Print
Back to Docs Hub

CORE Tutorials

Standalone tutorials. Tutorials are organized parallel to the CORE interface layout.

Welcome to TrueNAS CORE tutorials!

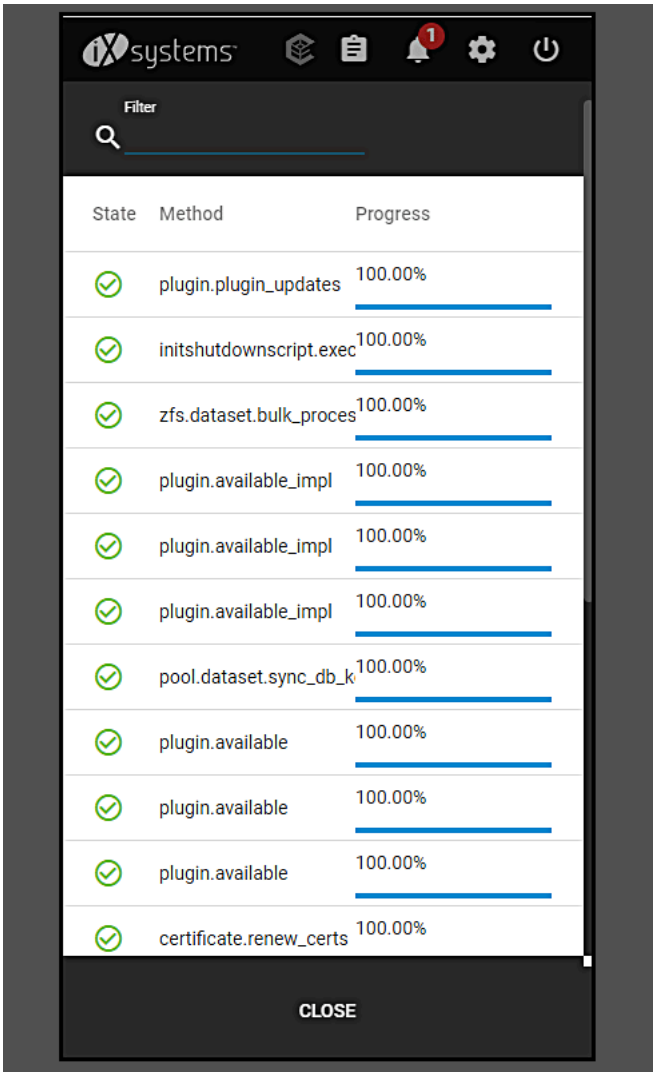
This guide collects various how-tos for both simple and complex tasks using primarily the TrueNAS web interface. Tutorials are organized parallel to the TrueNAS web interface structure and grouped by topic. Tutorials are living articles and continually updated with new content or additional in-depth tutorials that guide in unlocking the full potential of TrueNAS.

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

Task Manager

The **Task Manager** displays a list of tasks performed by the TrueNAS system. It starts with the most recent task.

Click the  to open the **Task Manager**.



Click a task name to display its start time, finish time, and whether the task succeeded. If a task fails, the error status shows.

Tasks with log file output have a **View Logs** button to show the log files.

Click **CLOSE** or anywhere outside the **Task Manager** dialog to close it, or press Esc.

Getting Support

There are several options to get support for your TrueNAS installation. TrueNAS CORE users can engage with the TrueNAS community to answer questions and resolve issues. TrueNAS Enterprise hardware customers can also access the fast and effective support directly provided by iXsystems.

TrueNAS CORE users are welcome to report bugs and vote for or suggest new TrueNAS features in the project Jira instance. Have questions? We recommend searching through the software documentation and community resources for answers.

Reporting a Bug

If you encounter a bug or other issue while using TrueNAS, create a bug report in the TrueNAS Jira Project. The web interface provides a form to report issues without logging out. We recommend searching the project first to see if another user already reported the issue. You must have a Jira account to create a bug ticket.

To report an issue using the web interface, go to **System > Support**.

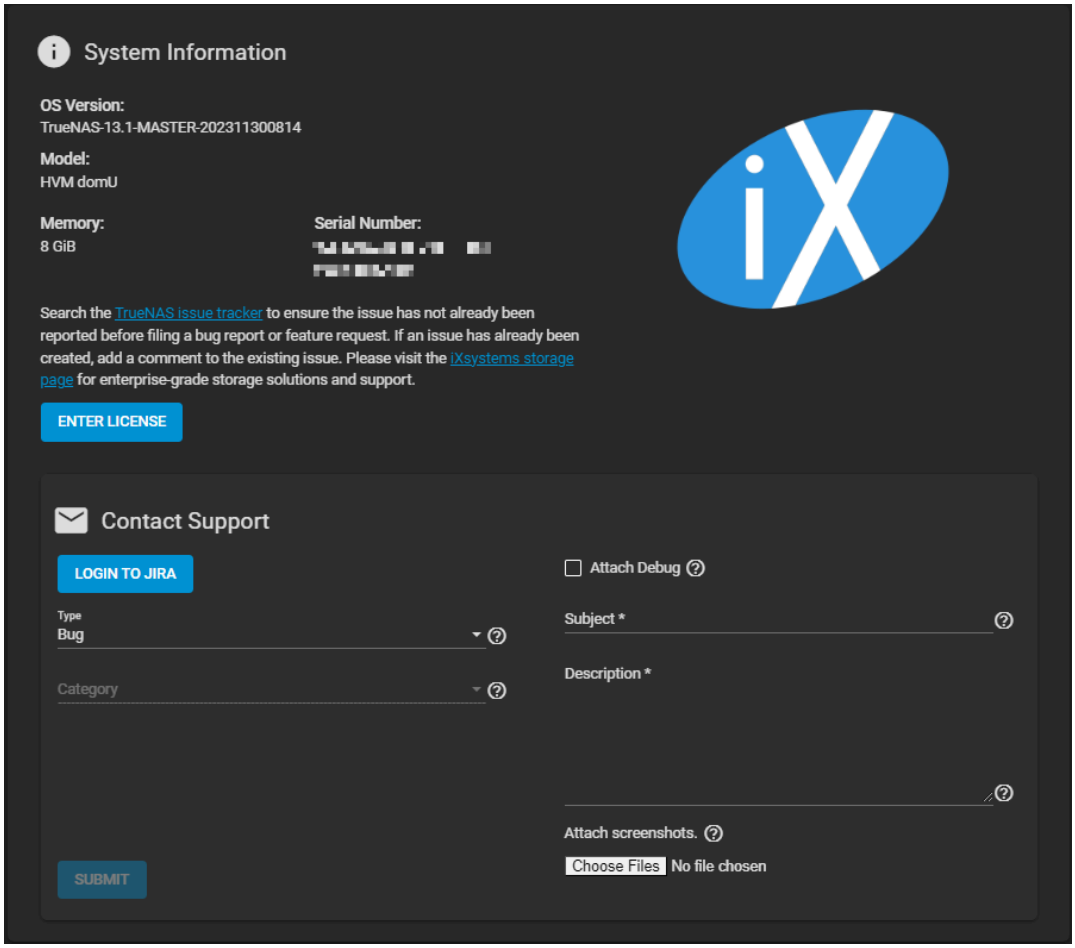


Figure 1: Writing a Bug Report

Enter your Jira **Username** and **Password** to verify your account credentials and unlock the **SUBMIT** button. The **Category** dropdown has a large number of options. Choose the category that best fits where you encountered the issue.

Attaching a debug file and screenshot(s) to your bug ticket is generally recommended to help find the bug and speed up response. Select **Attach Debug** to automatically generate a new debug and privately attach it to the issue. Private debug attachments are only visible to iXsystems engineering staff.

Keep the **Subject** brief and informative. Having a short, descriptive subject allows the community to easily find and respond to your issue. The **Description** should contain more details about the problem. We recommend keeping the description less than three paragraphs and including any steps to reproduce the issue.

Creating a Debug File

The TrueNAS web interface lets users save debugging information to a text file.

On TrueNAS CORE systems, go to **System > Advanced** and click **SAVE DEBUG**.

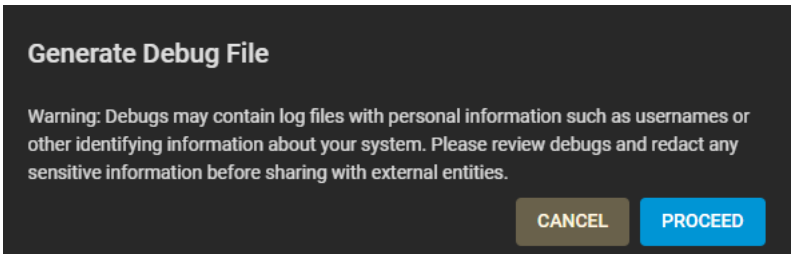


Figure 2: Generate Debug Warning

Click **PROCEED** to generate the debug file (might take a few minutes). After generating the debug file, TrueNAS prompts you to download it to your local system and saves a copy in /var/tmp/fndebug.

The `freenas-debug` command-line utility collects debugging information.

> Debug files contain log files which can include personal information such as usernames, networking configuration, device serial numbers, or other identifying information about your system. Files uploaded to an issue from the **System > Support** screen using **Attach Debug** or through the Jira Private File Upload service are only visible to iXsystems engineers. The iXsystems Privacy Policy contains a detailed statement of our commitment to data privacy.
>
> Always store debug files in a secure location. Please review debugs and redact any sensitive information before sharing with external entities. Use a file archiver utility, such as 7-zip, to open compressed debug archives and review log contents.

Suggesting New Features

Want to see a new feature added to TrueNAS? You can see and vote for community-proposed features in the TrueNAS Jira project and make your feature suggestions here. If you find a suggestion that you want to see implemented, open that ticket and click **Vote for this issue** in the **People** section.

Figure 3: Voting for a Suggestion

To suggest a new feature, go to https://ixsystems.atlassian.net/projects/NAS/, log in to your Jira account, and click **Create**.

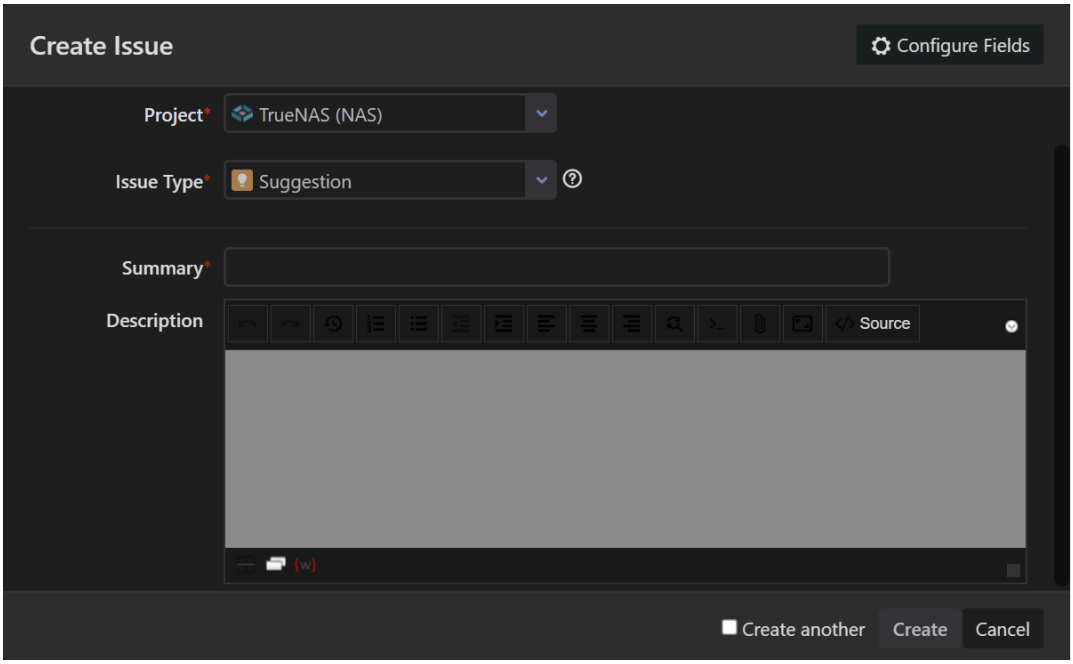


Figure 4: Creating a New Suggestion

Briefly describe the new feature you would like to see added in the **Summary** section. After creating your feature suggestion, it moves to the **Gathering Interest** stage, where the community can review and vote for the feature. After gathering enough interest, the TrueNAS Release Council reviews the suggestion for feasibility and determines where to add the feature in the software roadmap.

TrueNAS Community

The TrueNAS Community is an active online resource for asking questions, troubleshooting issues, and sharing information with other TrueNAS users. You must register to post.

We encourage new users to briefly review the forum rules and helpful tips before posting.

Community Resources are user-contributed articles about every facet of using TrueNAS. They are organized into broad categories and incorporate a community rating system to better highlight content that the whole community has found helpful.

Social Media

You are always welcome to network with other TrueNAS users using the various social media platforms!

- Reddit
- X (Formerly Twitter)
- LinkedIn
- Facebook

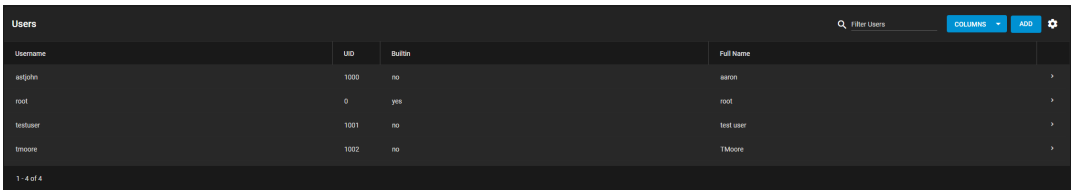
Setting Up Users and Groups

Creating users and assigning them to groups allows you to efficiently tune permissions and share data for large numbers of users.

> Only the root user account can log in to the TrueNAS web interface.

When the network uses a directory service, import the existing account information using the instructions in Directory Services. Using Active Directory requires setting Windows user passwords inside Windows.

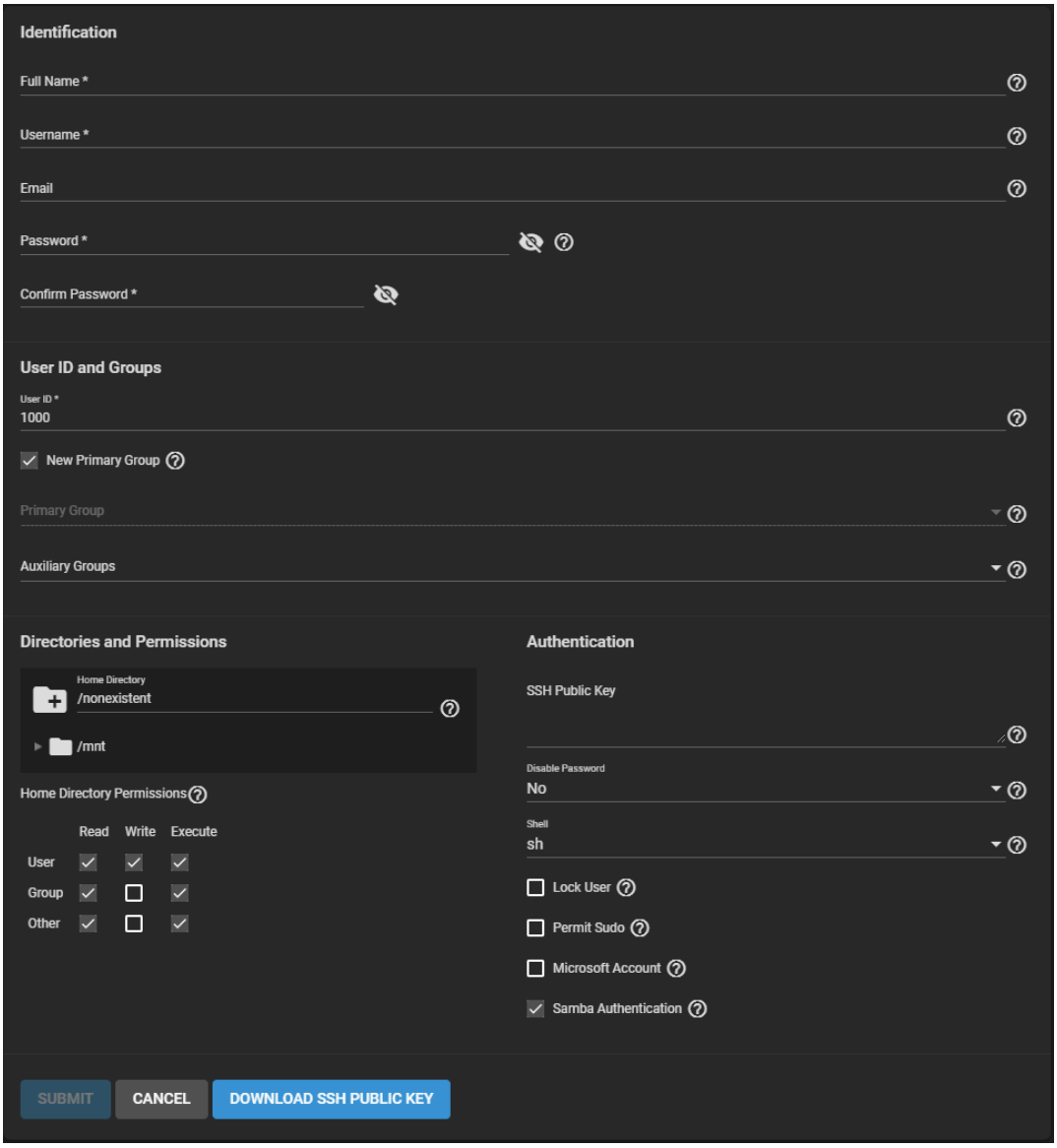
To see user accounts, go to **Accounts > Users**.



TrueNAS hides all built-in users by default. To see all built-in users, click ⚙ and **SHOW**.

Add a User

Go to **Accounts > Users** and click **ADD**.



> Fields with an * must be configured to submit or change the UI configuration.

TrueNAS subdivides account options into groups of similar options.

Identification

Enter a **Full Name**. TrueNAS suggests a simplified **Username** from the **Full Name**, but you override it with your own choice.

You can associate an **Email** address with a user account.

Set and confirm the user password.

User ID and Groups

Next, you must set a user ID. TrueNAS automatically suggests the user ID starting at *1000*, but you can change it. We recommend using an ID of *1000* or more for non-built-in users.

By default, TrueNAS creates a new primary group with the same name as the user. To add the user to an existing primary group instead, unset **New Primary Group** and select a group from the **Primary Group** drop-down. You can add the user to more groups using the **Auxiliary Groups** drop-down.

Directories and Permissions

When creating a user, TrueNAS sets the home directory path to /nonexistent, which does not create a user home directory. To set a home directory, select a path using the file browser. If the directory exists and matches the user name, it sets as the user home directory. When the path does not end with a subdirectory matching the user name, TrueNAS creates a new subdirectory. The full path to the user home directory displays here when editing a user.

Directly under the file browser, you can set the home directory permissions. TrueNAS default user accounts cannot change their permissions.

Authentication

You can assign a public SSH key to a user for key-based authentication by pasting the public key into the **SSH Public Key** field. If you are using an SSH public key, always keep a backup. Click **DOWNLOAD SSH PUBLIC KEY** to download the pasted key as a .txt file.

When **Disable Password** is *Yes*, the **Password** field is unavailable. The system removes the existing password from the account and disables the **Lock User** and **Permit Sudo** options. The account cannot use password-based logins for services. For example, disabling the password prevents using account credentials to log in to an SMB share or open an SSH session on the system. By default, **Disable Password** is *No*.

You can set a specific shell for the user from the **Shell** dropdown:

▼ Shell Options

Shell	Description
csh	C shell for UNIX system interactions.
sh	Bourne shell
tcsh	Enhanced C shell that includes editing and name completion.
bash	Bourne Again shell for the GNU operating system.
ksh93	Korn shell that incorporates features from both *csh* and *sh*.
mksh	MirBSD Korn Shell
rbash	Restricted bash
rzsh	Restricted zsh
scponly	scponly restricts the user's SSH usage to only the `scp` and `sftp` commands.
zsh	Z shell
git-shell	restricted git shell
nologin	Use when creating a system account or to create a user account that can authenticate with shares but which cannot log in to the TrueNAS system using `ssh`.

Setting **Lock User** disables all password-based functionality for the account until you unset the option.

Permit Sudo allows the account to act as the system administrator using the `sudo` command. For better security, leave this option disabled.

If the user account is accessing TrueNAS data using a Windows 8 or newer client, set **Microsoft Account** to enable additional authentication methods available from those operating systems.

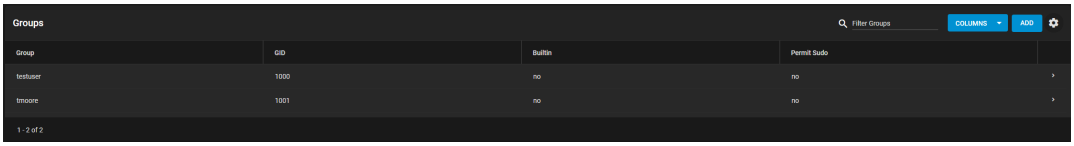
By default, **Samba Authentication** is enabled. It allows users to access SMB share data using account credentials.

Groups

Using groups in TrueNAS is an efficient way to manage permissions for many similar user accounts. The interface lets you manage UNIX-style groups. If the network uses a directory service, import the existing account information using the instructions in Active Directory.

View Existing Groups

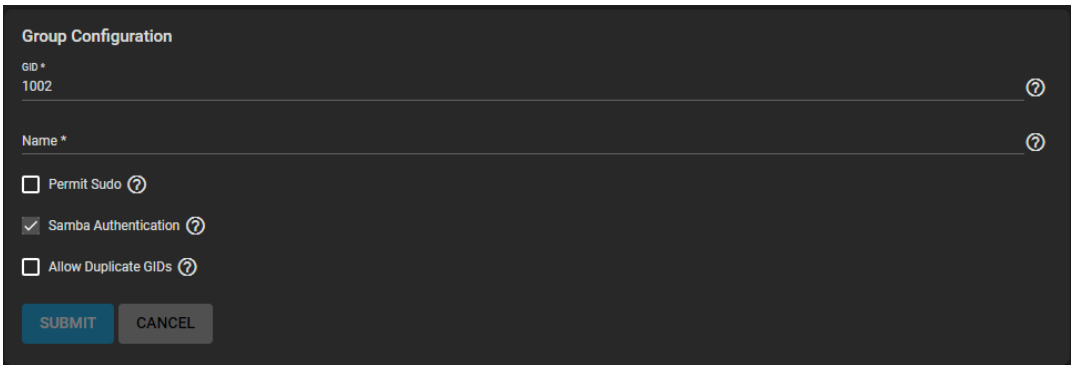
To see saved groups, go to **Accounts > Groups**



By default, TrueNAS hides built-in groups. To see built-in groups, click ⚙ and **SHOW**.

Add a Group

Go to **Accounts > Groups** and click **ADD**.



Each group gets a Group ID (**GID**). Enter a number above *1000* for a group with user accounts. You cannot change the GID later. Groups used by a system service must have an ID that matches the default port number used by the service.

Next, enter a descriptive group **Name**. Group names cannot begin with a hyphen (-) or contain a space, tab, or these characters: , : + & # % ^ ( ) ! @ ~ * ? < > =.

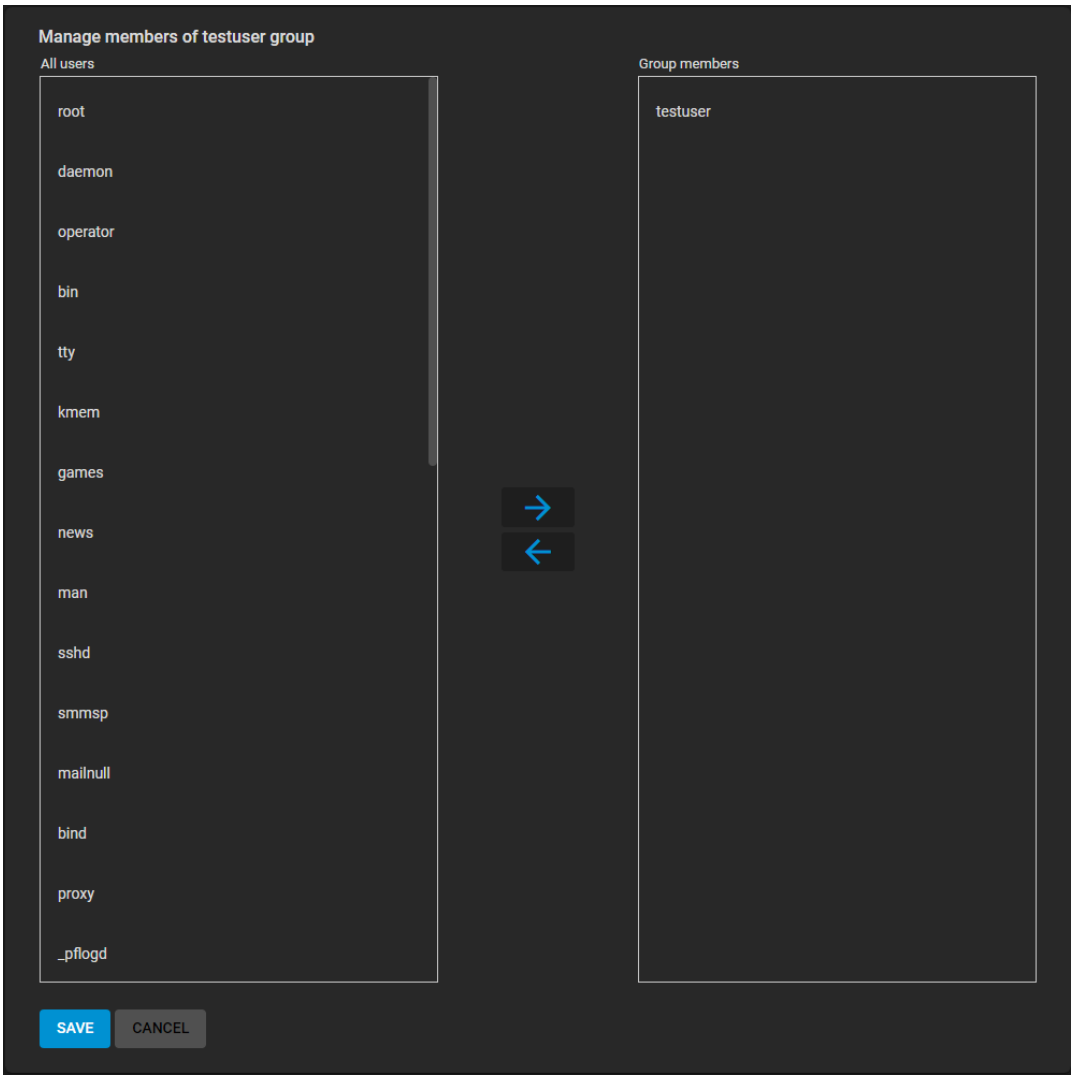
By default, the **Permit Sudo** option is unset. Setting it allows group members to act as the root account by using sudo. Leave **Permit Sudo** unset for better security.

Samba Authentication is set by default. It allows group members to use SMB permissions and authentication.

Finally, **Allow Duplicate GIDs** lets you duplicate group IDs but can complicate system configurations. We recommend leaving it unset.

Group Member Management

Register user accounts to a group to simplify permissions and access to many user accounts. To manage group membership, go to **Accounts > Groups**, click the › for a group, then click 👥 **MEMBERS**:



To add user accounts to the group, select them in **All users** and click →. Select multiple users by holding CTRL while clicking each entry.

System Configuration

Using Configuration Backups

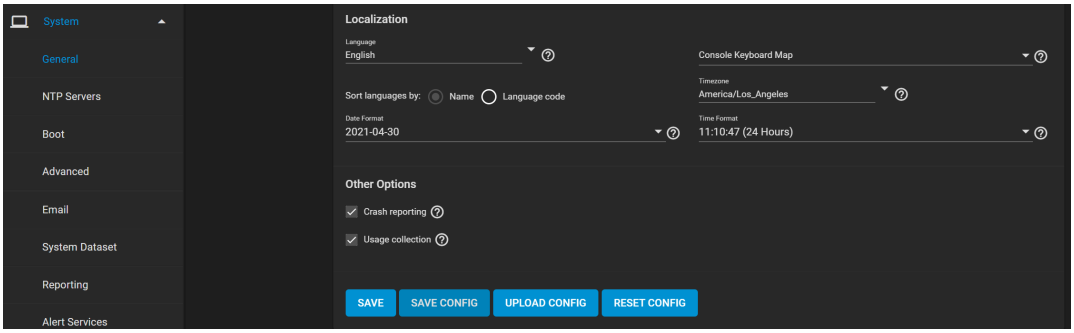
We highly recommend backing up the system configuration regularly. Doing so preserves settings when migrating, restoring, or fixing the system if it runs into any issues. Save the configuration file each time the system configuration changes.

Backup configs store information for accounts, network, services, tasks, virtual machines, and system settings. Backup configs also index ID's and credentials for account, network, and system services. Users can view the contents of the backup config using database viewing software like SQLite DB Browser.

Backing Up System Configurations

Manual Backup

Go to **System > General** and click **SAVE CONFIG**, then enter your password.



> The configuration file contains sensitive data about the TrueNAS system. Ensure that it is stored somewhere safe.

Automatic Backup

TrueNAS automatically backs up the configuration database to the system dataset every morning at 3:45 (relative to system time settings). However, this backup does not occur if the system is off at that time. If the system dataset is on the boot pool and it becomes unavailable, the backup also loses availability.

> You must backup SSH keys separately. TrueNAS does not store them in the configuration database. System host keys are files with names beginning with ssh_host_ in /usr/local/etc/ssh/. The root user keys are stored in /root/.ssh.

Passwords

The system backup affects two types of passwords: hashed and encrypted.

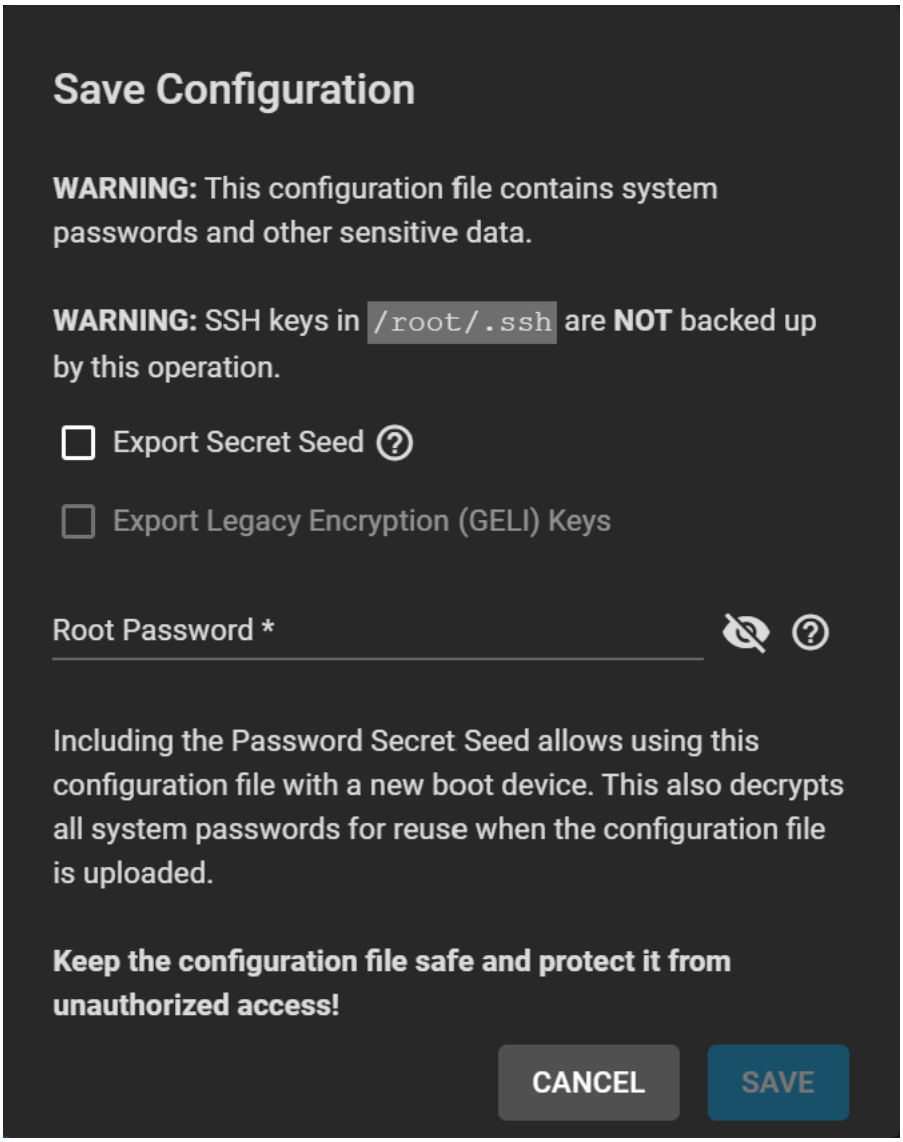
Hashed: TrueNAS stores user account passwords for the base operating system as hashed values. The system saves them in the system configuration backup, so they do not need to be encrypted to be secure.

Encrypted: The system saves other passwords, like iSCSI CHAP passwords, Active Directory bind credentials, and cloud credentials in an encrypted form to prevent them from being visible as plain text in the saved system configuration. The key or seed for this encryption is usually only on the operating system device.

There are two options after clicking **SAVE CONFIG**:

Export Password Secret Seed includes encrypted passwords in the configuration file. Encrypted passwords allow you to restore the configuration file to a different operating system device where the decryption seed is not present. Users must physically secure configuration backups containing the seed to prevent unauthorized access or password decryption.

Export Legacy Encryption (GELI) Keys includes encrypted legacy encryption keys in the configuration file. Users can restore the encryption keys by uploading the configuration file to the system using **UPLOAD CONFIG**.



Resetting and Restoring Configurations

Reset Configuration

To reset the system configuration to factory settings, go to **System > General** and click **RESET CONFIG**.

> **Save the system's current configuration before resetting.**
>
> If you do not save the system config before resetting it, you may lose any data that you did not back up. You cannot revert to the previous settings.

After resetting the system configuration, the system restarts, and you must set a new login password.

Restore Configuration

Users can restore configurations by going to **System > General** and clicking **UPLOAD CONFIG**.

When uploading a config, you can select any previously saved config files for their system.

Managing Boot Environments

TrueNAS supports a ZFS feature known as boot environments. These are snapshot clones that TrueNAS can boot into. You can only use one boot environment for booting.

▼ How does this help me?

A boot environment allows rebooting into a specific point in time and greatly simplifies recovering from system misconfigurations or other potential system failures. With multiple boot environments, the process of updating the operating system becomes a low-risk operation. The updater automatically creates a snapshot of the current boot environment and adds it to the boot menu before applying the update. If anything goes wrong during the update, the system administrator can boot TrueNAS into the previous environment to restore system functionality.

Changing Boot Environments

Sometimes, rolling back to an older boot environment can be useful. For example, if an update process doesn't go as planned, it is easy to roll back to a previous boot environment. TrueNAS automatically creates a boot environment when the system updates.

There are two different methods for changing the active boot environment: using the web interface and through a Command Line Interface (CLI)

Web Interface

Go to **System > Boot** and click ⋮ for the desired boot environment, then click **Activate**.

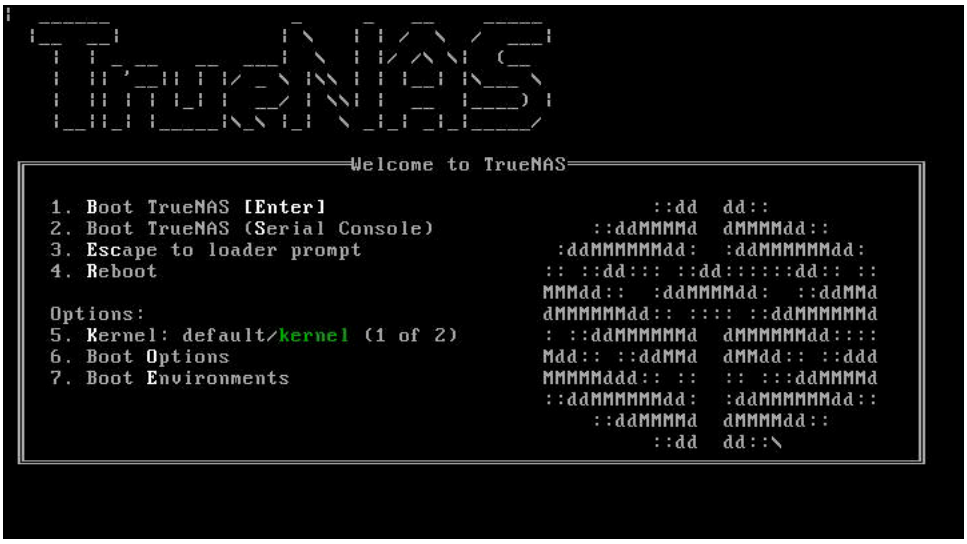
Reboot the system to activate the new boot environment.

Command Line Interface

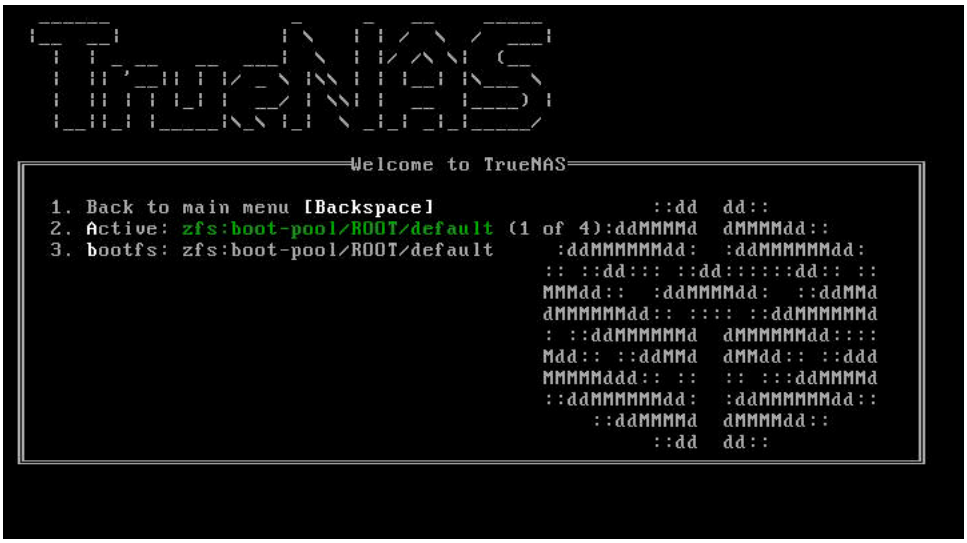
Reboot the system.

When the welcome screen appears, press the key that corresponds with the option **Boot Environments** (usually 7).

> The *Boot Environments* options does not appear when no additional boot environments are present.



Choose the new boot environment to activate byt pressing the key for the *Active:* option.



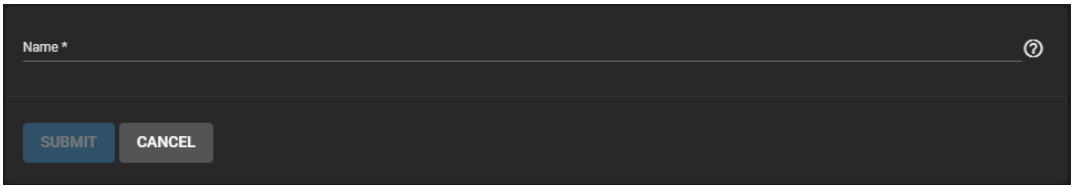
Press the key to cycle through existing boot environments. When you select the desired boot environment, press `Backspace` to return to the welcome menu, then press `4` to reboot the system.

Boot Actions

Go to **System > Boot** and click **ACTIONS**.

Add a New Boot Environment

Click Add to make a new boot environment from the active environment.



Name the new boot environment and click **SUBMIT**.

> You may only use alphanumeric characters, dashes (-), and underscores (_) in the **Name**.

View Stats/Settings

Click **Stats/Settings** to display statistics for the operating system device.

By default, TrueNAS scrubs the operating system device every 7 days. To change the default, input a different number in the **Scrub interval (in days)** field and click **UPDATE INTERVAL**.

View Boot Pool Status

Click **Boot Pool Status** to see the status of each boot-pool device, including any read, write, or checksum errors.

Scrub the Boot Pool

Click **Scrub Boot Pool** to perform a manual (data integrity check) of the operating system device.

Mirroring the Boot Pool

Adding a second storage device to the boot pool changes the configuration to a **Mirror**. This allows one of the devices to fail and the system still boots. If one of the two devices were to fail, that device is easily detached and replaced.

When adding a second device to create a mirrored boot pool, consider these caveats:

- **Capacity**: The new device must have at least the same capacity as the existing device. Larger capacity devices can be added, but the mirror will only have the capacity of the smallest device. Different models of devices which advertise the same nominal size are not necessarily the same actual size. For this reason, adding another device of the same model of is recommended.
- **Device Type**: We **strongly recommend** using SSDs rather than USB devices when creating a mirrored boot pool.

> Removing devices from storage pools can result in data loss!

Go to **System > Boot > ACTIONS > Boot Pool Status**.

Click ⋮ on the boot device, then click attach.

Select a new **Member Disk** from the drop-down and click **SUBMIT**.

▼ Use all disk space?

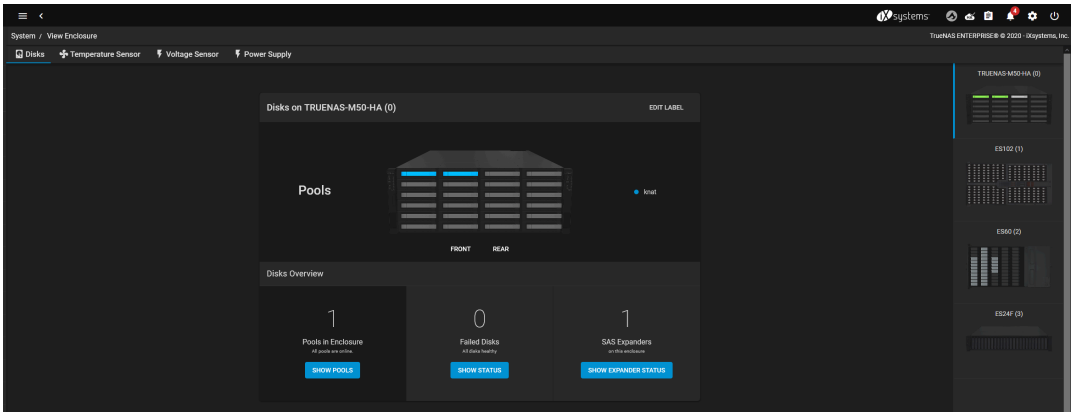
By default, TrueNAS partitions the new device to the same size as the existing device. When you select **Use all disk space**, TrueNAS uses the entire capacity of the new device.

If the original operating system device fails and is detached, the boot mirror changes to consist of just the newer device and grows to whatever capacity it provides. However, new devices added to this mirror must now be as large as the new capacity.

Managing Enclosures

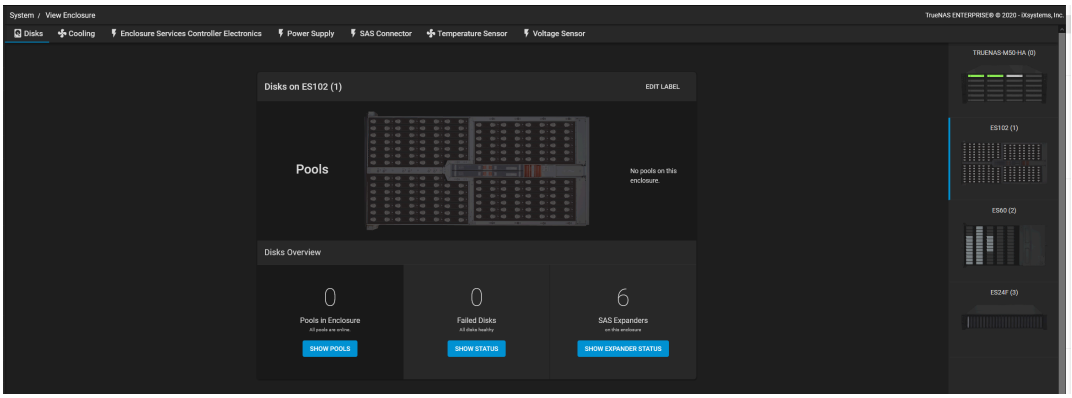
> Only compatible TrueNAS hardware and expansion shelves available from iXsystems allow seeing the **View Enclosure** option. To learn more about available iXsystems products, see the TrueNAS Systems Overview or browse the Hardware documentation.

Go to **System > View Enclosure** to display the status of connected disks and hardware.



Checking Enclosure Components

The screen shows the primary system. Other detected TrueNAS hardware is available from a column on the right side of the screen. Click an enclosure to show details about that hardware.



The screen is divided into different tabs which reflect the active sensors in the chosen hardware.

You can rename a system by clicking **EDIT LABEL**.

Identifying Disks

In the **Disks** tab, select a disk on the enclosure image and click **IDENTIFY DRIVE**. The drive LED on the physical system flashes so you can find it.

> The TrueNAS Mini Series models do not support drive light identification.

Configuring the System Email

An automatic script sends a nightly email to the administrator (root) account containing important information such as issues with the health of the disks, or other system functions. Alerts sent are based on the default options set on the **Alerts Settings** screen. TrueNAS emails alert events to the email set up for the root user account.

Configure the Root Email Address

Go to **Accounts > Users**, click ⋮ next to the **root** user, then click **Edit**. Enter a remote email address for the system administrator that regularly monitors the system in **Email**, then click **SAVE**.

Configuring user email addresses follows the same process.

Configure the System Email

Go to **System > Email** and enter a **From Name** for system emails.

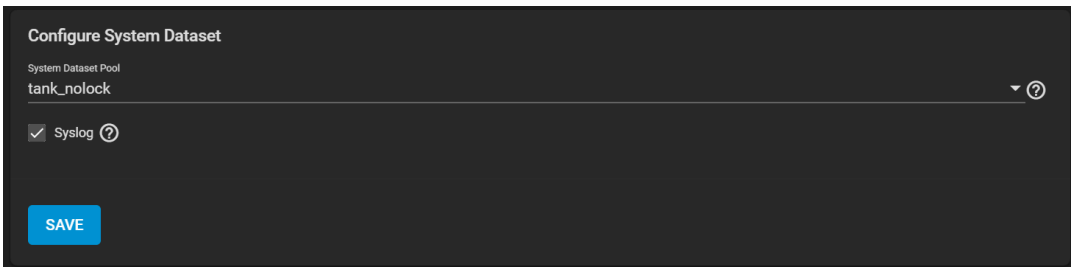
Next, select a **Send Mail Method** and fill out the remaining fields (SMTP) or log in (GMail OAuth).

Click **SEND TEST MAIL** to verify the configured email settings are working. If the test email fails, double-check that the root user **Email** field is correctly configured.

Setting the System Dataset

The system dataset stores debugging core files, encryption keys for encrypted pools, and Samba4 metadata such as the user and group cache and share level permissions.

To view the current location of the system dataset, go to **System > System Dataset**.



Store the System Log

Users can store the system log on the system dataset. We recommend users store the log information on the system dataset when the system generates large amounts of data and has limited memory or a limited-capacity operating system device.

Set **Syslog** to store the system log on the system dataset. Leave unset to store the system log in /var on the operating system device.

Change System Dataset

Select an existing pool from the **System Dataset Pool** dropdown.

You can move the system dataset to unencrypted pools or encrypted pools that do not have passphrases.

Moving the system dataset to an encrypted pool disables that volume's passphrase capability.

You cannot move the system dataset to a passphrase-encrypted or read-only pool.

> **Reboots Required**
>
> - The SMB service must restart, which causes a brief outage for any active SMB connections.
> - Highly Available TrueNAS systems must reboot the standby controller when the system dataset moves.

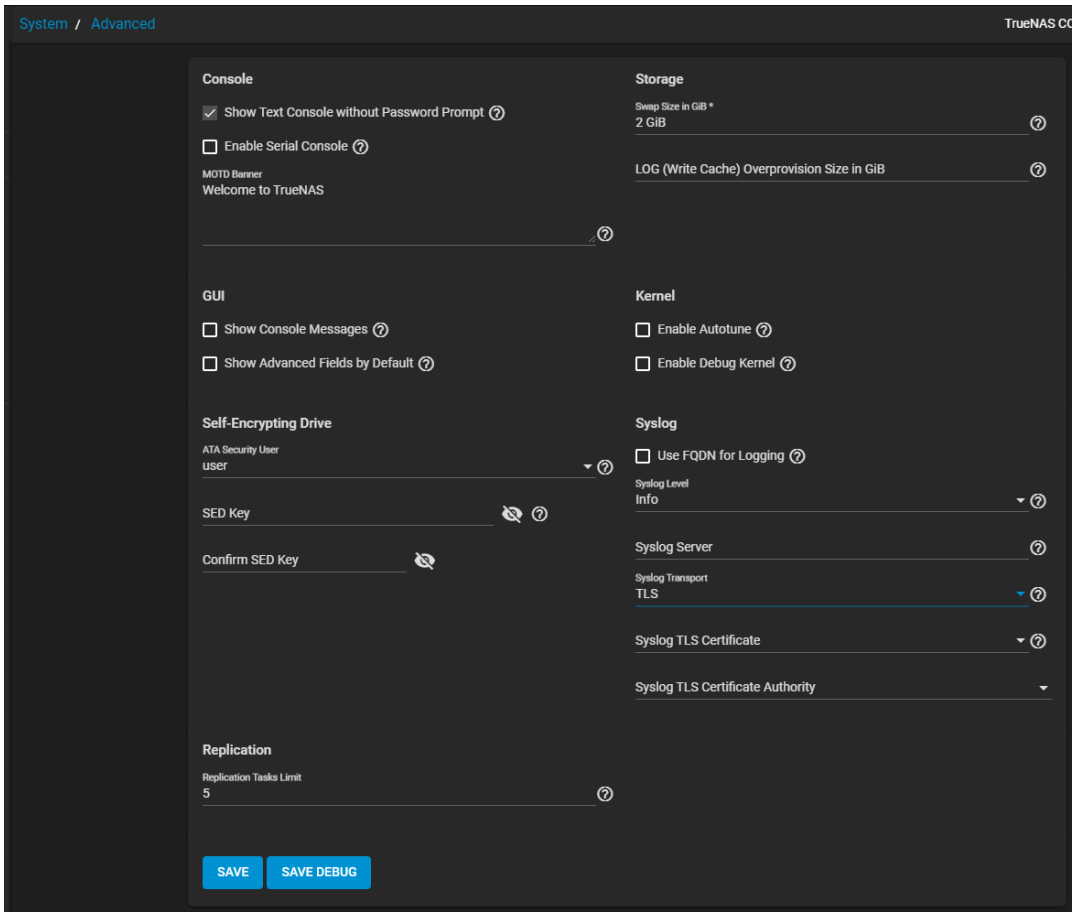
If a user changes the pool storing the system dataset later, TrueNAS migrates the existing data in the system dataset to the new location.

Setting Up a Remote Syslog Server

TrueNAS CORE allows users to configure a remote system logging server using any of the three transport protocols supported in CORE. Options are **UDP**, **TCP**, or **TLS**. The steps for all three protocols are the same except **UDP** and **TCP** do not require a certificate and certificate authority and **TLS** does.

Configuring a Syslog Server

1. (TLS only) Go to **System > CAs** and configure a certificate authority for the remote logging server. You can use a self-signed CA. Enter the IP address for the remote server in **Subject Alternate Names**.
2. (TLS only) Go to **System > Certificates** and configure a certificate for the remote logging server. Use the CA created for the remote syslog server. Enter the IP address for the remote server in **Subject Alternate Names**.
3. Go to **System > Advanced** and configure the syslog server settings.



   a. Select the level of logging in **Syslog Level**.

   b. Enter the IP address for the remote sever in **Syslog Server**.

   c. Select **TLS** in **Syslog Transport** or one of the other transport protocols. The system shows the certificate and certificate authority settings after selecting **TLS**. If selecting **UDP** or **TCL**, go to step four.

   d. Select the certificate created for the remote syslog server from the **Syslog TLS Certificate** dropdown list.

   e. Select the certificate authority created for the remote syslog server from the **Syslog TLS Certificate Authority** dropdown list.

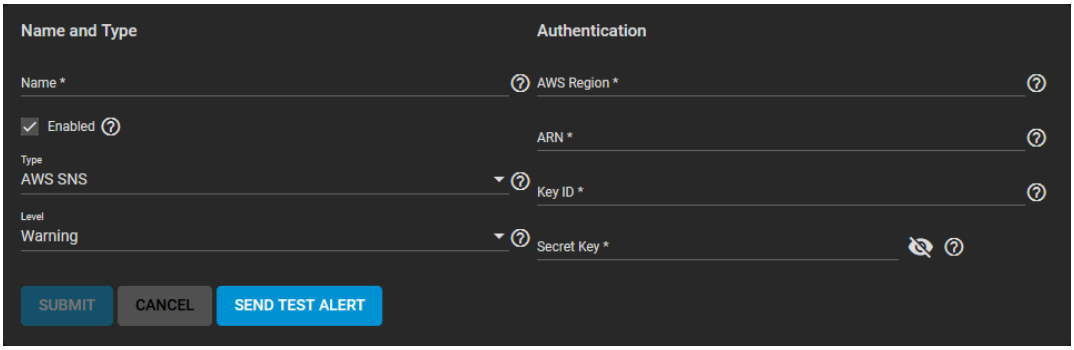
4. Click **SAVE**.

Creating Alerts

The alert system integrates with various third-party services. Tuning alerts helps personalize TrueNAS to any highly-sensitive issues.

Add an Alert Service

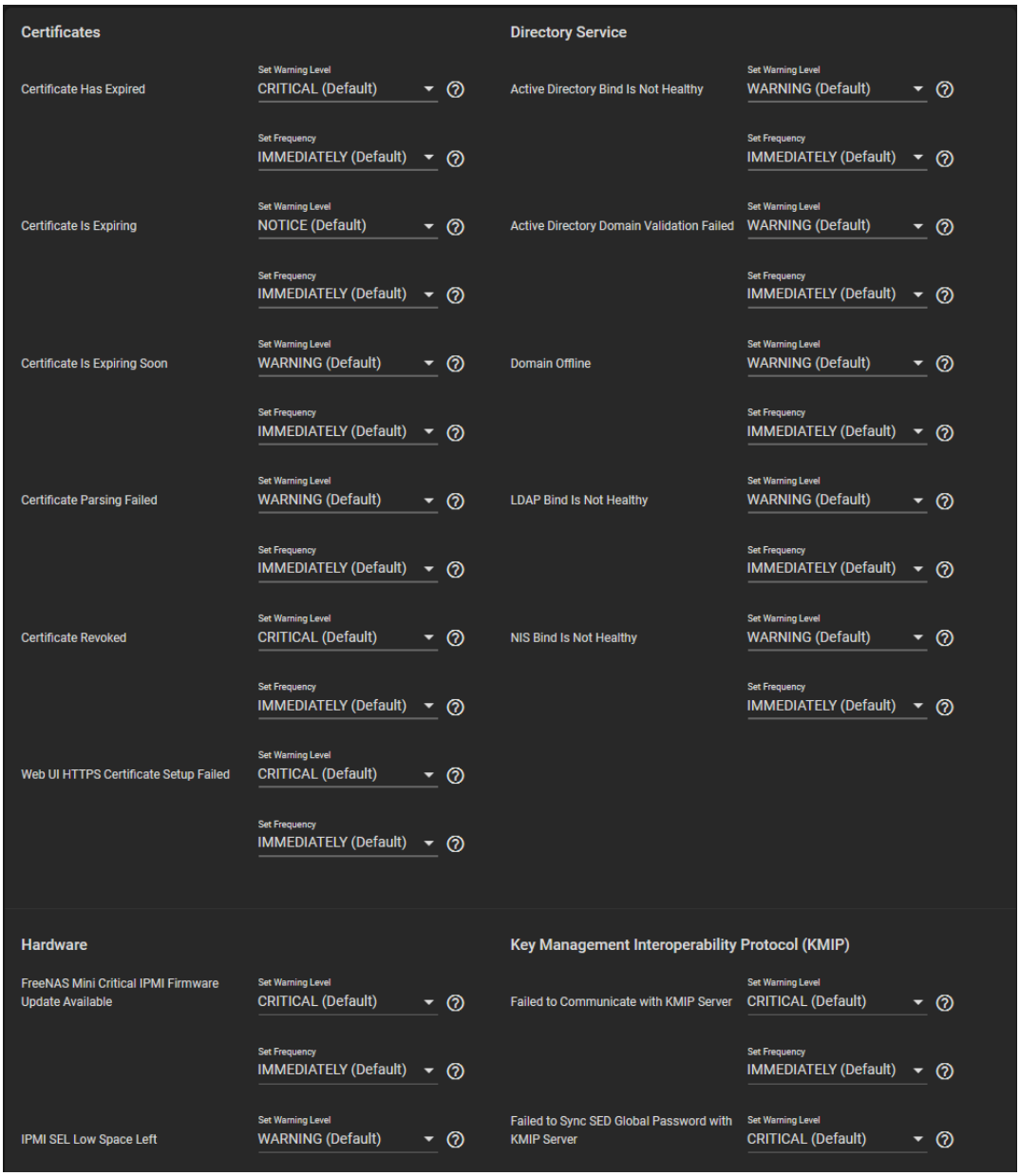
Go to **System > Alert Services** and click **ADD**.



Choose a **Type** and fill out the options specific to that alert service, then test the service configuration by clicking **SEND TEST ALERT**.

Customize Alert Settings

Go to **System > Alert Settings**.



The UI groups alerts based on type. For example, alerts related to pools appear in the **Storage** alert section.

Customize each alert **Warning Level** and **Frequency** using the drop-down menus.

Changing any of these options affects every configured alert service.

Click **SAVE** before leaving the page.

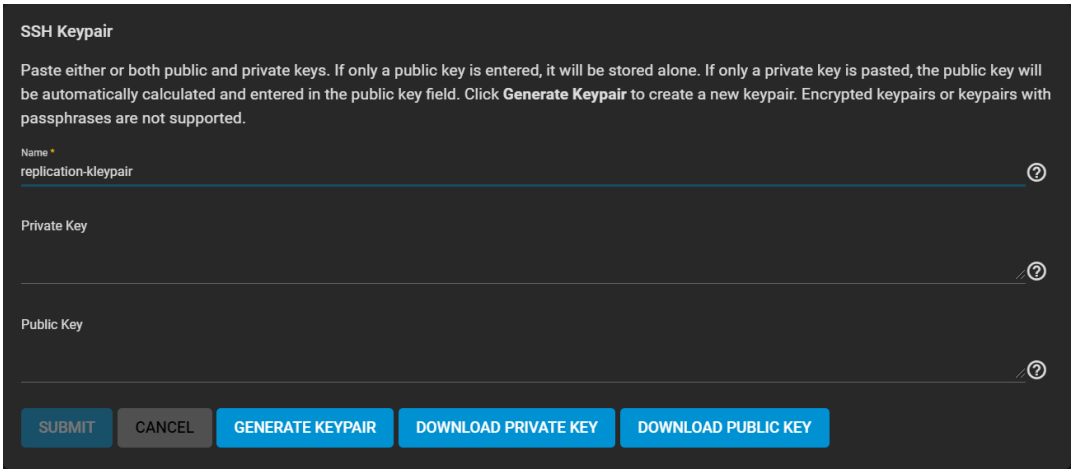
Configuring SSH Connections

Secure Socket Shell (SSH) is a cryptographic network protocol. It provides a secure method to access and transfer files between two hosts. This is possible even if the two hosts use an unsecured network. SSH establishes secure connections by means of user account credentials. It also uses key pairs shared between host systems for authentication.

Create SSH Keypairs

TrueNAS generates and stores RSA-encrypted SSH public and private keypairs in **System > SSH Keypairs**. The system typically uses keypairs when configuring **SSH Connections** or SFTP **Cloud Credentials**. Encrypted keypairs or keypairs with passphrases are not supported.

Creating a new **SSH Connection** or **Replication** task generates new keypairs. To manually generate a new keypair, go to **System > SSH Keypairs**, click **ADD**, and give the keypair a unique name.



Click **GENERATE KEYPAIR** to add values to the public and private key fields. Copy these strings or download them into text files for later use.

Create SSH Connections

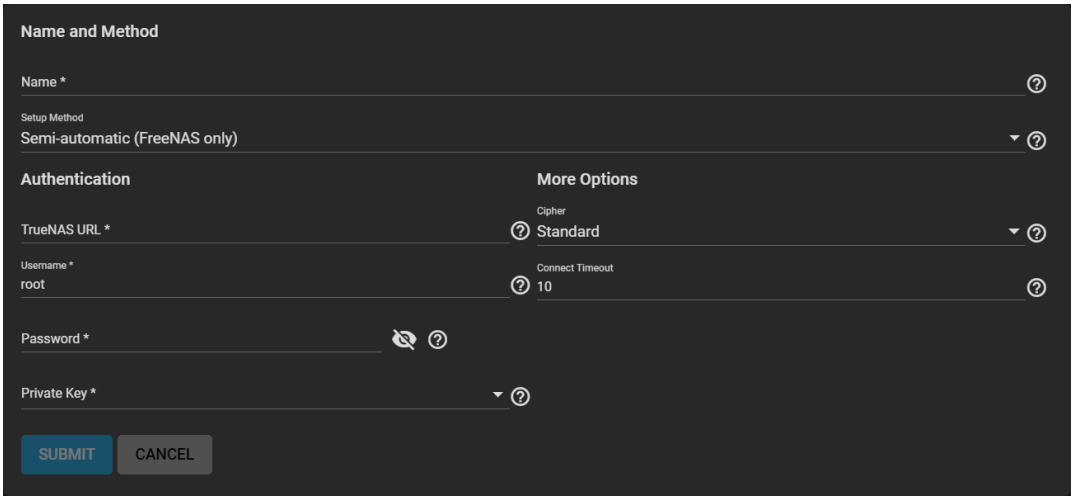
Semi-Automatic

TrueNAS offers a semi-automatic setup mode for setting up an SSH connection. This simplifies setting up an SSH connection with another FreeNAS or TrueNAS system. In semi-automatic setup mode it is not necessary to log in to the remote system to transfer SSH keys.

Semi-automatic setup requires an SSH keypair on the local system. You must have administrator account credentials for the remote TrueNAS. You must also configure the remote system to allow root access with SSH.

The semi-automatic configuration can generate the needed keypair. You can manually create the keypair by going to **System > SSH Keypairs**.

Go to **System > SSH Connections** and click **ADD**.



Use a valid URL scheme for the remote TrueNAS URL. Leave the username as **root** and enter the account password for the remote TrueNAS system. You can import the existing private key created from an SSH keypair, or create a new private key with a new SSH keypair.

Save the new configuration. TrueNAS opens a connection to the remote TrueNAS and exchanges SSH keys.

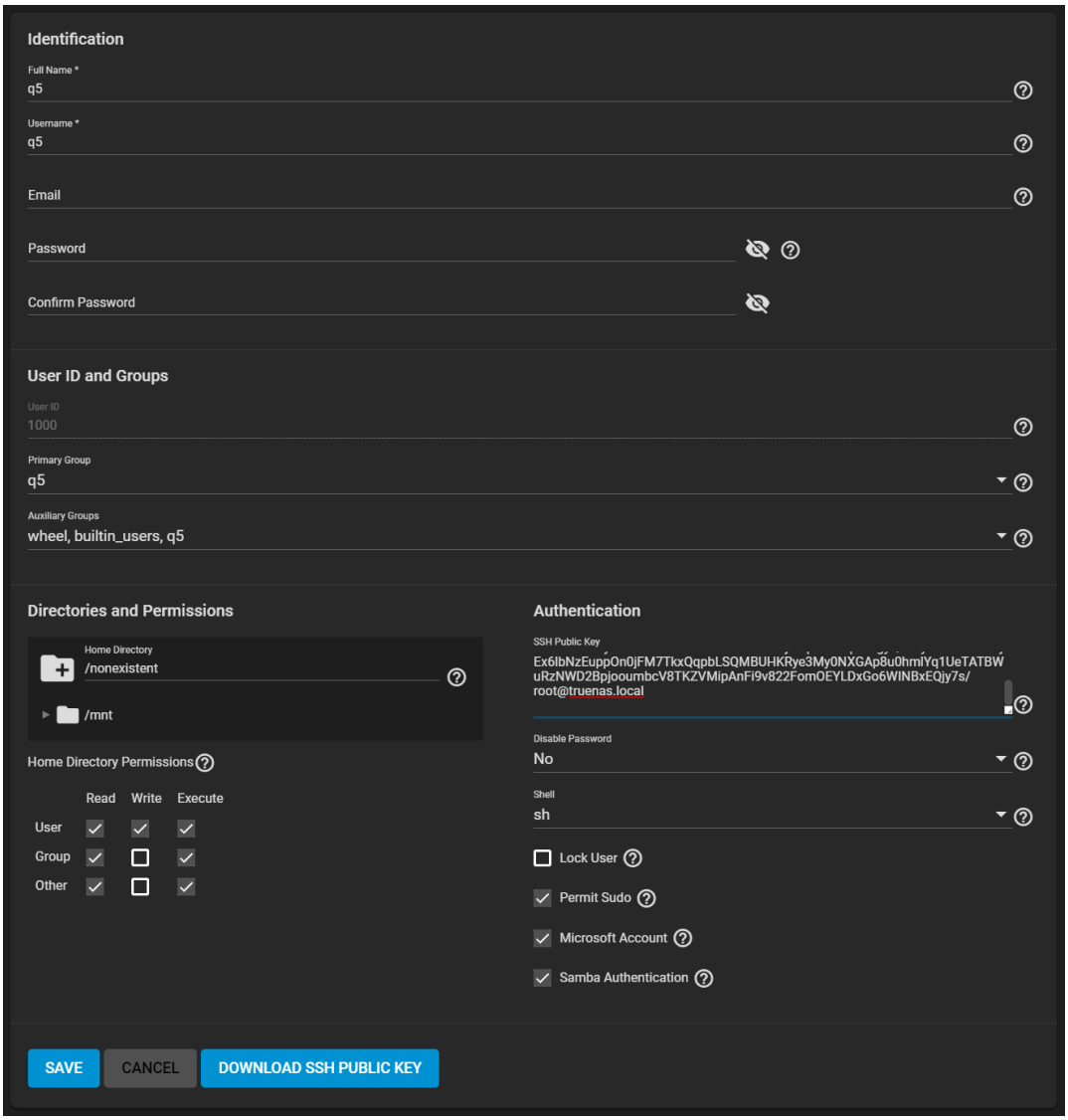
Manual Configuration

You can configure a secure SSH connection that does not generate a password prompt. This involves copying a public encryption key from the local system to the remote system.

Adding a SSH Public Key to the TrueNAS Root Account

Log in to the TrueNAS system that generated the SSH keypair and go to **System > SSH Keypairs**. Open the keypair you want to use for the SSH connection. Copy the text of the SSH public key or download the public key as a text file.

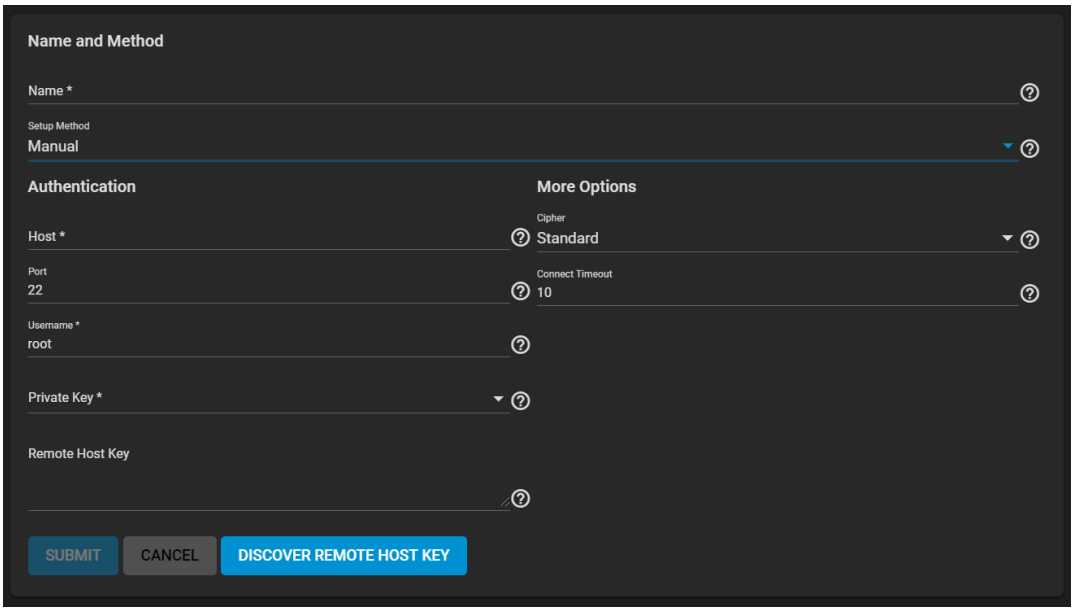
Log in to the TrueNAS system that needs to register the public key. Go to **Accounts > Users** and edit the *root* account. Paste the SSH public key text into the **SSH Public Key** field.



Generate a new SSH keypair in **System > SSH Keypairs**. Copy or download the value for the public key and add it to the remote NAS. If the remote NAS is not a TrueNAS system, please see the system documentation on adding a SSH public key.

Manually Configuring the SSH Connection on the Local TrueNAS

Log back into the local TrueNAS system and go to **System > SSH Connections**. Add a new connection and change the setup method to **Manual**.



Select the private key from the SSH keypair you used when you transferred the public key on the remote NAS.

Configuring Tunables

> Be careful when adding or editing the default tunables. Changing the default tunables can make the system unusable.

TrueNAS allows you to add system tunables from the web interface. You can manually define tunables, or TrueNAS can run an autotuning script to attempt to optimize the system. Tunables are used to manage TrueNAS sysctls, loaders, and rc.conf options.

- *loader* specifies parameters to pass to the kernel or load additional modules at boot time.
- *rc.conf* enables system services and daemons and only takes effect after a reboot.
- *sysctl* configures kernel parameters while the system is running and generally takes effect immediately.

> Adding a sysctl, loader, or rc.conf option is an advanced feature. A sysctl immediately affects the kernel running the TrueNAS system, and a loader can adversely affect the TrueNAS boot process. Do not create a tunable on a production system before testing the ramifications of that change.

Configure Tunables

To configure a tunable, go to **System > Tunables** and click **ADD**.

Select the **Type** of tunable to add or modify. Enter the name of the *loader*, *sysctl*, or *rc.conf* variable to configure.

Next, enter the value to use for the loader, sysctl, or rc.conf.

If you wish to create the system tunable but not immediately enable it, unset the **Enabled** checkbox. Configured tunables remain in effect until deleted or **Enabled** is unset.

We recommend restarting the system after making sysctl changes. Some sysctls only take effect at system startup, and restarting the system guarantees that the setting values correspond with what the running system uses.

Autotuning

TrueNAS provides an autotune script that optimizes the system depending on the installed hardware.

▼ Is this script available somewhere?

To see which checks are performed, find the autotune script in /usr/local/bin/autotune.

For example, if a pool exists on a system with limited RAM, the autotune script automatically adjusts some ZFS sysctl values to minimize memory starvation issues. Autotuning can introduce system performance issues. You must only use it as a temporary measure until you address the underlying hardware issue. Autotune always slows a RAM-starved system as it caps the ARC.

> We do not recommend TrueNAS Enterprise customers use the autotuning script, as it can override any specific tunings made by iXsystems Support.

Enabling autotune runs the autotuner script at boot. To run the script immediately, reboot the system.

Any tuned settings appear in **System > Tunables**.

▼ Can I manually tune a setting controlled by the autotuner?

Deleting tunables created by the autotune only affects the current session. Autotune-set tunables regenerate every time the system boots. You cannot manually tune any setting the autotuner controlls.

To permanently change a value set by autotune, change the description of the tunable. For example, changing the description to “*manual override*” prevents autotune from reverting the tunable back to the autotune default value.

Adding Certs, CAs, and CSRs

TrueNAS lets users create or import certificates, certificate signing requests (CSRs), and certificate authorities (CAs) that enable encrypted connections to the web interface.

Creating Certificate Authorities (CAs)

TrueNAS can act as a certificate authority (CA). When encrypting SSL or TLS connections to the TrueNAS system, you can import an existing CA or create a CA and certificate on the TrueNAS system. The certificate appears on the dropdown menus for services that support SSL or TLS.

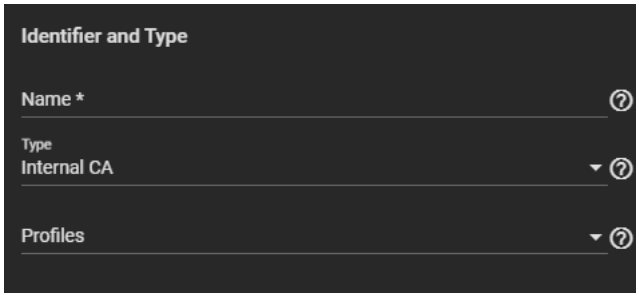
Go to **System > CAs** and click **ADD**. Enter a name for the CA, then choose the type from the **Type** dropdown list of three, **Internal CA**, **Intermediate CA**, or **Import CA**. The process to add a CA for each type is slightly different.

Creating CA

A CA must exist in CORE to add an Intermediate CA. This can be an internal or imported CA.

To create a CA:

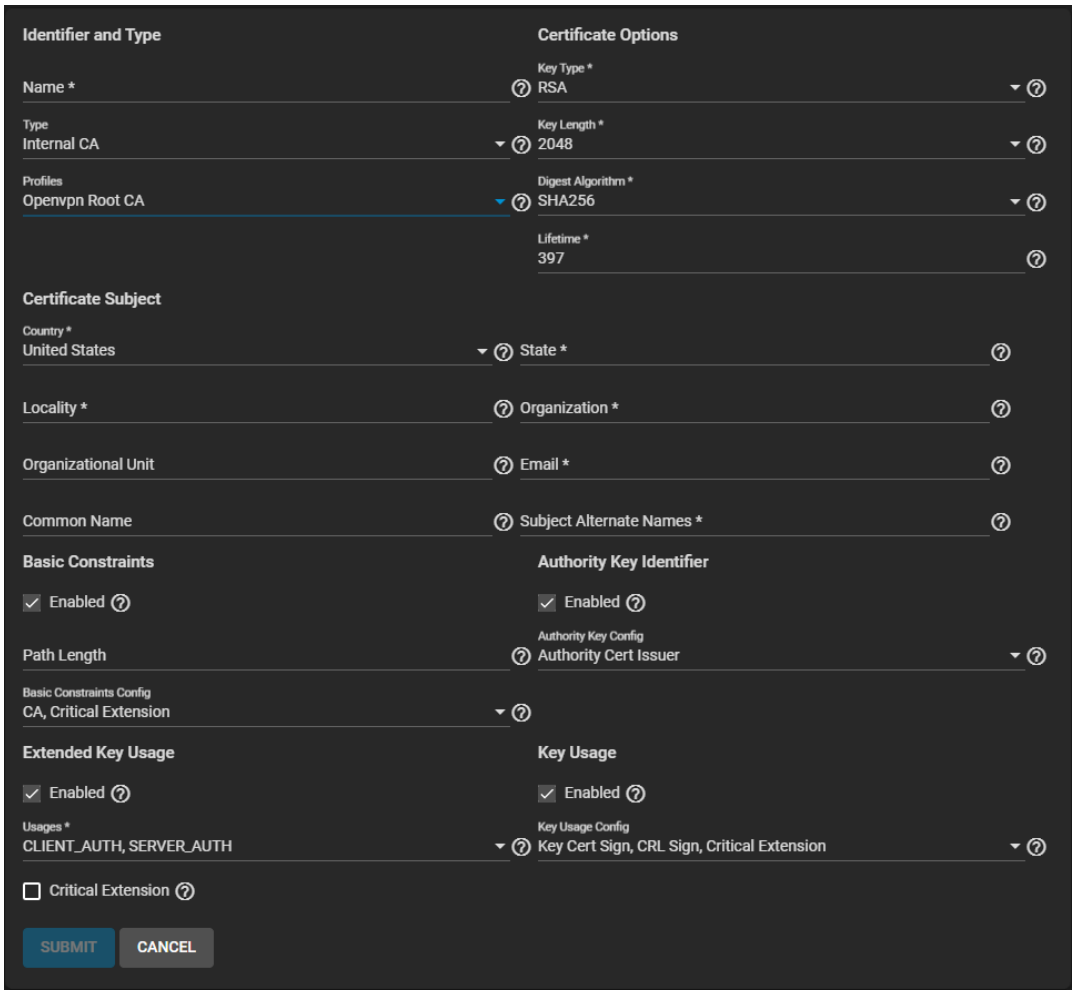
1. Enter or select the **Identifier and Type** setting options.



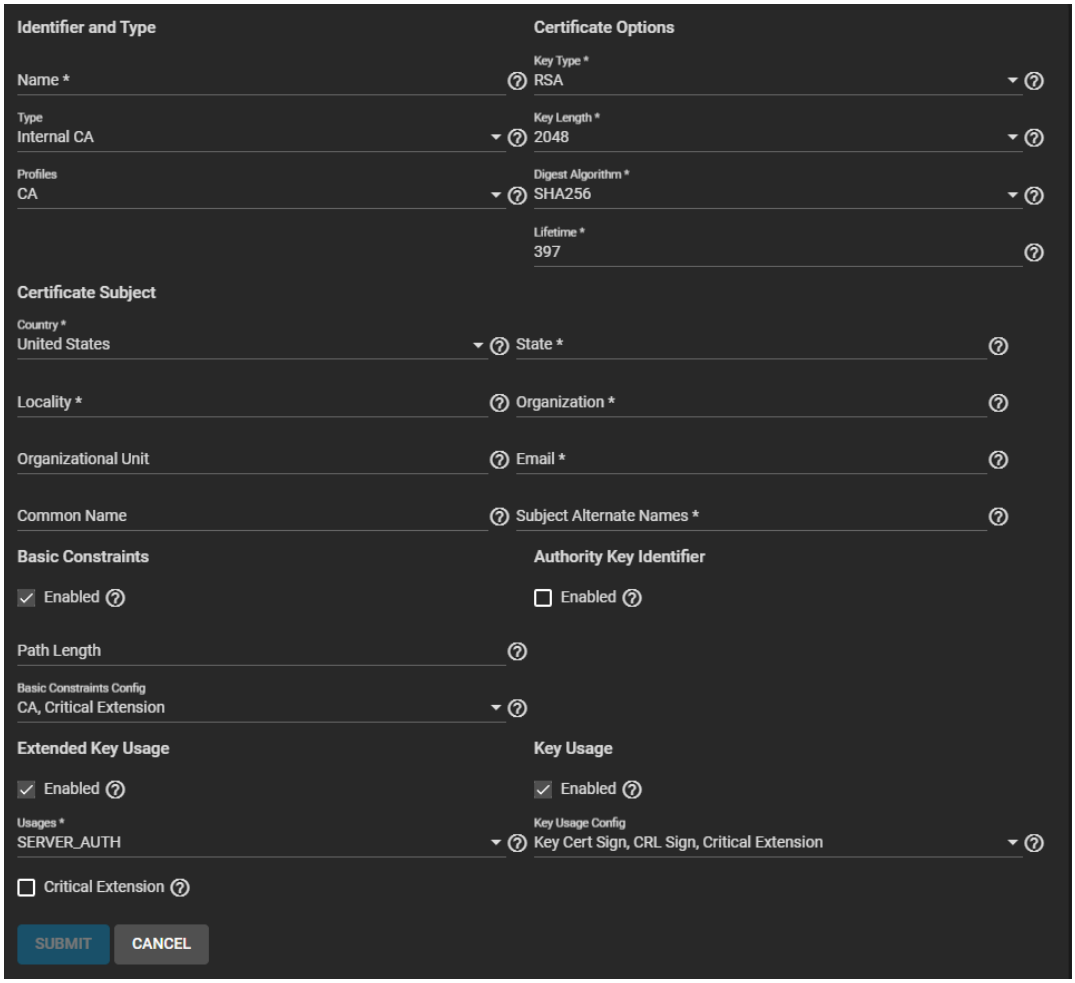
   a. Enter a name for this CA. b. Select **Internal CA** from the **Type** dropdown list to create an internal certificate. Select **Intermediate CA** to create an intermediate certificate. This displays the **Signing Certificate Authority** field in **Certificate Options**.

2. Select an option from the **Profiles** dropdown list. A profile for the CA auto-fills options like **Key Type**, **Key Length**, and **Digest Algorithm**. Otherwise, you must set options manually.

   To add an OpenVPN Root CA, select **OpenVPN Root CA**. The configuration form populates with default settings, enables **Basic Constraints**, **Authority Key Identifier**, **Extended Key Usage**, and **Key Usage**, and sets the options for each extension.



To add CA certificate, select **CA**. The configuration form populates with default settings, enables **Basic Constraints**, **Authority Key Identifier**, **Extended Key Usage**, and **Key Usage**, and sets the options for each extension.



3. Select the **Certificate Options**.

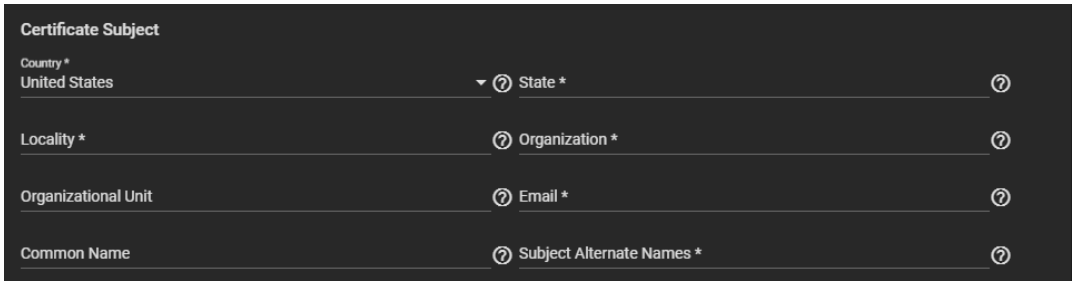
a. Select a **Key Type** from the dropdown list. We recommend the **RSA** key type. Use **EC** for elliptic curve certificates.

b. Select the **Key Length**. We recommend a minimum of **2048** for security reasons.

c. Select a **Digest Algorithm**. We recommend **SHA256**.

d. Enter the **Lifetime** of the CA in days to set how long the CA remains valid.

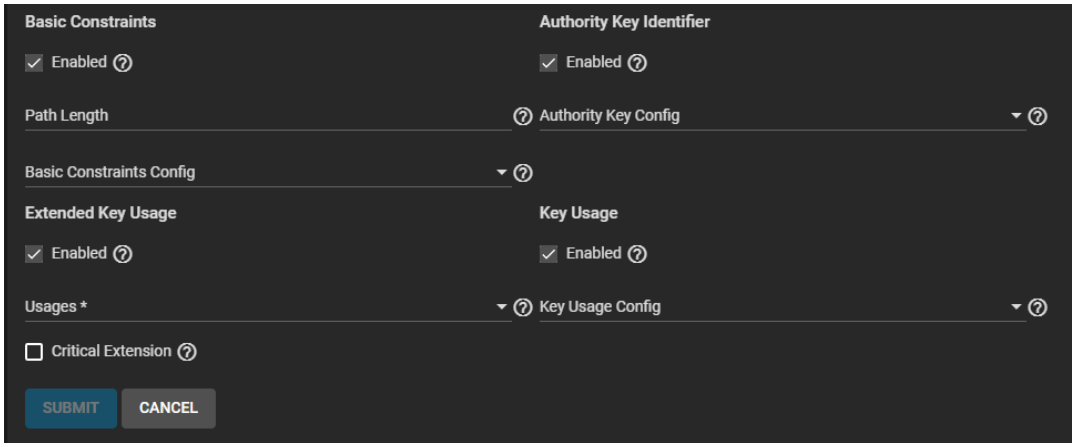
4. Enter or select the **Certificate Subject** settings.



a. Enter the geographic information in **Country**, **Locality**, **Organizational Unit** (optional), **Common Name**, **State**, **Organization**, **Email**, and **Subject Alternate Names**.

b. (Optional) Enter a fully-qualified hostname (FQDN) that is unique within a certificate chain in **Common Name**.

5. Select enable and select extensions to use if you did not select an option in **Profiles**. If manually selecting and entering extension:



a. Select **Enable**, then enter the extensions for **Basic Constraints**.

Enter a value in **Path Length** that determines how many non-self-issued intermediate certificates can follow the certificate in a valid certification path. Entering **0** allows a single additional certificate to follow in the certificate path. Then select the extension(s) to use.

Select an option from the **Basic Constraints Config** dropdown list. Select **CA** to use a certificate authority. Selecting **Critical Extension** can result in rejection of the certificate by the system that is using the certificate if that system does not recognize the extension.

b. Select **Enable**, then enter the extensions for **Authority Key Identifier**.

Enabling **Authority Key Config** adds the authority key identifier extension which provides a means of identifying the public key corresponding to the private key used to sign the certificate. Used when an issue has multiple signing keys, possibly due to multiple concurrent key pairs or due to changeover. Options are **Authority Cert Issuer** or **Critical Extension**.

c. Select **Enable**, then enter the extensions for **Extended Key Usage**. Select one or more usages for the public key from the **Usages** dropdown list. TrueNAS uses Extended Key Usage for end-entity certificates.

Enable **Critical Extension** to identify this extension as critical for the certificate. Do not enable **Critical Extension** if **Usages** contains **ANY_EXTENDED_KEY_USAGE**.

Using **Extended Key Usage** and **Key Usage** extensions requires that the certificate purpose is consistent with both extensions. See RFC 3280, section 4.2.1.13 for more details.

6. Click **Submit** to create the CA.

Importing a CA

Use this procedure to import a CA.

1. Enter a name for this certificate.

2. Select **Import CA** from the **Type** dropdown list.

3. Copy the certificate for the CA you want to import and paste it into the **Certificate** field.
4. Paste the certificate private key of at least 1024 bits in length into **Private Key** when available.
5. Enter and confirm the passphrase for the private key into **Passphrase** and **Confirm Passphrase**.
6. Click **Submit**.

Deleting a CA

Before deleting a CA, verify it is not used by another service such as S3, FTP, etc. You cannot delete a CA when in use by other services.

Also, before you can delete a CA, you need to delete certificates issued by the CA or those relying on the CA. If you receive an error that mentions foreign keys reference, ensure the certificates on your system do not use the CA you want to delete.

Adding Certificates or CSRs

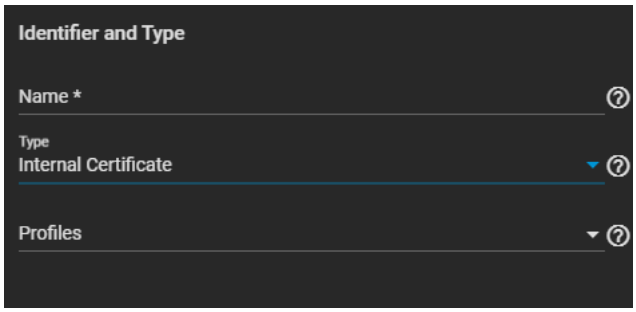
By default, TrueNAS comes equipped with an internal, self-signed certificate that enables encrypted access to the web interface.

You can either import or create a new certificate or signing request by navigating to **System > Certificates** and clicking **ADD**.

