

The **Create a SnapSync Performance Test** window opens.

3. Specify the destination IP address.

**Tip**

Click **Detect** to view the IP addresses of all QNAP NAS devices on the local network.

4. Specify the system port.

**Note**

The default port is 8080.

5. Optional: Select **Enable secure connections (HTTPS)**.
6. Specify the username and password of an administrator account of the destination NAS.
7. Click **Connect**.
8. Select the source storage pool.
9. Select the destination storage pool.
10. Select the IP address of the source network adapter.
11. Select the IP address of the destination network adapter.
12. Click **Run Test**.
A confirmation message window appears.
13. Click **Yes**.
QuTS hero runs the SnapSync performance test and displays the test results on the **Summary** screen.

8. iSCSI & Fibre Channel

iSCSI & Fibre Channel is a QuTS hero utility that enables you to configure iSCSI and Fibre Channel storage settings on your NAS.

Storage Limits

iSCSI Storage Limits


iSCSI Storage Limit	Maximum
iSCSI LUNs and targets per NAS	255 (combined)
Connections per iSCSI session	8
iSCSI sessions per target	The maximum number of sessions is determined by available NAS CPU resources, memory, and network bandwidth.
iSCSI sessions per NAS	The maximum number of sessions is determined by available NAS CPU resources, memory, and network bandwidth.

Fibre Channel Storage Limits

Fibre Channel Storage Limit	Maximum
Fibre Channel ports + port groups	256 (combined)
WWPN aliases	256
LUN masking rules	256
Port binding rules	256
LUNs mapped to 1 Fibre Channel port	256

iSCSI & Fibre Channel Global Settings

You can access global settings by clicking  in the **iSCSI & Fibre Channel** window.

Setting	Description
Enable iSCSI and Fibre Channel services	Enable these services to use iSCSI and Fibre Channel on your NAS.
iSCSI service port	View and modify the port that iSCSI initiators connect to.  Tip The default port is 3260.
Enable iSNS	SNS enables the automatic discovery and management of iSCSI initiators and targets within a TCP/IP network. iSNS server IP: Specify the IP address of the iSNS server.

LUNs


QNAP NAS devices allow other devices to access their storage space in the form of LUNs over iSCSI and Fibre Channel networks. The LUNs must first be created on the NAS, and then mapped to iSCSI targets or Fibre Channel port groups for access over the network.




Creating a Block-Based LUN

1. Go to one of the following screens.
 - **iSCSI & Fibre Channel > iSCSI Storage**
 - **iSCSI & Fibre Channel > Fibre Channel > FC Storage**
2. Click **Create**, and then select **New Block-Based LUN**.
The **Create LUN** window opens.
3. Specify a LUN name
 - Length: 1 to 32 characters
 - Valid characters: 0-9, a-z, A-Z, underscore (_)
4. Select the storage pool that this LUN will be created in.
5. Select a provisioning type.

Provisioning Type	Description
Thick provisioning	QuTS hero allocates storage pool space when creating the LUN. This space is guaranteed to be available later.
Thin provisioning	QuTS hero allocates storage pool space only when needed, such as when data is being written to the LUN. This ensures efficient use of space but there is no guarantee that space will be available.

6. Specify a LUN capacity.
Specify the maximum capacity of the LUN. The maximum capacity depends on the LUN allocation method:
 - Thick provisioning: Equal to the amount of free space in the parent storage pool.
 - Thin provisioning: 1 PB
7. Optional: Configure LUN guaranteed snapshot space.
LUN guaranteed snapshot space is storage pool space that is reserved for storing snapshots of a LUN. Enabling this feature ensures that QuTS hero always has sufficient space to store new snapshots for this LUN.
8. Optional: Configure the following LUN settings.

Setting	Description
Compression	<p>QuTS hero compresses the data in the LUN to reduce the size of stored data. Enabling compression also reduces the total number of blocks that QuTS hero needs to read and write, increasing read and write speeds.</p> <div style="display: flex; align-items: flex-start;">  <div> <p>Tip New shared folders and LUNs have compression enabled by default. Compression does not impact read/write and processor performance on ZFS filesystems. Only disable this setting when necessary.</p> </div> </div>

Setting	Description
Deduplication	<p>QuTS hero eliminates duplicate copies of data to reduce the required amount of storage space.</p> <p> Important To enable deduplication, your NAS must have at least 8 GB of memory.</p>
Alert threshold	<p>QuTS hero issues a warning notification when the percentage of used LUN space is equal to or above the specified threshold.</p>
SSD Cache	<p>The SSD cache will be used to improve LUN access performance.</p> <p> Important This setting is only available when the SSD cache is enabled.</p>
Fast clone	<p>Fast Clone enables QuTS hero to create copies of files faster. It also saves storage space by modifying file metadata, allowing original and copied files to share the same data blocks.</p> <p> Important</p> <ul style="list-style-type: none"> • Fast Clone only works when the copied file is created in the LUN containing the original file. • Fast Clone does not improve the speed of snapshot restoration operations such as restoring files from a snapshot, snapshot revert, and snapshot clone.
Synchronous I/O	<p>Select the ZFS Intent Log (ZIL) sync setting to improve either data consistency or performance. There are three options:</p> <ul style="list-style-type: none"> • Auto (Default): QuTS hero uses synchronous I/O or asynchronous I/O based on the application and the type of I/O request. • Always: (Default). All I/O transactions are treated as synchronous and are always written and flushed to a non-volatile storage (such as a SSD or HDD). This option gives the best data consistency, but might have a slight impact on performance. • None: All I/O transactions are treated as asynchronous. This option gives the highest performance, but has a higher risk of data loss in the event of a power outage. Ensure that a UPS (uninterrupted power supply) is installed when using this option.
Performance profile (block size)	<p>Specify the block size of the LUN.</p>

9. Optional: Select **Map LUN to an iSCSI target or FC port group**

If selected, the **Edit LUN Mapping** wizard appears after QuTS hero has finished creating the LUN.

10. Click **Create**

11. Optional: Map the LUN to an iSCSI target or Fibre Channel port group.

For details, see the following topics:

- [Mapping a LUN to an iSCSI Target](#)
- [Mapping a LUN to a Fibre Channel Port Group](#)

LUN Import/Export

With LUN Import/Export, you can back up a LUN as an image file to an SMB or NFS file server, local NAS folder, or external storage device. You can then import the LUN image file and restore the LUN on any QNAP NAS.

Creating a LUN Export Job

1. Go to **iSCSI & Fibre Channel > LUN Import/Export**.
2. Click **Create a Job**.
The **Create LUN Export Job** windows opens.
3. Select **Export a LUN**.
4. Select a LUN.
5. Optional: Specify a job name.
The name must consist of 1 to 55 characters from any of the following groups:
 - Letters: A to Z, a to z
 - Numbers: 0 to 9
 - Special characters: Underscore (_)
6. Click **Next**.
7. Select the destination folder.

Option	Description	Required Information
Linux Share (NFS)	NFS share on an external server	<ul style="list-style-type: none"> • IP address or host name • NFS folder or path
Windows Share (CIFS/SMB)	CIFS/SMB share on an external server	<ul style="list-style-type: none"> • IP address or host name • Username • Password • CIFS/SMB folder or path
Local Host	Local NAS shared folder or connected external storage device	<ul style="list-style-type: none"> • NAS shared folder or external device • Sub-folder

8. Click **Next**.
9. Optional: Specify a LUN image name.
 - The name must consist of 1 to 64 characters from any of the following groups:
 - Letters: A to Z, a to z
 - Numbers: 0 to 9
 - Special characters: Underscore (_), hyphen (-), space ()
 - The name cannot begin or end with a space.

10. Optional: Select **Use Compression** to compress the image file.
When enabled, the image file will be smaller but exporting will take longer and will use more processor resources.
11. Select when the job will run.

Option	Description
Now	Run the job immediately after the job has been created. After this first run, the job will only run when manually started.
<ul style="list-style-type: none"> • Hourly • Daily • Weekly • Monthly 	Run the job periodically according to the specified schedule.

12. Click **Next**.
13. Click **Apply**.

QuTS hero creates the job. The job then starts running if **Now** was selected as the scheduling option.


Importing a LUN from an Image File

1. Go to **iSCSI & Fibre Channel > LUN Import/Export** .
2. Click **Create a Job**.
The **Create LUN Export Job** windows opens.
3. Select **Import a LUN**.
4. Optional: Specify a job name.
The name must consist of 1 to 55 characters from any of the following groups:
 - Letters: A to Z, a to z
 - Numbers: 0 to 9
 - Special characters: Underscore (_)
5. Click **Next**.
6. Select the source folder.

Option	Description	Required Information
Linux Share (NFS)	NFS share on an external server	<ul style="list-style-type: none"> • IP address or host name • NFS folder or path
Windows Share (CIFS/SMB)	CIFS/SMB share on an external server	<ul style="list-style-type: none"> • IP address or host name • Username • Password • CIFS/SMB folder or path

Option	Description	Required Information
Local Host	Local NAS shared folder or connected external storage device	NAS shared folder or external device

7. Click **Next**.
8. Select the LUN image file.
9. Click **Next**.
10. Specify the import destination.

Option	Description	Required Information
Overwrite existing LUN	Import the image file data to an existing LUN.  Warning All existing data on the LUN will be overwritten.	An existing LUN.
Create a new LUN	Import the image file as a new LUN.	<ul style="list-style-type: none"> • LUN name • LUN location. This will be a storage pool.

11. Click **Next**.
12. Click **Apply**.

QuTS hero creates the job, and then immediately runs it.

LUN Import/Export Job Actions

You can perform various actions on LUN import/export jobs by going to **iSCSI & Fibre Channel > LUN Import/Export** . Select a LUN import/export job and then click **Action** to select the desired action.

Action	Description
Edit	Edit the job.
Delete	Delete the job.
Start	Start the job.
Stop	Stop a running job.
View Logs	View the job's status, properties, details of its last run, and event logs.

LUN Import/Export Job Status

You can view LUN import/export job statuses by going to **iSCSI & Fibre Channel > LUN Import/Export** .

Status	Description
--	The job has not run yet.
Initializing	The job is preparing to run.
Processing	The job is running. The job's progress is displayed a percentage next to the status.
Finished	The job has finished running or was canceled by a user.

Status	Description
Failed	The job failed. View the job's event log for details.

iSCSI

iSCSI enables computers, servers, other NAS devices, and virtual machines to access NAS storage in the form of LUNs over a TCP/IP network. Hosts can partition, format, and use the LUNs as if they were local disks.

Getting Started with iSCSI

1. Create an iSCSI target on the NAS.
For details, see [Creating an iSCSI Target](#).
2. Create a LUN on the NAS.
A LUN is a portion of storage space. LUNs are created from storage pool space.
For more information, see [Creating a Block-Based LUN](#)
3. Map the LUN to the iSCSI target.
Multiple LUNs can be mapped to one target.
For details, see [Mapping a LUN to an iSCSI Target](#).
4. Install an iSCSI initiator application or driver on the host.
The host is the service, computer, or NAS device that will access the LUN.
5. Connect the iSCSI initiator to the iSCSI target on the NAS.



Warning

To prevent data corruption, multiple iSCSI initiators should not connect to the same LUN simultaneously.

The LUNs mapped to the iSCSI target appear as disks on the host.

6. In the host OS, format the disks.

iSCSI Performance Optimization

You can optimize the performance of iSCSI by following one or more of these guidelines:

- Use thick provisioning (instant allocation). Thick provisioning gives slightly better read and write performance than thin provisioning.
- Create multiple LUNs, one for each processor thread on the NAS. For example, if the NAS has four processor threads, then you should create four or more LUNs.



Tip

Go to **Control Panel > System > System Status > System Information > CPU** to view the number of processor threads.

- Use separate LUNs for different applications. For example, when creating two virtual machines which intensively read and write data, you should create one LUN for each VM to distribute the load.
- You can use iSER (iSCSI Extensions for RDMA) for faster data transfers between QNAP NAS devices and VMware ESXi servers. Enabling iSER requires a compatible network card and switch. For a list of compatible network devices, see <https://www.qnap.com/solution/iser>.

iSCSI Targets

iSCSI targets allow iSCSI initiators from other devices on the network to access mapped LUNs on the NAS. You can create multiple iSCSI targets and also map multiple LUNs to a single iSCSI target.

Creating an iSCSI Target

1. Go to **iSCSI & Fibre Channel > iSCSI Storage** .
2. Click **Create**, and then select **New iSCSI Target**.
The **iSCSI Target Creation Wizard** window opens.
3. Click **Next**.
4. Specify a target name.
QuTS hero appends the specified name to the iSCSI qualified name (IQN). IQNs are unique names used to identify targets and initiators.
 - Valid characters: 0 to 9, a to z, A to Z
 - Length: 1 to 16 characters
5. Optional: Specify a target alias.
An alias enables you to identify the target more easily on the initiator.
 - Length: 1 to 32 characters
 - Valid characters: 0 to 9, a to z, A to Z, underscore (_), hyphen (-), space ()
6. Optional: Select **Allow clustered access to this target**.
When enabled, multiple iSCSI initiators can access this target and its LUNs simultaneously.



Warning

To prevent data corruption, the initiators and LUN filesystems must all be cluster-aware.

7. Optional: Enable CRC checksums.
Initiators and targets communicate over TCP connections using iSCSI protocol data units (PDU). The sending device can send a checksum with each PDU. The receiving device uses this checksum to verify the integrity of the PDU, which is useful in unreliable network environments. There are two checksum types, which can be enabled separately.

Checksum Type	Description
Data Digest	The checksum can be used to verify the data portion of the PDU.
Header Digest	The checksum can be used to verify the header portion of the PDU.

8. Click **Next**.
9. Optional: Enable CHAP authentication.
An initiator must authenticate with the target using the specified username and password. This provides security, as iSCSI initiators do not require a NAS username or password.
 - Username
 - Length: 1 to 127 characters
 - Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-)

- Password
 - Length: 12 to 16 characters
 - Valid characters: 0 to 9, a to z, A to Z, all special characters

10. Optional: Enable mutual CHAP authentication.

Both the initiator and the target must authenticate with each other for additional security. First, the initiator authenticates with the target using the CHAP authentication username and password. Next, the target authenticates with the initiator using the mutual CHAP username and password.

- Username
 - Length: 1 to 127 characters
 - Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-)
- Password
 - Length: 12 to 16 characters
 - Valid characters: 0 to 9, a to z, A to Z, all special characters

11. Click **Next.**

12. Optional: Select **Create a LUN and map it to this target.**


If selected, QuTS hero opens the **Block-Based LUN Creation Wizard** immediately after finishing this wizard. The new LUN will then be automatically mapped to this target.

13. Click **Apply.**

QuTS hero creates the iSCSI target, and then opens the **Block-Based LUN Creation Wizard** window if **Create an iSCSI LUN and map it to this target** was enabled.

Editing iSCSI Target Settings

1. Go to **iSCSI & Fibre Channel > iSCSI Storage** .
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
The **Modify iSCSI Target** window opens.
4. Modify any of the following settings.

Setting	Description
Target Alias	An alias enables you to identify the target more easily on the initiator. <ul style="list-style-type: none"> • Length: 1 to 32 characters • Valid characters: 0 to 9, a to z, A to Z, underscore (_), hyphen (-), space ()
Enable clustered access to the iSCSI target from multiple initiators	When enabled, multiple iSCSI initiators can access this target and its LUNs simultaneously. <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;">  <p>Warning To prevent data corruption, the initiators and LUN filesystems must all be cluster-aware.</p> </div>

Setting	Description
CRC/Checksum	<p>Initiators and targets communicate over TCP connections using iSCSI protocol data units (PDU). The sending device can send a checksum with each PDU. The receiving device uses this checksum to verify the integrity of the PDU, which is useful in unreliable network environments. There are two checksum types, which can be enabled separately.</p> <ul style="list-style-type: none"> • Data Digest: The checksum can be used to verify the data portion of the PDU. • Header Digest: The checksum can be used to verify the header portion of the PDU.
Use CHAP authentication	<p>An initiator must authenticate with the target using the specified username and password. This provides security, as iSCSI initiators do not require a NAS username or password.</p> <ul style="list-style-type: none"> • Username <ul style="list-style-type: none"> • Length: 1 to 127 characters • Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-) • Password <ul style="list-style-type: none"> • Length: 12 to 16 characters • Valid characters: 0 to 9, a to z, A to Z, all special characters
Mutual CHAP	<p>Both the initiator and the target must authenticate with each other for additional security. First, the initiator authenticates with the target using the CHAP authentication username and password. Next, the target authenticates with the initiator using the mutual CHAP username and password.</p> <ul style="list-style-type: none"> • Username <ul style="list-style-type: none"> • Length: 1 to 127 characters • Valid characters: 0 to 9, a to z, A to Z, colon (:), period (.), hyphen (-) • Password <ul style="list-style-type: none"> • Length: 12 to 16 characters • Valid characters: 0 to 9, a to z, A to Z, all special characters

5. Click **Apply**.

Binding an iSCSI Target to a Network Interface

You can bind an iSCSI target to one or more network interfaces so that the iSCSI target can only be accessed via specific IP addresses.

1. Go to **iSCSI & Fibre Channel > iSCSI Storage** .
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
The **Modify an iSCSI Target** window opens.

4. Select **Network Portal**.
5. Optional: Select one or more network interfaces to bind to the iSCSI target.
6. Optional: Deselect one or more network interfaces to remove from the iSCSI target.
7. Click **Apply**.

QuTS hero applies the iSCSI target binding settings.

iSCSI Target Actions

You can perform various actions on iSCSI targets by going to **iSCSI & Fibre Channel > iSCSI Storage** . Select a target and then click **Action** to select the desired action.

Action	Description
Disable	Disable an active target and disconnect all connected iSCSI initiators.
Enable	Enable a deactivated target.
Modify	Edit the target's settings. For details, see Editing iSCSI Target Settings .
View Connections	View the IP addresses and IQN information of all iSCSI initiators connected to this target.
Delete	Disconnect all connected iSCSI initiators and delete the target. Any LUNs mapped to the target will be unmapped and then added to the unmapped LUN list.

iSCSI Target Status

You can view iSCSI target statuses by going to **iSCSI & Fibre Channel > iSCSI Storage** .

Status	Description
Ready	The target is accepting connections but no initiators are currently connected.
Connected	An initiator is connected to the target.
Offline	The target is not accepting connections.

iSCSI LUN Management

Mapping a LUN to an iSCSI Target

1. Go to **iSCSI & Fibre Channel > iSCSI Storage** .
2. Select a LUN.



Tip

Double-click an iSCSI target to view all of its mapped LUNs.

3. Optional: If the LUN is already mapped to a target, disable the LUN.
 - a. Click **Action**, and then select **Disable** .
A confirmation message appears.
 - b. Click **OK**.
QuTS hero disables the LUN.

4. Click **Action**, and then select **Edit LUN Mapping**.
The **Edit LUN Mapping** window opens.
5. Select **Map to iSCSI target**.
6. Select an iSCSI target.
7. Optional: Select **Enable LUN**.
If selected, QuTS hero enables the LUN after mapping it to the target.
8. Click **OK**.

Changing the Target of an iSCSI LUN

1. Go to **iSCSI & Fibre Channel > iSCSI Storage**.
2. Select a mapped LUN.



Tip

Double-click an iSCSI target to view all of its mapped LUNs.

3. Click **Action**, and then select **Disable**.
A confirmation message appears.
4. Click **OK**.
QuTS hero disables the LUN.
5. Click **Action**, and then select **Edit LUN Mapping**.
The **Edit LUN Mapping** window opens.
6. Select **Map to iSCSI target**.
7. Select an iSCSI target.
8. Optional: Select **Enable LUN**.
If selected, QuTS hero enables the LUN after mapping it to the target.
9. Click **OK**.

iSCSI LUN Status


You can view iSCSI LUN statuses by going to **iSCSI & Fibre Channel > iSCSI Storage**. Expand a target to view its mapped LUNs.

Status	Description
Enabled	The LUN is active and visible to connected initiators.
Disabled	The LUN is inactive and invisible to connected initiators.

iSCSI LUN Actions

You can perform various actions on iSCSI LUNs by going to **iSCSI & Fibre Channel > iSCSI Storage**. Expand a target to view its mapped LUNs, then select a LUN and click **Action** to select the desired action.

LUN Action	Description
Disable	Disable the LUN. The LUN will become inaccessible to connected iSCSI initiators.

LUN Action	Description
Enable	Enable the LUN if it is currently disabled.
Modify	Edit the LUN settings.
Delete	<p>Delete the LUN and all data stored on it.</p> <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;">  <p>Important</p> <ul style="list-style-type: none"> This action is only available if the LUN is unmapped. To delete a VJBOD Cloud LUN, use the VJBOD Cloud app. </div>
Edit LUN Mapping	<p>Unmap the LUN, or map it to a different iSCSI target or Fibre Channel Port group.</p> <p>For details, see the following topics:</p> <ul style="list-style-type: none"> Mapping a LUN to a Fibre Channel Port Group Mapping a LUN to an iSCSI Target
Show in Storage & Snapshots	Manage the LUN at Storage & Snapshots > Storage > Storage/Snapshots .
LUN Import/Export	<p>Export the LUN to another server, a local NAS folder, or an external storage device.</p> <p>For details, see LUN Import/Export.</p>

iSCSI Access Control List

The iSCSI access control list (ACL) allows you to configure a LUN masking policy for each connected iSCSI initiator. A LUN masking policy determines which LUNs the initiator is able to see and access. If no policy is specified for an iSCSI initiator, then QuTS hero applies the default policy to it.



Tip

- The default policy gives all iSCSI initiators full read/write access to all LUNs.
- You can edit the default policy so that all LUNs are either read-only or not visible to all iSCSI initiators, except for initiators with specific permissions from a policy.

Adding an iSCSI LUN Masking Policy

- Go to **iSCSI & Fibre Channel > iSCSI Storage**.
- Click **iSCSI ACL**.
The **iSCSI ACL** window opens.
- Click **Add a Policy**.
The **Add a Policy** window opens.
- Specify the policy name.
The name must consist of 1 to 32 characters from any of the following groups:
 - Letters: a-z, A-Z
 - Numbers: 0-9
 - Special characters: Hyphen (-), space (), underscore (_)

5. Specify the initiator IQN.
6. Configure the access permissions for each LUN.

Permission	Description
Read Only	The iSCSI initiator can read data on the LUN, but cannot write, modify, or delete data.
Read/Write	The iSCSI initiator can read, write, modify, and delete data on the LUN.
Deny Access	The LUN is invisible to the iSCSI initiator.

**Tip**

Click the values in the columns to change the permissions.

7. Click **Apply**.

Editing an iSCSI LUN Masking Policy

1. Go to **iSCSI & Fibre Channel > iSCSI Storage** .
2. Click **iSCSI ACL**.
The **iSCSI ACL** window opens.
3. Select a policy.
4. Click **Edit**.
The **Modify a Policy** window opens.
5. Optional: Edit the policy name.
The name must consist of 1 to 32 characters from any of the following groups:
 - Letters: a-z, A-Z
 - Numbers: 0-9
 - Special characters: Hyphen (-), space (), underscore (_)
6. Optional: Configure the access permissions for each LUN.

Permission	Description
Read Only	The iSCSI initiator can read data on the LUN, but cannot write, modify, or delete data.
Read/Write	The iSCSI initiator can read, write, modify, and delete data on the LUN.
Deny Access	The LUN is invisible to the iSCSI initiator.

**Tip**

Click the values in the columns to change the permissions.

7. Click **Apply**.

Deleting an iSCSI LUN Masking Policy

1. Go to **iSCSI & Fibre Channel > iSCSI Storage** .
2. Click **iSCSI ACL**.
The **iSCSI ACL** window opens.

3. Select a policy.
4. Click **Delete**.
A confirmation message appears.
5. Click **OK**.

iSCSI Target Authorization

Each iSCSI target can be configured either to allow connections from all iSCSI initiators, or to only allow connections from a list of authorized initiators.



Important

By default, iSCSI target authorization is disabled.

Configuring an iSCSI Target's Authorized Initiators List

1. Go to **iSCSI & Fibre Channel > iSCSI Storage** .
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
The **Modify an iSCSI Target** window opens.
4. Click **Initiators**.
5. Select **Allow connections from the list only**.
6. Optional: Add one or more iSCSI initiators to the authorized iSCSI initiators list.
 - a. Click **Add**.
 - b. Specify the initiator IQN.
 - c. Click **Confirm**.
 - d. Repeat the previous steps for each additional iSCSI initiator that you want to add.
7. Optional: Delete one or more iSCSI initiators from the authorized iSCSI initiators list.
 - a. Select an initiator IQN.
 - b. Click **Delete**.
 - c. Repeat the previous steps for each additional iSCSI initiator that you want to delete.
8. Click **Apply**.

Enabling iSCSI Target Authorization

1. Go to **iSCSI & Fibre Channel > iSCSI Storage** .
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
The **Modify an iSCSI Target** window opens.
4. Click **Initiators**.

5. Select **Allow connections from the list only**.
6. Add one or more iSCSI initiators to the authorized iSCSI initiators list.
 - a. Click **Add**.
 - b. Specify the initiator IQN.
 - c. Click **Confirm**.
7. Repeat the previous steps for each additional iSCSI initiator that you want to add.
8. Click **Apply**.

Disabling iSCSI Target Authorization

1. Go to **iSCSI & Fibre Channel > iSCSI Storage**.
2. Select an iSCSI target.
3. Click **Action**, and then select **Modify**.
The **Modify an iSCSI Target** window opens.
4. Click **Initiators**.
5. Select **Allow all connections**.
6. Click **Apply**.

QNAP Snapshot Agent

QNAP Snapshot Agent enables QuTS hero to take application-consistent snapshots of iSCSI LUNs on VMware or Microsoft servers. Application-consistent snapshots record the state of running applications, virtual machines, and data. When QuTS hero takes a LUN snapshot, QNAP Snapshot Agent triggers the following actions:

- Windows: The server flushes data in memory, logs, and pending I/O transactions to the LUN before the snapshot is created.
- VMware: The server takes a virtual machine snapshot.



Tip

To download QNAP Snapshot Agent, go to <https://www.qnap.com/utilities> and then click **Enterprise**.

Snapshot Agent Server List

To view a list of all iSCSI initiators that are using QNAP Snapshot Agent with this NAS, go to **iSCSI & Fibre Channel > iSCSI Storage**. Click **Snapshot**, and then select **Snapshot Agent**.



Tip

To unregister an iSCSI initiator, select it in the list and then click **Remove**.

Snapshot Agent ✕

Registered Snapshot Agent List <https://www.qnap.com/utility>

Agent IP/FQDN	Agent...	Client OS	NAS LUN info	Status
172.17.48.71	1.3.052	Microsoft Windows NT 6.2.9200.0	LUN_1 (E:\)	Online

⏪ ⏩ | Page /1 | ⏪ ⏩ | ↻
Display item: 1-1, Total: 1 | Show Item(s)

Fibre Channel

Fibre Channel enables computers, servers, other NAS devices, and virtual machines to access NAS storage in the form of LUNs over a Fibre Channel network. Hosts can partition, format, and use the LUNs as if they were local disks.

Fibre Channel Ports

You can view and configure Fibre Channel ports and port groups on the NAS by going to **iSCSI & Fibre Channel > Fibre Channel > FC Ports** .

Fibre Channel Port Groups

A Fibre Channel port group is a group of one or more Fibre Channel ports. Fibre Channel port groups help you organize and manage LUN mappings more easily. When a LUN is mapped to a Fibre Channel port group, QuTS hero automatically maps the LUN to every Fibre Channel port in the group.



Important

- Each Fibre Channel port can be in one or more Fibre Channel port groups.
- Each LUN can only be mapped to one Fibre Channel group.
- There is a default port group that contains all Fibre Channel ports.

Creating a Fibre Channel Port Group

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC Ports** .
2. Click **Create Port Group**.
The **Create Port Group** window opens.

3. Specify a group name.
Name requirements:
 - Length: 1–20 characters
 - Valid characters: A–Z, a–z, 0–9
4. Select one or more Fibre Channel ports.
5. Click **Create**.

Mapping a LUN to a Fibre Channel Port Group

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC Storage**.
2. Select a LUN.
3. Click **Action**, and then select **Edit LUN Mapping**.
The **Edit LUN Mapping** window opens.
4. Select **Map to FC port group**.
5. Select a Fibre Channel port group.



Tip
The default group contains all Fibre Channel ports.

6. Choose whether you want to configure LUN masking.

Option	Description
Enable LUN and do not configure LUN masking	Do not configure LUN masking. Any initiator that is able to connect to a Fibre Channel port in the port group will be able to see the LUN.
Keep LUN disabled and configure LUN masking in the next step	Configure LUN masking. You can restrict which initiators can see the LUN.

7. Click **OK**.
8. Optional: Configure LUN masking.
 - a. Add one or more initiator WWPNs to the LUN's authorized initiators list.

Method	Steps
Add from WWPN list	<ol style="list-style-type: none"> 1. Select one or more initiator WWPNs in the WWPN list. 2. Click Add.
Add WWPNs as text	<ol style="list-style-type: none"> 1. Specify one WWPN per line using any of the following formats: <ul style="list-style-type: none"> • XXXXXXXXXXXXXXXXXXXX • XX : XX : XX : XX : XX : XX : XX : XX 2. Click Add.

- b. Optional: Select **Add unknown WWPNs to the FC WWPN Aliases List**.
When selected, QuTS hero will add any unknown WWPNs to the list of known aliases. To view the list, go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases**.
- c. Optional: Select **Enable LUN**.

If selected, QuTS hero enables the LUN after mapping it to the target.

- d. Click **OK**.

Configuring Fibre Channel Port Binding

Port binding is a Fibre Channel security method that enables you to restrict which initiator WWPNs are allowed to connect through a Fibre Channel port. It is similar to iSCSI target authorization.



Tip

By default, port binding is disabled on all Fibre Channel ports.

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC Ports** .
2. Select a Fibre Channel port.
3. Click **Action**, and then select **Edit Port Binding**.
The **Fibre Channel Port Binding** window opens.
4. Add one or more initiator WWPNs to the LUN's authorized initiators list.

Method	Steps
Add from WWPN list	<ol style="list-style-type: none"> a. Select one or more initiator WWPNs in the WWPN list. b. Click Add.
Add WWPNs as text	<ol style="list-style-type: none"> a. Specify one WWPN per line using any of the following formats: <ul style="list-style-type: none"> • XXXXXXXXXXXXXXXXXXXX • XX : XX : XX : XX : XX : XX : XX : XX b. Click Add.

5. Optional: Select **Add unknown WWPNs to the FC WWPN Aliases List**.
When selected, QuTS hero will add any unknown WWPNs to the list of known aliases. To view the list, go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases** .
6. Click **OK**.

Fibre Channel Port Actions

You can perform various actions on Fibre Channel ports by going to **iSCSI & Fibre Channel > Fibre Channel > FC Ports** . Select a port and then click **Action** to select the desired action.

Action	Description
Edit Alias	Edit the alias for the Fibre Channel port. The alias must consist of 1 to 20 characters from any of the following groups: <ul style="list-style-type: none"> • Letters: A-Z, a-z • Numbers: 0-9 • Special characters: Hyphen (-), underscore (_)
View initiators	View a list of all Fibre Channel initiators currently logged into the port.

Action	Description
Edit port binding	Modify the port binding for the port. Port binding allows you to restrict which initiators are allowed to connect to the port. For more information, see Configuring Fibre Channel Port Binding .

Fibre Channel Port Status

You can view Fibre Channel port statuses by going to **iSCSI & Fibre Channel > Fibre Channel > FC Ports** .

Status	Description
Connected	The port has an active network connection.
Disconnected	The port does not have an active network connection.

Fibre Channel Storage

You can manage and monitor Fibre Channel LUNs by going to **iSCSI & Fibre Channel > Fibre Channel > FC Storage** .

Masking a LUN from Fibre Channel Initiators

LUN masking is a security feature that enables you to make a LUN visible to some Fibre Channel initiators and invisible to other initiators.

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC Storage** .
2. Select a LUN.



Important


The LUN must be disabled.

3. Click **LUN Masking**.
The **LUN Masking** window opens.
4. Add one or more initiator WWPNs to the LUN's authorized initiators list.

Method	Steps
Add from WWPN list	<ol style="list-style-type: none"> a. Select one or more initiator WWPNs in the WWPN list. b. Click Add.
Add WWPNs as text	<ol style="list-style-type: none"> a. Specify one WWPN per line using any of the following formats: <ul style="list-style-type: none"> • XXXXXXXXXXXXXXXXXXXX • XX : XX : XX : XX : XX : XX : XX : XX b. Click Add.

5. Optional: Select **Add unknown WWPNs to the FC WWPN Aliases List**.
When selected, QuTS hero will add any unknown WWPNs to the list of known aliases. To view the list, go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases** .
6. Select **Enable LUN**.
If selected, QuTS hero will enable the LUN after mapping it to the target.
7. Click **OK**.

Fibre Channel LUN Actions

LUN Action	Description
Edit LUN Mapping	Unmap the LUN, or map it to a different iSCSI target or Fibre Channel Port group. For details, see the following topics: <ul style="list-style-type: none"> • Mapping a LUN to a Fibre Channel Port Group • Mapping a LUN to an iSCSI Target
Edit LUN Masking	LUN masking is an authorization method that makes a Logical Unit Number (LUN) visible to some initiators and invisible to other initiators. For details, see Masking a LUN from Fibre Channel Initiators .
Show in Storage & Snapshots	Manage the LUN at Storage & Snapshots > Storage > Storage/ Snapshots .
Modify	Edit the LUN settings.
Enable	Enable the LUN if it is currently disabled.
Disable	Disable the LUN. The LUN will become inaccessible to connected iSCSI initiators.
Delete	Delete the LUN and all data stored on it.  Important This action is only available if the LUN is unmapped.
LUN Import/Export	Export the LUN to another server, a local NAS folder, or an external storage device. For details, see Creating a LUN Export Job .

Fibre Channel LUN Status

You can view Fibre Channel LUN statuses by going to **iSCSI & Fibre Channel > Fibre Channel > FC Storage** . Expand a port group to view its LUNs.

Status	Description
Enabled	The LUN is active and visible to connected initiators.
Disabled	The LUN is inactive and invisible to connected initiators.

Fibre Channel WWPN Aliases

A WWPN (World Wide Port Name) is a unique identifier for Fibre Channel ports. A WWPN alias is a unique human-readable name for a Fibre Channel port that makes it easier to identify it.

You can view, edit, and add WWPNs and WWPN aliases by going to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases** .

Adding WWPNs

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases** .
2. Click **Add**.
The **Add WWPN** window appears.
3. Add one or more WWPNs to the list of known WWPNs using any of the following methods.

Method	Steps
Add WWPNs from logged-in Fibre Channel initiators.	Select Add WWPNs from all logged-in FC initiators .
Add WWPNs as text	Specify one WWPN per line using any of the following formats: <ul style="list-style-type: none"> • XXXXXXXXXXXXXXXXXXXX • XX:XX:XX:XX:XX:XX:XX:XX

4. Click **Add**.

Configuring a WWPN Alias

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases** .
2. Locate a WWPN.
3. Under **Alias**, specify an alias for the WWPN.
The alias must consist of 1 to 20 characters from any of the following groups:
 - Letters: A-Z, a-z
 - Numbers: 0-9
 - Special Characters: Underscore (_), hyphen (-)
4. Click **Save**.

Removing a WWPN Alias

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases** .
2. Locate a WWPN.
3. Clear the **Alias** field.
4. Click **Save**.

Exporting a List of WWPN Aliases

1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases** .
2. Click **Export**.
The file browser window opens.
3. In the file browser window, navigate to the folder where you want to save the file.
4. Specify a filename.
5. Click **Save**.

The list of WWPN aliases is saved to your local computer as a CSV file, in the format:

- Field 1: WWPN
- Field 2: Alias

```

11:00:24:5e:be:00:00:06,ja882c32p1
11:00:24:5e:be:00:00:07,ja88c32p2
11:00:00:24:5e:be:00:06,ja88c16p1
11:00:00:24:5e:be:00:07,ja882c16p2
10:00:00:10:9b:1b:cc:99,z640Emulex2
11:00:f4:e9:d4:54:89:49,z640Q32gport2
10:00:00:99:99:99:99:87,test3
10:00:00:99:99:99:99:99,test1
10:00:00:10:9b:1b:cc:98,z640Emulex1
11:00:f4:e9:d4:54:89:48,z640Q32gport1
10:00:00:99:99:99:99:89,test2
11:00:f4:e9:d4:58:23:46,QL16c1p1
11:00:f4:e9:d4:58:23:47,QL16c1p2
11:00:f4:e9:d4:58:31:bc,QL16c2p1
11:00:f4:e9:d4:58:31:bd,QL16c2p2

```

Example CSV Output

Importing a List of WWPN Aliases

You can import a list of WWPNs and aliases from a CSV file in the following format:

- Field 1: WWPN
- Field 2: Alias

```

11:00:24:5e:be:00:00:06,ja882c32p1
11:00:24:5e:be:00:00:07,ja88c32p2
11:00:00:24:5e:be:00:06,ja88c16p1
11:00:00:24:5e:be:00:07,ja882c16p2
10:00:00:10:9b:1b:cc:99,z640Emulex2
11:00:f4:e9:d4:54:89:49,z640Q32gport2
10:00:00:99:99:99:99:87,test3
10:00:00:99:99:99:99:99,test1
10:00:00:10:9b:1b:cc:98,z640Emulex1
11:00:f4:e9:d4:54:89:48,z640Q32gport1
10:00:00:99:99:99:99:89,test2
11:00:f4:e9:d4:58:23:46,QL16c1p1
11:00:f4:e9:d4:58:23:47,QL16c1p2
11:00:f4:e9:d4:58:31:bc,QL16c2p1
11:00:f4:e9:d4:58:31:bd,QL16c2p2

```

Example CSV File



Important

- Identical aliases will be overwritten from the CSV file.
- Lines not formatted correctly will be ignored.


1. Go to **iSCSI & Fibre Channel > Fibre Channel > FC WWPN Aliases** .

2. Click **Import**.
The file browser window opens.
3. Locate and open the CSV file.

9. ZFS Pool Profiling Tool

ZFS Pool Profiling Tool controls the creation and execution of storage pool over-provisioning tests. These tests help determine the optimum amount of over-provisioning to set when creating a storage pool.

Installing ZFS Pool Profiling Tool

1. Log on to QuTS hero as administrator.
2. Open **App Center**, and then click . A search box appears.
3. Enter `ZFS Pool Profiling Tool`. The ZFS Pool Profiling Tool application appears in the search results.
4. Click **Install**. The installation window appears.
5. Click **OK**.

QuTS hero installs ZFS Pool Profiling Tool.

Storage Pool Over-Provisioning

Over-provisioning reserves a specified percentage of space in a storage pool so that new data can be written into a complete block even if the pool is almost full. Higher pool over-provisioning provides higher write performance for intensive workloads and performance-demanding applications.

Creating a Storage Pool Over-Provisioning Test

During a storage pool over-provisioning test, ZFS Pool Profiling Tool first fills the storage pool with random data. It then tests the random write performance of the storage pool over several test phases, each using a different amount of over-provisioning.

For example, if a test is created with a test range of 0-20% and a test interval of 5%, ZFS Pool Profiling Tool will test pool write performance in five phases, with over-provisioning set to 0%, 5%, 10%, 15%, and 20%. If the random write performance of a disk is very low during any phase, ZFS Pool Profiling Tool will end the phase early and move to the next one.


1. Go to **ZFS Pool Profiling Tool > Review**.
2. Click **+ Create Test**. The **Create ZFS Pool Test** wizard opens.
3. Click **Next**.
4. Optional: Select an expansion unit from the **Enclosure Unit** list.



Important


You cannot select disks from multiple expansion units.

5. Select one or more disks. Selecting a single disk determines the optimum amount of over-provisioning for all disks of the same model and capacity. Selecting multiple disks determines the optimum amount of over-provisioning for that specific combination of disks and RAID type. Testing multiple disks gives more accurate results, but takes significantly longer than testing a single disk.


 **Important**
All selected disks must be of the same drive type (e.g., HDD, SSD).

 **Warning**
All data on the selected disks will be deleted.

6. Select a RAID type.
7. Click **Next**.
8. Optional: Configure the test settings.

Setting	Description
Over-provisioning test range	Specify the minimum and maximum amount of over-provisioning to test.
Test interval	Specify the over-provisioning increments to test.
End a test phase early if consistent performance is too low	<p>ZFS Pool Profiling Tool will end a test phase after 5 minutes of testing if the random write speeds during the phase are lower than a system-defined threshold.</p> <p> Tip Enabling this avoids wasting time testing disks when the specified amount of over-provisioning is producing no measurable benefits.</p>

9. Review the estimated time required.
For multiple disks, the test may take more than 24 hours.




 **Tip**
If the estimated test time is too long, reduce the test range or test interval.

10. Click **Next**.
11. Verify the test information.
12. Click **Create**.
A confirmation message appears.
13. Click **OK**.


ZFS Pool Profiling Tool creates and starts running the test. The test appears as a background task in QuTS hero.

Test Reports

You can view, export, and delete test results in **ZFS Pool Profiling Tool > Test Reports** .

Icon	Description
	Open the report in a new window.
	Download a copy of the report in XLSX format.
	Delete the report.

Test reports provide the following information to help you determine the optimal amount of over-provisioning.

Section	Description
Test Information	View information about the NAS, the disks being tested, and the settings used in this test.
Test Result	View the test results as a graph. Choose from the following views: <ul style="list-style-type: none"> • IOPS / Time • IOPS / Data Written • Data Written / Time <div style="display: flex; align-items: flex-start; margin-top: 10px;">  <div> <p>Tip</p> <p>Use these graphs to compare what effect different amounts of over-provisioning have on random write speeds (IOPS).</p> </div> </div>
Over-Provisioning Evaluation Results	Enter an IOPS value in Target write performance . ZFS Pool Profiling Tool will recommend the amount of over-provisioning needed to consistently achieve the target random write performance.
Temperature	View the temperature of the disks during each test phase.
Test RAID Group	View information about the test pool RAID group. Details include the RAID type, number of disks, model and capacity of each disk, and disk read/write performance.

Settings

You can configure settings in **ZFS Pool Profiling Tool** >  > **Settings** .

Setting	Description
Maximum number of reports	ZFS Pool Profiling Tool retains the specified number of reports. Creating additional reports deletes the oldest ones.

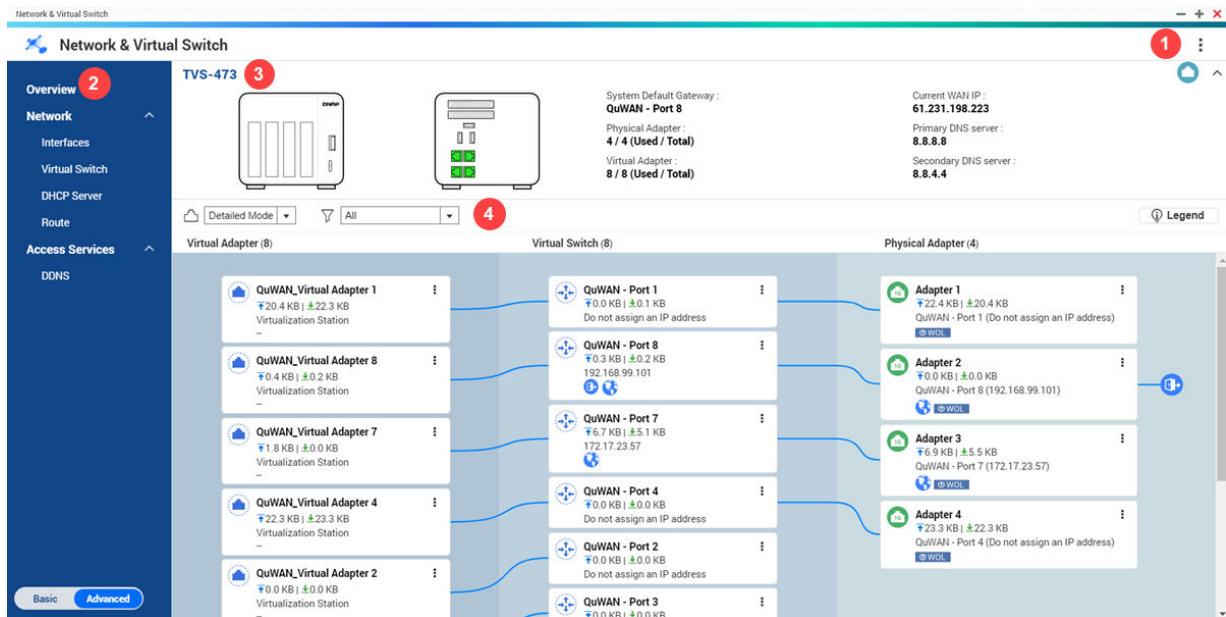
10. Network & Virtual Switch

About Network & Virtual Switch








Network & Virtual Switch is a QuTS hero utility that centralizes the creation, configuration, and control of network connections. Network & Virtual Switch also manages physical network interfaces, virtual adapters, Wi-Fi, and Thunderbolt connections in addition to controlling DHCP, DDNS, and gateway services.

Parts of the User Interface

The Network & Virtual Switch user interface has four main areas.



Label	Area	Description
1	Toolbar	<p>The toolbar displays the following buttons:</p> <ul style="list-style-type: none"> • More: Click and then select one of the following. <ul style="list-style-type: none"> • Quick Start: Opens the Network & Virtual Switch guide. • Help: Opens the Network & Virtual Switch Help panel. • About: Displays the application version.

Label	Area	Description
2	Menu	<p>Network & Virtual Switch features two separate usage modes in the menu pane. Switch between these modes by clicking Basic or Advanced.</p> <ul style="list-style-type: none"> • Basic: This mode is well-suited for most users, and requires minimal configuration of network settings. The following functions are disabled: <ul style="list-style-type: none"> • Static route • Virtual switch • Advanced: This mode is best-suited for power-users who need more control over the configuration of network settings. The following functions are enabled: <ul style="list-style-type: none"> • Static route • Virtual switch
3	Main panel	<p>The main panel displays the device network information. You can perform the following tasks on the main panel.</p> <ul style="list-style-type: none"> •  : Click to view the MAC address of the network adapters. •  : Click to collapse the main panel.
4	Network topology	<p>The network topology provides a visual representation of the connected physical and virtual network adapters. You can perform the following tasks on the network topology panel.</p> <ul style="list-style-type: none"> • Click the drop-down list beside  to view the topology in simple or detailed mode. • Click the drop-down list beside  to filter and view specific network topology components. • Click Legend to view the different icons and their descriptions. • Physical adapters: Click  and select one of the following. <ul style="list-style-type: none"> • Locate: Click to identify the network port on the main panel. • Setting: Click to configure the physical adapter settings. • Virtual switches: Click  and then click Settings to open the virtual switch configuration page. • Virtual adapters: Click  and then click Execute to view the virtual adapter information on Virtualization Station




Basic Network Adapter Configuration

Network & Virtual Switch allows QuTS hero users to configure and manage the basic network adapter settings including different IP addressing methods, routing protocols, and system default gateway.

Configuring IPv4 Settings

1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Identify the adapter that you want to configure, then click **Configure** .
The **Configure** window opens.
4. Configure the IPv4 settings.


Setting	Description
Obtain IP address settings automatically via DHCP	If the network supports DHCP, the adapter automatically obtains the IP address and network settings.
Use static IP address	Manually assign a static IP address. You must specify the following information: <ul style="list-style-type: none"> • Fixed IP Address • Subnet Mask • Default Gateway

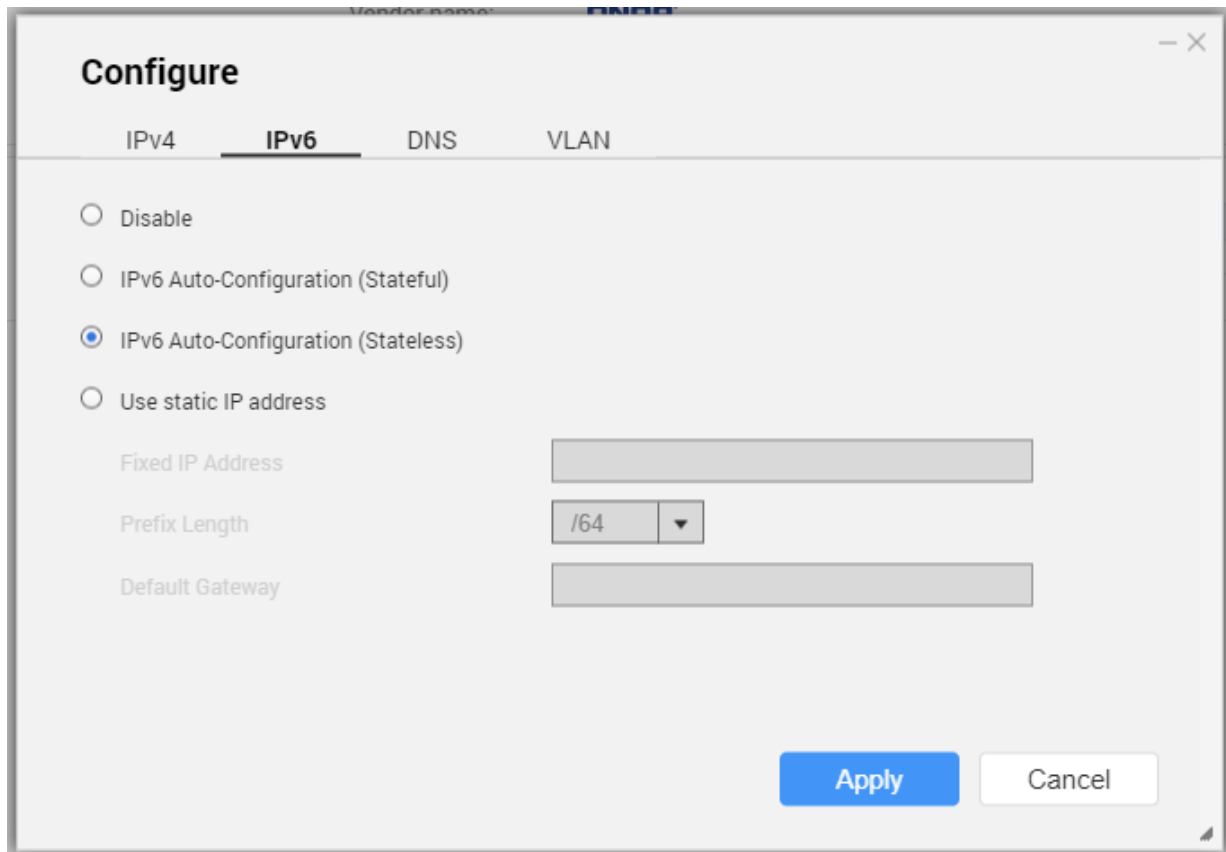
Setting	Description
Jumbo Frame	<p>Jumbo Frames are Ethernet frames that are larger than 1500 bytes. They are designed to enhance Ethernet networking throughput, and to reduce CPU usage when transferring large files. QuTS hero supports the following MTU sizes:</p> <ul style="list-style-type: none"> • 1500 bytes (default) • 4074 bytes • 7418 bytes • 9000 bytes <p> Important</p> <ul style="list-style-type: none"> • All connected network devices must enable Jumbo Frames and use the same MTU size. • Only certain NAS models support Jumbo Frames. • Using Jumbo Frames requires a network speed of 1000 Mbps or faster.
Network Speed	<p>Select the network transfer rate allowed by the network environment.</p> <p> Tip Selecting Auto-negotiation will automatically detect and set the transfer rate.</p> <p> Important The Network Speed field is automatically set to Auto-negotiation and hidden when configuring 10GbE & 40GbE adapters.</p>



5. Click **Apply**.


Network & Virtual Switch updates the IPv4 settings.

Configuring IPv6 Settings

1. Go to **Control Panel > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Identify the adapter that you want to configure and then click  > **Configure** .
The **Configure** window opens.
4. Go to the **IPv6** tab.
5. Configure the IPv6 settings.



Setting	Description
Disable	Do not assign an IPv6 address.
IPv6 Auto-Configuration (Stateful)	<p>The adapter automatically acquires an IPv6 address and DNS settings from the DHCPv6-enabled server.</p> <p> Important This option requires an available DHCPv6-enabled server on the network.</p>
IPv6 Auto-Configuration (Stateless)	<p>The adapter automatically acquires an IPv6 address and DNS settings from the router.</p> <p> Important This option requires an available IPv6 RA(router advertisement)-enabled router on the network.</p>

Setting	Description
Use static IP address	<p>Manually assign a static IP address to the adapter. You must specify the following information:</p> <ul style="list-style-type: none"> Fixed IP Address Prefix length <p> Tip Obtain the prefix length information from your network administrator.</p> <ul style="list-style-type: none"> Default Gateway

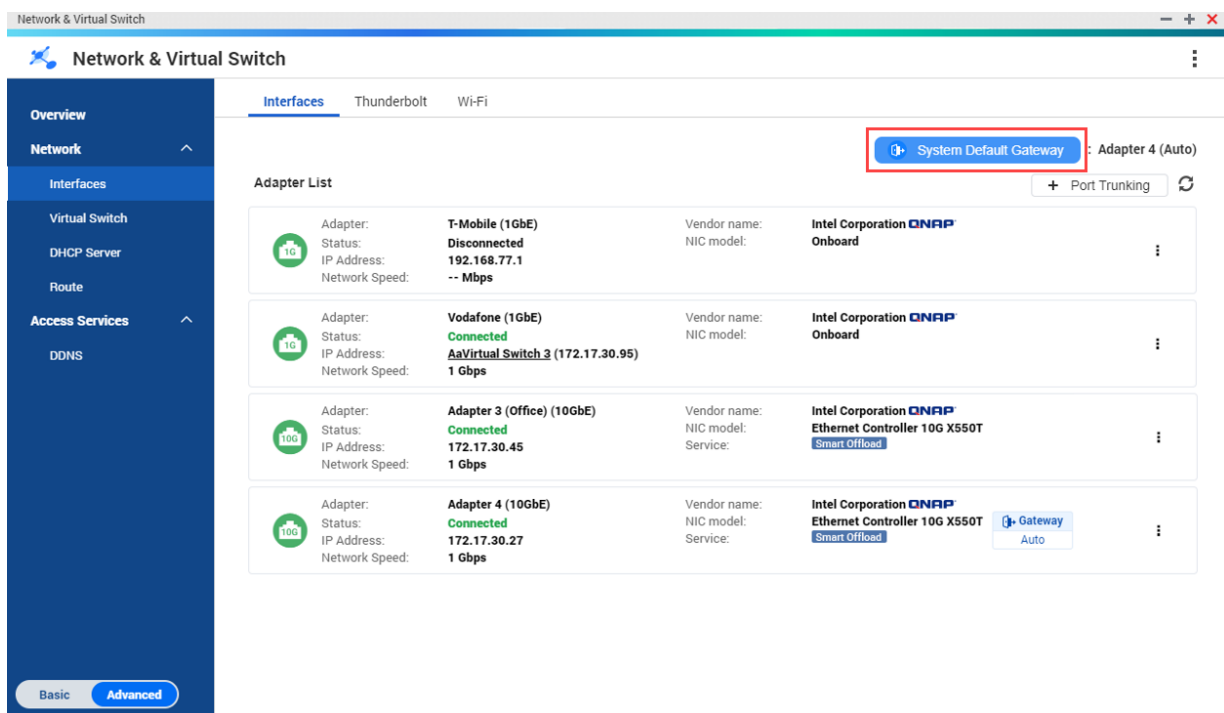
6. Click **Apply**.

Network & Virtual Switch updates the IPv6 settings.

