

TrueCommand

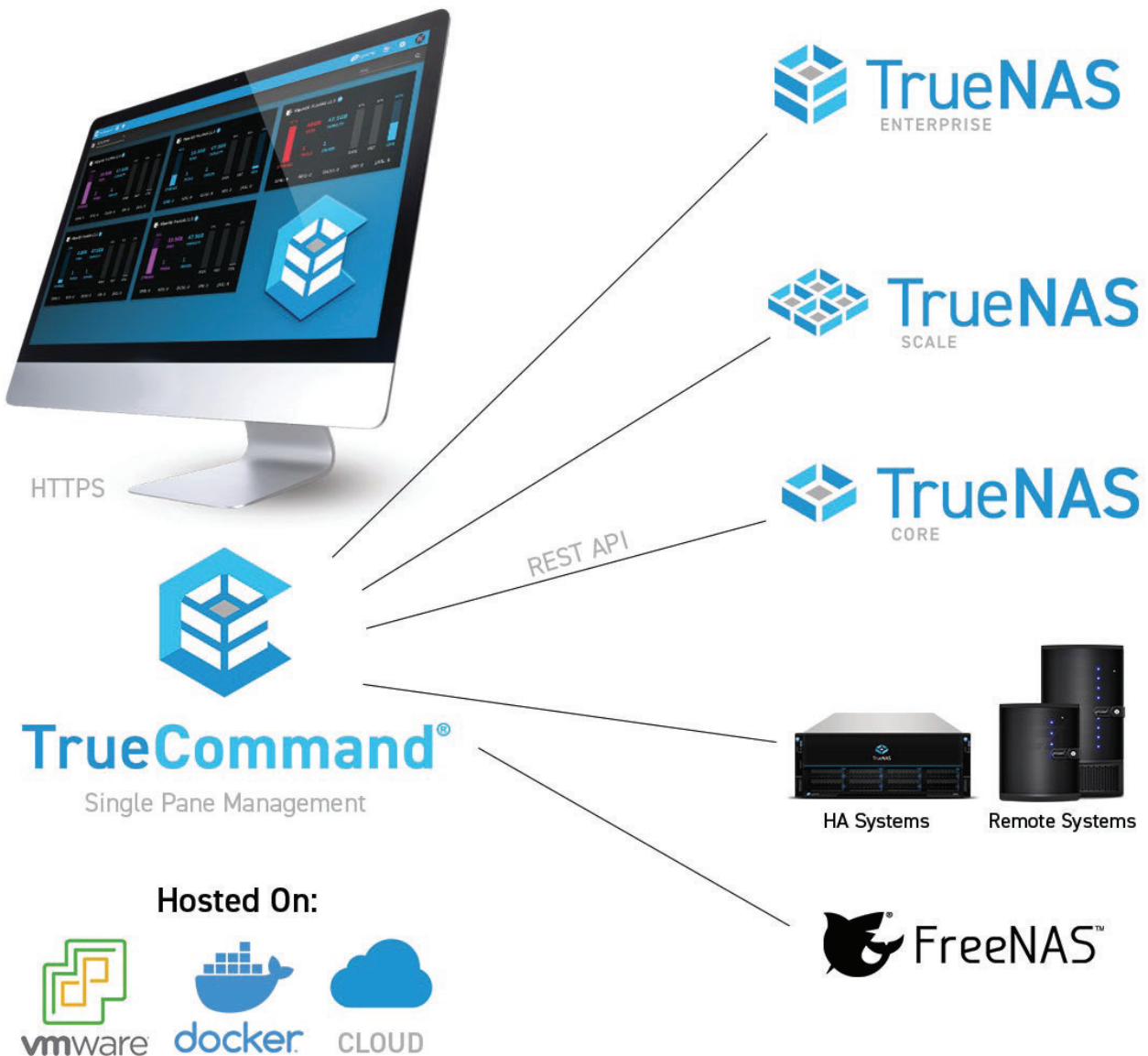
- 1: [TrueCommand 2.1 Release Notes](#)
- 2: [Introduction](#)
 - 2.1: [Support](#)
- 3: [Developer's Notes](#)
- 4: [Getting Started](#)
 - 4.1: [Installing or Updating](#)
 - 4.1.1: [Update Docker](#)
 - 4.1.2: [Migrate Legacy to 1.2+](#)
 - 4.2: [Interface Overview](#)
 - 4.3: [Creating User Accounts](#)
 - 4.4: [Connecting Your First TrueNAS System](#)
- 5: [Administration](#)
 - 5.1: [Systems](#)
 - 5.2: [Users](#)
 - 5.3: [Settings](#)
 - 5.3.1: [Configuring TrueCommand SAML](#)
 - 5.4: [System Log](#)
- 6: [System Management](#)
 - 6.1: [Single System Management](#)
 - 6.1.1: [System Settings](#)
 - 6.1.2: [Config Backups](#)
 - 6.1.3: [TrueCommand Storage Management](#)
 - 6.1.4: [TrueCommand Snapshots](#)
 - 6.1.5: [TrueCommand Sharing](#)
 - 6.2: [TrueNAS Configuration File Management](#)
 - 6.3: [Multiple Systems](#)
 - 6.4: [NAS Users and Groups](#)
- 7: [Reports](#)
 - 7.1: [Creating a Report](#)
 - 7.2: [Generating a System Report](#)
- 8: [Alerts](#)
 - 8.1: [Alert Management](#)
 - 8.2: [Colors](#)
- 9: [Clustering](#)
 - 9.1: [Creating Clustered Volumes](#)
 - 9.2: [Managing Clustered Storage](#)
 - 9.3: [Mounting Clustered Volumes](#)
- 10: [iSCSI Volume Management](#)
- 11: [Recommendations](#)
 - 11.1: [TrueCommand Cloud Security](#)
- 12: [API Guide](#)
- 13: [Notices](#)
 - 13.1: [TrueCommand SaaS Agreement](#)
 - 13.2: [TrueCommand Terms of Service](#)
 - 13.3: [End of Life Notices](#)
 - 13.3.1: [TrueCommand 1.1](#)
 - 13.3.2: [TrueCommand 1.0](#)



TrueCommand®

TrueCommand is a multi-system management “Single pane of Glass” system that helps control and monitor your TrueNAS fleet. TrueCommand assists in managing TrueNAS systems through REST APIs, WebSocket APIs, and a web user interface. The TrueCommand web interface provides single sign-on functionality and unified administration of users and TrueNAS systems.

TrueCommand can monitor an entire fleet of TrueNAS systems and thousands of online storage devices simultaneously. This includes displaying statistics on storage usage, network activity, active services, and more. TrueCommand also has the ability to create custom reports about individual systems or a combination of many systems.



What Features does TrueCommand have?

Multiple Deployment Options expand

TrueCommand docker container can be deployed as a VM since vhdK and vmdK are no longer supported in version 2.0. TrueCommand Cloud is also available as a cloud-based subscription option that allows you to offload TrueCommand resources and deployment and only focus on fine-tuning your configuration.

NAS Fleet Dashboard expand

The TrueCommand dashboard provides visibility to an organization's entire TrueNAS fleet. TrueCommand includes an auto-discovery tool that expedites identifying and integrating systems into TrueCommand.

Single Sign-on to all NAS Units expand

Authorized administrators can quickly log into a TrueNAS system through TrueCommand. This allows for quicker and simpler signons instead of looking up IP addresses and login credentials. This is even more beneficial when using different secure passwords for each TrueNAS instance instead of a single password across multiple systems.

Centralized system updates expand

Easily update any connected TrueNAS system. Monitor update progress, reboot the system, or even roll it back if something goes wrong.

Customized Alerts and Reports expand

TrueCommand centralizes the management of alerts across a fleet of TrueNAS systems. In addition to the standard system alerts, administrators can define custom alerts.

Administrators can also create custom graphical reports. Reports are configurable and can span as many systems as desired and/or set of metrics. This brings the information that the administrators deem the most relevant immediately to visibility. Report data can be exported in CSV or JSON for other uses.

Alerts for all managed systems are shown in TrueCommand's web-based dashboard. Notification groups can also be defined so that unique groups receive specific alerts via email. This enables TrueCommand to keep the right individuals informed of any current or potential problems.

Enterprise Security with Role-Based Access Control (RBAC) expand

TrueCommand administrators can define varied levels of system access. These access levels can be assigned to system groups. Individuals can be assigned to teams or departments. Doing so allows the administrator to control the level of access appropriate to each individual or group in a manageable and atomic fashion. TrueCommand's RBAC controls can leverage pre-existing LDAP and Active Directory identities and groups in your infrastructure, eliminating redundant management overhead.

Audit Logs expand

TrueCommand records all administration actions in secure audit logs. This allows for quick identification of what has been changed and who changed it.

What Does it Cost?

TrueCommand is free to use for up to 50 drives. Licenses to expand TrueCommand capabilities are purchased from the [iXsystems account portal](#). Pricing is based on the number of drives and the desired level of support.

Where do I get it?

TrueCommand is downloaded from the [TrueNAS website](#). TrueCommand Cloud subscriptions are available at the [iXsystems Account Services Portal](#).

What is TrueCommand Cloud?

TrueCommand Cloud is a secure SaaS offering that includes a WireGuard VPN capability to connect TrueNAS systems through firewalls. TrueCommand Cloud is compatible with TrueNAS versions **12.0+ or SCALE** for the Wireguard VPN capability. Subscribe to and set up TrueCommand Cloud using [these instructions](#).

1 - TrueCommand 2.1 Release Notes

- - [Software Lifecycle](#)
 - [TrueCommand Schedule](#)
 - [2.1.1](#)
 - [2.1.1 Changelog](#)
 - [Improvement](#)
 - [Bug Fixes](#)
 - [2.1](#)
 - [To Download this Release](#)
 - [Minimum Supported TrueNAS Versions](#)
 - [To Update to this Release](#)
 - [Known Issues](#)

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

TrueCommand 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
2.2.0-RC.1	Internal Testing Sprints	30 May > 03 June 2022
2.2.0	Code-freeze	08 June 2022
2.2.0	Internal Testing Sprints	09 June 2022 > 29 July 2022
2.2.0	Tag	01 Aug 2022
2.2.0	Release	02 Aug 2022

2.1.1

March 29, 2022

The TrueCommand team is pleased to announce [TrueCommand 2.1.1](#) is now available.

2.1.1 Changelog

Improvement

- [\[TC-1924\]](#) - Adjust log rotation to use max size
- [\[TC-1968\]](#) - Add build/deploy github workflow to release/2.1

Bug Fixes

- [\[TC-1913\]](#) - TrueCommand does not start when pointed to a custom certificate
- [\[TC-1921\]](#) - Imported Certificates Are Not Showing In The WebUI
- [\[TC-1934\]](#) - Mailserver Test Button Lacks Meaningful Output
- [\[TC-1937\]](#) - Docker Does Not Start Again After Import Certificates
- [\[TC-1941\]](#) - Unable to open TrueNAS proxy interface on cloud
- [\[TC-1948\]](#) - Removal of team in edit-user page is not working
- [\[TC-1966\]](#) - Removing Cluster Volume Hangs
- [\[TC-1967\]](#) - Deleting Certificate Authorities not working
- [\[TC-1982\]](#) - Cluster Volume not showing in UI
- [\[TC-1983\]](#) - Middleware API crash when I try verify email of my profile in truecommand docker version
- [\[TC-1985\]](#) - Handle instance where filewatcher util can fail on initialization
- [\[TC-1988\]](#) - Do not fail deployment if Influx already setup
- [\[TC-1990\]](#) - Trouble With Deleting Alerts

2.1

2.1 expand

January 4, 2022

The TrueCommand team is pleased to announce [TrueCommand 2.1](#) is now available.

TrueCommand 2.1 is the single pane of glass for:

- **TrueNAS CORE:** Manage systems on standard servers, Minis, or even AWS.
- **TrueNAS Enterprise:** Manage X-Series and M-Series systems with High Availability.
- **TrueNAS SCALE:** Manage a group of systems running a TrueNAS SCALE cluster.

2.1 Changelog

New Feature

- [\[TC-1184\]](#) - Add two-factor authentication support
- [\[TC-1581\]](#) - Have TC auto-generate and use an auth token after initial NAS connect
- [\[TC-1711\]](#) - NAS user management
- [\[TC-1757\]](#) - Add SAML SSO support
- [\[TC-1774\]](#) - Add ability to manage NAS users/groups for shares.
- [\[TC-1823\]](#) - Add ability to reset user passwords from login page

Improvement

- [\[TC-1468\]](#) - EULA needs to identify GPL components
- [\[TC-1489\]](#) - Question about the Dashboard System Options Menu
- [\[TC-1603\]](#) - Update selenium tests
- [\[TC-1655\]](#) - Include **Group** or **All** option for system selection for reports
- [\[TC-1663\]](#) - Add email verification to user email
- [\[TC-1772\]](#) - Multiple time formats in use
- [\[TC-1789\]](#) - Alerts for failed/suspicious login activity on a NAS
- [\[TC-1806\]](#) - Remove PostgreSQL and migration routine.
- [\[TC-1811\]](#) - Add **Test** button for LDAP settings
- [\[TC-1813\]](#) - Rewrite shell scripts to go binaries
- [\[TC-1816\]](#) - Unique name for the TC instance when it registers a token on the NAS
- [\[TC-1820\]](#) - Unix permissions widget

- [\[TC-1821\]](#) - Remove ng2-validation dependency
- [\[TC-1834\]](#) - Add verbose logging and log level config
- [\[TC-1835\]](#) - Update SMR disk model scanning
- [\[TC-1844\]](#) - Prune dead code
- [\[TC-1850\]](#) - Add warning to Cluster feature
- [\[TC-1857\]](#) - Delete Dataset shouldn't be an option for datasets with children
- [\[TC-1865\]](#) - Bugclerk for TrueCommand team
- [\[TC-1869\]](#) - Add a Confirmation screen when the cluster is successfully deleted
- [\[TC-1876\]](#) - Disable adding/replacing/removing peers/bricks
- [\[TC-1878\]](#) - Add Experimental flags to Users/Groups+SAML
- [\[TC-1884\]](#) - Safety belt for Clustering feature
- [\[TC-1893\]](#) - Add memory health check

Epic

- [\[TC-1800\]](#) - Enhanced Authentication Support
- [\[TC-1815\]](#) - SMB User Management

Bug Fixes

- [\[TC-1761\]](#) - Used space on system tiles reported as a whole number
- [\[TC-1768\]](#) - Storage Navigator and Datasets card issues
- [\[TC-1783\]](#) - SMR Alerts: Disk/Model desync from NAS?
- [\[TC-1784\]](#) - Share Count Numbers always 0
- [\[TC-1812\]](#) - DNS lookup failure
- [\[TC-1826\]](#) - Alert rules not staying paused
- [\[TC-1829\]](#) - Network speed reporting issues
- [\[TC-1833\]](#) - Clumsy resolving long alert messages
- [\[TC-1839\]](#) - NAS API Error - Can't view Storage
- [\[TC-1851\]](#) - Include the User's name and UID in the logs
- [\[TC-1856\]](#) - Cluster creation - API error
- [\[TC-1908\]](#) - Not deleting or reusing TSP
- [\[TC-1911\]](#) - Mismatch between ignore_alerts in MW and UI

To Download this Release

Login to the [TrueCommand Account Portal](#) for downloads, documentation links, and licensing options. For storage clusters with more than 50 disks, the account portal also offers a *free 60-day trial license with unlimited disks*.

Minimum Supported TrueNAS Versions

Due to the changes in integrating with the TrueNAS middleware, the minimum version for full-support of functionality has changed with TrueCommand 2.1:

- FreeNAS/TrueNAS 11.3 series - No longer supported. Does not provide realtime statistics or storage information, but you can still connect to them and use TrueCommand to initiate updates.
- TrueNAS 12 CORE/Enterprise - Supported after 12.0-U3. 12.0-U2.1 and older are missing some key metrics in the realtime stats (disk/network usage metrics in particular), but work otherwise.
- TrueNAS SCALE 21.03+ - Fully Supported (SCALE-20.12+ is supported excluding cluster functionality)

To Update to this Release

Prior To Updating

As a best practice, TrueCommand admins should backup their instance's data directory before deploying TrueCommand updates. If issues arise after updating, admins can simply pull the previous TC docker image and redeploy with their previous data directory.

Important Note for Upgrading from v1.3

Updating from TrueCommand v1.3 to v2.0 or higher involves a database migration process. This preserves all configuration data, but does not preserve old performance statistics. Additionally, it is not possible to roll back to TrueCommand v1.3 from v2.1. Please use caution when upgrading production TrueCommand systems. If necessary, run TrueCommand 1.3 and TrueCommand 2.1 in parallel for a transition period. Simply use the “ixsystems/truecommand:1.3.2” docker image to continue using that specific version of TrueCommand.

Docker: Re-run `docker pull ixsystems/truecommand` to fetch the latest version of TrueCommand, and then restart your docker instance.

VM Image: Either reboot the VM or run `systemctl restart truecommand.service`. This will automatically fetch and start the latest Docker image of TrueCommand within your VM.

Known Issues

Seen In	Key	Summary	Workaround	Resolved In

2 - Introduction

Welcome to TrueCommand!

This section contains licensing information and additional details about software support offerings from iXsystems, Inc.

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 - Support

Free Support

The [TrueCommand Community Forum](#) is an active online resource for asking questions, troubleshooting issues, and sharing information with other TrueCommand users. [Registering](#) is required for posting. New users are encouraged to briefly [introduce](#) themselves and review the [forum rules](#) before posting.

Paid Support

iXsystems offers different Support packages for TrueCommand customers. To find more details about the different Warranty and Service Level Agreement (SLA) options available, see the [TrueCommand Support overview](#).

TrueCommand Cloud

If any issues are found when using TrueCommand Cloud or an iX Portal account, log in to the Portal Account and click *Manage > Request Support*. Fill out the *Request Support* form with specific details of the issue and click *Send Request*. A copy of the support request is emailed to the registered email account.

3 - Developer's Notes

- - [System Requirements](#)
 - [Nightly Docker Images](#)
 - [Current Status](#)
 - [Summary of changes in version 2.0](#)
 - [Migration Notice](#)
 - [Minimum Supported TrueNAS Versions](#)

Recent Updates expand ☐

04/09/2021 - ISCSI creation process completed. Cluster creation routines finished up and streamlined.

03/17/2021 - Large update to Cluster creation/management. Requires latest TrueNAS SCALE nightlies to work properly (API's just changed on their end).

02/25/2021 - Initial nightly image release for TrueCommand 2.0

System Requirements

- Docker Environment (64-bit AMD or Intel system)
- 2GB of RAM (recommended minimum)
- 20GB of disk space (recommended minimum)

Nightly Docker Images

Nightly images for TrueCommand are built every 24 hours. These images are automatically pushed to the "nightly" tag on DockerHub if they pass the automated QA testing procedure.

Download information:

- [DockerHub](#)
- [Example in Documentation](#), replace "latest" with "nightly" in the docker pull commands.

Current Status

The nightly images are always considered a "work-in-progress" toward the next release of TrueCommand. They should be suitable for adventurous users and developers who are not afraid of diagnosing issues and opening up bug reports with the TrueCommand developers.

Ticket Tracker: [Jira](#)

Current Nightly Version: 2.0-Master

Summary of changes in version 2.0

- Version 2.0 is a complete rewrite of the middleware and database used in TrueCommand, as well as a complete re-integration with the TrueNAS middleware for statistics and analysis. Early tests indicate a sharp improvement in the performance of the system (details below), and some of the new features that this enables in TrueCommand 2.0 are: NAS metrics and state updates in realtime - no more 30s delay!
- The "Storage Explorer" interface lets you inspect the datasets and files on your storage pools, while also

giving you easy access to creating and managing snapshots, shares, zvols, and more.

- The “ISCSI Manager” is a new dashboard system that lets you view and create ISCSI volumes in bulk across your entire NAS fleet.
- “Cluster Volumes” is a new dashboard system that lets you view and create clustered datasets which span across multiple TrueNAS SCALE systems in your fleet.
- Marked performance improvements:
 - Docker image ~50% smaller
 - Network bandwidth usage ~40% less
 - CPU usage ~5% lower
 - Database growth rate ~99% lower

Table of features and current status (Timestamp references when the item status was last updated):

Feature	Status	Timestamp	Description
Users	OK	02/26/2021	Create and manage users and user permissions
Teams	OK	02/26/2021	Create and manage teams of users and permissions
Systems	OK	02/26/2021	Register NAS's and maintain connections/status info
Alert Rules	OK	02/26/2021	Create and manage custom alert rules
Alert Notices	OK	02/26/2021	Rolling feed of alerts that have been triggered with comment and resolution systems
Alert Services	OK	06/07/2021	Submission of new alert notices to external notification systems (email/pagerduty)
Reports	OK	02/26/2021	Historical charts of system information
Logs	OK	02/26/2021	Security logs of changes from users
System Administration	OK	02/26/2021	Configuration of TrueCommand system (SSL certificates, licensing, AD/LDAP, etc)
Dashboard	OK	06/07/2021	Top-level look at NAS state and information
NAS Explorer	OK	06/07/2021	Detailed inspection/management of storage on individual NAS's
Cluster Volumes	OK	06/07/2021	Create and manage clusters of TrueNAS SCALE systems (glusterfs)
ISCSI Manager	OK	06/07/2021	Create and manage ISCSI volumes in bulk

Migration Notice

Due to the change in database between the 1.x and 2.x versions of TrueCommand, there is an automatic database migration routine that will run the first time you start up the v2.0 image of TrueCommand.

Information Migrated:

- User accounts
- Teams
- System Registrations
- System Groups
- TrueCommand System Configuration
- NAS configuration backups

Information **NOT** migrated due to drastic changes in how these are performed now.

- Historical metrics from NAS's
- Alerts (both rules and notices)
- User-defined reports
- Security Logs

When you are using an LDAP-enabled system for user logins, please have your non-LDAP admin user

credentials handy before updating. The LDAP integration systems between 1.x and 2.x are different, and you need to login and verify that everything is still configured properly after the migration.

Minimum Supported TrueNAS Versions

Due to the changes in integrating with the TrueNAS middleware, the minimum version for full-support of functionality has changed with TrueCommand 2.0:

- FreeNAS/TrueNAS 11.3 series - No longer supported. Does not provide realtime statistics or storage information, but you can still connect to them and use TrueCommand to initiate updates.
- TrueNAS 12 CORE/Enterprise - Supported after 12.0-U3. 12.0-U2.1 and older are missing some key metrics in the realtime stats (disk/network usage metrics in particular), but work otherwise.
- TrueNAS SCALE 21.03+ - Fully Supported (SCALE-20.12+ is supported excluding cluster functionality)

4 - Getting Started

Thank you for trying TrueCommand! This Guide walks you through the initial installation and set up of TrueCommand.

- [Installing TrueCommand](#)
 - [Updating Docker on Linux](#)
 - [Migrate Legacy to v1.2+](#)
- [First time logins](#)
- [Creating User Accounts](#)
- [Connecting TrueNAS Systems](#)

4.1 - Installing or Updating

- [Install Options](#)
- [Adding Browser Security Exceptions](#)
 - [Browser Security Exceptions](#)
- [Creating the Administrator Account](#)

TrueCommand is versatile and offers several different install options. TrueCommand Cloud is the preferred method for using TrueCommand since it requires no local resources or specific hardware requirements to get started!

Install Options

TrueCommand Install Options expand ☐

Cloud Deployment expand ☐

TrueCommand Cloud is a SaaS offering of TrueCommand with a WireGuard VPN capability to connect TrueNAS systems through firewalls. TrueCommand Cloud is compatible with TrueNAS version v12.0 and newer.

Register an iXsystems Account

Open <https://portal.ixsystems.com> and click **Register**.



Account Services

[Register](#)

Login to your account



Login



Login with Facebook



Login with Google



Login with GitHub



Login with LinkedIn

Fill out the form using the email address you want to use.



Account Services

[Login](#)

Create an account

Passwords must contain at least 8 characters.

Email Address

Confirm Email Address

Password

Confirm Password

Register

By using this site you agree to the [iXsystems EULA](#) and [Privacy Policy](#)
2020 © iXsystems Inc • [Website Support](#)

Check the address spam folder if the email does not arrive within a few minutes. If the email is in the spam folder, mark it as *not spam* and add the account to the address book. After receiving the verification email, open the link provided to verify the account.

Create a New Subscription

Log in to the verified account and click **New Subscription**.



Account Services

[Logout](#)

Welcome jt@obs-sec.com

[Account Settings](#)

No active subscriptions!

[New Subscription](#)

Trial License

• TrueCommand 60 Day Trial

[Manage](#)

TrueCommand Quick Links

[User Guides and Documentation](#)

[Release Notes](#)

[Docker Images](#)

[Latest VM Image \(VHDX\)](#)

[Latest VM Image \(VMDK\)](#)

By using this site you agree to the [iXsystems EULA](#) and [Privacy Policy](#)
2020 © iXsystems Inc • [Website Support](#)



Account Services

[Back](#)

Please select a subscription plan:

TrueCommand Cloud (Early Access)



Please select an option



TrueCommand Site License (Self hosted)



Please select an option



By using this site you agree to the [iXsystems EULA](#) and [Privacy Policy](#)
2020 © iXsystems Inc • [Website Support](#)

Select the TrueCommand Cloud option and choose the subscription plan that best fits your current needs.



Account Services

[Back](#)

Please select a subscription plan:

TrueCommand Cloud (Early Access)



Please select an option

30 Drives, \$5.99/month
50 Drives, \$9.99/month
100 Drives, \$19.99/month
200 Drives, \$39.99/month
300 Drives, \$59.99/month
400 Drives, \$79.99/month
500 Drives, \$99.99/month
600 Drives, \$119.99/month
700 Drives, \$139.99/month
800 Drives, \$159.99/month
900 Drives, \$179.99/month
1000 Drives, \$199.99/month



By using this site you agree to the [iXsystems EULA](#) and [Privacy Policy](#)
2020 © iXsystems Inc - Website Support

Click **Continue** to proceed.



Account Services

[Back](#)

Please select a subscription plan:

TrueCommand Cloud (Early Access)



1000 Drives, \$199.99/month



Continue

TrueCommand Site License (Self hosted)



Please select an option



By using this site you agree to the [iXsystems EULA](#) and [Privacy Policy](#)
2020 © iXsystems Inc - Website Support

Next, fill out the payment form.

TrueCommand - 1000 Drive
Cloud Service

\$199.99 USD / 1 month

Contact Information

FIRST NAME *

LAST NAME *

PHONE NUMBER

COMPANY / ORGANIZATION NAME



CARD NUMBER *

EXPIRATION MONTH *

EXPIRATION YEAR *

CVV *

COUNTRY *

STREET ADDRESS *

ADDRESS 2

CITY *

STATE *

ZIP/POSTAL *

Order Summary

TrueCommand - 1000 Drive Cloud Service

\$199.99 USD

COUPON CODE



Subtotal

\$199.99 USD

Order Total

\$199.99 USD

TERMS AND PRIVACY

☐ I accept the Privacy Policy.

Subscribe

Powered by **Recurly**

Submit and wait for the form to be accepted. When ready, click **Provision Now**.



Account Services

[Logout](#)

Welcome jt@obs-sec.com

Account Settings

Active Subscriptions

- TrueCommand - 1000 Drive Cloud Service

[New Subscription](#)

[Provision Now](#)

Trial License

- TrueCommand 60 Day Trial

[Manage](#)

TrueCommand Quick Links

[User Guides and Documentation](#)

[Release Notes](#)

[Docker Images](#)

[Latest VM Image \(VHDX\)](#)

[Latest VM Image \(VMDK\)](#)

By using this site you agree to the [iXsystems EULA](#) and [Privacy Policy](#)
2020 © iXsystems Inc - Website Support

Select a **Subnet** that your network is not using.



Account Services

[Back](#)

Provision TrueCommand

Choose the subnet you wish to use for this instance (this can be changed later):

172.28.0.0/16

<


Create Instance

By using this site you agree to the iXsystems EULA and Privacy Policy
2020 © iXsystems Inc • Website Support

Managing a TrueCommand Cloud Account

From the account home page, click **Manage**. Add a client for desktop or laptop to obtain a TrueCommand WireGuard Config file.

[iXsystems](#) [TrueNAS](#) [FreeNAS](#) [TrueCommand](#) [iX Community](#)




iXsystems™

Account Services

Back

Service Details

Address	172.28.0.1
API Key	
Instance Status	healthy
Plan	TrueCommand - 1000 Drive Cloud Service
Plan State	active
Plan Pricing	\$199.99 / Month

Service Controls

Modify Subnet

Request Support

No clients found

Create Access Client

Nickname

Add


Service Administration

Your plan will automatically renew on 2020-10-25.

Edit Billing Information

Cancel Subscription

By using this site you agree to the [iXsystems EULA](#) and [Privacy Policy](#)
2020 © iXsystems Inc • [Website Support](#)

After adding the client, click  to download the configuration file.

[iXsystems](#) [TrueNAS](#) [FreeNAS](#) [TrueCommand](#) [iX Community](#)





iXsystems™

Account Services

Back

Service Details

Address 172.28.0.1 

API Key  xC7YwCjOu9Qb1p2 

Instance Status **healthy**

Plan TrueCommand - 1000 Drive Cloud Service

Plan State active

Plan Pricing \$199.99 / Month

Service Controls

Modify Subnet

Request Support

WireGuard Client Access


Show entries

Search:

Nickname 		Date Added 	Approved		
<input type="checkbox"/>	 Ops-Workstation 	Sep-25-2020 15:24	Yes		


Showing 1 to 1 of 1 entries

Previous Next

Select All

Clear Selection

Approve Selected 

Delete Selected 

Create Access Client

Nickname

Add

Service Administration

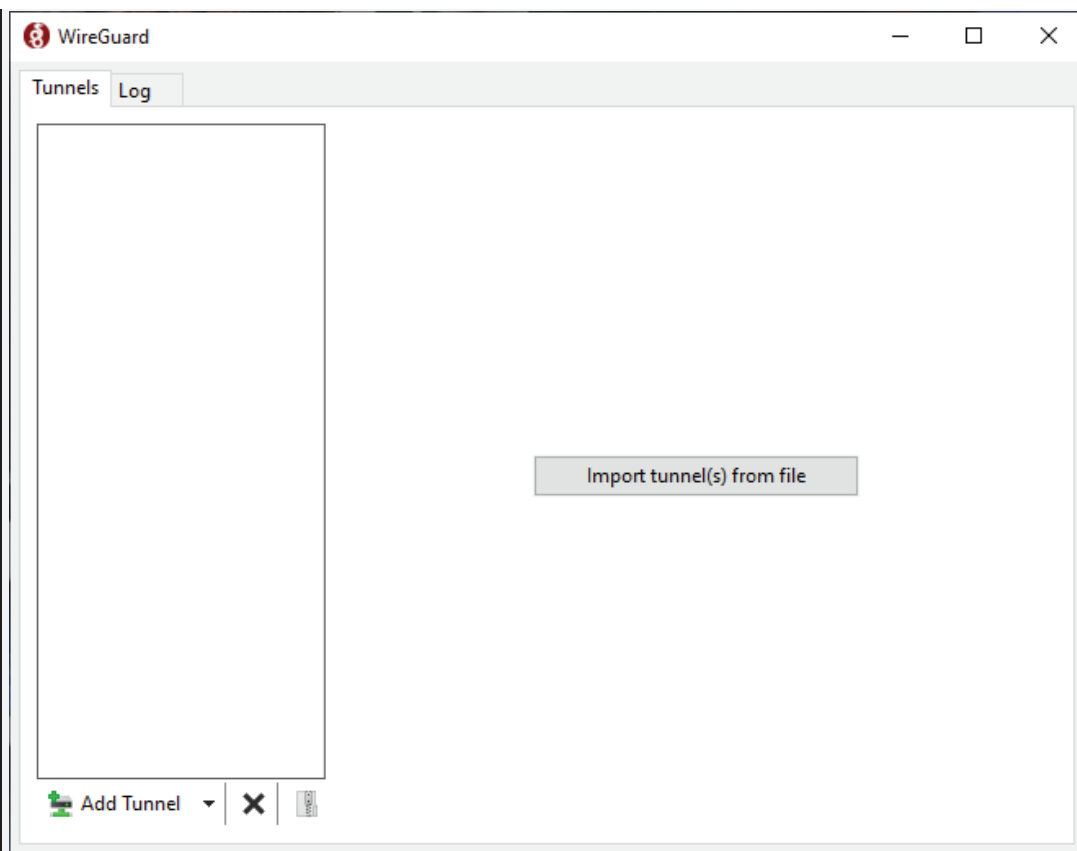
Your plan will automatically renew on 2020-10-25.

Edit Billing Information

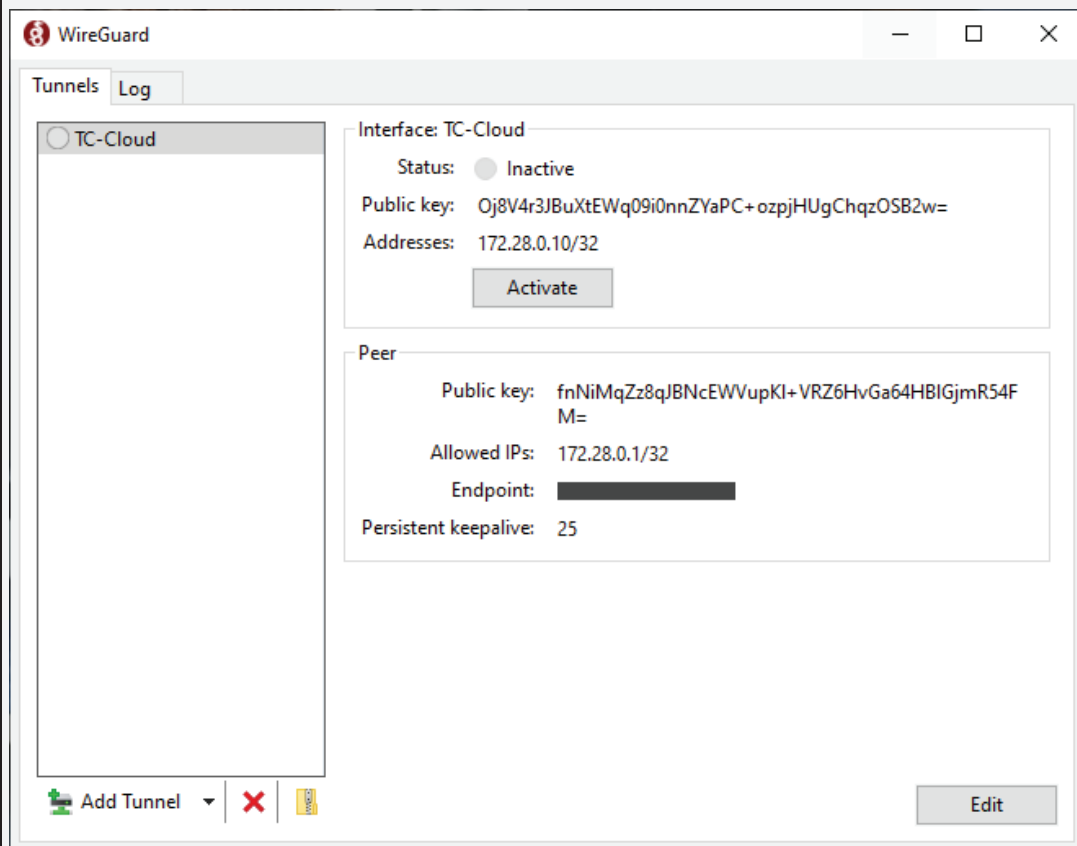
Cancel Subscription

By using this site you agree to the iXsystems EULA and Privacy Policy
2020 © iXsystems Inc - Website Support

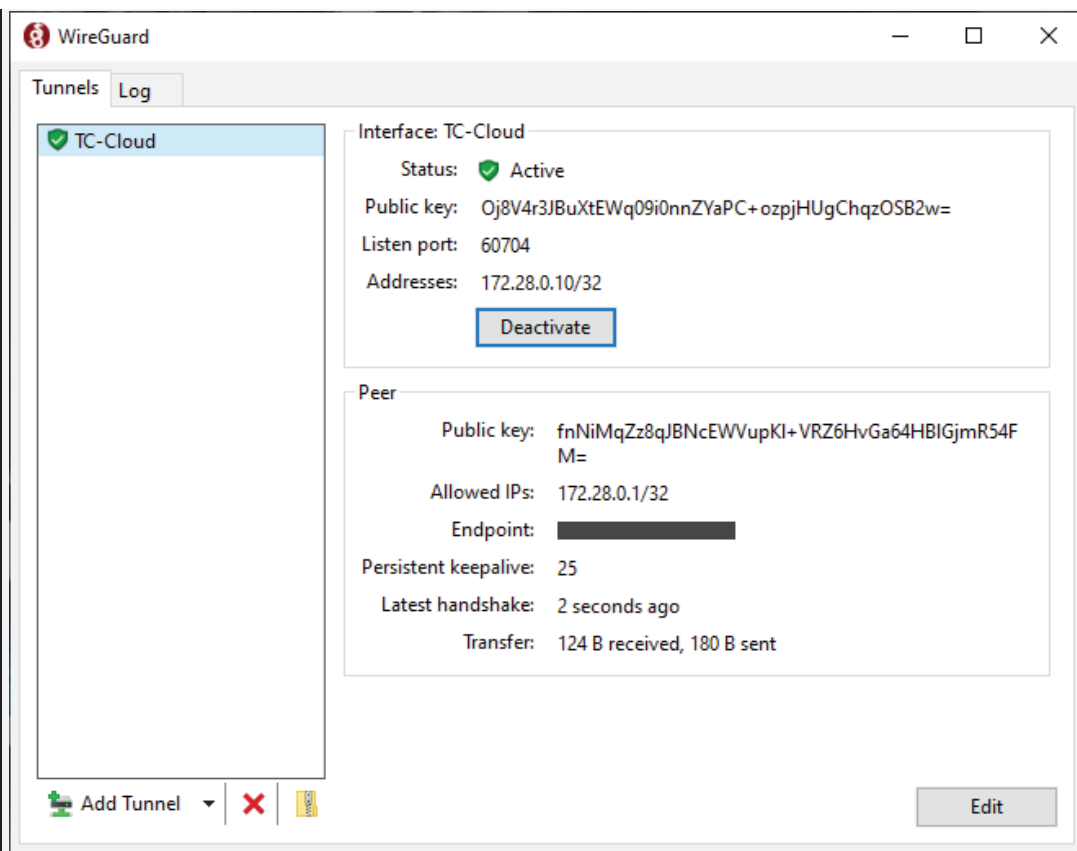
Open Wireguard on your machine and click **Add Tunnel**.



Select the TrueCommand WireGuard Configuration file you downloaded.



Click **Activate** to initialize the Wireguard tunnel.



See the [WireGuard home page](#) for more information on WireGuard and WireGuard clients.

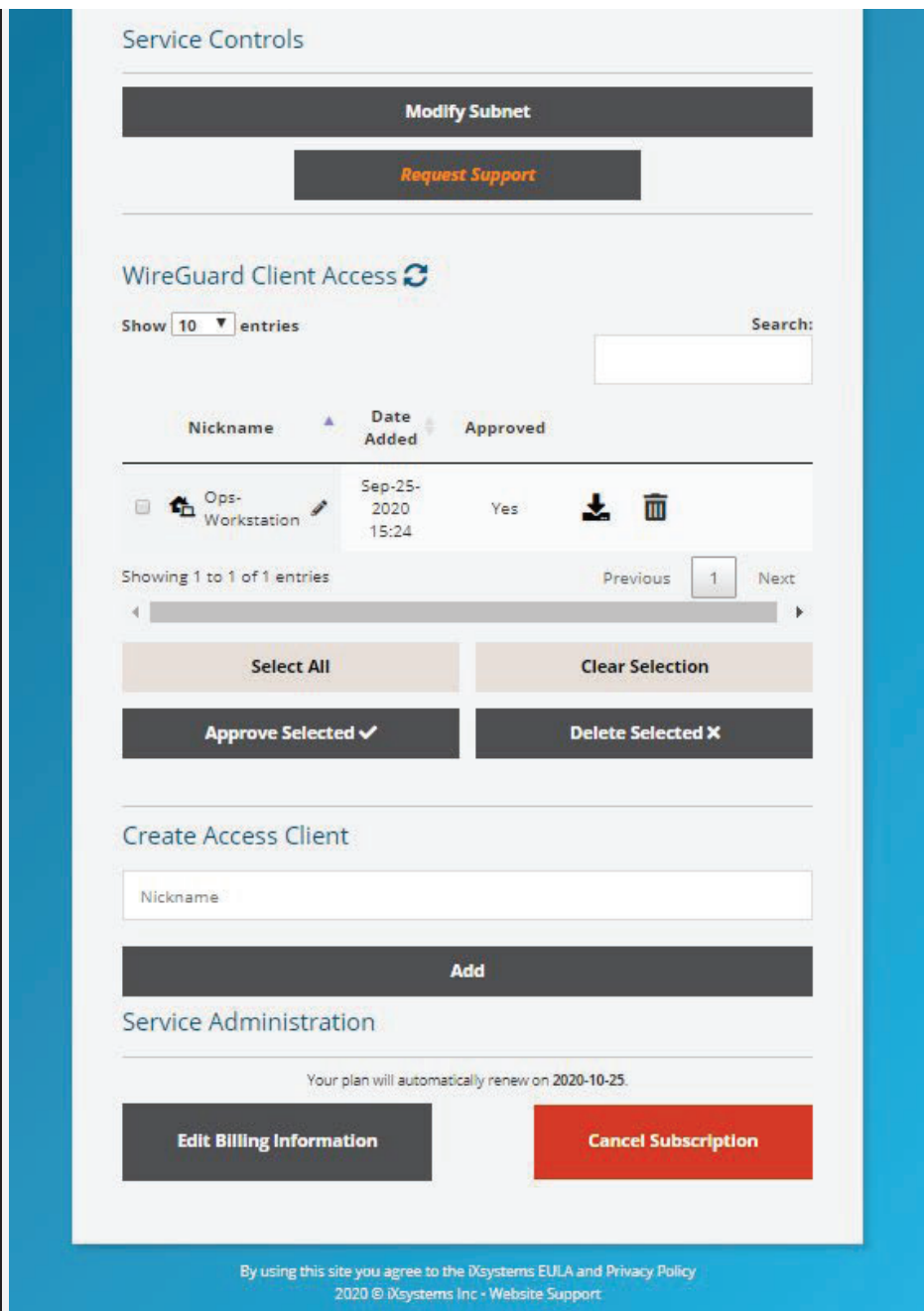
The TrueCommand Cloud IP address is on the iXsystems account portal.

When WireGuard is active, log in to the TrueCommand Cloud interface by clicking the TrueCommand IP address on the portal, or manually enter the TrueCommand Cloud IP in a browser.

Connecting Systems to a TrueCommand Cloud Instance

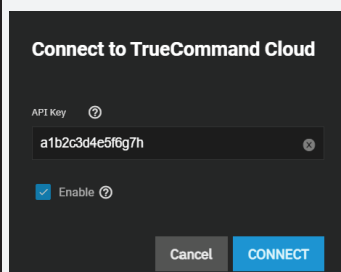
Log into the iXsystems cloud account and click **Manage**. Under **Service Details**, copy the **TrueCommand API Key**.





Log into a TrueNAS system and click the TrueCommand icon in the upper right.

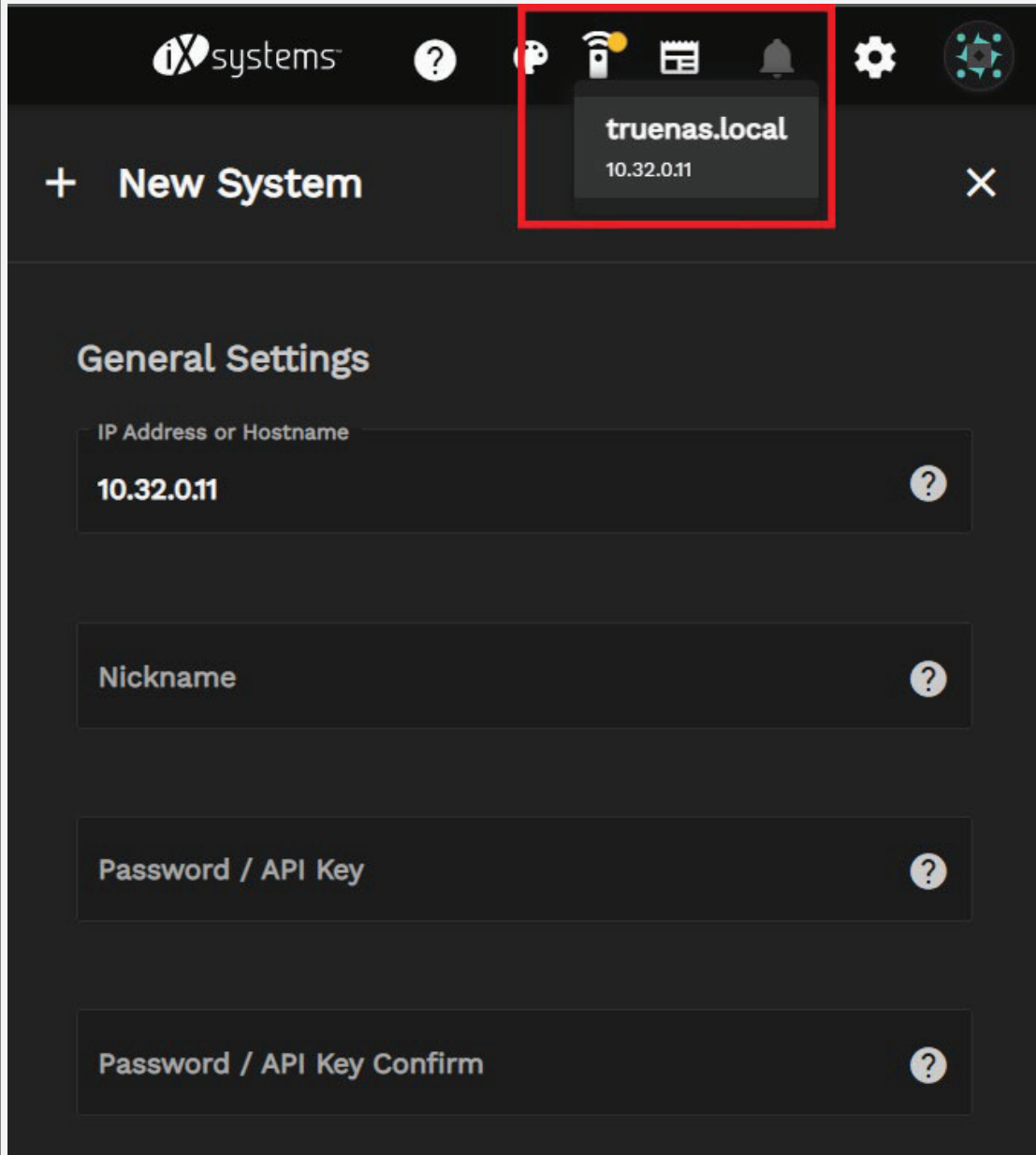
Paste the TrueCommand API Key copied from the iXsystems Account Portal into the TrueNAS dialog window.



When the True Command logo starts moving, check the TrueCommand Cloud email address for a verification message. The email contains a link to the portal to confirm the connection and activate the TrueNAS system.

Click the **Discovered Systems** icon and select the TrueNAS system. TrueCommand automatically fills out

the IP field using the WiredGuard address. Fill in the TrueNAS system nickname and password information from the TrueNAS system, and click **Add System**.



The screenshot shows the 'New System' configuration interface in TrueCommand. At the top, a navigation bar contains several icons, including a red box highlighting the 'truenas.local' dropdown menu which also shows the IP '10.32.0.11'. Below this, the 'General Settings' section contains four input fields: 'IP Address or Hostname' (pre-filled with '10.32.0.11'), 'Nickname', 'Password / API Key', and 'Password / API Key Confirm'. Each field has a help icon (question mark) to its right.

The TrueNAS instance can take 10 to 15 minutes to fully sync up with TrueCommand Cloud. When all systems are connected to TrueCommand Cloud, refer to the [TrueCommand Administration articles](#) for more instructions about setting up configuration backups, alerts, reports, and role-based access control.

Docker (Linux) expand ☐

Installing the TrueCommand Container

If you haven't already installed Docker on your machine, install the [Docker Engine](#), then install [Docker Desktop](#).

To run TrueCommand in Docker on Linux, you must have:

- A 64-bit Linux distro (we recommend Debian)
- Linux Kernel Support: 4.x+
- 1 CPU with 2 GiB RAM

- 1 Hard Disk with 10 - 50 GiB storage space
- Customer networking settings and internet access

Before fetching the TrueCommand docker image, create a local directory. Enter `mkdir directory`, replacing *directory* with the new name.

After creating the new directory, fetch and run the TrueCommand Docker image.

Open a terminal and enter `docker run --detach -v "/hostdir:/data" -p port:80 -p ssl:443 ixsystems/truecommand:latest`.

hostdir is a directory on the host machine for Docker container data, *port* is the TrueCommand web interface port number, and *ssl* is the port number for secure web interface access.

To install the container with an earlier TrueCommand release, replace *latest* with the desired TrueCommand version tag:

```
docker run --detach -v "/DockerDir:/data" -p 9004:80 -p 9005:443 ixsystems/truecommand:1.3.2
```

To install the container with the nightly TrueCommand release, replace *latest* with *nightly*:

```
docker run --detach -v "/DockerDir:/data" -p 9004:80 -p 9005:443 ixsystems/truecommand:nightly
```

Only use the nightly version on test systems.

Although Docker containers have several run methods, TrueCommand requires `-v /hostdirectory:/data` to function.

Do not try to use the same *hostdirectory* for two different containers! Doing so results in file conflicts and database corruption.

For a list of TrueCommand versions and tags, see the [Truecommand Docker](#) page.

Accessing the TrueCommand Web Interface

After fetching the TrueCommand Docker container, enter `docker ps` to see details about running containers.

root@debian:/home/	docker	ps							
CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS				NAMES
94aadb0be454	ixsystems/truecommand	"/start-truecomm..."	42 seconds ago	Up 40 seconds	0.0.0.0:80->80/tcp, 0.0.0.0:443->443/tcp,				modest

Use the port assigned to the container to access the web interface. The list from `docker ps` contains a **PORTS** column. Find the port associated with the *ixsystems/truecommand:latest* IMAGE. The **PORTS** entry is listed as *0.0.0.0:port->80/tcp, 0.0.0.0:sslport->443/tcp* where *port* and *sslport* are the ports specified earlier.

To access the web interface with no encryption, enter `hostsystemIPAddress:port` in a browser address bar, where *hostsystemIPAddress* is the IP address of the host system that is running the TrueCommand Docker container. To access the web interface with standard SSL encryption, enter `https://hostsystemIPAddress:sslport` in a browser address bar.

The connection can't be established? expand ☐

When a connection to the web interface cannot be established, add the container ports as an exception to the host system firewall.

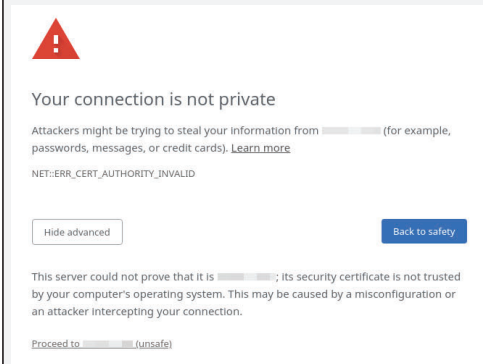
Adding Browser Security Exceptions

TrueCommand uses a [self signed certificate](#) for a secure connection. Because of this, many Internet browsers consider the IP address or DNS host name untrustworthy. In these cases, the IP address or DNS host name must be added as an exception to the browser to access the web interface. Adding an exception is shown here for two different browsers, but the procedure is similar for most browsers.

Browser Security Exceptions

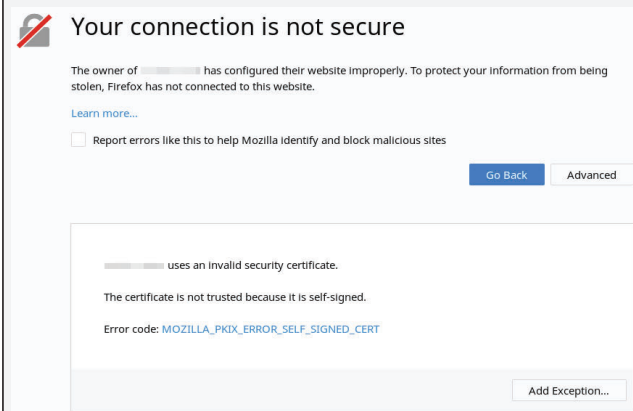
Chrome expand

Click **Advanced** to view information about the error code. Click **Proceed to hostname (unsafe)**.

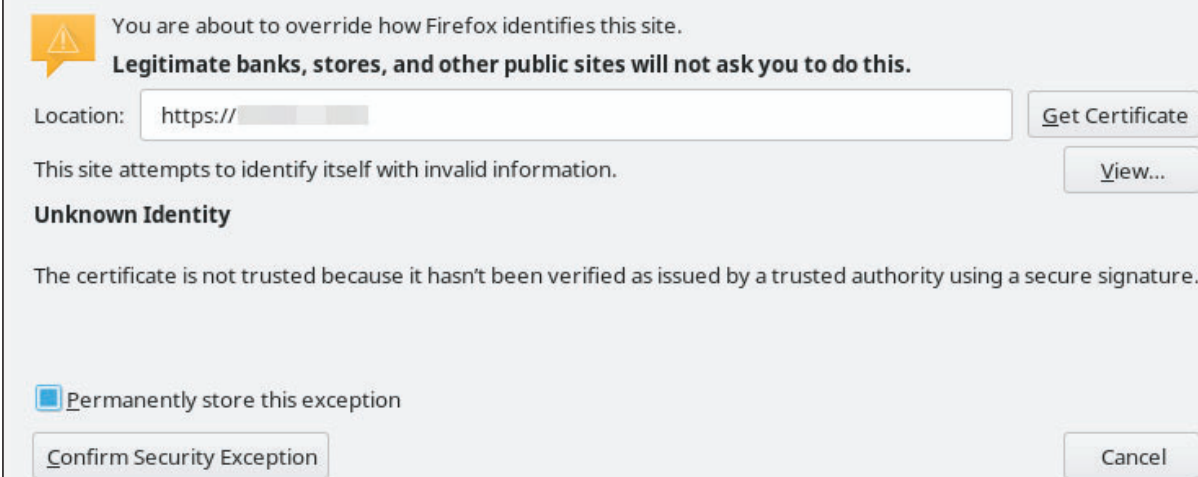


Firefox expand

Click **Advanced** to view information about the error code.



Click **Add Exception...** Set **Permanently store this exception** to permanently store the IP address or DNS host name in Firefox. Click **Confirm Security Exception**.

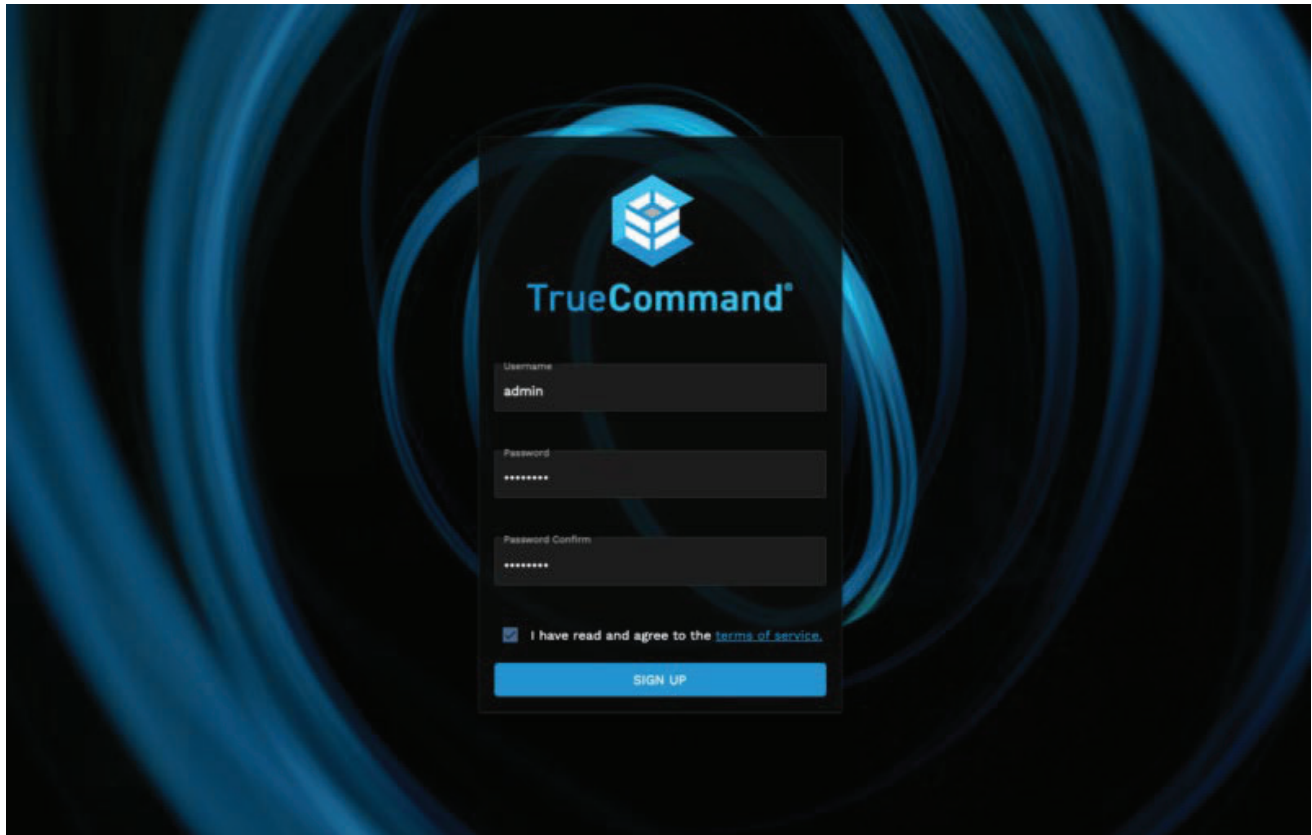


Creating the Administrator Account

Accessing the interface for the first time prompts to create an administrator account.

Follow these steps to create a new admin user:

- Enter a username and password.
- Read the Terms of Service, set **I have read and agree to the terms of service**, and click **SIGN UP**.



- The TrueCommand login screen reappears and you can now use these administrator credentials to log in to the TrueCommand web interface and begin connecting TrueNAS systems, creating more login accounts, and configuring statistical reports.

4.1.1 - Update Docker

- - [Docker Container Commands](#)
 - [Update Process](#)

Updating TrueCommand installed in a Docker container requires stopping the existing container, obtaining the latest software image from the `ixsystems/truecommand` hub, and starting an updated container using the preexisting TrueCommand storage volume.

This article shows how to do this using the command line, but different container management applications can be used to accomplish the same task. Log in to the Docker host system for the container update process.

On Linux systems, `docker` commands need to be run as the `root` account. You might need to add `sudo` in front of the example command to run the command as `root`: `sudo docker image pull ixsystems/truecommand`.

To view all active containers, enter `docker ps`:

```
joe@joe-minty:~$ sudo docker ps
[sudo] password for joe:
CONTAINER ID   IMAGE                                COMMAND                  CREATED
STATUS        PORTS                NAMES                    Up 15
d595961d9024   ixsystems/truecommand:latest      "/start.sh"             15 minutes ago
minutes       443/tcp, 0.0.0.0:8080->80/tcp      TrueCmd_contained
```

For the rest of the examples in this article, we'll be referring to `TrueCmd_contained` for the container name. Be sure to replace this with your TrueCommand container name.

You will also need to note the path to the volume that the container uses for your TrueCommand configuration. You'll need to use this volume when starting the updated Docker container to continue using your existing TrueCommand configuration.

Docker Container Commands

There are a few general Docker commands to remember when interacting with a TrueCommand container:

To start or stop the TrueCommand container, enter `docker start <container name>` or `docker stop <container name>` on the Docker host system.

To have the container automatically start when the Docker host system boots, ensure that the Docker daemon is configured to run at system boot and add the `--restart` flag to the initial `docker run` command:

```
docker run --name=<the name to call the container> -v"<local directory>:/data" -p <host port>:80
sslport <host port>:443 --detach --restart ixsystems/truecommand:latest
```

For a full history of every container that the host has run, use `docker ps -a`:

```
joe@joe-minty:~$ sudo docker ps -a
[sudo] password for joe:
CONTAINER ID   IMAGE                                COMMAND                  CREATED
STATUS        PORTS                NAMES                    Up 15
d595961d9024   ixsystems/truecommand:latest      "/start.sh"             15 minutes ago
minutes       443/tcp, 0.0.0.0:8080->80/tcp      TrueCmd_contained
214a0275a216   phpmyadmin/phpmyadmin             "/docker-entrypoint..." 7 weeks ago
Exited (0) 11 days ago             phpmyadmin
0a68db912cce   phpwork                           "docker-php-entrypoi..." 4 months ago
days ago                               phpwork_1
d0ae8d0a839f   mysql:5.7                         "docker-entrypoint.s..." 4 months ago
Exited (0) 11 days ago             phpwork_mySQL_1
```

Update Process

To update, download the latest TrueCommand image and remove the existing TrueCommand container. Then restart the container using the latest TrueCommand image and preexisting TrueCommand storage volume.

To remove the existing container, enter `docker rm TrueCmd_contained`. Now run `docker image pull`

ixsystems/truecommand. By default, the latest image of TrueCommand is pulled to the Docker host. Start a new container that uses the new image, but make sure to use the preexisting volume that was being used for the original TrueCommand container:

```
docker run --name <the name to call the container> -v "<local host directory>:/data" -p <host port>:80 sslport <host port>:443 --detach ixsystems/truecommand:latest
```

Example without https:

```
sudo docker run --name TrueCmd_contained -v "/home/joe/Documents/TrueCommandContainer:/data" -p 8080:80 -d ixsystems/truecommand:latest
```

When the container is created, Docker will use the image previously downloaded with `docker pull`. A page refresh might be required to view the changes, but previous settings and systems remain available due to the volume reference.

4.1.2 - Migrate Legacy to 1.2+

- - [Process Summary](#)
 - [Preparing an Existing Container for Migration](#)
 - [Migrating a Previous TrueCommand Configuration](#)

Starting with TrueCommand 1.2, TrueCommand is built and offered as a Docker container to drastically reduce system overhead and simplify TrueCommand updates. Migrating data can be done before or after installing the Docker container version of TrueCommand. The procedure is similar in both situations, with just a couple extra steps when the Docker container version of TrueCommand is already installed.

Process Summary

- Preparing an existing container
 - Turn off the container
 - Wipe the container database
- Migrating a previous TrueCommand Configuration
 - Find/Create local system directory to store TrueCommand Docker container data
 - Copy existing TrueCommand configuration files to new directory
 - Transform `ixdb` database into `ixdb.sql` and move `.sql` into container database directory

Preparing an Existing Container for Migration

Migrating the configuration from a previous version of TrueCommand will overwrite any existing configuration! Migrating the configuration before installing the Docker container is recommended, or as soon as possible after installing to prevent making and then losing any new configuration settings.

Migrating a previous configuration into an existing TrueCommand Docker container installation requires wiping the existing database from the container and replacing with the `ixdb.sql` database from the previous version of TrueCommand. Make sure the container is turned off. Open the directory you specified to use for managing the container and find the `ixdb` directory. Remove all existing files from this directory. The container is ready for data migration from the previous version of TrueCommand.

Follow the steps in the next section to transfer the certificate, license, and database files into the existing container configuration directory.

Migrating a Previous TrueCommand Configuration

To move an existing TrueCommand 1.1 or earlier configuration to a Docker container version, follow these migration steps:

1. Create a local system directory for Docker container data. This step is only needed when the Docker container version of TrueCommand is **not** already installed. This directory will contain all the TrueCommand docker container data, including configuration files. For the rest of these instructions, this directory will be referred to as `localhostdirectory/`. When the Docker container is already installed, find the existing `localhostdirectory/` you specified during container installation.
2. Find and copy any existing TrueCommand 1.1 or earlier configuration files to the new `localhostdirectory/`. Using a command like `ssh` or `rsync` is recommended. The Docker container will read these files and apply the existing configuration to the container when it is installed. The table lists the default location and required destination for all the different configuration files TrueCommand 1.1 or earlier can create. Only files that already exist need to be copied to the new TrueCommand `localhostdirectory/`.

Files from TrueCommand 1.1 and earlier	Copy destination in local host directory	Description
--	--	-------------

<code>`/usr/local/etc/truecommand/server. [cert</code>	<code>key].custom`</code>	<code>localhostdirectory/truecommand/</code>
<code>/var/nas-db-backup</code>	<code>localhostdirectory/</code>	Directory tree of NAS configuration backups.
<code>/var/db/.tv_license.sha512</code>	<code>localhostdirectory/</code>	License and signature for the license.

- For the TrueCommand 1.1 `/var/db/ixdb/` database, use `pg_dump ixdb > ixdb.sql` to transform the database into a single `.sql` file. Then move `ixdb.sql` to the `localhostdirectory/` for the TrueCommand Docker container.

You're now ready to install or start the TrueCommand Docker container. Be sure to specify the `localhostdirectory/` during container installation for TrueCommand to load the migrated data.

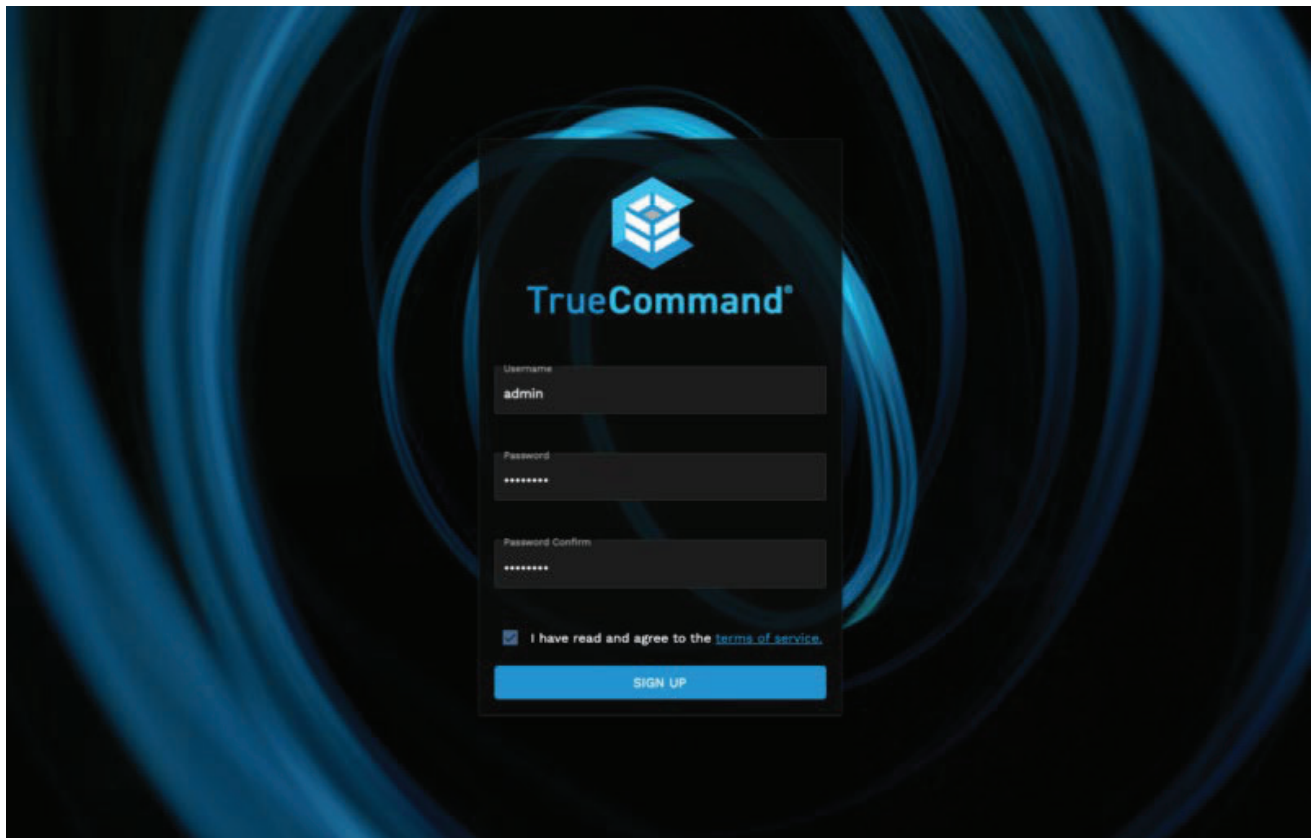
4.2 - Interface Overview

- - [First Time Login](#)
 - [Creating the Administrator Account](#)
 - [Resetting a User Password on the Login Screen](#)
 - [Top Bar](#)
 - [Themeing](#)
 - [Settings Menu](#)
 - [User Menu](#)

First Time Login

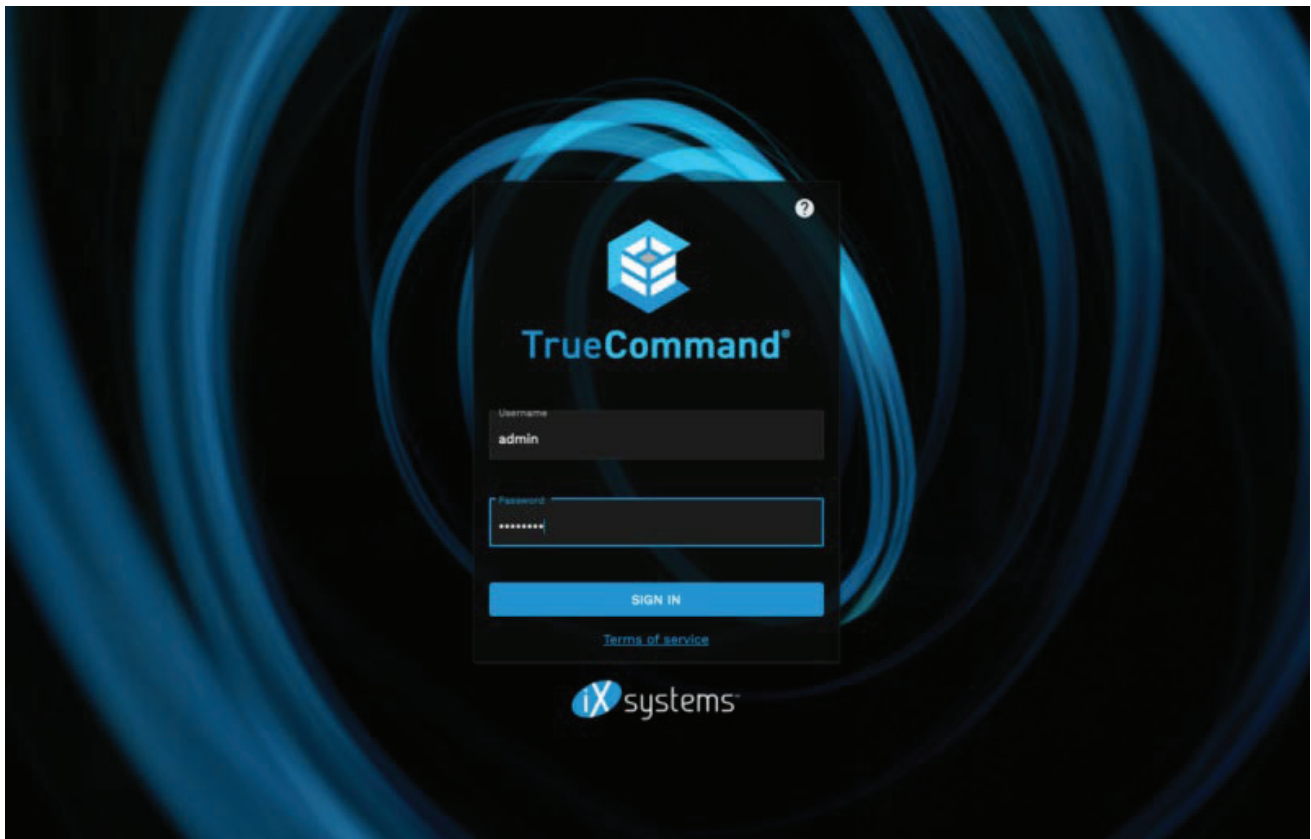
Creating the Administrator Account

When accessing the interface for the first time, you need to create an admin account.



