Tietoturvaopas

Ohjeita NAS-laitteen suojaamiseen

Tietoturvaesite – Perusasioita, joita ei pidä jättää huomiotta

NAS-LAITTEEN ENSIMMÄISELLÄ KÄYNNISTYSKERRALLA

Järjestelmänvalvoja

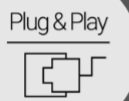
Älä käytä oletusasetuksia!
Luo uusi järjestelmänvalvojatili

Salasanat

Valitse turvalliset
salasanakäytännöt

Kaksivaiheinen vahvistus

Parantaa käyttäjätilien
tietoturvaa



UPnP

Ehkäise hyökkäyksiä poistamalla
Plug and Play käytöstä

JOKAPÄIVÄISET TEHTÄVÄT

Varmuuskopiointi

Varmuuskopioi useisiin
sijainteihin!
Noudata 3-2-1-strategiaa

Tilannevedokset

Estä datan menetys
tallentamalla se säännöllisesti

Päivitykset

Pidä sovellukset
ajan tasalla automaattisesti

VPN

Luo VPN-yhteys
etäkäyttöä varten

KERTALUONTOISET TEHTÄVÄT, JOTKA TARJOAVAT PYSYVÄÄ SUOJAA

QuFirewall

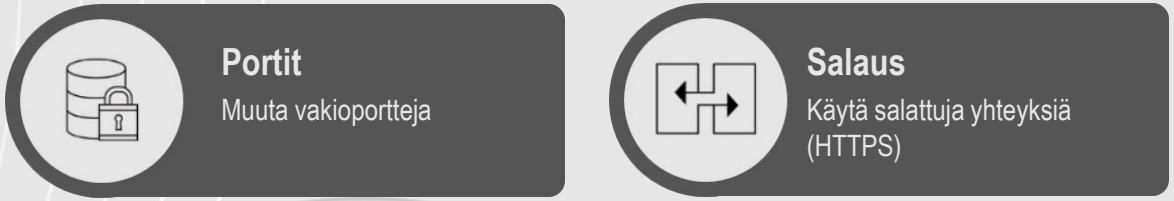
Lataa App Centeristä
ja ota käyttöön

Security Counselor

Lataa App Centeristä
ja ota käyttöön

Tietoturvaesite – Lisäasetuksia IT-osaajille

ASIANTUNTEVILLE KÄYTTÄJILLE



Johdanto

Tietoturvaopas

Tässä lyhyessä ja hyödyllisessä tietoturvaoppaassa käydään läpi asetuksia, jotka auttavat suojaamaan dataa optimaalisilla tavoilla.
Käyttömukavuus ja tietoturva ovat aina eri puolilla vaakaa, ja jokaisen käyttäjän on valittava itse, millaiseen tasapainoon ne asetetaan.
Tämä opas tarjoaa tiiviin yleiskatsauksen tärkeimpiin aiheisiin.
Yksityiskohtaisia lisätietoja ja ohjeita on saatavilla osoitteessa https://www.qnap.com/en.

Mitä ovat kiristysohjelmat?

Kiristysohjelmat ovat haitallisia ohjelmistoja, jotka estävät datan käytön lukitsemalla tietokoneen tai salaamalla tiedostoja. Jos uhri ei maksa kiristäjälle tämän vaatimaa summaa, tiedostot pysyvät salattuina eikä niitä voi enää käyttää.

Miten kiristysohjelmilta voi suojautua?

Kiristysohjelmat uhkaavat enenevissä määrin niin kotikäyttäjien kuin yritystenkin tietokoneita ja muita verkkoon yhdistettyjä laitteita. Hakkerit etsivät jatkuvasti uusia tapoja haittaohjelmien levittämiseen.
QNAP tuntee nämä riskit ja pyrkii jatkuvasti tarjoamaan parhaan mahdollisen suojan haittaohjelmia vastaan.
Alla olevissa esimerkeissä kerrotaan tapoja, joilla käyttäjät voivat suojautua tehokkaimmin omat tarpeensa huomioiden.

