G-Technology®

SECURITY

ESSENTIAL GUIDE

G|RACK™ 12

High-Performance NAS

g-technology.com

G|RACK™ 12

Security Essentials

G-Technology®

Table of Contents

Security Essentials

Overview

We live in a digital world. Keeping our files safe is more important each day. We not only are storing more and more of our lives on digital media but we have constant onslaught of attacks by individuals and governments that wish to take, alter, and delete our digital assets. It is with this backdrop that we cover the security measures that the G-RACK 12 has to protect data from unauthorized access.

What types of security are on the G-RACK 12

Since the G-RACK 12 has multiple methods of access it also has multiple methods of security. Each security method is matched with either a specific method of access or set for over server access control.

- User & Group
- Windows Active Directory - ACLS
- NFS Permissions and Restrictions
- iSCSI Connection Settings
- FTP Password and control list
- Rsync control
- Firewall

What does security protect?

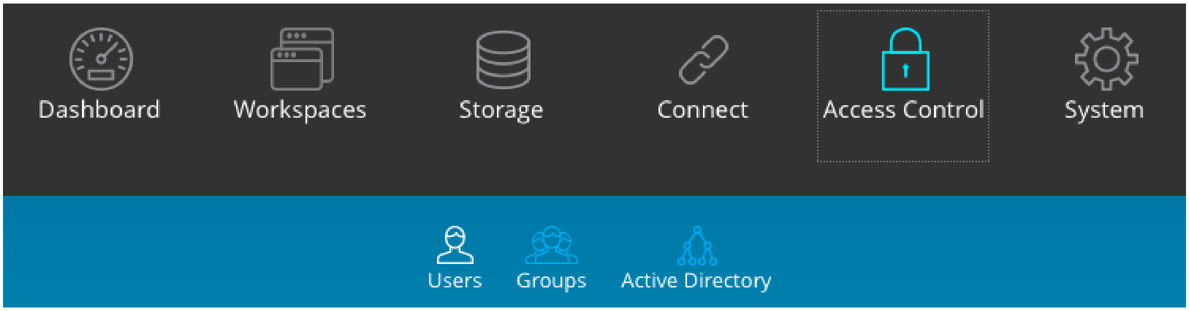
Security protects data from either being seen or from being altered. A user may have access to a file for copying or reading but not to rename or delete. It is even possible to allow a user to execute a file but not change it.

All control security breaks down into two modes, Allow and Deny. The most common model for access is deny every access and only allow access to specific users or computers. That is not to say that you can't have an Allow All setting and then only Deny specific IP addresses. For most cases, you can expect that the standard mode of security is deny all access.

G|RACK™ 12

User and Group Security

You are here



Access Control menu is used to create and manage user and groups accounts. Access rules can be created and edited in the Permissions menu under Workspaces.

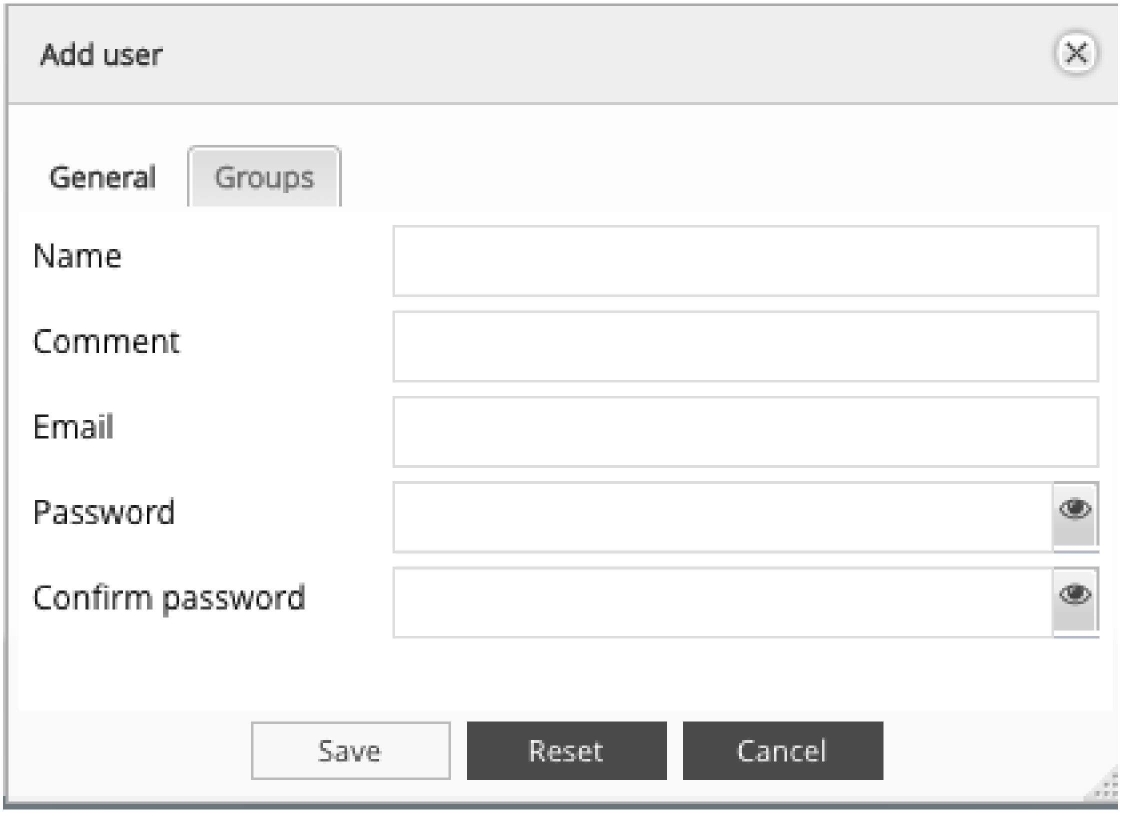
G-Technology®

User and Group Security > Users

Add/Edit user

User and Group Security > Users > Add/Edit user

Use this menu to create new users' account and to assign them to groups. To create new or to editing the existing one user account click the Add button, then fill out the required fields.



