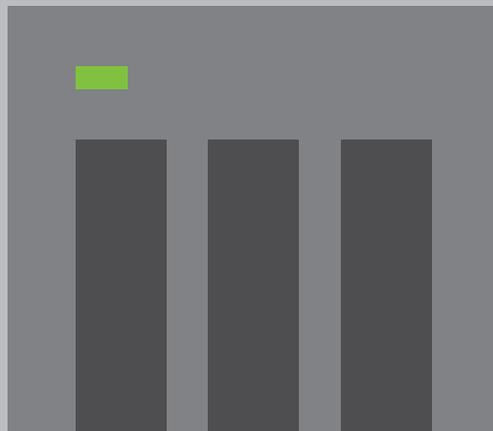


2 0 2 3

Sicherheitshandbuch



2 0 2 3

Sicherheitshandbuch

INDEX

- 1 Vorwort
- 2 Übliche Angriffe
- 3 Grundlegende Konzepte der Netzausrüstung
- 4 Verschiedene Möglichkeiten zur Verbindung von Internet und NAS

Vermeiden, das NAS dem Internet auszusetzen

- 8 Das NAS ordnungsgemäß verbinden
- 9 Router-Einstellungen überprüfen
- 12 NAS-Einstellungen überprüfen
- 15 Checkliste für netzwerkbezogene Einstellungen

NAS-Sicherheits-einstellungen

- 17 Systembenachrichtigungen einrichten
 - 46 QuFirewall
- 24 Automatisches Update der Firmware (QTS/QuTS hero) aktivieren
 - 51 Geplante Snapshots aktivieren
 - 53 Richtlinie für das Löschen von Snapshots festlegen
 - 54 Checkliste NAS-Sicherheitseinstellungen
- 25 App-Update-Einstellungen
- 27 Unnötige Funktionen deaktivieren oder entfernen
- 29 Telnet/SSH deaktivieren
- 30 Stärkung der Sicherheit von Systemkonten
- 34 Passwortrichtlinie festlegen
- 35 Zugriffsschutz aktivieren (IP/Konto)
- 36 Zwei-Schritt-Verifizierung (2SV) aktivieren
- 39 Standard-Ports ändern
- 40 Zugriffsprotokolle anzeigen
- 41 Sicherheits-Apps installieren und aktivieren
- 42 Security Counselor
- 45 Malware Remover

QNAP misst der Sicherheit große Bedeutung bei. Angesichts der zunehmenden Bedrohungen hat QNAP das Hardware- und Softwaredesign kontinuierlich verbessert, um den Anwendern Lösungen zu bieten, die sowohl sicher als auch bequem sind.

QNAPs Product Security Incident Response Team (PSIRT) ist für die Behandlung von Sicherheitsproblemen im Zusammenhang mit QNAP-Produkten zuständig. Neben der Bearbeitung von Vorfällen im Zusammenhang mit der Cybersicherheit kümmert sich PSIRT auch um die Meldung, Untersuchung, Behebung und Bekanntgabe von Schwachstellen in verschiedenen Produkten.

QNAP setzt sich auch für die Verbesserung der Produktsicherheit ein. In der Vergangenheit wurden Produkte so konzipiert, dass sie bequemer und für die Benutzer einfacher einzurichten und zu verwenden waren. Mit den zunehmenden Cyberangriffen auf vernetzte Geräte in den letzten Jahren hat sich auch die Produktdesign-Perspektive von QNAP geändert, und das Produktdesign hat sich auf "Security by Design" verlagert, um als Gatekeeper für die Benutzer zu dienen und sicherzustellen, dass die Benutzer mit den entsprechenden Bedrohungen umgehen können.

Das Tutorial hilft Benutzern bei der korrekten Einrichtung des NAS, um die Sicherheit zu verbessern. Wenn Sie Fragen haben, wenden Sie sich bitte an unser technisches Supportteam, das Ihnen gerne weiterhilft:



Informationen über Produktschwachstellen und sicherheitsrelevante Vorfälle finden Sie in den QNAP-Sicherheitshinweisen, die Sie abonnieren können:

<https://www.qnap.com/go/security-advisories/>



QNAP-Kundendienst:

<https://service.qnap.com/>



Um zu wissen, wie man sich vor Cyberangriffen schützen kann, muss man wissen, wie sie gestartet werden. Was Angriffe auf NAS betrifft, so werden die meisten Angriffe über das Internet gestartet. Die Angriffe erfolgen meist auf zwei Arten: "Passwort-Knacken" und "Schwachstellenangriff". In diesem Fall kann der "Schwachstellenangriff" in "N-Day" und "0-Day" unterteilt werden.

"N-Day" bezieht sich auf das Ausnutzen einer gepatchten Schwachstelle, um einen Angriff zu starten, und die meisten der derzeit aktiven Angriffe fallen in diese Kategorie. Sie können sich wirksam vor solchen Angriffen schützen, indem Sie immer die neuesten Sicherheitspatches und Updates installieren.

"0-Day" bedeutet, dass eine unbekannte Schwachstelle ausgenutzt wird, um einen Angriff zu starten, und die Hersteller können nur nachträglich Sicherheits-Patches herausgeben. Diese Angriffe können nur dann wirksam abgewehrt werden, wenn die Angreifer daran gehindert werden, sich mit dem Gerät zu verbinden.

In der folgenden Tabelle sind die Reaktionen auf verschiedene Angriffe für die Benutzer aufgeführt.

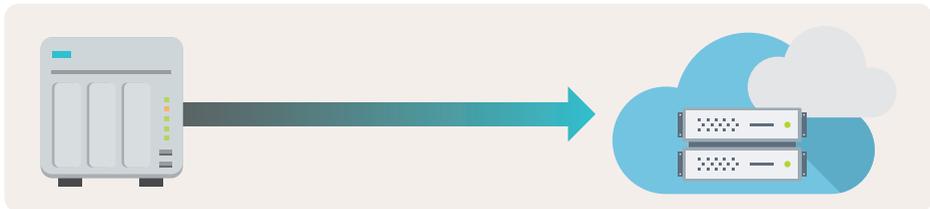
Antwort	Angriffe		
	Passwort-Knacken	Angriff auf Schwachstellen (N-Day)	Angriff auf Schwachstellen (0-Day)
Kontakt mit dem Internet vermeiden	V	V	V
Software aktualisieren (System und Apps)	X	V	o
Automatisches Update aktivieren (System und Apps)	X	V	o
Starke Passwörter für alle Konten verwenden	V	X	X
Standard-Konto "admin" deaktivieren	V	X	X
2-Schritt-Verifizierung	V	X	X
Zugriffsschutz aktivieren	o	X	X
Firewall aktivieren	o	o	o
Systembenachrichtigungen empfangen	o	o	o
Standard-Ports ändern	o	o	o
Unnötige Funktionen deaktivieren/entfernen	o	o	o

V: Wirksam X: Nicht wirksam Δ: Möglicherweise wirksam (bedeutet, dass der Angriff abgeschwächt werden kann oder das Risiko, angegriffen zu werden, verringert wird)

Mit der Option "Kontakt mit dem Internet vermeiden" können Sie Angreifer wirksam daran hindern, eine Verbindung zu Ihrem Gerät herzustellen und Angriffe darauf zu starten. Dieses Tutorial beginnt mit "Kontakt mit dem Internet vermeiden" und bietet dann ein vollständiges Tutorial zu den "NAS-Sicherheitseinstellungen", um die Verteidigungsfähigkeiten des NAS zu verbessern.

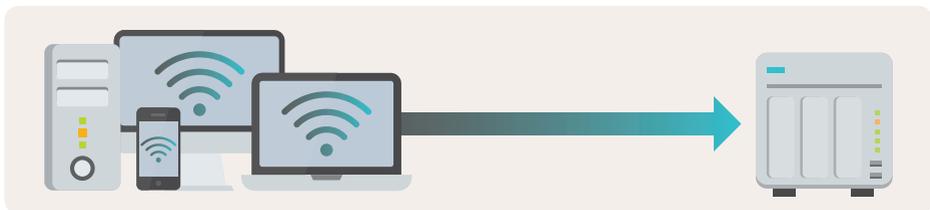
Als vernetztes Gerät haben NAS zwei Verbindungsrichtungen.

01 | Externe NAS-Verbindung



Ein NAS benötigt in der Regel eine externe Verbindung, um ordnungsgemäß zu funktionieren. Zum Beispiel grundlegende Systemfunktionen wie automatische Updates und das Senden von Benachrichtigungen. Wenn Sie außerdem NAS-Daten in einer öffentlichen Cloud sichern oder das NAS zur Sicherung von Daten von anderen Geräten oder öffentlichen Clouds (z. B. virtuelle Maschinen, Google Workspace oder Microsoft 365), Computern oder Servern verwenden möchten, muss das NAS in der Lage sein, ausgehende Verbindungen zu initiieren.

02 | Andere Geräte (wie Computer, Mobiltelefone oder andere Server), die eine Verbindung zum NAS herstellen



Wenn Sie die vom NAS bereitgestellten Funktionen oder Dienste verwenden möchten, einschließlich des Zugriffs auf Dateien und der Eingabe der Einstellungsschnittstelle, müssen Sie in der Lage sein, eine Verbindung mit dem NAS herzustellen.

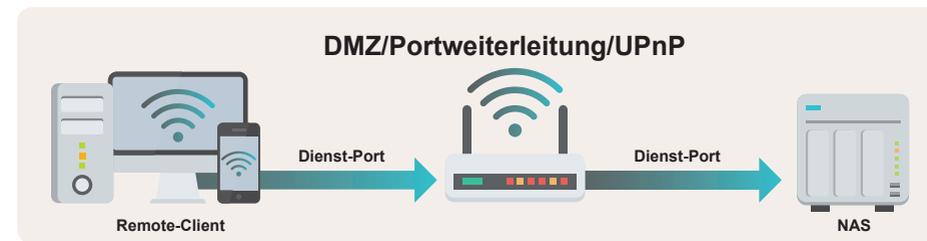
Wenn Ihr Router nicht über eine DMZ, Portweiterleitung oder UPnP verfügt, blockiert der Router den Datenverkehr aus dem Internet. Nur Geräte im lokalen Netzwerk können auf den NAS zugreifen.

Wenn der Router aktiviert ist und die oben genannten Funktionen eingestellt sind, kann jeder im Internet eine Verbindung zum offenen Port herstellen und dann gemäß den Regeln auf dem Router an das NAS weiterleiten, sich dann anmelden und die entsprechenden Funktionen normal nutzen. Dies bietet aber auch Hackern die Möglichkeit, Passwörter zu knacken oder Software-Schwachstellen auszunutzen, was ein Sicherheitsrisiko darstellt.

01 | DMZ, Portweiterleitung oder UPnP auf dem Router aktivieren und konfigurieren

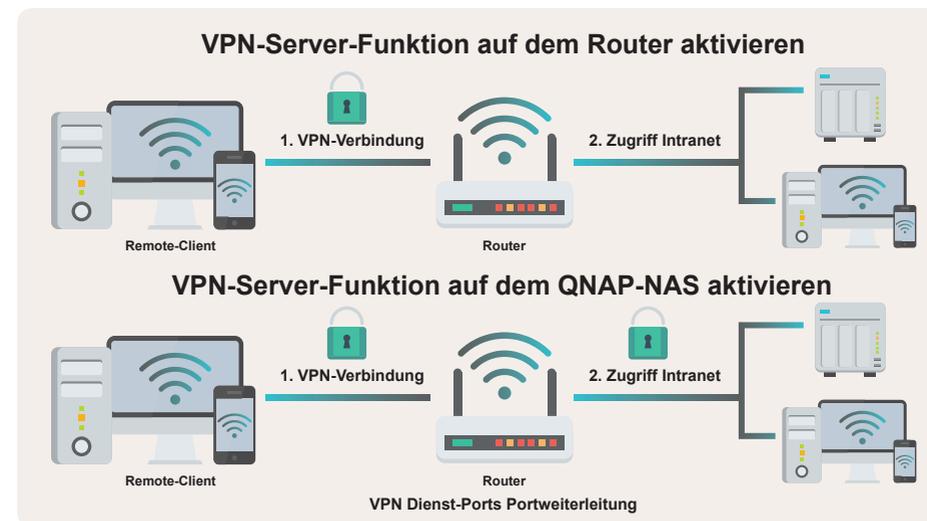
Diese Methode birgt Sicherheitsrisiken. Wenn Sie kein Experte für Netzwerkkonfigurationen sind und die damit verbundenen Risiken nicht verstehen, **empfiehlt QNAP die Verwendung dieser Funktion nicht***. Da der Router Datenverkehr an Intranet-Geräte weiterleitet, können Hacker leicht Netzwerkangriffe starten, wenn zwischen Router und NAS keine Firewall installiert ist, die böswärtigen Datenverkehr blockiert. Doch selbst wenn eine Firewall installiert ist (durch Verwendung einer einfachen Firewall oder den Kauf einer Firewall für Unternehmen), ist nicht gewährleistet, dass sie jeden Angriff abwehrt.

* QNAP empfiehlt, nur relativ risikoarme VPN-Dienst-Ports für das Internet zu öffnen, während andere risikoreiche Dienst-Ports wie Systemverwaltungs-, SMB- und SSH-Dienste nicht einfach vom Internet aus zugänglich sein sollten.



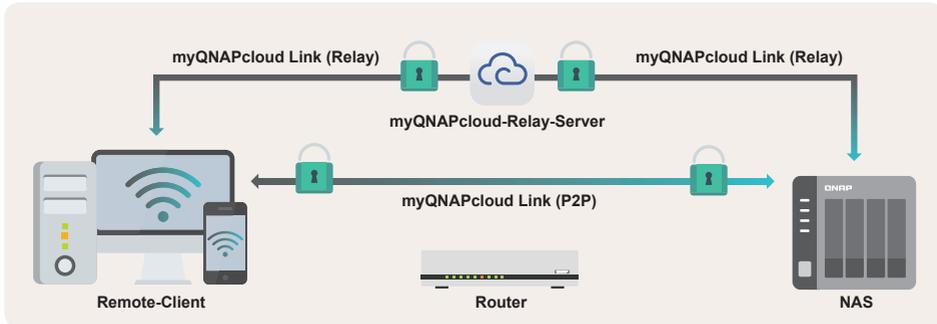
02 | VPN-Server-Funktion auf dem Router oder QNAP-NAS aktivieren

Einige Router unterstützen VPN-Serverfunktionen (z. B. Router der QNAP QHora- und QMiro-Serie), während das QNAP-NAS auch mehrere VPN-Server unterstützt. Nach der Aktivierung und ordnungsgemäßen Konfiguration können Sie auf jedes Gerät im Intranet mit einer VPN-verschlüsselten Verbindung vom Internet zum VPN-Server zugreifen, was ein hohes Maß an Sicherheit bietet.



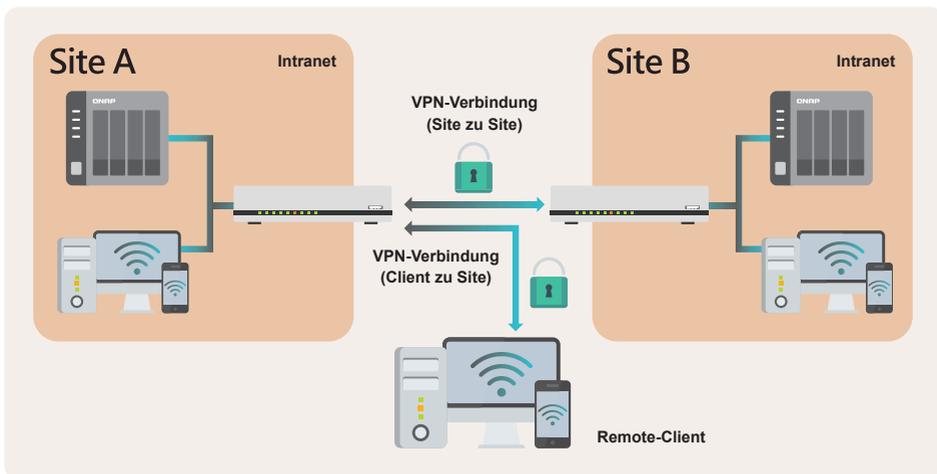
03 | Sichere myQNAPcloud Link-Verbindung verwenden

Die Einrichtung eines Routers ist nicht erforderlich, wenn Sie myQNAPcloud Link zur Verbindung mit dem NAS verwenden, da der NAS-Dienst direkt mit dem Internet verbunden werden kann. myQNAPcloud Link stellt je nach Netzwerkumgebung eine Verbindung über einen Relay-Server oder Peer-to-Peer-Technologie (P2P) her. Die gesamte Verbindung wird verschlüsselt, um die Sicherheit zu gewährleisten.



04 | SD-WAN- oder Site-to-Site-VPN-Produkte verwenden

Im Gegensatz zur oben erwähnten VPN-Server-Funktion (Client-to-Site-VPN) wird bei SD-WAN- oder Site-to-Site-VPN eine sichere verschlüsselte VPN-Verbindung zwischen zwei oder mehreren Routern an verschiedenen Standorten aufgebaut. Geräte können, einfach ausgedrückt, in einem Site-to-Site-VPN-Netzwerk so miteinander verbunden werden, als befänden sie sich im selben Intranet, was ideal für Benutzer mit mehreren Standorten ist. Mit Client-to-Site-VPN können Sie von überall aus auf Ihr NAS zugreifen.



Anhand der Vergleichstabelle können Sie die für Sie geeignete Verbindungsmethode auswählen. QNAP bietet mehrere sichere Verbindungslösungen an, um die Anforderungen der Benutzer zu erfüllen.

Verbindungsmethode	Vorteile	Nachteile	Geeignete Benutzer
Aktivieren und Konfigurieren der Router-DMZ/Portweiterleitung von UPnP	<ul style="list-style-type: none"> Schnellste Verbindung 	<ul style="list-style-type: none"> Anfällig für Cyberangriffe Kein Schutz gegen 0-Day-Angriffe auf Sicherheitslücken 	<ul style="list-style-type: none"> Haben ein klares Verständnis für damit verbundene Risiken Sind vertraut mit den Netzwerkeinstellungen Haben mehrere Sicherungen für wichtige Daten erstellt Haben einen Plan für die Notfallwiederherstellung
VPN-Server auf dem Router aktivieren*	<ul style="list-style-type: none"> Relativ einfach einzurichten 	<ul style="list-style-type: none"> Keine Benachrichtigung bei Anmeldefehlern, automatische Sperrung und Firewall-Funktion Weniger unterstützte VPN-Protokolle Durch Router-Hardware begrenzte Leistung 	<ul style="list-style-type: none"> Sind nicht vertraut mit den Netzwerkeinstellungen Interessiert die Übertragungsgeschwindigkeit nicht
VPN-Server-Funktion auf dem QNAP-NAS aktivieren*	<ul style="list-style-type: none"> Unterstützt mehrere VPN-Protokolle Kompatibel mit NAS-Firewall (QuFirewall) Unterstützt Benachrichtigung bei Anmeldefehlern und automatische Sperrung 	<ul style="list-style-type: none"> Die Einstellungen sind etwas komplizierter 	<ul style="list-style-type: none"> Sind vertraut mit den Netzwerkeinstellungen Müssen häufig auf viele Dateien im Internet zugreifen
 Sichere myQNAPcloud Link-Verbindung verwenden	<ul style="list-style-type: none"> Am einfachsten einzurichten Unterstützt Zugriffssteuerung NAS muss nicht mit dem Internet verbunden sein 	<ul style="list-style-type: none"> Langsamere Verbindung 	<ul style="list-style-type: none"> Sind nicht vertraut mit den Netzwerkeinstellungen Seltener Zugriff auf das NAS über das Internet Netzwerkumgebung, in der keine WAN-IP-Adresse bezogen werden kann
SD-WAN- oder Site-to-Site-VPN-Produkte verwenden*	<ul style="list-style-type: none"> Einmal eingerichtet, können die Intranet-Benutzer es verwenden, ohne einen Unterschied zu spüren Unterstützt auch Client-to-Site-VPN 	<ul style="list-style-type: none"> Zusätzliche Geräte erforderlich 	<ul style="list-style-type: none"> Erfordert Multi-Point-Zugriff und Remote-Sicherung Erfordert Mehrwertanwendungen

* Das QNAP-NAS unterstützt:
myQNAPcloud Link / VPN-Server (L2TP/IPsec, OpenVPN, WireGuard, QBelt) /QuWAN SD-WAN

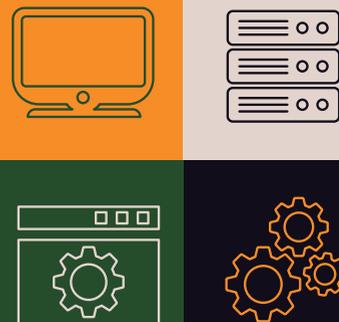
* Der QNAP-Router unterstützt:
QuWAN SD-WAN / VPN-Server (L2TP/IPsec, OpenVPN, WireGuard, QBelt)

Bezieht sich auf allgemeine Heimrouter

01

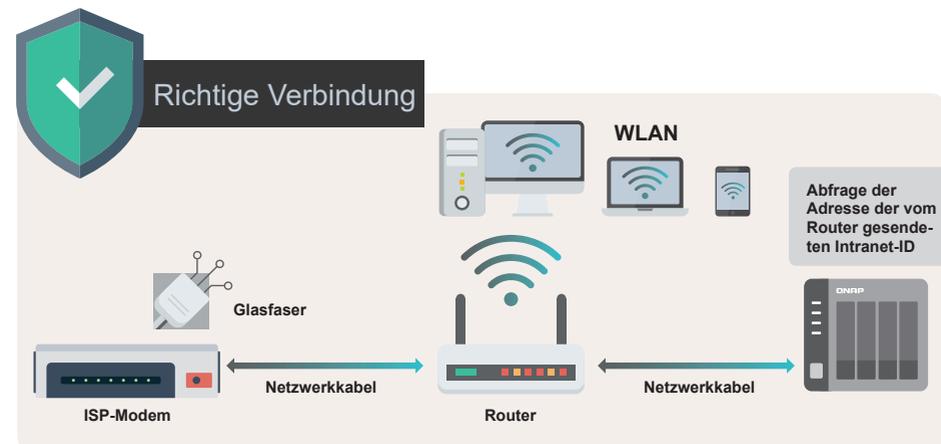
Anleitung für NAS-Sicherheitseinstellungen

Vermeiden, das NAS dem Internet auszusetzen

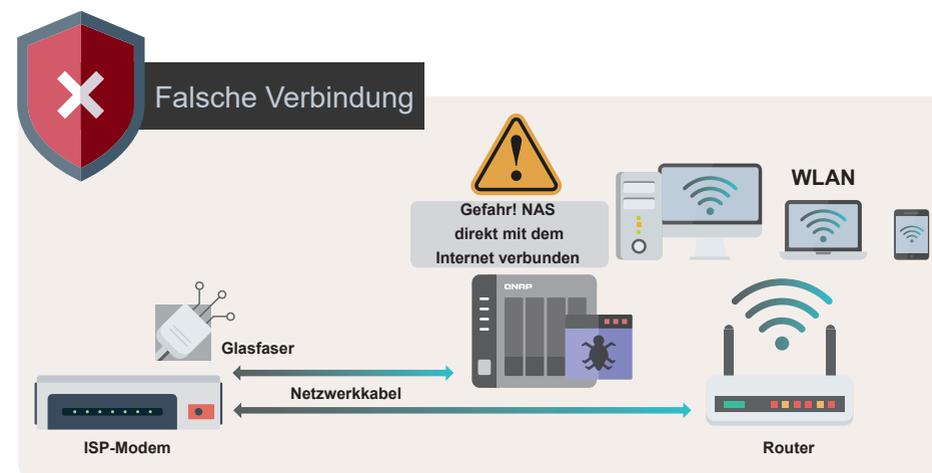


Das NAS ordnungsgemäß verbinden

Stellen Sie sicher, dass Ihr NAS mit dem Router verbunden ist. Bei richtiger Einrichtung kann der Router Verbindungen aus dem Internet für Sie blockieren, sodass Ihr NAS vor dem Internet verborgen bleibt und Cyberangriffe vermieden werden.



