

Sikkerhetsguide


Sikkerhetsretningslinjer for å bevare din NAS trygt og sikkert

Sikkerhetsark: Enkle ting du ikke kan ignorere

FØRSTE GANG DU BRUKER NAS




Administrator
Ikke bruk standardinnstillinger!
Opprett en ny admin.



Passord
Bruk sikre passord og følg anbefalinger



2FA
Øker sikkerheten for brukerkontoer




UPnP
Skr av plug and play for å unngå angrep


HVERDAGSLIGE/VANLIGE OPPGAVER




Backup
Ha mer enn én backuplokasjon!
Bruk 3-2-1 Backup Strategy



Skjermbilde
Sikre data konstant for å unngå å miste data



Oppdateringer
Hold softwaren oppdatert automatisk



VPN
Opprett en VPN-tilkobling for fjerntilgang

ONE TIME TASK – ENABLE & BE SAFE PERMANENTLY



QuFirewall
Last ned fra et APP center og aktiver det



Security Counselor
Last ned fra APP center og aktiver det

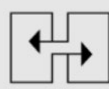
Sikkerhetsark: Avanserte stillinger for IT

FOR FOLK SOM ER MER VANTE



Porter

Endre standardportene



Kryptering

Bruk krypterte tilkoblinger
(HTTPS)

Introduksjon

Sikkerhetsguide

I denne korte sikkerhetsguiden vil du finne noe nyttige forklaringer på hvilke innstillinger du kann bruke for å sikre optimal beskyttelse av dine data.

Det er alltid en avveining mellom komfort og sikkerhet, noe enhver bruker selv må bestemme.

Denne guiden gir en kort oversikt over de viktigste temaene.

Detaljert informasjon og instruksjoner finner du på: <https://www.qnap.com/en>

Hva er ransomware?

Ransomware (løsepengevirus) er ondartede programmer som låser datamaskinen eller krypterer filer og blokkerrer deg fra å få tilgang til egne data. Ofre for dette vil ofte bli utpresset til å dekode de påvirkede filene, ellers får de ikke tilgang til filene igjen.

Hvordan kan du beskytte deg mot ransomware?

Ransomware er en økende trussel mot både selskap og private brukere som retter seg mot datamaskiner og nettverksbaserte enheter.

Hackere finner stadig nye måter å plassere ondartede programmer.

QNAP er klar over denne økende faren og jobber konstant med den beste beskyttelsen mot disse virusene.

De følgende eksemplene skal vise hvordan du best kan beskytte deg i henhold til dine behov.

Når man første gang åpner NAS

Administratorkonto

Administratorkontoen på QTS er «admin» automatisk. Av sikkerhetsårsaker er det ikke anbefalt å velge et generisk og lett gjettbart navn på en system-kritisk konto, siden da vil en hacker kun ville trenge å gjette passordet for å få fullstendig kontroll over ditt system. For å beskytte deg fra et slikt scenario, anbefaler vi på det sterkeste å opprette en annen systemadministratorkonto og deaktivere den automatiske «admin»-kontoen. Videre bør kun en administratorkonto brukes til administrative oppgaver, som vedlikeholdsarbeid. For den faktiske bruken av QNAP NAS er det anbefalt å skille mellom administratorfunksjoner og brukerfunksjoner.

Merk: Muligheten til å deaktivere «admin»-kontoen er kun tilgjengelig på QTS 4.1.2 eller nyere versjoner.