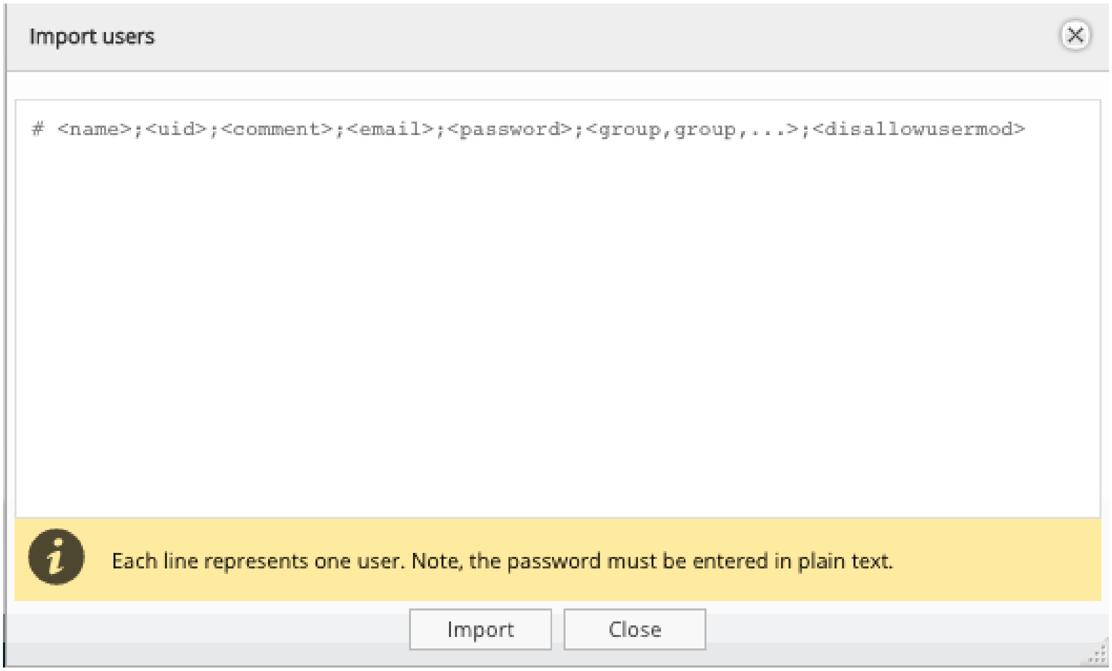
The following table describes the labels on the screen:

NOTE: The password is case-sensitive.
In text fields, you may enter from 4 to 20 characters using letters, numbers, symbols, hyphen, and underscore. Do not begin or end with a hyphen or underscore.

Import users

User and Group Security > Users > Import users

To create multiple users , use "Import" option.



Import users

```
# <name>;<uid>;<comment>;<email>;<password>;<group,group,...>;<disallowusermod>
```

Each line represents one user. Note, the password must be entered in plain text.

Mandatory fields are Name, Password and Disallowusermod. Disallowusermod can be a boolean value of true or false and stands for "do not allow user to modify account". When entering users to import do not use <>. To skip a field so not enter any text put semicolon separator, e.g. "john;;john smith;;grack12;PLM;false". A uid was not set and is not mandatory here because the G-RACK 12 will set the next user id in the line for them.

NOTE: It is not possible to set a group name that does not exist yet. In this case the standard work flow is to import groups first in the Group tab and then to import users.

NOTE: The manually assigned uid's must start off at 1000 or higher, otherwise they will not appear in the list.

Delete

User and Group Security > Users > Delete

Hightlight the desired user and press the Delete button. Confirm in the dialogue window.

Refresh

User and Group Security > Users > Refresh

The Refresh button will refresh the users list or updated information.

NOTE: Newly created users will appear automatically. Refresh button will display any new or updated information about the already existing users. It may take a few minutes to update the information.

Group

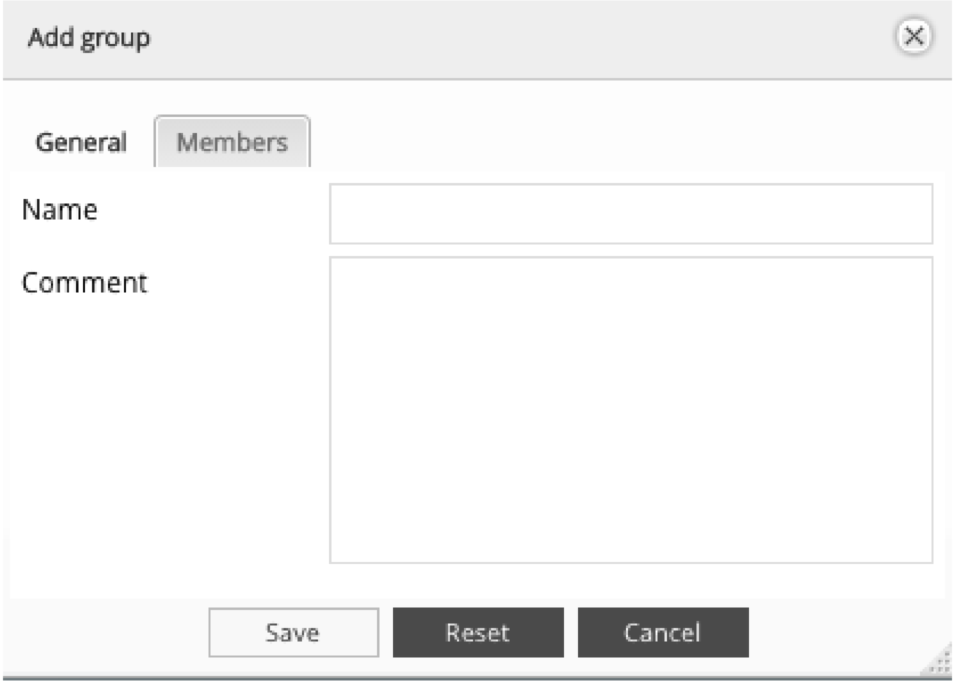
User and Group Security > Group

A user group is a collection of users with the same access right to the files or folders. Assigning users to groups gives you powerful tools to manage large numbers of users and their permissions. They allow administrators to change access rights to entire groups rather than individually. From this page, administrators can: create, modify, delete, and add users to groups.

Add/Edit group

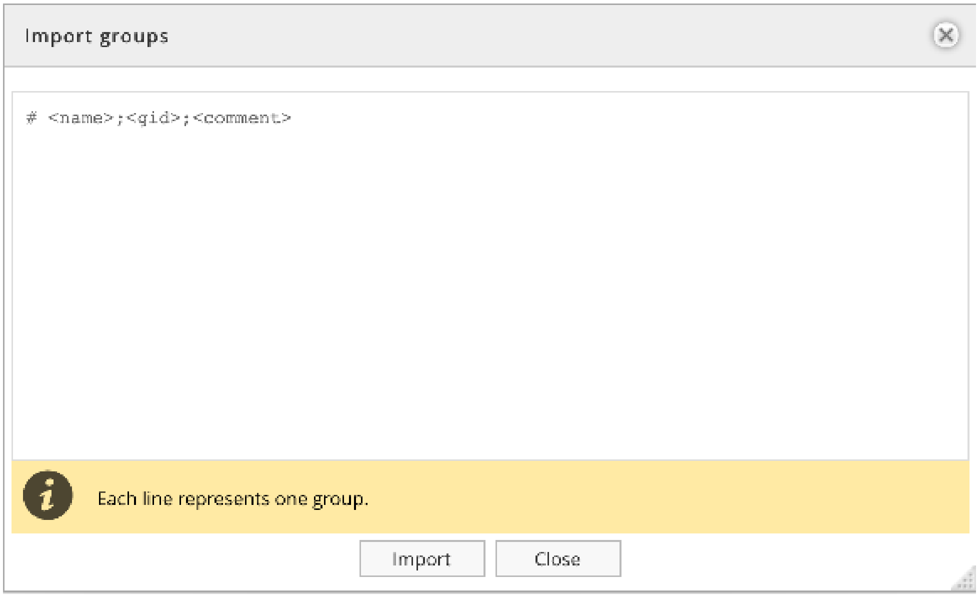
User and Group Security > Group > Add/Edit group

Use this menu to create a new group and assign users to it, then fill out the required fields.



