



Enhance your NAS data security with our in-depth guide



Live Broadcast Date:

MAY 9, 2018

Live Broadcast Date:

5:30 p.m. (UTC+8)



QNAP

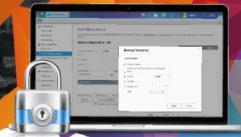


**Enhance your NAS data security
with our in-depth guide**

Targeted Attacks on your NAS

- Weak credentials / Default password
- Older firmware
- Default port
- Disabled HTTPS

Don't Forget the Little Things ! The easier things are, the more easily they'll be overlooked!



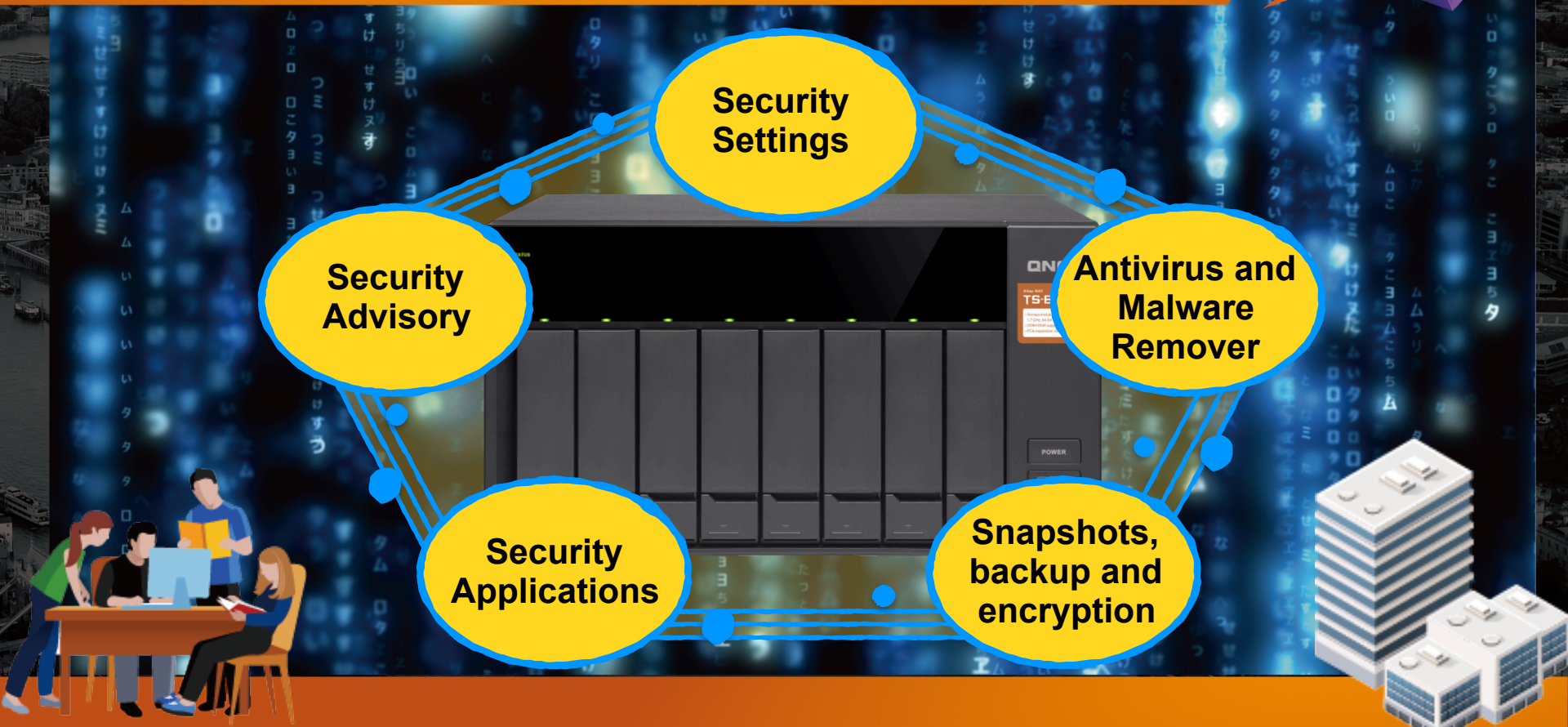
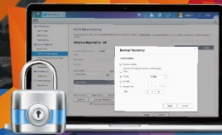


**Keep your NAS secured
and your data safe.**



QNAP

How to Secure Your NAS





**To fight against data
breach,
check the following categories**

Account

Network

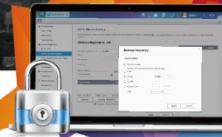
System

Update

QNAP

- **Password Strength** : Use strengthen password or force regularly change password.
- **2-step Verification** : 2-step verification is to enhance the security of user accounts.





Enhance Password Strength

Control Panel

← ControlPanel

System

Privilege

Network & File

Applications

General Settings

Storage & Snapshots

Security

Hardware

Power

Notification

Firmware Update

Backup / Restore

External Device

System Status

System Logs

Resource Monitor

License Center

Security Level

Network Access Protection

Certificate & Private Key

Password Policy

Password Strength

The following criteria could be applied to strengthen password security.

☐

A new password has to contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.

☐

No character in the new password may be repeated three (or more) times consecutively.

☐

The new password must not be the same as the associated username, or the username reversed.

Change Password

☐

Force NAS users to regularly change their password.

Maximum password age (days)

90

☐

Send a notification email to users a week in advance of their password expiring

i

Note: The "Disallow the user to change password" function will be disabled if "Force NAS users to regularly change their password" is enabled.

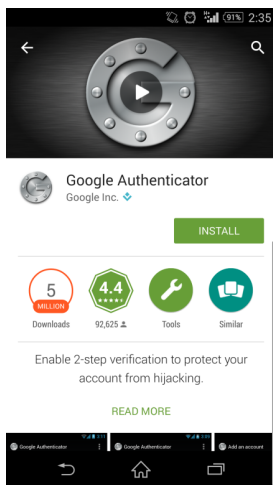
Apply



Enable 2-step Verification

(1) Install the authenticator app on your mobile device

- For Android and iOS devices, install the Google Authenticator app from their respective app stores.
- For Windows Phone, install the Authenticator from its Store.

