset replaces the ACL currently displayed on the Edit ACL screen and deletes any unsaved changes.

There are two different **Select a preset ACL** windows.

Click here for details

If using **POSIX** or **Inherit** as the **ACL Type** setting, the window with three setting options displays before you see the **Edit ACL** screen. These setting options allow you to select and use a pre-configured set of permissions that match general permissions situations or to create a custom set of permissions. You can add to a pre-configured ACL preset on the **Edit ACL** screen.



If using **NFSv4** as the **ACL Type** setting, you access the NFS4 **Select a Preset ACL** window from the **Edit ACL** screen by clicking **Use Preset ACL**.

NFS4SelectAPresetACLDialog

The **ACL Type** setting determines the pre-configured options presented on the **Default ACL Options** dropdown list on each of these windows. For POSIX, the options are **POSIX_OPEN**, **POSIX_RESTRICTED**, or **POSIX_HOME**. For NFSv4, the options are **NFS4_OPEN**, **NFS4_RESTRICTED**, **NFS4_HOME**, and **NFS4_DOMAIN_HOME**.

Setting	Description
Select a preset ACL	Click this radio button to populate the **Default ACL Options** dropdown list with a set of pre-configured POSIX permissions.
Create a custom ACL	Click this radio button to display the **Edit ACL** screen with no default permissions, users or groups to configure your own set of permissions after you click **Continue**.

Click **Continue** to display the **Edit ACL** screen.

Edit ACL Screen

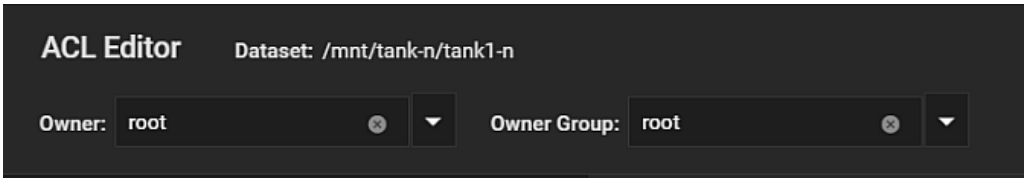
The **Edit ACL** screen displays different setting options based on the **ACL Type** setting on the **Add Dataset** or **Edit Dataset** screen in the **Advanced Options** section.

The section below describes the differences between screens for each ACL type.

ACL Editor Settings - POSIX and NFSv4

Select any user account or group manually entered or imported from a directory service in the **Owner** or **Owner Group**. The value entered or selected in each field displays in the **Access Control List** below these fields.

Dataset displays the dataset path (name) you selected to edit.



Access Control List - POSIX and NFS4

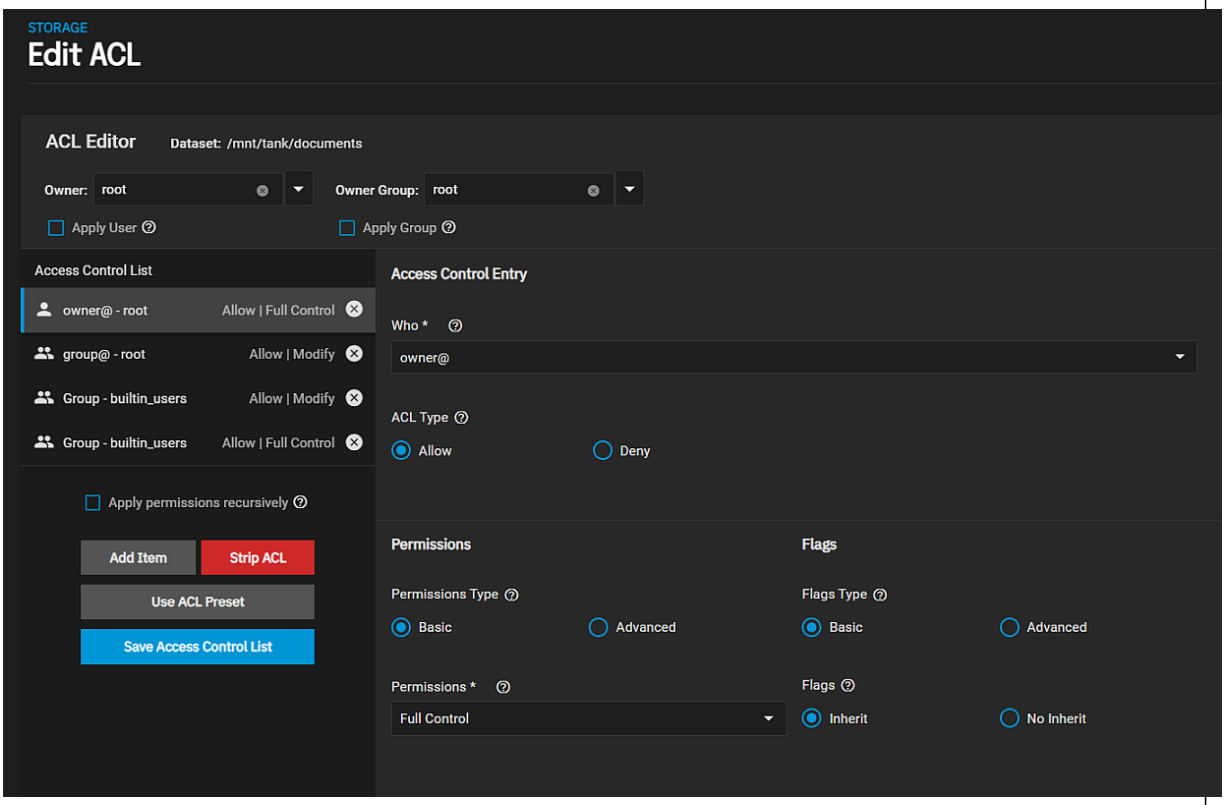
The **Access Control List** section displays the items and a permissions summary for the **owner@**, **group@**, and **everyone@** for both POSIX and NSFv4 ACL types. The list of items changes based on a selected pre-configured set of permissions.

To add a new item to the ACL, click **Add Item**, define **Who** the Access Control Entry (ACE) applies to, and configure permissions and inheritance flags for the ACE.

Edit ACL Functions - POSIX and NFS4

These functions display on the **Edit ACL** screen for both POSIX and NSFv4 ACL types except for **Strip ACL**, which only displays for NSFv4 types.

Click here for details

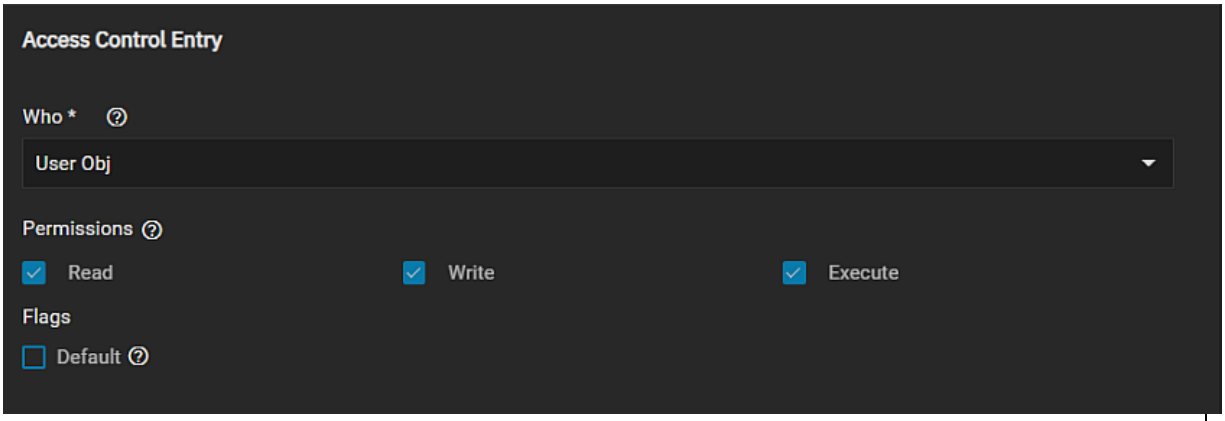


Setting	Description
Apply permissions recursively	Select to apply all settings or changes on the **Edit ACL** screen to all child datasets in the path in **Dataset**.
Add Item	Adds a new ACE to the **Access Control List**.
Strip ACL	(NSFv4 only) Remove all ACLs from the current dataset and any directories or files contained within this dataset. Stripping the ACL resets dataset permissions and can make data inaccessible until you create new permissions.
Permissions Editor	(POSIX only) Displays the **Unix Permissions Editor** screen for POSIX ACL types.
Use ACL Preset	Displays the **Select a preset ACL** window. If the **ACL Type** setting, found in the **Advanced Options** of both the **Add Dataset** and **Edit Dataset** screens, is **POSIX** or **Inherit** the **Default ACL Options** dropdown displays POSIX pre-configured options. If set to NFSv4, the preset options displayed are pre-configured NSFv4 options.
Save Access Control List	Saves settings or changes made on the **Edit ACL** screen.

POSIX Access Control Entry Settings

The POSIX **Access Control Entry** settings include **Who**, **Permissions** and **Flags** options.

Click here for details



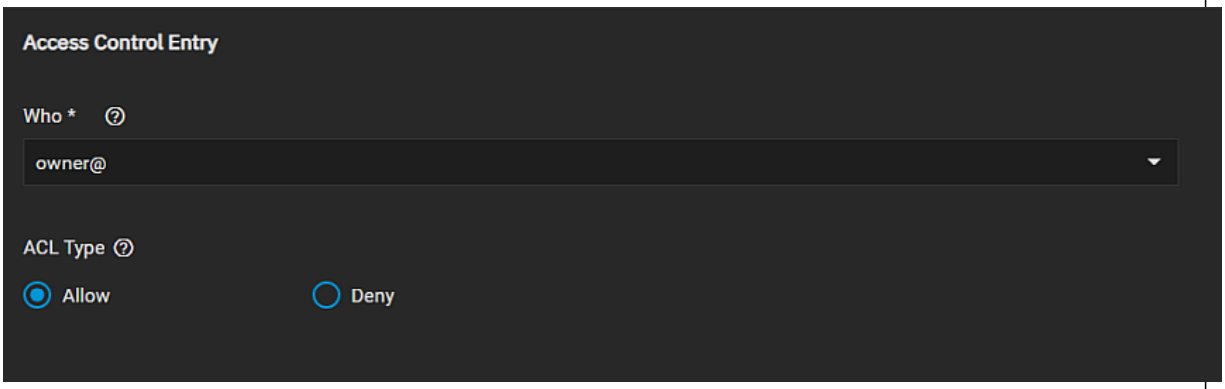
Setting	Description
Who	Select the user or group from the dropdown list the permissions apply to.
Permissions	Select the checkbox for each permission type (**Read**, **Write** and **Execute**) to apply to the user or group in **Who**. "
Flags	Select the **Default** option to include a flag setting for the user or group in **Who**.

NFS4 Access Control Entry Settings

There are two **Access Control Entry** settings, **Who** and **ACL Type**.

Click here for details

The NFSv4 **ACL Type** radio buttons change the **Permissions** and **Flags** setting options. Select **Allow** to grant the specified permissions or **Deny** to restrict the permissions for the user or group in **Who**.



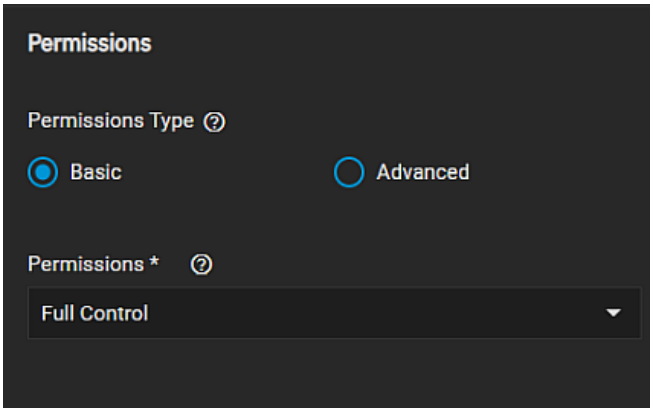
NFS4 Permissions and Flags

TrueNAS divides permissions and inheritance flags into basic and advanced options. The basic permissions options are commonly-used groups of advanced options. Basic inheritance flags only enable or disable ACE inheritance. Advanced flags offer finer control for applying an ACE to new files or directories.

Permissions Settings - Basic

Click the **Basic** radio button to display the **Permissions** dropdown list of options that applies to the user or group in **Who**.

Click here for details

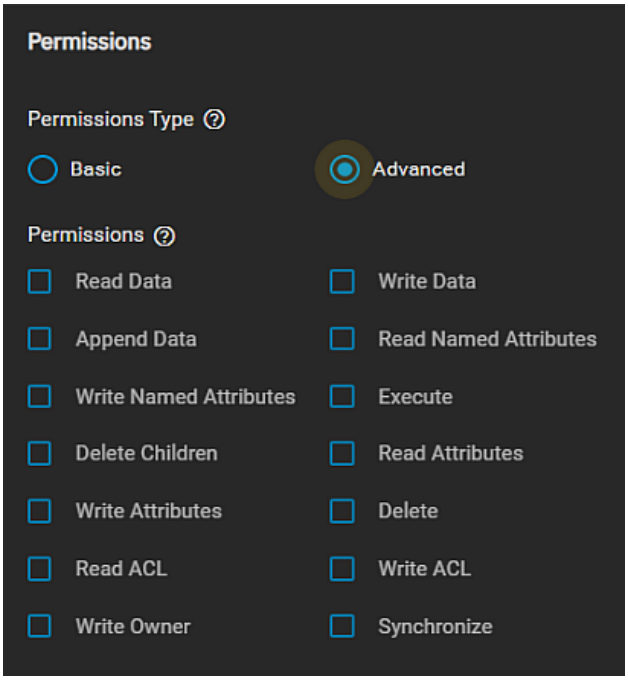


Permission	CLI Command	Description
Read	`r-x---a-R-c---`	View file or directory contents, attributes, named attributes, and ACL.
Modify	`rwxpDdaARWc--s`	Adjust file or directory contents, attributes, and named attributes. Create new files or subdirectories. Includes the *Traverse* permission.
Traverse	`--x---a-R-c---`	Execute a file or move through a directory.
Full Control	`rwxpDdaARWcCos`	Apply all permissions.

Permissions Settings - Advanced

Click the **Advanced** radio button to display the **Permissions** options that apply to the user or group in **Who**.

Click here for details ↕



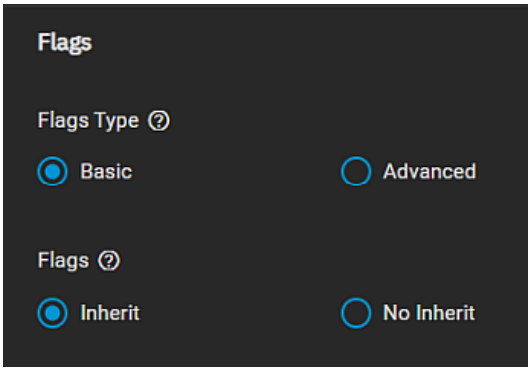
Permission	CLI Command	Description
Read Data	`r`	View file contents or list directory contents.
Write Data	`w`	Create new files or modify any part of a file.
Append Data	`p`	Add new data to the end of a file.
Read Named Attributes	`R`	View the named attributes directory.
Write Named Attributes	`W`	Create a named attribute directory. Must be paired with the Read Named Attributes permission.

Permission	CLI Command	Description
Execute	x	Execute a file, move through, or search a directory.
Delete Children	D	Delete files or subdirectories from inside a directory.
Read Attributes	a	View file or directory non-ACL attributes.
Write Attributes	A	Change file or directory non-ACL attributes.
Delete	d	Remove the file or directory.
Read ACL	c	View the ACL.
Write ACL	C	Change the ACL and the ACL mode.
Write Owner	o	Change the user and group owners of the file or directory.
Synchronize	s	Synchronous file read/write with the server. This permission does not apply to FreeBSD clients.

Flag Settings - Basic

Click the **Basic** radio button to display the flag settings that enable or disable ACE inheritance.

Click here for details

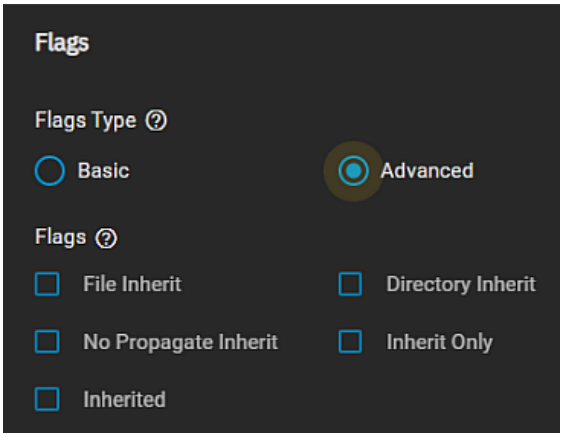


Flag	CLI Command	Description
Inherit	fd-----	Enable ACE inheritance.
No Inherit	-------	Disable ACE inheritance.

Flag Settings - Advanced

Click the **Advanced** radio button to display the flag settings that not only enable or disable ACE inheritance but also offer finer control for applying an ACE to new files or directories.

Click here for details



Flag	CLI Command	Description
File Inherit	`f`	The ACE is inherited with subdirectories and files. It applies to new files.
Directory Inherit	`d`	New subdirectories inherit the full ACE.
No Propagate Inherit	`n`	The ACE can only be inherited once.
Inherit Only	`i`	Remove the ACE from permission checks but allow new files or subdirectories to inherit it. Inherit Only is removed from these new objects.
Inherited	`I`	Set when this dataset inherits the ACE from another dataset.

Related Content

- Managing SMB Shares
- Adding and Managing Datasets
- Setting Up Permissions

Related Dataset Articles

- Advanced Settings Screen
- User and Group Quota Screens
- Adding and Managing Datasets
- Setting Up Permissions
- Storage Encryption
- Managing User or Group Quotas

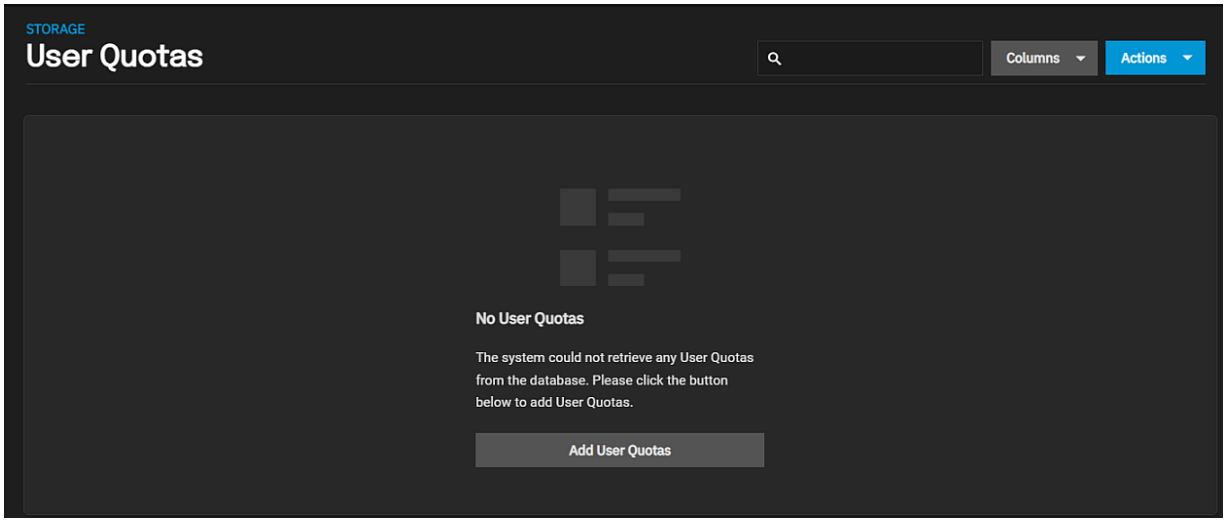
4.3.1.5 - User and Group Quota Screens

This article provides information on User and Group Quota screen settings and functions.

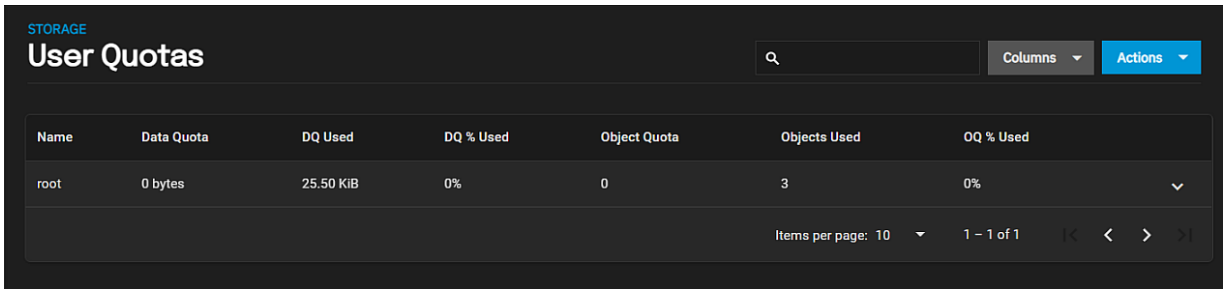
TrueNAS allows setting data or object quotas for user accounts and groups cached on or connected to the system.

User Quotas Screen

Select **User Quotas** on the **Dataset Actions** list of options to display the **User Quotas** screen. The **User Quotas** screen displays the names and quota data of any user accounts cached on or connected to the system. If no users exist, the screen displays the **Add Users Quotas** button in the center of the screen.



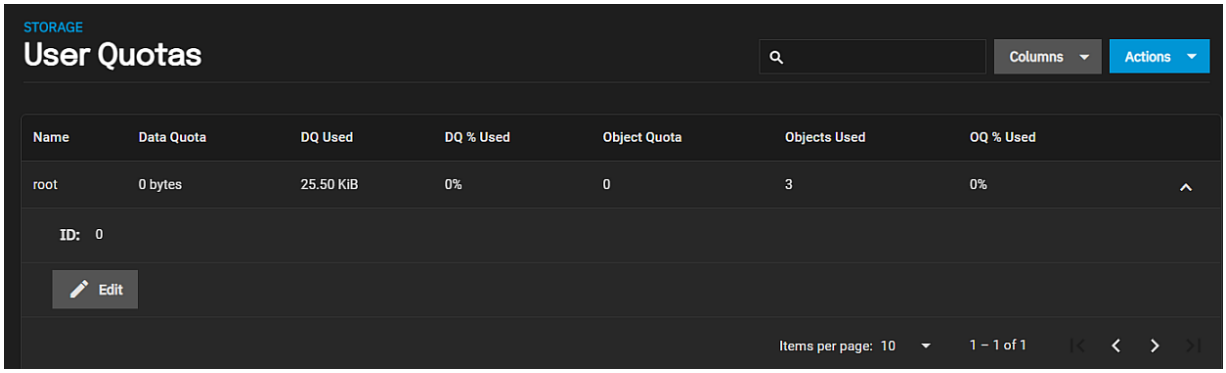
The **Actions** button displays two options, **Add** which displays the **Set User Quotas** screen and **Toggle Display**. **Toggle Display** changes the view from filter view to a list view. Click when the screen filters out all users except those with quotas. The **Show all Users** confirmation dialog displays. Click **Show** to display the list of all users. If you have a number of user quotas set up, the **Actions** options include **Set Quotas (Bulk)**.



Use the **Columns** button to displays options to customize the table view to add or remove information. Options are **Select All**, **ID**, **Data Quota**, **DQ Used**, **DQ % Used**, **Object Quota**, **Objects Used**, **OQ % Used**, and **Reset to Defaults**. After selecting **Select All** the option toggles to **Unselect All**.

User Expanded View

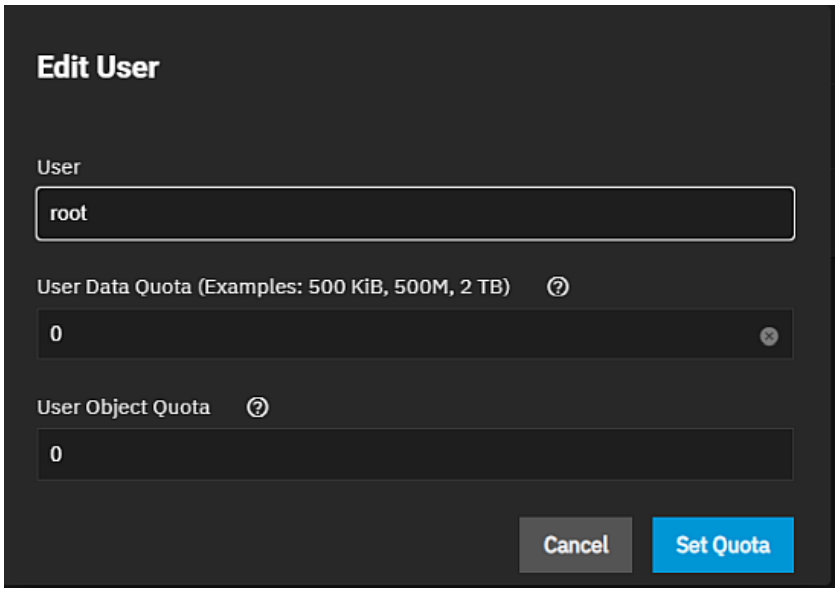
Click the ⌄ icon to display a detailed individual user quota screen.



Click the **Edit** button to display the **Edit User** window.

Edit User Configuration Window

The **Edit User** window allows you to modify the user data quota and user object quota values for an individual user.

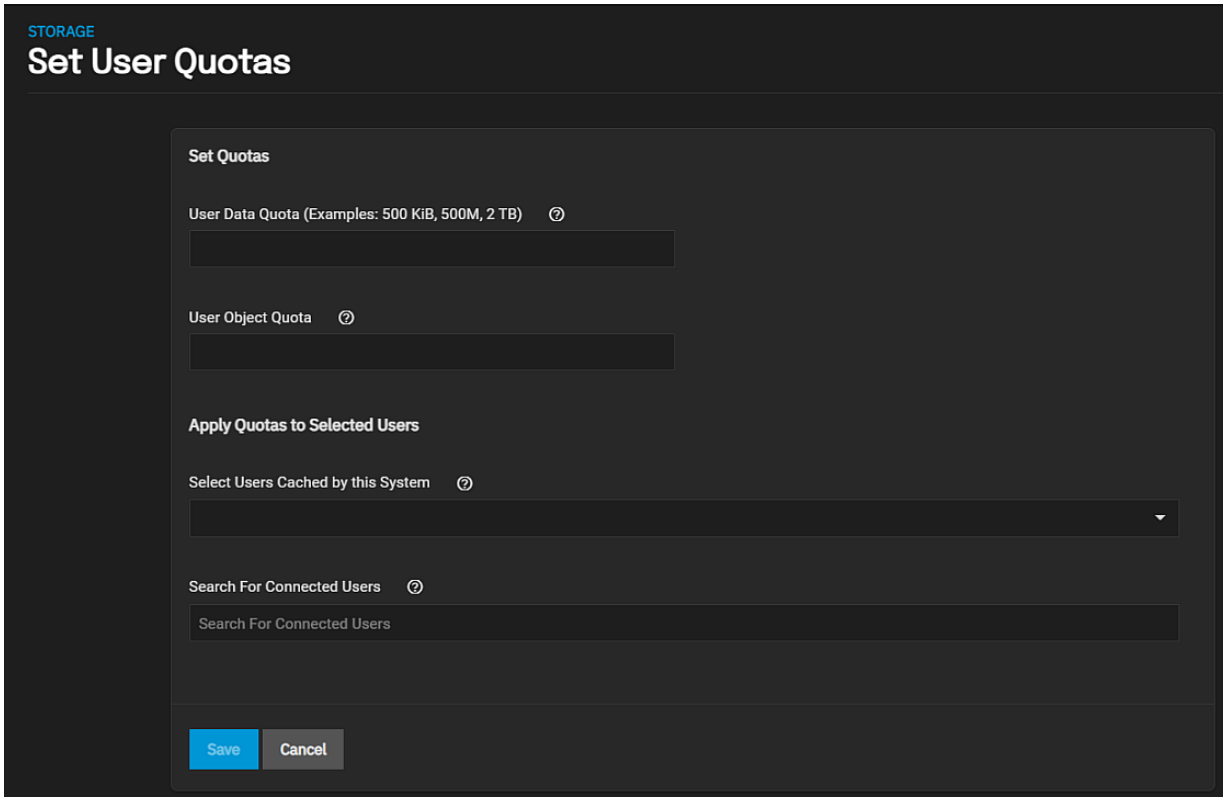


Settings	Description
User	Displays the name of the selected user.
User Data Quota (Examples: 500KiB, 500M, 2 TB)	Enter the amount of disk space the selected user can use. Entering **0** allows the user to use all disk space. You can enter human-readable values such as 50 GiB, 500M, 2 TB, etc.). If units are not specified, the value defaults to bytes.
User Object Quota	Enter the number of objects the selected user can own. Entering **0** allows unlimited objects.

Click **Set Quota** to save changes or **Cancel** to close the window without saving.

Set User Quotas Screen

To display the **Set User Quotas** screen click **Actions** or if the system does not have user quotas configured, click the **Add User Quotas** button.



Set Quotas Settings

Settings	Description
User Data Quota (Examples: 500KiB, 500M, 2 TB)	Enter the amount of disk space the selected user can use. Entering **0** allows the user to use all disk space. You can enter human-readable values such as 50 GiB, 500M, 2 TB, etc.). If units are not specified, the value defaults to bytes.
User Object Quota	Enter the number of objects the selected user can own. Entering **0** allows unlimited objects.

Apply Quotas to Selected Users Settings

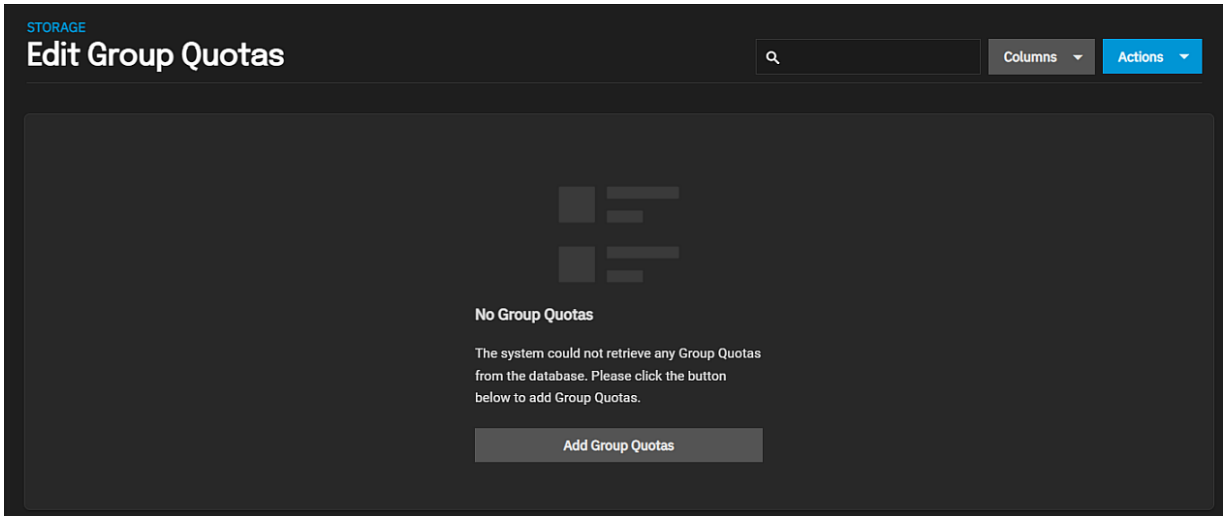
Settings	Description
Select Users Cached by this System	Select the users from the dropdown list of options.
Search for Connected Users	Click in the field to see the list of users on the system or type a user name and press `Enter`. A clickable list displays of found matches as you type. Click on the user to add the name. A warning dialog displays if there are not matches found.

Click **Save** to set the quotas or **Cancel** to exit without saving.

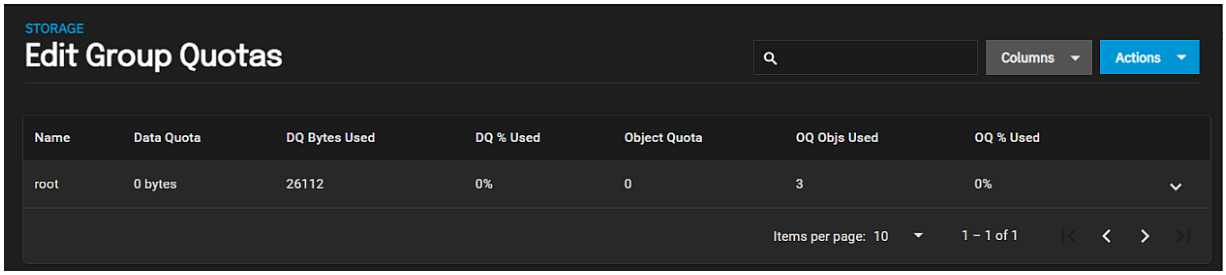
Group Quotas Screens

Select **Group Quotas** on the **Dataset Actions** list of options to display the **Edit Group Quotas** screen.

The **Edit Group Quotas** screen displays the names and quota data of any groups cached on or connected to the system. If no groups exist, the screen displays the **Add Groups Quotas** button in the center of the screen.



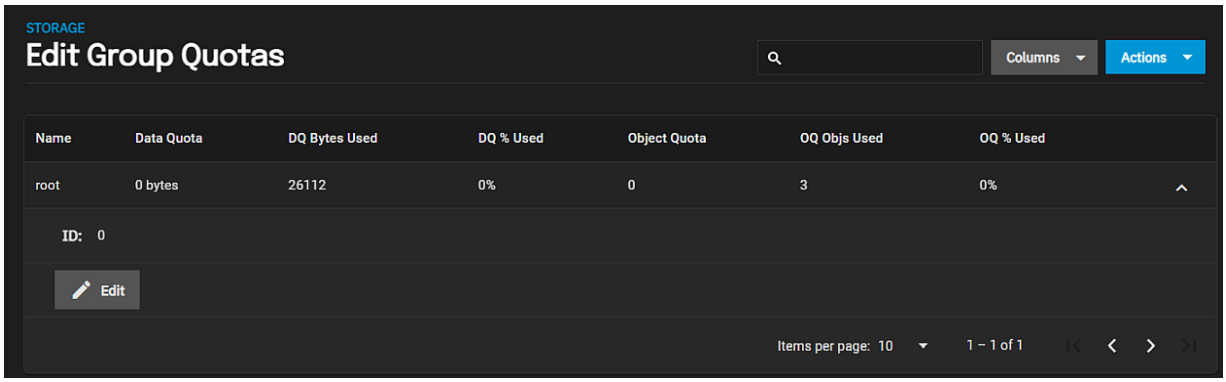
The **Actions** button displays two options, **Add** which displays the **Set Group Quotas** screen and **Toggle Display**. **Toggle Display** changes the view from filter view to a list view. Click when the screen filters out all groups except those with quotas. The **Show all Groups** confirmation dialog displays. Click **Show** to display the list of all groups.



Use the **Columns** button to displays options to customize the table view to add or remove information. Options are **Select All**, **ID**, **Data Quota**, **DQ Used**, **DQ % Used**, **Object Quota**, **Objects Used**, **OQ % Used**, and **Reset to Defaults**. After selecting **Select All** the option toggles to **Unselect All**.

Group Expanded View

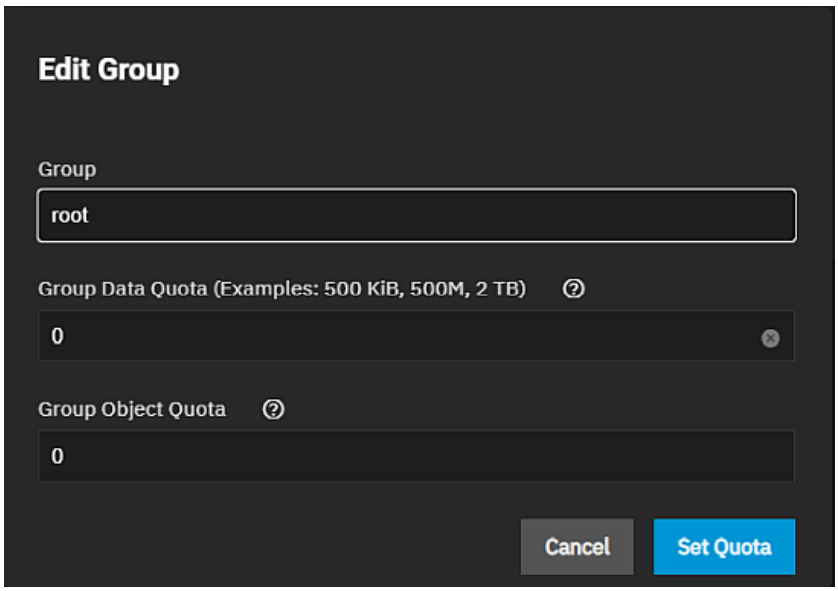
Click the ⌄ icon to display a detailed individual group quota screen.



Click the ✎ **Edit** button to display the **Edit Group** window.

Edit Group Configuration Window

The **Edit Group** window allows you to modify the group data quota and group object quota values for an individual group.

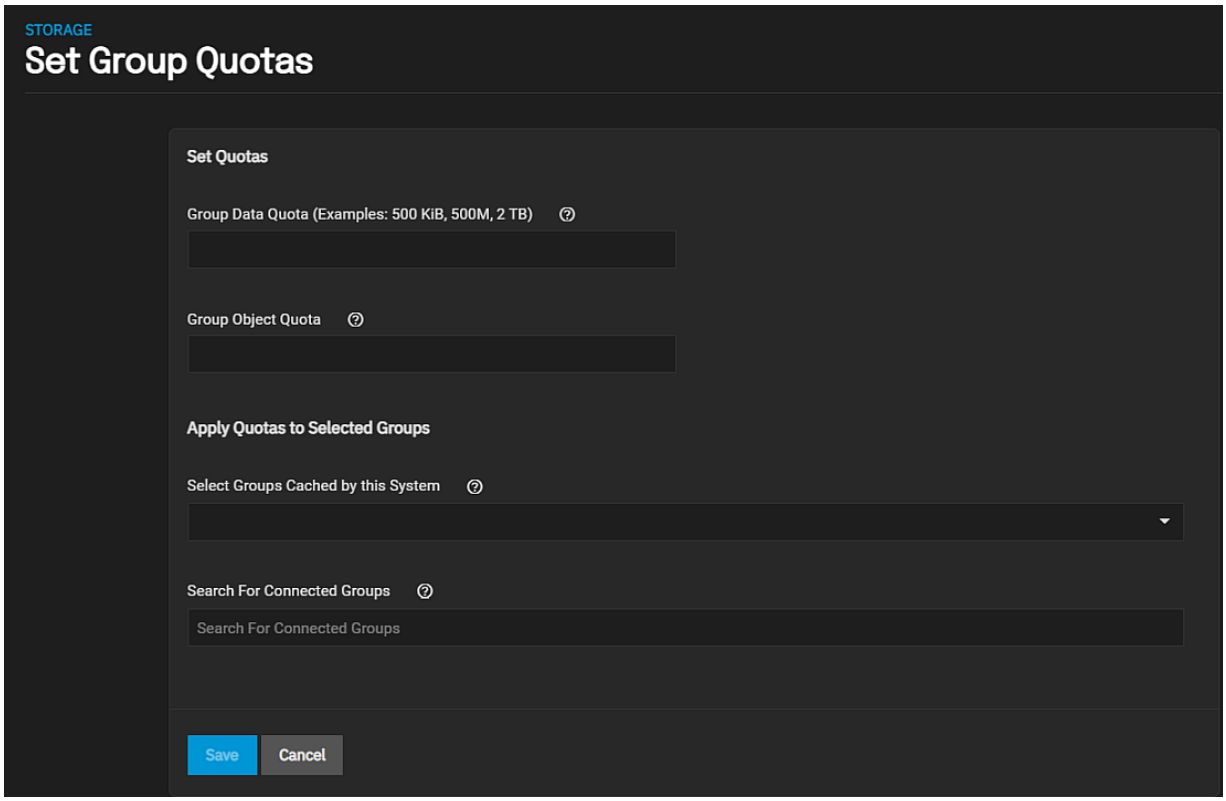


Settings	Description
Group	Displays the name of the selected group(s).
Group Data Quota (Examples: 500KiB, 500M, 2 TB)	Enter the amount of disk space the selected group can use. Entering **0** allows the group to use all disk space. You can enter human-readable values such as 50 GiB, 500M, 2 TB, etc.). If units are not specified, the value defaults to bytes.
Group Object Quota	Enter the number of objects the selected group can own or use. Entering **0** allows unlimited objects.

Click **Set Quota** to save changes or **Cancel** to close the window without saving.

Set User Quotas Screen

To display the **Set Group Quotas** screen click **Actions** or if the system does not have group quotas configured, click the **Add Group Quotas** button.



Set Quotas Settings

Settings	Description
Group Data Quota (Examples: 500KiB, 500M, 2 TB)	Enter the amount of disk space the selected group can use. Entering **0** allows the group to use all disk space. You can enter human-readable values such as 50 GiB, 500M, 2 TB, etc.). If units are not specified, the value defaults to bytes.
Group Object Quota	Enter the number of objects the selected group can own or use. Entering **0** allows unlimited objects.

Apply Quotas to Selected Groups Settings

Settings	Description
Select Groups Cached by this System	Select the users from the dropdown list of options.
Search for Connected Groups	Click in the field to see the list of groups on the system or type a group name and press `Enter`. A clickable list displays of found matches as you type. Click on the group to add the name. A warning dialog displays if there are no matches found.

Click **Save** to set the quotas or **Cancel** to exit without saving.

Related Content

- Adding and Managing Datasets
- Managing User or Group Quotas

Related Dataset Articles

- Advanced Settings Screen
- Edit ACL Screens
- Adding and Managing Datasets
- Setting Up Permissions
- Storage Encryption
- Managing User or Group Quotas

4.3.2 - Disks

This section describes UI screens and dialogs related to disk operations.

- Disks Screens

  This article provides information on the settings found on and functions of the Disks Screens.

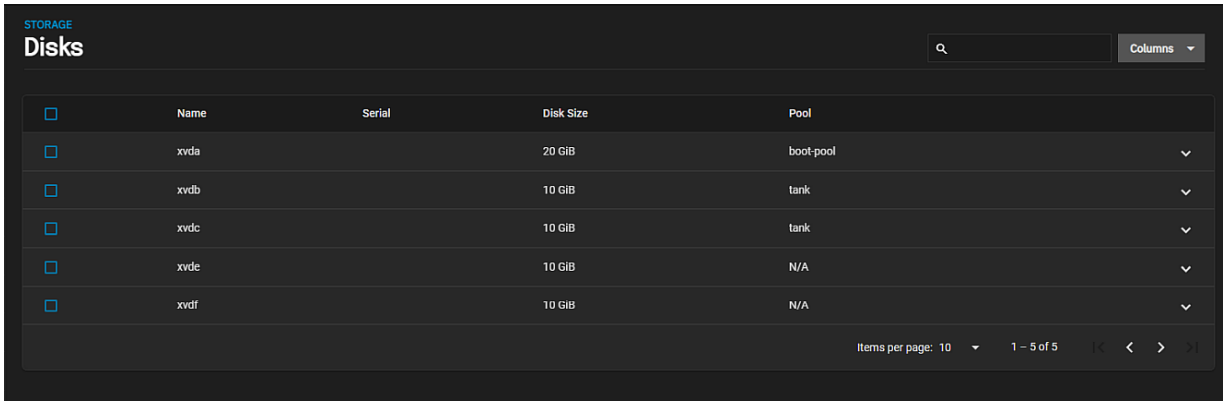
4.3.2.1 - Disks Screens

This article provides information on the settings found on and functions of the Disks Screens.

Use the disk screens to manage disk settings for all physical drives installed in your system.

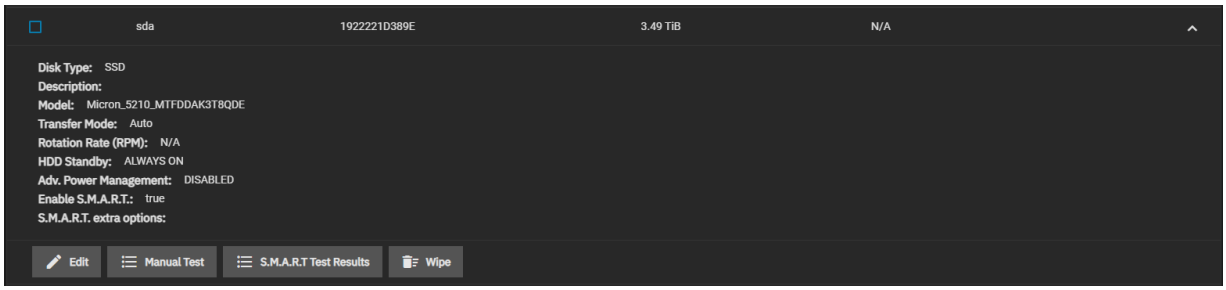
Disk Screen

The **Disks** screen displays a list of the physical drives (disks) in the system. The list includes the names, serial numbers, sizes, and pools for the system disks.



Use the **Columns** dropdown list to select options to customize disk columns displayed. Options are **Select All**, **Serial** (the disk serial number), **Disk Size**, **Pool** (where the disk is in use), **Disk Type**, **Description**, **Model**, **Transfer Mode**, **Rotation Rate (RPM)**, **HDD Standby**, **Adv. Power Management**, **Enable S.M.A.R.T.**, **S.M.A.R.T. extra options**, and **Reset to Defaults**. The information you enter in the **Edit Disk** screen or when you install the disk displays for each of these column options.

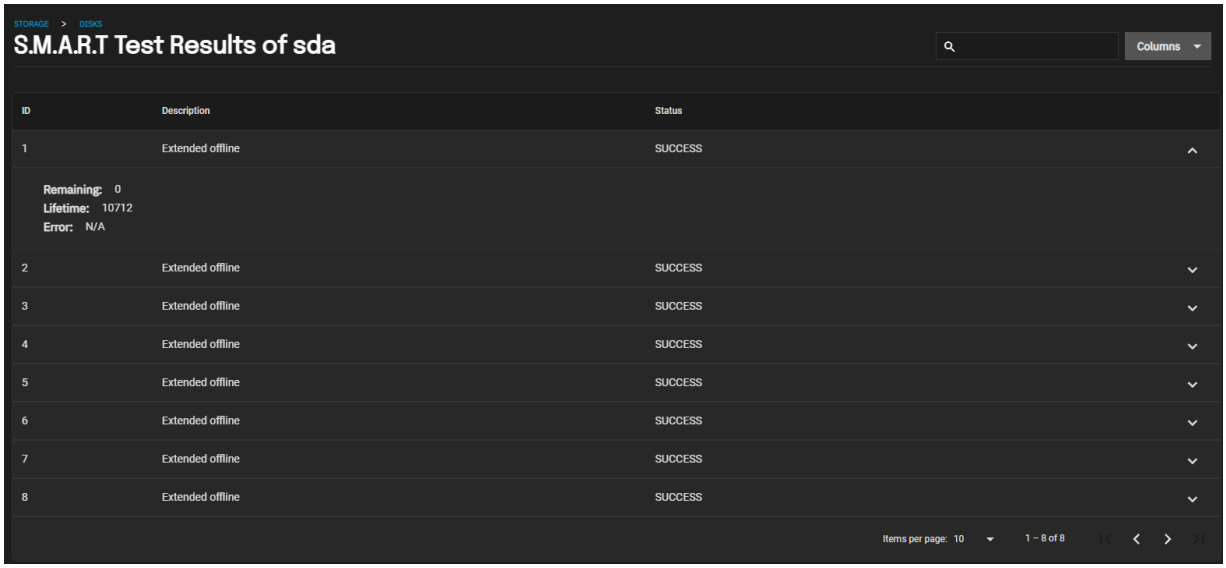
Click the the for a disk to expand it and show the traits specific to that disk.



Click **Edit** to display the **Edit Disk** screen.

Click **Manual Test** to initiate a S.M.A.R.T. test of the disk.

Click **S.M.A.R.T. Test Results** to open a new screen to view the results of each S.M.A.R.T. test that has run against that disk. In the test results screen, click an entry to view the results of the test:

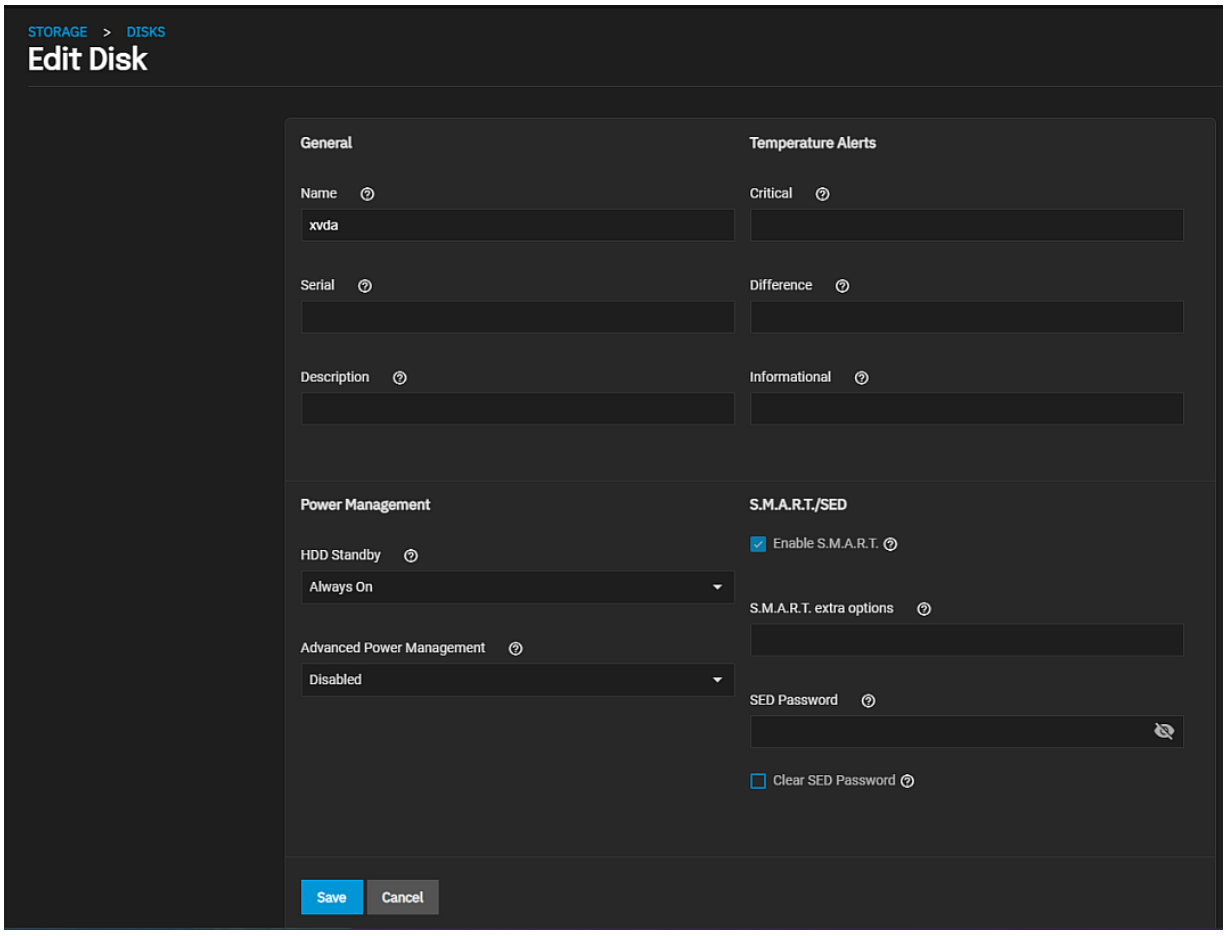


- **Remaining** shows how much of the test is left to perform. If the test encountered an error, the field shows at what point in the test the error occurred. A value of **0** means the test completed and no errors were encountered.
- **Lifetime** shows the age of the disk when the test ran.
- **Error** shows **N/A** when no error was encountered during the test. If an error is encountered, this field shows details about the error.

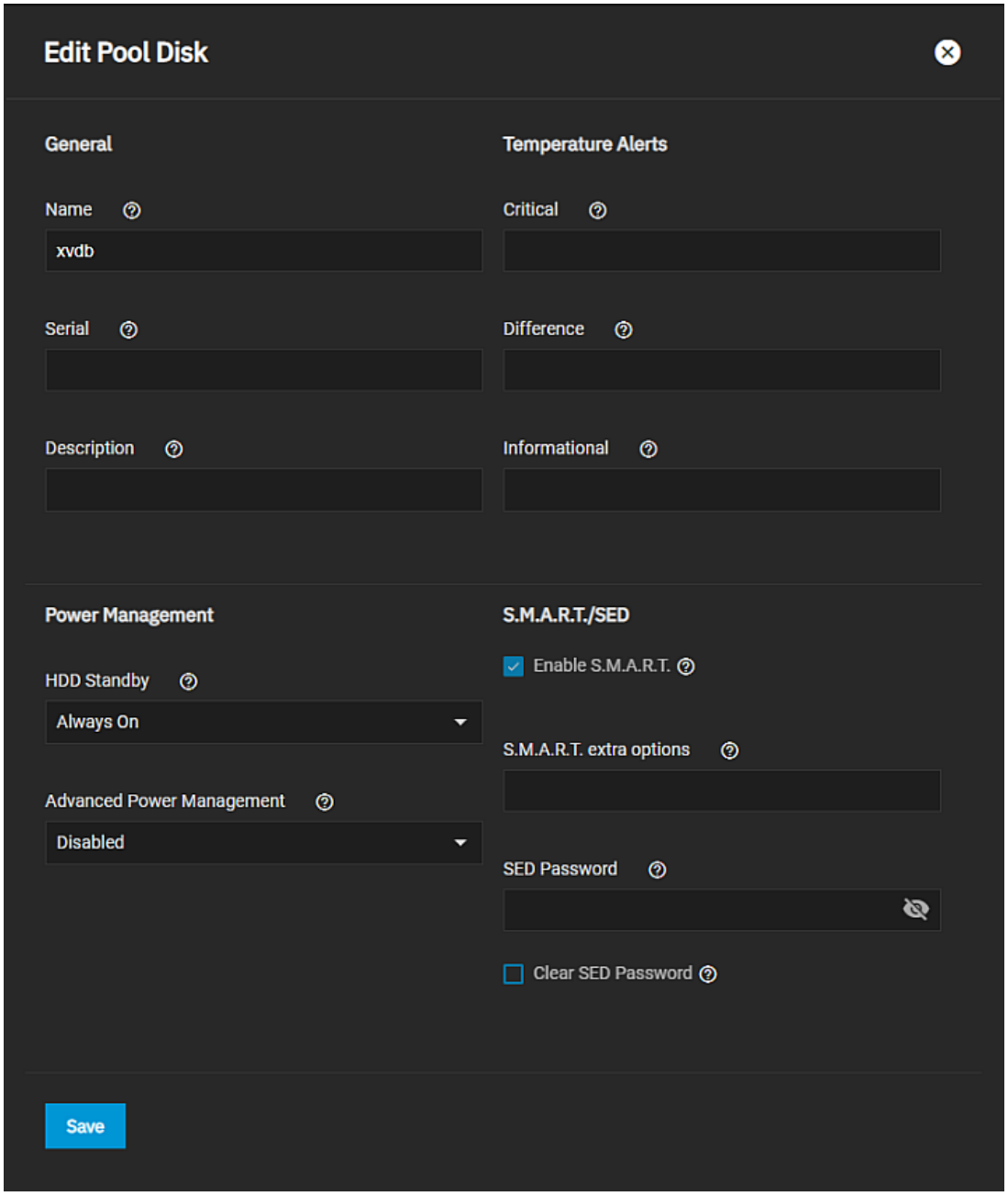
Click **Wipe** to wipe data from the disk. See Wiping Disks for more information.

Edit Disk Screen

The **Edit Disk** screen allows users to configure general disk, power management, temperature alert, S.M.A.R.T. and SED settings for system disks not assigned to a pool.



The **Edit Pool Disk** screen, accessed from the **Pool Status** screen, displays the same settings found on the **Edit Disk** screen you use when editing settings for disks assigned to a storage pool. Click the ⋮ for the disk to display the **Disk Actions** menu and select **Edit**.



General Settings

Setting	Description
Name	Enter a Linux disk device name.
Serial	Enter the disk serial number.
Description	Enter notes about this disk.

Power Management Settings

Setting	Description
HDD Standby	Select a value from the dropdown list of options or leave set to the default **Always On**. This specifies the minutes of inactivity before the drive enters standby mode. This forum post describes identifying spun down drives. Temperature monitoring is disabled for standby disks.
Advanced Power Management	Select a power management profile from the dropdown list of options that include **Disabled** (the default setting), **Level 1 - Minimum power usage with Standby (spindown)**, **Level 64 - Intermediate power usage with Standby**, **Level 127 - Maximum power usage with Standby**, **Level 128 - Minimum power usage withoout Standby (no spindown)**, **Level 192 - Intermediate power usage without Standby**, or **Level 254 - Maximum performance, maximum power usage**.

Temperature Alerts Settings

Setting	Description
Critical	Enter a threshold temperature in Celsius. If the drive temperature is higher than this value, it creates a LOG_CRIT level log entry and sends an email to the address entered in the Alerts. Enter **0** to disable this check.
Difference	Enter a value in degrees Celsius that triggers a report if the temperature of a drive changes by this value since the last report. Enter **0** to disable this check.
Informational	Enter a value in degrees Celsius that triggers a report if drive temperature is at or above this temperature. Enter **0** to disable this check.

S.M.A.R.T./SED Settings

Setting	Description
Enable S.M.A.R.T.	Select to enable the system to conduct periodic S.M.A.R.T. tests.
S.M.A.R.T. extra options	Enter additional smartctl(8) options.
SED Password	Enter a password to set or change the password of the SED for this disk and to use instead of the global SED password.
Clear SED Password	Select to clear the SED password for this disk.

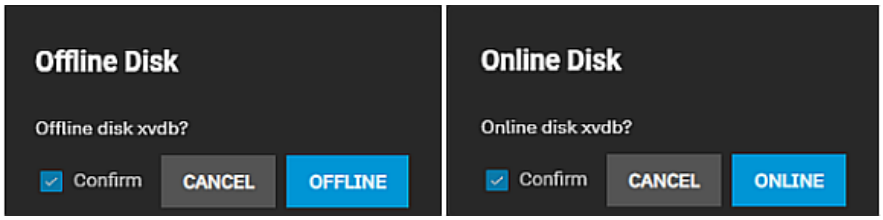
Disk Actions Options

The **Disk Actions** dropdown list provides options to edit, place a disk offline or online, replace, remove or detach a disk associated with a pool. To access these options, from the **Pool Status** screen, click the ⋮ for the disk.

Edit displays the **Edit Pool Disk** settings screen described in the section above.

Offline or Online Options

The **Offline** and **Online** options each display a confirmation dialog where you must confirm this action before the system initiates the process to take the disk offline or bring a disk online. Each diplays a status spinner that provides status the operation is in progress. You can also use the **Task Manager** to monitor the process. Both processes can take a while to complete.



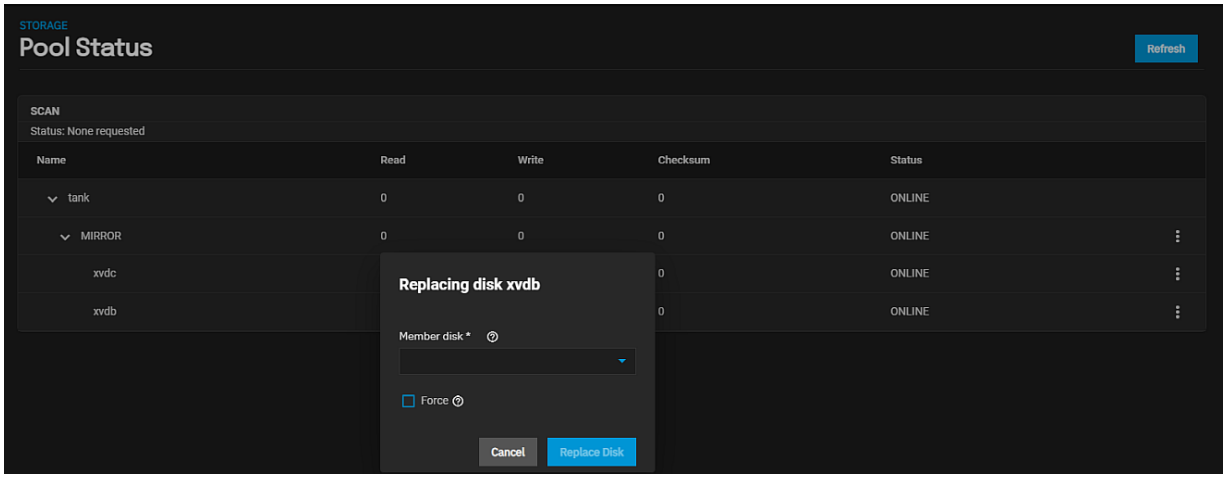
When the offline or online process completes the **Status** display changes to reflect the new status of that disk.

Replace Option

The **Replace** option displays a confirmation dialog for the disk selected. Select the disk from the **Member disk** dropdown list that to use as the replacement disk. The disk selected in **Member disk** is stopped if that disk is currently in use or if it has partitions present. To override this protection you must select **Force**.

> Replacing a disk can be a destructive process resulting in lost data especially if you use the **Force** option. Always back up all data before performing a replace operation as data might not be recoverable.

Force overrides the safety checks and adds the disk to the pool. This erases any data on the disk! Be sure you selected the correct disk before you use this option.

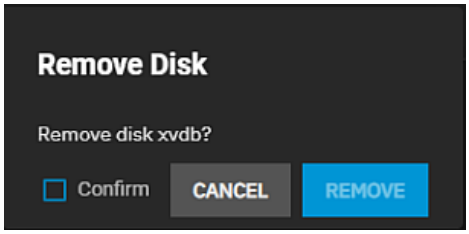


After you select the disk the **Replace Disk** button activates. Click to begin the replacement process.

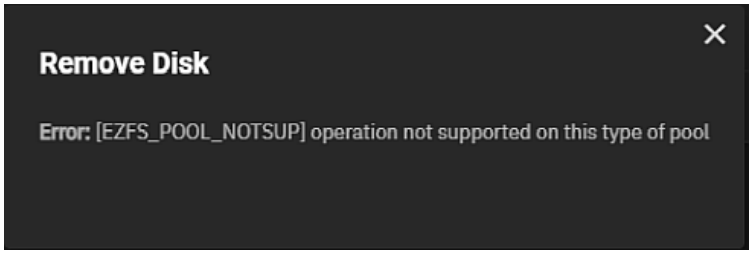
Remove Option

The **Remove** option removes a disk used as a hot spate, cache or log device. A confirmation dialog displays before the system performs the operation. You must select **Confirm** to activate the **Remove** button.

> Removing a disk can be a destructive process resulting in lost data. Always back up all data before performing a remove operation as data might not be recoverable.

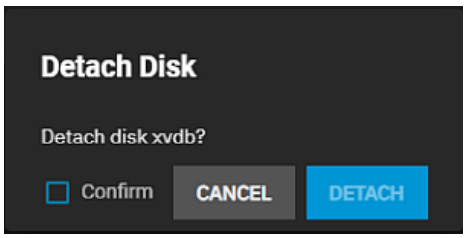


Click **Remove** to execute this operation. If you attempt to remove a disk you should not remove an **Failed** error window displays with information about the failed process.



Detach Option

The **Detach** option detaches a disk from a mirror only if another valid replica of the data exists, if not the operation is refused and an error message displays. A confirmation dialog displays where you must select **Confirm** before the **Detach** button activates. Select **Detach** to execute the process.



> Detaching a disk can be a destructive process resulting in lost data. Always back up all data before performing a detach operation as data might not be recoverable.

Related Content

- Advanced Settings Screen

- Managing Disks
- Importing Disks
- Managing SEDs
- Replacing Disks
- View Enclosure Screen
- Wiping a Disk
- SLOG Over-Provisioning

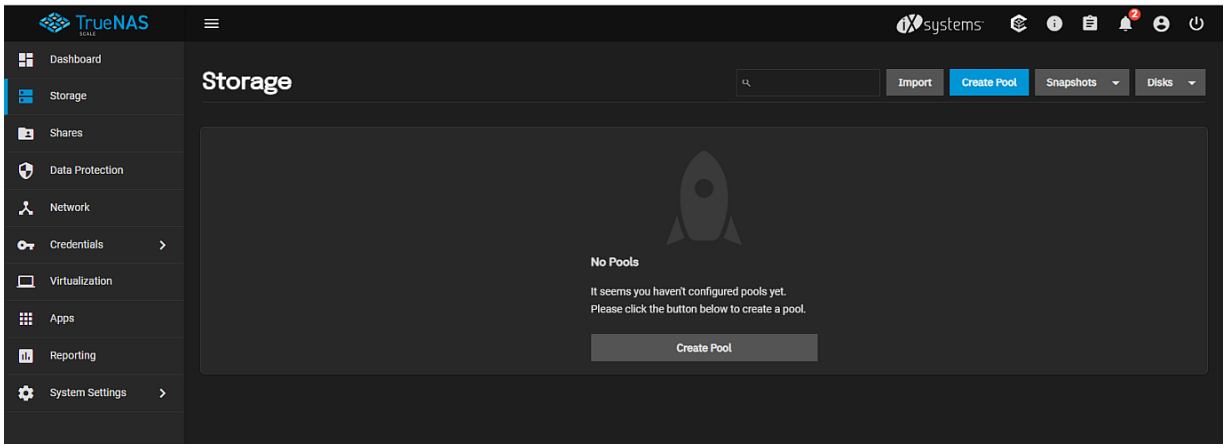
Related Storage Articles

- Storage Screens
- Snapshots Screens
- Setting Up Storage
- Zvol Screens
- Creating Storage Pools
- Edit ACL Screens
- Importing Storage Pools
- Adding and Managing Datasets
- Installing and Managing Self-Encrypting Drives
- Adding and Managing Zvols

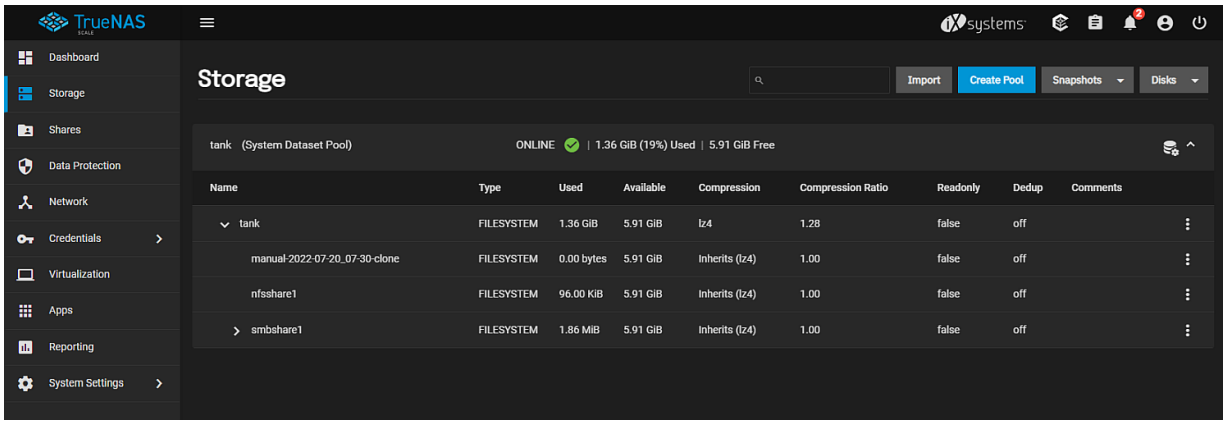
4.3.3 - Storage Screens

This article provides information on the **Storage** screen and options for pools, datasets or zvols listed on this screen.

The **Storage** screen displays a list of all the pools and datasets or zvols configured in your TrueNAS. If the system does not have any pools, it displays the **Create Pool** button in the center of the screen.



After creating pools, datasets and zvols, the screen lists each and provides status of the pool.



The **Storage** screen provides access disk, snapshots, and the pool import or creation wizard screens from the buttons and dropdown lists at the top right of the **Storage** screen.

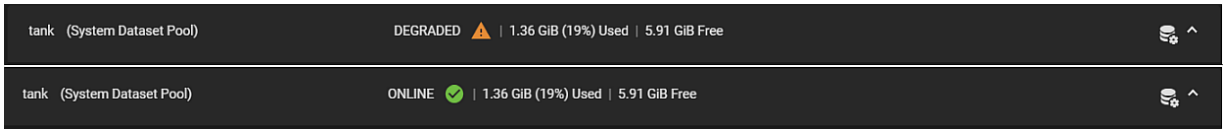
Use **Import** to open the **Import Pool** wizard where users reconnect pools exported/disconnected from the current system or created on another system. Import also reconnects pools after users reinstall or upgrade their TrueNAS system.

Use **Create Pool** to open the **Pool Manager** screen where you crate a ZFS data storage pool with physical disks to effectively store and protect data.

Use the **Snapshots** dropdown to open either the **Snapshots** or **VMware-Snapshots** screen. Snapshots create read-only point-in-time copies of a file system, volume or a running virtual machine.

Use the **Disk** dropdown to open either the **Disks** or **Import Disks** screen. The **Disks** screen lets users manage, wipe, and import storage disks that TrueNAS uses for ZFS storage.

The storage pool displays in a header row that includes the status as online, offline, or degraded and includes a color-coded symbol that corresponds to the state of the pool.



This same information displays on both the **Storage** widget and a pool widget you can add to the **Dashboard**. The pool header includes the **Pool Operations** icon that displays the **Pool Actions** dropdown list of options you can use for storage pools.

Pool Actions List

Click the icon button for the pool to display the **Pool Actions** dropdown list. The options are **Pool Options**, **Export/Disconnect**, **Add Vdevs**, **Scrub Pool**, **Status** and **Expand Pool**. See Pools Screens for more information on the UI screens, dialogs and windows.

Dataset Actions List

Click the ⋮ for a dataset to display the **Dataset Actions** dropdown list. The options are **Add Dataset**, **Add Zvol**, **Edit Options**, **View Permissions**, **User Quotas**, **Group Quotas** and **Create Snapshot**. See Datasets Screens for more information on the UI screens, dialogs and windows.

Zvol Actions List

Click the ⋮ for a dataset to display the **Zvol Actions** dropdown list. The options for the selected zvol are **Delete Zvol**, **Edit Zvol** and **Create Snapshot**. See Zvols Screens for more information on the UI screens, dialogs and windows.

Encryption Options

If you use encryption when you create a pool, the root and child datasets or zvols have the option to inherit the encryption, modify the type of encryption, or not use encryption at all. For more information see Storage Encryption.

If encryption is enabled, the **Dataset Actions** and **Zvol Actions** option lists include the **Encryption Options** list item used to configure encryption settings for that dataset or zvol.

Related Content

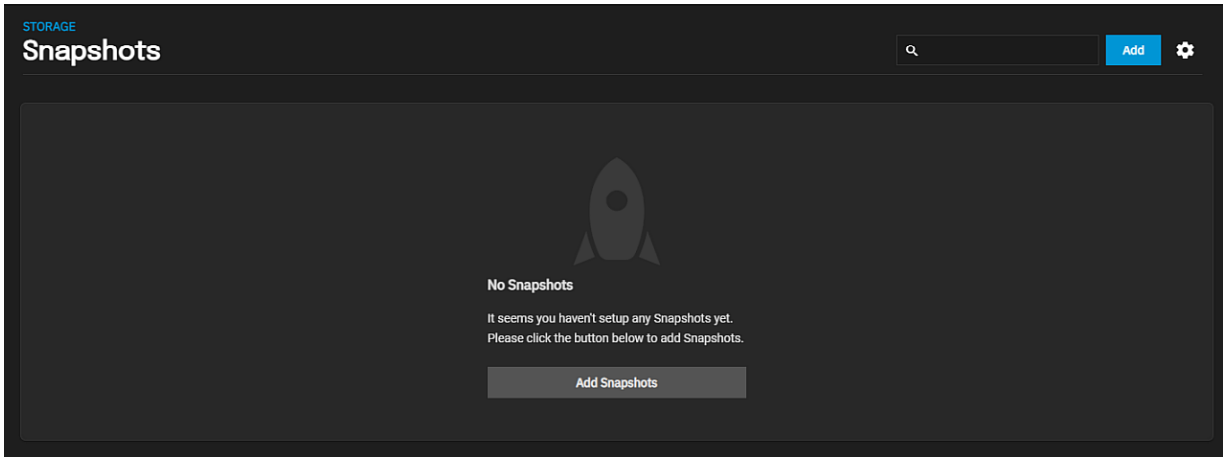
- Snapshots Screens
- Setting Up Storage
- Zvol Screens
- Creating Storage Pools
- Edit ACL Screens
- Importing Storage Pools
- Adding and Managing Datasets
- Installing and Managing Self-Encrypting Drives
- Adding and Managing Zvols

4.3.4 - Snapshots Screens

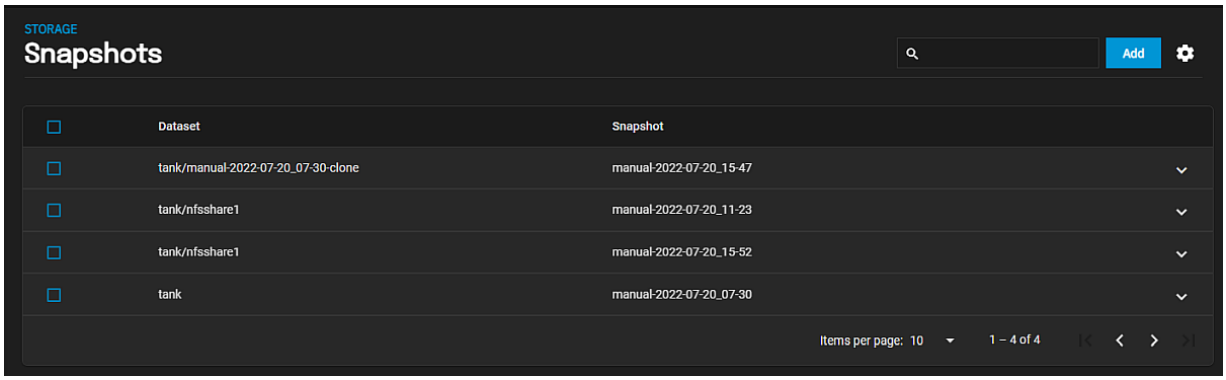
This article provides information on the Snapshots screen settings and functions.

Use the **Snapshots** screen to manage existing snapshots or to add new snapshots. To access the **Snapshots** screen, from the **Storage** screen, click the **Snapshots** button in the top right of the screen and select **Snapshots**.

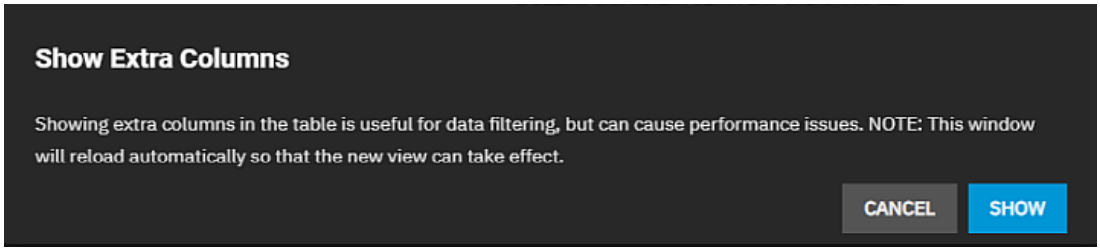
If you don't have snapshots created, the **Snapshots** screen displays the **Add Snapshots** option in the center of the screen.



If you have existing snapshots set up they display in the list on this screen.



Click the ⚙ icon to display the **Show Extra Columns** dialog displays.

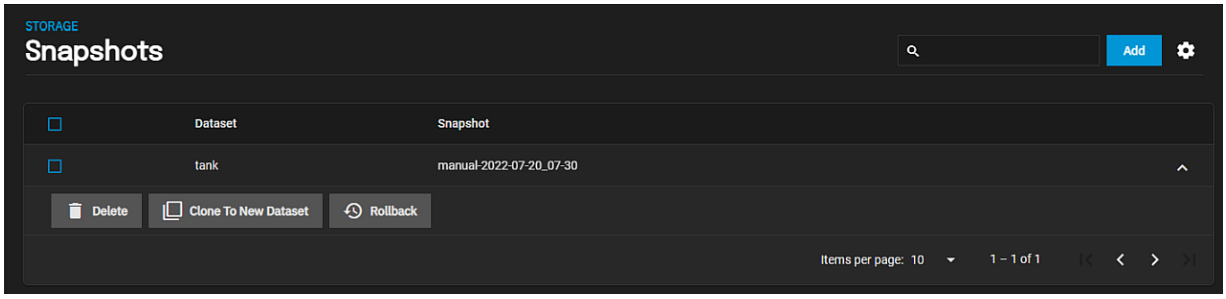


Click **Show** to add the **Used**, **Data Created** and **Referenced** columns to the list of snapshots. These columns add the space used (**Used**), the snapshot creation date, and the amount of data the dataset can access (**Referenced**).

Click the ⚙ icon again to view the **Hide Extra Columns** dialog. Click **Hide** to return to the default view with only the **Dataset** and **Snapshot** columns displayed.

Snapshot Details Screen

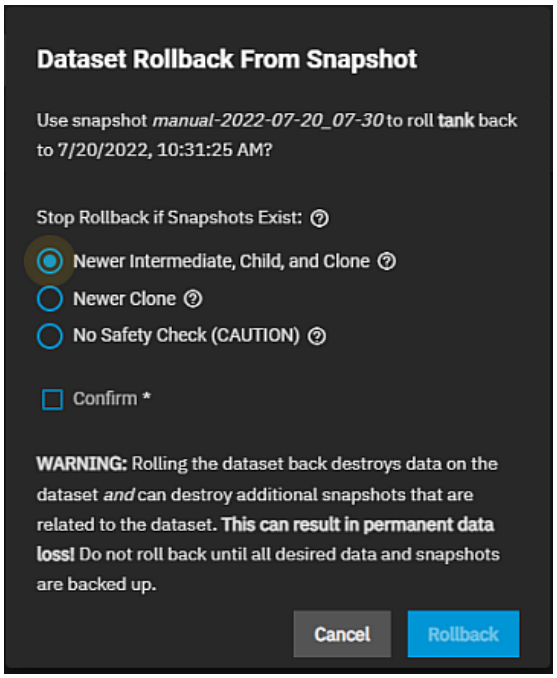
Click ⌄ to view snapshot details an additional options availabe for each snapshot. To view the options for the listed snapshots, click the ⌄ icon to expand the snapshot and display the options for managing that snapshot.



Setting	Icon	Description
Delete	Displays a delete confirmation dialog. Select **Confirm** to activate the *DELETE** button.	
Clone to New Dataset	Displays the **Clone to New Dataset** screen.	
Rollback	Displays the **Dataset Rollback From Snapshot** dialog.	

Dataset Rollback from Snapshot Dialog

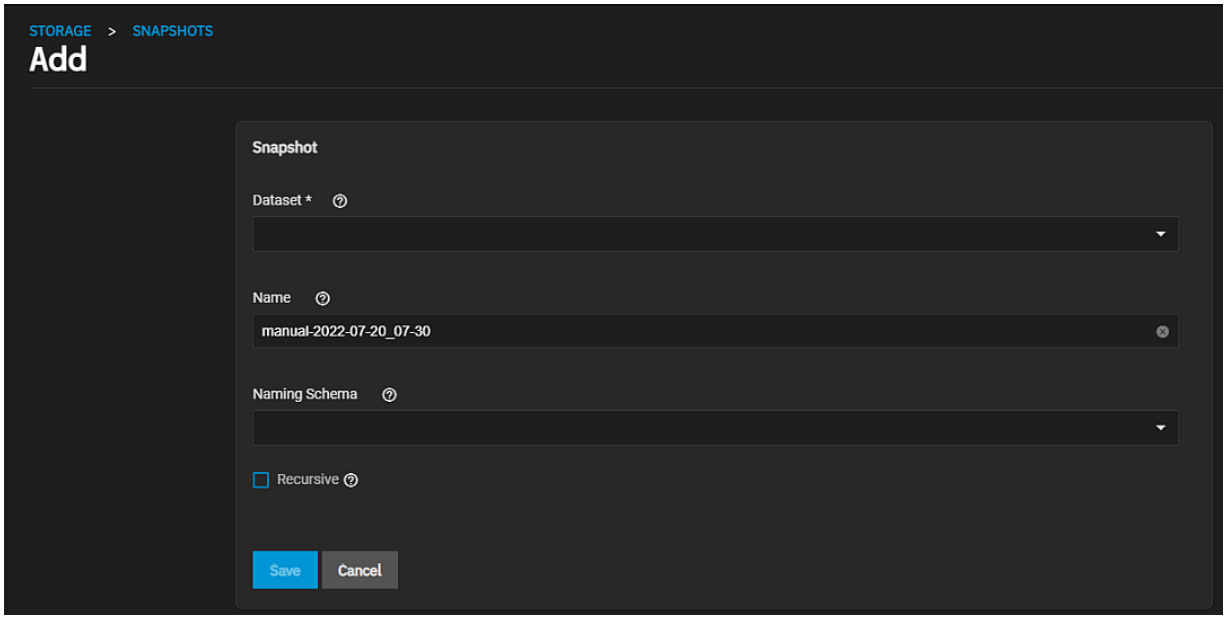
> WARNING: Rolling the dataset back destroys data on the dataset and can destroy additional snapshots that are related to the dataset. This can result in permanent data loss! Do not roll back until all desired data and snapshots are backed up.



Setting	Description
Stop Roolback if Snapshot Exists	Select radio button for the rollback action safety level for the selected snapshot. Select the radio button that best fits. When the safety check finds additional snapshots that are directly related to the dataset being rolled back it cancels the rollback.
Newer intermeidate, Child, and clone	Select to stop rollback when the safety check finds any related intermediate, child dataset, or clone snapshots that are newer than the rollback snapshots.
Newer Clone	Select to stop rollback when the safety check finds any related clone snapshots that are newer than the rollback snapshot.
No Safety Check (CAUTION)	Select to stop rollback if snapshot exists. The rollback destroys any related intermediate, child dataset, and cloned snapshots that are newer than the rollback snapshot.
Confirm	Select to confirm the selection and activate the **ROLLBACK** button.

Add Snapshot Screen

Click either **Add Snapshots** or **ADD** at the top right of the screen to display the **Add Snapshot** screen.



Setting	Description
Dataset	Select the dataset or zvol from the dropdown list. The snapshot created is from this dataset or zvol.
Name	TrueNAS populates this with a name but you can override the name with any string of your choice. You cannot use **Name** and **Naming Schema** for the same snapshot.
Naming Schema	Select an option from the dropdown list or leave this blank to use the name the system or you entered in **Name**. This generates a name for the snapshot using the naming schema from a previously-entered periodic snapshot. This allows the snapshot to be replicated. You cannot use **Naming Schema** with **Name**. Selecting a schema option overwrites the value in **Name**.
Recursive	Select to include child datasets or zvols in the snapshot.

Use **Save** to retain the settings and return to the **Snapshots** screen.

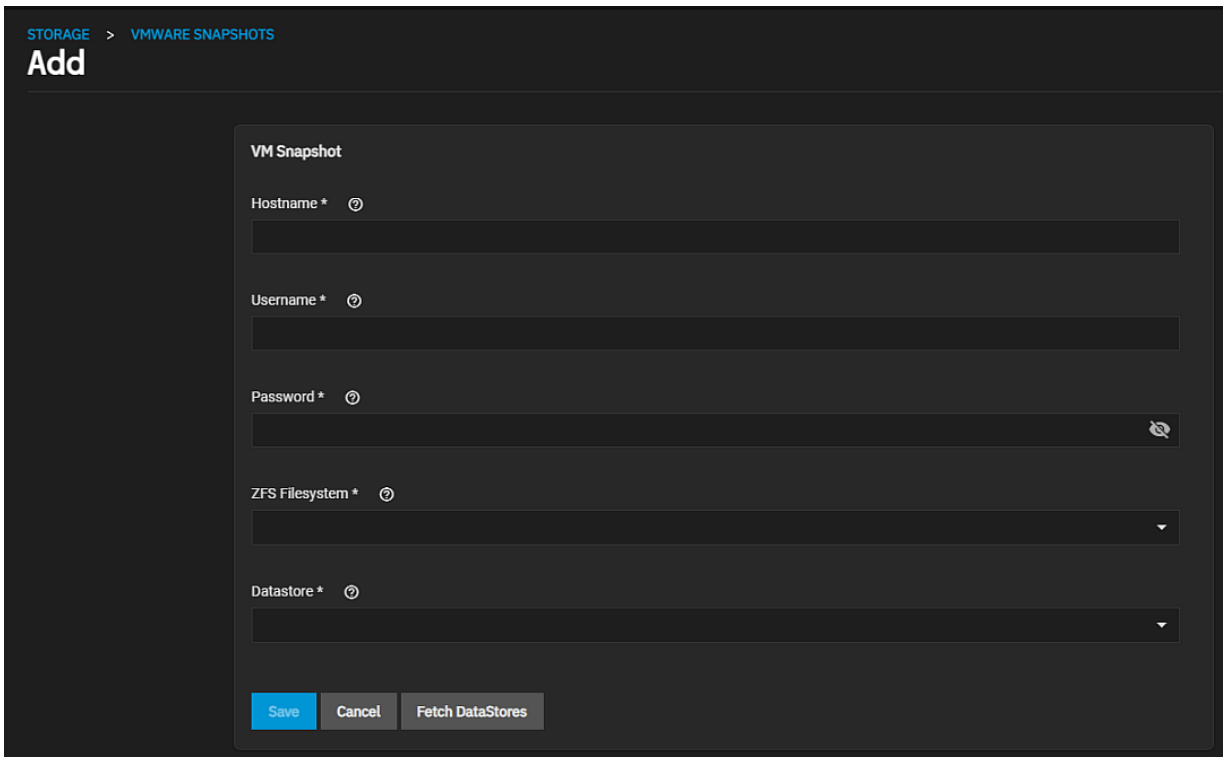
Related Content

- Creating VMWare Snapshots
- VMWare Snapshots Screen
- Periodic Snapshot Tasks Screens

4.3.5 - VMWare Snapshots Screen

This article provides information on the VMWare-Snapshot Add screen settings and functions.

Use the **VMware-Snapshots** option on the **Storage** sceen to create snapshots when TrueNAS SCALE is used as a VMWare datastore. Click **Snapshots** and select **VMware-Snapshots** from the dropdown list to display the **Add VMware-Snapshots** screen.



Setting	Description
Hostname	Enter the IP address or host name of the VMware host. When clustering, enter the vCenter server for the cluster.
Username	Enter the user on the VMware host with permission to snapshot virtual machines.
Password	Enter the password associated with the user entered in **Username**.
ZFS Filesystem	Select a file system to snapshot from the dropdown list of options. This field does not populate until you click **Fetch Datastores**. You must click **Fetch Datastores** before clicking in this field or the creation process fails.
Datastore	Select a datastore to synchronize with the host from the dropdown list of options. Click **Fetch DataStores** to populate this list with options from the VMWare host. You must click **Fetch Datastores** before you click in this field or the creation process fails. Selecting a datastore also selects any mapped datasets.

Click **Fetch DataStores** to connect TrueNAS connects to the VMware host. This synchronizes TrueNAS SCALE with the VMWare host and populates the **ZFS Filesystem** and **Datastore** dropdown lists with the information from the VMware host response.

Related Content

- Snapshots Screens
- Creating VMWare Snapshots
- Periodic Snapshot Tasks Screens

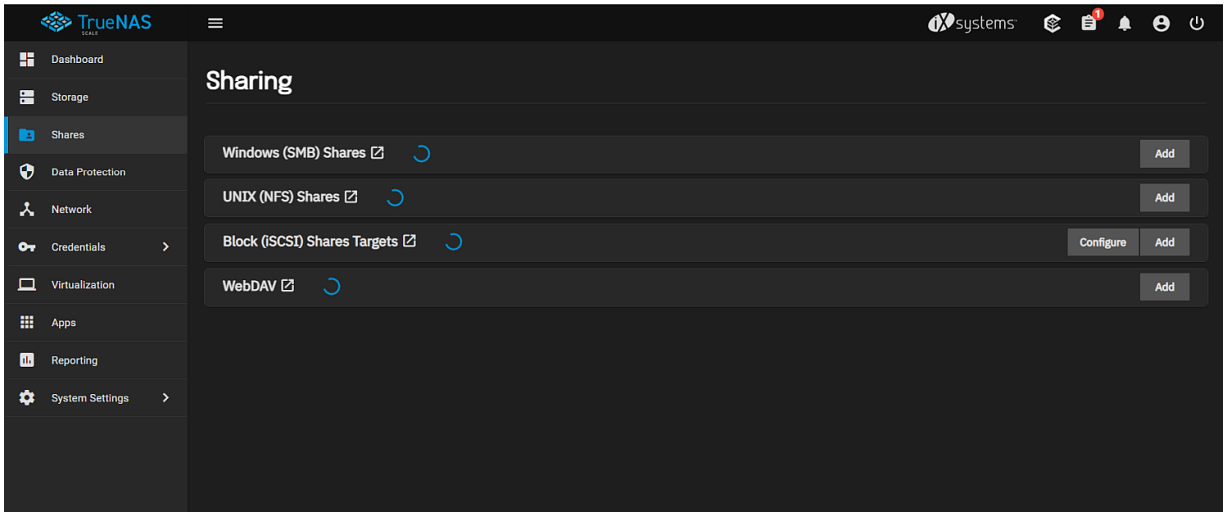
Related VMWare Articles

- Creating VMWare Snapshots

4.4 - Shares

File sharing is one of the primary benefits of a NAS. TrueNAS helps foster collaboration between users through network shares. TrueNAS SCALE allows users to create and configure block (iSCSI) shares targets, Windows SMB shares, Unix (NFS) shares, and WebDAV shares.

Click **Shares** on the main navigation panel to display the **Sharing** screen, which displays options to access SMB, NFS, iSCSI, and WebDAV shares.



Article Summaries

- Windows Shares (SMB)

  Article Summaries SMB Shares Screens This article provides information on SMB share screens and settings.

  - SMB Shares Screens

    This article provides information on SMB share screens and settings.

- Unix Shares (NFS)

  Article Summaries NFS Shares Screens This article provides information on NFS Shares screens and settings.

  - NFS Shares Screens

    This article provides information on NFS Shares screens and settings.

- Block Shares (iSCSI)

  - Block (iSCSI) Share Target Screens

    This article provides information on Block (iSCSI) Share Targets screens and settings.

- WebDAV Shares

  Article Summaries WebDAV Shares Screens This article provides information on WebDAV screens and settings.

  - WebDAV Shares Screens

    This article provides information on WebDAV screens and settings.

4.4.1 - Windows Shares (SMB)

Article Summaries

- SMB Shares Screens

  This article provides information on SMB share screens and settings.

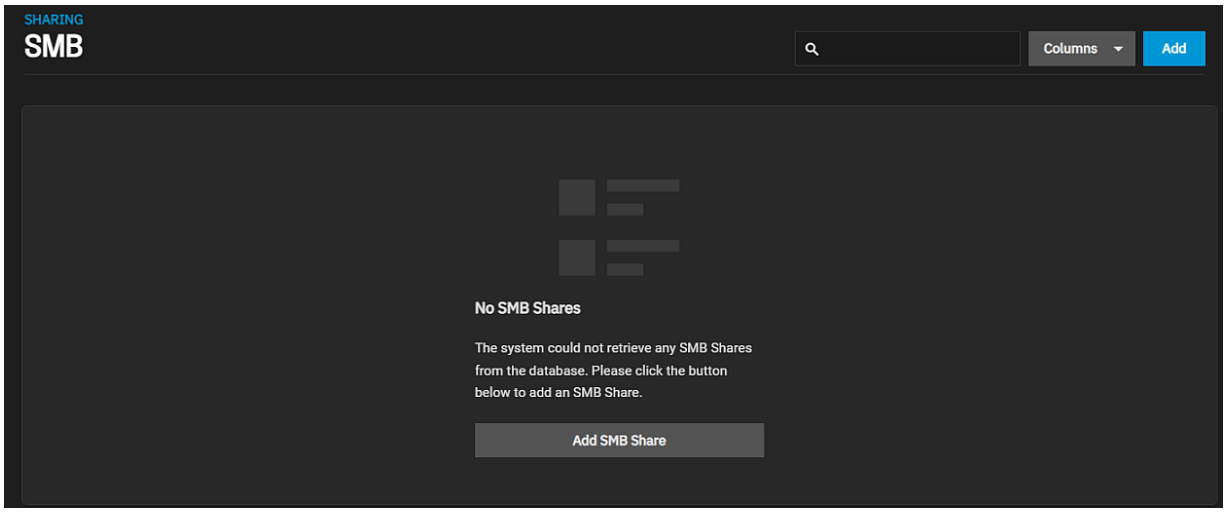
4.4.1.1 - SMB Shares Screens

This article provides information on SMB share screens and settings.

The first SMB share screen to display after you click **Shares** is the **Sharing** screen with the service widgets for the four supported share types.

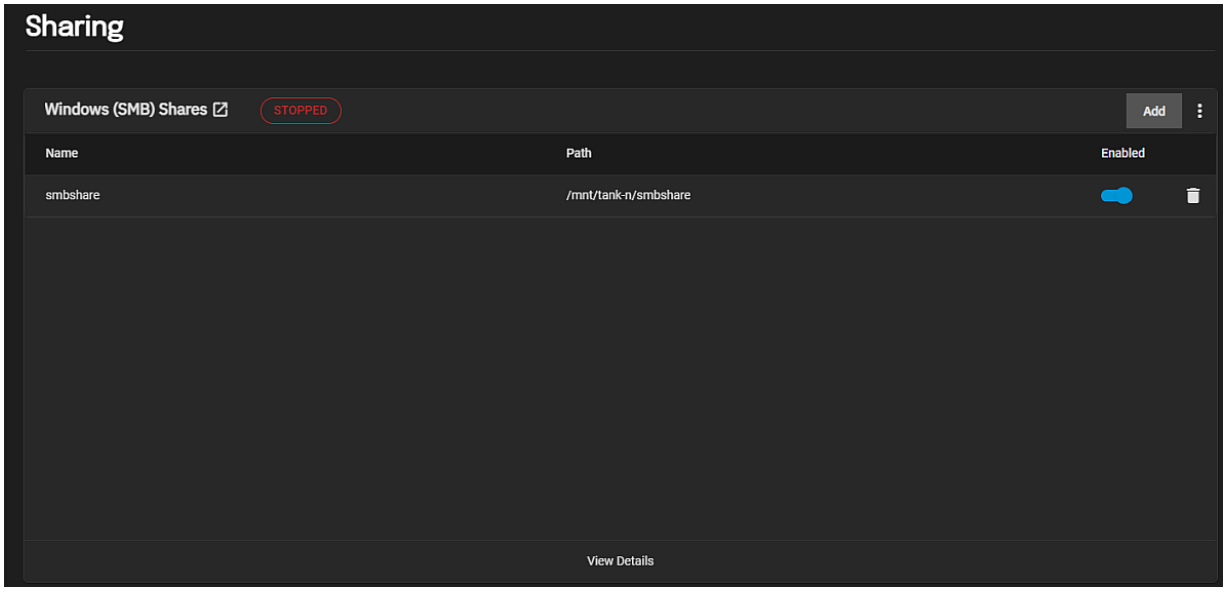
Sharing SMB Screen

If you have not added SMB shares to the system, clicking the **Windows SMB Share** option on the **Sharing** screen displays the **No SMB Shares** screen with the **Add SMB Share** button in the center of the screen.



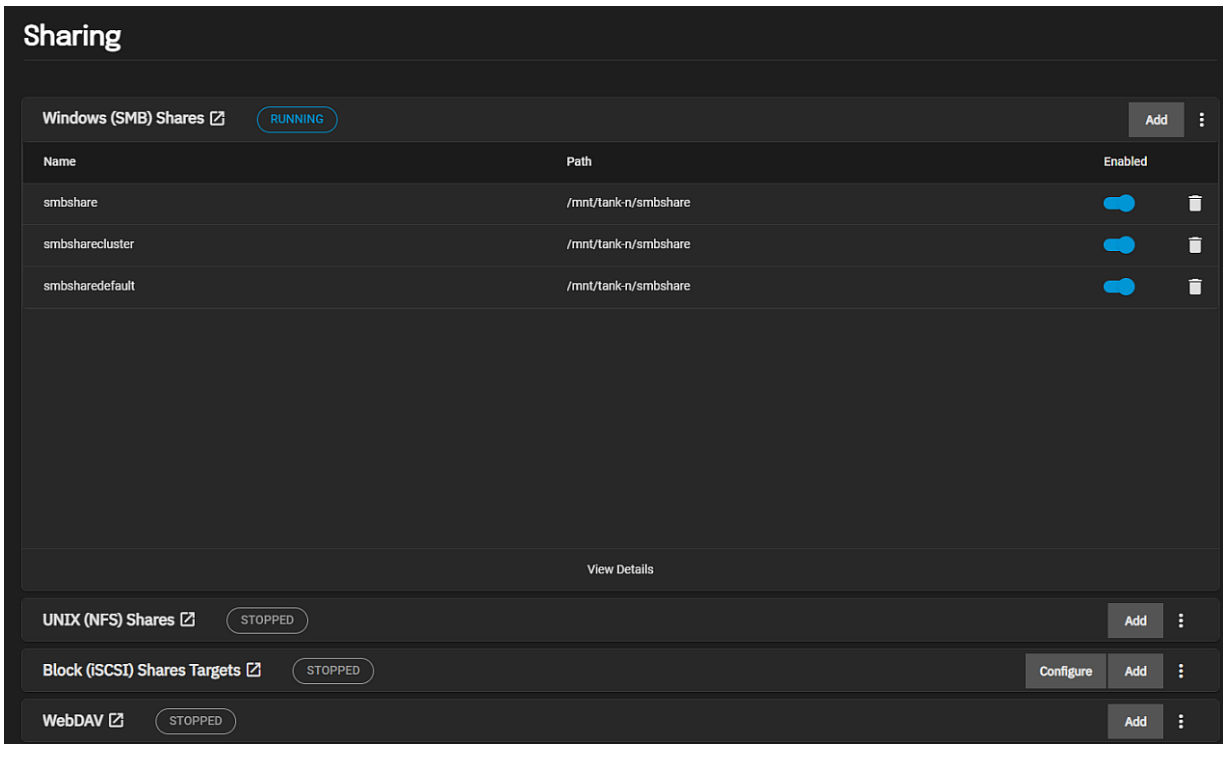
Use this button or the **Add** button at the top right of the screen to configure your first SMB share. After adding the first SMB share, the **Sharing SMB** screen displays.

If you return to the **Share** option (click **Shares** on the main navigation panel) the **Windows (SMB) Shares** widget dsiplays, expanded with the current service status and a list of the SMB shares below it.



Windows (SMB) Shares Widget

The **Windows (SMB) Shares** widget updates after adding SMB shares and every time you click **Shares** on the main navigation panel to return to the **Sharing** screen.



Each SMB share toggle provides quick access to enable or disable the share. Each share also has a delete option. The SMB share row is a link to the **Edit SMB** screen.

Windows (SMB) Shares Service Toolbar

The **Windows (SMB) Shares** toolbar displays the status of the SMB service as either **STOPPED** (red) or **RUNNING** (blue). Before adding the first share, **STOPPED** status displays in the default color.

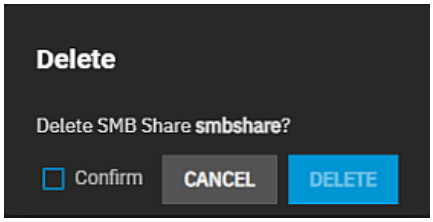
Both **Windows (SMB) Shares** and **View Detials** at the bottom of the widget display the **Sharing > SMB** details screen.

The **Add** button displays the **Add SMB** share configuration screen.

The ⋮ displays options turn the SMB service on or off. **Turn Off Service** displays if the service is running or **Turn On Service** if the service is stopped. The **Config Service** option displays the **System Settings > SMB** configuration screen.

Delete SMB Share Dialog

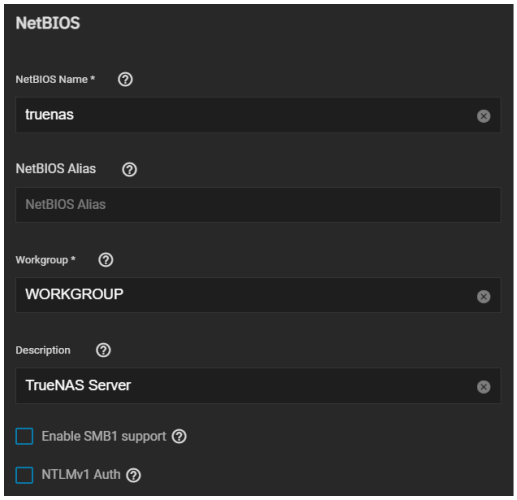
The 🗑 trash can icon to displays the **Delete** dialog.



Select **Confirm** to activate the **Delete** button.

Sharing SMB Details Screen

Windows SMB Share ⧉ or **View Details** displays The **Sharing >SMB** details screen. From this screen you can add or edit an SMB share on the list.



Add displays the **Add SMB** configuration screen.

Column button displays a dropdown list of options to customize the list view. Options include **Unselect All**, **Path**, **Description**, **Enabled** and **Reset to Defaults**.

The **Enabled** checkbox provides status of the share. If selected it indicates the share path is available when the SMB service is running, or if cleared disables but does not delete the share.

The ⋮ displays a dropdown list of options for each share. The options include **Edit** that displays the **Edit SMB** screen, **Edit Share ACL** that displays the **Edit Share ACL** screen, **Edit Filesystem ACL** that opens the **Edit Filesystem ACL** screen, and **Delete** that displays the **Delete** dialog.

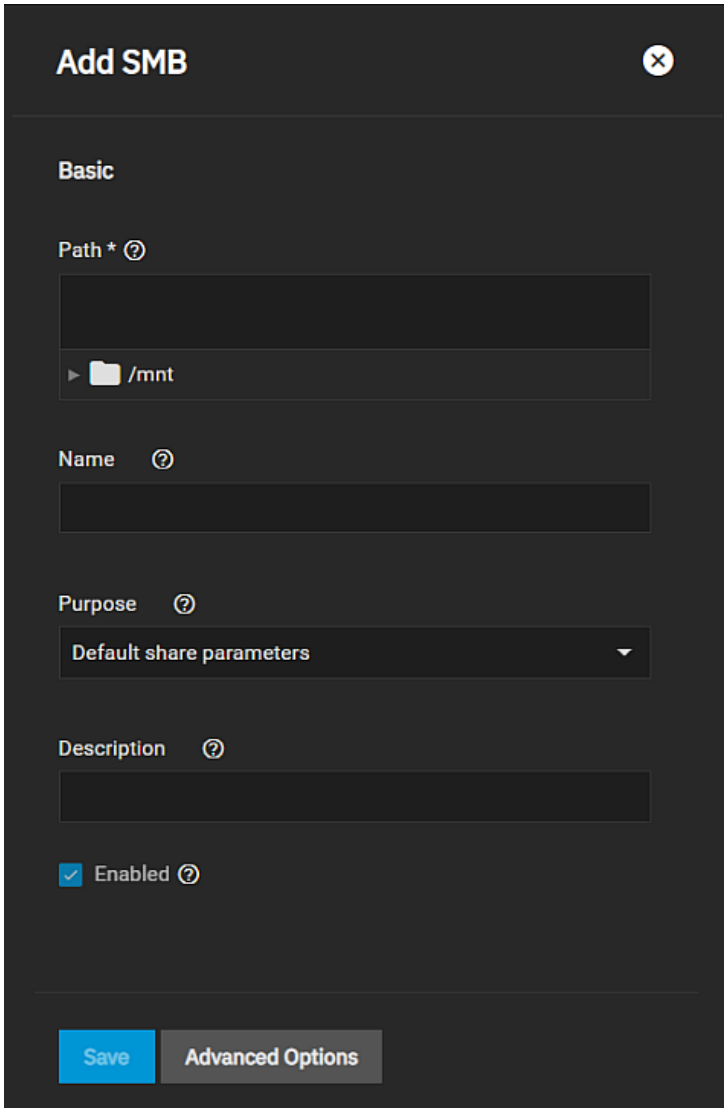
Add and Edit SMB Screens

The two SMB share configuration screens, **Add SMB** and **Edit SMB**, display the same setting options.

Click **Save** to create the share and add it to the **Shares > Windows (SMB) Shares** and **Sharing SMB** details lists, or to save changes made to an existing share.

Basic Options Settings

The **Basic Options** settings in this section display on the **Advanced Options** settings screen.



Setting	Description
Path	Enter the path or use the ▸ icon to the left of 🗀 **/mnt** to locate the dataset and populate the path. **Path** is the directory tree on the local file system that TrueNAS exports over the SMB protocol.
🗀 **/mnt**	Click the ▸ icon to expand the path at each dataset until you to get to the SMB share dataset you want to use. This populates the **Path**.
Name	Enter a name for this share that is less than or equal to 80 characters. Because of how the SMB protocol uses the name, the name must not exceed 80 characters. The name cannot have invalid characters as specified in Microsoft documentation MS-FSCC section 2.1.6. If not supplied, the share name becomes the last component of the path. This forms part of the full share path name when SMB clients perform and SMB tree connect.
Purpose	Select a preset option from the dropdown list. This applies predetermined settings (presets) and disables changing some share setting options. Select **No presets** to retain control over all **Advanced Options** settings. Select **Default parameters for cluster share** when setting up an SMB cluster share. **Default share parameters** is the default option when you open the **Add SMB** screen and to use for any basic SMB share.

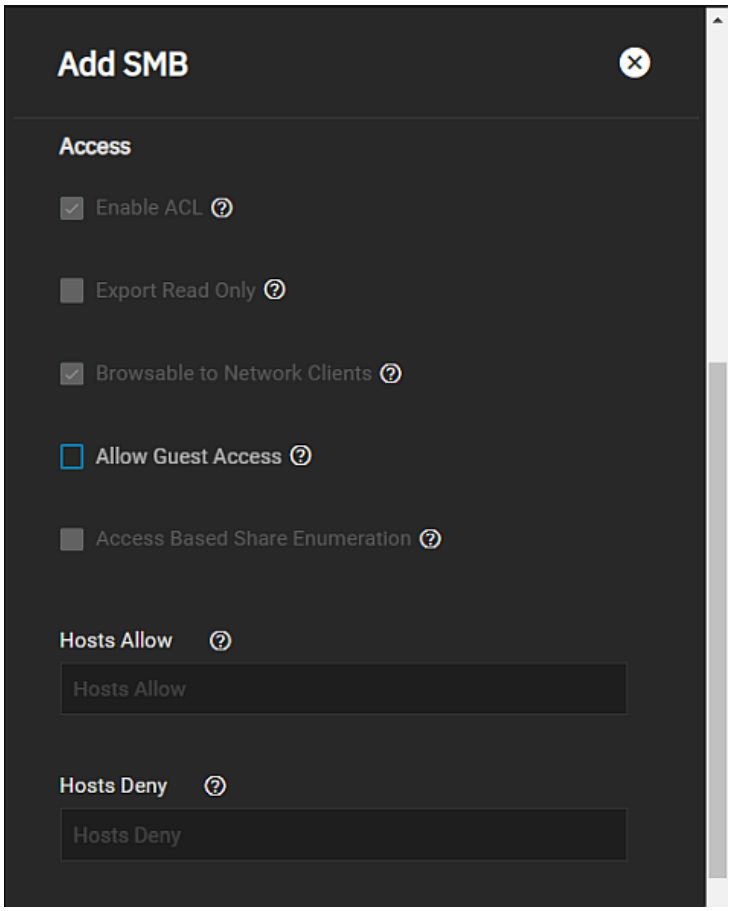
Setting	Description
	Other options are **Multi-User time machine**, **Multi-Protocol (NFSv3/SMB) shares**, **Private SMB Datsets and Shares**, or **SMB WORM. Files become readonly via SMB after 5 minutes**.
Description	Enter a brief description or notes on how you use this share.
Enabled	Selected by default to enable sharing the path when the SMB service is activated. Clear to disable this SMB share without deleting it.

Advanced Options Settings

Click **Advanced Options** to display settings made available or locked based on the option selected in **Purpose**.

Access Settings

The **Access** settings allow you to customize access to the share, files, and to specify allow or deny access for host names or IP addresses.

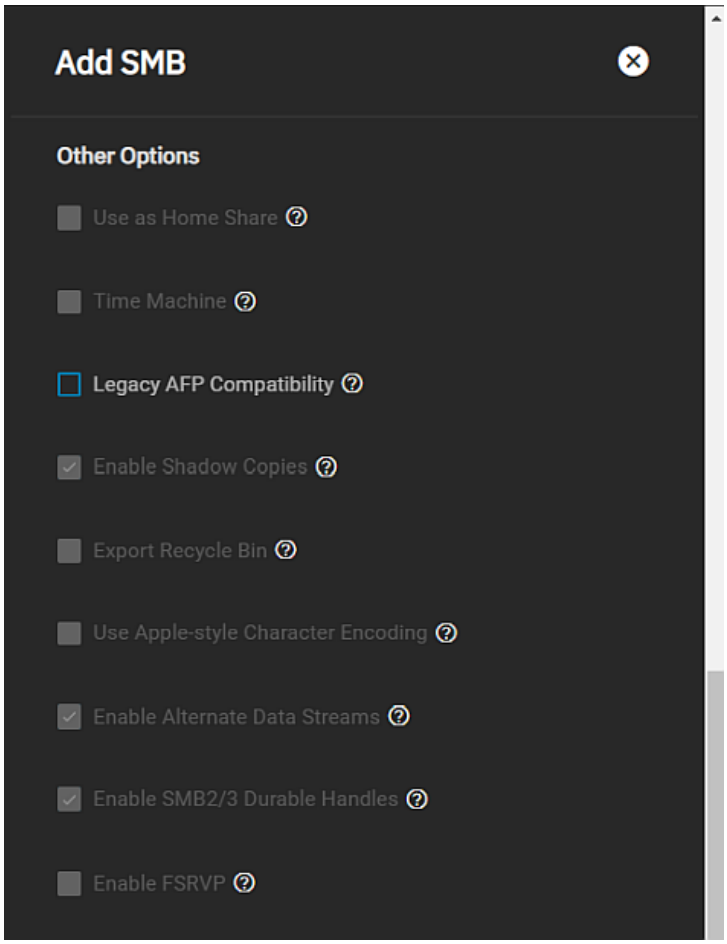


Setting	Description
Enable ACL	Select to enable ACL support for the SMB share. A warning displays if you clear this option and the SMB dataset has a ACL, and you are required to strip the ACL from the dataset prior to creating the SMB share.
Export Read Only	Select to prohibit writes to the share.
Browsable to Network Clients	Select to determine whether this share name is included when browsing shares. Home shares are only visible to the owner regardless of this setting. Enabled by default.
Allow Guest Access	Select to enable. Privileges are the same as the guest account. Guest access is disabled by default in Windows 10 version 1709 and Windows Server version 1903. Additional client-side configuration is required to provide guest access to these clients. **MacOS clients**: Attempting to connect as a user that does not exist in FreeNAS *does not* automatically connect as the guest account. You mus specifically select the **Connect As: Guest** option in macOS to log in as the guest account. See the Apple documentation for more details.
Access Based Share Enumeration	Select to restrict share visibility to users with read or write access to the share. See the smb.conf manual page.
Hosts Allow	Enter a list of allowed host names or IP addresses. Separate entries by pressing `Enter`. You can find a more detailed description with examples here.

Setting	Description
Hosts Deny	Enter a list of denied host names or IP addresses. Separate entries by pressing `Enter`.

Other Settings

The **Other Options** settings are for improving Apple software compatibility, ZFS snapshot features, and other advanced features.

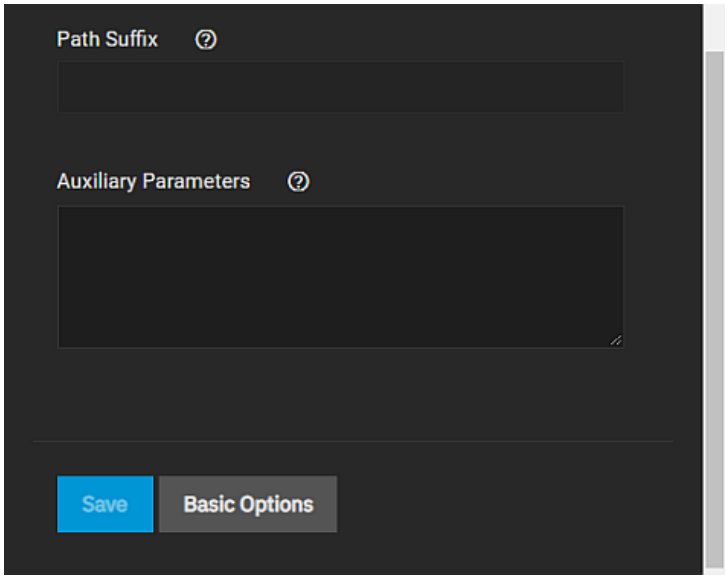


Setting	Description
Use as Home Share	Select to allow the share to host user home directories. Each user has a personal home directory they use when connecting to the share that is not accessible by other users. This allows for a personal, dynamic share. Only one share can be used as the home share. See Adding an SMB Home Share for more information.
Time Machine	Enables Apple Time Machine backups on this share. This option requires SMB2/3 protocol extenstion support. You can enable this in the general SMB server configuration.
Legacy AFP Compatibility	Select to enable the share to behave like the deprecated Apple Filing Protocol (AFP). Leave cleared for the share to behave like a normal SMB share. This option controls on how the SMB share reads and writes data. Only enable this when this share originated as an AFP sharing configuration. This is not required for pure SMB shares or MacOS SMB clients. This option requires SMB2/3 protocol extenstion support. You can enable this in the general SMB server configuration.
Enable Shadow Copies	Select to export ZFS snapshots as Shadow Copies for Microsoft Volume Shadow Copy Service (VSS) clients.
Export Recycle Bin	Select to enable. Deleted files from the same dataset move to the **Recycle Bin** and do not take any additional space. Deleting files over NFS removes the files permanently. Files in a different dataset or a child dataset are copied to the dataset with the recycle bin. To prevent excessive space usage, files larger than 20 MiB are deleted rather than moved. Adjust the **Auxiliary Parameter** by adding the `crossrename:sizelimit=` setting to allow larger files. For example, `crossrename:sizelimit=<i>50</i>` allows moves of files up to 50 MiB in size. This permanently deletes or moves files from the recycle bin. This is not a replacement for ZFS snapshots.
Use Apple-style Character Encoding	Select to converts NTFS illegal characters in the same manner as macOS SMB clients. By default, Samba uses a hashing algorithm for NTFS illegal characters.

Setting	Description
Enable Alternate Data Streams	Select to allow multiple NTFS data streams. Disabling this option causes macOS to write streams to files on the file system.
Enable SMB2/3 Durable Handles	Select to allow using open file handles that can withstand short disconnections. Support for POSIX byte-range locks in Samba is also disabled. This option is not recommended when configuring multi-protocol or local access to files.
Enable FSRVP	Select to enable support for the File Server Remote VSS Protocol (FSVRP). This protocol allows remote procedure call (RPC) clients to manage snapshots for a specific SMB share. The share path must be a dataset mount point. Snapshots have the prefix `fss-` followed by a snapshot creation timestamp. A snapshot must have this prefix for an RPC user to delete it.

Path Suffix and Auxiliary Parameters Settings

Use **Path Suffix** to provide unique shares on a per user, computer or IP address basis. Use **Auxiliary Parameters** to enter additional settings.



Setting	Description
Path Suffix	Appends a suffix to the share connection path. Use this to provide unique shares on a per-user, per-computer, or per-IP address basis. Suffixes can contain a macro. See the smb.conf manual page for a list of supported macros. The connect path must be preset before a client connects.
Auxiliary Parameters	Enter additional smb.conf settings.

Advanced Options Presets

The **Purpose** setting you select in the **Basic Options** affects the **Advanced Options** settings (presets) you can select, making some settings available or locked. The expandable below provides a comparison table that lists these presets and shows whether the option is available or locked.

What do all the presets do?

The following table shows the preset options for the different **Purpose** options and if those are locked.
A ☑ indicates the option is enabled while ☐ means the option is disabled. [ ] indicates empty text fields, and [%U] indicates the exact option the preset created.

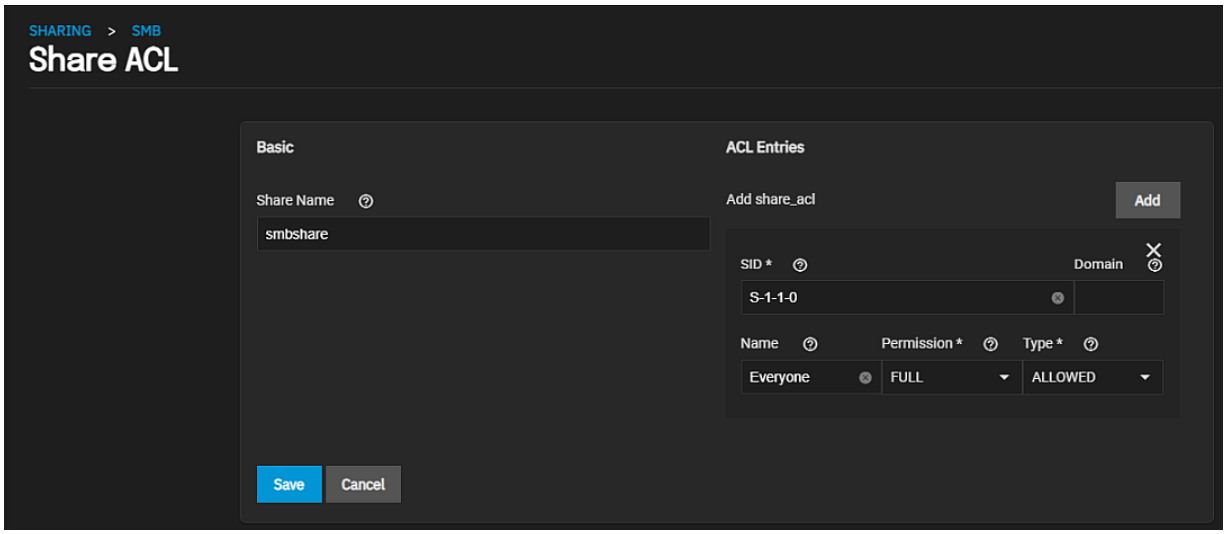
Setting	Default Share Parameters	Multi-User Time Machine	Multi-Protocol (NFSv3/SMB) Shares	Private SMB Datasets and Shares	SMB Files become Read Only after 5 minutes
Enable ACL	☑ (locked)	☑	☐ (locked)	☐	☐
Export Read Only	☐ (locked)	☐	☐	☐	☐
Browsable to Network Clients	☑ (locked)	☑	☑	☑	☑

Setting	Default Share Parameters	Multi-User Time Machine	Multi-Protocol (NFSv3/SMB) Shares	Private SMB Datasets and Shares	SMB Files become Read Only after 5 minutes
Allow Guest Access	☐	☐	☐	☐	☐
Access Based Share Enumeration	☐ (locked)	☐	☐	☐	☐
Hosts Allow	☐ (locked)	☐	☐	☐	☐
Hosts Deny	☐ (locked)	☐	☐	☐	☐
Use as Home Share	☐ (locked)	☐	☐	☐	☐
Time Machine	☐ (locked)	☐	☐	☐	☐
Enable Shadow Copies	☑ (locked)	☑	☑	☑	☑
Export Recycle Bin	☐ (locked)	☐	☐	☐	☐
Use Apple-style Character Encoding	☐ (locked)	☐	☑	☑	☑
Enable Alternate Data Streams	☑ (locked)	☑	☐ (locked)	☐	☐
Enable SMB2/3 Durable Handles	☑ (locked)	☑	☐ (locked)	☐	☐
Enable FSRVP	☐ (locked)	☐	☐	☐	☐
Path Suffix	[ ] (locked)	[%U] (locked)	[%U]	[%U] (locked)	[ ] (locked)
Auxiliary Parameters	[ ]	[ ]	[ ]	[ ]	[ ]

Back to Advanced Options Settings

SMB Share ACL screen

The **SMB Share ACL** screen displays when you click **Edit Share ACL** from the ⋮ options list on the **Sharing SMB** details screen. These settings configure new ACL entries for the selected SMB share and apply at the entire SMB share level, it is separate from file system permissions.



Basic Settings

Setting	Description
Share Name	Displays the name for the share. This field is read only.

ACL Entries Settings

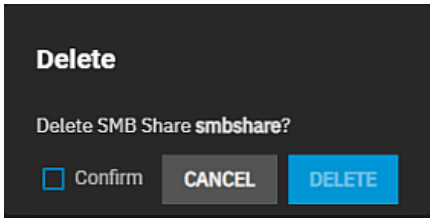
ACL Entries are listed as a block of settings. Click **Add** to add a new entry.

Setting	Description
SID	Enter a SID trustee value (who) this ACL entry (ACE) applies to. SID is a unique value of variable length that identifies the trustee. Shown as a Windows Security Identifier. If not specifed, you must enter a value in **Domain**.
Domain	Enter the domain for the user specified in **Name**. Required when a **SID** value is not entered. Local users have the SMB server NetBIOS name: *truenas\smbusers*.
Name	Enter a user name (who) this ACL entry applies to, shown as a user name. Requires adding the user **Domain**.
Permission	Select a predefined permission combinations from the dropdown list. Select **Read** to grant read access and execute permission on the object (RX). Select **Change** to grant read access, execute permission, write access, and delete object (RXWD) permissions. Select **Full** to grant read access, execute permission, write access, delete object, change permissions, and take ownership (RXWDPO) permissions. For more details, see smbacls(1).
Type	Select the option from the dropdown list that specifies how permissions are applied to the share. Select **Allowed** to deny all permissions by default except those that are manually defined. Select **Denied** to allow all permissions by default except those that are manually defined.

Save stores the share ACL and immediately applies it to the share.

Edit Filesystem ACL Screen

Edit Filesystem ACL opens **Storage > Edit *POSIX.1e* ACL** with an **ACL Editor** screen.



The type of ACL editor screen depends on the SMB dataset **ACL Type** selection. If set to **NFSv4** the editor displayed is an NFSv4 type editor. If set to **POSIX** the first screen displayed is the **Select a preset** window folllowed by the POSIX type editor. See Edit ACL Screens or Permissions for more information on configuring permissions.

Related Content

- Adding SMB Shares
- Managing SMB Shares
- Using SMB Shadow Copy
- Setting Up SMB Home Shares
- Configuring SMB Service
- SMB Service Screen
- Spotlight Support on a SCALE SMB Share

Related AFP Articles

- Adding SMB Shares
- Managing SMB Shares
- AFP Migration

4.4.2 - Unix Shares (NFS)

Article Summaries

- NFS Shares Screens

  This article provides information on NFS Shares screens and settings.

4.4.2.1 - NFS Shares Screens

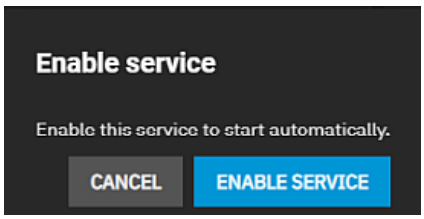
This article provides information on NFS Shares screens and settings.

The **Sharing** screen opens after you click **Shares** on the main navigation panel.

Unix (NFS) Share Widget

The **Unix (NFS) Share** widget includes the widget toolbar that displays the status of the NFS service and the **Add** button. After adding NFS shares, the widget displays a list of the shares below the toolbar.

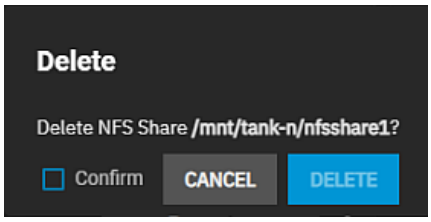
After adding the first NFS share, the system opens an enable service dialog.



Enable Service turns the NFS service on and changes the toolbar status to **Running**. If you added shares of other types, the widget occupies a quarter of the screen.

The **Enable** toggle for each share shows the current status of the share. When disabled, it disables the share but does not delete the configuration from the system.

The delete icon displays a delete confirmation dialog that removes the share from the system.

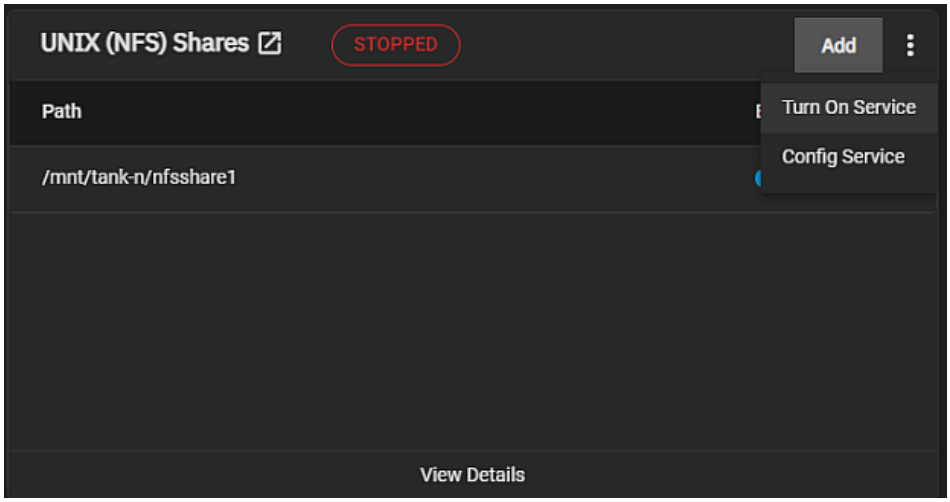


View Details and clicking anywhere on **Unix (NFS) Share** the opens the **Sharing > NFS** screen with the list view of NFS shares.

The NFS share on the widget opens the **Edit NFS** screen.

Unix (NFS) Share Widget Toolbar

The **Unix (NFS) Share** widget toolbar includes the **Add** button and an actions menu.



The ⋮ on the toolbar displays options turn the NFS service on or off. **Turn Off Service** displays if the service is running or **Turn On Service** if the service is stopped. The **Config Service** option opens the **Services > NFS** configuration screen.

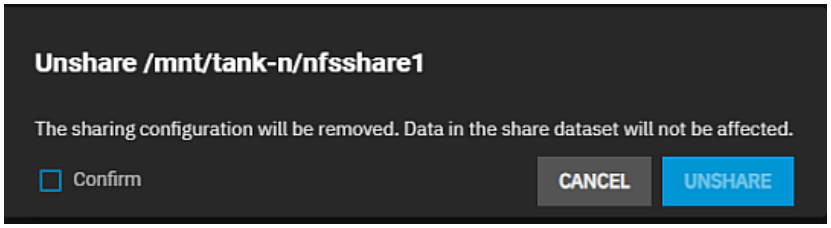
The toolbar displays the **STOPPED** service status in red before you start the service or click **Enable Service** when the dialog displays. When service is started it displays **RUNNING** in blue.

Sharing NFS Details Screen

The **Sharing > NFS** details screen displays the same list of NFS shares as the **Unix (NFS) Share** widget.

Customize the information using the **Columns** dropdown list. Select from the **Unselect All, Description**, **Enabled**, and **Reset to Defaults** options.

The ⋮ displays a list of options for the share. **Edit** opens the **Edit NFS** configuration screen. **Delete** opens an **Unshare *path*** confirmation dialog.

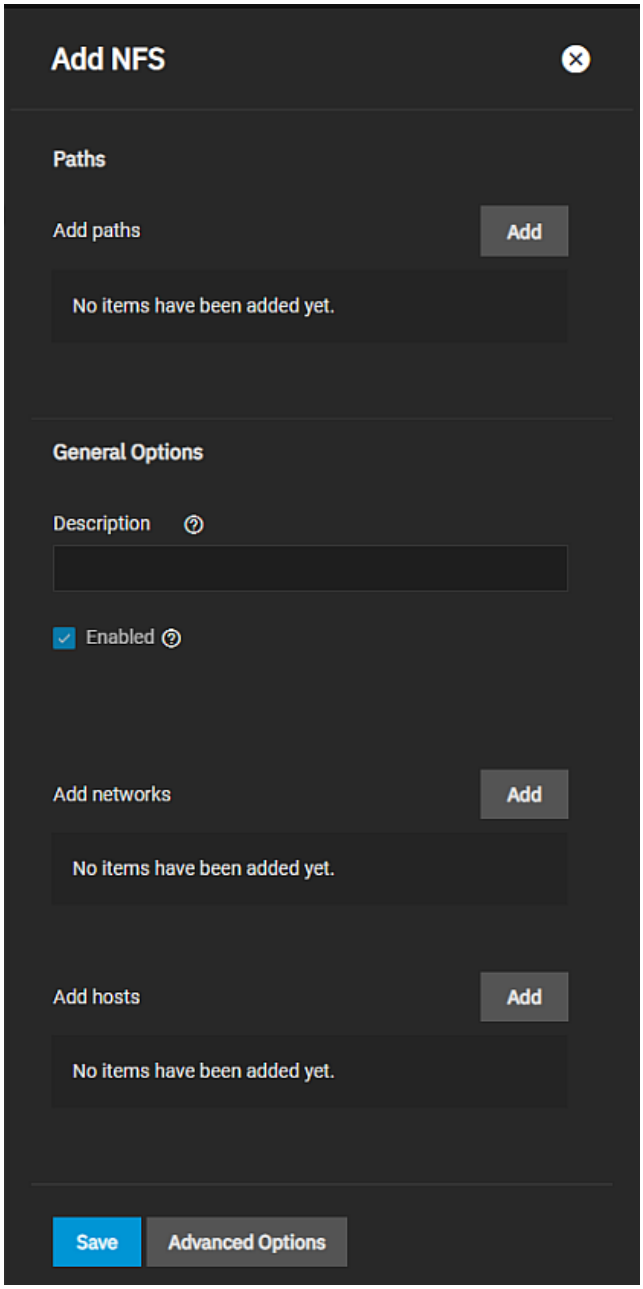


Select **Confirm** and then **UNSHARE** to remove the share without affecting the data in the share dataset.

Add and Edit NFS Screens

The **Add NFS** and **Edit NFS** display the same **Basic Options** and **Advanced Options** settings.

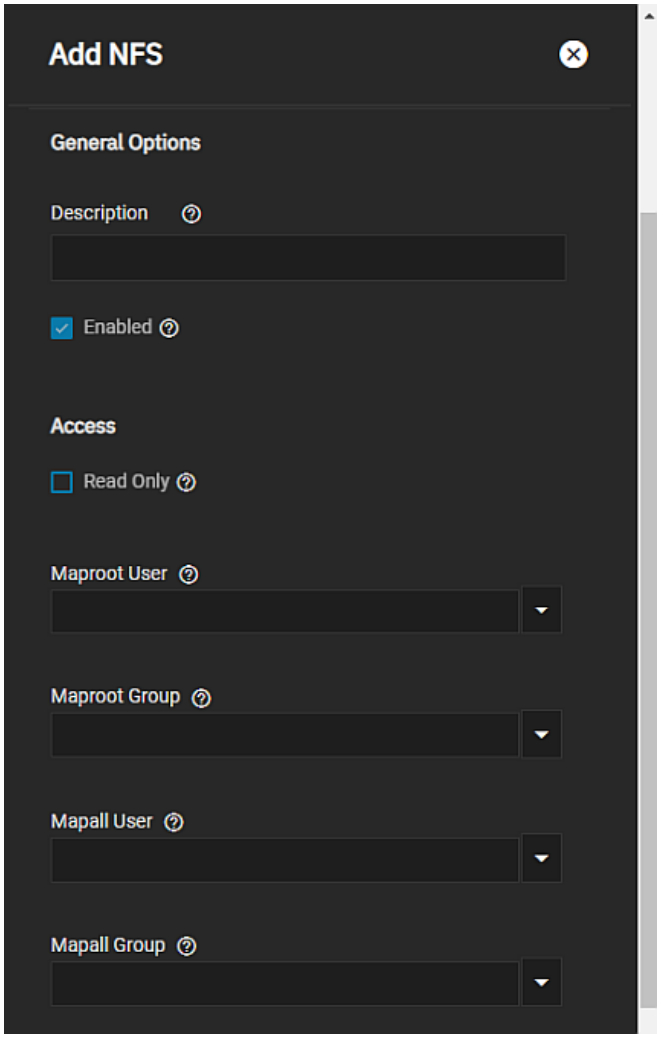
Basic Options Settings



Setting	Description
Path	Click **Add** to display the **Add paths** settings. Enter the path or use the ▸ icon to the left of 🗀**/mnt** to locate the dataset and populate the path. **Path** is the directory tree on the local file system that TrueNAS exports over the NFS protocol. Click **Add** for each path you want to add.
Description	Enter any notes or reminders about the share.
Enabled	Select to enable this NFS share. Clear the checkbox to disable this NFS share without deleting the configuration.
Add networks	Click **Add** to display the **Authorized Networks** IP address and CIDR fields. Enter an allowed network IP and select the mask CIDR notation. Click **Add** for each network address and CIDR you want to define as an authorized network. Defining an authorized network restricts access to all other networks. Leave empty to allow all networks.
Add hosts	Click **Add** to display the **Authorized Hosts and IP addresses** field. Enter a host name or IP address to allow that system access to the NFS share. Click **Add** for each allowed system you want to define. Defining authorized systems restricts access to all other systems. Leave the field empty to allow all systems access to the share.

Advanced Options Settings

Advanced Options settings tune the share access permissions and define authorized networks. **Advanced Options** includes these **Basic Options** settings. Only the **Access** settings display on the **Advanced Options** screen.



Setting	Description
Read Only	Select to prohibit writing to the share.
Maproot User	Enter a string or select a user from the dropdown to apply permissions for that user to the *root* user.
Maproot Group	Enter a string or select a group from the dropdown to apply permissions for that group to the *root* user.
Mapall User	Enter a string or select a user to apply the permission for the chosen user to all clients.
Mapall Group	Enter a string or select a group to apply the permission for the chosen group to all clients.

Related Content

- Configuring NFS Service
- NFS Services Screen
- Adding NFS Shares

4.4.3 - Block Shares (iSCSI)

4.4.3.1 - Block (iSCSI) Share Target Screens

This article provides information on Block (iSCSI) Share Targets screens and settings.

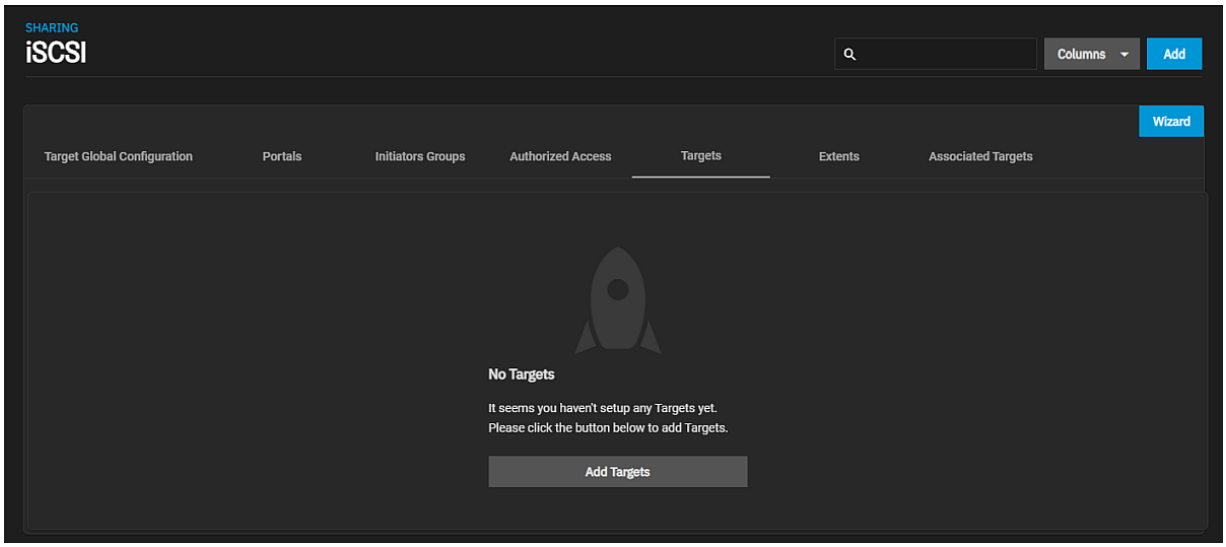
The **Sharing** screen opens after you click **Shares** on the main navigation panel.

Block (iSCSI) Shares Targets Widget

The **Block (iSCSI) Shares Targets** widget displays the widget toolbar with the status of the iSCSI service and two buttons, **Configure** and **Add**. After adding a block share the widget displays shares below the toolbar.

After adding a iSCSI target or share, the widget toolbar displays the **STOPPED** service status in red, and it includes the share below it.