Import groups
User and Group Security > Group > Import groups

To create multiple groups , use "Import" option.


Import groups

```
# <name>;<gid>;<comment>
```

Each line represents one group.

NOTE: The manually assigned uid's must start off at 1000 or higher, otherwise they will not appear in the list.

Delete
User and Group Security > Group > Delete

Hightlight the desired group and press the Delete button. Confirm in the dialogue window.

NOTE: Deleting a group will not affect user data.

Refresh
User and Group Security > Group > Refresh

The Refresh button will reload the screen and display any new or updated information about groups.

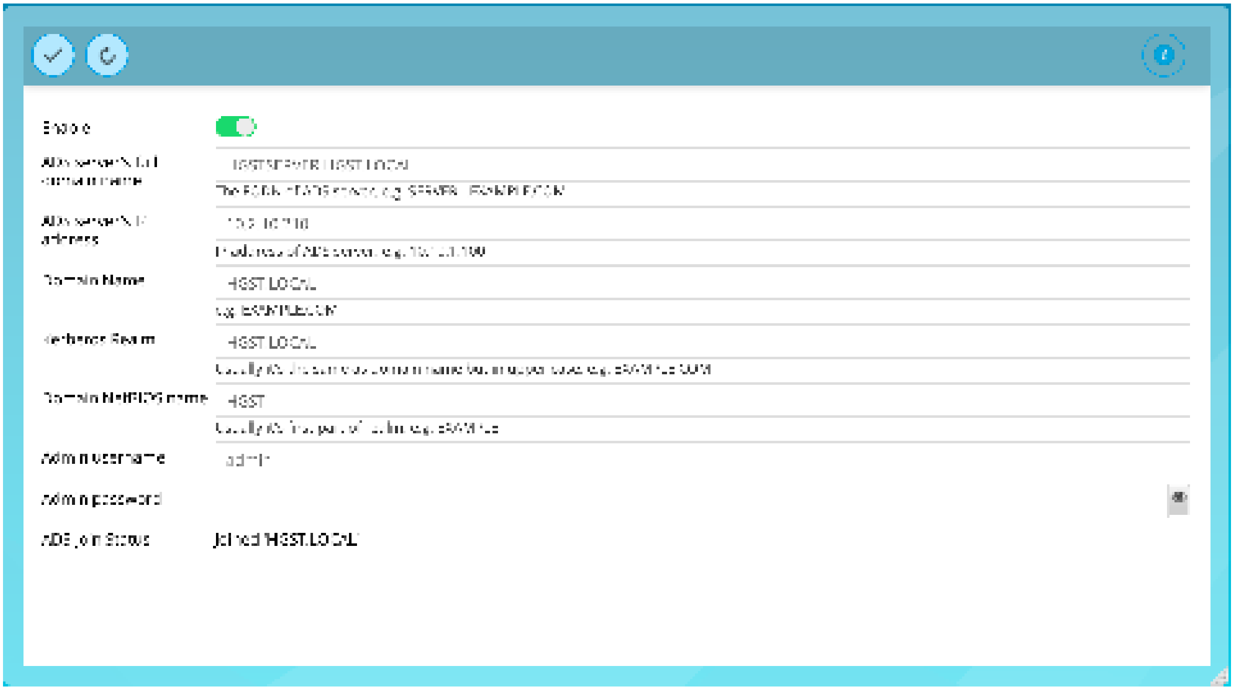
NOTE: Newly created groups will appear automatically. Refresh button will display any new or updated information about the already existing groups. It may take a few minutes to update the information.

Active Directory ACLS

Active Directory® is a Microsoft directory used in Windows environments to centrally store, share, and manage the information and resources on your network. It is a hierarchical data center which centrally holds the information of the users, user groups, and the computers for secure access management.

By joining the G-RACK 12 to the Active Directory, all the user accounts of the Active Directory server will be imported to the G-RACK 12 automatically. This will allow the administrator to configure the access rights (read only, read/write, or deny access) to the network shared workspaces.

NOTE: In order to join the domain you must have an administrator account for this domain.



Enable

ADS server's full domain name: HGSTSERVER.HGST.LOCAL
The FQDN of ADS server, e.g. SERVER1.EXAMPLE.COM

ADS server's IP address: [illegible]
IP address of ADS server, e.g. [illegible]

Domain Name: HGST.LOCAL
e.g. EXAMPLE.COM

Kerberos Realm: HGST.LOCAL
Usually it's the same as domain name but in upper case, e.g. EXAMPLE.COM

Domain NetBIOS name: HGST
Usually it's first part of realm, e.g. EXAMPLE

Admin username: admin

Admin password

ADS Join Status: Joined 'HGST.LOCAL'

The following table describes the labels on the screen:

Enable	Toggle on to enable the service
ADS server's full domain name	The FQDN of the server. e.g. server1.example.com
Domain name	e.g. example.com
Kerberos Realm	Usually it's the same as domain name but in upper case, e.g. EXAMPLE.COM
Domain NetBIOS name	Usually it's first part of realm, e.g. EXAMPLE
Admin username	Active Directory Server's admin user name
Admin password	Active Directory Server's admin password
ADS Join Status	The status will be displayed

Users local to the G-RACK 12 system that have the same name as imported ADS domain users will cause some conflicts. Users will merge as one and display as being part of both local and domain groups. This may cause issues when mounting shared workspaces or setting permissions. For best practice to avoid such conflicts:

1. Enable Active Directory and import ADS domain users
2. Create local G-RACK 12 users with unique names.

NOTE: It is important to note that additionally you can also enable a guest access for shared workspaces in the Connect menu for the protocol. This enables users to access the shared workspace through protocol services as long as correct permissions set.

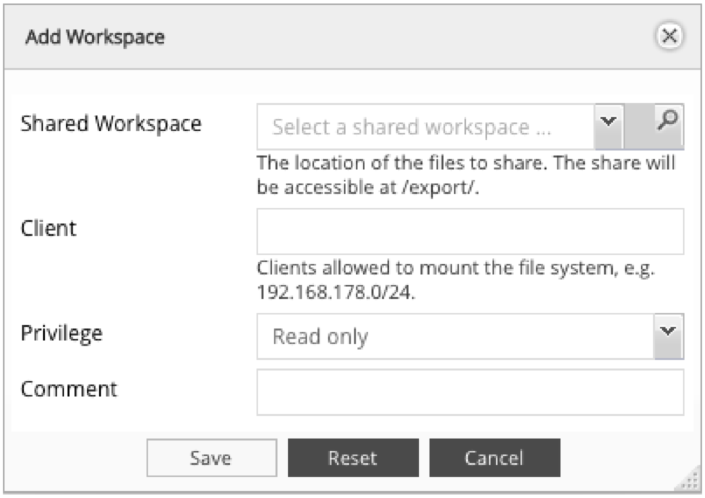
G|RACK™ 12

NFS Permissions

Share is a way a user will connect to the G-RACK 12 to transfer files. We are sharing a workspace. Need set NFS protocol to reach the workspace. i.e. to share a workspace.