Adding Internal Certificates

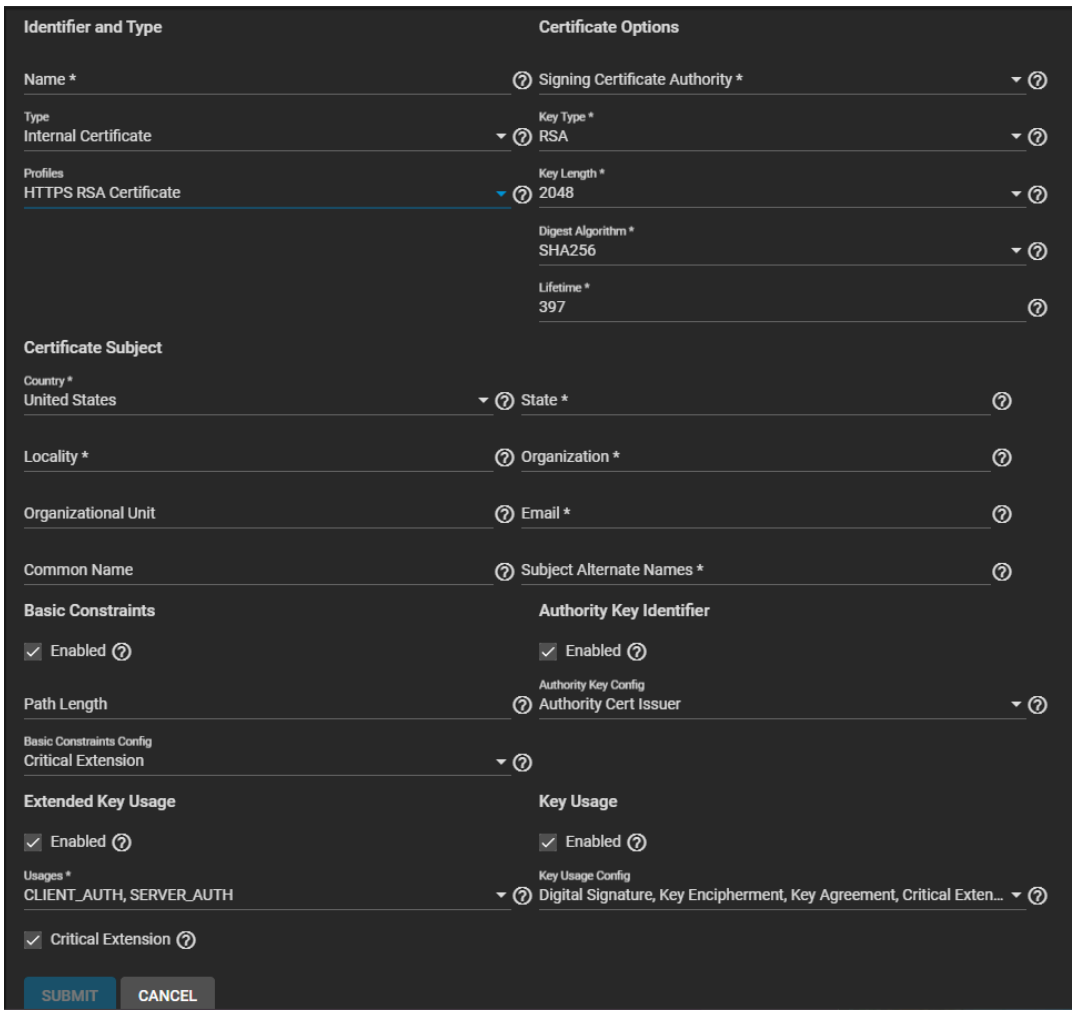
To add an internal certificate:

1. Enter the name for the certificate, then select **Internal Certificate** from the **Type** dropdown list.

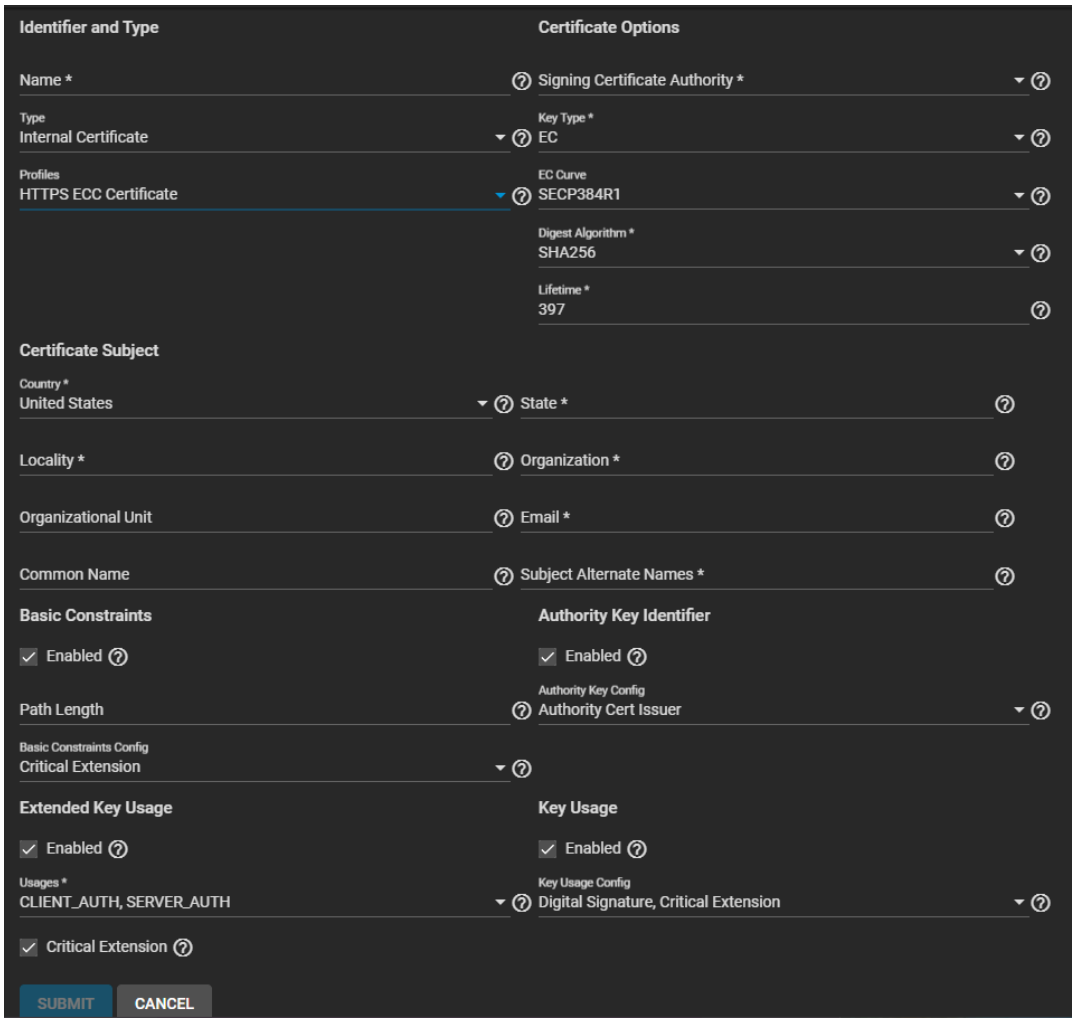


2. Select an option from the **Profiles** dropdown list. A profile for the certificate auto-fills options like **Key Type**, **Key Length**, **Digest Algorithm**. Otherwise, you must set options manually.

   To add an HTTPS RSA certificate, the default certificate type, select **HTTPS RSA Certificate**. The configuration form populates with default settings, enables **Basic Constraints**, **Authority Key Identifier**, **Extended Key Usage**, and **Key Usage**, and set the options for each extension.

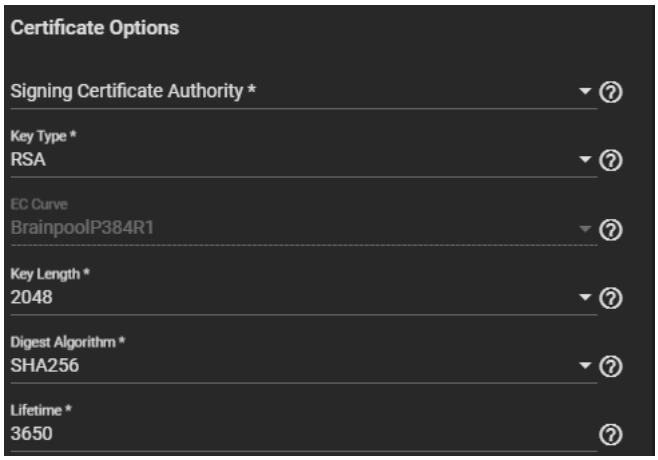


   To add an elliptical curve certificate select **HTTPS ECC Certificate**. The configuration form populates with default settings, enables **Basic Constraints**, **Authority Key Identifier**, **Extended Key Usage**, and **Key Usage**, and set the options for each extension.



To add an OpenVPN certificate, select the client or server option that fits the certificate type you want to create. The configuration form populates with default settings, enables **Basic Constraints**, **Authority Key Identifier**, **Extended Key Usage**, and **Key Usage**, and set the options for each extension.

3. Enter or select the **Certificate Options** settings if you did not select a **Profile** option.



   a. Select a **Signing Certificate Authority** from the dropdown list.

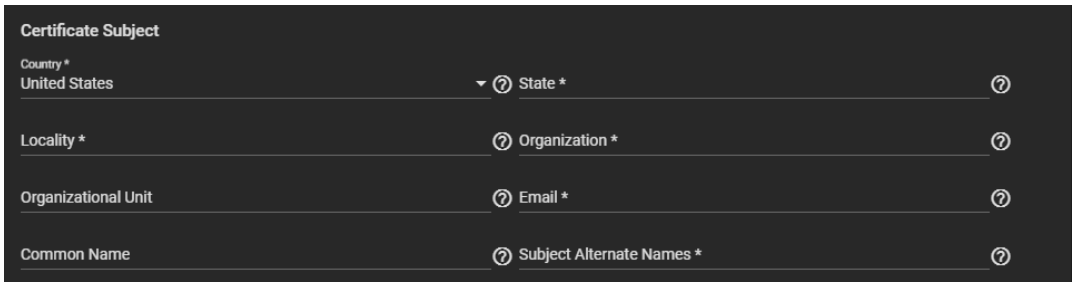
   b. Select a **Key Type** from the dropdown list. We recommend selecting **RSA**.

   c. Select the **Key Length**. We recommend a minimum of **2048** for security reasons.

   d. Select a **Digest Algorithm**. We recommend **SHA256**.

   e. Enter the **Lifetime** of the certificate CA in days to set how long the CA remains valid.

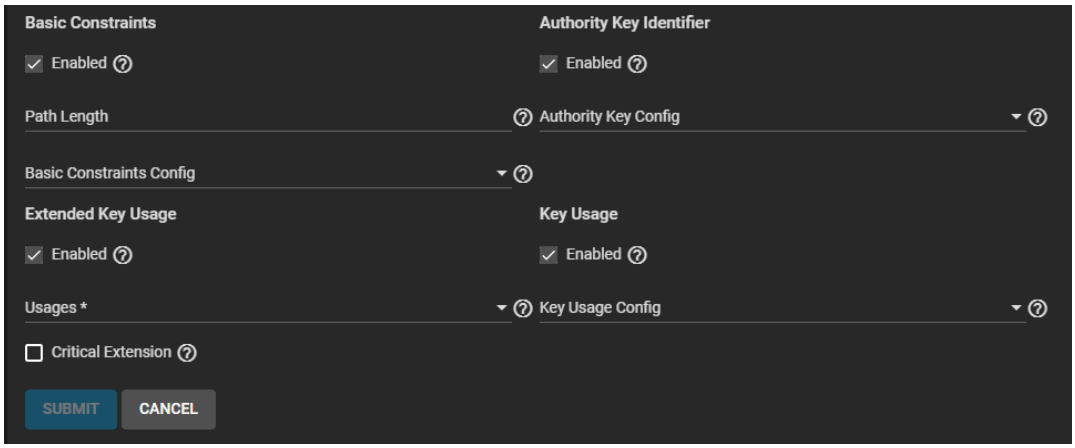
4. Enter or select the **Certificate Subject** setting options.



Enter the geographic and other information in **Country**, **Locality**, **Organizational Unit** (optional), **Common Name**, **State**, **Organization**, **Email**, and **Subject Alternate Names**.

Enter a fully-qualified hostname (FQDN) that us unique within a certificate chain in **Common Name**.

5. Select enable and select extensions to use if you did not select an option in **Profiles**. If manually selecting and entering extension:



a. Select **Enable**, then enter the extensions for **Basic Constraints**.

Enter a value in **Path Length** that determines how many non-self-issued intermediate certificates can follow the certificate in a valid certification path. Entering **0** allows a single additional certificate to follow in the certificate path. Then select the extension(s) to use.

b. Select **Enable**, then enter the extensions for **Authority Key Identifier**.

c. Select **Enable**, then enter the extensions for **Extended Key Usage**. Select one or more usages for the public key from the **Usages** dropdown list. TrueNAS uses Extended Key Usage for end-entity certificates.

Enable **Critical Extension** if you want to identify this extension as critical for the certificate. Do not enable **Critical Extension** if **Usages** contains **ANY_EXTENDED_KEY_USAGE**.

Using **Extended Key Usage** and **Key Usage** extensions requires that the certificate purpose is consistent with both extensions. See RFC 3280, section 4.2.1.13 for more details.

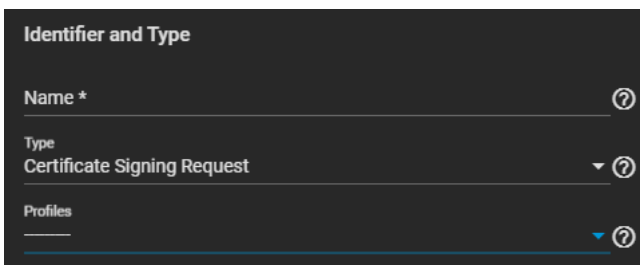
d. Select **Enable**, then enter the extensions for **Key Usage**. Select any extensions from the **Key Usage Config** dropdown list.

6. Click **Submit**.

Creating a Certificate Signing Request

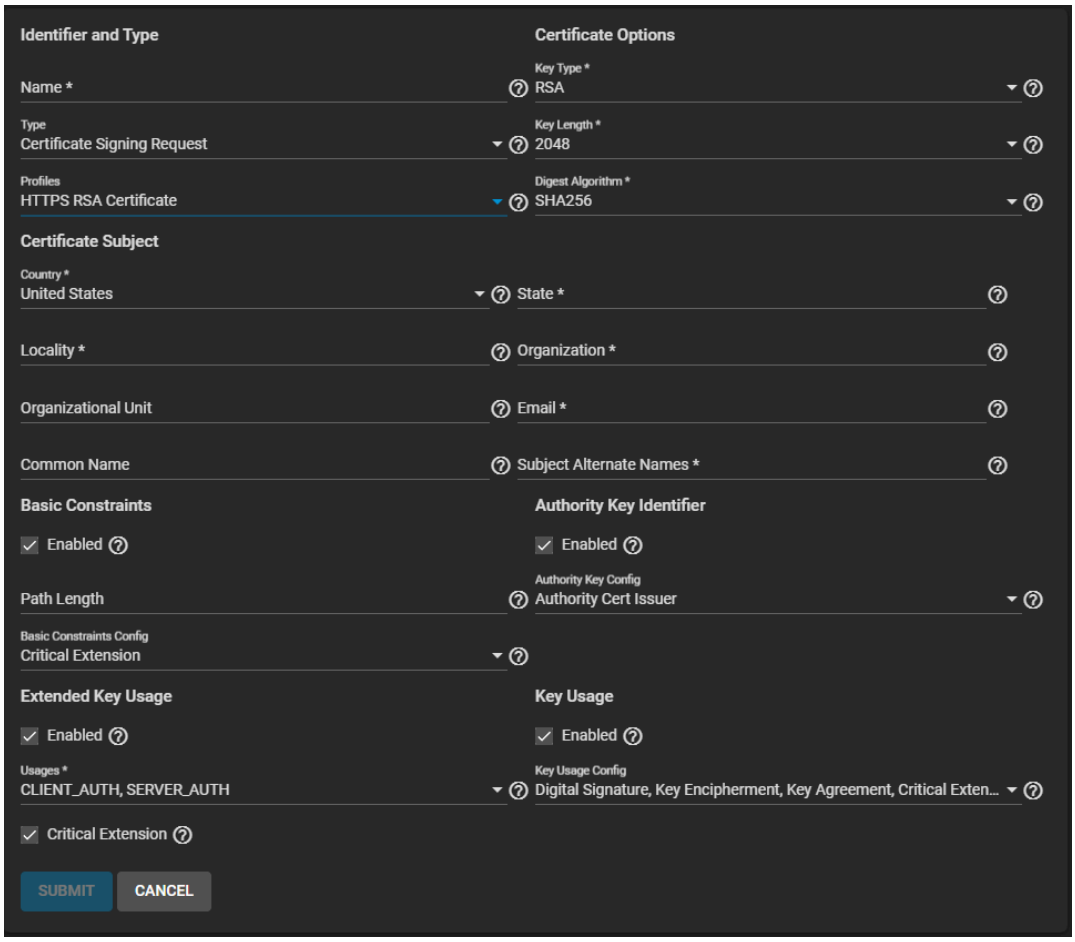
To add a certificate singing request (CSR) certificate:

1. Enter the name for the certificate, then select **Certificate Signing Request** from the **Type** dropdown list.

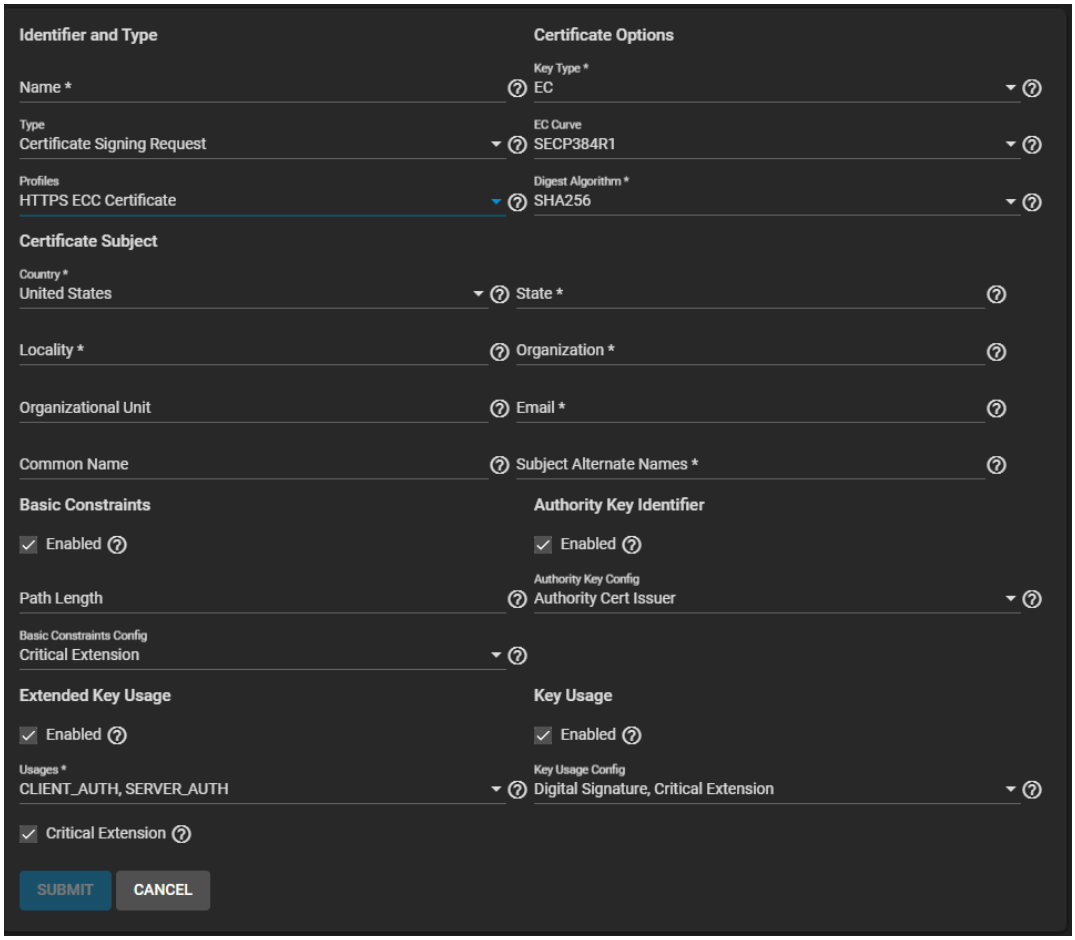


2. Select **Certificate Signing Request** from the **Profiles** dropdown list. A profile for the certificate auto-fills options like **Key Type**, **Key Length**, **Digest Algorithm**. Otherwise, you must set options manually.

To use an HTTPS RSA certificate, the default certificate type, select **HTTPS RSA Certificate**. The configuration form populates with default settings, enables **Basic Constraints**, **Authority Key Identifier**, **Extended Key Usage**, and **Key Usage**, and set the options for each extension.

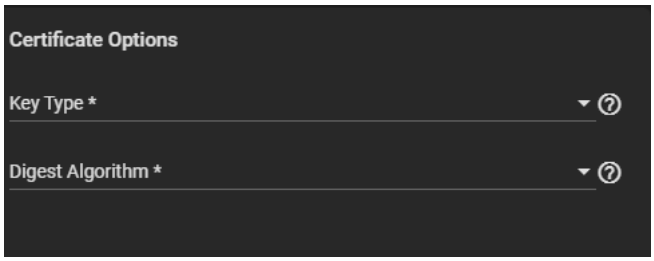


To use an elliptical curve certificate, select **HTTPS ECC Certificate**. The configuration form populates with default settings, enables **Basic Constraints**, **Authority Key Identifier**, **Extended Key Usage**, and **Key Usage**, and set the options for each extension.



To use an OpenVPN certificate, select the client or server option that fits the certificate type. The configuration form populates with default settings, enables **Basic Constraints**, **Authority Key Identifier**, **Extended Key Usage**, and **Key Usage**, and set the options for each extension.

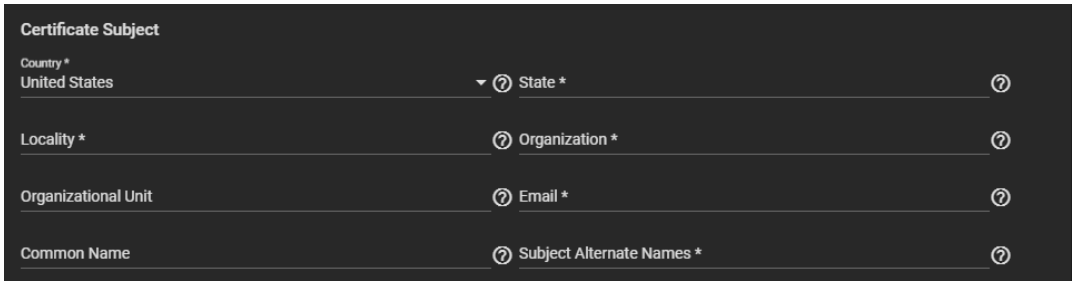
3. Enter or select the **Certificate Options** settings if you did not select a **Profile** option.



a. Select a **Key Type** from the dropdown list. We recommend selecting **RSA**.

b. Select a **Digest Algorithm**. We recommend **SHA256**.

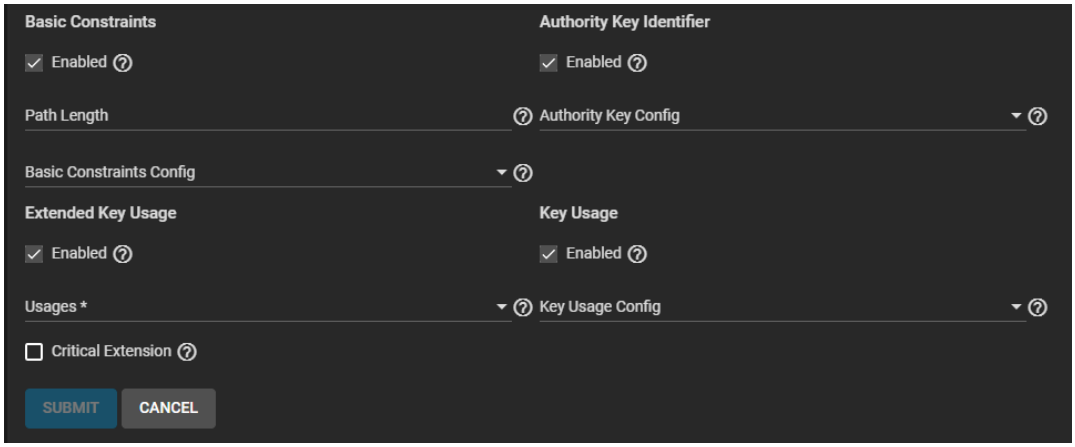
4. Enter or select the **Certificate Subject** setting options.



Enter the geographic and other information in **Country**, **Locality**, **Organizational Unit** (optional), **Common Name**, **State**, **Organization**, **Email**, and **Subject Alternate Names**.

Enter a fully-qualified hostname (FQDN) that us unique within a certificate chain in **Common Name**.

5. Select enable and select extensions to use if you did not select an option in **Profiles**. If manually selecting and entering extension:



a. Select **Enable**, then enter the extensions for **Basic Constraints**.

Enter a value in **Path Length** that determines how many non-self-issued intermediate certificates can follow the certificate in a valid certification path. Entering **0** allows a single additional certificate to follow in the certificate path. Then select the extension(s) to use.

b. Select **Enable**, then enter the extensions for **Authority Key Identifier**.

c. Select **Enable**, then enter the extensions for **Extended Key Usage**. Select one or more usages for the public key from the **Usages** dropdown list. TrueNAS uses Extended Key Usage for end-entity certificates.

Enable **Critical Extension** if you want to identify this extension as critical for the certificate. Do not enable **Critical Extension** if **Usages** contains **ANY_EXTENDED_KEY_USAGE**.

Using **Extended Key Usage** and **Key Usage** extensions requires that the certificate purpose is consistent with both extensions. See RFC 3280, section 4.2.1.13 for more details.

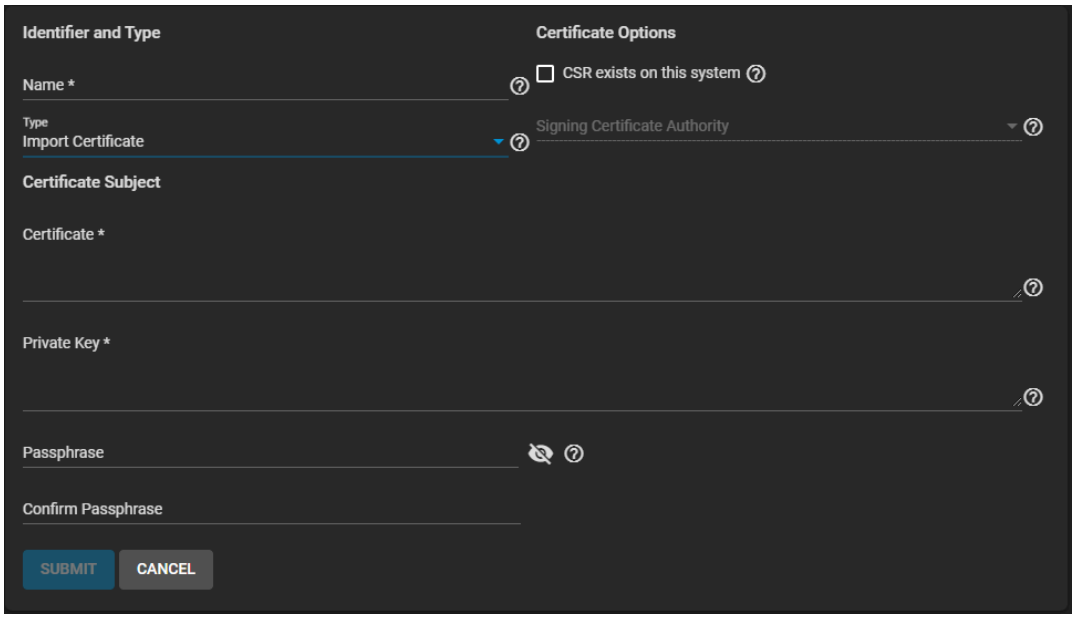
d. Select **Enable**, then enter the extensions for **Key Usage**. Select any extensions from the **Key Usage Config** dropdown list.

6. Click **Submit**.

Importing a Certificate

To import a certificate:

1. Select **Import Certificate** as the **Type**.

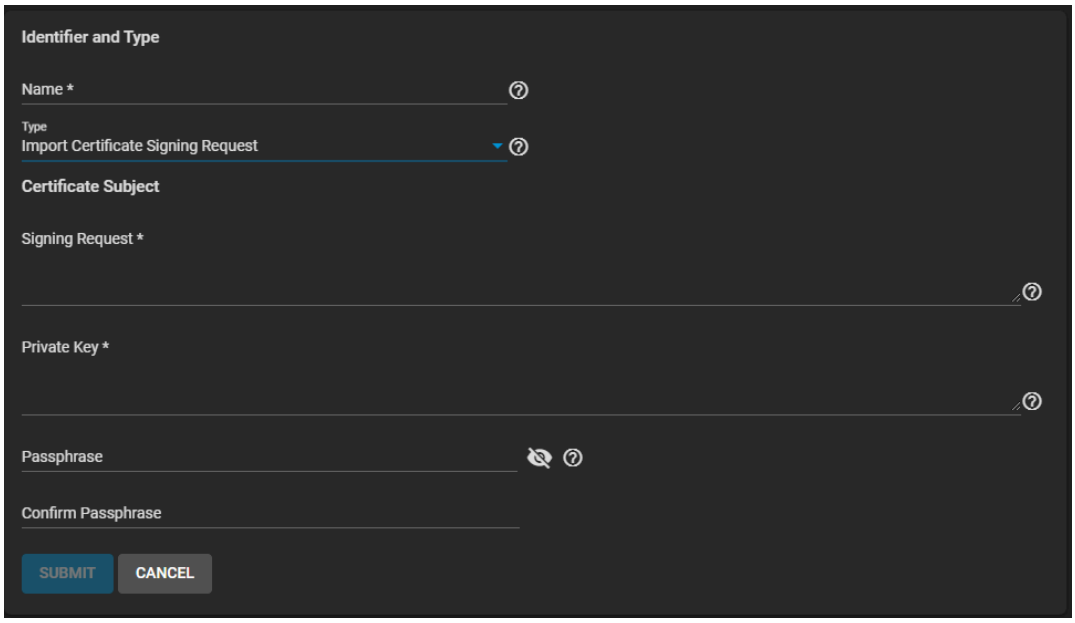


2. Select the **Certificate Options**. To import a previously-added certificate for a CSR, select **CSR exists on this system**, then select one from the **Signing Certificate Authority** dropdown list.
3. Copy the certificate for the CA you want to import and paste it into the **Certificate** field.
4. Paste the certificate key that is least 1024 bits long into **Private Key** when available.
5. Enter and confirm the Private Key **Passphrase**.
6. Click **Submit**.

Importing a Certificate Signing Request

To import a certificate signing request (CSR):

1. Select **Import Certificate Signing Request** as the **Type**.



2. Copy the certificate for the CA you want to import and paste it into the **Certificate** field.
3. Paste the certificate key that is least 1024 bits long into **Private Key** when available.
4. Enter and confirm the Private Key **Passphrase**.
5. Click **Submit**.

Configuring ACME DNS

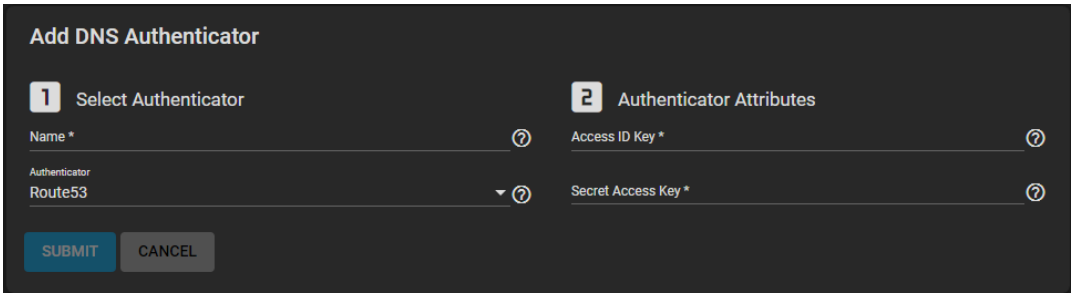
> This feature is only available in the open-source supported TrueNAS CORE.

Automatic Certificate Management Environment (ACME) is available for automating certificate issuing and renewal. The user must verify ownership of the domain before certificate automation is allowed.

ACME certificate automation requires an ACME DNS Authenticator and a Certificate Signing Request.

Adding ACME DNS Authenticators

Go to **System > ACME DNS** and click **ADD**.

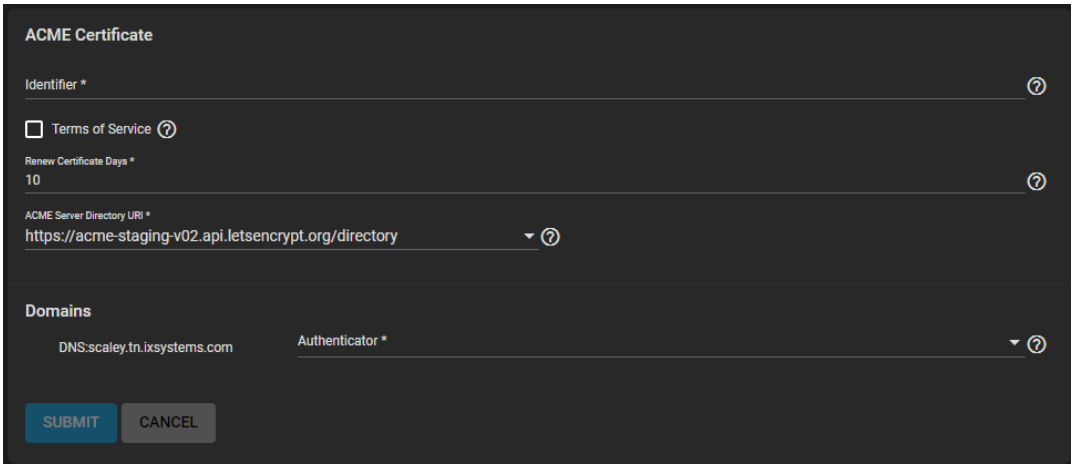


Name the authenticator. Leave **Authenticator** set to **Route53**. Enter the **Access ID Key** and **Secret Access Key** from Amazon.

> Amazon Route 53 is the only supported DNS provider in TrueNAS CORE. See the AWS documentation for more details about generating the **Access ID Key** and **Secret Access Key**.

Click **SUBMIT** to register the DNS Authenticator and add it to the authenticator options for ACME Certificates.

Creating ACME Certificates



You can create ACME certificates for existing certificate signing requests. The certificates use an ACME DNS authenticator to confirm domain ownership. Then, they are automatically issued and renewed.

To create a new ACME certificate, go to **System > Certificates**, click ⋮ (Options) for an existing certificate signing request, and select **Create ACME Certificate**.

Give the ACME certificate an identifier (name), and accept the TOS by setting **Terms of Service**.

For the **Authenticator**, select the ACME DNS authenticator you created, then click **SUBMIT**.

Using Two-Factor Authentication

We recommend two-factor authentication (2FA) for increased security. TrueNAS offers 2FA to ensure that a compromised administrator (*root*) password alone cannot grant access to the administrator interface. To utilize 2FA, you need a mobile device with Google Authenticator installed. Other authenticator applications can be used, but you will need to confirm the settings and QR codes generated in TrueNAS are compatible with your particular app before permanently activating 2FA.

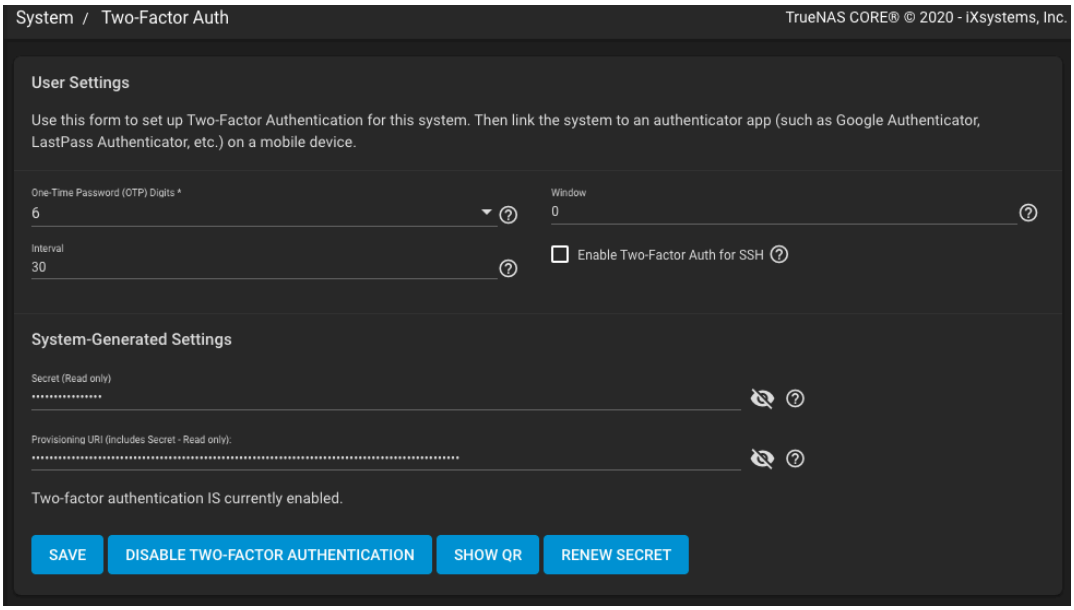
▼ What is 2FA, and why would I want to enable it?

Two-factor authentication (2FA) is an extra layer of security that prevents someone from logging in, even if they have your password. This extra security measure requires you to verify your identity using a randomized 6-digit code that regenerates every 30 seconds (unless modified).

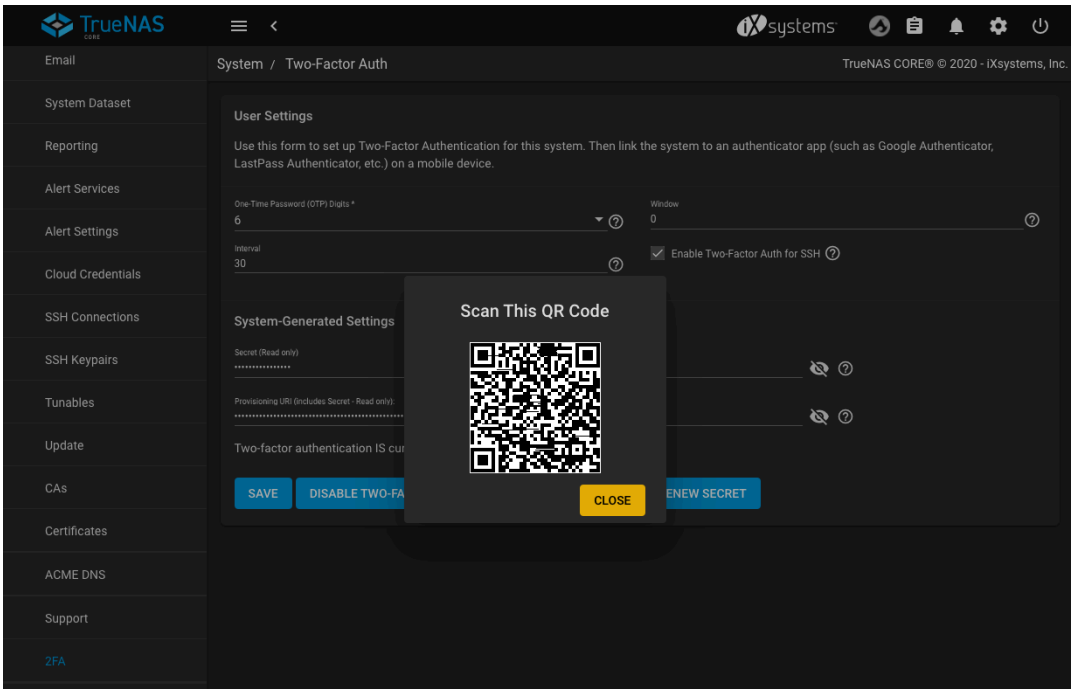
Setting Up Two-Factor Authentication

> Set up a second 2FA device as a backup before proceeding.

Go to **System > 2FA** and click **ENABLE TWO-FACTOR AUTHENTICATION**. Then, click **CONFIRM**.



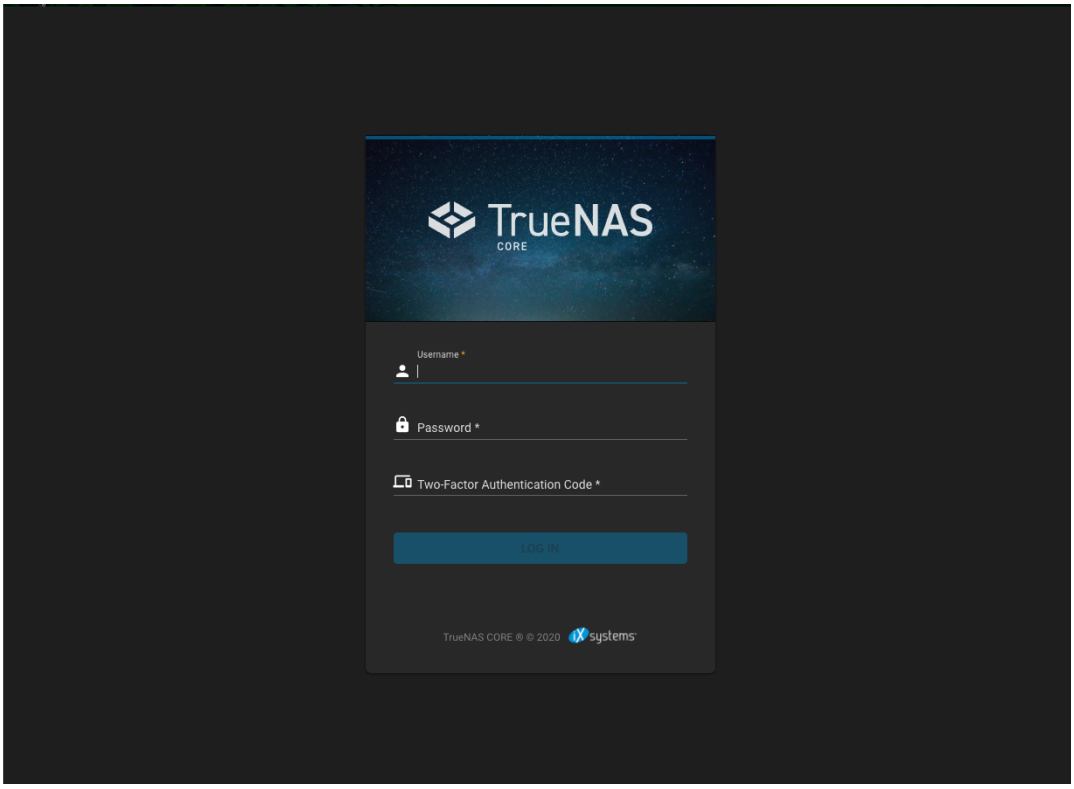
Click **SHOW QR**, then scan it using Google Authenticator on the mobile device.



Using 2FA to Log In to TrueNAS

Enabling 2FA changes the login process for both the TrueNAS web interface and SSH logins:

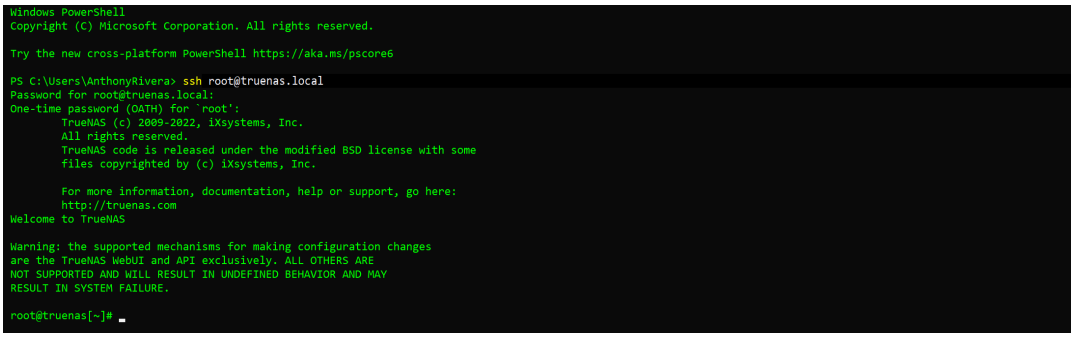
Web UI Login



The login screen has another field for the randomized authenticator code. If this field isn't immediately visible, refresh the browser.

Enter the code from the mobile device (complete without the space) in the login window with the *root* username and password.

SSH Login



Set **Enable Two-Factor Auth for SSH** in **System > 2FA**, then go to **Services > SSH** and click .

Set **Log in as Root with Password** and click **SAVE**. Toggle the **SSH** service and wait for the status to show that it is **RUNNING**.

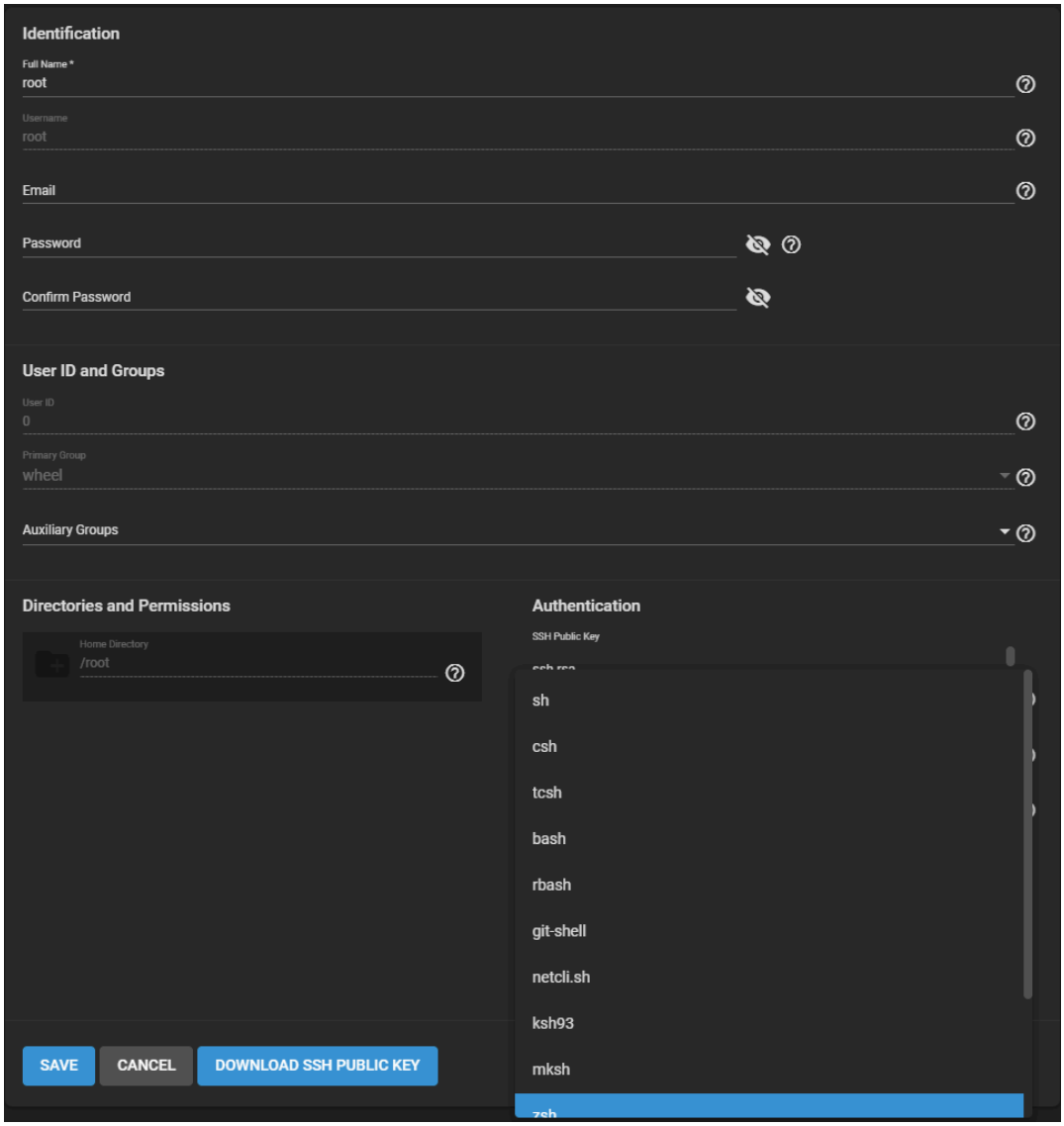
Open a Command Prompt or Terminal and SSH into TrueNAS using the system hostname or IP address, *root* account username and password, and the 2FA code from the mobile device.

Changing the Default Shell

The default shell for an account is the environment that user accesses in a local or SSH session. The default shell for a new installation is `zsh`.

You can change the default shell in **Accounts > Users**.

1. Click ❯ for the root user and click **Edit**.



2. Choose the desired shell from the **Shell** dropdown list and click **SAVE**. **Shell** options are:

Shell	Description
csh	C shell for UNIX system interactions.
sh	Bourne shell
tcsh	Enhanced C shell that includes editing and name completion.
bash	Bourne Again shell for the GNU operating system.
ksh93	Korn shell that incorporates features from both *csh* and *sh*.
mksh	MirBSD Korn Shell
rbash	Restricted bash
rzsh	Restricted zsh
scponly	scponly restricts the user's SSH usage to only the `scp` and `sftp` commands.
zsh	Z shell
git-shell	restricted git shell

Shell	Description
nologin	Use when creating a system account or to create a user account that can authenticate with shares but which cannot log in to the TrueNAS system using `ssh`.

Community Guides

Because TrueNAS is both Open Source and complicated, the massive user community often creates recommendations for specific hardware or environments. User-created recommendations can be added in this location, but be aware these are provided “as-is” and are not officially supported by iXsystems, Inc.

/etc/hosts IP Persistence

Description

Domain Name resolution is the process of mapping host or domain names, such as `mytruenas` or `truenas1.mycompany.com`, to their associated IP addresses. This is done by a variety of methods. The quickest method is to read entries in the **hosts** file, which is a local text file containing a list of IP addresses mapped to domain/host names. Every operating system (OS) that communicates through the TCP/IP protocol has a **hosts** file.

The **hosts** file can speed up name resolution when a DNS server is not available on the local network. A DNS server runs networking software that allows it to join the Domain Name System. This is the standard service used on the Internet for name resolution. When adding entries to a TrueNAS system **hosts** file, use the TrueNAS web interface to save the entries directly to the configuration database. Do *not* edit the **hosts** file directly, as any changes are overwritten by the configuration database during reboot.

Errors

▼ IвЂ™m trying to use NFS, SSH, and FTP, but I keep receiving reverse DNS or timeout errors.

The fastest domain name resolution method is for the operating system to read the **hosts** file, but if there are no matching entries in the **hosts** file, a DNS server is queried instead. This is a slower process as the OS has to find the DNS server, send it a query, and wait for an answer. Timeout errors are common for some network protocols, such as SSH, FTP and NFS, as their connection requests can time out before a DNS server replies. To speed up name resolution, add entries for commonly used hosts to the **hosts** file.

Fix

To add an entry to the **hosts** file, use a browser to log in to your TrueNAS web interface and follow these steps:

1. Go to **Network > Global Configuration**.
2. Scroll down to the **Host name database** field and add an entry for the TrueNAS system in the format *IP_address space hostname*.
3. Click **Save**.

Setting ACL Permissions for Jailed Applications

Various Plugin jails require permissions to access datasets.

Unless otherwise modified, a dataset is owned by the user **root** and group **wheel**. Jailed processes like Plex run as their own user. As a result, a default installation of the Plex plugin cannot read or write any datasets and thus cannot access media files stored in those datasets. The TrueNAS user must explicitly configure dataset permissions to allow the plugin to use the dataset.

Creating a Dataset Access Control List

To create a dataset Access Control List (ACL) for an application, you need to obtain the Application user ID. For example, the Plex ID is **972**.

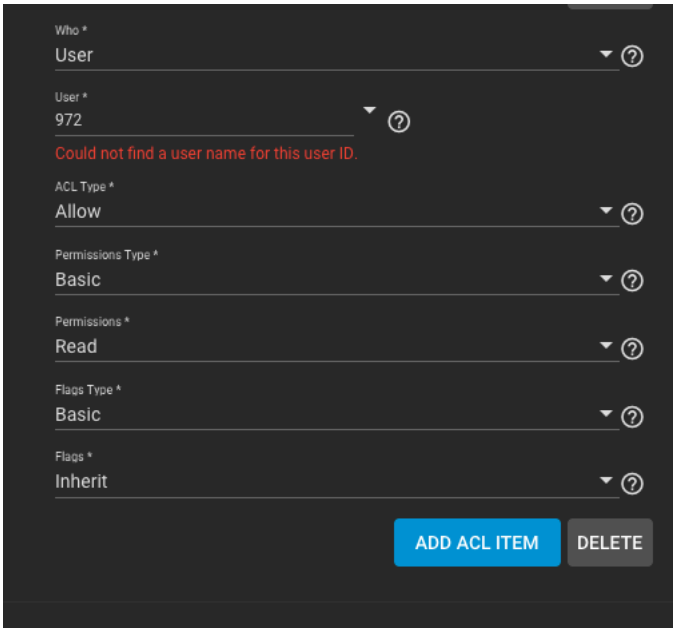
Other popular Plugin user IDs include:

- Radarr = **352**
- Sonarr = **351**
- Transmission = **921**
- Sabnzbd = **350**

To create an ACL for a dataset, log in to the UI and go to **Storage > Pools**. Click the three dot icon ⋮ and select **Edit Permissions**. Click the **Add ACL Item** button to create a new entry. New entries appear at the bottom of the list of existing ACL items.

Continuing with Plex as our example, we would enter the following:

```
Who: User
User: 972 (Don't worry if it says "Could not find a username for this ID")
ACL Type: Allow
Permissions Type:
Basic Permissions: Read
Flags Type: Basic
Flags: Inherit
```



If files already exist in the dataset, click the **Apply permissions recursively** checkbox and click **Save**.

Managing TLS Ciphers

TrueNAS accepts different Transport Layer Security (TLS) cipher suites for secure web interface connections. Only use TLS 1.2 or newer for best security. By default, all options are available if you need to adjust this setting to match your particular network environment or security concerns.

Allow or Restrict TLS Ciphers

Go to **System > General** and click on **HTTPS Protocols** to open a drop-down menu with the various cipher suites.

Unsetting a cipher restricts its use in TrueNAS. After enabling or disabling a cipher, you must reboot the TrueNAS system.

TLSv1

TLSv1 provides Internet communication security using encryption and other secure messaging techniques. While not officially deprecated, TLSv1 was considered obsolete in 2008. For security, we discourage enabling TLSv1 unless your network environment requires it.

TLSv1.1

TLSv1.1 is a revision of v1.0 with additional protections against CBC attacks. While not officially deprecated, TLSv1.1 was considered obsolete in 2008. For security reasons, users are encouraged to avoid enabling this suite unless required by the network environment.

TLSv1.2

TLSv1.2 increases the protocol's ability to handle cryptographic algorithms. TLSv1.2 represented a major step forward in security effectiveness and resulted in the "soft" deprecation of TLS versions 1.0 and 1.1.

TLSv1.3

TLSv1.3 represents another major improvement to the protocol. TLSv1.3 removes legacy or insecure encryption algorithms, adds encryption for handshake messages, and separates authentication and key exchange concepts.

Tasks

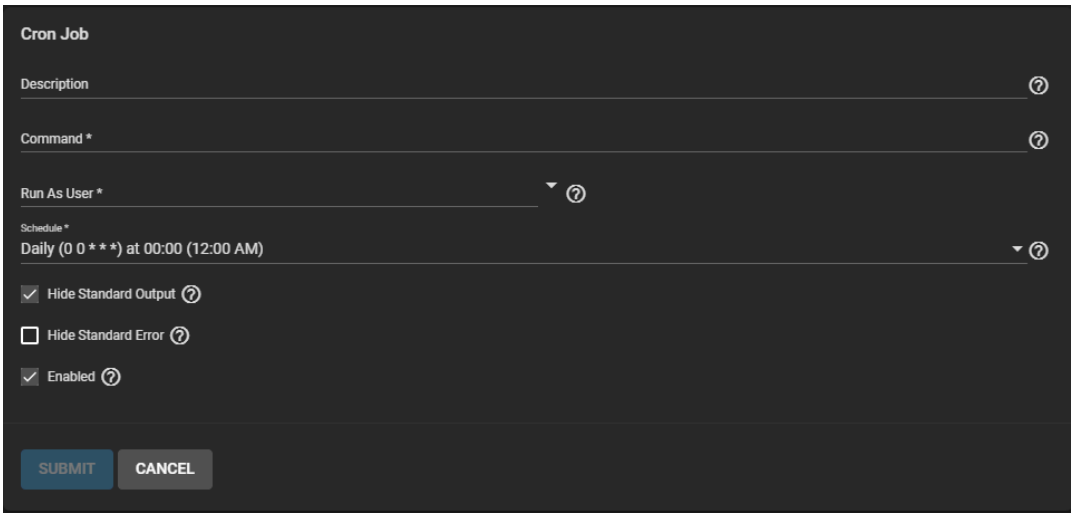
TrueNAS includes an easy to use interface for common tasks a sysadmin needs to preform on a NAS on a regular basis. These can roughly be broken down into three groups.

Creating Cron Jobs

TrueNAS allows users to run specific commands or scripts on a regular schedule using cron(8).

Creating a Cron Job

Go to **Tasks > Cron Jobs** and click **ADD**.



The **Description** helps identify the purpose of the cron job and is optional.

Enter the **Command** to run on the **Schedule**. Alternately, enter the path to a script file to run instead of a specific command.

> Don't forget to define the shell type when using a path to a script file. For example, a script written for *sh* must be specified as *sh /mnt/pool1/helloWorld.sh*.

Select a TrueNAS user account with the necessary permissions to run the **Command** or script.

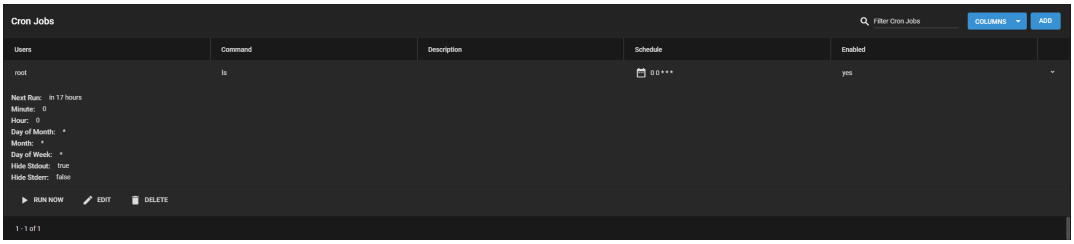
Next, define the **Command Schedule**.

Additional Options:

- When **Hide Standard Output** (stdout) is unset, TrueNAS mails any standard output to the user account that runs the **Command**.
- When **Hide Standard Error** (stderr) is unset, TrueNAS mails any error output to the user account that runs the **Command**. Unsetting **Hide Standard Error** helps debug the **Command** or script if an error occurs.
- Unsetting **Enabled** only keeps the task from automatically running. You can still save the cron job and run it manually.

Managing a Cron Job

Go to **Tasks > Cron Jobs** and click the ❯ next to an entry to see details and options.



Clicking **RUN NOW** immediately starts the job **Command**, separately from any **Schedule**. **EDIT** changes any setting available during task creation. **DELETE** removes the cron job from TrueNAS. Once you delete a cron job, you cannot restore the job configuration.

Creating Init/Shutdown Scripts

Create an Init/Shutdown Script

TrueNAS can schedule commands or scripts to run at system startup or shutdown.

Go to **Tasks > Init/Shutdown Scripts** and click **ADD**.

Enter a **Description**, then select a **Type**.

Command Type

Enter a command with any options you want. You can find commands here or on our Community Forums.

▼ Can I use a path for the Command?

You can also include the full path to a command in the entry. Scheduled commands must be in the default path. You can find the path to a command by entering `which COMMAND` in the shell, where *COMMAND* is the command you want to locate. When available, the path to the command displays:

```
[root@freenas ~]# which ls
/bin/ls
```

Select when you want the **Command** to run and fill out the rest of the fields to your needs, then click **SUBMIT**.

Script Type

Select the path to the **Script**. The **Script** runs using sh(1). You can find some helpful scripts on our Community Forums.

Select when you want the **Script** to run and fill out the rest of the fields to your needs, then click **SUBMIT**.

Managing an Init/Shutdown Script

> Always test the script to verify it executes and achieves the desired results. All init/shutdown scripts are run with `sh`.

All saved Init/Shutdown tasks are in **Tasks > Init/Shutdown Scripts**. Click ⋮ (Options) next to a task to **EDIT** or **DELETE** that task.

Creating Rsync Tasks

Rsync is a fast and secure way to copy data to another system, either for backup or data migration purposes. An rsync task requires configuration of both a **Host** and **Remote** system. These instructions assume a TrueNAS system for both the **Host** and **Remote** configurations.

Basic Requirements

Rsync requires a dataset with the needed data on the **Host** or **Remote** system. Rsync provides the ability to either push or pull data. When using rsync to push, data copies from a **Host** system to a **Remote** system. When using rsync to pull, data pulls from a **Remote** system. It is then put on the **Host** system.

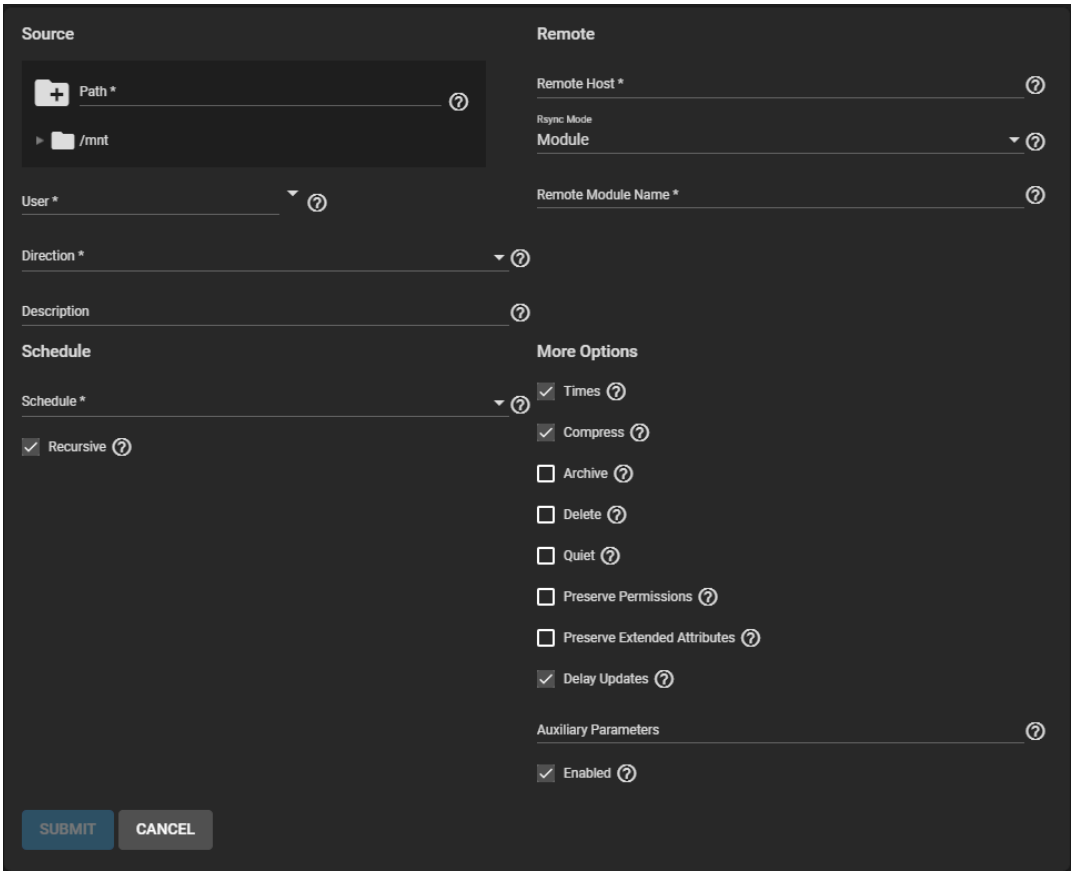
TrueNAS has extra requirements depending on if you choose the **Module** or **SSH** rsync mode.

Rsync Services Requirements

Before you create an rsync task on the **Host** system, you must create a module on the **Remote** system. The **Remote** system must have rsync service activated. When TrueNAS is the **Remote** system, create a module by going to **Services** and clicking ✎ for the rsync service. Click the **Rsync Module** tab, then click **ADD**. See ConfiguringRsync for more information.

Creating a Module Mode Rsync Task

Log in to the **Host** system interface, go to **Tasks > Rsync Tasks**, and click **ADD**.



Select the **Source** dataset to use with the rsync task and a **User** account to run the rsync task. Select a **Direction** for the rsync task.

Select a **Schedule** for the rsync task.

Enter the **Remote Host** IP address or host name. Use the format `username@remote_host` when the user name differs on the **Remote** host. Select **Module** in the **Rsync Mode** dropdown list. Enter the **Remote Module Name** as it appears on the **Remote** system.

Configure the remaining options according to your specific needs.

Clearing **Enabled** disables the task schedule. You can still save the rsync task and run it as a manual task.

Creating an SSH Mode Rsync Task

SSH Requirements

The **Remote** system must have **SSH** enabled. To enable SSH in TrueNAS, go to **Services** and click the **SSH** toggle button. The toggle button turns blue when the service is on.

The **Host** system needs an established SSH connection to the **Remote** for the rsync task. To create the connection, go to **System > SSH Connections** and click **ADD**. Configure a **Semi-automatic** connection and from the **Private Key** dropdown list select **Generate New**.

▼ Can this be set up in a command line instead?

Go to the shell on the system entered in the **Host** field. When a TrueNAS account other than *root* manages the rsync task, enter `su - USERNAME`, where *USERNAME* is the TrueNAS user account that runs the rsync task. Enter `ssh-keygen -t rsa` to create the key pair. When prompted for a password, press `Enter` without setting a password (a password breaks the automated task). Here is an example of running the command:

```
truenas# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter the same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:NZMgbuPvTHeEqi3SA/U5wW8un6AWrx8ZsRQdbJJHmR4 tester@truenas.local
The key randomart image is:
+---[RSA 2048]----+
|       . o=o+    |
|      . .ooE.    |
|       +.o==.    |
|      o.oo+.+    |
|       ...S+. .  |
|     . ..++o.    |
|      o oB+. .   |
|     . =Bo+.o    |
|      o+==oo     |
+----[SHA256]-----+
```

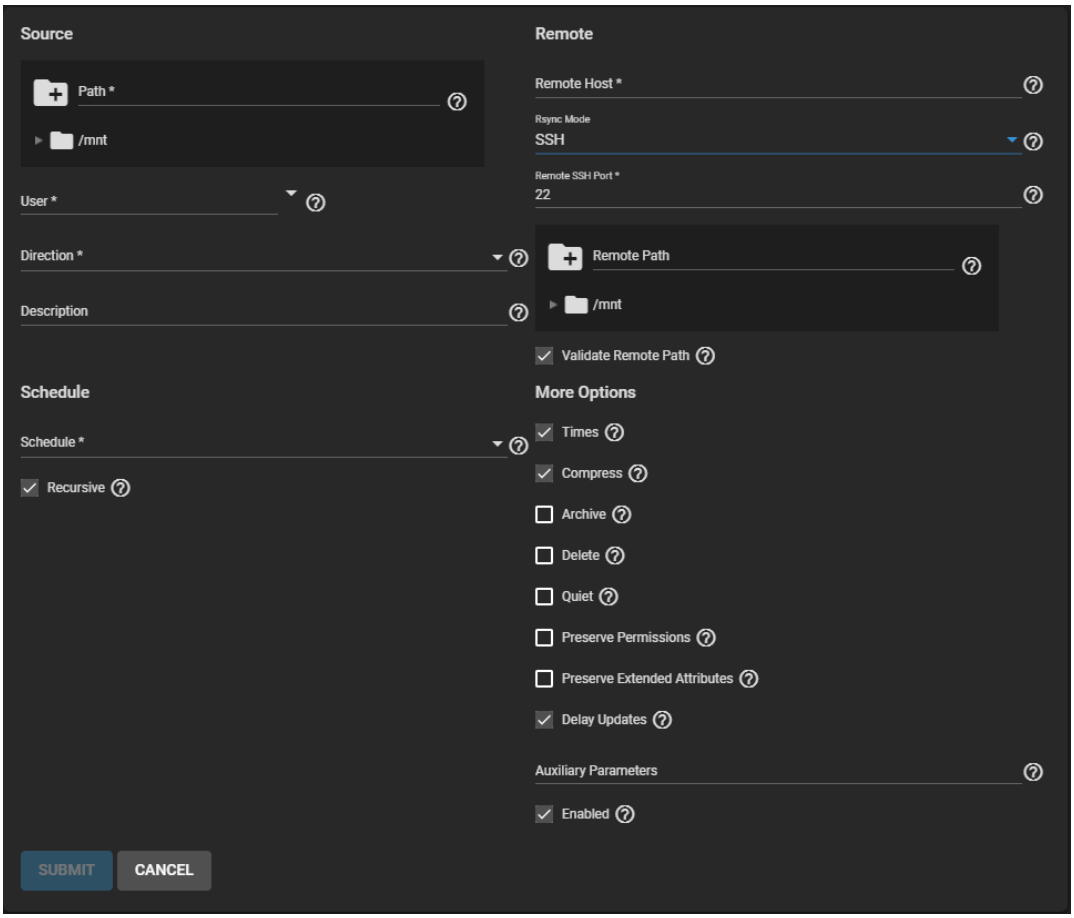
The default public key location is ~/.ssh/id_rsa.pub. Enter `cat ~/.ssh/id_rsa.pub` to see the key and copy the file contents. Copy it to the corresponding user account on the **Remote** system in **Accounts > Users**. Click **EDIT** and paste the key into **SSH Public Key**.

Next, copy the host key from the **Remote** system to the **Host** system user .ssh/known_hosts directory, using `ssh-keyscan`.

On the host system, open the shell and enter `ssh-keyscan -t rsa` *`remoteIPaddress`* `>>` *`userknown_hostsDir`* where *remoteIPaddress* is the **Remote** system IP address and *userknown_hostsDir* is the known_hosts directory on the host system. Example: `ssh-keyscan -t rsa 192.168.2.6 >> /root/.ssh/known_hosts`.

SSH Mode Process

Go to **Tasks > Rsync Tasks** and click **ADD**.



Configure the SSH settings first by selecting **SSH** in the **Rsync Mode** dropdown list. Enter the **Port** number and **Remote Path**.

Define the **Source** dataset for the rsync task and select an account in **User**. The name in **User** must be identical to the SSH Connection **Username**.

Select a direction for the rsync task, either **Push** or **Pull**, and define the task **Schedule**.

Enter the **Remote** host IP address or host name. Use the format `username@remote_host` if the user name differs on the **Remote** host. Configure the remaining options according to your specific needs.

Clearing the **Enabled** checkbox disables the task schedule without deleting the configuration. You can still run the rsync task by going to **Tasks > Rsync Tasks** and clicking ❯, then **RUN NOW**.

Rsync Service and Modules

The rsync task does not work when the related system service is off. To turn the rsync service on, go to **Services** and click the **rsync** toggle button. The toggle button turns blue when the service is on. See Configuring Rsync for more information on rsync configuration and module creation.

Running S.M.A.R.T. Tests

S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) is an industry standard for disk monitoring and testing. Disks are monitored for problems using several different kinds of self-tests. TrueNAS can adjust when and how alerts for S.M.A.R.T. are issued. When S.M.A.R.T. monitoring reports an issue, we recommend you replace that disk. Most modern ATA, IDE, and SCSI-3 hard drives support S.M.A.R.T. Refer to your respective drive documentation for confirmation.

S.M.A.R.T. tests run on a disk. Running tests can reduce drive performance, so we recommend scheduling tests when the system is in a low-usage state. Avoid scheduling disk-intensive tests at the same time! For example, do not schedule S.M.A.R.T. tests on the same day as a disk scrub or resilver.

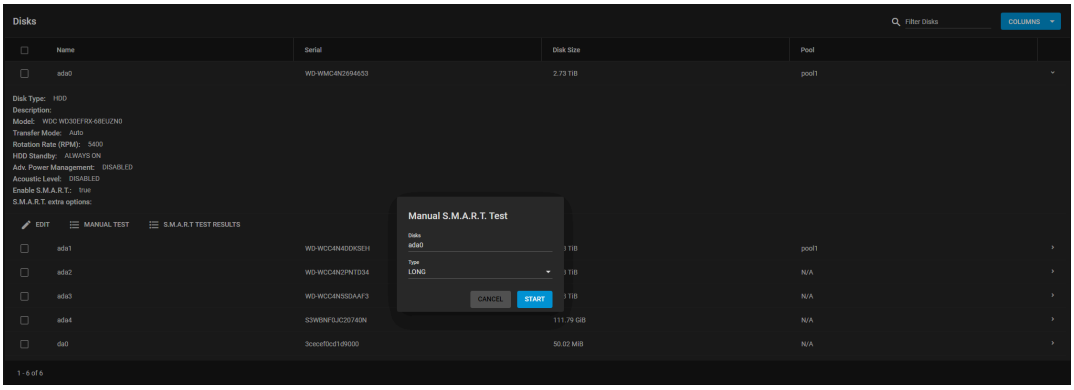
▼ How do I check or change S.M.A.R.T. testing for a disk?

Go to **Storage > Disks** and click › to expand an entry. **Enable S.M.A.R.T.** shows as **true** or **false**.

To enable or disable testing, click **EDIT DISK(S)** and find the **Enable S.M.A.R.T.** option.

Manual S.M.A.R.T. Tests

To quickly test a disk for errors, go to **Storage > Disks** and select the disks to be tested. After selecting the desired disks, click **MANUAL TEST**.



Next, select the test **Type**. Each test type can differ based on the drive connection, ATA or SCSI:

ATA Connection

- **Long** - runs S.M.A.R.T. Extended Self-Test. This scans the entire disk surface and can take many hours on large-volume disks.
- **Short** - runs S.M.A.R.T. Short Self-Test (usually under ten minutes). These are basic disk tests that vary by manufacturer.
- **Conveyance** - runs S.M.A.R.T. Conveyance Self-Test. This self-test routine identifies damage incurred during transporting of the device. This self-test routine requires only minutes to complete.
- **Offline** - runs S.M.A.R.T. Immediate Offline Test. Updates the S.M.A.R.T. attribute values. If the test finds errors, the errors only appear in the SMART error log.

SCSI Connection

- **Long** - runs the *Background long* self-test.
- **Short** - runs the *Background short* self-test.
- **Offline** - runs the default self-test in foreground. No entry is placed in the self-test log.

For more information, refer to smartctl(8).

Click **START** to begin the test. Depending on the test type you choose, the test can take some time to complete. TrueNAS generates alerts when tests discover issues.

▼ Where can I view the test results?

Go to **Storage > Disks**, expand an entry, and click **S.M.A.R.T. TEST RESULTS**. From the shell, use `smartctl` and the name of the drive: `smartctl -l selftest /dev/ada0`.

Automatic S.M.A.R.T. Tests

Go to **Tasks > S.M.A.R.T. Tests** and click **ADD**.

Select the **Disks** to test, **Type** of test to run, and **Schedule** for the task.

> S.M.A.R.T. tests can offline disks! Avoid scheduling S.M.A.R.T. tests simultaneously with scrub or resilver operations.

Saved schedules appear in the **Tasks > S.M.A.R.T. Tests** list.

▼ CLI

To verify the schedule is saved, you can open the shell and enter `smartd -q showtests`.

Service Options

You must enable S.M.A.R.T. service to run automatic S.M.A.R.T. tests.

▼ RAID controllers?

Disable the S.M.A.R.T. service when using a RAID disk controller. The controller monitors S.M.A.R.T. separately and marks disks as a **Predictive Failure** on a test failure.

Periodic Snapshot Tasks

A periodic snapshot task allows scheduling the creation of read-only versions of pools and datasets at a given point in time.

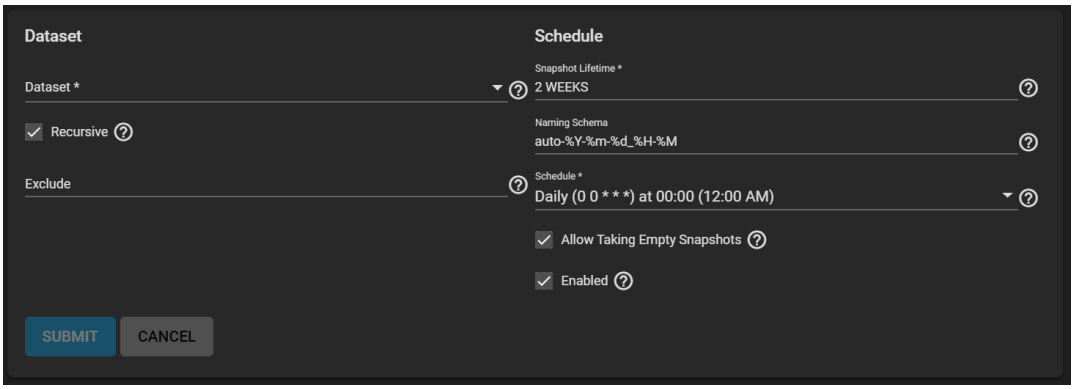
▼ How should I use snapshots?

Snapshots do not make copies of the data, so creating one is quick. It is common to take frequent snapshots every 15 minutes, even for large and active pools. A snapshot with no file changes takes no storage space, but as file changes happen, the snapshot size changes to reflect the size of the changes. In the same way as all pool data, you recover the space after deleting the last reference to the data.

Snapshots keep a history of files, providing a way to recover an older copy or even a deleted file. For this reason, many administrators take snapshots often, store them for a while, and store them on another system, typically using the **Replication Tasks** function. Such a strategy allows the administrator to roll the system back to a specific point in time. If there is a catastrophic loss, an off-site snapshot can restore data to when the last snapshot occured.

Creating a Periodic Snapshot Task

Go to **Tasks > Periodic Snapshot Tasks** and click **ADD**.



Choose the dataset (or zvol) to schedule as a regular backup with snapshots and determine how long to store them. Define the task **Schedule** and configure the remaining options for your use case.

Snapshot Lifetimes

TrueNAS deletes snapshots when they reach the end of their life and preserves snapshots when at least one periodic task requires it. For example, you have two schedules created where one schedule takes a snapshot every hour and keeps them for a week, and the other takes a snapshot every day and keeps them for three years. Each has an hourly snapshot taken. After a week, snapshots created at *01.00* through *23.00* get deleted, but you keep snapshots timed at *00.00* because they are necessary for the second periodic task. These snapshots get destroyed at the end of 3 years.

Naming Schemas

The **Naming Schema** determines how automated snapshot names generate. A valid schema requires the *%Y* (year), *%m* (month), *%d* (day), *%H* (hour), and *%M* (minute) time strings, but you can add more identifiers to the schema too, using any identifiers from the Python strptime function.

> For **Periodic Snapshot Tasks** used to set up a replication task with the **Replication Task** function:
>
> You can use custom naming schemas for full backup replication tasks. If you are using the snapshot for incremental replication tasks, use the default naming schema. Go to Using a Custom Schema for additional information.

This uses some letters differently from POSIX (Unix) time functions. For example, including `%z` (time zone) ensures that snapshots do not have naming conflicts when daylight time starts and ends, and *%S* (second) adds finer time granularity.

Examples:

Naming Scheme	Snapshot Names Look Like
replicationsnaps-1wklife-%Y%m%d_%H:%M	`replicationsnaps-1wklife-20210120_00:00`, `replicationsnaps-1wklife-20210120_06:00`
autosnap_%Y.%m.%d-%H.%M.%S-%z	`autosnap_2021.01.20-00.00.00-EST`, `autosnap_2021.01.20-06.00.00-EST`

> When referencing snapshots from a Windows computer, avoid using characters like : that are invalid in a Windows file path. Some applications limit filename or path length, and there might be limitations related to spaces and other characters. Always consider future uses and ensure the name given to a periodic snapshot is acceptable.

Managing Periodic Snapshot Tasks

Click **SUBMIT** to save the task in **Tasks > Periodic Snapshot Tasks**. You can find any snapshots from this task in **Storage > Snapshots**.

To check the log for a saved snapshot schedule, go to **Tasks > Periodic Snapshot Tasks** and click the task **State**.

Creating Replication Tasks

Local Replication

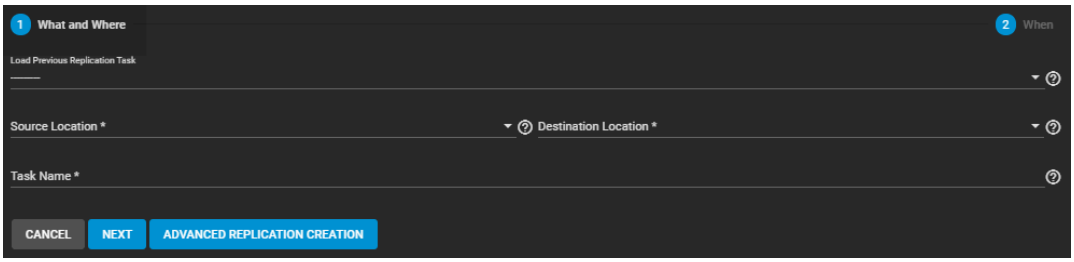
▼ Process Summary

Process Summary

- Requirements: Storage pools and datasets created in **Storage > Pools**.
- Go to **Tasks > Replication Tasks** and click **ADD**
  - Choose Sources.
    - Set the source location to the local system.
    - Use the file browser or type paths to the sources.
  - Define a Destination path.
    - Set the destination location to the local system.
    - Select or manually define a path to the single destination location for the snapshot copies.
  - Set the Replication schedule to run once.
  - Define how long the snapshots is stored in the **Destination**.
  - Clicking **START REPLICATION** immediately snapshots the chosen. Sources and copies those snapshots to the **Destination**.
    - Dialog might ask to delete existing snapshots from the **Destination**. Be sure to protect that all-important data before deleting anything.
- Clicking the task **State** shows the logs for that replication task.

Quick Backups with the Replication Wizard

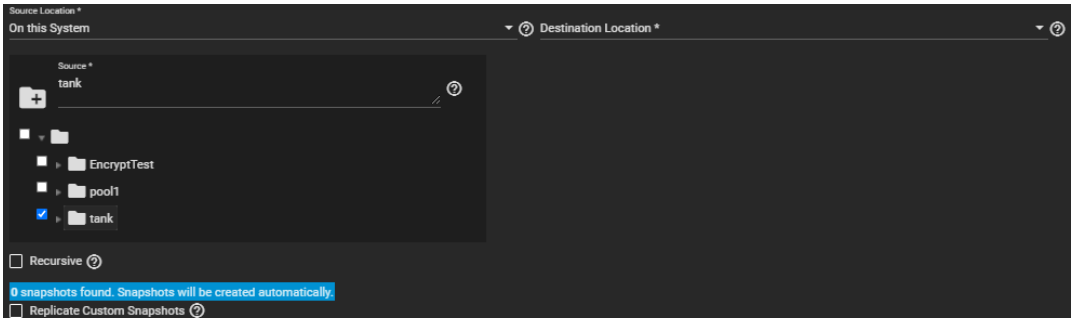
TrueNAS provides a wizard for quickly configuring different simple replication scenarios.



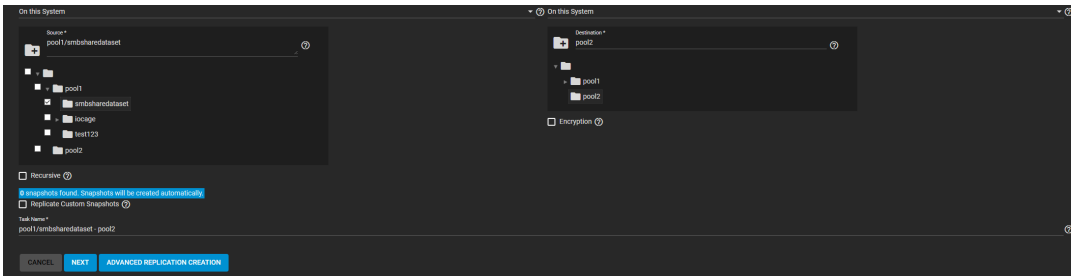
While we recommend regularly scheduled replications to a remote location as the optimal backup scenario, the wizard can quickly create and copy ZFS snapshots to another location on the same system. This is useful when you have no remote backup locations or when a disk is in danger of failure.

All you need to create a local replication are datasets or zvols in a storage pool to use as the replication source and (preferably) a second storage pool to store replicated snapshots. You can set up the local replication entirely in the Replication Wizard.

To open the Replication Wizard, go to **Tasks > Replication Tasks** and click **ADD**. Set the source location to the local system and pick which datasets to snapshot. The wizard takes new snapshots of the sources when it can't find existing source snapshots.
Enabling **Recursive** replicates all snapshots contained within the selected source dataset snapshots. Local sources can also use a naming schema to identify and include custom snapshots in the replication. A naming schema is a collection of strftime time and date strings and any identifiers that a user might have added to the snapshot name.



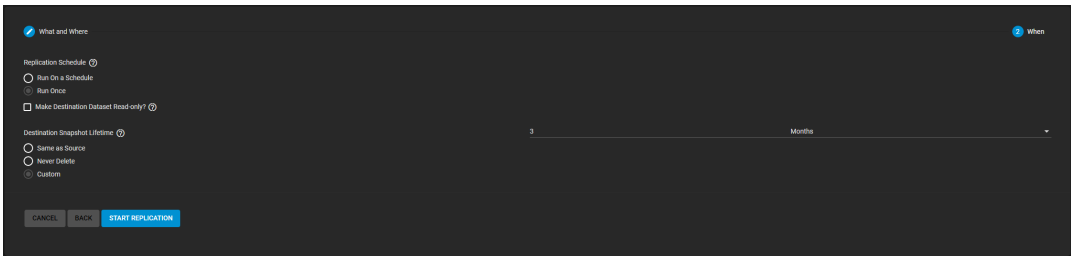
Set the **Destination** to the local system and define the path to the storage location for replicated snapshots. When manually defining the **Destination**, type the full path to the destination location.



TrueNAS suggests a default name for the task based on the selected source and destination locations, but you can type your name for the replication. You can load any saved replication task into the wizard to make creating new replication schedules even easier.

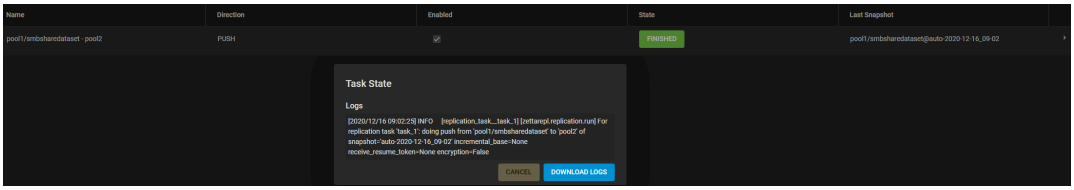
You can define a specific schedule for this replication or choose to run it immediately after saving the new task. Unscheduled tasks are still saved in the replication task list and can be run manually or edited later to add a schedule.

The destination lifetime is how long copied snapshots store in the **Destination** before the system deletes them. We usually recommend defining a snapshot lifetime to prevent storage issues. Choosing to keep snapshots indefinitely can require you to manually clean old ones from the system if or when the **Destination** fills to capacity.

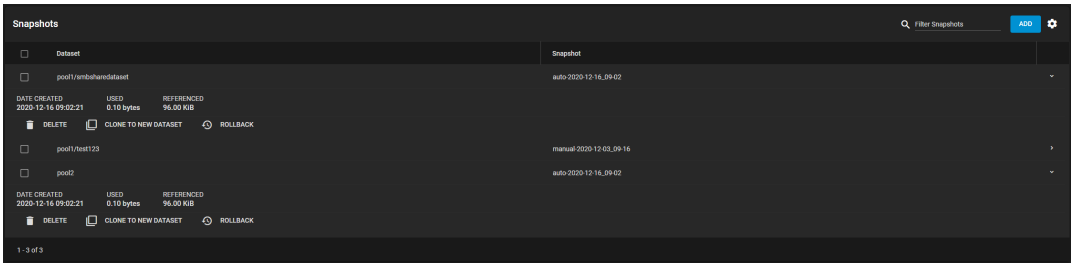


Clicking **START REPLICATION** saves the new task and immediately attempts to replicate snapshots to the **Destination**. When TrueNAS detects that the **Destination** already has unrelated snapshots, it asks to delete the unrelated ones and do a full copy of the new ones. **START REPLICATION** can delete data, so be sure you are okay with deleting any existing snapshots. Alternatively, back them up in another location.

The simple replication is added to the replication task list and shows that it is currently running. Clicking the task state shows the replication log with an option to download it to your local system.



To confirm that snapshots replicated, go to **Storage > Snapshots** and verify the destination dataset has new snapshots with correct timestamps.



Remote Replication

Configure SSH and automatic dataset snapshots in TrueNAS before creating a remote replication task. This ensures that both systems can connect and new snapshots are regularly available for replication.

To streamline creating simple replication configurations, the replication wizard assists with creating a new SSH connection and automatically creates a periodic snapshot task for sources with no existing snapshots.