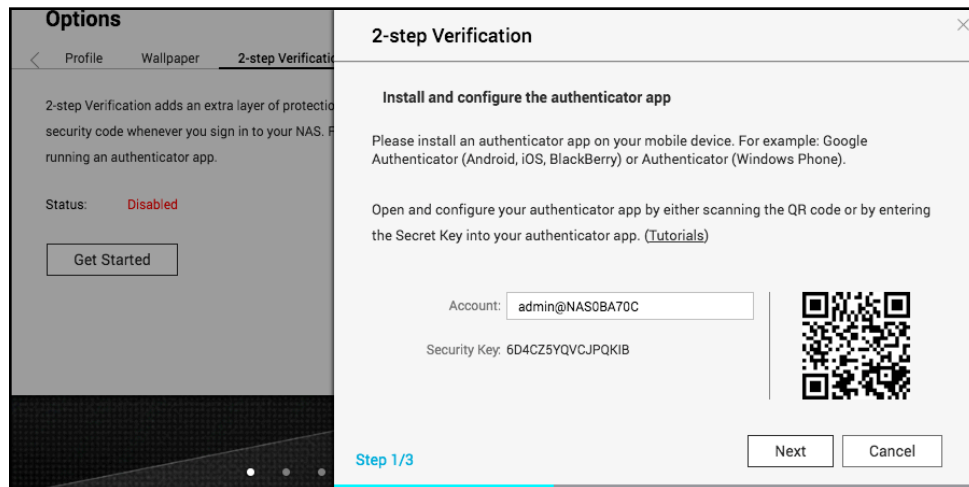


Kind Reminder:

The system time of your mobile device and NAS must be synchronized. It is recommended to use the time provided from the Internet.

(2) Enable 2-step Verification

Go to "Options" > "2-step Verification" and click "Get Started". Complete the steps in the wizard to set up the NAS and your mobile device.



1. **Disable Telnet/SSH/FTP/TFTP** if you don't need them.
2. **Change SSH/HTTPS/HTTP/FTP port**
3. **Enable SSL/TLS** if you need to use connection, eg FTP service





Disable Telnet/SSH/FTP/TFTP if you don't need them.

Control Panel

← ControlPanel

System

Privilege

Network & File

Applications

Network & Virtual Switch

Network Access

Win/Mac/NFS

Telnet / SSH

SNMP

Service Discovery

FTP

Network Recycle Bin

After enabling this option, you can access this server via Telnet or SSH connection.

Note: Only the account admin can login remotely.

☐ Allow Telnet connection (Only the account admin can login remotely.)

Port number: 13131

☐ Allow SSH connection (Only administrators can login remotely.)

Port number: 22

☒ Enable SFTP

Edit Access Permission

Apply



Change SSH/HTTPS/HTTP port

Control Panel

← ControlPanel

System

Privilege

Network & File

Applications

General Settings

Storage & Snapshots

Security

Hardware

Power

Notification

Firmware Update

Backup / Restore

External Device

System Status

System Logs

Resource Monitor

License Center

System Administration

Time

Daylight Saving Time

Codepage

Region

Login Screen

Server name:

NAS0BA70C

You can change the default port number (HTTP) for Web Administration.

System port:

8080

☒ Disable and hide multimedia functions (these functions include the Media Library, DLNA server, iTunes server, and more).

☒ Enable secure connection (HTTPS)

Port number:

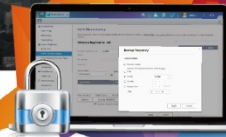
443

☒ Force secure connection (HTTPS) only

Note:After enabling the "Force secure connection (HTTPS) only" option, the Web Administration can only be connected via https.

Apply

Enable FTP with SSL/TLS (Explicit)



Control Panel

← ControlPanel

System

- Network & Virtual Switch
- Network Access
- Win/Mac/NFS
- Telnet / SSH
- SNMP
- Service Discovery
- FTP
- Network Recycle Bin

Privilege

Applications

FTP Service Advanced

General

☒ Enable FTP Service

Protocol type: ☒ FTP (Standard) ☐ FTP with SSL/TLS (Explicit)

Port number:

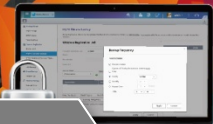
Unicode support: ☒ Yes ☐ No

Enable anonymous: ☐ Yes ☒ No

Note: If your FTP client does not support Unicode, please select "No" for Unicode Support and select a supported filename encoding from [\[Filename Encoding\]](#) under [\[General Settings\]](#)->[\[Codepage\]](#) so that the folders and files on FTP can be properly shown.

Connection

Apply



- **Deny/Allow connections list :**

You can set to allow or deny the connection of any specific IP address or the range.

- **Enable Network Access Protection :**

You can define the rules of IP blocking for different services or protocols. You can check the list of blocked IPs under “Security Level”.

- **Avoid installation of non-QNAP Store apps.**

- **Use SSL certificate :**

Certificates are used to verify the identity of a NAS and to create SSL/TLS encrypted communications between users and their NAS services (including web sites, FTP, and more).

Manage your Deny/Allow connections list



Control Panel

← ControlPanel

System | Privilege | Network & File | Applications

General Settings | Storage & Snapshots | Security | Hardware | Power | Notification | Firmware Update | Backup / Restore | External Device | System Status | System Logs | Resource Monitor | License Center

Security Level | Network Access Protection | Certificate & Private Key | Password Policy

☐ Allow all connections

☐ Deny connections from the list

☒ Allow connections from the list only

Enter the IP address or network from which the connection is made

Add Remove

Genre

Apply

Enter the IP address or network domain

☒ Single IP address

IP:

☐ Specify IP addresses of certain

IP:

Netmask: 255 255 0 0

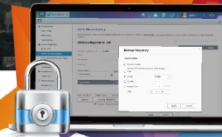
☐ IP Range

Start IP:

End IP:

The IP address value must be 0-255.

Create Cancel



Enable Network Access Protection

Control Panel

ControlPanel

System

Privilege

Network & File

Applications

General Settings

Storage & Snapshots

Security

Hardware

Power

Notification

Firmware Update

Backup / Restore

External Device

System Status

System Logs

Resource Monitor

License Center

Security Level

Network Access Protection

Certificate & Private Key

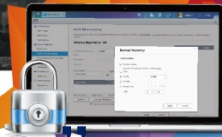
Password Policy

☒ Enable Network Access Protection

Network access protection automatically blocks a client's IP address if they fail to log in too many times within a specified time period. You can view the blocked IPs at [Security Level](#).

