


Säkerhetsguide


Vägledning i hur du håller din NAS skyddad

Grunderna i säkerhet – det allra viktigaste

Första uppstart av din NAS



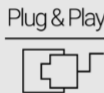
Admin-konto
Använd inte förvalda inställningar!
Skapa ett nytt admin-konto



Lösenord
Använd säkra lösenord




2-faktorautentisering
Stärker skyddet för alla konton




UPnP
Stäng av Universal Plug and Play för att skydda din enhet

Dagliga/återkommande aktiviteter




Backup
Backa upp till fler än ett ställe!
Bruka 3-2-1-strategin för backup



Snapshots
Skapa snapshots löpande




Uppdateringar
Håll systemet automatiskt uppdaterat




VPN
Anslut säkert över Internet med VPN

Engångsinställningar som skyddar permanent



QuFirewall
Ladda hem från App Center och aktivera



Security Counselor
Ladda hem från App Center och aktivera

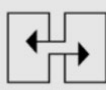
Mer avancerade inställningar

För avancerade användare



Portar

Ändra standardportarna



Kryptering

Använd krypterade anslutningar (HTTPS)

Inledning

Säkerhetsguide

I denna guide finner du nyttiga förklaringar till vilka inställningar du kan nyttja och ändra för att på bästa sätt säkra din data. Värt att ha i åtanke är att ökad säkerhet även ökar komplexiteten i åtkomsten – vilken nivå du lägger dig på måste du välja själv.

Denna guide är en sammanfattning över de viktigaste ämnena inom säkerhet, mer detaljerad information finner du på <https://www.qnap.com/>

Vad är ransomware?

Ransomware är skadlig kod som låser dig ute från ett visst system. Filerna krypteras, och du som användare bes betala en lösesumma i utbyte mot återställd åtkomst till dina filer.

Hur kan du skydda dig mot ransomware?

Ransomware är ett ständigt ökande hot mot både företags- och hemanvändare som använder nätverksanslutna enheter. Cyberkriminella letar ständigt efter nya sätt att distribuera skadlig kod, och den vanligaste attackmetoden är via e-post som sänds ut under falsk flagg.

QNAP är medvetet om denna ökande hotbild och arbetar ständigt för att erbjuda bästa möjliga skydd mot ransomware. Följande exempel är till för att visa hur du bäst kan skydda din data i situationer i scenarion som passar dina behov bäst.

Vid första uppstart

Administratörskonto

Användarkontot för en administratör i QTS är "admin" i grundutförandet. För bästa möjliga säkerhet är ett generiskt, lättgissat användarnamn med full tillgång till systemet inte att rekommendera. Genom att lämna användarnamnet "admin" behöver angripare endast gissa rätt lösenord för fullständig access. För att skydda din data från detta rekommenderar vi att ett administratörskonto med annat namn skapas och "admin" avaktiveras.

Admin-kontot bör därefter endast användas för faktiskt administration, likt uppdateringar och hantering av enheten. För dagligt användande rekommenderas ett separat användarkonto med färre privilegier.

OBS: Avaktivering av "admin"-kontot är möjligt i QTS 4.1.2 och senare.



