Sikkerhedsvejledning

Retningslinjer for at beskytte din NAS

Sikkerhedsliste – Grundlæggende ting du ikke kan ignorere

Første gang du bruger NAS

Administrator
Brug ikke standardindstillinger!
Opret en ny adminkonto

Adgangskoder
Brug sikre adgangskoder

2-faktorautorisering
Styrker sikkerheden
for alle kontoer

UPnP
Sluk Plug and Play
for at styrke sikkerheden

Hverdag/almindelige opgaver

Backup
Hav mere end en backup!
Brug 3-2-1
sikkerhedskopieringsstrategi

Snapshots
Tag snapshots løbende for
at forhindre tabt data

Opdateringer
Tænd for automatiske
softwareopdateringer

VPN
Opret en VPN-forbindelse
til fjernadgang

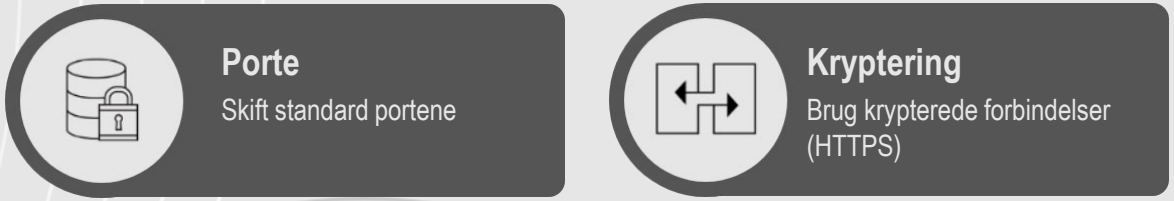
Engangsindstillinger der beskytter permanent

QuFirewall
Download QuFirewall
og aktiver

Sikkerhedsrådgiver
Download og aktiver

Mere avancerede indstillinger

For avancerede brugere



Introduktion

Sikkerhedsvejledning

I sikkerhedsvejledningen vil du finde nyttige forklaringer på, hvilke indstillinger du kan bruge til at sikre optimal beskyttelse af dine data. Der er dog altid en afvejning mellem komfort og sikkerhed, som hver bruger må tage stilling til.

Denne guide giver en kort oversigt over de vigtigste emner.

Yderligere detaljeret information og instruktioner kan findes på: https://www.qnap.com/

Hvad er ransomware?

Ransomware er ondsindede programmer der låser computeren, krypterer filer og blokerer dig fra adgang til dine egne data. Ofrene bliver ofte afpresset til at betale løsesum for at få sine filer dekrypteret, ellers vil de være ude af stand til at benytte filerne igen.

Hvordan kan du beskytte dig selv fra ransomware?

Ransomware er en stigende trussel mod både private brugere og erhvervslivet, og hackere er konstant på udkig efter nye måder at placere ondsindet software.

QNAP er bevidst om den stigende fare og arbejder konstant på at give den bedst mulige beskyttelse mod malware.

Følgende eksempler har til formål at vise, hvordan du bedst kan beskytte dig selv i tråd med dine behov.

Ved første opstart

Administratorkonto

Brugerkontoen på QTS er administrator. Af sikkerhedsgrunde anbefales det ikke at vælge et generisk eller letgenkendeligt navn for en systemkritisk konto, da dette muliggør, at hackere kan gætte dit kodeord og derved få styring over dit system. For at beskytte dig selv fra et sådant scenarie, vil vi stærkt anbefale at oprette en anden systemadministratorkonto og deaktivere den standard admininistrationskonto. Derudover bør en administrationskonto kun blive brugt til administrative opgaver, som f.eks vedligeholdelse. Til det faktiske brug af QNAP NAS anbefales det at adskille administratorfunktioner og brugerfunktioner.

Bemærk: Muligheden for at deaktivere administrationskontoen er kun tilgængelig på QTS 4.1.2 eller nyere versioner.

OPRET NY ADMINISTRATOR KONTO

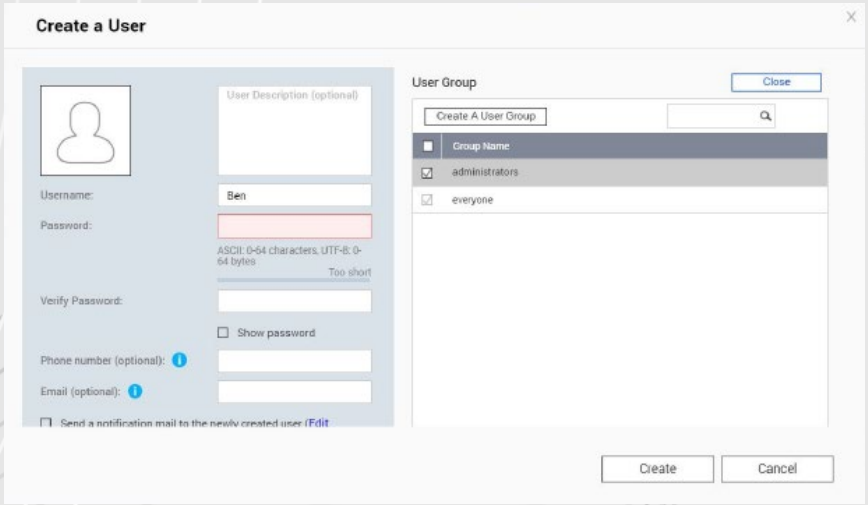
DEAKTIVER ADMINISTRATOR KONTO "ADMIN"