<input checked="" type="checkbox"/> SSH	Within: 30 minutes	Failed login attempts: 30	IP block length: 1 hour
<input checked="" type="checkbox"/> Telnet	Within: 10 minutes	Failed login attempts: 30	IP block length: 1 day
<input checked="" type="checkbox"/> HTTP(S)	Within: 30 minutes	Failed login attempts: 100	IP block length: forever
<input type="checkbox"/> FTP	Within: 1 minute	Failed login attempts: 5	IP block length: 5 minutes
<input type="checkbox"/> SAMBA	Within: 1 minute	Failed login attempts: 5	IP block length: 5 minutes
<input type="checkbox"/> AFP	Within: 1 minute	Failed login attempts: 5	IP block length: 5 minutes

Apply



Disable "Allow installation of non-QNAP Store apps."

App Center

AppCenter

Settings

General App Repository Update

☐ Allow installation of non-QNAP Store apps

Installing non-QNAP Store apps may expose your NAS to security risks.

Apply

Close

Install Updates: [C All](#)

QNAP Store

My Apps

All Apps

QTS Essentials

Recommended

Partners

Backup/ Sync

Business

Content Manage

Communications

Developer Tools

Download

Entertainment

Surveillance

Utilities

Home Automation

Security

Network & Virtual Switch Utilities

Resource Monitor 1.1.0 Utilities

Qsync Central 3.0.3 Backup/ Sync

License Center 1.0.1 Utilities

Proxy Server 1.3.2 Utilities

QTS SSL Certificate Utilities

[Open](#)

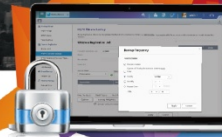
[Open](#)

[Open](#)

[Open](#)

[Open](#)

[Open](#)



Choices to Secure the Connection

QTS SSL Certificate



myQNAPcloud
SSL Certificate

Paid License

Full Technical Support

Enterprise's top choice

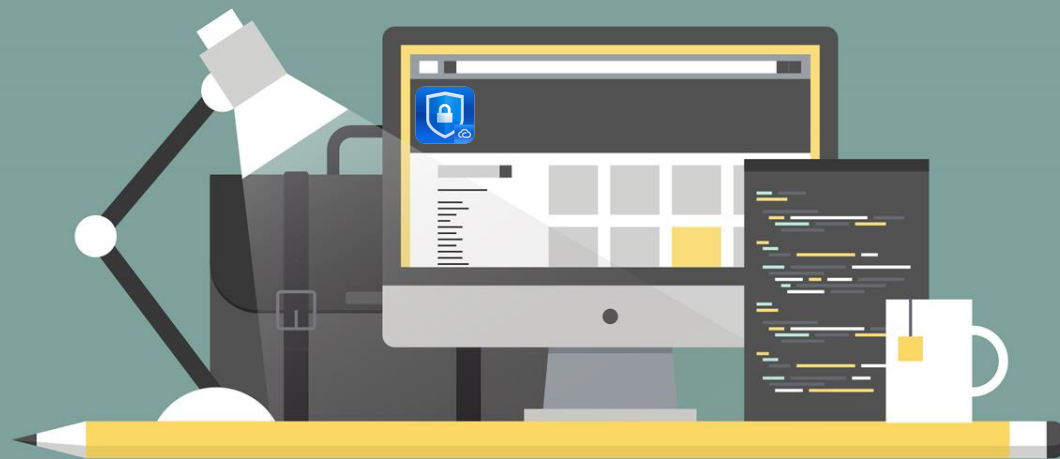


Let's Encrypt

Free

Partly Support

Auto Renew License



DEMO TIME

A horizontal navigation bar with seven chevron-shaped buttons. From left to right: 'Security Settings' (blue), 'Account' (light gray), 'Network' (light gray), 'System' (light gray), 'Update' (light blue), 'Antivirus & Malware Remover' (dark gray), 'Snapshots, backup and encryption' (dark gray), 'Security Applications' (dark gray), and 'Security Advisory' (dark gray).

Security Settings

Account

Network

System

Update

Antivirus &
Malware
Remover

Snapshots,
backup and
encryption

Security
Applications

Security
Advisory

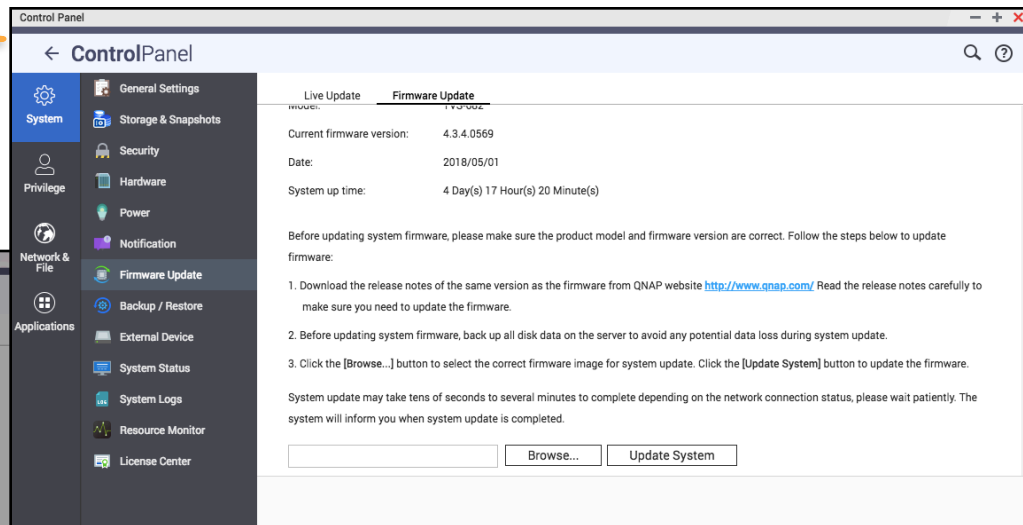
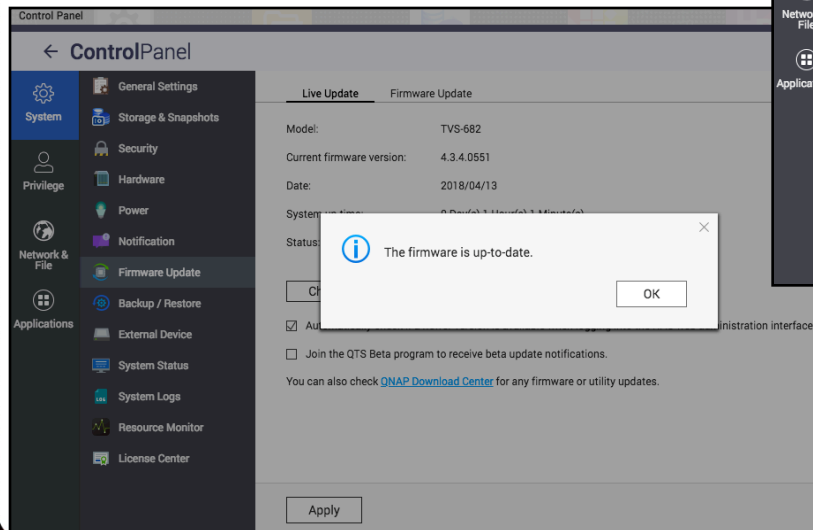
Always use the most up-to-date version of firmware and applications to ensure that known security issues are fixed.