Configuring the System Default Gateway

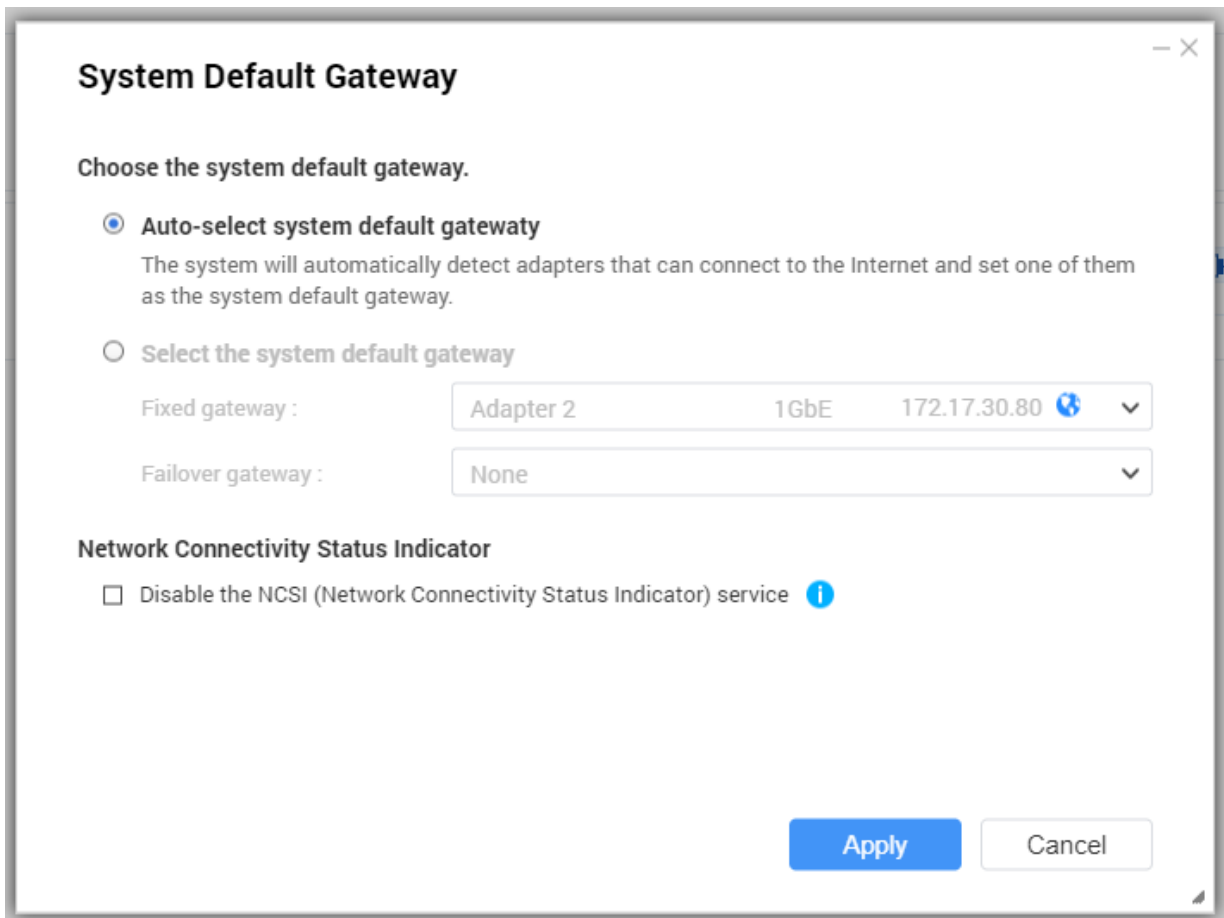
The system default gateway serves as the network access point for the NAS. By default, all external network traffic will pass through the gateway. You must configure a network interface first prior to assigning the default gateway.


- Go to **Control Panel > Network & File Services > Network & Virtual Switch**. The **Network & Virtual Switch** window opens.
- Go to **Network > Interfaces**.
- Click **System Default Gateway**.



The **System Default Gateway** window opens.

- Configure the system default gateway.



Setting	User Action
Auto-select system default gateway	Select to allow QuTS hero automatically detect all adapter, virtual switch, PPPoE, and VPN connections that can be used to connect to the internet. It selects one of these connections and then sets it as the default gateway.
Select the system default gateway	Manually assign an adapter to serve as the system default gateway. Optionally, set a backup failover gateway. The failover default gateway field is only available when multiple interfaces are connected. <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"></div> <div> <p>Tip When assigning a PPPoE or VPN connection as the default gateway, ensure a stable physical connection is also set as the failover default gateway.</p> </div> </div>

5. Optional: Disable the NCSI service.



Tip

The QuTS hero Network Connectivity Status Indicator (NCSI) periodically performs tests to check the speed and status of NAS network connections.

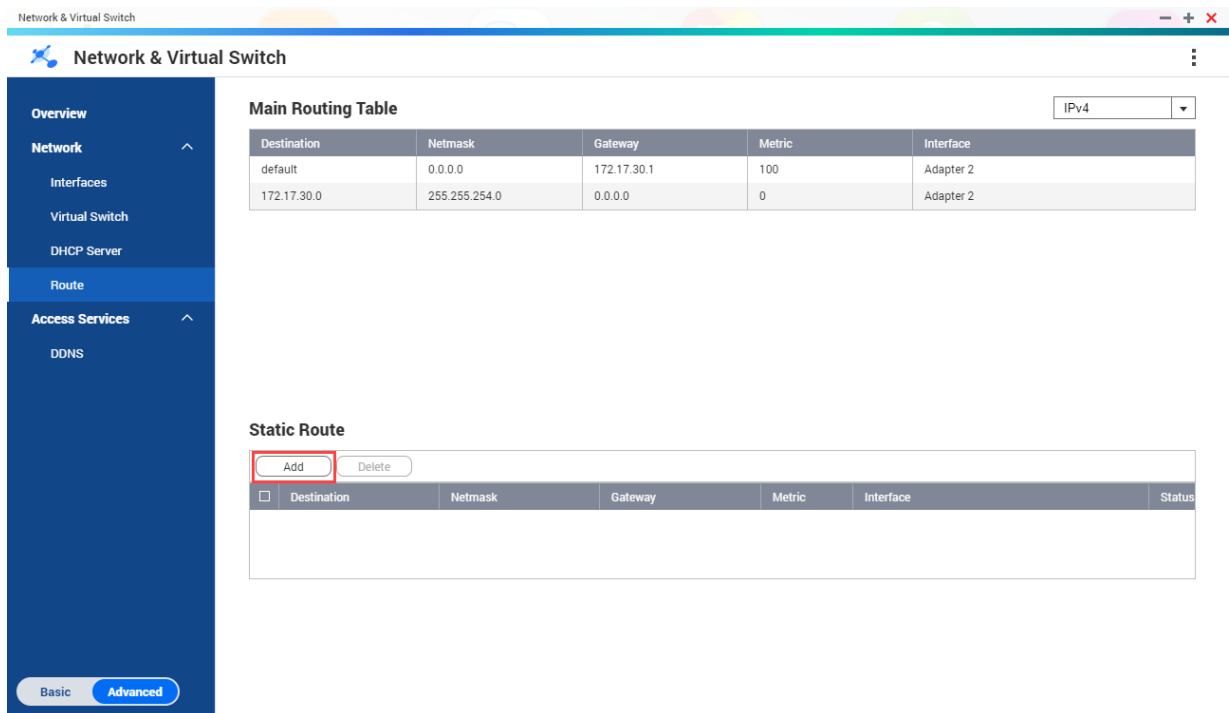
6. Click **Apply**.

Network & Virtual Switch updates the system default gateway.

Configuring Static Route Settings

You can create and manage IPv4 and IPv6 static routes in the **Route** section of Network & Virtual Switch. Under normal circumstances, QuTS hero automatically obtains routing information after it has been configured for Internet access. Static routes are only required in special circumstances, such as having multiple IP subnets located on your network.

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Route** .
3. Select a method for adding the IP static route.
 - IPv4 static route
 - IPv6 static route
4. Configure the IPv4 static route settings.
 - a. Beside Main Routing Table, select **IPv4** from the drop-down menu.
 - b. Click **Add**.



The **Static Route (IPv4)** window opens.

- c. Configure the IP address settings.

Static Route (IPv4) — X

Destination:


Netmask: ▼

Gateway:

Metric:

Interface: ▼

Apply
Close

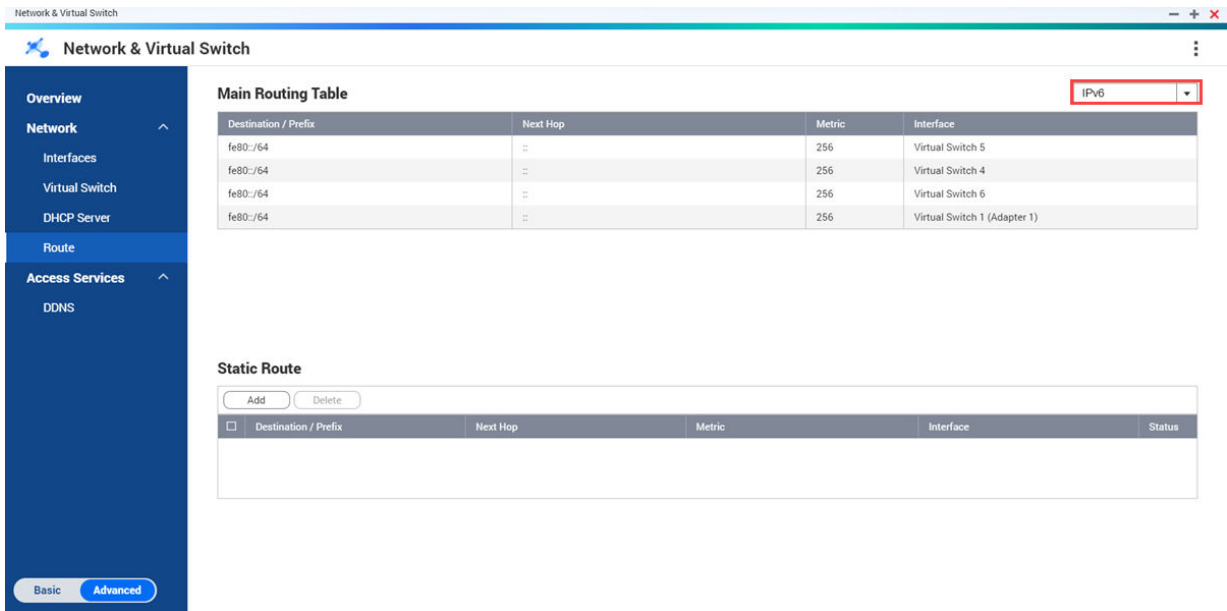
Setting	Description
Destination	Specify a static IP address where connections are routed to.
Netmask	Specify the IP address of the destination's netmask.
Gateway	Specify the IP address of the destination's gateway.
Metric	Specify the number of nodes that the route will pass through. <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"></div> <div> <p>Note Metrics are cost values used by routers to determine the best path to a destination network.</p> </div> </div>
Interface	Select the interface that connections should be routed through.

d. Click **Apply**.

Network & Virtual Switch adds the IPv4 static route.

5. Configure the IPv6 static route settings.


a. Beside Main Routing Table, select **IPv6** from the drop-down menu.



- b. Click **Add**.
The **Static Route (IPv6)** window opens.
- c. Configure the IP address settings.



Setting	Description
Destination	Specify a static IPv6 address where connections are routed to.
Prefix Length	Select the destination prefix length for the IPv6 static route.
Next Hop	Specify the next hop IP address in IPv6 format. <div style="display: flex; align-items: center;"> <div> <p>Tip IPv6 next hop format: 2001:db8::1</p> </div> </div>

Setting	Description
Metric	Specify the number of nodes that the route will pass through.  Note Metrics are cost values used by routers to determine the best path to a destination network.
Interface	Select the interface that connections should be routed through.

d. Click **Apply**.


Network & Virtual Switch adds the IPv6 static route.

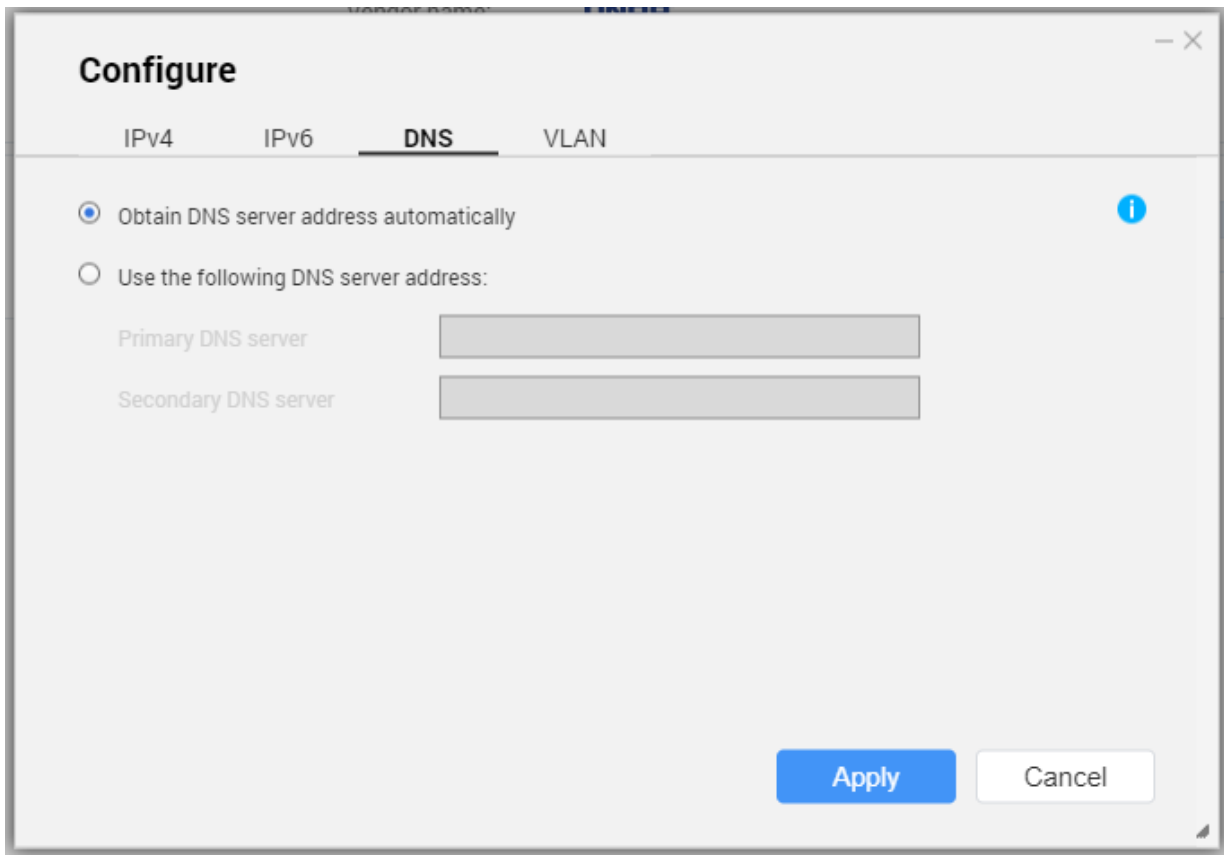
IP Addressing Services Configuration


QNAP provides IP addressing services for network adaptability and scalability. You can deploy dynamic address allocation and resolution techniques such as DNS, DDNS, DHCP server, and RADVR settings to meet evolving network requirements.

Configuring DNS Server Settings

A Domain Name System (DNS) server translates a domain name into an IP address. You can either automatically obtain a public DNS server IP address or manually assign an IP address for the DNS server.

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Identify the adapter that you want to configure, then click  > **Configure** .
The **Configure** window opens.
4. Go to the **DNS** tab.
5. Select one of the following options:




Setting	User Action
Obtain DNS server address automatically	Automatically obtain the IP address using DHCP.
Use the following DNS server address	Manually assign the IP address for the primary and secondary DNS servers.  Important QNAP recommends specifying at least one DNS server to allow URL lookups.

6. Click **Apply.**

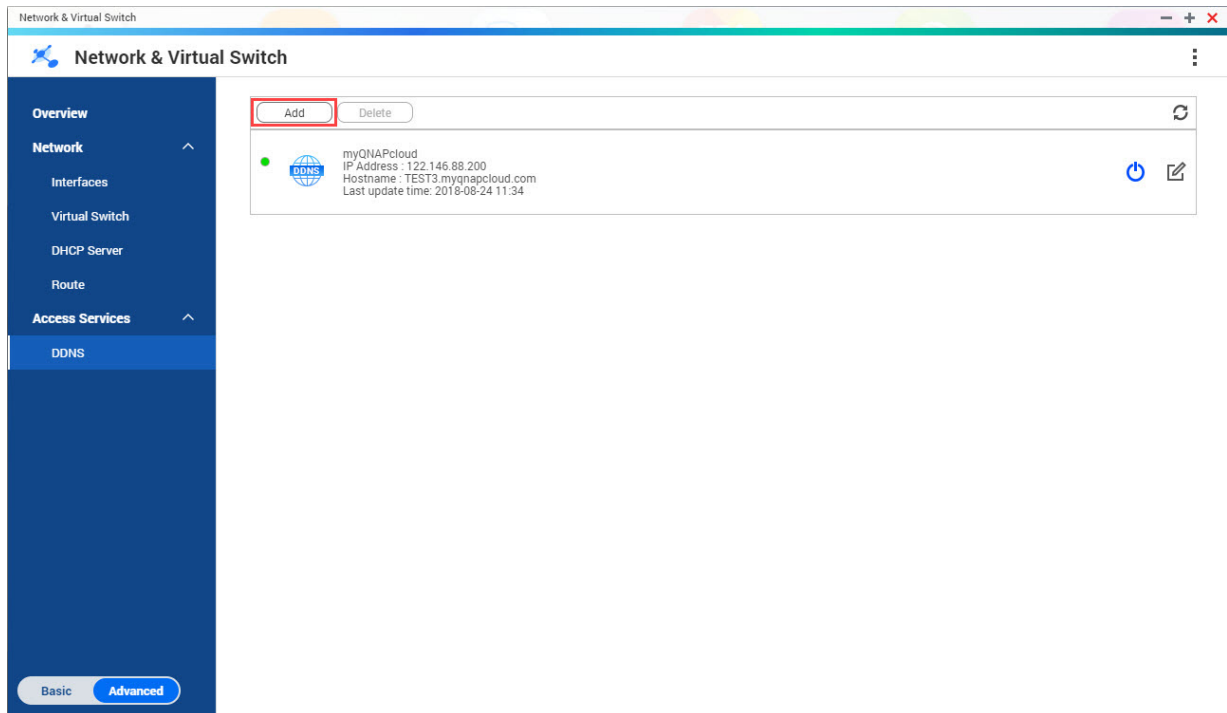
Network & Virtual Switch updates the DNS server settings.

Configuring DHCP Server Settings

The Dynamic Host Configuration Protocol (DHCP) allows devices in a TCP/UDP network to be automatically configured for the network as the device is booted. The DHCP service uses a client-server mechanism, wherein a DHCP server stores and manages network configuration information for clients and offers necessary data when a client requests the information. The information includes the IP address and subnet mask, the IP address of the default gateway, the DNS server IP address, and the IP lease information.

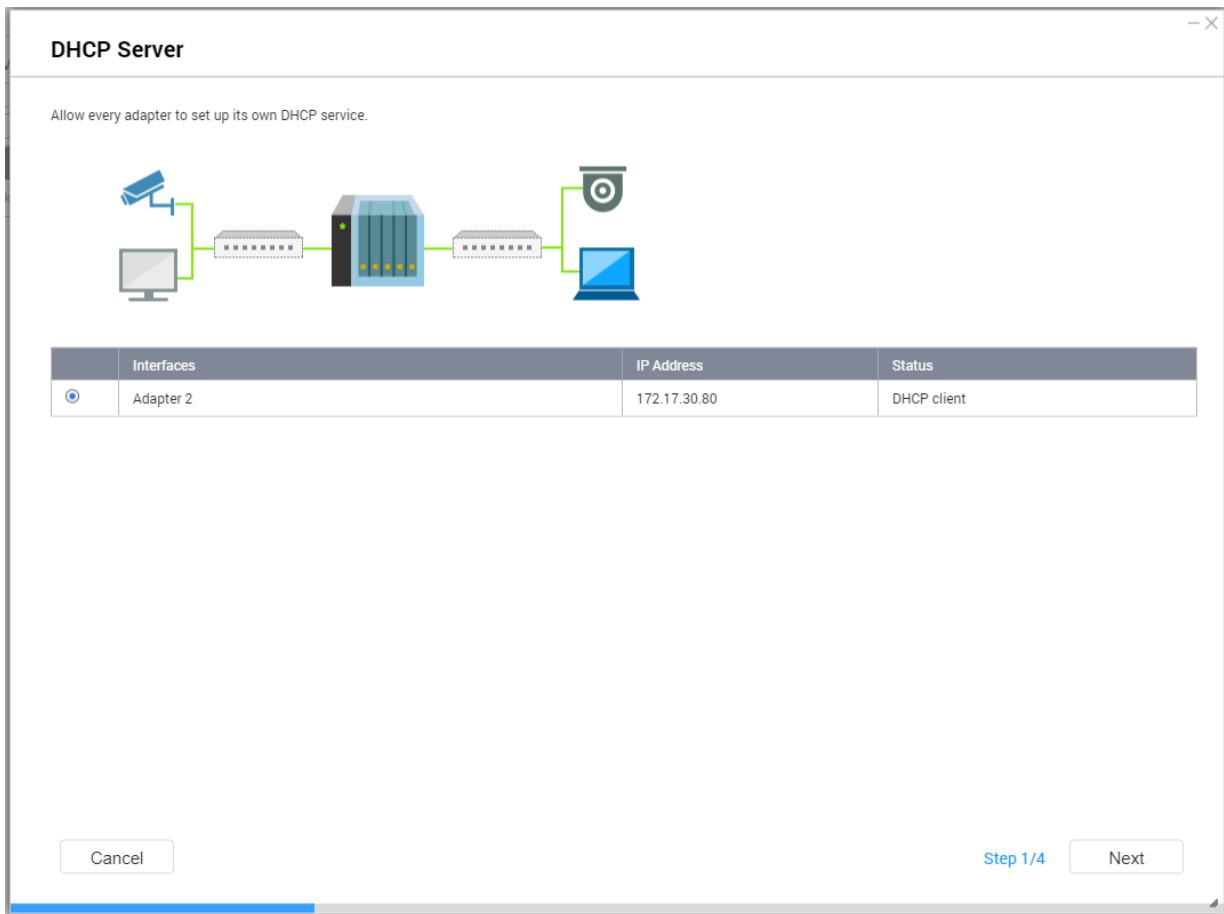
 **Important**
 Do not create a new DHCP server if one already exists on the network. Enabling multiple DHCP servers on the same network can cause IP address conflicts or network access errors.

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > DHCP Server** .
3. Click **Add**.

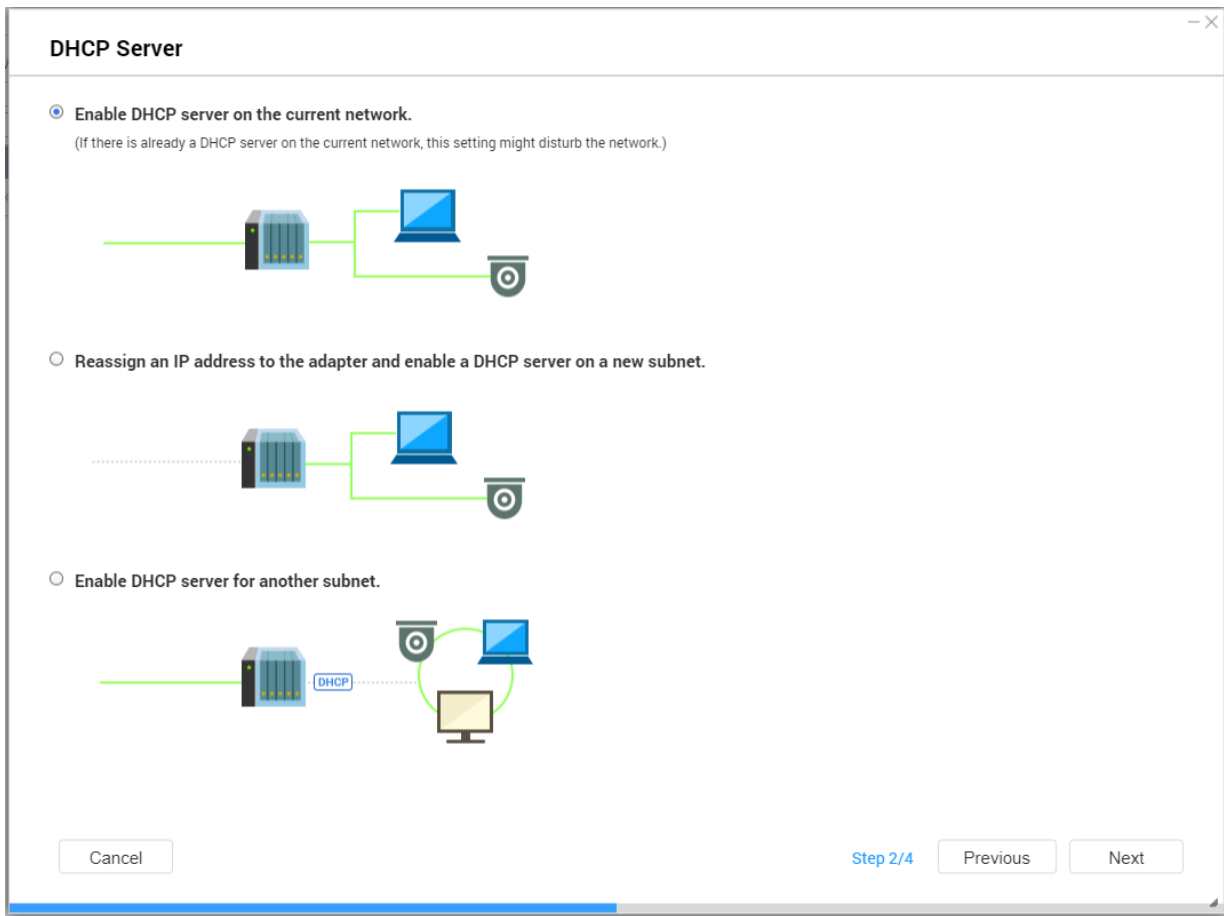


The **DHCP Server** window opens.

4. Select an interface.



5. Click **Next**.
6. Select the network environment for the DHCP server.



Option	Description
Enable DHCP server on the current network.	<ul style="list-style-type: none"> • The adapter keeps the existing IP address and subnet mask. • The DHCP server shares the subnet mask with the adapter and is assigned the next available IP address.
Reassign an IP address to the adapter and enable a DHCP server on a new subnet.	<ul style="list-style-type: none"> • The adapter is assigned a new IP address and subnet mask. • The DHCP server uses a different subnet mask and IP address.
Enable DHCP server for another subnet.	<ul style="list-style-type: none"> • The adapter keeps the existing IP address and subnet mask. • The DHCP server uses a different subnet mask and IP address.

7. Click **Next**.

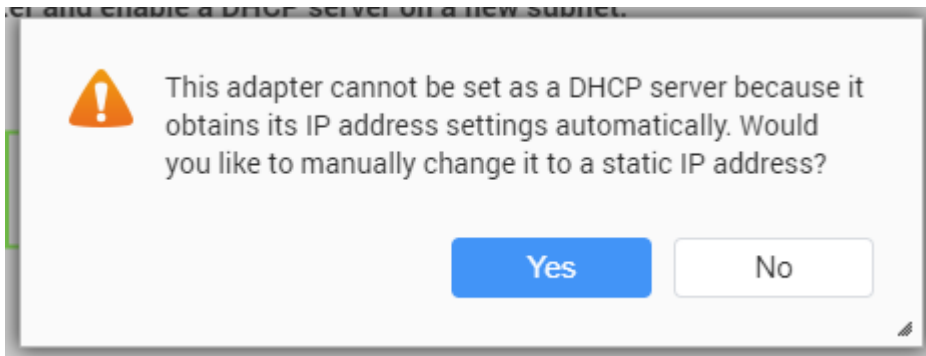
8. Configure a static IP address for the adapter.



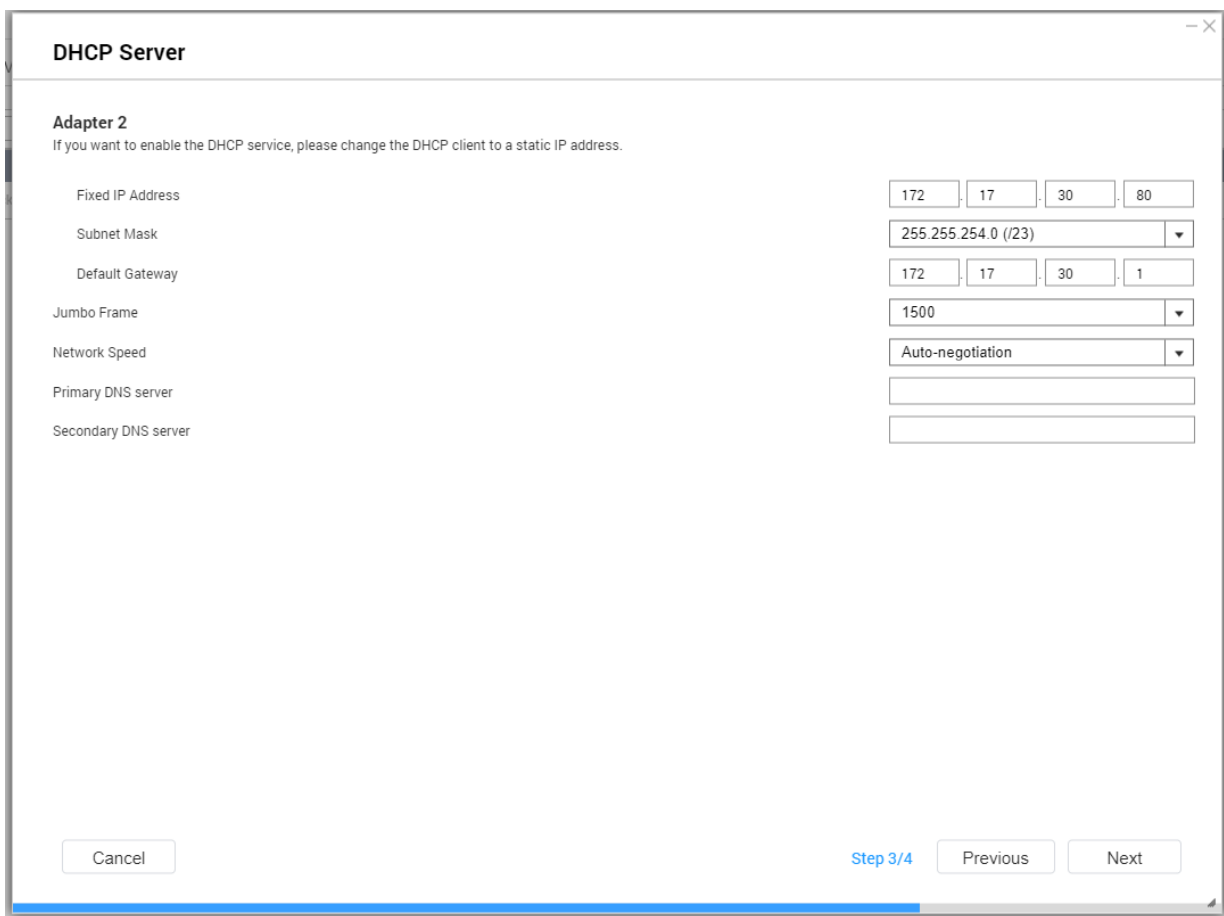
Important


A static IP address must be configured when creating a DHCP server.




a. Click **Yes**.



b. Configure IP address settings.

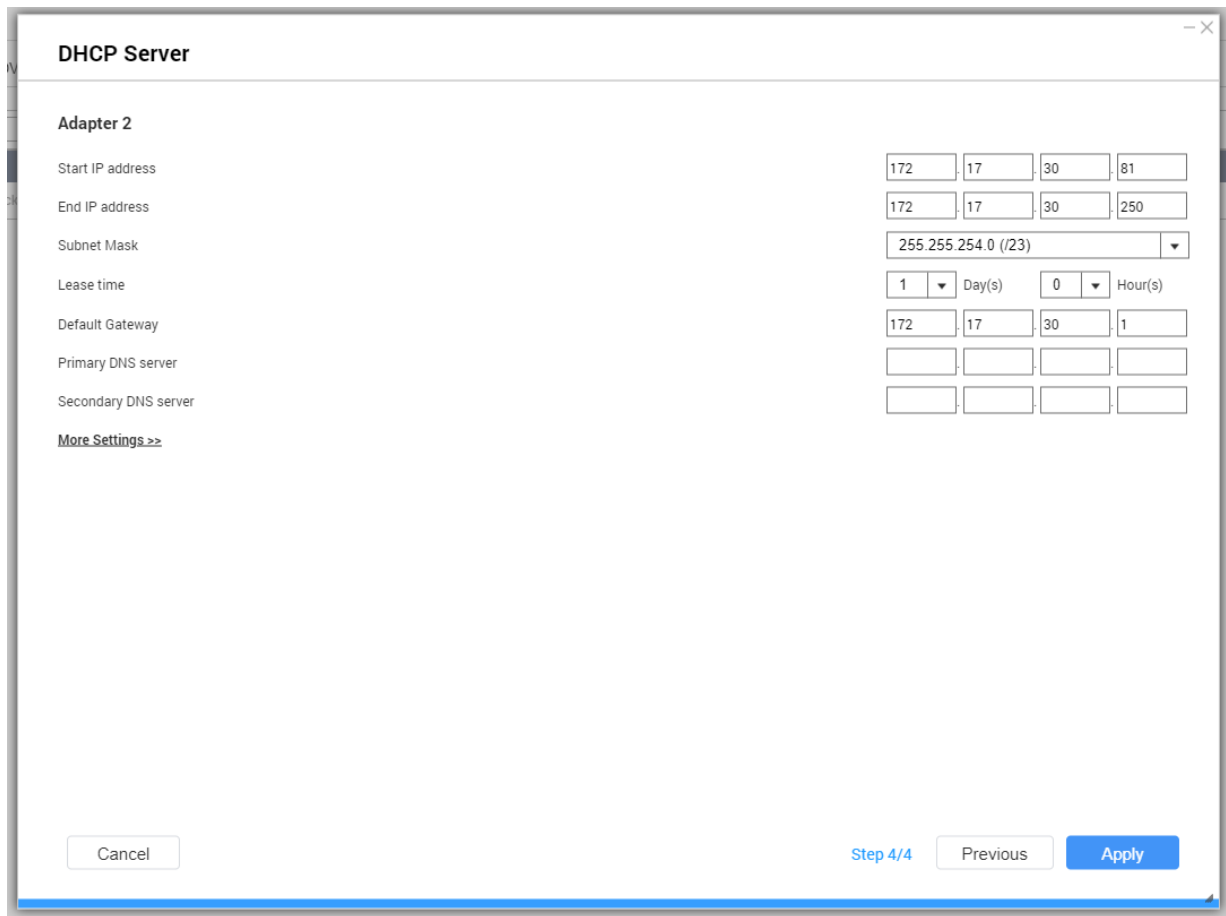


Setting	Description
Fixed IP Address	Specify a fixed IP address.  Tip Examine your network setup for guidance on how to best configure these settings.
Subnet Mask	Specify the subnet mask used to subdivide your IP address.
Default Gateway	Specify the IP address of the default gateway for the adapter.




Setting	Description
Jumbo Frame	<p>Jumbo Frames are Ethernet frames that are larger than 1500 bytes. They are designed to enhance Ethernet networking throughput, and to reduce CPU usage when transferring large files. QuTS hero supports the following Jumbo Frame sizes:</p> <ul style="list-style-type: none"> • 1500 bytes (default) • 4074 bytes • 7418 bytes • 9000 bytes <p> Important</p> <ul style="list-style-type: none"> • Jumbo Frames are only supported by certain NAS models. • Using Jumbo Frames requires a network speed of 1000 Mbps or faster. All connected network devices must enable Jumbo Frames and use the same MTU size.
Network Speed	<p>Specify the speed at which the adapter will operate.</p> <p> Tip Auto-negotiation will automatically detect and set the transfer rate.</p>
Primary DNS Server	Assign an IP address for the primary DNS server.
Secondary DNS server	<p>Assign an IP address for the secondary DNS server.</p> <p> Important QNAP recommends specifying at least one DNS server to allow URL lookups.</p>

c. Click **Next**.

9. Configure DHCP settings.



Setting	Description
Start IP Address	Specify the starting IP address in a range allocated to DHCP clients.
End IP Address	Specify the ending IP addresses in a range allocated to DHCP clients.
Subnet Mask	Specify the subnet mask used to subdivide your IP address.
Lease Time	Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires.
Default Gateway	Specify the IP address of the default gateway for the DHCP server.
Primary DNS Server	Specify a DNS server for the DHCP server.
Secondary DNS Server	Specify a secondary DNS server for the DHCP server. <div style="display: flex; align-items: center;"> <div> <p>Important</p> <p>QNAP recommends specifying at least one DNS server to allow URL lookups.</p> </div> </div>
WINS Server	Specify the WINS server IP address. <div style="display: flex; align-items: center;"> <div> <p>Tip</p> <p>Windows Internet Naming Service (WINS) converts computer names (NetBIOS names) to IP addresses, allowing Windows computers on a network to easily find and communicate with each other.</p> </div> </div>

Setting	Description
DNS Suffix	Specify the DNS suffix.  Tip The DNS suffix is used for resolving unqualified or incomplete host names.
TFTP Server	Specify the public IP address for the TFTP server.  Tip QuTS hero supports both PXE and remote booting of devices.
Boot File	Specify location and file name of the TFTP server boot file.  Tip QuTS hero supports both PXE and remote booting of devices.



10. Click **Apply**.


Network & Virtual Switch adds the DHCP server.

Adding DHCP Clients to a DHCP Server

A DHCP client is a network device using DHCP service to obtain network configuration parameters such as an IP address from a DHCP server. When a DHCP client sends a broadcast message to locate a DHCP server, the DHCP server provides configuration parameters (IP address, MAC address, domain name, and a lease for the IP address) to the client.

The following table describes the two types of DHCP clients employed in Network & Virtual Switch.

DHCP Client	Description
Physical Adapter DHCP Client	Enabling a DHCP IPv4 address allows the device to automatically acquire an IPv4 address for a specific physical adapter from a DHCP server. The physical adapter is assigned an IP address by the DHCP server for a predefined lease time.  Note For details on obtaining a DHCP provided IP address, see Configuring IPv4 Settings .
Virtual Switch DHCP Client	Virtual switches allow virtual machines to obtain IP-related configurations automatically from an external DHCP server. The virtual switch obtains the IP address from the DHCP server through the connected physical adapter on the device.  Note <ol style="list-style-type: none"> 1. A virtual switch configured with an automatic DHCP IP address cannot utilize the NAT and DHCP server functions. 2. Virtual switches cannot automatically acquire the IP address of the physical adapter unless the virtual switch has been configured to connect to a physical adapter in Network > Virtual Switch.

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > DHCP Server** .
3. Identify a DHCP server.
4. Under Actions, click  .
The **DHCP Client Table** window appears.
5. Click **Add Reserved IP**.
The **Add Reserved IP** window appears.
6. Configure the DHCP client information.

Setting	User Action
Device Name	Specify a device name for the DHCP client.
IP Address	Specify the IP address of the DHCP client.
MAC Address	Specify the MAC address of the DHCP client.

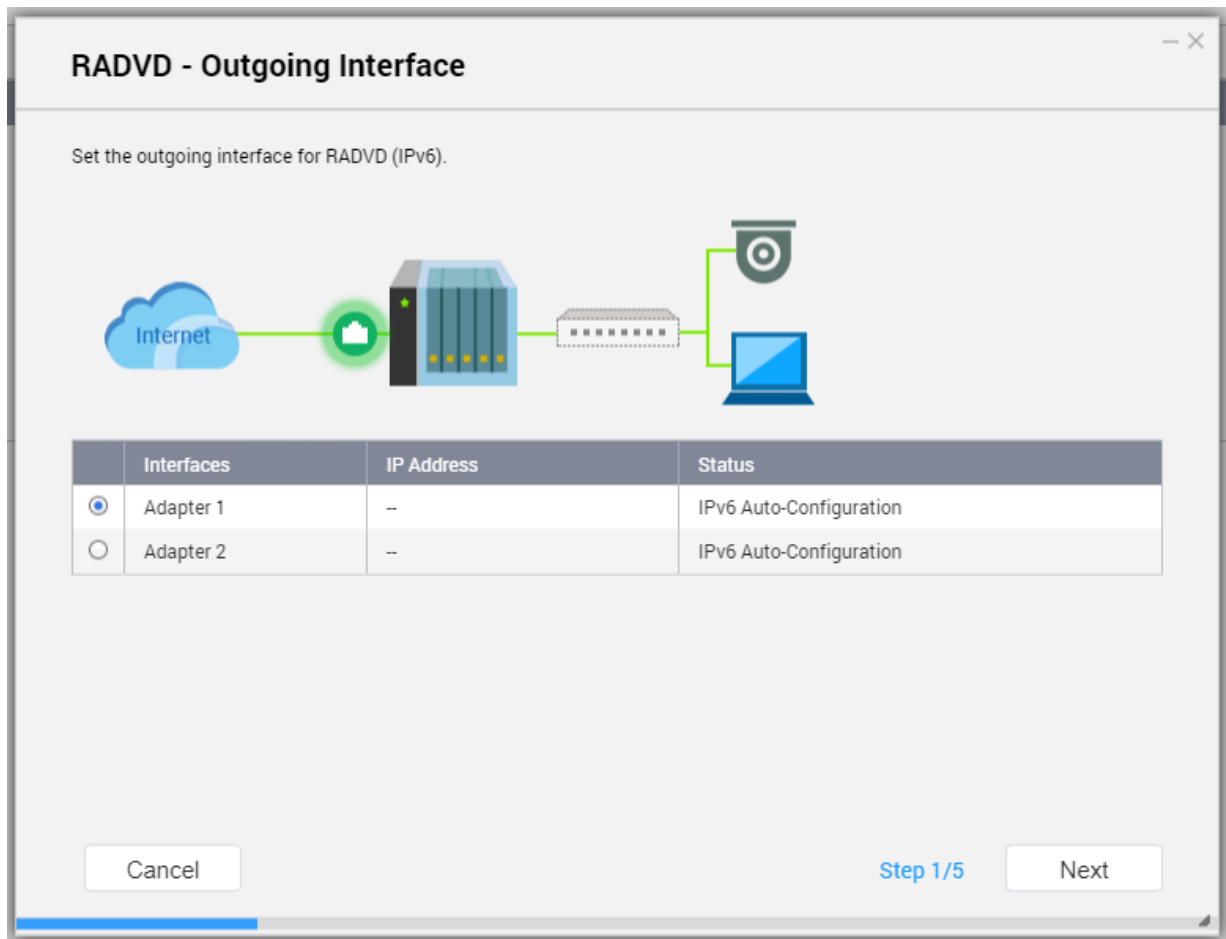
7. Click **Apply**.

Network & Virtual Switch adds the DHCP client.

Configuring RADVD Server Settings

This **RADVD** screen controls the creation and management of Router Advertisement Daemon (RADVD) servers. This service sends messages required for IPv6 stateless auto-configuration. This service periodically sends router advertisement (RA) messages to devices on the local network, and can also send a router solicitation messages when requested from a connected node.

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > DHCP Server** .
3. Go to the **RADVD** tab.
4. Click **Add**.
The **RADVD - Outgoing Interface** window opens.
5. Select the outgoing interface.



6. Click **Next**.

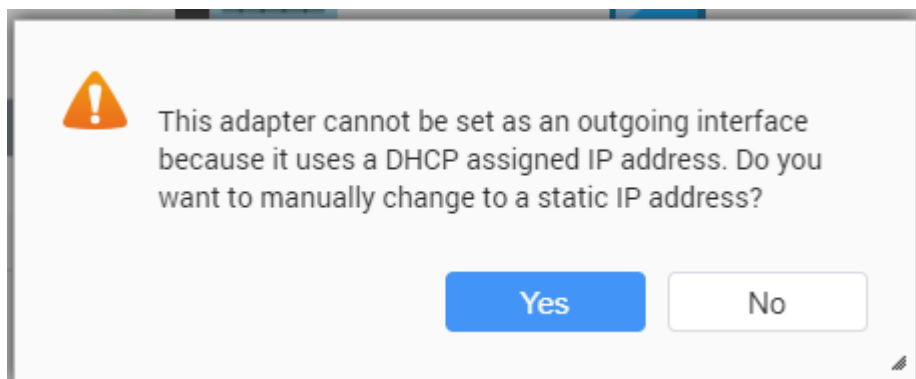
7. Configure a static IP address for the adapter.



Important

A static IP address must be configured when creating a RADVD server.

a. Click **Yes**.



b. Optional: Configure Static IP address settings.

RADVD - Outgoing Interface

Adapter 1
A static IP must be configured to enable RADVD.

Fixed IP Address

Prefix Length

Default Gateway

Primary DNS server

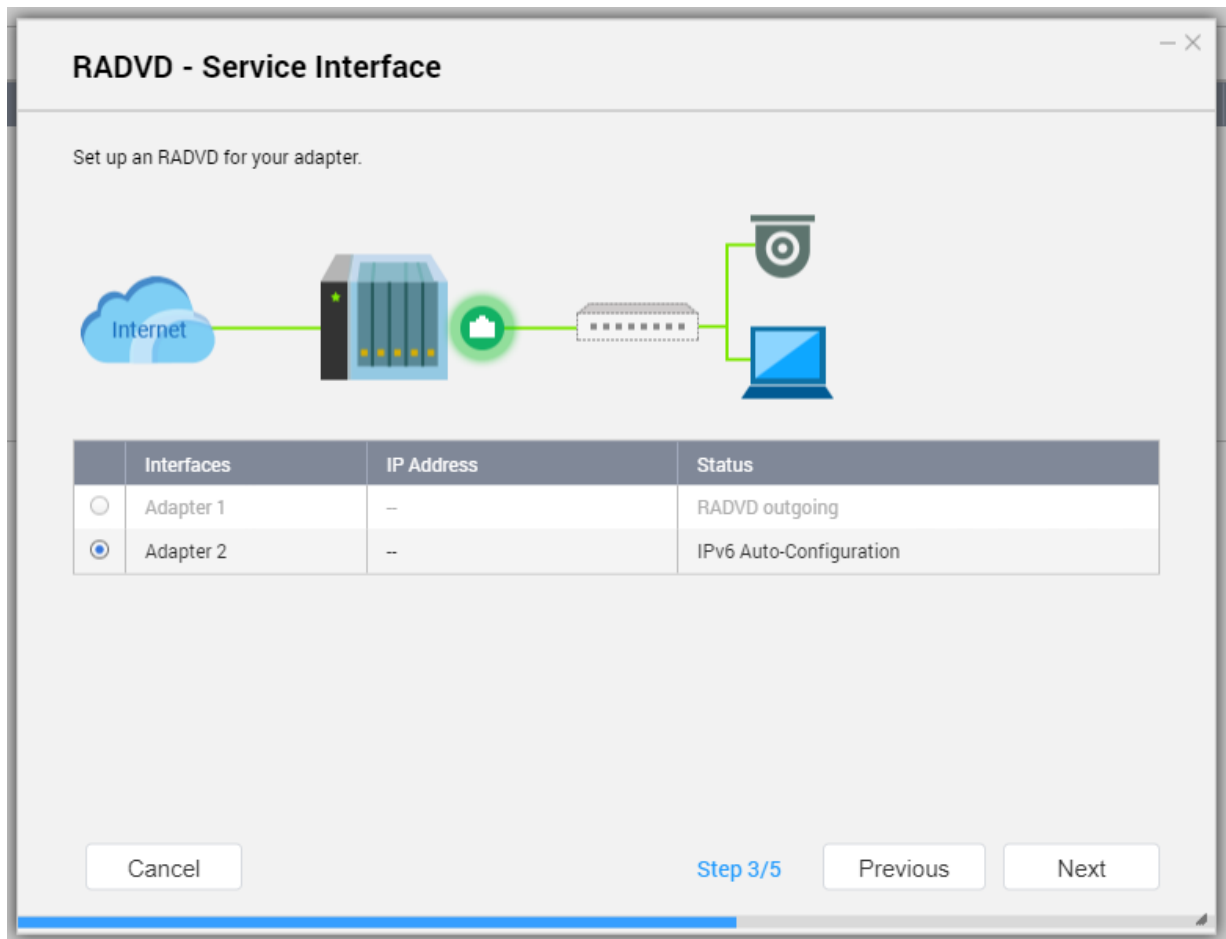
Secondary DNS server

Step 2/5

Setting	Description
Fixed IP Address	Specify a fixed IP address. <div style="display: flex; align-items: center;"> <div> <p>Tip Examine your network setup for guidance on how to best configure these settings.</p> </div> </div>
Prefix Length	Specify the prefix length for the adapter. <div style="display: flex; align-items: center;"> <div> <p>Tip Obtain the prefix and the prefix length information from your ISP.</p> </div> </div>
Default Gateway	Specify the IP address of the default gateway for the DHCP server.
Primary DNS Server	Assign an IP address for the primary DNS server.
Secondary DNS server	Assign an IP address for the secondary DNS server. <div style="display: flex; align-items: center;"> <div> <p>Important QNAP recommends specifying at least one DNS server to allow URL lookups.</p> </div> </div>

c. Click **Next**.

8. Select a second adapter for the RADVD service interface.



9. Click **Next**.

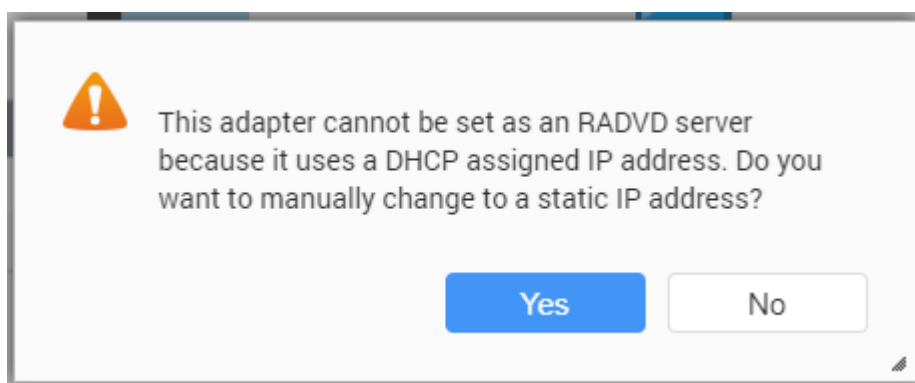
10. Optional: Configure a static IP address for the second RADVD adapter.



Important

Creating an RADVD interface requires that the adapter use a static IP address. If the adapter already uses a static IP address, skip this step.

a. Click **Yes**.



b. Configure Static IP address settings.

RADVD - Service Interface - X

Adapter 2
A static IP must be configured to enable RADVD.

Fixed IP Address

Prefix Length ▼

Default Gateway

Primary DNS server

Secondary DNS server

Cancel
Step 4/5
Previous
Next

Setting	Description
Fixed IP Address	Specify a fixed IP address. <div style="display: flex; align-items: center;"> <div> <p>Tip Examine your network setup for guidance on how to best configure these settings.</p> </div> </div>
Prefix Length	Specify the prefix length for the adapter. <div style="display: flex; align-items: center;"> <div> <p>Tip Obtain the prefix and the prefix length information from your ISP.</p> </div> </div>
Default Gateway	Specify the IP address of the default gateway for the adapter.
Primary DNS Server	Specify the DNS server address.
Secondary DNS server	Specify the DNS server address. <div style="display: flex; align-items: center;"> <div> <p>Important QNAP recommends specifying at least one DNS server to allow URL lookups.</p> </div> </div>

c. Click **Apply**.

11. Configure the RADVD server settings.

RADVD Service - X

Adapter 2

Prefix




Prefix Length ▼

Lease time ▼ Hour(s)

Primary DNS server

Secondary DNS server

Cancel
Step 5/5
Previous
Apply

Setting	Description
Prefix	<p>Specify the routing prefix for the adapter.</p> <p> Tip Examine your network setup for guidance on how to best configure these settings.</p>
Prefix Length	<p>Specify the prefix length for the adapter.</p> <p> Tip Obtain the prefix and the prefix length information from your ISP.</p>
Lease Time	<p>Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires.</p>
Primary DNS Server	<p>Specify the DNS server address.</p>
Secondary DNS server	<p>Specify the DNS server address.</p> <p> Important QNAP recommends specifying at least one DNS server to allow URL lookups.</p>

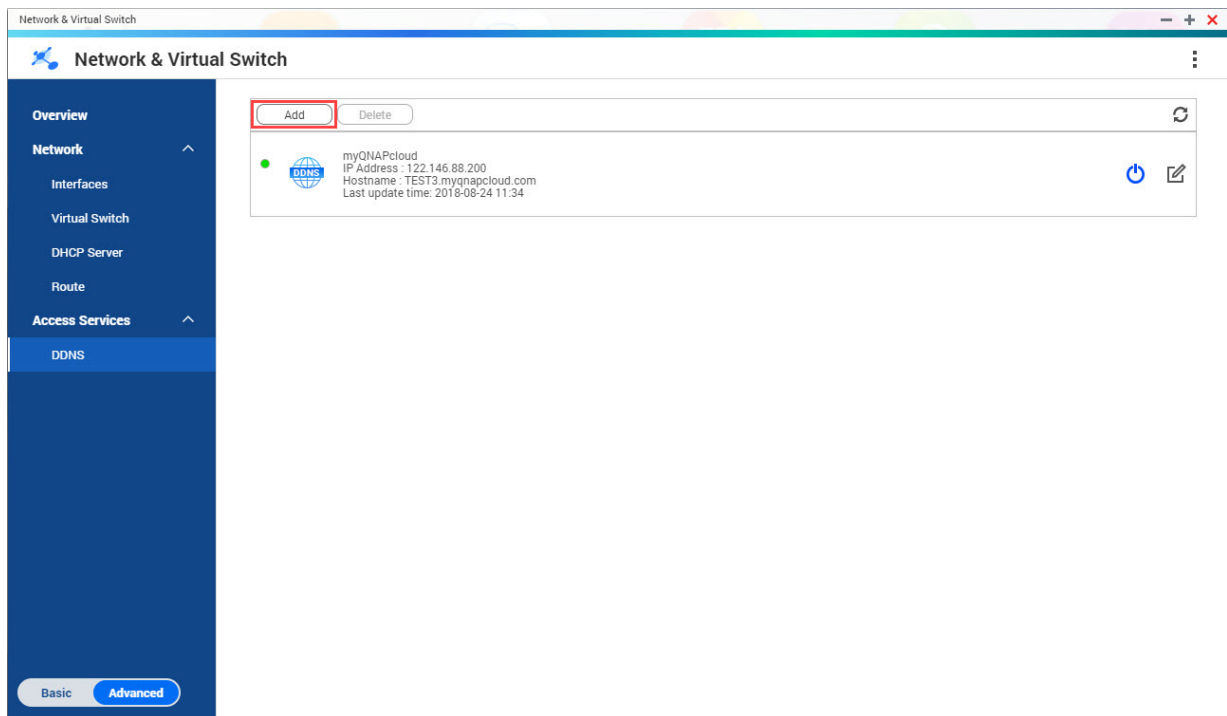
12. Click **Apply**.

Network & Virtual Switch adds the RADVD server.

Configuring DDNS Service Settings

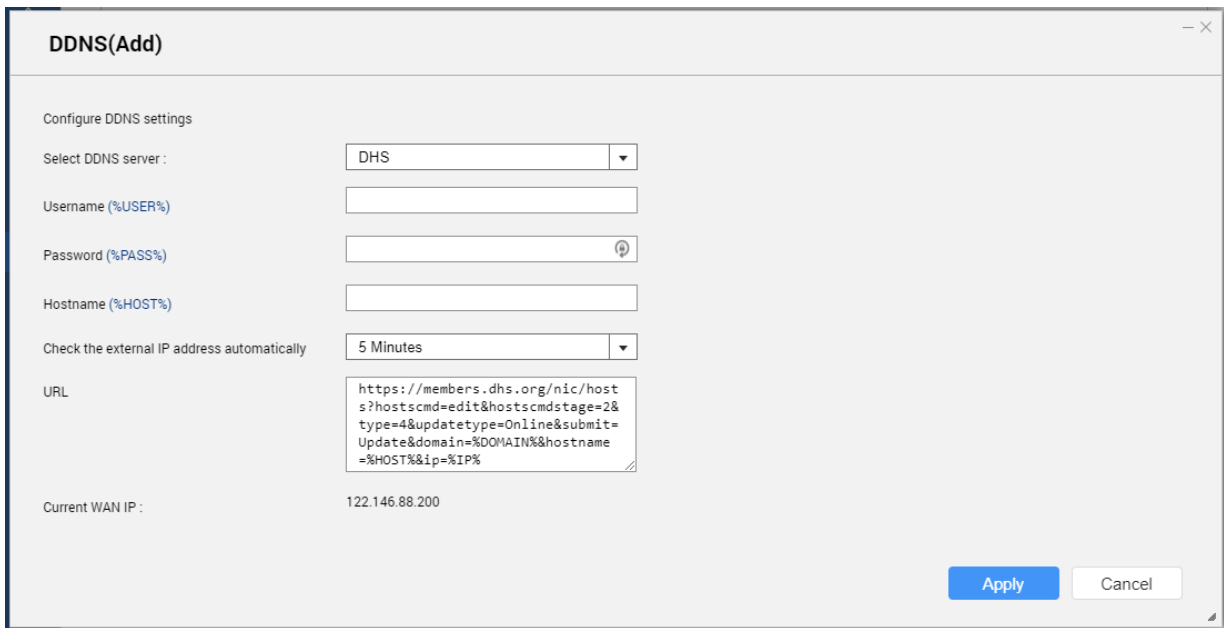
This **DDNS** screen controls the management of Dynamic Domain Name System (DDNS) services. DDNS allows access to the NAS from the internet using a domain name rather than an IP address.