**OPPRETT NY
ADMINISTRATOR-
KONTO**



**DEAKTIVER
ADMINISTRATOR-
KONTO «admin»**

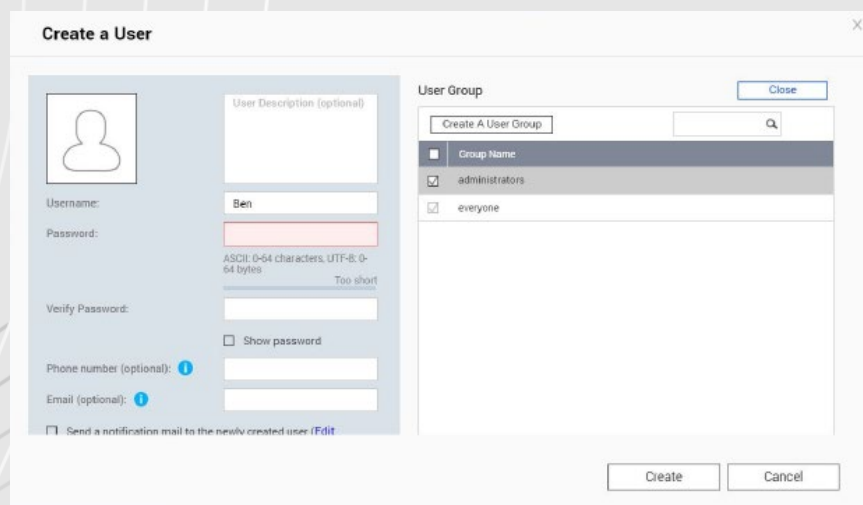


**BRUK
ADMINISTRATOR-
KONTOEN KUN TIL
ADMINISTRATIVE
OPPGAVER**

Når man først begynner å bruke NAS

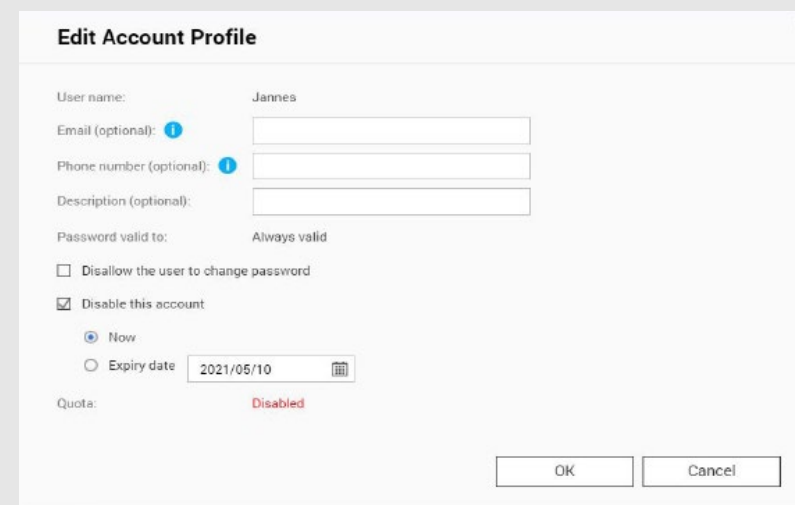
Hvordan deaktivere «admin»-kontoen

For passord på QNAP NAS er det noen oppsettsvalg som vil øke sikkerheten til systemet ditt. Selvfølgelig, hvis det kun er du som bruker QNAP NAS, er det kun du som er ansvarlig for å iverksette de anbefalte passordretningslinjene. Retningslinjene for sikre passord er enkle:



Opprett en ny administratorkonto

1. Logg inn på QTS ved å bruke administratorkontoen
2. Velg Control Panel > Users.
3. Opprett en bruker (i dette eksempelet kalt Ben) og tilegn ham til Administrator-brukergruppen.



Deaktivering av administratorkontoen

1. Logg in på QTS som Ben.
2. Velg Control Panel > Users and Edit account profile
3. Velg «disable this account» og velg «OK»

Når man først begynner å bruke NAS

Retningslinjer for passord

For passord på QNAP NAS er det noen oppsettsvalg som vil øke sikkerheten til systemet ditt. Selvfølgelig, hvis det kun er du som bruker QNAP NAS, er det kun du som er ansvarlig for å iverksette de anbefalte passordretningslinjene.

Retningslinjene for sikre passord er enkle:



Tilstrekkelig lengde



Spesielle karakterer

aA

Store og små bokstaver



**Aldri bruk samme passord på
ulike applikasjoner**



Endre passord jevnlig

Hvis QNAP NAS er tilgjengelig for andre, bør administratoren sette retningslinjer for passord som QNAP NAS håndhever. Dette vil sikre at retningslinjene følges. En kort forklaring finnes på neste side.

Når man først begynner å bruke NAS

Retningslinjer for passord

1. Gå til Control panel > System > Security > Password policy
2. Under Password Strength, velg kriterier
 1. Det nye passordet må inneholde karakterer fra minst tre av følgende klasser:
Små bokstaver, store bokstaver, tall og spesielle karakterer
 2. Ingen karakterer i det nye passordet kann bli gjentatt mer enn tre ganger (eller flere) (eksempel: AAA).
 3. Passordet kan ikke være det samme som brukernavnet. Heller ikke baklengs.
3. Under Change Password, velg at brukere må endre passordet periodevis

Viktig: å aktivere denne innstillingen deaktiverer innstillingen om at brukere ikke kan endre passordet sitt.

 1. Spesifiser maks antall dager passordet er gjeldende.
 2. Valgfritt: Velg å sende en epost til brukere en uke før passordet utgår
4. Klikk Use.

The screenshot shows the QNAP Control Panel interface. The left sidebar contains navigation options: System, Privilege, Network & File Services, and Applications. The main content area is titled 'ControlPanel' and shows the 'Password Policy' settings under the 'Security' tab. The settings include:

- Includes the following characters:
 - 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
- Change Password:
 - 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.