- Firmware (QTS)
- Application (NAS App)
- Malware Remover
- Antivirus



Check for updated Firmware

Firmware update



Live update

Check for updated Applications



App Center

AppCenter

QNAP Store

My Apps 1

All Apps

QTS Essentials

Recommended

Partners

Backup/ Sync

Business

Content Management

Communications

Developer Tools

Download

Entertainment

Surveillance

Utilities

Home Automation

Security

Volume Info

QNAP Store (Update:1 | Installed:8)

Install Updates: [C All](#)

Update:1

Helpdesk 1.1.18 Utilities

[C Update](#)

Installed:8

Network & Virtual Switch Utilities

Resource Monitor 1.1.0 Utilities

Qsync Central 3.0.3 Backup/ Sync

License Center 1.0.1 Utilities

Proxy Server 1.3.2 Utilities

QTS SSL Certificate Utilities

[O Open](#)

[O Open](#)

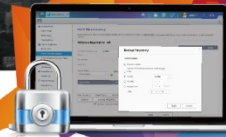
[O Open](#)

[O Open](#)

[O Open](#)

[O Open](#)

Check for updated Antivirus (Clam AV / McAfee)



Control Panel

← ControlPanel

System Privilege Network & File Applications

- HybridDesk Station
- Transcode Management
- Web Server
- LDAP Server
- SQL server
- Syslog Server
- Antivirus**
- RADIUS Server
- TFTP Server
- NTP Service

Overview Scan Jobs Reports Quarantine

Status: Updating...

Update

☐ Check and update automatically. Frequency in days:

Online update:

Manual update (*.cvd):

Update file available at: <http://www.clamav.net>

Quarantine

DataVol1: --

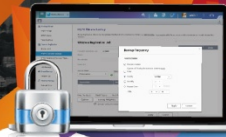
DataVol2: --



**To fight against malware
attacks,**

enable Antivirus and Malware Remover

QNAP

Security
SettingsAntivirus &
Malware
RemoverSnapshots,
backup and
encryptionSecurity
ApplicationsSecurity
Advisory

- **McAfee** helps to protect your data from viruses and malware by identifying, quarantining, and deleting infected files.



- **ClamAV** will scan the NAS manually or on recurring schedule and delete, quarantine, or report files infected by viruses, malware, Trojans, and other malicious threats.



- **Malware Remover** will scan your QNAP NAS and quarantine any detected malware.

To buy McAfee, go to License.qnap.com




QNAP STORE

Sign in Sign up (0) USD

License Store

Home > McAfee Antivirus



McAfee Antivirus

Item	McAfee Antivirus - 1 year
Unit price	USD \$25.00
Quantity	<div>- 1 +</div>
Payment types	<div>PayPal VISA MasterCard JCB American Express</div>
Total price USD \$25.00	

Add to Cart

or

Checkout

☐ I have read and agree to the [Terms of Service and Product Agreement.](#)

Description

The McAfee antivirus engine for QTS helps you protect your data from viruses and malware. The app lets you manually start or schedule scans, quarantine malicious files, and automatically update virus definitions.

Clam AV



Overview Scan Jobs **Reports** Quarantine

Number of days to keep the logs:

☐ Archive logs after expiration.

Save the archive files in the folder:

Job Name	Last Scan	Infected Files	Action
test	2018/05/04 01:08:30	0	 
test	2018/04/11 03:00:43	0	 

ClamAV

Page 1 / 1 | Display item: 1-2, Total: 2 | Show 10 Item(s)

Download All Logs

Malware Remover



Control Panel



File Station



myQNAPcloud



App Center



Help Center



Help Center



Qsirch



Qfiling



QButton



Ocean



Malware Remover



Schedule

Weekly, Sunday, 6:00 PM

Last Scanned Information

2018/01/08 03:24:12

Last Scanned Status

Scan Completed

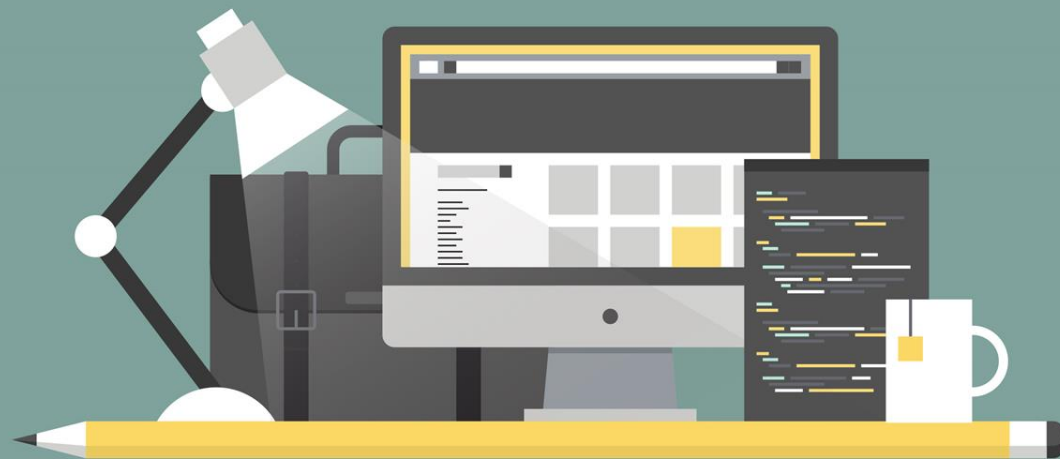
[View logs](#)



Scanning...