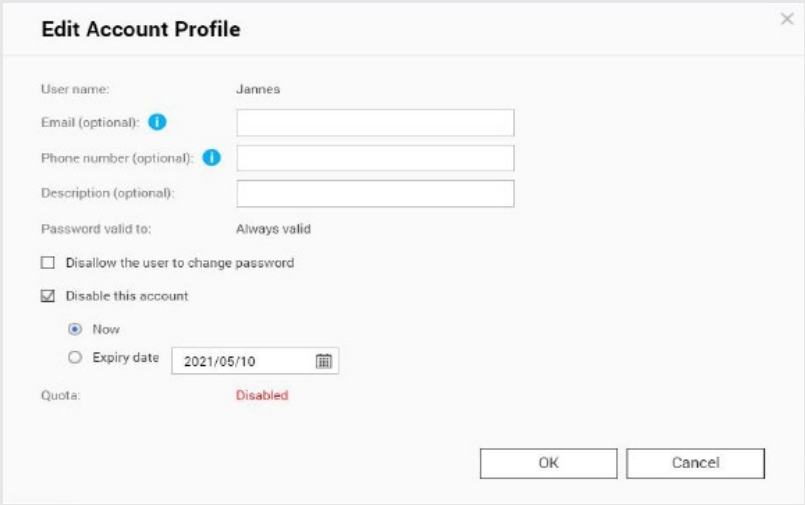
BRUG KUN ADMINISTATOREN TIL ADMINISTRATIVE OPGAVER

Ved første opstart

Hvordan deaktiveres “admin“-kontoen

Når det kommer til din QNAP NAS, er der et par enkle ting, du kan gøre for at forbedre sikkerheden drastisk. Det vigtigste er at oprette en ny brugerkonto med administratorrettigheder med et andet navn end "admin". Det gør du på følgende måde:





Opret en ny administratorkonto

1. Log ind på QTS vha. "admin"-kontoen.

2. Vælg Kontrolpanel > Brugere.

3. Opret en ny bruger (i dette eksempel "Ben") og placer ham i brugergruppen "administratorer".

Deaktiver “admin"-konto

1. Log ind på QTS som Ben.

2. Vælg Kontrolpanel > Brugere og rediger "admin"-kontoens profil.

3. Klik på Deaktiver konto og vælg "OK".

Ved første opstart

Adgangskodepolitikker

Når det kommer til adgangskoder, er der et par ting at huske på vedrørende sikkerhed. Hvis du er den eneste bruger af din NAS fra QNAP, kan du naturligvis frit vælge den type kodeord, du vil have, men øget kompleksitet øger vanskeligheden for udefrakommende at gætte det.
Følgende grundlæggende ting er gode at huske på, når du vælger en adgangskode:

Tilstrækkeligt langt

Specialtegn

Små og storesag bogstaver

Brug aldrig samme adgangskode til forskellige applikationer

Skift adgangskode regelmæssigt

Hvis du deler din NAS fra QNAP med andre brugere, bør du som administrator opsætte regler for adgangskoder og håndhæve disse. Det betyder, at alle skal følge de regler, du sætter. Læs mere på næste side.

Ved første opstart

Adgangskodepolitikker

1 . Gå til Kontrolpanel > System > Sikkerhed > Adgangskodepolitik.

2. Under Adgangskodestyrke skal du vælge kriterier

1. Det nye adgangskode indeholder tegn fra

mindst tre af det følge klasser:

Små bogstaver, store bogstaver, cifre og specielle tegn.