Before you add your first iSCSI block share, click anywhere on **Block (iSCSI) Shares Targets** to open the **Sharing > iSCSI** screen with **Targets** iSCSI configuration tab displayed. The **No Targets** screen opens only when the system does not have an iSCSI target configured on the system.

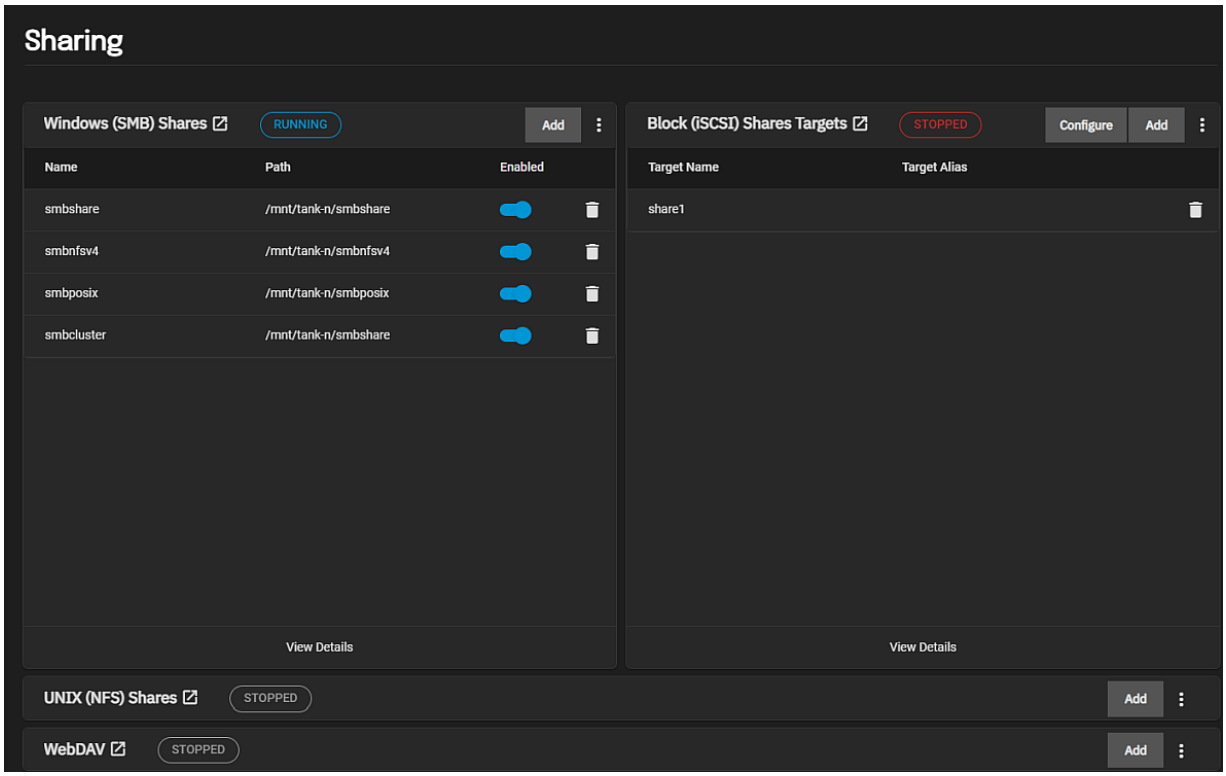


Add Targets and the **Add** button on the toolbar opens the **Add ISCSI Target** screen.

Configure on the widget tooldbar opens the **Sharing > iSCSI** screen with the configuration tabs displayed. **Target Global Configuration** displays the first time you click **Configure**.

The ⋮ on the toolbar displays options turn the iSCSI service on or off. **Turn Off Service** displays if the service is running or **Turn On Service** if the service is stopped. The **Config Service** option opens the configuration tabs **Target Global Configuration** screen.

If you have other share types added to your TrueNAS, the widget displays as a card occupying a quarter of the main **Sharing** screen.



View Details also opens the iSCSI configuration tabs. Each tab includes details on the block shares added to the system.

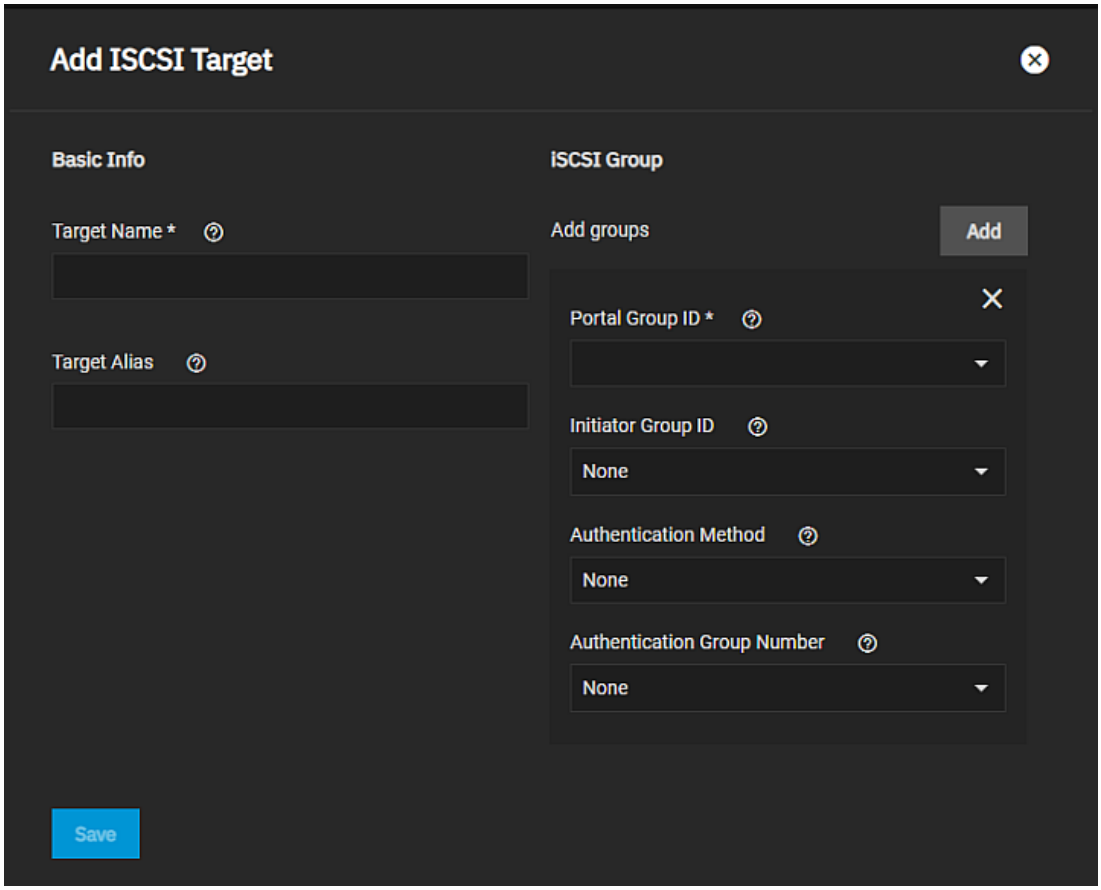
Add and Edit iSCSI Target Screens

The **Add iSCSI Target** and **Edit iSCSI Target** screens display the same settings but the current settings populate the **Edit iSCSI Target** screen settings for the selected share.

To access this screen from the **Block (iSCSI) Shares Targets** widget toolbar, click **Add**. To access the **Edit iSCSI Target** screen from the widget click on the share.

To access the **Add iSCSI Target** screen from the configuration tabs, while on the **Targets** tab, click **Add** at the top of the screen.

To access the **Edit iSCSI Target** screen from the configuration tabs, while on the **Targets** tab, click ⋮ next to the share and then click **Edit**.



Basic Info Settings

Setting	Description
Target Name	Required. Enter a name using lowercase alphanumeric characters. Allowed characters are plus dot (.), dash (-), and colon (:). A name longer than 63 characters can prevent access to the block. See the “Constructing iSCSI names using the iqn.format” section of RFC3721. The base name is automatically prepended if the target name does not start with **iqn**.
Target Alias	Enter an optional user-friendly name.

iSCSI Group Settings

To display the **iSCSI Group** settings, click **Add**.

Setting	Description
Portal Group ID	Required. Select the number of the existing portal to use or leave empty.
Initiator Group ID	Select the existing initiator group ID that has access to the target from the dropdown list of options. **None**, **1(init1)**, or **3(ALL initiators Allowed)**.
Authentication Method	Select the method from the dropdown list of options. **None**, **CHAP** or **Mutual Chap**. iSCSI supports multiple authentication methods that targets can use to discover valid devices. **None** allows anonymous discovery. If set to **None** you can leave **Discovery Authentication Group** set to **None** or empty. If set to **CHAP** or **Mutual CHAP** you must enter or create a new group in **Discovery Authentication Group**.
Authentication Group Number	Select the option from the dropdown list. This is the group ID created in **Authorized Access**. Required when the **Discovery Authentication Method** is set to **CHAP** or **Mutual CHAP**. Select **None** or the value representing the number of the existing authorized accesses.

iSCSI Configuration Screens

The iSCSI configuration screens display across seven tabs, one for each of the share configuration areas.

The **Add** button at the top of the **Sharing > iSCSI** screen, when it displays the configuration tabs, works with the tab or screen currently selected. For example, if **Portals** is the current tab/screen selected, the **Add** button opens the **Sharing > iSCSI > Portals > Add** screen.

The ⋮ on configure tab screens with list views displays the **Edit** and **Delete** options. **Edit** opens the **Edit** screen for the selected tab screen. For example, when on the **Portals** tab/screen the **Sharing > iSCSI > Portals > Edit** screen opens.

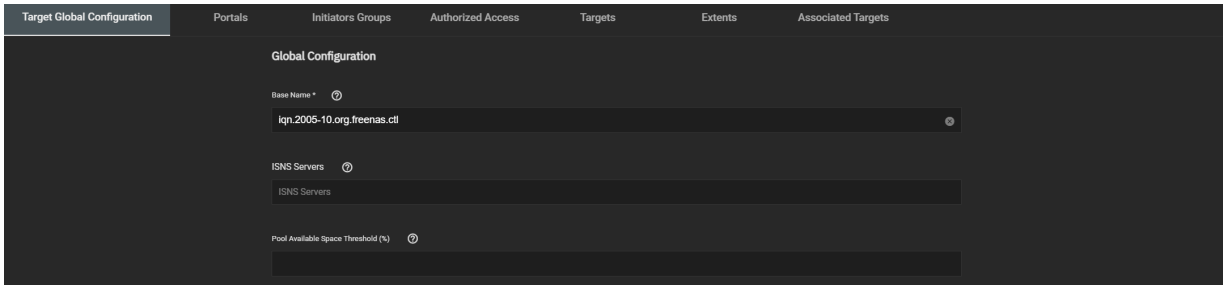
The **Delete** option opens the delete dialog for the screen currently selected.

The **Add** and **Edit** screens display the same settings.

Target Global Configuration Screen

The **Target Global Configuration** displays configuration settings that apply to all iSCSI shares. There are no add, edit or delete options for this screen. It opens after you click **Configure** on the **Block (iSCSI) Share Target** widget on the main **Sharing** screen. It also opens when you click **Config Service**.

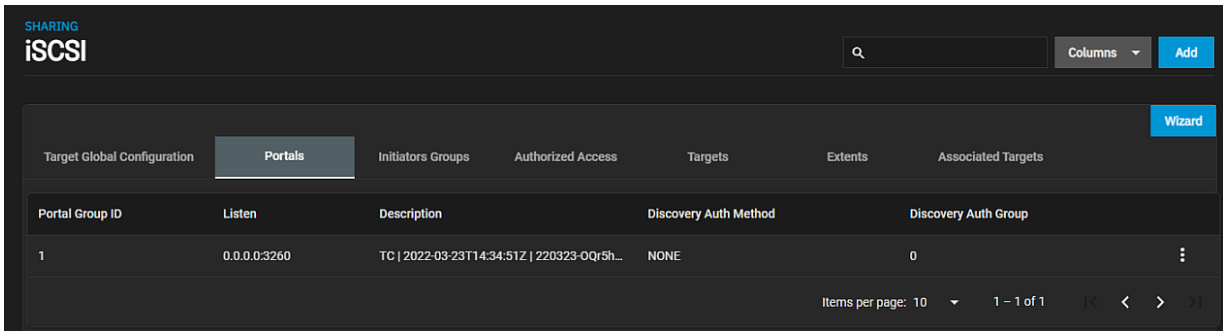
The **System Settings > Services > iSCSI** displays the **Target Global Configuration** and all the other configuration screens after you click the iSCSI **Config** option on the **Services** screen.



Setting	Description
Base Name	Enter a name using lowercase alphanumeric characters. Allowed characters include dot (.), dash (-), and colon (:). See the “Constructing iSCSI names using the iqn.format” section of RFC3721.
ISNS Servers	Enter host names or IP addresses of the ISNS servers to register with the iSCSI targets and portals of the system. Separate entries by pressing `Enter`.
Pool Available Space Threshold (%)	Enters a value for the threshold percentage that generates an alert when the pool has this percent space remaining. This is typically configured at the pool level when using zvols or at the extent level for both file and device-based extents.

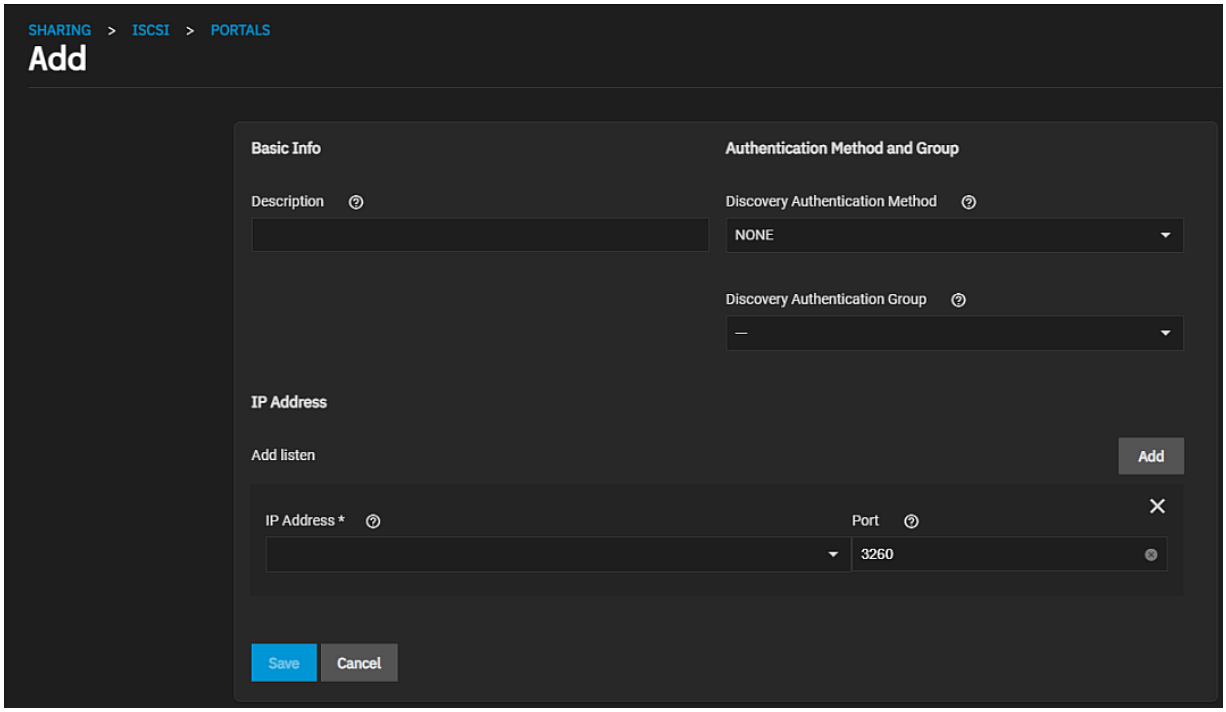
Portal Screens

The configuration tabs **Portals** screen displays a list of portal ID groups on the TrueNAS system.



The ⋮ next to the portal displays the **Edit** and **Delete** options. **Delete** opens the **Delete** dialog for the selected portal ID. Click **Confirm** and then **Delete** to delete the selected portal.

Add opens the **Sharing > iSCSI > Portals > Add** screen. **Edit** opens the **Sharing > iSCSI > Portals > Edit** screen. Both screens have the same setting options.



Basic Info Settings

Setting	Description
Description	Enter an optional description. Portals are automatically assigned a numeric group.

Authentication Method and Group Settings

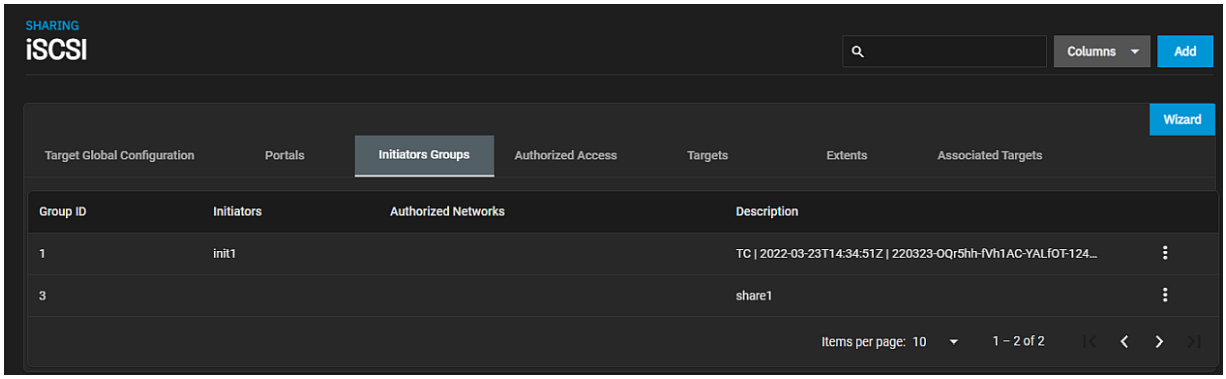
Setting	Description
Discovery Authentication Method	Select the discovery method you want to used for authentication from the dropdown list. iSCSI supports multiple authentication methods that targets can use to discover valid devices. **None** allows anonymous discovery. If set to **None** you can leave **Discovery Authentication Group** set to **None** or empty. If set to **CHAP** or **Mutual CHAP** you must enter or create a new group in **Discovery Authentication Group**.
Discovery Authentication Group	Select the discovery authentication group you want to use from the dropdown list. This is the group ID created in **Authorized Access**. Required when the **Discovery Authentication Method** is set to **CHAP** or **Mutual CHAP**. Select **None** or **Create New**. **Create New** displays additional setting options.

IP Address Settings

Setting	Description
IP Address	Select the IP addresses the portal listens to. Click **Add** to add IP addresses with a different network port. **0.0.0.0** listens on all IPv4 addresses and **::** listens on all IPv6 addresses.
Port	TCP port used to access the iSCSI target. Default is **3260**.
ADD	Adds another IP address row.

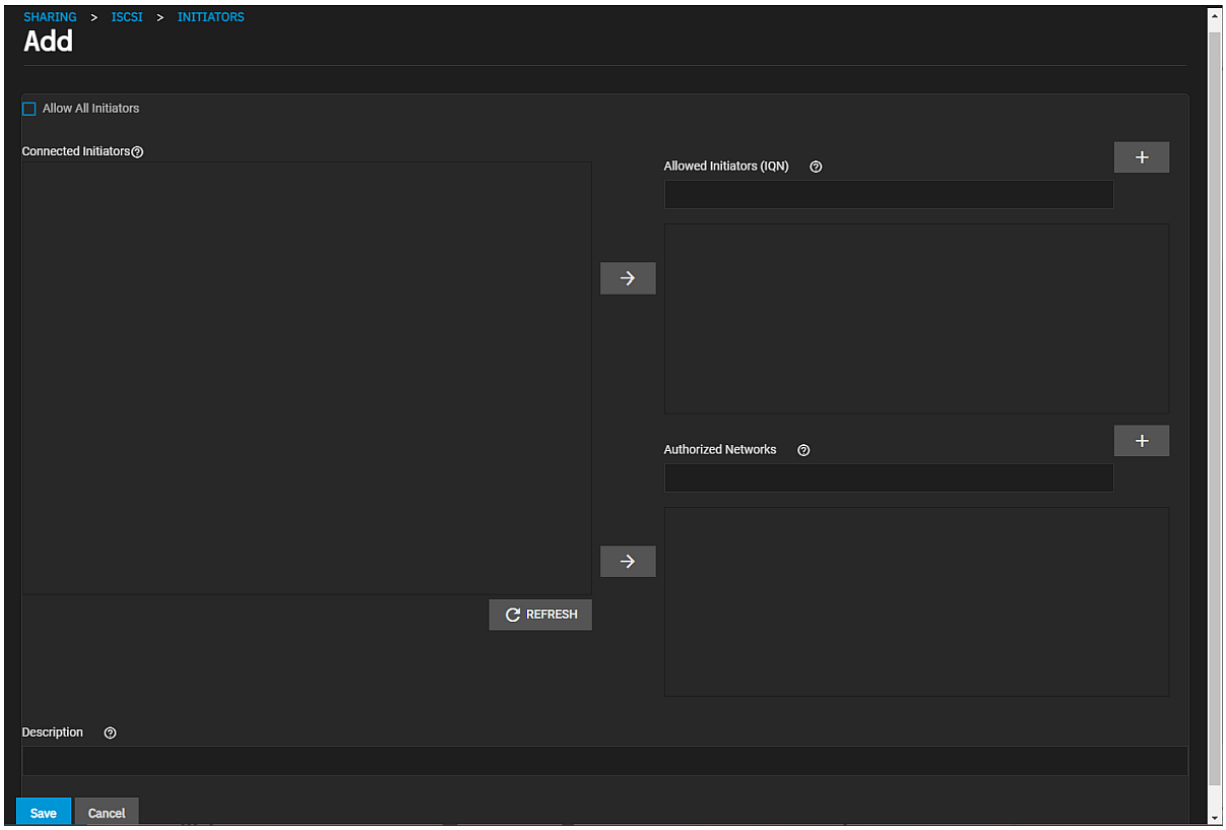
Initiators Groups Screen

The **Initiators Groups** screen display settings to create new authorized access client groups or edit existing ones in the list.



The ⋮ next to the initiator group displays the **Edit** and **Delete** options. **Delete** opens the **Delete** dialog for the selected group ID. Click **Confirm** and then **Delete** to delete the selected portal.

Add opens the **Sharing > iSCSI > Initiators > Add** screen. **Edit** opens the **Sharing > iSCSI > Initiators > Edit** screen. Both screens have the same setting options.

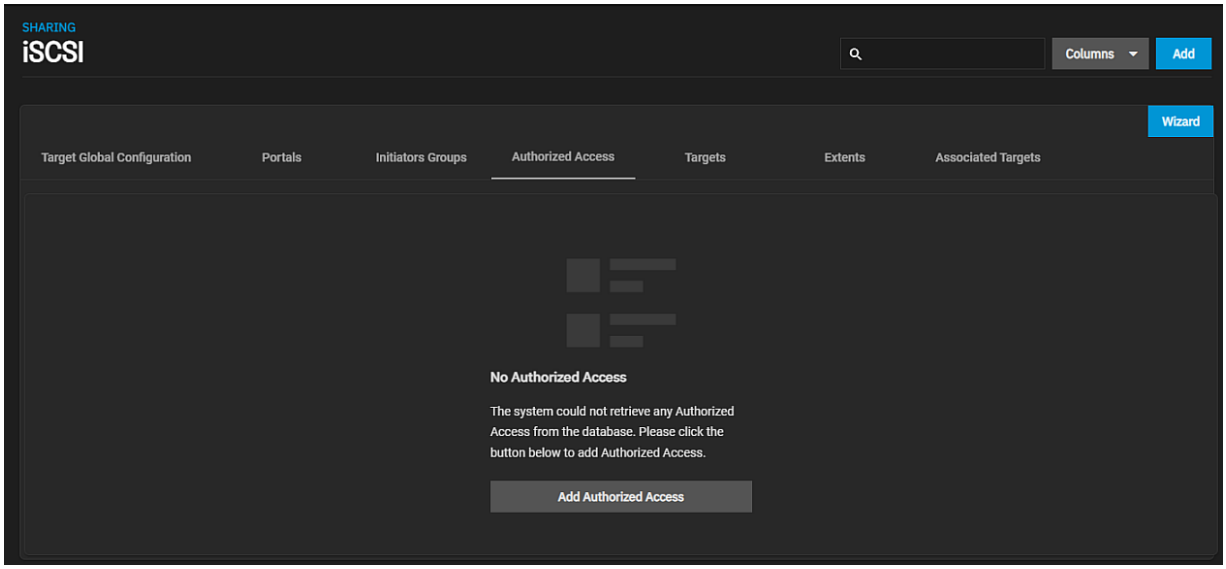


Setting	Description
Allow All Initiators	Select to allows all initiators.
Allowed Initiators (IQN)	Enter initiators allowed access to this system. Enter an iSCSI Qualified Name (IQN) and click **+** to add it to the list. Example: *iqn.1994-09.org.freebsd:freenas.local*.
Authorized Networks	Enter network addresses allowed to use this initiator. Each address can include an optional CIDR netmask. Click **+** to add the network address to the list. Example: *192.168.2.0/24*.
Description	Enter any notes about the initiators.

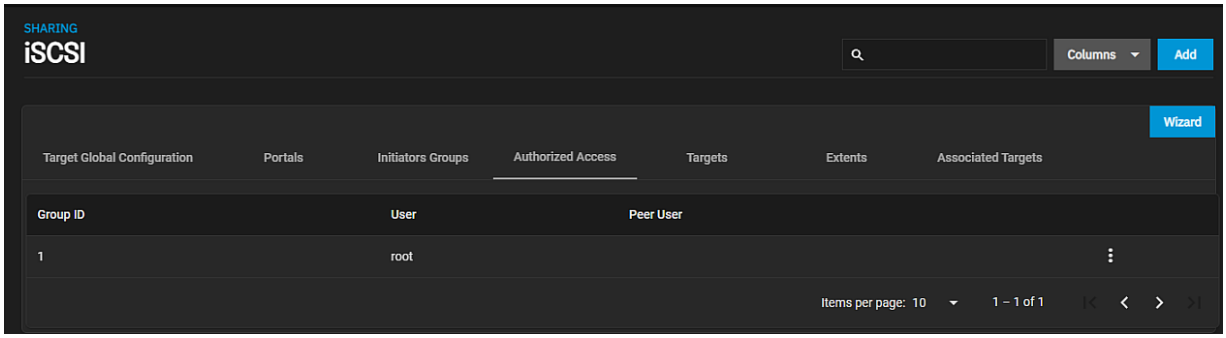
Authorized Access Screen

The **Authorized Access** screen displays settings to create new authorized access networks or edit existing ones in the list.

If authorized access is not set up yet, if you use the set up wizard and do not include the authorized access at that time, the **No Authorized Access** screen displays with the **Add Authorized Access** button in the center of the screen. **Add Authorized Access** or **Add** at the top of the screen opens the **Sharing > iSCSI > Authorized Access > Add** screen.

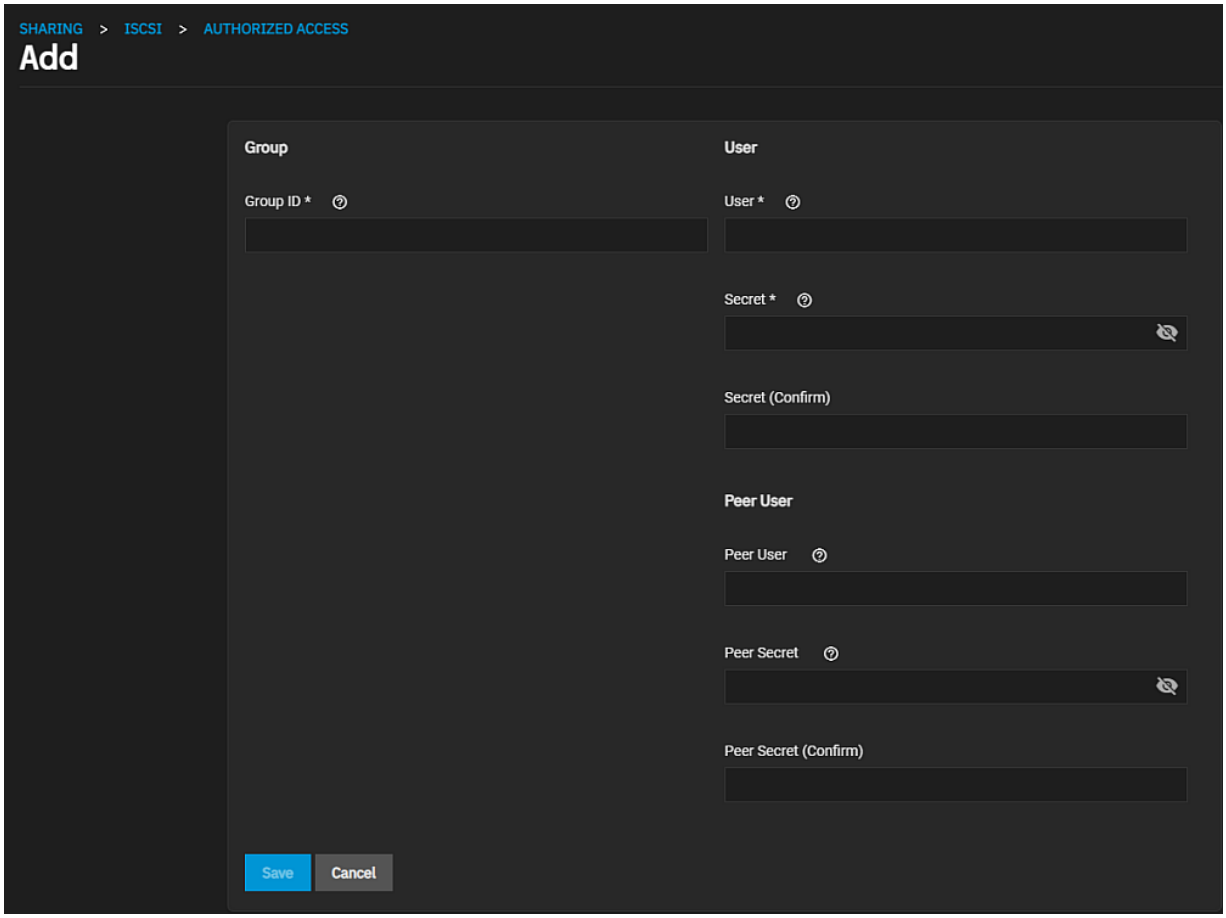


After adding authorized access to the system, the **Authorized Access** screen displays a list of users.



ADD opens the **Sharing > iSCSI > Authorized ACcess > Add** screen.

The ⋮ next to each entry displays two options, **Edit** and **Delete**. **Edit** opens the **Sharing > iSCSI > Authorized ACcess > Edit** screen and **Delete** opens a dialog to delete the authorized access for the selected user. The **Add** and **Edit** screens display the same settings.



Group Settings

Setting	Description
Group ID	Enter a number. This allows configuring different groups with different authentication profiles. Example: all users with a group ID of *1* inherits the authentication profile associated with *Group 1*.

User Settings

Setting	Description
User	User account to create for CHAP authentication with the user on the remote system. Many initiators use the initiator name as the user name.
Secret	Enter the user password. Must be at least 12 and no more than 16 characters long. The screen displays a “password does not match” error until you enter the same password in **Secret (Confirm)**.
Secret (Confirm)	Enter the same password to confirm the user password.

Peer User Settings

Setting	Description
Peer User	Optional. Enter only when configuring mutual CHAP. Usually the same value as **User**.
Peer Secret	Enter the mutual secret password. Required if entering a **Peer User**. Must be a different password than the password in **Secret**.
Peer Secret (Confirm)	Enter the same password to confirm the mutual secret password.

Targets Screen

The **Targets** screen displays settings to create new TrueNAS storage resources or edit existing ones in the list.

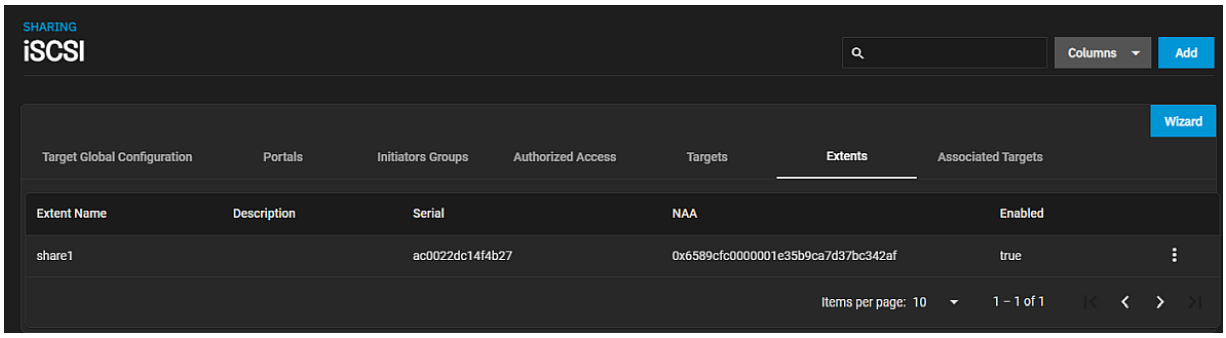
SharingiSCSITargetsScreen change

ADD opens the **Add iSCSI Targets** screen.

The ⋮ next to each entry displays two options, **Edit** and **Delete**. **Edit** opens the **Edit iSCSI Targets** screen and **Delete** opens a dialog to delete the select target. The **Add iSCSI Targets** and **Edit iSCSI Targets** screens display the same settings.

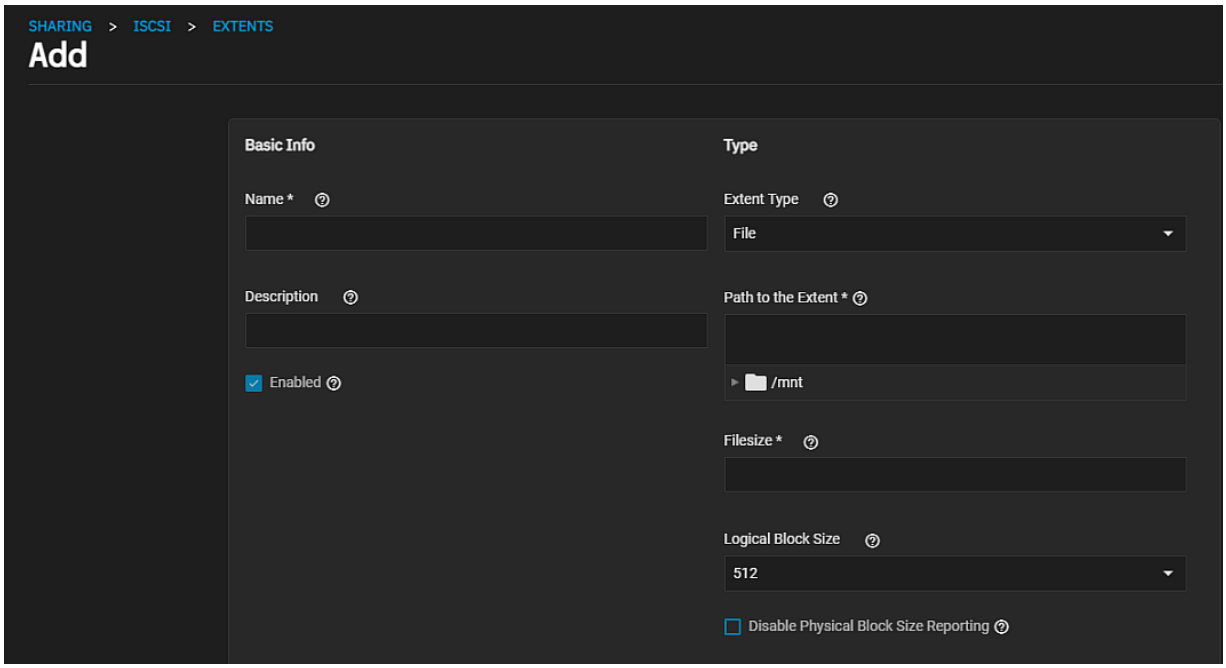
Extents Screen

The **Extents** screen displays settings to create new shared storage units or edit existing ones in the list.



ADD opens the **Sharing > iSCSI > Extents > Add** screen.

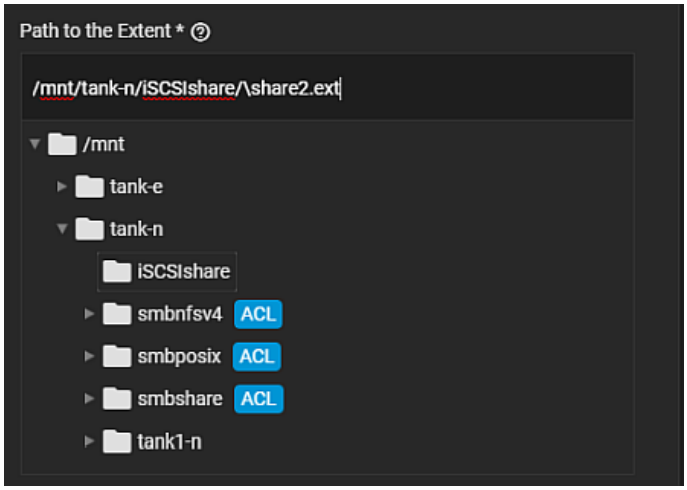
The ⋮ next to each entry opens two options, **Edit** and **Delete**. **Edit** opens the **Sharing > iSCSI > Extents > Edit** screen and **Delete** opens a dialog to delete the extents for the selected user. The **Add** and **Edit** screens display the same settings.



Basic Info Settings

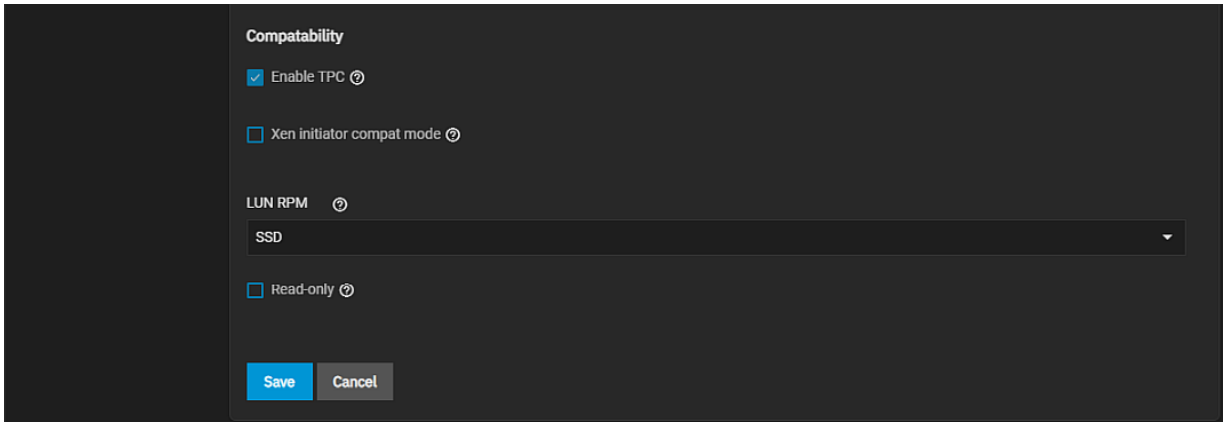
Setting	Description
Name	Enter a name for the extent. An **Extent** where the size is not **0**, cannot be an existing file within the pool or dataset.
Description	Enter any notes about this extent.
Enabled	Select to enable the iSCSI extent.

Type Settings



Setting	Description
Extent Type	elect the extent (zvol) option from the dropdown list. **Device** provides virtual storage access to zvols, zvol snapshots, or physical devices. **File** provides virtual storage access to a single file. **Device** provides virtual storage access to zvols, zvol snapshots, or physical devices. **File** provides virtual storage access to a single file.
Device	Required. Displays if **Extent Type** is set to **Device**. Select the unformatted disk, controller, or zvol snapshot.
Path to the Extent	Displays when **Extent Type** is set to **File**. Click the ▶ to browse to an existing file. Create a new file by browsing to a dataset and appending /{filename.ext} to the path. Users cannot create extents inside a jail root directory.
Filesize	Only appears if **File** is selected. Entering **0** uses the actual file size and requires that the file already exists. Otherwise, specify the file size for the new file.
Logical Block Size	Enter a new value or leave at the default of **512** unless the initiator requires a different block size.
Disable Physical Block Size Reporting	Select if the initiator does not support physical block size values over 4K (MS SQL).

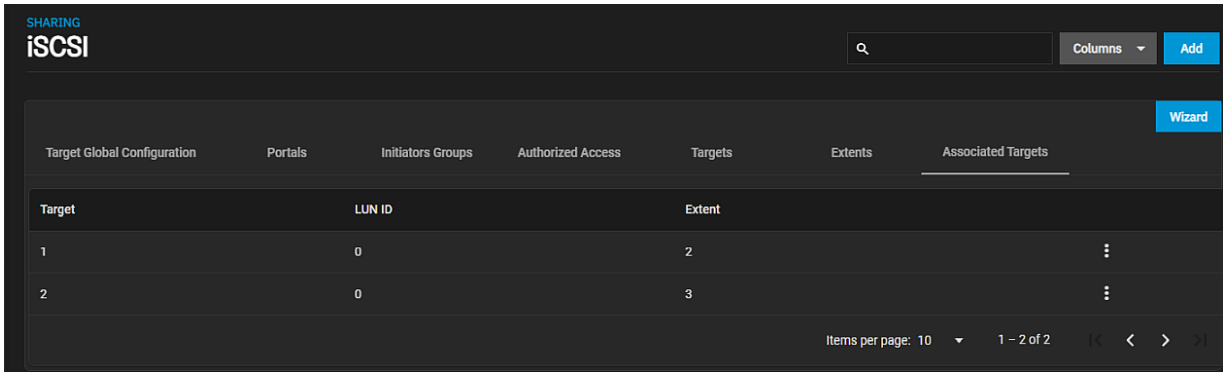
Compatibility Settings



Setting	Description
Enable TPC	Select to allow an initiator to bypass normal access control and access any scannable target. This allows xcopy operations that are otherwise blocked by access control.
Xen initiator compat mode	Select when using Xen as the iSCSI initiator.
LUN RPM	Select the option from the dropdown list. Options are **UNKNOWN**, **5400**, **7200**, **10000** or **15000**. Do *not* change this setting when using Windows as the initiator. Only change in large environments where the number of systems using a specific RPM is needed for accurate reporting statistics.
Read-only	Select to prevent the initiator from initializing this LUN.

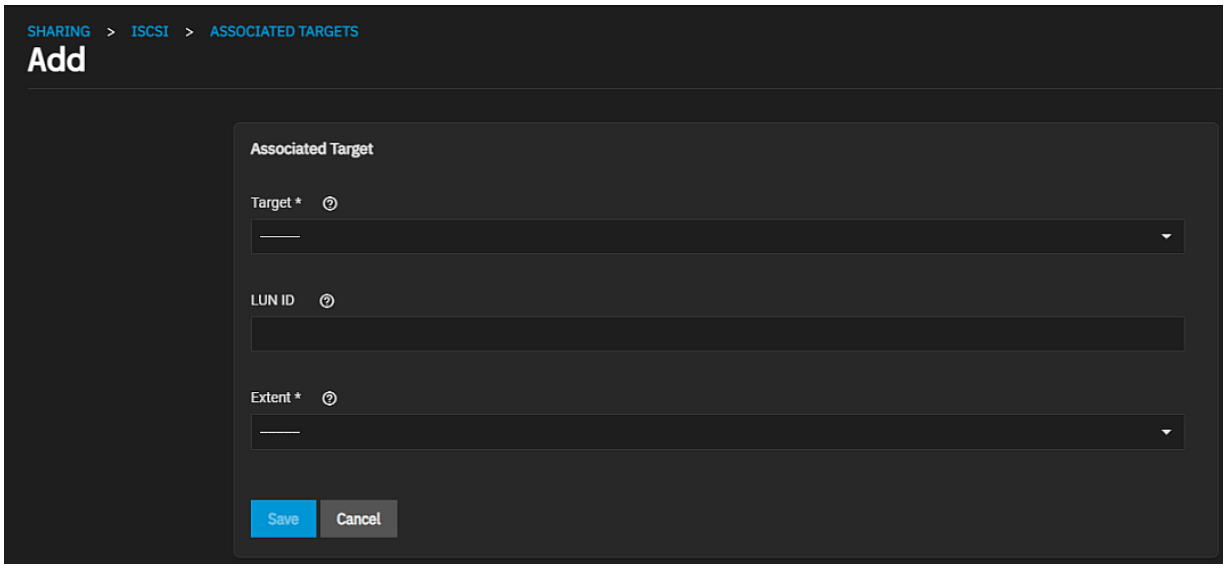
Associated Targets Screen

The **Associated Targets** screen displays settings to create new associated TrueNAS storage resources or edit existing ones in the list.



ADD opens the **Sharing > iSCSI > Associated Targets > Add** screen.

The ⋮ next to each entry displays two options, **Edit** and **Delete**. **Edit** opens the **Sharing > iSCSI >Associated Targets > Edit** screen and **Delete** opens a dialog to delete the associated targets for the selected user. The **Add** and **Edit** screens display the same settings.



Setting	Description
Target	Required. Select an existing target.
LUN ID	Select the value or enter a value between 0 and 1023. Some initiators expect a value below 256. Leave this field blank to automatically assign the next available ID.
Extent	Required. Select an existing extent.

Related Content

- Adding iSCSI Block Shares
- Using an iSCSI Share
- Increasing iSCSI Available Storage

4.4.4 - WebDAV Shares

Article Summaries

- WebDAV Shares Screens

  This article provides information on WebDAV screens and settings.

4.4.4.1 - WebDAV Shares Screens

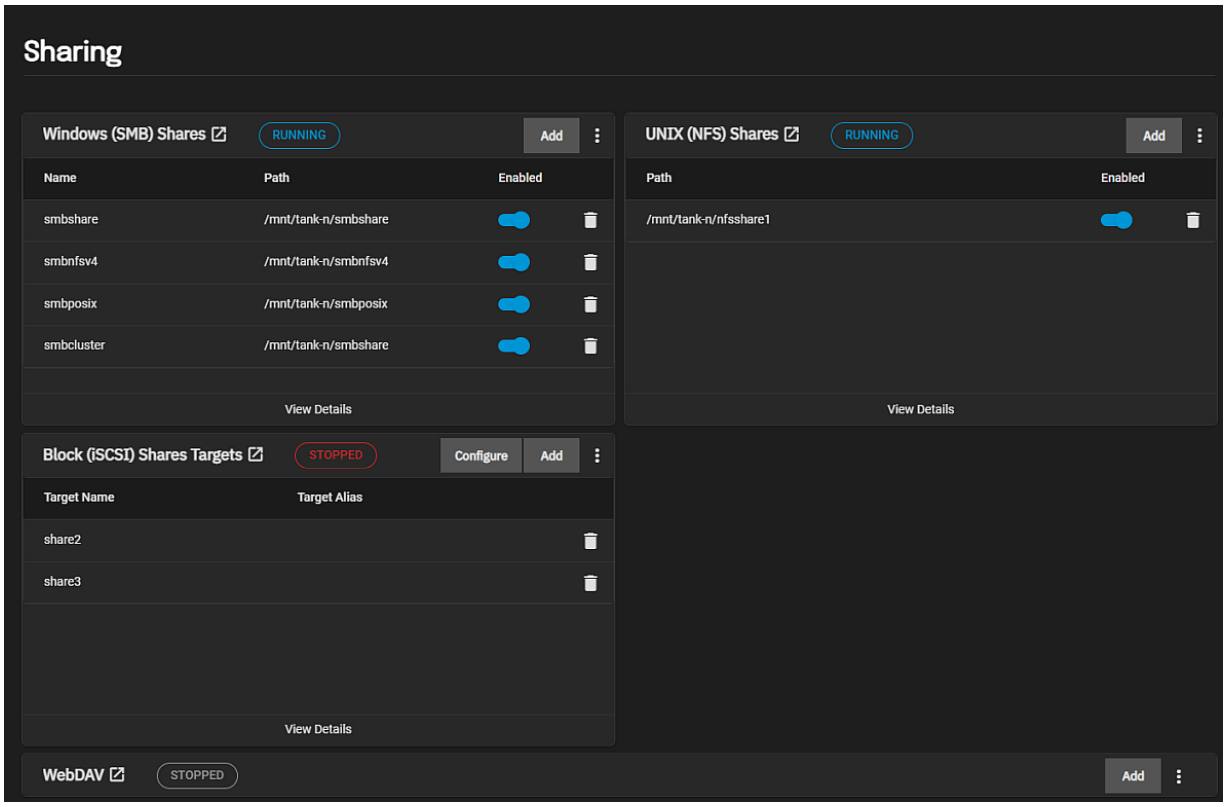
This article provides information on WebDAV screens and settings.

A Web-based Distributed Authoring and Versioning (WebDAV) share makes it easy to share a TrueNAS dataset and its contents over the web.

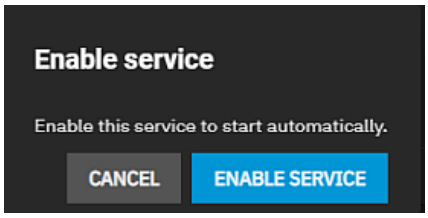
The **Sharing** screen opens after you click **Shares** on the main navigation panel.

WebDAV Widget

The **WebDAV** widget includes the widget toolbar that displays the status of the WebDAV service and the **Add** button. After adding WebDAV shares, the widget displays a list of the shares below the toolbar.



After adding the first WebDAV share, the system opens an enable service dialog.

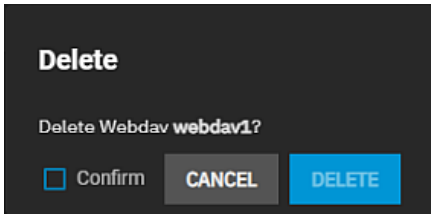


Enable Service turns the WebDAV service on and changes the toolbar status to **Running**. If you added shares of other types, the widget occupies a quarter of the screen.

The **Enable** toggle for each share shows the current status of the share. When disabled, it disables the share but does not delete the configuration from the system.

The shares list on the widget includes a **Read Only** toggle that turns this on or off.

The delete icon displays a delete confirmation dialog that removes the share from the system.



View Details and clicking anywhere on **WebDAV** the opens the **Sharing > WebDAV** screen with the list view of WebDAV shares.

The WebDAV share on the widget opens the Edit WebDAV screen.

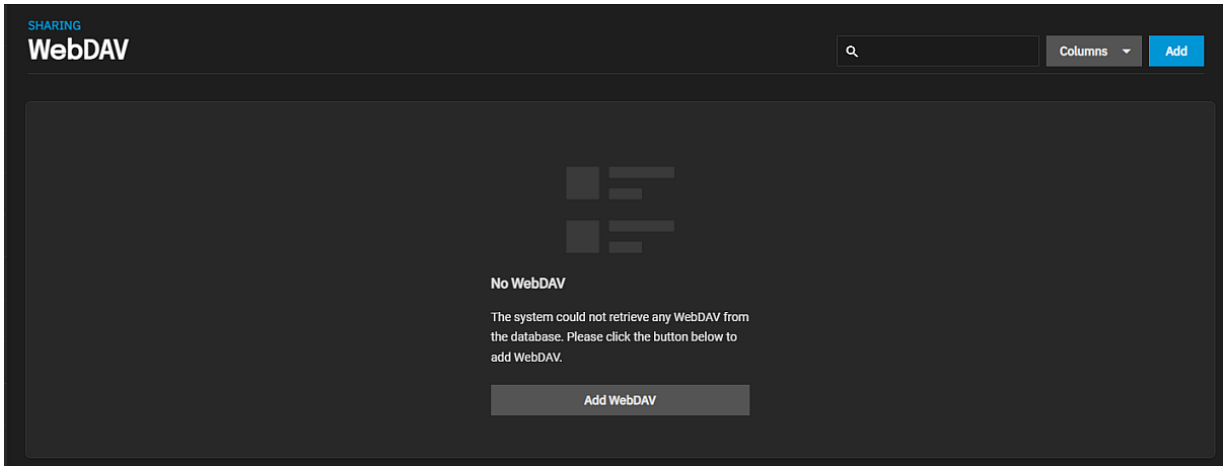
WebDAV Widget Toolbar

The **WebDAV** widget toolbar includes the **Add** button and an actions menu.

The on the toolbar displays options turn the WebDAV service on or off. **Turn Off Service** displays if the service is running or **Turn On Service** if the service is stopped. The **Config Service** option opens the Services > WebDAV configuration screen.

The toolbar displays the **STOPPED** service status in red before you start the service or click **Enable Service** when the dialog displays. When service is started it displays **RUNNING** in blue.

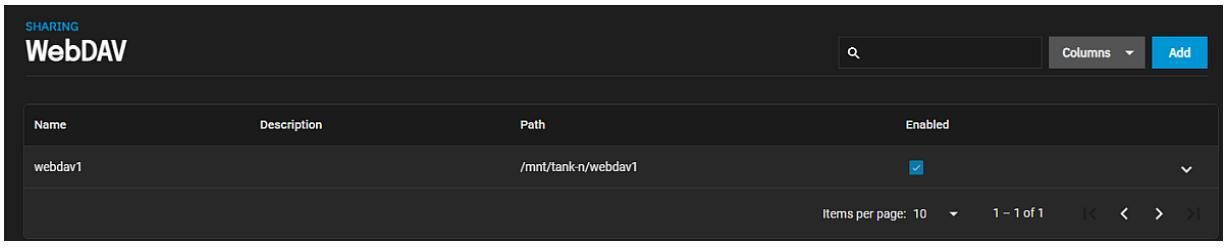
Add opens the **No WebDAV** screen if no shares exist on the system.



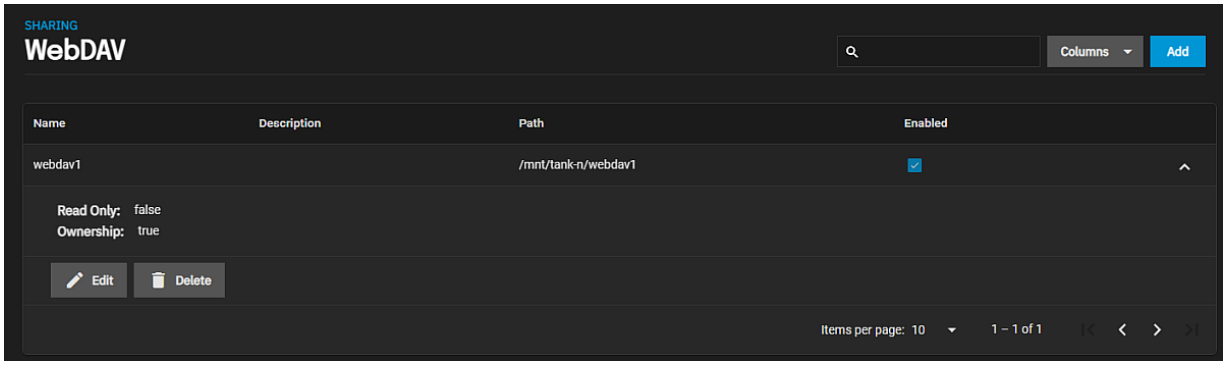
Add WebDAV opens the Add WebDAV screen. If the system has WebDAV shares, **Add** opens the **Add WebDAV** screen to add more shares.

Sharing WebDAV Details Screen

The **Sharing > WebDAV** details screen displays the same list of shares as the **WebDAV** widget.



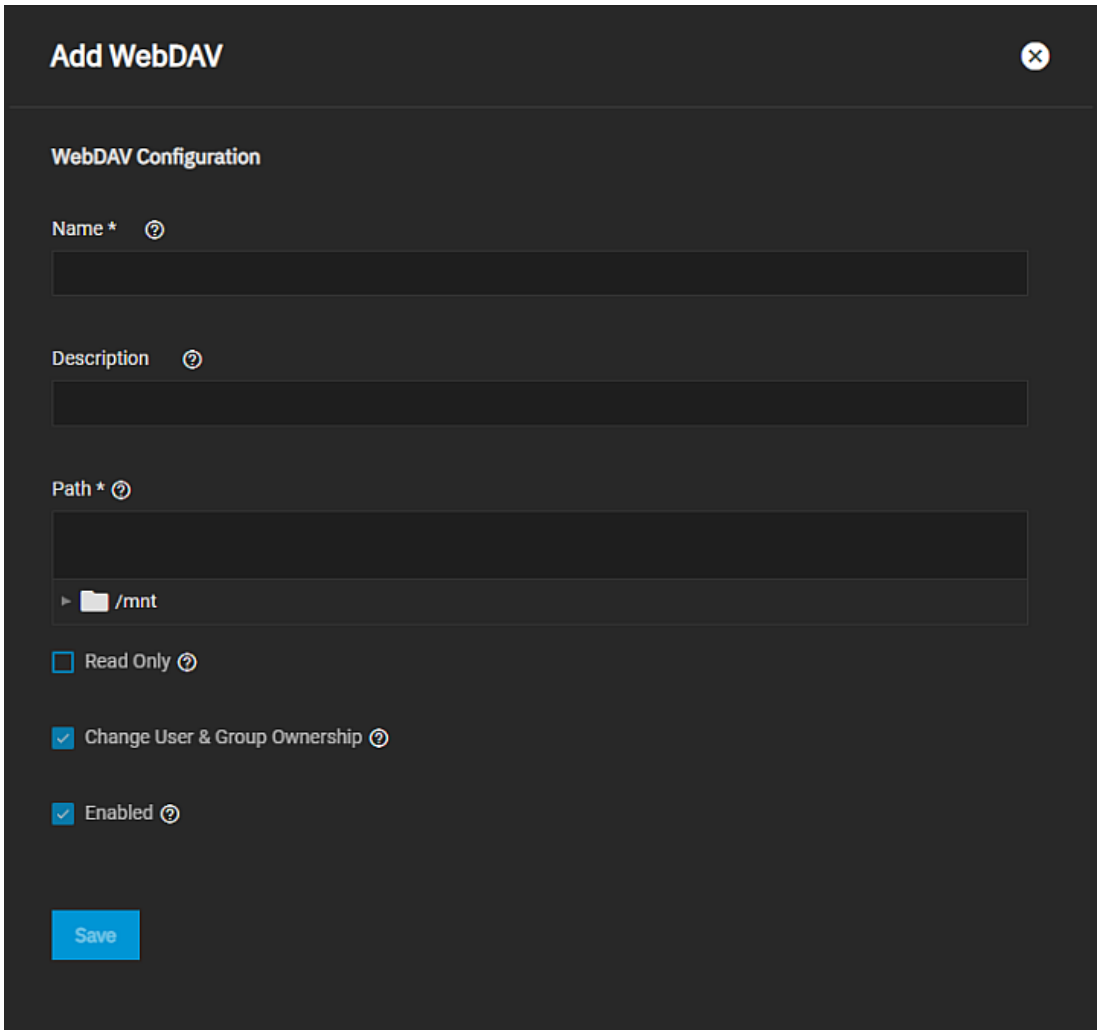
Customize the information using the **Columns** dropdown list. Select from the **Select All, Description**, **Path**, **Enabled**, **Read Only**, **Ownership** and **Reset to Defaults** options.



The ⌄ displays share details and the option to **Edit** or **Delete** the share. **Edit** opens the **Edit WebDAV** configuration screen. **Delete** opens an **Delete** confirmation dialog. Select **Confirm** and then **Delete** to remove the share without affecting the data in the share dataset.

Add and Edit WebDAV Screens

The **Add WebDAV** and **Edit WebDAV** display the same settings.



Setting	Description
Name	Required. Enter a name for the share.
Description	Enter any notes or reminders about the share.
Path	Enter the path or use the ▸ icon to the left of 🗀 **/mnt** to locate the dataset and populate the path. **Path** is the directory tree on the local file system.

Setting	Description
Read Only	Select to prohibit users from writing to this share. The **Read Only** toggle on the **WebDAV** widget displays this setting status.
Change User & Group Ownership	Select to change existing ownership of all files in the share to the **webdav** user and group. This displays a warning dialog. If left clear, you must manually set ownership of the files accessed through WebDAV to **webdav** or **www** user and group.
Enabled	Select to enable this WebDAV share. Clear the checkbox to disable the share without deleting the configuration.

Related Content

- Adding Cloud Credentials
- Cloud Credentials Screens
- Configuring WebDAV Shares
- Configuring WebDAV Service
- WebDAV Service Screen

4.5 - Data Protection

The **Data Protection** screen allows users to set up multiple redundant tasks that protect and/or backup data in case of drive failure.

Scrub tasks and S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) tests can provide early disk failure alerts by identifying data integrity problems and detecting various indicators of drive reliability.

Cloud sync, periodic snapshot, rsync, and replication tasks provide backup storage for data and allow users to revert the system to a previous configuration or point in time.

Ready to get started? Choose a topic or article from the left-side **Navigation** pane. Click the **<** symbol to expand the menu to show the topics under this section.

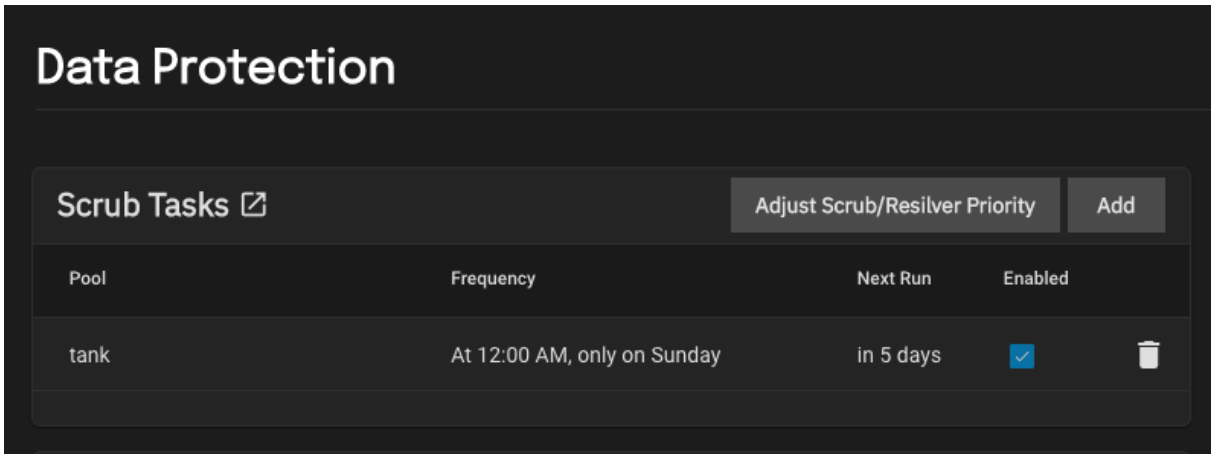
Article Summaries

- Scrub Tasks Screens
- Cloud Sync Tasks Screens
- Rsync Tasks Screens
- Periodic Snapshot Tasks Screens
- S.M.A.R.T. Tests Screens
- Replication Task Screens

4.5.1 - Scrub Tasks Screens

This article provides information on data protection scrub task settings and screens.

The **Data Protection** screen **Scrub Task** widget displays a list of scrub tasks configured on the system. Scrubs identify data integrity problems, detect silent data corruptions caused by transient hardware issues, and provide early disk failure alerts. TrueNAS generates a default scrub task when you create a new pool and sets it to run every Sunday at 12:00 AM.



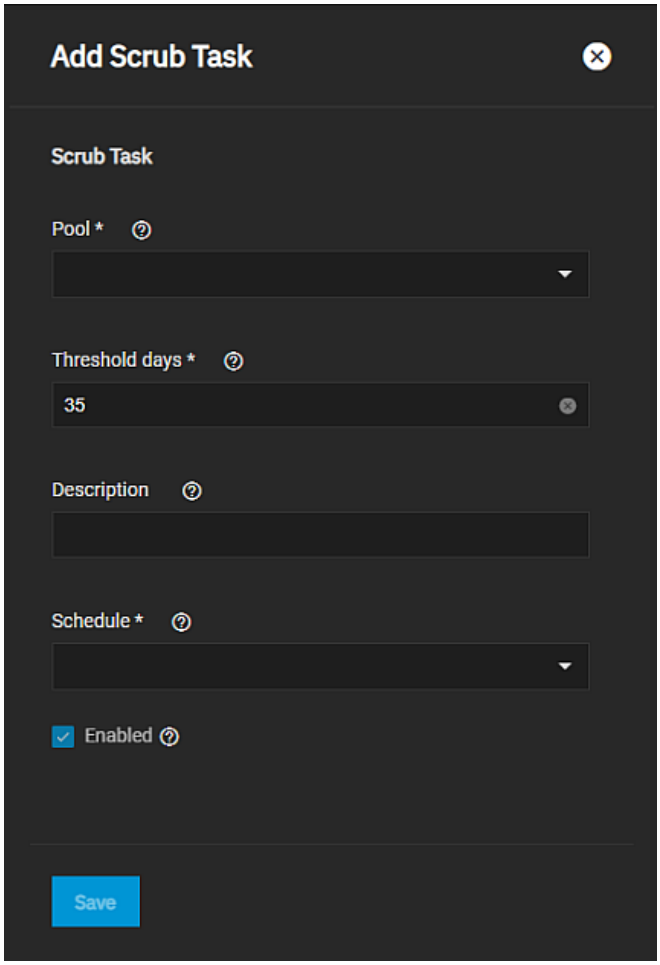
Add opens the **Add Scrub Task** screen.

Each task is a link that opens the **Edit Scrub Task** Screen.

The icon opens a delete confirmation dialog.

Add and Edit Scrub Task Screen

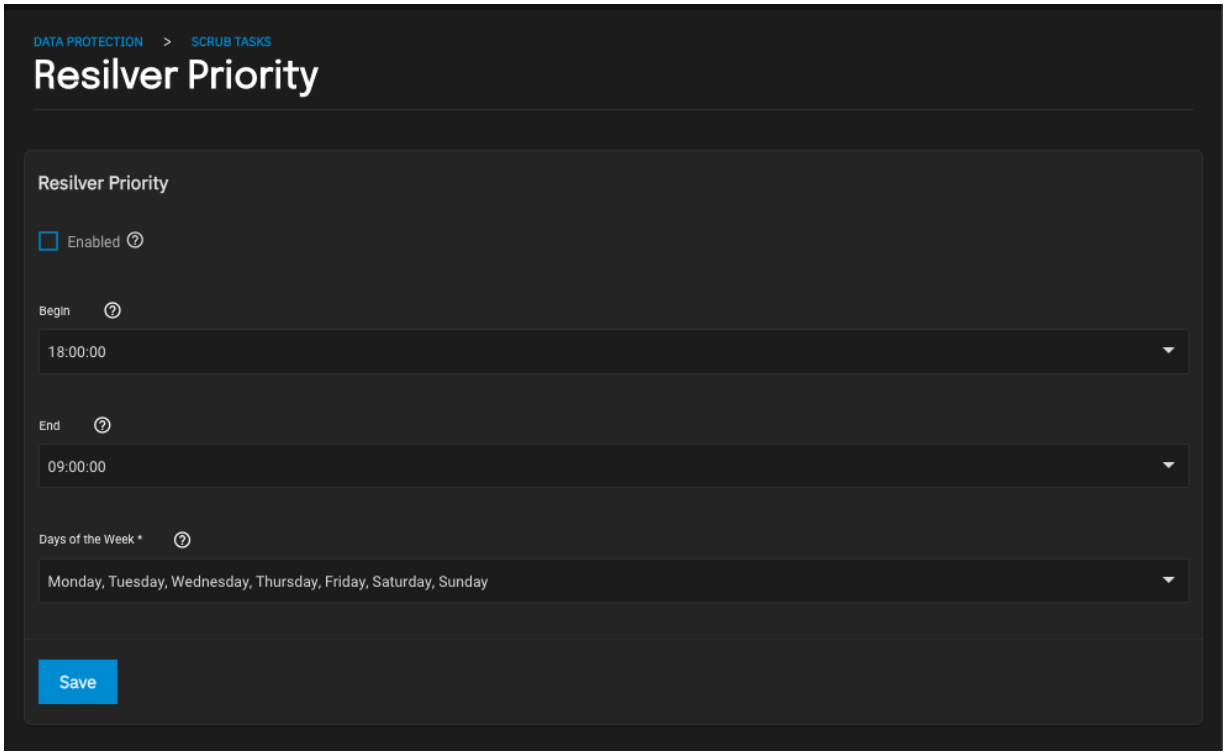
The **Add Scrub Task** and **Edit Scrub Task** screens display the same settings that specify the pool, threshold, and schedule for when to run the ZFS scan on the data in a pool.



Setting	Description
Pool	Select the pool to scrub from the dropdown list.
Threshold days	Enter the number of days before a completed scrub is allowed to run again. This controls the task schedule. For example, scheduling a scrub to run daily and setting **Threshold days** to 7 means the scrub attempts to run daily. When the scrub succeeds, it continues to check daily but does not run again until the seven days have elapsed. Using a multiple of seven ensures the scrub always occurs on the same weekday.
Description	Enter a description for this scrub tasks.
Schedule	Select a preset from the dropdown list that runs the scrub task according to that schedule time. Select **Custom** to use the advanced scheduler.
Enabled	Select to enable the scrub task to run. Leave checkbox clear to disable the task without deleting it.

Scrub/Resilver Priority Screen

The settings specify times when new resilver tasks can start, and run, at a higher priority or when a resilver task cannot run at a lower priority.



Setting	Description
Enabled	Select to run resilver tasks between the configured times.
Begin	Select the hour and minute when a resilver task can start from the dropdown list. The resilver process can run at a higher priority.
End	Select the hour and minute when new resilver tasks are not allowed to start. This does not affect active resilver tasks. The resilver process must return to running at a lower priority. A resilver process running after this time likely takes much longer to complete due to running at a lower priority compared to other disk and CPU activities, such as replications, SMB transfers, NFS transfers, Rsync transfers, S.M.A.R.T. tests, pool scrubs, user activity, etc.
Days of the Week	Select the days to run resilver tasks from the dropdown list.

Related Content

- Managing Scrub Tasks

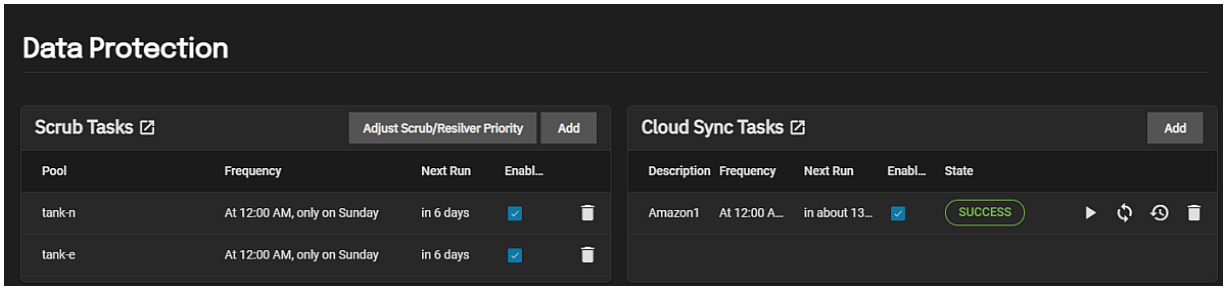
4.5.2 - Cloud Sync Tasks Screens

This article provides information on the cloud sync task screens and settings.

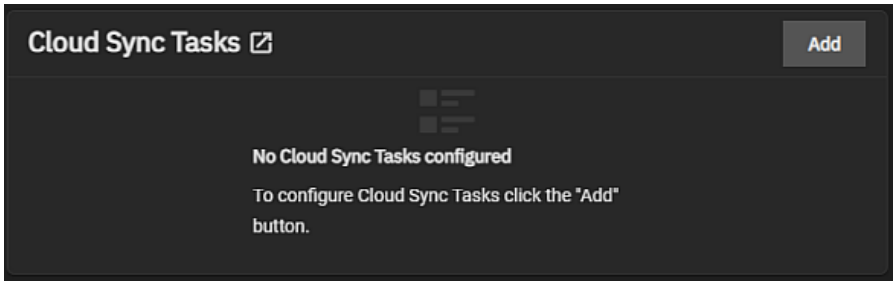
The **Cloud Sync Tasks** widget on the **Data Protection** screen provides access to cloud sync tasks configured on SCALE and to configuration screens with settings to add single-time or scheduled recurring transfers between TrueNAS SCALE and a could storage provider. They are an effective method to back up data to a remote location.

Cloud Sync Task Widget

The **Cloud Sync Task** widget displays a list of tasks configured on the system.

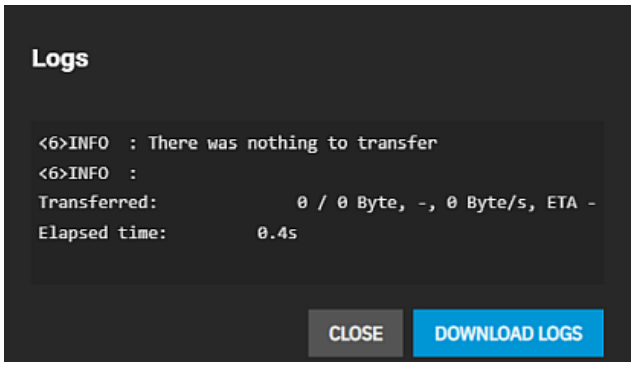


If cloud sync task are not yet configured **No Cloud Sync Tasks configured** displays in the widget.



Add opens the **Add Cloud Sync Task** screen. Each task listed is a link that opens the **Edit Cloud Sync Task** screen populated with with the settings for that task. Click on the **Description**, **Frequency** or **Next Run** column entry to open the edit task screen.

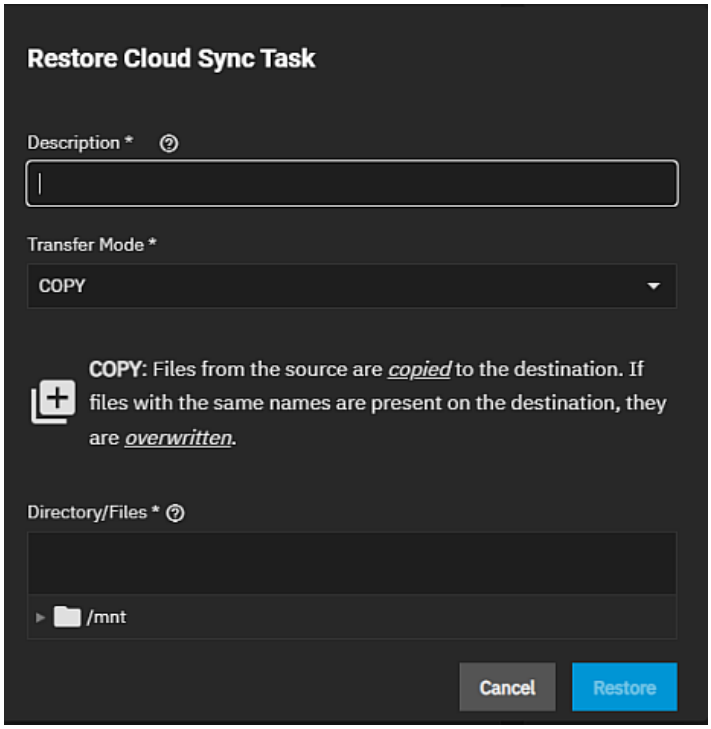
State displays the status of the next cloud sync task. Click on the state for the cloud sync task to display a **Logs** window for that task. Click **Download Logs** to save a copy of the current task logs.



The ▶ **Run Now** icon starts the cloud sync, running outside of the time scheduled in the saved configuration.

The **Dry Run** icon performs the same function as the **Dry Run** button on the add and edit configuration screens. It performs a test of the configured settings.

The **Restore** icon creates a new cloud sync task from an existing task that uses the same options but reverses the data transfer.



The **Delete** icon opens a simple delete dialog where you confirm before the system deletes the saved cloud sync task.

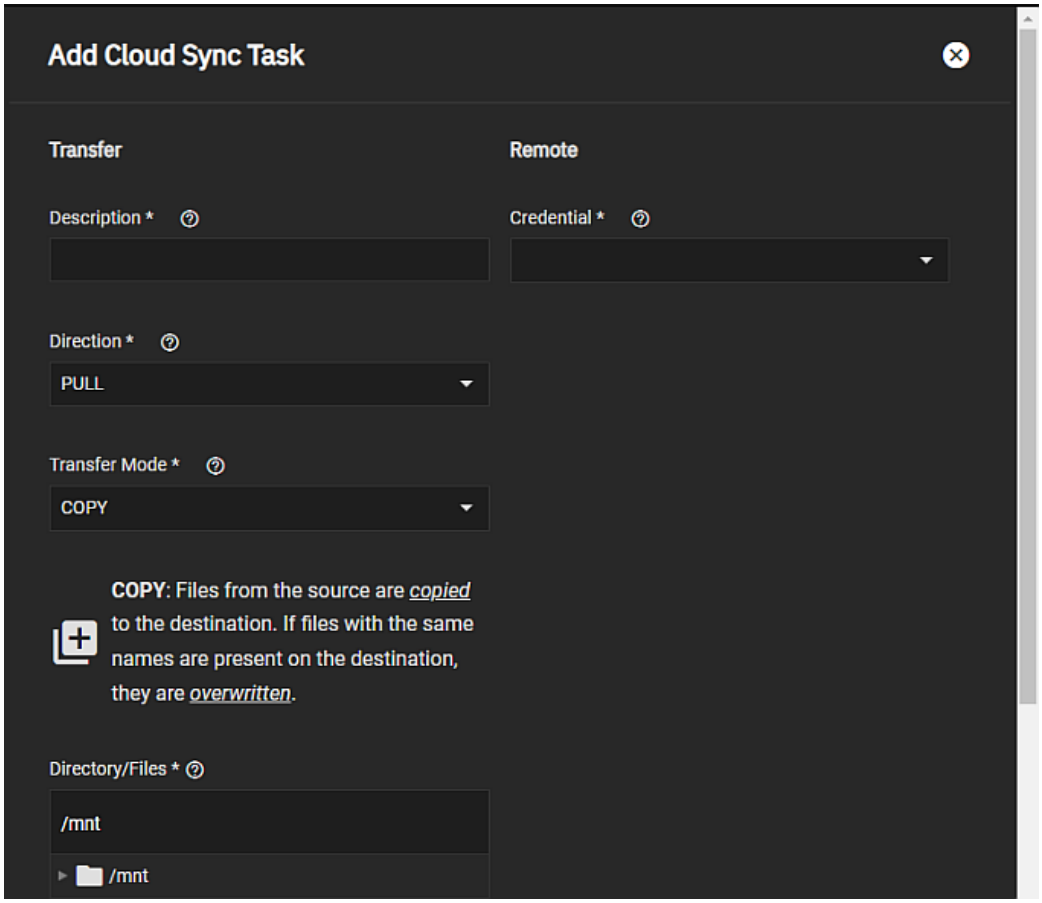
Add and Edit Cloud Sync Task Screens

The **Add Cloud Sync Task** and **Edit Cloud Sync Task** display the same settings.

The **Add a backup credential** option on the **Credential** dropdown list opens a window where you enter the cloud storage provider settings.

Transfer Settings

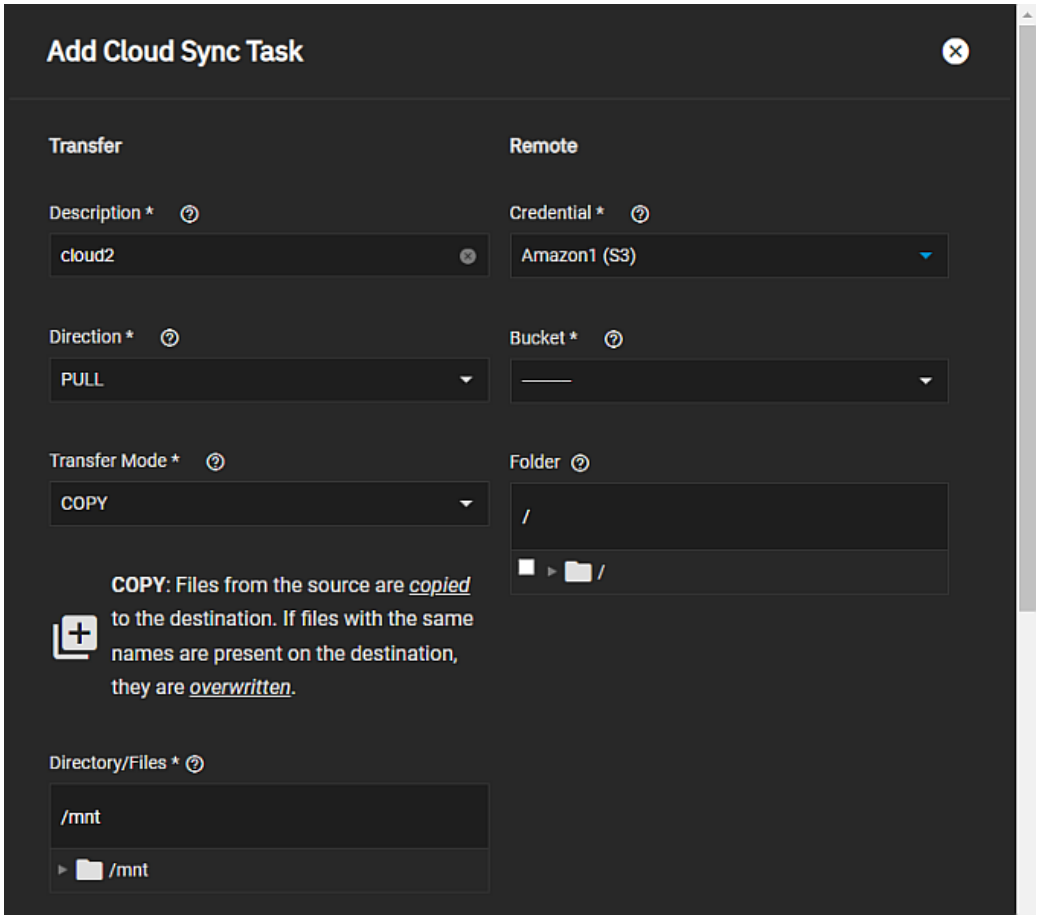
Transfer setting options change the



Settings	Description
Description	Enter a description of the cloud sync task.
Direction	Select a direction option from the dropdown list. **PUSH** sends data to cloud storage. **PULL** receives data from cloud storage and is the default setting. Changing the direction from **PULL** to **PUSH** or visa versa displays a **Transfer Mode Reset** information dialog and resets the **Transfer Mode** to **COPY**.
Transfer Mode	Select the transfer mode type from the dropdown list. To keep all files identical between the two storage locations, select **SYNC**. It changes files on the destination to match those on the source. If a file does not exist on the source, it is also deleted from the destination. To duplicate each source file into the destination and overwrite destination files using the same source select **COPY**. It copies files from the source to the destination. If files with the same names are present on the destination, they are overwritten. To transfer files from the source to the destination and delete source files select **MOVE**. If first copies files from the source to the destination and then deletes them from the source. Files with the same names on the destination are overwritten.
Directory/Files	Enter or click the ▸ arrow to the left of /mnt and at each dataset until you locate the dataset, directory location you want to send to the cloud for push syncs, or the destination to write to for pull syncs. Be cautious with pull destinations to avoid overwriting existing files. Click the ▸ arrow to the left of /mnt again to collapse the directory tree.

Remote Settings

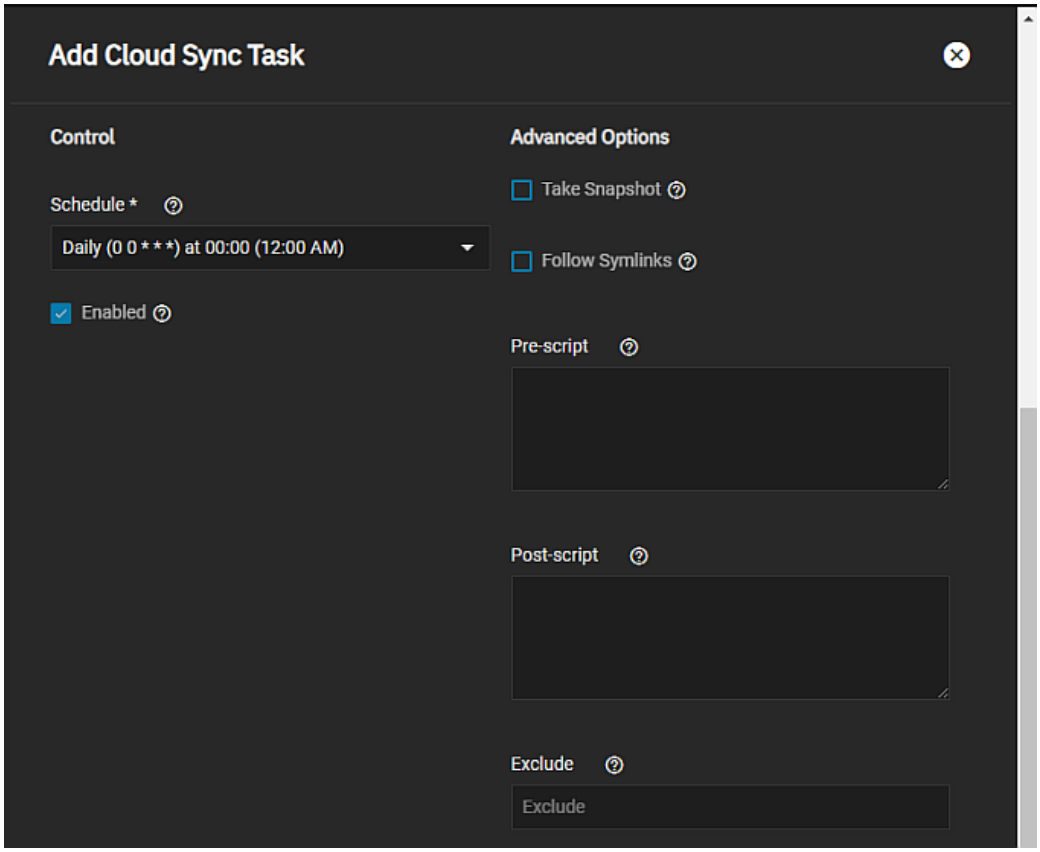
The option selected in **Credential** changes settings displayed in the **Remote** settings area or it opens a window with cloud provider settings.



Settings	Description
Credential	Select either **Add a backup credential** or a backup cloud storage provider credential from the dropdown list. **Add a backup credential** opens the cloud service provider settings window. The **Bucket** setting displays after selecting a credential that uses S3, like **Amazon S3**. TrueNAS automatically validates the selected credential. If you select a credential with invalid authentication settings the system displays an error dialog. Click **Fix Credential** opens the **Credentials > Backup Credentials > Cloud Credentials** configuration screen for that backup credential.
Bucket	Select the pre-defined bucket S3 to use.
Folder	Enter or click the ▸ arrow to the left of the 🗀 icon and at each directory or folder to reach the storage location to uses for this task.

Control Settings

Control settings establish when the cloud sync task occurs.



Settings	Description
Schedule	Select a schedule preset or choose Custom to open the advanced scheduler.
Enabled	Select to enable this Cloud Sync Task. To disable this cloud sync task without deleting it and make the configuration available without allowing the specified schedule to run the task, clear the checkbox. You can use the **Enable** column on the **Cloud Sync Tasks** widget to enable or disable the task.

Advanced Options Settings

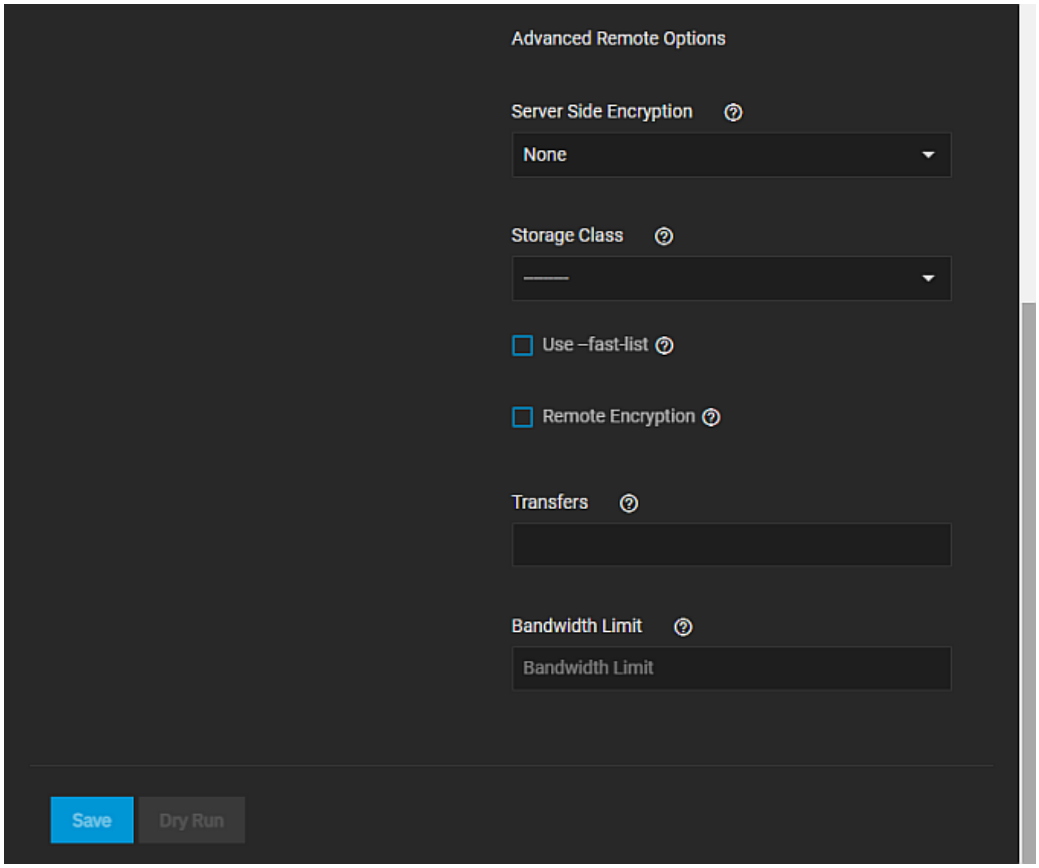
Advanced Options settings include settings for advanced users.

DataProtectionCloudSyncAdd change image

Settings	Description
Follow Symlinks	Select to follow symlinks and copy the items to which they link.
Pre-Script	For advanced users. Enter a script to execute before running sync. See for more information.
Post-Script	For advanced user. Enter a script to execute after running sync. See for more information.
Exclude	Enter a list of files and directories to exclude from sync. Separate entries by pressing `Enter`. Examples of proper syntax used to exclude files/directories are: • `photos</code>` excludes a file named *photos* • `/photos>` excludes a file named *photos* from root directory (but not subdirectories) • `photos/` excludes a directory named *photos • `/photos/` excludes a directory named *photos* from root directory (but not subdirectories). See rclone filtering for more details about the `--exclude` option.

Advanced Remote Options

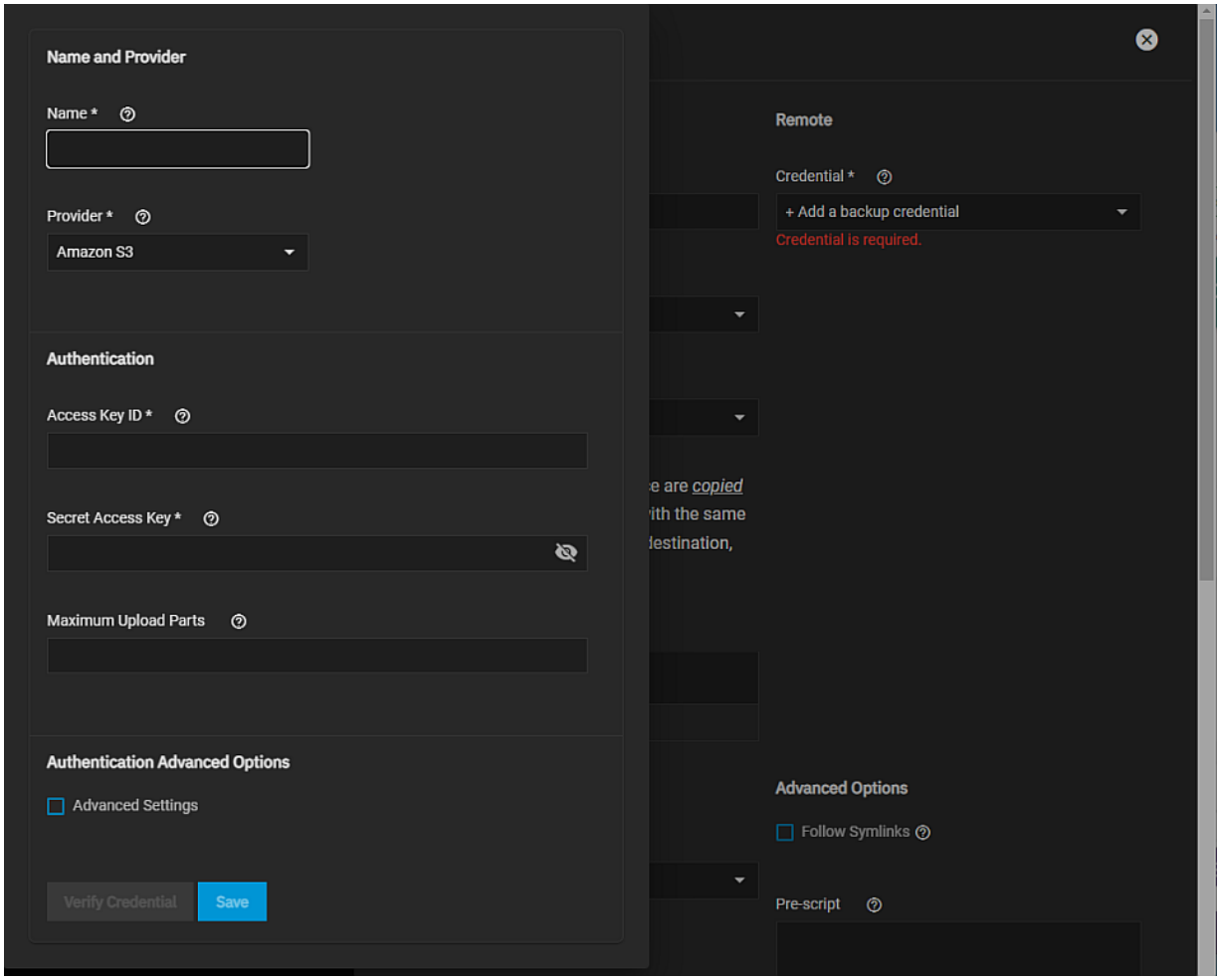
Advanced Remote Options configure settings related to the remote system.



Settings	Description
Remote Encryption	Selecting **PUSH** in **Direction** encrypts files before transfer and stores the encrypted files on the remote system. Files are encrypted using the encryption password and encryption salt values. Selecting **PULL** decrypts files stored on the remote system before the transfer. Transferring the encrypted files requires entering the same encryption password and encryption salt used to encrypt the files. Additional details about the encryption algorithm and key derivation are available in the rclone crypt File formats documentation.
Transfers	Enter the number of simultaneous file transfers. Enter a number based on the available bandwidth and destination system performance. See rclone –transfers.
Bandwidth limit	Enter a single bandwidth limit or bandwidth limit schedule in rclone format. Separate entries by pressing <kbdEnter. Example: *08:00,512 12:00,10MB 13:00,512 18:00,30MB 23:00,off*. You can specify units with the beginning letter: **b**, **k** (default), **M**, or **G**. See rclone –bwlimit.

Add Backup Credential Settings Window

After selecting **Add a backup credential** a new cloud storage provider window opens with TrueNAS **Name** and **Provider**, and after selecting the provider, the authentication settings that provider requires.



The settings in this backup credential window are also found on the **Credentials > Cloud Credentials** add or edit configuration screens. See Cloud Credentials Screens for more information on the cloud storage provider authentication settings.

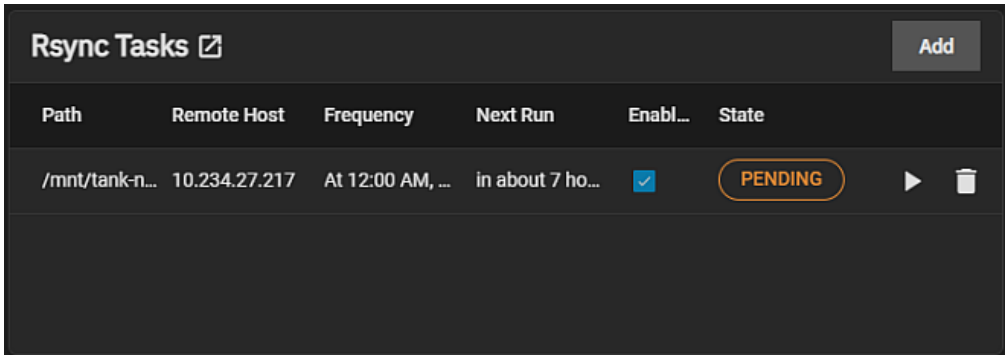
Related Content

- Adding Cloud Credentials
- Adding Cloud Sync Tasks
- Backing Up Google Drive to TrueNAS SCALE
- Cloud Credentials Screens
- Cloud Sync Tasks

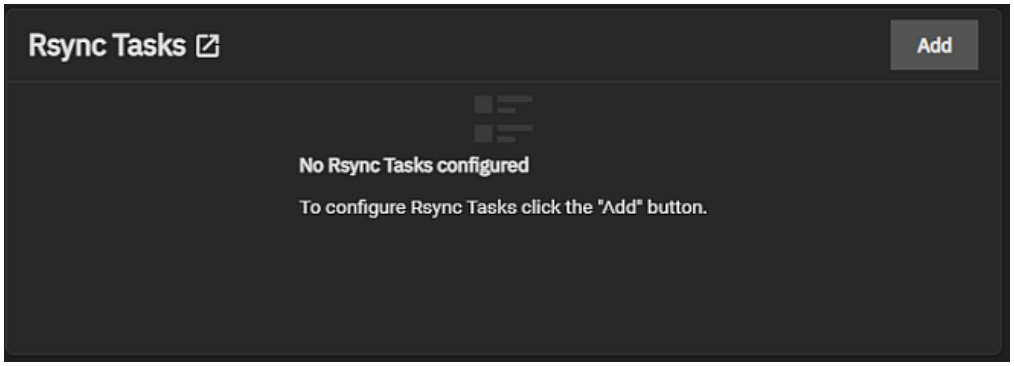
4.5.3 - Rsync Tasks Screens

This article provides information on the rsync task screens and settings.

The **Rsync Task** widget on the **Data Protection** screen lists rsync tasks configured on the TrueNAS system.



The **Rsync Tasks** widget displays **No Rsync Tasks configured** before you add a task.



Add opens the **Add Rsync Task** screen.

Each rsync task is a link to open the **Edit Rsync Task** screen.

The widget displays the status of a task as **PENDING**, **RUNNING**, **SUCCESS** or **FAILED**.

Use the ▶ **Run Now** icon to manually run the task.

Use the 🗑 icon to open a delete confirmation dialog.

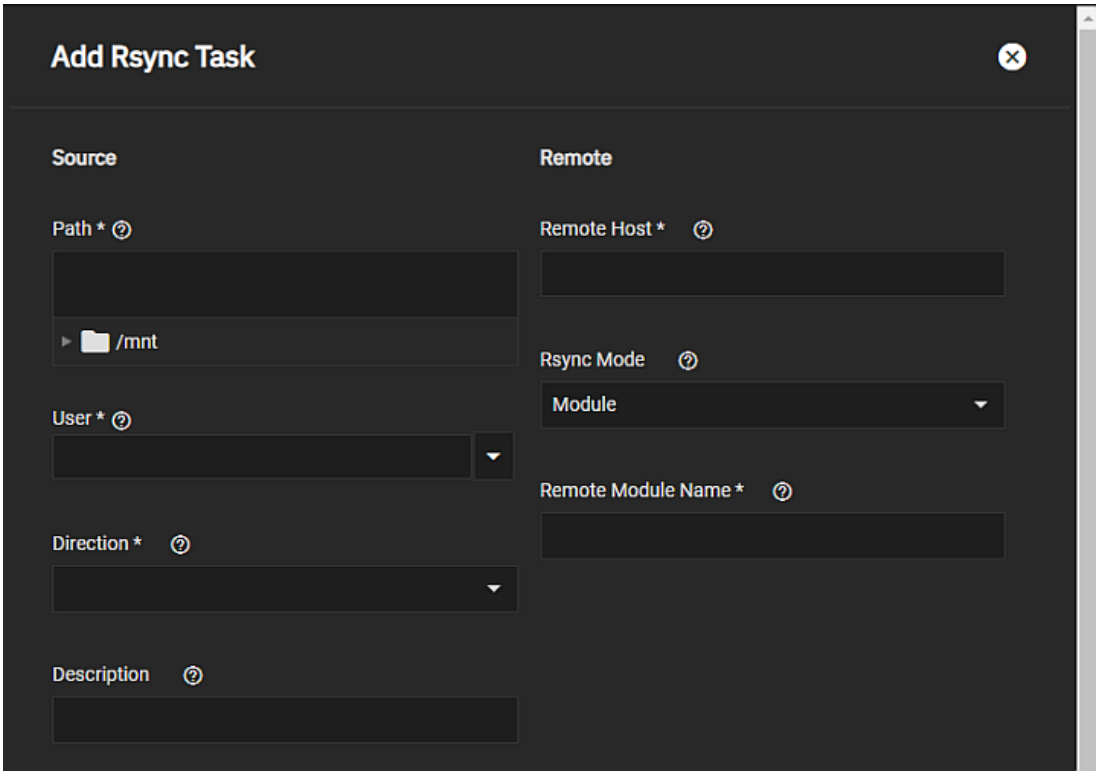
Add and Edit Rsync Task Screens

The **Add Rsync Task** and **Edit Rsync Task** display the same settings.

Source and Remote Settings

Source and **Remote** settings specify the direction of the remote sync, the TrueNAS system and the remote rsync server paths to or from the data location, the method to uses to sync the TrueNAS and remote servers and the user with permissions to do the remote sync operation.

Click Here for More Information

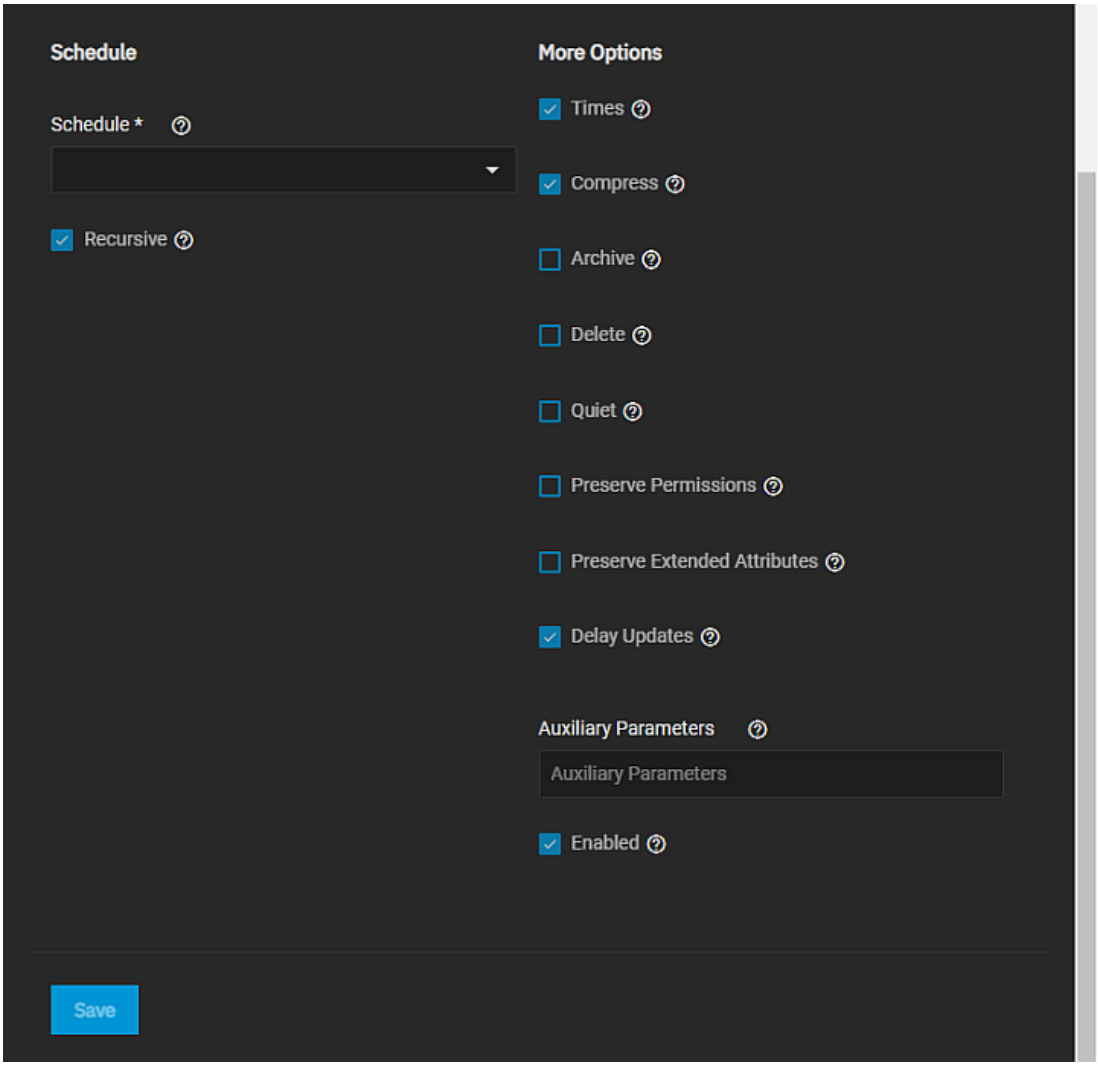


Setting	Description
Path	Required. Enter or use the ▸ to the left of **/mnt** to browse to the path to copy. Linux file path limits apply. Other operating systems can have different limits which might affect how you can use them as sources or destinations.
User	Required. Select the user to run the rsync task. Select a user that has permissions to write to the specified directory on the remote host.
Direction	Required. Select the direction of the flow of data to the remote host. Options are **Push** or **Pull**. During a push, the dataset transfers to the remote module. During a pull, the dataset stores files from the remote system.
Description	Enter a description of the rsync task.
Remote Host	Required. Enter the IP address or host name of the remote system that stores the copy. Use the format `username@remote_host` if the user name differs on the remote host.
Rsync Mode	Select the mode from the dropdown list. Select **Module** to use a custom-defined remote module of the rsync server or if the remote server is a TrueNAS, and then define the rsync module or select **SSH** to use an SSH configuration for the rsync task. The remote system must have SSH enabled. The host system needs an established SSH connection to the remote for the rsync task. **SSH** displays more settings.
Remote Module Name	Required. If **Rsync Mode** is **Module** specify the name of the module on the remote rsync server. Define at least one module in rsyncd.conf(5) or the rsync server or in the **Rsync Modules** of another TrueNAS system. Type the **Remote Module Name** exactly as it appears on the remote system.
Remote SSH Port	Required when **Rsync Mode** is **SSH**. Enter the SSH port number of the remote system. By default, **22** is reserved in TrueNAS.
Remote Path	Enter or use the ▸ to the left of **/mnt** to browse to the existing path on the remote host to sync with, or use **Validate Remote Path** to automatically create and define the path if it does not exist. Maximum path length is 255 characters.
Validate Remote Path	Displays if **Rsync Mode** is **Module**. Select to automatically create the defined **Remote Path** if it does not exist.

Schedule and More Options Settings

Schedule defines when the remote sync task occurs and **More Options** specify other settings related to when and how the rsync occurs.

Click Here for More Information



Setting	Description
Schedule	Select a schedule preset or select **Custom** to open the advanced scheduler.
Recursive	Select to include all subdirectories of the specified directory. When cleared, only the specified directory is included.
Times	Select to preserve modification times of files.
Compress	Select to reduce the size of data to transmit. Recommended for slow connections.
Archive	Select to preserve symlinks, permissions, modification times, group and special files. When selected, rsync runs recursively. When run as root, owner, device files, and special files are also preserved. Equal to passing the flags `-rlptgoD` to rsync.
Delete	Select to delete files in the destination directory that do not exist in the source directory.
Quiet	Select to suppress informational messages from the remote server.
Preserve Permissions	Select to preserve original file permissions. Useful when the user is set to root.
Preserve Extended Attributes	Select to preserve extended attributes, but this must be supported by both systems.
Delay Updates	Select to save a temporary file from each updated file to a holding directory until the end of the transfer. All transferred files renamed once the transfer is complete.
Auxiliary Parameters	Enter additional rsync(1) options to include. Separate entries by pressing `Enter`. Note: You must escape the * character with a backslash (\) or used inside single quotes ('*.txt').
Enabled	Select to enable this rsync task. Clear to disable this rsync task without deleting it.

Related Content

- Adding SSH Credentials

- Configuring Rsync Tasks
- Configuring Rsync Modules
- Rsync Services Screen

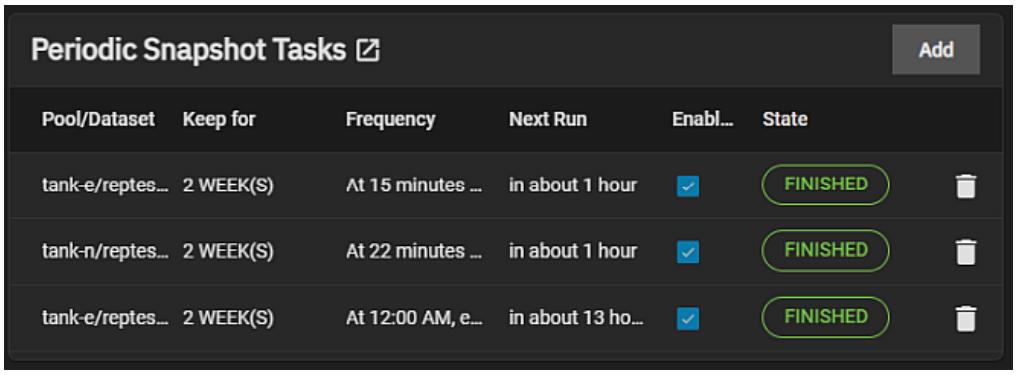
4.5.4 - Periodic Snapshot Tasks Screens

This article provides information on the data protection periodic snapshot task settings and screens.

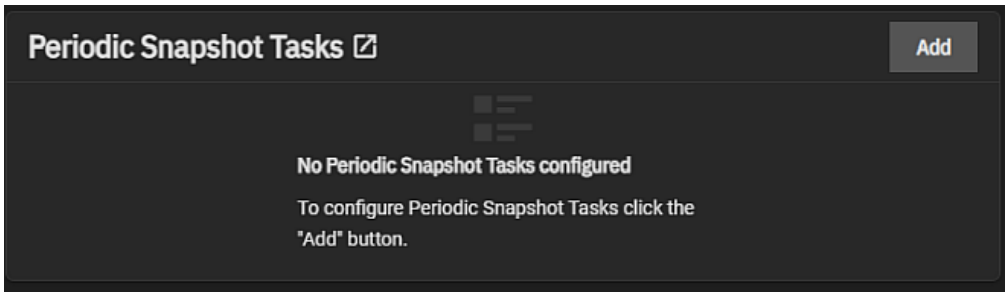
The **Data Protection** screen **Periodic Snapshot Task** widget displays periodic snapshot tasks created on the system. A periodic snapshot task allows scheduling the creation of read only versions of pools and datasets at a given point in time.

Periodic Snapshot Task Widget

The **Periodic Snapshot Task** widget displays a list of tasks configured on the system.



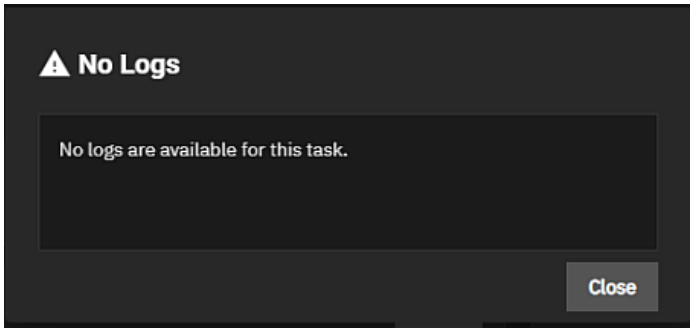
If a periodic snapshot task is not yet configured **No Periodic Snapshot Task configured** displays in the widget.



Add opens the **Add Periodic Snapshot Task** screen.

Each task listed is a link that opens the **Edit Periodic Snapshot Task** screen populated with with the settings for that task. Click on the **Description**, **Frequency**, or **Next Run** column entry to open the edit task screen.

State displays the status of the next cloud sync task. While on the widget, click on the state for the task to display a **Logs** window for that task. Click **Download Logs** to save a copy of the current task logs.



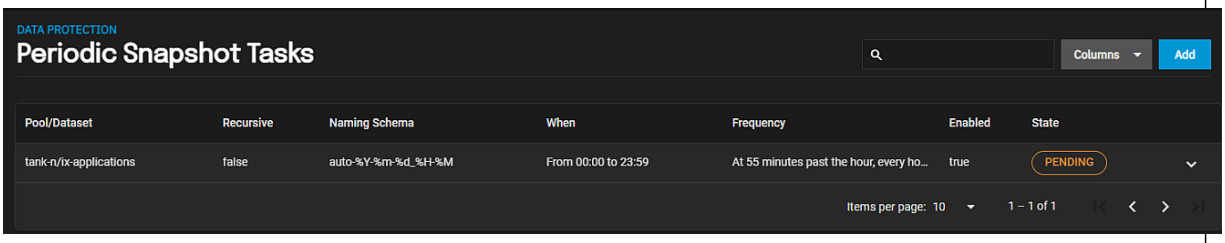
The **Delete** icon opens a simple delete dialog where you confirm before the system deletes the saved periodic snapshot task.

Periodic Snapshot Task List Screen

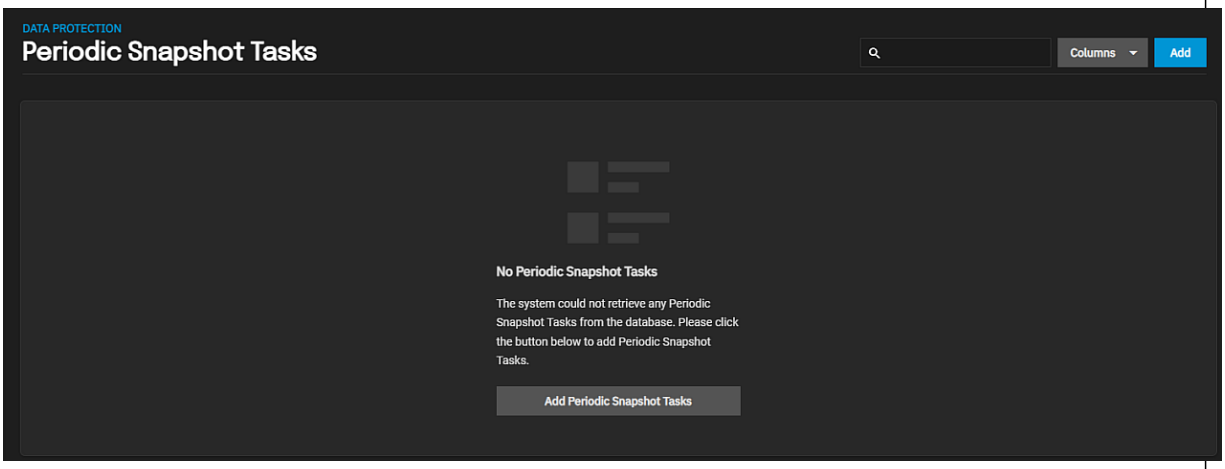
Periodic snapshot tasks display on both the **Data Protection** widget and **Periodic Snapshot Tasks** list screen.

Click Here for More Information

Click on the **Periodic Snapshot Task** header to open the **Data Protection > Periodic Snapshot Task** list screen.



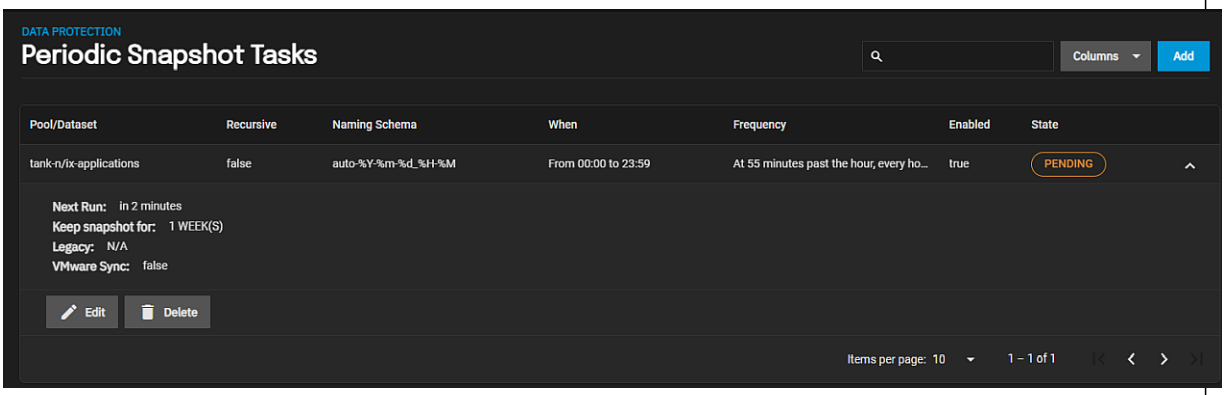
If a task is not added, the list view displays **Add Periodic Snapshot Tasks** which opens the **Add Periodic Snapshot Task** screen.



Columns displays a dropdown list of options to customize the list view. Options are **Select All**, **Recursive**, **Naming Schema**, **When**, **Frequency**, **Next Run**, **Keep snapshot for**, **VMWare Sync**, **Enabled**, **State**, and **Reset to Defaults**.

The **State** on the list view does not link to the log file or anything else. It just displays the current state of the task.

Click the expand icon at the right of the task to open the details for the selected task.



Edit opens the **Edit Periodic Snapshot Task** screen.

Delete opens the delete dialog that removes the task from the system.

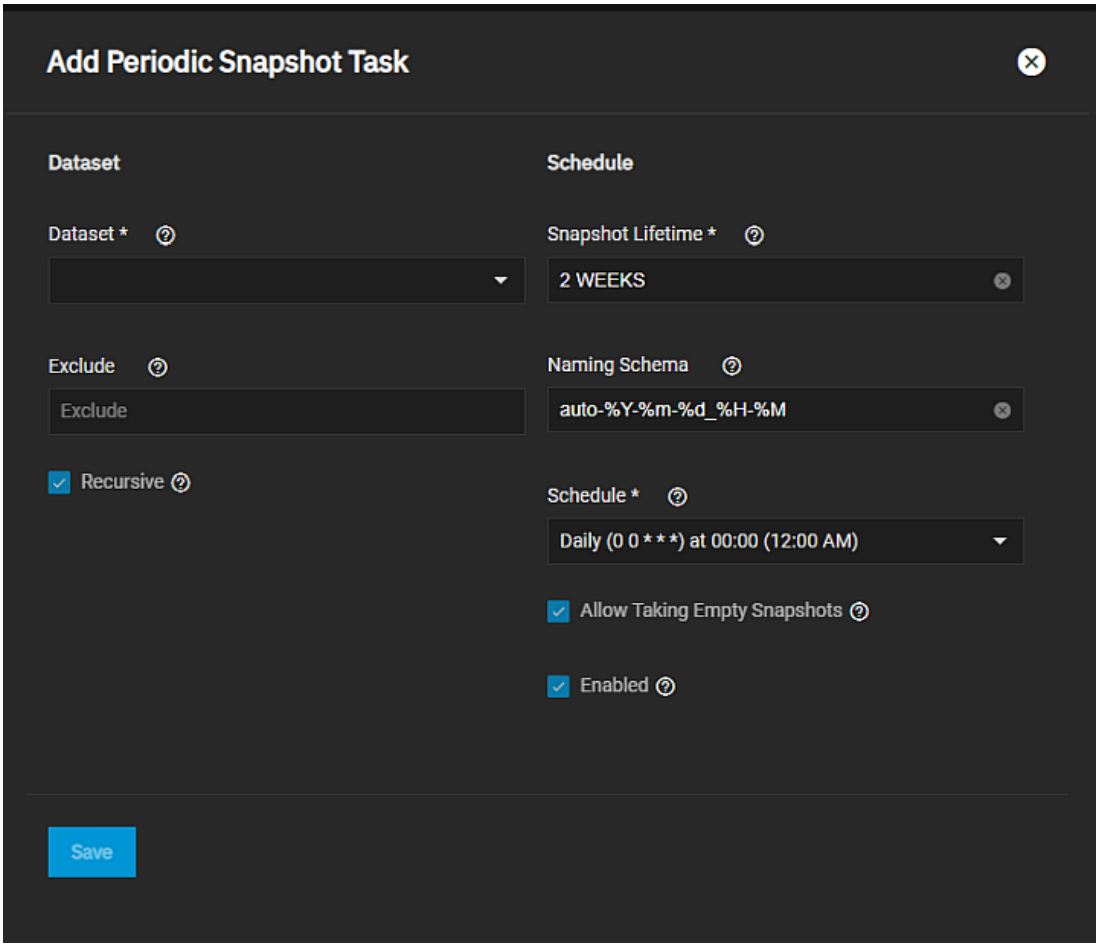
Add and Edit Periodic Snapshot Screens

The **Add Periodic Snapshot Task** and **Edit Periodic Snapshot Task** display some of the same settings.

Dataset Options

The **Dataset** setting options display on both the add and edit configuration screens.

Click Here for More Information



Setting	Description
Dataset	Select a pool, dataset, or zvol.
Exclude	Exclude specific child datasets from the snapshot. Use with recursive snapshots. List paths to any child datasets to exclude. Example: `pool1/dataset1/child1`. A recursive snapshot of pool1/dataset1 includes all child datasets except child1. Separate entries by pressing `Enter`.
Recursive	Select to take separate snapshots of the dataset and each of its child datasets. Leave checkbox clear to take a single snapshot only of the specified dataset without child datasets.

Schedule Options

These **Schedule** setting options display on both the add and edit configuration screens.

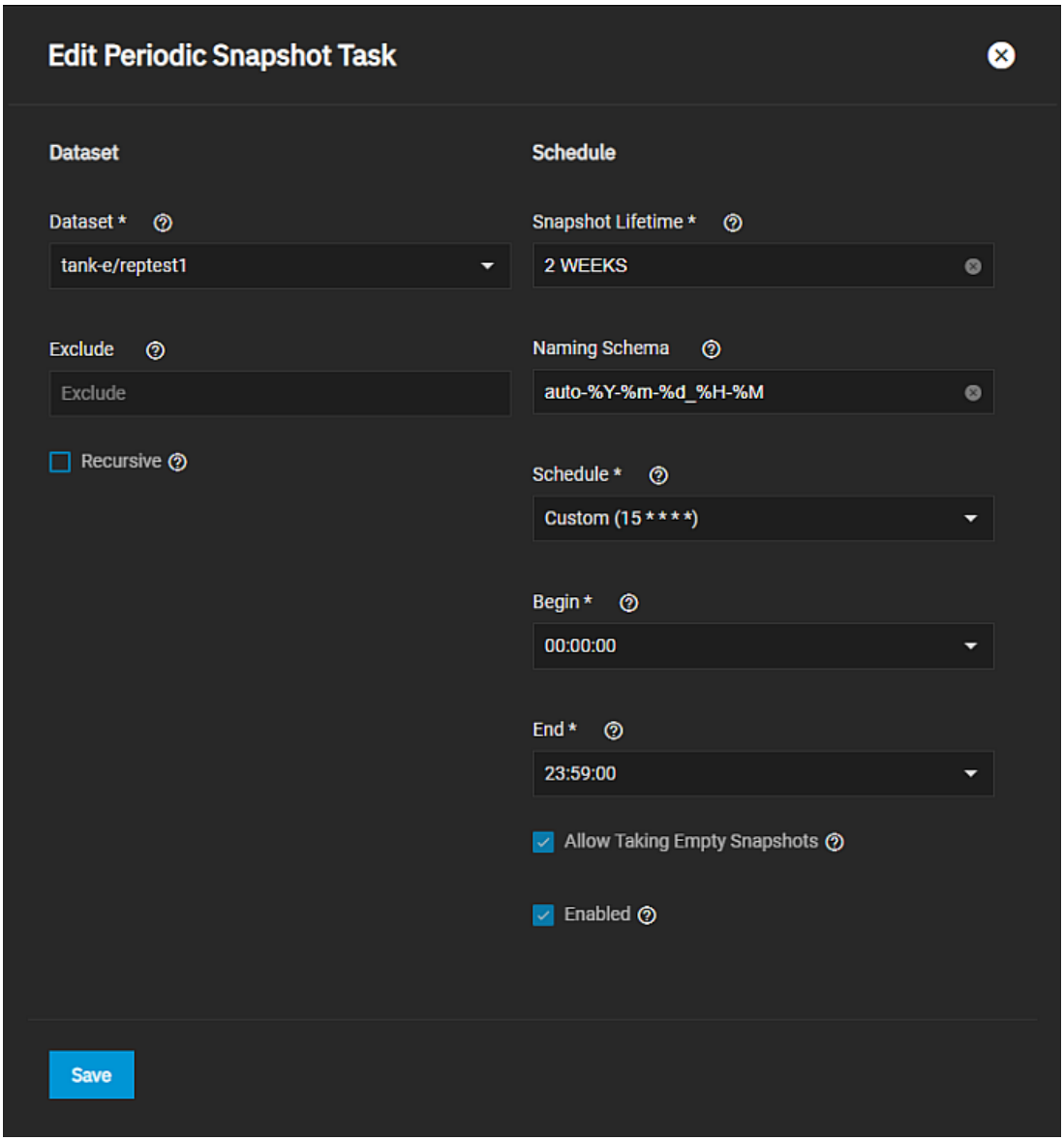
Click Here for More Information

Setting	Description
Snapshot Lifetime	Enter the length of time to retain the snapshot on this system using a numeric value and a single lowercase letter for units. Examples: *3h* is three hours, *1m* is one month, and *1y* is one year. Does not accept minute values. After the time expires, the snapshot is removed. Snapshots replicated to other systems are not affected.
Naming Schema	Snapshot name format string. The default is `auto-%Y-%m-%d_%H-%M`. Must include the strings `%Y`, `%m`, `%d`, `%H`, and `%M`, which are replaced with the four-digit year, month, day of month, hour, and minute as defined in strftime(3). For example, snapshots of *pool1* with a Naming Schema of `customsnap-%Y%m%d.%H%M` have names like *pool1@customsnap-20190315.0527*.
Schedule	Select a presets from the dropdown list. Select *Custom* to open the advanced scheduler.
Allow Taking Empty Snapshots	Select to Create dataset snapshots even when there are no changes to the dataset from the last snapshot. Recommended for long-term restore points, multiple snapshot tasks pointed at the same datasets, or compatibility with snapshot schedules or replications created in TrueNAS 11.2 and earlier. For example, you can set up a monthly snapshot schedule to take monthly snapshots and still have a daily snapshot task taking snapshots of any changes to the dataset.
Enabled	Select to activate this periodic snapshot schedule. To disable this task without deleting it, leave the checkbox cleared.

Schedule Options - Edit Periodic Snapshot Task

These **Schedule** setting options only display on the **Edit Periodic Snapshot Task** screen.

Click Here for More Information



Setting	Description
Begin	Enter the hour and minute when the system can begin taking snapshots.
End	Enter the hour and minute the system must stop creating snapshots. Snapshots already in progress continue until complete.

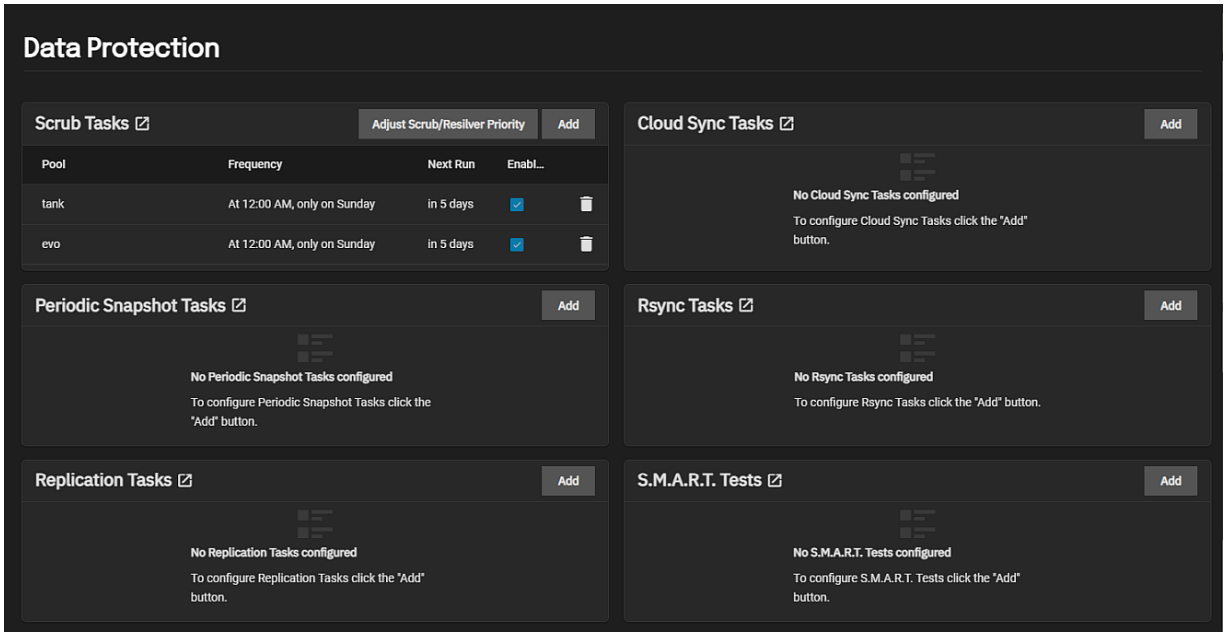
Related Content

- Snapshots Screens
- Creating VMWare Snapshots
- VMWare Snapshots Screen

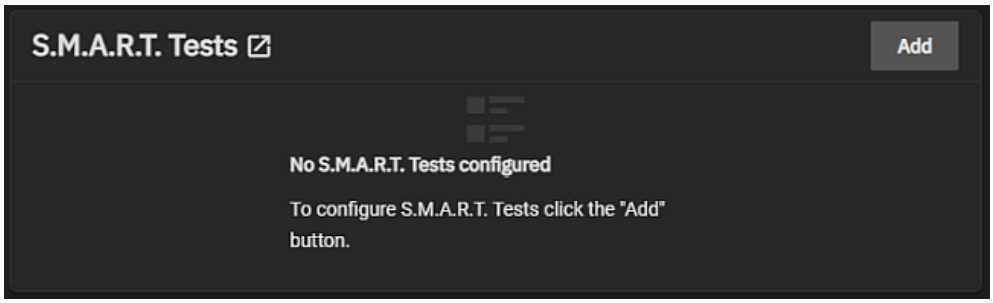
4.5.5 - S.M.A.R.T. Tests Screens

- Add and Edit SMART Test Screens

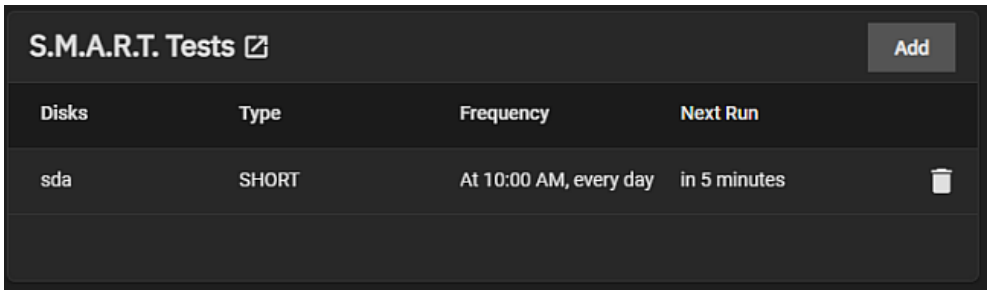
The **Data Protection** screen **S.M.A.R.T. Tests** widget displays the S.M.A.R.T. tests configured on the system and provides access to create or edit S.M.A.R.T. tests.



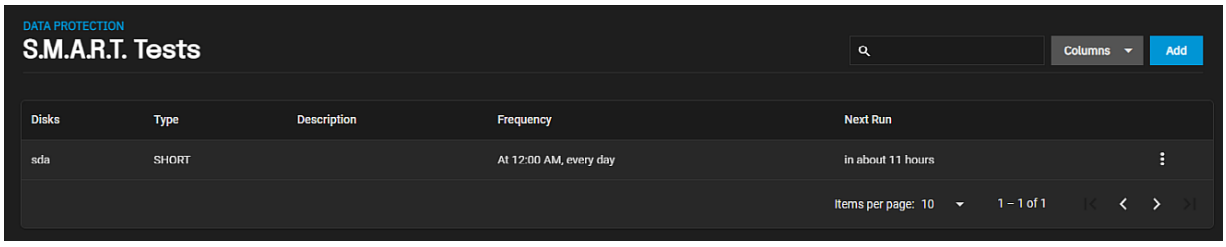
The **S.M.A.R.T. Tests** widget displays **No S.M.A.R.T. Tests configured** when no tests are configured on the system.



After adding tests, each becomes a link to open the **Edit S.M.A.R.T. Tests** screen.



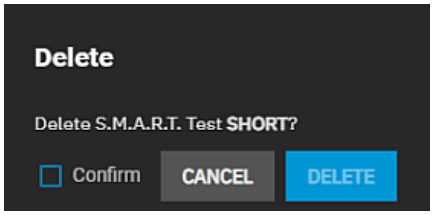
Click on **S.M.A.R.T. Tests** widget header to open the **S.M.A.R.T. Tests** list screen.



Use **Columns** to display options to customize the information displayed in the list screen. Options are **Unselect All**, **Description**, **Frequency**, **Next Run**, and **Reset to Defaults**.

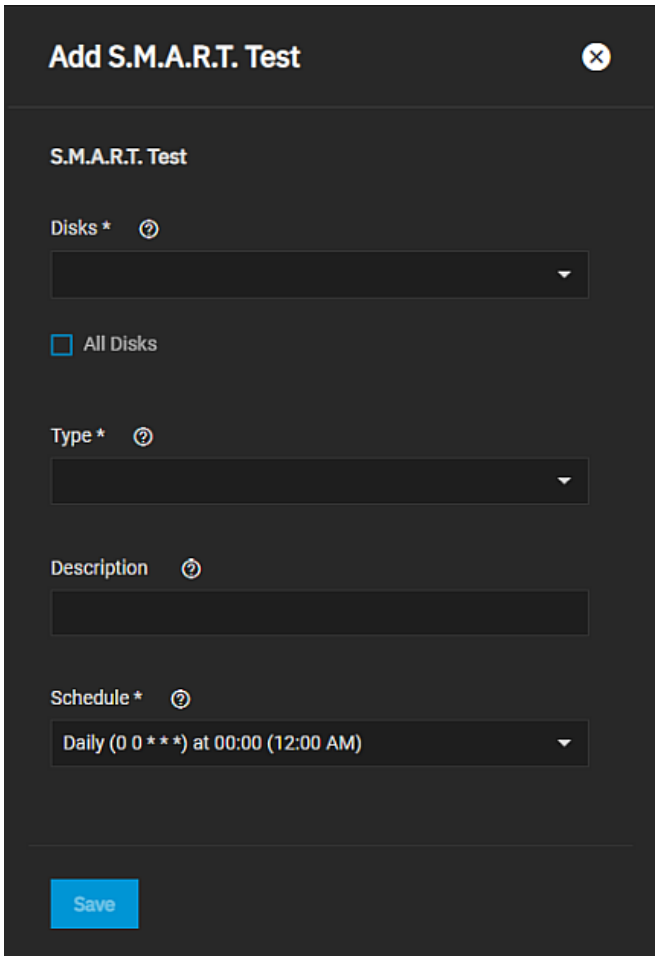
Add opens the **Add S.M.A.R.T. Test** configuration screen.