**SKAPA NYTT
ADMIN-KONTO**



**AVAKTIVERA
KONTOT "ADMIN"**

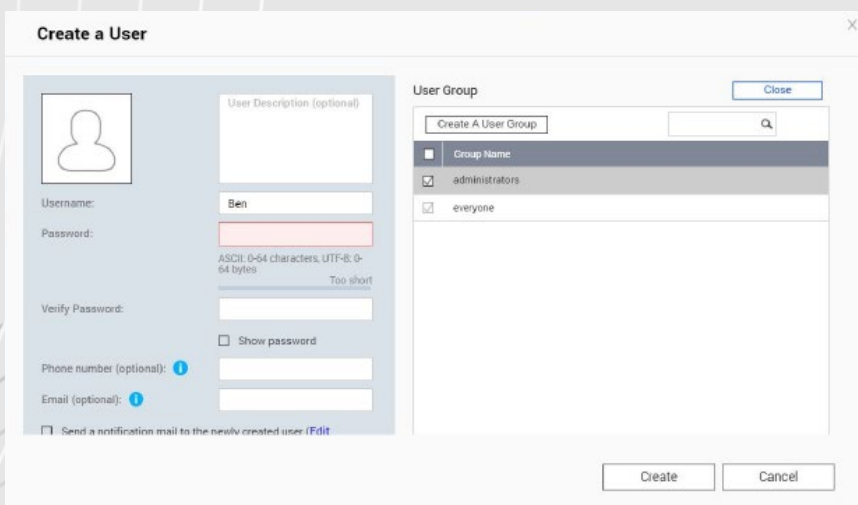


**ANVÄND ADMIN-KONTO
ENBART FÖR
ADMINISTRATION**

Vid första uppstart

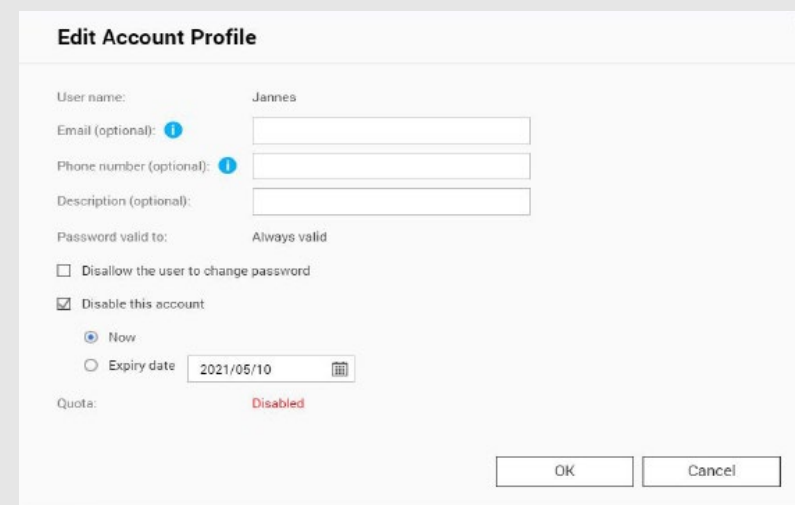
Hur du avaktiverar "admin"-kontot

När det kommer till din NAS från QNAP finns det några enkla saker du kan göra för att drastiskt förbättra säkerheten. Det kanske viktigaste är att skapa ett nytt användarkonto med administratörsrättigheter med ett annat namn än "admin". Det gör du på följande vis:



Skapa ett nytt administratörskonto

1. Logga in i operativsystemet QTS med "admin"-kontot
2. Gå till Control Panel > Users
3. Skapa en ny användare (i detta exempel "Ben") och placera honom i användargruppen "administrators"



Avaktivera kontot "admin"

1. Logga in i QTS med ditt nya konto
2. Gå till Control Panel > Users och redigera kontot "admin"
3. Klicka "Disable this account" och tryck därefter "OK"

Vid första uppstart

Lösenordsregler

När det gäller lösenord finns det några saker att tänka på när det kommer till säkerhet. Om du är ensam användare av din NAS från QNAP är du givetvis fri att välja typen av lösenord efter tycke och smak, men ökad komplexitet ökar svårigheten att gissa det för utomstående.

Följande grundläggande saker är bra att ha i åtanke när du väljer lösenord:



Tillräcklig längd



Specialtecken



Gemener och versaler



**Unika lösenord för alla
enheter och konton**



Byt lösenord regelbundet

Om du nyttjar din NAS från QNAP tillsammans med andra användare bör du som administratör sätta upp regler för lösenord och tvinga dessa i enheten. Det betyder att alla måste följa de regler du sätter – läs mer på nästa sida.

Vid första uppstart

Lösenordsregler

1. Gå till Control Panel > System > Security > Password Policy
2. Under "Password strength", välj från följande regler:
 1. Lösenord måste innehålla något av följande av följande tre typer: Både gemener och versaler, siffror eller specialtecken.
 2. Inga tecken får upprepas tre gånger eller fler i rad (t.ex. "AAA")
 3. Lösenordet får inte vara detsamma som användarnamnet eller användarnamnet baklänges
3. Under "Change Password", välj "Require users to change passwords periodically" för att tvinga regelbundna uppdateringar av lösenord

Detta inaktiverar möjligheten att förbjuda användare från att byta sina lösenord

 1. Ange antal dagar ett lösenord är giltigt
 2. Valfritt: Skicka mail till användare en vecka innan lösenord löper ut
4. Klicka "Verkställ"

The screenshot shows the QNAP Control Panel interface. The left sidebar contains a navigation menu with categories: System, Privilege, Network & File Services, and Applications. The main content area is titled "ControlPanel" and shows the "Password Policy" settings. The "Password Policy" tab is selected, and the "Includes the following characters:" section is expanded. The settings are as follows:

- English letters: No restrictions
- Digits
- Special characters
- Must not include characters repeated three or more times consecutively
- Must not be the same as the associated username, or the username reversed
- Minimum length: 8

The "Change Password" section is also expanded, showing the following settings:

- Require users to change passwords periodically
- Maximum password age (days): 90
- Send a notification email to users one week before their password expires

A note at the bottom states: "Note: Enabling 'Require users to change passwords periodically' will disable 'Disallow the user to change password'". An "Apply" button is visible at the bottom right of the settings area.