Når man først begynner å bruke NAS

2FA

2-trinnsverifikasjon bedrer sikkerheten til brukere. Når den er aktivert vil du måtte benytte deg av en engangskode (6 sifre) i tillegg til passordet ditt når du logger inn på NAS. 2-trinnsverifikasjon behøver en mobil med en autentiseringsapp som støtter Time-based One-Time password (TOTP-protokollen). Støttede apper inkluderer Google Authenticator (Android/iPhone/BlackBerry) eller Authenticator (Windows Phone). For å bruke denne funksjonen, følg disse stegene:

1. Installer autentiseringsappen på din mobile enhet
2. Under Password Strength, velg kriteriene
3. Gå til Options > 2-step Verification og klikk Get started.
 1. Konfigurer autentiseringsappen med å skanne QR-koden eller ved å skrive inn the secret key i appen.
 2. Skriv inn koden generert i appen til NAS for å verifisere korrekt konfigurasjon
 3. Velg en alternativ verifiseringsmetode ved å å motta en sikkerhetskode på mail eller ved å svare på et sikkerhetsspørsmål, dersom du ikke kann bruke din mobile enhet. For å motta en sikkerhetskode, må SMTP-serveren være konfigurert under Control Panel > Notifications > E-mail

A detaljert forklaring på oppsettet kan bli funnet på tutorial-nettstedet vårt.

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

The screenshot shows the QNAP web interface. At the top right, there is a user profile for 'admin' and a notification icon with '10+'. Below this, a menu is visible with 'Options' highlighted in a red box. The main content area is titled 'Options' and has a sub-menu with 'Profile', 'SSH Keys', 'Wallpaper', '2-step Verification' (selected), 'Password Settings', and 'E-mail Acc'. The text under '2-step Verification' reads: '2-step Verification adds an extra layer of protection to your account by requiring an additional one-time security code whenever you sign in to your NAS. For this function, you need a mobile device capable of running an authenticator app.' Below this, the status is 'Disabled' in red. A 'Get Started' button is highlighted with a red box. At the bottom right, there is an 'Apply' button. On the right side of the screenshot, a sidebar menu is visible with 'Options' highlighted in a red box, and other items like 'Locate my NAS', 'Restart', 'Shutdown', and 'Logout'.

Når man først begynner å bruke NAS

Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) blir brukt til å kontrollere enheter (lydenheter, rutere, printere, smart-Tver) på tvers av produsenter. Det tillater enheter i nettverket å koble seg sammen og få enkelte funksjoner til å kjøres automatisk. I dette tilfellet kan for eksempel QNAP bruke UPnP til å instruere ruterer til å tillate innkommende tilkoblingsforespørsler. Igjen så er det opptil balansen mellom komfort og sikkerhet. For mindre erfarne brukere anbefales det å deaktivere UPnP-muligheten på ruterer og inn i din QNAP NAS. Du finner ut hvordan du kan gjøre disse endringene i innstillinger på ruterer fra brukerveiledningen dens.

Viktig:

Hvis UPnP er aktivert på ruterer, kan all software og enheter på ditt hjemmenettverk konfigurere ruterer som de vil.

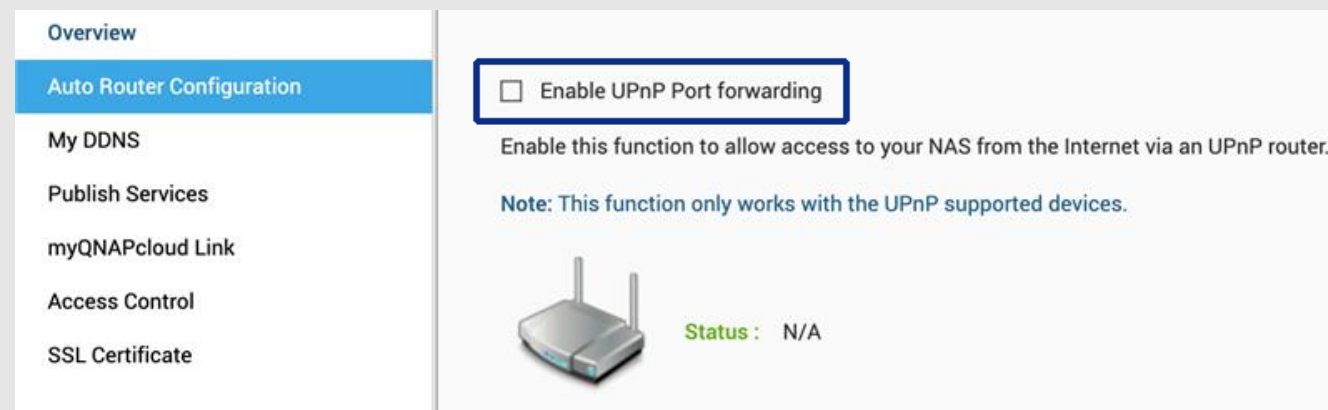
Derfor er det mulig at enkelte porter i brannmuren åpnes.

Disse kan være inngangspunkter for angrep fra utsiden.