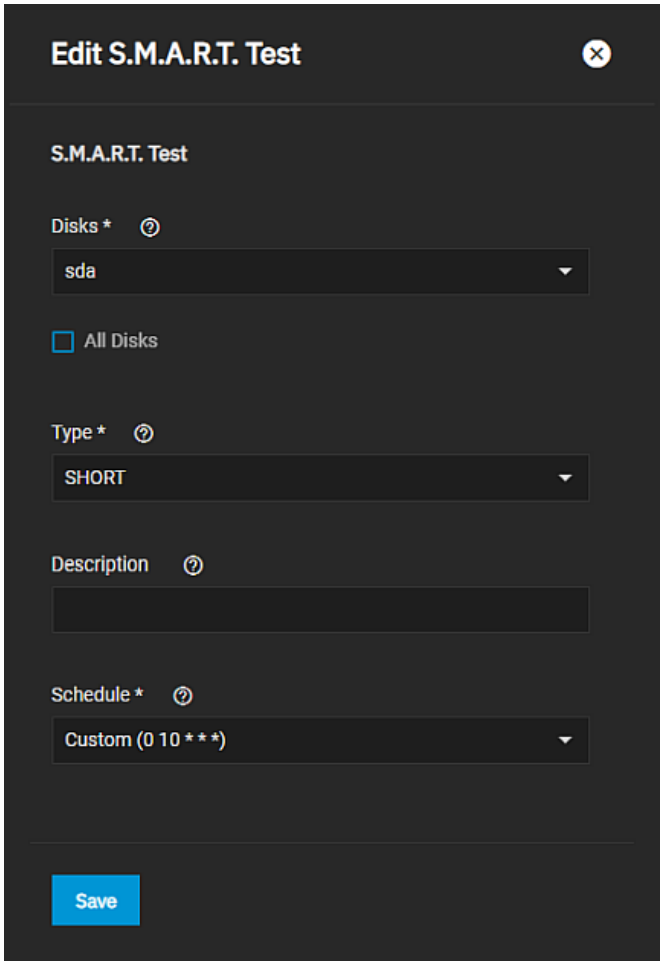
The ⋮ for each test has two options, **Edit** and **Delete**. **Edit** opens the **Edit S.M.A.R.T. Test** configuration screen and **Delete** opens a confirmation **Delete** dialog. The 🗑 delete icon on the widget also opens the **Delete** dialog for the selected S.M.A.R.T. test. Click **Confirm** to activate **Delete**.



Add and Edit SMART Test Screens

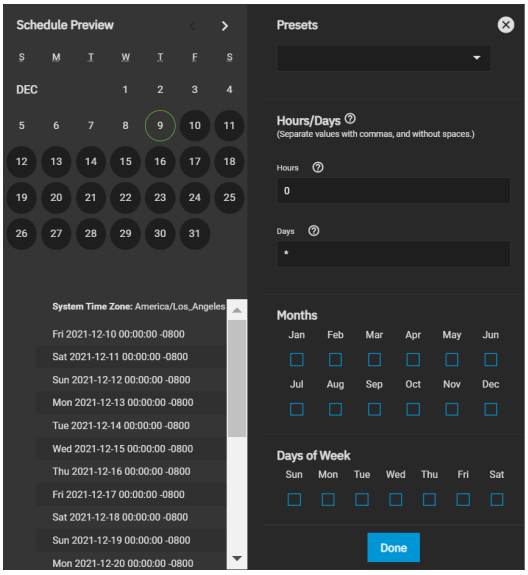
The **Add S.M.A.R.T. Test** and **Edit S.M.A.R.T. Test** configuration screens displays the same settings.





Name	Description
Disks	Select the disks to monitor from the dropdown list.
All Disks	Setect to monitor every disk on the system with S.M.A.R.T. enabled. Leave clear to choose individual disks on the **Disks** dropdown list to include in the test.
Type	Select the test type from the dropdown list. Options are **LONG**, **SHORT**, **CONVEYANCE** or **OFFLINE**. See smartctl(8) for descriptions of each type. Some types degrade performance or take disks offline.
Description	Enter information about the S.M.A.R.T. test.
Schedule	Select a preset test schedule from the dropdown list. Select **Custom** to open the advanced scheduler and define a new schedule for running the test.

Advanced Scheduler



Choosing a **Presets** option populatess in the rest of the fields. To customize a schedule, enter crontab values for the `Minutes/Hours/Days`.

These fields accept standard cron values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering *10* means that the job runs when the time is ten minutes past the hour.

An asterisk (*) means match all values.

You can set specific time ranges by entering hyphenated number values. For example, entering *30-35* in the **Minutes** field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.

You can also enter lists of values. Enter individual values separated by a comma (`,`). For example, entering *1,14* in the **Hours** field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).

A slash (`/`) designates a step value. For example, entering `*` in **Days** runs the task every day of the month. Entering `*/2` runs it every other day.

Combining the above examples creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

TrueNAS has an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days in addition to any listed days. For example, entering *1* in **Days** and setting *Wed* for **Days of Week** creates a schedule that starts a task on the first day of the month *and* every Wednesday of the month.

The **Schedule Preview** dipslays when the current settings mean the task runs.

Examples of CRON syntax

Syntax	Meaning	Examples
*	Every item.	* (minutes) = every minute of the hour. * (days) = every day.
*/N	Every N^{th} item.	*/15 (minutes) = every 15th minute of the hour. */3 (days) = every 3rd day. */3 (months) = every 3rd month.
Comma and hyphen/dash	Each stated item (comma) Each item in a range (hyphen/dash).	1,31 (minutes) = on the 1st and 31st minute of the hour. 1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour. mon-fri (days) = every Monday to Friday inclusive (every weekday). mar,jun,sep,dec (months) = every March, June, September, December.

You can specify days of the month or days of the week.

TrueNAS lets users create flexible schedules using the available options. The table below has some examples:

Desired schedule	Values to enter
3 times a day (at midnight, 08:00 and 16:00)	months=*; days=*; hours=0/8 or 0,8,16; minutes=0 (Meaning: every day of every month, when hours=0/8/16 and minutes=0)
Every Monday/Wednesday/Friday, at 8.30 pm	months=*; days=mon,wed,fri; hours=20; minutes=30
1st and 15th day of the month, during October to June, at 00:01 am	months=oct-dec,jan-jun; days=1,15; hours=0; minutes=1
Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday	Note that this requires two tasks to achieve: (1) months=*; days=mon-fri; hours=8-18; minutes=*/15 (2) months=*; days=mon-fri; hours=19; minutes=0 We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00.

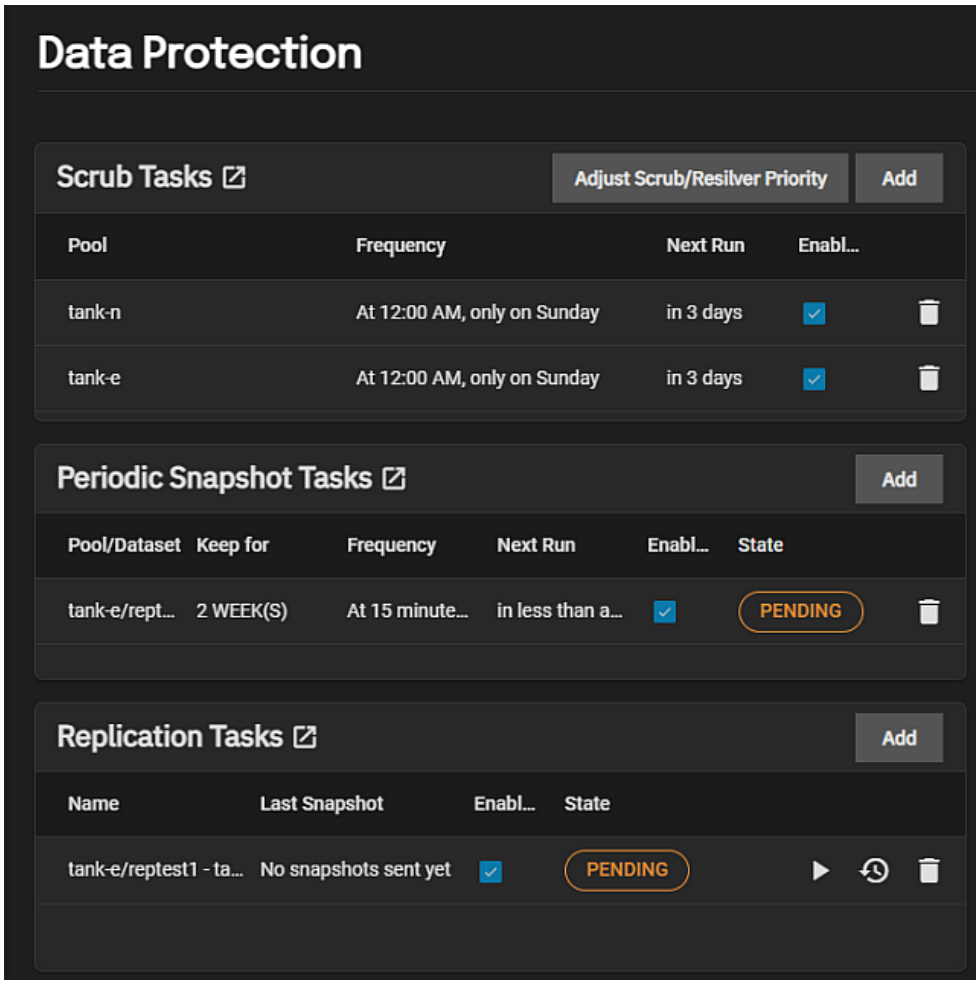
Related Content

- Configuring S.M.A.R.T. Service
- S.M.A.R.T. Service Screen
- Managing S.M.A.R.T. Tests

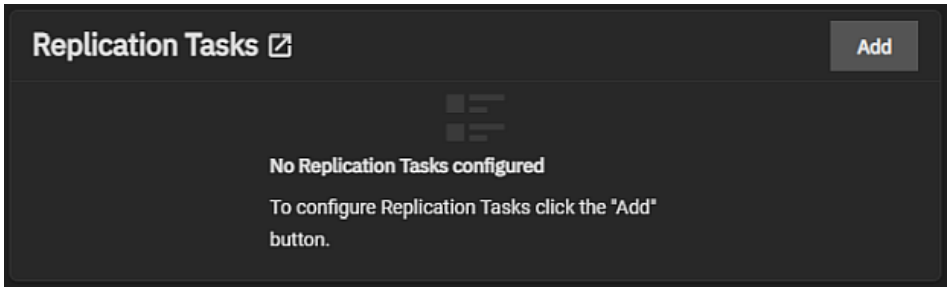
4.5.6 - Replication Task Screens

This article provides information on the replication screens, wizard, and settings to add or edit replication tasks.

The **Replication Task** widget on the **Data Protection** screen lists replication tasks configured on the TrueNAS system. Replication tasks work with periodic snapshot tasks to complete the replication.



The **Replication Tasks** widget displays **No Replication Tasks configured** before you add a task.



The **Replication Task** widget heading is a link that opens the **Data Protection > Replications Tasks** list view screen.

Add opens the **Add Replication Task** wizard.

Each replication task is a link to open the **Edit Replication Task** screen.

The widget displays the status of a task as **PENDING**, **RUNNING**, **SUCCESS** or **FAILED**. Click on the status to open a **Logs** window where you can see details on the task and download the log file.

The **Run Now** icon opens a dialog.

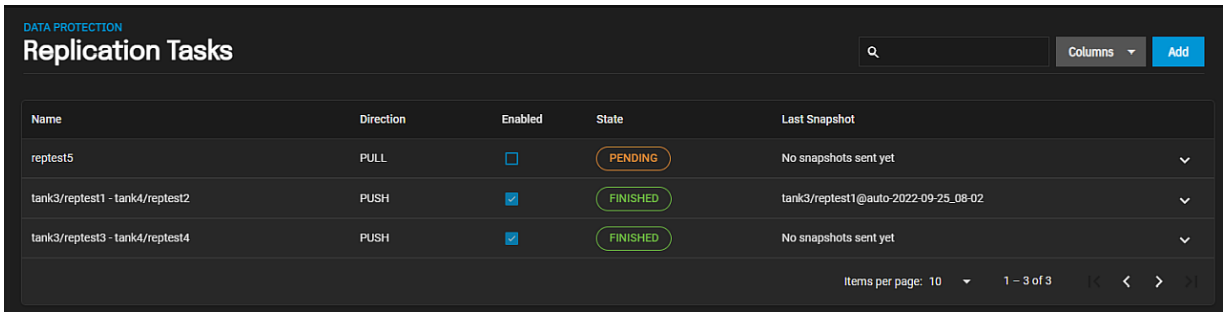
The **Restore** icon to opens the **Restore Replication Task** window.

The **Delete** icon opens a delete confirmation dialog.

Configure SSH in TrueNAS before creating a remote replication task. This ensures that new snapshots are regularly available for replication.

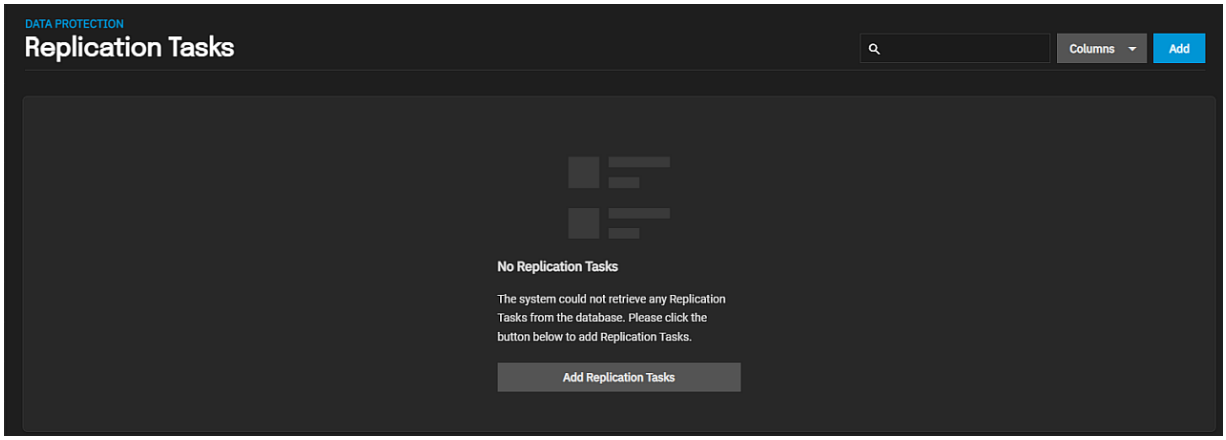
Replication Tasks List Screen

The **Data Protection > Replications Tasks** list view screen displays a the replication tasks configured on the system.



Columns displays a list of option to customize the list view to add or remove information to the table. Options are **Select All**, **Direction**, **Transport**, **SSH Connection**, **Source Dataset**, **Target Dataset**, **Recursive**, **Auto**, **Enabled**, **State**, **Last Snapshot**, and **Reset to Defaults**.

If no tasks are configured on the system, this screen displays **Not Replication Tasks** and the option to **Add Replication Tasks** that opens the **Add Replication Task** wizard.

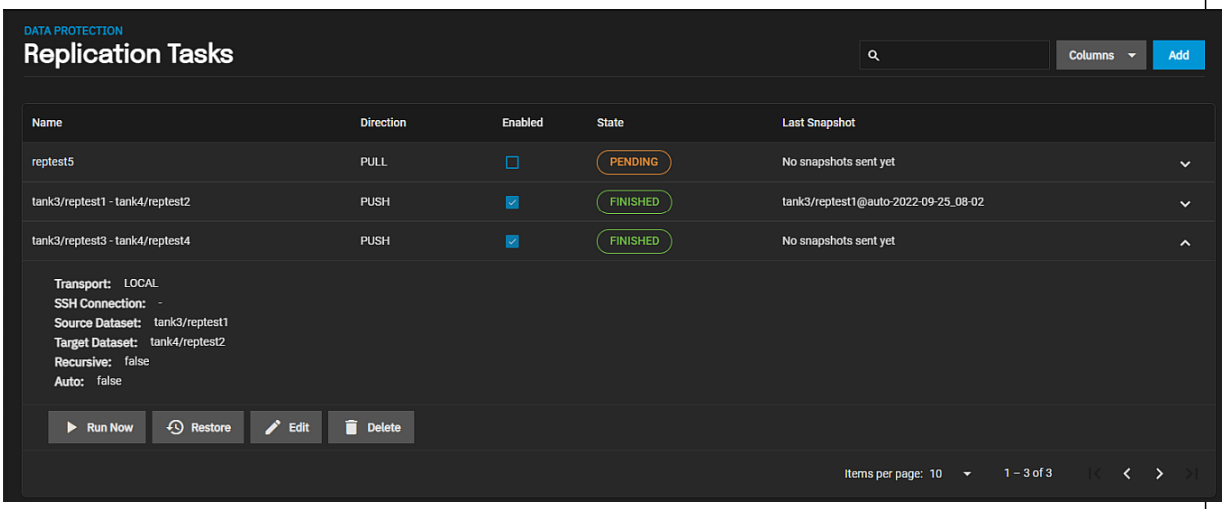


Click anywhere on a task listed to expand the task and show details about that task and options to run, restore, edit or delete that task.

Replication Task Details

The details view of each replication task shows the **Transport**, **SSH Connection**, **Source Dataset**, **Target Dataset**, **Recursive**, and **Auto** settings.

Click Here for More Information

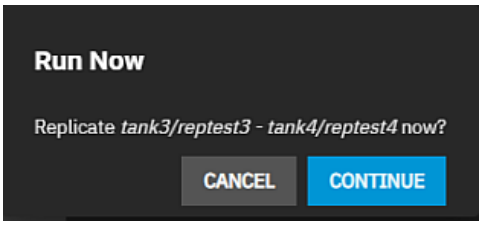


The **Edit** button opens the Edit Replication Task screen.

Run Now Option

The **Run Now** button opens a **Run Now** dialog.

Click Here for More Information

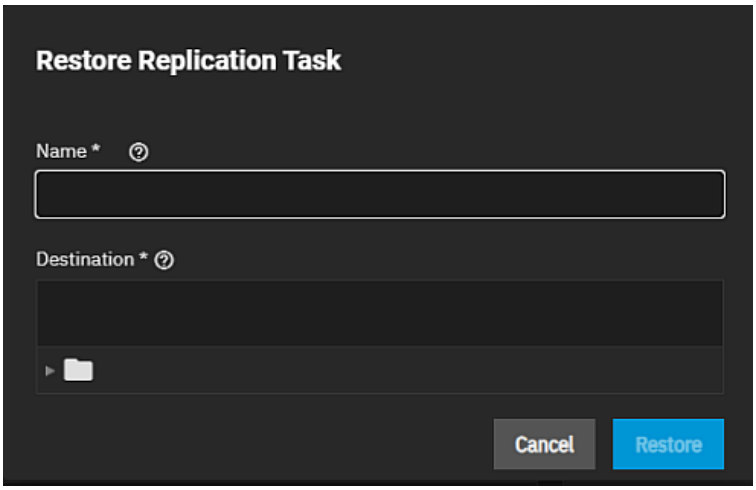


Click **CONTINUE** to start the replication task.

Restore Option

The **Restore** button opens the **Restore Replication Task** window.

Click Here for More Information

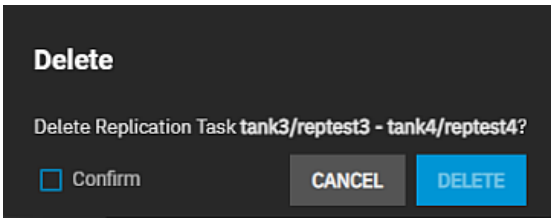


Enter a new name for the task and select the location to store the data, then click **Restore**. The system creates the new file and displays the task on both the widget and list screen with the **PENDING** status.

Delete Option

the **Delete** icon to open a delete confirmation dialog.

Click Here for More Information



Click **Confirm** to activate **Delete**.

Add Replication Task Options

There are two ways to add a replication task, the wizard and the advanced creation screen. These two methods share many settings. The section below describe each setting. Some settings shared by the wizard and the advanced creation screen display more related setting options. These separate sections document the shared settings to make finding the information easier:

- **Encryption**
- **Also include snapshots with the name**
- Schedule

Add, or if no replication task exist, **Add Replication Tasks** open the wizard.

Add Replication Task Wizard

The wizard has two screens.

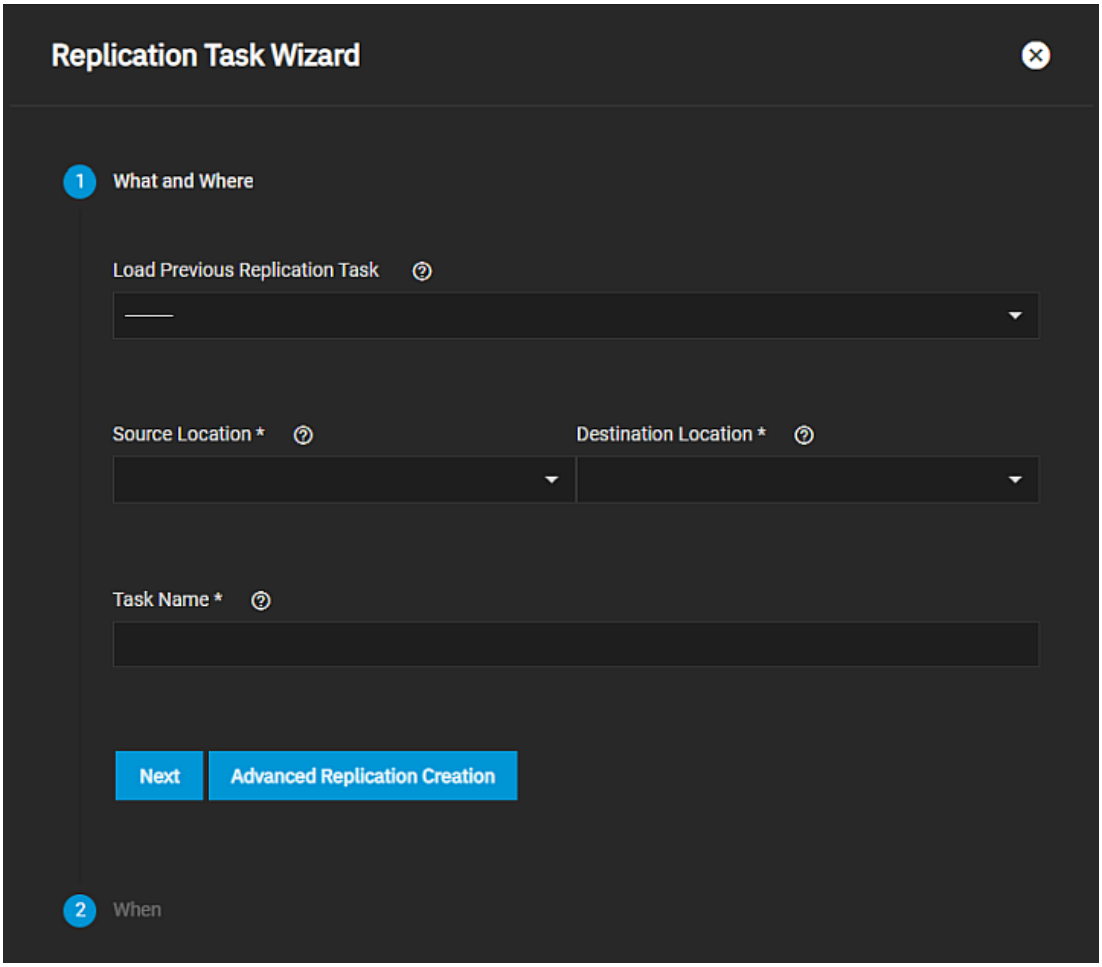
- **What and When** settings specify the task name, data source and destinations, the type of replication (local or remote), transport options (SSH connection).
- **When** setting specify when to run the task.

Advanced Replication Creation on the **What and When** screen opens the advanced replication creation screen.

What and When Wizard Screen

The **What and When** screen options specify a previous replication task, source and destination information and a name for the task. The **Encryption** option, used in both the replication task wizard and advanced creation screen, displays more options based on the selection made. The **Source Location** and **Destination Location** selections each display more options based on the selection made. The **SSH Connection** option displays for both source and destination if the location setting is **On a Different System**. The **Also include snapshots with the name** options display in both the wizard and advanced creation screen but different replicating snapshots settings related to naming result in them displaying.

Click Here for More Information

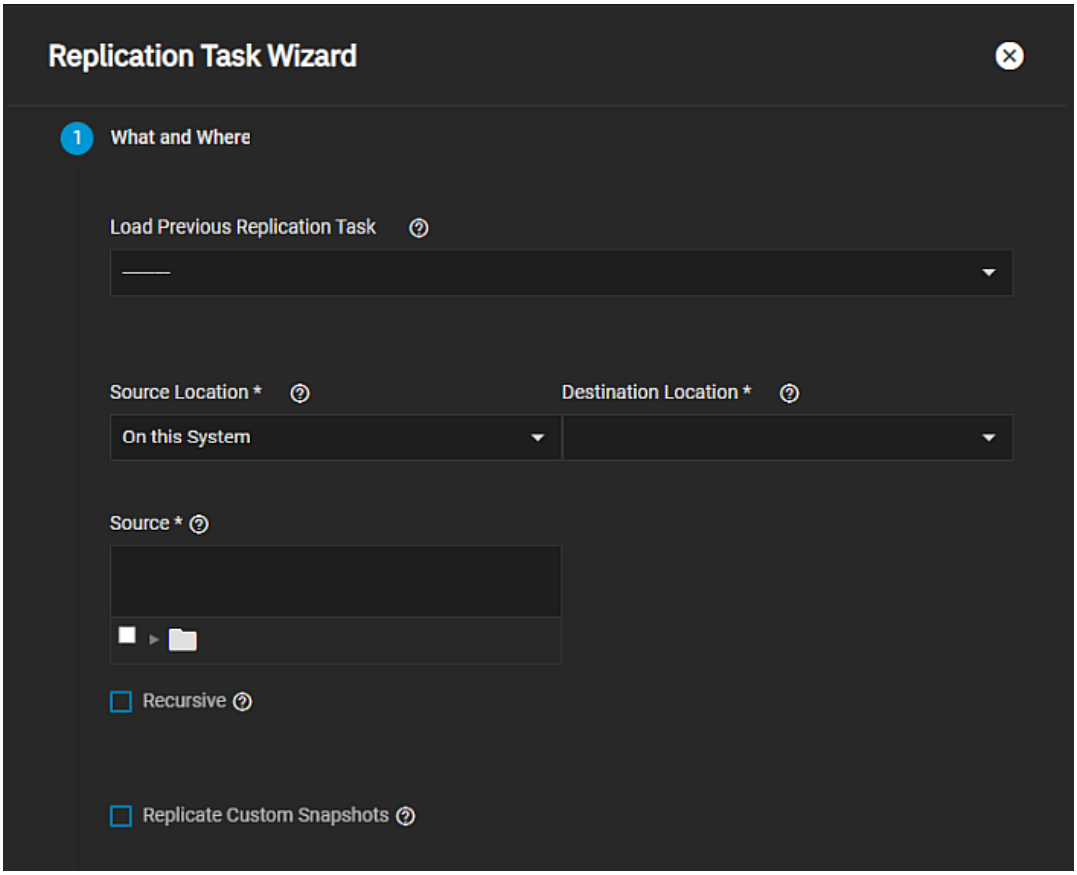


Setting	Description
Load Previous Replication Task	Use settings from a saved replication. Selecting an existing snapshot populates the **Source Location**, **Destination Locations**, **Source**, and **Destination** fields with the locations of the snapshots. It also populates the **Task Name** field at the bottom of the screen with a name that is a combination of the source-destination for the selected task.
Source Location	Select the storage location for the original replicated snapshots. Options are **On this System** or **On a Different System**. If set to **On a Different System**, the **Destination Location** changes to **On this System** and the **Destination** field displays the path to the snapshot location. For more information on these setting options see Source Location Setting Options.
Destination Location	Select the storage location for the replicated snapshots. ptions are **On this System** or **On a Different System**. If **Source Location** is set to **On a Different System**, the destination is automatically set to **On this System** and the **Destination** field displays.
Task Name	Enter the name of this replication configuration. Populates with the source-destination names from the task selected in **Load Previous Replication Tasks**.

Source Location Setting Options

Wizard screen settings change based on the option selected in **Source Location**. Selecting **On this system** displays the **Source** field with the option to browse to the dataset location, and the **Recursive** option. Selecting **On a Different System** displays the **Source** and the **Recursive** options. It changes the **Destination Location** to **On this System**. It displays the **Encryption** option under **Destination**, adds **SSH Connections** to the source setting options, adds snapshot naming options, and the **SSH Transfer Security** options.

Click Here for More Information

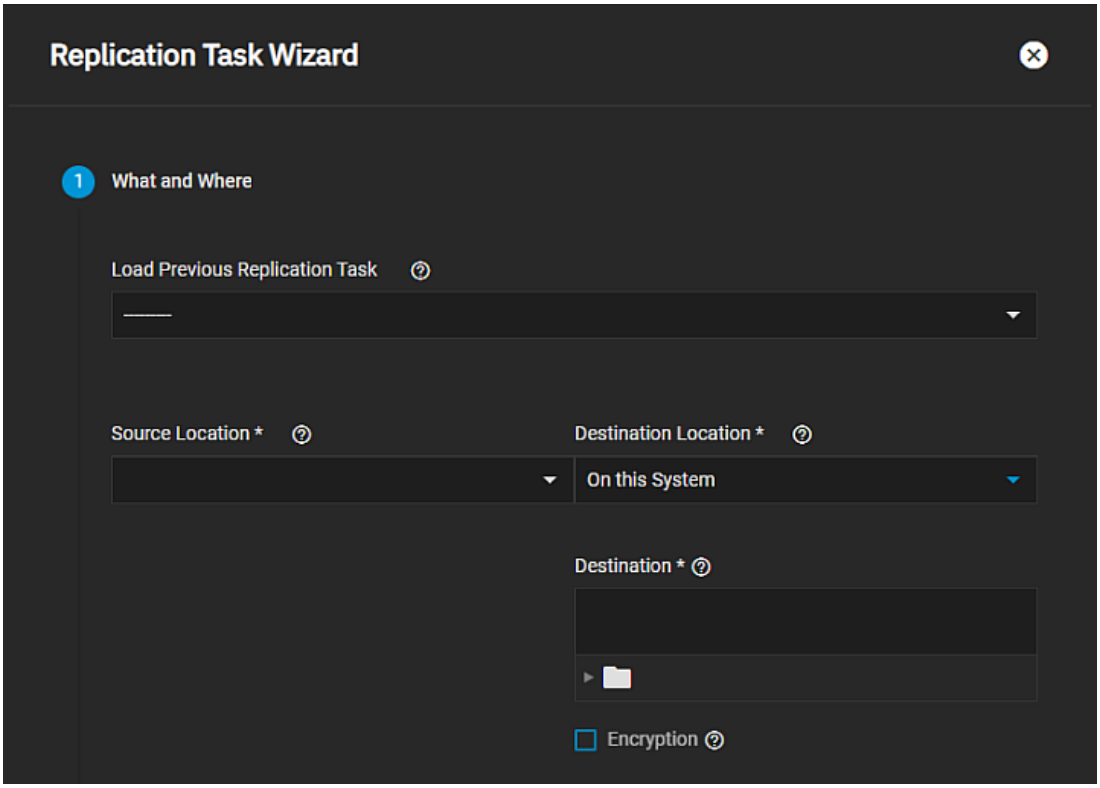


Setting	Description
Source	Required. Enter or use ▸ to the left of **/mnt** and at each dataset to expand the dataset tree to browse to the dataset location that has snapshots to replicate. Click on the or checkbox to select the checkbox to the left of the dataset. To enter multiple datasets, enter a comma (,) after each path in the **Source** field and then select another dataset. Click the ▾ at the **/mnt** to collapse the dataset tree.
SSH Connection	Select an existing SSH connection to a remote system or select **Create New** to open the **Create SSH Connection** window to configure a new SSH connection.
Recursive	Select to also replicate all snapshots contained within the selected source dataset snapshots. Leave clear to only replicate the selected dataset snapshots.
Replicate Custom Snapshots	Select to replicate snapshots that are not created by an automated snapshot task. Requires setting a naming schema for the custom snapshots. Displays the **Also include snapshots with the name** radio buttons and fields.

Destination Location Setting Options

Wizard screen settings change based on the option selected in **Destination Location** and in the **Source Location** fields. Selecting **On this System** in **Destination Location** displays the **Destination** field with the option to browse to the dataset location and **Encryption** option under **Destination**. Selecting **On a Different System** displays the **SSH Connections** and **SSH Transfer Security** options.

Click Here for More Information

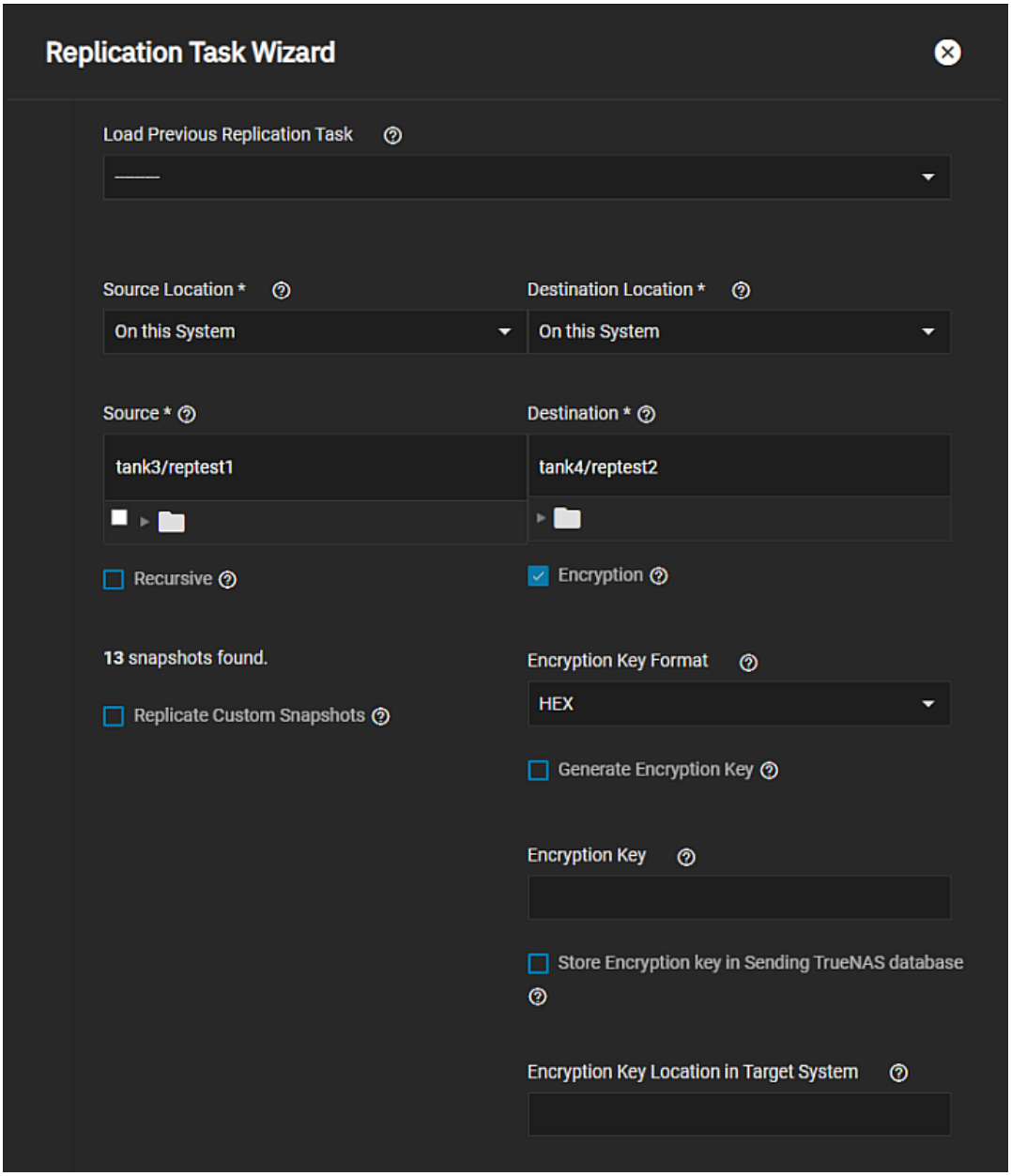


Setting	Description
Destination	Required. Enter or use ▸ to the left of **/mnt** and at each dataset to expand the dataset tree to browse to the dataset location that has snapshots to replicate. Click on the folder or checkbox to select the checkbox to the left of the dataset. To enter multiple datasets, enter a comma (,) after each path in the **Destination** field and then select another dataset. Click the ▾ at the **/mnt** to collapse the dataset tree.
Encryption	Select to use encryption when replicating data. For more information on all options see Encryption.

Encryption Setting Options

These setting options display on the **Add Replication Task** wizard **What and Where** screen after selecting the **Destination Location**, and on the advanced creation **Add Replication Task** screen in the **Destination** settings. After selecting **Encryption** more setting options display.

Click Here for More Information

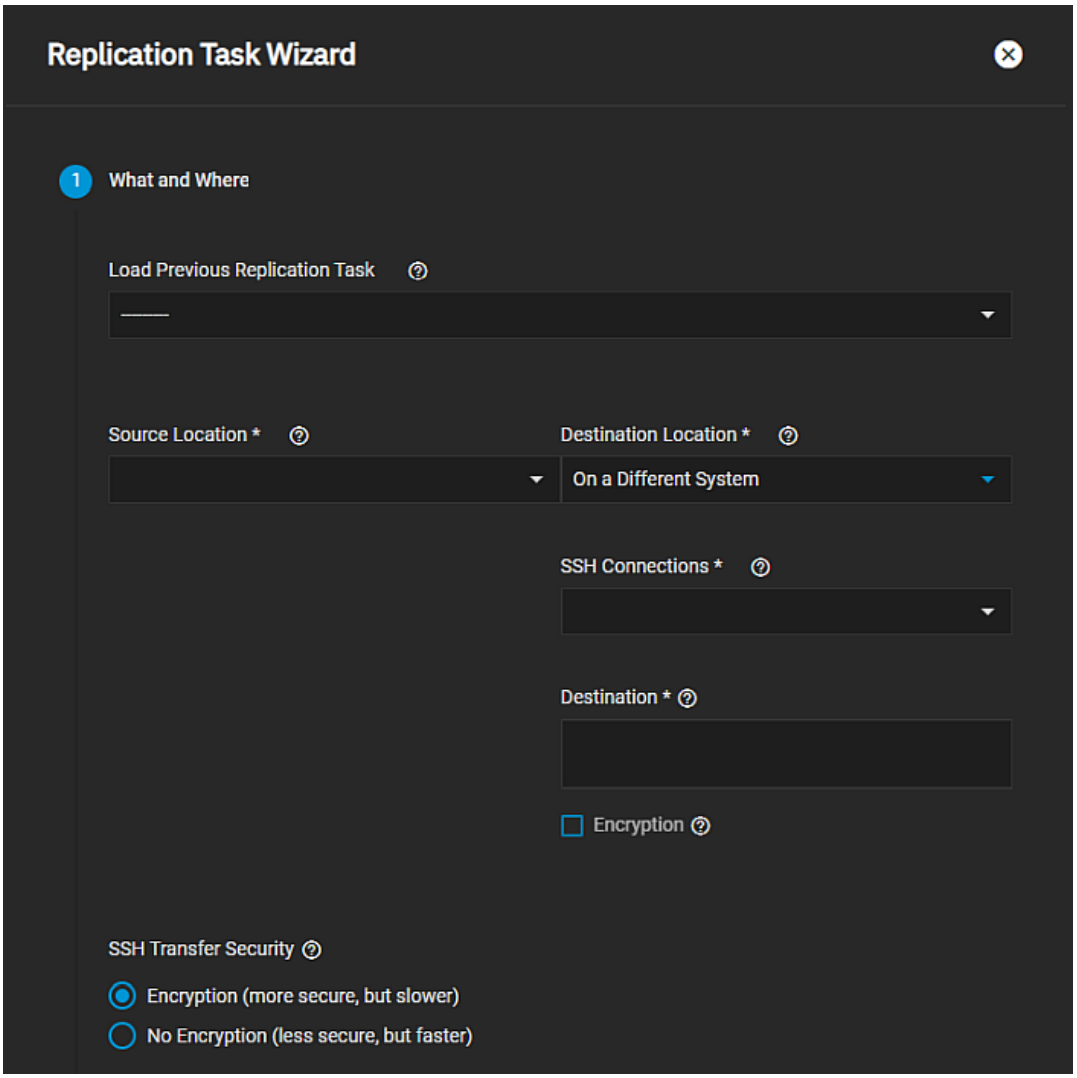


Setting	Description
Encryption	Select to use encryption when replicating data. Displays the **Encryption Key Format** and **Store Encryption key in Sending TrueNAS database** options.
Encryption Key Format	Select the encryption option from the dropdown list. **Hex** (base 16 numeral) or **Passphrase** (alphanumeric) style encryption key. Selecting **Hex** displays the **Generate Encryption Key** option. Selecting **Passphrase** displays the **Passphrase** option.
Generate Encryption Key	Displays after selecting **Hex** in **Encryption Key Format**. Displays selected by default. Clearing the checkbox displays the **Encryption Key** field.
Encryption Key	Displays after clearing the **Generate Encryption key** checkbox. Use to import a custom hex key.
Passphrase	Displays when **Encryption Key Format** is set to **Passphrase**. Enter the alphanumeric passphrase to use as an encryption key.
Store Encryption key in Sending TrueNAS database	Displays after selecting **Encryption**. Displays selected by default. Select to store the encryption key in the TrueNAS database. Clearing the checkbox displays the **Encryption Key Location in Target System** field.
Encryption Key Location in Target System	Displays after clearing the **Store Encryption key in sending TrueNAS database** checkbox. Enter a temporary location for the encryption key that decrypts replicated data.

SSH Settings

Setting the source anor destination location options to **On a Different System** displays more SSH setting options for whichever location has this setting.

Click Here for More Information

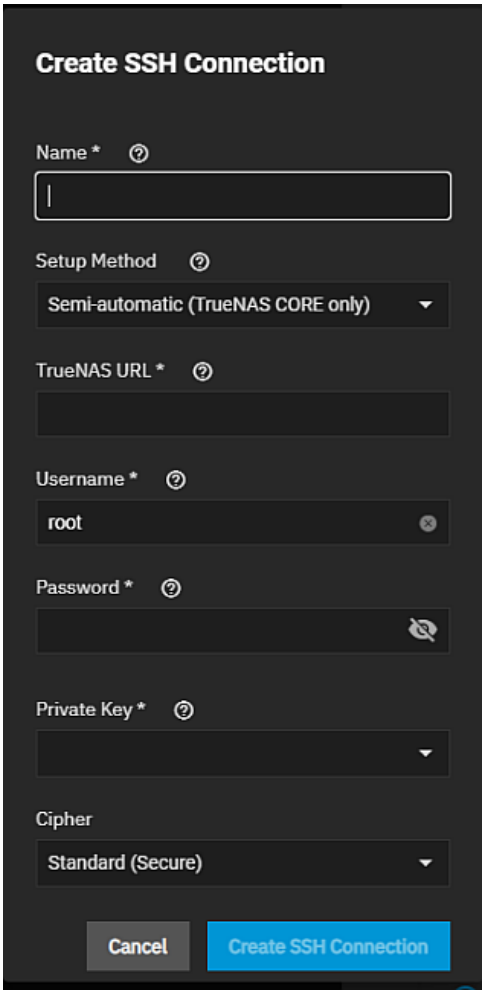


Setting	Description
SSH Connection	Select an existing SSH connection to a remote system or select **Create New** to open the **Create SSH Connection** window to configure a new SSH connection.
SSH Transfer Security	Provides the data transfer security. SSH authenticates the connection. Encryption is recommended but can be disabled for increased speed on more secure network. Select the radio button below to set the level of security for data transfer. Select **Encryption (more secure, but slower)** to use encryption over the SSL connection, or **No Encryption (less secure, but faster)** to not encrypt data transferred over the SSL connection.

Create SSH Connection

This window allows you to set up a new SSH connection for the remote system.

Click Here for More Information



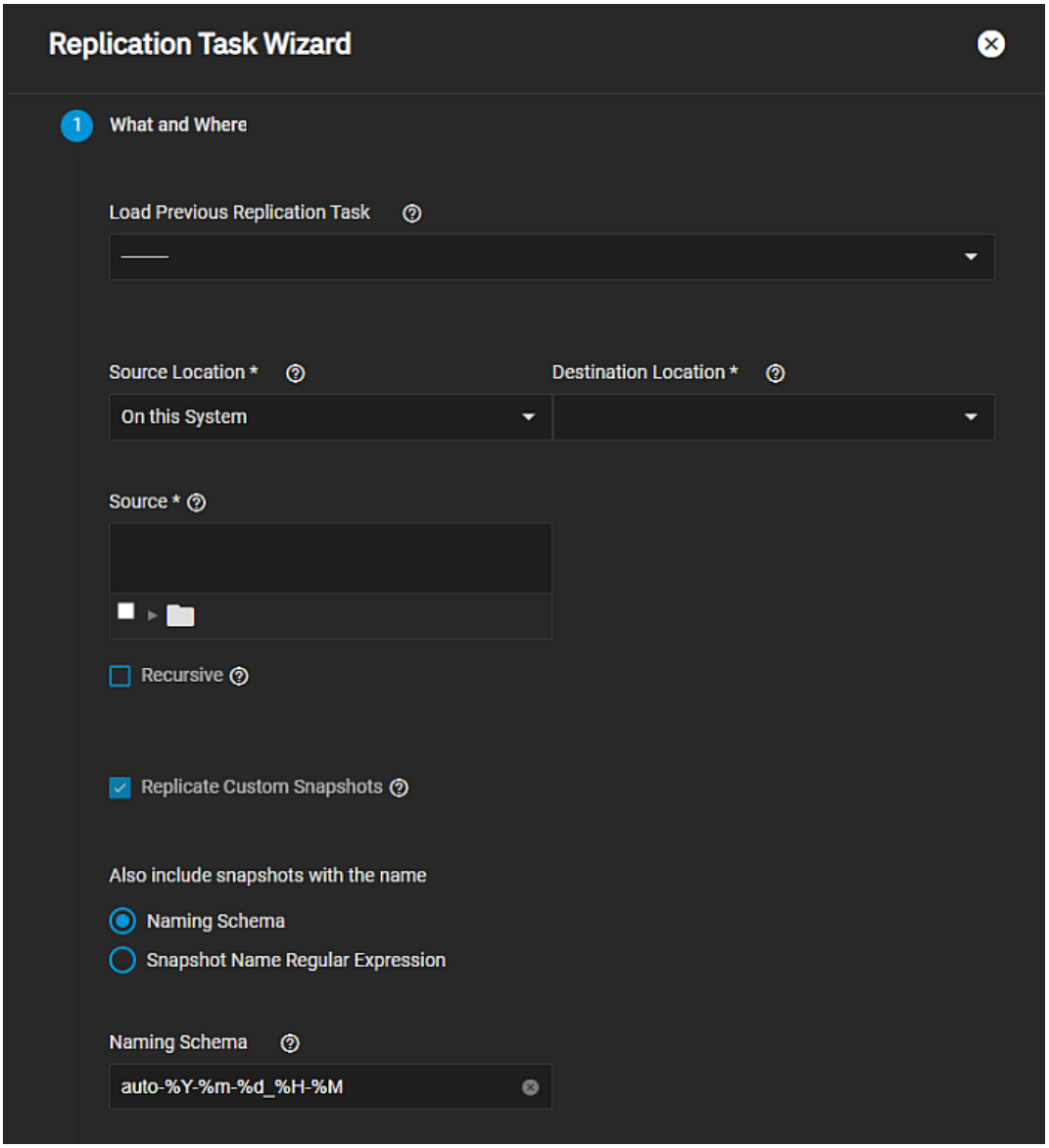
Setting	Description
Name	Required. Enter a unique name for this SSH connection.
Setup Method	Select how to configure the connection from the dropdown list. Select **Manual** to configure authentication on the remote system. This option can include copying SSH keys and modifying the root user account on that system. Select **Semi-Automatic** when configuring an SSH connection with a remote TrueNAS system. This method uses the URL and login credentials of the remote system to connect with and exchange SSH keys. This option only works when the other system is a TrueNAS system.
TrueNAS URL	Ener the host name or IP address of the remote system. A valid URL scheme is required. For example, *https://10.235.12.20*.
Username	Enter the user name for logging into the remote system.
Password	Enter the password for logging into the remote system.
Private Key	Select a saved SSH keypair or select **Generate New** to create a new keypair and use it for this connection.
Cipher	Select a cipher from the dropdown list.

Snapshot Naming Options

Also include snapshots with the name radio button options set the snapshot naming pattern as schema or regular expression. This field display on both the wizard and advanced creation screens but the radio buttons have different names. See Various Snapshot Options below for details.

Click Here for More Information

Also include snapshots with the name radio button options display after selecting **On a Different System** as either the **Source Location** or **Destination Location** or after selecting **Replicate Custom Snapshots**.



Setting	Description
Naming Schema	Select to use naming schema and display the **Naming Schema** field below the radio buttons.
Snapshot Name Regular Expression	Select to use regular expression and display the **Snapshot Name Regular Expression** field below the radio buttons.
Naming Schema	Enter the pattern of naming custom snapshots to replicate. Enter the name and strftime(3) %Y, %m, %d, %H, and %M strings that match the snapshots to include in the replication. Separate entries by pressing `Enter`. The number of snapshots matching the patterns display on the screen.
Snapshot Name Regular Expression	Enter the regular expressions snapshot should match. Using this option replicates all snapshots which names match specified regular expression. This option slows regular performance on the systems with large number of snapshots as the process reads snapshots metadata in order to determine snapshots creation order.

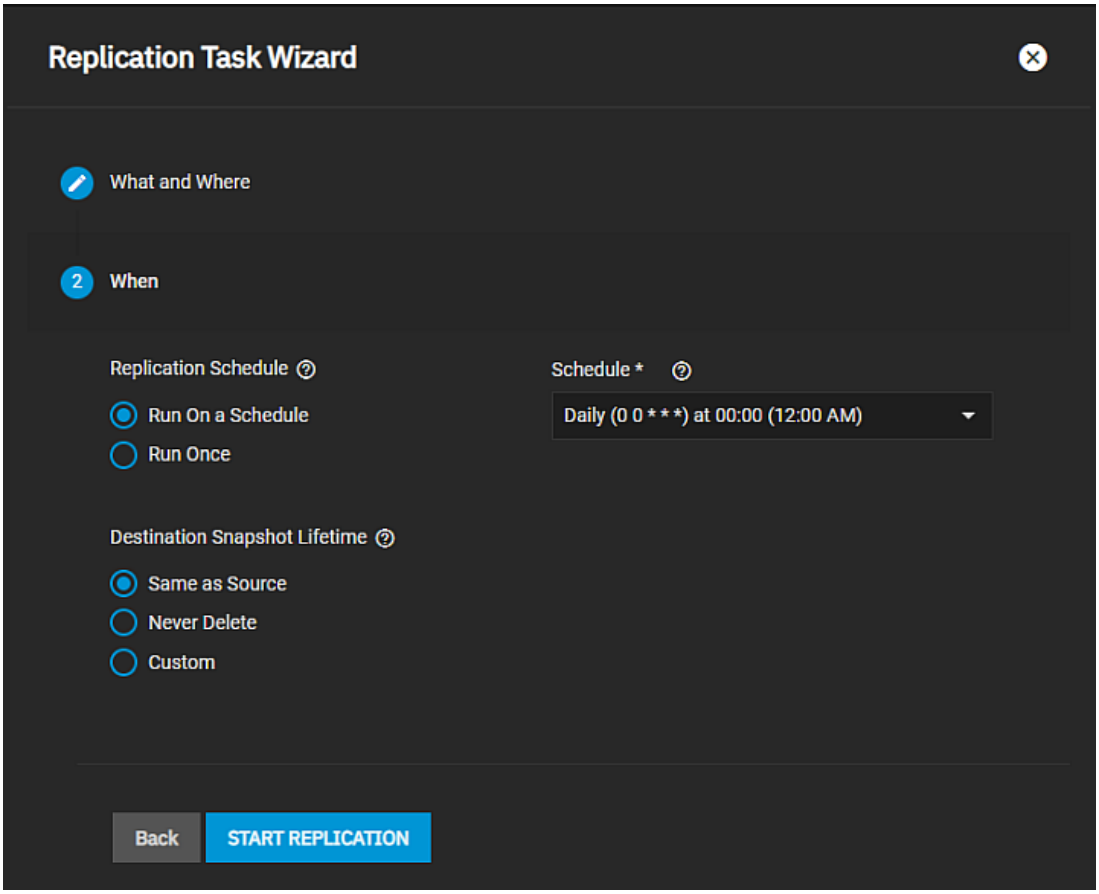
When Wizard Screen

The **Replication Schedule** and **Destination Snapshot Lifetime** radio button selection changes the setting options displayed.

Replication Schedule Options

The **Replication Schedule** radio button options set the task to run on the schedule defined in **Schedule** or one time. Each radio button changes options displayed on the screen.

Click Here for More Information

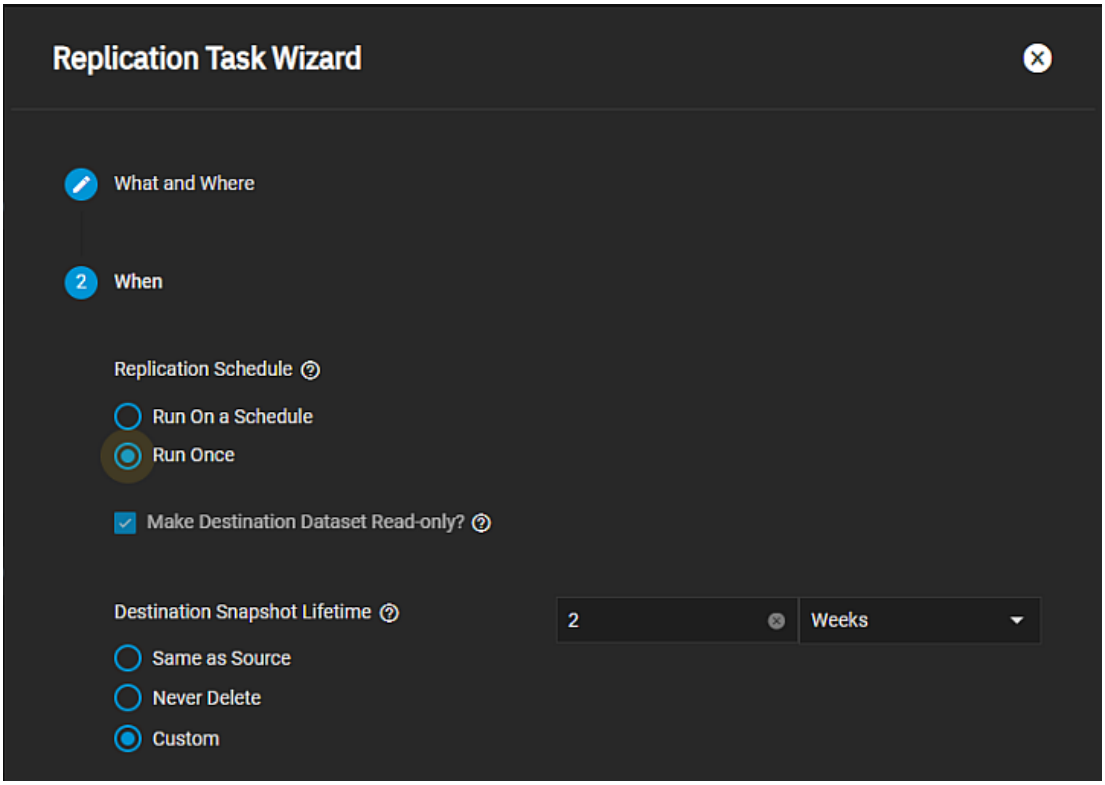


Setting	Description
Run On a Schedule	Displays the **Schedule** option where you select a preset time or can select **Custom** to use the advanced scheduler.
Run Once	Runs the replication task after you click **Start Replication**. Displays the **Make Destination Dataset Read-only?** option. Removes the **Schedule** option.
Schedule	Displays after selecting the **Run On a Schedule** radio button. Select a preset time or can select **Custom** to use the advanced scheduler.
Make Destination Dataset Read-only?	Select to change the destination dataset to be read-only. To continue using the default or existing dataset read permissions, leave this checkbox cleared.

Destination Snapshot Lifetime Options

The radio buttons change settings displayed. Select when replicated snapshots are deleted from the destination system. Options are the three radio buttons below. Select **Same as Source** to use the configured snapshot Lifetime value from the source dataset periodic snapshot task. Select **Never Delete** to never delete snapshots from the destination system. Select **Custom** to define how long the snapshot remains on the destination system.

Click Here for More Information



Setting	Description
Same as Source	Select to use the configured snapshot Lifetime value from the source dataset periodic snapshot task.
Never Delete	Select to never delete snapshots from the destination system.
Custom	Select to define how long the snapshot remains on the destination system. Displays the number of and measure of time fields to set the schedule.
Number of	Enter a numeric value to work with the measure of time selection to set the custom lifetime of the snapshot.
Measure of time	Select the option for **Hours**, **Days**, **Weeks**, **Months**, or **Years** to work with the number of field to set the custom lifetime of the snapshot.

Advanced Replication Creation changes to the advanced **Add Replication Task** configuration screen. Click before or after adding values to any setting on the **What and When** wizard screen.

Advanced Replication Creation Screen

Advanced Replication Creation on the **What and Where** wizard screen opens the **Add Replication Task** advanced creation screen. Click this button before or after adding settings on the wizard screen.

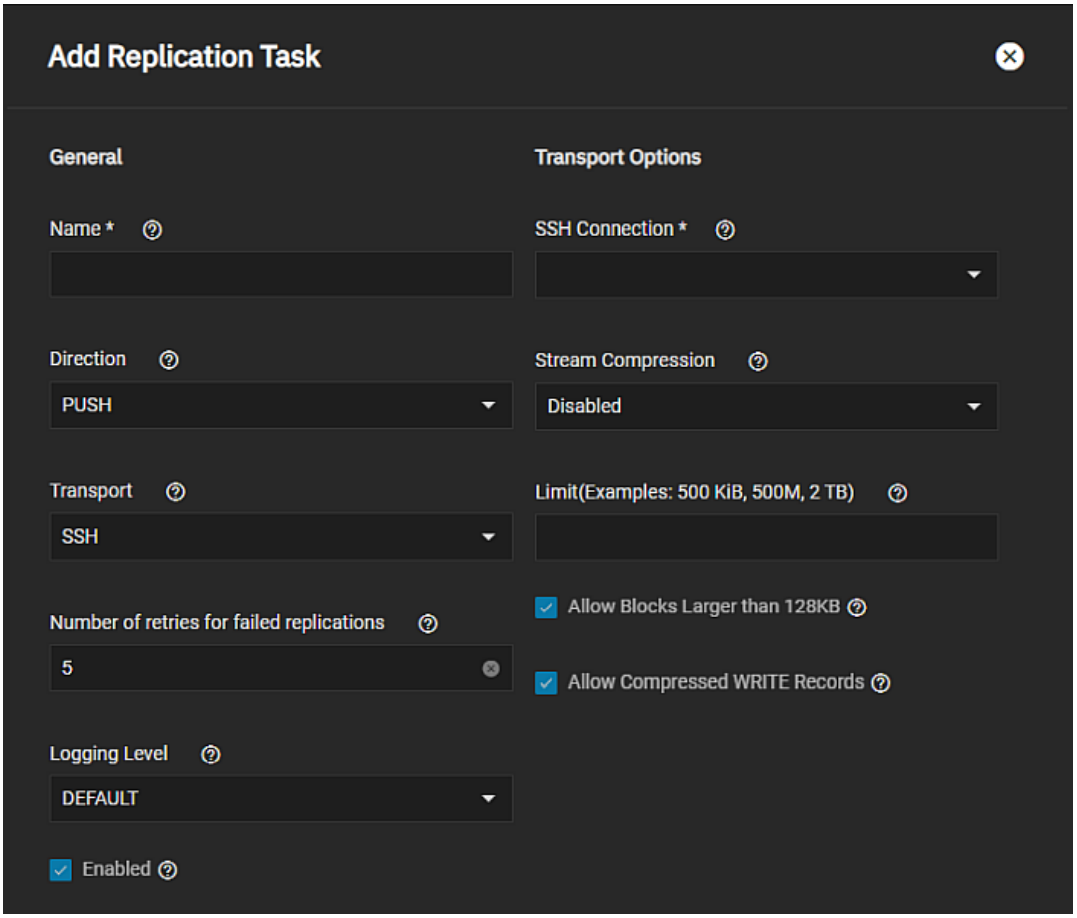
> Before adding a replication task, create an SSH connection to use when connecting to a remote system. The **Add Replication Task** wizard provides the option to configure a new SSH connection when adding the task but the advanced creation screen does not.
>
> If adding a local replication task, where you replicate data from one pool and dataset to different pool and dataset on the same system, the SSH connection is not a required element.

General and Transport Options Settings

The settings in **General** and **Transport Options** specify the name of the task, the direction of the data transfer, the transport connection type and method settings for each type. The **Transport** setting changes options displayed in the **Transport Options** area (**SSH** is the default setting).

Click Here for More Information

All three **Transport** field options share the two settings displayed for **Local**, and the **SSH Connection** field displays for both the **SSH** and **SSH+NETCAT** transport selections.



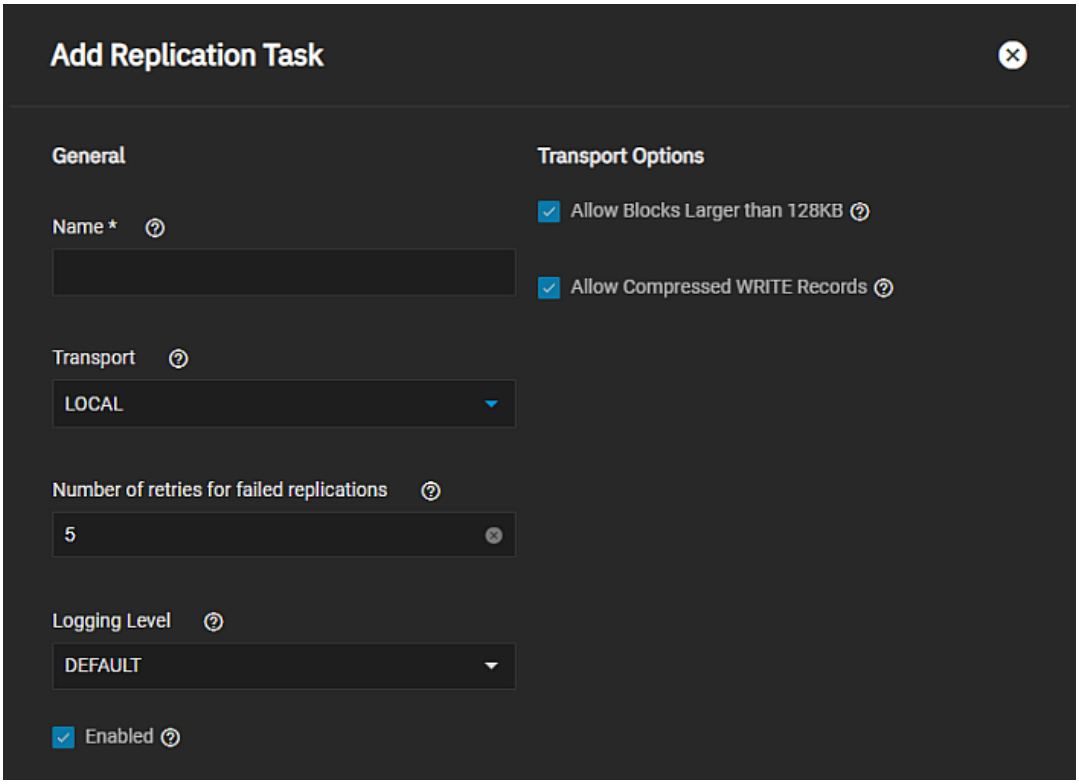
General Settings

Setting	Description
Name	Required. Enter a descriptive name for the replication.
Direction	Select the direction for the replication from the dropdown list. **Push** sends snapshots to a destination system. **Pull** connect to a remote system and retrieves snapshots matching the value specified in **Naming Schema**.
Transport	Select the method of connecting to a remote system for exchanging data from the dropdown list. **SSH** is the supported by most systems. It requires a previously created SSH connection on the system. **SSH+NETCAT** uses SSH to establish a connection to the destination system, then uses py-libzfs to send an unencrypted data stream for higher transfer speeds. This only works when replicating to a FreeNSAS, TrueNAS, or other system with py-libzfs installed. **LOCAL** efficiently replicates snapshots to another dataset on the same system without using the network. **Legacy** uses the legacy replication engine from FreeNAS 11.2 and earlier.
Number of retries for failed replications	Enter the number of times the replication is attempted before stopping and marking the task as failed.
Logging Level	Select the level of message verbosity in the replication task log from the dropdown list. Options are **Default**, **Debug**, **Info**, **Warning**, and **Error**.
Enabled	Select to enable the replication schedule.

Transport Options Settings - Local Transport Option

These setting display for all three **Transport** options.

Click Here for More Information



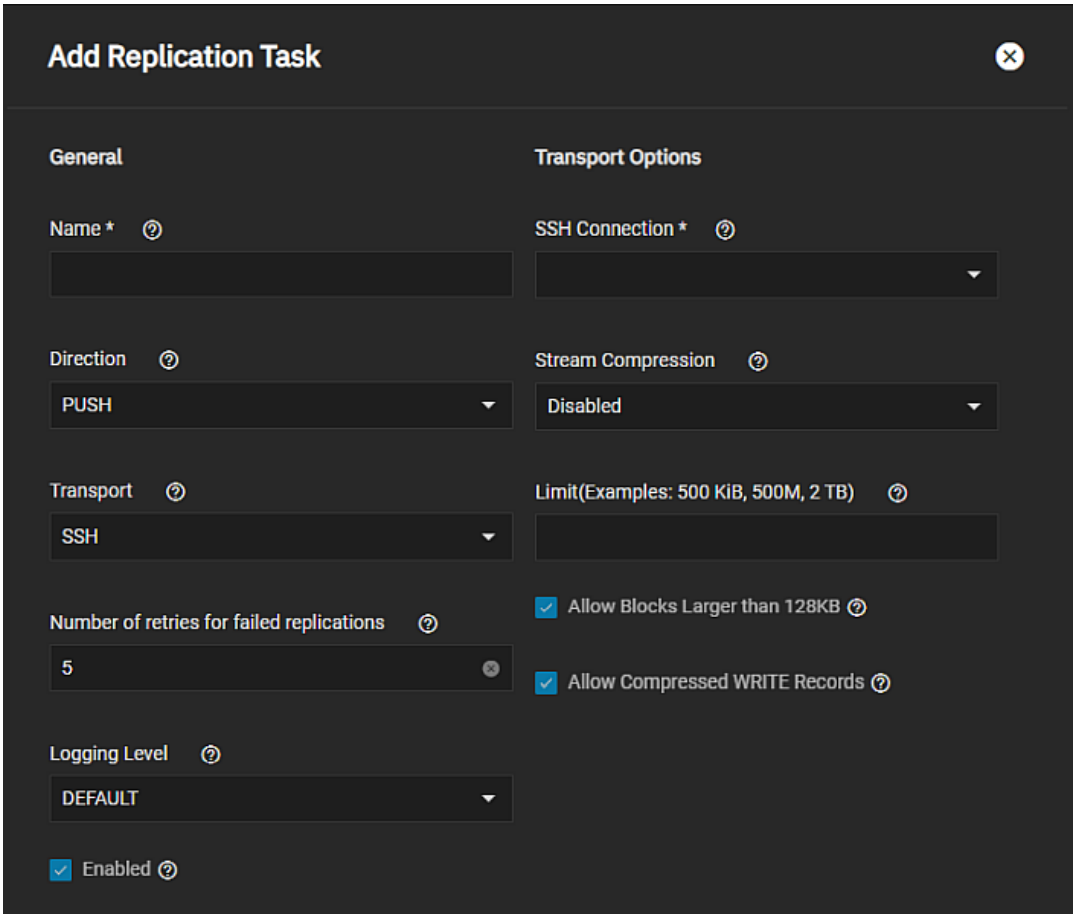
These settings display for all three **Transport** options.

Setting	Description
Allow Blocks Larger than 128KB	Select to allow this replication to send large data blocks. The destination system must also support large blocks. This setting cannot be changed after it is enabled and the replication task is created. For more details, see zfs(8).
Allow Compressed WRITE Records	Use compressed WRITE records to make the stream more efficient. The destination system must also support compressed WRITE records. See zfs(8).

Transport Options Settings - SSH Transport Option

These setting options display in addition to the two options displayed when **Transport** is set to **Local**.

Click Here for More Information

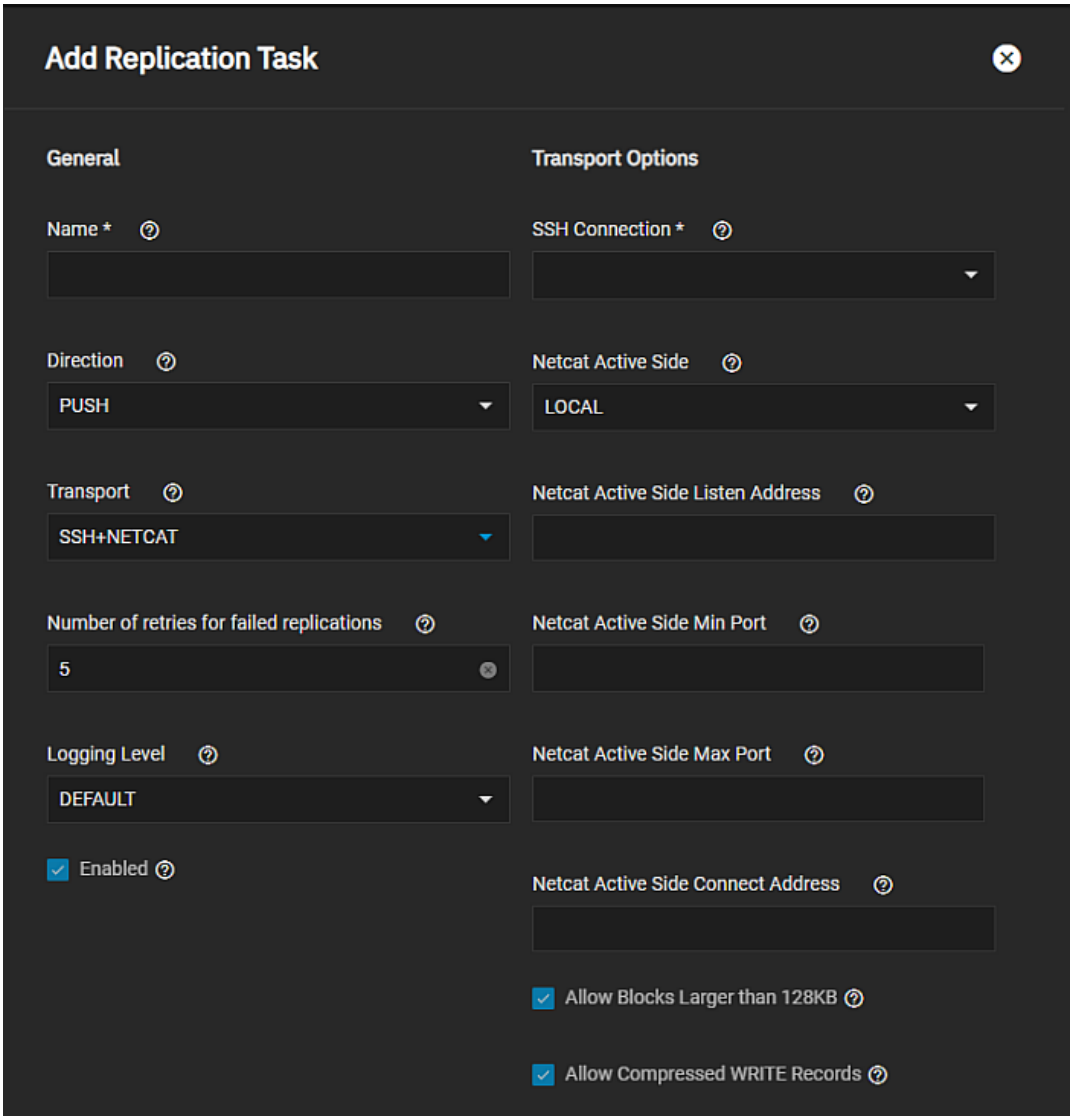


Setting	Description
SSH Connection	Select a connection created and saved in **Credentials > Backup Credentials > SSH Connections**. If a connection does not display on the the dropdown list, exit the task creation screen. Open **Credentials > Backup Credentials** and add an SSH connection.
Stream Compression	Select a compression algorithm from the dropdown list to reduce the size of the data being replicated. Only appears when SSH is chosen for **Transport** type.
Limit (Examples: 500 KiB, 500M, 2 TB)	Enter the number of bytes per second to limit replication speed to this number of bytes per second.

Transport Options Settings - SSH+NETCAT Transport Option

These setting options display in addition to the two options displayed when **Transport** is set to **Local**.

Click Here for More Information



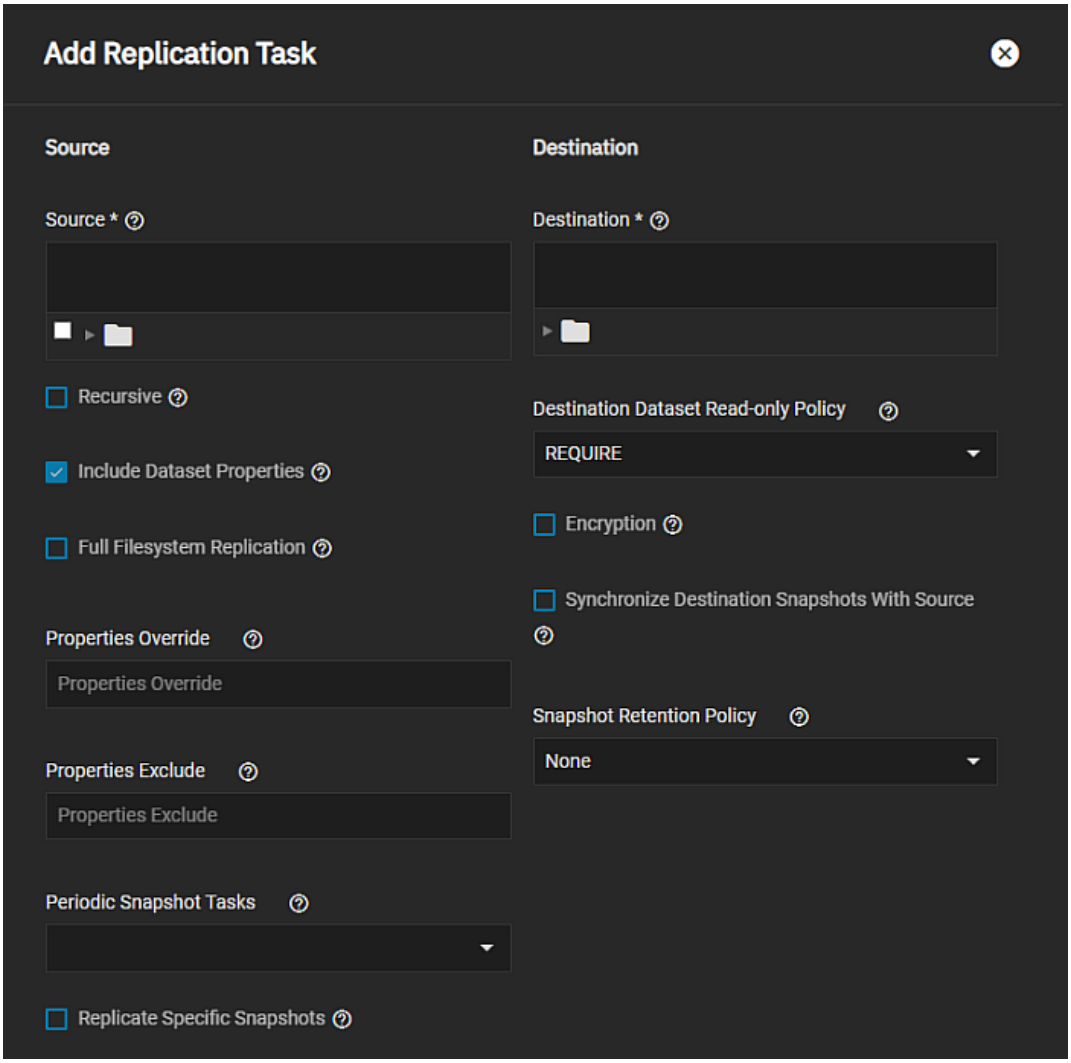
Setting	Description
SSH Connection	Select a connection created and saved in **Credentials > Backup Credentials > SSH Connections**. If a connection does not display on the the dropdown list, exit the task creation screen. Open **Credentials > Backup Credentials** and add an SSH connection.
Netcat Active Side	Select the option for the system that opens ports from the dropdown list. Options are **Local** or **Remote**. Establishing a connection requires that one of the connection systems has open TCP ports. Consult your IT department to determine which systems are allowed to open ports.
Netcat Active Side Listen Address	Enter the IP address on which the connection Active Side listens. Defaults to 0.0.0.0.
Netcat Active Side Min Port	Enter the lowest port number of the active side listen address that is open to connections.
Netcat Active Side Max Port	Enter the highest port number of the active side listen address that is open to connections. The first available port between the minimum and maximum is used.
Netcat Active Side Connection Address	enter the host name or IP address used to connect to the active side system. When the active side is **Local**, this defaults to the **SSL_CLIENT** environment variable. When the active side is **Remote**, this defaults to the SSH connection host name.

Advanced Source Options

The settings in **Source** specify the location of files you push or pull in the replication task, and the properties applied to the replicated data.

Click Here for More Information

The Source setting options change based on selections made in **Recursive** and **Replicate Specific Snapshots** and each display additional setting options.



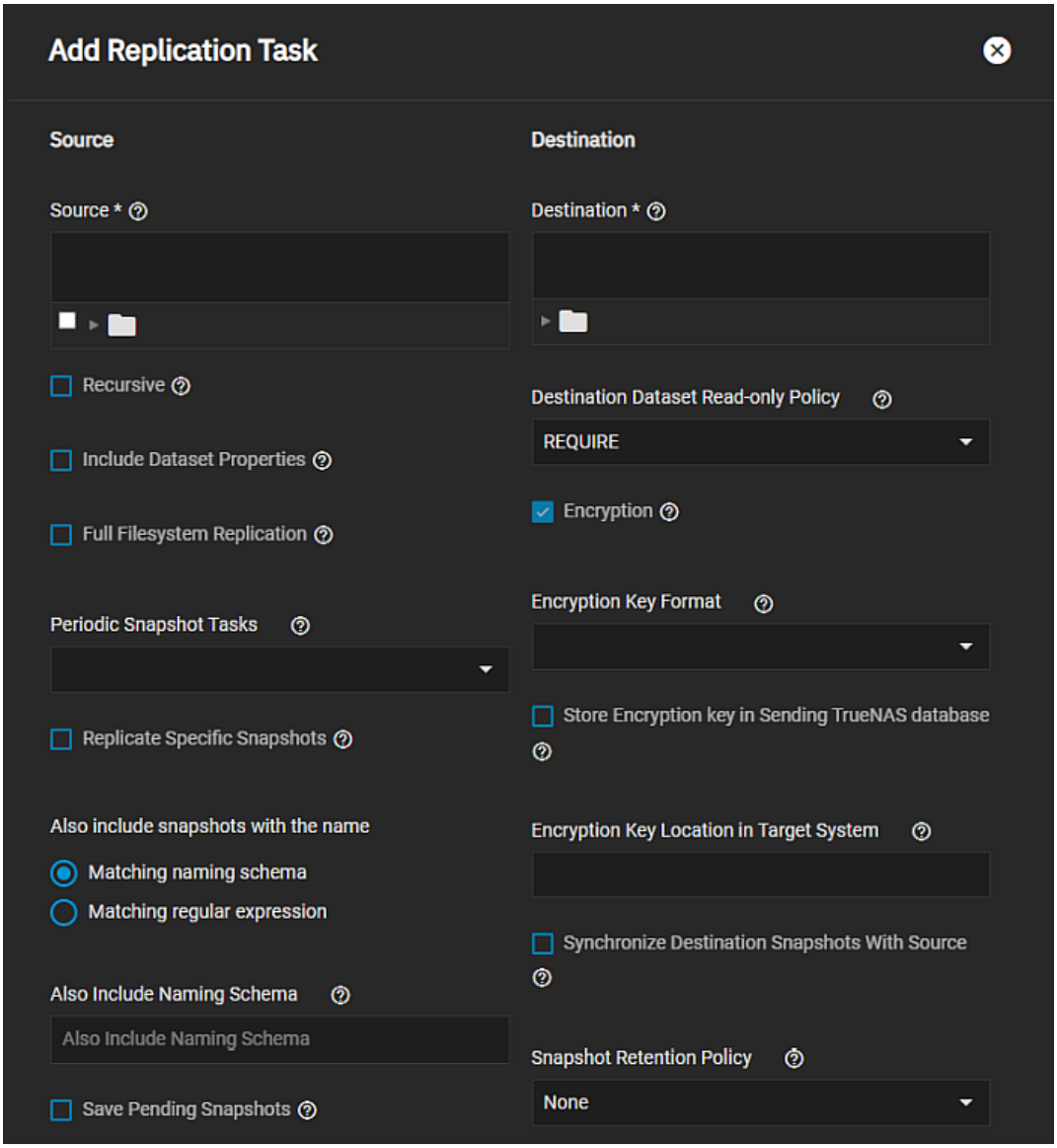
Setting	Description
Source	Required. Enter or use ▸ to the left of 🖿 **/mnt** and at each dataset to expand the dataset tree to browse to the dataset location that has snapshots to replicate. Click on the 🖿 or checkbox to select the checkbox to the left of the dataset. To enter multiple datasets, enter a comma (,) after each path in the **Source** field and then select another dataset. Click the ▾ at the 🖿 **/mnt** to collapse the dataset tree.
Recursive	Select to replicate all child dataset snapshots. When selected, **Exclude Child Datasets** displays.
Exclude Child Datasets	Displays after selecting **Recursive**. Enter the specific child dataset snapshots from the replication. Separate each entry by pressing `Enter`.
Include Dataset Properties	Select to include dataset properties with the replicated snapshots.
Full Filesystem Replication	Select to completely replicate the selected dataset. The target dataset gets all the properties of the source dataset, child datasets, clones and snapshots that match the specified naming schema. Hides the **Recursive** and **Include Dataset Properties** options.
Properties Override	Enter properties to replace existing dataset properties with in the replicated files.
Properties Exclude	Enter any existing dataset properties to remove from the replicated files.

Advanced Destination Options

The settings in **Destination** specify the location of files you push or pull in the replication task, and the properties applied to the replicated data.

Click Here for More Information ↧

The destination setting options change based on selections made in **Encryption** and **Snapshot Retention Policy** which display additional setting options.



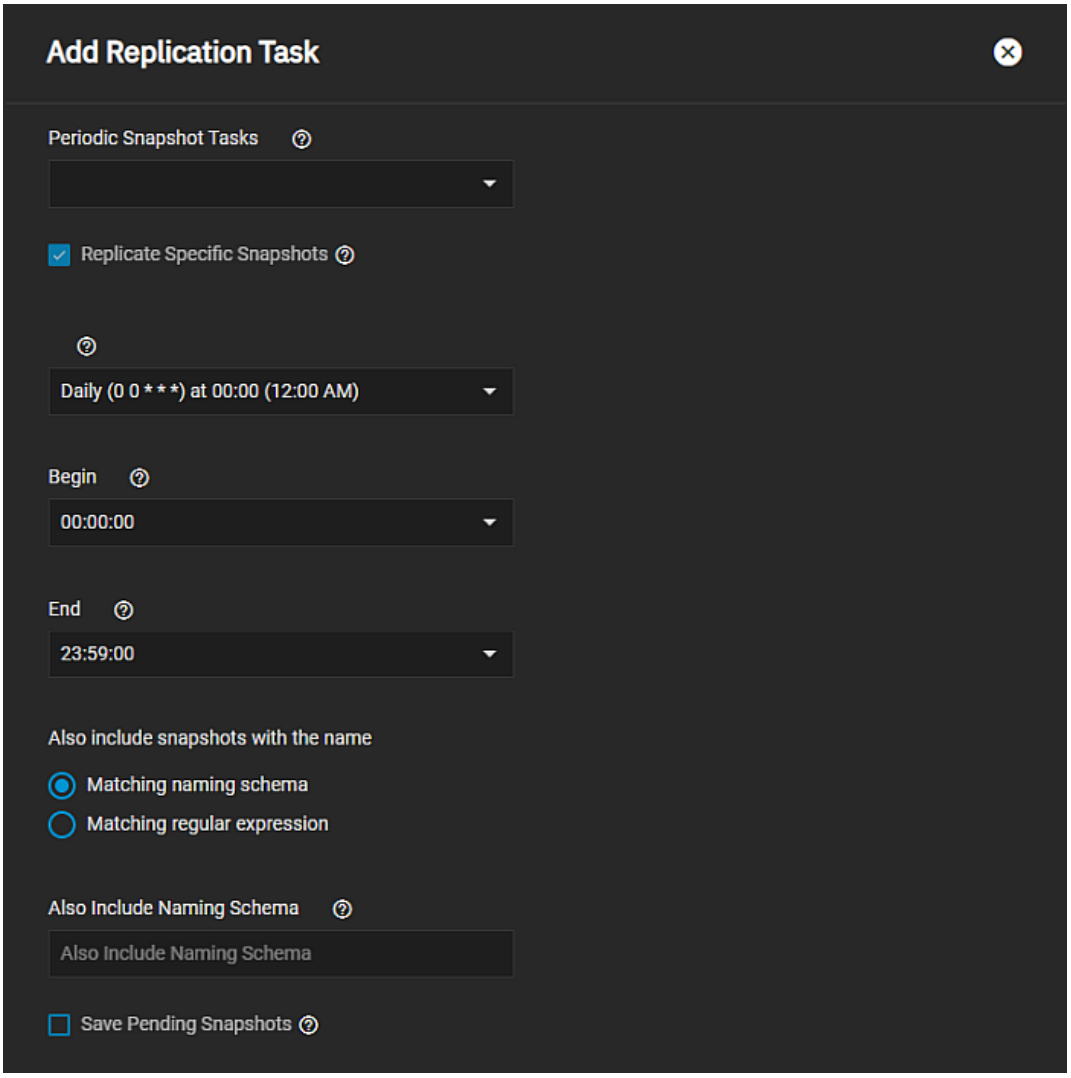
Setting	Description
Destination	Required. Enter or use ▸ to the left of /mnt and at each dataset to expand the dataset tree to browse to the dataset location to store the replicated snapshots. Click on the or checkbox to select the checkbox to the left of the dataset. Selecting a location defines the full path to that location as the destination. Appending a name to the path creates a new zvol at that location. For example, selecting *pol1/dataset1* stores snapshots in *dataset 1*, but adding */zvol1* after *dataset*1 creates *zvol1* for snapshot storage. Click the
arrow_drop_down at the /mnt to collapse the dataset tree.	
Destination Dataset Read-Only Policy	Select the policy from the dropdown list. Options are **Set** that changes all destination datasets to `readonly=on` after finishing the replication. **Require** stops replication unless all existing destination datasets have the property `readonly=on`. **Ignore** disables checking the `readonly` property during replication.
Encryption	Select to use encryption when replicating data. For more information on all options see Encryption.
Synchronize Destination Snapshots With Source	Select if the destination system has snapshots but they do not have any data in common with the source snapshot, destroy all data destination snapshots and do a full replication. WARNING! Enabling this option can cause data loss or excessive data transfer if the replication is misconfigured.

Setting	Description
Snapshot Retention Policy	Select the policy from the dropdown list to apply when replicated snapshots are deleted from the destination system. Options are **Same as Source**, **Custom** and **None**. When selecting **Same as Source** use the **Snapshot Lifetime** from the source periodic snapshot task. When selecting **Custom** define a **Snapshot Lifetime** for the destination system. Also displays the **Snapshot Lifetime** and measure of time options. When selecting **None** never delete snapshots from the destination system.
Snapshot Lifetime	Use to enter a numeric value to work with the measure of time field below to specify how long a snapshot remains on the destination system.
Measure of time	Select the measure of time from the dropdown list to work with the numeric value in **Snapshot Lifetime**. Options are **Hour(s)**, **Day(s)**, **Week(s)**, **Month(s)**, and **Year(s)**.

Various Snapshot Options

The snapshot settings below change options displayed based on selections made.

Click Here for More Information



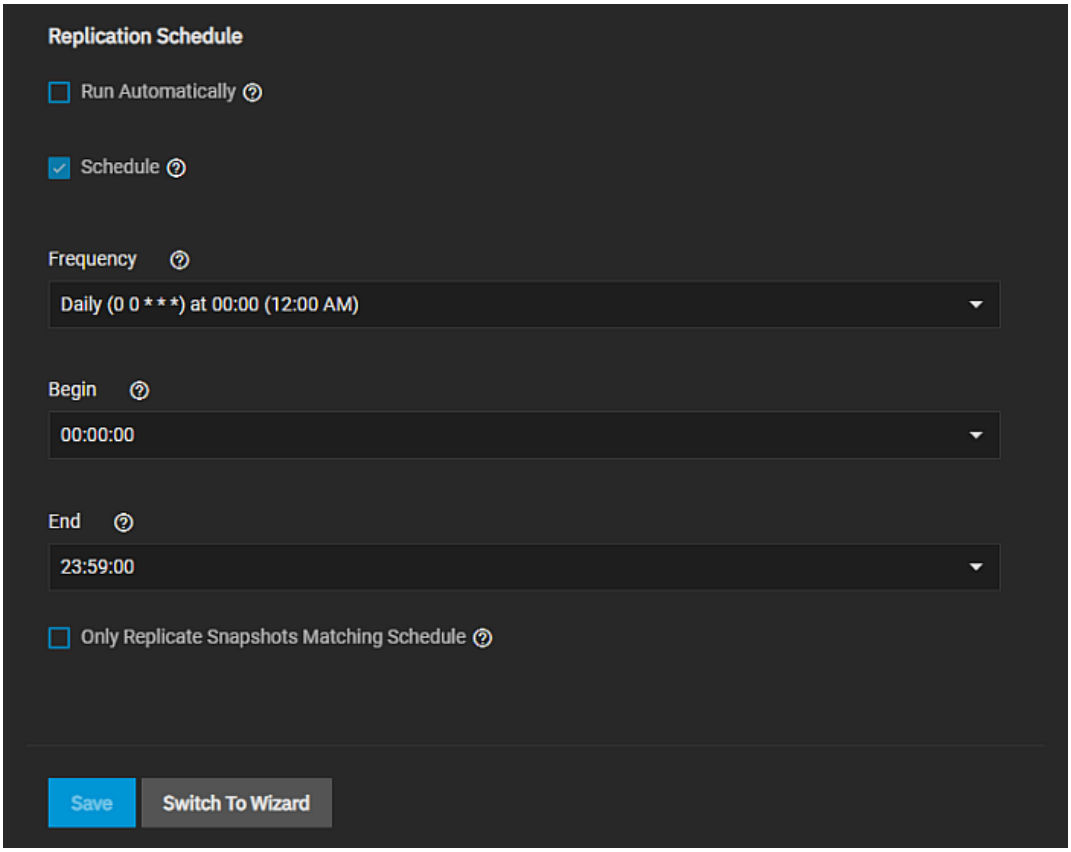
Setting	Description
Replicate Specific Snapshots	Select to only replicate snapshots that match a defined creation time. Selecting this option displays a schedule preset field and the **Begin** and **End** fields. Sselect the preset schedule or **Custom** to use the advanced scheduler, and then select a time in the **Begin** and **End** fields. A schedule field displays after selecting **Replicate Specific Snapshots**. Again, select a preset schedule or **Custom** to use the advanced scheduler.
Begin	Displays after selecting **Replicate Specific Snapshots**. Select a time range for the specific periodic snapshots to replicate, in 15 minute increments. Periodic Snapshots created before this selected time are not included in the replication.

Setting	Description
End	Displays after selecting **Replicate Specific Snapshots**. Select a time range for the specific periodic snapshots to replicate, in 15 minute increments. Periodic Snapshots created after this selected time are not included in the replication.
Periodic Snapshot Tasks	Select the snapshot schedule for this replication task from the dropdown list. Select from previously configured periodic snapshot tasks. This replication task must have the same **Recursive** and **Exclude Child Dataset** values as the selected periodic snapshot task. Selecting a periodic snapshot schedule removes the **Schedule** field.
Also include snapshots with the name	These radio buttons change the naming schema setting option below it. See Snapshot Naming in the wizard section for details on this option and the radio buttons.
Matching naming schema	Displays the **Also Include Naming Schema** setting.
Matching regular expression	Displays the **Matching regular expression** setting.
Also Include Naming Schema	Displays after selecting the **Matching naming schema** radio button. Enter the pattern of naming custom snapshots to include in the replication with the periodic snapshot schedule. Enter the strftime(3) strings that match the snapshots to include in the replication. When a periodic snapshot is not linked to the replication, enter the naming schema for manually created snapshots. Has the same %Y, %m, %d, %H, and %M string requirements as the **Naming Schema** in a **Add Periodic Snapshot Task**. Separate entries by pressing `Enter`.
Matching regular expression	Displays after selecting the **Matching regular expression** radio button. Enter the regular expressions snapshot should match. Using this option replicates all snapshots with names matching the specified regular expression. This process reads snapshot metadata to determine snapshot creation order. This slows regular performance on the systems with large number of snapshots.
Save Pending Snapshots	Select to prevent source system snapshots that have failed replication from being automatically removed by the **Snapshot Retention Policy**.

Replication Schedule Advanced Options

These schedule setting options are common to both the **Add Replication Task** wizard **When** and the advanced creation **Add Replication Task** screens.

Click Here for More Information



Setting	Description
Run Automatically	Select to either start this replication task immediately after the linked periodic snapshot task completes.
Schedule	Select to create a replication schedule if not selecting **Run Automatically**. Displays the **Frequency**, **Begin**, **End** and **Only Replicate Snapshots Matching Schedule** options.
Frequency	Displays after selecting **Schedule**. Select a preset schedule or choose **Custom** to use the advanced scheduler.
Begin	Displays after selecting **Schedule**. Select the start time for the replication task.
End	Displays after selecting **Schedule**. Select the end time for the replication task. A replication that is already in progress can continue to run past this time.
Only Replicate Snapshots Matching Schedule	Displays after selecting **Schedule**. Select to use the **Schedule** in place of the **Replicate Specific Snapshots** time frame. The **Schedule** values are read over the **Replicate Specific Snapshots** time frame.

Edit Replication Task Screen

The **Edit Replication Task** screen displays most of the settings found on the advanced **Add Replication Task** screen with a few exceptions.

- **General** settings do not include the **Direction** option. The **Transport** is setting on the edit screen are the same setting as the advanced creation settings.
- **Source** and **Destination** setting options are the same as the advanced creation settings.
- **Replication Schedule** setting options are the same as the advanced creation settings.

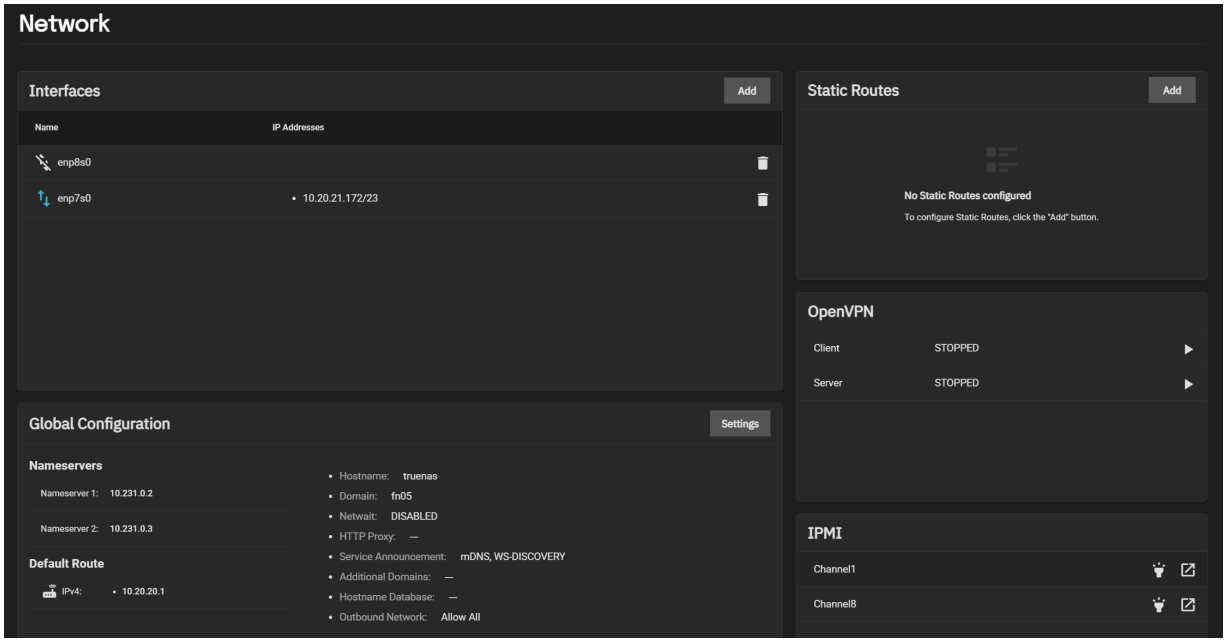
See the section linked above for information on the **Edit Replication Task** screen settings.

Related Content

- Adding Replication Tasks
- Managing Advanced Settings
- Setting Up a Local Replication Task
- Advanced Settings Screen
- Setting Up Advanced Replication Tasks
- Periodic Snapshot Tasks Screens
- Setting Up a Remote Replication Task
- Unlocking a Replication Encrypted Dataset or Zvol

4.6 - Network Screen

The SCALE **Network** screen has network configuration and settings options, in widgets, for active interfaces, static routes, and the global configuration. The **Network** screen also displays OpenVPN information and IPMI channels. IPMI only displays on systems with physical hardware and not on virtual machine deployments.



Click the buttons or on an existing widget entry to view configuration options on side panels.

Networking Tour Video

This video demonstrates configuring networking settings.

Additional Network Articles

- Network Interface Screens

  This article provides information on the **Network** screen **Interfaces** widget and configuration screens.

- Global Configuration Screens

  The **Global Configuration** widget displays the general TrueNAS network settings *not* specific to any interface.

- Static Route Screens

  The **Static Routes** widget displays existing static routes or to set up new ones.

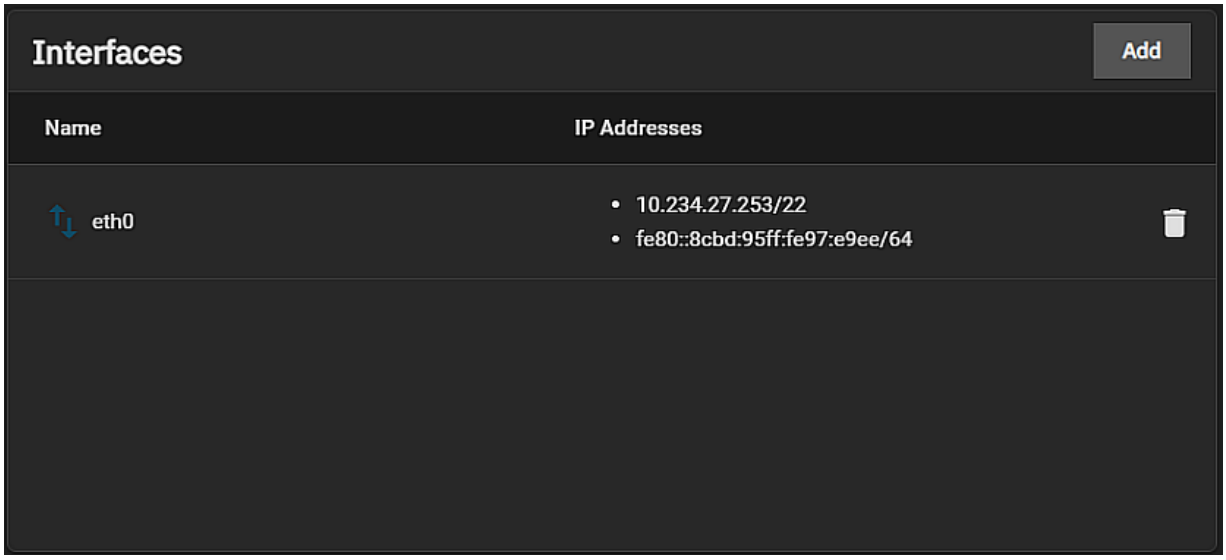
- IPMI Screens

  This article provides information on the **Network** screen **IPMI** widget and configuration screen.

4.6.1 - Network Interface Screens

This article provides information on the **Network** screen **Interfaces** widget and configuration screens.

The **Interfaces** widget on the **Network** screen displays interface port names and IP addresses configured on your TrueNAS system, as well as their upload/download rates.



Use **Add** to display the **Add Interface** configuration screen.

Click on an interface to display the **Edit Interface** configuration screen.

Click the icon next to an interface to delete that interface.

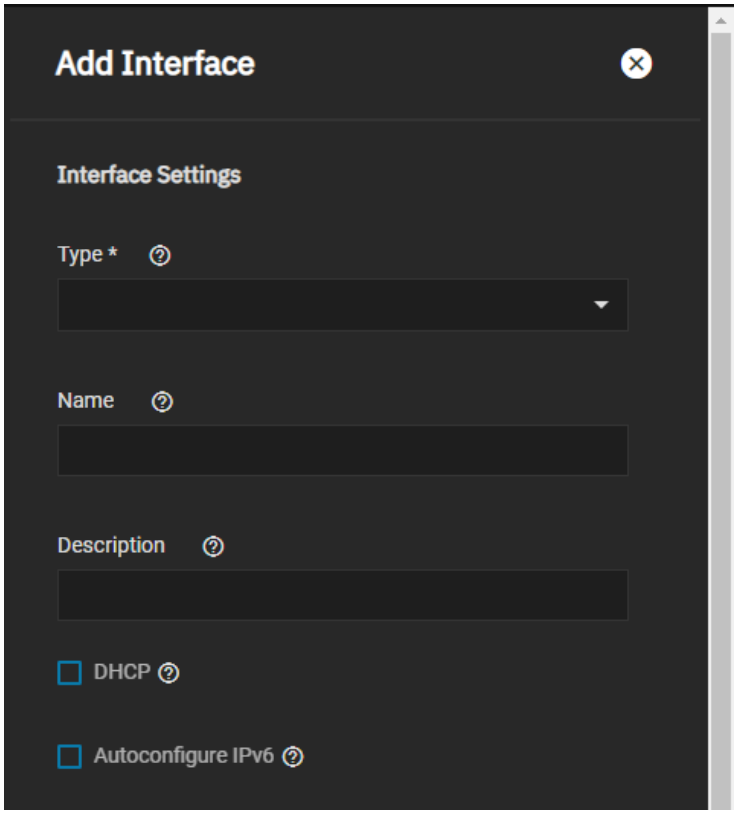
Add/Edit Interface Configuration Screens

The fields on the **Edit Interface** are almost identical to the **Add Interface** configuration screen except for the **Type** field that only displays on the **Add Interface** configuration screen. **Type** is a required field and after selecting the interface type additional configuration fields display for the type selected.

Use **Apply** to save your setting changes.

Interface Settings

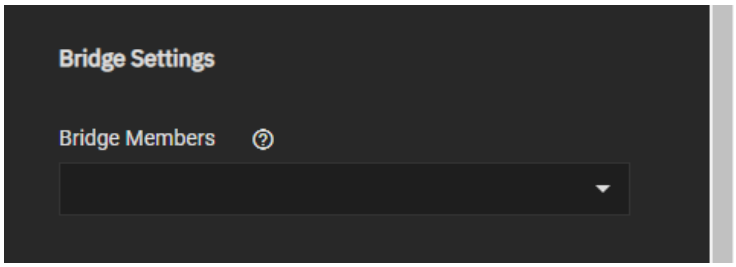
These settings display for all interface types. The **Type** setting is only available and required on the **Add Interface** configuration screen.



Setting	Description
Type	Required field. Select the type of interface from the dropdown list or options **Bridge**, **Link Aggregation** or **VLAN**. Each option displays additional configuration settings for that type. Select **Bridge** to create a logical link between multiple networks. Select **Link Aggregation** to combine multiple network connections into a single interface. Select **Virtual LAN** (VLAN) to partition and isolate a segment of the connection. This field does not display on the **Edit Interface** screen.
Name	Enter a name for the interface. Use the format bond*X*, vlan*X*, or br*X* where *X* is a number representing a non-parent interface. You cannot change the interface name after you click **Apply**. It becomes a read-only field when editing an interface.
Description	Enter a description for the interface.
DHCP	Select to enable DHCP. Leave checkbox clear to create a static IPv4 or IPv6 configuration. Only one interface can be configured using DHCP.
Autoconfigure IPv6	Select to automatically configure the IPv6 address with rtsol(8). Only one interface can be configured this way.

Bridge Settings

Bridge Settings only display after you select **Bridge** in for **Type**.

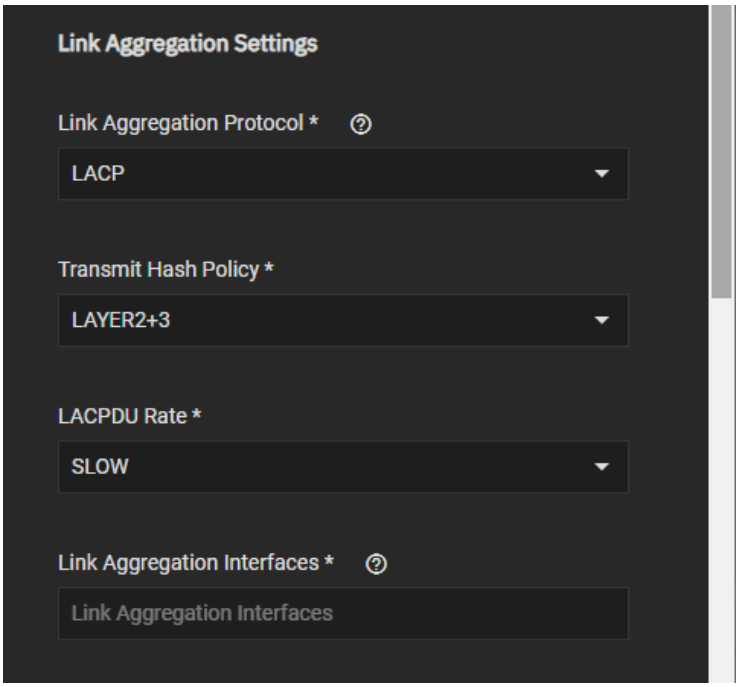


Setting	Description
Bridge Members	Select the network interfaces to include in the bridge from the dropdown list of options.

Link Aggregation Settings

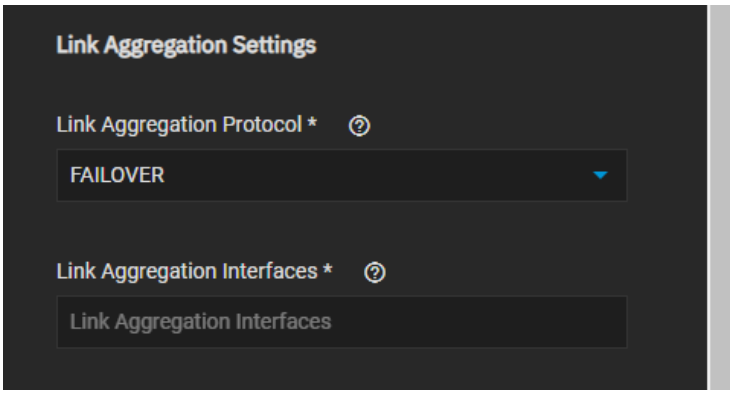
Link aggregation settings only display after you select **Link Aggregation** as the **Type**. Additional settings display based on the selection in **Link Aggregation Protocol**.

Click here for LACP settings



Setting	Description
Link Aggregation Protocol	Select the protocol to use from the dropdown list of options. The protocol determines the outgoing and incoming traffic ports. Select **LACP** if the network switch is capable of active LACP (this is the recommended protocol). **LACP** displays additional settings. Select **Failover** if the network switch does not support active LACP. This is the default protocol choice and should be only used if the network switch does not support active LACP. **Failover** uses only the **Link Aggregation Interfaces** setting. Select **Loadbalance** to set up loadbalancing. **Loadbalance** does not use any other link aggregation settings.
Transmit Hash Policy	Displays when the protocol is set to **LCAP** or **Loadbalance**. Select the hash policy from the dropdown list of options, **LAYER2**, **LAYER2+3** the default, or **LAYER3+4**..
LACPDU Rate	Displays only when the protocol is set to **LCAP**. Select either **Slow** or **Fast** from the dropdown list of options.
Link Aggregation Interfaces	Displays when protocol is set to **LACP**, **Failover** or **Loadbalance**. This is a required field. Select the interfaces to use in the aggregation. Warning! Link Aggregation creation fails if any of the selected interfaces have been manually configured!

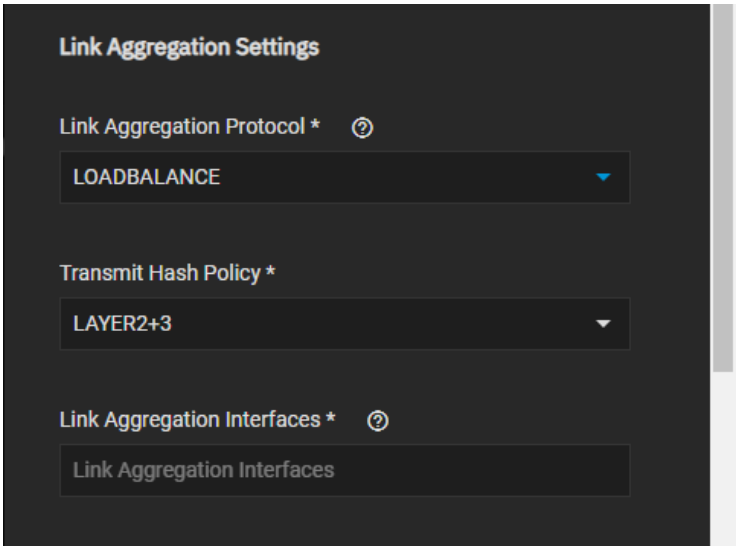
Click here for Failover settings



Setting	Description
Link Aggregation Protocol	Select the protocol to use from the dropdown list of options. The protocol determines the outgoing and incoming traffic ports. Select **LACP** if the network switch is capable of active LACP (this is the recommended protocol). **LACP** displays additional settings.

Setting	Description
	Select **Failover** if the network switch does not support active LACP. This is the default protocol choice and should be only used if the network switch does not support active LACP. **Failover** uses only the **Link Aggregation Interfaces** setting. Select **Loadbalance** to set up loadbalancing. **Loadbalance** does not use any other link aggregation settings.
Link Aggregation Interfaces	This is a required field. Select the interfaces to use in the aggregation. Warning! Link Aggregation creation fails if any of the selected interfaces have been manually configured!

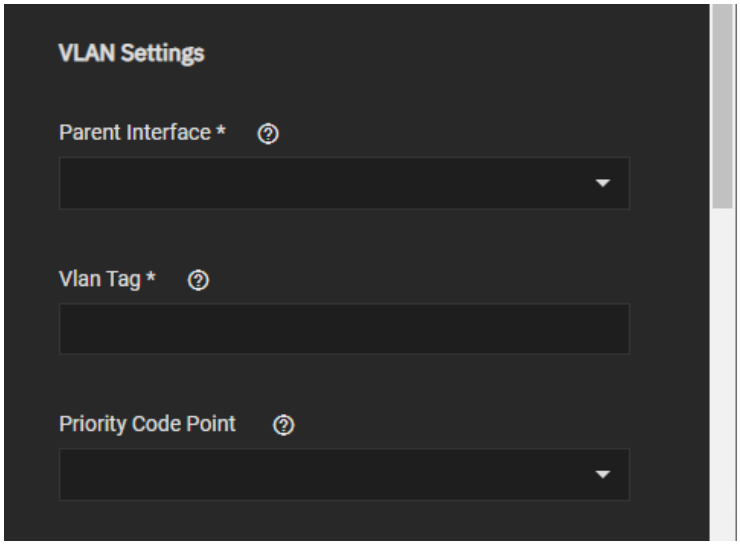
Click here for Loadbalance settings



Setting	Description
Link Aggregation Protocol	Select the protocol to use from the dropdown list of options. The protocol determines the outgoing and incoming traffic ports. Select **LACP** if the network switch is capable of active LACP (this is the recommended protocol). **LACP** displays additional settings. Select **Failover** if the network switch does not support active LACP. This is the default protocol choice and should be only used if the network switch does not support active LACP. **Failover** uses only the **Link Aggregation Interfaces** setting. Select **Loadbalance** to set up loadbalancing. **Loadbalance** does not use any other link aggregation settings.
Transmit Hash Policy	Displays when the protocol is set to **LCAP** or **Loadbalance**. Select the hash policy from the dropdown list of options, **LAYER2**, **LAYER2+3** the default, or **LAYER3+4**.
Link Aggregation Interfaces	Displays when protocol is set to **LACP**, **Failover** or **Loadbalance**. This is a required field. Select the interfaces to use in the aggregation. Warning! Link Aggregation creation fails if any of the selected interfaces have been manually configured!

VLAN Settings

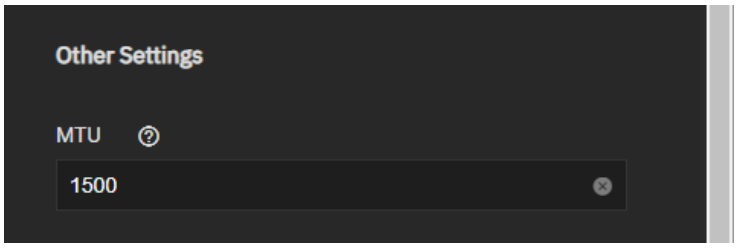
Link aggregation settings only display after you select **VLAN** as the **Type**.



Setting	Description
Parent Interface	Select the VLAN parent interface from the dropdown list of options. Usually and Ethernet card connected to a switch port configured for the VLAN. New link aggregations are not available until you restart the system.
VLAN Tag	Required field. Enter the numeric tag configured in the switched network.
Priority Code Point	Select the Class of Service from the dropdown list of options. The available 802.1p Class of Service ranges from **Best effort (default)** to **Network control (highest)**.

Other Settings

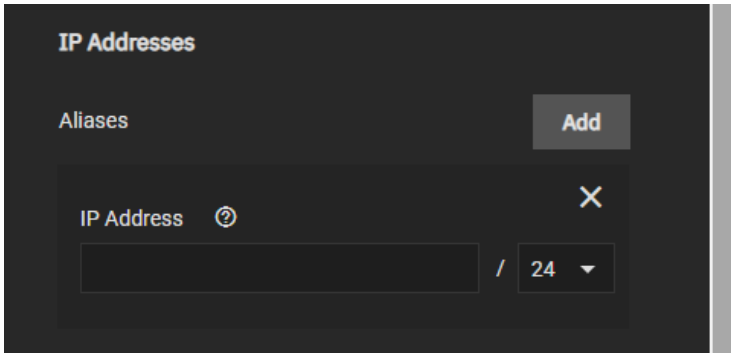
Other Settings display for all types of interfaces.



Setting	Description
MTU	*Maximum Transmission Unit* (MTU), or the largest protocol data unit that can be communicated. The largest workable MTU size varies with network interfaces and equipment. 1500 and 9000 are standard Ethernet MTU sizes. Leaving blank restores the field to the default value of **1500**.

IP Addresses

Use the **IP Address Add** to define an alias for the interface on the TrueNAS controller. The alias can be an IPv4 or IPv6 address.



Users may also select how many bits are a part of the network address from the dropdown list of options.

Related Content

- Managing Interfaces
- Console Setup Menu Configuration
- Setting Up a Network Bridge
- Setting Up a Link Aggregation
- Setting Up a Network VLAN
- Configuring Static Routes
- Setting Up Static IPs

Related Network Articles

- Dashboard
- Adding Network Settings
- Managing Interfaces
- Console Setup Menu Configuration
- Global Configuration Screens
- Managing Network Global Configurations
- Setting Up a Network Bridge
- Static Route Screens
- Setting Up a Link Aggregation

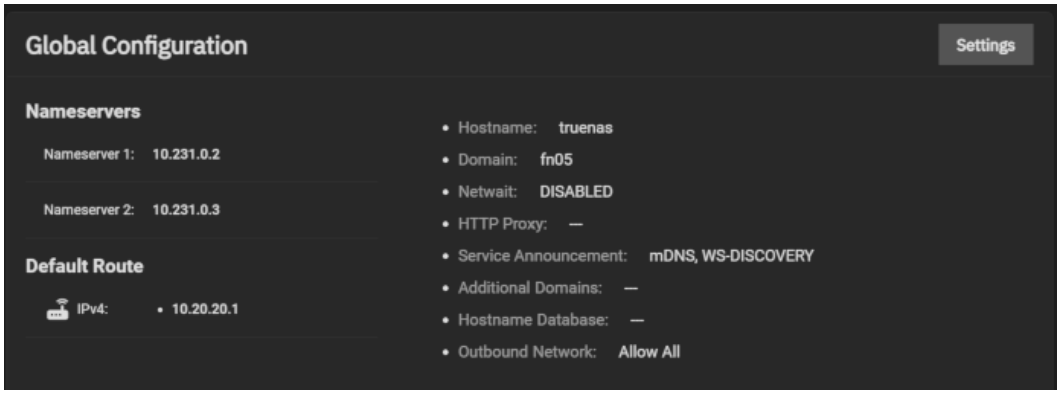
4.6.2 - Global Configuration Screens

The **Global Configuration** widget displays the general TrueNAS network settings *not* specific to any interface.

{{ toc }}

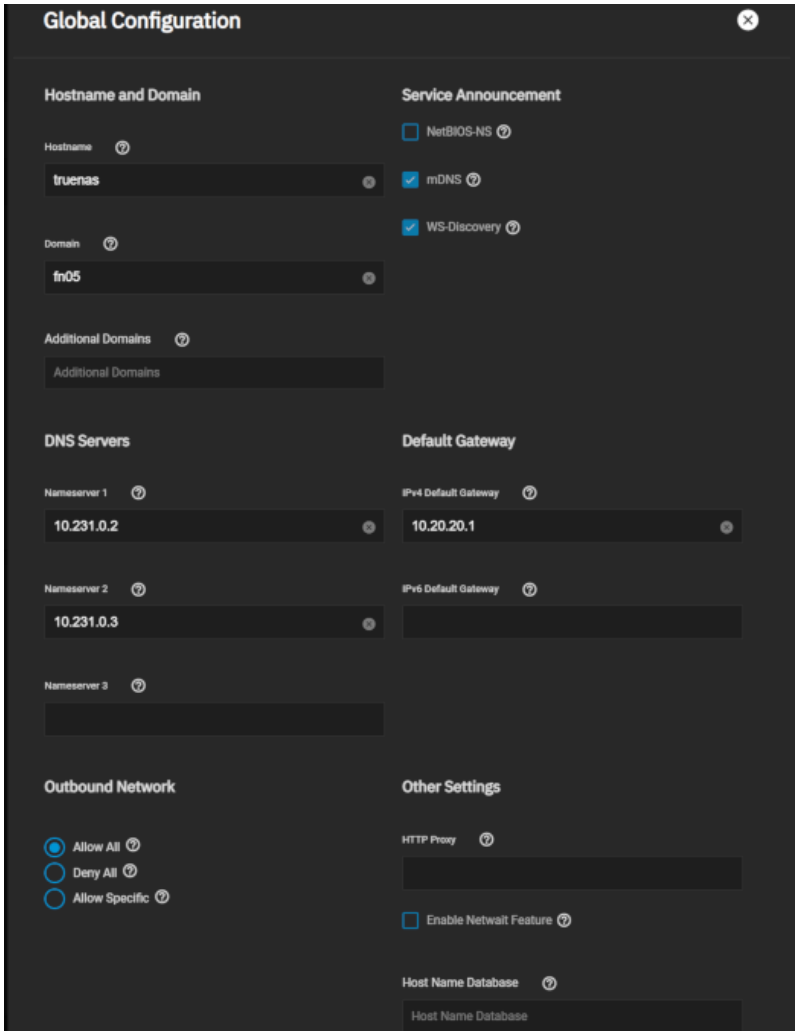
The **Global Configuration** widget displays the general TrueNAS networking settings *not* specific to any interface.

> The SCALE information dislplayed the **Global Configuration** widget is the equivalent of the information displayed on the TrueNAS CORE **Network Summary** screen. **Global Configuration** settings configuration screens are similar in both SCALE and CORE but SCALE includes external communication settings.



Use **Settings** to display the **Global Configuration** screen where you can add or change global network settings.

> **Disruptive Change**
>
> You can lose your TrueNAS connection if you change the network interface that the web interface uses!
> You might need command line knowledge or physical access to the TrueNAS system to fix misconfigured network settings.



Hostname and Domain Settings

Many of these fields have default values, but users can change them to meet local network requirements.

TrueNAS displays the **Hostname** and **Domain** in the **Dashboard System Information** widget.

> Some fields only display in the **Global Configuration** screen when the appropriate hardware is present.

Setting	Description
Hostname	System host name.
Hostname (TrueNAS Controller 2)	System host name for a second controller that displays only for High Availability (HA) systems where there is a second TrueNAS controller. Upper and lower case alphanumeric, (.) and (-) characters are allowed.
Hostname (Virtual)	Virtual host name that displays when using a virtual host; this is also used as the Kerberos principal name. Enter the fully qualified host name plus the domain name. Upper and lower case alphanumeric, (.), and (-) characters are allowed.
Domain	System domain name, like example.com
Additional Domains	Additional domains to search. Separate entries by pressing `Enter`. Adding search domains can cause slow DNS lookups.

Service Announcement Settings

Setting	Description
NetBIOS-NS	Select to use legacy NetBIOS name server. Advertises the SMB service NetBIOS name. Can be required for legacy SMB1 clients to discover the server. When advertised, the server appears in **Network Neighborhood**.
mDNS	Select to multicast DNS. Uses the system host name to advertise enabled and running services. For example, this controls if the server appears under **Network** on MacOS clients.

Setting	Description
WS-Discovery	Select to use the SMB Service NetBIOS name to advertise the server to WS-Discovery clients. This causes the computer to appear in the **Network Neighborhood** of modern Windows OSes.

DNS Servers Settings

Setting	Description
Nameserver 1	Primary DNS server.
Nameserver 2	Secondary DNS server.
Nameserver 3	Third DNS server.

Default Gateway Settings

Setting	Description
IPv4 Default Gateway	Enter an IPv4 address. This overrides the default gateway provided by DHCP.
IPv6 Default Gateway	Enter an IPv6 address. This overrides the default gateway provided by DHCP.

Outbound Network Settings

Select the radio button for the setting that matches your prefered system services external communicate ability.

Setting	Description
Allow All	Select to allow any system service to communicate externally.
Deny All	Select to restrict this system so it cannot communicate externally.
Allow Specific	select to define the system services that are allowed to communicate externally. All other external traffic is restricted. If selected, a dropdown list field displays where you can select the services to enable external communication.

Other Settings

Setting	Description
HTTP Proxy	When using a proxy, enter the proxy information for the network in the format *http://my.proxy.server:3128* or *http://user:password@my.proxy.server:3128*.
Enable Netwait Feature	Select to delay the start of network services until pings return from the IP addresses added to the **Netwait IP List** field that displays only after you select the checkbox.
Netwait IP List	Displays only after selecting the **Enable Netwait Feature** checkbox. Enter a list of IP addresses to ping. Separate entries by pressing `Enter`. Each address is tried until one is successful or the list is exhausted. Leave empty to use the default gateway.
Host Name Database	Enter additional hosts to append to */etc/hosts*. Separate entries by pressing. Separate entries by pressing `Enter`. Use the format *`IP_address space hostname`* where multiple hostnames can be used if separated by a space. Hosts defined here are still accessible by name even when DNS is not available. See hosts for additional information.

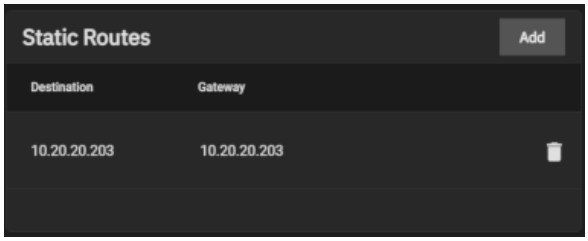
Related Content

- Dashboard
- Network Interface Screens
- Adding Network Settings
- Managing Interfaces
- Console Setup Menu Configuration
- Managing Network Global Configurations
- Setting Up a Network Bridge
- Static Route Screens
- Setting Up a Link Aggregation

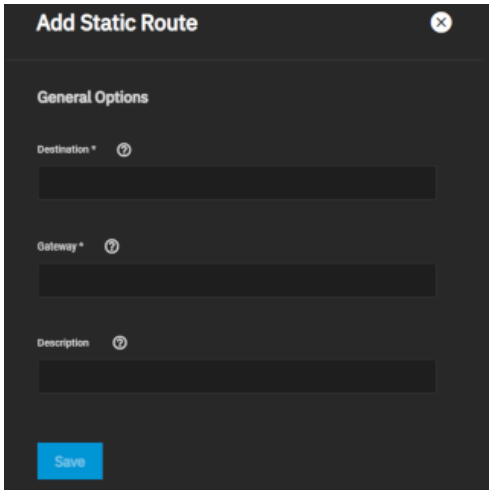
4.6.3 - Static Route Screens

The **Static Routes** widget displays existing static routes or to set up new ones.

The **Static Routes** widget on the **Network** screen displays static IP addresses configured as static routes. Use this to manually enter routes to network destinations outside the TrueNAS network so the router can send packets to a destination network.



TrueNAS does not have defined static routes by default. If you need a static route to reach portions of the network, add the route by going to **Network** and clicking **Add** in the **Static Routes** window.



Setting	Description
Destination	Enter the destination IP address using the format *A.B.C.D/E* where *E* is the CIDR mask. This is a required field.
Gateway	Enter the IP address of the gateway. This is a required field.
Description	Enter notes or an identifier describing the route.

Use **Save** to add the static route.

Related Content

- Dashboard

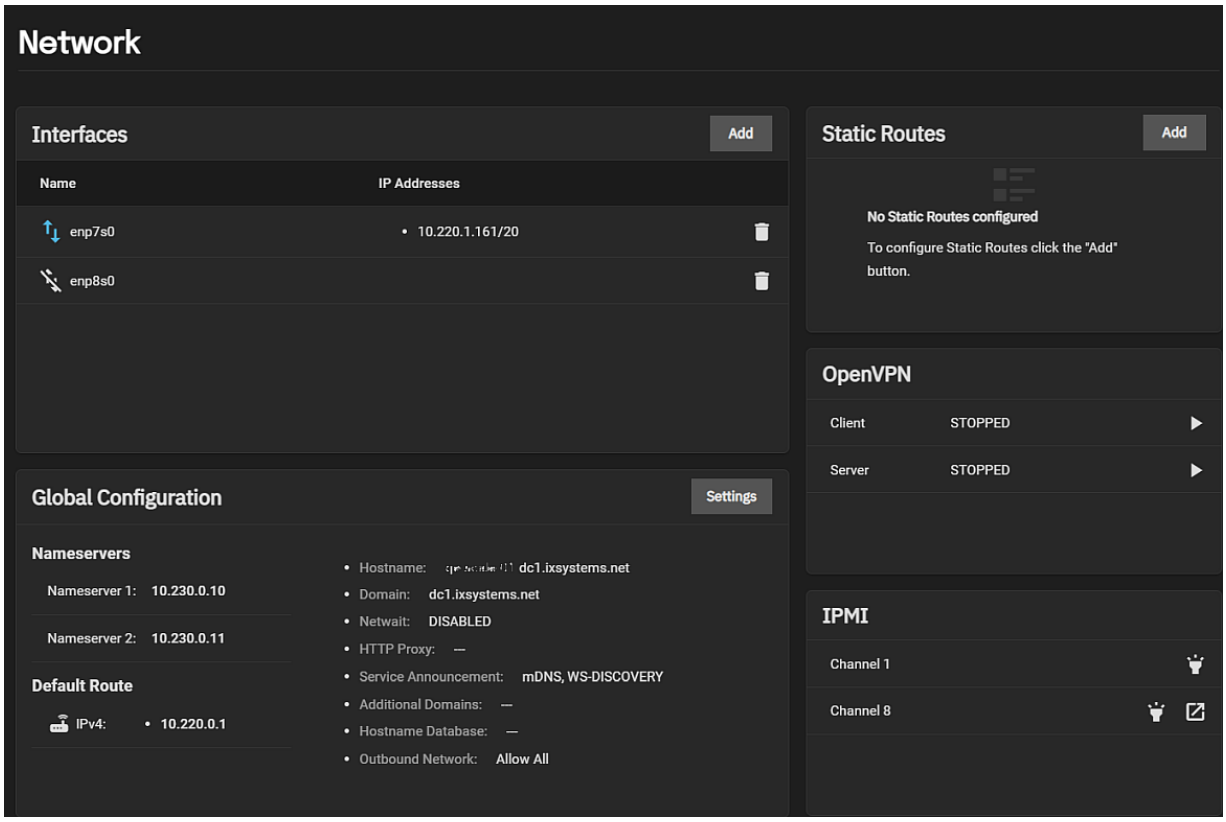
Related Network Articles

- Dashboard
- Network Interface Screens
- Adding Network Settings
- Managing Interfaces
- Console Setup Menu Configuration
- Global Configuration Screens
- Managing Network Global Configurations
- Setting Up a Network Bridge
- Setting Up a Link Aggregation

4.6.4 - IPMI Screens

This article provides information on the **Network** screen **IPMI** widget and configuration screen.

The **IPMI** widget on the **Network** screen displays the available IPMI channels.



The **Identify Light** button displays a dialog where users can select a duration for the system IPMI to flash so they can identify it.

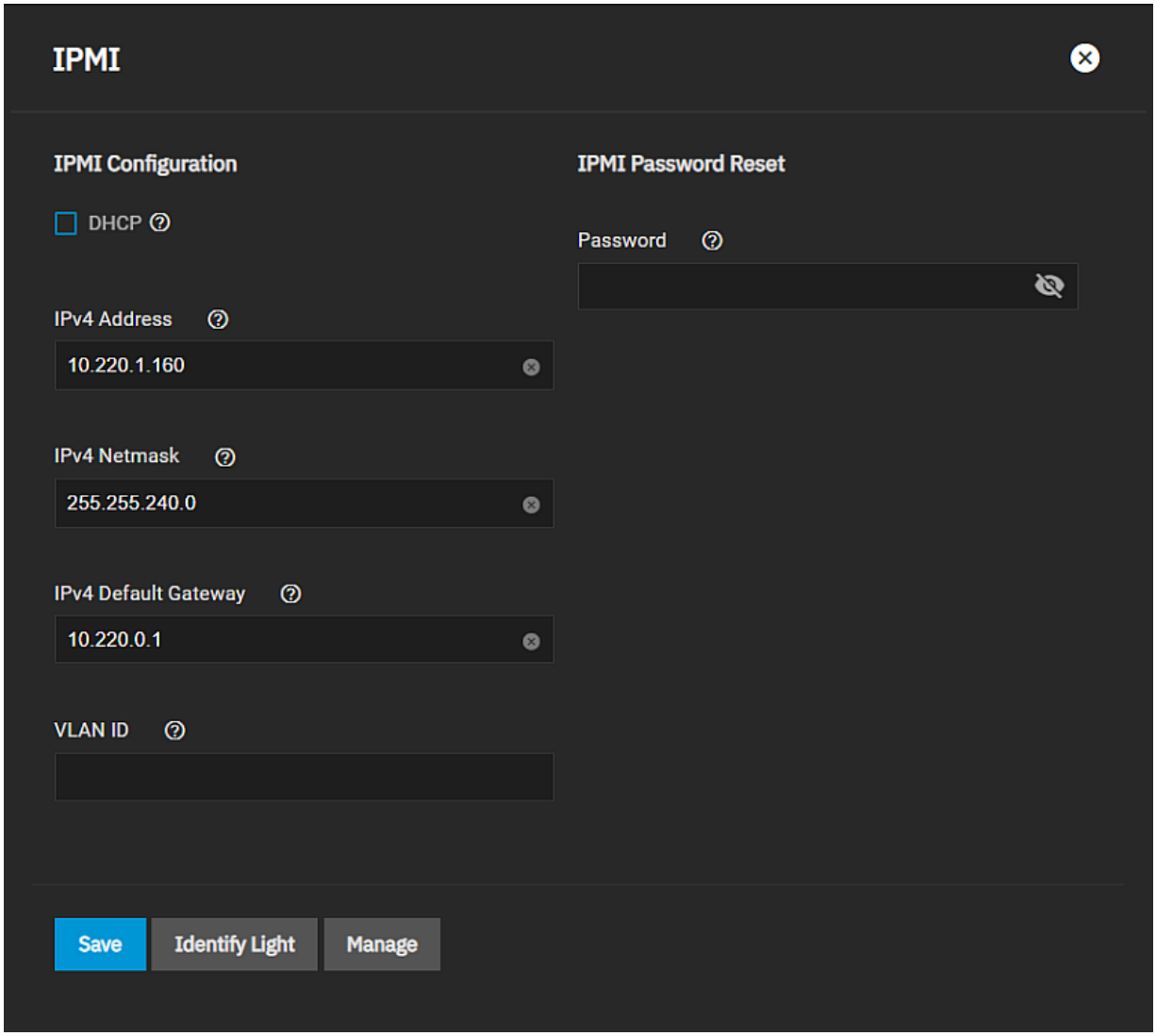
The **Manage** button opens the IPMI manager in a new browser tab where users can log into the IPMI web interface.

Click in the IPMI channel to display the **IPMI** configuration screen.

> IPMI requires compatible hardware! Refer to your hardware documentation to determine if the TrueNAS web interface has IPMI options.

IPMI Configuration Screen

Click on the channel you wish to edit to open the configuration screen.



Setting	Description
DHCP	Select to use DHCP to assign IPv4 network values. Clear checkbox to manually configure a static IPv4 connection.
IPv4 Address	Enter the static IPv4 address of the IPMI web interface.
IPv4 Netmask	Enter the subnet mask of the IPv4 address.
IPv4 Default Gateway	Enter the default gateway of the IPv4 connection.
VLAN ID	Enter the VLAN identifier if the IPMI out-of-band management interface is not on the same VLAN as management networking.
Password	Enter a password for connecting to the IPMI interface from a web browser. The password must include at least one upper case letter, one lower case letter, one digit, and one special character (punctuation, e.g. ! # $ %, etc.). It must also be 8-16 characters long.
Identify Light	Like the button on the **IPMI** widget, displays the same dialog and dropdown list of options users can select for the duration to flash the system IPMI light on the compatible connected hardware.
Manage	Like the button on the **IPMI** widget, this opens the same IPMI manager in a new browser tab where users can communicate with the server without having direct to the hardware.

Related Content

- SCALE Hardware Guide
- Setting Up IPMI

Related Network Articles

- Dashboard
- Network Interface Screens
- Adding Network Settings

- Managing Interfaces
- Console Setup Menu Configuration
- Global Configuration Screens
- Managing Network Global Configurations
- Setting Up a Network Bridge
- Static Route Screens
- Setting Up a Link Aggregation

4.7 - Credentials

SCALE Credential options are collected in this section of the UI and organized into a few different screens:

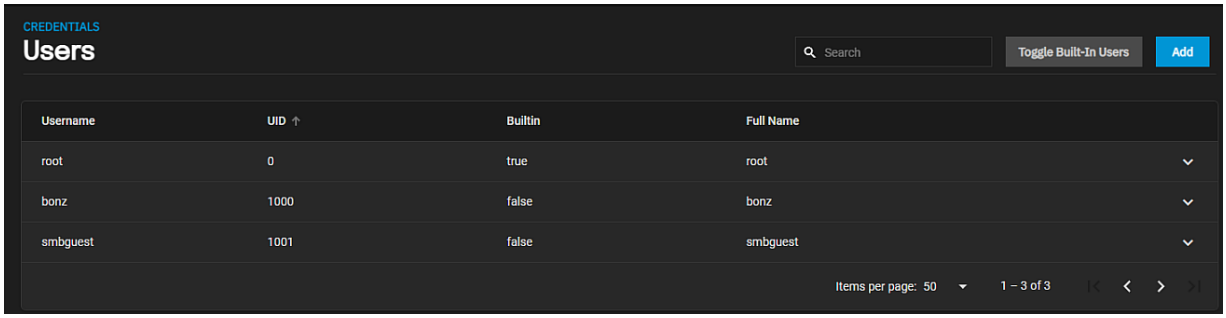
- **Local Users** allows those with permissions to add, configure, and delete users on the system. There are options to search for keywords in usernames, display or hide user characteristics, and toggle whether the system shows built-in users.
- **Local Groups** allows those with permissions to add, configure, and delete user groups on the system. There are options to search for keywords in group names, display or hide group characteristics, and toggle whether the system shows built-in groups.
- **Directory Services** contains options to edit directory domain and account settings, set up Idmapping, and configure access and authentication protocols. Specific options include configuring Kerberos realms and key tables (keytab), as well as setting up LDAP validation.
- **Backup Credentials** stores credentials for cloud backup services, SSH Connections, and SSH Keypairs. Users can set up backup credentials with cloud and SSH clients to back up data in case of drive failure.
- **Certificates** contains all the information for certificates, certificate signing requests, certificate authorities, and DNS-authenticators. TrueNAS comes equipped with an internal, self-signed certificate that enables encrypted access to the web interface, but users can make custom certificates for authentication and validation while sharing data.
- **2FA** allows users to set up Two-Factor Authentication for their system. Users can set up 2FA, then link the system to an authenticator app (such as Google Authenticator, LastPass Authenticator, etc.) on a mobile device.