Vid första uppstart

2-faktorautentisering

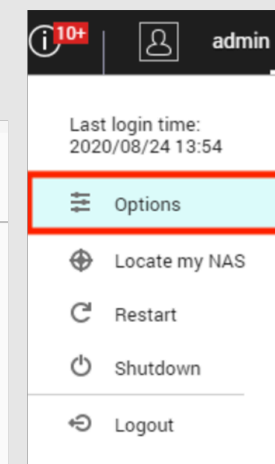
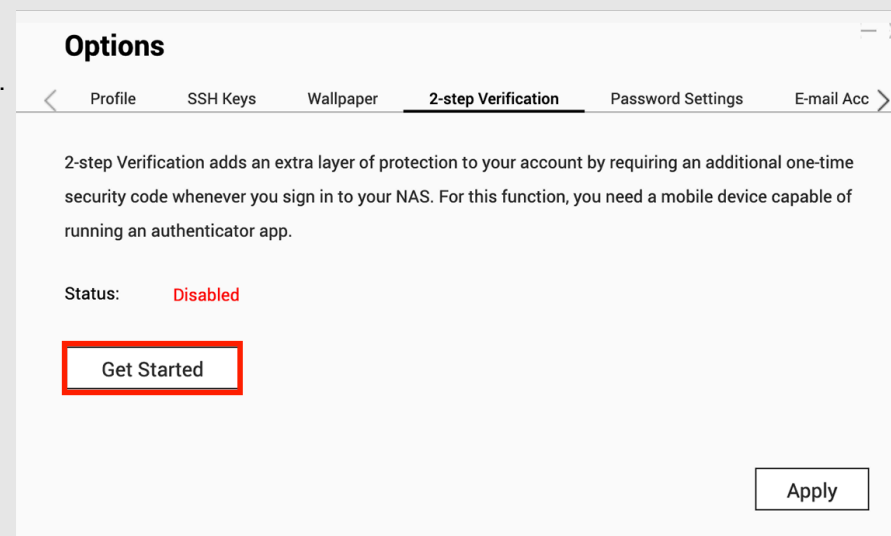
Du kan förbättra säkerheten med 2-faktorautentisering. När det aktiveras kommer du behöva mata in en engångskod (6 tecken) utöver ditt lösenord när du loggar in. För att 2-faktorautentisering krävs en autentiseringsapp med stöd för protokollet Time-based One-Time Password (TOTP), till exempel Google Authenticator eller Authenticator (Microsoft).

För att aktivera funktionen, följ nedanstående steg:

1. Installera en autentiseringsapp på din mobila enhet
 2. I din NAS, gå till "Options" > "2-step verification" och klicka "Get Started"
 1. Synkronisera enheterna genom att skanna QR-koden med din autentiseringsapp eller genom att mata in Secret Key
 2. Mata in koden som genereras i din NAS för att verifiera inställningarna
 3. Välj en backup-metod så som att skicka koder via SMS eller genom att svara på en säkerhetsfråga om du inte kan använda din mobila enhet
- E-post är endast tillgängligt om en SMTP-server är korrekt konfigurerad under "Kontrollpanel" > "Notifikationer" > Epost

En fullständig, detaljerad guide på engelska finns på vår hemsida:

<https://www.qnap.com/en/how-to/tutorial/article/how-to-enhance-account-security-using-2-step-verification>



Vid första uppstart

Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) används för att kontrollera enheter (t.ex. ljudenheter, routrar, skrivare, smart-TV) från olika tillverkare. Det medger för enheter på samma nätverk att förstå varandra och köra vissa automatiska funktioner utan användarens inblandning. UPnP kan i detta fall användas för att låta din QNAP NAS släppa igenom en viss typ av trafik – vi rekommenderar endast avancerade användare att ha denna funktion aktiverad. För standardanvändaren rekommenderas avaktivering av UPnP i både din router och NAS-enhet. Konsultera din routertillverkare om hur du avaktiverar funktionen och se nedan för hur du gör på din QNAP NAS.

OBS!

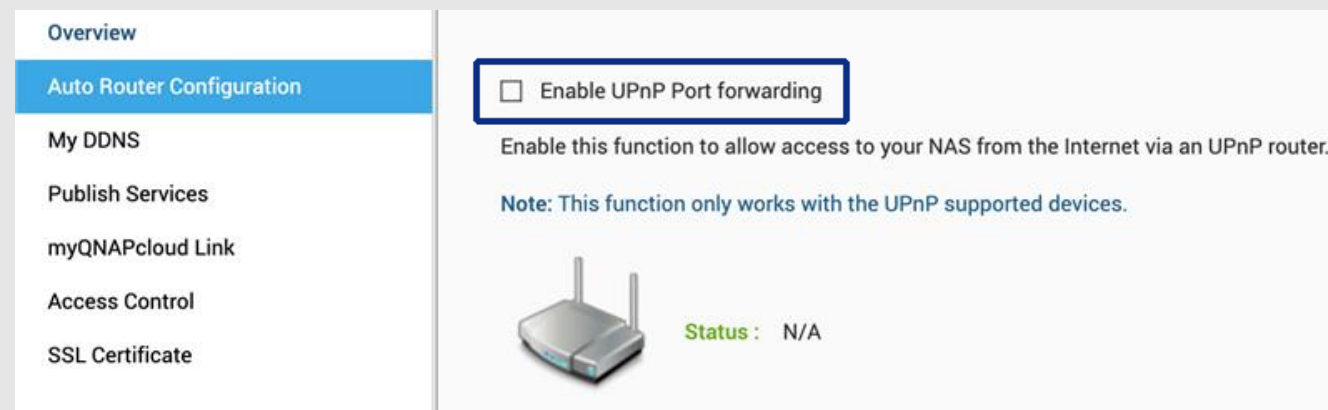
Om UPnP är aktiverat i din router kan mjukvara och enheter på ditt nätverk konfigurera routern efter eget tycke och smak.