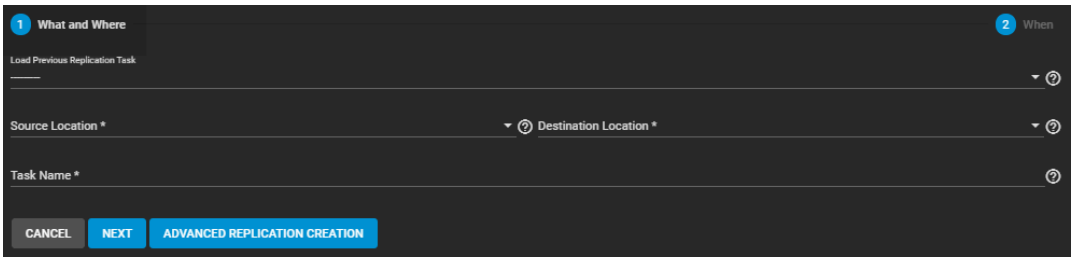
▼ Process Summary

Process Summary

- **Tasks > Replication Tasks**
  - Choose sources for snapshot replication.
    - Remote sources require an SSH connection.
    - TrueNAS shows how many snapshots will replicate.
  - Define the snapshot destination.
    - A remote destination requires an SSH connection.
    - Choose a destination or define it manually by typing a path.
      - Adding a new name at the end of the path creates a new dataset.
  - Choose replication security.
    - We always recommend replication with encryption.
    - Disabling encryption is only meant for absolutely secure networks.
  - Schedule the replication.
    - Schedule can be standardized presets or a custom-defined schedule.
    - Running once runs the replication immediately after creation.
      - Task is still saved and can be rerun or edited.
  - Choose how long to keep the replicated snapshots.

Creating a Remote Replication Task

Go to **Tasks > Replication Tasks** and click **ADD**.

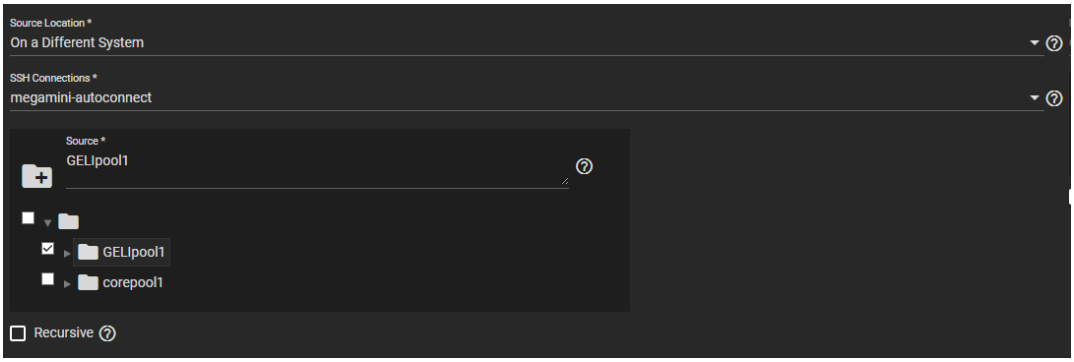


You can load any saved replication to prepopulate the wizard with that configuration. Saving changes to the configuration creates a new replication task without altering the one you loaded into the wizard. This saves time when creating multiple replication tasks between the same two systems.

Sources

Start by configuring the replication sources. Sources are the datasets or zvols with snapshots to use for replication. Choosing a remote source requires selecting an SSH connection to that system. Expanding the directory browser shows the current datasets or zvols available for replication. You can select multiple sources or manually type the names into the field.

TrueNAS shows how many snapshots are available for replication. We recommend you manually snapshot the sources or create a periodic snapshot task before creating the replication task. However, when the sources are on the local system and don't have any existing snapshots, TrueNAS can create a basic periodic snapshot task and snapshot the sources immediately before starting the replication. Enabling **Recursive** replicates all snapshots contained within the selected source dataset snapshots.

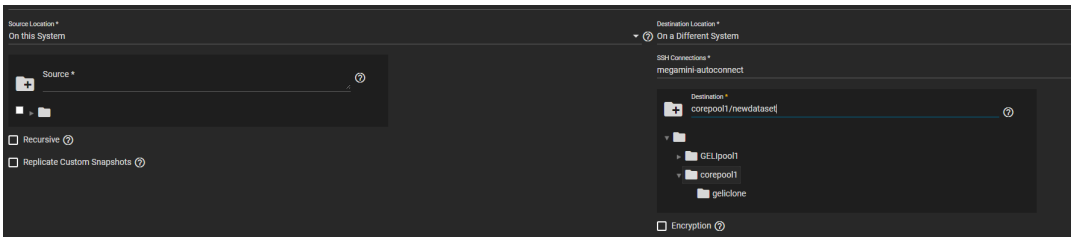


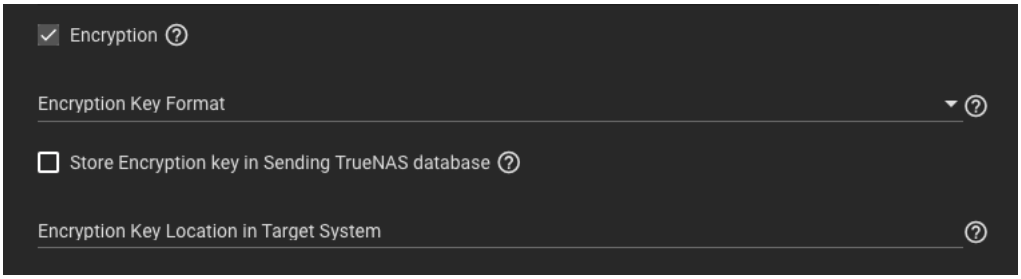
Remote sources require entering a **Snapshot Naming Schema** to identify the snapshots to replicate. A naming schema is a collection of strftime time and date strings and any identifiers that a user might have added to the snapshot name.

Local sources can also use a naming schema to identify and include custom snapshots in the replication.

Destination

The destination is where replicated snapshots are stored. Choosing a remote destination requires an SSH connection to that system. Expanding the directory browser shows the current datasets that are available for replication. You can select a destination dataset or manually type a path in the field. You cannot use Zvols as a remote replication destination. Adding a name to the end of the path creates a new dataset in that location.





Encryption: To use encryption when replicating data, check the Encryption box.

- *Encryption Key Format* allows the user to choose between a Hex (base 16 numeral) or Passphrase (alphanumeric) style encryption key.
- *Store Encryption key in Sending TrueNAS database* allows the user to either store the Encryption key in the sending TrueNAS database (box checked) or choose a temporary location for the encryption key to decrypt replicated data (box unchecked).

Security and Task Name

> Using encryption for SSH transfer security is always recommended.

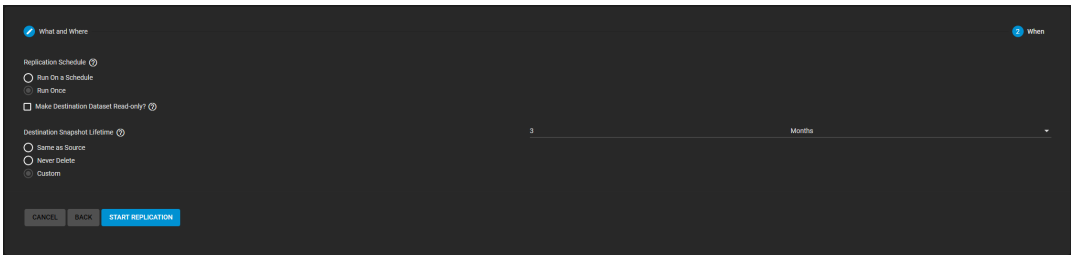
If you are using two systems within a secure network for replication, disabling encryption speeds up the transfer. However, the data is not protected from malicious sources.

Choosing no encryption for the task is the same as choosing the *SSH+NETCAT* transport method from the advanced options screen. NETCAT uses common port settings, but these can be overridden by switching to the advanced options screen or editing the task after creation.

TrueNAS suggests a name based on the selected sources and destination, but you can overwrite it with a custom name.

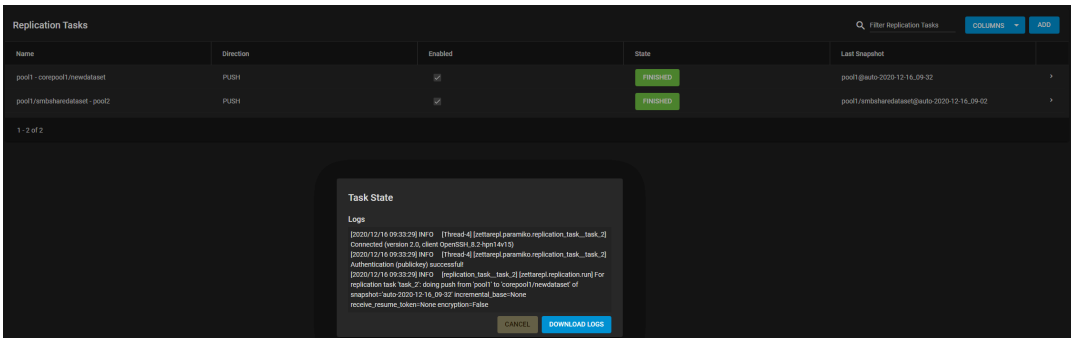
Adding a schedule automates the task to run according to your chosen times. You can choose between several preset schedules or create a custom schedule for when the replication runs. Choosing to run the replication once runs the replication immediately after saving the task, but you must manually trigger any additional replications.

Finally, define how long you want to keep snapshots on the destination system. We recommend defining snapshot lifetime to prevent cluttering the system with obsolete snapshots.



Starting the Replication

Start Replication saves the new replication task. TrueNAS enables new tasks by default and activates them according to their schedule (or immediately if you didn't choose a schedule). The first time a replication task runs, it takes longer because the snapshots must copy entirely fresh to the destination. Later replications run faster, as only the subsequent changes to snapshots replicate. Clicking the task state opens the log for that task.


Replication Tasks
Filter Replication Tasks
COLUMNS
ADD
Name
Direction
Enabled
State
Last Snapshot
pool1 - corepool1/newdataset
PUSH
FINISHED
pool1@auto-2020-12-16_09-32
pool1/smbsharedataset - pool2
PUSH
FINISHED
pool1/smbsharedataset@auto-2020-12-16_09-02
1 - 2 of 2
Task State
Logs
[2020/12/16 09:33:29] INFO [Thread-4] [zettarepl.paramiko.replication_task__task_2] Connected (version 2.0, client OpenSSH_8.2-hpn14v15)
[2020/12/16 09:33:29] INFO [Thread-4] [zettarepl.paramiko.replication_task__task_2] Authentication (publickey) successful
[2020/12/16 09:33:29] INFO [replication_task__task_2] [zettarepl.replication.run] For replication task 'task_2': doing push from 'pool1' to 'corepool1/newdataset' of snapshot='auto-2020-12-16_09-32' incremental_base=None receive_resume_token=None encryption=False
CANCEL
DOWNLOAD LOGS

Advanced Replication

Requirements:

- Storage pools with datasets and data to snapshot.
- SSH configured with a connection to the remote system saved in **System > SSH Connections**.
- Dataset snapshot task saved in **Tasks > Periodic Snapshot Tasks**.

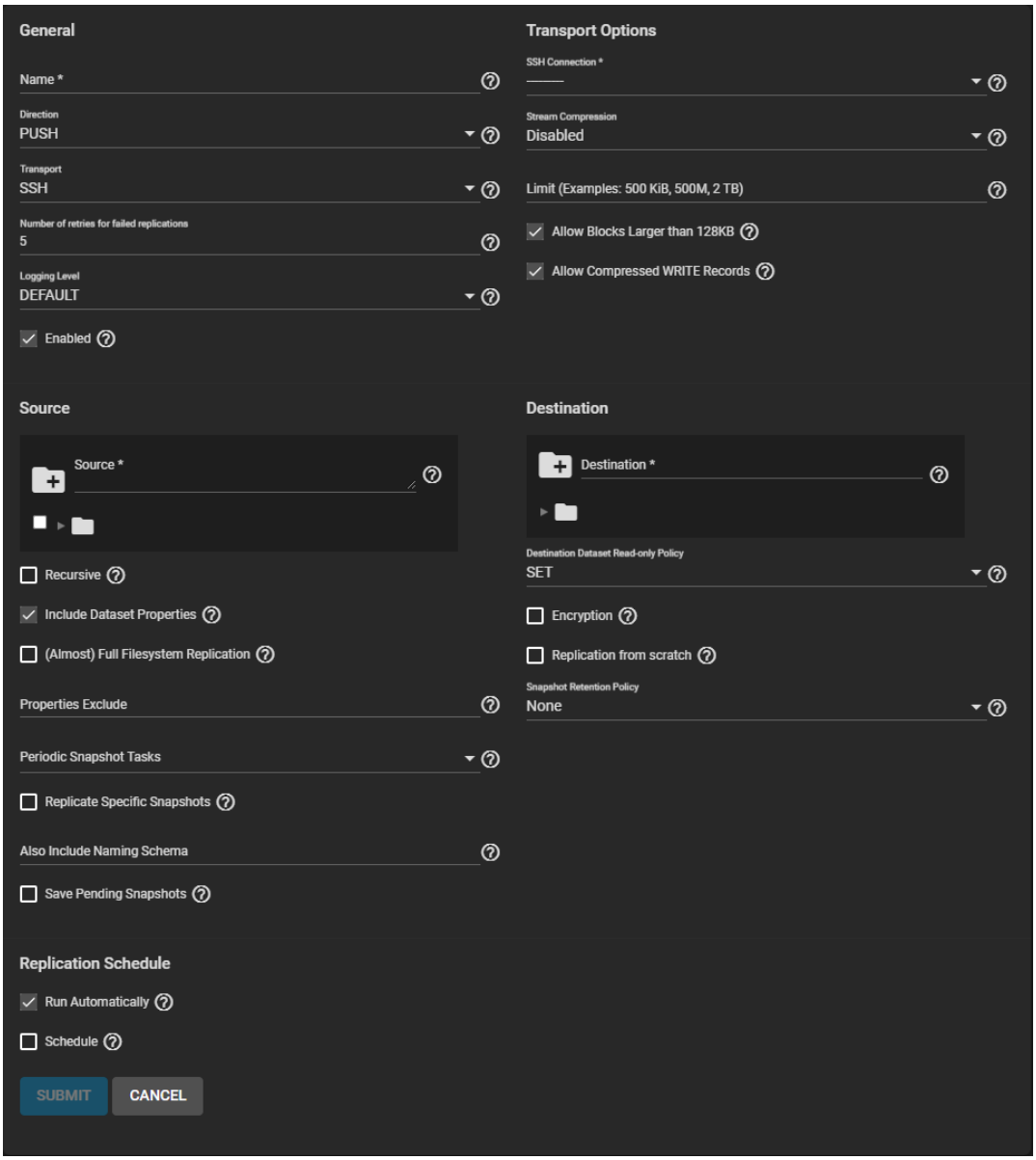
▼ Process Summary

Go to **Tasks > Replication Tasks** and click **ADD**, then select **ADVANCED REPLICATION CREATION**.

- General Options:
  - Name the task.
  - Select Push or Pull for the local system.
  - Select a replication transport method.
    - SSH is recommended.
    - SSH+Netcat is used for secured networks.
    - Local is for in-system replication.
- Configure the replication transport method:
  - Remote options require an SSH connection.
  - SSH+Netcat requires defining Netcat ports and addresses.
- Sources:
  - Select sources for replication.
  - Choose a periodic snapshot task as the source of snapshots to replicate.
  - Remote sources require defining a snapshot naming schema.
- Destination:
  - Remote destination requires an SSH connection.
  - Select a destination or type a path in the field.
  - Define how long to keep snapshots in the destination.
- Scheduling:
  - Run automatically starts the replication after a related periodic snapshot task completes.
  - To automate the task according to its schedule, set that option and define a schedule for the replication task.

Creating an Advanced Replication Task

To use the advanced editor to create a replication task, go to **Tasks > Replication Tasks**, click **ADD** to open the Wizard, then click **ADVANCED REPLICATION CREATION**.



Options group by category. Options can appear, disappear, or be disabled depending on the configuration choices you make. Start by configuring the **General** options first, then the **Transport** options before configuring replication **Sources** and **Destination**.

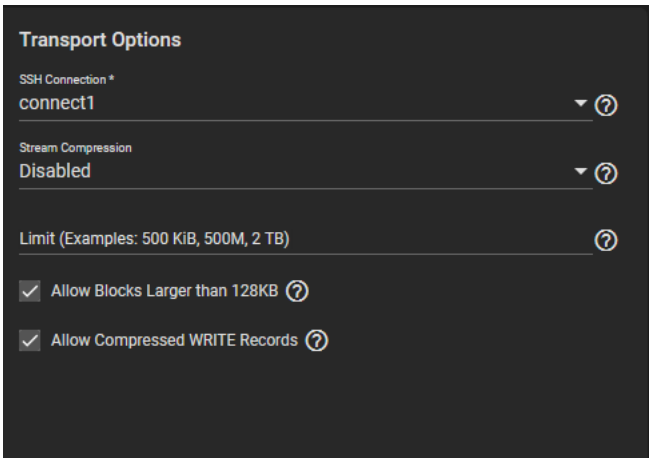
Name the task. Each task name must be unique, and we recommend you name it in a way that makes it easy to remember what the task is doing.

Choose whether the local system is sending (*Push*) or receiving data (*Pull*) and decide what **Transport** method to use for the replication before configuring the other sections.

Transport Options

The **Transport** selector determines the method to use for the replication: *SSH* is the standard option for sending or receiving data from a remote system, but *SSH+NETCAT* is faster for replications within completely secure networks. *Local* is only used for replicating data to another location on the same system.

With SSH-based replications, configure the transport method by selecting the **SSH Connection** to the remote system that sends or receives snapshots. Options for compressing data, adding a bandwidth limit, or other data stream customizations are available. **Stream Compression** options are only available when using SSH. Before enabling **Compressed WRITE Records**, verify that the destination system supports compressed WRITE records.

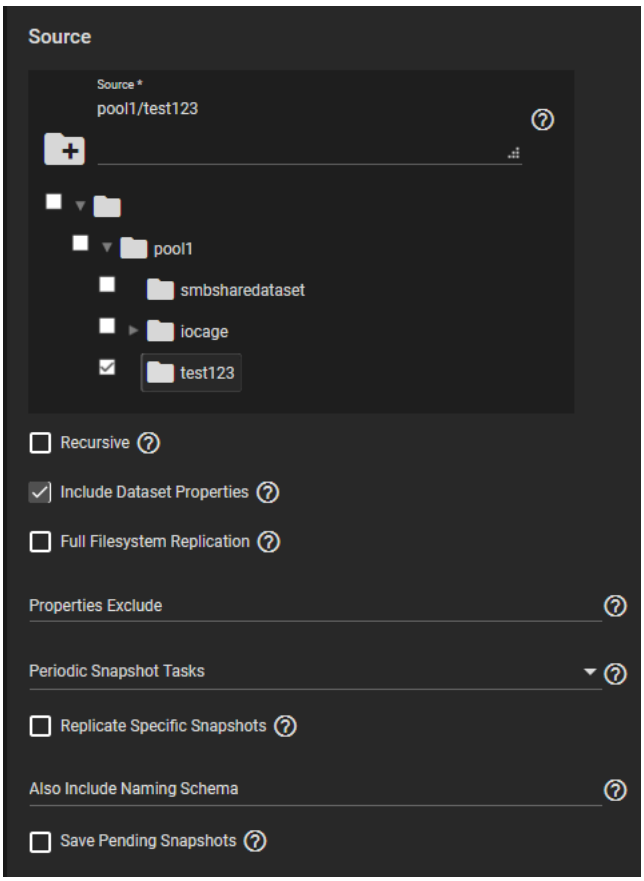


For *SSH+NETCAT* replications, you also need to define the addresses and ports to use for the Netcat connection.

> **Allow Blocks Larger than 128KB** is a one-way toggle. Replication tasks using large block replication only continue to work as long as this option remains enabled.

Source

The replication **Source** is the datasets or zvols to replicate. Select the sources for the replication task by opening the file browser or entering dataset names in the field. Pulling snapshots from a remote source requires a valid **SSH Connection** before the file browser can show any directories. If the file browser shows a connection error after selecting the correct **SSH Connection**, you might need to log in to the remote system and ensure it allows SSH connections. Go to the **Services** screen and check the **SSH** service configuration. Start the service.



By default, replication tasks use snapshots to quickly transfer data to the receiving system. When **Full Filesystem Replication** is set, the chosen **Source** completely replicates, including all dataset properties, snapshots, child datasets, and clones. When choosing this option, we recommend allocating additional time for the replication task to run. Leaving **Full Filesystem Replication** unset but setting **Include Dataset Properties** includes just the dataset properties in the snapshots to be replicated. Additional options allow you to recursively replicate child dataset snapshots or exclude specific child datasets or properties from the replication.

Local sources replicate by snapshots you generated from a periodic snapshot task or from a defined naming schema that matches manually created snapshots. Remote sources require entering a snapshot naming schema to identify the snapshots to replicate. A naming schema is a collection of strftime time and date strings and any identifiers that a user might have added to the snapshot name. For example, entering the naming schema `custom-%Y-%m-%d_%H-%M` finds and replicates snapshots like `custom-2020-03-25_09-15`. Multiple schemas can be entered by pressing `Enter` to separate each schema.

To define specific snapshots from the periodic task to replicate, set **Replicate Specific Snapshots** and enter a schedule. The only periodically generated snapshots in the replication task are those that match your defined schedule. Alternately, you can

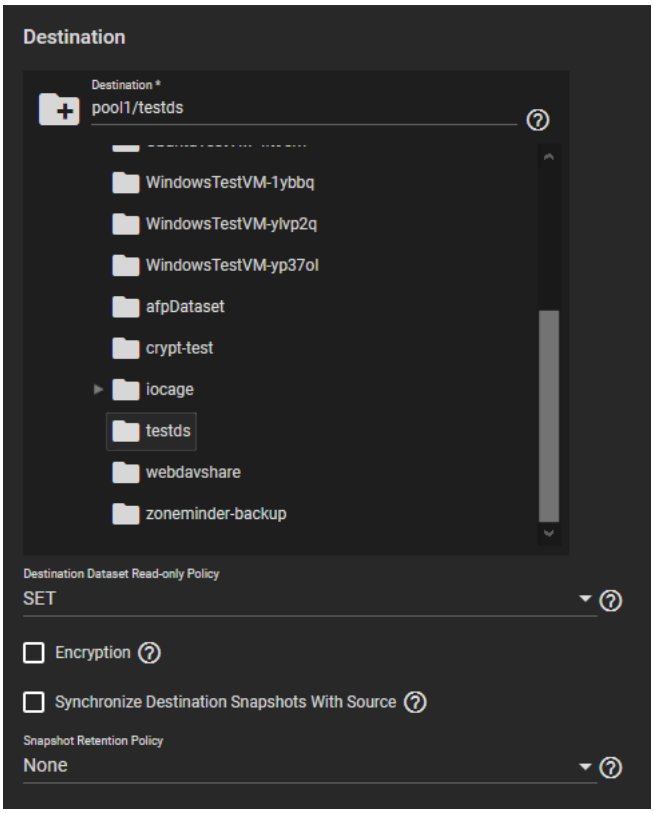
use your **Replication Schedule** to determine which snapshots replicate by setting **Run Automatically**, **Only Replicate Snapshots Matching Schedule**, and defining when the replication task runs.

When a replication task has difficulty completing, set **Save Pending Snapshots**. **Save Pending Snapshots** prevents the source TrueNAS from automatically deleting any snapshots that fail to replicate to the destination system.

Destination

The destination is where replicated data is stored. Choosing a remote destination requires an *SSH Connection* to that system. Expanding the file browser shows the current available datasets on the destination system. You can click a destination or manually type a path in the field. Adding a name to the end of the path creates a new dataset in that location.

> **DO NOT** use zvols for a remote destination



By default, the destination dataset is *SET* to be **read-only** after the replication is complete. You can change the **Destination Dataset Read-only Policy** to only start replication when the destination is read-only (*REQUIRE*) or to disable checking the dataset's read-only state (*IGNORE*).

Encryption adds another layer of security to replicated data by encrypting the data before transfer and decrypting it on the destination system. Setting the checkbox allows using a *HEX* key or defining your own encryption *PASSPHRASE*. The encryption key can be stored in the TrueNAS system database or in a custom-defined location.

> **Synchronizing Destination Snapshots With Source** destroys any snapshots in the destination that do not match the source snapshots. TrueNAS also fully replicates the source snapshots as if the replication task had never run before, which leads to excessive bandwidth consumption. This can be a destructive option, so be sure that any snapshots that the task deletes from the destination are obsolete or otherwise backed up in a different location.

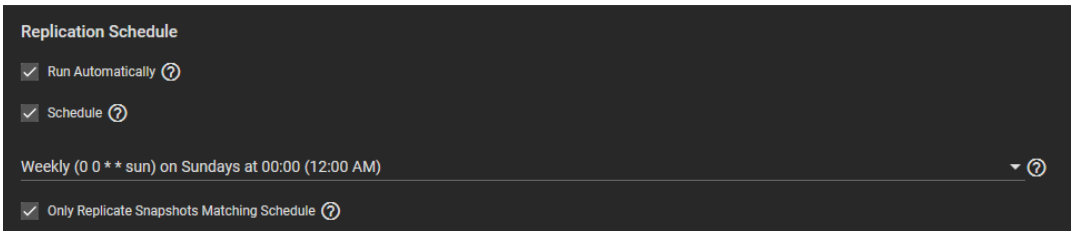
Defining the **Snapshot Retention Policy** is generally recommended to prevent cluttering the system with obsolete snapshots. Choosing **Same as Source** keeps the snapshots on the destination system for the same duration as the defined snapshot lifetime from the source system periodic snapshot task. You can also define your own *Custom* lifetime for snapshots on the destination system.

Schedule

By default, setting the task to **Run Automatically** starts the replication immediately after the related periodic snapshot task is complete.

Setting the **Schedule** checkbox allows scheduling the replication to run at a separate time.

Setting **Only Replicate Snapshots Matching Schedule** restricts the replication to only replicate those snapshots created at the same time as the replication schedule.


Replication Schedule
Run Automatically
Schedule
Weekly (0 0 * * sun) on Sundays at 00:00 (12:00 AM)
Only Replicate Snapshots Matching Schedule

Troubleshooting Tips

Using a Custom Schema

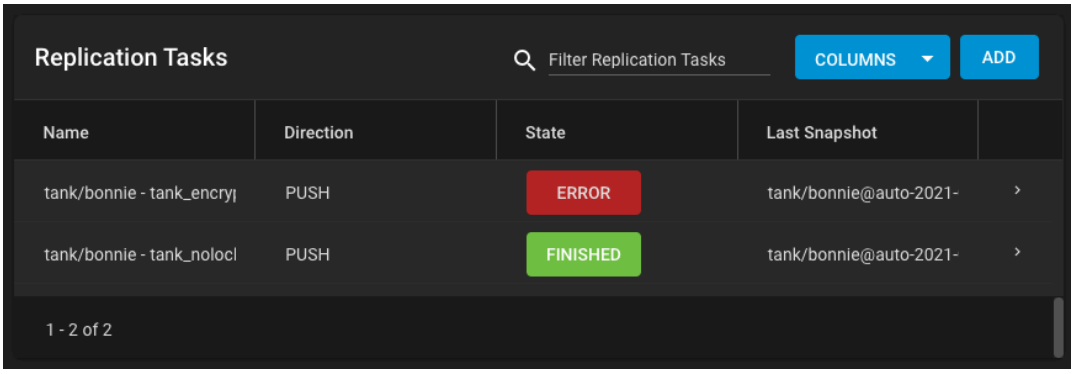
You can use **Snapshot Tasks** set up or imported with a custom schema name for “full backup” replication tasks. Incremental replication tasks will not work.

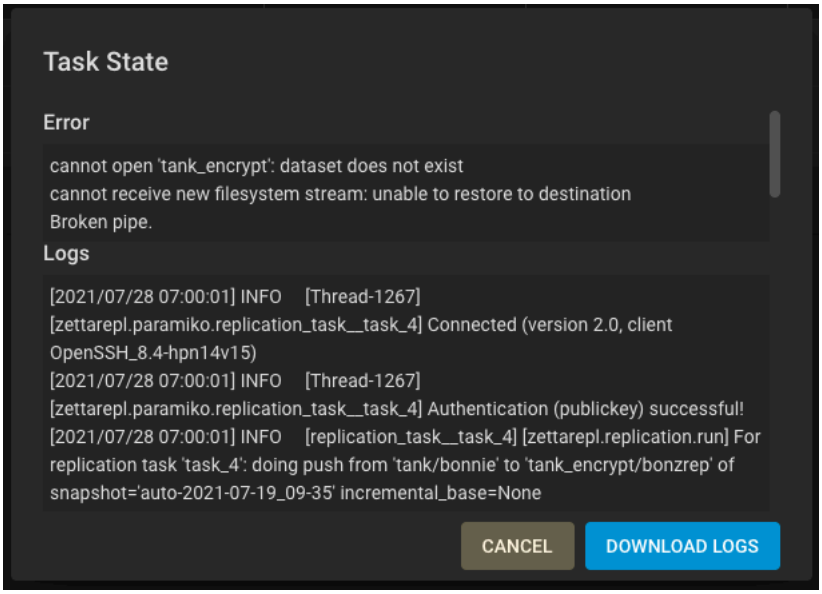
There are several ways to create a custom schema:

- Importing a ZFS dataset with snapshots into TrueNAS with a schema that doesn’t match the TrueNAS schema.
- Creating a custom schema name in the **Snapshot Task** occurs when the *Naming Schema* field in a **Periodic Snapshot Task** is not the default.

Replication Task Log

To view and download the replication task log, go to **Tasks > Replication Tasks**. Click on the *state* of the replication task.

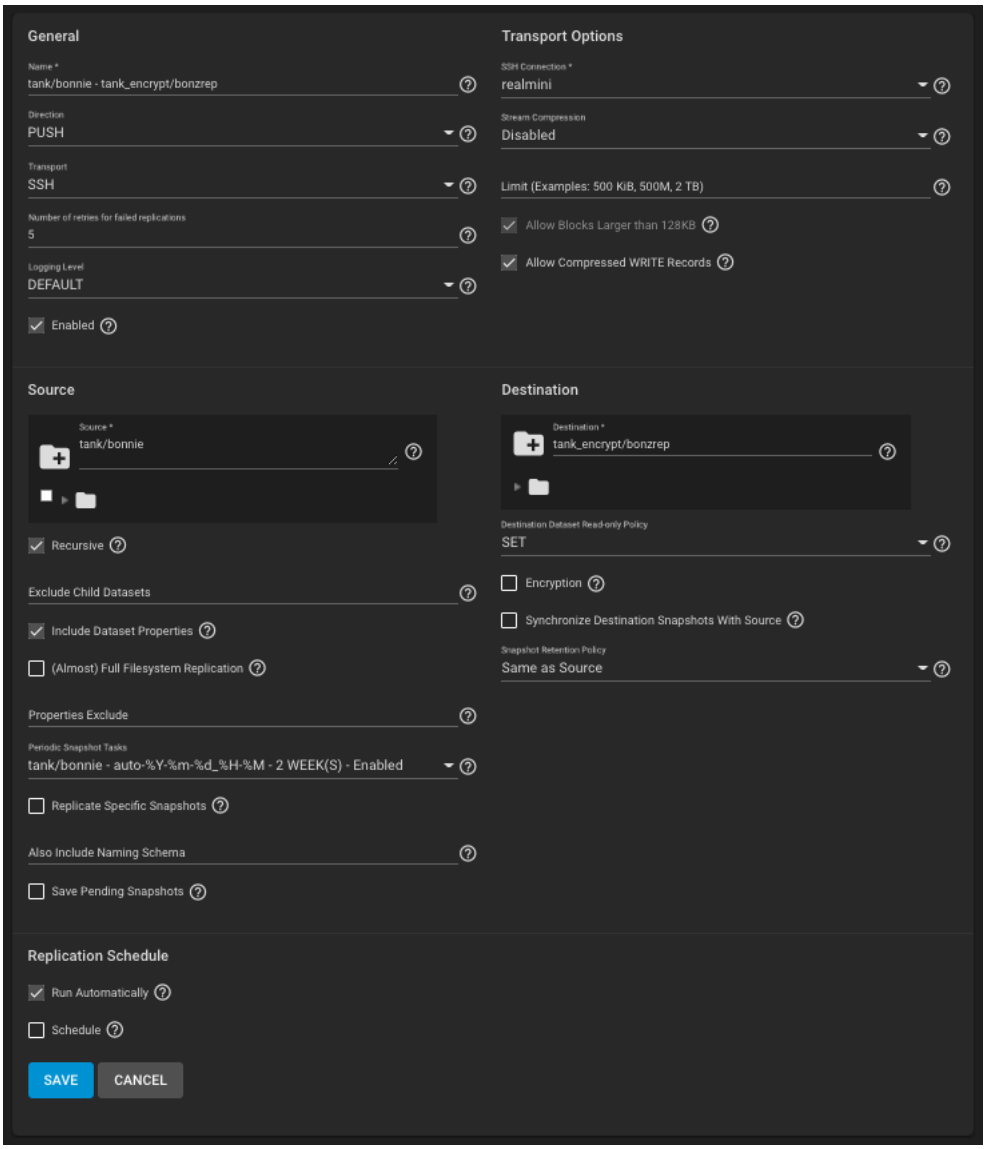




Click the *DOWNLOAD LOGS* button to download the log file.

Editing a Replication Task

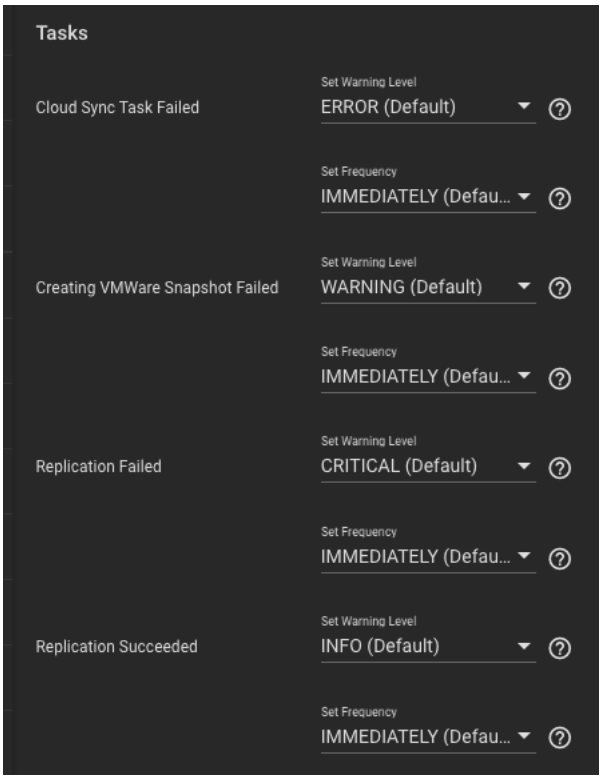
To edit the replication task, go to **Tasks > Replication Tasks**. Click the › to expand the replication task information, then click **EDIT**.



See **Replication Advanced Options** for descriptions of the available fields.

Replication Task Alert Priorities

To customize the importance and frequency of a Replication task alert (success or failure), go to **System > Alert Settings** and scroll down to the *Tasks* area. Set the *Warning Level* and how often the alert notification sends.



See **Alert Settings** for more information about this UI screen.

FAQ

Question: If the internet connection goes down for a while, does the replication restart where it left off - including any intermediate snapshots?

Answer: Yes.

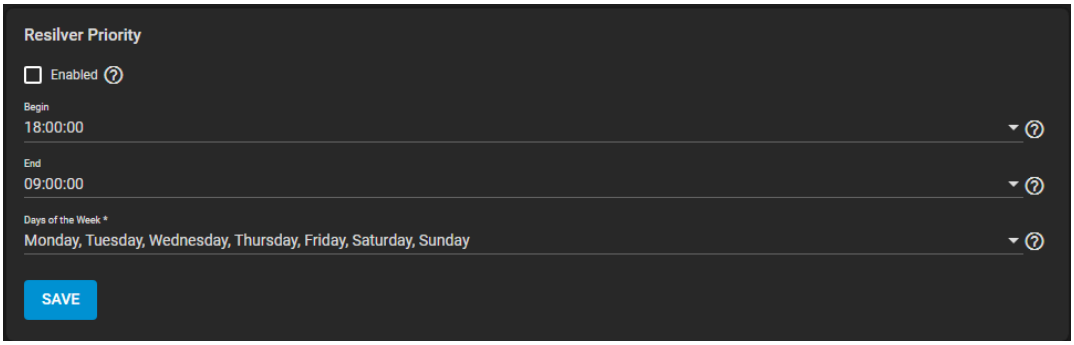
Question: If a site changes a lot of data at once and the internet bandwidth is not enough to finish sending the snapshot before the next one begins, do the replication jobs run one after the other and not stomp on each other?

Answer: Yes.

Using Resilver Priority

Resilvering is a process that copies data to a replacement disk. Complete it as quickly as possible. Resilvering is a high-priority task. It can run in the background while performing other system functions. However, this can put a higher demand on system resources. Increasing the priority of resilvers helps them finish faster as the system runs tasks with higher priority ranking.

Use the **Resilver Priority** screen to schedule a time when a resilver task can become a higher priority for the system and when the additional I/O or CPU use does not affect normal usage.



Select **Enabled**, then use the dropdown lists to select a start time in **Begin** and time to finish in **End** to define a priority period for the resilver. To select the day(s) to run the resilver, use the **Days of the Week** dropdown to select when the task can run with the priority given.

> A resilver process running during the time frame defined between the beginning and end times likely runs faster than during times when demand on system resources is higher. We advise you to avoid putting the system under any intensive activity or heavy loads (replications, SMB transfers, NFS transfers, Rsync transfers, S.M.A.R.T. tests, pool scrubs, etc.) during a resilver process.

Creating Scrub Tasks

A “scrub” is when ZFS scans the data on a pool. Scrubs identify data integrity problems, detect silent data corruptions caused by transient hardware issues, and provide early disk failure alerts.

Edit Default Scrub Tasks

By default, TrueNAS creates a scrub task when you create a new pool. The default schedule for a scrub is to run every Sunday at 12:00 AM. To edit the default scrub, go to **Tasks > Scrub Tasks**, click ⋮, and **EDIT**.

Create New Scrub Tasks

To create a scrub task for a pool, go to **Tasks > Scrub Tasks** and click **ADD**.

Select a **Pool**, enter the **Threshold** (in days), and give the scrub a description. Assign a **Schedule** and click **SUBMIT**.

Creating Cloud Sync Tasks

Cloud sync tasks let TrueNAS integrate with a Cloud Storage provider for additional backup storage. Cloud Sync tasks allow for single time transfers or recurring transfers on a schedule, and are an effective method to back up data to a remote location.

These providers are supported for Cloud Sync tasks in TrueNAS CORE:

- Amazon S3
- Backblaze B2
- Box
- Dropbox
- File Transfer Protocol (FTP)
- Google Cloud Storage
- Google Drive
- Hypertext Transfer Protocol (HTTP)
- Hubic (closed to new accounts)
- Mega
- Microsoft Azure Blob Storage
- Microsoft OneDrive
- OpenStack Swift
- pCloud
- SSH File Transfer Protocol (SFTP)
- Storj iX
- WebDAV
- Yandex

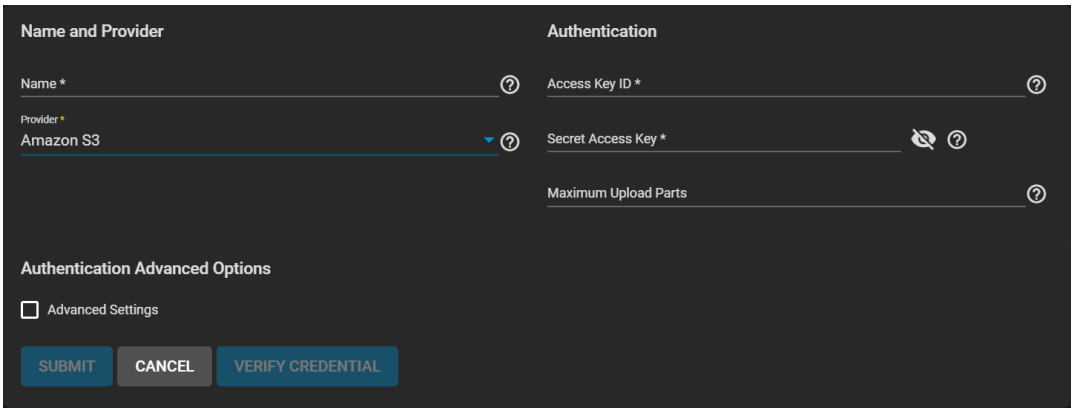
> Using the Cloud means that data can go to a third party commercial vendor not directly affiliated with iXsystems. Please investigate and fully understand vendor pricing policies and services before creating any Cloud Sync task. iXsystems is not responsible for any charges incurred from the use of third party vendors with the Cloud Sync feature.

Create a Cloud Storage Credential

Transferring data from TrueNAS to the Cloud requires saving Cloud Storage Provider credentials on the system.

To maximize security, TrueNAS encrypts credentials after saving. However, this means that to restore any cloud credentials from a TrueNAS configuration file, you must enable **Export Password Secret Seed** when generating that configuration backup. Remember to protect any downloaded TrueNAS configuration files.

Go to **System > Cloud Credentials** and click **ADD**.



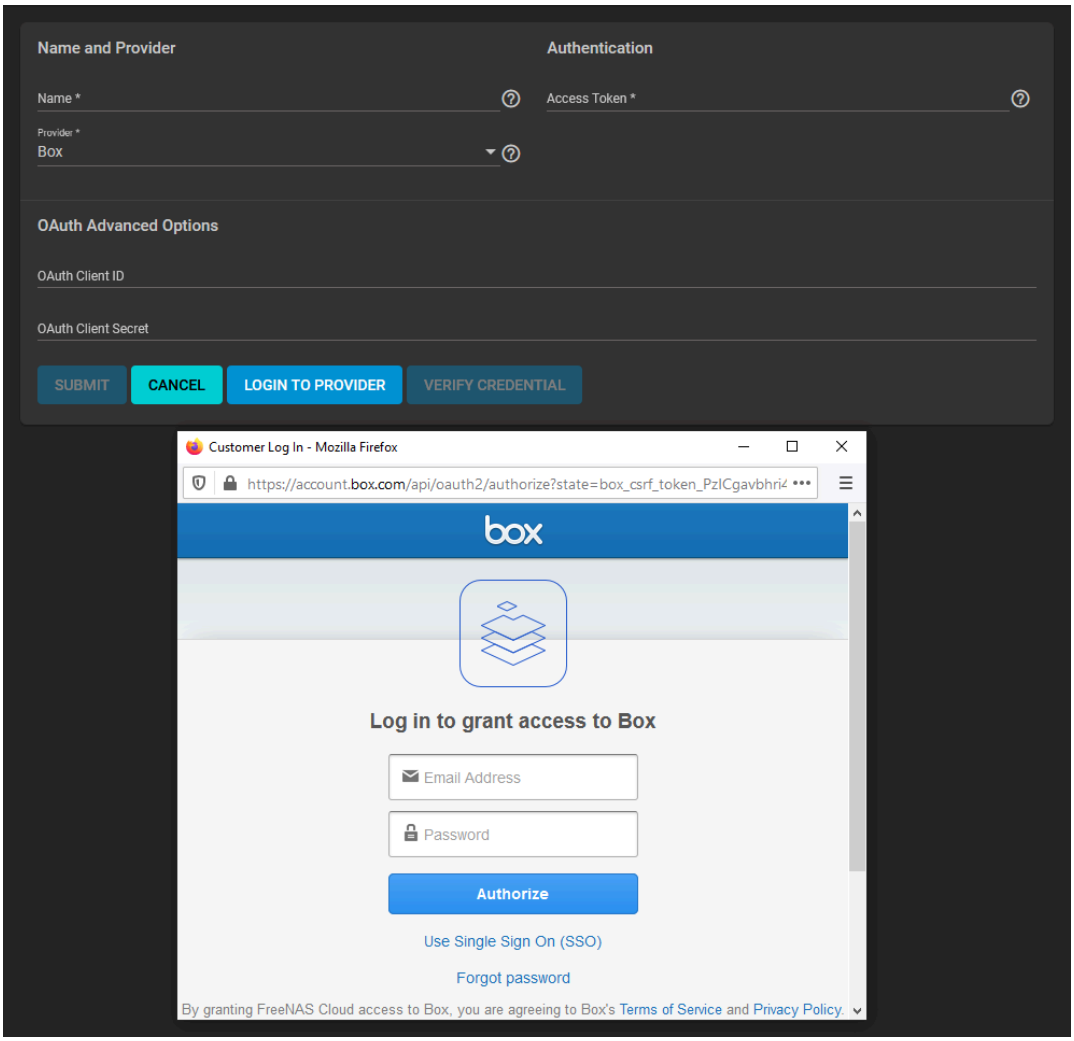
Enter a credential **Name** and choose a **Provider**. The rest of the options vary by **Provider**.

Enter the required **Authentication** strings to enable saving the credential.

See Cloud Credentials for provider-specific fields and settings.

Automatic Authentication

Some providers can automatically populate the required **Authentication** strings by logging in to the account. To automatically configure the credential, click **Login to Provider** and entering your account username and password.



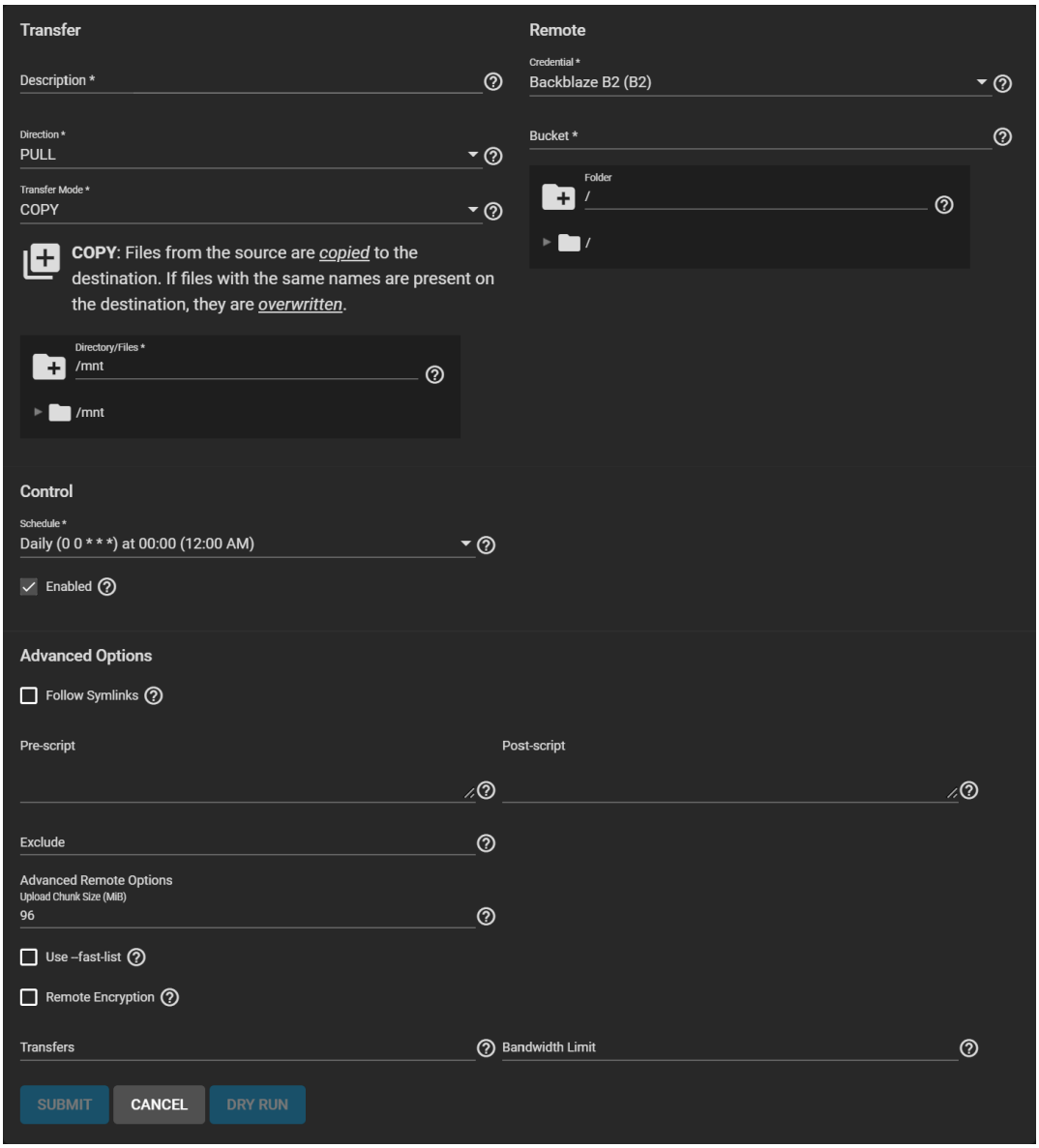
We recommend verifying the credential before saving it.

Create a Cloud Sync Task

▼ Requirements

- All system Storage configured and ready to receive or send data.
- A Cloud Storage provider account and a cloud storage location (like an Amazon S3 bucket).
- Cloud Storage account credentials must be saved in **System > Cloud Credentials**.

Go to **Tasks > Cloud Sync Tasks** and click **ADD**.



Give the task a **Description** and select a cloud credential. TrueNAS connects to the chosen Cloud Storage Provider and shows the available storage locations.

Decide if data is transferring to (**PUSH**) or from (**PULL**) the Cloud Storage location (**Remote**).

Choose a **Transfer Mode**:

SYNC keeps all the files identical between the two storage locations. If a sync encounters an error, the destination does not delete the files.

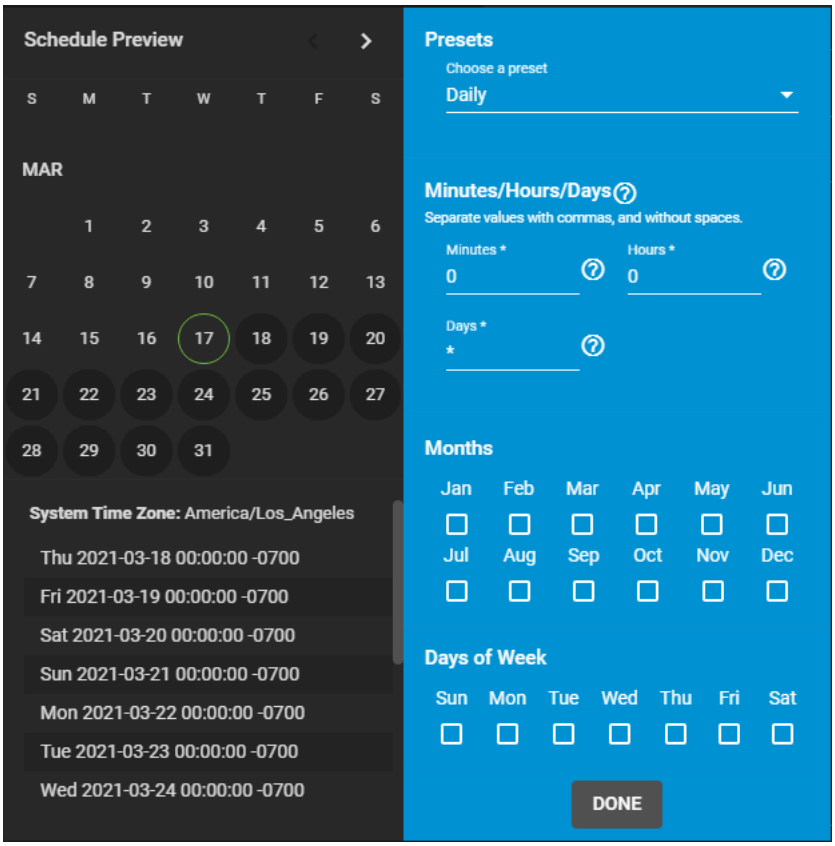
> Syncing to a Backblaze B2 bucket does not delete files from the bucket, even when you delete those files locally. Instead, Backblaze tags files with a version number or moves them to a hidden state. To automatically delete old or unwanted files from the bucket, adjust the Backblaze B2 Lifecycle Rules.

COPY duplicates each source file into the destination, overwriting any destination files with the same name as the source. Copying is the least potentially destructive option.

MOVE transfers the files from the source to the destination and deletes the original source files. It also overwrites files with the same names on the destination.

Next, select a **Schedule** from the drop-down, or unset **Enable** to make the task available without running on a schedule.

▼ Advanced Scheduler



Choosing a **Presets** option populates the rest of the fields. To customize a schedule, enter crontab values for the `Minutes/Hours/Days`.

These fields accept standard cron values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering *10* means that the job runs when the time is ten minutes past the hour.

An asterisk (`*`) means match all values.

Specific time ranges are set by entering hyphenated number values. For example, entering *30-35* in the **Minutes** field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.

You can also enter lists of values. Enter individual values separated by a comma (`,`). For example, entering *1,14* in the **Hours** field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).

A slash (`/`) designates a step value. For example, while entering `*` in **Days** means the task runs every day of the month, `*/2` means the task runs every other day.

Combining all the above examples together creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

There is an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days. This is in addition to any listed days. For example, entering *1* in **Days** and setting *Wed* for **Days of Week** creates a schedule that starts a task on the first day of the month *and* every Wednesday of the month.

The **Schedule Preview** displays when the current settings mean the task runs.

Examples of CRON syntax

Syntax	Meaning	Examples
*	Every item.	* (minutes) = every minute of the hour. * (days) = every day.
*/N	Every Nth item.	*/15 (minutes) = every 15th minute of the hour (every quarter hour). */3 (days) = every 3rd day. */3 (months) = every 3rd month.
Comma and hyphen/dash	Each stated item (comma) Each item in a range (hyphen/dash).	1,31 (minutes) = on the 1st and 31st minute of the hour. 1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour. mon-fri (days) = every Monday to Friday inclusive (every weekday). mar,jun,sep,dec (months) = every March, June, September, December.

Days can be specified as days of month, or days of week.

With these options, you can create flexible schedules similar to these examples:

Desired schedule	Values to enter
3 times a day (at midnight, 08:00 and 16:00)	months=*; days=*; hours=0/8 or 0,8,16; minutes=0 (Meaning: every day of every month, when hours=0/8/16 and minutes=0)
Every Monday, Wednesday and Friday, at 8.30 pm	months=*; days=mon,wed,fri; hours=20; minutes=30
1st and 15th day of the month, during October to June, at 00:01 am	months=oct-dec,jan-jun; days=1,15; hours=0; minutes=1
Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday	Note that this requires two tasks to achieve: (1) months=*; days=mon-fri; hours=8-18; minutes=*/15 (2) months=*; days=mon-fri; hours=19; minutes=0 We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00.

▼ Advanced Options

Scripting and Environment Variables

Advanced users can write scripts that run immediately before or after the Cloud Sync task. The **Post-script** field runs when the Cloud Sync task successfully completes. You can pass a variety of task environment variables into the **Pre-script** and **Post-script** fields:

- CLOUD_SYNC_ID
- CLOUD_SYNC_DESCRIPTION
- CLOUD_SYNC_DIRECTION
- CLOUD_SYNC_TRANSFER_MODE
- CLOUD_SYNC_ENCRYPTION
- CLOUD_SYNC_FILENAME_ENCRYPTION
- CLOUD_SYNC_ENCRYPTION_PASSWORD
- CLOUD_SYNC_ENCRYPTION_SALT
- CLOUD_SYNC_SNAPSHOT

There also are provider-specific variables like CLOUD_SYNC_CLIENT_ID or CLOUD_SYNC_TOKEN or CLOUD_SYNC_CHUNK_SIZE.

Remote storage settings:

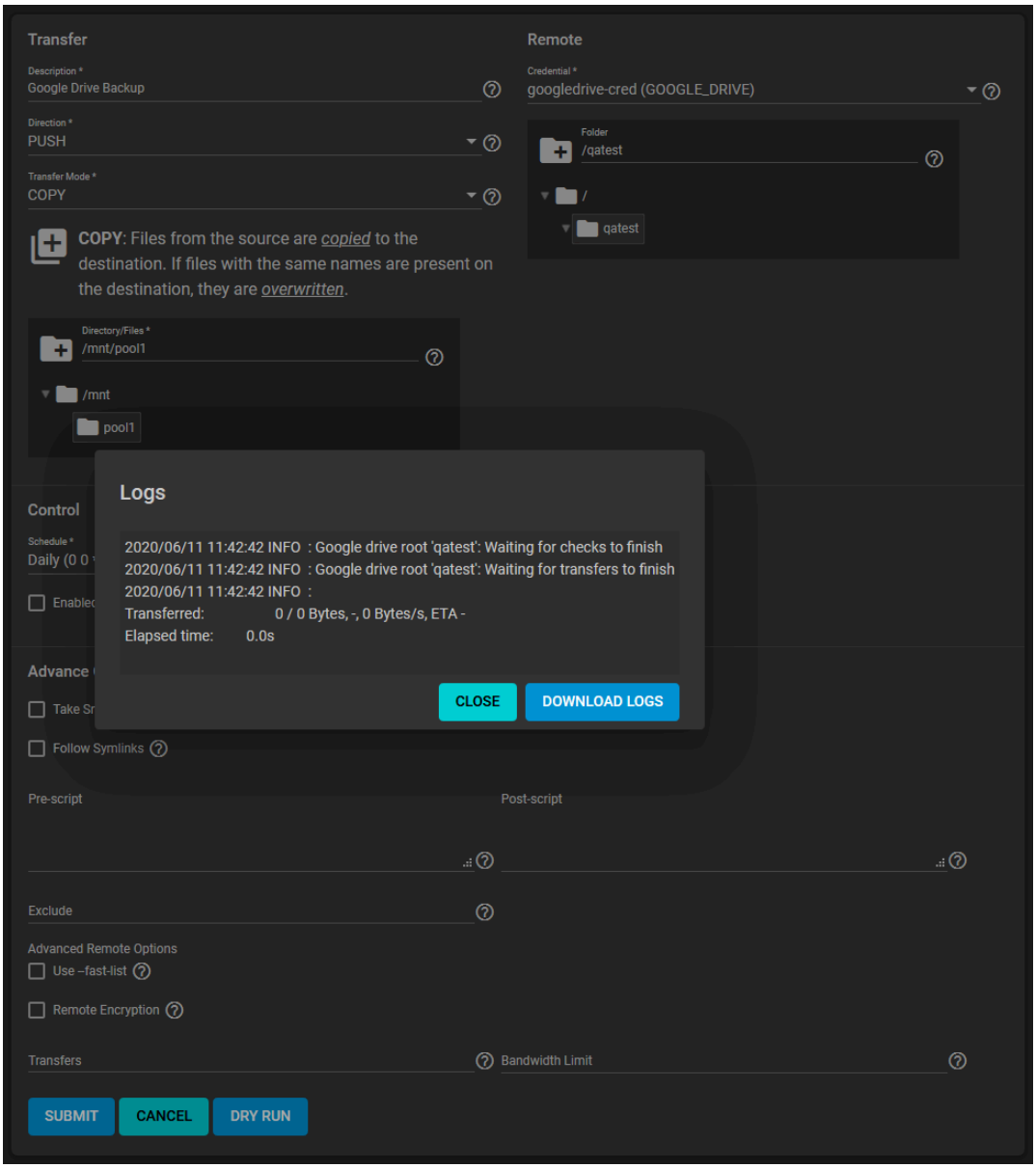
- CLOUD_SYNC_BUCKET
- CLOUD_SYNC_FOLDER

Local storage settings:

- CLOUD_SYNC_PATH

Testing Settings

Test the settings before saving by clicking **DRY RUN**. TrueNAS connects to the Cloud Storage Provider and simulates a file transfer without sending or receiving data.



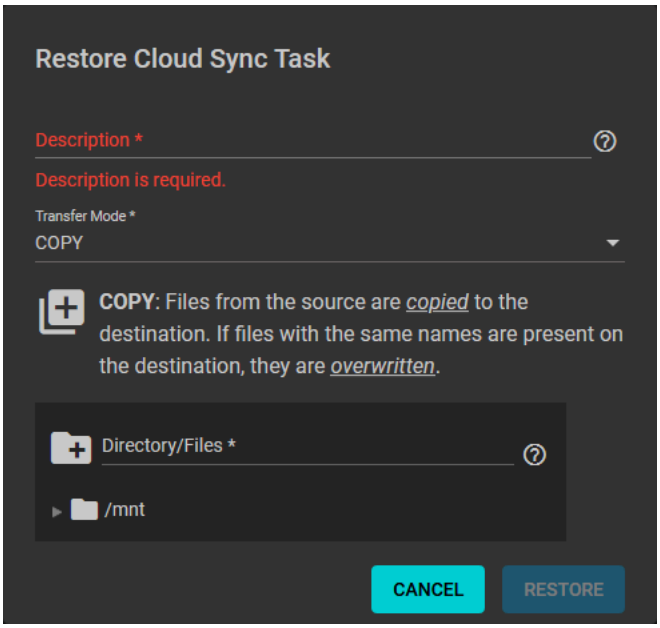
Cloud Sync Behavior

Saved tasks activate based on their schedule, or when you click **RUN NOW**. An in-progress cloud sync must finish before another can begin. Stopping an in-progress task cancels the file transfer and requires starting the file transfer over.

To view logs about a running task or a task most recent run, click the task status.

Cloud Sync Restore

To quickly create a new cloud sync task that uses the same options but reverses the data transfer, expand (❯) on an existing task and click **RESTORE**.

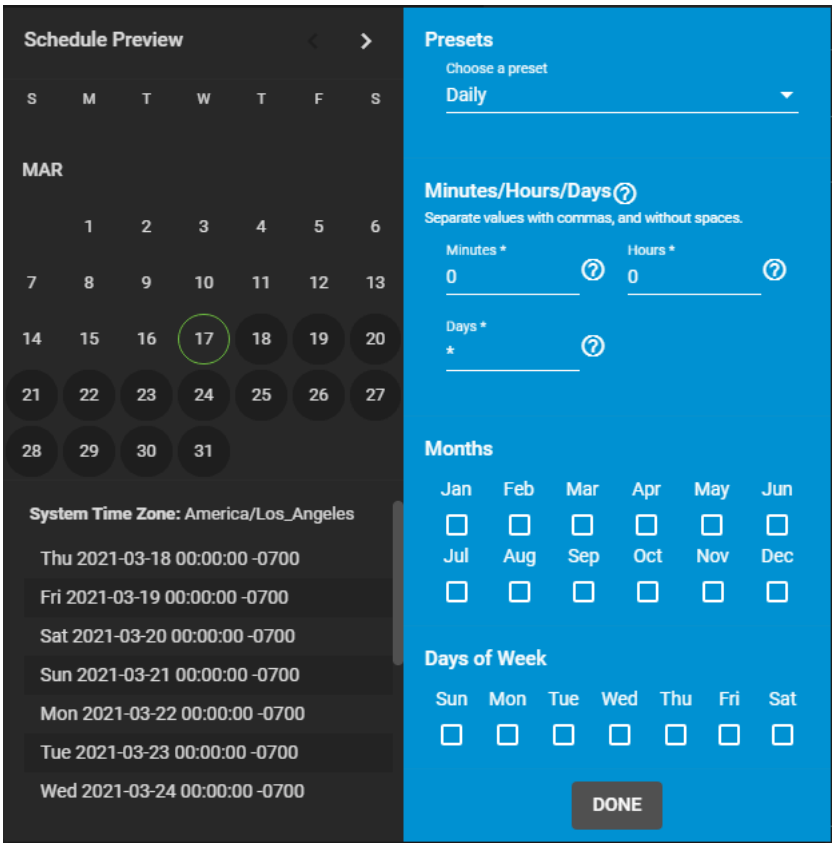


Give the new task a **Description** and define the path to a storage location for the transferred data.

TrueNAS saves the restored cloud sync task as another entry in **Tasks > Cloud Sync Tasks**.

If the restore destination dataset is the same as the original source dataset, the restored files might have their ownership altered to *root*. If *root* did not create the original files and they need a different owner, you can recursively reset ACL Permissions of the restored dataset through the GUI or by running `chown` from the CLI.

Using the Advanced Scheduler



Choosing a **Presets** option automatically populates all fields.

To customize a schedule, enter crontab values for the **Minutes**/**Hours**/**Days**.

The simplest option is to enter a single number in the field. The task runs when the time value matches that number. Entering *10* runs the task when the time is ten minutes past the hour.

An asterisk (*) matches all values.

Set specific time ranges by entering hyphenated number values. Entering *30-35* in the **Minutes** field runs the task at minutes 30, 31, 32, 33, 34, and 35.

You can list individual values separated by a comma (,). Entering *1,14* in the **Hours** field runs the task at 1:00 AM (0100) and 2:00 PM (1400).

A slash (*/*) designates a step value. Entering * in **Days** runs the task every day of the month, while **/2* runs it every other day.

Combining all the above examples creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

There is an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days plus any listed days. Entering *1* in **Days** and setting *Wed* for **Days of Week** creates a schedule that starts a task on the first day of the month *and* every Wednesday of the month.

The **Schedule Preview** displays when the current settings mean the task runs.

▼ Examples of CRON syntax

Syntax	Meaning	Examples
*	Every item.	* (minutes) = every minute of the hour. * (days) = every day.
*/N	Every Nth item.	*/15 (minutes) = every 15th minute of the hour (every quarter hour). */3 (days) = every 3rd day. */3 (months) = every 3rd month.
Comma and hyphen/dash	Each stated item (comma) Each item in a range (hyphen/dash).	1,31 (minutes) = on the 1st and 31st minute of the hour. 1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour. mon-fri (days) = every Monday to Friday inclusive (every weekday). mar,jun,sep,dec (months) = every March, June, September, December.

You can specify days as days of the month or days of the week.

With these options, you can create flexible schedules similar to these examples:

Desired schedule	Values to enter
3 times a day (at midnight, 08:00 and 16:00)	months=*; days=*; hours=0/8 or 0,8,16; minutes=0 (Meaning: every day of every month, when hours=0/8/16 and minutes=0)
Every Monday, Wednesday and Friday, at 8.30 pm	months=*; days=mon,wed,fri; hours=20; minutes=30
1st and 15th day of the month, during October to June, at 00:01 am	months=oct-dec,jan-jun; days=1,15; hours=0; minutes=1
Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday	Note that this requires two tasks to achieve: (1) months=*; days=mon-fri; hours=8-18; minutes=*/15 (2) months=*; days=mon-fri; hours=19; minutes=0 We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround is to stop at 18:45 or 19:45 rather than 19:00.

Backing Up Google Drive to TrueNAS

Google Drive and G Suite are widely used to create and share documents, spreadsheets, and presentations with team members.

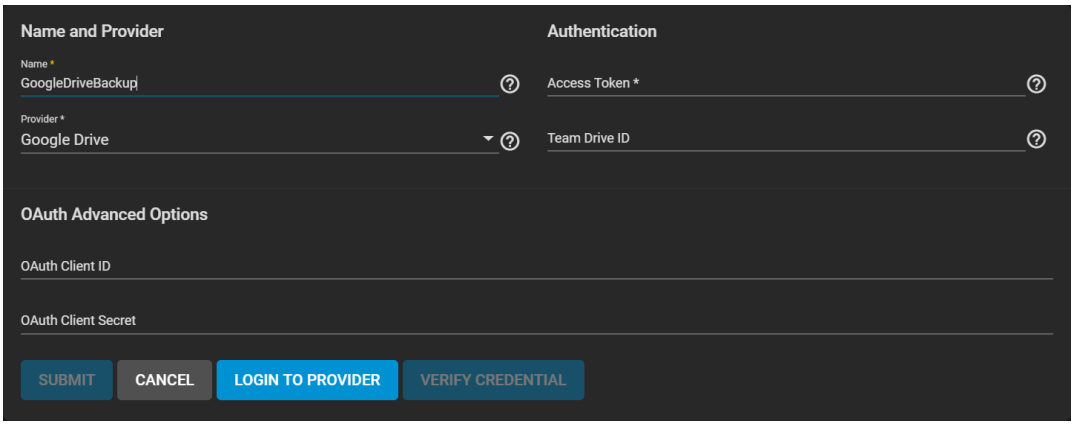
Although cloud-based tools have inherent backups and replications included by the cloud provider, certain users may require additional backup or archive capabilities.

For example, companies using G Suite for important work may need to keep records for years, potentially beyond the scope of the G Suite subscription.

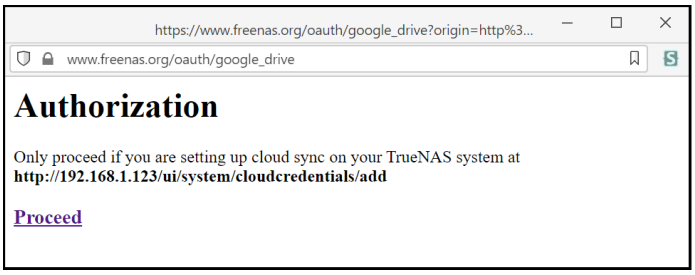
TrueNAS can easily back up Google Drive using its built-in cloud sync.

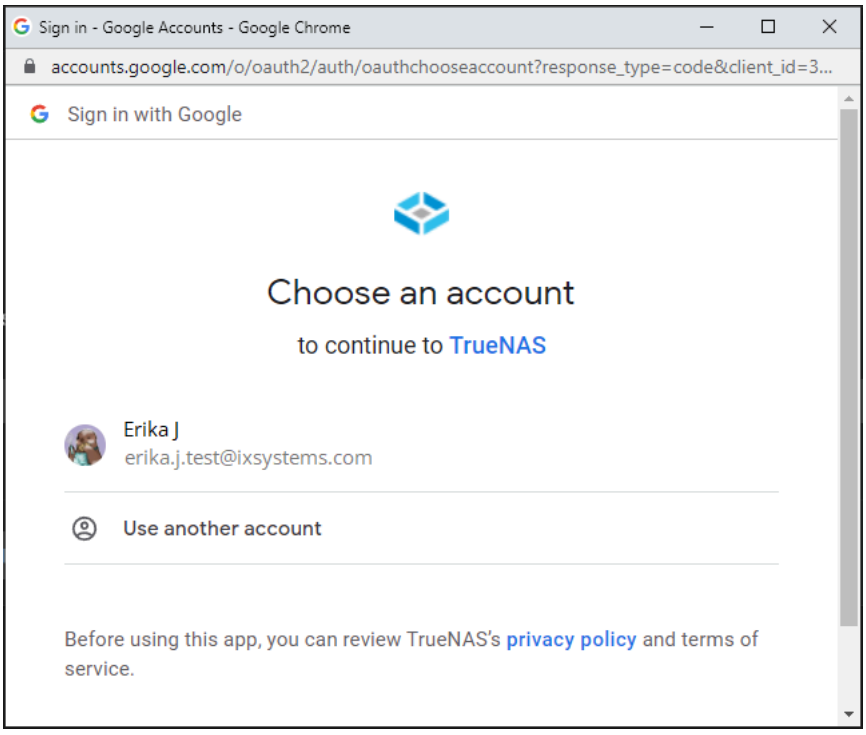
Set up Google Drive Credentials

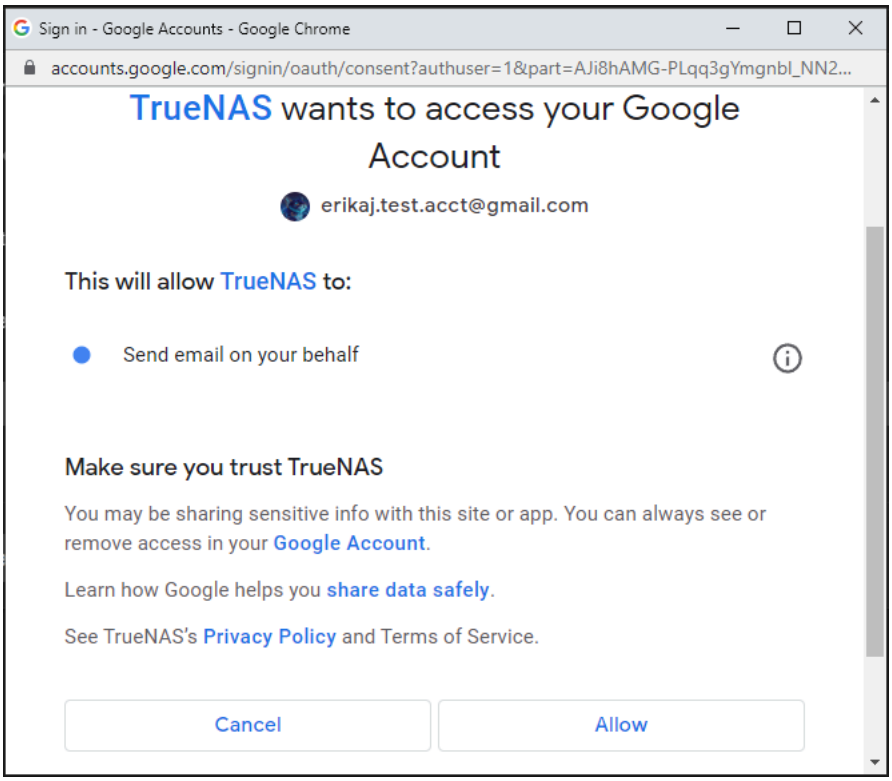
Go to **System > Cloud Credentials** and click **ADD**. Name the Credential and select **Google Drive** as the Provider. Click **LOGIN TO PROVIDER** and log in with the appropriate Google user account.



Google requests permission to access all the Google Drive files for the FreeNAS device.

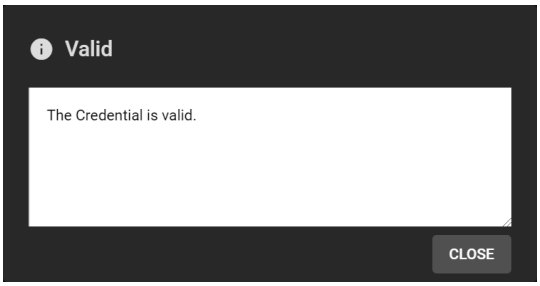






Allow access. The appropriate access key generates in the FreeNAS access token. You may assign a Team ID if necessary.

Click **VERIFY CREDENTIAL** and wait for it to verify, then click **SUBMIT**

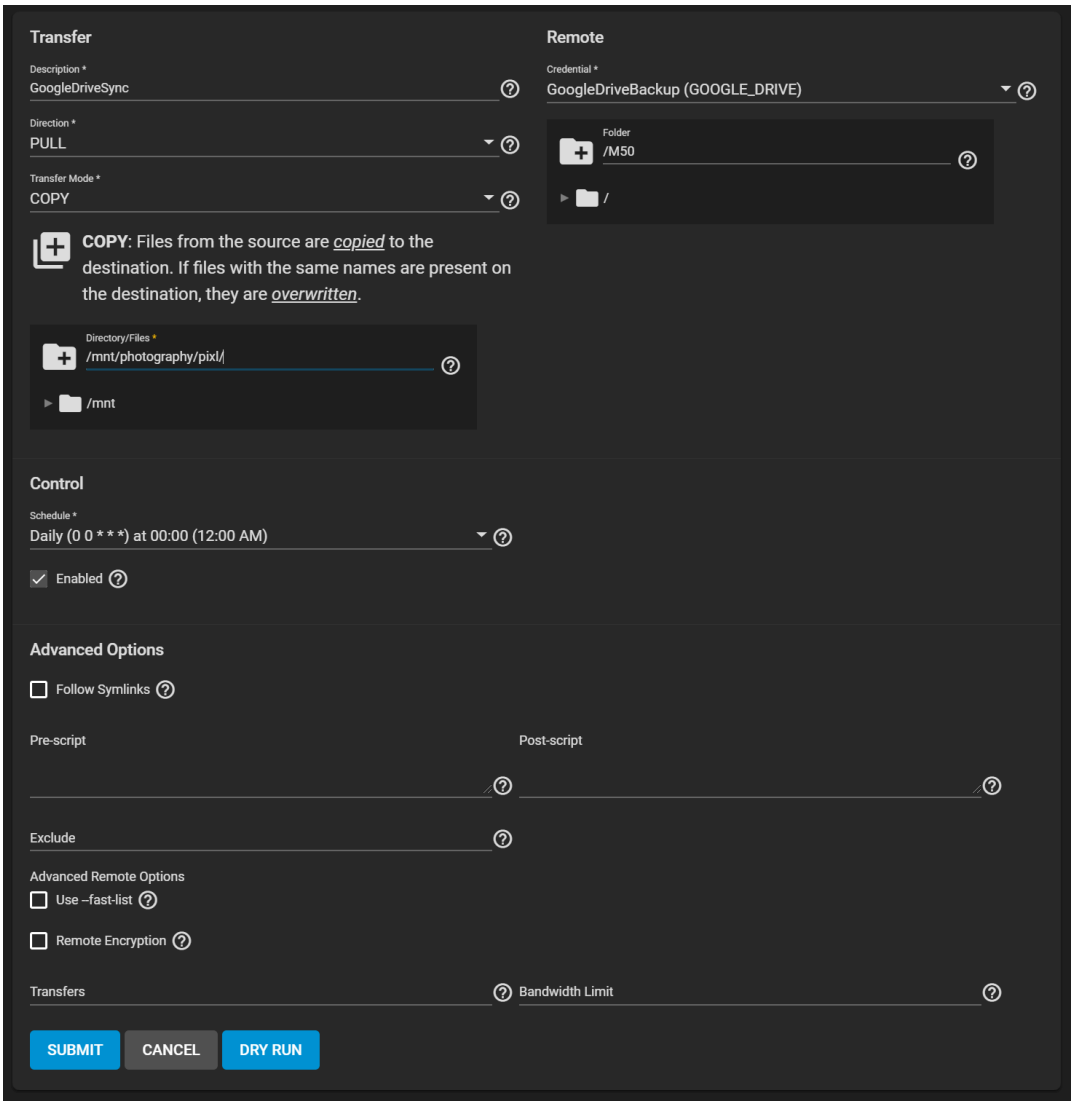


Create the Cloud Sync Task

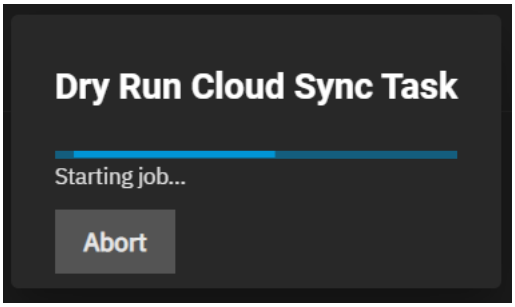
Go to **Tasks > Cloud Sync Tasks** and set the backup time frame, frequency, and folders (cloud-based folder and TrueNAS dataset). Set whether the synchronization should sync all changes, copy new files, or move files. Add a description for the task and select the cloud credentials. Choose the appropriate cloud folder target and TrueNAS storage location.

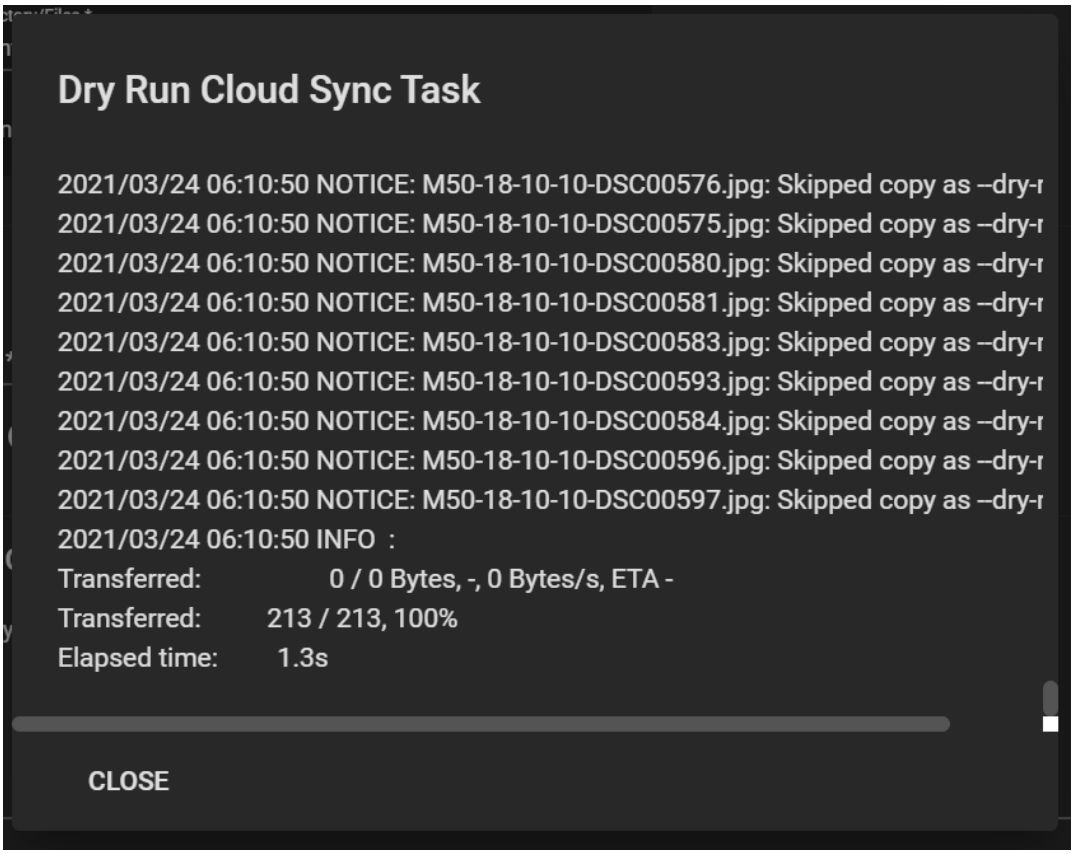
Select the file transfer mode:

- **Sync**: Keep files newly created or deleted the same.
- **Copy**: Copy new files to the appropriate target (i.e., TrueNAS pulls files from Google Drive or pushes files to Google Drive).
- **Move**: Copy files to the target and delete them from the source. With **Move**, users can set a folder in Google Drive for archival and move older documents to that folder from their Drive account. The task would automatically back up the files to the TrueNAS storage.

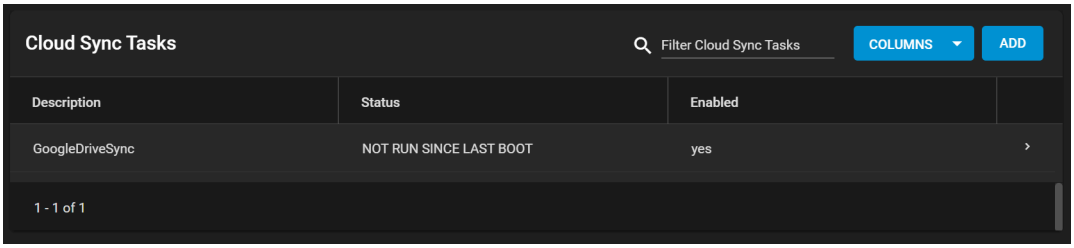


Once you create the task, attempt a **Dry Run**.

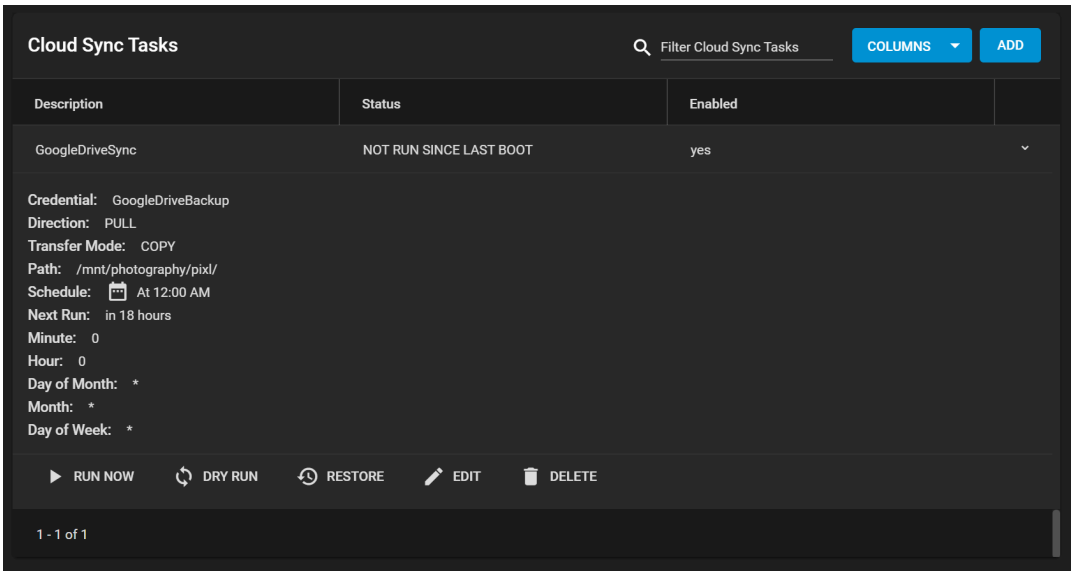




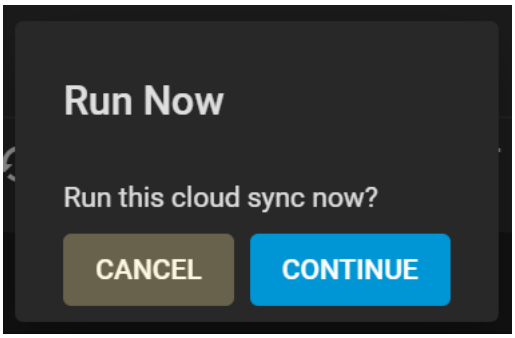
If the Dry Run succeeds, click **SAVE**..

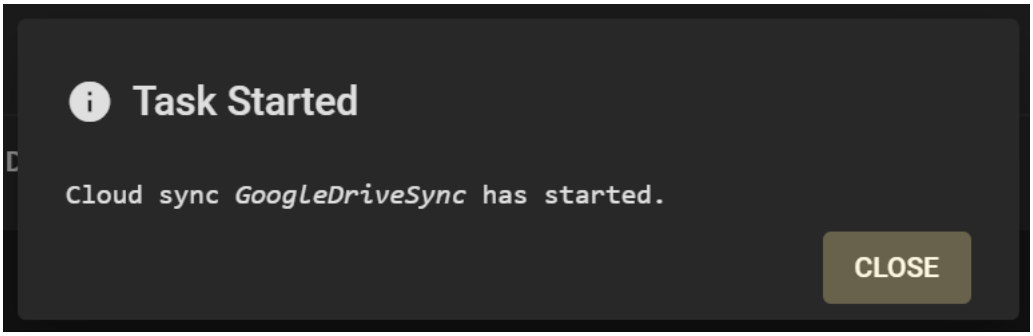


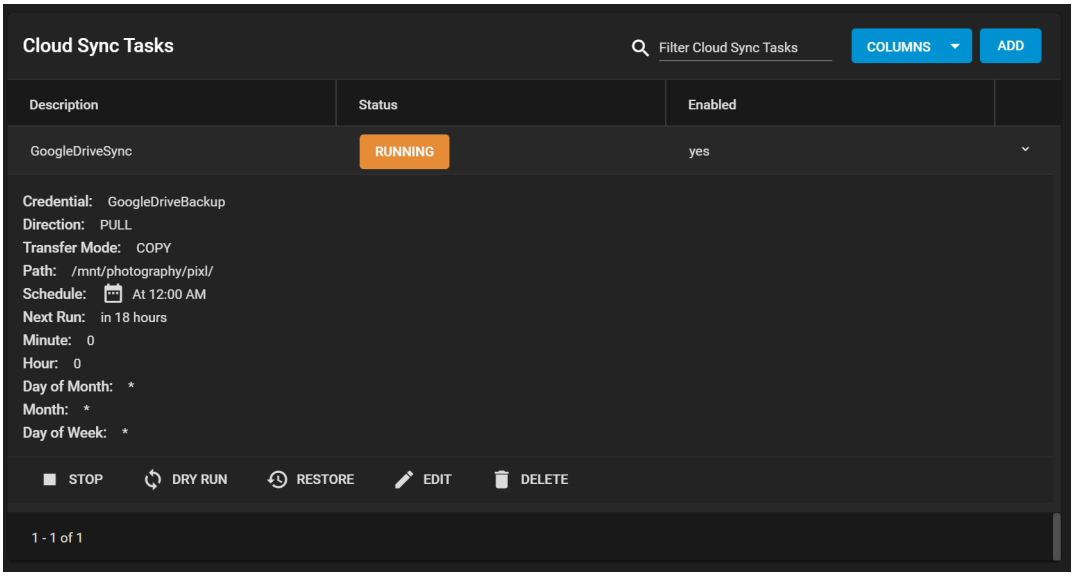
Expand the section down to see the task options.



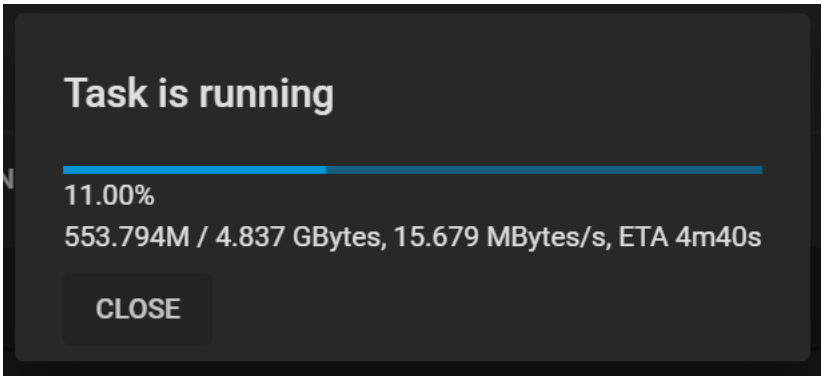
Clicking **RUN NOW** prompts the task to start immediately.