Ready to get started? Choose a topic or article from the left-side **Navigation** pane. Click the **<** symbol to expand the menu to show the topics under this section.

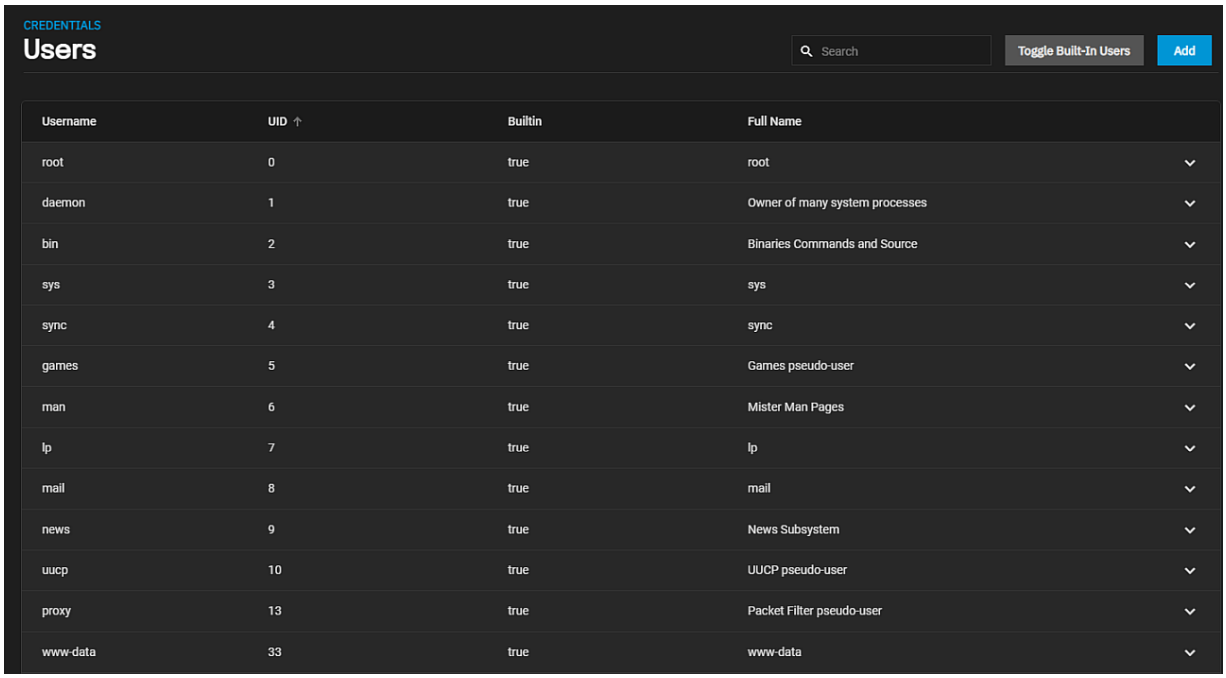
4.7.1 - Local Users Screens

This article provides information on the **Local User** screens and settings.

The **Credentials > Users** screen displays a list of user accounts added to the system. By default built-in users except for **root** are hidden until you make them visible.



Toggle Build-In Users displays either the **Show Built-In Users** or **Hide Built-in Users** dialogs based on the current **Users** list view. If built-in users are hidden, the **Show Built-in Users** dialog opens. Click **Show** to displays the hidden list of users.

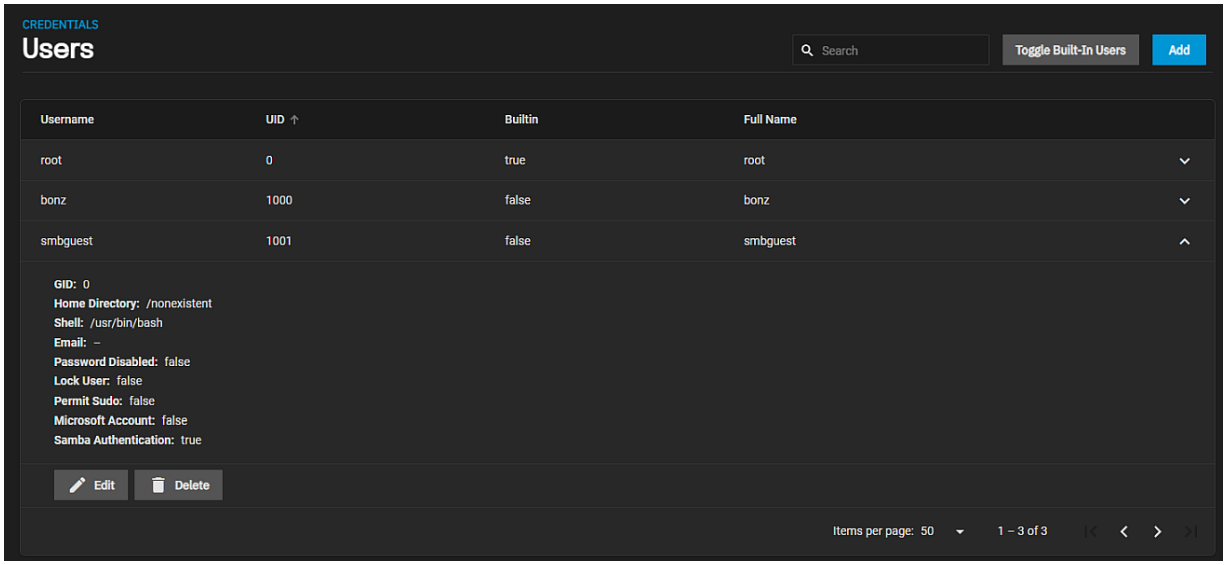


To hide the built-in users, click **Toggle Built-In Users** again to open the **Hide Built-in Users** dialog. Click **Hide** to only display non-built-in users again.

Add Opens the **Add User** screen.

User Details Screen

The expanded view of each users includes details on that user and provides the option to edit or delete the user. Click the ⌄ arrow to show the user details screen.



Edit opens the Edit User screen. **Delete** opens a delete confirmation dialog.

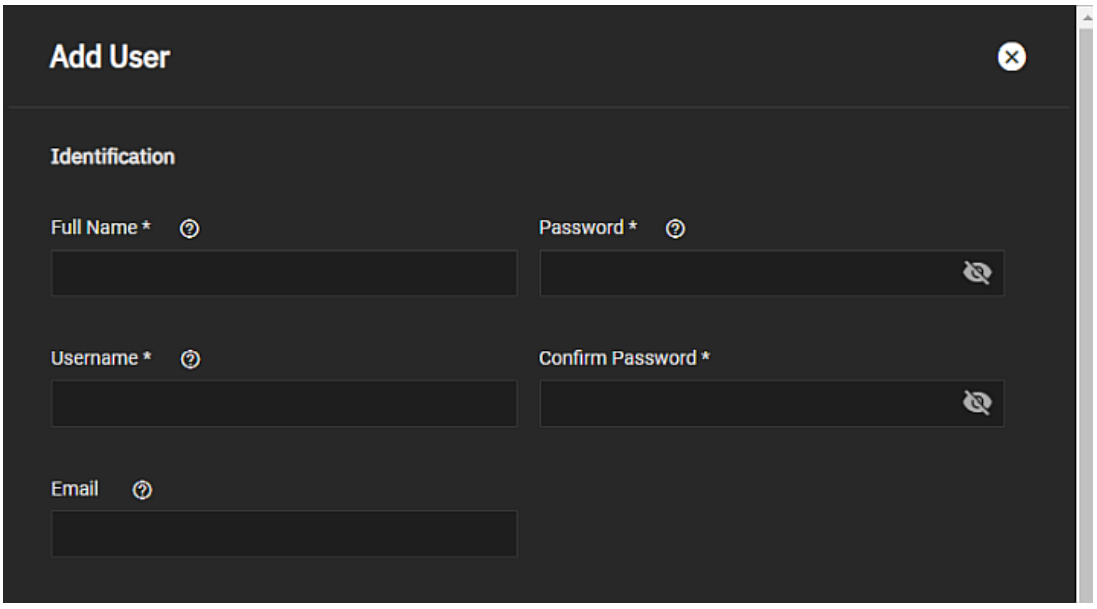
Add or Edit User Screens

The **Add User** and **Edit User** configuration screens display the same setting options. Built-in users (except the **root** user) do not include the **Home Directory Permissions** settings, but all new users created, such as those for an SMB share like the **smbguest** user do.

Identification Settings

Identification settings specify the name, user name, password and email for the user.

Click Here for More Information



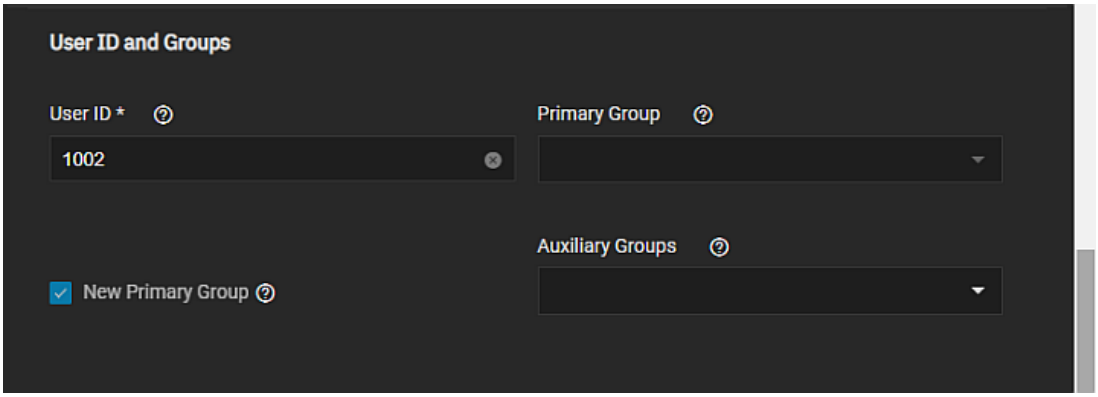
Setting	Description
Full Name	Required. Enter a name for the user with our without spaces.
Username	Required. Enter a user name of up to 16 characters in length. When using NIS or other legacy software with limited user name lengths, keep names to eight characters or less for compatibility. Do not begin the user name with a hyphen (-), and do not include a space, tab, the comma (,), plus (+), ampersand (&), percent (%), carat (^), open or close parenthesis ( ), exclamation mark (!), at symbol (@), tilde (~), question mark (?), greater or less than symbols (<)(>), or equals (+) in the name. You can use the dollar sign ($) as the last character of the user name.
Password	Required. Enter a user password unless **Enable Password login** is set to **No**. The password cannot contain a question mark (?).
Confirm Password	Required. Re-enter the value entered in **Password**.

Setting	Description
Email	Enter the email address of the new user. This email address receives notifications, alerts, messages based on the settings configured.

User ID and Groups Settings

User ID and Group settings specify the user ID and groups this user belongs to.

Click Here for More Information

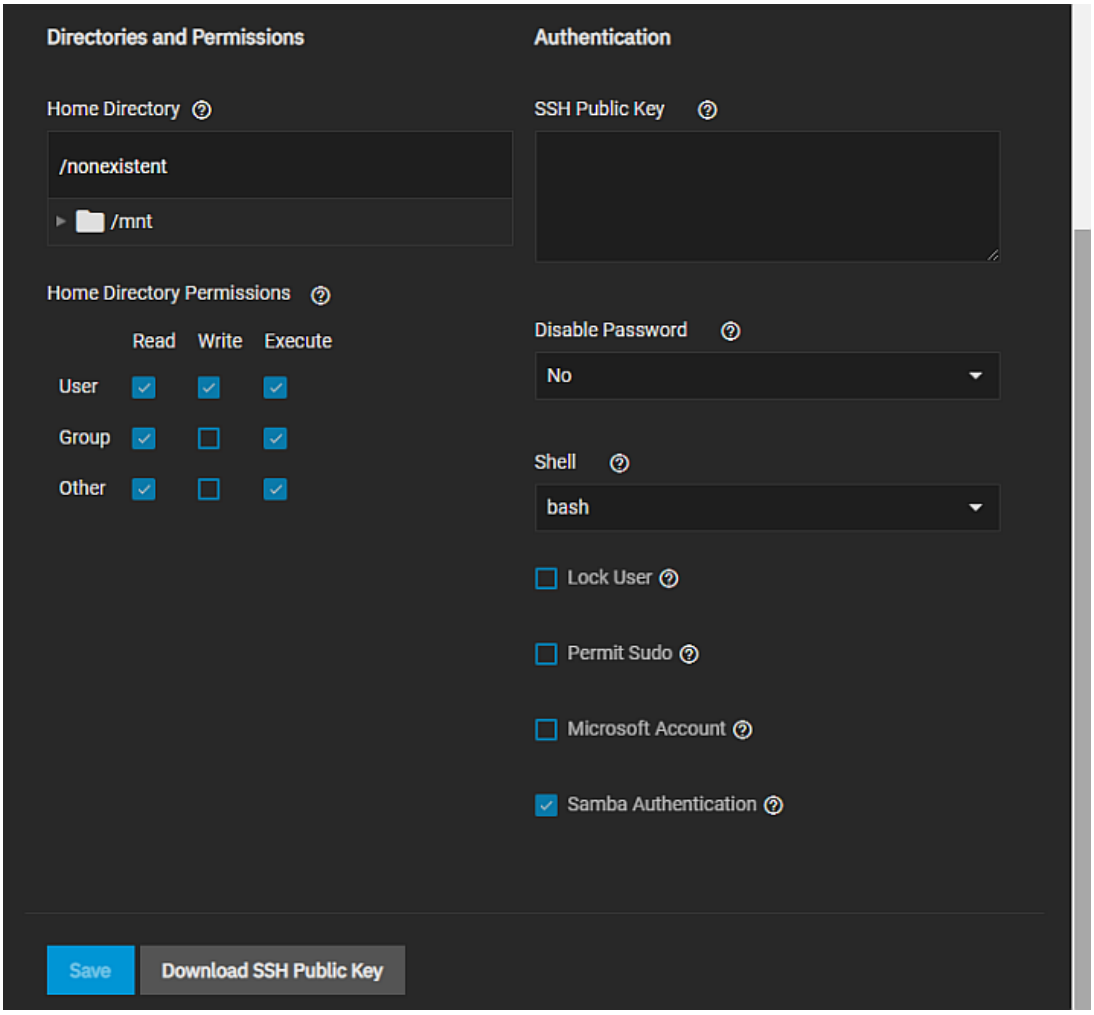


Setting	Description
User ID	Required. Enter a number greater than 1000 for user accounts. For system accounts use an ID equal to the default port number used by the service.
Primary Group	Select a group from the dropdown list. New users are not assigned **su** permissions if **wheel** is their primary group.
Auxiliary Groups	Select group(s) from the dropdown list to add this new user to additional groups.
New Primary Group	Select to create a new primary group with the same name as the user. Clear to select an existing group from the **Primary Group** dropdown list.

Directories and Permissions settings

Directory and Permissions settings pecify the user home directory and the permissions for that home directory.

Click Here for More Information

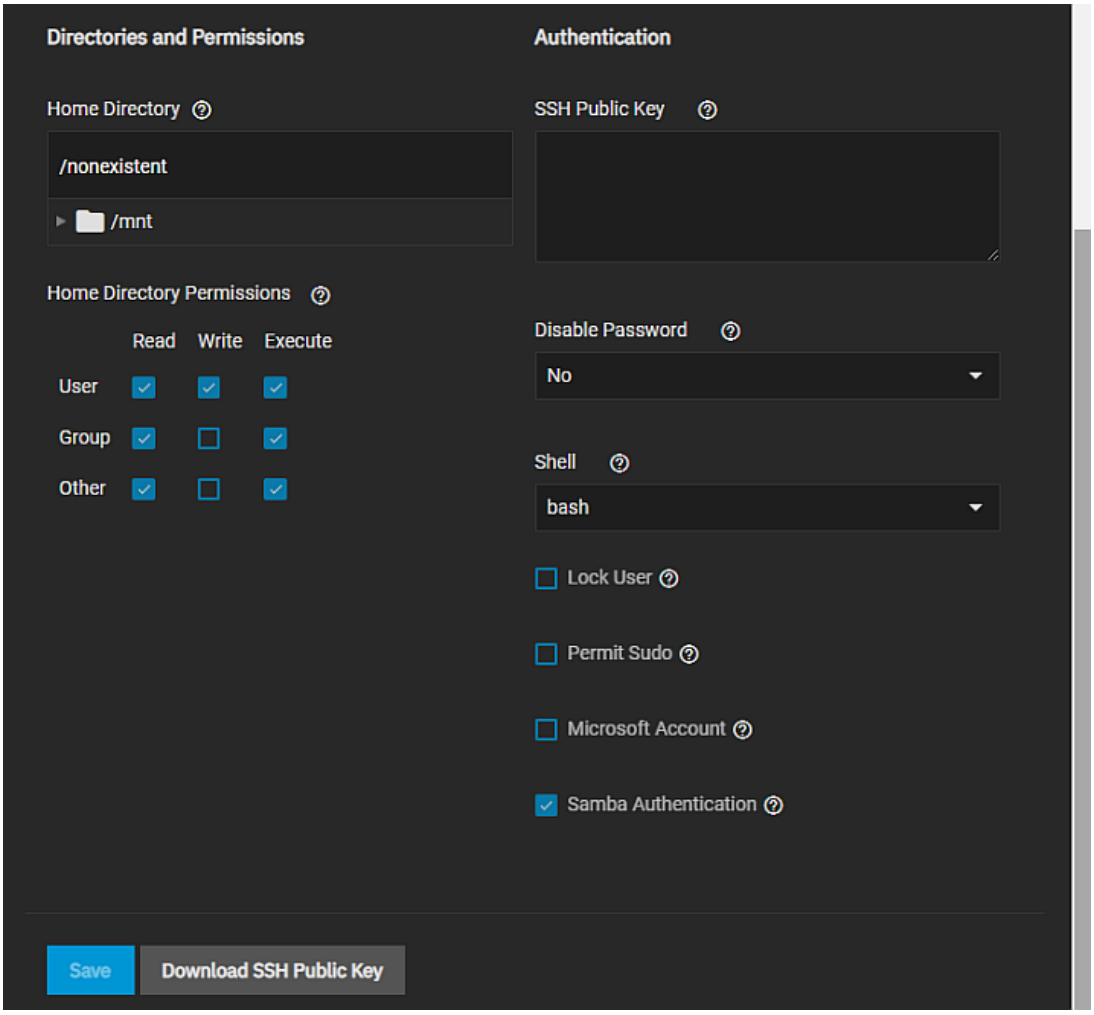


Setting	Description
Home Directory	Enter or browse to enter the path to the home directory for this user. If the directory exists and matches the **Username**, it is set as the home directory for the user. When the path does not end with a subdirectory matching the username, a new subdirectory is created. The full path to the user home directory displays here on the **Edit User** screen when editing this user.
Home Directory Permissions	Select the permissions checkboxes (**Read**, **Write**, **Execute**) for each (**User**, **Group**, **Other**) to set default Unix permissions for the user home directory. Built-in users are read-only and do not see these permissions settings.

Authentication settings

Authentication settings specify authentication methods, the public SSH key, user administration access, and enables/disables password authentication. It also covers the Shell options.

Click Here for More Information



Setting	Description
SSH Public Key	Enter or paste the **public** SSH key of the user for any key-based authentication. Use **Download SSH Public Key** to obtain a public key text file. Keep a backup copy of the public key! Do not paste the private key in this field!
Disable Password	Select the password option from the dropdown list. Select **Yes** to disable the **Password** and **Confirm Password** fields and remove the password from the account. The account cannot use password-based logins for services. For example, disabling the password prevents using account credentials to log into an SMB share or open and SSH session on the system. This also removes the **Lock User** and **Permit Sudo** options. Select **No** to requires adding a password to the account. The account can us the saved **Password** to authenticate with password-based services.
Shell	Select the shell to use for local and SSH logins from the dropdown list. Options are **bash**, **rbash**, **dash**, **sh**, **zsh**, **tmux** and **nologin**.
Lock User	Select to prevent the user from logging in or using password-based services until you clear this checkbox. Locking an account is only possible when **Disable Password** is set to **No** and the account has a created password in **Password**.
Permit Sudo	Select to give this user administrator permissions and the ability to use sudo. When using sudo, a user is prompted for their account password.
Microsoft Account	Select to allow additional user name authentication methods when the user connects from a Windows 8 or newer operating system.
Samba Authentication	Select to allow this user to authenticate to and access data share with SMB samba shares.
Download SSH Public Key	Click to generate and download a public key text file to past into **SSH Public Key**.

Shell Options

You can set a specific shell for the user from the **Shell** dropdown list options:

Shell	Description
bash	Bourne Again shell for the GNU operating system.

Shell	Description
rbash	Restricted bash
dash	Debian Almquist shell
sh	Bourne shell
zsh	Z shell
tmux	terminal multiplexer
nologin	Use when creating a system account or to create a user account that can authenticate with shares but that cannot log in to the TrueNAS system using `ssh`.

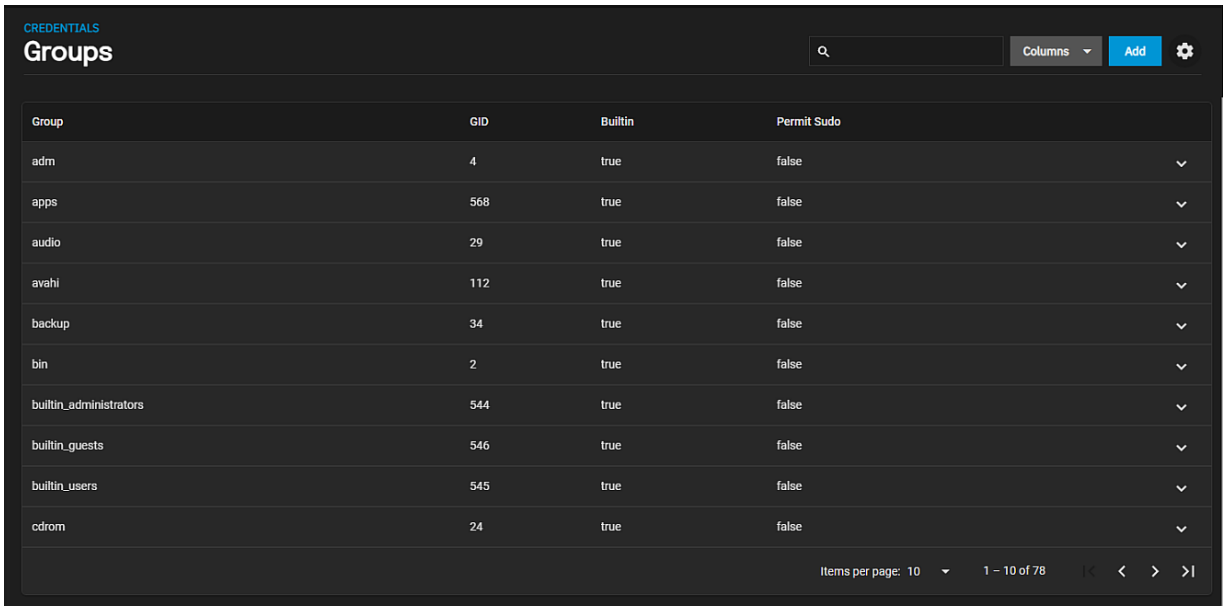
Related Content

- Managing Users

4.7.2 - Local Groups Screens

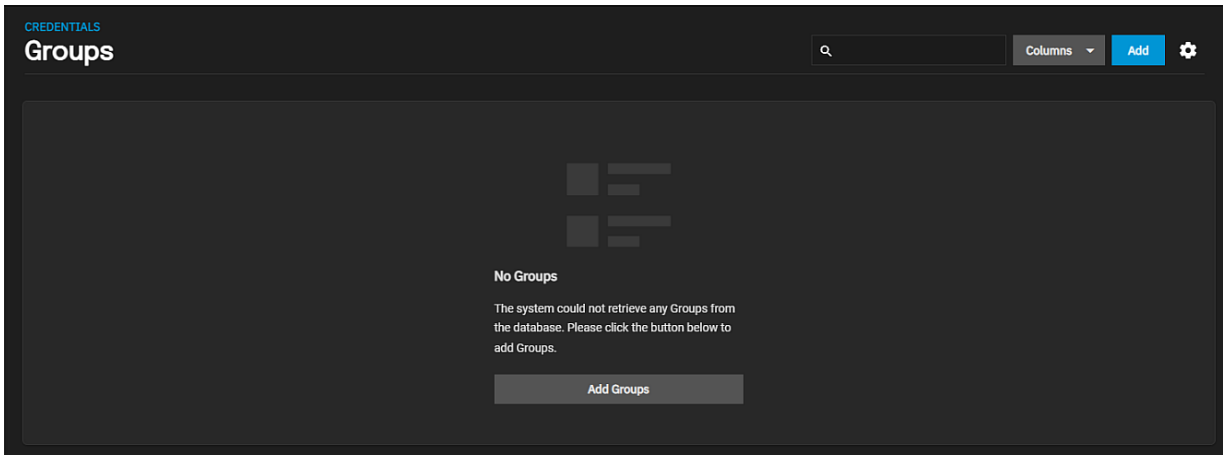
This article provides information on group settings and screens.

The **Credentials > Groups** screen displays a list of groups configured on the screen. By default, built-in groups are hidden until you make them visible.



To see built-in groups, click the **Toggle Built-In Groups** icon to open the **Show Built-In Groups** dialog. Click **Show**. To hide the built-in groups, click the **Toggle Built-In Groups** icon again to open the **Hide Built-in Groups** dialog. click **Hide**.

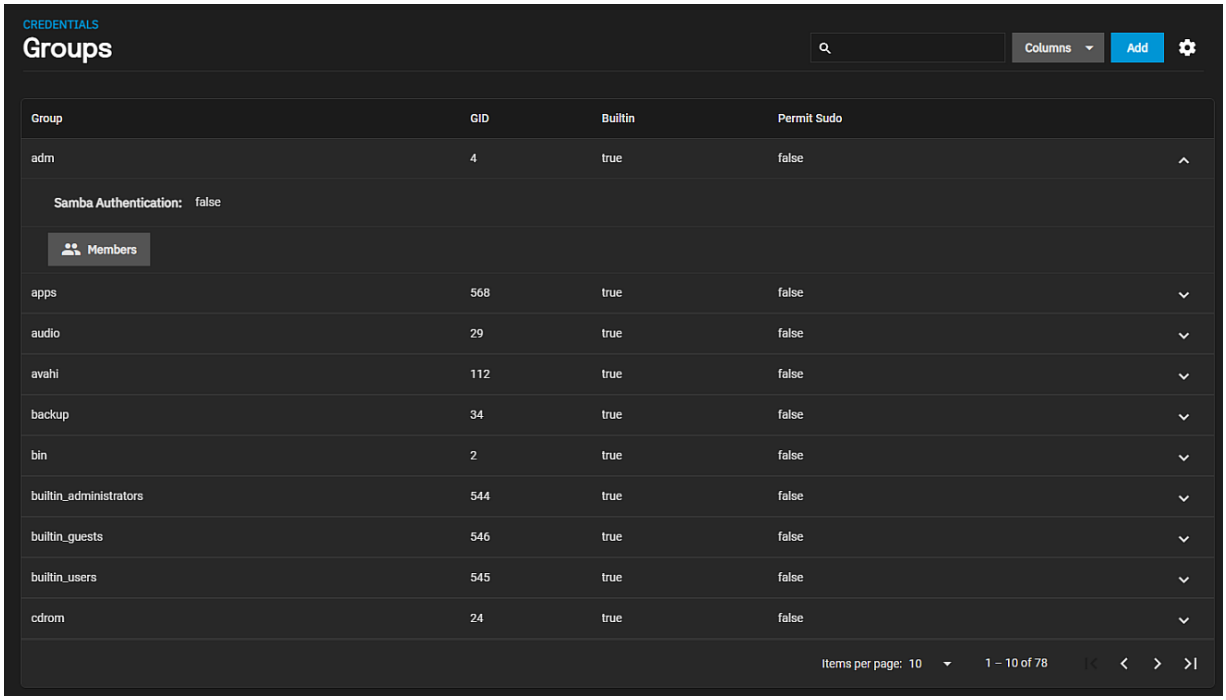
The **Credentials > Groups** screen displays the **No groups** screen if no groups other than built-in groups are configured on the system.



Add or **Add Groups** opens the **Add Group** configuration screen.

Groups Details Screen

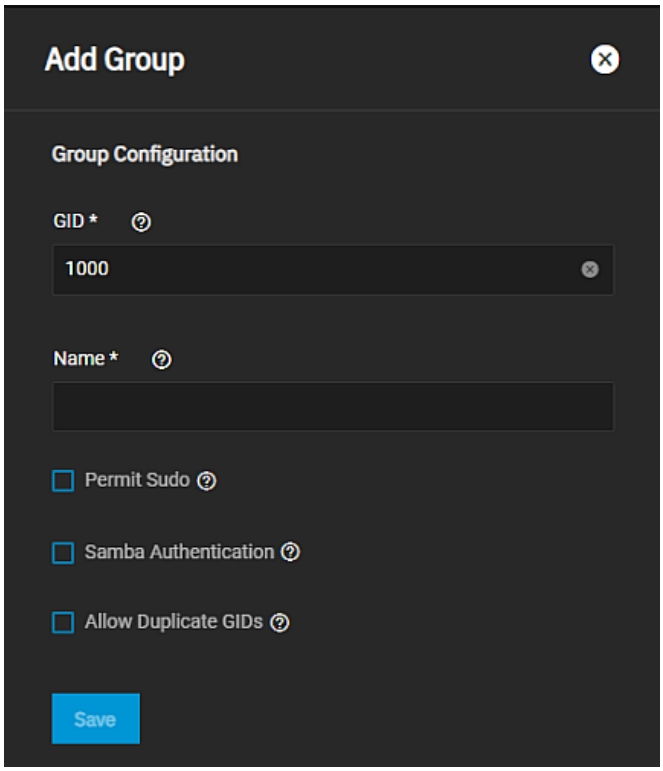
The expanded view of each group includes details on that group and provides the option to edit members. Click the arrow to show the group details screen.



Members opens the **Update Members** screen. **Delete** opens a delete confirmation dialog.

Add Group Screen

The **Add User** and **Edit User** configuration screens display the same setting options. Built-in users (except the **root** user) do not include the **Home Directory Permissions** settings, but all new users created, such as those for an SMB share like the **smbguest** user do.

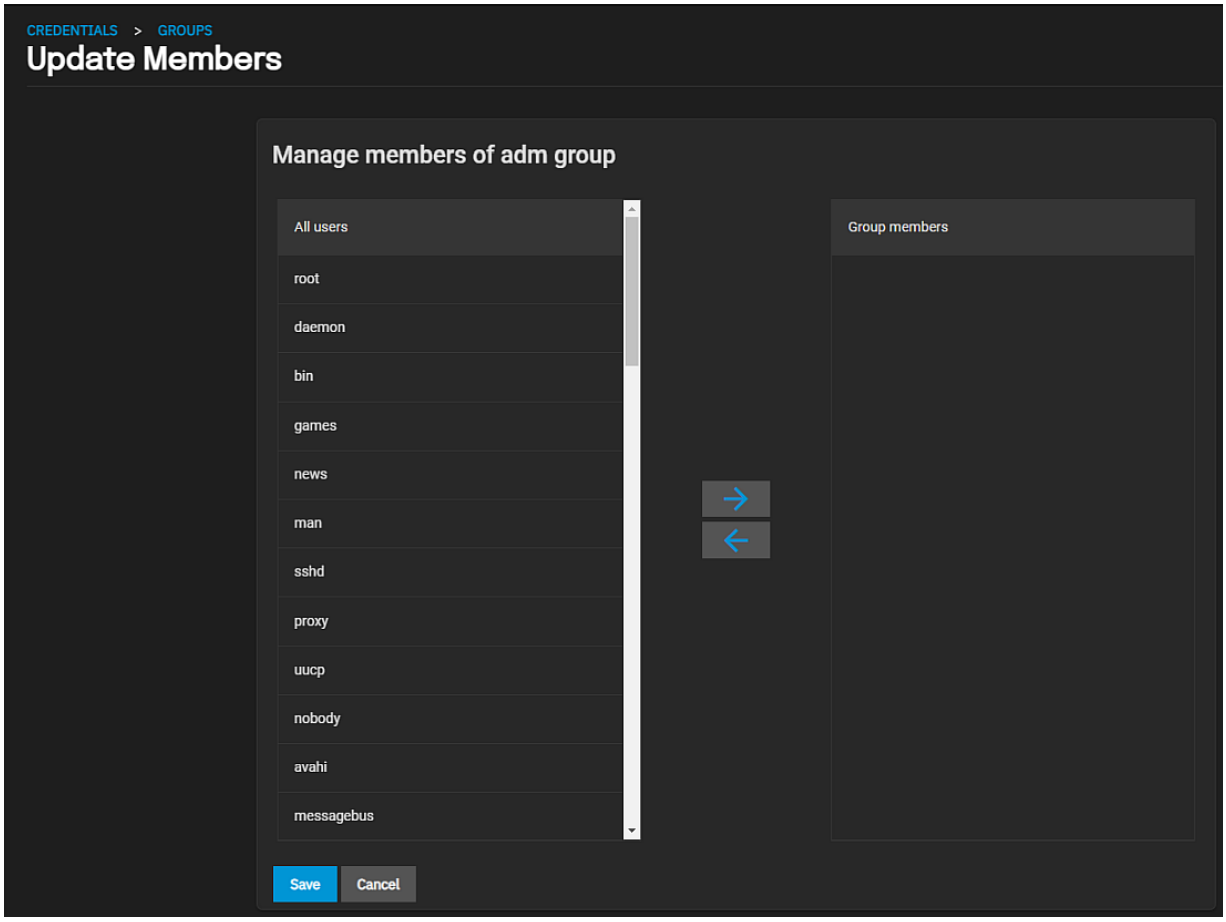


Setting	Description
GID	Required. Enter a unique number for the group ID (**GID**) TrueNAS uses to identify a Unix group. Enter a number above 1000 for a group with user accounts (you cannot change the GID later). If a system service uses a group, the group ID must match the default port number for the service.
Name	Required. Enter a name for the group. The group name cannot begin with a hyphen (-) or contain a space, tab, or any of these characters: colon (:), plus (+), ampersand (&), hash (#), percent (%), carat (^), open or close parentheses ( ), exclamation mark (!), at symbol (@), tilde (~), asterisk (*), question mark (?) greater or less than (<) (>), equal). You can only use the dollar sign ($) as the last character in a user name.

Setting	Description
Permit Sudo	Select to give this group administrator permissions and the ability to use sudo. When using sudo, a group is prompted for their account password. Leave **Permit Sudo** checkbox clear for better security.
Samba Authentication	Select to allow Samba permissions and authentication to use this group.
Allow Duplicate GIDs	Not recommended. Select to allow more than one group to have the same group ID.

Update Members Screen

Use the **Update Members** screen to manage group permissions and access for large numbers of user accounts.



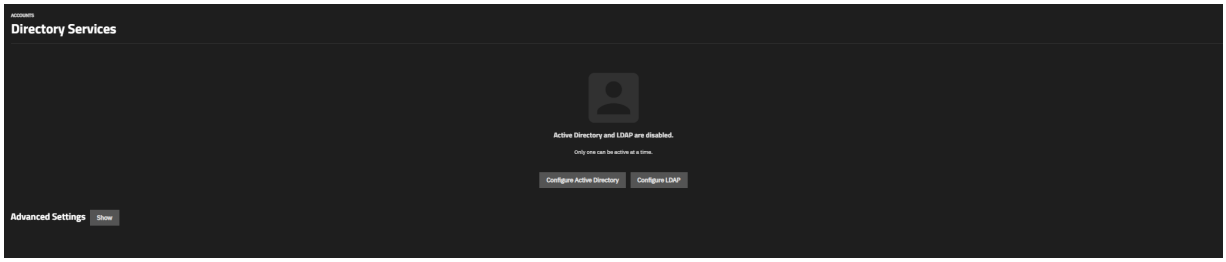
To add user accounts to the group, select users and then click ➔. Select **All Users** to move all users to the selected group, or select multiple users by holding `Ctrl` while clicking each entry.

Related Content

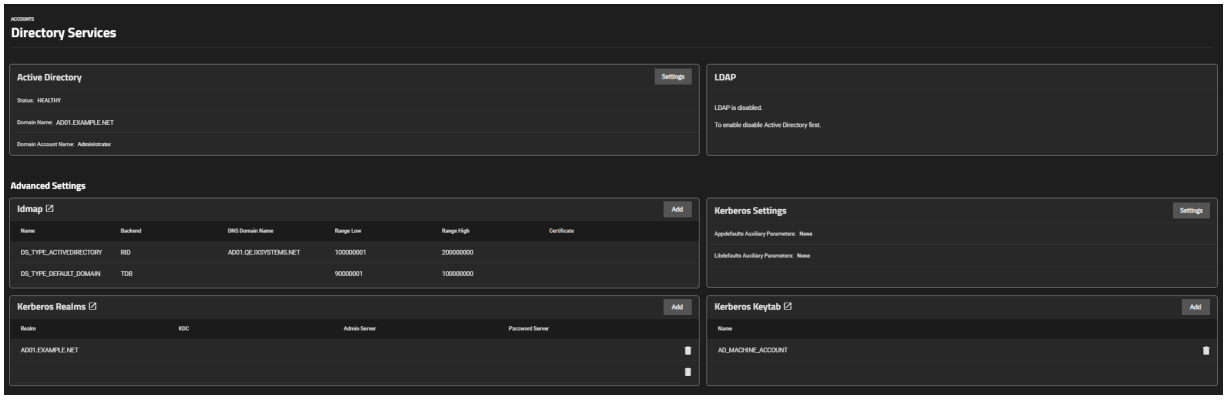
- Managing Local Groups

4.7.3 - Directory Services

The SCALE Directory Services section contains options to edit directory domain and account settings, set up Idmapping, and configure authentication and authorization services in TrueNAS SCALE.



The Directory Services screen is mostly empty until you connect TrueNAS to either an Active Directory or an LDAP server.



To display Kerberos settings, click **Show** next to Advanced Settings.

> Changing Advanced settings can be dangerous when done incorrectly. Please use caution before saving.

Article Summaries

- Active Directory

  Basic Options Advanced Options Click Configure Active Directory in Credentials > Directory Services to open the Active Directory form. Basic Options Setting Description Domain Name Enter the Active Directory domain (example.com) or child domain (sales.example.com). Domain Account Name Enter the Active Directory administrator account name. Domain Account Password Password for the Active Directory administrator account.

- LDAP

  Basic Options Advanced Options Click Configure LDAP in Credentials > Directory Services to open the LDAP form. Basic Options Setting Description Hostname LDAP server hostnames/IP addresses. Separate entries with Space. You can enter multiple hostnames/IP addresses to create an LDAP failover priority list. If a host does not respond, TrueNAS will try the next host until it establishes a connection.

- Idmap

  Options Click an Idmap name to edit an Idmap, or click Add in the Credentials > Directory Services Idmap widget to open the Idmap form. Setting Description Name Enter the pre-Windows 2000 domain name. Idmap Backend Provides a plugin interface for Winbind to use varying backends to store SID/uid/gid mapping tables.

- Kerberos Settings

  Click an Settings in the Credentials > Directory Services Kerberos Settings widget to open the Kerberos Settings form. Setting Description Appdefaults Auxiliary Parameters Additional Kerberos application settings. See the “appdefaults” section of [krb.conf(5)]. for available settings and usage syntax. Libdefaults Auxiliary Parameters Additional Kerberos library settings. See the “libdefaults” section of [krb.conf(5)]. for available settings and usage syntax.

- Kerberos Realms

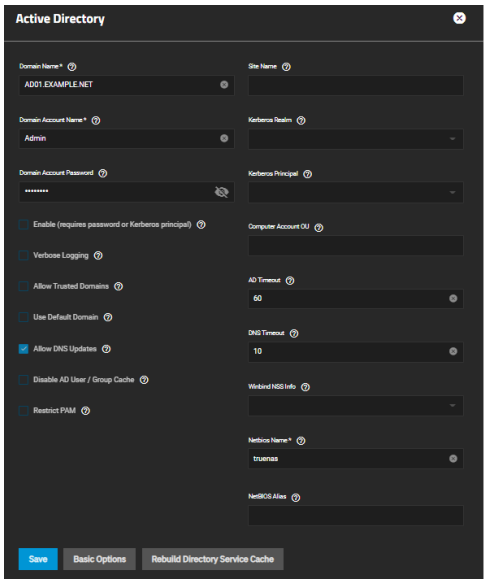
  Click a Kerberos Realm name to edit a Kerberos Realm, or click Add in the Credentials > Directory Services Kerberos Realms widget to open the Kerberos Realms form. Setting Description Realm Enter the name of the realm. KDC Enter the name of the Key Distribution Center. Separate multiple values by pressing Enter. Admin Server Define the server that performs all database changes.

- Kerberos Keytab

Click a Kerberos Keytab name to edit a Kerberos Realm, or click Add in the Credentials > Directory Services Kerberos Keytab widget to open the Kerberos Keytab form. Setting Description Name Enter a name for this Keytab. Kerberos Keytab Browse to the keytab file to upload.

4.7.3.1 - Active Directory

Click **Configure Active Directory** in **Credentials > Directory Services** to open the **Active Directory** form.



Basic Options

Setting	Description
Domain Name	Enter the Active Directory domain (example.com) or child domain (sales.example.com).
Domain Account Name	Enter the Active Directory administrator account name.
Domain Account Password	Password for the Active Directory administrator account. Required the first time a domain is configured. After initial configuration, the password is not needed to edit, start, or stop the service.
Enable (requires password or Kerberos principal)	Enable the Active Directory service. The first time this option is set, the Domain Account Password must be entered.

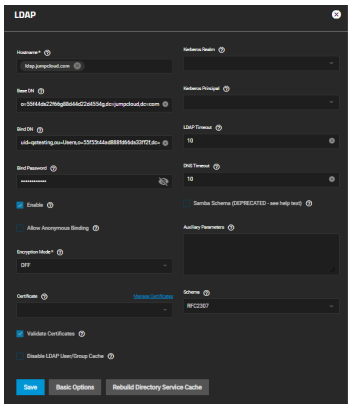
Advanced Options

Setting	Description
Verbose Logging	Logs attempts to join the domain in /var/log/messages.
Allow Trusted Domains	When selected, usernames do not include a domain name. Clear to prepend domain names to user names. Clearing this option prevents username collisions when there are identical usernames across multiple domains.
Use Default Domain	Unset to prepend the domain name to the username and prevent name collisions when using Allow Trusted Domains with the same username across multiple domains.
Allow DNS Updates	Enables Samba to do DNS updates when joining a domain.
Disable AD User/Group Cache	Disables caching AD users and groups, which can help when unable to bind to a domain with a lot of users or groups.
Restrict PAM	Restricts SSH access to BUILTIN\Administrators members in certain circumstances.
Site Name	Enter the relative distinguished name of the site object in the Active Directory.
Kerberos Realm	Select an existing realm from *Kerberos Realms*.
Kerberos Principal	Select the location of the principal in the keytab created in Directory Services > Kerberos Keytabs.
Computer Account OU	The OU that creates new computer accounts. TrueNAS reads the OU string from top to bottom without RDNs. Uses forward slashes (/) as delimiters, like Computers/Servers/NAS. Use backslashes (\) to escape

Setting	Description
	characters but not as a separator. TrueNAS interprets backslashes at multiple levels, so you might have to use several for them to work. When this field is blank, TrueNAS creates new computer accounts in the AD default OU.
AD Timeout	Number of seconds before timeout. To view the AD connection status, open the interface Task Manager.
DNS Timeout	Number of seconds before a timeout. Increase this value if AD DNS queries time out.
Winbind NSS Info	Choose the schema to use when querying AD for user/group info. *rfc2307* uses the Windows 2003 R2 schema support, *sfu* is for Service For Unix 3.0 or 3.5, and *sfu20* is for Service For Unix 2.0.
Netbios Name	Netbios Name of this NAS. This name must differ from the Workgroup name and be no greater than 15 characters.
NetBIOS Alias	Alternative names (no greater than 15 characters) that SMB clients can use when connecting to this NAS. Can be no greater than 15 characters.
Leave Domain	Disconnects the TrueNAS system from the Active Directory.

4.7.3.2 - LDAP

Click **Configure LDAP** in **Credentials > Directory Services** to open the **LDAP** form.



Basic Options

Setting	Description
Hostname	LDAP server hostnames/IP addresses. Separate entries with `Space`. You can enter multiple hostnames/IP addresses to create an LDAP failover priority list. If a host does not respond, TrueNAS will try the next host until it establishes a connection.
Base DN	Top level of the LDAP directory tree to be used when searching for resources. Example: dc=test,dc=org.
Bind DN	Administrative account name on the LDAP server. Example: cn=Manager,dc=test,dc=org.
Bind Password	Password for the Bind DN.
Enable	Activates the configuration. Unset to disable the configuration without deleting it. You can re-enable it later without reconfiguring it.

Advanced Options

Setting	Description
Allow Anonymous Binding	Set for the LDAP server to disable authentication and allow read and write access to any client.
Encryption Mode	Options for encrypting the LDAP connection: *OFF*: do not encrypt the LDAP connection. *ON*: encrypt the LDAP connection with SSL on port 636. *START_TLS*: encrypt the LDAP connection with STARTTLS on the default LDAP port *389*.
Certificate	Certificate to use when performing LDAP certificate-based authentication. To configure LDAP certificate-based authentication, create a Certificate Signing Request for the LDAP provider to sign. TrueNAS does not need a certificate when using username/password or Kerberos authentication. To configure LDAP certificate-based authentication, create a Certificate Signing Request for the LDAP provider to sign.
Validate Certificates	Verify certificate authenticity.
Disable LDAP User/Group Cache	Disable caching LDAP users and groups in large LDAP environments. When caching is disabled, LDAP users and groups do not appear in drop-down menus but are still accepted when manually entered.
Kerberos Realm	Select an existing realm from *Kerberos Realms*.
Kerberos Principal	Select the location of the principal in the keytab created in *Kerberos Keytab*.
LDAP Timeout	LDAP timeout in seconds. Increase this value if a Kerberos ticket timeout occurs.
DNS Timeout	DNS timeout in seconds. Increase this value if DNS queries timeout.
Samba Schema (DEPRECATED - see help text)	Only set if you configured the LDAP server with Samba attributes and it requires LDAP authentication for SMB shares.

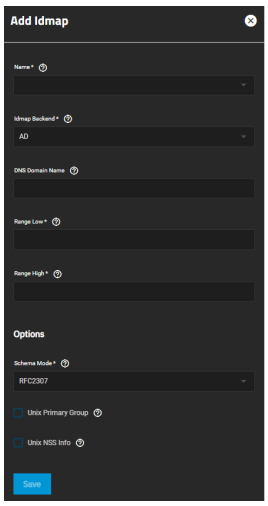
Setting	Description
Auxiliary Parameters	You can specify additional options for nslcd.conf.
Schema	Schema to use with Samba Schema.

> **DEPRECATED:** Samba Schema support is deprecated in Samba 4.13. We will remove this feature after Samba 4.14. Users should begin upgrading legacy Samba domains to Samba AD domains.

4.7.3.3 - Idmap

- Options

Click an **Idmap** name to edit an Idmap, or click **Add** in the **Credentials > Directory Services Idmap** widget to open the **Idmap** form.



Setting	Description
Name	Enter the pre-Windows 2000 domain name.
Idmap Backend	Provides a plugin interface for Winbind to use varying backends to store SID/uid/gid mapping tables. The correct setting depends on the environment you deployed the NAS in.
DNS Domain Name	DNS name of the domain.
Range Low	Range Low and Range High set the range of UID/GID numbers the IDMap backend translates. If an external credential like a Windows SID maps to a UID or GID number outside this range, TrueNAS will ignore it.
Range High	Range Low and Range High set the range of UID/GID numbers the IDMap backend translates. If an external credential like a Windows SID maps to a UID or GID number outside this range, TrueNAS will ignore it.

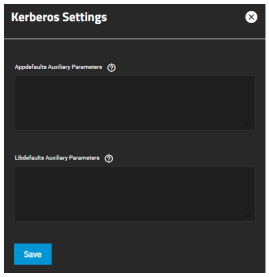
Options

Some options only display when either adding or editing an Idmap.

Setting	Description
Schema Mode	Choose the schema to use with LDAP authentication for SMB shares. The LDAP server must be configured with Samba attributes to use a Samba Schema. Options include RFC2307 (included in Windows 2003 R2) and Service for Unix (SFU). For SFU 3.0 or 3.5, choose “SFU”. For SFU 2.0, choose “SFU20”.
Unix Primary Group	When checked, the primary group membership is fetched from the LDAP attributes (gidNumber). When not checked, the primary group membership is calculated via the “primaryGroupID” LDAP attribute.
Unix NSS Info	When checked, winbind will retrieve the login shell and home directory from the LDAP attributes. When not checked or when the AD LDAP entry lacks the SFU attributes the smb4.conf parameters `template shell` and `template homedir` are used.
SSSD Compat	Generate Idmap low range based on the same algorithm that SSSD uses by default.

4.7.3.4 - Kerberos Settings

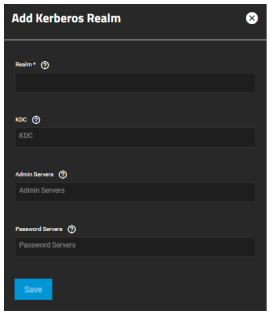
Click an **Settings** in the **Credentials > Directory Services Kerberos Settings** widget to open the **Kerberos Settings** form.



Setting	Description
Appdefaults Auxiliary Parameters	Additional Kerberos application settings. See the “appdefaults” section of [krb.conf(5)]. for available settings and usage syntax.
Libdefaults Auxiliary Parameters	Additional Kerberos library settings. See the “libdefaults” section of [krb.conf(5)]. for available settings and usage syntax.

4.7.3.5 - Kerberos Realms

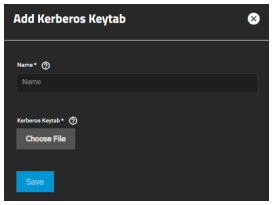
Click a **Kerberos Realm** name to edit a Kerberos Realm, or click **Add** in the **Credentials > Directory Services Kerberos Realms** widget to open the **Kerberos Realms** form.



Setting	Description
Realm	Enter the name of the realm.
KDC	Enter the name of the Key Distribution Center. Separate multiple values by pressing `Enter`.
Admin Server	Define the server that performs all database changes. Separate multiple values by pressing `Enter`.
Password Server	Define the server that performs all password changes. Separate multiple values by pressing `Enter`.

4.7.3.6 - Kerberos Keytab

Click a **Kerberos Keytab** name to edit a Kerberos Realm, or click **Add** in the **Credentials > Directory Services Kerberos Keytab** widget to open the **Kerberos Keytab** form.

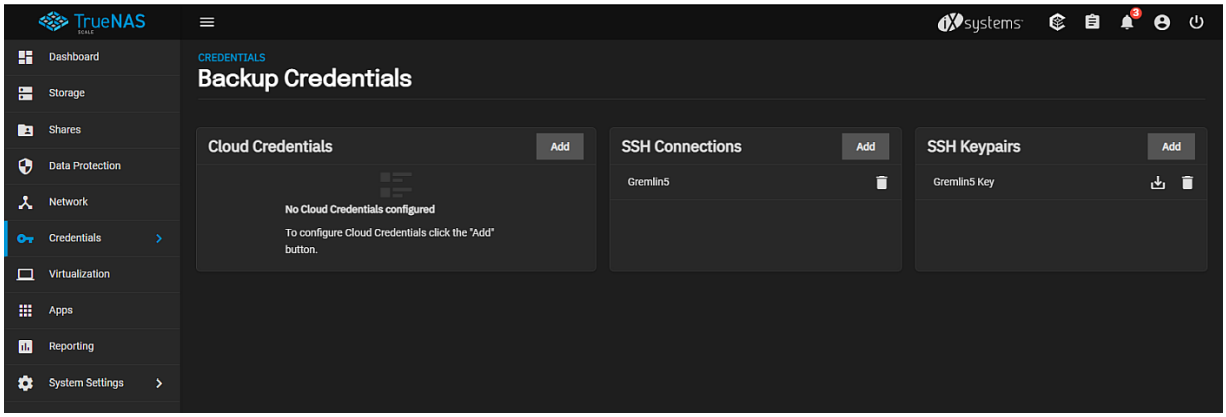


Setting	Description
Name	Enter a name for this Keytab.
Kerberos Keytab	Browse to the keytab file to upload.

4.7.4 - Backup Credentials

This article provides infomation on backup credential screens and settings to integrate TrueNAS with cloud storage providers by setting up SSH connections and keypairs.

TrueNAS stores cloud backup services credentials, SSH connections, and SSH keypairs configured using the widgets on the **Backup Credentials** screen. Users can set up backup credentials with cloud and SSH clients to back up data in case of drive failure.



Article Summaries

- Cloud Credentials Screens

  This article provides information on Cloud Credentials widget, screens, and settings.

- SSH Screens

  This article provides information on the SSH Connections and SSH Keypairs screen widgets and settings.

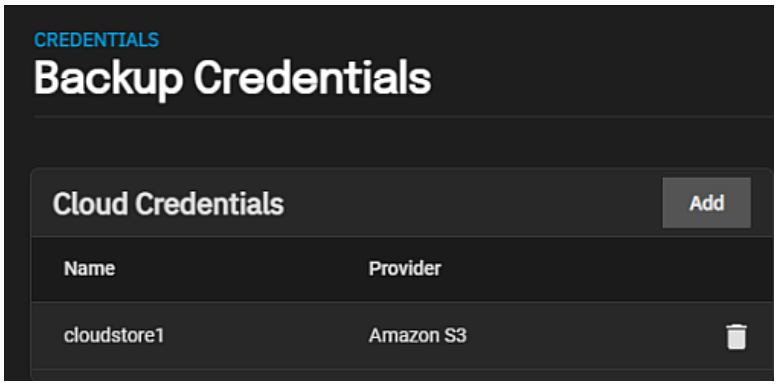
4.7.4.1 - Cloud Credentials Screens

This article provides information on Cloud Credentials widget, screens, and settings.

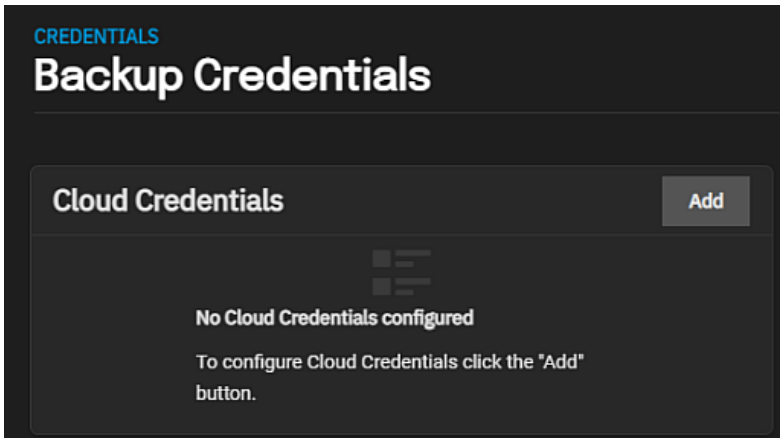
The **Backup Credentials** screen displays the **Cloud Credentials**, **SSH Connections** and **SSH Keypairs** widgets.

Cloud Credentials Widget

The **Cloud Credentials** widget displays a list of cloud storage credentials configured on the system.



Before adding cloud credentials for a cloud storage provider, the **Cloud Credentials** widget displays **No Cloud Credentials configured**.

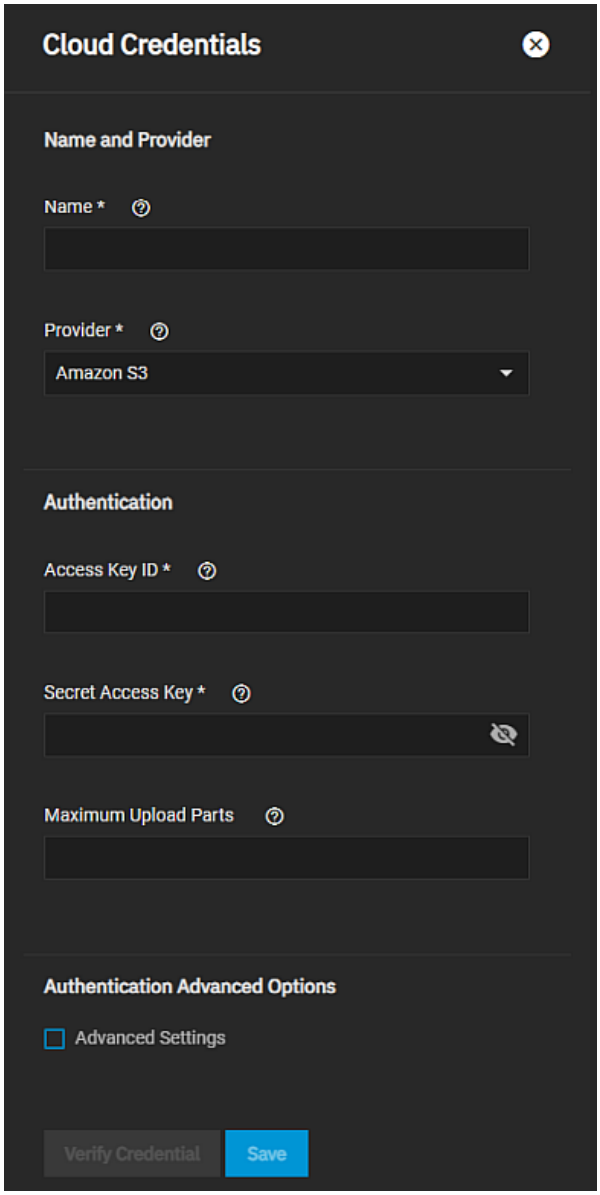


Add opens the **Cloud Credentials** configuration screen.

Click the name of a cloud credential to open the **Cloud Credentials** configuration screen populated with the settings for that credential.

Cloud Credentials Screen

The **Cloud Credentials** configuration screen displays settings to add or edit cloud credentials TrueNAS uses to integrate with cloud storage providers.



Use **Verify Credentials** after entering the authentication settings to verify you can access the cloud storage provider account with the credentials you entered.

Name and Provider Settings

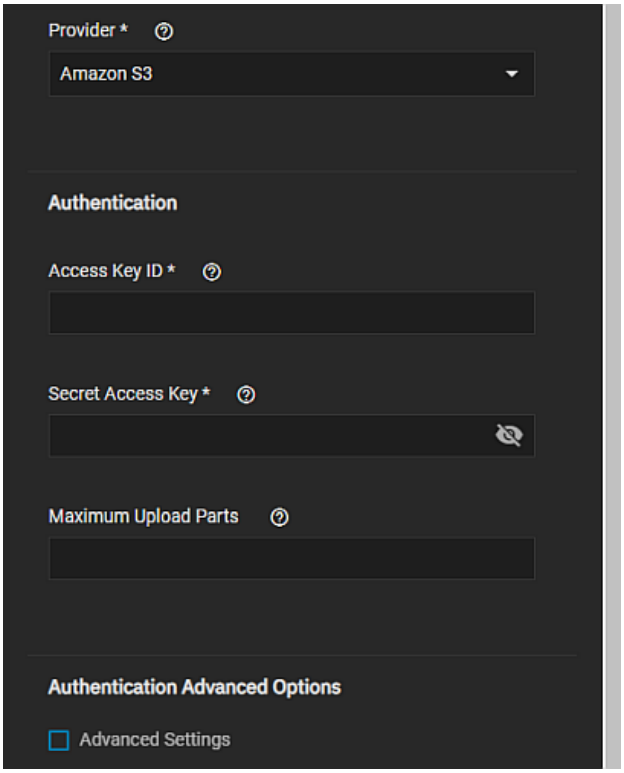
The **Authentication** settings change based on the selection in **Provider**.

Name	Description
Name	Enter a name for this cloud credential. For example, *cloud1* or *amazon1*.
Provider	Required. Default is set to **Amazon S3**. Select the cloud storage provider from the options on the dropdown list.

Amazon S3 Authentication Settings

Amazon S3 has basic authentication and advanced authentication settings. This section provides information on the basic authentication settings.

Click Here for Settings

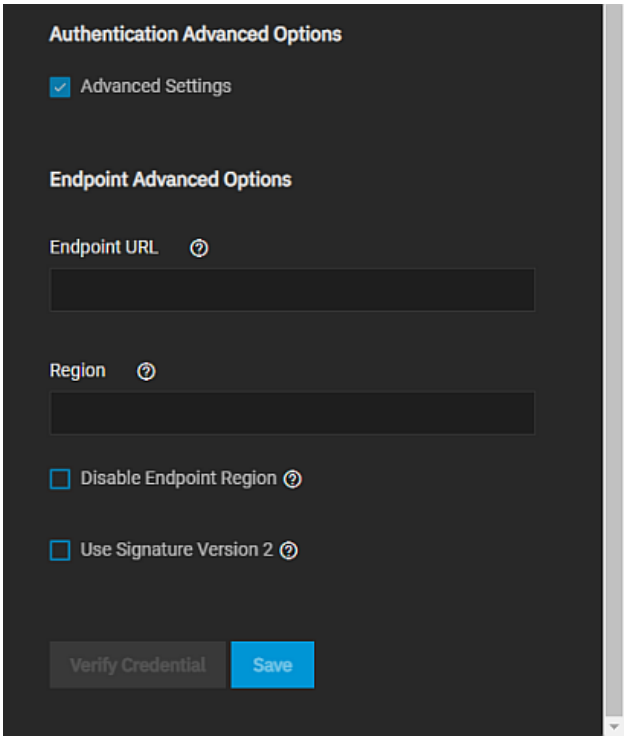


Name	Description
Access Key ID	Enter the alphanumeric key that is between 5 and 20 characters for the Amazon Web Services Key ID. Find this on Amazon AWS by going through **My account > Security Credentials > Access Keys** (Access Key ID and Secret Access Key).
Secret Access Key	Enter the alphanumeric key that is between 8 and 40 characters for the Amazon Web Services password. If you cannot find the Secret Access Key, go to **My Account > Security Credentials > Access Keys** and create a new key pair.
Maximum Upload Ports	Enter a value to define the maximum number of chunks for a multipart upload. Setting a maximum is necessary if a service does not support the 10,000 chunk AWS S3 specification.
Advanced Settings	Select to display the optional **Endpoint Advanced Options** settings.

Amazon S3 Advanced Authentication Options

This section provides information on Amazon S3 advanced authentication settings for endpoints. The basic authentication settings are required when using the advanced settings.

Click Here for Settings

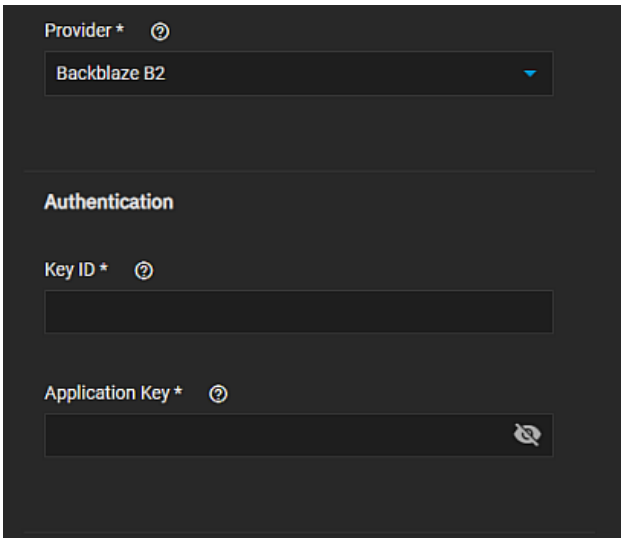


Name	Description
Endpoint URL	Optional. When using AWS, you can leave the endpoint field empty to use the default endpoint for the region and automatically fetch available buckets, or enter an S3 API endpoint URL. Refer to the AWS Documentation for a list of Simple Storage Service Website Endpoints.
Region	Optional. Enter an AWS resources in a geographic area. Leave empty to detect the correct public region for the bucket. Entering a private region name allows interacting with Amazon buckets created in that region. For example, enter *us-gov-east-1* to discover buckets created in the eastern AWS GovCloud region.
Disable Endpoint Region	Select to skip automatic detection of the endpoint URL region and to configuring a custom Endpoint URL.
User Signature Version 2	Select to force using Signature Version 2 to sign API requests. Select this when configuring a custom Endpoint URL.

BackBlaze B2 Authentication Settings

This section provides information on the BackBlaze B2 authentication settings.

Click Here for Settings

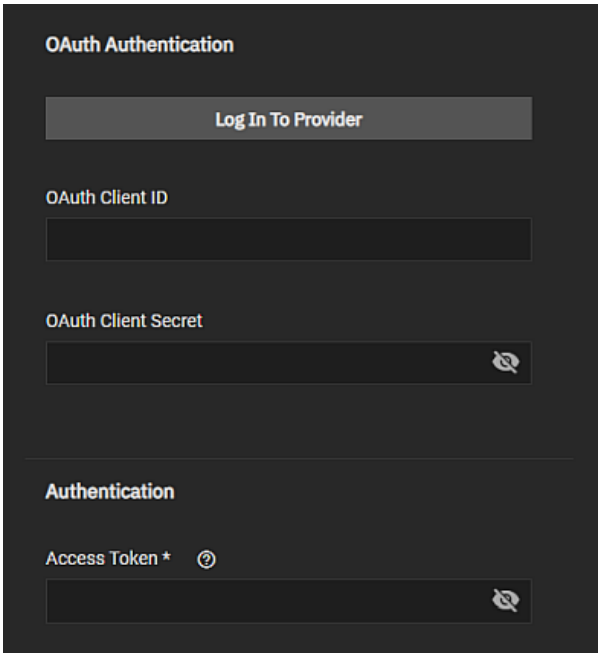


Name	Description
Key ID	Enter or copy and paste the alphanumeric Backblaze B2 Application Key ID string into this field. To generate a new application key, log in to the Backblaze account, go to the **App Keys** page, and add a new application key.
Application Key	Enter or copy and paste the alphanumeric Backblaze B2 Application Key string into this field. To generate a new application key, log in to the Backblaze account, go to the **App Keys** page, and add a new application key.

OAuth and Access Token Authentication Settings

Several cloud storage providers use OAuth authentication and a required access token to authenticate the cloud storage account. Providers that use these methods are Box, Dropbox, Google Photo, pCloud, and Yandex.

Click here for Settings



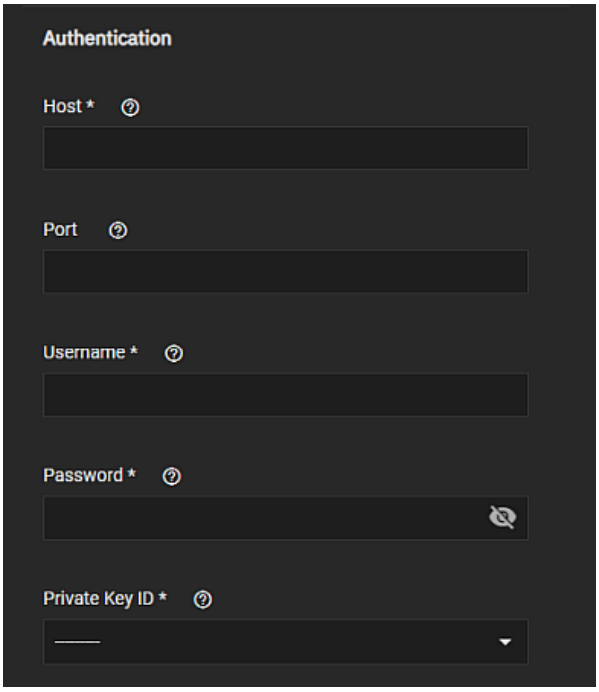
Name	Description
OAuth Client ID	Enter the public identifier for the cloud application.
OAuth Client Secret	Enter the secret phrase known only to the cloud application and the authorization server.
Access Token	Enter a User Access Token for Box. An access token enables Box to verify a request belongs to an authorized session. Example token: T9cE5asGnuyYCCqIZFoWjFHvNbvVqHjl.
Hostname	pCloud only. Optional. Enter the host name to connect to.

Use **Login to Provider** to enter the account username and password.

FTP and SMTP Authentication Settings

FTP and SMTP cloud storage providers use host name, port, and user credentials to authenticate accounts. SMTP uses SSH hosts, port, and user credentials and also uses a private key.

Click Here for Settings



Name	Description
Host	Enter the FTP host name or for SMTP the SSH host name to connect. For example, *ftp.example.com*.
Port	Enter the FTP or for SMTP, the SSH port number. Leave blank to use the default port **21** for FTP or **22** for SMTP.
Username	Enter a username on the FTP or for the SMTP host system the SSJ user name. This user must already exist on the host.
Password	Enter the password for the user account.
Private Key ID	SNMP only. Import the private key from an existing SSH keypair or, if no keypairs exist on the system, select **Add** on the **SSH Keypairs** widget to open the **SSH Keypairs** screen. Enter a name, and then click **Generate New** to create a new SSH key for this credential.

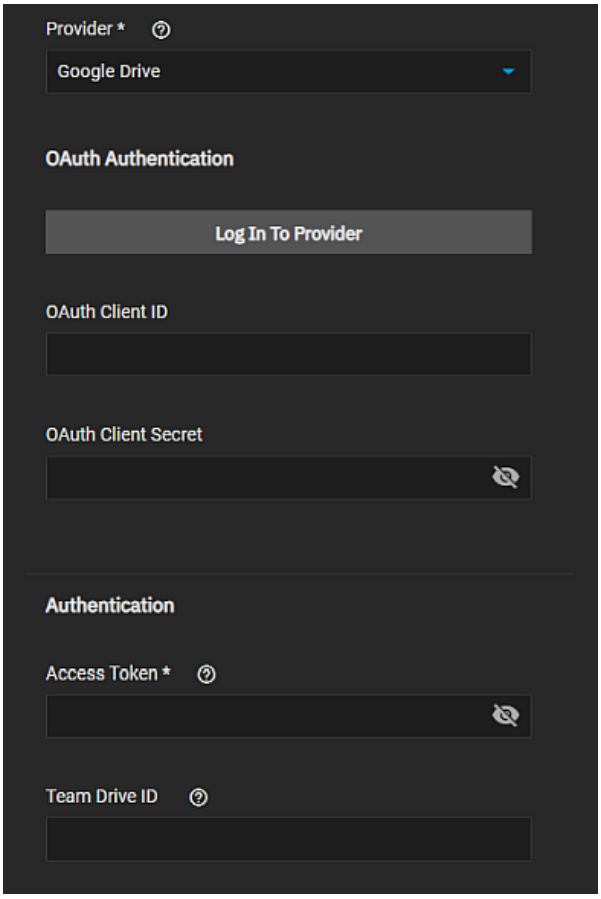
Google Cloud Storage Authentication Settings

Google Cloud Storage authentication uses a Google service account json key credential file generated by the Google Cloud Platform Console to authenticate the account. Obtain the json file, download it to the system server and then upload it to the **Preview JSON Service Account Key** field. Use **Choose File** to browse to the file location on the server.

Google Drive Authentication Settings

Google Drive uses OAuth authentication, a required access token, and a team drive ID to authenticate accounts.

Click Here for Settings



Name	Description
OAuth Client ID	Enter the public identifier for the cloud application.
OAuth Client Secret	Enter the secret phrase known only to the cloud application and the authorization server.
Access Token	Required. Token created with Google Drive. Access Tokens expire periodically, so you must refresh them.
Team Drive ID	Optional. Only needed when connecting to a Team Drive, and is the top-level folder ID for the Team Drive.

Use **Login to Provider** to enter the account username and password.

HTTP Authentication Settings

HTTP uses a HTTP host URL to authenticate account credentials.

Hubic Authentication Settings

Hubic uses an access token to authenticate the account. Enter the token generated by a Hubic account into the **Access Token** field.

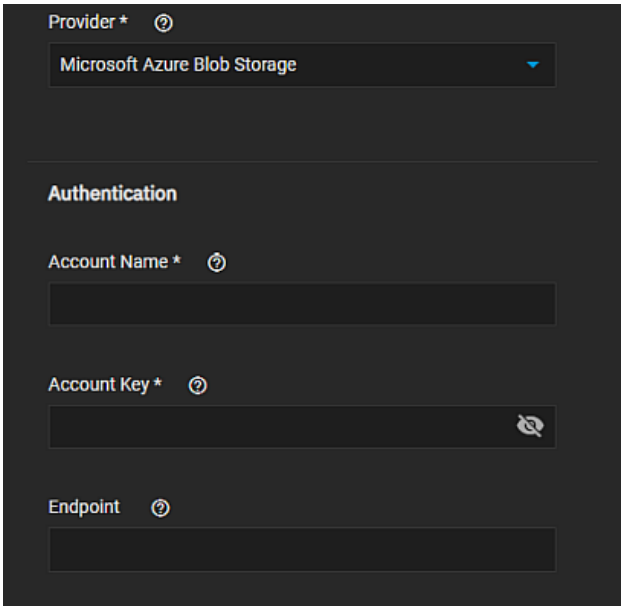
Mega Authentication Settings

Mega uses the username and password for the MEGA user account to authenticate the account credentials.

Microsoft Azure Blob Storage Authentication Settings

Microsoft Azure Blob Storage uses the Microsoft Azure account name and account key to authenticate the account credentials.

Click Here for Settings

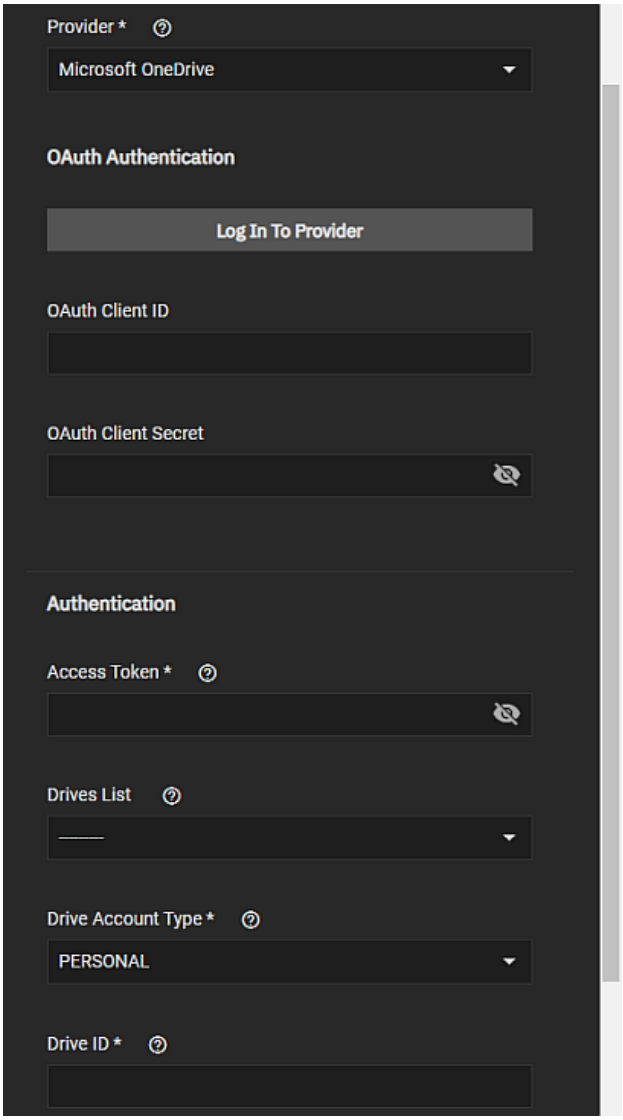


Name	Description
Account Name	Enter the Microsoft Azure account name.
Account Key	Enter the base64 encoded key for Azure account.
Endpoint	Enter an endpoint. For example, *blob.core.usgovcloudapi.net*.

Microsoft OneDrive Authentication

Microsoft OneDrive uses OAuth authentication, access tokens, drives and drive account type and ID to authenticate account credentials.

Click Here for Settings



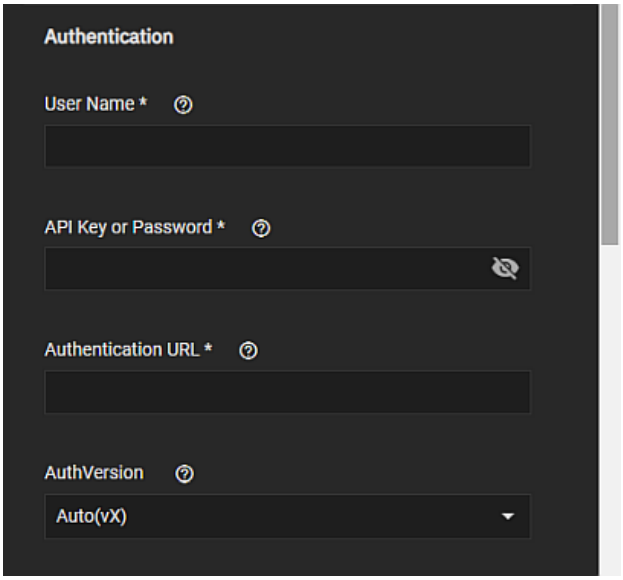
Name	Description
OAuth Client ID	Enter the public identifier for the cloud application.
OAuth Client Secret	Enter the secret phrase known only to the cloud application and the authorization server.
Access Token	Enter the Microsoft Onedrive access token. Log in to the Microsoft account to add an access token.
Drives List	Select the drives and IDs registered to the Microsoft account. Selecting a drive also populates the **Drive ID** field.
Drive Account Type	Select the type of Microsoft account from the dropdown options, **PERSONAL**, **BUSINESS**, or **DOCUMENT_LIBRARY**. Logging in to a Microsoft account selects the correct account type.
Drive ID	Enter the unique drive identifier if not pre-populated after selecting the drive in **Drives List**. Log in to a Microsoft account and choose a drive from the **Drives List** dropdown list to add a valid ID.

Use **Login to Provider** to enter the account username and password.

OpenStack Swift Authentication Settings

OpenStack Swift uses several required settings to authenticate credential accounts.

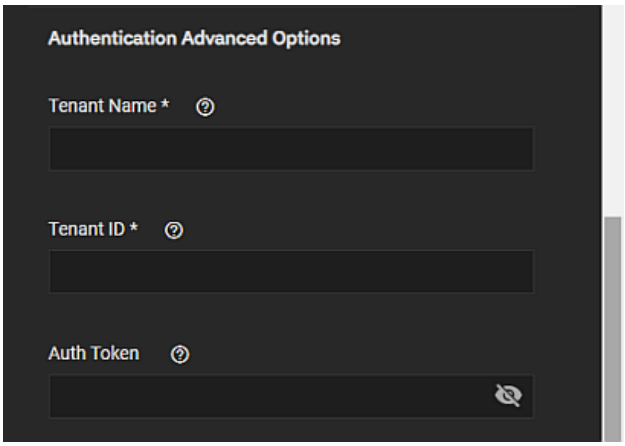
Click Here for Settings



Name	Description
User Name	Required. Enter the OpenStack user name (OS_USERNAME) from an OpenStack credentials file.
API Key or Password	Required. Enter the Openstack API key or password. This is the OS_PASSWORD from an OpenStack credentials file.
Authentication URL	Required. Enter the authentication URL for the server. This is the OS_AUTH_URL from an OpenStack credentials file.
AuthVersion	Select the authentication version from the dropdown list if your auth URL has no version (rclone documentation).

Authentication Advanced Options**

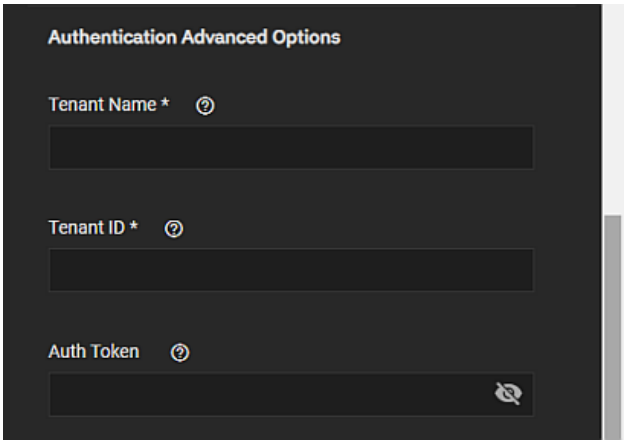
The **AuthVersion** option selected changes the settings displayed in **Authentication Advanced Options**. **Auto(vX)**, **v1**, and **v2** use the same advanced authentication settings but **V3** displays additional settings.



Name	Description
Tenant Name	Enter the OS_TENANT_NAME from an OpenStack credentials file.
Tenant ID	(Optional for v1 auth) Enter the tenant ID Enter the tenant ID. For more information see rclone documentation.
Auth Token	(Optional) Enter the auth token from alternate authentication. For more information see rclone documentation.

Authentication Advanced Options for v3**

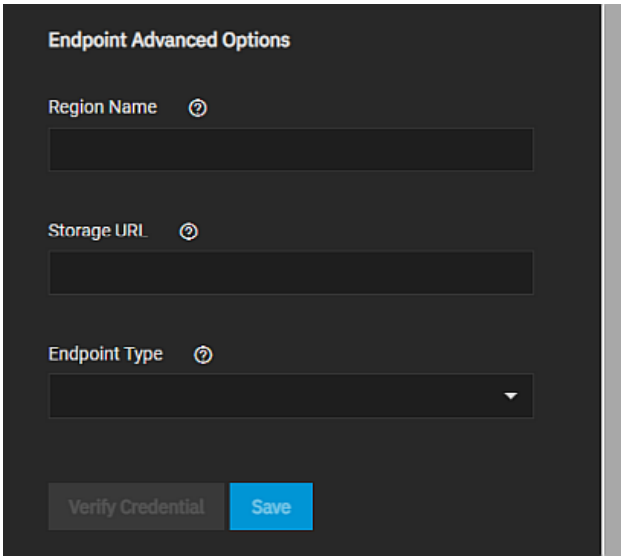
When **v3** is the **AuthVersion** option settings **Authentication Advanced Options** displays additional settings.



Name	Description
User Id	Optional. Enter the user ID to log in. To log into most swift systems leave this blank. For more information see rclone documentation.
User Domain	Optional. Enter the user domain. For more information see rclone documentation.
Tenant Name	Required. Enter the OS_TENANT_NAME from an OpenStack credentials file.
Tenant ID	Required for **v2** and **v3**. Enter the tenant ID. For more information see rclone documentation.
Tenant Domain	Optional. Enter the tenant domain. For more information see rclone documentation.
Auth Token	Optional. Enter the auth token from alternate authentication. For more information see rclone documentation.

Endpoint Advanced Options Settings

These settings apply to all OpenStack Swift credentials.

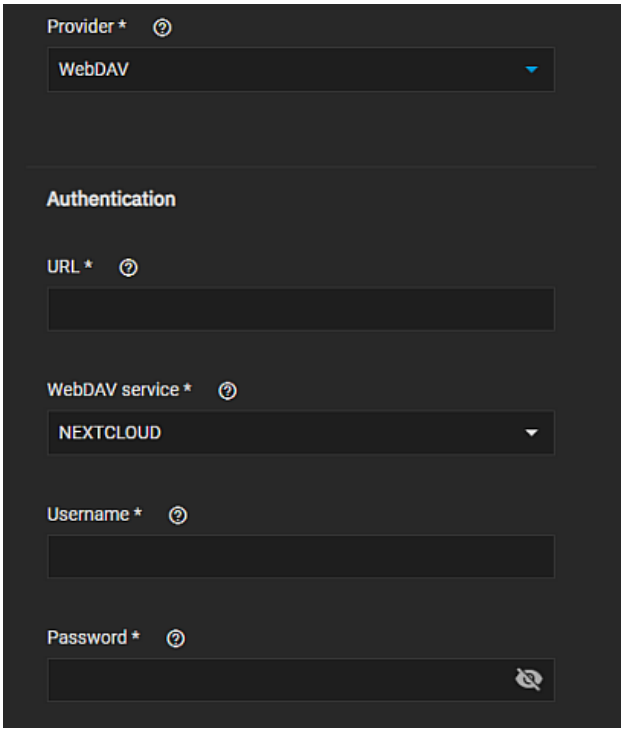


Name	Description
Region Name	Optional. Enter the region name. For more information see rclone documentation.
Storage URL	Optional. Enter the storage URL. For more information see rclone documentation.
Endpoint Type	Select service catalogue option from the **Endpoint Type** dropdown. Options are **Public**, **Internal** and **Admin**. **Public** is recommended. For more information see rclone documentation.

WebDAV Authentication Settings

WebDAV uses the URL, service type and user credentials to authenticate the account credentials.

Chick Here for Settings



Name	Description
URL	Required. Enter the URL of the HTTP host to connect to.
WebDAV Service	Required. Select the name of the WebDAV site, service, or software used from the dropdown list. Options are **NEXTCLOUD**, **OWNCLOUD**, **SHAREPOINT**, or **OTHER**.
Username	Required. Enter the WebDAV account user name.
Password	Required. Enter the WebDAV account password.

Related Content

- Adding Cloud Credentials
- Adding Cloud Sync Tasks
- Backing Up Google Drive to TrueNAS SCALE
- Cloud Sync Tasks
- Cloud Sync Tasks Screens

Related Backup Articles

- Adding Cloud Credentials
- Adding Cloud Sync Tasks
- Adding Replication Tasks
- Backing Up Google Drive to TrueNAS SCALE
- Managing the System Configuration
- Cloud Sync Tasks Screens
- Setting Up a Local Replication Task
- Setting Up Advanced Replication Tasks
- Backup Credentials

Related WebDAV Articles

- Adding Cloud Credentials
- Configuring WebDAV Shares
- WebDAV Shares Screens
- Configuring WebDAV Service
- WebDAV Service Screen

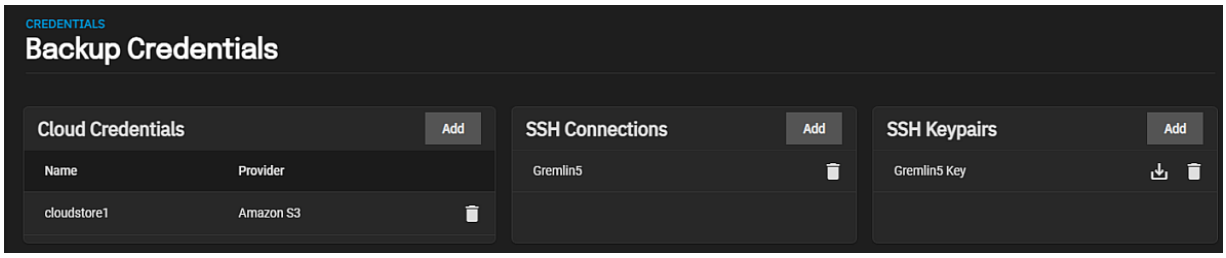
4.7.4.2 - SSH Screens

This article provides information on the SSH Connections and SSH Keypairs screen widgets and settings.

The **Backup Credentials** screen displays the **SSH Connections** and **SSH Keypairs** widgets.

SSH Connection and Keypairs Widgets

The **SSH Connections** and **SSH Keypairs** widgets display a list of SSH connections and keypairs configured on the system.



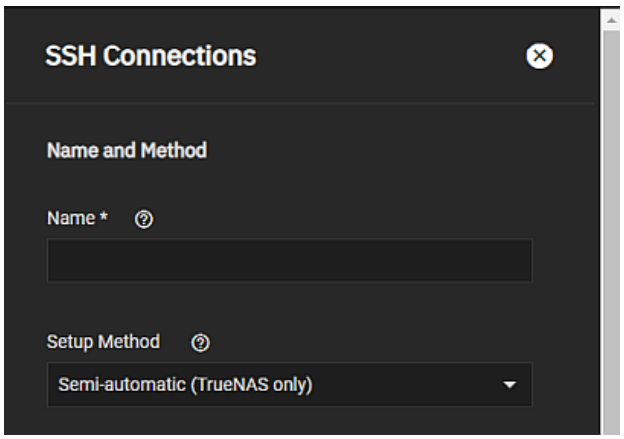
The **SSH Connections** widget allows users to establish Secure Socket Shell (SSH) connections. The **SSH Keypairs** widget allows users to generate SSH keypairs required to authenticate the identity of a user or process that wants to access the system using SSH protocol.

Add button in the **SSH Connections** widget opens the **SSH Connections** configuration window. The connection name on the widget is a link that opens the **SSH Connections** configuration screen already populated with the saved settings for the selected connection.

SSH Connections Screens

The settings displayed on the **SSH Connections** configuration screens are the same whether you add a new connection or edit an existing connection.

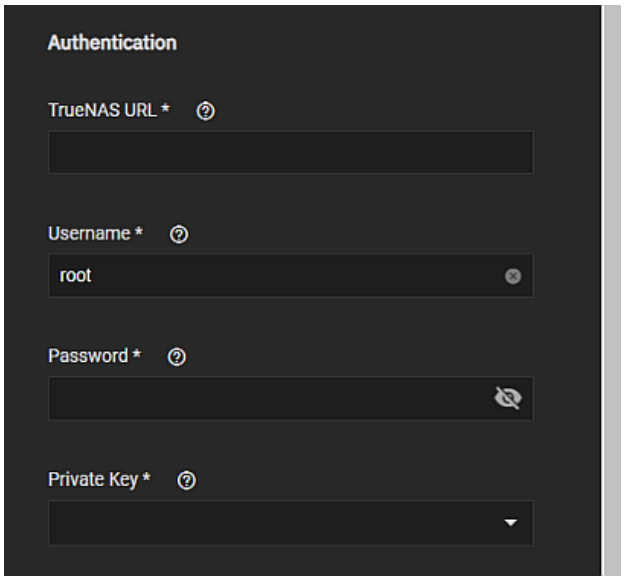
Name and Method Settings



Name	Description
Name	Required. Enter a unique name for this SSH connection. For example, use *ssh* and a server name or number like *sshsys1* or *sshtn121* where *sys1* or *tn121* are server designations.
Setup Method	Default is set to **Semi-automatic (TrueNAS only)**. Select **Semi-automatic (TrueNAS only)** to simplify setting up an SSH connection with another TrueNAS or FreeNAS system without logging into that system to transfer SSH keys. Select **Manual** to enter all settings when setting up an SSH connection with a non-TrueNAS server. Displays other setting options required to manually configure an SSH connection. Requires copying a public encryption key from the local system to the remote system. A manual setup allows a secure connection without a password prompt.

Authentication Settings - Semi-Automatic Method

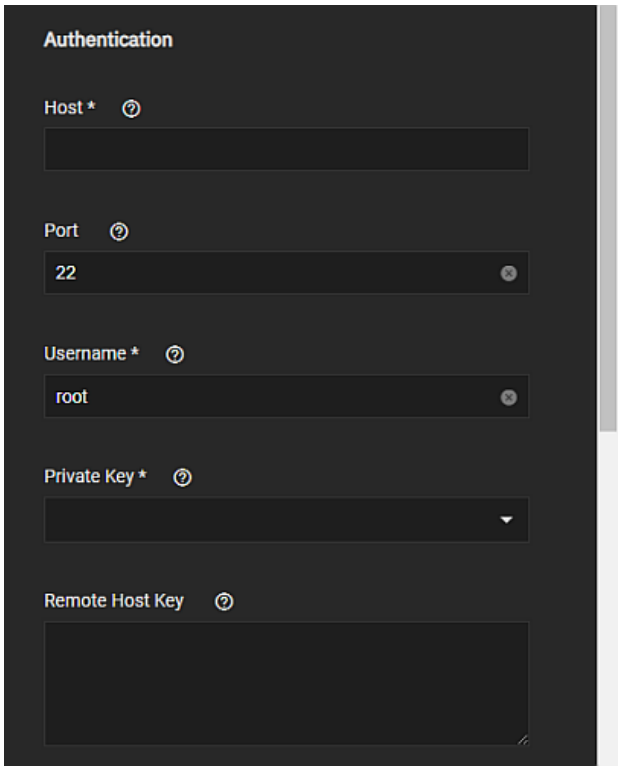
These authentication settings display when **Setup Method** is **Semi-automatic (TrueNAS only)**.



Name	Description
TrueNAS URL	Enter the host name or IP address of the remote system. Use a valid URL scheme for the remote TrueNAS URL. IP address example of *https://10.231.3.76*.
Username	Enter the user name for logging into the remote system.
Password	Enter the user account password for logging into the remote system.
Private Key	Select a saved SSH keypair or you can import the private key from a previously created SSH keypair or select **Generate New** to create a new keypair to use for the connection to this remote system.

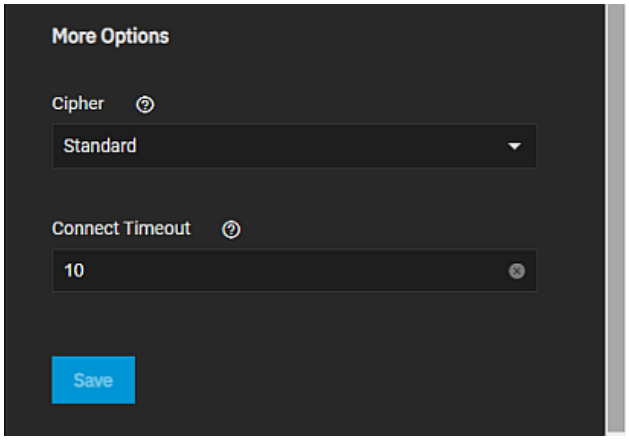
Authentication Settings - Manual Method

These authentication settings display when **Setup Method** is **Manual**. You must copy a public encryption key from the local system to the remote system. A manual setup allows a secure connection without a password prompt.



Name	Description
Host	Enter the host name or IP address of the remote system. A valid URL scheme is required. An IP address example is *https://10.231.3.76*.
Port	Enter the port number on the remote system to use for the SSH connection.
Username	Enter the user name for logging into the remote system.
Private Key	Select a saved SSH keypair or select **Generate New** to create a new keypair to use for the connection to this remote system.
Remote Host Key	Enter the remote system SSH key for this system to authenticate the connection. Click **Discover Remote Host Key** after properly configuring all other fields to query the remote system and automatically populate this field.
Discover Remote Host Key	Click to connect to the remote system and attempt to copy the key string to the related TrueNAS field.

More Options Settings

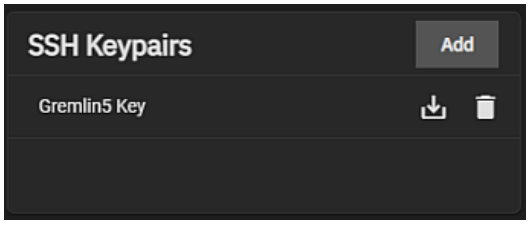


Name	Description
Cipher	Select the security option from the dropdown list. Select **Standard** for the most secure option, but with the greatest impact on connection speed. Select **Fast** for a less secure option than **Standard** but it can give reasonable transfer rates for devices with limited cryptographc speed. Select **Disabled** to remove all security in favor of maximizing connection speed. Only disable security when used within a secure, trusted network.
Connect Timeout	Enter time (in seconds) before the system stops attempting to establish a connection with the remote system.

Save automatically opens a connection to the remote TrueNAS and exchanges SSH keys.

SSH Keypairs Widget

The **SSH Keypairs** widget on the **Backup Credentials** screen lists SSH keypairs added to the TrueNAS SCALE system.



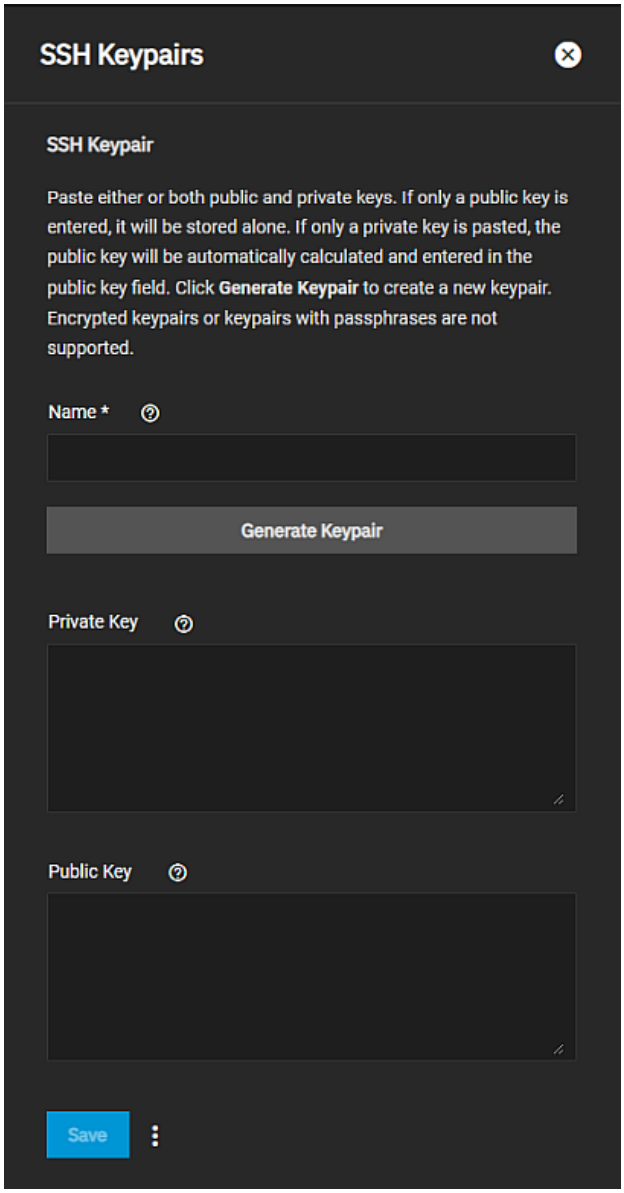
The name of the keypair listed on the widget is a link that opens the **SSH Keypairs** configuration screen.

The download icon, and the ⋮ at the bottom of the **SSH Keypairs** configuration screen, download the public and private key strings as text files for later use.

The 🗑 delete icon opens the a delete dialog. Click **Confirm** and then **Delete** to remove the stored keypairs from the system.

SSH Keypairs Screen

The **SSH Keypairs** configuration screen displays the same settings for both add and edit options. Click **Add** to open a new configuration form, or click on an existing keypair to open the configuration screen populated with the settings for the selected keypair.



Name	Description
Name	Required. Enter a unique name for this SSH keypair. Automatically generated keypairs are named after the object that generated the keypair with **key** appended to the name.
Generate Keypair	Click to have TrueNAS SCALE automatically generate a new keypair and populate the **Private Key** and **Public Keys** fields with these values.
Private Key	See **Authentication** in SSH/Authentication.
Public Key	See **Authentication** in SSH/Authentication

Save adds the keypair to the widget and activates the ⋮ with options to **Download Private Key** and **Download Public key**.

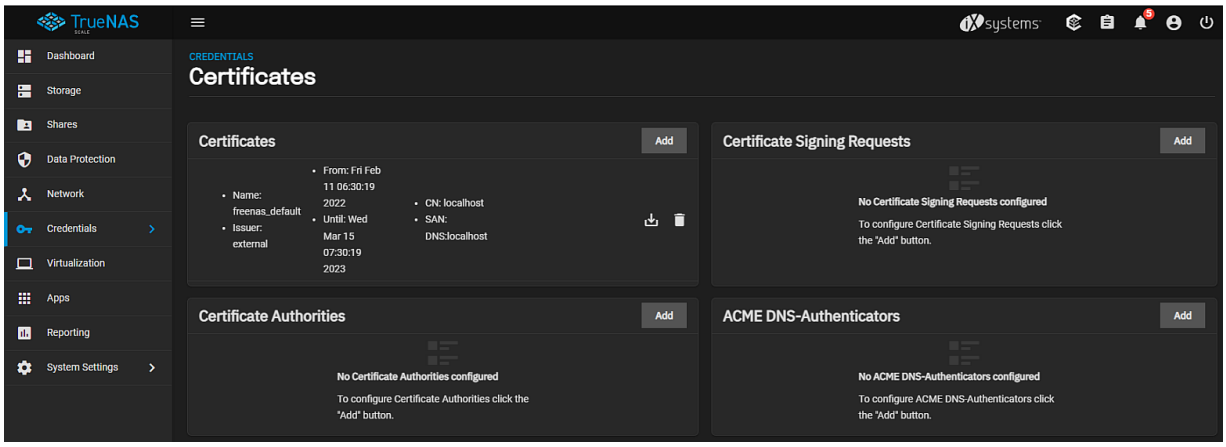
Related Content

- Adding SSH Credentials
- Configuring Rsync Tasks
- Rsync Tasks Screens
- Security Recommendations
- Configuring SSH Service
- SSH Service Screen
- Using 2FA (Two-Factor Authentication)

4.7.5 - Certificates

This article provides general information about the **Certificates** screen and widgets and article summaries.

The **Certificates** screen displays widgets for **Certificates**, **Certificate Signing Requests** (CSRs), **Certificate Authorities** (CA), and **ACME DNS-Authenticators** that each provice access to all the information for certificates, certificate signing requests (CSRs), certificate authorities (CA), and ACME DNS-authenticators respectively.



Each TrueNAS comes equipped with an internal, self-signed certificate that enables encrypted access to the web interface, but users can make custom certificates for authentication and validation while sharing data.

Article Summaries

- Certificates Screens

  This article provides information on SCALE certificates screens and settings.

- Certificates Authorities Screens

  This article provides information on SCALE certificate authroities screens and settings.

- Certificate Signing Requests Screens

  This article provides information on SCALE certificates signing request screens and settings.

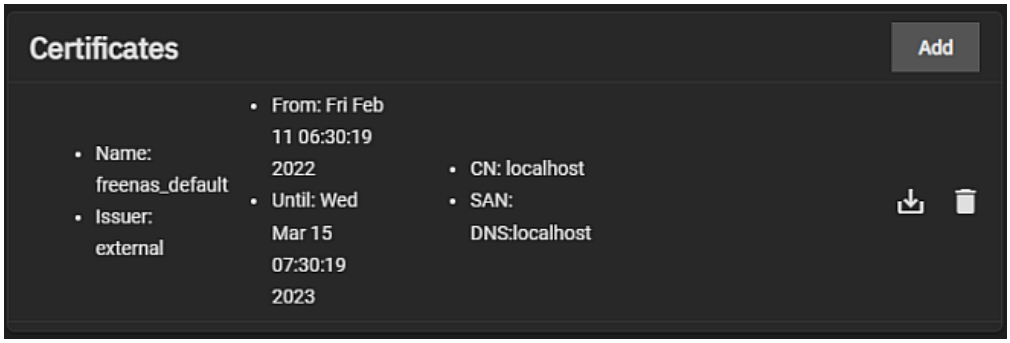
- ACME DNS-Authenticators Screens

  This article provides information on SCALE Certificates screens and settings.

4.7.5.1 - Certificates Screens

This article provides information on SCALE certificates screens and settings.

The **Certificates** widget on the **Credentials > Certificates** screen displays certificates added to SCALE, and allows you to add new certificates, or download, delete, or edit the name of an existing certificate. Each TrueNAS comes equipped with an internal, self-signed certificate that enables encrypted access to the web interface.



The download icon downloads the certificate to your server.

deletes the certificate from your server.

Each certificate listed on the widget is a link that opens the **Edit Certificate screen.

Add opens the **Add Certificate** wizard.

Add Certificate Wizard

The **Add Certificate** wizard screens step users through configuring a new certificate on TrueNAS SCALE. The wizard has five different configuration screens, one for each step in the certificate configuration process:

1 **Identifier and Type**

2 **Certificate Options**

3 **Certificate Subject**

4 **Extra Constraints**

5 **Confirm Options**

> Before creating a new certificate, configure a new CA if you do not already have one on your system. Creating a internal certificate requires a CA exist on the system.

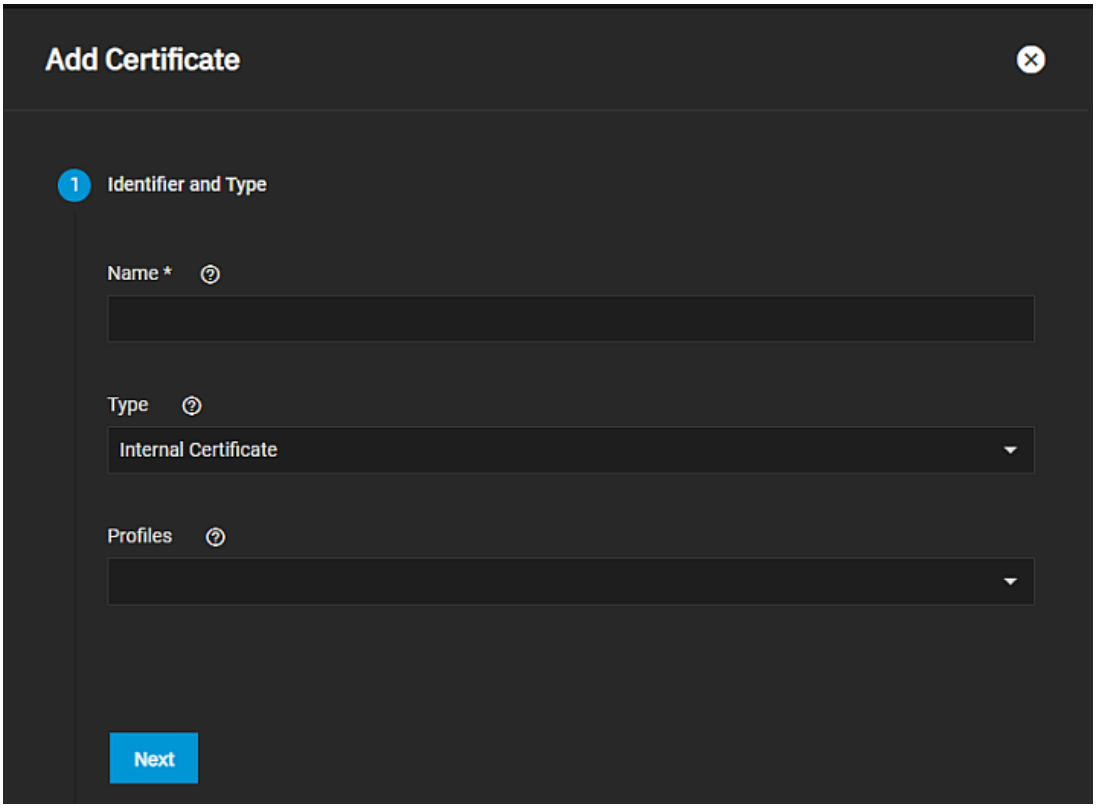
Many of the settings in the **Add Certificate** wizard are the same as those in the **Add CA** and **Add Certificate Signing Request** wizards.

Identifier and Type Options

The **Identifier and Type** options specify the certificate name and choose whether to use it for internal or local systems, or import an existing certificate.
Users can also select a predefined certificate extension from the **Profiles** dropdown list.

Click Here for More Information

The selection in **Type** changes setting options on this screen, the **Certificate Options** and **Extra Constraints** screens, and determines if the **Certificate Subject** screen displays at all.



Setting	Description
Name	Required. Enter a descriptive identifier for this certificate.
Type	Select the certificate type from the dropdown list. **Internal Certificate** uses system-managed CAs for certificate issuance. **Import Certificate** allows you to import an existing certificate onto the system. **Import Certificate** removes the **Profiles** field, changes other screens and fields displayed on other wizard screens.
Profiles	Select a predefined certificate extension. Options are **Openvpn Server Certificate** or **Openvpn Client Certificate**. Choose a profile that best matches your certificate usage scenario.

Certificate Options

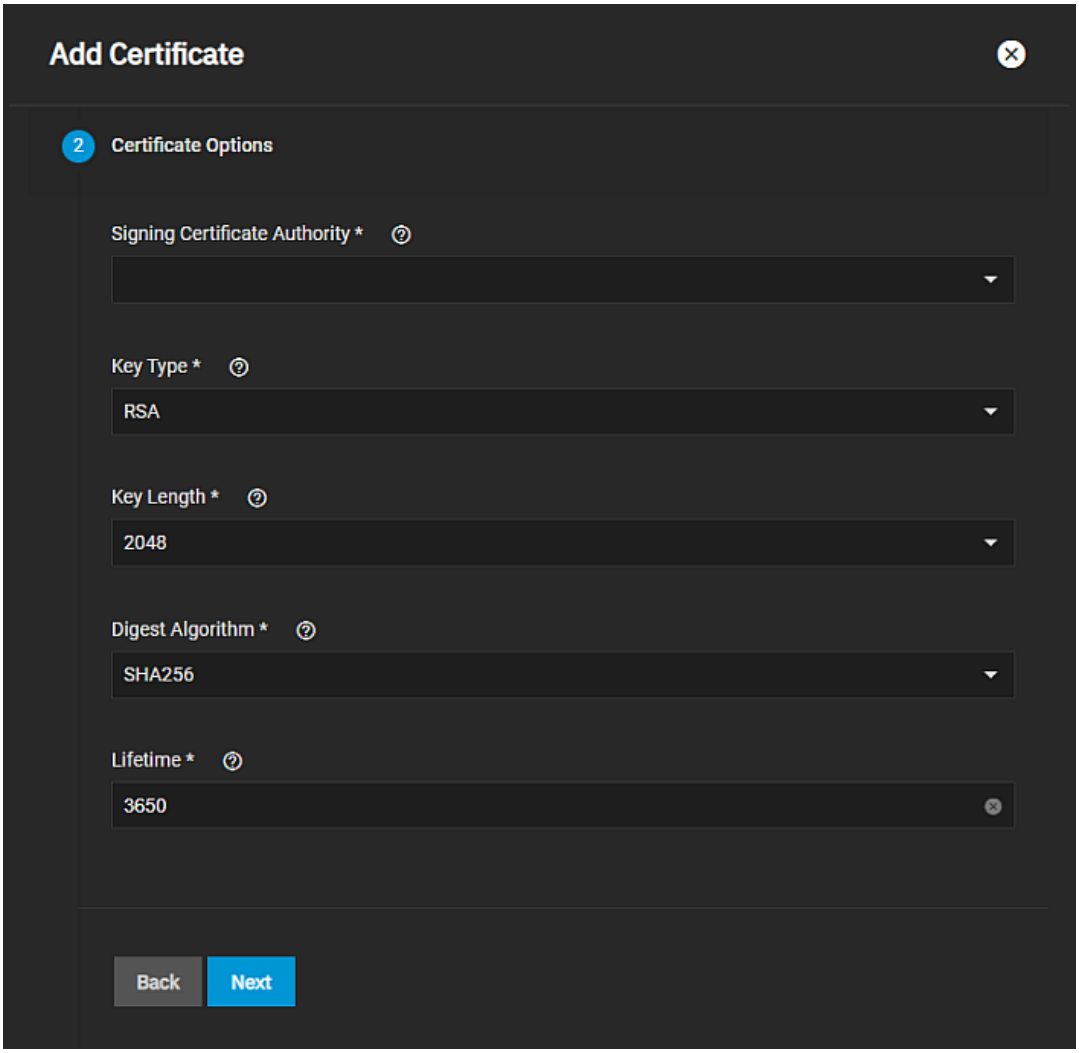
Certificate Options settings choose the signing certificate authority (CSR), the type of private key type to use (as well as the number of bits in the key used by the cryptographic algorithm), the cryptographic algorithm the certificate uses, and how many days the certificate authority lasts.

The **Certificate Options** settings change based on the selection in **Type** on the **Identifier and Type** screen.

Certificate Options - Internal Certificate

The **Key Type** selection changes fields displayed. **RSA** is the default setting in **Key Type**. The **Signing Certificate Authority** field requires you have a CA already configured on your system. If you do not have a Certificate Authority (CA) configured on your system, exit the **Add Certificate** wizard and add the required CA.

Click Here for More Information

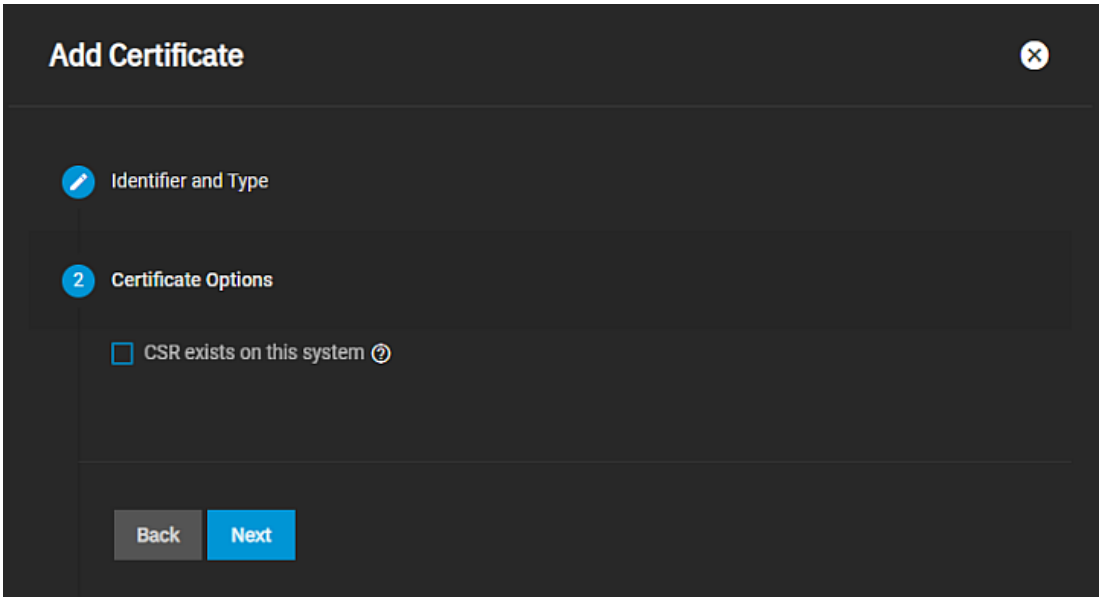


Setting	Description
Signing Certificate Authority	Required. Select a previously imported or created CA from the dropdown list.
Key Type	Required. Select an option (**RSA** or **EC**) from the dropdown list. See why is elliptic curve cryptography not widely used, compared to RSA?for more information about key types. Selecting **EC** displays the **EC Curve** field and removes the **Key Length** field.
Key Length	Required. Displays when **Key Type** is set to **RSA**. The number of bits in the key used by the cryptographic algorithm. For security reasons, a minimum key length of **2048** is recommended.
EC Curve	Displays when **Key Type** is set to **EC**. Select the Brainpool or SECP curve that fits your scenario. Brainpool curves can be more secure than SECP curves but SECP curves can be faster. Options are **BrainpoolP512R1**, **BrainpoolP384R1**, **BrainpoolP256R1**, **SECP256K1**, **SECP384R1**, **SECP521R1**, and **ed25519**. See Elliptic Curve performance: NIST vs Brainpool for more information.
Digest Algorithm	Required. Select the cryptographic algorithm to use from the dropdown list. Options are **SHA1**, **SHA224**, **SHA256**, **SHA384** or **SHA512**. Only change the default **SHA256** if the organization requires a different algorithm.
Lifetime	Required. Enter the number days for the lifetime of the CA.

Certificate Options - Import Certificate

Setting **Type** on the **Identifier and Type** screen to **Import Certificate** changes the options displayed on the **Certificate Options** configuration screen.

Click Here for More Information



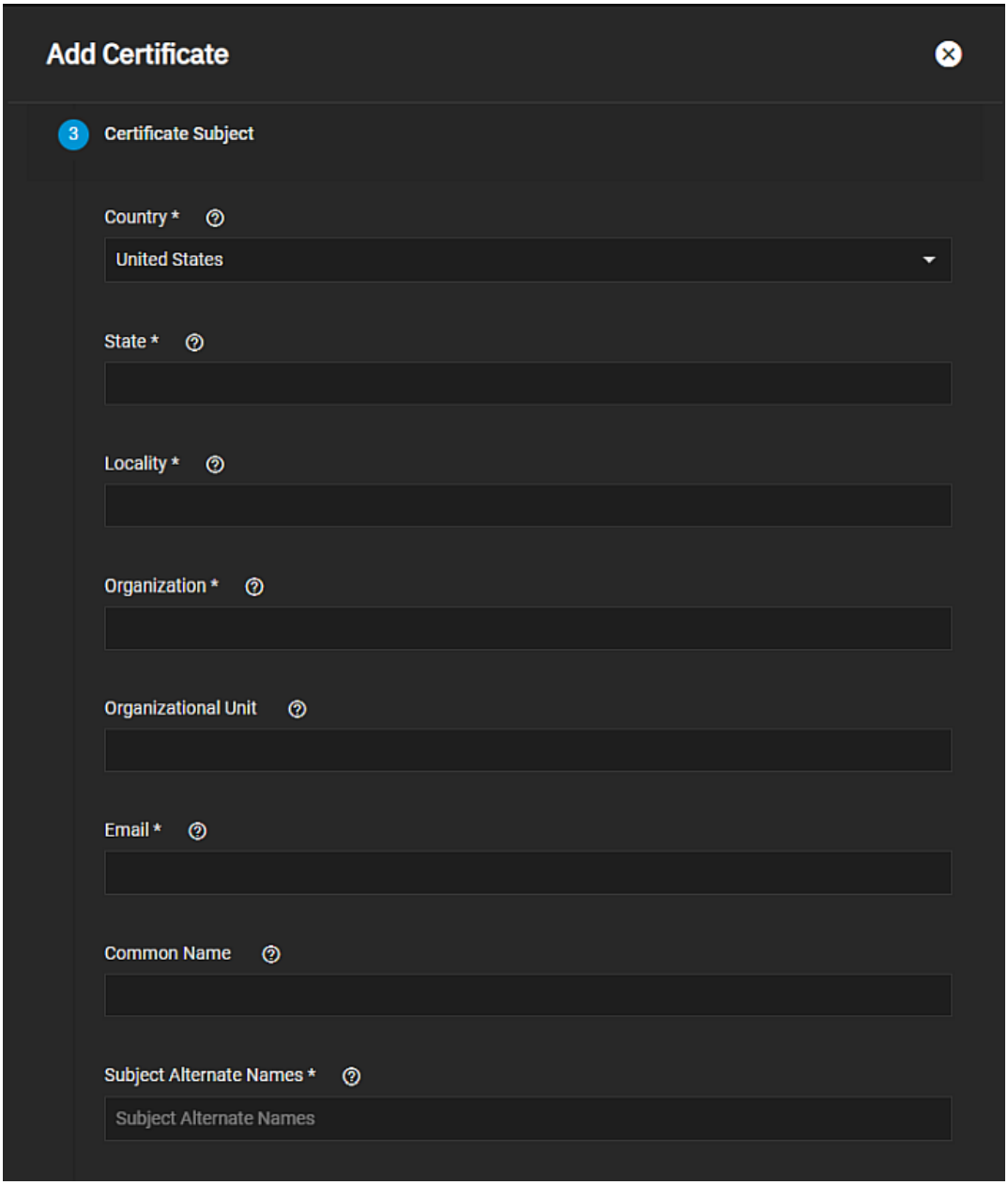
Setting	Description
CSR exists on this system	Select if importing a certificate for which a CSR exists on this system.
Certificate Signing Request	Select the existing CSR from the dropdown list.

Certificate Subject Options

The **Certificate Subject** step lets users define the location, name, and email for the organization using the certificate. Users can also enter the system fully-qualified hostname (FQDN) and any additional domains for multi-domain support.

The **Certificate Subject** screen does not display when **Type** on **Internal Certificate** is set to **Import Certificate**.

Click Here for More Information



Setting	Description
Country	Required. Select the country of the organization from the dropdown list.
State	Required. Enter the state or province of the organization.
Locality	Required. Enter the location of the organization. For example, the city.
Organization	Required. Enter the name of the company or organization.
Organizational Unit	Enter the organizational unit of the entity.
Email	Required. Enter the email address of the person responsible for the CA.
Common Name	Enter the fully qualified host name (FQHN) of the system. This mname must be unique within a certificate chain.
Subject Alternate Names	Required. Enter additional domains to secure for multi-domain support. Separate each domain by pressing `Enter`. For example, if the primary domain is *example.com*, entering *www.example.com** secures both addresses.

Extra Constraints Options

The **Extra Constraints** step contains certificate extension options.

- **Basic Constraints** that when enabled limits the path length for a certificate chain.
- **Authority Key Identifier** that when enabled provides a means of identifying the public key corresponding to the private key used to sign a certificate.

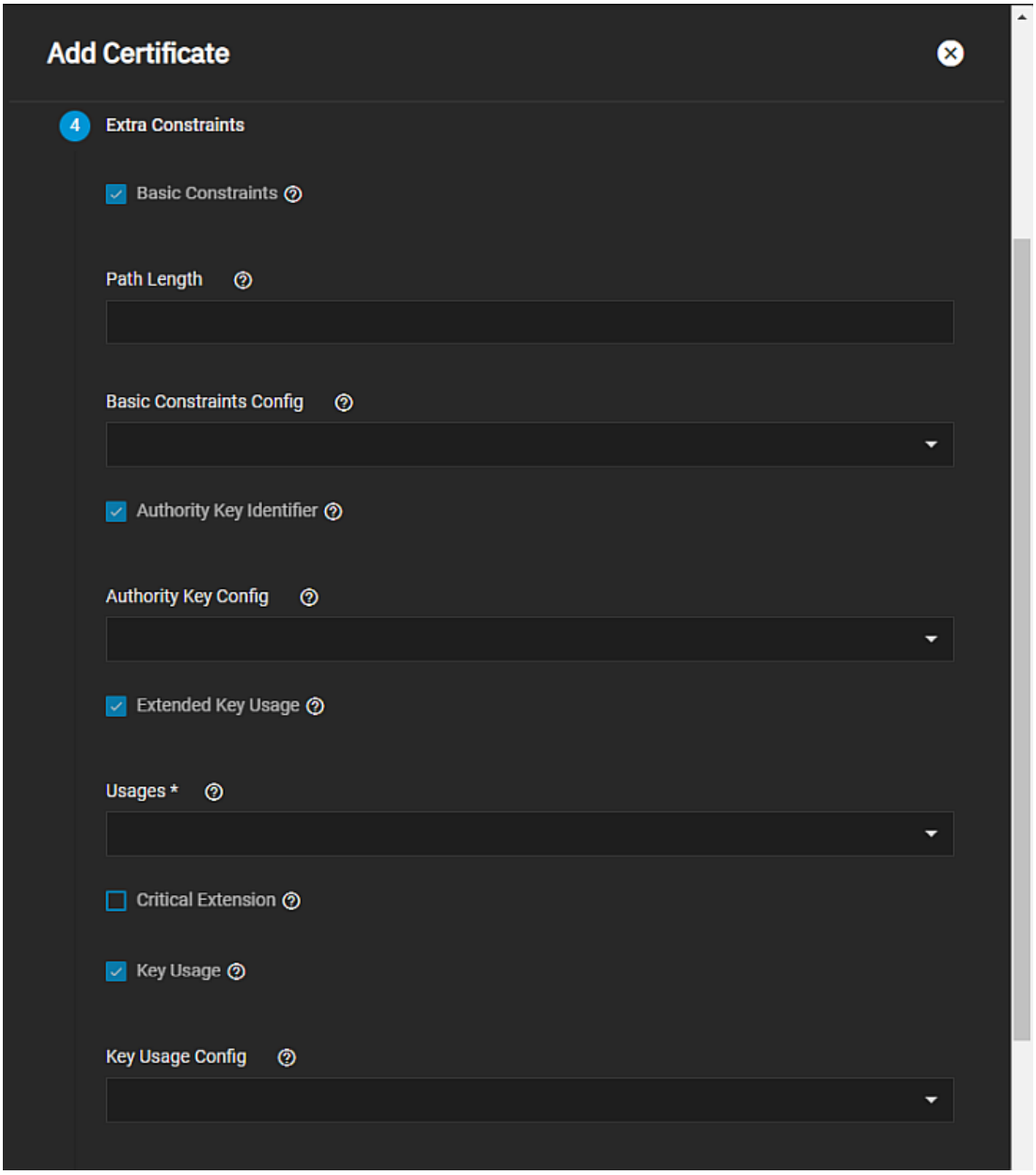
- **Key Usage** that when enable defines the purpose of the public key contained in a certificate.
- **Extended Key Usage** that when enable to further refines key usage extensions.

The **Extra Constraints** settings change based on the selection in **Type** on the **Identifier and Type** screen.

Extra Constraints - Internal Certificate

After selecting **Basic Constraints**, **Authority Key Identifier**, **Extended Key Usage**, or **Key Usage**, each displays more settings that option needs.

Click Here for More Information



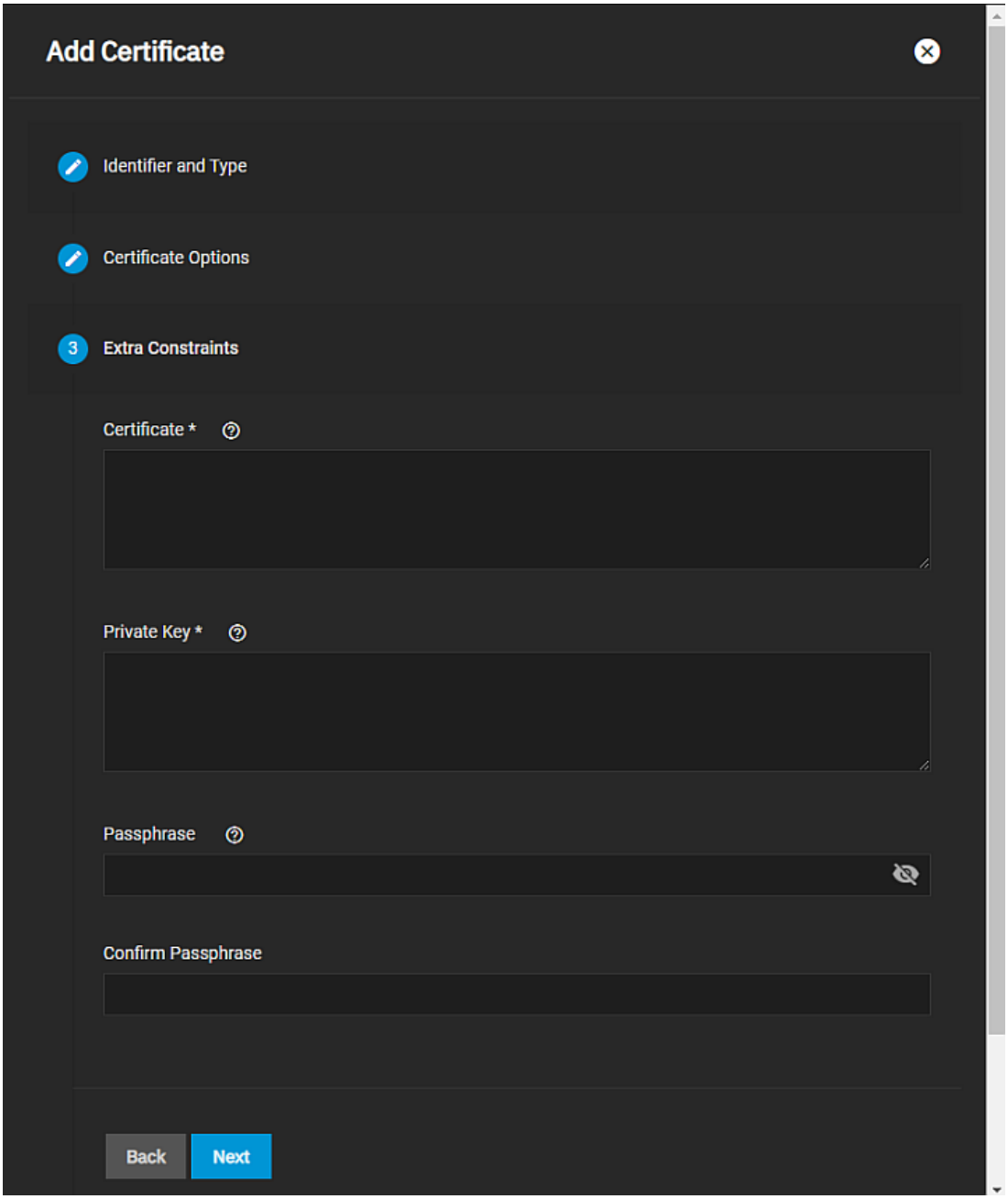
Setting	Description
Basic Constraints	Select to activate this extension to identify whether the certificate subject is a CA and the maximum depth of valid certification paths that include this certificate. Options are **CA** or **Critical Extension**. Selecting **Basic Constraints** displays the **Path Length** and **Basic Constraints Config** fields.
Path Length	Displays after selecting **Basic Constraints**. Enter a value of **0** or greater to set how many non-self-issued intermediate certificates can follow this certificate in a valid certification path. Entering **0** allows a single additional certificate to follow in the certificate path. Value cannot be less than **0**.
Basic Constraints Config	Select the option to specify whether to uses the certificate for a Certificate Authority and whether this extension is critical. Clients must recognized critical extension to prevent rejection. Web certificates typically require you to disable **CA** and enable **Critical Extension** in **Basic Constraints**.
Authority Key	Select to activate this extension. The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate. This extension is used where the issuer

Setting	Description
Identifier	has multiple signing keys (either due to multiple concurrent key pairs or due to changeover). The identification might be based on either the key identifier (the subject key identifier in the issuer certificate) or on the issuer name and serial number. See RFC 3280, section 4.2.1.1 for more information. Displays the **Authority Key Config** field.
Authority Key Config	Displays after selecting **Authority Key Identifier**. Select the option to specify whether the issued certificate should include authority key identifier information, and whether the extension is critical. Critical extension must be recognized by the client or be rejected. Options are **Authority Cert Issuer** and or **Critical Extension**. Multiple selections display separated by a comma (,).
Extended Key Usage	Select to activate this certificate extension. The Extended Key Usage extension identifies and limits valid uses for this certificate, such as client authentication or server authentication. See RFC 3280, section 4.2.1.13 for details. Displays the **Usages** field.
Usages	Displays after selecting **Extended Key Usage**. Select the option to identify the purpose of this public key from the dropdown list. Typically used for the end entity certificates. You can select multiple usages that display separated by a comma (,). Options are **ANY_EXTENDED_KEY_USAGE**, **CLIENT_AUTH**, **CODE_SIGNING**, **EMAIL_PROTECTION**, **OCSP_SIGNING**, **SERVER_AUTH**, or **TIME_STAMPING**. Do not mark this extension critical when set to **ANY_EXTENDED_KEY_USAGE**. The purpose of the certificate must be consistent with both extensions when using both **Extended Key Usage** and **Key Usage** extensions. See [RFC 3280, section 4.2.1.13 for more details.
Critical Extension	Select to identify this extension as critical for the certificate. The certificate-using system must recognize the critical extensions to prevent this certificate being rejected. The certificate-using system can ignore extensions identified as not critical and still approve the certificate.
Key Usage	Select to activate this certificate extension. The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate. The usage restriction might be employed when a key that can be used for more than one operation is to be restricted. For example, when an RSA key should be used only to verify signatures on objects other than public key certificates and CRLs, the Digital Signature bits are asserted. Likewise, when an RSA key should be used only for key management, the Key Encipherment bit is asserted. See RFC 3280, section 4.2.1.3 for more information. Displays the **Key Usage Config** field.
Key Usage Config	Displays after selecting **Extended Key Usage** or **Key Usage**. Select the option that specifies valid key usages for this certificate. Options are **Digital Signature**, **Content Commitment**, **Key Encipherment**, **Data Encipherment**, **Key Agreement**, **Key Cert Sign**, **CRL Sign**, **Encipher Only**, **Decipher Only** or **Critical Extension**. Web certificates typically need at least **Digital Signature** and possibly **Key Encipherment** or **Key Agreement**, while other applications might need other usages.

Extra Constraints - Import Certificate

When **Type** on **Identifier and Type** is set to **Import Certificate** the **Extra Constraints** screen does not include the options to set extension types.

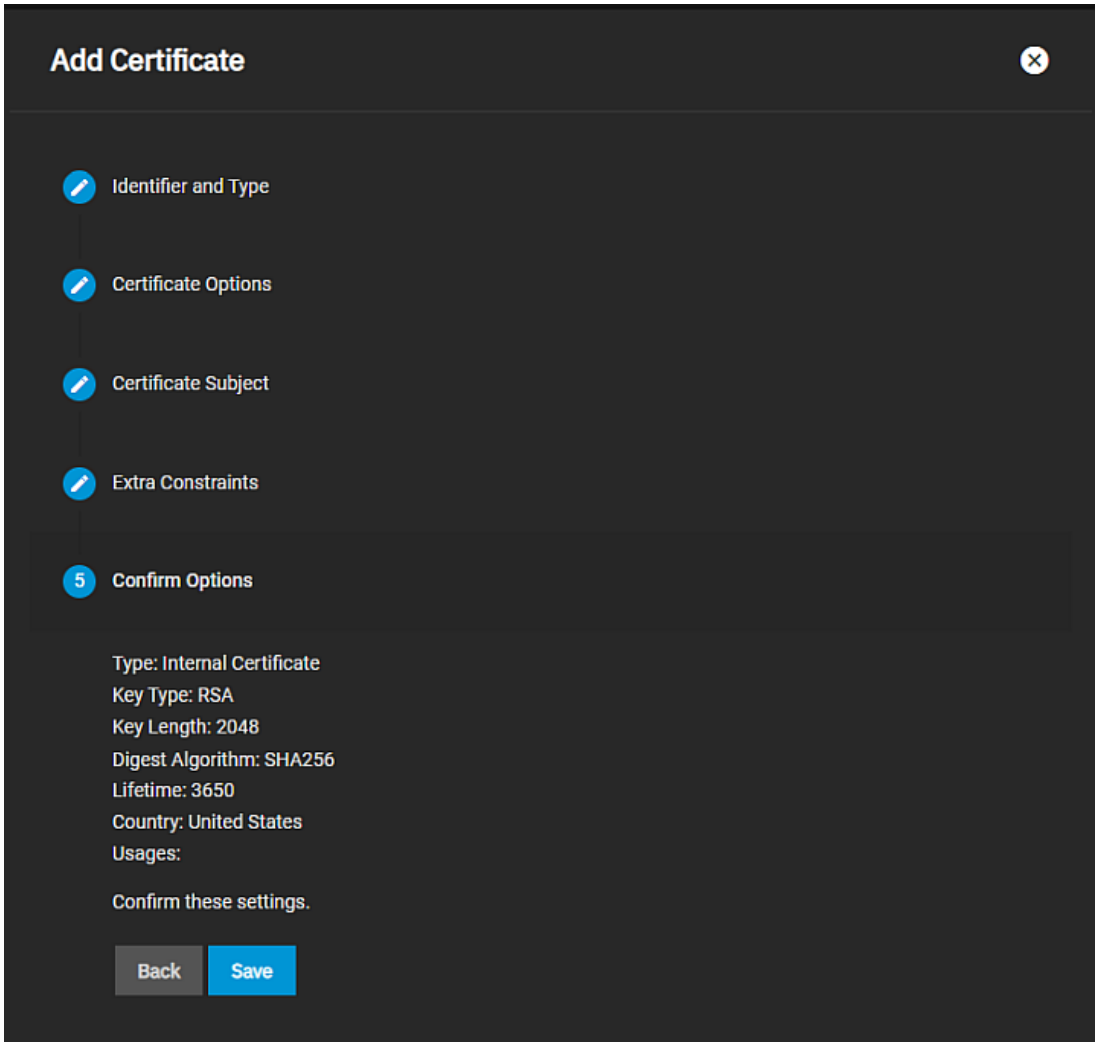
Click Here for More Information



Setting	Description
Certificate	Required. Paste the certificate for the CA into this field.
Private Key	Required. Paste the private key associated with the certificate when available. Provide a key at least 1024 bits long.
Passphrase	Enter the passphrase for the private key.
Confirm Passphrase	Re-enter the passphrase for the private key.