Det innebär att de kan öppna portar i din brandvägg, vilket exponerar ditt nätverk till attacker från Internet.

Anslut inte din NAS till Internet från ett modem. Vi rekommenderar starkt att ha din NAS bakom en router.

Avaktivera UPnP forwarding på din QNAP NAS

1. Gå till myQNAPcloud > Auto Router Configuration
2. Avaktivera "Enable UPnP Port forwarding" och välj "verkställ"



Overview

Auto Router Configuration

My DDNS

Publish Services

myQNAPcloud Link


Access Control

SSL Certificate

Enable UPnP Port forwarding

Enable this function to allow access to your NAS from the Internet via an UPnP router.

Note: This function only works with the UPnP supported devices.

 Status: N/A

Dagliga/återkommande aktiviteter

3-2-1-strategi för backup

Backup

Var, hur och hur ofta du backar upp din data är upp till dig. Du bör alltid väga behovet av säkerhet, vikten av ditt data och möjligheterna du har att lagra dem.

Det finns däremot en tumregel för hur du säkert och tillförlitligt backar upp viktig data.

OBS! RAID är inte backup, det skyddar endast dig mot havererade hårddiskar. Snapshots skyddar dig mot ransomwareattacker från din lokala dator.

Backup-strategin 3-2-1

Även om du gör allt för att hålla skadlig kod borta från din NAS bör du alltid backa upp din data utfall det värsta händer.

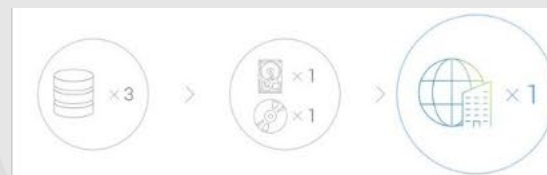
Med 3-2-1-strategin får du en robust grund att bygga vidare på. Ha 3 kopior av viktiga filer, lagra dem på minst 2 typer av lagringsmedia och ha 1 kopia *off-site*, alltså på en säker plats.

Viktig data bör backas upp i minst **3 exemplar**

3 kopior: 1 originalfil och 2 backup-filer



Filerna bör sparas på **2 olika** typer av media för ytterligare ett lager av säkerhet



Slutligen bör **1** backup sparas på annan fysisk plats (utanför kontor eller hem)



Dagliga/återkommande aktiviteter

Snapshots

Vad är snapshots?

Snapshots är avbildningsfiler av data du lagrat på din QNAP NAS. Första gången du tar en snapshot avbildas all data du lagrat. Efterföljande snapshots noterar sedan endast ändringar som skett sedan föregående avbildning. Snapshots är blockbaserade och är således platsbesparande.

OBS!

Snapshots är inte backuper. De gör det möjligt att rulla tillbaka till tidigare filversioner om de av misstag raderas eller ändras.

Se detaljerad genomgång (engelska) av snapshots på vår hemsida: <https://www.qnap.com/solution/snapshots/en-us/>

Konfigurera snapshots

The screenshot shows the configuration interface for snapshots and RAID groups. It is divided into two main sections: a highlighted 'Snapshot' section and a 'RAID Group' section.

Snapshot Section (highlighted with a green border and shield icon):

- Snapshot:** Represented by a star and a camera icon.
- Volume/LUN:** Represented by a star and icons for Volume and LUN. Below the icons, it says "Volume (Thick /Thin) / LUN (Block-based)".
- Storage Pool:** Represented by a star and three RAID Group icons.

RAID Group Section (grey border):

- Volume (Static) LUN (File-based):** Represented by a star and two icons (a cube and a cylinder).
- RAID Group:** Represented by a star and one RAID Group icon.

Dagliga/återkommande aktiviteter

Automatiska uppdateringar

Uppdateringar

Uppdaterad mjukvara är viktigt för din NAS-enhet. QNAP arbetar ständigt med att täppa till nya säkerhetshål som upptäcks och lägger dessutom emellanåt till nya funktioner i systemet.

Uppdateringar bör därför alltid installeras snarast möjligt för bästa möjliga skydd för dina filer.