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Access Services > DDNS** .
3. Click **Add**.



The **DDNS (Add)** window opens.

4. Configure the DDNS settings.



Setting	Description
Select DDNS server	Select the DDNS service provider.
Username	Specify the username for the DDNS service.
Password	Specify the password for the DDNS service.
Hostname	Specify the hostname or domain name for the DDNS service.
Check the External IP Address	Specify how often to update the DDNS record.

5. Click **Apply**.

Network & Virtual Switch adds the DDNS server service.

LAN Switching Configuration

LAN switching enables users to resolve bandwidth issues by increasing the efficiency of LANs using VLAN and port trunking technologies.


Configuring VLAN Settings

A virtual LAN (VLAN) groups multiple network devices together and limits the broadcast domain. Members of a VLAN are isolated and network traffic is only sent between the group members. You can use VLANs to increase security and flexibility while also decreasing network latency and load.




Important

When using both port trunking and a VLAN, port trunking must be configured first.

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Identify the adapter that you want to configure, then click  .

4. Select **Add VLAN**.
The **Add VLAN** window opens.

5. Specify a VLAN ID.

 **Important**
The VLAN ID must be between 1 and 4094.

6. Specify a description for the VLAN.
7. Select one of the following options.

Option	Steps
Automatically obtain the IP address using DHCP	Select Obtain IP address settings automatically via DHCP .
Use a static IP address	<ol style="list-style-type: none"> Select Use static IP address Specify a fixed IP address. Select a subnet mask. Specify the default gateway.

8. Click **Apply**.

Network & Virtual Switch adds the VLAN.

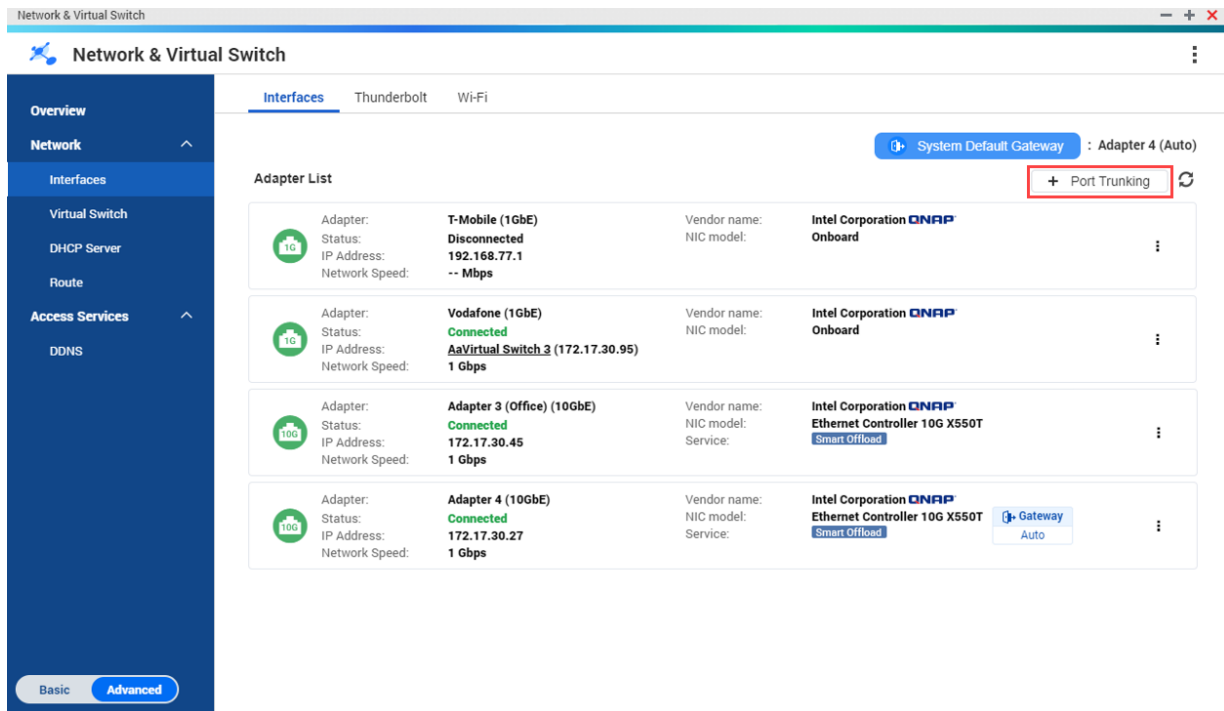
Configuring Port Trunking Settings

Port trunking combines two or more Ethernet interfaces for increased bandwidth, load balancing and fault tolerance (failover). Load balancing is a feature that distributes workloads evenly across multiple Ethernet interfaces for higher redundancy. Failover ensures that a network connection remains available even if a port fails.

 **Important**

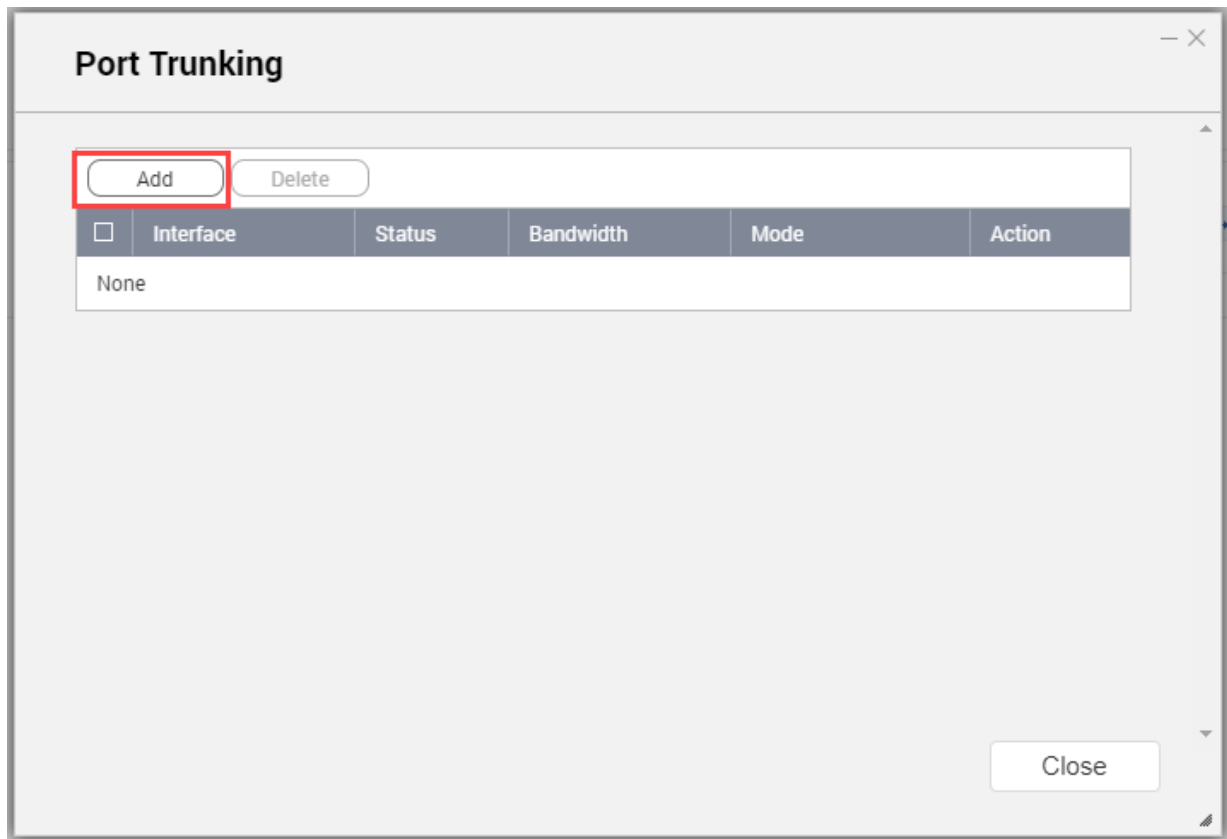
Before configuring port trunking settings, ensure at least two network interfaces are connected to the same switch.

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Click **Port Trunking**.



The **Port Trunking** window opens.

4. Click **Add**.



The **Port Trunking (Add)** window opens.

5. Select two or more network interfaces to add to the trunking group.

Port Trunking(Add)

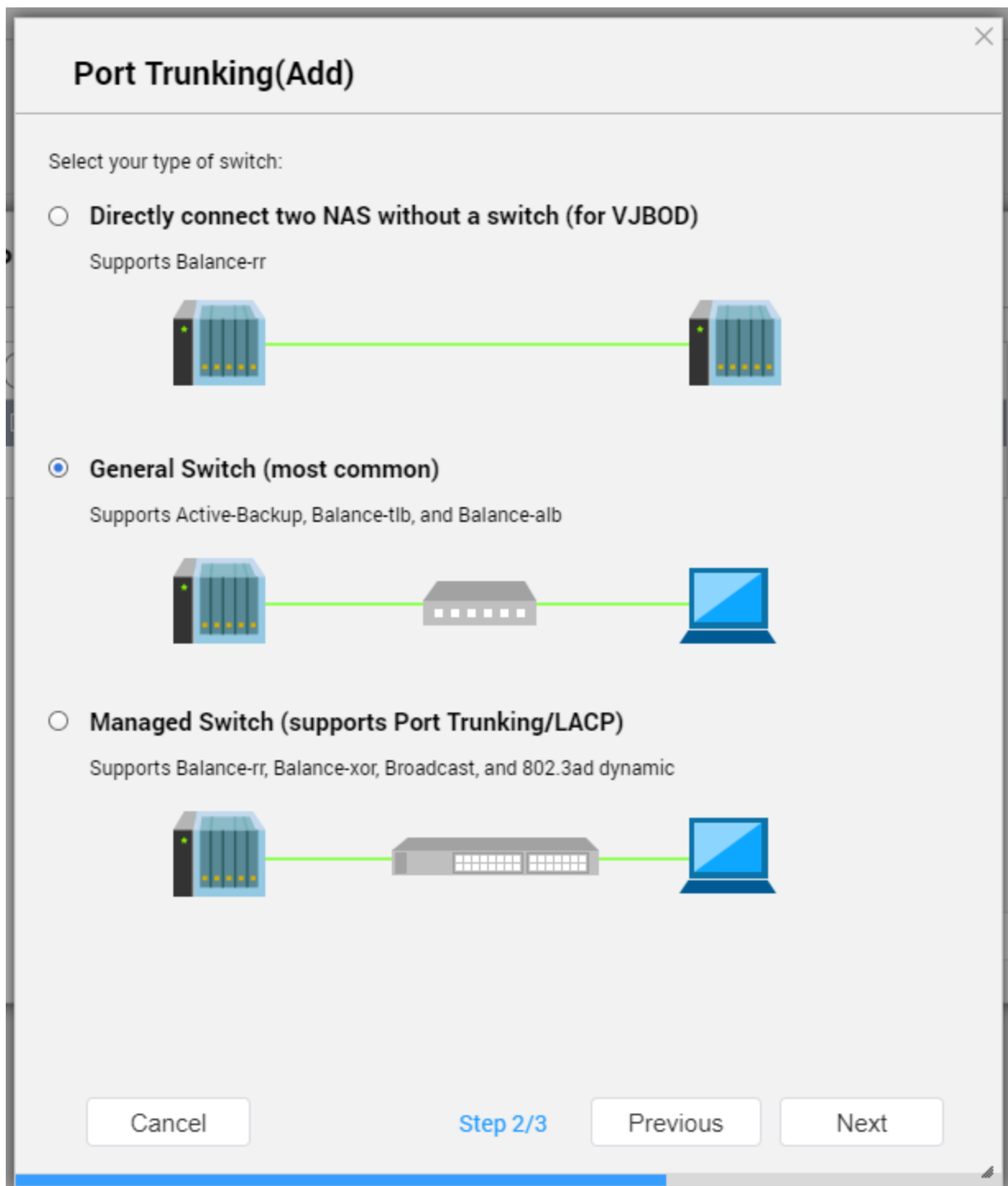
Select the port trunking membership and mode. Please note that incompatible mode settings may affect overall performance or cause the network interface to hang. For more information, please click [here](#).

<input checked="" type="checkbox"/>	Interface	Status	Speed
<input checked="" type="checkbox"/>	Adapter 1	<input type="radio"/>	-- Mbps
<input checked="" type="checkbox"/>	Adapter 2	<input checked="" type="radio"/>	1 Gbps

Warn me if a network cable is disconnected from the trunking group

Step 1/3

6. Click **Next**.
7. Select a switch type.



8. Click **Next**.

9. Select a trunking mode.

Port Trunking(Add) ✕

Please choose a trunking mode:

Failover
Provides failover to ensure that the network connection will remain available even if a port fails.

Active-Backup
Only one NIC in the bond is active. Another NIC will become active if the first one fails.

Load balancing & Failover
Increases the bandwidth to maintain the transmission speed for multiple clients and provides failover to ensure that the network connection will remain available even if a port fails.

Balance-tlb
The outgoing traffic is distributed according to the current load on each NIC slave (relative to its speed). The incoming traffic is received by the currently-designated NIC slave. If this receiving slave fails, another slave will take over its MAC address.

Balance-alb
Similar to Balance-tlb, but it additionally offers load balancing for incoming IPv4 traffic.

Cancel

Step 3/3

Previous

Apply



Important

Some port trunking modes must be supported by your network switches. Selecting an unsupported mode may affect network performance or cause the network interface to freeze.

Mode	Description
Fault Tolerance (Failover)	

Mode	Description
Active-Backup	All traffic is sent and received using the interface that was first added to the trunking group. If this primary interface becomes unavailable, the secondary interface will become active.
Broadcast	Transmits the same network packets to all the network interface cards.
Load balancing & Failover	
Balance-tlb	Incoming traffic is received by the current interface. If the interface fails, a secondary interface takes over the MAC address of the failed interface. Outgoing traffic is distributed based on the current load for each interface relative to the interface's maximum speed.
Balance-alb	Similar to Balance-tlb, but offers additional load balancing for incoming IPv4 traffic.
Balance-rr	Transmits network packets sequentially to each network interface card in order to distribute the internet traffic among all the NICs.
Balance-xor	Transmits network packets using the Hash algorithm, which selects the same NIC slave for each destination MAC address.
802.3ad dynamic	Uses a complex algorithm to aggregate NICs and configure speed and duplex settings.


10. Click **Apply**.

Network & Virtual Switch applies the port trunking settings.

Virtual Switch Configuration

The **Virtual Switch** screen controls the configuration and management of virtual switches running on the NAS. Virtual Switches allow physical interfaces and virtual adapters to communicate with each other.

QuTS hero supports three different virtual switch modes.

Mode	Description
Basic	This mode is well-suited for most users, and requires minimal configuration of network settings.
Advanced	This mode is best-suited for power-users who need more control over the configuration of network settings.
Software-Defined Switch	This mode is suited for power-users who need to simulate an L2 physical switch.  Important Packet forwarding rates are limited when using this mode.

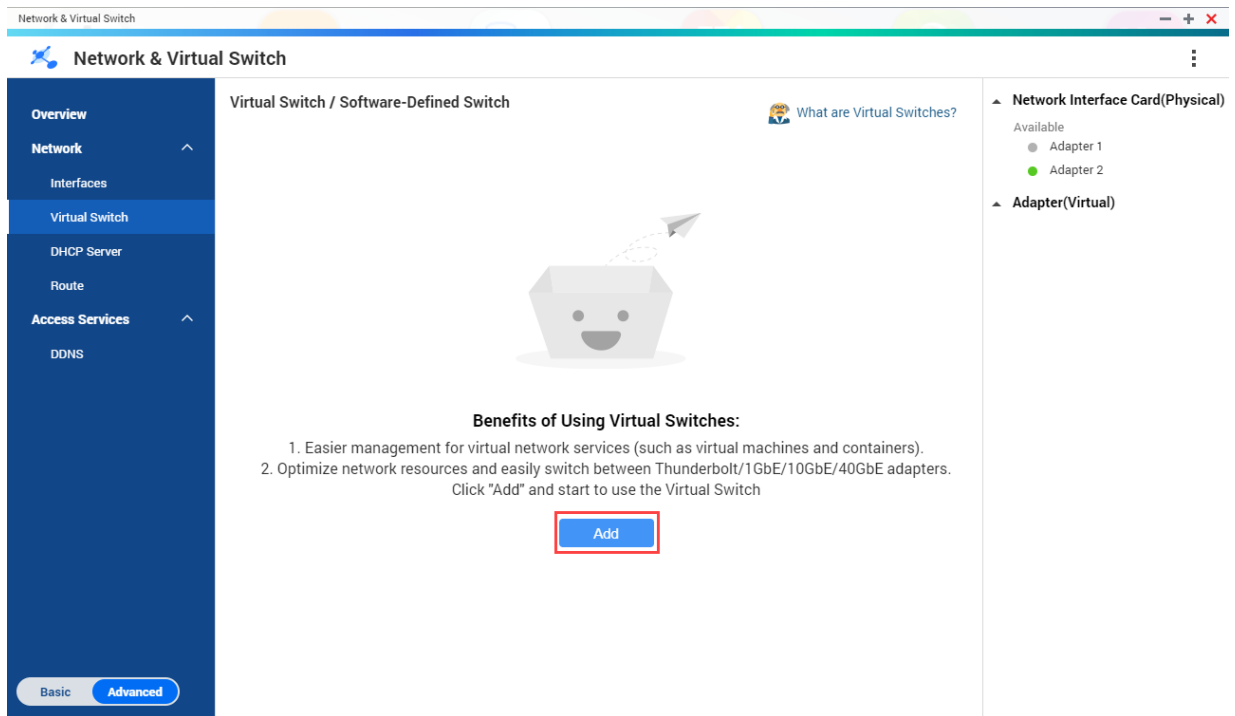


Tip

To access this page, Network & Virtual Switch must be operating in **Advanced Mode**.

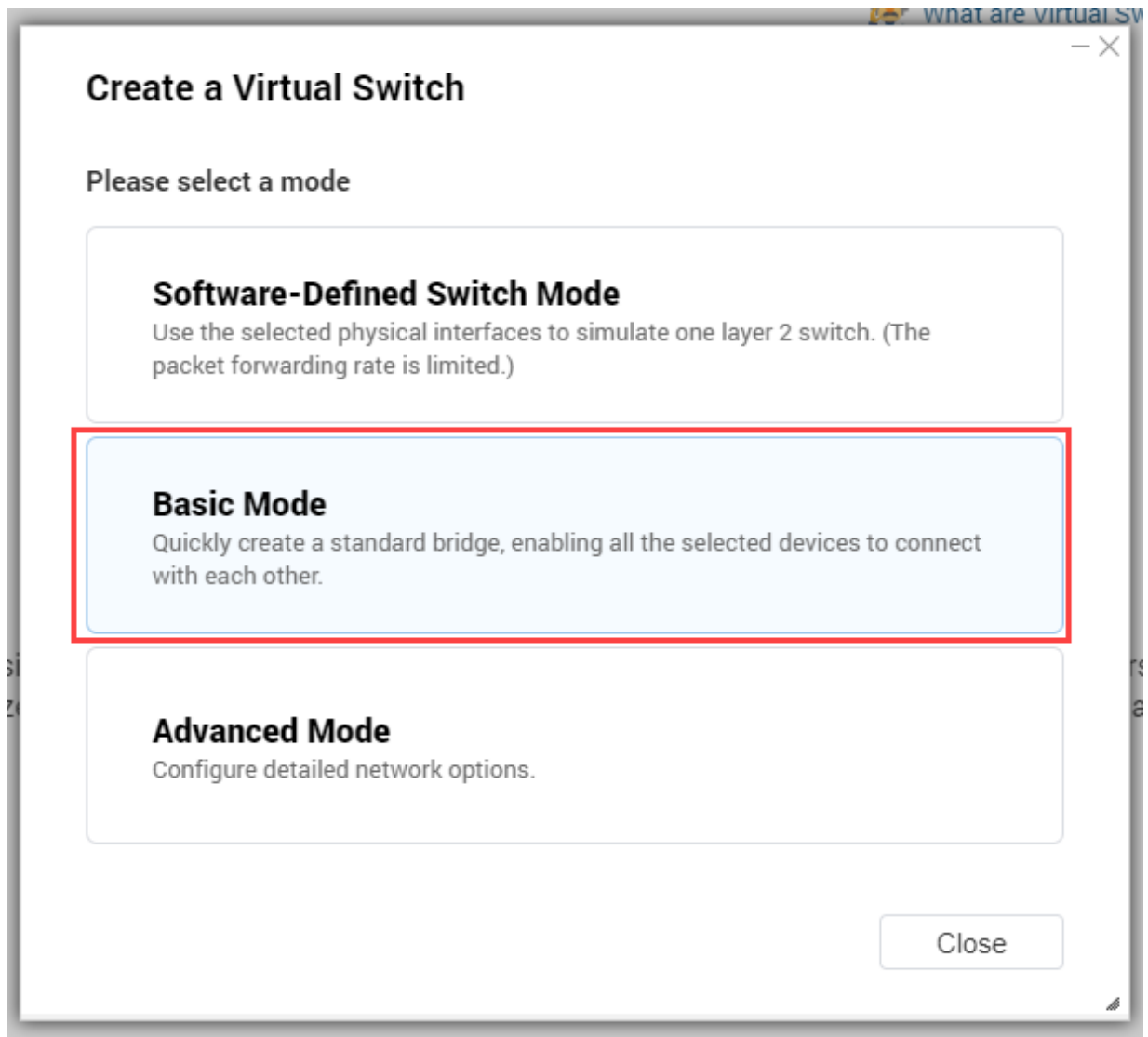
Creating a Virtual Switch in Basic Mode

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** . The **Network & Virtual Switch** window opens.
2. Go to **Network > Virtual Switch** .
3. Click **Add**.

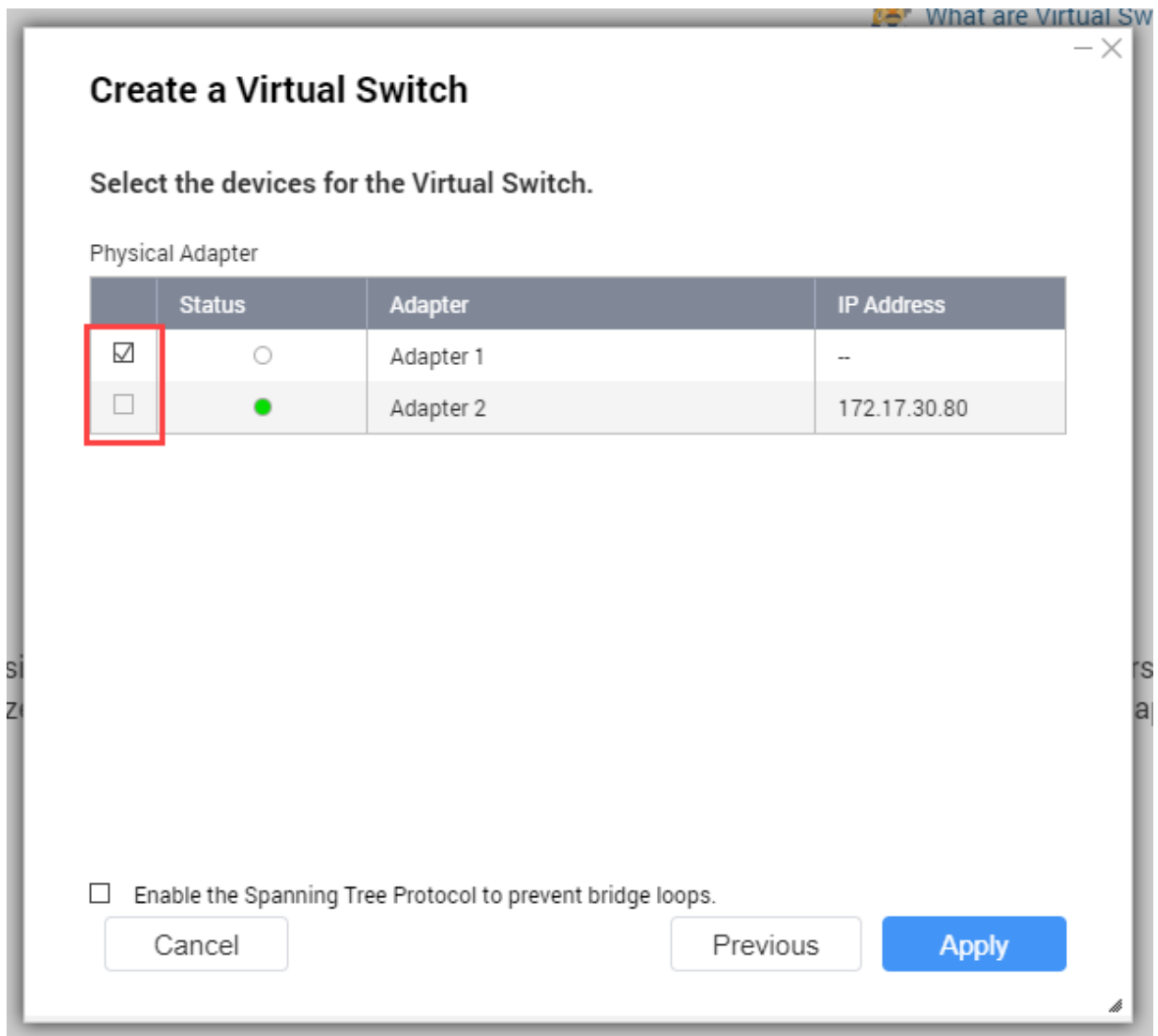


The **Create a Virtual Switch** window opens.

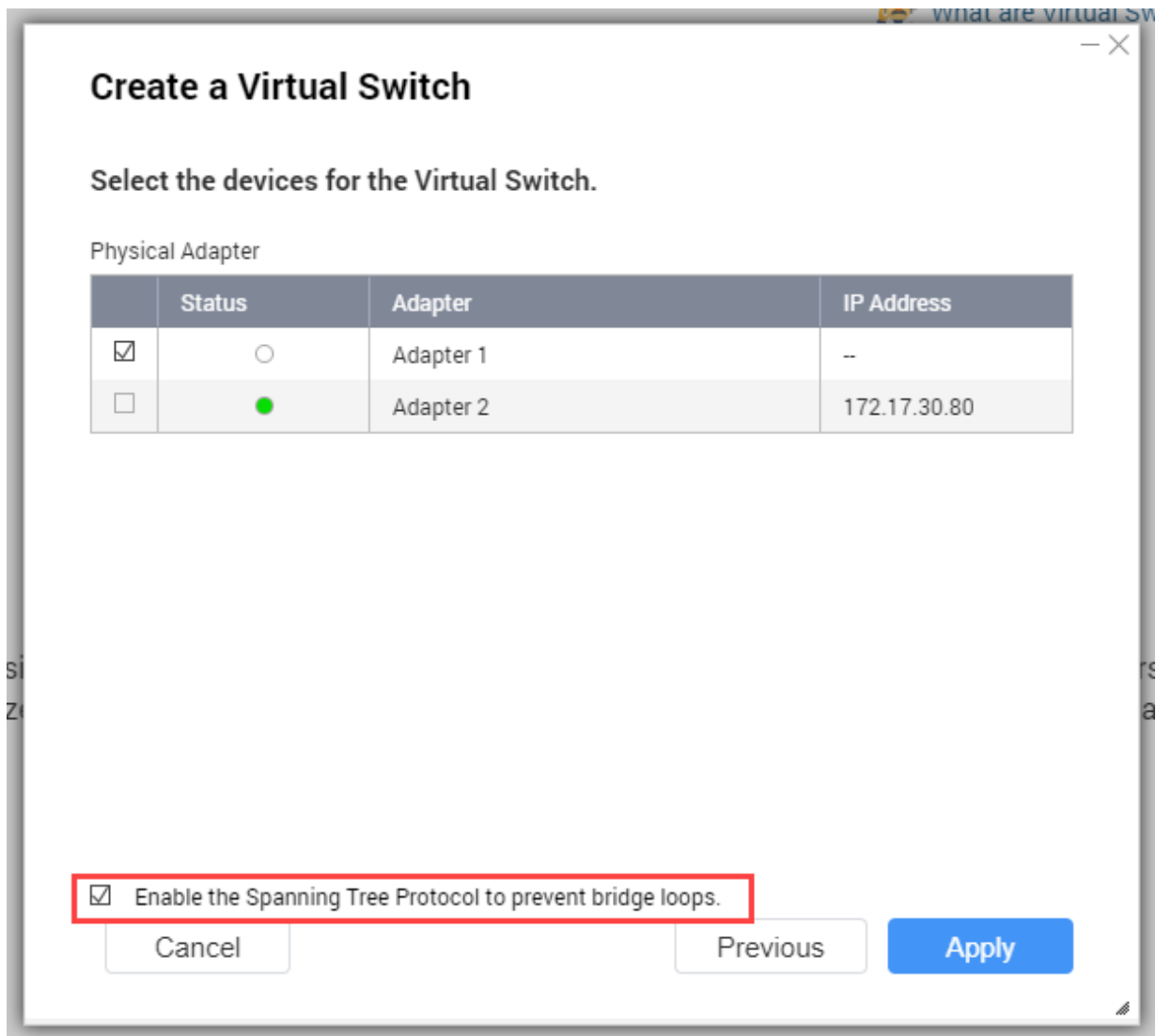
4. Select Basic Mode.



5. Select one or more adapters.



6. Optional: Select **Enable the Spanning Tree Protocol**.

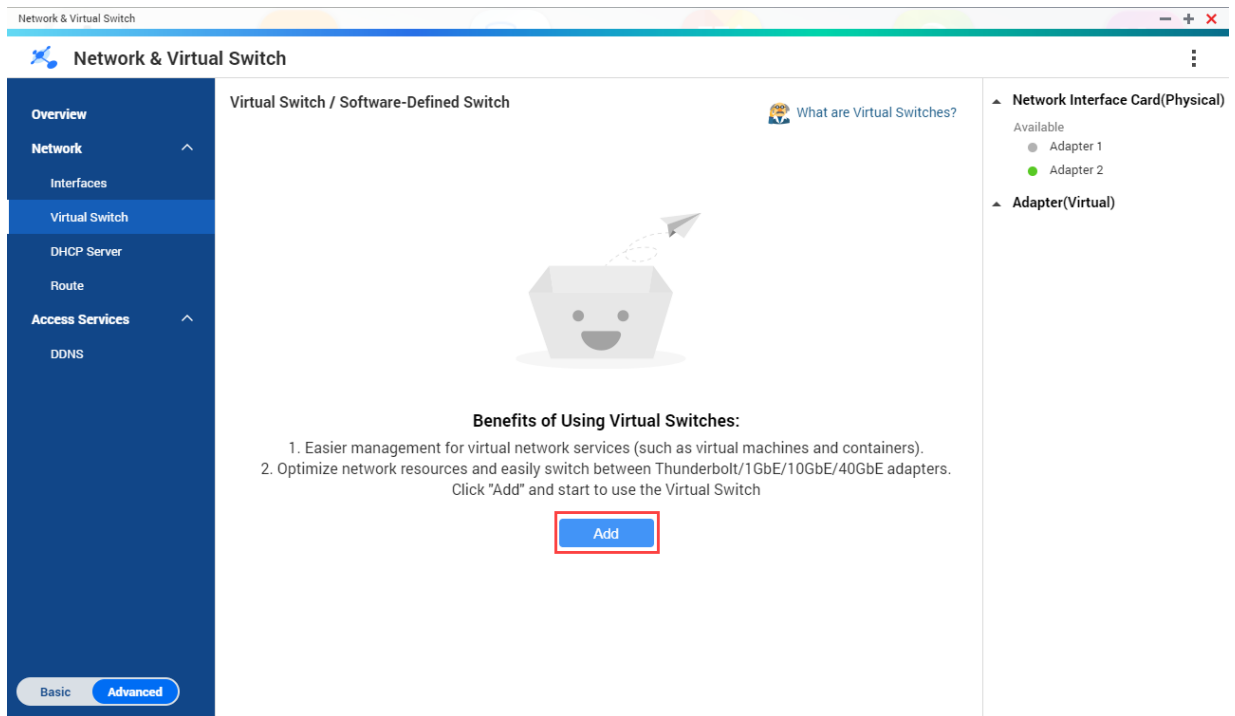
**Tip**

Enabling this setting prevents bridge loops.

7. Click **Apply**.

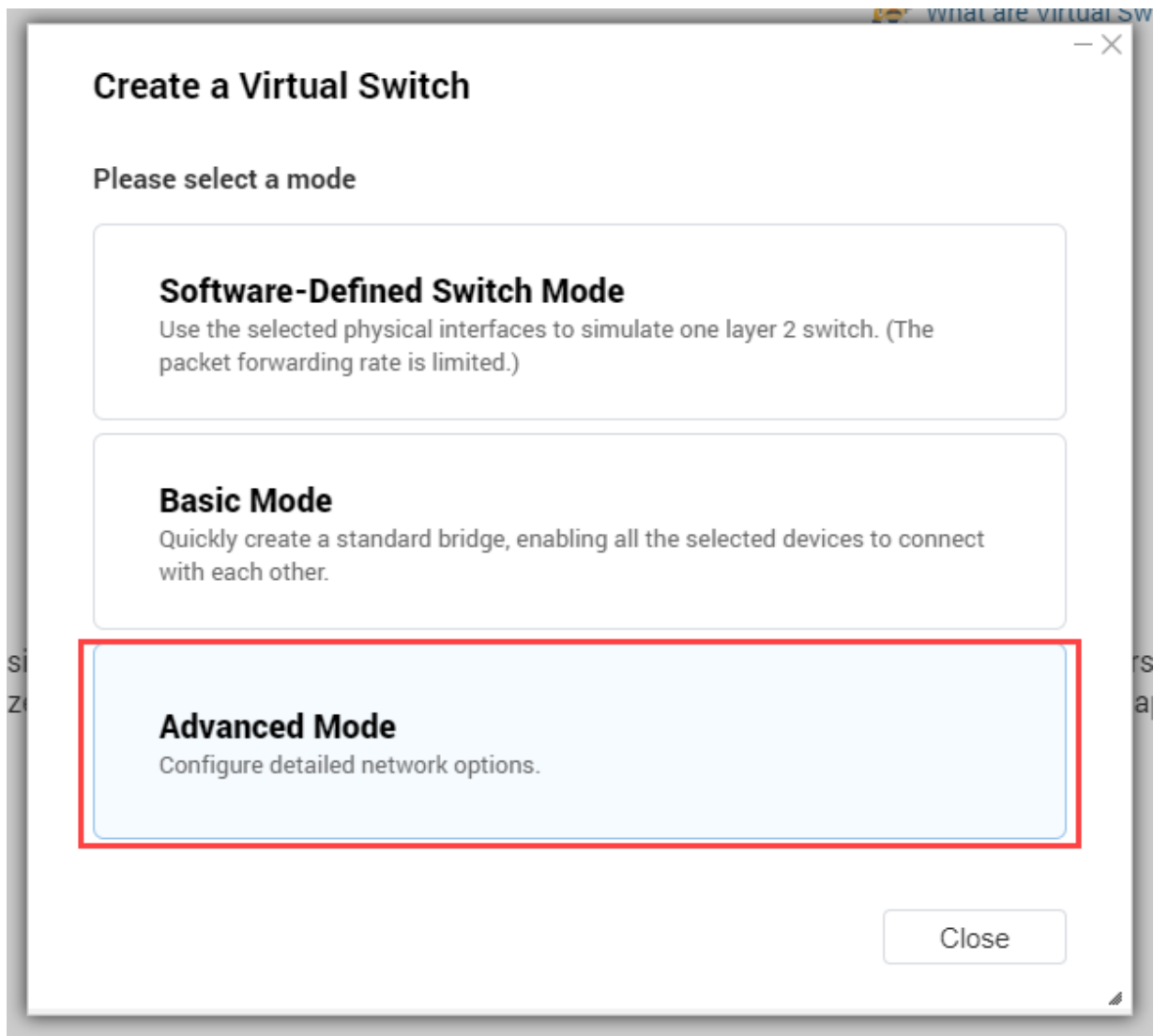
Creating a Virtual Switch in Advanced Mode

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Virtual Switch** .
3. Click **Add**.

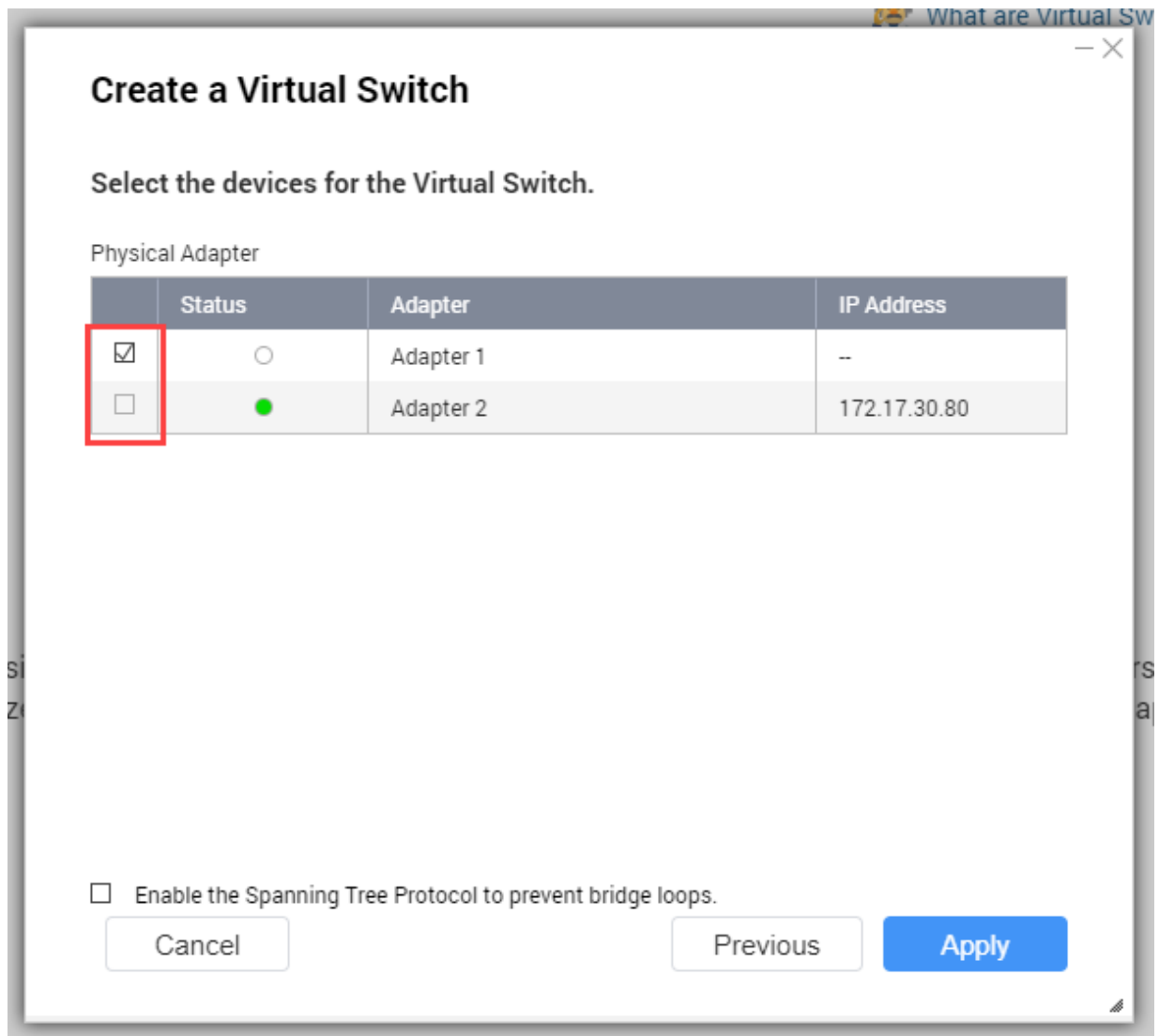


The **Create a Virtual Switch** window opens.

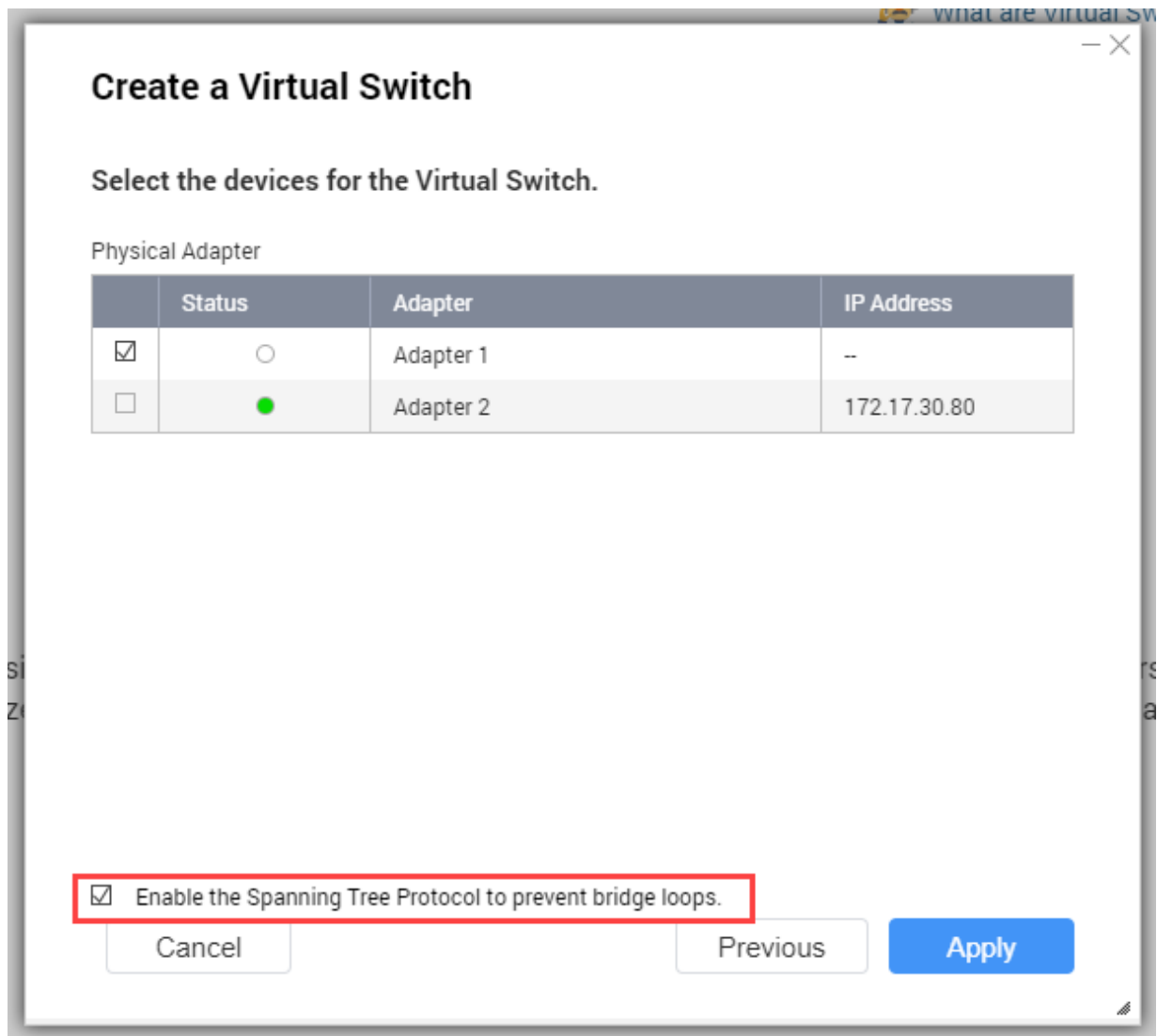
4. Select Advanced Mode.



5. Select one or more adapters.

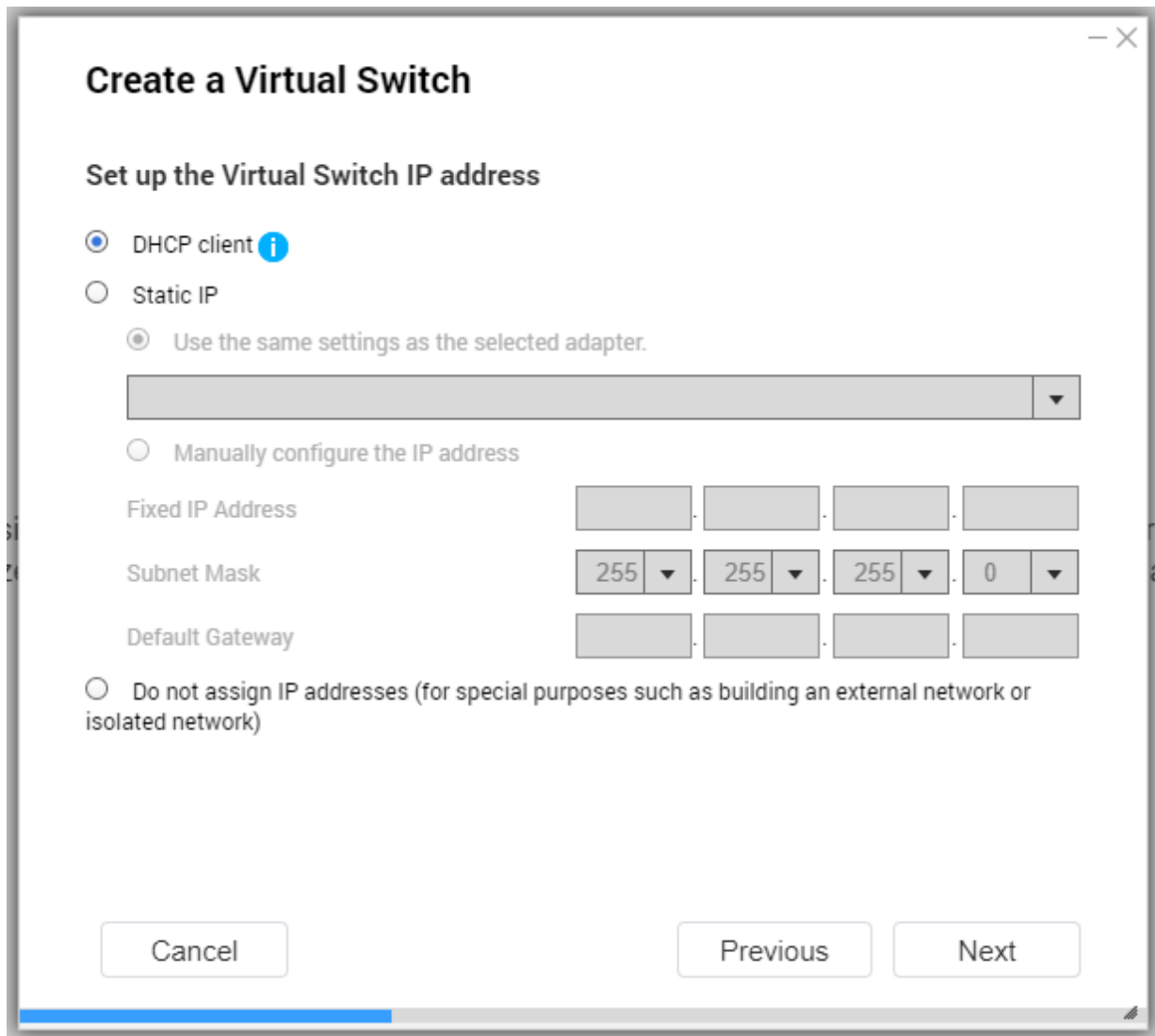




6. Optional: Select **Enable the Spanning Tree Protocol**.

**Tip**

Enabling this setting prevents bridge loops.

7. Click **Next**.
8. Configure the virtual switch IP address.

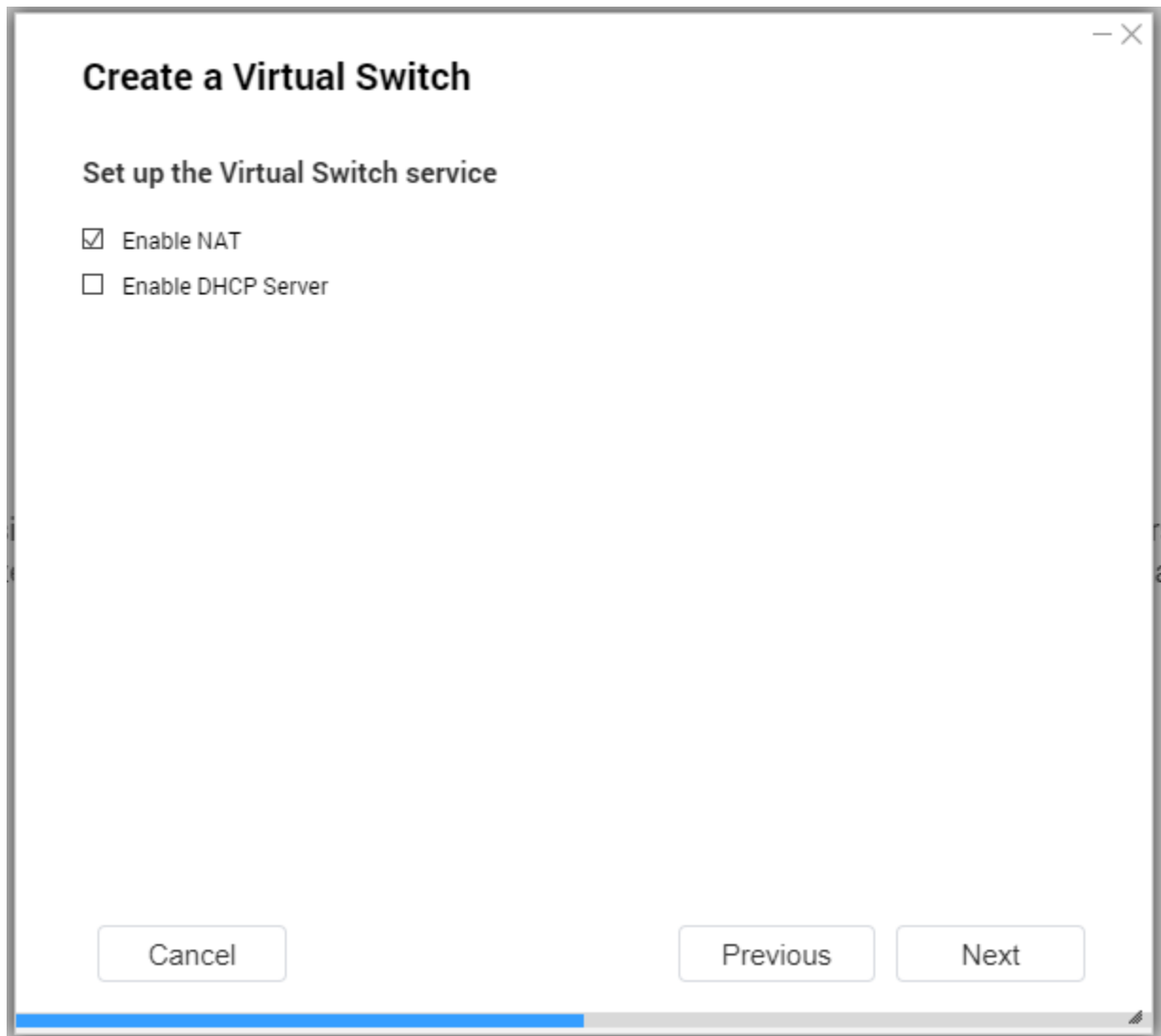


Address Type	Description
DHCP Client	Assigns a dynamic IP address to the virtual switch.
Static IP	Assigns a static IP address to the virtual switch.  Tip Examine your network setup for guidance on how to best configure these settings.
Do not assign IP Addresses	Does not assign an IP address to the virtual switch after creation.  Tip This setting should be used when creating a virtual switch for special purposes, such as when building an external or isolated network.

9. Click **Next**.

10. Configure the virtual switch services.

- a. Enable the NAT service.



Important

- The virtual switch must be configured with a static IP address. The IP address cannot be within the subnet of an interface that is currently in use.
- The IP address of the virtual switch cannot be in a reserved range that doesn't support forwarding:
 - 127.xxx.xxx.xxx
 - 169.254.xxx.xxx
 - 192.0.2.xxx
 - 198.51.100.xxx
 - 203.0.113.xxx

- b. Optional: Enable the DHCP Server.

Create a Virtual Switch

Set up the Virtual Switch service

Enable NAT

Enable DHCP Server

Start IP address: 123 . 255 . 255 . 124

End IP address: 123 . 255 . 255 . 250

Subnet Mask: 255.255.255.0 (/24)

Lease time: 1 Day(s) 0 Hour(s)

Default Gateway: 123 . 255 . 255 . 123

Primary DNS server: 10 . 8 . 2 . 11

Secondary DNS server: 172 . 16 . 2 . 11

WINS Server:

DNS suffix:

TFTP server:






Boot file:



Important

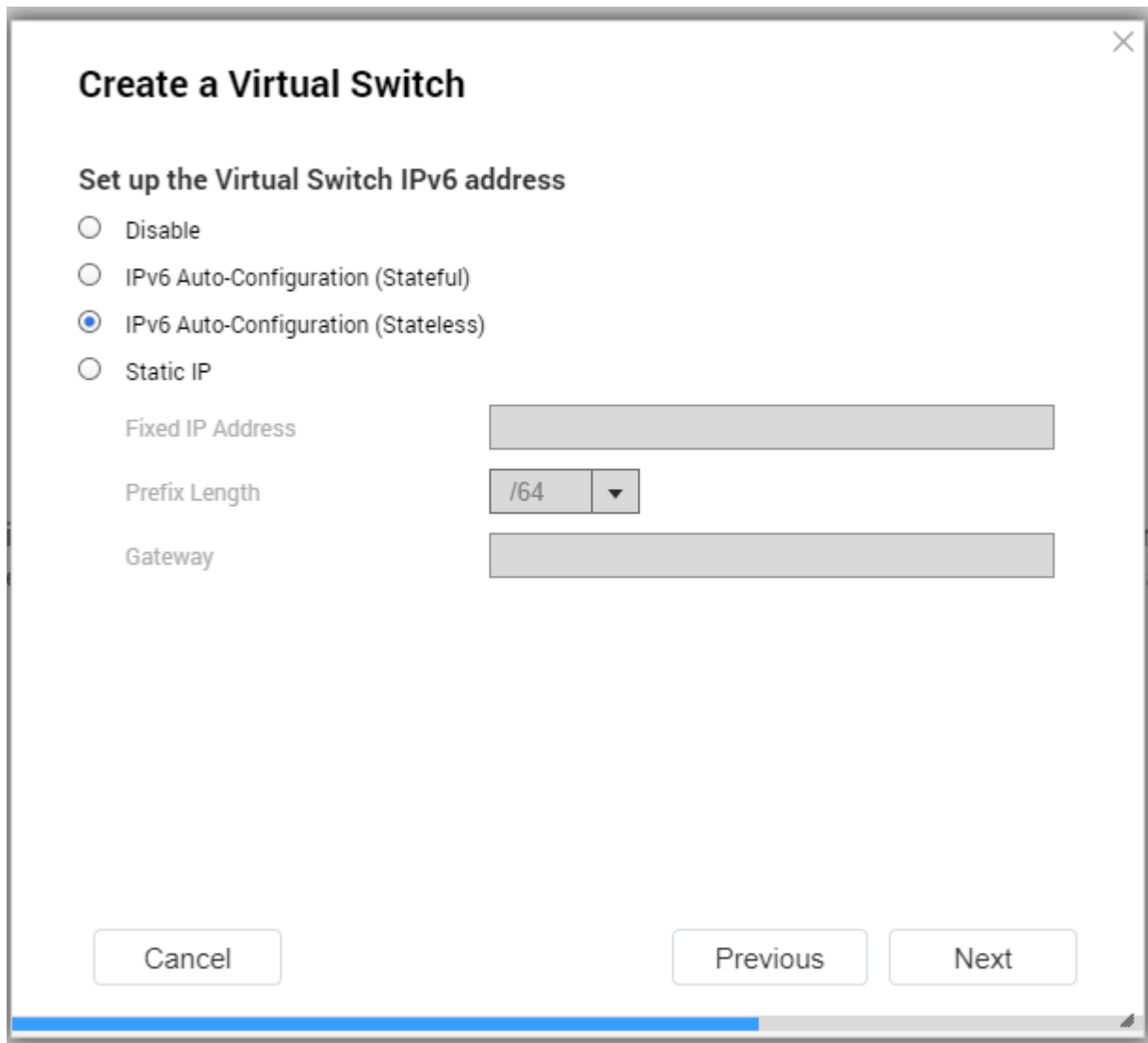
- The virtual switch must be configured with a static IP address. The IP address cannot be within the subnet of an interface that is currently in use.
- To avoid IP address conflicts, do not enable DHCP server if there is another DHCP server running on the local network.