Wenn Sie das NAS an das vom ISP bereitgestellte Modem anschließen, erhält Ihr NAS die WAN-IP-Adresse direkt. In diesem Fall kann jeder (auch Hacker) über das Internet eine Verbindung zu Ihrem NAS herstellen und sogar versuchen, es anzugreifen und in es einzudringen.

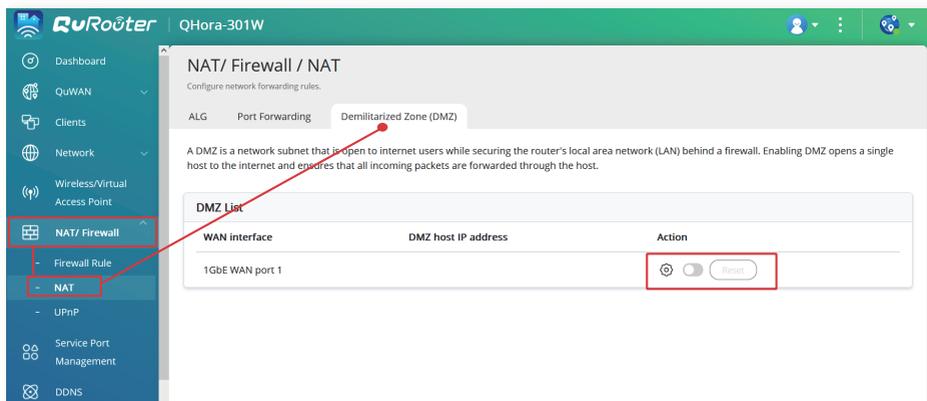
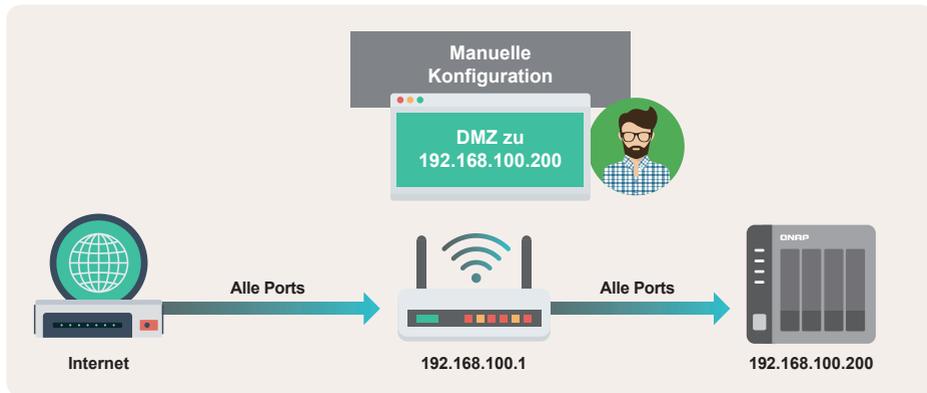


Router-Einstellungen überprüfen

Standardmäßig kann theoretisch niemand eine direkte Verbindung vom Internet zu Ihrem Gerät hinter dem Router herstellen. Wenn Sie jedoch "DMZ (Demilitarized Zone)", "Portweiterleitung" oder "UPnP (Universal Plug and Play)" aktivieren, leitet Ihr Router die Pakete gemäß den von Ihnen festgelegten Regeln an das von Ihnen ausgewählte Gerät weiter und macht Ihr Gerät damit dem Internet zugänglich. Falls nicht benötigt, sollten Sie überprüfen und sicherstellen, dass die folgenden Funktionen **deaktiviert** sind.

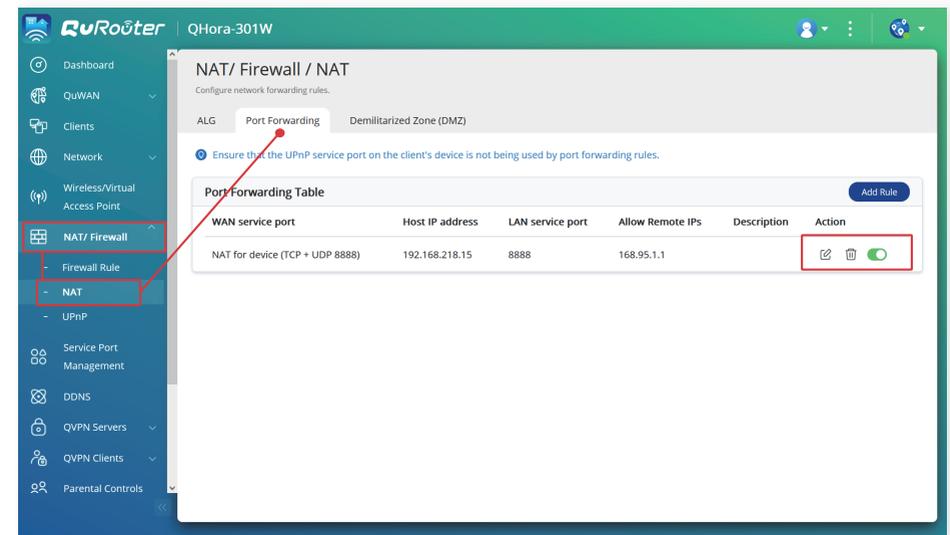
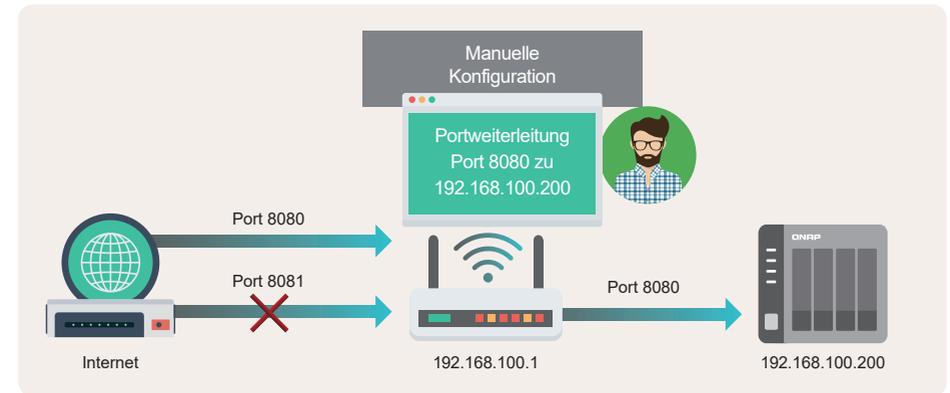
01 | DMZ (Demilitarisierte Zone) überprüfen

Nachdem Sie diese Funktion aktiviert haben, sind alle Dienst-Ports des von Ihnen ausgewählten Geräts direkt für das Internet geöffnet, d. h. sie sind dem Internet vollständig ausgesetzt. Um Sicherheitsrisiken zu verringern, sollten Sie diese Funktion deaktivieren.



02 | Portweiterleitung überprüfen

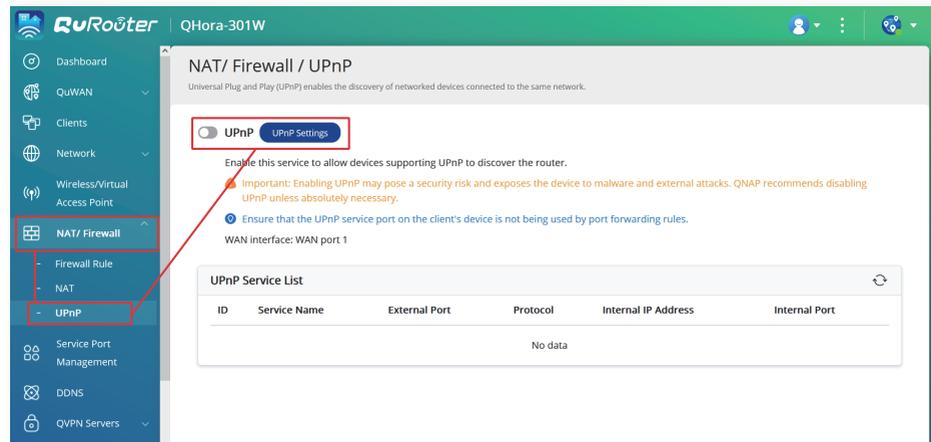
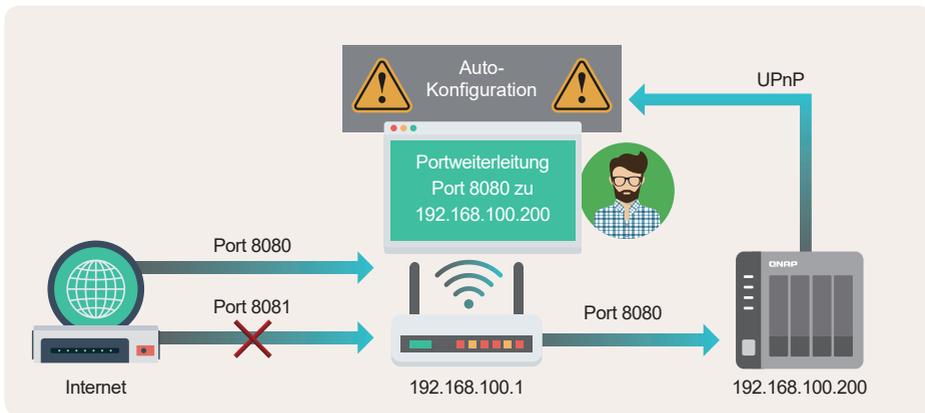
Mit dieser Funktion können Sie einen bestimmten Dienst-Port auf einem Gerät für das Internet öffnen, sodass jeder über das Internet auf die entsprechenden Dienste zugreifen kann. Hacker können aber auch vom Internet aus Angriffe auf offene Dienste starten. Es wird daher empfohlen, zunächst alle Regeln für die Portweiterleitung zu deaktivieren, dann die NAS-Sicherheitseinstellungen einzurichten und anschließend wichtige Daten zu sichern, bevor Sie diese Funktion nutzen, um einige wichtige Dienste für das Internet zu öffnen.



NAS-Einstellungen überprüfen

03 | UPnP (Universal Plug and Play) überprüfen

Diese Funktion ist gleichbedeutend mit einer automatischen Portweiterleitung. Nachdem Sie diese Funktion aktiviert haben, kann Ihr Gerät automatisch eine Portweiterleitung unter Verwendung des entsprechenden Protokolls konfigurieren. Diese Funktion birgt ernsthafte Sicherheitsrisiken, da sie Ihre Dienste ohne Ihr Wissen dem Internet preisgeben oder von Hackern ausgenutzt werden kann, um Hintertüren zu öffnen.



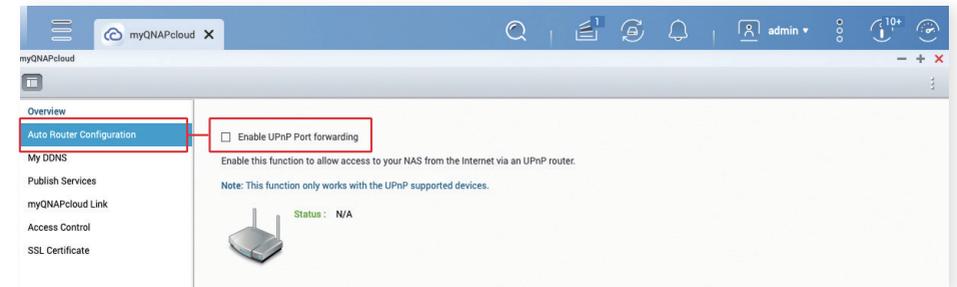
01 | Automatische Router-Konfiguration, UPnP-Portweiterleitung

Da einige Router die Deaktivierung der UPnP-Funktion nicht unterstützen, überprüfen Sie bitte gleichzeitig die Einstellung "Automatische Router-Konfiguration" auf dem NAS, um sicherzustellen, dass diese Funktion deaktiviert ist.

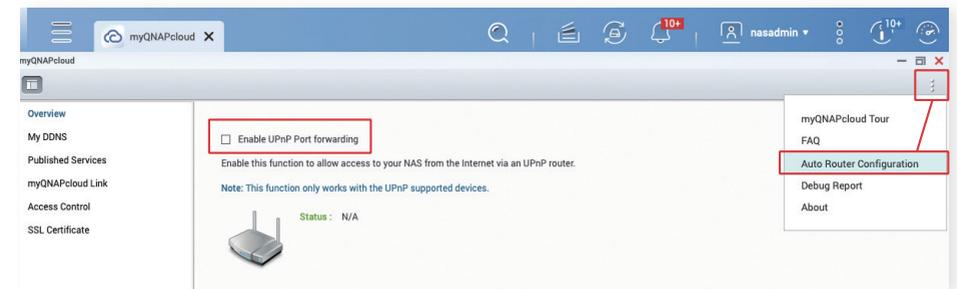
*** Diese Funktion ist ab QTS 4.5.0/QuTS hero h4.5.3 standardmäßig deaktiviert.**

So deaktivieren Sie die Funktion "Automatische Router-Konfiguration":

1. Melden Sie sich mit einem Administratorkonto bei der Webverwaltungsschnittstelle von QTS/QuTS hero an.
2. Öffnen Sie das Menü in der oberen linken Ecke der Verwaltungsschnittstelle und klicken Sie auf "myQNAPcloud"
3. **QTS 5.0.0 / QuTS hero h5.0.0 oder früher:** Klicken Sie im linken Menü auf "Automatische Router-Konfiguration"



QTS 5.0.1 / QuTS hero h5.0.1 oder höher: Klicken Sie auf das Menüsymbol in der oberen rechten Ecke und wählen Sie "Automatische Router-Konfiguration"



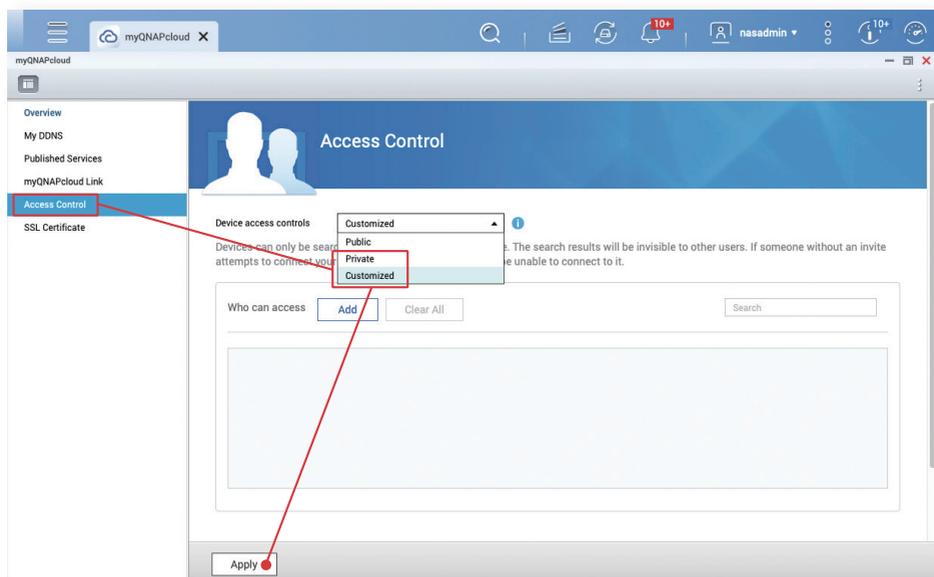
4. Deaktivieren Sie auf der Einstellungsseite "Automatische Router-Konfiguration" die Option "UPnP-Portweiterleitung aktivieren" und klicken Sie auf "Übernehmen".

02 | myQNAPcloud Link-Zugriffssteuerung

myQNAPcloud Link ist ein sicherer Cloud-Dienst, der von QNAP bereitgestellt wird. Benutzer können sich über den von ihnen gewählten myQNAPcloud-Gerätenamen mit ihrem QNAP-NAS verbinden. myQNAPcloud Link bietet Zugriffskontrolleinstellungen. Wenn die Zugriffskontrolle auf "Öffentlich" eingestellt ist, kann jeder, der Ihren Gerätenamen kennt, myQNAPcloud Link verwenden, um sich mit Ihrem NAS zu verbinden. Wir empfehlen daher, **die Zugriffskontrolle auf "Privat" oder "Benutzerdefiniert" einzustellen**. In beiden Modi müssen sich Benutzer mit ihrer QNAP ID in der Liste der zulässigen Zugriffe anmelden, bevor sie myQNAPcloud Link für eine sichere Verbindung zu Cloud-Diensten nutzen können.

* Die Standardeinstellung Q TS 4.5.0 / Qu TS hero h4.5.3 (oder höher) ist "Benutzerdefiniert"

1. Melden Sie sich mit einem Administratorkonto bei der Webverwaltungsschnittstelle von QTS/QuTS hero an
2. Klicken Sie auf das Menü in der oberen linken Ecke der Verwaltungsschnittstelle und dann auf "myQNAPcloud"
3. Klicken Sie im Menü auf der linken Seite auf "Zugriffssteuerung"
4. Stellen Sie auf der Einstellungsseite "Zugriffskontrolle" die Option "Gerätezugriffskontrolle" auf "Privat" oder "Benutzerdefiniert" und klicken Sie dann auf "Übernehmen".



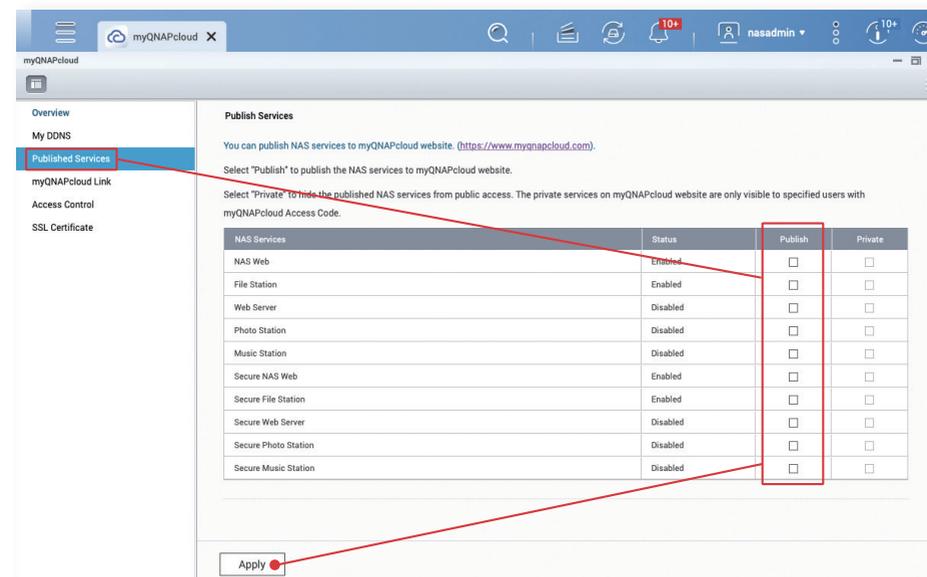
03 | Veröffentlichte Dienste

Veröffentlichte Dienste können es den Benutzern erleichtern, verwandte Funktionen auf der myQNAPcloud-Website zu nutzen, aber sie erhöhen auch die Sicherheitsrisiken. Wenn Sie diese Funktion nicht benötigen, empfiehlt es sich, sie zu deaktivieren, um die Sicherheit zu erhöhen.

* Diese Funktion ist ab QTS 4.5.0/QuTS hero h4.5.3 standardmäßig deaktiviert

Funktion "Veröffentlichte Dienste":

1. Melden Sie sich mit einem Administratorkonto bei der Webverwaltungsschnittstelle von QTS/QuTS hero an
2. Klicken Sie auf das Menü in der oberen linken Ecke der Verwaltungsschnittstelle und dann auf "myQNAPcloud"
3. Klicken Sie im Menü auf der linken Seite auf "Veröffentlichte Dienste"
4. Entfernen Sie im Feld "Veröffentlichen" alle Häkchen und klicken Sie auf "Übernehmen".



Checkliste Netzwerkeinstellungen

Hardware-bezogen

- NAS befindet sich hinter einem Router
- NAS bezieht eine Intranet-IP-Adresse

Router

- "DMZ"-Funktion des Routers deaktivieren
- Regel "Portweiterleitung" des Routers deaktivieren
- "UPnP"-Funktion des Routers deaktivieren

NAS

- NAS-Funktion "Automatische Router-Konfiguration, UPnP-Portweiterleitung" deaktivieren
- NAS-Funktion "myQNAPcloud Link-Zugriffssteuerung" auf "Privat" oder "Benutzerdefiniert" setzen
- Funktion "Veröffentlichte Dienste" deaktivieren

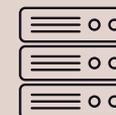
Nach dem Überprüfen und Anwenden der oben genannten Einstellungen ist Ihr QNAP-NAS nicht mehr dem Internet ausgesetzt, und das Risiko eines Hackerangriffs ist stark reduziert. Lesen Sie weiter und überprüfen Sie die restlichen Einstellungen zur Stärkung des QNAP-NAS.