Om din QNAP-NAS är uppkopplad och du inte har ändrat några inställningar kommer du notifieras när uppdateringar finns tillgängliga – du bör uppdatera snarast möjligt.

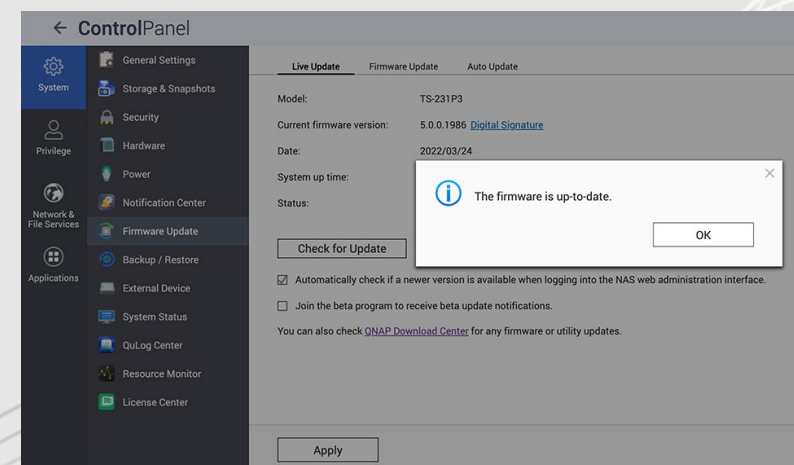
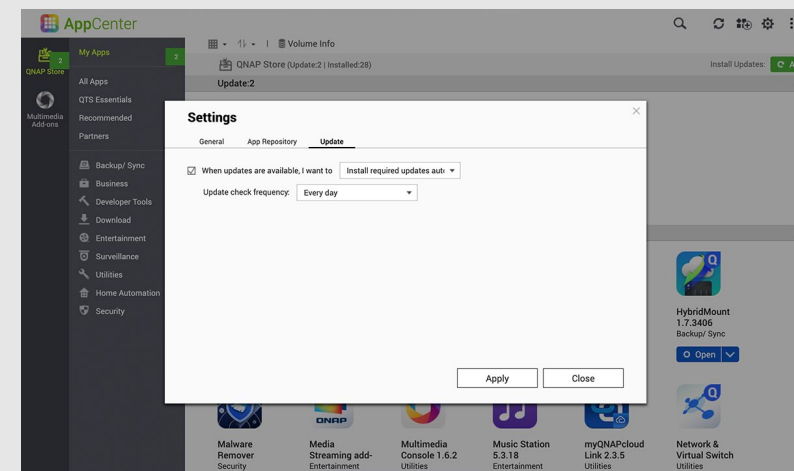
Uppdateringen kräver en omstart och gör enheten otillgänglig i 5–10 minuter. Du har också möjligheten att manuellt uppdatera mjukvaran om din enhet inte är uppkopplad. Om du vill se om ditt system är uppdaterat, gör följande:

Systemuppdatering

1. Logga in med administratörsbehörigheter
2. Gå till Control Panel > Firmware Update
3. Öppna Live Update
4. Klicka "Check for update"

Uppdatera appar automatiskt

1. Gå till App Center
2. Gå till Settings
3. Öppna "Update"
4. Välj "When updates are available..."
5. Välj "Install all updates automatically"



Dagliga/återkommande aktiviteter

VPN

Vad är VPN?

VPN står för Virtual Private Network – ett virtuellt privat nätverk. I detta fall används VPN för att säkert ansluta till din QNAP-NAS från ett externt nätverk. En VPN-server körs på QNAP-enheten och VPN-mjukvara körs på enheten som används på distans och en tunnel ansluter dessa två över Internet.

Fördelen är att anslutningen skyddas med autentisering och kryptering och endast kan användas av behöriga användare. Användarupplevelsen är precis som du och enheten var på samma nätverk.

Efter att en VPN-anslutning konfigurerats kan den användas om och om igen. Vi rekommenderar att alltid ansluta till din QNAP-enhet över VPN när du befinner dig på ett externt nätverk för maximal säkerhet.

Att konfigurera VPN

En detaljerad genomgång av konfigurationen finns på vår hemsida (engelska):

<https://www.qnap.com/en/how-to/tutorial/article/how-to-set-up-and-use-qvpn>

Rekommenderad mjukvara för fjärråtkomst

myQNAPcloud Link & VPN (Port Forwarding VPN krävs, QuFirewall rekommenderas för bästa skydd)