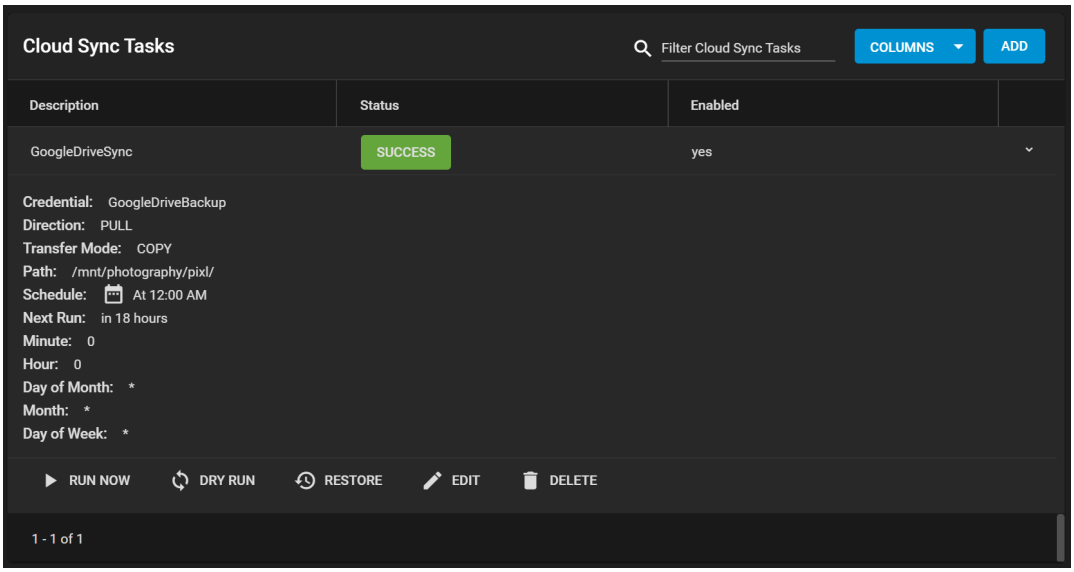




The web interface shows the status as **RUNNING** and **SUCCESS** upon completion. You can see details in the **Task Manager**. While the task runs, clicking on the **RUNNING** button reveals a popup log.

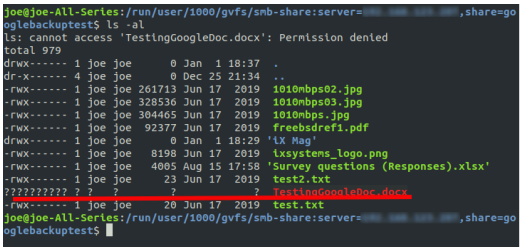


Once the sync reports **SUCCESS**, you can verify it by opening the folder on another computer if it is a share, through SSH access, or by checking the destination directory through the TrueNAS CLI.

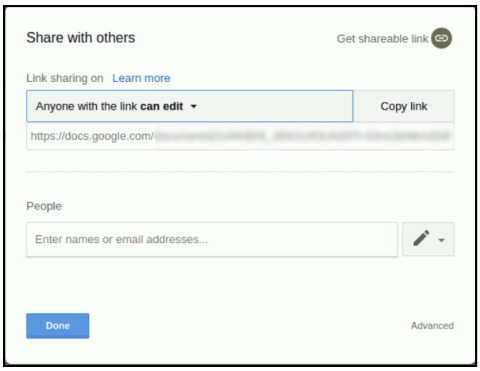


Working with Google-Created Content

One caveat is that Google Docs and other files created with Google tools have their own proprietary set of permissions and their read/write characteristics unknown to the system over a standard file share. Files are unreadable as a result.



To allow Google-created files to become readable, allow link sharing to access the files before the backup. Doing so ensures that other users can open the files with read access, make changes, and then save them as another file if further edits are needed. Note that this is only necessary if the file was created using Google Docs, Google Sheets, or Google Slides; other files should not require modification of their share settings.

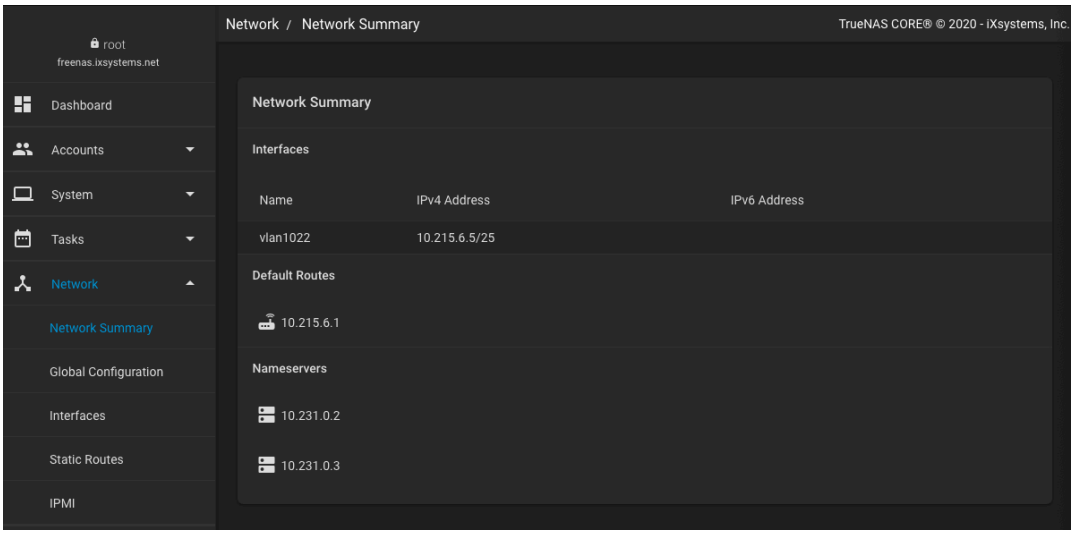


TrueNAS is perfect for storing content, including cloud-based content, for the long term. Not only is it simple to sync and backup from the cloud, but users can rest assured that their data is safe, with snapshots, copy-on-write, and built-in replication functionality.

Network

Network Summary

The **Network Summary** screen gives a concise overview of the current network setup. It provides information about the currently active interfaces, default routes, and name servers configured on the system. These areas are not editable.



- **Interfaces** shows configured physical, bridge, link aggregation LAGG, and virtual LAN vlan interfaces. All detected physical interfaces are listed, even when unconfigured. The IPv4 or IPv6 address displays when a static IP is saved for an interface.
- **Default Routes** lists all saved TrueNAS default routes. Go to **Network > Global Configuration** to configure default routes.
- **Nameservers** lists any configured DNS name servers that TrueNAS uses. To change this list, go to **Network > Global Configuration**. **Network > Global Configuration** contains the TrueNAS host name and domain, and default gateway. It also contains other options.

Define a static route in **Network > Static Routes**.

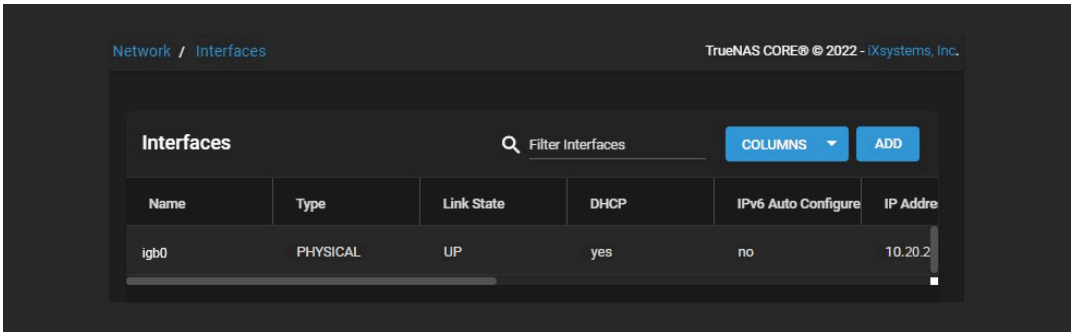
Out-of-band management is managed from **Network > IPMI**. This option is visible only when TrueNAS detects the appropriate physical hardware.

Interfaces

Editing an Interface

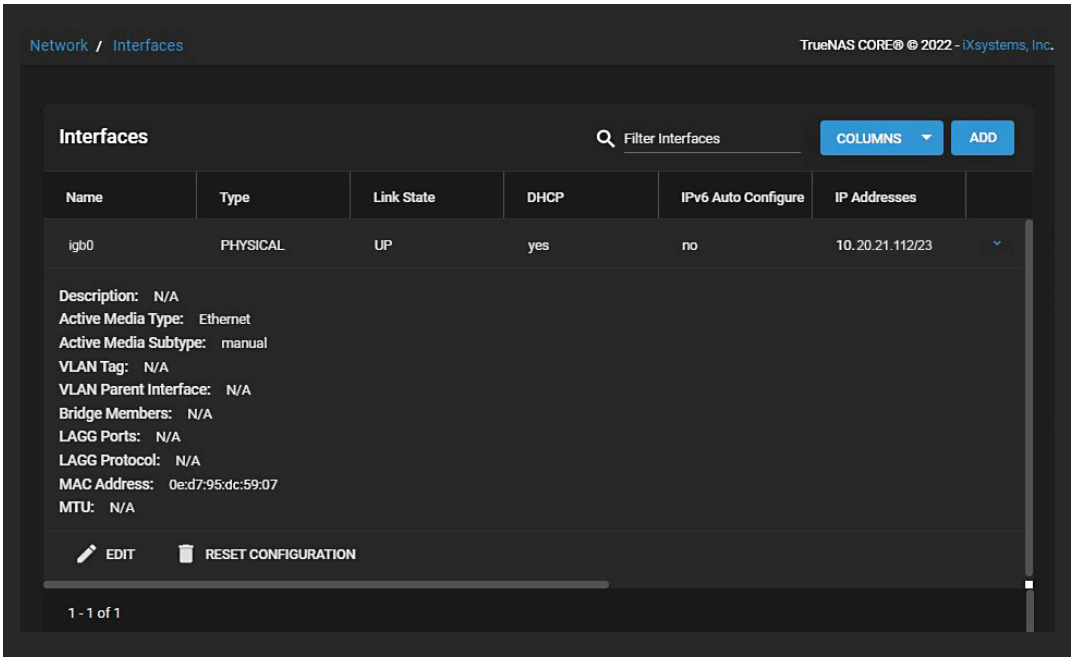
> Be careful when configuring the network interface that controls the TrueNASB® web interface. An error can result in the loss of web connectivity.

Network > Interfaces lists all physical Network Interface Controllers (NICs) connected to your TrueNASB® system.



To edit an interface, click **>** next to it to expand the view. This provides a general description about the chosen interface. Click **EDIT**.

> TrueNAS Enterprise customers: you cannot edit an interface with High Availability (HA) enabled.
> Go to **System > Failover** and check the **Disable Failover** box, then click **SAVE**.

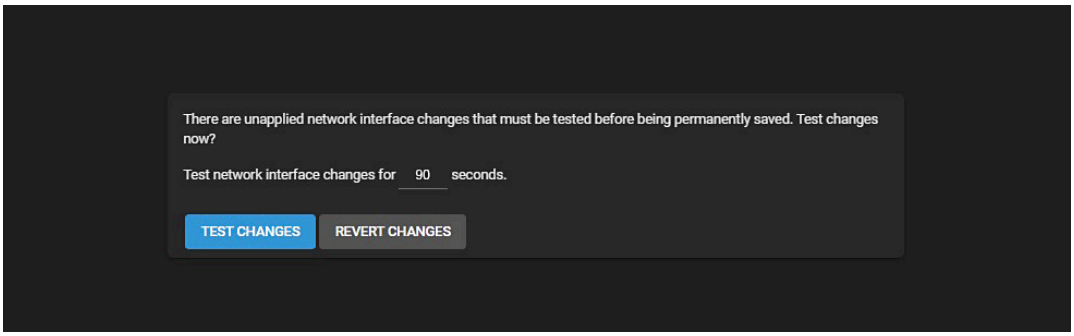


> The **Type** of interface determines the interface editing options available.

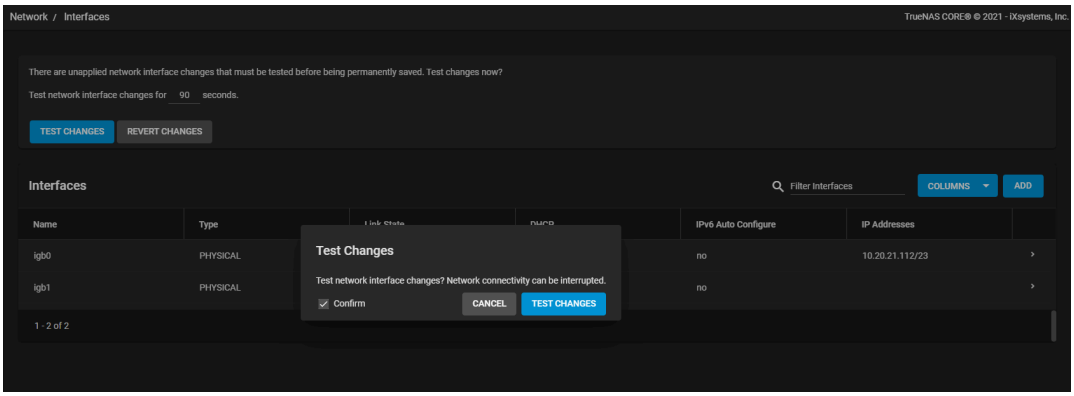
See Interfaces Screen for more information on settings.

Saving Interface Changes

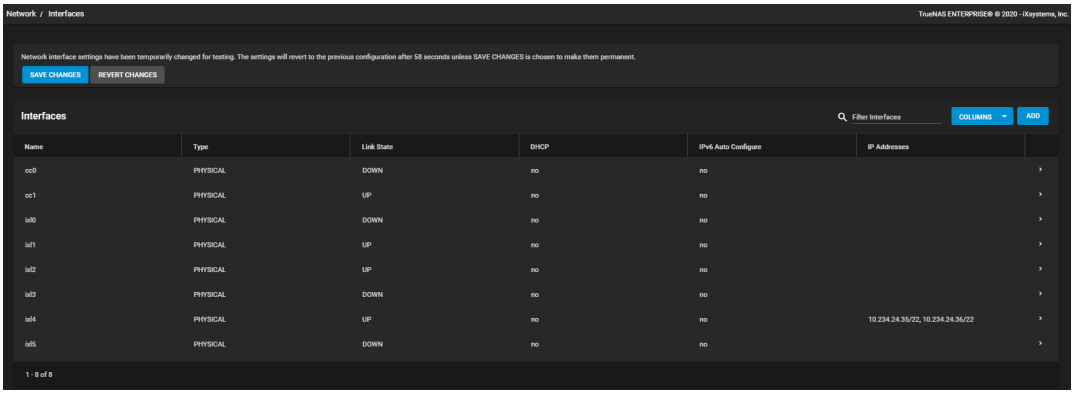
After completing interface editing, click **SAVE**. You have the option to **TEST CHANGES** or **REVERT CHANGES**. The default time for testing changes is 60 seconds, but you can change it to your desired setting.

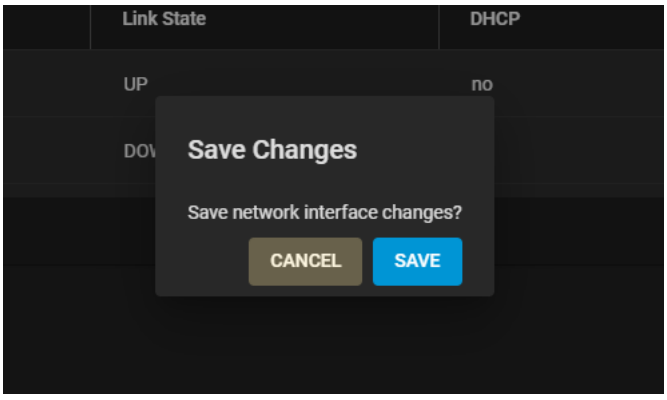


After clicking **TEST CHANGES**, confirm your choice and click **TEST CHANGES** again.

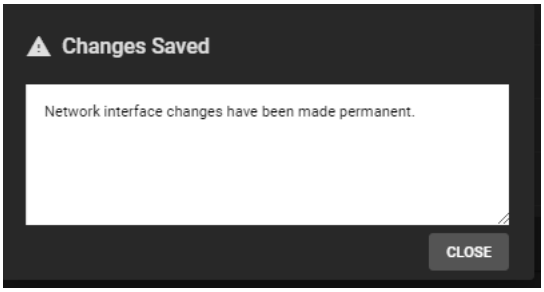


Either click **SAVE CHANGES** or **REVERT CHANGES**. You have the time specified to make this choice. Clicking **SAVE CHANGES** opens a dialog with the option to **CANCEL** or **SAVE** network interface changes. Click **SAVE**.





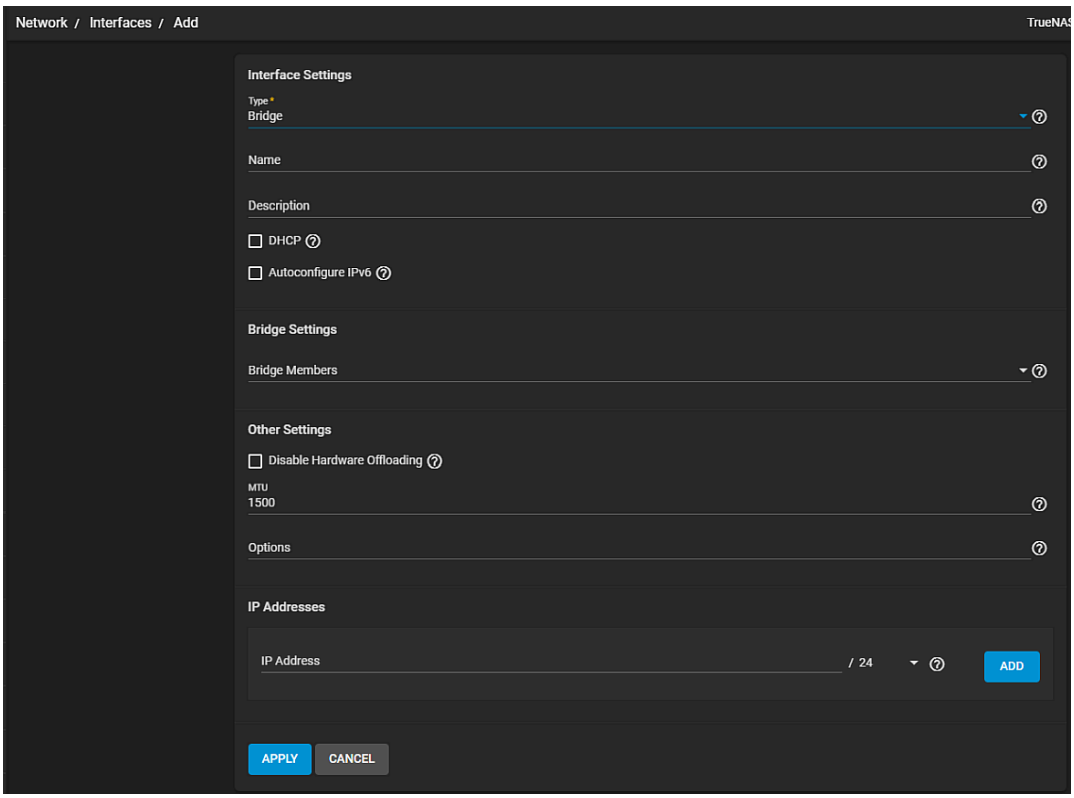
The system displays a dialog that shows the network interface changes are now permanent.



Setting Up a Network Bridge

A bridge generally refers to various methods of combining (aggregating) many network connections. These form a single total network. TrueNAS uses bridge(4) to manage bridges.

To set up a bridge interface, go to **Network > Interface > Add**.



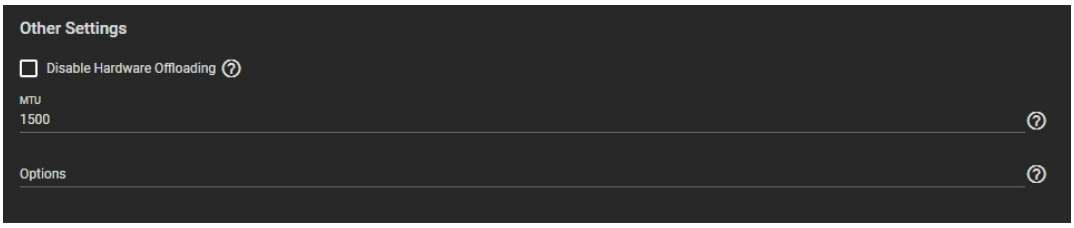
Select **Bridge** as the **Type** and enter a name for the interface. The name must use the format **bridge**X*, where *X* is a number representing a non-parent interface. It is also recommended to add any notes or reminders. Enter details about this particular bridge in **Description**.

The next section is **Bridge Settings**. Use the dropdown list next to **Bridge Members** to select the correct interfaces. Configure the remaining interface options to match your networking needs.

See Interfaces Screen for more information on settings.

Other Settings

Every kind of network interface has common settings:



Disabling **Hardware Offloading** can reduce network performance. It is not recommended.

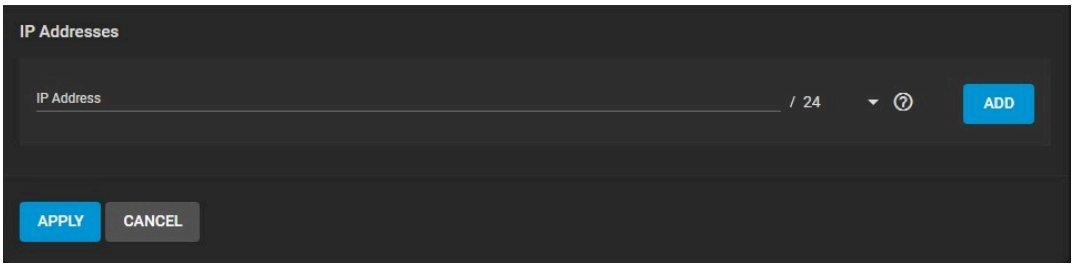
Disabling this option is sometimes necessary. For example, when the interface is managing jails, plugins, or virtual machines.

MTU stands for maximum transmission unit. It is the largest protocol unit for transferring data. MTU size varies. Physical hardware and available network interfaces determine the largest workable MTU size. 1500 and 9000 are standard Ethernet MTU sizes. The recommendation is to use the default 1500. The permissible range of MTU values is 1492-9216. Leaving this field blank sets the default value of **1500**.

You can enter more tuning ifconfig settings in the **Options**.

IP Addresses

Additional aliases for the interface can also be defined:

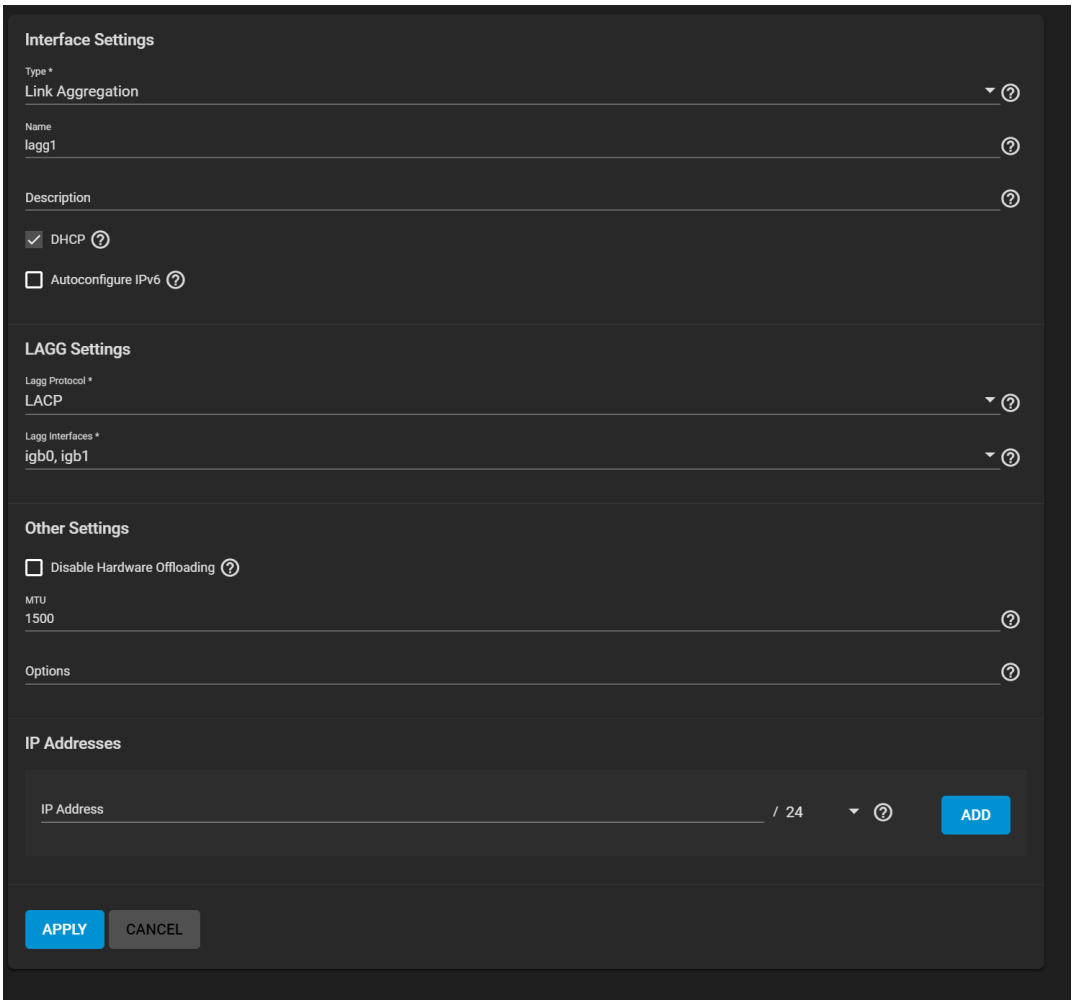


It is possible to define either IPv4 or IPv6 addresses and subnets from 1-32. Clicking **Add** provides another field for defining an IP address.

Setting Up Link Aggregations

A Link Aggregation (LAGG) is a general method of combining (aggregating) many network connections. The connections are either parallel or in series. This provides extra bandwidth or redundancy for critical networking situations. TrueNAS uses lagg(4) to manage LAGGs.

To set up a LAGG interface, go to **Network > Interface > Add**.



Set the **Type** to **Link Aggregation**.

Enter a name for the interface. The name must use the format *laggX*, where *X* is a number representing a non-parent interface. Enter any notes or reminders about this particular LAGG in the **Description** field.

Go to **LAGG Settings** and then **Lagg Protocol** to configure the interface ports to match your networking needs:

Lagg Protocols

LACP

The most commonly used LAGG protocol. It is one part of IEEE specification802.3ad. LACP mode performs negotiation with the network switch to form a group of ports. These are all active at the same time. The network switch must support LACP for this option to function.

Failover

Failover sends traffic through the primary interface of the group. Traffic diverts to the next available interface in the LAGG if the primary is not accessible.

Load Balance

Load Balance accepts inbound traffic on any port of the LAGG group. It then balances the outgoing traffic on the active ports in the LAGG group. It is a static setup that does not watch the link state nor does it negotiate with the switch.

Round Robin

Round robin accepts inbound traffic on any port of the LAGG group. It sends outbound traffic using a round robin scheduling algorithm. The outbound traffic sends in sequence, using each LAGG interface in turn.

None

This mode disables traffic on the LAGG interface without disabling the LAGG interface.

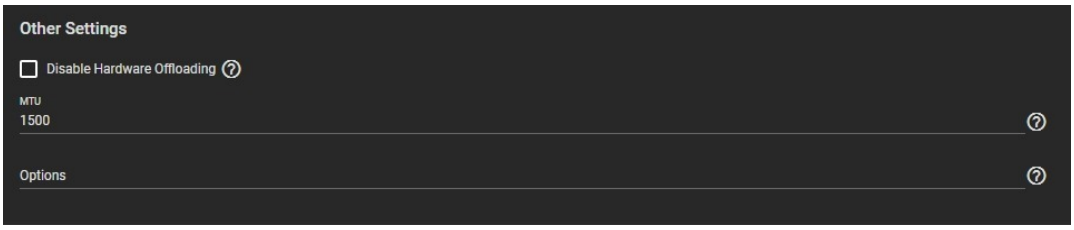
Lagg Interfaces

Now define the **Lagg Interfaces** and review the remaining interface options.

See Interfaces Screen for more information on settings.

Other Settings

Every kind of network interface has common settings:



Disabling **Hardware Offloading** can reduce network performance. It is not recommended.

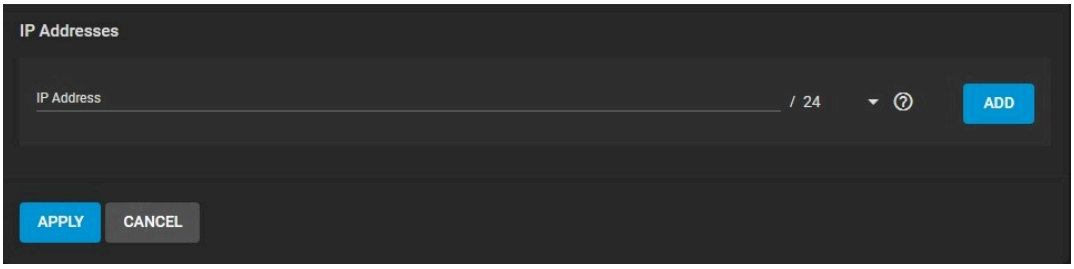
Disabling this option is sometimes necessary. For example, when the interface is managing jails, plugins, or virtual machines.

MTU stands for maximum transmission unit. It is the largest protocol unit for transferring data. MTU size varies. Physical hardware and available network interfaces determine the largest workable MTU size. 1500 and 9000 are standard Ethernet MTU sizes. The recommendation is to use the default 1500. The permissible range of MTU values is 1492-9216. Leaving this field blank sets the default value of **1500**.

You can enter more tuning ifconfig settings in the **Options**.

IP Addresses

Additional aliases for the interface can also be defined:

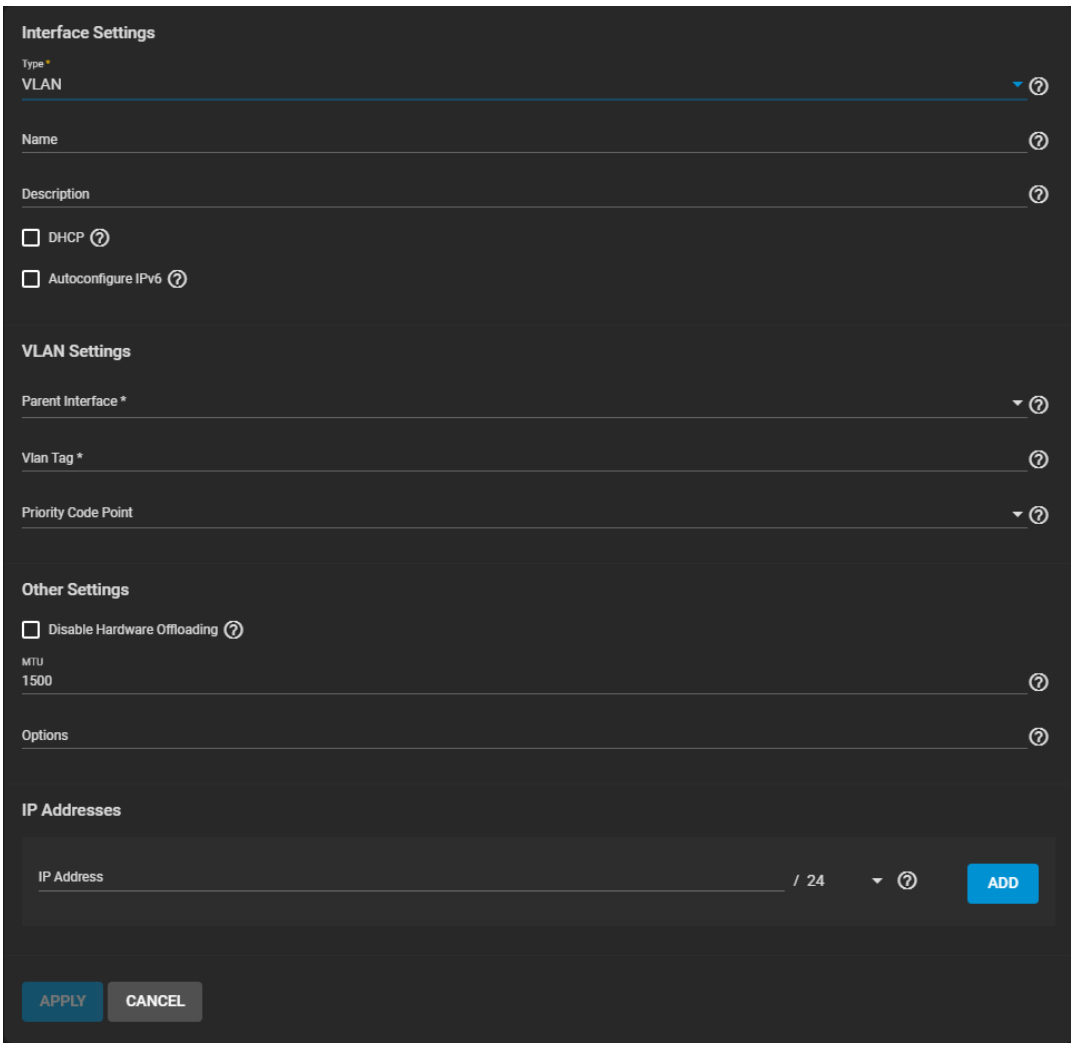


It is possible to define either IPv4 or IPv6 addresses and subnets from 1-32. Clicking **Add** provides another field for defining an IP address.

Setting Up a Network VLAN

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

To set up a VLAN interface, go to **Network > Interface > Add**.



Set the **Type** to **VLAN** and enter a name for the interface in **Name**. The name must use the format **vlan***X*, where *X* is a number representing a non-parent interface. Enter any notes or reminders about this VLAN in the **Description** field.

Determine the requirements of your network environment before enabling **DHCP** or **AutoconfigureIPv6**. It is important to understand how this new interface functions in your situation. By default, TrueNAS allows only one network interface to have **DHCP** enabled.

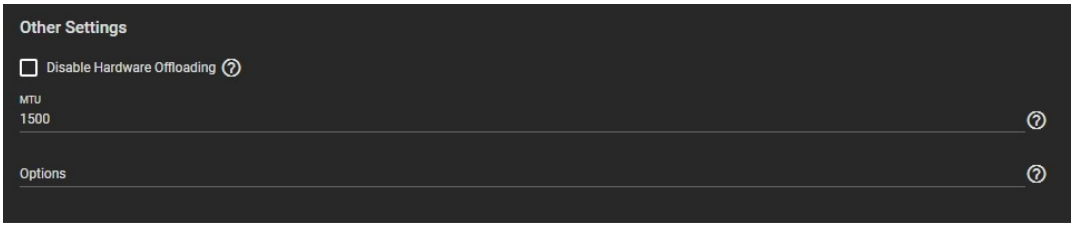
Give careful attention to the remaining **VLAN Settings**. These need proper configuration in order for the network interface to function.

- **Parent Interface** where you select the VLAN parent interface. This is usually an Ethernet card connected to a switch port already configured for the VLAN.
- **Vlan Tag** where you enter a numeric tag for this interface. This is usually preconfigured in the switched network.
- **Priority Code Point** where you define the VLAN Class of Service.

There are a few extra interface options to review after the VLAN options are set.
See Interfaces Screen for more information on settings.

Other Settings

Every kind of network interface has common settings:



Disabling **Hardware Offloading** can reduce network performance. It is not recommended.

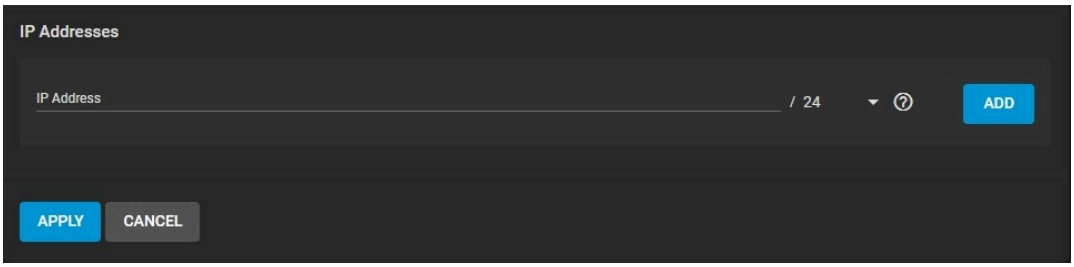
Disabling this option is sometimes necessary. For example, when the interface is managing jails, plugins, or virtual machines.

MTU stands for maximum transmission unit. It is the largest protocol unit for transferring data. MTU size varies. Physical hardware and available network interfaces determine the largest workable MTU size. 1500 and 9000 are standard Ethernet MTU sizes. The recommendation is to use the default 1500. The permissible range of MTU values is 1492-9216. Leaving this field blank sets the default value of **1500**.

You can enter more tuning ifconfig settings in the **Options**.

IP Addresses

Additional aliases for the interface can also be defined:



It is possible to define either IPv4 or IPv6 addresses and subnets from 1-32. Clicking **Add** provides another field for defining an IP address.

Setting a Static IP Address for the TrueNAS UI

> **Disruptive Change**
>
> It is possible to make changes to the network interface that the web interface uses. But this can result in losing connection to the TrueNAS system! Very often fixing misconfigured network settings requires command line knowledge. Physical access to the system is often required as well.

Multiple interfaces connected to a single TrueNAS system cannot be members of the same subnet.

You can combine multiple interfaces with link aggregation (LAGG) or a network bridge. Alternatively, you can assign multiple static IP addresses to a single interface by configuring aliases.

▼ Click for more information

When multiple network interface cards (NICs) connect to the same subnet, users might incorrectly assume that the interfaces automatically load balance. However, ethernet network topology allows only one interface to communicate at a time. Additionally, both interfaces must handle broadcast messages since they are listening on the same network. This configuration adds complexity and significantly reduces network throughput.

If you require multiple NICs on a single network for performance optimization, you can use a link aggregation (LAGG) configured with Link Aggregation Control Protocol (LACP). A single LAGG interface with multiple NICs appears as a single connection to the network.

While LACP is beneficial for larger deployments with many active clients, it might not be practical for smaller setups. It provides additional bandwidth or redundancy for critical networking situations. However LACP has limitations as it does not load balance packets.

On the other hand, if you need multiple IP addresses on a single subnet, you can configure one or more static IP aliases for a single NIC.

In summary, we recommend using LACP if you need multiple interfaces on a network. If you need multiple IP addresses, define aliases. Deviation from these practices might result in unexpected behavior.

For a detailed explanation of ethernet networking concepts and best practices for networking multiple NICs, refer to this discussion from National Instruments.

▼ Process Summary

Configuring a static IP address involves both the TrueNAS web UI and the Console Setup menu.

- Web UI
  - **Network > Interfaces** > **Add** or **Edit**
    - Type address into **IP Address** and select a subnet mask.
    - **Add** or **Delete** additional addresses as needed.
  - Test saved changes before permanently applying them.
    - Dialog asks to temporarily apply changes.
    - After you apply the network settings changes, they don't immediately become permanent. You can choose the amount of time the new settings will work as temporary settings. After this designated amount of time, the new network settings become permanent if you save them. Saving the new network changes overwrites the previous configuration.
  - **Network > Network Summary** summarizes addressing information of every configured interface.
- Console menu
  - Physical Interfaces: select **Configure Network Interfaces** (options are similar for other interface types)
    - Delete interface? enter or select `n`
    - Remove interface settings? enter or select `n`
    - Configure IPv4? enter or select `y`
      - Enter IP address and subnet mask
    - Configure IPv6 enter or select `y`
      - Enter IP address
    - Configure failover? enter or select `n`
  - Saving changes interrupts the web interface and could require a system reboot.

Setting Static IP Addresses

TrueNAS can configure physical network interfaces with static IP addresses. Use either the web interface or the system console menu.

> The recommendation is to use the web interface for this process. There are extra safety features to prevent saving misconfigured interface settings.

Adding Static IP Addresses Using the Web Interface

Log in to the web interface and go to **Network > Interfaces**. This contains creation and configuration options for physical and virtual network interfaces.

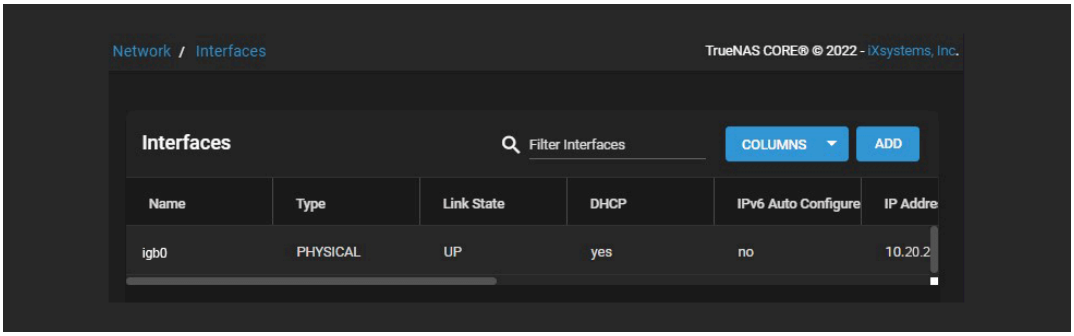


Figure 1: Interfaces List

You can configure static IP addresses while creating or editing an interface.

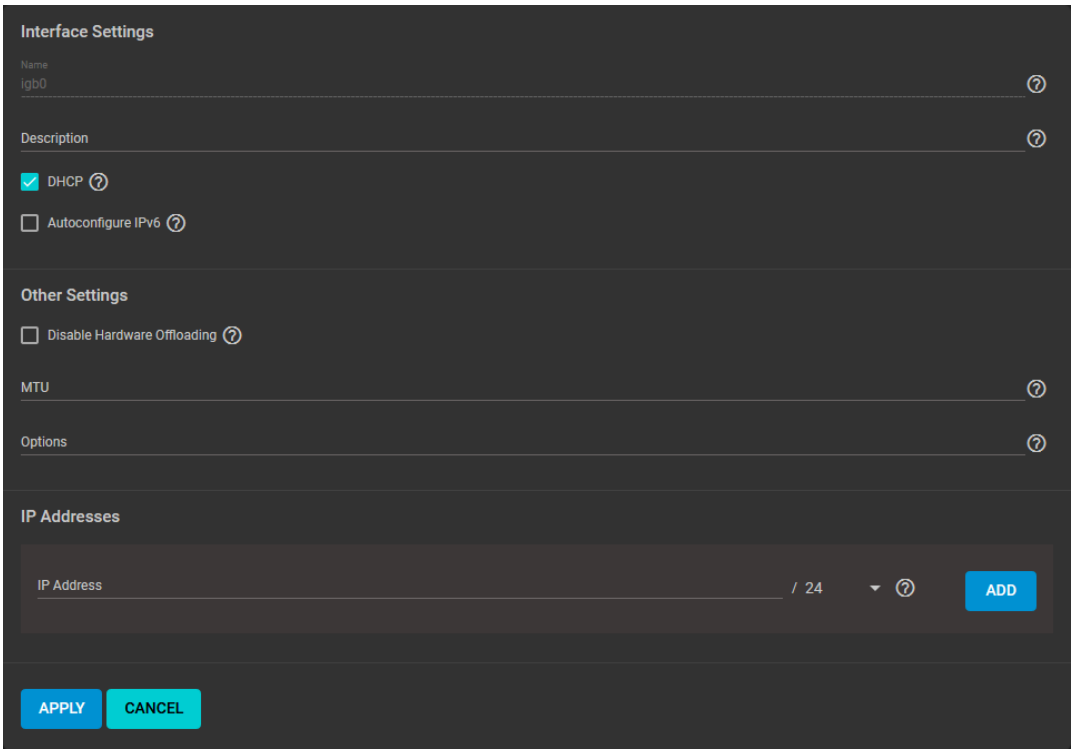


Figure 2: Editing an Interface

Type the desired address in the **IP Address** field and select a subnet mask.

> Multiple interfaces cannot be members of the same subnet.
>
> If an error displays when setting the IP addresses on multiple interfaces, check the subnet.

Use the buttons to **Add** and **Delete** more IP addresses as needed.

To avoid saving invalid or unusable settings, network changes are at first temporary. Applying any interface changes adds a dialog to the **Network > Interfaces** list.

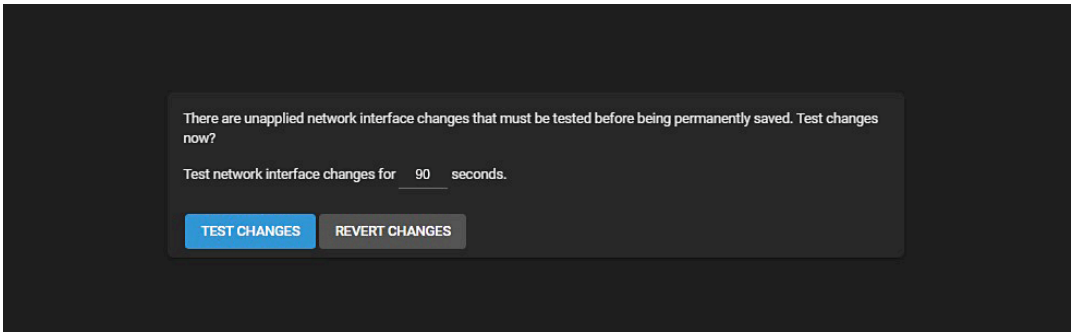


Figure 3: Interface Changes Detected

You can adjust how long to test the network changes before they revert back to the previous settings. If the test is successful, another dialog allows making the network changes permanent.

To view system networking settings, go to **Network > Network Summary**.

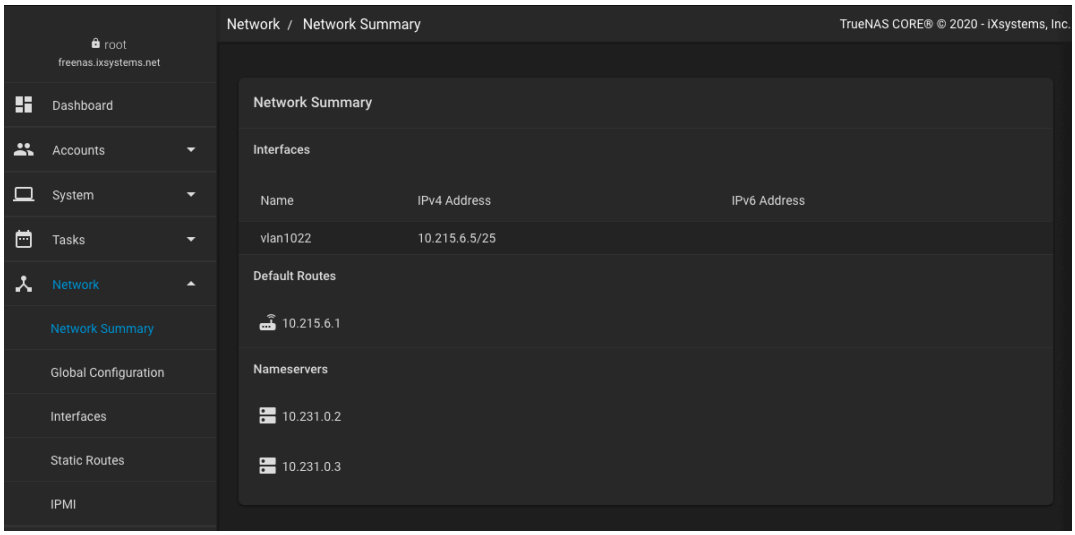


Figure 4: Network Summary

Using the System Console Menu to Assign Static IP Addresses to a Physical Interface

You need to have a monitor and keyboard attached to the system to use the console. If the system hardware allows it, you can connect with IPMI. The console menu displays after the system completes booting.

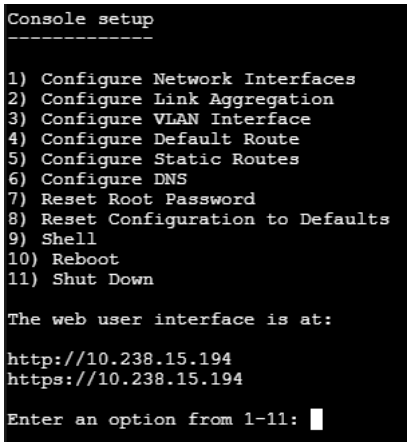


Figure 5: TrueNAS Console Setup Menu

To add static IP addresses to a physical interface, go to **Configure Network Interfaces**. Other interface types have a similar process to add static IP addresses. Interfaces that are already configured for DHCP have that option disabled. There are many prompts to answer before you can add a static address. This example shows adding static IPv4 addresses to interface *igb0*:

▼ Example

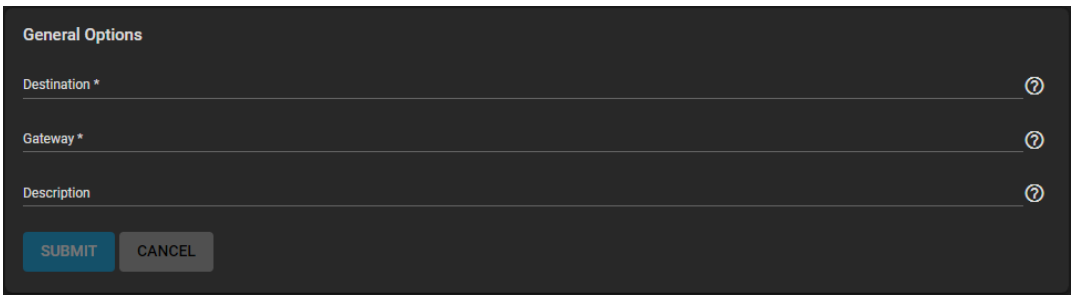
```
Enter an option from 1-11: 1
1) igb0
2) igb1
Select an interface (q to quit): 1
Delete interface? (y/n) n
Remove the current settings of this interface? (This causes a momentary disconne
ction of the network.) (y/n) n
Configure IPv4? (y/n) y
Interface name:
Several input formats are supported
Example 1 CIDR Notation:
    192.168.1.1/24
Example 2 IP and Netmask separate:
    IP: 192.168.1.1
    Netmask: 255.255.255.0, /24 or 24
IPv4 Address:10.238.15.194/22
Saving interface configuration: Ok
Configure IPv6? (y/n) n
Configure failover settings? (y/n) n
Restarting network: ok
Restarting routing: ok
```

Saving interface configuration changes disrupts the web interface while system networking restarts. The new settings might need a system reboot to take effect. If the web interface is unavailable, this could also require a reboot. Check if the network interface you changed is the one utilized by the web interface.

Define Static Routes

Static routes are fixed, or non-adaptive routes. They are manually configured routes in the routing table.

It is recommended to use the web UI for all configuration tasks. TrueNAS does not have static routes defined by default. When required, add a static route by going to **Network** > **Static Routes** and clicking **ADD**.



- Enter a **Destination** IP address. Use the format *A.B.C.D/E* where *E* is the CIDR mask.
- Enter the IP address of the **Gateway**.
- Enter any notes or identifiers describing the route in **Description**.

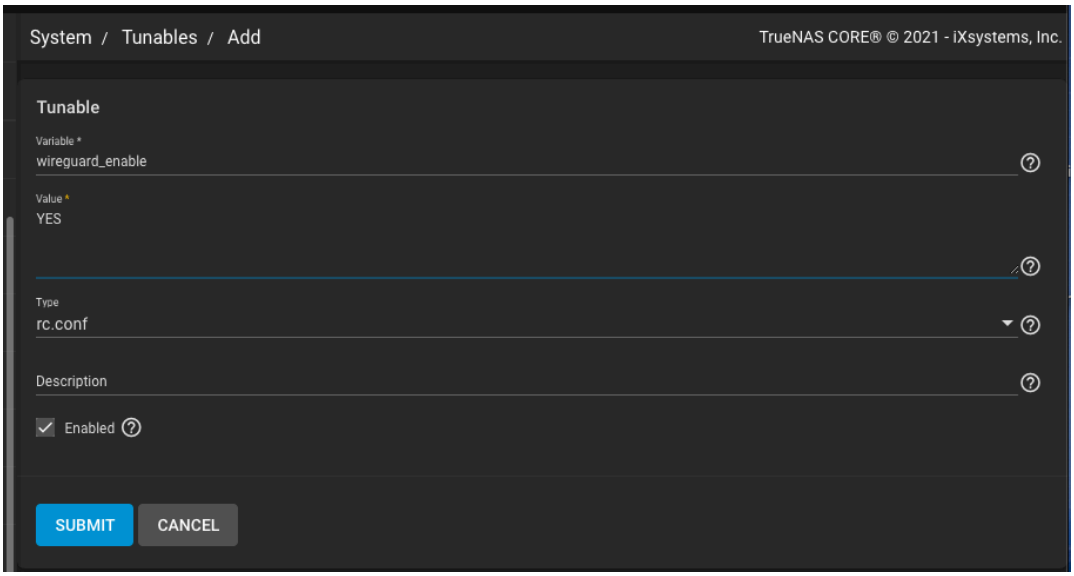
Enabling WireGuard

WireGuard is a popular option in the VPN marketplace. It is fast, simple, and uses modern cryptography standards. It is possible to connect your NAS to a WireGuard network in a few easy steps. Systems running FreeNAS version 11.3-RC1 through TrueNAS 13.0 have WireGuard capability.

Configure System Tunables for WireGuard

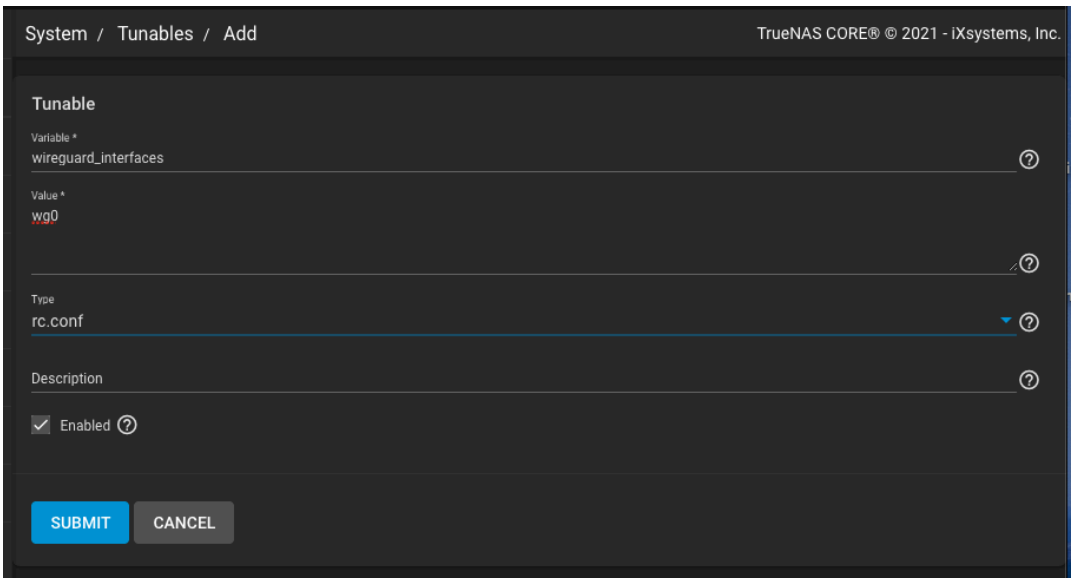
Go to **System > Tunables > Add** and use these settings to enable the service:

- **Variable** = **wireguard_enable**
- **Value** = **YES**
- **Type** = **rc.conf**

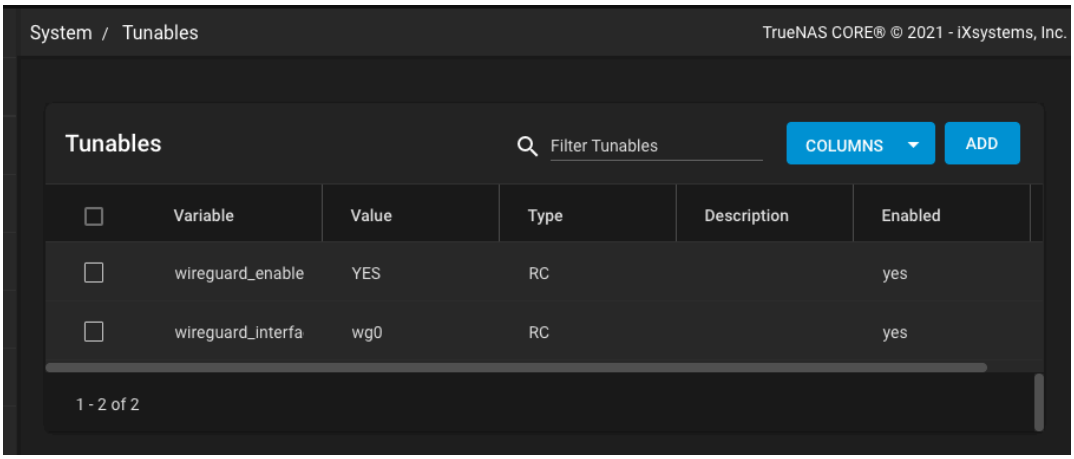


Next, create another tunable to define the networking interface:

- **Variable** = **wireguard_interfaces**
- **Value** = **wg0**
- **Type** = **rc.conf**



When finished, TrueNAS sets and enables the two variables.



Configure a Init/Shutdown Script

Next, create a post-init script. This places the WireGuard config in the correct location at startup.

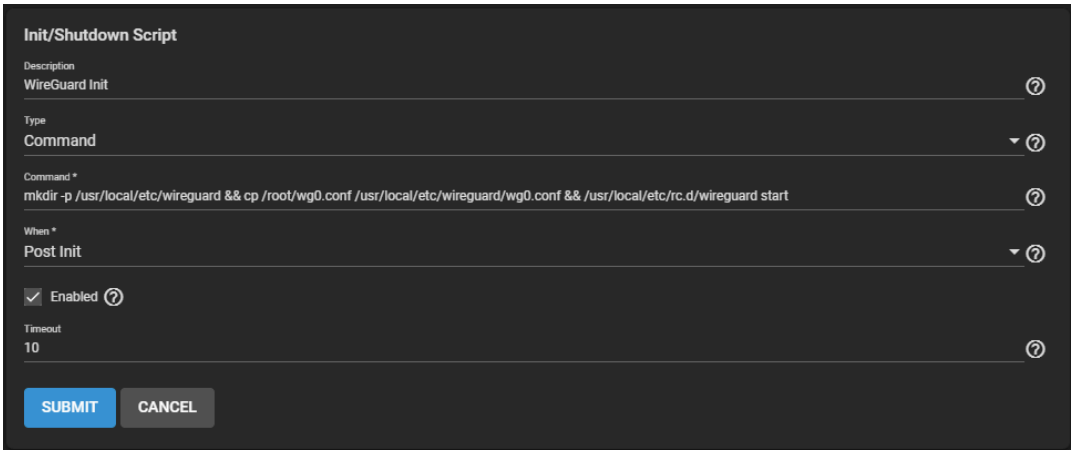
Go to **Tasks > Init/Shutdown Scripts** and click **Add**. Configure the script to load the WireGuard .conf file each time the system boots:

- **Type** = **Command**
- **Command** = `mkdir -p /usr/local/etc/wireguard && cp /root/wg0.conf /usr/local/etc/wireguard/wg0.conf && /usr/local/etc/rc.d/wireguard start`
- **When** = **Post Init**

Configure the WireGuard File

You can configure the /root/wg0.conf file. This applies a WireGuard configuration to attach to whatever WireGuard network you define. It can be a single point-to-point to anything running WireGuard. It can even use full routing. Example use cases are:

- Access data on a NAS from your Remote Laptop
- Linking NAS to NAS for replication
- Attaching a managed NAS to a remote network
- Access to your NAS from your smartphone



Create the File with WireGuard Configuration to Apply at Boot

Now create the /root/wg0.conf. This is the specific WireGuard configuration to apply at boot. These file settings depend on your specific networking environment and requirements. Their configuration is beyond the scope of this article.

There are quickstart guides and tutorials available online as well as the built-in wg-quick manpage.

Determine that you have a valid /root/wg0.conf. If so, rebooting the system brings up the WireGuard interface with a wg0 device in the output of `ifconfig`.

```
# ifconfig wg0
wg0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu 1420
        options=80000<LINKSTATE>
        inet 192.168.X.X --> 192.168.X.X netmask 0xffffff00
        nd6 options=101<PERFORMNUD,NO_DAD>
        groups: tun
        Opened by PID 1734
```

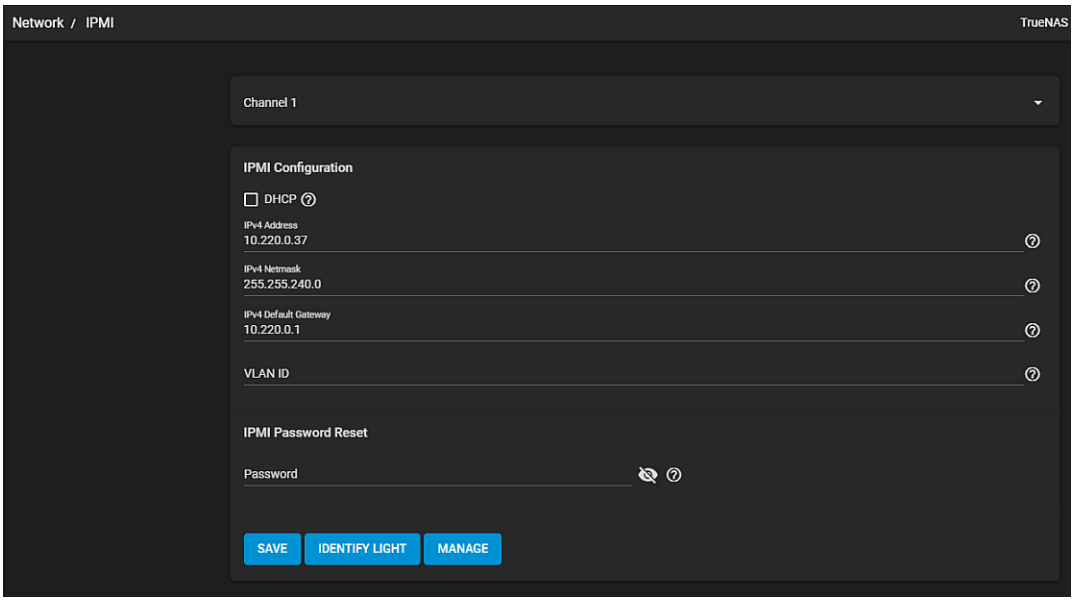
IPMI

> IPMI requires compatible hardware! Refer to your hardware documentation. Hardware compatibility determines if the IPMI option displays in the TrueNAS web interface.

Many TrueNAS Storage Arrays provide a built-in out-of-band management port. If the system becomes unavailable through the web interface, you can use this port to provide side-band management. Use IPMI to perform several vital functions. These include checking the log, accessing the BIOS setup, and powering on the system. IPMI does not need physical access to the system. You can use it to allow another person remote access to the system. This is useful when investigating a configuration or troubleshooting issue.

> Some IPMI implementations need updates to work with newer versions of Java. See PSA: Java 8 Update 131 breaks ASRockвЂ™s IPMI Virtual console for more information.

Configure **IPMI** by going to **Network > IPMI**. The IPMI configuration screen provides a shortcut to the most basic IPMI configuration.



IPMI Configuration

Use the **Network > IPMI** screen to configure IPMI settings. See IPMI Screen for more information on IPMI settings.

Click **SAVE** to save the IPMI settings.

Connecting to the IPMI

Save the configuration. Access the IPMI interface using a web browser and the IP address specified in **Network > IPMI**. The management interface prompts for login credentials. Refer to your IPMI device documentation to learn the default administrator account credentials.

Log in to the management interface. Here you can change the default administrative user name and create extra IPMI users. The appearance of the IPMI utility and the functions that are available vary by hardware.

Storage

Pools

TrueNAS uses ZFS data storage *pools* to efficiently store and protect data.

▼ What is a pool?

Storage *pools* are attached drives organized into virtual devices (vdevs). Drives are arranged inside vdevs to provide varying amounts of redundancy and performance. This allows for high performance pools, pools that maximize data lifetime, and all situations in between.

ZFS and TrueNAS periodically reviews and heals whenever a bad block is discovered in a pool.

Review Storage Needs

We strongly recommend that you review the available system resources and plan the storage use case before creating a storage pool. Review when:

- Storing critical information. More drives allocated to the pool increases redundancy.
- Maximizing total available storage at the expense of redundancy or performance means allocating large volume disks and configuring the pool for minimal redundancy.
- Maximizing pool performance means installing and allocating high-speed SSD drives to the pool.

Determining your specific storage requirements is a critical step before creating a pool.

You can use the ZFS Capacity Calculator and ZFS Capacity Graph to compare configuration options.

Creating a Pool

To create a new pool, go to **Storage > Pools** and click **ADD**. The **Create or Import Pool** screen of the pool creation screens opens. Select **Create new pool** and click **CREATE POOL** to open the **Pool Manager**.

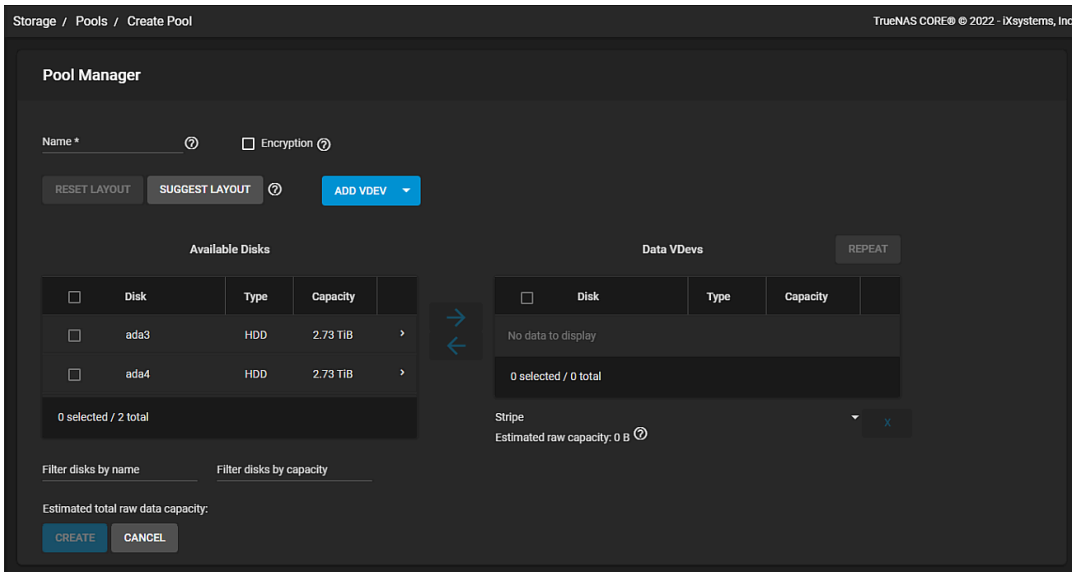


Figure 1: Create Pool Manager

To begin, enter a name for the pool in **Name**. Do not include spaces in the pool name as this could cause problems with other functions.

▼ Encryption?

Encryption algorithms are available as an option for maximizing data security, however, this also complicates how data is retrieved and risks permanent data loss! Refer to the Encryption article for more details and decide if encryption is necessary for your use case before setting any encryption options.

Next, configure the virtual devices (vdevs) that make up the pool.

Using Suggest Layout

Clicking **SUGGEST LAYOUT** allows TrueNAS to review all available disks and populate the primary data vdevs with identically sized drives in a balanced configuration between storage capacity and data redundancy. To clear the suggestion, click **RESET LAYOUT**.

To manually configure the pool, add vdevs according to your use case. Select the **Disk** checkboxes and click the →B to move the disks into the **Data VDevs** list.

> USB-connected disks might report their serial numbers inaccurately, making them indistinguishable from each other.

Using Vdev Types

Pools have many different kinds of vdevs available. These store data or enable unique features for the pool:

▼ Data

Standard vdev for primary storage operations. Each storage pool requires at least one data vdev. **Data** vdev configuration typically affects how the other kinds of vdevs are configured.

Duplicating a Data VDev

A **Data VDev** with disks is duplicated by clicking **REPEAT**. When more disks are available and equal in size, the **REPEAT** button creates another vdev with an identical configuration called a *mirror* of vdevs.

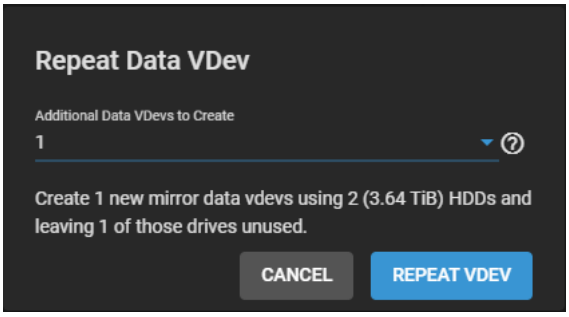


Figure 2: Duplicating a Data VDev

When even more same-size disks are available, you can create multiple copies of the original vdev.

> Do not have multiple data vdevs with different numbers of disks in each vdev as this complicates and limits the pool capabilities.

▼ Cache

ZFS L2ARC read-cache is used with fast devices to accelerate read operations. You can add or remove this after creating the pool.

▼ Log

ZFS LOG is a device that improves synchronous write speeds. You can add or remove this after creating the pool.

▼ Hot Spare

A hot spare vdev sets up drives as reserved to prevent larger pool and data loss scenarios TrueNAS automatically inserts an available hot spare into a data vdev when an active drive fails. The pool resilvers once the hot spare is activated.

Click **Detach** to remove the failed drive from the pool The activated hot spare is promoted to a full data vdev member and is no longer available as a hot spare. After physically replacing the failed disc, create a new hot spare vdev to reserve the replacement disc.

Alternately, after physically replacing the failed disc, click **Replace** on the failed drive to activate the new drive The hot spare reverts to an inactive state and is available again as a hot spare. We do not recommend this method, because it causes two resilver events: one when activating the hot spare and again when replacing the failed disk. Resilvering degrades system performance until completed and causes unnecessary strain on the disk.

▼ Metadata

Metadata vdevs are a special allocation class used to create Fusion Pools for increased metadata and small block I/O performance.

▼ Dedup

Dedup vdevs store ZFS de-duplication. Requires allocating *X* GiB for every *X* TiB of general storage. For example, 1 GiB of dedup vdev capacity for every 1 TiB of data vdev availability.

To add a different vdev type during pool creation, click **ADD VDEV** and select the type. Select disks from **Available Disks** and use the ➔B (right arrow) next to the new **VDev** to add it to that section.

Vdev Layout

Disks added to a vdev arrange in different layouts, according to the specific pool use case.

▼ Can I create vdevs with different layouts in one pool?

Adding multiple vdevs with different layouts to a pool is not supported. Create a new pool when a different vdev layout is required. For example, *pool1* has a data vdev in a *mirror* layout, so create *pool2* for any *raid-z* vdevs.

▼ Stripe

Each disk is used to store data. Requires at least one disk and has no data redundancy.

> Never use a stripe type vdev to store critical data! A single disk failure results in losing all data in the vdev.

▼ Mirror

Data is identical in each disk. Requires at least two disks, has the most redundancy, and the least capacity.

▼ RAIDZ1

Uses one disk for parity while all other disks store data. Requires at least three disks.

▼ RAIDZ2

Uses two disks for parity while all other disks store data. Requires at least four disks.

▼ RAIDZ3

Uses three disks for parity while all other disks store data. Requires at least five disks.

The **Pool Manager** suggests a vdev layout from the number of disks added to the vdev. For example, if adding two disks, TrueNAS automatically configures the vdev as a mirror, where the total available storage is the size of one added disk while the other disk provides redundancy.

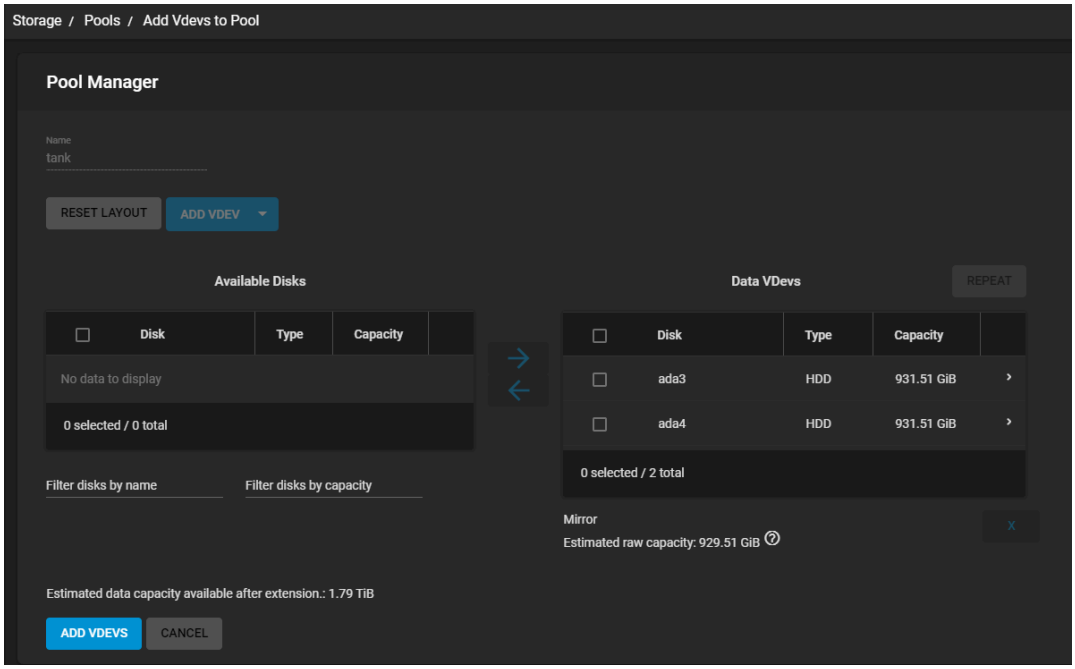


Figure 3: Mirrored Vdev

To change the vdev layout, open the **Data VDevs** list and select the desired layout.

Importing Pools

> This procedure only applies to disks with a ZFS storage pool. To import disks with different file systems, see Import Disk.

ZFS pool importing works for pools that were exported or disconnected from the current system, created on another system, and pools to reconnect after reinstalling or upgrading the TrueNAS system. To import a pool, go to **Storage > Pools > ADD**.

▼ Do I need to do anything different with disks installed on a different system?

When physically installing ZFS pool disks from another system, use the command `zpool export poolname` in the command line or a web interface equivalent to export the pool on that system. Shut that system down and move the drives to the TrueNAS system. Shutting down the original system prevents an *in use by another machine* error during the TrueNAS import.

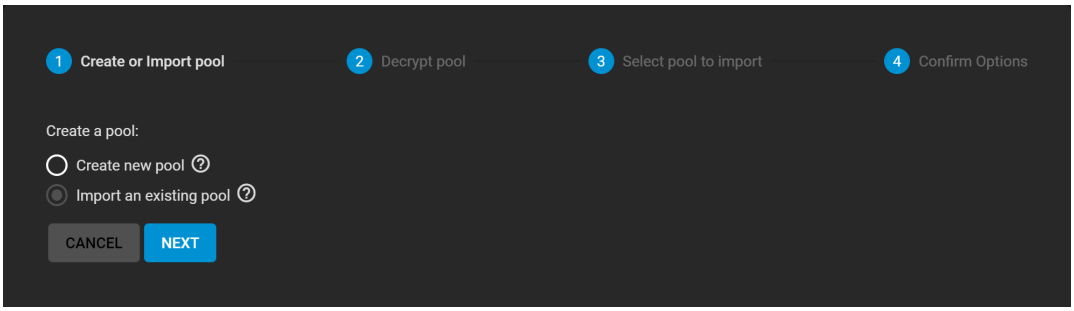
There are two kinds of pool imports, standard ZFS pool imports and ZFS pools with legacy GELI encryption.

Pool Import Options

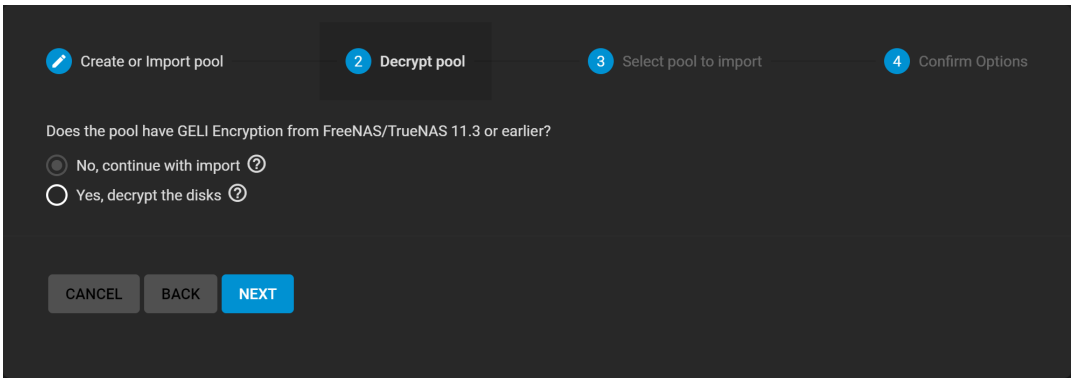
▼ Standard ZFS Pool

Standard ZFS Pools

Select **Import Existing Pool** and click **NEXT**.

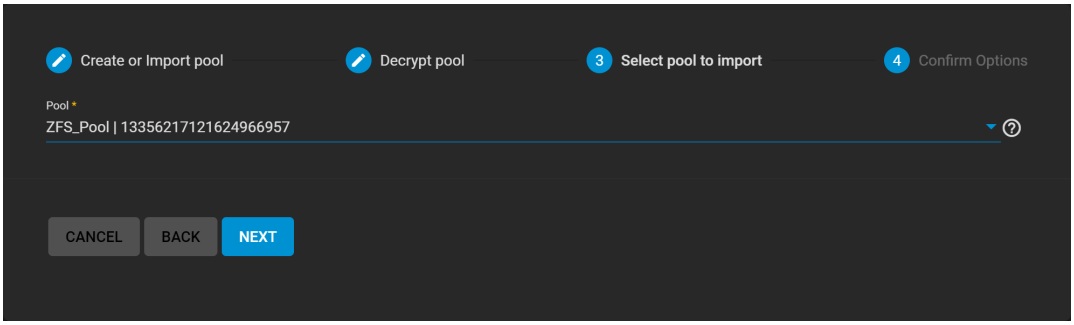


The wizard asks if the pool has legacy GELI encryption.



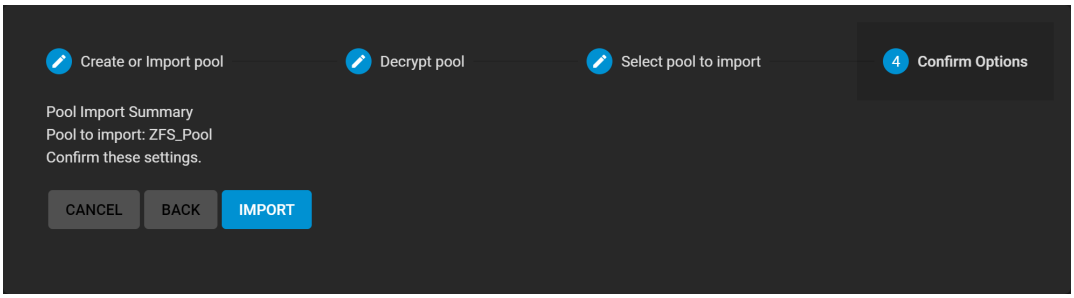
Select **No, continue with import** and click **NEXT**.

TrueNAS detects any pools that are present but unconnected.



Choose the ZFS pool to import and click **NEXT**.

Review the Pool Import Summary and click **IMPORT**.

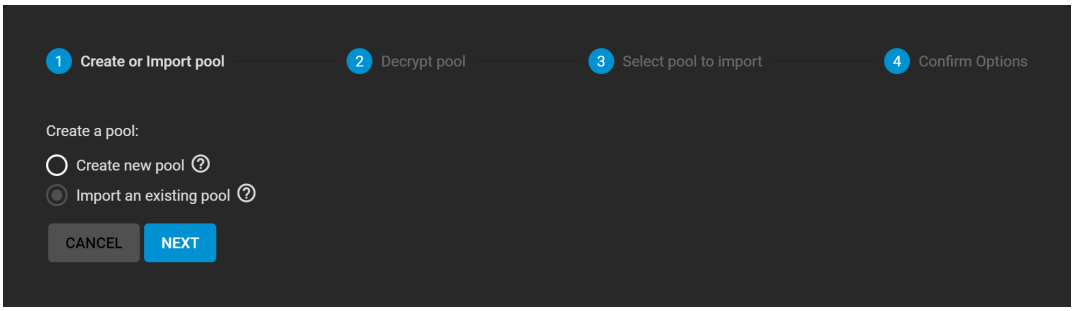


▼ ZFS Pool with GELI

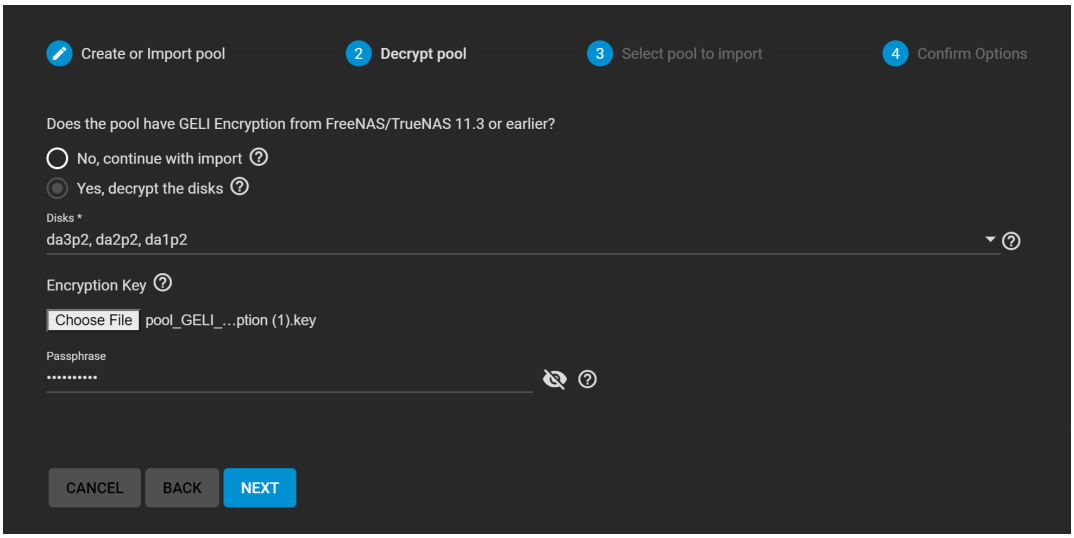
Encrypted GELI Pools

> Importing a GELI-encrypted pool requires using the encryption key file and passphrase to decrypt the pool *before* importing. When a pool cannot be decrypted, it cannot be re-imported after a failed upgrade or lost configuration, and the data is *irretrievable*! Always have a copy of the pool GELI key file and passphrase available.

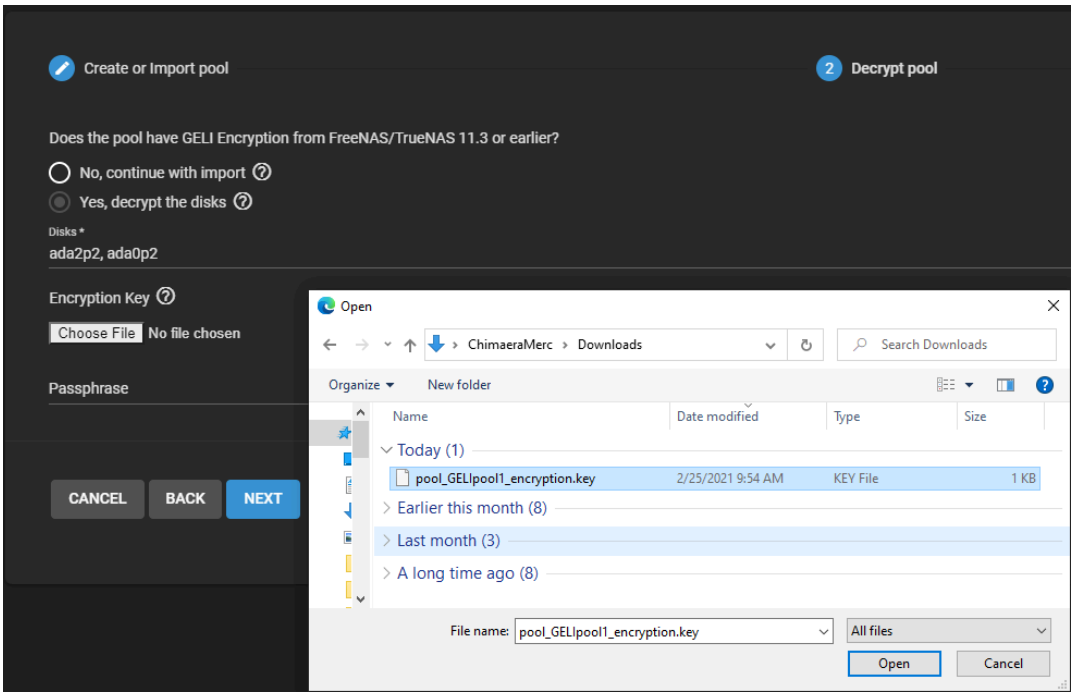
Select **Import Existing Pool** and click **NEXT**.



The wizard asks if the pool has legacy GELI encryption. Select **Yes, decrypt the disks** and review the decryption options.

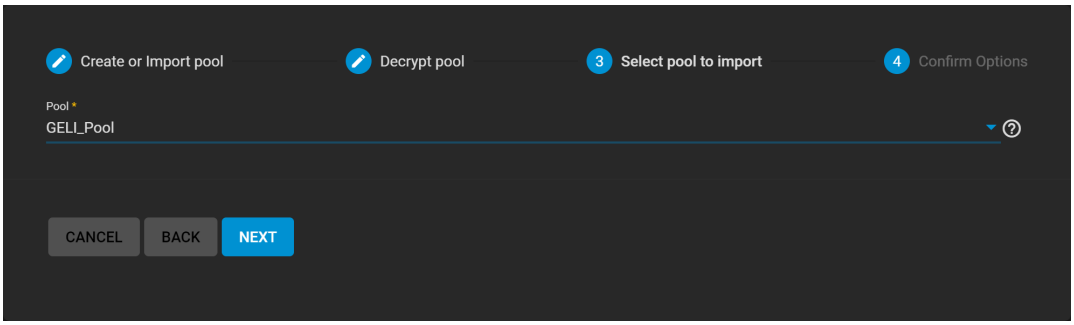


Make sure the **Disks** selection shows the encrypted disks and partitions that are part of the incoming pool. Apply the GELI encryption key file by clicking **Choose File** and uploading the file from your local system.

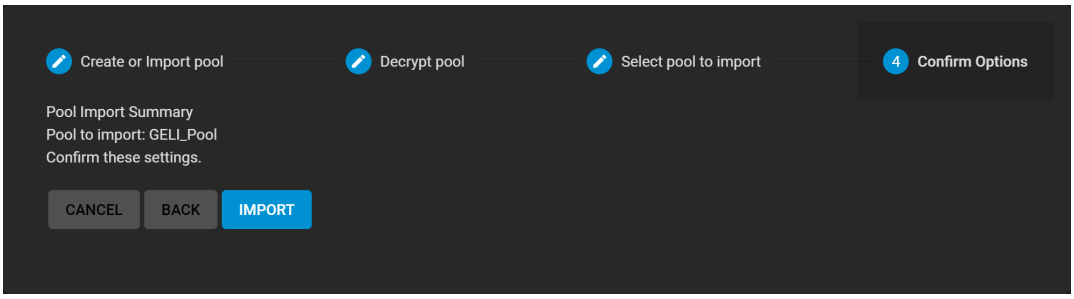


When a passphrase is also present, enter it in **Passphrase**. Click **Next** and wait for the disks to decrypt.