- Enter a username and password.
- Read the Terms of Service, set **I have read and agree to the terms of service**, and click **SIGN UP**.

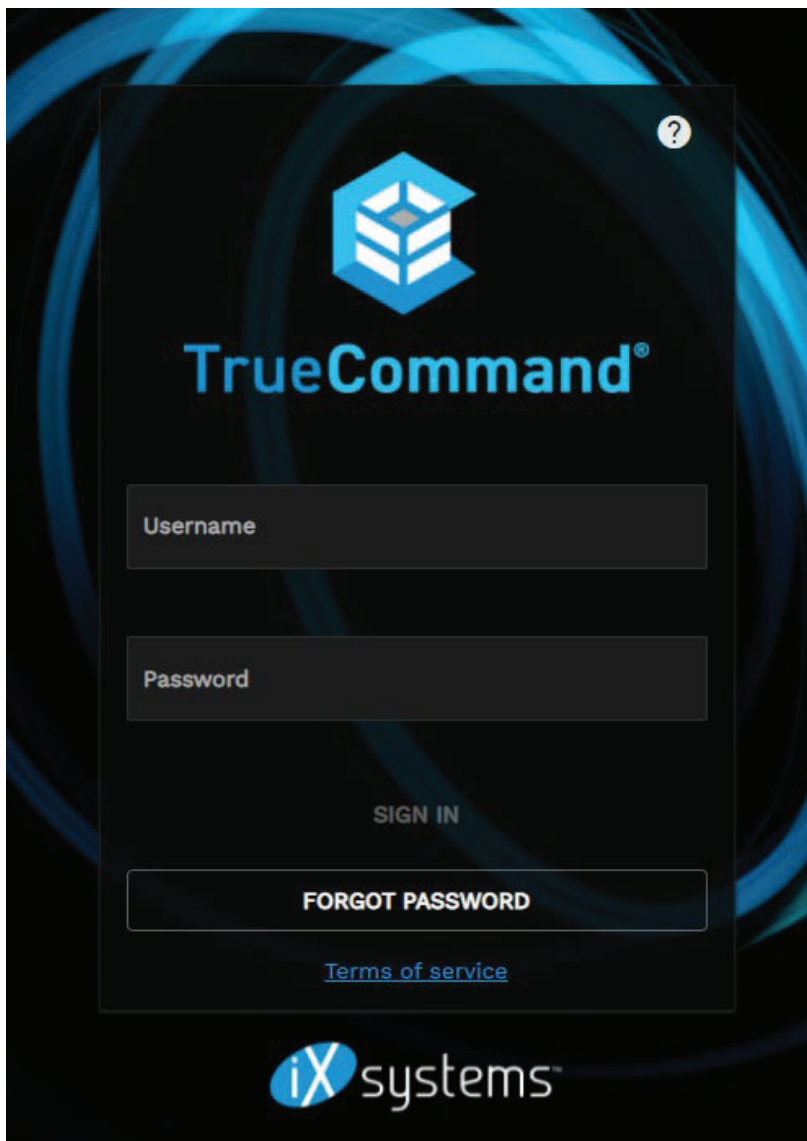
TrueCommand creates the admin login credentials and displays the login page.



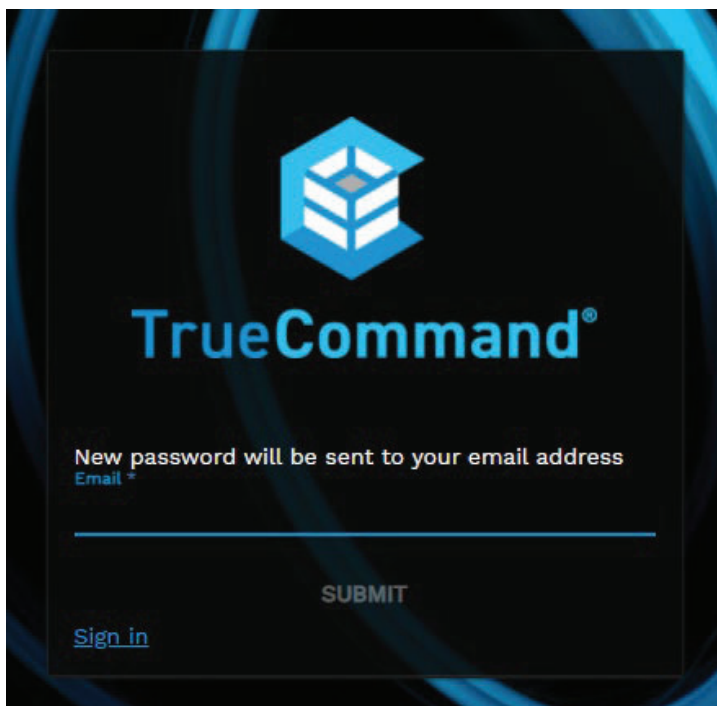
You can now log in to the TrueCommand web interface with the new administrator account credentials.

Resetting a User Password on the Login Screen

TrueCommand users can reset their passwords from the login screen. After typing their username click the **FORGOT PASSWORD** button.



Enter the user email address (or where you want to send the reset login code).



An **[AUTH] TrueCommand Password Reset** email should arrive with the reset password login code. After receiving the code, enter the user name in the login screen and the reset password code and click **SIGN IN**. The user can then go to their profile to change their password.

The screenshot shows the user profile page for 'tazzie'. The page is divided into two main sections. The left section contains the user's avatar, a 'User Details' form with fields for Username (tazzie), Full Name (tazlina may spyworth), Title, Email (erikaj.test.acct@gmail.com), and Phone, and an 'Auth method' section with Password and Password Confirm fields. The right section contains three panels: 'Joined Teams' with a 'CREATE A NEW TEAM' button, 'System Access' with a 'MANAGE SYSTEMS' button, and 'System Groups'.

Top Bar







The top bar has various quick links, configuration options, alerts, and menus.

- Clicking opens the [Cluster Volume](#) page.
- Clicking opens the [iSCSI Manager](#) page.
- Clicking opens the [Reports](#) page.
- Clicking **help** toggles documentation tooltips.
- Clicking opens the [Theme settings](#) dropdown.
- Clicking **newspaper** opens a dialog window with a TrueCommand releases and maintenance news feed.
- Clicking opens the [Alert Notifications](#) page.
- Clicking **settings** opens the settings menu dropdown.
- Clicking the user avatar displays the user **Profile** option where you can set a custom avatar to change the default user gravtar. It also provides access to the **API Interface**, the **EULA** and the **Log Out** options.

Themeing

TrueCommand includes the ability to customize the alert colors to user preferences. The **Theme settings** pallet is located in the top banner on the right. To open the theme configuration menu, click the **palette** icon.

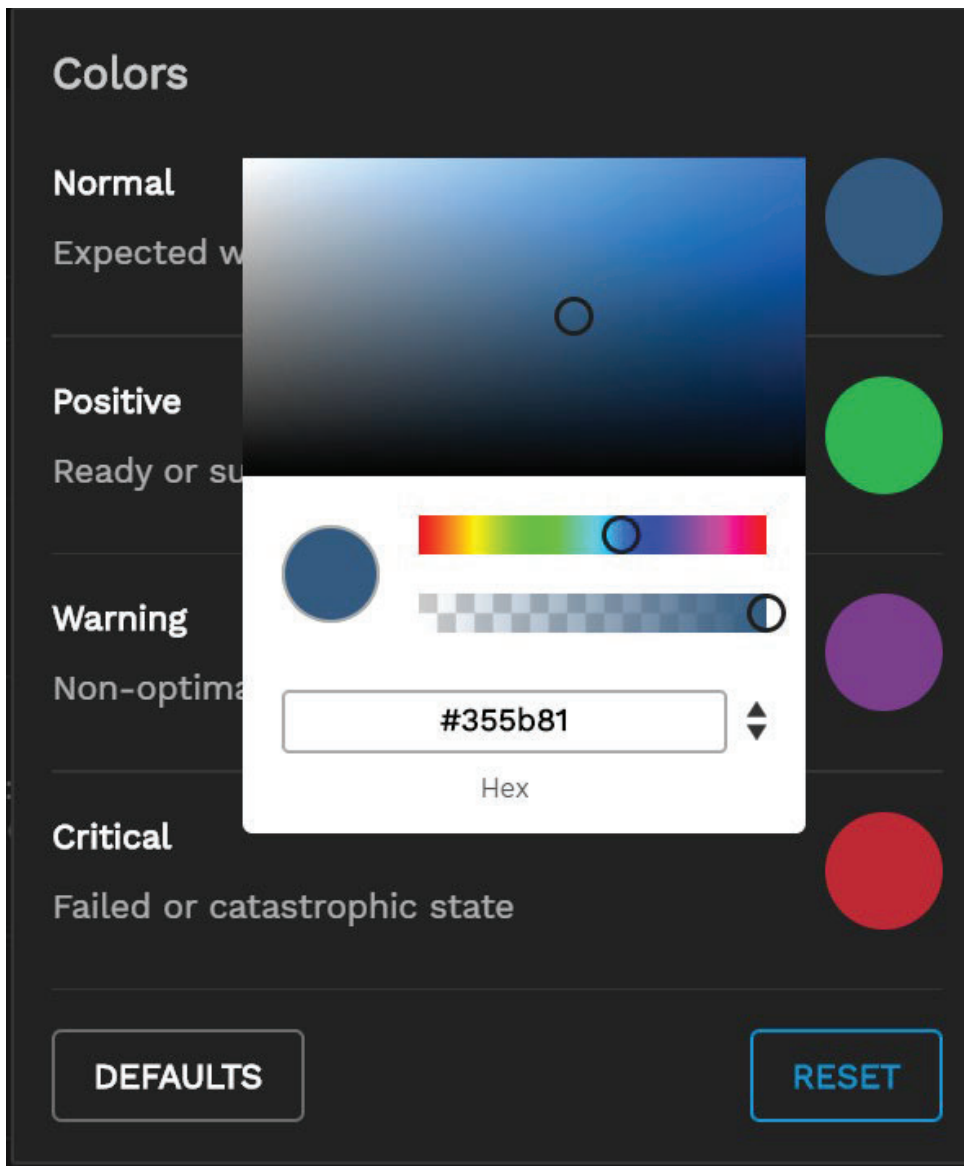
Colors

Normal Expected working state	
Positive Ready or successful state	
Warning Non-optimal state that is not catastrophic	
Critical Failed or catastrophic state	

DEFAULTS

RESET

To change a color, click on the color to open a selection menu, then choose a color or enter its HEX color value.



To remove changes and revert to the currently saved settings, click **RESET**. To reset all colors to the application defaults, click **DEFAULTS**.

Settings Menu

The Settings menu has the following options:

- Clicking opens the main TrueCommand Dashboard.
- Clicking opens the [System Inventory](#) page.
- Clicking opens the [Cluster Volume](#) page.
- Clicking opens the [iSCSI Manager](#) page.
- Clicking opens the [Reports](#) page.
- Clicking `playlist_add_check` opens the [All Alerts](#) page.
- Clicking `notification_important` opens the [Alert Rules](#) page.
- Clicking opens the [Alert Services](#) page.
- Clicking `settings_remote` opens the [Systems](#) page.
- Clicking `person` opens the [Users](#) page.
- Clicking `supervised_user_circle` opens the [Teams](#) page.
- Clicking `short_text` opens the [Logs](#) page.
- Clicking `vpn_key` opens the [Administration](#) page.

User Menu

The user menu (avatar) has the following options:

- Clicking **person** opens the [Users](#) page.
- Clicking opens the [API Interface](#) testing page.
- Clicking opens the [TrueCommand EULA](#).
- Clicking **exit_to_app** logs the user out of TrueCommand.

4.3 - Creating User Accounts

- - [Administrator Accounts](#)
 - [Users Accounts](#)
 - [Two Factor Authentication](#)
 - [Automatic Creation with LDAP](#)
 - [Teams and Permissions](#)
 - [Resetting a User Password at Login](#)

TrueCommand has a robust user management system designed to allow TrueCommand administrators to personalize the TrueCommand experience for each user account. You can create user accounts in the TrueCommand interface. Alternatively, LDAP can automatically create new user accounts when someone logs into TrueCommand with their LDAP credentials.

TrueCommand also organizes user accounts into *teams* so admins can simultaneously manage many user accounts.

Administrator Accounts

TrueCommand has two levels of accounts - administrators, and users:



Administrators can add and remove users and servers. Administrators can also assign users to teams and servers to groups. Administrators have full access to all alerts and reports.

Users, however, can only interact with the servers they are assigned by an administrator. Users can configure alerts and generate reports on their respective systems.

Users Accounts

To create a new user account, open the **Configure settings** menu and click **Users > + NEW USER**. Enter a descriptive user name and an authentication method for the user.

TrueCommand uses the *default* authentication method to create unique credentials for logging in to the web interface. The administrator must provide these credentials to the intended user.


 **New User** 

User Details

☐ TrueCommand® Administrator

Username

Full name

Teams 

Auth method

Password

Password Confirm

CANCEL

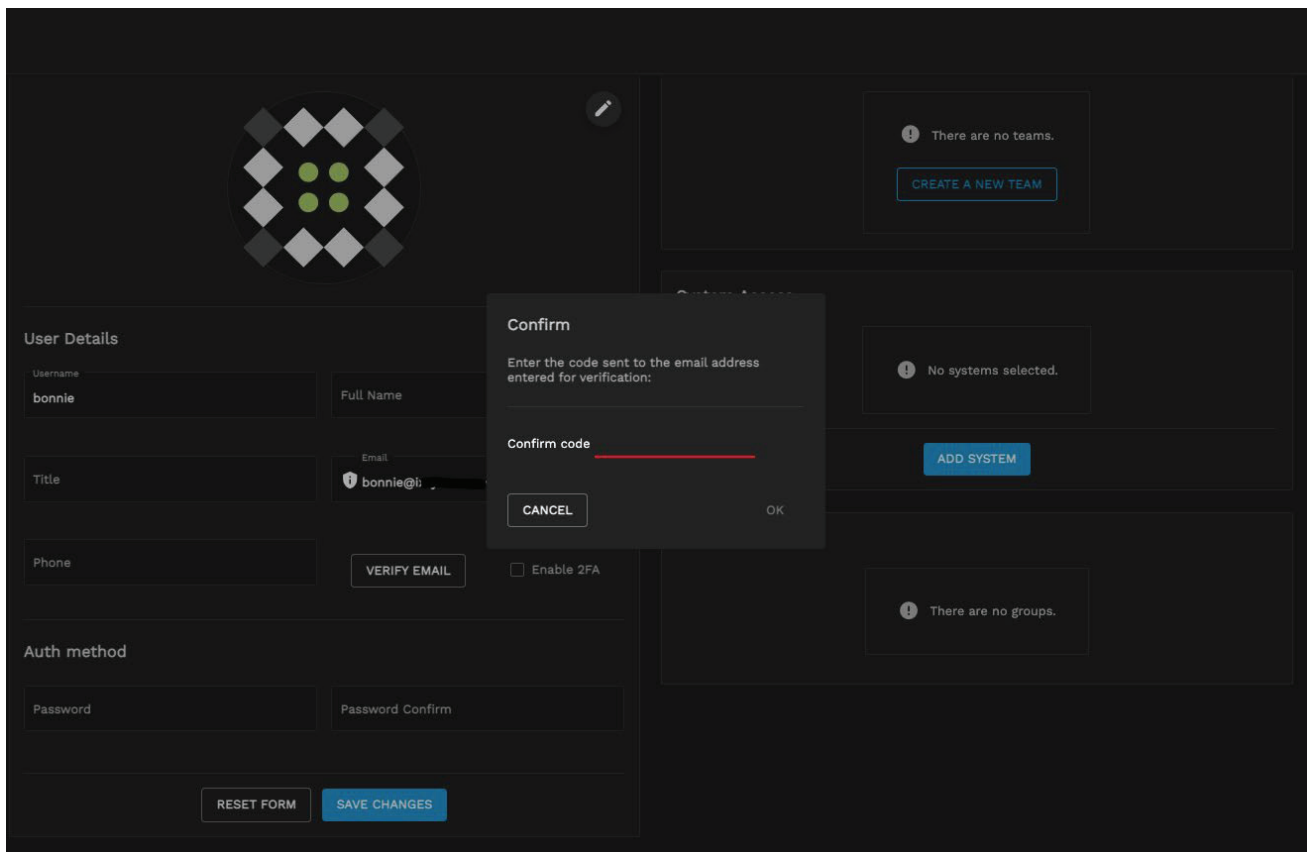
CREATE USER

Two Factor Authentication

Two-factor authentication double-checks the authentication of an account user. The first verification occurs when the user logs in with a username and a password. Two-factor authentication adds an extra step in the process, a second security layer, that re-confirms their identity. If basic password security measures are in place, two-factor authentication makes it more difficult for unverified users to log in to your account.

Enabling two-factor authentication requires an already-authenticated email address. Authenticating a user email address requires first setting up [SMTP Email](#) in **Settings-> Alert Services**.

To verify a user email address and set 2FA:



- Enter the email address for the user and click **Save Changes**.
- Check the user's email account for the verification code. Copy the code from the email.
- Paste the code in the **Confirmation code** field in the confirmation window. Click **OK**.
- Set **Enable 2FA** and click **Save Changes**.

Automatic Creation with LDAP

TrueCommand supports using [LDAP](#) to better integrate within an established network environment. *LDAP/AD* allows using single sign-on credentials from the [Lightweight Directory Access Protocol \(LDAP\)](#) or [Active Directory \(AD\)](#). Users can log in with an LDAP or AD account without creating a separate TrueCommand login.

LDAP and AD require the server IP address or DNS hostname and domain to use. The LDAP or AD Username (optional) is required when the TrueCommand user name does not match the LDAP or AD credentials.



Click on the **settings (Gear) > Administration**.

Click on the **Configuration** tab and scroll down to access the LDAP configuration section. Click **ADD SERVER** to begin configuring LDAP in TrueCommand. The screen changes to display the LDAP configuration settings fields.

LDAP

☐ Allow LDAP user creation

Ldap Servers

LDAP Server URL	Domain	 
Group Domain	<input checked="" type="checkbox"/> Verify SSL	
User ID Field	Group ID Field	
BIND User Domain	BIND Password	

ADD SERVER

To configure LDAP, type the LDAP server IP address or DNS hostname into the **LDAP Server URL** field, type the domain name in the **Domain** field, and click **ADD SERVER**. You can add multiple LDAP servers and domains.

The **Test LDAP Config** icon opens a window that allows you to test your connection to the LDAP server. The **Remove LDAP Server** icon removes the selected LDAP server.

LDAP

☐ Allow LDAP user creation

Ldap Servers

LDAP Server URL

Domain

Group Domain

☒ Verify SSL

User ID Field

Group ID Field

BIND User Domain

BIND Password

ADD SERVER

LDAP Teams

!

There are no teams.

CREATE A NEW TEAM

Field	Value
LDAP Server URL (string, required)	IP or DNS name of the LDAP server, with port number on the end. Example: <i>ldap.mycorp.com:636</i> (SSL port is typically 636 for AD/LDAP)
Domain (string, required)	Base domain settings of the user. Example: <i>dc=mycorp,dc=com</i> for a typical username@mycorp.com user account
Group Domain (string)	The alternative domain setting to use when searching for groups. The default value is the same as Domain
Verify SSL (bool)	Require strict SSL certificate verification. The default value is false. Disable this option if the hostname of the system is different than the one listed on the SSL certificate, an IP is used for the connection instead of the DNS hostname, or if a self-signed certificate is used by the LDAP server.
User ID Field (string)	Domain fieldname to use for user-matching. The default value is uid (user ID). Another field commonly-used is cn (common name)
Group ID Field (string)	The domain fieldname to use when searching for a group name. The default value is cn (common name).
BIND User Domain (string)	The full domain setting for a pre-authenticated bind to the server. Example: <i>uid=binduser,cn=read-only-bind,dc=mycorp,dc=com</i> For an unauthenticated bind set this field to just a name (example: <i>truecommand-bin</i>). This is sometimes used for logging purposes on the LDAP, but otherwise is not validated.

BIND Password (string)	The password to use for the bind user. For an unauthenticated bind, leave this field blank while setting the BIND User Domain to a non-empty value.
------------------------	---

LDAP connection options

TrueCommand supports two common methods of validating LDAP user credentials:

Direct Bind

The direct BIND method uses the **Domain** and **User ID Field** values to create a static domain string for user authentication.

Example:

- Domain: *dc=mycorp,dc=com*
- User ID Field: *uid*

When *bobby.singer* attempts to log in, TrueCommand establishes an SSL-secure connection to the LDAP server and then attempts to bind with the static domain *uid=bobby.singer,dc=mycorp,dc=com* and the user-provided password. If successful, the user authentication is verified, and Bobby Singer may access TrueCommand.

Indirect Bind

The indirect BIND authentication method is more dynamic and searches for the proper user domain settings rather than making format assumptions. With TrueCommand, indirect BIND configures a *bind user* (typically a read-only, minimal-permissions user account) with a known domain/password to perform the initial bind to the LDAP server. Once logged in, TrueCommand searches for the user domain currently requesting to login. It then attempts a second bind with the user domain and provided password.

Example:

- Domain: *dc=mycorp,dc=com*
- User ID Field: *uid*
- BIND User Domain: *uid=binduser,cn=read-only-bind,dc=mycorp,dc=com*
- BIND Password: *pre-shared-key*

When *bobby.singer* attempts to log in, TrueCommand establishes an SSL-secure connection to the LDAP server. TrueCommand uses the **BIND User Domain** and **BIND Password** settings to perform an initial bind using pre-known settings from your LDAP provider. Once bound, TrueCommand searches for the user matching *uid=bobby.singer*, but only within the subdomains that include the domain setting (*dc=mycorp,dc=com* in this example). If TrueCommand finds a user, it uses the entire user domain string from the search result to initialize a second bind along with the user-provided password. If successful, TrueCommand verifies the user authentication, and Bobby Singer is allowed access to TrueCommand.

SSL/TLS Connection Info

WARNING: AD/LDAP authentication *requires* SSL connections.

If the LDAP server uses an SSL certificate generated by a custom certificate authority (CA), then one of two things must occur before TrueCommand can use the LDAP server:

- (Option 1) Users must register the custom certificate authority with TrueCommand via the **Certificates** tab on the **Administration** screen.
- (Option 2) Users can disable the **Verify SSL** option to accept whatever SSL certificate the server provides. Users might need to choose Option 2 if the LDAP server hostname differs from the one listed on the certificate or if the server uses a self-signed SSL certificate.

Selecting **Allow LDAP user creation** means TrueCommand creates user accounts when someone logs in to the User Interface with their LDAP credentials. **JOIN TEAM** automatically adds LDAP users to specific TrueCommand teams.

Teams and Permissions

You can assign users to existing teams by selecting a team from the **Teams** drop-down to add the user to that team. You can assign users to multiple teams. TrueCommand applies team permissions to any user added to a team, but setting specific permissions for the user can override related team permissions. For more indepth information regarding teams, see the [Teams Documentation](#).

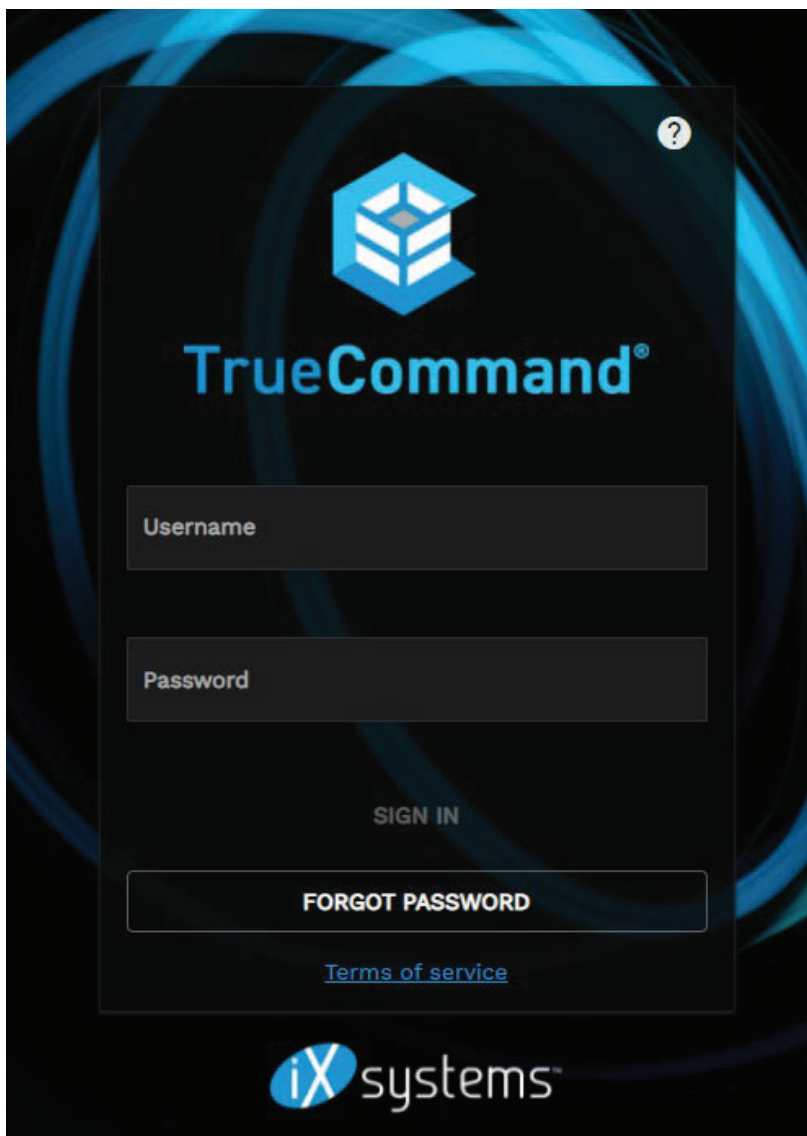
To limit non-administrative account access to connected systems, configure the **System Access** and/or **System Groups** sections. This requires first configuring [system connections](#) and/or system groups in TrueCommand.

Click **ADD SYSTEM** and select a system from the drop-down to give the user access to that system. To restrict the user to only viewing details about the system, set the **read** permission. To remove user access to a particular system, click - (minus) on that system.

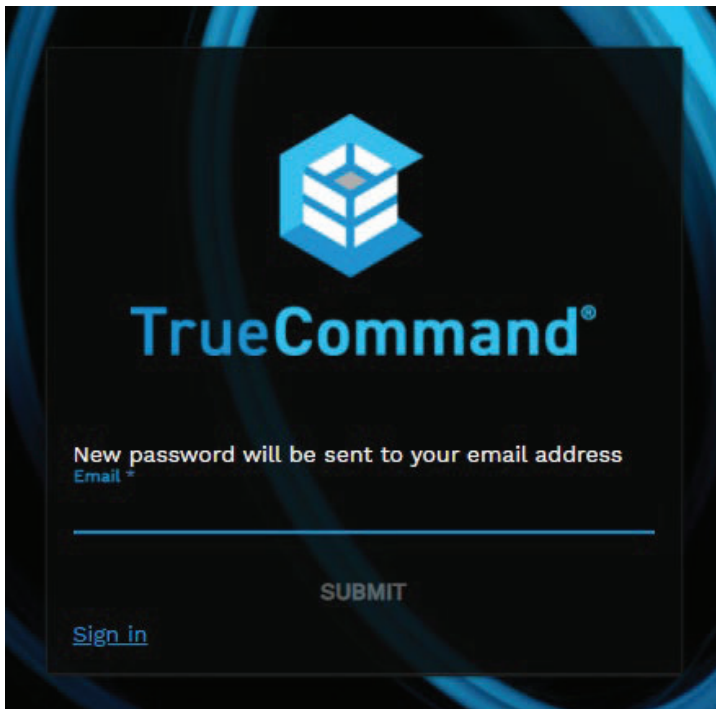
When system groups are available, an **ADD GROUP** button displays. Click **ADD GROUP** and select a group from the drop-down list to give the user access to all the systems in that group. To assign a user a type of access to the group, choose **read** or **read/write** permissions. To remove user access to a particular system group, click - (minus) on the desired group.

Resetting a User Password at Login

TrueCommand users can reset their passwords from the login screen. After typing their username click the **FORGOT PASSWORD** button.

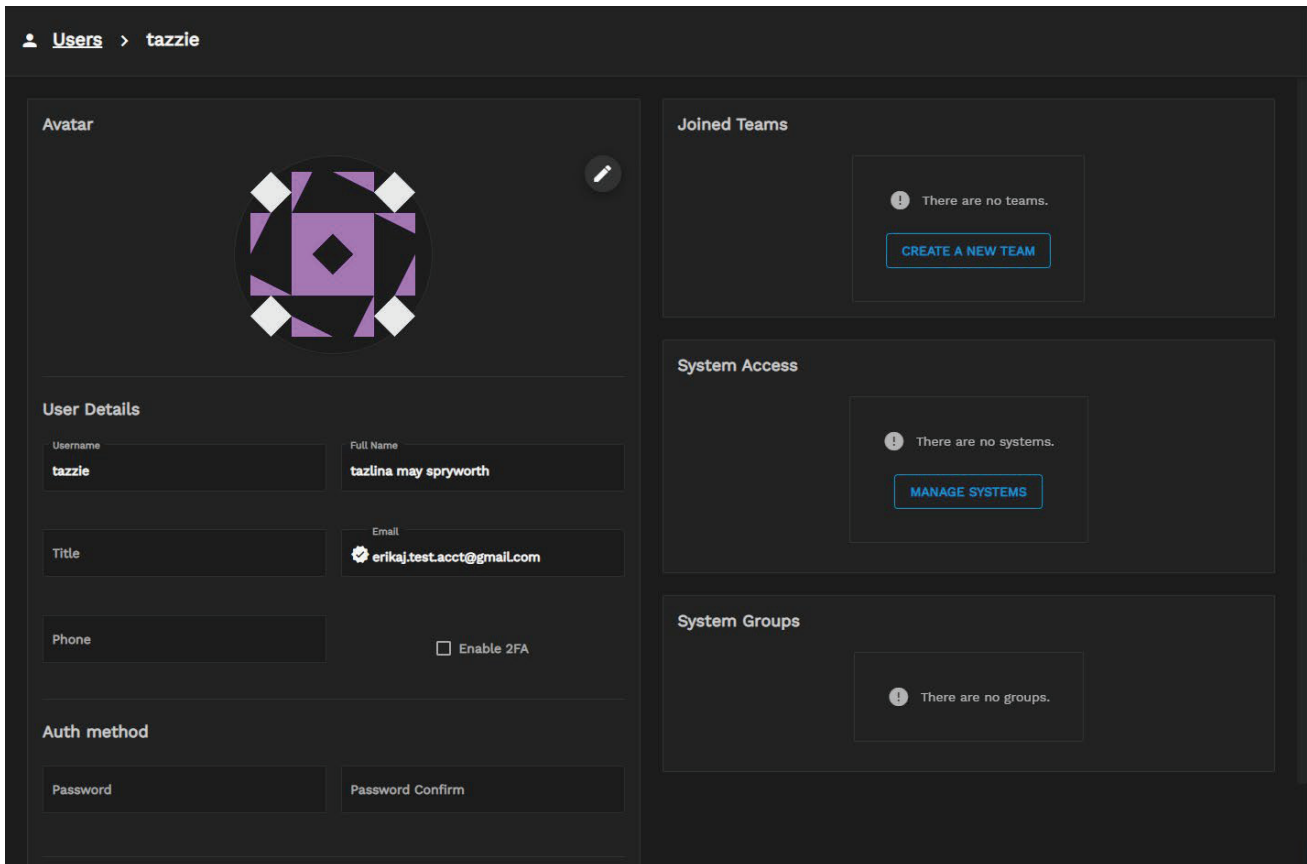


Enter the user email address (or where you want to send the reset login code).



The image shows a TrueCommand password reset form. At the top is the TrueCommand logo, a blue hexagon with a white cube inside. Below the logo, the text "TrueCommand®" is displayed in blue. Underneath, a message states "New password will be sent to your email address". Below this message is a text input field labeled "Email *". At the bottom of the form is a "SUBMIT" button. In the bottom left corner, there is a link that says "Sign in". The entire form is set against a dark background with blue abstract patterns.

An **[AUTH] TrueCommand Password Reset** email should arrive with the reset password login code. After receiving the code, enter the user name in the login screen and the reset password code and click **SIGN IN**. The user can then go to their profile to change their password.



The image shows a user profile page in TrueCommand. The page has a dark theme. At the top, there is a breadcrumb navigation: "Users > tazzie". The main content area is divided into two columns. The left column contains the user's profile information, and the right column contains system-related information.

User Profile Information:

- Avatar:** A circular profile picture with a purple and white geometric pattern. There is an edit icon (pencil) to the right of the avatar.
- User Details:**
 - Username:** tazzie
 - Full Name:** tazlina may spryworth
 - Title:** (empty field)
 - Email:** erikaj.test.acct@gmail.com
 - Phone:** (empty field)
 - Enable 2FA:** ☐
- Auth method:**
 - Password:** (empty field)
 - Password Confirm:** (empty field)

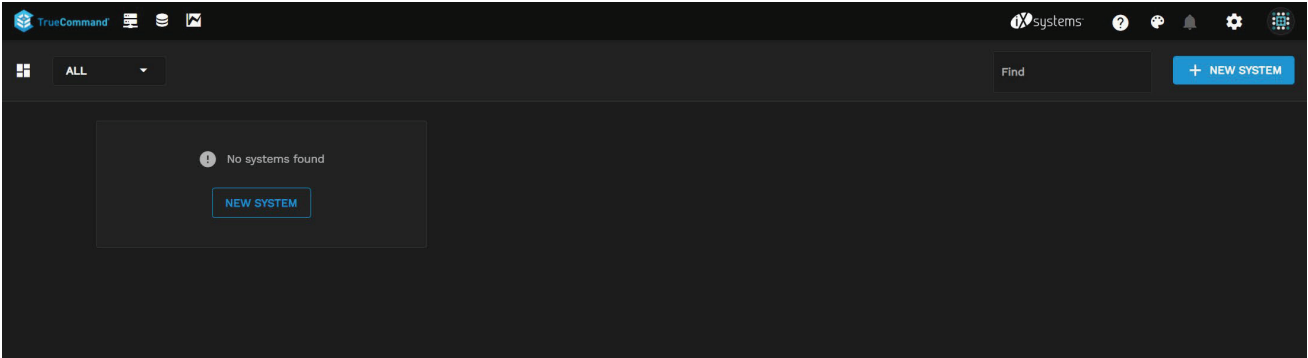
System Information:

- Joined Teams:** A message says "There are no teams." with a "CREATE A NEW TEAM" button.
- System Access:** A message says "There are no systems." with a "MANAGE SYSTEMS" button.
- System Groups:** A message says "There are no groups." with no visible button.

4.4 - Connecting Your First TrueNAS System

- [Connecting Your First TrueNAS System](#)
 - [Adjusting Systems](#)
- [Organizing Systems into Groups](#)
- [Connecting Systems to a TrueCommand Cloud Instance](#)
 - [Getting an API Key](#)
 - [Connecting from the TrueNAS UI](#)
 - [Approving the Connection Request](#)
- [Making Manual Connections](#)

Connecting Your First TrueNAS System



To connect your first system to TrueCommand, click **NEW SYSTEM** on the dashboard.

A screenshot of the 'New System' form in TrueCommand. The form has a title bar with a plus icon and a close icon. It contains four input fields: 'IP Address or Hostname', 'Nickname', 'Password / API Key', and 'Password / API Key Confirm'. Each field has a help icon (a question mark in a circle). At the bottom, there are three buttons: 'RESET FORM', 'ADD AND CONTINUE', and 'ADD SYSTEM'.

Setting	Description
IP Address or Hostname	The system’s IP address or DNS host name.
Nickname	Required short-form identifier for this system. You cannot use system nicknames more than once.
Password / API Key	New password or API key. TrueCommand hides characters for security.
Password / API Key Confirm	Re-enter the password or API key.

Enter the system IP address or DNS host name, then enter a system nickname and password.

Click **RESET FORM** to clear the fields and reset the form if you make a mistake. To display the list of systems in TrueCommand, click the **settings** icon and select either **System Inventory** or **Systems**.

Systems

+ NEW SYSTEM
+ NEW GROUP

Systems
System Groups

Filter

NICKNAME	HOSTNAME	CONNECTION	LAST SYNC	UPDATES
fn_miniv2.0	truenas.local	Connected		
gm1	truenas.local	Connected		Available
gm4	Gremlin4.local	Connected		Available
sc01_cluster		OFFLINE		
tn02_ha	tn02a.qe.ixsystems.net	Connected		Available
tn03	tn03a.qe.ixsystems.net	Connected		Available
tn36		OFFLINE		

Adjusting Systems

Misconfigured systems (such as one created with an incorrect password) appear offline on both the TrueCommand **Dashboard** and **Systems** list.

You can edit a system from the **Systems** list by clicking the edit icon and then enter new connection details. Click **RESET FORM** to clear the fields and reset the form if you make a mistake.

To remove a system from TrueCommand monitoring, click **Delete**.

Organizing Systems into Groups

TrueCommand administrators can organize systems into collections called *groups*.

Grouping systems enables efficient system permissions and reporting management.

Open the **System Groups** tab to view the list of created groups and the systems they contain. Create a group by clicking **Configure settings > Systems > + NEW GROUP**. Enter a name for the new group and click **ADD SYSTEM** to add a system to the group. After you add all the desired systems to the group, click **CREATE GROUP**.

+ New Group
X

General Settings

Group Name

Systems

No systems selected.

ADD SYSTEM

SAVE GROUP

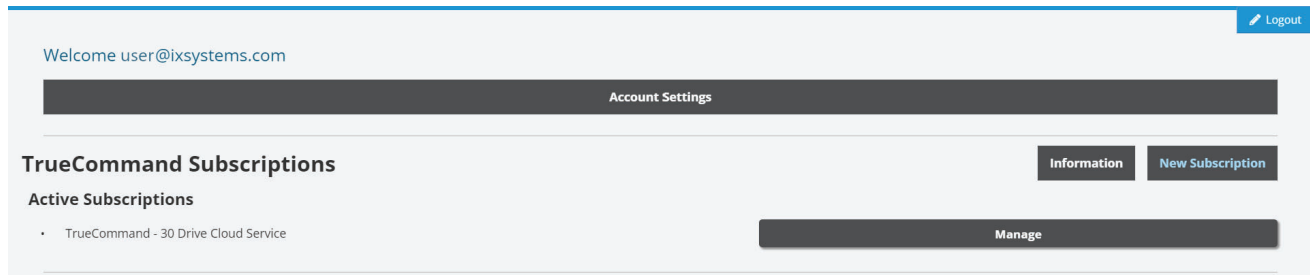
Editing a group allows you to update the group name or change which systems are members of that group.

To delete a system group, click **Delete** . Click **Yes** to confirm the deletion.

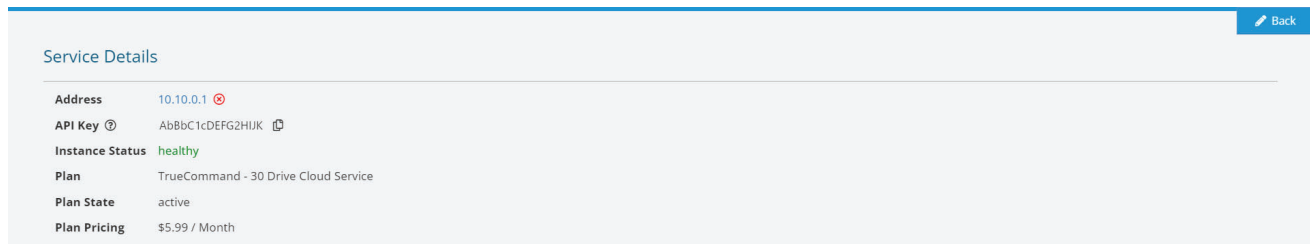
Connecting Systems to a TrueCommand Cloud Instance

Getting an API Key

Log into the ixSystems cloud account and click **Manage**. Under **Service Details**, copy the **TrueCommand API Key**.



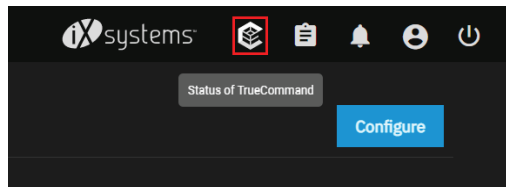
Log into your [ixSystems cloud account](#) and click **Manage** next to your TrueCommand subscription.



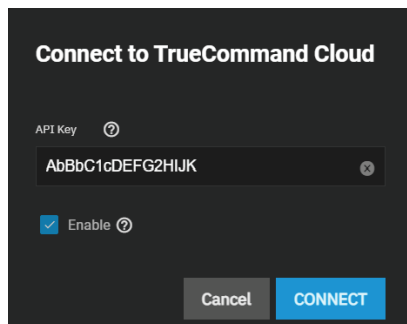
Copy the **API Key** under **Service Details**.

Connecting from the TrueNAS UI

Log into a TrueNAS system and click the TrueCommand icon in the upper right.



Paste the TrueCommand API Key copied from the ixSystems Account Portal into the TrueNAS dialog window.



Approving the Connection Request

When the TrueCommand logo starts moving, check the TrueCommand Cloud email address for a verification message. The email contains a link to the portal to confirm the connection and activate the TrueNAS system.

Click on the **New System** alert, fill in the information from the TrueNAS system, and click **Add System**.

The screenshot shows the TrueNAS TrueCommand web interface. At the top, there is a navigation bar with the iXsystems logo and several icons. A red box highlights a dropdown menu that is open, showing a system entry for 'truenas.local' with the IP address '10.32.0.11'. Below the navigation bar, there is a '+ New System' button. The main content area is titled 'General Settings' and contains four input fields, each with a help icon (question mark in a circle): 'IP Address or Hostname' (containing '10.32.0.11'), 'Nickname', 'Password / API Key', and 'Password / API Key Confirm'.

It can take 10 to 15 minutes for the TrueNAS instance to fully sync up with TrueCommand Cloud. When all systems are connected to TrueCommand Cloud, refer to the [TrueCommand Administration articles](#) for more instructions about setting up configuration backups, alerts, reports, and role-based access control.

Making Manual Connections

To connect a system to TrueCommand, open the **Configure settings** menu and click **Systems**. The **Systems** menu has two tabs: **Systems** and **System Groups**. These tabs contain all the options to connect and organize systems in TrueCommand. TrueCommand lists all added systems and their connection statuses in the **Systems** tab.








To connect a new system, click **+ NEW SYSTEM**.

Enter the system IP address or DNS host name, then enter a system nickname and password. Click **RESET FORM** to clear the fields and reset the form if you make a mistake.

Systems

System Groups

Filter

NICKNAME	HOSTNAME	CONNECTION	LAST SYNC	UPDATES
fn_miniv2.0	truenas.local	Connected		
gm1 	truenas.local	Connected		Available
gm4	Gremlin4.local	Connected		Available
 sc01_cluster		 OFFLINE		
tn02_ha 	tn02a.qe.ixsystems.net	Connected		Available
tn03 	tn03a.qe.ixsystems.net	Connected		Available
 tn36		 OFFLINE		

5 - Administration

Initial configuration and general administration articles.

TrueCommand includes an easy to use interface for administrative configurations. Access to some of these areas may require a TrueCommand administrator account.

- NAS Fleet Administration
 - NAS Configuration
 - Creating NAS groups
 - Alerts for NAS systems
 - Reports of various metrics
- TrueCommand Instance Administration
 - TrueCommand Configuration Options
 - TrueCommand system Audit Logs
 - User and Team Management
 - UI Theme settings

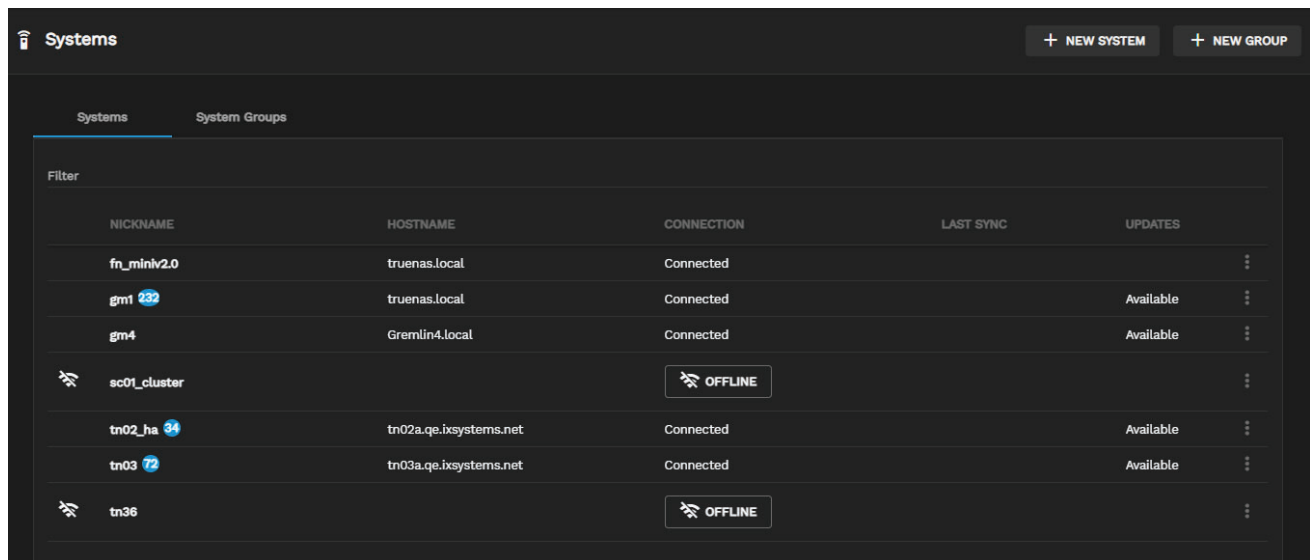
Ready to get started? Choose a topic or article from the left-side **Navigation** pane. Click the < symbol to expand the menu to show the topics under this section.

5.1 - Systems








- - [Connecting Systems to TrueCommand](#)
 - [Adding a System Manually](#)
 - [Adjusting Systems](#)
 - [Organizing Systems into Groups](#)
 - [Managing Groups](#)

Connecting Systems to TrueCommand

To connect a system to TrueCommand, open the **Configure settings** menu and click **Systems**. The **Systems** menu has two tabs: **Systems** and **System Groups**. The **Systems** and **System Groups** tabs contain all the options to connect and organize systems in TrueCommand. The **Systems** tab lists all added systems and their current connection statuses.



The screenshot shows the 'Systems' tab in the TrueCommand interface. At the top right, there are buttons for '+ NEW SYSTEM' and '+ NEW GROUP'. Below the tabs, there is a 'Filter' input field. The main table lists systems with the following columns: NICKNAME, HOSTNAME, CONNECTION, LAST SYNC, and UPDATES. The systems listed are:

NICKNAME	HOSTNAME	CONNECTION	LAST SYNC	UPDATES
fn_miniv2.0	truenas.local	Connected		
gm1 	truenas.local	Connected		Available
gm4	Gremlin4.local	Connected		Available
 ec01_cluster		 OFFLINE		
tn02_ha 	tn02a.qe.ixsystems.net	Connected		Available
tn03 	tn03a.qe.ixsystems.net	Connected		Available
 tn36		 OFFLINE		

Adding a System Manually

To connect a new system, click **+ NEW SYSTEM**.

Enter the system IP address or DNS hostname, the nickname, and the password. If you make a mistake, you can reset the form by clicking **RESET**.

New System

General Settings

IP Address or Hostname

Nickname

Password / API Key

Password / API Key Confirm


RESET

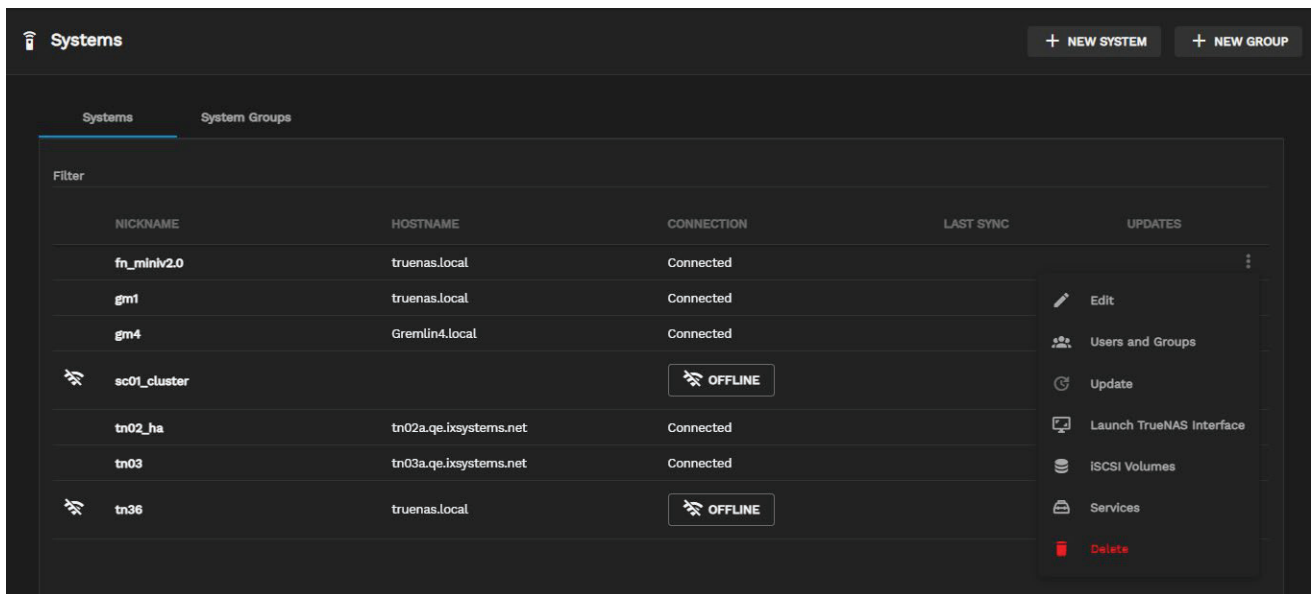
ADD AND CONTINUE

ADD SYSTEM

If the system has alerts or alarms, a blue circle with the number of current alerts displays to the right of the system name.

Adjusting Systems



Each TrueNAS system listed on the **Systems** screen has an options menu that allows you to edit, delete or modify configuration settings for that system. Click the  for the system to display the options menu.



- **Edit:** edit
- **Users and Groups:**
- **Update :** update
- **Launch TrueNAS Interface:**
- **iSCSI Volumes:**
- **Services:**
- **Delete:** delete


🕒 Edit

Clicking the edit button **edit** opens a panel on the right of the screen that displays the system setting fields you can edit. After making your changes, click **Save Changes** to update the system with the new values entered. Click **Reset** to clear the form and reset values to the previously saved settings for the NAS.


 **Edit gm4** 

General Settings


IP Address or Hostname

10.234.27.217 


Nickname

gm4 



Password / API Key



Password / API Key Confirm



Alert Options

Ignore  

RESET

SAVE CHANGES

Users and Groups

Click the **Users and Groups** button to display the list of users or groups for the selected system.

FN_MINIV2.0

>

USERS

+ USER

Filter				REMOVE
<input type="checkbox"/>	UID	USERNAME	SMB	ACTIONS
> <input type="checkbox"/>	1000	jmaloney	true	
> <input type="checkbox"/>	1001	tony	true	
> <input type="checkbox"/>	1003	bonnie	true	
> <input type="checkbox"/>	1004	smbclient1	true	
> <input type="checkbox"/>	1005	ixuser	true	
> <input type="checkbox"/>	1006	user1	true	
> <input type="checkbox"/>	1007	user2	true	
> <input type="checkbox"/>	1008	User3	true	
> <input type="checkbox"/>	1010	User4	true	

○ Update

If the system has **Available** in the **Updates** column, it has system updates ready to apply. Click the **Update** button **update** on the option menu to open a dialog window with information on the update. Check the **Confirm** box, then click **OK** to update the system. Click **Cancel** to close the window without updating.

Update NAS

System **gm4** will be updated. The system will restart after the update is complete.

Current version:
TrueNAS-12.0-U6

New version:
TrueNAS-12.0-U7

☐ Confirm

CANCEL

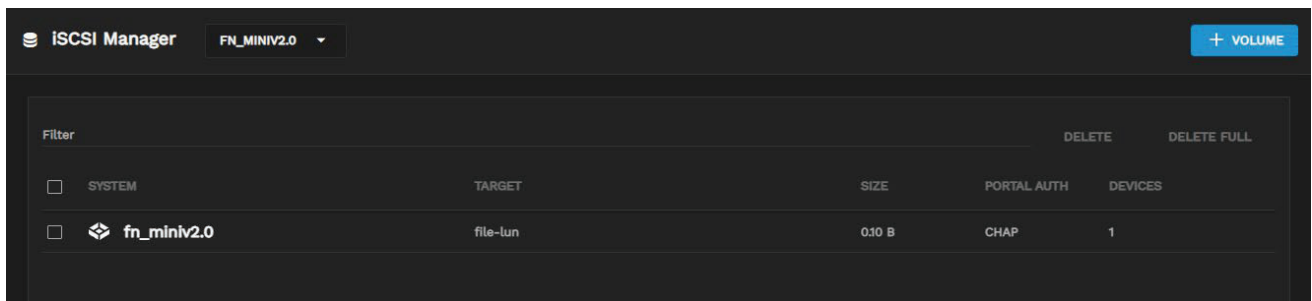
OK

○ Launch TrueNAS Interface

Use the **Launch TrueNAS Interface** button to open a new browser tab with the TrueNAS dashboard for the system selected on the **System** screen.

○ iSCSI Volumes

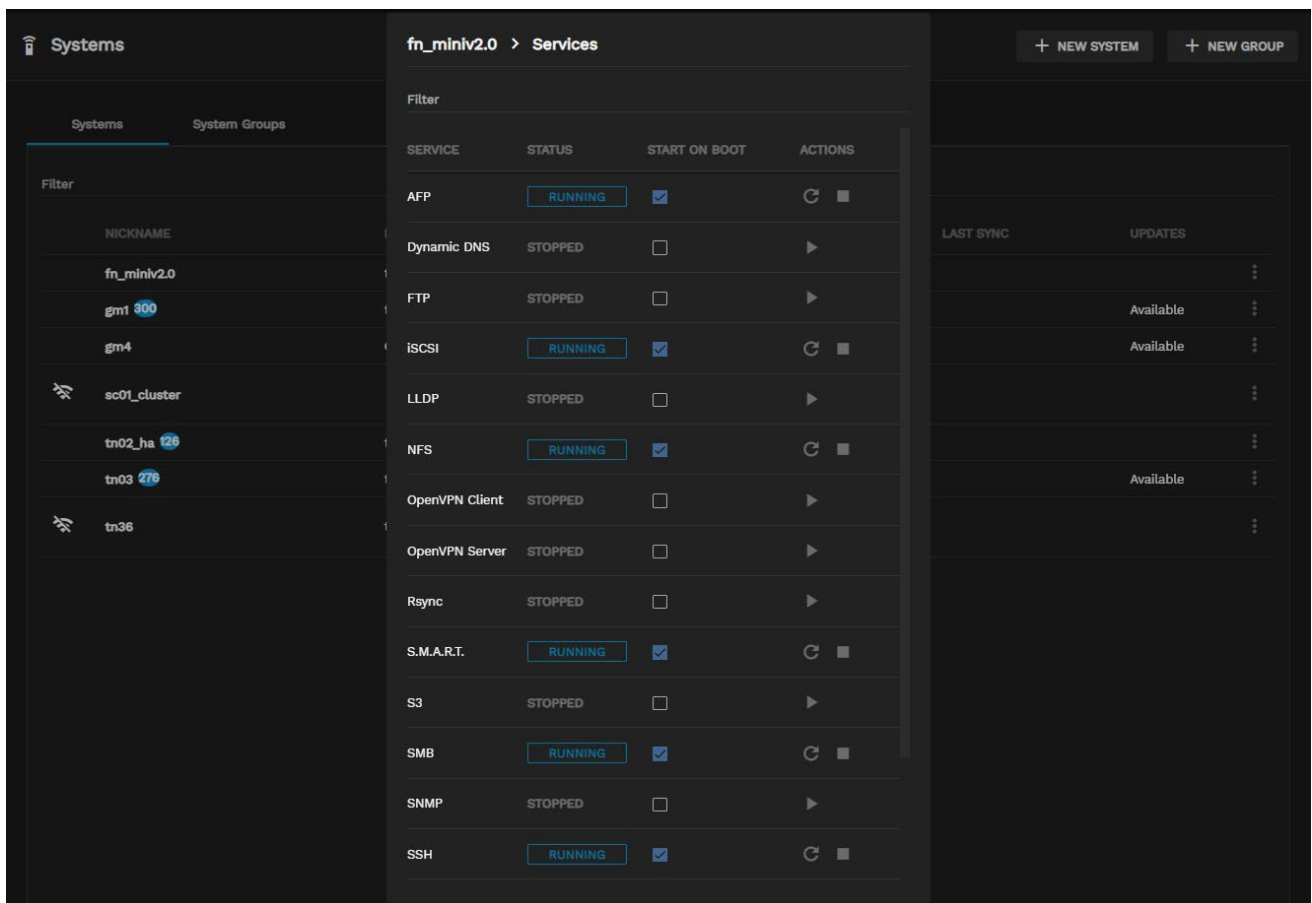
If a system is configured with iSCSI volumes, click the **iSCSI Volumes** button to display the iSCSI volumes page for the selected server.



○ Services

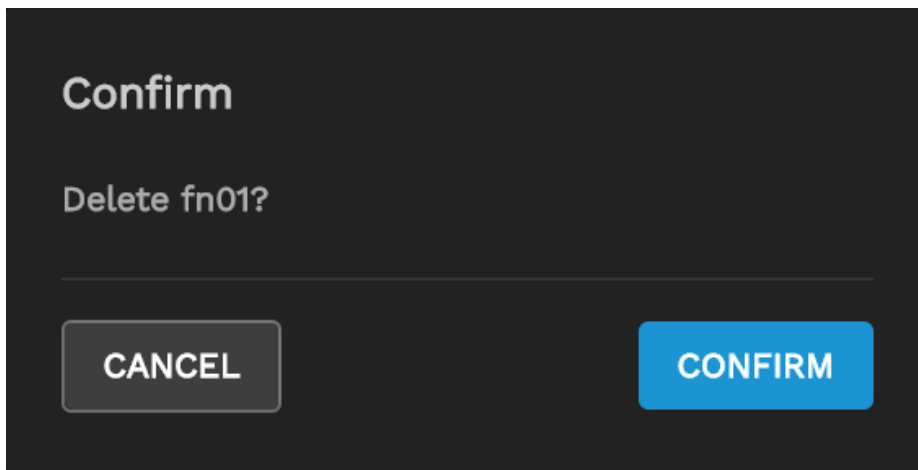
Click the **Services** button to display the **Services** window with a list of services running or stopped for the selected system.

The options for services are adding it to start on boot-up, stopping, or starting/restarting. Click the **START ON BOOT** checkbox to add the selection to the services started at boot-up. Click the stop icon to stop a running service. Click the start/restart icon to start a stopped service.



○ Delete

Clicking the **delete** button displays a popup window to confirm you want to delete a selected system.

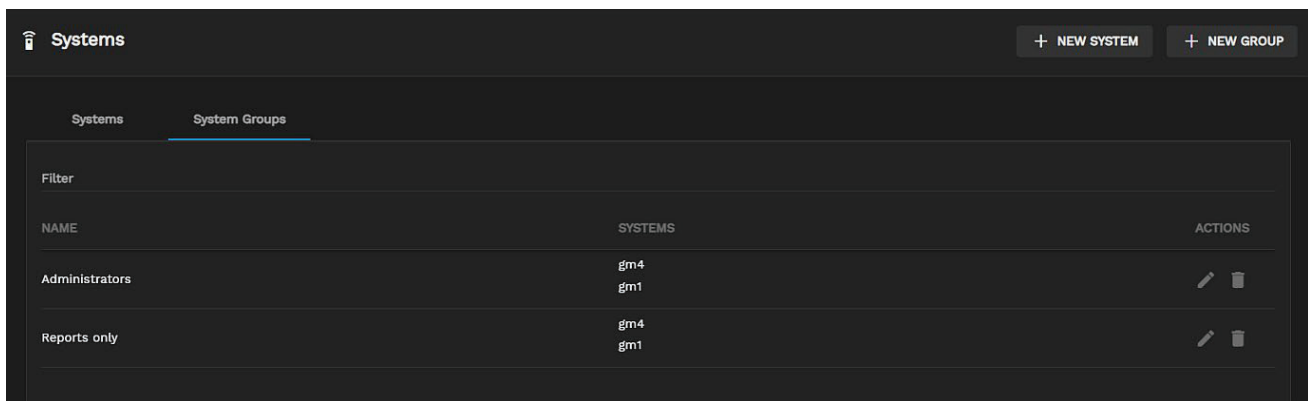


Deleting a system purges all collected data from the database.

Organizing Systems into Groups

TrueCommand administrators can organize systems into collections called Groups. Grouping systems lets you efficiently manage system permissions and reporting.

Open the **System Groups** tab to view the list of created groups and the systems they contain.



Create a group by clicking **Configure settings > Systems > + NEW GROUP**. Type a name for the new group and click **ADD SYSTEM** to add a system to the group. After adding all the desired systems to the group, click **CREATE GROUP**.

New Group

General Settings

Group Name

Systems

!

No systems selected.

ADD SYSTEM

SAVE GROUP



Managing Groups

Each group has two management options:

- Edit System : **edit**
- Delete System : **delete**

⦿ Edit

Clicking the edit button **edit** opens a side bar menu. You can make adjustments to the Group in this manner. Add or remove systems from the group by using the **Add System** button or the remove **delete** button. Click **Save Changes** when finished with your changes to update the group to the new group settings.



 **Edit undefined** 

General Settings

Group Name

Docs Group

Systems

Name	
megamini	
realmini	

ADD SYSTEM

SAVE GROUP

☐ Delete

Clicking the delete button displays a popup confirmation box to delete a group.

Confirm

Delete Docs Group?

CANCEL

CONFIRM

5.2 - Users

- - [Adding Local User Accounts](#)
 - [Configuring User Accounts](#)
 - [User Details](#)
 - [Joined Teams](#)
 - [System Access](#)
 - [Resetting a User Password at Login](#)
 - [Resetting a User Password from the Command Line](#)
 - [Deleting User Accounts](#)
 - [Organizing Users into Teams](#)
 - [Configuring Teams](#)
 - [Deleting Teams](#)



TrueCommand has a robust user management system that lets administrators personalize the experience for each user account. You can create user accounts in the TrueCommand interface. Alternatively, LDAP can automatically create new user accounts when someone logs into TrueCommand with their LDAP credentials.

You can also manage many user accounts simultaneously by organizing them into Teams.

Adding Local User Accounts

To create a new user account, open the **Configure settings** menu and click **Users > + NEW USER**. Assign them a descriptive name and authentication method.

TrueCommand uses the default authentication method to create unique credentials for logging in to the web interface. The administrator must provide the user with their login credentials.


 **New User** 

User Details

☐ TrueCommand® Administrator

Username

Full name

Teams 

Auth method

Password

Password Confirm

CANCEL

CREATE USER


You can assign users to existing teams. After creating the team, you can add the user in the **New User** configuration panel by selecting **Teams** on the drop-down menu. You can assign users to multiple teams.


If the user needs to be an administrator, check the **TrueCommand Administrator** box.













When finished, click **Create User**.

Configuring User Accounts

To configure account details and permissions, open the **Configure settings** menu and click **Users**.

 **Users**



Filter				
	USERNAME	STATUS	ADMIN	ACTIONS
	erika	inactive		 
	Joey	inactive		  
	mic1	active		 

To edit a user click the edit icon .

There are several different user elements that you can configure, including their avatar, personal details, contact email address, team membership, and system permissions.

User Details

Users or admins can add personal details about the user on this page.

To go back to the original contents of the fields, click **RESET FORM** before you click **SAVE CHANGES**.

☒ Administrator

You can select the **TrueCommand Administrator** checkbox to designate the account as an administrator.

☐ Change Password

You can change the account password by typing the new password into both the **Password** and **Password Confirm** fields. When prompted, enter the user existing password. Click **SAVE CHANGES** to make the change.

☐ Email

You can set up or change user email on this screen. If [SMTP](#) is not set up, an error message displays at the bottom of the screen stating **Failed to send email. Are your SMTP settings configured?**. Admins can click the **CONFIGURE** button to open the SMTP settings window. Before adding a user email, go to **Alert Services** and verify you have set up the SMTP service.

☐ Two Factor Authentication

You can set user [Two Factor Authentication](#), which requires they enter a validation code emailed to them after they enter their username, password, and click **SIGN IN** on the login screen.

Joined Teams

The **CREATE A NEW TEAM** button displays if a TrueCommand team does not exist. When teams exist, the **JOIN TEAM** button displays instead.

Click **JOIN TEAM** to display the list of existing teams, then select a team to add the user to it. You can add users to multiple teams. TrueCommand applies team permissions to any user added to a team, but setting

specific permissions for users can override related team permissions. Use the **Teams** screen to create new teams or edit existing ones.