G-Technology®

Share is a way a user will connect to the G-RACK 12 to transfer files. We are sharing a workspace. Need set NFS protocol to reach the workspace. i.e. to share a workspace.



Add Workspace

Shared Workspace: Select a shared workspace ...

The location of the files to share. The share will be accessible at /export/.

Client:

Clients allowed to mount the file system, e.g. 192.168.178.0/24.

Privilege: Read only

Comment:

The following table describes the labels on the screen:

Shared Workspace	The name of the workspace you wish to share. You can choose an existing workspace or create a new one. Find your Workspace by using the drop down option or you can use the search feature to locate the Workspace desired. The NFS share will be accessible at /export/ when your NFS client is pointed to the share.
Client	This defines the scope of network access to the NFS share. You can limit or expand access to the NFS share by setting these parameters. • The most limiting parameter would be to type in an exact IP address. An example of this is setting of 192.168.0.12 and by doing so you would limit the NFS share to exactly the one computer that had that IP address. • The next level of access is to provide access to all computers on a specific subnet. An example of this is a setting of 192.168.0.0/24 and by doing so you would limit the NFS share to all computers that have a matching subnet. This means all computers with IP addresses in the 192.168.0.0 to 192.168.0.254 range would be able to mount this NFS share. • Finally, the least restrictive setting available for this Client parameter is leaving it blank. If you leave it blank then any computer that can negotiate traffic to the IP address of the G-RACK 12 will have access to the NFS share. You will only want to use this in networks where outside traffic is limited by other means such as a secure firewall.

Privilege	This is a dropdown box that has two options that are fairly clear. 1) Read-only which means you will be able read and copy the files on this NFS share but you will not be able to edit them and 2) Read-Write that gives you privileges to read, edit, copy, and delete the files available on this NFS share.
Advanced options	Advanced Options - Additional information on these settings can be found online at http:// linux.die.net/man/5/exports
Comment	This is fairly self explanatory. Place text in this box that you want associated with this NFS share. It can be notes on why it was created or any other information you choose

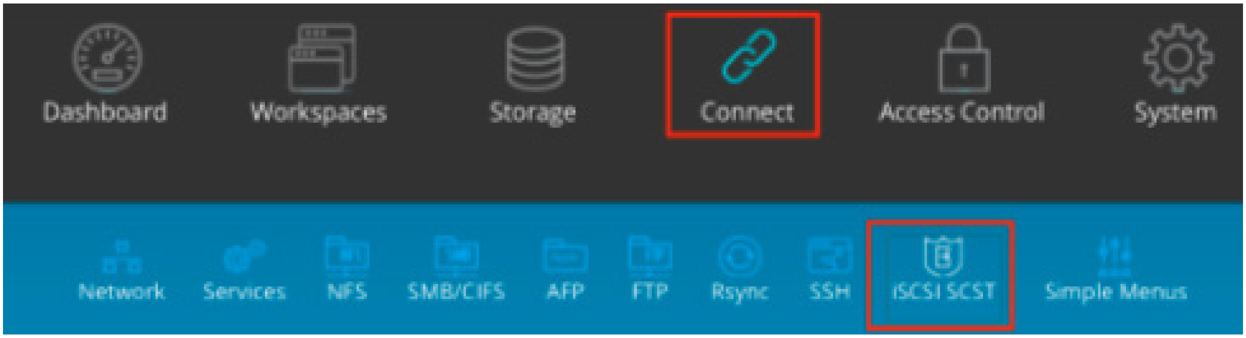
iSCSI Security

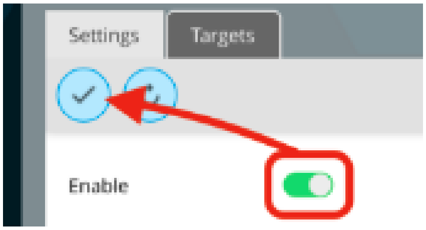
Security under iSCSI is a little different than other modes of security. The basis for iSCSI security is knowing exactly the right settings for the target you wish to attach to for storage. There is simply the settings and a username and password field.

How to create an iSCSI target and LUNs on the G-RACK 12?

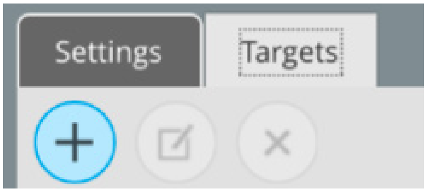
iSCSI Target Creation

Navigate to the iSCSI SCST under the Connect menu

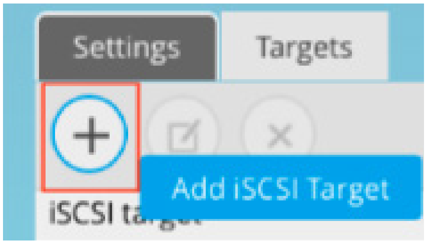




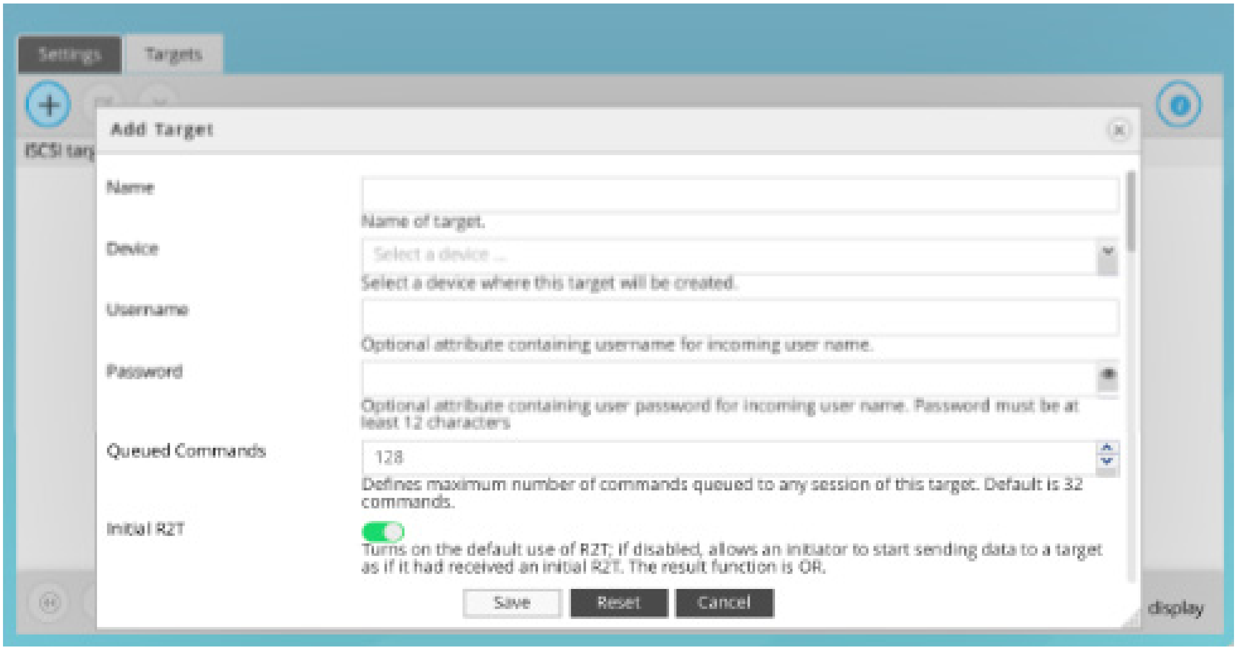
You will be brought to the iSCSI Settings page where you must first enable the iSCSI service by switching the **enable toggle to On (green) and pressing the Save button**. The iSCSI service might already be toggled On if you created iSCSI targets in the Wizard setup process.