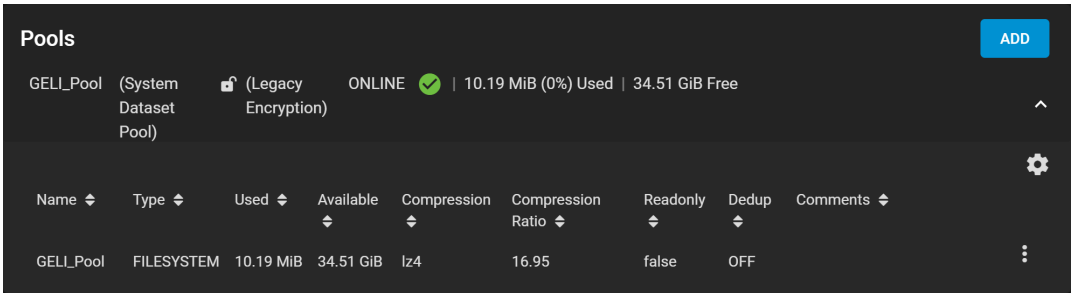
When the disks are decrypted, select the GELI pool to import.



Review the **Pool Import Summary** and click **IMPORT**.



GELI encrypted pools show in **Storage > Pools** as **(Legacy Encryption)**.



Back Up the Pool Key

For security reasons, encrypted pool keys do not save to a configuration backup file. When TrueNAS is installed to a new device and restored with a saved configuration file, keys for encrypted disks are not present and the system does not request them.

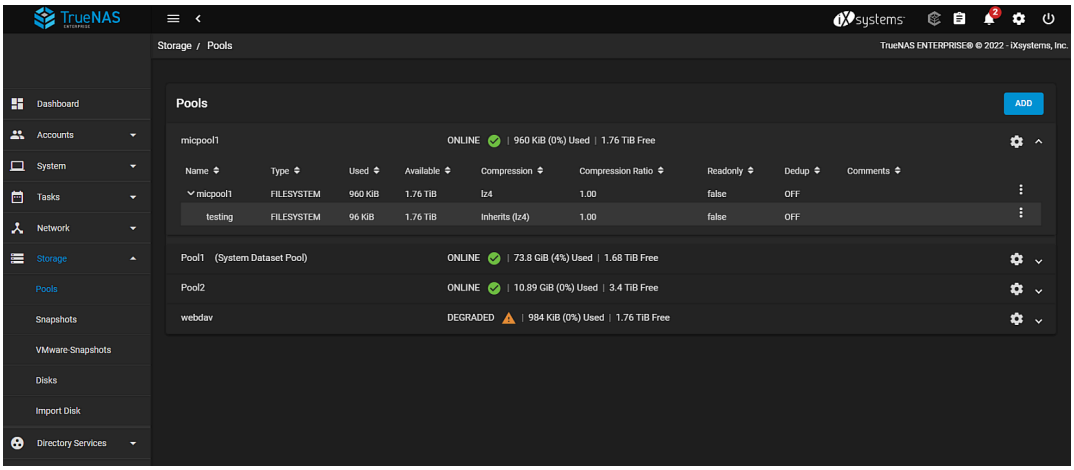
To correct this, export the encrypted pool in **Storage > Pools** with ⚙ > **Export/Disconnect**.

> Do *not* select **Destroy data on this pool?**.

Now import the pool again. During the import, add the encryption keys as described previously.

Managing Pools

After creating a data storage pool, there are a variety of options to change the initial configuration of that pool. Changing a pool can be disruptive, so make sure you are aware of existing resources on the system and consider backing up any stored data before changing the pool. To find an existing pool, log in to the web interface and go to **Storage > Pools**.

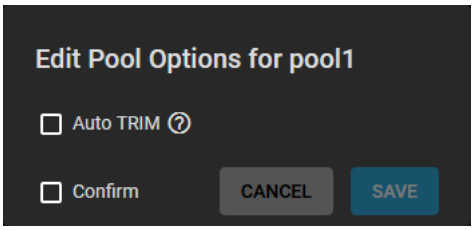


The current status and storage usage of each pool is shown. To see more details about a pool, click the expand_more expand symbol on the right side of the pool entry. Click the for all pool management options.

Pool Actions

▼ Pool Options

Contains any additional high-level settings for the pool.

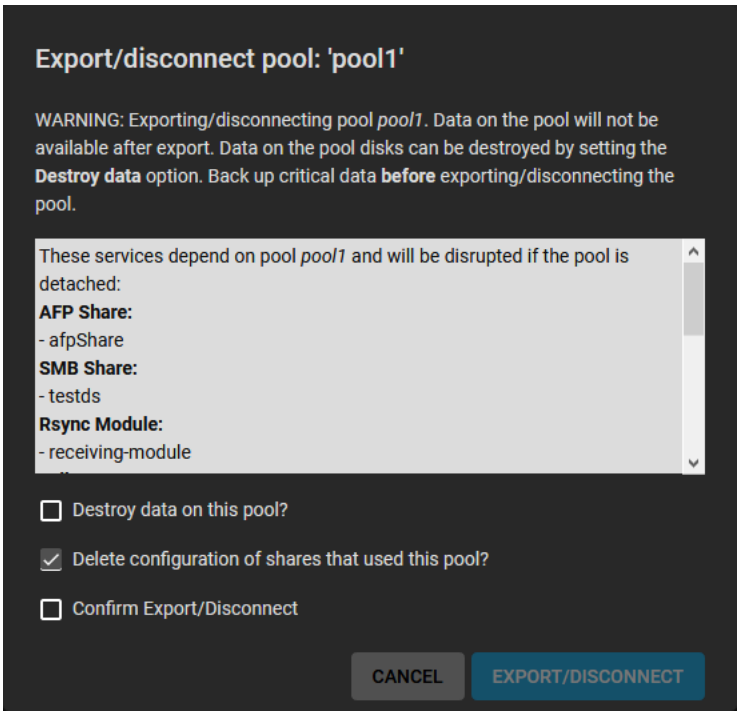


Auto TRIM allows TrueNAS to periodically check the pool disks for storage blocks that can be reclaimed. This can have a performance impact on the pool, so the option is disabled by default. For more details about TRIM in ZFS, see the `autotrim` property description in zpool.8.

▼ Export/Disconnect

Removes the pool from the system.

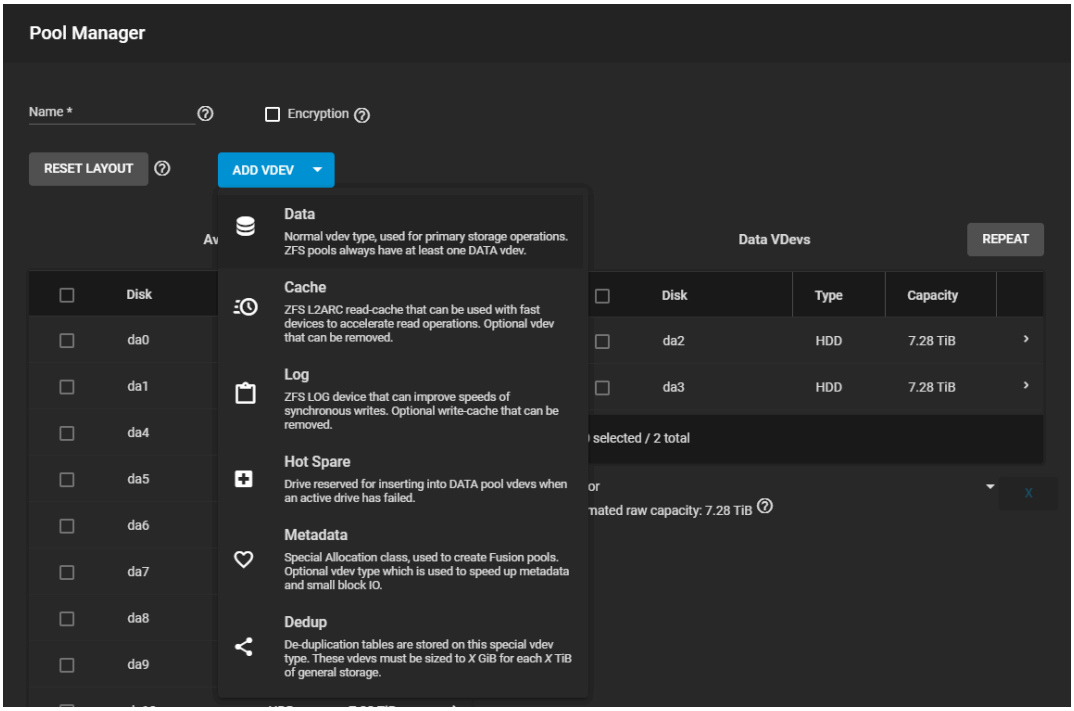
Use to prepare drives for transfer to a new system and import the pool or completely delete the pool and any data stored on it. A dialog warns about the risks of disconnecting the pool and shows any system services that are affected by removing the pool.



Because this is a destructive action, you must select additional checkboxes and enter the name of the pool when also deleting stored data. You can also remove existing shares to this data when the pool is disconnected.

▼ Add Vdevs

Opens the **Pool Manager** to add more vdevs to the pool. Changing the original encryption and data vdev configuration is not allowed.



A new data vdev is chosen by default.

To add different kinds of vdevs to the pool, click **ADD VDEV** and select the type from the dropdown list.

When adding disks to increase the capacity of a pool, ZFS supports the addition of virtual devices, or vdevs, to an existing ZFS pool.

After a vdev is created, more drives cannot be added to that vdev, but a new vdev can be striped with another of the same type to increase the overall size of the pool. To extend a pool, the vdev added must be the same type as existing vdevs.

Some vdev extending examples:

- Extend a ZFS mirror: Add the same number of drives. The result is a striped mirror. For example, if ten new drives are available, a mirror of two drives can be created initially, then extended by adding another mirror of two drives, and repeating three more times until all ten drives are added.
- Extend a three-drive RAIDZ1: Add another three drives. The resulting pool is a stripe of two RAIDZ1 vdevs, similar to RAID 50 on a hardware controller.
- Extend a four-drive RAIDZ2: Add another four drives. The result is a stripe of RAIDZ2 vdevs, similar to RAID 60 on a hardware controller.

- Add a disk as a *hot spare* to the pool.

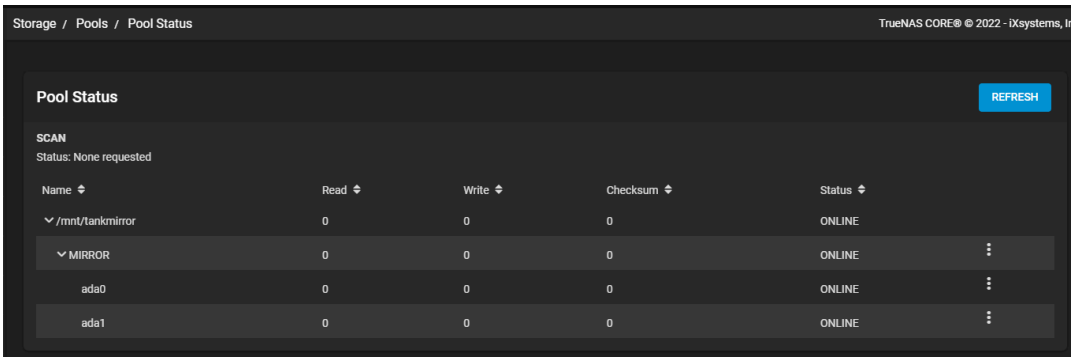
▼ Scrub Pool

Initiate a data integrity check of the pool.

Any problems detected during the scrub are either automatically corrected or generate an alert in the web interface. By default, every pool is automatically checked on a reoccurring scrub schedule.

▼ Status

Opens the **Pool Status** screen to show the state of the last scrub and disks in the pool.



Additional options for managing connected disks are available in this screen.

▼ Expand Pool

Increases the size of the pool to match all available disk space. This option is typically used when virtual disks are resized apart from TrueNAS.

▼ Upgrade Pool

This option only displays when the pool can be upgraded to use new ZFS feature flags. Before upgrading an existing pool, be aware of these caveats:

- Upgrading a pool is one-way. This means that if you change your mind. You cannot go back to an earlier ZFS version or downgrade to an earlier version of the software that does not support those ZFS features.
- Upgrading can affect data. Before performing any operation that can affect the data on a storage disk, always back up all data first and verify the integrity of the backup. While it is unlikely that the pool upgrade affects the data, it is always better to be safe than sorry.
- Upgrading a ZFS pool is optional. Do not upgrade the pool if the possibility of reverting to an earlier version of TrueNAS or repurposing the disks in another operating system that supports ZFS is desired. It is not necessary to upgrade the pool unless the end user has a specific need for the newer ZFS Feature Flags. If you upgrade a pool to the latest feature flags, you cannot import that pool into another operating system that does not yet support those feature flags.

The upgrade itself only takes a few seconds and is non-disruptive. It is not necessary to stop any sharing services to upgrade the pool. However, it is best to upgrade when the pool is not in heavy use. The upgrade process suspends I/O for a short period, but is nearly instantaneous on a quiet pool.

Creating Datasets

A TrueNAS dataset is a file system that is created within a data storage pool. Datasets can contain files, directories (child datasets), and have individual permissions or flags. Datasets can also be encrypted, either using the encryption created with the pool or with a separate encryption configuration.

It is recommended to organize your pool with datasets before configuring data sharing, as this allows for more fine-tuning of access permissions and using different sharing protocols.

Creating a Dataset

To create a dataset in the desired pool, go to **Storage > Pools**.

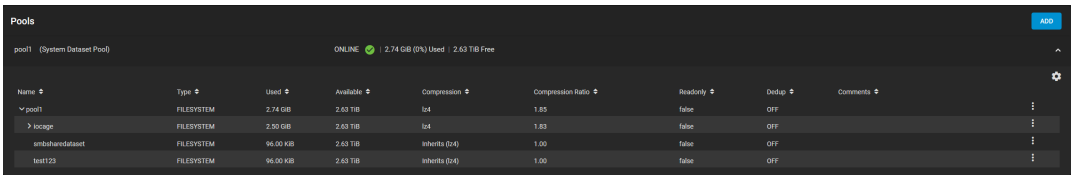


Figure 1: Pools list with one example

Find the pool and top-level (root) dataset for that pool, then click ⋮ and **Add Dataset**.

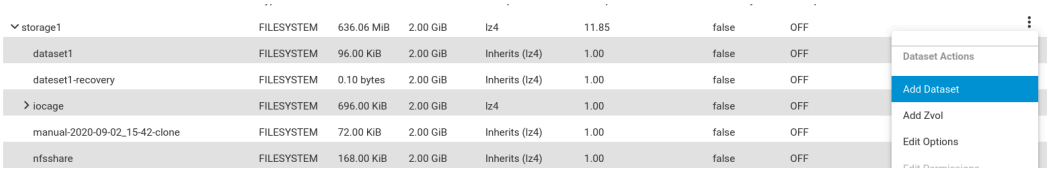


Figure 2: Add Dataset

To quickly create a dataset with the default options, enter a name for the dataset and click **SUBMIT**.

Dataset Options

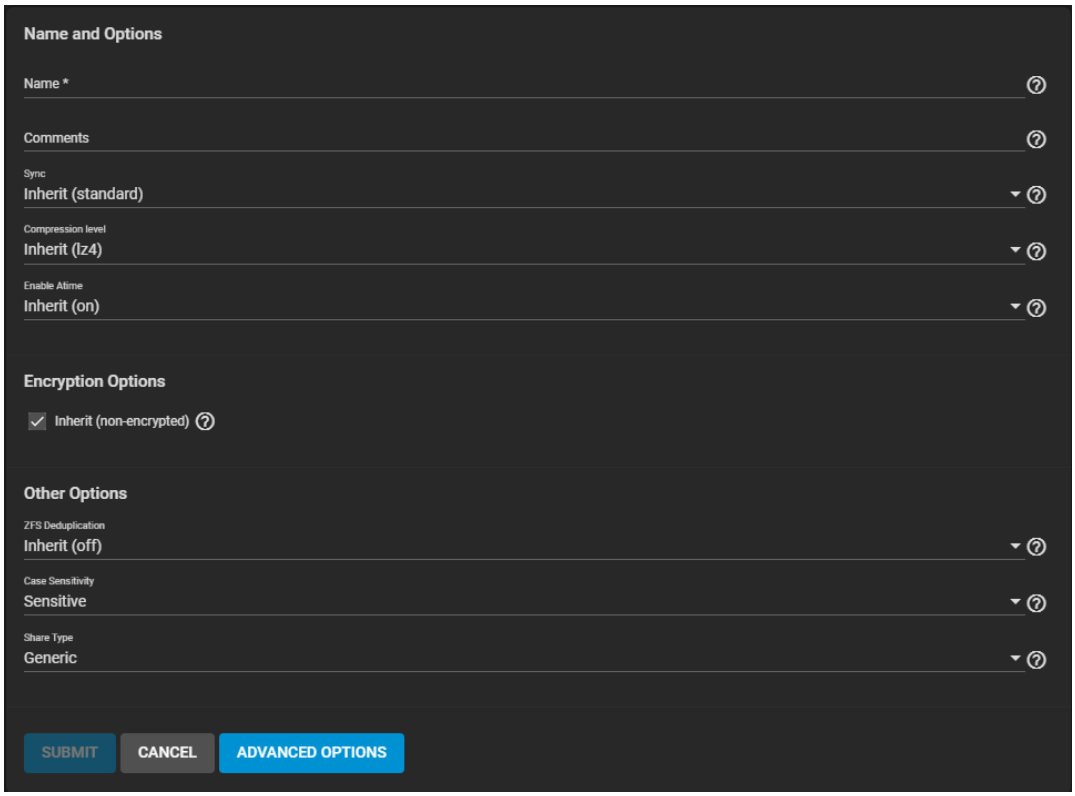


Figure 3: Basic Options

The **Name and Options** fields is required to create the dataset. Datasets typically inherit most of these settings from the root or parent dataset, only a dataset name is required before clicking **SUBMIT**.

See Dataset Screens for more information on basic and advanced settings.

For the **Sync** option, we recommend production systems with critical data use the default **Standard** choice or increase to **Always**. Choosing **Disabled** is only suitable in situations where data loss from system crash or power loss is acceptable.

By default, datasets inherit the **Encryption Options** from the root or parent dataset. To configure the dataset with different encryption settings, clear the checkmark from **Inherit** and choose the new in **Encryption Options**. For detailed descriptions of

the encryption options, see the Encryption article.

Clicking **ADVANCED OPTIONS** adds dataset quota management tools and a few additional fields to the **Other Options**:

Managing Datasets

After a dataset is created, additional management options are available by going to **Storage > Pools** and clicking ⋮ for a dataset:

- **Add Dataset**: create a new dataset that is a child of this dataset. Datasets can be continuously layered in this manner.
- **Add Zvol**: create a new ZFS block device as a child of this dataset.
- **Edit Options**: opens the dataset options to make adjustments to the dataset configuration. The dataset **Name**, **Case Sensitivity**, and **Share Type** cannot be changed.
- **Edit Permissions**: opens the editor to set access permissions for this dataset. Depending on the dataset creation options, this can be a simple permissions editor or the full ACL editor. For more information about editing permissions, read the permissions article.
- **User Quotas**: shows options to set data or object quotas for user accounts cached on the system or user accounts that are connected to this system.
- **Group Quotas**: shows options to set data or object quotas for user groups cached on the system or user groups that are connected to this system.
- **Delete Dataset**: removes the dataset, all stored data, and any snapshots of the dataset from TrueNAS.

> Deleting datasets can result in unrecoverable data loss! Be sure that any critical data is moved off the dataset or is otherwise obsolete.

- **Create Snapshot**: take a single ZFS snapshot of the dataset to provide additional data protection and mobility. Created snapshots are listed in **Storage > Snapshots**.

Quotas

TrueNAS allows setting data or object quotas for user accounts and groups cached on or connected to the system.

Setting a quota defines the maximum allowed space for the dataset. You can also reserve a defined amount of pool space for the dataset to help prevent situations where automatically generated data like system logs consume all space on the dataset. Quotas can be configured for either the new dataset or to include all child datasets in the quota.

Dataset Screens for more information on quota settings.

Quota Types

User Qutoas

To view and edit user quotas, go to **Storage > Pools** and click ⋮ to open the **Dataset Actions** menu, and then click **User Quotas**.

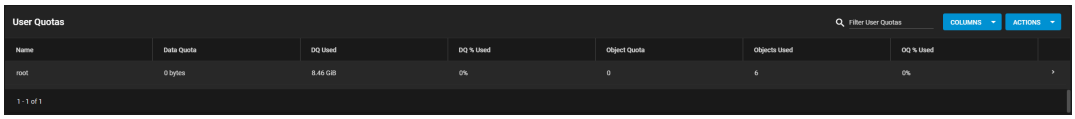


Figure 4: User Quotas List

The **User Quotas** page displays the names and quota data of any user accounts cached on or connected to the system.

To edit individual user quotas, go to the user row and click the ⋮ button, then click ✎.

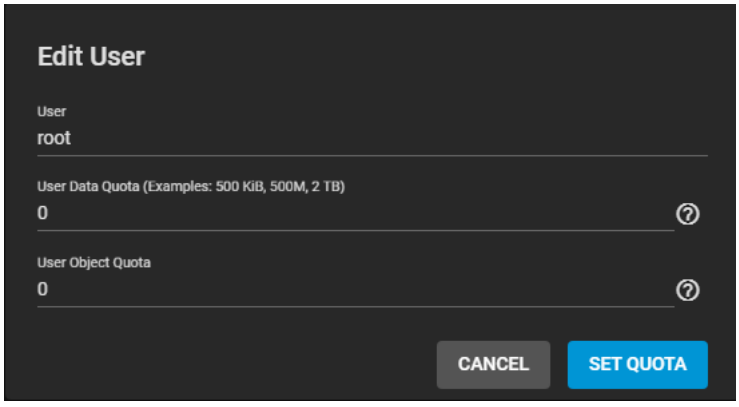


Figure 5: Editing a Single User

The **Edit User** window allows editing the **User Data Quota**, which is the amount of disk space that can be used by the selected users, and the **User Object Quota**, which is the number of objects that can be owned by each of the selected users.

To edit user quotas in bulk, click **Actions** and select **Set Quotas (Bulk)**.

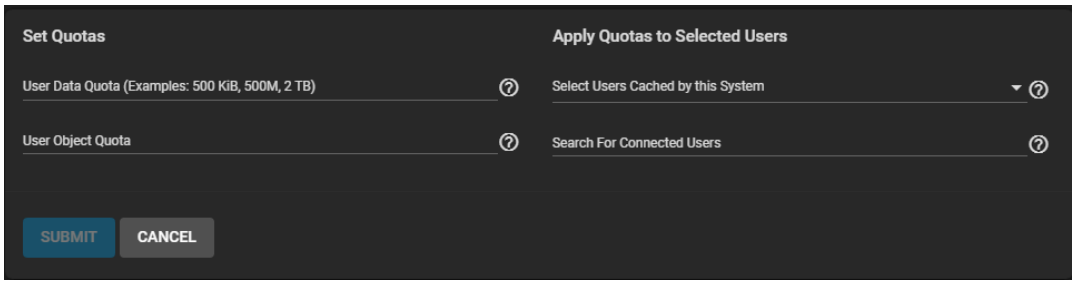


Figure 6: Bulk Edits

The **Set Quotas** window allows editing user data and object quotas after selecting any cached or connected users.

Group Quotas

Go to **Storage > Pools** and click ⋮ to open the **Dataset Actions** menu. Click **Group Quotas**.

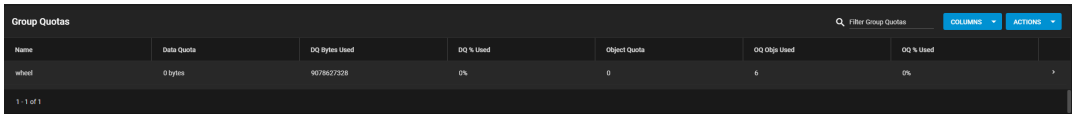


Figure 7: Group Quotas List

The **Group Quotas** page displays the names and quota data of any groups cached on or connected to the system.

To edit individual group quotas, go to the group row and click the **>** button, then click ✎.

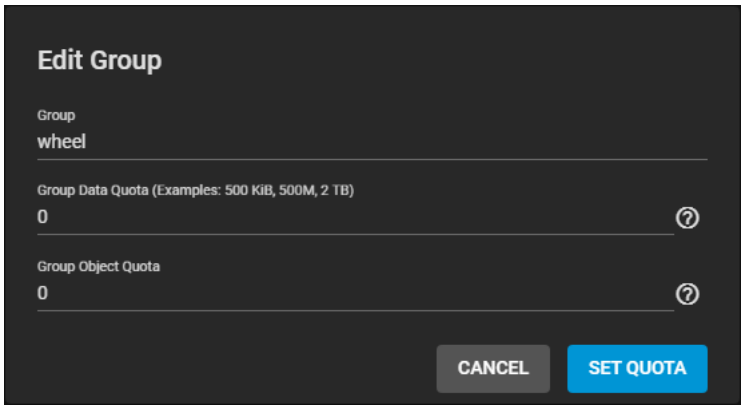


Figure 8: Edit a Single Group

The **Edit Group** window allows editing the **Group Data Quota** and **Group Object Quota**.

To edit group quotas in bulk, click **Actions** and select **Set Quotas (Bulk)**.

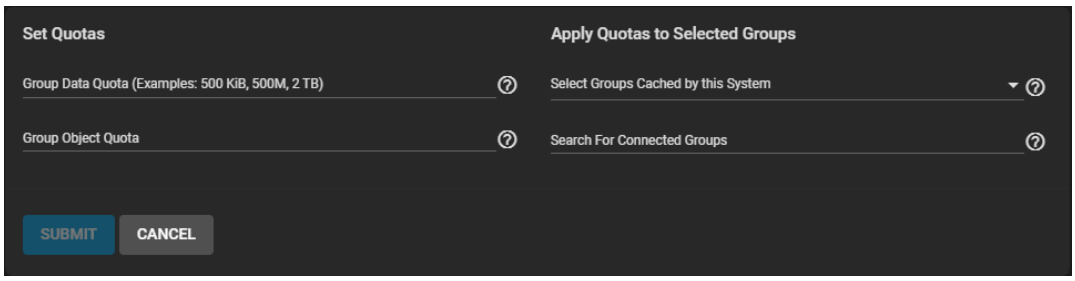


Figure 9: Bulk Edit

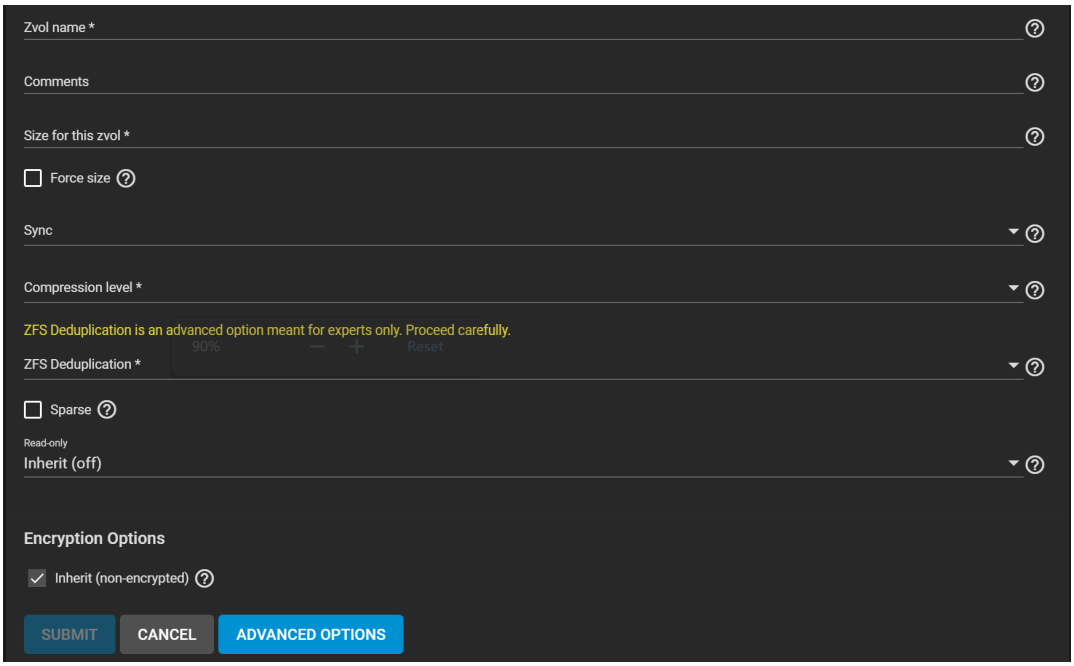
The same options for single groups are presented, along with choosing groups for these new quota rules.

Adding Zvols

A ZFS Volume (Zvol) is a dataset that represents a block device. These are needed when configuring an iSCSI Share.

To create a zvol in a pool, go to **Storage > Pools** then click ⋮ and *Add Zvol*.

Options



To quickly create a Zvol with the default options, enter a name for the Zvol, a size, and click **SAVE**.

See Zvols Screen for more information on zvol settings.

Setting Zvol Block Sizes

To set the zvol block size, click **ADVANCED OPTIONS** on the **ADD ZVOL** screen. This adds the **Block Size** setting near the bottom of the screen. Select that option that suits the use case or uses the information below to help determine the correct setting to use.

▼ Optimal Zvol Block Sizes

TrueNAS automatically recommends a space-efficient block size for new zvols. This table shows the minimum recommended volume block size values. To manually change this value, use the **Block size** dropdown list.

Configuration	Number of Drives	Optimal Block Size
Mirror	N/A	16k
Raidz-1	3	16k
Raidz-1	4/5	32k
Raidz-1	6/7/8/9	64k
Raidz-1	10+	128k
Raidz-2	4	16k
Raidz-2	5/6	32k
Raidz-2	7/8/9/10	64k
Raidz-2	11+	128k
Raidz-3	5	16k
Raidz-3	6/7	32k
Raidz-3	8/9/10/11	64k
Raidz-3	12+	128k

Additional tuning might be required for optimal performance, depending on the workload. iXsystems engineers are available to assist Enterprise customers with tuning their TrueNAS hardware. The workload tuning chapter of the OpenZFS handbook is

also a good resource.

Managing Zvols

To see options for an existing zvol, click ⋮ next to the desired zvol in **Storage** > **Pools**:

Use **Delete zvol** to remove the zvol from TrueNAS.

> Deleting zvols can result in unrecoverable data loss! Be sure that any critical data is moved off the zvol or is otherwise obsolete.

Deleting a zvol also deletes all snapshots of that zvol. Use **Edit Zvol** to open the zvol creation form to change the previously saved settings. Similar to datasets, a zvol name cannot be changed. Use **Create Snapshot** to take a single current-point-in-time image of the zvol and save it to **Storage > Snapshots**. A snapshot name is suggested in **Name** along with an extra option to make the snapshot **Recursive** is available.

When the selected zvol is cloned from an existing snapshot, **Promote Dataset** is available. When a clone is promoted, the original volume becomes a clone of the clone, making it possible to delete the volume that the clone was created from. Otherwise, a clone cannot be deleted while the original volume exists.

When the zvol is created with encryption enabled, additional **Encryption Actions** are displayed.

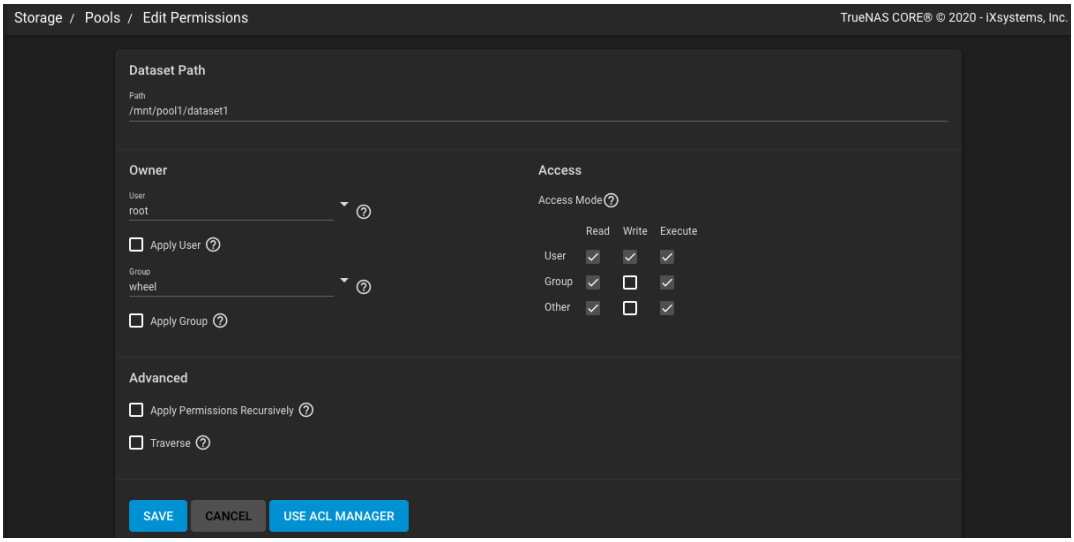
Permissions

Permissions control the actions users can perform on dataset contents. TrueNAS allows using both a simple permissions manager and editing a full Access Control List (ACL) for defining dataset permissions.

To change dataset permissions, go to **Storage > Pools >** ⋮ **Edit Permissions** for a dataset.

Basic Permissions Editor

The **Edit Permissions** option allows basic adjustments to a datasets ACL.



Options

The **Owner** section controls which TrueNAS user and group has full control of this dataset.

Access Mode defines the basic read, write, and execute permissions for the user, group, and other accounts that might access this dataset.

Advanced has several tuning options to set how permissions apply to directories and files within the current dataset.

To switch from the basic editor to the advanced ACL editor, click **USE ACL MANAGER**.

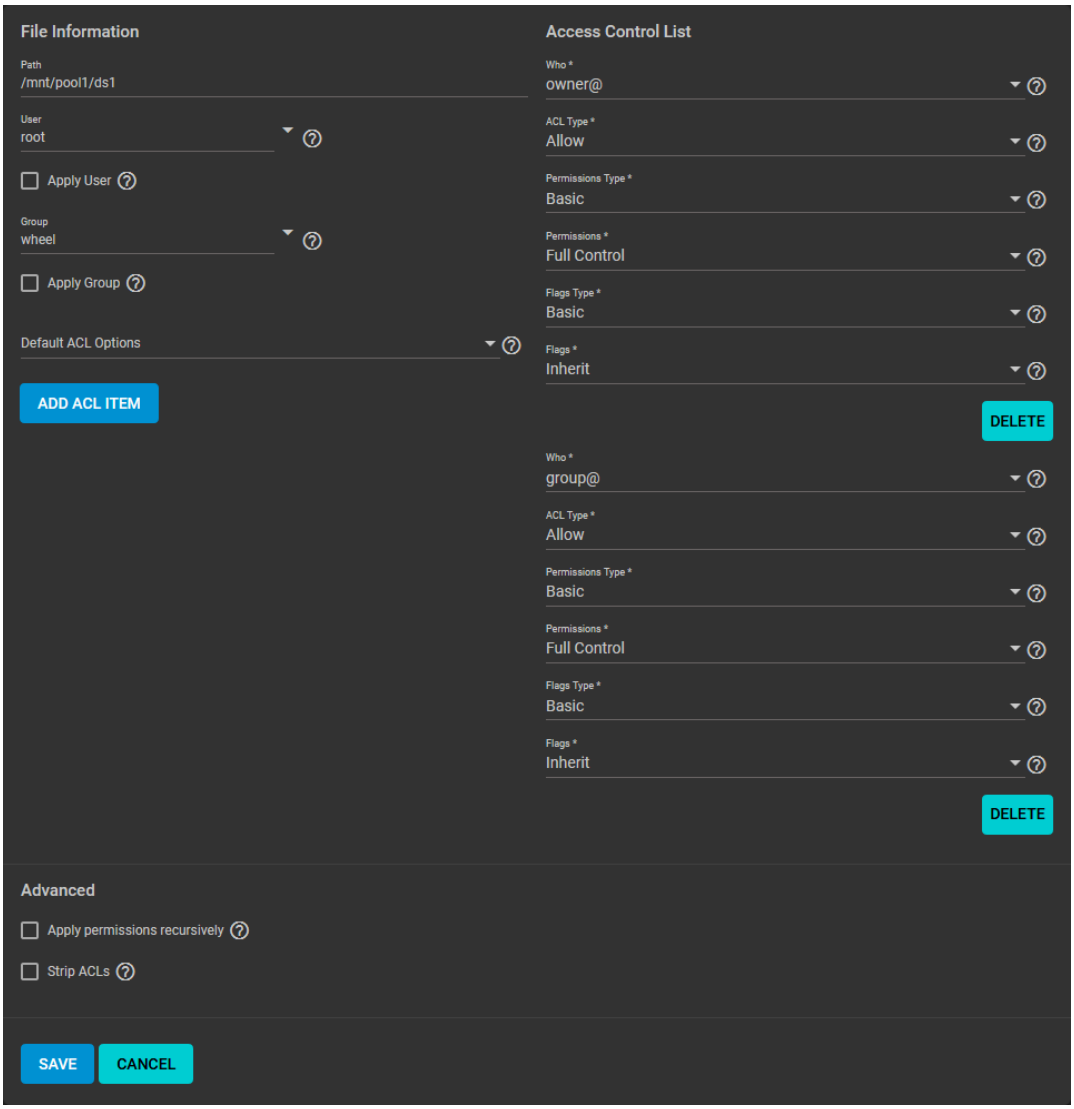
Access Control Lists

An Access Control List (ACL) is a set of account permissions associated with a dataset and applied to directories or files within that dataset. ACLs are typically used to manage user interactions with shared datasets and are created when a dataset is added to a pool.

When creating a dataset, you can choose how the ACL can be modified by selecting an **ACL Mode**:

- **Passthrough** only updates ACL entries (ACEs) that are related to the file or directory mode.
- **Restricted** does not allow `chmod` to make changes to files or directories with a non-trivial ACL. An ACL is trivial if it can be fully expressed as a file mode without losing any access rules. Setting the **ACL Mode** to **Restricted** is typically used to optimize a dataset for SMB sharing, but can require further optimizations. For example, configuring an rsync task with this dataset could require adding `--no-perms` as an extra option for the task.

To view an ACL, go to **Storage > Pools >** ⋮ **Edit Permissions** for a nested dataset within a pool.



▼ Tutorial Video

ACL Inheritance

The ACL for a new file or directory is typically inherited from the parent directory and is preserved when it is moved or renamed within the same dataset. An exception is when there are no **File Inherit** or **Directory Inherit** flags in the parent ACL **owner@**, **group@**, or **everyone@** entries. These non-inheriting entries are added to the ACL of the newly created file or directory based on the Samba create and directory masks or the umask value.

Editing an ACL

Click **ACL Manager** to adjust file ownership or account permissions to the dataset. The first time viewing the ACL Manager a dialog suggests using basic presets. The ACL can be edited at any time after choosing to either apply a preset or create a custom ACL.

Choose **Select a preset ACL** and choose a preset. The preset options are **OPEN**, **RESTRICTED**, or **HOME**.

Choose **Create a custom ACL** to create a new list of customized permissions.

File Information

The selected **User** controls the dataset and always has permission to modify the ACL and other attributes. The selected **Group** also controls the dataset, but permissions change by adding or modifying a **group@** ACE. Any user accounts or groups imported from a directory service can be selected as the primary in **User** or **Group**.

Access Control List (ACEs)

To add a new item to the ACL, define **Who** the Access Control Entry (ACE) applies to, and configure permissions and inheritance flags for the ACE.

▼ ACL Details from Shell

To view an ACL information from the console, connect to a shell session and enter:

```
getfacl /mnt/path/to/dataset
```

Permissions

Permissions are divided between **Basic** and **Advanced** options. The basic options are commonly used groups of the advanced options.

Basic Permissions

- **Read** (`r-x---a-R-c---`): view file or directory contents, attributes, named attributes, and ACL. Includes the **Traverse** permission.
- **Modify** (`rwxpDdaARWc--s`): adjust file or directory contents, attributes, and named attributes. Create new files or subdirectories. Includes the **Traverse** permission. Changing the ACL contents or owner is not allowed.
- **Traverse** (`--x---a-R-c---`): Execute a file or move through a directory. Directory contents are restricted from view unless the **Read** permission is also applied. To traverse and view files in a directory, but not be able to open individual files, set the **Traverse** and **Read** permissions, then add the advanced **Directory Inherit** flag.
- **Full Control** (`rwxpDdaARWcCos`): Apply all permissions.

Advanced Permissions

- **Read Data** (`r`): View file contents or list directory contents.
- **Write Data** (`w`): Create new files or modify any part of a file.
- **Append Data** (`p`): Add new data to the end of a file.
- **Read Named Attributes** (`R`): view the named attributes directory.
- **Write Named Attributes** (`W`): create a named attribute directory. Must be paired with the Read Named Attributes permission.
- **Execute** (`x`): Execute a file, move through, or search a directory.
- **Delete Children** (`D`): delete files or subdirectories from inside a directory.
- **Read Attributes** (`a`): view file or directory non-ACL attributes.
- **Write Attributes** (`A`): change file or directory non-ACL attributes.
- **Delete** (`d`): remove the file or directory.
- **Read ACL** (`c`): view the ACL.
- **Write ACL*** (`C`): change the ACL and the ACL mode.
- **Write Owner** (`o`): change the user and group owners of the file or directory.
- **Synchronize** (`s`): synchronous file read/write with the server. This permission does not apply to FreeBSD clients.

Inheritance Flags

Basic inheritance flags only enable or disable ACE inheritance. Advanced flags offer finer control for applying an ACE to new files or directories.

Basic Flags

- **Inherit** (`fd-----`): enable ACE inheritance.
- **No Inherit** (`-------`): disable ACE inheritance.

Advanced Flags

- **File Inherit** (`f`): The ACE is inherited with subdirectories and files. It applies to new files.
- **Directory Inherit** (`d`): new subdirectories inherit the full ACE.
- **No Propagate Inherit** (`n`): The ACE can only be inherited once.
- **Inherit Only** (`i`): Remove the ACE from permission checks but allow it to be inherited by new files or subdirectories. Inherit Only is removed from these new objects.
- **Inherited** (`I`): set when the ACE has been inherited from another dataset.

Storage Encryption

TrueNAS supports different encryption options for critical data.

> Users are responsible for backing up and securing encryption keys and passphrases! Losing the ability to decrypt data is similar to a catastrophic data loss.

Data-at-rest encryption is available with:

- Self Encrypting Drives (SEDs) using OPAL or FIPS 140.2 (Both AES 256)
- Encryption of specific datasets (AES-256-GCM in TrueNAS 12.0)

The local TrueNAS system manages keys for data-at-rest. The user is responsible for storing and securing their keys.

▼ Encryption Drawbacks and Considerations

Always consider the following drawbacks/considerations when encrypting data:

- All datasets contained within an encrypted pool inherit encryption.
- If there is only one pool and it is encrypted, all datasets are also encrypted.
- If the encryption keys and passwords are lost, encrypted data is unrecoverable.

Unrelated encrypted datasets do not support deduplication.

We do not recommend using GELI or ZFS encryption with deduplication because of the sizable performance impact.

Be cautious when using many encryption and deduplication features at once since they all compete for the same CPU cycles.

Encrypting a Storage Pool

Encrypting the root dataset of a new storage pool further increases data security. All datasets added to a pool with encryption applied inherit encryption. This means all datasets added to a pool with encryption are also encrypted.

Create a new pool and set **Encryption** in the **Pool Manager**. TrueNAS shows a warning.

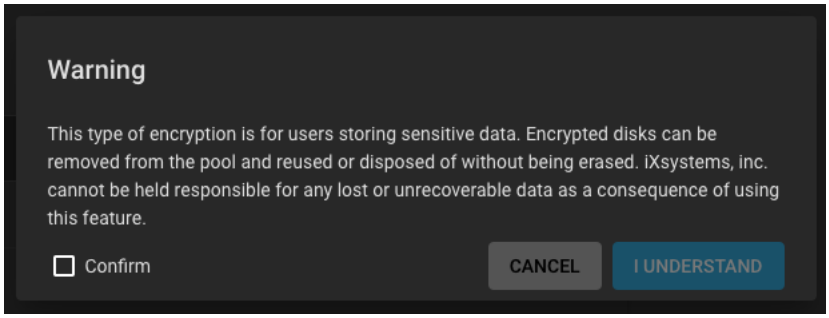


Figure 1: Storage Pools Add Encryption Warning

Read the warning, select **Confirm**, and click **I Understand**.

We recommend using the default encryption in **Cipher**, but other ciphers are available.

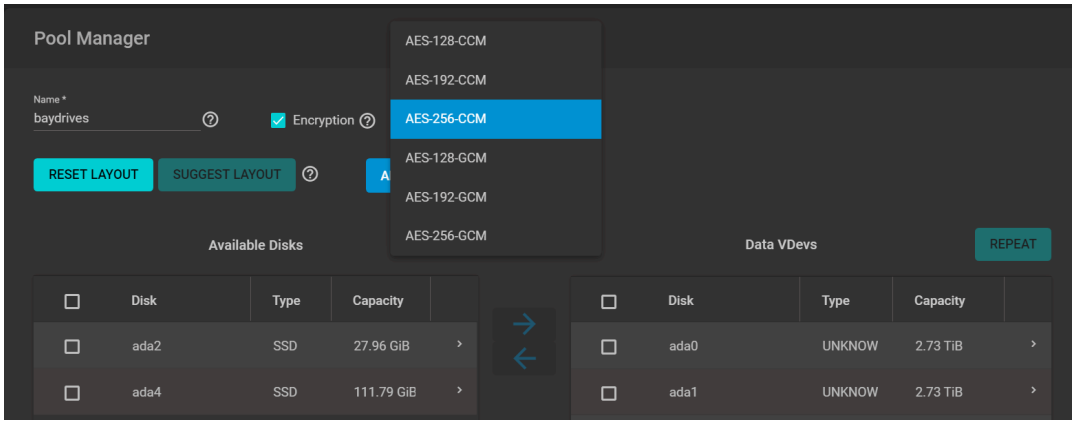


Figure 2: Choosing an encryption cipher

▼ What are these options?

TrueNAS supports AES Galois Counter Mode (GCM) and Counter with CBC-MAC (CCM) algorithms for encryption. These algorithms provide authenticated encryption with block ciphers.

Encrypting a New Dataset

TrueNAS can encrypt new datasets within an existing unencrypted storage pool without having to encrypt the entire pool. To encrypt a single dataset, go to **Storage > Pools**, open the ⋮ for an existing dataset, and click **Add Dataset**.

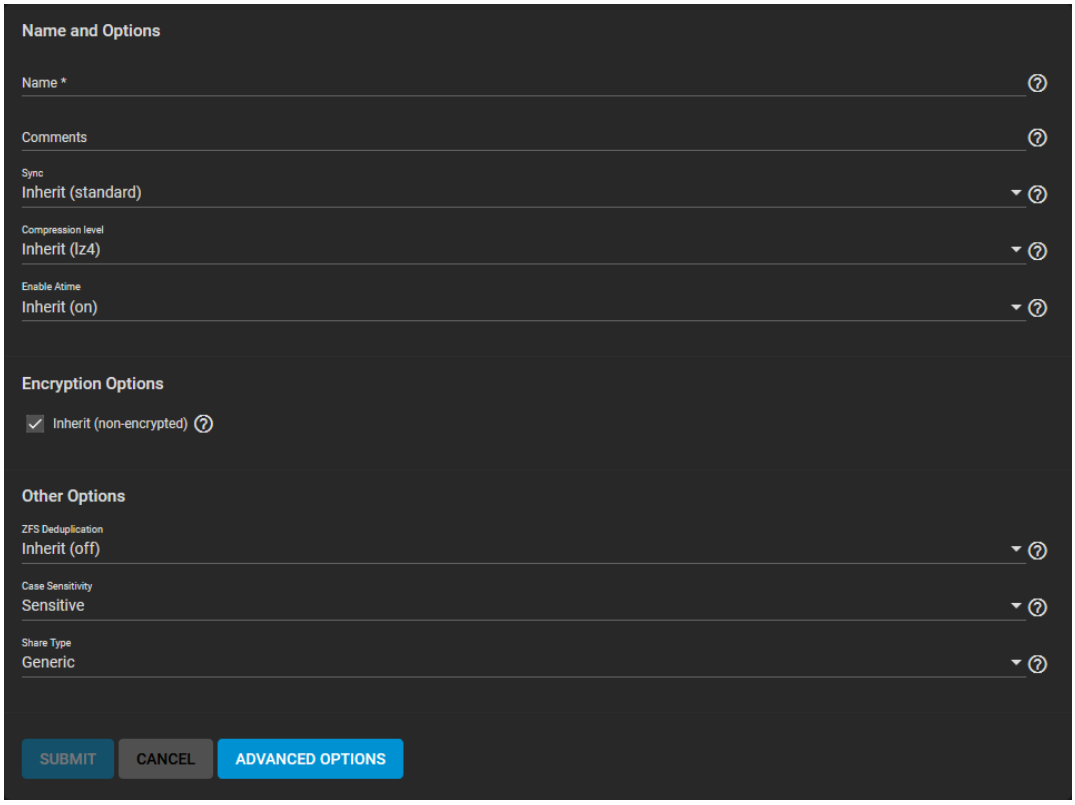


Figure 3: New Dataset Options

In the **Encryption Options** area, clear the **Inherit** checkbox, then select **Encryption**.

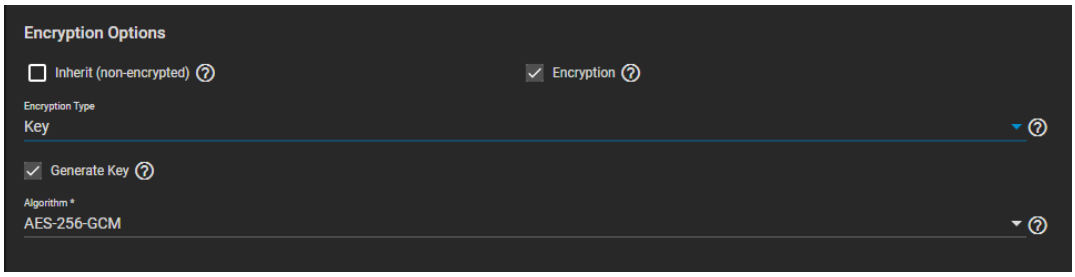


Figure 4: Dataset Encryption Options

Now select the authentication to use from the two options in **Type**: either a **Key** or **Passphrase**. The remaining options are the same as a new pool. Datasets with encryption enabled show additional icons on the **Storage > Pools** list.

Locking and Unlocking Datasets

The dataset locked/unlocked status is determined from an icon:

- The dataset unlocked icon: .
- The dataset locked icon: .
- A Dataset on an encrypted pool with encryption properties that don't match the root dataset shows this icon:

> NOTE: An unencrypted pool with an encrypted dataset also shows this icon:

You can only lock or unlock encrypted datasets when they are secured with a passphrase instead of a key file. Before locking a dataset, verify that it is not currently in use, then click ⋮ (Options) and **Lock**.

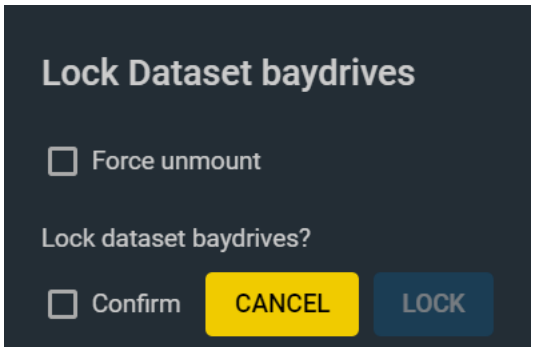


Figure 5: Dataset Locking Options

Use the **Force unmount** option only if you are certain no one is currently accessing the dataset. After locking a dataset, the unlock icon changes to a locked icon. While the dataset is locked, it is not available for use.

To unlock a dataset, click ⋮ and **Unlock**.

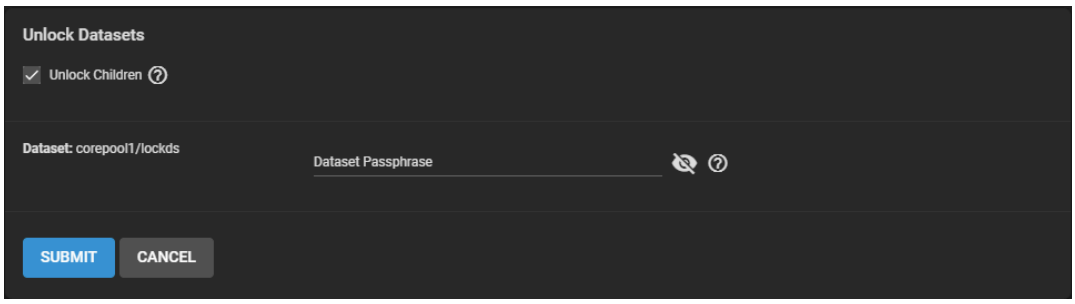


Figure 6: Dataset Unlock Options

Enter the passphrase and click **Submit**. To unlock child datasets, select **Unlock Children**. Child datasets that inherited encryption settings from the parent dataset unlock when the parent unlocks. Users can simultaneously unlock child datasets with different passphrases from the parent by entering their passphrases.

Confirm unlocking the datasets and wait for a dialog to show the unlock is successful.

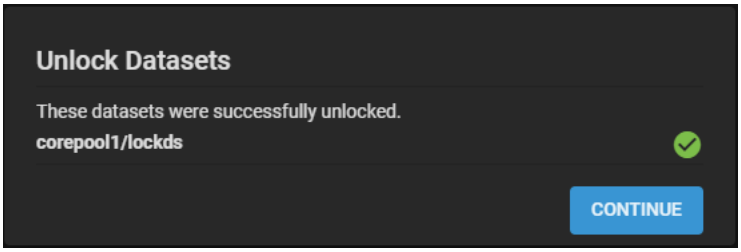


Figure 7: Dataset Unlock Success

▼ Example

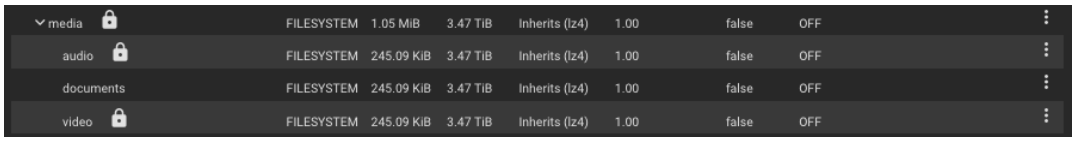


Figure 8: Encrypted locked Datasets

The parent dataset is *media*. It has three child datasets. The *documents* child dataset inherits the parent encryption settings and password. The other two child datasets (*audio* and *video*) have their own passphrases. When you lock the parent dataset all child datasets are also locked.

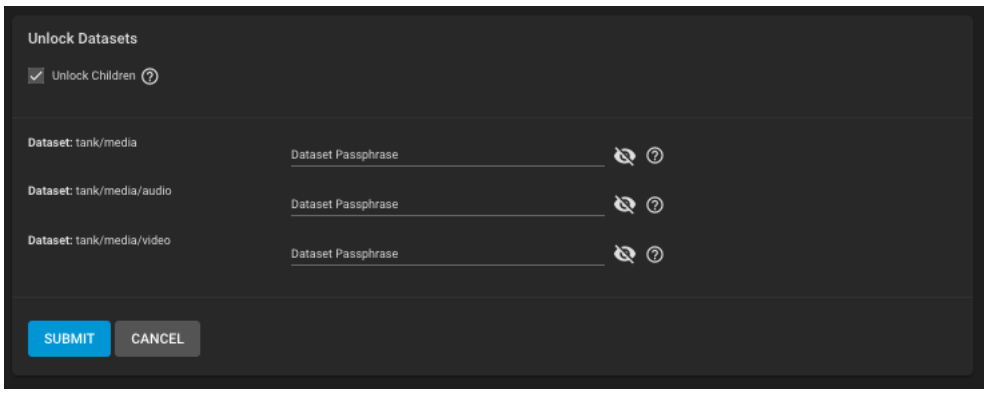


Figure 9: Password for locked Datasets

Open the ⋮ for the parent dataset and select **unlock**. To unlock all the datasets, select **Unlock Children** and enter the passphrase for each dataset to unlock.

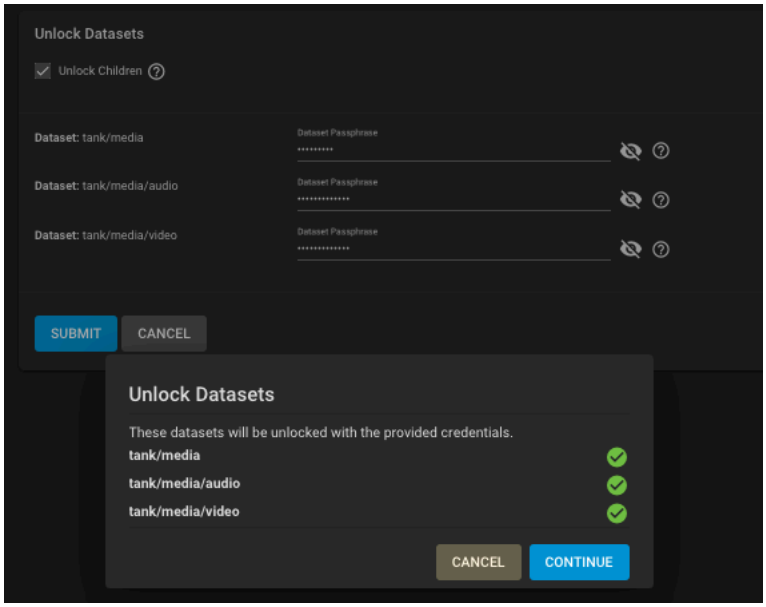


Figure 10: Successfully unlocked Datasets

Click the **Continue** button in the dialog window that confirms that the unlocking was successful. The dataset listing changes to show the unlocked icon.

Encryption Management

There are two ways to manage the encryption credentials, with either key files or passphrases.

> Always back up the key file to a safe and secure location!

Key Files

Creating a new encrypted pool automatically generates a new key file and prompts you to download it.

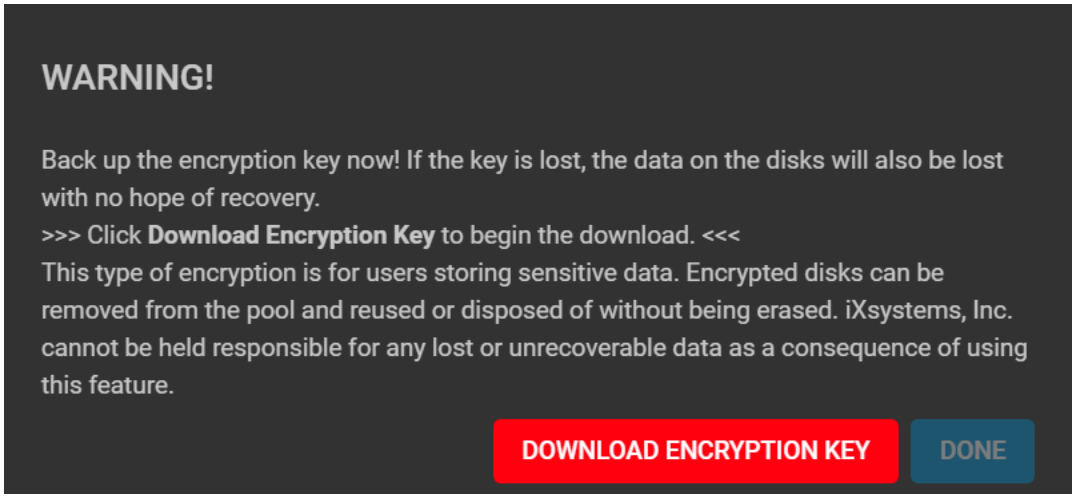
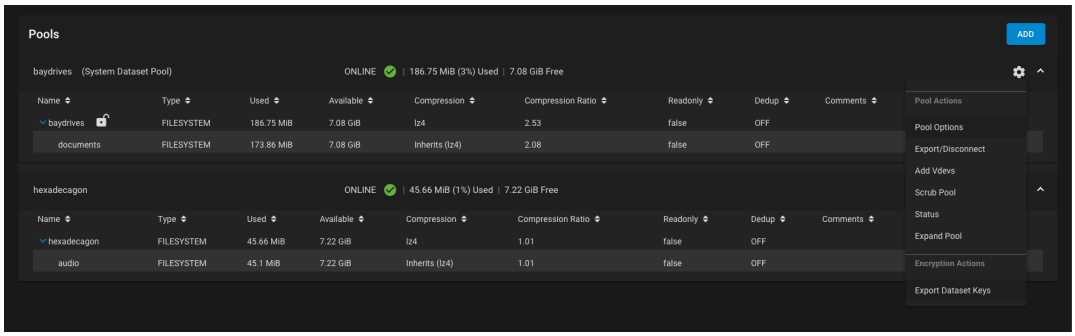


Figure 11: Encryption Backup Warning

Pool Key File

Manually download a copy of the inherited and non-inherited encrypted dataset key files for the pool by opening the pool ⚙ menu and selecting **Export Dataset Keys**. Enter the root password and click **CONTINUE**.

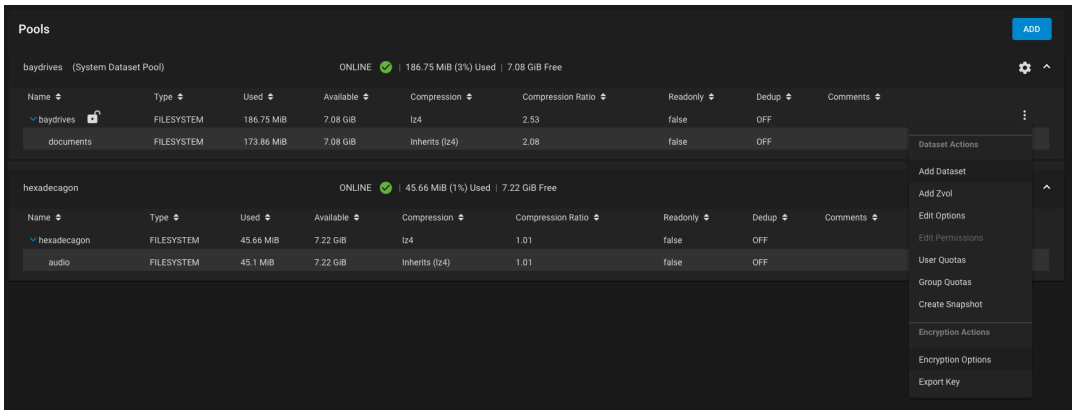


[Figure 12: Exporting Key Files]

Dataset Key File

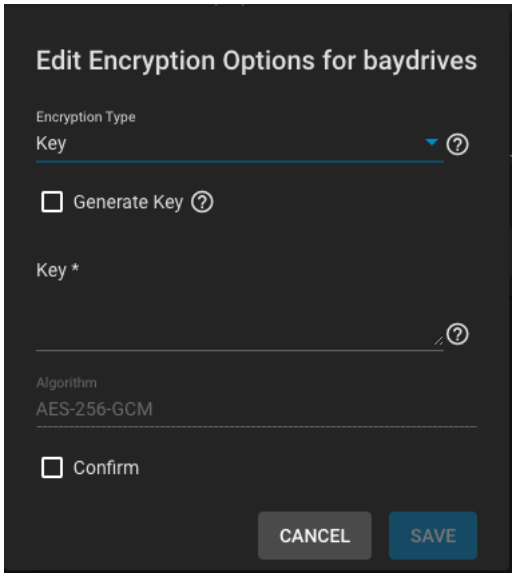
To manually download a back up of a single key file for the dataset, click the dataset ⋮ and select **Export Key**. Enter the root password and click **CONTINUE**. Click **DOWNLOAD KEY**.

To change the key, click the dataset ⋮ and **Encryption Options**.



[Figure 13: Encryption Options]

Enter your custom key or click **Generate Key**.



[Figure 14: Editing Encryption Options]

Passphrases

> The passphrase is the only means to decrypt the information stored in a dataset using passphrase encryption keys. Be sure to create a memorable passphrase or physically secure the passphrase.

To use a passphrase instead of a key file, click the dataset ⋮ and **Encryption Options**. Change the **Encryption Type** from **Key** to **Passphrase**.

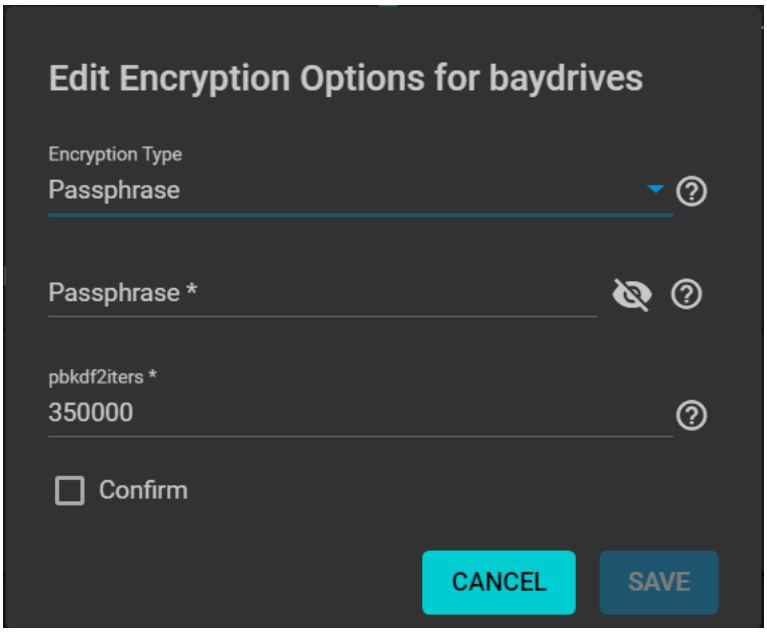


Figure 15: Dataset Encryption Passphrase Options

Set the rest of the options:

- **Passphrase** is a user-defined string of eight to 512 characters in length, to use instead of an encryption key to decrypt the dataset.
- **pbkdf2iters** is the number of password-based key derivation function 2 (PBKDF2) iterations to use for reducing vulnerability to brute-force attacks. Entering a number greater than **100000** is required.

Unlocking a Replicated Encrypted Dataset or Zvol Without a Passphrase

Users with TrueNAS CORE or Enterprise installations without KMIP should either replicate the dataset or zvol without properties to disable encryption at the remote end or construct a special json manifest to unlock each child dataset/zvol with a unique key.

Unlocking Methods

▼ Method 1: Construct JSON Manifest

1. Replicate every encrypted dataset you want to replicate with properties.
2. Export key for every child dataset which has a unique key.
3. Construct a proper json for each child dataset with *poolname*/*datasetname* of the destination system and key from the source system. For example: `{"tank/share01": "57112db4be777d93fa7b76138a68b790d46d6858569bf9d13e32eb9fda72146b"}`
4. Save this file with the extension .json.
5. Unlock the dataset(s) on the remote system using properly constructed json files.

▼ Method 2: Replicate Encrypted Dataset/zvol Without Properties

To not encrypt the dataset on the remote side so it does not require a key to unlock, clear properties when replicating.

1. Go to **Tasks > Replication Tasks** and click **ADD**.
2. Click **ADVANCED REPLICATION CREATION**.
3. Fill out the form as needed and do not select **Include Dataset Properties**.
4. Click **SUBMIT**.

Legacy GELI Encryption

TrueNAS no longer supports GELI encryption (deprecated).

▼ Can I directly convert a GELI-encrypted pool to native ZFS encryption?

No. You must migrate data out of the GELI pool and into a ZFS encrypted pool.

GELI Pool Migrations

Data can be migrated from the GELI-encrypted pool to a new ZFS-encrypted pool. Unlock the GELI-encrypted pool before attempting any data migrations. The new ZFS-encrypted pool must be at least the same size as the previous GELI-encrypted pool. Do not delete the GELI dataset until you verify the data migration.

There are a few options to migrate data from a GELI-encrypted pool to a new ZFS-encrypted pool:

- Using the Replication Wizard
- Using file transfer

- Using ZFS send and receive

Using the Replication Wizard

GELI encrypted pools continue to be detected and supported in the TrueNAS web interface as **Legacy Encrypted** pools. As of TrueNAS version 12.0-U1, a decrypted GELI pool can migrate data to a new ZFS encrypted pool using the Replication Wizard.

▼ Replication Wizard Method

Start the Replication Wizard, go to **Tasks** > **Replication Task** and click **ADD**.

1. In **Source Location**, select **On this System**, then set the dataset to transfer.
2. In **Destination Location**, select **On a Different System**, then:

   a. Create or select an existing **SSH Connection**. Either click **Create New** or select the destination system SSH connection from the list of available connections.

   b. In **Destination**, select the dataset to replicate files to.

   c. (Optional) Select **Encryption** to apply encryption to the SSH transfer. Select either **PASSPHRASE** or **HEX** as the **Encryption Key Format**. If you selected **PASSPHRASE**, enter the passphrase. If you selected **HEX**, set **Generate Encryption Key**. Select **Store Encryption key in Sending TrueNAS database**. Click **Next**
3. Select **Run Once** as the replication schedule.
4. Clear the **Make Destination Dataset Read-Only** checkbox.
5. Click **START REPLICATION**

File Transfer Method

> This method does not preserve file ACLs.

The web interface supports using **Tasks > Rsync Tasks** to transfer files out of the GELI pool.

▼ File Transfer Method

In the shell, `rsync` and other file transfer mechanisms (`scp`, `cp`, `sftp`, `ftp`, `rdiff-backup`) are available for copying data between pools.

ZFS Send and Receive

> These instructions are an example walk-through, and not an exact step-by-step guide for all situations. Research ZFS send/receive before attempting this. A simple example cannot cover every edge case.

▼ ZFS Send and Receive Method

Legend:

- GELI pool = pool_a
- Origin dataset = dataset_1
- Latest snapshot of GELI pool = snapshot_name
- ZFS native-encrypted pool = pool_b
- Receiving dataset = dataset_2

1. Create a new encrypted pool in **Storage > Pools**.
2. Open the shell. Make a new snapshot of the GELI pool and dataset with the data to migrate. Enter command: `zfs snapshot -r pool_a/dataset_1@snapshot_name.`
3. Create a passphrase: `echo passphrase > /tmp/pass.`
4. Use ZFS send/receive to transfer the data between pools. Enter command: `zfs send -Rv pool_a/dataset_1@snapshot_name | zfs recv -o encryption=on -o keyformat=passphrase -o keylocation=file:///tmp/pass pool_b/dataset_2.`
5. After the transfer completes, go to **Storage > Pools** and lock the new dataset. After locking the dataset, immediately unlock it. TrueNAS prompts for the passphrase. After entering the passphrase and unlocking the pool, you can delete the `/tmp/pass` file used for the transfer.
6. If desired, you can convert the dataset to use a key file instead of a passphrase. To use a key file, click the dataset ⁝B (Options) and click **Encryption Options**. Change the **Encryption Type** from **Passphrase** to **Key** and save. Back up your key file immediately!
7. Repeat this process for every dataset in the pool that you need to migrate.

Fusion Pools

Fusion Pools are also known as ZFS allocation classes, ZFS special vdevs, and metadata vdevs (**Metadata** vdev type on the **Pool Manager** screen.).

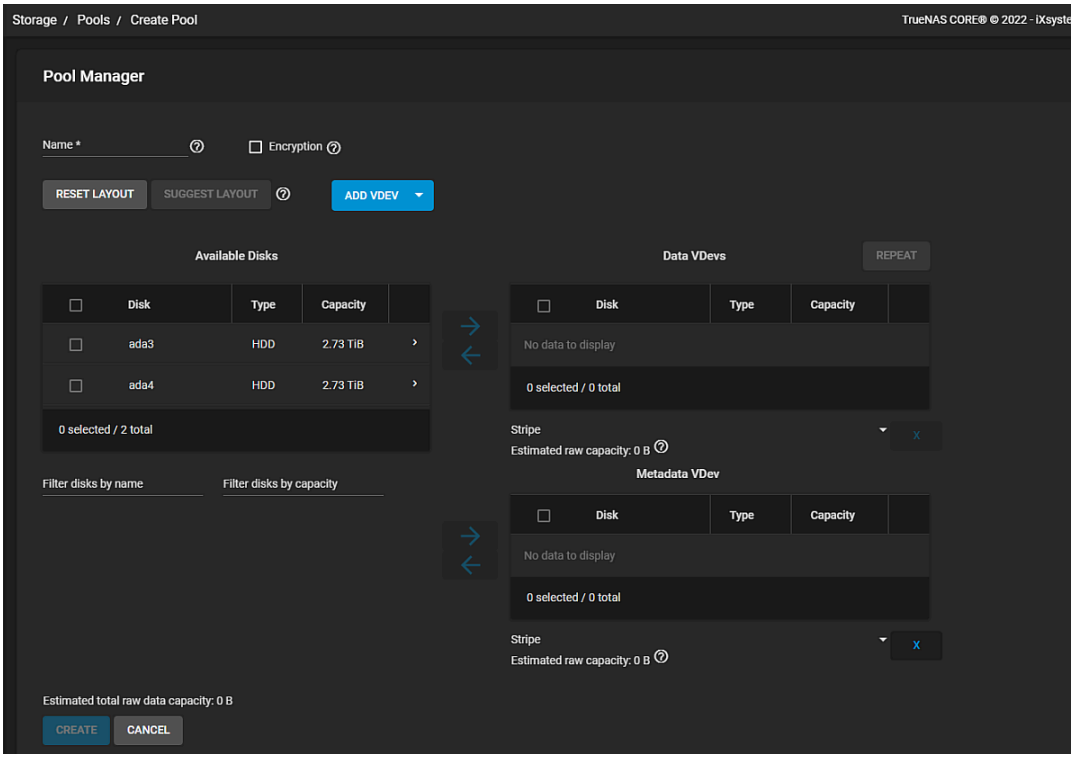
▼ What's a special VDEV?

A special VDEV can store metadata such as file locations and allocation tables. The allocations in the special class are dedicated to specific block types. By default, this includes all metadata, the indirect blocks of user data, and any deduplication tables. The class can also be provisioned to accept small file blocks. This is a great use case for high performance but smaller sized solid-state storage. Using a special vdev drastically speeds up random I/O and cuts the average spinning-disk I/Os needed to find and access a file by up to half.

Creating a Fusion Pool

Go to **Storage > Pools**, click **ADD**, and select **Create new pool**.

A pool must always have one normal (non-dedup/special) VDEV before other devices can be assigned to the special class. Configure the **Data VDevs**, then click **ADD VDEV** and select **Metadata**.



Add SSDs to the new **Metadata VDev** and select the same layout as the **Data VDevs**.

> The metadata special VDEV is critical for pool operation and data integrity, so you must protect it with hot spare(s).

▼ UPS Recommendation

When using SSDs with an internal cache, add uninterruptible power supply (UPS) to the system to help minimize the risk from power loss.

Using special VDEVs identical to the data VDEVs (so they can use the same hot spares) is recommended, but for performance reasons you can make a different type of VDEV (like a mirror of SSDs). In that case you must provide hot spare(s) for that drive type as well. Otherwise, if the special VDEV fails and there is no redundancy, the pool becomes corrupted and prevents access to stored data.

> Drives added to a metadata VDEV cannot be removed from the pool.

When more than one metadata VDEV is created, then allocations are load-balanced between all these devices. If the special class becomes full, then allocations spill back into the normal class.

After the fusion pool is created, the **Status** shows a **Special** section with the metadata SSDs.

See Managing Pools.

SLOG Overprovisioning

Over-provisioning SLOG SSDs is useful for different scenarios. The most useful benefit of over-provisioning is greatly extending SSD life. Over-provisioning an SSD distributes the total number of writes and erases across more flash blocks on the drive.

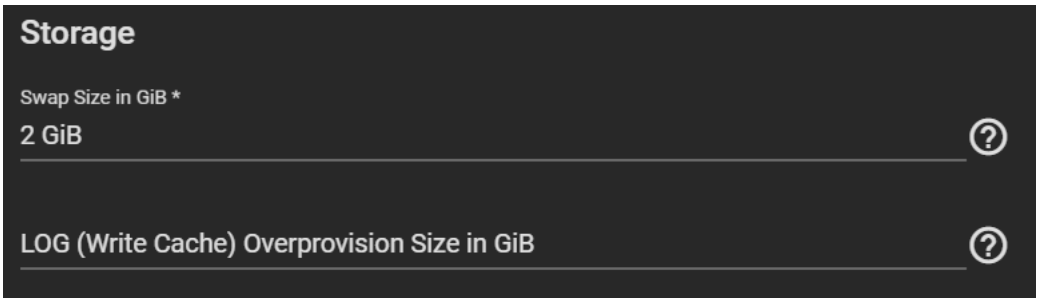
Seagate provides a thoughtful investigation into over-provisioning SSDs here: https://www.seagate.com/blog/ssd-over-provisioning-benefits-master-ti/.

> Some SATA devices are limited to one resize per power cycle. Some BIOS can block resize during boot and require a live power cycle.

Overprovision Options

▼ Web Interface

To over provision a SLOG device, log in to TrueNAS and go to **System > Advanced**. Enter an over-provision value corresponding to the new size in GB in the **Log (Write Cache) Overprovision Size in GiB** field.



When this value is applied, the over-provision value is applied whenever a pool is created with a SLOG device. It is impossible to restore an over-provisioned SLOG device back to original capacity without running the `disk_resize` command after first destroying the pool it was part of and issuing a full power cycle.

> Only one over-provision/under-provision operation occurs per power cycle.

Erasing the over-provision setting in **System > Advanced Log (Write Cache) Overprovision Size in GiB** field and setting to *none* prevents future SLOG devices from being over-provisioned.

▼ Shell

Use `disk_resize` in the shell to over-provision.

The command to over-provision an SSD is `disk_resize {DEVICE} {SIZE}`, where *{DEVICE}* is the SSD device name and *{SIZE}* is the new provision size in GiB or TiB. Example: `disk_resize ada5 16GB`. When no size is specified, it reverts the provision back the full size of the device.

Creating Snapshots

Snapshots are one of the most powerful features of ZFS. A *snapshot* provides a read only point-in-time copy of a file system or volume. This copy does not consume extra space in the ZFS pool. The snapshot only records the differences between storage block references whenever the data is modified.

▼ Why do I want to keep snapshots?

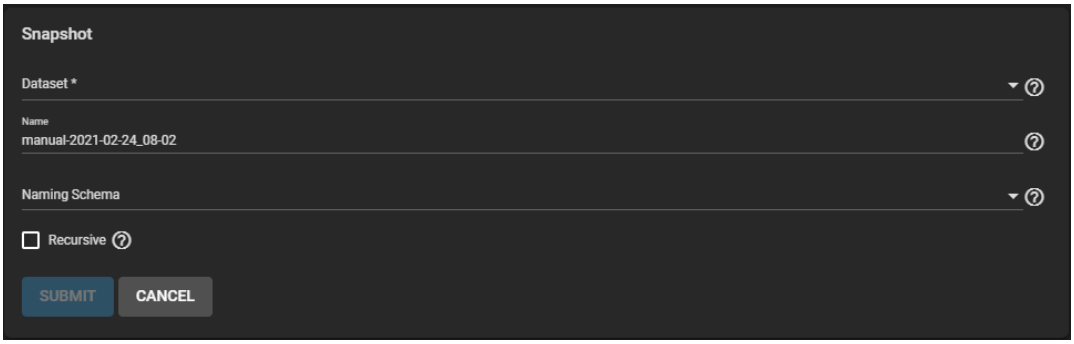
Snapshots keep a history of files and provide a way to recover an older or even deleted files. For this reason, many administrators take regular snapshots, store them for some time, and copy them to a different system. This strategy allows an administrator to roll the system data back to a specific point in time. In the event of catastrophic system or disk failure, off-site snapshots can restore data up to the most recent snapshot.

Taking snapshots requires the system have all pools, datasets, and zvols already configured.

Creating a Single Snapshot

> Consider making a Periodic Snapshot Task to save time and create regular, fresh snapshots.

To perform a quick snapshot of existing storage, go to **Storage > Snapshots** and click **ADD**.



Use the **Dataset** dropdown list to select an existing ZFS pool, dataset, or zvol to snapshot.

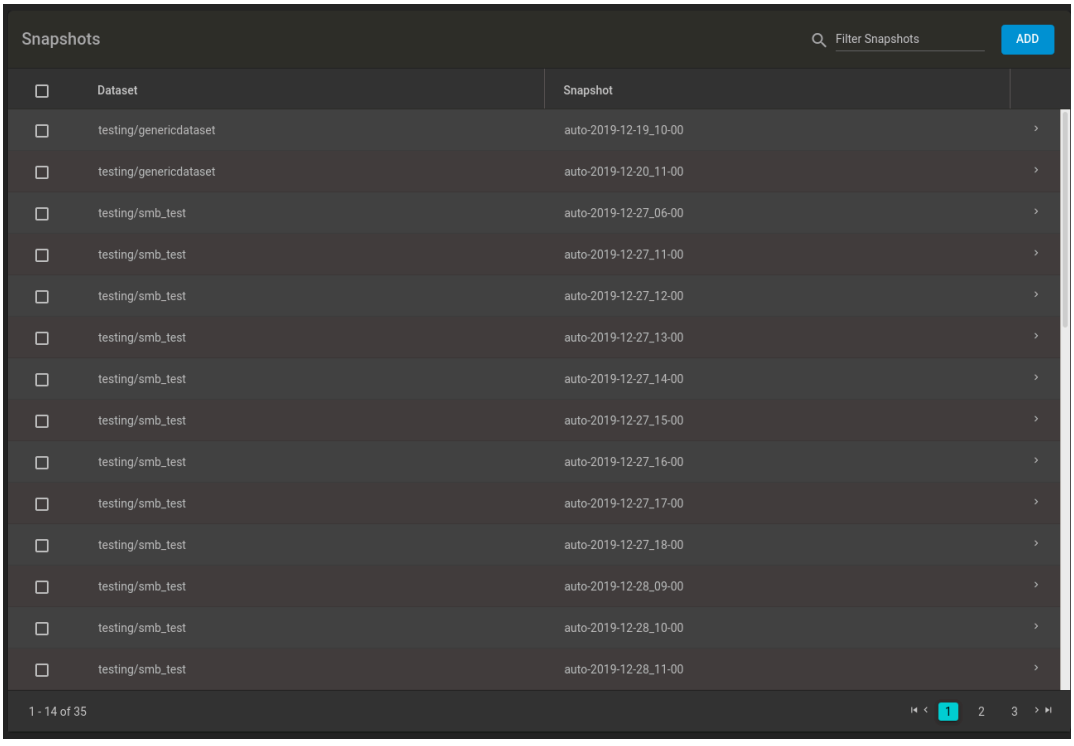
The TrueNAS software displays a suggested name that you can override with any custom string.

To include the snapshot in local or remote replication tasks choose a proper naming schema. The **Naming Schema** drop-down list populates with schemas already created from periodic snapshot tasks.

To include child datasets with the snapshot, select **Recursive**.

Managing Snapshots

Go to **Storage > Snapshots** to manage created snapshots.



Each entry in the list includes the dataset and snapshot names. Click › to view options for a snapshot.

DATE CREATED shows the exact time and date of the snapshot creation.

USED shows the amount of space consumed by this dataset and all of its descendants. This value, checked against the dataset quota and reservation, shows the space used but does not include the dataset reservation. It takes into account the reservations of any descendant datasets. The amount of space that a dataset consumes from its parent, and the amount of space freed if this dataset is recursively deleted, is the greater of its space used and its reservation.

At creation, a snapshot shares space between the snapshot, file system, and even with previous snapshots. File system changes reduce the shared space and count toward space used by a snapshot. Deleting a snapshot often increases the space that is unique and used in other snapshots.

REFERENCED shows the amount of data accessible by this dataset. This could be shared with other datasets in the pool. New snapshots or clones reference the same amount of space as the file system it was created from, as the contents are identical.

Viewing Used Space with Shell

Another method to view the space used by an individual snapshot is to go to the shell and enter command `zfs list -t snapshot`.

The space used, available, or referenced does not account for pending changes. In general, pending changes update within a few seconds, but larger disk changes slow usage updates.

Deleting a Snapshot

The **Delete** option destroys the snapshot. You must delete child clones before you can delete their parent snapshot. While creating a snapshot is instantaneous, deleting one is I/O intensive and can take a long time, especially when deduplication is enabled.

▼ Why?

ZFS has to review all allocated blocks before deletion to see if another process is using that block. If not used, the ZFS can free that block.

Cloning a Snapshot

Use **CLONE TO NEW DATASET** to create a new snapshot *clone* (dataset) from the snapshot contents.

▼ What is a clone?

A *clone* is a writable copy of the snapshot. Because a clone is actually a mountable dataset, it appears in the **Pools** screen rather than the **Snapshots** screen. Creating a new snapshot adds **-clone** to the name by default.
A dialog prompts for the new dataset name. The suggested name derives from the snapshot name.

Rolling Back

Reverts the dataset back to the point in time saved by the snapshot.

> Rollback is a dangerous operation that causes any configured replication tasks to fail. Replications use the existing snapshot when doing an incremental backup, and rolling back can put the snapshots out of order. To restore the data within a snapshot, the recommended steps are:
>
> 1. Clone the desired snapshot.
> 2. Share the clone with the share type or service running on the TrueNAS system.
> 3. Allow users to recover their needed data.
> 4. Delete the clone from **Storage > Pools**.
>
> This approach does not destroy any on-disk data and has no impact on replication.

TrueNAS asks for confirmation before rolling back to the chosen snapshot state. Clicking **Yes** reverts all dataset files to the state they were in at the time of snapshot creation.

Bulk Operations

To delete multiple snapshots, select the left column box for each snapshot to include. Click the **Delete** button that displays.

To search through the snapshots list by name, type a matching criteria into the **Filter Snapshots** text field. The list now displays only the snapshot names that match the filter text.

Browsing a Snapshot Collection

All dataset snapshots are accessible as an ordinary hierarchical file system, accessed from a hidden .zfs located at the root of every dataset.

> A snapshot and any files it contains are not accessible or searchable if the snapshot mount path is longer than 88 characters. The data within the snapshot is safe but to make the snapshot accessible again shorten the mount path.

A user with permission to access the dataset contents can view the list of snapshots by going to the dataset .zfs directory from a share, like **SMB**, **NFS**, and **iSCSI**, or in the TrueNAS SCALE CLI. Users can browse and search any files they have permission to access throughout the entire dataset snapshot collection.

When creating a snapshot, permissions or ACLs set on files within that snapshot might limit access to the files. Snapshots are read-only, so users do not have permission to modify a snapshot or its files, even if they had write permissions when creating the snapshot.

From the **Datasets** screen, select the dataset and click **Edit** on the **Dataset Details** widget. Click **Advanced Options** and set **Snapshot Directory** to **Visible**.

To access snapshots:

- Using a share, configure the client system to view hidden files. For example, in a Windows SMB share, enable **Show hidden files, folders, and drives** in **Folder Options**. From to the dataset root folder, open the .zfs directory and navigate to the snapshot.
- Using the TrueNAS SCALE CLI, enter `storage filesystem listdir path="/PATH/TO/DATASET/.zfs/PATH/TO/SNAPSHOT"` to view snapshot contents.

  ▼ Command Example

```
storage filesystem listdir path="/mnt/tank/test/.zfs/snapshot/SNAPSHOT1"
+--------------+-----------------------------------------------------+-----------------------------------------------------+---------
| name         | path                                                | realpath                                            | type
+--------------+-----------------------------------------------------+-----------------------------------------------------+---------
| tuser        | /mnt/tank/test/.zfs/snapshot/SNAPSHOT1/tuser        | /mnt/tank/test/.zfs/snapshot/SNAPSHOT1/tuser        | DIRECTOR
| FILENAME.tar | /mnt/tank/test/.zfs/snapshot/SNAPSHOT1/FILENAME.tar | /mnt/tank/test/.zfs/snapshot/SNAPSHOT1/FILENAME.tar | FILE
| FILE.tar     | /mnt/tank/test/.zfs/snapshot/SNAPSHOT1/FILE.tar     | /mnt/tank/test/.zfs/snapshot/SNAPSHOT1/FILE.tar     | FILE
+--------------+-----------------------------------------------------+-----------------------------------------------------+---------
```

A user with permission to access the hidden file can view and explore all snapshots for a dataset from the shell or the **Sharing** screen using services like **SMB**, **NFS**, and **SFTP**.

Creating VMware-Snapshots

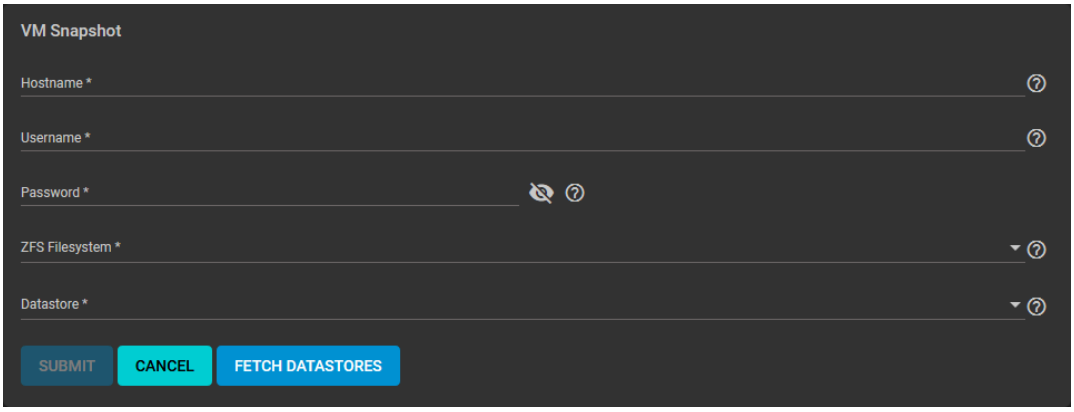
Storage > **VMware-Snapshots** coordinates ZFS snapshots when using TrueNAS as a VMware datastore. When a ZFS snapshot is created, TrueNAS automatically snapshots any running VMware virtual machines before taking a scheduled or manual ZFS snapshot of the dataset or zvol backing that VMware datastore.