Wenn Sie über das Internet auf NAS zugreifen müssen, können Sie diese drei sicheren Alternativen in Betracht ziehen:

		
myQNAPcloud Link	QVPN Service	QuWAN SD-WAN
		
Mehr erfahren	Mehr erfahren	Mehr erfahren

02

Anleitung für NAS-Sicherheitseinstellungen



NAS-Sicherheitseinstellungen



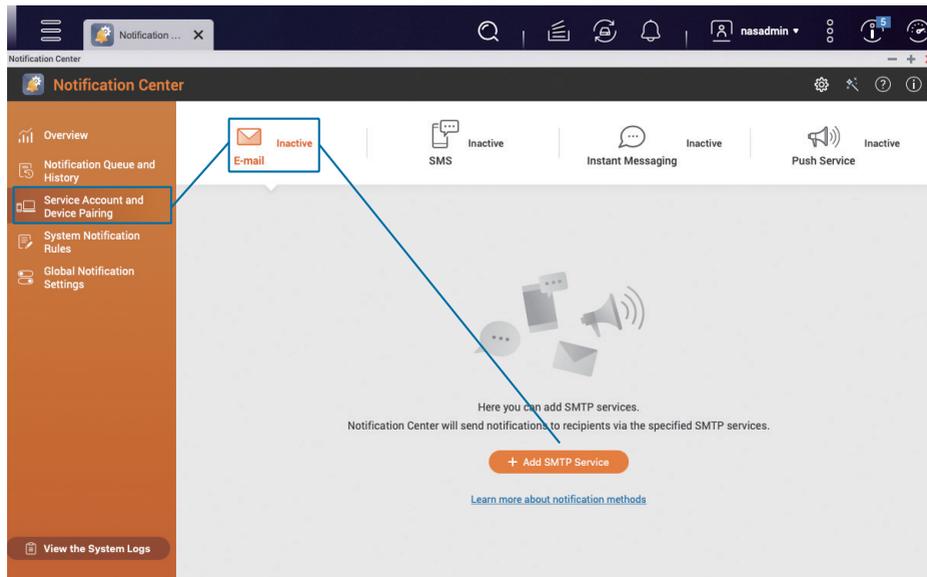
Systembenachrichtigungen einrichten

Das integrierte Notification Center kann auf der Grundlage Ihrer Einstellungen Benachrichtigungen versenden, sodass Benutzer den NAS-Status im Auge behalten und auf Anomalien reagieren können, sobald diese erkannt werden.

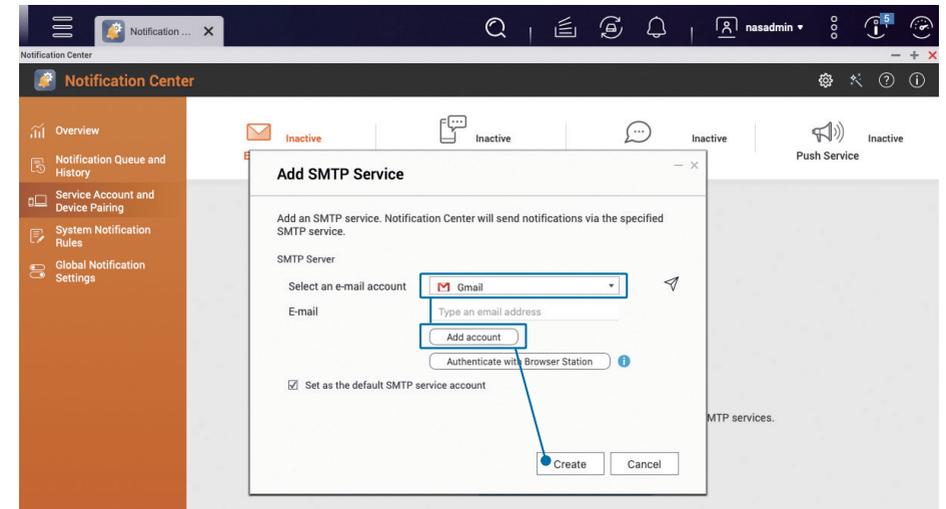
Im folgenden Tutorial lernen Sie, wie Sie zwei Grundregeln für "E-Mail" zum Versenden von "Alarmbenachrichtigungen" und "Firmware-Updates" erstellen und bei Bedarf weitere Regeln hinzufügen können.

01 | Benachrichtigungsmethode "E-Mail" hinzufügen

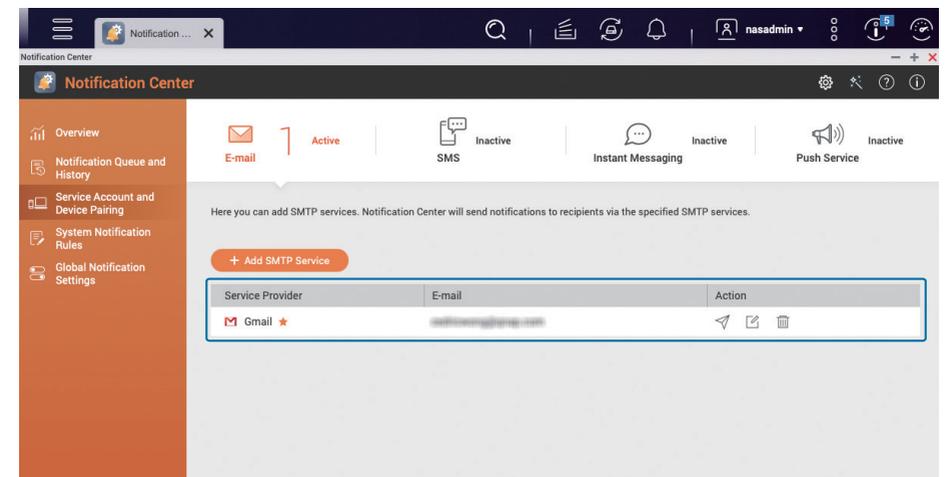
Öffnen Sie das "Notification Center", klicken Sie im linken Menü auf "Dienstkonto und Gerätekopplung", wählen Sie "E-Mail" und klicken Sie dann auf "SMTP-Dienst hinzufügen"



Wählen Sie ein E-Mail-Konto aus (im Folgenden wird Gmail als Beispiel verwendet), klicken Sie auf "Konto hinzufügen", folgen Sie den Anweisungen, um den Gmail-Verifizierungsprozess abzuschließen, und klicken Sie auf "Erstellen", nachdem die Überprüfung abgeschlossen ist.

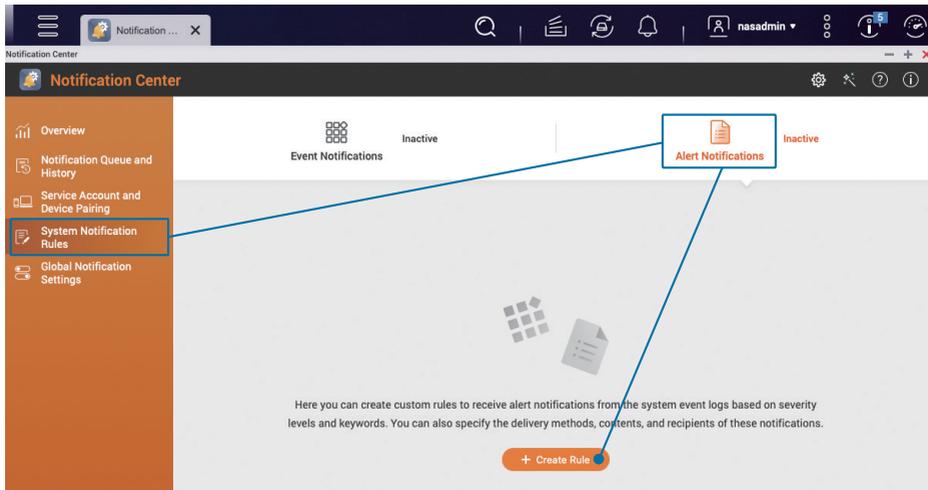


⇓ Einmal erstellt, sehen Sie das E-Mail-Konto, das Sie in der Liste hinzugefügt haben.

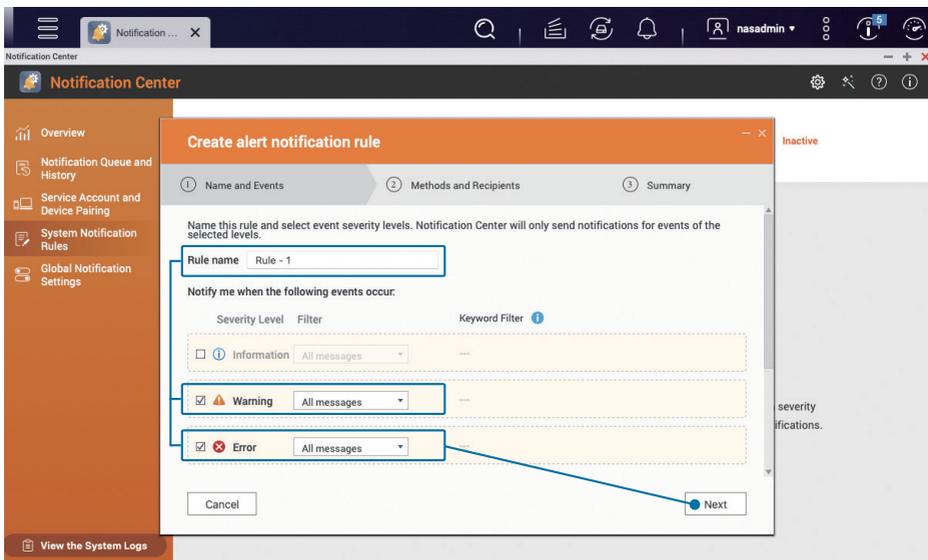


02 | "Alarbenachrichtigungen" einrichten

Klicken Sie im Menü auf der linken Seite "Notification Center" auf "Regeln für Systembenachrichtigungen", wählen Sie "Alarbenachrichtigungen" und klicken Sie auf "Regel erstellen".

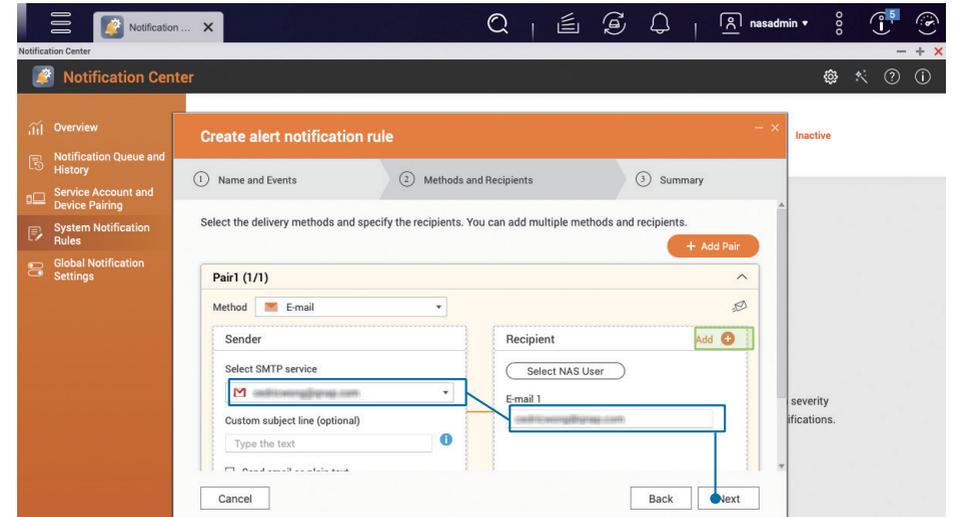


Ändern Sie "Regelname" nach Ihren Anforderungen, wählen Sie die beiden Schweregrade "Warnung" und "Fehler" und klicken Sie auf "Weiter".

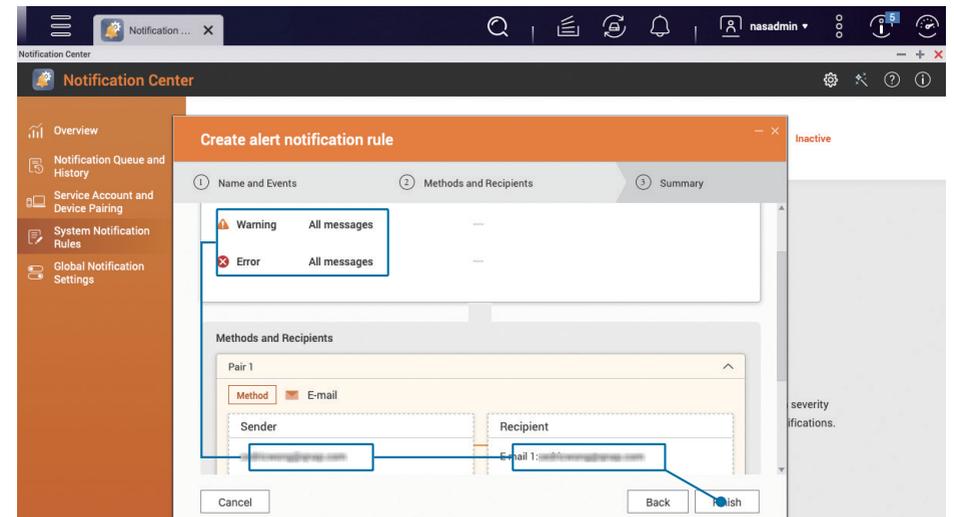


Legen Sie die Zustellungsmethode und den Empfänger fest, wählen Sie das soeben hinzugefügte E-Mail-Konto als "Absender" in der Paarung aus, geben Sie die "E-Mail-Adresse" des "Empfängers" ein und klicken Sie auf "Weiter".

Bei Bedarf können Sie mehrere Empfänger eingeben, indem Sie neben "Empfänger" auf "Hinzufügen" klicken. Sie können auch "Paare hinzufügen" wählen, um Benachrichtigungen auf mehrere Arten gleichzeitig zu versenden.

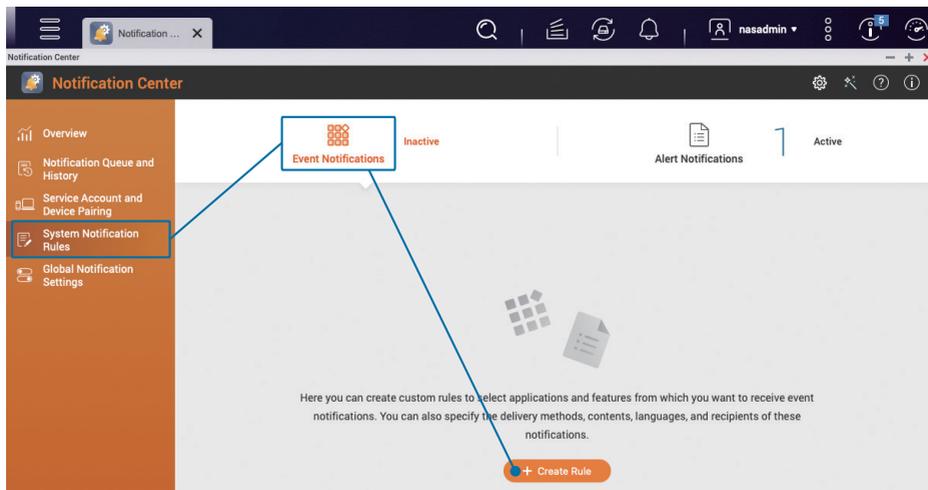


Nachdem Sie bestätigt haben, dass die Einstellungen korrekt sind, klicken Sie auf "Fertigstellen", und die Einstellungen für die "Alarbenachrichtigungen" sind abgeschlossen.

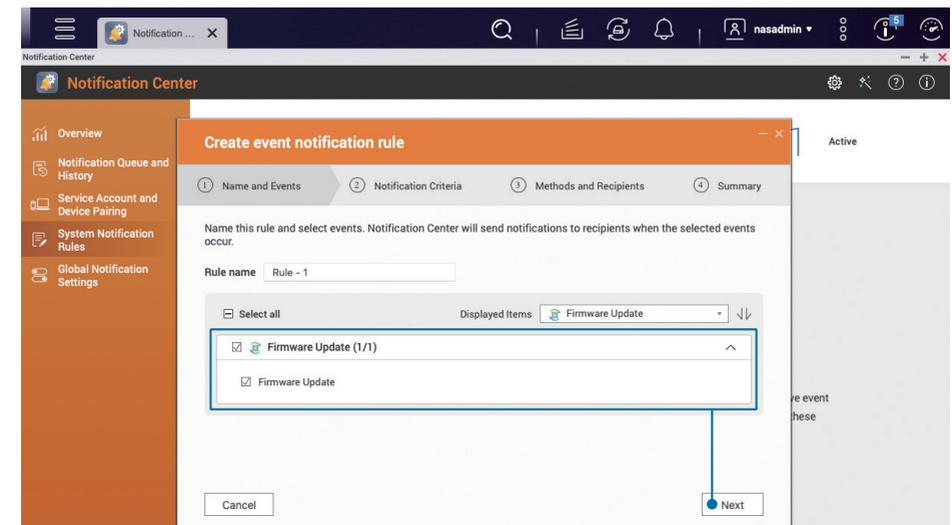


03 | "Firmware-Update"-Benachrichtigungen konfigurieren

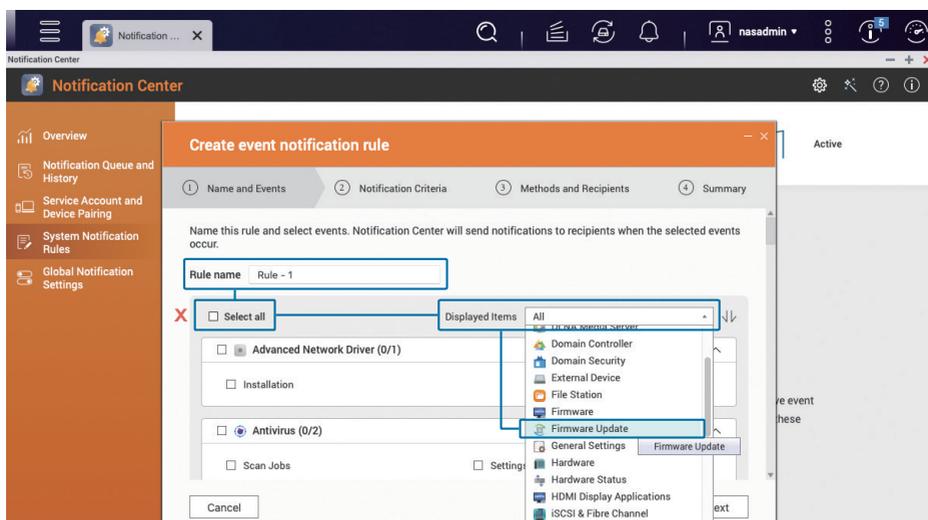
Klicken Sie auf "Regeln für Systembenachrichtigungen" im linken Menü des "Notification Center", wählen Sie "Ereignisbenachrichtigungen" und klicken Sie dann auf "Regel erstellen".



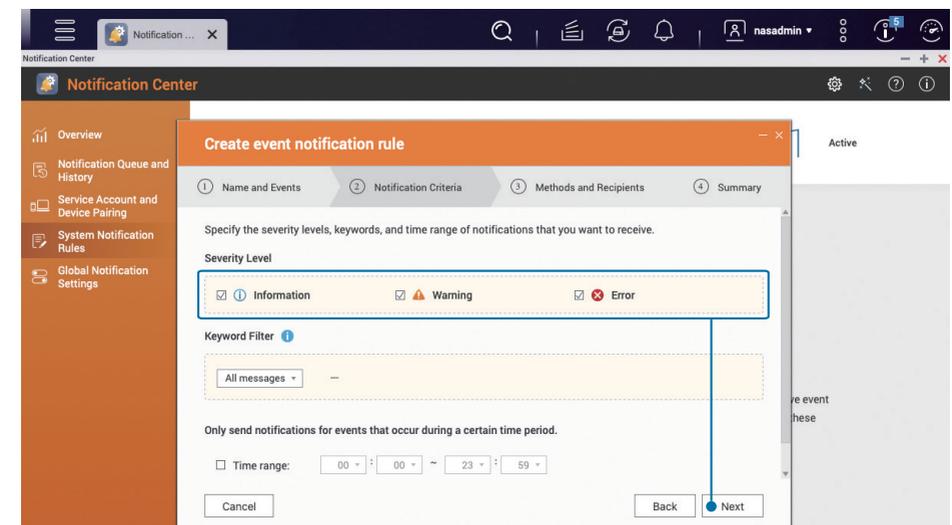
Aktivieren Sie die Option "Firmware-Update" und klicken Sie auf "Weiter".



Ändern Sie "Regelname" entsprechend Ihren Anforderungen, deaktivieren Sie "Alle auswählen", wählen Sie dann "Firmware-Update" in der Liste "Angezeigte Elemente" auf der linken Seite und wählen Sie die Option "Firmware-Update" darunter.



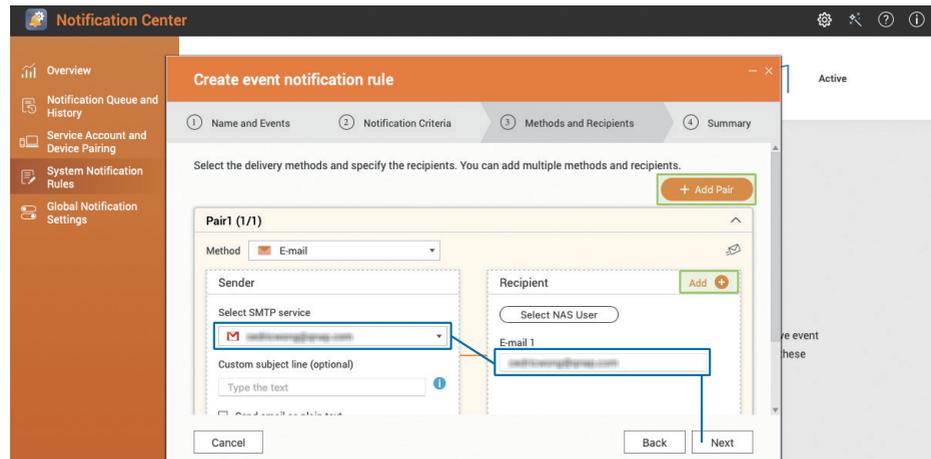
Aktivieren Sie alle Schweregrade, einschließlich "Information", "Warnung" und "Fehler" und klicken Sie auf "Weiter".



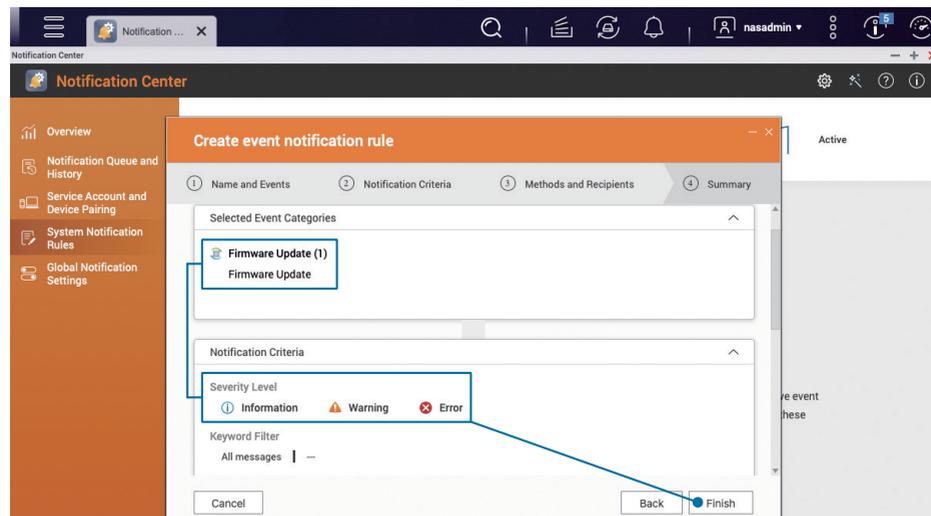
Automatisches Update der Firmware (QTS/QuTS hero) aktivieren

Legen Sie die Zustellmethode und den Empfänger fest. Da derzeit nur die "E-Mail"-Benachrichtigung festgelegt ist, wählen Sie das soeben hinzugefügte E-Mail-Konto als "Absender" in der Paarung aus, geben Sie dann die "E-Mail-Adresse" des "Empfängers" ein und klicken Sie auf "Weiter".