2. Ingen tegn i den nye adgangskode kan gentages tre gange eller mere. (eksempel : AAA).

3. Adgangskoden må ikke være det samme som det tilsvarende brugernavn. Heller ikke skrevet baglæns.

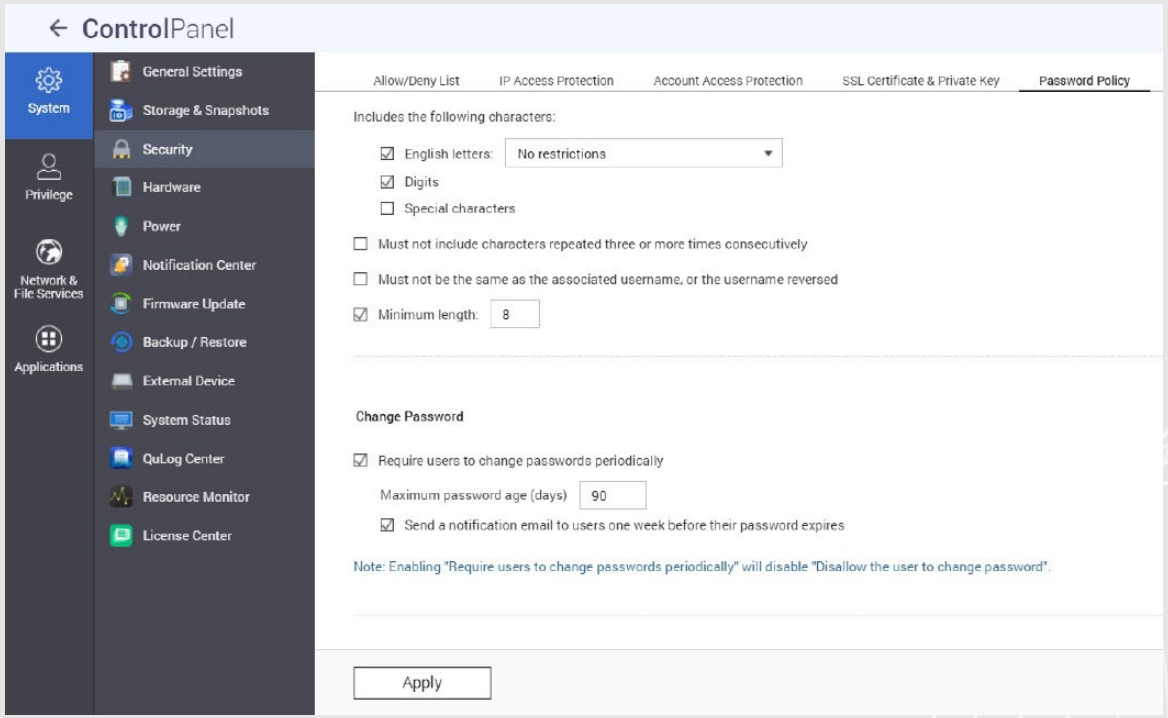
3. Vælg under “Skift adgangskode”, at du kræver at adgangskoden skiftes kontinuerligt.

Vigtigt : Aktiveres dette deaktiverer det muligheden for andre brugere at skifte kodeord

1. Angiv det maksimale antal af dage til adgangskoden gyldighed

2. Valgfrit: Send en notifikationse-mail til brugere en uge før deres adgangskode udløber

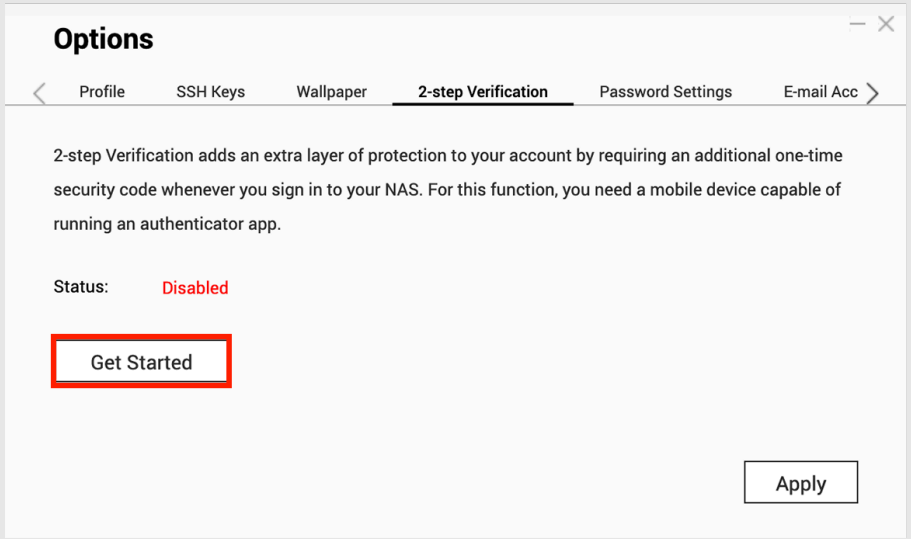
4. Klik på anvend .

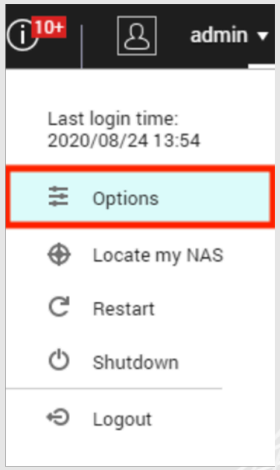


Ved første opstart

2-faktorautorisering

Du kan forbedre sikkerheden med 2-faktor godkendelse. Når den er aktiveret, skal du indtaste en engangskode (6 tegn) ud over din adgangskode, når du logger ind. 2-faktor godkendelse kræver en godkendelsesapp, der understøtter den tidsbaserede engangskodeord (TOTP) protokol, såsom Google Authenticator eller Authenticator (Microsoft).