To copy TrueNAS snapshots to VMWare, virtual machines must be powered-on. The temporary VMware snapshots are then deleted on the VMware side but still exist in the ZFS snapshot and are available as stable restore points. These coordinated snapshots go on the **Storage > Snapshots** list.

> You need a paid-edition for VMware ESXi to use VMware-Snapshots. If you try to use them with ESXi free edition you see the following error message: **Error: Can't create snapshot, current license or ESXi version prohibits execution of the requested operation.** ESXi free has a locked (read-only) API that prevents using TrueNAS VMware-Snapshots. The cheapest ESXi edition that is compatible with TrueNAS VMware-Snapshots is **VMware vSphere Essentials Kit**.

Create a VMware Snapshot

Go to **Storage > VMware Snapshots** and click **ADD**.



After entering the **Hostname**, **Username**, and **Password**, click **FETCH DATASTORES** to populate the menu and then select the datastore to synchronize.

TrueNAS connects to the VMware host after clicking *FETCH DATASTORES*. The **ZFS Filesystem** and **Datastore** drop-down menus populate from the VMware host response. Choosing a datastore also selects any previously mapped dataset.

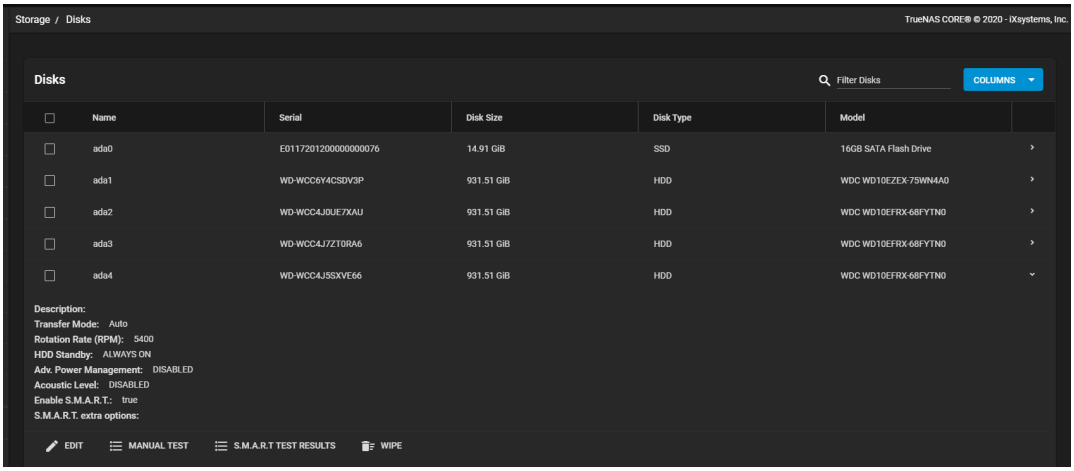
Disks

Wiping a Disk

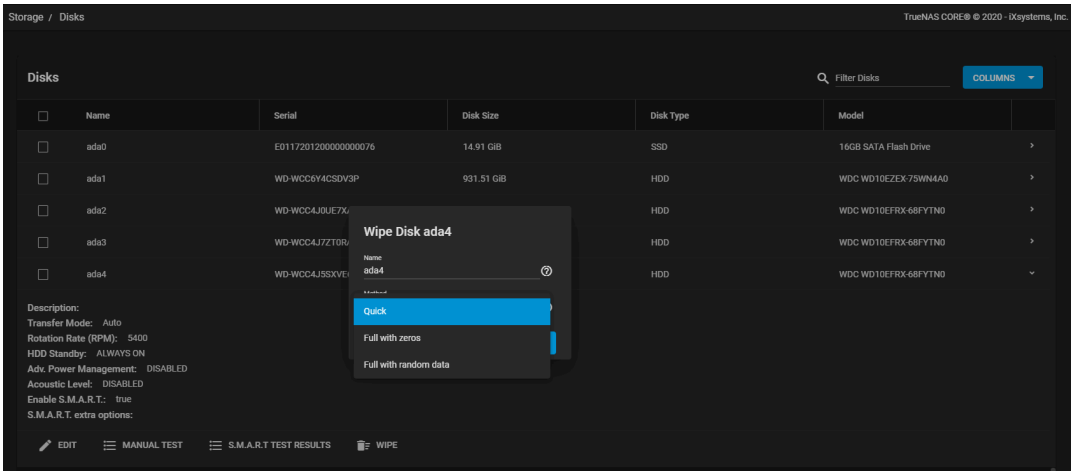
The wipe function deletes obsolete data off an unused disk.

> This is a destructive action and results in permanent data loss! Back up any critical data off the disk to be wiped.

To wipe a disk, go to **Storage** > **Disks**. Click the › for a disk to see all the options.



The wipe option is only available when the disk is not in use. Click **WIPE** to open a dialog with additional options:

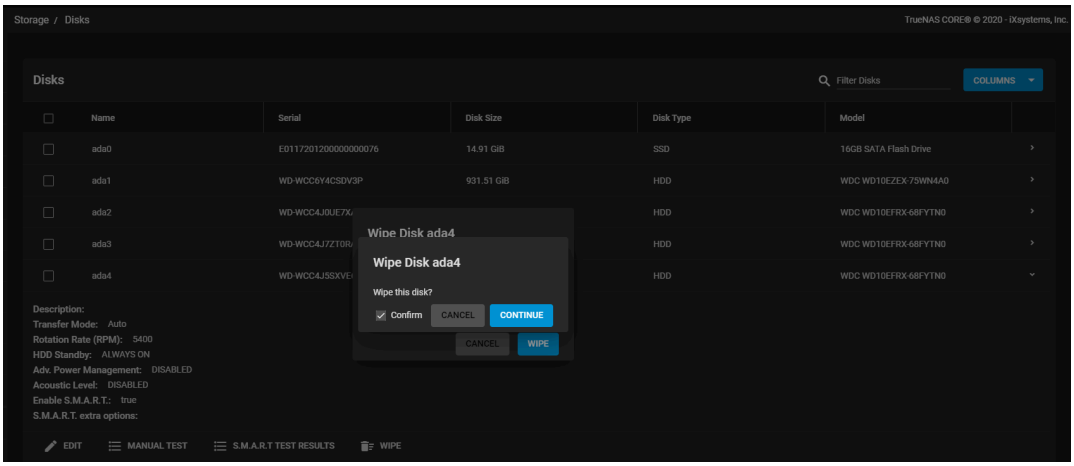


The disk **Name** (da1, da2, ada4) helps confirm that you have selected the right disk to wipe.

The **Method** dropdown list shows the different available wipe options available. Select **Quick** to erase only the partitioning information on a disk, making it easy to reuse but without clearing other old data. Quick wipes take only a few seconds. Select **Full with zeros** to overwrite the entire disk with zeros. This can take several hours to complete. Select **Full with random** to overwrite the entire disk with random binary code and takes even longer than **Full with zeros** to complete.

> Ensure all data is backed up and the disk is no longer in use. Triple check that the correct disk is selected for the wipe. Recovering data from a wiped disk is usually impossible.

After selecting the appropriate method, click **WIPE**. A dialog asks for confirmation of the action.



Verify the name to ensure you have the correct disk chosen. When satisfied the disk can be wiped, select **Confirm** and click **CONTINUE**. A dialog shows the disk wipe progress.

See Disks Screens for more information on Disks screen settings.

Disk Replacement

Hard drives and solid-state drives (SSDs) have a finite lifetime and can fail unexpectedly. When a disk fails in a Stripe (RAID0) pool, you must recreate the entire pool and restore all data backups. We always recommend creating non-stripe storage pools that have disk redundancy.

To prevent further redundancy loss or eventual data loss, always replace a failed disk as soon as possible! TrueNAS integrates new disks into a pool to restore it to full functionality.

> TrueNAS requires you to replace a disk with another disk of the same or greater capacity as a failed disk. You must install the disk in the TrueNAS system. It should not be part of an existing storage pool. TrueNAS wipes the data on the replacement disk as part of the process.
>
> Disk replacement automatically triggers a pool resilver.

▼ Can I replace a disk in a GELI-encrypted (Legacy) pool?

Although GELI encryption is deprecated, TrueNAS implements GELI encryption during a “GELI-Encrypted (Legacy) pool” disk replacement. TrueNAS uses GELI encryption for the lifetime of that pool, even after replacement.

The TrueNAS **Pool** widget on the main **Dashboard** shows when a disk failure degrades a pool.

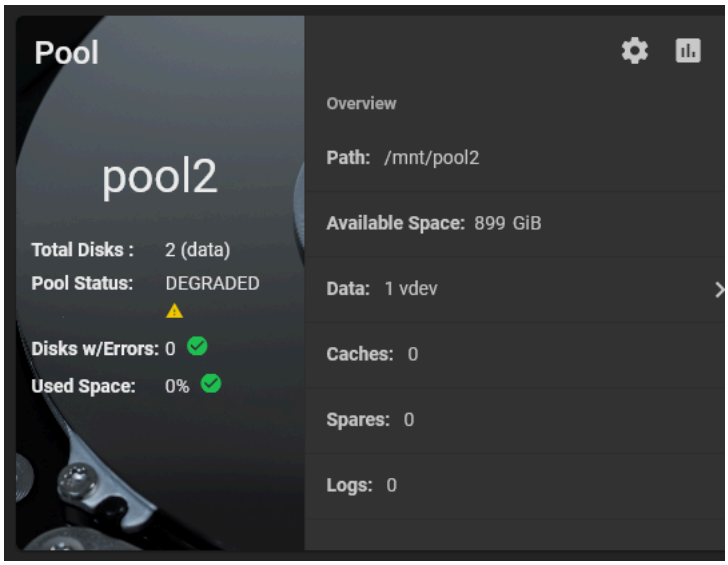


Figure 1: Degraded pool on dashboard widget

Click the ⚙ on the pool card to go to the **Storage > Pools > Pool Status** screen to locate the failed disk.

▼ My disk is faulted. Should I replace it?

If a disk shows a faulted state, TrueNAS has detected an issue with that disk and you should replace it.

To replace a disk in a pool without a hot spare available:

1. Take the disk offline.
2. Replace the disk.
3. Refresh the screen.

To replace a disk in a pool with a hot spare:

1. Take the disk offline.
2. Detach the failed disk to promote the hot spare.
3. Refresh the screen.
4. Recreate the hot spare VDEV.

Taking a Failed Disk Offline

We recommend you take the disk offline before starting the replacement. This removes the device from the pool and can prevent swap issues. To offline a disk:

Go to the **Storage > Pools** screen, click on the ⚙ settings icon, and then select **Status** to open the **Pool Status** screen and display the disks in the pools.

Click the ⋮ icon for the disk you plan to remove and then click **Offline**.

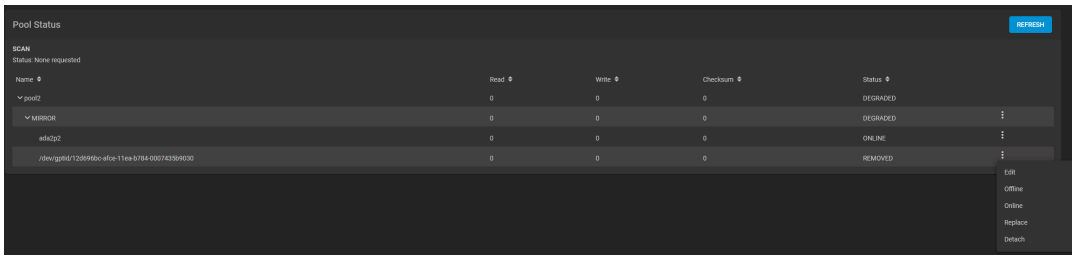


Figure 2: Pool Status disk options

Select **Confirm**, then click **OFFLINE**.

When the disk status shows as **Offline**, physically remove the disk from the system.

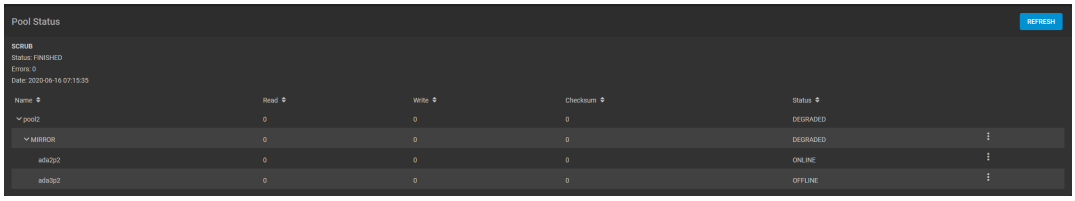


Figure 3: Pool Status disk offline

▼ The offline failed?

If the offline operation fails with a **Disk offline failed - no valid replicas** message, go to **Storage > Pools**, click the ⚙ for the degraded pool, and select **Scrub Pool**. When the scrub operation finishes, reopen the pool **Status** and try to offline the disk again.

Replacing a Failed Disk

If replacing the failed disk that you have taken offline and removed, insert the replacement disk now. If replacing a failed disk with an available disk in the system, proceed to the next step.

In the **Pool Status** screen, open the options for the offline disk and click **Replace**

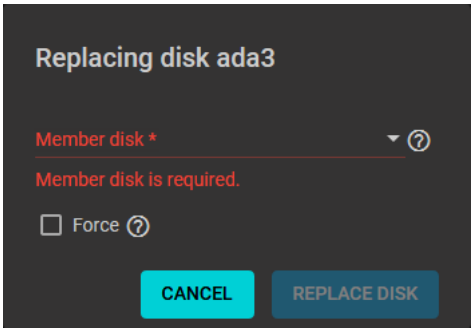


Figure 4: Replacing disk screen

Select a new member disk and click **Replace Disk**. The new disk must have the same or greater capacity as the disk you are replacing. The replacement fails when the chosen disk has partitions or data present. To destroy any data on the replacement disk and allow the replacement to continue, set the **Force** option.

When the disk wipe completes and TrueNAS starts replacing the failed disk, the **Pool Status** screen changes to show the in-progress replacement.

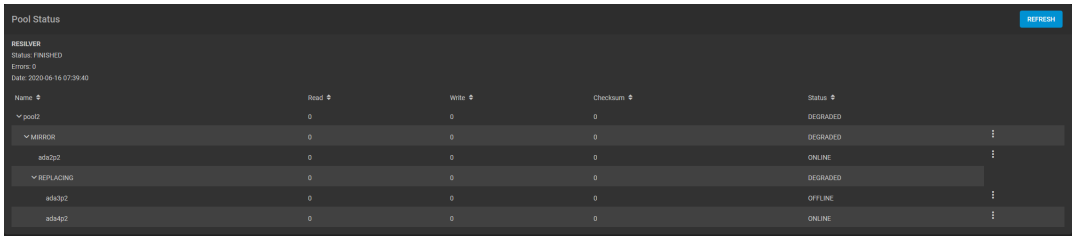


Figure 5: Pool Status replacing disk

TrueNAS resilvers the pool during the replacement process. For pools with large amounts of data, resilvering can take a long time.

When the resilver completes, the **Pool Status** screen updates to show the new disk, and the pool status returns to **Online**.

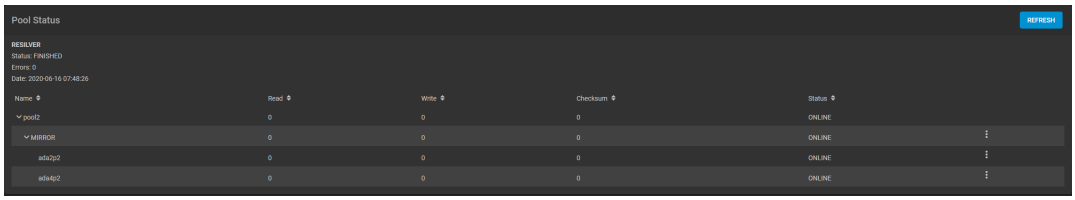


Figure 6: Pool Status disk replacement complete

Replacing a Failed Disk with a Hot Spare

A **Hot Spare** vdev sets up drives as reserved to prevent larger pool and data loss scenarios. TrueNAS automatically inserts an available hot spare into a **Data** vdev when an active drive fails. The pool resilvers after the hot spare is activated.

To replace a disk in a pool with a hot spare:

1. Take the disk offline.
2. Detach the failed disk to promote the hot spare.
3. Refresh the screen.
4. Recreate the hot spare VDEV.

Detaching a Failed Disk

Go to the **Storage > Pools** screen, click on the ⚙ settings icon, and then select **Status** to open the **Pool Status** screen and display the disks in the pools.

After taking the failed disk offline and removing it from the system, the disk status changes to **REMOVED** and the disk name displays the gptid.

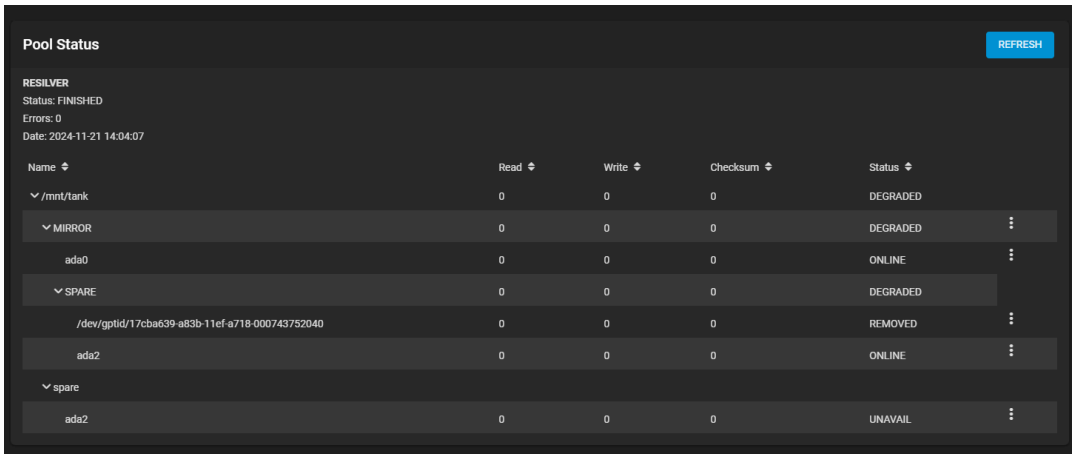


Figure 7: Disk Removed - Hot Spare Active

Click the ⋮ icon for the removed disk and then click **Detach**.

Select **Confirm**, then click **DETACH**. TrueNAS detaches the disk from the pool and promotes the hot spare disk to a full member of the pool.

Recreating the Hot Spare

After promoting the hot spare, recreate the **Spare** vdev and assign a disk to it.

▼ Do I really need to promote the hot spare and then recreate the spare vdev?

If you have a hot spare inserted into the pool and then follow the instructions in Replacing a Failed Disk, TrueNAS automatically returns the hot spare disk to the existing **Spare** vdev and **ONLINE** status.

However, we do not recommend this method, because it causes two resilver events: one when activating the hot spare and again when replacing the failed disk. Resilvering degrades system performance until completed and causes unnecessary strain on the disk.

To avoid unnecessary resilvers, promote the hot spare then recreate the hot spare vdev.

If recreating the spare with a replacement in place of the failed disk, insert the replacement disk now. If recreating the spare with an available disk in the system, proceed to the next step.

Go to the **Storage > Pools** screen, click on the ⚙ settings icon, and then select **Add Vdevs** to open the **Pool Manager** screen and display the disks in the pools.

Click **ADD VDEV** and select **Hot Spare**.

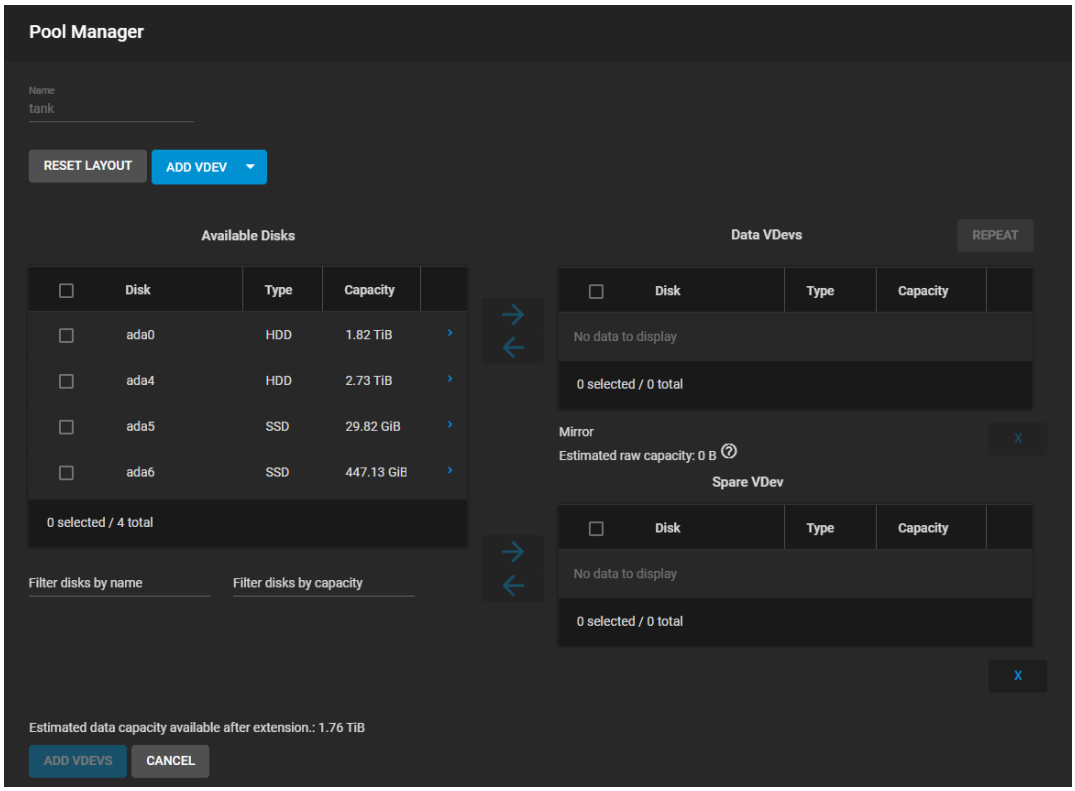


Figure 8: Add Vdev Hot Spare

Select an available disk and click ➔ to add it to the **Spare VDev**.

Click **ADD VDEVS**. Select **Confirm**, then click **ADD VDEVS**.

After completing the job, TrueNAS returns to the **Storage > Pools** screen. Click on the ⚙ settings icon, and then select **Status** to open the **Pool Status** screen and confirm the hot spare is added.

Self-Encrypting Drives

TrueNAS version 11.1-U5 introduced Self-Encrypting Drive (SED) support.

Supported Specifications

- Legacy interface for older ATA devices (Not recommended for security-critical environments!)
- TCG Opal 1 legacy specification
- TCG OPAL 2 standard for newer consumer-grade devices
- TCG Opalite which is a reduced form of OPAL 2
- TCG Pyrite Version 1 and Version 2 are similar to Opalite, but with hardware encryption removed Pyrite provides a logical equivalent of the legacy ATA security for non-ATA devices. Only the drive firmware protects the device.

  > Pyrite Version 1 SEDs do not have PSID support and can become unusable if the password is lost.

- TCG Enterprise designed for systems with many data disks These SEDs cannot unlock before the operating system boots.

See this Trusted Computing Group and NVM ExpressB® joint white paper for more details about these specifications.

TrueNAS Implementation

TrueNAS implements the security capabilities of camcontrol for legacy devices and sedutil-cli for TCG devices. When managing a SED from the command line, it is recommended to use the `sedhelper` wrapper script for `sedutil-cli` to ease SED administration and unlock the full capabilities of the device. Examples of using these commands to identify and deploy SEDs are provided below.

A SED can be configured before or after assigning the device to a pool.

By default, SEDs are not locked until the administrator takes ownership of them. Ownership is taken by explicitly configuring a global or per-device password in the web interface and adding the password to the SEDs. Adding SED passwords in the web interface also allows TrueNAS to automatically unlock SEDs.

A password-protected SED protects the data stored on the device when the device is physically removed from the system. This allows secure disposal of the device without having to first wipe the contents. Repurposing a SED on another system requires the SED password.

> For TrueNAS High Availability (HA) systems, SED drives only unlock on the active controller!

Deploying SEDs

Enter command `sedutil-cli --scan` in the shell to detect and list devices. The second column of the results identifies the drive type:

Character	Standard
no	non-SED device
1	Opal V1
2	Opal V2
E	Enterprise
L	Opalite
p	Pyrite V1
P	Pyrite V2
r	Ruby

Example:

```
root@truenas1:~ # sedutil-cli --scan
Scanning for Opal compliant disks
/dev/ada0  No  32GB SATA Flash Drive SFDK003L
/dev/ada1  No  32GB SATA Flash Drive SFDK003L
/dev/da0   No  HGST    HUS726020AL4210  A7J0
/dev/da1   No  HGST    HUS726020AL4210  A7J0
/dev/da10    E WDC     WUSTR1519ASS201  B925
/dev/da11    E WDC     WUSTR1519ASS201  B925
```

TrueNAS supports setting a global password for all detected SEDs or setting individual passwords for each SED. Using a global password for all SEDs is strongly recommended to simplify deployment and avoid maintaining separate passwords for each SED.

Setting a Global Password for SEDs

Go to **System > Advanced > SED Password** and enter the password.

> Record this password and store it in a safe place!

Now configure the SEDs with this password. Go to the shell and enter command `sedhelper setup <password>`, where `<password>` is the global password entered in **System > Advanced > SED Password**.

`sedhelper` ensures that all detected SEDs are properly configured to use the provided password:

```
root@truenas1:~ # sedhelper setup abcd1234
da9                 [OK]
da10                [OK]
da11                [OK]
```

Rerun command `sedhelper setup <password>` every time a new SED is placed in the system to apply the global password to the new SED.

Creating Separate Passwords for Each SED

Go to **Storage > Disks**. Click the **>** next to an SED, then select **Edit**. Enter and confirm the password in the **SED Password** field.

You must configure the SED to use the new password. Go to the shell and enter command `sedhelper setup --disk <da1> <password>`, where `<da1>` is the SED to configure and `<password>` is the created password from **Storage > Disks > Edit Disks > SED Password**.

Repeate this process for each SED and any SEDs added to the system in the future.

> Remember SED passwords! If you lose the SED password, you cannot unlock SEDs or access their data. Always record SED passwords whenever they are configured or modified and store them in a secure place!

Check SED Functionality

When SED devices are detected during system boot, TrueNAS checks for configured global and device-specific passwords.

Unlocking SEDs allows a pool to contain a mix of SED and non-SED devices. Devices with individual passwords are unlocked with their password. Devices without a device-specific password are unlocked using the global password.

To verify SED locking is working correctly, go to the shell. Enter command `sedutil-cli --listLockingRange 0 <password> </dev/da1>`, where `<dev/da1>` is the SED and `<password>` is the global or individual password for that SED. The command returns `ReadLockEnabled: 1`, `WriteLockEnabled: 1`, and `LockOnReset: 1` for drives with locking enabled:

```
root@truenas1:~ # sedutil-cli --listLockingRange 0 abcd1234 /dev/da9
Band[0]:
    Name:            Global_Range
    CommonName:      Locking
    RangeStart:      0
    RangeLength:     0
    ReadLockEnabled: 1
    WriteLockEnabled:1
    ReadLocked:      0
    WriteLocked:     0
    LockOnReset:     1
```

Managing SED Passwords and Data

This section contains command line instructions to manage SED passwords and data. The command used is sedutil-cli(8). Most SEDs are TCG-E (Enterprise) or TCG-Opal (Opal v2.0). Commands are different for the different drive types, so the first step is identifying which type is used.

> These commands can be destructive to data and passwords. Keep backups and use the commands with caution.

Check SED version on a single drive, */dev/da0* in this example:

```
root@truenas:~ # sedutil-cli --isValidSED /dev/da0
/dev/da0 SED --E--- Micron_5N/A U402
```

All connected disks can be checked at once:

```
root@truenas:~ # sedutil-cli --scan
Scanning for Opal compliant disks
/dev/ada0 No 32GB SATA Flash Drive SFDK003L
/dev/ada1 No 32GB SATA Flash Drive SFDK003L
/dev/da0 E Micron_5N/A U402
/dev/da1 E Micron_5N/A U402
/dev/da12 E SEAGATE XS3840TE70014 0103
/dev/da13 E SEAGATE XS3840TE70014 0103
/dev/da14 E SEAGATE XS3840TE70014 0103
/dev/da2 E Micron_5N/A U402
/dev/da3 E Micron_5N/A U402
/dev/da4 E Micron_5N/A U402
/dev/da5 E Micron_5N/A U402
/dev/da6 E Micron_5N/A U402
/dev/da9 E Micron_5N/A U402
No more disks present ending scan
root@truenas:~ #
```

Instructions for Specific Drives

TCG-Opal

Reset the password without losing data with command:

```
sedutil-cli --revertNoErase <oldpassword> </dev/device>
```

Use **both** of these commands to change the password without destroying data:

```
sedutil-cli --setSIDPassword <oldpassword> <newpassword> </dev/device>
sedutil-cli --setPassword <oldpassword> Admin1 <newpassword> </dev/device>
```

Wipe data and reset password to default MSID with this command:

```
sedutil-cli --revertTPer <oldpassword> </dev/device>
```

Wipe data and reset password using the PSID with this command:

`sedutil-cli --yesIreallywanttoERASEALLmydatausingthePSID <PSINODASHED> </dev/device>` where is the PSID located on the pysical drive with no dashes (-).

TCG-E

Change or Reset the Password without Destroying Data

Run these commands for every *LockingRange* or *band* on the drive. To determine the number of bands on a drive, use command `sedutil-cli -v --listLockingRanges </dev/device>`. Increment the `BandMaster` number and rerun the command with `--setPassword` for every band that exists.

Use **all** of these commands to reset the password without losing data:

```
sedutil-cli --setSIDPassword <oldpassword> "" </dev/device>
sedutil-cli --setPassword <oldpassword> EraseMaster "" </dev/device>
sedutil-cli --setPassword <oldpassword> BandMaster0 "" </dev/device>
sedutil-cli --setPassword <oldpassword> BandMaster1 "" </dev/device>
```

Use **all** of these commands to change the password without destroying data:

```
sedutil-cli --setSIDPassword <oldpassword* newpassword */dev/device*
sedutil-cli --setPassword <oldpassword> EraseMaster <newpassword> </dev/device>
sedutil-cli --setPassword <oldpassword> BandMaster0 <newpassword> </dev/device>
sedutil-cli --setPassword <oldpassword> BandMaster1 <newpassword> </dev/device>
```

Reset Password and Wipe Data

Reset to default MSID:

```
sedutil-cli --eraseLockingRange 0 <password> </dev/device>
sedutil-cli --setSIDPassword <oldpassword> "" </dev/device>
sedutil-cli --setPassword <oldpassword> EraseMaster "" </dev/device>
```

Reset using the PSID:

```
sedutil-cli --PSIDrevertAdminSP <PSIDNODASHS> /dev/<device>
```

If it fails use:

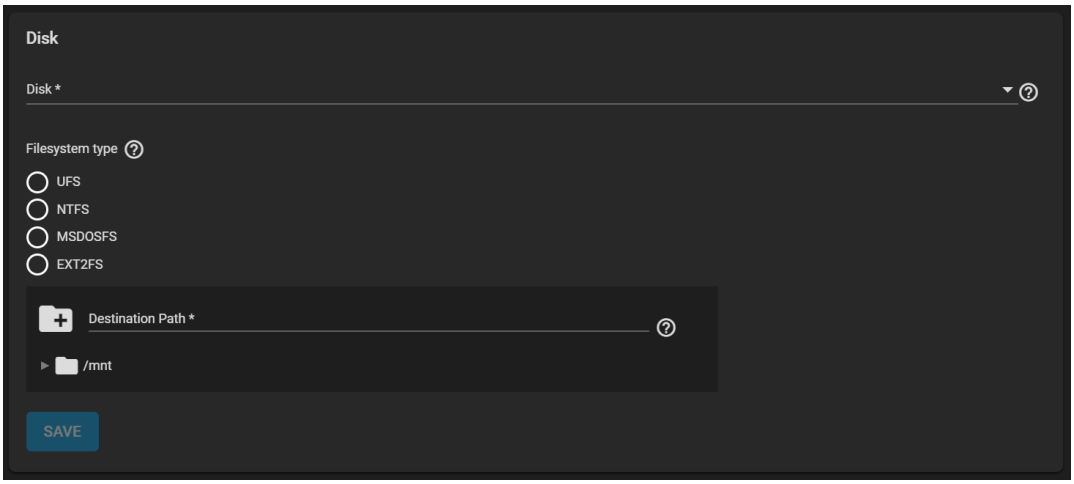
```
sedutil-cli --PSIDrevert <PSIDNODASHS> /dev/<device>
```

Import Disk

Use **Storage > Import Disk** to integrate UFS (BSD Unix), NTFS (Windows), MSDOS (FAT), or EXT2 (Linux) formatted disks into TrueNAS. This is a one-time import, copying the data from that disk into a TrueNAS dataset. Only one disk can be imported at a time, and the disk must be installed or physically connected to the TrueNAS system.

▼ What about EXT3 or EXT4 filesystems?

Importing an EXT3 or EXT4 filesystem is possible in some cases, although neither is fully supported. EXT3 journaling is not supported, so those file systems must have an external `fsck` utility, like the one provided by E2fsprogs utilities, run on them before import. EXT4 file systems with extended attributes or inodes greater than 128 bytes are not supported. EXT4 file systems with EXT3 journaling must have an `fsck` run on them before import, as described above.



Use the dropdown list to select the **Disk** to import.

TrueNAS attempts to detect and select the the **Filesystem type**. Selecting the MSDOSFS file system shows an additional **MSDOSFS locale** dropdown menu. Use this option to select the locale when non-ASCII characters are present on the disk.

Finally, browse to the ZFS dataset to hold the copied data and define the **Destination Path**.

After clicking **SAVE**, the chosen disk mounts and its contents copied to the specified dataset at the end of the entry in **Destination Path**. To monitor an in-progress import, open the **Task Manager** by clicking the in the top menu bar. The disk unmounts after the copy operation completes. A dialog allows viewing or downloading the disk import log.

▼ The import was interrupted!

Use the same import procedure to restart the task. Choose the same entry in **Destination Path** as the interrupted import for TrueNAS to scan the destination for previously imported files and resume importing any remaining files.

Directory Services

Setting Up Active Directory

The Active Directory (AD) service shares resources in a Windows network. AD provides authentication and authorization services for the users in a network. This eliminates the need to recreate the user accounts on TrueNAS.

Domain users and groups in local ACLs are accessible after joining AD. Setting up shares acts as a file server.
Joining an AD domain configures the Privileged Access Manager (PAM). This allows domain users to log on via SSH or authenticate to local services.

It is possible to configure AD services on Windows. Or on Unix-like operating systems running Samba version 4.

To configure a connection, you need to know the following items:

- Determine the Active Directory domain controller domain.
- Make sure you have the account credentials for that system.

Preparation

Preparing the following before configuring Active Directory helps ensure the connection process.

Verify Name Resolution

Confirm that name resolution is functioning. Connect to shell and use `ping` to check the connection to the AD domain controller.

```
truenas# ping ad01.lab. ixsystems.com
PING ad01. lab. ixsystems.com (10.215.5.200) : 56 data bytes
64 bytes from 10.215.5.200: icmp_seq=0 ttl=126 time=0.800 ms
64 bytes from 10.215.5.200: icmp_seq=1 ttl=126 time=0.933 ms
64 bytes from 10.215.5.200: icmp_seq=2 ttl=126 time=0.810 ms
64 bytes from 10.215.5.200: icmp_seq=3 ttl=126 time=0.876 ms
^C
ad01. lab. ixsystems.com ping statistics
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.800/0.855/0.933/0.054 ms
```

The ability to send and receive packets without loss verifies the connection. Press `Ctrl + C` to cancel the `ping`.

Another option is to use the command `host -t srv _ldap._tcp.domainname.com`. This checks the network SRV records and verifies DNS resolution.

▼ The ping failed!

If the ping fails, go to **Network > Global Configuration**. Update the **DNS Servers** and **Default Gateway** settings. Enter more than one value in **Nameserver** for the AD domain controllers.

This helps DNS queries for the required SRV records succeed. Domain controllers are not always available. Using more than one name server helps maintain the AD connection in these instances.

Time Synchronization

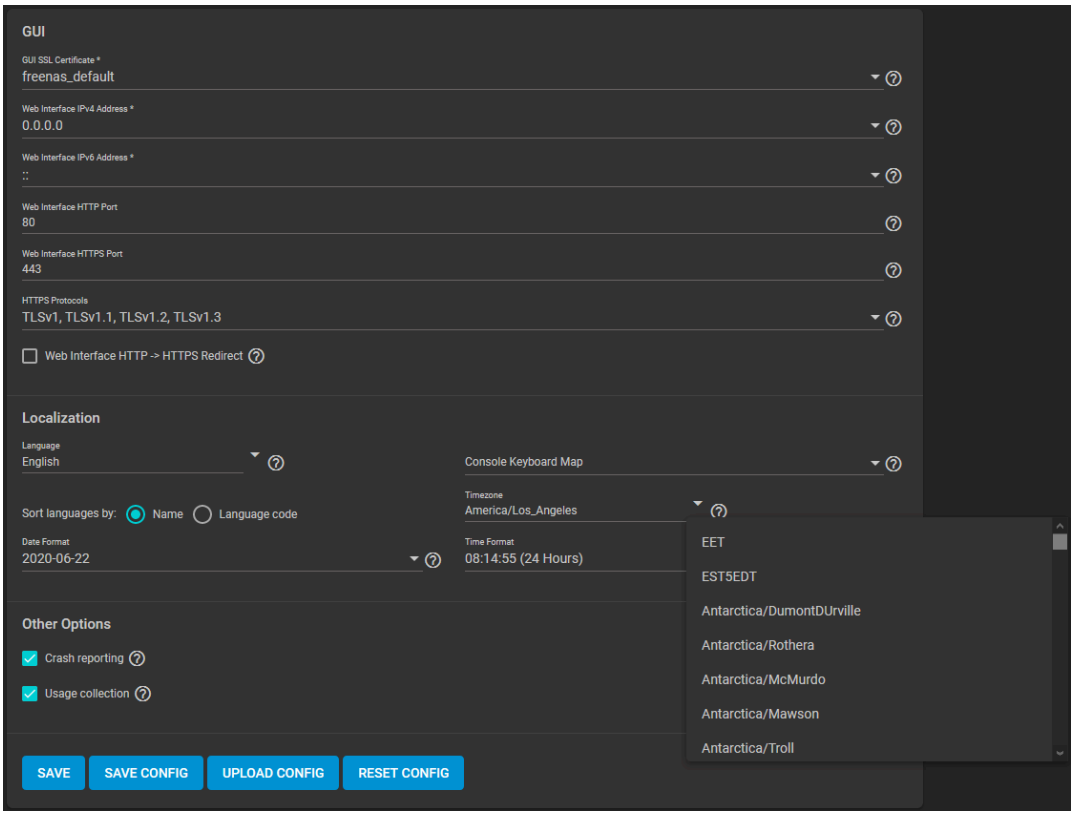
Active Directory relies on Kerberos, a time-sensitive protocol. During the domain join process, the AD domain controller with the PDC Emulator FSMO Role is added as the preferred NTP server.

You can change NTP server settings in **System > NTP Servers** if necessary.

In a default AD environment, the local system time must be in sync with the AD domain controller time. Their times cannot differ from each other by more than 5 minutes. Use an external time source when configuring a virtualized domain controller.
TrueNAS creates an **Alert** if the system time gets out of sync with the AD domain controller time.

The following options apply to time synchronization in TrueNAS:

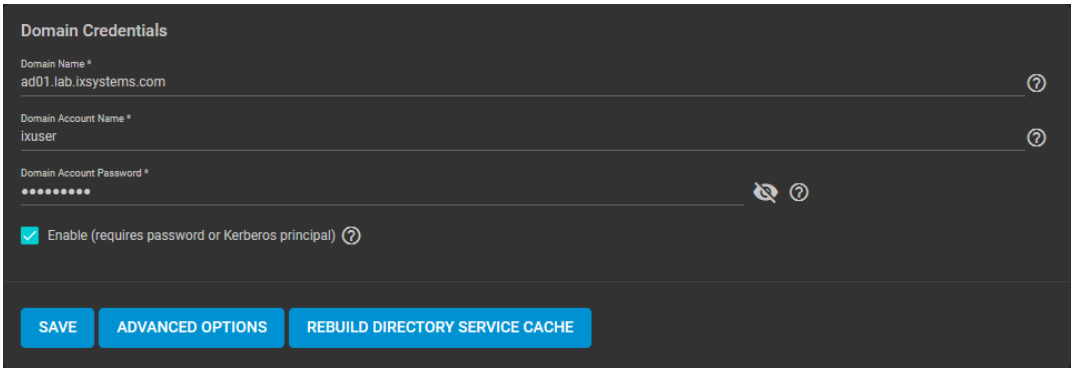
- Go to **System > General** and make sure the value in **Timezone** matches the AD Domain Controller.



- Select either local time or universal time in the system BIOS.

Connect to the Active Directory Domain

To connect to Active Directory, go to **Directory Services > Active Directory**. Enter the AD **Domain Name** and account credentials. Select **Enable** to attempt to join the AD domain immediately after saving the configuration.



The preconfigured defaults are generally suitable. Advanced options are available for fine-tuning the AD configuration. Click **ADVANCED OPTIONS** to access extra options.

Click **REBUILD DIRECTORY SERVICE CACHE** to resync the cache if it becomes out of sync. Or if fewer users than expected are available in the permissions editors.

▼ I don't see any AD information!

After configuring the Active Directory service, there can be a delay. TrueNAS can take a few minutes to populate the AD information. To check the AD join progress, open the **Task Manager** in the upper-right corner. TrueNAS displays any errors during the join process in the **Task Manager**.

When the import completes, AD users and groups become available. These have basic dataset permissions or an Access Control List (ACL). Enabled is the default status for the TrueNAS cache.

Joining AD adds default Kerberos realms and generates a default `AD_MACHINE_ACCOUNT` keytab. TrueNAS automatically begins using this default keytab. TrueNAS removes any administrator credentials stored in the TrueNAS configuration file.

Related Services: FTP Access

The recommendation is to use SFTP over FTP. But joined systems do allow FTP access. Keep these caveats in mind:

- Authentication uses *DOMAIN\username* as the user name by default.
- A user home directory needs to exist before joining.
- You cannot add an AD user to the FTP group. Enable local user auth for FTP instead.

- An existing samba homes share created in the GUI is set as the *template homedir* for AD users. This means that AD user home directories are set inside that path. Proper permissions are vital.
- There are no guarantees about how `proftpd` handles ACLs.
- AD users can have populated homedir information in their LDAP schema. The admin (or `pam_mkhomedir`) must ensure that these paths exist.
- When the admin is pulling home directories from their LDAP schema, take an extra step of caution. Ensure that users aren't writing files to the boot device.

Troubleshooting

Resync the cache if it becomes out of sync. Or if fewer users than expected are available in the permissions editors. Go to **Directory Services > Active Directory > REBUILD DIRECTORY SERVICE CACHE**.

If you are using Windows Server with 2008 R2 or older, try the following options:

Create a **Computer** entry on the Windows server Organizational Unit (OU). When creating this entry, enter the TrueNAS host name in the name field. Make sure it is the same name as the one set in the **Hostname** field in **Network > Global Configuration**. Must match the **NetBIOS alias** from **Directory Services > Active Directory > Advanced Options**.

▼ Shell Commands

You can enter various shell commands to get more details about the AD connection and users:

- AD current state: `midclt call activedirectory.get_state`.
- Details about the currently connected Lightweight Directory Access Protocol (LDAP) server: `midclt call activedirectory.domain_info | jq`. Example:

```
truenas# midclt call activedirectory.domain_info | jq
{
  "LDAP server": "192.168.1.125",
  "LDAP server name": "DC01.HOMEDOM.FUN",
  "Realm": "HOMEDOM.FUN",
  "Bind Path": "dc=HOMEDOM,dc=FUN",
  "LDAP port": 389,
  "Server time": 1593026080,
  "KDC server": "192.168.1.125",
  "Server time offset": 5,
  "Last machine account password change": 1592423446
}
```

- View AD users: `wbinfo -u`. To see more details about a user, enter `getent passwd DOMAIN\\<user>`. Replace `<user>` with the desired user name. With the TrueNAS cache enabled `wbinfo -u` can show more users than appear to be available when configuring permissions. Go to **Directory Services > Active Directory** and increase the *AD Timeout* value.
- View AD groups: `wbinfo -g`. To see more details, enter `getent group DOMAIN\\domain\ users`.
- View domains: `wbinfo -m`.
- Test AD connection: `wbinfo -t`. A successful test shows a message similar to `checking the trust secret for domain YOURDOMAIN via RPC calls succeeded`.
- User connection test to an SMB share: `smbclient '//127.0.0.1/smbshare -U AD01.LAB.IXSYSTEMS.COM\ixuser`, replacing `127.0.0.1` with your server address, `smbshare` with the SMB share name, `AD01.LAB.IXSYSTEMS.COM` with your trusted domain, and `ixuser` with the user account name for authentication testing.

Setting Up LDAP

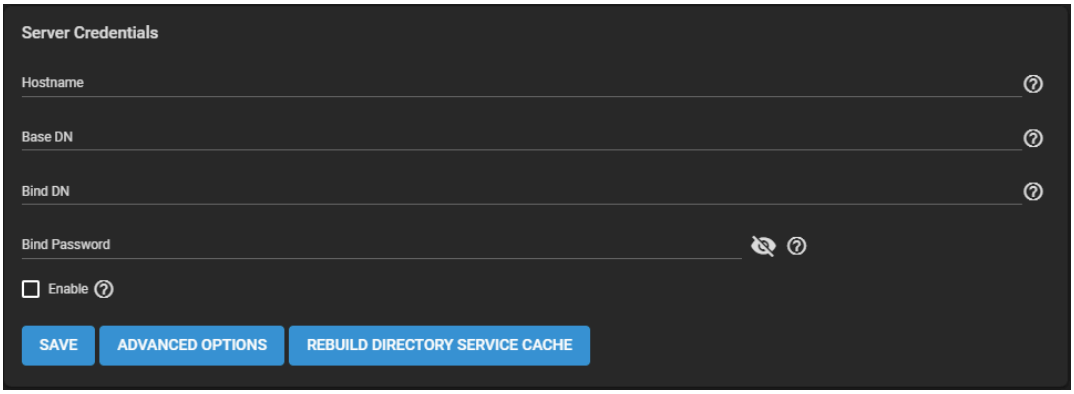
Lightweight Directory Access Protocol (LDAP) is an open and cross-platform protocol. It is often used to centralize authentication. TrueNAS includes an Open LDAP client for accessing information from an LDAP server. An LDAP server provides directory services for finding network resources. This includes finding users and their associated permissions.

▼ Does LDAP work with SMB?

LDAP authentication for SMB shares is not enabled. To enable, first determine if LDAP authentication for SMB shares is a requirement. If so, configure the LDAP directory and populate it with Samba attributes. The most popular script for performing this task is `smbldap-tools`. The LDAP server must support SSL/TLS. Import the certificate for the LDAP server CA. Non-CA certificates are not currently supported.

Integrating an LDAP Server with TrueNAS

To integrate an LDAP server with TrueNAS, go to **Directory Services > LDAP**.



Enter any LDAP server host names or IP addresses. Separate entries with an empty space. Entering more than one host name or IP address creates an LDAP failover priority list.

▼ What does this do?

If a host does not respond, the system tries the next host in the list until it establishes a new connection.

Enter the **Base DN**. This is the top level of the LDAP directory tree used when searching for resources. For example, `dc=test,dc=org`.

Enter the **Bind DN**. This is the administrative account name on the LDAP server. For example, `cn=Manager,dc=test,dc=org`.

Enter the **Bind Password**. This is the password associated with the account in **Bind DN**.

The final basic option is **Enable**. Clearing the **Enable** checkbox disables the LDAP configuration without deleting it. Enable it at a later time without reconfiguring the options.

To make further changes to the LDAP configuration, click **ADVANCED OPTIONS**.

See LDAP Screen for information on basic and advanced option settings.

See Kerberos for more information on using Kerberos.

To configure LDAP certificate-based authentication for the LDAP provider to sign, see Certificate Signing Requests.

> Samba 4.13.0 deprecated **Samba Schema**. Select if SMB shares need LDAP authentication and the LDAP server is already configured with Samba attributes. If selected, specify the type of schema from the **Schema** dropdown list.

Setting up NIS

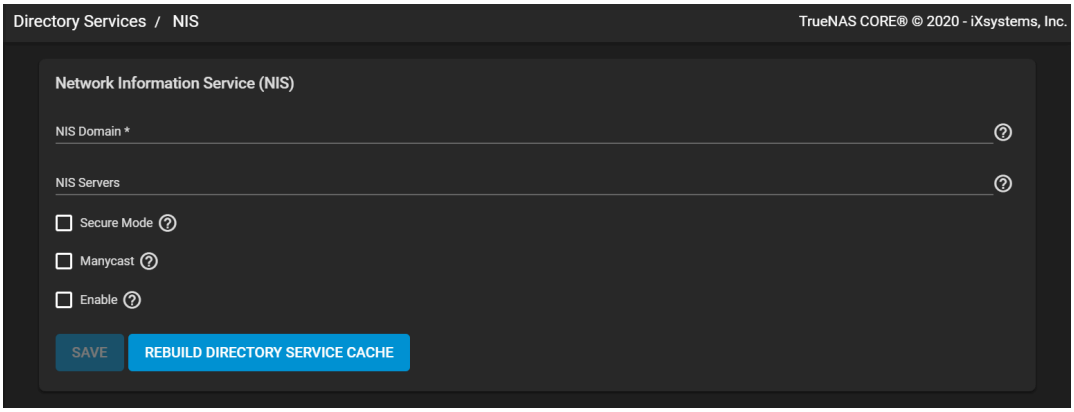
NIS (Network Information Service) is a clientвЂ“server directory service protocol. It assists in distributing system configuration data between computers on a network. This data can include user and host names.

▼ What exactly does this do?

A NIS system maintains and distributes a central directory. This central directory contains user and group information. It also contains other text-based tables of information. These tables can include host names and e-mail aliases. In FreeBSD, the file /etc/passwd contains the list of users. The file /etc/shadow contains the authentication hashes. NIS adds another global user list to identify users on any NIS domain client.

> NIS is limited in scalability and security. For modern networks, LDAP has replaced NIS.

To configure NIS, go to **Directory Services > NIS**.



Enter the **NIS Domain** name and list any **NIS Servers** (host names or IP addresses). Press `Enter` to separate server entries. Configure the remaining options as needed:

- **Secure Mode** : Select to have ypbind(8) refuse to bind to any NIS server not running as *root* on a TCP port over **1024**.
- **Manycast** : Select for `ypbind` to bind to the fastest responding server.
- **Enable** : Leave the checkbox clear to disable the configuration without deleting it.

Click **SAVE** to save configuration settings.

Click **REBUILD DIRECTORY SERVICE CACHE** to resync the cache if it becomes out of sync. Or if fewer users than expected are available in the permissions editors.

Setting Up Kerberos

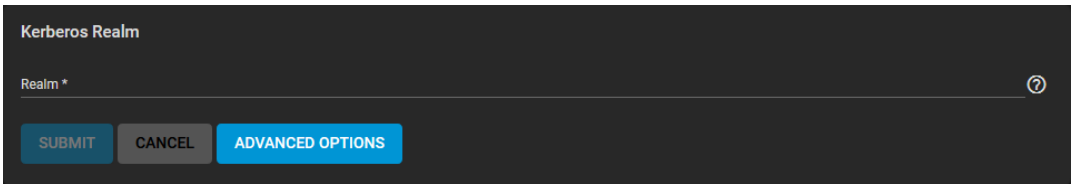
Kerberos is a web authentication protocol that uses strong cryptography. It proves the identity of both client and server over an insecure network connection.

Kerberos uses *realms* and *keytabs* to authenticate clients and servers. A Kerberos realm is an authorized domain that a Kerberos server can use to authenticate a client. Kerberos keytabs allow systems and clients to join an Active Directory or LDAP. Keytabs make it possible to join without entering a password.

TrueNAS allows configuring both Kerberos realms and keytabs.

Kerberos Realms

Your network must contain a Key Distribution Center (KDC) to add a realm. Users can configure Kerberos realms. Go to **Directory Services** > Kerberos Realms** and click **ADD**. By default, TrueNAS creates a Kerberos realm for the local system.



Enter the **Realm** name and click **SUBMIT**.

See Kerberos Screens for more information on Kerberos screens and settings.

Kerberos Keytabs

Kerberos keytabs allow systems and clients to join an Active Directory or LDAP. Keytabs make it possible to join without entering a password. A keytab (key table) is a file that stores encryption keys for various authentication scenarios. With keytabs, the TrueNAS system database benefits from this security feature. It does not store the Active Directory or LDAP administrator account password. This could be a security risk in some environments.

When using a keytab, create and use a less privileged account to perform any required queries. The TrueNAS system database stores the password for that account.

Create Keytab on Windows Server for Active Directory

To create the keytab on a Windows Server system, open a command prompt and use the `ktpass` command:

`ktpass -princ USERNAME@REALM.COM -pass PASSWORD -crypto ENCRYPTION TYPE -ptype KRB5_NT_PRINCIPAL -kvno 0 -out c:\PATH\KEYTABNAME.KEYTAB` where `USERNAME@REALM.COM` is the Windows Server user and principal name written in the format `username@KERBEROS.REALM`. The Kerberos realm is typically in all caps, but the Kerberos realm case should match the realm name. Refer to this note about using `/princ` for more details.

`PASSWORD` is the Windows Server user password.

`ENCRYPTION TYPE` is the cryptographic type you want to use. Setting `ENCRYPTION TYPE` to `ALL` allows using all supported cryptographic types. Users can specify each key instead of ALL:

- **DES-CBC-CRC** is used for compatibility.
- **DES-CBC-MD5** is used for compatibility and adheres more closely to the MIT implementation.
- **RC4-HMAC-NT** uses 128-bit encryption.
- **AES256-SHA1** uses AES256-CTS-HMAC-SHA1-96 encryption.
- **AES128-SHA1** uses AES128-CTS-HMAC-SHA1-96 encryption.

Specifying cryptographic types creates a keytab with enough privileges to grant tickets.

`PATH\KEYTABNAME.KEYTAB` is the path where you want to save the keytab and the name you want it to have.

▼ Example ktpass Command

```
ktpass -princ admin@WINDOWSSERVER.NET -pass Abcd1234! -crypto ALL -ptype KRB5_NT_PRINCIPAL -kvno 0 -out
c:\kerberos\freenas.keytab
```

Add Windows Keytab to TrueNAS

After generating the keytab, add it to the TrueNAS system in **Directory Services > Kerberos Keytabs > Add Kerberos Keytab**.

To instruct the Active Directory service to use the keytab, go to **Directory Services > Active Directory** and click **Advanced Options**. Select the installed keytab using the **Kerberos Principal** dropdown list.

When using a keytab with Active Directory, **username** and **userpass** in the keytab should match the **Domain Account Name** and **Domain Account Password** fields in **Directory Services > Active Directory**.

To instruct LDAP to use a principal from the keytab, go to **Directory Services > Active Directory**. Click **Advanced Options**, then select the installed keytab using the **Kerberos Principal** dropdown list.

Sharing

File sharing is a core benefit of a NAS. TrueNAS helps foster collaboration between users through network shares. TrueNAS can use AFP, iSCSI shares, Unix NFS shares, Windows SMB shares, and WebDAV shares.

AFP Share Creation

The Apple Filing Protocol (AFP) is a network protocol that allows file sharing over a network. It is like SMB and NFS, but it is for Apple systems.

> Apple began using the SMB sharing protocol as the default option for file sharing in 2013. At that time Apple ceased development of the AFP sharing protocol. The recommendation is to use SMB sharing instead of AFP. AFP sharing is still used if files are being shared with legacy Apple products. Please see https://en.wikipedia.org/wiki/Apple_Filing_Protocol and https://appleinsider.com/articles/13/06/11/apple-shifts-from-afp-file-sharing-to-smb2-in-os-x-109-mavericks

To create a new share, make sure a dataset is available with all the data for sharing.

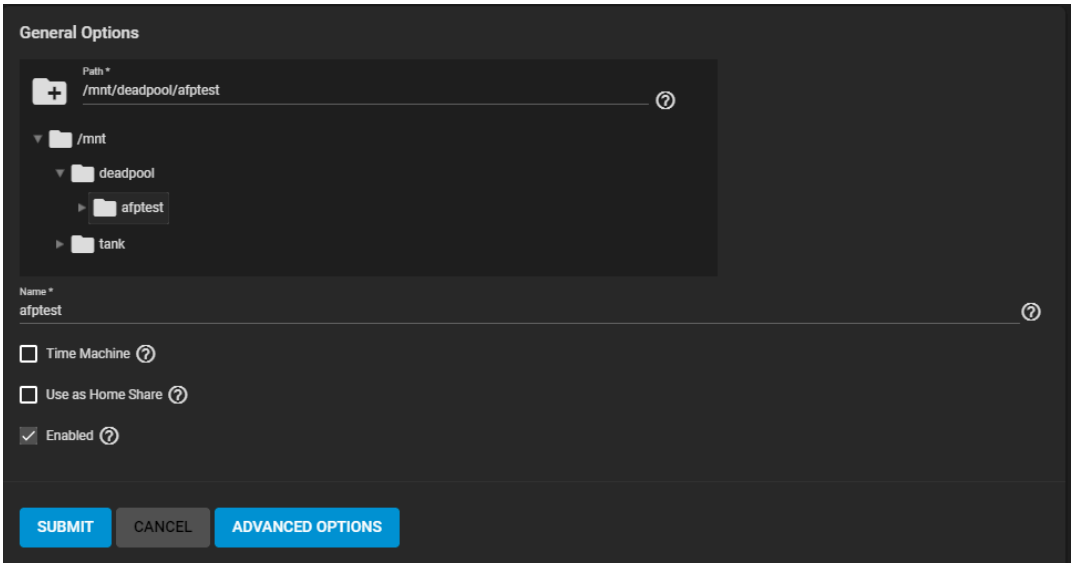
AFP Share Configuration

To configure the new share, go to **Sharing > Apple Shares (AFP)** and click **ADD**. Because AFP sharing is deprecated, confirm that you intend to create an AFP share. Next, use the file browser to select a dataset to share and enter a descriptive name for the share in **Name**.

Select **Time Machine** if the share is to have Apple Time Machine backups. This advertises the share to other Mac systems as a disk that stores Time Machine backups. Having multiple AFP shares configured for Time Machine backups is not recommended.

Select **Use as Home Share** to create home directories for users that connect to the share. Only one AFP share can be a home share.

The AFP share is enabled by default. To create the share but not immediately enable it, clear **Enabled**. Clicking **SUBMIT** creates the share.



See Sharing AFP screen for more information on screen settings.

To edit an existing AFP share, go to **Sharing > Apple Shares (AFP)** and click ⋮.

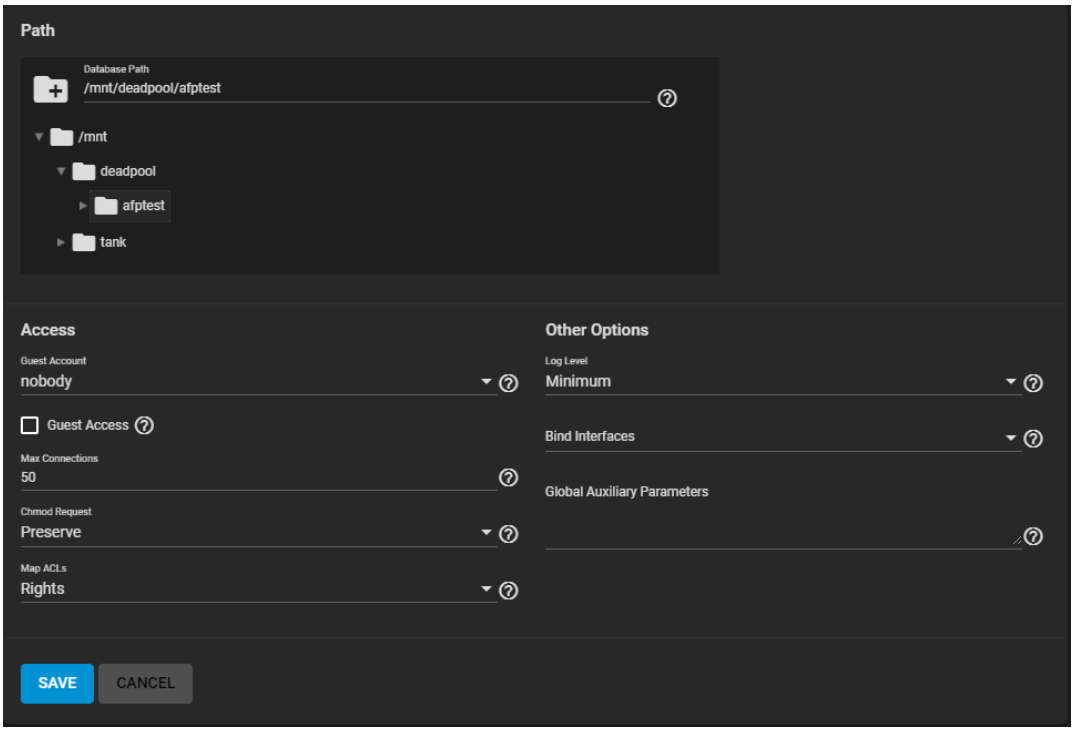
Start or Stop AFP Service

To begin advertising the AFP shared location, go to **Services**. To determine the current state of the AFP service, hover the mouse over the toggle. The toggle turns blue when it is running. Click the AFP toggle to start the service if it is not running, or to stop the service if it is already running. To automatically start the service after TrueNAS boots, select **Start Automatically**.

Changing AFP Service settings

If the AFP service is running, stop it before attempting to edit settings.

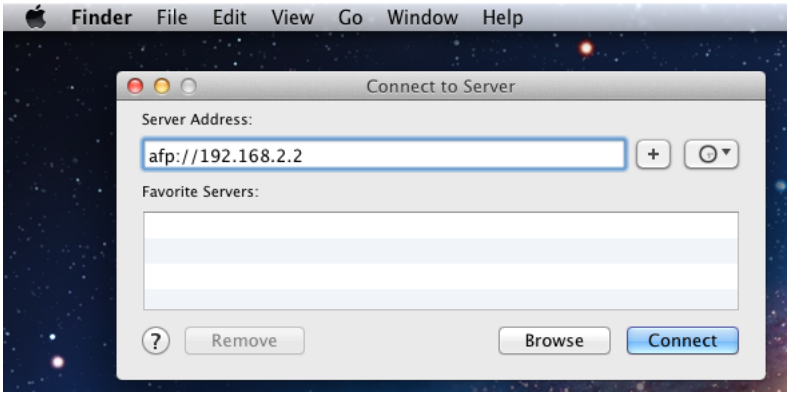
It is recommended to use the default settings for the AFP service. To adjust the service settings, click the ✎ icon.



See Adding AFP Service for more information on AFP service settings.

Connecting to the AFP Share

Use an Apple operating system to connect to the share. Open the **Finder** app on the Mac and click **Go > Connect to Server…** in the top menu bar on the Mac. Enter `afp://{IPofTrueNASsystem}` and click **Connect**. For example, entering `afp://192.168.2.2` connects to the TrueNAS AFP share at 192.168.2.2.



Block Shares (iSCSI)

Internet Small Computer Systems Interface (iSCSI) represents standards for using Internet-based protocols for linking binary data storage device aggregations. IBM and Cisco submitted the draft standards in March 2000. Since then, iSCSI has seen widespread adoption into enterprise IT environments.

iSCSI functions through encapsulation. The *Open Systems Interconnection Model* (OSI) encapsulates SCSI commands and storage data within the session stack. The OSI further encapsulates the session stack within the transport stack, the transport stack within the network stack, and the network stack within the data stack. Transmitting data this way permits block-level access to storage devices over LANs, WANs, and even the Internet itself (although performance may suffer if your data traffic is traversing the Internet).

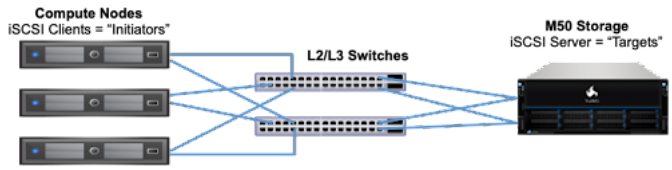
The table below shows where iSCSI sits in the OSI network stack:

OSI Layer Number	OSI Layer Name	Activity as it relates to iSCSI
7	Application	An application tells the CPU that it needs to write data to non-volatile storage.
6	Presentation	OSI creates a SCSI command, SCSI response, or SCSI data payload to hold the application data and communicate it to non-volatile storage.
5	Session	Communication between the source and the destination devices begins. This communication establishes when the conversation starts, what it talks about, and when the conversion ends. This entire dialogue represents the session. OSI encapsulates the SCSI command, SCSI response, or SCSI data payload containing the application data within an iSCSI Protocol Data Unit (PDU).
4	Transport	OSI encapsulates the iSCSI PDU within a TCP segment.
3	Network	OSI encapsulates the TCP segment within an IP packet.
2	Data	OSI encapsulates the IP packet within the Ethernet frame.
1	Physical	The Ethernet frame transmits as bits (zeros and ones).

Unlike other sharing protocols on TrueNAS, an iSCSI share allows block sharing *and* file sharing. Block sharing provides the benefit of block-level access to data on the TrueNAS. iSCSI exports disk devices (zvols on TrueNAS) over a network that other iSCSI clients (initiators) can attach and mount.

▼ iSCSI Terminology

- **Challenge-Handshake Authentication Protocol (CHAP)**: an authentication method that uses a shared secret and three-way authentication to determine if a system is authorized to access the storage device. It also periodically confirms that the session has not been hijacked by another system. In iSCSI, the client (initiator) performs the CHAP authentication.
- **Mutual CHAP**: a CHAP type in which both ends of the communication authenticate to each other.
- **Internet Storage Name Service (iSNS)**: protocol for the automated discovery of iSCSI devices on a TCP/IP network.
- **Extent**: the storage unit to be shared. It can either be a file or a device.
- **Portal**: indicates which IP addresses and ports to listen on for connection requests.
- **Initiators and Targets**: iSCSI introduces the concept of *initiators* and *targets* which act as sources and destinations respectively. iSCSI initiators and targets follow a client/server model. Below is a diagram of a typical iSCSI network. The TrueNAS storage array acts as the iSCSI target and can be accessed by many of the different iSCSI initiator types, including software and hardware-accelerated initiators.



The iSCSI protocol standards require that iSCSI initiators and targets is represented as iSCSI nodes. It also requires that each node is given a unique iSCSI name. To represent these unique nodes via their names, iSCSI requires the use of one of two naming conventions and formats, IQN or EUI. iSCSI also allows the use of iSCSI aliases which are not required to be unique and can help manage nodes.

- **Logical Unit Number (LUN)**: LUN represents a logical SCSI device. An initiator negotiates with a target to establish connectivity to a LUN. The result is an iSCSI connection that emulates a connection to a SCSI hard disk. Initiators treat iSCSI LUNs as if they were a raw SCSI or SATA hard drive. Rather than mounting remote directories, initiators format and directly manage filesystems on iSCSI LUNs. When configuring multiple iSCSI LUNs, create a new target for each LUN. Since iSCSI multiplexes a target with multiple LUNs over the same TCP connection, there can be TCP contention when more than one target accesses the same LUN. TrueNAS supports up to 1024 LUNs.
- **Jumbo Frames**: Jumbo frames are the name given to Ethernet frames that exceed the default 1500 byte size. This parameter is typically referenced by the nomenclature as a maximum transmission unit (MTU). A MTU that exceeds the default 1500 bytes necessitates that all devices transmitting Ethernet frames between the source and destination support the specific jumbo frame MTU setting, which means that NICs, dependent hardware iSCSI, independent hardware iSCSI

cards, ingress and egress Ethernet switch ports, and the NICs of the storage array must all support the same jumbo frame MTU value. So, how does one decide if they should use jumbo frames?

Administrative time is consumed configuring jumbo frames and troubleshooting if/when things go sideways. Some network switches might also have ASICs optimized for processing MTU 1500 frames while others might be optimized for larger frames. Systems administrators should also account for the impact on host CPU utilization. Although jumbo frames are designed to increase data throughput, it may measurably increase latency (as is the case with some un-optimized switch ASICs); latency is typically more important than throughput in a VMware environment. Some iSCSI applications might see a net benefit running jumbo frames despite possible increased latency. Systems administrators should test jumbo frames on their workload with lab infrastructure as much as possible before updating the MTU on their production network.

iSCSI Configuration Methods

There are a few different approaches for configuring and managing iSCSI-shared data:

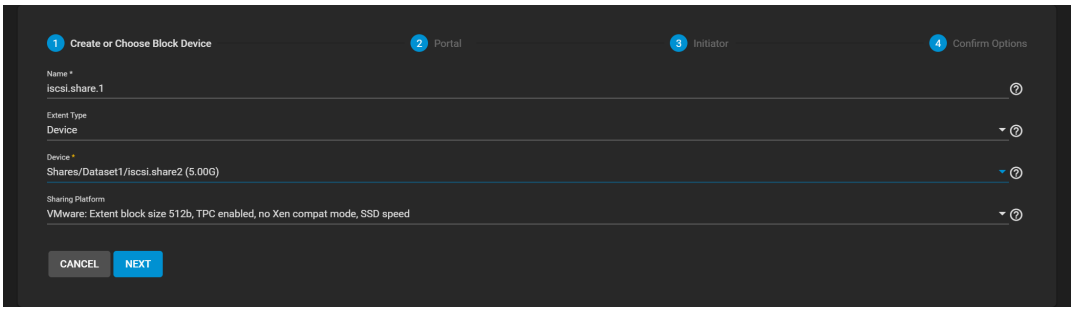
- TrueNAS CORE web interface: the TrueNAS web interface is fully capable of configuring iSCSI shares. This requires creating and populating zvol block devices with data, then setting up the iSCSI Share. TrueNAS Enterprise licensed customers also have additional options to configure the share with Fibre Channel.
- TrueNAS SCALE web interface: TrueNAS SCALE offers a similar experience to TrueNAS CORE for managing data with iSCSI; create and populate the block storage, then configure the iSCSI share.

Adding an iSCSI Share

To get started, make sure you have created a zvol or a dataset with at least one file to share.

Go to **Sharing > Block Shares (iSCSI)**. You can either set one up manually or use **WIZARD** to guide you through creation.

Wizard Setup Process



On **Create or Choose Block Device**:

1. Enter a name for the iSCSI share. It can only contain lowercase alphanumeric characters plus a dot (.), dash (-), or colon (:). We recommend keeping the name short or at most 63 characters.
2. Choose the **Extent Type**.
   - If the **Extent Type** is **Device**, select the Zvol to share from the **Device** menu.
   - If the **Extent Type** is **File**, select the path to the extent and indicate the file size.
3. Select the type of platform to use for the share. For example, if using the share from an updated Linux OS, choose **Modern OS**.
4. Click **Next**. The **Portals** screen displays.
5. Select an existing portal or click **Create New** to add a portal.

   If you create a new portal, you must select a discovery authentication method.

   a. Select either **CHAP** or **MUTUAL CHAP** in the **Discovery Authentication Method** field.

   b. Select either **None** or **Create New** in the **Discovery Authentication Group** field. **Create New** displays additional configuration fields. If you select **None** you can leave **Discovery Authentication Group** empty.

   c. Enter a number in the **Group ID** field to identify the group.

   d. Enter the user name in the **User** field. This can be the same as the initiator.

   e. Enter a password of 12 to 16 characters in the **Secret** field and again in **Secret (Confirm)**.

   f. Select the IP address(es) to use. If adding more than one IP address, click **ADD** and then select the IP address. Use **0.0.0.0.** to listen on all IPv4 or **::** to listen on all IPv6 IP addresses.

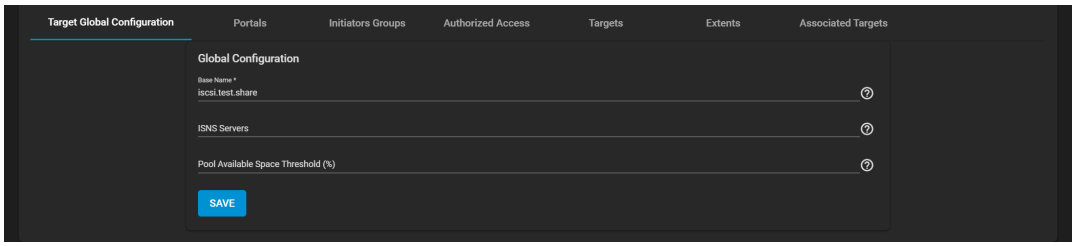
   G. Select the TCP port number to use if different from the default.

   H. Click Next to display the **Initiator** screen.
6. Enter the initiator information to use. Decide which initiators or networks can use the iSCSI share. Leave the list empty to allow all initiators or networks, or add entries to the list to limit access to those systems. Use the keyboard `Enter` between each entry. Click **Next** to display the **Confirm Options** screen.
7. Confirm the settings you entered. To change any setting click **BACK** until you see the screen where you want to make changes.
8. Click **SUBMIT** to save the iSCSI block share.

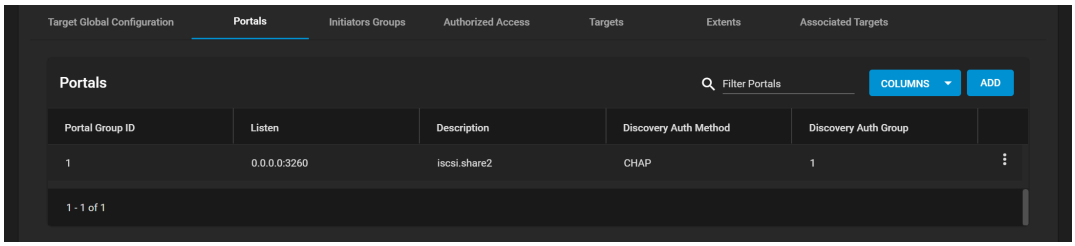
Manual Setup Process

To add or edit an existing iSCSI share, use the seven tab to access the various iSCSI configuration screens.

1. Configure the share global configuration settings. Click the **Target Global Configuration** tab.



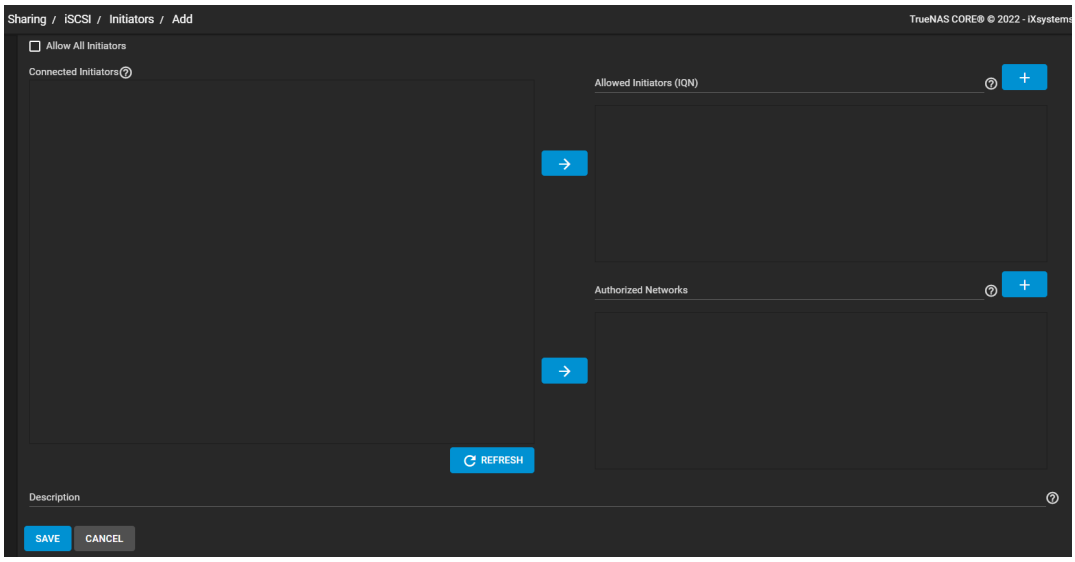
2. Configure the portal settings. Click on the **Portals** tab.



To add a new portal, click **ADD** and enter the basic and IP address information.

To edit an existing portal, click ⋮ next to the portal and select **Edit**.

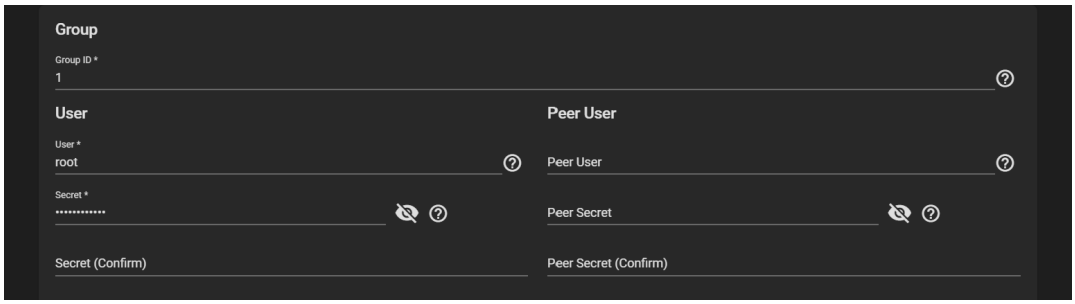
3. Configure the initiator settings (not required). Click on the **Initiators Groups** tab. Both the **Add** and **Edit** forms have the same settings fields.



Use **ADD** to display the **Initiators Add** configuration screen. Either leave **Allow All Initiators** checked or configure your own allowed initiators and authorized networks.

Click the ⋮ icon for the initiator group and select **Edit** to display the **Initiator Group Edit** configuration screen.

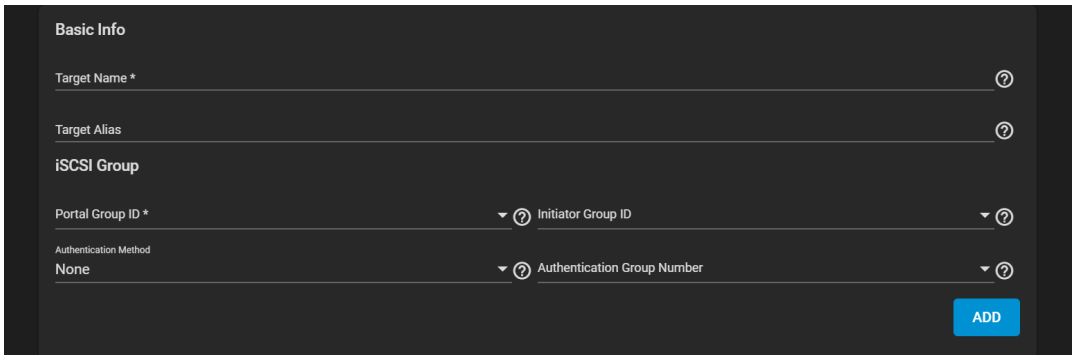
4. Configure authorized access networks. Click the **Authorized Access** tab.



Click **ADD** to add a new authorized access network. Fill out the group, user and peer user information.

Click ⋮ next to the authorized access network and select **Edit**.

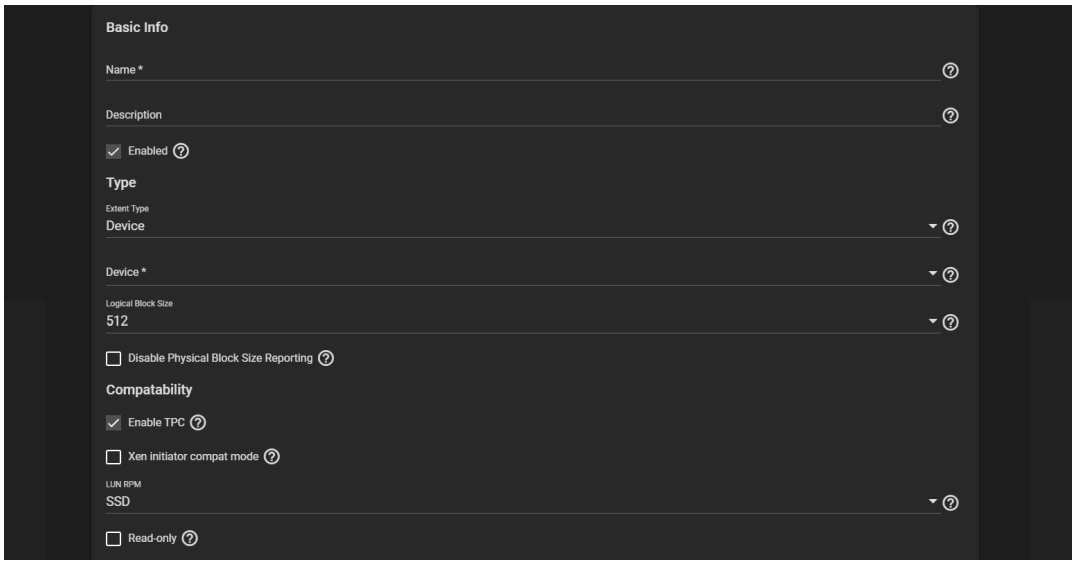
5. Configure targets. Click the **Targets** tab.



To add a new target, click **ADD** and enter the basic and iSCSI group information.

To edit an existing target, click ⋮ next to it and select **Edit**.

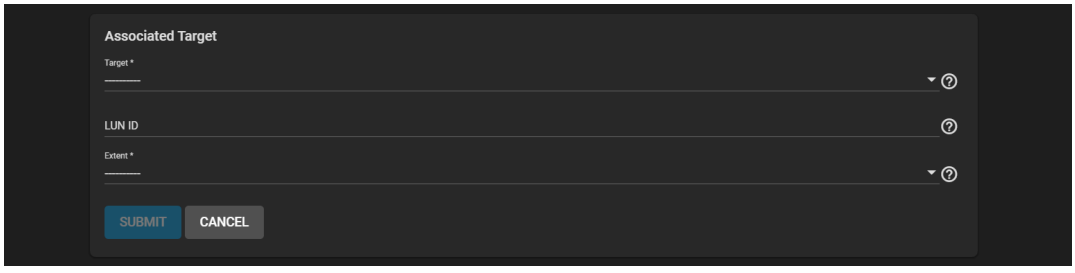
6. Configure extents. Click the **Extents** tab.



To add a new extent, click **ADD** and enter the basic, type, and compatibility information.

To edit an existing extent, click ⋮ next to it and select **Edit**.

7. Configure any associated targets. Click on the **Associated Targets** tab.



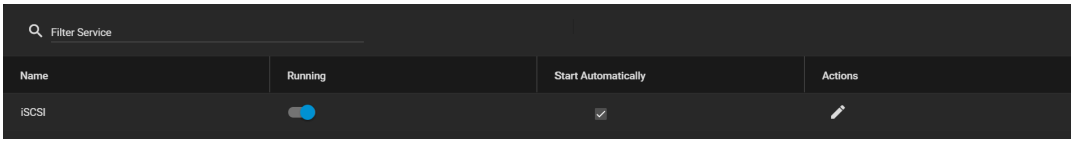
To add a new associated target, click **ADD** and fill out the information.

To edit an existing associated target, click ⋮ next to it and select **Edit**.

Starting the iSCSI Service

To turn on the iSCSI service, go to **Services** locate **iSCSI** and click on the toggle. It should display the status **Running**.

To set it to start automatically when TrueNAS boots up, select the **Start Automatically** checkbox.



Click on the ✎ returns to the options in **Sharing > iSCSI**.

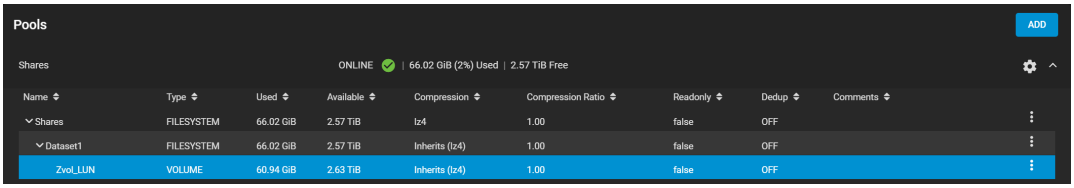
Increasing iSCSI Share Available Storage

Expanding LUNs

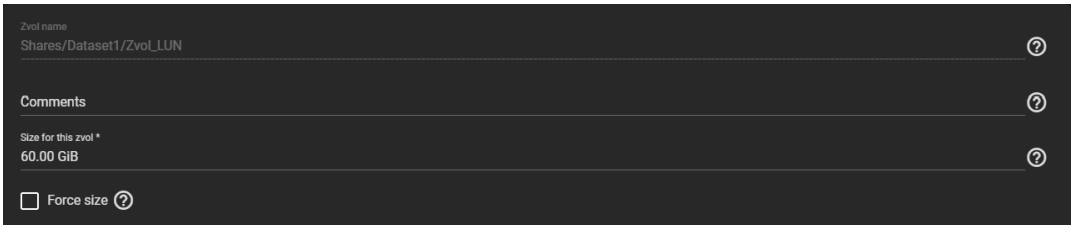
TrueNAS lets users expand Zvol and file-based LUNs to increase the available storage that the iSCSI shares.

Expanding Zvol LUNs

To expand a Zvol LUN, go to **Storage > Pools** and click the ⋮ next to the Zvol LUN, then select **Edit Zvol**.



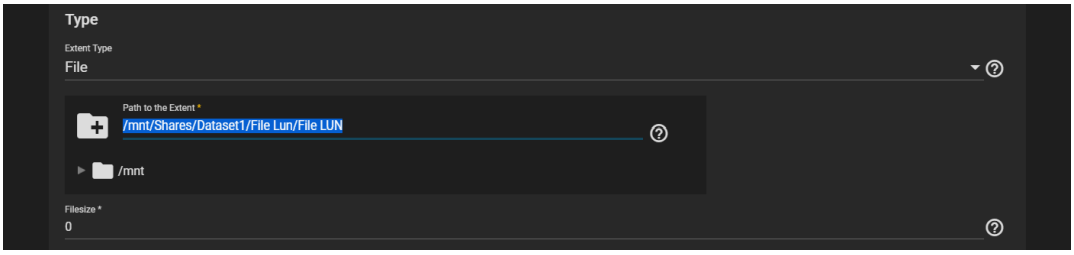
Enter a new size in the **Size for this zvol** field, then click **SAVE**.



> To prevent data loss, the web interface does not allow users to reduce the Zvol size. TrueNAS also does not allow users to increase the Zvol size past 80% of the pool size.

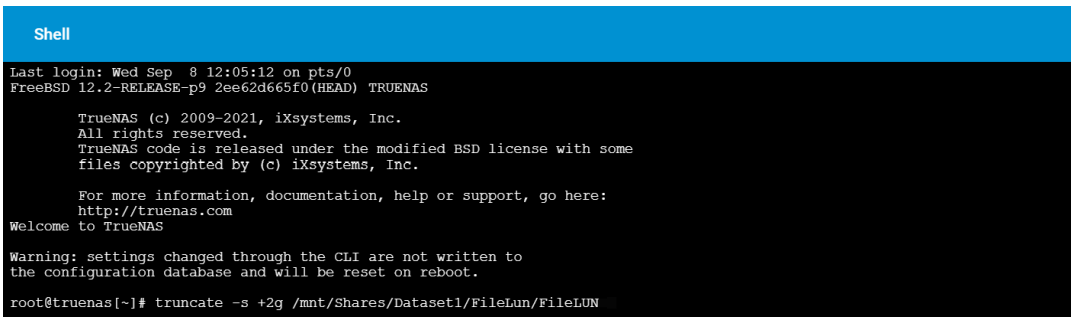
Expanding a File-Based LUN

To expand a file-based LUN, you need to know the path to the file. To find the path, go to **Sharing > Block Shares (iSCSI)** and click the **Extents** tab. Click the ⋮ next to the file-based LUN and select **Edit**.



Highlight and copy the path, then click **CANCEL**

Go to the shell and enter `truncate -s +size path/to/file` where *size* is how much space you want to grow the file by, and *path/to/file* is the file path you copied earlier, then press `Enter`.



An example of the command could look like this: `truncate -s +2g /mnt/Shares/Dataset1/FileLun/FileLUN`

Lastly, go back to the extent in **Sharing > Block Shares (iSCSI)** and make sure the **Filesize** is set to **0** so that the share uses the actual file size.