System Access

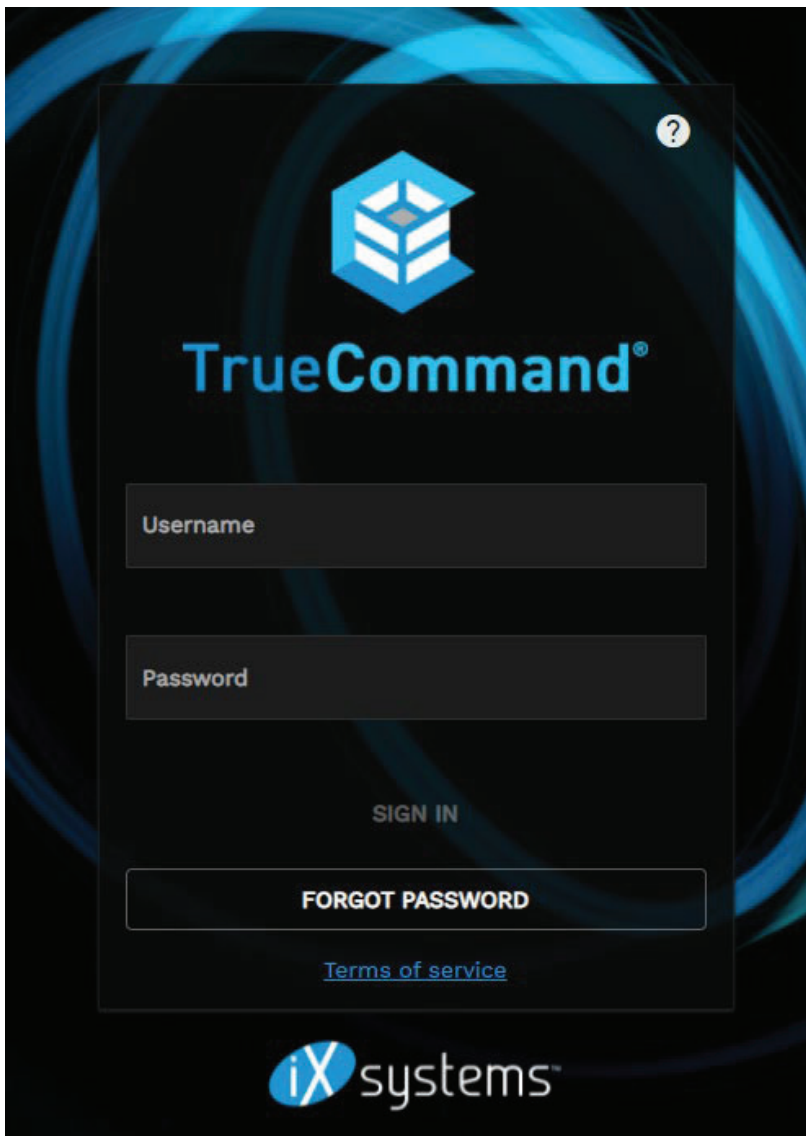
To limit non-administrative account access to connected systems, configure the **System Access** and **System Groups** sections. You must first configure [system connections](#) and/or [system groups](#) in TrueCommand. Add systems from either the **Dashboard** or **Systems** screens.

Click **ADD SYSTEM** and select a system from the drop-down to give the user access to that system. To restrict them to viewing system details, select the **read** permission. To remove their access to a particular system, click - minus on that system.

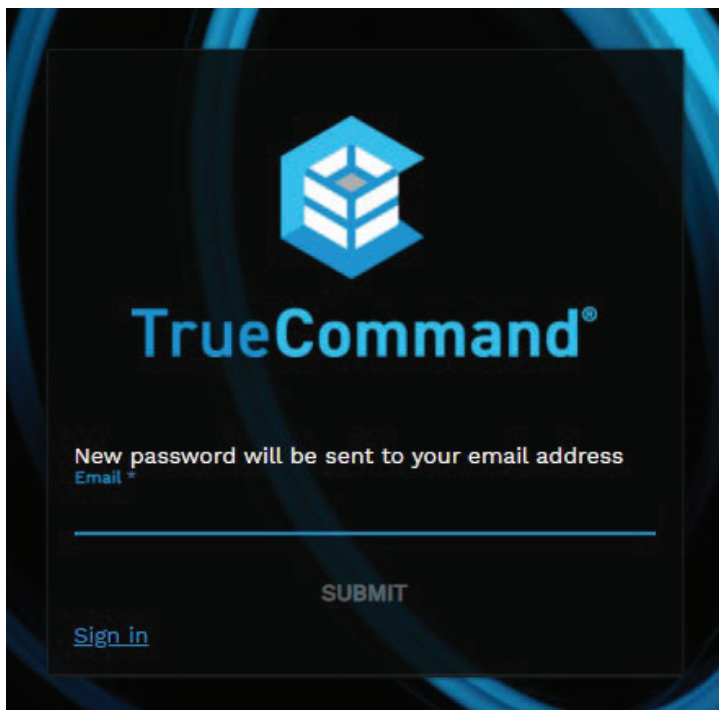
When TrueCommand has system groups, the **ADD GROUP** button displays. Click **ADD GROUP** and select a group from the drop-down to give the user access to all the systems in that group. To choose the user group permissions, select **read** or **read/write**. To remove their access to a particular system group, click - (minus) on that group.

Resetting a User Password at Login

TrueCommand users can reset their passwords from the login screen. After typing their username click the **FORGOT PASSWORD** button.



Enter the user email address (or where you want to send the reset login code).



An **[AUTH] TrueCommand Password Reset** email should arrive with the reset password login code. After receiving the code, enter the user name in the login screen and the reset password code and click **SIGN IN**. The user can then go to their profile to change their password.


A screenshot of the TrueCommand user profile page for a user named 'tazzie'. The page has a dark theme. At the top, there's a breadcrumb trail: "Users > tazzie". The main content is divided into two columns. The left column contains: an "Avatar" section with a purple and white geometric profile picture; a "User Details" section with fields for Username (tazzie), Full Name (tazlina may spryworth), Title, and Email (erikaj.test.acct@gmail.com); a "Phone" field and an "Enable 2FA" checkbox; and an "Auth method" section with "Password" and "Password Confirm" fields. The right column contains three sections: "Joined Teams" with a message "There are no teams." and a "CREATE A NEW TEAM" button; "System Access" with a message "There are no systems." and a "MANAGE SYSTEMS" button; and "System Groups" with a message "There are no groups.".

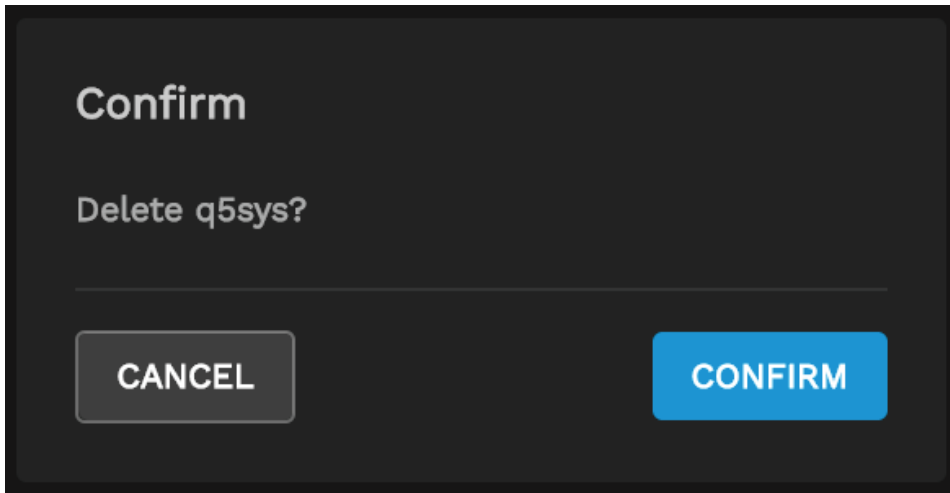
Resetting a User Password from the Command Line

The Docker version of TrueCommand allows you to reset user passwords from the command line. Open the **Shell** on the TrueNAS system running the TrueCommand container and use the following command, replacing the values in brackets with their appropriate values.

```
docker exec -it [docker instance ID] resetpw [username]
```

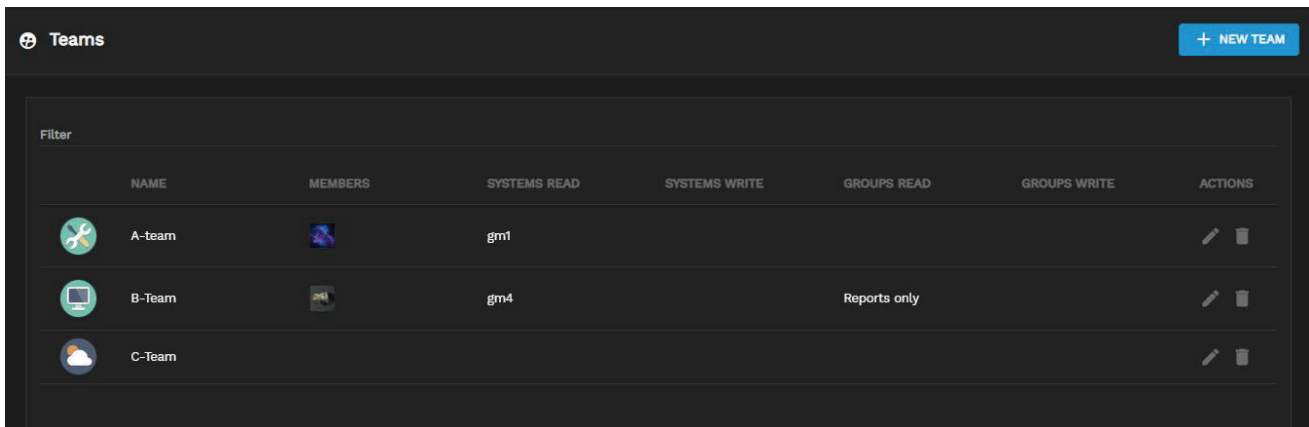
Deleting User Accounts

To delete an account, open the **Configure settings** menu and click **Users**. On the **Users** page, click the delete icon  to the right of the user you want to delete. A popup displays to confirm user deletion.



Organizing Users into Teams

To create a team, open the **Configure settings** menu and click **Teams**.



Clicking **NEW TEAM** displays the **New Team** configuration panel.

+

New Team

×

Team Details

Team name

Avatar

CANCEL

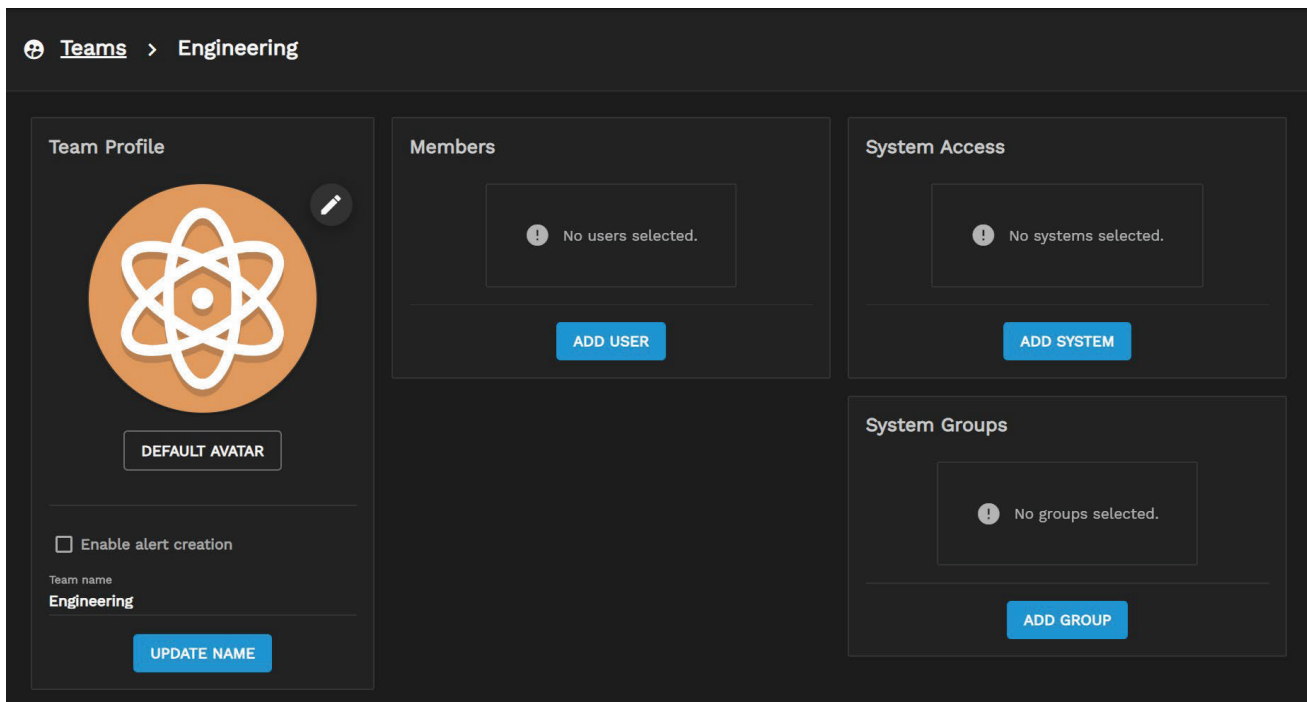
CREATE TEAM

Type a name and select an avatar for the new team. You can edit team permissions and settings after creating it.

Configuring Teams

To configure a team, click on the **Configure settings** icon and then click **Teams**. To change team members or permissions, click on the edit icon **edit** for the team you selected on the list.

<https://www.truenas.com/docs/truecommand/printview/>[8/2/2022 2:08:35 PM]



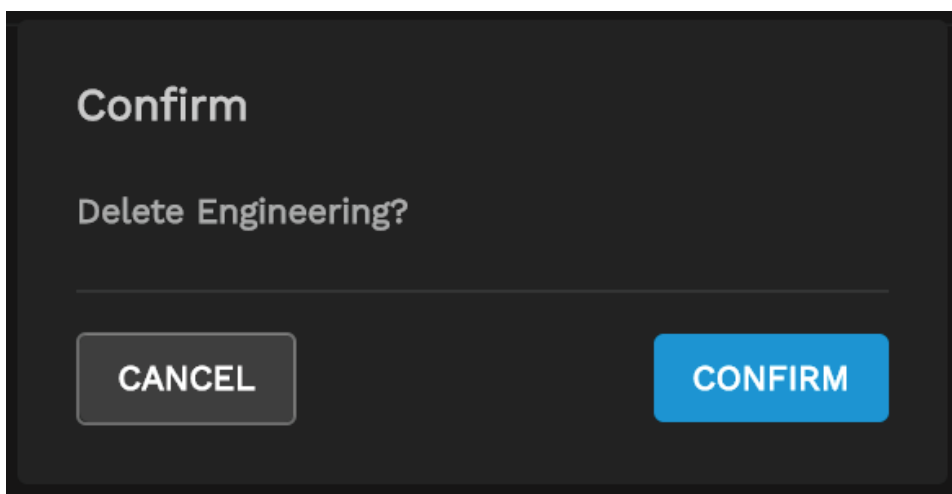
You can change a team profile avatar, name, or grant team members permission to create new TrueCommand alert rules by selecting the **Enable alert creation** checkbox.

The **Members** section shows which accounts are in the team. To add users to the team, click **ADD USER** and select users on the drop-down list. To remove users from the team, click the - (minus) next to the users you want to remove.

You can configure system permissions the same way as individual user system access. Note that individual user account permissions can override team permissions.

Deleting Teams

To delete an account details and permissions, open the **Configure settings** menu and click **Teams**. On the **Users** page, click the delete icon **delete** to the right of the user you want to delete. A popup displays to confirm Team deletion.



Deleting a team does not remove users or systems assigned to that team.

5.3 - Settings

TrueCommand configuration.

The **Administration** page, available to users with administrator permissions, displays additional system details and offers a variety of TrueCommand configuration options. Click the **Configure settings** icon and select **Administration** to access the **Administration** page. It is organized into function tabs **About**, **Certificates**, and **Configuration**.

ⓘ About

The **About** tab contains the current TrueCommand system ID and version, contact information for iXsystems, and license details.

The screenshot shows the TrueCommand Administration page with the 'About' tab selected. The page has a dark theme. At the top, there's a navigation bar with 'Administration' and three tabs: 'About' (selected), 'Certificates', and 'Configuration'. Below the tabs, the 'System Info' section displays the iXsystems logo, the text 'TrueCommand® is built and maintained by', the System ID '210225-5P27Zm-YKWjxt-ln2xsf-183653', the Master System Version 'Master-20210225', and the Master Middleware Version '20210225'. The 'Contact' section lists the Support Phone '1-408-943-4100', Sales Phone '1-408-943-4100', Support Email 'support@ixsystems.com', and Sales Email 'truecommand-sales@ixsystems.com'. It also includes links for 'Support website' and 'Sales website'. The 'License' section shows the Default License 'IX Internal', License ID '1', Used systems '0', Used disks '0', and Max Disks '50'. There is a 'GET A LICENSE' button. The 'Upload License' section has a 'Choose File' button and a 'No file chosen' status, with an 'UPLOAD LICENSE' button below.

System Info				
TrueCommand® is built and maintained by	210225-5P27Zm-YKWjxt-ln2xsf-183653	Master System Version	Master-20210225 Middleware Version	

Contact				
1-408-943-4100	1-408-943-4100	support@ixsystems.com	truecommand-sales@ixsystems.com	
Support Phone	Sales Phone	Support Email	Sales Email	
Support website		Sales website		

License				
Default License	IX Internal	1	0	50
License Name	License ID	Used systems	Used disks	Max Disks

[GET A LICENSE](#)

Upload License

[Choose File](#) No file chosen

[UPLOAD LICENSE](#)

Updating the License

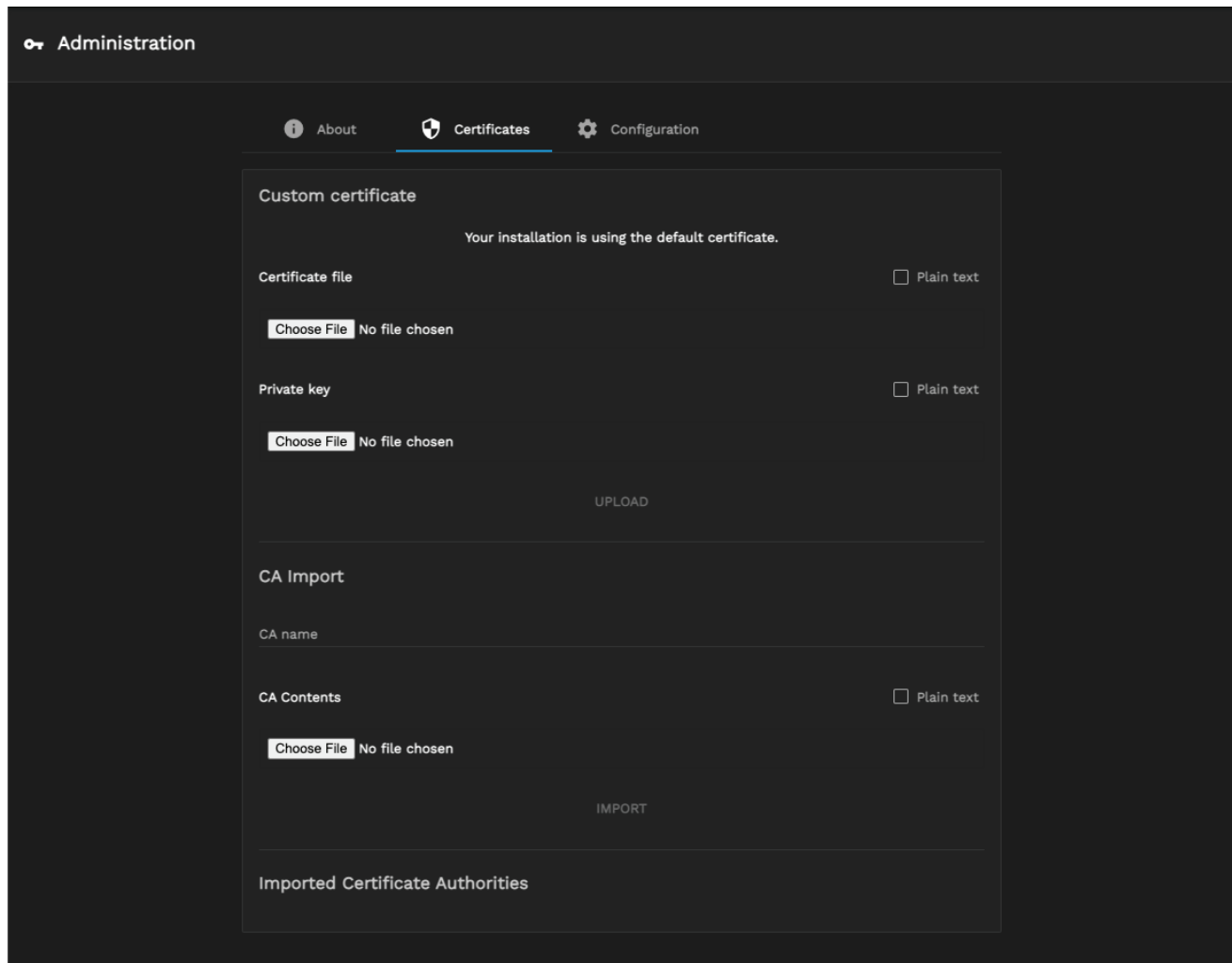
You can expand TrueCommand to monitor more disks by upgrading or purchasing a license from iXsystems. Click **GET A LICENSE** to open a new browser tab to purchase a TrueCommand license. You can also contact iXsystems to upgrade the current license.

After you upgrade or purchase a new license, you must upload it to TrueCommand. Click **Browse...** to open a file browser on your local system. Select the new license file to upload and click **UPLOAD LICENSE** to apply the new license to TrueCommand.

○ Certificates

The **Certificates** tab shows the certificates and Certificate Authorities (CAs) TrueCommand uses and has

options to upload or import a certificate or CA.



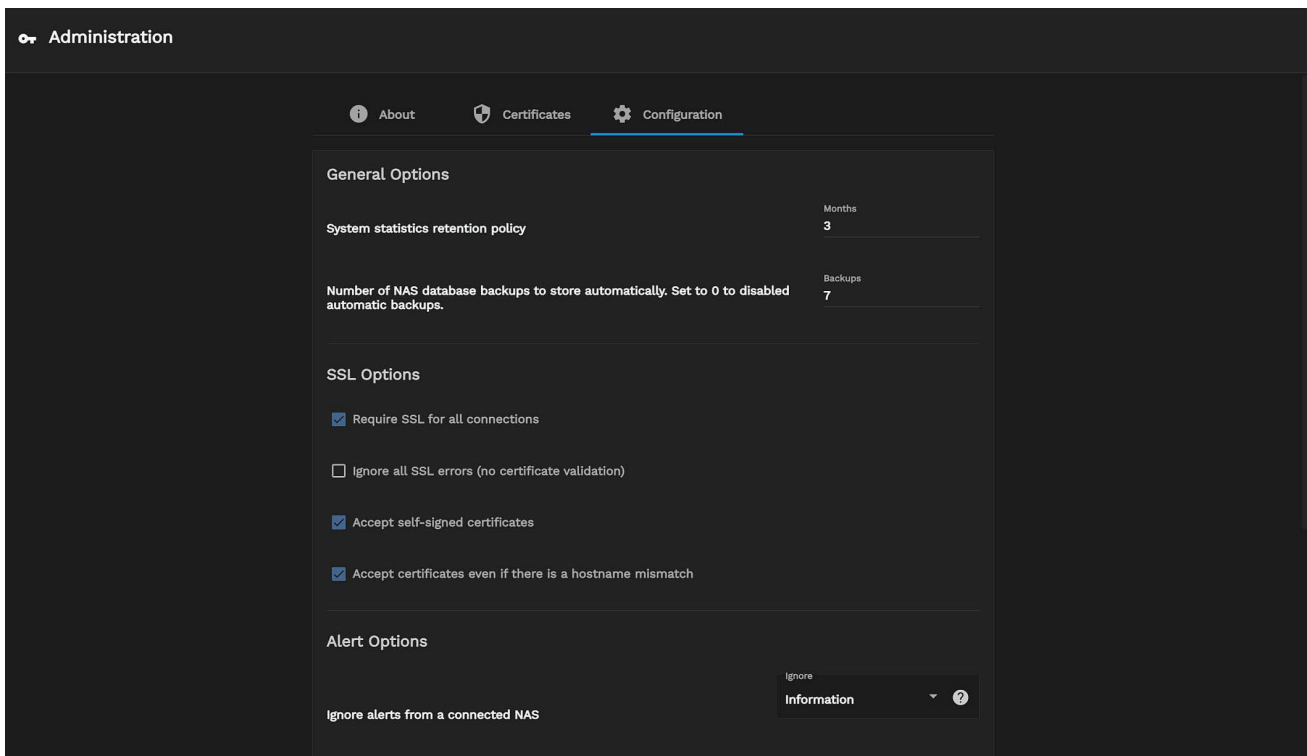
The screenshot shows the 'Administration' section of the TrueCommand interface. The 'Certificates' tab is selected, displaying two main sections: 'Custom certificate' and 'CA Import'. The 'Custom certificate' section includes a message 'Your installation is using the default certificate.', a 'Certificate file' field with a 'Choose File' button and 'No file chosen' text, a 'Private key' field with a 'Choose File' button and 'No file chosen' text, and a 'Plain text' checkbox. An 'UPLOAD' button is located below these fields. The 'CA Import' section includes a 'CA name' text input field, a 'CA Contents' field with a 'Choose File' button and 'No file chosen' text, and a 'Plain text' checkbox. An 'IMPORT' button is located below these fields. At the bottom, there is a section titled 'Imported Certificate Authorities'.

Clicking **Browse...** opens a dialog to upload a file from the local system. Selecting **Plain text** allows you to copy and paste the raw text instead of uploading a file.

○ Configuration

The **Configuration** tab contains options to configure various features of TrueCommand. The configuration options accessible are:

- General Options
- SSL Options
- Alert Options
- LDAP
- SAML
- Telemetry



Scroll down to reveal all options on the **Configuration** tab.

After changing any options, click ***SAVE** at the bottom of the tab to save the new system configuration. To reset fields back to their previous values, click **CANCEL**.

General options include how long TrueCommand stores system statistics and the number of database backups from an iXsystems NAS to store.

SSL options

This feature is only available for local installations or containerized TrueCommand deployments.

By default, TrueCommand attempts an SSL connection, then a non-SSL connection if the first attempt fails. You can disable non-SSL connection attempts by setting **Require SSL for all connections**, which is useful when a monitored system uses a custom port or does not allow SSL-secured access.

There are additional options to configure how TrueCommand handles certificates. By default, TrueCommand accepts self-signed certificates and certificate hostname mismatches. Self-signed certificates enable the first-time login to TrueCommand. Certificate hostname mismatches let TrueCommand accept certificates from systems that use a hostname, even though it registered them with an IP address (or vice-versa).

SSL Options

- ☐ Require SSL for all connections
- ☐ Ignore all SSL errors (no certificate validation)
- ☒ Accept self-signed certificates
- ☒ Accept certificates even if there is a hostname mismatch

Alert Options

You can adjust the alert levels that TrueCommand shows from a connected NAS to tune the system messages displayed according to your use case. Choose an alert category to ignore. You can select multiple categories.

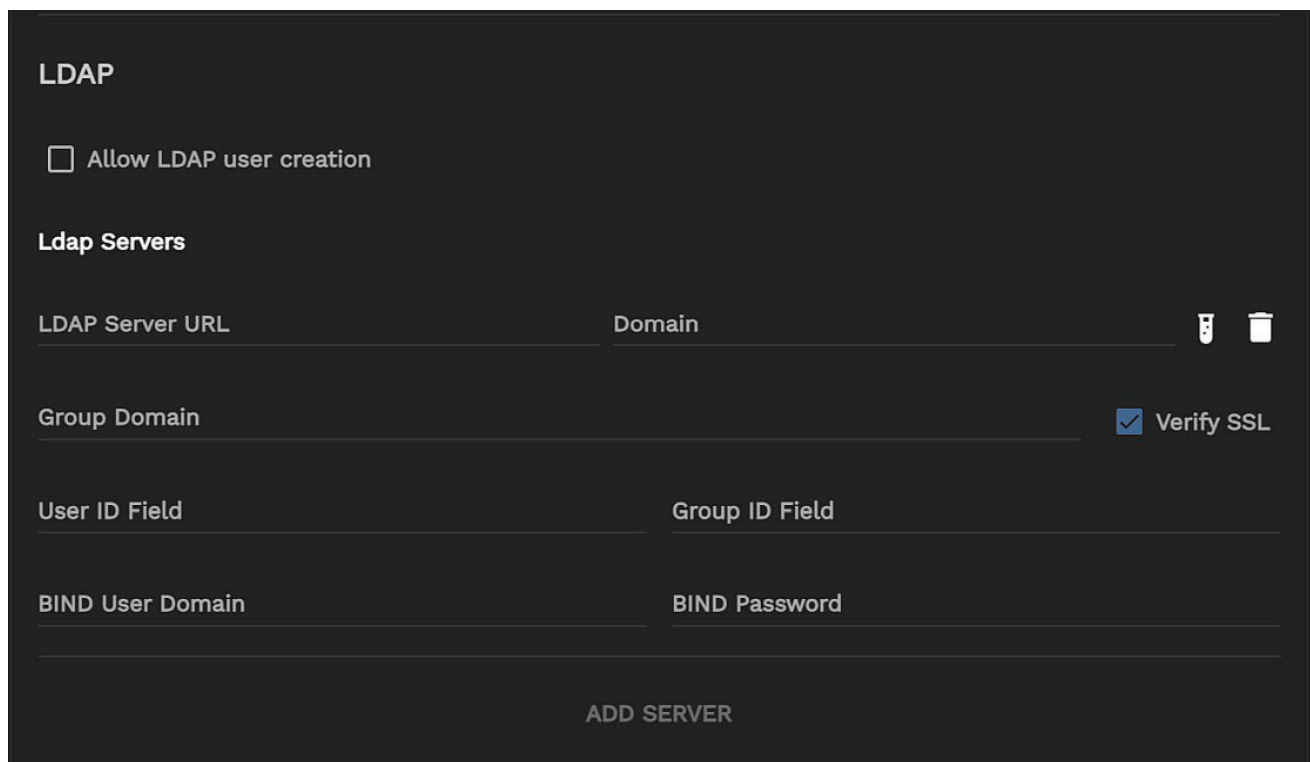
LDAP

TrueCommand supports using [LDAP](#) to better integrate within an established network environment. *LDAP/AD* allows using single sign-on credentials from the [Lightweight Directory Access Protocol \(LDAP\)](#) or [Active Directory \(AD\)](#). Users can log in with an LDAP or AD account without creating a separate TrueCommand login.

LDAP and AD require the server IP address or DNS hostname and domain to use. The LDAP or AD Username (optional) is required when the TrueCommand user name does not match the LDAP or AD credentials.

Click on the **settings (Gear) > Administration**.

Click on the **Configuration** tab and scroll down to access the LDAP configuration section. Click **ADD SERVER** to begin configuring LDAP in TrueCommand. The screen changes to display the LDAP configuration settings fields.

The image shows a dark-themed web interface for LDAP configuration. At the top, the title 'LDAP' is displayed. Below it is a checkbox labeled 'Allow LDAP user creation'. A section header 'Ldap Servers' is followed by a table with two columns: 'LDAP Server URL' and 'Domain'. To the right of the 'Domain' column are two icons: a test icon (a person with a checkmark) and a delete icon (a trash can). Below the table, there is a 'Group Domain' field and a 'Verify SSL' checkbox which is checked. Further down are fields for 'User ID Field' and 'Group ID Field'. At the bottom are fields for 'BIND User Domain' and 'BIND Password'. A large 'ADD SERVER' button is centered at the very bottom of the form.

To configure LDAP, type the LDAP server IP address or DNS hostname into the **LDAP Server URL** field, type the domain name in the **Domain** field, and click **ADD SERVER**. You can add multiple LDAP servers and domains.

The **Test LDAP Config** icon opens a window that allows you to test your connection to the LDAP server. The **Remove LDAP Server** icon removes the selected LDAP server.

LDAP

☐ Allow LDAP user creation

Ldap Servers

LDAP Server URL

Domain

Group Domain

☒ Verify SSL

User ID Field

Group ID Field

BIND User Domain

BIND Password

ADD SERVER

LDAP Teams

!

There are no teams.

CREATE A NEW TEAM

Field	Value
LDAP Server URL (string, required)	IP or DNS name of the LDAP server, with port number on the end. Example: <i>ldap.mycorp.com:636</i> (SSL port is typically 636 for AD/LDAP)
Domain (string, required)	Base domain settings of the user. Example: <i>dc=mycorp,dc=com</i> for a typical username@mycorp.com user account
Group Domain (string)	The alternative domain setting to use when searching for groups. The default value is the same as Domain
Verify SSL (bool)	Require strict SSL certificate verification. The default value is false. Disable this option if the hostname of the system is different than the one listed on the SSL certificate, an IP is used for the connection instead of the DNS hostname, or if a self-signed certificate is used by the LDAP server.
User ID Field (string)	Domain fieldname to use for user-matching. The default value is uid (user ID). Another field commonly-used is cn (common name)
Group ID Field (string)	The domain fieldname to use when searching for a group name. The default value is cn (common name).
BIND User Domain (string)	The full domain setting for a pre-authenticated bind to the server. Example: <i>uid=binduser,cn=read-only-bind,dc=mycorp,dc=com</i> For an unauthenticated bind set this field to just a name (example: <i>truecommand-bin</i>). This is sometimes used for logging purposes on the LDAP, but otherwise is not validated.

BIND Password (string)	The password to use for the bind user. For an unauthenticated bind, leave this field blank while setting the BIND User Domain to a non-empty value.
------------------------	---

LDAP connection options

TrueCommand supports two common methods of validating LDAP user credentials:

Direct Bind

The direct BIND method uses the **Domain** and **User ID Field** values to create a static domain string for user authentication.

Example:

- Domain: *dc=mycorp,dc=com*
- User ID Field: *uid*

When *bobby.singer* attempts to log in, TrueCommand establishes an SSL-secure connection to the LDAP server and then attempts to bind with the static domain *uid=bobby.singer,dc=mycorp,dc=com* and the user-provided password. If successful, the user authentication is verified, and Bobby Singer may access TrueCommand.

Indirect Bind

The indirect BIND authentication method is more dynamic and searches for the proper user domain settings rather than making format assumptions. With TrueCommand, indirect BIND configures a *bind user* (typically a read-only, minimal-permissions user account) with a known domain/password to perform the initial bind to the LDAP server. Once logged in, TrueCommand searches for the user domain currently requesting to login. It then attempts a second bind with the user domain and provided password.

Example:

- Domain: *dc=mycorp,dc=com*
- User ID Field: *uid*
- BIND User Domain: *uid=binduser,cn=read-only-bind,dc=mycorp,dc=com*
- BIND Password: *pre-shared-key*

When *bobby.singer* attempts to log in, TrueCommand establishes an SSL-secure connection to the LDAP server. TrueCommand uses the **BIND User Domain** and **BIND Password** settings to perform an initial bind using pre-known settings from your LDAP provider. Once bound, TrueCommand searches for the user matching *uid=bobby.singer*, but only within the subdomains that include the domain setting (*dc=mycorp,dc=com* in this example). If TrueCommand finds a user, it uses the entire user domain string from the search result to initialize a second bind along with the user-provided password. If successful, TrueCommand verifies the user authentication, and Bobby Singer is allowed access to TrueCommand.

SSL/TLS Connection Info

WARNING: AD/LDAP authentication *requires* SSL connections.

If the LDAP server uses an SSL certificate generated by a custom certificate authority (CA), then one of two things must occur before TrueCommand can use the LDAP server:

- (Option 1) Users must register the custom certificate authority with TrueCommand via the **Certificates** tab on the **Administration** screen.
- (Option 2) Users can disable the **Verify SSL** option to accept whatever SSL certificate the server provides. Users might need to choose Option 2 if the LDAP server hostname differs from the one listed on the certificate or if the server uses a self-signed SSL certificate.

Selecting **Allow LDAP user creation** means TrueCommand creates user accounts when someone logs in to the User Interface with their LDAP credentials. **JOIN TEAM** automatically adds LDAP users to specific TrueCommand teams.

Telemetry

TrueCommand reports some (completely anonymous) basic usage telemetry back to iXsystems for product improvement analysis.

Click the **PREVIEW** button to see what your system is sending.

You can disable telemetry by checking the **Disable Telemetry** box and clicking **SAVE**.

5.3.1 - Configuring TrueCommand SAML

- - [Activating TrueCommand SAML Service](#)

Security Assertion Markup Language (SAML) is a single sign-on (SSO) standard for logging users into applications that require authentication credentials (like GitHub, G-Mail, etc.). Single Sign-on (SSO) works by transferring a user's known identity to another location that provides services to the user. SAML accomplishes the transfer by exchanging digitally-signed XML documents.

A SAML configuration requires an Identity Provider (IdP) and Service Provider (SP). Active Directory is an example of an IdP.

Activating TrueCommand SAML Service

☉ Active Directory

Log in to your TrueCommand system (i.e., server, container, VM). Go to **Config > Administration**, then click on the **Configuration** tab.

Enter `http://ds.yourcompany.net/FederationMetadata/2007-06/FederationMetadata.xml` in the **SAML Identity Provider URL** field, then click **Save**. The URL is from Active Directory.

Click the **Start the SAML service** checkbox, then click **Save** to start the service.

Log out of TrueCommand.

Configuring Active Directory FS for SAML

To configure AD as the IdP, you must create and modify a Relying Party Trust. After accessing the server hosting AD, you must:

- Create an AD FS Relying Party Trust.
- Download and modify your TrueCommand system certificate. Each TrueCommand has a unique certificate you must use for the configuration to work.
- Configure the TrueCommand URL in Active Directory as a trusted URL
- Configure the identifiers.
- Modify the Relying Party Trust properties to add and edit endpoints.
- Configure the Claim Issuance Policy to add the incoming and outgoing claim types.

The example below describes each top-level step in detail.

Setting Up TrueCommand and AD SAML Service

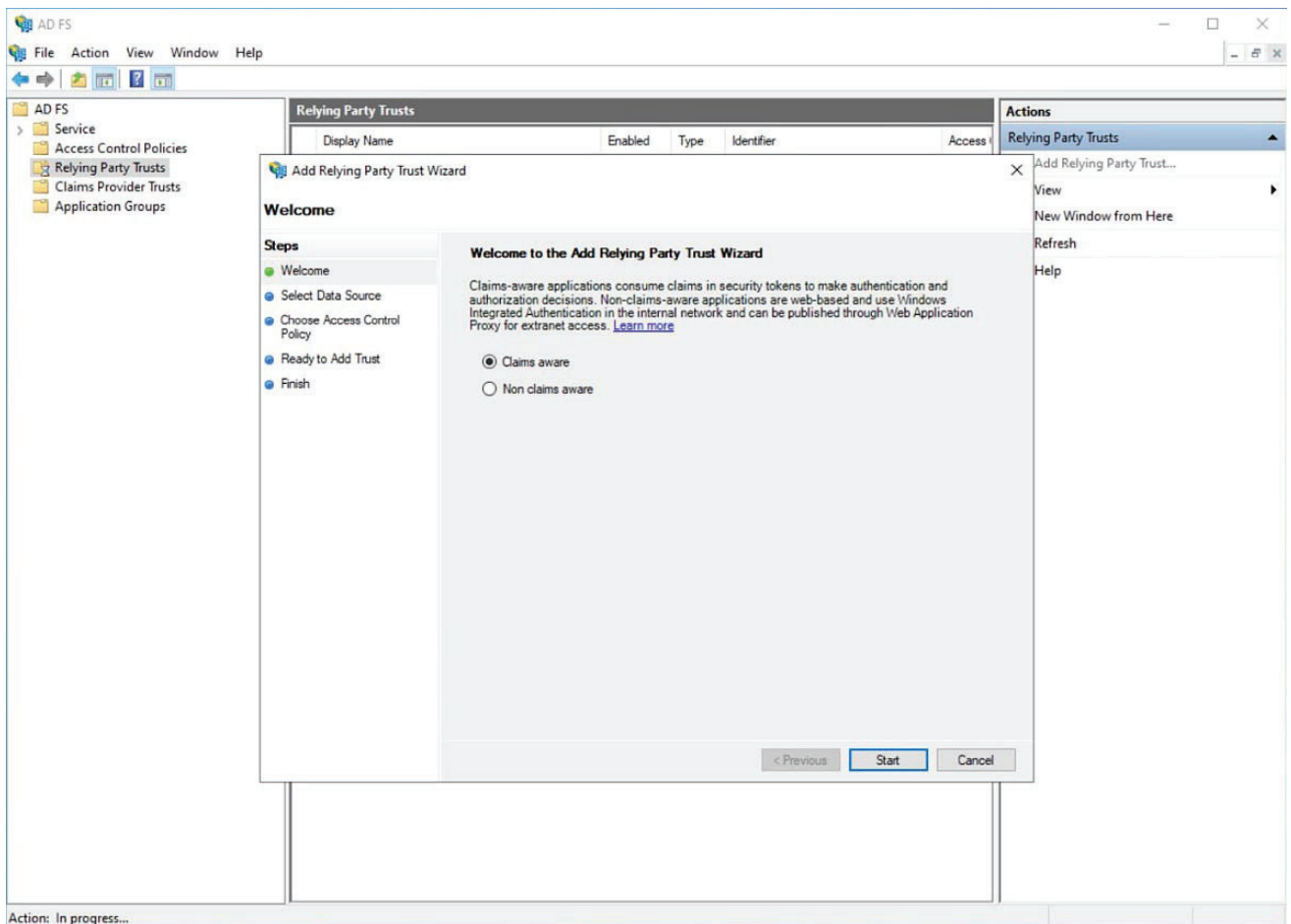
This procedure assumes the Windows administrator user is QE. Substitute your system addresses (URLs, IP address, port number, names, etc.) where variables are present.

1. Access the TrueCommand web interface via `http://IP:PORT` where `IP:PORT` is the IP address and port number assigned to your TrueCommand system.
2. Go to **Config > Administration** and select the **Configuration** tab.
 - a. Enter `http://ds.yourcompany.net/FederationMetadata/2007-06/FederationMetadata.xml` in the **SAML Identity Provider URL** field, then click **Save**. The URL is from Active Directory.
 - b. Click the **Start the SAML service** checkbox, then click **Save** to start the service.

3. Log out of TrueCommand

Configure your Active Directory Server (Identity Server for SAML service)

1. Log into your Microsoft AD system as the Windows administrator user (QE is the administrator user in this example procedure).
2. Create an AD FS Relying Party Trust. Go to **Tools** and select **AD FS Management**.
 - a. Go to **Trust Relationships > Relying Party Trusts** and then delete any entries found. Each TrueCommand has a unique certificate. To ensure you have the correct TrueCommand certificate, delete existing certificates and obtain a new one.
 - b. Select **Add Relying Party Trust** on the **AD FS** to open the **Add Relying Party Trust Wizard**. Click **Start**.



- c. Select **Enter data about the relying party manually**, then click **Next**.

Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

☐ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

☐ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

☒ Enter data about the relying party manually

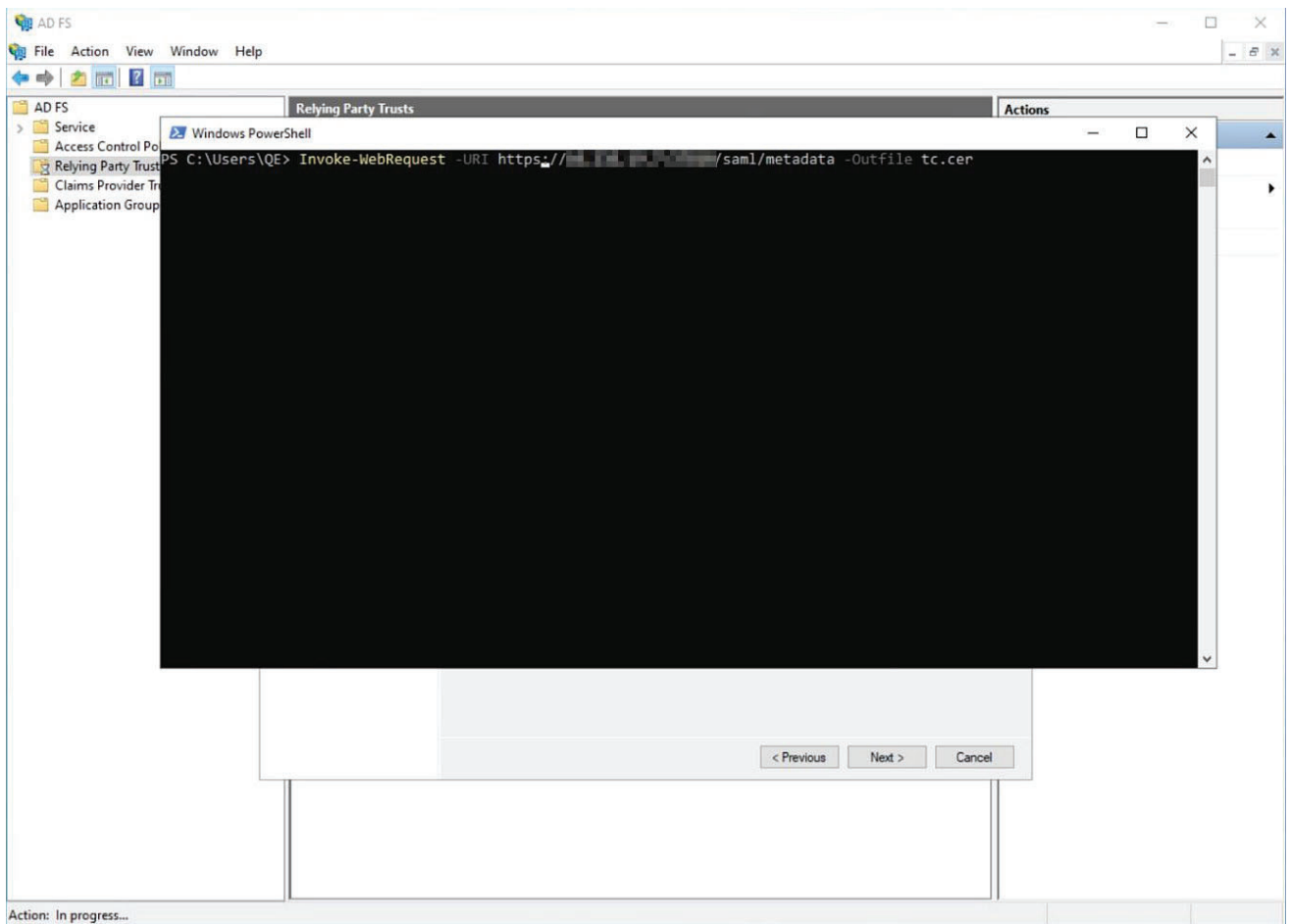
Use this option to manually input the necessary data about this relying party organization.

< Previous Next > Cancel

d. Enter the name for the Relying Party Trust in the **Display Name** field. For this example, we use *QE SAML*. QE is the Windows administrator name, and SAML is the service name.

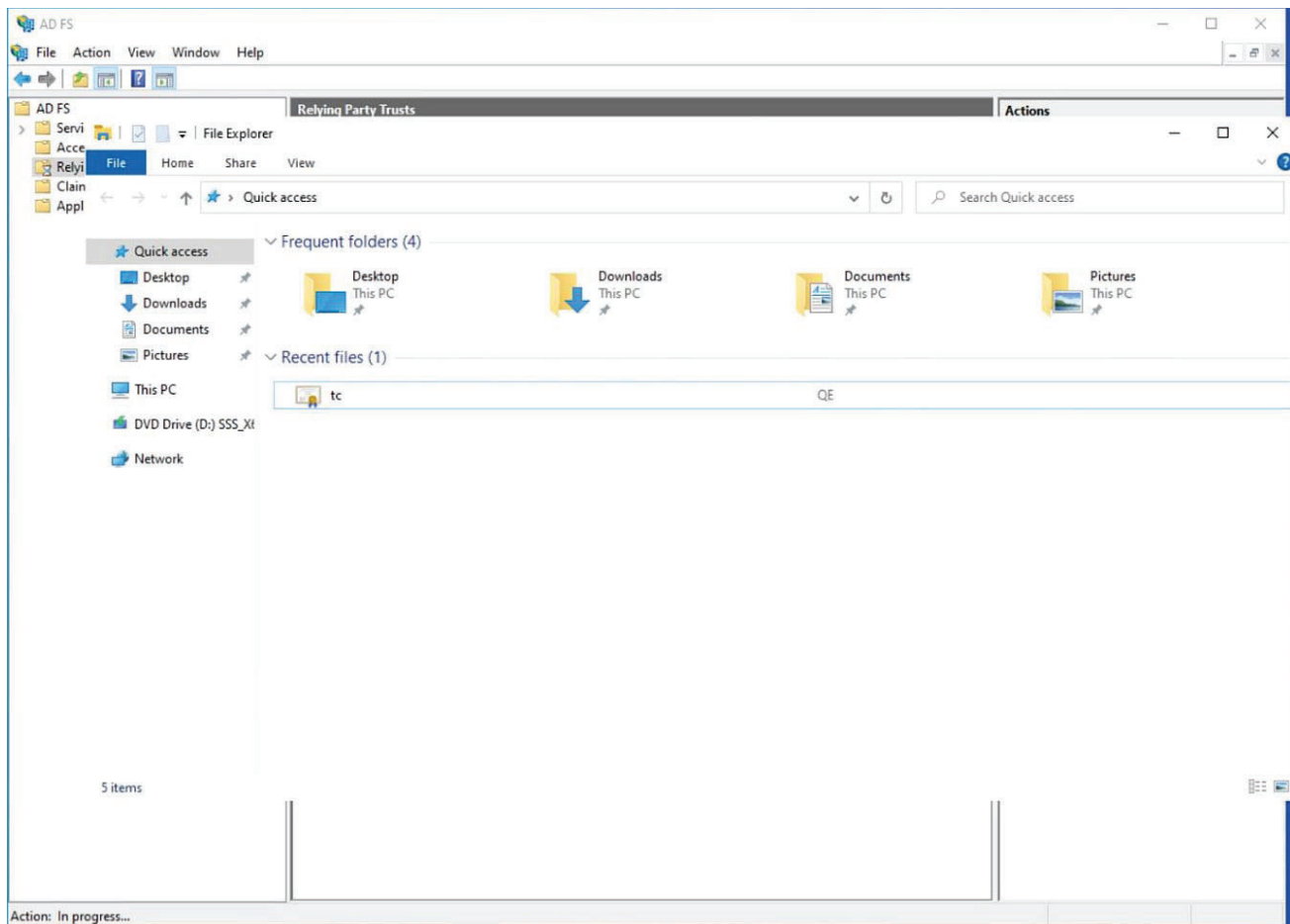
The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Specify Display Name'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name (which is highlighted), Configure Certificate, Configure URL, Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains the instruction 'Enter the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' label followed by a text box containing 'QE SAML'. Below the text box is a 'Notes:' label followed by a large, empty text area with a vertical scrollbar. At the bottom right, there are three buttons: '< Previous', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

- e. Click **Next** to move on to the **Configure Certificate** window.
- 3. Modify the TrueCommand Certificate (tc.cer).
 - a. Open PowerShell and type `Invoke -webRequest -uri http://IP:PORT/saml/metadata -outfile tc.cer`.
IP:PORT is your TrueCommand system IP address/port number.

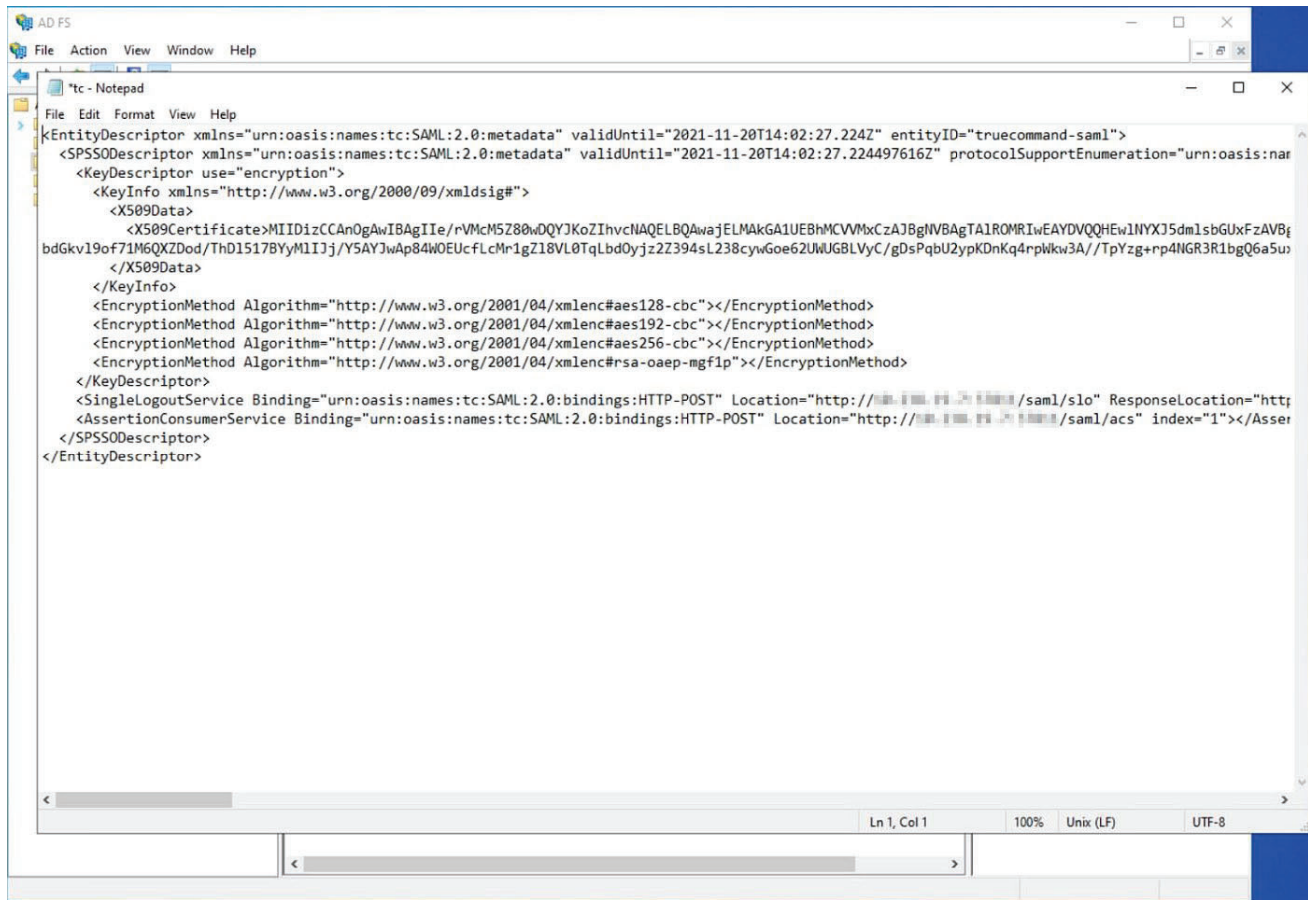


b. Edit the certificate as follows:

1. Open a File Explorer window and locate the tc.cer file in C:/local data/user/QE.

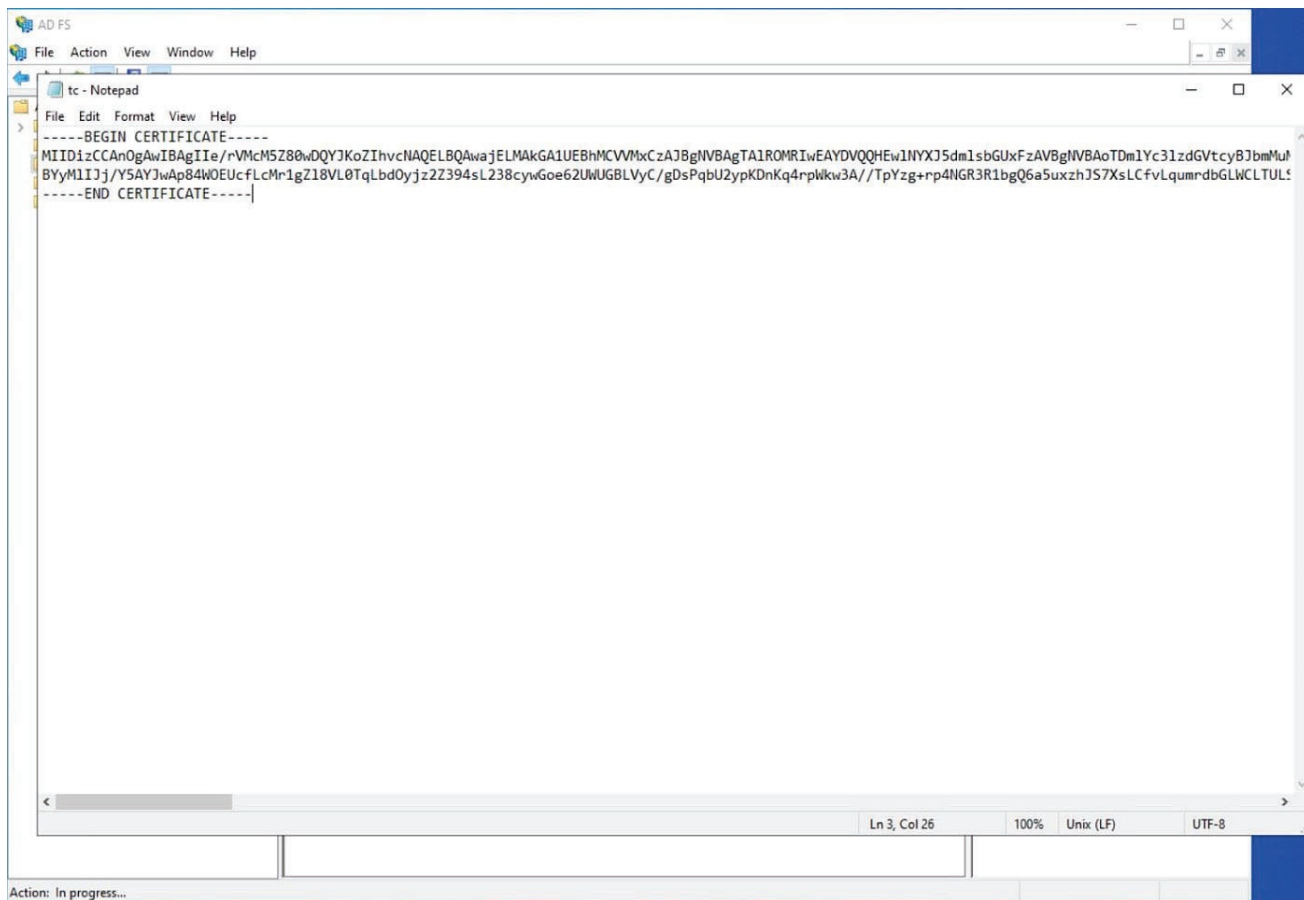


2. Select the tc.cer file, right-click, then select **Open with Notepad**.
3. Delete everything before the `<x509Certificate>` tag, and everything after the `</x509Certificate>` tag.

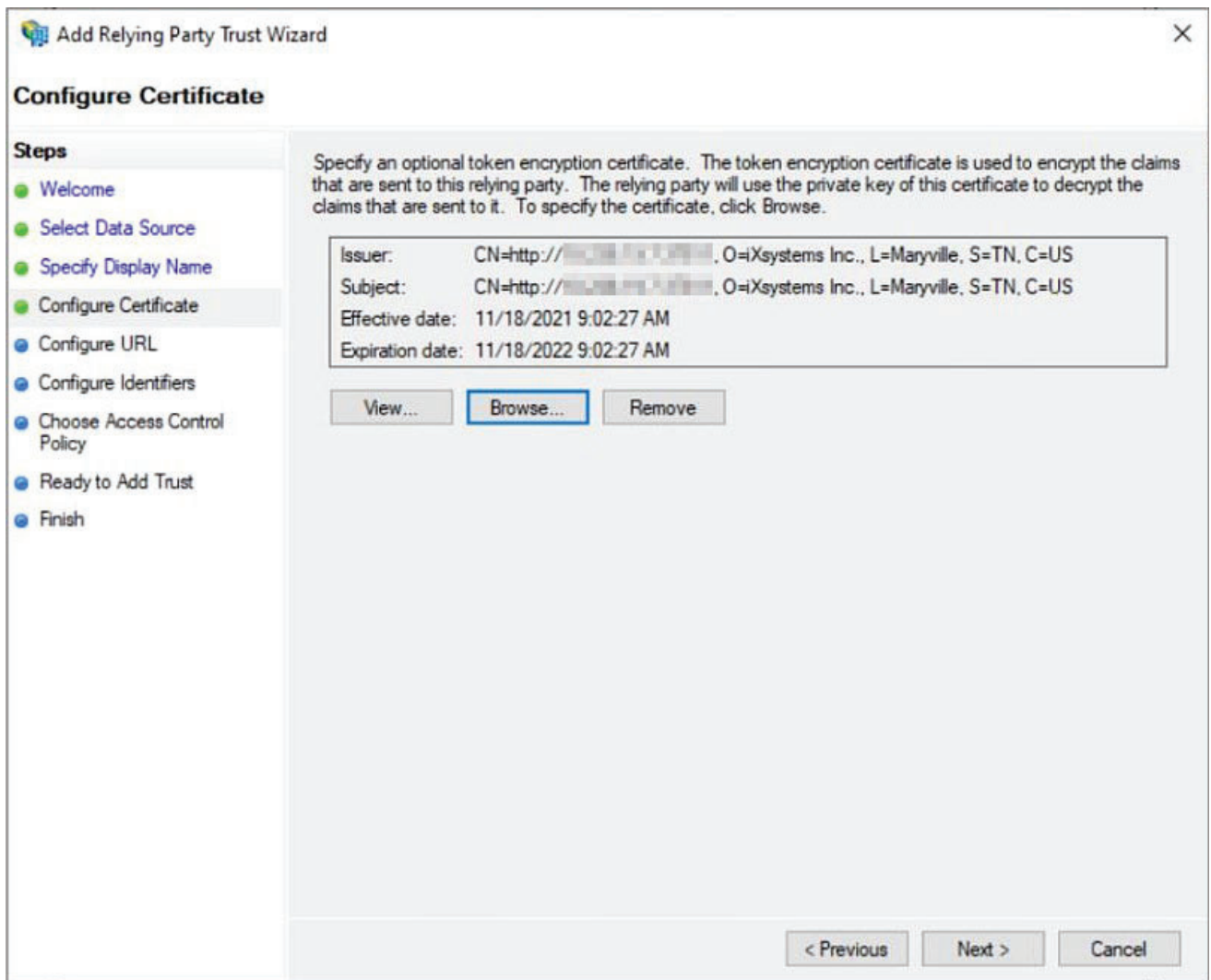


```
<?xml version="1.0" encoding="UTF-8"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2021-11-20T14:02:27.224Z" entityID="truecommand-saml">
  <SPSSODescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2021-11-20T14:02:27.224497616Z" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="encryption">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data>
          <X509Certificate>MIIDizCCAn0gAwIBAgIIe/rVMcM5Z80wDQYJKoZIhvcNAQELBQAwajELMAkGA1UEBhMCVWxkZzAJBgNVBAGTA1ROMRlWEEYDVQQHEw1NYXJ5J5dmlsbGUxZzAVBgkqhkiG9w0f71M6QXZDod/ThD1517BYyMlIj/Y5AYJwAp84W0EUcFLCmr1gZ18VL0TqLbd0yJzZ394sL238cywGoe62UwUG8LVyC/gDsPqbU2ypKdKq4rpWkw3A//TpYzg+rp4NGR3R1bgQ6a5u:
        </X509Data>
      </KeyInfo>
      <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmenc#aes128-cbc"></EncryptionMethod>
      <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmenc#aes192-cbc"></EncryptionMethod>
      <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmenc#aes256-cbc"></EncryptionMethod>
      <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmenc#rsa-oaep-mgf1p"></EncryptionMethod>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://10.10.10.10/saml/slo" ResponseLocation="http://10.10.10.10/saml/slo"></SingleLogoutService>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://10.10.10.10/saml/acs" index="1"></AssertionConsumerService>
  </SPSSODescriptor>
</EntityDescriptor>
```

4. Type the following string exactly as -----BEGIN CERTIFICATE----- before the certificate with five dashes before and after.
5. Type the following string exactly as -----END CERTIFICATE----- after the certificate with five dashes before and after.



6. Click **Save** (or **Ctrl-S**) and then close Notepad.
- c. Close Powershell.
- d. Select **Browse** in the **Configure Certificate** window. The **Encryption Certificate** window opens.



e. Locate the tc.cer file (C:/local disk/users/QE and then select the tc.cer). Click **Open** to view the **Configure Certificate** window and see information about the certificate. Click **Next** to move on to the **Configure URL** window.

4. Configure the URL. In the **Configure URL** window:
 - a. Select **Enable support for the SAML 2.0 WebSSO protocol**.

Add Relying Party Trust Wizard

Configure URL

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL**
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

☐ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: `https://fs.contoso.com/adfs/ls/`

☒ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

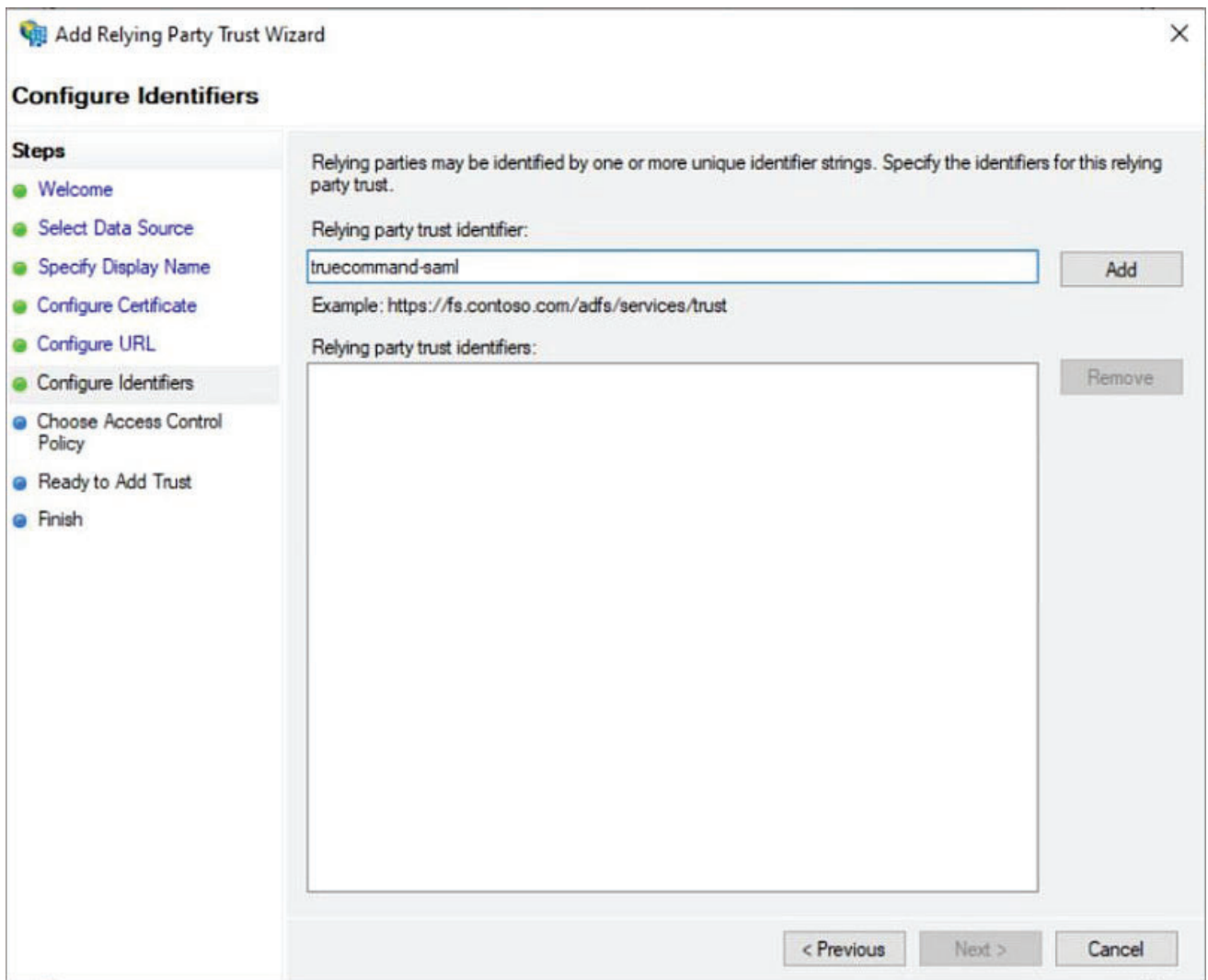
Relying party SAML 2.0 SSO service URL:

`https://[IP:PORT]/saml/acs`

Example: `https://www.contoso.com/adfs/ls/`

< Previous **Next >** Cancel

- b. Type or copy/paste the TrueCommand login URL (`http://IP:PORT/saml/acs`) in the **Relying party SAML 2.0 SSO service URL** field. *IP:PORT* is your TrueCommand system IP and port address.
 - c. Click **Next** to continue to the **Configure Identifiers** window.
5. Configure the SAML identifiers.
- a. Type **truecommand-sml** into the **Relying party trust identifier** field and click **Add**.