Setting	Description
Start IP Address	Specify the starting IP address in a range allocated to DHCP clients.
End IP Address	Specify the ending IP addresses in a range allocated to DHCP clients.
Subnet Mask	Specify the subnet mask used to subdivide your IP address.


Setting	Description
Lease Time	Specify the length of time that an IP address is reserved for a DHCP client. The IP address is made available to other clients when the lease expires.
Default Gateway	Specify the IP address of the default gateway for the DHCP server.
Primary DNS Server	Specify a DNS server for the DHCP server.
Secondary DNS Server	Specify a secondary DNS server for the DHCP server.  Important QNAP recommends specifying at least one DNS server to allow URL lookups.
WINS Server	Specify the WINS server IP address.  Tip Windows Internet Naming Service (WINS) converts computer names (NetBIOS names) to IP addresses, allowing Windows computers on a network to easily find and communicate with each other.
DNS Suffix	Specify the DNS suffix.  Tip The DNS suffix is used for resolving unqualified or incomplete host names.
TFTP Server	Specify the public IP address for the TFTP server.  Tip QuTS hero supports both PXE and remote booting of devices
Boot File	Specify location and file name of the TFTP server boot file.  Tip QuTS hero supports both PXE and remote booting of devices

11. Click **Next**.

12. Configure the virtual switch IPv6 address.



Setting	Description
Disable	Do not assign an IPv6 address.
IPv6 Auto-Configuration (Stateful)	<p>The adapter automatically acquires an IPv6 address and DNS settings from the DHCPv6-enabled server.</p> <p> Important This option requires an available DHCPv6-enabled server on the network.</p>
IPv6 Auto-Configuration (Stateless)	<p>The adapter automatically acquires an IPv6 address and DNS settings from the router.</p> <p> Important This option requires an available IPv6 RA(router advertisement)-enabled router on the network.</p>

Setting	Description
Use static IP address	<p>Manually assign a static IP address. You must specify the following information:</p> <ul style="list-style-type: none"> • Fixed IP Address • Prefix length <p> Tip Obtain the prefix length information from your network administrator.</p> <ul style="list-style-type: none"> • Default Gateway

13. Click **Next**.

14. Configure the DNS settings.

✕


Create a Virtual Switch

Configure DNS Settings

Obtain DNS server address automatically
 Use the following DNS server address:

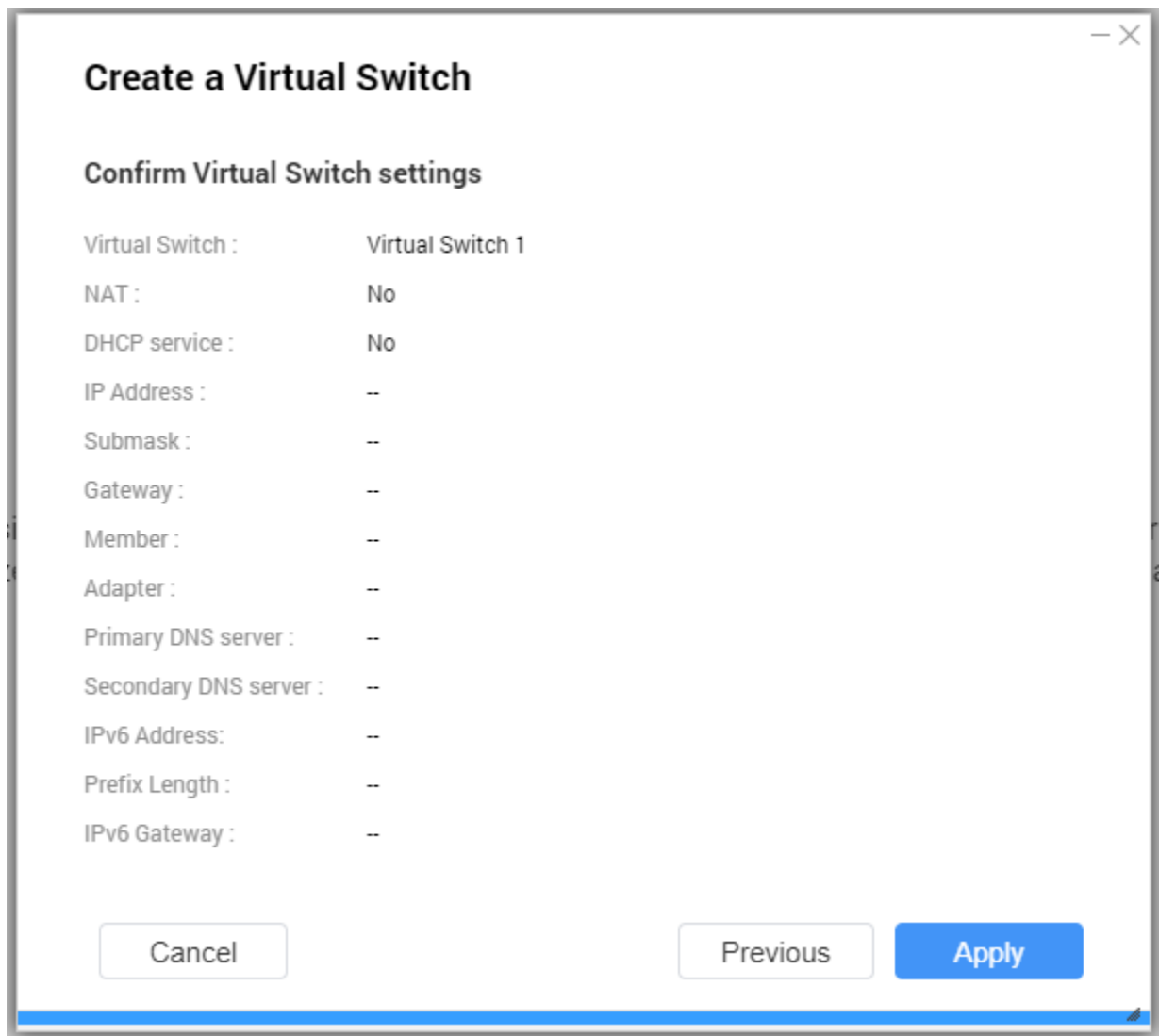
Primary DNS server
 Secondary DNS server

Cancel
Previous
Next

Setting	Description
Obtain DNS server address automatically	Automatically obtain the DNS server address using DHCP.
Use the following DNS server address	Manually assign the IP address for the primary and secondary DNS servers.  Important QNAP recommends specifying at least one DNS server to allow URL lookups.

15. Click **Next**.

16. Confirm the virtual switch settings.



17. Click **Apply**.

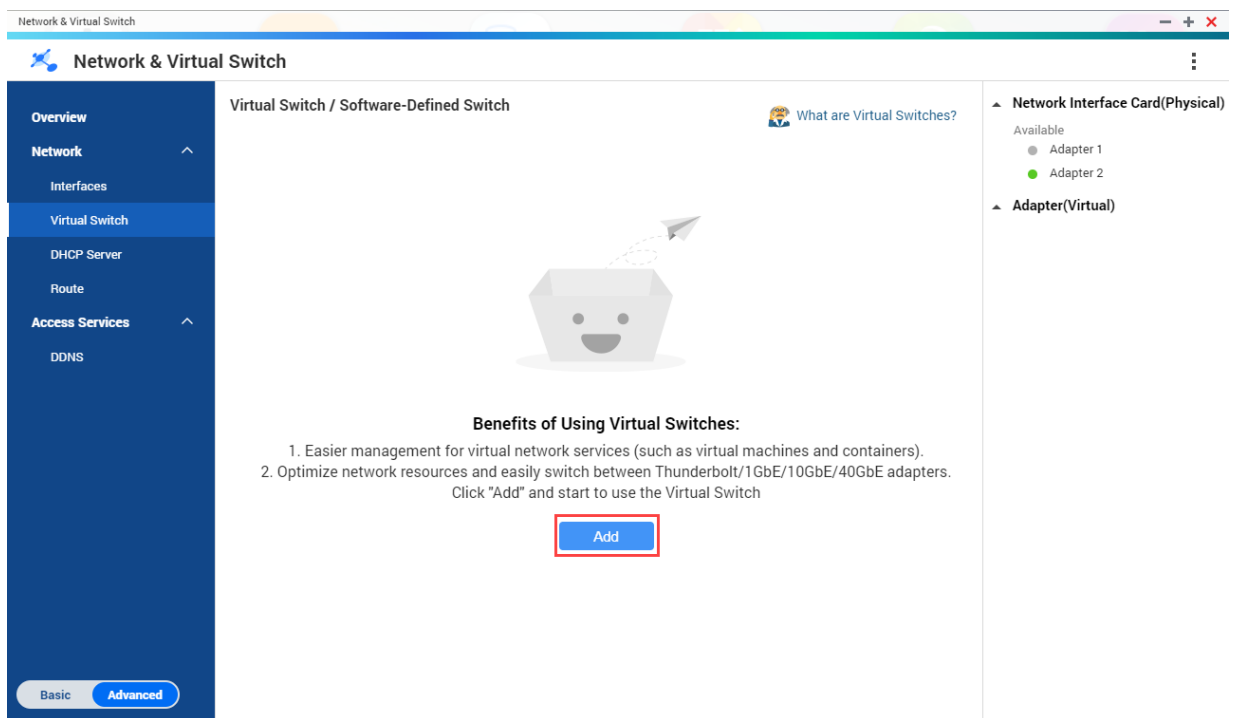
Creating a Virtual Switch in Software-defined Switch Mode



Important

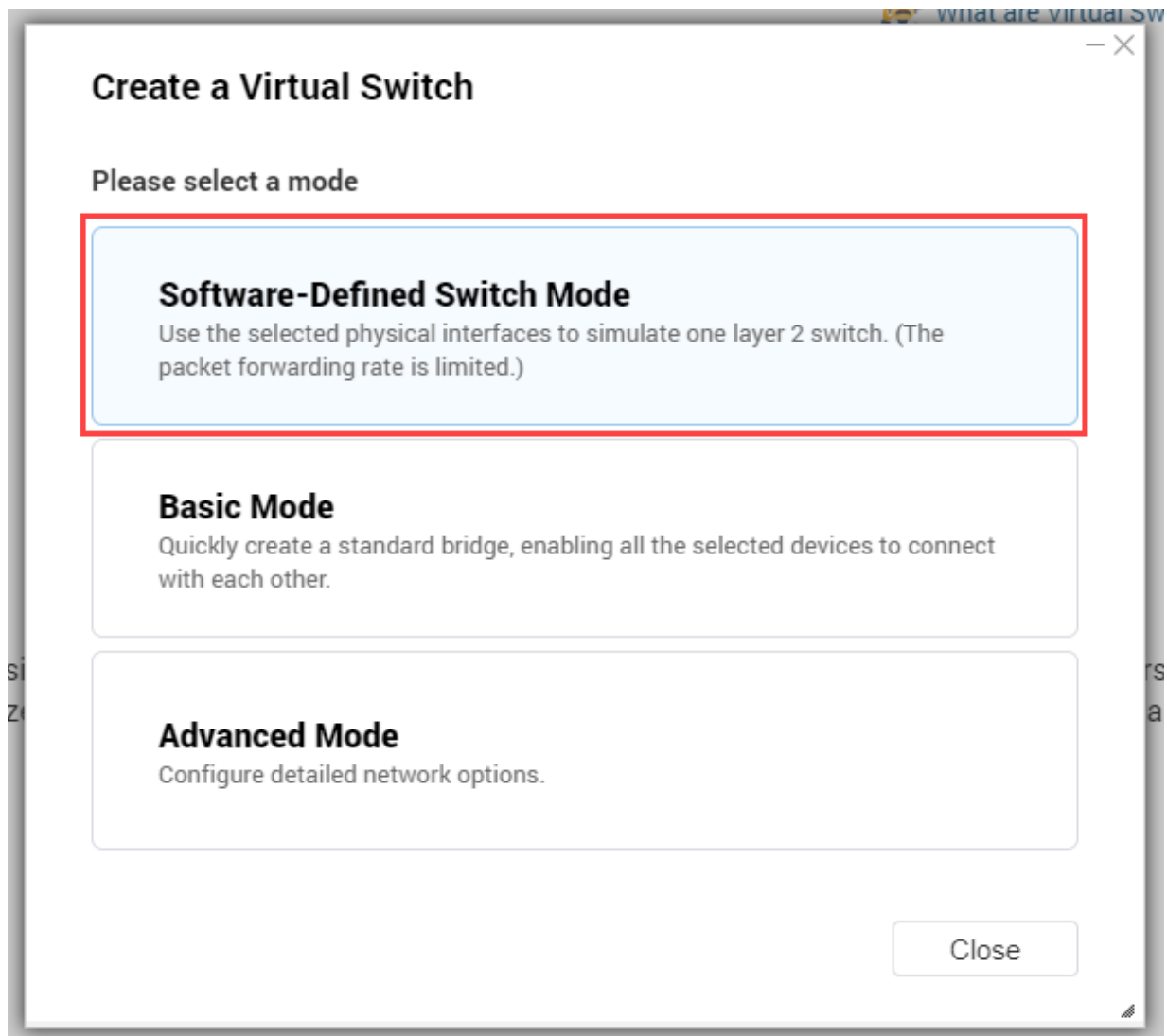
To avoid bridge loops, please ensure any Ethernet cables are connected to the same switch before configuring a Software-defined Switch.

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Virtual Switch** .
3. Click **Add**.

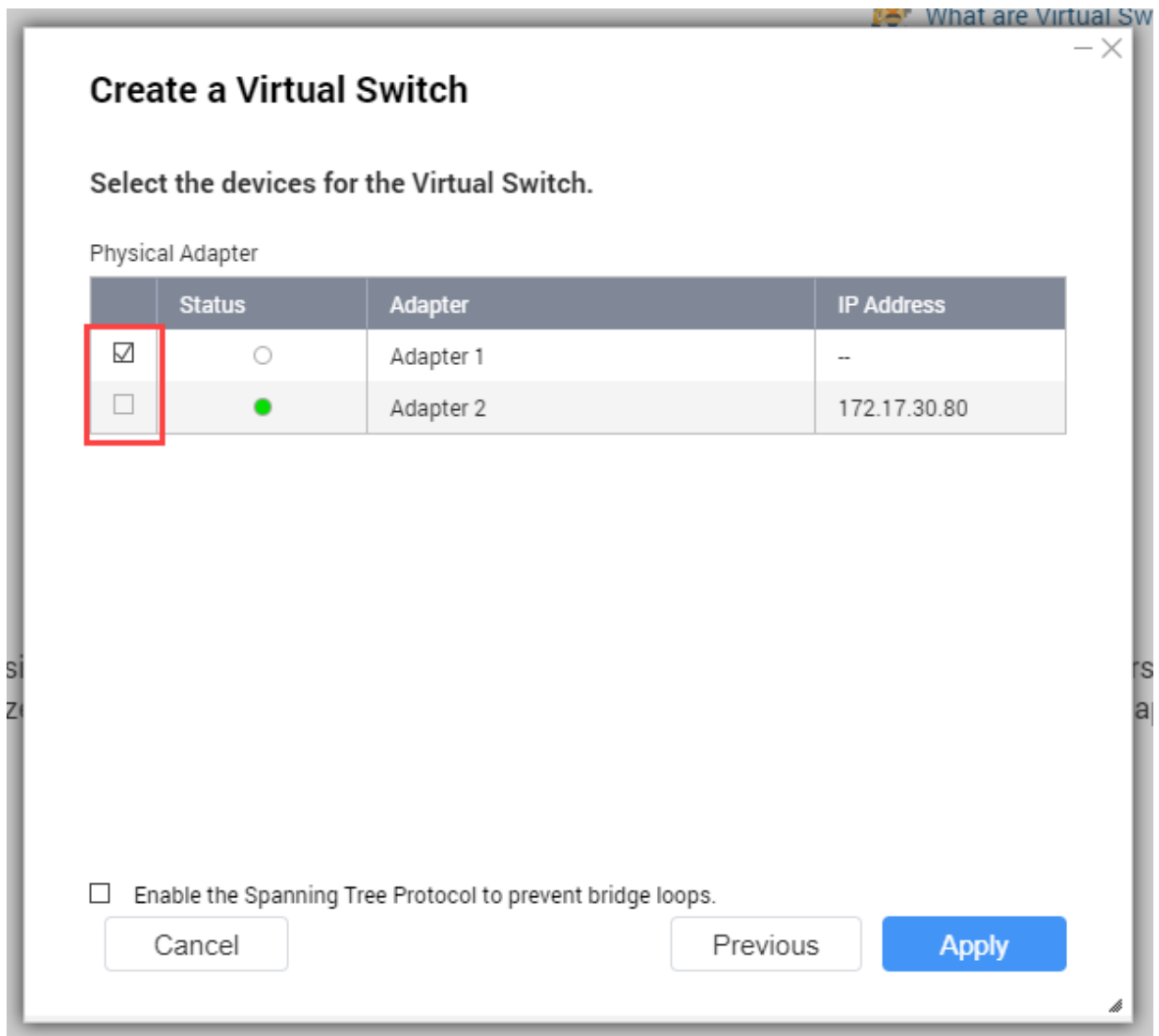


The **Create a Virtual Switch** window opens.

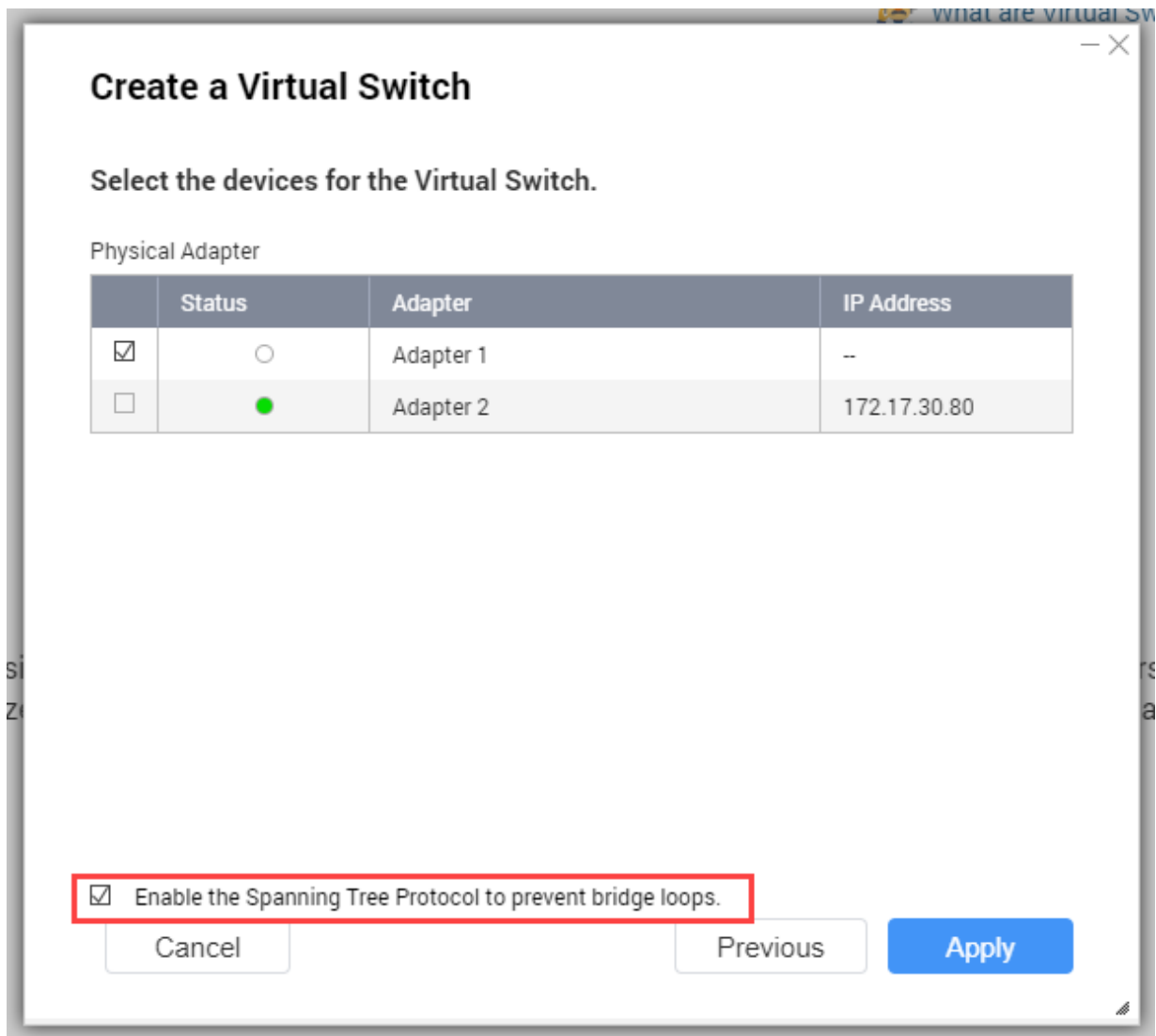
4. Select **Software-defined Switch Mode**.



5. Select one or more adapters.



6. Optional: Select **Enable the Spanning Tree Protocol**.

**Tip**

Enabling this setting prevents bridge loops.

7. Click **Apply**.


Network Policies Configuration

Network policies allow QuTS hero users to manage data traffic by implementing data reliability policies on the network adapters of the device.

Configuring Forward Error Correction (FEC) Settings

Forward Error Correction (FEC) is a digital signal processing technique to recover lost packets on a link by sending extra parity packets. Enabling FEC enhances data reliability by introduces redundant data or error correcting data before the system stores or transmits data.

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.

2. Go to **Network > Interfaces** .
3. Identify the adapter that you want to configure, then click  > **Configure** .
The **Configure** window opens.
4. Click **FEC Settings**.
5. Click **Enable forward error correction (FEC)**.
6. Select an FEC mode.

Setting	Description
Auto-negotiation	The device automatically selects the best FEC mode.
BASE-R FEC	BASE-R FEC (also known as Fire Code FEC or IEEE 802.3 Clause 74) offers simple, low latency (less than 100 nanoseconds) protection against bursty errors. This mode offers a weaker error correction but with lower latency.
RS-FEC	RS-FEC (also known as Reed Solomon FEC or IEEE 802.3 Clause 91) offers better error protection but adds latency (approximately 250 nanoseconds).



Important

The same FEC mode should be selected on both ends of the network link.

7. Click **Apply**.

Network & Virtual Switch applies the FEC settings.

Wireless Network Configuration

The Network & Virtual Switch Wi-Fi service provides all the functions of a wired network, while also providing location flexibility to QuTS hero users within the wireless signal range. The **Wi-Fi** screen controls the configuration and management of Wi-Fi connections accessible from the device.

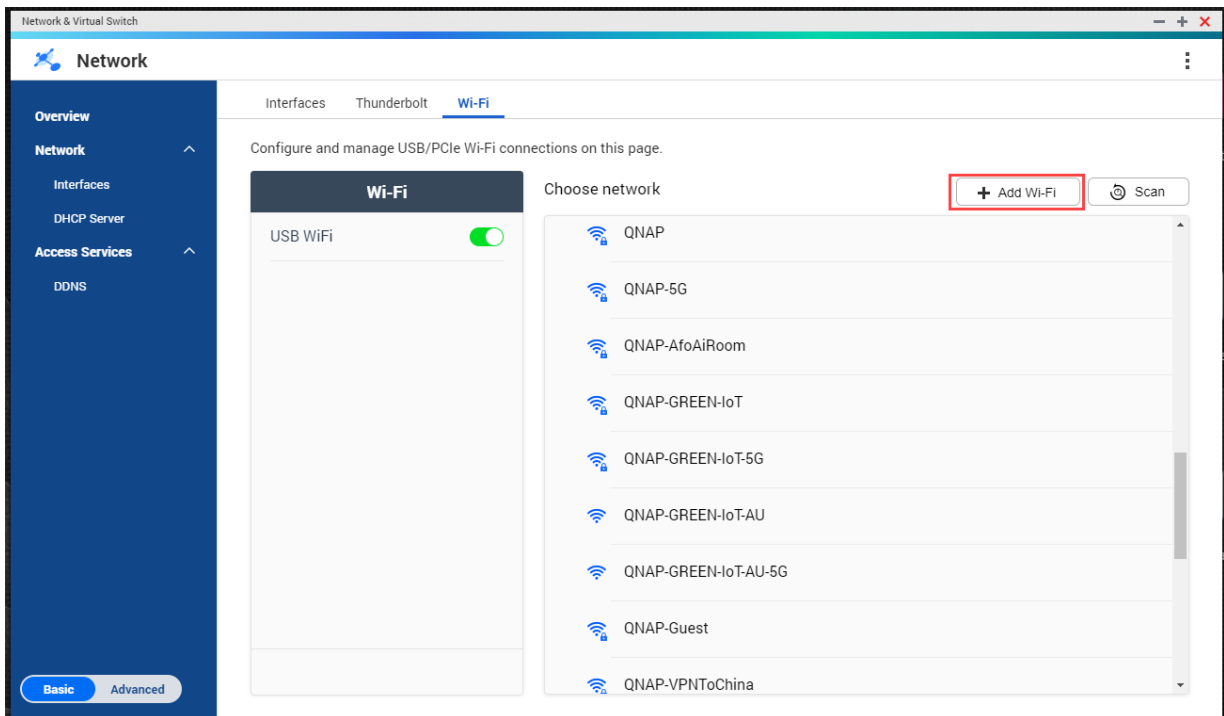


Important

- A USB or PCIe Wi-Fi device must be installed to access wireless features.
 - For a list of compatible USB Wi-Fi dongles, visit <http://www.qnap.com/compatibility>, then select **Search by Devices > USB Wi-Fi** .
 - For a list of compatible PCIe Wi-Fi cards, visit <http://www.qnap.com/compatibility>, then select **Search by Devices > Expansion Card > QNAP** .
- QuTS hero supports the simultaneous use of multiple PCIe Wi-Fi cards, but only one USB Wi-Fi dongle can be in used at a time.

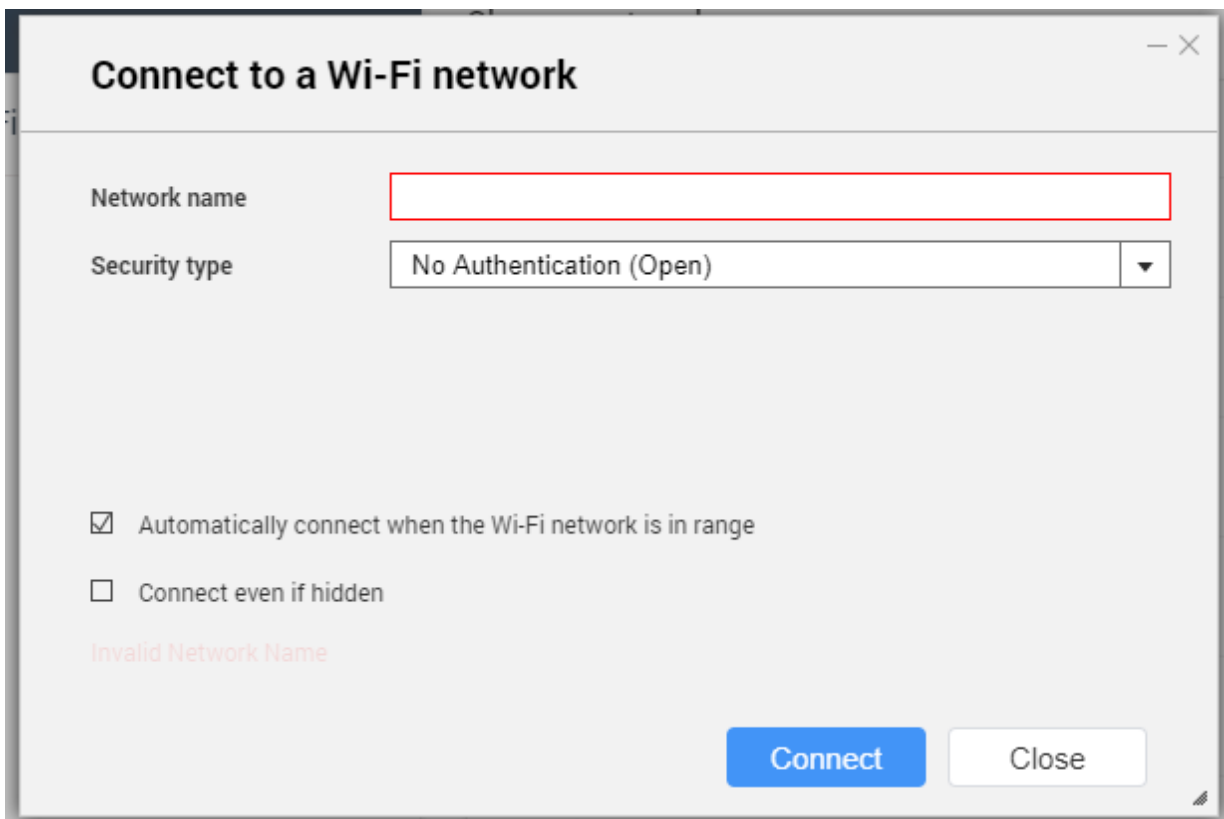
Adding a Wireless Network



1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Go to the **Wi-Fi** tab.
4. Click **Add Wi-Fi**.




The **Connect to a Wi-Fi network** window opens.



5. Configure connection settings.



Setting	User Action
Network Name	Enter the name of the wireless network.
Security Type	<p>Select the encryption used by the wireless network.</p> <ul style="list-style-type: none"> • No Authentication (Open): Any wireless device can connect to the network. This is the default setting. • WEP: Use Wired Equivalent Privacy (WEP) if the wireless device does not support WPA or WPA2. • WPA- Personal: Use Wi-Fi Protected Access (WPA)- Personal as an intermediate security measure if the wireless device does not support WPA2. • WPA2-Personal: Uses Advanced Security Encryption (AES) for data encryption. This is the suggested security mechanism if the wireless device supports WPA2. • WPA- & WPA2- Enterprise: Use this security mechanism if the wireless device supports transition from WPA-Enterprise to WPA2-Enterprise. The network automatically chooses the encryption method used by the wireless device.
Password	<p>Enter the password provided by the network administrator.</p> <p> Tip Click  to make the password visible.</p>
Automatically connect when the	Automatically connect to this network whenever it is in range.
Connect even if hidden	Attempt to connect to this network even if the SSID is hidden.

6. Optional: Configure WPA- & WPA2 Enterprise settings.



Setting	User Action
Authentication	<p>Authentication is specific to WPA- and WPA2- Enterprise encryption. Select a method based on the authentication supported by your device.</p> <ul style="list-style-type: none"> • Protected EAP (PEAP): Protected Extensible Authentication Protocol (PEAP) provides a more secure authentication to 802.11 WLANs. • EAP-TTLS: EAP Tunneled Transport Layer Security (EAP-TTLS) supports legacy authentication mechanisms.
Certificate Authority (CA) File	<p>A data file that contains identification credentials to help authenticate the WPA-WPA2 public key ownership.</p> <p> Note Select CA file is not required if you do not have access to a digital certificate.</p>

Setting	User Action
Inner Authentication	Select an inner authentication method based on PEAP or EAP-TTLS authentication. MS-CHAPv2 is the default inner authentication method for PEAP. The following inner authentication methods are available if the authentication method is set to EAP-TTLS: <ul style="list-style-type: none"> • PAP • CHAP • MS-CHAP • MS-CHAPv2
Username	Enter the username provided by the network administrator.
Password	Enter the password provided by the network administrator. <div style="display: flex; align-items: center;">  <div> <p>Tip</p> <p>Click  to make the password visible.</p> </div> </div>

7. Click **Connect**.

Network & Virtual Switch adds the wireless network.

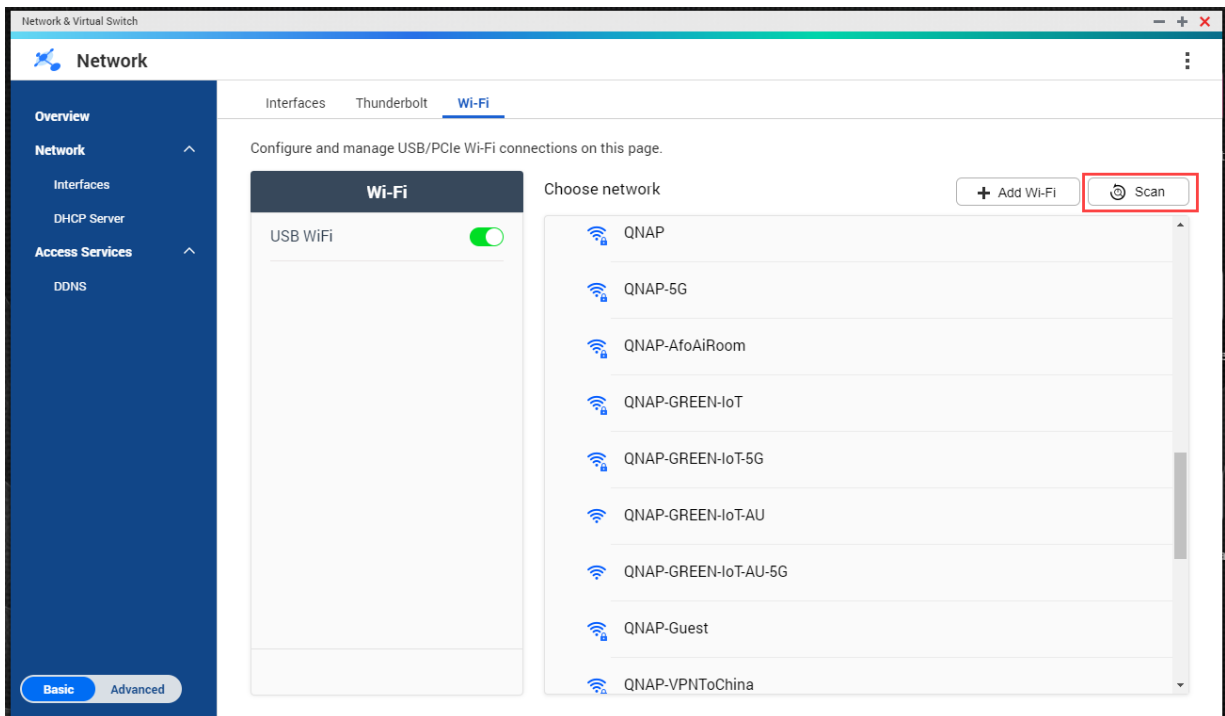
Enabling Wi-Fi

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Go to the **Wi-Fi** tab.
4.  .
Click  .

Network & Virtual Switch enables the Wi-Fi function.

Connecting to a Wireless Network

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Go to the **Wi-Fi** tab.
4. Optional: Click **Scan** to search for accessible networks.

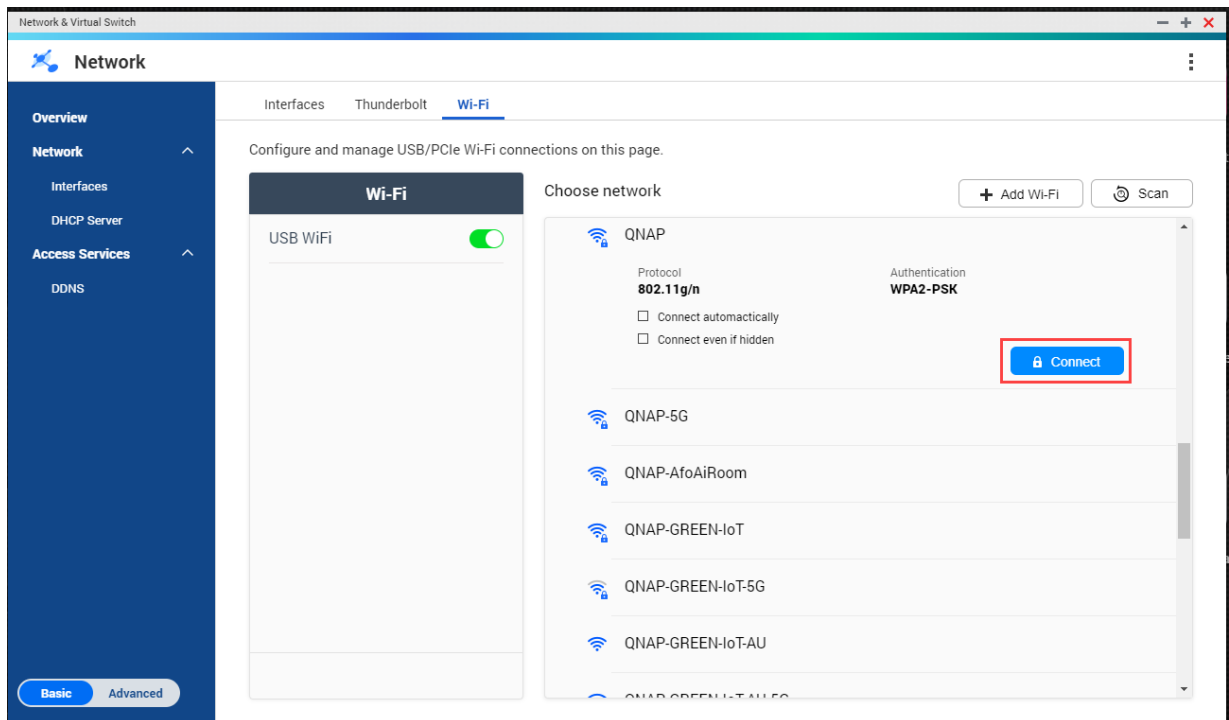


5. Select a wireless network from the list.

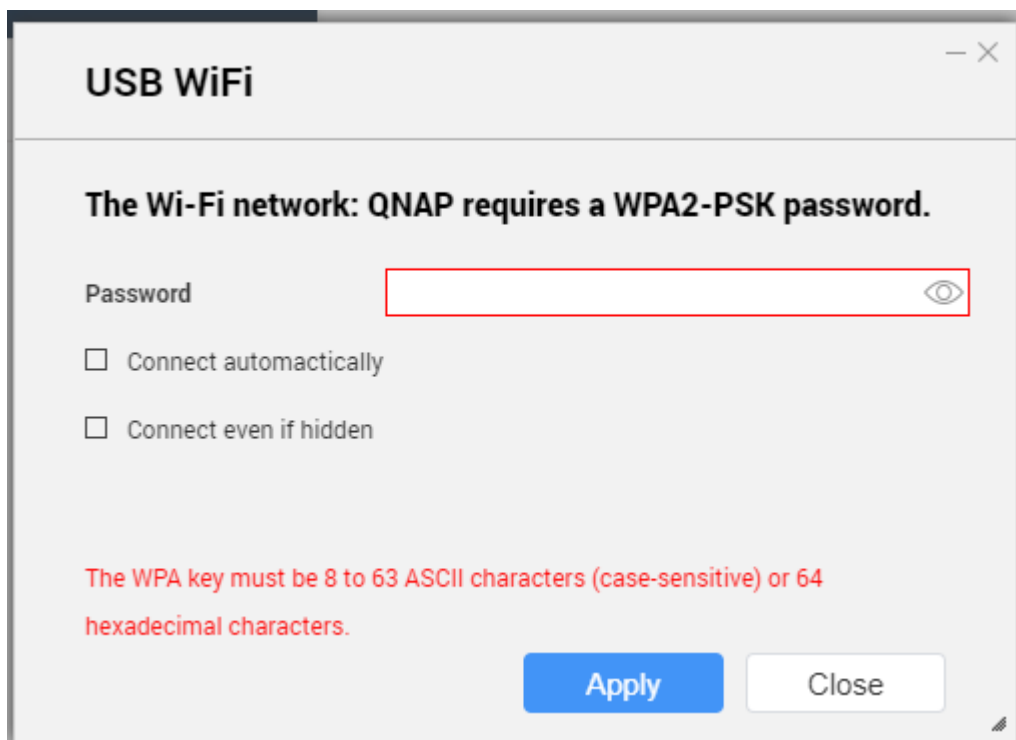
Icon	Description
	The Wi-Fi network requires a password.
	Connect to a Wi-Fi network without a password.
	<ul style="list-style-type: none"> The Wi-Fi connection cannot access the internet. The Wi-Fi connection requires an additional login. <p> Tip QuTS hero does not support networks that require an additional login.</p>



The settings panel expands.

6. Click **Connect**.



7. Optional: Configure connection settings.



Setting	User Action
Password	Enter the password provided by the network administrator.  Tip Click  to make the password visible.
Connect automatically	Automatically connect to this network whenever it is in range.
Connect even if hidden	Attempt to connect to this network even if the SSID is hidden.

8. Click **Apply**

The device connects to the wireless network.

Connecting to a Captive-Portal-Enabled Wireless Network Using Browser Station

A captive portal allows organizations to easily share their network environment with customers, employees, and other guests.

QuTS hero supports the captive portal function that connects to the internet through an access point in the wireless network.



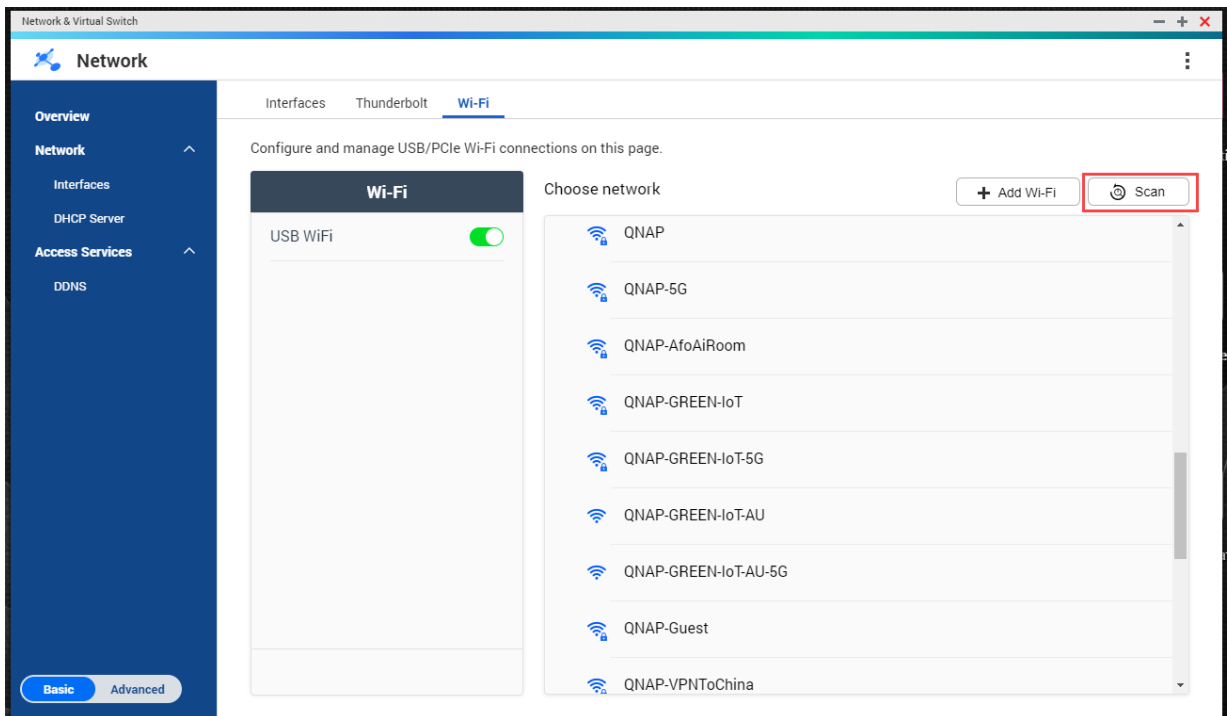
Note

Download and install Browser Station from App Center to access the captive portal functions.

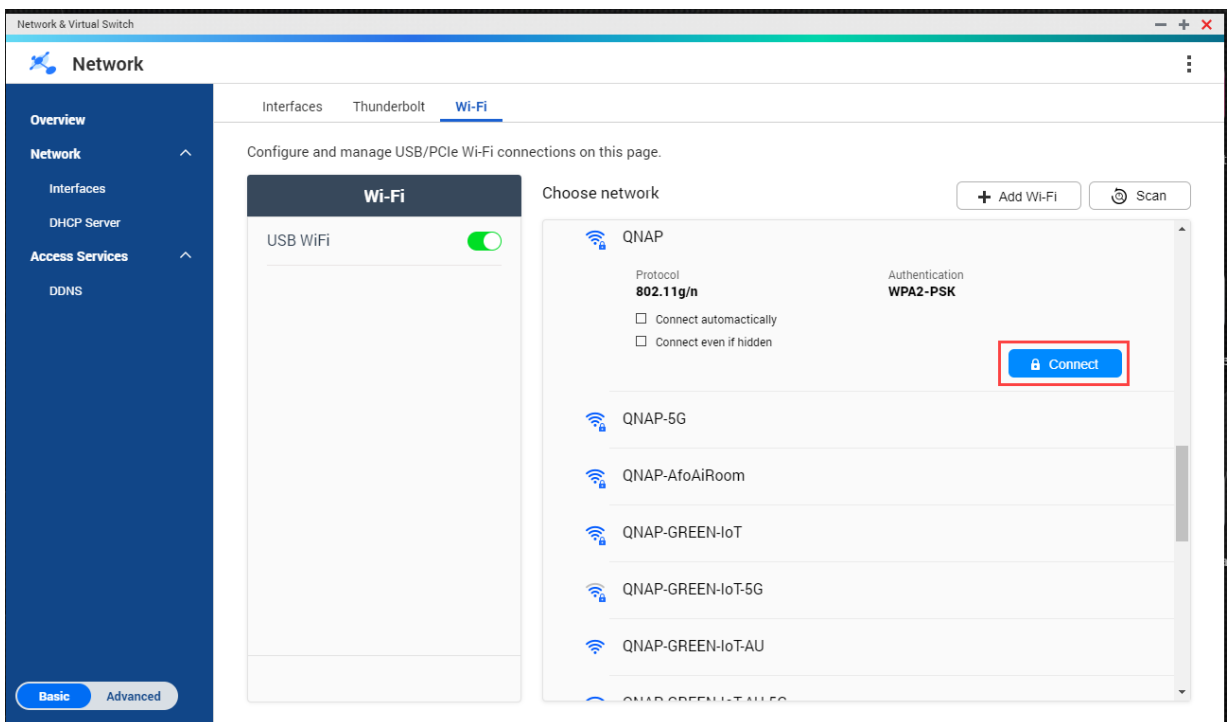
Alternatively, QNAP recommends installing Qfinder Pro (6.9.2 or later) to utilize the captive portal function on a wireless network.

For details, see [Connecting to a Captive-Portal-Enabled Wireless Network Using Qfinder Pro](#).

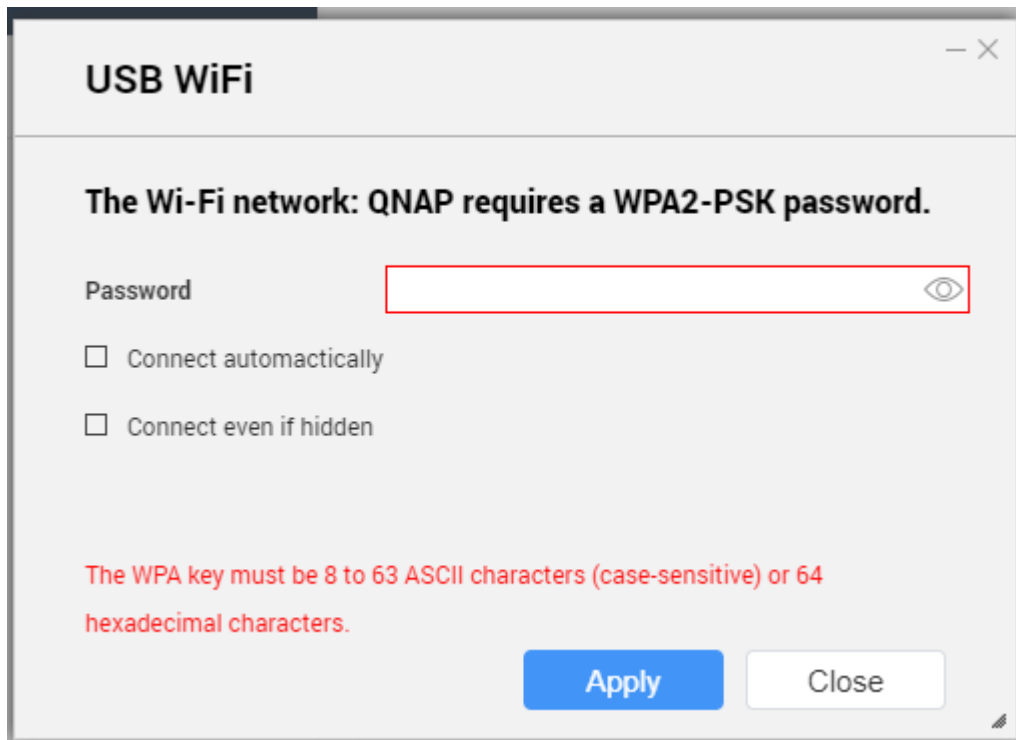
1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Go to the **Wi-Fi** tab.
4. Optional: Click **Scan** to search for accessible wireless networks with a captive portal.



5. Select the captive-portal-enabled wireless network from the list. The settings panel expands.
6. Click **Connect**.



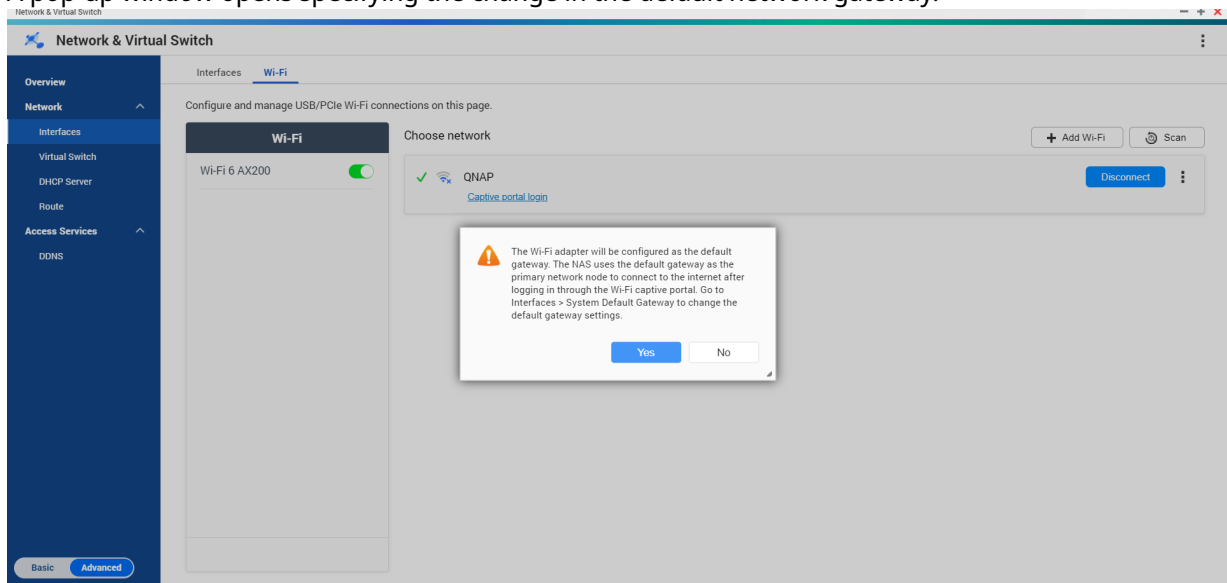
7. Optional: Configure connection settings.



For configuration details and wireless icon descriptions, see [Connecting to a Wireless Network](#).

8. Click **Apply.**

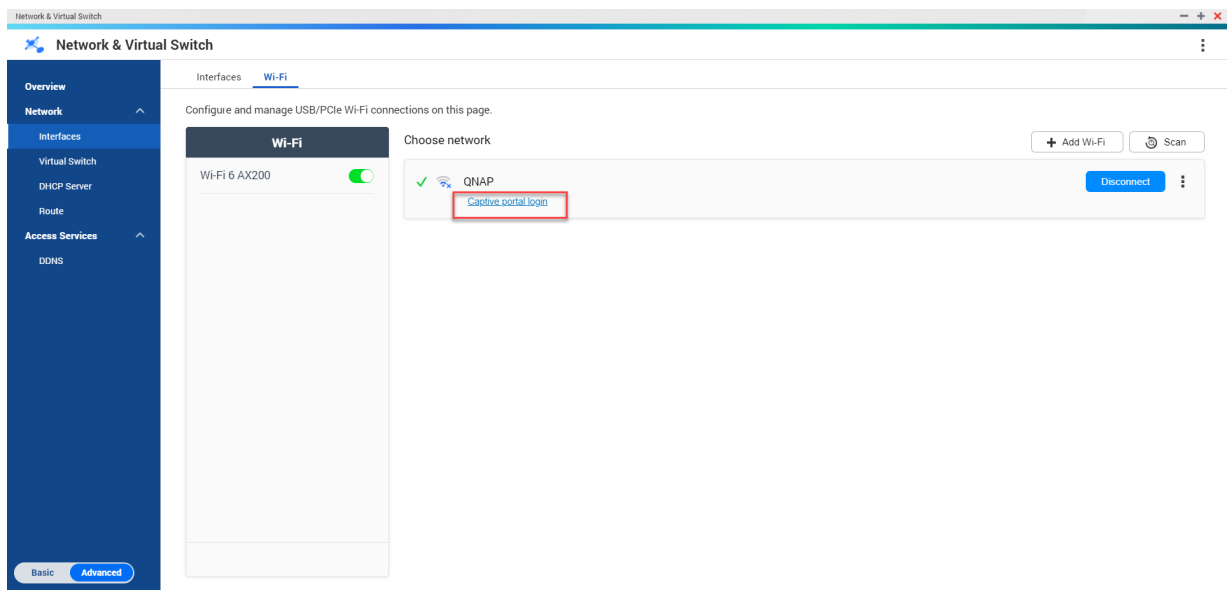
A pop-up window opens specifying the change in the default network gateway.



9. Click **Yes.**

10. Optional: Go to **Interfaces > System Default Gateway** to change the default network gateway settings.

11. Click **Captive portal login.**



Browser Station automatically redirects you to the captive portal landing page.

12. Enter the username and password to connect to the wireless network.

Connecting to a Captive-Portal-Enabled Wireless Network Using Qfinder Pro




Note

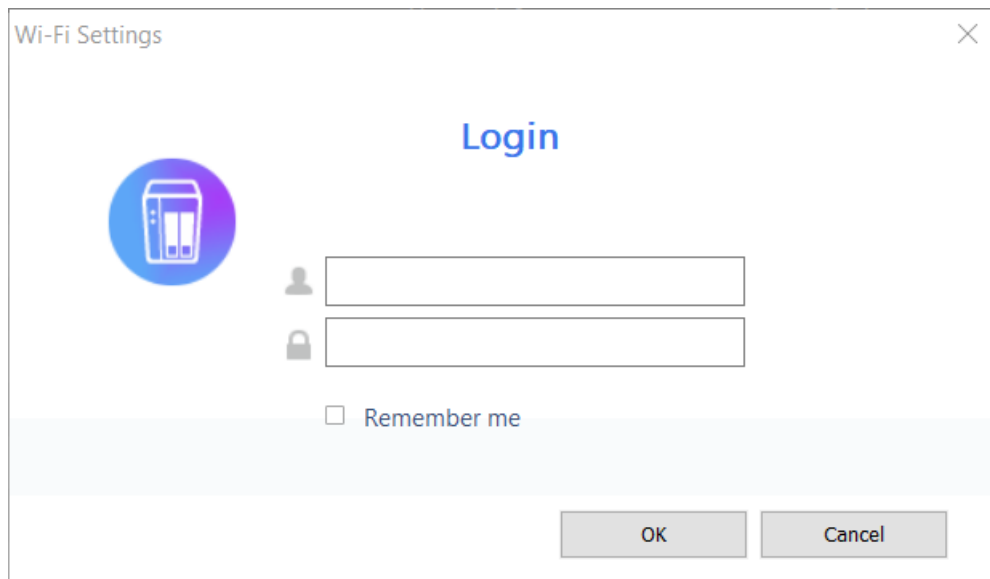
QNAP recommends installing Qfinder Pro (Windows 6.9.2 or later and MacOS/Linux 7.3.2 or later) to utilize the captive portal function on a wireless network.