18:23

Thu., Mar 23



DEMO TIME



To avoid ransomware,
use snapshots, backup and encryption

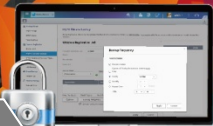
QNAP

**Security
Settings****Antivirus &
Malware
Remover****Snapshots,
backup and
encryption**

Snapshot

Backup

Encryption

**Security
Applications****Security
Advisory**

Make a recovery plan against encryption-based locker malware!



Block-based snapshots

QNAP's block-based snapshot supports incremental backups to save storage space. While copying only the changes made, it also saves time for backing up and restoring.



Restore in a click

Data recovery through snapshots only takes a few minutes. As they are separated from the file system, snapshots allow users to restore the original, unencrypted files even if the volume is affected by ransomware.



Snapshot Replica

After creating snapshots, you can efficiently copy them to another QNAP NAS for double protection.



Snapshot Reserve Space

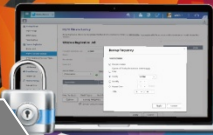
Ransomware's continual writing of data may cause snapshot protection to fail due to running out of space. QNAP's unique "Snapshot Reserve Space" helps prevent this by reserving dedicated space for snapshots.

Security
SettingsAntivirus &
Malware
RemoverSnapshots,
backup and
encryption

Snapshot

Backup

Encryption

Security
ApplicationsSecurity
Advisory

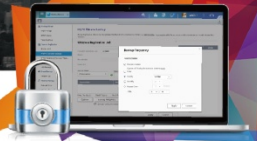
Multifunctional backup and recovery plan

- Hybrid Backup Sync is a multifunctional backup solution where you can easily back up data from a QNAP NAS to several local, remote and the cloud storage.
- Hybrid Backup Sync can help prevent data loss from accidents and disasters.





Hybrid Backup Sync - A central management system for backup/restore/sync of local, remote and cloud storage.



Hybrid Backup Sync

Overview

All Jobs

Storage Space

Backup Server

External Backup



Backup

Back up selected folders to a destination folder. Local backup and remote backup support multi-version backup, and all backup features support incremental backup.

Create Backup Job

Supported services:



Restore

Restore backed-up data to its original folder or to any other destination folder.

Create Restore Job

Supported services:

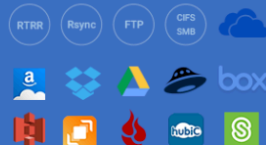


One-way Sync

Create folder pairing and synchronize the source folder with the destination folder if files are modified in the source folder.

Create Sync Job

Supported services:



Two-way Sync

Create folder pairing and synchronize the source folder with the destination folder if files are modified in either the source or destination folder.

Supported services:

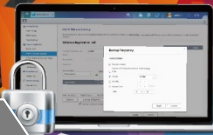


Security
SettingsAntivirus &
Malware
RemoverSnapshots,
backup and
encryption

Snapshot

Backup

Encryption

Security
ApplicationsSecurity
Advisory

Hardware-accelerated AES-256 encryption for volumes/LUNs to protect confidential data.

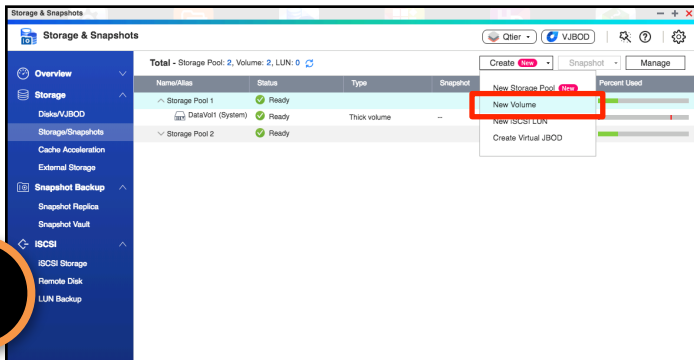
- **Encrypted disk volumes** can only be mounted for normal read/write access by using the authorized password. Encryption protects confidential data from unauthorized access even if the hard drives or the entire NAS were stolen.
- **Encrypt share folders** to protect confidential data from unauthorized access.