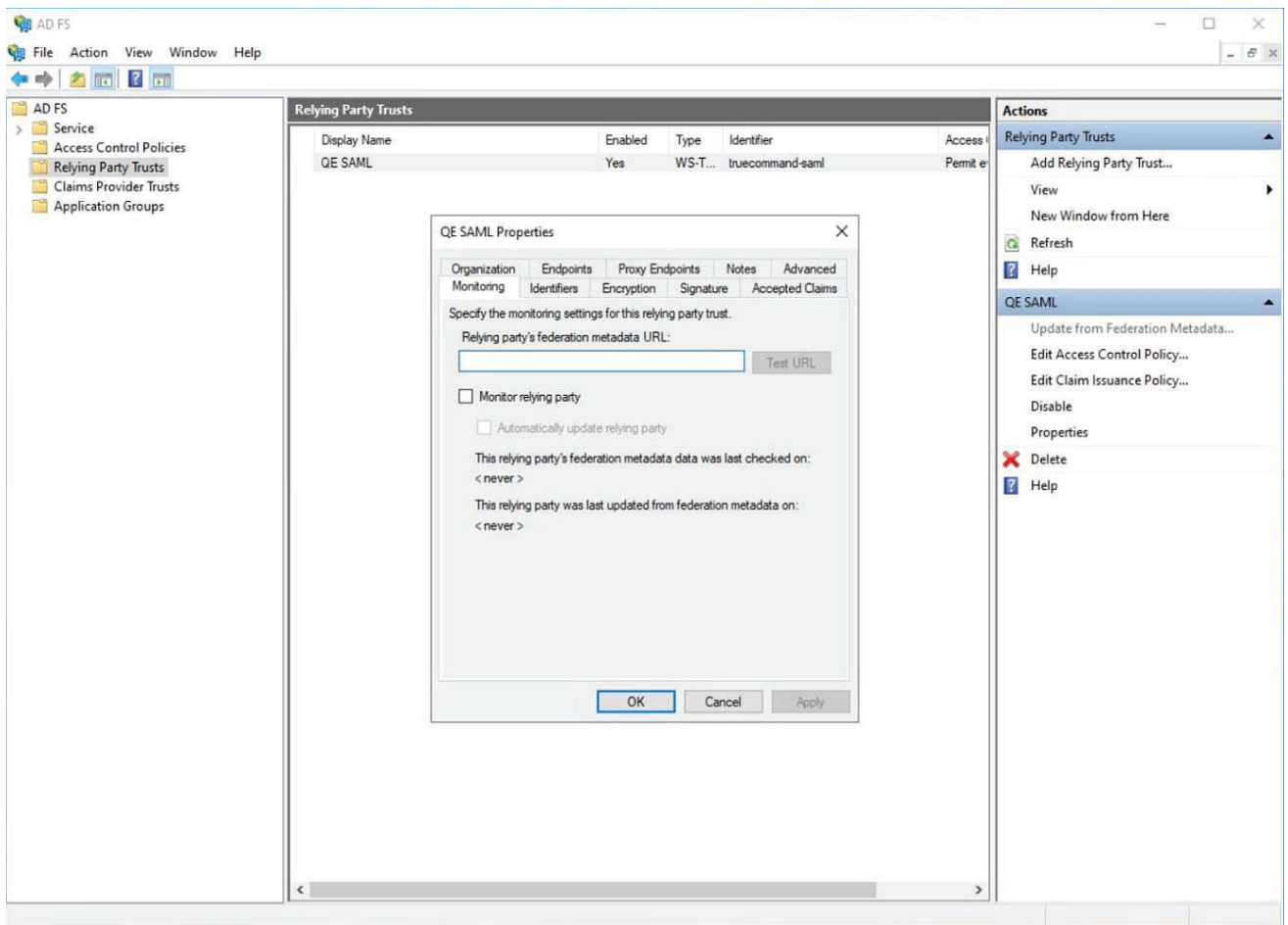
b. Click **Next** to move on to the **Choose Access Control Party** window.

c. Click **Next** again to view the **Ready to Add Trust** window, then click **Next** once more and select **Close**.

! [WizardClickFinishCropped] (/images/SAML/WizardClickFinishCropped.png "Wizard Click Finish Cropped")

6. Modify the newly-created Relying Party Trust.

a. Select the new SAML Relying Party Trust and then select **Properties** in the **Actions** menu to open the **Properties** window.



- b. Select the **Endpoints** tab, then click **Edit** to open the **Edit Endpoint** window.
- c. Change the **Index** value to **1** and click **OK**.

QE SAML Properties

Edit Endpoint

Endpoint type:
SAML Assertion Consumer

Binding:
POST

☐ Set the trusted URL as default

Index: 1

Trusted URL:
https://[IP]:[PORT]/saml/acs
Example: https://sts.contoso.com/adfs/ls

Response URL:

Example: https://sts.contoso.com/logout

OK Cancel

d. Click the **Add SAML** button to open the **Add an Endpoint** window.

e. Type or copy/paste the TrueCommand URL (<http://IP:PORT/saml/slo>) in the **Trusted URL** field.

QE SAML Properties

Add an Endpoint

Endpoint type:
SAML Assertion Consumer

Binding:
Artifact

☐ Set the trusted URL as default

Index: 0

Trusted URL:
https://[IP]:[PORT]/saml/slo
Example: https://sts.contoso.com/adfs/ls

Response URL:

Example: https://sts.contoso.com/logout

OK Cancel

f. Click **OK**, **Apply**, and then **OK**.

7. Configure the Claim Issuance Policy.

- a. Select **Edit Claim Issuance Policy** in the **Actions** menu to open the **Edit Claim Issuance Policy for QE SAML** window. The QE SAML is the name you gave your new SAML Relying Party Trust in the preceding steps.

```
![EditQESAMLCI Claim IssuancePolicyWindowCropped]
(/images/SAML/EditQESAMLCI ClaimIssuancePolicyWindowCropped.png "Edit QE SAML Claim Issuance Policy Window Cropped")
```

- b. Click **Add Rule** and select **Transform an Incoming Claim**, then click **Next**.

```
![EditClaimIssuancePolicyAddRuleTransformAnIncomingClaimCropped]
(/images/SAML/EditClaimIssuancePolicyAddRuleTransformAnIncomingClaimCropped.png "Edit Claim Issuance Policy Add Rule Transform An Incoming Claim Cropped")
```

- c. Select **Windows account name** in the **Incoming claim type** drop-down menu.

- d. Select **Name ID** in the **Outgoing claim type** drop-down menu.

- e. Select **Persistent Identifier** in the **Outgoing name ID format** drop-down menu, then click **Finish**.

```
![EditClaimIssuancePolicySetPersistentIdentifierCropped]
(/images/SAML/EditClaimIssuancePolicySetPersistentIdentifierCropped.png "Edit Claim Issuance Policy Set Persistent Identifier Cropped")
```

- f. Click **Add Rule** to add a new rule.

- g. Select **Send LDAP Attributes as Claims** (the default choice) and click **Next**.

```
![EditClaimIssuancePolicyAddRuleSendLDAPAttributesCropped]
(/images/SAML/EditClaimIssuancePolicyAddRuleSendLDAPAttributesCropped.png "Edit Claim Issuance Policy Add Rule Send LDAP Attributes Cropped")
```

- h. Select **Active Directory** as the **Attribute Store**. Type the attributes exactly as below:

```
![EditClaimIssuancePolicyAddLDAPAttributesCropped]
(/images/SAML/EditClaimIssuancePolicyAddLDAPAttributesCropped.png "Edit Claim Issuance Policy Add LDAP Attributes Cropped")
```

Parameter	Value
E-Mail-Addresses	email
Display-Name	given_name
User-Principal-Name	unique_name
Telephone-Number	telephoneNumber
Title	title

- i. Click **Finish**, **Apply**, and **OK**.

8. Close **Active Directory**.

9. Go to the TrueCommand login page and use the **SAML Login**.

○ Google Admin

To configure Google Admin as the IdP, you must:

- Create a new App for SAML
- Configure the SAML app properties to act as the IdP service.
- Add the TrueCommand IP and port number as the ACS URL.
- Configure the SAML app LDAP attributes properties

The example procedure below describes these top-level steps in detail.

Activating TrueCommand SAML Service for Google Admin

After configuring SAML in Google Admin, log into your TrueCommand system (i.e., server, container, VM). Go

to **Config > Administration**, then click the **Configuration** tab. Scroll down to the **SAML settings** section.

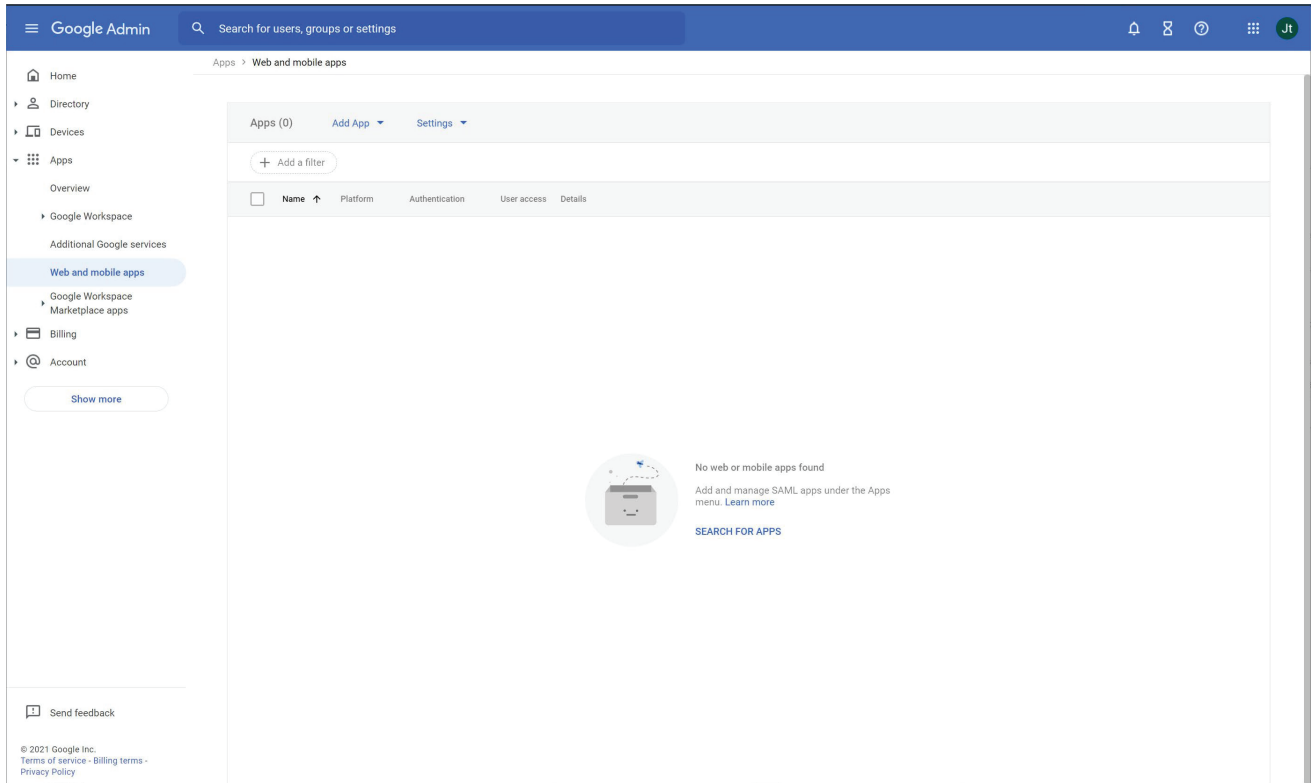
Enter the XML metadata file from Google Admin into the **SAML Identity Provider Metadata XML Upload** field, then click **Save**.

Click the **Start the SAML service** checkbox, then click **Save** to start the service.

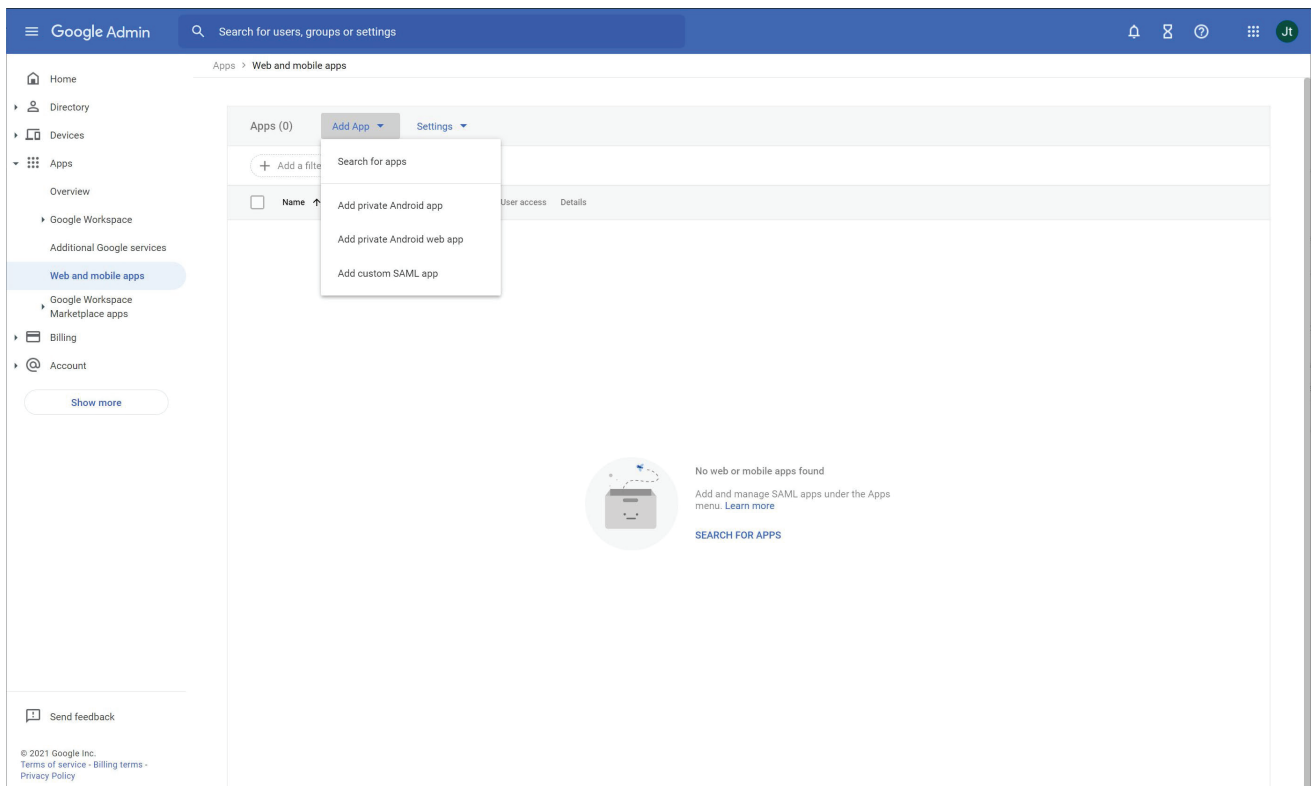
Log out of TrueCommand.

Configuring a Google Admin SAML App

1. Open Google Admin and go to **Apps > Web and mobile apps**



2. Click **Add App**, then select **Add custom SAML app** to open the **App details** screen.



3. Configure the SAML app details.

- a. Type any name you want to use in the **App Name** field. This example uses *tcsaml*.
 - b. Upload any picture or avatar you want to use into the **App icon** area to identify the app in your Google Admin account.
 - c. Click **CONTINUE**. to view the **Google Identity Provider** screen.
4. Click **CONTINUE** to view the **Service Provider details** screen.

5. Configure the service provider details.

The screenshot shows the 'Add custom SAML app' configuration page with four steps: 1. App details, 2. Google Identity Provider details, 3. Service provider details (active), and 4. Attribute mapping. The 'Service provider details' form includes the following fields:

- ACS URL:** A red error message 'ACS URL is required' is displayed below the field.
- Entity ID:** A red error message 'Entity ID is required' is displayed below the field.
- Start URL (optional):** An empty text field.
- Signed response:** An unchecked checkbox.
- Name ID:** A section with a description: 'Defines the naming format supported by the identity provider. [Learn more](#)'.
- Name ID format:** A dropdown menu currently set to 'UNSPECIFIED'.
- Name ID:** A dropdown menu currently set to 'Basic Information > Primary email'.

At the bottom of the form are three buttons: 'BACK', 'CANCEL', and 'CONTINUE'.

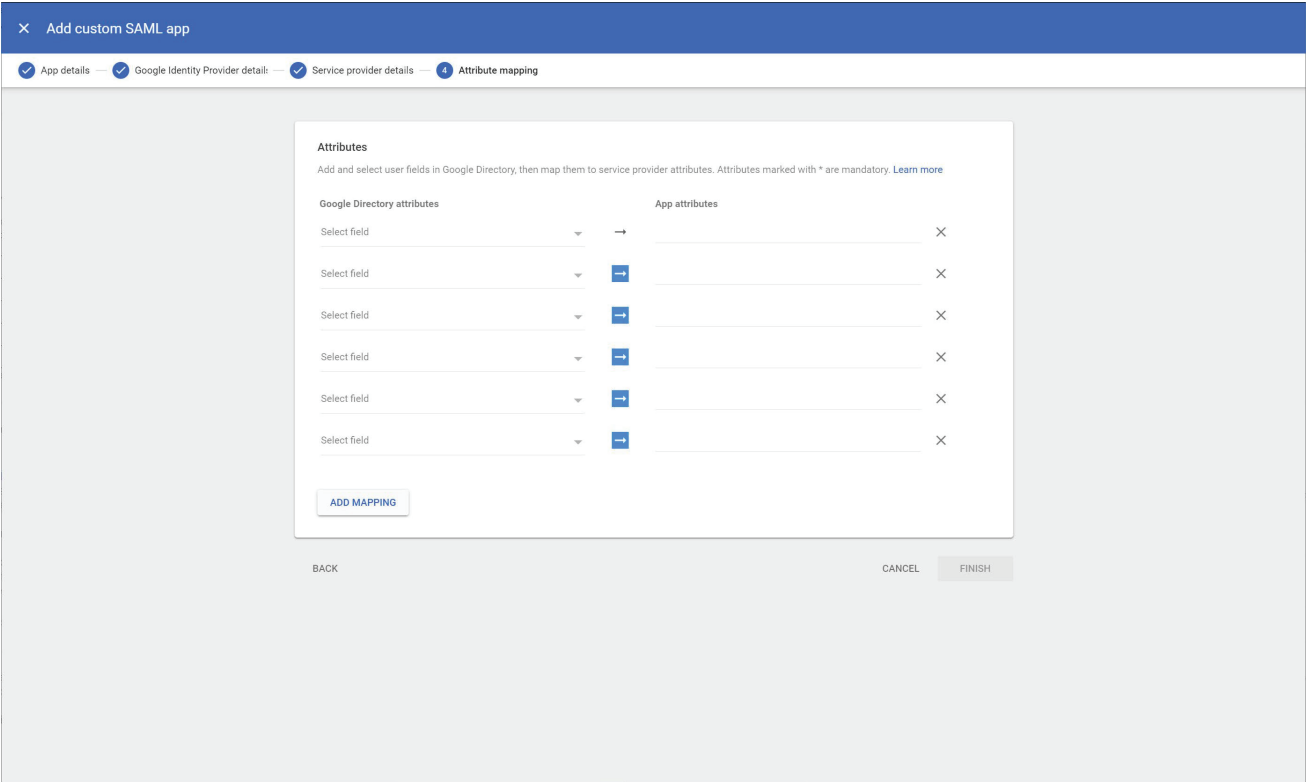
- Type or copy/paste the TrueCommand login URL `http://IP:PORT/saml/acs` into the **ACS Url** field. *IP:PORT* is your TrueCommand system IP and port address.
- Type any name you want into the **Entity ID** field (ex. truecommand-saml).
- Type the `https://IP:PORT/saml/helloURL` into the **Start URL** field. *IP:PORT* is your TrueCommand system IP and port address.
- Set **Name ID** format to **PERSISTENT**.

This screenshot shows the same 'Service provider details' form after configuration. The fields are now populated:

- ACS URL:** `https://10.20.20.1/saml/acs`
- Entity ID:** `truecommand-saml`
- Start URL (optional):** `https://10.20.20.1/saml/hello`
- Signed response:** Still unchecked.
- Name ID format:** The dropdown menu is now set to 'PERSISTENT'.
- Name ID:** Still set to 'Basic Information > Primary email'.

The 'CONTINUE' button is now highlighted in blue, indicating the next step in the process.

- e. Set **Name ID** to **Basic Information > Primary Email**.
- f. Click **CONTINUE** to view the **Attribute Mapping** screen.



- g. Enter the **Attributes**. Select the attribute using the **Google Directory attributes** drop-down menus, then type the attributes exactly as below into the **App attributes** fields:

Parameter	Value
E-Mail-Addresses	email
Display-Name	given_name
User-Principal-Name	unique_name
Telephone-Number	telephoneNumber
Title	title

- h. Click **FINISH**.

- 6. Verify the information is correct. Select **TEST SAML LOGIN** in the **tcsaml** area on the left side of the screen to open the **TrueCommand SAML Test** screen.

User access

To make the managed app available to select users, choose a group or organizational unit. [Learn more](#)

View details

ON for 1 organizational unit

Digital Services

Service provider details

Certificate	ACS URL	Entity ID
Google_2026-11-22-6365_SAML2_0 (Expires Nov 22, 2026)	https://[redacted]/saml/acs	truecommand-saml

SAML attribute mapping

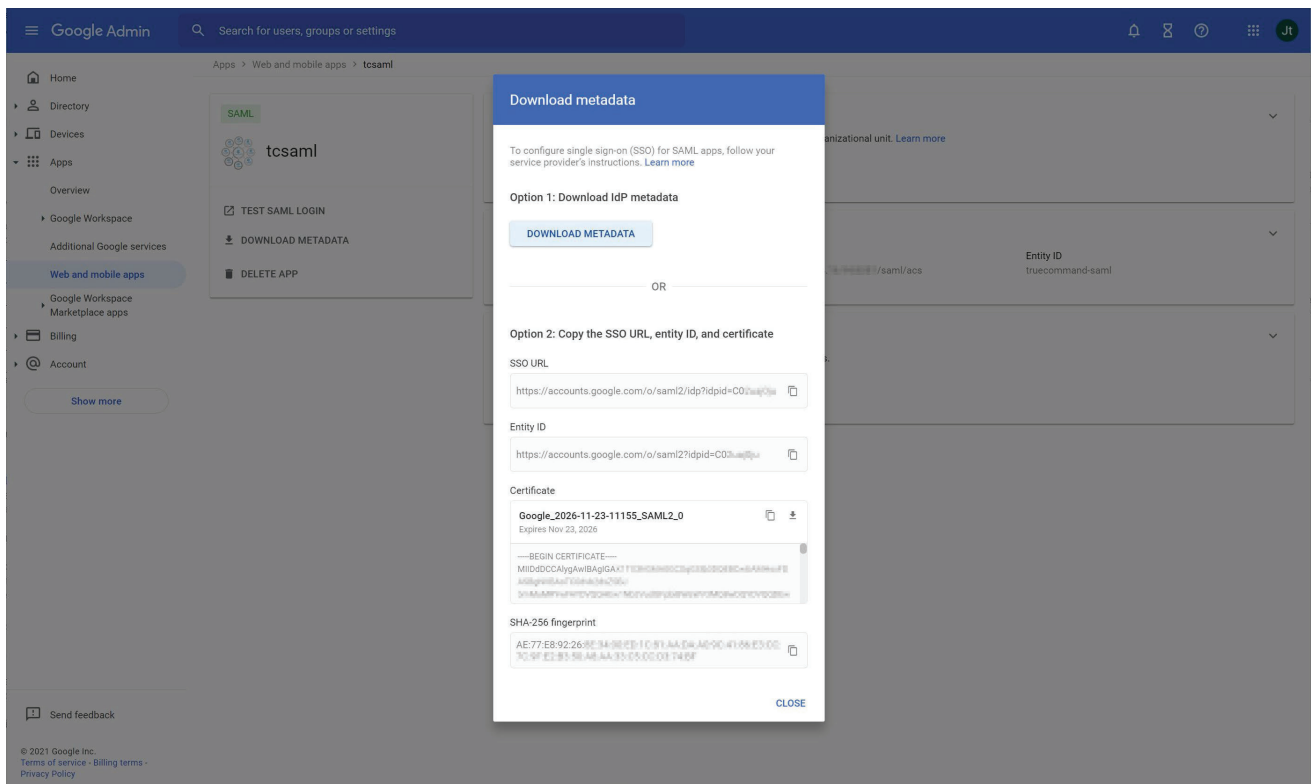
Map Google directory user profile fields to SAML service provider attributes.

display_name	mail	telephone_number
Basic Information > First name	Basic Information > Primary email	Contact Information > Phone number
title	unique_name	
Employee Details > Title	Employee Details > Employee ID	

7. Download the metadata.

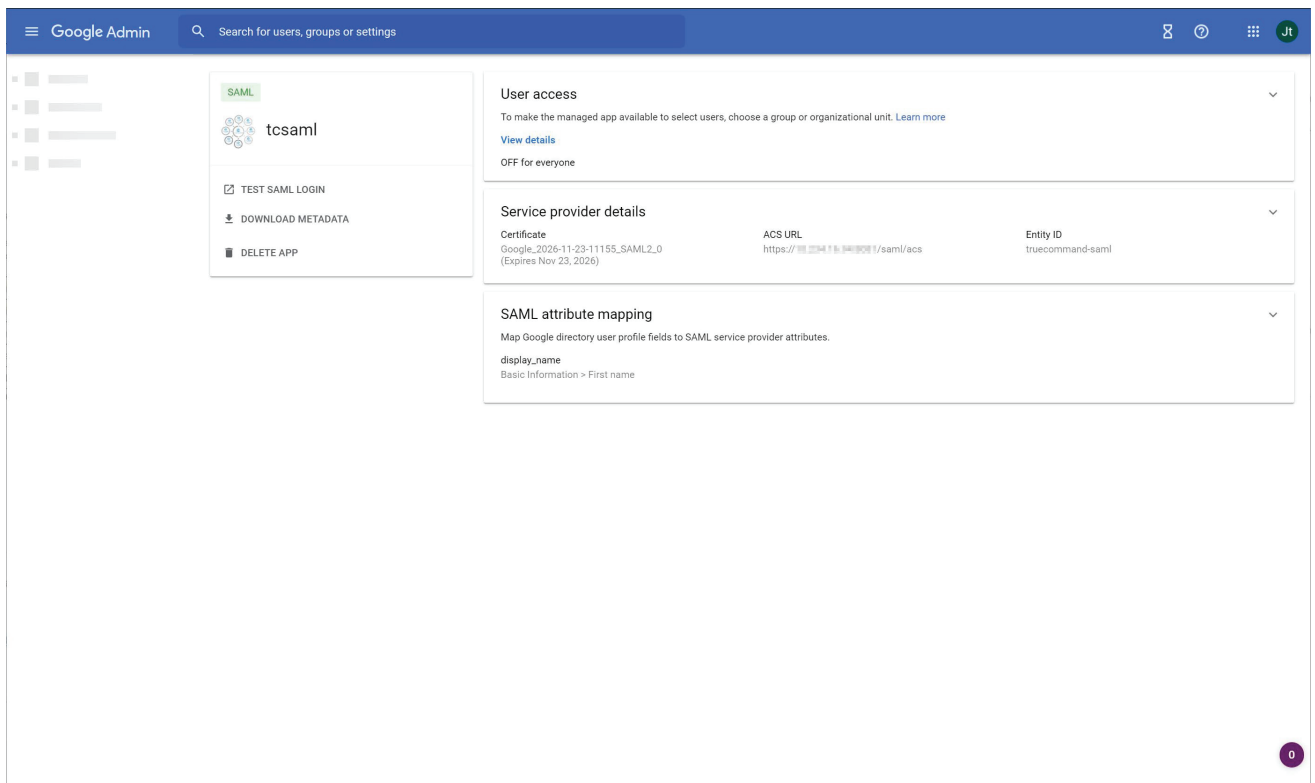
The screenshot shows the Google Admin console interface. On the left, a sidebar contains a list of apps, with 'tcsaml' selected. A blue arrow points to the 'DOWNLOAD METADATA' button in the sidebar. The main content area on the right displays the configuration for the 'tcsaml' app, including sections for 'User access', 'Service provider details', and 'SAML attribute mapping'.

- Select **DOWNLOAD METADATA** to open the **Download Metadata** window.
- Click **DOWNLOAD METADATA** again. When complete, click **CLOSE**.

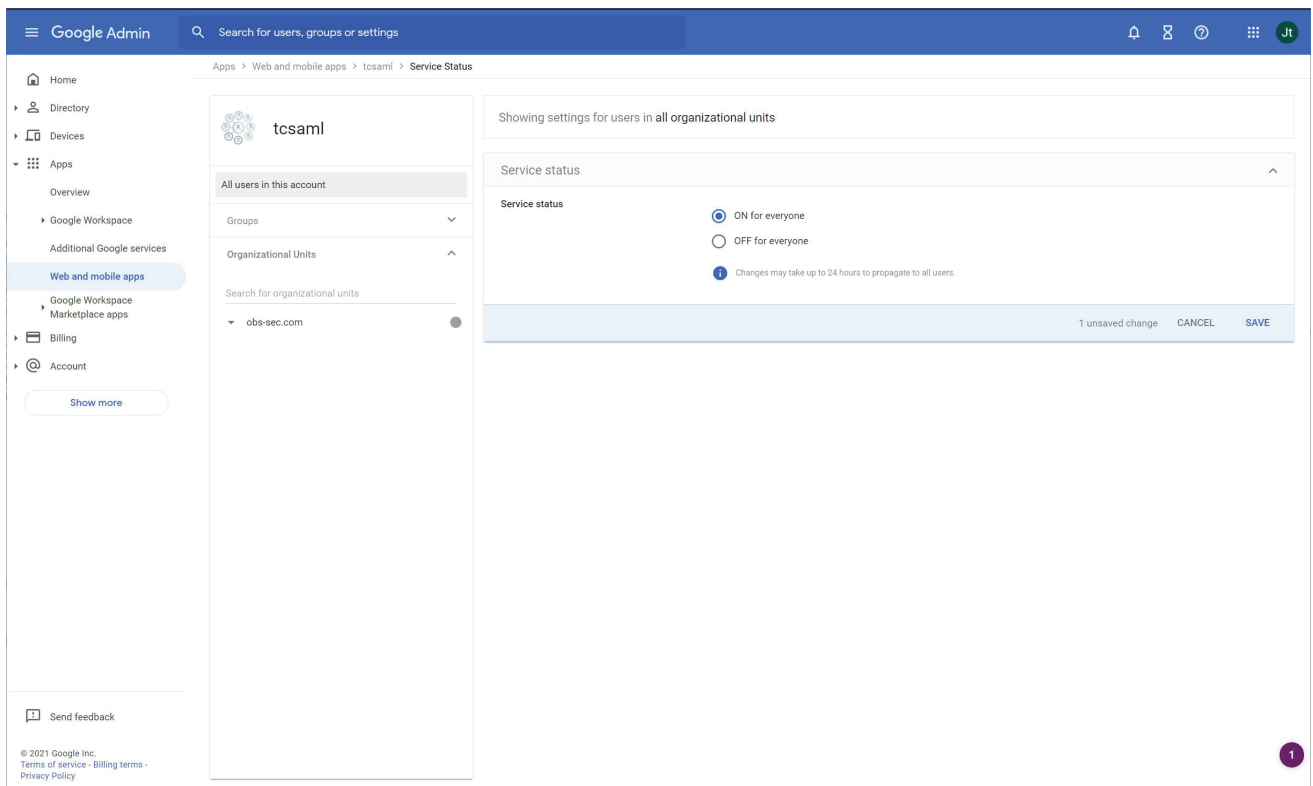


8. Verify user access details.

a. Click **View Details** under **User access** to display the **Service status** details.



b. Select **ON for everyone** and click **SAVE**.



If you want granular user control, use this area to set it.

9. Wait up for approximately 10-20 minutes for Google to populate all settings through its servers

Configuring TrueCommand for SAML Service

1. Log into TrueCommand as an administrator.
2. Click the **settings** button on the top toolbar. Click **Administration**, then select the **Configuration** tab. Scroll down to **SAML settings**.
3. Upload the file to True Command using the **SAML Identity Provider Metadata XML File Upload** box, then click **Save**.
4. Click the **Start the SAML service** checkbox to enable the service, and click **Save** again.
5. Log out of TrueCommand.
6. Login with the **SAML Login**.

5.4 - System Log

TrueCommand records all user activity in a system log. For example, if a user deletes a system from TrueCommand, the log records which user deleted it, along with other information associated with the deleted system.

To view the system log, open the **Configure settings** menu and click **Logs**.

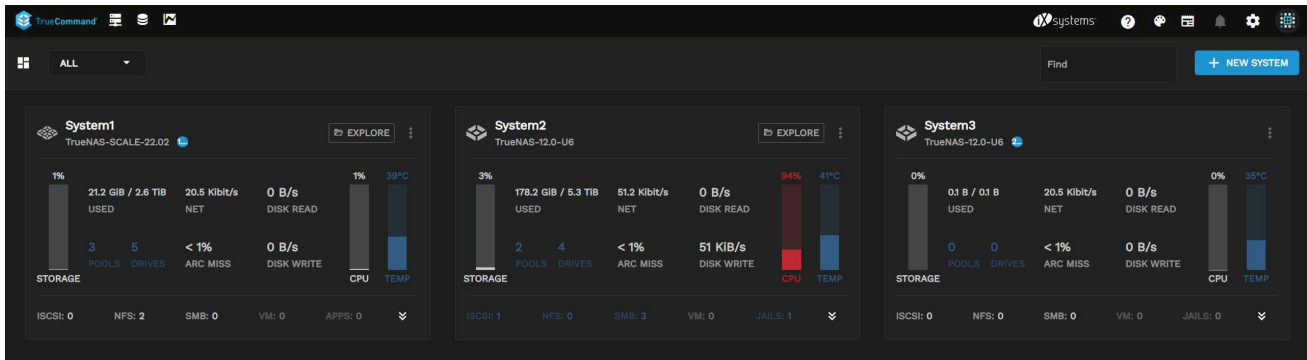
	DATE	API	USER
>	2021-05-10T15:52:29.230295084Z	servers/edit	q5sys
>	2021-05-10T15:52:19.987371327Z	servers/add	q5sys
>	2021-05-10T15:52:06.884224976Z	servers/add	q5sys
>	2021-05-10T15:51:50.731625642Z	servers/add	q5sys
>	2021-05-10T15:51:21.926981139Z	servers/add	q5sys
>	2021-05-10T15:51:00.980308916Z	users/edit	q5sys
>	2021-05-10T15:50:59.571918114Z	users/edit	q5sys
>	2021-05-10T15:50:49.360722059Z	rpc/auth	q5sys
>	2021-05-10T15:50:44.620802701Z	users/add	
>	2021-05-10T15:50:36.219719923Z	rpc/auth	

TrueCommand shows all system log entries by default. To hide specific log entry categories, select them in the **Hide** drop-down. You can display all system logs again by clicking **SHOW ALL**. You can also filter logs by entering strings in the **Filter** field.

Click an entry in the log to show detailed information about the event. Clicking **DOWNLOAD ALL LOGS** downloads a .json file that contains all system log entries.

6 - System Management

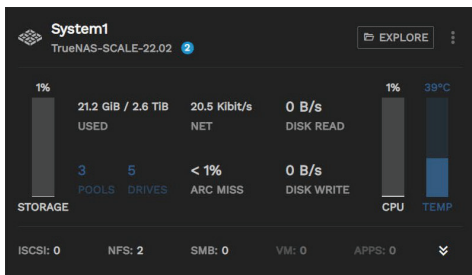
The TrueCommand dashboard provides status overviews of each connected TrueNAS system.



For information on the Top Bar and its options, refer to the [Interface Overview](#) article in the Getting Started Documentation.

System Cards

Each system has a unique card to display statistics. When the system has an alert, an **Alerts** bubble appears next to the system version to show how many alerts there are for that specific system. See [Alert Management](#) for further information.



The **Storage** graph shows how many pools and drives the system is using. It also displays used and available storage by size and percentage.

ARC MISS shows how often the system is using disks instead of the ARC cache. Anything above 0% means that the system is using RAM. The numbers vary by use case and workload.

There are also several “hot spots” on the card that open system-specific areas for management.

Clicking the system name on the card shows an expanded view of the system with more [Single System Management options](#).

Clicking the **Alerts** bubble next to the system version opens an expanded system information screen that lists the current system alerts.

Clicking **DRIVES**, **DISK WRITE**, **DISK READ** displays the disk activity graph.

Clicking **NET** displays the Net Activity graph.

Clicking **CPU** displays the CPU Usage percentages graph.

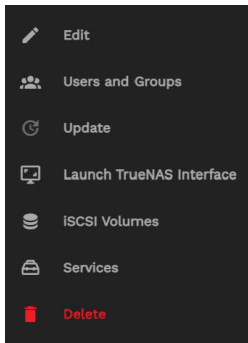
Clicking **TEMP** displays the CPU Temperature percentages graph.

Clicking **ISCSI**, **NFS**, and **SMB** opens a **Services** window that allows users to stop/start services for the system.

Clicking **VM** opens a **Virtual Machines** window that allows users to start/stop VMs on the system.

Clicking **APPS** (SCALE) or **Jails** (CORE 12.x) allows users to start/stop apps/jails on the system.

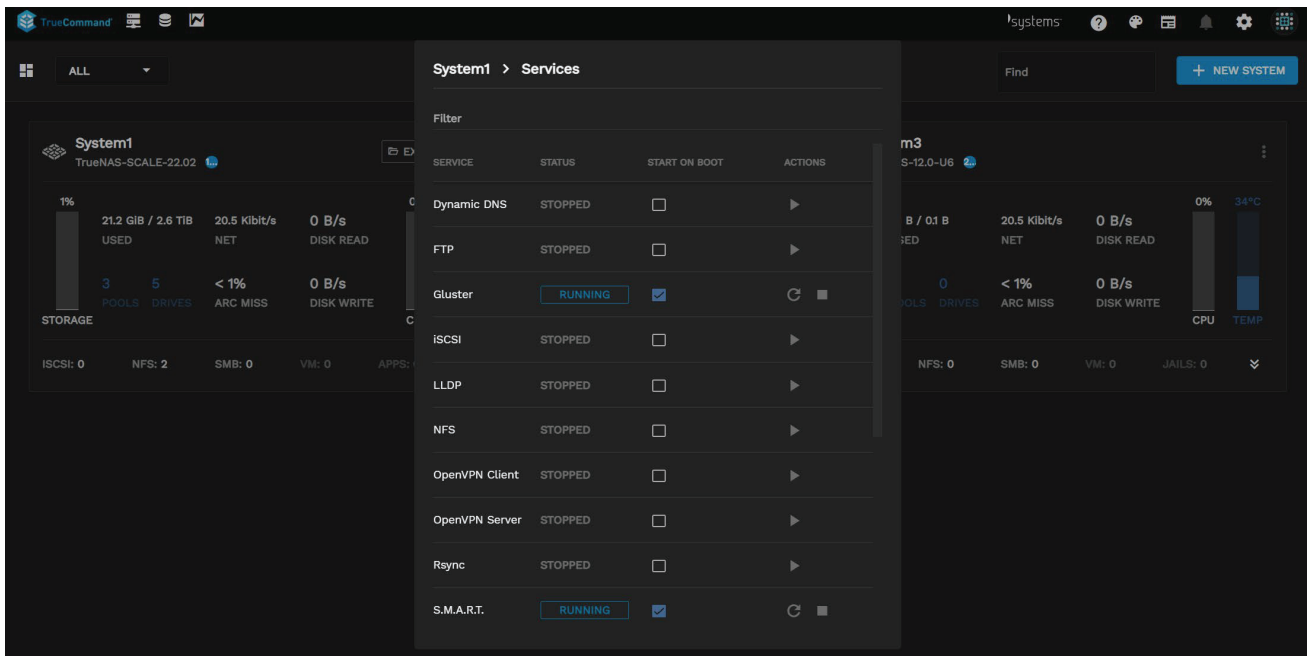
Options Menu



The *Options* menu has several shortcuts to simple tasks.

- **Edit** opens the edit window for the TrueNAS connection details and nickname.
- **Users and Groups** lets users manage NAS users and groups.
- **Update** updates the TrueNAS system.
- **Launch TrueNAS Interface** opens a new tab for the full TrueNAS Web UI.
- **iSCSI Volumes** opens the specific TrueNAS's iSCSI management page.
- **Services** lets users see service statuses and control service actions.
- **Delete** removes the system from TrueCommand. Deleting does not affect any data stored on the TrueNAS system. However, it does delete all system metrics saved in TrueCommand.

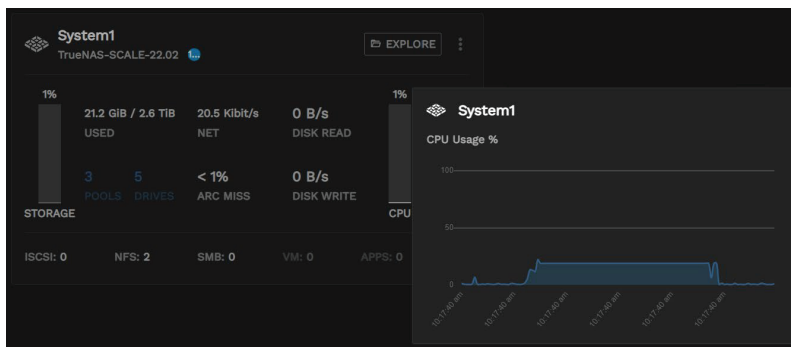
Services



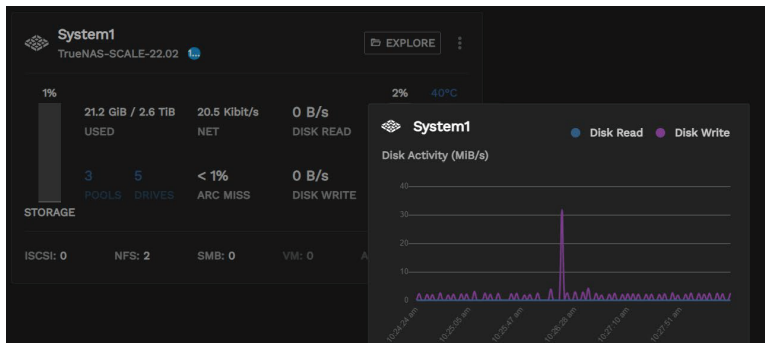
Graphs

Click on the **CPU**, **Disk**, and **Network** values displays the system statistical history.

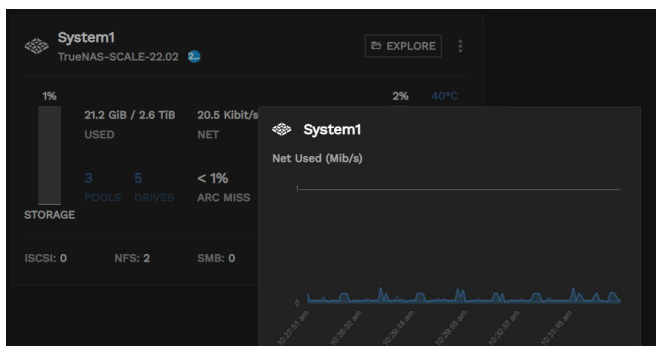
- CPU



- Disk

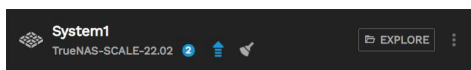





- Network



Activity Indicator Icons

TrueCommand's activity icons provide an at-a-glance indication of what the system is doing. The indicators appear next to the system nickname.

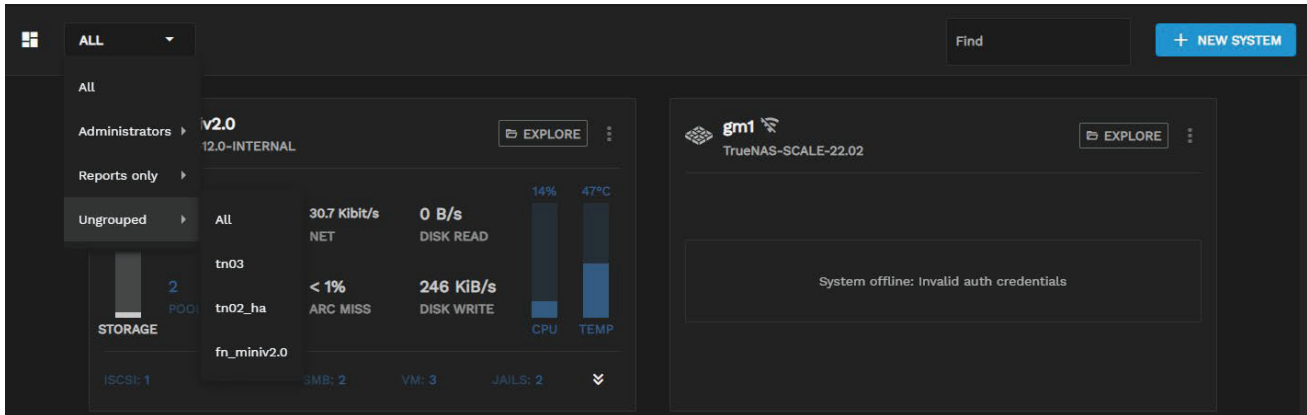


- Update: 
- Replication: 
- Resilver/Scrub : 

6.1 - Single System Management

While TrueCommand allows users to manage all of their systems on a single dashboard, it also lets users view single systems at a time.

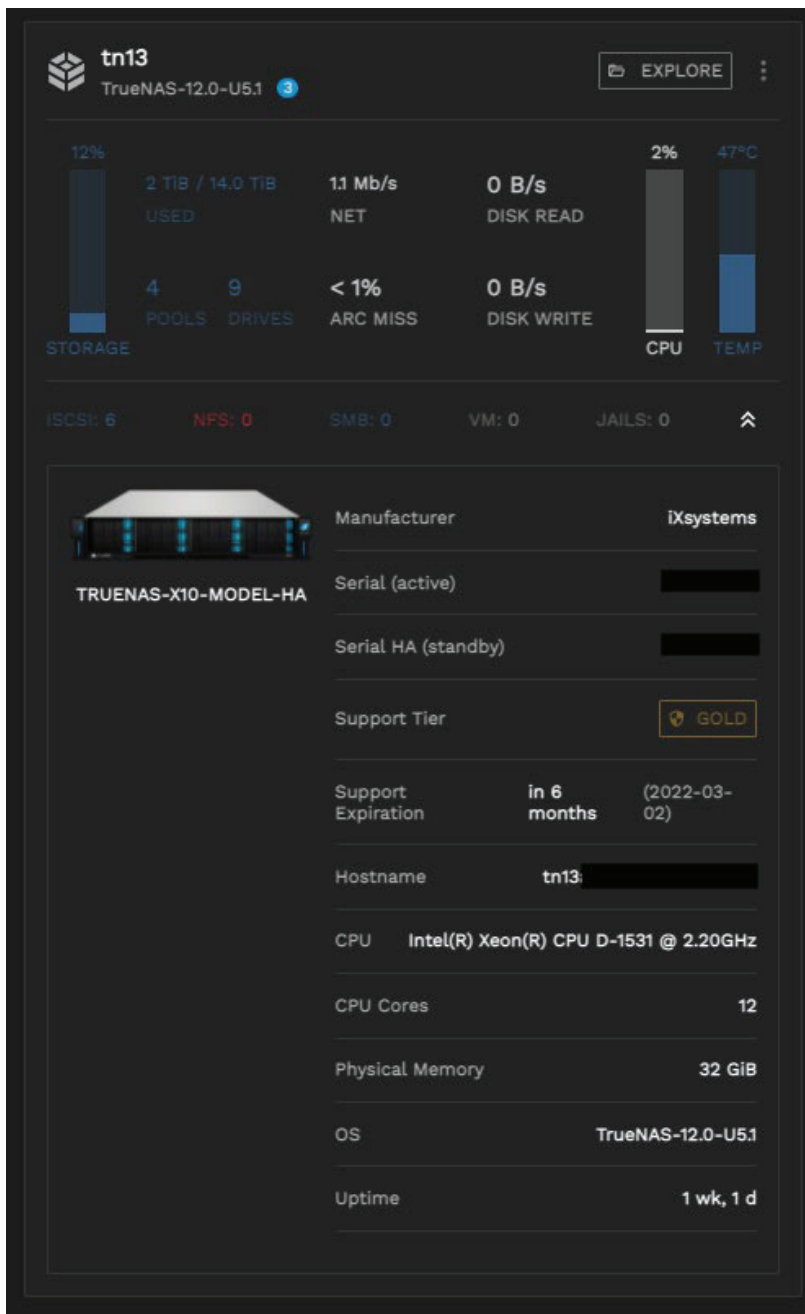
To manage a single system, click on the system name in its card or click on the dashboard drop-down menu, and hover over **Ungrouped** to see the systems list. Select the system you want to manage.



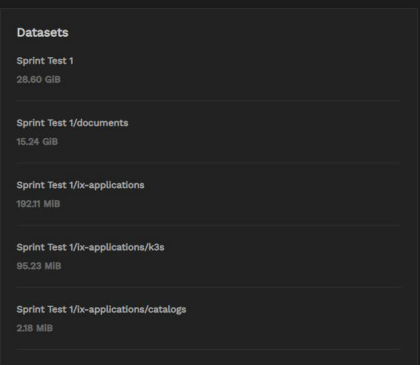
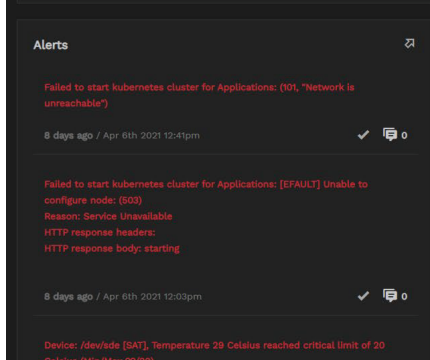
While viewing a single system, users can see various statistics like CPU, memory, disk, network, and storage usage, as well as existing datasets and [alerts](#).

Users can create and manage storage, snapshots, and shares using the **File Explorer**.

Users can view expanded TrueNAS information details by clicking on the double arrows located at the lower right corner of the system card. Information includes the system manufacturer, serial numbers, support tier, support expiration date, hostname, CPU, CPU cores, physical memory, OS, and uptime.

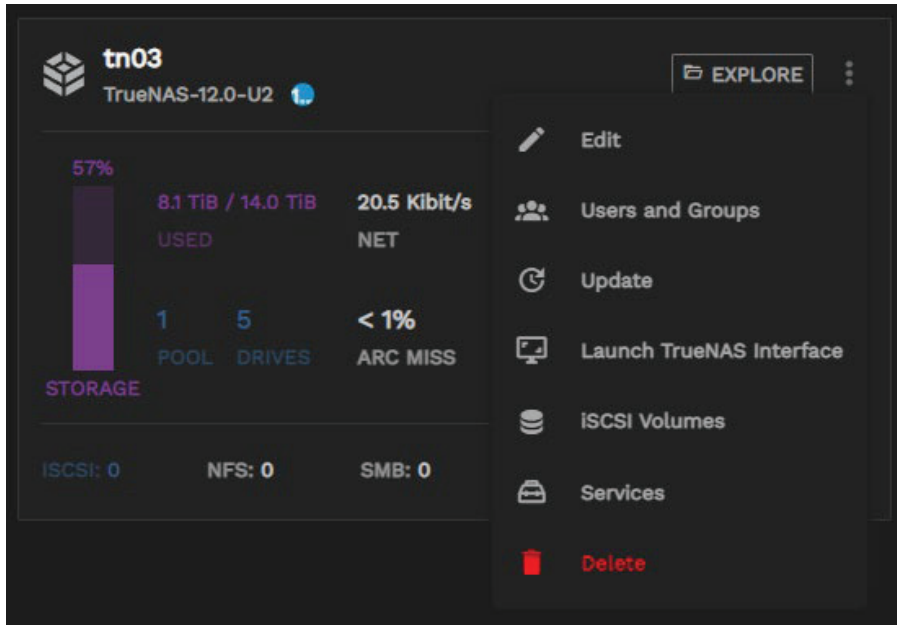


Users with adequate permissions can update the system, [configure backups](#), and generate system audits and [reports](#). If a system update is available, the **Update** label and icon turn green. You can also see which systems have updates pending on the **Systems** screen.



6.1.1 - System Settings



TrueCommand lets users customize select settings when managing a single system. To see the system settings menu, click the three-dot icon in a system card window on the TrueCommand dashboard to display the menu.



🕒 Edit


To edit system general settings, click the **Edit** button in the system settings menu.

The **General Settings** window lets users edit the system IP address/hostname, nickname, password/API key, and alert options. Click **SAVE CHANGES** to keep your changes, or **RESET** reset and start over. Click off the window back to the dashboard to close the edit window without making changes.


 Edit tn03

General Settings


IP Address or Hostname

tn03.qe.ixsystems.net


Nickname

tn03



Password / API Key



Password / API Key Confirm



Alert Options

Ignore

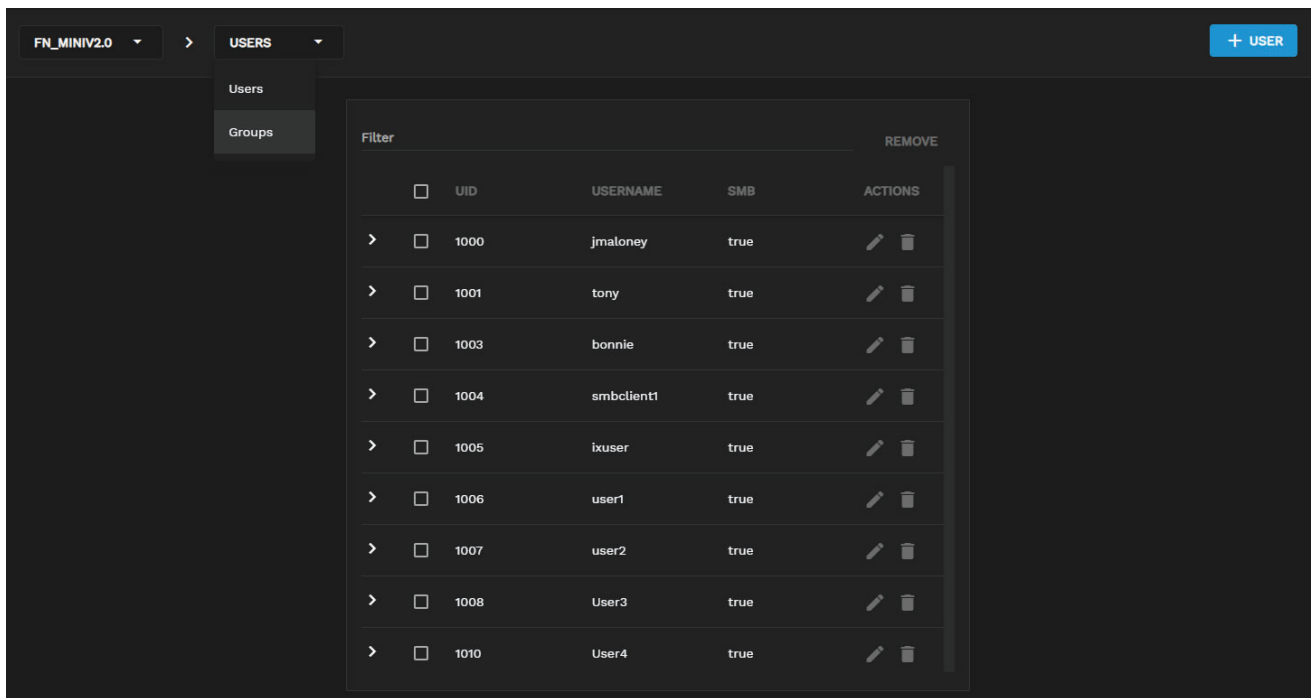
RESET

SAVE CHANGES

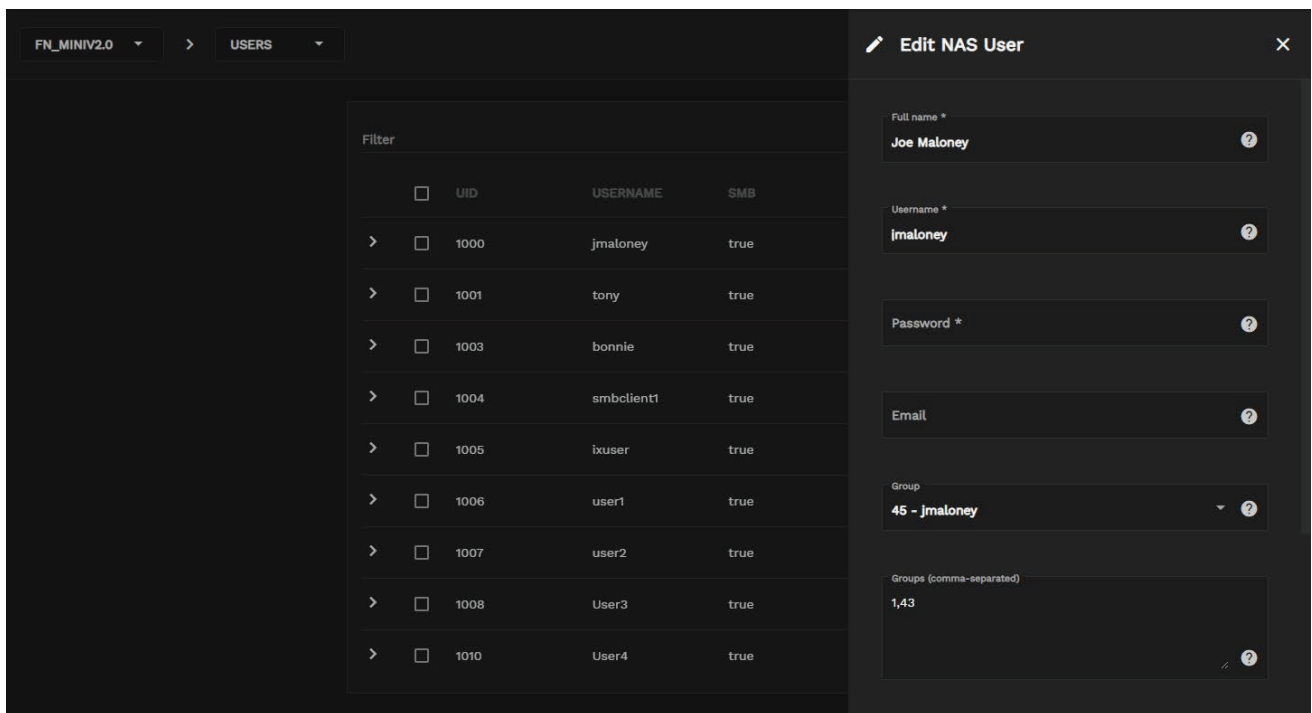
○ Users and Groups

To displays a list of users or groups on the selected system, click the **Users and Groups** button . Click the **Users** dropdown to select **Groups** to change the list to groups on the system.

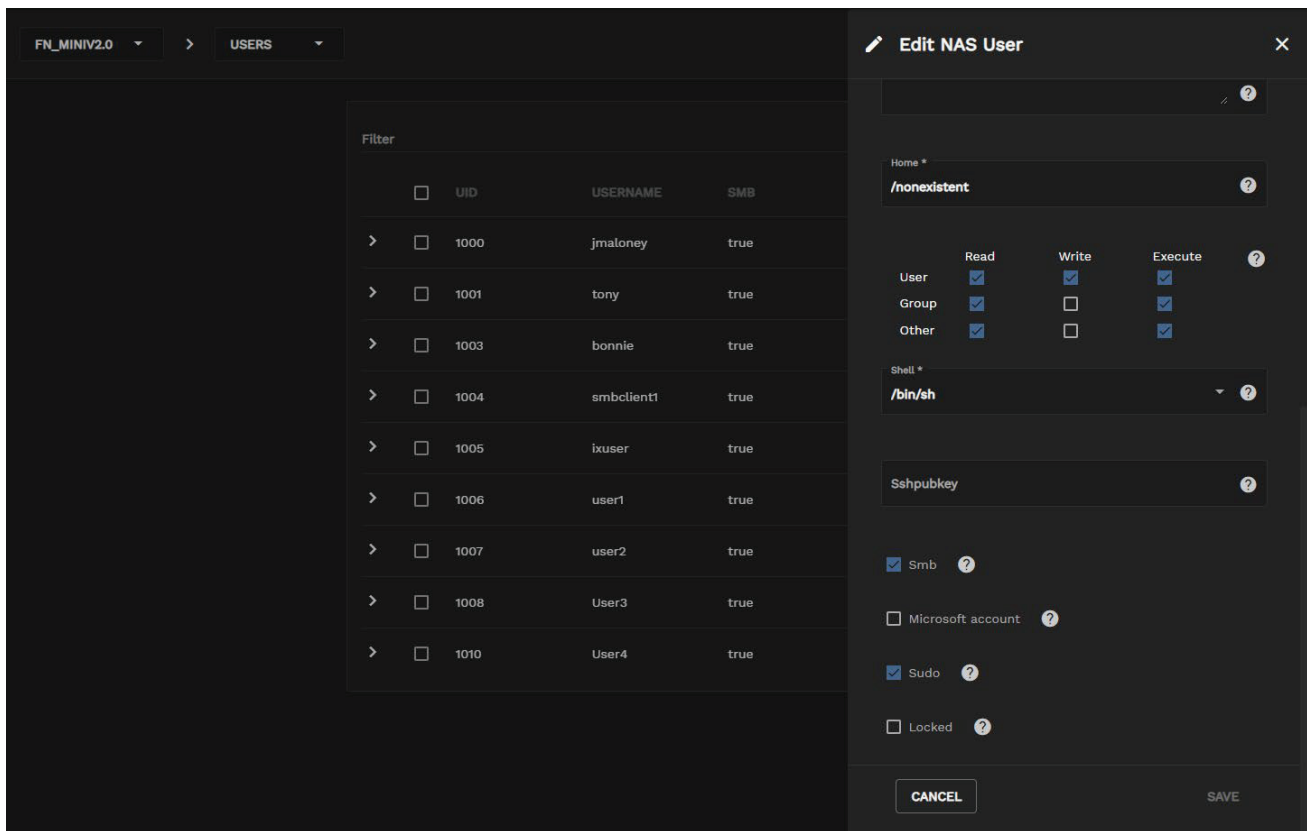
This new 2.1 Users And Groups function is an experimental feature that could be radically changed or removed in future releases. Use with caution!



Click the edit icon **edit** to display the edit user window.

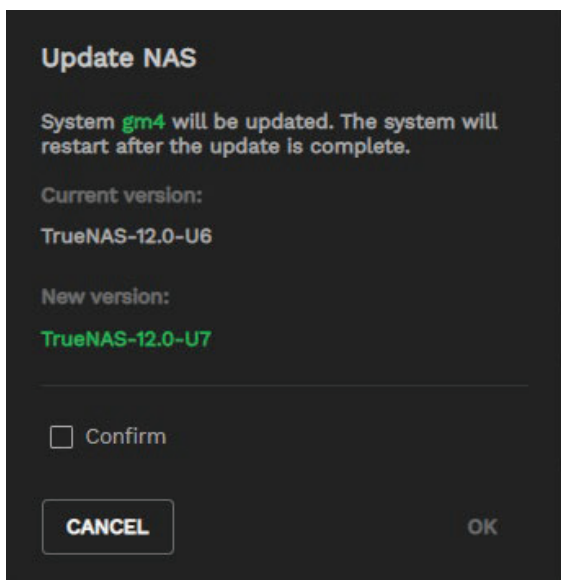


Scroll down to view all edit fields. Click **SAVE** to keep changes or **CANCEL** to discard any changes made. Click the **X** to close the window.



○ Update

Click the **Update** button **update** in the system settings menu to update the system to the latest build. After clicking the **Update** button, an update window with system and update information displays. Click **Confirm** and then **OK** to begin the update, or click **CANCEL** to exit without updating. During a system update, the system card changes to indicate that the system is offline and finishing the update.

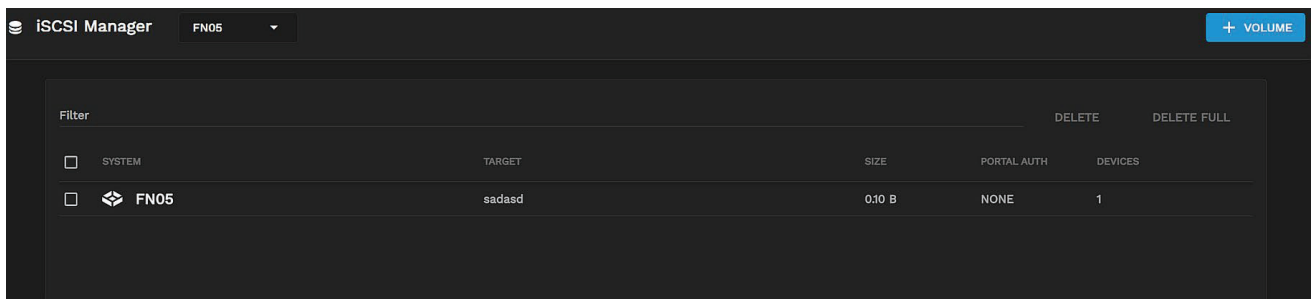


○ Launch TrueNAS Interface

Click the **Launch TrueNAS Interface** button on the system settings menu to open a new browser tab pointed at the selected system's web interface.

○ iSCSI Volumes

Click the **iSCSI Volumes** button on the system settings menu to display the **iSCSI Volumes** screen. It allows users to filter, create, and delete one or more iSCSI volumes.

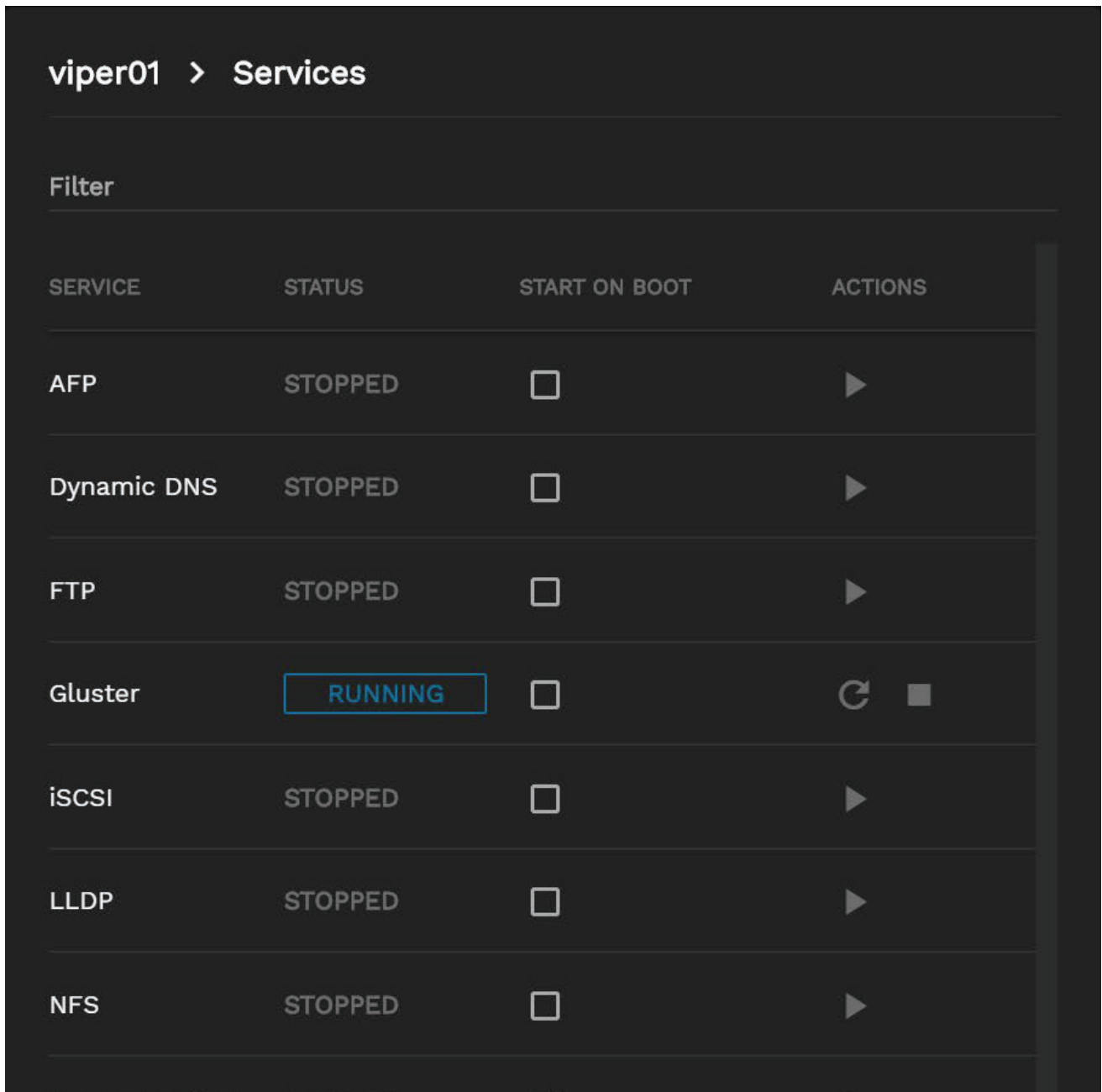


See the full [iSCSI Management](#) article for more information.