Press the Targets tab in the iSCSI SCST menu to continue to the iSCSI target/LUN creation.



In the iSCSI SCST Targets tab you may notice previously created Wizard-generated target. This page allows you to view the current iSCSI targets and, if highlighted, edit your LUNs associated with that target or delete the Target altogether. To create a new Target, **press the Add iSCSI target button**.



Add Target

Name
Name of target.

Device
Select a device ...
Select a device where this target will be created.

Username
Optional attribute containing username for incoming user name.

Password
Optional attribute containing user password for incoming user name. Password must be at least 12 characters

Queued Commands
128
Defines maximum number of commands queued to any session of this target. Default is 32 commands.

Initial R2T
Turns on the default use of R2T; If disabled, allows an initiator to start sending data to a target as if it had received an initial R2T. The result function is OR.

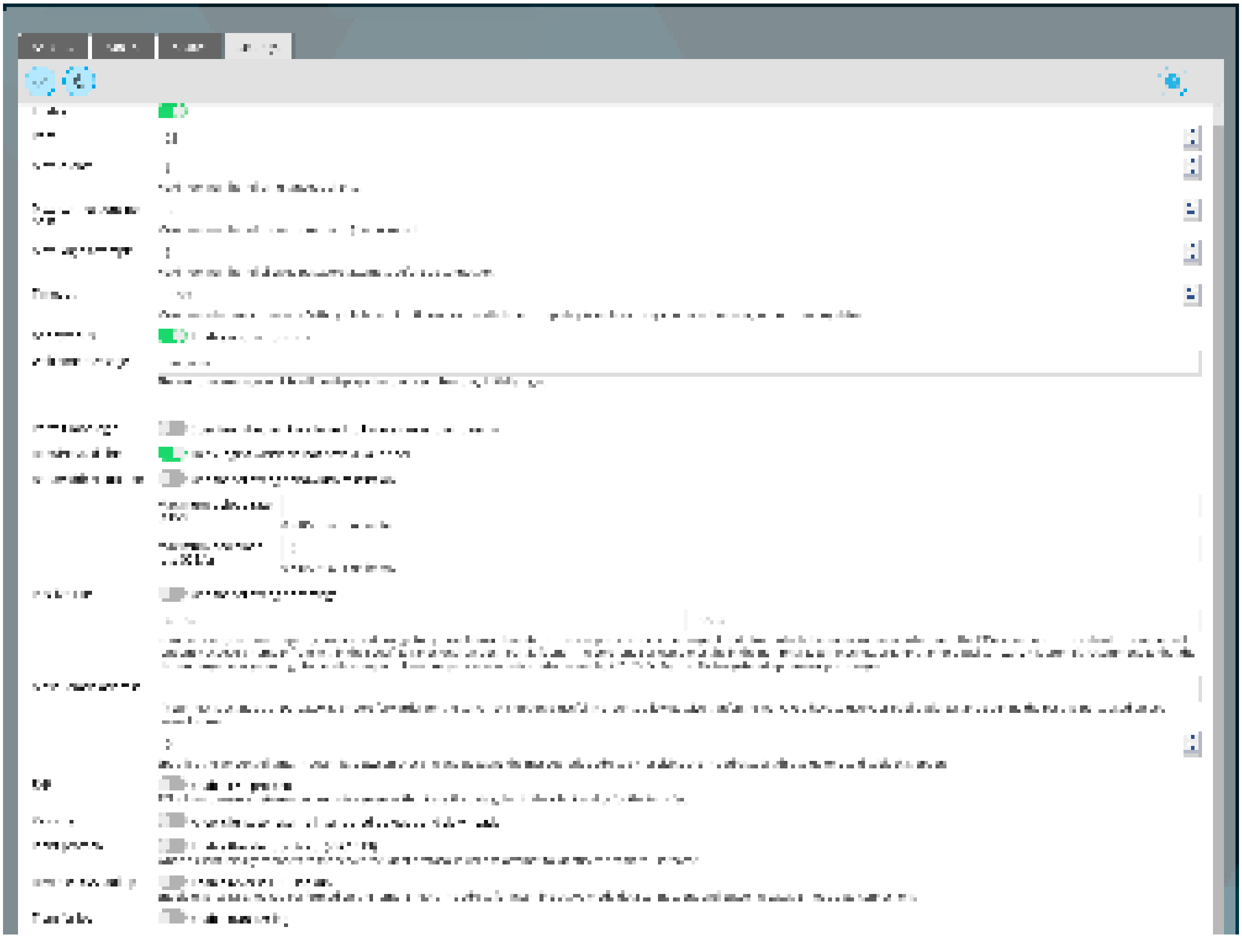
G-RACK's iSCSI Add Target page allows you to give your Target a name, associate it with a RAIDWorkspace, access credentials like username / password assignments (known by iSCSI initiators as username & secret) as well as a multitude of performance and initiator parameters. G-RACK 12's default advanced parameter configuration has already been maximized for performance but if your network or administrator choose to personalize the advanced parameters for iSCSI targets you will find those attributes here. To expedite this lesson however all you need to proceed is a Target Name and a File device.

Press the Save button to create the target, press the Reset button to return to the default settings or press the Cancel button to exit the iSCSI Add Target page.

FTP Security

In order to use FTP on the G-RACK 12 a user must be already created on the system and use their ID and Password to access an available share. In addition to standard users the administrator can also allow for anonymous FTP where the user does not need to be a regular user on the system.

Use this menu to enable the FTP service



The following table describes the labels on the screen:

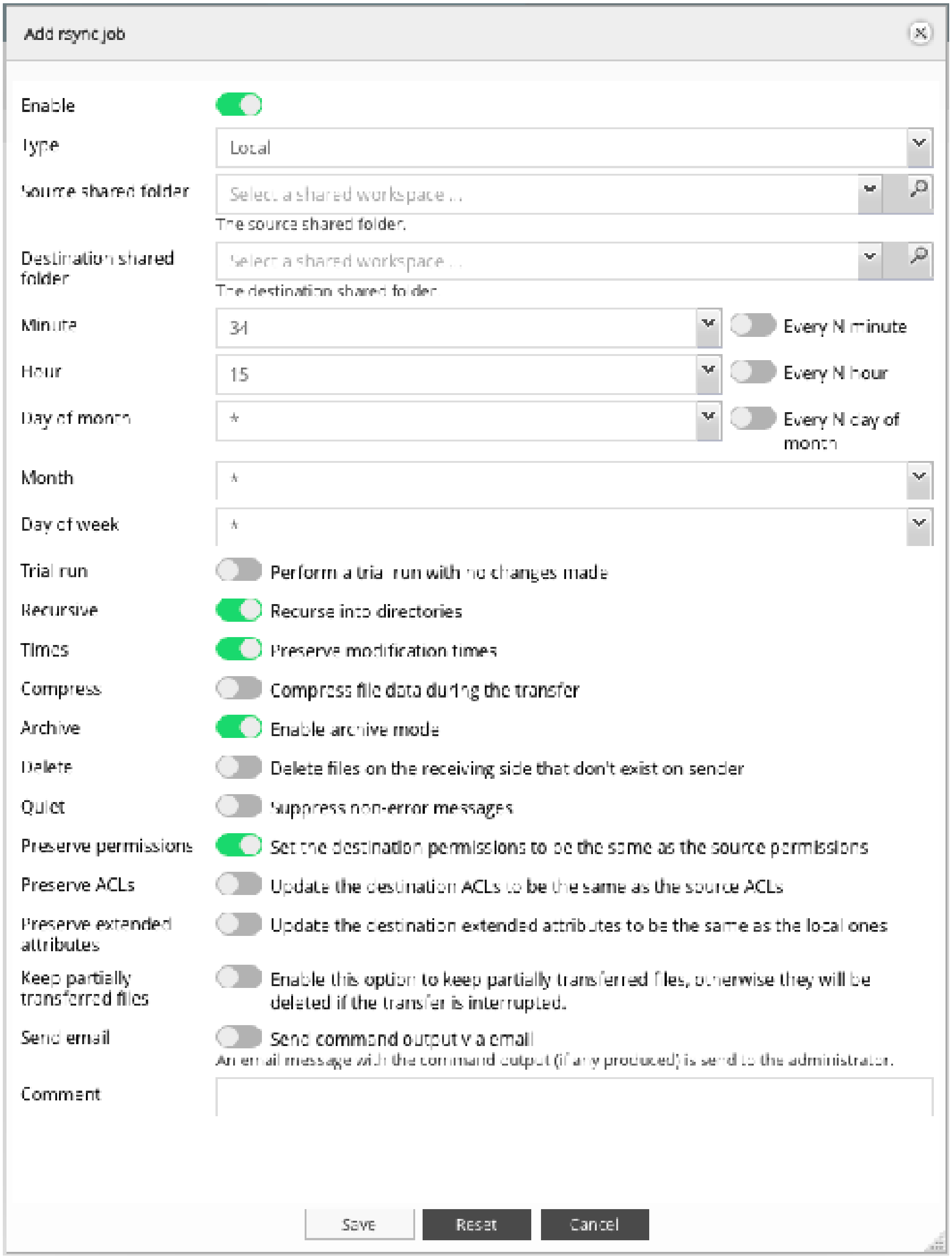
Enable	Toggle on to enable the service
Port	Specify the port to be used
Max. clients	Set the maximum number of simultaneous clients that can connect to the FTP server
Max.connections per host	Maximum number of connections per IP (0 = unlimited).
Max. login attempts	Maximum number of allowed password attempts before disconnection.

Timeout	Maximum idle time in seconds. Setting idle timeout to 0 disables the idle timer completely (clients can stay connected for ever, without sending data).
Anonymous FTP	Enable anonymous FTP
Welcome Message	The welcome message which will be displayed to the user when they initially login.
Permit root login	Specifies whether it is allowed to login as superuser directly
Require Valid Shell	Deny logins which do not have a valid shell
Bandwidth restriction	Use the following bandwidth restriction: 0 KiB/s means unlimited.
Passive FTP	Use the following port range: In some cases you have to specify passive ports range to by-pass firewall limitations. Passive ports restricts the range of ports from which the server will select when sent the PASV command from a client. The server will randomly choose a number from within the specified range until an open port is found. The port range selected must be in the non-privileged range (eg. greater than or equal to 1024). It is strongly recommended that the chosen range be large enough to handle many simultaneous passive connections (for example, 49152-65534, the IANA-registered ephemeral port range).
Masquerade address	If your host is acting as a NAT gateway or port forwarder for the server, this option is useful in order to allow passive transfers to work. You have to use your public address and opening the passive ports used on your firewall as well. Specifies the amount of time, in seconds, between checking and updating the masquerade address by resolving the IP address. Set this value to 0 to disable this option.
FXP	Enable FXP protocol FXP allows transfers between two remote FTP servers without any file data going to the client asking for the transfer. **Note:** In order to use FXP (File Exchange Protocol) for server-to-server data transfer, make sure to change the port from 21 to some other port. Also, make sure to open the corresponding port on your router and forward that port from your router to the device.
Resume	Allow clients to resume interrupted uploads and downloads
Ident protocol	Enable the ident protocol (RFC1413) When a client initially connects to the server the ident protocol is used to attempt to identify the remote username.
Reverse DNS lookup	Enable reverse DNS lookup performed on the remote host's IP address for incoming active mode data connections and outgoing passive mode data connections.
Transfer log	Enable transfer log

Rsync Security

Rsync has two aspects of security. The first aspect is the ability to transfer over the ACLs information between the sending and receiving servers. This is useful to the the users so that they can have the same access privileges on both servers. The second security aspect has to with with which Rsync servers can talk to each other but utilizing either or both IP addresses (Host Allow/Deny) and/or username and passwords for Authenticate users.

To add a new rsync task press the Add button. These parameters define the overall behavior of Rsync.