Engångsinställningar

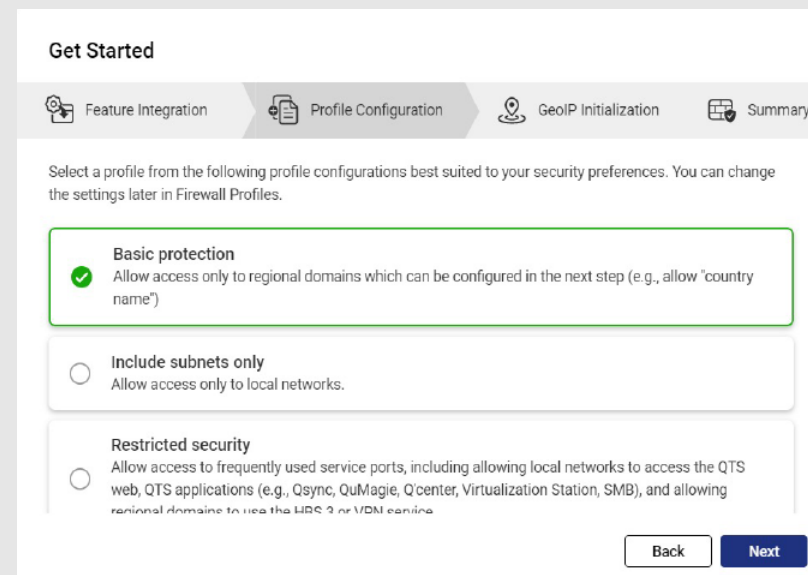
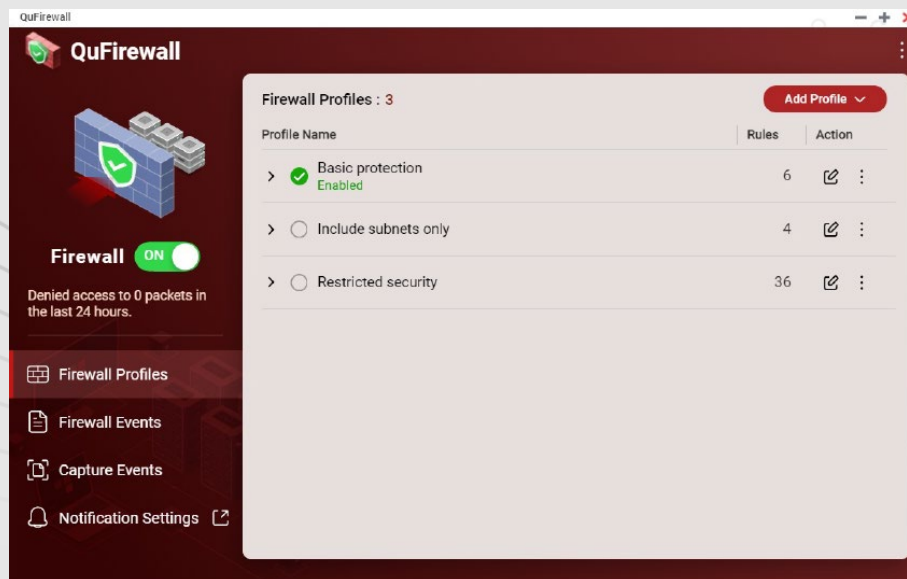
QuFirewall

Vad är QuFirewall?

QuFirewall är en mjukvara för hantering av brandväggar i din QNAP-enhet. Med kraftfulla och lättanvända profiler kan du med appen kontrollera och verifiera anslutningar till din enhet. Vi rekommenderar att du installerar QuFirewall på din QNAP-NAS och begränsar IP-adresser med tillgång till en specifik geografisk region eller subnät.

Konfigurera QuFirewall

1. Installera QuFirewall från App Center
2. Välj Profilkonfiguration
3. Välj din region
4. Klicka verkställ



Engångsinställningar

Security Counselor

Vad är Security Counselor?

Security Counselor är en mjukvaruportal för din QNAP-NAS. Det genomsöker systemet för sårbarheter och ger råd om hur du bäst säkrar din data mot varierande typer av attacker. Baserat på kraven ditt nätverk ställer på säkerhet kan du välja en av tre säkerhetspolicies: Basic, Intermediate och Advanced, eller skapa din egen. Funktionen Security Checkup kommer använda sig av dessa säkerhetspolicies vid scanning av systemet.



Basic



Intermediate



Advanced



Custom

En säkerhetsscanning kan köras manuellt eller schemaläggas.

Schemat kan anpassas efter dina behov och köras dagligen, under arbetsdagar, helger eller specifika veckodagar.