Confirm Options

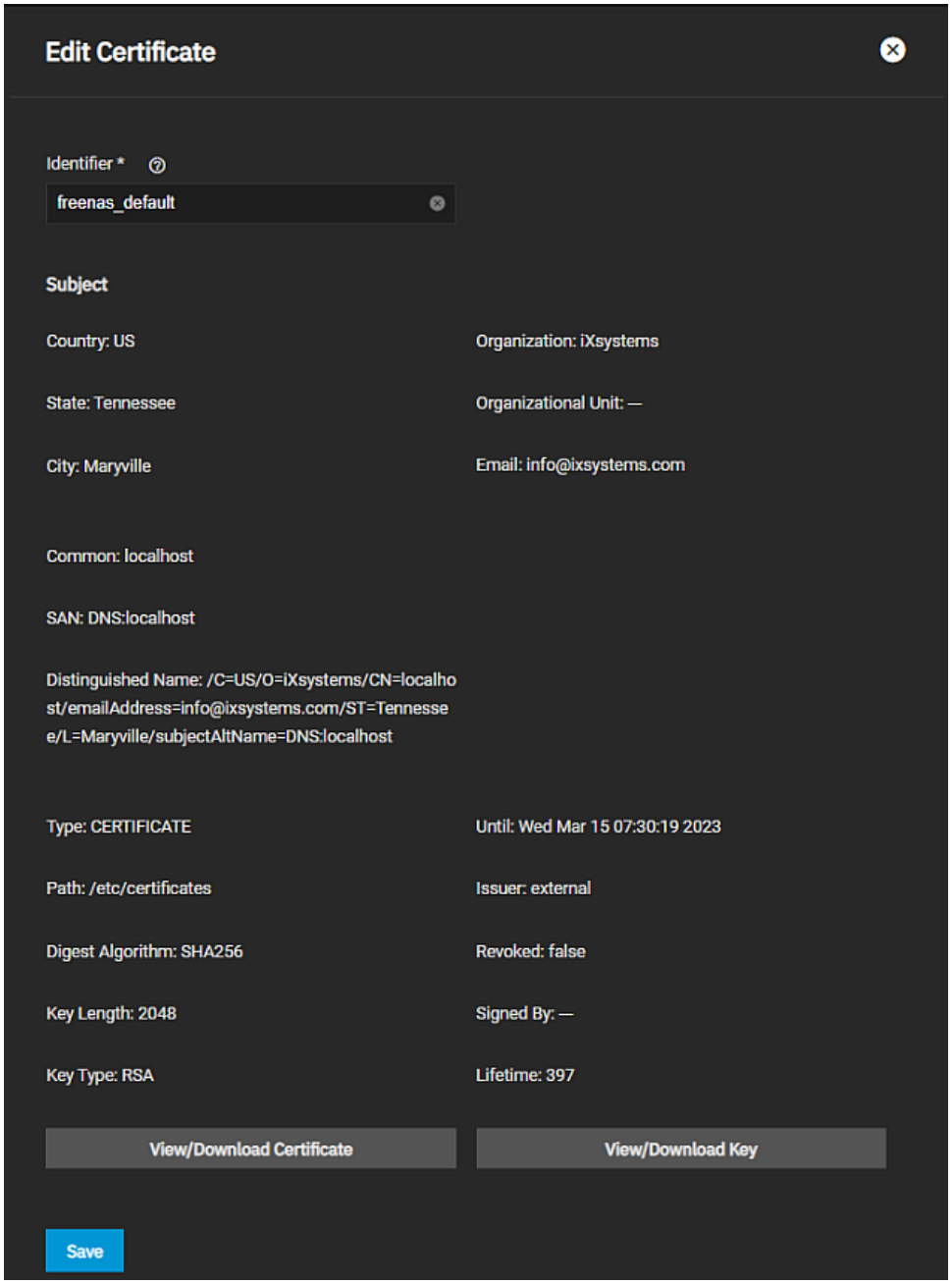
The final step screen is the **Confirm Options** that displays the certificate **Type**, **Key Type**, **Key Length**, **Digest Algorithm**, **Lifetime**, **Country**, and any configured **Usages**.



Save adds the certificate to SCALE. **Back** returns to previous screens to make changes before you save. **Next** advances to the next screen in the sequence to return to **Confirm Options**.

Edit Certificate Screen

The certificate listed on the **Certificates** widget is a link that opens the **Edit Certificate** screen.



The **Edit Certificate** screen displays the fixed **Subject** settings, the type, path, and other details about that certificate that are not editable. You can enter an alphanumeric name for the certificate in **Identifier** if you want to rename the certificate. You can use underscore (_) and or dash (-) characters in the name.

View/Download Certificate opens a window with the certificate string. Use the clipboard icon to copy the certificate to the clipboard or **Download** to download the certificate to your server. Keep the certificate in a secure area where you can back up and save it.

View/Download Key opens a window with the certificate private key. Use the clipboard icon to copy the public key to the clipboard or **Download** to download the key to your server. Keep the private key in a secure area where you can back up and save it.

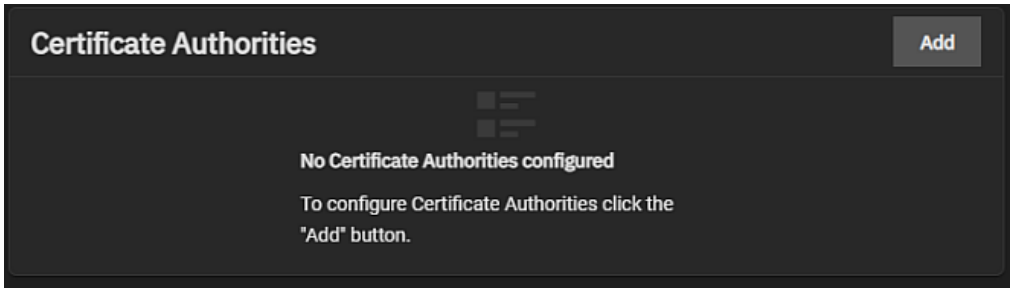
Related Content

- Managing Certificates
- Certificates Authorities Screens
- Managing Certificate Authorities
- Certificate Signing Requests Screens
- Managing Certificate Signing Requests
- ACME DNS-Authenticators Screens
- Adding ACME DNS-Authenticators
- Certificates
- Certificates

4.7.5.2 - Certificates Authorities Screens

This article provides information on SCALE certificate authroities screens and settings.

The **Certificate Authorities** widget on the **Credentials > Certificates** screen displays certificate authorities(CAs) added to SCALE, and allows you to add new CAs, or download, delete, or edit the name of an existing CA.



The download icon downloads the CA to your server.

deletes the CA from your server.

Each CA listed on the widget is a link that opens the **Edit CA** screen.

Add opens the **Add CA** wizard that steps you through setting up a certificate authority (CA) that certifies the ownership of a public key by the named subject of the certificate.

Add CA Wizard Screens

The **Add CA** wizard screens step users through configuring a new certificate authority on TrueNAS SCALE. The wizard has five different configuration screens, one for each step in the CA configuration process:

1 **Identifier and Type**

2 **Certificate Options**

3 **Certificate Subject**

4 **Extra Constraints**

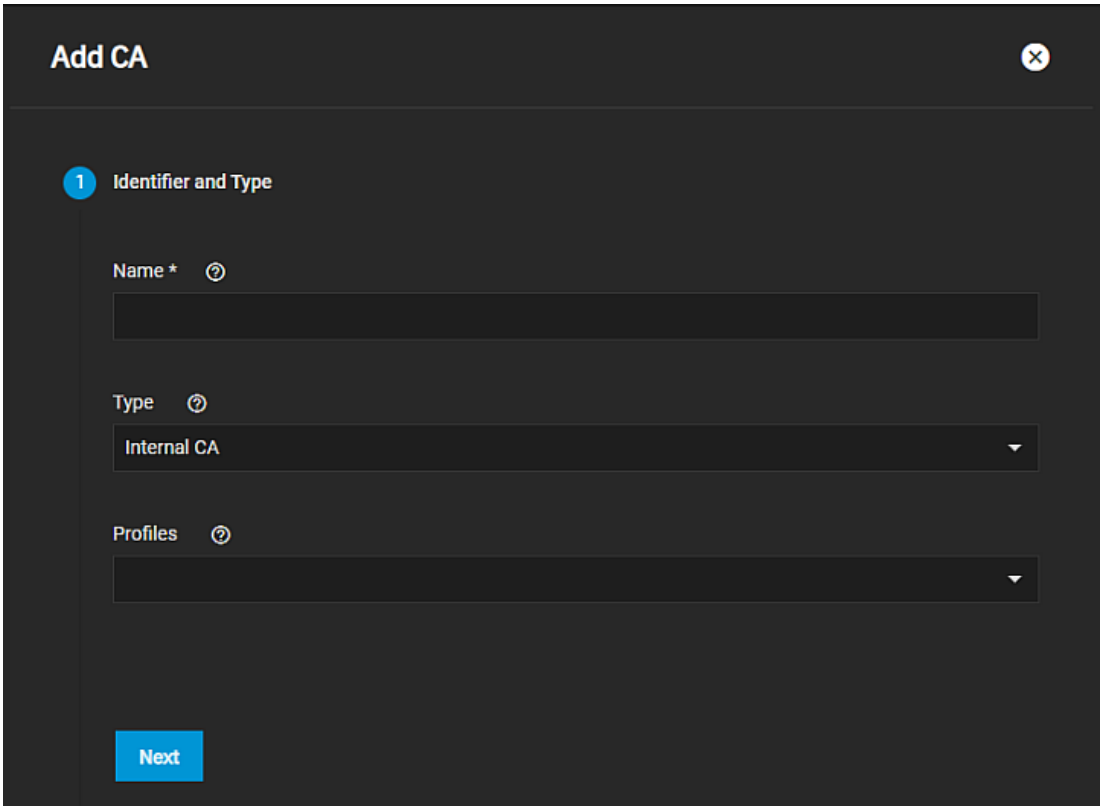
5 **Confirm Options**

Identifier and Type Options

The **Identifier and Type** options specify the CA name and choose whether to create a new CA or import an existing CA. Users can also select a predefined certificate extension from the **Profiles** dropdown list.

Click Here for More Information

The selection in **Type** changes setting options on this screen, the **Certificate Options** and **Extra Constraints** screens, and determines if the **Certificate Subject** screen displays at all.



Setting	Description
Name	Required. Enter a descriptive identifier for this certificate authority(CA).
Type	Select the type of CA from the dropdown list. Options are **Internal CA**, **Intermediate CA**, and **Import CA**. **Internal CA** functions like a publicly trusted CA to sign certificates for an internal network. They are not trusted outside the private network. **Intermediate CA** lives between the root and end entity certificates and its main purpose is to define and authorize the types of certificates you can request from the root CA. **Import CA** allows you to import an existing CA onto the system. For more information see What are Subordinate CAs and Why Would You Want Your Own?.
Profiles	Displays if **Internal CA** or **Intermediate CA** are set in **Type**. Select a predefined certificate extension from the dropdown list. Choose a profile that best matches your certificate usage scenario. Options are **Openvpn Root CA** and **CA**.

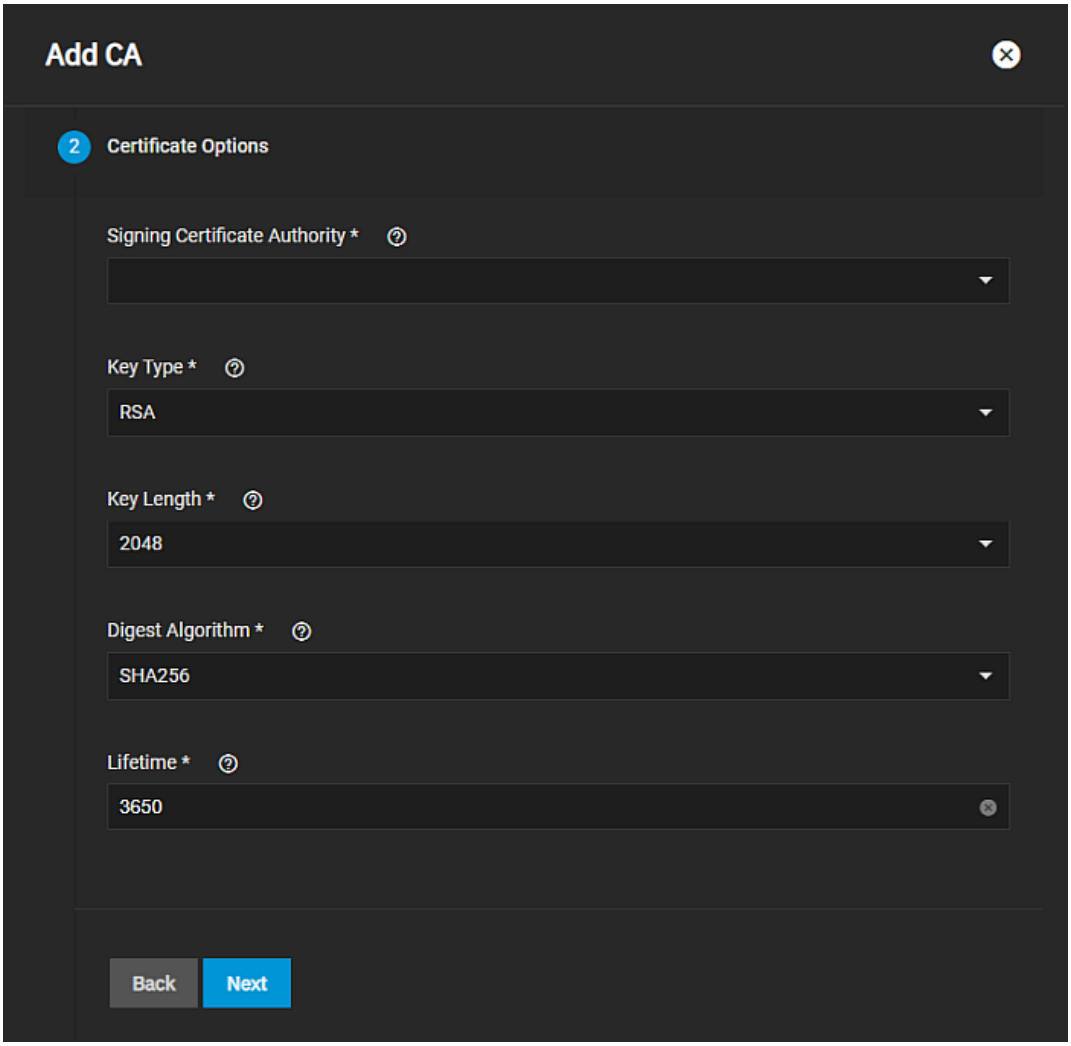
Certificate Options

The **Certificate Options** settings specify the type of private key to use (as well as the number of bits in the key used by the cryptographic algorithm), the cryptographic algorithm the CA uses, and how many days the CA lasts.

The **Certificate Options** settings do not display if **Type** on the **Identifier and Type** screen is set to **Import CA**.

The **Key Type** selection changes fields displayed. **RSA** is the default setting in **Key Type**.

Click Here for More Information



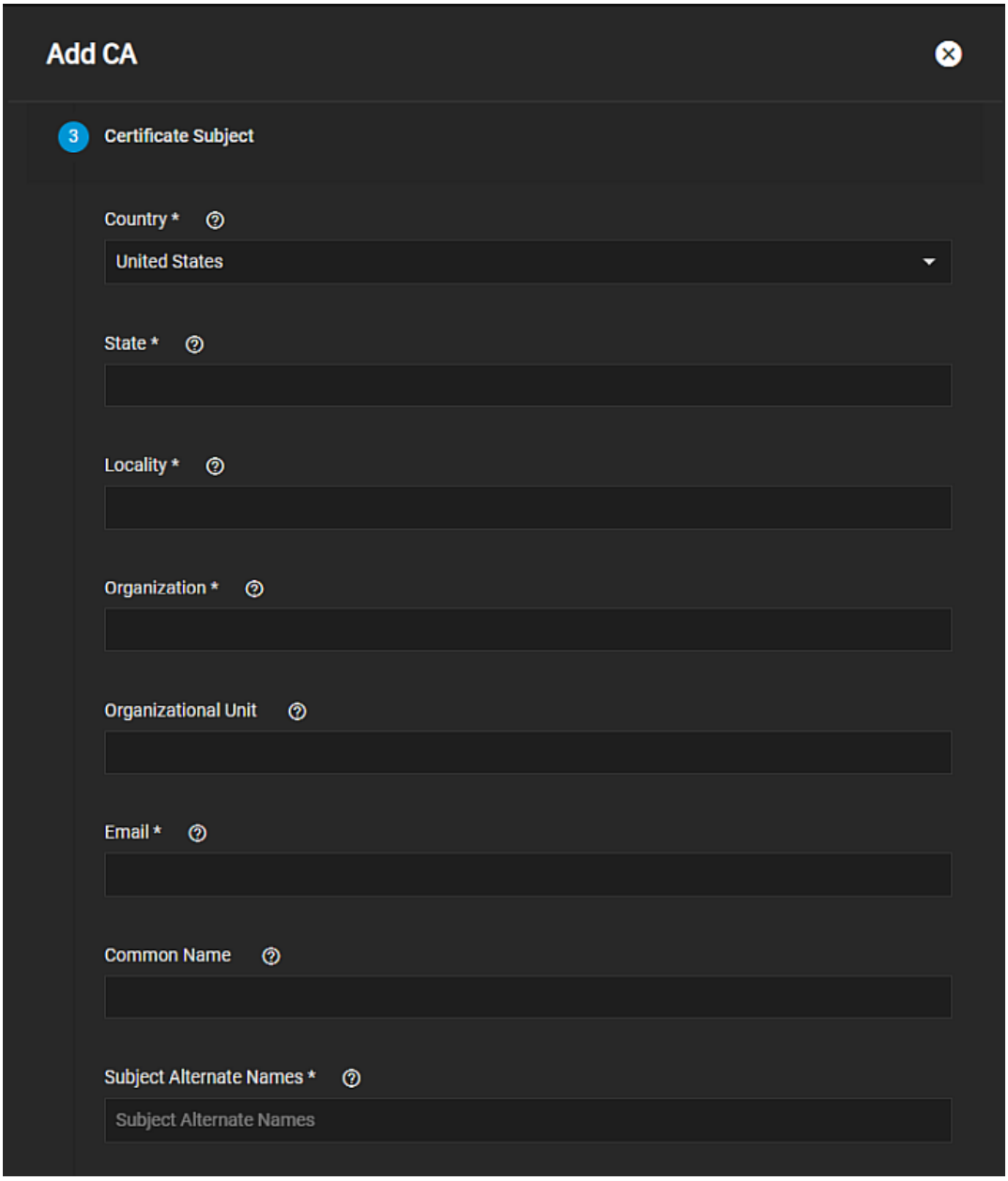
Setting	Description
Key Type	Select the key type from the dropdown list. Options are **RSA** or **EC**. **RSA** displays the **Key Length** field. **EC** displays the **EC Curve** field. See Why is elliptic curve cryptography not widely used, compared to RSA? for more information about key types.
EC Curve	Displays when **EC** is selected in **Key Type**. Select the curve type from the dropdown list. Options are **BrainpoolP512R1**, **BrainpoolP384R1**, **BrainpoolP256R1**, **SECP256K1**, **SECP384R1**, **SECP521R1**, and **ed25519**. Brainpool curves can be more secure while SECP curves can be faster. See Elliptic Curve performance: NIST vs Brainpool for more information.
Key Length	Required. Displays when **RSA** is selected in **Key Type**. Select the number of bits in the key used by the cryptographic algorithm from the dropdown list. Options are **1024**, **2048** or **4096**. For security reasons, a minimum key length of 2048 is recommended.
Digest Algorithm	Select the cryptographic algorithm to use from the dropdown list.Options are **SHA1**, **SHA224**, **SHA256**, **SHA384** and **SHA512**. Only change the default **SHA256** if the organization requires a different algorithm.
Lifetime	Enter the number of days for the lifetime of the CA.

Certificate Subject Options

The **Certificate Subject** settings define the location, name, and email for the organization using the certificate.
Users can also enter the system fully-qualified hostname (FQDN) and any additional domains for multi-domain support.

The **Certificate Subject** settings do not display if **Type** on the **Identifier and Type** screen is set to **Import CA**.

Click Here for More Information



Setting	Description
Country	Required. Select the country of the organization from the dropdown list.
State	Required. Enter the state or province of the organization.
Locality	Required. Enter the location of the organization. For example, the city.
Organization	Required. Enter the name of the company or organization.
Organizational Unit	Enter the organizational unit of the entity.
Email	Required. Enter the email address of the person responsible for the CA.
Common Name	Enter the fully qualified host name (FQHN) of the system. This name must be unique within a certificate chain.
Subject Alternate Names	Required. Enter additional domains to secure for multi-domain support. Separate each domain by pressing `Enter`. For example, if the primary domain is *example.com*, entering *www.example.com* secures both addresses.

Extra Constraints Options

The **Extra Constraints** options contain certificate extension options.

- **Basic Constraints** that when enabled limits the path length for a certificate chain.
- **Authority Key Identifier** that when enabled provides a means of identifying the public key corresponding to the private key used to sign a certificate.

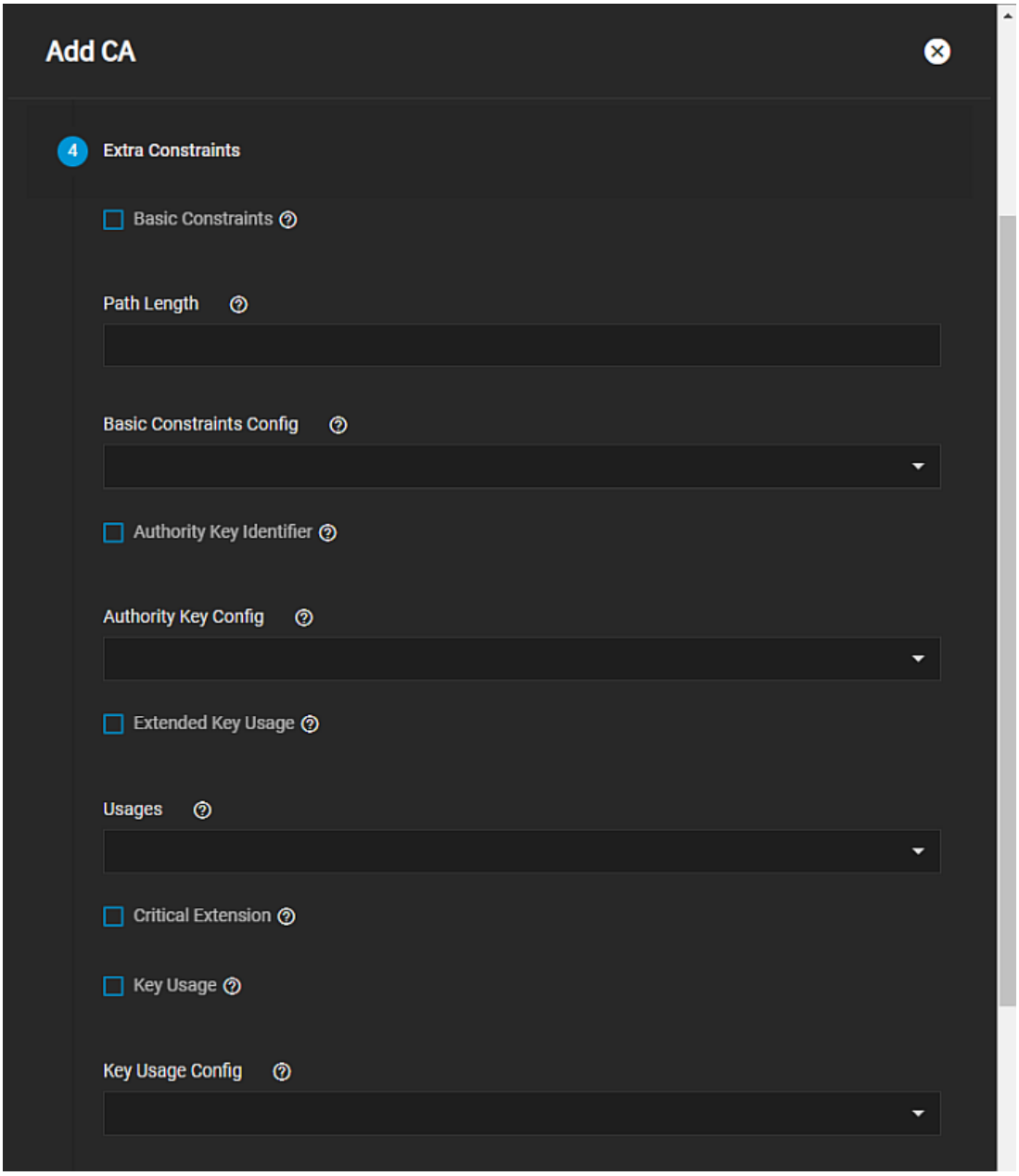
- **Key Usage** that when enable defines the purpose of the public key contained in a certificate.
- **Extended Key Usage** that when enable to further refines key usage extensions.

The **Extra Constraints** settings change based on the selection in **Type** on the **Identifier and Type** screen.

Extra Constraints - Internal or Intermediate CA

After selecting **Basic Constraints**, **Authority Key Identifier**, **Extended Key Usage**, or **Key Usage**, each displays more settings that option needs.

Click Here for More Information



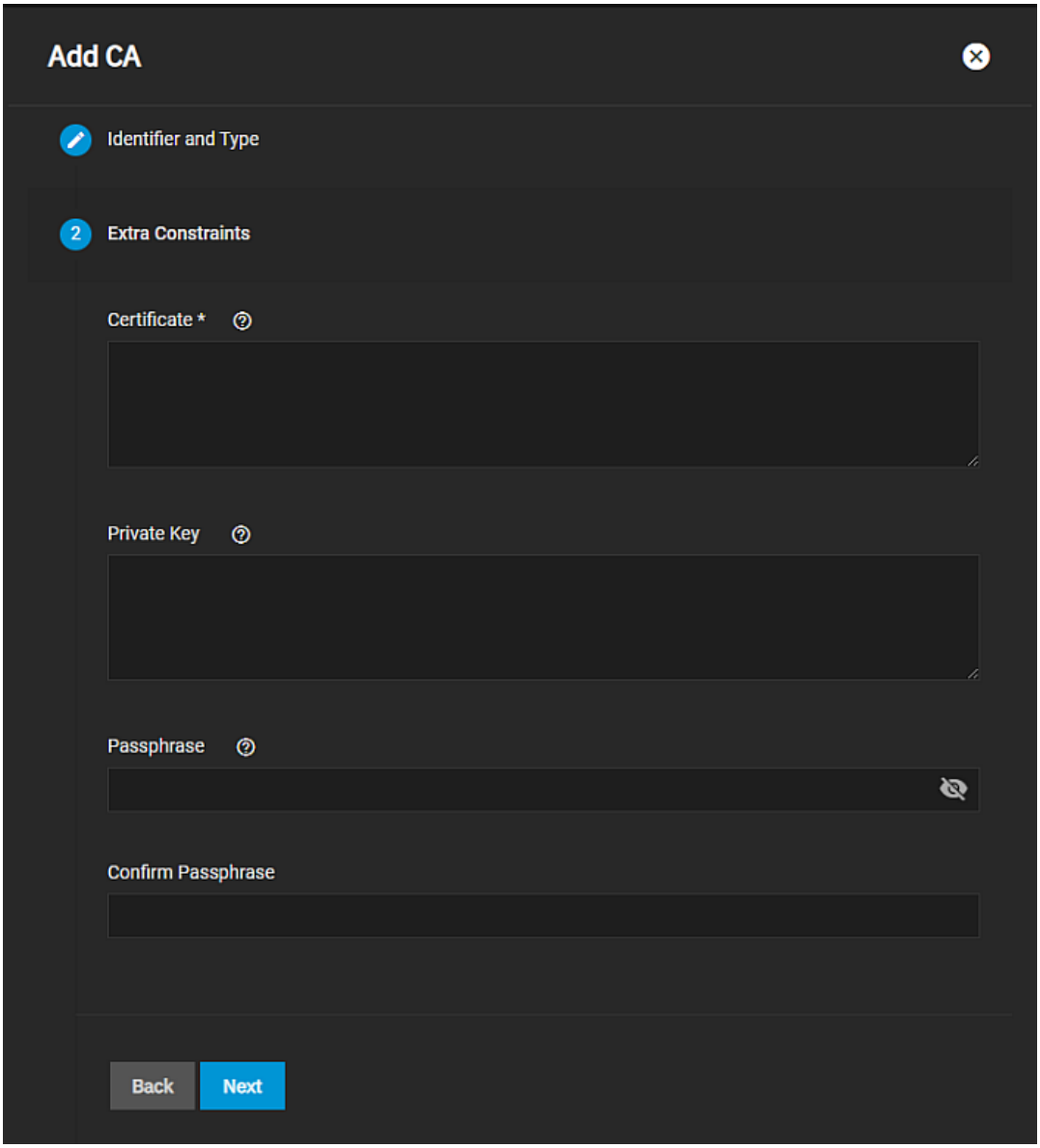
Setting	Description
Basic Constraints	Select to activate this extension.
Path Length	Displays after selecting **Basic Constraints**. Enter the number of non-self-issued intermediate certificates that can follow this certificate in a valid certification path. Entering **0** allows a single additional certificate to follow in the certificate path. Value cannot be less than **0**.
Basic Constraints Config	Select the option to specify the extension type from the dropdown list. Options are **CA** and **Critical Extension**. The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate. See RFC 3280, section 4.2.10 for more information.

Setting	Description
Authority Key Identifier	Select to activate this extension. Displays the **Authority Key Config** field.
Authority Key Config	Displays after selecting **Authority Key Identifier**. Select the option to specify whether the authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate. Options are **Authority Cert Issuer** and or **Critical Extension**. This extension is used where an issuer has multiple signing keys (either due to multiple concurrent key pairs or due to changeover). The identification might be based on either the key identifier (the subject key identifier in the issuer certificate) or on the issuer name and serial number. See RFC 3280, section 4.2.1.1 for more information.
Extended Key Usage	Select to activate this certificate extension. Displays the **Usages** field.
Usages	Displays after selecting **Extended Key Usage**. Select the option to identify the purpose of this public key from the dropdown list. Typically used for the end entity certificates. You can select multiple usages that display separated by a comma (,). Options are **ANY_EXTENDED_KEY_USAGE**, **CLIENT_AUTH**, **CODE_SIGNING**, **EMAIL_PROTECTION**, **OCSP_SIGNING**, **SERVER_AUTH**, or **TIME_STAMPING**. Do not mark this extension critical when set to **ANY_EXTENDED_KEY_USAGE**. Using both **Extended Key Usage** and **Key Usage** extensions requires that the purpose of the certificate is consistent with both extensions. See RFC 3280, section 4.2.13 for more details.
Critical Extension	Displays after selecting **Extended Key Usage**. Select to identify this extension as critical for the certificate. The certificate-using system must recognize critical extensions or this certificate is rejected. T he certificate-using system can ignore the extensions identified as not critical and still approve the certificate.
Key Usage	Select to activate this certificate extension. Displays the **Key Usage Config** field.
Key Usage Config	Displays after selecting **Extended Key Usage** or **Key Usage**. Select the key usage extension from the dropdown list. Options are **Digital Signature**, **Content Commitment**, **Key Encipherment**, **Data Encipherment**, **Key Agreement**, **Key Cert Sign**, **CRL Sign**, **Encipher Only**, **Decipher Only** or **Critical Extension**. The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate. The usage restriction might be employed when a key that could be used for more than one operation is to be restricted. For example, when an RSA key should be used only to verify signatures on objects other than public key certificates and CRLs, the **Digital Signature** bits would be asserted. Likewise, when an RSA key should be used only for key management, the **Key Encipherment** bit would be asserted.
See RFC 3280, section 4.2.1.3 for more information.	

Extra Constraints - Import CA

When **Type** on **Identifier and Type** is set to **Import CA** the **Extra Constraints** screen does not include the options to set extension types.

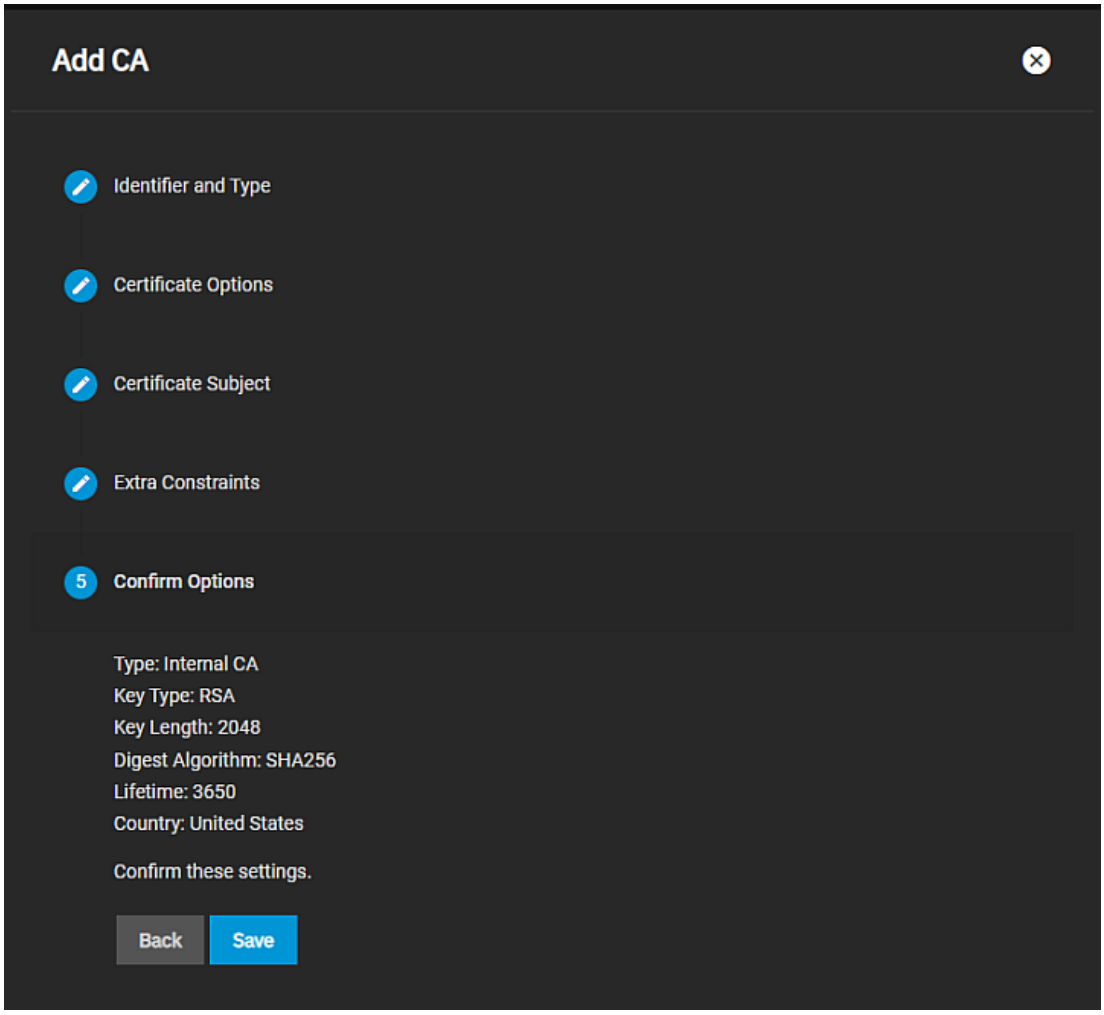
Click Here for More Information



Setting	Description
Certificate	Required. Paste the certificate for the CA into this field.
Private Key	Required. Paste the private key associated with the certificate when available. Provide a key at least 1024 bits long.
Passphrase	Enter the passphrase for the private key.
Confirm Passphrase	Re-enter the passphrase for the private key.

Confirm Options

The final step screen is the **Confirm Options** that displays the CA **Type**, **Key Type**, **Key Length**, **Digest Algorithm**, **Lifetime**, **Country**, and any configured **Usages**. For **Import CA** type, the screen displays **Type** and **Certificate**.



Save adds the certificate to SCALE. **Back** returns to previous screens to make changes before you save. **Next** advances to the next screen in the sequence to return to **Confirm Options**.

Related Content

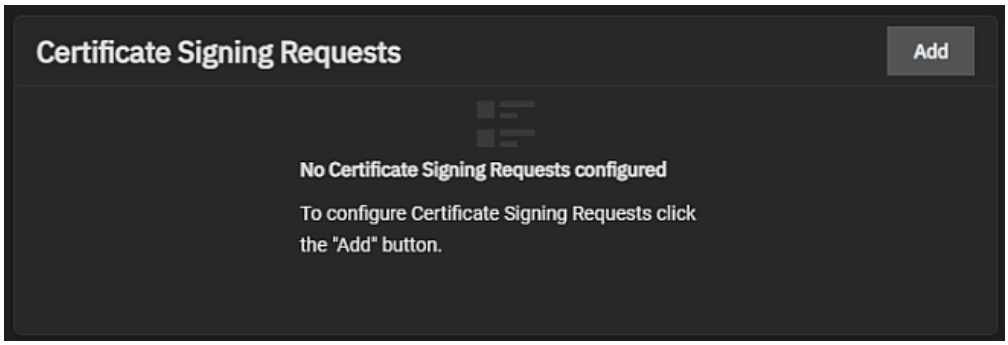
- Certificates Screens
- Managing Certificates
- Managing Certificate Authorities
- Certificate Signing Requests Screens
- Managing Certificate Signing Requests
- Adding ACME DNS-Authenticators

4.7.5.3 - Certificate Signing Requests Screens

This article provides information on SCALE certificates signing request screens and settings.

The **Certificates** screen includes the **Certificate Signing Requests** widget that displays a list of certificate signing requires (CSRs) configured on the system.

Each CSR listed is a link that opens the **Edit CA** screen for the selected CSR.



The download icon downloads the CSR to your server.

deletes the CSR from your server.

Each CSR listed on the widget is a link that opens the **Edit CSR** screen.

Add opens the **Add CSR** wizard that steps you through setting up a CSR that certifies the ownership of a public key by the named subject of the certificate. The **Certificate Signing Requests** section allows users configure the message(s) the system sends to a registration authority of the public key infrastructure to apply for a digital identity certificate.

Add CSR Wizard Screens

The **Add CSR** wizard screens step users through configuring a new certificate signing request (CSR) on TrueNAS SCALE. The wizard has five different configuration screens, one for each step in the CA configuration process:

1 **Identifier and Type**

2 **Certificate Options**

3 **Certificate Subject**

4 **Extra Constraints**

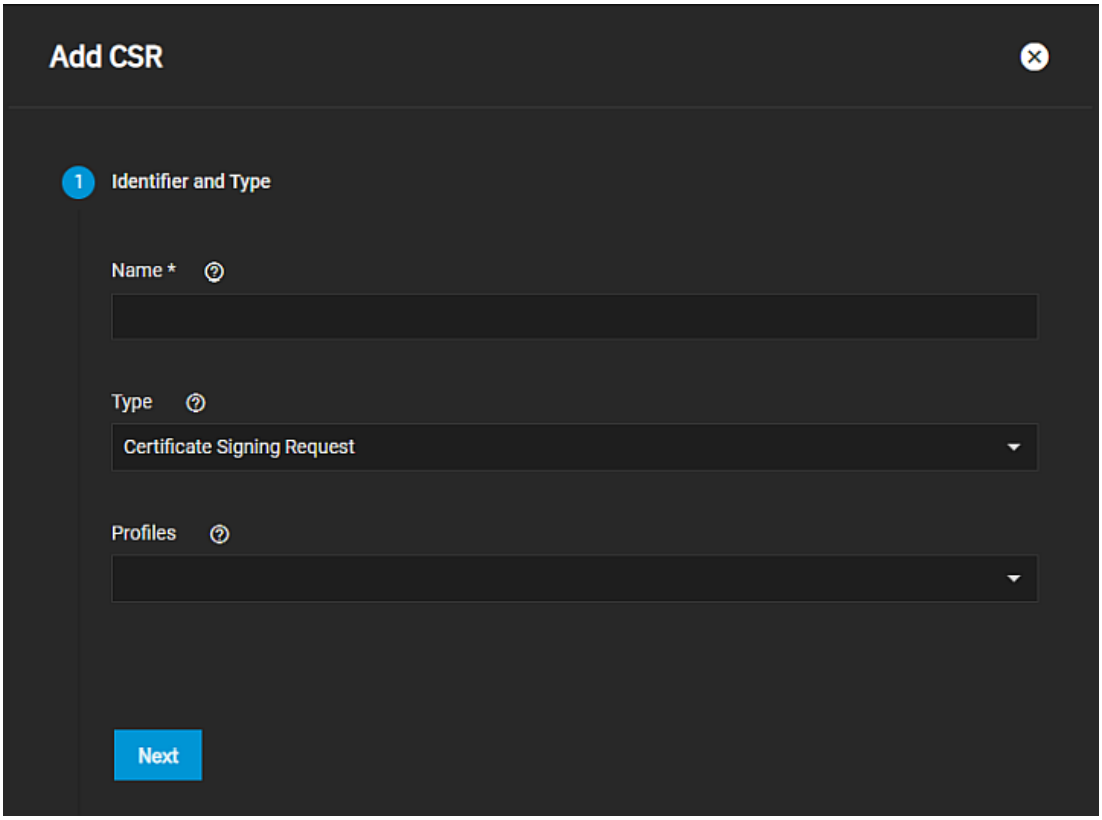
5 **Confirm Options**

Identifier and Type Options

The **Identifier and Type** settings specify the certificate signing request (CSR) name and whether to create a new CSR or import an existing CSR.
Users can also select a predefined certificate extension from the **Profiles** dropdown list.

Click Here for More Information

The selection in **Type** changes setting options on this screen, the **Certificate Options** and **Extra Constraints** screens, and determines if the **Certificate Subject** screen displays at all.



Setting	Description
Name	Required. Enter a descriptive identifier for this certificate.
Type	Select the type of CSR from the dropdown list. Options are **Certificate Signing Request** and **Import Certificate Signing Request**. **Certificate Signing Requests** control when an external CA issues (signs) the certificate. Typically used with ACME or other CAs that most popular browsers trust by default. **Import Certificate Signing Request** lets you import an existing CSR onto the system. Typically used with ACME or internal CAs. Selecting **Import Certificate Signing Request** removes the **Profiles** field.
Profiles	Displays if **Certificate Signing Request** is set in **Type**. Select a predefined certificate extension from the dropdown list. Choose a profile that best matches your certificate usage scenario. Options are **Openvpn Server Certificate** and **Openvpn Client Certificate**.

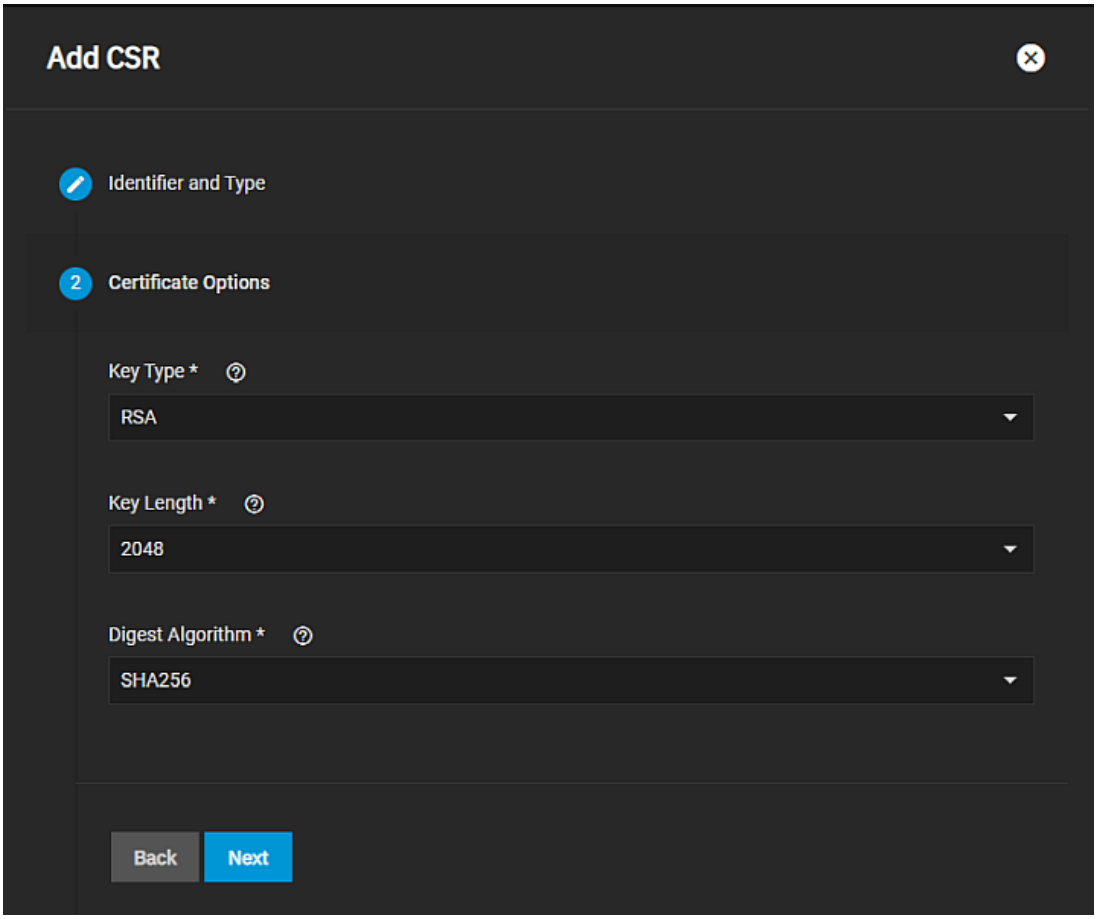
Certificate Options

The **Certificate Options** settings specify the type of private key type to use, the number of bits in the key used by the cryptographic algorithm, and the cryptographic algorithm the CSR uses.

There are no **Certificate Options** settings if **Type** on the **Identifier and Type** screen is set to **Import Certificate Signing Request**.

The **Key Type** selection changes fields displayed. **RSA** is the default setting in **Key Type**.

Click Here for More Information



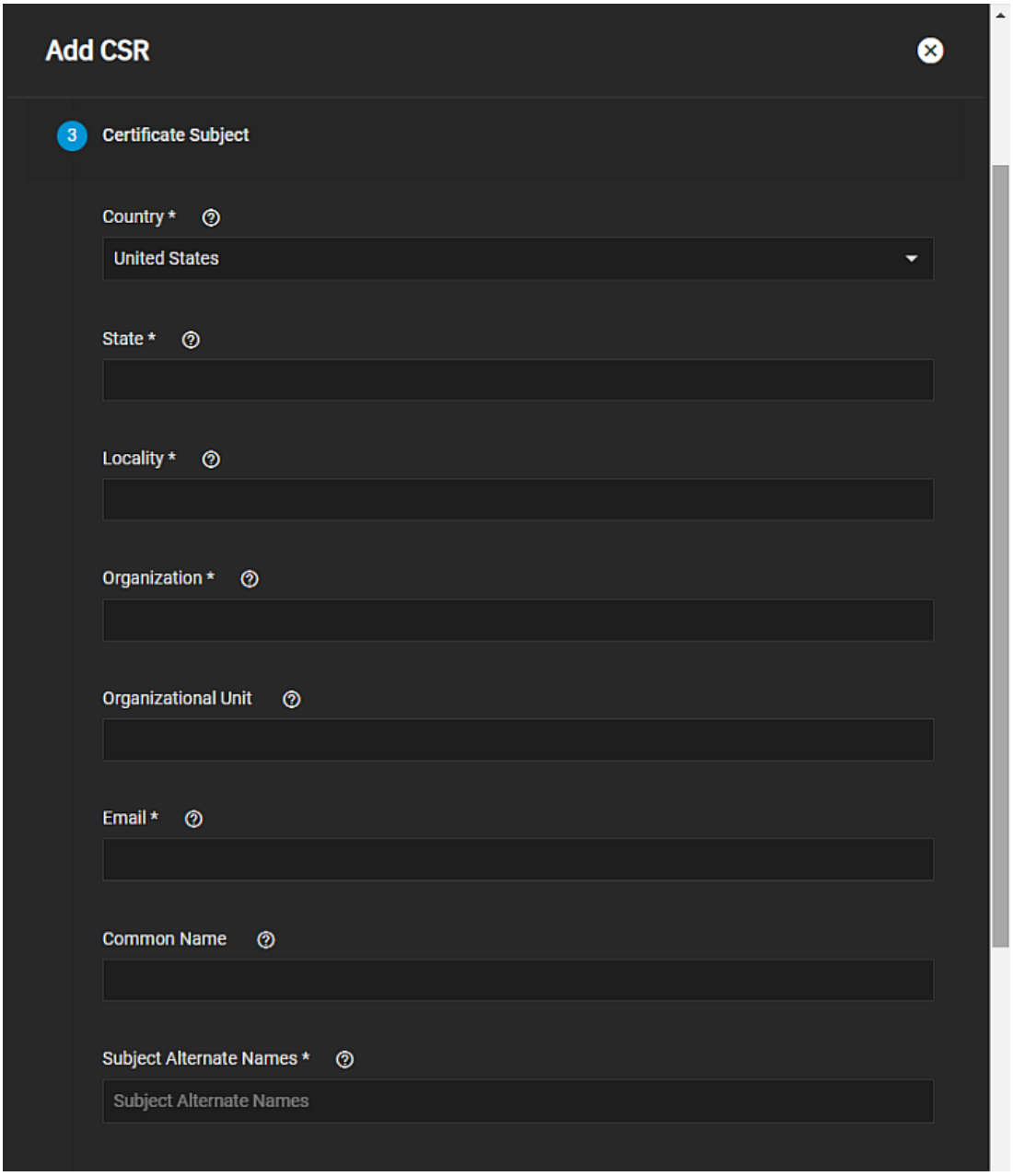
Setting	Description
Key Type	Select the key type from the dropdown list. Options are **RSA** or **EC**. **EC** displays the **EC Curve** field. See Why is elliptic curve cryptography not widely used, compared to RSA? for more information about key types.
EC Curve	Displays when **EC** is selected in **Key Type**. Select the curve type from the dropdown list. Options are **BrainpoolP512R1**, **BrainpoolP384R1**, **BrainpoolP256R1**, **SECP256K1**, **SECP384R1**, **SECP521R1**, and **ed25519**. Brainpool curves can be more secure while SECP curves can be faster. See Elliptic Curve performance: NIST vs Brainpool for more information.
Key Length	Required. Displays when **RSA** is selected in **Key Type**. Select the number of bits in the key used by the cryptographic algorithm from the dropdown list. Options are **1024**, **2048** or **4096**. For security reasons, a minimum key length of 2048 is recommended.
Digest Algorithm	Select the cryptographic algorithm to use from the dropdown list. Options are **SHA1**, **SHA224**, **SHA256**, **SHA384** and **SHA512**. Only change the default **SHA256** if the organization requires a different algorithm.
Lifetime	Enter the number of days for the lifetime of the CA.

Certificate Subject Settings

The **Certificate Subject** settings lets users define the location, name, and email for the organization using the certificate. Users can also enter the system fully-qualified hostname (FQDN) and any additional domains for multi-domain support.

The **Certificate Subject** settings do not display if **Type** on the **Identifier and Type** screen is set to **Import Certificate Signing Request**.

Click Here for More Information



Setting	Description
Country	Required. Select the country of the organization from the dropdown list.
State	Required. Enter the state or province of the organization.
Locality	Required. Enter the location of the organization. For example, the city.
Organization	Required. Enter the name of the company or organization.
Organizational Unit	Enter the organizational unit of the entity.
Email	Required. Enter the email address of the person responsible for the CA.
Common Name	Enter the fully qualified host name (FQHN) of the system. This name must be unique within a certificate chain.
Subject Alternate Names	Required. Enter additional domains to secure for multi-domain support. Separate each domain by pressing `Enter`. For example, if the primary domain is *example.com*, entering *www.example.com* secures both addresses.

Extra Constraints Settings

The **Extra Constraints** settings contains certificate extension options:

- **Basic Constraints** that when enabled limits the path length for a certificate chain.

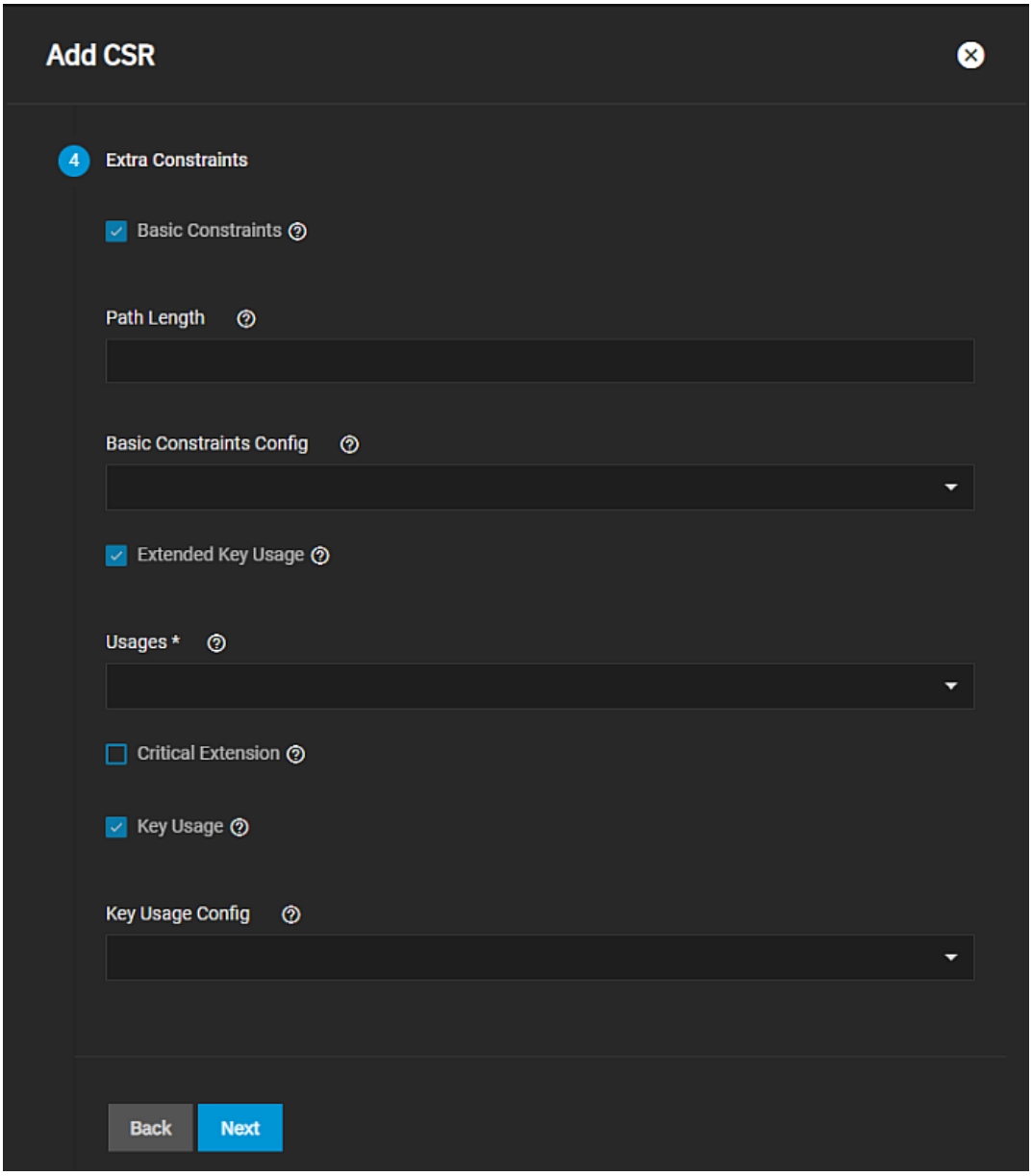
- **Authority Key Identifier** that when enabled provides a means of identifying the public key corresponding to the private key used to sign a certificate.
- **Key Usage** that when enabled defines the purpose of the public key contained in a certificate.
- **Extended Key Usage** that when enabled further refines key usage extensions.

The **Extra Constraints** settings change based on the selection in **Type** on the **Identifier and Type** screen.

Extra Constraints - Certificate Signing Request Type

After selecting **Basic Constraints**, **Authority Key Identifier**, **Extended Key Usage**, or **Key Usage**, each displays more settings that option needs.

Click Here for More Information



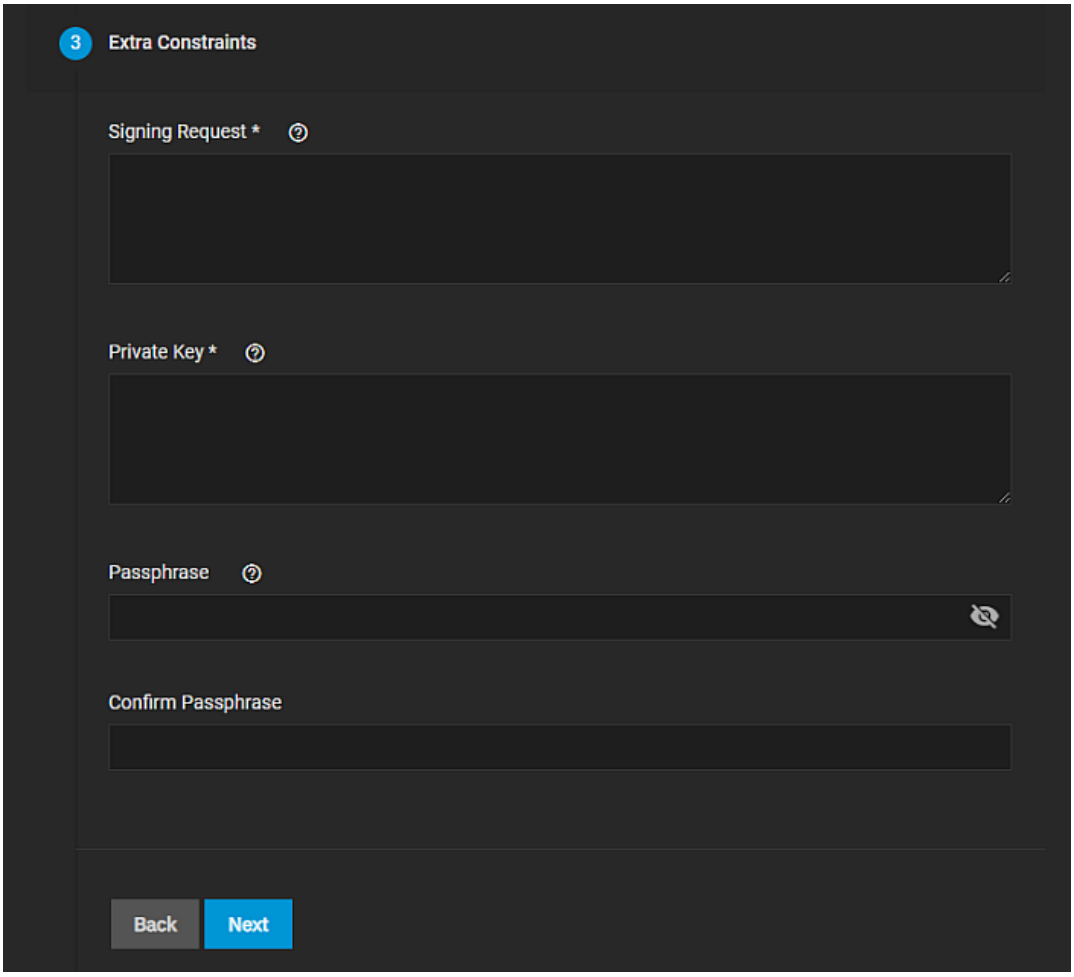
Setting	Description
Basic Constraints	Select to activate this extension. Basic Constraints extension identifies whether this certificate subject is a CA and the maximum depth of valid certification paths that include this certificate.
Path Length	Displays after selecting **Basic Constraints**. Enter how many non-self-issued intermediate certificates that can follow this certificate in a valid certification path. Entering **0** allows a single additional certificate to follow in the certificate path. Value cannot be less than **0**.
Basic Constraints Config	Select the option to specify the extension type from the dropdown list. Options are **CA** and **Critical Extension**. Specify whether to use the certificate for a Certificate Authority and whether this extension is critical. Clients must recognize critical extensions to prevent rejection. Web certificates typically require you to disable **CA** and enable **Critical Extension**.

Setting	Description
Extended Key Usage	Select to activate this certificate extension. The Extended Key Usage extension identifies and limits valid uses for this certificate, such as client authentication or server authentication. See RFC 3280, section 4.2.1.13 for more details. Displays the **Usages** field.
Usages	Displays after selecting **Extended Key Usage**. Select the option to identify the purpose of this public key from the dropdown list. Typically used for the end entity certificates. You can select multiple usages that display separated by a comma (,). Options are **ANY_EXTENDED_KEY_USAGE**, **CLIENT_AUTH**, **CODE_SIGNING**, **EMAIL_PROTECTION**, **OCSP_SIGNING**, **SERVER_AUTH**, or **TIME_STAMPING**. Do not mark this extension critical when set to **ANY_EXTENDED_KEY_USAGE**. Using both **Extended Key Usage** and **Key Usage** extensions requires that the purpose of the certificate is consistent with both extensions. See RFC 3280, section 4.2.13 for more details.
Critical Extension	Displays after selecting **Extended Key Usage**. Select to identify this extension as critical for the certificate. Critical extensions must be recognized by the certificate-using system or this certificate is rejected. Extensions identified as not critical can be ignored by the certificate-using system and the certificate still approved.
Key Usage	Select to activate this certificate extension. Displays the **Key Usage Config** field. The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate. The usage restriction might be employed when a key that could be used for more than one operation is to be restricted. For example, when an RSA key should be used only to verify signatures on objects other than public key certificates and CRLs, the **Digital Signature** bits are asserted. Likewise, when an RSA key should be used only for key management, the **Key Encipherment** bit is asserted. See RFC 3280, section 4.2.13 for more information.
Key Usage Config	Displays after selecting **Extended Key Usage** or **Key Usage**. Select the key usage extension from the dropdown list. Options are **Digital Signature**, **Content Commitment**, **Key Encipherment**, **Data Encipherment**, **Key Agreement**, **Key Cert Sign**, **CRL Sign**, **Encipher Only**, **Decipher Only** or **Critical Extension**. Web certificates typically need at least Digital Signature and possibly Key Encipherment or Key Agreement, while other applications may need other usages.

Extra Constraints - Import Certificate Signing Request Type

When **Type** on **Identifier and Type** is set to **Import Certificate Signing Request** the **Extra Constraints** screen does not include the options to set extension types.

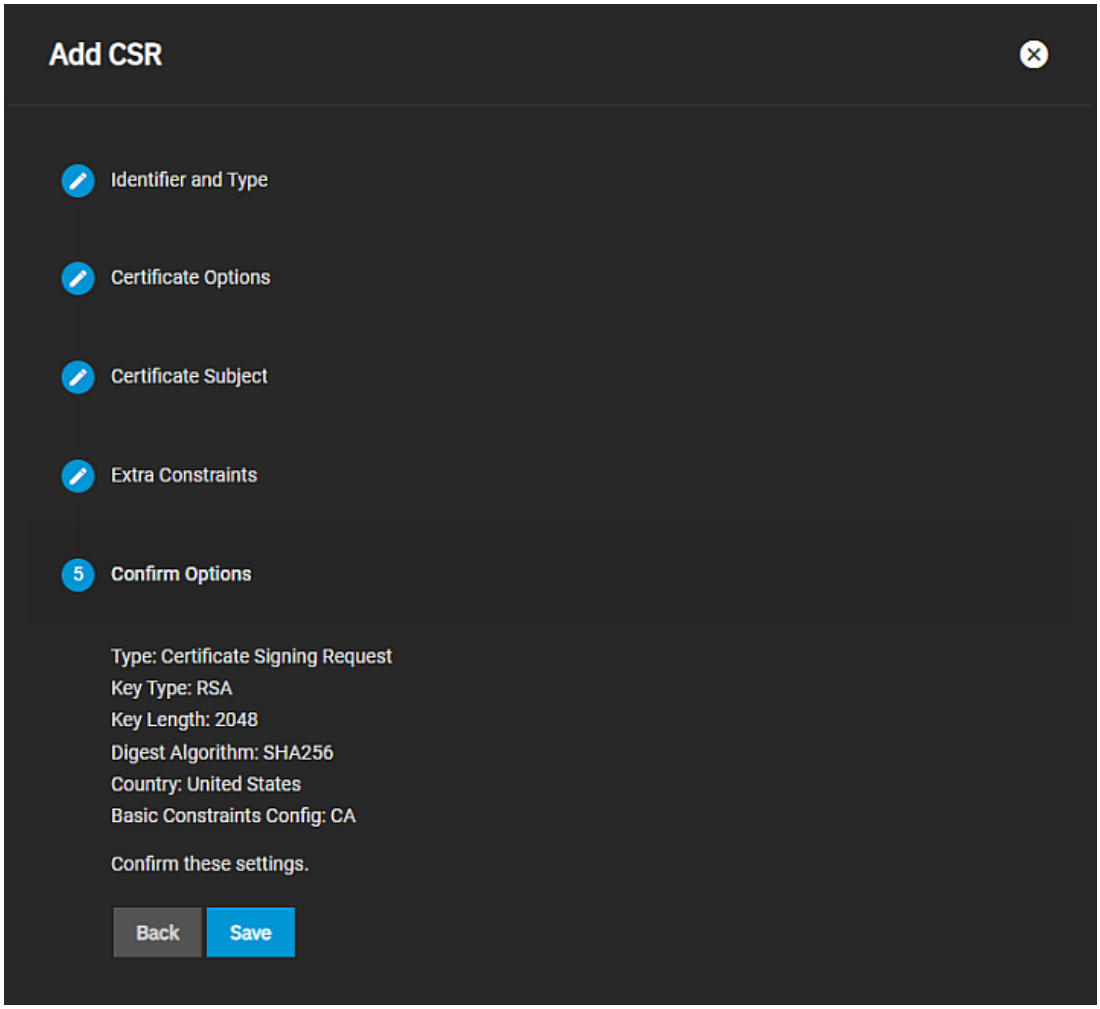
Click Here for More Information ↧



Setting	Description
Certificate	Required. Paste the certificate for the certificate signing request into this field.
Private Key	Required. Paste the private key associated with the certificate when available. Provide a key at least 1024 bits long.
Passphrase	Enter the passphrase for the private key.
Confirm Passphrase	Re-enter the passphrase for the private key.

Confirm Options

The final step screen is the **Confirm Options** that displays the CA **Type**, **Key Type**, **Key Length**, **Digest Algorithm**, **Lifetime**, **Country**, and **Basich Constraints Config**. For **Import Certificate Signing Request** type, the screen displays **Type**, **Signing Request** and **Private Key**.



Save adds the certificate to SCALE. **Back** returns to previous screens to make changes before you save. **Next** advances to the next screen in the sequence to return to **Confirm Options**.

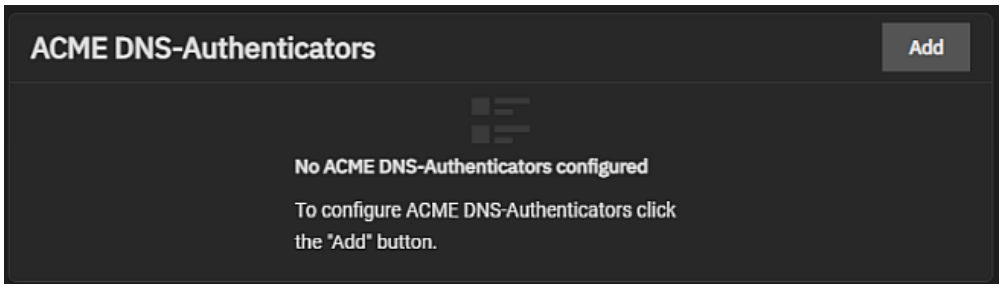
Related Content

- Certificates Screens
- Managing Certificates
- Certificates Authorities Screens
- Managing Certificate Authorities
- Managing Certificate Signing Requests
- Adding ACME DNS-Authenticators

4.7.5.4 - ACME DNS-Authenticators Screens

This article provides information on SCALE Certificates screens and settings.

The **Certificates** screen includes the **ACME DNS-Authenticators** widget that displays a list of authenticators configured on the screen. The Automatic Certificate Management Environment (ACME) DNS-Authenticators screen allows users to automate certificate issuing and renewal. The user must verify ownership of the domain before certificate automation is allowed.



Each authenticator listed is a link that opens the **Edit ACME DNS-Authenticator** screen for the selected authenticator.

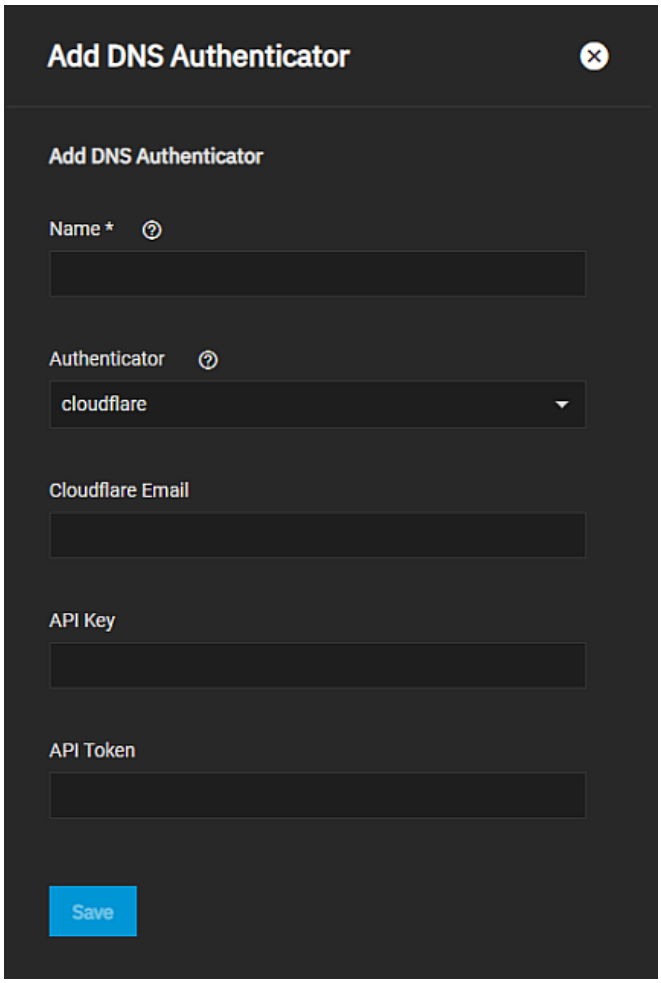
deletes the authenticator from your server.

Add opens the **Add ACME DNS-Authenticator** screen.

> The system requires an ACME DNS authenticator and CSR to configure ACME certificate automation.

Add DNS Authenticator

The settings change based on the **Authenticator** selection.



Setting	Description
Name	Required. Enter an internal identifier for the authenticator.
Authenticator	Select a DNS provider from the dropdown list and configure any required authenticator attributes. Options are **cloudflare** and Amazont **route53**.
Cloudflaire Email	Enter the email address for the cloudflare account.
API Key	Displays when **Authenticator** is set to **cloudflare**. Enter the API Key.
API Token	Displays when **Authenticator** is set to **cloudflare**. Enter the API token.
Access Key Id	Required. Displays when **Authenticator** is set to **route53**. Enter the access key ID.
Secret Access Key	Required. Displays when **Authenticator** is set to **route53**. Enter the secret access key.

Related Content

- Adding ACME DNS-Authenticators

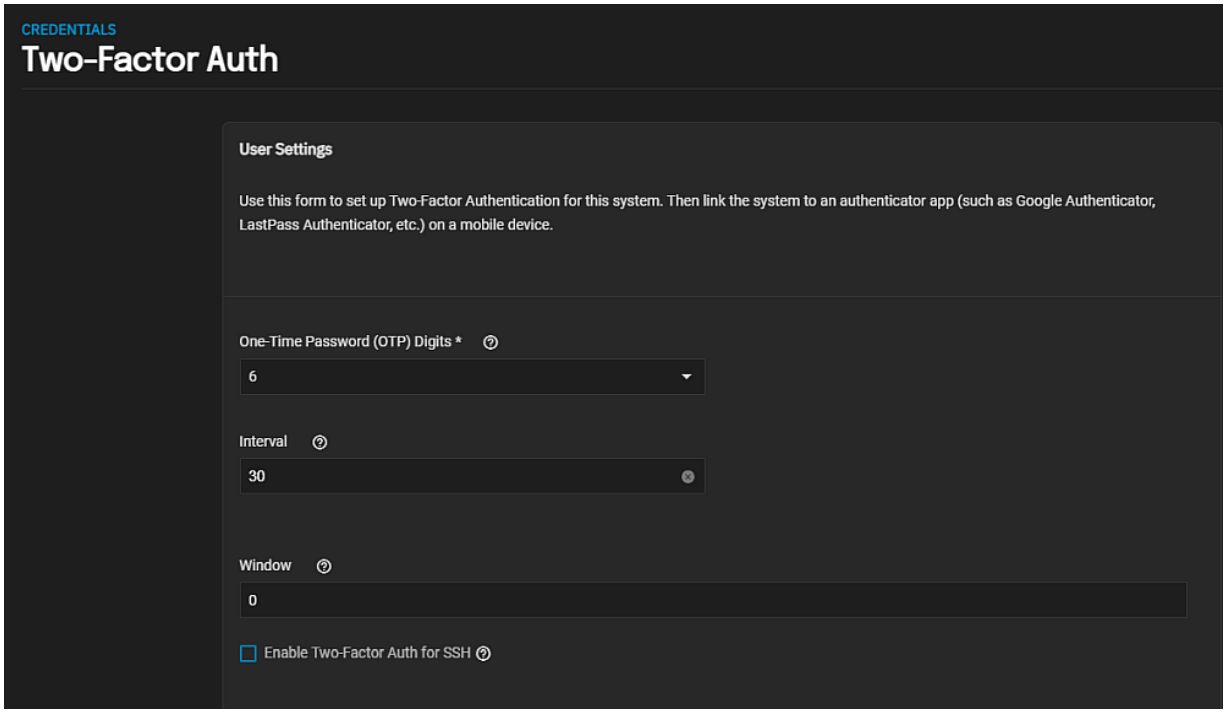
4.7.6 - Two-Factor Auth Screen

This article provides information on two-factor authentication screen settings.

The **Two-Factor Auth** screen displays setting to configure and enable two-factor authentication (2FA) on TrueNAS SCALE.

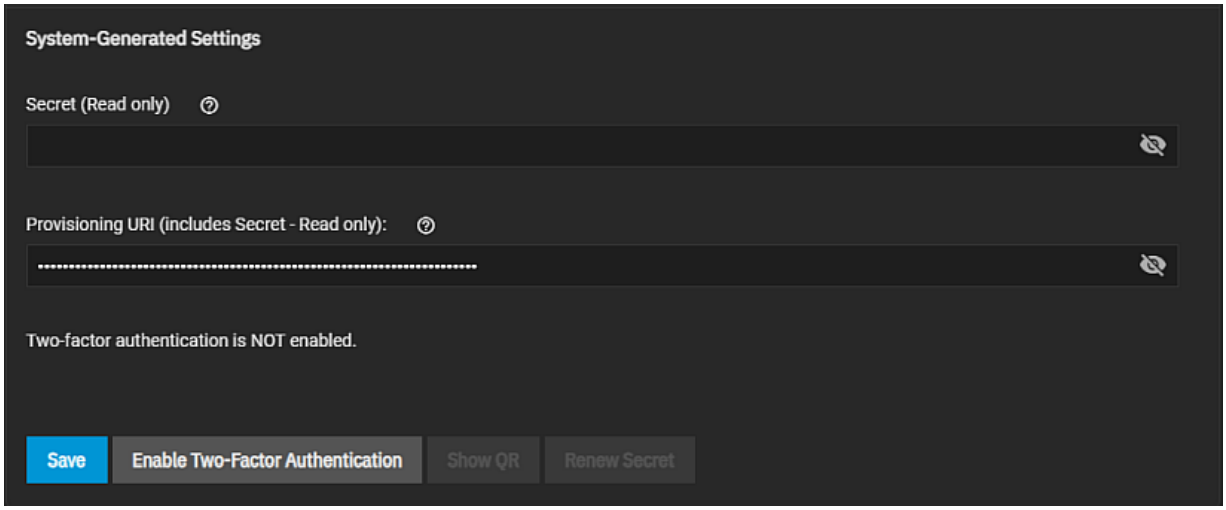
> Two-factor authentication is time-based and requires a correct system time setting.

User Settings



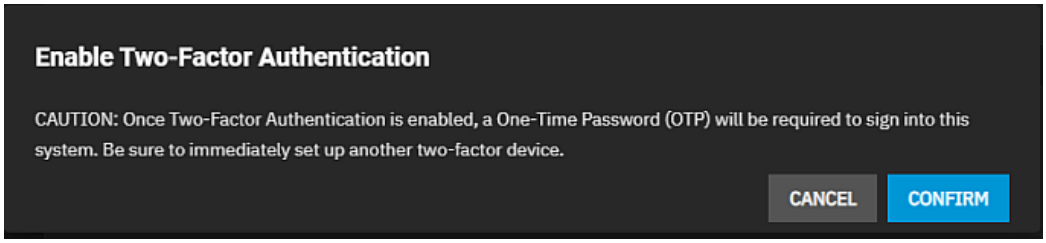
Name	Description
One Time Password (OTP) Digits	Select the number of digits for the length of the one-time password (OTP). The default is **6**, which is the standard OTP length for Google OTPs. Check your app/device settings before selecting a value.
Interval	Enter the number of seconds for the lifespan of each OTP. Default is **30** seconds. The minimum is 5 seconds.
Window	Enter the number of valid passwords. Extends password validity beyond the **Interval** setting. For example, *1* means that one password before and after the current password is valid, leaving three valid passwords. Extending the window is useful in high-latency situations.
Enable Two-Factor Auth for SSH	Select to enable 2FA for system SSH access. Leave this disabled until you complete a successful test of 2FA with the UI.

System Generated Settings



Name	Description
Secret (Read-only)	TrueNAS creates the secret and uses it to generate OTPs when you first enable 2FA.
Provisioning URI (includes Secret - Read-only)	TrueNAS created the URI used to provision an OTP. TrueNAS encodes the URI (which contains the secret) in a QR Code. To set up an OTP app like Google Authenticator, use the app to scan the QR code or enter the secret manually into the app. TrueNAS produces the URI when you first activate 2FA.

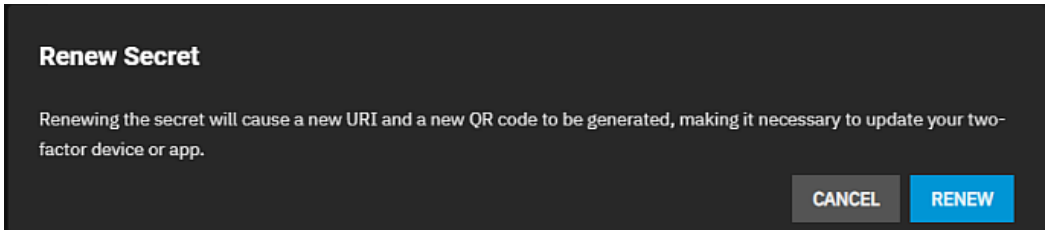
Enable Two Factor Authentication opens the **Enable Two-Factor Authentication** confirmation dialog. Click **Confirm** to enable 2F.



The enable button changes to **Disable Two-Factor Authentication**.

Show QR opens a QR code dialog. Scan with a mobile device that has the Google Authenticator app.

Renew Secret changes the system-generated **Secret** and **Provisioning URI** values.



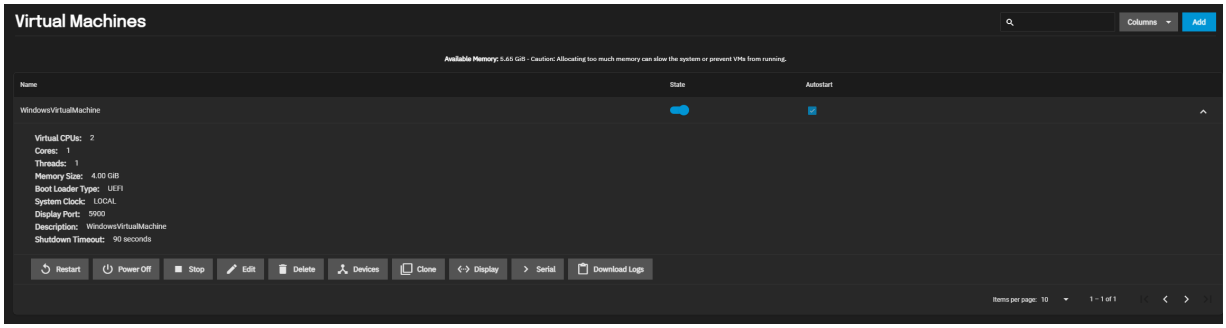
The icon in the **Secret** and **Provisioning URI** fields displays the alphanumeric string. The icon converts the alphanumeric characters back to asterisks.

Related Content

- Using 2FA (Two-Factor Authentication)

4.8 - Virtualization Screens

The Virtualization section allows users to set up Virtual Machines (VMs) to run alongside TrueNAS. Delegating processes to VMs reduces the load on the physical system, which means users can utilize additional hardware resources. Users can customize six different segments of a VM when creating one in TrueNAS SCALE.



Ready to get started? Choose a topic or article from the left-side **Navigation** pane. Click the **<** symbol to expand the menu to show the topics under this section.

Article Summaries

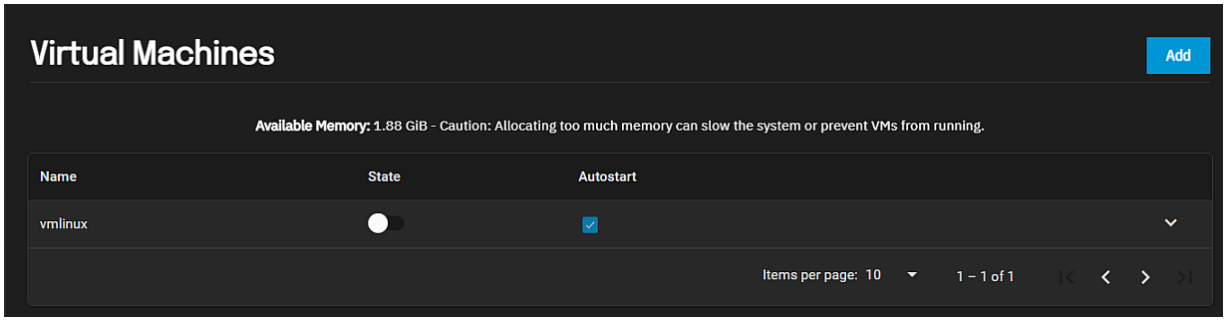
- Virtualization Screens

  This article provides information on the screens and settings to add virtual machines and devices VMs use to your TrueNAS SCALE system.

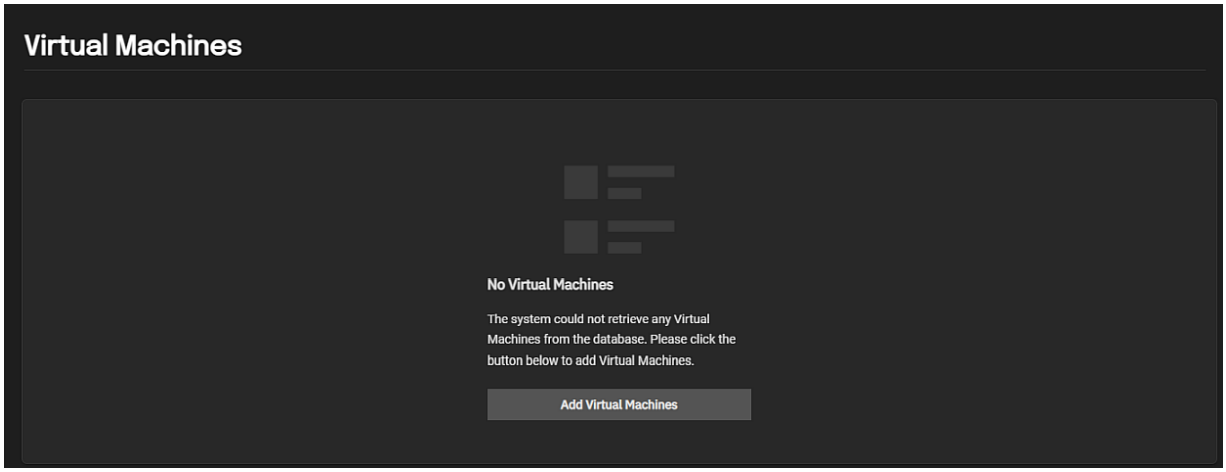
4.8.1 - Virtualization Screens

This article provides information on the screens and settings to add virtual machines and devices VMs use to your TrueNAS SCALE system.

The **Virtualization** option displays the **Virtual Machines** screen that displays the list of VMs configured on the TrueNAS SCALE system.



If there are no VMs configured on the system, the **No Virtual Machines** screen displays. This also displays if you delete all VMs on the system.



Add Virtual Machines and the **Add** button in the top right of the screen opens the **Create Virtual Machine** wizard configuration screens.

After adding virtual machines (VMs) to the system the screen displays a list of the VMs.

Click on the VM name or the expand down arrow to the right of a VM to open the details screen for that VM.

The **State** toggle displays and changes the state of the VM. The **Autostart** checkbox, when selected, automatically starts the VM if the system reboots. When cleared you must manually start the VM.

Create Virtual Machine Wizard Screens

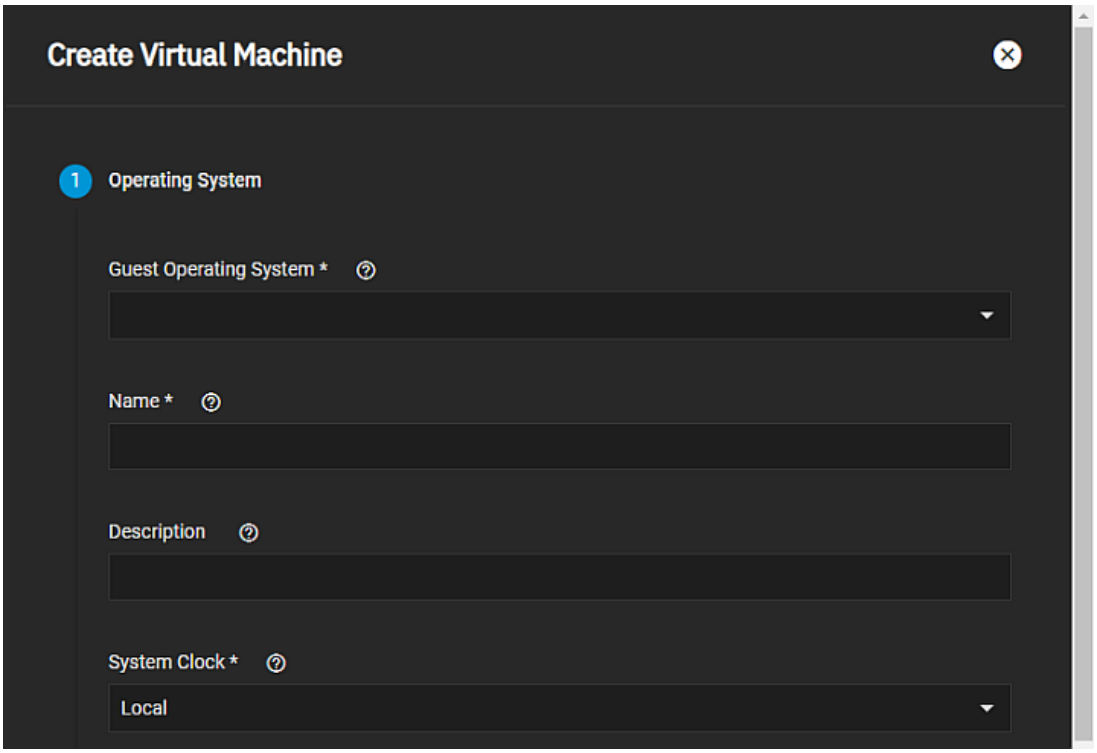
The **Create Virtual Machine** configuration wizard displays all settings to set up a new virtual machine.

Use **Next** and **Back** to advance to the next or return to the previous screen to change a setting. Use **Save** to close the wizard screens and add the new VM to the **Virtual Machines** screen.

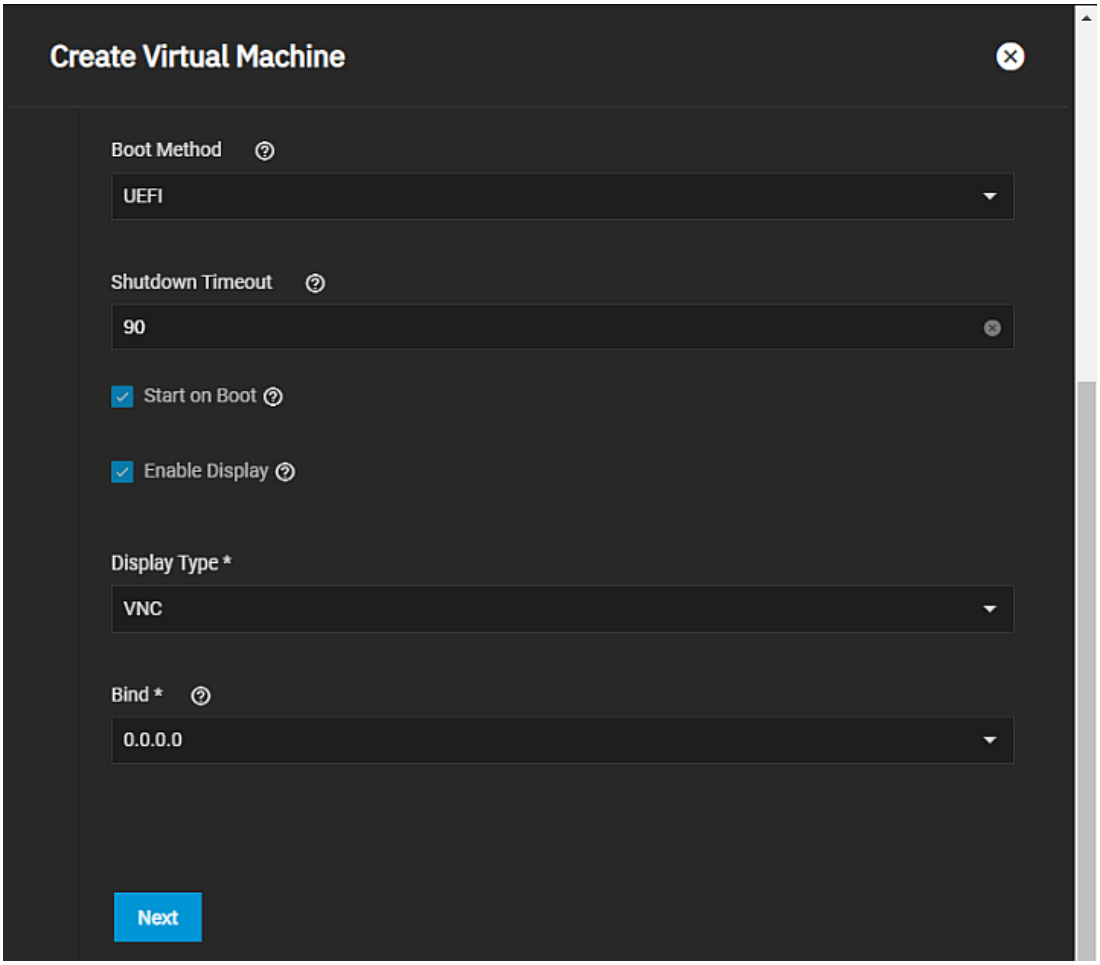
Operating System Screen

The **Operating System** configuration screen settings specify the VM operating system type, the time it uses, its boot method, and its display type.

Click Here for More Information



Field	Description
Guest Operating System	Required. Select the VM operating system type from the dropdown list. Select from **Windows**, **Linux** or **FreeBSD**.
Name	Required. Enter an alphanumeric name for the virtual machine.
Description	Enter a description (optional).
System Clock	Select the VM system time from the dropdown list. Options are **Local** or **UTC**. Default is **Local**.

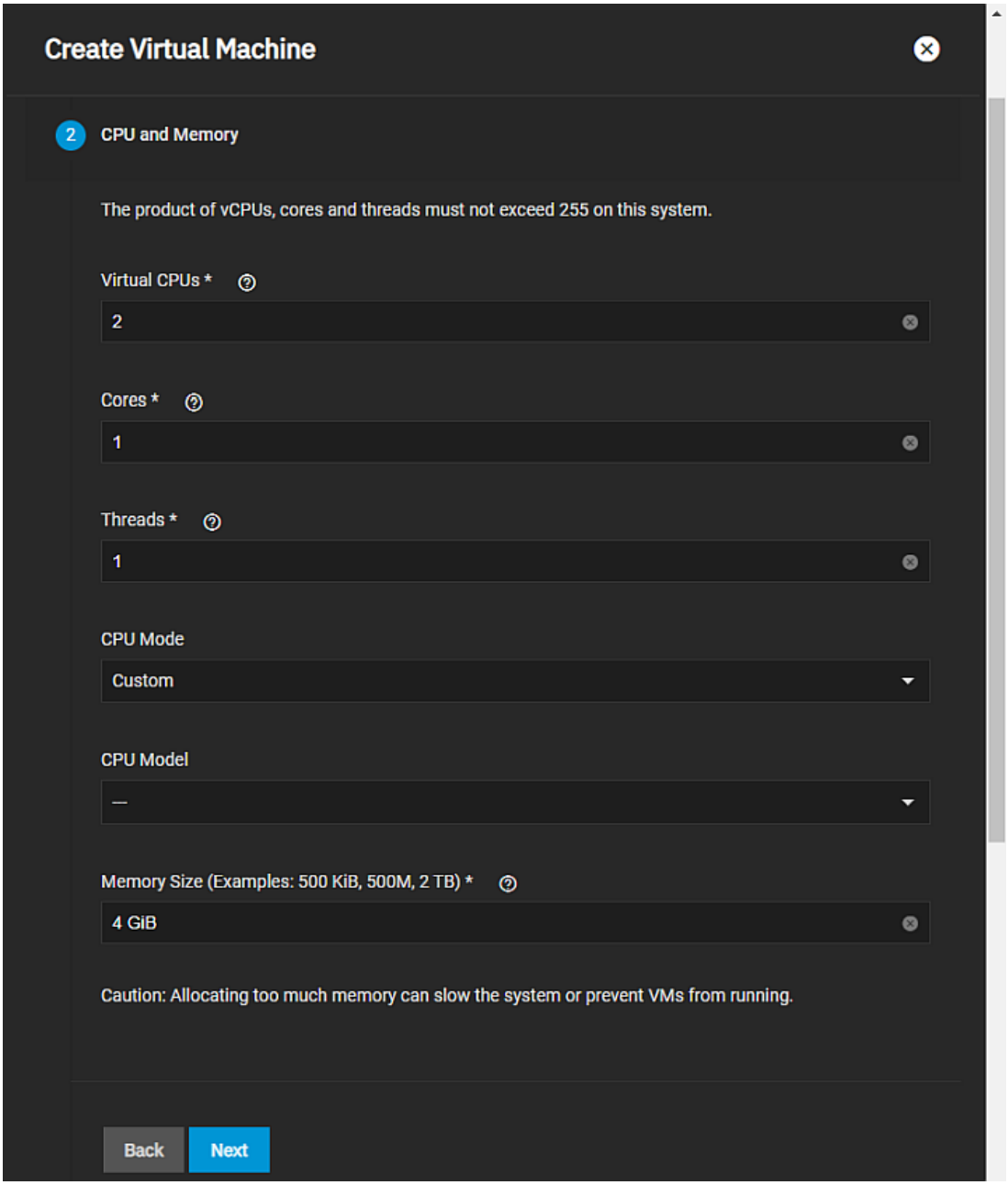


Field	Description
Boot Method	Select the boot method option from the dropdown list. Select **UEFI** for newer operating systems or **Legacy BIOS** for older operating systems that only support BIOS booting.
Shutdown Timeout	Enter the time in seconds the system waits for the VM to cleanly shut down. During system shutdown, the system initiates power-off for the VM after the shutdown timeout entered expires.
Start on Boot	Select to start this VM when the system boots.
Enable Display	Enable a Display (Virtual Network Computing) remote connection. Requires UEFI booting.
Display Type	Select either VNC or SPICE from the dropdown list.
Bind	Select the IP address option from the dropdown list. The primary interface IP address is the default. A different interface IP address can be chosen.

CPU and Memory Screen

The **CPU and Memory** configuration wizard screen settings specify the number of virtual CPUs to allocate to the virtual machine, cores per virtual CPU socket, and threads per core. Also to specify the CPU mode and model, and the memory size.

Click Here for More Information

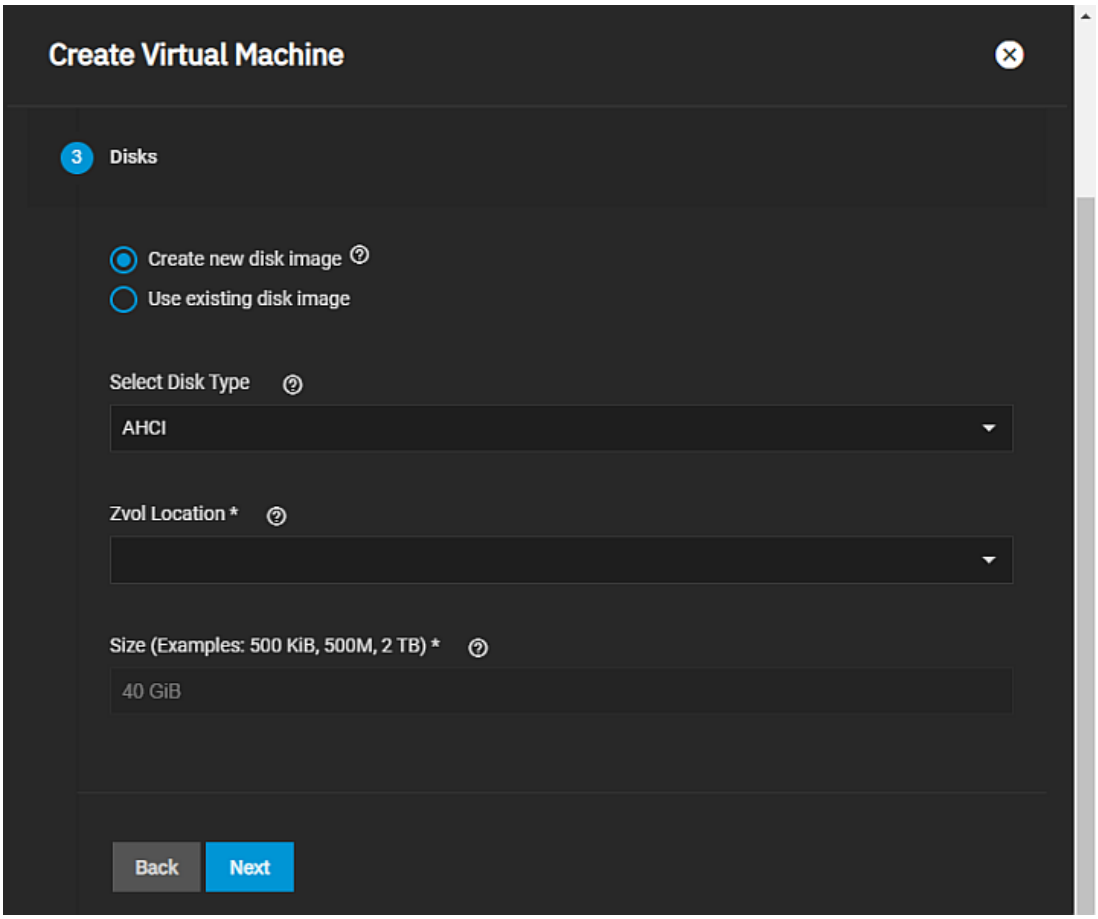


Field	Description
Virtual CPUs	Required. Enter the number of virtual CPUs to allocate to the virtual machine. The maximum is 16, or fewer if the host CPU limits the maximum. The VM operating system might impose operational or licensing restrictions on the number of CPUs.
Cores	Required. Enter the number of cores per virtual CPU socket. The product of vCPUs, cores, and threads must not exceed 16.
Threads	Required. Enter the number of threads per core. A single CPU core can have up to two threads per core. A dual core could have up to four threads. The product of vCPUs, cores, and threads must not exceed 16.
CPU Mode	Select the CPU mode attribute from the dropdown list to allow your guest VM CPU to be as close to the host CPU as possible. Select **Custom** to make it so a persistent guest virtual machine sees the same hardware no matter what physical physical machine the guest VM boots on. It is the default if the CPU mode attribute is not specified. This mode describes the CPU presented to the guest. Select **Host Model** to use this shortcut to copying the physical host machine CPU definition from the capabilities XML into the domain XML. As the CPU definition copies just before starting a domain, a different physical host machine can use the same XML while still providing the best guest VM CPU each physical host machine supports. Select **Host Passthrough** when the CPU visible to the guest VM is exactly the same as the physical host machine CPU, including elements that cause errors within libvirt. The downside of this is you cannot reproduce the guest VM environment on different hardware.
CPU Model	Select a CPU model to emulate.
Memory Size	Allocate RAM for the VM. Minimum value is 256 MiB. This field accepts human-readable input (Ex. 50 GiB, 500M, 2 TB). If units are not specified, the value defaults to bytes.

Disks Screen

The **Disks** configuration wizard screen settings specify whether to create a new zvol on an existing dataset for a disk image or use an existing zvol or file for the VM. You also specify the disk type, zvol location and size.

Click Here for More Information

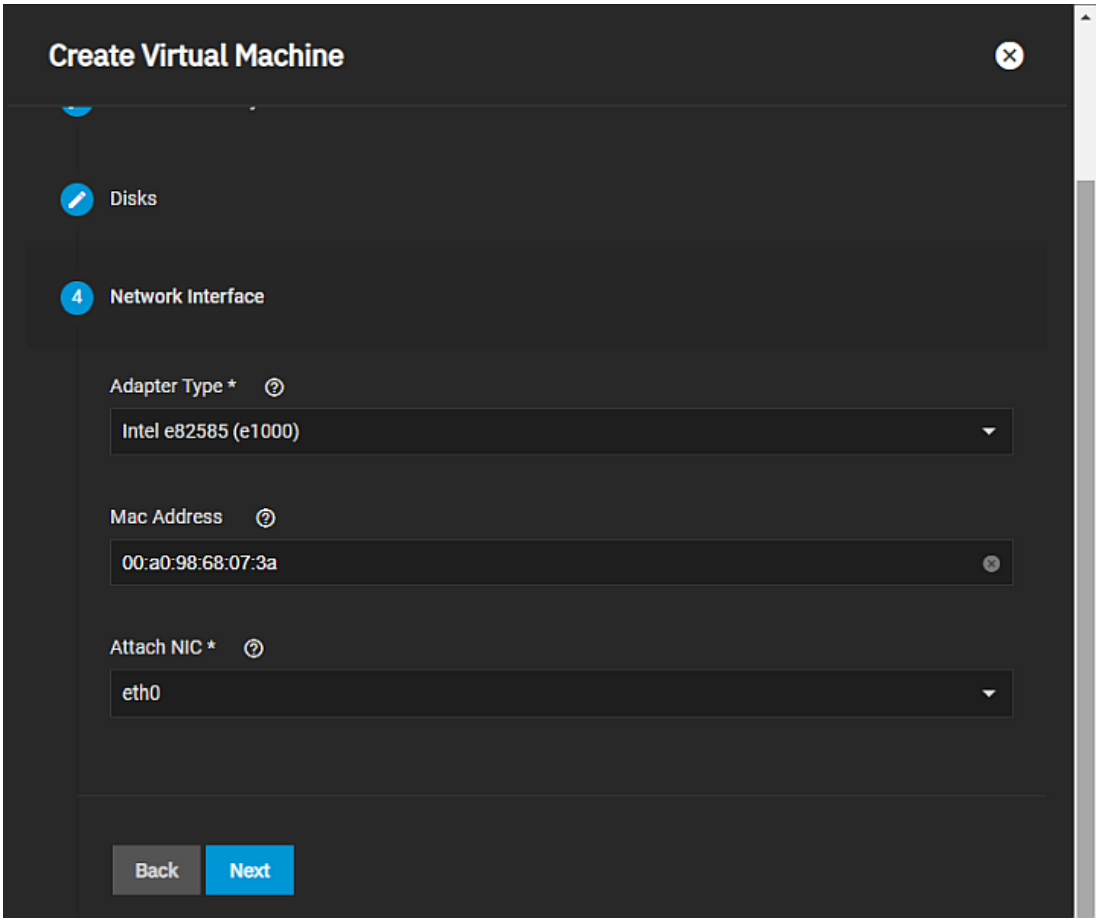


Field	Description
Create new disk image	Select this radio button to create a new zvol on an existing dataset to use as a virtual hard drive for the VM.
Use existing disk image	Select this radio button to use an existing zvol or file for the VM. Displays the **Select Existing Zvol** dropdown list field.
Select Disk Type	Select desired disk type as either **AHCI** or **VirtIO** from the dropdown list. Select**AHCI** for Windows VMs. **VirtIO** requires a guest OS that supports VirtIO paravirtualized network drivers.
Zvol Location	Select a dataset for the new zvol from the dropdown list of datasets on the system.
Size	Required. Allocate space for the new zvol. (Examples: 500 KiB, 500M, 2 TB). Units smaller than MiB are not allowed.
Select Existing Zvol	Displays after selecting the **Use existing disk image** radio button. Select an existing zvol from the dropdown list of zvols on the system.

Network Interface Screen

The **Network Interface** screen settings specify the network adaptor type, mac address and the physical network interface card associated with the VM.

Click Here for More Information

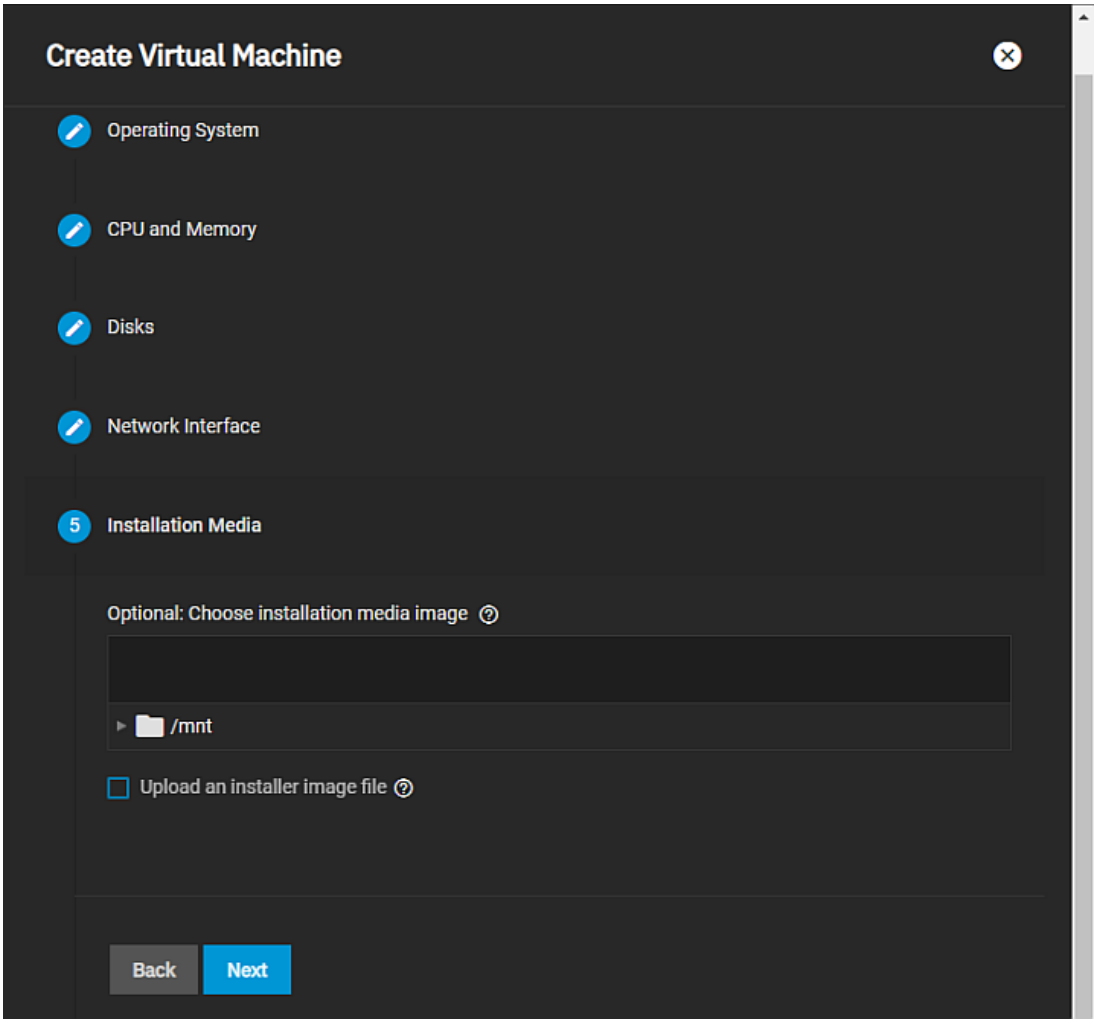


Field	Description
Adapter Type	Select the adaptor type from the dropdown list. **Intel e82545 (e1000)** emulates the same Intel Ethernet card and provides compatibility with most operating systems. **VirtIO** provides better performance when the operating system installed in the VM supports VirtIO para-virtualized network drivers.
Mac Address	Enter the desired address into the field to override the randomized MAC address.
Attach NIC	Select the physical interface to associate with the VM from the dropdown list.

Installation Media Screen

The **Installation Media** screen settings specify the operation system installation media image on a dataset or upload one from the local machine.

Click Here for More Information

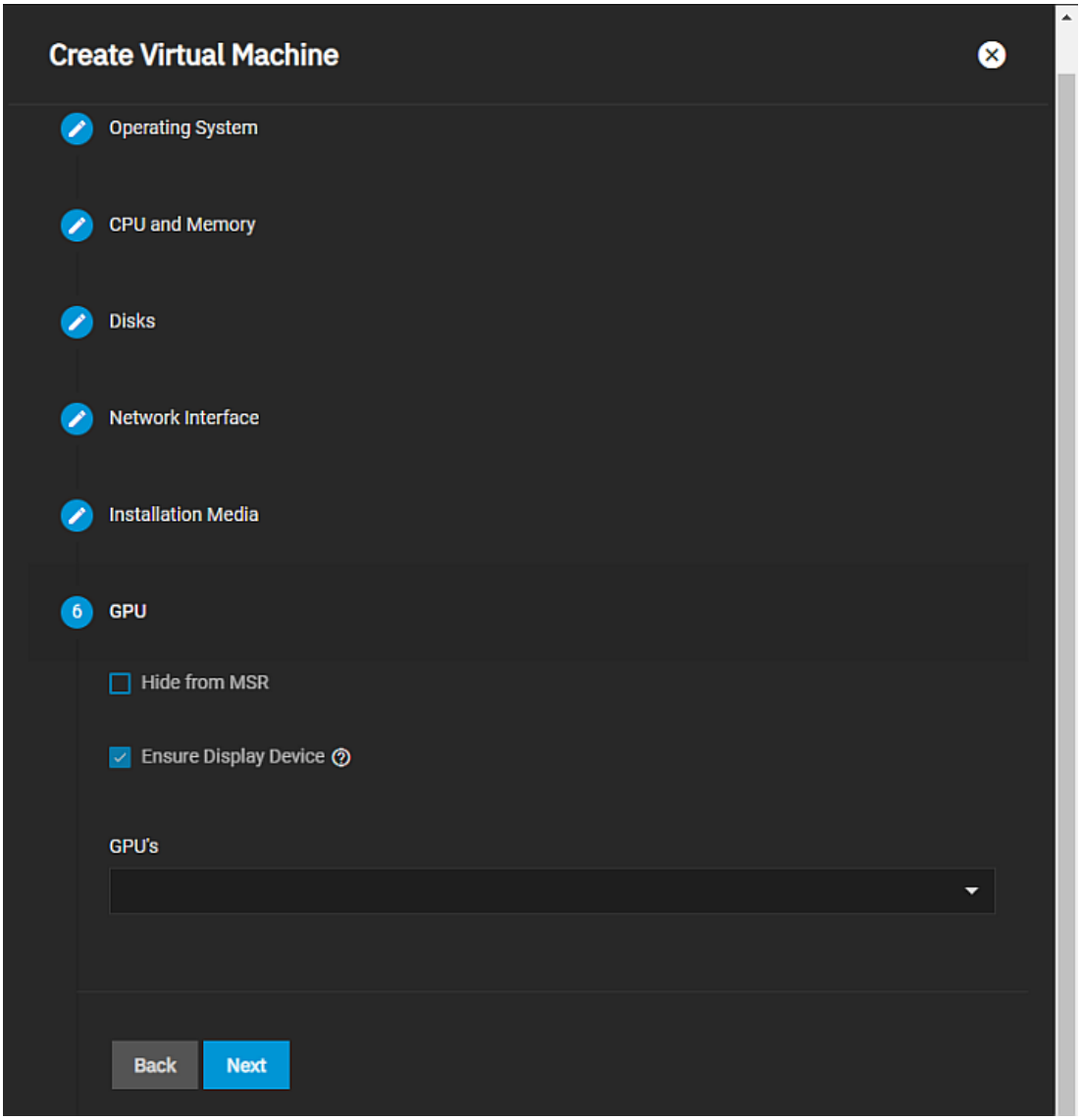


Field	Description
Choose Installation Media Image	Ether the path or browse to the operating system installer image file. To collapse the browse tree click on the to the left of **/mnt**.
Upload an Installer Image File	Select to display image upload the **ISO save location** and browse **/mnt** options that populate the field with the mount path, and the **Choose File** button.
Choose File	Click to save the path populated in the **ISO save location** field.
Upload	Click to upload the file selected in the **ISO save location** field.

GPU Screen

The **GPU** screen settings specify graphic processing unit (GPU) for the VM. It also provides the option to hide the VM from the Microsoft Reserved Partition (MSR) on Windows systems.

Click Here for More Information



Field	Description
Hide from MSR	Select to enable the VM to hide the GPU from the Microsoft Reserved Partition (MSR).
Ensure Display Device	Select to ensure that the guest always has access to a video device. Required for headless installations like ubuntu server for the guest to operate properly. Leave checkbox clear for cases where want to use a graphic processing unit (GPU) passthrough and do not want a display device added.
GPU's	Select a physical GPU on your system from the dropdown list to use for the VM.

Confirm Options Screen

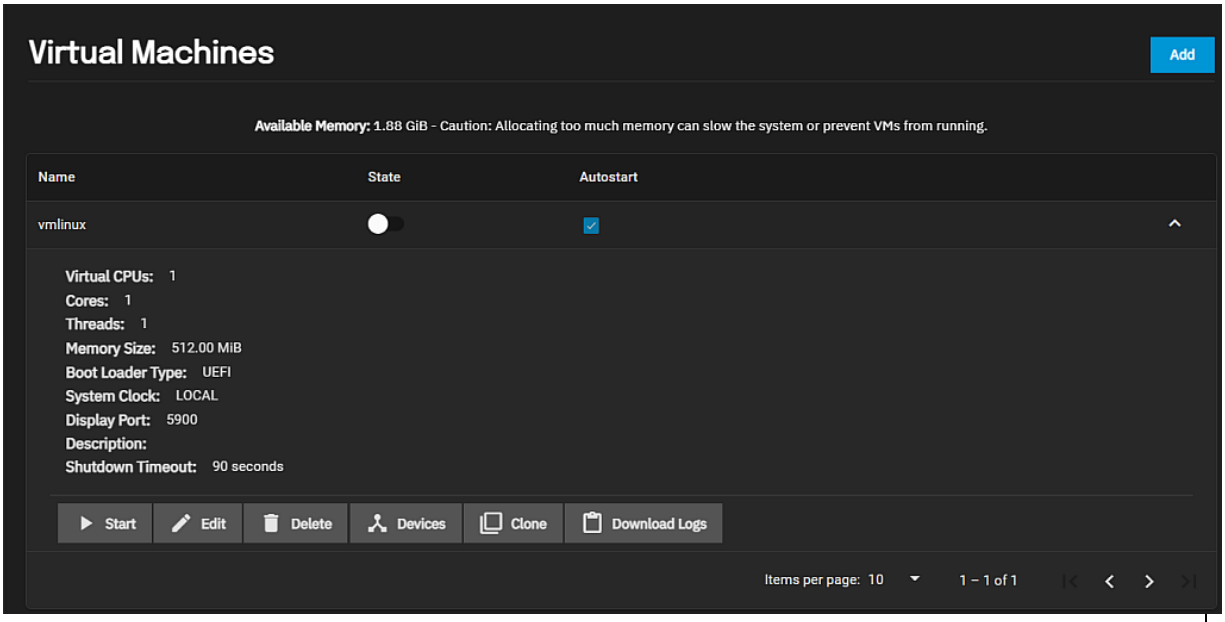
The **Confirm Options** screen displays the settings selected using the **Create Virtual Machine** wizard screens. It displays the number CPUs, cores, threads, the memory, name of the VM and the disk size.

Click **Save** to add the VM to the **Virtual Machines** screen. Click **Back** to return to the previous screens to make changes.

Virtual Machine Detail Screen

The details view of any VM displays the basic information on the number of virtual CPUS, cores, and threads, the amount of memory, boot load and system clock types, the display port number and the shutdown timout in seconds.

Click Here for More Information



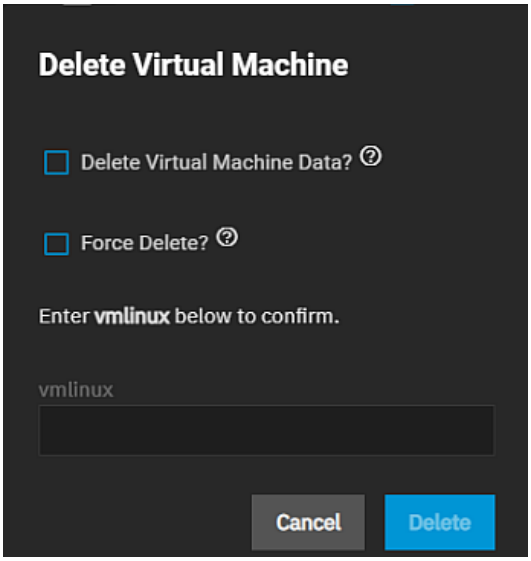
The buttons below the details show the actions options for each VM.

Operation	Icon	Description
START		Starts a VM. The toggle turns blue when the VM switches to running. Toggles to **Stop**. After clicking **Start** the **Restart**,**Power Off**, **Display** and **Serial Shell** option buttons display.
RESTART		Retarts the VM.
POWER OFF		Powers off and halts the VM, similar to turning off a computer power switch.
STOP		Stops a running VM. Because a virtual machine does not always respond well to **STOP** or the command might time-out if the VM does not have an OS. Use **Power Off** instead.
EDIT		Opens the **Edit Virtual Machine** that displays editable VM settings. You cannot edit a VM while it is running. You must first stop the VM and then you can edit the properties and settings.
DELETE		Deletes a VM. Opens a delete dialog that allows you to remove the VM from your system. You cannot delete a virtual machine that is running. You must first stop the VM and then you can delete it.
DEVICES		opens the **Virtual Machine Devices** screen with a list of virtual machine devices configured on the system.
CLONE		Makes an exact copy or *clone* of the VM that you can select and edit. Opens the **Clone** dialog that allows you to clone the selected VM. Enter a name for the cloned VM. Naming the clone VM is optional. The cloned VM displays on the Virtual Machines list with the extension **_clone0**. If you clone the same VM again the extension for the second clone is **clone1**.
Display		Opens a **noVCN** window that allows you to connect to a
SERIAL		Opens the TrueNAS **VM Serial Shell** screen.
Download Logs		Downloads a .log file to the system.

Delete Virtual Machine Dialog

Delete removes the VM configuration from your system.

Click Here for More Information



Field	Description
Delete Virtual Machine Data	Select to remove the data associated with this virtual machine. This results in data loss if the data is not backed up. Leave unselected to keep the VM data intact.
Force Delete	Select to ignore the virtual machine status during the delete operation. Leave unselected to prevent deleting the VM when it is still active or has an undefined state.
Enter *vmname* below to confirm	Enter the name of the VM to confirm you want to delete the selected VM.

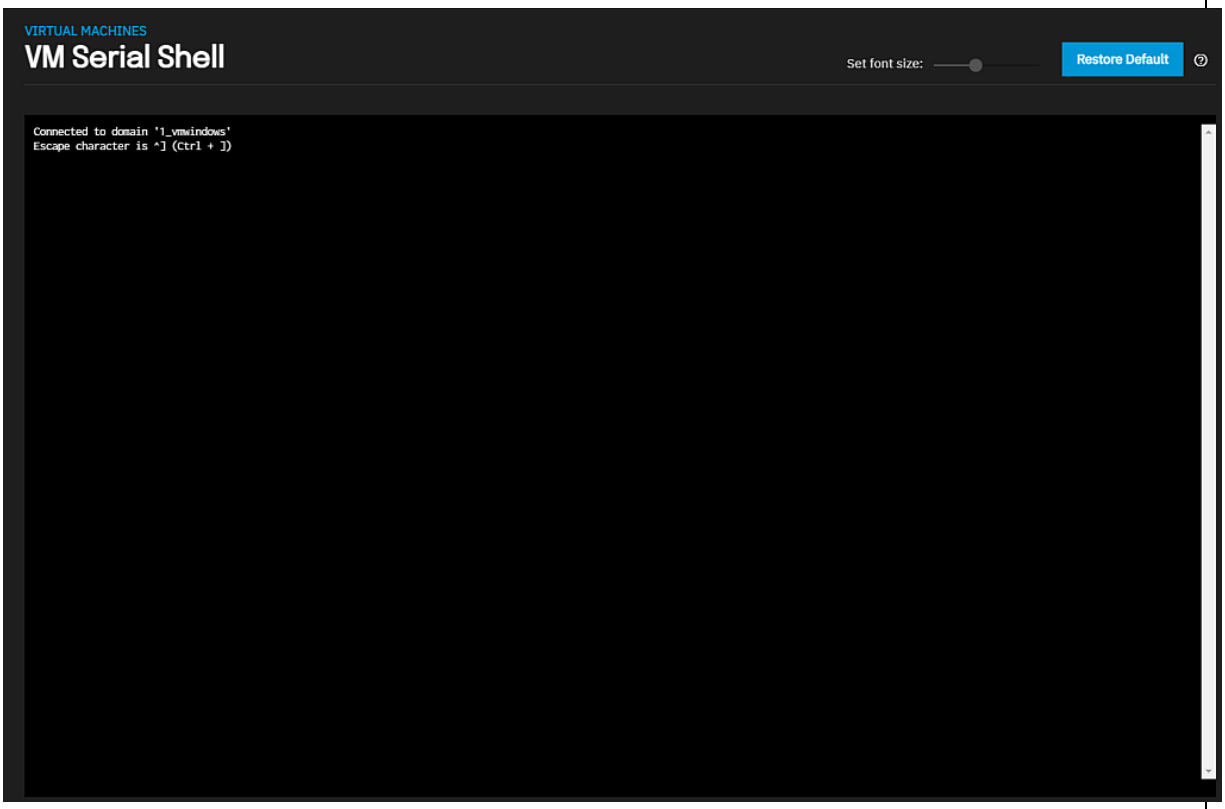
Clone Virtual Machine Window

The **Clone** option opens a **Name** dialog where you can enter an optional name for a clone or exact duplicate of the selected VM.

VM Serial Shell Screen

Serial Shell opens the **VM Serial Shell** window where you can enter commands for the selected virtual machine.

Click Here for More Information



Click **Virtual Machines** in the header to return to the **Virtual Machine** screen.

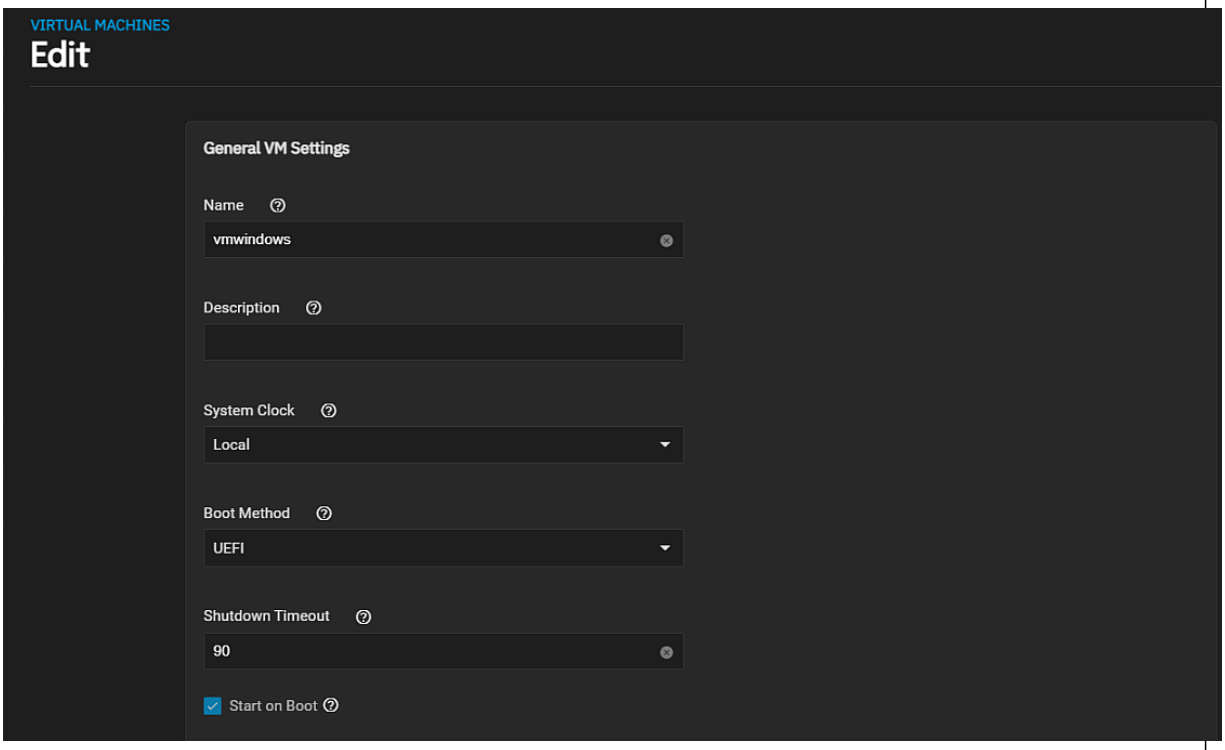
Edit Virtual Machine Screen

The **Virtual Machine > Edit** screens settings are a subset of those found on the **Create Virtual Machine** settings.

Edit General Settings

The **Edit** screen **General Settings** specify the basic settings for the VM. Unlike the **Create Virtual Machine** wizard, you cannot change the **Enable** or **Start on Boot** status or change the display type or bind address for a saved VM.

Click Here for More Information

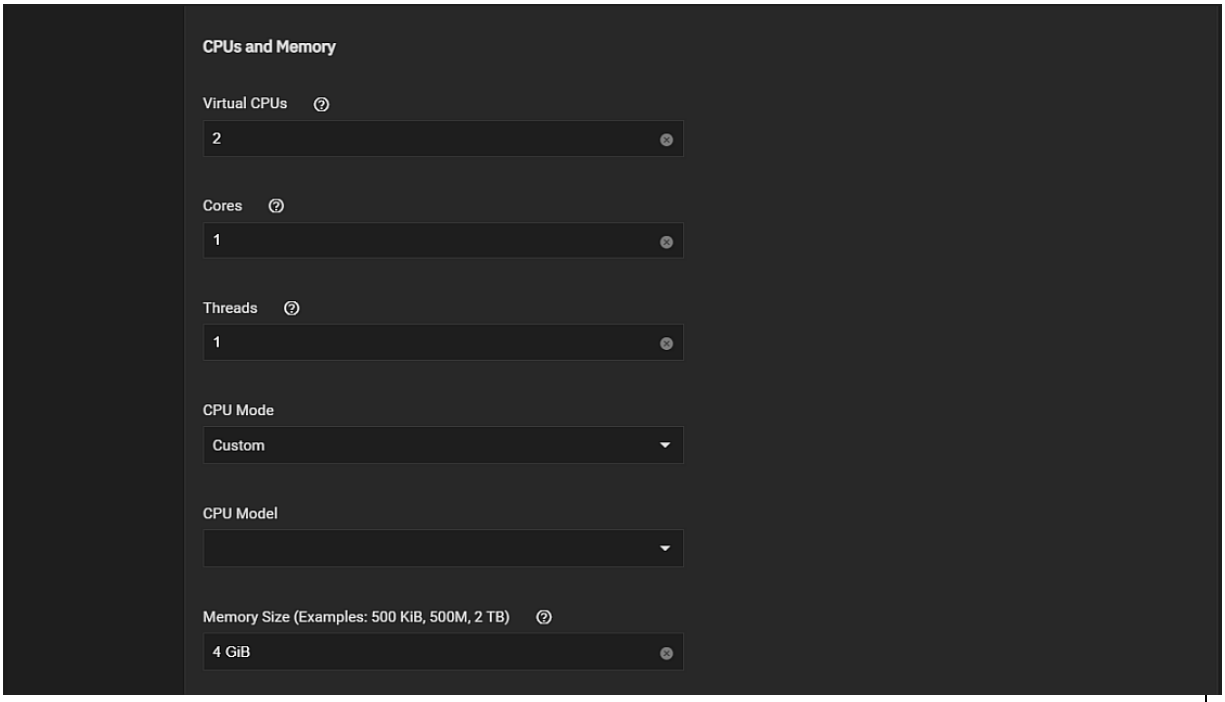


Field	Description
Guest Operating System	Required. Select the VM operating system type from the dropdown list. Select from **Windows**, **Linux** or **FreeBSD**.
Name	Required. Enter an alphanumeric name for the virtual machine.
Description	Enter a description (optional).
System Clock	Select the VM system time from the dropdown list. Options are **Local** or **UTC**. Default is **Local**.
Boot Method	Select the boot method option from the dropdown list. Select **UEFI** for newer operating systems or **Legacy BIOS** for older operating systems that only support BIOS booting.
Shutdown Timeout	Enter the time in seconds the system waits for the VM to cleanly shut down. During system shutdown, the system initiates power-off for the VM after the shutdown timeout entered expires.
Start on Boot	Select to start this VM when the system boots.

Edit CPU and Memory Settings

The **Edit** screen **CPU and Memory** settings are the same as those in the **Create Virtual Machine** wizard screen.

Click Here for More Information

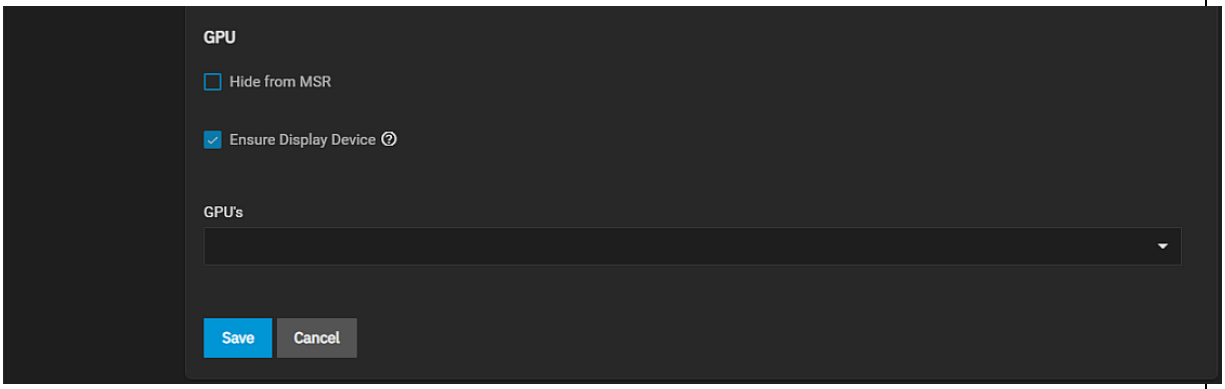


Field	Description
Virtual CPUs	Required. Enter the number of virtual CPUs to allocate to the virtual machine. The maximum is 16, or fewer if the host CPU limits the maximum. The VM operating system might impose operational or licensing restrictions on the number of CPUs.
Cores	Required. Enter the number of cores per virtual CPU socket. The product of vCPUs, cores, and threads must not exceed 16.
Threads	Required. Enter the number of threads per core. A single CPU core can have up to two threads per core. A dual core could have up to four threads. The product of vCPUs, cores, and threads must not exceed 16.
CPU Mode	Select the CPU mode attribute from the dropdown list to allow your guest VM CPU to be as close to the host CPU as possible. Select **Custom** to make it so a persistent guest virtual machine sees the same hardware no matter what physical physical machine the guest VM boots on. It is the default if the CPU mode attribute is not specified. This mode describes the CPU presented to the guest. Select **Host Model** to use this shortcut to copying the physical host machine CPU definition from the capabilities XML into the domain XML. As the CPU definition copies just before starting a domain, a different physical host machine can use the same XML while still providing the best guest VM CPU each physical host machine supports. Select **Host Passthrough** when the CPU visible to the guest VM is exactly the same as the physical host machine CPU, including elements that cause errors within libvirt. The downside of this is you cannot reproduce the guest VM environment on different hardware.
CPU Model	Select a CPU model to emulate.
Memory Size	Allocate RAM for the VM. Minimum value is 256 MiB. This field accepts human-readable input (Ex. 50 GiB, 500M, 2 TB). If units are not specified, the value defaults to bytes.

Edit GPU Settings

The **Edit** screen **GPU** settings are the same as those in the **Create Virtual Machine** wizard screens.

Click Here for More Information

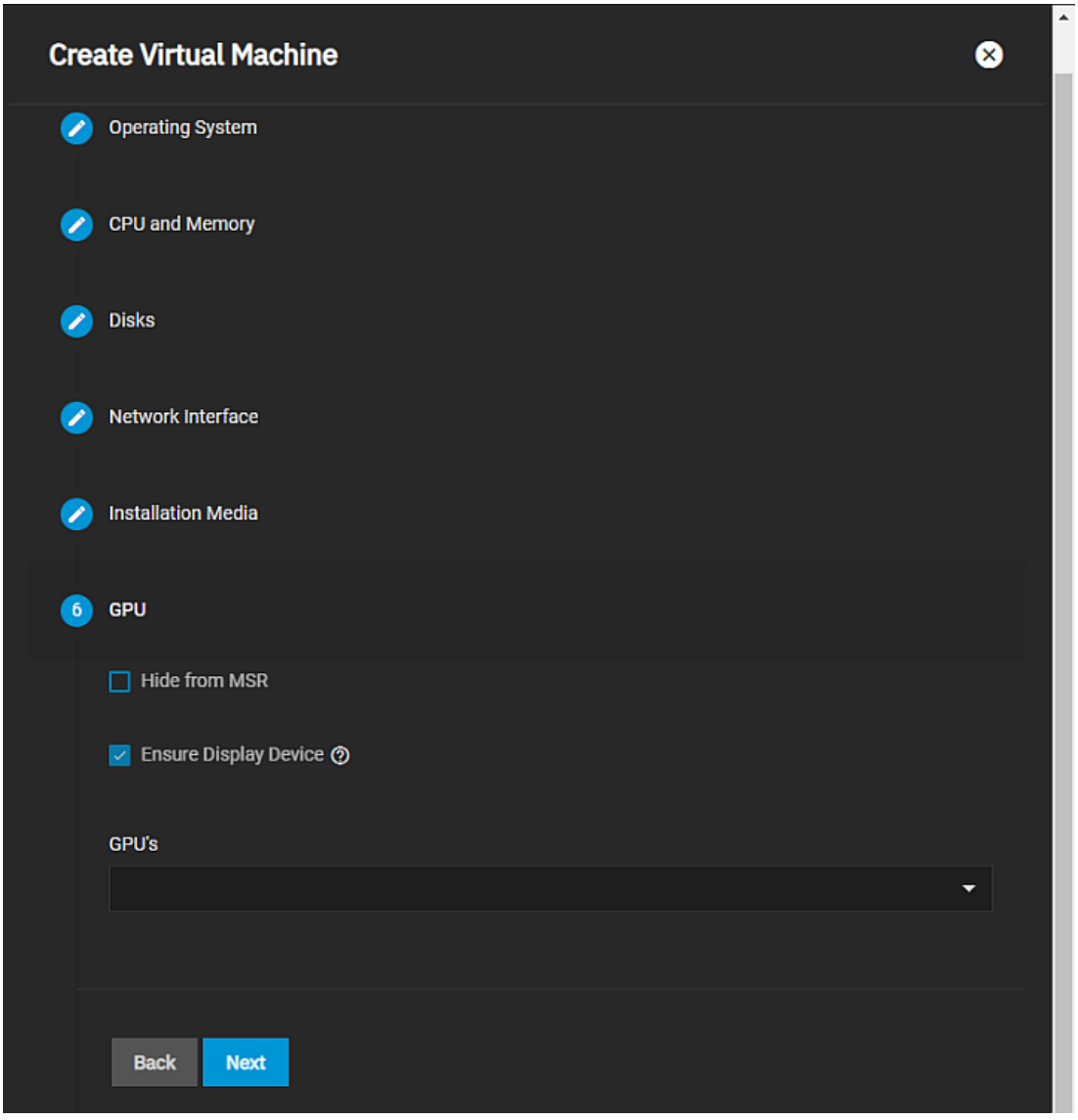


Field	Description
Hide from MSR	Select to enable the VM to hide the GPU from the Microsoft Reserved Partition (MSR).
Ensure Display Device	Select to ensure that the guest always has access to a video device. Required for headless installations like ubuntu server for the guest to operate properly. Leave checkbox clear for cases where want to use a graphic processing unit (GPU) passthrough and do not want a display device added.
GPU's	Select a physical GPU on your system from the dropdown list to use for the VM.

Devices Screens

The **Virtual Machines > Devices** screen displays a list of VM devices configured on your system.