Følg nedenstående trin for at aktivere funktionen:

1. Installer en godkendelsesapp på din mobilenhed
2. I din NAS skal du gå til "Valgmuligheder" > "2-trins verifikation" og klikke på "Kom godt i gang" 1. Synkroniser enhederne ved at scanne QR-koden med din godkendelsesapp eller ved at indtaste den hemmelige nøgle
2. Indtast koden genereret i din NAS for at bekræfte indstillingerne
3. Vælg en backupmetode, såsom at sende koder via SMS eller ved at besvare et sikkerhedsspørgsmål, hvis du ikke kan bruge din mobilenhed. E-mail er kun tilgængelig, hvis en SMTP-server er korrekt konfigureret under "Kontrolpanel" > "Meddelelser" > E-mail

En komplet, detaljeret guide på engelsk er tilgængelig på vores hjemmeside: https:// www.qnap.com /da/ how-to / tutorial / article /how-to-enhance-account-security-using-2-step-verification

Ved første opstart

Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) bruges til at styre enheder (f.eks. lydenheder, routere, printere, smart-tv'er) fra forskellige producenter. Det giver enheder på det samme netværk mulighed for at forstå hinanden og køre visse automatiske funktioner uden brugerindblanding. UPnP kan i dette tilfælde bruges til at tillade din QNAP NAS at lade en bestemt type trafik komme igennem - vi anbefaler kun avancerede brugere at have denne funktion aktiveret. For standardbrugeren anbefales det at deaktivere UPnP i både din router og NAS-enhed. Kontakt din routerproducent om, hvordan du deaktiverer funktionen, og se nedenfor for, hvordan du gør det på din QNAP NAS.

OPMÆRKSOMHED!

Hvis UPnP er aktiveret i din router, kan software og enheder på dit netværk konfigurere routeren efter deres smag. Det betyder, at de kan åbne porte i din firewall og udsætte dit netværk for angreb fra internettet.

Tilslut ikke din NAS til internettet fra et modem. Vi anbefaler stærkt at have din NAS bag en router.

Deaktiver UPnP- videresendelse på QNAP NAS

1. Gå til myQNAPcloud > Auto Router Configuration

2. Fjern markeringen i “Enable UPnP Port forwarding“ og tryk anvend.

Daglige/faste opgaver

3-2-1 Backup-strategi

Backup

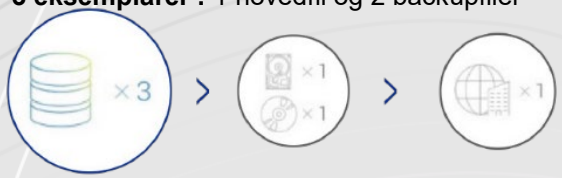
Hvor, hvordan og hvor ofte du sikkerhedskopierer dine data er op til dig. Du bør altid afveje sikkerhedsbehov, vigtigheden af dine data og de muligheder, du har for at gemme dem. Der er dog en tommelfingerregel for, hvordan du sikkert og pålideligt sikkerhedskopierer vigtige data.

Obs! RAID er ikke backup, det beskytter dig kun mod defekte harddiske. Snapshots beskytter dig mod ransomware-angreb fra din lokale computer.

Backup-strategien 3-2-1

Selvom du gør alt, hvad du kan for at holde malware væk fra din NAS, bør du altid sikkerhedskopiere dine data, hvis det værste skulle ske. Med 3-2-1 strategien får du et solidt fundament at bygge videre på. Hav 3 kopier af vigtige filer, gem dem på mindst 2 typer lagringsmedier og hav 1 kopi off-site, dvs. på et sikkert sted

Vigtig data skulle gerne være sikkerhedskopieret i hvert fald **3 eksemplarer :** 1 hovedfil og 2 backupfiler



Arkiver er gemt på **2 forskellige** backupmedier til beskytte mod forskellige typer af farer

En af sikkerhedskopierneer til være gemt på anden fysisk plads (uden for hjem eller forretning).

Daglige/faste opgaver

Snapshots

Hvad er snapshots?

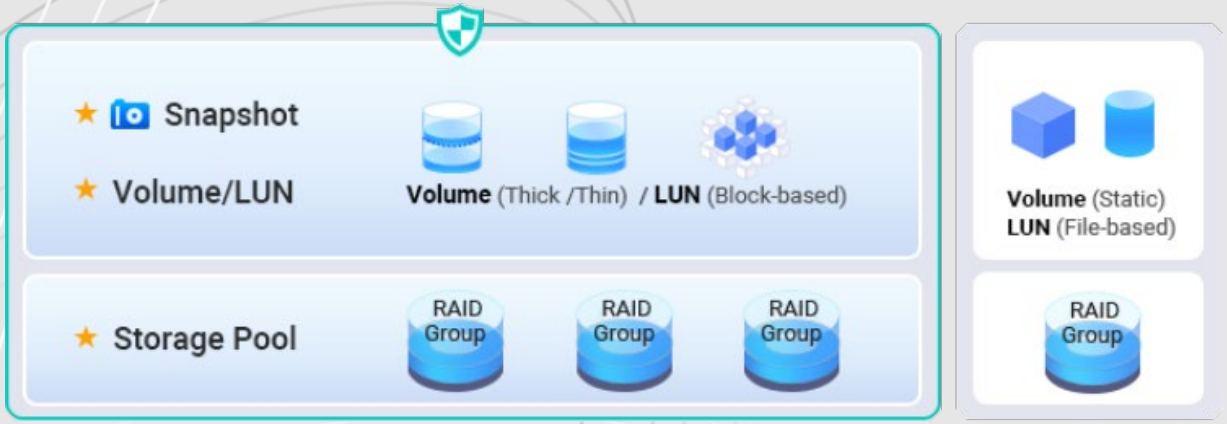
Snapshots er billeder af det data du har gemt på din QNAP NAS. Første gang tager du et snapshots af al din data. Alle efterfølgende snapshots behøver kun at være af det indhold du har ændret.. Snapshots giver plads besparelse fordi de er blokbaserede.