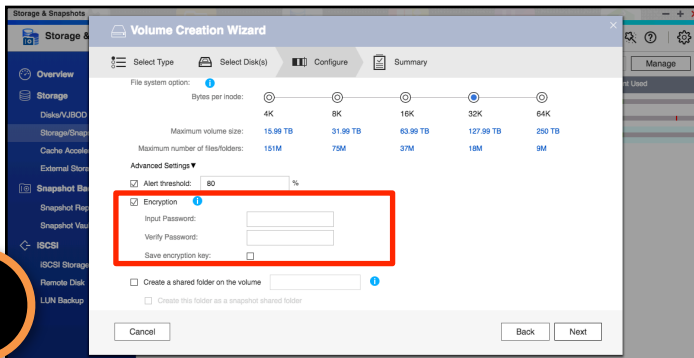
Encrypt disk volumes

1. Create a New Volume
2. Check "Encryption" and input password

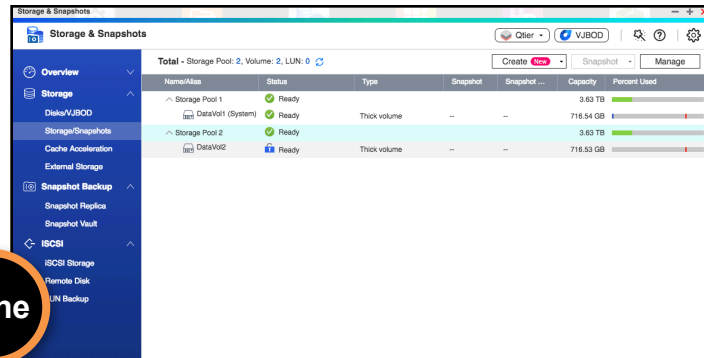
1



2



Done



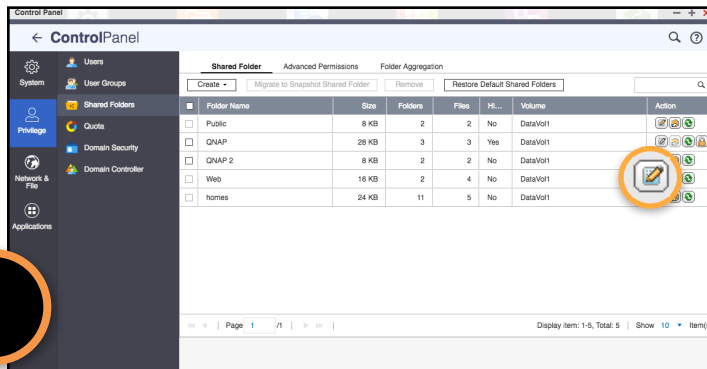


Encrypt share folders

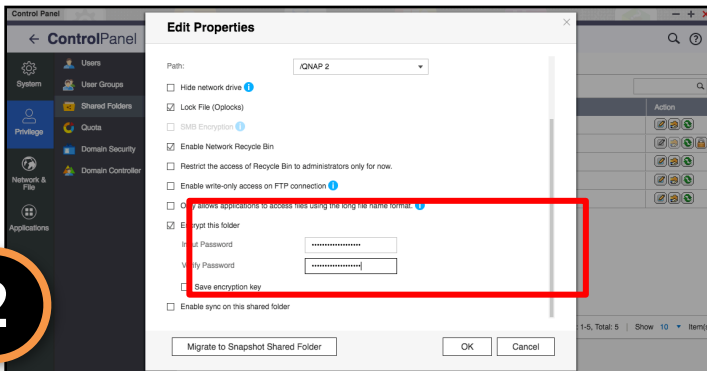
1. Go to “Control Panel” > “Share Folders”, choose the folder and then click “Edit Properties”
2. Check “Encrypt this folder” and input password.



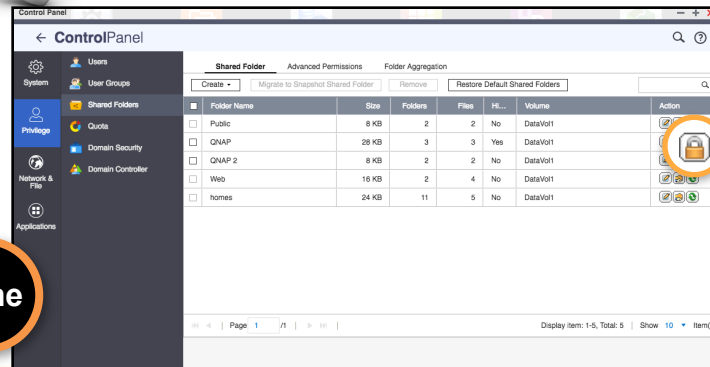
1



2



Done





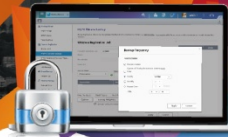
**Reduce the risk of being
attacked by hackers,
use QVPN Service and Proxy Server**

QNAP

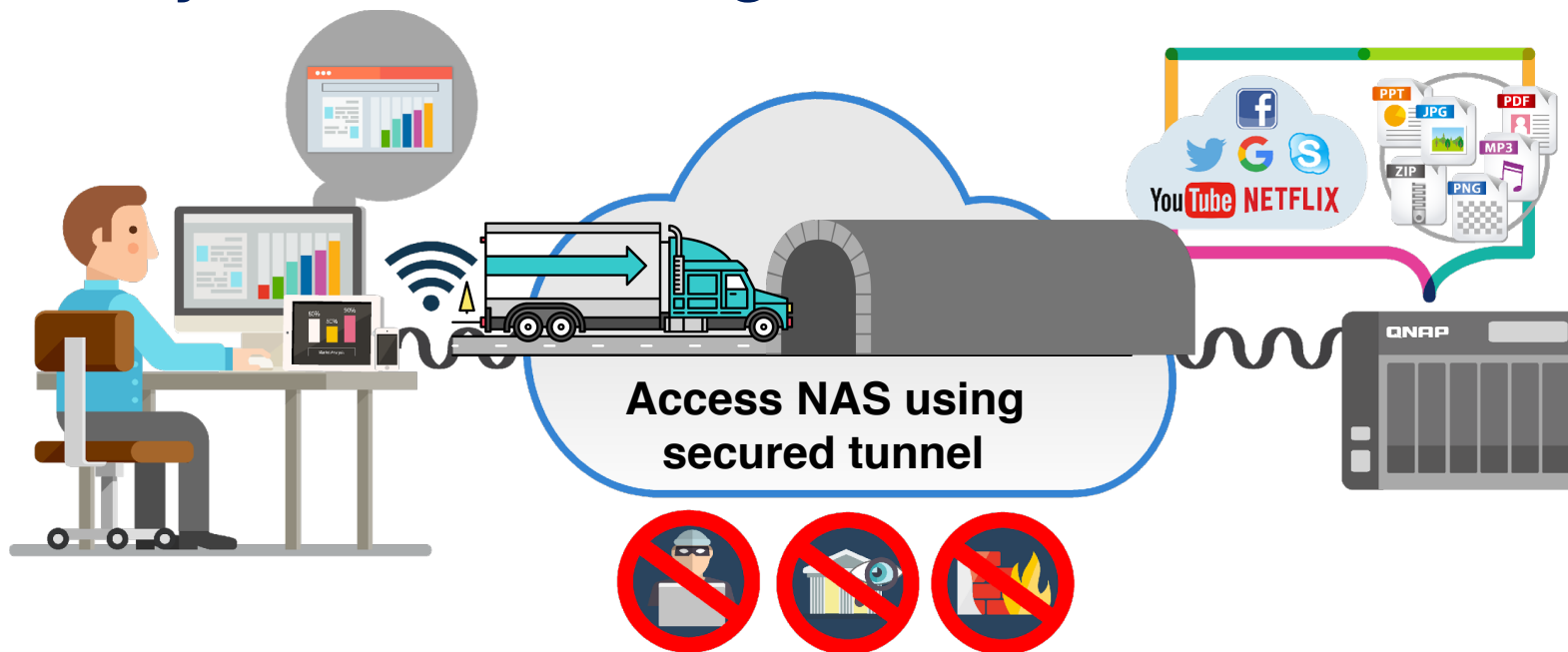
Security
SettingsAntivirus &
Malware
RemoverSnapshots,
backup and
encryptionSecurity
Applications