Important

Connect the NAS directly to the PC using an ethernet cable in order to connect to a wireless network enabled with captive portal.

1. Open Qfinder Pro.
2. Locate the NAS in the list and click the unconfigured Wi-Fi icon  located under the Status table header.
3. Optional: Alternatively, select the NAS and go to **Settings > Wi-Fi Settings** . The **Login** page opens.



The image shows a 'Wi-Fi Settings' dialog box with a close button (X) in the top right corner. The title 'Wi-Fi Settings' is in the top left. The word 'Login' is centered in blue. On the left, there is a circular icon with a smartphone. To the right of the icon are two input fields: the first is preceded by a person icon, and the second by a lock icon. Below these fields is a checkbox labeled 'Remember me'. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

4. Enter the username and password.
5. Click **OK**.
The **Wi-Fi Connection Settings** page opens.

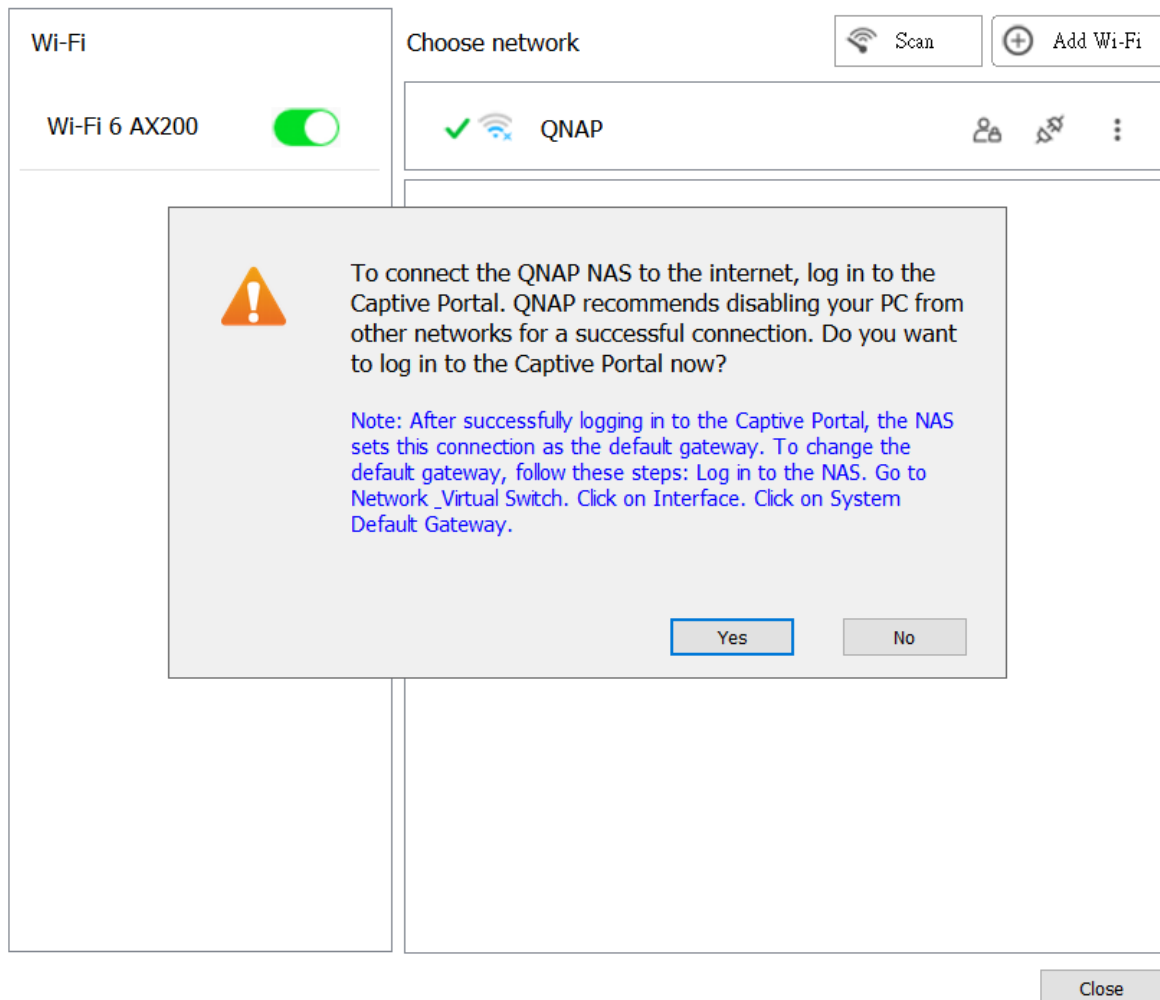
Wi-Fi Connection Settings



You can manage and configure Wi-Fi connection settings here.

6. Select the wireless network from the list.
The settings panel expands.
7. Click **Connect**.
8. Configure connection settings.
9. Click **Apply**.
A pop-up window opens.

You can manage and configure Wi-Fi connection settings here.



10. Click Yes.


The default browser automatically opens and redirects you to the captive portal landing page.



Note

Network & Virtual Switch automatically enables NAT and DHCP on the Wi-Fi adapter in the background.

11. Enter the username and password to connect to the wireless network.

Qfinder Pro displays the wireless connection icon  in the Qfinder Pro NAS status panel.

Understanding the Wireless Connection Messages

Message	Description
Connected	The NAS is currently connected to the Wi-Fi network.
Connecting	The NAS is trying to connect to the Wi-Fi network.
Out of range or hidden SSID	The wireless signal is not available or the SSID is not being broadcast.

Message	Description
Failed to get IP	The NAS is connected to the Wi-Fi network but could not get an IP address from the DHCP server. Check the router settings.
Association failed	The NAS cannot connect to the Wi-Fi network. Check the router settings.
Incorrect key	The entered password is incorrect.
Auto connect	Automatically connect to the Wi-Fi network. This is not supported if the SSID of the Wi-Fi network is hidden.

Accessing the Wireless Access Point (AP) Settings

The Network & Virtual Switch utility enables users to configure and manage wireless access points through the WirelessAP Station utility.




Note

The WirelessAP Station is not a built-in application on QuTS hero 5.0.0. To install the application, go to **App Center > All Apps**, and then install the WirelessAP Station application.

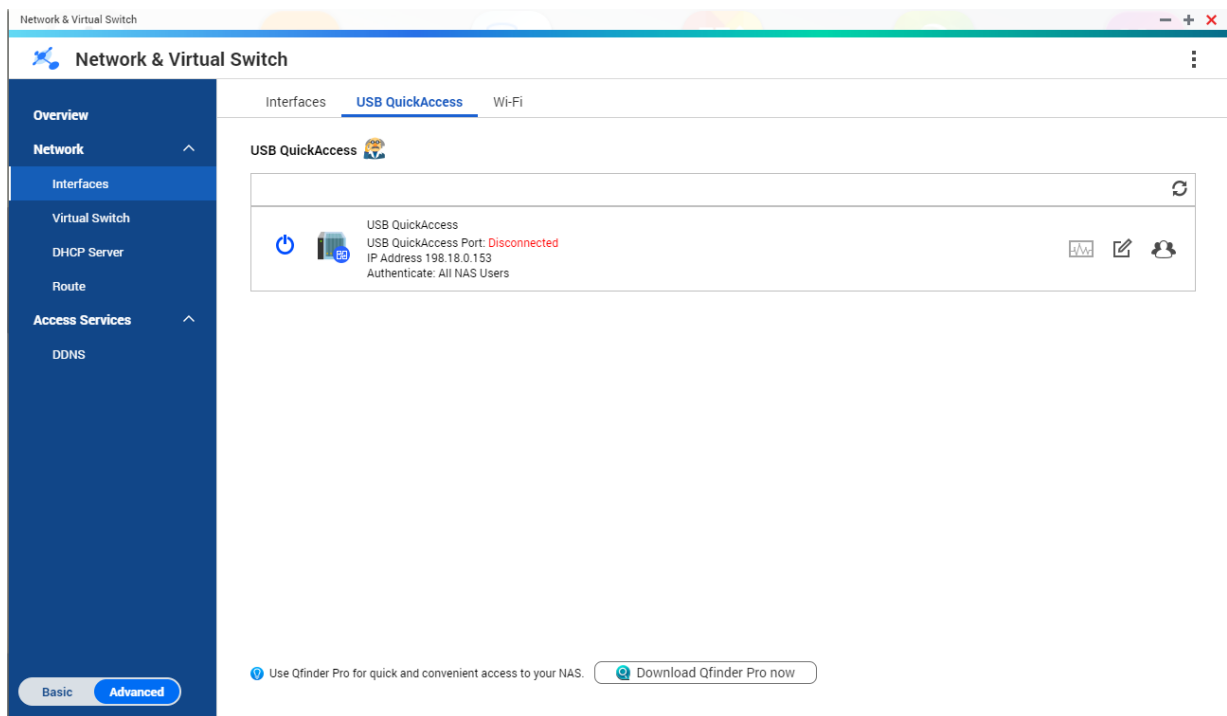
1. Go to **Control Panel > Network & File Services > Network & Virtual Switch**. The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces**.
3. Click the **WirelessAP Station** tab.

QuTS hero opens the WirelessAP Station application.

For details on configuring the access point settings, click  on the application taskbar.

USB QuickAccess Configuration


The **USB QuickAccess** screen controls the configuration and management of USB QuickAccess services on the NAS. USB QuickAccess allows a computer to connect to the NAS using a USB cable and the Common Internet File System (CIFS).



Important

- USB QuickAccess is only available on certain models.
- It is not possible to configure, delete, or disable DHCP servers created with USB QuickAccess.



Enabling USB QuickAccess

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Go to the **USB QuickAccess** tab.
4. Click  .

Network & Virtual Switch enables USB QuickAccess.



Configuring the USB QuickAccess IP address


1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Go to the **USB Quick Access** tab.

4.  Click  .
The **Configure** window opens.
5. Enter a fixed IP Address.
6. Click **Apply**.

Network & Virtual Switch applies the IP address settings.

Configuring USB QuickAccess Authentication

1. Go to **Control Panel > Network & File Services > Network & Virtual Switch** .
The **Network & Virtual Switch** window opens.
2. Go to **Network > Interfaces** .
3. Go to the **USB Quick Access** tab.
4.  Click  .
The **Configuration** window opens.
5. Select an authentication method:

Authentication Method	Description
All NAS Users	A QuTS hero username and password is required to access files.
Everyone	No username or password is required to access files.
Selected Users/Groups	Administrators can grant access to specific QuTS hero users or groups. A QuTS hero username and password is required to access files.  Tip To grant access to domain users, first set up Domain Security. Go to Control Panel > Privilege > Domain Security .

6. Click **Apply**.


Network & Virtual Switch applies the USB QuickAccess authentication settings.

Thunderbolt Interface Configuration

The **Thunderbolt** screen displays port and connection information related to any Thunderbolt interfaces on the NAS.

Thunderbolt to Ethernet (T2E)

Thunderbolt to Ethernet functionality allows the Thunderbolt port to act as an Ethernet interface.

 **Tip**
QNAP recommends using Qfinder Pro when configuring Thunderbolt to Ethernet.

 **Important**

Due to Thunderbolt driver issues, T2E connections using Thunderbolt port 2 may have connectivity problems when connecting to Windows. Thunderbolt port 3 connections are unaffected.

Enabling T2E with Qfinder Pro

Qfinder Pro is a utility for Windows, Mac, and Linux that allows you to quickly find and access a QNAP NAS over a LAN.

For the current version of Qfinder Pro, please visit <https://www.qnap.com/utilities>.



Tip

Qfinder Pro automatically configures the `/etc/sysctl.conf` settings file on macOS.

1. Open **Qfinder Pro**.
2. Locate the NAS using **Qfinder Pro**.
3. Click the Thunderbolt icon.
The T2E window opens.
4. Select **Enable T2E**.
5. Click **Apply**.

Enabling T2E on macOS

1. Open the Terminal.
2. Run the command.

Command	Notes
<code>sudo sysctl net.inet.tcp.path_mtu_discovery=0 && sudo sysctl net.inet.tcp.tso=0</code>	This command will only temporarily enable T2E. Restarting the Mac will delete the connection.
<code>sudo bash -c 'printf "#QNAP\nnet.inet.tcp.path_mtu_discovery=0\nnet.inet.tcp.tso=0\n#QNAP\n" >> /etc/sysctl.conf'</code>	This command will permanently apply these settings.

11. Network & File Services

About Network & File Services

The Network & File Services utility allows QuTS hero users to configure and control network and file protocols over a LAN or WAN connection. You can access shared resources over file sharing services and also handle data transfer using various file transfer protocols.

Network administrators can enable multiple protocols for clients to perform remote file editing functions over a web server and allow clients to automatically create a network of devices without manual configuration using service discovery protocols.

QNAP Service Ports

QNAP uses designated ports for communication. These ports are assigned to a specific service and users must manually open the required ports by adding the port number.



Note

For these services to operate correctly, their ports should remain open. This may require additional configuration of your firewall or router.

Backup Service

Service	Default Port	Protocol
Rsync	873	TCP
RTRR	8899	TCP

Download

Service	Default Port	Protocol
BitTorrent	6681-6999	TCP/UDP

File Transfers

Service	Default Port	Protocol
AFP	548	TCP
Netbios/SAMBA	137, 138, 139, 445	139, 445(TCP/UDP), 137, 138(UDP)
FTP/FTPES	20 and 21	TCP
NFS	2049, 111, dynamic ports	TCP/UDP
TFTP	69	UDP

Multimedia

Service	Default Port	Protocol
Twonkymedia	9000	TCP/UDP
UPnP Internet Gateway Device daemon	49152	TCP/UDP

Q'center

Service	Default Port	Protocol
Q'center Server	6600, 6606	TCP/UDP
Q'center Client NAS	6600, 6621, 6623	TCP/UDP

Qsync

Service	Default Port	Protocol
NAS Web	8080	TCP
NAS Web (HTTPS)	443	TCP

System Management

Service	Default Port	Protocol
LDAP Server	389	TCP
MySQL	3306	TCP
SNMP	161	TCP/UDP
SMTP	25	TCP
Syslog	514	TCP/UDP
Telnet	13131	TCP
SSH/SFTP Server	22	TCP

Virtualization Station

Service	Default Port	Protocol
Virtualization Station	8088	TCP
Virtualization Station (HTTPS)	8089	TCP

VPN

Service	Default Port	Protocol
QVPN (OpenVPN)	1194	UDP
QVPN (PPTP Server)	1723	TCP
QVPN (L2TP/IPSec Server)	500, 4500, 1701	UDP
QVPN (QBelt Server)	443	UDP

Web

Service	Default Port	Protocol
NAS Web	8080	TCP
NAS Web (HTTPS)	443	TCP
Web Server (HTTP, HTTPS)	80, 8081	TCP

Configuring Network Access Settings

QuTS hero users can use network access settings to connect applications to supported services using service binding and securely route traffic between networks using proxy and reverse proxy servers.

Configuring Service Binding Settings

NAS services run on all available network interfaces by default. Service binding enables you to bind services to specific network interfaces to increase security. You can bind services to one or more specific wired or wireless network interfaces.



Important

Configuring service binding does not affect users currently connected to the NAS. When users reconnect they will only be able to access the configured services using the specified network interfaces.

1. Go to **Control Panel > Network & File Services > Network Access > Service Binding**.
2. Select **Enable Service Binding**.
A list of available services and interfaces is displayed.
3. Bind services to interfaces.



Important

- By default, QuTS hero services are available on all network interfaces.
- Services must be bound to at least one interface.



Tip

Click **Use Default Value** to bind all services.

- a. Identify a service.
 - b. Deselect interfaces not bound to the service.
4. Click **Apply**.

Network & File Services saves the service binding settings.

Configuring Proxy Server Settings

A proxy server acts as an intermediary between the NAS and the internet. When enabled, QuTS hero will route internet requests through the specified proxy server.



Important

Prior to enabling the proxy server, ensure that Web Server is enabled in **Control Panel > Services > Applications > Web Server**.

1. Go to **Control Panel > Network & File Services > Network Access > Proxy**.
2. Select **Use a proxy server**.
3. Specify the proxy server URL or IP address.
4. Specify a port number.
5. Optional: Configure proxy authentication.
 - a. Select **Authentication**.
 - b. Specify a username.

- c. Specify a password.

6. Click **Apply**.

Network & File Services saves the proxy server settings.


Configuring Reverse Proxy Rule Settings

Reverse proxy settings allow users to configure a control point closer to web resources, enabling efficient and secure data distribution between users and websites.



Note
You can add up to 64 reverse proxy rules.

1. Go to **Control Panel > Network & File Services > Network Access** .
2. Click the **Reverse Proxy** tab.
3. Click **Add**.
The **Add Reverse Proxy Rule** window appears.
4. Configure the rule settings.

Setting	User Action
Rule name	Specify a name for the reverse proxy rule.
Source	
Protocol	Select a connection protocol from the following: <ul style="list-style-type: none"> • HTTP: Select to establish an unencrypted connection with the website. • HTTPS: Select to establish an encrypted connection with the website. Select Enable HTTP Strict Transport Security (HSTS) to advertise to clients that the device accepts only HTTPS requests.
Domain name	Specify the domain name of the website. Example: www.example.com  Note You can only specify one domain name for a reverse proxy rule.
Port number	Specify a port number for the reverse proxy port for recording the HTTP or HTTPS traffic.

Setting	User Action
Access control profile	Select from the following: <ul style="list-style-type: none"> • Allow all connections • Use existing profile: Select from configured access control profile • Create a new profile: Select to create a new access control rule. <ol style="list-style-type: none"> 1. Specify the access control permission. 2. Click Add. The Add Access Control Rule window appears. 3. Select the IP address type. <ul style="list-style-type: none"> • Single IP address • CIDR: Specify an IP address with the subnet mask. Example: 192.0. 1.0/24 4. Click Add.
Destination	
Protocol	Select the destination protocol. <ul style="list-style-type: none"> • HTTP • HTTPS • WebSocket • WebSocket Secure
Hostname	Specify the destination hostname.
Port number	Specify the destination port number.

5. Configure the advanced settings.
 - a. Click **Edit**.
 - b. Specify the proxy connection timeout in seconds.
 - c. Specify a custom header name containing a custom response to generated server responses.



Warning

You cannot repeat header names.

- d. Specify the custom header macro value to define the custom response.






6. Click **Apply**.

Network & File Services saves the reverse proxy settings.

Modifying Reverse Proxy Rules

1. Go to **Control Panel > Network & File Services > Network Access** .
2. Click the **Reverse Proxy** tab.

3. Perform the following tasks on configured reverse proxy rules.


Task	User Action
Delete a reverse proxy rule	<p>a. Beside the reverse proxy rule name, select the checkbox.</p> <p> Tip You can select multiple rules.</p> <p>b. Click Delete. A confirmation message appears.</p> <p>c. Click OK.</p>
Edit a reverse proxy rule	<p>a. Identify a reverse proxy rule.</p> <p>b. User Action, select . The Edit Reverse Proxy Rule window appears.</p> <p>c. Configure the rule settings.</p> <p> Note For details, see Configuring Reverse Proxy Rule Settings</p> <p>d. Click Apply.</p>
Enable a reverse proxy rule	<p>a. Beside the reverse proxy rule name, select the checkbox.</p> <p> Tip You can select multiple rules.</p> <p>b. Click Enable.</p>
Disable a reverse proxy rule	<p>a. Beside the reverse proxy rule name, select the checkbox.</p> <p> Tip You can select multiple rules.</p> <p>b. Click Disable.</p>

Configuring Network Protocol Settings

Network protocols enable QuTS hero users to remotely access network devices over the internet or a TCP/IP network. These protocols can be used to map, manage, and monitor network performance and notify users during events of network warnings, failures, bottlenecks, and other events.

Configuring Telnet Connections

Telnet is a network protocol used to provide a command line interface for communicating with the NAS.

 **Important**
Only administrator accounts can access the NAS through Telnet.

1. Go to **Control Panel > Network & File Services > Telnet/SSH** .
2. Select **Allow Telnet connection**.
3. Specify a port number.

Port numbers range from 1 to 65535.



Tip

The default Telnet port is 13131.

4. Click **Apply**.

Network & File Services saves the Telnet settings.

Configuring SSH Connections

Secure Shell (SSH) is a network protocol used for securely accessing network services over an unsecured network. Enabling SSH allows users to connect to the NAS using an SSH-encrypted connection or a SSH client such as PuTTY.

SSH File Transfer Protocol (SFTP) is a secure network protocol that works with SSH connections to transfer files and navigate through the QuTS hero filesystem. SFTP can be enabled after allowing SSH connections on the NAS.



Important

Only administrator accounts can access the NAS through SSH.

1. Go to **Control Panel > Network & File Services > Telnet/SSH**.
2. Select **Allow SSH connection**.
3. Specify a port number.
Port numbers range from 1 to 65535.



Tip

The default SSH port is 22.

4. Optional: Select **Enable SFTP**.
5. Click **Apply**.

Network & File Services updates the SSH connection settings.

Editing SSH Access Permissions

1. Go to **Control Panel > Network & File Services > Telnet/SSH**.
2. Click **Edit Access Permission**.
The **Edit Access Permission** window opens.
3. Select user accounts to give access permissions.



Important

Only administrator accounts can log in using an SSH connection.

4. Click **Apply**.

Network & File Services updates the SSH access permissions.

Configuring SNMP Settings



The Simple Network Management Protocol (SNMP) is used to collect and organize information about managed devices on a network. Enabling the QuTS hero SNMP service allows for the immediate reporting of NAS events, such as warnings or errors, to a Network Management Station (NMS).

1. Go to **Control Panel > Network & File Services > SNMP**.
2. Select **Enable SNMP Service**.
3. Configure the SNMP settings.

Setting	User Action
Port number	Specify the port that the Network Management Station (NMS) will use to connect to QuTS hero.
SNMP Trap Level	<p>Select the type of alert messages that the NAS will send to the NMS.</p> <ul style="list-style-type: none"> • Information: QuTS hero sends information regarding ongoing or scheduled NAS operations. • Warning: QuTS hero sends alerts when NAS resources are critically low or the hardware behaves abnormally. • Error: QuTS hero sends alerts when NAS features or applications fail to be enabled or updated.
Trap Address	Specify the IP addresses of the NMS. You can specify a maximum of 3 trap addresses.

4. Select the SNMP version that the NMS uses.

Option	User Action
SNMP V1/V2	<p>Specify an SNMP community name that contains 1 to 64 characters from any of the following groups:</p> <ul style="list-style-type: none"> • Letters: A to Z, a to z • Numbers: 0 to 9 <p>The SNMP community string functions as a password that is used to authenticate messages sent between the NMS and the NAS. Every packet that is transmitted between the NMS and the SNMP agent includes the community string.</p>

Option	User Action
<p>SNMP V3</p>	<p>Specify the username, authentication protocol and password, and privacy protocol and password.</p> <p>a. Specify a username.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-left: 20px;"> <p> Note The username should contain 1 to 32 characters from any of the following groups:</p> <ul style="list-style-type: none"> • Letters: A to Z, a to z • Numbers: 0 to 9 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • Special characters: All except " ' / \ </div> <p>b. Optional: Select Use Authentication.</p> <p style="padding-left: 20px;">1. Specify the authentication protocol.</p> <div style="border-left: 2px solid #FFC000; padding-left: 10px; margin-left: 20px;"> <p> Tip You can select either HMAC-MD5 or HMAC-SHA. If you are unsure about this setting, QNAP recommends selecting HMAC-SHA.</p> </div> <p style="padding-left: 20px;">2. Specify an authentication password that contains 8 to 64 ASCII characters.</p> <p>c. Optional: Select Use Privacy.</p> <p style="padding-left: 20px;">1. Specify a privacy password that contains 8 to 64 ASCII characters.</p>

5. Click **Apply**.

QuTS hero saves the SNMP settings.

Downloading the SNMP MIB

The Management Information Base (MIB) is a type of database in ASCII text format that is used to manage the NAS in the SNMP network. The SNMP manager uses the MIB to determine the NAS status or understand the messages that the NAS sends within the network. You can download the MIB and then view the contents using any word processor or text editor.

MIBs describe the structure of the management data of a device subsystem. They use a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that you can read or set using SNMP. You must assign the correct OID to retrieve the NAS information. The default OID for QNAP NAS devices is 1.3.6.1.4.1.24681.2.

- 1.** Go to **Control Panel > Network & File Services > SNMP** .
- 2.** Under **SNMP MIB**, click **Download**.
QuTS hero downloads the NAS.mib file to your computer.

Configuring File Sharing Protocol Settings

File sharing protocols allows users to access shared resources on a server that supports the file sharing protocol of each client. Shared file access is implemented over local area network (LAN) service and implements automatic synchronization of folder information whenever a folder is changed on the server.

Configuring Samba (Microsoft Networking) Settings

Microsoft Networking refers to Samba, a network protocol that allows data to be accessed over a computer network and provides file and print services to Windows clients.

1. Go to **Control Panel > Network & File Services > Win/Mac/NFS/WebDAV > Microsoft Networking**.
2. Select **Enable file service for Microsoft networking**.
3. Configure Microsoft networking settings.




Setting	User Action
Server description (Optional)	Specify a description that contains a maximum of 256 characters. The description should enable users to easily identify the NAS on a Microsoft network.
Workgroup	Specify a workgroup name that contains 1 to 15 characters from any of the following groups: <ul style="list-style-type: none"> • Letters: A to Z, a to z • Numbers: 0 to 9 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • Special characters: ~ ! @ # \$ ^ & () - _ { } . ' .






4. Select an authentication method.

Option	Description
Standalone server	QuTS hero uses the local user account information for authentication.
AD domain member	QuTS hero uses Microsoft Active Directory (AD) for authentication.
LDAP domain authentication	QuTS hero uses an LDAP directory for authentication.

5. Configure the advanced settings.
 - a. Click **Advanced Options**.
The **Advanced Options** window opens.
 - b. Configure the advanced settings.
 - c. Configure any of the following settings.

Option	User Action
Enable WINS server	Select to run a WINS server on the NAS.
Use the specified WINS server	Select to specify a WINS server IP address that QuTS hero will use for name resolution.

Option	User Action
Local master browser	<p>Select to use the NAS as a local master browser. A local master browser is responsible for maintaining the list of devices in a specific workgroup on a Microsoft network.</p> <p> Important To use the NAS as local master browser, specify the workgroup name when configuring Microsoft networking. The default workgroup in Windows is "workgroup".</p>
Allow only NTLMSSP authentication	<p>Select to authenticate clients using only NT LAN Manager Security Support Provider. When this option is deselected, QuTS hero uses NT LAN Manager (NTLM).</p>
Name resolve priority	<p>Select a name service to use for name resolution. The default service is DNS only. If a WINS server is specified, Try WINS then DNS is selected by default.</p>
Alternative login style	<p>Select to change how usernames are structured when accessing FTP, AFP, or File Station services. After selecting this option, users can access NAS services using Domain\Username, instead of Domain+Username.</p>
Automatically register in DNS	<p>Select to register the NAS on the DNS server. If the NAS IP address changes, the NAS automatically updates the IP address on the DNS server. This option is only available if AD authentication is enabled.</p>
Enable trusted domains	<p>Select to join users from trusted AD domains. This option is only available if AD authentication is enabled.</p>
Enable Asynchronous I/O	<p>Select to improve the Samba performance using asynchronous I/O. Asynchronous I/O refers to the I/O behavior on the CIFS protocol layer. This is different from the synchronous I/O feature found in the shared folder settings, which only applies to specific shared folders on the file system level.</p> <p> Tip To prevent power interruption, use a UPS when asynchronous I/O is enabled.</p>
Enable WS-Discovery to help SMB clients discover the NAS	<p>Select to enable Web Services Dynamic Discovery (WS-Discovery). WS-Discovery makes the NAS visible in File Explorer on Windows 10 computers.</p>
Highest SMB version	<p>Select the highest SMB protocol version used in your networking operation. Use the default SMB version if you are unsure about this setting.</p> <p> Note Selecting SMB3 will also include SMB 3.1 and SMB 3.1.1.</p>

Option	User Action
Lowest SMB version	Select the lowest SMB protocol version used in your networking operation. Use the default SMB version if you are unsure about this setting.  Note Selecting SMB 3 will also include SMB 3.1 and SMB 3.1.1.
Allow Symbolic links within a shared folder	Select to allow symbolic links within shared folders.  Important You must enable this setting in order to restore files from snapshots on Windows using Windows Previous Versions. For details, see Snapshot Data Recovery .
Allow Symbolic links between different shared folders	Select to allow symbolic links between shared folders.  Note This setting requires Allow Symbolic links within a shared folder to be selected first.
Restrict anonymous users from accessing SMB shared folders	Select to enable user login before accessing SMB shared folders.  Note This setting will be locked to Enabled (strict) if ABSE is enabled on any shared folder.
Veto files	Enable to hide files from users accessing the NAS via SMB. Files are hidden if their filename matches a pattern in the veto criteria file.
Veto criteria	Specify filename criteria for hiding files from SMB NAS users.  Note This option is only available when Veto files is selected.

- d. Click **Apply**.
 The **Advanced Options** window closes.

6. Click **Apply**.

Network & File Services saves the Samba settings.

Configuring AFP (Apple Networking) Settings

The Apple Filing Protocol (AFP) is a file service protocol that allows data to be accessed from a macOS device and supports many unique macOS attributes that are not supported by other protocols.

1. Go to **Control Panel > Network & File Services > Win/Mac/NFS/WebDAV > Apple Networking** .
2. Select **Enable AFP (Apple Filing Protocol)**.
3. Optional: Select **DHX2 authentication support**.
4. Click **Apply**.

Network & File Services saves the AFP settings.

Configuring NFS Service Settings

Network File System (NFS) is a file system protocol that allows data to be accessed over a computer network. Enabling the NFS service allows Linux and FreeBSD users to connect to the NAS.

The NFS service supports the following permissions in the NFS host access settings. You can apply these permissions to shared folders in **Control Panel > Privilege > Shared Folders > Edit Shared Folder Permissions** , and then selecting **NFS host access** as the permission type.

Permission	Status	Description
sync	Disabled	Disabling sync allows the NFS server to override the NFS protocol and reply to requests before any changes made by that request have been committed to stable storage. Using this option usually improves performance, but could result in an unclean server restart (e.g., a server crash), data loss, or corruption.
	Enabled	<ul style="list-style-type: none"> • wdelay: Causes the NFS server to delay writing to the disk to accommodate requests committed to stable storage. • no wdelay: The NFS server normally delays committing a write request to disc if it suspects another related write request is in progress or arriving soon. This allows multiple write requests to be committed to the disc with the one operation which can improve performance. no wdelay is available to turn off the delay behavior if an NFS server received mainly small unrelated requests. The default can be explicitly requested with the wdelay option.
secure	Disabled	Disabling secure requires that requests originate on TCP/IP ports above 1024.
	Enabled	Enabling secure requires that requests originate on TCP/IP ports between 1-1024.
Security	Enabled	<p>The transparent file sharing system offered by NFS exposes the data to several security vulnerabilities. The security mechanism allows safe network transmission over trusted networks. NFS protocol provides the following security options to enable secure data transfer between the server and the client.</p> <ul style="list-style-type: none"> • sys: sys or AUTH_SYS is the default unencrypted NFS version 3 security mechanism • krb5: Use Kerberos for authentication only. • krb5i: Use Kerberos for authentication, and include a hash with each transaction to ensure data integrity. Traffic can still be intercepted and examined, but modifications to the traffic are made apparent. • krb5p: Use Kerberos for authentication, and encrypt all traffic between the client and server. This authentication is the most secure mechanism but also incurs the most load.

Permission	Status	Description
Squash	Enabled	<p>Remote root users can change any file on the shared file system and expose other users to executable Trojan-infected applications. The squash permission enables the NFS server to transfer the client root role and prevent possible security threats.</p> <ul style="list-style-type: none"> • Squash root users: Maps the remote root user identity to a single anonymous identity and denies the user special access rights on the specified host. • Squash all users: Maps all the client requests to a single anonymous identity on the NFS server. • Squash no users: The default option does not transfer the client root role.

1. Go to **Control Panel > Network & File Services > Win/Mac/NFS/WebDAV > NFS Service** .
2. Enable NFS Service.
 - a. Optional: Click **Enable NFS v2/v3 Service**.
 - b. Optional: Click **Enable NFS v4 Service**.
3. Click **Enable manage-gids**.



Tip

Enable to increase the default maximum number of groups a user can belong to. This option replaces the list of group IDs (GIDs) received from the client with a list of GIDs mapped to the user ID (UID) that can access NFS share if the appropriate client UID also exists in the NAS.

4. Click **Apply**.

Network & File Services saves the NFS service settings.

Accessing FTP (QuFTP Service) Settings

QuFTP Service is the QTS File Transfer Protocol (FTP) application that you can access through Network & File Services.

1. Go to **Control Panel > Network & File Services** .
2. Click **QuFTP Service**.

QTS opens the QuFTP Service application.



Note

To use this feature, install QuFTP Service from App Center. For more information on QuFTP Service, go to the QNAP website.

Configuring WebDAV Settings

The Web Distributed Authoring and Versioning (WebDAV) protocol allows you to share, copy, move and edit remote content on the web.

1. Log on to QuTS hero as administrator.
2. Go to **Control Panel > Network & File Services > Win/MAC/NFS/WebDAV > WebDAV** .

3. Select **Enable WebDAV**.
4. Select one of the following options.
 - **Shared folder permission**
 - **WebDAV permission**
5. Optional: Configure the WebDAV port number settings.

Setting	User Action
Dedicated port number	Manually specify the port numbers for unencrypted (HTTP) and encrypted (HTTPS) connections. <ul style="list-style-type: none"> • HTTP port number • HTTPS port number
Web server port number	Select to use the default WebDAV port numbers.

6. Click **Apply**.

Network & Virtual Switch enables WebDAV and saves the settings.

Mounting a Shared Folder using WebDAV on Windows



Important

Before beginning this task, ensure that you have enabled WebDAV in the Control Panel. For details, see [Configuring WebDAV Settings](#).

WebDAV allows users to access and manage files on remote servers. You can mount a shared folder on your Windows computer as a network drive via WebDAV.

1. On your Windows computer, open File Explorer.
2. Right-click **This PC** and select **Map network drive**. **Map Network Drive** window appears.
3. Specify the path of the shared folder that you want to access.



Tip

The shared folder path uses the following format: `http://NAS-IP-address: port number/shared-folder-name`. For example: `http://172.17.45.155:80/Public`

4. Enable **Reconnect at sign-in** and **Connect using different credentials**.
5. Click **Finish**. **Windows Security** window appears.
6. Specify your NAS login credentials.
7. Click **Connect**.



Tip

If you cannot connect to the NAS shared folders using WebDAV, see [Troubleshooting WebDAV Connectivity Issues on Windows](#).

The NAS shared folder is mounted as a network drive via WebDAV. You can now access and manage the files in this shared folder using Windows File Explorer.

Troubleshooting WebDAV Connectivity Issues on Windows

If you are unable to connect to the NAS shared folders using WebDAV protocol on a Windows computer, follow the instructions below to modify the basic authentication level.

1. Right click **Start**.
2. Select **Run**.
3. Type `regedit`.
4. Click **OK**.
5. Open **Registry Editor**.
6. Go to **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > WebClient > Parameters** .
7. Open **BasicAuthLevel**.
8. Set the value data to 2.
9. Restart your computer.
10. Try using WebDAV to connect your computer to the NAS shared folder again.

Mounting a Shared Folder Using WebDAV on Mac



Important

Before beginning this task, ensure that you have enabled WebDAV in the Control Panel. For details, see [Configuring WebDAV Settings](#).

WebDAV allows users to access and manage files on remote servers. You can mount a shared folder on your Mac as a network drive via WebDAV.

1. On your Mac, go to **Finder > Go > Connect to Server** .
The **Connect to Server** window appears.
2. Specify the path of the shared folder that you want to access.



Tip

The shared folder path uses the following format: `http://NAS-IP-address: port number/shared-folder-name`. For example: `http://172.17.45.155:80/Public`

3. Click **Connect**.
4. Specify your NAS login credentials.
5. Click **Connect**.

The NAS shared folder is mounted as a network drive via WebDAV. You can now access and manage the files in this shared folder using macOS Finder.

Enabling Service Discovery Settings

Service discovery enables QuTS hero users to automatically detect and locate services on the network. Service discovery uses zero-configuration networking (zeroconf) to create a usable network based on the Internet Protocol Suite (TCP/IP) when devices are interconnected.

Enabling the UPnP Discovery Service

Universal Plug and Play (UPnP) is a networking technology that enables the discovery of networked devices connected to the same network. After enabling this service, devices supporting UPnP can discover the NAS.

1. Go to **Control Panel > Network & File Services > Service Discovery > UPnP Discovery Service** .
2. Select **Enable UPnP Discovery Service**.
3. Click **Apply**.

Network & File Services enables UPnP discovery service.

Enabling the Bonjour Discovery Service

Bonjour is a networking technology developed by Apple that enables devices on the same local area network to discover and communicate with each other.

1. Go to **Control Panel > Network & File Services > Service Discovery > Bonjour** .
2. Select **Enable Bonjour Service**.
3. Select the services to be advertised by Bonjour.



Important

You must enable the services in QuTS hero before advertising them with Bonjour.

4. Click **Apply**.



Network & File Services enables Bonjour discovery service.

Network Recycle Bin Management

The Network Recycle Bin contains files deleted from the device through File Station, FTP settings, or by clients connected using Samba (Microsoft networking).

Configuring the Network Recycle Bin

1. Go to **Control Panel > Network & File Services > Network Recycle Bin** .
2. Select **Enable Network Recycle Bin**.
3. Optional: Configure the Network Recycle Bin settings.


Setting	Description
File retention time	<p>Specify the number of days files are retained. The Daily check time controls when recycled files are checked against the retention time.</p> <p> Tip This field supports a maximum of 9999 days. The default is 180 days.</p>
Exclude these file extensions	<p>Specify which file extensions are excluded from the Network Recycle Bin.</p> <p> Important File types are case insensitive and must be separated by a comma.</p>

4. Click **Apply**.

Deleting All Files in the Network Recycle Bin

1. Go to **Control Panel > Network & File Services > Network Recycle Bin**.
2. Click **Empty All Network Recycle Bin**.
A warning message appears.
3. Click **OK**.
QuTS hero deletes all files from the Network Recycle Bin.

Restricting Access to the Network Recycle Bin

1. Go to **Control Panel > Privilege > Shared Folders**.
2. Identify a shared folder.
3. Under **Actions**, click .
The **Edit Properties** window appears.
4. Select **Enable Network Recycle Bin**.
5. Select **Restrict the access to Recycle Bin to administrators only for now**.
6. Click **OK**.

12. myQNAPcloud

myQNAPcloud is a service that allows you to access, manage, and share files stored on your QNAP devices remotely through the internet.

Getting Started

1. Create a QNAP ID.
For details, see [Creating a QNAP ID With Email or Phone Number](#).
2. Register the device to myQNAPcloud.
For details, see [Registering a Device to myQNAPcloud](#).
3. Optional: Configure any of the following settings.

Settings	Description
Port forwarding	Port forwarding allows you to access your device on the internet through a UPnP router. For details, see Configuring UPnP Port Forwarding .
My DDNS	My DDNS allows you to specify a dedicated myQNAPcloud subdomain name that you can use to access your device on the internet. For details, see Configuring DDNS Settings
Published services	You can publish QNAP services on your device, such as the QNAP desktop and File Station, so they can be accessible on myQNAPcloud. For details, Configuring Published Services .
myQNAPcloud Link	myQNAPcloud Link allows you to access your device on the myQNAPcloud website or through mobile apps and client utilities without changing your router settings. Using shared links, you can also simultaneously download and sync files to a remote NAS without needing to first save them to client device. For details, see Enabling myQNAPcloud Link .
Access controls	Access controls allow you to configure device access permissions for myQNAPcloud users. For details, see Configuring Device Access Controls .
SSL certificates	myQNAPcloud allows you to add SSL certificates to help secure your network communication. You can either download and install a myQNAPcloud or Let's Encrypt certificate. For details, see Installing an SSL Certificate .

Account Setup

Before using myQNAPcloud services, you must first create a QNAP ID and then configure required settings using your QNAP ID.

Creating a QNAP ID With Email or Phone Number

1. Go to <https://account.qnap.com/>.
The **QNAP Account** login page displays.
2. Click **Create Account**.
The **Create Account** screen appears.
3. Specify a nickname, a valid email address or phone number, and a password.
4. Read and acknowledge the Terms of Service and Privacy Policy.

5. Click **Sign Up**.
The **Data Privacy Notice** box appears.
6. Read the notice, and then click **I Agree**.
myQNAPcloud sends a verification email or message.
7. Confirm the registration.
Your QNAP ID is activated.


**Tip**

The registration link automatically expires in 15 days. You can go to [QNAP Account](#) to send a new activation email.

Registering a Device to myQNAPcloud

1. Log in as administrator.
2. Go to **myQNAPcloud > Overview** .
3. Click **Get Started**.
The **myQNAPcloud wizard** appears.

Welcome to myQNAPcloud!



Hello! Welcome to myQNAPcloud wizard.

This wizard helps you set up the QNAP NAS for remote access on the Internet by the steps below:

1. Create or sign in a QNAP ID
2. Register your NAS
3. Enable myQNAPcloud remote access services

Start

Quit

4. Click **Start**.

Welcome to myQNAPcloud! ✕

Sign in QNAP ID

Please sign in QNAP ID to proceed. (or [Create QNAP ID](#))

QNAP ID : ℹ

Password :

[Forgot your password?](#) | [Resend activation email](#)

Step 1/5 Next Cancel

5. Specify your QNAP ID and password.
6. Click **Next**.

Welcome to myQNAPcloud! ✕

Register your myQNAPcloud device name

Please enter a new name for your QNAP NAS. This name will be used to remotely access your NAS.

Device name : ✔

After finishing the wizard, you can access your QNAP NAS remotely with the following Internet address:

johndoe01.myqnapcloud.com

SmartURL - Finding the suitable way to access your device remotely. [Get more info](#)

<https://qlink.to/johndoe01>

Register with an existing device name? Please click [here](#) to start.

Step 2/5

7. Specify a device name containing up to 30 alphanumeric characters.
You may reuse an existing device name. The device currently using this name will be deregistered from myQNAPcloud.
8. Click **Next**.
9. Select the services you want to enable.

Service	Description
Auto Router Configuration	This allows you to configure port forwarding.
DDNS	This allows you to access your device on the internet using a dedicated address.
Published Services	This allows you to select which services you want to publish on the myQNAPcloud website.

Service	Description
myQNAPcloud Link	myQNAPcloud Link allows you to access your device on the myQNAPcloud website or through mobile apps and client utilities without changing your router settings. Using shared links, you can also simultaneously download and sync files to a remote NAS without needing to first save them to a client device. If you enable this option and your device does not have myQNAPcloud Link, myQNAPcloud Link will automatically be downloaded and installed after you click Next .


10. Select an access control option.

Option	Description
Public	All users can search for your device and view the published services on the myQNAPcloud website. They can also access your device with a SmartURL.
Private	Your device will not appear in the search results. Only you can access your device on the myQNAPcloud website.
Customized	Your device will only be visible to you and invited users. Other users will not be able to access your device even with a SmartURL.

11. Click **Next**.
myQNAPcloud applies your settings.
The **Summary** screen appears.
12. Review the details, and then click **Finish**.




Installing myQNAPcloud Link


Only perform this task if you did not enable myQNAPcloud Link when registering your device to your myQNAPcloud account.







1. Log in to QNAP as administrator.
2. Open **App Center**.
3. Click .
A search box appears.
4. Type `myQNAPcloud Link` and then press `ENTER`.
The myQNAPcloud Link application appears in the search results list.
5. Click **Install**.
App Center installs myQNAPcloud Link on your device.

Overview

The **Overview** screen displays your basic myQNAPcloud settings, as well as the device network connectivity and DDNS status.

Status Icon	Description
	The item is enabled and functioning properly.
	The item is disabled.
	One or more settings need to be configured for the item to function properly.

Status Icon	Description
	There is no network connectivity.

Button	Description
	Click this to view your QNAP ID details.
	Click this to sign out of myQNAPcloud.
	Click this to modify your device name.
	Click this to copy the SmartURL to your clipboard.
	Click this to open the myQNAPcloud FAQ page on your browser.
	Click this to diagnose connection problems.
Test	Click this to test the internet connectivity.

Configuring UPnP Port Forwarding

UPnP allows your devices to automatically configure port forwarding settings and discover other devices on the network. Port forwarding is only available if your router supports UPnP.



Warning

Despite its convenience, UPnP may expose your device to public networks. This may allow malicious attackers to access your sensitive data, scan your private networks, and use your devices for DDoS attacks. To ensure your device and data security, we recommend disabling UPnP and manually configuring port forwarding settings on your router.

1. Go to **Auto Router Configuration**.
2. Enable **UPnP Port Forwarding**.
A confirmation message appears.
3. Read the instructions carefully and understand the risks of enabling UPnP.
4. Select **Enable**.
Your device scans for UPnP routers on the network.



Tip

- You can go to **Overview** to verify that there are no connectivity errors.
 - If your device cannot locate the router, click **Rescan**. If the issue persists, click **Diagnostics**, and then verify your network configuration or contact QNAP support through **Helpdesk**.
5. Optional: Add a new service to the **Forwarded Services** table.
 - a. Click **Add NAS Service**.
The **Add NAS Service** window appears.
 - b. Specify a NAS service name that contains 1 to 64 ASCII characters.
 - c. Specify a port number.
 - d. Select an external port setting.
 - **Automatic**: myQNAPcloud automatically selects an available external port.

- **Manual:** You can specify a new port if the current service port is being used by other services.
- e. Select a protocol.
If you are unsure about this setting, select **TCP**.
 - f. Click **OK**.
6. In the **Forwarded Services** table, select the services you want to forward.
 7. Click **Apply to Router**.

Configuring DDNS Settings

1. Open myQNAPcloud.
2. Go to **My DDNS**.
3. Enable **My DDNS**.
4. Perform any of the following tasks.

Task	User Action
Change the myQNAPcloud DDNS domain name	<ol style="list-style-type: none"> a. Click here. The Change Device Name Wizard appears. b. Specify a device name containing up to 30 alphanumeric characters. c. Click Apply.
Update myQNAPcloud	Click Update .
Manually configure the DDNS IP address	<ol style="list-style-type: none"> a. Click Manually configure your DDNS IP address. The Public IP Address window appears. b. Select an option. <ul style="list-style-type: none"> • Assign static IP addresses: myQNAPcloud binds the DDNS to the specified static IP address regardless of changes to the network environment. • Automatically obtain IP address: myQNAPcloud automatically detects the WAN IP. c. Click Apply.

Restarting DDNS Service

DDNS service may sometimes be disabled or suspended due to security concerns. You can restart the DDNS service in myQNAPcloud to regain access to the service.

1. Clear the cache on your web browser.
2. Log on to QuTS hero as administrator.
3. Open myQNAPcloud.
4. Go to **My DDNS**.
5. Disable **My DDNS**.

6. Enable **My DDNS**.

myQNAPcloud DDNS service is restarted and resumed.



Tip

If you still cannot connect to the NAS via myQNAPcloud DDNS, the service may be temporarily blocked by your Internet Service Provider (ISP). Wait at least two hours before attempting to restart the DDNS service.

Configuring Published Services

1. Open myQNAPcloud.
2. Go to **Published Services**.
3. In the **Publish** column, select all the services you want published.
Published services are accessible through the myQNAPcloud website.
4. Optional: In the **Private** column, select all the services you want publish privately.
Private services are only available to specified users with the access code.
 - a. Specify an access code containing 6 to 16 alphanumeric characters.
 - b. In the **User Management** table, select the users you want to grant access to.
You can select a maximum of 9 users.



Tip

Click **Add Users** to add users to the list.
Click **Delete** to remove users from the list.

- c. Optional: Modify user access privileges.

Option	Description
myQNAPcloud Connect (VPN)	Select this option to grant users access to private NAS services when they use the myQNAPcloud Connect utility. Users can download myQNAPcloud Connect from the QNAP Utilities page (https://www.qnap.com/en/utilities/essentials).
myQNAPcloud Website	Select this option to grant users access to private NAS services published in the myQNAPcloud website (https://www.myqnapcloud.com/).

5. Click **Apply**.

Enabling myQNAPcloud Link

1. Open myQNAPcloud.
2. Go to **myQNAPcloud Link**.
3. Enable **myQNAPcloud Link**.




Tip

If there are issues with the connection, click **Reconnect**.

Configuring Device Access Controls

1. Open myQNAPcloud.
2. Go to **Access Control**.
3. Select an access control option.

Option	Description	User Action
Public	All users can search for your device and view the published services on the myQNAPcloud website.	Select Public .
Private	Your device will not appear in the search results. Only you can access your device on the myQNAPcloud website.	Select Private .
Customized	Your device will only be visible to you and invited users. Other users will not be able to access your device even with a SmartURL	<p>a. Select Customized.</p> <p>b. Optional: Add a user.</p> <ol style="list-style-type: none"> 1. Click Add. 2. Specify the user's email address or phone number. 3. Click . <p>c. Optional: Remove a user.</p> <ul style="list-style-type: none"> • From the list of users, identify a user you want to remove. • Click x.

4. Click **Apply**.

Installing an SSL Certificate



Important

myQNAPcloud SSL web service and Let's Encrypt certificates can only be used with the myqnapcloud domain.

1. Open myQNAPcloud.
2. Go to **SSL Certificate**.
3. Download and install a certificate.

Type	Description	User Action
myQNAPcloud SSL web service certificate	This certificate provides a secure environment for exchanging confidential information online and confirms the identity of your site to employees, business partners, and other users. You can purchase certificates on the myQNAPcloud website.	<p>a. Under myQNAPcloud SSL Certificate, click Download and install. The Download & Install SSL Certificate window appears.</p> <p>b. Select a license from the list. A notification appears if you have not yet purchased a myQNAPcloud certificate.</p>
Let's Encrypt certificate	Let's Encrypt is a free, automated, and open certificate authority that issues domain-validated security certificates. You can install Let's Encrypt certificates with the myQNAPcloud DDNS service. You can choose to automatically renew this certificate before it expires.	<p>a. Under Let's Encrypt, click Download and install. The Download & Install SSL Certificate window appears.</p> <p>b. Specify a valid email address. This address is required for the Let's Encrypt account registration.</p> <p>c. Optional: Select Automatically renew domain before expiration.</p>

- 4. Click **Confirm**.**
myQNAPcloud applies the certificate and displays the details.



Tip

To delete the certificate from the device, click **Release** and then **Confirm**.

13. App Center

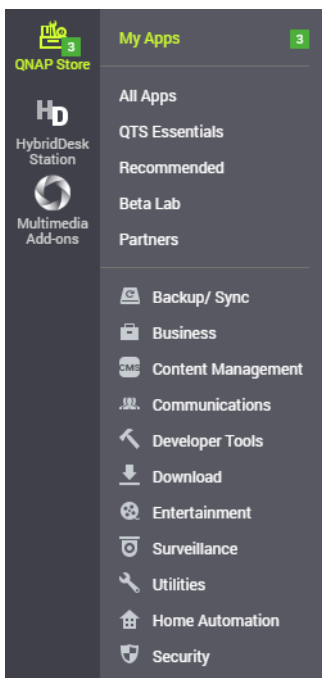
App Center is a digital distribution and management platform in QuTS hero where you can browse, download, and manage applications and utilities developed for the QNAP NAS.

Navigation

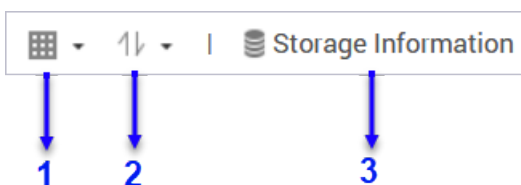
You can view all App Center apps in the left panel or configure a number of settings using the toolbar.

Left Panel

The left panel allows you to browse available apps in various categories. You can go to the **My Apps** section to view all your installed apps. App Center displays a badge count to indicate the number of available updates.




Toolbar



Left side

No.	Elements	Possible User Actions
1	View mode	<ul style="list-style-type: none"> Click the icon to switch between two view modes. Click \wedge and select a view mode.

No.	Elements	Possible User Actions
2	App sorting	Click  and select an app sorting method.
3	Storage information	View the basic storage pool information and the installation locations of your apps. For more storage pool information, click Details .

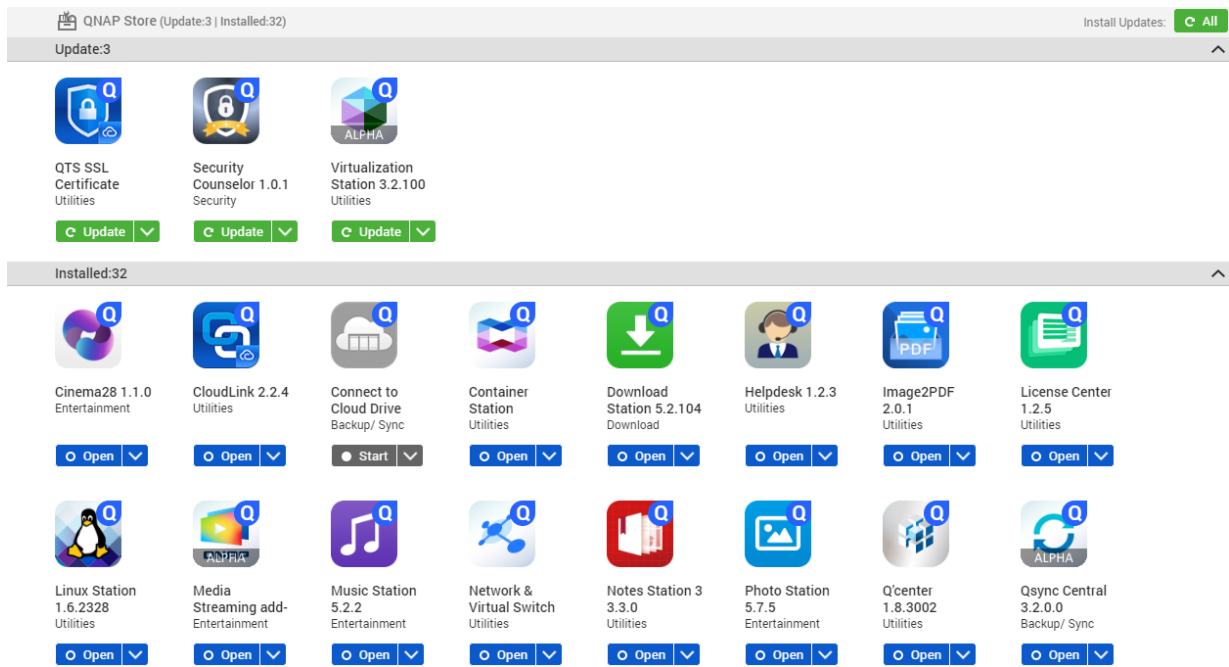


Right side

No.	Elements	Possible User Actions
1	Search	Specify keywords to search for apps. App Center instantly displays search results based on specified keywords.
2	Refresh	Reload the data in App Center to view the current status of your apps.
3	Manual installation	Manually install an app by uploading an installation package. For details, see Installing an App Manually .
4	Settings	Configure various App Center settings. For details, see App Center Settings .
5	More	View the Quick Start or the Help document for more information about App Center.

Main Area

The main area allows you to browse available apps and manage your installed apps. For details, see [App Management](#).



App Management

The App Center allows you to enable or disable an app, assign CPU resources to load-intensive apps, update apps, and configure app update settings.

Viewing App Information

You can browse apps and view their descriptions in the App Center. This helps you decide whether to install or update an app.

1. Open App Center.
2. Locate an app.
3. Click the app icon.
App Center displays the app information in a new window.
4. Perform one of the following actions.
 - View the app description
 - View the digital signature details
 - View the app changelog
 - Go to the QNAP forum
 - View the app tutorial
 - Download the app installation package

Installing an App from App Center



Warning

QNAP recommends only installing apps from the App Center or from the QNAP website. QNAP shall not be held liable for any damages, data loss, or security vulnerabilities resulting from the installation and use of unauthorized apps from untrusted sources.