Vigtigt:

Snapshots er ikke en sikkerhedskopi. Det tillader adgang til tidligere versioner i tilfælde af de ved en fejltagelse bliver slettet.

Du kan finde en detaljeret beskrivelse af emnet på vores hjemmeside:
https://www.qnap.com/solution/snapshots/en-us/

Opsætning af snapshots



Daglige/faste opgaver

Automatiske opdateringer

Opdateringer

Opdateret software er vigtig for din NAS-enhed. QNAP arbejder konstant på at lukke nye sikkerhedshuller, der opdages, og tilføjer også af og til nye funktioner til systemet.

Opdateringer bør derfor altid installeres så hurtigt som muligt for den bedst mulige beskyttelse af dine filer.

Hvis din QNAP NAS er tilsluttet, og du ikke har ændret nogen indstillinger, får du besked, når opdateringer er tilgængelige - du bør opdatere hurtigst muligt.

Opdateringen kræver en genstart og gør enheden utilgængelig i 5-10 minutter. Du har også mulighed for manuelt at opdatere softwaren, hvis din enhed ikke er tilsluttet. For at kontrollere, om dit system er opdateret, skal du gøre følgende:

Realtids firmwareopdatering

1. Log ind som 'Administrator'

2. Åbn Kontrolpanel > Firmwareopdatering

3. Åbn Live Update

4. Klik på søg efter opdatering

Opdater automatisk

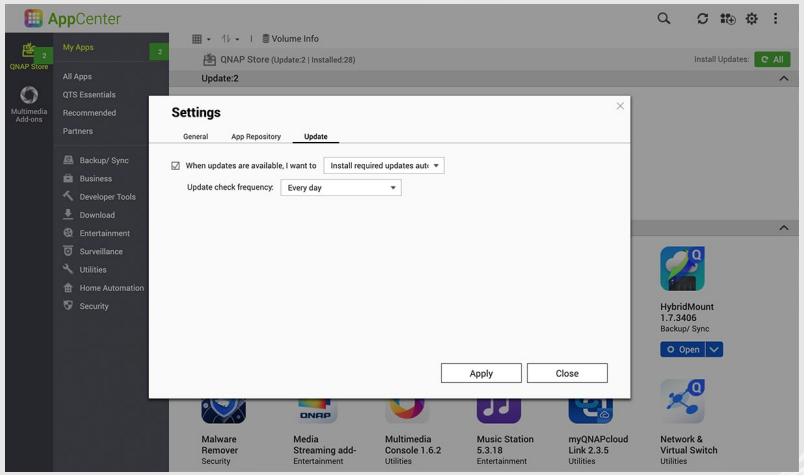
1. Gå til App Center

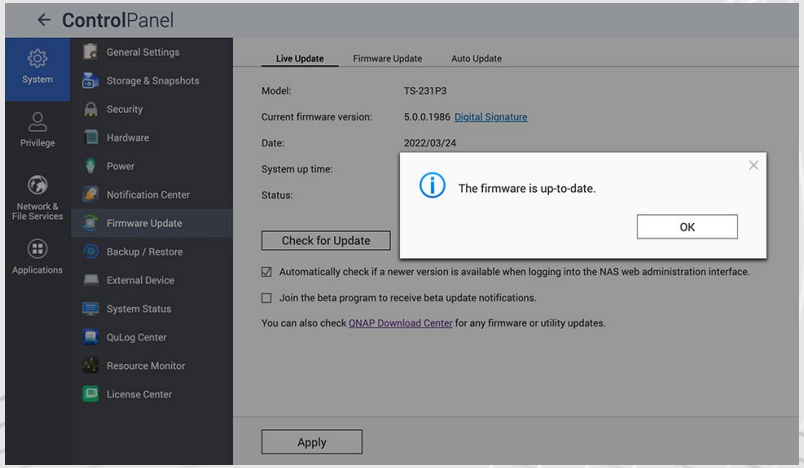
2. Gå til indstillinger

3. Åbn Opdater

4. Vælg “Hvornår opdateringer er tilgængelig“

5. Vælg installer alle opdateringer automatisk





Daglige/faste opgaver

VPN

Hvad er VPN?

VPN står for Virtual Private Network - et virtuelt privat netværk. I dette tilfælde bruges VPN til sikker forbindelse til din QNAP NAS fra et eksternt netværk. En VPN-server kører på QNAP-enheden, og VPN-softwaren kører på den enhed, der bruges eksternt, og en tunnel forbinder de to over internettet.