Using the iSCSI Share

Using the iSCSI Share

Connecting to and using an iSCSI share can differ between operating systems. This article provides instructions for Linux and Windows.

▼ Configuring Linux to Use the iSCSI Share

iSCSI Utilities and Service

First, open the command line and ensure that the `open-iscsi` utility is installed.

To install the utility on an Ubuntu/Debian distribution, enter command `sudo apt update && sudo apt install open-iscsi`. After the installation completes, ensure the iscsid service is running with command `sudo service iscsid start`. With the iscsid service started, run the command `iscsiadm` with the discovery arguments and get the necessary information to connect to the share.

```
truenas@LinuxMachine:~$ sudo apt update && sudo apt install open-iscsi
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:1 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:1 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:1 http://us.archive.ubuntu.com/ubuntu focal-security InRelease
Reading package lists... Done
```

Discover and Log In to the iSCSI Share

Run the command `sudo iscsiadm \--mode discovery \--type sendtargets \--portal {IPADDRESS}` where `{IPADDRESS}` is IP address (without curly brackets) you configured in the UI on the **iSCSI > Portals > Add** screen. The output provides the base name and target name that TrueNAS configured.

```
truenas@LinuxMachine:~$ sudo iscsiadm \--mode discovery \--type sendtargets \--portal 10.10.10.
10.238.15.118:3260,-1 iqn.2005-10.org.freenas.ctl:iscsishare
10.238.15.118:3260,-1 iqn.2005-10.org.freenas.ctl:iscsishare2
10.238.15.118:3260,-1 iqn.2005-10.org.freenas.ctl:iscsifile
truenas@LinuxMachine:~$
```

Alternatively, to get the same output enter command `sudo iscsiadm -m discovery -t st -p {IPADDRESS}` where `{IPADDRESS}` is IP address (without curly brackets) you configured for the iSCSI share. Note the base name and target name given in the output, since you need them to log in to the iSCSI share.

When a portal discovery authentication method** set to CHAP (on the UI **Sharing > iSCSI> Portals** screen), add the three following command lines to /etc/iscsi/iscsid.conf.

```
discovery.sendtargets.auth.authmethod = CHAP
discovery.sendtargets.auth.username = user
discovery.sendtargets.auth.password = secret
```

The user for command `discovery.sendtargets.auth.username` is set in the authorized access used by the portal of the iSCSI share (UI **iSCSI > Portals**). Likewise, the password to use for command `discovery.sendtargets.auth.password` is the in the **iSCSI > Authorized Access** screen **Secret** field. Without those lines, the iscsiadm does not discover the portal configured to use the CHAP authentication method.

Next, enter command `sudo iscsiadm \--mode node \--targetname {BASENAME}:{TARGETNAME} \--portal {IPADDRESS} \--login`, where `{BASENAME}` and `{TARGETNAME}` (without curly brackets) is the information from the discovery command.

```
truenas@LinuxMachine:~$ sudo iscsiadm \--mode discovery \--type sendtargets \--portal freenas.local
freenas.local:3260,-1 iqn.2005-10.org.freenas.ctl:iscsi.share
truenas@LinuxMachine:~$ sudo iscsiadm \--mode node \--targetname iqn.2005-10.org.freenas.ctl:iscsi.
share \--portal freenas.local \--login
Loggin in to [iface: default, target: iqn.2005-10.org.freenas.ctl:iscsi.share, portal: freenas.loca
l,3260] (multiple)
Login to [iface: default, target: iqn.2005-10.org.freenas.ctl:iscsi.share, portal: freenas.local,32
60] successful.
truenas@LinuxMachine:~$
```

Partition iSCSI Disk

When the iSCSI share login succeeds, the device shared through iSCSI shows on the Linux system as an *iSCSI Disk*. To view a list of connected disks in Linux, enter command `sudo fdisk -l`.

```
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/sda: 476.96 GiB, 512110190592 bytes, 1000215216 sectors
Disk model: SAMSUNG MZNLN512
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: B7D9E3B0-EBED-4CEA-9CC6-08F2918A54FB

Device       Start        End   Sectors   Size Type
/dev/sda1     2048    1050623   1048576   512M EFI System
/dev/sda2  1050624 1000214527 999163904 476.4G Linux filesystem


Disk /dev/loop8: 240.82 MiB, 252493824 bytes, 493152 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/loop9: 29.84 MiB, 31272960 bytes, 61080 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/sdb: 10 GiB, 10737434624 bytes, 2621444 sectors
Disk model: iSCSI Disk
Units: sectors of 1 * 4096 = 4096 bytes
Sector size (logical/physical): 4096 bytes / 16384 bytes
I/O size (minimum/optimal): 16384 bytes / 1048576 bytes
truenas@LinuxMachine:~$
```

Because the connected iSCSI disk is raw, you must partition it. Identify the iSCSI device in the list and enter command `sudo fdisk {/PATH/TO/iSCSIDEVICE}` where `{/path/to/iSCSIDEVICE}` (without curly brackets) is the path for your iSCSI device.

```
truenas@LinuxMachine:~$ sudo fdisk /dev/sdb

Welcome to fdisk (util-linux 2.34).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.


Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1):
First sector (256-2621443, default 256):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (256-2621443, default 2621443):

Created a new partition 1 of type 'Linux' and of size 10 GiB.

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

truenas@LinuxMachine:~$
```

View the iSCSI device path in shell with the `sudo fdisk -l` command. Use the `fdisk` command defaults when partitioning the disk.

> Remember to type `w` when finished partitioning the disk. The `w` command tells `fdisk` to save any changes before quitting.

```
truenas@LinuxMachine:~$ sudo mkfs /dev/sdb1
mke2fs 1.45.5 (07-Jan-2020)
Discarding device blocks: done
Creating filesystem with 2621188 4k blocks and 655360 inodes
Filesystem UUID: 1b38f07a-bb23-40ab-b1eb-255480e4dbbc
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done

truenas@LinuxMachine:~$
```

After creating the partition on the iSCSI disk, a partition slice displays on the device name. For example, /dev/sdb1. Enter `fdisk -l` to see the new partition slice.

Make a File System on the iSCSI Disk

Finally, use `mkfs` to make a file system on the new partition slice on the device. To create the default filesystem (ext2), enter the `sudo mkfs {/PATH/TO/iSCSIDEVICEPARTITIONSLICE}` command where `{/PATH/TO/iSCSIDEVICEPARTITIONSLICE}` (without curly brackets) is the path to your partition slice on your device.

```
truenas@LinuxMachine:~$ sudo mkfs /dev/sdb1
mke2fs 1.45.5 (07-Jan-2020)
Discarding device blocks: done
Creating filesystem with 2621188 4k blocks and 655360 inodes
Filesystem UUID: 1b38f07a-bb23-40ab-b1eb-255480e4dbbc
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done
```

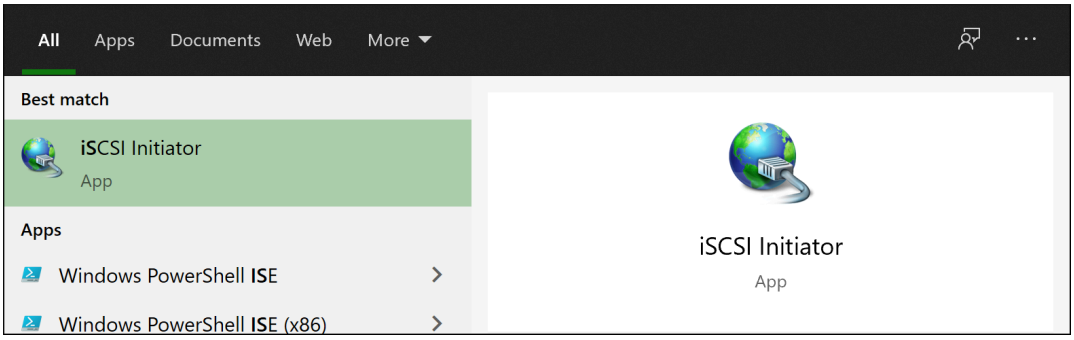
Mount the iSCSI Device

Now the iSCSI device can mount and share data. Enter command `sudo mount {/PATH/TO/iSCSIDEVICEPARTITIONSLICE}` where `{/PATH/TO/iSCSIDEVICEPARTITIONSLICE}` (without curly brackets) is the path to your partition slice on your device. For example, `sudo mount /dev/sdb1 /mnt` mounts the iSCSI device *sdb1* to /mnt.

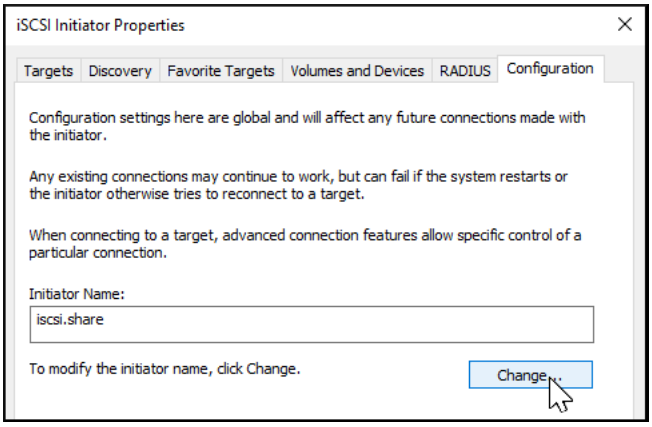
▼ Configuring Windows to Use the iSCSI Share

To access the data on the iSCSI share, clients need to use iSCSI Initiator software. An iSCSI Initiator client is pre-installed in Windows 7 to 10 Pro, and Windows Server 2008, 2012, and 2019. Windows Professional Edition is usually required.

First, click the **Start Menu** and search for the **iSCSI Initiator** application.



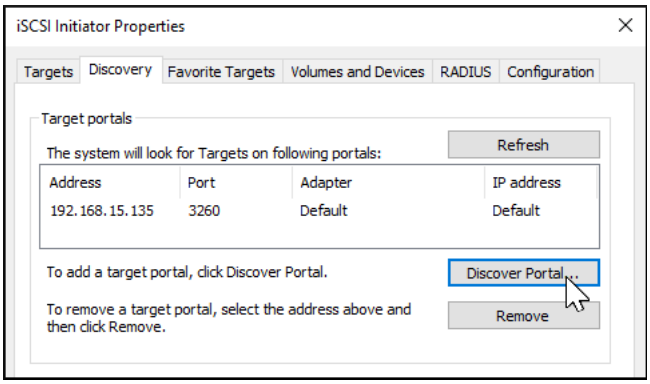
Next, go to the **Configuration** tab and click **Change** to change the iSCSI initiator to the same name created earlier. Click **OK**.



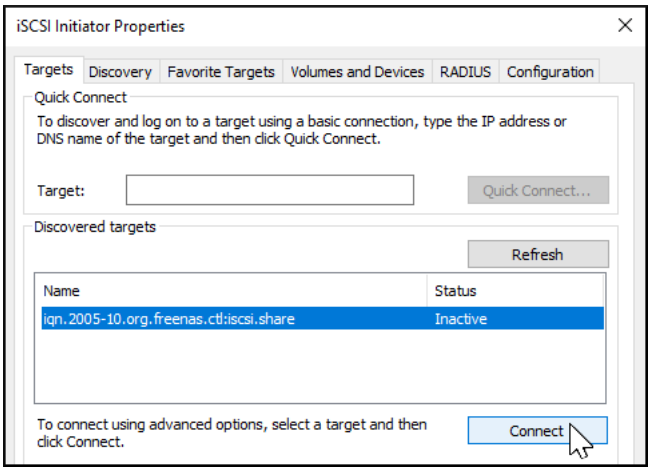
Next, switch to the **Discovery Tab**, click **Discover Portal**, and type in the TrueNAS IP address.

- If TrueNAS changed the port number from the default **3260**, enter the new port number.
- If you set up CHAP when creating the iSCSI share, click **Advanced...**, set **Enable CHAP log on**, and enter the initiator name and the same target/secret set earlier in TrueNAS.

Click **OK**.

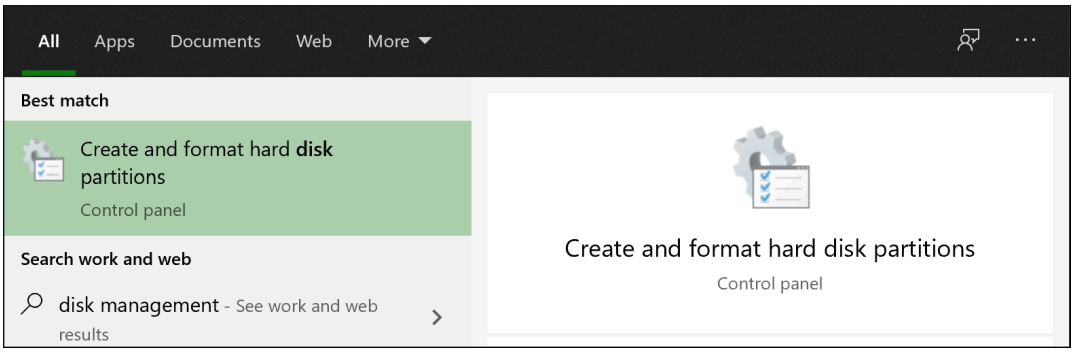


Go to the **Targets** tab, highlight the iSCSI target, and click **Connect**.

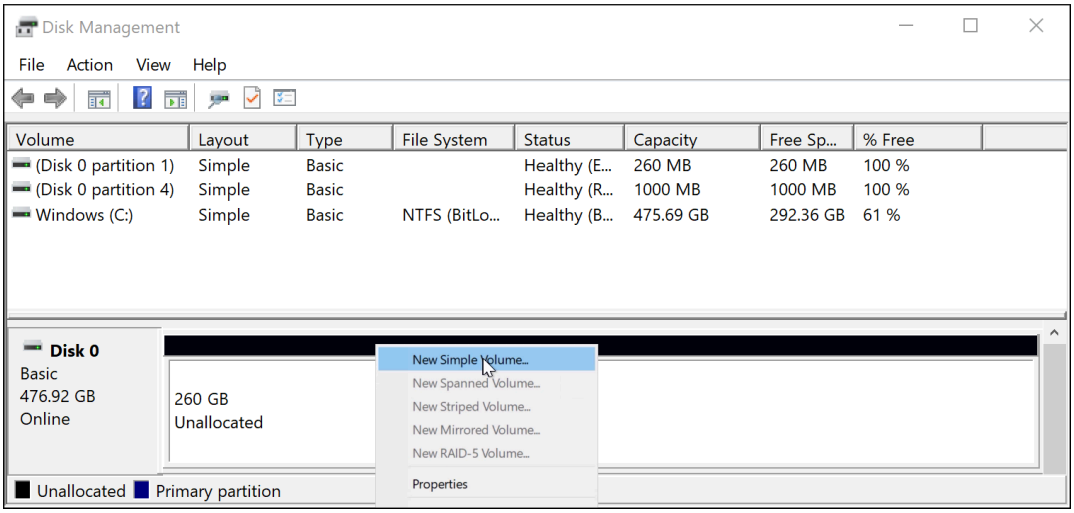


After Windows connects to the iSCSI target, you can partition the drive.

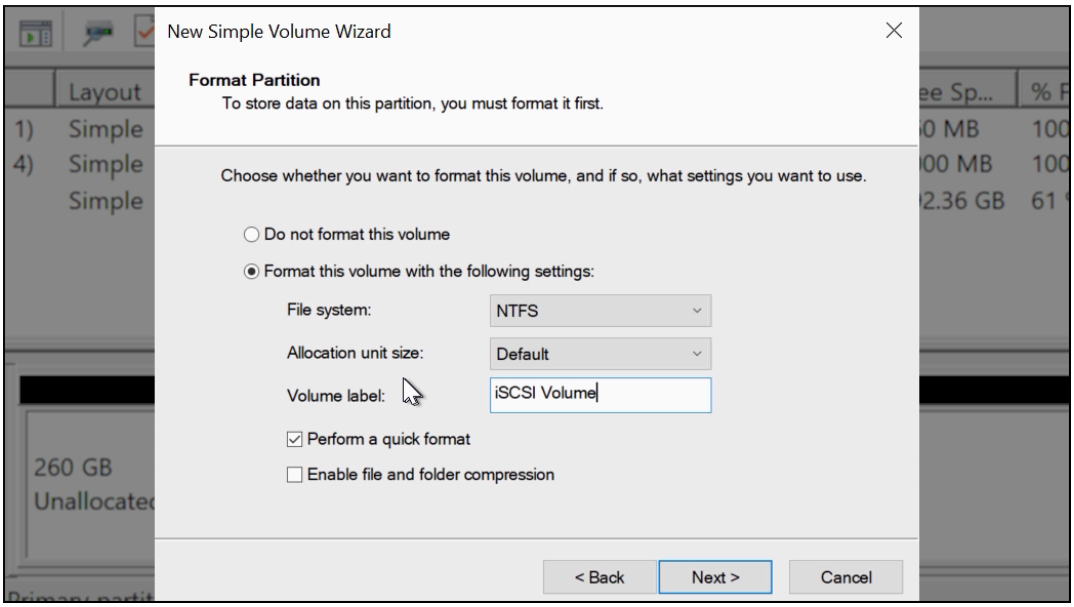
Search for and open the **Disk Management** app.



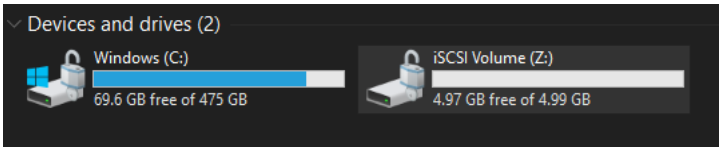
Your drive should currently be *unallocated*. Right-click the drive and click **New Simple Volume…**.



Complete the Wizard to format the drive and assign a drive letter and name.



Finally, go to **This PC** or **My Computer** in File Explorer. The new iSCSI volume should show up under the list of drives. You should now be able to add, delete, and modify files and folders on your iSCSI drive.



NFS Share Creation

Creating a Network File System (NFS) share on TrueNAS makes a lot of data available for anyone with share access. Depending on the share configuration, it can restrict users to read or write privileges.

> NFS treats each dataset as its own file system. When creating the NFS share on the server, the specified dataset is the location that client accesses. If you choose a parent dataset as the NFS file share location, the client cannot access any nested or child datasets beneath the parent.
>
> If you need to create shares that include child datasets, SMB sharing is an option. Note that Windows NFS Client versions currently support only NFSv2 and NFSv3.

Adding an NFS Share Dataset

Before creating an NFS share, create the dataset you want the share to use for data storage.

> It is best practice to use a dataset instead of a full pool for SMB and/or NFS shares. Sharing an entire pool makes it more difficult to later restrict access if needed.

We recommend creating a new dataset with the **Share Type** set to **Generic** for the new NFS share.

Creating an NFS Share

Go to **Sharing > Unix Shares (NFS)** and click **ADD**.

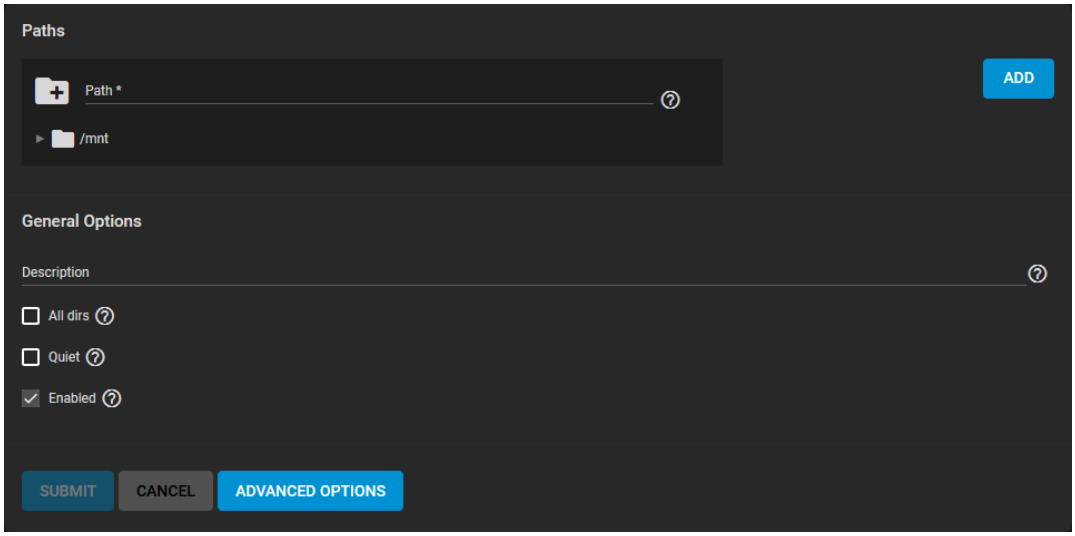


Figure 1: Add NFS Share

Use the file browser to select the dataset to share. Enter an optional **Description** to help identify the share. Clicking **SUBMIT** creates the share. There is the option to select **ENABLE SERVICE** while creating the share to start the service. With this option selected, the service starts automatically after any reboots.

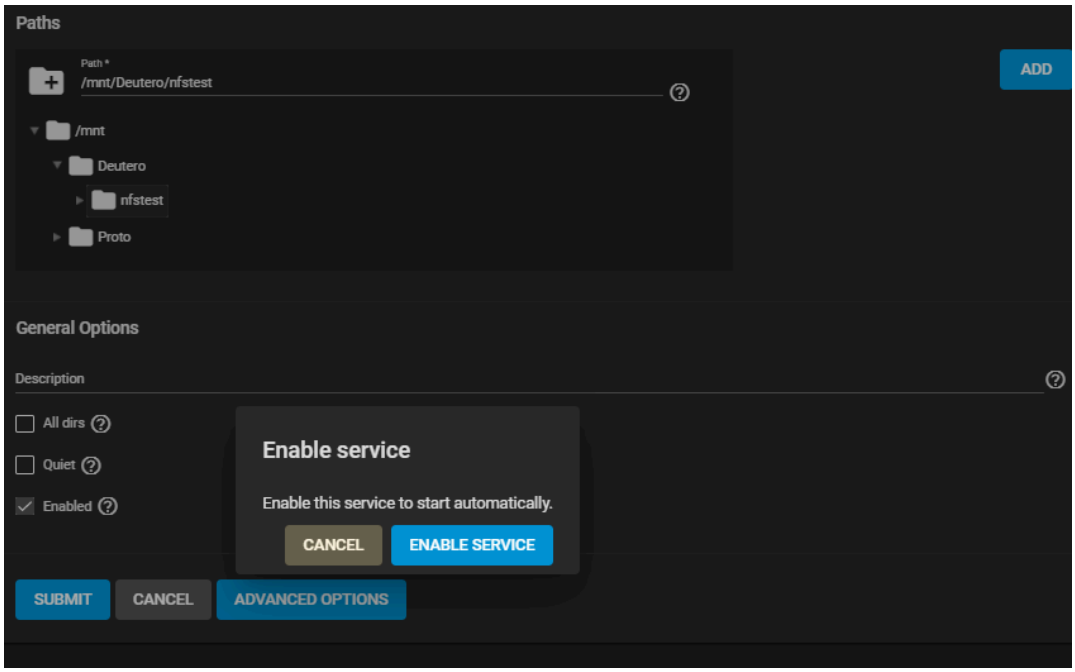


Figure 2: Enable NFS Service

If you wish to create the share but not immediately enable it, select **CANCEL**.

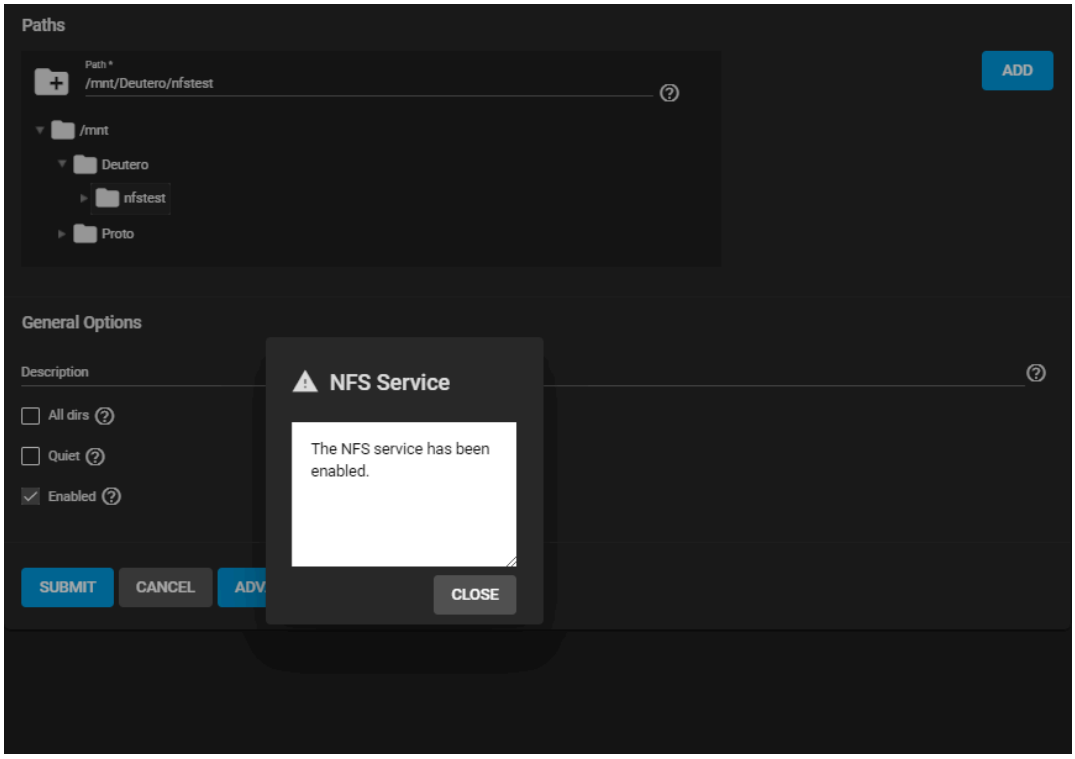


Figure 3: NFS Enabled

NFS Share Settings

See Sharing NFS Screen for more information on NFS share settings.

To edit an existing NFS share, go to **Sharing > Unix Shares (NFS)** and click ⋮ **> Edit**. The options available are identical to the share creation options.

Configure the NFS Service

To begin sharing the data, go to **Services** and click the **NFS** toggle. If you want NFS sharing to activate immediately after TrueNAS boots, set **Start Automatically**.

NFS service settings can be configured by clicking (Configure). See NFS Screen for details.

Unless a specific setting is needed, we recommend using the default settings for the NFS service. When TrueNAS is already connected to Active Directory, setting **NFSv4** and **Require Kerberos for NFSv4** also requires a kerberos keytab.

Connecting to the NFS Share with a Linux/Unix OS

The NFS share connects with various operating systems. The recommendation is to use a Linux/Unix operating system. Using a Linux/Unix operating system, download the `nfs-common` kernel module. Do this using the package manager of the installed distribution. For example, on Ubuntu/Debian, enter `sudo apt-get install nfs-common` in the terminal.

After installing the module, connect to an NFS share by entering `sudo mount -t nfs {IPaddressOfTrueNASsystem}: {path/to/nfsShare} {localMountPoint}`, where *{IPaddressOfTrueNASsystem}* is the IP address of the remote TrueNAS system that contains the NFS share, *{path/to/nfsShare}* is the path to the NFS share on the TrueNAS system, and *{localMountPoint}* is a local directory on the host system configured for the mounted NFS share. For example, `sudo mount -t nfs 10.239.15.110:/mnt/pool1/photoDataset /mnt` mounts the NFS share *photoDataset* to the local directory `/mnt`.

By default, anyone that connects to the NFS share only has the read permission. To change the default permissions, edit the share. Go to **Advanced Options** and change the **Access** settings.

> ESXI 6.7 or later is required for read/write functionality with NFSv4 shares.

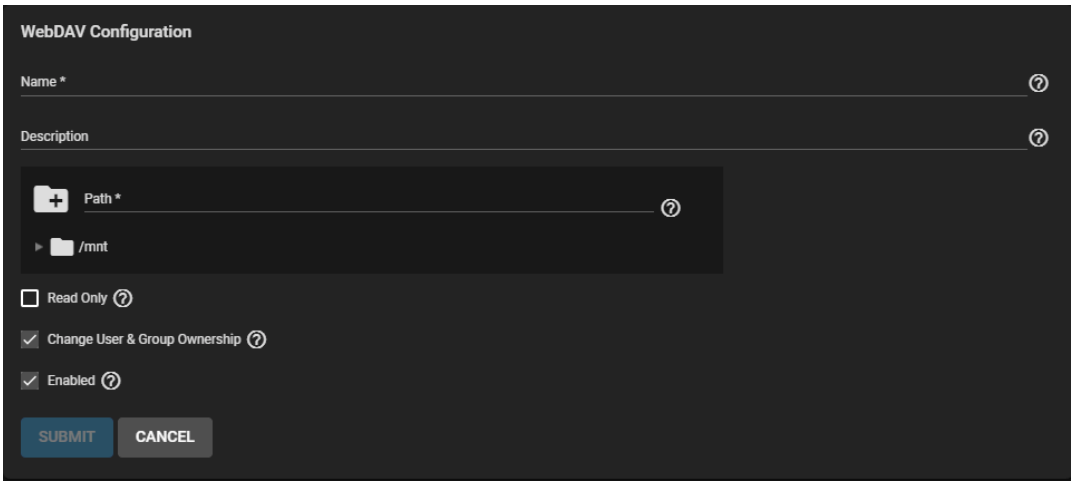
WebDav Share Creation

TrueNAS supports (WebDAV), or Web-based Distributed Authoring and Versioning. WebDAV makes it easy to share a TrueNAS dataset and its contents over the web.

To create a new share, make sure a dataset is available with all the data for sharing.

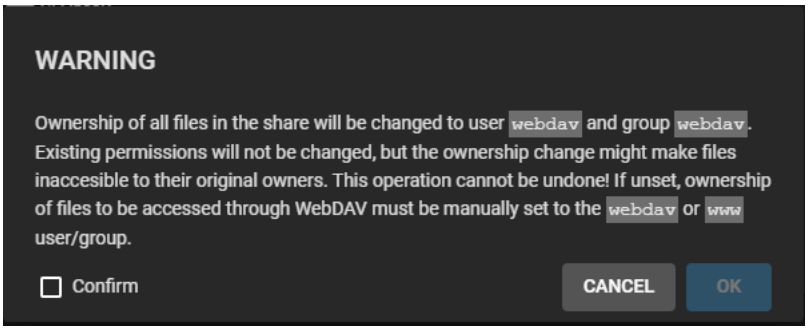
Share Configuration

Go to **Sharing > WebDAV Shares** and click **ADD**.



Enter a name for the share in **Name** and use the file browser to select the dataset to share. Enter an optional description for the share in **Description** to help identify it. To prevent user accounts from modifying the shared data, select **Read Only**.

> The default selection is **Change User & Group Ownership**. This changes existing ownership of all files in the share to the **webdav** user and group accounts. The default selection simplifies WebDAV share permission. This unexpected change causes the web interface to display a warning:

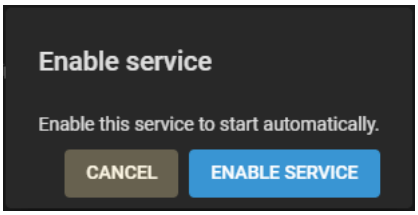


Clearing the checkbox labeled **Change User & Group Ownership** prevents the warning from displaying. You must manually set shared file ownership to the **webdav** or **www** user and group accounts in that case.

By default, the new WebDAV share is immediately active. To create the share but not immediately activate it, clear the checkmark in **Enable**. Click **SUBMIT** to create the share.

Service Activation

Creating a share immediately opens a dialog to activate the WebDAV service:



It is possible to enable or disable the WebDAV system service at a later time. Go to **Services** and click the **WebDAV** toggle to stop the service. To automatically start the service when TrueNAS boots, select **Start Automatically**. Click the ✎ to change the service settings.

For better data security, select **HTTPS** as the **Protocol**. This requires choosing an SSL certificate. The **freenas_default** certificate is available as an option. All **Protocol** options require defining a **Port** number. Verify that the WebDAV service port is not already in use on the network before defining a **Port** number.

Select either **Basic** or **Digest** as the method of **HTTP Authentication**. Create a new **Webdav Password**. This prevents unauthorized access to the shared data.

Click **SAVE** after making any changes.

Connecting to the WebDAV Share

WebDAV shared data is accessible from a web browser. To see the shared data, open a new browser tab and enter the following in the URL field `{PROTOCOL}://{TRUENASIP}:{PORT}/{SHAREPATH}` where the elements in curly brackets **{}** are your chosen settings from the WebDAV share and service. Example: *https://10.2.1.1:8081/newdataset*

When the **Authentication** WebDAV service option is configured to either **Basic** or **Digest**, a user name and password is required. Enter the user name **webdav** and the password defined in the WebDAV service.

> Depending on your webserver and client software, you might experience issues uploading files over 1 GB.

Windows Shares (SMB)

SMB Background

SMB (also known as CIFS) is the native file sharing system in Windows. SMB shares can connect to any major operating system. This includes Windows, MacOS, and Linux.

TrueNAS can use SMB to share files among one or many users or devices. SMB supports a wide range of permissions and security settings. SMB can support advanced permissions (ACLs) on Windows and other systems. SMB also supports Windows Alternate Streams and Extended Metadata. SMB is suitable for the management and administration of large or small pools of data.

> TrueNAS uses Samba to provide SMB services. There are many versions of the SMB protocol. During SMB session negotiation, an SMB client attempts to negotiate the highest SMB protocol. Industry-wide, the usage of the SMB1 protocol (sometimes referred to as NT1) is being deprecated for security reasons. However, most SMB clients support SMB 2 or 3 protocols, even when they are not the default protocols.

> Legacy SMB clients rely on NetBIOS name resolution to discover SMB servers on a network. The NetBIOS name server (nmbd) is disabled by default in TrueNAS. You can enable it in **Network > Global Configuration** if this functionality is required.
>
> MacOS clients use mDNS to discover the presence of SMB servers on the network. The mDNS server (avahi) is enabled by default on TrueNAS.
>
> Windows clients use WS-Discovery to discover the presence of SMB servers. Check the version of the Windows client. In some versions of the Windows client, the default settings disable network discovery.
>
> Discoverability through broadcast protocols is a convenience feature. It is not required to access an SMB server.

First Steps

1. Create a dataset.

   > It is best practice to use a dataset instead of a full pool for SMB and/or NFS shares. Sharing an entire pool makes it more difficult to later restrict access if needed.

   For the new SMB share, the recommendation is to create a new dataset and set the **Share Type** to **SMB**.

   Create the ZFS dataset with these settings:

   - **aclmode** = restricted
   - **case sensitivity** = insensitive

   A default Access Control List is also applied to the dataset. This default ACL is restrictive and only allows access to the dataset owner and group. You can change this ACL later according to your use case.

2. Create local user accounts.

   By default, all new local users are members of a built-in SMB group called **builtin users**. You can use this group to grant access to all local users on the server. You can use additional groups to fine-tune permissions to large numbers of users. User accounts built-in to TrueNAS cannot access SMB. User accounts that do not have the **smb** flag set cannot access SMB.

   As of 13.3, SMB user passwords can include the question mark (?).

   ▼ Why not just allow anonymous access to the share?

   Anonymous or guest access to the share is possible, but this is a security vulnerability. Anonymous or guest access is being deprecated by the major SMB client vendors. This partly because signing and encryption are not possible for guest sessions.

   ▼ What about LDAP users?

   With LDAP configured, users from the LDAP server can have access the SMB share. Go to **Directory Services > LDAP > ADVANCED MODE** and set **Samba Schema**. Caution: local TrueNAS user accounts no longer have access to the share.

3. Tune the dataset ACL.

   After creating a dataset and the needed accounts, determine the access requirements and adjust the dataset ACL to match. To edit the ACL, go to **Storage > Pools**, open the options for the new dataset, and click **Edit Permissions**. Many home users often add a new entry that grants this access: **FULL_CONTROL** to the **builtin_users** group with the flags set to **INHERIT**. See the Permissions article for more details.

Creating an SMB Share

To create a Windows SMB share, go to **Sharing > Windows Shares (SMB)** and click **ADD**.

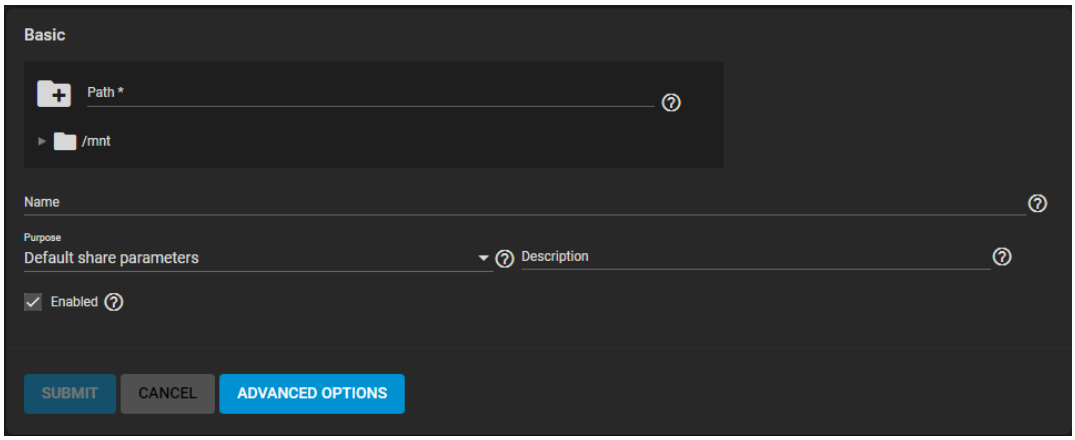


Figure 1: Basic SMB Share Options

The **Path** and **Name** of the SMB share define the smallest amount of information required to create a new SMB share. The **Path** is the directory tree on the local file system exported over the SMB protocol. **Name** is the name of the SMB share. This forms a part of the full share path name when SMB clients perform an SMB tree connect. Enter a name that is less than or equal to 80 characters in length. The name shoud not contain any invalid characters. Microsoft documentation MS-FSCC section 2.1.6 lists these invalid characters. The last component of the value in **Path** becomes the share name if **Name** is blank or empty.

You can set a share **Purpose** to apply and lock pre-defined advanced options for the share. To keep full control over all the share **Advanced Options**, choose **No presets**.

You can specify an optional value in **Description** to help explain the purpose of the share.

Enabled shares this path when the SMB service is activated. Clearing **Enabled** disables the share without deleting the configuration.

See SMB Share Screen for more information on SMB Share settings.

Activating the SMB Service

Connecting to an SMB share does not work when the related system service is not activated. To make an SMB share available on the network, go to **Services** and click the **SMB** toggle to start the service. If you want the service to activate whenever TrueNAS boots, select **Start Automatically**.

See SMB Service Screen for more information on SMB services settings.

Mounting an SMB Share on Another Machine

▼ Mount Commands

Linux

Verify that the required CIFS packages are installed for your distribution of Linux. Create a mount point. Enter `sudo mkdir /mnt/smb_share`.

Mount the volume. Enter `sudo mount -t cifs //computer_name/share_name /mnt/smb_share`.

If your share requires user credentials, add the switch `-o username=` with your username after `cifs` and before the share address.

Windows

To mount the SMB share to a drive letter on Windows, open the command line and enter the following command with the appropriate drive letter, computer name, and share name.

```
net use Z: \\computer_name\share_name /PERSISTENT:YES
```

> In case of Windows reporting an incorrect password, you might have to change your Windows security settings using **Local Security Policy > Local Policies > Security Options > Network security: LAN Manager authentication level > Send NTLMv2 response only**.

Apple

Open **Finder > Go > Connect To Server** Enter the SMB address: `smb://192.168.1.111`.

Input the username and password for the user assigned to that pool or guest if gGuest access is enabled on the share.

FreeBSD

Create a mount point. Enter `sudo mkdir /mnt/smb_share`.

Mount the volume. Enter `sudo mount_smbfs -I computer_name\share_name /mnt/smb_share.`

Managing SMB Shares

Share Management

After creating the SMB share, additional management options are available by going to **Sharing > Windows Shares (SMB)** and clicking ⋮ for a share entry:

Name	Description
Edit	Opens the share creation screen to reconfigure the share or disable it.
Edit Share ACL	Opens a screen to configure an Access Control List (ACL) for the share. The default is open.

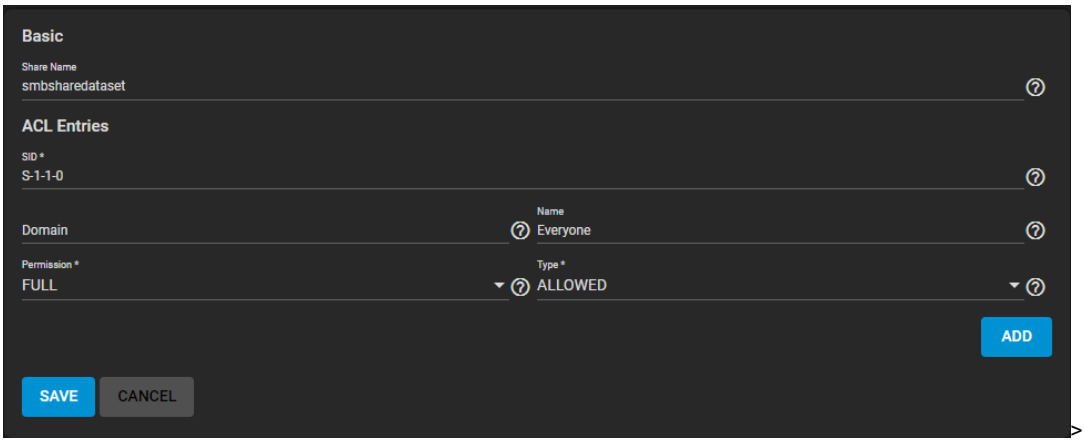
Edit Share ACL

- This is separate from file system permissions, and applies at the level of the entire SMB share.
- Permissions defined here are not interpreted by clients of other file sharing protocols.
- Permissions defined here are not interpreted by other SMB shares. Even if the other SMB shares export the same share **Path** value.
- Enabling **Access Based Share Enumeration** uses this ACL to determine the browse list.

Name	Description
Edit Filesystem ACL	Opens a screen to configure an Access Control List (ACL) for the path defined in the share **Path**.
Delete	Remove the share configuration from TrueNAS. Shared data is unaffected.

Configure Share ACL

To see the share ACL options, click ⋮ > **Edit Share ACL**.



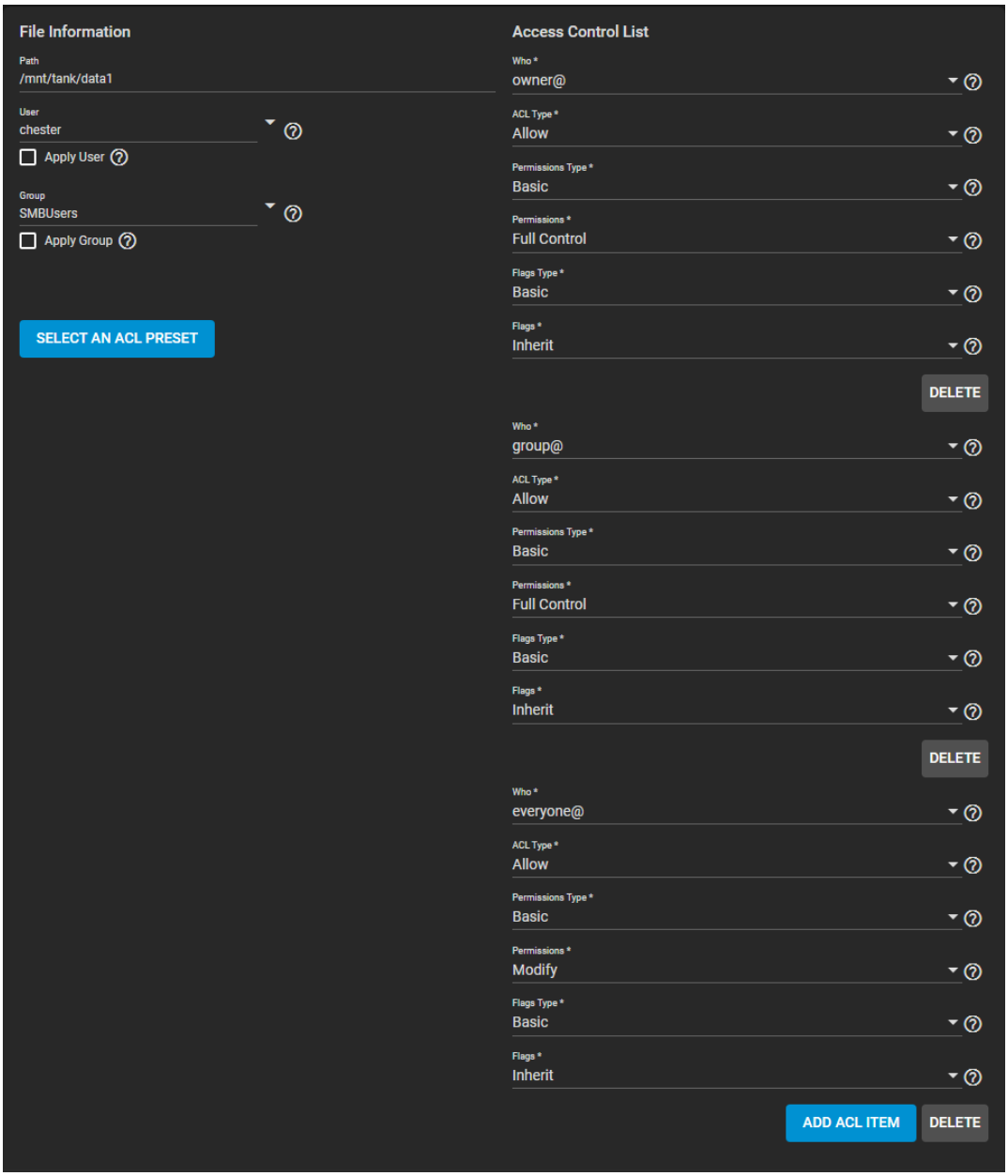
The **Share Name** is shown, but cannot be changed. **ACL Entries** are listed as a block of settings. Click **ADD** to register a new entry.

Name	Description
SID	Who this ACL entry (ACE) applies to, shown as a Windows Security Identifier. Either a **SID** or a **Domain** with **Name** is required for the ACL.
Domain	Enter a domain for the user **Name**. Required when a **SID** is not entered. Local users have the SMB server NetBIOS name: *truenas\smbusers*.
Permission	Dropdown list of predefined permission combinations: Select **Read** for read access and execute permission on the object (RX). Select **Change** for read access, execute permission, write access, and delete object (RXWD). Select **Full** for read access, execute permission, write access, delete object, change Permissions, and take ownership (RXWDPO). For more details, see smbacls(1).
Name	Enter the name of who this ACL entry applies to, shown as a user name. Requires adding the user **Domain**.
Type	Select from the dropdown list how permissions are applied to the share. Select **Allowed** to deny all permissions by default except those that are manually defined. Select **Denied** to allow all permissions by default except those that are manually defined.

Click **SAVE** to store the share ACL and apply it to the share immediately.

Configure File System ACL

Click ⋮ **> Edit Filesystem ACL** to quickly return to **Storage > Pools** and edit the dataset ACL.



This ACL defines the user accounts or groups that own or have specific permissions to the shared dataset. The **User** and **Group** values show which accounts own, or have full permissions to the dataset. Change the default settings to your preferred primary account and group. Select the **Apply** checkboxes before saving any changes.

ACL Presets

To rewrite the current ACL with a standardized preset, click **SELECT AN ACL PRESET** and choose an option:

Open

Has three entries:

- **owner@** has full dataset control.
- **group@** has full dataset control.
- All other accounts can modify the dataset contents.

Restricted

Has two entries:

- **owner@** has full dataset control.
- **group@** can modify the dataset contents.

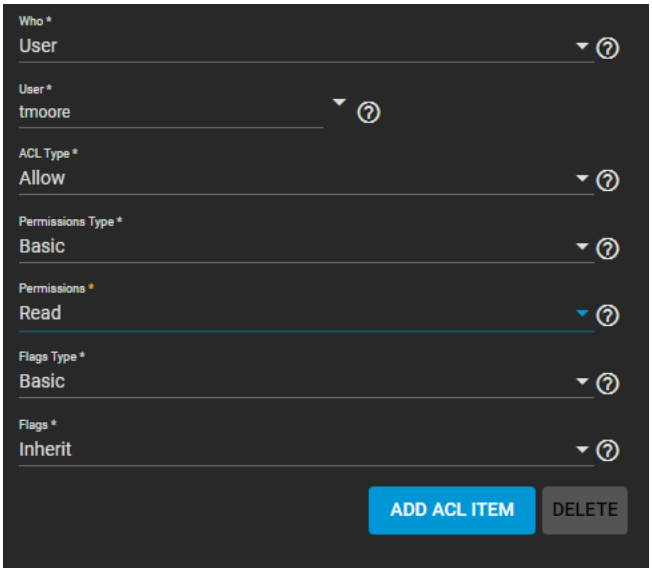
Home

Has three entries:

- **owner@** has full dataset control.
- **group@** can modify the dataset contents.
- All other accounts can traverse through the dataset.

Adding ACL Entries (ACEs)

To define permissions for a specific user account or group, click **ADD ACL ITEM**. Open the **Who** dropdown list, select **User** or **Group**, and select a specific user or group account. Define the settings for the account. Define the permissions to apply to that account. For example, to allow the *tmoore* user permission to view dataset contents but not make changes, define the **ACL Type** as **Allow**. Define **Permissions** for this user as **Read**.



Home Shares

TrueNAS offers the **Use as Home Share** option for organizations or SMEs that want to use a single SMB share to provide a personal directory to every user account.

> The **Use as Home Share** feature is available for a single TrueNAS SMB share. You can create additional SMB shares as described in the SMB sharing article but without the **Use as Home Share** option enabled.

Create a Pool and Join Active Directory

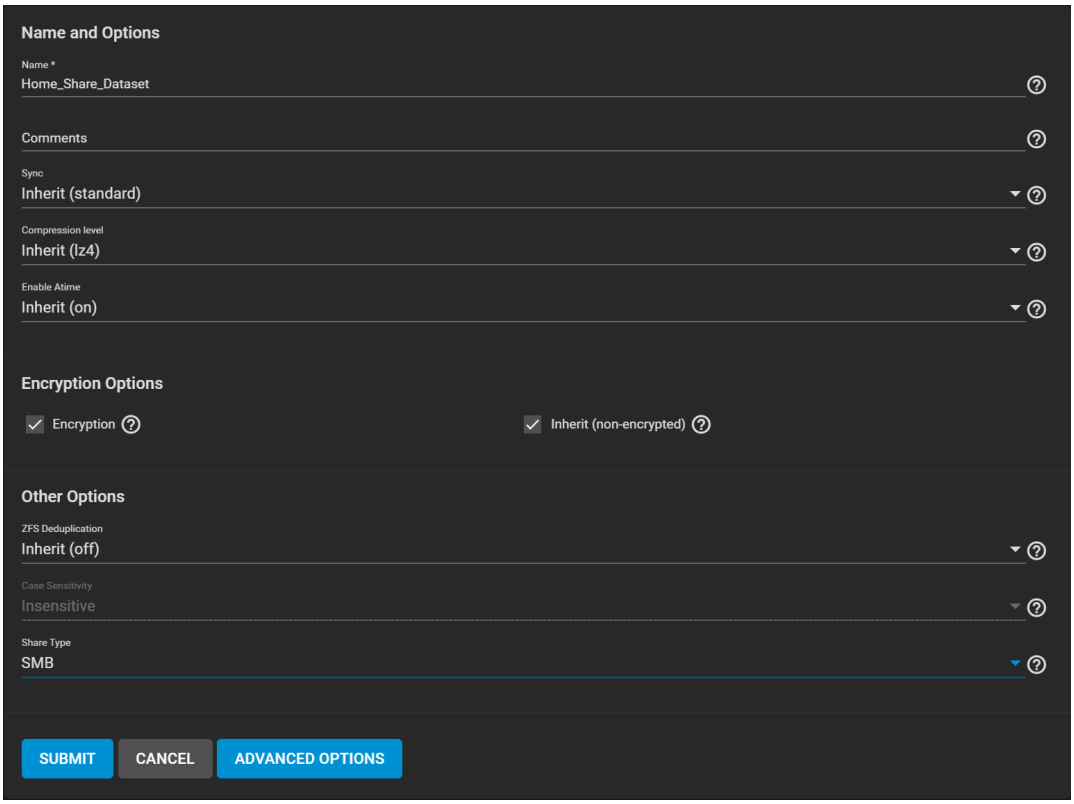
First, go to **Storage > Pools** and create a pool.

Next, set up the Active Directory that you want to share resources with over your network.

Prepare a Dataset

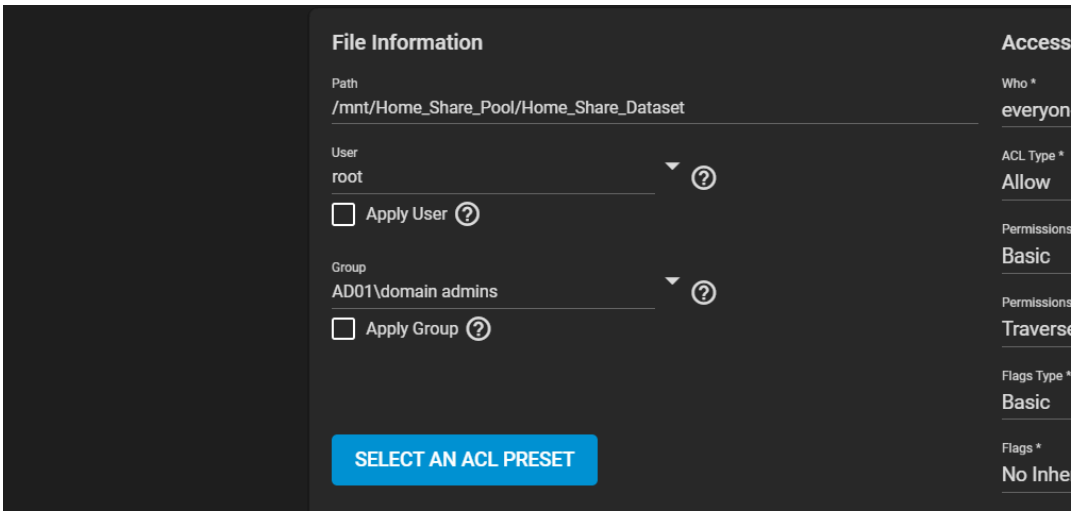
Go to **Storage > Pools** and open the ⋮ next to the root dataset in the pool you just created, then click **Add Dataset**.

Name the dataset (this article uses *Home_Share_Dataset* as an example) and set the **Share Type** to **SMB**.

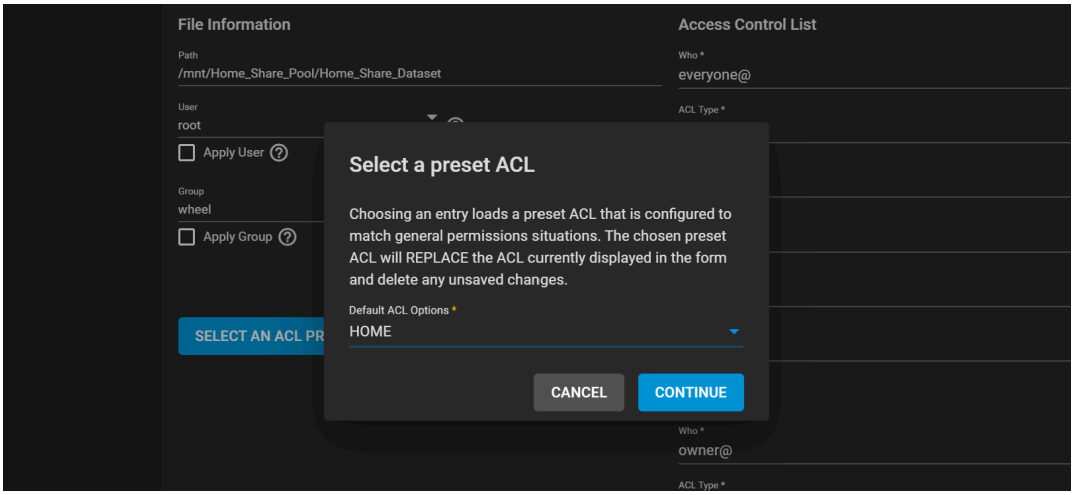


After creating the dataset, go to **Storage > Pools** and open ⋮ next to the new dataset. Select **Edit Permissions**.

Click the **Group** dropdown menu and change the owning group to your Active Directory domain admins and check **Apply Group**.



Click **Select an ACL Preset** and choose **HOME**. Then, click **SAVE**.



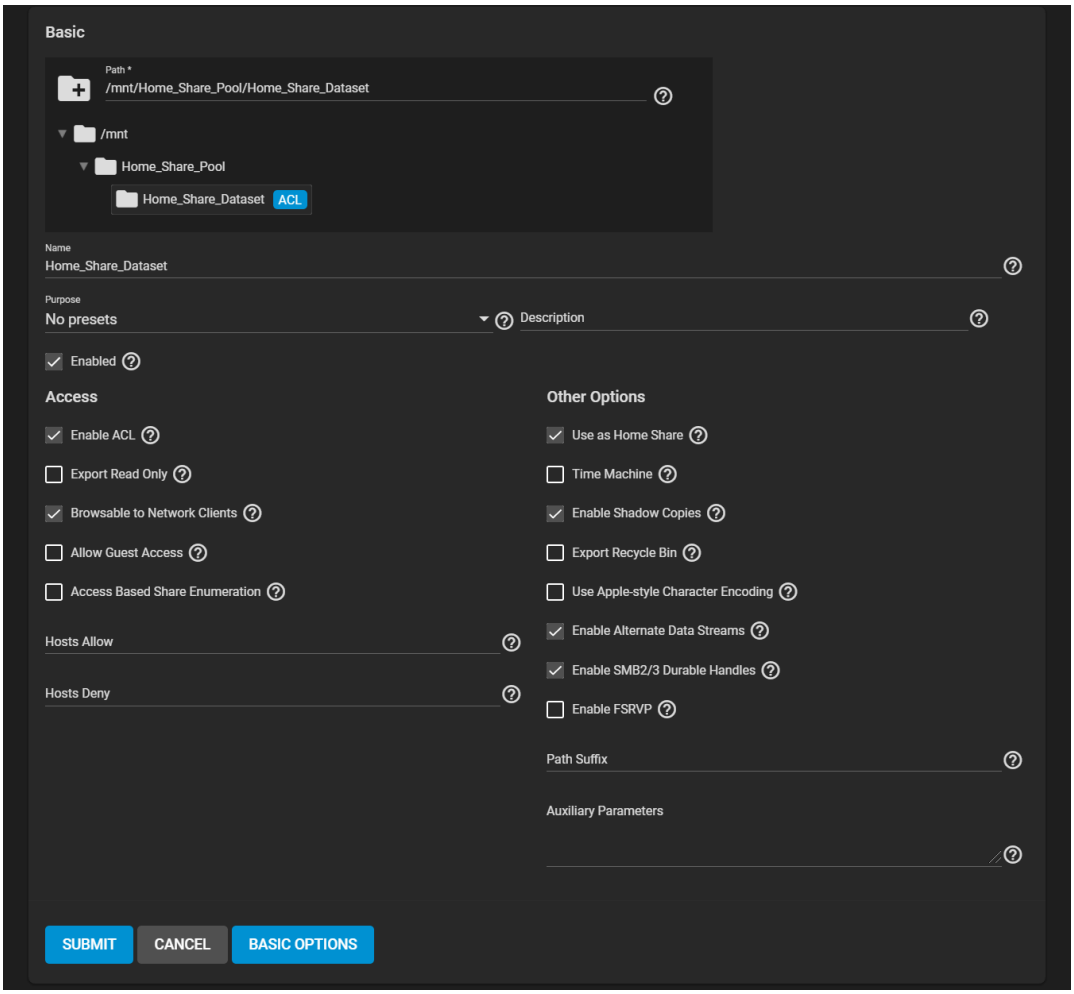
Create the Share

Go to **Sharing > Windows Shares (SMB)** and click **ADD**.

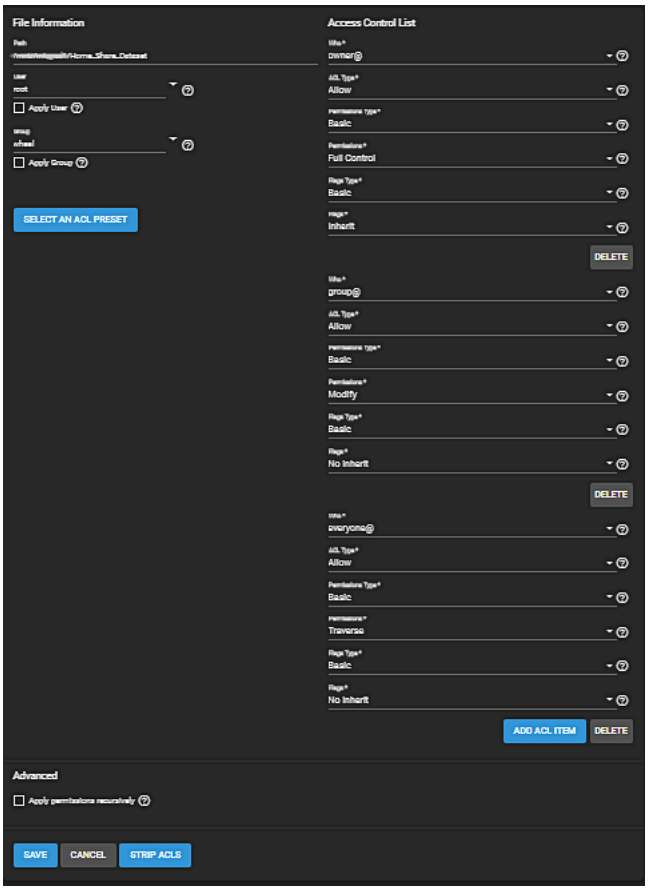
Set the **Path** to the prepared dataset (*Home_Share_Dataset* for example).

The **Name** automatically changes to be identical to the dataset. Leave this at the default.

Set the **Purpose** to **No presets**, then click **ADVANCED OPTIONS** and check **Use as Home Share**. Click **SUBMIT**.



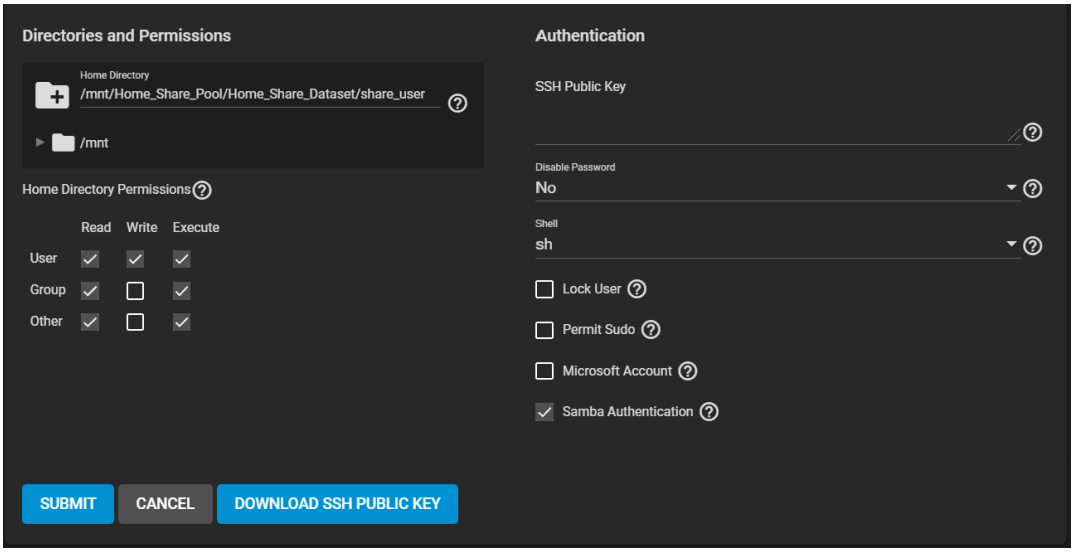
The ACL editor opens, displaying the home ACL preset values.



Click **SAVE**. Enable the **SMB** service in **Services** to make the share available on your network.

Add Users

Go to **Accounts > Users** and click **ADD**. Create a new user name and password. By default, the user **Home Directory** is titled from the user account name and added as a new subdirectory of *Home_Share_Dataset*.



If existing users require access to the home share, go to **Accounts > Users** and edit an existing account.

Adjust the user home directory to the appropriate dataset and give it a name to create their own directory.

After the user accounts have been added and permissions configured, users can log in to the share and see a folder matching their user name.

Shadow Copies

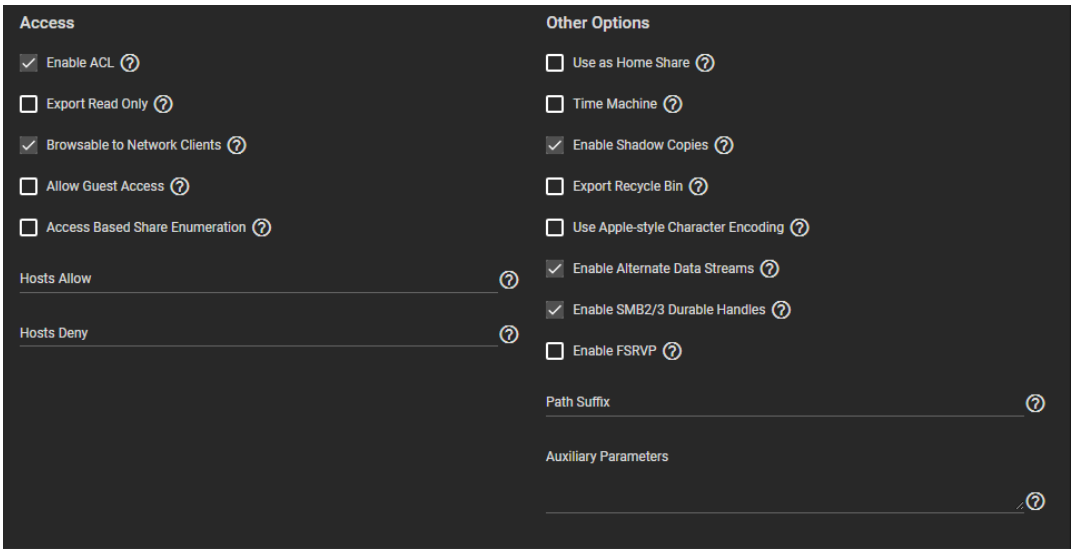
Shadow Copies, also known as the Volume Shadow Copy Service (VSS) or Previous Versions, is a Microsoft service for creating volume snapshots. Shadow copies can be used to restore previous versions of files from within Windows Explorer.

By default, all ZFS snapshots for a dataset underlying an SMB share path are presented to SMB clients through the volume shadow copy service or are accessible directly with SMB when the hidden ZFS snapshot directory is located within the path of the SMB share.

There are a few caveats about shadow copies to be aware of before activating the feature in TrueNAS:

- When the Windows system is not fully patched to the latest service pack, Shadow Copies might not work. If no previous versions of files to restore are visible, use Windows Update to ensure the system is fully up-to-date.
- Shadow copy support only works for ZFS pools or datasets.
- Appropriate permissions must be configured on the pool or dataset shared by SMB.
- Users cannot use an SMB client to delete shadow copies. Instead, the administrator uses the TrueNAS web interface to remove snapshots. Shadow copies can be disabled for an SMB share by clearing the checkmark from **Enable shadow copies** for the SMB share. This does not prevent access to the hidden .zfs/snapshot directory for a ZFS dataset when the directory is located within the path for an SMB share.

To enable Shadow Copies, go to **Sharing > Windows Shares (SMB)** and **Edit** an existing share. Open the **Advanced Options**, find the **Other Options** and select **Enable Shadow Copies**.



▼ Windows 10 v2004 Issue

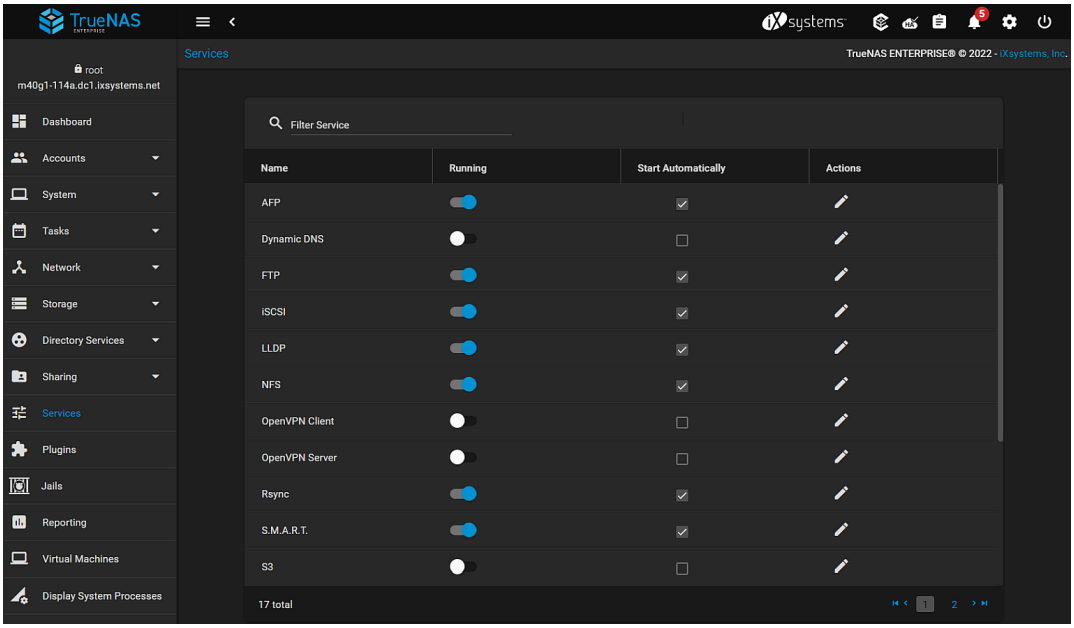
Some users have experienced issues in the Windows 10 v2004 release where network shares can't be accessed. The problem appears to come from a bug in gpedit.msc, the Local Group Policy Editor. Unfortunately, setting the **Allow insecure guest logon** flag value to **Enabled** in **Computer Configuration > Administrative Templates > Network > Lanman Workstation** appears to have no effect on the configuration.

To work around this issue, edit the Windows registry. Use **Regedit** and go to **HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters**. The **DWORD AllowInsecureGuestAuth** is an incorrect value: **0x00000000**. Change this value to **0x00000001** (Hexadecimal 1) to allow adjusting the settings in gpedit.msc. You can apply this to a fleet of Windows machines with a Group Policy Update.

Services

The **Services** screen lists all services available on the TrueNAS.

Activate or configure a service on the **Services** page.



Use the right slider to scroll down to the bottom of the list of services or click on page **2**, or the or arrows.

To locate a service, type in the **Filter Search** field to narrow down the list of services.

Select **Start Automatically** for configured services that need to start after the system boots.

Click the toggle to start or stop the service, depending on the current state. Hover the mouse over the toggle to see the current state of that service. The toggle turns blue when it is running.

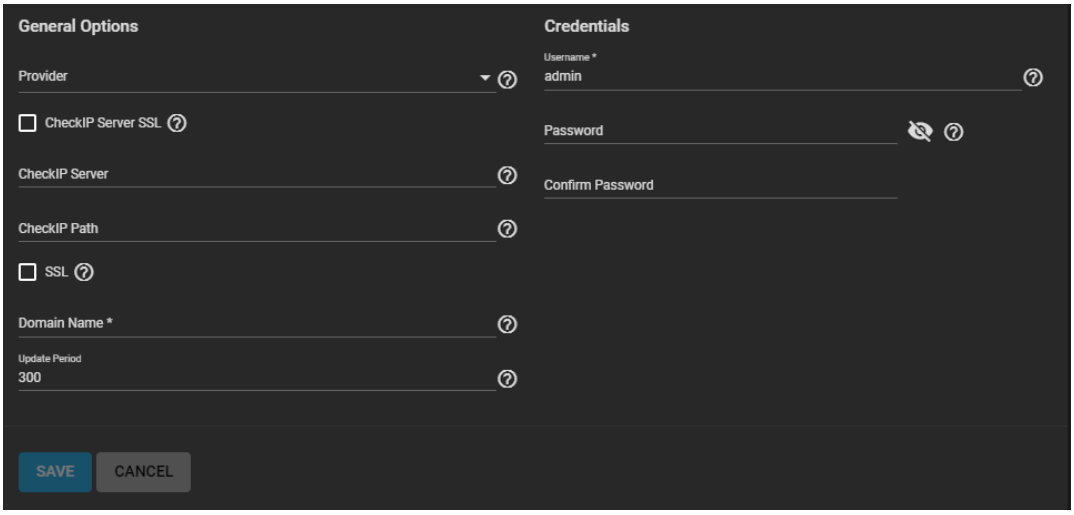
Click the icon to display the settings screen for a service.

Services related to data sharing or automated tasks are documented in their respective Sharing or Tasks.

Configuring Dynamic DNS

ISPs often change the IP address of the system. With Dynamic Domain Name Service (DDNS) the current IP address continues to point to a domain name to provide access to TrueNAS.

DDNS requires registration with a DDNS service such as DynDNS before configuring TrueNAS. Open your specific DDNS service settings in another browser tab for reference while configuring TrueNAS. Log in to the TrueNAS web interface and go to **Services > Dynamic DNS**.



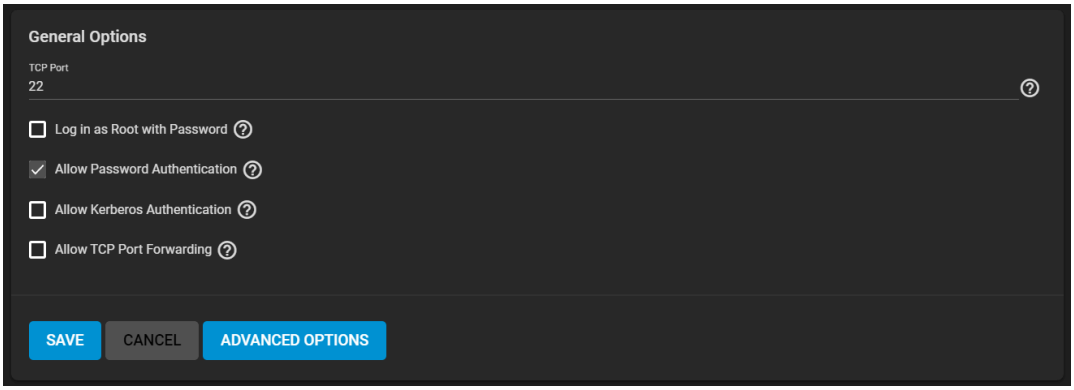
Your DDNS solution provides the required values for these fields. Start the DDNS service after choosing your **Provider** options and saving the settings.

Configuring SFTP

Configuring SFTP Service

SSH File Transfer Protocol (SFTP), is available by enabling SSH remote access to the TrueNAS system. SFTP is more secure than standard FTP as it applies SSL encryption on all transfers by default.

Go to **Services**, find the **SSH** entry, and click the ✎.



Select **Allow Password Authentication**.

> Evaluate **Log in as Root with Password** for your security environment: SSH with root is a security vulnerability. It allows more than SFTP transfer access. SSH with root also allows full remote control over the NAS with a terminal.

Review the remaining options and configure according to your environment or security needs.

SSH Service Options

Use the **SSH** screen to configure the system for SFTP. See ServicesSSH for information on SSH screen settings.

SFTP Connections

Open FileZilla or another FTP client, or command line. This example uses FileZilla. Using FileZilla, enter `SFTP://TrueNAS IP`, `username`, `password`, and port `22` to connect. Where `TrueNAS IP` is the IP address for your system, and `username` and `password` are those you use to connect to the FTP client. Or enter `SFTP://'TrueNAS IP'`, `'username'`, `'password'`, and port `22` to connect.

> Chroot is not 100% secure, but SFTP does not have chroot locking. The lack of chroot allows users to move up to the root directory. They can view internal system information. If this level of access is a concern, FTP with TLS may be the more secure choice.

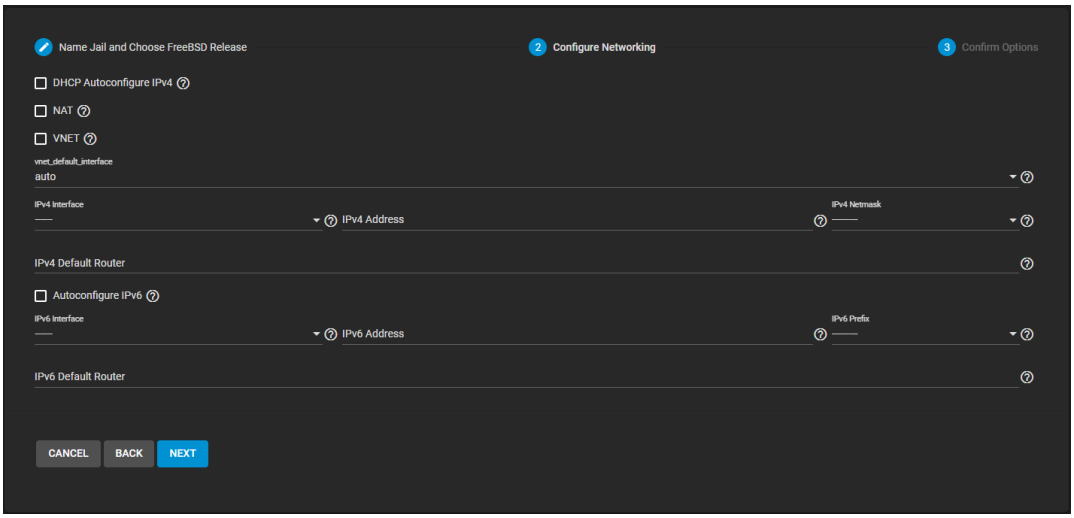
SFTP in a TrueNAS Jail

Setting up a jail and enabling SSH is another way to allow SFTP access. This does not grant read access to other areas of the NAS itself.

▼ Setting up a Jail for SFTP

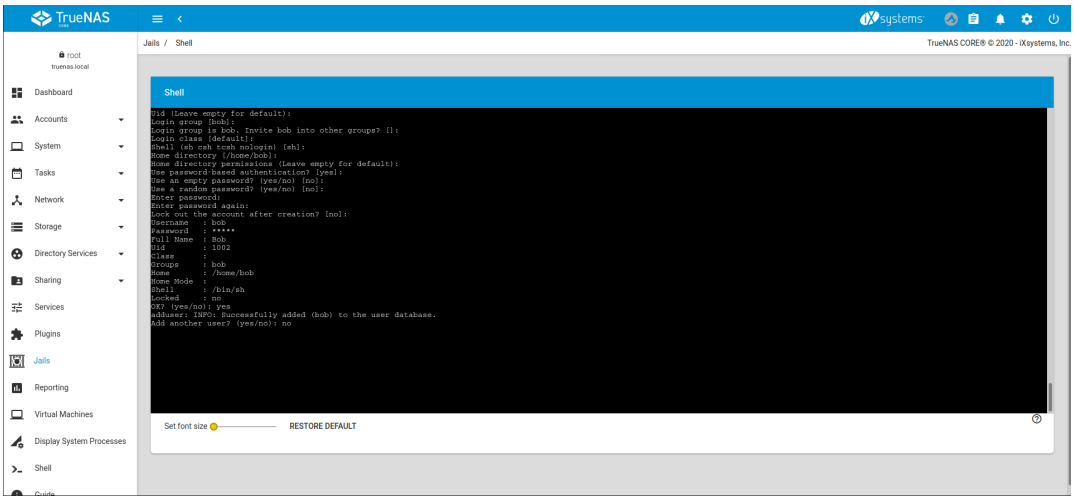
Go to **Jails > Add**. Provide a name for the jail and pick a target FreeBSD image. This example uses 11.3.

Select the networking options for either DHCP or a static IP and confirm to create.

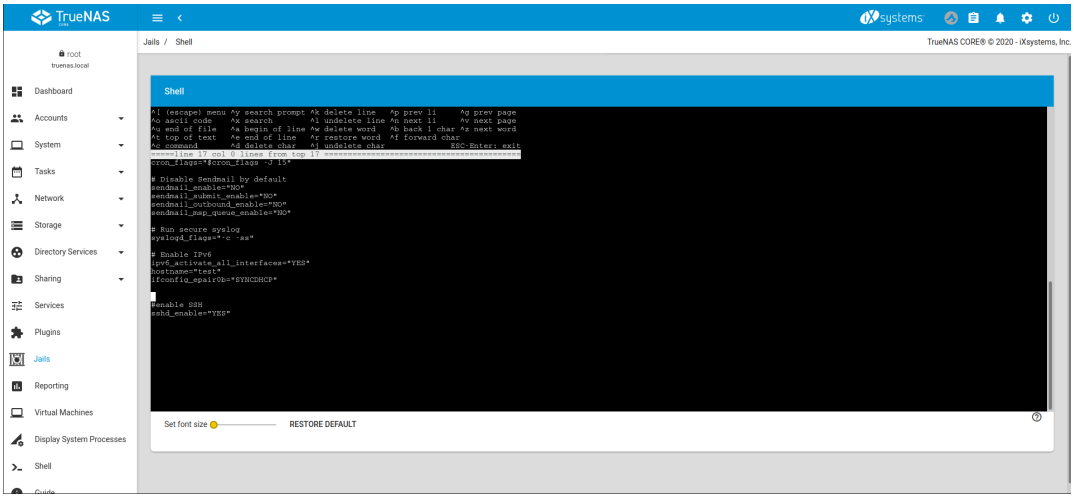


After the jail is created, click the expand icon **>** on the right-hand side of the jail to open it. Click **START** and open **> SHELL**.

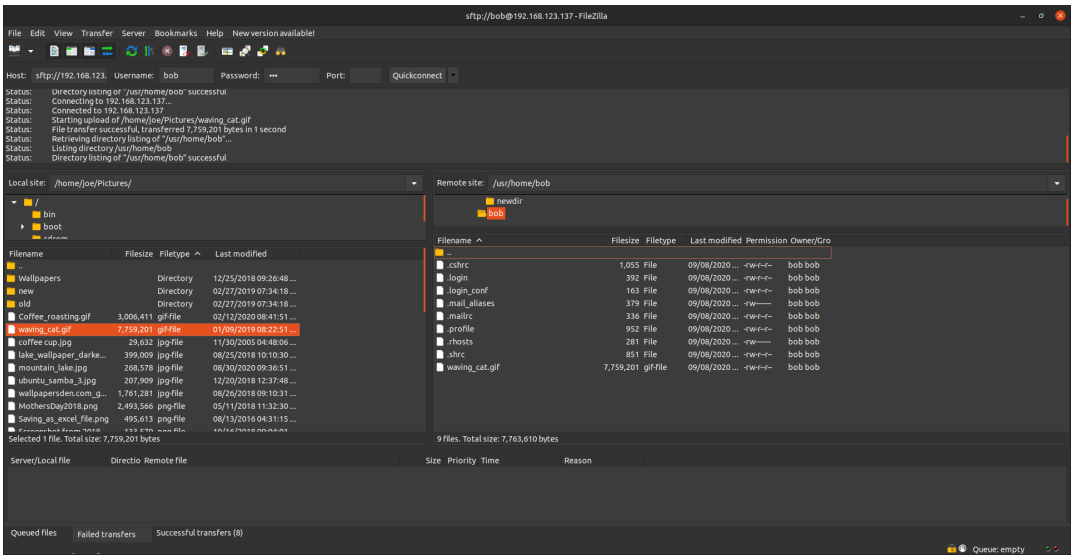
Create a user in the jail. Enter command `adduser`. Follow the prompts. Include the password and home directory location. When complete, the jail asks to confirm the credentials.



Enable SSH by editing the /etc/rc.conf file. Enter command `vi /etc/rc.conf` or `ee /etc/rc.conf` depending on preference, add `sshd_enable = "YES"` to the file, save, and exit. Enter command `service sshd enabled` to enable the service (enabled vs start indicates whether sshd starts one time or on every reboot).



Using an FTP client, such as FileZilla, log in with the jail IP address and user credentials. It is like SSH on TrueNAS. Browsing to other folders and locations beyond the user home directory is possible. But unlike running on TrueNAS directly, only the components of the jail are available.

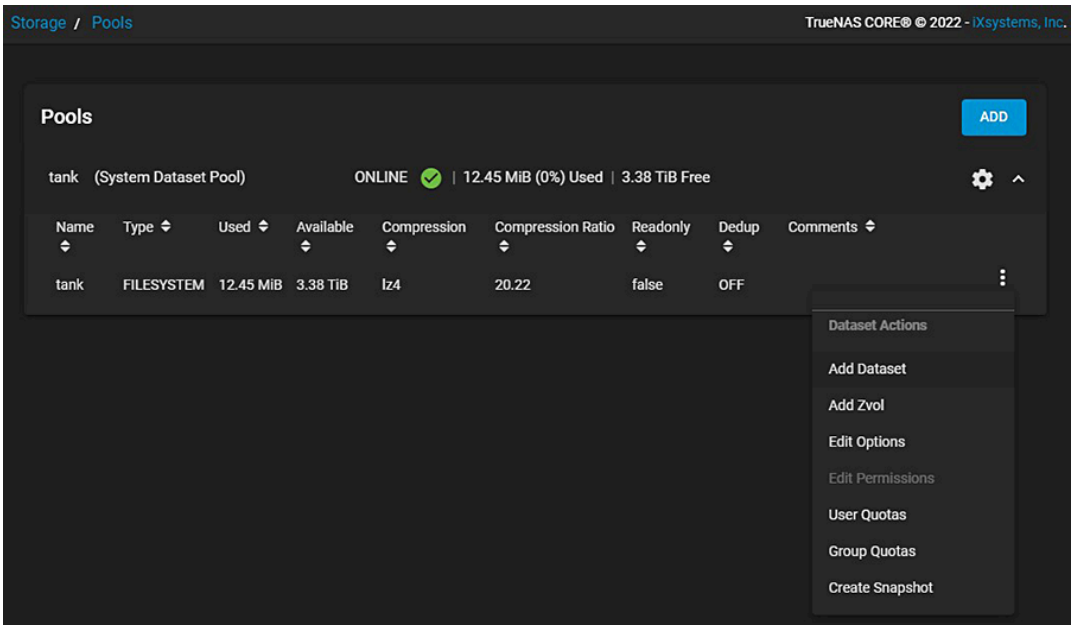

sftp://bob@192.168.123.137 - FileZilla
File Edit View Transfer Server Bookmarks Help New version available!
Host: sftp://192.168.123. Username: bob Password: Port: Quickconnect
Status: Directory listing of "/usr/home/bob" successful
Status: Connecting to 192.168.123.137...
Status: Connected to 192.168.123.137
Status: Starting upload of /home/joe/Pictures/waving_cat.gif
Status: File transfer successful, transferred 7,759,201 bytes in 1 second
Status: Retrieving directory listing of "/usr/home/bob"...
Status: Listing directory /usr/home/bob
Status: Directory listing of "/usr/home/bob" successful
Local site: /home/joe/Pictures/
Remote site: /usr/home/bob
Filename Filesize Filetype Last modified
wallpapers Directory 12/25/2018 09:26:48 ...
new Directory 02/27/2019 07:34:18 ...
old Directory 02/27/2019 07:34:18 ...
Coffee_roasting.gif 3,006,411 gif-file 02/12/2020 08:41:51 ...
waving_cat.gif 7,759,201 gif-file 01/09/2019 08:22:51 ...
coffee cup.jpg 29,632 jpg-file 11/30/2005 04:48:06 ...
lake_wallpaper_darke... 399,009 jpg-file 08/25/2018 10:10:30 ...
mountain_lake.jpg 268,578 jpg-file 08/30/2020 09:36:51 ...
ubuntu_samba_3.jpg 207,909 jpg-file 12/20/2018 12:37:48 ...
wallpapersden.com_g... 1,761,281 jpg-file 08/26/2018 09:10:31 ...
MothersDay2018.png 2,493,566 png-file 05/11/2018 11:32:30 ...
Saving_as_excel_file.png 495,613 png-file 08/13/2016 04:31:15 ...
Selected 1 file. Total size: 7,759,201 bytes
newdir
bob
Filename Filesize Filetype Last modified Permission Owner/Gro
.cshrc 1,055 File 09/08/2020 ... -rw-r--r-- bob bob
.login 392 File 09/08/2020 ... -rw-r--r-- bob bob
.login_conf 163 File 09/08/2020 ... -rw-r--r-- bob bob
.mail_aliases 379 File 09/08/2020 ... -rw------ bob bob
.mailrc 336 File 09/08/2020 ... -rw-r--r-- bob bob
.profile 952 File 09/08/2020 ... -rw-r--r-- bob bob
.rhosts 281 File 09/08/2020 ... -rw------ bob bob
.shrc 851 File 09/08/2020 ... -rw-r--r-- bob bob
waving_cat.gif 7,759,201 gif-file 09/08/2020 ... -rw-r--r-- bob bob
9 files. Total size: 7,763,610 bytes
Server/Local file Directio Remote file Size Priority Time Reason
Queued files Failed transfers Successful transfers (8)
Queue: empty

Configuring FTP

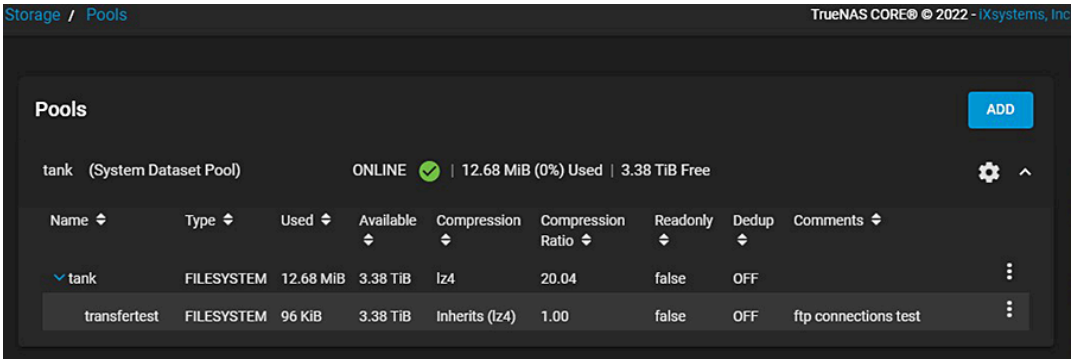
FTP Connections

FTP connections cannot share connections with other accounts, such as SMB connections. FTP connections need a new dataset and local user account.