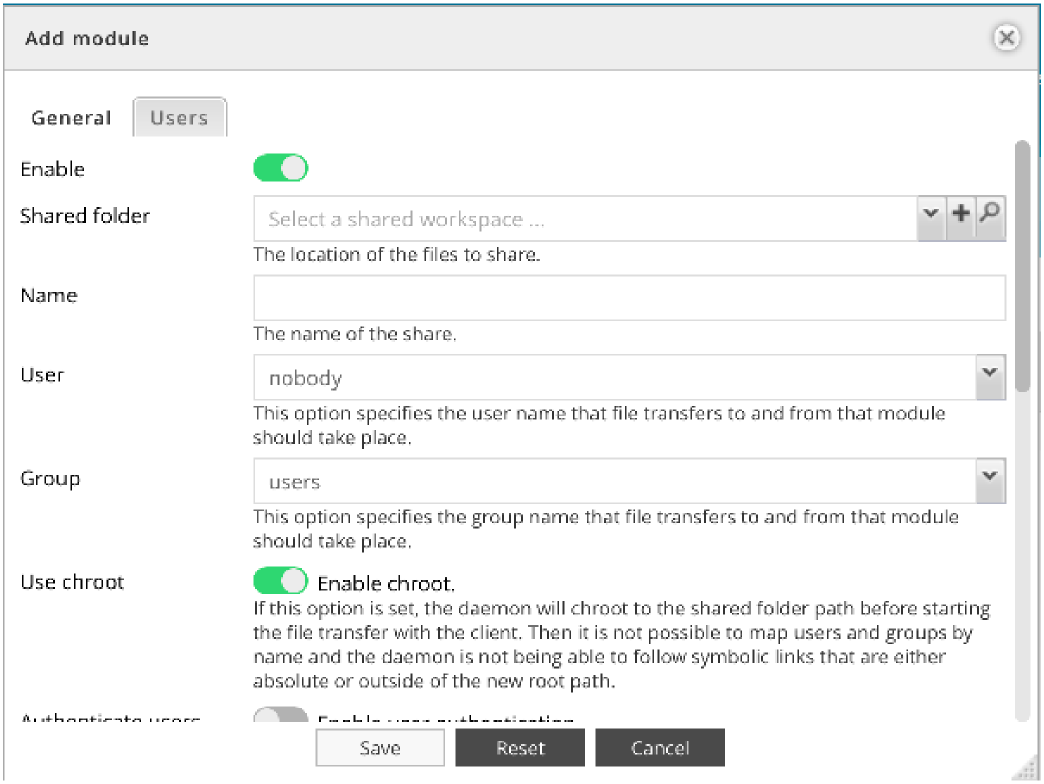
Add rsync job

Enable	●
Type	Local
Source shared folder	Select a shared workspace ... The source shared folder.
Destination shared folder	Select a shared workspace ... The destination shared folder.
Minute	34 ○ Every N minute
Hour	15 ○ Every N hour
Day of month	* ○ Every N day of month
Month	*
Day of week	*
Trial run	○ Perform a trial run with no changes made
Recursive	● Recurse into directories
Times	● Preserve modification times
Compress	○ Compress file data during the transfer
Archive	● Enable archive mode
Delete	○ Delete files on the receiving side that don't exist on sender
Quiet	○ Suppress non-error messages
Preserve permissions	● Set the destination permissions to be the same as the source permissions
Preserve ACLs	○ Update the destination ACLs to be the same as the source ACLs
Preserve extended attributes	○ Update the destination extended attributes to be the same as the local ones
Keep partially transferred files	○ Enable this option to keep partially transferred files, otherwise they will be deleted if the transfer is interrupted.
Send email	○ Send command output via email An email message with the command output (if any produced) is send to the administrator.
Comment	

The following table describes the labels on the screen:

Enable	Toggle the button to enable RSync
Type	Choose the type: Local - synchronizes two local directories Remote - synchronizes a local directory to a remote one. Obtain SSH access to perform this. The remote system is to have synchronizing enabled
Mode	This option will be available if "remote" type has been chosen. Is specifies the synchronizing direction. Push - pushes the directory from the local system to a remote system Pull - is used to sync a remote directory to the local system.
Source shared folder	The source shared folder to be synchronized
Destination shared folder	The destination shared folder.
Trial run	Perform a trial run with no changes made
Recursive	Recurse into directories
Times	Preserve modification times
Compress	Compress file data during the transfer
Archive	Enable archive mode
Delete	Delete files on the receiving side that don't exist on sender
Quiet	Suppress non-error messages
Preserve permissions	Set the destination permissions to be the same as the source permissions
Preserve ACLs	Update the destination ACLs to be the same as the source ACLs
Preserve extended attributes	Update the destination extended attributes to be the same as the local ones
Keep partially transferred files	Enable this option to keep partially transferred files, otherwise they will be deleted if the transfer is interrupted.
Send email	Send command output via email. An email message with the command output (if any produced) is send to the administrator.
Comment	Optional comment text box

Use this menu to set a folder to be shared.



Enable

Shared folder Select a shared workspace ...
The location of the files to share.

Name
The name of the share.

User nobody
This option specifies the user name that file transfers to and from that module should take place.

Group users
This option specifies the group name that file transfers to and from that module should take place.

Use chroot Enable chroot.
If this option is set, the daemon will chroot to the shared folder path before starting the file transfer with the client. Then it is not possible to map users and groups by name and the daemon is not being able to follow symbolic links that are either absolute or outside of the new root path.

Authenticate users Enable user authentication

The following table describes the labels on the screen:

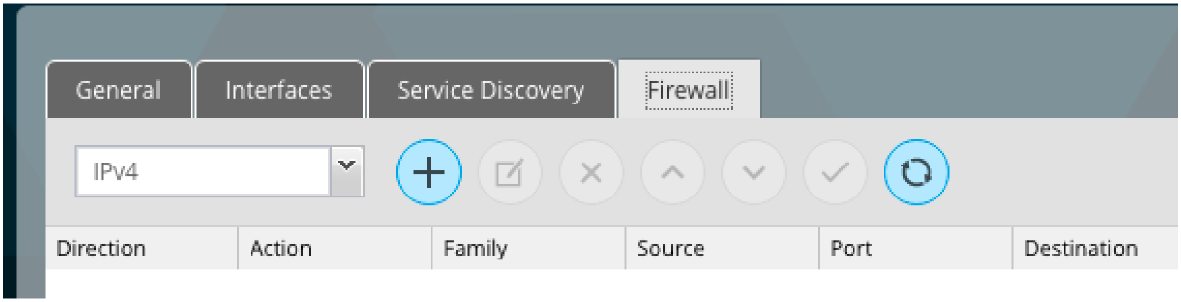
Enable	Toggle the button to enable
Shared folder	The location of the files to share.
Name	The name of the share
User	This option specifies the user name that file transfers to and from that module should take place.
Group	This option specifies the group name that file transfers to and from that module should take place.

Use chroot	Enable chroot. If this option is set, the daemon will chroot to the shared folder path before starting the file transfer with the client. Then it is not possible to map users and groups by name and the daemon is not being able to follow symbolic links that are either absolute or outside of the new root path.
Authenticate users	Enable user authentication. If set then the client will be challenged to supply a username and password to connect to the module.
Read only	Set read only If this option is set, then any attempted uploads will fail.
Write only	Set write only. If this option is set, then any attempted downloads will fail.
List	Enable module listing This option determines if this module should be listed when the client asks for a listing of available modules.
Max.connections	This option specifies the maximum number of simultaneous connections. 0 means no limit.
Hosts allow	This option is a comma, space, or tab delimited set of hosts which are permitted to access this module. You can specify the hosts by name or IP number. Leave this field empty to use default settings.
Hosts deny	This option is a comma, space, or tab delimited set of host which are NOT permitted to access this module. Where the lists conflict, the allow list takes precedence. In the event that it is necessary to deny all by default, use the keyword ALL (or the netmask 0.0.0.0/0) and then explicitly specify to the hosts allow parameter those hosts that should be permitted access. Leave this field empty to use default settings.
Comment	Add an optional text here