Bei Bedarf können Sie mehrere Empfänger eingeben, indem Sie neben "Empfänger" auf "Hinzufügen" klicken. Sie können auch "Paare hinzufügen" wählen, um Benachrichtigungen auf mehrere Arten gleichzeitig zu versenden.

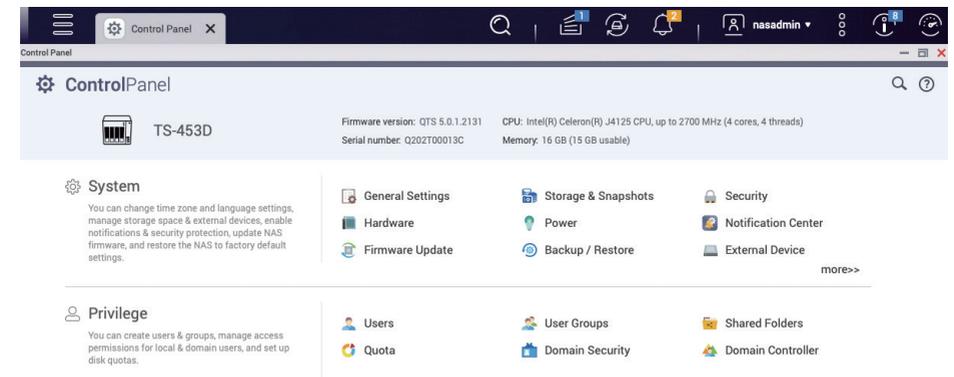


Nachdem Sie bestätigt haben, dass die Einstellungen korrekt sind, klicken Sie auf "Fertigstellen", um die Einstellung von "Firmware-Update" abzuschließen.



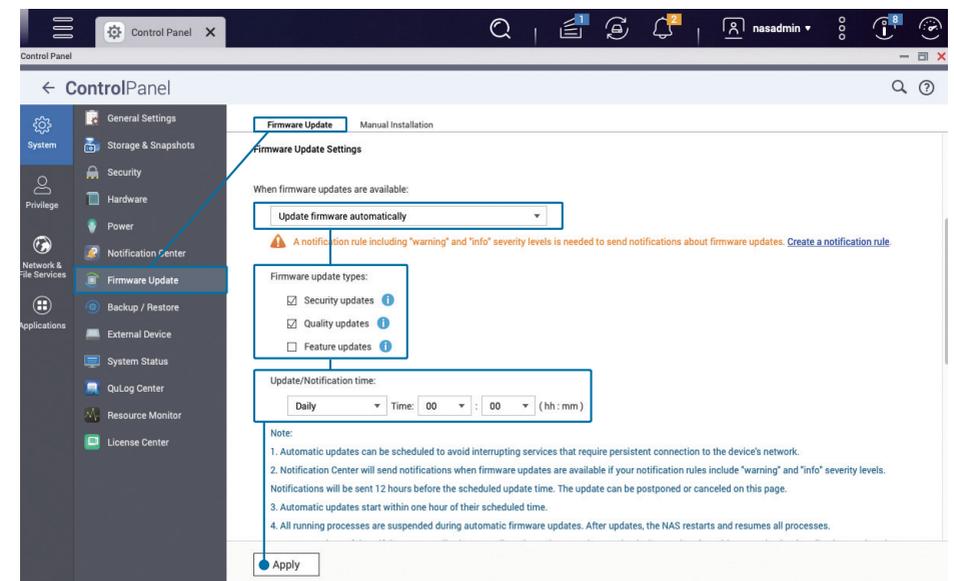
Die automatische Aktualisierungsfunktion erleichtert die Installation von Updates für neue Funktionen, Fehlerbehebungen und Sicherheitslücken.

Öffnen Sie die "Systemsteuerung" und klicken Sie auf "Firmware-Update"



Wählen Sie unter "Firmware-Update-Einstellungen" die Option "Firmware automatisch aktualisieren" und aktivieren Sie die Optionen "Sicherheitsaktualisierung" und "Qualitätsaktualisierung"; für "Aktualisierungs-/Benachrichtigungszeit" empfiehlt es sich, eine Nebenzeit wie "00: 00" festzulegen. Klicken Sie dann auf "Übernehmen".

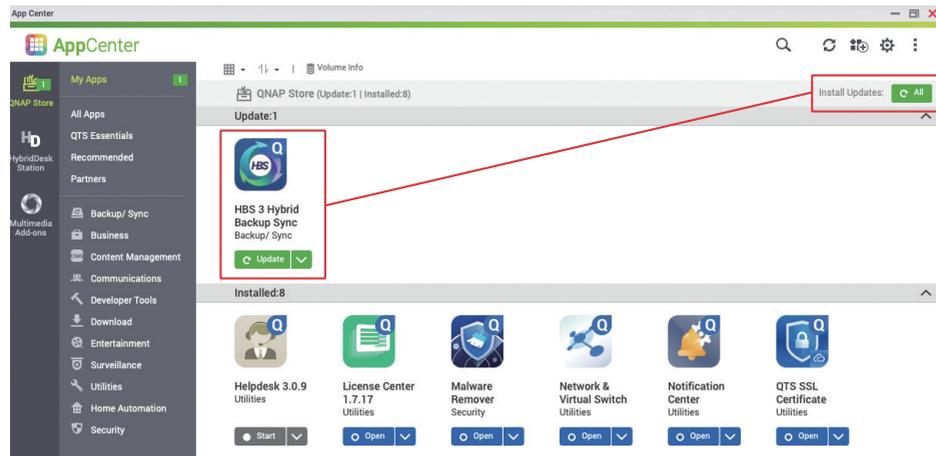
*** Für QTS 5.0.0/QuTS hero h5.0.0 (oder früher) aktivieren Sie "Empfohlene Version" auf der Seite "Automatisches Update"**



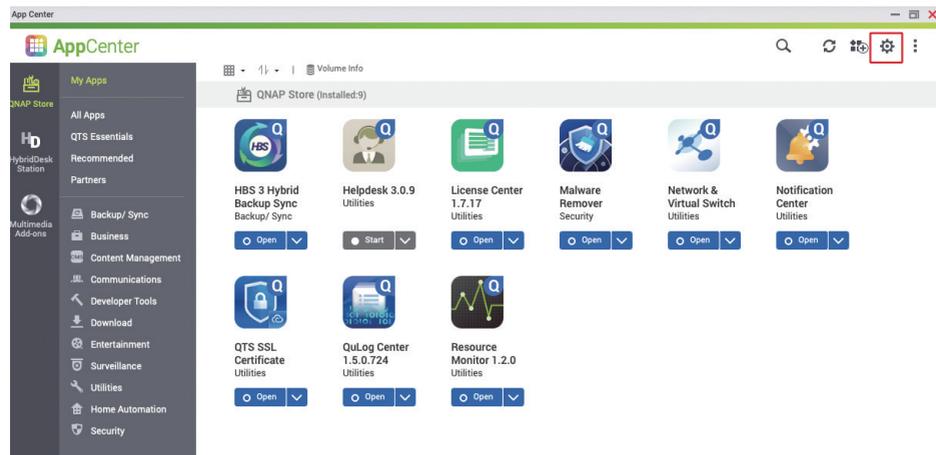
App-Update-Einstellungen

Das App Center bietet mehrere Apps, mit denen Sie Ihrem QNAP-NAS weitere Funktionen hinzufügen können. Die Apps müssen jedoch auch aktualisiert werden, um App-Funktionen zu verbessern, Probleme und Schwachstellen zu beheben und die Benutzerfreundlichkeit zu erhöhen.

Öffnen Sie das "App Center", um zu sehen, ob es Anwendungen gibt, die aktualisiert werden müssen. Ist dies der Fall, klicken Sie oben rechts auf die Schaltfläche "Alle  All", um alle Anwendungen zu aktualisieren.

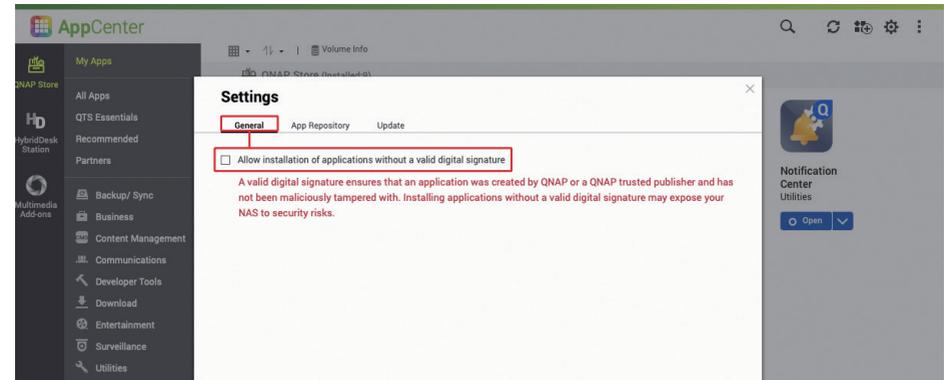


Nach Abschluss des Updates klicken Sie auf das Symbol  "Einstellungen" in der oberen rechten Ecke, um die Einstellungsseite des App Centers aufzurufen.



QNAP oder vertrauenswürdige QNAP-Entwickler fügen der App eine digitale Signatur hinzu, um sicherzustellen, dass sie echt ist. Es wird empfohlen, die Option "Installation von Anwendungen ohne gültige digitale Signatur zulassen" zu deaktivieren, um die Sicherheit zu erhöhen.

*** Die Option ist standardmäßig nicht aktiviert, sodass es unmöglich ist, Anwendungen ohne gültige digitale Signatur zu installieren**

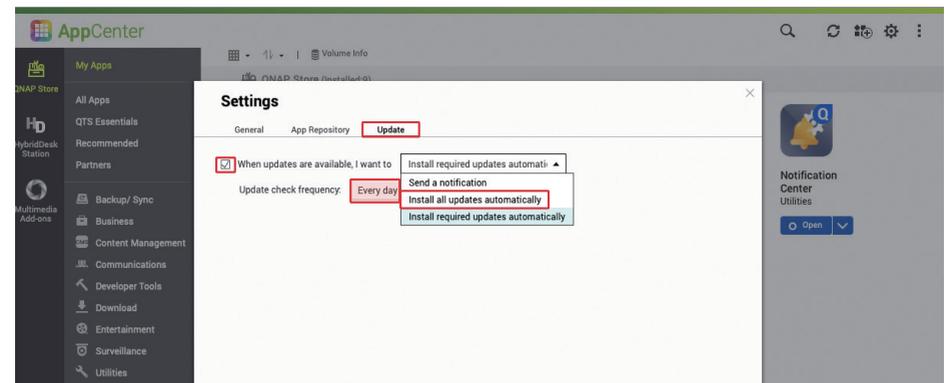


Klicken Sie auf die Registerkarte "Update". Wenn kein besonderer Bedarf besteht, empfiehlt es sich, die Option "Alle Updates automatisch installieren" zu wählen, die Häufigkeit auf "Täglich" einzustellen und auf "Übernehmen" zu klicken, um die Einstellung abzuschließen.

⇒ "Erforderliche Updates" werden hauptsächlich verwendet, um App- und Firmware-Abhängigkeiten zu erfüllen, und umfassen auch "Updates für größere Sicherheitslücken".

⇒ "Alle Updates" enthalten alle Funktionsverbesserungen, Fehlerbehebungen und alle Patches für Sicherheitslücken. Das Update wird in kürzeren Abständen durchgeführt.

*** Die Standardeinstellung ist "Alle Updates automatisch installieren"**

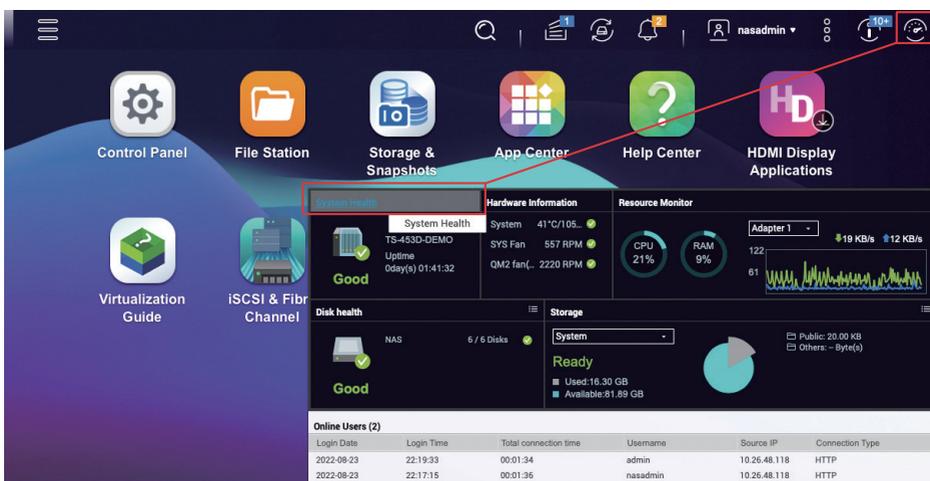


Unnötige Funktionen deaktivieren oder entfernen

Das QNAP-NAS bietet eine Vielzahl von Funktionen und Anwendungen, aber je mehr Funktionen aktiviert sind, desto mehr potenzielle Angriffsvektoren gibt es. Sie sollten regelmäßig prüfen und unnötige Funktionen deaktivieren (oder entfernen), um die Sicherheit zu erhöhen und das System reibungsloser arbeiten zu lassen.

★ Um die Produktsicherheit zu erhöhen, werden ab **QTS 5.0.0/QuTS hero h5.0.0** nicht essentielle Funktionen bei der Systeminitialisierung standardmäßig deaktiviert und das **App Center** installiert standardmäßig keine nicht essentiellen Anwendungen. Wenn das System vor der Aktualisierung auf **QTS 5.0.0/QuTS hero h5.0.0** initialisiert wurde, überprüfen Sie, welche Anwendungen installiert wurden.

Klicken Sie in der oberen rechten Ecke auf die Schaltfläche "☺", um das "Dashboard" des Systems zu öffnen, klicken Sie auf "Systemzustand", um das Fenster "Systemstatus" zu öffnen.



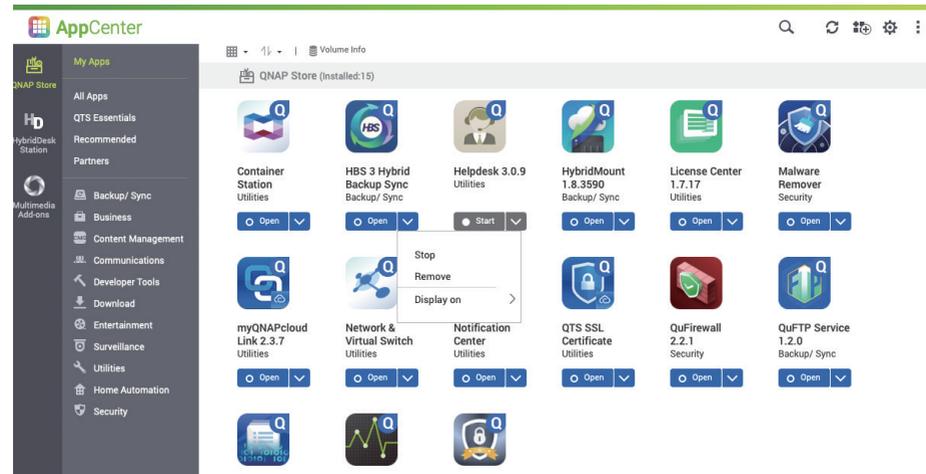
Klicken Sie auf "Systemdienst", um die aktivierten Systemfunktionen anzuzeigen. Sie können zur Systemsteuerung wechseln, um nicht benötigte Systemfunktionen zu deaktivieren.

System Status

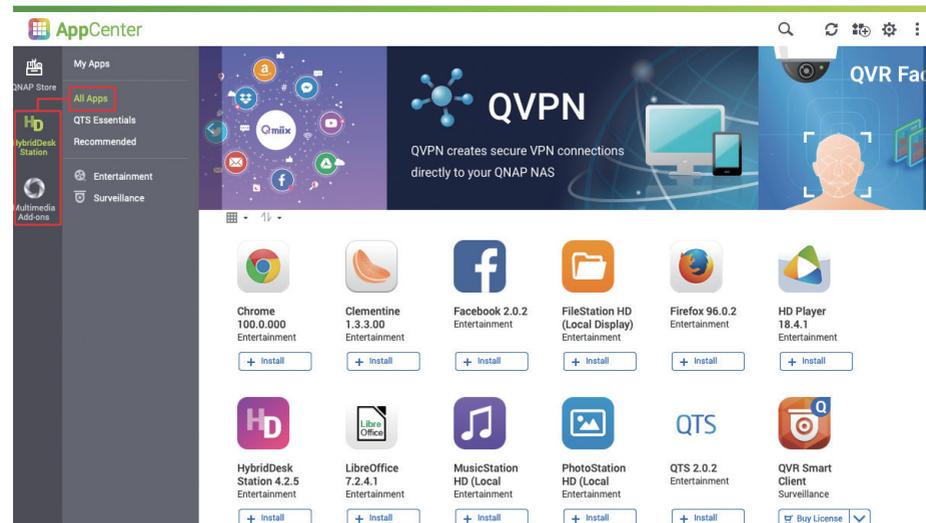
System Information Network Status **System Service** Hardware Information

Service	Status	Port	Description
Antivirus	Disabled	-	
Apple Networking	Disabled	-	
DDNS Service	Disabled	-	
Disk Management	Disabled	3260	
Domain Controller	Disabled	-	
FTP Service	Disabled	21	Maximum connections:30
LDAP Server	Disabled	-	
Microsoft Networking	Enabled	-	Server type :Standalone server Workgroup:WORKGROUP Enable WINS server:Disabled

Zusätzlich zu den im System integrierten Funktionen müssen Sie auch prüfen, welche Funktionen im App Center installiert sind.



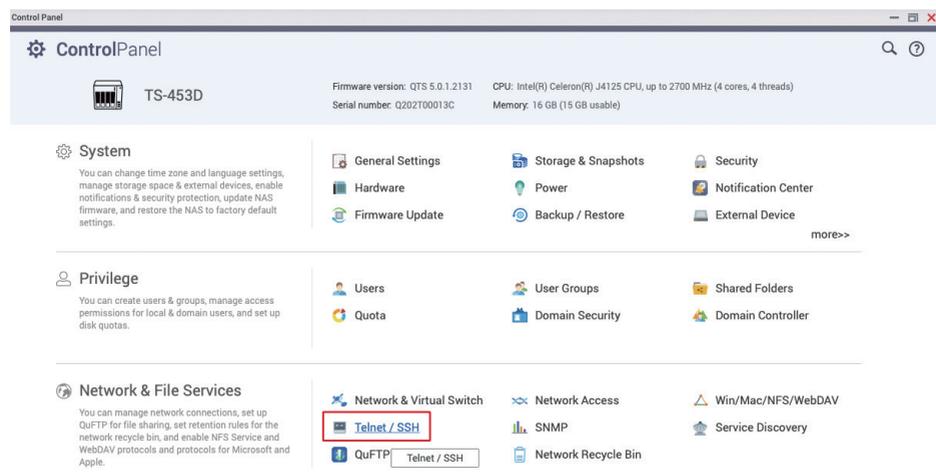
Klicken Sie auf der linken Seite auf "HybridDesk Station" und "Multimedia Add-ons", um den Status der entsprechenden Anwendungen anzuzeigen,



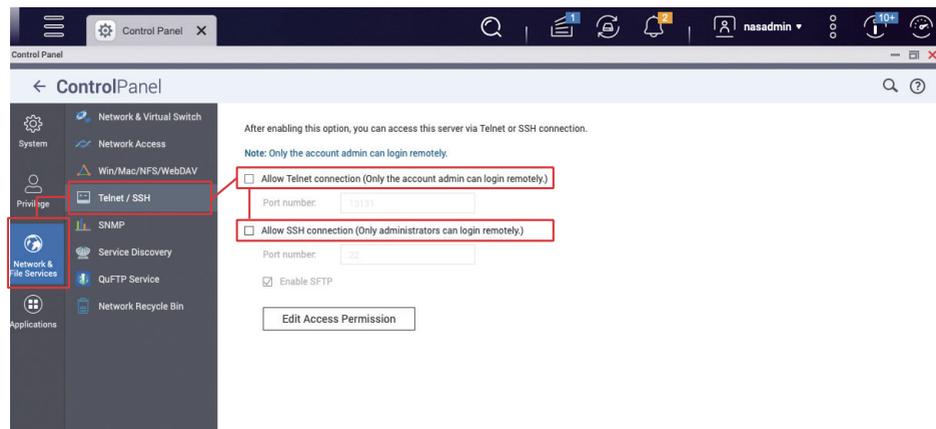
Telnet/SSH deaktivieren

Es wird dringend empfohlen, **Telnet und SSH zu deaktivieren**, wenn Sie sie nicht verwenden. Diese beiden Funktionen werden im Allgemeinen vom QNAP-Kundendienst oder von professionellem IT-Personal zur Wartung des Systems verwendet. Allgemeine Benutzer sollten sie nicht benötigen, daher wird empfohlen, sie zu deaktivieren.

Öffnen Sie die "Systemsteuerung" und klicken Sie auf "Telnet / SSH"



Deaktivieren Sie "Telnet-Verbindung zulassen" und "SSH-Verbindung zulassen" und klicken Sie dann auf "Übernehmen".