○ Services

TrueCommand offers limited control over system services. Click on the **Services** button on the system settings menu to display the list of services on the selected system. The **Services** window displays the current status of the service.

You cannot edit service parameters with TrueCommand, but you can set them to start automatically on boot, stop, and start.



OpenVPN Client	STOPPED	<input type="checkbox"/>	▶
OpenVPN Server	STOPPED	<input type="checkbox"/>	▶
Rsync	STOPPED	<input type="checkbox"/>	▶
S.M.A.R.T.	STOPPED	<input checked="" type="checkbox"/>	▶
S3	STOPPED	<input type="checkbox"/>	▶
SMB	STOPPED	<input type="checkbox"/>	▶
SNMP	STOPPED	<input type="checkbox"/>	▶
SSH	RUNNING	<input checked="" type="checkbox"/>	↺ ■
TFTP	STOPPED	<input type="checkbox"/>	▶
UPS	STOPPED	<input type="checkbox"/>	▶

○ Delete

Click the **Delete** button ~~delete~~ on the system settings menu to delete the selected system from TrueCommand. A confirmation window displays prompting you to confirm by selecting the **Confirm** checkbox and then click **OK** to delete the system. Click **CANCEL** to close the window without deleting the selected system.

Confirm

Delete FN05?



Confirm

CANCEL

OK

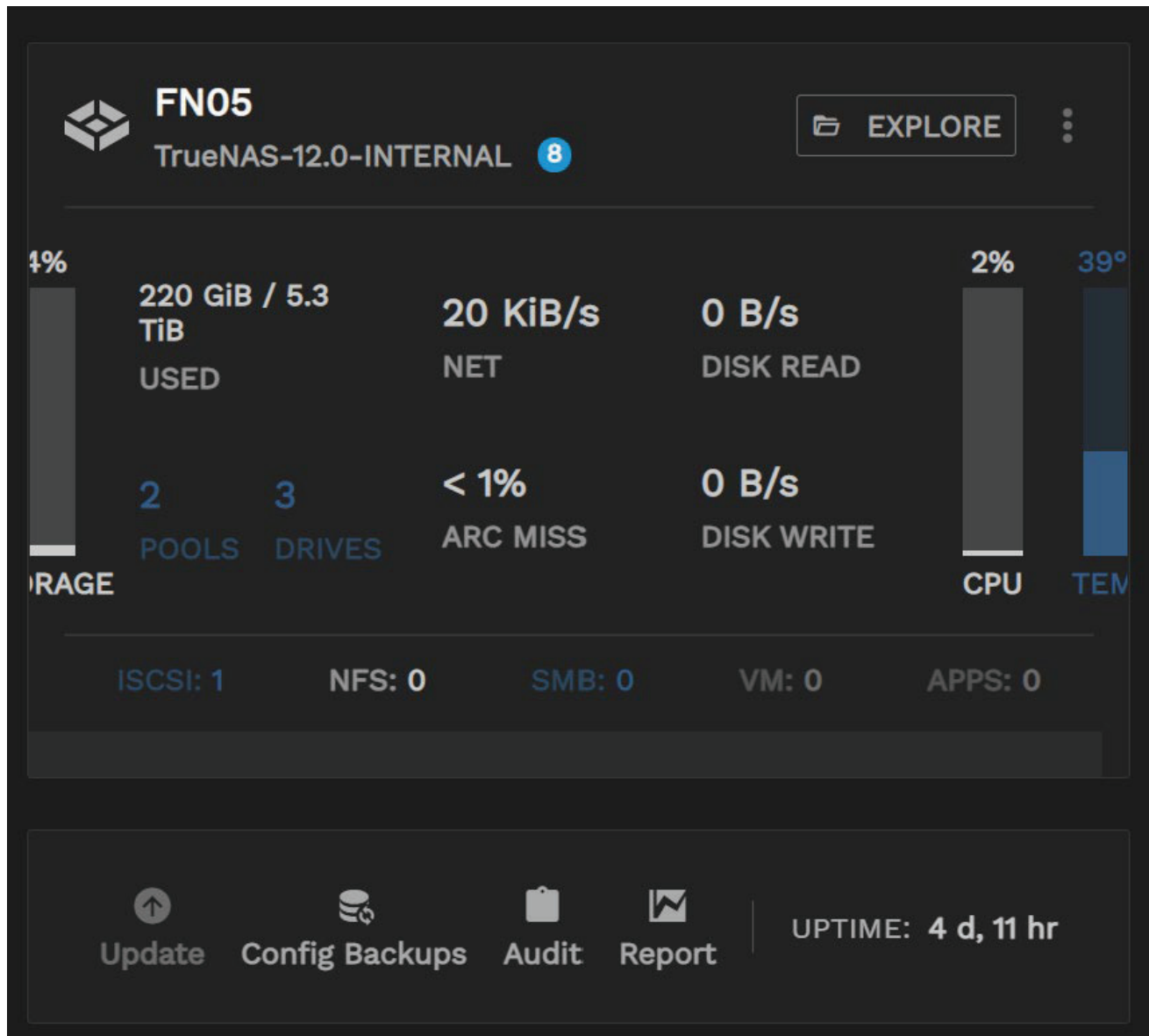
6.1.2 - Config Backups

- - [Create a Backup](#)
 - [Restore a Database](#)
 - [Delete Config Backups](#)

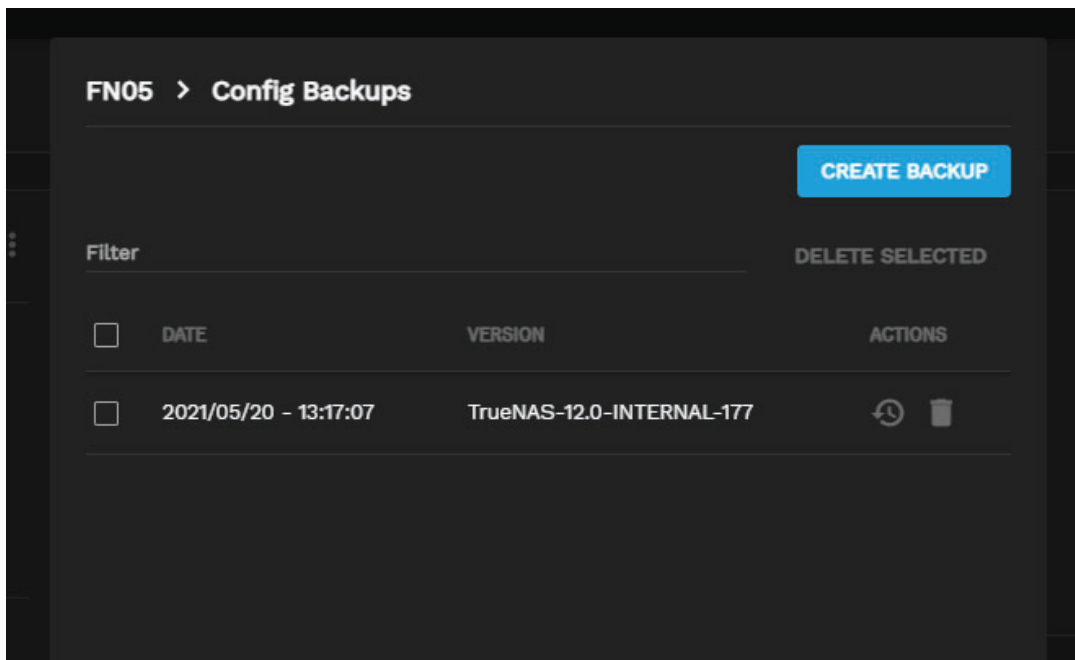
Create a Backup

To create a config backup for a single system, select that system from the dashboard drop-down or click the system's name in the dashboard window.

On the system's management page, click the *Config Backups* button, then click *CREATE BACKUP*.

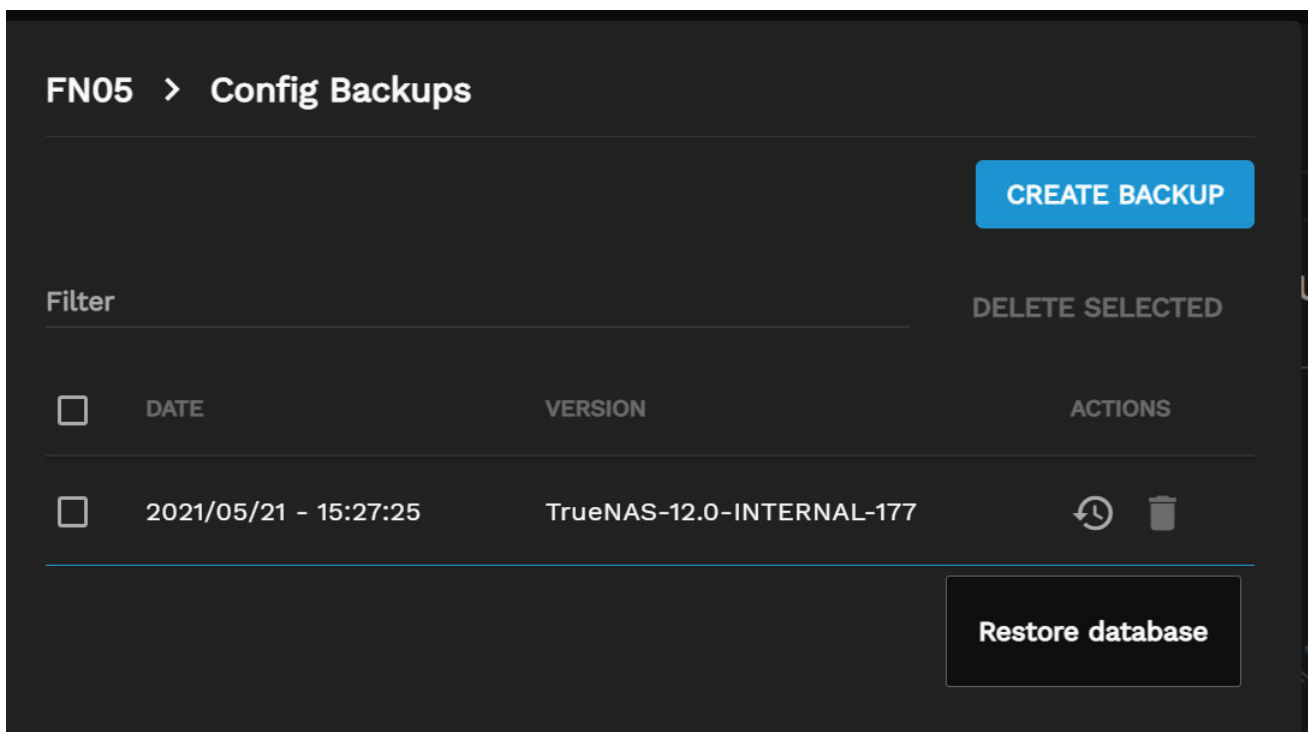


TrueCommand will create a config backup and display the date it was created, as well as what version of truenas the system was using at the time.



Restore a Database

To restore the system to a backed-up config, click the *Config Backups* button on the system's management page, then click the *Restore database* button to the right of the config.



Delete Config Backups

To delete a backup config, click the *Config Backups* button on the system's management page, then click the *Delete backup* button to the right of the config.

To delete multiple backup configs, check the boxes to the left of any configs you want to delete, then click the *DELETE SELECTED* button.

FN05 > Config Backups

CREATE BACKUP

Filter

DELETE SELECTED



DATE

VERSION

ACTIONS



2021/05/21 - 15:27:25

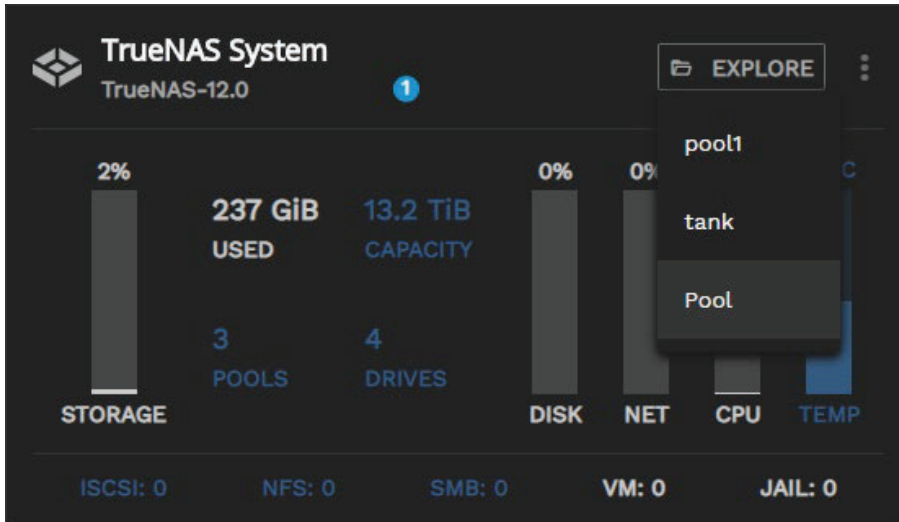
TrueNAS-12.0-INTERNAL-177



6.1.3 - TrueCommand Storage Management

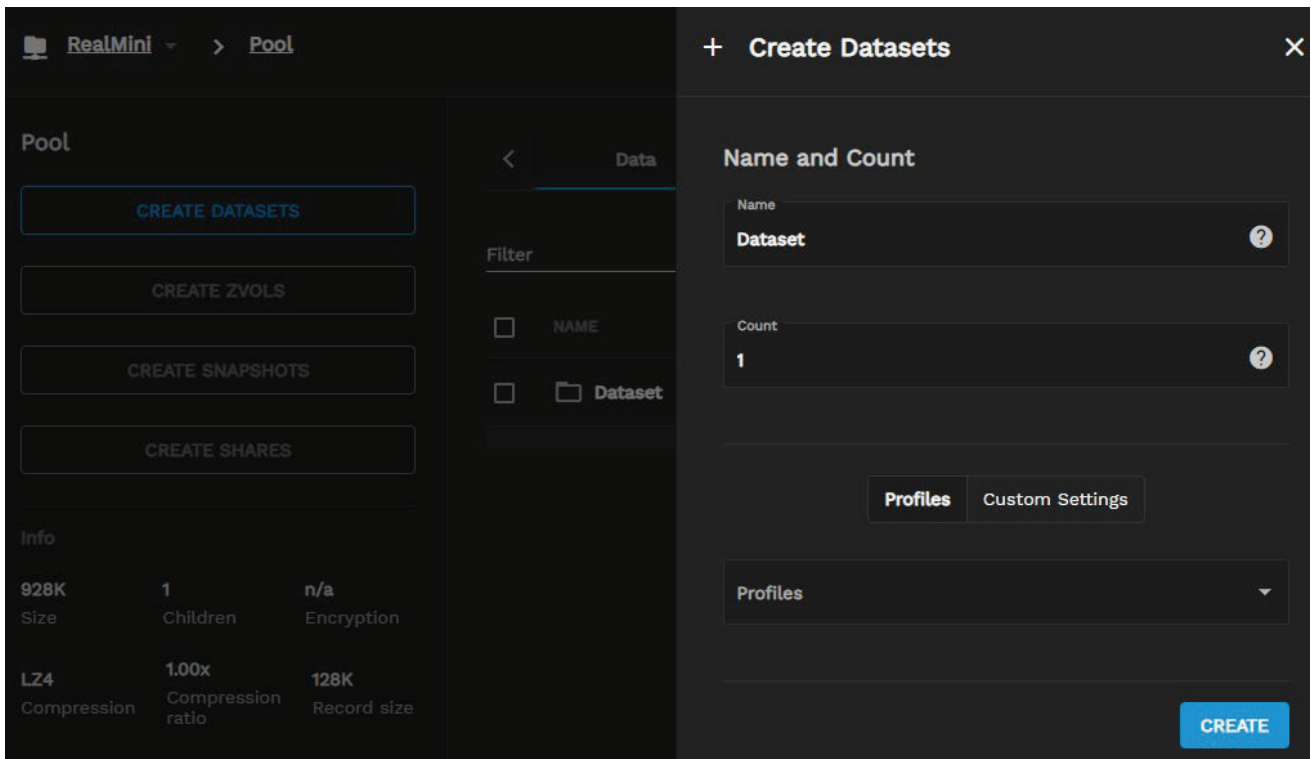
- [Adding a Dataset](#)
- [Adding a Zvol](#)
- [Deleting Storage](#)

To view, add, and delete storage from a single system in TrueCommand, click *EXPLORE* in that system's window, then select the pool you want to work with.



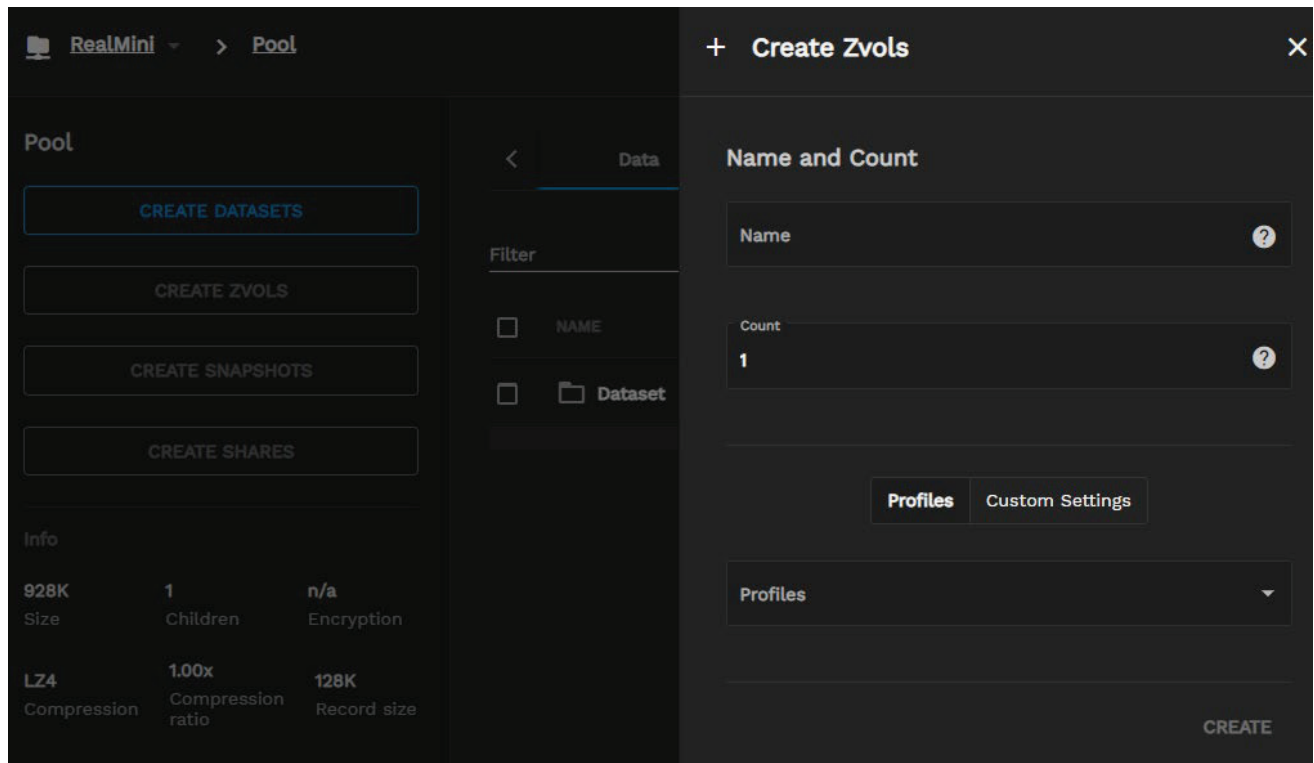
Adding a Dataset

1. In the pool's menu, click *CREATE DATASET*.
2. Name the dataset(s) and set how many you want to create.
3. Select a user-defined configuration profile or apply custom settings to the dataset(s), then click *CREATE*.



Adding a Zvol

1. In the pool's menu, click *CREATE ZVOLS*.
2. Name the zvol(s) and set how many you want to create.
3. Select a user-defined configuration profile or apply custom settings to the dataset(s), then click *CREATE*.



Deleting Storage

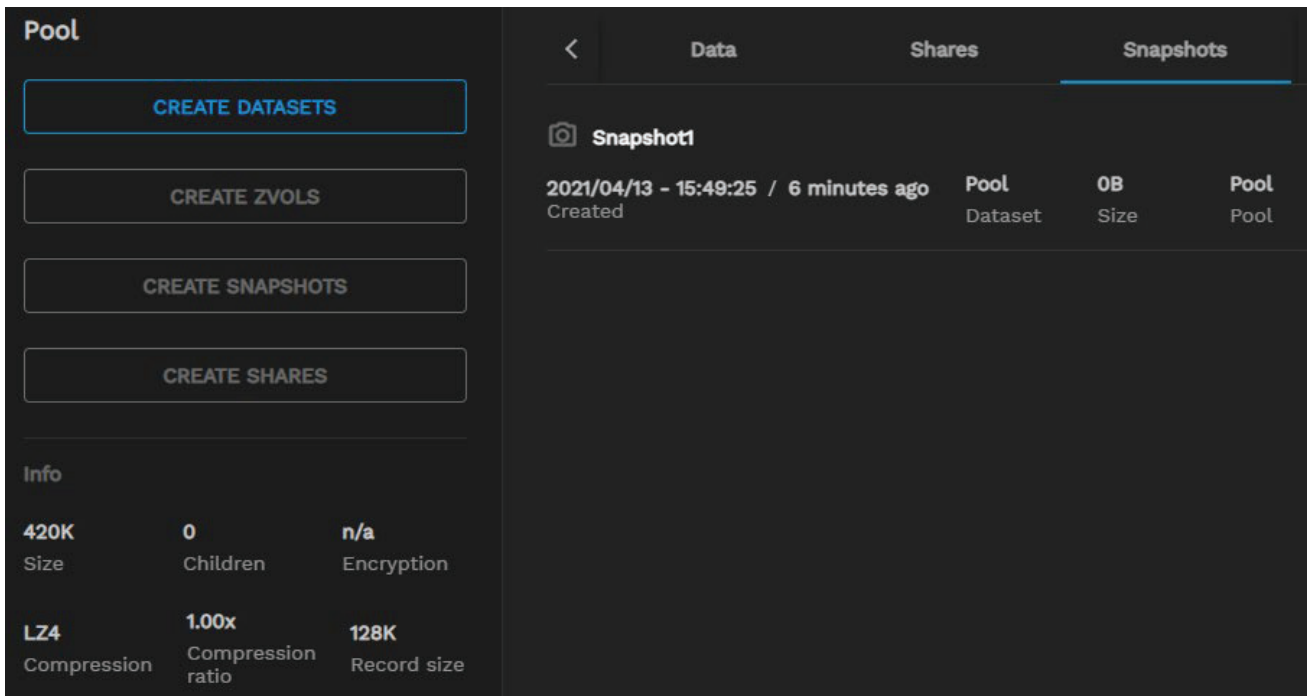
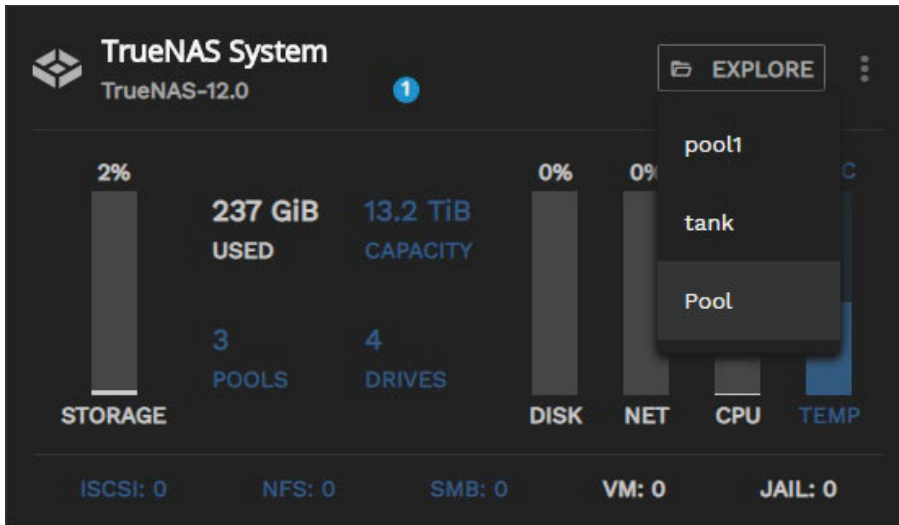
1. In the pool's menu, select the *Data* tab.
2. Check the boxes next the each item you want to delete, then click *DELETE*.
 - Alternatively, you can click the three dot menu button next to each item and select either *Delete Dataset Recursively* or *Delete Dataset*.
3. Click *CONFIRM* to delete the item(s).

6.1.4 - TrueCommand Snapshots

- - [View Snapshots](#)
 - [Create Single Snapshots](#)
 - [Create Recurring Snapshot Tasks](#)
 - [Timezones](#)

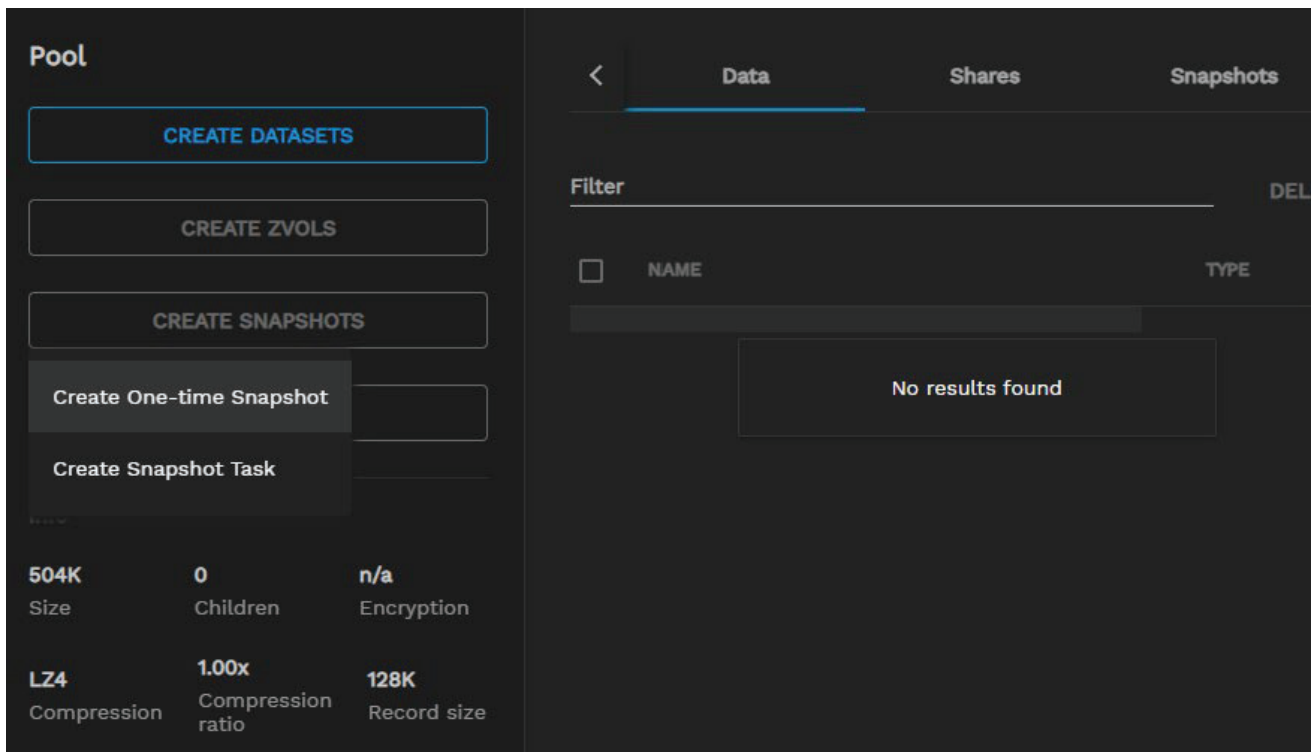
View Snapshots

To view a system's already existing snapshots, click *EXPLORE* in that system's window and select a storage pool. Once the pool loads, select the *Snapshots* tab.



Create Single Snapshots

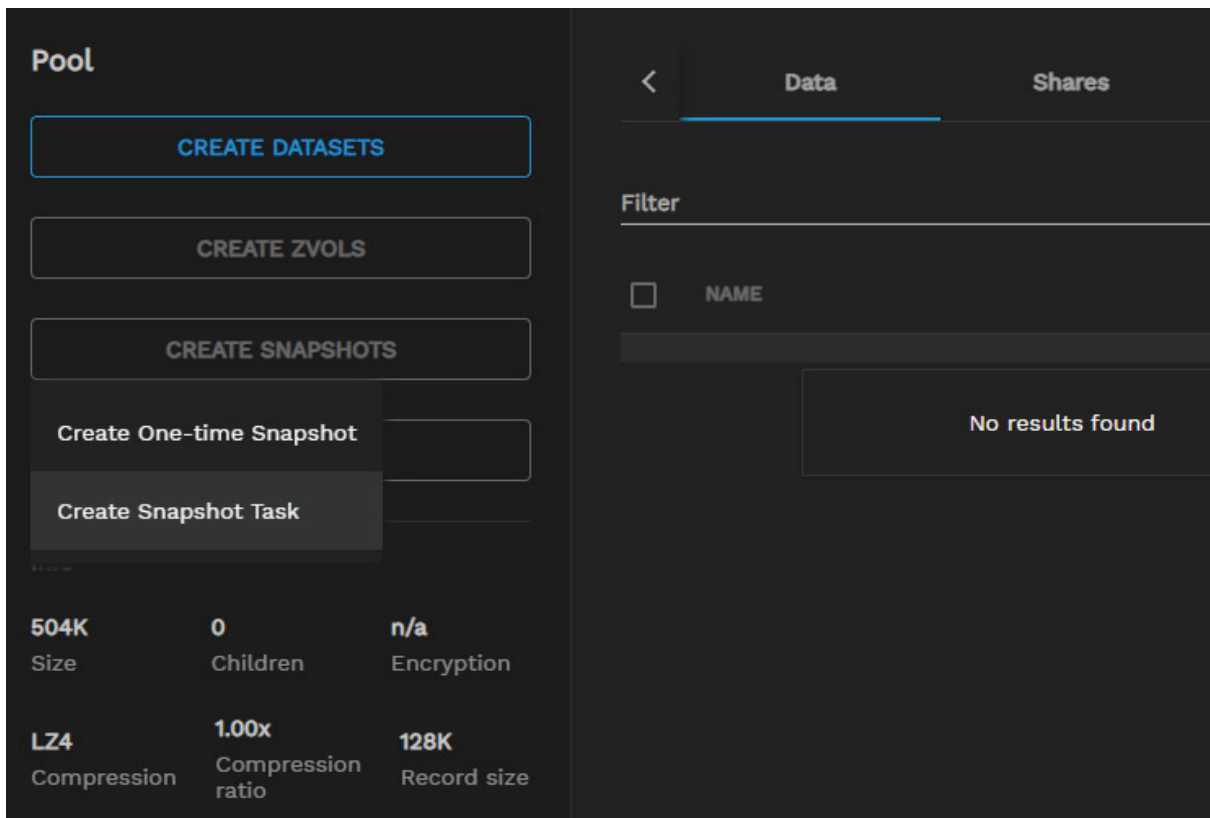
To create single snapshots, select a pool in the system's *EXPLORE* menu and click *CREATE SNAPSHOTS*, then select *Create One-Time Snapshot*.



Name the snapshot and click *CONFIRM*.

Create Recurring Snapshot Tasks

To create recurring snapshot tasks, select a pool in the system's *EXPLORE* menu and click *CREATE SNAPSHOTS*, then select *Create Snapshot Task*.



Set the task's schedule and determine the snapshot lifetime, then click *CONFIRM*.

Timezones

When you create snapshot tasks, TrueCommand uses the system the dataset is mounted in to determine what timezone it will use.

For example, if you are in New York and the dataset is mounted to a system with a Los Angeles timezone, a snapshot task set to occur at 12:00 P.M. will actually occur at 3:00 P.M. your time.

To see what timezone a system is in, go to that system's UI and navigate to **System > General (System Settings > General** in SCALE).

That system's timezone information is in the *Localization* section. Administrators can change the system's timezone using the drop-down menu.

The screenshot shows the TrueCommand GUI's 'System Settings' page, specifically the 'Localization' section. The 'GUI' section at the top includes fields for 'GUI SSL Certificate *' (freenas_default), 'Web Interface IPv4 Address *' (0.0.0.0), 'Web Interface IPv6 Address *' (::), 'Web Interface HTTP Port' (80), 'Web Interface HTTPS Port' (443), 'HTTPS Protocols' (TLSv1, TLSv1.1, TLSv1.2, TLSv1.3), and a checkbox for 'Web Interface HTTP -> HTTPS Redirect'. The 'Localization' section contains 'Language' (English), 'Console Keyboard Map', 'Sort languages by' (Name selected), 'Date Format' (2021-06-07), 'Timezone' (America/Los_Angeles), and 'Time Format' (11:36:07 (24 Hours)). A dropdown menu for 'Timezone' is open, showing a list of options including Africa/Windhoek, America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Araguaina, and America/Argentina/Buenos_Aires. The 'Other Options' section has checkboxes for 'Crash reporting' and 'Usage collection', both of which are checked. At the bottom, there are four buttons: 'SAVE', 'SAVE CONFIG', 'UPLOAD CONFIG', and 'RESET CONFIG'.

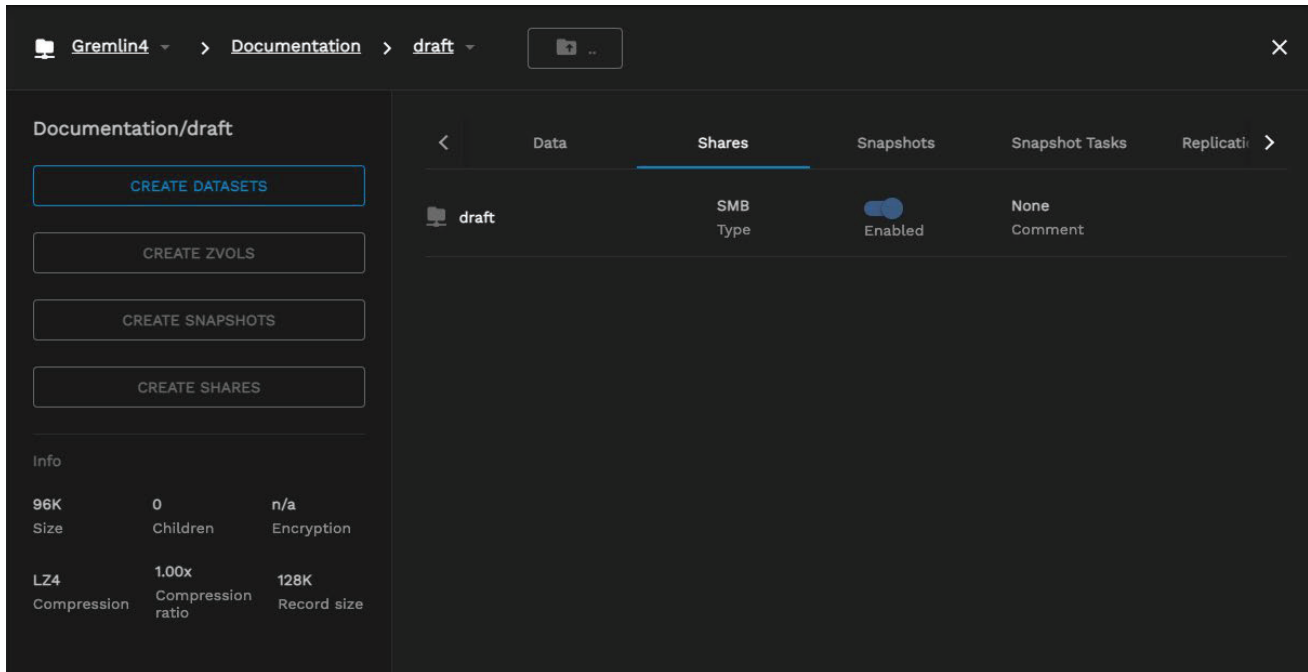
6.1.5 - TrueCommand Sharing

- - [View Existing Shares](#)
 - [Add NFS Shares](#)
 - [Add SMB Shares](#)

View Existing Shares

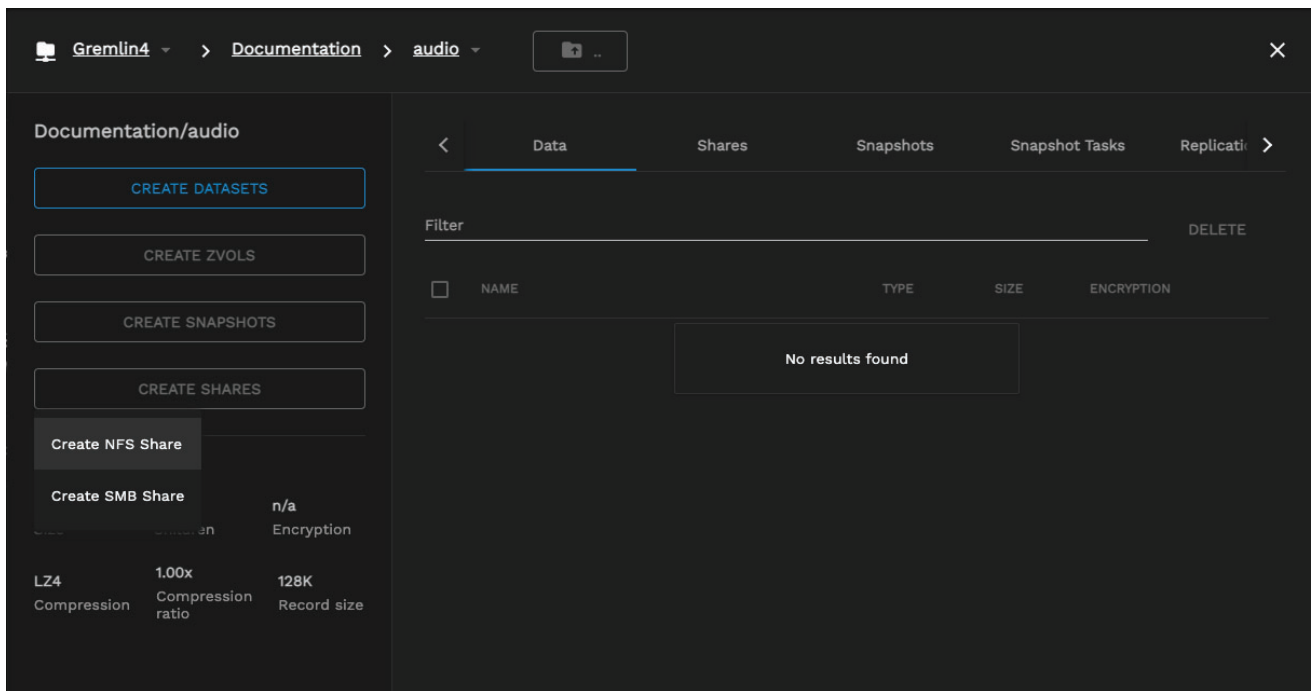
To view existing shares for a pool, click **EXPLORE** in your system window, then select the pool.

After the pool datasets load, click the dataset being shared, then click the **Shares** tab to view the existing shares.



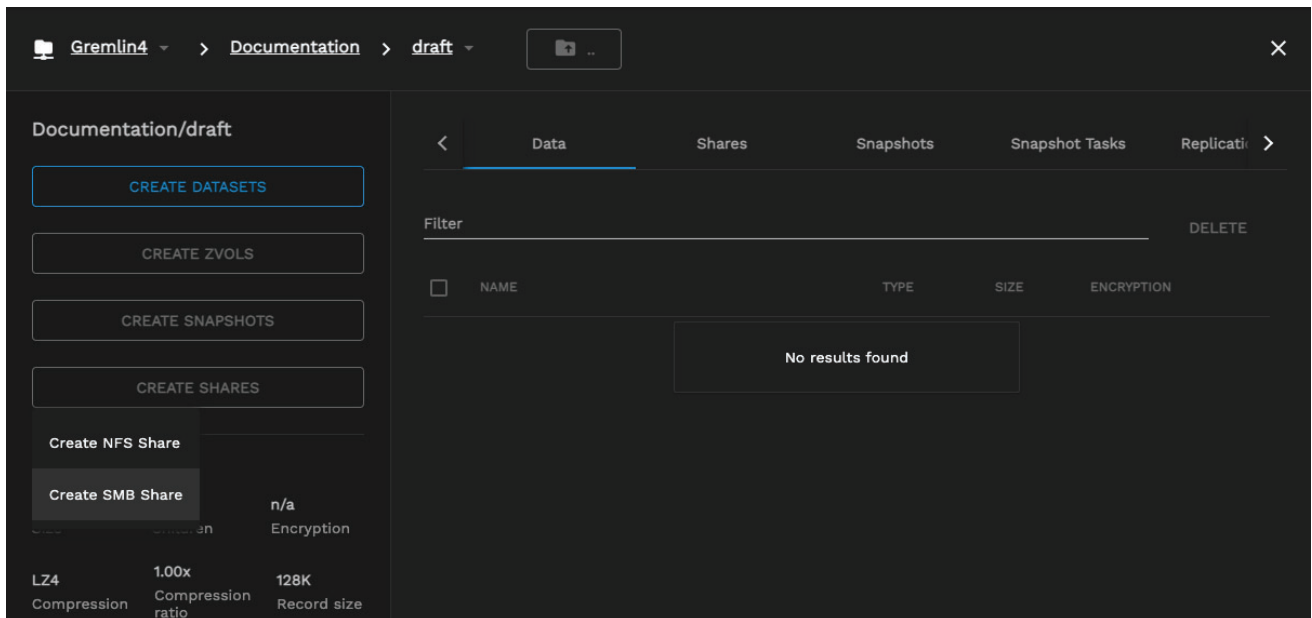
Add NFS Shares

To add an NFS share to a pool, open the pool using the **EXPLORE** menu in your system window. Once the pool datasets load, click on the dataset you want share. Click **CREATE SHARE** and select **Create NFS Share**.



Add SMB Shares

To add an SMB share to a pool, open the pool using the **EXPLORE** menu in your system window then select the pool. After the pool loads, select the dataset you want to share and then click **CREATE SHARE** and select **Create SMB Share**.



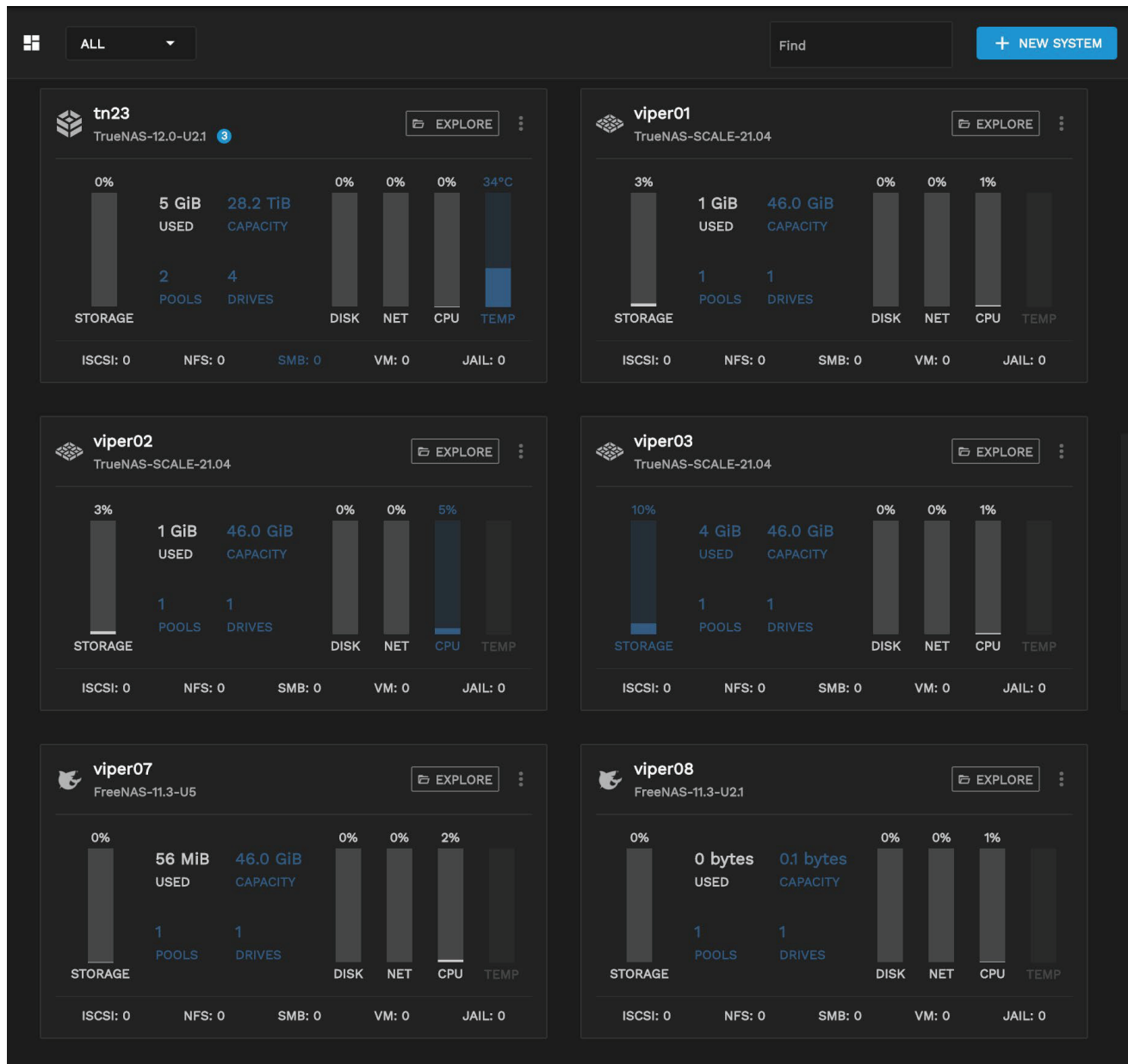
6.2 - TrueNAS Configuration File Management

TrueCommand automatically backs up the TrueNAS configuration every 24 hours and any time users make database changes or TrueCommand audit log entries.

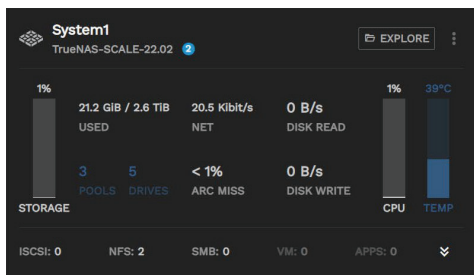
Users can create manual backups as needed.

Viewing Backups

To view the current TrueNAS configuration backups, open the **Dashboard**.



Click on the system name of a TrueNAS server to open the single system view.



Click the **Config Backups** button to open the config backup window.

The **Configuration Backup** window displays a list of backups along with the time and date of their creation.

Create a Config Backup

To create a new backup, click **Create Backup**.

tn23 > Config Backups

CREATE BACKUP

Filter

DELETE SELECTED

<input type="checkbox"/>	DATE	VERSION	ACTIONS
No results found			

A maximum of one config backup per day can exist.

If a prior config backup for the current day exists, creating a new one overwrites the previous one.

By default, TrueCommand retains seven backups. You can increase or decrease the number on the **Administration** page **Configuration** tab. Local instances of TrueCommand can increase or decrease this figure as desired.

Apply a Config Backup



To reset a TrueNAS system to a previous configuration, click the **history** icon. Choose the configuration file to use. You must reset the TrueNAS system to apply the configuration changes.

tn23 > Config Backups

CREATE BACKUP

Filter

DELETE SELECTED

<input type="checkbox"/>	DATE	VERSION	ACTIONS
<input type="checkbox"/>	2021/04/08 - 14:20:41	TrueNAS-12.0-U2.1	 

Delete a Config Backup

To delete a backup, click the delete ~~delete~~ icon or mark the checkbox and click **Delete Backups**.

Confirm

Are you sure you want to delete this database?

CANCEL

CONFIRM

6.3 - Multiple Systems

- - [Config Management](#)
 - [System Inventory](#)
 - [iSCSI Management](#)
 - [Cluster Management](#)

TrueCommand has several multisystem management capabilities with more in development for future releases.

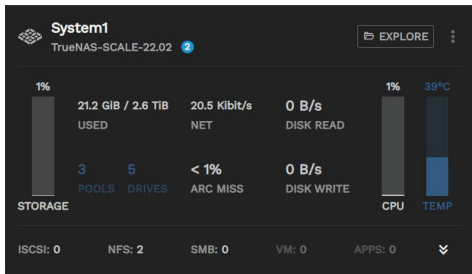
TrueCommand 2.0 added cluster capability. It can also apply TrueNAS configurations to multiple systems at once.

Config Management

TrueCommand can manage TrueNAS [Config files](#). TrueCommand can also restore a single config file to multiple systems.

To apply a config to multiple systems, you must first create a config backup from the TrueNAS system with the settings you want to apply to other TrueNAS units.

Click on the system name for a TrueNAS server to open the single system view.



Click **Config Backups** to open the **Config Backup** window.

The **Configuration Backup** window displays a list of backups with their creation times and dates.


Set the checkbox for the config to restore and click the **restore** **Restore** icon.

<input type="checkbox"/>	DATE	VERSION	ACTIONS
<input checked="" type="checkbox"/>	2021/05/17 - 19:09:42	TrueNAS-SCALE-21.05-MASTER-20210506-052858	
<input type="checkbox"/>	2021/05/18 - 12:10:09	TrueNAS-SCALE-21.05-MASTER-20210506-05...	

Click **ADD SYSTEM** to select a system that the config file restores.

Restore System Config

Select one or more systems to restore to config **TrueNAS-SCALE-21.05-MASTER-20210506-052858** created on system **hydra027.ds.ixsystems.net** on **2021-05-17**. The selected systems will go offline during the restoration process.

 No systems selected.

ADD SYSTEM

CANCELCONFIRM

You can add more servers as needed.

Restore System Config

Select one or more systems to restore to config **TrueNAS-SCALE-21.05-MASTER-20210506-052858** created on system **hydra027.ds.ixsystems.net** on **2021-05-17**. The selected systems will go offline during the restoration process.



No systems selected.

ADD SYSTEM

CAN

hydra029.ds.ixsystems.net

hydra030.ds.ixsystems.net

hydra028.ds.ixsystems.net

hydra027.ds.ixsystems.net

Click **CONFIRM** to upload the config backup to the chosen TrueNAS systems.

Restore System Config

Select one or more systems to restore to config **TrueNAS-SCALE-21.05-MASTER-20210506-052858** created on system **hydra027.ds.ixsystems.net** on **2021-05-17**. The selected systems will go offline during the restoration process.

Name

hydra030.ds.ixsystems.net



hydra029.ds.ixsystems.net



hydra028.ds.ixsystems.net



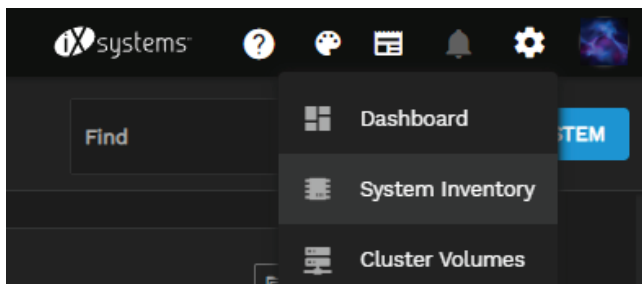
ADD SYSTEM

CANCEL

CONFIRM

System Inventory

To access the **System Inventory** page, click the **Settings** icon and select **System Inventory**.



To download a comma-delimited CVS file for the current inventory page, click **CVS** in the upper-right area of the screen.

There are three inventory information tabs:


⦿ System

The **System** tab provides information on the **Manufacturer**, the controllers' **Serial** numbers, the system **Support Tier**, the support Contract expiration date, the active controller **Hostname**, the **CPU**, the number of **CPU Cores**, the amount of **Physical Memory**, what **OS** the system is running, and the **Uptime**.

Filter

< tn13

System Network Storage



TRUENAS-X10-MODEL-HA

Manufacturer	iXsystems
Serial (active)	[REDACTED]
Serial HA (standby)	[REDACTED]
Support Tier	GOLD
Support Expiration	in 6 months (2022-03-02)
Hostname	tn13a [REDACTED]
CPU	Intel(R) Xeon(R) CPU D-1531 @ 2.20GHz
CPU Cores	12
Physical Memory	32 GiB
OS	TrueNAS-12.0-U5.1
Uptime	1 wk, 1 d

○ Network

The **Network** tab provides information about the **Interface** names, **Type**, **Link State** and **MAC** address.

Filter

< tn13

System Network Storage

Default Routes

10. [REDACTED]

Nameservers

10. [REDACTED]

10. [REDACTED]

10. [REDACTED]

Interfaces CSV

NAME	TYPE	LINK STATE	MAC
> igb0	PHYSICAL	LINK_STATE_UP	[REDACTED]
> igb1	PHYSICAL	LINK_STATE_UP	[REDACTED]

○ Storage

The **Storage** tab provides information about the **Drives**, such as **Name**, **Type**, **Size**, **Model**, **Serial** number, and **Enclosure** location.

tn13

System

Network

Storage

Drives

Filter

NAME

TYPE

SIZE

MODEL

SERIAL

ENCLOSURE

da0	HDD (7200 RPM)	1.82 TiB	TOSHIBA MK2001TRKB		0 slot 2
ada0	SSD	119.24 GiB	SanDisk SD8SN8U128G1122		
da1	HDD (7200 RPM)	1.82 TiB	TOSHIBA MK2001TRKB		0 slot 3
da2	HDD (7200 RPM)	1.82 TiB	TOSHIBA MK2001TRKB		0 slot 4
da3	HDD (7200 RPM)	3.64 TiB	HGST HUS724040ALS640		0 slot 1
da4	HDD (7200 RPM)	3.64 TiB	HGST HUS724040ALS640		0 slot 5
da5	HDD (7200 RPM)	3.64 TiB	HGST HUS724040ALS640		0 slot 6
da6	HDD (7200 RPM)	3.64 TiB	HGST HUS724040ALS640		0 slot 7
da7	SSD	3.49 TiB	SEAGATE XS3840TE70014		0 slot 11
da8	HDD (7200 RPM)	3.64 TiB	HGST HUS724040ALS640		0 slot 8
da9	HDD (7200 RPM)	3.64 TiB	HGST HUS724040ALS640		0 slot 9
da10	HDD (7200 RPM)	3.64 TiB	HGST HUS724040ALS640		0 slot 10
da11	SSD	745.21 GiB	SEAGATE XS800LE70014		0 slot 12
da12	HDD (15000 RPM)	50.00 GiB	TrueNAS iSCSI Disk		

CSV

iSCSI Management

With TrueCommand, you can configure iSCSI volumes on multiple systems simultaneously. Refer to the [iSCSI section](#) for more information.

Cluster Management

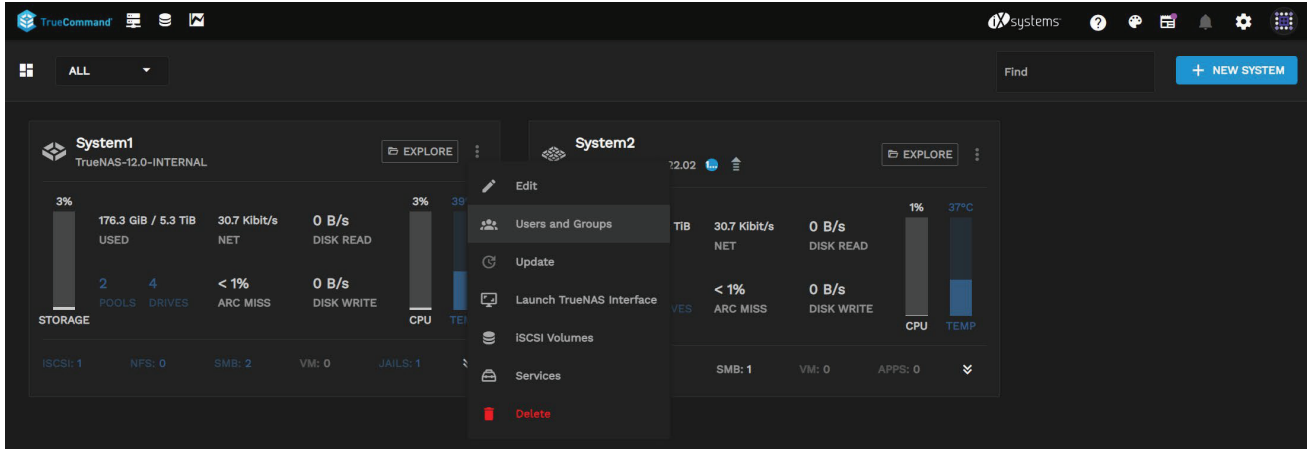
By definition, clusters span across multiple systems. TrueCommand instances with three or more connected TrueNAS SCALE systems can create clustered volumes. Refer to the [Clustering section](#) for more information.

6.4 - NAS Users and Groups

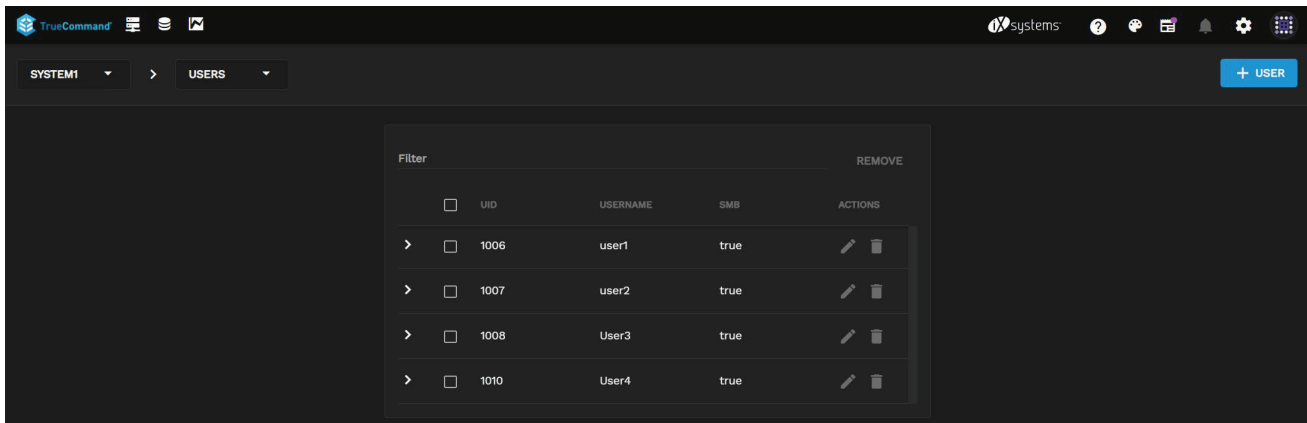
TrueCommand lets you create NAS users and groups across multiple systems.

NAS Users

Adding a New User

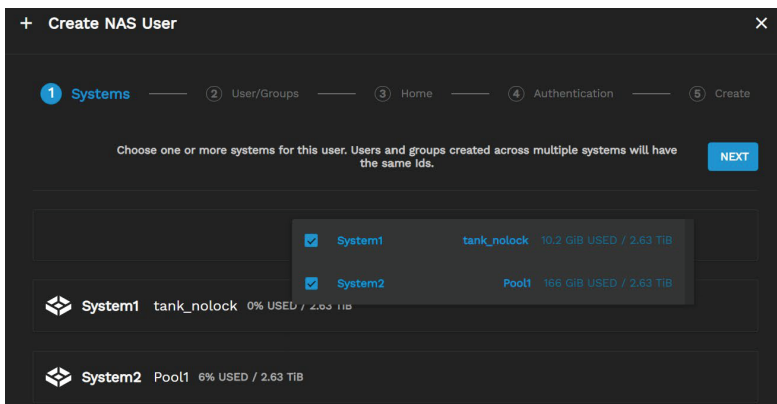


To add a NAS user to one or more systems, go to the dashboard and click the **more_vert** in a system window, then select **Users and Groups**.



Click **+ User** to open the user creation wizard.

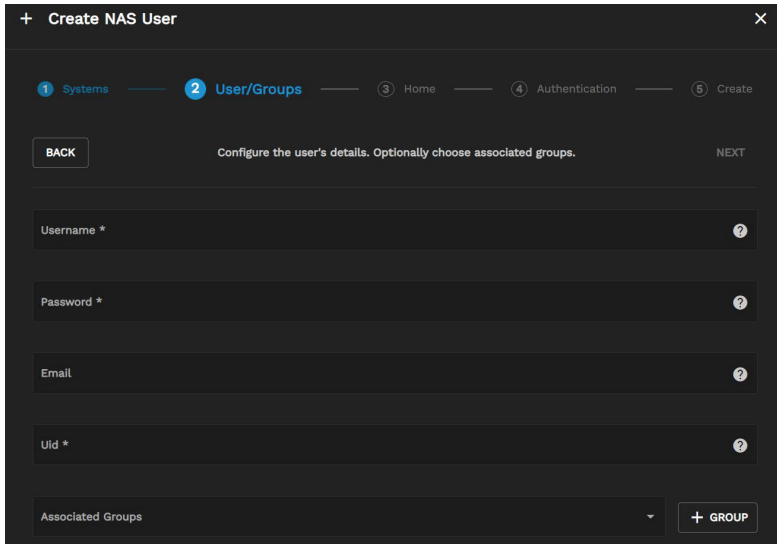
⌕ Systems



You can add users to one or several TrueNAS systems. Click **+ Add System** and select one or more systems,

then click **NEXT**. Users and groups created across multiple systems will share IDs.

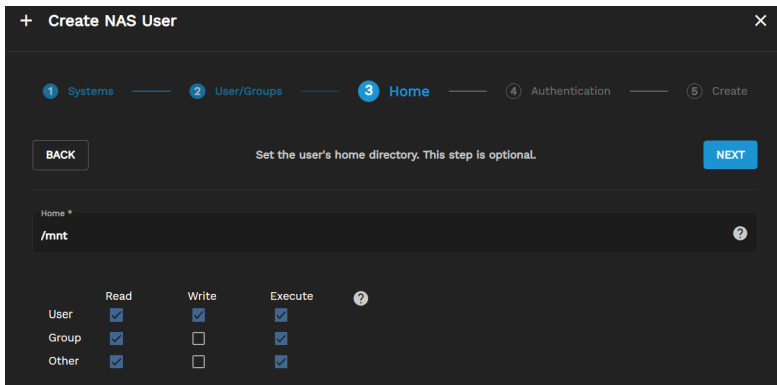
○ User/Groups



Enter a **Username**, **Password**, **Email** (optional), and **Uid** (user ID). You can also associate the user with existing groups or create new ones using the **+ GROUP** button (optional).

Once you are finished, click **NEXT**.

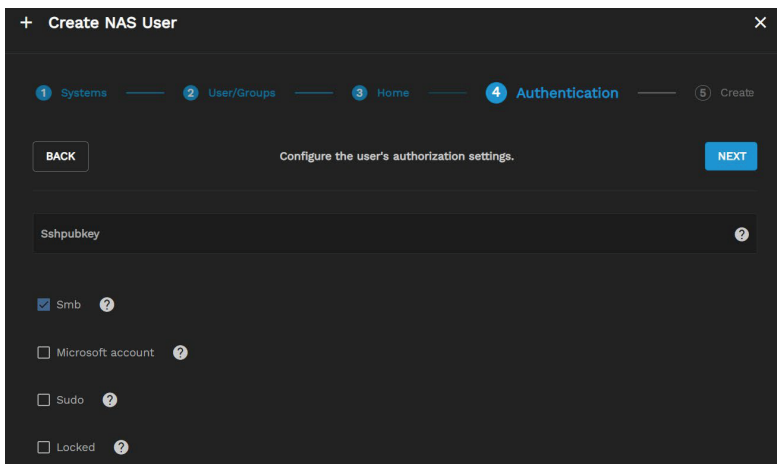
○ Home



	Read	Write	Execute
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Other	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

If you want the user to have a home directory, enter the path to the directory and set the default UNIX permissions, then click **NEXT**.

○ Authentication



You can enter or paste the user public SSH key in the **Sshpubkey** field.

You can also allow users to authenticate with Samba, connect from a Windows machine with their Microsoft account, and use sudo commands.

Check **Locked** to prevent users from logging in or using password-based services.

After configuring the user authorization settings, click **NEXT**.

☐ **Create**

Systems		
System1	tank_nolock	10.2 GiB% Used / 2.63 TiB
System2	Pool1	166 GiB% Used / 2.63 TiB

Review the settings. If you are satisfied, click **CREATE**. You can also click **BACK** to edit their settings again before finishing.

Managing Users

To manage NAS user accounts, go to your dashboard and click the **more_vert** in a system's window, then select **Users and Groups**.

To edit a user, click the **edit** in that user's row.

To delete a single user, click the **delete** in that user row.

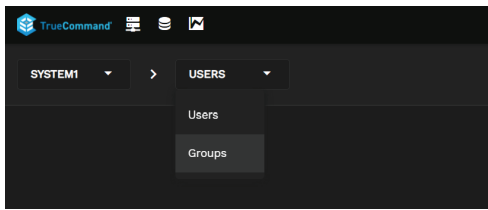
To delete multiple users, check them and click **REMOVE**.

Filter	UID	USERNAME	SMB	ACTIONS
<input type="checkbox"/>	1006	user1	true	
<input type="checkbox"/>	1007	user2	true	

NAS Groups

Adding a New Group

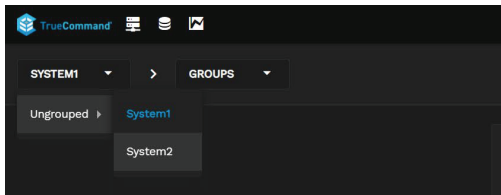
Go to the dashboard and click the **more_vert** in a system card and select **Users and Groups**, then click the **USERS** drop-down and select **GROUPS**.



Enter a **Gid** and a **Name**, then select **Smb** and **Sudo** permissions.

Click **SAVE** to create the group.

If you want to add groups to other systems, switch to them using the system drop-down.



Managing Groups

To manage NAS user accounts, go to your dashboard and click the **more_vert** in a system's window, then select **Users and Groups**.

To edit a group, click the **edit** in that group's row.

To delete a single group, click the **delete** in that group's row.

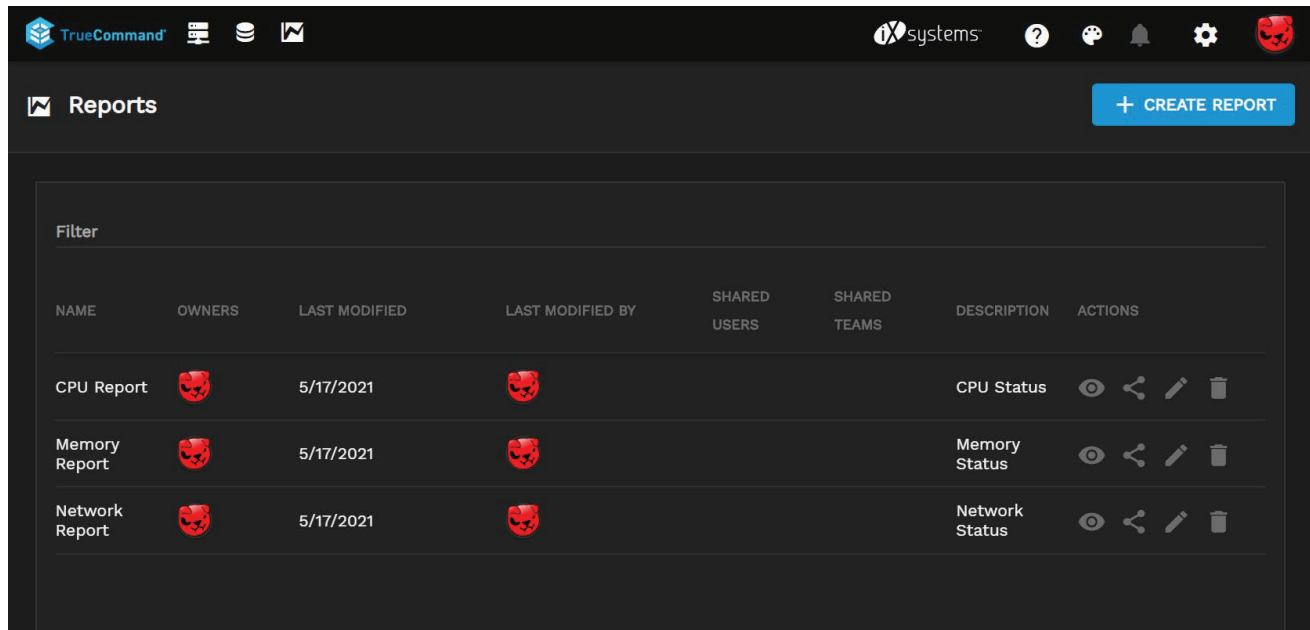
To delete multiple groups, check every group you want to delete and click **REMOVE**.