Ikke koble NAS til WANen fra et Modem. Vi anbefaler på det sterkeste å bygge opp NAS bak ruterer

Deaktiver UPnP videresending på QNAP NAS

1. Gå til myQNAPcloud > Auto Router Configuration
2. Ta bort «enable UPnP port forwarding» og apply



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

Hverdagslige/vanlige oppgaver

3-2-1 Backup Strategy

Backup

Det er et individuelt spørsmål hvor, hvordan og hvor ofte du sikkerhetskopierer data. De avgjørende faktorene her er nødvendighetene som følge av sikkerhet, relevansen til dataen og de tilgjengelige mulighetene.

Forøvrig så er det en tommelfingerregel som må følges for å sikkerhetskopiere viktig data på en pålitelig måte.

Viktig: RAID er ikke backup, det beskytter deg mot harddiskfeil. Disse bildene beskytter deg mot ransomware-angrep fra din lokale datamaskin.

The 3-2-1 Backup Strategy

Selv om førstelinjen i forsvaret blir påvirket av ondartede programmer er å være forsiktig og å ha fornuftige vaner (som å jevnlig oppdatere programvaren, ikke åpne mistenkelige eposter, ikke besøke ukjent nettsteder osv), så bør du alltid huske å sikkerhetskopiere dataene dine.

Ingen backup-plan er perfekt, men 3-2-1 Backup er en god start. Behold 3 kopier av viktige filer, behold filene på minst to typer lagringsenheter og én på en off-site-lokasjon.

Viktig data bør bli sikkerhetskopiert

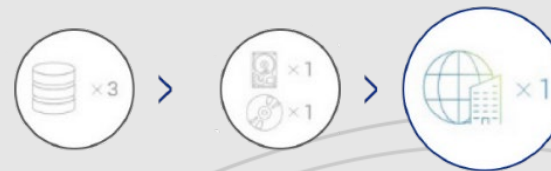
3 ganger: 1 hovedfil and 2 backup filer



Arkivene oppbevares på 2 forskjellige backuplokasjoner for å beskytte mot ulike farer.



Én av backupfilene skal oppbevares offsite (utenfor hjemmet eller jobben)



Hverdagslige/vanlige oppgaver

Skjermbilder

Hva er skjermbilder?

Skjermbilder er bilder av dataen som du har lagret på din QNAP NAS. Første gangen du tar et skjermbilde, blir alt du har lagret med. Skjermbilder etter det tar kun med seg det som er endret siden forrige skjermbilde. Skjermbilder er veldig lagringsvennlige ettersom de er blokkbaserte.

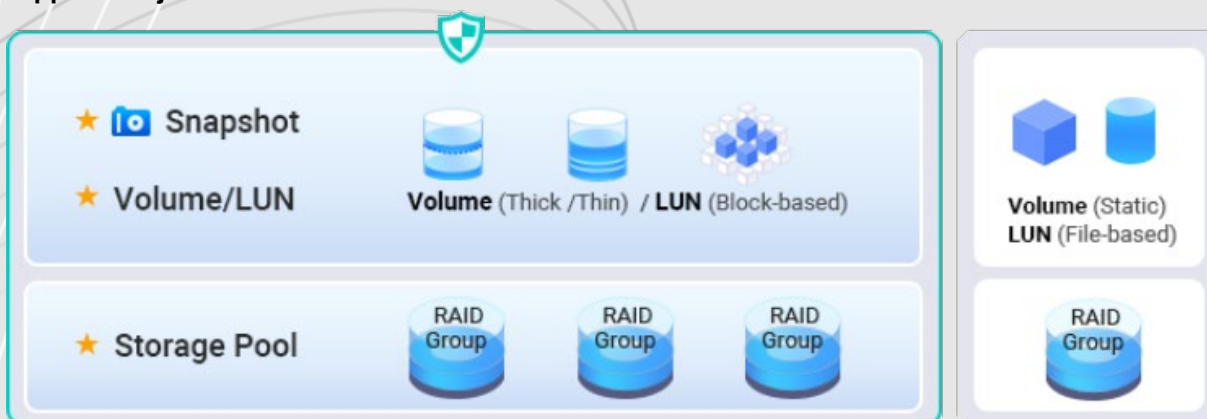
Viktig:

Skjermbilde er ikke en sikkerhets kopi. Den gir tilgang til tidligere versjoner i tilfelle de ved en feil er blitt slettet eller innhold er blitt feilaktig endret.