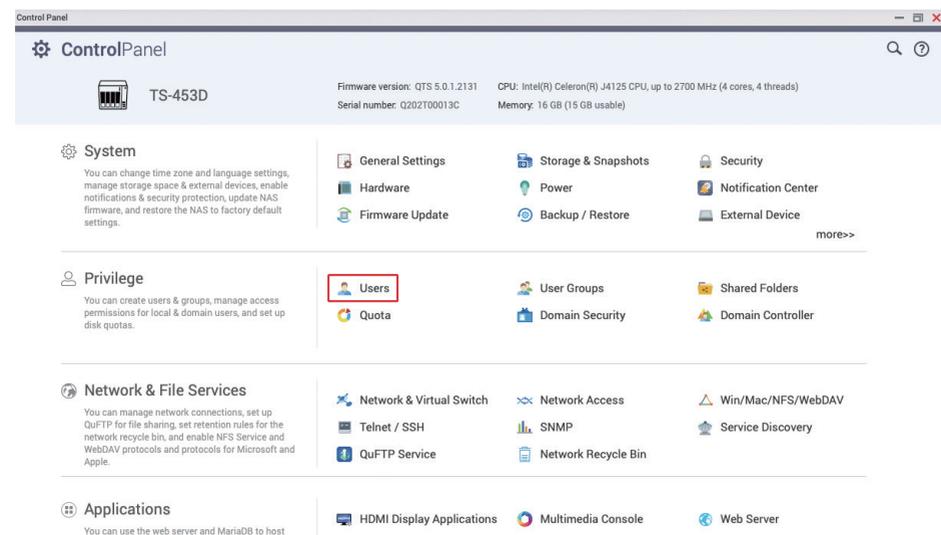


Stärkung der Sicherheit von Systemkonten

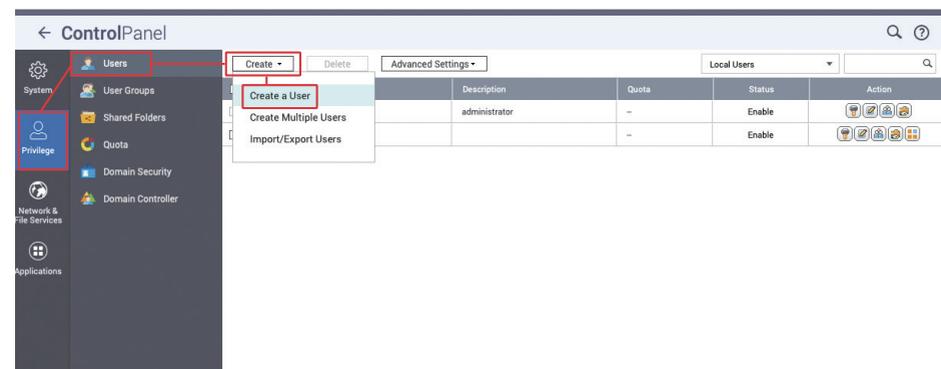
Das Standard Administratorkonto "admin" deaktivieren

Hacker, die Brute-Force-Passwort-Knacken verwenden, haben es in der Regel auf das Standard-Administratorkonto "admin" abgesehen. Wenn das System mit QTS 4.5.4 / QuTS hero h4.5.4 (oder früher) initialisiert wurde, ist das Standard-Administratorkonto "admin" aktiv. Gehen Sie folgendermaßen vor, um ein neues Administratorkonto zu erstellen und das "admin"-Konto zu deaktivieren.

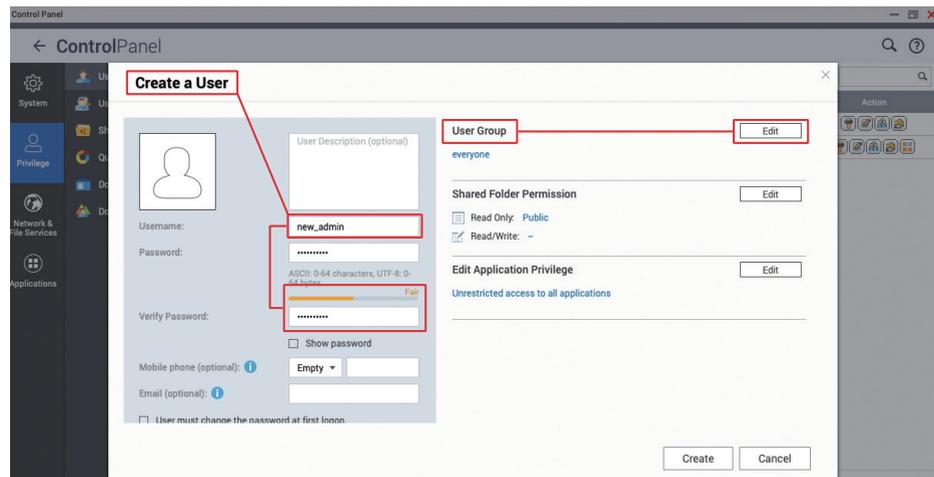
Öffnen Sie die "Systemsteuerung" und klicken Sie auf "Benutzer"



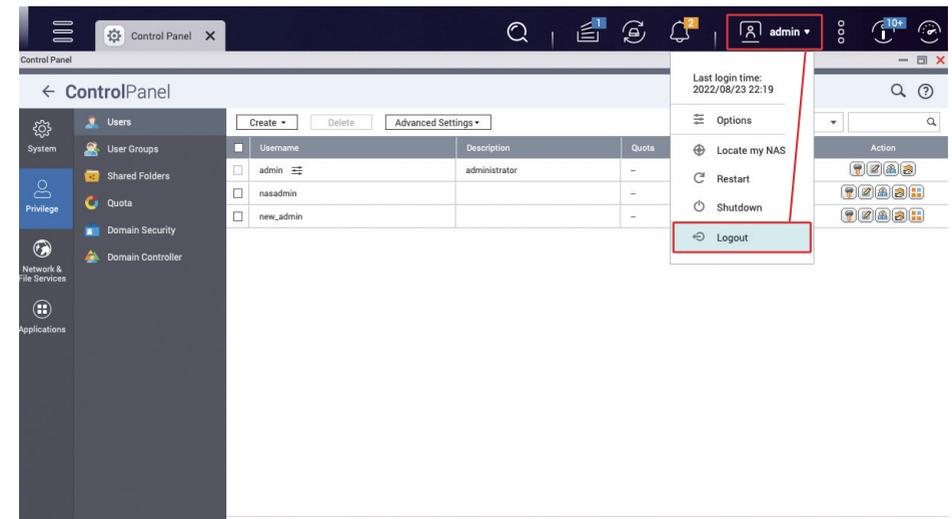
Klicken Sie auf "Erstellen" > "Benutzer erstellen"



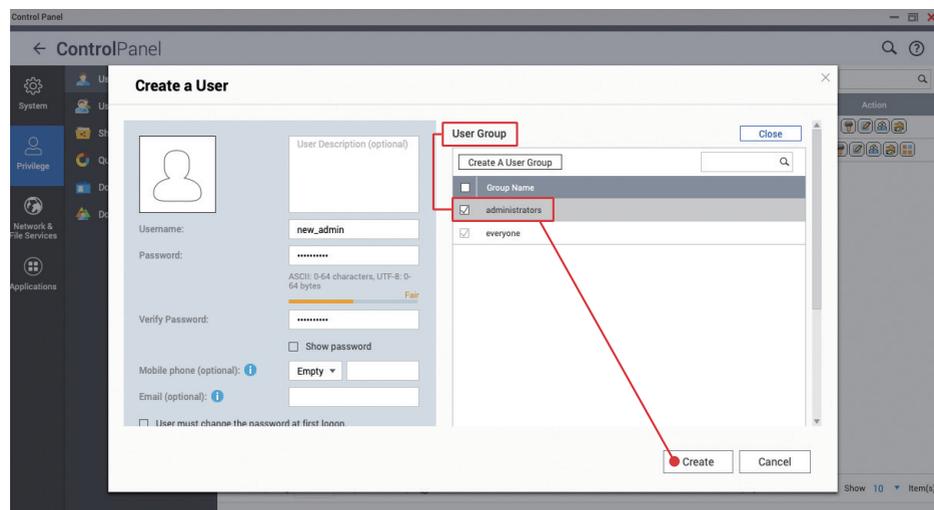
Geben Sie den Benutzernamen für das Administratorkonto ein, z. B. "new_admin", und legen Sie ein sicheres Passwort fest.



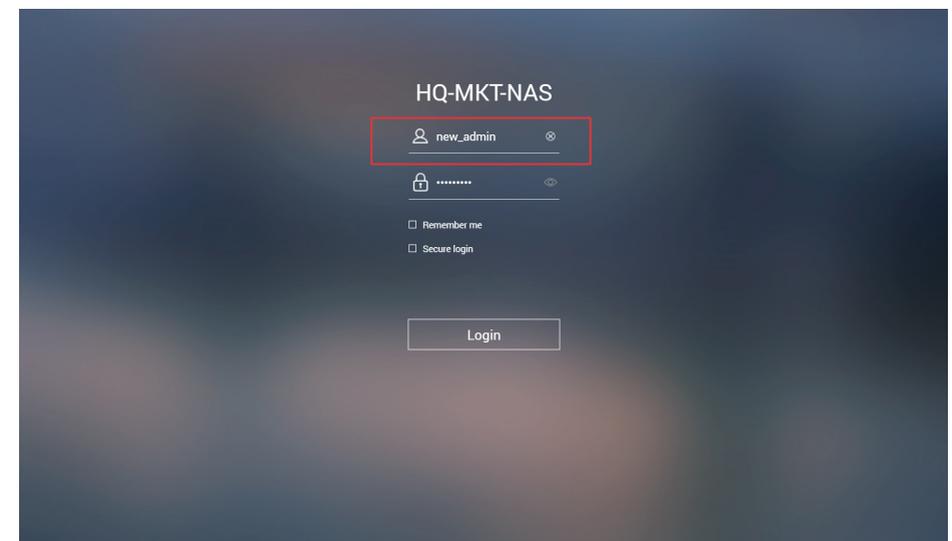
Klicken Sie oben auf "admin", öffnen Sie das Menü und klicken Sie auf "Abmelden", um sich von der QTS-Webverwaltungsschnittstelle abzumelden.



Klicken Sie im Abschnitt "Benutzergruppe" auf "Bearbeiten", aktivieren Sie die Gruppe "Administratoren" und klicken Sie auf "Erstellen", um einen neuen Benutzer hinzuzufügen.

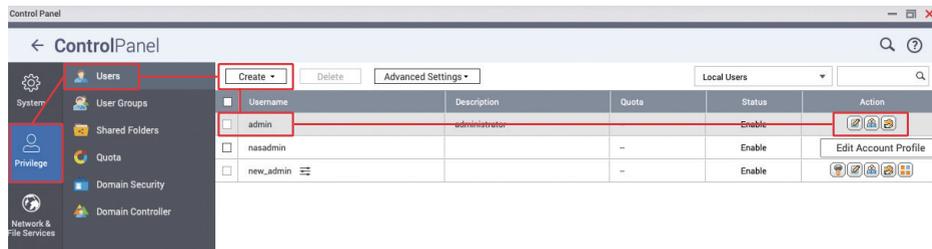


Verwenden Sie das soeben erstellte "Administratorkonto", um sich bei der QTS-Webverwaltungsschnittstelle anzumelden.

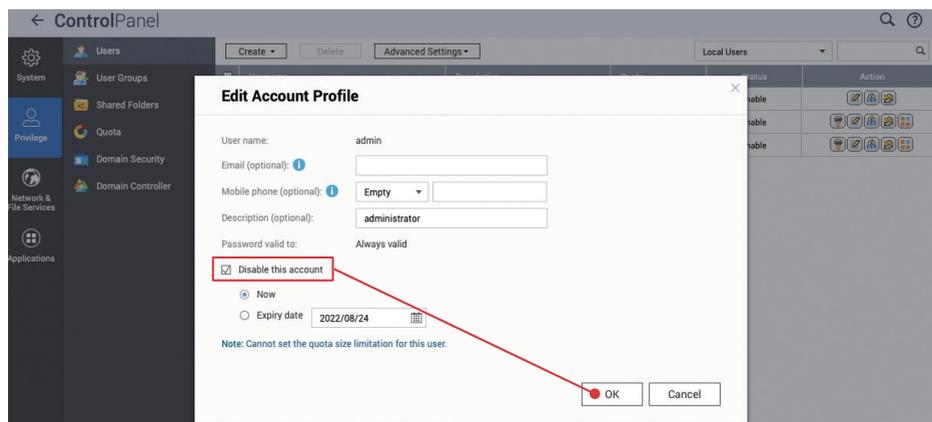


Passwortrichtlinie festlegen

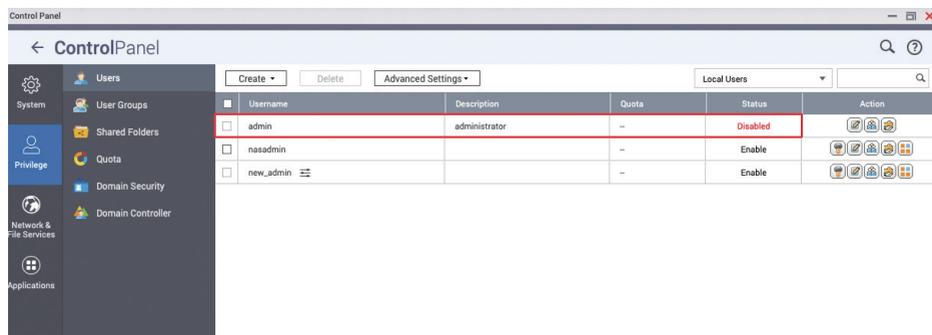
Öffnen Sie die "Systemsteuerung" erneut, klicken Sie auf "Benutzer", und klicken Sie in der Zeile "Admin" auf "Kontoprofil bearbeiten"



Aktivieren Sie "Dieses Konto deaktivieren" und klicken Sie zum Abschluss auf "OK"

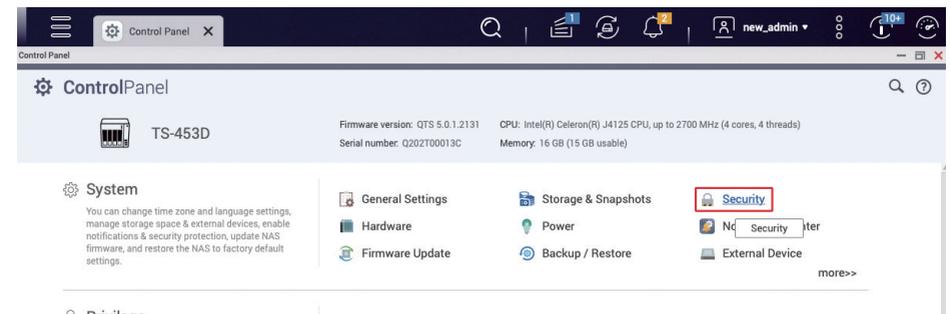


Nach der Fertigstellung können Sie sehen, dass der "admin"-Status "Deaktiviert" ist

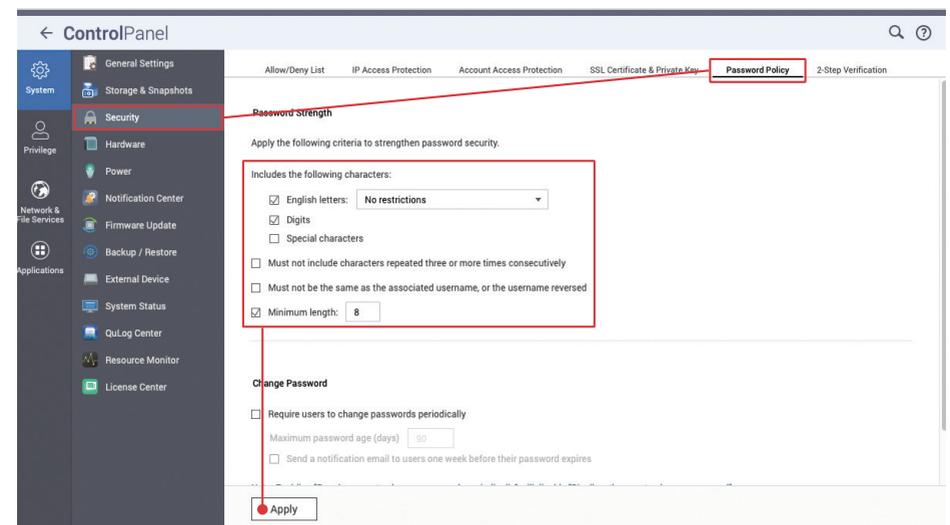


Neben der Deaktivierung des Standard-Administratorkontos "admin" müssen Sie auch sicherstellen, dass alle Konten sichere Passwörter haben. Mit dem "Zugriffsschutz" können Sie böswillige Anmeldeversuche blockieren. Zur Erhöhung der Sicherheit können Sie für alle Konten eine zweistufige Verifizierung (2SV) erzwingen, um das Knacken von Passwörtern und böswillige Anmeldungen zu verhindern.

Öffnen Sie die "Systemsteuerung" und klicken Sie auf "Sicherheitseinstellungen"



Klicken Sie auf "Passwortrichtlinie", um die Einstellungsseite zu öffnen. Wenn das System in QTS 5.0.0 / QuTS hero h5.0.0 (oder später) initialisiert wurde, sind die grundlegenden Bedingungen für die Passwortstärke standardmäßig aktiviert. Sie können die Bedingungen für sichere Passwörter nach Ihren Bedürfnissen festlegen. Das Passwort kann "Groß- und Kleinbuchstaben" und "Zahlen" enthalten, und es wird empfohlen, dass das Passwort mindestens "10 Zeichen" lang ist. Klicken Sie anschließend auf "Übernehmen".



Zugriffsschutz aktivieren (IP/Konto)

"IP-Zugriffsschutz" und "Kontozugriffsschutz" können dazu beitragen, dass Passwörter nicht mit Brute Force geknackt werden können. Wenn sich eine bestimmte IP oder ein bestimmtes Konto zu oft nicht anmeldet, wird die IP gesperrt oder das Konto deaktiviert, sodass Angreifer keine Passwörter mehr ausprobieren können.

Klicken Sie auf "IP-Zugriffsschutz", um die Einstellungsseite aufzurufen, markieren Sie alle Dienste, stellen Sie das "Zeitintervall", die "Fehlgeschlagene Anmeldeversuche" und die "Dauer der IP-Sperre" nach Ihren Anforderungen ein und klicken Sie dann auf "Übernehmen", um die Einstellungen abzuschließen.

Allow/Deny List **IP Access Protection** Account Access Protection SSL Certificate & Private Key Password Policy 2-Step Verification

Automatically block client IP addresses after too many failed login attempts within the specified time period. You can view blocked IP addresses in [QuFirewall](#).

Service	Time interval	Failed login attempts
<input checked="" type="checkbox"/> SSH	1 minute(s)	5
<input checked="" type="checkbox"/> Telnet	1 minute(s)	5
<input checked="" type="checkbox"/> HTTP(S)	1 minute(s)	5
<input checked="" type="checkbox"/> FTP	1 minute(s)	5
<input checked="" type="checkbox"/> SAMBA	1 minute(s)	5
<input checked="" type="checkbox"/> AFP	1 minute(s)	5
<input checked="" type="checkbox"/> RTTR	1 minute(s)	5
<input checked="" type="checkbox"/> Rsync	1 minute(s)	5

Apply

*** Wenn die IP-Adresse eines normalen Benutzers versehentlich blockiert wird, können Sie die Blockierliste anpassen, indem Sie Folgendes ausführen:**

- Melden Sie sich von einem anderen Computer aus bei der Verwaltungsschnittstelle von QTS/QuTS hero an**
- Ändern Sie die IP-Adresse und melden Sie sich bei der QTS/QuTS hero-Verwaltungsschnittstelle an**
- Melden Sie sich mit einem mobilen Browser bei der Verwaltungsschnittstelle von QTS/QuTS hero an**
- Verwenden Sie die QManager-App**

Klicken Sie auf "Kontozugriffsschutz", um die Einstellungsseite aufzurufen, aktivieren Sie die entsprechenden Dienste, stellen Sie das "Zeitintervall" und die "Fehlgeschlagene Anmeldeversuche" entsprechend Ihren Anforderungen ein und klicken Sie auf "Übernehmen", um die Einstellung abzuschließen.

Allow/Deny List IP Access Protection **Account Access Protection** SSL Certificate & Private Key Password Policy 2-Step Verification

Disable accounts automatically when they fail too many login attempts within a specified time period. You can view the disabled accounts in [Users](#).

Users: All users not in the administrators group

Service	Time interval	Failed login attempts
<input type="checkbox"/> SSH	5 minute(s)	5
<input type="checkbox"/> Telnet	5 minute(s)	5
<input type="checkbox"/> HTTP(S)	5 minute(s)	5
<input type="checkbox"/> FTP	5 minute(s)	5
<input type="checkbox"/> SAMBA	5 minute(s)	5
<input type="checkbox"/> AFP	5 minute(s)	5
<input type="checkbox"/> RTTR	5 minute(s)	5
<input type="checkbox"/> Rsync	5 minute(s)	5

Apply

*** Wenn "Kontozugriffsschutz" für das Administratorkonto aktiviert ist, besteht die Möglichkeit, dass alle Administratorkonten aufgrund von Passwort-Cracking-Angriffen deaktiviert werden. Zu diesem Zeitpunkt kann das "admin"-Konto nur über die Rücksetzfunktion wieder aktiviert werden, und das Passwort für das "admin"-Konto wird ebenfalls zurückgesetzt. Denken Sie daran, Ihr Passwort nach dem Zurücksetzen zu ändern.**

Zwei-Schritt-Verifizierung (2SV) aktivieren

Klicken Sie auf "2-Schritt-Verifizierung", um die Einstellungsseite zu öffnen. Sie können die Verwendung der "2-Schritt-Verifizierung (2SV)" für "Benutzer" oder "Benutzergruppen" erzwingen. Es wird dringend empfohlen, 2SV für Konten in der "Administratorengruppe" zu aktivieren. Bei anderen Konten sollten Sie die Risiken selbst einschätzen und entsprechende Einstellungen vornehmen.

Klicken Sie auf "Lokale Benutzer", um das Menü zu öffnen, und wählen Sie "Lokale Gruppen".

Control Panel

← ControlPanel

Allow/Deny List IP Access Protection Account Access Protection SSL Certificate & Private Key Password Policy **2-Step Verification**

2-Step Verification

2-Step Verification (2SV) adds an extra layer of protection to a user's account by requiring an additional one-time security code whenever a user signs in to your NAS. You can enforce 2-step verification for specific users and groups.

Note: The configuration of "Enforce 2SV" between the group and users in the group may not be consistent. See "Status" to check the final 2SV status of users.

Enforce 2SV	Username	Description
<input type="checkbox"/>	admin	administrator
<input type="checkbox"/>	naadmin	
<input type="checkbox"/>	new_admin	

Local Users

- Local Users
- Local Groups
- Domain Users
- Domain Groups

Disabled

Aktivieren Sie "2SV erzwingen" unter "Administratoren" und klicken Sie auf "Übernehmen", um die Einstellung abzuschließen.

Control Panel

← ControlPanel

Allow/Deny List IP Access Protection Account Access Protection SSL Certificate & Private Key Password Policy **2-Step Verification**

2-Step Verification

2-Step Verification (2SV) adds an extra layer of protection to a user's account by requiring an additional one-time security code whenever a user signs in to your NAS. You can enforce 2-step verification for specific users and groups.