	GID	GROUP	SMB	ACTIONS
>	1011	group1	true	
>	1012	group2	true	
>	1013	group3	true	

7 - Reports

TrueCommand users can create reports and share them with other TrueCommand users. We designed default reports that generate a basic system overview chart. Default reports show details like network traffic, storage, and the chosen system's memory utilization.

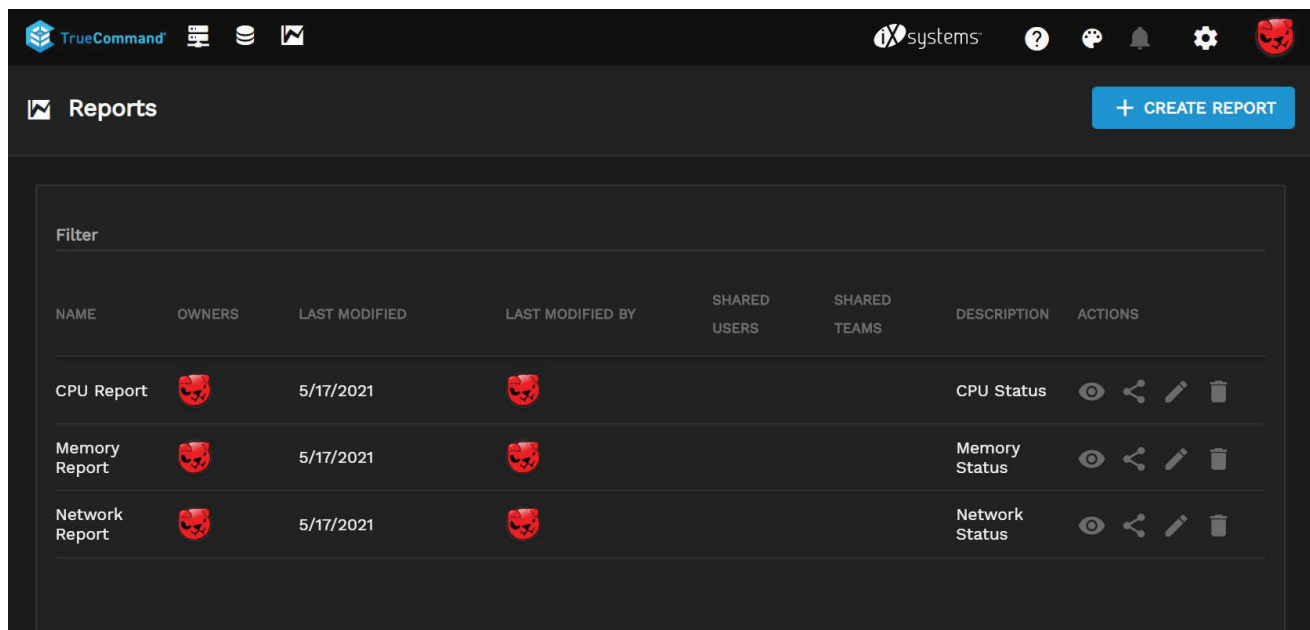
Users must have access to the analyzed systems to view their reports.



7.1 - Creating a Report

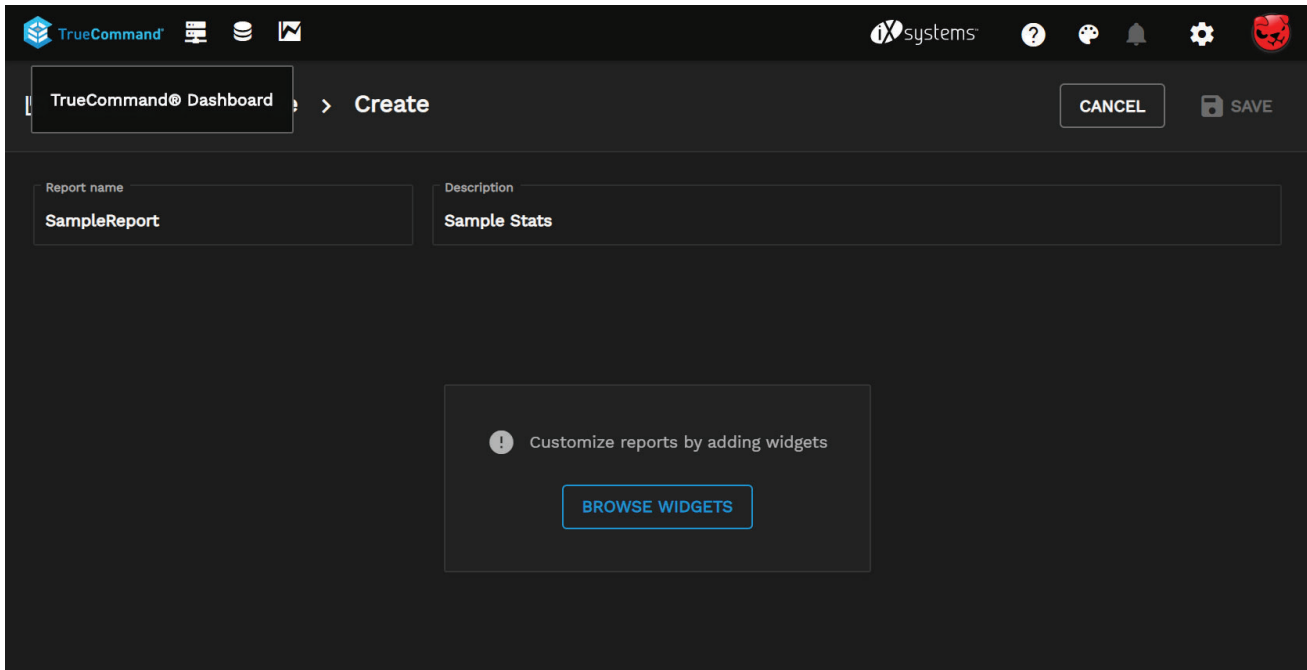
- - [Creating a Report](#)
 - [Custom Charts](#)
 - [Edit a Report](#)
 - [Share Report](#)
 - [Delete a Report](#)

The **Reports** page customizes system metrics charts for data analysis.



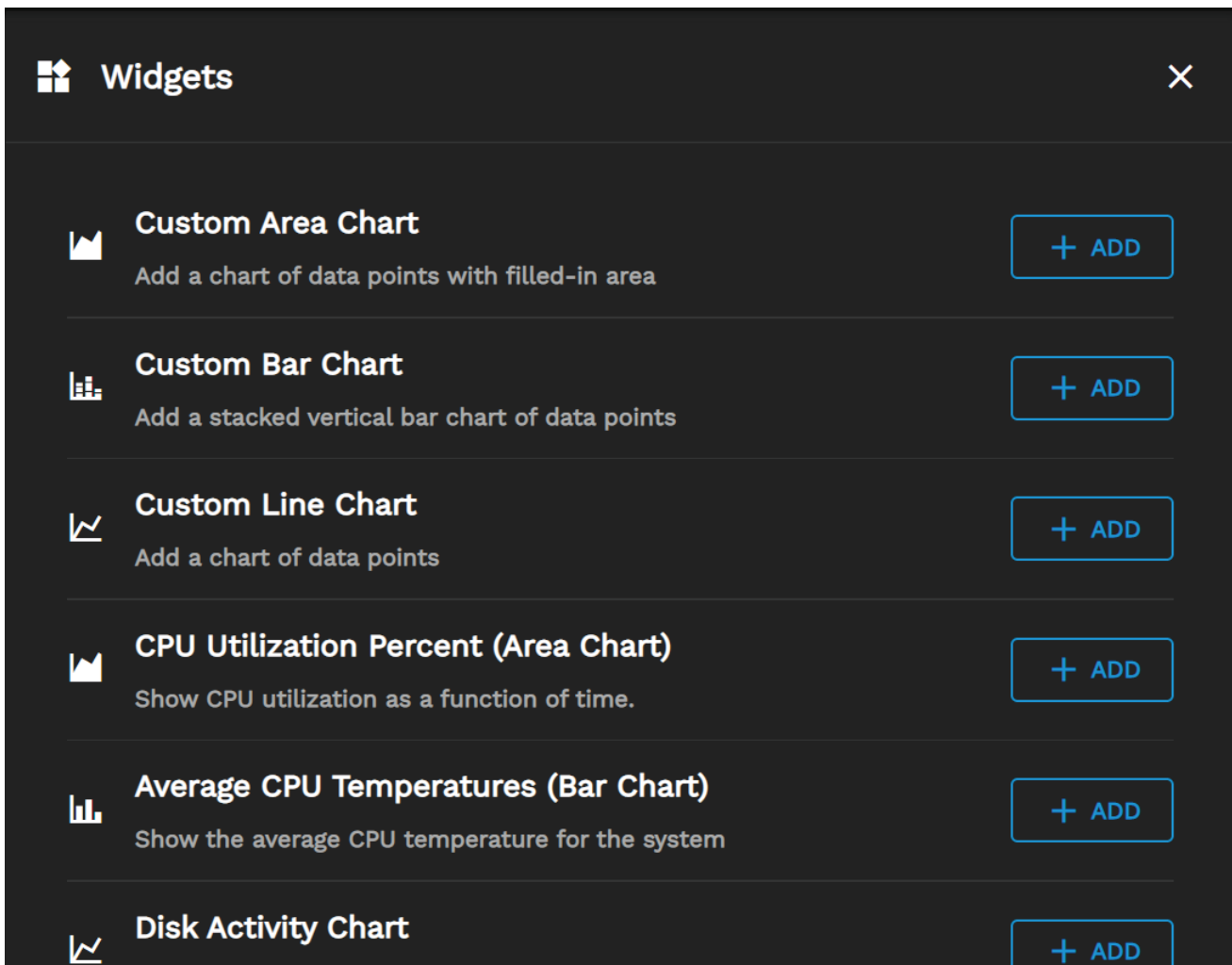
Creating a Report

Click **+ CREATE REPORT** to create a customizable report. Give the report a name and an optional description.



The screenshot shows the 'Create' report interface in TrueCommand. At the top, there's a breadcrumb 'TrueCommand® Dashboard > Create' and buttons for 'CANCEL' and 'SAVE'. Below this, there are two input fields: 'Report name' with the value 'SampleReport' and 'Description' with the value 'Sample Stats'. In the center, there is a message box with an exclamation mark icon, the text 'Customize reports by adding widgets', and a button labeled 'BROWSE WIDGETS'.


Click **BROWSE WIDGETS** or **WIDGET** to add charts to the report.



The screenshot shows a 'Widgets' modal window with a close button (X) in the top right. It lists six widget options, each with an icon, a title, a description, and an '+ ADD' button:


- Custom Area Chart**: Add a chart of data points with filled-in area.
- Custom Bar Chart**: Add a stacked vertical bar chart of data points.
- Custom Line Chart**: Add a chart of data points.
- CPU Utilization Percent (Area Chart)**: Show CPU utilization as a function of time.
- Average CPU Temperatures (Bar Chart)**: Show the average CPU temperature for the system.
- Disk Activity Chart**

Show disk activity as a percentage of capabilities.

**Memory Utilization Percent (Area Chart)**


+ ADD

Show memory utilization of system as a function of time.

**Network Traffic Chart**


+ ADD

Chart of network traffic

**Network Device Chart (Download)**


+ ADD

Monitor network traffic per adapter

**Network Device Chart (Upload)**


+ ADD

Monitor network traffic per adapter

**Storage Utilization Chart**

+ ADD

Track storage used over time

**Storage Pool Utilization Chart**

+ ADD

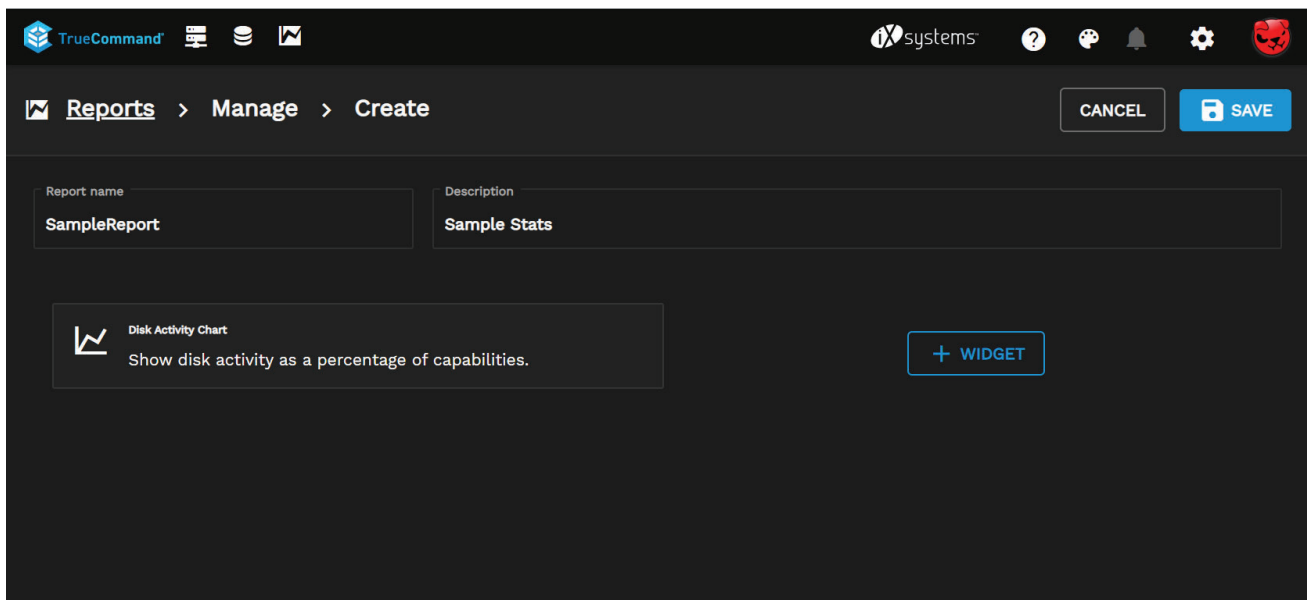
Track storage used per-pool over time

Custom Charts

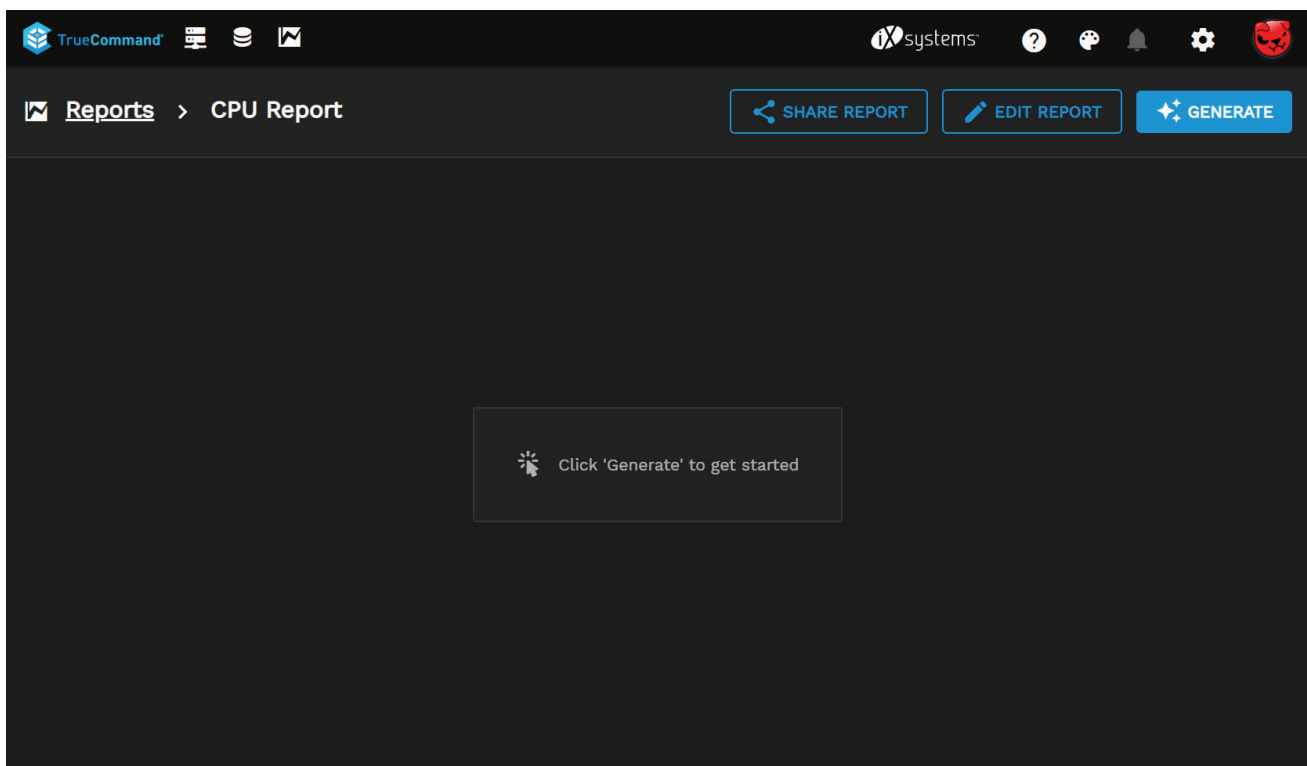
TrueCommand already configures most charts to report specific settings. To create a custom chart with custom settings, add a **Custom Area Chart**, **Custom Bar Chart**, or **Custom Line Chart**. Fill in the following options when adding a custom chart:

- General settings: Enter a Title, Subtitle (optional), Axis label (optional), Point size, Line size, Y min (optional), and Y max (optional) for the chart. You can set `Stack the values` to bring data points on the chart closer together. `Stack the values` is helpful for charts with many different data points at the max Y value.
- Data sources: Add data sources to the chart by expanding a category and selecting which sources you want. You can add multiple data sources to one chart.
- Summary: This step shows all chosen values. Click **SAVE** to add the custom chart to the report. Click **BACK** to change a setting or data source.

After adding charts to the report, click **SAVE** to make it available for use.



After creating a report, you can click **GENERATE** to [generate the report](#), or you can go back to the reports page and create another.

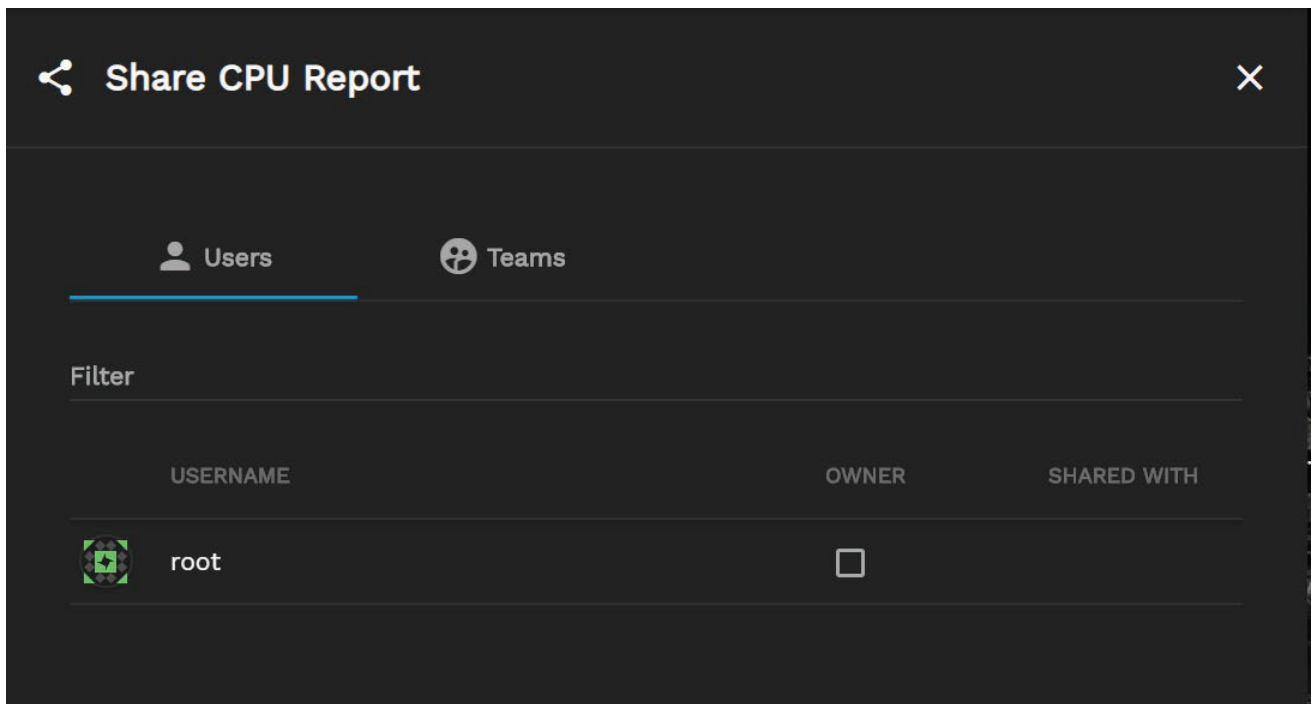


Edit a Report

Open the **Reports** page and click **edit** next to a report name to rename it, add a description, or add/delete a widget.

Share Report

By default, user-created reports are available only to that user. To share a report with other users or teams, open the **Reports** page and click the **share** icon for the chart.



You can share reports with individual users or entire teams.

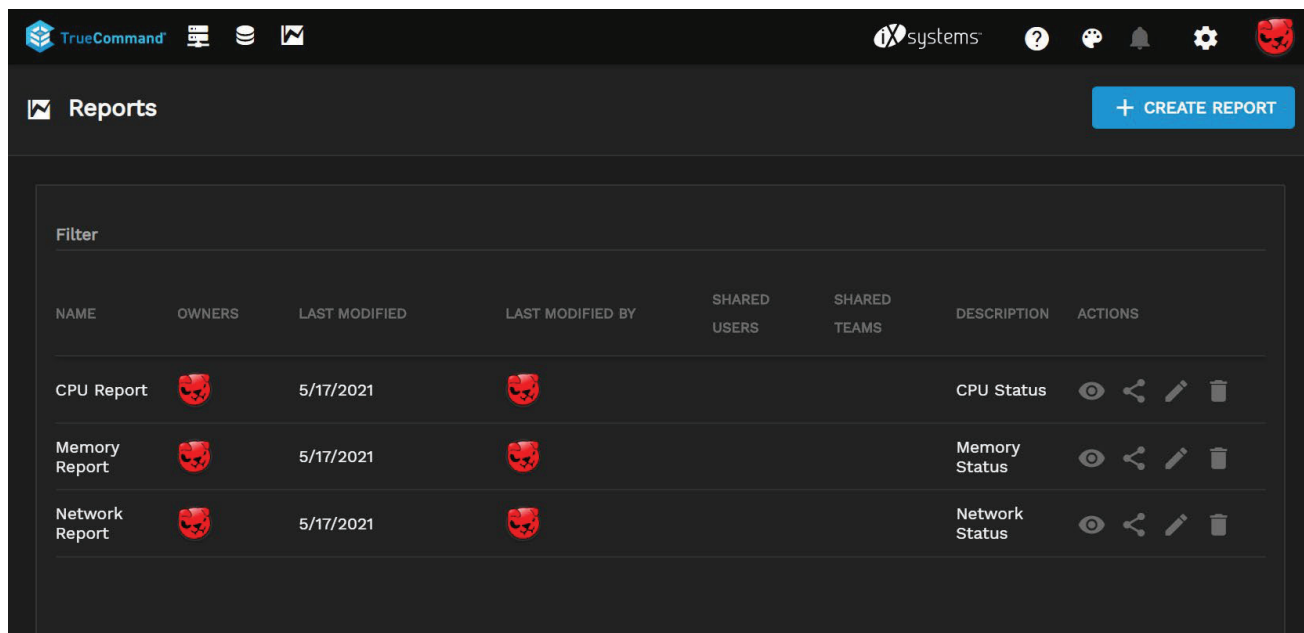
Delete a Report

To delete a report click **delete**. This permanently deletes the report but you can recreate it as needed.

7.2 - Generating a System Report

- - [Generating a report](#)

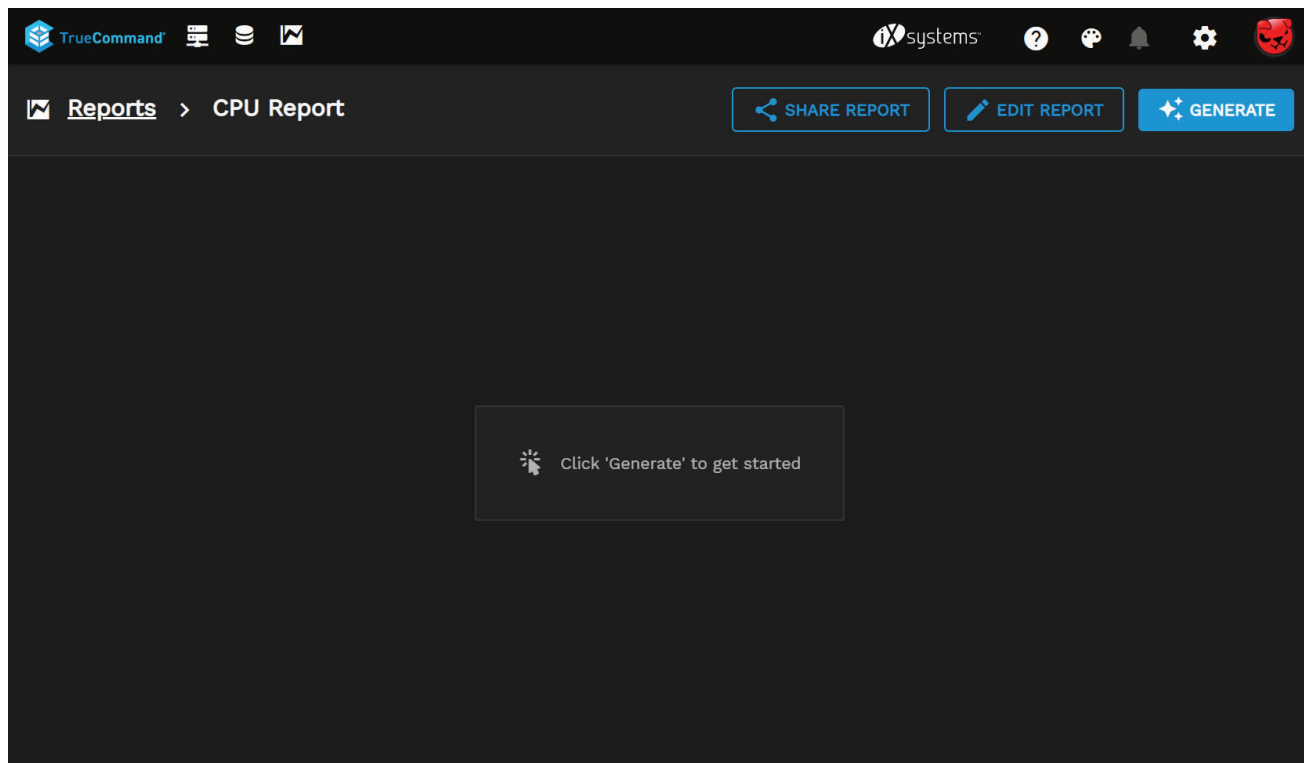
The **Reports** page customizes system metrics charts for data analysis.



You must [create a report](#) before you can run the report.

Generating a report

To generate a report click the `remove_red_eye` (eye) icon to launch the Generation Page.



Click **Generate** to open the date and system selection window.

Start date/time

5/18/2021, 7:56:36 AM

End date/time

5/18/2021, 8:56:36 AM

Systems

CANCEL

GENERATE

Select the report beginning and end dates using the drop-down.

Start date/time

5/18/2021, 7:56:36 AM

End date/time

5/18/2021, 8:56:36 AM

MAY 2021

<

>

Su

Mo

Tu

We

Th

Fr

Sa

MAY

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

07

:

56

AM

✓

GENERATE

After you set the date range, use the **systems** drop-down menu to select the systems you want to include in the report.

A dark-themed dialog box with a title bar. It contains two date/time fields at the top: 'Start date/time' with the value '5/17/2021, 7:56:36 AM' and 'End date/time' with the value '5/18/2021, 8:56:36 AM'. Below these are four system names, each preceded by a checkbox. The first two are 'hydra029.ds.ixsystems.net' and 'hydra030.ds.ixsystems.net', both with unchecked checkboxes. The next two are 'hydra028.ds.ixsystems.net' and 'hydra027.ds.ixsystems.net', both with checked checkboxes. The dialog box is slightly offset from the top-left corner of the screen.

Start date/time
5/17/2021, 7:56:36 AM

End date/time
5/18/2021, 8:56:36 AM

☐ hydra029.ds.ixsystems.net

☐ hydra030.ds.ixsystems.net

☒ hydra028.ds.ixsystems.net

☒ hydra027.ds.ixsystems.net

After you select the systems, click **Generate**

A dark-themed dialog box with a title bar. It contains two date/time fields at the top: 'Start date/time' with the value '5/17/2021, 7:56:36 AM' and 'End date/time' with the value '5/18/2021, 8:56:36 AM'. Below these is a text field containing the text 'hydra029.ds.ixsystems.net, hydra030.ds.ixsystems.net, hydr...' followed by a dropdown arrow. Below the text field is a label 'Systems'. At the bottom right are two buttons: 'CANCEL' and 'GENERATE'.

Start date/time
5/17/2021, 7:56:36 AM

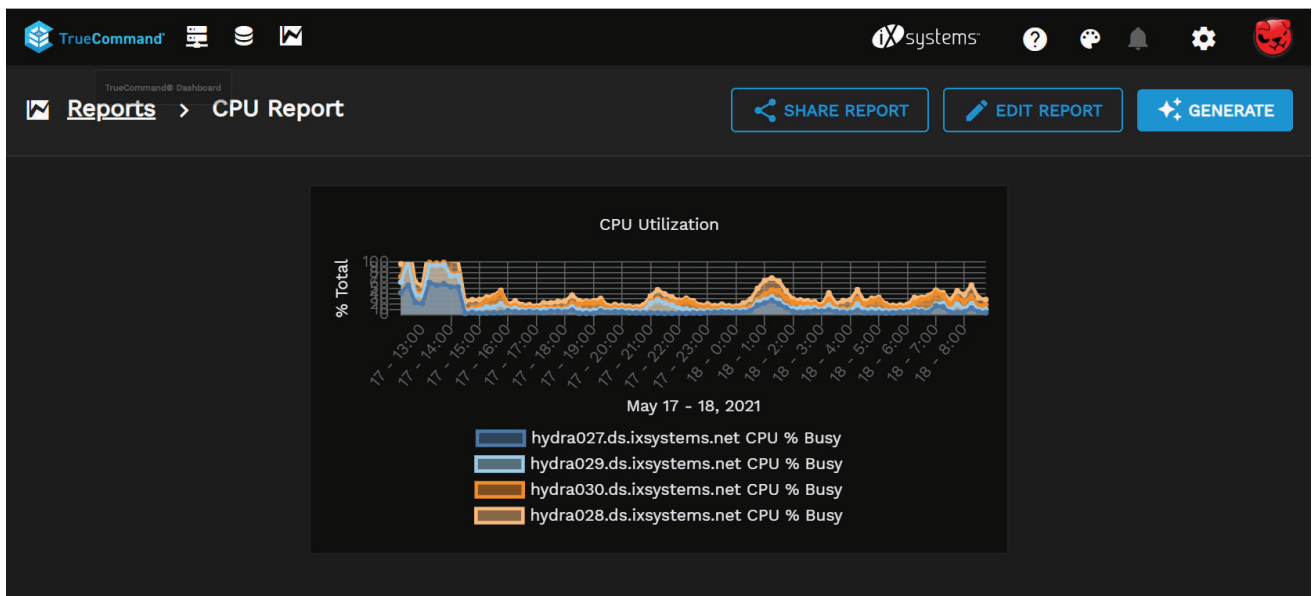
End date/time
5/18/2021, 8:56:36 AM

hydra029.ds.ixsystems.net, hydra030.ds.ixsystems.net, hydr... ▼

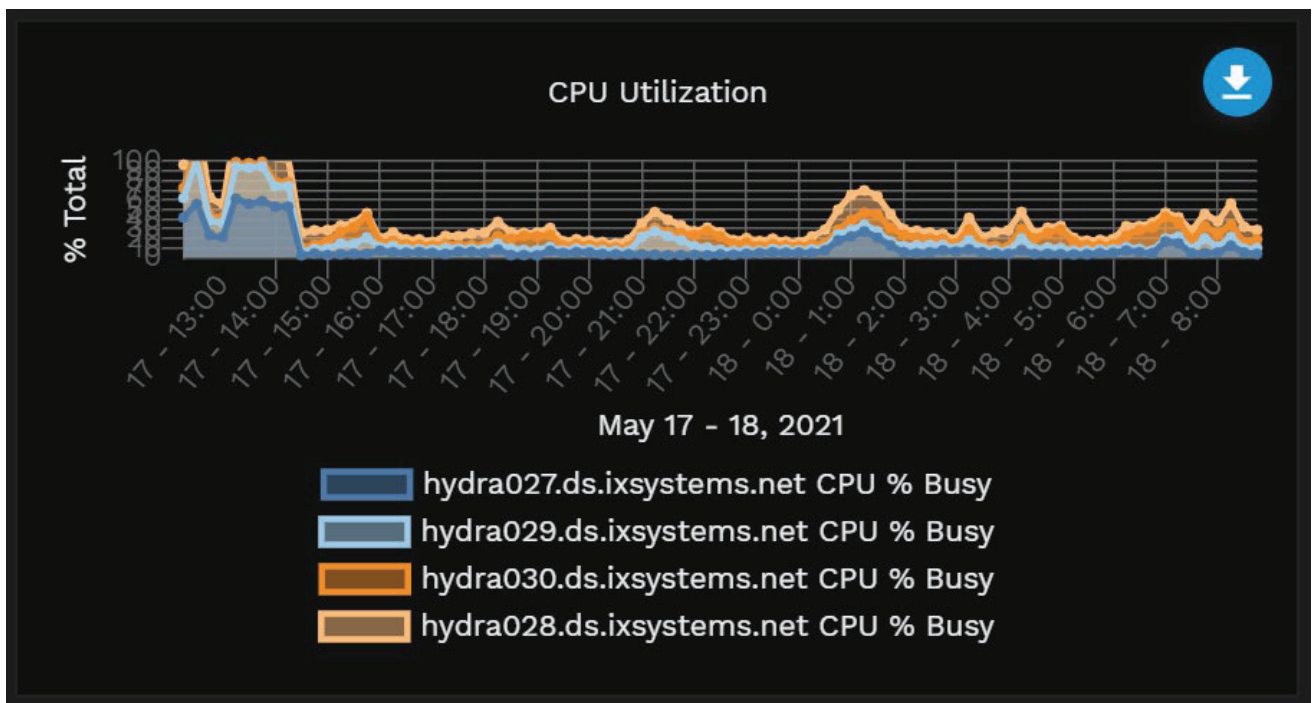
Systems

CANCEL GENERATE

The report generates, and the graph displays.



To download the report metrics in JSON format, hover your cursor over the report and click the blue down-arrow that displays.



8 - Alerts

TrueCommand allows for user notification based on custom defined alerts for connected TrueNAS systems. Method of alert notifications as well as theming of alerts in the TrueCommand interface can be user customized.

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.

8.1 - Alert Management

TrueCommand alerts provide visual warnings for monitored systems that require attention. Monitored systems and TrueCommand alert rules can both generate alerts.

TrueCommand provides three alert screen options:

- **All Alerts** displays all alerts from systems that TrueCommand monitors.
- **Alert Rules** allows administrators and users with permissions to configure alerts for monitored systems.
- **Alert Services** allows administrators to configure communication plugins.

The **All Alerts**, **Dashboard**, and **Systems** screens display alert indications.

🕒 All Alerts

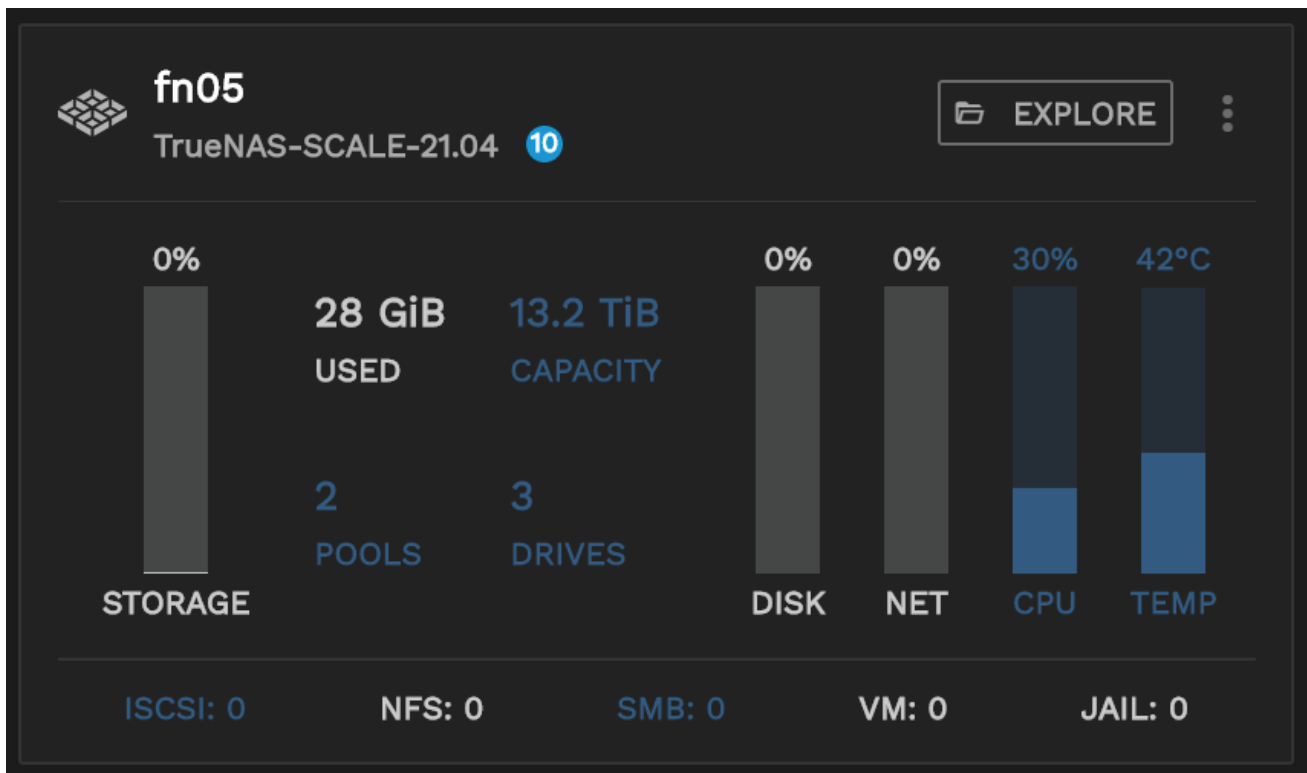
Viewing Alerts

To see all alerts TrueCommand has discovered, open the **Configure settings** menu and click **All Alerts**. Administrator accounts can see all system alerts. Non-administrator accounts can only view alerts according to their team and user account permissions.

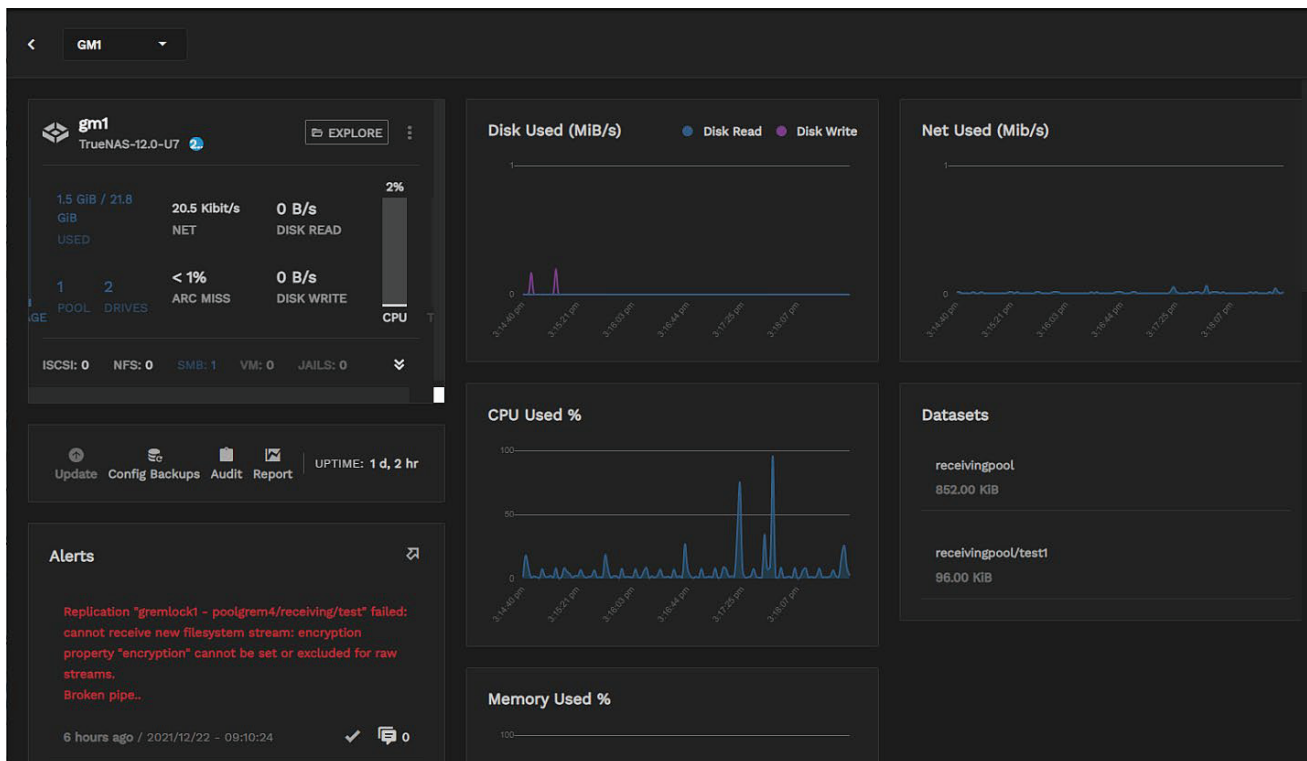
Alert Notices							
Filter				RESOLVE SELECTED		DELETE SELECTED	
<input type="checkbox"/>	CREATED	SYSTEM	PRIORITY	RESOLVED	TEXT	COMMENTS	ACTIONS
<input type="checkbox"/>	2021/12/22 - 14:30:01	gm4	critical		Replication "sendingpool/test1 - receivingpool/test1" failed: Unable to send encrypted dataset "sendingpool/test1" to existing unencrypted or unrelated dataset "receivingpool/test1".		
<input type="checkbox"/>	2021/12/22 - 09:10:24	gm1	critical		Replication "gremlock1 - poolgrem4/receiving/test" failed: cannot receive new filesystem stream: encryption property "encryption" cannot be set or excluded for raw streams. Broken pipe..		
<input type="checkbox"/>	2021/12/22 - 09:10:24	gm1	critical		Replication "gremlock1 - poolgrem4/receiving/test" failed: cannot receive new filesystem stream: encryption property "encryption" cannot be set or excluded for raw streams. Broken pipe..		
<input type="checkbox"/>	2021/12/22 - 07:07:47	gm1	warning		Storage pool "gremlock1" is predicted to reach 88.0% full in 14 days. Start preparing to expand your storage with additional disks.		
<input type="checkbox"/>	2021/12/21 - 16:15:10	gm1	critical		Replication "gremlock1/fromrep - poolgrem4/replfiles" failed: cannot receive new filesystem stream: zfs receive -F cannot be used to destroy an encrypted filesystem or overwrite an unencrypted one with an encrypted one warning: cannot send "gremlock1/fromrep@auto-2021-12-21_11-20": signal received..		
<input type="checkbox"/>	2021/12/21 - 16:15:10	gm1	critical		Replication "gremlock1/fromrep - poolgrem4/replfiles" failed: cannot receive new filesystem stream: zfs receive -F cannot be used to destroy an encrypted filesystem or overwrite an unencrypted one with an encrypted one warning: cannot send "gremlock1/fromrep@auto-2021-12-21_11-20": signal received..		
<input type="checkbox"/>					Replication "gremlock1/fromrep - poolgrem4/replfiles" failed: cannot receive new filesystem stream: zfs receive -F cannot be used		

Viewing Alerts by System

Alerts generated by a monitored system display on both the **Systems** screen and the system card or detail single system view on the **Dashboard** as a number to the right of the system name.



To view all alerts for a single system from the **Dashboard**, click on the system name to open the system details screen. The **Alerts** area displays the system's alerts.



Click the icon in the **Alerts** area of the system detail screen to display the **Notice Details** side panel with information about the alert and any user comments made.

To view all alerts from the **Systems** screen system list, click the **Configure settings** menu and then click **Systems**.

Systems

+ NEW SYSTEM

+ NEW GROUP

Systems

System Groups

Filter

NICKNAME	HOSTNAME	CONNECTION	LAST SYNC	UPDATES	ACTIONS
fn01 6	truenas.fn01			Available	
fn02		OFFLINE			
fn05 10	truenas.fn05			Available	
megamini		OFFLINE			
realmini 2	truenas.local				
scaley 4	truenas.local			Available	
tn02		OFFLINE			
tn03		OFFLINE			
tn23 3	tn23a.lab.				
viper01	viper01.lab.				

Just as with the systems detail alerts, click on the icon in the **COMMENTS** column to display the **Notice Details** side panel with information about the alert and any user comments made.

Resolving Alerts

You can move an alert in the **All Alerts** screen to the **RESOLVED** column by clicking the **Resolve check** to the right of the delete icon.

To resolve multiple alerts, select each alert checkbox, then click **RESOLVE SELECTED**.

Click the icon in the **COMMENTS** column to display the **Notice Details** side panel with information about the alert and any user comments made.

Alert Notices

Filter

Filter	CREATED	SYSTEM	PRIORITY	RESOLVED	TEXT
<input type="checkbox"/>	2021/12/22 - 14:30:01	gm4	critical		Replication "sendingpool/test1 - receivingpool/test1" failed: Unable to send encrypted dataset "sendingpool/unencrypted or unrelated dataset" "receivingpool/test1"..
<input type="checkbox"/>	2021/12/22 - 14:30:01	gm4	critical		Replication "sendingpool/test1 - receivingpool/test1" failed: Unable to send encrypted dataset "sendingpool/unencrypted or unrelated dataset" "receivingpool/test1"..
<input type="checkbox"/>	2021/12/22 - 13:30:01	gm4	critical		Replication "sendingpool/test1 - receivingpool/test1" failed: Unable to send encrypted dataset "sendingpool/unencrypted or unrelated dataset" "receivingpool/test1"..
<input type="checkbox"/>	2021/12/22 - 13:30:01	gm4	critical		Replication "sendingpool/test1 - receivingpool/test1" failed: Unable to send encrypted dataset "sendingpool/unencrypted or unrelated dataset" "receivingpool/test1"..
<input type="checkbox"/>	2021/12/22 - 13:30:01	gm4	critical		Replication "sendingpool/test1 - receivingpool/test1" failed: Unable to send encrypted dataset "sendingpool/unencrypted or unrelated dataset" "receivingpool/test1"..
<input type="checkbox"/>	2021/12/22 - 13:30:01	gm4	critical		Replication "sendingpool/test1 - receivingpool/test1" failed: Unable to send encrypted dataset "sendingpool/unencrypted or unrelated dataset" "receivingpool/test1"..
<input type="checkbox"/>	2021/12/22 - 13:30:01	gm4	critical		Replication "sendingpool/test1 - receivingpool/test1" failed: Unable to send encrypted dataset "sendingpool/unencrypted or unrelated dataset" "receivingpool/test1"..
<input type="checkbox"/>	2021/12/22 - 13:30:01	gm4	critical		Replication "sendingpool/test1 - receivingpool/test1" failed: Unable to send encrypted dataset "sendingpool/unencrypted or unrelated dataset" "receivingpool/test1"..

Notice Details > gm4

1970/01/19 - 18:36:41

Replication "sendingpool/test1 - receivingpool/test1" failed: Unable to send encrypted dataset "sendingpool/unencrypted or unrelated dataset" "receivingpool/test1"..

Comment

ADD COMMENT

No comments so far. Use the text field above to add comments.

To resolve an alert on the system detail screen **Alerts** area, click **Resolve alert notice** check to the left of the comments icon.

Alerts

Replication "gremlock1 - poolgrem4/receiving/test" failed: cannot receive new filesystem stream: encryption property "encryption" cannot be set or excluded for raw streams. Broken pipe..

Resolve alert notice

6 hours ago / 2021/12/22 - 09:10:24

✓ 0

Deleting Alerts

Administrator accounts can delete an alert by clicking the **delete** icon. Deleting an alert cannot be undone. To delete multiple alerts, select each alert checkbox and click **DELETE SELECTED** delete.

Alert Rules

Alert rules generate alerts in TrueCommand. TrueCommand has several built-in default rules. TrueCommand administrators and [team members](#) with the appropriate permissions can create new alert rules.

To view all TrueCommand alert rules, open the **Configure settings** menu and click **Alert Rules**.

Alert Rules

+ NEW ALERT RULE

Filter					
PRIORITY	OWNER	NAME	SYSTEM	TRIGGERS	ACTIONS
		NAS Offline Notice	All		
		SMART Disk Error	All		
		SMR Disk Detection	All		
		Storage Pool Errors	All		
		Storage Pool Expansion Required (90%)	All		
		Storage Pool Expansion Soon (80%)	All		

The **Alert Rules** screen details each TrueCommand alert rule and shows which user account created it.

Managing Alert Rules

Users can activate, suspend, edit, or delete alert rules using either an administrator account or the one that created them. Users can create new TrueCommand alert rules to monitor system information and generate a TrueCommand alert if specific conditions occur. To create a new alert rule, click **+ NEW ALERT RULE** and follow the creation wizard:

Alert Rules > create

SAVE ALERT RULE

Alert Options

Alert Rule Name

System

All

Priority

Warning

Description

Alert Triggers

☒ All conditions must be true

Metric

Comparator

Greater Than

Value

0

ADD TRIGGER

To create a new rule:

- Specify the **Alert Options**: a. Enter a name into the **Alert Rule Name** field. b. Select a system from the **System** drop-down. The rule applies to the selected system(s). Non-administrative user accounts require appropriate system permissions. c. Select the alert type on the **Priority** drop-down list. Choose **Information**, **Warning**, or **Critical** to determine the alert category generated. d. Type a description for the alert.
- Specify the **Alert Triggers**: Select a data source or rule type from the drop-down list to determine what can trigger an alert. For example, *cpu_temperature* means the alert rule monitors the temperature of the chosen system. Scroll down the list to find the desired source.

b. Select the comparison type from the **Comparator** drop-down list (**Greater Than**, **Less Than**, or **Not Equals**). The comparison type applies to the data source and comparison value. c. Specify the comparison value by entering an integer appropriate for the selected options in the **Value** field. The integer acts as a threshold or limitation for when the rule generates an alert.

3. To finish creating the new alert rule, click **CREATE ALERT**. To start over, click **RESET**.

○ Alert Services

Configurable alert services are only available for local installations or containerized TrueCommand deployments. TrueCommand Cloud instances use email alerts by default; PagerDuty is not an option.

TrueCommand uses different service plugins to expand how it communicates alerts to users or administrators. Individual user accounts can use service plugins to manage how TrueCommand notifies them of a system alert.

Configuring Alert Services

To configure an alert service plugin, open the **Configure settings** menu and click **Alert Services**. There are two services listed:

- **PagerDuty** is a plugin to configure a pager to receive an alert.
- **SMTP Email** is a plugin to configure system and user email services.

Alert Services		
NAME	DESCRIPTION	ACTIONS
PagerDuty	Forward alerts to a PagerDuty account	
SMTP Email	Send email alerts via SMTP	

Each plugin has three options:

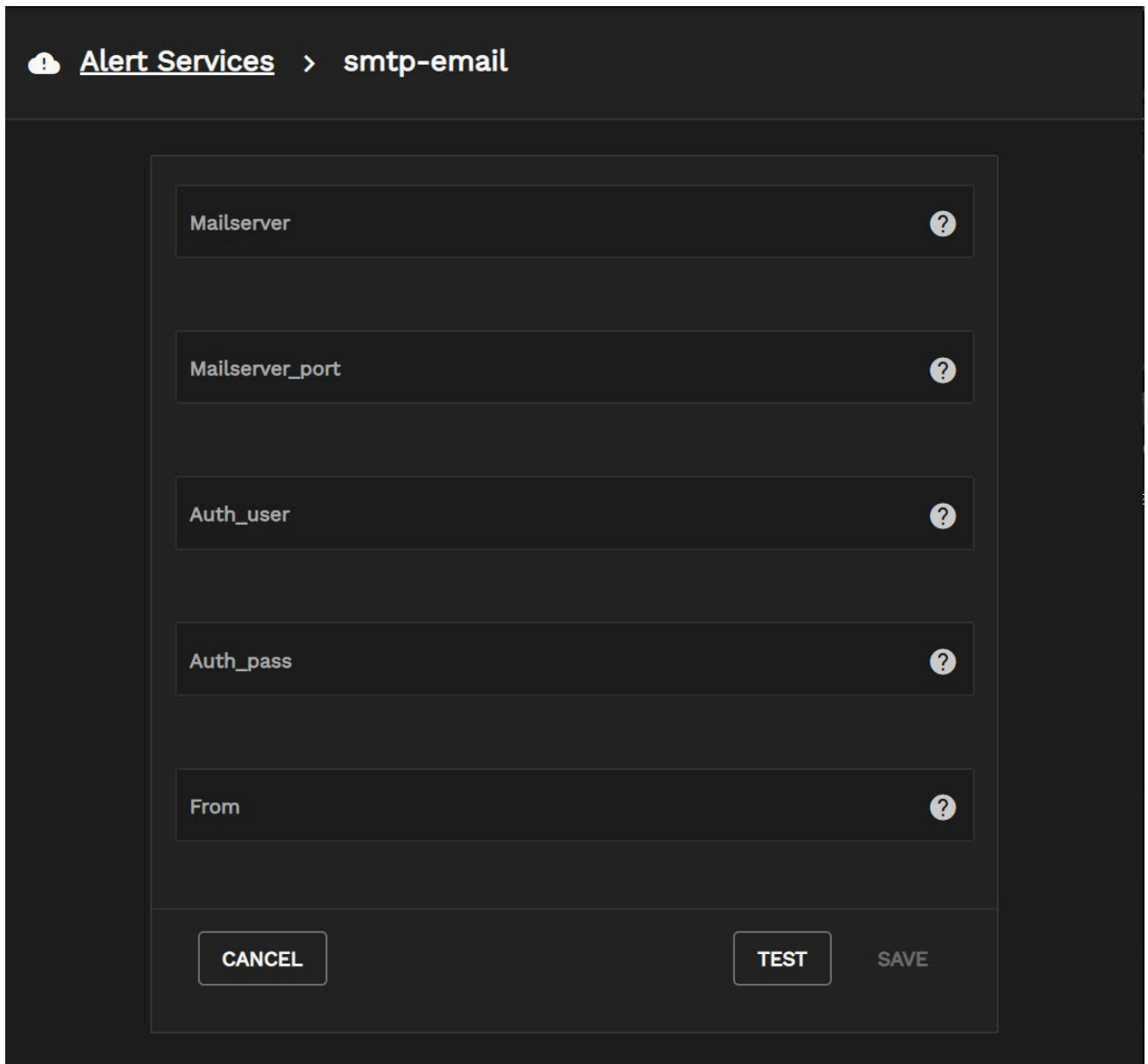
- **Send test email**
- **Configure plugin settings**
- **Clear plugin configuration remove_circle**

Configuring SMTP Email

Before proceeding, verify that the sending mailserver has TLS enabled. TrueCommand cannot send emails through a mailserver without TLS. The user's profile page must have an email address to receive emails.

To properly configure SMTP email:

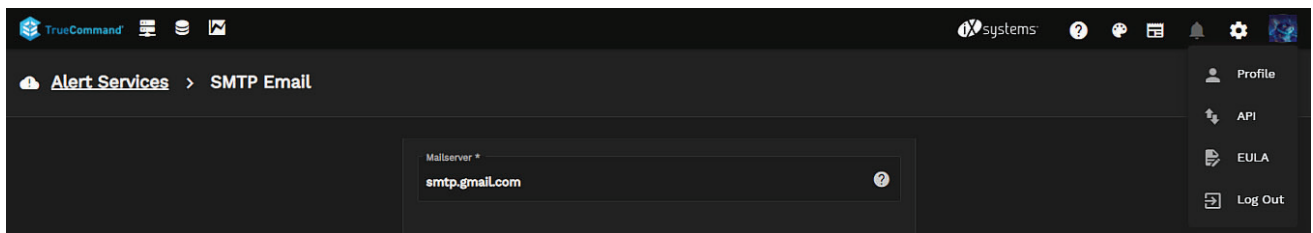
1. Enter values in all fields on the **SMTP Email** screen and then click **SAVE**:



- **Mailserver** (*smtp.gmail.com* for example)
- **Mailserver port** number
- **Auth user** email address for plain authentication, for example, adminuser@yourmail.com
- **Auth pass** password for the plain authentication; for a *No-Auth* SMTP configuration, leave the password field blank
- **From** is what sends the email (i.e., no-reply@TrueCommand.io) or allows you to customize the sender field of the email

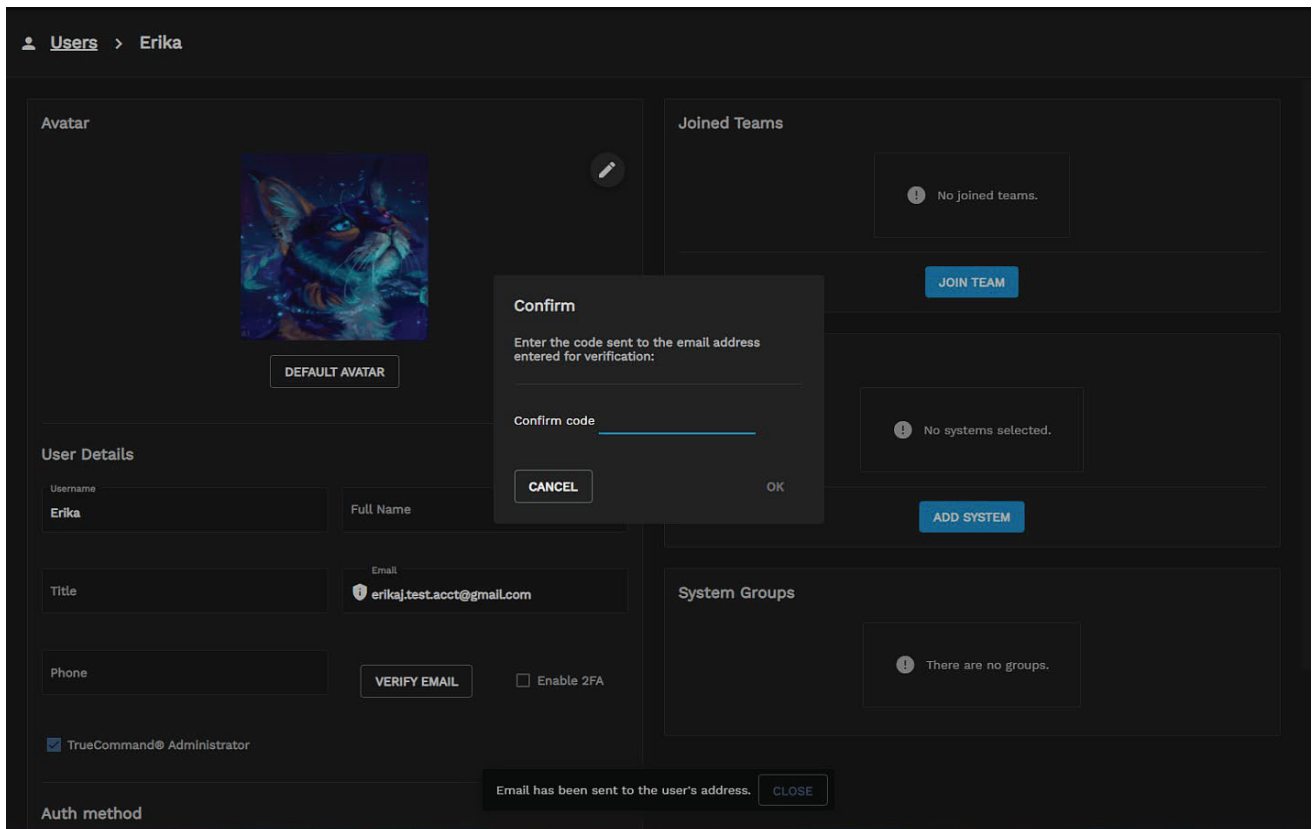
Click **Test** on the **SMTP Email** configuration screen to verify that the configuration is correct. If you did not receive a test alert email, check the values entered for accuracy.

2. Click on the avatar to the right of the **Configure settings** menu and then click **Profile** from the drop-down list.




3. Type the email for that user in the **Email** field and click **SAVE CHANGES**. The first time you set up SMTP email, a **VERIFY EMAIL** button displays below the **Email** field to the left of the **Enable 2FA** checkbox.


The system should automatically send a test email to the specified email address. If it doesn't, click **VERIFY EMAIL**. In the **Confirm** dialog box, enter or copy/paste the emailed code to verify the email.



Configuring PagerDuty

Open the **Configure Plugin settings** for PagerDuty. Enter your PagerDuty API key in the **Auth token** field. If you have an active subscription with PagerDuty, the key should be available to you. Click **TEST**.

 **Alert Services** > pagerduty

Authtoken 

CANCEL

TEST


SAVE


Log in to your PagerDuty account and check for open incidents. You should see the triggered test alert from TrueCommand.


0 acknowledged

0 acknowledged

! Acknowledge

 Reassign

 Resolve

 Snooze

Merge Incidents

Go to incident #...

Open

Triggered

Acknowledged

Resolved

Any Status

Assigned to meAll

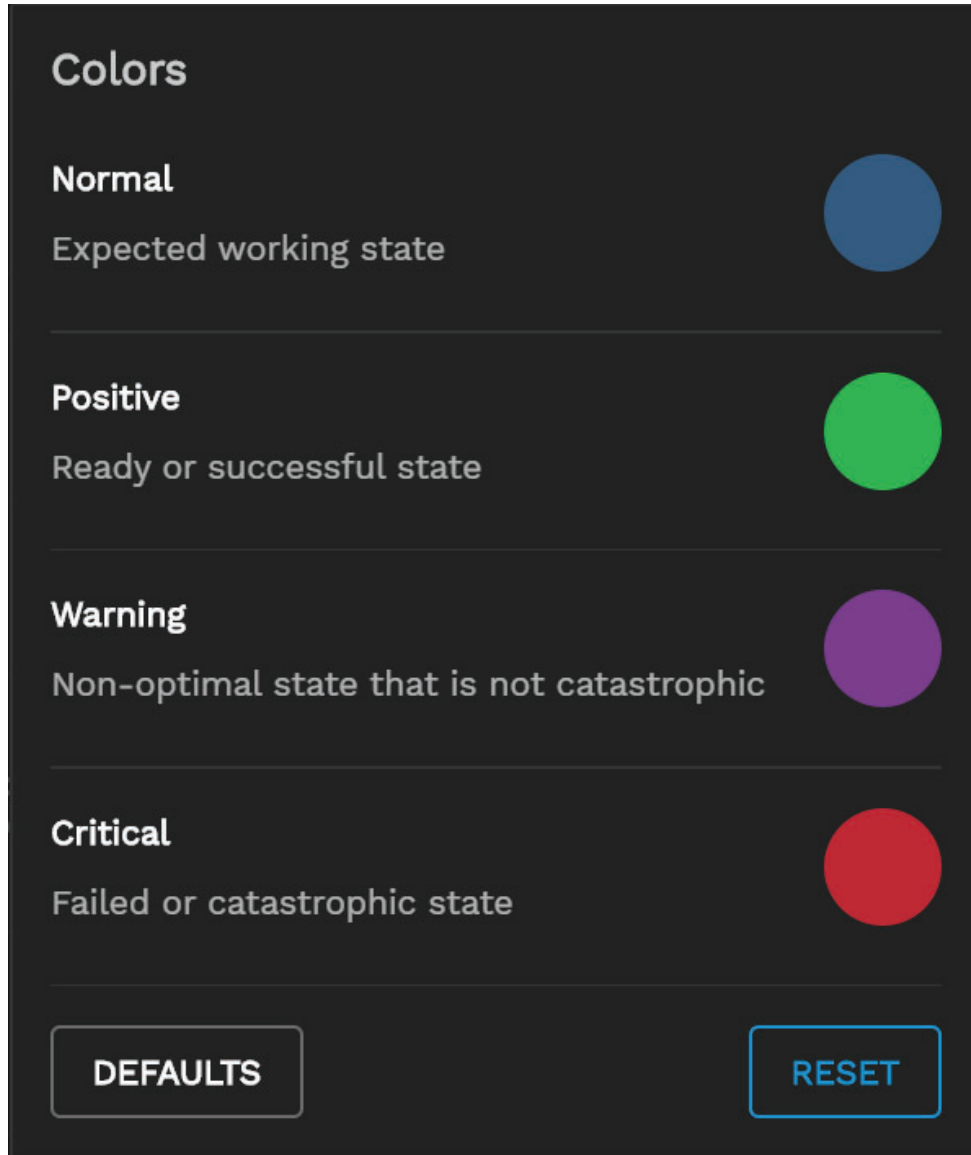
<input checked="" type="checkbox"/>	Status	Urgency	Title	Created	Service	Assigned To
<input checked="" type="checkbox"/>	Triggered	High	This is a test of the TrueCommand pagerduty notification system <small>(SHOW DETAILS (1 triggered alert))</small>	at 1:36 PM <small>#1143</small>	Consul-FreeNAS	Kris Moore

Per Page: 25 1-1

If you did not receive a test alert, check the PagerDuty API key for accuracy in the alert service plugin configuration section.

8.2 - Colors

TrueCommand includes the ability to customize the alert colors to user preferences. The Theme pallet is located in the top banner on the right. To open the theme configuration menu, click the **palette** icon.

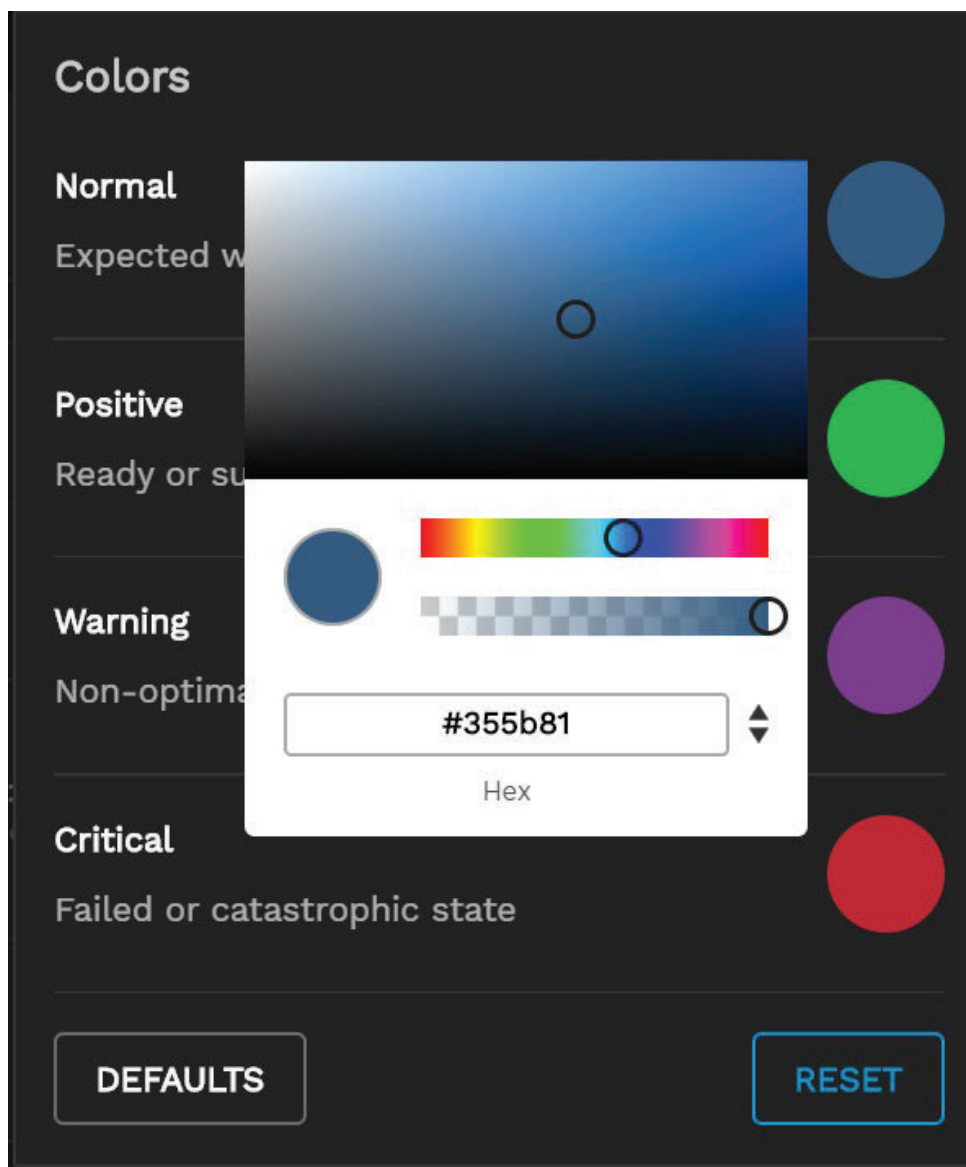


The screenshot shows a dark-themed configuration window titled "Colors". It contains four rows, each with a label, a description, and a color swatch:

- Normal**: Expected working state (Blue swatch)
- Positive**: Ready or successful state (Green swatch)
- Warning**: Non-optimal state that is not catastrophic (Purple swatch)
- Critical**: Failed or catastrophic state (Red swatch)

At the bottom of the window are two buttons: "DEFAULTS" and "RESET".