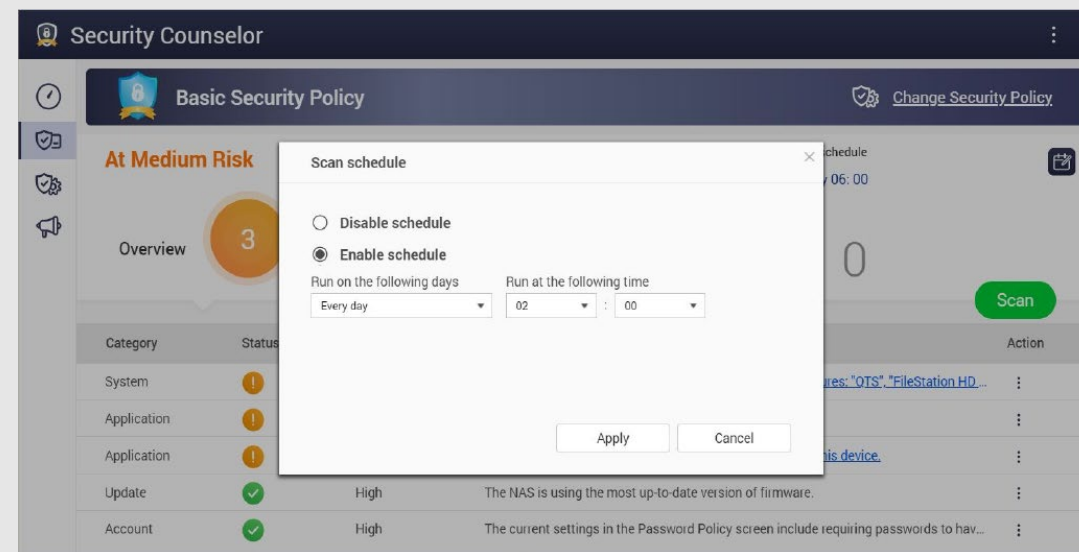
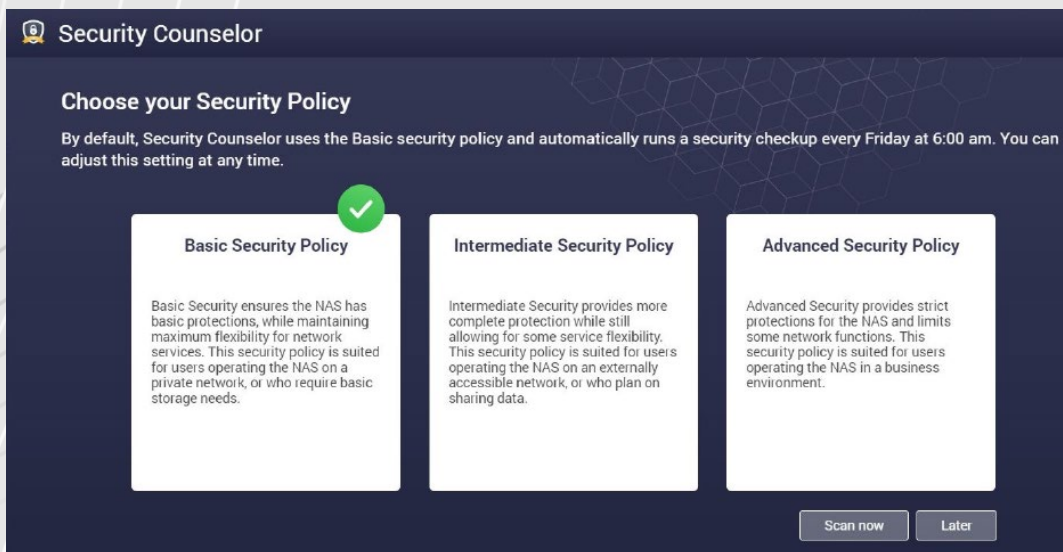
Du kan se resultaten av scannningar och dess efterföljande rekommendationer för att säkra din NAS i Security Counselor.

Engångsinställningar

Security Counselor

Konfigurera Security Counselor

1. Ladda ned Security Counselor från App Center
2. Välj en säkerhetspolicy och välj "Scan now"
3. Skapa ett schema genom att gå till Security Checkup (grön)
4. Gå till Schema (röd)
5. Välj önskad frekvens och klicka Verkställ