Note: The configuration of "Enforce 2SV" between the group and users in the group may not be consistent. See "Status" to check the final 2SV status of users.

Enforce 2SV	Group Name	Description	Status
<input checked="" type="checkbox"/>	administrators		-
<input type="checkbox"/>	everyone		-

Local Groups

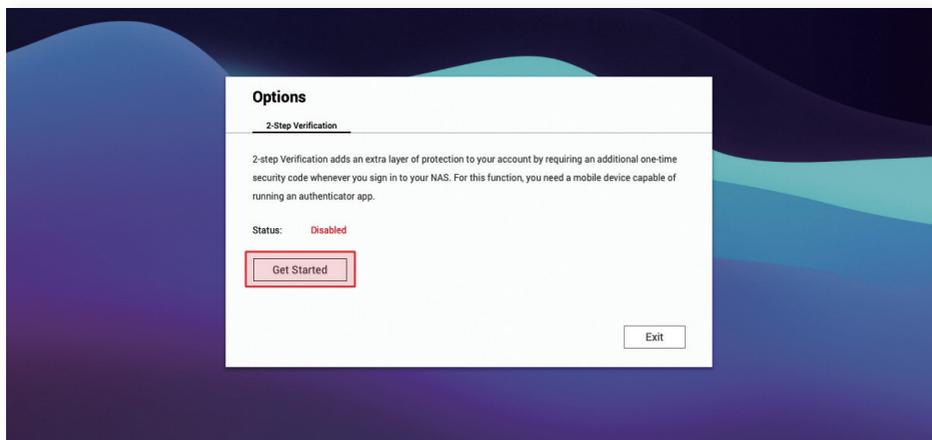
Page 1 / 1

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

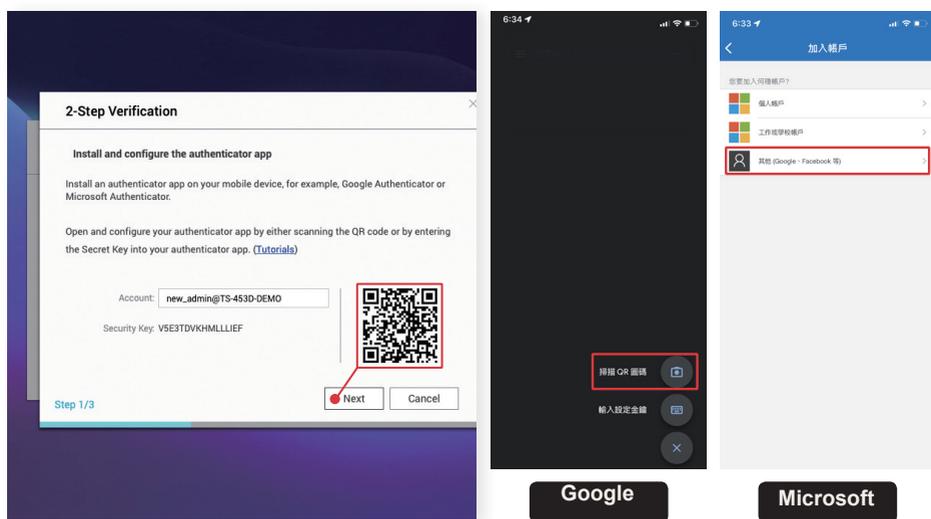
Apply

Wenn Sie nach dem Aktivieren von "2SV erzwingen" das Konto "Administrator" nicht mit der "2-Schritt-Verifizierung (2SV)" eingerichtet haben, werden Sie bei der nächsten Anmeldung zwangsweise auf die Einstellungsseite für die "2-Schritt-Verifizierung (2SV)" geleitet, um das Konto einzurichten.

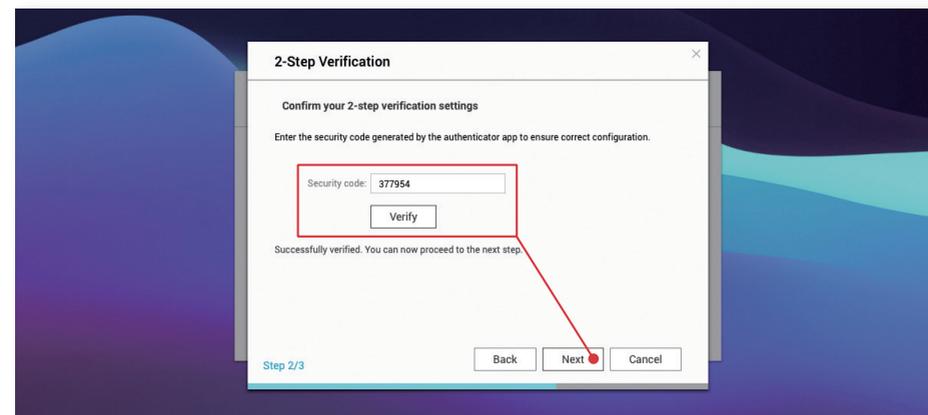
Melden Sie sich erneut mit dem Konto "Systemadministrator" an und klicken Sie auf "Erste Schritte", um die Einstellung zu starten.



Installieren Sie "Google Authenticator" oder "Microsoft Authenticator" auf Ihrem mobilen Gerät, scannen Sie den QR-Code im Programm, um das Gerät hinzuzufügen, und klicken Sie dann auf "Weiter".

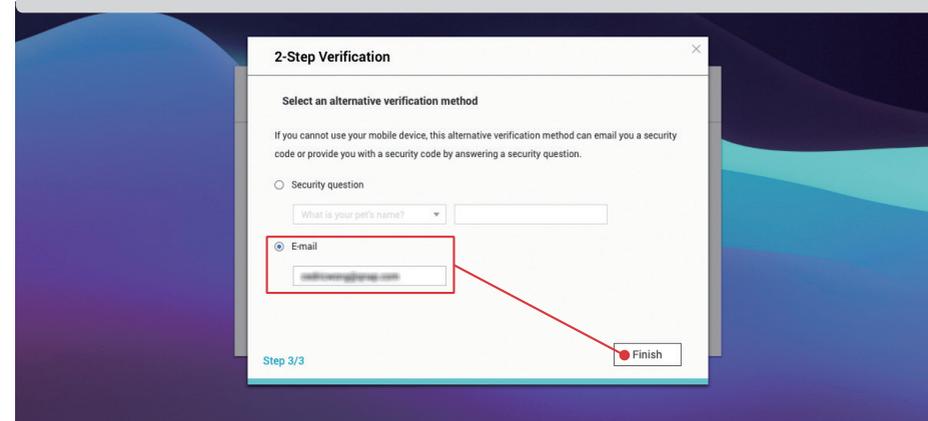


Geben Sie den sechsstelligen "Sicherheitscode" ein, der von "Google Authenticator" oder "Microsoft Authenticator" generiert wurde, und klicken Sie auf "Bestätigen". Klicken Sie nach der Verifizierung auf "Weiter", um fortzufahren.



Um eine alternative Verifizierungsmethode* einzurichten, können Sie "Sicherheitsfrage"*** oder "E-Mail"*** auswählen, ausfüllen und auf "Fertigstellen" klicken, um die "2-Schritt-Verifizierung (2SV)" zu aktivieren.

- * Wenn Sie den "Sicherheitscode" nicht von einer Authentifizierungs-App erhalten können, können Sie einen "Sicherheitscode" erhalten, indem Sie die "Sicherheitsfrage" beantworten oder "E-Mail" verwenden.
- ** Beantworten Sie die "Sicherheitsfrage" richtig, um die 2-Schritt-Verifizierung zu bestehen. Verwenden Sie keine einfachen oder leicht zu erratenden Fragen und Antworten.
- *** Sie müssen die Benachrichtigungsmethode "E-Mail" im "Notification Center" hinzufügen, um diese Funktion verwenden zu können.



Standard-Ports ändern

Jeder auf dem NAS ausgeführte Dienst hat einen entsprechenden Dienst-Port. Mit Ausnahme einiger standardisierter Dienst-Ports, die nicht geändert werden können, kann der Rest von den Benutzern definiert werden.

Wenn ein Hacker nach einem Angriffsziel sucht oder die IoT-Suchmaschine verwendet, die häufig von Hackern eingesetzt wird, wird in der Regel zuerst der Standard-Port ausprobiert. Um das Risiko eines Angriffs zu verringern, müssen Sie die Standard-Ports der gängigen Dienste ändern. Was Angriffe auf NAS betrifft, so ist das häufigste Ziel der "Systemport". Im Folgenden wird gezeigt, wie Sie den "Systemport" ändern können. Die Ports für andere Funktionen können auf der entsprechenden Einstellungsseite geändert werden. Ändern Sie diese aus Sicherheitsgründen, bevor Sie die entsprechenden Dienste verwenden.

Öffnen Sie "Systemsteuerung", klicken Sie auf "Allgemeine Einstellungen", der "Systemport (HTTP)" ist standardmäßig "8080", Sie können eine Portnummer zwischen 1 und 65535 eingeben, z. B. "56789"; für den "Systemport (HTTPS)", d. h. den **Systemport** (standardmäßig "443") mit aktivierter Funktion **"sichere Verbindung" (HTTPS) erzwingen** zu aktivieren, um sicherzustellen, dass alle Benutzer ihre Daten über HTTPS übertragen, und um zu verhindern, dass Hacker sensible Informationen wie Kontopasswörter abfangen.

Außerdem wird **empfohlen, die Option "URL-Umleitung auf NAS-Anmeldeseite zulassen" zu deaktivieren**, um zu verhindern, dass der "Systemport" durch die automatische Umleitung offengelegt wird. Klicken Sie nach der Änderung auf "Übernehmen", um die Einstellung abzuschließen.

Control Panel

System Administration

Server name: TS-453D-DEMO

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

System port: 8080

Enable HTTP compression

Enable secure connection (HTTPS)

TLS version compatibility: 1.2 and later

Enable strong cipher suites

Port number: 443

Force secure connection (HTTPS) only

Custom HTTP Server header

Do not allow QTS embedding in iFrames

Allow specific websites to embed QTS

Enable X-Content-Type-Options HTTP

Enable Content-Security-Policy HTTP

Allow redirect URL to NAS login page

Apply

Zugriffsprotokolle anzeigen

Mit Hilfe von Zugriffsprotokollen können Sie den Dateizugriff, den Betrieb und den Anmeldeverlauf des Benutzers anzeigen. Wenn ein Problem auftritt, sollte die Überprüfung der Zugriffsprotokolle der erste Schritt sein, um die zugrunde liegenden Probleme zu diagnostizieren.

QuLog Center

Access Log

Grouping mode: [v] Display style: [v] Export Logs: [v] Specify keywords: [v]

Total log entries: 50

0 [x] 13 [!] 37 [i]

Tip: Click a severity level button to display the selected severity level logs.

<input type="checkbox"/>	Se...	Time	User	Source IP	Compute...	Connecti...	Accesse...	Action	...
<input type="checkbox"/>	[i]	2022/08/28 00:49:36	new_admin	10.26.48...	cedric-m...	SMB	Public/@...	Read	⋮
<input type="checkbox"/>	[i]	2022/08/28 00:49:33	new_admin	10.26.48...	cedric-m...	SMB	Public/Ac...	Deleted	⋮
<input type="checkbox"/>	[i]	2022/08/28 00:49:12	new_admin	10.26.48...	cedric-m...	SMB	Public/Ac...	Read	⋮
<input type="checkbox"/>	[i]	2022/08/28 00:49:12	new_admin	10.26.48...	cedric-m...	SMB	Public/Ac...	Read	⋮
<input type="checkbox"/>	[i]	2022/08/28 00:49:12	new_admin	10.26.48...	cedric-m...	SMB	Public/Ac...	Read	⋮
<input type="checkbox"/>	[i]	2022/08/28 00:49:00	new_admin	10.26.48...	cedric-m...	SMB	Public/D...	Read	⋮
<input type="checkbox"/>	[i]	2022/08/28 00:49:00	new_admin	10.26.48...	cedric-m...	SMB	---	Logged in	⋮
<input type="checkbox"/>	[!]	2022/08/28 00:48:58	new_admin	10.26.48...	cedric-m...	SMB	---	Failed to log in	⋮
<input type="checkbox"/>	[!]	2022/08/28 00:48:57	new_admin	10.26.48...	cedric-m...	SMB	---	Failed to log in	⋮
<input type="checkbox"/>	[i]	2022/08/28 00:17:00	nasadmin	10.26.48...	---	HTTP	Administ...	Logged in	⋮
<input type="checkbox"/>	[i]	2022/08/27 23:59:01	new_admin	10.26.48...	---	SSH/SETP	---	Logged in	⋮

Page 1 / 1

Display item: 1 - 50, Total: 50

Öffnen Sie "QuLog Center", klicken Sie im linken Menü auf "Protokolleinstellungen", wechseln Sie zur Seite "Zugriffsprotokolleinstellungen", aktivieren Sie unter "Verbindungstypen" alle Verbindungen und klicken Sie dann auf "Übernehmen", um die Einstellung abzuschließen.

QuLog Center

Log Settings

Event Log Settings | Access Log Settings | Event Indicators

Destination: System

Maximum number of entries: 5 million

Log retention time: Last 180 days

Archive and move log entries to the specified location after reaching the database limit.

Destination folder: Please choose a destination. Browse

Delete All Access Logs

Connection Types

Select the connections you want to log.

HTTP/HTTPS SSH/SFTP iSCSI

FTP AFP (Mac) RADIUS

Telnet SMB WebDAV

Apply

Sicherheits-Apps installieren und aktivieren

QNAP bietet mehrere Sicherheitsanwendungen zur Verbesserung der NAS-Sicherheit. Die Einrichtung dieser Apps kann die NAS-Sicherheit verbessern und gibt den Benutzern ein Gefühl der Sicherheit.



Security Counselor überprüft regelmäßig die Sicherheit Ihrer NAS-Einstellungen und informiert Sie über mögliche Risiken.



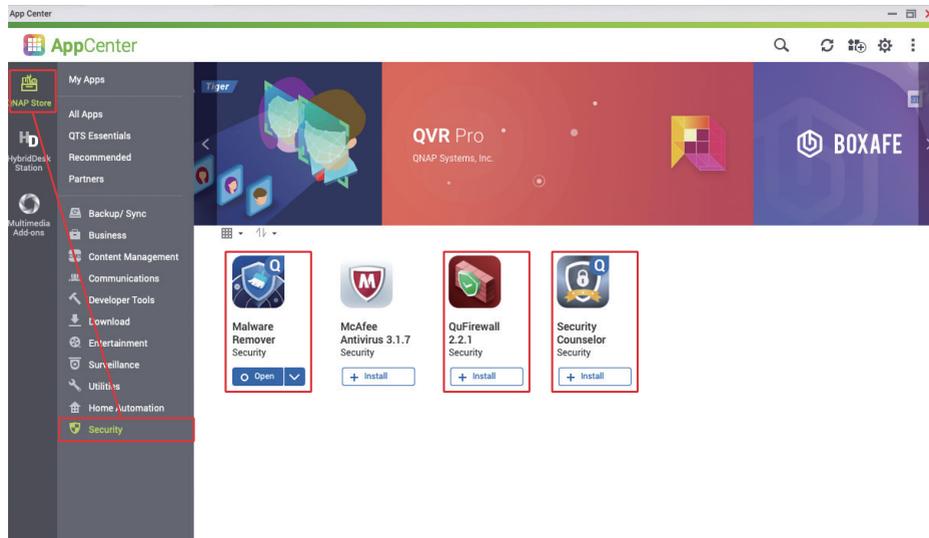
Malware Remover scannt und entfernt erkannte Malware von Ihrem NAS.



QuFirewall bietet grundlegende Firewall-Funktionen für das QNAP-NAS, die so viele Hacker wie möglich davon abhalten, sich mit Ihrem NAS zu verbinden.

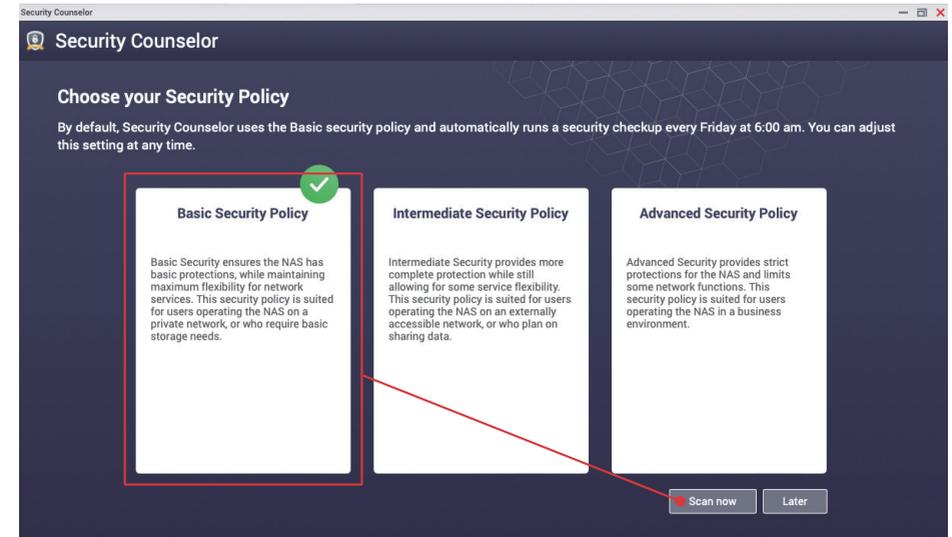
Öffnen Sie "APP Center", klicken Sie links auf "Sicherheit", installieren Sie "Security Counselor", "Malware Remover" und "QuFirewall".

★ Malware Remover ist auf QTS 4.4.3 (und höher) und QuTS hero vorinstalliert

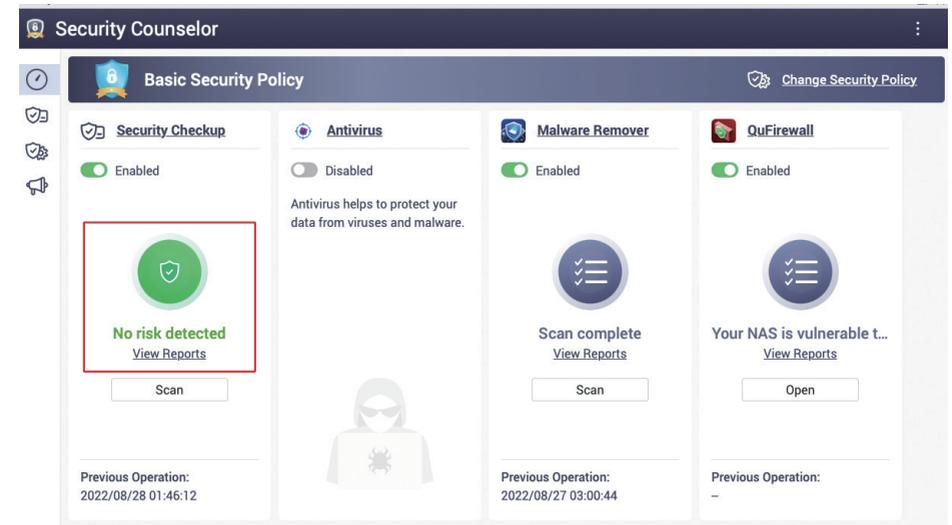


Security Counselor

Öffnen Sie "Security Counselor", wählen Sie "Einfache Sicherheitsrichtlinie" und klicken Sie auf "Jetzt scannen".



Nach Abschluss des Scans lautet das Ergebnis normalerweise "Kein Risiko erkannt". Wenn ein Risiko erkannt wird, klicken Sie auf "Berichte anzeigen", um Einzelheiten zu erfahren, und folgen Sie den Anweisungen, um die Einstellungen zu ändern.



Im Folgenden sind die Scan-Ergebnisse aufgeführt, die durch "hohes Risiko" mit absichtlich geänderten falschen Einstellungen verursacht wurden. Klicken Sie auf "Assistent für vorgeschlagene Einstellungen", der Ihnen bei der Anpassung der Einstellungen hilft.

Security Counselor

Basic Security Policy Change Security Policy

At High Risk Last scan status: Finished Last scan time: 2022/08/28 01:53:30 Scan schedule: Friday 06:00

Overview **1** High **1** Medium **0** Low **0** Scan

Category	Status	Risk	Result	Action
Account	❌	High	Either this setting is deselected in the Password Policy screen or the current required mini...	⋮
Update	✅	High	The	⋮
Account	✅	High	The	⋮
Network	✅	High	Either this setting is deselected in the Password Policy screen or the current required minimum length for passwords is below 8 characters.	⋮
Network	✅	High	The web server on your device cannot be directly accessed from the internet using the foll...	⋮
Network	✅	High	The NAS doesn't allow Telnet connections.	⋮
System	✅	High	Run user defined processes during startup is disabled.	⋮

Der "Assistent für vorgeschlagene Einstellungen" listet relevante Vorschläge auf. Nach dem Lesen und Bestätigen klicken Sie auf "Vorschlag übernehmen" und das System übernimmt die entsprechenden Einstellungen automatisch für Sie. Einige Einstellungen müssen manuell geändert werden. Klicken Sie auf die Registerkarte "Manuell" auf der linken Seite und passen Sie die Einstellungen wie vorgeschlagen an. Nachdem die Änderungen übernommen wurden, wird der Scanvorgang automatisch neu gestartet. Sie können die Scanergebnisse erneut überprüfen, um sicherzustellen, dass keine Sicherheitsrisiken auf dem NAS entdeckt wurden.

Security Counselor

Suggested Settings Assistant

The Suggested Settings Assistant offers suggestions that help improve NAS security.

Automatic Adjustment: There are **1** at-risk settings. Select the risk items below to automatically adjust the related settings.

At-risk User Settings	Suggestion
<input checked="" type="checkbox"/> Either this setting is deselected in the Password Policy screen or the current required minimum length for passwords is below 8 characters.	<input checked="" type="checkbox"/> Configure the settings in the Password Policy screen and require the use of passwords with a minimum of 8 characters.

Apply suggestion Close

Klicken Sie links auf "Sicherheitsüberprüfung", um den Bildschirm mit den Scan-Ergebnissen aufzurufen, und klicken Sie dann rechts auf "Scan-Zeitplan" , um den Bildschirm mit den Scan-Zeitplaneinstellungen zu öffnen.

Security Counselor

Basic Security Policy Change Security Policy

No risk detected Last scan status: Finished Last scan time: 2022/08/28 02:08:53 Scan schedule: Friday 06:00 Scan schedule

Overview **0** High **0** Medium **0** Low **0** Scan

Category	Status	Risk	Result	Action
Update	✅	High	The NAS is using the most up-to-date version of firmware.	⋮
Account	✅	High	The current settings in the Password Policy screen include requiring passwords to have a ...	⋮
Account	✅	High	The default administrator password is not the default password.	⋮
Network	✅	High	The system administration service on your device cannot be directly accessed from the int...	⋮
Network	✅	High	The web server on your device cannot be directly accessed from the internet using the foll...	⋮
Network	✅	High	The NAS doesn't allow Telnet connections.	⋮
System	✅	High	Run user defined processes during startup is disabled.	⋮

Es wird empfohlen, "Scan-Zeitplan" auf **mindestens einmal pro Monat** einzustellen, damit das System regelmäßig die Einstellungen und den Systemstatus überprüfen kann. Wenn ein Risiko erkannt wird und das Notification Center korrekt eingerichtet ist, erhalten Sie eine Benachrichtigung, damit das Problem so schnell wie möglich behoben werden kann.