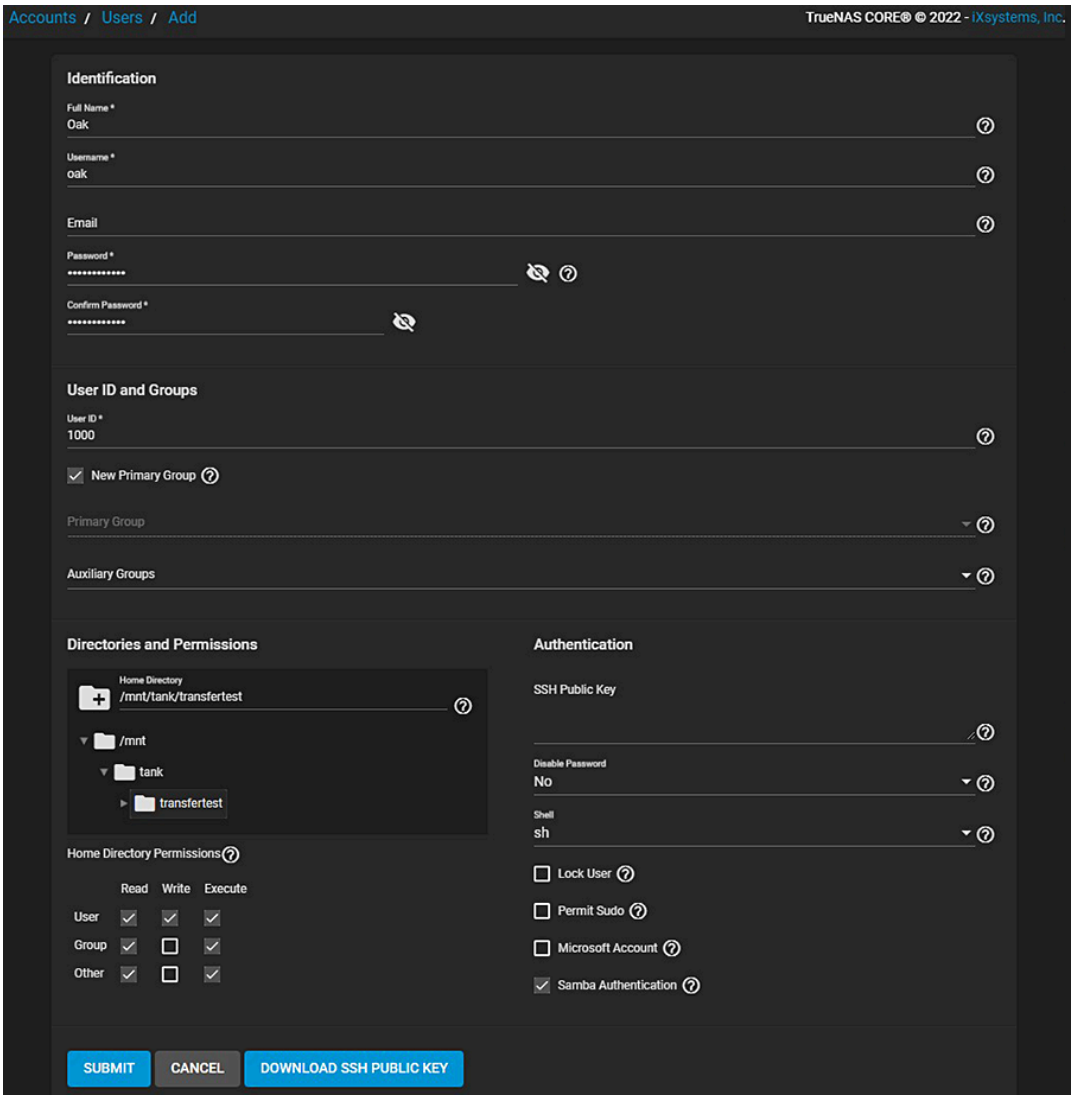
Go to **Storage > Pools** to add a new dataset.



See Creating Datasets for information on how to create the dataset. After this step is completed, the new dataset appears nested beneath the pool.

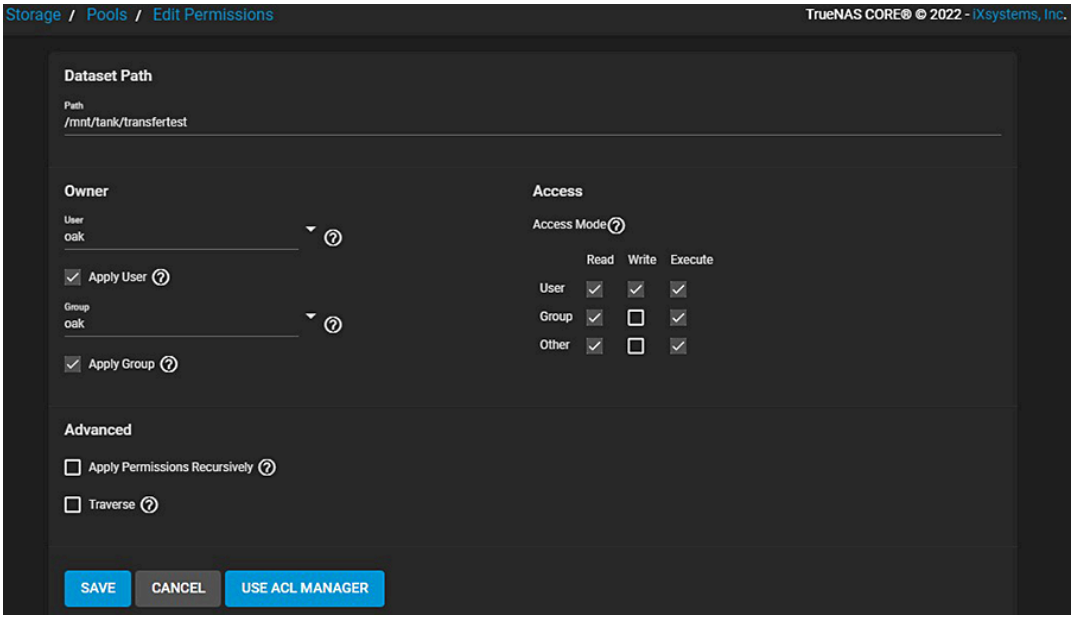


Next, go to **Accounts > Users > Add** to create a local user on the TrueNAS.



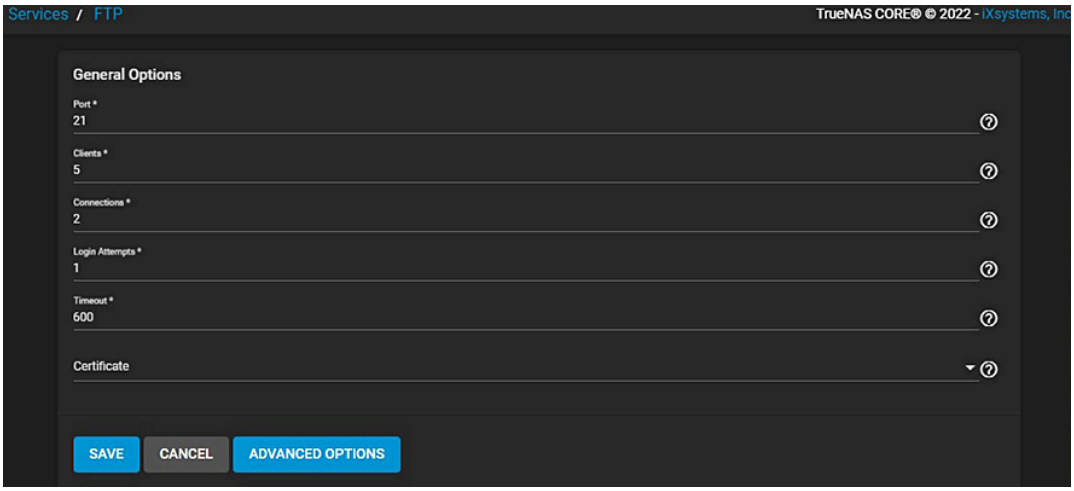
Assign a user name and password. Link the new dataset for the FTP share as the home directory of the user. Link the new dataset for the FTP share on a per user basis, or create a global account for FTP. Example: OurOrgFTPacnt, etc.

Return to **Storage > Pools**, find the new dataset, and click ⋮ **> Edit Permissions**. In the **Owner** fields, select the new user account as the **User** and **Group** from the dropdown list. Be sure to select **Apply User** and **Apply Group** before saving.



Service Configuration

To configure FTP, go to the **Services** page, find the **FTP** entry, and click the ✎.



Configure the options according to your environment and security considerations. See FTP Screen

Advanced Options

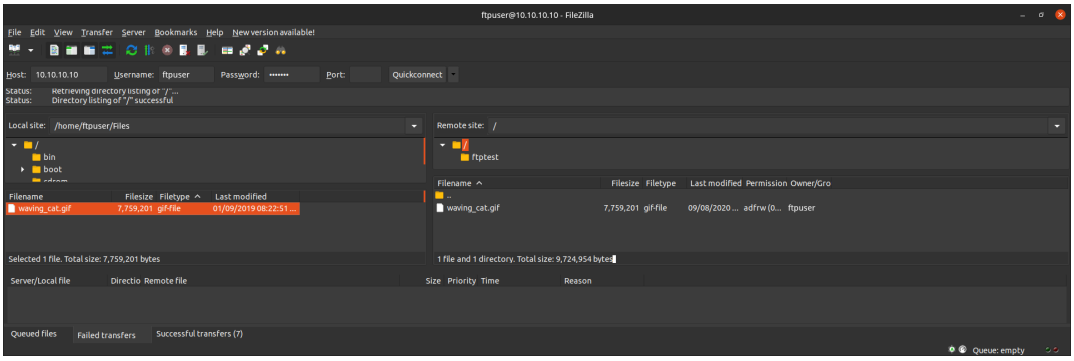
Enable **chroot** to help confine FTP sessions to a local user home directory and allow **Local User Login**.

> Unless necessary, do not allow anonymous or root access. For better security, enable TLS when possible. This is effectively FTPS. Enable TLS when FTP involves a WAN.

FTP Connection

Use a browser or FTP client to connect to the TrueNAS FTP share. The images here show using FileZilla, a free option.

The user name and password are those of the local user account on the TrueNAS. The default directory is the same as the user /home directory. After connecting, you can create directories and upload or download files.



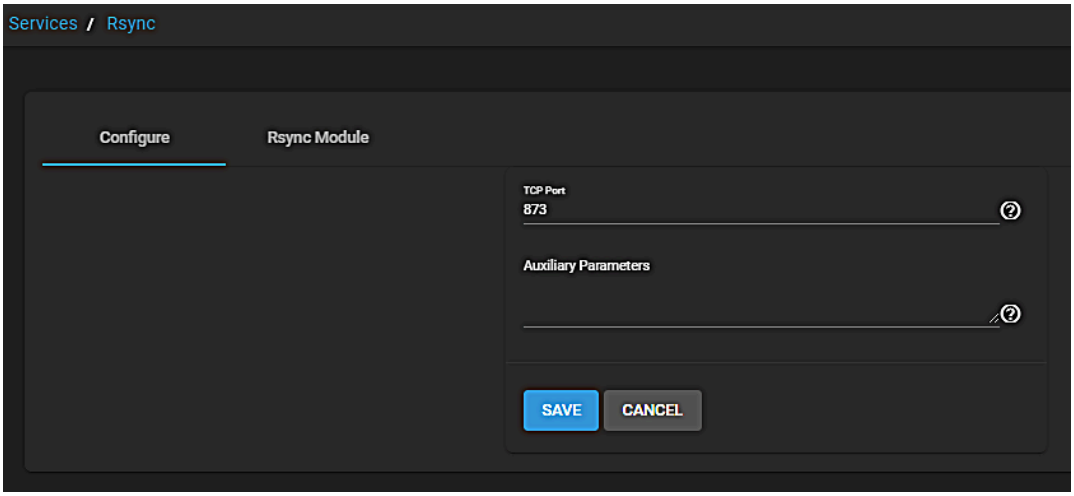
Configuring Rsync

Rsync is an open source cross-platform file transfer and synchronization utility. It is a fast and secure way to copy data to another system for backup or to migrate data to a new system. Use the default settings unless you require a specific change. Don't forget to click **SAVE** after changing any settings.

Log in to the TrueNAS web interface and go to **Services > Rsync**. Click the icon to edit the Rsync settings.

Rsync Configuration Screen

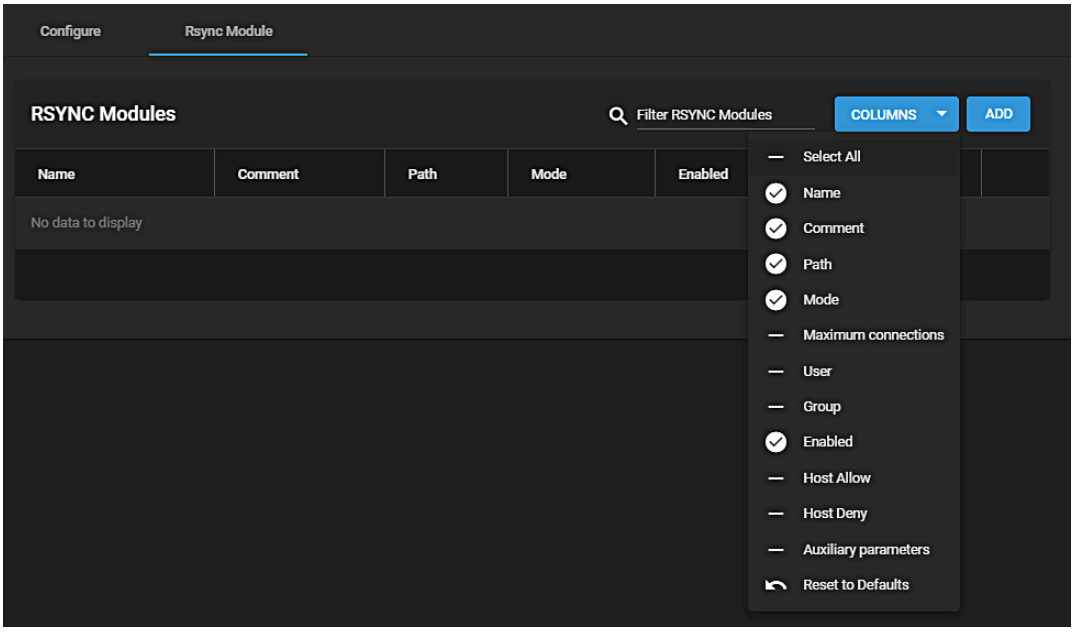
Enter the **TCP Port** you want Rsync to listen on, then enter any rsyncd.conf(5) **Auxiliary Parameters**.



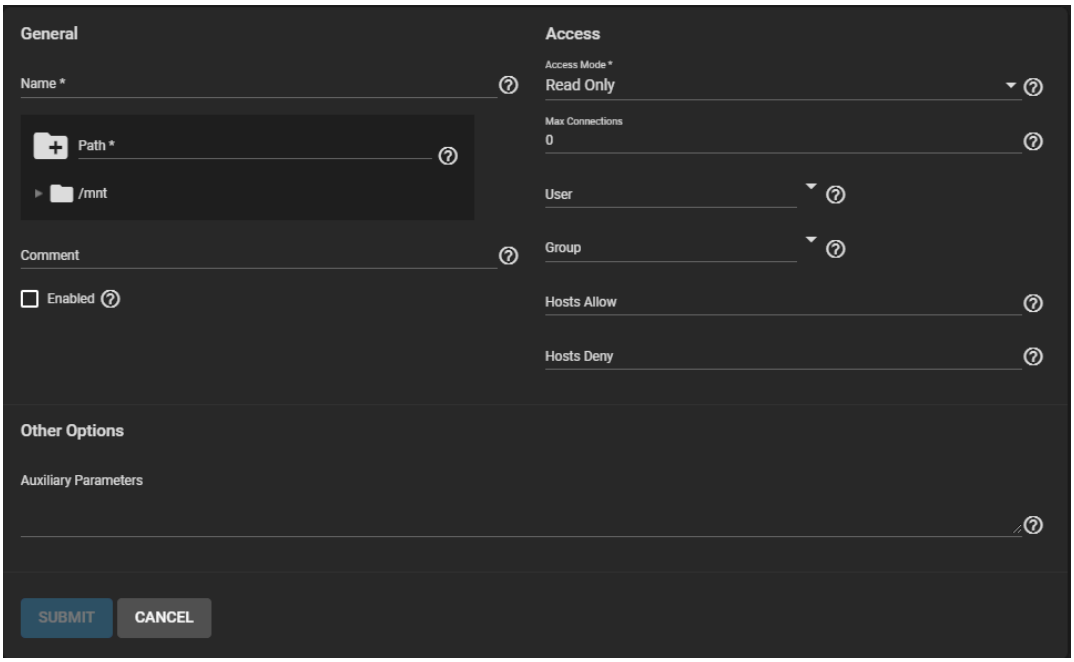
Rsync Modules

TrueNAS lists all created modules here.
Use this **Rsync Modules** list to **EDIT** or **DELETE** a module. Click ❯ to select a module to edit.

To create a new module, click **ADD**.



Name the module and select a **Path** to store it in. Select an **Access Mode** and fill out the rest of the fields to your needs.



▼ Rsync Services Add Module Options Defined

General

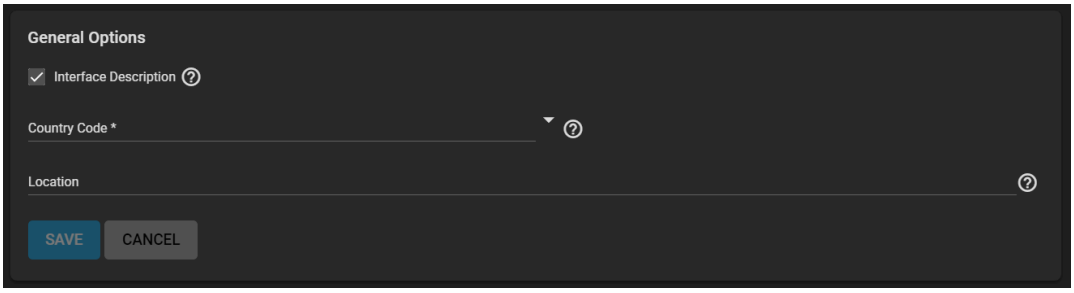
Name	Description
Name	Enter the IP address or host name of the system that will store the copy. Use the format `username@remote_host` if the user name differs on the remote host.
Path	Browse to pool or dataset to store received data.
Comment	Enter a description for this module.
Enabled	Select to activate this rsync module. Clear to deactivate but retain module configuration.
Access Mode	Select from dropdown list. **Read Only**, **Write Only**, **Read and Write**.
Max Connections	Enter a maximum number of connections. 0 is unlimited.
User	Select from dropdown list a user to run as during file transfers to and from this module.
Group	Select from dropdown list a group to run as during file transfers to and from this module.
Hosts Allow	Enter a value from rsyncd.conf(5). A list of patterns to match with the host name and IP address of a connecting client. Connection rejected if no patterns match. Separate entries by pressing `Enter`.
Hosts Deny	Enter a value from rsyncd.conf(5). A list of patterns to match with the host name and IP address of a connecting client. Connection rejected when the patterns match. Separate entries by pressing `Enter`.
Other Options: Auxiliary Parameters	Enter any additional parameters from rsyncd.conf(5).

> When a **Hosts Allow** list is defined, only the IPs and hostnames on the list are able to connect to the module.

Configuring LLDP

Network devices use the Link Layer Discovery Protocol (LLDP) to advertise their identity, capabilities, and neighbors on an Ethernet network. TrueNAS uses the ladvd LLDP implementation. LLDP service is often used in a local network environment with managed switches. Configuring and starting the LLDP service allows the TrueNAS system to advertise itself on the network.

To configure LLDP, go to the **Services** page, find the **LLDP** entry, and click the icon.



Select **Interface Description** and enter a **Country Code**. The location of the system is optional.

Click **SAVE** to save the current selections and return to the **Services** screen.

Click the toggle on the **Services** screen to turn the LLDP service on. The toggle turns blue when it is running.

Configuring OpenVPN

About OpenVPN

A virtual private network (VPN) is an extension of a private network over public resources. It allows remote clients on a public network to access a private network via a secure connection. TrueNAS provides OpenVPN as a system level service that provides VPN server or client functionality. TrueNAS uses a single TCP or UDP port to act as a primary VPN server. This allows remote clients access to data stored on the system. VPN integration is possible even if the system is in a separate physical location, or only has access to public networks.

Obtaining a Public Key Infrastructure (PKI)

Public key infrastructure (PKI) must be in place before configuring TrueNAS as either an OpenVPN server or client. PKI utilizes certificates and certificate authorities created in or imported to TrueNAS.

▼ What does this do?

TrueNAS authenticates with clients or servers by confirming network credentials. These must be signed by a valid master certificate authority (CA). To read more about the required PKI for OpenVPN, see the OpenVPN PKI Overview.

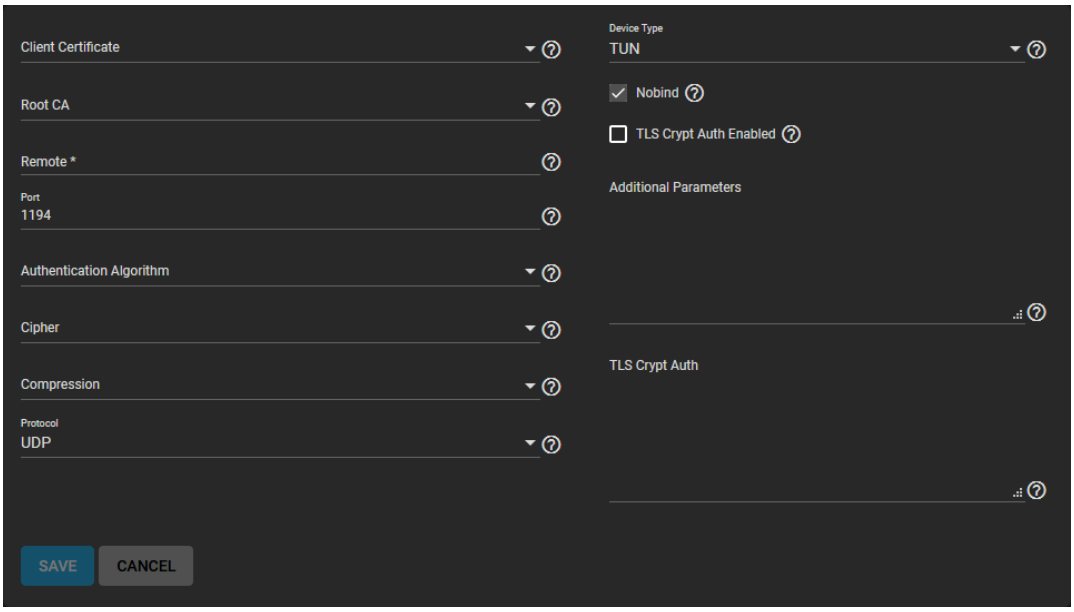
Configuring OpenVPN: Process Overview

The general process to configure OpenVPN (server or client) on TrueNAS is to:

- Select the networking credentials
- Set the connection detail
- Choose any additional security or protocol options

Configuring OpenVPN Client

Go to the **Services** page and find the **OpenVPN Client** entry. Click the ✎ to configure the service.



Choose the certificate to use as an OpenVPN client. This certificate must exist in TrueNAS and be in an active (unrevoked) state.

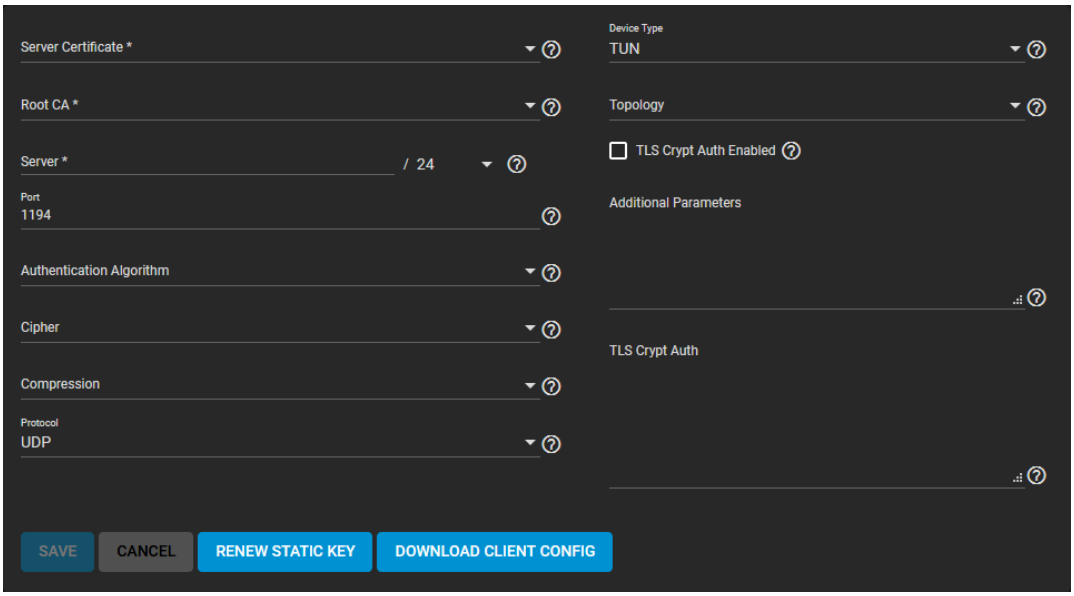
Enter the host name or IP address of the **Remote** OpenVPN server.

Select any other connection settings that fit with your network environment. Check for performance requirements. The **Device Type** must match with the OpenVPN server **Device Type**. **Nobind** prevents using a fixed port for the client. Enabled by default, it allows the OpenVPN client and server to run at the same time.

Review the Security Options and select settings that meet your network security requirements. Determine if the OpenVPN server is using TLS Encryption. If so, copy the static TLS encryption key and paste into the **TLS Crypt Auth** field.

OpenVPN Server

Go to the **Services** page and find the **OpenVPN Server** entry. Click the ✎ to configure the service.



Choose a **Server Certificate** for this OpenVPN server. This certificate must exist in TrueNAS and be in an active (unrevoked) state.

Define a IP address and netmask for the OpenVPN. Enter these values in **Server**. Continue to select the remaining Connection Settings that fit with your network environment and performance requirements. When selecting **TUN** in **Device Type**, you can select a virtual addressing method for the server in **Topology**. Options are:

- **NET30**: Use one **/30** subnet per client in a point-to-point topology. Designed for use when connecting clients are Windows systems.
- **P2P**: Point-to-point topology. Points the local server and remote client endpoints to each other. One IP address given to each client. This is only recommmended when none of the clients are a Windows system.
- **SUBNET**: The interface uses an IP address and subnet. One IP address given to each client. Windows clients need the **TAP-Win32 driver** version 8.2 or newer. **TAP** devices always use the **SUBNET** specified in **Topology**.

The **Topology** selection is automatically applied to any connected clients.

When **TLS Crypt Auth Enabled** is selected, TrueNAS generates a static key for the **TLS Crypt Auth** field after saving the options. To change this key, click **RENEW STATIC KEY**. Any clients connecting to the server need this key. Keys stored in the system database are included in a generated client config file. A good practice is to back up keys in a secure location.

Review the Security Options and choose settings that meet your network security requirements.

Configure and save your OpenVPN server settings.

OpenVPN client systems that are connecting to this server will need to import client configuration files. To generate client configuration files, you need the client certificate from the client system. The client certificate was previously imported to the client system. Click **DOWNLOAD CLIENT CONFIG** and select the **Client Certificate**.

Connection Settings

See OpenVPN Screens for more information on the client and server settings.

Security Options

Connecting to a private network still sends data over less secure public resources. OpenVPN includes several security features that are optional. These optional security features help protect the data sent into or out of the private network.

- **Authentication Algorithm**: This is used to validate packets that are sent over the network connection. Your network environment might require a specific algorithm. **SHA1 HMAC** is a good standard algorithm to use if a particular algorithm is not required.
- **Cipher**: This is an algorithm to encrypt data packets sent through the connection. While not required, choosing a cipher can increase connection security. Verify the required ciphers for your networking environment. If there are no specific cipher requirements, **AES-256-GCM** is a good default choice.
- **TLS Encryption**: Selecting **TLS Crypt Auth Enabled** encrypts all TLS handshake messages. This adds another layer of security. OpenVPN server and clients share a required static key.

Service Activation

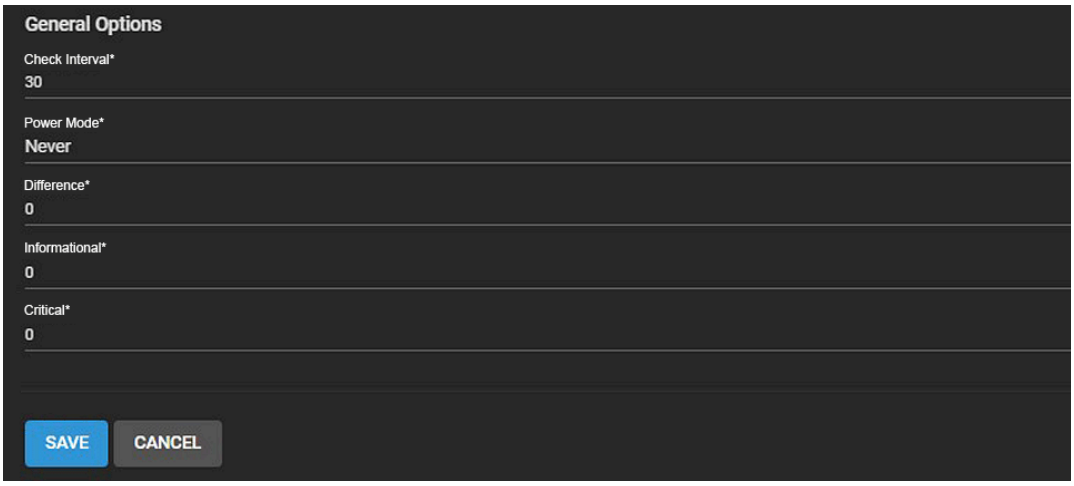
When finished configuring the server or client service, click **SAVE**. Start the service by clicking the related toggle in **Services**. To check the current state of the service, hover over the toggle.

Start Automatically: Selecting this option starts the OpenVPN service whenever TrueNAS completes booting. The network and data pools must be running.

Configuring S.M.A.R.T.

S.M.A.R.T. Self-Monitoring, Analysis and Reporting Technology (SMART) is an industry standard. It performs disk monitoring and testing. Several different kinds of self-tests check disks for problems.

Click the ✎ in **Services > S.M.A.R.T.** to configure the service.



General Options

Name	Description
Check Interval	Enter number of minutes to determine how often the smartd daemon monitors for configured tests to be run.
Power Mode	Select from dropdown list: **Never**, **Sleep**, **Standby** or **Idle**. Tests only run with **Never**.
Difference	Enter in degrees Celsius. S.M.A.R.T. sends alerts if the temperature of a drive changes by N degrees Celsius since the last report.
Informational	Enter in degrees Celsius. S.M.A.R.T. sends messages with a log level of LOG_INFO if the temperature exceeds the threshold.
Critical	Enter in degrees Celsius. S.M.A.R.T. sends messages with a log level of LOG_CRIT if the temperature exceeds the threshold.

Service Activation

Click **SAVE** when finished configuring the server or client service. Start the service by clicking the related toggle in **Services**. To check the current state of the service, hover over the toggle.

Selecting **Start Automatically** starts the service whenever TrueNAS completes booting. The network and data pools must be running.

Configuring S3 (deprecated)

Due to security vulnerabilities and maintainability issues, the S3 service is deprecated in TrueNAS 13.0 and removed in TrueNAS 22.12 and newer versions. Beginning in CORE 13.0-U6, the CORE web interface generates an alert when the deprecated service is either actively running or is enabled to start on boot.

TrueNAS Enterprise

Beginning in CORE 13.0-U6, Enterprise customers with the S3 service running or enabled are prevented from upgrading to 13.3.

Please contact iX Support to review options for migrating to a TrueNAS release that has Minio applications available.

▼ Contacting Support

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.

iXsystems Customer Support	
Support Portal	https://support.ixsystems.com
Email	support@ixsystems.com
Telephone and Other Resources	https://www.ixsystems.com/support/

S3 for MinIO (deprecated)

Due to security vulnerabilities and maintainability issues, the S3 service is deprecated in TrueNAS 13.0 and removed in TrueNAS 22.12 and newer versions. Beginning in CORE 13.0-U6, the CORE web interface generates an alert when the deprecated service is either actively running or is enabled to start on boot.

TrueNAS Enterprise

Beginning in CORE 13.0-U6, Enterprise customers with the S3 service running or enabled are prevented from upgrading to 13.3.

Please contact iX Support to review options for migrating to a TrueNAS release that has Minio applications available.

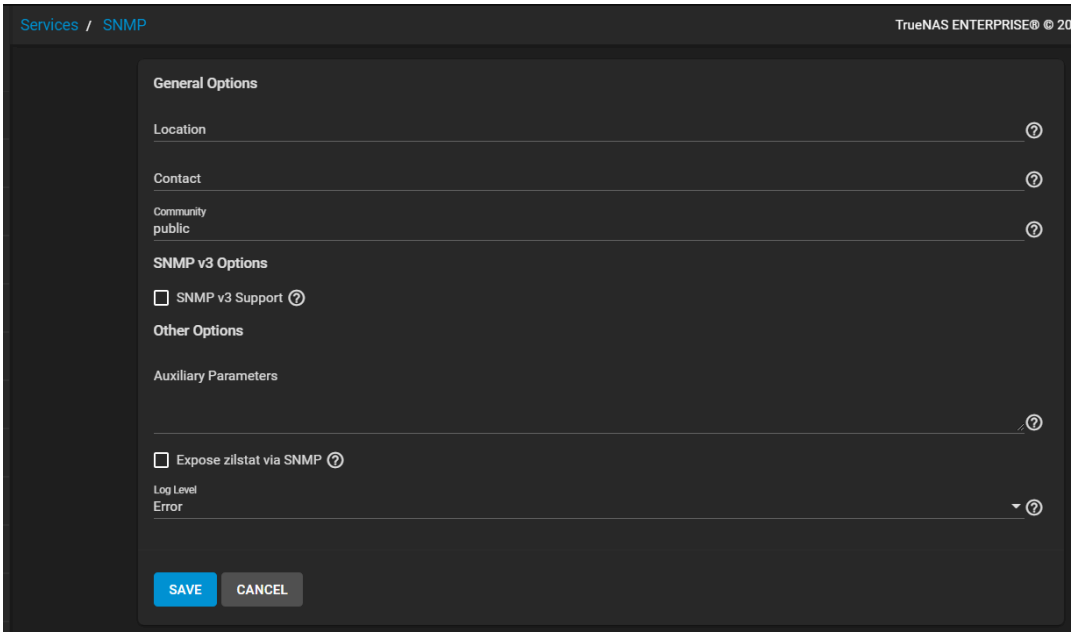
▼ Contacting Support

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.

iXsystems Customer Support	
Support Portal	https://support.ixsystems.com
Email	support@ixsystems.com
Telephone and Other Resources	https://www.ixsystems.com/support/

Configuring SNMP

SNMP (Simple Network Management Protocol) monitors network-attached devices for conditions that warrant administrative attention. TrueNAS uses Net-SNMP to provide SNMP. To configure SNMP, go to the **Services** page, find the **SNMP** entry, and click the ✎.

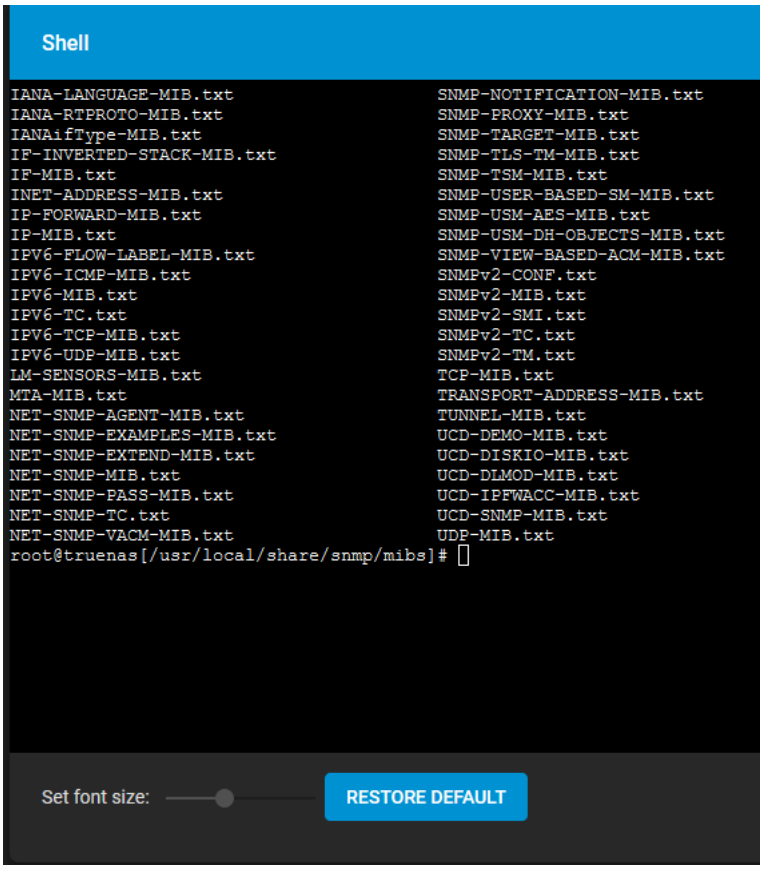


See SNMP screen for information on settings.

After starting the SNMP service, port **UDP 161** listens for SNMP requests.

Checking the Management Information Bases (MIBs) Directory

Locate available Management Information Bases (MIBs). Go to /usr/local/share/snmp/mibs. This directory contains many files routinely added or removed from the directory. Check the directory on your system. Open the shell and enter command `ls /usr/local/share/snmp/mibs`. Here is a sample of the directory contents:



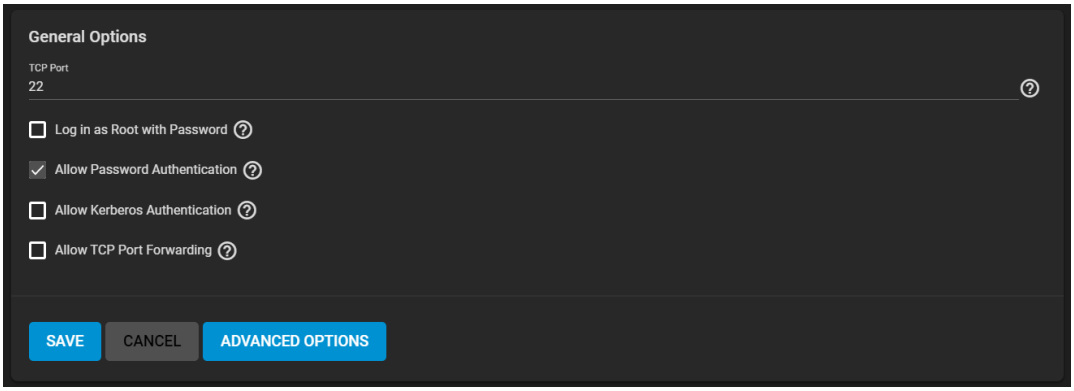
Configuring SSH

The SSH service allows connections to TrueNAS with the Secure Shell Transport Layer Protocol. To use TrueNAS as an SSH server, the users in the network must use SSH client software to transfer files with SSH.

> Allowing external connections to TrueNAS is a security vulnerability! Only enable SSH when there is a need for external connections. See Security Recommendations for more security considerations when using SSH.

Service Configuration

To configure SSH, disable the service and click the ✎.



Configure the options as needed to match your network environment.

See SSH Screen

> Root access to the system from a remote client is never recommended. If an unavoidable critical situation requires allowing root access, it is recommended to configure two-factor authentication first. Also, disable root logins as soon as possible.

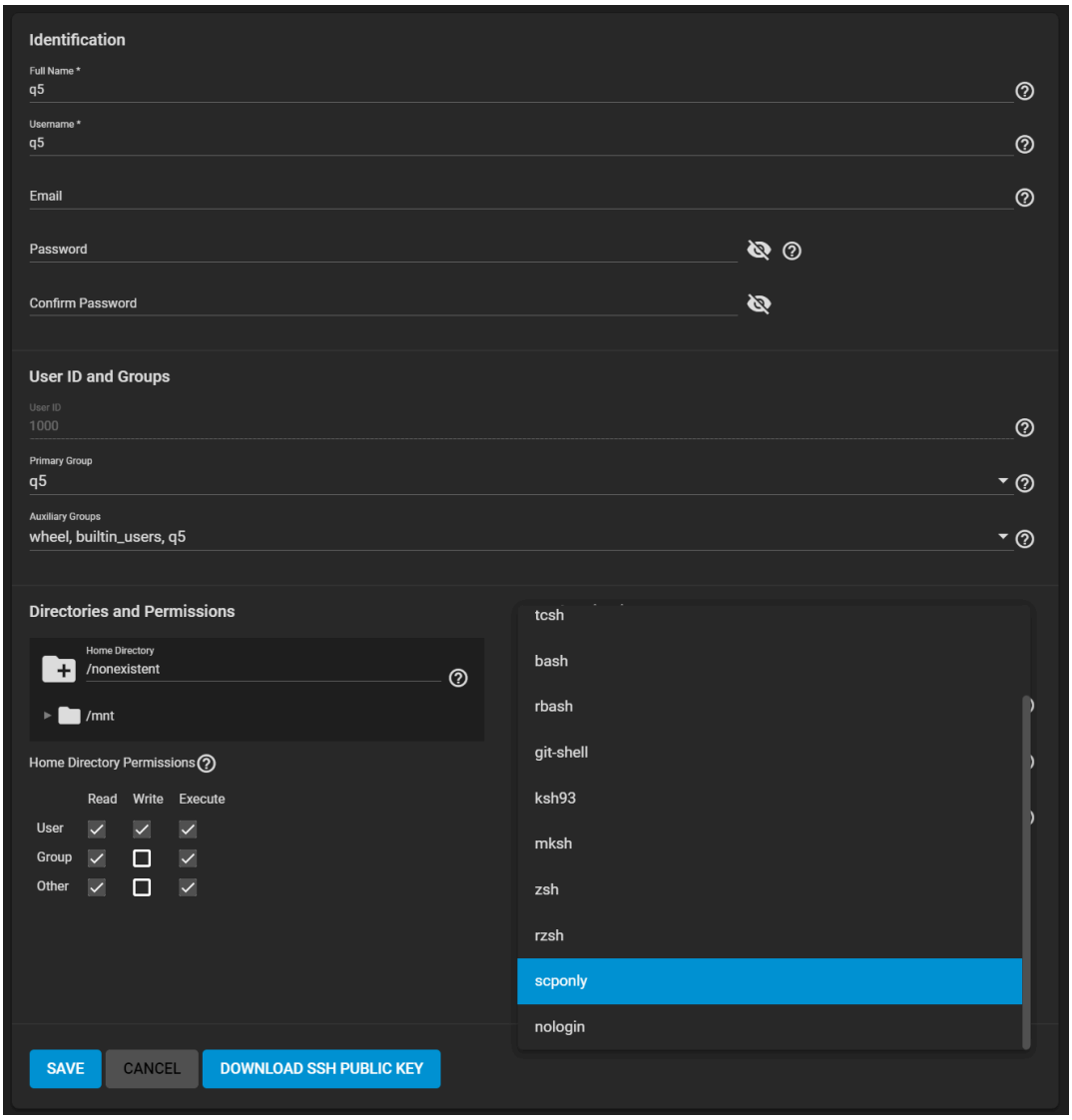
Re-enable the SSH service on the **Services** page when all configuration changes are complete. To create and store specific SSH connections and keypairs, go to the **System** menu section.

▼ Advanced: Restricting Command Line Users to scp or sftp

This only works for users that use command line versions of commands `scp` and `sftp`. With SSH configured, authenticated users with a user account can use `ssh` to log into the TrueNAS system over the network. Create user accounts by going to **Accounts > Users** and clicking **ADD**.

By default, the user sees their home directory after logging in with SSH. The user can still find system locations outside their home directory. Take security precautions before granting users SSH access to the system. One method to increase security is to change shell for a user to only allow file transfers. Users can still use commands `scp` and `sftp` to transfer files between their local computer and their home directory. But the TrueNAS system restricts them from logging into the system using `ssh`.

To configure this scenario, go to **Accounts > Users** and edit the desired user account. Change the **Shell** to **scponly**. Repeat for each user that needs restricted SSH access.



Test the configuration from another system. Run the `sftp`, `ssh`, and `scp` commands as that user account. `sftp` and `scp` work but `ssh` fails.

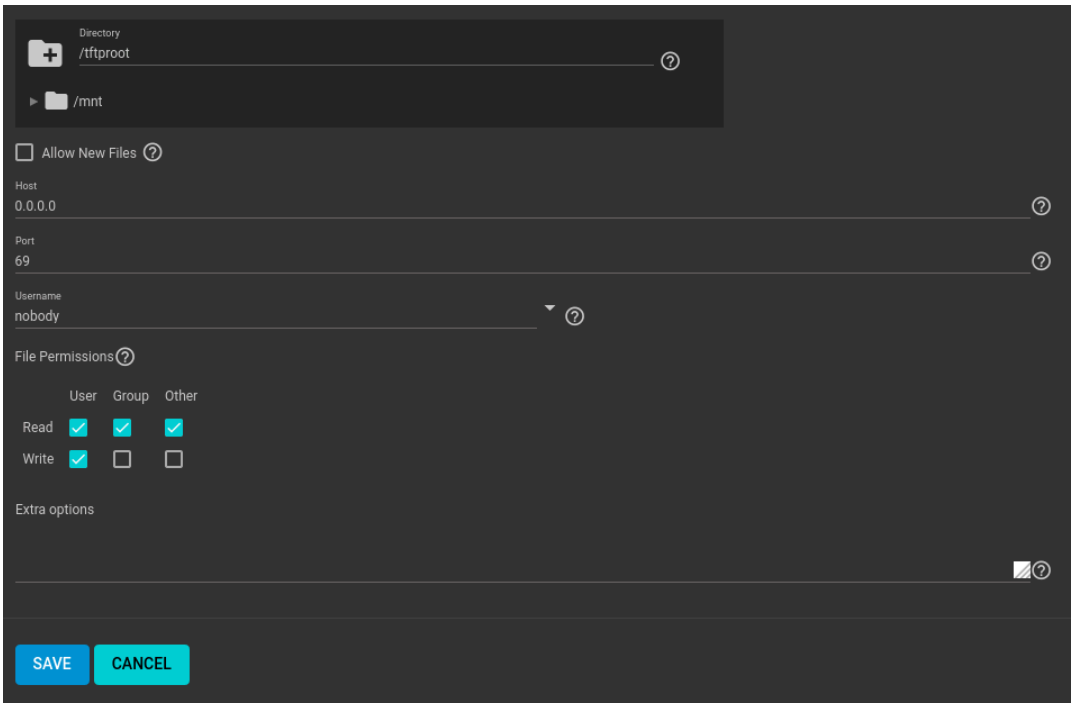
Configuring TFTP

Setting Up TFTP

The Trivial File Transfer Protocol (TFTP) is a light-weight version of FTP. It is often used in a local environment. It can transfer configuration or boot files between machines, such as routers. TFTP offers a very limited set of commands and provides no authentication.

Determine the usage requirements for the TrueNAS system. If they are minimal, configure TFTP. For example, if the TrueNAS system is only used for storing images. Or if it is only used to store configuration files for network devices.

If the system has minimal usage requirements, start the service. Starting the TFTP service opens UDP port **69**.



Use the **TFTP** screen to configure the system for SFTP.

Configuring UPS

An Uninterruptible Power Supply (UPS) is a power backup system that ensures continuous electricity during outages, preventing downtime and damage.

> TrueNAS uses NUT (Network UPS Tools) to provide UPS support. For supported device and driver information, see their hardware compatibility list.
>
> Report UPS bugs and feature requests to the NUT project.

Setting Up UPS Service

Connect the TrueNAS system to the UPS device. Configure the UPS service by going to **Services**, finding the **UPS** entry, and clicking edit icon.

> **TrueNAS Enterprise**
> TrueNAS High Availability (HA) systems are not compatible with uninterruptible power supplies (UPS).

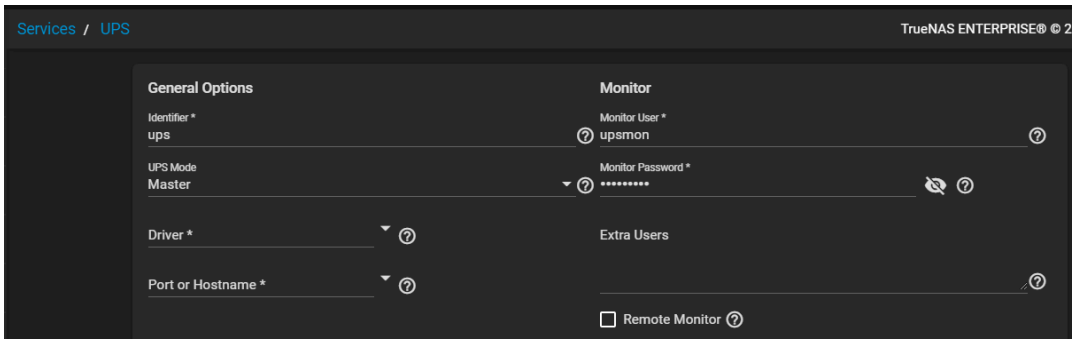


Figure 1: UPS Service Screen (Top)

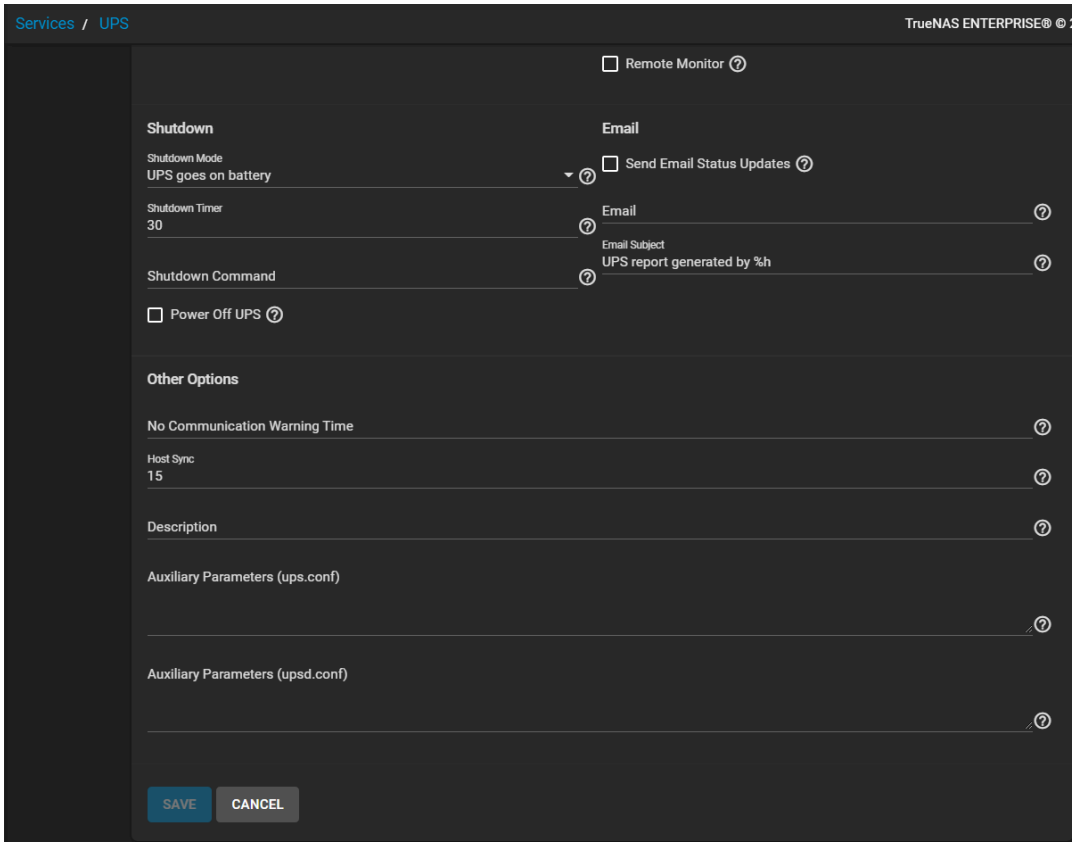


Figure 2: UPS Service Screen (Bottom)

See UPS Screen for more information on UPS settings. Some UPS models can be unresponsive with the default polling frequency. This shows in TrueNAS logs as a recurring error like `libusb_get_interrupt: Unknown error`. The default polling frequency is **two** seconds. Decrease the polling frequency by adding an entry to **Auxiliary Parameters (ups.conf)**: `pollinterval = 10`. This should resolve the error.

upsc(8) can get status variables like the current charge and input voltage from the UPS daemon. Run this command from the shell using the syntax `upsc ups@localhost`. The upsc(8) manual page has other usage examples.

If the hardware supports sending the command, upscmd(8) can send commands directly to the UPS. Only users with administrative rights can administer these commands. Create these users in the **Extra Users** field.

▼ How do I find a device name?

Determine the correct device name for the UPS. Go to **System > Advanced** and select **Show console messages**. Plug in the USB device and look for a /dev/ugen or /dev/uhid device name in the console messages.

▼ Can I attach multiple computers to one UPS?

A UPS with adequate capacity can power multiple computers. Connect one computer to the UPS data port with a serial or USB cable. This primary system makes UPS status available on the network for other computers. The secondary computers receive UPS status data from the primary computer. The secondary computers receive power from the UPS. See the NUT User Manual and NUT User Manual Pages.

FTP, SFTP, and TFTP

The File Transfer Protocol (FTP) is a simple option for data transfers. The additional SSH options provide secure config file transfer methods. Trivial FTP options provide only simple config file transfer methods.

Options for configuring **FTP**, **SSH**, and **TFTP** are in the system **Services**. Click the ✎ to configure the related service.

Virtualization (Obsolete)

As of TrueNAS 13.3, virtualization features (plugins, jails, and virtual machines) are obsolete and provided without support to the TrueNAS Community.

Users with a critical need to use containers or virtualization solutions in production should migrate to the tested and supported virtualization features available in TrueNAS SCALE.

TrueNAS Enterprise customers can contact iXsystems to schedule a TrueNAS 24.04 or newer deployment. See CORE to SCALE Migrations for more information.

Updating CORE

TrueNAS CORE has an integrated update system to make it easy to keep up to date.

> **TrueNAS Enterprise**
> TrueNAS 13.3 is not available for Enterprise deployments. Instead, 13.0 support continues with security and major bug fix releases. See the official announcement for details and software status page for up to date deployment recommendations.

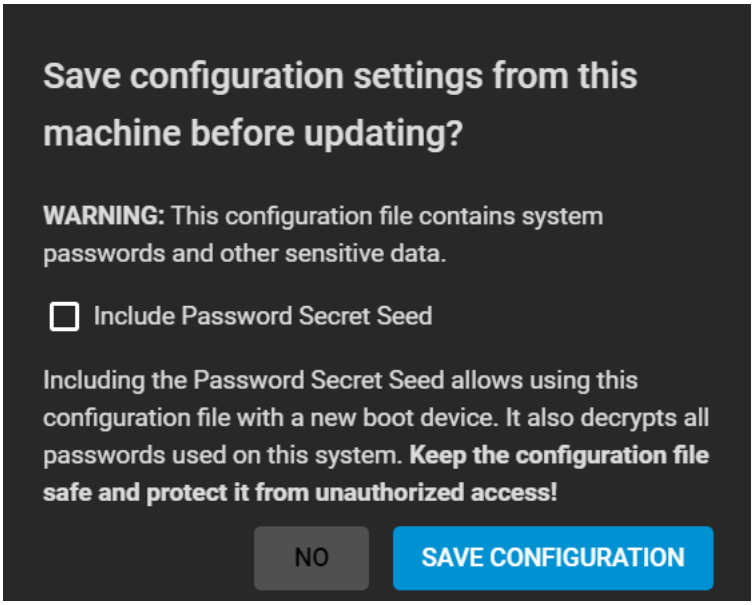
Prepare the System

We recommend performing updates when the TrueNAS system is idle, with no clients connected and no scrubs or other disk activity happening. Most updates require a system reboot. Plan updates around scheduled maintenance times to avoid disrupting user activities.

The update process does not proceed unless there is enough free space in the boot pool for the new update files. If a space warning displays, go to **System > Boot** to remove unneeded boot environments.

Save the Configuration File

A dialog to save the system configuration file appears before installing updates.



> Keep the system configuration file secure after saving it. The security information in the configuration file can grant unauthorized access to your TrueNAS system.

Update the System

Ensure the system is in a low-usage state as described above in Preparing for Updates.

Each update creates a boot environment. If the update process needs more space, it attempts to remove old boot environments. TrueNAS does not remove boot environments marked with the *Keep* attribute as shown in **System > Boot**. The upgrade fails if your system does not have space for a new boot environment. Space on the operating system device can be manually freed by going to **System > Boot** and removing the *Keep* attribute or deleting any boot environments that are no longer needed.

Manual Updates

You can manually download and apply updates in **System > Update**.

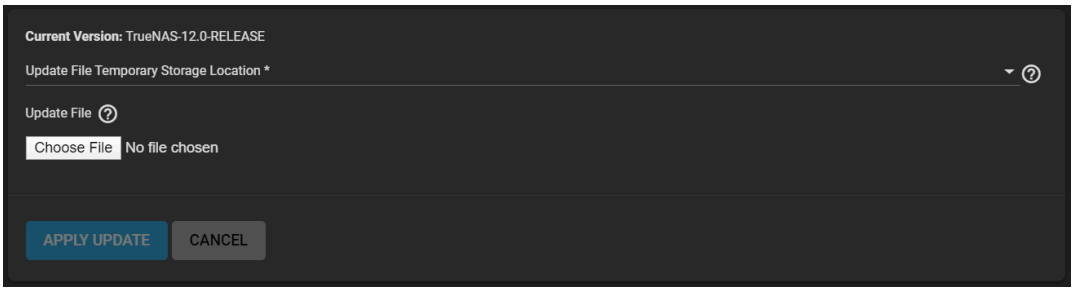
Go to https://www.truenas.com/download-truenas-core/ to find the latest 13.3 manual update file. Manual update file names end with manual-update.tar.

Download the desired update file to your local system. Log in to the TrueNAS web interface and go to **System > Update**. Click **INSTALL MANUAL UPDATE FILE**.

The **Save Configuration** dialog opens. You can save a copy of the current configuration to external media for backup in case of an update problem.

After the dialog closes, the manual update screen displays.

The current TrueNAS version displays for verification.



Select the manual update file saved to your local system using **Browse**. Set **Reboot After Update** to reboot the system after the update installs. Click **APPLY UPDATE** to begin the update.

Starting an update shows a progress dialog. When an update is in progress, the web interface shows an animated icon in the top row. Dialogs also appear in every active web interface session to warn that a system update is in progress. **Do not** interrupt a system update.

Upgrade Via ISO

To upgrade TrueNAS to a new major version using an .iso file, use the Release List to download the .iso to the computer that prepares the installation media.

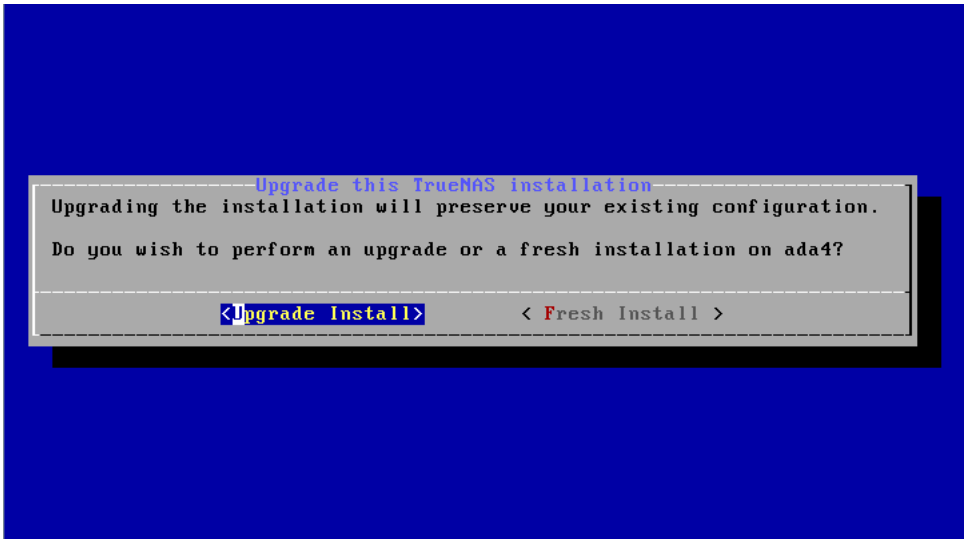
Burn the downloaded .iso file to a CD or USB stick. Refer to the Prepare the Install File instructions in the Installation article for tips about burning the .iso to media using different Operating Systems.

Insert the prepared media into the system and boot from it. The installer waits ten seconds in the installer boot menu before booting the default option. If needed, press `Spacebar` to stop the timer and choose another boot option. After the media finishes booting into the installation menu, press `Enter` to select the default option `1 Install/Upgrade`. The installer presents a screen showing all available drives.

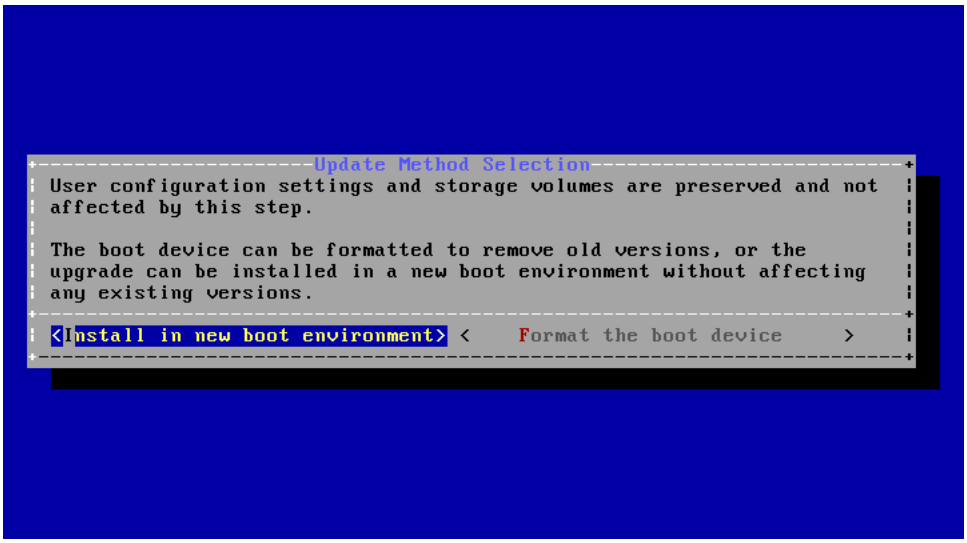
> All drives display, including boot drives and storage drives. Only choose boot drives when upgrading. **Choosing the wrong drives to upgrade or install causes data loss.** If you are unsure which drives contain the TrueNAS operating system, reboot and remove the install media. Log in to the TrueNAS web interface and go to **System > Boot > ACTIONS > Boot Pool Status** to identify the boot drives. More than one drive displays when using a mirror.

Highlight the drive where TrueNAS is installed and press `Spacebar` to mark it with a star. If using a mirror for the operating system, mark all the drives where the TrueNAS operating system is installed. Press `Enter` when done.

The installer recognizes earlier versions of FreeNAS/TrueNAS installed on the boot drives and asks to either upgrade or do a fresh install:

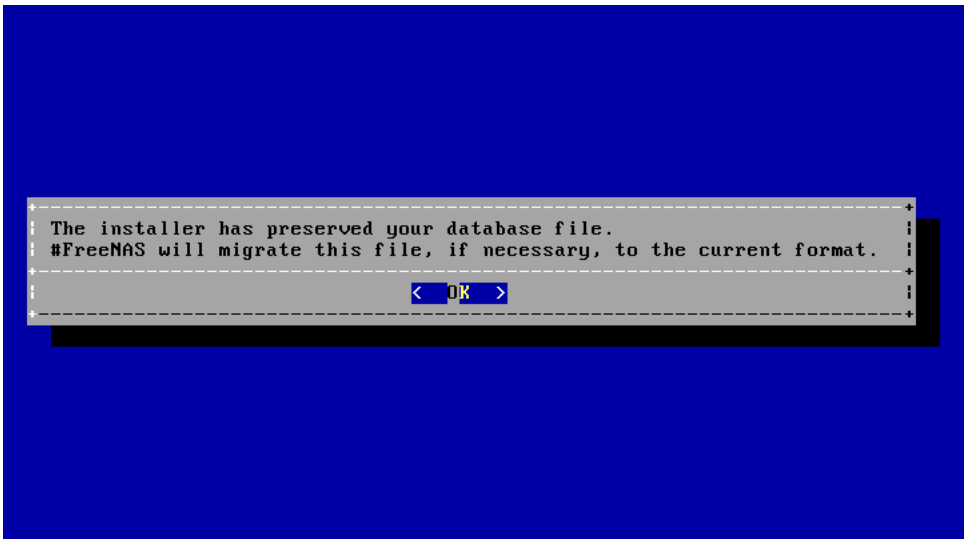


To perform an upgrade, press `Enter` to accept the default Upgrade Install. The installer displays another reminder that you should install the operating system on a disk you are not using for storage.



You can install the updated system in a new boot environment or format the entire operating system device to start fresh. Installing into a new boot environment preserves the old code, allowing a rollback to previous versions if necessary. Formatting the boot device is usually not necessary but can reclaim space. TrueNAS preserves user data and settings when installing in a new boot environment and formatting the operating system device. Move the highlight to one of the options and press `Enter` to start the upgrade.

The installer unpacks the new image and checks for upgrades to the existing database file. The database file that is preserved and migrated contains your TrueNAS configuration settings.



Press `Enter`. TrueNAS indicates that the upgrade is complete and a reboot is required. Press *OK*, highlight `3 Reboot System`, then press `Enter` to reboot the system. If the upgrade installer was booted from a CD, remove the CD.

During reboot, the previous configuration database can convert to the new version. The conversion happens during the reboot `Applying database schema changes` line. The conversion can take a long time to finish, sometimes fifteen minutes or more, and can cause the system to reboot again. The system boots normally afterward. If database errors display but the web interface is accessible, log in, go to **System > General**, and use the **UPLOAD CONFIG** button to upload the configuration backup you downloaded before starting the upgrade.

Updating CORE Enterprise

> **TrueNAS Enterprise**
> This is Enterprise content that specifically applies to High Availability (HA) systems with a TrueNAS Enterprise license active.

Updating a TrueNAS Enterprise system configured for High Availability (HA) has a slightly different flow from non-HA systems or TrueNAS Core. The system downloads the update to both controllers, updates and reboots the standby TrueNAS controller, and finally fails over from and updates the active TrueNAS controller.

Prepare the System

An update usually takes between thirty minutes and an hour. The system must reboot after the update, so it is recommended to schedule updates during a maintenance window, allowing two to three hours to update, test, and possibly roll back if issues appear. On large systems, we recommend a proportionally longer maintenance window.

For individual support during an upgrade, please contact iXsystems Support to schedule your upgrade.

▼ Contacting iXsystems Support

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.

iXsystems Customer Support	
Support Portal	https://support.ixsystems.com
Email	support@ixsystems.com
Telephone and Other Resources	https://www.ixsystems.com/support/

Scheduling at least two days ahead of a planned upgrade gives time to ensure a specialist is available for assistance. Updating from earlier than version 9.3 of TrueNAS must be scheduled with iXsystems Support.

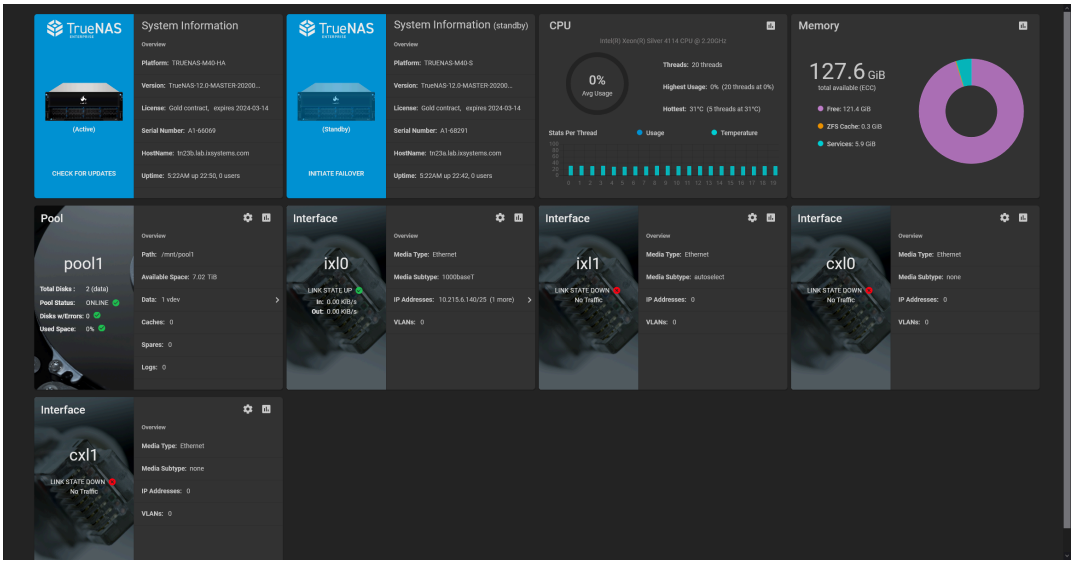
The update process will not proceed unless there is enough free space in the boot pool for the new update files. If a space warning displays, go to **System > Boot** and remove any unneeded boot environments.

Operating system updates only modify the OS devices and do not affect end-user data on storage drives.

> An update could involve upgrading the version of ZFS installed on the storage drives. When a ZFS version upgrade is available, an **Alert** appears in the web interface. We do not recommend upgrading the ZFS version on storage drives until you verify that you do not need to roll back to previous operating system versions or swap the storage drives with another system with an earlier ZFS version. After a ZFS version upgrade, the storage devices are not accessible by earlier TrueNAS versions.

Start the Update

In the web interface **Dashboard**, find the entry for the active TrueNAS controller and click **CHECK FOR UPDATES**. This button changes to **UPDATES AVAILABLE** when there is an available update.



Clicking the button goes to **System > Update** and shows the option to **Download Updates** or, when the system has detected and staged an update, **Apply Pending Update**.

When you click **Download Updates** or **Apply Pending Update**, TrueNAS gives an opportunity to save the current system configuration. We recommend backing up the system configuration before starting the update. Including the **Password Secret Seed** in the system configuration removes the encryption from sensitive system data, like stored passwords. When enabling this option, take extra precautions to store the downloaded system configuration file in a secure location.

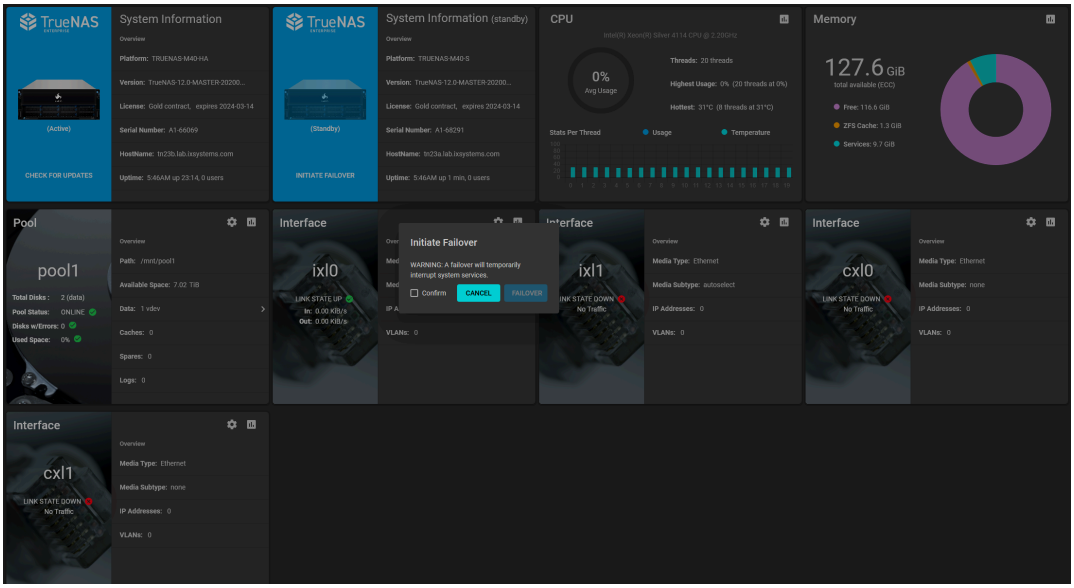
After downloading the system configuration, you can continue the system update. While updating and rebooting controllers, HA and other system services are briefly unavailable.

Other users logged in to the web interface see a warning dialog. A **System Updating** icon displays in the top bar of the web interface while the update is in progress.

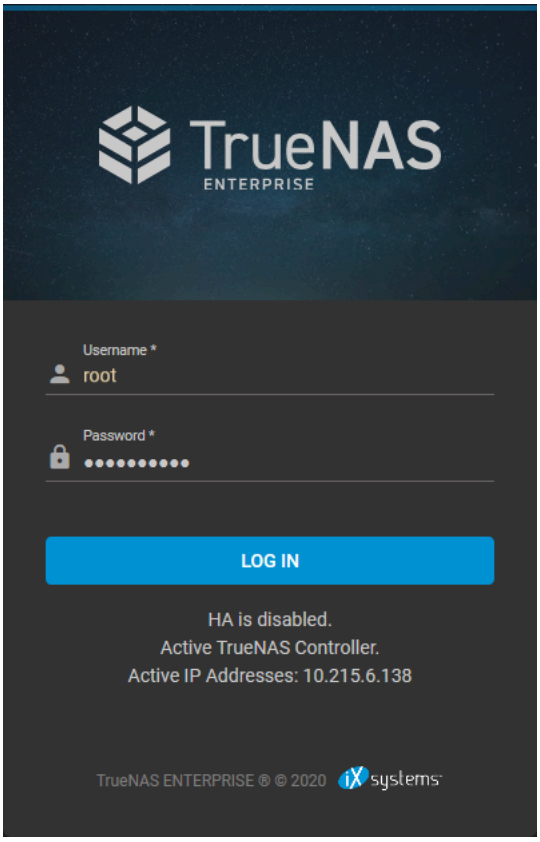
Update progress displays for both TrueNAS controllers. The standby TrueNAS controller reboots when it finishes updating. This can take several minutes. When the standby controller finishes booting, the system must fail over to update and reboot the active TrueNAS controller.

Failover to Complete the Update

To deactivate the active TrueNAS controller and finish the update, go to the **Dashboard**, find the entry for the Standby controller, and click **INITIATE FAILOVER**.



The failover briefly interrupts TrueNAS services and availability. The browser logs out of the web interface while the active TrueNAS controller deactivates and the standby TrueNAS controller is brought online. The web interface login screen reappears when the standby TrueNAS controller finishes activating.

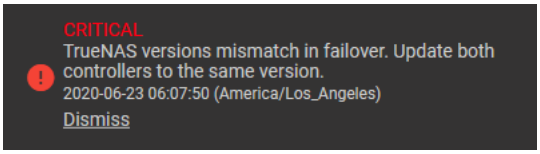


Log in to the web interface and check the HA status in the top toolbar. This icon shows that HA is unavailable while the previously active TrueNAS controller reboots. When HA is available, a dialog asks to finish the update. Click **CONTINUE** to finish updating the previously active TrueNAS controller.

Verify that the update is complete by going to the **Dashboard** and confirming that the **Version** is the same on both TrueNAS controllers.

▼ Reverting an Update

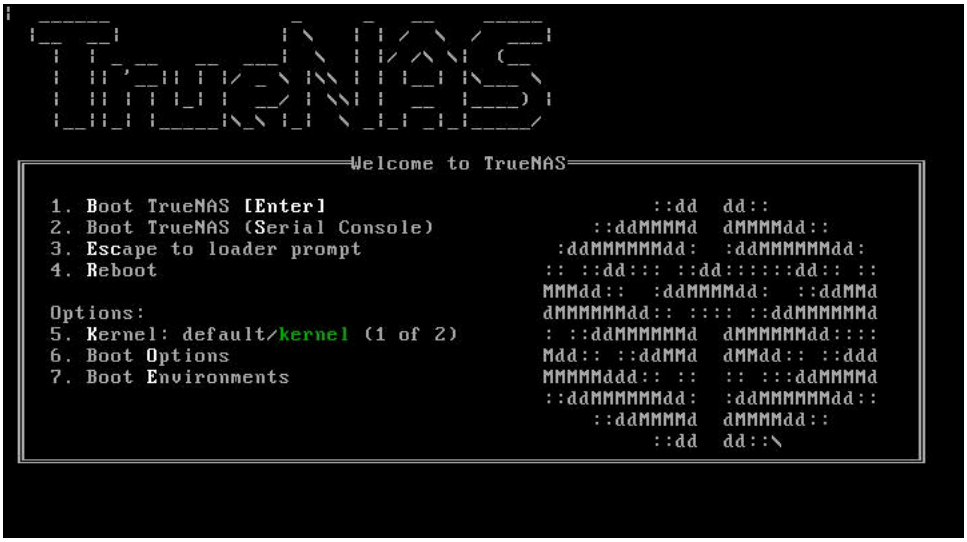
If the update did not install on one of the controllers, the web interface generates an alert about a mismatch between controller versions.



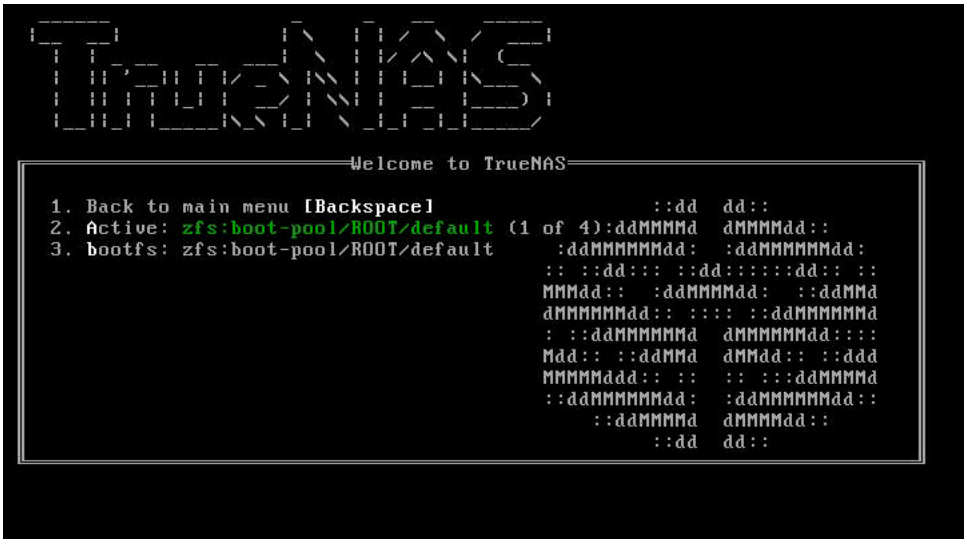
If something else goes wrong with the update, the system generates an alert and writes details to /data/update.failed.

You can return the system to its pre-update state by activating a previous boot environment during system boot. To ensure the versions match, do this procedure for both TrueNAS controllers. This requires physical or IPMI access to the TrueNAS controller console.

Reboot the system and press the space bar when the boot menu appears, pausing the boot process.



Open the **Boot Environments** menu and cycle the **Active** boot environment until one dated prior to the update displays.



Return to the first screen and press `Enter` to boot into that version of TrueNAS.

▼ Manually Updating an Enterprise HA System

Enterprise customers should contact iX Support for assistance updating their TrueNAS system.

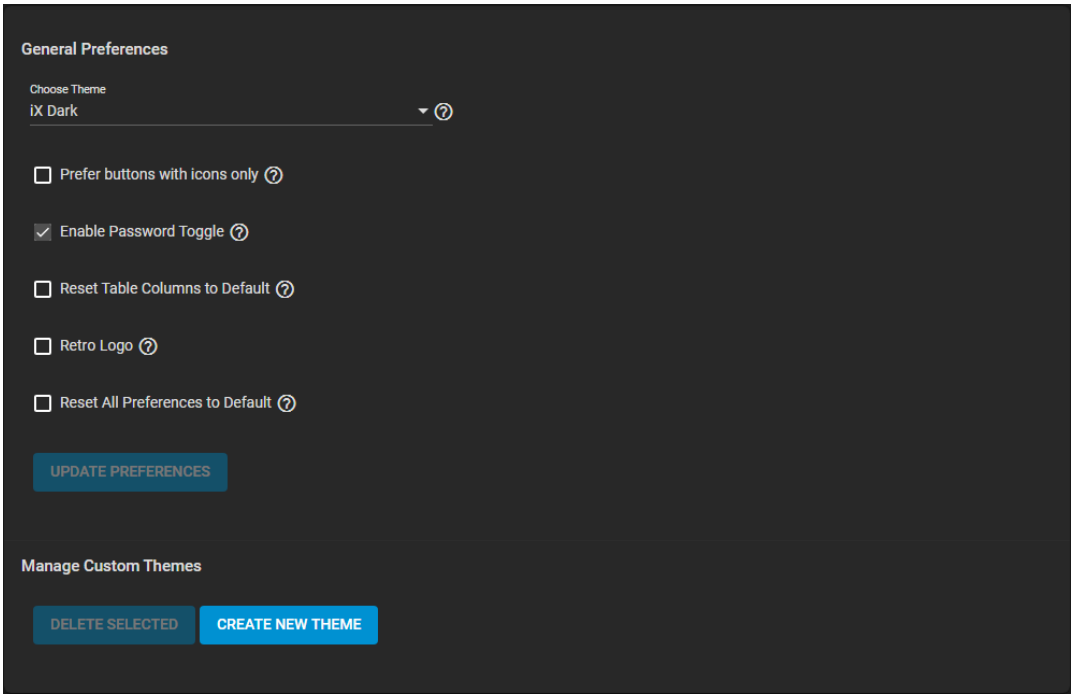
- Download the manual update file located at the TrueNAS/FreeNAS Download Page.
- Go to **System -> Update**.
- Click the **INSTALL MANUAL UPDATE** button.
- Set the **Include Password Secret Seed** checkbox and click the **Save Configuration** button.

- Select the **Update File Temporary Storage Location** and click **Choose File**. Select the manual upgrade file you downloaded. Wait for the file to upload, then click **APPLY UPDATE**.
- The Manual update uploads the file, installs it to both controllers, then reboots the Standby Controller. To complete the upgrade, click **Close** in the dialog box. Initiate a failover of the standby controller, as instructed, by clicking **INITIATE FAILOVER** from the Standby Controller's Dashboard card.
- Log into the system.
- Click **Continue** in the **Pending Upgrade** dialog box. The standby controller reboots completing the upgrade.

Setting UI Preferences

There are a few adjustable interface preferences. Also included is a built-in theme editor for creating your own TrueNAS color schemes.

To access user preferences, click **> Preferences**. This page has options to adjust global settings in the web interface. There are also options to manage custom themes and create new themes.



Tuning the Visibility of UI Elements.

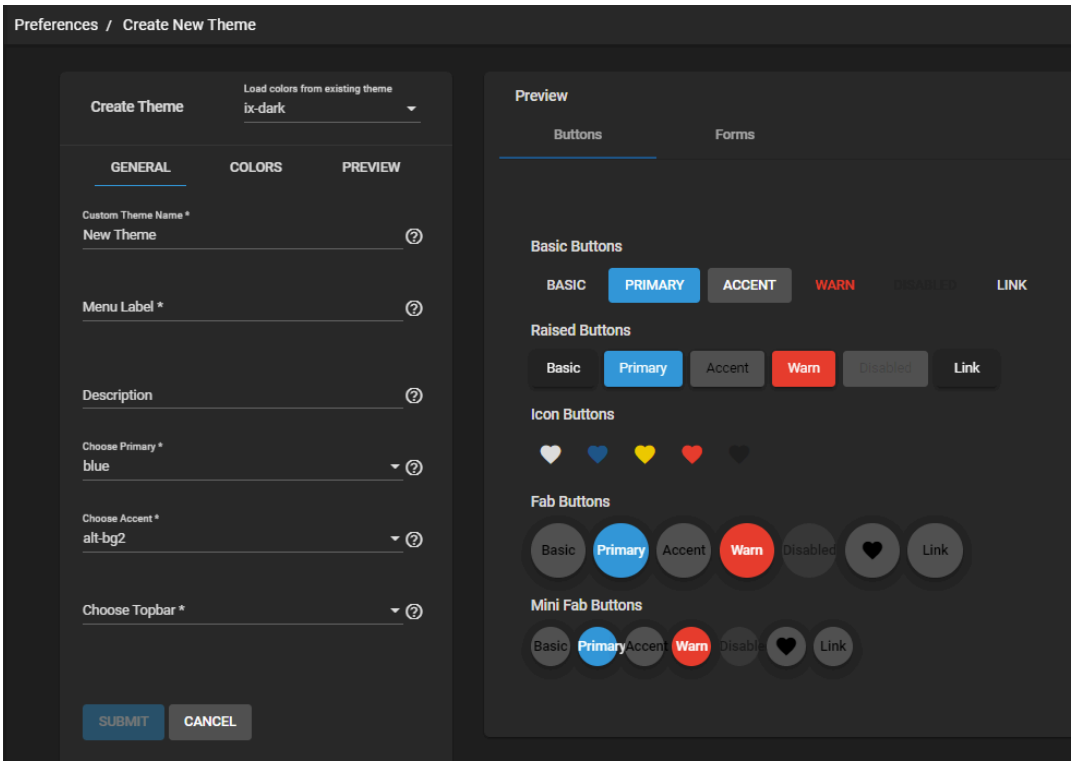
Click the **Choose Theme** dropdown list to change the color appearance of the web interface. Select from a range of pre-built or custom created themes. The **High Contrast** option offers the most visibility.

Select **Prefer buttons with icons only** when working with limited screen space. This displays icons and tooltips without text labels.

For increased security, clear the **Enable Password Toggle** checkbox. This removes all the icons next to password fields. It prevents the actual password characters from being visible.

Creating a Custom Theme

To create a custom theme, click **CREATE NEW THEME**.



1. Click **Load colors from existing theme** to change colors within an existing theme. Select an existing theme from the dropdown list to import into the configuration. This is useful when you have a theme you like but want to change a few colors within it.
2. Click the **COLORS** tab to define the color values for this new theme. Define color choices as either RGBA or hexadecimal values. Or click a color swatch to open a visual color picker.
3. Define color selections in the **COLORS** tab. These selections determine the options available on the **GENERAL** tab.
4. Color selections display in the **Preview**. The **Preview** updates to reflect your current choices. You can turn this feature off. Click the **PREVIEW** tab then click the **Global Preview** toggle. This allows you to compare these selections with the currently active theme.
5. Go to the **GENERAL** tab and choose the primary, accent, and topbar colors for the theme. The color selections you made in the **COLORS** tab determine the options shown here.
6. Name and label the theme. Click **SUBMIT** to save it and add it to the options on the **Preferences** page.