Important

- Certain apps require activating a subscription or license before app installation. For details, see [Licenses](#).
- Based on the app you choose to install, App Center may display a confirmation message that provides more information and asks for your approval for installation. Certain apps also require you to specify the installation location. Read the message carefully before installing the app.

1. Open App Center.
2. Locate an app.
3. Optional: Click the app icon to view the app information.
4. Select the app update frequency.
5. Click **Install**.
The app is installed.

Installing an App Manually




Warning

- QNAP recommends only installing apps from the App Center or from the QNAP website. QNAP shall not be held liable for any damages, data loss, or security vulnerabilities resulting from the installation and use of unauthorized apps from untrusted sources.
- App Center does not allow the installation of invalid apps, including apps with invalid digital signatures, apps not approved by App Center, or from the [Software Store](#). If App Center detects the app installed is invalid, it will immediately terminate app installation and request you to remove the app.



Important

Certain apps require activating a subscription or license before app installation. You can go to [Software Store](#) to purchase an app license or subscription. For details about activating an app license, see [Licenses](#).

1. Open App Center.
2. Click  on the toolbar.
The **Install Manually** window appears.
3. Click **Browse**.
4. Locate and select the installation package.
5. Click **Install**.

A message appears.

6. Depending on the scenario, perform one of the following actions.

Scenario	Actions
The app has a valid digital signature.	<ol style="list-style-type: none"> a. Read the confirmation message. b. Click OK.
The app does not have a valid digital signature, and you enabled the installation of apps without valid digital signatures.	<ol style="list-style-type: none"> a. Read the confirmation message. b. Click OK.
The app does not have a valid digital signature, and you did not enable the installation of apps without valid digital signatures.	<ol style="list-style-type: none"> a. Read the warning message. b. Select I understand the risks and want to install this application. c. Click Install.



Tip

For more information on this setting, see [Enabling Installation of Apps without Digital Signatures](#).

App Center installs the app.

Updating an App

When updates are available for an installed app, App Center moves the app to the **Update** or **Required Update** section based on the importance of updates. You must perform required updates to ensure the functionality, compatibility, and data security of your apps.

1. Open App Center.
2. Locate an app in the **Update** or **Required Update** section.
3. Click **Update** or **Required Update**.
A confirmation message appears.
4. Click **OK**.

Batch Updating Multiple Apps

1. Open App Center.
2. Perform one of the following updates.

Updates	Action
Only required updates	Below the toolbar, click Required Update .
All available updates	Below the toolbar, click All .

A confirmation message appears.

3. Click **OK**.

Enabling or Disabling an App


You can enable or disable non-built-in apps in App Center.



Note

- Disabling an app may affect the functionality of other apps.
- Disabling an app does not remove or uninstall the app.


1. Open App Center.
2. Locate an app.
3. Perform one of the following actions.

Action	Steps
Enable the app	Click Start .
Disable the app	<ol style="list-style-type: none"> a. Click . b. Select Stop.

- After an app is enabled, its action button displays **Open**.
- After an app is disabled, its action button displays **Start**.


Migrating an App

You can migrate an installed app to another volume to better allocate system resources.

1. Open App Center.
2. Locate an app.
3. Click .
4. Select **Migrate to**.
The **App Migration** window appears.
5. Select the destination volume.
6. Click **Migrate**.
A confirmation message appears.
7. Click **OK**.

Granting or Denying User Access to an App

QuTS hero administrators can grant or deny user access to apps. The main menu of non-administrator users only display the apps that they have access to.

1. Open App Center.
2. Locate an app.
3. Click .

4. Hover the mouse pointer over **Display on**.
5. Select one of the following options:
 - Administrator's main menu

**Note**


This is the only available option for many built-in system utilities, which non-administrators cannot be granted access to.

- Every user's main menu
- Every user's main menu and as an app shortcut on the login screen

Uninstalling an App

**Warning**

Uninstalling an app also deletes the related user data.


1. Open App Center.
2. Locate an app.
3. Click .
4. Select **Remove**.
A confirmation message appears.
5. Click **OK**.

App Center Settings

You can configure the app repository, update settings, and enable installation of apps without digital signatures.

Adding an App Repository

You can add an app repository to enrich the content in App Center. This allows you to download and install apps from third-party sources.

1. Open App Center.
2. Click  on the toolbar.
3. Go to **App Repository**.
4. Click **Add**.
The **Add** window appears.
5. Specify the following connection information.
 - Name
 - URL
6. Optional: Specify the login credentials.
 - Username

- Password

7. Click **Add**.


App Center adds the repository to the list. You can select the repository and then click **Edit** to modify its settings or click **Delete** to remove this repository from App Center.

Configuring App Update Settings



Important

To protect the NAS from security vulnerabilities, QuTS hero by default will check for app updates every day.

1. Open App Center.
2. Click  .
3. Go to **Update**.
4. Select **When updates are available** and then select one of the following options.

Option	Description
Send a notification	QuTS hero sends notification messages when updates are available for your apps. You can click Configure Notification Rule to create rules in Notification Center. For details, see Notification Center .
Install all updates automatically	App Center automatically installs all available updates for your apps. You can select how often App Center should check for available updates.
Install all required updates automatically	App Center automatically installs all required updates for your apps to ensure their functionality, compatibility, and data security. You can select how often App Center should check for required updates.

5. Select an automatic update detection frequency.
6. Click **Apply**.

Digital Signatures

QNAP uses digital signatures to validate apps created by QNAP or QNAP-trusted publishers. The use of digital signatures prevent the unauthorized tampering of apps that may lead to security risks.

A digital signature is considered valid if it meets the following criteria.

- The digital signature has not been tampered with.
- The digital signature has not expired.
- The digital signature is certified by QNAP.

Enabling Installation of Apps without Digital Signatures



Warning

- A valid digital signature ensures that an application was created by QNAP or a QNAP-trusted publisher. It also ensures that the app has not been maliciously tampered with. Installing apps without valid digital signatures may expose your NAS to security risks. QNAP shall not be held liable for any damages, data loss, or security vulnerabilities resulting from the installation and use of such apps.
- App Center does not allow the installation of invalid apps, including apps with invalid digital signatures, apps unapproved by App Center, or from [Software Store](#). If App Center detects the app installed is invalid, it will immediately terminate app installation and request you to remove the app.

1. Open App Center.
2. Click  on the toolbar.
The **Settings** window appears.
3. Go to **General**.
4. Select **Allow installation and execution of applications without a digital signature**.



Important

App Center does not allow the installation of apps with tampered digital signatures even when this setting is enabled.

5. Click **Apply**.

14. Licenses

QNAP licenses enable users to gain access to certain advanced features or premium products. This chapter introduces important concepts and demonstrate essential tasks to help you start using QNAP licenses.

About QNAP Licenses

QNAP offers a wide variety of licenses. Some basic licenses are provided free of charge. You can purchase premium licenses to further enhance the functionality of your QNAP products. QNAP also provides multiple management portals, flexible subscription plans, and various activation options to meet your different needs.

License Types and Plans

The licensing mechanisms and available plans of QNAP licenses vary depending on corresponding software products. They can be divided into the following categories.

License Types

License Types	Description
Device-based	<ul style="list-style-type: none"> Allows users to use a software product installed on hardware devices, such as applications. Multi-seat licenses can be activated and used on multiple devices.
Floating	<ul style="list-style-type: none"> Allows users to use a software product in the cloud or on a virtual platform, such as QuTSCloud and applications in QuTSCloud. Can be activated and used on a limited number of devices at a time
User-based	<ul style="list-style-type: none"> Allows a limited number of authorized users to access a web-based service, such as Qmiix.

License Plans

License Plans	Description
Subscription	Authorizes users to use a software product with a recurring monthly or annual fee
Perpetual	Authorizes users to use a software product indefinitely
One-time	Authorizes users to use a software product within a predefined period of time

Validity Period

The validity period of a QNAP subscription-based license starts from the date of purchase, not from the date of activation.

For example, if a user starts the subscription of an annual license on January 1, 2020, the next billing date will be January 1, 2021, regardless of the date of activation. If the user cancels the subscription, the license will still remain valid until January 1, 2021.

If the user unsubscribes from a license but subscribes to the same product later, the validity period and billing cycle will begin from the date of the new subscription.

License Portals and Utility

Portal	Description	URL
QNAP Software Store	The QNAP Software Store is a one-stop shop where you can purchase licenses for QNAP and QNAP-affiliated software.	https://software.qnap.com
QNAP License Center	The QNAP License Center allows you to monitor and manage licenses of applications running on your local device.	-
QNAP License Manager	QNAP License Manager is a portal that allows you and your organizations to remotely activate and manage licenses under your QNAP ID.	https://license.qnap.com
Old QNAP License Store	Users of QuTS hero 4.3.4 (or earlier) can purchase licenses from this online store.	https://license2.qnap.com

Software Store

Software Store allows you to purchase licenses for applications. Through Software Store, you can perform the following actions.

- Purchase or upgrade licenses
- Manage your account information
- View purchased subscriptions
- Cancel your subscriptions
- Request a refund for your orders

License Center

License Center allows you to monitor and manage the licenses of your applications running on your local device. Through License Center, you can perform the following actions.

- Activate and deactivate licenses either online or offline
- Remove licenses from the local device
- Recover licenses if your device is reset, reinitialized, or restored to factory default
- Transfer licenses purchased from the old QNAP License Store to the new QNAP License Manager

License Manager

License Manager is a portal that allows you to manage all licenses under QNAP IDs and organizations. Through License Manager, you can perform the following actions.

- View details of your licenses
- Activate and deactivate licenses
- Assign a user-based license to a QNAP ID

**Important**

To remotely activate or deactivate licenses, you must enable myQNAPcloud Link on your QNAP device.

Buying a License Using QNAP ID

Before buying a license, ensure the following.

- The application is already installed on your device.
 - You are signed in to myQNAPcloud.
1. Go to <https://software.qnap.com/>.
 2. Sign in with your QNAP ID.
 3. Locate the product on the list, and then click **Buy** or **Subscribe Now**. The license details appear.
 4. Select the item you want to buy, and then review the price.
 5. Click **Checkout Now**.

**Tip**

You can also click **Add to Cart** and then continue shopping.

The purchase summary page appears in your web browser.

6. Select a payment method.

Payment Method	User Action
Credit card	<ol style="list-style-type: none"> a. Specify your card information. b. Verify the items and the price on the order. c. Agree to QNAP terms and conditions. d. Click Place Order.
PayPal	<ol style="list-style-type: none"> a. Verify the items and the price on the order. b. Agree to QNAP terms and conditions. c. Click Pay with PayPal PayPal authentication window appears. d. Specify your PayPal login credentials. e. Click Next. f. Follow PayPal instructions to complete the payment.
Google Pay	<ol style="list-style-type: none"> a. Verify the items and the price on the order. b. Agree to QNAP terms and conditions. c. Click Buy with Google Pay. Google Pay authentication window appears. d. Follow Google Pay instructions to complete the payment.

After the payment, you can view order details in **My Orders** and manage your subscriptions in **My Subscriptions**.

You can activate your license right after the purchase or at a later time.

For details, see [License Activation](#).

License Activation

You need to activate purchased licenses to access features provided by the license. You can activate QNAP or QNAP-affiliated licenses using the following methods.

Activation Method	Description
Using QNAP ID	Licenses purchased through Software Store are stored in your QNAP ID account. They can be accessed through both License Center and the QNAP License Manager website.
Using a license key	You can generate the 25-character license key after purchasing licenses through the QNAP Software Store . For details, see Generating a License Key . You can use license keys to activate licenses in License Center. For details, see Activating a License Using a License Key .
Using a product key	The 25-character product key is purchased together with the product from either QNAP or an authorized reseller. The product key is normally printed on the product package. You can use product keys to activate licenses in License Center. For details, see Activating a License Using a Product Key or PAK .
Using a product authorization key (PAK)	The 24-character PAK is purchased together with the product from either QNAP or an authorized reseller. The product key is normally printed on the product package. If you are using NAS devices running QuTS hero version 4.3.4 or older, use PAKs to activate licenses through License Center. If you are using NAS devices running QuTS hero version 4.3.4 or later, you can transfer PAKs purchased from the Old QNAP License Store to NAS devices. For details, see Activating a License Using a Product Key or PAK .
Offline	Use this method when the NAS is not connected to the internet. For details, see Activating a License Offline .



Activating a License Using QNAP ID


Before activating your license, ensure the following.

- Your device is connected to the internet.
- You are signed in to myQNAPcloud.

Users can activate their licenses using QNAP ID in either Qfinder Pro, License Center, or License Manager.

- Activate your license using one of the following methods.

Method	Steps
Qfinder Pro	<p>Qfinder Pro allows you to discover QNAP devices on your local network.</p> <ol style="list-style-type: none"> a. Open Qfinder Pro on your computer. <p> Tip You can download Qfinder Pro from the QNAP website.</p> <ol style="list-style-type: none"> b. Select your device form the list. c. Right-click the device and select License Activation. d. Specify your device username and password. The License Activation windows appears. e. Select Activate with QNAP ID. f. Click Select License. g. Specify your QNAP ID and password. h. Click Select License. i. Select a license from the list. j. Click Activate. License Server activates the license. A confirmation message appears. k. Click Close. The license is activated for the device.
License Center	<ol style="list-style-type: none"> a. Open License Center. b. Go to My Licenses. c. Click Activate License. The License Activation window appears. d. Select Activate with QNAP ID. e. Click Select License. f. Select a license from the list. <p> Tip If you select a multi-seat license, you can specify the number of seats that you want to activate.</p> <ol style="list-style-type: none"> g. Click Add. License Center activates the license. A confirmation message appears. h. Click Close. The license appears on the list of active licenses.

Method	Steps
License Manager	<ul style="list-style-type: none"> a. Open your web browser. b. Go to https://license.qnap.com. c. Sign in with your QNAP ID. d. Locate a license from the license list. e. Click . The Activate License window appears. f. Select Online Activation. g. Select a device. h. Specify your credentials on the device. i. Click Allow. A confirmation message appears. j. Click OK. License Manager activates the license. k. Click Close. The license appears on the list of active licenses.

Activating a License Using a License Key

Before activating your license, ensure that your device is connected to the internet and you have signed in with your QNAP ID.

You can activate a license using a license key. After purchasing a license from QNAP Software Store, you can generate a license key from the License Manager website and apply the key in License Center. A license key contains 25 characters and always starts with the letter L.

For details, see [Generating a License Key](#).

1. Open License Center.
2. Go to **My Licenses**.
3. Click **Activate License**. The **License Activation** window appears.
4. Select **Activate with a License Key**.
5. Specify the key.
6. Read and agree to the terms of service.
7. Click **Verify Key**.
8. Verify the license information.
9. Optional: Specify the number of seats to activate.




Note

This option is only available for licenses that support multiple seats.

10. Click **Activate**.
The license is activated.
A confirmation message appears.
11. Click **Close**.
The license appears on the list of active licenses.


Generating a License Key

1. Open your web browser.
2. Go to <https://license.qnap.com>.
3. Sign in with your QNAP ID.
4. From the list of licenses, select the license you want to generate a key for.
5. Click .
The **Activate License** window appears.
6. Select **License Key**.
License Manager generates the license key.



Tip

Click **Renew License Key** to generate a new key.
This renews your license key and protects you from any unauthorized access to your existing license key.

7. Hover the mouse pointer over the license key and click .
Your system copies the license.
8. Click **Done**.

The copied license key can be pasted later for license activation.

Activating a License Using a Product Key or PAK

Before activating a license using a product key or a product authorization key (PAK), ensure the following.

- Your NAS is connected to the internet.
- You are signed in to myQNAPcloud.

You can activate a license with a product key or PAK. You may find a product key printed on a physical copy of your product. A product key contains 25 characters and always starts with the letter P.

On the other hand, you may obtain a product authorization key (PAK) if you purchase a license from the old QNAP License Store. A PAK contains 24 digits of random numbers.


1. Open License Center.
2. Go to **My Licenses**.
3. Click **Activate License**.
4. The **License Activation** window appears.
5. Select **Activate with a Product Key or PAK**.

6. Specify the key.
7. Read and agree to the terms of service.
8. Click **Verify Key**.
9. Verify the license information.
10. Click **Activate**.
The license is activated.
A confirmation message appears.
11. Click **Close**.
The license appears on the list of active licenses.


Activating a License Offline

You can activate your license offline if your QNAP device is not connected to the Internet. You first need to generate a device identity file (DIF) from Qfinder Pro or from License Center on your device and then upload the DIF to License Manager in exchange for the license install file (LIF). You can then activate the license using the LIF in Qfinder Pro or in License Center on your device.

1. Choose one of the following methods.

Methods	User Action
Offline activation using Qfinder Pro	<p>Qfinder Pro allows you to discover QNAP devices on your local network.</p> <ol style="list-style-type: none"> a. Open Qfinder Pro on your computer. <div style="display: flex; align-items: center; margin-bottom: 10px;">  <div> <p>Tip</p> <p>You can download Qfinder Pro from the QNAP website.</p> </div> </div> <ol style="list-style-type: none"> b. Select your device from the list. c. Right-click the device and then select License Activation. d. Specify your username and password. The License Activation window appears. e. Select Offline Activation.
Offline activation using License Center	<ol style="list-style-type: none"> a. Log in to your QNAP device. b. Open License Center. c. Go to My Licenses. d. Click Activate License. The License Activation window appears. e. Select Offline Activation.

2. Read and agree to the Terms of Service.
3. Click **Generate Device Identity File**.
Qfinder Pro or License Center downloads the device identity file (DIF) to your computer.

4. Read the instructions and click **Go to License Manager**.
Your web browser opens the **QNAP License Manager** website.
5. Sign in with your QNAP ID.
6. From the list of licenses, select the license you want to activate.
7. Click  (**Upload Device Identity File**).
The **Activate License** window appears.
8. Click **Browse**.
The file browser appears.
9. Locate and select the DIF from your computer.
10. Click **Upload**.
A confirmation message appears.
11. Click **Download**.
QNAP License Manager downloads the license install file (LIF) to your computer.
12. Click **Done**.
13. Go back to Qfinder Pro or License Center.
14. In the **License Activation** window, click **Upload License File**.
15. Click **Browse**.
The file browser appears.
16. Locate and select the LIF from your computer.
17. Click **Import**.
Qfinder Pro or License Center uploads the LIF and displays the license summary.
18. Click **Activate**.
The license appears on the list of active licenses.

License Deactivation

You can deactivate QNAP or QNAP-affiliated licenses using the following methods.

Activation Method	Description
Using QNAP ID	Licenses purchased through Software Store are stored in your QNAP ID account, and can be accessed through both License Center and the QNAP License Manager website To deactivate this type of license, see Deactivating a License Using QNAP ID .
Offline	Use this method when the NAS is not connected to the internet. For details, see Deactivating a License Offline .

Deactivating a License Using QNAP ID



Before deactivating your license, ensure the following.

- Your device is connected to the internet.


- You are signed in to myQNAPcloud.

Users can deactivate their licenses using QNAP ID in either License Center or License Manager.


- Deactivate your license using one of the following methods.

Method	Steps
License Center	<ol style="list-style-type: none"> a. Open License Center. b. Go to My Licenses. c. Identify the license you want to deactivate, and then click . The License Deactivation window appears. d. Select Use QNAP ID. e. Read and acknowledge the warning. f. Click Deactivate. A confirmation message appears. g. Click Close. License Center deactivates the license and removes the license from the list of active licenses.
License Manager	<ol style="list-style-type: none"> a. Open your web browser. b. Go to https://license.qnap.com. c. Sign in with your QNAP ID. d. From the list of licenses, select the license you want to deactivate. e. Click . The Deactivate License window appears. f. Read and acknowledge the warning. g. Click Deactivate. License Center deactivates the license. A confirmation message appears. h. Click Close. License Center removes the license from the list of active licenses.

Deactivating a License Offline

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to deactivate, and then click . The **License Deactivation** window appears.
4. Select **Offline Deactivation**.
5. Read and acknowledge the warning.
6. Read the instructions, and then click **Generate License Uninstall File**.

License Center downloads the license uninstall file (LUF) to your computer.

7. Open your web browser.
8. Go to <https://license.qnap.com>.
9. Sign in with your QNAP ID.
10. From the list of licenses, select the license you want to deactivate.
11. Under **Advanced Options**, click . The **Deactivate License** window appears.
12. Read and agree to the terms.
13. Click **Offline Deactivation**.
14. Click **Browse**. The file browser appears.
15. Locate and select the LUF from your computer.
16. Click **Upload**. QNAP License Manager deactivates the license. A confirmation message appears.
17. Click **Done**.

License Extension

License Center will notify you soon before any of your subscription-based licenses expire. The exact dates vary depending on the type of your licenses (ranging from one week to one month before the expiration date). You can extend your QNAP or QNAP-affiliated licenses using the following methods.

Activation Method	Description
Using QNAP ID	Licenses purchased through License Center or Software Store are stored in your QNAP ID account, and can be accessed through both License Center and the QNAP License Manager website. If you have an existing valid, unused subscription-based license in License Center, you can use this to extend your expiring license. For details, see Extending a License Using QNAP ID .
Offline using an unused license	If you have a valid, unused subscription-based license and your NAS is not connected to the internet, you can use this method to extend your expiring license. For details, see Extending a License Offline Using an Unused License .
Offline using a product key	The 25-character product key is purchased together with the product from either QNAP or an authorized reseller. The product key is normally printed on the product package. If you have a valid, unused product key for a subscription-based license, and your NAS is not connected to the internet, you can use this method to extend your expiring license. For details, see Extending a License Offline Using a Product Key .

Extending a License Using QNAP ID

Before extending licenses, ensure the following.

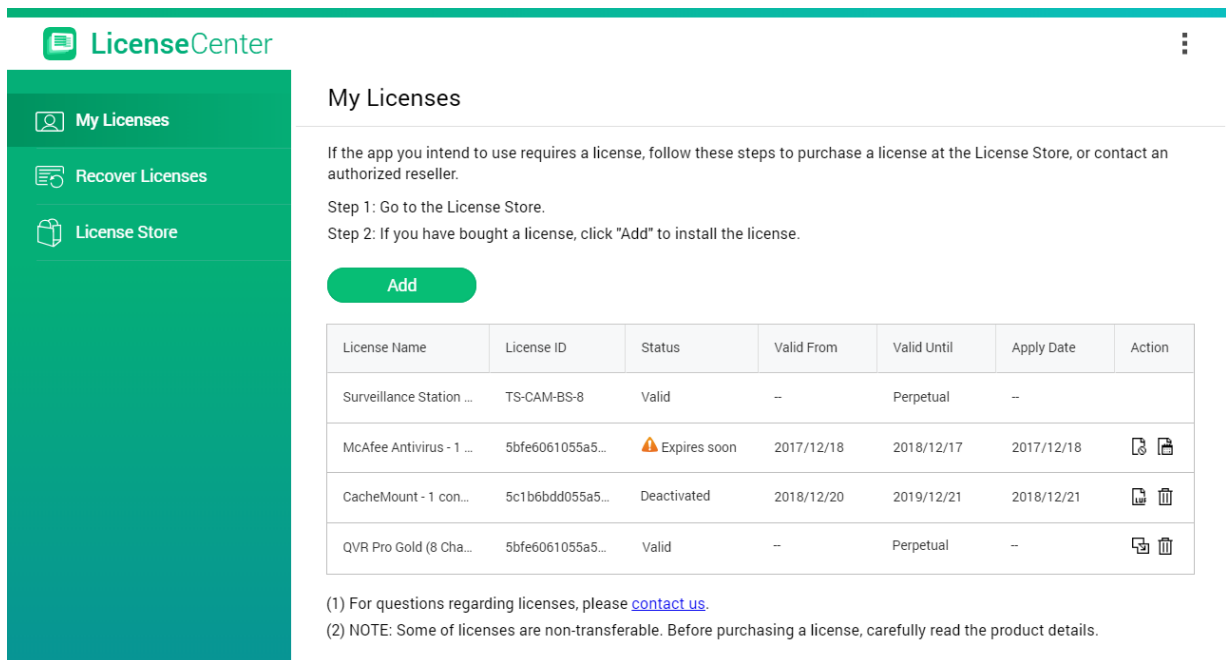
- Your device is connected to the internet.
- You are signed in to myQNAPcloud.
- You have an existing valid, unused license.



Note

Subscription-based licenses will be automatically renewed in License Manager. You cannot manually extend a subscription-based license.

1. Open License Center.
2. Go to **My Licenses**.



3. Identify the license you want to extend, and then click .



Tip

If a license is expiring in 30 days or less, its status is `Expires soon`.

The **License Extension** window appears.

License Extension ✕

Select the license you want to extend, Once the selected license is used to extend your current license, it will be removed from license list. Note: You can also [manually extend a license](#).

Warning: This action is irreversible.

License Name	License ID	Valid From	Valid Until
McAfee Antivirus - 2 years	5bfe6061055a53131f8c67c6	2018/11/28	--
McAfee Antivirus - 2 years	5bfe6061055a53131f8c67c9	2018/11/28	--
McAfee Antivirus - 2 years	5bfe6061055a53131f8c67cc	2018/11/28	--
McAfee Antivirus - 1 year	5bfe6061055a53131f8c67cf	2018/11/28	--

⏪ ⏩ | Page /1 | ⏪ ⏩ | ↻
Display item: 1-4, Total: 4

Extend
Close

4. Select an unused license.



Warning

License Center will use this license to extend your expiring license. This process is irreversible. Once this license is used for extension, you cannot use it for anything else.

5. Click **Extend**.
License Center extends the license.
A confirmation message appears.
6. Click **Close**.

Extending a License Offline Using an Unused License

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to extend, and then click



Tip

If a license is about to expire, its status is `Expires soon`.

The **License Extension** window appears.

4. Select **manually extend a license**.
5. Select **Extend offline**.

6. Click **Next**.
7. Read the instructions, and then click **Download**.
License Center downloads the device identity file (DIF) file to your computer.
8. Read and agree to the terms of service.
9. Click **Next**.
10. Read the instructions, and then click **Go to License Manager**.
Your web browser opens the QNAP License Manager website.
11. Sign in with your QNAP ID.
12. Go to **My Licenses**.
13. From the list of licenses, select the license you want to activate.
14. In the table below, click **Activation and Installation**.
The license activation details appear.
15. Click **Extend on QuTS Hero**.
The **Extend License** window appears.
16. Select **Use an unused license**, and then click **Next**.
The list of unused licenses appears.
17. Select an unused license.

**Warning**


License Center will use this license to extend your expiring license. This process is irreversible. Once this license is used for extension, you cannot use it for anything else.

18. Click **Next**.
19. Click **Browse**.
The file browser appears.
20. Locate and select the DIF from your computer.
21. Click **Upload**.
A confirmation message appears.
22. Click **Download**.
QNAP License Manager downloads the license install file (LIF) to your computer.
23. Click **Done**.
24. Go back to License Center.
25. In the **License Extension** window, click **Next**.
26. Click **Browse Files**.
The file browser appears.
27. Locate and select the LIF from your computer.
28. Click **Next**.
License Center uploads the LIF and displays the license summary.
29. Click **Extend**.

A confirmation message appears.

30. Click **Close**.
The license appears on the list of active licenses.

Extending a License Offline Using a Product Key

1. Open License Center.
2. Go to **My Licenses**.
3. Identify the license you want to extend, and then click .



Tip

If a license is about to expire, its status is `Expires soon`.

The **License Extension** window appears.

4. Click **manually extend a license**.
5. Select **Extend offline**.
6. Click **Next**.
7. Read the instructions, and then click **Download**.
A notification message appears.
8. Click **Download**.
License Center downloads the device identity file (DIF) file to your computer.
9. Read and agree to the terms of service.
10. Click **Next**.
11. Read the instructions, and then click **Go to License Manager**.
Your web browser opens the QNAP License Manager website.
12. Sign in with your QNAP ID.
13. Go to **My Licenses**.
14. From the list of licenses, select the license you want to activate.
15. In the table below, click **Activation and Installation**.
The license activation details appear.
16. Click **Extend on QuTS Hero**.
The **Extend License** window appears.
17. Select **Use a product key**, and then click **Next**.
18. Specify the product key.
19. Click **Next**.
A confirmation message appears.
20. Click **Download**.
QNAP License Manager downloads the license install file (LIF) to your computer.
21. Click **Done**.



22. Go back to License Center.
23. In the **License Extension** window, click **Next**.
24. Click **Browse Files**.
The file browser appears.
25. Locate and select the LIF from your computer.
26. Click **Next**.
License Center uploads the LIF and displays the license summary.
27. Click **Extend**.
A confirmation message appears.
28. Click **Close**.
The license appears on the list of active licenses.

Upgrading a License

Before upgrading a license, ensure the following.

- The application is already installed on your device.
- You are signed in to myQNAPcloud.


Users can upgrade their existing basic licenses to premium licenses to gain access to advanced features.

1. Open your web browser.
2. Go to <https://software.qnap.com>.
3. Click your account name and select **MY ACCOUNT**.
4. Click **Upgrade Plans**.
A list of upgradable subscriptions is displayed.
5. From the list of subscriptions, find the license you want to upgrade and click **Upgrade**.
The **Current Plan** window appears.
6. From the list of upgrade plans, select an upgrade and click **Add to Cart**.
7. Click .
Click .
8. Click **GO TO CHECKOUT**.
9. Select a payment method.

Payment Method	User Action
Credit card	<ol style="list-style-type: none"> a. Specify your card information. b. Verify the items and the price on the order. c. Agree to QNAP terms and conditions. d. Click Place Order.

Payment Method	User Action
PayPal	<ul style="list-style-type: none"> a. Verify the items and the price on the order. b. Agree to QNAP terms and conditions. c. Click Pay with PayPal PayPal authentication window appears. d. Specify your PayPal login credentials. e. Click Next. f. Follow PayPal instructions to complete the payment.
Google Pay	<ul style="list-style-type: none"> a. Verify the items and the price on the order. b. Agree to QNAP terms and conditions. c. Click Buy with Google Pay. Google Pay authentication window appears. d. Follow Google Pay instructions to complete the payment.

10. Apply the license upgrade to your QNAP device.

- a.** Open your web browser.
- b.** Go to <https://license.qnap.com>.
- c.** Sign in with your QNAP ID.
- d.** Locate the license from the license list.
- e.** Click  .
The **Activate Upgraded License** window appears.
- f.** Select **Online Activation**
- g.** Click **Next**.
- h.** Specify your credentials on the device.
- i.** Click **Allow**.
A confirmation message appears.
- j.** Click **Close**.

The upgraded license is activated.

Viewing License Information

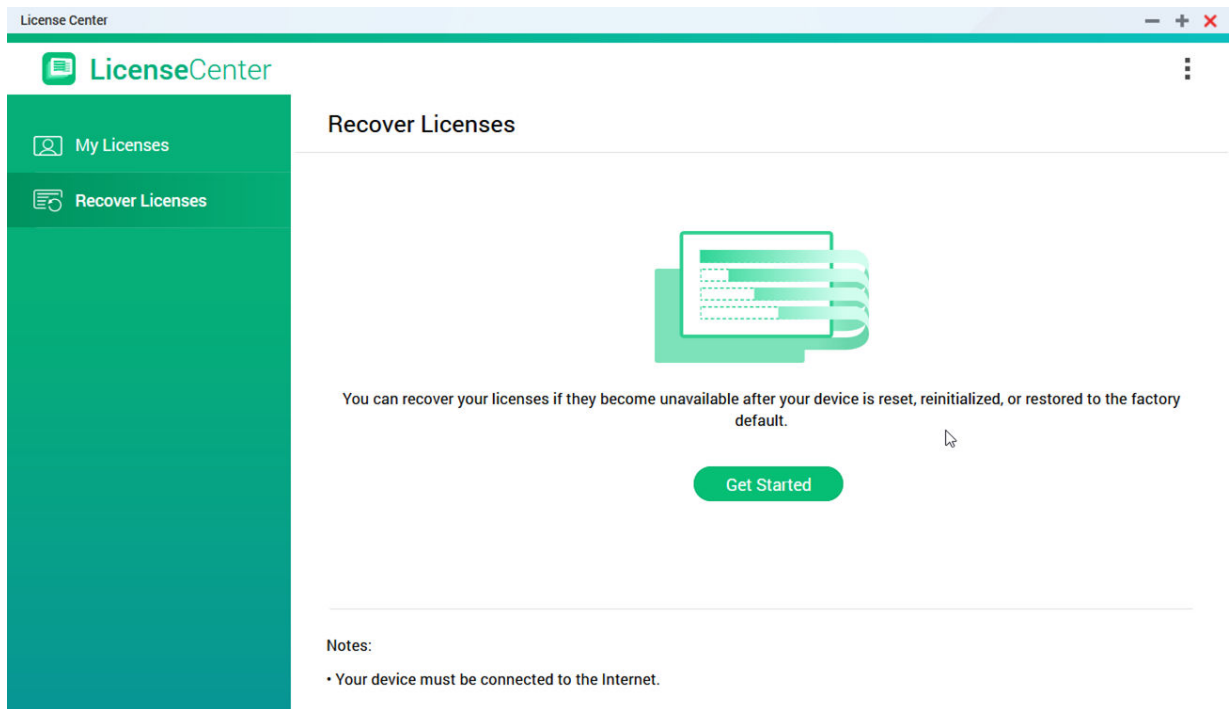
1. Open your web browser.
2. Go to <https://license.qnap.com>.
3. Sign in with your QNAP ID.
4. View the license information using one of the following modes.

Viewing Mode	User Actions
List by Device	<p>This mode displays all the activated licenses on each device. This allows you to quickly view and manage your licenses on a specific device.</p> <ul style="list-style-type: none"> • Click a device and then click Device Details to view the details of the selected device. • Click a device and then click Activation and Installation to view the details of your licenses. You can also activate or deactivate licenses.
List by License	<p>This mode displays your purchased licenses and their details, including available seats, license types, validity period, and status.</p> <ul style="list-style-type: none"> • Click a license and then click License Details to view the details. • Click a license and then click Activation and Installation to view the details. You can also activate licenses, deactivate licenses, download the license file, or upload the device identity file. • Click a license and then click Usage Record to view the history of the selected license.
List by Product	<p>This mode displays your purchased licenses for each product. This allows you to view and manage all related licenses designed for the same product.</p> <ul style="list-style-type: none"> • Click a product to view the details of your licenses. You can also activate licenses, deactivate licenses, download the license file, or upload the device identity file.

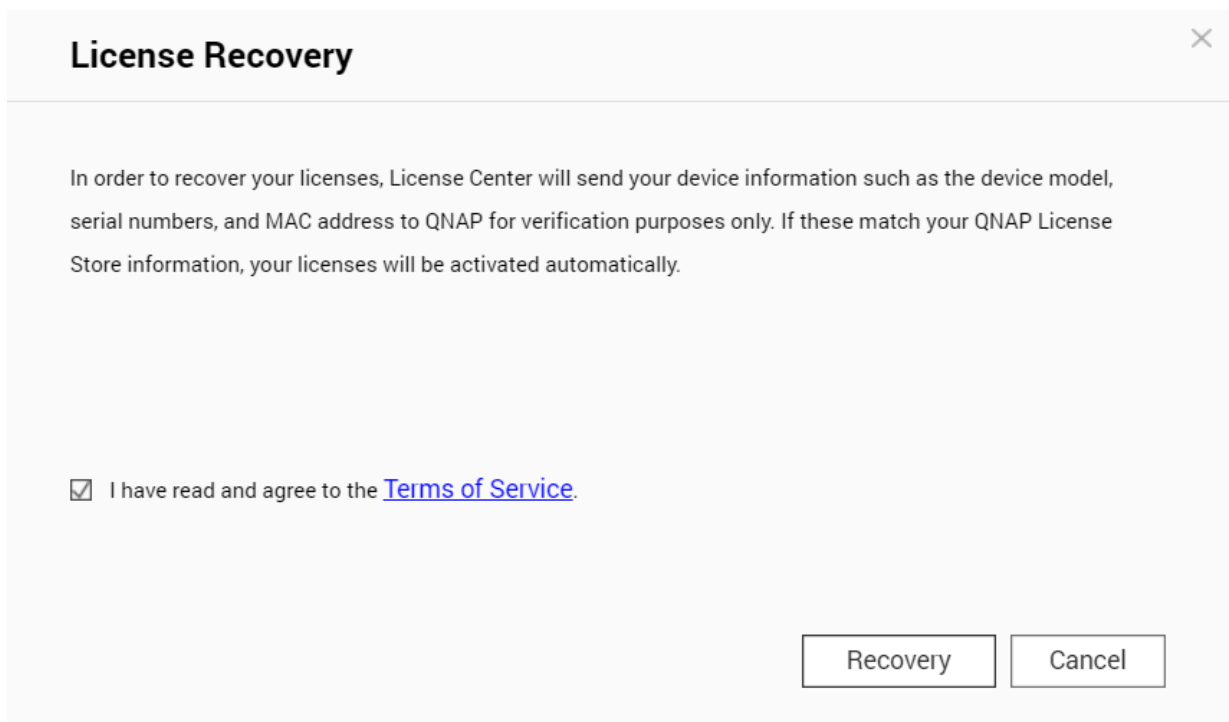
Recovering Licenses

Before recovering licenses, ensure that your device is connected to the internet.

1. Open License Center.
2. Go to **Recover Licenses**.



3. Click **Get Started**.
The **License Recovery** dialog box appears.



4. Read and agree to the terms of service.
5. Click **Recovery**.
License Center automatically recovers all available licenses for applications installed on your devices.

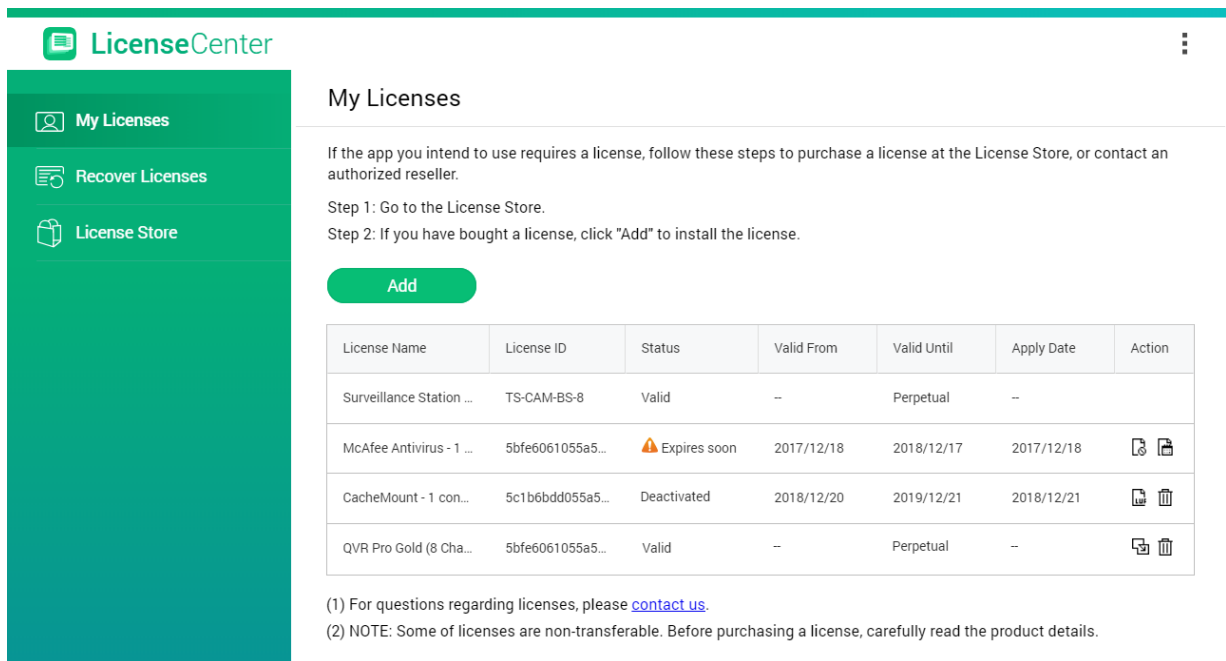
Transferring a License to the New QNAP License Server

This task only applies to existing licenses that have been activated using PAK.

Before transferring licenses, ensure the following.

- Your NAS is connected to the internet.
- You are signed in to myQNAPcloud.

1. Open License Center.
2. Go to **My Licenses**.



3. Identify the license you want to transfer, and then click . A confirmation message appears.

4. Read the terms of service, and then click **Transfer & Activate**.



Warning

After you register a license with your current QNAP ID, it will no longer be transferable.

License Center transfers the license.
A confirmation message appears.

5. Optional: Click **QNAP License Manager** to review the license details.
6. Click **Close**.

Deleting a License

Before deleting a license, ensure that you have deactivated this license.

1. Open License Center.

2. Go to **My Licenses**.

My Licenses

If the app you intend to use requires a license, follow these steps to purchase a license in the QNAP Software Store or contact authorized resellers.

Step 1: Go to the [Software Store](#).

Step 2: If you have bought a license, click "Add" to install the license.

Add

License Name	License ID	Status	Valid From	Valid Until	Apply Date	Action
Surveillance Station - 8 E...	TS-CAM-BS-8	Valid	-	Perpetual	-	
Test - 1 days	5ea7e866055a537cd4f0...	Expired	2020/04/28	2020/05/01	2020/04/28	
[DQV] HybridMount - 1 fil...	5ea7df07055a537cd4f0...	Expired	2020/04/28	2020/04/29	2020/04/28	
Test - 1 days (9)	5eaf7fd3055a530769f5a...	Expired	2020/05/04	2020/05/05	2020/05/04	
[DOV] HybridMount - 1 fil...	5ea693ca055a537cd5f0...	Deactiva...	2020/04/27	2020/05/27	2020/04/27	...

(1) For questions regarding licenses, please [contact us](#).

(2) NOTE: Some of licenses are non-transferable. Before purchasing a license, carefully read the product details.

3. Identify the license you want to delete, and then click . A confirmation message appears.

4. Click **Yes**. License Center deletes the license.



Tip

If the license has not yet expired, the license will still be listed in the **License Activation** table.

15. Multimedia

QuTS hero provides a range of applications and utilities for viewing, playing, and streaming multimedia files stored on the NAS.

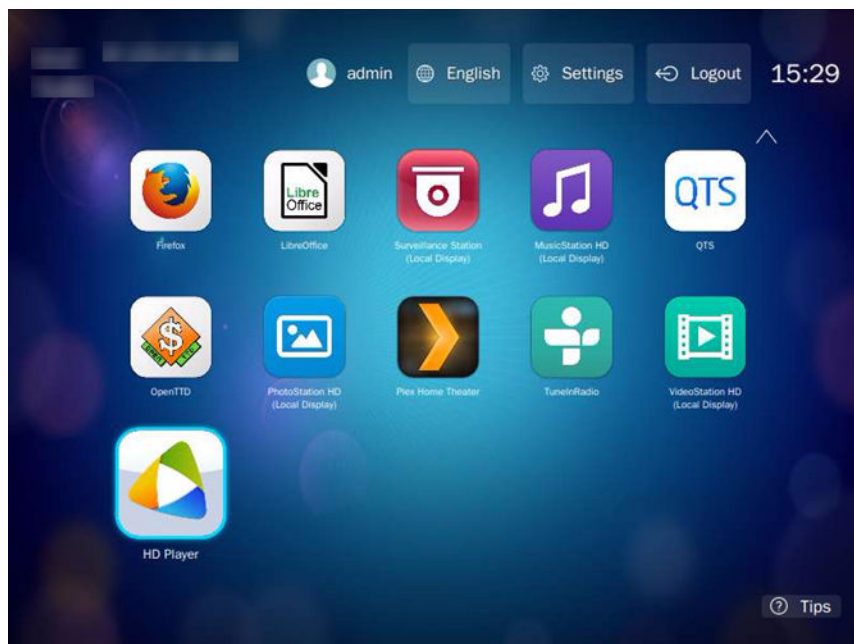
Application/Utility	Description
HybridDesk Station (HD Station)	Connect to an HDMI display to access multimedia content on your NAS.
DLNA Media Server	Configure your NAS as a Digital Living Network Alliance (DLNA) server to access media files on your NAS from devices on your home network.
Media Streaming Add-on	Stream media from your NAS to DLNA, Chromecast, and HDMI-connected devices.
Multimedia Console	Manage multimedia apps and content on the NAS. You can index files, transcode videos, and generate thumbnails for multimedia content.

HybridDesk Station (HD Station)

HybridDesk Station (HD Station) allows you to connect to an HDMI display and directly access multimedia content and use other applications on your NAS. You can use your NAS as a home theater, multimedia player, or desktop substitute. After installing HD Station and connecting the NAS to an HDMI display, you can navigate your NAS using HD Station.

HD Station requires:

- A TV or monitor with an HDMI port
- A mouse, keyboard, or remote control for navigation
- A graphics card (some NAS models only). Go to <https://www.qnap.com> to check the software specifications for your NAS and verify that it is compatible with HD Station.



Installing HD Station

1. Go to **Control Panel > Applications > HDMI Display Applications** .
2. Choose one of the following installation methods.

Installation Method	Steps
Guided installation	<ol style="list-style-type: none"> a. Click Get Started Now. The HybridDesk Station window appears. b. Review the list of selected applications. <div style="display: flex; align-items: center; margin-top: 10px;"> <div> <p>Tip All applications are selected by default. You can deselect applications that you do not want to install.</p> </div> </div> <ol style="list-style-type: none"> c. Click Apply.
Manual installation	<ol style="list-style-type: none"> a. Under Install Manually, click Browse. b. Select HD Station. c. Click Install.

QuTS hero installs HD Station and the selected applications.





Note

Multimedia Services must be enabled to play multimedia content in HD Station. Go to **Main Menu > Applications > Multimedia Console** to enable Multimedia Services. HD Player, Photo Station, Music Station, and Video Station must also be installed on the NAS to play multimedia content from the respective applications.

Configuring HD Station

1. Go to **Control Panel > Applications > HDMI Display Applications > Local Display settings** .
2. Perform any of the following actions.

Action	Steps
Enable HD Station	<p>Click Enable.</p> <div style="display: flex; align-items: center; margin-top: 10px;"> <div> <p>Note HD Station must be disabled to perform this action.</p> </div> </div>
Disable HD Station	<p>Click Disable.</p> <div style="display: flex; align-items: center; margin-top: 10px;"> <div> <p>Note HD Station must be enabled to perform this action.</p> </div> </div>
Install all HD Station applications	<ol style="list-style-type: none"> a. Click Install All Apps. A dialog box appears. b. Click OK.
Update installed apps	Click Update .
Restart HD Station	Click Restart .

Action	Steps
Remove HD Station and related applications	<p>a. Click Remove. A dialog box appears.</p> <p>b. Click OK.</p>
Edit HD Station settings	<p>a. Click Settings. The Settings window appears.</p> <p>b. Modify any of the following settings:</p> <ul style="list-style-type: none"> • Output resolution: Change the resolution of HD Station. • Overscan: Reduce the visible area of a video displayed in HD Station. • Enable Remote Desktop: View the NAS HDMI output using your web browser. <p> Note</p> <ul style="list-style-type: none"> • Enabling Remote Desktop may affect the playback quality of local videos. • You must restart Remote Desktop after changing the output resolution. <p> Tip You can also open and restart Remote Desktop from this screen.</p>
Install HD Station apps	<p>a. Under Install Manually, click Browse.</p> <p>b. Select the application.</p> <p>c. Click Install.</p>

HD Station Applications

Go to **App Center > HybridDesk Station** to install or configure applications used with HD Station.

Using HD Player in HD Station

You can use HD Player to browse and play multimedia content in Photo Station, Music Station, and Video Station.

1. Connect an HDMI display to the NAS.
2. Select your NAS account.
3. Specify your password.
4. Start HD Player.
5. Select your NAS account.
6. Specify your password.

DLNA Media Server

You can configure your NAS as a Digital Living Network Alliance (DLNA) server, allowing you to access media files on your NAS through your home network using DLNA devices such as TVs, smartphones, and computers.

The contents displayed in DLNA Media Server are based on user account permissions and Multimedia Console settings.



Important

- You must enable Multimedia Services before using DLNA Media Server. Go to **Control Panel > Applications > Multimedia Console > Overview** to enable Multimedia Services.
- The first time you enable DLNA Media Server, QuTS hero automatically installs the Media Streaming Add-on if it is not already installed on the NAS. For details, see [Media Streaming Add-on](#).

Enabling DLNA Media Server

You can configure your NAS as a DLNA server, allowing you to access media files on your NAS through your home network using DLNA devices such as TVs, smartphones, and computers.

The contents displayed in DLNA Media Server are based on user account permissions and Multimedia Console settings.



Important

The first time you enable DLNA Media Server, QuTS hero automatically installs the Media Streaming Add-on if it is not already installed on the NAS. For details, see [Media Streaming Add-on](#).

1. Go to **Control Panel > Applications > DLNA Media Server**.
2. Select **Enable DLNA Media Server**.
3. Optional: Specify the following information.


Field	Description
Service Name	Specify a name for the DLNA Media Server.
Select default user account	Select the user account that will be the directory for the DLNA Media Server.

4. Click **Apply**.

Configuring DLNA Media Server

1. Go to **Control Panel > Applications > DLNA Media Server**.
2. Perform any of the following actions.

Action	Steps
Scan for multimedia content	Click Scan now .
Restart DLNA Media Server	Click Restart .

Action	Steps
Configure advanced settings	<p>a. Click Advanced Settings. The Media Streaming Add-on portal opens in a new browser window.</p> <p>b. Configure the settings.</p> <p> Note Media Streaming Add-on must be installed to configure advanced settings. For details, see Media Streaming Add-on.</p>

Media Streaming Add-on

Media Streaming Add-on allows you to stream media from your NAS to different DLNA, Chromecast, and HDMI-connected devices simultaneously using the following QuTS hero multimedia applications:

- File Station
- Photo Station
- Music Station
- Video Station

Go to App Center to install Media Streaming Add-on.



Tip

You can restart Media Streaming Add-on anytime by clicking **Restart** on the home screen.

Configuring General Settings


1. Open **Media Streaming Add-on**.
Media Streaming Add-on opens in a new tab.



Note

Media Streaming Add-on logs you in based on your QuTS hero user credentials. If a login screen appears, you will need to specify your username and password to log in.

2. Go to **General Settings**.
3. Modify any of the following settings.

Setting	Description
Service name	This is the name that devices on the local network will see when connecting to the NAS.
Default user account	Select the user account that media devices receive content from. To connect using a different user account, you must specify the account's username and password in the connection settings of the media receiver.
Network interface	Select the network interface.
Port	Specify the port number.
Menu language	Select the language displayed for menu items.
Default menu style	Select the type of menu style. <ul style="list-style-type: none"> • Simple • All categories • Custom Select one of the Custom options and click Customize to configure the display options for the menu.
Always stream videos to Apple TV and Chromecast in original file formats	When selected, the NAS streams videos to these devices without transcoding or embedding subtitles. <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;">  <p>Important Ensure that Apple TV and Chromecast support the file formats of videos on your NAS when selecting this option.</p> </div>

4. Click **Apply All**.

Configuring Browsing Settings

1. Open **Media Streaming Add-on**.
Media Streaming Add-on opens in a new tab.



Note

Media Streaming Add-on logs you in based on your QuTS hero user credentials. If you see a login screen, you will need to specify your username and password and log in.

2. Go to **Browsing Settings**.
3. Modify any of the following settings.

Setting	Description
Display Photo	Select the display size of the thumbnail for photo albums.
Music title display style	Select the type of information that is displayed for music files.

Setting	Description
Video title display style	Select whether video titles display the file name of the video or the embedded information.

4. Click **Apply All**.

Configuring Media Receivers

1. Open **Media Streaming Add-on**.
Media Streaming Add-on opens in a new tab.



Note

Media Streaming Add-on logs you in based on your QuTS hero user credentials. If you see a login screen, you will need to specify your username and password and log in.

2. Go to **Media Receivers**.
3. Perform any of the following actions.

Action	Steps
Enable device sharing	Select Enable sharing for new media receivers automatically . When enabled, newly discovered devices will automatically be allowed to connect to DLNA Media Server.
Scan for new devices	Click Scan for devices Media Streaming Add-on searches for new media devices connected to the NAS.
Modify device connections	Select or deselect media devices. Only selected devices can connect to DLNA Media Server.

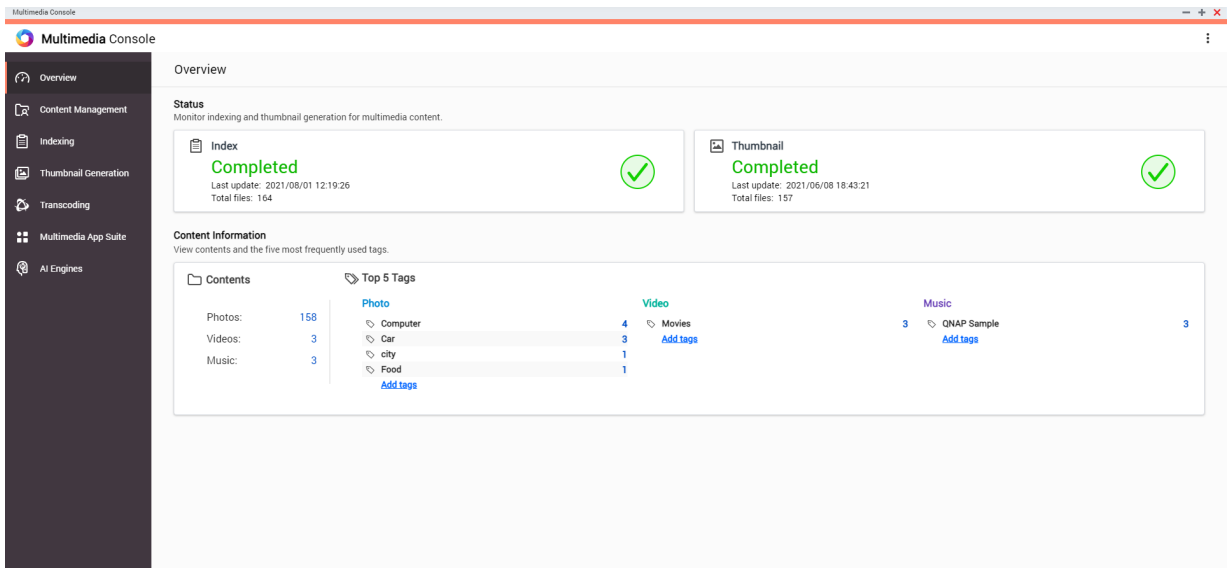
4. Click **Apply All**.

Multimedia Console

Multimedia Console helps you manage installed multimedia apps and content stored on the NAS. Multimedia Console can index files, transcode videos, and generate thumbnails for apps and system services such as Photo Station, Video Station, Music Station, and DLNA Server.

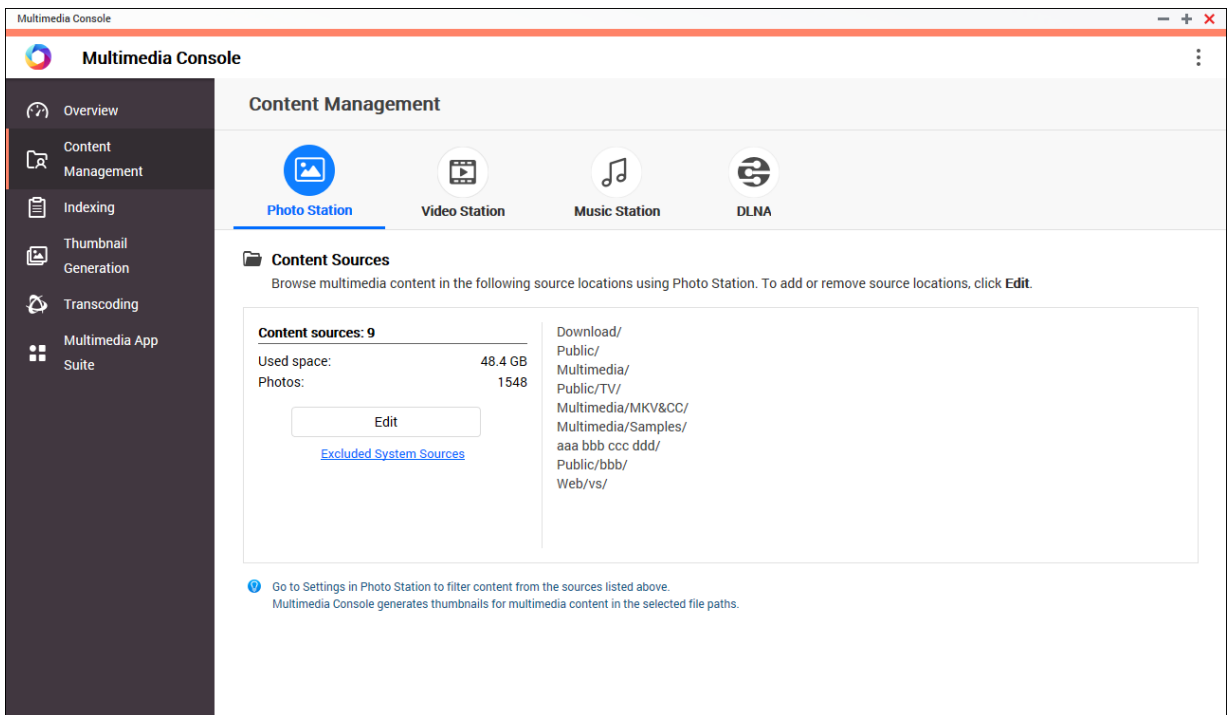
Overview

The **Overview** screen displays the indexing and thumbnail generation status for multimedia files as well as the total number of photos, videos, and music files on your NAS



Content Management

The **Content Management** screen displays the content source folders for multimedia apps installed on the NAS. You can view and edit the content source folders for apps and system services such as Photo Station, Video Station, Music Station, and DLNA Media Server.