Click Here for More Information



change image

Add opens the [Virtual Machine > Devices > Add] configuration screen. Settings change based on the various device types.

Device Actions

The displays a list of options for each device listed on the **Devices** screen.

Edit *type* Device

Edit opens the **Edit *type* Device** screen where *type* is the device type selected. Settings displayed vary based on the type of device set when at device creation, and are the same as those displayed on the [Add Device] screen except for the **Device Type**

field that only displays on the Add Device screens.

Delete Device

Delete opens a dialog where you click **Delete Device** to confirm you want to delete the device.

Change Device Order

Change Device Order opens a dialog for the selected device. Enter the number that represents the order the VM looks to the device during boot-up. The lower the number places the device earlier in the boot process. Enter the number and click **Save**.

Details

Details displays an information dialog for the selected device that lists the port, type, bind IP and other details about the device. Click **Close** to close the dialog.

Devices Add Screens

Add on the **Devices** screen opens the **Add Device** configuration screen. Settings change base on the selection in **Device Type**.

Select **CD-ROM** to configure a new CD-ROM location and the boot order for that device.

Select **NIC** to configure a new network adapter and the boot order for that device.

Select **Disk** to configure a new disk location, drive type and sector size, and the boot order for that device.

Select **Raw File** to configure a new file location and file size, the disk sector and mode, and the boot order for that device.

Select **PCI Passthru Device** to select a PCI Passthru device from the dropdown list and the boot order for that device.

Select **Display** to configure a new display device and the boot order for that device.

Add Device Type CD-ROM

Select **CD-ROM** in the **Add** device screen **Device Type** to configure the device setings and boot order.

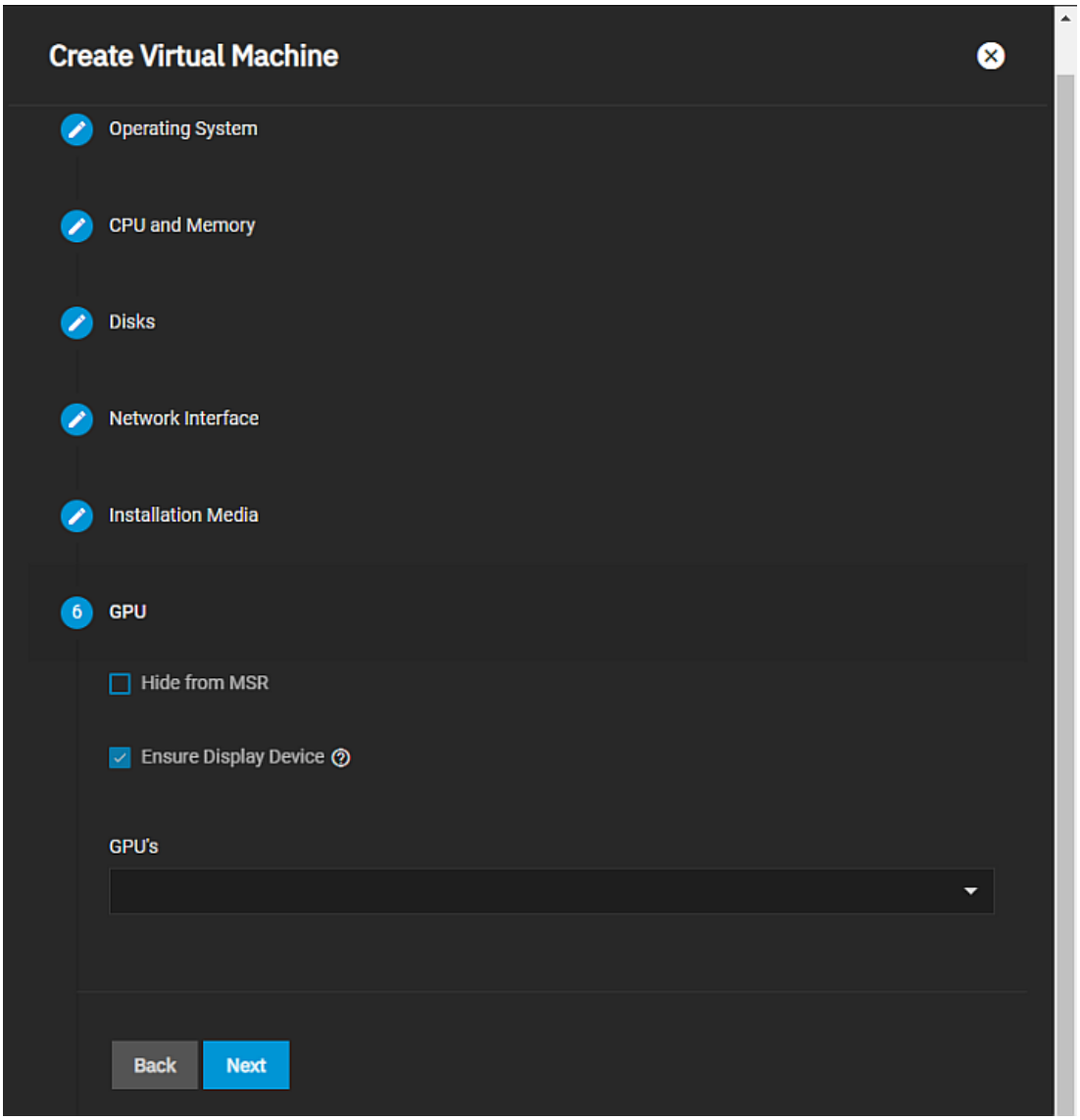
Click Here for More Information

Field	Description
Type	Select the device type from the dropdown list. **CD-ROM** is the default setting.
CD-ROM Path	Use the to the left of **/mnt** to browse to the location of the CD-ROM file on the system.
Device Order	Enter the number (such as *1003*) that represents where in the boot order this device should be. The higher the number the later in the boot-up process the device falls. If you want the CD-ROM to be the first device checked assign it a lower number.

Add Device Type NIC

Select **NIC** in the **Add** device screen **Device Type** to configure network interface card settings and boot order.

Click Here for More Information

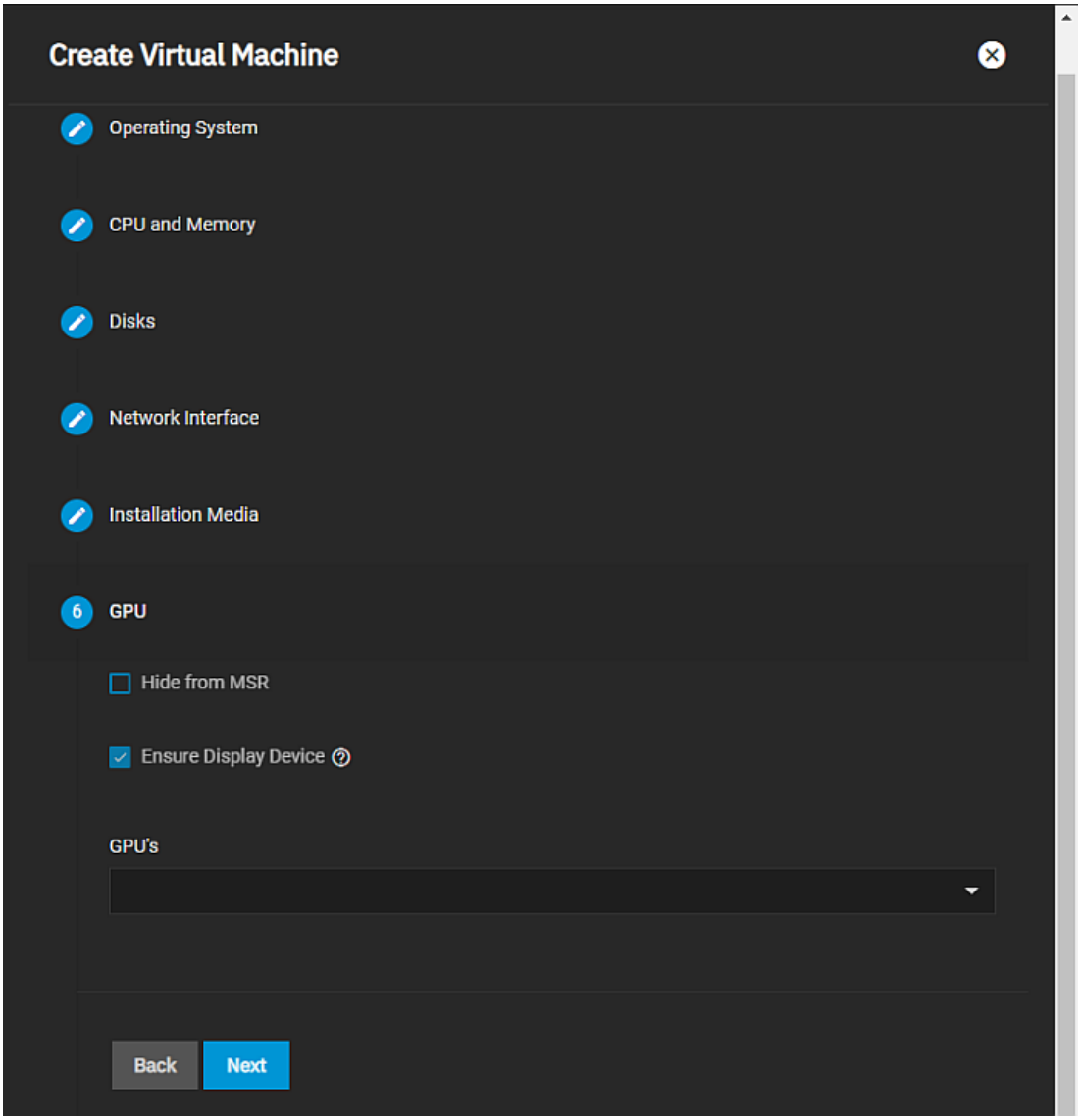


Field	Description
Type	Select the device type from the dropdown list.
Adapter Type	Required. Select the emulator type from the dropdown list. Emulating an **Intel e82545 (e1000)** Ethernet card provides compatibility with most operating systems. Change to **VirtIO** to provide better performance on systems with VirtIO paravirtualized network driver support.
MAC Address	Displays the default auto-generated random MAC address the VM receives. Enter a custom address to override the default.
NIC to attach	Select a physical interface from the dropdown list to assoicate with the VM.
Device Order	Enter the number (such as *1003*) that represents where in the boot order this device should be. The higher the number the later in the boot-up process the device falls. If you want the CD-ROM to be the first device checked assign it a lower number.
Generate MAC Address	Click to add a new randomized address in **MAC Address**.

Add Device Type Disk

Select **Disk** in the **Add** device screen **Device Type** to configure a new disk location, drive type and disk sector size and boot order.

Click Here for More Information

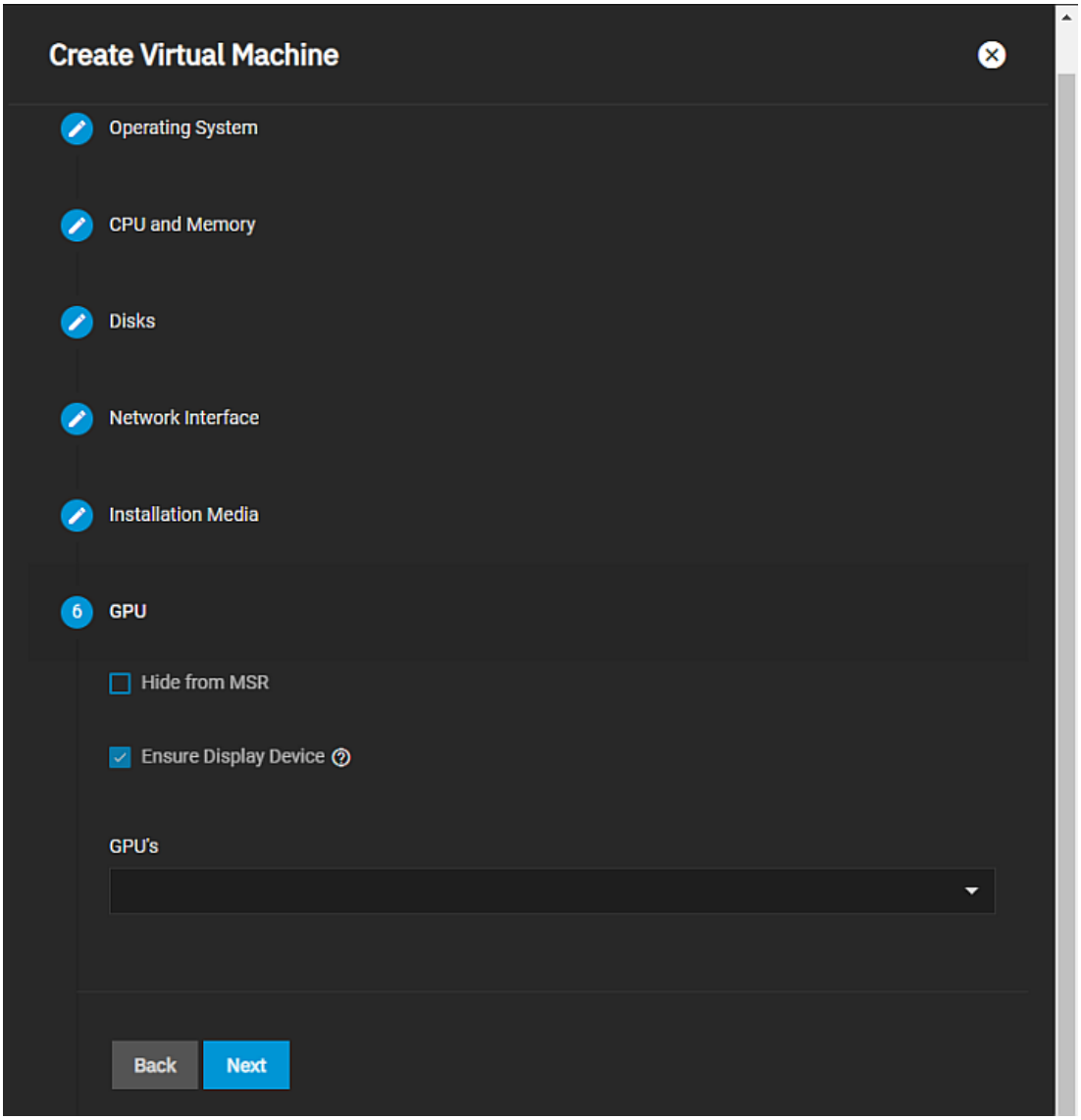


Field	Description
Type	Select the device type from the dropdown list.
Zvol	Select the zvol path from the dropdown list.
Mode	Select the drive type from the dropdown list. Options are **AHCI** or **VirtIO**.
Disk sector size	Select the disk sector size from the dropdown list or leave set as **Default**. Options are **Default**, **512** or **4096**.
Device Order	Enter the number (such as *1003*) that represents where in the boot order this device should be. The higher the number the later in the boot-up process the device falls. If you want the CD-ROM to be the first device checked assign it a lower number.

Add Device Type Raw File

Select **Raw File** in the **Add** device screen **Device Type** to configure the location and size of the file, disk sector size and type, and boot order.

Click Here for More Information

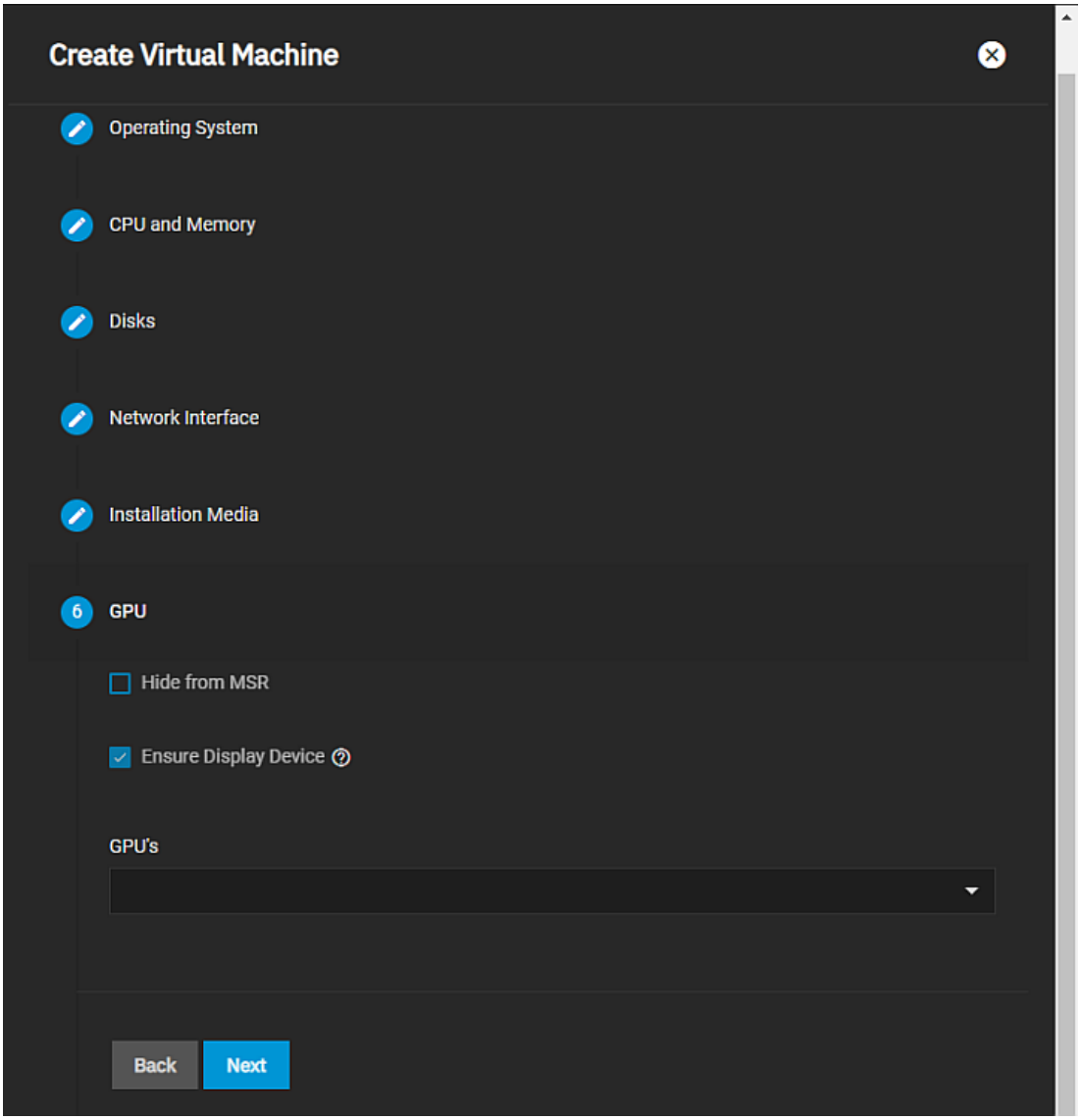


Field	Description
Type	Select the device type from the dropdown list.
Raw File	Enter or use the to the left of **/mnt** to browse to the location of the file on the system.
Disk sector size	Select the disk sector size from the dropdown list or leave set as **Default**. Options are **Default**, **512** or **4096**.
Mode	Select the drive type from the dropdown list. Options are **AHCI** or **VirtIO**.
Device Order	Enter the number (such as *1003*) that represents where in the boot order this device should be. The higher the number the later in the boot-up process the device falls. If you want the CD-ROM to be the first device checked assign it a lower number.
Raw filesize	Enter the size of the file in GiB.

Add Device Type PCI Passthru Device

Select **PCI Passthru Device** in the **Add** device screen **Device Type** to configure the PCI passthru device and boot order.

Click Here for More Information

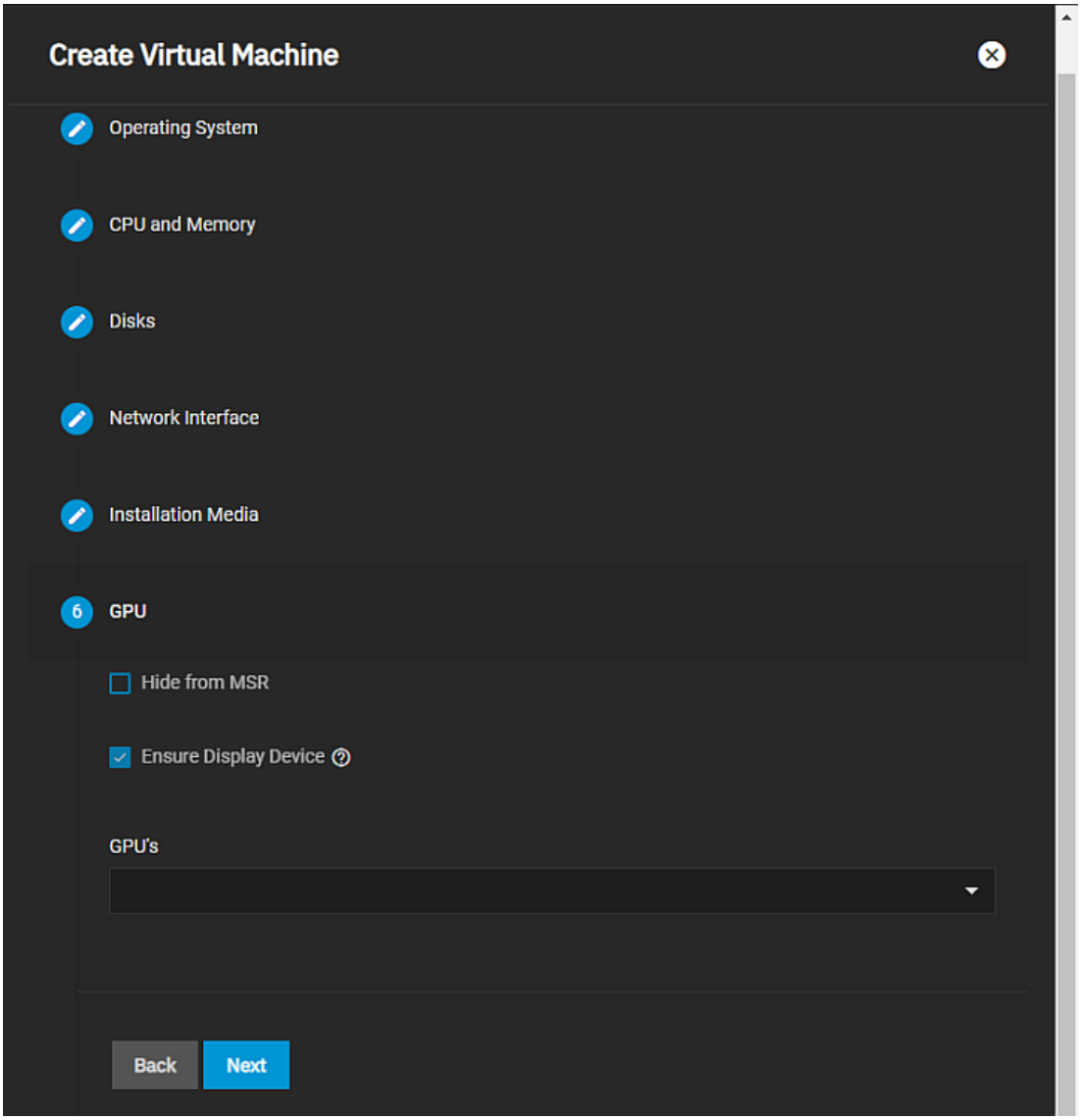


Field	Description
Type	Select the device type from the dropdown list.
PCI Passthru Device	Enter or select the device from the dropdown list of options. Enter as (bus#/slot#/fcn#).
Device Order	Enter the number (such as *1003*) that represents where in the boot order this device should be. The higher the number the later in the boot-up process the device falls. If you want the CD-ROM to be the first device checked assign it a lower number.

Add Device Type Display

Select **NIC** in the **Add** device screen **Device Type** to configure a new display device and boot order.

Click Here for More Information



Field	Description
Type	Select the device type from the dropdown list. **Display** is the default setting.
Port	Enter the port number. You can assign **0**, leave empty for TrueNAS to assign a port when the VM is started, or set to a fixed preferred port number.
Resolution	Select a screen resolution to use for VNC sessions.
Bind	Select an IP address to use for VNC sessions or use the default **0.0.0.0**.
Password	Enter a VNC password of no more than eight characters in length to automatically pass to the VNC session.
Display Type	Select the display type from the dropdown list. Options are **VNC** or **SPICE**.
Web Interface	Select to enable connecting to the VNC web interface.
Device Order	Enter the number (such as *1003*) that represents where in the boot order this device should be. The higher the number the later in the boot-up process the device falls. If you want the CD-ROM to be the first device checked assign it a lower number.

Related Content

- Adding and Managing VMs
- Installing SCALE
- Accessing NAS From a VM

Related GPU Articles

- Adding and Managing VMs

- Advanced Settings Screen
- Managing GPUs

4.9 - Apps Screens

Article Summaries

- Applications Screens

  This article provide information on application screens and settings in SCALE.

- Launch Docker Image Screens

  This article provides information on the **Launch Docker Image** wizard configuration screens and settings.

4.9.1 - Applications Screens

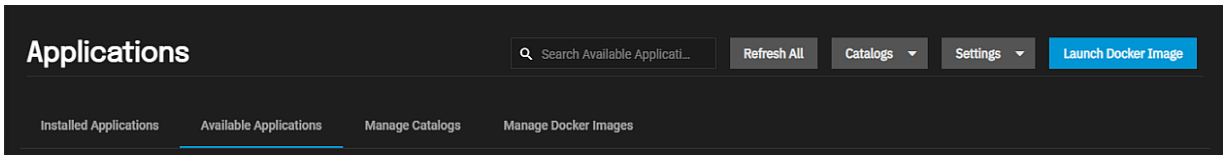
This article provide information on application screens and settings in SCALE.

The application screen displays with **Installed Applications** displayed by default.

The first time time you select **Apps** on the main feature navigation panel, the **Applications** screen displays the **Choose a pool for Apps** dialog. Select a pool from the dropdown list and then click **Choose** to set the selected pool as the one applications use for data storage.

Applications Screen Options

The options at the top right of the **Applications** screen change with the screen tab selected.



Bulk Actions

The **Bulk Action** option that displays at the top right of the **Installed Applications** screen allows you to select more than one, or all installed apps on your system. After selecting the apps, use the other action buttons to either **Start**, **stop** or **Delete** the selected apps.

Select All places a checkmark in the top left corner of the widget for each installed application. Toggles to **Unselect All**. **Start** starts all selected apps, and displays s **Success** dialog for each app after it starts without issue. **Stop** stops all selected apps and displays a **Success** dialog for each app after it stops without issue.

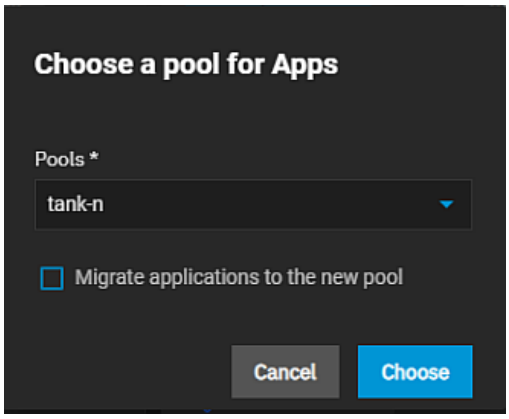
Settings

Settings displays at the top right of all four **Applications** screens, but they are only functional when on the **Available Applications** screen. Setting options are:

Choose Pool opens the **Choose a pool** window. **Advanced Settings** opens the **Kubernetes Settings** configuration screen. **Unset Pool** opens a dialog confirming the pool is unset.

Choose Pool Window

Selecting **Choose Pool** on the **Settings** list opens a different **Choose a pool for Apps** window than the one that first displays before you add your first application. Use the **Settings > Choose Pool** option to change the pool applications use for storage.

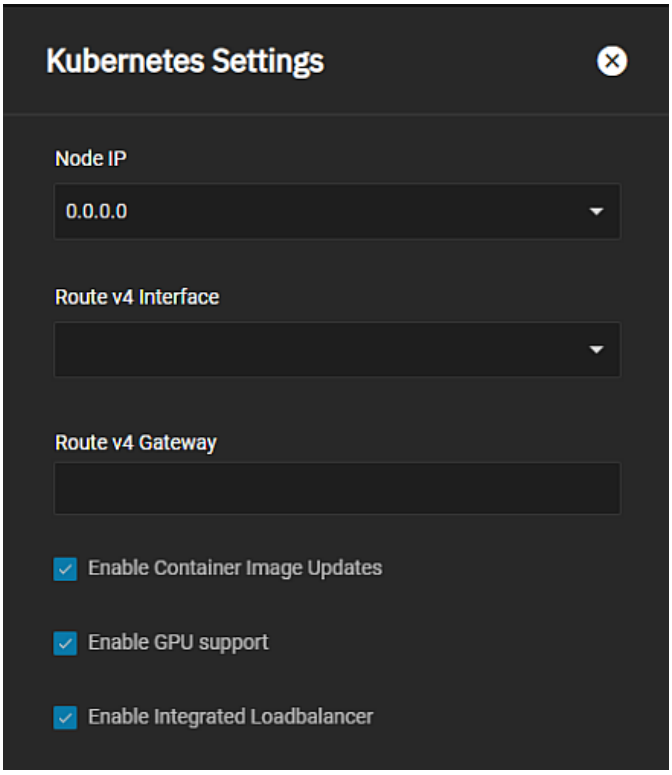


Migrate applications to the new pool starts the process of moving your application data from the existing pool to the new pool specified after you click **Choose**. Select **Migrate applications to the new pool** if you change your applications pool and want to migrate data from the existing pool to the new pool.

Kubernetes Settings Screen

The **Advanced Settings** option opens the **Kubernetes Settings** configuration screen.

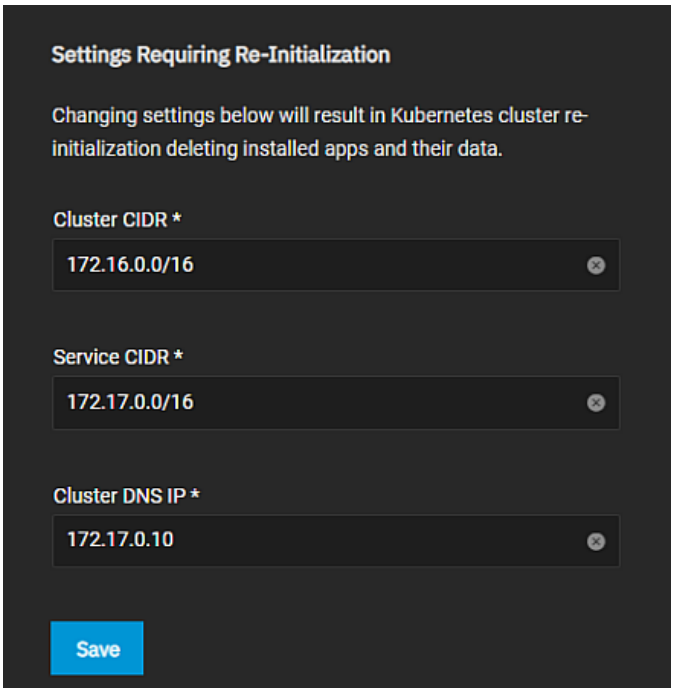
Click Here for More Information



Setting	Description
Node IP	Select the IP address for the node from the dropdown list.
Route v4 Interface	Select the network interface from the dropdown list.
Route v4 Gateway	Enter the IP address for the route v4 gateway.
Enable Container Image Updates	Select to enable updates of the container image.
Enable GPU support	Select to enable GPU support.
Enable Integrated	Select to enable the integrated loadbalancer. The default uses servicelb but if disabled, allows

Setting	Description
Loadbalancer	using metallb and allows users to speicfy any IP from the local network.

Settings Requiring Re-Initializtion



Setting	Description
Cluster CIDR	Required. Enter the IP address and CIDR number for the Kubernetes cluster.
Service CIDR	Required. Enter the IP address and CIDR number for the Kubernetes service.
Cluster DNS IP	Required. Enter the IP address for the cluster DNS.

Unset Pool

The **Unset Pool** option on the **Settings** list displays a confirmation dialog. Click **UNSET** to unset the pool. When complete a **Success** dialog displays.

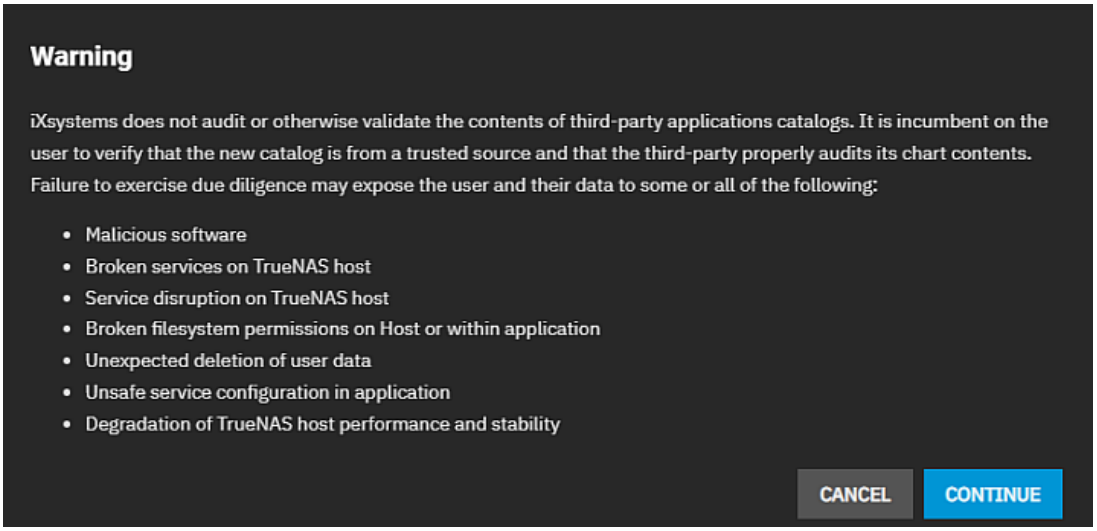
Refresh All

Opens a **Refreshing** counter with status of the refresh options. When complete, the **Task Manager** displays with the status of each app refresh operation.

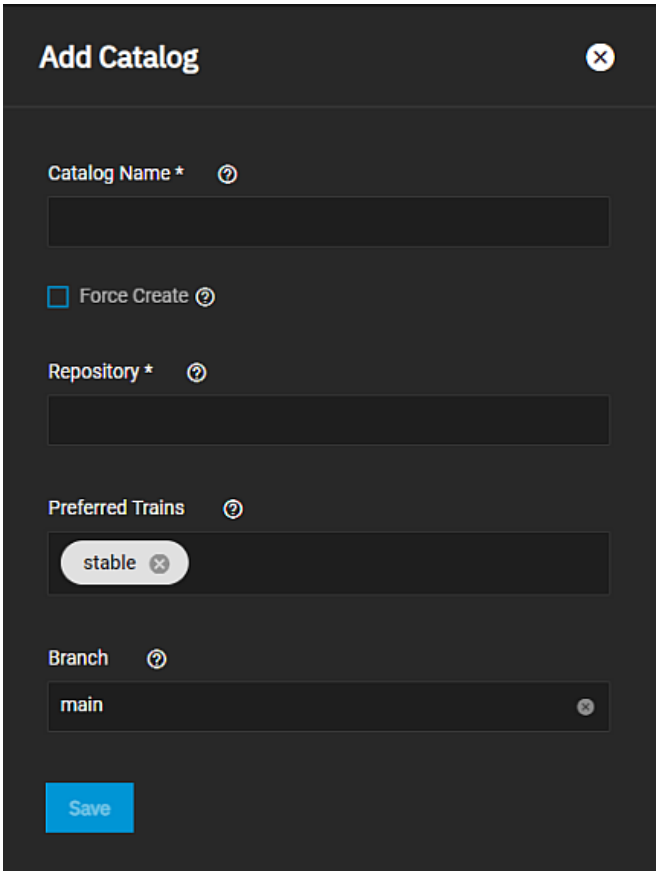
Add Catalog

Add Catalog at the top of the **Manage Catalogs** screen opens a warning dialog before it opens the **Add Catalog** screen.

Click Here for More Information



Click **CONTINUE** to open the **Add Catalog** screen.

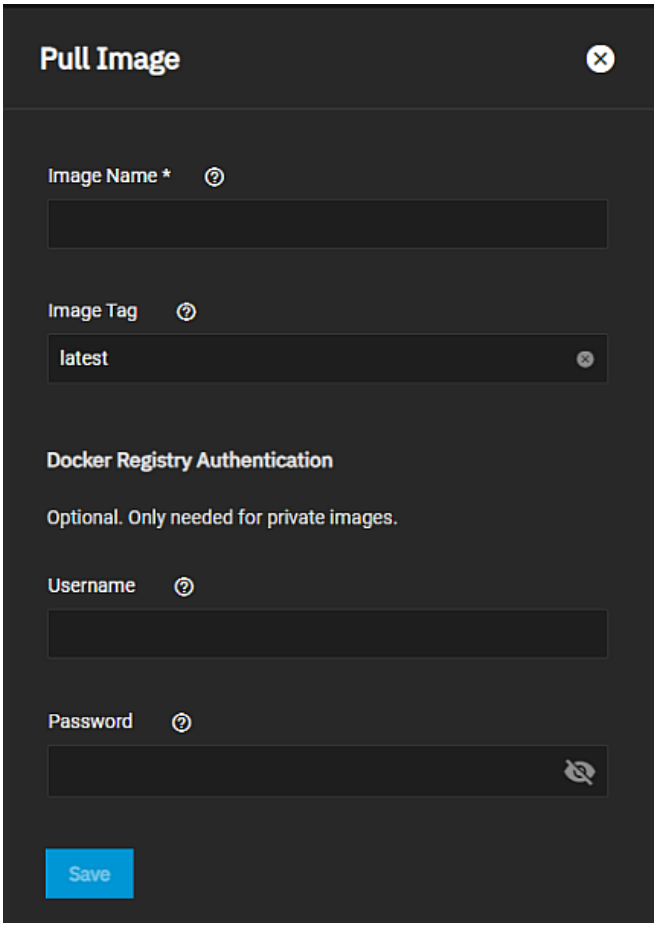


Field	Description
Catalog Name	enter the name the TrueNAS uses to look up the catalog. For example, *truecharts*.
Force Create	Select to add the catalog to the system even if some trains are unhealthy.
Repository	Enter the valid git repository URL. For example, *https://github.com/truecharts/catalog*.
Preferred Trains	The trains TrueNAS uses to retrieve available applications for the catalog. Default is **stable** (and optionally: **incubator**).
Branch	Specify the git repository branch TrueNAS should use for the catalog. Default is **main**.

Pull Image

The **Pull Image** option at the top right of the **Manage Docker Images** screen opens the **Pull Image** screen.

Click Here for More Information



Setting	Description
Image Name	Enter the name of the image to pull. Format for the name is `registry/repo/image`.
Image Tag	Enter the tag of the image. For example, *latest*.

Docker Registry Authentication Settings

These settings are optional, and only needed for private images.

Setting	Description
Username	Enter the input user name.
Password	Enter the input user password.

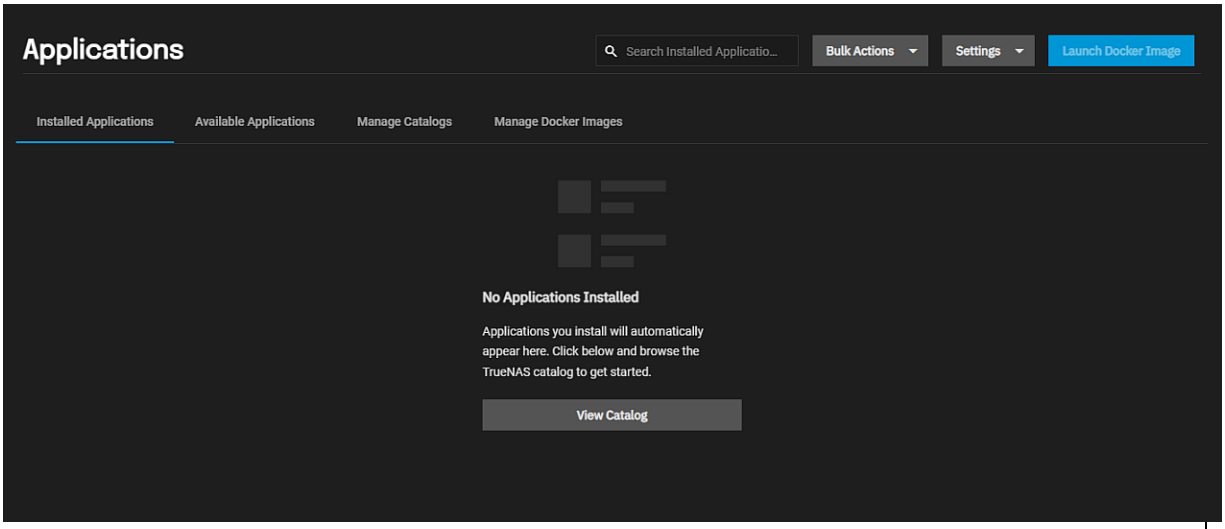
Launch Docker Image

Launch Docker Image opens the Docker Image wizard where you can configure third-party applications not listed on the **Available Applications** screen. These docker image options are derived from the Kubernetes container options. See Launch Docker Image Screens for more information.

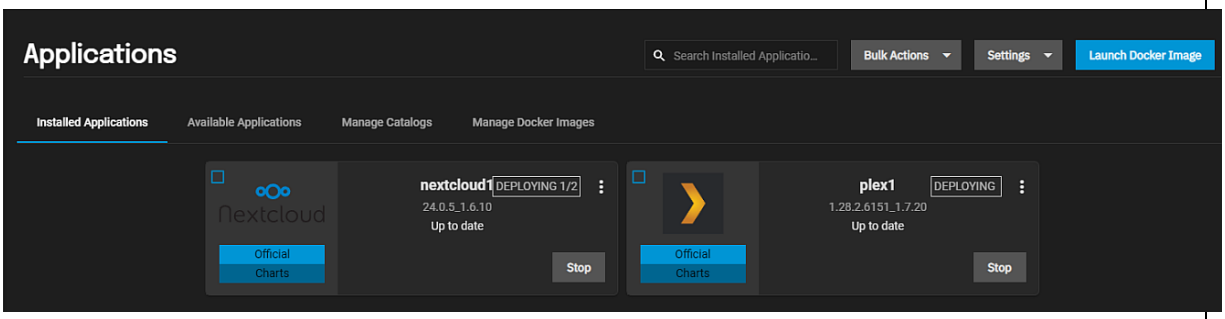
Installed Applications Screen

The **No Applications Installed** screen displays before you install your first application. **View Catalog** opens the **Available Applications** screen.

Click Here for More Information



After installing your application(s), this screen displays the application(s).



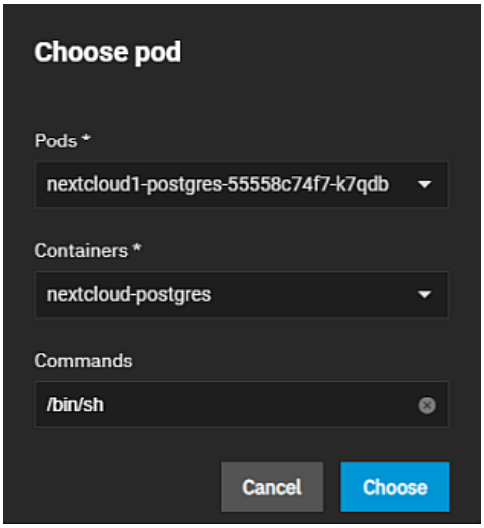
Click the ✎ on the application widget to open the action options dropdown list. Options are:

- **Edit** opens the configuration form for the selected application.
- **Shell** opens the **Choose pod** window before opening the **Applications > Pod Shell** screen.
- **Logs** opens the **Choose Log** window before opening the **Applications > Pod Log** screen.
- **Delete** opens a confirmation dialog.

Choose Pod Window

The **Choose Pod** window specifies which pod or active container, and the shell commands you want to use when the **Applications > Pod Shell** screen displays.

Click Here for More Information ↕



Setting	Description
Pods	Required. Select the pod installed from the dropdown list.

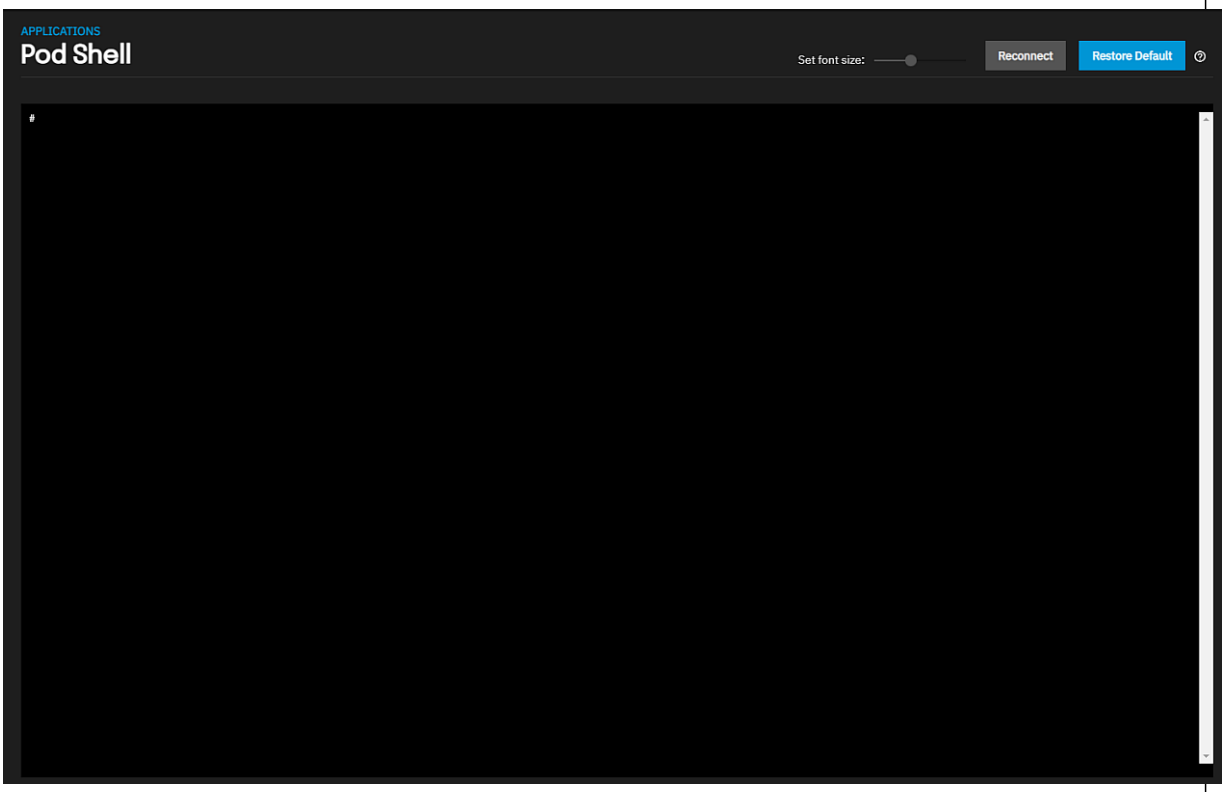
Setting	Description
Containers	Required. Select the container from the dropdown list.
Commands	Enter the shell command.

Select **Choose** to open the **Applications > Pod Shell** screen.

Pod Shell Screen

The **Pod Shell** screen allows users to enter TrueNAS CLI commands to access information about their applications.

Click Here for More Information



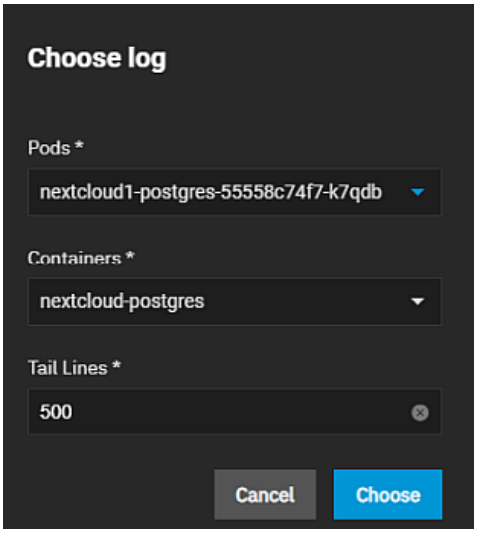
The following are examples of commands you can enter to access information on an active container. You can also use the **System Settings > Shell** to access the same information.

To view container namespaces: `k3s kubectl get namespaces`. To view pods by namespace: `k3s kubectl get -n <NAMESPACE> pods`. To access container shell: `k3s kubectl exec -n <NAMESPACE> --stdin --tty <POD> -- /bin/bash`. To view details about all containers: `k3s kubectl get pods,svc,daemonsets,deployments,statefulset,sc,pvc,ns,job --all-namespaces -o wide`. To get container status: `k3s kubectl describe -n <CONTAINER NAMESPACE> <POD-ID>`.

Choose Log Window

The **Logs** options opens the **Choose Log** window.

Click Here for More Information

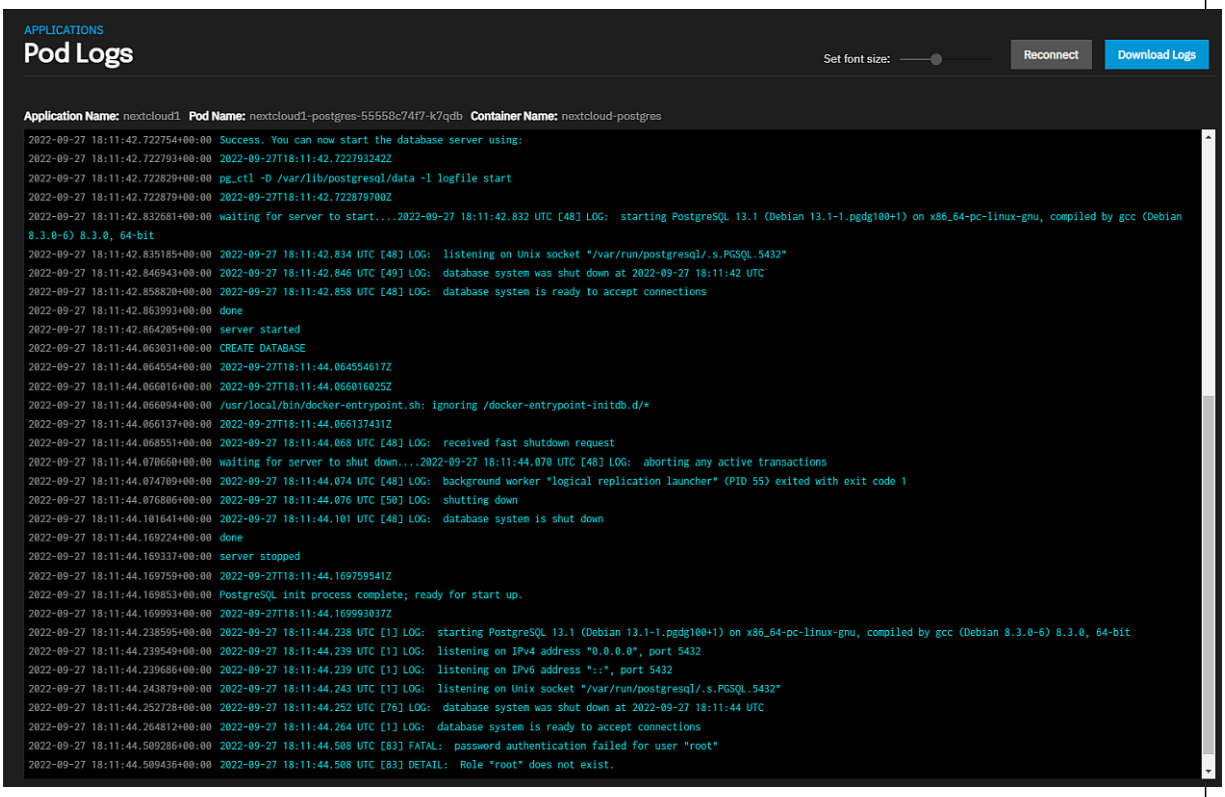


Setting	Description
Pods	Select the pod from the dropdown list to open the shell screen with the log for this pod.
Containers	Select the containers from the dropdown list to include in the log shell screen.
Tail Lines	Enter the number of log file lines to include in the shell screen for the log file.

Pod Log Window

The **Pod Log** shell screen displays with the information selected in the **Choose Log** window.

Click Here for More Information

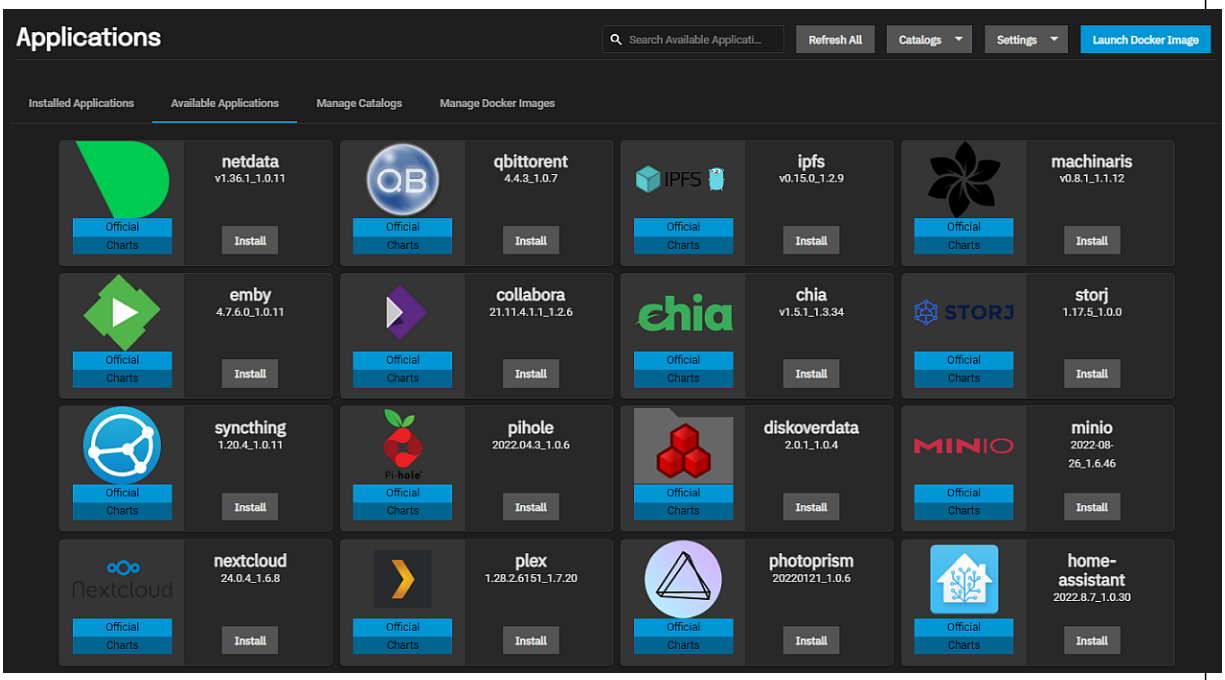


Use the **Set font size** slider to increase or decrease the size of the font displayed on the screen. **Reconnect** re-establishes a connection with the application service. **Download Logs** downloads the logs to your server.

Available Applications

The **Available Applications** screen displays the widgets for all applications in the **Official** catalog.

Click Here for More Information



The **Install** button on each application card opens the configuration wizard for that application.

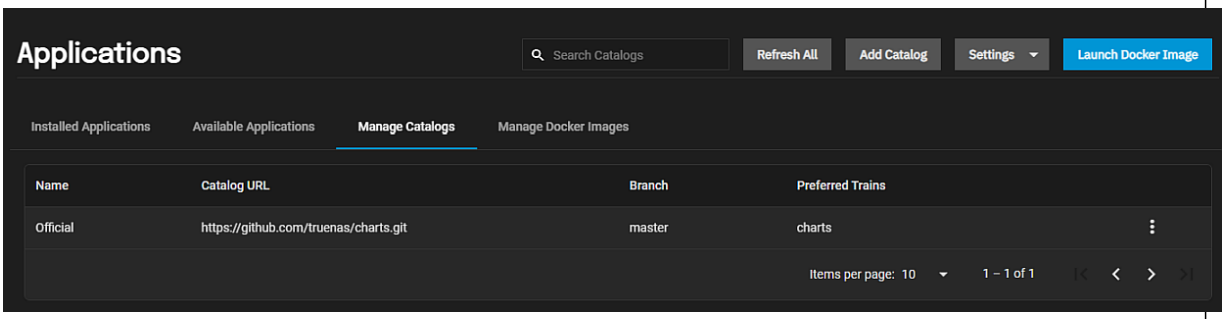
Click on the application icon or name to open an ***appname* Application Summary** window that includes information on the **Catalog**, **Categories**, **Train**, **Status** and **Versions** for that application.

Manage Catalogs

The **Manage Catalog** screen displays the list of application catalogs installed on TrueNAS SCALE. The **Official** catalog contains all the applications listed on the **Available Applications** screen.

Click Here for More Information

The options at the top right of the screen include the **Refresh All** and **Add Catalog** options.



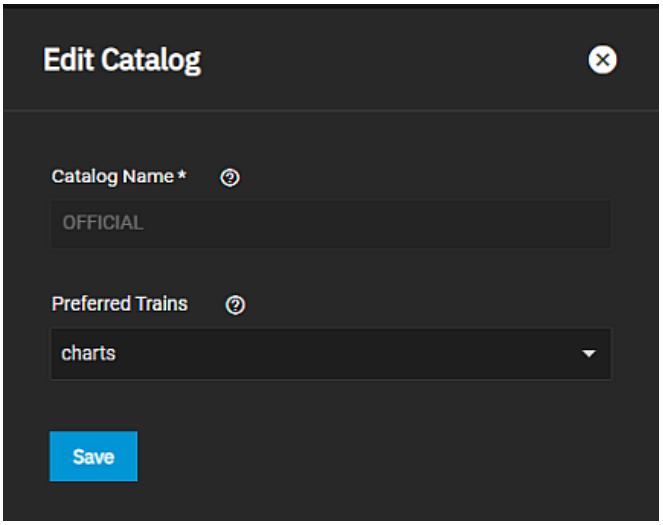
The ⋮ to the right of each catalog displays the catalog options **Edit**, **Refresh**, **Delete** or **Summary**.

Edit Catalog Screen

The **Edit Catalog** screen settings specify the name and train the UI should use to look up the catalog and retrieve applications for the catalog.

Click Here for More Information

The **Official** catalog name is not editable, but you can change the train.



Setting	Description
Catalog Name	Enter a name TrueNAS should use to look up the catalog.
Preferred Train	Select the train(s) the UI should use to retrieve available applications for the catalog from the dropdown list. Options are **charts**, **test**, **enterprise**, and **community**.

Refresh Catalog

Opens a **Refreshing** counter that shows the status of the refresh operation. You can minimze the counter while the process continues.

Delete Catalog

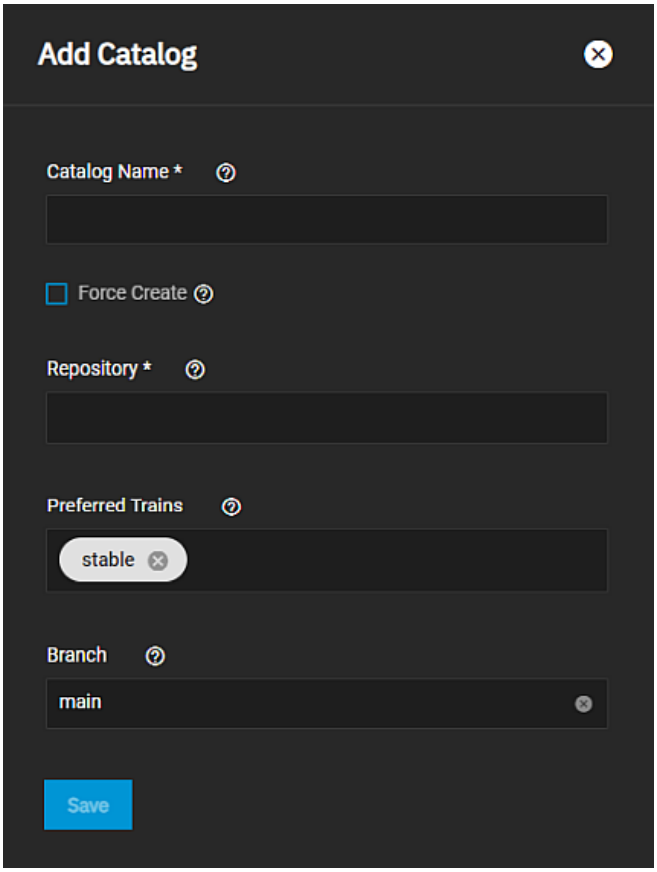
Opens a confirmation dialog before deleting the catalog. The **Official** catalog **Delete** option is inactive. You cannot delete the official catalog.

Catalog Summary Window

The **Summary** option for each catalog listed on **Manage Catalogs** opens the ***Name* Catalog Summary** window where *Name* is the name of the catalog. The summary displays the catalog status, application and train, and allows you to select the train and status you want to include in the summary.

Click Here for More Information

Add Catalog opens the **Add Catalog** screen.

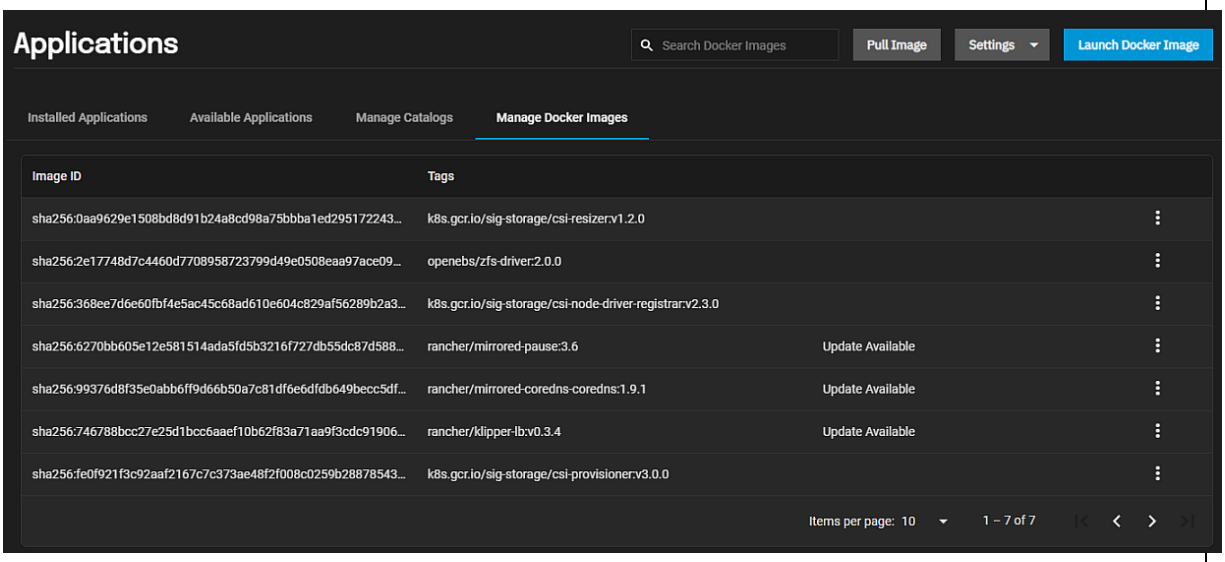


Setting	Description
Train	Select the trains you want to include in the catalog summary information. Options are **All**, **charts**, **test**, **enterprise** or **community**.
Status	Select the statuses you want to include in the catalog summary information. Options are **All**, **Healthy**, or **Unhealthy**. This is useful to filter the summary to locate trains or applications with the **Unhealthy** status.

Manage Docker Images

The **Manage Docker Images** displays a list of Docker image IDs and tags on the system. The list displays **Update Available** for container images you can update.

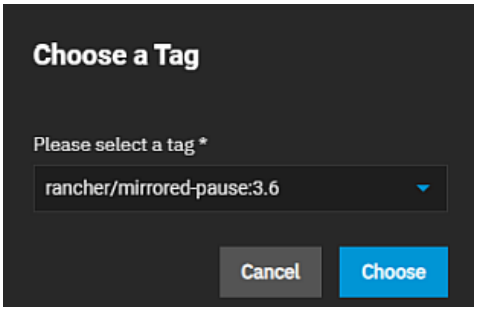
Click Here for More Information



Use the ⋮ to display the options for each Docker image listed. Options are **Update Image** or **Delete**. **Update Image** is only available when the Docker image displays **Update Available**.

Update Image

Select **Update** to open the **Choose a tag** dialog. Select the image tag and click **Choose**.



After updating the Docker image, the option becomes inactive until a new update becomes available.

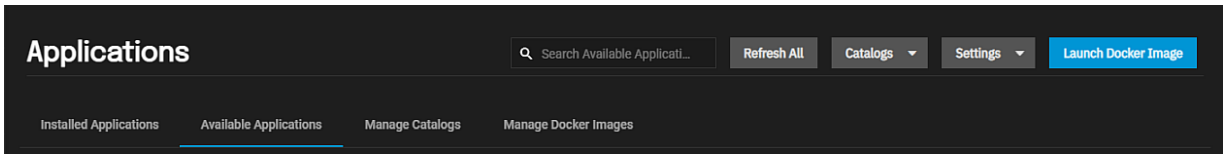
Related Content

- Updating MinIO from 1.6.58
- Using Apps
- Using SCALE Catalogs
- Launch Docker Image Screens
- Using Docker Image
- Adding NextCloud for Media Previews
- Configuring the Chia App
- Collabora App
- MinIO Clusters

4.9.2 - Launch Docker Image Screens

This article provides information on the **Launch Docker Image** wizard configuration screens and settings.

Launch Docker Image on the **Applications** screen opens a configuration wizard that steps through the application creation process using Docker image when selected while on the **Available Applications** tab.

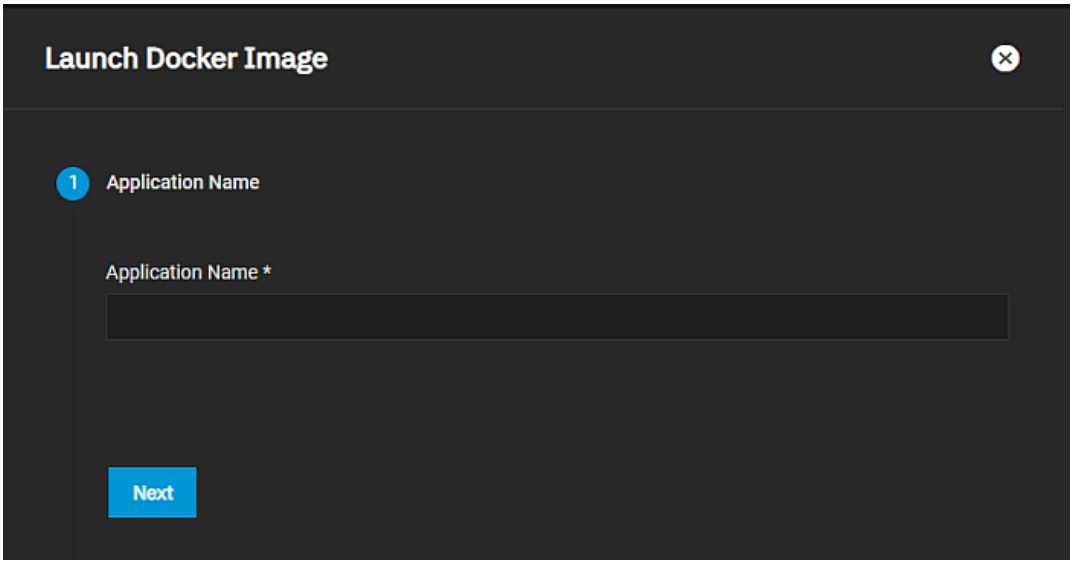


The docker image wizard includes 12 configuration screens and a **Confirm Options** screen that displays a summary of some of the setting options configured. The **Launch Docker Image** wizard allows you to configure third-party applications using settings based on Kubernetes. You can use the wizard to configure applications not included in the **Official** catalog or to do a more advanced installation of official catalog applications.

Application Name Screen

The **Application Name** screen is the first step in the **Launch Docker Image** configuration wizard.

Click Here for More Information



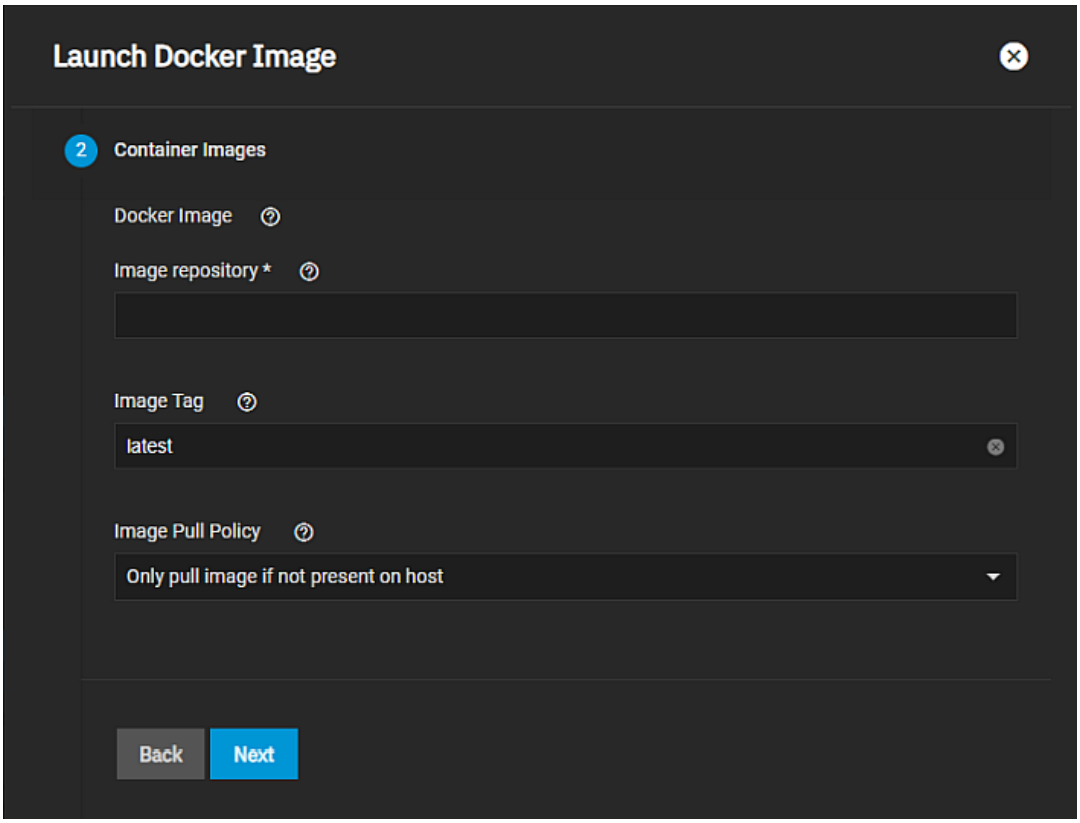
Setting	Description
Application Name	Enter a name for the application you are adding. The name must have lowercase alphanumeric characters, must begin with an alphabet character and can end with an alphanumeric character. The name can contain a hyphen (-) but not as the first or last character in the name. For example, using *chia-1* but not *-chia1* or *1chia-* as a valid name.

Container Images Screen

The **Container Images** settings specify the Docker image details. Always refer to the dockerhub page for information on what the docker container requires.

Click Here for More Information

Define the image tag, when the image is pulled from the remote repository, how the container is updated, and when a container automatically restarts with these settings.



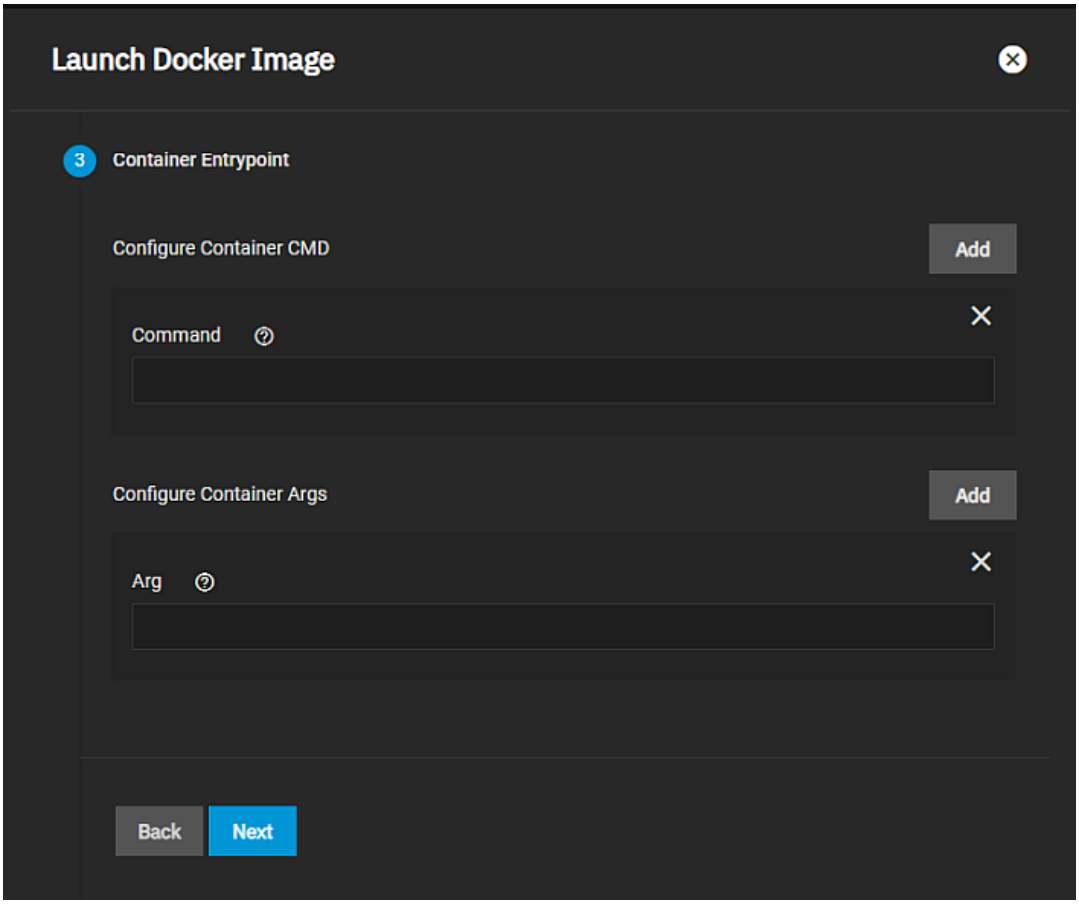
Setting	Description
Image Repository	Required. Enter the Docker image repository name. For example, for Plex enter *plexinc/pms-docker*.
Image Tag	Enter the tag for the specified image. For example, for Plex enter *1.20.2.3402-0fec14d92*.
Image Pull Policy	Select the Docker image pull policy from the dropdown list. Options are **Only pull image if not present on host**, **Always pull image even if present on host**, or **Never pull image even if it's not present on host**.

Container Entrypoint

The **Container Entrypoint** settings specify both commands and arguement options the application requires.

Click Here for More Information

Define any commands and arguments to use for the image. These can override any existing commands stored in the image. Check the documentation for the application you want to install using a Docker Image for entrypoint commands or arguments you need to enter.



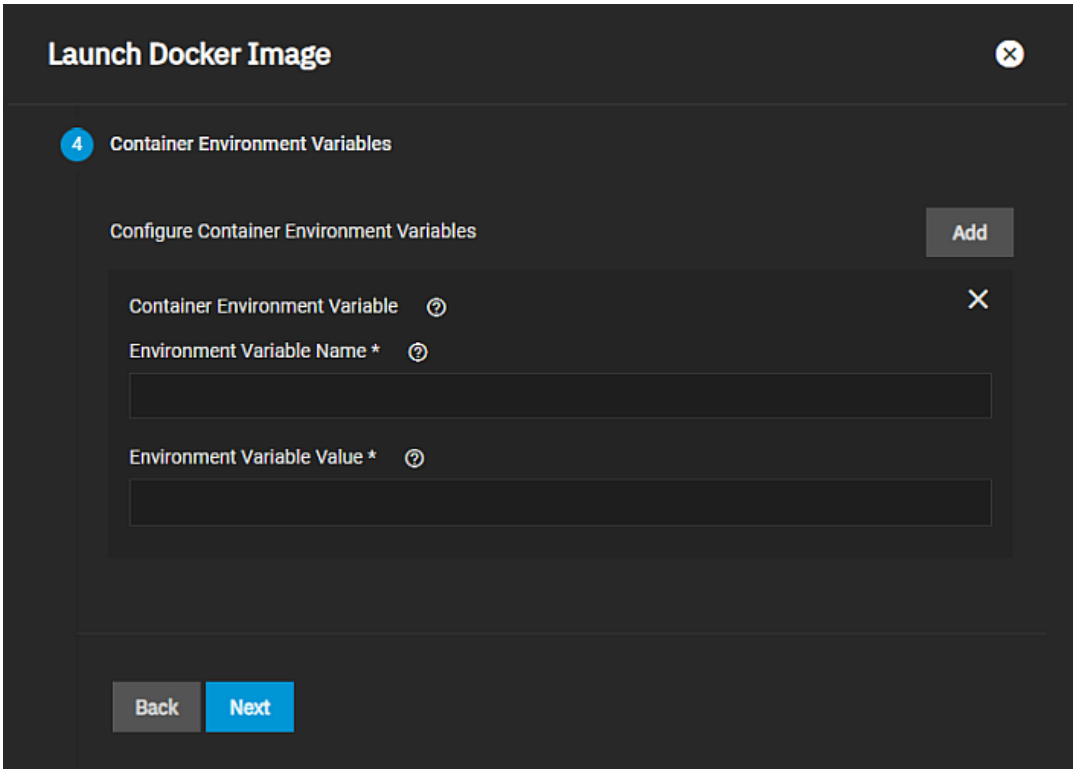
Setting	Description
Configure Container CMD	Click **Add** to display a **Command** field.
Command	Enter container command. For example, if adding MinIO, enter *SERVER*.
Configure Container Args	Click **Add** to display an argument entry **Arg** field. Click again to add more arguments.
Argument	Enter an argument. For example, if adding MinIO, enter the IP and port string such as *http://0.0.0.0/9000/data*.

Container Environment Variables

The **Container Environment Variables** settings specify container environment variables the container/image needs.

Click Here for More Information

You can also define additional environment variables for the container. Be sure to check the documentation for the image you are trying to deploy and add any required variables here.



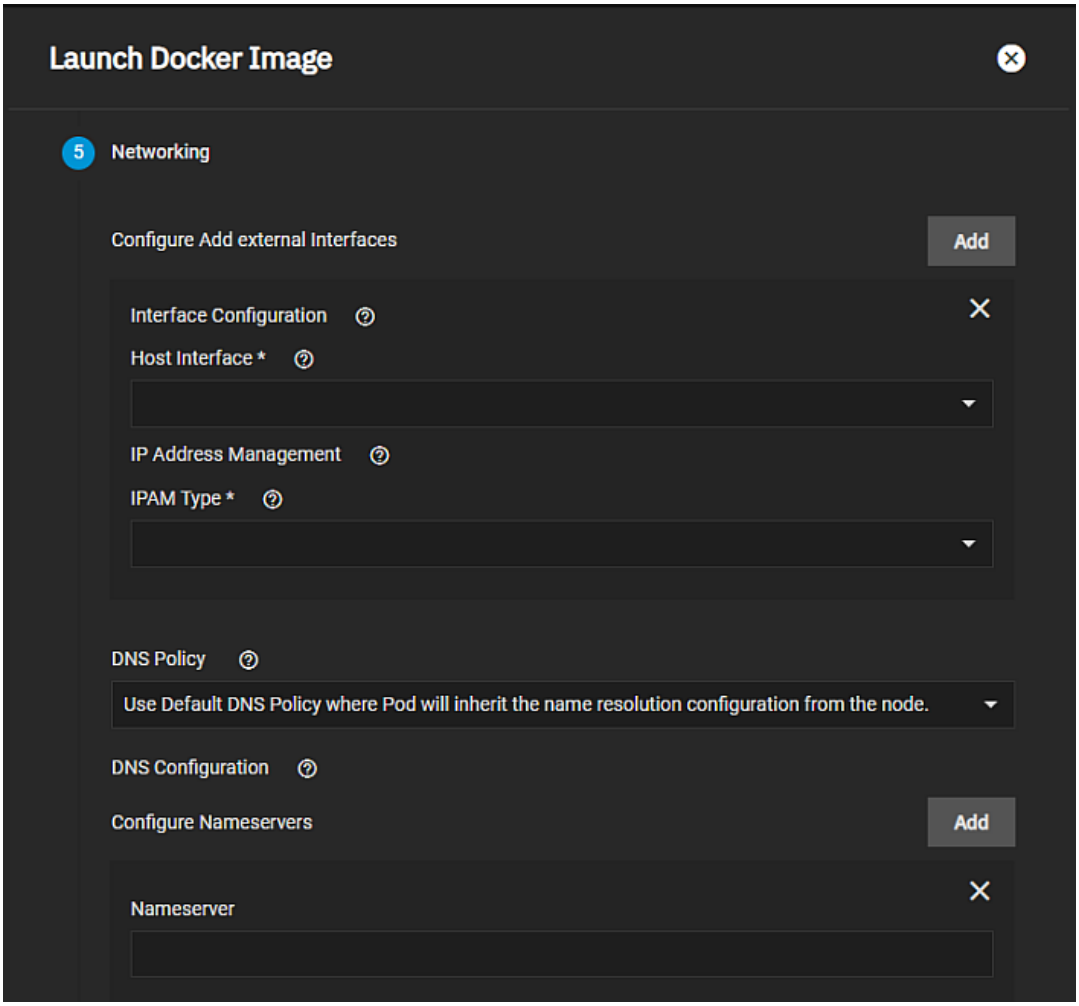
Setting	Description
Configure Container Environment Variables	Click **Add** to display a block of **Container Environment Variables**. Click again to add more blocks for environment variables.
Container Environment Variables	Container environmental variable name and value fields.
Environment Variable Name	Enter the environment variable name. For example, if installing Pi-Hole enter ***TZ** for timezone.
Environment Variable Value	Enter the value for the variable specified in **Environment Variable Name**. For example, for Pi-Hole timezone variable, enter *AmericaNewYork*.

Networking

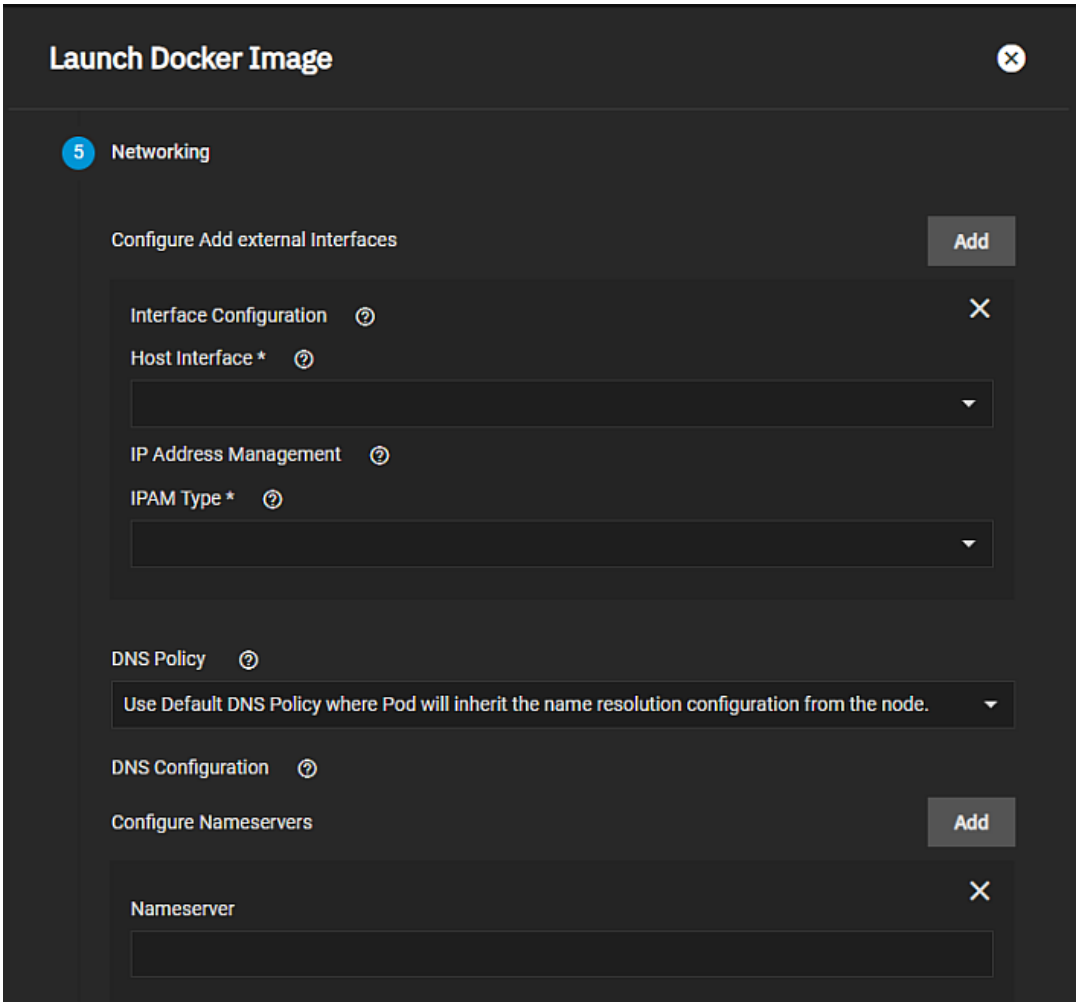
The **Networking** settings specify network policy, addresses, and DNS services if the container needs special networking configuration.

Click Here for More Information

See the Docker documentation for more details on host networking. Users can create additional network interfaces for the container if needed or give static IP addresses and routes to new interface. By default, containers use the DNS settings from the host system. You can change the DNS policy and define separate nameservers and search domains. See the Docker DNS services documentation for more details.



Setting	Description
Configure Add External Interfaces	Click **Add** to displays a block of interface settings.
Interface Configuration	Required. Select an interface from the **Host Interface** dropdown list.
Host Interface	Required. Select a host interface on your system from the dropdown list.
IP Address Management	Select an option for how to manage the IP address from the **IPAM Type** dropdown list.
IPAM Type	Required. Select an option from the dropdown list to specify the type for IPAM. Options are **Use DHCP** or **Use Static IP**. To add a default route, select **Add route** allow you to enter route destination IP /subnet 0.0.0.0/0. Enter the gateway (for example, *192.168.1.1*). After submitting the docker image, navigate to **Installed Applications**, locate the docker image you added, select **Edit** and change the route destination/subnet to equal 0.0.0.0 /0.
DNS Policy	Select the option from the dropdown list that specifies the policy. Default behavior is where Pod inherits the name resolution configuration from the node that the pods run on. If **None** is specified, it allows a pod to ignore DNS settings from the Kubernetes environment. Options are: **Use Default DNS Policy where Pod inherits the name resolution configuration from the node**. **Kubernetes internal DNS is prioritized and resolved first.** If the domain does not resolve with internal kubernetes DNS, the DNS query forwards to the upstream nameserver inherited from the node. This useful if the workload to access other services, workflows, using kubernetes internal DNS. **For Pods running with hostNetwork and wanting to prioritize internal kubernetes DNS should make use of this policy.** **Ignore DNS settings from the Kubernetes cluster**.
DNS Configuration	Specify custom DNS configuration to apply to the pod. Click **Add** to dsiplay a **Nameserver** entry field. Click again to add another name server.
Nameserver	Enter the IP address of the name server.



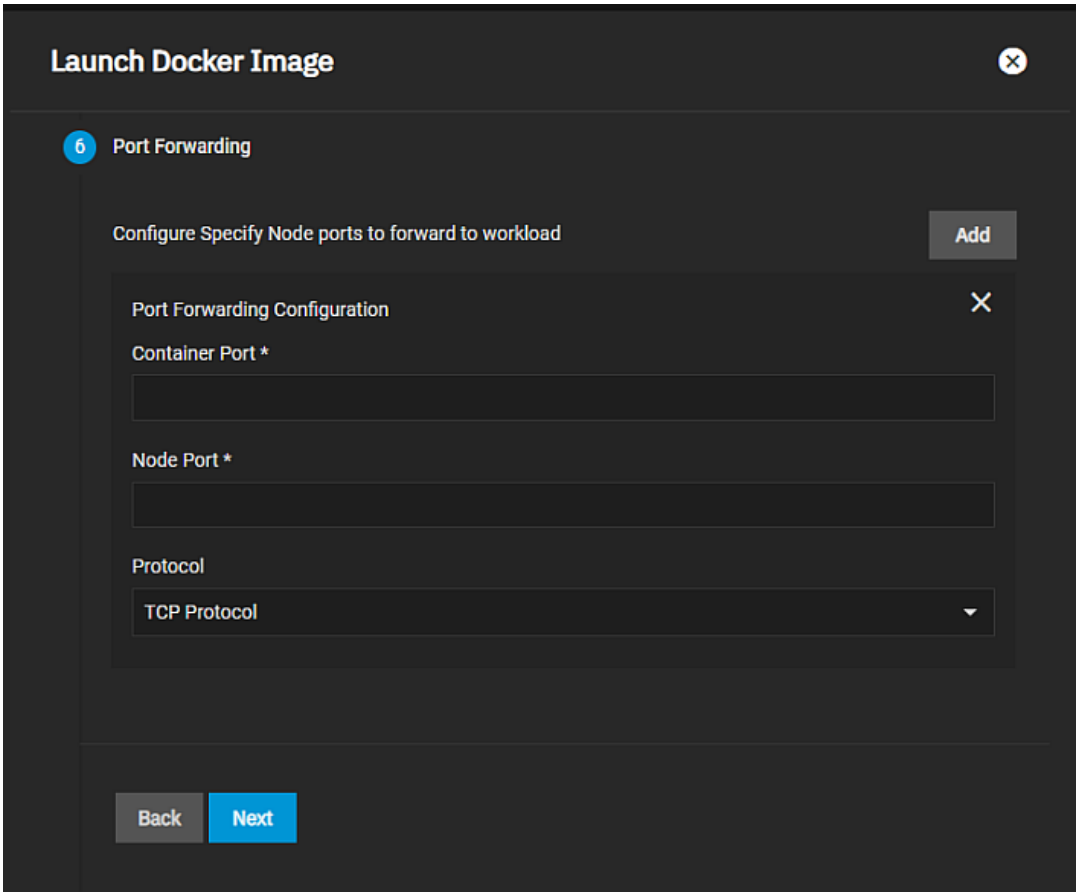
Setting	Description
Configure Searches	Click **Add** to display a **Search Entry** field.
Search Entry	Enter the search value you want to configure.
Configure DSN Options	Click **Add** to display a block of **Option Entry Configuration** settings. Click again to display another block of settings if needed.
Option Name	Required. Enter the option name.
Option Value	Required. Enter the value for the option name.
Provide access to node network namespace for the workload	Select to enable.

Port Forwarding

The **Port Forwarding** settings specify the container and node ports and the transfer protocol to use.

Click Here for More Information

Choose the protocol and enter port numbers for both the container and node. You can define multiple port forwards.



Setting	Description
Configure Specify Node ports to forward to workload	Click **Add** to display a block of **Port Forwarding Configuration** settings.
Container Port	Required. Do not enter the same port number used by another system service or container.
Node Port	Required. Enter a node port number over **9000**.
Protocol	Select the protocol to use from the dropdown list. Options are **TCP Protocol** or **UDP Protocol**.

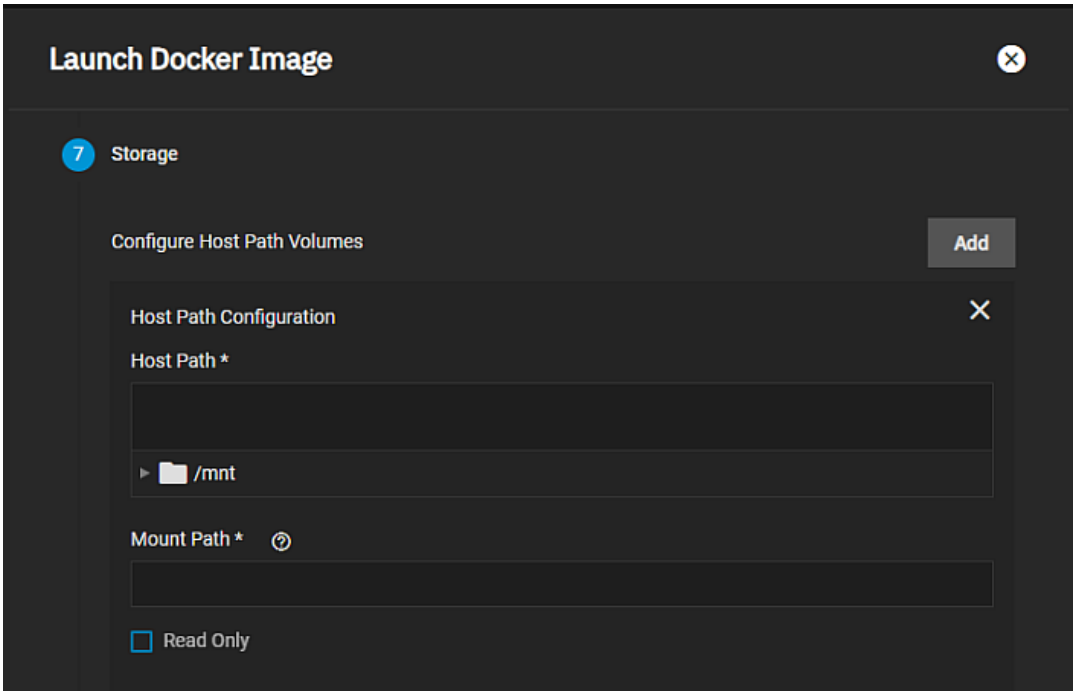
Storage

The **Storage** settings specify the host path configuration, memory backed volumes, and storage volumes.

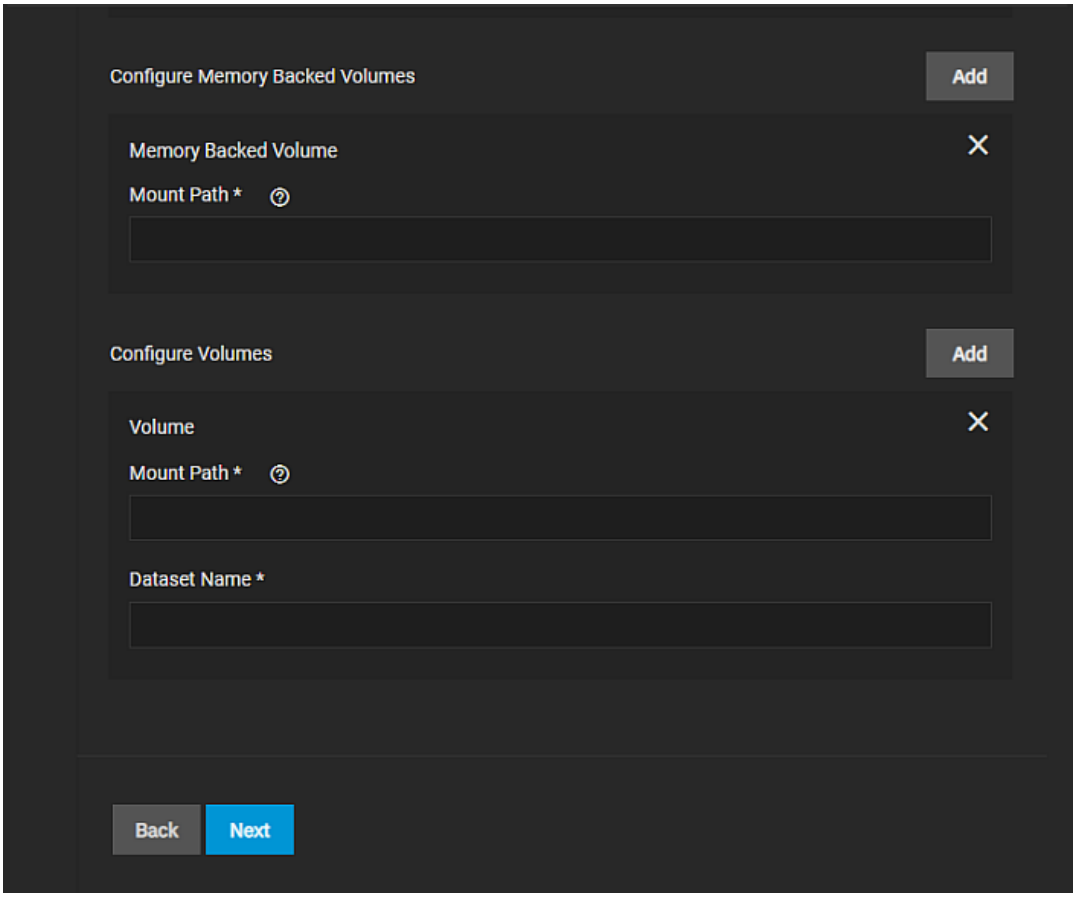
> Create the pool, dataset, zvol or directory for the container to use before you begin configuring the container as leaving the wizard closes it without saving.

Click Here for More Information

Set the Host Path volume to a dataset and directory path. Somme apps like Pi-Hole use volumes store data between container upgrades. For host path volumes, you can mount SCALE storage locations inside the container. Define the path to the system storage and the container internal path for the system storage location to appear. For more details, see the Kubernetes hostPath documentation. Users can create additional Persistent Volumes (PVs) for storage within the container. PVs consume space from the pool chosen for application management. To do this, name each new dataset and define a path where that dataset appears inside the container.



Setting	Description
Configure Host Path Volumes	Click **Add** to display a block of **Host Path Configuration** settings. Click again to add another block of settings.
Host Path	Require. Enter or click ▸ to the left of 🗀 **/mnt** to browse to the location of the host path. Click on the dataset to select and display it in the **Host Path** field.
Mount Path	Required. Enter the **/data** directory where host path mounts inside the pod.
Read Only	Select to make the mount path inside the pod read only and prevent using the container to store data.

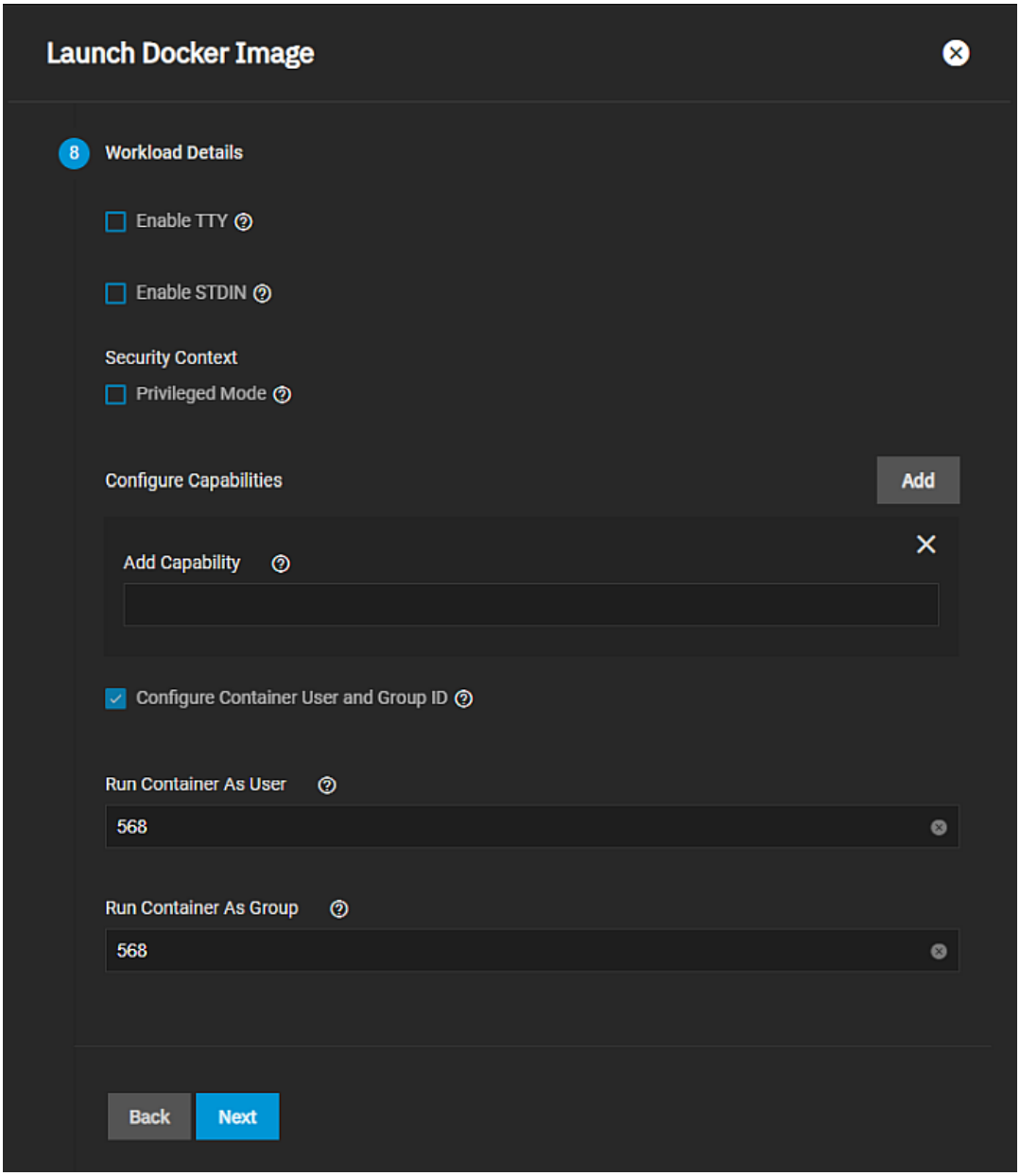


Setting	Description
Configure Memory Backed Volumes	Click **Add** to display a block of **memory Backed Volume** settings. Click again to display another block of settings.
Mount Path	Required. Enter the path where temporary path mounts inside the pod.
Configure Volumes	Click **Add** to display a block of **Volume** settings. Click again to add another block of settings.
Mount Path	Required. Enter the path where the volume mounts inside the pod.
Dataset Name	Required. Enter the name of the dataset.

Workload Details

The **Workload Details** settings specify if containers in a pod run with TTY or STDIN enabled, allow it to enable any device on the host or configure host capabilities, and if you run the container as a user or group.

Click Here for More Information



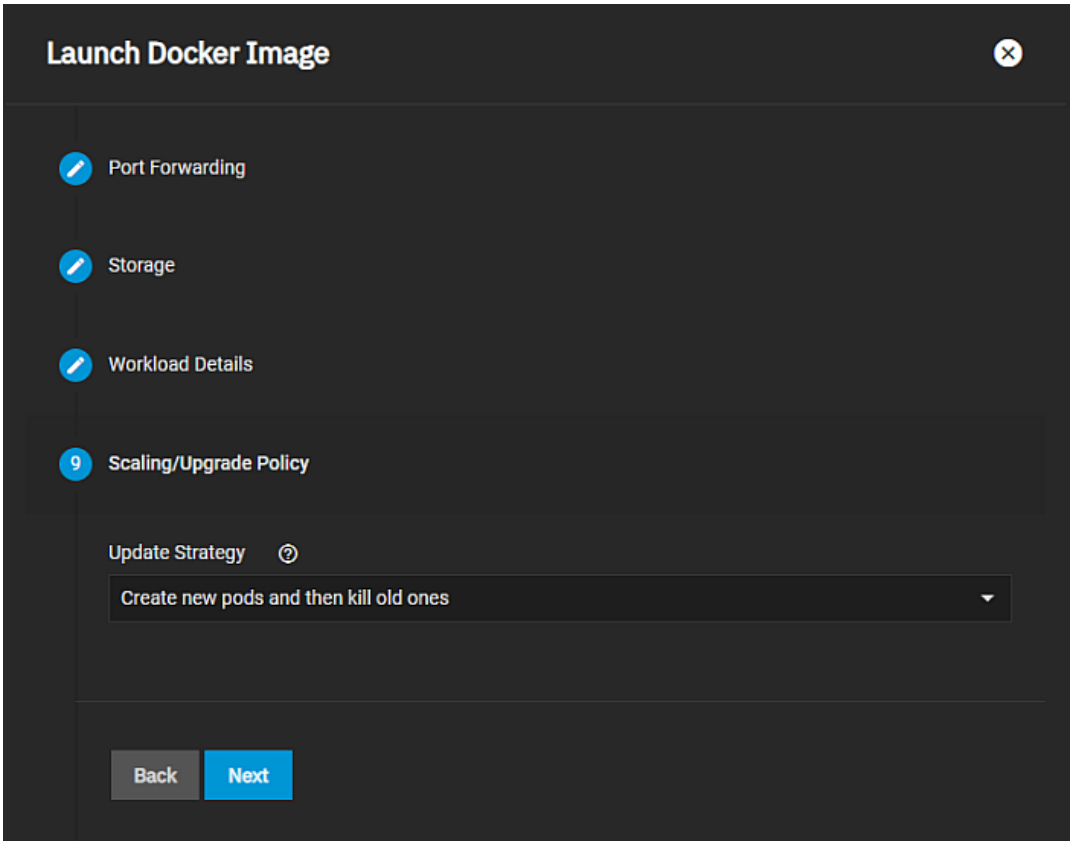
Setting	Description
Enable TTY	Select to set containers in a pod to run with TTY enabled. Disabled by default.
enable STDIN	Select to set containers in a pod to run with STDIN enabled. Disabled by default.

Setting	Description
Privileged Mode	Select to allow any container in a pod to enable any device on the host, but a **privileged** container is given access to all devices on the host. This allows the container nearly all the same access as processes running on the host.
Configure Capabilities	Click **Add** to display a **Add Capability** field**. Click again to add another field.
Add Capability	Enter a capability.
Configure Container User and Group ID	Select to display the **Run Container as User** and **Run Container as Group** settings to add security context (`runAsUser` and `runAsGroup` variables).
Run Container As User	Enter a user ID (numeric value) for container.
Run Container as Group	Enter a group ID (numeric value) for container.

Scaling/Upgrade Policy

Use **Kill existing pods before creating new ones** to recreate the container or **Create new pods and then kill old ones** if you want rolling upgrades.

Click Here for More Information



Select **Create new pods and then kill the old ones** to retain your existing configuration and container until the upgrade completes before removing it. Select **Kill existing pods before creating new ones** to remove the exiting pod and start with a new updated pod. This is useful if your old pod was not functioning properly. For fewer issues, select **Kill existing pods before creating new ones**.

Resource Reservation

The **Resource Reservation** screen specifies the **GPU configuration**.

Resource Limits

The **Resource Limits** setting specifies whether to **Enable Pod resource limits**.

Portal Configuration

The **Portal Configuration** setting specifies whether to **Enable WebUI Portal (only supported in TrueNAS SCALE Bluefin)**.

Confirm Options

The **Confirm Options** screen displays a summary of the image/container configuration. Click **Back** to return to previous screens to make changes and **Next** to advance back to **Confirm Options**. Click **Save** to create the image and add the application to the **Installed Applications** screen.

Related Content

- Updating MinIO from 1.6.58
- Using SCALE Catalogs
- Using Docker Image
- MinIO Clusters
- Adding Pi-Hole Using Docker Image

Related Apps Articles

- Applications Screens
- Updating MinIO from 1.6.58
- Using Apps
- Using SCALE Catalogs
- Using Docker Image
- Adding NextCloud for Media Previews
- Configuring the Chia App
- Collabora App
- MinIO Clusters

4.10 - Reporting

Article Summaries

- Reporting Screens

  This article provides information on TrueNAS reporting graph screens and settings.

4.10.1 - Reporting Screens

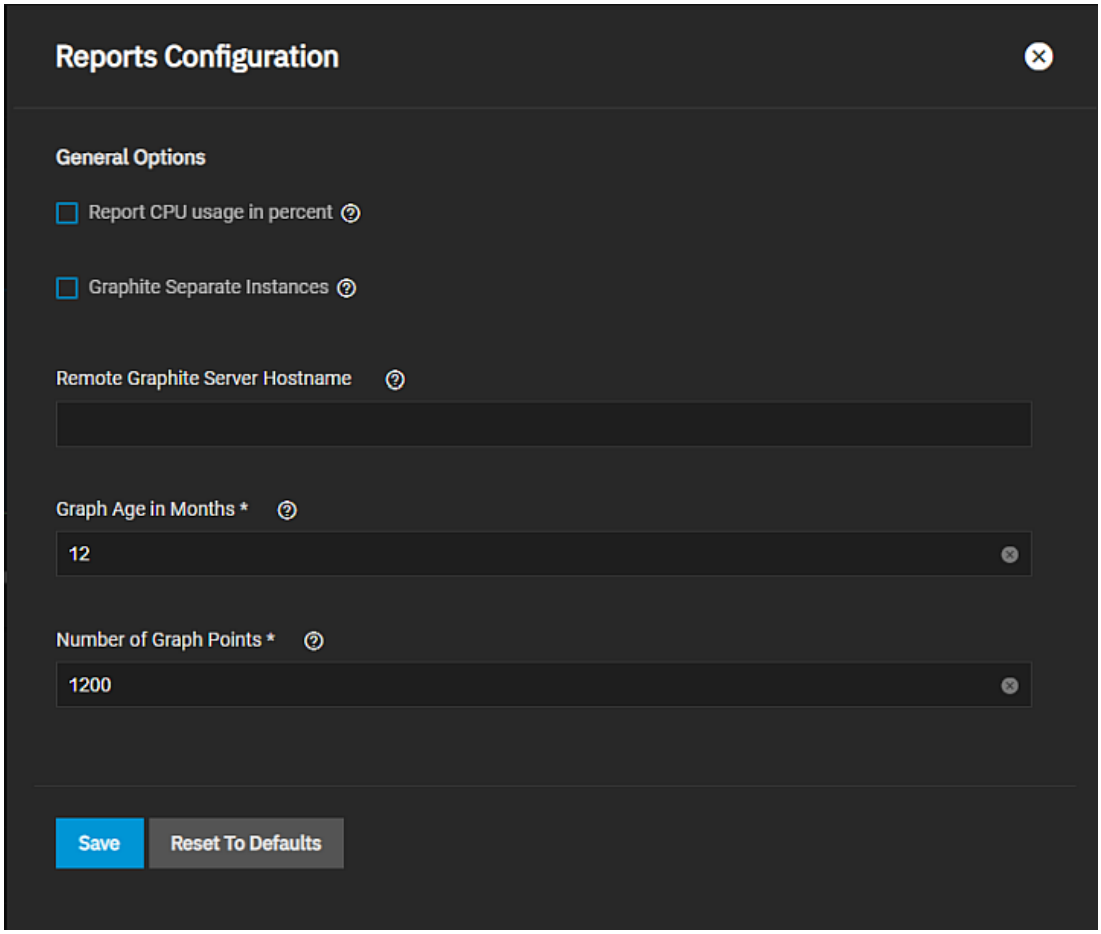
This article provides information on TrueNAS reporting graph screens and settings.

The **Reporting** screen displays graphs of system information for CPU, disk, memory, network, NFS, partition, target, UPS, ZFS, and system functions. The **CPU** report displays by default.

The ⚙ opens the **Reports Configuration** configuration screen.

Reports Configuration Screen

Reports Configuration settings specify how TrueNAS displays the graphs and the host name of the Graphite server.



General Options

Name	Description
Report CPU usage in Percent	Reports CPU usage in percent instead of units of kernel time.
Graphite Separate Instances	Sends the plugin instance and type instance to Graphite as separate path components: *host.cpu.0.cpu.idle*. Disabling sends the plugin and plugin instance as one path component and type and type instance as another: *host.cpu-0.cpu-idle*.
Remote Graphite Server Hostname	Remote Graphite server host name or IP address.
Graph age in Months	Maximum time (in months) TrueNAS stores a graph. Allowed values are 1-60. Changing this value causes the **Confirm RRD Destroy** dialog to display. Changes do not take effect until TrueNAS destroys the existing reporting database.
Number of Graph Points	The number of points for each hourly, daily, weekly, monthly, or yearly graph. Allowed values are 1-4096. Changing this value displays the **Confirm RRD Destroy** dialog. Changes do not take effect until TrueNAS destroys the existing reporting database.
Reset to Defaults	Resets all entered values and settings back to defaults.

Reporting Screen Display Options

Setting	Description
CPU	Displays the **CPU Temperature**, **CPU Usage**, and **System Load** graphs.
Disk	Displays graphs for each selected system disk and by report type.
Memory	Displays both the **Physical memory utilization** and **Swap utilization** graphs.
Network	Displays an **Interface Traffic** graph for each interface in the system.
NFS	Displays the **NFS Stats (Operations)** and **NFS Stats (Bytes)** graphs.
Partition	Displays graphs showing disk space allocations.
System	Displays both the **Processes** and **Uptime** graphs.
Target	Displays graphs only for systems with iSCSI ports configured and shows the bandwidth statistics for iSCSI ports.
UPS	Displays the graphs only if the system is configured for and uses a UPS.
ZFS	Displays the **ARC Size**, **ARC Hit Ratio**, **ARC Requests demand_data**, **ARC Requests demand_metadata**, **ARC Requests prefetch_data**, and **ARC Requests prefetch_metadata** graphs with the Arc and L2 gigabytes and hits (%), and the hits, misses and total number of requests.

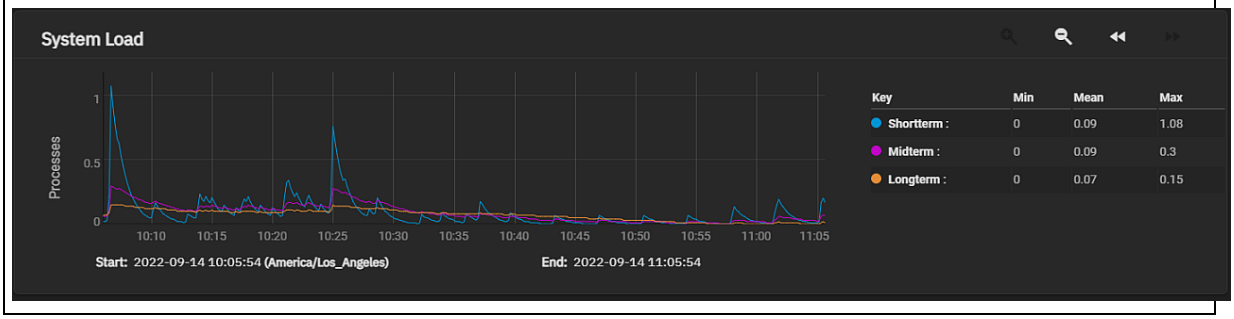
Report Graphs

The following sections provide examples of each report graph.

CPU Graphs

Click Here for More Information

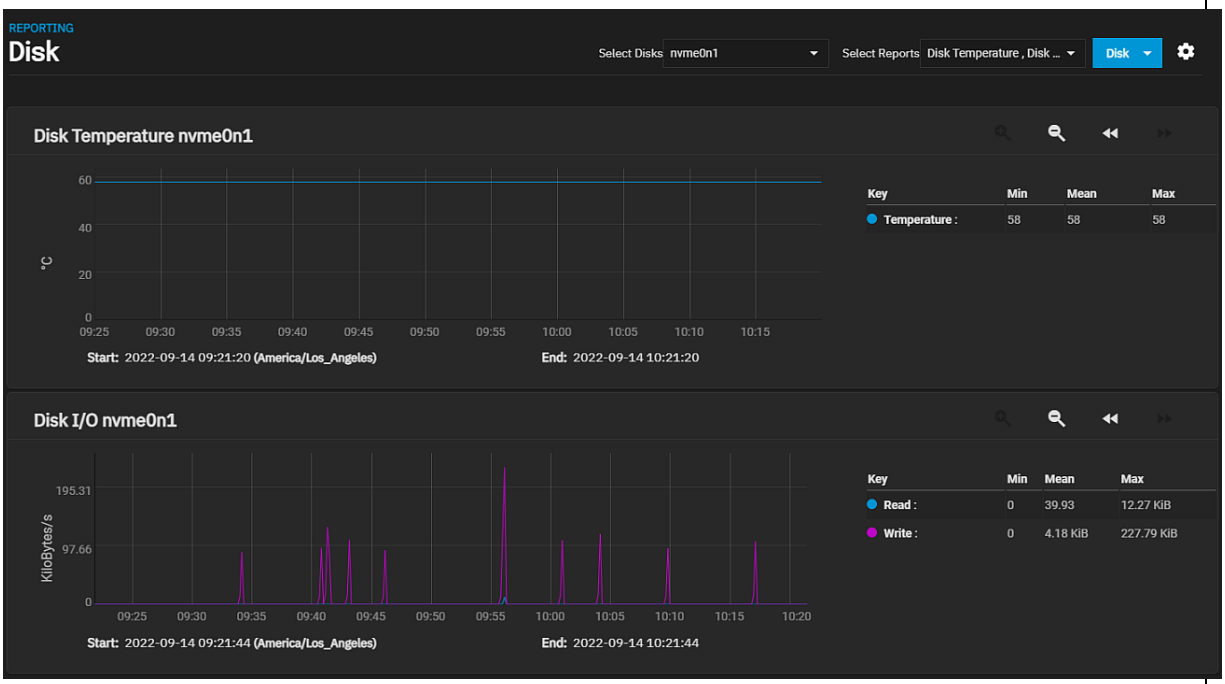
CPU graphs show the amount of time spent by the CPU in various states such as executing user code, executing system code, and being idle. Graphs of short-, mid-, and long-term load are shown, along with CPU temperature graphs.



Disk Graphs

Click Here for More Information

Disk graphs shows read and write statistics on I/O, percent busy, latency, operations per second, pending I/O requests, and disk temperature. Use the **Select Disks** dropdown list to select the disks and the **Select Reports** dropdown to select the report types to display.



Disk Report Options

Setting	Description
Select All	Displays all available graphs for any or all disks selected on the **Disks** dropdown list.
Disk Temperature	Displays the minimum, maximum and mean temperature reading for the disk selected.
Disk I/O	Displays the disk read and write I/O stats in bytes/s.

> Temperature monitoring for the disk is disabled if **HDD Standby** is enabled. Check the **Storage > Disks Edit Disk*** configuration form for any or all disks in the system if you do not see the temperature monitoring graph.

Memory Graphs

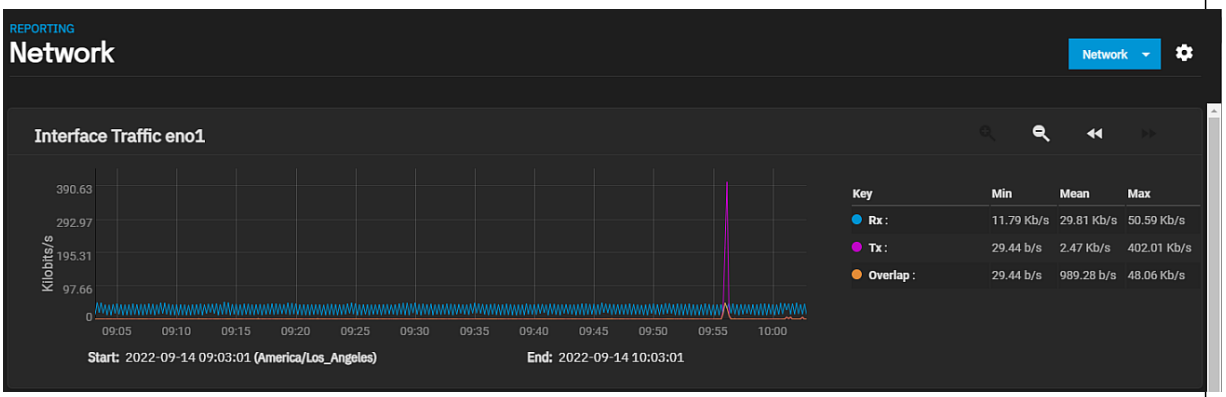
Click Here for More Information

Memory graphs display memory usage and swap graphs display the amount of free and used swap space.

Network Graphs

Click Here for More Information

Network graph report received and transmitted traffic in megabytes per second for each configured interface.



NFS Graphs

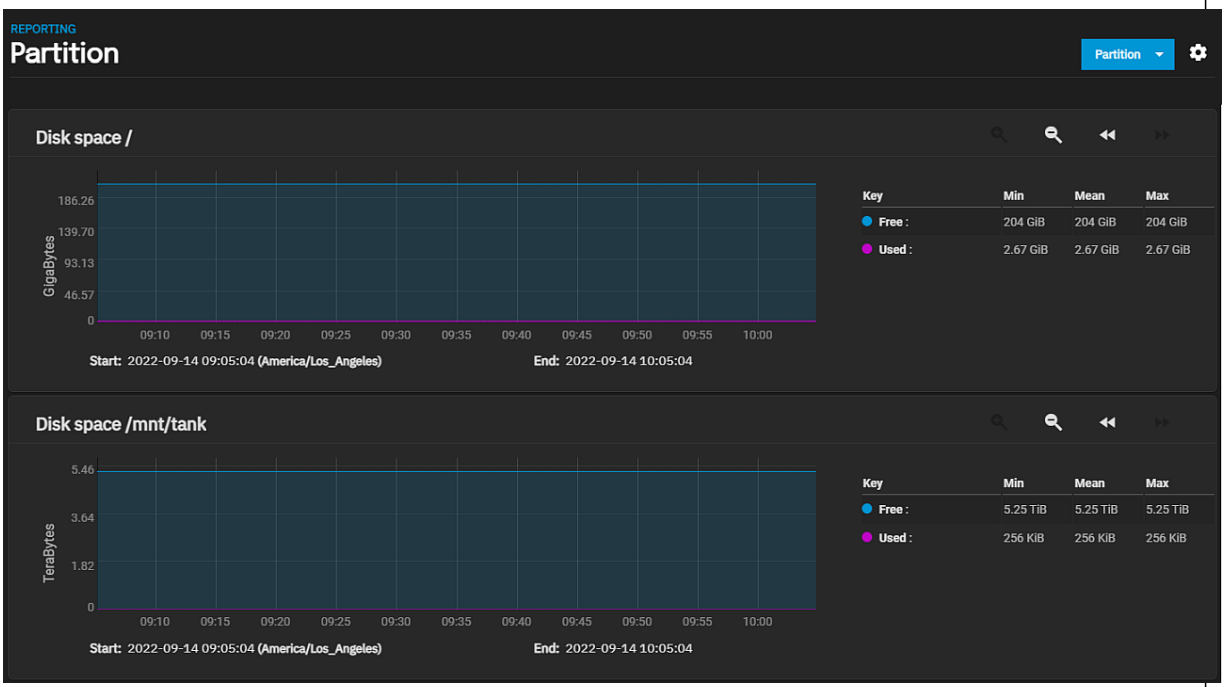
Click Here for More Information

NFS graphs show information about the number of calls for each procedure and whether the system is a server or client.

Partition Graphs

Click Here for More Information

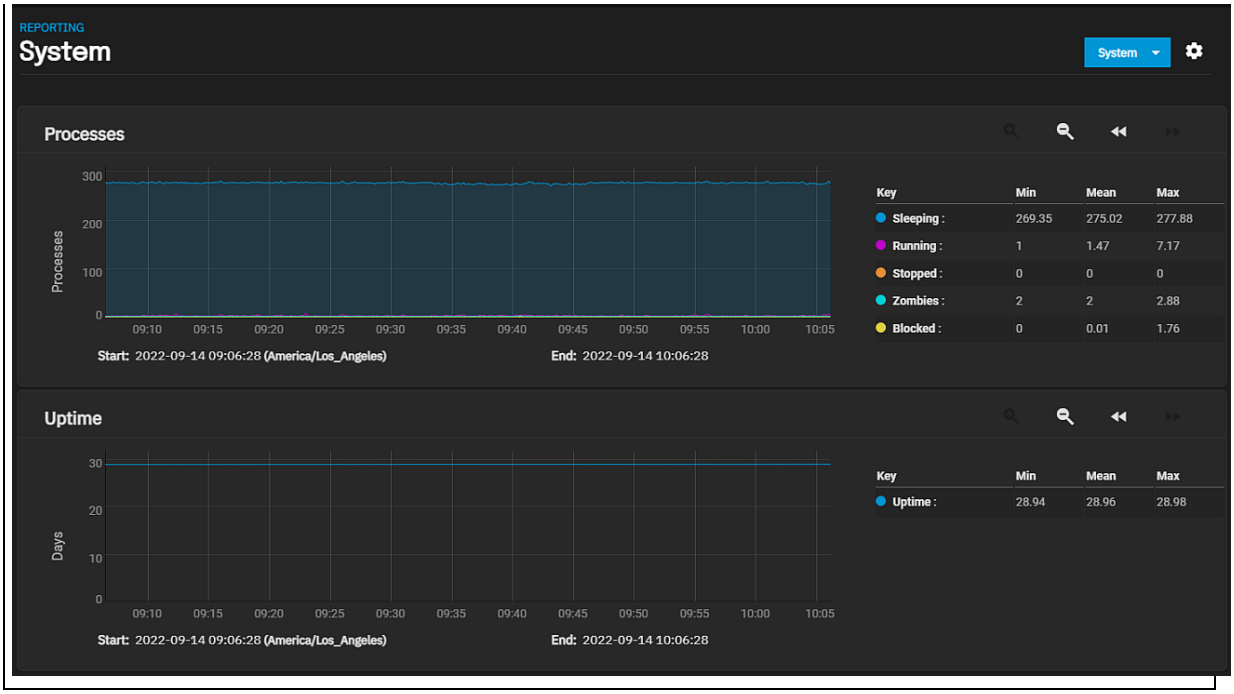
Partition graphs display free, used, and reserved space for each pool and dataset. However, the disk space used by an individual zvol is not displayed as it is a block device.



System Graphs

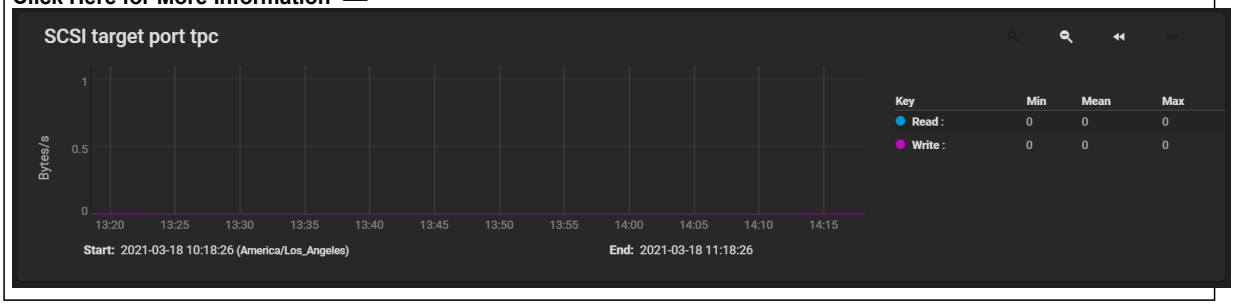
Click Here for More Information

System graphs display the number of processes grouped by state, sleeping, running, stopped, zombies and blocked, and system uptime.



Target Graphs

Click Here for More Information



UPS Graphs

Click Here for More Information

UPSgraphs show statistics about an uninterruptible power supply (UPS) using Network UPS tools. Statistics include voltages, currents, power, frequencies, load, and temperatures.

ZFS Graphs

Click Here for More Information

ZFS graphs show compressed physical ARC size, hit ratio, demand data, demand metadata, and prefetch data and metadata.

Related Content

- Configuring Reporting

4.11 - System Settings

Article Summaries

- Update Screens

  System Update No Upgrade Screen Save Configuration Settings Window Manual Update Screen The TrueNAS SCALE Update screen lets users update their system using two different methods: manual and automatic. If updates are available the screen inludes the options to Download Updates, Apply Pending Update and Install Manual Update File. The upgrade available displays in the center of the screen. When selected, Check for Updates Daily and Download if Available checks the update server daily for any updates on the chosen train.

- General Settings Screen

  This article provides information on general system setting screen widgets and settings for getting support, changing console or the GUI, localization and keyboard setups, and adding NTP servers.

- Advanced Settings Screen

  This article provides information on the **System > Advanced** screen widgets and configuration screen settings.

- System Boot Screens

  This article provides information on the boot environment screens and settings.

- Services

  This article provides general information on the **Services** screen, and a summary of each indiviual service article in the Services area.

  - Dynamic DNS Service Screen

    This article provides information on Dynamic DNS screen settings.

  - FTP Service Screen

    This article provides information on the FTP services screens and settings.

  - LLDP Services Screen

    This article provides information on the LLDP service settings.

  - NFS Services Screen

    This article provides information on NFS service screen and settings.

  - OpenVPN Screens

    This article provides information on OpenVPN client and server screens and settings.

  - Rsync Services Screen

    This article provides information on the rsync services screens and settings.

  - S.M.A.R.T. Service Screen

    This article provides information on S.M.A.R.T. service screen settings.

  - S3 Service Screen

    This article provides information on the the S3 service screen settings.

  - SMB Service Screen

    This article provides information in the SMB service screen and settings.

  - SNMP Service Screen

    This article provides information on SNMP service screen settings.

  - SSH Service Screen

    This article provides information on the SSH service screens and settings.

  - TFTP Services Screen

    This article provides information on the TFTP screen settings.

  - UPS Services Screen

    This article provides information on the UPS service screen settings.

    - WebDAV Service Screen

      This article provides information on WebDAV service screen and settings.
- Shell Screen

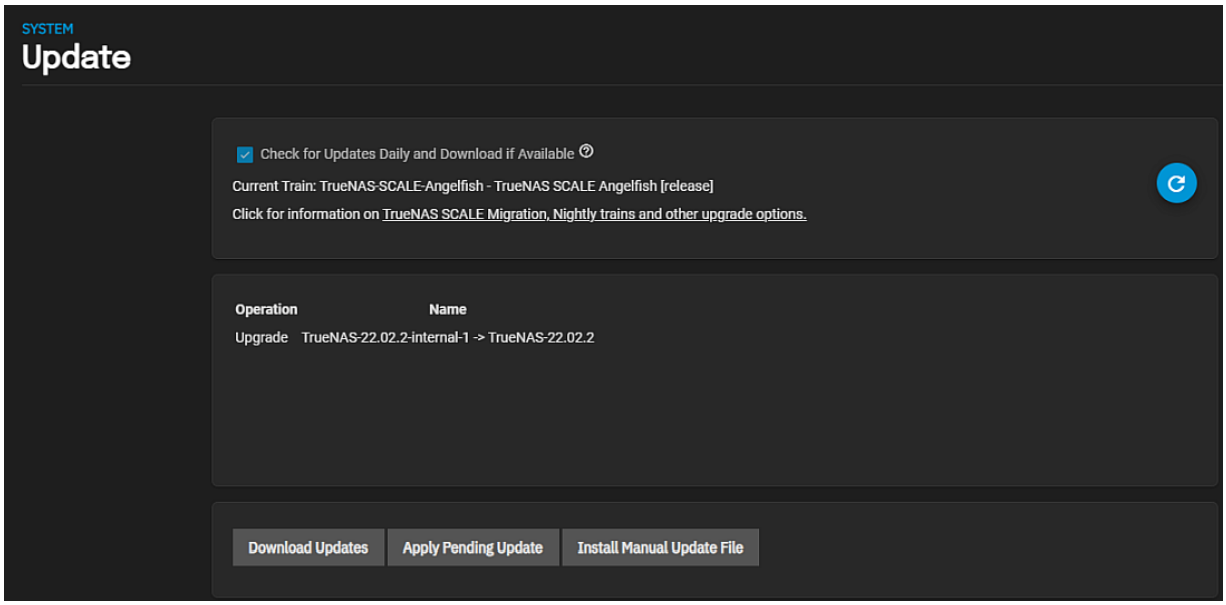
  This article provides information on the SCALE **Shell** screen, buttons and slider.

- View Enclosure Screen

  This article provides information on the TrueNAS **View Enclosure** screen, and the information you can find there.

4.11.1 - Update Screens

The TrueNAS SCALE **Update** screen lets users update their system using two different methods: manual and automatic. If updates are available the screen inludes the options to **Download Updates**, **Apply Pending Update** and **Install Manual Update File**. The upgrade available displays in the center of the screen.



When selected, **Check for Updates Daily and Download if Available** checks the update server daily for any updates on the chosen train. It automatically downloads an update if one is available.

Refresh refreshes the information displayed on the screen.

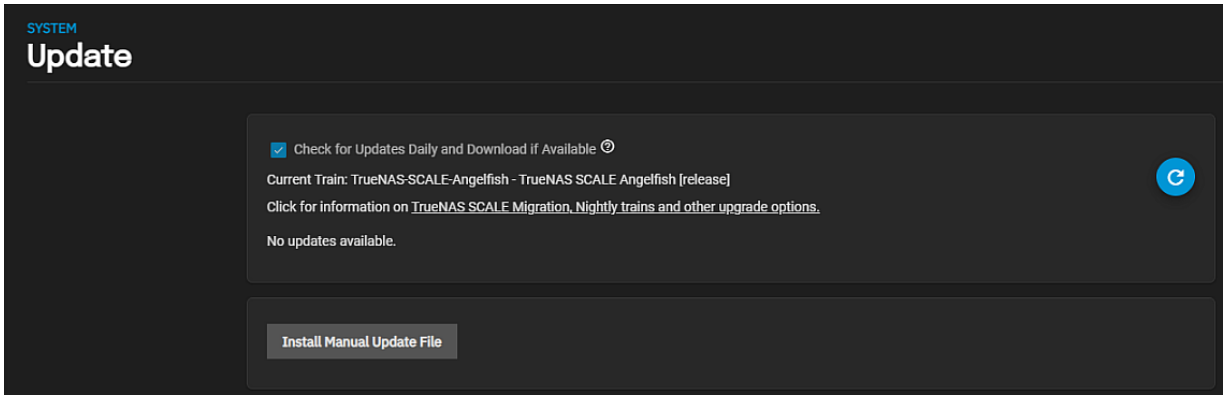
Download Updates begins downloading the update file to the system.

Apply Pending Update begins the automatic installation process for the update file you downloaded beginning with the **Save configuration settings from this machine before updating** window.

Install Manual Update File opens the **Save configuration settings from this machine before updating** window first.

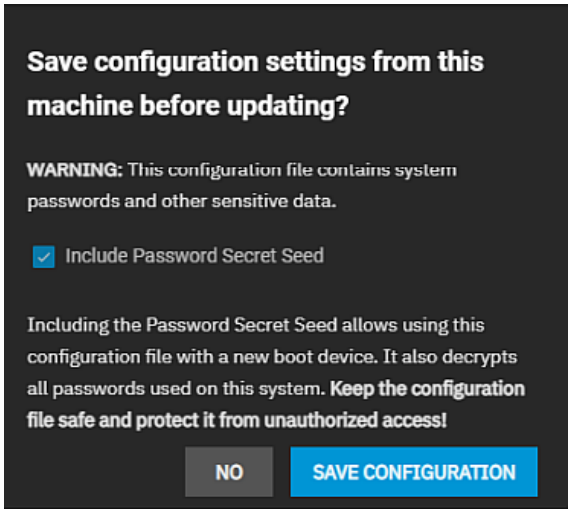
System Update No Upgrade Screen

If **Check for Updates Daily and Download if Available** is selected, and the system does not find a new update file, the screen only displays the **Install Manual Update File** option.



Save Configuration Settings Window

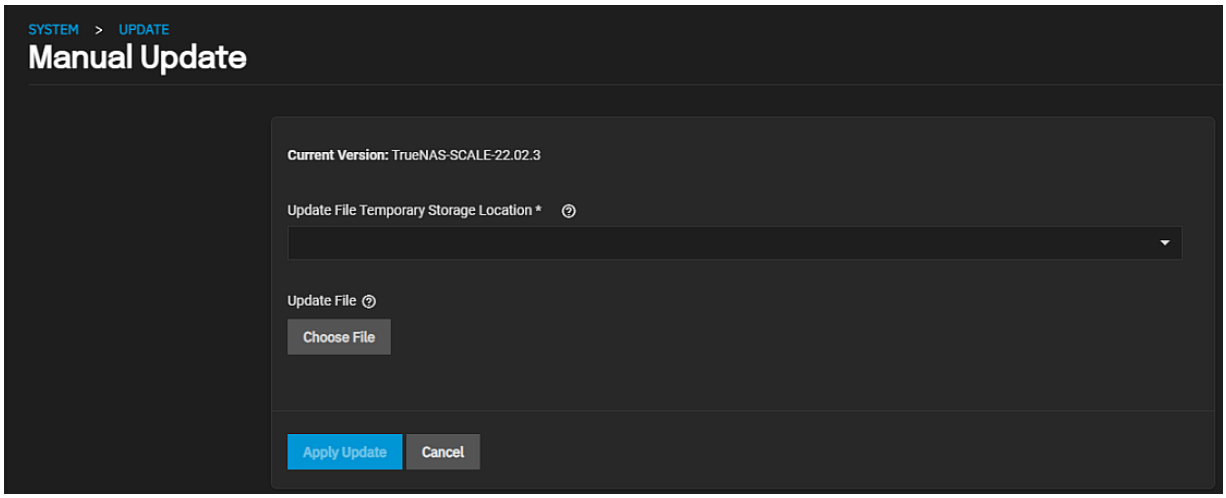
Before the automatic or manual update installation process begins the **Save configuration settings from this machine before updating** window displays.