Det finnes en detaljert oversikt over dette temaet på vår nettside:

<https://www.qnap.com/solution/snapshots/en-us/>

Oppsettsskjermbilder:



Hverdagslige/vanlige oppgaver

Automatiske oppdateringer

Oppdateringer

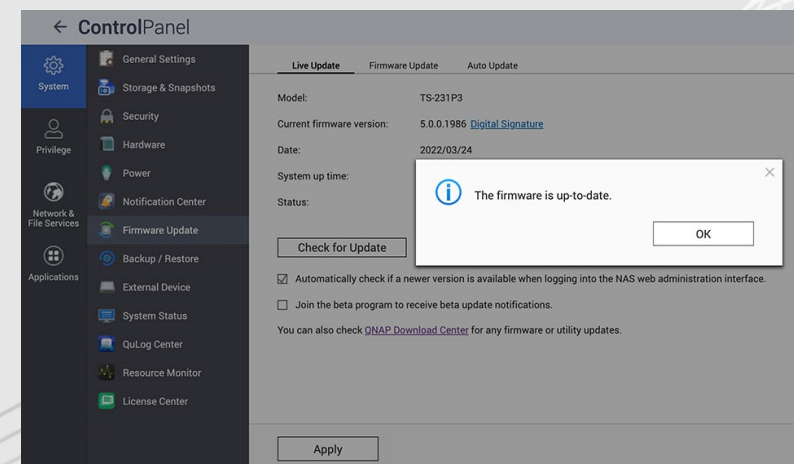
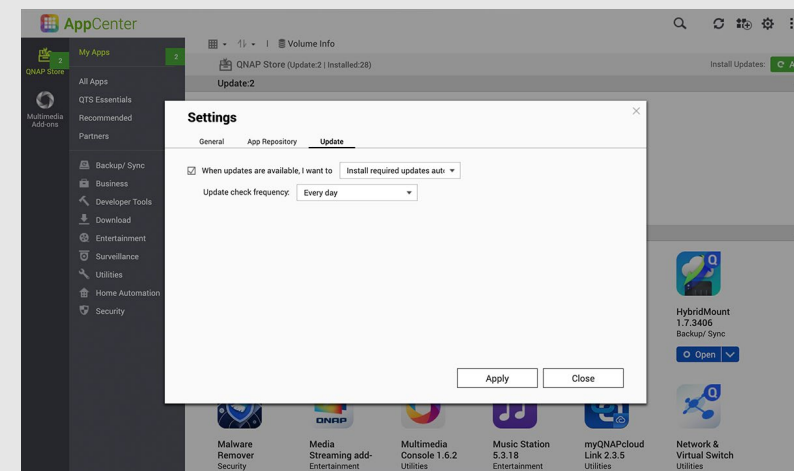
Et oppdatert programvaresystem er viktig for din NAS. QNAP jobber alltid med å tette sikkerhetshull og tidvis legge til flere egenskaper. Oppdateringer bør derfor alltid gjøres snarest, for å beskytte dataen din best mulig. Hvis din QNAP NAS er tilkoblet internett og du ikke har endret standardinnstillingene, vil enheten din automatisk se etter den siste programvaresystem og varsle deg om at en ny oppdatering er tilgjengelig. Du må da sørge for å oppdatere det. Vær oppmerksom på at din QNAP NAS vil trenge å bli skrudd av og på for å gjøre dette, og da vil være utilgjengelig i 5—10 minutter. Du har også muligheten til å manuelt installere den siste programvaren. Dette er nødvendig hvis din QNAP NAS ikke er tilkoblet nettet og dermed ikke automatisk kan se etter og laste ned oppdateringer. Hvis du lurer på om din firmware er oppdatert, gjør følgende:

Finware-oppdatering i sanntid

1. Logg inn som administrator
2. Åpne Control Panel > Finware update
3. Åpne live update
4. Klikk Check for updates

Oppdater apper automatisk

1. Gå til App Center
2. Gå til settings
3. Åpne oppdatering
4. Velg When updates are available
5. Velg Install updates automatically



Hverdagslige/vanlige oppgaver

VPN

Hva er VPN?

VPN er et virtuelt privat nettverk. I vårt tilfelle er det tiltenkt å etablere sikker tilgang til QNAP NAS mens man er på reise. En VPN-server kjøres på QNAP NAS og en spesiell VPN-programvare kjøres på enheten som brukes på reise. En tunnel blir satt opp mellom disse gjennom internett. Fordelen med dette er at tilkoblingen er beskyttet av autentisering og kryptering og kun kan bli brukt av autoriserte personer. En VPN-tilkobling oppfører seg dermed på samme som om begge enheter var logget inn på samme nett. Dette betyr at de lokale ressursene kan bli brukt uten noe men. Når VPN-en er satt opp kan den enkelt bli brukt om igjen, og gi sikker tilgang til hjemmenettverket. Vi anbefaler alltid å etablere en tilkobling via VPN når man er på reise. Det kan gjøre at data lastes ned noe saktere enn vanlig, men tilkoblingen er sikker.

Hvordan sette opp og bruke VPN?

En detaljert forklaring finnes på nettsiden:

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

Anbefaling for remote tilgang:

myQNAPcloud Link & VPN (Port Forwarding VPN Service Ports kreves, vi anbefaler å bruke QuFirewall for bedre beskyttelse.