To change a color, click on the color to open a selection menu. Select the desired color or enter its HEX color value.



To remove changes and revert to the currently saved settings, click *Reset*. To reset all colors to the application defaults, click *Defaults*.

9 - Clustering

TrueCommand 2.1, in conjunction with TrueNAS SCALE, can create clustered volumes that span across multiple volumes.

There are five volume types:

- Replicated - Use Replicated for better reliability and data redundancy, and to overcome the risk of data loss in a distributed volume. It creates copies of files across multiple bricks in the volume. Use replicated volumes in environments where high-availability and high-reliability are critical.
- Distributed - Use Distributed to distribute files across the various bricks in the volumes. Use where scalable storage and redundancy is either not important, or is provided by other hardware or software layers.
- Dispersed - Use Dispersed to disperse data across the bricks in the volume. The volume data is broken into fragments, expanded and encoded with redundant data pieces and stored across a set of different bricks. Dispersed volumes allow a configurable level of reliability with minimal waste of storage space.
- Distributed Replicated - Use Distributed Replicated to distributed data across replicated sets of bricks. This volume creates distributed copies of multiple bricks in the volume. Use distributed replicated volumes in environments where high-availability and high-reliability are critical.
- Distributed Dispersed - Use Distributed Dispersed when you want data distributed and broken into fragments, expanded and encoded with redundant data pieces and stored across a set of different bricks. This feature is not implemented at this time.

Cluster volume management is a BETA feature in TrueCommand 2.0 and 2.1. Before using such features, please back up all your data. Do not rely on this for critical data.

TrueNAS does not support distributed dispersed volumes at this time.

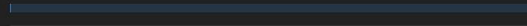
The cluster feature uses reverse DNS lookup. A valid reverse lookup is required.



Dispersed-Cluster

STARTED ⋮

768.00 KiB used / 3.00 GiB

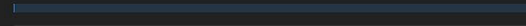


▼ Dispersed-Cluster-disperse-0 Health: UP

Distributed-Cluster

STARTED ⋮

768.00 KiB used / 3.00 GiB



▼ Distributed-Cluster-distribute-0 Health: UP

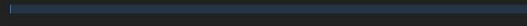
▼ Distributed-Cluster-distribute-1 Health: UP

▼ Distributed-Cluster-distribute-2 Health: UP

Distributed-Replicated-Cluster

STARTED ⋮

512.00 KiB used / 2.00 GiB



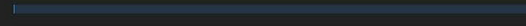
▼ Distributed-Replicated-Cluster-replicate-0 Health: UP

▼ Distributed-Replicated-Cluster-replicate-1 Health: UP

Replicated-Cluster

STARTED ⋮

256.00 KiB used / 1.00 GiB



▼ Replicated-Cluster-replicate-0 Health: UP

9.1 - Creating Clustered Volumes

Cluster volume management is a BETA feature in TrueCommand 2.0. Back up your data *before* using BETA features. Do not rely on cluster volume management for critical data.

Gluster requires TrueNAS systems to have a static IP. TrueNAS systems with DHCP enabled can not be part of a cluster volume.

To create a cluster volume, click the **Cluster Volume** icon in the top left of the top menu bar or the **Cluster Volume** button on the **Settings settings** menu drop-down.

Click **Create** on the **Cluster Volumes** page. Name the cluster, select the desired type in the **Volume Type** drop-down list, then set the redundancy level for distributed replicated and dispersed volumes.

1 Cluster Configuration — 2 Review and Create

Configure the volume type

DISTRIBUTED

REPLICATED

DISTRIBUTED REPLICATED

DISPERSED

Redundancy Count

Name

ClusterA

Brick Choices

Size

10 GiB

☒ Sync Sizes

NEXT

TrueCommand has five cluster volume types.

⦿ Distributed

DISTRIBUTED volumes distribute files across the various bricks in the volume. *File-A* can be stored in *Brick-1* or *Brick-2* but not on both. As a result, the volume has no data redundancy. A distributed volume's purpose is to cheaply and easily scale the volume size. However, it can suffer significant data loss during a disk or server failure because directory contents are spread randomly across the bricks in the volume.

Warning: Brick failure in a distributed volume results in complete data loss.





Click the **Brick Choices** drop-down, then select the locations to use for bricks.


1 Cluster Configuration — **2 Review and Create**

Configure the volume's type and bricks.


NEXT

Name Distributed-Cluster	Volume Type DISTRIBUTED ?
------------------------------------	-------------------------------------


<input type="checkbox"/>  hydra30 h029 1.24 GiB USED / 7.27 GiB	<input type="checkbox"/> Sync Sizes
<input checked="" type="checkbox"/>  hydra028 h028 5.97 GiB USED / 7.27 GiB	
<input checked="" type="checkbox"/>  hydra027 h027 3.96 GiB USED / 7.27 GiB	
<input checked="" type="checkbox"/>  hydra029 h029 5.96 GiB USED / 7.27 GiB	

 **hydra028** **h028** 5.97 GiB USED / 7.27 GiB
/mnt/h028/.gluster/Distributed-Cluster/brick0

Size: **1** GiB

 **hydra027** **h027** 3.96 GiB USED / 7.27 GiB
/mnt/h027/.gluster/Distributed-Cluster/brick0

Size: **1** GiB IP: **10.234.56.127**

 **hydra029** **h029** 5.96 GiB USED / 7.27 GiB
/mnt/h029/.gluster/Distributed-Cluster/brick0

Size: **1** GiB IP: **10.234.56.129**

When finished, click **Next**.

1 Cluster Configuration — **2 Review and Create**

Configure the volume's type and bricks.

NEXT

Name

Distributed-Cluster

Volume Type

DISTRIBUTED



Brick Choices

Size

1

GiB



Sync Sizes

**hydra028****h028**

5.97 GiB USED / 7.27 GiB



/mnt/h028/.gluster/Distributed-Cluster/brick0

Size

1

GiB

IP

10.234.56.128

**hydra027****h027**

3.96 GiB USED / 7.27 GiB



/mnt/h027/.gluster/Distributed-Cluster/brick0

Size

1

GiB

IP

10.234.56.127

**hydra029****h029**

5.96 GiB USED / 7.27 GiB



/mnt/h029/.gluster/Distributed-Cluster/brick0

Size

1

GiB

IP

10.234.56.129

Review the configuration and click **Create** to create the volume.

1 Cluster Configuration — 2 Review and Create

[BACK](#)

Review the summary information and click CREATE.

[CREATE](#)

Distributed-Cluster

Type



DISTRIBUTED

Distribute files across the bricks in the volume. You can use distributed volumes where the requirement is to scale storage and the redundancy is either not important or is provided by other hardware/software layers.

Bricks



hydra028 h028 5.97 GiB USED / 7.27 GiB 10.234.56.128

1 GiB /mnt/h028/.glusterfs/Distributed-Cluster/brick0



hydra027 h027 3.96 GiB USED / 7.27 GiB 10.234.56.127

1 GiB /mnt/h027/.glusterfs/Distributed-Cluster/brick0



hydra029 h029 5.96 GiB USED / 7.27 GiB 10.234.56.129

1 GiB /mnt/h029/.glusterfs/Distributed-Cluster/brick0

You can view the volume status after creating it.

Distributed-Cluster

STARTED



768.00 KiB used / 3.00 GiB



- ▼ Distributed-Cluster-distribute-0 Health: UP
- ▼ Distributed-Cluster-distribute-1 Health: UP
- ▼ Distributed-Cluster-distribute-2 Health: UP

☐ Replicated

REPLICATED volumes offer better reliability and data redundancy, and overcome the risk of data loss in a distributed volume. All bricks maintain exact copies of all data. You determine the number of replicas for the volume when you create it. Replicated volumes require at least three bricks, but you can add more bricks for additional redundancy. Three-brick volumes have three replicas, and four-brick volumes have four replicas. Replicated volumes allow data access even if a single brick fails.

Click the **Brick Choices** drop-down, then select the locations to use for bricks.



1 Cluster Configuration — **2 Review and Create**

Configure the volume's type and bricks.

NEXT

Name	Volume Type
Replicated-Cluster	REPLICATED ?

Size		<input checked="" type="checkbox"/> Sync Sizes
<input type="checkbox"/> hydra030	h029 1.27 GiB USED / 7.27 GiB	
<input checked="" type="checkbox"/> hydra028	h028 5.99 GiB USED / 7.27 GiB	
<input checked="" type="checkbox"/> hydra027	h027 3.98 GiB USED / 7.27 GiB	
<input checked="" type="checkbox"/> hydra029	h029 5.98 GiB USED / 7.27 GiB	

 **hydra028** h028 5.99 GiB USED / 7.27 GiB 



/mnt/h028/.gluster/Replicated-Cluster/brick0

Size

1 GiB

IP

10.234.56.127

 **hydra027** h027 3.98 GiB USED / 7.27 GiB 



/mnt/h027/.gluster/Replicated-Cluster/brick0

Size

1 GiB

IP

10.234.56.127

 **hydra029** h029 5.98 GiB USED / 7.27 GiB 

/mnt/h029/.gluster/Replicated-Cluster/brick0

Size

1 GiB

IP

10.234.56.129

When finished, click **Next**.

1 Cluster Configuration — **2 Review and Create**

Configure the volume's type and bricks.

NEXT

Name

Replicated-Cluster

Volume Type

REPLICATED



Brick Choices

Size

1

GiB



Sync Sizes

**hydra028****h028**

5.99 GiB USED / 7.27 GiB



/mnt/h028/.gluster/Replicated-Cluster/brick0

Size

1

GiB

IP

10.234.56.128

**hydra027****h027**

3.98 GiB USED / 7.27 GiB



/mnt/h027/.gluster/Replicated-Cluster/brick0

Size

1

GiB

IP

10.234.56.127

**hydra029****h029**

5.98 GiB USED / 7.27 GiB



/mnt/h029/.gluster/Replicated-Cluster/brick0

Size

1

GiB

IP

10.234.56.129

Review the configuration and click **Create** to create the volume.

1 Cluster Configuration

2 Review and Create

BACK

Review the summary information and click CREATE.

CREATE

Replicated-Cluster

Type



REPLICATED

Replicate files across bricks in the volume. You can use replicated volumes in environments where high-availability and high-reliability are critical.

Replica Count: 3

Bricks

**hydra028** h028 5.99 GiB USED / 7.27 GiB 10.234.56.128

1 GiB /mnt/h028/.glusterfs/Replicated-Cluster/brick0

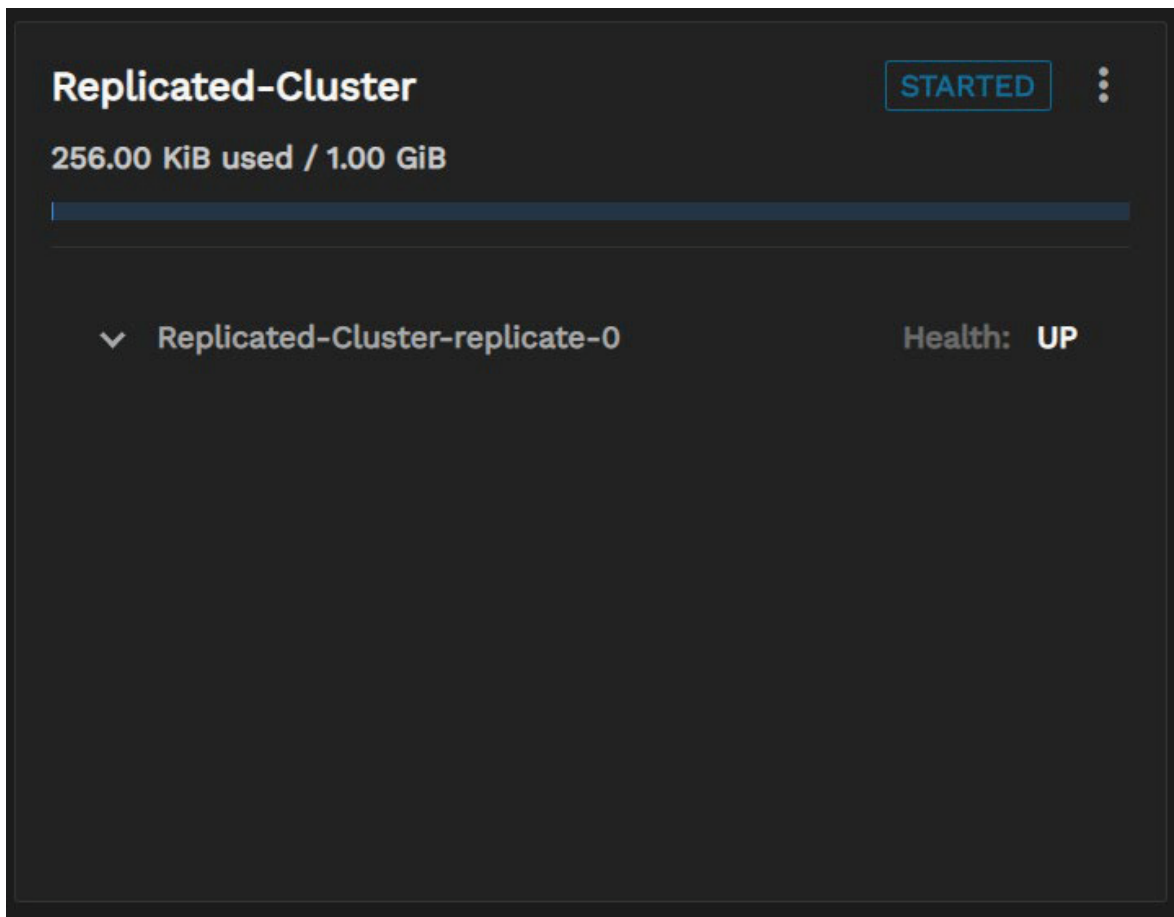
**hydra027** h027 3.98 GiB USED / 7.27 GiB 10.234.56.127

1 GiB /mnt/h027/.glusterfs/Replicated-Cluster/brick0

**hydra029** h029 5.98 GiB USED / 7.27 GiB 10.234.56.129

1 GiB /mnt/h029/.glusterfs/Replicated-Cluster/brick0

You can view the volume status after creating it.

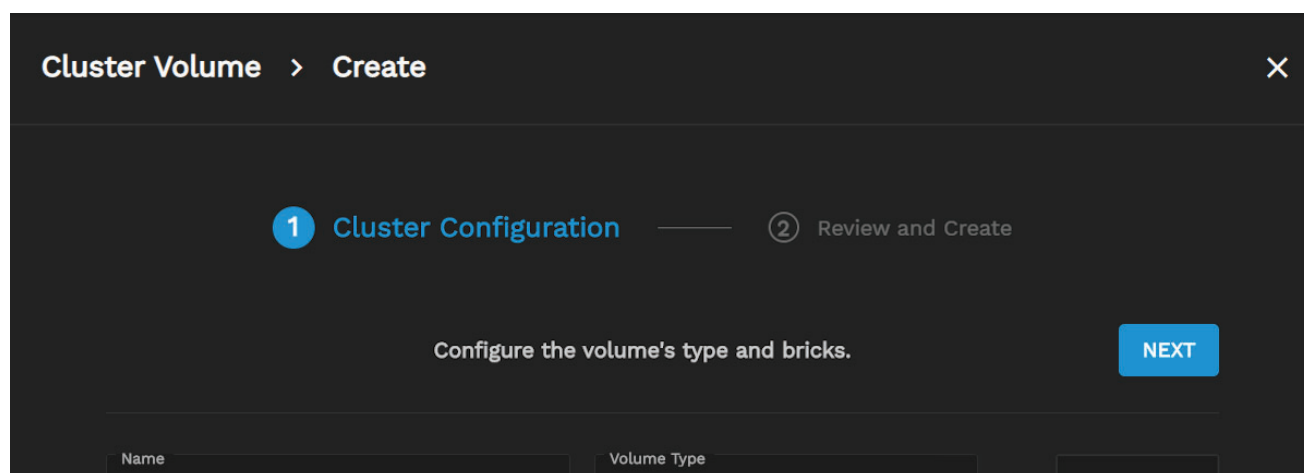


☐ Distributed Replicated

DISTRIBUTED REPLICATED volumes distribute data across replicated sets of bricks. The brick number must be a multiple of the replica count. The order in which you specify bricks is important because adjacent bricks become replicas of each other. Distributed replicated volumes are best when you need high data availability due to redundancy and scaling storage. For example, an eight-brick volume with a replica count of two would result in the first two bricks becoming replicas of each other, and then the next two and so on. This volume is called a 4x2. By contrast, in this eight brick example, a replica count of four results in four bricks becoming replicas of each other. This volume is called a 2x4. The distributed replicated volume's **Replica value** must be a divisor of the total number of bricks selected. If you use eight bricks, the replica count can be two or four. A replica count of two creates a 4x2 volume where pairs of bricks replicate each other. A replica count of four generates a 2x4 volume where sets of four bricks replicate each other.

Using a replica count that is not a divisor of the total brick number will cause volume creation to fail.

Click the **Brick Choices** drop-down, then select the locations to use for bricks.



Select the **Replica Count** from the list. When finished, click **Next**.

1 Cluster Configuration — **2** Review and Create

Configure the volume's type and bricks.

NEXT

Name Distributed-Replicated-Cluster	Volume Type DISTRIBUTED REPLICATED	Replica Count 2
--	---------------------------------------	--------------------

Brick Choices	Size 1 GiB	<input checked="" type="checkbox"/> Sync Sizes
---------------	---------------	--

**hydra030** h029 1.24 GiB USED / 7.27 GiB

/mnt/h029/.gluster/Distributed-Replicated-Cluster/brick0

Size 1 GiB	IP 10.234.56.130
---------------	---------------------

**hydra028** h028 5.97 GiB USED / 7.27 GiB

/mnt/h028/.gluster/Distributed-Replicated-Cluster/brick0

Size 1 GiB	IP 10.234.56.128
---------------	---------------------

**hydra027** h027 3.96 GiB USED / 7.27 GiB

/mnt/h027/.gluster/Distributed-Replicated-Cluster/brick0

Size 1 GiB	IP 10.234.56.127
---------------	---------------------

**hydra029** h029 5.96 GiB USED / 7.27 GiB

/mnt/h029/.gluster/Distributed-Replicated-Cluster/brick0

Size 1 GiB	IP 10.234.56.129
---------------	---------------------

Review the configuration and click **Create** to create the volume.

Cluster Volume > Create

1 Cluster Configuration

2 Review and Create


BACK

Review the summary information and click CREATE.

CREATE

Distributed-Replicated-Cluster


Type

 **DISTRIBUTED_REPLICATED**


Distribute files across replicated bricks in the volume. You can use distributed replicated volumes in environments where the requirement is to scale storage and high-reliability is critical. Distributed replicated volumes also offer improved read performance in most environments.

Replica Count: **2**


Bricks

 **hydra030** h029 1.24 GiB USED / 7.27 GiB 10.234.56.130


1 GiB /mnt/h029/.glusterfs/Distributed-Replicated-Cluster/brick0

 **hydra028** h028 5.97 GiB USED / 7.27 GiB 10.234.56.128

1 GiB /mnt/h028/.glusterfs/Distributed-Replicated-Cluster/brick0

 **hydra027** h027 3.96 GiB USED / 7.27 GiB 10.234.56.127

1 GiB /mnt/h027/.glusterfs/Distributed-Replicated-Cluster/brick0

 **hydra029** h029 5.96 GiB USED / 7.27 GiB 10.234.56.129

1 GiB /mnt/h029/.glusterfs/Distributed-Replicated-Cluster/brick0

You can view the volume status after creating it.

Distributed-Replicated-Cluster

STARTED

512.00 KiB used / 2.00 GiB

Distributed-Replicated-Cluster-replicate-0
Health: UP

Distributed-Replicated-Cluster-replicate-1
Health: UP

○ Dispersed

DISPERSED volumes disperse data across the bricks. Dispersed volumes use Erasure Coding (EC), a data protection method in which data is broken into fragments, expanded and encoded with redundant data pieces, and stored across a set of different locations. EC lets users recover the data stored on one or more bricks in case of failure. The redundancy count setting determines the number of bricks that can fail without losing data. Dispersed volumes allow a configurable level of reliability with minimal storage space waste. You define the number of redundant bricks in the volume when you create it. The number of redundant bricks determines how many bricks the volume can lose without interrupting operation.

The dispersed volume's **Redundancy value** must be greater than 0 and less than $n-1$. Think of the redundancy value as the number of bricks you can lose before data loss occurs.

The data protection offered by erasure coding can be represented in simple form by the following equation: $n = k + m$.

Here, n is the total number of bricks. We would require any k bricks out of n bricks for recovery. In other words, we can tolerate failure up to any m bricks.





Click the **Brick Choices** drop-down, then select the locations to use for bricks.



1 Cluster Configuration — **2** Review and Create



Configure the volume's type and bricks.



NEXT

Name Dispersed-Cluster	Volume Type DISPERSED	Redundancy Count 1
----------------------------------	---------------------------------	------------------------------

<input checked="" type="checkbox"/>  hydra030 h029 1.24 GiB USED / 7.27 GiB	<input checked="" type="checkbox"/> Sync Sizes
<input checked="" type="checkbox"/>  hydra028 h028 5.97 GiB USED / 7.27 GiB	
<input checked="" type="checkbox"/>  hydra027 h027 3.96 GiB USED / 7.27 GiB	
<input checked="" type="checkbox"/>  hydra029 h029 5.96 GiB USED / 7.27 GiB	

 hydra028 h028 5.97 GiB USED / 7.27 GiB	
/mnt/h028/.gluster/Dispersed-Cluster/brick0	
Size 1 GiB	IP 10.234.56.128

 hydra027 h027 3.96 GiB USED / 7.27 GiB	
/mnt/h027/.gluster/Dispersed-Cluster/brick0	
Size 1 GiB	IP 10.234.56.127

 hydra029 h029 5.96 GiB USED / 7.27 GiB	
/mnt/h029/.gluster/Dispersed-Cluster/brick0	
Size 1 GiB	IP 10.234.56.129

Select the **Redundancy value**. When finished, click **Next**.

1 Cluster Configuration — 2 Review and Create

Configure the volume's type and bricks.

NEXT

Name	Volume Type	Redundancy Count
Dispersed-Cluster	DISPERSED	1

Brick Choices	Size	<input checked="" type="checkbox"/> Sync Sizes
	1 GiB	



hydra030 h029 1.24 GiB USED / 7.27 GiB



/mnt/h029/.gluster/Dispersed-Cluster/brick0

Size

1

GiB

IP

10.234.56.130



hydra028 h028 5.97 GiB USED / 7.27 GiB



/mnt/h028/.gluster/Dispersed-Cluster/brick0

Size

1

GiB

IP

10.234.56.128



hydra027 h027 3.96 GiB USED / 7.27 GiB



/mnt/h027/.gluster/Dispersed-Cluster/brick0

Size

1

GiB

IP

10.234.56.127



hydra029 h029 5.96 GiB USED / 7.27 GiB



/mnt/h029/.gluster/Dispersed-Cluster/brick0

Size

1

GiB

IP

10.234.56.129

Review the configuration and click **Create** to create the volume.

Cluster Volume > Create

1 Cluster Configuration

2 Review and Create


BACK

Review the summary information and click CREATE.

CREATE

Dispersed-Cluster


Type

 **DISPERSED**


Dispersed volumes are based on erasure codes, providing space-efficient protection against disk or server failures. It stores an encoded fragment of the original file to each brick in a way that only a subset of the fragments is needed to recover the original file. The number of bricks that can be missing without losing access to data is configured by the administrator on volume creation time.

Redundancy Count: **1**


Bricks

 **hydra030** h029 1.24 GiB USED / 7.27 GiB 10.234.56.130


1 GiB /mnt/h029/.glusterfs/Dispersed-Cluster/brick0

 **hydra028** h028 5.97 GiB USED / 7.27 GiB 10.234.56.128

1 GiB /mnt/h028/.glusterfs/Dispersed-Cluster/brick0

 **hydra027** h027 3.96 GiB USED / 7.27 GiB 10.234.56.127

1 GiB /mnt/h027/.glusterfs/Dispersed-Cluster/brick0

 **hydra029** h029 5.96 GiB USED / 7.27 GiB 10.234.56.129

1 GiB /mnt/h029/.glusterfs/Dispersed-Cluster/brick0

You can view the volume status after creating it.

Dispersed-Cluster

STARTED

768.00 KiB used / 3.00 GiB

Dispersed-Cluster-disperse-0

Health: UP

○ Distributed Dispersed

We have not implemented Distributed Dispersed volumes yet.

9.2 - Managing Clustered Storage

Clustered volumes have differing management options based on the cluster type.

Removing or replacing bricks from a clustered volume can lead to data corruption. Do not attempt to use this feature at this time.

☐ Distributed

Distributed-Cluster

STARTED

768.00 KiB used / 3.00 GiB

▼ Distributed-Cluster-distribute-0

Health: UP

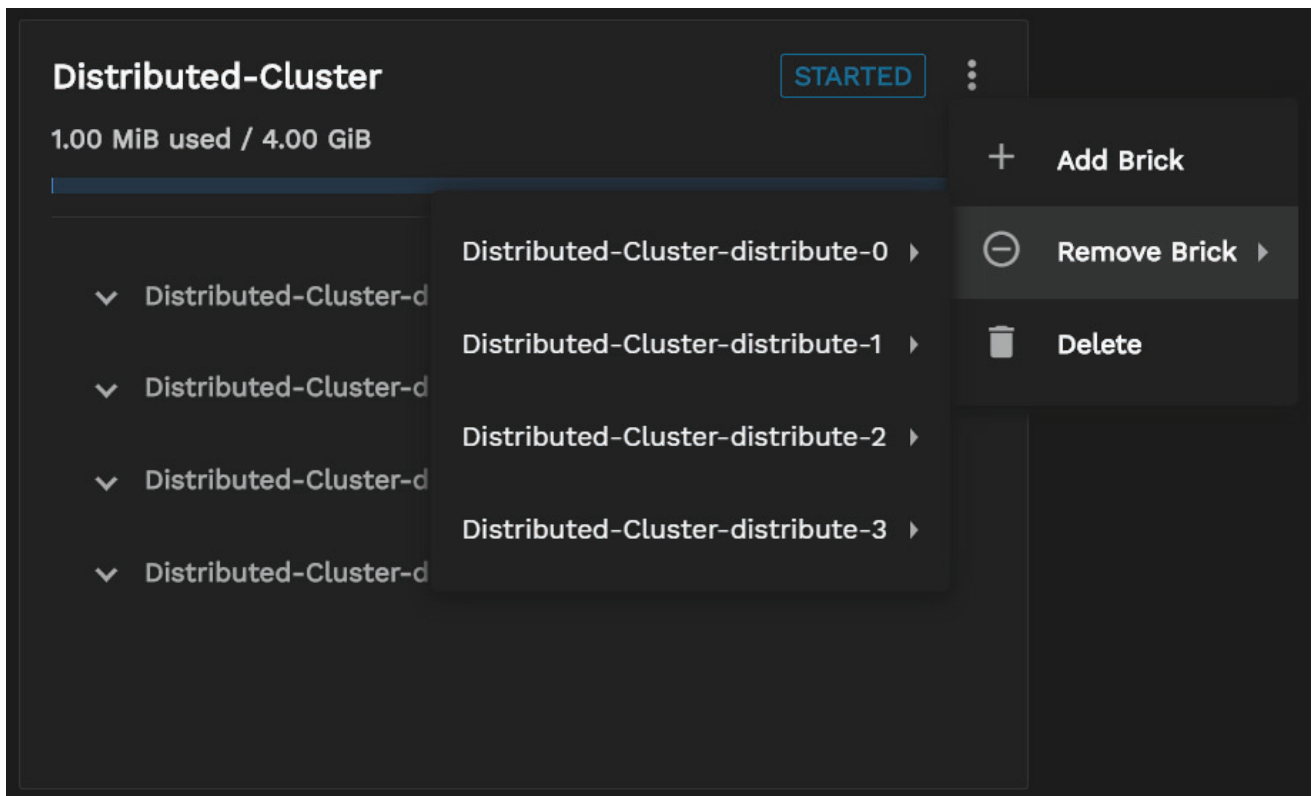
▼ Distributed-Cluster-distribute-1

Health: UP


▼ Distributed-Cluster-distribute-2

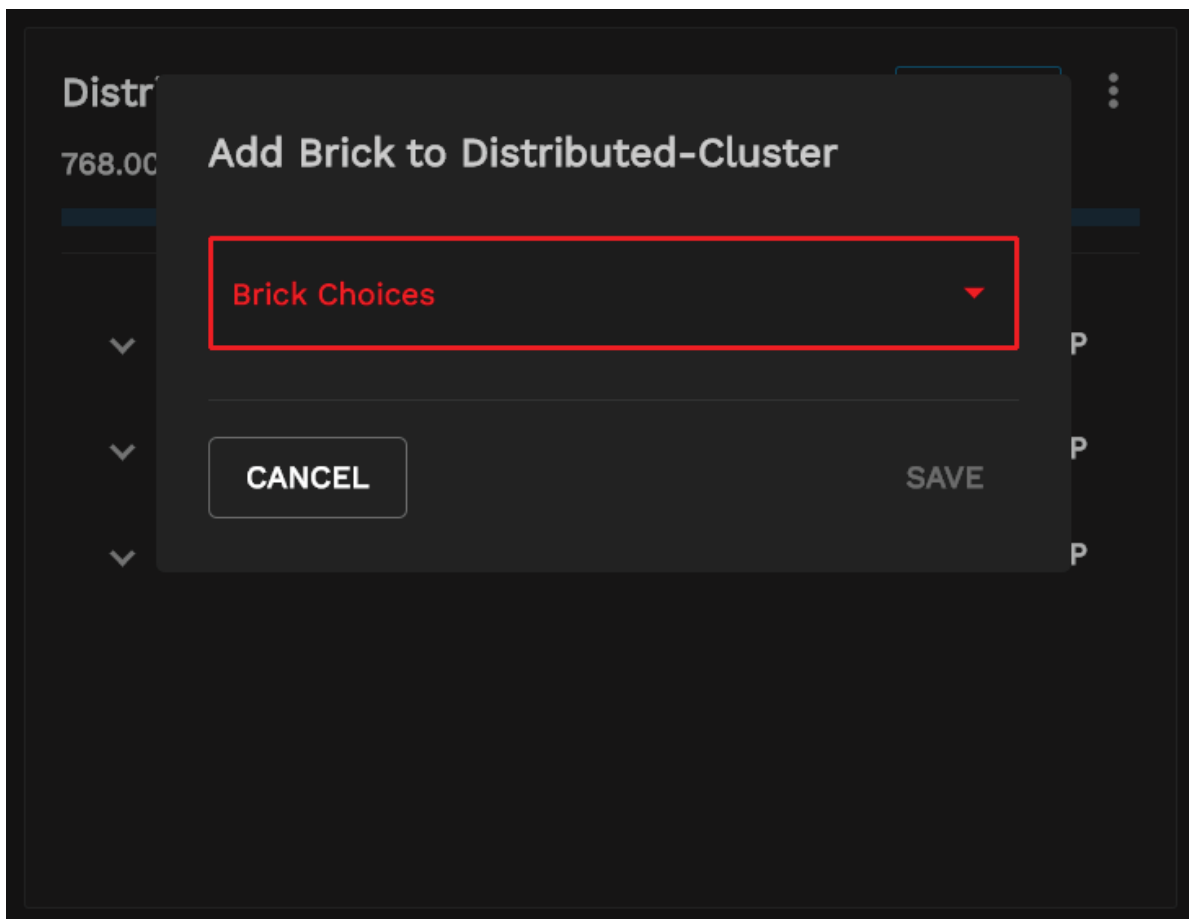
Health: UP

Distributed-Cluster volumes have three editing options: **Add Brick**, **Remove Brick**, and **Delete**.

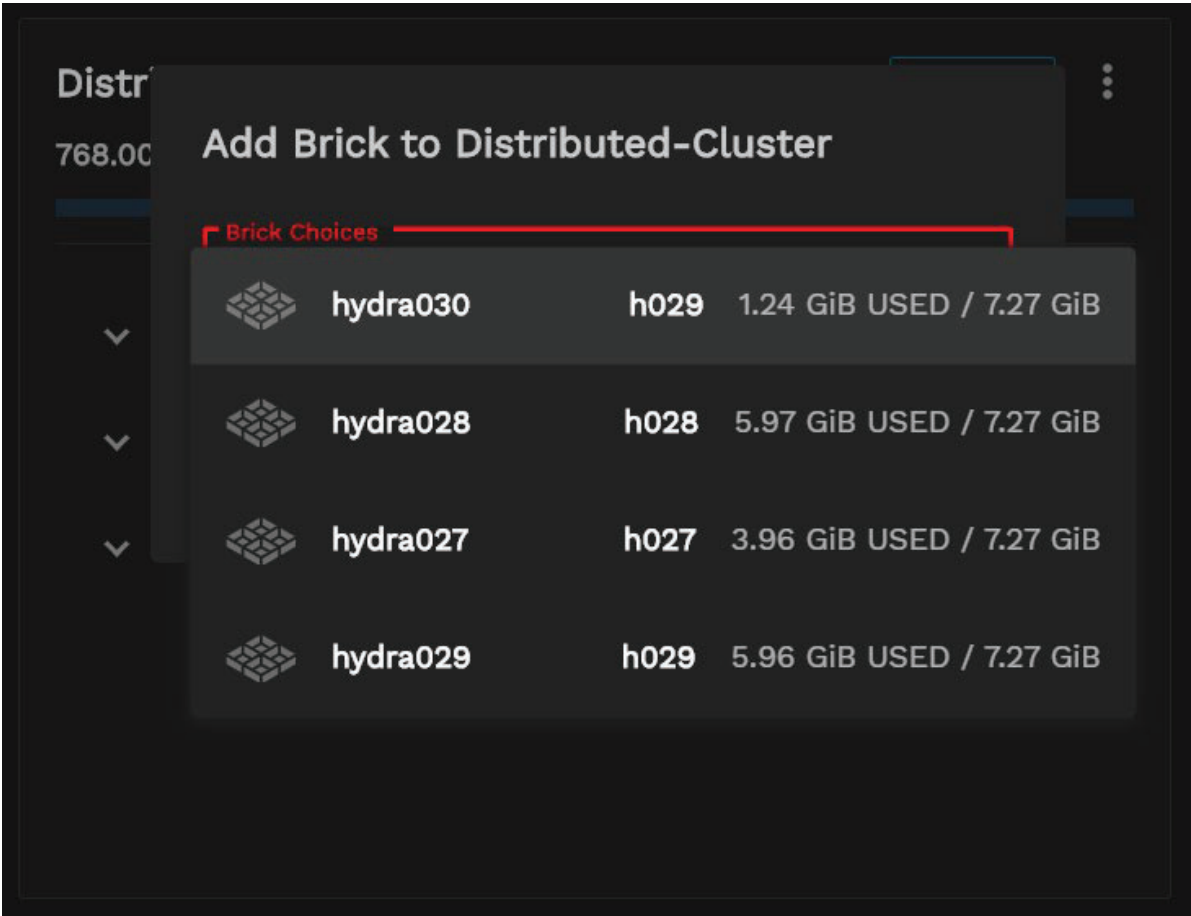


Add a brick to a Distributed Cluster

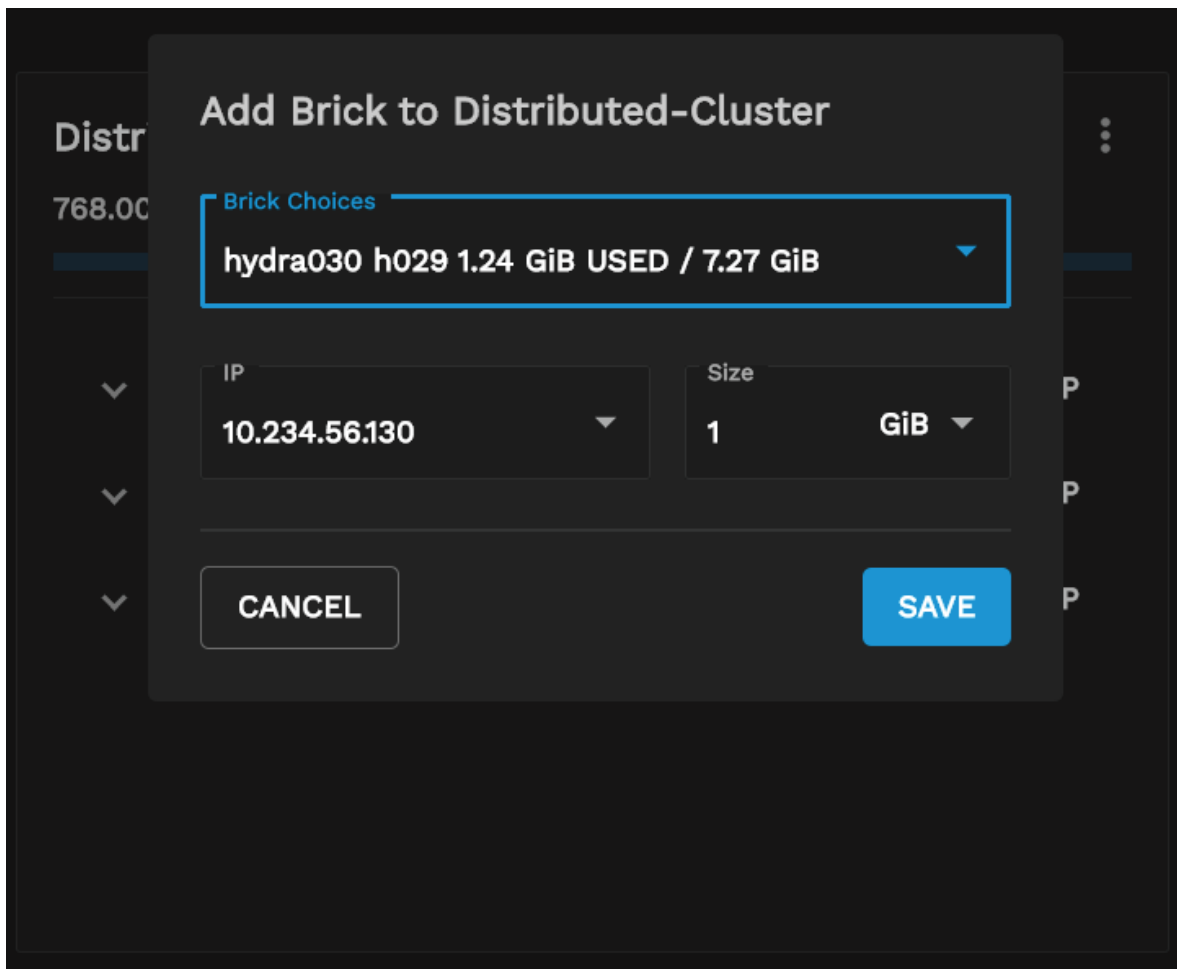
Click the  icon on the cluster overview card and select the **+ Add Brick** option to open the **Add Brick to Distributed-Cluster** menu.



Click **Brick Choices** to display the list of available systems.



Selecting a system displays options for the brick. iXsystems strongly recommends that you match the size of the existing bricks, but you can change this if required.



After you are satisfied with the settings, click **SAVE** to add the brick to the cluster.

Distributed-Cluster

768.00 KiB used / 3.00 GiB

Please wait

▼ Distributed-Cluster-distribute-0

Health: UP

▼ Distributed-Cluster-distribute-1

Health: UP

▼ Distributed-Cluster-distribute-2

Health: UP

After adding the new brick, the cluster card reflects the change.

Distributed-Cluster

1.00 MiB used / 4.00 GiB

▼ Distributed-Cluster-distribute-0

Health: UP

▼ Distributed-Cluster-distribute-1

Health: UP

▼ Distributed-Cluster-distribute-2

Health: UP


▼ Distributed-Cluster-distribute-3

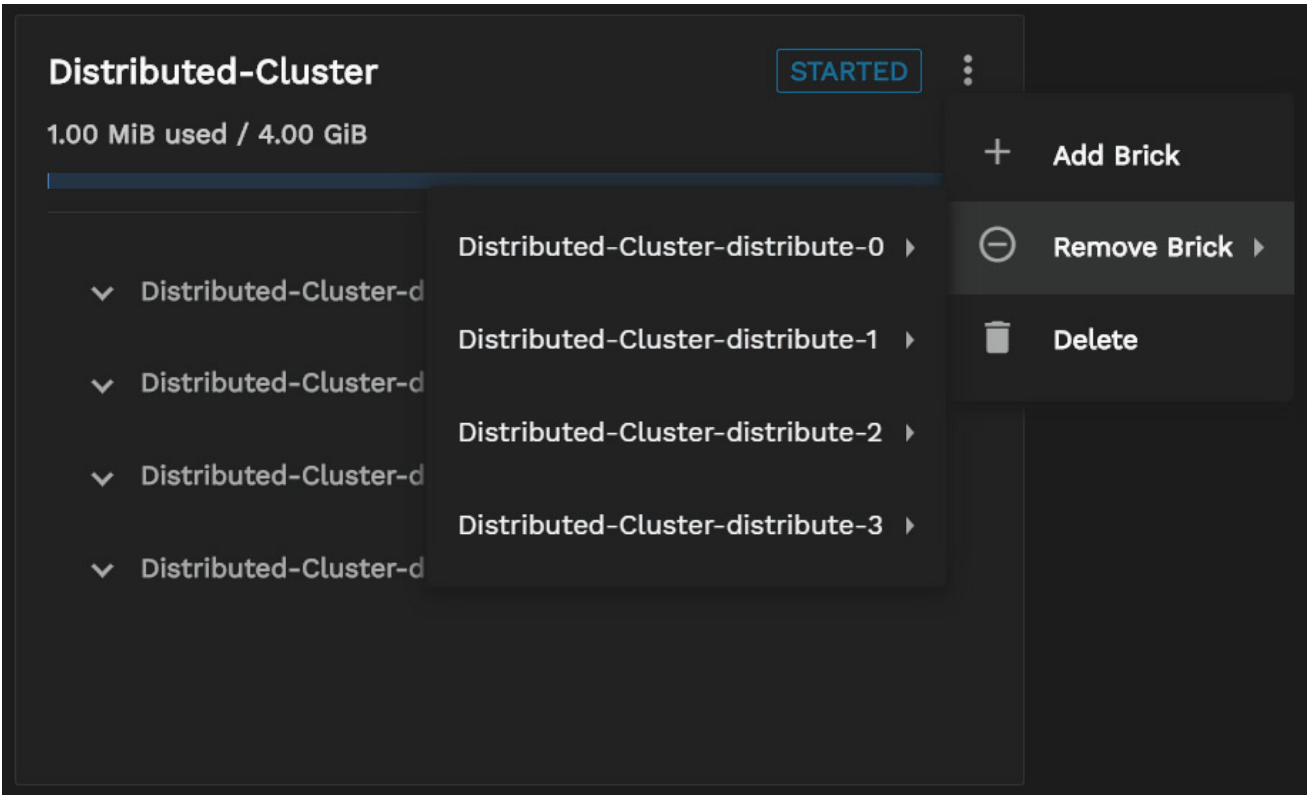
Health: UP

Removing a brick in a Distributed Cluster

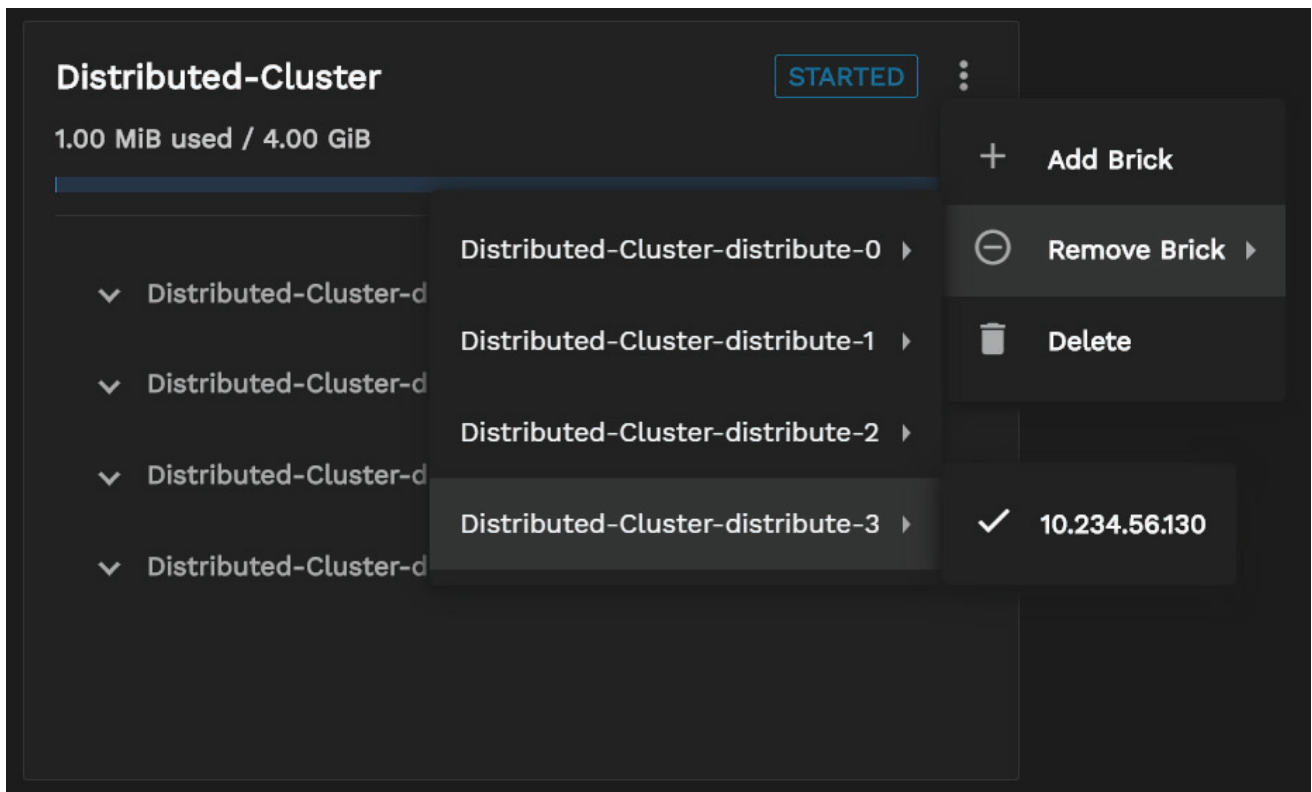
This option is only available if a cluster has four or more bricks.

This feature is not yet fully implemented.

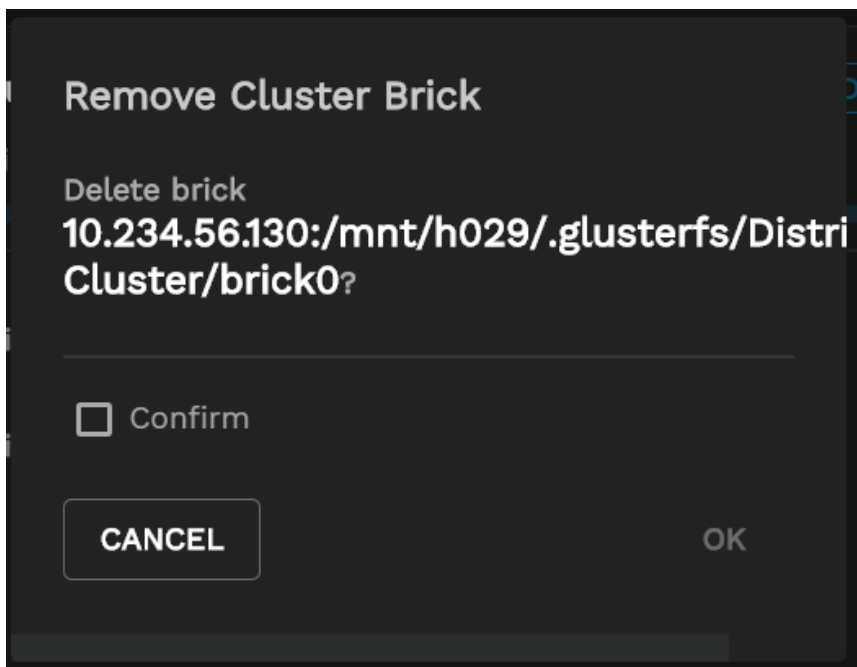
Click the  icon on the cluster overview card and hover your cursor over the **Remove Brick** option to display the list of bricks.



Hover your cursor over the listed items to display their bricks. Click on the IP to remove the brick.

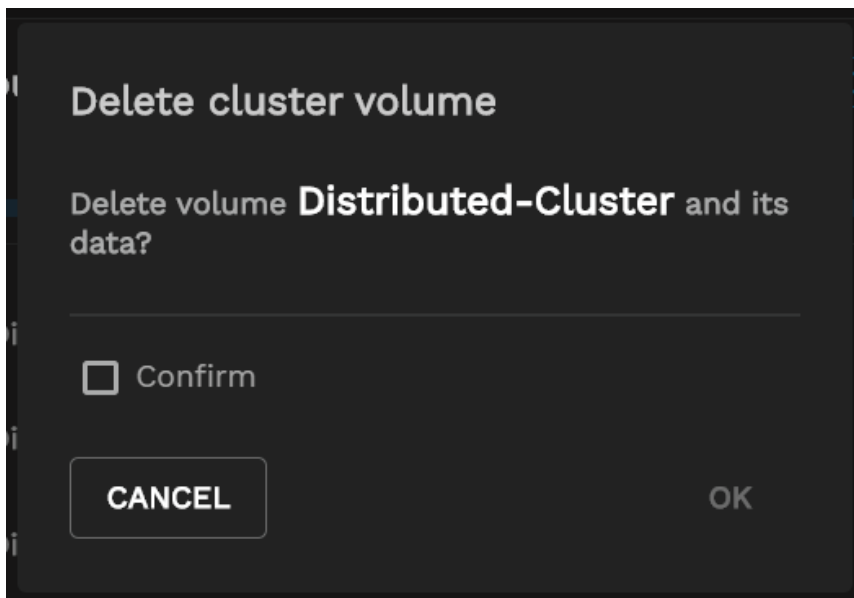


Check the **Confirm** box, then click **OK** to remove the brick.



Deleting a Distributed Cluster

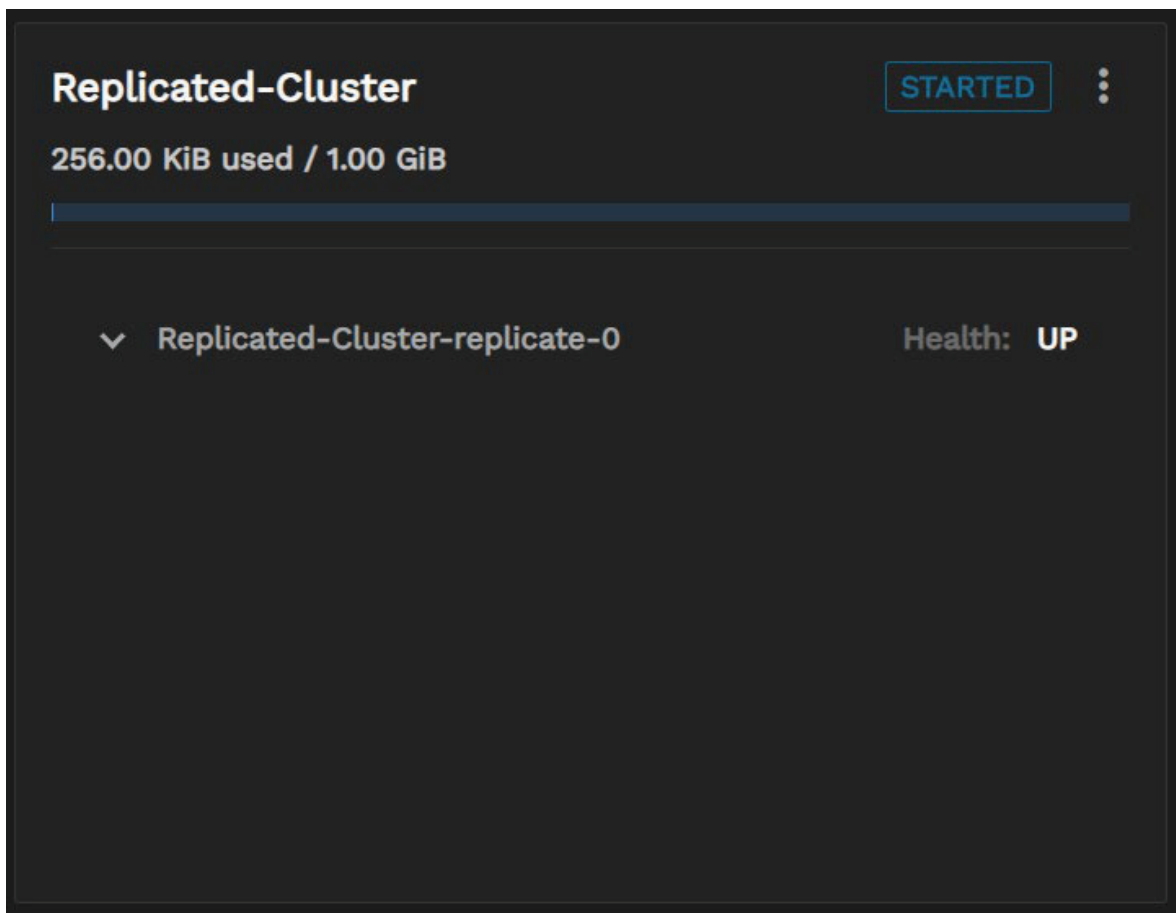
Click the  icon on the cluster overview card and select **Delete**.



Check the **Confirm** box, then click **OK** to delete the cluster.

On the **Dashboard**, click the  icon and select **Services**. Stop the **Gluster** service and clear the **START ON BOOT** checkbox.

☐ **Replicated**

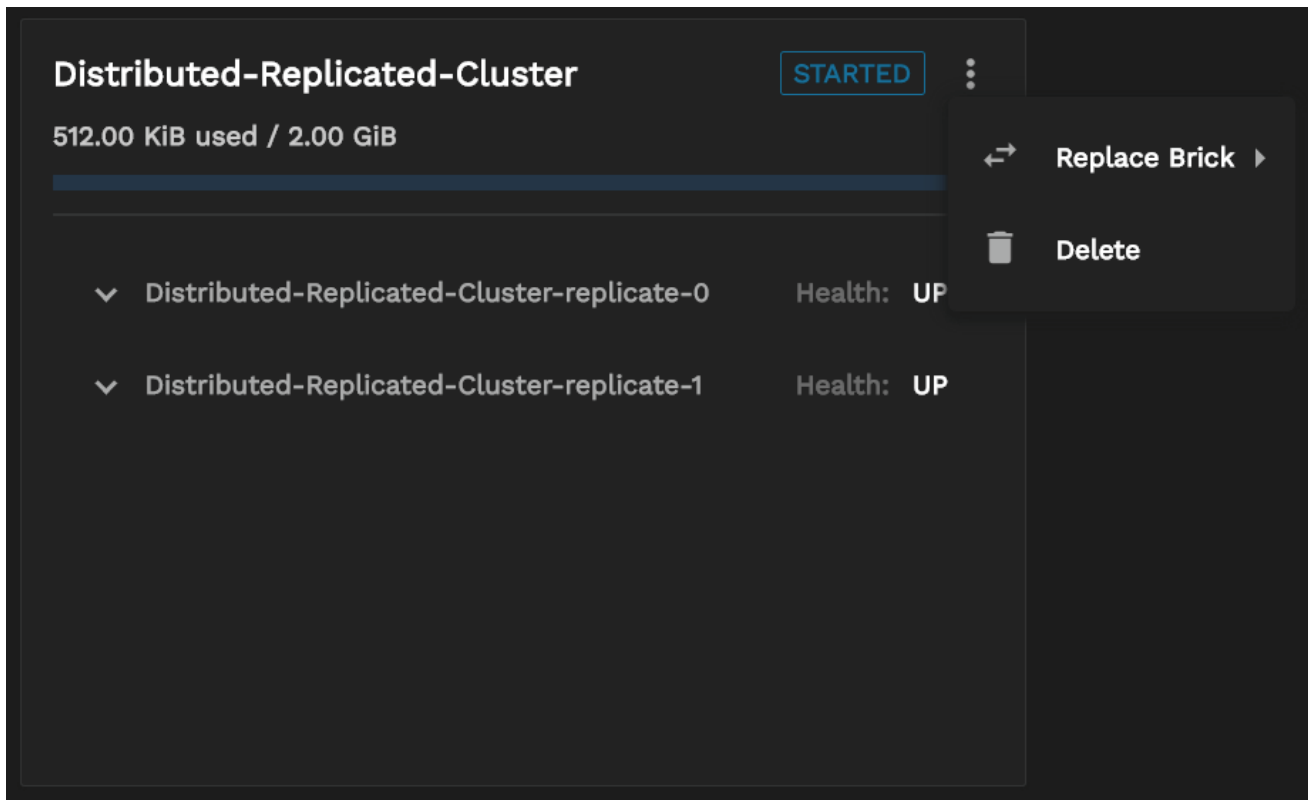


Replicated-Cluster volumes have two editing options: **Replace Brick** and **Delete**.

Replacing a Brick in a Replicated Cluster

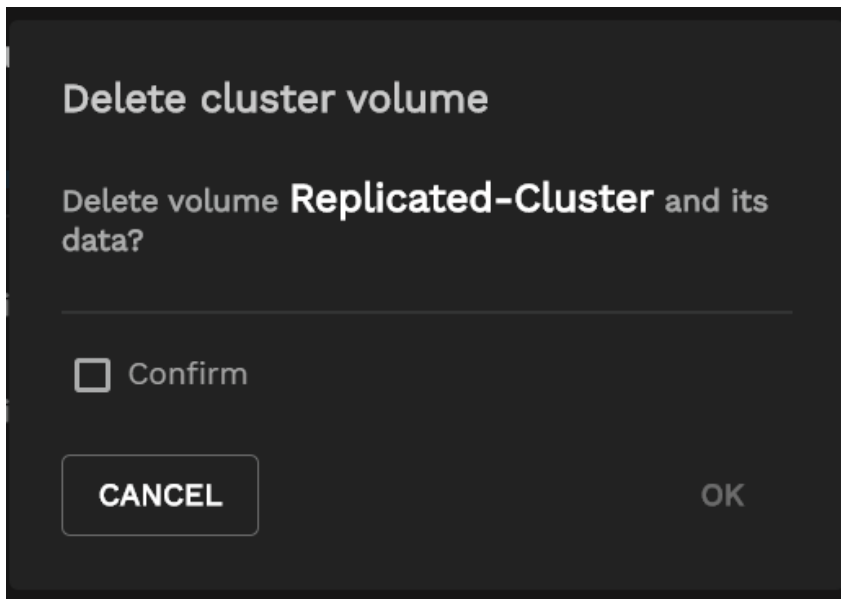


This feature is not yet fully implemented.



Deleting a Replicated Cluster

Click the  icon on the cluster overview card and select **Delete**.



Check the **Confirm** box, then click **OK** to delete the cluster.

On the **Dashboard**, click the  icon and select **Services**. Stop the **Gluster** service and clear the **START ON BOOT** checkbox.

☐ **Distributed Replicated**

Distributed-Replicated-Cluster

STARTED

512.00 KiB used / 2.00 GiB

▼ Distributed-Replicated-Cluster-replicate-0

Health: UP

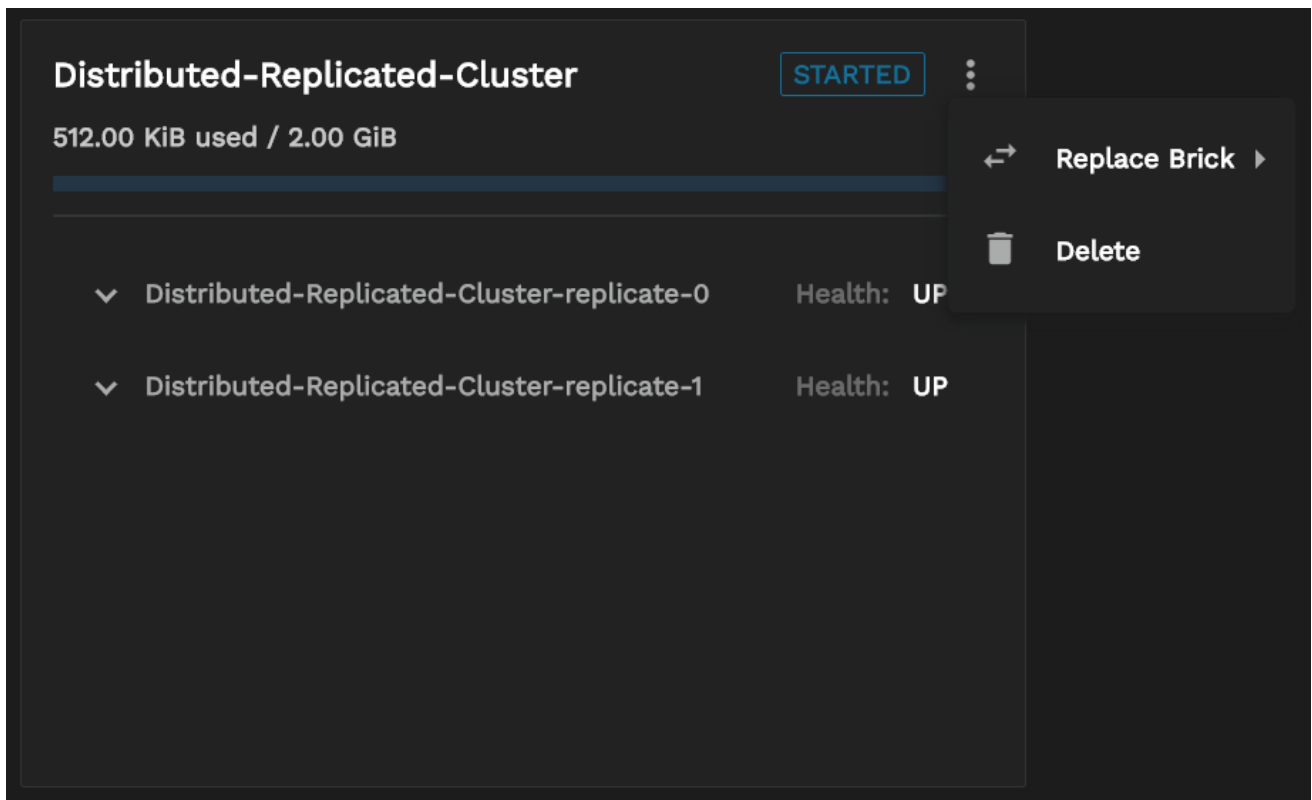
▼ Distributed-Replicated-Cluster-replicate-1

Health: UP

Distributed-Replicated-Cluster volumes have two editing options: **Replace Brick** and **Delete**.

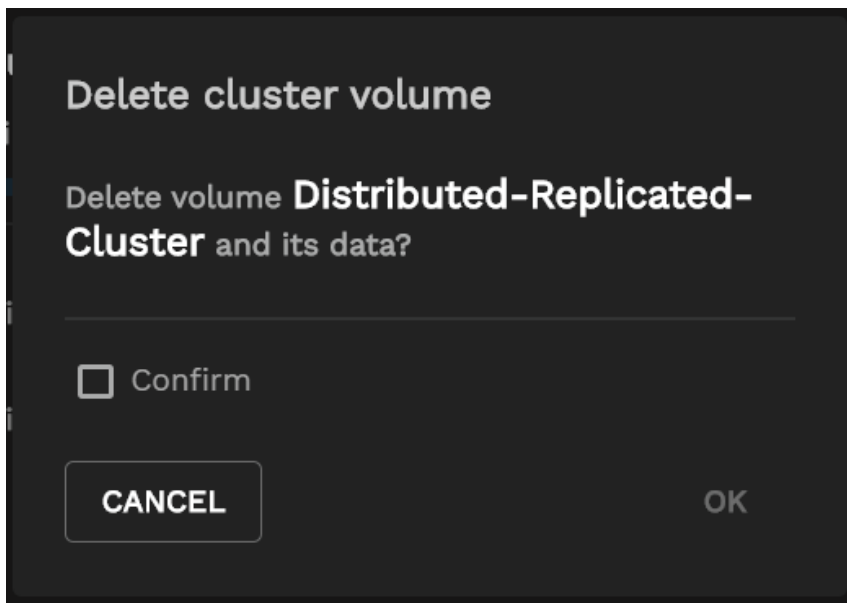
Replacing a Brick in a Distributed Replicated Cluster

This feature is not yet fully implemented.



Deleting a Distributed Replicated Cluster

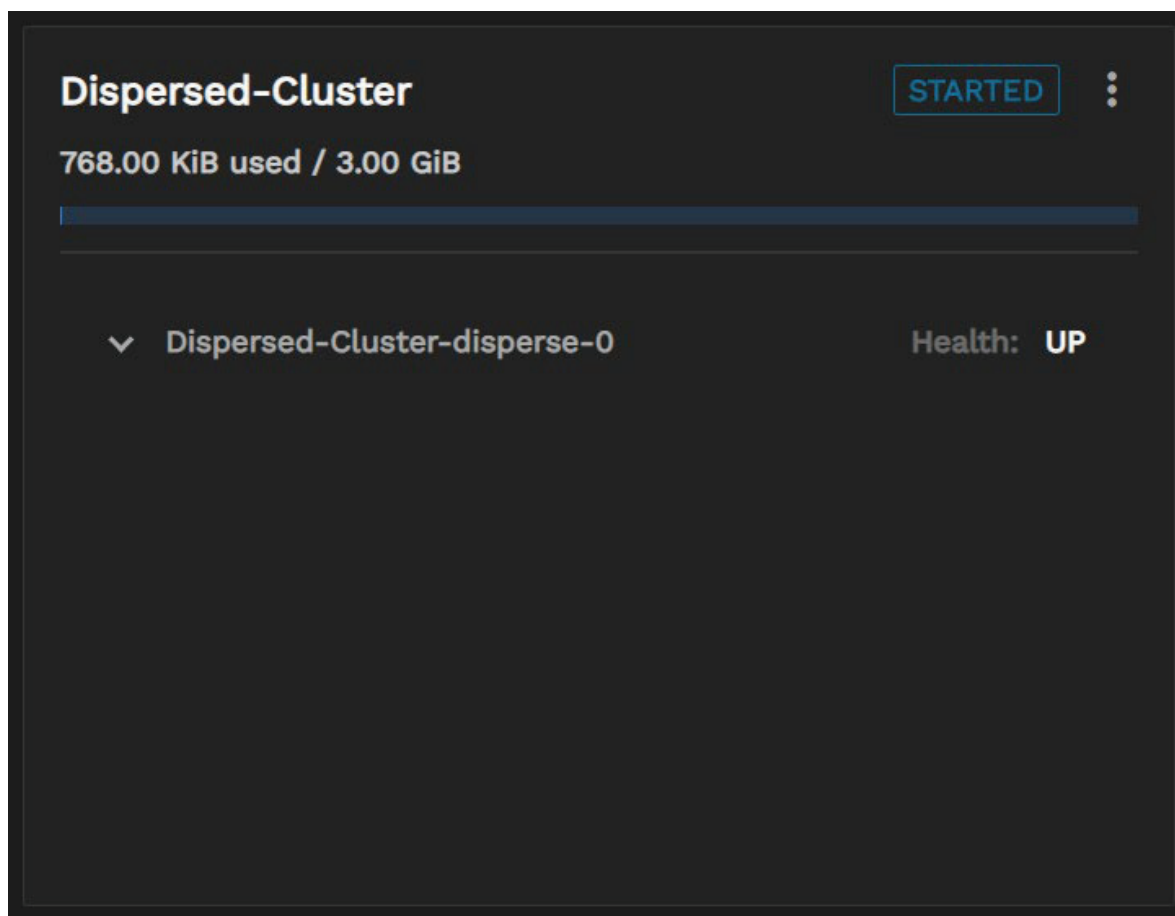
Click the  icon on the cluster overview card and select **Delete**.



Check the **Confirm** box, then click **OK** to delete the cluster.