Security Counselor

Basic Security Policy Change Security Policy

No risk detected Last scan status: Finished Last scan time: 2022/08/28 02:08:53 Scan schedule: Friday 06:00 Scan schedule

Overview **0** High **0** Medium **0** Low **0** Scan

Scan schedule

Disable schedule

Enable schedule

Run on the following days: Friday

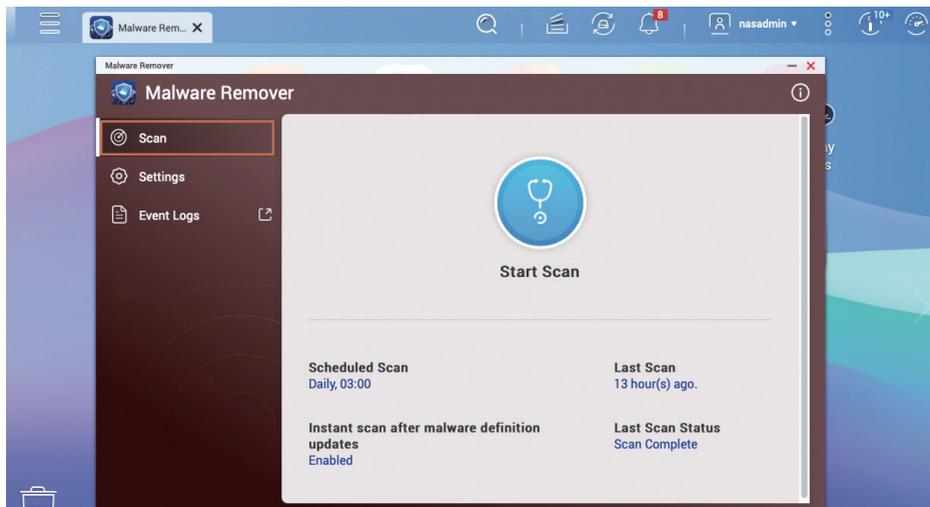
Run at the following time: 06:00

Apply Cancel

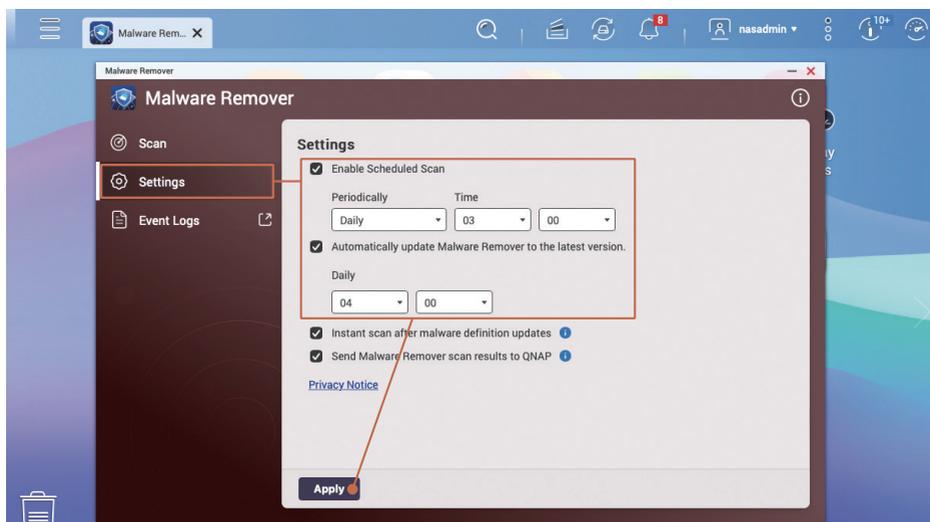
Category	Status	Risk	Result	Action
Update	✅	High	The NAS is using the most up-to-date version of firmware.	⋮
Account	✅	High	The current settings in the Password Policy screen include requiring passwords to have a ...	⋮
Account	✅	High	The default administrator password is not the default password.	⋮
Network	✅	High	The system administration service on your device cannot be directly accessed from the int...	⋮
Network	✅	High	The web server on your device cannot be directly accessed from the internet using the foll...	⋮
Network	✅	High	The NAS doesn't allow Telnet connections.	⋮
System	✅	High	Run user defined processes during startup is disabled.	⋮

Malware Remover

Öffnen Sie "Malware Remover", der Status des letzten Scans wird angezeigt. Klicken Sie auf "Einstellungen" auf der linken Seite.

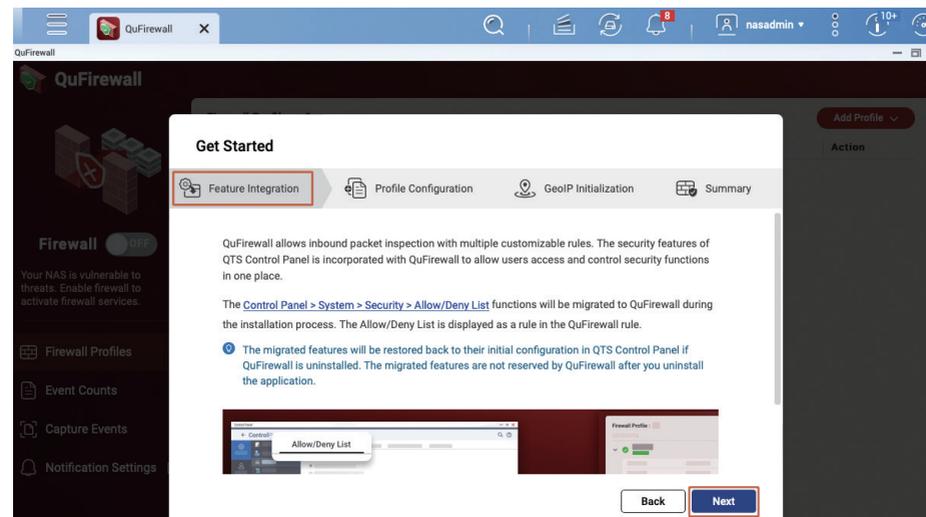


Es wird empfohlen, den "Scan-Zeitplan" auf **einmal pro Tag** einzustellen, damit "Malware Remover" regelmäßig den Systemstatus überprüft. Stellen Sie außerdem sicher, dass die Option "Malware Remover automatisch auf die neueste Version aktualisieren" aktiviert bleibt.

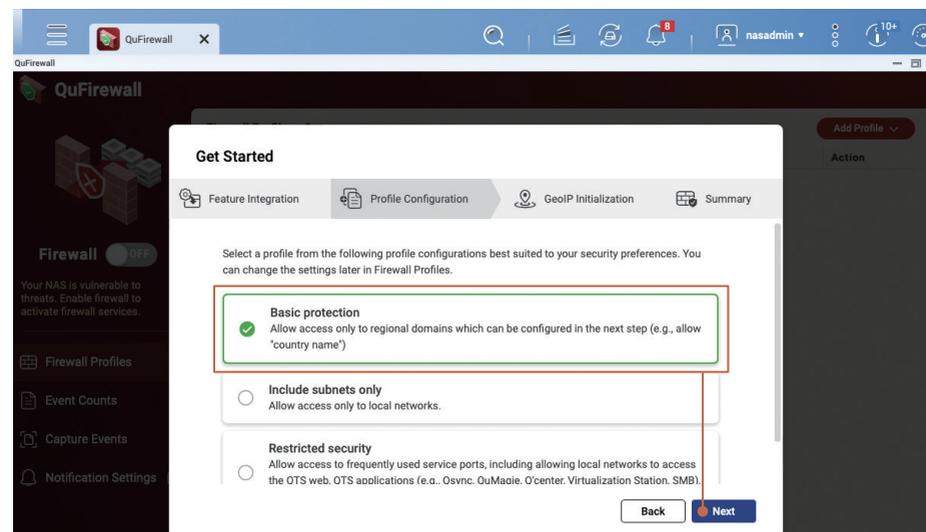


QuFirewall

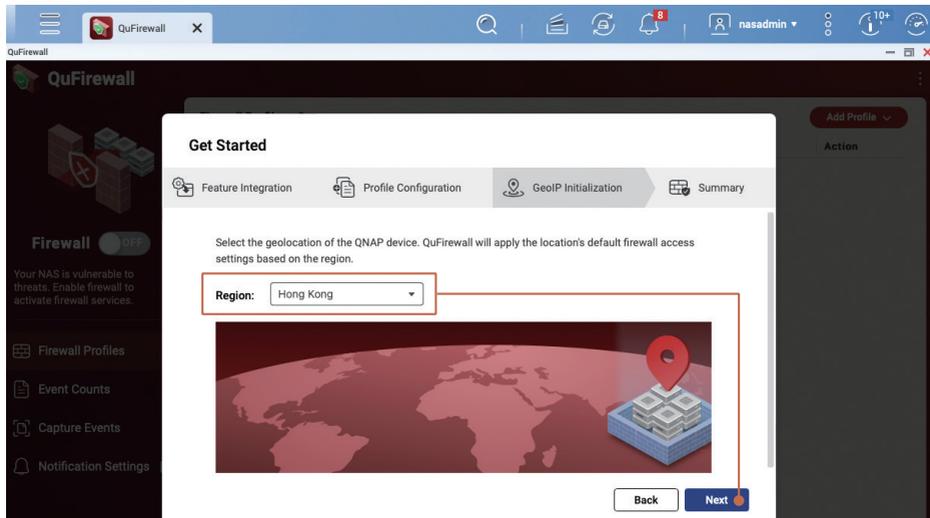
Öffnen Sie "QuFirewall". Wenn Sie QuFirewall zum ersten Mal verwenden, wird der Bildschirm "Erste Schritte" angezeigt. Klicken Sie nach dem Lesen auf "Weiter", um fortzufahren.



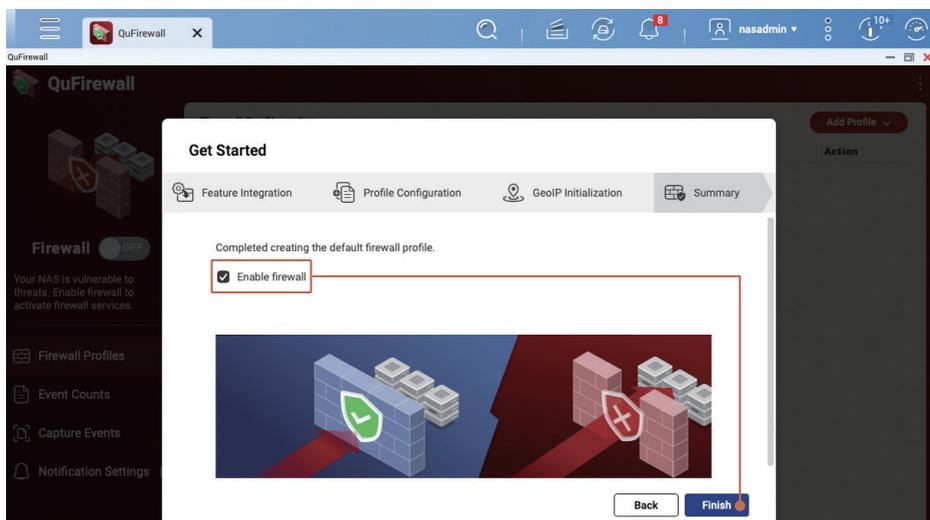
Wenn Ihr Netzwerk keine besonderen Anforderungen stellt, empfiehlt es sich, "Einfacher Schutz" zu wählen und dann auf "Weiter" zu klicken, um fortzufahren.



Legen Sie eine Region entsprechend Ihrem Standort fest. Beispiel: Wenn Sie sich in Taiwan befinden, wählen Sie "Taiwan"; wenn Sie sich in Hongkong befinden, wählen Sie "Hongkong"; wenn Sie sich in Macau befinden, wählen Sie bitte "Macao". Sie können später weitere Regionen hinzufügen. Klicken Sie zum Fortfahren auf "Weiter".

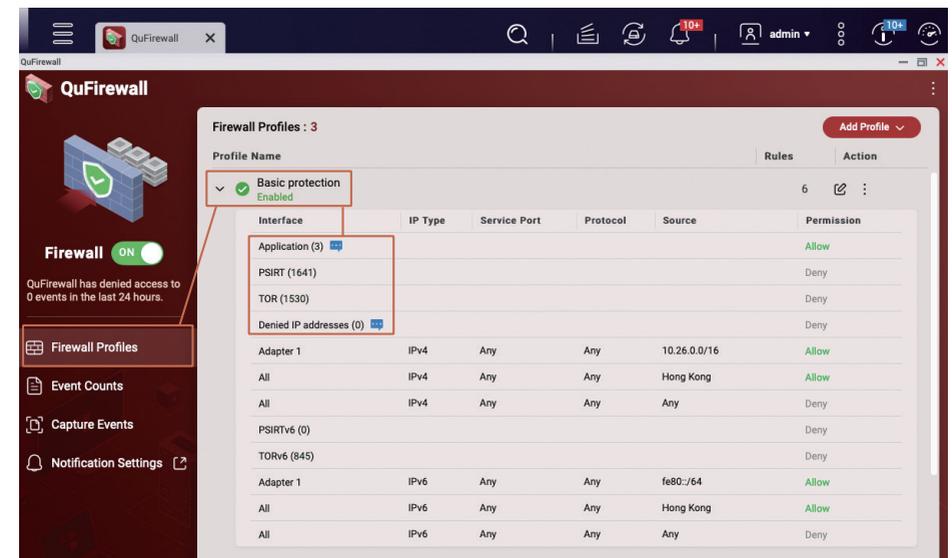


Aktivieren Sie "Firewall aktivieren" und klicken Sie dann auf "Fertigstellen", um die Einstellungen zu übernehmen und die Firewall zu aktivieren.



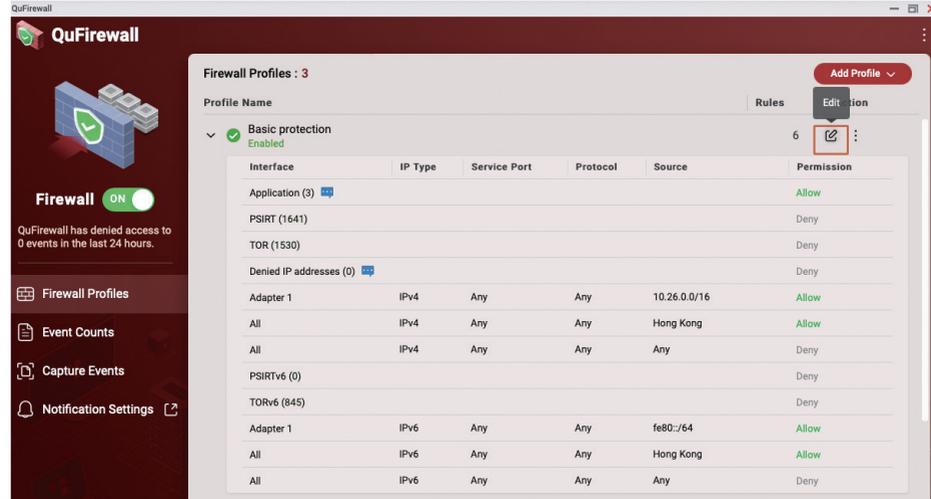
Auf der Seite "QuFirewall-Profil" sehen Sie, dass "Einfacher Schutz" aktiviert ist. Klicken Sie auf "Einfacher Schutz", um die entsprechenden Firewall-Regeln zu erweitern und anzuzeigen. Die Regeln werden mit den Informationen in den eingehenden Paketen abgeglichen, die entsprechend den Firewall-Regeln zugelassen oder blockiert werden. Die Firewall-Regeln werden nacheinander ausgeführt. Wenn die Bedingungen nicht erfüllt sind, wird die nächste Regelzeile geprüft. Wenn sie nicht erfüllt sind, fallen sie unter die letzte "Alle ablehnen"-Regel, und die Firewall blockiert die betreffenden Verbindungen.

- "Anwendung"-Regeln werden vom System erstellt, um das ordnungsgemäße Funktionieren des Systems zu gewährleisten.
- Die "PSIRT"-Regel ist eine von QNAP PSIRT erstellte Blacklist. Sie enthält IP-Adressen, von denen bekannt ist, dass sie das QNAP-NAS angreifen.
- Die "TOR"-Regel wird verwendet, um Verbindungen aus dem TOR-Netzwerk zu blockieren. Das TOR-Netzwerk wird wegen seiner Anonymität häufig von Kriminellen genutzt, und seine Sperrung kann das Risiko eines Angriffs verringern.
- "Abgelehnte IP-Adressen" sind IP-Adressen, die durch die Funktion "IP-Zugriffsschutz" oder die vom Benutzer manuell hinzugefügte Blacklist blockiert werden.

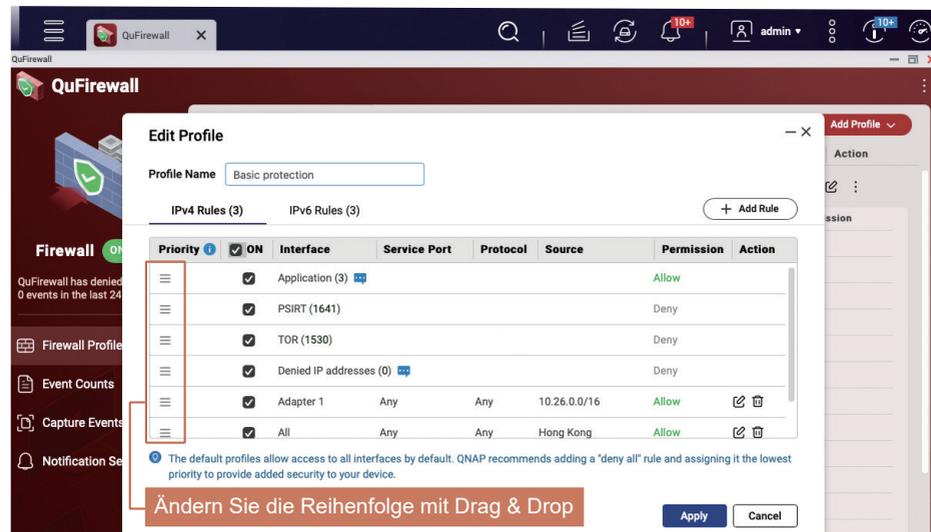


Andere Regeln können vom Benutzer angepasst werden, und unter den grundlegenden Schutzeinstellungen werden nur Internetverbindungen aus demselben Intranet und aus derselben Region "zugelassen". QNAP empfiehlt die Verwendung des Konzepts der "Whitelist" zur Verwaltung Ihrer benutzerdefinierten Regeln, um die IP-Adressen, die sich mit dem NAS verbinden können, streng zu begrenzen.

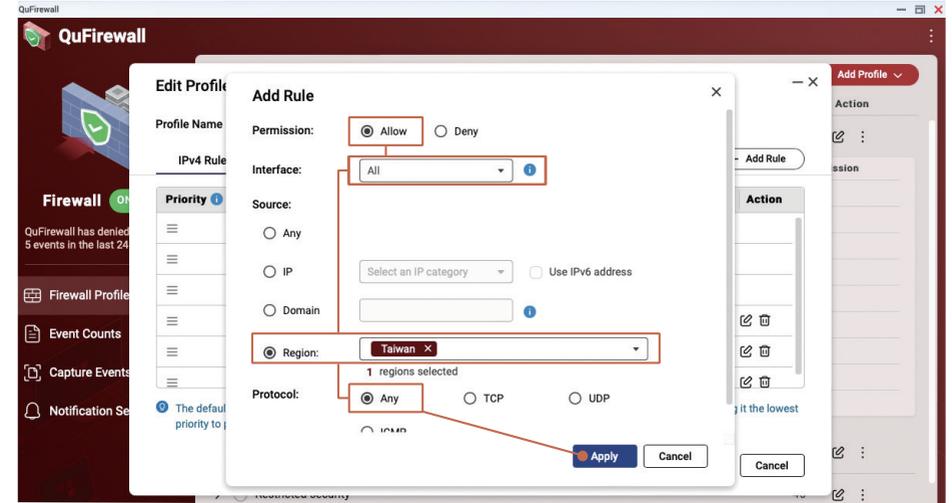
Im Folgenden wird gezeigt, wie Sie Firewall-Regeln bearbeiten können. Klicken Sie auf die Schaltfläche "Bearbeiten", um den Bildschirm "Firewall-Profil" zu bearbeiten.



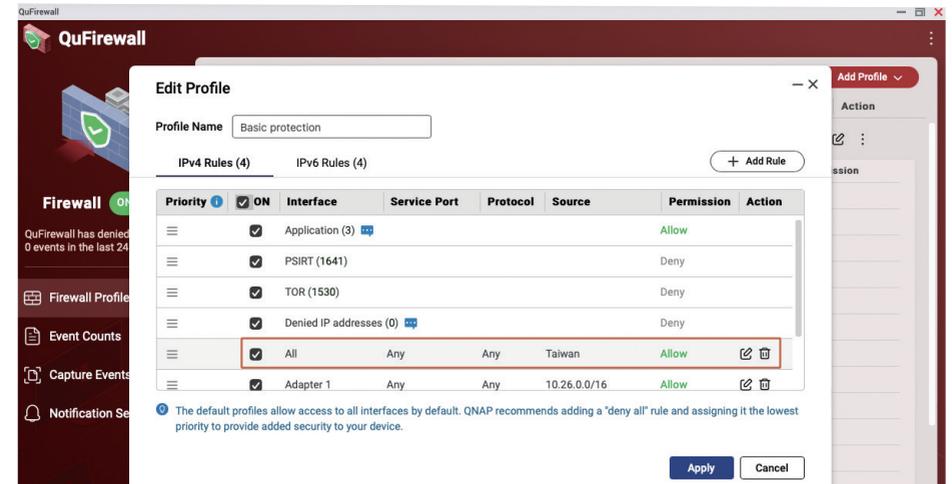
Auf dem Bildschirm "Profil bearbeiten" können Sie die Reihenfolge der Regeln ändern oder neue Regeln hinzufügen. Im folgenden Beispiel wird eine weitere Region hinzugefügt, die eine Verbindung zulässt. Klicken Sie auf "Regel hinzufügen", um den Einstellungsbildschirm aufzurufen.