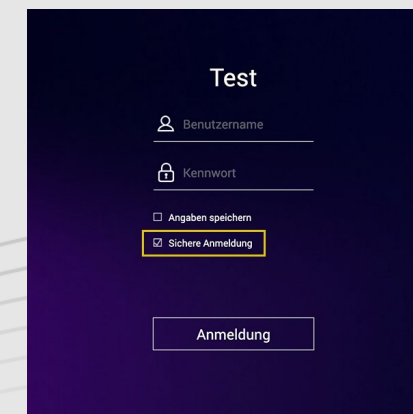
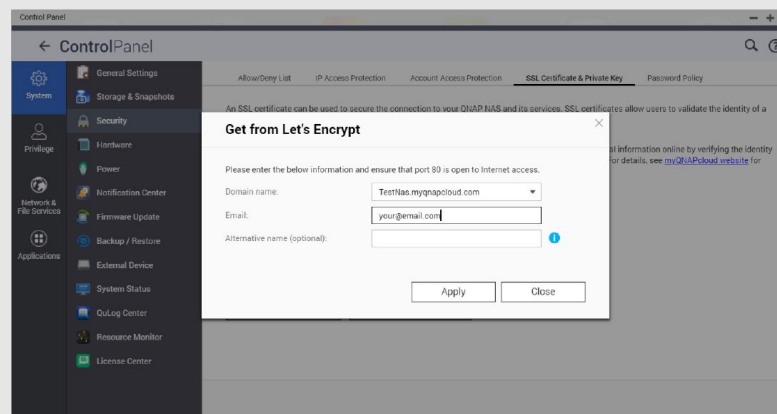
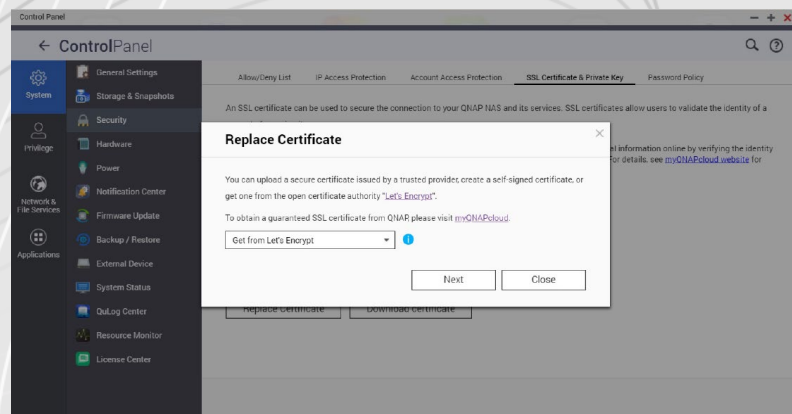
Avancerade inställningar

Krypterad anslutning

Använd krypterade anslutningar

Om du vill ansluta till din QNAP-enhet från utanför ditt eget nätverk bör du kryptera din anslutning. Det skyddar utomstående från att kunna läsa data som skickas till och från din enhet. Detta kan göras genom att nyttja säkra anslutningar, till exempel HTTPS och FTPS, där S:et står för "Secure", eller säker. Dataöverföringarna krypteras med certifikat, vilket innebär att enheterna kan verifiera varandras identiteter.

1. Gå till Kontrollpanel > System > Säkerhet, och gå till SSL-Certifikat & Privat Nyckel
2. Klicka på "Ersätt Certifikat"
3. Välj "Skaffa från Let's Encrypt"
4. Under domännamn, ange namnet eller DDNS där NAS-enheten kan nå
5. Ange din epostadress du vill använda för att registrera hos Let's Encrypt
6. Välj Säker Inloggning när du loggar in på din enhet



Avancerade inställningar

Portar

Vad är portar?

Portar tillåter kommunikation mellan din dator och andra datorer såväl som Internet. Brandväggar stänger oanvända portar för att hindra att skadlig kod distribueras till din dator över dessa. Genom att aktivera "Port forwarding" kan du använda onlinetjänster och andra applikationer över Internet som kräver inkommande anslutningar, eller medge användare från Internet åtkomst till tjänster på ditt hemnätverk.

Ändra standardportarna

Du kan öka säkerheten i ditt system genom att ändra portnumrena i din router från de vanliga 21, 22, 80, 443, 8080 samt 8081 till slumpmässiga portnummer. Konsultera din routertillverkare om hur du gör detta.

OBS! Tillåt EJ Port forwarding för oanvända tjänster (t.ex. SSH/Telnet)

Att stänga av oanvända portar kan minska mängden attacktytor för potentiella förövare. Genom att aktivera port forwarding exponeras port forwarding för användare på Internet – deaktivera därför tjänster du inte använder.

Instruktioner

- Backup:** <https://www.qnap.com/en/how-to/tutorial/article/hybrid-backup-sync>
- Admin account:** <https://www.qnap.com/en/how-to/faq/article/can-i-rename-the-default-admin-account>
- Password policy:** <https://www.qnap.com/en/how-to/knowledge-base/article/setup-the-password-policy-to-require-the-change-periodically>
- UPnP:** <https://docs.qnap.com/nas-outdated/QTS4.3.5/en/GUID-907F01D9-68D9-4449-A4D1-3213E19D0124.html?>
- Encryption:** <https://www.qnap.com/en/how-to/tutorial/article/how-to-use-ssl-certificates-to-increase-the-connection-security-to-your-qnap-nas>
- VPN:** <https://www.qnap.com/en/how-to/tutorial/article/how-to-set-up-and-use-qvpn>
- Port forwarding:** <https://www.qnap.com/en/how-to/faq/article/how-do-i-set-up-port-forwarding-on-the-nas>
- How to use QuFirewall:** <https://www.qnap.com/en/how-to/tutorial/article/how-to-use-qufirewall>
- Updates:** <https://www.qnap.com/en/how-to/tutorial/article/how-to-update-your-qnap-nas-firmware>
- Security Counselor:** <https://www.qnap.com/solution/security-counselor/en-us/>