Firewall Security

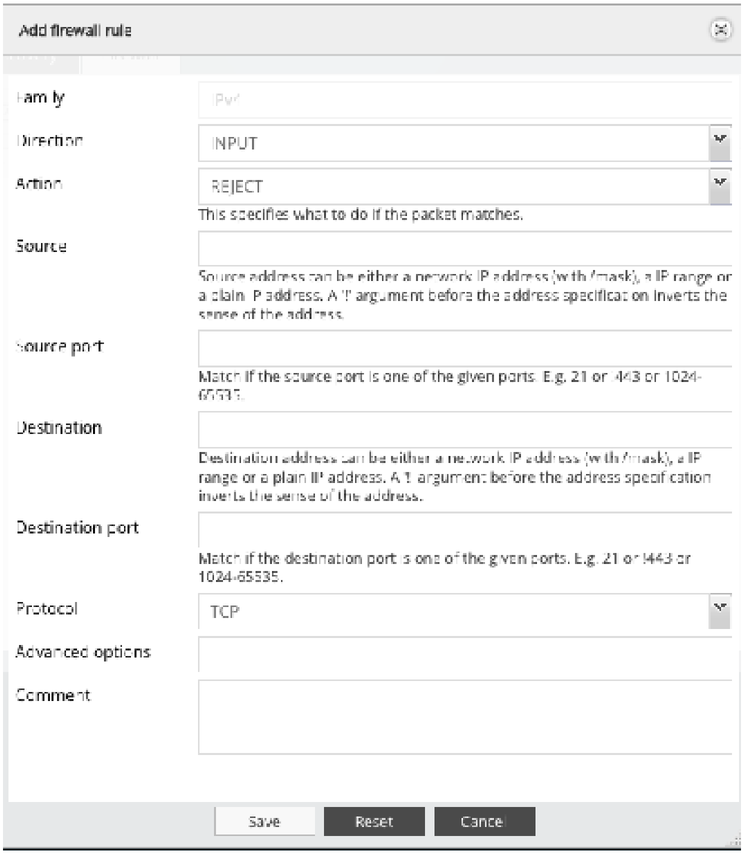
If you want to make sure that only certain networks or computers can access the G-RACK 12 then you will want enable the Firewall Settings. These settings allow you to control what computers and networks can access the server and also which ports are allowed to pass to the server. Firewall rules will inhibit all other traffic than that allowed by the rules. This can be very helpful if you are using the G-RACK 12 in a single department or in a network where it can be exposed to the Internet in general.

Firewall Filters the network traffic based on specific ruled, added by the administrator .



Direction	Action	Family	Source	Port	Destination

By adding custom rules , it is possible to allow or block access based on the service or application, source or destination IP addresses, time of the day. its also possible to choose to log traffic that matches or does not match the defined rule.



Add firewall rule

Family: IPv4

Direction: INPUT

Action: REJECT

This specifies what to do if the packet matches.

Source:

Source address can be either a network IP address (with /mask), a IP range or a plain IP address. A '!' argument before the address specification inverts the sense of the address.

Source port:

Match if the source port is one of the given ports. E.g. 21 or 443 or 1024-65535.

Destination:

Destination address can be either a network IP address (with /mask), a IP range or a plain IP address. A '!' argument before the address specification inverts the sense of the address.

Destination port:

Match if the destination port is one of the given ports. E.g. 21 or 443 or 1024-65535.

Protocol: TCP

Advanced options:

Comment:

The following table describes the labels on the screen:

Family	For IPv4
Direction	Choose the direction of the traffic to filter
Action	This specifies what to do if the packet matches
Source	Source address can be either a network IP address (with/mask), an IP range or a plain IP address. A"!" argument before the address specification inverts the sense of the address
Source port	Match if the source port is one of the given ports. E.g. 21 or !443 or 1024-65535
Destination	Destination address can be either a network IP address (with/mask), an IP range or a plain IP address. A"!" argument before the address specification inverts the sense of the address
Destination port	Match if the destination port is one of the given ports, E.g. 21 or !443 or 1024-65535
Protocol	Choose the protocol from drop down menu
Advanced options	Text field for adding additional commands
Comment	Add an optional text

About G-RACK12

The G-RACK 12 Network-Attached Storage (NAS) delivers the ultimate in high-performance, centralized storage for small-to-medium size post-production houses, ad agencies, TV/broadcast studios and in-house creative departments that use Avid Media Composer, Final Cut Pro X, or Adobe Premiere.

The G-RACK 12 brings G-Technology's industry-leading reliability, scalability and studio-friendly technology to shared storage. Streamline demanding media and entertainment workflows of 4K and above with:

- A flexible 12-Bay server in 48TB to 120TB capacities;
- An optional 48TB to 120TB Expansion Module;
- Seamless integration with your data network and non-linear editing (NLE) suites; and
- The latest Btrfs file system for better data protection and faster content recovery.

Key Features:

- Enterprise-grade Network-Attached Storage (NAS)
- Seamless integration with top non-linear editing suites
- Internet Small Computer System Interface (iSCSI) support for simple shared storage management over data networks
- G-Technology NAS operating system with easy-to-use workstation interface and setup Wizard
- Advanced B-tree file system (Btrfs) for superior data protection
- Scalable 12-bay server with 48, 72, 96, 120TB capacities
- Expandable to 240TB capacity with optional 120TB Expansion Module
- Up to (TBD) MB/s transfer rates
- Ultra-reliable premium quality G-Technology hard disk drives
- Outstanding 5-Year limited warranty

Safety Notice

Please read and observe the following precautions to assure personal safety. Improper use can result in hazardous situations.

1. The G-RACK 12 operates normally in the temperature range of 0ºC–50ºC and relative humidity of 8%–90%. Please make sure the environment is well ventilated.
2. The power cord and devices connected to the G-RACK 12 must provide correct supply voltage (100W, 90–264V). If unsure, please contact the distributor or the local power supply company.
3. Do NOT place the G-RACK 12 in direct sunlight or near chemicals.
4. Unplug the power cord and all the connected cables before cleaning. Wipe the G-RACK 12 with a dry towel. Do NOT use chemical or aerosol to clean the G-RACK 12.
5. Do NOT place any objects on the G-RACK 12 during normal system operations to avoid overheat.
6. Use the flat head screws in the product package to lock the hard disk drives in the G-RACK 12 when installing the hard drives for proper operation.
7. Do NOT place the G-RACK 12 on any uneven surface to avoid falling off and damage.
8. Do NOT expose the G-RACK 12 to dampness, dust, corrosive or any liquids.
9. Do NOT attempt to repair the G-RACK 12 in any occasions. Improper dissemblance of the product may expose you to electric shock or other risks. For any inquiries, please contact the distributor.
10. Do NOT use the G-RACK 12 near water, for example, in a wet basement or near a swimming pool.
11. Do NOT place any object on the power cord. Do NOT locate the G-RACK 12 where it can be stepped on or tripped over.
12. Do NOT install, use, or service the G-RACK 12 during a thunder storm. There is a remote risk of electric shock from lightning.
13. If an extension cord is used with the G-RACK12, make sure that the total ampere rating of the equipment plugged into the extension cord does not exceed the extension cord ampere rating. Also, make sure that the total rating of all products plugged into the wall outlet does not exceed the fuse rating.
14. Do NOT drop the G-RACK 12.
15. Do NOT use the G-RACK 12 outside, and make sure all the connections are indoors.
16. Never push objects of any kind into the G-RACK 12 through the chassis slots as they may touch dangerous voltage points or short out parts that could result in a fire or electric shock.
17. ONLY qualified service personnel should service or disassemble the G-RACK 12.
18. If the power adapter or cord is damaged, remove it from the power outlet. Do NOT attempt to repair the power adapter or cord. Contact your local vendor to order a new one.