Engangsoppgaver

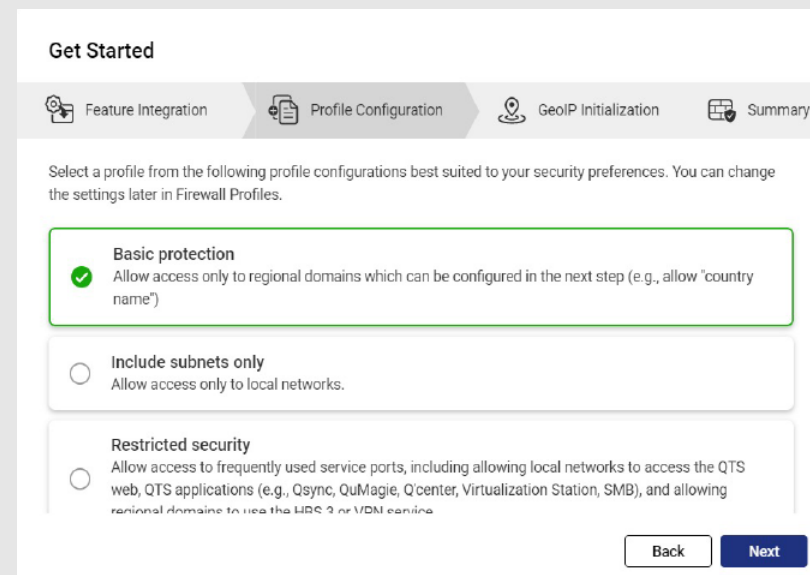
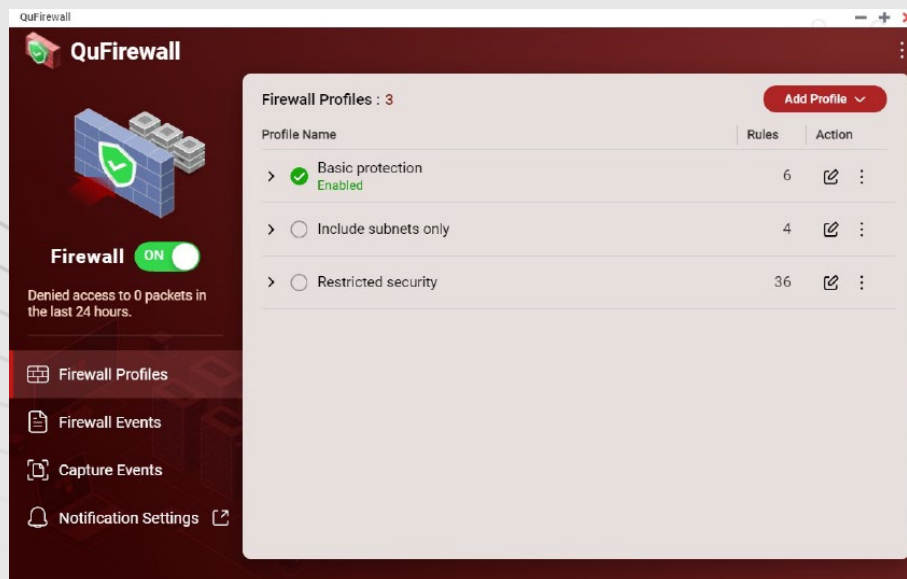
QuFirewall

Hva er QuFirewall

QuFirewall er en brannmuradministreringsapp for din QNAP-enhet. Ved å integrere et kraftig og enkelt å bruke system, gir QuFirewall deg mulighet til å kontrollere og verifisere tilkoblinger til din enhet. QNAP anbefaler at du installerer QuFirewall på din QNAP NAS og begrenser tillatte IP-adresser til en spesifikk region.

Setup QuFirewall

1. Installer QuFirewall fra App Center
2. Velg profilkonfigurasjon
3. Velg din region
4. Klikk ferdig



Engangsoppgaver

Security Counselor

Hva er Security Counselor?

Security Counselor er din sikkerhetsportal for QNAP NAS. Den skanner systemet for sårbarheter og gir anbefalinger for hvordan man beskytter dataen mot ulike angrepsmetoder. Basert på sikkerhetskravene til ditt nettverk, kan du velge én av tre standard sikkerhetsnivåer (basic, intermediate, advanced). Security Checkup funksjonen vil bruke ditt valgte sikkerhetsnivå når det skanner systemet. Du kan også konfigurere din egen policy ved å velge Custom security policy.



Basic



Intermediate



Advance



Custom

Et sikkerhetsskann kan bli gjort manuelt eller planlagt for å sikre maks sikkerhet.

Planlagt skann kan bli satt opp på forskjellige måter (daglige/ukedager/helger/utvalgt dag) for å sørge for at jobb ikke blir påvirket.