QVPN

Proxy

Security
Advisory

When you connect through the VPN





Q1, 2018 QNAP proprietary VPN protocol - QBelt



**Secure
Encrypted
Connection :**

**DTLS + SSL +
AES-256
encryption**



New protocol:

decrease the
chance of being
detected



**Works on all
your devices**



Easy to Use

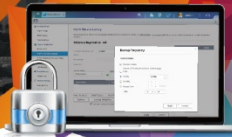


For QTS 4.3.5

Security
SettingsAntivirus &
Malware
RemoverSnapshots,
backup and
encryptionSecurity
Applications

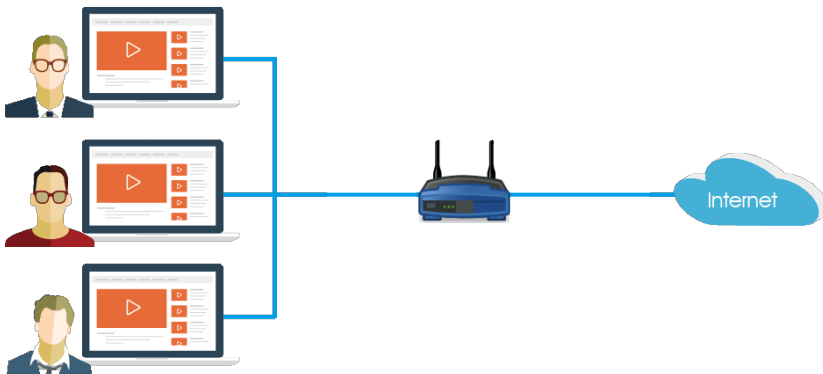
QVPN

Proxy

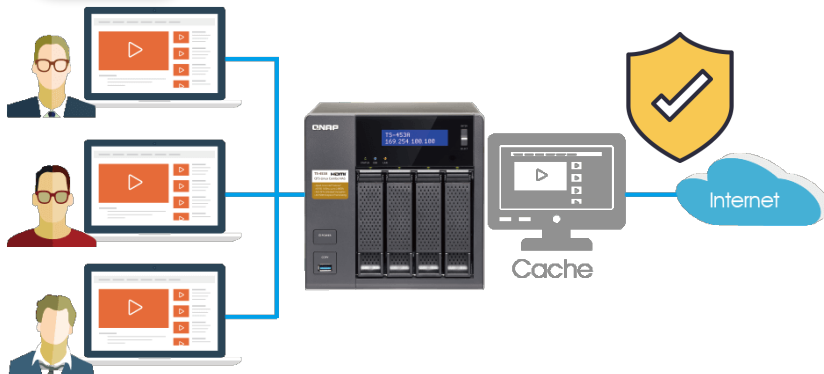
Security
Advisory

Proxy Server provides protected connection and able to utilize network usage more effectively.

Every computer connect to Internet via a router. All the connections and data protections are handled by themselves. And may result some weak points in LAN when browse malicious websites from unprotected computer.



Using Proxy Server can surf internet via NAS may save outgoing bandwidth. And server also provide unified protection to prevent accidental access to vicious websites.



Proxy Server suggested configuration



1 Enable virus scan

Proxy Server will notify you to download latest virus definition file if you did not enable ClamAV on this NAS before.

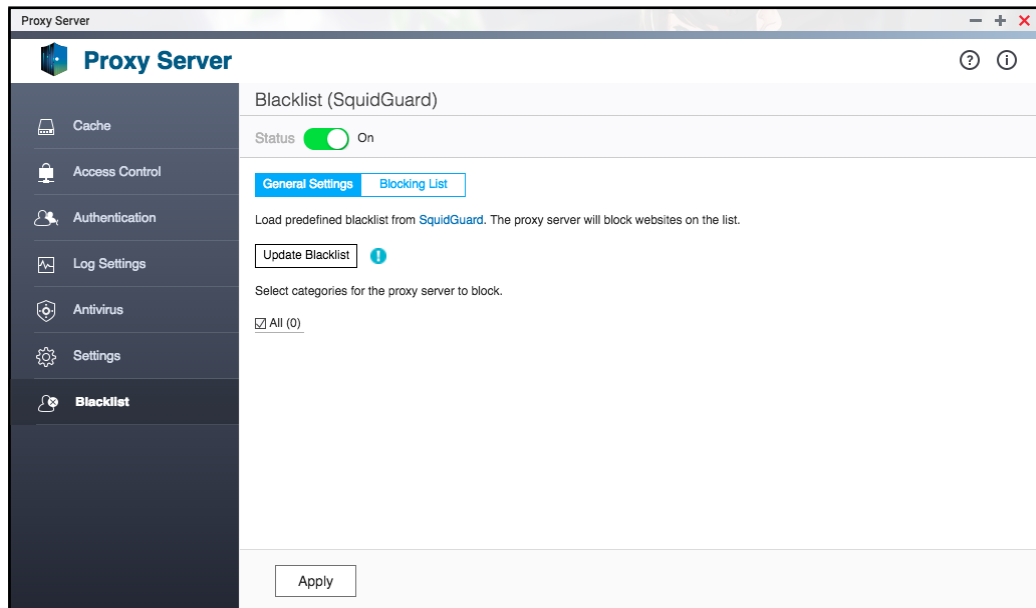
The image displays two screenshots from the QNAP web interface. The top screenshot shows the 'Proxy Server' configuration page. On the left is a sidebar menu with options: Cache, Access Control, Authentication, Log Settings, Antivirus (highlighted), Settings, and Blacklist. The main content area is titled 'Enable antivirus (SquidClamav)'. It features a 'Status' toggle switch set to 'On', which is highlighted with a red box. Below this, there is a section 'Set the whitelist:' with checkboxes for 'Account', 'File types', and 'Maximum file size for scanning'. At the bottom of this section is an 'Apply' button, also highlighted with a red box. The bottom screenshot shows the 'Control Panel' window. The left sidebar lists various services: System, Privilege, Network & File, Applications (highlighted), and others. Under 'Applications', 'Antivirus' is selected. The main area shows the 'Antivirus' configuration. It has tabs for 'Overview', 'Scan Jobs', 'Reports', and 'Quarantine'. The 'Overview' tab is active, showing 'Enable antivirus' as a checkbox (unchecked), 'Virus definitions' as '2018/04/09 16:23', 'Last virus scan' as '--', 'Last infected file found' as '--', and 'Status' as 'Update complete'. At the bottom, there is an 'Update' section with a checkbox for 'Check and update automatically' (unchecked) and a frequency dropdown set to 'Frequency in days'. An 'Update now' button is highlighted with a red box. Other buttons like 'Manual update (*.ovd)', 'Browse...', 'Import', and 'Apply' are also visible.