Um beispielsweise Verbindungen aus Taiwan zuzulassen, muss "Berechtigung" auf "Zulassen" gesetzt werden; "Schnittstelle" auf "Alle"; "Region" für "Quelle". Dann wählen Sie "Taiwan"; "Protokoll" auf "Beliebig", dann klicken Sie auf "Übernehmen", um die Regel hinzuzufügen, wenn Sie fertig sind.



Auf der Seite "Profil bearbeiten" können Sie die neu hinzugefügten Regeln sehen. Falls erforderlich, können Sie die Reihenfolge der Regeln anpassen. Klicken Sie nach dem Bestätigen der Richtigkeit auf "Übernehmen".



Geplante Snapshots aktivieren

Die Snapshot-Funktion kann Ihre wichtigen Daten durch das Erstellen von Wiederherstellungspunkten für mehrere Versionen schützen. Sie können einen Snapshot-Zeitplan auf dem QNAP-NAS einstellen, damit das System automatisch Snapshots gemäß dem Zeitplan als grundlegenden Datenschutz erstellen kann.

- Geplante Snapshots sind standardmäßig für "Volle/Thin-Volumes" aktiviert, die mit QTS 5.0.0 erstellt wurden
- In QTS 5.0.1 (und später) sind nur für "Thin-Volumes" geplante Snapshots standardmäßig aktiviert
- Von QuTS hero h5.0.1 (und höher) erstellte "Freigabeordner" ermöglichen standardmäßig geplante Snapshots

Öffnen Sie "Speicher & Snapshots", klicken Sie links auf "Speicher/Snapshots" und stellen Sie sicher, dass "Speicherplatz" eine "Speicherpool"-Struktur ist und dass der "Speicherpool" über genügend freien Speicherplatz verfügt, damit die Snapshot-Funktion funktioniert. Wenn Ihr Volume-Typ "Volles Volume" ist, können Sie "Volumegröße ändern*" und "In Thin-Volume konvertieren*" in Betracht ziehen, um Speicherplatz im "Speicherpool" für die Snapshot-Funktion freizugeben.

- * Sie müssen Ihre Daten vor dem Konvertieren von Datenträgern sichern, um einen möglichen Datenverlust zu vermeiden.

Storage & Snapshots

Storage Space Storage Pool: 1, Volume: 3, LUN: 0

Name/Alias	Status	Type	Snapshot Re...	Snapshot	Capacity	Percent Used
Storage Pool 1	Ready				5.83 TB	
Data	Ready	Thin volume	--	--	2.97 TB	
System (System)	Ready	Thin volume	--	ts :9	98.20 GB	
Thick	Ready	Thick volume	--	--	494.54 GB	

Thick Management

Name/Alias: Thick

Capacity: 494.54 GB

Free Size: 494.47 GB

Thin: No

SSD cache: --

Status: Ready

Utilization

100 %

75 %

50 %

25 %

Used: 0.01% (72.04 MB) Free Size: 99.99%

Actions

- Remove
- Resize Volume
- Set Threshold
- Set Caching Storage
- Check File System
- Rename Volume Alias
- Format
- Convert to Thin Volume

* Öffnen Sie "Thick-Verwaltung", um entsprechende Anpassungen vorzunehmen, um Speicherplatz im "Speicherpool" freizugeben

Nachdem Sie bestätigt haben, dass im "Speicherpool" auf dem NAS genügend Platz vorhanden ist, klicken Sie zunächst auf "Volume", dann oben auf "Snapshot" und im Menü auf "Snapshot Manager".

Storage & Snapshots

Storage Space Storage Pool: 1, Volume: 2, LUN: 0

Name/Alias	Status	Type	Snapshot Rep...	Snapshot	Cap...
Storage Pool 1	Ready				
Data	Ready	Thin volume	--	--	
System (System)	Ready	Thin volume	--	ts :9	

Snapshot Manager

Wechseln Sie zur Einstellungsseite "Snapshot Manager" von "Volume" und klicken Sie oben rechts auf "Snapshot planen".

Snapshot Manager

Pool Guaranteed Snapshot Space

Schedule Snapshot

Take Snapshot

Daily 01:00

Name (0/0)	Replicated	Capacity	Retention Policy	Taken	Taken By	Status
------------	------------	----------	------------------	-------	----------	--------

Schalten Sie "Zeitplan aktivieren" auf "Aktivieren" und ändern Sie dann den Zeitplan nach Ihren Bedürfnissen. Es wird empfohlen, "Täglich" oder "Wöchentlich" zu verwenden.

Snapshot Settings

Schedule Snapshot

Enable schedule:

Repeat: Daily Time: 01:00 (hh:mm)

Snapshot retention policy: Smart Versioning

The snapshot will be stored in Storage Pool 1 (5.65 TB available).

Enable smart snapshot

Description

Note: The performance of a volume or LUN may be affected after taking a snapshot, due to data structure change.

Note: Snapshots will be automatically recycled when available storage pool space is low. [Change policy.](#)

Sie können eine Snapshot-Aufbewahrungsrichtlinie festlegen, um die Anzahl der Snapshots zu begrenzen und zu verhindern, dass Snapshots zu viel Speicherplatz beanspruchen.

Es wird empfohlen, "Smart Versioning" einzustellen einzustellen, d. h. die Großvater-Vater-Sohn-Regel (GFS), um genügend Versionen zum Schutz der Daten zu erhalten. Klicken Sie nach Abschluss der Einstellungen auf "OK", um die Einstellungen zu übernehmen.

Snapshot Settings

Snapshot Retention

How many Snapshot can I have?

The snapshot retention policy determines how long to keep a snapshot or how many total snapshots to keep. When the specified value is exceeded, the system deletes the expired snapshot or the oldest snapshot automatically.

Maximum amount of time to keep: 0 Months

Maximum number of snapshots to keep: 0 Snapshots

Smart Versioning

Hourly snapshots: 24

Daily snapshots: 7

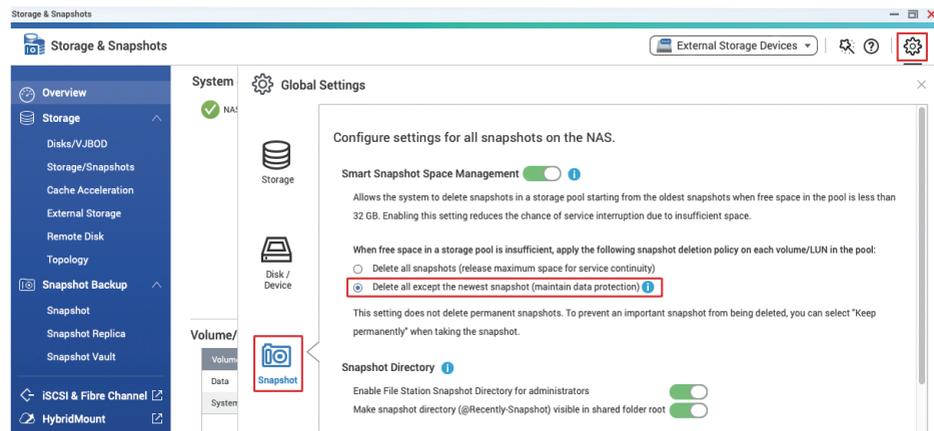
Weekly snapshots: 4

Monthly snapshots: 12

Richtlinie für das Löschen von Snapshots festlegen

Wenn der Speicherpool nicht über genügend Speicherplatz verfügt, löscht das System Snapshots auf der Grundlage Ihrer Einstellungen, um den normalen Systemdienst aufrechtzuerhalten und eine mögliche Unterbrechung des Dienstes aufgrund von Speichermangel zu vermeiden.

Klicken Sie in "Speicher & Snapshots" auf die Schaltfläche "Einstellungen" in der oberen rechten Ecke, öffnen Sie "Globale Einstellungen" und klicken Sie auf "Snapshot". Es wird empfohlen, die Option "Alle außer dem neuesten Snapshot löschen" zu wählen, um zu vermeiden, dass alle Snapshots wiederhergestellt werden und der Schutz verloren geht.

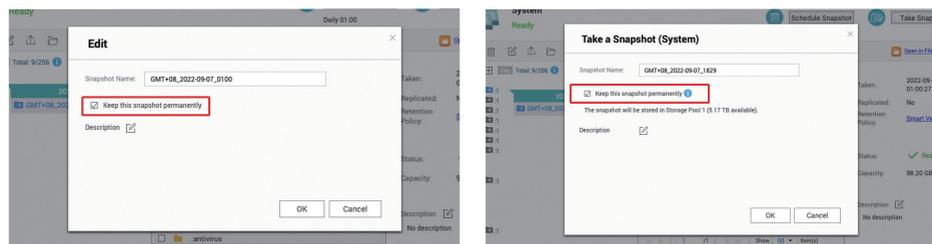


Wenn Sie möchten, dass das System alle Snapshots beibehält, auch wenn der "Speicherpool" nicht genügend Speicherplatz hat, deaktivieren Sie "Intelligente Snapshot-Speicherplatz-Verwaltung". Beachten Sie, dass dies dazu führt, dass der "Speicherpool" in den Zustand "schreibgeschützt/gelöscht" übergeht, wenn der Speicherplatz im "Speicherpool" nicht ausreicht. Sie müssen den Snapshot manuell löschen, um den normalen Betrieb des Speicherpools wiederherzustellen. Überprüfen Sie nach dem Deaktivieren dieser Funktion regelmäßig die Speicherplatznutzung.



Um ein Versagen des Schutzes aufgrund der Richtlinie zum Löschen von Snapshots zu vermeiden, wird empfohlen, alle oder einen Teil der Snapshots auf "Snapshot dauerhaft aufbewahren"* zu setzen, nachdem eine große Datenmenge gespeichert wurde, um zu verhindern, dass die Snapshots vom System wiederverwendet werden.

* Muss manuell gelöscht werden, um Speicherplatz freizugeben. Es wird empfohlen, regelmäßig manuell zu erstellen und zu löschen.



Checkliste NAS-Sicherheitseinstellungen

- Notification Center einrichten**
 - Mindestens eine Benachrichtigungsmethode festlegen
 - Regeln für "Alarmbenachrichtigungen" erstellen
 - Regeln für die "Firmware-Update"-Benachrichtigung erstellen
- Automatisches Firmware-Update aktivieren (QTS/QuTS hero)**
- App Center konfigurieren**
 - Alle Apps auf die neueste Version aktualisieren
 - Installation von Anwendungen ohne gültige digitale Signatur untersagen
 - Automatische Updates aktivieren
- Unnötige Funktionen deaktivieren oder entfernen**
 - Überprüfen, ob aktivierte Dienste erforderlich sind
 - Überprüfen, ob aktivierte App Center-Apps erforderlich sind
 - SSH deaktivieren**
 - Telnet deaktivieren**
- Sicherheit von Systemkonten stärken**
 - Standard-Konto "admin" deaktivieren
 - Passwortrichtlinie festlegen
 - IP-Zugriffsschutz aktivieren
 - Zwei-Schritt-Verifizierung (2SV) aktivieren
- Standard-Systemport ändern**
- Zugriffsprotokoll aktivieren**
- Sicherheits-Apps installieren und aktivieren**
 - Security Counselor**
 - Geplanten Scan starten
 - Malware Remover**
 - Geplanten Scan starten
- QuFirewall**
 - Firewall aktivieren
 - Geo-IP-Region** festlegen
 - PSIRT-Regeln** aktivieren
 - TOR-Regeln** aktivieren
- Geplante Snapshots aktivieren**
 - "Snapshot dauerhaft aufbewahren" regelmäßig festlegen

Q Ist es sicherer, die Verbindung des NAS zum Internet zu trennen?

A Nein. Das "Trennen" eines NAS bezieht sich im Allgemeinen auf die Trennung des NAS vom Netzwerk, sodass es keine Verbindungen zur Außenwelt herstellen kann. Obwohl einige Malware-Programme eine externe Verbindung benötigen, um ausgeführt werden zu können, gibt es auch Malware-Programme, die ohne eine externe Verbindung erfolgreich bössartige Aktionen durchführen können. Dadurch wird nicht nur verhindert, dass Hacker illegale Aktionen durchführen, sondern auch, dass einige Systemfunktionen wie automatische Software-Updates und Benachrichtigungen ordnungsgemäß funktionieren. Der richtige Ansatz besteht darin, den Datenverkehr zum NAS einzuschränken, z. B. die Verbindung zum Internet zu vermeiden, um die Sicherheit zu verbessern.

Q Meine Festplatte ist mit RAID konfiguriert. Bedeutet das, dass ich keine Sicherung benötige?

A Nein. RAID ist keine Sicherungsmethode. RAID-Level über 0 sind nur dazu gedacht, Redundanz gegen Datenträgerfehler zu bieten. RAID bietet keinen Schutz vor Datenlöschung oder Verschlüsselung. Es wird daher empfohlen, [die Daten nach dem 3-2-1-Sicherungsprinzip](#) ordnungsgemäß zu sichern.

Q Ich habe "Snapshots" bereits eingerichtet. Bedeutet das, dass ich keine Sicherung benötige?

A Nein. Da "Snapshots" auf demselben Datenträgersatz wie Ihre Daten gespeichert werden, gehen die Daten auch bei einem RAID-Ausfall verloren. Darüber hinaus kann der "Snapshot" auch gelöscht werden, wenn sich Hacker ausreichende Berechtigungen verschaffen können (z. B. durch erfolgreiches Knacken des Administratorkontos). Es wird daher empfohlen, die Snapshot-Dateien nach dem 3-2-1-Sicherungsprinzip zu sichern.

Q Mein NAS ist nicht mit dem Internet verbunden. Heißt das, dass es unmöglich ist, angegriffen zu werden?

A Nein. Obwohl die meisten Cyberangriffe aus dem Internet kommen, ist der NAS immer noch dem Risiko ausgesetzt, im Intranet angegriffen zu werden. Wenn beispielsweise ein anderer Computer oder ein Gerät in Ihrem Intranet gehackt oder von Malware befallen wird, kann diese dazu verwendet werden, andere Geräte im Intranet anzugreifen und zu infizieren. Die Installation von Antiviren-Software und der Einsatz von Netzwerksicherheitsprodukten auf Ihrem Computer können Ihnen helfen, mit den damit verbundenen Bedrohungen umzugehen. QNAP ADRA NDR kann beispielsweise verdächtige Intranet-Aktivitäten erkennen und automatisch isolieren. Es wird daher auch empfohlen, die Daten nach dem 3-2-1-Sicherungsprinzip ordnungsgemäß zu sichern.

Q Mein NAS ist schon lange in Gebrauch. Wie kann ich überprüfen, ob Malware installiert ist?

A Wenn Sie bemerken, dass die Prozessorlast ungewöhnlich hoch ist, Softwareaktualisierungen fehlschlagen oder unbekannte Anwendungen im App Center angezeigt werden, ist es möglich, dass ein bössartiges Programm installiert wurde. Es wird empfohlen, die neueste Version von Malware Remover zu installieren und zu verwenden. Wenn Sie das Problem immer noch nicht lösen können, wenden Sie sich bitte an das technische Supportteam von QNAP.

Q Was sollte ich tun, um die Sicherheit zu gewährleisten, wenn ich einige Dienste für das Internet öffnen muss?

A Stellen Sie sicher, dass auf dem NAS die neueste Version der Firmware und der Anwendungen installiert ist. Sie können QuFirewall aktivieren, um einen grundlegenden Firewall-Schutz zu bieten, und die Regeln "PSIRT" und "TOR" können Ihnen helfen, einige Hacker-Verbindungen zu blockieren. Wenn Sie ein Geschäfts- oder Unternehmensnutzer sind, wird empfohlen, eine höherwertige Firewall-Lösung zu verwenden. Wenn der Speicherplatz im Pool es zulässt, können Sie darüber hinaus "Snapshots" zur grundlegenden Datensicherung erstellen. Es wird auch empfohlen, die Daten nach dem 3-2-1-Sicherungsprinzip zu sichern, um für den schlimmsten Fall gerüstet zu sein und einen möglichen Datenverlust zu verhindern.

Q Mein NAS ist alt und unterstützt nicht die neueste Version von QTS. Kann es trotzdem sicher verwendet werden?

A Legacy- und End of Life (EOL)-Modelle werden nur begrenzt unterstützt und sollten nur für Intranet/Offline-Sicherungen verwendet werden.

Q Warum erhalte ich ständig die Warnung, dass die NAS-Anmeldung fehlgeschlagen ist?

A Wenn die IP-Adresse der fehlgeschlagenen Anmeldung aus dem Internet stammt, bedeutet dies, dass Ihr NAS einem Brute-Force-Angriff zum Knacken des Passworts ausgesetzt ist. Sie sollten es vermeiden, Ihr NAS dem Internet auszusetzen, und diese Anleitung befolgen, um Ihr NAS zu stärken. Wenn die IP-Adresse der fehlgeschlagenen Anmeldung aus dem Intranet stammt, überprüfen Sie bitte, ob auf dem Gerät mit dieser IP-Adresse Malware installiert ist.

Q Warum haben alle meine Dateien seltsame Dateinamen?

A Dies ist ein Symptom für eine Ransomware-Infektion. Überprüfen Sie die NAS-Zugriffsprotokolle, um festzustellen, ob die Verschlüsselungsaktion von einem anderen Computer oder dem NAS selbst ausgeht. Wenn Ihr NAS von Ransomware betroffen ist, sollten Sie geeignete Maßnahmen ergreifen, um die Ausbreitung der Infektion zu stoppen. Wenden Sie sich bei Bedarf an den technischen Support von QNAP, um Unterstützung zu erhalten.

Q Was sollte ich tun, wenn mein NAS mit Ransomware infiziert ist?

A Die meisten Ransomware-Programme verwenden unknackbare Verschlüsselungsmethoden. Wenn es keinen richtigen Schlüssel gibt, können die Dateien nicht entsperrt werden, sodass sie nur durch eine Sicherung oder einen Snapshot wiederhergestellt werden können.

Ändern Sie die Router-Einstellungen gemäß dieser Anleitung sofort, um zu verhindern, dass das NAS dem Internet ausgesetzt wird, und um sekundäre Angriffe zu verhindern. Zweitens sollten Sie sofort alle Synchronisierungsaufgaben aussetzen und Snapshots als dauerhaft aufbewahrbar einstellen, um den Verlust von Sicherungsdateien zu vermeiden. Wenn Ihre Daten über Sicherungen oder Snapshots verfügen, die Sie wiederherstellen können, können Sie die Dateien nach der Aktualisierung der NAS-Firmware und -Anwendungen und nach Abschluss des Malware Remover-Scans wiederherstellen. Wenn die Daten nicht gesichert sind, sichern Sie bitte die von der Ransomware hinterlassene Lösegeldforderung und die Methode zur Zahlung des Lösegelds und versuchen Sie dann, mit Methoden wie der Datenwiederherstellung einige Daten wiederherzustellen. Wenden Sie sich bei Bedarf an den technischen Support von QNAP, um Unterstützung zu erhalten.

Q In den Medien wird immer wieder über die Behebung von Sicherheitslücken bei QNAP-Produkten berichtet. Bedeutet dies, dass QNAP-Produkte nicht sicher sind?

A Es gibt keine perfekte Software und Hardware auf der Welt. Unabhängig davon, ob es sich um proprietäre Software verschiedener Hersteller oder um Open-Source-Software oder sogar um Hardware handelt, werden immer wieder Schwachstellen gefunden, die dann von den Herstellern behoben werden. Wie andere große Technologieunternehmen patcht auch QNAP ständig bekannte Sicherheitslücken und veröffentlicht dann so schnell wie möglich Aktualisierungsdateien für die Benutzer, um die Sicherheit der Geräte und Daten der Benutzer zu gewährleisten. QNAP PSIRT gibt auch Cybersicherheits-Benachrichtigungen für die externe Offenlegung aus, sodass die Benutzer auf auftretende Probleme reagieren können. QNAP ist davon überzeugt, dass ein offener und transparenter Umgang mit Schwachstellen das Recht der Benutzer auf Information schützt und zur Verbesserung der Produktsicherheit beiträgt. Benutzer sind außerdem eingeladen, die QNAP-Sicherheitshinweise zu abonnieren, um relevante, genaue und vollständige Informationen zu erhalten, bevor die Medien darüber berichten.



QNAP-Sicherheitshinweise:

<https://www.qnap.com/go/security-advisories/>

Q Was ist das 3-2-1-Sicherungsprinzip?

A Das 3-2-1-Sicherungsprinzip ist ein bekanntes Sicherungsprinzip in der IT-Branche. Es bereitet auf den schlimmsten Fall vor. Es stellt sicher, dass im Falle einer Katastrophe Sicherungsdateien zur Wiederherstellung der Daten vorhanden sind, um Verluste zu vermeiden und Sicherheit zu gewährleisten.

"3" in 3-2-1-Sicherung bedeutet mindestens drei Sicherungskopien, "2" bedeutet mindestens zwei Speichermedien, und "1" bedeutet, dass mindestens eine Kopie eine Offsite-Sicherung ist.

Auf der Grundlage des 3-2-1-Sicherungsprinzips gibt es Sicherungsdateien, die unabhängig von versehentlichen Änderungen, Löschungen, Hardwareschäden, Virenbefall und Katastrophen wie Bränden und Überschwemmungen wiederhergestellt werden können.

Um diesem Prinzip gerecht zu werden, umfasst das QNAP-NAS Hybrid Backup Sync 3 (HBS3), Snapshot Replica und SnapSync (nur von QuTS hero unterstützt) zur Sicherung von Daten auf dem NAS auf einem externen NAS, einer öffentlichen Cloud, einem externen Speicher, anderen Dateiservern und/oder anderen Geräten, um sicherzustellen, dass nichts verloren geht.

Tutorials zu Hybrid Backup Sync 3 (HBS3):

<https://www.qnap.com/go/how-to/tutorial/article/hybridbackup-sync>



Snapshot Replica-verwandte Tutorials:

<https://www.qnap.com/go/how-to/tutorial/article/savesnapshots-to-other-qnap-nas-with-snapshot-replica>



SnapSync-Tutorials:

<https://www.qnap.com/go/how-to/tutorial/article/bestpractices-for-the-configuration-of-realtime-snapsync>



Um die Sicherheit zu erhöhen, können Sie Offline-Sicherungen oder Sicherungen auf dem WORM-Speicherplatz (Write Once Read Many) von QuTS hero hinzufügen, um Daten vor Manipulationen zu schützen.

MEMO



2 0 2 3

Sicherheitshandbuch

QNAP



QNAP SYSTEMS, INC.

TEL: +886-2-2641-2000 FAX: +886-2-2641-0555 E-Mail: qnapsales@qnap.com

Adresse: 3F, No.22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221, Taiwan

QNAP kann technische Daten und Produktbeschreibungen jederzeit ohne Ankündigung ändern.

Copyright © 2023 QNAP Systems, Inc. Alle Rechte vorbehalten.

QNAP® und Namen von QNAP-Produkten sind Marken oder eingetragene Marken der QNAP Systems, Inc. Andere hierin erwähnte Produkte und Firmennamen sind die Marken ihrer jeweiligen Inhaber.