Fordelen er, at forbindelsen er beskyttet med autentificering og kryptering og kun kan bruges af autoriserede brugere. Brugeroplevelsen er ligesom du og enheden var på det samme netværk.

Efter en VPN-forbindelse er oprettet, kan den bruges igen og igen. Vi anbefaler altid at oprette forbindelse til din QNAP-enhed over VPN, når du er på et eksternt netværk for maksimal sikkerhed.

For at konfigurere VPN

En detaljeret gennemgang af konfigurationen kan findes på vores hjemmeside (engelsk):
https://www.qnap.com/en/how-to/tutorial/article/how-to-set-up-and-use-qvpn

Anbefalet software til fjernadgang

myQNAPcloud Link & VPN (Port Forwarding VPN påkrævet, QuFirewall anbefales for den bedste beskyttelse)

Engangsopgaver

QuFirewall

Hvad er QuFirewall

QuFirewall er software til styring af firewalls i din QNAP-enhed. Med kraftfulde og brugervenlige profiler giver appen dig mulighed for at kontrollere og verificere forbindelser til din enhed. Vi anbefaler, at du installerer QuFirewall på din QNAP NAS og begrænser IP-adresser med adgang til et specifikt geografisk område.

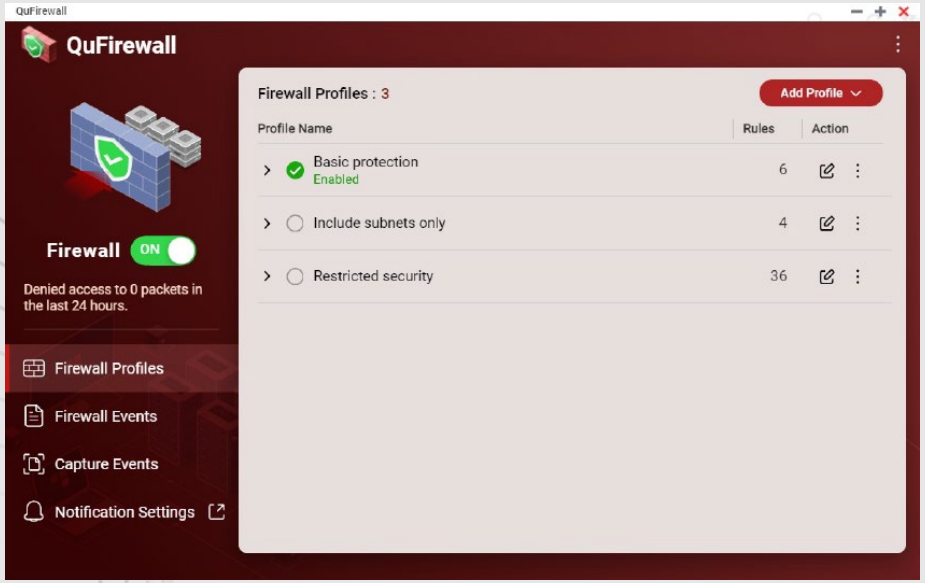
Opsæt QuFirewall

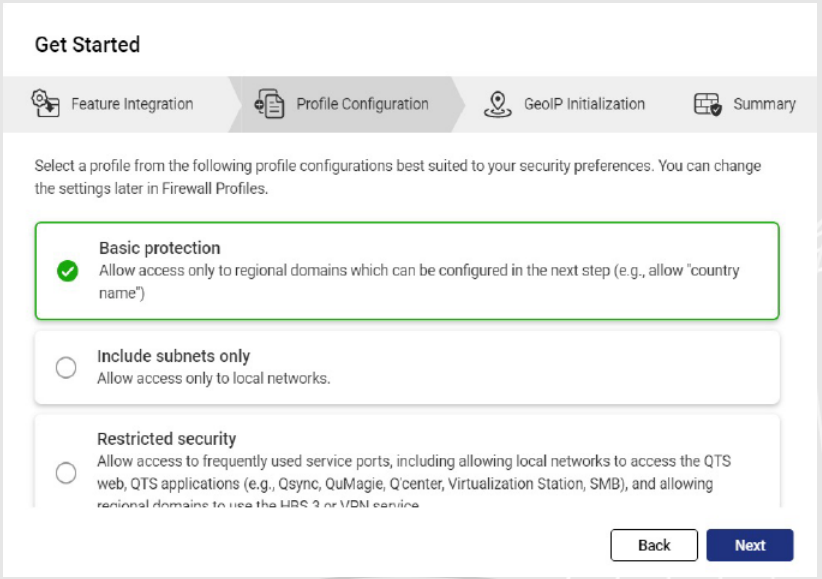
1. Installer QuFirewall fra App Center

2. Vælg en profilkonfiguration

3. Vælg din område

4. Klik på Udfør





Engangsopgaver

Sikkerhedsrådgiver _

Hvad er en sikkerhedsrådgiver?