On the **Dashboard**, click the  icon and select **Services**. Stop the **Gluster** service and clear the **START ON BOOT** checkbox.

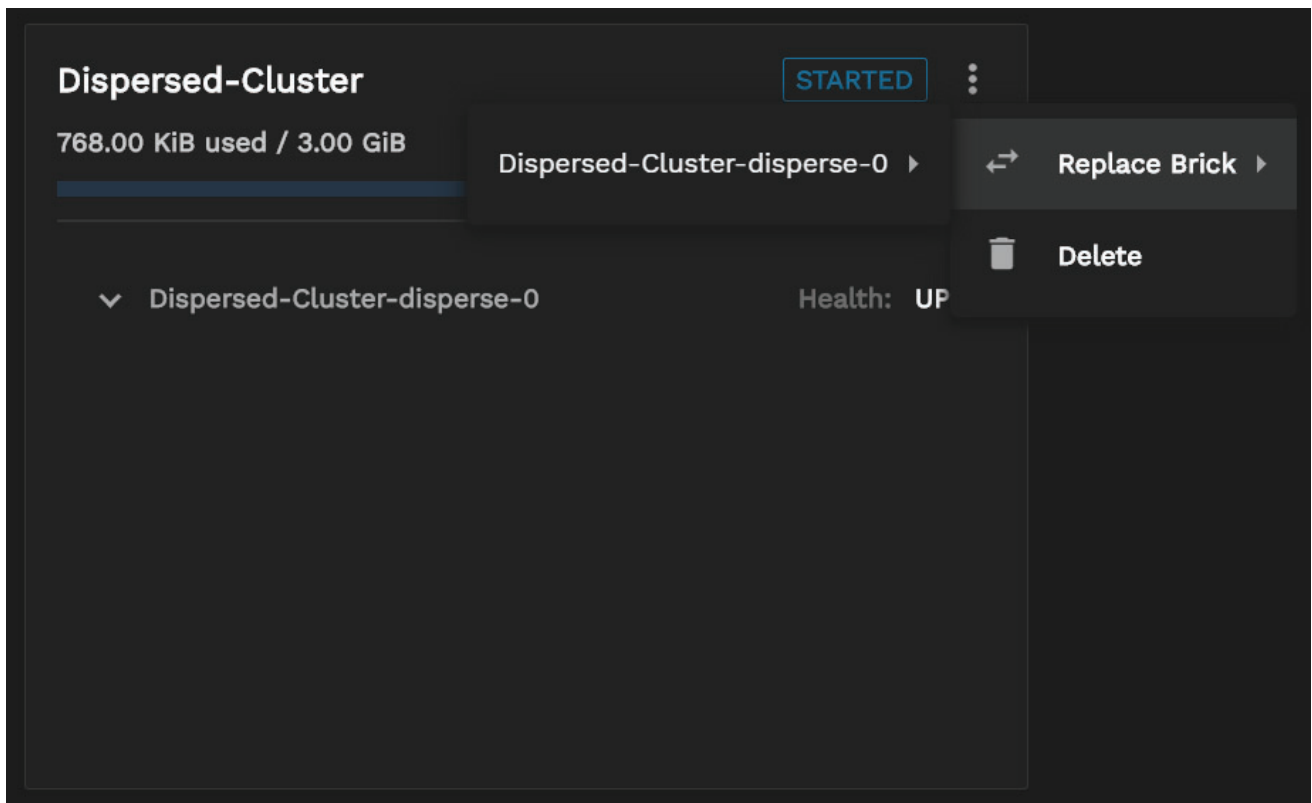
☐ **Dispersed**




Dispersed-Cluster volumes have two editing options: **Replace Brick** and **Delete**.

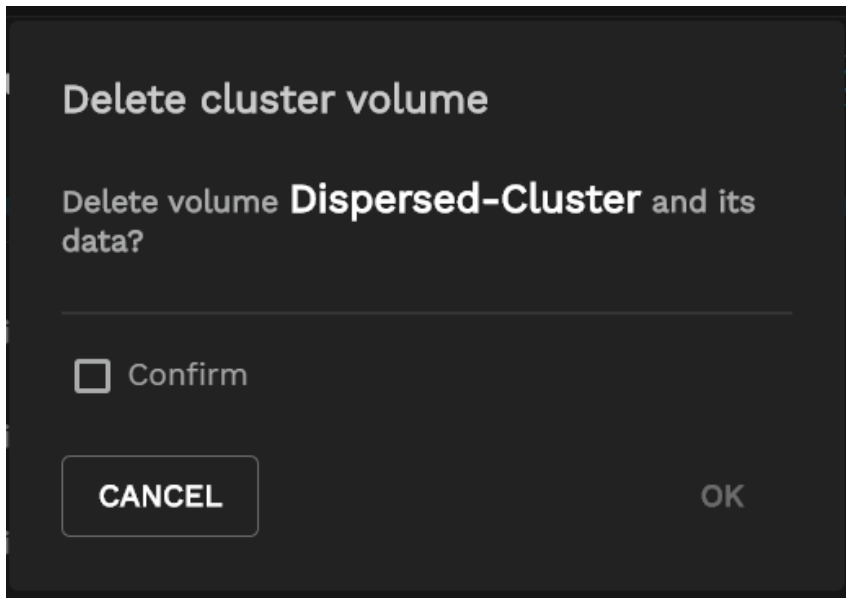
Replacing a Brick in a Dispersed Cluster

This feature is not yet fully implemented.



Deleting a Dispersed Cluster

Click the  icon on the cluster overview card and select **Delete**. A confirmation box displays and you must confirm the deletion to proceed.



Check the **Confirm** box, then click **OK** to delete the cluster.

On the **Dashboard**, click the  icon and select **Services**. Stop the **Gluster** service and clear the **START ON BOOT** checkbox.

☐ Distributed Dispersed

iXsystems has not implemented Distributed dispersed volumes at this time.

9.3 - Mounting Clustered Volumes

Manually Mounting Volumes

Install the glusterfs client for your Linux distribution first, consult with your systems package documentation on specific steps to start that process.

To mount a volume, use the following command:

```
mount -t glusterfs HOSTNAME-OR-IPADDRESS:/VOLNAME MOUNTDIR
```

For example:

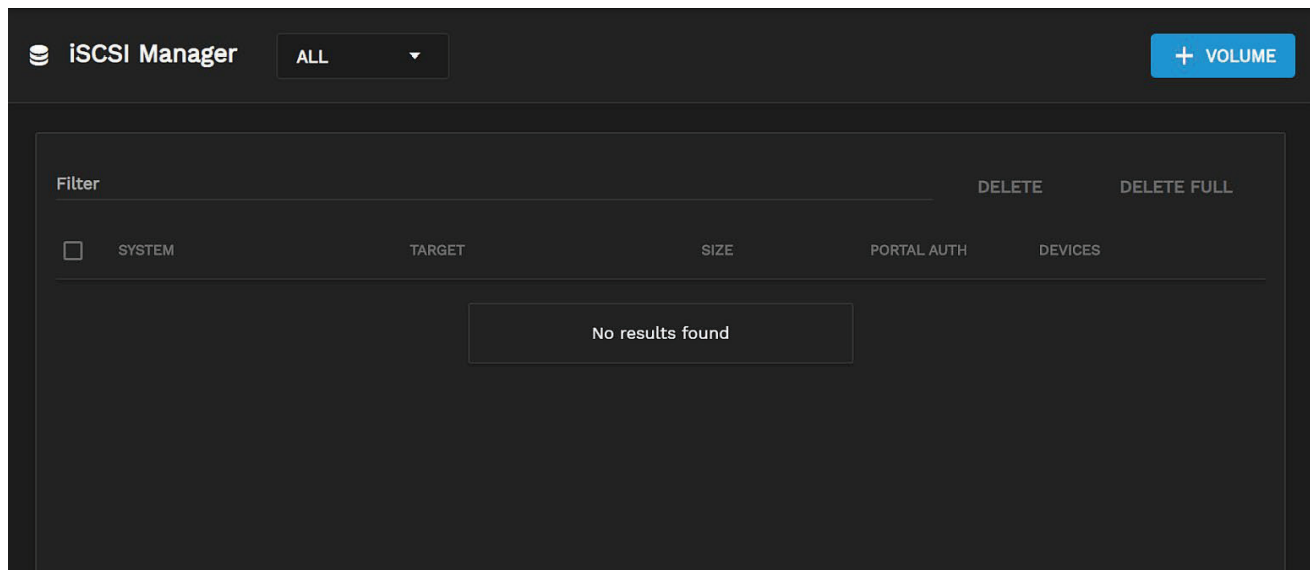
```
mount -t glusterfs server1:/test-volume /mnt/glusterfs
```

If you are not able to mount the volume for some reason and want to debug further check -
/var/log/glusterfs/mnt-mountdir.log. In this case /var/log/glusterfs/mnt-glusterfs.log See <http://gluster.org/> for additional references.

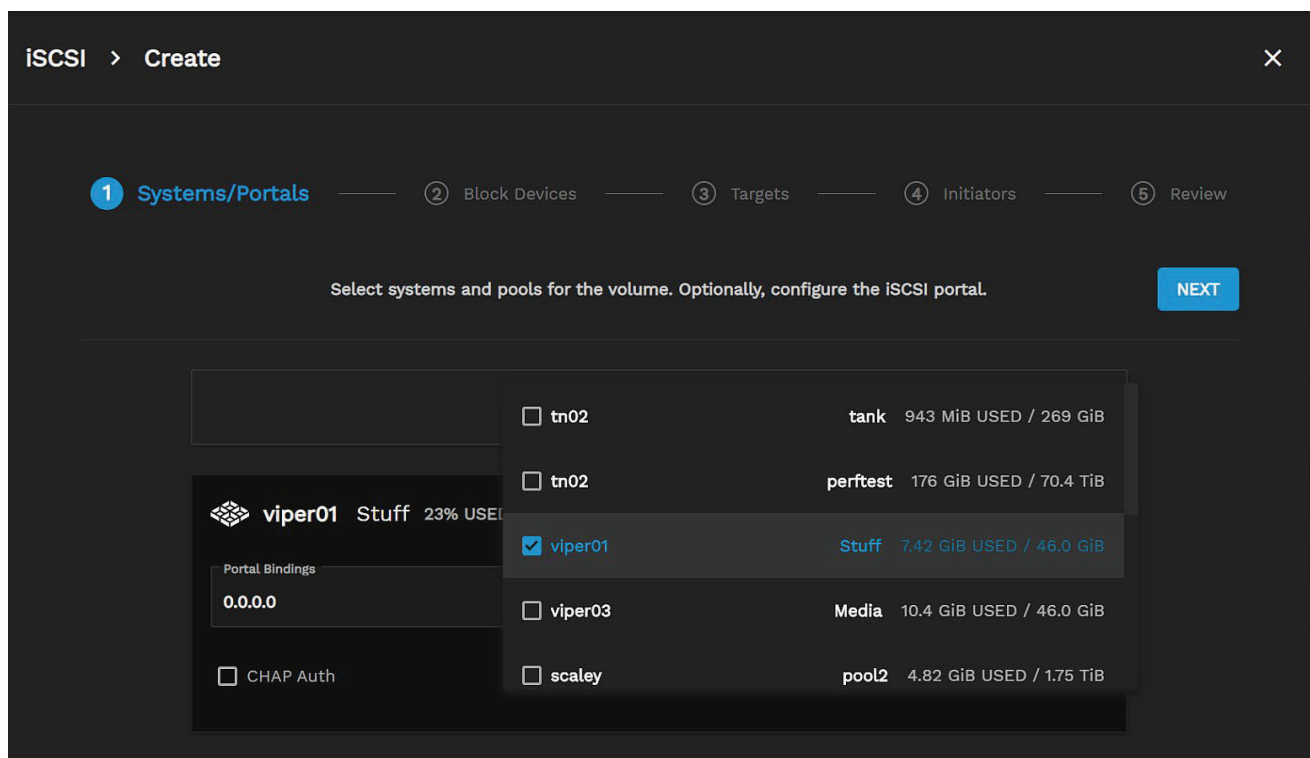
10 - iSCSI Volume Management

iSCSI management is a brand new feature in TrueCommand 2.0. Always back up any data intended for storage or sharing!

Open the **iSCSI Manager** page by clicking the icon on the top bar.



Begin creating an iSCSI volume by clicking **+ Volume**. After the **iSCSI Manager** page opens, click **+ Add System Pool** and select a pool or multiple pools.



Click **Next**.

Click **+ Block Devices** to add block devices. The **Count** field creates a batch of iSCSI datastores with identical settings in the number specified.

iSCSI > Create ×

1 Systems/Portals — 2 Block Devices — 3 Targets — 4 Initiators — 5 Review

BACK Configure the number and sizes of the block devices. NEXT

Block Device Group

Name

blockdevice

Size

1 GiB

Count

1

Volblocksize

512

☐ Xen

CANCEL SAVE

Click **SAVE** when finished, and then click **NEXT**.

Click **+ Target** and name the target.

iSCSI > Create ×

1 Systems/Portals — 2 Block Devices — 3 Targets — 4 Initiators — 5 Review

BACK Create target groups and map block devices to them. NEXT

blockdevice

+

Target

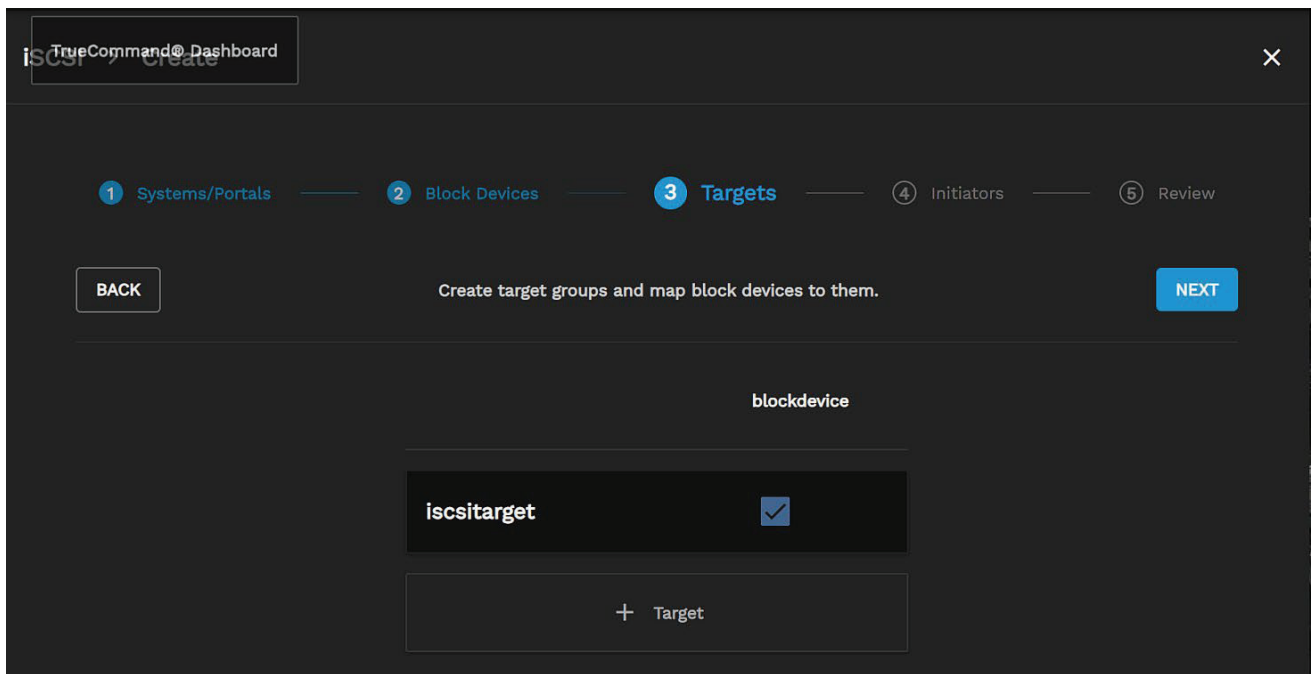
Name

iscsitarget

CANCEL SAVE

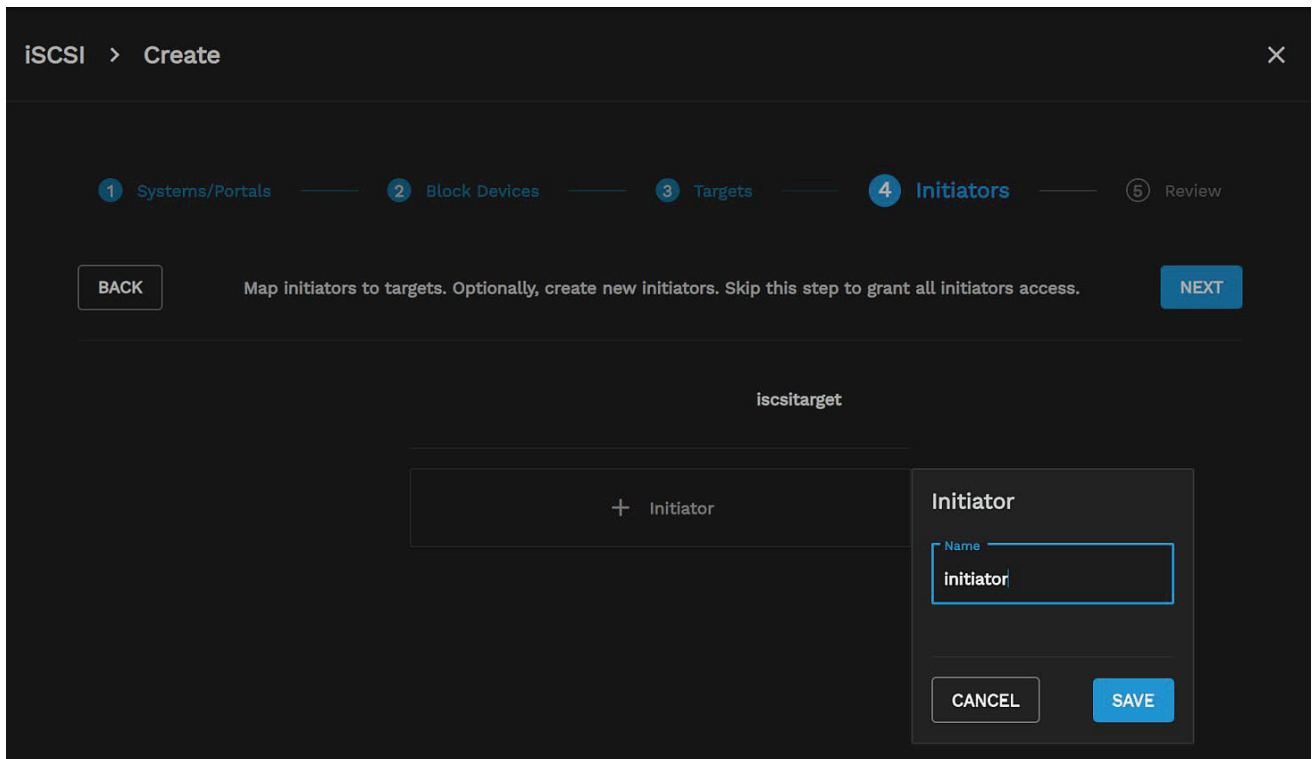
Click **SAVE** when finished and then click **NEXT**.

Click the checkbox to assign the target to the block device.



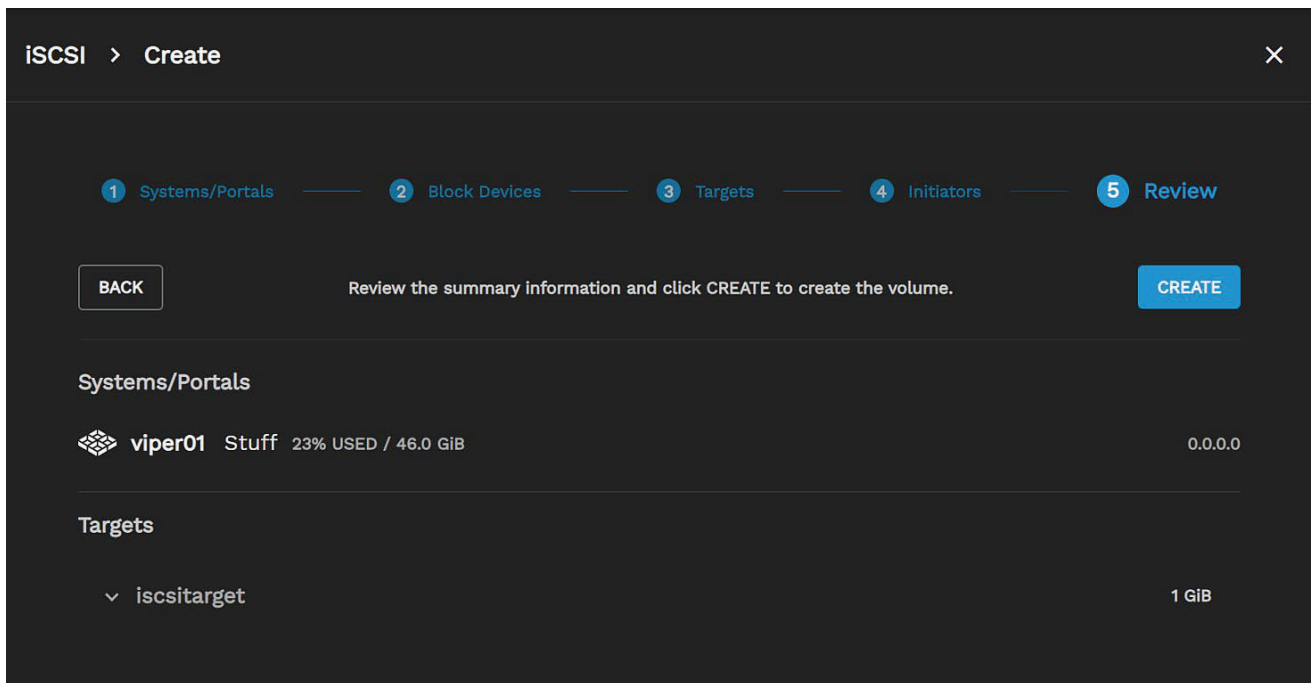
Click **NEXT**.

By default, TrueCommand grants target access to all initiators. To change this, click **+ Initiator**. Name the new initiator and click the checkbox to assign it to the target.

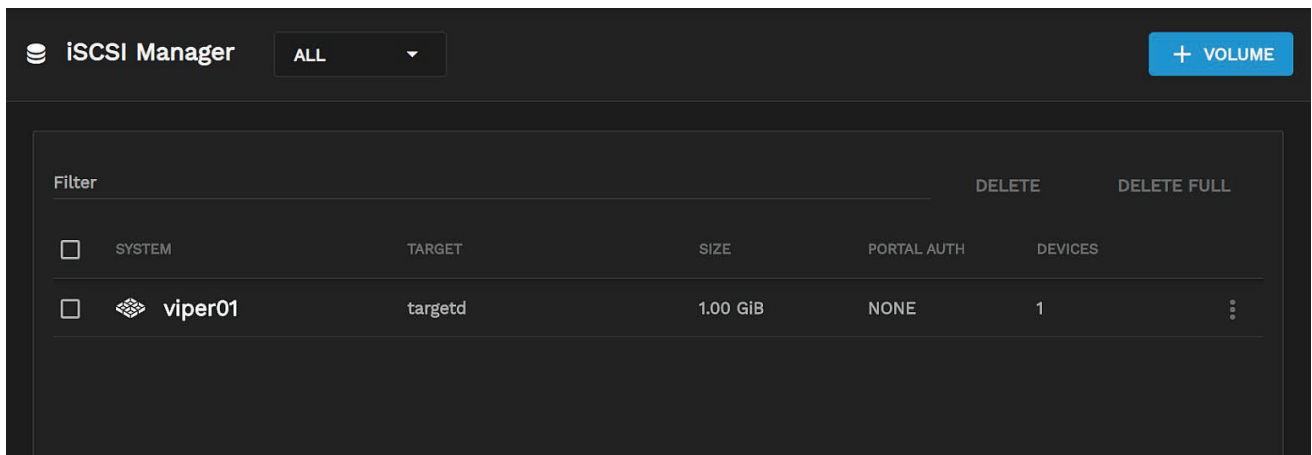


Click **NEXT**.

Review the configuration and click **Create**.



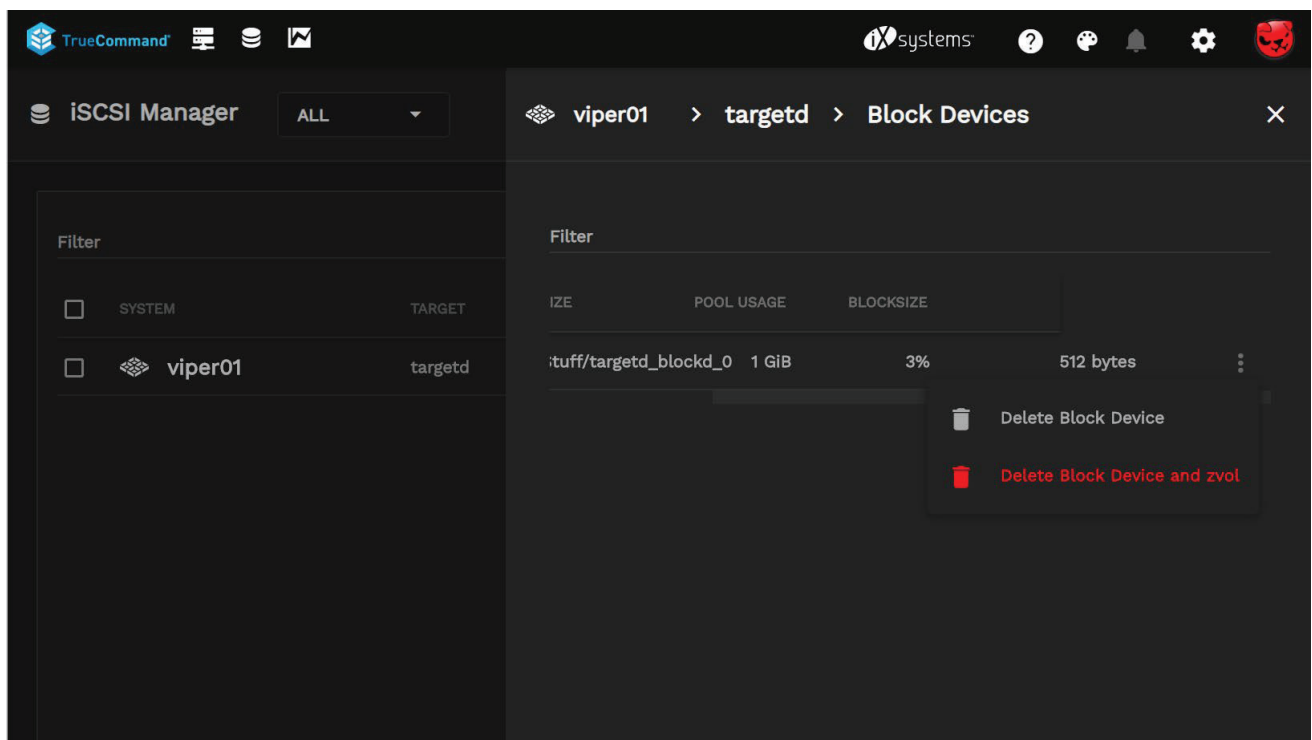
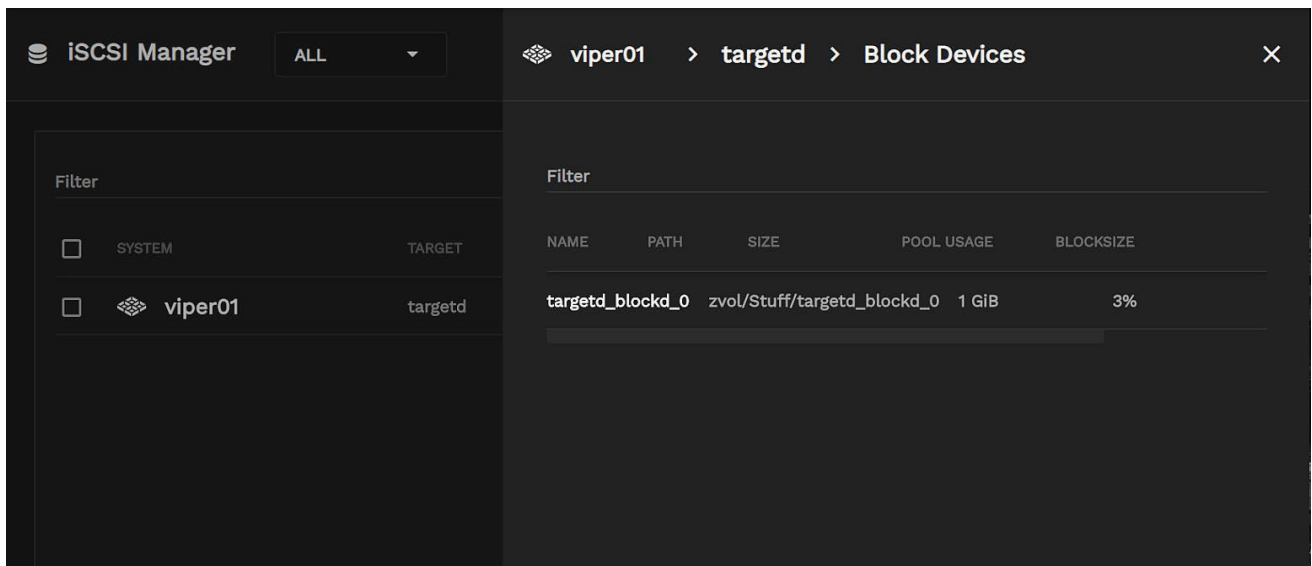
TrueCommand creates the iSCSI volume on the TrueNAS system and adds it to the iSCSI Manager.



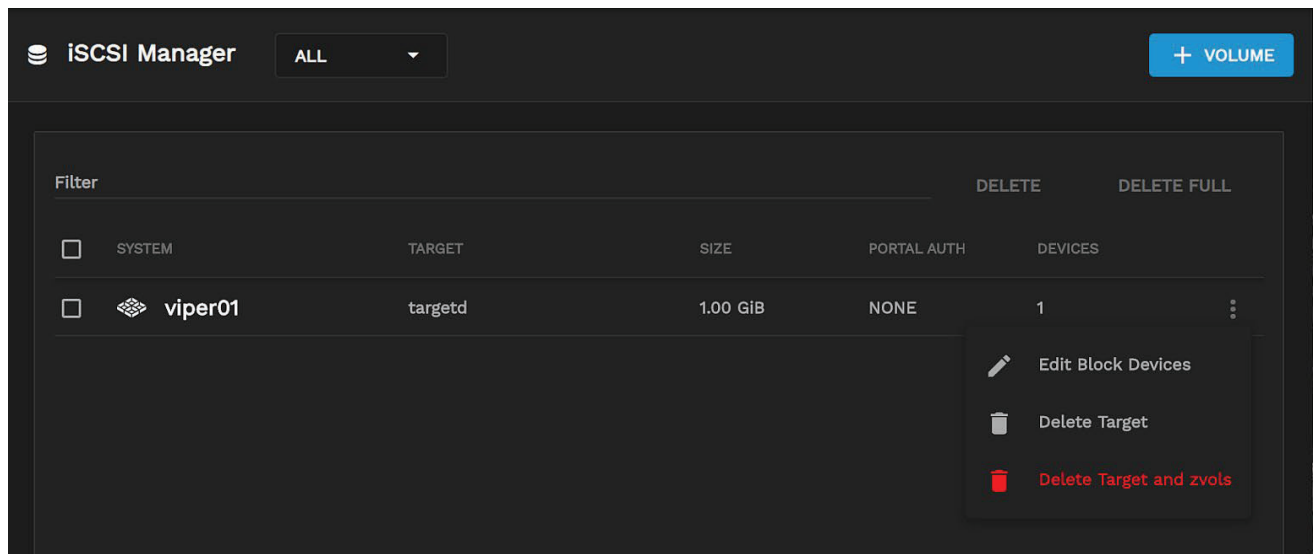
Using the TrueNAS web interface to update iSCSI settings takes approximately five minutes to resync with TrueCommand.

Deleting a Share

To delete a block device, click the ☐ icon to open the options, select **Edit**, then click the ☐ icon in the pop-out panel.



To delete the target click the ☐ icon and select **Delete Target**. To delete everything click the ☐ icon and select **Deleting Target and zvols** which is the full cleanup.



TrueCommand cannot delete initiators and init groups because they might be tied to multiple targets. To remove these settings, delete them from each TrueNAS system.

11 - Recommendations

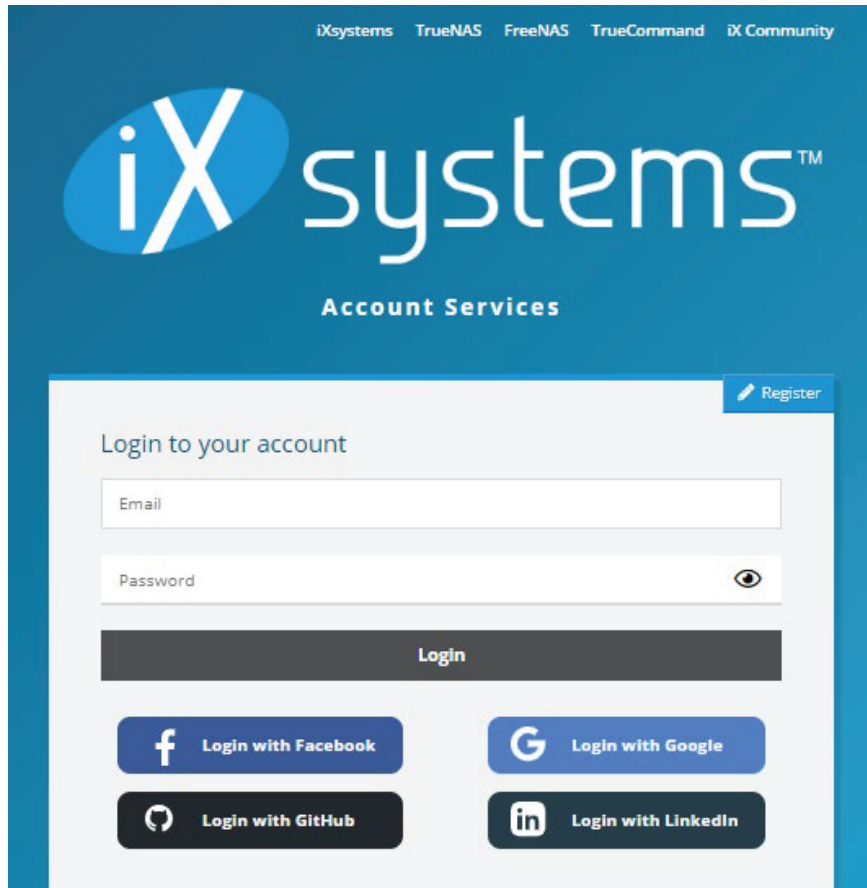
User-created recommendations are provided here, but be aware these are provided “as-is” and might not be officially supported by iXsystems, Inc.

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.

11.1 - TrueCommand Cloud Security

The iX Portal

The [iXsystems Account Services Portal](#) is an easy to use site to manage TrueCommand Cloud Subscriptions and TrueNAS Mini Warranties.



The iX Portal and TrueCommand Cloud use several security solutions to safeguard the application and connections.


- [OAuth](#) (Open Authorization) is an open standard for access rights and is a way for individuals on the Internet to grant websites or applications access to their information on another website without divulging a password. Commonly, OAuth provides clients secure access to server resources on behalf of a resource owner. It is a process for site owners to authorize third-party access to their server without providing credentials.
- [WireGuard](#) is an open-source communication protocol that implements encrypted virtual private networks (VPNs). WireGuard is designed to be easy to use, offer high speed performance, and have a low attack surface. WireGuard is an alternative to IPsec and OpenVPN tunneling protocols.
- [Two Factor Auth](#) (2FA) is a form of Multi-Factor Authentication method. 2FA is an extra layer of security to validate that an individual trying to gain access to an online account is actually who they say they are. A typical 2FA use case begins with a user entering their username and a password. Next, they are required to provide another piece of information. This second 'factor' could come from one of these categories: Something you know, Something you have, or Something you are. 2FA allows for one of those factors to be compromised and still prevent attackers from gaining access.

The iX Portal has the ability to use OAuth in place of a regular login and can utilize Two Factor Auth (2FA) if your OAuth provider provides that service.

The iX Portal also has email-based 2FA verification systems for sensitive operations to accounts.

TrueCommand Cloud services requires 2 forms of authentication. A user must have their username and password credentials to log in, but this depends on obtaining the Wireguard Configuration for their Client from the iX Portal. Administrators can create as many configurations as needed. Client configurations should never be used on more than one machine. TrueCommand Cloud logins can be across multiple systems, but each client system should use its own configuration. Client access can be revoked at any time from within the iX Portal.

iXsystems TrueNAS FreeNAS TrueCommand iX Community



systems™

Account Services

[Back](#)

Service Details

Address	172.28.0.1
API Key	XZ7YbcQJ0w9Gbp2
Instance Status	healthy
Plan	TrueCommand - 1000 Drive Cloud Service
Plan State	active
Plan Pricing	\$199.99 / Month

Service Controls

[Modify Subnet](#)

[Request Support](#)

WireGuard Client Access

Show 10 entries Search:

Nickname	Date Added	Approved
<input checked="" type="checkbox"/> Ops-Workstation	Sep-25-2020 15:24	Yes

Showing 1 to 1 of 1 entries Previous 1 Next

[Select All](#)

[Clear Selection](#)

[Approve Selected ✓](#)

[Delete Selected ✕](#)

Create Access Client

[Add](#)

Service Administration

Your plan will automatically renew on 2020-10-25.

[Edit Billing Information](#)

[Cancel Subscription](#)

By using this site you agree to the [iXsystems EULA](#) and [Privacy Policy](#)
2020 © iXsystems Inc • [Website Support](#)

12 - API Guide

TrueCommand API documentation is available from the web interface by opening the user menu and clicking **API**.

A static build of this version's API documentation is also provided [here](#).

13 - Notices

13.1 - TrueCommand SaaS Agreement

Software as a Service Agreement

This Software as a Service Agreement (this “**Agreement**”) is a legally binding agreement between you (“**you**” or “**Customer**”) and iXsystems, Inc., a Delaware corporation (“**Provider**”). Provider and Customer may be referred to herein collectively as the “**Parties**” or individually as a “**Party**.” This Agreement governs your access to specific products, applications, tools, services and features that Provider makes available to you under an “**Order**,” as such term is hereafter defined.

WHEREAS, Provider provides access to the Services to its customers; and

WHEREAS, Customer desires to access the Services, and Provider desires to provide Customer access to the Services, subject to the terms and conditions of this Agreement.

WHEREAS, Customer’s right to access and use the Services, is expressly conditioned on your acceptance of this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants, terms, and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. Definitions.

(a) “**Aggregated Statistics**” means data and information related to Customer’s use of the Services that is used by Provider in an aggregate and anonymized manner, including to compile statistical and performance information related to the provision and operation of the Services.

(b) “**Authorized User**” means Customer’s employees, consultants, contractors, clients, and agents (i) who are authorized by Customer to access and use the Services under the rights granted to Customer pursuant to this Agreement and (ii) for whom access to the Services has been purchased hereunder.

(c) “**Customer Data**” means, other than Aggregated Statistics, information, data, and other content, in any form or medium, that is submitted, posted, or otherwise transmitted by or on behalf of Customer or an Authorized User through the Services.

(d) “**Documentation**” means Provider’s end user documentation relating to the Services available at www.truenas.com/docs/.

(e) “**Effective Date**” means the earliest of (i) the date you click I Agree; (ii) the date you access the Services; or (iii) the effective date set forth in the Order.

(f) “**Order**” means any order form or other ordering document, including any online subscription order specifying the level of the Services to be provided and the associated fees, and any addenda and supplements thereto. By entering into any Order, you agree to be bound by the terms of this Agreement.

(g) “**Provider IP**” means the Services, the Documentation, and any and all intellectual property provided to Customer or any Authorized User in connection with the foregoing. For the avoidance of doubt, Provider IP includes Aggregated Statistics and any information, data, or other content derived from Provider’s monitoring of Customer’s access to or use of the Services, but does not include Customer Data.

(h) “**Services**” means the products, applications, tools, services and features that Provider makes available to you as the software-as-a-service offering described in the Order.

(i) “**Third-Party Materials**” means materials and information, in any form or medium, including any open-source

or other software, services (including, but not limited to, software as a service), documents, data, content, specifications, products, equipment, or components of or relating to the Services that are not proprietary to Provider.

2. Access and Use.

(a) Provision of Access. Subject to and conditioned on Customer's payment of Fees and compliance with all other terms and conditions of this Agreement, Provider hereby grants Customer a non-exclusive, non-transferable (except in compliance with Section 12(g)) right to access and use the Services during the Term, solely for use by Authorized Users in accordance with the terms and conditions herein. Such use is limited to Customer's legitimate business purposes. Provider shall provide to Customer the necessary passwords and network links or connections to allow Customer to access the Services.

(b) Documentation License. Subject to the terms and conditions contained in this Agreement, Provider hereby grants to Customer a non-exclusive, non-sublicensable, non-transferable (except in compliance with Section 12(g)) license to use the Documentation during the Term solely for Customer's internal business purposes in connection with its use of the Services.

(c) Use Restrictions. Customer shall not use the Services for any purposes beyond the scope of the access granted in this Agreement. Customer shall not at any time, directly or indirectly, and shall not permit any Authorized Users to: (i) copy, modify, or create derivative works of the Services or Documentation, in whole or in part; (ii) rent, lease, lend, sell, license, assign, distribute, publish, transfer, or otherwise make available the Services or Documentation; (iii) reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to any software component of the Services, in whole or in part; (iv) remove any proprietary notices from the Services or Documentation; or (v) use the Services or Documentation in any manner or for any purpose that infringes, misappropriates, or otherwise violates any intellectual property right or other right of any person, or that violates any applicable law.

(d) Reservation of Rights. Provider reserves all rights not expressly granted to Customer in this Agreement. Except for the limited rights and licenses expressly granted under this Agreement, nothing in this Agreement grants, by implication, waiver, estoppel, or otherwise, to Customer or any third party any intellectual property rights or other right, title, or interest in or to the Provider IP.

(e) Suspension. Notwithstanding anything to the contrary in this Agreement, Provider may temporarily suspend Customer's and any Authorized User's access to any portion or all of the Services if: (i) Provider reasonably determines that (A) there is a threat or attack on any of the Provider IP; (B) Customer's or any Authorized User's use of the Provider IP disrupts or poses a security risk to the Provider IP or to any other customer or vendor of Provider; (C) Customer, or any Authorized User, is using the Provider IP for fraudulent or illegal activities; (D) subject to applicable law, Customer has ceased to continue its business in the ordinary course, made an assignment for the benefit of creditors or similar disposition of its assets, or become the subject of any bankruptcy, reorganization, liquidation, dissolution, or similar proceeding; or (E) Provider's provision of the Services to Customer or any Authorized User is prohibited by applicable law; (ii) any vendor of Provider has suspended or terminated Provider's access to or use of any third-party services or products required to enable Customer to access the Services; or (iii) in accordance with Section 5(a)(iii) (any such suspension described in subclause (i), (ii), or (iii), a "**Service Suspension**"). Provider shall use commercially reasonable efforts to provide written notice of any Service Suspension to Customer and to provide updates regarding resumption of access to the Services following any Service Suspension. Provider shall use commercially reasonable efforts to resume providing access to the Services as soon as reasonably possible after the event giving rise to the Service Suspension is cured. Provider will have no liability for any damage, liabilities, losses (including any loss of data or profits), or any other consequences that Customer or any Authorized User may incur as a result of a Service Suspension.

(f) Aggregated Statistics. Notwithstanding anything to the contrary in this Agreement, Provider may collect and compile Aggregated Statistics. As between Provider and Customer, all right, title, and interest in Aggregated Statistics, and all intellectual property rights therein, belong to and are retained solely by Provider. Customer acknowledges that Provider may compile Aggregated Statistics based on Customer Data input into the Services. Customer agrees that Provider may (i) make Aggregated Statistics publicly available in compliance with applicable law, and (ii) use Aggregated Statistics to the extent and in the manner permitted under applicable law; provided that such Aggregated Statistics do not identify Customer or Customer's Confidential Information.

3. Customer Responsibilities.

(a) General. Customer is responsible and liable for all uses of the Services and Documentation resulting from access provided by Customer, directly or indirectly, whether such access or use is permitted by or in violation of this Agreement. Without limiting the generality of the foregoing, Customer is responsible for all acts and omissions of Authorized Users, and any act or omission by an Authorized User that would constitute a breach of this Agreement if taken by Customer will be deemed a breach of this Agreement by Customer. Customer shall use reasonable efforts to make all Authorized Users aware of this Agreement's provisions as applicable to such Authorized User's use of the Services, and shall cause Authorized Users to comply with such provisions.

(b) Third-Party Materials. Provider may from time to time utilize Third-Party Materials in the provision of the Services. For purposes of this Agreement, such Third-Party Materials are subject to their own terms and conditions and the applicable flow-through provisions listed on www.ixsystems.com/support/, as amended. If Customer does not agree to abide by the applicable terms for any such Third-Party Materials, then Customer should not install or use the Services.

4. Service Levels and Support.

(a) Service Levels. Subject to the terms and conditions of this Agreement, Provider shall use commercially reasonable efforts to make the Services available in accordance with the service levels set out on the Order or as otherwise set forth in a separate Service Level Addendum.

(b) Support. The access rights granted hereunder entitle Customer to the support services described from time to time on Provider's website located at www.ixsystems.com/support/.

5. Fees and Payment.

(a) Fees. Customer shall pay Provider the fees ("**Fees**") as set forth in the Order, without offset or deduction. Customer shall make all payments hereunder in US dollars on or before the due date set forth on the Order. If Customer fails to make any payment when due, without limiting Provider's other rights and remedies, Provider may terminate this Agreement and Customer's and its Authorized Users' access to any portion or all of the Services, or suspend such access until such amounts are paid in full.

(b) Taxes. All Fees and other amounts payable by Customer under this Agreement are exclusive of taxes and similar assessments. Customer is responsible for all sales, use, and excise taxes, and any other similar taxes, duties, and charges of any kind imposed by any federal, state, or local governmental or regulatory authority on any amounts payable by Customer hereunder, other than any taxes imposed on Provider's income.

6. Confidential Information. From time to time during the Term, either Party may disclose or make available to the other Party information about its business affairs, products, confidential intellectual property, trade secrets, third-party confidential information, and other sensitive or proprietary information that is marked, designated, or otherwise identified as "confidential" (collectively, "**Confidential Information**"). Confidential Information does not include information that, at the time of disclosure is: (a) in the public domain; (b) known to the receiving Party at the time of disclosure; (c) rightfully obtained by the receiving Party on a non-confidential basis from a third party; or (d) independently developed by the receiving Party. The receiving Party shall not disclose the disclosing Party's Confidential Information to any person or entity, except to the receiving Party's employees who have a need to know the Confidential Information for the receiving Party to exercise its rights or perform its obligations hereunder. Notwithstanding the foregoing, each Party may disclose Confidential Information to the limited extent required (i) in order to comply with the order of a court or other governmental body, or as otherwise necessary to comply with applicable law, provided that the Party making the disclosure pursuant to the order shall first have given written notice to the other Party and made a reasonable effort to obtain a protective order; or (ii) to establish a Party's rights under this Agreement, including to make required court filings. On the expiration or termination of the Agreement, the receiving Party shall promptly return to the disclosing Party all copies, whether in written, electronic, or other form or media, of the disclosing Party's Confidential Information, or destroy all such copies and certify in writing to the disclosing Party that such Confidential Information has been destroyed. Each Party's obligations of non-disclosure with regard to Confidential Information are effective as of the Effective Date and will expire five years from the date first disclosed to the receiving Party; provided, however, with respect to any Confidential Information that constitutes a trade secret (as determined under applicable law), such obligations of non-disclosure will survive the termination or expiration of this Agreement for as long as such Confidential Information remains subject to trade secret protection under applicable law.

7. Intellectual Property Ownership; Feedback.

(a) Provider IP. Customer acknowledges that, as between Customer and Provider, Provider owns all right, title, and interest, including all intellectual property rights, in and to the Provider IP and, with respect to Third-Party Materials, the applicable third-party providers own all right, title, and interest, including all intellectual property rights, in and to the Third-Party Materials.

(b) Customer Data. Provider acknowledges that, as between Provider and Customer, Customer owns all right, title, and interest, including all intellectual property rights, in and to the Customer Data. Customer hereby grants to Provider a non-exclusive, royalty-free, worldwide license to reproduce, distribute, and otherwise use and display the Customer Data and perform all acts with respect to the Customer Data as may be necessary for Provider to provide the Services to Customer, and a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to reproduce, distribute, modify, and otherwise use and display Customer Data incorporated within the Aggregated Statistics.

(c) Feedback. If Customer or any of its employees or contractors sends or transmits any communications or materials to Provider by mail, email, telephone, or otherwise, suggesting or recommending changes to the Provider IP, including without limitation, new features or functionality relating thereto, or any comments, questions, suggestions, or the like ("**Feedback**"), Provider is free to use such Feedback irrespective of any other obligation or limitation between the Parties governing such Feedback. Customer hereby assigns to Provider on Customer's behalf, and on behalf of its employees, contractors and/or agents, all right, title, and interest in, and Provider is free to use, without any attribution or compensation to any party, any ideas, know-how, concepts, techniques, or other intellectual property rights contained in the Feedback, for any purpose whatsoever, although Provider is not required to use any Feedback.

8. Warranty Disclaimer.

(a) THE PROVIDER IP IS PROVIDED "AS IS" AND PROVIDER HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. PROVIDER SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. PROVIDER MAKES NO WARRANTY OF ANY KIND THAT THE PROVIDER IP, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, OPERATE WITHOUT INTERRUPTION, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR FREE.

9. Indemnification.

(a) Provider Indemnification.

(i) Provider shall indemnify, defend, and hold harmless Customer from and against any and all losses, damages, liabilities, costs (including reasonable attorneys' fees) ("**Losses**") incurred by Customer resulting from any third-party claim, suit, action, or proceeding ("**Third-Party Claim**") that the Services, or any use of the Services in accordance with this Agreement, infringes or misappropriates such third party's US patents, copyrights, or trade secrets, provided that Customer promptly notifies Provider in writing of the claim, cooperates with Provider, and allows Provider sole authority to control the defense and settlement of such claim.

(ii) If such a claim is made or appears possible, Customer agrees to permit Provider, at Provider's sole discretion, to (A) modify or replace the Services, or component or part thereof, to make it non-infringing, or (B) obtain the right for Customer to continue use. If Provider determines that neither alternative is reasonably available, Provider may terminate this Agreement, in its entirety or with respect to the affected component or part, effective immediately on written notice to Customer.

(iii) This Section 9(a) will not apply to the extent that the alleged infringement arises from: (A) use of the Services in combination with data, software, hardware, equipment, or technology not provided by Provider or authorized by Provider in writing; (B) modifications to the Services not made by Provider; (C) Customer Data ; or (D) Third-Party Materials.

(b) Customer Indemnification. Customer shall indemnify, hold harmless, and, at Provider's option, defend Provider from and against any Losses resulting from any Third-Party Claim that the Customer Data, or any use of the Customer Data in accordance with this Agreement, infringes or misappropriates such third party's intellectual property rights and any Third-Party Claims based on Customer's or any Authorized User's (i)

negligence or willful misconduct; (ii) use of the Services in a manner not authorized by this Agreement; (iii) use of the Services in combination with data, software, hardware, equipment, or technology not provided by Provider or authorized by Provider in writing; or (iv) modifications to the Services not made by Provider, provided that Customer may not settle any Third-Party Claim against Provider unless Provider consents to such settlement, and further provided that Provider will have the right, at its option, to defend itself against any such Third-Party Claim or to participate in the defense thereof by counsel of its own choice.

(c) Sole Remedy. THIS SECTION 9 SETS FORTH CUSTOMER'S SOLE REMEDIES AND PROVIDER'S SOLE LIABILITY AND OBLIGATION FOR ANY ACTUAL, THREATENED, OR ALLEGED CLAIMS THAT THE SERVICES INFRINGE, MISAPPROPRIATE, OR OTHERWISE VIOLATE ANY INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY. IN NO EVENT WILL PROVIDER'S LIABILITY UNDER THIS SECTION 9 TWO TIMES THE TOTAL AMOUNTS PAID TO PROVIDER UNDER THIS AGREEMENT IN THE TWELVE MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO THE CLAIM OR ONE MILLION DOLLARS (\$1,000,000), WHICHEVER IS LESS.

10. Limitations of Liability. IN NO EVENT WILL PROVIDER BE LIABLE UNDER OR IN CONNECTION WITH THIS AGREEMENT UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE, FOR ANY: (a) CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, ENHANCED, OR PUNITIVE DAMAGES; (b) INCREASED COSTS, DIMINUTION IN VALUE OR LOST BUSINESS, PRODUCTION, REVENUES, OR PROFITS; (c) LOSS OF GOODWILL OR REPUTATION; (d) USE, INABILITY TO USE, LOSS, INTERRUPTION, DELAY, OR RECOVERY OF ANY DATA, OR BREACH OF DATA OR SYSTEM SECURITY; OR (e) COST OF REPLACEMENT GOODS OR SERVICES, IN EACH CASE REGARDLESS OF WHETHER PROVIDER WAS ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES OR SUCH LOSSES OR DAMAGES WERE OTHERWISE FORESEEABLE. IN NO EVENT WILL PROVIDER'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE EXCEED TWO TIMES THE TOTAL AMOUNTS PAID TO PROVIDER UNDER THIS AGREEMENT IN THE TWELVE MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO THE CLAIM OR ONE MILLION DOLLARS (\$1,000,000), WHICHEVER IS LESS.

11. Term and Termination.

(a) Term. The term of this Agreement begins on the Effective Date and, unless terminated earlier pursuant to this Agreement's express provisions, will continue in effect until such date as provided on the Order (the "**Term**").

(b) Termination. In addition to any other express termination right set forth in this Agreement:

(i) Provider may terminate this Agreement, effective on written notice to Customer, if Customer: (A) fails to pay any amount when due under an Order; or (B) breaches any of its obligations under Section 2(c) or Section 6;

(ii) either Party may terminate this Agreement, effective on written notice to the other Party, if the other Party materially breaches this Agreement, and such breach: (A) is incapable of cure; or (B) being capable of cure, remains uncured 30 days after the non-breaching Party provides the breaching Party with written notice of such breach; or

(iii) either Party may terminate this Agreement, effective immediately upon written notice to the other Party, if the other Party: (A) becomes insolvent or is generally unable to pay, or fails to pay, its debts as they become due; (B) files or has filed against it, a petition for voluntary or involuntary bankruptcy or otherwise becomes subject, voluntarily or involuntarily, to any proceeding under any domestic or foreign bankruptcy or insolvency law; (C) makes or seeks to make a general assignment for the benefit of its creditors; or (D) applies for or has appointed a receiver, trustee, custodian, or similar agent appointed by order of any court of competent jurisdiction to take charge of or sell any material portion of its property or business.

(c) Effect of Expiration or Termination. Upon expiration or earlier termination of this Agreement, Customer shall immediately discontinue use of the Provider IP and, without limiting Customer's obligations under Section 6, Customer shall delete, destroy, or return all copies of the Provider IP and certify in writing to the Provider that the Provider IP has been deleted or destroyed. Provider may delete or destroy all copies of Customer Data in its system or otherwise in its possession or control upon the expiration or termination of this Agreement. No expiration or termination will affect Customer's obligation to pay all Fees that may have become due before such expiration or termination or entitle Customer to any refund.

(d) Survival. This Section 11(d) and Section 1, 5, 6, 7, 8, 9, 10, and 12 survive any termination or expiration of this Agreement. No other provisions of this Agreement survive the expiration or earlier termination of this Agreement.

12. Miscellaneous.

(a) Entire Agreement. This Agreement, together with any other documents incorporated herein by reference and all related addenda and exhibits, constitutes the sole and entire agreement of the Parties with respect to the subject matter of this Agreement and supersedes all prior and contemporaneous understandings, agreements, and representations and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the body of this Agreement, the related addenda and exhibits, and any other documents incorporated herein by reference, the following order of precedence governs: (i) first, the Order; (ii) second, this Agreement; (iii) third, any other documents incorporated herein by reference.

(b) Notices. All notices, requests, consents, claims, demands, waivers, and other communications hereunder (each, a "**Notice**") must be in writing and addressed to the Parties at the addresses set forth on the Order (or to such other address that may be designated by the Party giving Notice from time to time in accordance with this Section). All Notices must be delivered by personal delivery, nationally recognized overnight courier (with all fees pre-paid), facsimile or email (with confirmation of transmission), or certified or registered mail (in each case, return receipt requested, postage pre-paid). Except as otherwise provided in this Agreement, a Notice is effective only: (i) upon receipt by the receiving Party; and (ii) if the Party giving the Notice has complied with the requirements of this Section.

(c) Force Majeure. In no event shall either Party be liable to the other Party, or be deemed to have breached this Agreement, for any failure or delay in performing its obligations under this Agreement (except for any obligations to make payments), if and to the extent such failure or delay is caused by any circumstances beyond such Party's reasonable control, including but not limited to acts of God, flood, fire, earthquake, explosion, war, terrorism, invasion, riot or other civil unrest, strikes, labor stoppages or slowdowns or other industrial disturbances, or passage of law or any action taken by a governmental or public authority, including imposing an embargo.

(d) Amendment and Modification; Waiver. No amendment to or modification of this Agreement is effective unless it is in writing and signed by an authorized representative of each Party. No waiver by any Party of any of the provisions hereof will be effective unless explicitly set forth in writing and signed by the Party so waiving. Except as otherwise set forth in this Agreement, (i) no failure to exercise, or delay in exercising, any rights, remedy, power, or privilege arising from this Agreement will operate or be construed as a waiver thereof, and (ii) no single or partial exercise of any right, remedy, power, or privilege hereunder will preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.

(e) Severability. If any provision of this Agreement is invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability will not affect any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal, or unenforceable, the Parties shall negotiate in good faith to modify this Agreement so as to effect their original intent as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

(f) Governing Law; Submission to Jurisdiction. This Agreement is 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 that would require or permit the application of the laws of any jurisdiction other than those of the State of California. Any legal suit, action, or proceeding arising out of or related to this Agreement or the licenses granted hereunder will be instituted exclusively in the federal courts of the United States or the courts of the State of California in each case located in San Jose, California, and each Party irrevocably submits to the exclusive jurisdiction of such courts in any such suit, action, or proceeding.

(g) Assignment. Customer may not assign any of its rights or delegate any of its obligations hereunder, in each case whether voluntarily, involuntarily, by operation of law or otherwise, without the prior written consent of Provider, which consent shall not be unreasonably withheld, conditioned, or delayed. Any purported assignment or delegation in violation of this Section will be null and void. No assignment or delegation will relieve the assigning or delegating Party of any of its obligations hereunder. This Agreement is binding upon and inures to the benefit of the Parties and their respective permitted successors and assigns.

(h) Export Regulation. Customer shall comply with all applicable federal laws, regulations, and rules, and complete all required undertakings (including obtaining any necessary export license or other governmental approval), that prohibit or restrict the export or re-export of the Services or any Customer Data outside the US.

(i) US Government Rights. Each of the Documentation and the software components that constitute the Services is a "commercial item" as that term is defined at 48 C.F.R. § 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 C.F.R. § 12.212. Accordingly, if Customer is an agency of the US Government or any contractor therefor, Customer only receives those rights with respect to the Services and Documentation as are granted to all other end users, in accordance with (a) 48 C.F.R. § 227.7201 through 48 C.F.R. § 227.7204, with respect to the Department of Defense and their contractors, or (b) 48 C.F.R. § 12.212, with respect to all other US Government users and their contractors.

(j) Equitable Relief. Each Party acknowledges and agrees that a breach or threatened breach by such Party of any of its obligations under Section 6 or, in the case of Customer, Section 2(c), would cause the other Party irreparable harm for which monetary damages would not be an adequate remedy and agrees that, in the event of such breach or threatened breach, the other Party will be entitled to equitable relief, including a restraining order, an injunction, specific performance, and any other relief that may be available from any court, without any requirement to post a bond or other security, or to prove actual damages or that monetary damages are not an adequate remedy. Such remedies are not exclusive and are in addition to all other remedies that may be available at law, in equity, or otherwise.

(k) Acceptance. You accept this Agreement, by: (i) checking the box indicating acceptance or (ii) signing an Order that references and incorporates this Agreement. If the individual accepting this Agreement is accepting on behalf of a company or other legal entity, such individual represents that they have the authority to bind such entity and its affiliates to these terms and conditions, in which case the term "Customer" shall refer to such entity and its affiliates. If the individual accepting this Agreement does not have such authority, or does not agree with the terms and conditions of this Agreement, such individual must not accept this agreement or use the Services.

SERVICE LEVEL ADDENDUM

Capitalized terms used but not defined in this Service Level Addendum ("SLA") shall have the meaning given to those terms in the Software as a Service Agreement by and between iXsystems, Inc. and _____.

The parties intend to review this on either party's reasonable request. Any revisions to the service levels must be authorized by both parties.

1. Defined Terms. For purposes of this SLA, the following terms shall have the following meanings:

"Key Performance Indicator (KPI)" means a Service Level measurement that is not subject to Service Credits, but that is important to Customer's business. Upon reasonable notice, Customer may request that a KPI be converted to a Service Level, in which case the parties will negotiate in good faith a Service Credit applicable to such measurement. The parties will amend this SLA to reflect any such change.

"Service Credit" means a percentage of Service Fees to be credited to Customer if Provider fails to meet a Service Level, as set forth in this SLA.

"Service Level" means a performance standard that Provider is required to meet in providing the Services, as set forth in this SLA.

2. Service Scope. This SLA covers the following Services:

3. [LIST OF INCLUDED SERVICES]

This SLA does not cover the following:

[LIST OF EXCLUDED SERVICES]

3. Customer Obligations. The Customer's responsibilities and obligations in support of this SLA include the following:

- (a) Providing information, and authorizations, as required by the Provider for performing the Services.
- (b) Adhering to policies and processes established by the Provider for reporting service failures and incidents and prioritizing service requests.
- (c) Making a representative available (i) for regular meetings to review the SLA and (ii) to consult with the Provider for resolving service-related incidents or requests.
- (d) Paying fees and costs as required by the Agreement.

4. Provider Obligations. The Provider's responsibilities and obligations in support of this SLA include:

- (a) Meeting applicable incident response times.
- (b) Adhering to the Customer's policies and practices as applicable to the performance of the Services.
- (c) Making a representative available (i) for regular meetings to review the SLA and (ii) to resolve service-related incidents or requests.

5. Assumptions. Provider's performance of the Services under this SLA is subject to the following assumptions, constraint, and dependencies:

- (a) Information provided by Customer to Provider as required for the Services will be accurate and timely.
- (b) Provider's procedures and delivery of Services may be affected by changes in relevant Customer internal policies or in applicable laws or regulations.

6. Service Levels and Service Credits.

(a) The following table sets forth the Services measured under this SLA, the applicable Service Levels, and the Service Credits to which Customer will be entitled if Provider fails to meet the Service Levels during any monthly measurement period. The total amount of Service Credits shall not exceed 100% of Provider's fees in any monthly measurement period.

Service	Measurement	Service Level	Service Credit
[SERVICE A]	[CALCULATION]	[NUMBER][%/[UNIT]]	[NUMBER]%
[SERVICE B]	[CALCULATION]	[NUMBER][%/[UNIT]]	[NUMBER]%

(c) The Service Credits set forth in this SLA shall be considered liquidated damages or Customer's sole and exclusive remedy for Provider's failure to meet Service Levels. Customer shall not be entitled to any other rights or remedies set forth in the Agreement.

7. Other Terms and Conditions.

(a) Single Point of Contact. Provider and Customer shall each appoint a person (a "Single Point of Contact") who shall be available to receive communications and coordinate responses to questions or failures with respect to the Service Levels. Notwithstanding the foregoing sentence, in the event of any emergency relating to any Service, a party shall attempt to contact the appointed Single Point of Contact of the other party, but may also directly contact any person most able to resolve the emergency quickly. The initial Single Points of Contact for each party shall be:

For Provider: [NAME AND TITLE]

For Customer: [NAME AND TITLE]

Either party may change its Single Point of contact upon notice to the other party.

13.2 - TrueCommand Terms of Service

iXsystems Software 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 IXSYSTEMS 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 IXSYSTEMS 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 "iXsystems Software" means the iXsystems software.

1.3 "Device" means digital computer equipment and peripheral equipment.

1.4 "Product" means, individually and collectively, iXsystems Software.

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 iXsystems End User License Agreement.

2.0 License

Subject to the terms set forth in this Agreement, iXsystems grants You a non-exclusive, non-transferable, revocable, limited license without the option to sublicense, to use iXsystems Software on Your Device(s) in accordance with Your authorized purchase and use of a Product(s) or iXsystems Software for Your internal business purposes. This use includes but is not limited to using or viewing the instructions, specifications, and documentation provided with the Product.

3.0 License Restrictions

The Product, is protected by copyright laws and international treaties, as well as other intellectual property laws, statutes, and treaties. The Product is licensed, not sold to You the end user. You do not acquire any ownership interest in the Product or any other rights to such Product, other than to use such Product 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 Product, and all intellectual property rights arising out of or relating to the Product, subject to the license expressly granted to You in this Agreement.

The Product may contain iXsystems' trademarks, trade secrets, and proprietary collateral. iXsystems strictly

prohibits the acts of decompiling, reverse engineering, or disassembly of the Product. You agree to use commercially reasonable efforts to safeguard the Product and iXsystems' intellectual property, trade secrets, or other proprietary information You may have access to, from infringement, misappropriation, theft, misuse, or unauthorized access. You will promptly notify iXsystems if You become aware of any infringement of the Product and cooperate with iXsystems in any legal action taken by iXsystems to enforce its intellectual property rights. By accepting this Agreement, You agree You will not disclose, copy, transfer, or publish benchmark results relating to the Product without the express written consent of iXsystems. You agree not to use, or permit others to use, the Product beyond the scope of the license granted under Section 2, unless otherwise permitted by iXsystems, or in violation of any law, regulation or rule, and you will not modify, adapt, or otherwise create derivative works or improvements of the Product. You are responsible and liable for all uses of the Product through access thereto provided by You, directly or indirectly.

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 agreement between You and iXsystems for use of the iXsystems 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 Product 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 Foreign Corrupt Practices Act - You will comply with the requirements of the United States Foreign Corrupt Practices Act (the "FCPA") and will refrain from making, directly or indirectly, any payments to third parties which constitute a breach of the FCPA. You will notify Company immediately upon Your becoming aware that such a payment has been made. You will indemnify and hold harmless Company from any breach of this provision.

4.6. Title - iXsystems retains all rights, titles, and interest in iXsystems Software and in 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.

4.7 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.

4.8 Maintenance and Support - You may be entitled to support services from iXsystems after purchasing iXsystems Software, Products, 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 the 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. For more information on our Maintenance and Support contract, refer to ixsystems.com/ixsystems_SLA.

4.9 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.

4.10 Termination - iXsystems may terminate or suspend Your license to use the Product or Software and cease any and all support, services, or maintenance under this Agreement without prior notice, or liability, and for any reason whatsoever, including, without limitation, if any of the terms and conditions of this Agreement are breached. Upon termination, rights to use the Product and Software will immediately cease. Other provisions of this Agreement will survive termination including, without limitation, ownership provisions, warranty disclaimers, indemnity, and limitations of liability.

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

4.12 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 or Software may be subject to US export control laws, including the US Export Administration Act and its associated regulations. 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 federal laws, regulations, and rules, and complete all required undertakings (including obtaining any necessary export license or other governmental approval), prior to exporting, re-exporting, releasing, or otherwise making the Product available outside the US.

6.0 Data Collection and Privacy

iXsystems Software may collect information relating to Your use of the Product, including information that has been provided directly or indirectly through automated means. Usage of iXsystems Software, geolocation information, user login credentials, and device and operating system identification are allowed according to iXsystems' privacy policy. 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 accepting this agreement or continuing to use this product.

13.3 - End of Life Notices

13.3.1 - TrueCommand 1.1

September 29, 2020

TrueCommand 1.1 has reached its End of Life and is no longer receiving security updates. The TrueCommand 1.3.2 release announcement can be found at <https://www.ixsystems.com/blog/truecommand-1-3-2/>.

Please schedule a time to upgrade to the latest version of TrueCommand. If assistance is required, please contact the iXsystems Support Team.

Customers who purchase iXsystems hardware or that want additional support must have a support contract to use iXsystems 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)

13.3.2 - TrueCommand 1.0

September 29, 2020

TrueCommand 1.0 has reached its End of Life and is no longer receiving security updates. The TrueCommand 1.3.2 release announcement can be found at <https://www.ixsystems.com/blog/truecommand-1-3-2/>.

Please schedule a time to upgrade to the latest version of TrueCommand. If assistance is required, please contact the iXsystems Support Team.

Customers who purchase iXsystems hardware or that want additional support must have a support contract to use iXsystems 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)