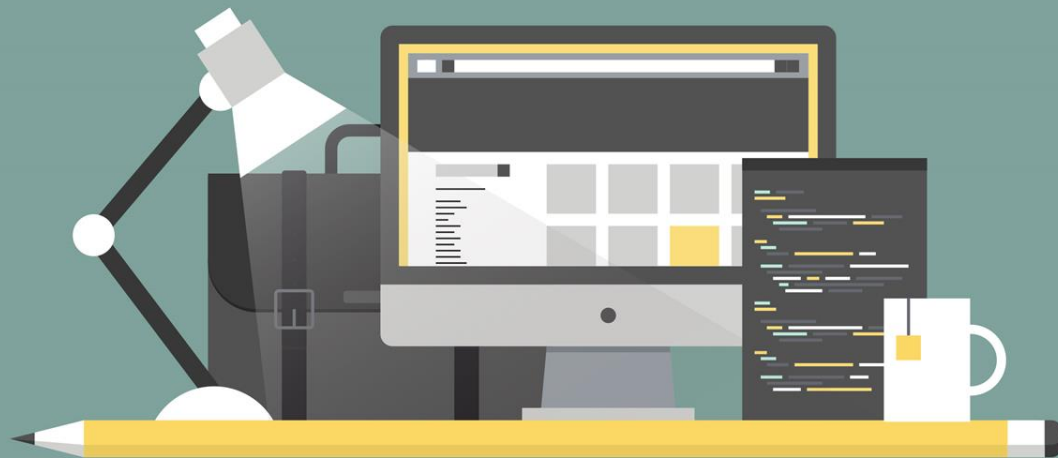
Proxy Server suggested configuration



2 Enable smart blacklist

Click [Update Blacklist] when enable Blacklist feature. Proxy Server will download and process latest blacklist information. It may take ten or more minutes to finish the process. You may choose catalogues you want to block from the list.



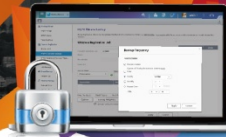


DEMO TIME



**Reduce vulnerability risk,
follow Security Advisory**

QNAP



- **CVE:** QNAP is a recognized CNA (CVE Numbering Authority) by the MITRE Corporation. QNAP has the power to assign a CVE ID for vulnerabilities within our software. All security issues are handled transparently.
- **Security Advisory:** The QNAP Security Response Team continuously investigates all security threats and releases updates as necessary to safeguard QNAP NAS users from the impact of malware and attacks.



Only 87 organizations in the world have obtained CNA status. There are only 3 in Taiwan.

Growth of CNA Program Worldwide

There are **87** organizations participating as CNAs as of **April 24, 2018**:

Vendors and Projects: **72**
Vulnerability Researchers: **7**
National and Industry CERTs: **3**
Bug Bounty Programs: **2**
Root CNAs: **2**
Primary CNA: **1**

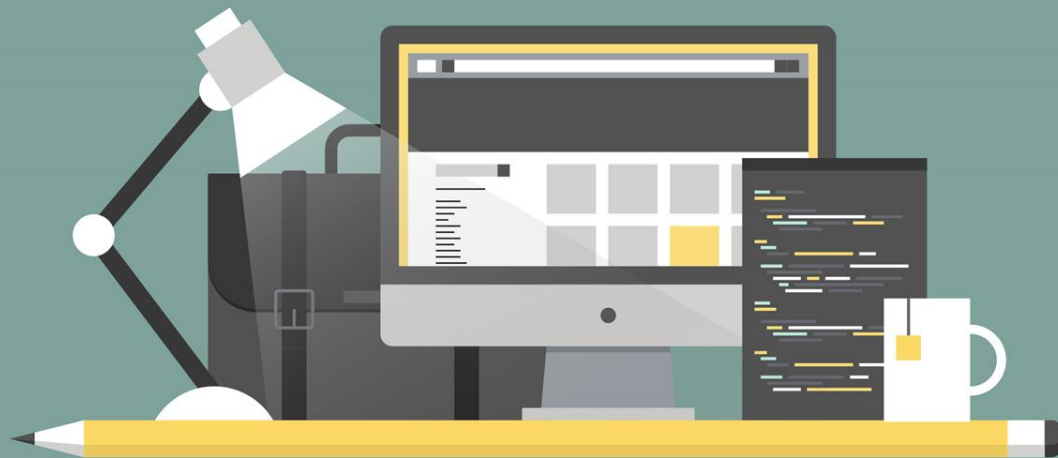
Number of CNAs by country as shown at right:

Australia: **1**
Austria: **1**
Canada: **3**
China: **8**
France: **1**
Germany: **2**
Israel: **1**
Japan: **3**
Netherlands: **2**
Russia: **2**
South Korea: **1**
Taiwan: 3
UK: **1**
USA: **58**



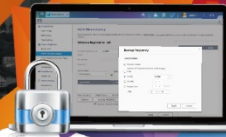
CNAs World Map as of April 2018

Source: <https://cve.mitre.org/cve/cna.html>



DEMO TIME

No sweat! QNAP keeps your NAS safe!



Vulnerability Scan

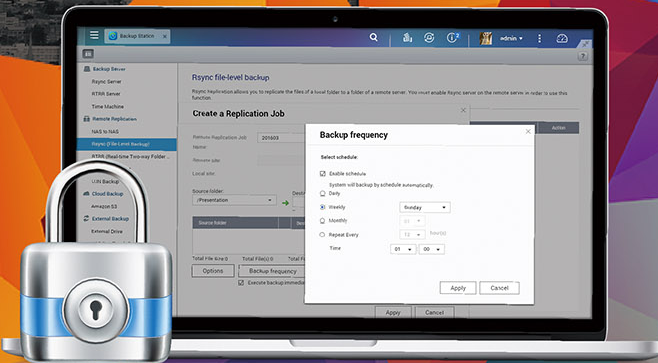
Use scan tools to discover any vulnerabilities on QNAP NAS.



Penetration Test

Work with security experts to perform penetration testing to find security holes and watch for any signs of cyber attacks.

Keep your NAS
secured and
your data safe



Security
Settings



Antivirus
and Malware
Remover



Snapshots,
backup and
encryption



Security
Applications



Security
Advisory