Editing Content Sources

The **Content Management** screen displays the content source folders for multimedia apps installed on the NAS. You can view and edit the content source folders for apps and system services such as Photo Station, Video Station, Music Station, and DLNA Media Server.

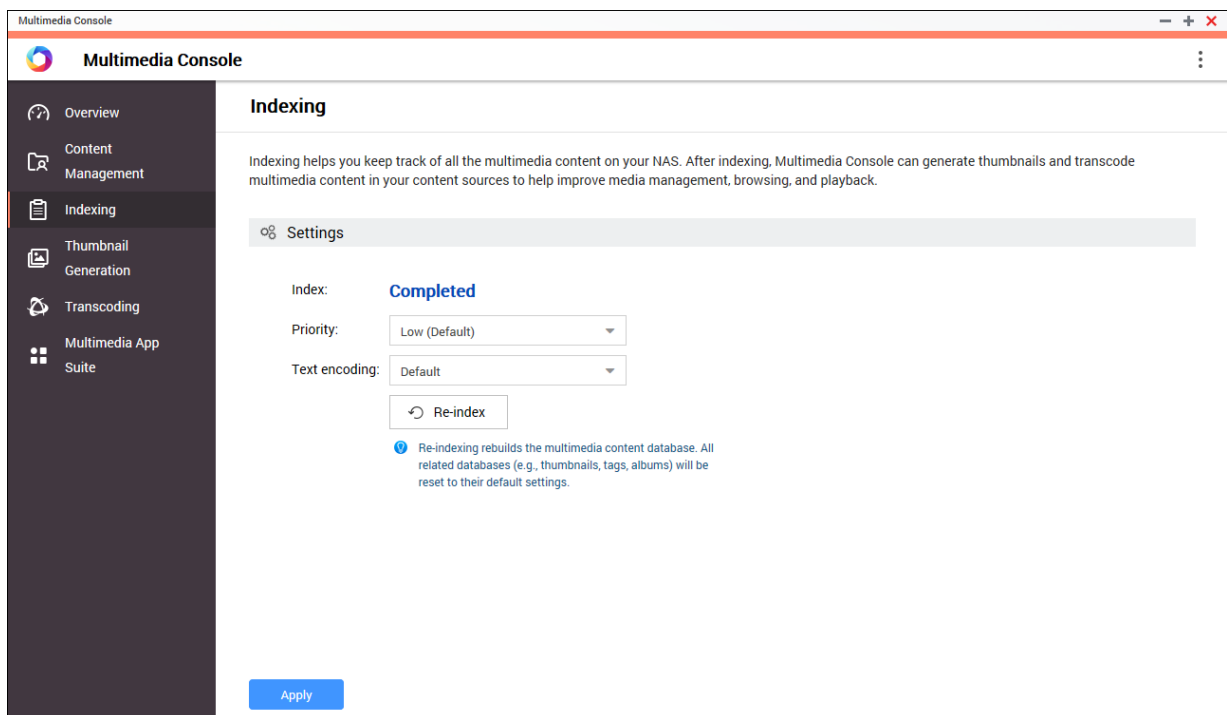
1. Open Multimedia Console.
2. Go to **Content Management**.
3. Select an app or service.
4. Click **Edit**.
The **Edit Content Sources** window appears.
5. Select or deselect content source folders.
The **Selected Folder Paths** list updates.
6. Click **Apply**.

**Tip**

Click **Excluded System Sources** on the **Content Management** screen to view system folder paths that are excluded from Multimedia Services.

Indexing

Multimedia Console improves content management, browsing, and playback when accessing files in various multimedia apps by scanning and indexing multimedia files on your NAS.



Indexing Multimedia Content

Multimedia Console improves content management, browsing, and playback when accessing files in various multimedia apps by scanning and indexing multimedia files on your NAS.

1. Open Multimedia Console.
2. Go to **Indexing**.
3. Select the **Priority**.

- **Low (Default)**
- **Normal**

The **Priority** determines the amount of system resources allocated to the indexing process.

4. Select the type of Text encoding.

The type of **Text encoding** determines the character encoding scheme that Multimedia Console uses to index text and data in your multimedia files. The default encoding scheme is Unicode.

5. Click Apply.



Tip

Click **Re-index** to rebuild the multimedia content database and revert dependent databases to their default settings.

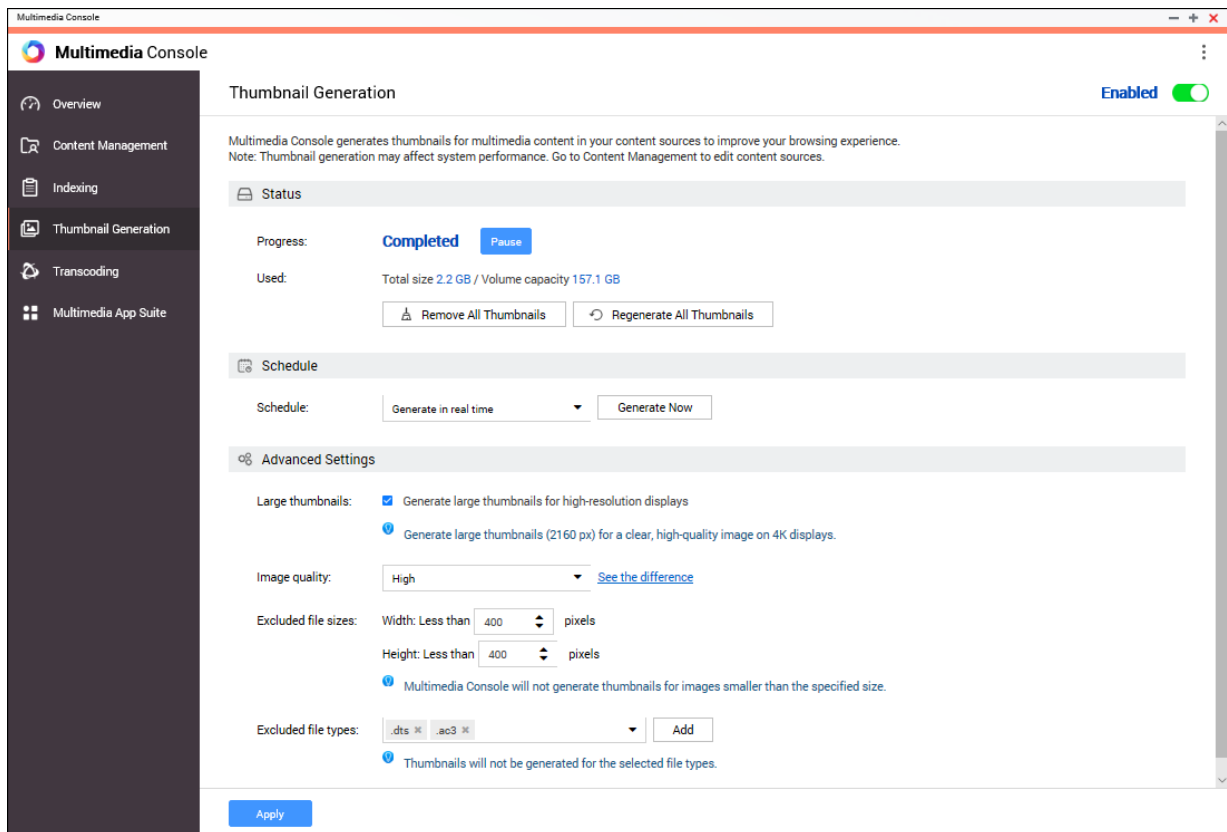
Thumbnail Generation

Multimedia Console generates thumbnails for multimedia files to improve browsing.





Note

- Thumbnail generation is enabled by default if Multimedia Services is enabled.
- You can disable thumbnail generation in the upper right of the **Thumbnail Generation** screen.
- Generating thumbnails may affect system performance.



Configuring Status


1. Open Multimedia Console.
2. Go to **Thumbnail Generation > Status** .
3. Perform any of the following tasks.

Task	Steps
Pause thumbnail generation	<p>a. Next to Progress, click Pause. The Pause window opens.</p> <p>b. Select Pause.</p> <p>c. Click OK.</p> <p> Tip Click Resume when thumbnail generation is paused to resume thumbnail generation.</p>
Postpone thumbnail generation	<p>a. Next to Progress, click Pause. The Pause window opens.</p> <p>b. Select Postpone.</p> <p> 1. Select the duration.</p> <p>c. Click OK.</p> <p> Tip Click Resume when thumbnail generation is postponed to resume thumbnail generation.</p>
Remove thumbnails	<p>a. Under Used, click Remove All Thumbnails. A dialog box appears.</p> <p>b. Click OK.</p>
Regenerate thumbnails	<p>a. Under Used, click Regenerate All Thumbnails. A dialog box appears.</p> <p>b. Click OK.</p>

Configuring Schedule

1. Open Multimedia Console.
2. Go to **Thumbnail Generation > Schedule** .
3. Next to **Schedule**, select one of the following options.

Option	Description
Generate in real time	Multimedia Console generates thumbnails for new files as soon as they are detected.

Option	Description
Generate using schedule	Multimedia Console generates thumbnails according to a specified schedule.  Note When selected, you must specify a thumbnail generation schedule.
Generate manually	Multimedia Console generates thumbnails only after clicking Generate Now .




Tip

Click **Generate Now** to force Multimedia Console to start generating thumbnails immediately.

4. Click **Apply**.

Configuring Advanced Settings

1. Open Multimedia Console.
2. Go to **Thumbnail Generation > Advanced Settings**.
3. Configure any of the following settings.

Setting	Description
Large thumbnails	When selected, Multimedia Console generates high-resolution thumbnails (2160 px) for media files.
Image quality	Select High or Low .  Tip Click See the difference to view a side-by-side comparison of high- and low-quality thumbnails.
Excluded file sizes	Multimedia Console only generates thumbnails for images that are larger than the specified resolution.
Excluded file types	Multimedia Console will not generate thumbnails for the selected file types.

4. Click **Apply**.

Transcoding

The transcoding feature in Multimedia Console converts video files to MPEG-4 format for improved compatibility with media players on mobile devices, smart TVs, and web browsers. Transcoding can also scale down the resolution of video files to prevent buffering in slower network environments.

You can create and manage transcoding tasks and configure settings from the **Transcoding** screen in Multimedia Console.

Managing Transcoding Tasks

You can manage Background Transcoding and On-the-Fly Transcoding tasks from the Overview tab on the **Transcoding** screen.



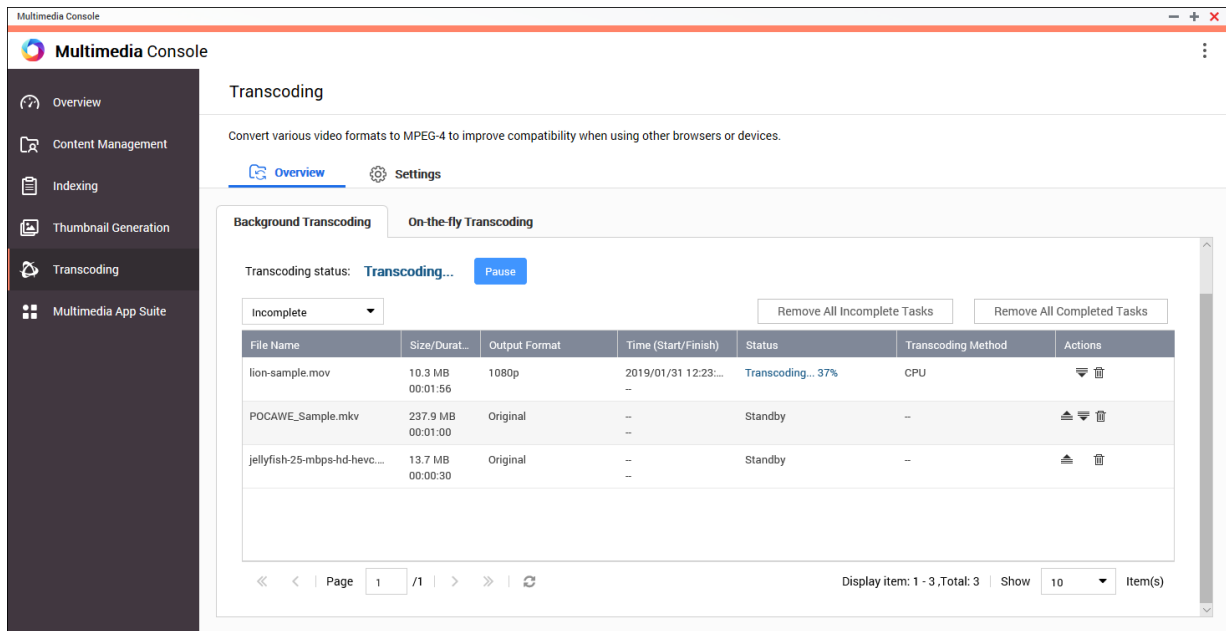
Note

- Transcoding is only available for certain NAS models. Go to <https://www.qnap.com/en/compatibility> to view specifications for your NAS and verify that it is compatible.
- Transcoding uses additional NAS storage space to store transcoded files.



Type	Description
<p>Background Transcoding</p>	<p>Background Transcoding converts videos asynchronously to minimize consumption of system resources if the video is accessed by multiple users simultaneously.</p> <p>The Background Transcoding tab displays the overall background transcoding status as well as additional information about specific background transcoding tasks. You can view and manage background transcoding tasks from this tab.</p> <p>You can manually add videos to background transcoding folders using File Station, Photo Station, or Video Station.</p> <p>For details on managing background transcoding folders, see Configuring Background Transcoding Folders.</p>
<p>On-the-Fly Transcoding</p>	<p>On-the-Fly Transcoding converts videos in real time as you watch them.</p> <p>The On-the-Fly Transcoding tab displays information about on-the-fly transcoding tasks. You can view and manage on-the-fly transcoding tasks from this tab.</p> <div data-bbox="592 1025 651 1084" style="float: left; margin-right: 10px;"> </div> <p>Note</p> <ul style="list-style-type: none"> • You cannot specify the output format for On-the-Fly Transcoding. • On-the-Fly Transcoding uses more system resources than Background Transcoding and may affect the performance of your NAS. <div data-bbox="592 1308 651 1366" style="float: left; margin-right: 10px;"> </div> <p>Tip</p> <p>You can install CodexPack to increase transcoding speed and reduce system resource consumption. You can check whether your NAS supports GPU-accelerated transcoding on the Transcoding Settings screen. For details, see Configuring Transcoding Resources.</p>

Background Transcoding

The Background Transcoding tab displays the overall background transcoding status as well as additional information about specific background transcoding tasks. You can view and manage background transcoding tasks from this tab.






General Tasks

Task	User Action
Pause background transcoding	<ol style="list-style-type: none"> 1. Click Pause. The Pause window opens. 2. Select Pause. 3. Click OK. <p> Tip Click Resume when background transcoding is paused to resume background transcoding.</p>
Postpone background transcoding	<ol style="list-style-type: none"> 1. Click Pause. The Pause window opens. 2. Select Postpone. <ol style="list-style-type: none"> a. Select the duration. 3. Click OK. <p> Tip Click Resume when background transcoding is postponed to resume background transcoding.</p>
View completed tasks	Above the background transcoding task table, select Completed from the drop-down list. Multimedia Console displays completed background transcoding tasks.
View incomplete tasks	Above the background transcoding task table, select Incomplete from the drop-down list. Multimedia Console displays incomplete background transcoding tasks.

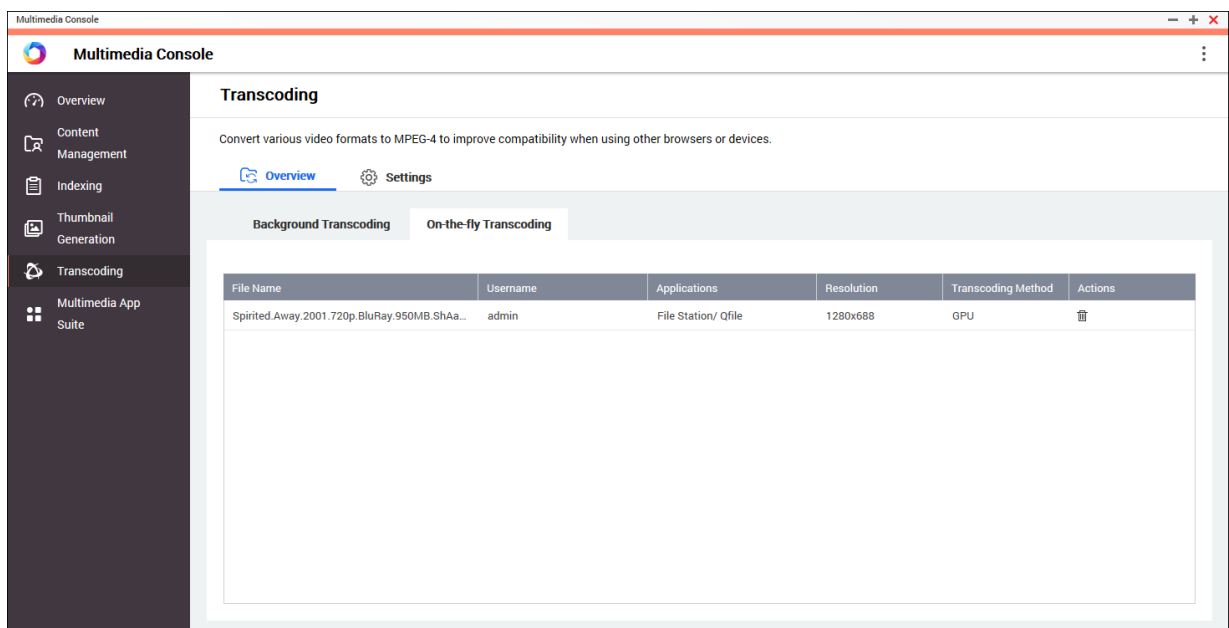
Task	User Action
Remove incomplete tasks	<ol style="list-style-type: none"> 1. Click Remove All Incomplete Tasks. A dialog box appears. 2. Click OK.
Remove completed tasks	<ol style="list-style-type: none"> 1. Click Remove All Completed Tasks. A dialog box appears. 2. Click OK.


Task Table Configuration (Incomplete Tasks)

Button	Description
	Moves a task up in the list and increases its priority.
	Moves a task down in the list and decreases its priority.
	Removes a task from the list.

On-the-fly Transcoding

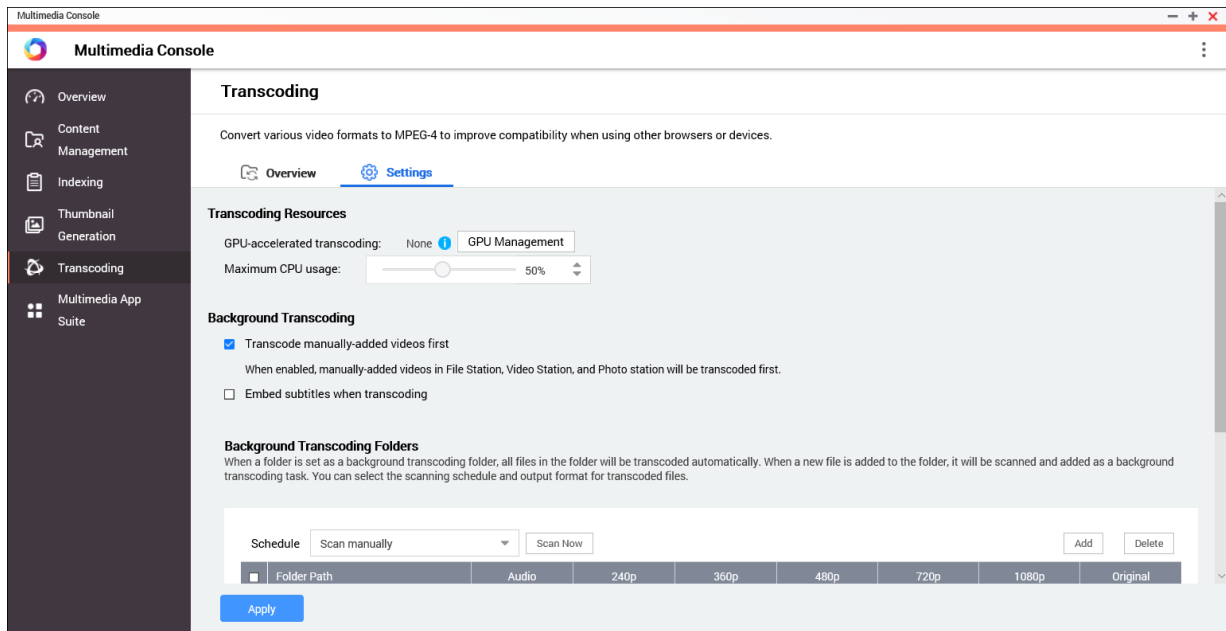
The On-the-Fly Transcoding tab displays information about on-the-fly transcoding tasks. You can view and manage on-the-fly transcoding tasks from this tab.



Tip
Click  to remove a task from the list.

Settings

You can manage Background Transcoding and On-the-Fly Transcoding settings from the Settings tab on the **Transcoding** screen.



Configuring Transcoding Resources

1. Open Multimedia Console.
2. Go to **Transcoding > Settings > Transcoding Resources** .
3. Optional: Enable **GPU-accelerated transcoding**.
 - a. Click **GPU Management**.
The **System > Hardware > Graphics Card** screen appears.
 - b. Configure graphics card settings.
4. Specify the **Maximum CPU usage** allocated to transcoding tasks.
5. Click **Apply**.

Configuring Background Transcoding Settings



1. Open Multimedia Console.
2. Go to **Transcoding > Settings > Background Transcoding** .
3. Configure any of the following settings.

Setting	Description
Transcode manually-added videos first	Videos in File Station, Video Station, and Photo Station that are manually added will be transcoded first.
Embed subtitles when transcoding	Multimedia Console automatically embeds subtitles to videos when transcoding them.

4. Click **Apply**.

Configuring Background Transcoding Folders

1. Open Multimedia Console.
2. Go to **Transcoding > Settings > Background Transcoding Folders** .
3. Perform any of the following tasks.

Task	User Action
Configure the scanning schedule for background transcoding folders	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Scan in real time: Multimedia Console scans background transcoding folders for new files and adds the files as background transcoding tasks as soon as they are detected. • Scan using schedule: Multimedia Console scans background transcoding folders for files according to a specified schedule. <p> Note When selected, you must specify the time of day that Multimedia Console generates thumbnails.</p> <ul style="list-style-type: none"> • Scan manually: Multimedia Console scans background transcoding folders only when you click Scan Now.
Add a background transcoding folder	<ol style="list-style-type: none"> a. Click Add. The Add Background Transcoding Folders window appears. b. Select a folder. c. Specify the output format. d. Click Apply.
Remove a background transcoding folder	<ol style="list-style-type: none"> a. Select a background transcoding folder. b. Click Delete.
Configure transcoding output format	<ol style="list-style-type: none"> a. Locate a background transcoding folder on the list. b. Select the output format. <p> Note Multimedia Console upscales the video if the selected resolution is higher than the original resolution of the video.</p> <ol style="list-style-type: none"> c. Click Apply.

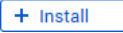
Multimedia App Suite

You can view statuses and configure user and group access permissions for installed multimedia apps and services from the **Multimedia App Suite** screen.

Configuring Multimedia Apps and Services

1. Open Multimedia Console.
2. Go to **Multimedia App Suite**.

3. Perform any of the following tasks.

Task	User Action
Install an app or service	<p>a. Locate an app or service with the status Not Installed under the app or service name.</p> <p>b. Click Not Installed. The App Center and app installation windows open.</p> <p>c. Click .</p>
Enable an app or service	<p>a. Locate an app or service with the status Disabled under the app or service name.</p> <p>b. Click Disabled.</p> <p>c. The app or service opens in a new window.</p> <p>d. Enable the app or service.</p>
Disable an app or service	<p>a. Locate an app or service with the status Enabled under the app or service name.</p> <p>b. Click Enabled.</p> <p>c. The app or service opens in a new window.</p> <p>d. Disable the app or service.</p>

Configuring Multimedia App Permissions



1. Open Multimedia Console.
2. Go to **Multimedia App Suite**.
3. Locate an app with access permissions.
4. Under **Permissions**, click the permission status.
The **Permission Settings** window opens.
5. Select a permission type.

Permission Type	Description
All Users	All users can access the app.
Local Administrator Group Only	Only users in the local administrator group can access the app.
Custom	Specified users and user groups can access the app.

A dialog box appears.

6. Click **OK**.
7. Perform any of the following actions.

Permission Type	User Action
All Users	Click Close .
Local Administrator Group Only	Click Close .

Permission Type	User Action
Custom	<p>a. Select a user or user group type:</p> <ul style="list-style-type: none"> • Local • Domain <p>b. Choose to deny or allow access to selected users or groups. A dialog box appears.</p> <ol style="list-style-type: none"> 1. Click OK. <p>c. Filter the list by users or groups.</p> <p> Tip Use the Search field to quickly find users or groups.</p> <p>d. Select a user or group.</p> <p>e. Click Add. The user or group is added to the Selected Users/Groups list.</p> <p> Tip</p> <ul style="list-style-type: none"> • Select a user or group and click Delete to remove the user or group from the list. • Click Delete All to remove all users or groups from the list. <p>f. Click Save.</p> <p>g. Click Close.</p>

16. QuLog Center

QuLog Center allows you to centrally manage and monitor logs from local devices and remote devices. You can specify log filters, create notification rules, and configure log settings to stay informed of your device status and important events. You can view and manage system logs in **Control Panel > System > QuLog Center**.

Monitoring System Logs

The **Overview** screen provides statistical graphics to help you visualize system log data and monitor device status.

System Event Log

The **System Event Log** tab provides the following widgets to visualize the statistical data of the system event logs from your devices.



Important

You must configure a log destination to enable the system event log feature. For details, see [Configuring Event Log Settings](#).



Tip

The System Event Log page allows you to view log data from local devices or sender devices. You can view data from all sender devices or view each device's information separately. You can also specify the displayed statistics period.

Widget	Description
Logs Over Time	<p>This widget displays a line chart to visualize the number of log entries over time.</p> <div style="display: flex; align-items: flex-start;"> <p>Tip</p> <ul style="list-style-type: none"> • Click ⋮ to specify the event types that you want to include in the line chart. • Hover the mouse pointer over the line chart to see the number of logs at a particular point in time. </div>
Top 5 Applications for Error Logs	This widget displays the five applications that have the largest numbers of error log entries.
Top 5 Applications for Warning Logs	This widget displays the five applications that have the largest numbers of warning log entries.



System Access Logs

The **System Access Log** tab provides the following widgets to visualize the statistical data of the system access logs from your devices.



Tip

The System Access Log page allows you to view log data from local devices or sender devices. You can view data from all sender devices or view each device's information separately. You can also specify the displayed statistics period.

Section	Description
Logs Over Time	<p>This widget displays a line chart to visualize the number of log entries over time.</p> <div style="display: flex; align-items: flex-start;">  <div> <p>Tip</p> <ul style="list-style-type: none"> • Click  to specify the event types that you want to include in the line chart. • Hover the mouse pointer over the line chart to see the number of logs at a particular point in time. </div> </div>
Currently Online	This widget lists the current online users and provides the information of their user sessions.
Connection Types	This widget displays a pie chart to visualize the numbers of user sessions for each communication protocol.
Logged in	This widget displays a pie chart to visualize the numbers of successful logins using each IP address or user account.
Failed to log in	This widget displays a pie chart to visualize the numbers of failed login attempts using each IP address or user account.

Local Logs

Local Device Logs allows you to monitor system event logs, system access logs, and online user status on one local device. You can also configure log filters, log settings, and remove event indicators.

Local System Event Logs






You can monitor and manage system event logs from local devices in **Local Device > System Event Log** .










Important

- You must configure a log destination to enable the local system event log feature. For details, see [Configuring Event Log Settings](#).
- QuLog Center can download or export a maximum of 10,000 log entries. You can use log filters to specify the maximum number of log entries per file for download or export. For details, see [Adding a Log Filter](#).

On the **System Event Log** screen, you can perform the following tasks:

Task	Steps
Select a group mode	<ol style="list-style-type: none"> 1. Click . 2. Select one of the following grouping modes. <ul style="list-style-type: none"> • No grouping: this mode displays and lists all log entries. • By app: this mode groups log entries by app name. • By date: this mode groups log entries by date. • By content: this mode groups log entries by log content. • By user: this mode groups log entries by users. • By source IP: this mode groups log entries by source IP address.
Select a display style	<ol style="list-style-type: none"> 1. Click . 2. Select a display style. <p> Tip You can also click Add Style to create a display style. For details, see Configuring a Display Style.</p>
Export logs	<ol style="list-style-type: none"> 1. Click . The Export Logs drop-down menu appears. 2. Click Export. 3. Select an export file format. <p> Note QuLog Center supports CSV and HTML log file formats.</p> <ol style="list-style-type: none"> 4. Optional: Compress the export file and specify a password. 5. Specify the destination shared folder for exporting logs. <ol style="list-style-type: none"> a. Click Browse. The Select a shared folder window appears. b. Select a shared folder. 6. Click Export.

Task	Steps
Download export logs	<ol style="list-style-type: none"> 1. Click  . The Export Logs drop-down menu appears. 2. Click Download. 3. Select an export file format. <p> Note QuLog Center supports CSV and HTML log file formats.</p> <ol style="list-style-type: none"> 4. Optional: Compress the export file and specify a password. 5. Click Download. The log file is downloaded to your computer.
Perform a search	<ol style="list-style-type: none"> 1. Specify keywords in the search field. 2. Press Enter. 3. Optional: Click Add as Customized Tab and specify a tab name. This allows you to create a custom tab using the keywords and criteria that you have specified. For details, see Creating a Custom Filter Tab for System Event Log.
Select display items	<ol style="list-style-type: none"> 1. Click . 2. Select the item category to display.
Create an event notification rule	<p>You can quickly create an event notification rule using a log entry. This allows you to receive notifications for events similar to the selected log entry.</p> <ol style="list-style-type: none"> 1. Locate a log entry. 2. Click . 3. Select Create event notification rule. Notification Center opens and the Create event notification rule windows appears. For details, see Creating an Event Notification Rule.
Create an event flag rule	<ol style="list-style-type: none"> 1. Locate a log entry. 2. Click . 3. Select Create Event Flag Rule. The Create Event Flag Rule window appears. 4. Click Create. The event is flagged. Go to Log Settings > Event Indicators to view all event flags.
Select all log entries	<ol style="list-style-type: none"> 1. Click Select multiple entries. The select multiple entries drop-down menu appears. 2. Click Select all.

Task	Steps
Invert selection	<ol style="list-style-type: none"> 1. Click Select multiple entries. The select multiple entries drop-down menu appears. 2. Click Invert selection.
Copy one or more log entries	<ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click . The content of the selected log entries is copied to the clipboard and can be pasted elsewhere.
Delete one or more log entries	<ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click . A confirmation message appears. 3. Click Yes.

Local System Access Logs


You can monitor and manage system access logs from local devices in **Local Device > System Access Log**.












Important

- You must configure a log destination to enable the system access logs feature. For details, see [Configuring Access Log Settings](#).
- QuLog Center can download or export a maximum of 10,000 log entries. You can use log filters to specify the maximum number of log entries per file for download or export. For details, see [Adding a Log Filter](#).

On the **System Access Log** screen, you can perform the following tasks:

Task	Steps
Select a group mode	<ol style="list-style-type: none"> 1. Click . 2. Select one of the following grouping modes. <ul style="list-style-type: none"> • No grouping: this mode displays and lists all log entries. • By date: this mode groups log entries by date. • By user: this mode groups log entries by user. • By source IP: this mode groups log entries by source IP address.

Task	Steps
Select a display style	<ol style="list-style-type: none"> 1. Click . 2. Select a display style. <p> Tip You can also click Add Style to create a display style. For details, see Configuring a Display Style.</p>
Export logs	<ol style="list-style-type: none"> 1. Click . The Export Logs drop-down menu appears. 2. Click Export. 3. Select an export file format. <p> Note QuLog Center supports CSV and HTML log file formats.</p> <ol style="list-style-type: none"> 4. Optional: Compress the export file and specify a password. 5. Specify the destination shared folder for exporting logs. <ol style="list-style-type: none"> a. Click Browse. The Select a shared folder window appears. b. Select a shared folder. 6. Click Export.
Download export logs	<ol style="list-style-type: none"> 1. Click . The Export Logs drop-down menu appears. 2. Click Download. 3. Select an export file format. <p> Note QuLog Center supports CSV and HTML log file formats.</p> <ol style="list-style-type: none"> 4. Optional: Compress the export file and specify a password. 5. Click Download. The log file is downloaded to your computer.

Task	Steps
Perform a search	<ol style="list-style-type: none"> 1. Specify keywords in the search field. 2. Press Enter. 3. Optional: Click Add as Customized Tab and specify a tab name. This allows you to create a custom tab using the keywords and criteria that you have specified. For details, see Creating a Custom Filter Tab for Local System Access Log.
Select display items	<ol style="list-style-type: none"> 1. Click . 2. Select the item category to display.
Select all log entries	<ol style="list-style-type: none"> 1. Select one log entry. 2. Click Select multiple entries. The Select multiple entries drop-down menu appears. 3. Click Select all . All log entries are selected.
Invert selection	<ol style="list-style-type: none"> 1. Select one log entry. 2. Click Select multiple entries. The Select multiple entries drop-down menu appears. 3. Click Invert selection.
Copy one or more log entries	<ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click . The content of the selected log entries is copied to the clipboard and can be pasted elsewhere.
Delete one or more log entries	<ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click . A confirmation message appears. 3. Click Yes.
Add one or more log entry to the block list	<ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click Add to block list. The Add to block list drop-down menu appears. 3. Select a block period option.

Online Users

On the **Online Users** screen, you can see the list of online users and their detailed information, such as login date, login time, username, source IP address, computer name, connection type, and accessed resources.

You can perform the following tasks:

Tasks	Steps
Remove a connection	<ol style="list-style-type: none"> 1. Locate a user from the list. 2. Right-click the user. 3. Select Disconnect. A confirmation message appears. 4. Click Yes.
Block a user	<ol style="list-style-type: none"> 1. Locate a user from the list. 2. Right-click the user. 3. Select Add to block list. 4. Select a block period option.
Remove the connection and block the user	<ol style="list-style-type: none"> 1. Locate a user from the list. 2. Right-click the user. 3. Select Disconnect and add to a block list. A confirmation message appears. 4. Select a block period option.
Select the items to display on the list	<ol style="list-style-type: none"> 1. Click +. 2. Select the item category to display.

Creating a Custom Filter Tab for Local Device System Logs


You can create custom filter tabs for Local System Event Logs and Local System Access Logs. The customized filter tabs can filter logs or user information based on specified keywords or criteria. For details, see the following topics:

- [Creating a Custom Filter Tab for System Event Log](#)
- [Creating a Custom Filter Tab for Local System Access Log](#)

Creating a Custom Filter Tab for System Event Log

1. Open QuLog Center.
2. Go to **Local Device > System Event Log**.
3. Go to the search bar.
4. Click **▼**.
The **Advanced Search** window appears.
5. Specify the following filter fields:


Fields	Steps
Severity Level	<ol style="list-style-type: none"> a. Click ▼. The severity level drop-down menu appears. b. Select a severity level option.








Fields	Steps
Application	<p>a. Click ▾ . The application drop-down menu appears.</p> <p>b. Select an application. The Category option appears.</p> <p> Note The Category option only appears when you specify the application.</p> <p>c. Specify the application Category.</p>
Date	<p>a. Click ▾ . The date drop-down menu appears.</p> <p>b. Select a date option.</p>
Content	<p>a. Click ▾ . The content condition option appears.</p> <p>b. Select a condition.</p> <p>c. Specify the content keywords.</p>
User	<p>a. Click ▾ . The user condition option appears.</p> <p>b. Select a condition.</p> <p>c. Specify the keywords.</p>
Source IP	<p>a. Click ▾ . The source IP address condition option appears.</p> <p>b. Select a condition.</p> <p>c. Specify the source IP address.</p>

6. Optional: Click **Reset** to clear all search filters.
Respecify search filters as many times as required.
7. Click **Search**.
The list of filtered results is displayed.
8. Click **Add as Customized Tab**.
The **Add as Customized Tab** window appears.
9. Enter a tab name.
10. Click **Apply**.
 - The custom filter tab is created.
 - The custom filter tab is displayed next to the **Main** tab.

Creating a Custom Filter Tab for Local System Access Log

1. Open QuLog Center.

2. Go to **Local Device > System Access Log**.
3. Go to the search bar.
4. Click  .
The **Advanced Search** window appears.
5. Specify the following filter fields:

Fields	Steps
Severity Level	<ol style="list-style-type: none"> a. Click  . The severity level drop-down menu appears. b. Select a severity level option.
Accessed Resources	<ol style="list-style-type: none"> a. Click  . The content condition option appears. b. Select a condition. c. Specify the keywords.
Date	<ol style="list-style-type: none"> a. Click  . The date drop-down menu appears. b. Select a date option.
Connection type	<ol style="list-style-type: none"> a. Click  . The connection type option appears. b. Select a connection type.
User	<ol style="list-style-type: none"> a. Click  . The user condition option appears. b. Select a condition. c. Specify the keywords.
Action	<ol style="list-style-type: none"> a. Click  . The action drop-down menu appears. b. Select an action option.
Source IP	<ol style="list-style-type: none"> a. Click  . The source IP address condition option appears. b. Select a condition. c. Specify the source IP address.

6. Optional: Click **Reset** to clear all search filters.
Respecify search filters as many times as required.
7. Click **Search**.
The list of filtered results is displayed.
8. Click **Add as Customized Tab**.
The **Add as Customized Tab** window appears.

9. Enter a tab name.

10. Click **Apply**.

- The custom filter tab is created.
- The custom filter tab is displayed next to the **Main** tab.





Local Log Settings

Log Settings allows you to configure the following types of settings: event logs, access logs, display styles, and event indicators.

Configuring Event Log Settings

You can specify the database size and the log language or delete all the log entries for system event logs.

1. Open QuLog Center.
2. Go to **Local Device > Log Settings > Event Log Settings**.
3. Specify the following settings:

Settings	Steps
Destination	<ol style="list-style-type: none"> Click  . The log destination option drop-down menu appears. Select a log destination. <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;"> <p> Important</p> <ul style="list-style-type: none"> • You must configure a log destination to enable event logging features. • You cannot select a volume that is encrypted or has less than 10% of free volume space. </div>
Maximum number of entries	<ol style="list-style-type: none"> Click  . The maximum number of entries option drop-down menu appears. Select the maximum number of entries allowed. The log database size is specified.
Log retention time	<ol style="list-style-type: none"> Click  . The log retention time drop-down menu appears. Select the log retention time.

Settings	Steps
Archive overflow log entries to a standby log destination	<ol style="list-style-type: none"> a. Click Archive and move log entries to the specified location after reaching the database limit. The destination folder option is activated. b. Click Browse. The Select a shared folder window appears. c. Select a shared folder. d. Click OK. The shared folder is selected as the standby log destination.

4. Optional: Delete all event logs.
 - a. Click **Delete All Event Logs.**
A confirmation message appears.
 - b. Click **Yes.**




Warning
You cannot restore deleted logs.




5. Select the log language.
 - a. Click **▼**.
The log language drop-down menu appears.
 - b. Select a language.
6. Click **Apply.**

Configuring Access Log Settings


You can specify the database size, log retention time, connection type or delete all system access log entries.

1. Open QuLog Center.
2. Go to **Local Device > Log Settings > Access Log Settings**.
3. Specify the following settings:

Settings	Steps
Destination	<ol style="list-style-type: none"> a. Click ▼. The log destination option drop-down menu appears. b. Select a log destination. <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;"> <p> Important</p> <ul style="list-style-type: none"> You must configure a log destination to enable event logging features. You cannot select a volume that is encrypted or has less than 10% of free volume space. </div>

Settings	Steps
Maximum number of entries	<p>a. Click  . The maximum number of entries option drop-down menu appears.</p> <p>b. Select the maximum number of entries allowed.</p>
Log retention time	<p>a. Click  . The log retention time drop-down menu appears.</p> <p>b. Select the log retention time.</p>
Connection Types	<p>Select the connection types you want to log.</p> <p> Tip You can select multiple connection types.</p>

4. Optional: Delete all event logs.
 - a.** Click **Delete All Access Logs**.
A confirmation message appears.
 - b.** Click **Yes**.

 **Warning**
You cannot restore deleted logs.


5. Click **Apply**.

Configuring a Display Style



You can customize your log display style to enhance readability or to highlight certain entries.


1. Open QuLog Center.
2. Open **Display Settings** through one of the following methods:

Accessing Display Setting Method	Steps
System Event Log	Go to Local Device > System Event Log > Display style .
System Access Log	Go to Local Device > System Access Log > Display style .

3. Click  .
The display style drop-down menu appears.
4. Click **Settings**.
The **Display Style Settings** window appears.
5. Perform one or more of the following tasks:

Task	Steps
Add a display style	<p>a. Click Add Style. The Add Style window appears.</p> <p>b. Specify a name for the style.</p> <p>c. Click Apply.</p>

Task	Steps
Delete a style	<ul style="list-style-type: none"> a. Select a display style. b. Click Delete Style. A confirmation message appears. c. Click Yes.
Add a rule to a display style	<ul style="list-style-type: none"> a. Select a display style. b. Click Add Rule. The Style Rule window appears. c. Select a field. d. Select a keyword. e. Select one or more formatting effects. <div style="margin-left: 20px;">  Tip You can instantly preview the results of the selected formatting effects. </div> <ul style="list-style-type: none"> f. Click Apply.
Edit a rule	<ul style="list-style-type: none"> a. Select a display style. b. Select a rule from the list. c. Click Edit. The Style Rule window appears. d. Select a field. e. Specify the condition. f. Select one or more formatting effects. <div style="margin-left: 20px;">  Tip You can instantly preview the results of selected formatting effects. </div> <ul style="list-style-type: none"> g. Click Apply.
Remove a rule	<ul style="list-style-type: none"> a. Select a display style. b. Select a rule from the list. c. Click Delete. A confirmation message appears. d. Click Yes.

Task	Steps
Specify the priority of rules	<ol style="list-style-type: none"> a. Select a display style. b. Select a rule from the list. c. Beside Priority, click ^ or v to change its priority. <div style="display: flex; align-items: flex-start; margin-top: 10px;">  <p>Note The formatting results of rules with a higher priority overwrite those with a lower priority.</p> </div>


Removing Event Indicators

1. Open QuLog Center.
2. Go to **Local device > Log Settings > Event Indicators** .
3. Select an event flag rule.



Tip

Click the box in the top left column to select all event flag rules.

4. Click **Remove** or  .
The event flag rule is removed.

QuLog Service

QuLog Service allows you to centrally manage logs from multiple remote devices. You can configure a single device as a Log Receiver to manage and monitor all incoming system logs from other devices, or configure the device as a Log Sender that sends all system logs to a remote QuLog Center.

Configuring Log Sender Settings

The Log Sender allows you to send system event logs and system access logs on the local device to a remote QuLog Center or Syslog Server.

Adding a Destination IP Address

1. Open QuLog Center.
2. Select one of the following options:

Options	User Actions
Send to QuLog Center	<ol style="list-style-type: none"> a. Go to QuLog Service > Log Sender > Send to QuLog Center . b. Enable Send logs to a remote QuLog Center. System event logs and access logs from the local device are sent to a remote QuLog Center.
Send to Syslog Server	<ol style="list-style-type: none"> a. Go to QuLog Service > Log Sender > Send to Syslog Server . b. Enable Send logs to a remote syslog server. System event logs and access logs from the local device are sent to a remote syslog server.

3. Click **Add Destination**.
The **Add Destination** window appears.
4. Specify the following IP address information:
 - **Destination IP**



Tip

You can enter the destination IP address manually or click **Search** to automatically select a device from your local network. This option is only available for sending logs to a remote QuLog Center.

- **Port**
- **Transfer protocol**
- **Log type**
- **Format**




Note

You can click **Send a Test Message** to test the connection. This option is only available for sending logs to a remote QuLog Center.

5. Click **Apply**.



Editing a Destination IP Address

1. Open QuLog Center.
2. Go to **Log Sender**.
3. Select **Send to QuLog Center** or **Send to Syslog Server**.
4. Select a destination IP address.
5. Click .
The **Edit Destination** window appears.
6. Edit the IP address information.
For details, see [Adding a Destination IP Address](#).
7. Click **Apply**.

Sending a Test Message


1. Open QuLog Center.
2. Select one of the following options:

Methods	Actions
Add Destination IP Address	Add a destination IP address. For details, see Adding a Destination IP Address
Send a Test Message	<ol style="list-style-type: none"> a. Select a destination IP address. b. Click Send a Test Message.

Methods	Actions
	Click  .

A test message is sent to the destination IP address to test the network connection.

Removing a Destination IP Address

1. Open QuLog Center.
2. Go to **QuLog Service > Log Sender** .
3. Select **Send to QuLog Center** or **Send to Syslog Server**.
4. Select one or multiple destination IP addresses.
5. Click **Remove** or  .
A confirmation message window appears.
6. Click **Yes**.
The destination IP address is removed.

Configuring Log Reciever Settings

The Log Reciever allows you to configure a local device as the recipient of remote device logs. You can centrally manage and monitor system event logs and access logs from remote QNAP devices. Additionally, you can configure customized filters to search for logs efficiently.

Configuring Log Receiver General Settings






1. Open QuLog Center.
2. Go to **QuLog Service > Log Receiver > General Settings** .
3. Select **Receive logs from a remote QuLog Center**.
4. Select transfer protocols and then specify the port number.



Note

QuLog Center supports TCP and UDP protocols.

5. Optional: Click **Enable Transport Layer Security (TLS)**.
6. Select **System Event Log** or **System Access Log**.
7. Specify the following settings:

Settings	Steps
Destination	<p>a. Click  . The log destination option drop-down menu appears.</p> <p>b. Select a log destination.</p> <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;">  Important You cannot select a volume that is encrypted or has less than 10% of free volume space. </div>
Maximum number of entries	<p>a. Click  . The maximum number of entries option drop-down menu appears.</p> <p>b. Select the maximum number of entries allowed. The log database size is specified.</p>
Log retention time	<p>a. Click  . The log retention time drop-down menu appears.</p> <p>b. Select the log retention time.</p>
Archive overflow log entries to a standby log destination	<p>a. Click Archive and move log entries to the specified location after reaching the database limit. The destination folder option is activated.</p> <p>b. Click Browse. The Select a shared folder window appears.</p> <p>c. Select a shared folder.</p> <p>d. Click OK. The shared folder is selected as the standby log destination.</p>
Delete all event logs	<p>a. Click Delete All Event Logs. A confirmation window appears.</p> <div style="border-left: 2px solid red; padding-left: 10px; margin-top: 10px;">  Warning You cannot restore deleted logs. </div> <p>b. Click Yes.</p>

8. Click **Apply**.

Log Filter Configurations

You can specify log filter conditions for system logs received from multiple sender devices on the Log Receiver to simplify locating specific types of logs and monitoring large volume of logs.

Configuring a Log Filter Criterion

You can specify log filter criteria to choose the types of log entries that will be received by Log Receiver.


1. Open QuLog Center.
2. Go to **QuLog Service > Log Receiver > Filter Criteria** .
3. Select **System Event Log** or **System Access Log**.
4. Click **Add Filter Criteria**.
The filter criteria window appears.
5. Specify the following information:

Log Type	Settings
System Event Log	<ul style="list-style-type: none"> • Severity level • User • Source IP • Application • Category • Content • Hostname
System Access Log	<ul style="list-style-type: none"> • Severity level • User • Source IP • Accessed resources • Hostname • Connection type • Action

6. Click **Apply**.

QuLog Center adds the specified log filter criteria.


Editing a Log Filter Criterion

1. Open QuLog Center.
2. Go to **QuLog Service > Log Receiver > Filter Criteria** .
3. Go to **System Event Log** or **System Access Log**.
4. Select a filter criteria.
5. Optional: Click **Reset** to clear all filter criteria settings.
6. Click  .
The **Filter Criteria** window appears.
7. Edit the log filter fields.


For details, see [Configuring a Log Filter Criterion](#).

8. Click **Apply**.
All changes are applied.

Deleting a Log Filter Criterion

1. Open QuLog Center.
2. Go to **QuLog Service > Log Receiver > Filter Criteria** .
3. Select **System Event Log** or **System Access Log**.
4. Select a filter criteria.
5. Click  .
A confirmation window appears.
6. Click **Yes**.

Importing a Custom Filter Criterion

1. Open QuLog Center.
2. Go to **QuLog Service > Log Receiver > Filter Criteria** .
3. Click **System Event Log** or **System Access Log**.
4. Click **Add Filter Criteria**.
5. Go to **Import custom filter criteria from the selected tab**.
6. Click  .
The custom filter criteria drop-down menu appears.
7. Select the custom filter tab from the drop-down menu.



Note

For details on how to create a custom filter tab, see the following topics:

- [Creating a Custom Filter Tab for System Event Log on a Sender Device](#)
- [Creating a Custom Filter Tab for System Access Log on a Sender Device](#)

The selected custom filter criteria are applied to the log.

Viewing and Managing Remote Logs

You can view and manage remote logs under the Sender Devices section in QuLog Center. This section lists all remote devices that send their logs to the QuLog Center on the local device. You can monitor logs from all sender devices or from individual sender devices. QuLog Center can manage up to 500 sender devices on a log receiver.

Managing System Event Logs on the Log Receiver





You can monitor and manage system event logs received by the **Log Receiver** in **QuLog Service > All Devices > System Event Log** . You can also monitor system event logs from individual sender devices.










Important

You must configure the log destination of the log receiver to enable this feature. For details, see [Configuring Log Receiver General Settings](#).

On the **System Event Log** screen, you can perform the following tasks:

Task	Steps
Select a group mode	<ol style="list-style-type: none"> 1. Click . 2. Select one of the following grouping modes. <ul style="list-style-type: none"> • No grouping: this mode displays and lists all log entries. • By app: this mode groups log entries by app name. • By date: this mode groups log entries by date. • By content: this mode groups log entries by log content. • By user: this mode groups log entries by users. • By source IP: this mode groups log entries by source IP address. • By Host Name: this mode groups log entries by the host name.
Select a display style	<ol style="list-style-type: none"> 1. Click . 2. Select a display style. <div style="margin-top: 10px;">  <p>Tip You can also click Add Style to create a display style. For details, see Configuring a Display Style.</p> </div>
Create an event flag rule	<p>You can quickly create an event flag rule using a log entry. This allows you to set event indicators for malware detection.</p> <ol style="list-style-type: none"> 1. Locate a log entry. 2. Click . 3. Select Create event flag rule. The Create Event Flag Rule window appears. 4. Click Create. The log flag rule is created.

Task	Steps
Export logs	<ol style="list-style-type: none"> 1. Click  . The Export Logs drop-down menu appears. 2. Click Export. 3. Select an export file format. <p> Note QuLog Center supports CSV and HTML log file formats.</p> <ol style="list-style-type: none"> 4. Select the maximum number of log entries per file. 5. Optional: Compress the export file and specify a password. 6. Specify the destination shared folder for exporting logs. <ol style="list-style-type: none"> a. Click Browse. The Select a shared folder window appears. b. Select a shared folder. 7. Click Export.
Download export logs	<ol style="list-style-type: none"> 1. Click  . The Export Logs drop-down menu appears. 2. Click Download. 3. Select an export file format. <p> Note QuLog Center supports CSV and HTML log file formats.</p> <ol style="list-style-type: none"> 4. Select the maximum number of log entries per file. 5. Optional: Compress the export file and specify a password. 6. Click Download. The log file is downloaded to your computer.
Perform a search	<ol style="list-style-type: none"> 1. Specify keywords in the search field. 2. Press Enter. 3. Optional: Click Add as Customized Tab and specify a tab name. This allows you to create a custom tab using the keywords and criteria that you have specified. <p>For details, see Creating a Custom Filter Tab for System Event Log on the Sender Device.</p>
Select display items	<ol style="list-style-type: none"> 1. Click . 2. Select the items to display.

Task	Steps
Select all log entries	<ol style="list-style-type: none"> 1. Click Select multiple entries. The select multiple entries drop-down menu appears. 2. Click Select all.
Invert selection	<ol style="list-style-type: none"> 1. Click Select multiple entries. The select multiple entries drop-down menu appears. 2. Click Invert selection.
Copy one or more log entries	<ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click . The content of the selected log entries is copied to the clipboard and can be pasted elsewhere.
Delete one or more log entries	<ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click . A confirmation message appears. 3. Click Yes.

Managing System Access Logs on the Log Receiver


You can monitor and manage system access logs received by the **Log Receiver** in **QuLog Service > All Devices > System Access Log** . You can also monitor system access logs from individual sender devices by clicking on the device.












Important

You must configure the log destination of the log receiver to enable this feature. For details, see [Configuring Log Receiver General Settings](#).

On the **System Access Log** tab, you can perform the following tasks:

Task	Steps
Select a group mode	<ol style="list-style-type: none"> 1. Click . 2. Select one of the following grouping modes. <ul style="list-style-type: none"> • No grouping: this mode displays and lists all log entries. • By date: this mode groups log entries by date. • By user: this mode groups log entries by user. • By source IP: this mode groups log entries by source IP. • By Host Name: this mode groups log entries by host name.

Task	Steps
Select a display style	<ol style="list-style-type: none"> 1. Click . 2. Select a display style. <p> Tip You can also click  and select Create a Style to create a display style. For details, see Configuring a Display Style.</p>
Export logs	<ol style="list-style-type: none"> 1. Click . The Export Logs window appears. 2. Select an export file format. 3. Specify the maximum number of log entries per file. 4. Optional: Compress the export file and specify a password. 5. Click Export.
Download exported logs	<ol style="list-style-type: none"> 1. Click . The Export Logs drop-down menu appears. 2. Click Download. 3. Select an export file format. <p> Note QuLog Center supports CSV and HTML log file formats.</p> <ol style="list-style-type: none"> 4. Select the maximum number of log entries per file. 5. Optional: Compress the export file and specify a password. 6. Click Download. The log file is downloaded to your computer.
Perform a search	<ol style="list-style-type: none"> 1. Specify keywords in the search field. 2. Press Enter. 3. Optional: Click Add as Customized Tab and specify a tab name. This allows you to create a custom tab using the keywords and criteria that you have specified. For details, see Creating a Custom Filter Tab for System Access Log on the Sender Device.
Select display items	<ol style="list-style-type: none"> 1. Click . 2. Select the items to display.
Select all log entries	<ol style="list-style-type: none"> 1. Click Select multiple entries. The select multiple entries drop-down menu appears. 2. Click Select all.

Task	Steps
Invert selection	<ol style="list-style-type: none"> 1. Click Select multiple entries. The select multiple entries drop-down menu appears. 2. Click Invert selection.
Copy one or more log entries	<ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click . The content of the selected log entries is copied to the clipboard and can be pasted elsewhere.
Delete one or more log entries	<ol style="list-style-type: none"> 1. Select one or more log entries. 2. Click . A confirmation message appears. 3. Click Yes.


Logging in a Sender Device

1. Open QuLog Center.
2. Go to **QuLog Service > Sender Devices** .
3. Select a device.
4. Click **Settings**.
5. Specify the following:
 - **Host IP address**
 - **Port**
 - **Username**
 - **Password**
6. Optional: Select **Secure login (HTTPS)**.
7. Click **Sign in**.
 - You are logged into the sender device.
 - All destination IP addresses of the sender device are listed.
 - You can configure the destination for sender device logs.
For details, see [Configuring Log Sender Settings](#).