Security Counselor er en softwareportal til din QNAP NAS. Den scanner systemet for sårbarheder og rådgiver, hvordan du bedst sikrer dine data mod forskellige typer angreb. Baseret på sikkerhedskravene til dit netværk kan du vælge en af tre sikkerhedspolitikker: Basic, Intermediate og Advanced, eller oprette din egen. Sikkerhedstjek-funktionen vil bruge disse sikkerhedspolitikker, når systemet scannes.

Grundlæggende

Mellemliggende

Rykke

Brugerdefinerede

En sikkerhedsscanning kan køres manuelt eller planlægges.

Tidsplanen kan tilpasses til dine behov og køre dagligt, på hverdage, weekender eller bestemte dage i ugen.

Du kan se resultaterne af scanninger og deres efterfølgende anbefalinger til sikring af din NAS i Security Counselor.

Engangsopgaver

Sikkerhedsrådgiver

Konfigurer

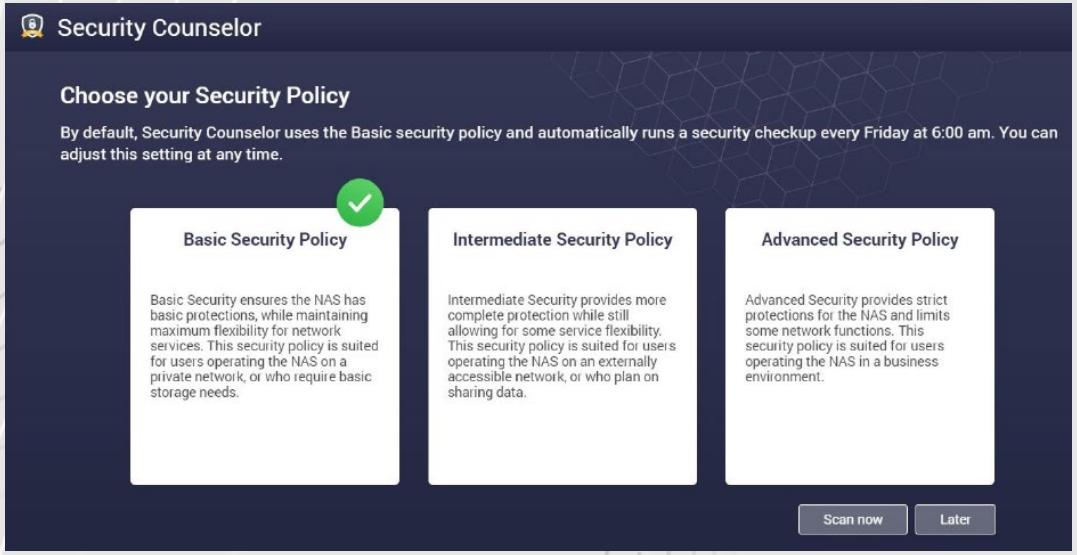
1. Download Security Counselor fra App Center

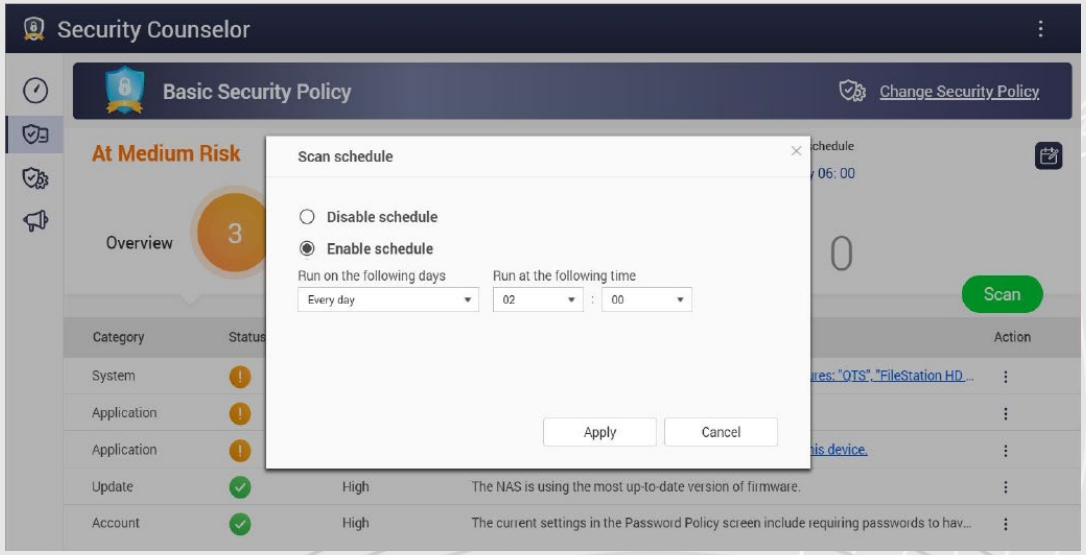
2. Vælg en sikkerhedspolitik, og klik på scan nu

3. For at lave en tidsplan: gå til sikkerhedstjekket (grøn)

4. Gå til Scanningsplan (rød)

5. Vælg din ønsket frekvens og klik anvend





Avancerede indstillinger

Krypteret forbindelse

Brug krypterede forbindelser

Hvis du vil oprette forbindelse til din QNAP-enhed uden for dit eget netværk, bør du kryptere din forbindelse. Det beskytter udefrakommende mod at kunne læse de data, der sendes til og fra din enhed. Dette kan gøres ved at bruge sikre forbindelser, for eksempel HTTPS og FTPS, hvor S'et står for "Secure". Dataoverførslerne er krypteret med certifikater, hvilket betyder, at enhederne kan verificere hinandens identiteter.