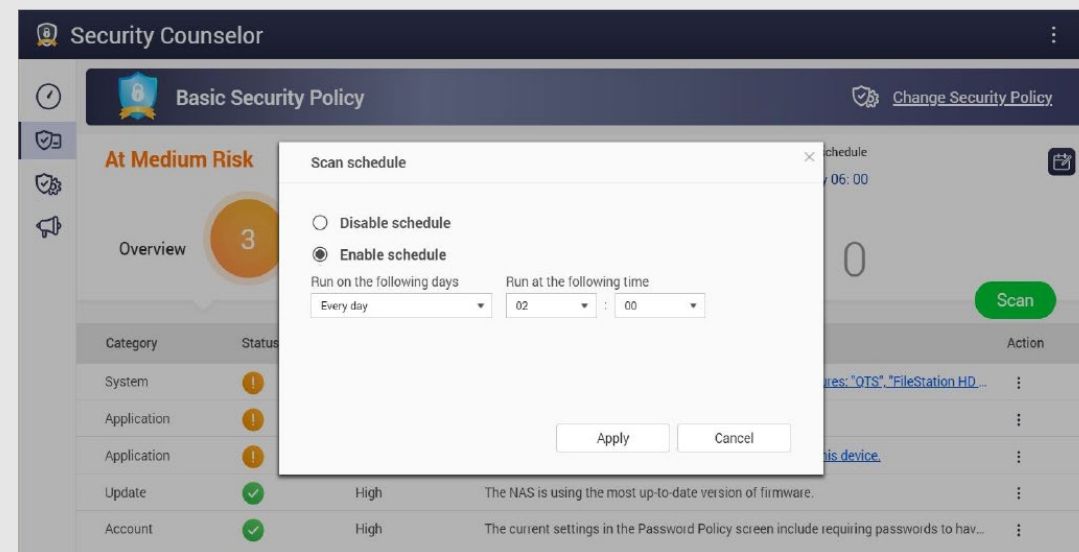
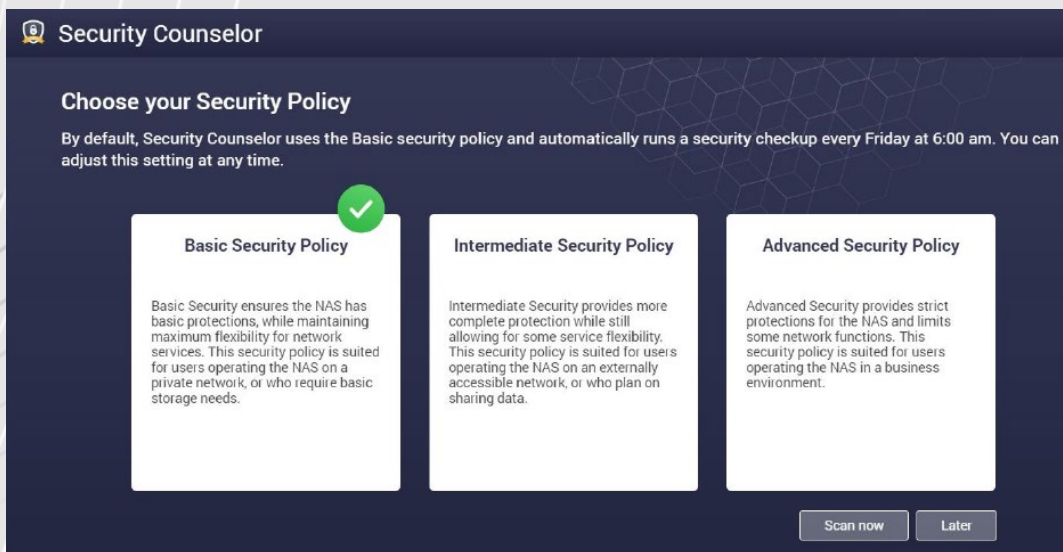
Du kan klikke på de skannede resultatene og Security Counselor vil guide deg med det nødvendige systemet for å endre innstillinger for å sikre din NAS:

Engangsoppgaver

Security Counselor

Sett opp Security Counselor

1. Last ned Security Counselor fra App Center
2. Velg en Security Policy og klikk Scan now
3. For å opprette et planlagt skann, gå til Security Checkup (markert i grønn)
4. Gå til Planned scans.
5. Velg dine foretrukne tidspunkt og trykk Apply.