Always select **Include Password Secret Seed** before you click **Save Configuration**.

Manual Update Screen

The **Manual Update** screen displays after you click **Save Configuration** or **No** on the save configuration settings window.



The update **Current Version** displays the SCALE release version running on your system.

Use **Update File Temporary Storage Location** dropdown to specify the temporary location to store the upgrade or update file. Select **Memory Device** or to keep a copy in the server, select one of the mount locations on the dropdown list.

Choose File opens a browse window that allows you to locate the downloaded update filed.

Click **Apply Update** to start the installation.

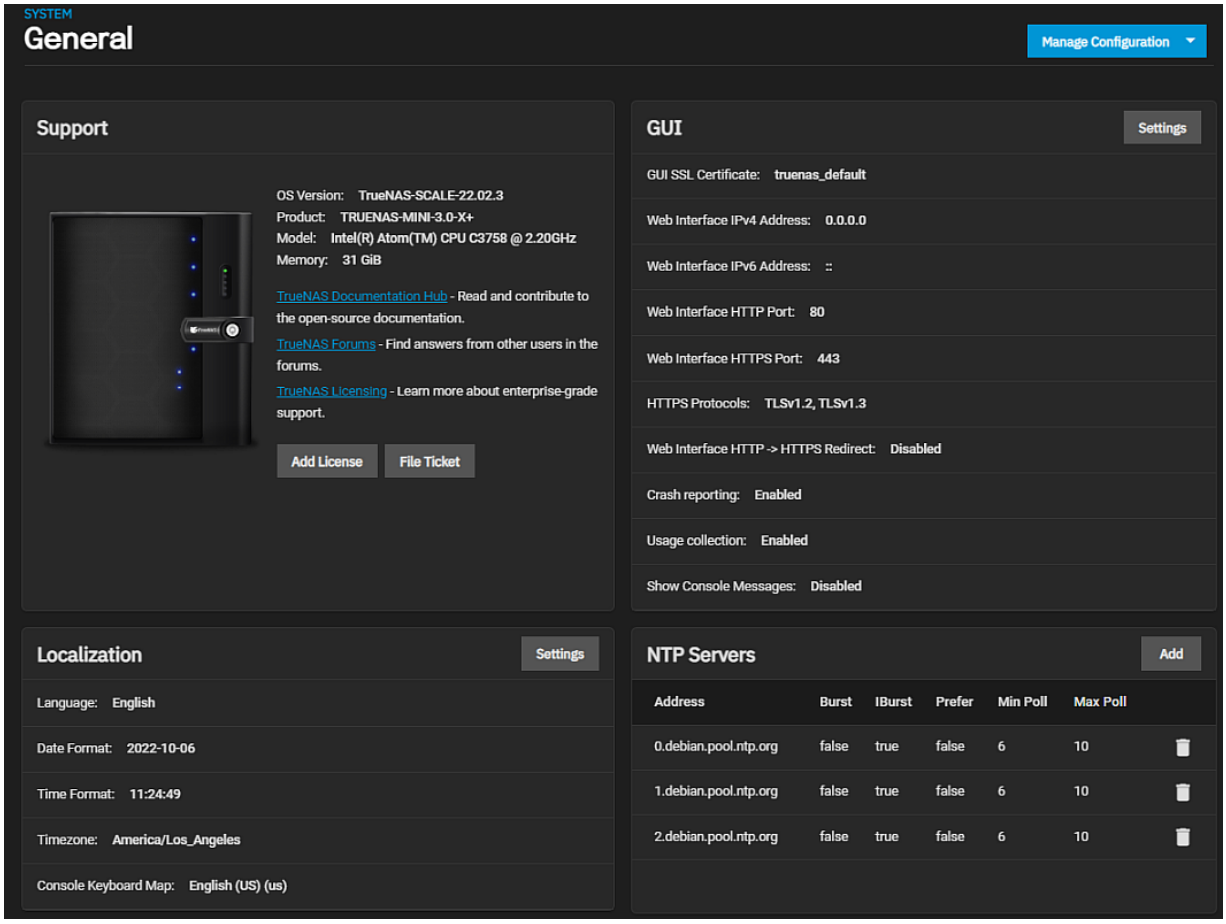
Related Content

- Updating SCALE
- Installing SCALE

4.11.2 - General Settings Screen

This article provides information on general system setting screen widgets and settings for getting support, changing console or the GUI, localization and keyboard setups, and adding NTP servers.

The TrueNAS SCALE **System Settings > General** screen includes widgets for **Support**, **GUI**, **Localization**, and **NTP** functions.



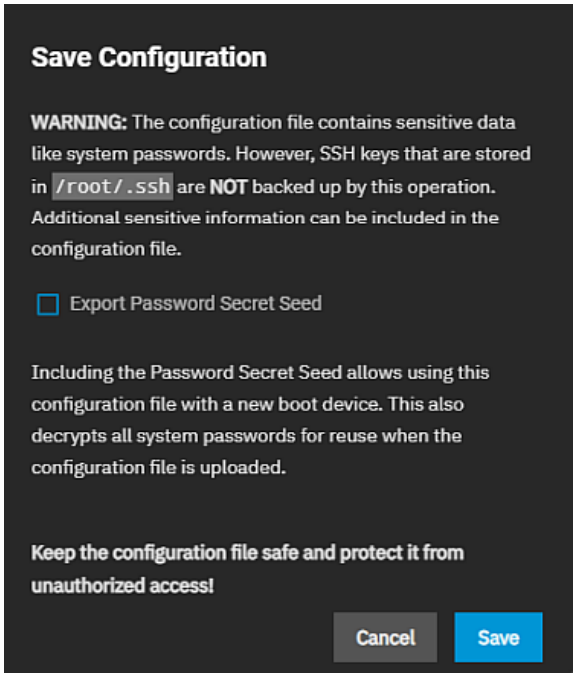
Manage Configuration provides three options to backup, restore, or reset system configuration settings.

Manage Configuration Screens

TrueNAS SCALE allows users to manage the system configuration via uploading/downloading configurations or resetting the system to the default configuration.

Download File Window

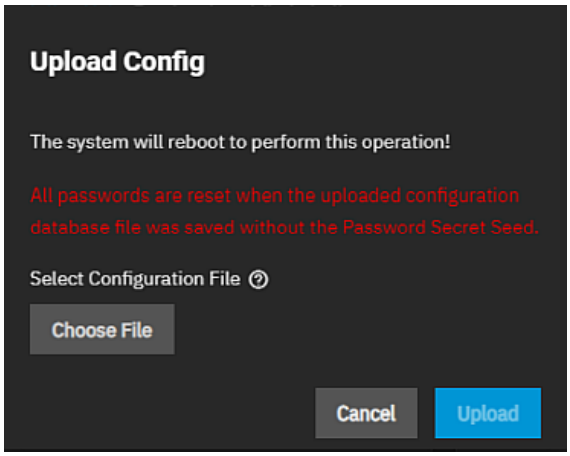
The **Download File** option opens the **Save Configuration** window. This allows you to download the TrueNAS SCALE current configuration for your system to the local machine.



The **Export Password Secret Seed** includes encrypted passwords in the downloaded configuration file. This allows you to restore the configuration file to a different operating system device where the decryption seed is not already present. Users must physically secure configuration backups containing the seed to prevent unauthorized access or password decryption.

Upload File Window

The **Upload File** option opens the **Upload Config** window with the **Choose File** option that lets you replace the current system configuration with any previously saved TrueNAS SCALE configuration file.

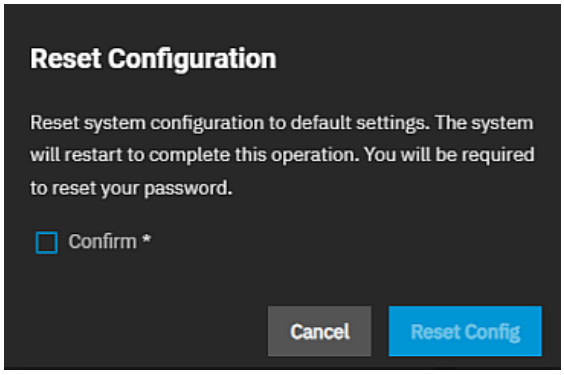


Choose File opens a file browser window where you can locate the downloaded and saved configuration. After selecting the file it displays in the **Upload Config** window. **Upload** uploads the selected configuration file.

> All passwords are reset if the uploaded configuration file was saved without the selecting **Export Password Secret Seed**.

Reset to Defaults Window

The **Reset to Defaults** option opens the **Reset Configuration** window. This resets the system configuration to factory settings and restarts the system. Users must set a new login password.

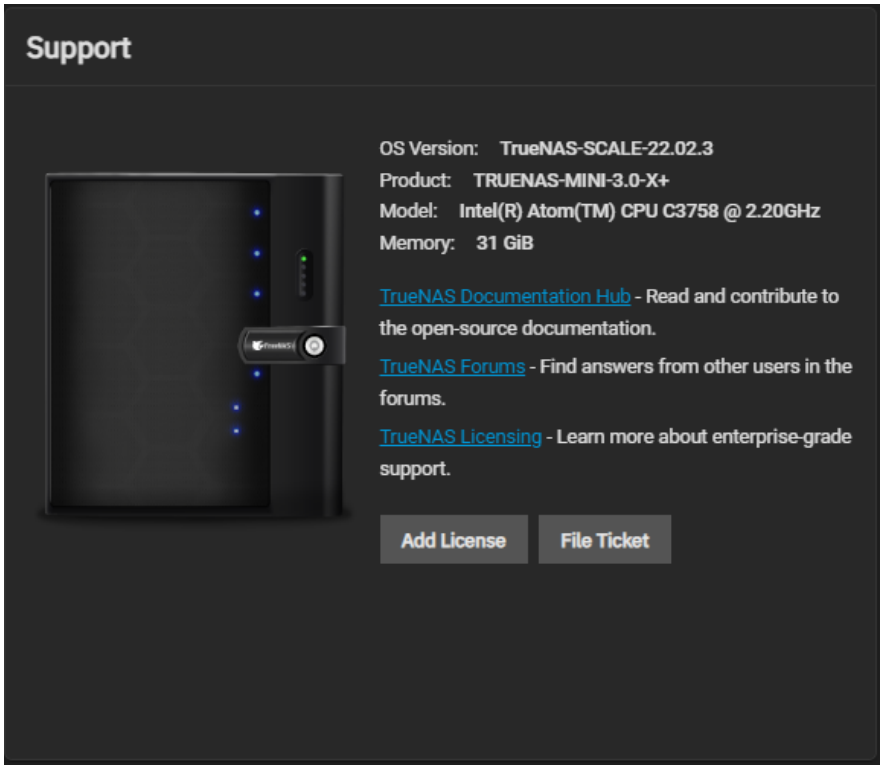


Save the system current configuration with the *Download File* option before resetting the configuration to default settings.

If you do not save the system configuration before resetting it, you may lose data that was not backed up, and you will not be able to revert to the previous configuration.

Support Widget

The **Support** widget displays the systems general hardware and software specs and contains links to the Documentation Hub, TrueNAS Forums, and offers TrueNAS Licensing information.



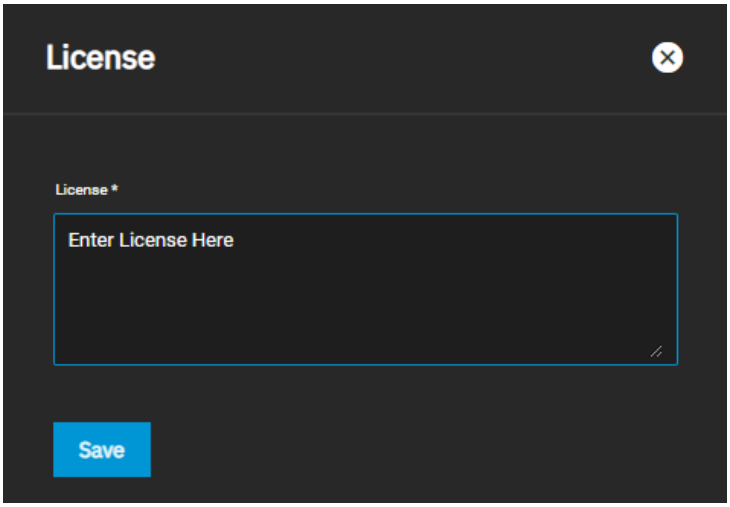
Add License opens the **License** screen.

File Ticket opens the **File Ticket** screen.

License Screens

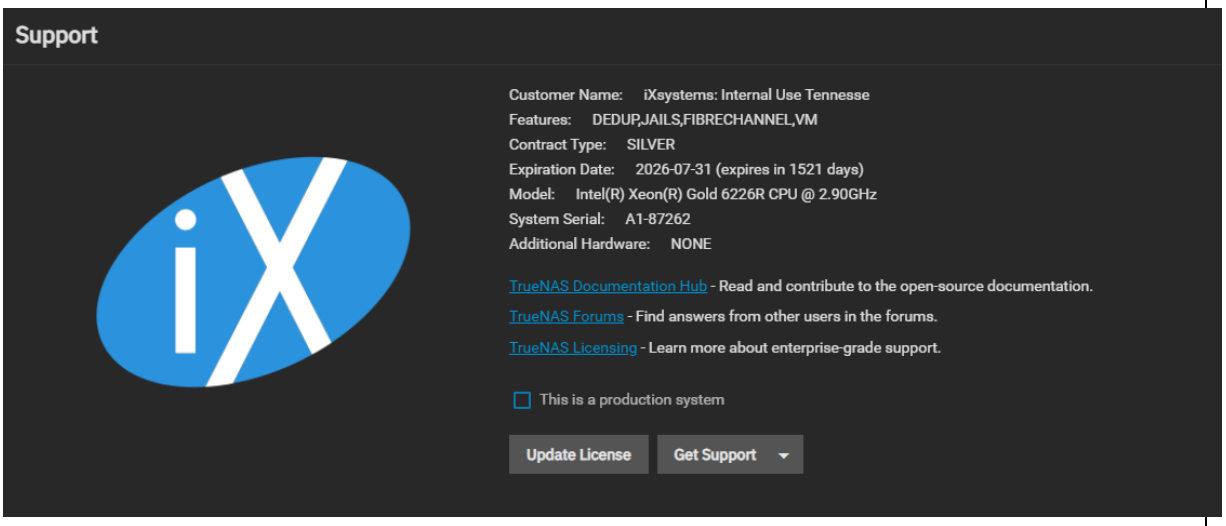
The **License** screen allows you to copy your license into the box and then save it.

Click Here for More Information



When prompted to reload the page, click **Reload Now**.

When the **End User License Agreement (EULA)** opens, read it thoroughly and completely, click **I AGREE**.

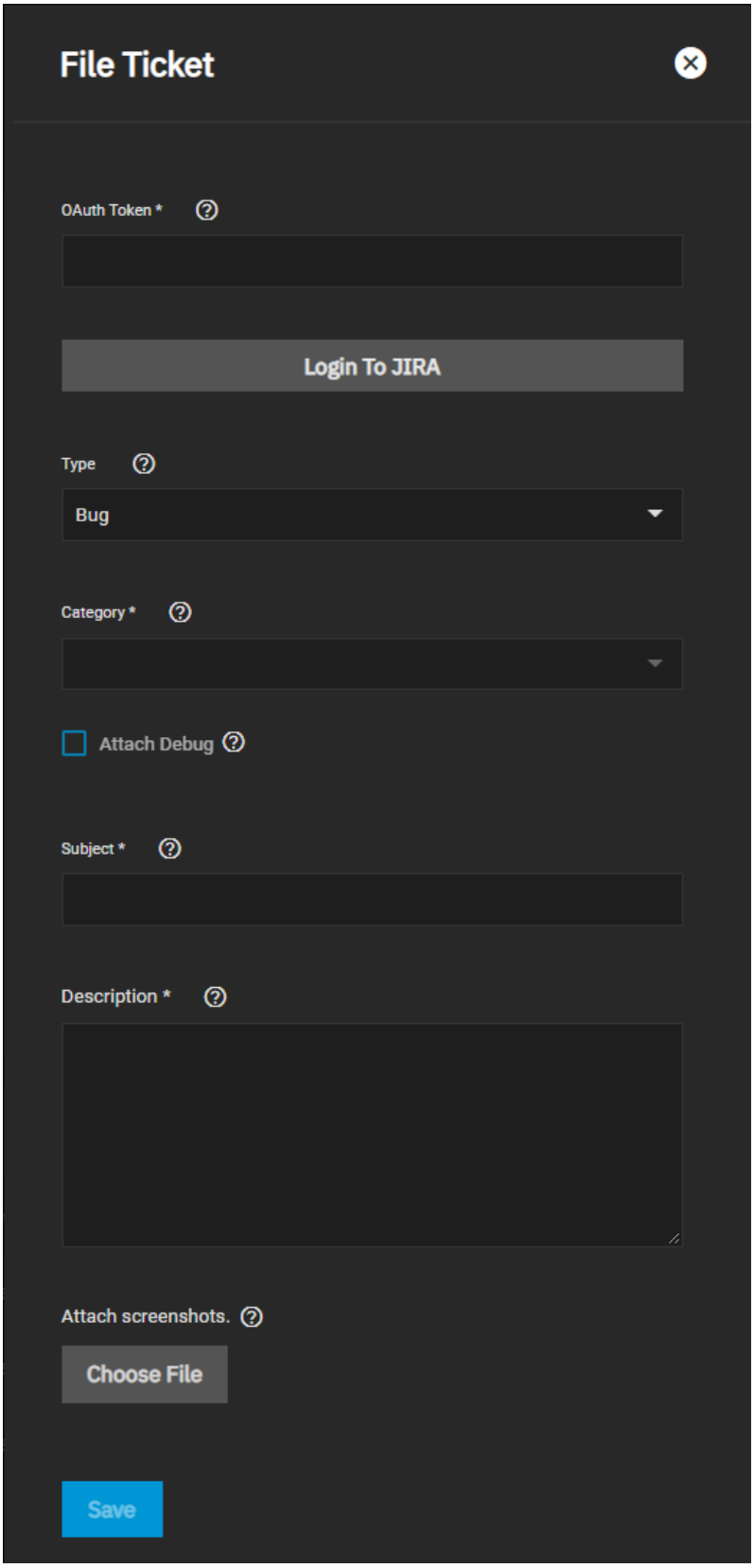


Select the **This is a production system** option and click the **Proceed** to notify iXsystems through an email the system sends declaring that the system is in production.

File Ticket Screen

The **File Ticket** screen settings allow you to log into Jira where you can submit a ticket. The screen provides the required ticket information fields to complete when submitting an issue report.

Click Here for More Information



Setting	Description
OAuth Token	Populated with the authentication token generated by logging into to Jira.
Login to JIRA	Opens a login widow where you enter your Jira credentials. After logging in to Jira, select **Allow** to give TrueNAS read and write access to your data on the Jira site. This generates token that displays in the **OAuth Token** field.
Type	Select the issue type from the dropdown list. Select **Bug** to report a problem, **Feature** to submit a new feature request.

Setting	Description
Category	Select the option from the dropdown list that best fits your report. Becomes active after logging into Jira.
Attach Debug	Select to downloads and attach a debug file to the issue ticket. If the debug file is too large to attach to your ticket, a window with instructions opens.
Subject	Enter a brief summary of the issue as the title or subject of the ticket.
Description	Enter details or an outline that describes the reason for submitting the ticket. Be complete with your description.
Choose File	Opens a file browser that allows you to add any screenshots or log files as attachments.
Save	Submits the ticket and then opens a window with a link to the ticket.

Get Support

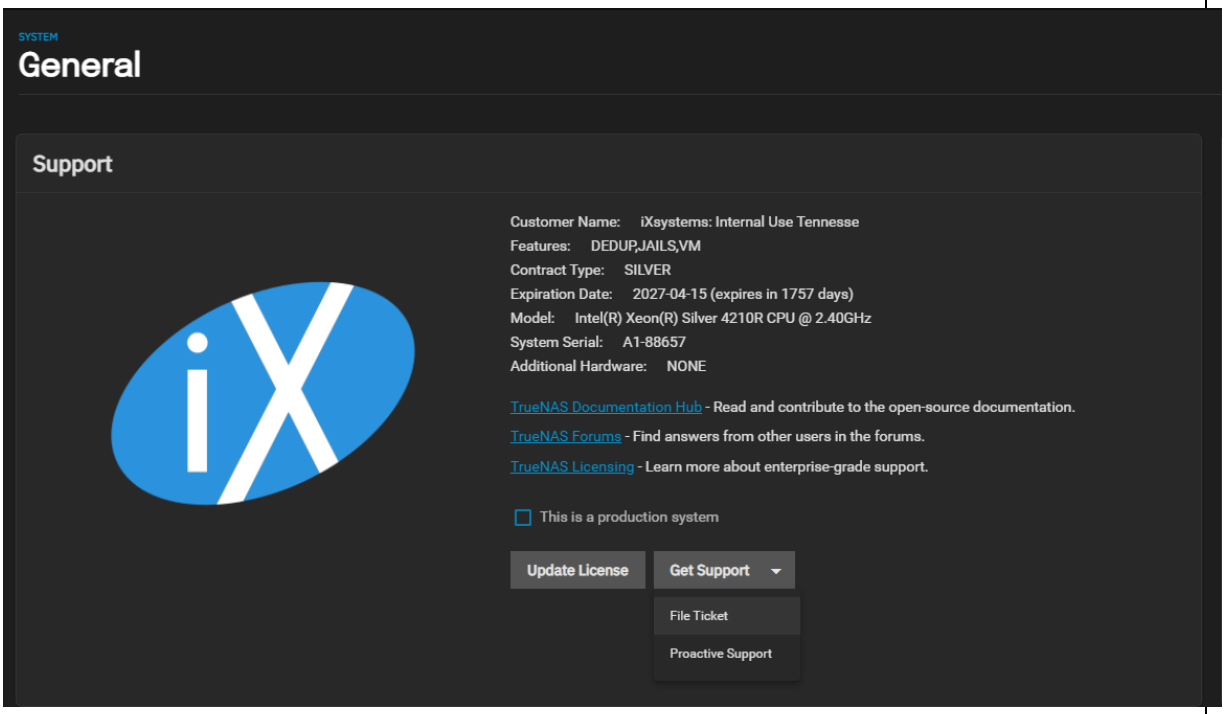
For Enterprise customers, the **Get Support** option displays on the **Support** widget and provides the options **File Ticket** and **Proactive Support**.

Proactive Support Screen

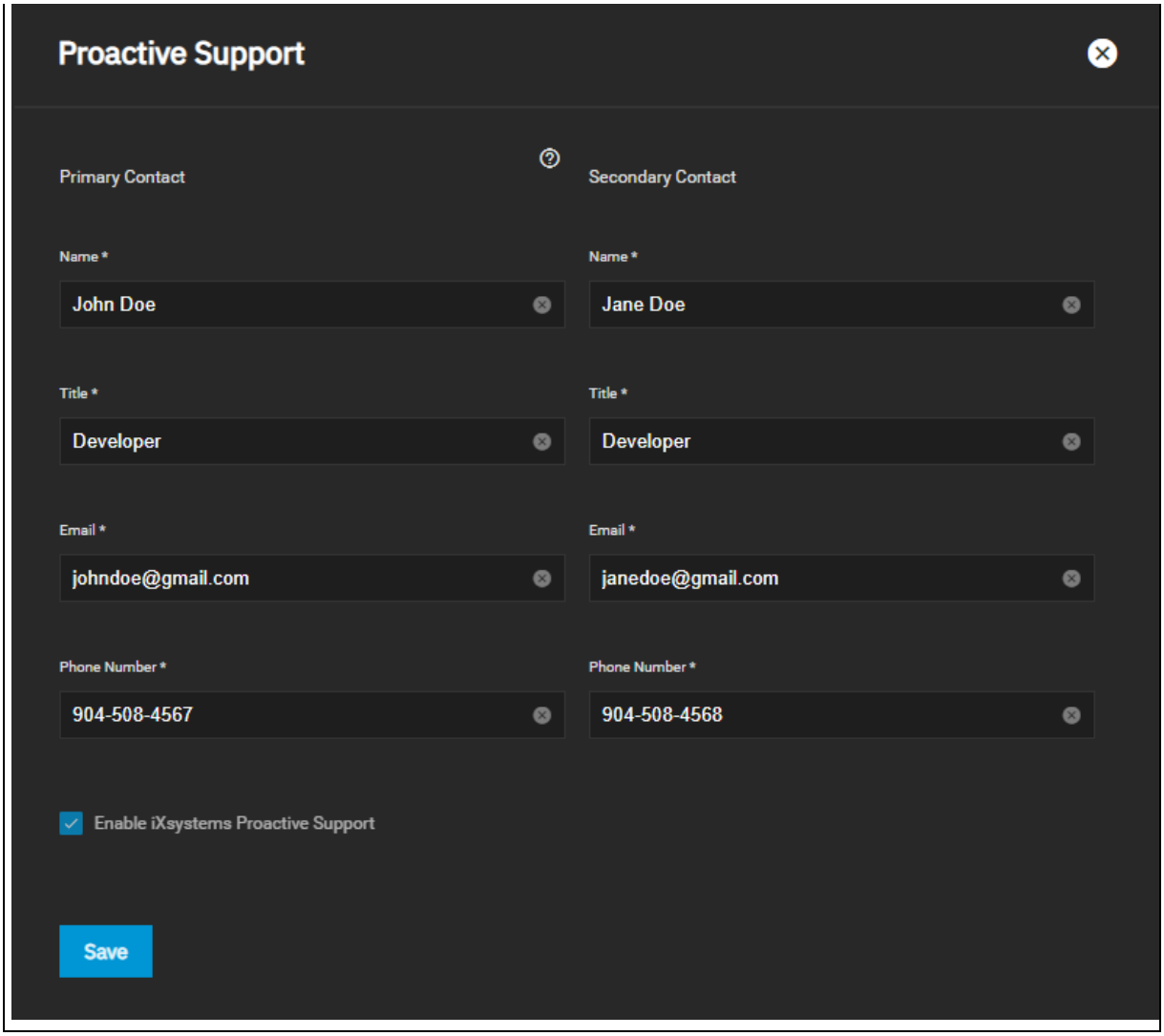
Silver/Gold Coverage Customers can enable iXsystems Proactive Support. This feature automatically emails iXsystems when certain conditions occur in a TrueNAS system.

Click Here for More Information

To configure Proactive Support, click the **Get Support** dropdown and select **Proactive Support**.



Complete all available fields and ensure the **Enable iXsystems Proactive Support** box is checked, click **Save**.

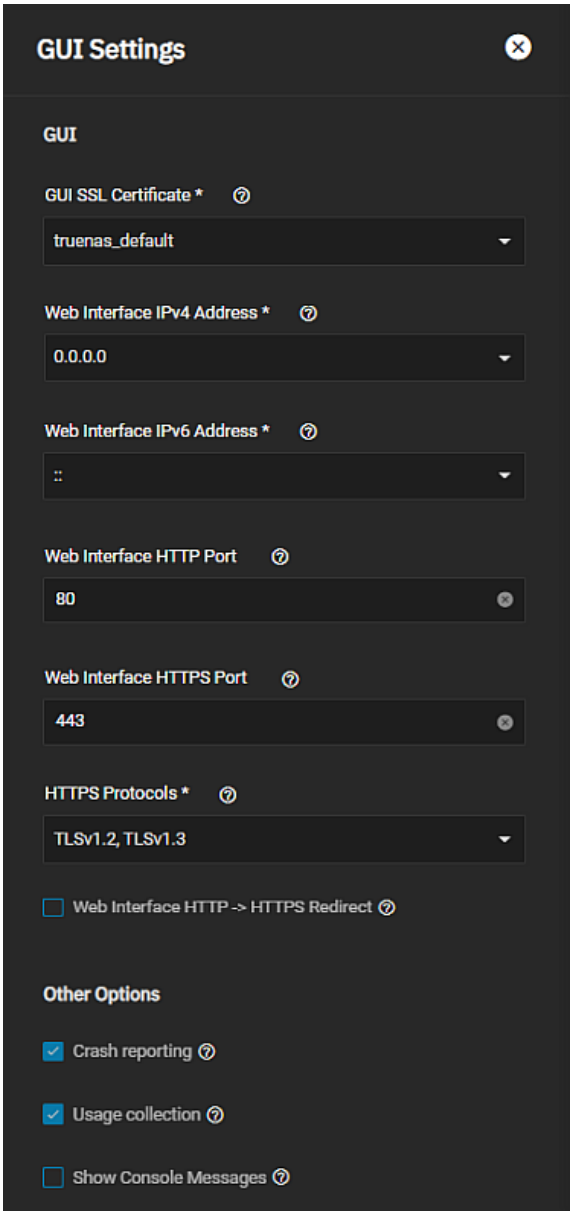


GUI

The **GUI** widget allows users to configure the TrueNAS SCALE web interface address.

Click Here for More Information

Click **Settings** to open the **GUI Settings** screen.



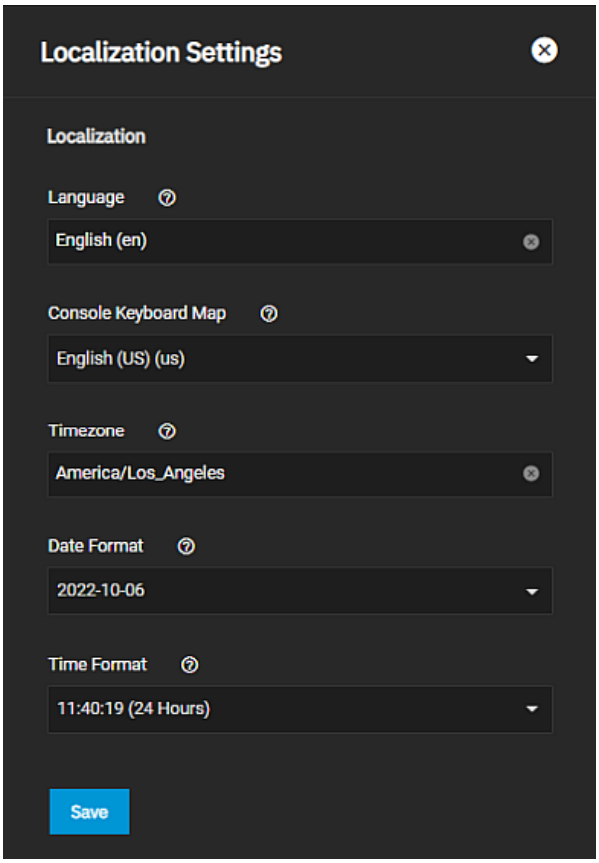
Setting	Description
GUI SSL Certificate	Select a self-signed certificate from the dropdown list. The system uses a self-signed certificate to enable encrypted web interface connections.
Web Interface IPv4 Address	Select a recent IP address from the dropdown list to limit the usage when accessing the administrative GUI. The built-in HTTP server binds to the wildcard address of **0.0.0.0** (any address) and issues an alert if the specified address becomes unavailable.
Web Interface IPv6 Address	Select a recent IPv6 address from the dropdown list to limit the usage when accessing the administrative GUI. The built-in HTTP server binds to the wildcard address of **0.0.0.0** (any address) and issues an alert if the specified address becomes unavailable.
Web Interface HTTPS Port	Enter a port number for an HTTPS connection to the web interface. This field allows configuring a non-standard port to access the GUI over HTTPS.
HTTPS Protocols	Select the Transport Layer Security (TLS) versions TrueNAS SCALE can use for connection security from the dropdown list. Cryptographic protocol for securing client/server connections.
Web Interface HTTP -> HTTPS Redirect	Select to redirect HTTP connections to HTTPS. A GUI SSL Certificate is required for HTTPS. Activating this also sets the HTTP Strict Transport Security (HSTS) maximum age to 31536000 seconds (one year). This means that after a browser connects to the web interface for the first time, the browser continues to use HTTPS and renews this setting every year.
Crash Reporting	Select to send failed HTTP request data, which can include client and server IP addresses, failed method call tracebacks, and middleware log file contents, to iXsystems.
Usage Collection	Select to enable sending anonymous usage statistics to iXsystems.
Show Console Messages	Select to display console messages in real time at the bottom of the browser.

Localization

The **Localization** widget lets users localize their system to a specific region.

Click Here for More Information

Click **Settings** to open the **Localization Settings** screen.



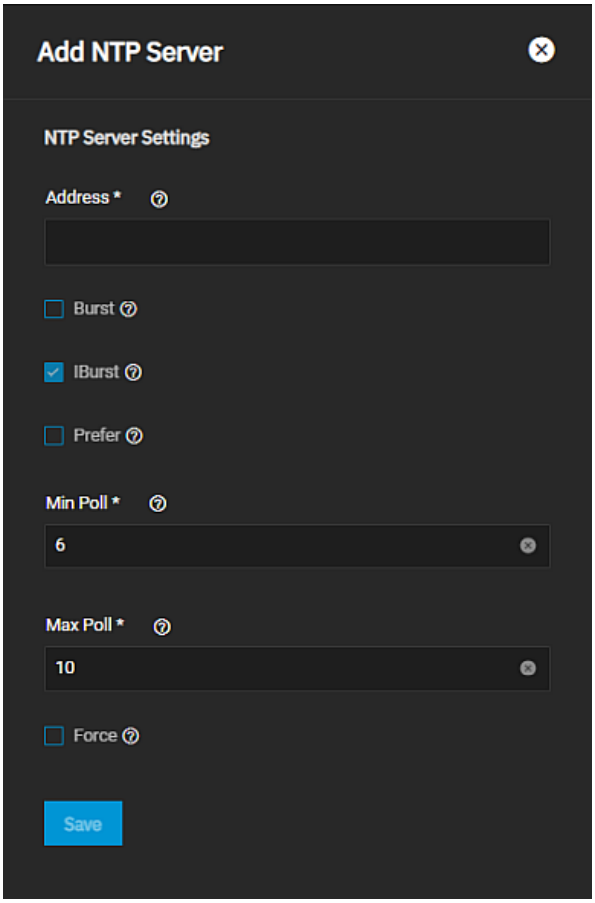
Setting	Description
Language	Select a language from the dropdown list.
Console Keyboard Map	Select a language keyboard layout from the dropdown list.
Timezone	Select a time zone from the dropdown list.
Date Format	Select a date format from the dropdown list.
Time Format	Select a time format from the dropdown list.

NTP Servers

The **NTP Servers** widget allows user to configure Network Time Protocol (NTP) servers, which sync the local system time with an accurate external reference.

Click Here for More Information

By default, new installations use several existing NTP servers. TrueNAS SCALE supports adding custom NTP servers. Click **Add** to open the **Add NTP Server** screen.



Setting	Description
Address	Enter the hostname or IP address of the NTP server.
Burst	Select to use a non-public NTP server. Recommended when **Max Poll** is greater than **10**. Only use on personal NTP servers or those under direct control. Do not enable when using public NTP servers.
IBurst	Select to speed up the initial synchronization (seconds instead of minutes).
Prefer	Select when using a highly accurate NTP servers such as those with time monitoring hardware. Only use for these highly accurate NTP servers.
Min Poll	Enter the minimum polling interval, in seconds, as a power of 2. For example, 6 means 2^6, or 64 seconds. The default is 6, minimum value is 4.
Max Poll	Enter the maximum polling interval, in seconds, as a power of 2. For example, 10 means 2^10, or 1,024 seconds. The default is 10, maximum value is 17.
Force	Select to force the addition of the NTP server, even if it is currently unreachable.

Related Content

- Settings Options
- Web Interface Preference Screen
- Getting Support
- Managing Advanced Settings
- Managing Cron Jobs
- Managing the Console Setup Menu
- Managing the System Configuration
- Managing General Settings
- Managing System Logging

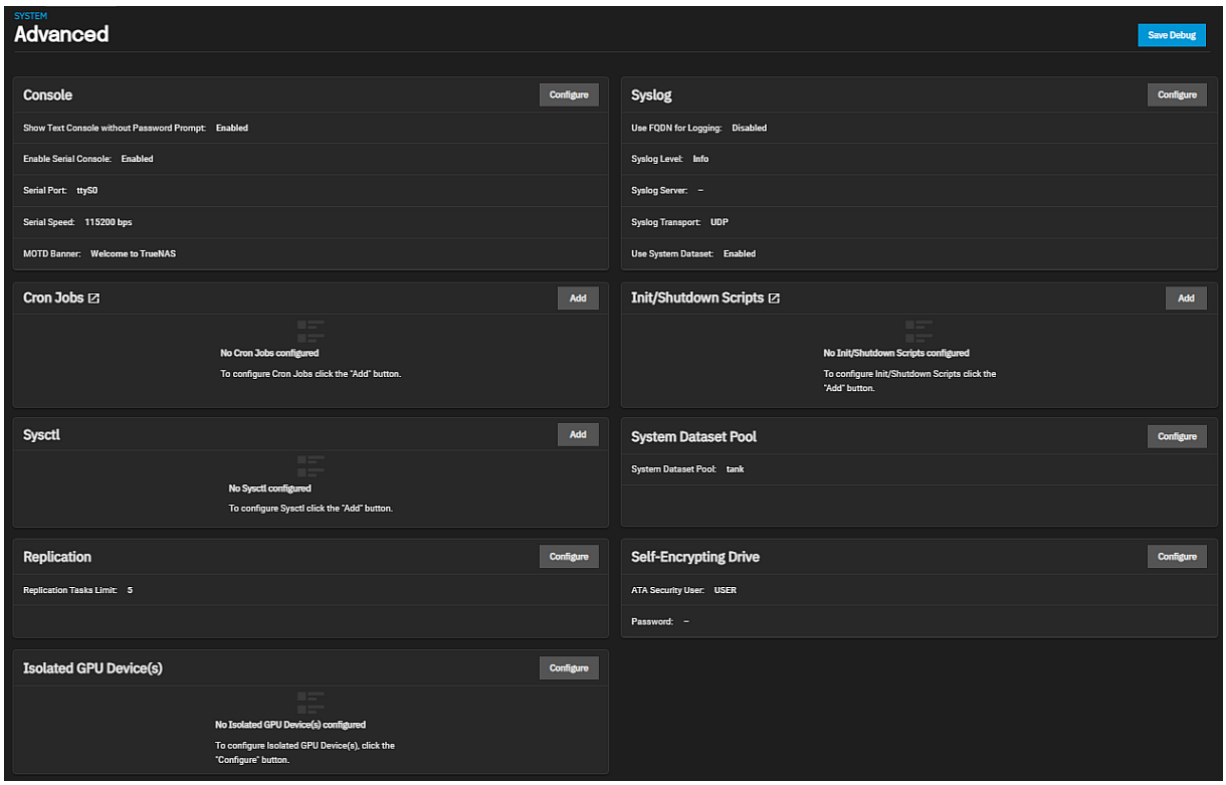
Related Console Articles

- Managing the Console Setup Menu
- Console Setup Menu Configuration
- Advanced Settings Screen

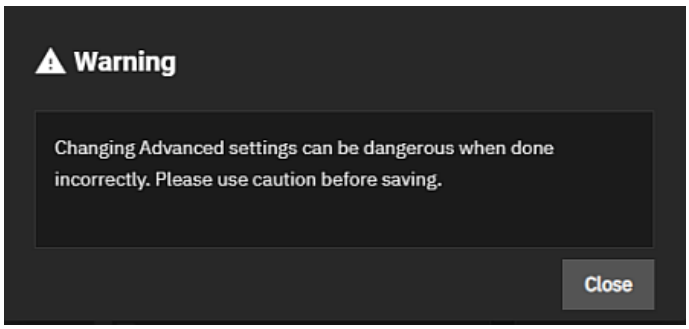
4.11.3 - Advanced Settings Screen

This article provides information on the **System > Advanced** screen widgets and configuration screen settings.

TrueNAS SCALE advanced settings screen provides configuration options for the console, syslog, sysctl, replication, cron jobs, init/shutdown scripts, system dataset pool, isolated GPU device(s), and self-encrypting drives.



> Advanced settings have reasonable defaults in place. A warning message displays for some settings advising of the dangers making changes. Changing advanced settings can be dangerous when done incorrectly. Use caution before saving changes.

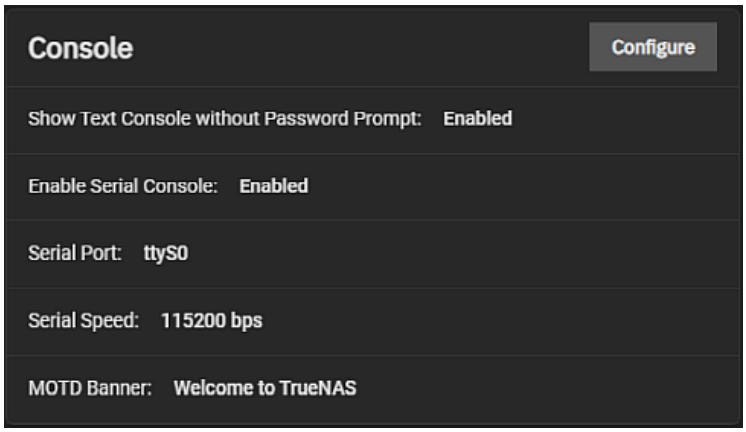


> Make sure you are comfortable with ZFS, Linux, and system configuration backup and restoration before making any changes.

Save Debug saves a system debug file as a downloaded file on your system.

Console Widget

The **Console** widget on the **System Setting > Advanced** screen displays current console settings for TrueNAS.

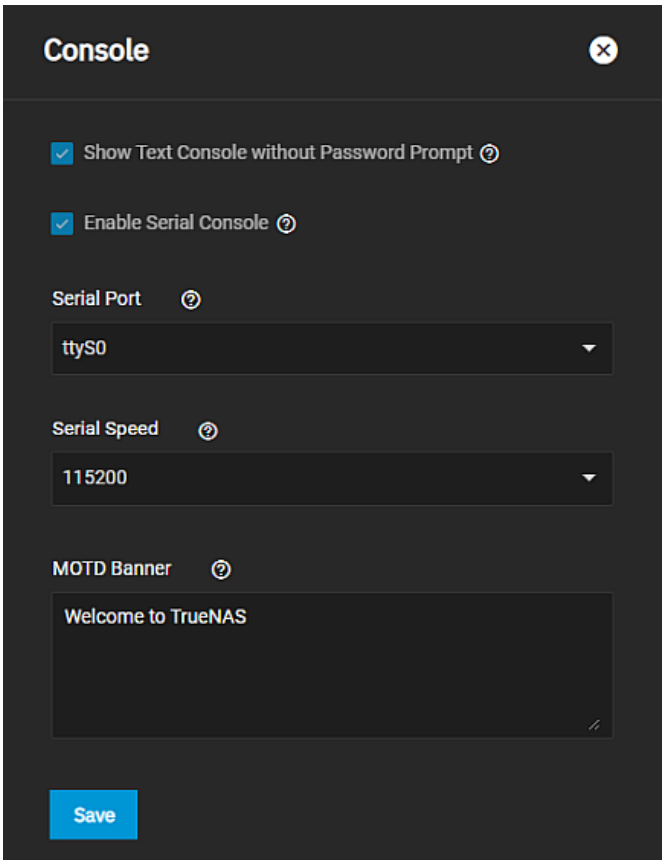


Configure opens the **Console** configuration screen.

Console Configuration Screen

Console settings configure how the Console setup menu displays, the serial port it uses and the speed of the port, and the banner users see when it is accessed.

Click Here for More Information

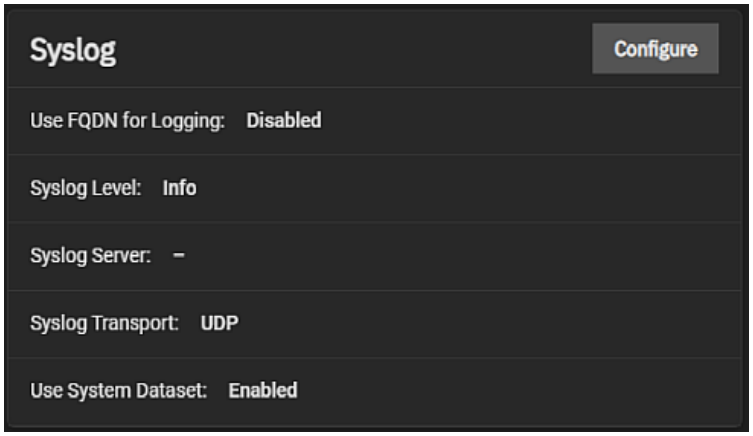


Settings	Description
Show Text Console without Password Prompt	Select to display the console without being prompted to enter a password. Leave clear to add a login prompt to the system before showing the console menu.

Settings	Description
Enable Serial Console	Select to enable the serial console. Do not select this if the serial port is disabled.
Serial Port	Enter the serial console port address.
Serial Speed	Select the speed (in bits per second) the serial port uses from the dropdown list. Options are 9600, 19200, 38400, 57600 or 115200.
MOTD Banner	Enter the message you want to display when a user logs in with SSH.

Syslog Widget

The **Syslog** widget displays the existing system logging settings that specify how and when the system sends log messages to the syslog server.

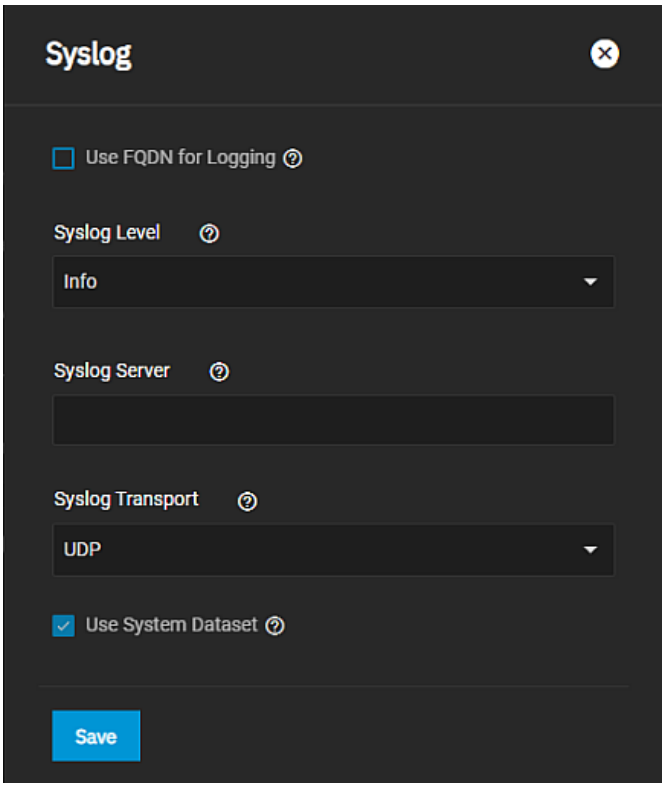


Configure opens the **Syslog** configuration screen.

SysLog Configuration Screen

The **Syslog** configuration screen settings specify the logging level the system uses to record system events, the syslog server DNS host name or IP, the transport protocol it uses, and if using TLS, the certificate and certificate authority (CA) for that server, and finally if it uses the system dataset to store the logs.

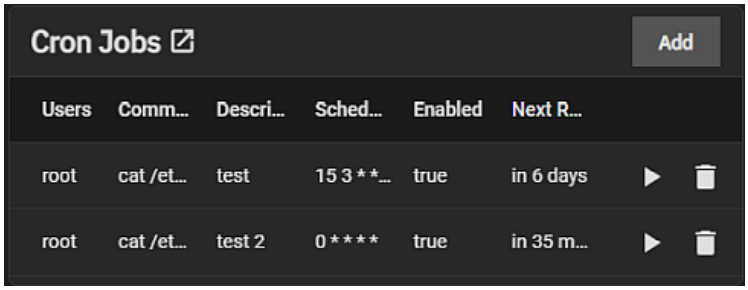
Click Here for More Information



Settings	Description
Use FQDN for Logging	Select to include the fully-qualified domain name (FQDN) in logs to precisely identify systems with similar host names.
Syslog Level	Select the logging level the syslog server uses when creating system logs; the system only sends logs matching this level.
Syslog Server	Enter the remote syslog server DNS host name or IP address. add a colon and the port number to the host name to use non-standard port numbers, like *mysyslogserver:1928*. Log entries are written to local logs and sent to the remote syslog server.
Syslog Transport	Enter the transport protocol for the remote system log server connection. Selecting Transport Layer Security (TLS) displays the **Syslog TLS Certificate** and **Syslog TSL Certificate Authority** fields. This requires preconfiguring both the system certificate and the certificate authority (CA) for the server.
Syslog TLS Certificate	Displays after selecting **TLS** in **Syslog Transport**. Select the transport protocol for the remote system log server TLS certificate from the dropdown list. Select either the default, or add the certificate and CA for the server using the **Credentials > Certificates** screen **Certificates** widget.
Syslog TLS Certificate Authority	Displays after selecting **TLS** in **Syslog Transport**. Select the TLS CA for the TLS server from the dropdown list. If not using the default, create the CA for the systlog server TLS certificate on the **Credentials > Certificates > Certificate Authorities** screen.
Use System Dataset	Select to store system logs on the system dataset. Leave clear to store system logs in `/var/` on the operating system device.

Cron Jobs Widget

The **Cron Jobs** widget displays **No Cron Jobs configured** until you add a cron job, then it displays information on cron job(s) configured on the system.

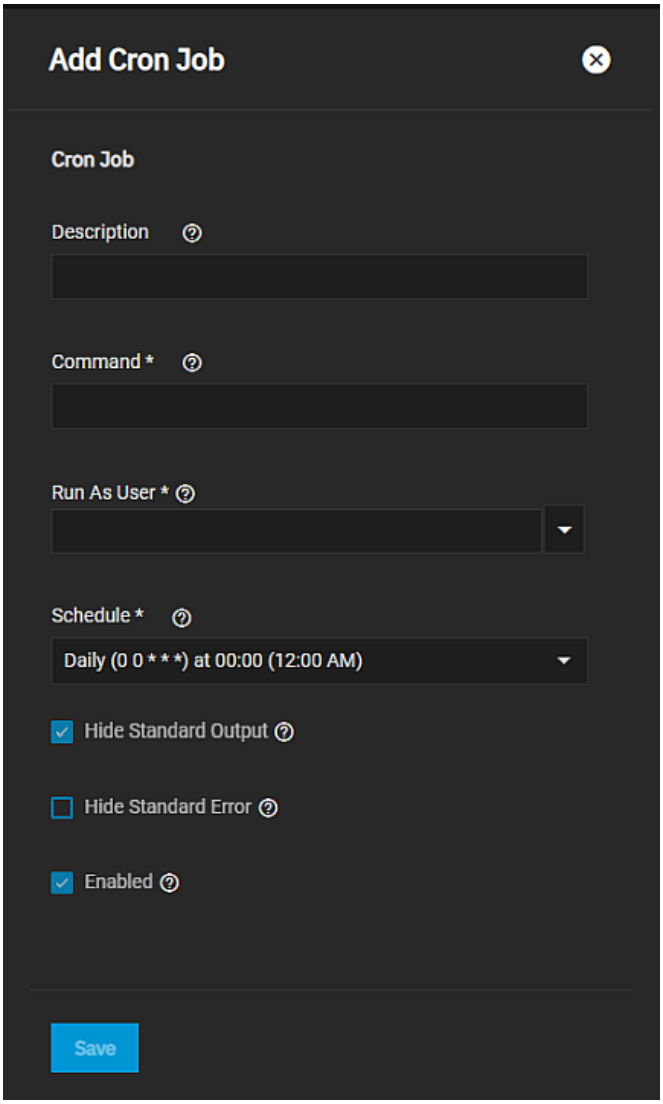


Add opens the **Add Cron Job configuration screen. Click on any job listed in the widget to open the **Edit Cron Jobs configuration screen populated with the settings for that cron job.

Add or Edit Cron Job Configuration Screen

The **Add Cron Job** and **Edit Cron Job** configuration screens display the same settings. **Cron Jobs** lets users configure jobs that run specific commands or scripts on a regular schedule using cron(8). Cron Jobs help users run repetitive tasks.

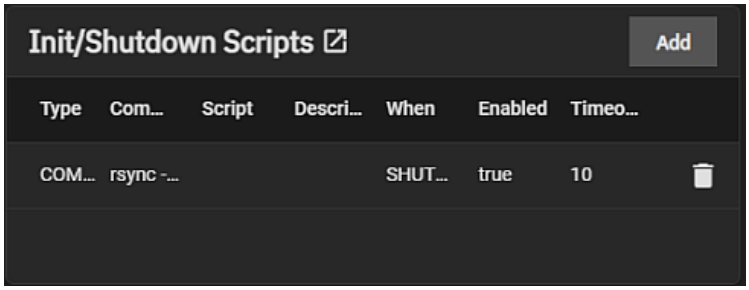
Click Here for More Information



Settings	Description
Description	Enter a description for the cron job.
Command	Enter the full path to the command or script to run. For example, a command string to create a list of users on the system and write that list to a file enter `cat /etc/passwd > users_$(date +%F).txt`.
Run As User	Select a user account to run the command. The user must have permissions allowing them to run the command or script.
Schedule	Select a schedule preset or choose **Custom** to open the advanced scheduler. Note that an in-progress cron task postpones any later scheduled instance of the same task until the running task is complete.
Hide Standard Output	Select to hide standard output (stdout) from the command. If left cleared, TrueNAS mails any standard output to the user account cron that ran the command.
Hide Standard Error	Select to hide error output (stderr) from the command. If left cleared, TrueNAS mails any error output to the user account cron that ran the command.
Enabled	Select to enable this cron job. Leave cleared to disable the cron job without deleting it.

Init/Shutdown Scripts Widget

The **Init/Shutdown Scripts** widget displays **No Init/Shutdown Scripts configured** until you add either a command or script, then the widget lists the scrips configured on the system.

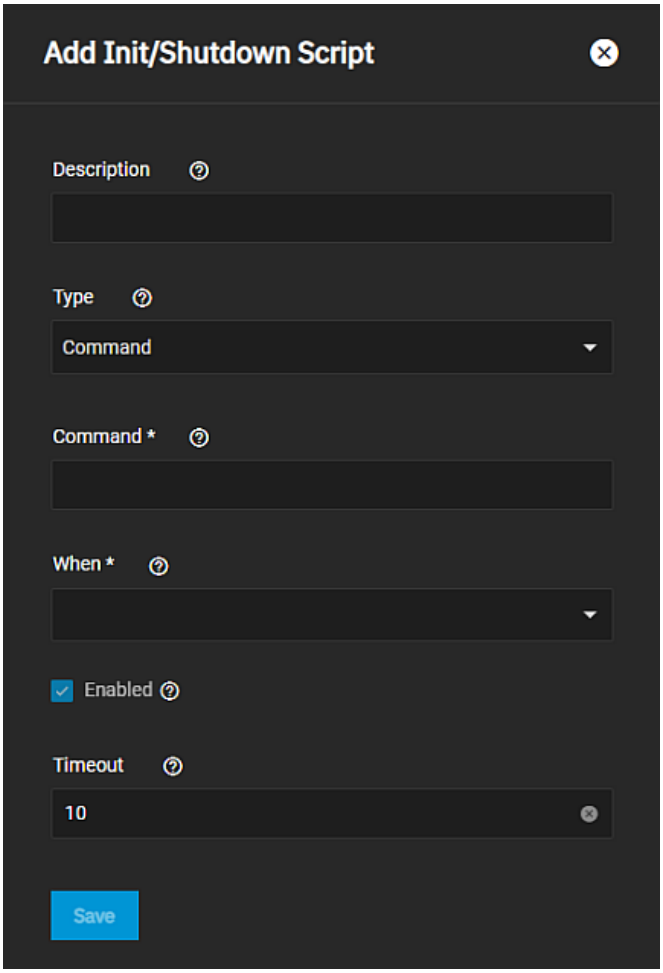


Add opens the **Add Init/Shutdown Script** configuration screen. Any script listed is a link that opens the **Edit Init/Shutdown Script** configuration screen populated with the settings for that script.

Add or Edit Init/Shutdown Script Configuration Screens

Init/Shutdown Scripts lets users schedule commands or scripts to run at system startup or shutdown.

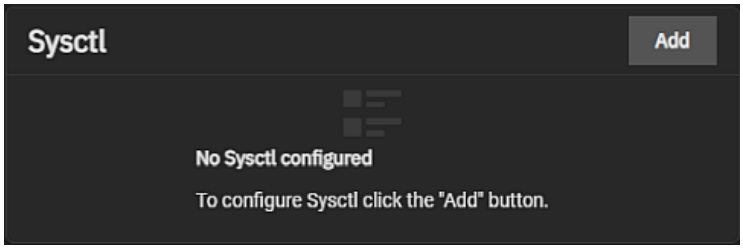
Click Here for More Information



Settings	Description
Description	Comments about this script.
Type	Select Command for an executable or Script for an executable script.
Command	Enter the command with any options.
Script	Select the script. The script runs using dash(1).
When	Select when the command or script runs from the dropdown list. Options are **Pre Init** for early in the boot process, after mounting file systems and starting networking. **Post Init** runs at the end of the boot process, before Linux services start. **Shutdown** runs during the system power-off process.
Enabled	Select to enable this script. When left cleared, it disables the script without deleting it.
Timeout	Automatically stop the script or command after the specified number of seconds.

Sysctl Widget

The **Sysctl** widget displays either **No Sysctl configured** or the existing sysctl settings on the system.

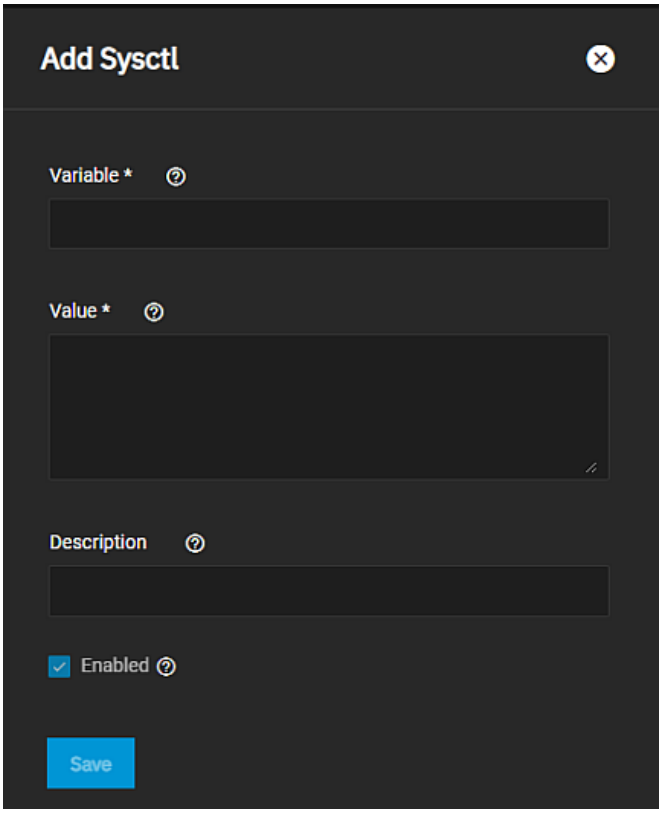


Add to add a tunable that configures a kernel module parameter at runtime.

Add or Edit Sysctl Configuration Screen

The **Add Sysctl** or **Edit Sysctl** configuration screen settings lets users set up tunables that configure kernel parameters at runtime.

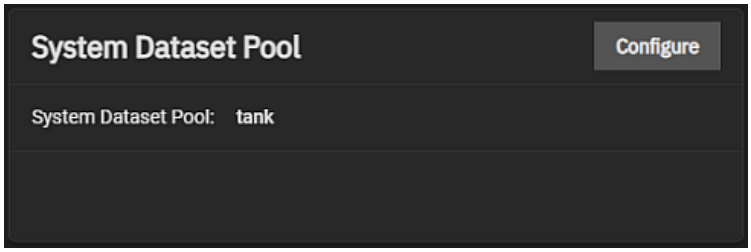
Click Here for More Information



Settings	Description
Variable	Enter the name of the sysctl variable to configure. sysctl tunables are used to configure kernel parameters while the system is running and generally take effect immediately.
Value	Enter a sysctl value to use for the loader, **sysctl** variable.
Description	Enter a description for the tunable.
Enabled	Select to enable this tunable. Leave clear to disable this tunable without deleting it.

System Dataset Pool Widget

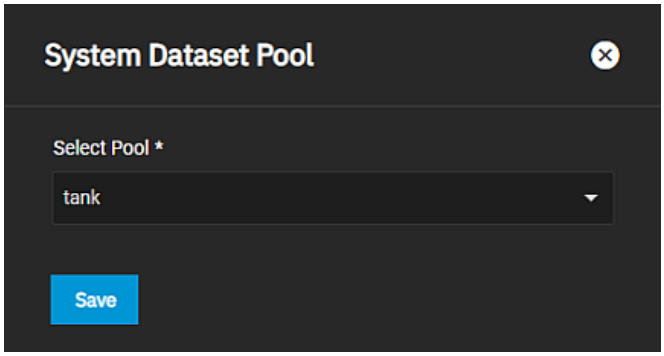
System Dataset Pool widget displays the pool configured as the system dataset pool. The widget allows users to select the storage pool they want to hold the system dataset. The system dataset stores debugging core files, encryption keys for encrypted pools, and Samba4 metadata, such as the user and group cache and share level permissions.



Configure opens the **System Dataset Pool** configuration screen.

System Dataset Pool Configuration Screen

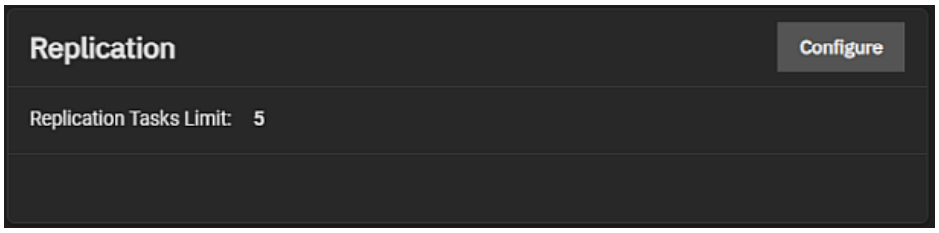
If the system has one pool, TrueNAS configures that pool as the system dataset pool. If your system has more than one pool, you can select the system dataset pool from the dropdown list of available pools. Users can move the system dataset to unencrypted pools or encrypted pools without passphrases.



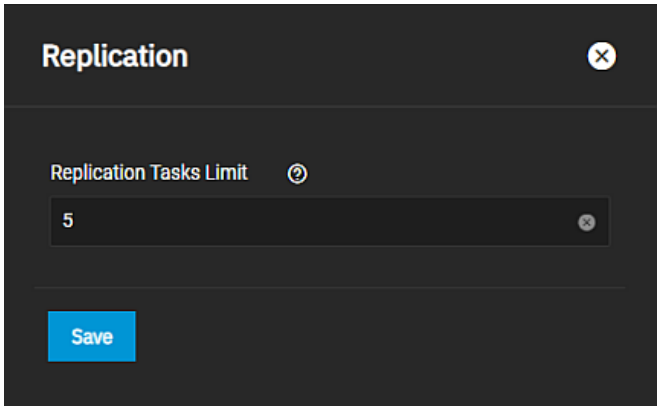
Users can move the system dataset to a key-encrypted pool, but cannot change the pool encryption type afterward. If the encrypted pool already has a passphrase set, you cannot move the system dataset to that pool.

Replication

The **Replication** widget displays the number of replication tasks that can execute simultaneously configured on the system. It allows users to adjust the maximum number of replication tasks the system can execute simultaneously.



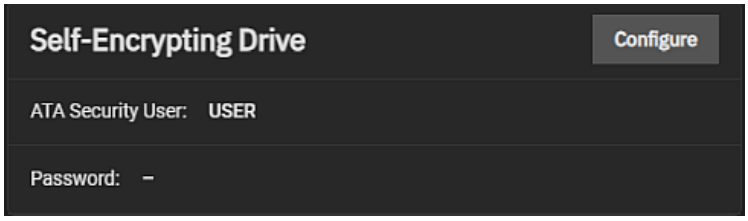
Click **Configure** to open the **Replication** configuration screen.



Enter a number for the maximum number of simultaneous replication tasks you want to allow the system to process and click **Save**.

Self-Encrypting Drive

The **Self-Encrypting Drive** (SED) widget displays the ATA security user and password configured on the system.

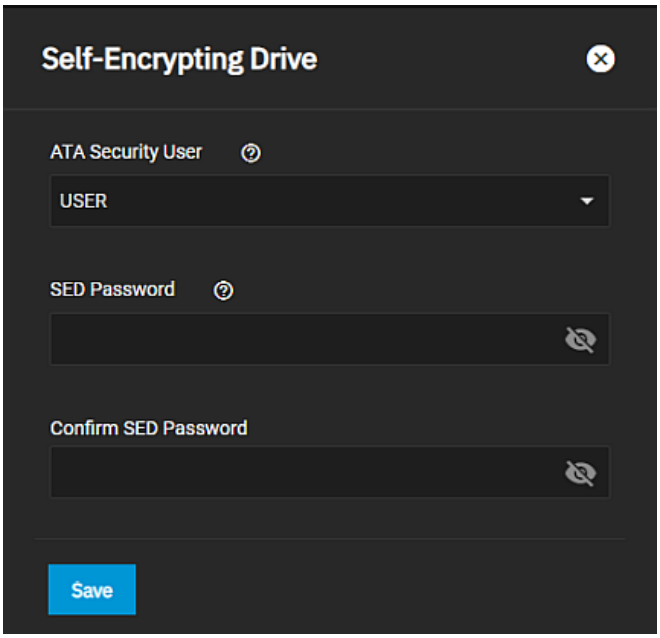


Configure opens the **Self-Encrypting Drive** configuration screen.

Self-Encrypting Drive Configuration Screen

The **Self-Encrypting Drive** configuration screen allows users set the ATA security user and create a SED global password.

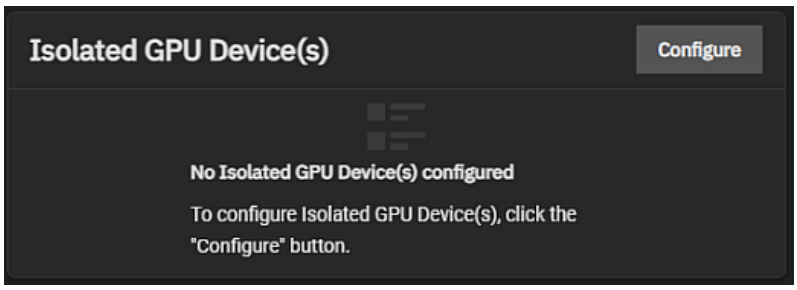
Click Here for More Information



Settings	Description
ATA Security User	Select the user passed to camcontrol security -u to unlock SEDs from the dropdown list. Options are **USER** or **MASTER**.
SED Password	Enter the global password to unlock SEDs.
Confirm SED Password	Re-enter the global password to unlock SEDs.

Isolated GPU Device(s)

The **Isolated GPU Device(s)** widget displays an graphics processing unit (GPU) device(s) configured on your system.



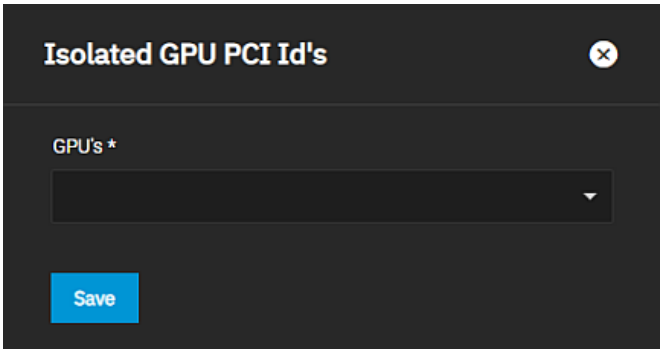
Configure opens the **Isolate GPU PCI's ID** screen that allows users to isolate additional GPU devices for GPU passthrough.

Isolate GPU PCI's ID Configuration Screen

The **Isolate GPU PCI's ID** configuration screen allows you to add GPU devices to your system.

Click Here for More Information

GPU passthrough allows the TrueNAS SCALE kernel to directly present an internal PCI GPU to a virtual machine (VM).



The GPU device acts like the VM is driving it, and the VM detects the GPU as if it is physically connected. Select the GPU device ID from the dropdown list. To isolate a GPU you must have at least two in your system; one allocated to the host system for system functions and the other available to isolate for use by a VM or application. Isolating the GPU prevents apps and the system from accessing it.

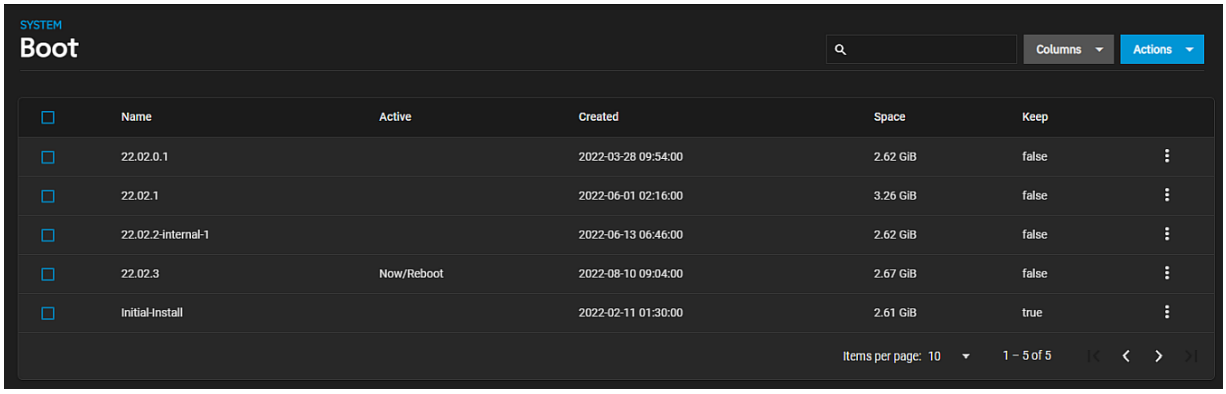
Related Content

- Settings Options
- Web Interface Preference Screen
- Getting Support
- Managing Advanced Settings
- Managing Cron Jobs
- Managing the Console Setup Menu
- Managing the System Configuration
- General Settings Screen
- Managing General Settings
- Managing System Logging

4.11.4 - System Boot Screens

This article provides information on the boot environment screens and settings.

The **System > Boot** screen displays a list of boot environments on the TrueNAS system. Each time the system updates to a new software release it creates a new boot environment.

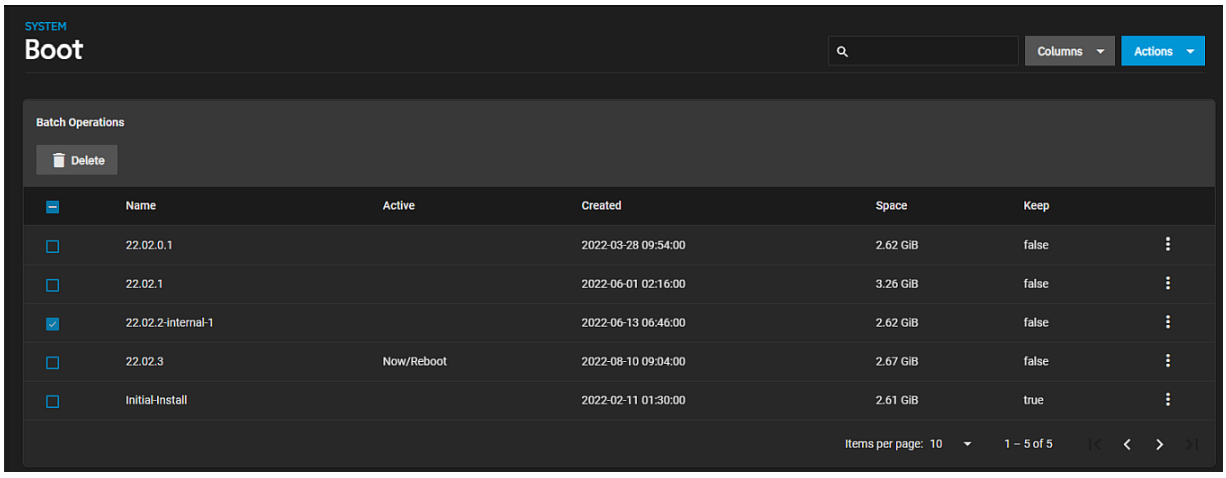


Each boot environment on the list includes:

- **Name** which is the name of the boot entry as it appears in the boot menu
- **Active** that indicates which entry boots by default if a boot environment is not active. Activated environment displays **Non/Reboot**.
- **Created** that shows creation date and time, **Space** that shows boot environment size
- **Keep** that indicates whether TrueNAS deletes this boot environment when a system update does not have enough space to proceed.

Batch Operations

Select the checkbox(es) for each boot environment displays the **Batch Operations** that allows you to delete the selected environments at one time.



The ⋮ displays a list of boot environment actions that change based on whether it is activated or not.

Boot Environment Actions Lists

The ⋮ for an environment displays actions available to that environment.

Action	Boot State	Description
Activate	Deactivated	Opens the **Activate** dialog. Changes the **System Boot** screen status to **Reboot** and changes the current **Active** entry from **Now/Reboot** to **Now**, indicating that it is the current boot environment but is not used on next boot.

Action	Boot State	Description
Clone	Both states	Opens the **Clone Boot Environment** window. Copies the selected boot environment into a new entry. Enter a new name using only alphanumeric characters, and/or the allowed dashes (-), underscores (_), and periods (.) characters.
Delete	Deactivated	Opens the **Delete** dialog. Does not display if the boot environment is activated/ You cannot deleted the default or activated boot environment. Removes the highlighted entry and also removes that entry from the boot menu.
Rename	Both states	Opens the **Rename Boot Environment** window. Enter a new name using only alphanumeric characters, and/or the allowed dashes (-), underscores (_), and periods (.) characters.
Keep	If set to false	Opens the **Keep** dialog, and toggles the boot environment action to **Unkeep**. Use to prevent the TrueNAS updater from automatically deleting the environment to make more space for a new environment when there is insufficient space for it.
Unkeep	If **Keep** is set to **True**	Opens the **Unkeep** dialog, and toggles the boot environment action to **Keep**. Use to allow TrueNAS updater to automatically delete the environment to make space for a new boot environment when there is not enough space for it.

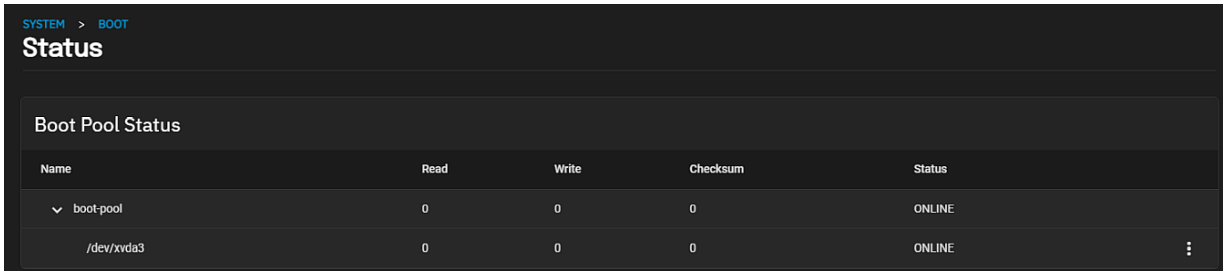
System Boot Actions

ACTIONS at the top right corner of the **System > Boot** screen displays four options.

Setting	Description
Add	Opens the **Create Boot Environment** window where you make a new boot environment from the active environment. Enter a new name using only alphanumeric characters, and/or the allowed dashes (-), underscores (_), and periods (.) characters.
Stats/Settings	Opens the **Stats/Settings** window with the **Boot pool Condition**, **Size** and **Used**, and **Last Scrub Run** statistics for the operating system device, and provides the option to change the default duration between the operating system device scrubs from every 7 days to a new duration in days.
Boot Pool Status	Opens the **Boot Pool Status** screen that displays the status of each device in the operating system device (boot pool), and lists any read, write, or checksum errors.
Scrub Boot Pool	Opens the **Scrub** dialog. Performs a manual data integrity check (scrub) of the operating system device.

Boot Pool Status Screen

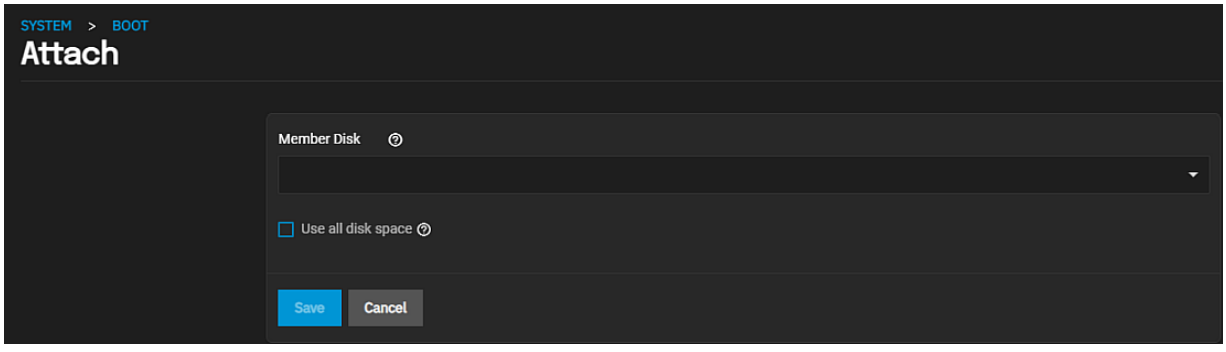
The **System > Boot > Status** screen shows the **Boot Pool Status** of the current **boot-pool**. It includes the current status, the path, and the number of read, write and checksum errors.



The ⋮ displays two options, **Attach** or **Replace**.

Attach Screen

The boot status **Attach** screen settings specify a device as the disk member and how much of the device is used.



Select a device from the **Member Disk** dropdown.

Select **Use all disk space** to use the entire capacity of the new device.

Replace Screen

Replace settings specify a replacement device from the **Member Disk** dropdown

To return to the **System > Boot** screen, click **Boot** in the breadcrumb header.

Related Content

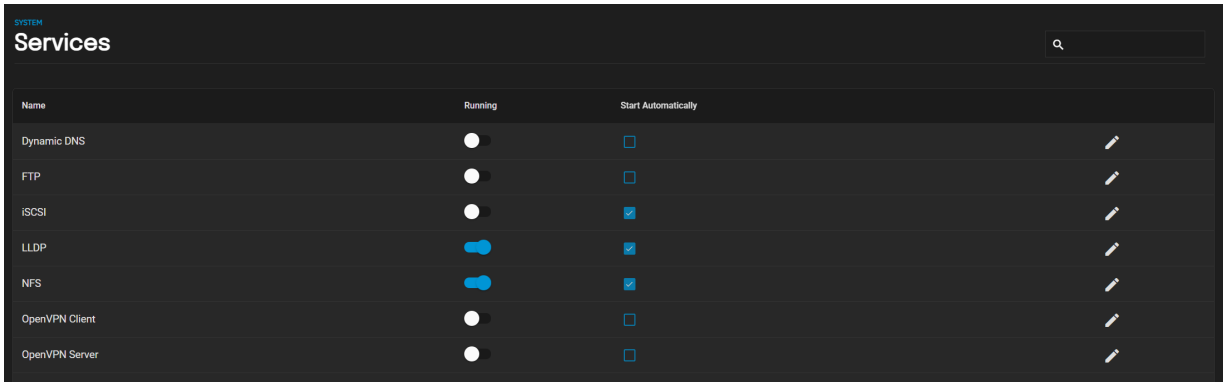
- Managing Boot Environments

4.11.5 - Services

This article provides general information on the **Services** screen, and a summary of each indiviual service article in the Services area.

System Settings > Services displays each system component that runs continuously in the background. These typically control data-sharing or other external access to the system. Individual services have configuration screens and activation toggles, and you can set them to run automatically.

Documented services related to data sharing or automated tasks are in their respective Shares and Tasks articles.



Use the **Configure** icon to open the service configuration screen.

Select **Start Automatically** to set the service to start after the system reboots.

Click on the **Running** toggle to start the service or to stop it if it is running. Stop services before changing configuration settings.

Article Summaries

- Dynamic DNS Service Screen

  This article provides information on Dynamic DNS screen settings.

- FTP Service Screen

  This article provides information on the FTP services screens and settings.

- LLDP Services Screen

  This article provides information on the LLDP service settings.

- NFS Services Screen

  This article provides information on NFS service screen and settings.

- OpenVPN Screens

  This article provides information on OpenVPN client and server screens and settings.

- Rsync Services Screen

  This article provides information on the rsync services screens and settings.

- S.M.A.R.T. Service Screen

  This article provides information on S.M.A.R.T. service screen settings.

- S3 Service Screen

  This article provides information on the the S3 service screen settings.

- SMB Service Screen

  This article provides information in the SMB service screen and settings.

- SNMP Service Screen

  This article provides information on SNMP service screen settings.

- SSH Service Screen

  This article provides information on the SSH service screens and settings.

- TFTP Services Screen

  This article provides information on the TFTP screen settings.

- UPS Services Screen

  This article provides information on the UPS service screen settings.

- WebDAV Service Screen

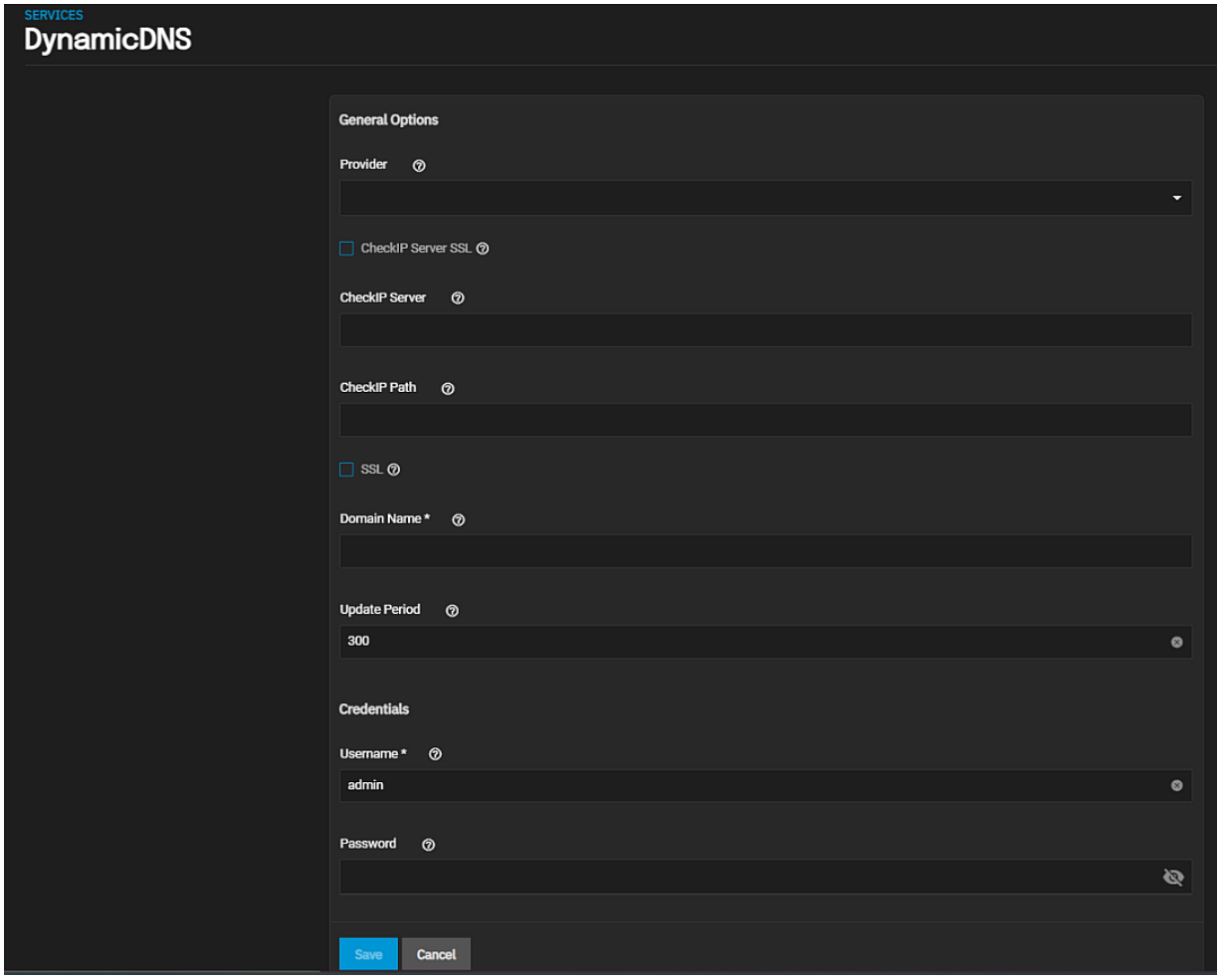
  This article provides information on WebDAV service screen and settings.

4.11.5.1 - Dynamic DNS Service Screen

This article provides information on Dynamic DNS screen settings.

The **Services > DynamicDNS** screen settings specify settings so the system can automatically associate its current IP address with a domain name and continues to provide access to TrueNAS even if the system IP address changes.

To configure Dynamic DNS, go to **System Settings > Services** and find **DynamicDNS**, then click .



Settings	Description
Provider	Select the provider from the dropdown list of supported providers. If a specific provider is not listed, select **Custom Provider** and enter the information in the **Custom Server** and **Custom Path** fields below the **SSL** checkbox.
Custom Server	Displays after selecting **Custom Provider** in the **Provider** field. Enter the DDNS server name. For example, *members.dyndns.org* denotes a server similar to dyndns.org.
Custom Path	Displays after selecting **Custom Provider** in the **Provider** field. Enter the DDNS server path. Paht syntax can vary by provider and must be obtained from that provider. For example, */update?hostname=* is a simple path for the update.twodns.de custom sever. The host name is automatically appended by default. For more examples see In-A-Dyn documentation.
CheckIP-Server SSL	Select to use HTTPS for the connection to the CheckIP Server.
CheckIP Server	Enter the name and port of the server that reports the external IP address. For example, entering *checkip.dyndns.org:80* uses Dyn IP detection to discover the remote socket IP address.
CheckIP Path	Enter the path to the CheckIP server. For example, *no-ip.com* uses a CheckIP Server of *dynamic.zoneedit.com* and CheckIP Path of */checkip.html*.
SSL	Select to use HTTPS for the connection to the server that updates the DNS record.
Domain Name	Enter the fully qualified domain name of the host with the dynamic IP address. Separate multiple domains with a space, comma (,), or semicolon (;). For example, *myname.dyndns.org; myothername.dyndns.org*.

Settings	Description
Update Period	Enter the number of seconds for how often the IP is checked.

Credentials

Settings	Description
Username	Enter the user name for logging in to the provider and updating the record.
Password	Enter the user password for logging in to the provider and updating the record.

Related Content

- Configuring Dynamic DNS Service

4.11.5.2 - FTP Service Screen

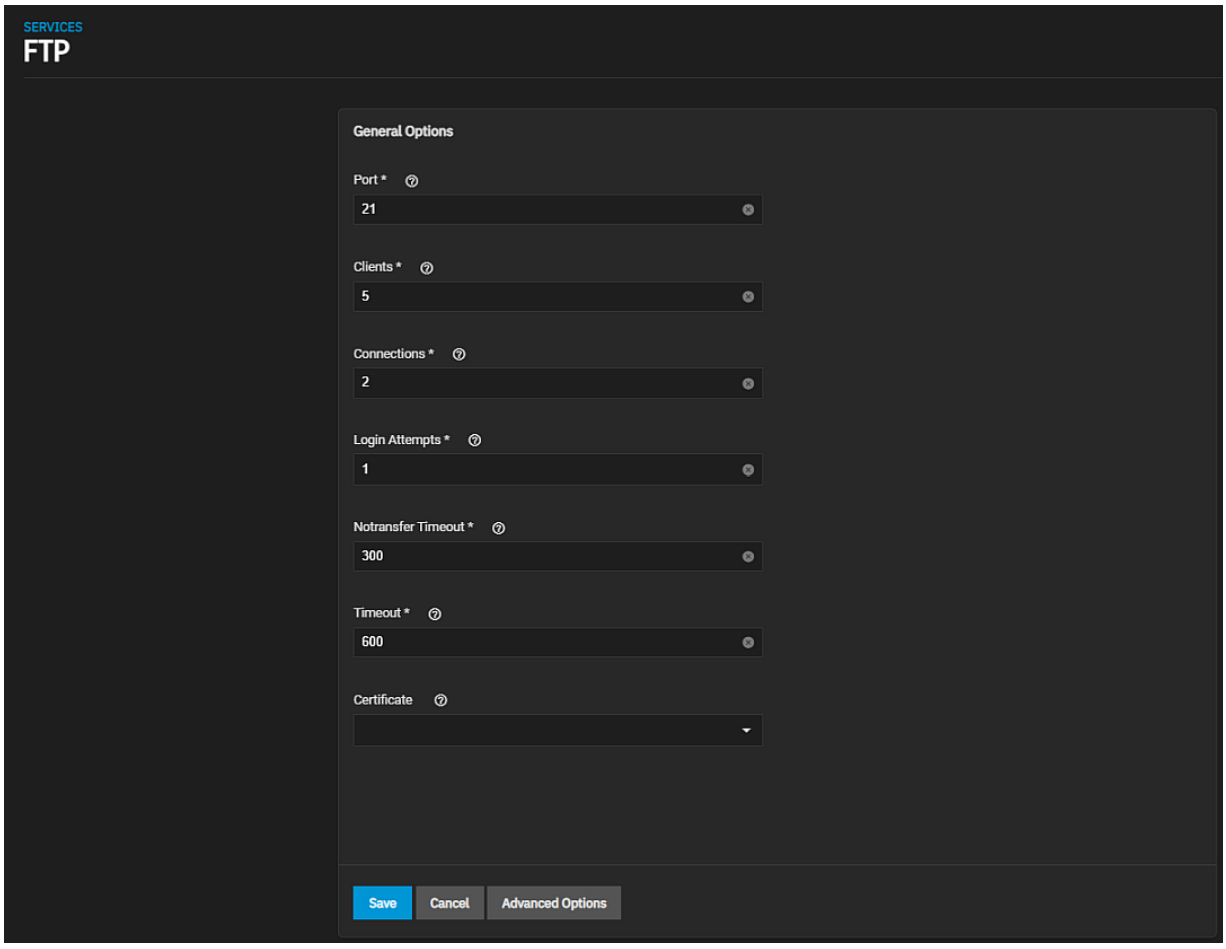
This article provides information on the FTP services screens and settings.

The File Transfer Protocol (FTP) is a simple option for data transfers. The SSH and Trivial FTP options provide secure or simple config file transfer methods respectively.

The **FTP** service has basic and advanced setting options. Click the ✎ for **FTP** to open the **Basic Settings** configuration screen.

FTP Basic Settings

To configure FTP, go to **System Settings > Services** and find **FTP**, then click ✎ .



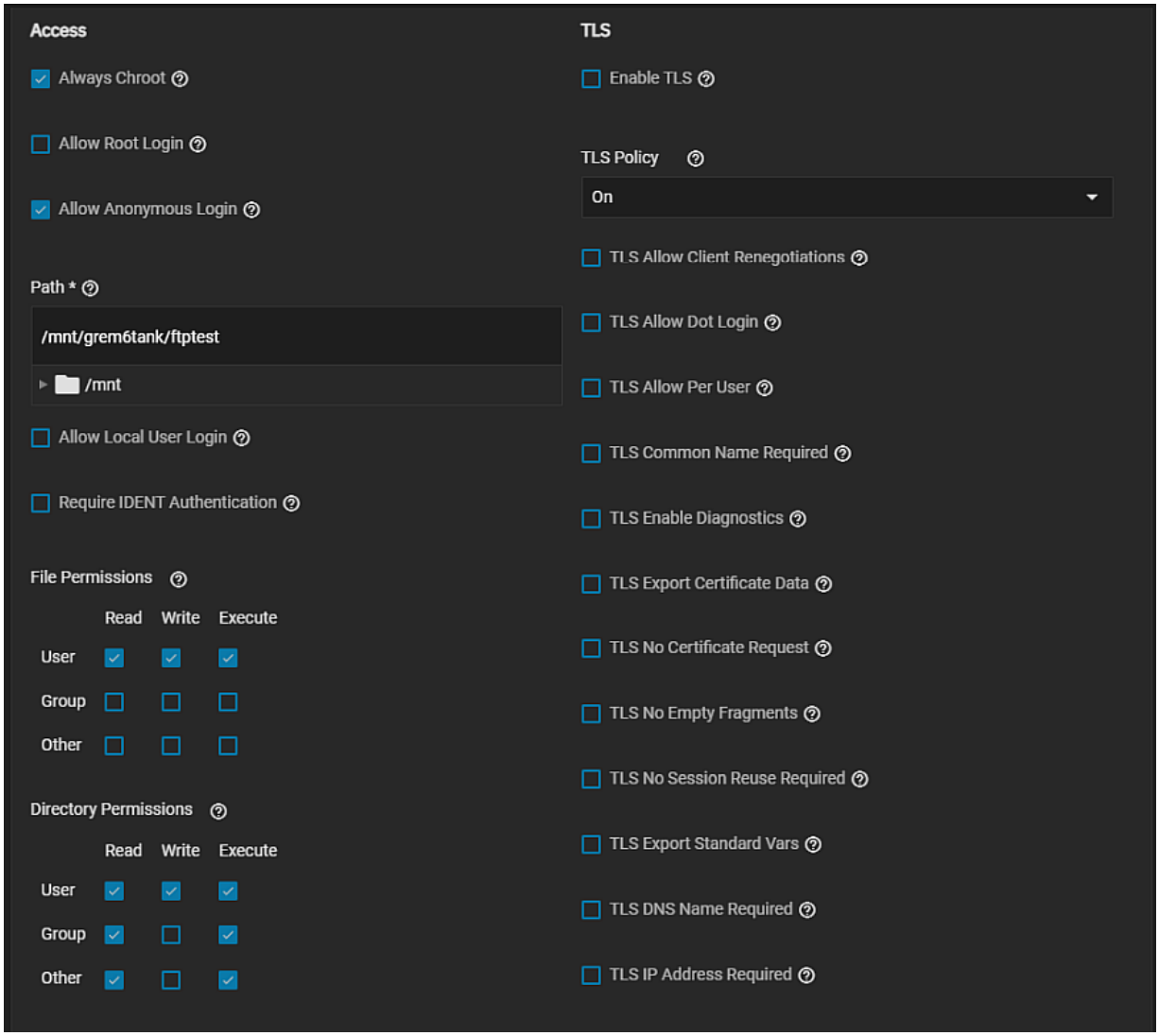
Settings	Description
Port	Enter the port the FTP service listens on.
Clients	Enter the maximum number of simultaneous clients.
Connections	Enter the maximum number of connections per IP address. **0** is unlimited.
Login Attempts	Enter the maximum attempts before client is disconnected. Increase if users are prone to misspellings or typos.
Notransfer Timeout	Enter the maximum number of seconds a client is allowed to spend connected, after authentication, without issuing a command which results in creating an active or passive data connection (i.e. sending/receiving a file, or receiving a directory listing).

Settings	Description
Timeout	Enter the maximum client idle time in seconds before disconnect. Default value is **600** seconds.
Certificate	Select the SSL certificate to use for TLS FTP connections from the dropdown list. To create a certificate, go to **System > Certificates**.

FTP Advanced Settings

Advanced Settings include the **General Options** on the **Basic Settings** configuration screen, and allow you to specify access permissions, TLS settings, bandwidth and other setting to further customize FTP access.

Access and TLS Setting Options



Access Settings

Access settings specify user login, file and directory access permissions.

Settings	Description
Always Chroot	Select to only allow users access their home directory if they are in the **wheel** group. This option increases security risk. To confine FTP sessions to a home directory of a local user, enable **chroot** and select **Allow Local User Login**.
Allow Root Login	Select to allow root logins. This option increases security risk so enabling this is discouraged. Do *not* allow anonymous or root access unless it is necessary.
For better security, enable TLS when possible (especially when exposing FTP to a WAN). TLS effectively makes this FTPS.	

Settings	Description
Allow Anonymous Login	Select to allow anonymous FTP logins with access to the directory specified in **Path**. Selecting this displays the **Path** field. Enter or browse to the loction to populate the field.
Allow Local User Login	Select to allow any local user to log in. By default, only members of the **ftp** group are allowed to log in.
Require IDENT Authentication	Select to require IDENT authentication. Setting this option results in timeouts when ident (or in **Shell** `identd`) is not running on the client.
File Permissions	Select the default permissions for newly created files.
Directory Permissions	Select the default permissions for newly created directories.

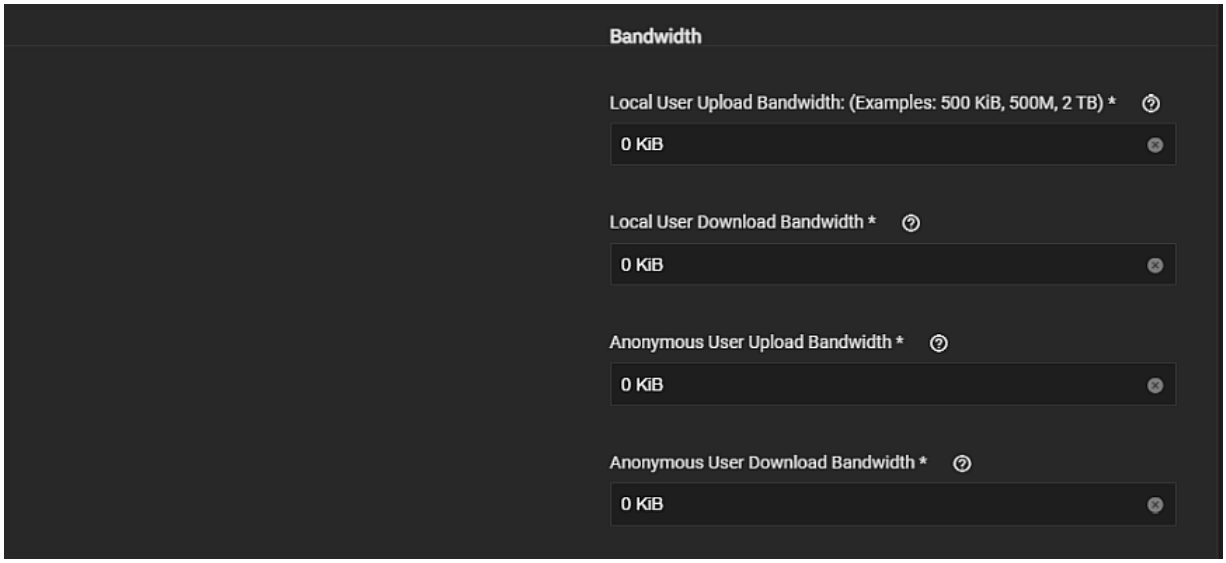
TLS Settings

TLS settings specify the authentication methods you want to apply and whether you want to encrypt the data you transfer across the Internet.

Settings	Description
Enable TLS	Select to allow encrypted connections. Requires a certificate (created or imported using **System > Certificates**.
TLS Policy	Select the policy from the dropdown list of options. Options are **On**, **off**, **Data**, **!Data**, **Auth**, **Ctrl**, **Ctrl + Data**, **Ctrl +!Data**, **Auth + Data** or **Auth +!Data**. Defines whether the control channel, data channel, both channels, or neither channel of an FTP session must occur over SSL/TLS. The policies are described here.
TLS Allow Client Renegotiations	Select to allow client renegotiations. This option is not recommended. Setting this option breaks several security measures. See mod_tls for details.
TLS Allow Dot Login	If select, TrueNAS checks the user home directory for a .tlslogin file containing one or more PEM-encoded certificates. If not found, the user is prompted for password authentication.
TLS Allow Per User	If set, allows sending a user password unencrypted.
TLS Common Name Required	Select to require the common name in the certificate to match the FQDN of the host.
TLS Enable Diagnostics	Selected to logs more verbose, which is helpful when troubleshooting a connection.
TLS Export Certificate Data	Select to export the certificate environment variables.
TLS No Certificate Request	Select if the client cannot connect likely because the client server is poorly handling the server certificate request.
TLS No Empty Fragments	Not recommended. This option bypasses a security mechanism.
TLS No Session Reuse Required	This option reduces connection security. Only use it if the client does not understand reused SSL sessions.
TLS Export Standard Vars	Selected to set several environment variables.
TLS DNS Name Required	Select to require the client DNS name to resolve to its IP address and the cert contain the same DNS name.
TLS IP Address Required	Select to require the client certificate IP address to match the client IP address.

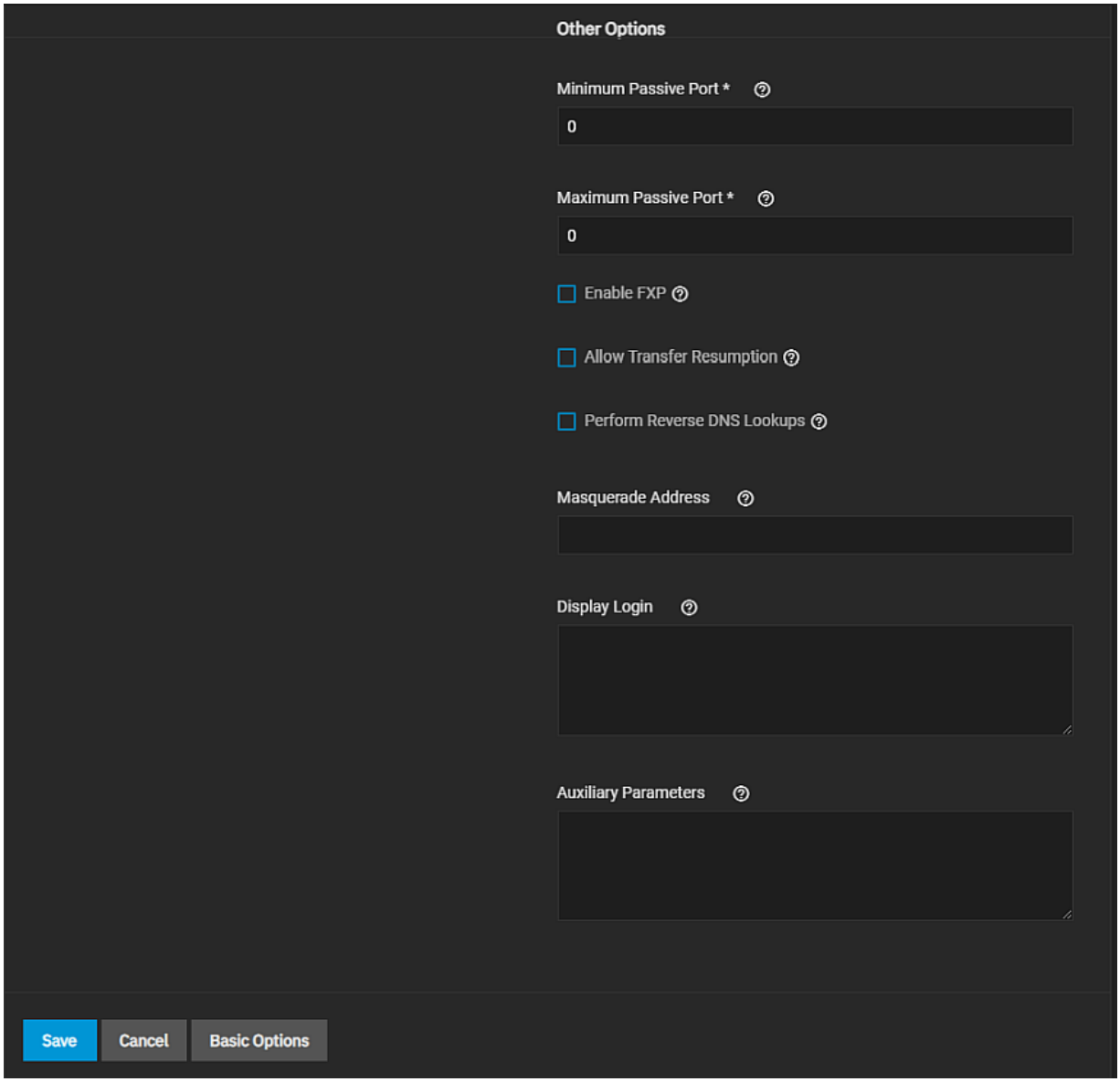
Bandwidth Settings

Bandwidth settings specify the amount of space you want to allocate for local and anonymous user uploads and downloads.



Settings	Description
Local User Upload Bandwidth: (Examples: 500 KiB, 500M, 2 TB)	Enter a value in KiBs or greater. A default of **0 Kib** means unlimited. If measurement is not specified it defaults to KiB. This field accepts human-readable input in KiBs or greater (M, GiB, TB, etc.). Default **0 KiB** is unlimited.
Local User Download Bandwidth	Enter a value in KiBs or greater. A default of **0 Kib** means unlimited. If measurement is not specified it defaults to KiB. This field accepts human-readable input in KiBs or greater (M, GiB, TB, etc.). Default **0 KiB** is unlimited.
Anonymous User Upload Bandwidth	Enter a value in KiBs or greater. A default of **0 Kib** means unlimited. If measurement is not specified it defaults to KiB. This field accepts human-readable input in KiBs or greater (M, GiB, TB, etc.). Default **0 KiB** is unlimited.
Anonymous User Download Bandwidth	Enter a value in KiBs or greater. A default of **0 Kib** means unlimited. If measurement is not specified it defaults to KiB. This field accepts human-readable input in KiBs or greater (M, GiB, TB, etc.). Default **0 KiB** is unlimited.

Other Options



Settings	Description
Minimum Passive Port	Enter a numeric value. Used by clients in PASV mode. A default of **0** means any port above 1023.
Maximum Passive Port	Enter a numeric value. Used by clients in PASV mode. A default of **0** means any port above 1023.
Enable FXP	Select to enable the File eXchange Protocol (FXP). Not recommended as this leaves the server vulnerable to FTP bounce attacks.
Allow Transfer Resumption	Select to allow FTP clients to resume interrupted transfers.
Perform Reverse DNS Lookups	Select to allow performing reverse DNS lookups on client IPs. Causes long delays if reverse DNS isn't configured.
Masquerade Address	Enter a public IP address or host name. Set if FTP clients cannot connect through a NAT device.
Display Login	Enter a message that displays to local login users after authentication. Anonymous login users do not see this message.
Auxiliary Parameters	Used to add additional proftpd(8 parameters.

Related Content

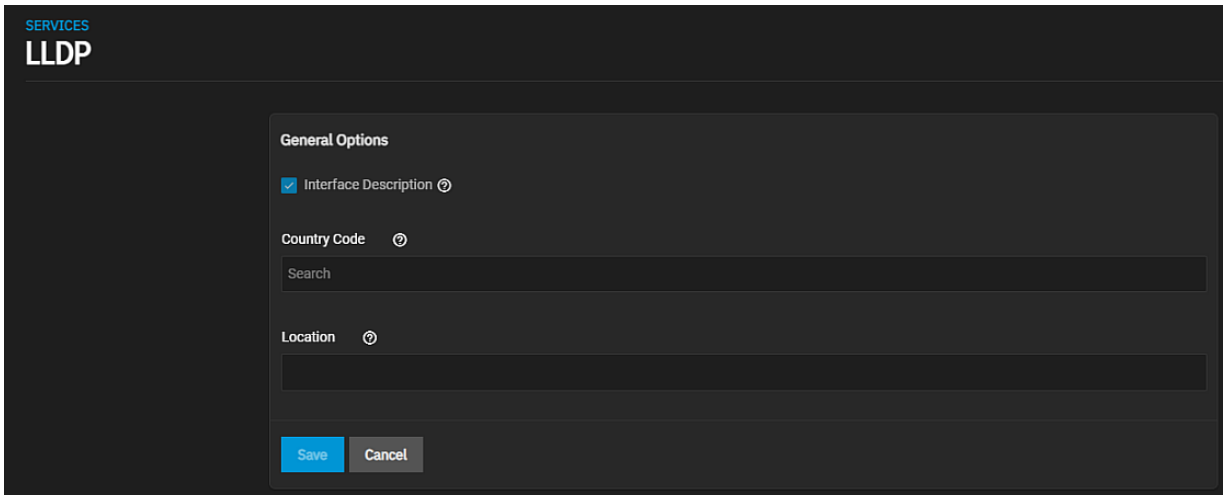
- Configuring FTP Service
- TFTP Services Screen

4.11.5.3 - LLDP Services Screen

This article provides information on the LLDP service settings.

The **Services > LLDP** screen settings specify settings so TrueNAS can advertise itself on the network.

To configure LLDP, go to **System Settings > Services** and find **LLDP**, then click .



Settings	Description
Interface Description	Enables receive mode. Any received peer information is saved in interface descriptions.
County Code	Two-letter ISO 3166-1 alpha-2 code used to enable LLDP location support.
Location	The physical location of the host.

Related Content

- Configuring LLDP Services

4.11.5.4 - NFS Services Screen

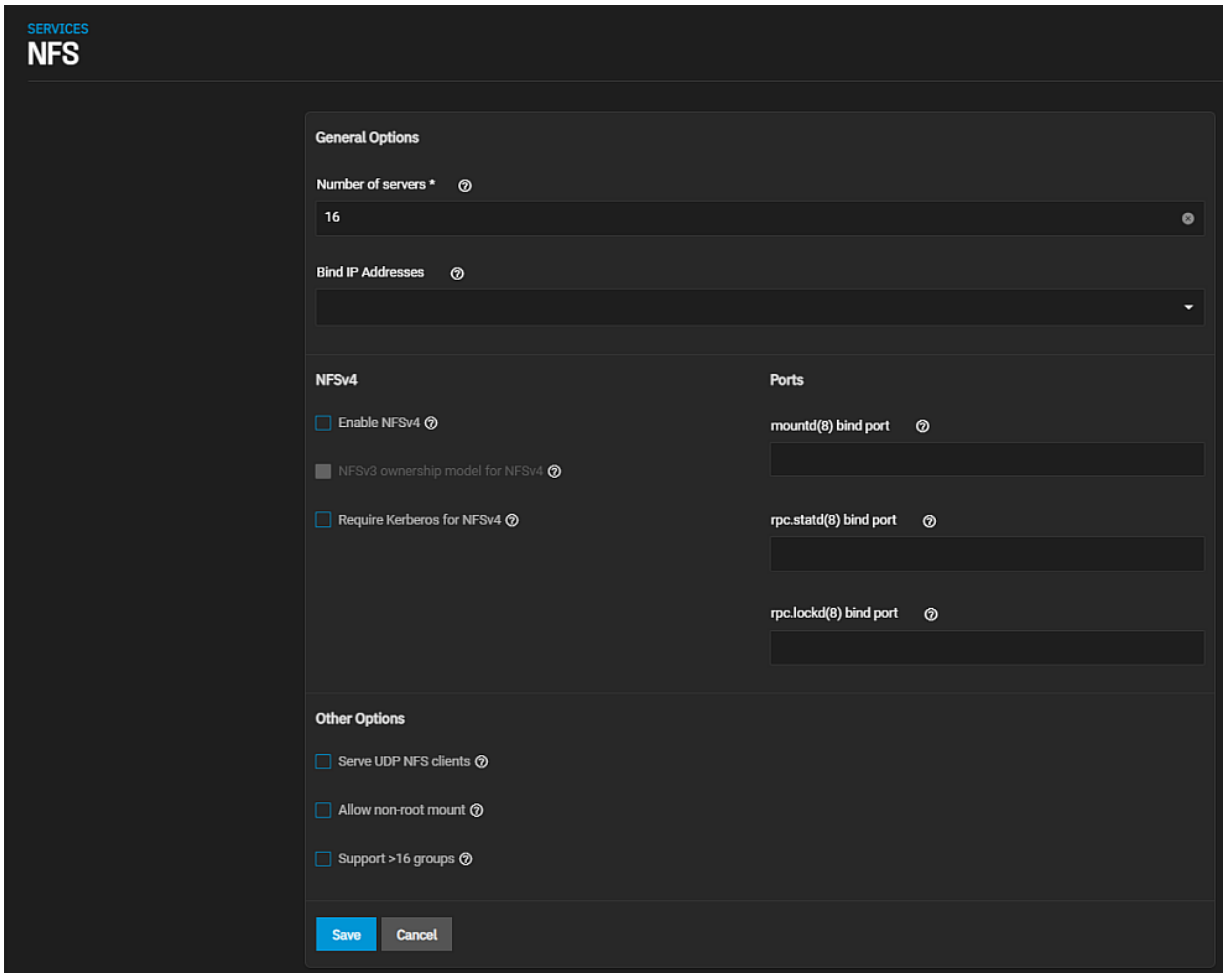
This article provides information on NFS service screen and settings.

NFS Service Screen

The **Services > NFS** configuration screen displays settings to customize the TrueNAS NFS service.

You can access it from **System Settings > Services** screen. Locate **NFS** and click ✎ to open the screen, or use the **Config Service** option on the **Unix (NFS) Share** widget options menu found on the main **Sharing** screen.

Select **Start Automatically** to activate NFS service when TrueNAS boots.



General Options Settings

Setting	Description
Number of servers	Required. Enter the number of servers to create. Increase if NFS client responses are slow. Keep this less than or equal to the number of CPUs reported by `SYSCTL -n kern.smp.cpus` to limit CPU context switching.
Bind IP Addresses	Select IP addresses to listen to for NFS requests. Leave empty for NFS to listen to all available addresses. You must configure static IPs on the interface to appear on the dropdown list.

NFSv4 Settings

Setting	Description
Enable NFSv4	Select to switch from NFSv3 to NFSv4. If selected, **NFSv3 ownership model for NFSv4** clears, allowing you to select or leave it clear.
NFSv3 ownership model for NFSv4	Becomes selectable after selecting **Enable NFSv4**. Select when NFSv4 ACL support is needed without requiring the client and the server to sync users and groups.
Require Kerberos for NFSv4	Select to force NFS shares to fail if the Kerberos ticket is unavailable.

Ports Settings

Setting	Description
mountd(8) bind port	Enter a port to bind mountd(8).
rpc.statd(8) bind port	Enter a port to bind rpc.stad(8).
rpc.lockd(8) bind port	Enter a port to bind rpc.lockd(8).

Other Options Settings

Setting	Description
Serve UDP NFS clients	Select if NFS clients need to use the User Datagram Protocol (UDP).
Support >16 groups	Select when a user is a member of more than 16 groups. This assumes group membership is configured correctly on the NFS server.
Allow non-root mount	Select only if required by the NFS client to allow serving non-root mount requests.

Unless a specific setting is required, we recommend using the default NFS settings.

When TrueNAS is already connected to Active Directory, setting **NFSv4** and **Require Kerberos for NFSv4** also requires a Kerberos Keytab.

Related NFS Articles

- Configuring NFS Service
- NFS Shares Screens
- Adding NFS Shares

4.11.5.5 - OpenVPN Screens

This article provides information on OpenVPN client and server screens and settings.

A virtual private network (VPN) is an extension of a private network over public resources. It lets clients securely connect to a private network even when remotely using a public network. TrueNAS provides OpenVPN as a system-level service to provide VPN server or client functionality. TrueNAS can act as a primary VPN server that allows remote clients to access system data using a single TCP or UDP port. Alternatively, TrueNAS can integrate into a private network, even when the system is in a separate physical location or only has access to publicly visible networks.

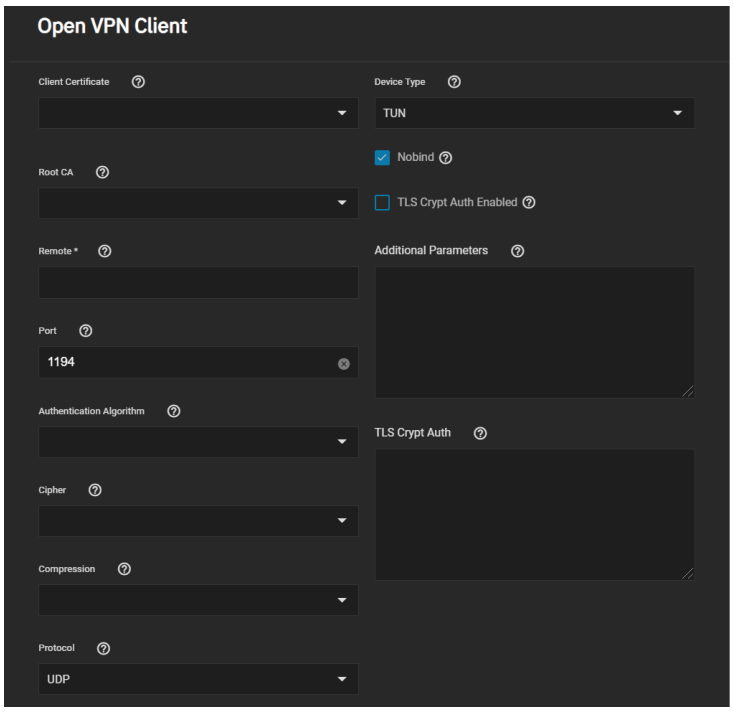
Before configuring TrueNAS as either an OpenVPN server or client, you need an existing public key infrastructure (PKI) with Certificates and Certificate Authorities created in or imported to TrueNAS.

What does this do?
Certificates allow TrueNAS to authenticate with clients or servers by confirming a valid master Certificate Authority (CA) signed the network credentials. To read more about the required PKI for OpenVPN, see the OpenVPN PKI Overview.

In general, configuring TrueNAS OpenVPN (server or client) includes selecting networking credentials, setting connection details, and choosing additional security or protocol options.

OpenVPN Client

Go to **System Settings > Services** and find **OpenVPN Client**. Click the pencil to configure the service.



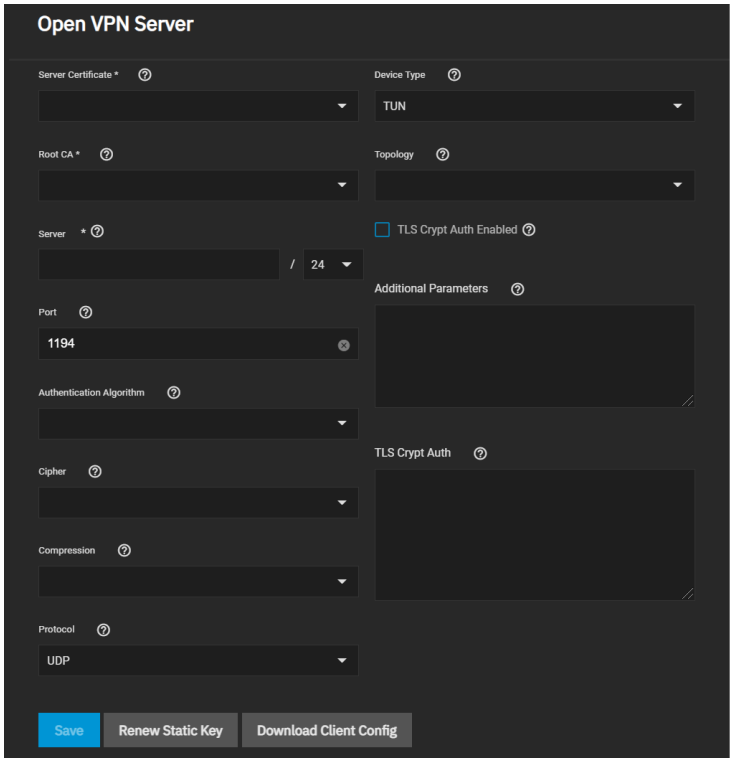
Choose the certificate to use as an OpenVPN client. The certificate must exist in TrueNAS and be active (unrevoked). Enter the **Remote** OpenVPN server's hostname or IP address.

Continue to review and choose any other Connection Settings that fit your network environment and performance requirements. The **Device Type** must match the OpenVPN server **Device Type**. **Nobind** prevents using a fixed port for the client and is enabled by default so the OpenVPN client and server run concurrently.

Finally, review the Security Options and ensure they meet your network security requirements. If the OpenVPN server uses TLS Encryption, copy the static TLS encryption key and paste it into the **TLS Crypt Auth** field.

OpenVPN Server

Go to **System Settings > Services** and find **OpenVPN Server**. Click the pencil to configure the service.



Choose a **Server Certificate** for the OpenVPN server. The certificate must exist in TrueNAS and be active (unrevoked).

Now define an IP address and netmask for the OpenVPN **Server**. Select the remaining Connection Settings that fit your network environment and performance requirements. If using a **TUN Device Type**, you can choose a virtual addressing topology for the server in **Topology**:

- **NET30**: Use one */30* subnet per client in a point-to-point topology. Use when connecting clients are Windows systems.
- **P2P**: Point-to-point topology that points the local server and remote client endpoints to each other. Each client gets one IP address. Use when none of the clients are Windows systems.
- **SUBNET**: The interface uses an IP address and subnet. Each client gets one IP address. Windows clients require the **TAP-Win32 driver** version 8.2 or newer. **TAP** devices always use the **SUBNET Topology**.

TrueNAS applies the **Topology** selection to any connected clients.

When **TLS Crypt Auth Enabled** is selected, TrueNAS generates a static key for the **TLS Crypt Auth** field after saving the options. To change this key, click **Renew Static Key**. Clients connecting to the server require the key. TrueNAS stores keys in the system database and includes them in client config files. We recommend always backing up keys in a secure location.

Finally, review the Security Options and choose settings that meet your network security requirements.

After configuring and saving your OpenVPN Server, generate client configuration files to import to any OpenVPN client systems connecting to this server. You need the certificate from the client system already imported into TrueNAS. To generate the configuration file, click **Download Client Config** and select the **Client Certificate**.

Common Options (Client or Server)

Many OpenVPN server or client configuration fields are identical. This section covers these fields and lists specific configuration options in the Server and Client sections.

The **Additional Parameters** field manually sets any core OpenVPN config file options. See the OpenVPN Reference Manual for descriptions of each option.

Connection Settings

Setting	Description
Root CA	The Certificate Authority (CA) must be the root CA you used to sign the client and server certificates.
Port	The port that the OpenVPN connection is to use.
Compression	Choose a compression algorithm for traffic. Leave empty to send data uncompressed. **LZO** is a standard compression algorithm that is backward compatible with previous (pre-2.4) versions of OpenVPN. **LZ4** is newer and typically faster and requires fewer system resources.
Protocol	Choose between **UDP** or **TCP** OpenVPN protocols. **UDP** sends packets in a continuous stream. **TCP** sends packets sequentially.

Setting	Description
	UDP is usually faster and less strict about dropped packets than TCP. To force the connection to be IPv4 or IPv6, choose one of the 4 or 6 UDP or TCP options.
Device Type	Use a **TUN** or **TAP** virtual networking device and layer with OpenVPN. The device must be identical between the OpenVPN server and clients.

Security Options

OpenVPN includes several security options since using a VPN involves connecting to a private network while sending data over less secure public resources. Security options are not required, but they help protect data users send over the private network.

Setting	Description
Authentication Algorithm	Validates packets sent over the network connection. Your network environment might require a specific algorithm. If not, **SHA1 HMAC** is a reliable algorithm to use.
Cipher	Encrypts data packets sent through the connection. Ciphers aren't required but can increase connection security. You might need to verify which ciphers your networking environment requires. If there are no specific cipher requirements, AES-256-GCM is a good default choice.
TLS Encryption	When **TLS Crypt Auth Enabled** is selected, OpenVPN adds another layer of security by encrypting all TLS handshake messages. This setting requires sharing a static key between the OpenVPN server and clients.

Service Activation

Click **Save** after configuring the server or client service. Start the service by clicking the related toggle in **System Settings > Services**. Hover over the toggle to check the service current state.

Selecting **Start Automatically** starts the service whenever TrueNAS completes booting.

Related Content

- Configuring OpenVPN Service

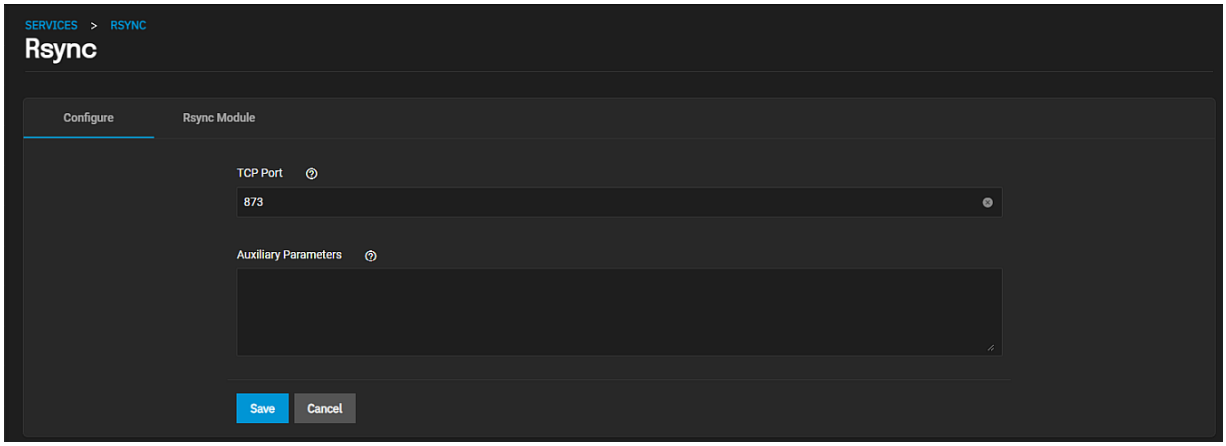
4.11.5.6 - Rsync Services Screen

This article provides information on the rsync services screens and settings.

Rsync is a utility that copies data across a network. The **Services > Rsync** screen has two tabs: **Configure** and **Rsync Module**.

Configure Screen

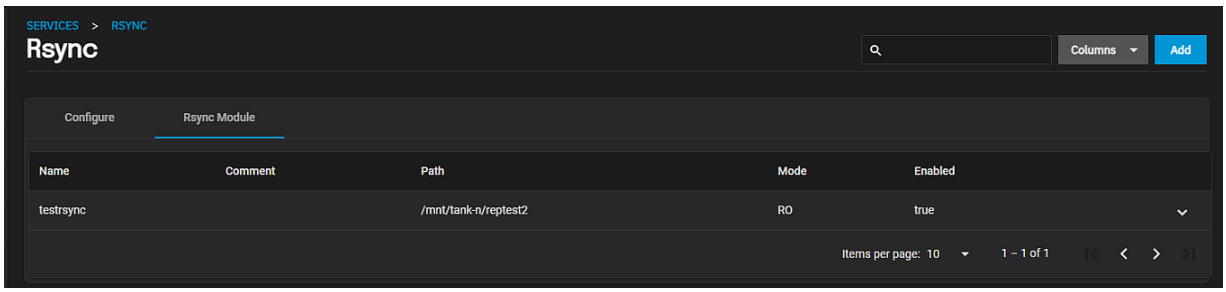
The **Rsync > Configure** screen displays the **TCP Port** and **Auxiliary Parameters** settings.



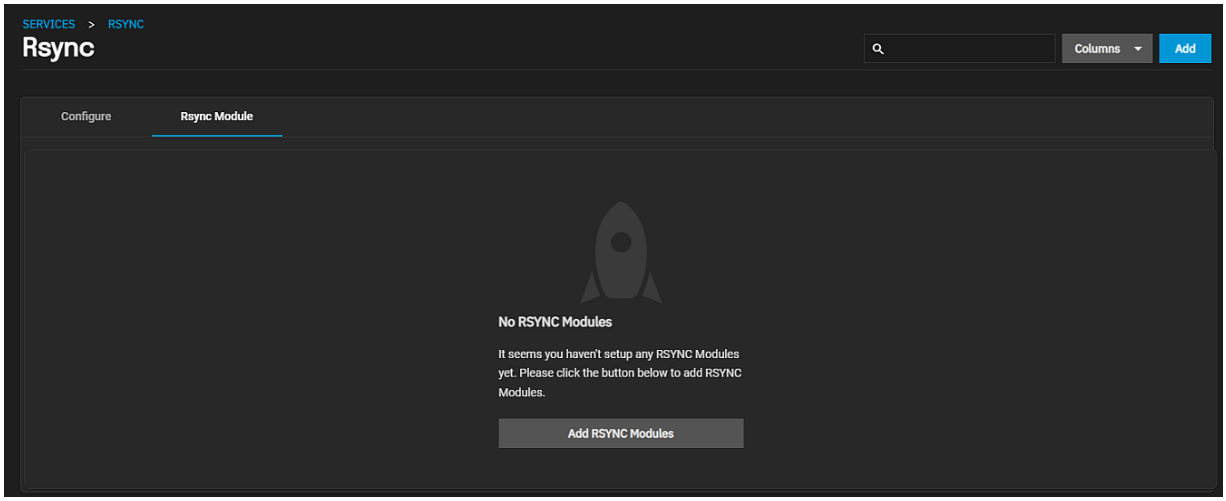
Setting	Description
TCP Port	Enter the port **rsyncd** listens on.
Auxiliary Parameters	Enter any additional parameters from rsyncd.conf(5).

Rsync Module Screen

The **Rsync Module** screen displays a list of current rsync modules configured on the system. When setting up an rsync task you have the option to use either SSH or an rsync module as the



Before an rsync module is configured the **Modules** screen displays the **No RSYNC Modules** screen displays with **Add RSYNC Modules** in the center of the screen. Use either **Add RSYNC Modules** or **Add** to configure a module to use as the mode (when you select **Module** in **Rsync Mode**).

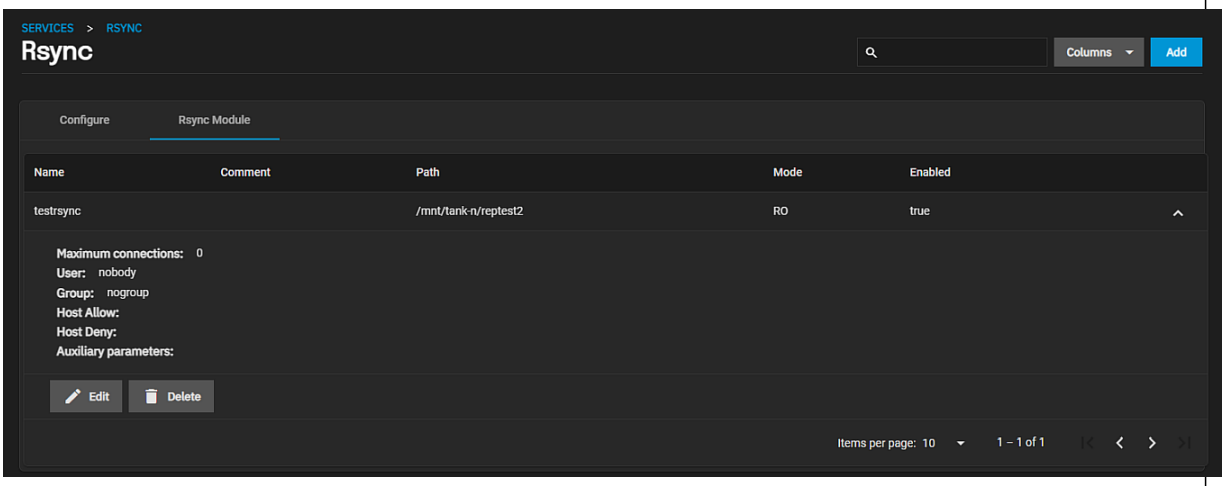


The name of the module or the › arrow expand the module to display the details of the module.

Rsync Module Details Screen

The rsync module details screen displays connections, user, group, allow and deny host information, and any auxiliary parameters configured for that module.

Click Here for More Information

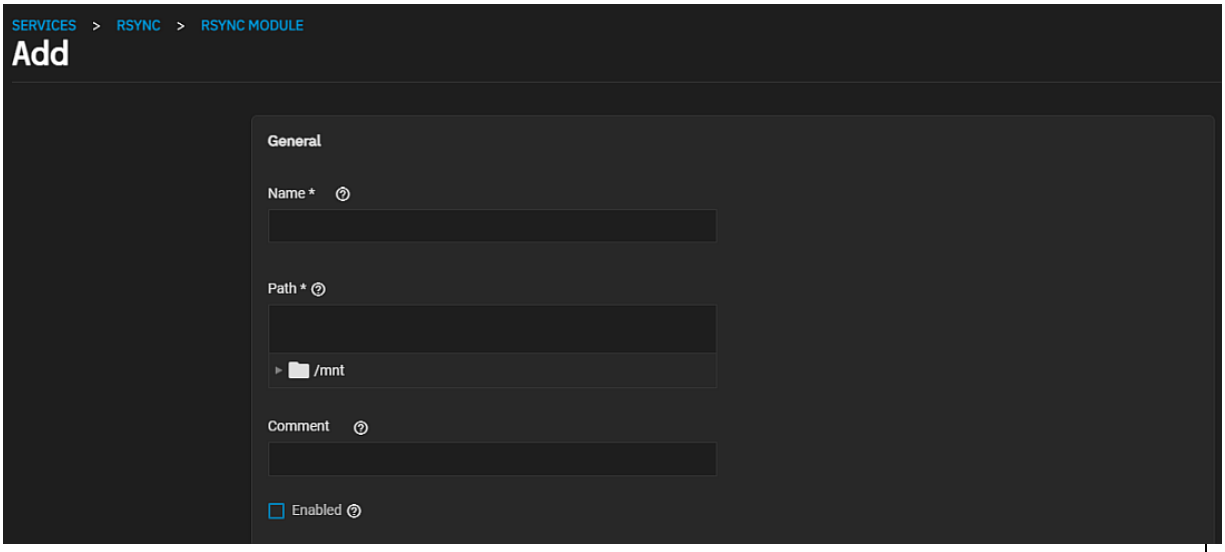


Edit opens the **Edit Rsync Module** screen. **Delete** opens a confirmation dialog.

Add or Edit Rsync Module Screens

Rsync > Add and **Rsync > Edit** screens specify the general, access and other settings for the rsync module.

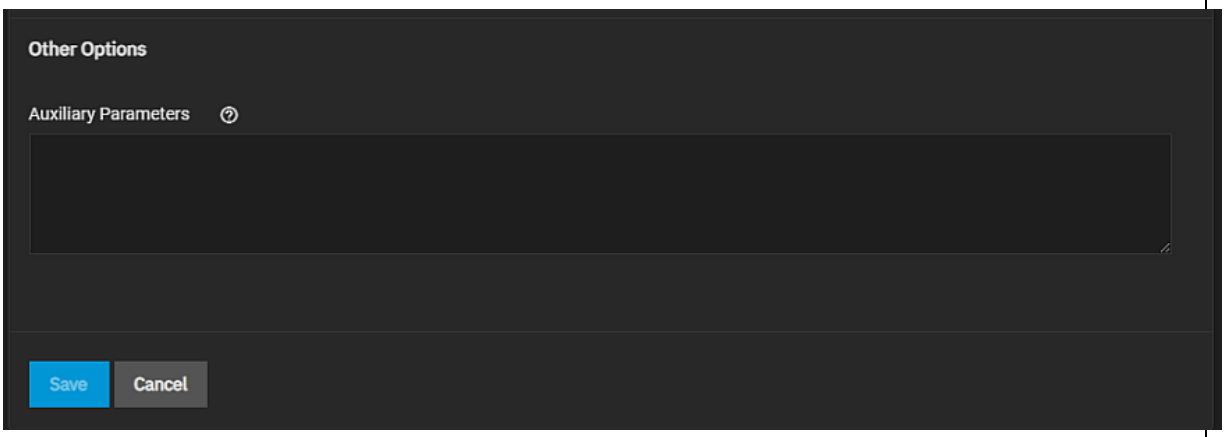
Click Here for More Information



Setting	Description
Name	Enter a module name that matches the name requested by the rsync client.
Path	Enter or uses the ▸ to the left of 📁 **/mnt** to browse to the pool or dataset to store received data.
Comment	Enter a description for this module.
Enabled	Select to activate this module for use with Rsync. Leave clear to deactivate the module without completely removing it.

Setting	Description
Access Mode	Select the permission level for this rsync module from the dropdown list. Options are **Read Only**, **Write Only**, or **Read and Write**.
Max Connections	Enter the maximum number of connections to this module. **0** is unlimited.
User	Enter or select the TrueNAS user account that runs the rsync command during file transfers to and from this module from the dropdown list.
Group	Enter or select the TrueNAS group account that runs the rsync command during file transfers to and from this module from the dropdown list.

Setting	Description
Hosts Allow	Enter a list of patterns to match with the host name and IP address of a connecting client (from rsyncd.conf(5). The connection is rejected if no patterns match. Separate entries by pressing `Enter`.
Hosts Deny	Enter a list of patterns to match with the hostname and IP address of a connecting client (from rsyncd.conf(5). The connection is rejected when the patterns match. Separate entries by pressing `Enter`.



Setting	Description
Auxiliary Parameters	Enter any additional parameters from rsyncd.conf(5).