1. Gå til Kontrolpanel > System > Sikkerhed, og gå til SSL-certifikat og privat nøgle

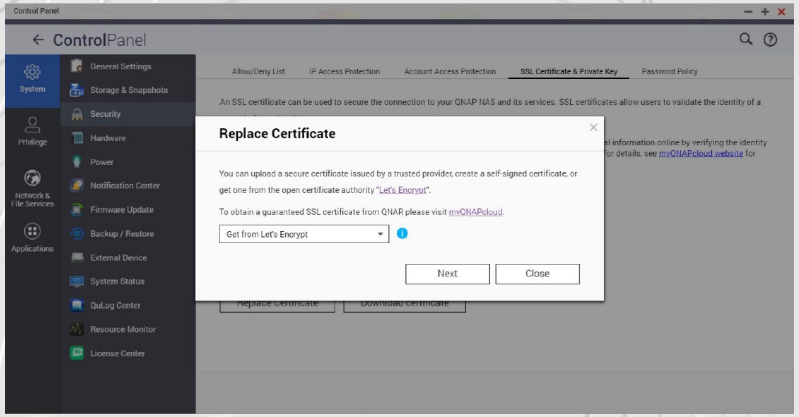
2. Klik på "Erstat certifikat"

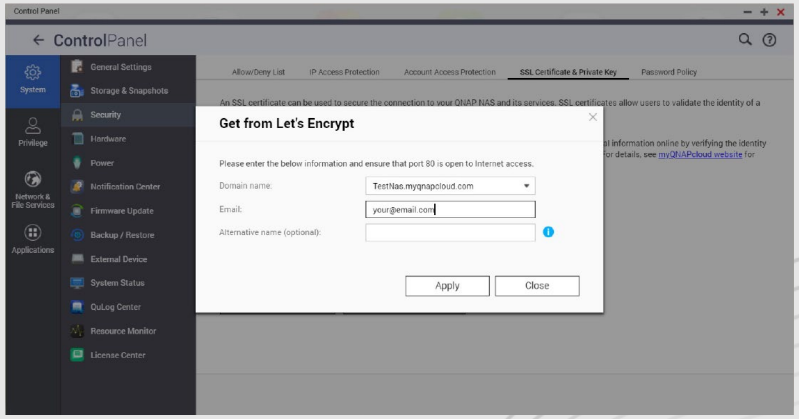
3. Vælg "Get from Let's Encrypt"

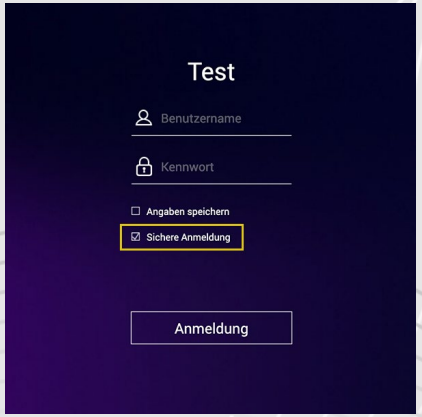
4. Under Domænenavn skal du indtaste det navn eller DDNS, hvor NAS'en kan nås

5. Indtast din e-mailadresse, du vil bruge til at registrere dig hos Let's Encrypt

6. Vælg Sikkert login, når du logger på din enhed







Avancerede indstillinger

Porte

Hvad er porte?

Porte tillader kommunikation mellem din computer og andre computere samt internettet. Firewalls lukker ubrugte porte for at forhindre malware i at blive distribueret til din computer over dem. Ved at aktivere "Port forwarding" kan du bruge onlinetjenester og andre applikationer over internettet, der kræver indgående forbindelser, eller tillade brugere fra internettet at få adgang til tjenester på dit hjemmenetværk.

Skift standardportene

Du kan øge dit systems sikkerhed ved at ændre portnumrene i din router fra de sædvanlige 21, 22, 80, 443, 8080 og 8081 til tilfældige portnumre. Kontakt din routerproducent om, hvordan du gør dette.

Obs! Tillad IKKE portvideresendelse for ubrugte tjenester (f.eks. SSH/Telnet)

Nedlukning af ubrugte porte kan reducere antallet af angrebsflader for potentielle angribere. Ved at aktivere port forwarding bliver port forwarding eksponeret for brugere på internettet – deaktiver derfor tjenester du ikke bruger.

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-nass-firmware
Security Counselor:	https://www.qnap.com/solution/security-counselor/en-us/