Creating a Custom Filter Tab for System Event Log on a Sender Device

1. Open QuLog Center.
2. Go to **QuLog Service > Sender Devices** .
3. Click on a sender device.
4. Go to **System Event Log** .

5. Go to the search bar.
6. Click ▾ .
7. Specify the following filter fields:

Fields	Steps
Severity Level	<ol style="list-style-type: none"> a. Click ▾ . The severity level drop-down menu appears. b. Select a severity level option.
Application	<ol style="list-style-type: none"> a. Click ▾ . The application drop-down menu appears. b. Select an application. The Category option appears. <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p> Note The Category option does not appear if you select any applications or do not specify the application.</p> </div> <ol style="list-style-type: none"> c. Specify the application Category.
Date	<ol style="list-style-type: none"> a. Click ▾ . The date drop-down menu appears. b. Select a date option.
Content	<ol style="list-style-type: none"> a. Click ▾ . The content condition option appears. b. Select a condition. c. Specify the content keywords.
User	<ol style="list-style-type: none"> a. Click ▾ . The user condition option appears. b. Select a condition. c. Specify the keywords.
Source IP	<ol style="list-style-type: none"> a. Click ▾ . The source IP address condition option appears. b. Select a condition. c. Specify the source IP address.


8. Optional: Click **Reset** to clear all search filters.
Respecify search filters as many times as required.
9. Click **Search**.
The list of filtered results is displayed.
10. Click **Add as Customized Tab**.
The **Add as Customized Tab** window appears.

11. Enter a tab name.
12. Click **Apply**.
 - The custom filter tab is created.
 - The custom filter tab is displayed next to the **Main** tab.

Creating a Custom Filter Tab for System Access Log on a Sender Device

1. Open QuLog Center.
2. Go to **QuLog Service > Sender Devices** .
3. Click on a sender device.
4. Go to **System Access Log** .
5. Go to the search bar.
6. Click ▾ .
7. Specify the following filter fields:


Fields	Steps
Severity Level	<ol style="list-style-type: none"> a. Click ▾ . The severity level drop-down menu appears. b. Select a severity level option.
Accessed Resources	<ol style="list-style-type: none"> a. Click ▾ . The content condition option appears. b. Select a condition. c. Specify the keywords.
Date	<ol style="list-style-type: none"> a. Click ▾ . The date drop-down menu appears. b. Select a date option.
Connection type	<ol style="list-style-type: none"> a. Click ▾ . The connection type option appears. b. Select a connection type.
User	<ol style="list-style-type: none"> a. Click ▾ . The user condition option appears. b. Select a condition. c. Specify the keywords.
Action	<ol style="list-style-type: none"> a. Click ▾ . The action drop-down menu appears. b. Select an action option.

Fields	Steps
Source IP	<ol style="list-style-type: none"> a. Click  . The source IP address condition option appears. b. Select a condition. c. Specify the source IP address.

8. Optional: Click **Reset** to clear all search filters.
Respecify search filters as many times as required.
9. Click **Search**.
The list of filtered results is displayed.
10. Click **Add as Customized Tab**.
The **Add as Customized Tab** window appears.
11. Enter a tab name.
12. Click **Apply**.
 - The custom filter tab is created.
 - The custom filter tab is displayed next to the **Main** tab.

Configuring Event Indicators on the Sender Device

The event severity indicators on the device list are displayed according to the event severity level (information, warning, and error) that occurs over a specified period. Only the highest severity level icon is displayed when multiple events occur.

1. Open QuLog Center.
2. Go to **QuLog Service > Sender Devices** .
3. Select a device.
4. Click **Event Indicators**.
5. Click  .
The event period drop-down menu appears.
6. Select the event period.
Events that meet the specified criteria are listed in the Event Flag Rules table below.



Tip

You can remove event flag rules from the list.




Notification Settings

You can configure notification rules in Notification Center. You can also create filters for sending local NAS system access logs, QuLog Service system event logs, and QuLog Service system access logs.

Configuring Notification Rule Settings

QuLog Center can send notifications to recipients when the **Log Receiver** receives system event logs or system access logs from the **Log Sender**.


1. Open QuLog Center.
2. Go to **Notification Settings**.
3. Select the log types.
4. You can perform any of the following actions:

Setting	Steps
Create a notification rule	<p>a. Click Configure Notification Rule. Notification Center opens. Follow the instructions on the Create event notification rule wizard to add an event notification rule for QuLog Center. For details, see Creating an Event Notification Rule.</p> <p> Important You must select the Log filter criteria option in System Notification Rules when creating QuLog Center notification rules for receiving local device logs, QuLog Service system event logs, and QuLog Service system access logs. To enable the Log filter criteria option, go to Notification Center > System Notification Rules > QuLog Center > Log Filter Criteria .</p> <p>b. Click Apply. The notification rule is created.</p>
Edit a notification rule	Click  .
Enable or disable a notification rule	Click toggle.
Delete a notification rule	<p>a. Click  . A confirmation message window appears.</p> <p>b. Click Yes. The notification rule is deleted.</p>
View notification history	Click View notification history . Notification Center opens and displays the QuLog Center notification history page.

Adding a Log Filter


You can add filter criteria to local NAS system access logs, QuLog Service system event logs, and QuLog Service system access logs. The filtered log results are sent to Notification Center.

1. Open QuLog Center.
2. Go to **Notification Settings**.
3. Select a system log type.
4. Click **Add Filter Criteria**.
The filter criteria window appears.
5. Specify the following information:

Log Type	Settings
System Event Log	<ul style="list-style-type: none"> • Severity level • User • Source IP • Application • Category • Content • Hostname
System Access Log	<ul style="list-style-type: none"> • Severity level • User • Source IP • Accessed resources • Hostname <div style="margin-top: 10px;">  Note This option is only available for QuLog Service devices. </div> <ul style="list-style-type: none"> • Connection type • Action


6. Click **Apply**.
The filter is applied to logs sent to Notification Center.

Editing a Log Filter

1. Open QuLog Center.
2. Go to **QuLog Service > Notification Settings**.
3. Select a filter criteria.
4. Optional: Click **Reset** to clear all filter criteria settings.
5. Click .
The **Filter Criteria** window appears.
6. Edit the log filter criteria.
For details, see [Adding a Log Filter](#).
7. Click **Apply**.
All changes are applied.

Removing a Log Filter

1. Open QuLog Center.
2. Go to **QuLog Service > Notification Settings**.

3. Select a filter criteria.
4. Click  .
A confirmation message window appears.
5. Click **Yes**.
The filter criteria is removed.

17. Notification Center

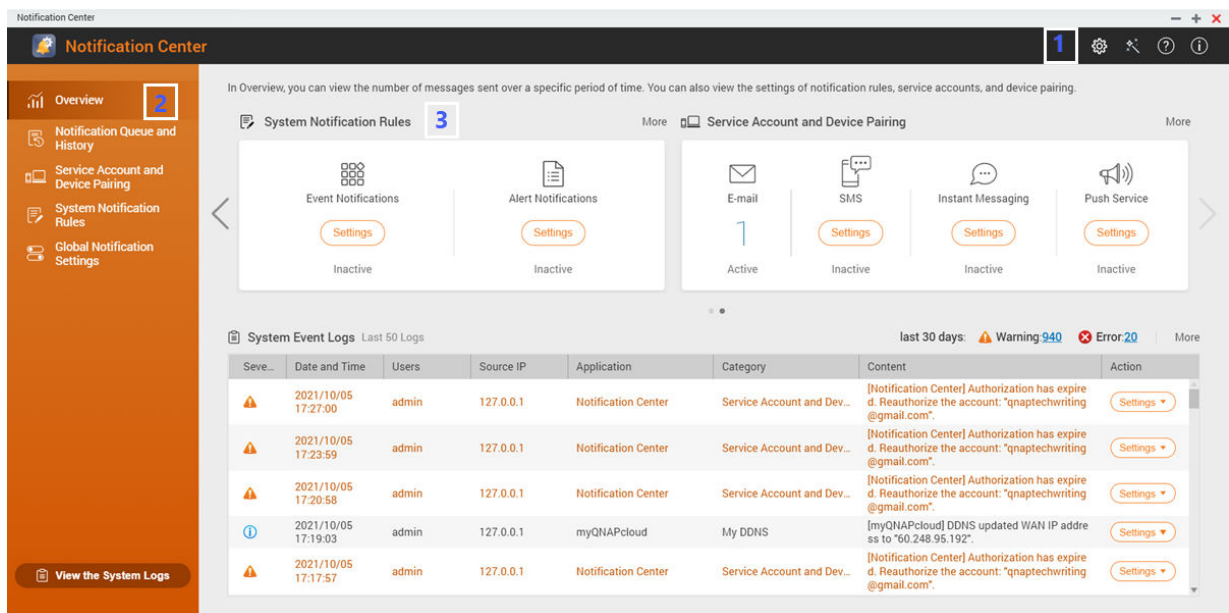
About Notification Center



Notification Center consolidates all QuTS hero notifications to help you monitor the status of your NAS and its applications and address potential issues more closely and promptly.

To send notifications to recipients, you must create custom notification rules, specify the delivery method, and define additional notification criteria in Notification Center. The application supports different delivery channels including emails, SMS, instant messaging, and other push services.

Parts of the User Interface

The Notification Center user interface has three main areas.



Label	Area	Description
1	Toolbar	<p>The toolbar displays the following options:</p> <ul style="list-style-type: none"> • Settings: Allows you to send Notification Center data to QNAP. <p> Important QNAP does not collect your personal data or information.</p> <ol style="list-style-type: none"> Click . The Send Notification data to QNAP window appears. Select Send Notification data to QNAP. Click Apply. <ul style="list-style-type: none"> • Quick Start: Opens the Notification Center guide. • Help: Opens the Notification Center Help panel. • About: Displays the application version.
2	Menu	The menu allows access to different configuration sections of Notification Center.
3	Main panel	The main panel displays the selected menu option. The Overview screen displays the number of notifications delivered over a specific period of time. It also displays the number of notification rules, service accounts, and paired devices you configured.

Managing Notification Queue and History


Notification Center allows you to view notification queues and notification history. You can view pending notification messages that Notification Center will send on the **Queue** screen, or go to the **History** screen to view all delivered notification messages.

Queue

The **Queue** screen displays the messages that Notification Center is going to send. The required transmission time depends on the current status of your device. You can remove messages at any time before they are sent. Removed messages do not appear on the **History** screen.

History

The **History** screen displays the messages that Notification Center has sent. You can view details, resend messages, configure settings, and export the history as a CSV file. You can also specify how long notification records are retained and where they are stored in **Settings**.

Tasks	User Actions
Export the notification message history.	Click Export . Notification Center saves the CSV file on your computer.
Resend the notification.	Identify the notification you want to resend, and then click  . This button only appears when Notification Center is unable to send the notification to the recipient.







Tasks	User Actions
Configure the history settings.	<ol style="list-style-type: none"> 1. Click Settings. The Settings window appears. 2. Specify the maximum number of days to retain notification records before deletion. 3. Click Confirm. Notification Center saves your settings.

Service Account and Device Pairing

Service Account and Device Pairing allows you to configure the simple mail transfer protocol (SMTP) and short message service center (SMSC) settings so you can receive notifications through email and SMS. You can also pair your instant messaging accounts and devices with your NAS to receive notifications through instant messaging or push services.

Email Notifications


The **Email** screen allows you to add and view email notification recipients, and also configure the SMTP service settings.

Button	Task	User Action
	Send a test message to the specified recipient	<ol style="list-style-type: none"> 1. Click  . 2. Specify an email address. 3. Click Send.
	Edit configurations of an existing email server	<ol style="list-style-type: none"> 1. Click  . The Edit SMTP Service Account window appears. 2. Edit the email account settings. 3. Optional: Click Re-authorization. The configured email account is authorized again. 4. Optional: Click Authenticate with Browser Station. For details, see Pairing Notification Center with a Web Browser. 5. Optional: Click Set as the default SMTP service account. 6. Click Confirm.
	Delete an email server	<ol style="list-style-type: none"> 1. Click  . A confirmation message appears. 2. Click Confirm.

Configuring an Email Notification Server

1. Go to **Service Account and Device Pairing > E-mail** .


2. Click **Add SMTP Service**.
The **Add SMTP Service** window appears.
3. Select an email account.
4. Configure the following.

Service Providers	User Actions
Gmail or Outlook	<ol style="list-style-type: none"> a. Click Add account. The email account window appears. b. Specify the email address that will act as the sender for QuTS hero notifications. A confirmation message appears. c. Click Allow.
Yahoo	<div style="border-left: 2px solid red; padding-left: 10px;">  <p>Important You must configure settings in Yahoo Mail before specifying your account information in Notification Center.</p> <ol style="list-style-type: none"> a. Log in to your Yahoo Mail account. b. Go to Help > Account Info > Account Security. c. Enable Allow apps that use less secure sign in. </div> <p>Return to Notification Center and specify a valid Yahoo mail address and password.</p>
Custom	<ol style="list-style-type: none"> a. Specify the domain name or the IP address of your SMTP service such as <code>smtp.gmail.com</code>. b. Specify the port number for the SMTP server. If you specified an SMTP port when you configured the port forwarding settings, use this port number. c. Specify the email address that will act as the sender for QuTS hero notifications. d. Specify a username that contains a maximum of 128 ASCII characters. e. Specify a password that contains a maximum of 128 ASCII characters. f. Select one of the following secure connection options. <ul style="list-style-type: none"> • SSL: Use SSL to secure the connection. • TLS: Use TLS to secure the connection. • None: Do not use a secure connection. <p>QNAP recommends enabling a secure connection if the SMTP server supports it.</p>
Others	Specify a valid email address and its account password.



Tip

To configure multiple email servers, click **Add SMTP Service**, and then perform the previous steps.

5. Optional: Select **Set as default SMTP service account**.
6. Optional: Click .
The SMTP server sends a test email.

7. Click **Create**.
Notification Center adds the SMTP service to the list.

Configuring an Email Server Account Using Browser Station

You can add an email server account using **Browser Station** authentication to secure your remote email server without setting up a VPN.



Important

Before using **Browser Station** to authenticate an email server account, ensure that:

- You have **File Station** access permission.
- **Container Station** is installed on your device.
- Any proxy server you are using to access **Browser Station** supports WebSocket.
- For details, see:
 - [How to Use Browser Station](#)
 - [How to Use Container Station](#)

1. Go to **Service Account and Device Pairing > E-mail**.
2. Click **Add SMTP Service**.
The **Add SMTP Service** window appears.
3. Click **Authenticate with Browser Station**.
The **Browser Station** window appears.









Note

It may take a few minutes for the **Browser Station** window to load.

4. Specify your gmail account.
5. Click **Next**.
6. Enter your password.
7. Click **Next**.
A warning appears.
8. Click **Allow**.
Add SMTP Service window appears.
9. Optional: Select **Set as default SMTP service account**.
10. Click **Create**.
The SMTP service is added.

SMS Notifications


The **SMS** screen allows you to view and configure the short message service center (SMSC) settings. You can either configure a custom SMSC or use any of the currently supported SMS service providers: Clickatell, Vonage (Nexmo), and Twilio.

Button	Task	User Action
	Send a test message to a specified recipient	<ol style="list-style-type: none"> 1. Click . The Send test message window appears. 2. Specify a country code and phone number. 3. Click Send.
	Edit configurations of an existing SMS server	<ol style="list-style-type: none"> 1. Click . The Edit SMSC Service Account window appears. 2. Edit the settings. 3. Click Confirm.
	Delete an email server	<ol style="list-style-type: none"> 1. Click . A confirmation message appears. 2. Click Confirm.

Configuring an SMS Notification

1. Go to **Service Account and Device Pairing > SMS** .
2. Click **Add SMSC Service**.
The **Add SMSC Service** window appears.
3. Select a service provider.
4. Specify an alias.
5. Specify the following information.


SMS Service Provider	Information
Clickatell - Communicator/Central	Clickatell username, password, and API ID
Clickatell - SMS Platform	Clickatell API key
Vonage (Nexmo)	Vonage API key and secret question, and a sender name The sender name can contain a maximum of 32 characters.
Twilio	Your Twilio account SID, access token, and the Twilio-provided phone number linked to your account

SMS Service Provider	Information
Custom	<ul style="list-style-type: none"> • URL template text formatted according to the format specified by your SMS service provider. Use the following replaceable URL template parameters. <ul style="list-style-type: none"> • @@UserName@@: Specify the username for this connection. • @@Password@@: Specify the password for this connection. • @@PhoneNumber@@: Specify the phone number where the SMS messages are sent. This parameter is required. • @@Text@@: Specify the text content of the SMS message. This parameter is required. <p> Important You cannot receive SMS messages if the template text does not match the format used by your SMS service provider.</p> <ul style="list-style-type: none"> • The name of the service provider. The name can contain a maximum of 32 ASCII characters. • A password. The password can contain a maximum of 32 ASCII characters.







Tip

To configure multiple SMS servers, click **Add SMSC Service**, and then perform the previous steps.

6. Click  .
The SMS server sends a test message.
7. Click **Create**.
Notification Center adds the SMS service to the list.

Instant Messaging Notifications

The **Instant Messaging** screen allows you to pair Notification Center with instant messaging accounts such as Skype and Facebook Messenger. Notification Center sends notifications to the specified recipients through QBot, the QNAP instant messaging bot account.

Button	Task	User Action
	Send a test message	Click  .
	Unpair from and remove the instant messaging account	<ol style="list-style-type: none"> 1. Click  . A confirmation message appears. 2. Click Confirm.

Pairing Notification Center with Skype

Before configuring Skype notifications, ensure that:

- Your NAS is registered to an active myQNAPcloud account.
- You have an active Skype account.
- Skype is installed on your device.

1. Go to **Service Account and Device Pairing > Instant Messaging** .
2. Click **Add IM Account**.
The **Notification IM Wizard** appears.
3. Select Skype.
The **Add Bot to Contacts** window appears.
4. Log in to the Skype account you want to pair.
Skype adds QNAP Bot as a contact.
5. Close the **Add Bot to Contacts** window.
6. Click **Next**.
A verification code appears.
7. On Skype, enter the verification code.
Notification Center verifies and pairs with the Skype account.
8. Click **Finish**.
Notification Center adds the Skype account to the list.

Pairing Notification Center with Facebook Messenger

Before configuring instant messaging (IM) notifications, ensure the following.

- Your NAS is registered to an active myQNAPcloud account.
- You have an active Facebook Messenger account.

1. Go to **Service Account and Device Pairing > Instant Messaging** .
2. Click **Add IM Account**.
The **Notification IM Wizard** appears.
3. Select Facebook Messenger.
The **Add Bot to Contacts** window appears.
4. Log in to the Facebook Messenger account you want to pair.
Facebook Messenger adds QNAP Bot as a contact.
5. Click **Get Started**.
A verification code appears on the **Notification IM Wizard**.
6. On Facebook Messenger, enter the verification code.
Notification Center verifies and pairs with the Facebook Messenger account.
7. Click **Finish**.
Notification Center adds the Facebook Messenger account to the list.

Push Notifications


The **Push Service** screen allows you to configure push services for web browsers and mobile devices. Notification Center supports pairing the application with multiple third-party push notification services.

Pairing Notification Center with a Mobile Device

Before pairing, ensure that:

- Your NAS is registered to an active myQNAPcloud account.
- Qmanager iOS 1.8.0 or Qmanager Android 2.1.0 (or later versions) is installed on your mobile device.
- Your NAS is added to Qmanager.

1. Open Qmanager on the mobile device.
2. Perform one of the following.

Pairing Option	User Action
Automatic pairing	<ol style="list-style-type: none"> a. From the device list, click the NAS you want to pair. A confirmation message appears. b. Click Confirm.
Manual pairing	<ol style="list-style-type: none"> a. Identify your NAS from the device list, and then click . The device settings screen appears. b. Select Push notifications. c. Click Save. A confirmation message appears. d. Click Confirm.

Notification Center pairs with the mobile device.


3. In Notification Center, go to **Service Account and Device Pairing > Push Service**.
4. Verify that the mobile device appears in the list of paired devices.

Pairing Notification Center with a Web Browser

Before pairing, ensure that:

- Your device is registered to an active myQNAPcloud account.
- You are using one of the following web browsers:
 - Chrome 42 (or later versions)
 - Firefox 50 (or later versions)

1. Go to **Service Account and Device Pairing > Push Service**.
2. Under Browser, click **Pair**.
Notification Center pairs with your current browser.
The browser appears in the list of paired devices.

3. Change your browser name.
 - a. Beside your browser name, click .
 - b. Specify a browser name.
The field accepts up to 127 ASCII characters.
 - c. Press the Enter or Return key on the keyboard.
Notification Center saves your browser name.

System Notification Rules

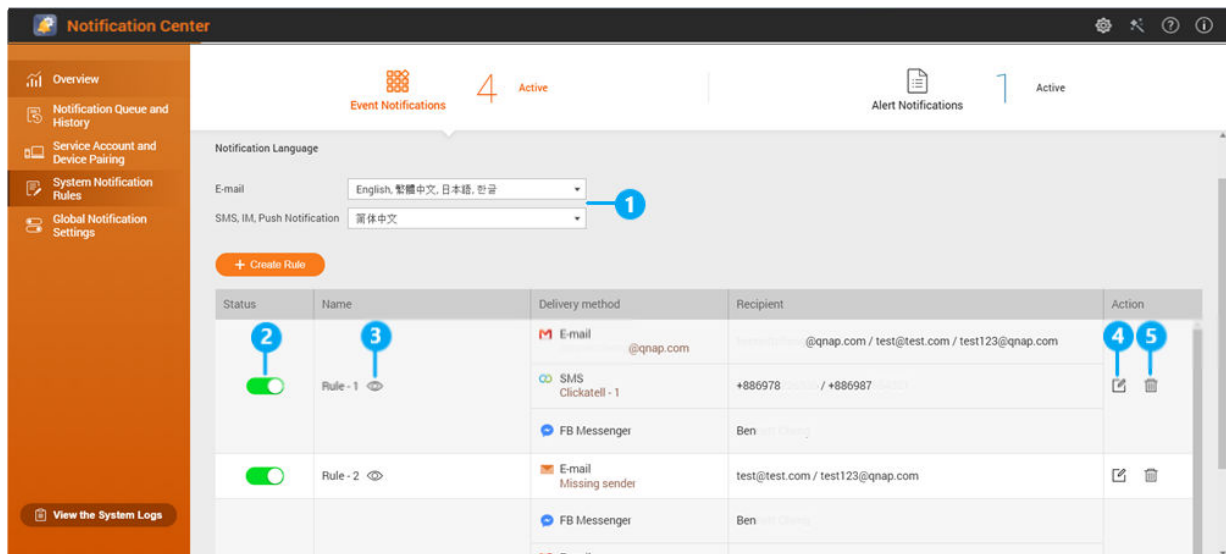
You can create and manage event notification rules in the **Event Notifications** page to receive event notifications promptly.


You can also configure alert notifications to specified recipients in the **Alert Notifications** page by setting the alert severity levels.




Managing Event Notification Rules

The **Event Notifications** screen allows you to create and customize rules to send notifications to target recipients. To send notifications, you must first create and enable rules that determine which application event triggers the outbound notification. You can customize the message type, delivery method, keywords, and time range to further define notification types or narrow the scope.

Notification Center supports sending event notifications in multiple languages and provides four delivery methods to meet your different needs, including emails, SMS, instant messaging, and push services.



Label	Tasks	User Actions
1	Specify a notification language	<ol style="list-style-type: none"> 1. Select one or more languages for email notifications. 2. Select a language for SMS, IM, and push notifications.
2	Enable or disable the rule	Click  .

Label	Tasks	User Actions
3	Preview rule settings	<ol style="list-style-type: none"> 1. Click . The Event Notifications window appears. 2. Review the settings, and then click Close.
4	Edit the rule	<ol style="list-style-type: none"> 1. Click . The Edit Rule for Event Notifications window appears. 2. Edit the settings. 3. Click Confirm.
5	Delete a rule	<ol style="list-style-type: none"> 1. Click . A confirmation message appears. 2. Click Confirm.

Creating an Event Notification Rule

Before creating a notification rule, ensure that your NAS is registered to an active myQNAPcloud account.

1. Go to **System Notification Rules > Event Notifications**.
2. Click **Create Rule**.
The **Create event notification rule** window appears.
3. Specify a rule name.
4. Select the events you want recipients to be notified of.



Tip



To select all events, select **Select all**.
To display only the events for a specific application or service, select the item from the **Displayed Items** drop-down menu.

5. Click **Next**.
6. Select a severity level.

Severity Level	Description
Information	Information messages inform users of changes in the NAS settings or its applications.
Warning	Warning messages inform users of events when NAS resources, such as storage space and memory, are critically low, or when the hardware behaves abnormally.
Error	Error messages inform users of problems that occur when the system tries to update or run applications or processes or when it fails to enable or disable NAS features.

7. Optional: Specify a keyword filter.

Filter	Description
All messages	Notification Center sends all notifications that are classified under the types you selected.



Filter	Description
Includes	Notification Center sends only the notifications that are classified under the types you selected and includes the keywords you specify. To add keyword filters, click  , and then specify one or more keywords.
Excludes	Notification Center sends only the notifications that are classified under the types you selected and excludes the keywords you specify. To add keyword filters, click  , and then specify one or more keywords.









Important


The event notification filter only accepts keywords that are in English or in any of the languages specified on the **Event Notifications** screen.

- 8. Optional: Specify a time range when you want to receive notifications.
- 9. Click **Next**.
- 10. Select a delivery method.
- 11. Configure the sender information.

Method	User Action
Email	<p>a. Select an SMTP server.</p> <div style="display: flex; align-items: flex-start;">  <div> <p>Tip To add an SMTP server, see Configuring an Email Notification Server.</p> </div> </div> <p>b. Optional: Specify a custom subject line. This text replaces the original email subject line. Use this to help recipients better understand the notifications they receive.</p> <p>c. Optional: Select Send email as plain text.</p> <p>d. Optional: Add an email account using Browser Station. For details, see Configuring an Email Server Account Using Browser Station.</p>
SMS	<p>Select an SMSC server.</p> <div style="display: flex; align-items: flex-start;">  <div> <p>Note To add an SMSC server, see Configuring an SMS Notification Server.</p> </div> </div>
Instant Messaging or Push Service	<p>Notification Center automatically assigns Qbot.</p>

- 12. Configure the recipient information.









Method	User Action
Email	<p>a. Click Select NAS User. The Select NAS User window appears.</p> <p>b. Select one or more NAS users.</p> <p>c. Click Finish. The Select NAS User window closes.</p> <p> Tip</p> <ul style="list-style-type: none"> • To add a recipient, click Add, and then specify their email address. • To delete a recipient, click .
SMS	<p>a. Click Select NAS User. The Select NAS User window appears.</p> <p>b. Select one or more NAS users.</p> <p>c. Click Finish. The Select NAS User window closes.</p> <p>d. Select a country code for each recipient.</p> <p> Tip</p> <ul style="list-style-type: none"> • To add a recipient, click Add, and then specify their cell phone number. • To delete a recipient, click .
Instant Messaging	<p>Select one or more recipients.</p> <p> Tip To add instant messaging notification recipients, see the following topics:</p> <ul style="list-style-type: none"> • Pairing Notification Center with Skype • Pairing Notification Center with Facebook Messenger
Push Service	<p>Select one or more recipients.</p> <p> Tip To add push notification recipients, see the following topics:</p> <ul style="list-style-type: none"> • Pairing Notification Center with a Mobile Device • Pairing Notification Center with a Web Browser

13. Optional: Click  to send a test message.
14. Optional: Click **Add Pair** to create a new pair.
15. Click **Next**.
16. Verify the rule settings.

- Click **Finish**.
Notification Center displays the new rule on the **Event Notifications** screen.

Managing Alert Notification Rules

You can create custom rules to receive alert notifications from the System Logs based on the notification type and keywords in the **Alert Notifications** screen. You can also specify the delivery methods, contents, and recipients of these notifications.

Button	Task	User Action
	Enable or disable the rule	Click  .
	Preview rule settings	<ol style="list-style-type: none"> Click . The Alert Notifications window appears. Review the settings, and then click Close.
	Edit the rule	<ol style="list-style-type: none"> Click . The Edit Rule for Alert Notifications window appears. Edit the settings. Click Confirm.
	Unpair from and remove the device or browser	<ol style="list-style-type: none"> Click . A confirmation message appears. Click Confirm.



Creating an Alert Notification Rule

Before creating a notification rule, ensure that your NAS is registered to an active myQNAPcloud account.

- Go to **System Notification Rules > Alert Notifications**.
- Click **Create Rule**.
The **Create alert notification rule** window appears.
- Specify a rule name.
- Select the events you want recipients to be notified of.
 - Select a severity level.

Severity Level	Description
Information	Information messages inform users of changes in the NAS settings or its applications.
Warning	Warning messages inform users of events when NAS resources, such as storage space and memory, are critically low, or when the hardware behaves abnormally.
Error	Error messages inform users of problems that occur when the system tries to update or run applications or processes or when it fails to enable or disable NAS features.

- Optional: Specify a keyword filter.



Filter	Description
All messages	Notification Center sends all notifications that are classified under the types you selected.
Includes	Notification Center sends only the notifications that are classified under the types you selected and includes the keywords you specify. To add keyword filters, click  , and then specify one or more keywords.
Excludes	Notification Center sends only the notifications that are classified under the types you selected and excludes the keywords you specify. To add keyword filters, click  , and then specify one or more keywords.









Important


The alert notification filter only accepts keywords that are in English.

5. Optional: Specify a time range when you want to receive notifications.
6. Optional: Specify a notification message threshold.
7. Click **Next**.
8. Select a delivery method.
9. Configure the sender information.

Method	User Action
Email	<p>a. Select an SMTP server.</p> <p> Tip To add an SMTP server, see Configuring an Email Notification Server.</p> <p>b. Optional: Specify a custom subject line. This text replaces the original email subject line. Use this to help recipients better understand the notifications they receive.</p> <p>c. Optional: Select Send email as plain text.</p>
SMS	<p>Select an SMSC server.</p> <p> Note To add an SMSC server, see Configuring an SMS Notification Server.</p>
Instant Messaging or Push Service	Notification Center automatically assigns Qbot.


10. Configure the recipient information.

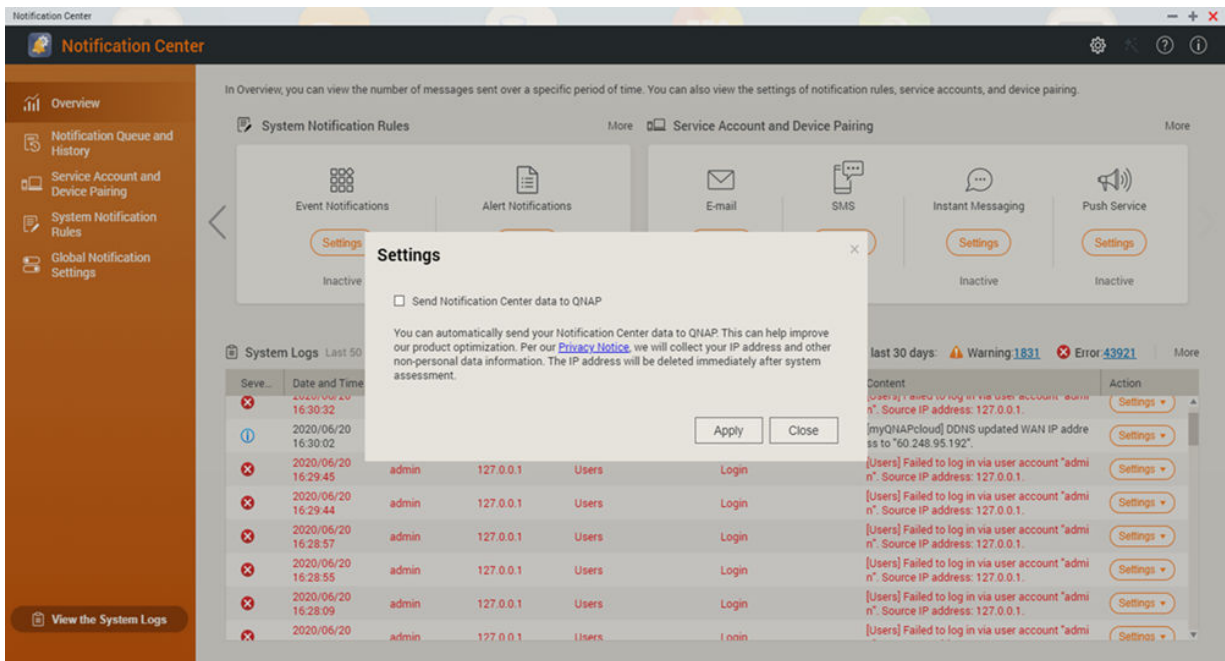
Method	User Action
Email	<p>a. Click Select NAS User. The Select NAS User window appears.</p> <p>b. Select one or more NAS users.</p> <p>c. Click Finish. The Select NAS User window closes.</p> <p> Tip</p> <ul style="list-style-type: none"> • To add a recipient, click Add, and then specify their email address. • To delete a recipient, click .
SMS	<p>a. Click Select NAS User. The Select NAS User window appears.</p> <p>b. Select one or more NAS users.</p> <p>c. Click Finish. The Select NAS User window closes.</p> <p>d. Select a country code for each recipient.</p> <p> Tip</p> <ul style="list-style-type: none"> • To add a recipient, click Add, and then specify their cell phone number. • To delete a recipient, click .
Instant Messaging	<p>Select one or more recipients.</p> <p> Tip To add instant messaging notification recipients, see the following topics:</p> <ul style="list-style-type: none"> • Pairing Notification Center with Skype • Pairing Notification Center with Facebook Messenger
Push Service	<p>Select one or more recipients.</p> <p> Tip To add push notification recipients, see the following topics:</p> <ul style="list-style-type: none"> • Pairing Notification Center with a Mobile Device • Pairing Notification Center with a Web Browser

11. Optional: Click  to send a test message.
12. Optional: Click **Add Pair** to create a new pair.
13. Click **Next**.
14. Verify the rule settings.

15. Click **Finish**.
Notification Center displays the new rule on the **Alert Notifications** screen.

Settings

The **Settings** screen allows you to enable or disable submitting Notification Center data to QNAP. Click  to open the **Settings** window.




Enabling Send Notification Data to QNAP



Important

QNAP does not collect your personal data or information.


1. Open **Notification Center**.
2. Click .
The **Send Notification data to QNAP** window appears.
3. Select **Send Notification data to QNAP**.
4. Click **Apply**.

Disabling Send Notification Data to QNAP



Important

QNAP does not collect your personal data or information.

1. Open **Notification Center**.
2. Click .
The **Send Notification data to QNAP** window appears.

3. Deselect **Send Notification data to QNAP**.
4. Click **Apply**.

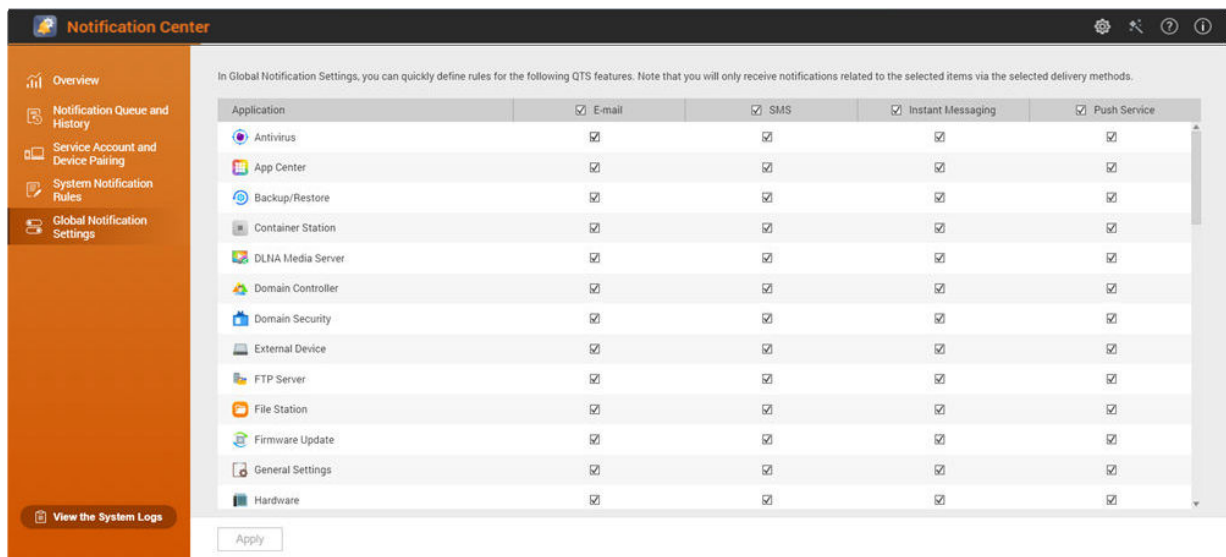
Global Notification Settings

The **Global Notification Settings** screen allows you to quickly define global notification rules. From the list, you can select or deselect, and then apply the delivery methods for each QuTS hero feature or application.

Users only receive notifications related to the selected features through their selected delivery methods.





Tip Ensure that you click **Apply** after configuring the global notification settings.



System Event Logs

The **System Event Logs** screen displays all the recorded system events on the NAS. On this screen, you can sort and filter the logs or create notification rules based on existing logs.

Task	User Action
Filter system logs	Select a severity level.

Task	User Action
Search system logs	<p>Search for logs by keywords or through advanced search. To use advanced search follow the instructions below:</p> <ol style="list-style-type: none"> 1. Click  in the search bar. The advanced search option drop down menu appears. 2. Specify the following parameters where applicable: <ul style="list-style-type: none"> • Keyword • Severity Level • Date • Users • Source IP • Application • Category 3. Click Search. Lists all log entries that meet the specified conditions.
Create a notification rule	<ol style="list-style-type: none"> 1. Click Settings. 2. Select one of the following options. <ul style="list-style-type: none"> • Create event notification rule • Create alert notification rule <p>The Create notification rule window appears.</p> 3. Select one of the following options. <ul style="list-style-type: none"> • Add as a new rule • Add to an existing rule 4. Click Confirm. <p> Tip To add or edit notification rules, see the following topics:</p> <ul style="list-style-type: none"> • Creating an Event Notification Rule • Creating an Alert Notification Rule

18. Malware Remover

About Malware Remover

Malware Remover is a built-in utility designed to protect QNAP devices against harmful software. Malware programs are often disguised as or embedded in nonmalicious files and software. They often attempt to gain access to sensitive user information and may negatively impact device performance.

Implementing several layers of protection, Malware Remover allows you to perform instant and scheduled scans on your QNAP device and prevents malicious software from putting your data at risk.

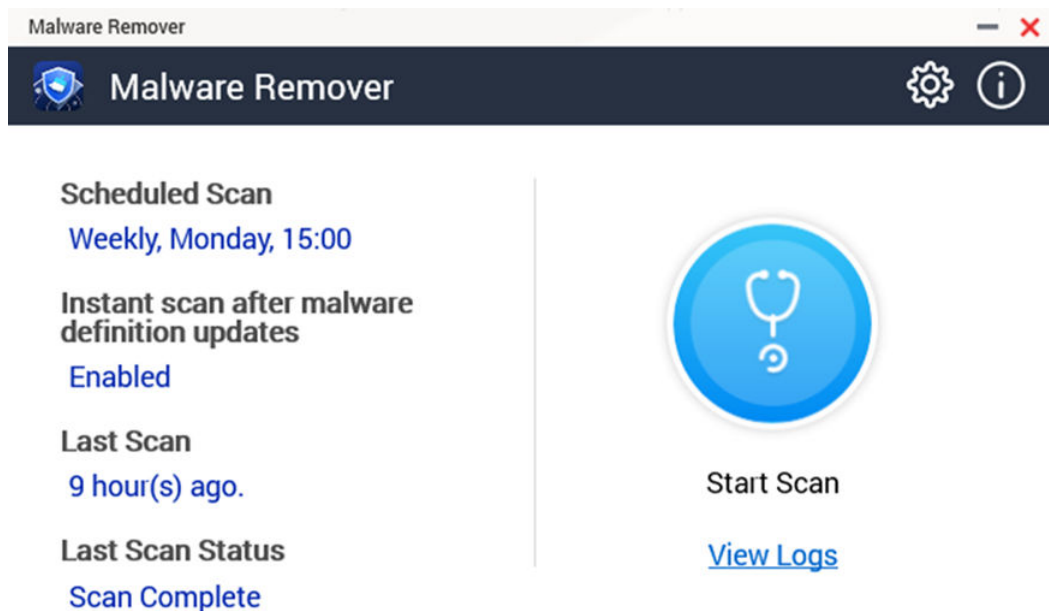


Important

QNAP strongly recommends running routine scans to prevent malware infections and protect the system from advanced risks, threats, and vulnerabilities.

Overview

This screen displays information and controls connected to Malware Remover.




Running a Malware Scan

1. Open Malware Remover.

2.



Click . Malware Remover begins the scan.

3. Optional: After the scan finishes, click **View Logs** to view the results.


Running a Scheduled Scan

Scheduled scans periodically look for security threats on your QNAP device.



Note


The **Enable scheduled scan** checkbox is enabled by default.

1. Open Malware Remover.
2. Click .
3. Choose from the scheduled scan drop-down menu to configure the settings.

Setting	Description
Daily	The scheduled scan runs daily at the specified time.
Weekly	The scheduled scan runs once a week on the specified day and time.
Monthly	The scheduled scan runs once a month on the specified date and time.

4. Click **Apply**.

Configuring Malware Remover

1. Open Malware Remover.
2. Click .
The **Settings** window opens.
3. Configure the settings.





Note


All settings are enabled by default to prevent malware threats from infecting the system.



Tip

QNAP recommends running scans during off-peak hours.

Setting	Description
Enable scheduled scan	<p>Enable to scan all applications and files at the user-configured frequency and time. For details, see Running a Scheduled Scan.</p> <p> Note Enabling this setting ensures Malware Remover performs routine scans of your device.</p>
Instant scan after malware definition updates	<p>Enable this option to run instant scans once Malware Remover updates the malware definitions.</p> <p> Note Malware Remover automatically updates malware signatures and security patches to have the most up-to-date security content.</p>

Setting	Description
Send Malware Remover scan results to QNAP	<p data-bbox="592 255 1382 320">Enable this option to submit the scan results for malware analysis. QNAP collects the following data:</p> <ul data-bbox="616 344 1353 701" style="list-style-type: none"><li data-bbox="616 344 772 376">• NAS model<li data-bbox="616 405 1353 470">• NAS IP address (The IP address is immediately deleted after analyzing the malware scan results.)<li data-bbox="616 499 772 530">• Scan status<li data-bbox="616 560 772 591">• Scan errors<li data-bbox="616 620 1034 651">• Malware detection date and time<li data-bbox="616 680 772 712">• Malware ID <p data-bbox="592 734 1326 831"> Note Disabling this option prevents Malware Remover from sending any data to QNAP.</p>

4. Click **Apply**.
Malware Remover saves the settings.

19. Helpdesk


Helpdesk is a built-in application that allows you to quickly find solutions or contact the QNAP support team when you encounter any issues while using QuTS hero and related applications.

Overview

On the **Overview** screen, you can contact the QNAP support team, browse frequently asked questions and application notes, download QNAP user manuals, find out how to use a QNAP devices, search the QNAP knowledge base, and find compatible devices. This screen also displays Helpdesk message logs.

Title	Description
Help Request	Contact the QNAP support team by submitting your issues or questions.
QNAP Online Tutorial & FAQ	Browse frequently asked questions and application notes for QNAP NAS and applications.
User Manual	View or download QNAP user manuals.
QNAP Helpdesk Knowledge Base	Search the QNAP knowledge base for answers from the support team for different issues.
Compatibility List	Find drives and devices that are compatible with QNAP NAS.
My Tickets	View your submitted tickets status.

Configuring Settings

1. Open **Helpdesk**.
2. Go to **Overview**.
3. Click .
The **Settings** window appears.
4. Specify the message retention time.
5. Optional: Click **Retain all messages**.
6. Optional: Click **I am allowing QNAP Support to access my system logs**.
7. Optional: Click **Sign In**.
The **Settings** window appears.
8. Specify your QNAP ID.
9. Specify the password.
10. Click **Sign In**.
11. Click **Apply**.

Help Request

Help Request allows users to directly submit requests to QNAP from your NAS. Helpdesk automatically collects and attaches NAS system information and system logs to your request to help the QNAP technical support team identify and troubleshoot potential issues.

Submitting a Ticket

You can submit a Helpdesk ticket to receive support from QNAP. Helpdesk automatically collects and attaches device system information and system logs to your request to help the QNAP technical support team identify and troubleshoot potential issues.

1. Open **Helpdesk**.
2. Go to **Help Request**.
3. Sign in with your QNAP ID.
4. Specify the ticket details.

Fields	User Actions
Subject	Specify the subject.
Issue Category	Select an issue category, and then select an issue.
Issue Type	Select an issue type.
Operating System	Select an operating system.
Description	Specify a short description for each issue.

5. Upload the attachments.
 - a. Optional: Select **I am allowing QNAP Support to access my system logs**.
 - b. Upload screenshots or other related files.



Note

- You can upload up to 8 attachments, including system logs.
- Each file must be less than 5 MB.

6. Specify the following information.

Fields	User Actions
Your Email Address	Specify your email address.
Phone number	Specify your phone number.
Customer type	Select a customer type.
Company name	Specify your company name. <div style="display: flex; align-items: center;"> <div> <p>Note This field only appears when you select Business User as the Customer type.</p> </div> </div>
Your timezone	Select a timezone.
Apply the changes to my profile in QNAP Account	Click to apply your profile changes in QNAP Account.
First name	Specify your first name.
Last name	Specify your last name.
Your location	Select a location.

7. Optional: Select **Apply the changes to my profile in QNAP Account**.

8. Click **Submit**.

Remote Support

Remote Support allows the QNAP support team to access your NAS directly to assist you with your issues.

Enabling Remote Support

1. Open **Helpdesk**.
2. Go to **Remote Support**.
3. Specify your ticket ID.
4. Specify your email address.
5. Click **Enable Remote Support**.
The **QNAP Helpdesk Terms of Service** window appears.
6. Accept the terms of service.
 - a. Click **I agree to these Terms of Service**.
 - b. Click **Agree**.
The **Enable Remote Support** window appears.



Note

Enable Remote Support is only required when you enable the feature for the first time.

7. Click **Yes**.
The **Enable Remote Support** window appears.
8. Click **Confirm**.
Helpdesk creates a private key and temporary account.

Extending Remote Support

Extending Remote Support allows the users to extend the remote session by a week in case users want to have the remote session at a specific time. QNAP will also notify the user to extend the session if the issue is unsolved.

1. Open **Helpdesk**.
2. Go to **Remote Support**.
3. Click **Extend**.



Note

The **Extend** button only appears after Remote Support is enabled.

Disabling Remote Support

1. Open **Helpdesk**.
2. Go to **Remote Support**.
3. Click **Disable**.

**Note**

The **Disable** button only appears after Remote Support is enabled.

4. Click **Finish**.

**Note**

Remote Support will also be disabled when the support team has completed the remote session, or when the private key has expired.

Diagnostic Tool

The Diagnostic Tool provides several features for checking the stability of the NAS. Users can export system kernel records to quickly check whether abnormal operations have recently occurred. In addition, users can send the records to QNAP technical support for further investigation. The Diagnostic Tool also provides features for checking the file system, hard drives, and RAM.

Downloading Logs

The Diagnostic Tool provides download log features for checking the device stability. You can export the system kernel records to quickly check for exceptions or errors that have occurred. In addition, you can send the records to QNAP technical support for further investigation.

1. Open **Helpdesk**.
2. Go to **Diagnostic Tool > Download Logs** .
3. Click **Download**.
Helpdesk generates a ZIP file.
4. Download the ZIP file.
5. Optional: Send the file to QNAP through Help Request for further investigation.

Performing an HDD Standby Test

1. Open **Helpdesk**.
2. Go to **Diagnostic Tool > HDD Standby Test** .
3. Select an enclosure to analyze.
4. Click **Start**.
Helpdesk performs an HDD standby test.
5. Optional: Click **Download** to download the test reports.

Performing an HDD Stress Test

1. Open **Helpdesk**.
2. Go to **Diagnostic Tool > HDD Stress Test** .
3. Click **Start**.
Helpdesk performs an HDD stress test.

20. Console Management

Console Management is a text-based tool that helps system administrators perform basic configuration or maintenance tasks, and provide technical support to the NAS users. The program is accessible only after the operating system has finished initialization. Console Management is enabled by default, but you can disable it in the Control Panel. For details, go to the System Settings section of the QuTS hero User Guide. Currently, disabling Console Management only applies to QuTS hero.

Only users in the administrator group can use Console Management, which launches automatically when administrators log in using SSH login, a serial console, or an HDMI monitor and a USB keyboard.

Enabling Secure Shell (SSH)

Secure Shell (SSH) is a cryptographic network protocol that can access Console Management. If you want to access Console Management using SSH, you must first enable SSH on the NAS.

Enabling SSH on the NAS

1. Log in to the NAS as administrator.
2. Go to **Control Panel > Network & File Services > Telnet / SSH**.
3. Select **Allow SSH connection (Only administrators can login remotely.)**.
4. Optional: Change the port number.
5. Click **Apply**.

Enabling SSH on the NAS Using Qfinder Pro

1. Open **Qfinder Pro**, and then locate the NAS you want to access.
2. Click **Settings**.
3. Select **Connect via SSH**.
The **Connect via SSH** screen appears.
4. Log in to the NAS as administrator.

Accessing Console Management

Before you can access Console Management, you must first enable SSH using the NAS or Qfinder Pro. A third-party software is also required on Windows platforms but not on Mac platforms.

Accessing Console Management from Windows

1. Download PuTTY from <https://www.putty.org/>, and then follow the on-screen instructions to install the software.
2. Open PuTTY, and type the device's IP address underneath **Host Name (or IP address)**.
3. Select **SSH** as the connection type.



Note

This option is selected by default.

4. Click **Open**.
The **PuTTY Security Alert** window appears.

**Note**

This window only appears when you first run the application.

5. Click **Yes**.
A login screen appears.

Accessing Console Management from Mac

1. Open **Terminal**.
2. Enter `ssh USERNAME@NAS_IP`.

**Note**

Replace `NAS_IP` with the device's IP address.

**Tip**

If you encounter an error, enter `ssh-keygen -R NAS_IP`. Replace `NAS_IP` with the device's IP address.

3. Press **ENTER**.
A login screen appears.

Logging In to Console Management

**Important**

Before performing this task, you must first complete the following tasks:

- Enable Secure Shell (SSH).
- Download the third-party software for your platform if it is required. For details, see the following topics:
 - [Accessing Console Management from Windows](#)
 - [Accessing Console Management from Mac](#)

1. Log in as administrator.
 - a. Enter the username.
 - b. Enter the password.

**Note**

For security purposes, the password does not show.

**Tip**

Do not copy and paste the password to the program.

The **Console Management - Main menu** screen appears.

Managing Existing Applications

1. Log in to Console Management, and then enter 5.

The App window and three options appear.

2. Enter the alphanumeric character corresponding with the action you want to perform.



Tip

To browse your applications, enter **n** or **p** to go to the next or previous page.

Option	User Action
List installed apps	Enter 1. Console Management displays a list of all installed applications on the operating system.
List enabled apps	Enter 2. Console Management displays a list of all enabled applications on the operating system.
List disabled apps	Enter 3. Console Management displays a list of all disabled applications on the operating system.
Return	Enter r . Console Management returns to Main menu.

A list of applications appear.

3. Enter the alphanumeric character corresponding with the application you want to perform an action on.
Five options appear.
4. Enter the alphanumeric character corresponding with the action you want to perform.

Option	User Action
Start	Enter 1. The application starts.
Stop	Enter 2. The application stops.
Restart	Enter 3. The application restarts.
Remove	Enter 4. The application is removed. <div style="display: flex; align-items: center;"> <p>Note If an application can't be removed, Console Management tells you that this function is currently unavailable.</p> </div>
Return	Enter r . Console Management returns to Main menu.

The system performs the specified action and tells you whether the action has succeeded or not.

Activating or Deactivating a License

1. Log in to Console Management, and then enter 4.
Two options appear.

2. Enter the alphanumeric character corresponding with the action you want to perform.

Option	User Action
Activate a License	<ol style="list-style-type: none"> Enter 1. Enter a license activation key.
Deactivate a License	<ol style="list-style-type: none"> Enter 2. Enter a license activation key.
Return	Enter \uparrow . Console Management returns to Main menu.

The system performs the specified action.

Sorting and Filtering System Logs

1. Log in to Console Management, and then enter 2.
Eleven options appear.
2. Enter the alphanumeric character corresponding with the action you want to perform.



Note

System logs are displayed in the following format: record_id, date, time, user, app_id, application, category_id, category, msg_id, message.

Option	User Action
date in ascending order	Enter 1. Console Management displays all system logs in ascending order according to the date.
date in descending order (default)	Enter 2. Console Management displays all system logs in descending order according to the date.
user in ascending order	Enter 3. Console Management displays all system logs in ascending order according to the username.
user in descending order	Enter 4. Console Management displays all system logs in descending order according to the username.
IP in ascending order	Enter 5. Console Management displays all system logs in ascending order according to the IP address.
IP in descending order	Enter 6. Console Management displays all system logs in descending order according to the IP address.
app name in ascending order	Enter 7. Console Management displays all system logs in ascending order according to the application name.
app name in descending order	Enter 8. Console Management displays all system logs in descending order according to the application name.

Option	User Action
category in ascending order	Enter 9. Console Management displays all system logs in ascending order according to the application category.
category in descending order	Enter 10. Console Management displays all system logs in descending order according to the application category.

The filter screen appears.

3. Optional: Enter a filter query.



Note

- Ensure all filter conditions follow the relevant on-screen format. For example, filtering by an application name should follow this format: A={myQNAPcloud}.
- To filter by multiple conditions, use '&' in between filters. For example, filtering by severity level and an application name should follow this format: T={0} &A={myQNAPcloud}.

Filter	User Action
Severity level	<p>a. Enter one of the following options.</p> <ul style="list-style-type: none"> • T={ 0 } <p> Note This filter only includes system logs classified as information. This type of system log is indicated as in QuLog Center.</p> <ul style="list-style-type: none"> • T={ 1 } <p> Note This filter only includes system logs classified as warnings. This type of system log is indicated as in QuLog Center.</p> <ul style="list-style-type: none"> • T={ 2 } <p> Note This filter only includes system logs classified as errors. This type of system log is indicated as in QuLog Center.</p> <p>Console Management filters all system logs according to the specified severity level.</p>
Keyword	Enter a keyword. Console Management filters all system logs according to the specified keyword.
Username	Type an username. Console Management filters all system logs according to the specified username.
Source IP	Enter a source IP. Console Management filters all system logs according to the specified source IP.
Application name	Enter an application name. Console Management filters all system logs according to the specified application name.

Filter	User Action
Category name	Enter an application category. Console Management filters all system logs according to the specified category.

A list of system logs appear.



Tip

To browse your applications, enter **n** or **p** to go to the next or previous page.

Showing Network Settings

1. Log in to Console Management as administrator, and then enter **1**.



Note

Network settings appear in the following format: adapter, virtual switch, status, IP, MAC address.

The Network settings window appears.

Restoring or Reinitializing the Device

1. Log in to Console Management as administrator, and then enter **3**.
The **Reset** window and five options appear.
2. Enter the alphanumeric character corresponding with the action you want to perform.



Note

The admin password is required to reset the settings or reinitialize the device.

Option	User Action
Reset network settings	Enter 1 . Console Management resets the network settings.
Reset system settings	Enter 2 . Console Management restores system settings to default without erasing user data.
Restore factory defaults & format all volumes	Enter 3 . Console Management restores the system settings to default and formats all disk volumes.
Reboot to reinitialize the device	Enter 4 . Console Management erases all data and reinitializes the device.
Return	Enter r . Console Management returns to Main menu.

Rebooting the NAS

You can reboot the NAS into rescue or maintenance mode from Console Management.

Rebooting the Device Into Rescue Mode

1. Log in to **Console Management** as administrator, and then type **6** and press **ENTER**.
The **Reboot in rescue mode** window opens.

2. Type `y`, and then press **ENTER**.

**Note**

Press escape or type `n` and press to go to the **Main Menu**.

Console Management reboots the device.

Rebooting the Device Into Maintenance Mode

1. Log in to **Console Management** as administrator, and then type `7` and press **ENTER**.
The **Reboot in maintenance mode** window opens.
2. Type `y`, and then press **ENTER**.
Press escape or type `n` and press to go to the **Main Menu**.
Console Management reboots the device.