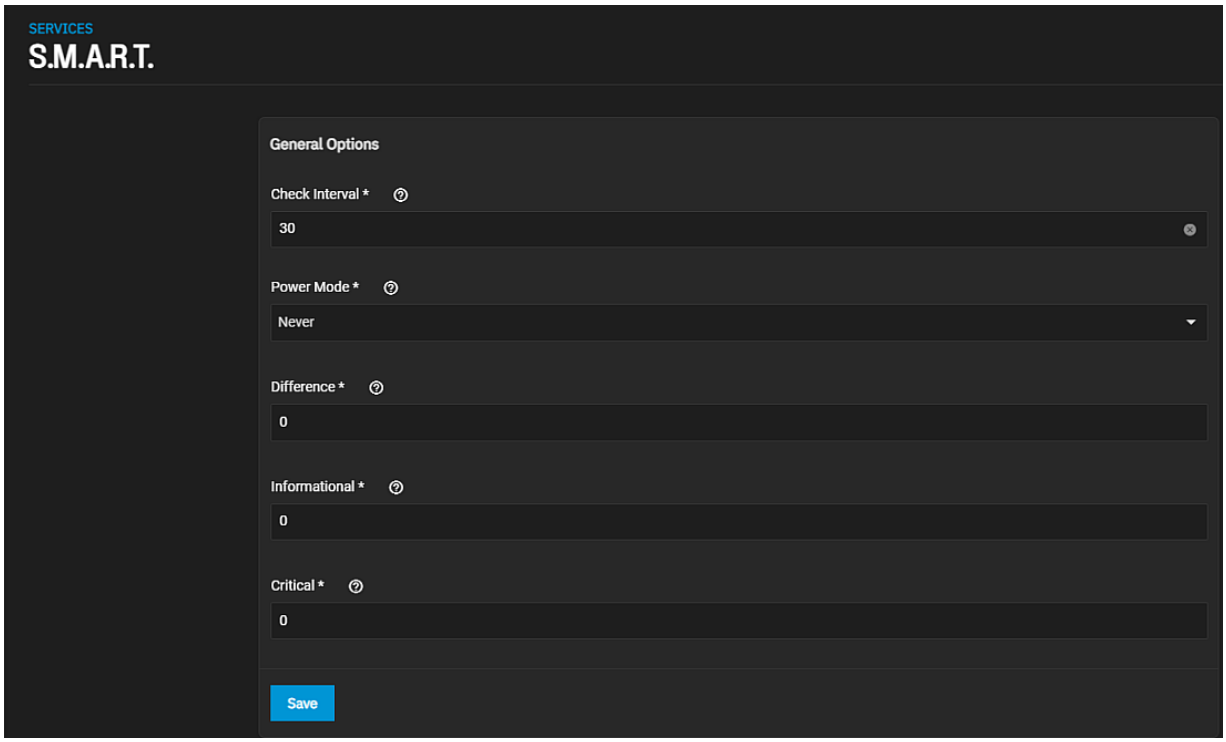
Related Content

- Adding SSH Credentials
- Configuring Rsync Tasks
- Rsync Tasks Screens
- Configuring Rsync Modules

4.11.5.7 - S.M.A.R.T. Service Screen

This article provides information on S.M.A.R.T. service screen settings.

The **Services > S.M.A.R.T.** screen displays settings to configure when S.M.A.R.T. tests run and when to trigger alert warnings and send emails.



Name	Description
Check Interval	Enter the time in minutes for smartd to wake up and check if any tests are configured to run.
Power Mode	Select the power mode from the dropdown list. Options are **Never**, **Sleep**, **Standby** or **Idle**. S.M.A.R.T. only tests when the **Power Mode** is **Never**.
Difference	Enter a number of degrees in Celsius. S.M.A.R.T. reports if a drive temperature changes by N degrees Celsius since the last report.
Informational	Enter a threshold temperature in Celsius. S.M.A.R.T. sends a message with a LOG_INFO log level if the temperature is above the threshold.
Critical	Enter a threshold temperature in Celsius. S.M.A.R.T. sends a message with a LOG_CRIT log level and send an email if the temperature is above the threshold.

Click **Save** after changing any settings.

Related Content

- Configuring S.M.A.R.T. Service
- Managing S.M.A.R.T. Tests
- S.M.A.R.T. Tests Screens

4.11.5.8 - S3 Service Screen

This article provides information on the the S3 service screen settings.

The **Services > S3** screen allows you to specify settings to connect to TrueNAS from a networked client system with the Minio browser, s3cmd, or S3 browser.

![S3ServiceSettings(/images/SCALE/22.02/S3ServiceSettings.png “S3 Service Options”)

Settings	Description
IP Address	Select an IP address from the dropdown list options **0.0.0.0**, **::**, or to enter the IP address that runs the S3 service. Select **0.0.0.0** to tell the server to listen on all addresses. Select the TrueNAS IP address to constrain it to a specific network.
Port	Enter the TCP port that provides the S3 service.
Console Port	Enter a static port for the MinIO web console. Default is 9001.
Access Key	Enter the S3 access ID. See Access keys for more information.
Secret Key	Enter the S3 secret access key. See Access keys for more information.
Disk	Enter or use to the left of **/mnt** to browse to a directory to define the S3 file system path.
Enable Browser	Enables the S3 service web UI. Access the MinIO web UI by entering the IP address and port number separated by a colon in the browser address bar. Example: *192.168.1.0:9000*.
Certificate	Use an SSL certificate created or imported in **Credentials > Certificates** for secure S3 connections.
TLS Server URI	Displays after selecting an SSL certificate. Enter the TLS server host name. Or enter a MinIO server address that can be a proxy.

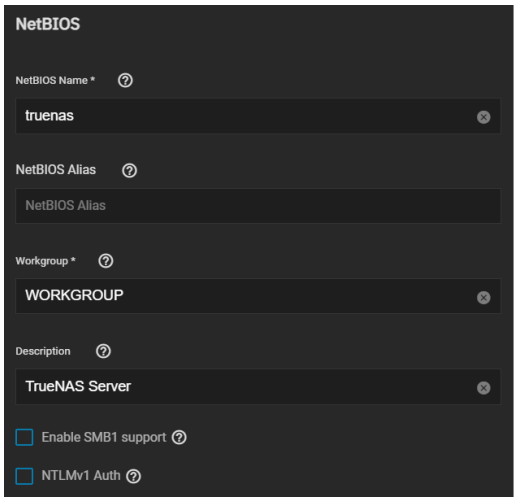
Related Content

- Adding Cloud Credentials
- Cloud Credentials Screens
- Configuring S3 Service

4.11.5.9 - SMB Service Screen

This article provides information in the SMB service screen and settings.

The **SMB Services** screen displays setting options to configure TrueNAS SMB settings to fit your use case. The **Basic Options** settings continue to display after selecting the **Advanced Options** screen.



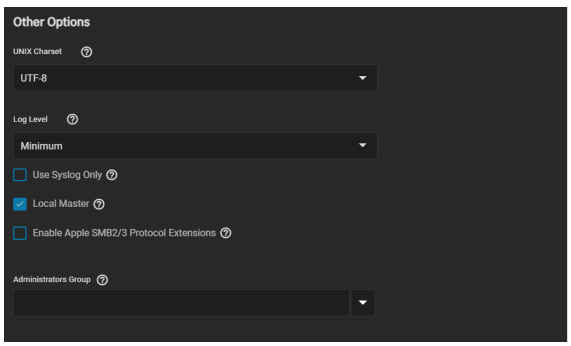
Click **Save** or **Cancel** to close the configuration screen and return to the **Services** screen.

Basic Options Settings

Setting	Description
NetBIOS Name	Automatically populated with the original system host name. This name is limited to 15 characters and cannot be the **Workgroup** name.
NetBIOS Alias	Enter any alias name that is up to 15 characters long. Separate alias names with a space between them.
Workgroup	Enter a name that matches the Windows workgroup name. When unconfigured and Active Directory or LDAP is active, TrueNAS detects and sets the correct workgroup from these services.
Description	(Optional) Enter any notes or descriptive details about the service configuration.
Enable SMB1 support	Select to allow legacy SMB1 clients to connect to the server. Note: SMB1 is being deprecated. We advise you to upgrade clients to operating system versions that support modern SMB protocol versions.
NTLMv1 Auth	Off by default. Select to allow smbd attempts to authenticate users with the insecure and vulnerable NTLMv1 encryption. This setting allows backward compatibility with older versions of Windows, but is not recommended. Do not use on untrusted networks.

Advanced Options Settings

The **Basic Options** settings also display on the **Advanced Options** settings screen with the **Other Options** settings.



Setting	Description
UNIX Charset	Select the character set to use internally from the dropdown list of options. **UTF-8** is standard for most systems as it supports all characters in all languages.

Setting	Description
Log Level	Record SMB service messages up to the specified log level from the dropdown list. Options are **None**, **Minimum**, **Normal**, **full** and **Debug**. By default, error and warning level messages are logged. It is not recommended to use a log level above **Minimum** for production servers.
Use Syslog Only	Select to log authentication failures in */var/log/messages* instead of the default */var/log/samba4/log.smbd*.
Local Master	Selected by default and determines if the system participates in a browser election. Clear this checkbox when the network contains an AD or LDAP server, or when Vista or Windows 7 machines are present.
Enable Apple SMB2/3 Protocol Extensions	Select to allow MacOS to use these protocol extensions to improve the performance and behavioral characteristics of SMB shares. This is required for Time Machine support.
Administrators Group	Enter or select members from the dropdown list. Members of this group are local administrators and automatically have privileges to take ownership of any file in an SMB share, reset permissions, and administer the SMB server through the Computer Management MMC snap-in.
Guest Account	Select the account to use for guest access from the dropdown list. Default is **nobody**. The selected account must have permissions to the shared pool or dataset. To adjust permissions, edit the dataset Access Control List (ACL), add a new entry for the chosen guest account, and configure the permissions in that entry. If the selected **Guest Account** is deleted the field resets to **nobody**.
File Mask	Overrides default **0666** file creation mask which creates files with read and write access for everybody.
Directory Mask	Overrides default directory creation mask of **0777** which grants directory read, write and execute access for everybody.
Bind IP Addresses	Select static IP addresses that SMB listens on for connections from the dropdown list. Leaving all unselected defaults to listening on all active interfaces.
Auxiliary Parameters	Enter additional smb.conf options. Refer to the [Samba Guide]9http://www.oreilly.com/openbook/samba/book/appb_02.html) for more information on these settings. You can use **Auxiliary Parameters** to override the default SMB server configuration, but such changes could adversely affect SMB server stability or behavior. To log more details when a client attempts to authenticate to the share, add `log level = 1, auth_audit:5`.

Related Content

- Adding SMB Shares
- SMB Shares Screens
- Managing SMB Shares
- Using SMB Shadow Copy
- Setting Up SMB Home Shares
- Configuring SMB Service
- Spotlight Support on a SCALE SMB Share

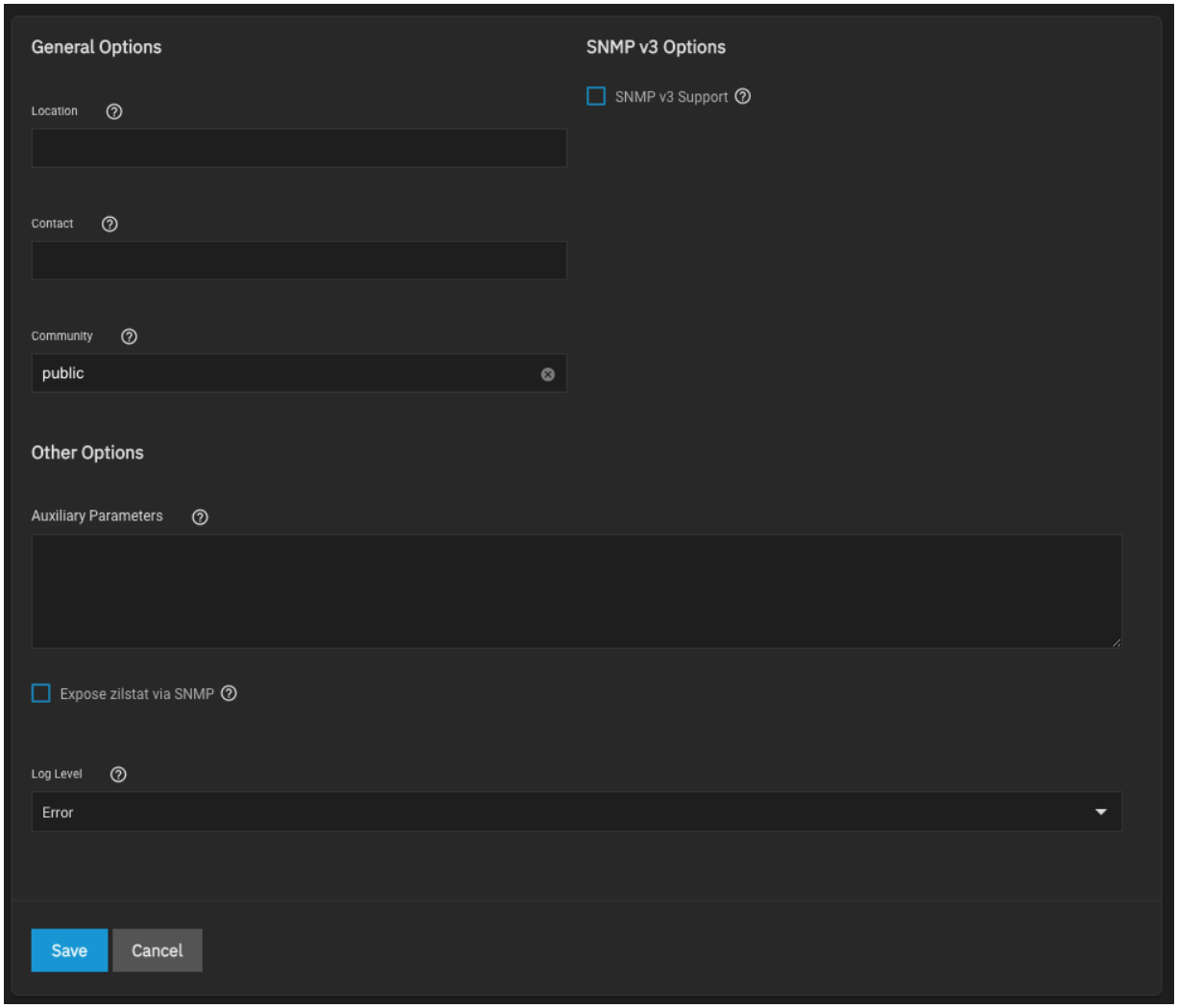
4.11.5.10 - SNMP Service Screen

This article provides information on SNMP service screen settings.

The **Service > SNMP** screen settings configure SNMP (Simple Network Management Protocol) that monitors network-attached devices for conditions that warrant administrative attention.

Click the ✎ to open the **Services > SNMP** configuration screen.

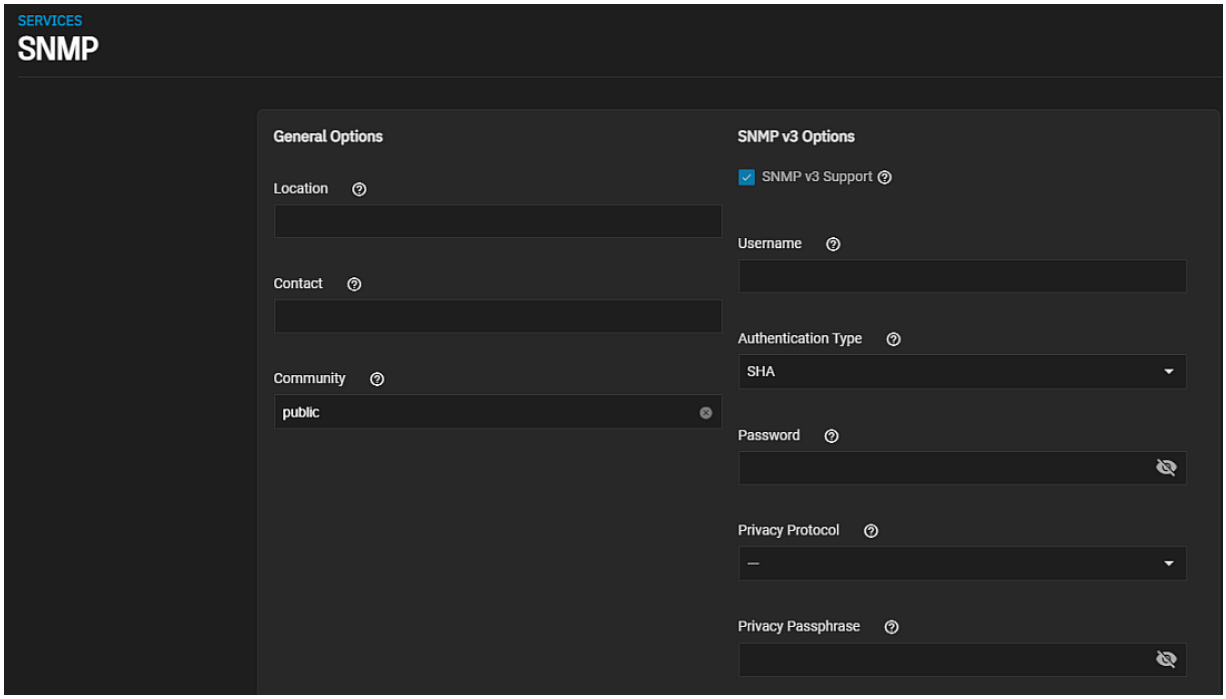
General Options



SNMP v3 Options

Setting	Description
Location	Enter the location of the system.
Contact	Enter the email address to receive SNMP service messages.
Community	Enter a community other than the default **public** to increase system security. Value can only contain alphanumeric characters, underscores (_), dashes (-), periods (.), and spaces. Not required and can leave this empty for SNMPv3 networks.

SNMP v3 Options



Setting	Description
SNMP v3 Support	Select to to enable support for SNMP version 3 and display the SNMP v3 setting fields. See snmpd.conf(5) for configuration details.
Username	Enter a user name to register with this service.
Authentication Type	Select an authentication method: **—** for none, **SHA**, or **MD5** from the dropdown list.
Password	Enter a password of at least eight characters.
Privacy Protocol	Select a privacy protocol: **—** for none, **AES**, or **DES** from the dropdown list.
Privacy Passphrase	Enter a separate privacy passphrase. **Password** is used when this is left empty.

Other Options

Setting	Description
Auxiliary Parameters	Enter any additional snmpd.conf options. Add one option for each line.
Expose zilstat via SNMP	Select to enable. If enabled this option might have performance implications on your pools.
Log Level	Select how many log entries to create. Dropdown list options are **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Info** and **Debug**.

Related Content

- Configuring SNMP Service

4.11.5.11 - SSH Service Screen

This article provides information on the SSH service screens and settings.

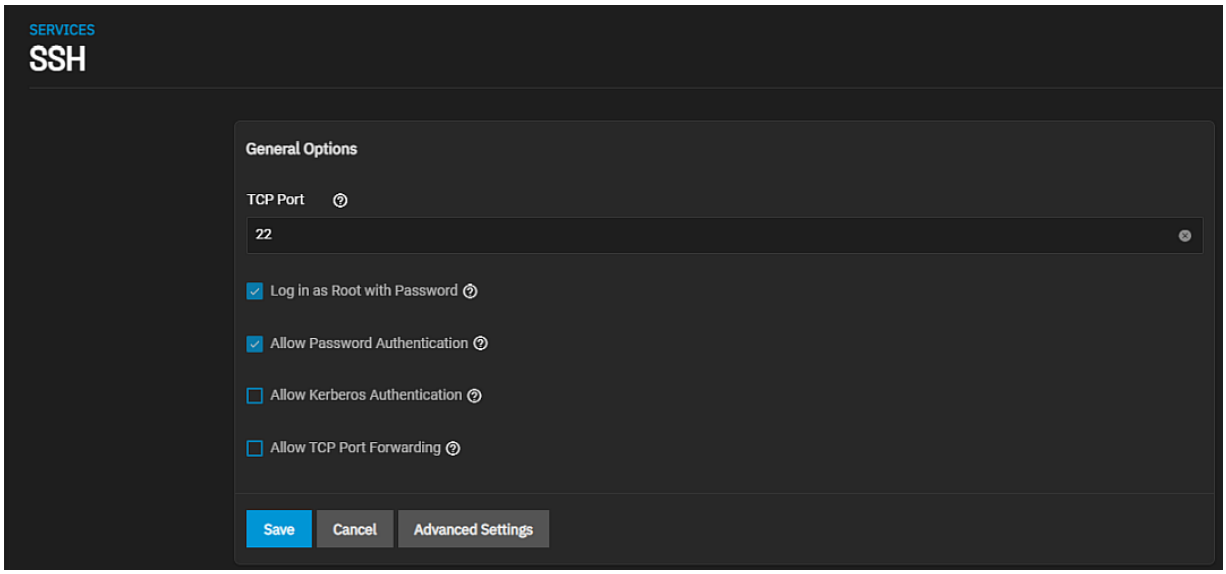
The **System Settings > Services > SSH** screen allows you to set up SSH service on TrueNAS SCALE.

Click ✎ to open the **Services > SSH** configuration screen.

> Allowing external connections to TrueNAS is a security vulnerability! Do not enable SSH unless you require external connections. See Security Recommendations for more security considerations when using SSH.

SSH Basic Settings Options

The **Basic Settings** options display by default when you edit the SSH service.

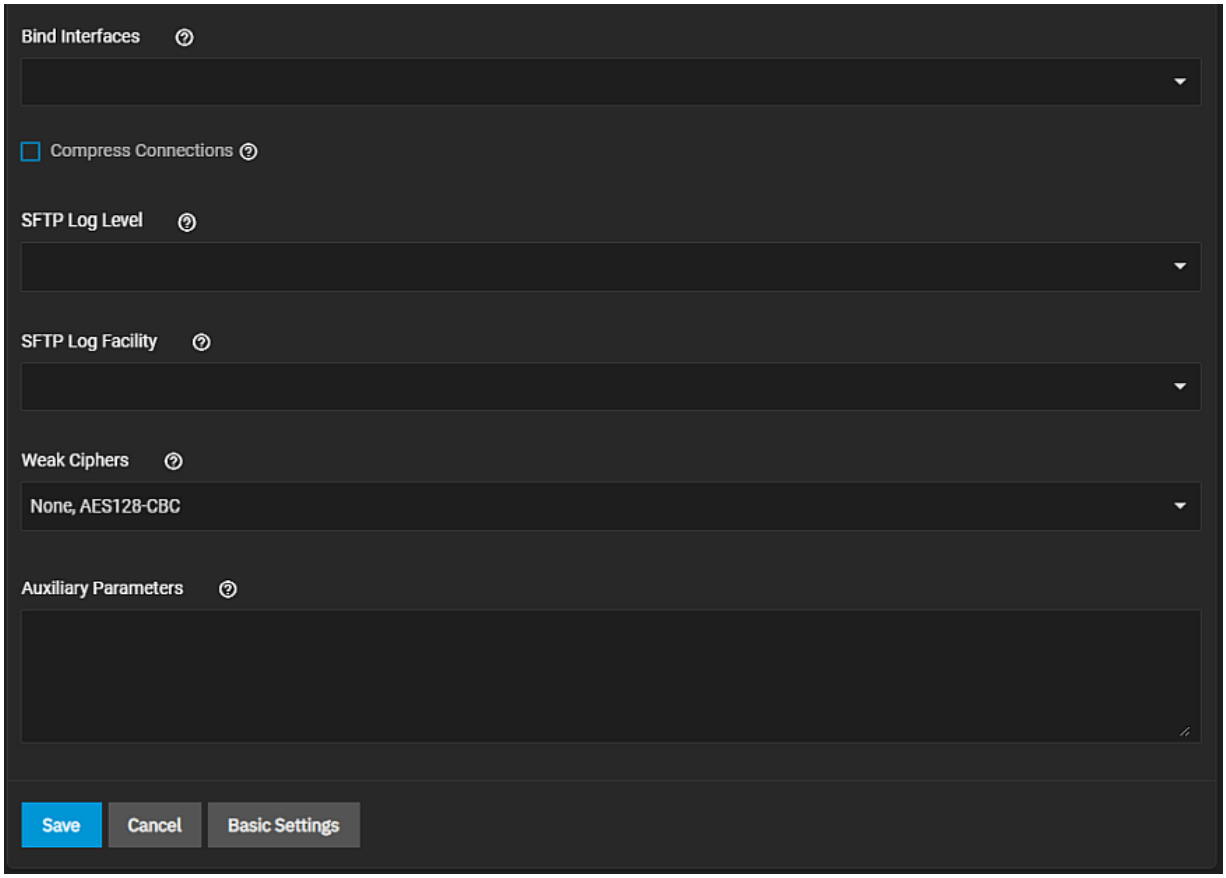


General Options

Setting	Description
TCP Port	Enter the port number for SSH connection requests.
Log in as Root with Password	Select to allow the root (administration) account to log into TrueNAS with a password. You must set a password for the root user account. Root logins are discouraged!
Allow Password Authentication	Select to allow all user accounts to login via SSH and the account password. Leave checkbox clear to disable and require exchanging SSH keypairs for client systems attempting to access this system. Warning: when directory services are enabled, this setting grants access to all users the directory service imported. When disabled, authentication requires keys for all users. This requires additional SSH client and server setup.
Allow Kerberos Authentication	Select to allow kerberos authentication. Ensure valid entries exist in **Directory Services > Kerberos Realms** and **Directory Services > Kerberos Keytabs** and the system can communicate with the kerberos domain controller before enabling this option.
Allow TCP Port Forwarding	Select to allow users to bypass firewall restrictions using the SSH port forwarding feature. For best security leave this option disabled.

SSH Advanced Settings Options

Advanced Settings include the **General Options** settings. Advanced settings specify bind interfaces, SFTP settings, ciphers and any additional parameters you want to use.



Setting	Description
Bind Interfaces	Select the network interface on your system for SSH to listen on from the dropdown list. Leave all options unselected for SSH to listen on all interfaces.
Compress Connections	Select to attempt to reduce latency over slow networks.
SFTP Log Level	Select the syslog(3) level of the SFTP server from the dropdown list options. Options are **Quiet**, **Fatal**, **Error**, **Info**, **Verbose**, **Debug**, **Debug2** or **Debug3**.
SFTP Log Facility	Select the syslog(3) facility of the SFTP server option from the dropdown list. Options are **Daemon**, **User**, **Auth** and **Local 0** through **Local7**.
Weak Ciphers	Select a cypher from the dropdown list. Options are **None** or **AES128-CBC**. To allow more ciphers for sshd(8) in addition to the defaults in sshd_config(5). Use **None** to allow unencrypted SSH connections. Use **AES128-CBC** to allow the 128-bit Advanced Encryption Standard. WARNING: These ciphers are security vulnerabilities. Only allow them in a secure network environment.
Auxiliary Parameters	Enter any sshd_config(5) options not covered in this screen. Enter one option per line. Options added are case-sensitive. Misspellings can prevent the SSH service from starting.

Related Content

- Adding SSH Credentials
- SSH Screens
- Configuring Rsync Tasks
- Rsync Tasks Screens
- Security Recommendations
- Configuring SSH Service
- Using 2FA (Two-Factor Authentication)

4.11.5.12 - TFTP Services Screen

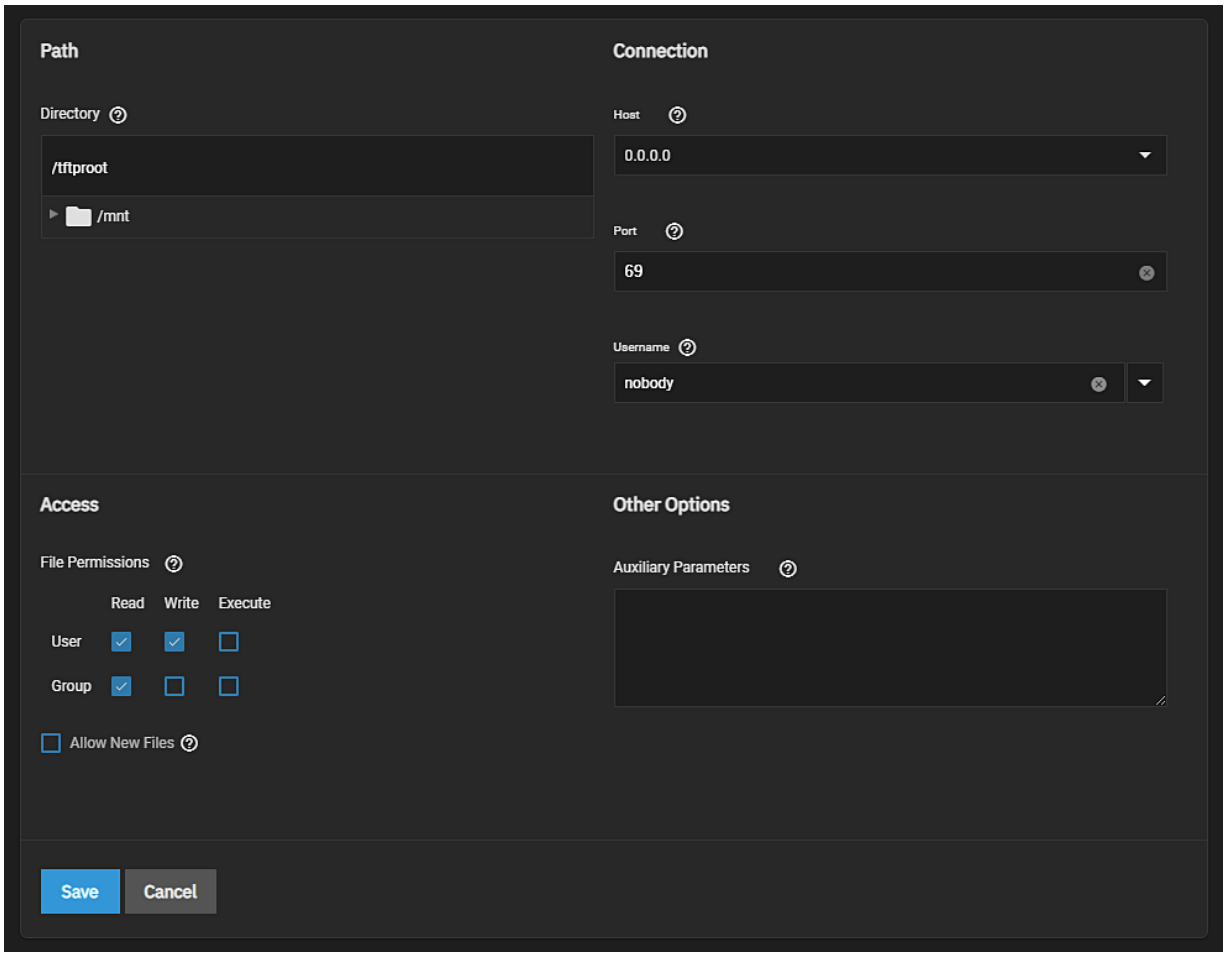
This article provides information on the TFTP screen settings.

The File Transfer Protocol (FTP) is a simple option for data transfers. The SSH and Trivial FTP options provide secure or simple config file transfer methods respectively.

Click the ✎ to open the **Services > TFTP** configuration screen.

TFTP Service

The **TFTPS** screen displays settings that specify the directory location to use for storing files, the connection information, file permissions and any auxiliary parameters you want to use to further customize this service.



Path Settings

Settings	Description
Directory	Enter or click the ▸ to the left of 🗀 **/mnt** to browse to an existing directory to used for storage. Some devices can require a specific directory name. Consult the documentation for that device for any name restrictions.

Connection Settings

Settings	Description
Host	Enter or select the default host name or IP address to use for TFTP transfers from the dropdown list. To use **Shell**, enter an IP address. For example, *192.0.2.1*.

Settings	Description
Port	Enter the UDP port number that listens for TFTP requests. For example, *8050* or in **Shell** `8050`.
Username	Select the user account to use for TFTP requests from the dropdown list of options that includes but are not limted to **root**, **daemon**, **operator**, **nobody** and all the other usernames on the system. This account must have permission to what you specified in **Directory**.

Access Settings

Settings	Description
File Permissions	Select **Read**, **Write** and **Execute** permissions for both **User** and **Group** to adjust the file permissions. Select all that apply.
Allow New Files	Select to allow network devices that need to send files to the system to send files.

Other Options Settings

Settings	Description
Auxiliary Parameters	Enter any options from tftpd, one option on each line, to further customize the TFTP service.

Related Content

- Configuring FTP Service
- FTP Service Screen

4.11.5.13 - UPS Services Screen

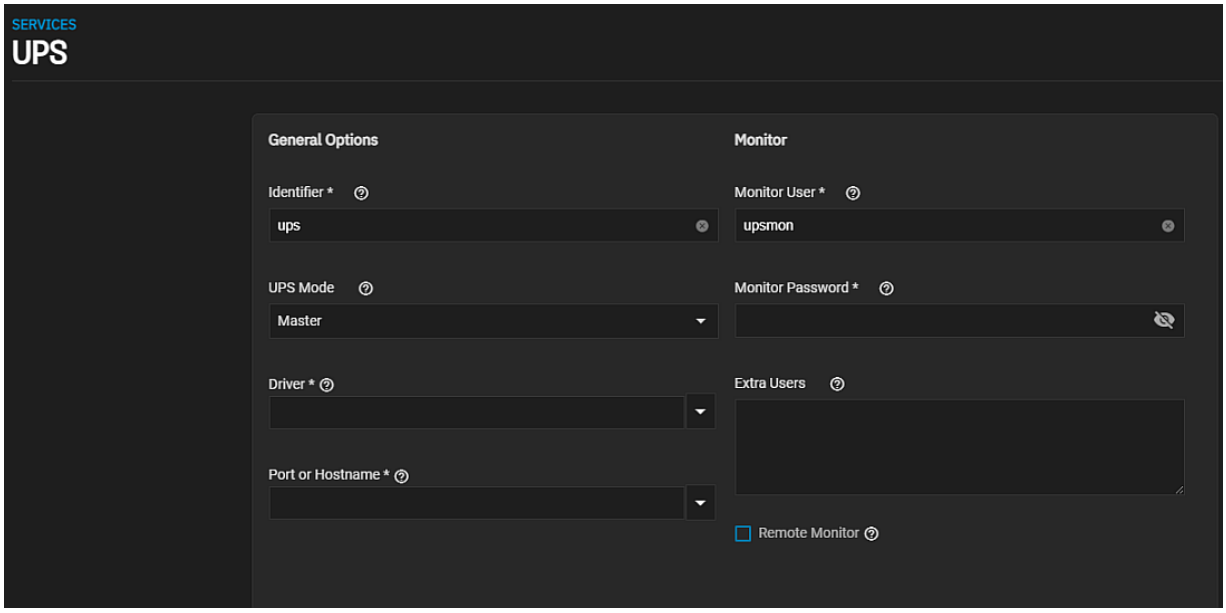
This article provides information on the UPS service screen settings.

The **Services > UPS** screen settings specify connection, shutdown and other settings to configure UPS service for servers running TrueNAS SCALE.

Click ✎ to open the **Services > UPS** configuration screen.

General Options and Monitor Settings

General Options setting specify required UPS mode and connection. These settings change based on the **Master** or **Slave** UPS mode setting.



Setting	Description
Identifier	Required. Type a description for the UPS device. You can use alphanumeric, period (.), comma (,), hyphen (-), and underscore (_) characters.
UPS Mode	Select the either **Master** or **Slave** mode from the dropdown list. Select **Master** if the UPS is plugged directly into the system serial port, or **Slave** to shut down this system before the master system. **Slave** displays the **Remote Hostname** and **Remote Port** fields, and removes the **Driver** field. The UPS remains the last item to shut down. See the Network UPS Tools Overview.
Remote Hostname	Required. Enter a valid IP address for the remote system with the **UPS Mode** set to **Master**. This field displays only when **UPS Mode** is set to **Slave**.
Remote Port	Required. Enter the open network port number of the UPS master system. The default port is 3493. This field displays only when **UPS Mode** is set to **Slave**.
Driver	Required. Enter or select the device driver from the dropdown list. See the Network UPS Tools compatibility listfor a list of supported UPS devices. This field displays only when **UPS Mode** is set to **Master**.
Port or Hostname	Required. Enter or select the serial or USB port connected to the UPS from the dropdown list. Options include a list of port on your system and **auto**. Select **auto** to automatically detect and manage the USB port settings. When selecting an SNMP driver, enter the IP address or host name of the SNMP UPS device.

Monitor Settings

Monitor settings specify the primary username and password, other users that have administrative access to the UPS service, and whether the default configuration listens on all interfaces.

Setting	Description
Monitor User	Enter a user to associate with this service. Keeping the default is recommended.

Setting	Description
Monitor Password	Change the default password to improve system security. The new password cannot include a space or #.
Extra Users	Enter accounts that have administrative access. See upsd.users(5) for examples.
Remote Monitor	Select to have the default configuration to listen on all interfaces using the known values of user: **upsmon** and password: **fixmepass**.

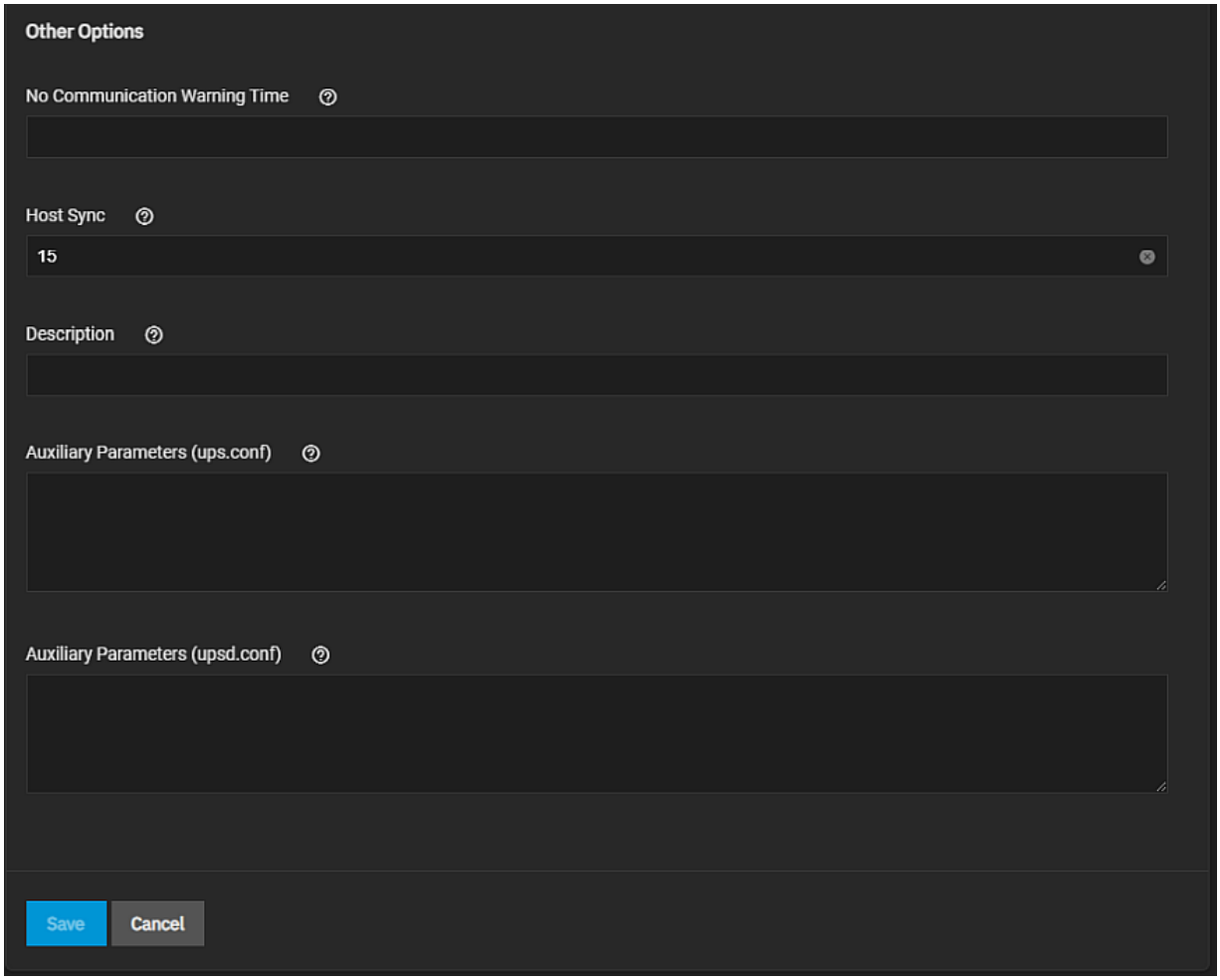
Shutdown Settings

Shutdown settings specify the UPS shutdown mode, command, and timer for the UPS service.

Setting	Description
Shutdown Mode	Select the battery option to used when the UPS initiates shutdown from the dropdown list. Options are **UPS reaches low battery** or **UPS goes on battery**.
Shutdown Timer	Enter a value in seconds for the UPS to wait before initiating shutdown. Shutdown does not occur if power is restored while the timer is counting down. This value only applies when **Shutdown Mode** is set to **UPS goes on battery**.
Shutdown Command	Enter a command to shut down the system when either battery power is low or the shutdown timer ends.
Power off UPS	Select to power off the UPS after shutting down the system.

Other Options Settings

Other Options settings specify warning and host sync times, a description for the UPS, and any additional parameters you want to apply to the UPS service.



Setting	Description
No Communication Warning Time	Enter the number of seconds to wait before alerting that the service cannot reach any UPS. Warnings continue until the situation is fixed.
Host Sync	Upsmon waits up to this many seconds in master mode for the slaves to disconnect during a shutdown situation.
Description	Enter a description for this service.
Auxiliary Parameters (ups.conf)	Enter any extra options from ups.conf.
Auxiliary Parameters (upsd.conf)	Enter any extra options from upsd.conf.

Related Content

- SCALE Hardware Guide
- Configuring UPS Service

4.11.5.14 - WebDAV Service Screen

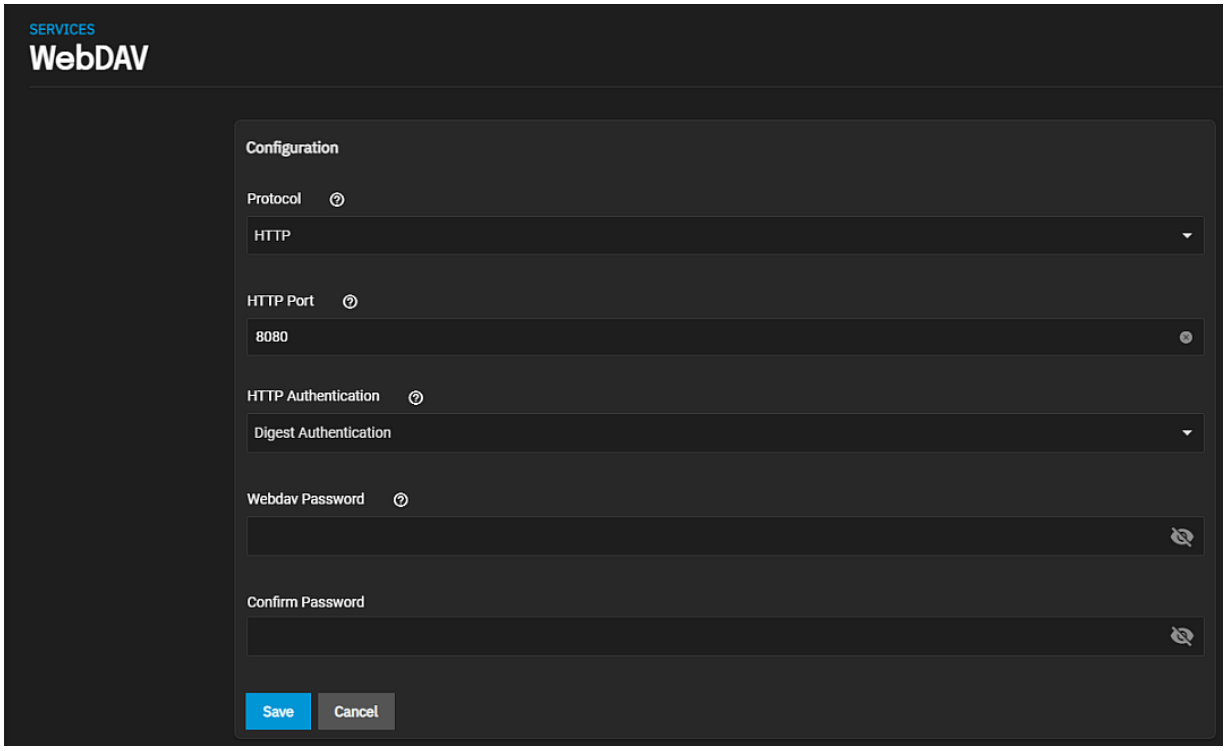
This article provides information on WebDAV service screen and settings.

WebDAV Service Screen

The **Services > WebDAV** configuration screen displays settings to customize the TrueNAS WebDAV service.

You can access it from **System Settings > Services** screen. Locate **WebDAV** and click to open the screen, or use the **Config Service** option on the **WebDAV** widget options menu found on the main **Sharing** screen.

Select **Start Automatically** to activate the service when TrueNAS boots.



If you require it, you must choose an SSL certificate (*freenas_default* is always available). All **Protocol** options require you to define a number in the **Port** field. Make sure the network is not already using the WebDAV service port.

To prevent unauthorized access to the shared data, set the **HTTP Authentication** to either **Basic** or **Digest** and create a new **Webdav Password**.

WebDAV Configuration Settings

Setting	Description
Protocol	Select the protocol option from the dropdown list. Options are **HTTP**, **HTTPS** or **HTTP+HTTPS**. For better security, select **HTTPS**.
HTTP Port	Enter a port number for unencrypted connections. The default **8080** is not recommended. Do not reuse a port number.
HTTP Authentication	Select the authentication method from the dropdown list. Select **Basic Authentication** for unencrypted or **Digest Authentication** for encrypted. **No Authentication** to not use any authentication method.
WebDAV Password	Enter a password. **davtest** is the default password, but you should change this as it is a known password.
Confirm Password	Reenter the password to confirm it.

Related WebDAV Articles

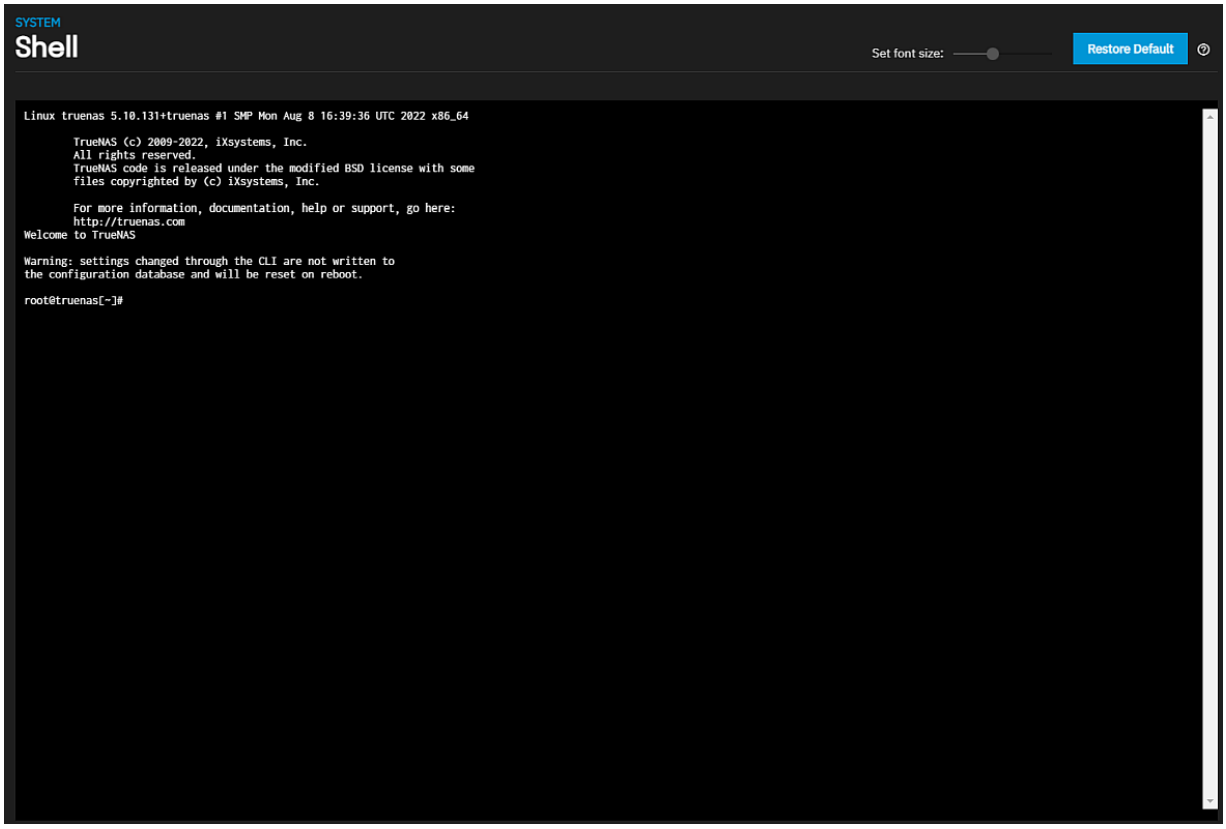
- Adding Cloud Credentials

- Cloud Credentials Screens
- Configuring WebDAV Shares
- WebDAV Shares Screens
- Configuring WebDAV Service

4.11.6 - Shell Screen

This article provides information on the SCALE **Shell** screen, buttons and slider.

SCALE **System Settings > Shell** is convenient for running command lines tools, configuring different system settings, or finding log files and debug information.



The **Set font size** slider adjusts the **Shell** displayed text size. **Restore Default** resets the font size to default.

The **Shell** stores the command history for the current session.

Leaving the **Shell** screen clears the command history.

Click **Reconnect** to start a new session.

Related Content

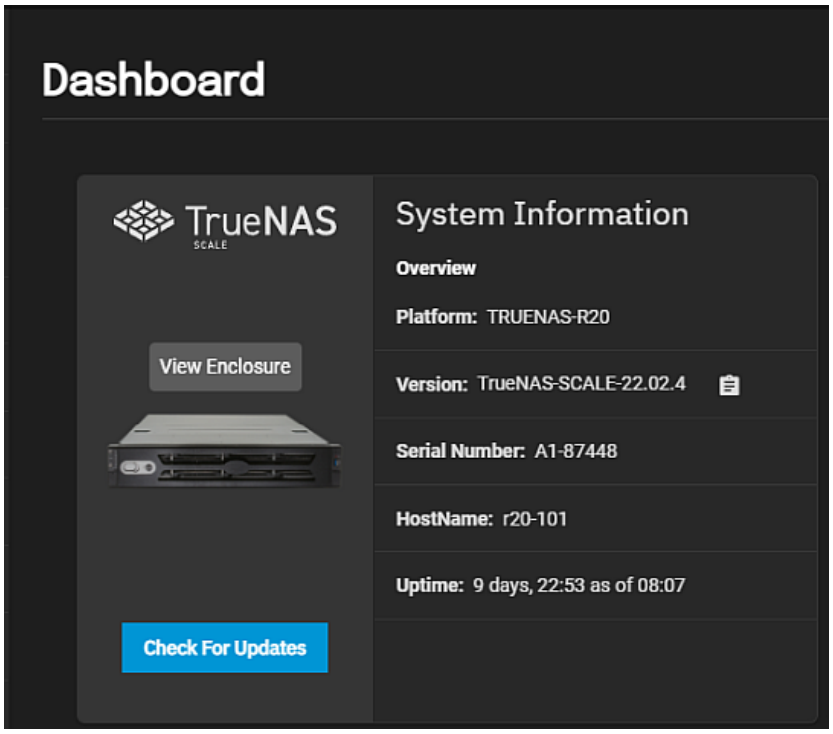
- Using Shell

4.11.7 - View Enclosure Screen

This article provides information on the TrueNAS **View Enclosure** screen, and the information you can find there.

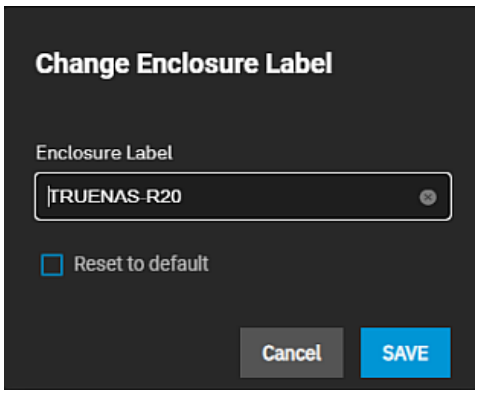
The **View Enclosure** screen displays an image of the TrueNAS-provided system hardware with drive images you can select. The screen includes information on system pools, disks and their status, HDD details and stats that change with the drive you select on the system image. Based on the system hardware, the screen provides additional display and information options that reflects the system hardware model using TrueNAS SCALE.

To access the **System > View Enclosure** screen, either click the image on the main dashboard or go to **System Settings > Enclosure>**.



System Images

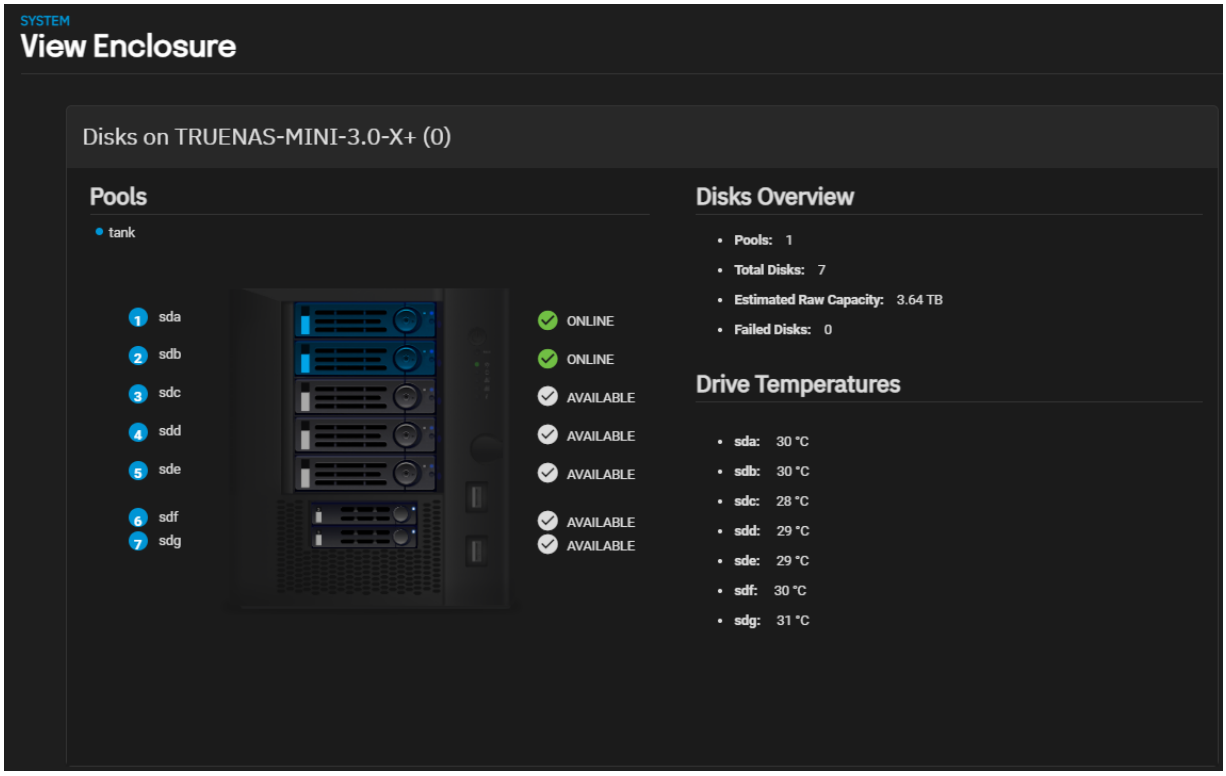
System images display with the front view shown by default. If the system model includes a rear view, click **Rear** to change the image to the rear view of the system hardware. Click **Front** to switch to the front view of the system chassis. **Edit Label** displays for system models other than the Mini.



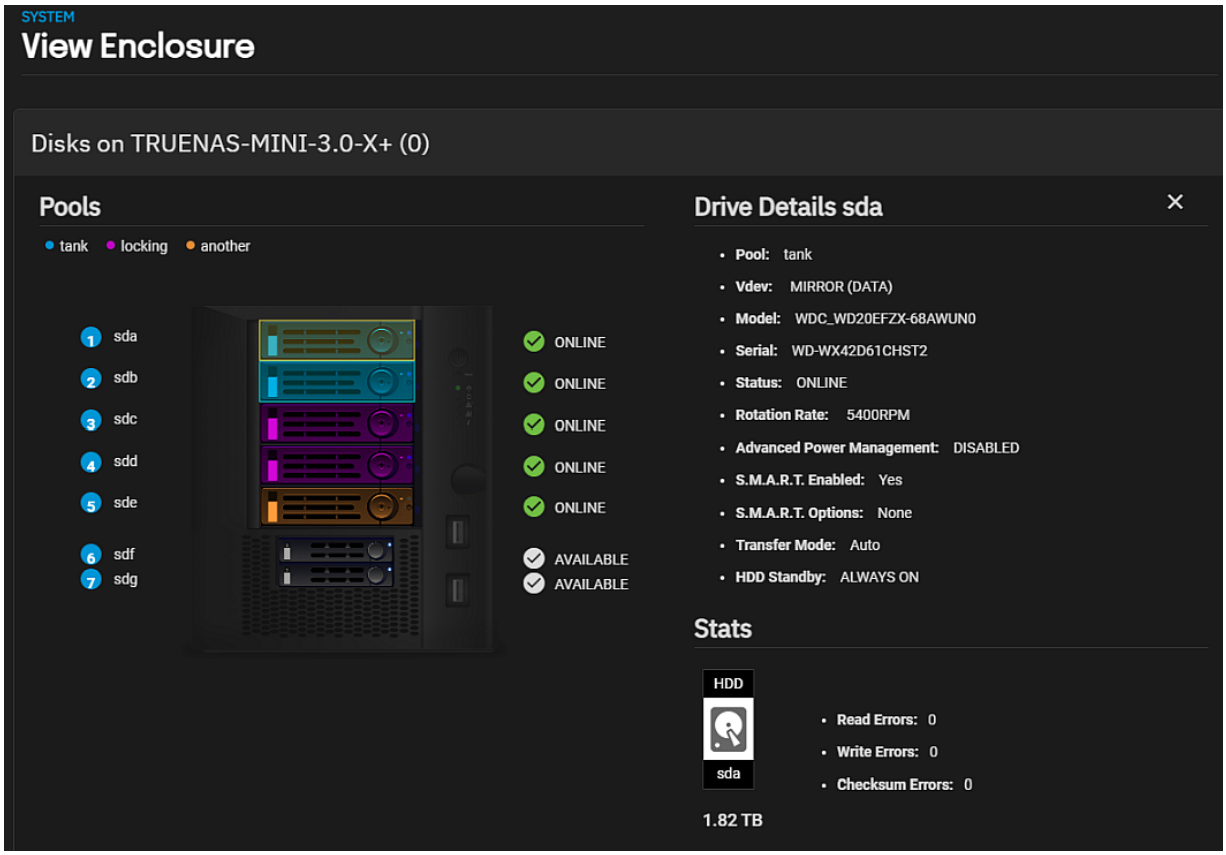
Click on **Edit Label** to open the **Change Enclosure Label** window. Type a name or description for the system and click **Save** to apply the label. Select **Reset to Default** to restore the default name for the system.

Mini Enclosure Screen Example

TrueNAS Mini systems only display the front view of the system hardware.

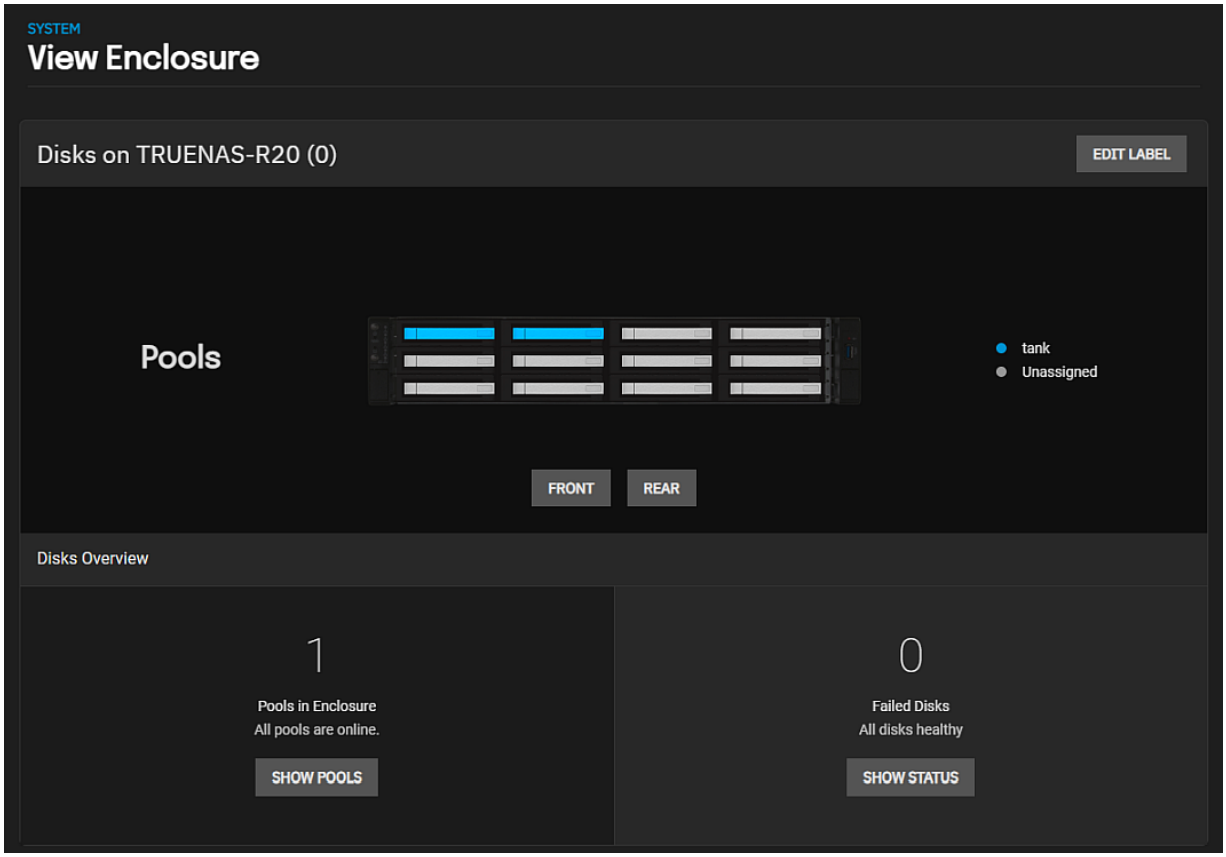


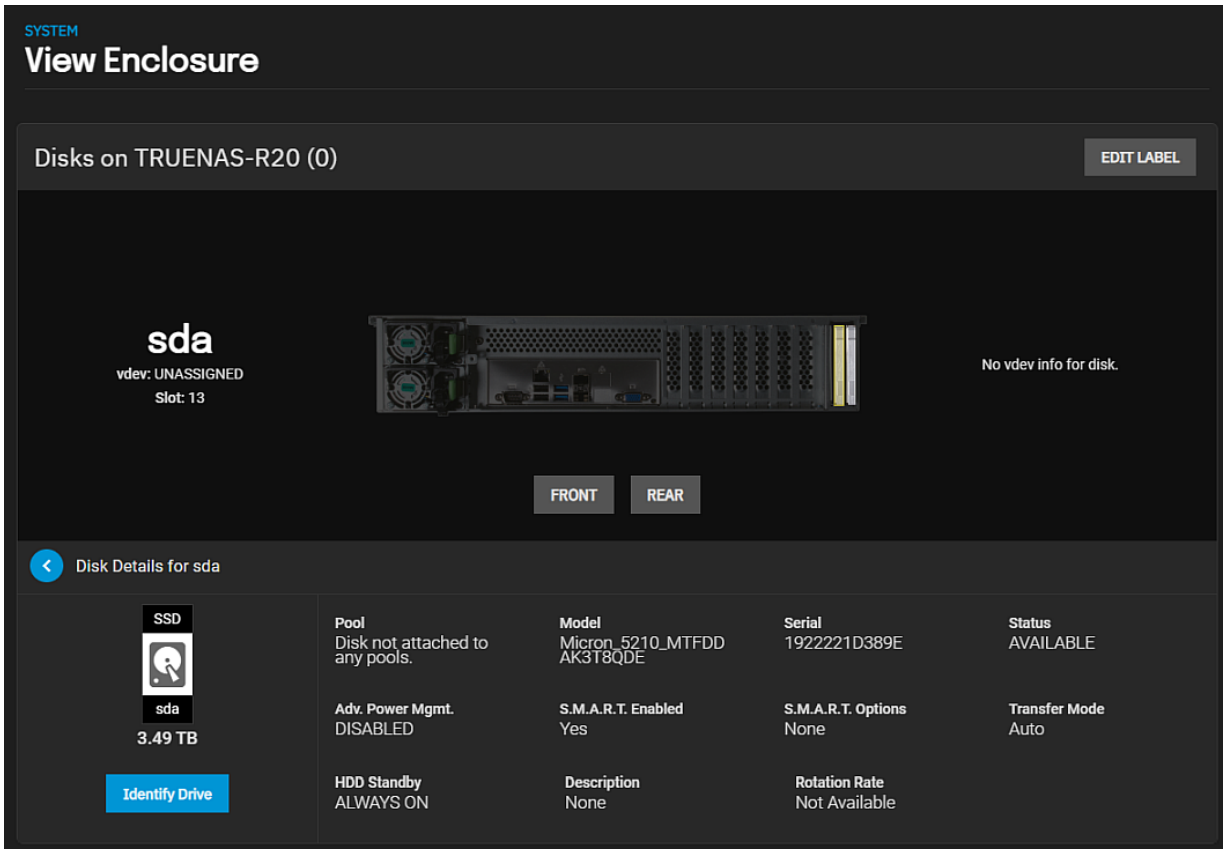
Pool information displays at the top of the screen. The drive bay number and disk label displays to the left of the image and the status to the right of the image. Select a disk to show details for that drive. The **Disk Overview** section provides general details on the system drive hardware and capacity. The **Drive Temperatures** displays current readings for each drive in the system.



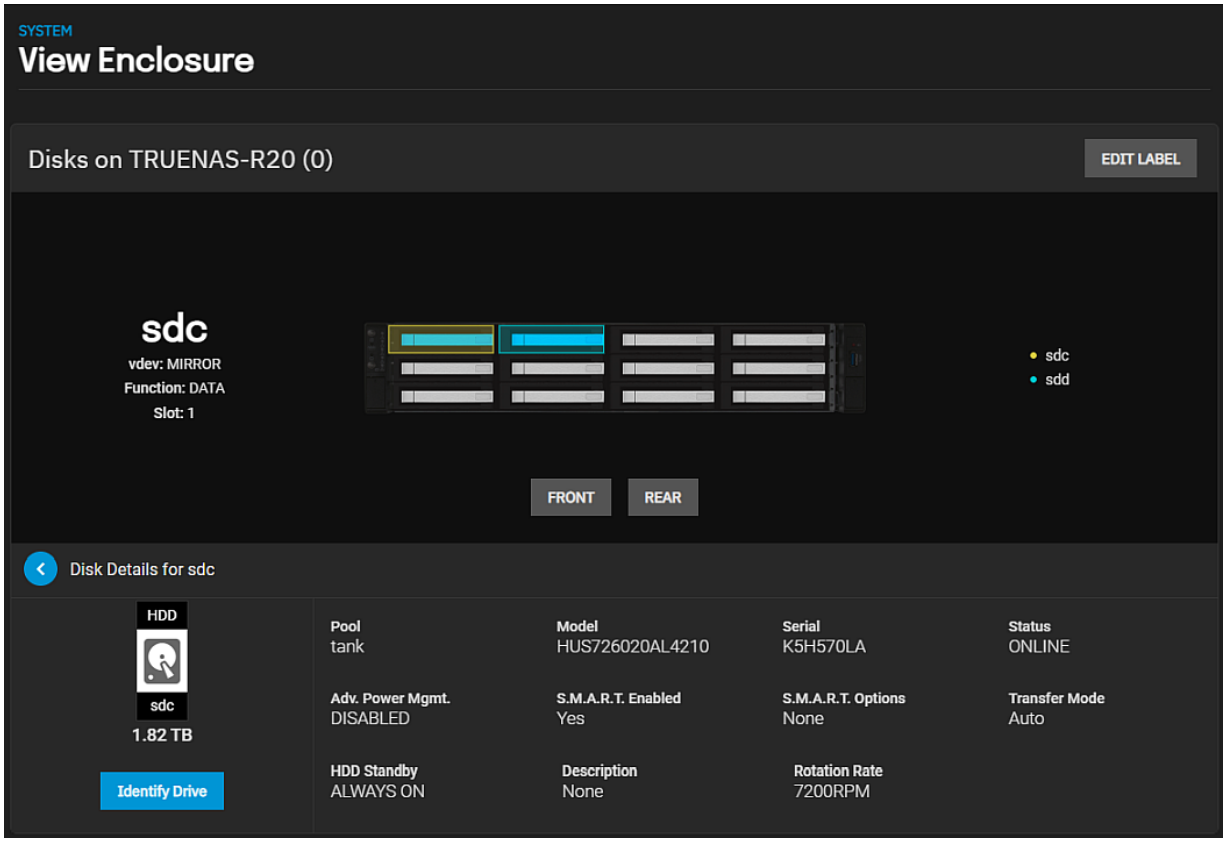
R20 Enclosure Screen Examples

Larger TrueNAS hardware system images include a front and rear view of the chassis to show all drive bays and installed disk drives.





Click on a drive to display details for that selected drive and to access the **Identify Drive** option.



Identify Drive helps you identify which physical drive bay corresponds to the SCALE identification number for that drive. Select the drive, click **Identify Drive** and go to the location of the system server to locate the drive bay with the LED indication turned on to identify the physical drive that corresponds to the software drive location.

Disk details include the pool, drive model and serial number, status, and other options for the selected drive.

Related Content

Related Disks Articles

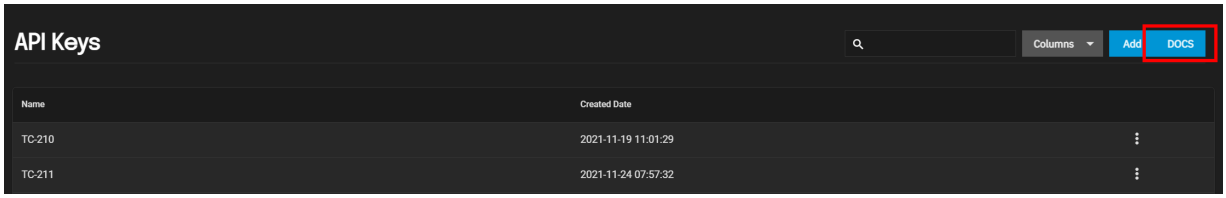
- Advanced Settings Screen
- Disks Screens
- Managing Disks
- Importing Disks
- Managing SEDs
- Replacing Disks
- Wiping a Disk
- SLOG Over-Provisioning

Related Pools Articles

- Dashboard
- Managing Advanced Settings
- Advanced Settings Screen
- Setting Up Permissions
- Storage Encryption
- SLOG Over-Provisioning
- Fusion Pools

5 - SCALE API

You can access TrueNAS SCALE API documentation in the web interface by clicking **> API Keys > DOCS**.



Alternatively, append `/api/docs/` to your TrueNAS hostname or IP address in a browser to access the API documentation.

For convenience, we store static builds of the current 2.0 API documentation on the Docs Hub:

- Websocket Protocol
- RESTful

SCALE Documentation Sections

TrueNAS SCALE documentation is divided into several sections or books:

- The Getting Started Guide provides the first steps for your experience with TrueNAS SCALE:
    - Software Licensing information.
    - Recommendations and considerations when selecting hardware.
    - Installation tutorials.
    - First-time software configuration instructions.
- Configuration Tutorials have many community and iXsystems -provided procedural how-tos for specific software use-cases.
- The UI Reference Guide describes each section of the SCALE web interface, including descriptions for each configuration option.
- API Reference describes how to access the API documentation on a live system and includes a static copy of the API documentation.
- SCALE Security Reports links to the TrueNAS Security Hub and also contains any additional security-related notices.

6 - SCALE Security Reports

TrueNAS SCALE is not currently an enterprise release. We only recommended SCALE for early adopters who have a backup plan.

The SCALE 22.02 Security report is available here.

SCALE Documentation Sections

TrueNAS SCALE documentation is divided into several sections or books:

- The Getting Started Guide provides the first steps for your experience with TrueNAS SCALE:
    - Software Licensing information.
    - Recommendations and considerations when selecting hardware.
    - Installation tutorials.
    - First-time software configuration instructions.
- Configuration Tutorials have many community and iXsystems -provided procedural how-tos for specific software use-cases.
- The UI Reference Guide describes each section of the SCALE web interface, including descriptions for each configuration option.
- API Reference describes how to access the API documentation on a live system and includes a static copy of the API documentation.
- SCALE Security Reports links to the TrueNAS Security Hub and also contains any additional security-related notices.

7 - SCALE 22.12 Bluefin Release Notes

While the current version of TrueNAS SCALE receives maintenance updates, the next major version is in active development. This article collects various details about this upcoming major version: early release notes, developer notes, and how to help test the in-development version. This is a work in progress and details are added as development progresses on this SCALE release.

> Early releases are intended for testing and early feedback purposes only. Do not use early release software for critical tasks.

Want to get involved by collaborating on TrueNAS SCALE? Join our Official Discord Server.

Software Lifecycle

TrueNAS Quality Lifecycle

Release Stage	Completed QA Cycles	Typical Use	Description
NIGHTLY	0	Developers	Incomplete
ALPHA	1	Testers	Not much field testing
BETA	2	Enthusiasts	Major Feature Complete, but expect some bugs
RC	4	Home Users	Suitable for non-critical deployments
RELEASE	6	General Use	Suitable for less complex deployments
U1	7	Business Use	Suitable for more complex deployments
U2+	8	Larger Systems	Suitable for higher uptime deployments

> The Software Status page shows the latest recommendations for using the various TrueNAS software releases.

SCALE Schedule

> All release dates listed are **tentative and are subject to change**. The items in this list might not show every deadline or testing cycle that iXsystems uses to manage internal effort.

The progress and specific work is being tracked through tickets opened in Jira. If you have a feature suggestion or bug report, create a Jira account and file a ticket in the TrueNAS or TrueCommand projects. TrueNAS SCALE tickets are also tracked in the TrueNAS Jira Project.

Version	Checkpoint	Scheduled Date
SCALE 22.12.RC.1	Code-freeze	26 October 2022
SCALE 22.12.RC.1	Internal Testing Sprints	31 October 2022 - 11 November 2022
SCALE 22.12.RC.1	Tag	14 November 2022
SCALE 22.12.RC.1	Release	15 November 2022
SCALE 22.12.0	Code-freeze	23 November 2022
SCALE 22.12.0	Internal Testing Sprints	24 November 2022 - 09 December 2022
SCALE 22.12.0	Tag	12 December 2022

Version	Checkpoint	Scheduled Date
SCALE 22.12.0	Release	13 December 2022
SCALE 22.12.1	Code-freeze	18 January 2023
SCALE 22.12.1	Internal Testing Sprints	19 January 2023 - 03 February 2023
SCALE 22.12.1	Tag	06 February 2023
SCALE 22.12.1	Release	07 February 2023

Obtaining the Release

To download an .iso file for installing SCALE Bluefin, go to https://www.truenas.com/truenas-scale/ and click **Download**. Manual update files are also available at this location.

To upgrade an existing SCALE install, log in to your SCALE web interface and go to **System Settings > Update**.

> SCALE is developed as an appliance that uses specific Linux packages with each release. Attempting to update SCALE with `apt` or methods other than the SCALE web interface can result in a nonfunctional system.

22.12-RC.1

November 15, 2022

TrueNAS SCALE 22.12-RC.1 has been released and includes many new features and improved functionaltiy. SCALE 22.12-RC.1 features include:

- Adds FIPS-validated SSL module (Enterprise Only)
- Adds the R50M to the Enclosure screen
- Adds USB passthrough support and allows users to specify USB vendor/product IDs in the UI
- Adds increased functionality in the new Storage screens that include overprovisioning on zpool creation and the ability to see the full name for datasets with long names
- Adds support for creating S3 buckets in Cloud Sync Backups
- Updates Kubernetes to 1.25 and Samba to 4.17.0.rc5

> SCALE 22.12-RC.1 introduces a change in Applications. Users upgrading to 22.12-RC.1 now use the Docker overlay2 driver instead of ZFS. This change brings a considerable performance boost to applications but applications installed in 22.12-RC.1 are incompatible with any previous version of SCALE 22.12.

22.12-RC.1 Change Log

Epic

- NAS-110327 WebUI Refactoring
- NAS-116607 FIPS Validated SSL Module (Enterprise Only)

New Feature

- NAS-109036 OverlayFS support for docker on zfs
- NAS-116558 `special_small_block_size` dataset option is inheritable
- NAS-117028 Offline/errored out pools on new storage pages
- NAS-117236 Check for keyboard support on new storage pages
- NAS-117302 Integrate overprovisioning on zpool creation on SCALE
- NAS-118325 Add USB passthrough support in the UI
- NAS-118446 add MISMATCH_VERSIONS to webUI
- NAS-118505 R50BM needs to be added to webUI codebase
- NAS-118593 Update kubernetes to 1.25 and related deps
- NAS-118642 Allow users to specify USB vendor/product id in UI
- NAS-118701 add new public endpoint to return whether or not truenas is clustered
- NAS-118749 Branchout mirrors for RC1
- NAS-118923 Fix broken k3s build

Improvement

- NAS-111509 Empty job field on replication task after failover
- NAS-111781 VMware snapshot improvements
- NAS-116286 Rework ZFS Log Size Limit
- NAS-116557 Ensure that users have ability to view full dataset names in storage form in webui
- NAS-116675 Add info about RSS support to interfaces API
- NAS-117837 disk.get_unused should maybe include info from ID_FS_LABEL in output
- NAS-117958 Fix chart colors on different themes
- NAS-118073 Update samba to 4.17.0.rc5 in nightlies
- NAS-118077 Add python bindings for libwbclient
- NAS-118088 Publish unit tests workflow for SCALE master branch

- NAS-118101 Function clean up for Datasets module
- NAS-118134 Add CTDB mutex helper using libgfapi-python
- NAS-118176 Support creating S3 Buckets in CloudSync Backups
- NAS-118213 Wireframes: Apps Available and Apps Discovery
- NAS-118256 Wireframes: App Install Form
- NAS-118301 investigate removing docker on zfs
- NAS-118335 Make spinners look the same across the app
- NAS-118341 libzfsacl - add function to convert ZFS ACL to string
- NAS-118387 USB passthrough should allow USB VID/PID and dynamic location
- NAS-118390 Refactor `UpdateComponent` to use ix-form
- NAS-118394 implement get_real_filename_at_fn() in vfs_shadow_copy_zfs in Samba 4.17
- NAS-118408 Type safety/linter improvements
- NAS-118411 Fix swatch colour in space-management-chart
- NAS-118420 Extract user/group deletion dialog forms
- NAS-118432 Acpidump on scale
- NAS-118480 Do not spam daemon logs with kube-router logs
- NAS-118493 need integration tests for middleware port validation
- NAS-118499 Extract some VM dialogs into separate components
- NAS-118514 Remove DocReplaceService
- NAS-118526 Partially enable no-restricted-syntax
- NAS-118543 Provide better indication when user password is set
- NAS-118545 Make Dataset Space Management chart smaller
- NAS-118612 Linter for attribute order in html
- NAS-118662 Remove `any` in chart-form.component
- NAS-118668 Remove usages of any
- NAS-118677 Implement jest eslint rules
- NAS-118683 Extract some dialogs into separate components
- NAS-118692 Whitelist Rsync Module in docker host path validations
- NAS-118699 Use snack bar to inform users about success actions
- NAS-118737 Whitelist cloud sync tasks in docker host path validation
- NAS-118783 update SCST with upstream

Bug

- NAS-107288 GUI slow/consuming GBs of RAM with large number of datasets (10k)
- NAS-110305 report page graphs no scroll back
- NAS-112088 Don’t do validation on empty textboxes if they are not set required: true.
- NAS-112650 Onedrive for Business
- NAS-114884 WebUI - displayed reorder & configure buttons on the other pages not dashboard
- NAS-115225 “client certificate chain could not be verified with specified root CA.”
- NAS-115869 NTP service broken when DHCP provides NTP servers.
- NAS-115943 3080 GPU not detected / won’t install
- NAS-116495 Run blocking calls in threads in sysdataset plugin
- NAS-116526 Enabling the wrong PCI Passthrough bricked host SCALE
- NAS-116537 Replace disk dialog does not include any identifying information about the disk
- NAS-116716 [SCALE] OpenEBS failing to start after update
- NAS-117316 [SCALE] Prevent user from deploying app with port conflicts
- NAS-117392 Add clustered time health check
- NAS-117473 Scrub causes system to be unresponsive
- NAS-117935 Rootless login: local authentication and authorization
- NAS-117941 Error when going to datasets after removing all pools
- NAS-118011 On TrueNAS SCALE, when performing GPU passthrough with high-memory cards QEMU options are required
- NAS-118177 Storj integration doesn’t work with existing accounts
- NAS-118210 webUI making unnecessary calls on reporting page
- NAS-118244 Pool creation silently fails on former MDRAID disks
- NAS-118255 Scale UI shows all VMs in stopped state, but they are running
- NAS-118290 [SCALE] Apps logs, keep repeating every few seconds
- NAS-118291 Data Protection - Replication Tasks - Snapshot Retention
- NAS-118305 Changing network settings in CLI on initial install
- NAS-118327 Restore Angular loading indication
- NAS-118328 Kubernetes migration hangs if encryption is turned on
- NAS-118339 No Snapshots are shown
- NAS-118348 ZFS snapdirs stats are gathered by collectd df plugin
- NAS-118349 Fix Datasets table to cut off really long dataset names
- NAS-118354 Nextcloud on SCALE crashes when Postgres Backup Volume option is selected
- NAS-118369 recycle touch file causes SMB assertion on 4.17.0 release
- NAS-118375 UI Breaks on mobile screens if you have dataset details open and you delete the dataset
- NAS-118381 test_create_schema_formattion unit test failing
- NAS-118383 [TrueNAS SCALE-22.12-BETA.1] Config Import not working
- NAS-118421 openvpn: Options error: In [CMD-LINE]:1: Error opening configuration file: client.conf
- NAS-118423 Reporting is broken - Cannot read properties of undefined
- NAS-118428 Add upgrade strategy for storj app
- NAS-118444 add MISMATCH_VERSIONS to failover.disabled.reasons
- NAS-118447 During Select an unused disk progress-spinner is not render
- NAS-118464 `Metadata (Special) Small Block Size` on the dataset form has a null default value
- NAS-118465 Config upload error message is not displayed
- NAS-118470 Multiselect styles are broken
- NAS-118477 Cleanup all the cluster things
- NAS-118478 fix cluster smb config test

- NAS-118513 prevent swap on data drives on ix enterprise hardware
- NAS-118517 CalledProcessError dialog appears when I open /ui/storage page
- NAS-118519 webUI showing wrong HA status
- NAS-118520 WebUI elements missing from System Settings -> General page after migrating from CORE to SCALE
- NAS-118524 WebUI: Atime is displayed differently.
- NAS-118530 Advanced system settings, a few boxes appear twice
- NAS-118535 Apps stopped working
- NAS-118536 K3s not starting
- NAS-118541 Progress bar overflows jobs dialog
- NAS-118546 Disable some cloud sync buckets
- NAS-118557 Replication: Only Same as Source and None retention policies can be used with Naming regex
- NAS-118563 fix service.restart and journal sync race
- NAS-118567 Allow migrating applications when encrypted
- NAS-118573 Apps lead to deathlocks due to low inotify.max_user_watches
- NAS-118580 Remove k8s cronjobs when scaling down apps
- NAS-118583 Time Zone is right. System time is not
- NAS-118586 Fix VMware snapshot delete test
- NAS-118594 Avoid unnecessary avahi reload_config() calls
- NAS-118599 Do not expose MIXED case sensitivity as user choice
- NAS-118614 Cloud tasks for Move and Sync transfer mode reverts to Copy
- NAS-118616 SMB Share Option Edit FilesystemACL Opens Main Dashboard Not the Edit Filesystem ACL Configuration Form
- NAS-118624 Remove unnecessary freebsd rc files in scale
- NAS-118627 Employ new method of testing if storj bucket is related to iX as conf…
- NAS-118628 Rework UI for replacing an unavailable disk
- NAS-118635 (py-libzfs) zed core dump after merging zfs-2.1.6 patchset
- NAS-118695 [SCALE] k3s crash loop
- NAS-118697 (openzfs) zed core dump after merging zfs-2.1.6 patchset
- NAS-118765 SMB Share ACLs do not open/work on TrueNAS Scale 22.12-BETA.2
- NAS-118782 Update samba to 4.17.2
- NAS-118856 SCALE nightlies includes kernel modules for wrong kernel
- NAS-118949 pywbclient - Fix refcounting on PyUidGid class init error path

Notice

MinIO has removed backwards compatibility with version 2022-10-24_1.6.58.

MinIO fails to deploy if you update your version 2022-10-24_1.6.58 Minio app to 2022-10-29_1.6.59 or later using the TrueNAS web UI. Use the app roll back function and return to 2022-10-24_1.6.58 to make your MinIO app functional again. See the MinIO Migration documentation to manually update your MinIO app to the latest version without losing functionality.

22.12-BETA.2

22.12-BETA.2

October 18, 2022

TrueNAS SCALE 22.12-BETA.2 has been released and includes many new features and improved functionaltiy. SCALE 22.-BETA.2 features include:

- Removes old Storage pages, renames storage modules, and makes minor improvements to storage pages
- Adds the offical Filecoin application to the Apps catalog

22.12-BETA.2 Change Log

New Feature

- NAS-118403 Branchout for BETA2
- NAS-118325 Add USB passthrough support in the UI
- NAS-118303 Need to add new reasons to FailoverDisabledReason enum in webUI
- NAS-118270 Remove old storage pages
- NAS-118209 Hold option for snapshots
- NAS-118147 Refactor html components, improve readability and restructure Input, Output priorities
- NAS-118068 Add R50BM to enclosure mapping code and to keyserver
- NAS-118050 Research usage stats for Apps Redesign
- NAS-118037 Fix out of bounds text for the Apps page
- NAS-118036 Add Ukrainian UA Translations to the APP | 22.12
- NAS-117938 Rename storage modules
- NAS-117867 Roles card sometimes doesn't match roles cell
- NAS-117827 New cloud sync provider: "Storj iX" (13 and Angelfish)
- NAS-117813 Improve indication for which apps use dataset
- NAS-117812 Minor updates to storage pages
- NAS-117754 Fix font rendering
- NAS-117491 Improve error handling in new storage pages
- NAS-117474 Replace sticky search with sticky table headers in Datasets
- NAS-117427 Fix out of bounds text for the new disks and datasets page
- NAS-116194 Review and break down the tasks required to restructure and refactor the storage page

- NAS-110516 Storage → (cog) → Snapshots: New column “retention”

Improvement

- NAS-118526 Partially enable no-restricted-syntax
- NAS-118514 Remove DocReplaceService
- NAS-118499 Extract some VM dialogs into separate components
- NAS-118480 Do not spam daemon logs with kube-router logs
- NAS-118466 Create RootPath enum with MNT variable to avoid strings ‘/mnt’ in code
- NAS-118432 Acpidump on scale
- NAS-118420 Extract user/group deletion dialog forms
- NAS-118412 Pool process modal width depends on content [width jumping]
- NAS-118411 Fix swatch colour in space-management-chart
- NAS-118387 USB passthrough should allow USB VID/PID and dynamic location
- NAS-118364 `make reinstall` of middleware should apply systemd unit changes
- NAS-118334 ScreenType across APP => make sure we use `enum` and use in .html instead of just string
- NAS-118333 App Icons improvements & text colors near icons
- NAS-118273 Refactor some dialog components into separate components
- NAS-118269 Improve UI layout on forms, chips
- NAS-118262 Improvements for Boot Pool Status page
- NAS-118216 Record midclt enclosure.query in debug (Core/Enterprise/Scale)
- NAS-118198 Tuning to improve Storj / rclone performance
- NAS-118185 Reduce number of any’s
- NAS-118151 Hide Aliases section if DHCP/Autoconfiguration radio box(es) is/are checked
- NAS-118130 Upgrade rxjs
- NAS-118101 Function clean up for Datasets module
- NAS-118058 Sync [visual-ui] data on the Pool and Storage widgets
- NAS-118044 Refactor console message footer
- NAS-118041 Do not backup catalogs dataset on kubernetes backup
- NAS-118039 Clean up topbar.component
- NAS-118007 Remove BaseService
- NAS-118006 Refactor ReportsDashboard module
- NAS-118003 Refactor Cloud Sync Form to ix-forms
- NAS-117968 Add tooltips to status icons on Pools Dashboard
- NAS-117947 Add `otp_token` field when creating an SSH connection in semi-automatic mode
- NAS-117945 Invert customValidator
- NAS-117942 Code cleanup in new Storage module
- NAS-117937 Refactor AlertConfigComponent to ix-forms
- NAS-117932 Enable more linter rules
- NAS-117905 A way to indicate which “unused” disks are part of importable pools
- NAS-117892 Bump up starting range for UIDS / GIDS on SCALE and Core
- NAS-117887 hactl needs to be improved on SCALE
- NAS-117874 Handle incorrectly formatted disks
- NAS-117870 Properly handle change of an icon name at `ix-icon`
- NAS-117859 Fix sidenav bar overlapping with truenas text at the bottom
- NAS-117854 UI should add validate host path attribute in apps settings
- NAS-117848 subprocessing 16 times in main event loop on middleware startup
- NAS-117847 add endpoint to retrieve VM log files
- NAS-117846 Find a better way of handling max concurrent calls errors on storage dashboard
- NAS-117837 disk.get_unused should maybe include info from ID_FS_LABEL in output
- NAS-117836 Use new method for updating isolating gpu pci ids in UI
- NAS-117796 Don’t allow unsetting host path validation for enterprise users
- NAS-117766 Extract ix-label from ix-form components
- NAS-117759 Investigate setting permissions on /data to 0o700
- NAS-117699 add tests for copy_file_range (server-side copy) for NFSv4.2
- NAS-117618 Review pickle module usage in middlewared
- NAS-117614 middleware files in /var/run should be in dedicated run directory
- NAS-117445 Charts MinIO pod does not follow standard min.io folder structure
- NAS-117372 Add client side validation for app names
- NAS-117298 Expose timemachine_quota key if users enable time machine on share
- NAS-117261 Investigate on reducing usages of IxEntityTreeTable
- NAS-117134 Improvement for Bugclerk
- NAS-115917 use secrets module instead of random
- NAS-115636 Expose Cluster Volume Locations
- NAS-114416 Document how to start middleware in debug mode
- NAS-114415 Document how to build custom SCALE ISO
- NAS-112452 Hold option for snapshots
- NAS-111781 VMware snapshot improvements
- NAS-111464 Add who field to filesystem.get_default_acl
- NAS-100748 Remove Internet Explorer support

Bug

- NAS-118582 debug symbols for ZFS userspace tools appear to be missing in SCALE
- NAS-118576 Correctly whitelist openvpn.client/server namespace when validating port
- NAS-118575 Upgraded catalog item(s)
- NAS-118568 Avoid spamming log files with docker mounts
- NAS-118565 Fix vmware migration
- NAS-118564 fix iommu number detection

- NAS-118558 Update machinaris from 0.8.3 to 0.8.4
- NAS-118547 Fix pihole helm test failing
- NAS-118512 Cloud Sync Task can no-longer work for onedrive due to missing parameters for –checkers and –tpslimit
- NAS-118510 When staying on one page and want to directly change url by hands (to view another page), it redirects to previous page
- NAS-118508 Editing stopped app configuration starts the app
- NAS-118500 Include avahi-utils in the build
- NAS-118498 regression: file name search of samba share from macOS Finder no longer works since Core 12 to 13 upgrade
- NAS-118496 Fix docs build
- NAS-118494 Document how to fake CPU temperature reporting on a VM
- NAS-118490 Extract strings from app routes for translations
- NAS-118478 fix cluster smb config test
- NAS-118476 Override avahi hostname with hostname_virtual in HA
- NAS-118471 Unexpected directory explorer behaviour in Cloud Sync Task
- NAS-118469 call ctdb shared vol methods explicitly
- NAS-118463 VMware snapshot tests
- NAS-118459 Fix and enhance recycle test
- NAS-118452 Add git workflows for upgrade strategy / info linting
- NAS-118450 optimize zfs.{pool/dataset}.query
- NAS-118447 During Select an unused disk progress-spinner is not render
- NAS-118444 add MISMATCH_VERSIONS to failover.disabled.reasons
- NAS-118429 properly wait on job in dir services
- NAS-118428 Add upgrade strategy for storj app
- NAS-118424 Improve test_420_smb - use python SMB client
- NAS-118423 Reporting is broken - Cannot read properties of undefined
- NAS-118416 impose limit on max length of pool name
- NAS-118415 Tree select sets undefined to form element if clicked twice
- NAS-118414 Warning modal icon bug
- NAS-118413 [SCALE] openEBS crashing - CoreDNS won’t start
- NAS-118393 Apps - ‘NoneType’ object is not subscriptable
- NAS-118391 Cannot create VM - NoneType object is not subscriptable
- NAS-118384 dont block event loop in ws_can_access
- NAS-118383 [TrueNAS SCALE-22.12-BETA.1] Config Import not working
- NAS-118381 test_create_schema_formattion unit test failing
- NAS-118375 UI Breaks on mobile screens if you have dataset details open and you delete the dataset
- NAS-118373 Fix a few HA issues on SCALE
- NAS-118372 Add some more delay to fix k8s logs/exec tests
- NAS-118362 drammatically optimize retrieving drive temps
- NAS-118354 Nextcloud on SCALE crashes when Postgres Backup Volume option is selected
- NAS-118353 Fix loading for mobile screens on the Datasets page
- NAS-118352 Incorrect current train
- NAS-118351 Disable middleware debug mode being the default
- NAS-118349 Fix Datasets table to cut off really long dataset names
- NAS-118348 ZFS snapdirs stats are gathered by collectd df plugin
- NAS-118338 Avoid logging on FileNotFoundError for sysdataset
- NAS-118331 fix interface unit tests
- NAS-118330 fix m-series nvme unit test
- NAS-118329 fix validation error
- NAS-118328 Kubernetes migration hangs if encryption is turned on
- NAS-118326 Bring back VMware snapshots page
- NAS-118324 Fix build
- NAS-118305 Changing network settings in CLI on initial install
- NAS-118304 Avoid blocking calls in smb plugin
- NAS-118302 netbios_name_check_sid integration test failing on SCALE HA
- NAS-118297 Fix keyerror during idmap_create
- NAS-118296 revert 058034a092b8d1d5df55a49c2f0e65dba763e218
- NAS-118295 dont run boot_attach tests on HA VMs
- NAS-118294 move test_008_hactl to test_14_failover_related
- NAS-118291 Data Protection - Replication Tasks - Snapshot Retention
- NAS-118290 [SCALE] Apps logs, keep repeating every few seconds
- NAS-118289 fix copy and paste typo….
- NAS-118283 fix failover.disabled.reasons
- NAS-118282 Unexpected results when filtering datasets
- NAS-118278 GUI element “SSH Public Key” incorrectly named
- NAS-118267 Disallow mat-icon selector in styles
- NAS-118261 Fix `test__get_smartd_config`
- NAS-118260 Keep column in Boot Environments in confusing
- NAS-118258 Fix icon color in sidebar
- NAS-118257 fix mapping rear NVMe on M50/60 HA systems
- NAS-118252 Failed to replace route to service VIP
- NAS-118250 SMB2 not working unless SMB1 checked
- NAS-118249 dont call pool.query in vmware plugin
- NAS-118244 Pool creation silently fails on former MDRAID disks
- NAS-118243 `boot.attach`/`boot.replace`/`boot.detach` tests
- NAS-118242 `boot.replace` is a job now
- NAS-118241 Fix boot device replace
- NAS-118234 When uploading a manual update file, an accidental click outside the upload progress window cancels the entire job
- NAS-118228 Send correct label when replacing a vdev in the boot pool

- NAS-118227 Boot pool vdev replace dialog disk dropdown misses disk size
- NAS-118222 Fix keyerror in ACL template domain info lookup
- NAS-118205 Fix tests Suites
- NAS-118200 Hardcoded alert message with old Jira link
- NAS-118197 Fix k3s logs/exec issue
- NAS-118191 Initialize csource before zfs_prop_get
- NAS-118184 Fix link to create a new pool
- NAS-118178 fix typo in failover_/event.py
- NAS-118177 Storj integration doesn't work with existing accounts
- NAS-118171 rsync task remote path widget offers to select a local path
- NAS-118169 When I edit an rsync task that uses SSH connection from keychain "SSH connection" field is empty
- NAS-118168 Do not require `remotehost` when rsync task is configured using an SS…
- NAS-118167 Dashboard crashing due to `WidgetNetworkComponent` bug
- NAS-118165 Wrong width of blocks with charts after expansion the sidenav
- NAS-118164 fix AttributeError crash in update.get_trains
- NAS-118148 Translate tooltips in navigation and page title
- NAS-118146 freenas_default expiring alert cannot be removed once the certificate is deleted
- NAS-118141 allow easy checking of sha256 checksum
- NAS-118139 Catalogs need to be synced after restoring k8s backup
- NAS-118138 Fix unused disks issue
- NAS-118136 fix crash(es) in webui_auth::addr_in_allowlist
- NAS-118135 fix crash in nginx.get_remote_addr_port
- NAS-118131 fix ctdb shared volume teardown integration test
- NAS-118123 Alert in TrueNAS Scale won't go away even after clicking on "dismiss"
- NAS-118117 move gluster fuse mounts to root cgroups
- NAS-118113 [SCALE] WebUI cannot get the properties of the dataset correctly
- NAS-118111 Fix undefined name in vm/devices.cdrom.py
- NAS-118110 move fenced process to root cgroup
- NAS-118107 Application Snapshots are getting high
- NAS-118104 Allow to subscribe to events for unauthenticated users
- NAS-118103 add connect_timeout to remote client
- NAS-118098 improve failover.disabled.reasons
- NAS-118097 Allow non-coroutine to be passed to `register_hook` and executed corr…
- NAS-118094 Use libwbclient bindings
- NAS-118093 Dont block event look in check_permission hook
- NAS-118083 fix AttributeError crash in ha_permission hook
- NAS-118080 fix scale nightlies build (update collectd to 5.12.0-11)
- NAS-118078 fix test_is_outdated_alert
- NAS-118076 Switch to using vfs_ixnas for default ACL module
- NAS-118075 fix ssl integration test (typo)
- NAS-118074 (SCALE) Plugins HPE MicroServer Gen8 not working with more, than 4 Drives
- NAS-118072 Update Dataset Roles
- NAS-118071 Fix expand button indentation on datasets tree
- NAS-118065 Cannot convert stripe to mirror in UI
- NAS-118064 cache failover.hardware.detect
- NAS-118059 fix blank graphs when UPSBase plugin crashes
- NAS-118055 Add ability to configure environment variables for nextcloud application
- NAS-118053 Fix CI runs on master
- NAS-118048 remove trailing forward slash in corssl package
- NAS-118040 Introduce an internal job for retrieving catalog items
- NAS-118025 Bluefin (22.12) fails to bring up interface
- NAS-118019 Prohibit trailing spaces in ZFS dataset names
- NAS-118015 prevent blocking event loop when checking updates
- NAS-118014 fix failover.get_ips
- NAS-118013 Improve `core.bulk` documentation
- NAS-118011 On TrueNAS SCALE, when performing GPU passthrough with high-memory cards QEMU options are required
- NAS-118004 Preserve pool disks for Disk Temperature Reports
- NAS-117997 Fix hostname spelling
- NAS-117996 Inherit border width for inputs on focus
- NAS-117991 Use zfs.pool.query_imported_fast in failover.status
- NAS-117987 certificate verify failed: self signed certificate in certificate chain
- NAS-117986 Number in CPU widget looks weird on Safari
- NAS-117983 Clickable logo on mobile screens
- NAS-117973 Simplify ixDetailsHeight
- NAS-117972 No error message when trying to delete snapshot with hold
- NAS-117962 Remove freebsd services
- NAS-117959 UI Setting automatically switches to browser language
- NAS-117953 [SCALE] Arrays are getting removed when editing
- NAS-117952 [Apps] App logs dropdown, doesn't allow selecting initcontainer
- NAS-117950 mask ndctl-monitor.service
- NAS-117944 Allow passing OTP token to `keychaincredential.remote_ssh_semiautomat…
- NAS-117943 Browser navigation doesn't close slide-in
- NAS-117933 remove migrate call in make reinstall_container
- NAS-117931 Using HTTP Basic Auth will bypass 2FA
- NAS-117927 Remove dead smartctl code and fix functional tests
- NAS-117926 fix test_mountinfo unit test
- NAS-117925 Make container.prune a job
- NAS-117921 add `reinstall_container` make argument
- NAS-117917 hitting ctrl +C via OOB managemnt on truenas console menu locks up console

- NAS-117916 NFS does not start on boot
- NAS-117911 Samba Share ACL resets to Everyone when disabled and re-enabled
- NAS-117903 CPU Usage graph key shows incorrect values when zooming
- NAS-117902 [SCALE]: show_if '!=' does not work, but '=' does work.
- NAS-117901 Optimize Zpool related alerts
- NAS-117897 webUI isn't showing what controller the alert was generated on
- NAS-117895 CRITICAL ERROR ON UPDATE TrueNAS-22.02.0.1 -> TrueNAS-22.02.3
- NAS-117890 Truecharts Applications failing to deploy due to snapshot task on latest bluefin nightly
- NAS-117872 License Apps and VMs for Enterprise (Backend)
- NAS-117871 Hide/Disable Apps and VMs based on License for Enterprise (UI)
- NAS-117857 WebUI shell breaks on long strings
- NAS-117853 UI should not specify path attribute when zvol is being created for disk based vm devices
- NAS-117843 cli app container config prune failed
- NAS-117831 Update on disk GRUB configuration for serial
- NAS-117800 Systemd Services fail
- NAS-117794 /etc/resolv.conf in Live ISO's filesystem.squash contains development information
- NAS-117777 Unable to join active directory if SMB is not started first
- NAS-117752 Unable to boot into previous boot environment
- NAS-117748 Application States incorrectly reports available update
- NAS-117747 vm.stop services do not stop
- NAS-117736 Installed chart in TrueNAS SCALE gives Middleware error
- NAS-117722 After migrating Core to Scale, cannot resilver boot mirror
- NAS-117715 [SCALE] Data Protection pages is broken
- NAS-117710 ZFS space efficiency on devices with huge physical blocks
- NAS-117708 Wireguard setup stuck in loop if wireguard connection is not established with cloud
- NAS-117688 Cannot Edit VMs
- NAS-117674 Pool import fails randomly
- NAS-117658 TrueNAS-SCALE-22.02.4-MASTER-20220805-041141 can't start VMs after importing old config or upgrading from 22.02.3 or earlier
- NAS-117653 GUI allows creation of SMB shares for nonexistent paths
- NAS-117631 Retrieve and display metadata for a single snapshot
- NAS-117599 Installing netdata gets stuck at 75%
- NAS-117508 SCALE ACL inheritance not working when migrated from POSIX to NFSv4
- NAS-117464 Network widget does not show active interface
- NAS-117409 Unable to isolate GPU or see in apps in SCALE.
- NAS-117379 WS-Discovery Name not using specified hostname
- NAS-117316 [SCALE] Prevent user from deploying app with port conflicts
- NAS-117230 A pool scrub shows up twice in task manager
- NAS-117104 PiHole Docker Install
- NAS-116678 Refuse to download update if insufficient space avail
- NAS-116539 TrueNAS CLI does not provide a pager mechanism
- NAS-116537 Replace disk dialog does not include any identifying information about the disk
- NAS-116495 Run blocking calls in threads in sysdataset plugin
- NAS-116318 SQL unique constraint error when incorrectly editing an idmap
- NAS-115737 Space in Pool Name / Path to Zlog kills iSCSI
- NAS-115648 Low Encryption Performance on Atom Processors
- NAS-115586 Enable `pool.replace_disk` tests
- NAS-115238 Removed drive from pool does not degrade pool status (SCALE)
- NAS-113889 Remove Microsoft Account in User
- NAS-113216 New dataset does not inherit ACL Type from Pool's root dataset.
- NAS-112650 Onedrive for Business
- NAS-112326 Deprecate and remove "media" user and group
- NAS-112088 Don't do validation on empty textboxes if they are not set required: true.
- NAS-111962 "Not an interger" error in Transfers field in Sync Cloud task
- NAS-110795 Can't create unencrypted dataset on Encrypted pool

22.12-BETA.1

22.12-BETA.1

September 13, 2022

TrueNAS SCALE 22.12-BETA.1 has been released and includes many new features and improved functionality. SCALE 22.12-Beta.1 features:

- Redesign of Storage web UI including new dashboards for Storage, Pools, Dashboards, Devices and other storage related areas
- Storj iX Cloud Sync backup solution now available.
- Apps improvements including adding Storj to the official catalog and adding a default Apps catalog exclusive for Enterprise customers (SCALE 22.12-Beta.1)
- STIG hardening through limiting web login and API access by restricting access for non-approved IP addresses and ranges. Additional STIG hardening through disabling root login access and tying user to API ACLs (target SCALE 22.12-Beta.2).
- Enclosure management for all iXsystems platforms
- Improved clustering over the Angelfish clustered SMB (aka Windows storage).

Additional feature in future Bluefin releases:

- Applications improvements include:
  - Add bulk upgrade action for selected apps (target SCALE 22.12-RC.1)
  - Add new Apps widget (target SCALE 22.12-RC.1)
  - Add a better Apps directory (target SCALE 22.12-RC.1)
  - Improve and simplify the app installation process (22.12-RC.1)
- FIPS validated SSL Module for SCALE Enterprise (target SCALE 22.12-RC.1)
- Replacing gluster node API (target SCALE 22.12-RC.1)
- FIPS 140-3 Level 1 Compliant Crypto Module for Enterprise Only using CorSSL module as a replacement for OpenSSL (target SCALE 22.12-RC.1)
- Add disk count scalability that includes improved boot time (targe SCALE 22.12-RC.1)
- Replacing nodes (target SCALE 22.12-RC.1)
- High-Availability Active/Standby (target SCALE 22.12 release)
- Improved TrueNAS feedback system (target SCALE 22.12 release)
- Support for Enterprise and Pro license keys (target SCALE 22.12 release)

22.12-BETA.1 Change Log

Epic

- NAS-116606 Storj iXsystems Backup Solution
- NAS-114484 Storage Page Redesign
- NAS-111233 WebUI Unit Tests
- NAS-110834 WebUI Code Cleanup

New Feature

- NAS-117909 Branch out for 22.12 BETA1
- NAS-117820 Hide unused resources card
- NAS-117813 Improve indication for which apps use dataset
- NAS-117734 Handle nulls in disk temperatures
- NAS-117676 New cloud sync provider: “Storj iX”
- NAS-117628 Dataset quota is not shown
- NAS-117615 Hide Add Datasets / Add Zvol buttons on zvols
- NAS-117573 Pre-filter data protection items when clicking on Manage links
- NAS-117572 Handle empty states better on new storage pages
- NAS-117566 Add support for snapdev
- NAS-117558 Fix loading progress on storage pages
- NAS-117520 Reimplement disk health card
- NAS-117510 Extract dashboard pool loading into a separate store
- NAS-117492 Adds tests to DatasetDetailsCardComponent
- NAS-117475 Group disks in Unassigned disks dialog
- NAS-117407 Clean up `pool.dataset.query` calls in the new `Datasets` module
- NAS-117405 Fix IxDynamicFormItemComponent tests
- NAS-117383 investigate adding io type to VM devices
- NAS-117368 Add missing attributes to `pool.dataset.details` response
- NAS-117365 Extract device loading into a separate store
- NAS-117348 Make request to `pool.dataset.details` on the Datasets Management page
- NAS-117323 Implement the click action for “Add vDev” button on the Device Management page
- NAS-117321 Adopt new datasets API
- NAS-117319 Allow vdevs to be selected in Devices
- NAS-117317 Smaller fixes for Storage pages
- NAS-117302 Integrate overprovisioning on zpool creation on SCALE
- NAS-117253 Add loading indication to storage dashboard
- NAS-117239 2 new endpoints for webUI network changes
- NAS-117235 Test new storage pages in different browsers
- NAS-117216 Fix card scaling in storage dashboard
- NAS-117212 Show auto trim value in ZFS Health Card
- NAS-117203 Separate the dataset capacity management form from the dataset edit form
- NAS-117177 Finish Space Management Card
- NAS-117082 Better loading indication for datasets and devices
- NAS-117024 Fix the column layout of details panel for the storage redesign pages
- NAS-117023 Investigate the “Mirror XYZ” row on the Devices table
- NAS-117021 What should the “Add VDEV” button do on the Device Management page
- NAS-117019 Which cards should be removed under certain conditions for the Dataset Management page
- NAS-117017 Investigate the conditions for Encryption card on Dataset Management page
- NAS-117015 Icon for ‘Locked by parent’
- NAS-116964 Add URL support to Devices tree view
- NAS-116916 Add details to the IxTreeTable on the Devices page
- NAS-116915 Add the pool header row on Datasets IxTreeTable
- NAS-116807 Synchronize storage design changes
- NAS-116806 Design for Dataset Capacity Management
- NAS-116788 Create the Dataset Capacity Management Card chart
- NAS-116715 Review and fix card sizes for storage redesign pages
- NAS-116635 Storj App in Official Catalog
- NAS-116413 Device Management Page
- NAS-116411 Information for different roles attached to a dataset or child datasets
- NAS-116410 The Roles details Card/Widget
- NAS-116406 Data Protection Card/Widget
- NAS-116403 Dataset Management Page

- NAS-116397 Disk Health card
- NAS-116393 Pool Topology details widget/card
- NAS-116391 Single Pool details component on Pools dashboard
- NAS-116389 Create Pools Dashboard
- NAS-114198 Advanced boot options for SCALE (udev rules and kernel parameters)
- NAS-111020 Assigning Host USB device to a Guest VM in SCALE
- NAS-102765 Ask for EC2 Instance ID when setting initial root password

Improvement

- NAS-117841 Ban `res` as variable name
- NAS-117803 Blank dashboard of the first login
- NAS-117802 Use truenas tls endpoint for usage stats
- NAS-117775 Update kubernetes related dependencies from upstream
- NAS-117769 Add support for multi selection in ix-explorer
- NAS-117719 Do not run CI checks when only RE tests were changed
- NAS-117707 Merge zfs-2.1.6-staging
- NAS-117704 Enforce linting rules in CI
- NAS-117699 add tests for copy_file_range (server-side copy) for NFSv4.2
- NAS-117696 Update bluefin nightlies mirrors
- NAS-117646 Reduce amount on any's
- NAS-117634 Refactor bootenv-status.component
- NAS-117614 middleware files in /var/run should be in dedicated run directory
- NAS-117606 Refactor Alert Services to ix-forms
- NAS-117595 Add webdav shares to the `pool.dataset.details`
- NAS-117576 Optimize calls on Storage pages
- NAS-117574 Update Roles column on Datasets page
- NAS-117540 Select the correct pool on datasets page when clicking on "Manage Datasets" on Pools Dashboard
- NAS-117539 Make the first row of table selected state when Datasets page first loads
- NAS-117528 ctdb.public.ips.interface_choices require interfaces with an IP
- NAS-117445 Charts MinIO pod does not follow standard min.io folder structure
- NAS-117401 In UI allow users to set trust_guest_rx_filters for NIC device in VMs
- NAS-117398 Add Storj as Cloud Sync service
- NAS-117385 options.only_cached: Field was not expected when calling disk.temperatures
- NAS-117372 Add client side validation for app names
- NAS-117371 Make `type` field in pool topology and boot.get_state similar
- NAS-117366 Disable `patch` status check from codecov
- NAS-117363 Split Vdev type into separate types
- NAS-117354 Change AD cache setting label
- NAS-117333 UX: Wrong lock icons on datasets table
- NAS-117308 Minor improvements to pool.dataset.details endpoint
- NAS-117301 UX Remove redundant close icon on VM>Devices page
- NAS-117299 less expensive chart.release.query endpoint
- NAS-117279 Please add provisioning info to pool.dataset.query
- NAS-117269 failover.disabled_reasons returns a new NO_FENCED that webUI needs to account for
- NAS-117255 Add units tests for Dataset Capacity Management Card
- NAS-117233 New Google Cloud Storage task field: bucket_policy_only
- NAS-117221 Improvements for custom icons
- NAS-117215 IPv6 NDP doesn't work by default on VMs
- NAS-117198 Enable linter rule no-trailing-spaces
- NAS-117172 webui should use filesystem.acltemplate APIs for presenting templates to users
- NAS-117119 Change loading animation in permissions card
- NAS-117108 Find a different way of hiding dynamic controls other than disabled
- NAS-117041 CLONE - Allow custom Management URLs for Apps
- NAS-116905 ZFS scrub performance optimizations
- NAS-116902 Expose ZFS dataset case sensitivity setting via sb_opts
- NAS-116838 Add a query-option for pool.dataset.query to join dataset alerts with results
- NAS-116755 Reword label for ACL types in SCALE permission editor
- NAS-116736 Expand information available in simple dataset handles is libzfs snapshot iterator
- NAS-116685 Add file size to manifest.json
- NAS-116675 Add info about RSS support to interfaces API
- NAS-116570 Refactor CloudCredentialsFormComponent
- NAS-116482 Investigate whether to expose zvol snapdev
- NAS-116375 Locate source of periodic writes to boot-pool and minimize
- NAS-116343 Refactor bootenv-list.component to ix-tables
- NAS-116138 Implement validation for Interface name
- NAS-115959 User Feedback Service API
- NAS-115620 Use newer nft tables syntax for failover iptables plugin
- NAS-113922 gluster volume deletion integration tests
- NAS-113681 Add support for prefer-as-const for class members
- NAS-113183 Add loading state for ix-select/ix-combobox
- NAS-112616 Enable prefer-early-return
- NAS-112047 Investigate quiescing of VMs and Pods (PVCs?) during snapshot
- NAS-111488 Implement disk_resize equivalent in SCALE
- NAS-111356 network settings general improvements
- NAS-108490 Add nvdimm related management tools

Bug

- NAS-118080 fix scale nightlies build (update collectd to 5.12.0-11)
- NAS-118048 remove trailing forward slash in corssl package
- NAS-117992 VM not created in SCALE 22.12-BETA.1 testing
- NAS-117987 certificate verify failed: self signed certificate in certificate chain
- NAS-117931 Using HTTP Basic Auth will bypass 2FA
- NAS-117889 fix KeyError in pool.dataset.details
- NAS-117886 Fix `Manage Datasets` button link on the `Pools Dashboard`
- NAS-117885 Shift winbindd_cache.tdb path in middleware
- NAS-117877 Improve KDC detection during domain join
- NAS-117868 Do not run post stop actions if VM is suspended
- NAS-117865 Fix timeout during idmap updates
- NAS-117864 Fix edge case for k8s node ca
- NAS-117860 Ensure that we always have a valid krb5.conf during AD start
- NAS-117858 relax zfs_space VFS object validation
- NAS-117852 Fix path behaviour when disk type vm device is created
- NAS-117842 fix creating/updating bonds
- NAS-117840 Remove customized nss-pam-ldap from build
- NAS-117829 fix failover.disabled.reasons….again
- NAS-117825 Remove python nslcd client
- NAS-117823 Restore loading indication on Storage pages
- NAS-117806 update network configuration domain to match AD one
- NAS-117801 Add some explicit tests for firstboot
- NAS-117795 Move replace-disk-dialog to storage2
- NAS-117789 Errors in ix-page-title-header on one pages disable header on all pages
- NAS-117779 Enforce passwd/group specified reference files
- NAS-117777 Unable to join active directory if SMB is not started first
- NAS-117776 Clean chroot mounts when making update image
- NAS-117768 undefined in filter box on some pages
- NAS-117762 Build with BlueFin with Samba 4.17
- NAS-117761 fix typo of nft fw rules for SCALE HA
- NAS-117755 * [SCALE] Downloading Logs from VMs is not working
- NAS-117749 Unable to select “category” when submitting a bug report from TrueNAS Scale 22.02.3
- NAS-117745 Add AMD NTB driver to the build as a module.
- NAS-117735 Only break out of fuse mount loop early on success
- NAS-117728 Shift timeouts to a single dict for cluster tests
- NAS-117727 NaN in disk.temperature_agg
- NAS-117725 Deleting cluster does not wipe the ctdb_shared_vol brick / dataset causing many issues on new create
- NAS-117723 FIPS self test failure broke installer
- NAS-117718 No pools message flashing when switching to Storage
- NAS-117716 Storj tests
- NAS-117714 FTP “Certificate” dropdown should be under “Enable TLS” checkbox
- NAS-117713 Change how API keys are created
- NAS-117700 Dashboard Config settings revert after save
- NAS-117695 use asterisk to explicitly indicate full API access
- NAS-117692 Explicitly reference min_memory
- NAS-117688 Cannot Edit VMs
- NAS-117684 Separately test basic NFS ops for version 3 and version 4
- NAS-117681 Remove overlay_dirs
- NAS-117680 Bug with Dataset Icon in Details Panel header
- NAS-117675 Add basic tests for ctdb managed services
- NAS-117673 enforce minimum zfs passphrase length
- NAS-117669 The “snapdev” field is returned in lowercase
- NAS-117661 Minor bug fix for vm plugin
- NAS-117658 TrueNAS-SCALE-22.02.4-MASTER-20220805-041141 can’t start VMs after importing old config or upgrading from 22.02.3 or earlier
- NAS-117655 Active Directory gets disabled on reboot
- NAS-117637 If middleware_OVERRIDE is specified, let’s also override truenas and truenas_files
- NAS-117635 remove unused startup_seq file
- NAS-117630 Update `test__iscsi_extent__disk_choices`
- NAS-117627 `zfs.dataset.query_for_quota_alert` returns only top-level datasets
- NAS-117625 Add “run as user” option in ix chart
- NAS-117624 No existing ZVOL images detected when creating new VM and trying to import existing zvol. Bluefin 05082022 and 100822
- NAS-117622 Add SMB client failover test for cluster
- NAS-117620 HA issue on M30 after loading SCALE Bluefin, ntb device problem
- NAS-117617 Allow setting snapdev field for filesystems
- NAS-117616 Do not try to revoke ACME certificate which has expired
- NAS-117604 Node is unable to rejoin cluster after power off/on of 1/4 nodes
- NAS-117602 Privilege Management API
- NAS-117601 system.general.get_ui_urls blocks main event loop
- NAS-117599 Installing netdata gets stuck at 75%
- NAS-117596 Redirect to Disks Reports with pre-selected disks
- NAS-117594 Add Vdev Form raises `Maximum call stack size exceeded`
- NAS-117592 24h clock in tasks
- NAS-117587 Fix regression in getgrnam for gid 0
- NAS-117584 fix Makefile MWPATH
- NAS-117575 Add more properties to dataset details
- NAS-117562 Add more dataset details
- NAS-117560 Unable to Delete Expired certificates
- NAS-117557 Improvements to ctdb.public.ips APIs

- NAS-117556 fix IndexError in failover.vip.get_states
- NAS-117553 Require at least one public IP address before joining cluster to AD
- NAS-117551 Fix `ftp_server_with_user_account` asset
- NAS-117544 NOT FOUND when querying for a list of support categories
- NAS-117524 huge optimization to query_for_quota_alert
- NAS-117519 Various improvements to builder
- NAS-117513 Import ZFS Pools failed
- NAS-117511 Remove zpool_get_physpath
- NAS-117509 Sync colors on cards
- NAS-117506 MatchNotFound on pool.query after update
- NAS-117501 disk_resize: Don't trigger udev events for NVMe
- NAS-117500 call install-dev-tools before setup_test.py
- NAS-117499 disk.query sometimes doesn't return pool disk if it was just attached
- NAS-117498 No Applications after cron job reboot
- NAS-117495 fix and improve middlewared Makefile
- NAS-117479 Skipping RAW device to be created
- NAS-117478 Revert change to SMB etc generation
- NAS-117476 bucket_policy_only: Field was not expected when expanding folders in Cloudsync task
- NAS-117472 minor grammar fix
- NAS-117471 Improve AD health checks
- NAS-117467 Reuse tdb / ctdb handles
- NAS-117465 Fix broken icon links
- NAS-117459 Post NAS-113963 - pool can't be locked while system-dataset is present
- NAS-117451 Unable to download debug
- NAS-117449 credentials.verify doesn't timeout on incorrect SFTP credentials
- NAS-117443 Fix clustered SMB service management events
- NAS-117442 fix test_cluster_path_snapshot test
- NAS-117441 Added better support for python virtual environment
- NAS-117439 Misaligned text on Topology Card
- NAS-117437 Remove microsoft account option
- NAS-117436 stop running file IO in main event loop
- NAS-117435 move thick_provision key to dataset level
- NAS-117434 VM Clone does not account for explicit web port
- NAS-117430 Simplify/Improve VM devices validation
- NAS-117428 Improper regex used on name validation for apps
- NAS-117426 Add common method for defining cpu/memory/gpu limitations
- NAS-117424 freenas-debug: Restore ZFS kstat capture
- NAS-117423 Errors waterfall on new Storage page
- NAS-117420 Initialize cluster so that all nodes have all public IPs
- NAS-117419 Pull-Replication failed
- NAS-117418 Fix iscsi tests
- NAS-117416 Plex wont deply (kubernetes.io/not-ready)
- NAS-117409 Unable to isolate GPU or see in apps in SCALE.
- NAS-117404 Remove unused library common charts
- NAS-117400 Fix activedirectory join in cluster
- NAS-117395 iscsi_/extents.py blocks main event loop in many places
- NAS-117391 Remove redundant dataset.query
- NAS-117382 Handle case of non-existent path during smbconf generation
- NAS-117378 Bump up timeout values for permissions tests on cluster
- NAS-117377 Fix clustered filesystem test
- NAS-117376 Remove port from portal configuration in issci
- NAS-117367 Ensure that required paths are auto-created for clustered pwenc
- NAS-117362 improve ntp alert verbiage
- NAS-117360 disk_resize: Don't wait 15 seconds for SAS flash
- NAS-117357 fix typo in disabled_reasons
- NAS-117353 Fix Failover_disks alert typo
- NAS-117330 vfs_fruit can write invalid timestamp as BTIME to user.DOSATTRIB xattr
- NAS-117328 Fixes an empty line in SMB share presets
- NAS-117327 NAS-117318: Fixes and empty line in SMB share presets
- NAS-117322 Minor improvements to pool.dataset.details
- NAS-117320 CLONE - Do not allow immutable fields to be modified in UI - Bluefin
- NAS-117318 Empty line in SMB share presets
- NAS-117313 Active Directory randomly automatically getting disabled during server reboot
- NAS-117307 Invesitgate/fix ix-volumes being migrated on apps migration
- NAS-117306 Fix ctdb jobs on pnn 0
- NAS-117305 fill in app information in pool.dataset.details
- NAS-117303 use ejson in kubernetes backup plugin
- NAS-117293 Deprecate legacy behavior to allow empty homes path
- NAS-117289 Attempting to delete VM causes system crash
- NAS-117285 [required] validator from FormsModule conflicts with * [required] input ix-* components
- NAS-117284 TrueNAS Scale nightly is trying to update to an older version
- NAS-117278 Missing Provisioning Type Field in Space Management Card
- NAS-117277 Space Management Card console error
- NAS-117273 sedutil-cli fails to identify SAS SED drives on Linux
- NAS-117264 Updater size estimates seem quite off
- NAS-117231 Add CTDB event integration
- NAS-117201 Fix qbittorrent upgrade strategy
- NAS-117186 Change ProFTPD TLS Protocol
- NAS-117175 unable to flash chelsio cards on SCALE
- NAS-117166 Syncthing App will not deploy on TrueNAS SCALE Bluefin nightly

- NAS-117159 save/rollback default gateway on interface changes
- NAS-117158 Network dashboard widget fails due to permissions after Scale update
- NAS-117153 Cloud Sync `create_empty_src_dirs` checkbox
- NAS-117144 Swagger documentation line on API Keys screen incorrect if default port has been changed
- NAS-117125 middleware worker process core dumped
- NAS-117118 Invalid update image file when trying to update nightlies
- NAS-117109 Apps: Plex: Plex can't start sometimes "No such file or directory"
- NAS-117104 PiHole Docker Install
- NAS-117101 Charts MinIO pod cannot connect to itself when hostname is used
- NAS-117076 Resource Limits are not applied to pod
- NAS-117045 Improve error messaging for 'min_memory' when creating a VM
- NAS-117039 Failed to check for alert ZpoolCapacity
- NAS-117037 Python message
- NAS-116998 SCALE: Cannot bind second network adapter to new VM
- NAS-116987 TrueNAS SCALE webui become very slow
- NAS-116933 UI won't allow UPS on ttyS0
- NAS-116927 ZFS replication causing unscheduled reboot on destination
- NAS-116894 CLONE - [SCALE] Application Events is not sorted
- NAS-116859 `pool.dataset.summary`
- NAS-116808 Improve IPMI password validation
- NAS-116777 [Scale 22.12-master] Apps won't start
- NAS-116702 Trivial (I think) Task Manager timing out
- NAS-116688 A Start Job is Running for Import ZFS Pools (xxmin xxs / 15min 11s)
- NAS-116674 [SCALE] BlockingIOError: [Errno 11] Resource temporarily unavailable
- NAS-116664 Stopped Apps/Docker spamming msg on syslog No Destination Avaliable
- NAS-116662 Non boot-drive swap space "unclean" and re-constructed every boot
- NAS-116603 Exclusive default Apps Catalog for Enterprise
- NAS-116574 Apps Node IP Not Matching What is Configured
- NAS-116513 pmem on SCALE doesn't report serial information
- NAS-116483 Can't add zvol with space in name to VM as disk
- NAS-116380 Trivial: On Network, Scale is displaying 2 default Gateways
- NAS-116295 Free RAM reported mismatch
- NAS-116098 nmbd breaks system dataset migration
- NAS-116071 On Angelfish Nightly after pressing Failover at the login it display "Failover is in an error state."
- NAS-116023 Boot Issues with TrueNAS-SCALE-22.02.0.1
- NAS-115994 Idmap issue with "OWNER RIGHTS" SID
- NAS-115992 NFSv4 not configured properly when active directory domain name != server subdomain
- NAS-115869 NTP service broken when DHCP provides NTP servers.
- NAS-115858 Fix netdata hitting apparmor profile
- NAS-115235 Restrict job log dir to root
- NAS-115058 Exception disable_offload_capabilities when configuring network interface from CLI
- NAS-114575 [SCALE] When using OneDrive as a Backup the Client sends tens of thousands of DNS Requests
- NAS-114305 Network Interfaces - Test/Save Changes bug (back-end)
- NAS-114064 IPV6 Neighbor Solicitation if started by TrueNas SCALE fails => NO IPV6
- NAS-113833 /update/check_available API call crashes when update-master.ixsystems.com is unavailable
- NAS-113830 SCALE: Time Machine does not work for large source on macOS Monterey (12.0.1 and 12.1)
- NAS-113534 sqlilte error creating link aggregation
- NAS-113529 VERIFY(PageUptodate(pp)) failed
- NAS-112995 Alert reads "…replication from scratch…" but entry is called differently in GUI
- NAS-112877 Docker networking configuration prevents certain images from working correctly
- NAS-112277 /usr/local/bin/zilstat not functional on SCALE
- NAS-110490 Scale - NVMe drives in USB case show same Serial Number
- NAS-103225 clear Enclosure Status when not OK

Known Issues

Seen In	Key	Summary	Workaround	Resolved In
22.12-RC.1	NAS-118922	Device Screen does't update after replacing a disk	When replacing a disk the UI doesn't update to show the replace operation completed and might display an error message. After replacing a disk, return to the Storage Dashboard and then the Devices screen to see the status of the disk replacement as complete.	Targeted 22.12(Bluefin)
22.12-RC.1	NAS-119005	On Enterprise systems, the Open Ticket button doesn't work	On Enterprise systems, when filing a ticket using the Open Ticket button should open an issue reporting screen but it does not. Customers should either contact Support directly or open a ticket directly in Jira.	Targeted 22.12 (Bluefin)
22.12-RC.1	NAS-119011	iSCSI wizard does not function properly	The Extent Type device dropdown list is empty and the Portal dropdown list does not include the create new option so users can not select or add a new device, or add a new portal.	Targeted 22.12 (Bluefin)
22.12-RC.1	NAS-119008	On HA systems, the Dashboard Standby controller and status do not update after changing the system dataset.	Issue is related to another UI screen caching issues where the HA Dashboard does not show updated system information. Clear your browser cache to update the UI.	Targeted 22.12 (Bluefin)

Seen In	Key	Summary	Workaround	Resolved In
22.12-RC.1	NAS-119006	Enclosure view only updates after leaving the page	Related to a known screen caching issue. Either clear your browser cache or change to a different UI screen and return to the Enclosure screen see the updates.	Targeted 22.12.1 (Bluefin)
22.12-RC.1	NAS-119007	API call 'pool.dataset.details' responds to an object with a field "snapshot_count = 0"	API call to obtain number of zvol snapshots returns an incorrect value of zero when there are two snapshots.	Targeted 22.12.1 (Bluefin)
22.12-RC.1	NAS-119010	SCALE drive replacement within a pool produces drive busy error	During HDD testing, replacing a drive in a pool resulted in the Error: [EFAULT] Railed to wipe disk sdb: [Errno 16] Device or resource busy: '/dev/sdb'. Appears to be a ZFS error.	Targeted 22.12(Bluefin)
22.12-BETA.2	NAS-118632	Traceback received during pool creation	This is an occasional noncritical race condition with the disk temperatures widget during pool creation. The traceback can be acknowledged and ignored; the issue is temporary and does not impact pool creation..	22.12-RC.1
22.12-BETA.2	NAS-118616	SMB Share option Edit Filesystem ACL does not open the filesystem editor screen.	After adding an SMB share, if you select the option to Edit Filesystem ACL, the main Dashboard opens instead of the filesystem ACL editor screen. To workaround this issue, go to the Storage > Dashboard screen, select the dataset for the SMB share, scroll down to the Permissions widget and click Edit.	22.12-RC.1
22.12-BETA.2	NAS-118614	Cloud tasks for Move and Sync transfer modes revert to Copy	When creating a cloud sync task where the Transfer Mode is set to either Move or Sync, when the task completes successfully and runs for the first time, the notification to the user states the transfer mode was reset to Copy.	22.12-RC.1
22.12-BETA.2	NAS-118613	Cannot mount WebDAV share in Windows when WebDAV service is set to Basic Authentication	If the TrueNAS WebDAV service is set to Basic Authentication, you cannot mount the share in Windows. This is a security protection on the part of Windows as Basic Authentication is considered an insecure way to input passwords. While the Windows Registry can be edited to allow for basic authentication, this is not recommended. It is recommended to access WebDAV shares using a browser with https security enabled or mounting shares with Digest Authentication enabled.	N/A
22.12-BETA.2	n/a	TrueNAS Bluefin no longer supports MS-DOS based SMB clients.	As of SCALE 22.12, Bluefin, TrueNAS now uses Samba 4.17. Samba 4.16 announced in their release notes that they deprecated and disabled the whole SMB1 protocol as of 4.11. If needed for security purposes or code maintenance they continue to remove older protocol commands and unused dialects or that are replaced in more modern SMB1 version. Refer to Samba release notes for more information.	n/a
22.12-BETA.1	n/a	Upgrading from 22.02.4 to 22.12-BETA.1 is known to not work.	Workaround is to either upgrade from a version before 22.02.4 or to upgrade to 22.12-BETA.2 when it is released.	22.12-BETA.2
22.12-BETA.1	NAS-117940	Implements temporary fix for the return from `glfs_open()` to honor `O_DIRECTORY` flag	Pertains to an internal issue in Samba. This temporary fix reverts after gluserfs is fixed with a permanent solution to this issue.	Targeted 22.12 (Bluefin)
22.12-BETA.1	NAS-117974	Replication Task Wizard Source and Destination fields cut off the path information	The **Source** and **Destination** fields in the **Replication Task Wizard** window are cutoff. UI form issue that positions the paths in the fields such that only part of the value is visible.	Backlog
22.12-BETA.1	NAS-118063	SCALE Cluster growth/resize features	Currently, there is no way to grow or resize an existing cluster without the user destroying their cluster and starting with a new cluster. This issue looks to implement a solution using TrueCommand and TrueNAS API that provides the ability to have shared volumes that do not occupy all nodes in the cluster, add one or more nodes to a cluster without impacting existing shared volumes, "grow" a shared volume, and temporarily remove nodes from a cluster without destroying the cluster.	Targeted Backlog
22.12-BETA.1	NAS-118066	UI is not updating or properly showing snapshots	UI isn't showing dataset snapshots without creating one from Shell, but the UI doesn't display this Shell-created snapshot in Manage Snapshots.	22.12-BETA.2
22.12-BETA.1	NAS-118054	Replication Warning: Cannot receive sharesmb property	Replication created sending from an encrypted dataset to a non-encrypted dataset. After running replication the screen displays an orange warning icon. After clicking on the warning the "cannot receive sharesmb property in *tank/repwizrd/*set: pool and dataset must be upgraded to	Targeted 22.12-BETA.2

Seen In	Key	Summary	Workaround	Resolved In
			set this property or value." where *tank/repwizrd* is the pool/dataset path.	
22.12-BETA.1	NAS-118095	Core dumps on ctdb at startup	Traceback received that indicates ctdb core-dumps when starting nodes after a fresh install.	Unscheduled
22.02.1	NAS-116473	Large Drive Count Issues	iX is investigating issues with booting SCALE on systems with more than 100 Disks.	23.10-ALPHA.1 (Cobia)
22.02.0	NAS-115238	Removed drive from pool does not degrade pool status (SCALE).	Issue is being investigated and a fix provided in a future release	22.12-BETA.2
		Unable to mount an NFS export after migrating from CORE > SCALE or updating to 22.02.0.	The /etc/exports file is no longer generated when the NFS configuration contains *mapall* or *maproot* entries for unknown users or groups. This can impact users who previously had a mapping group set to *wheel*, which does not exist in SCALE. If you are unable to mount an NFS export, review your NFS share configuration and change any *wheel* entries to something specific for your environment or *root*.	
		SCALE Gluster/Cluster.	Gluster/Cluster features are still in testing. Administrators should use caution when deploying and avoid use with critical data.	
	NAS-110263	AFP sharing is removed from TrueNAS SCALE. The protocol is deprecated and no longer receives development effort or security fixes.	TrueNAS SCALE automatically migrates any existing AFP shares into an SMB configuration that is preset to function like an AFP share.	21.06-BETA.1
21.06-BETA.1	NAS-111547	ZFS shouldn't count vdev IO errors on hotplug removal	Pool status isn't being updated immediately on disk exchange events.	Targeted 22.12 (Bluefin)

> TrueNAS SCALE Bluefin includes Linux Kernel 5.15 which can enable Alderlake GPU acceleration by using the following boot loader tunable and rebooting:
>
> `midclt call system.advanced.update '{"kernel_extra_options": "i915.force_probe=4690" }'`
>
> NOTE: 4690 can be replaced with your specific Alderlake GPU version.

OpenZFS Feature Flags

For more details on feature flags see OpenZFS Feature Flags.

For more details on zpool.features.7 see OpenZFS zpool-feature.7.

Feature Flag	GUID	Dependencies	Description
blake3	org.openzfs.blake3	extensible)dataset	Enables use of the BLAKE3 hash algorithm for checksum and dedup. BLAKE3 is a secure hash algorithm focused on high performance. When enabled, the administrator can turn on the blake3 checksum on any dataset using `zfs set checksum=blake dset` see zfs-set(8).
head_errlog	com.delphix:head_errlog	n/a	Enables the upgraded version of `errlog`. The error log of each head dataset is stored separately in the zap object and keyed by the head id. Every dataset affected by an error block is listed in the output of `zpool status`.
zilsaxattr	org.openzfs:zilsaxattr	extensible_dataset	Enables `xattr-sa` extended attribute logging in the ZIL. If enabled, extended attribute changes from both `xattrdir=dir` and `xattr=sa` are guaranteed to be durable if either `sync=always` is set for the dataset when a change is made or sync(2) is called on the dataset after making changes.

Bluefin Unstable Nightly Images (Unstable Branch, developers and brave testers)

> Nightly builds are considered experimental and highly unstable. Do not use a nightly build for anything other than testing and development.

Nightly images for TrueNAS SCALE are built every 24 hours, at around 2AM Eastern (EDT/EST) time. These images are made publicly available when they pass automated basic usability testing. This means that during times of heavy development, nightly images might be less frequently available. Online updates are created every 2 hours and are available in the SCALE UI online updating page.

- ISO Installation Files
- Manual Update File