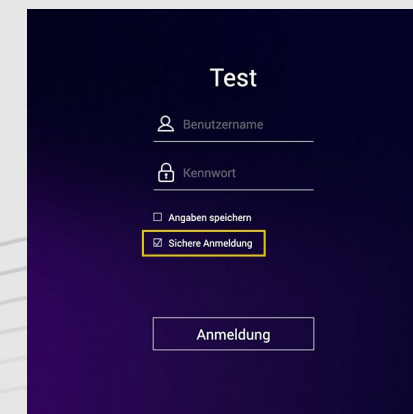
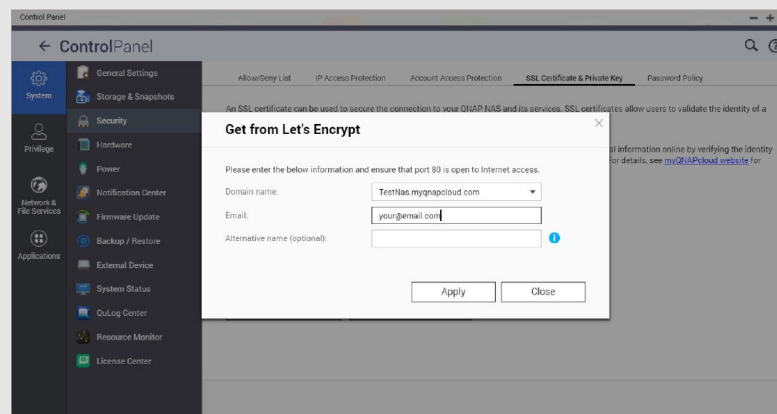
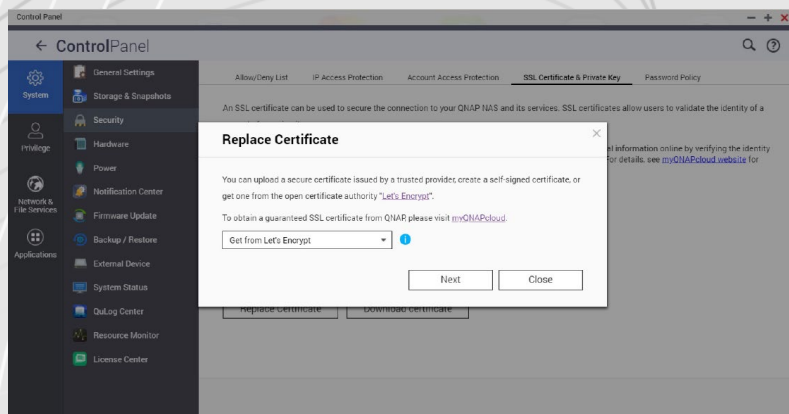
Avanserte innstillinger

Encrypted Connection

Bruk krypterte HTTPS-tilkoblinger

Hvis du vil koble til din QNAP NAS utenfra ditt nettverk, må du sørge for at dataen er kryptert. Dette beskytter tredjeparter fra å være i stand til å lese din data. Du kan sørge for dette ved å bruke beskyttede tilkoblinger. Dette er for eksempel HTTPS istedenfor HTTP eller FTPS istedenfor FTP. S-en står for «secure». Dataoverføringen er nå kryptert med et sertifikat så autentiseringen er sikret.

1. Åpne Control panel > System > Security og gå til SSL Certificate & Private Key .
2. Klikk på Replace Certificate
3. Velg Get fra Encrypt
4. Under domenenavn, skriv inn navner eller DDNS-en NAS kan nås på
5. Skriv inn e-postadressen din for registrering med «Let's Encrypt»
6. Velg sikker innlogging når du logger på nettsiden.



Avanserte innstillinger

Porter

Hva er porter?

En port muliggjør kommunikasjon mellom din datamaskin og en annen datamaskin, i tillegg til internettet. En brannmur lukker ubrukte porter for å beskytte dem fra virus. Ved å sette opp portvideresending kan man bruke online tjenester eller andre internettapplikasjoner som tillater tilkobling fra internett eller brukere på internett til å bruke nett- og remote-servere og andre tjenester på ditt hjemmenettverk.

Endre standardporter

Du bør endrer standardportene i din ruters konfigurasjon som 21, 22, 80, 443, 8080 og 8081 til tilfeldig portnumre. For eksempel, endre 8080 til 9527. for informasjon om hvordan du gjør dette, kontakt din ruterleverandør.

Ikke videresend «System Port» / unødvendige serviceporter (e.g. SSH, Telnet)

Deaktiver portvideresending på unødvendige service-porter. Det kan redusere angrepsmuligheter. Etter portvideresending kan service-porter brukes av alle via internett.

Instruksjoner

- Sikkerhetskopiering:** <https://www.qnap.com/en/how-to/tutorial/article/hybrid-backup-sync>
- Adminkonto:** <https://www.qnap.com/en/how-to/faq/article/can-i-rename-the-default-admin-account>
- Passordretningslinjer:** <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?>
- Kryptering:** <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>
- Portvideresending:** <https://www.qnap.com/en/how-to/faq/article/how-do-i-set-up-port-forwarding-on-the-nas>
- Hvordan bruke QuFirewall:** <https://www.qnap.com/en/how-to/tutorial/article/how-to-use-qfirewall>
- Oppdateringer:** <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/>