NAS-laitteen ensimmäisellä käyttökerralla

Järjestelmänvalvojatili

QTS:n järjestelmänvalvojatilin nimi on oletuksena ”admin”. Järjestelmän kannalta kriittisen tilin nimi kannattaa valita huolellisesti turvallisuussyistä: jos nimi on yleinen ja helposti arvattava, potentiaalisen hakkerin tarvitsee vain selvittää oikea salasana saadakseen koko järjestelmän haltuunsa. Tällaisten tapauksien varalta suosittelemme vahvasti luomaan uuden järjestelmänvalvojatilin ja poistamaan ”admin”-oletustilin käytöstä. Lisäksi järjestelmänvalvojatiliä on hyvä käyttää vain ylläpitotoimiin ja muihin järjestelmänvalvontaan liittyviin tehtäviin. QNAP NAS -laitteen varsinaista käyttöä ajatellen on suositeltavaa erottaa järjestelmänvalvojan ja käyttäjien toiminnot selkeästi toisistaan.

Huomioitavaa: ”Admin”-tili on mahdollista poistaa käytöstä vain QTS:n versiosta 4.1.2 alkaen.

LUO UUSI JÄRJESTELMÄN-VALVOJATILI

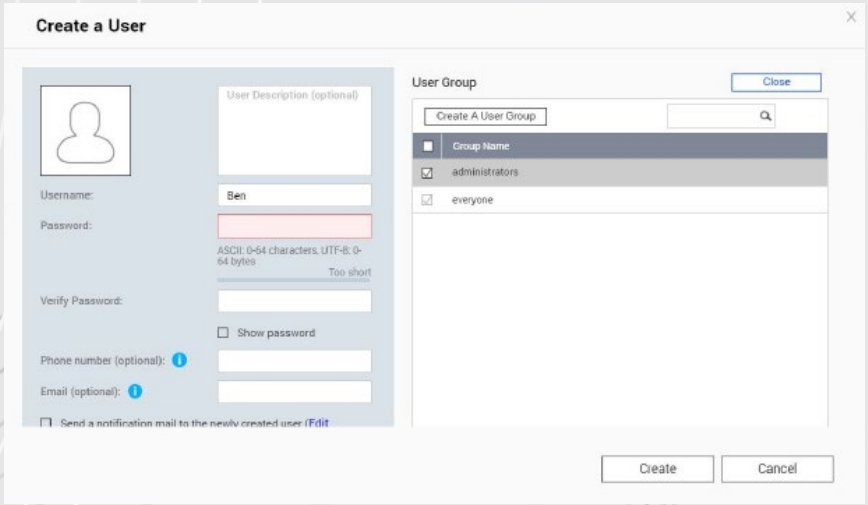
POISTA KÄYTÖSTÄ JÄRJESTELMÄN-VALVOJAN ”ADMIN”-TILI

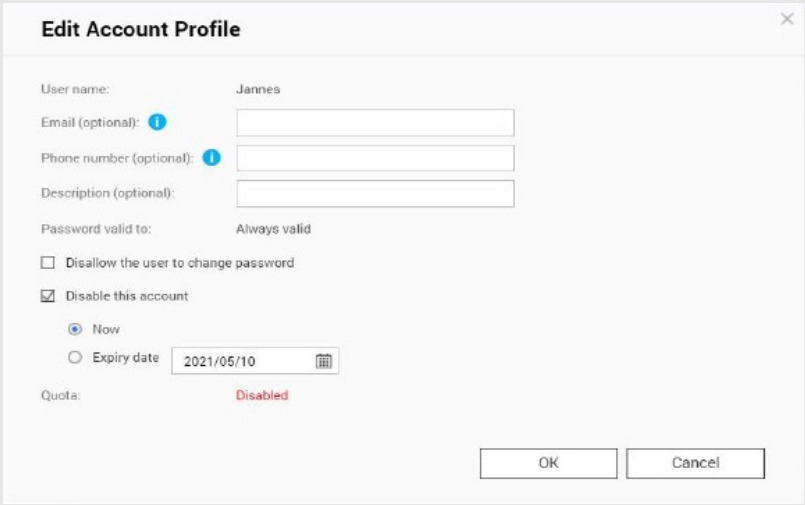
KÄYTÄ JÄRJESTELMÄN-VALVOJAN TILIÄ VAIN ASIAN-MUKAISIIN TEHTÄVIIN

NAS-laitteen ensimmäisellä käyttökerralla

”Admin”-käyttäjätilin poistaminen käytöstä

QNAP NAS -laite tarjoaa muutamia salasanoihin liittyviä asetuksia, jotka parantavat järjestelmän tietoturvaa huomattavasti. On hyvä muistaa, että jos QNAP NAS -laite on pelkästään henkilökohtaisessa käytössä, suositeltujen salasanasääntöjen noudattaminen on yksinomaan käyttäjän vastuulla. Turvallisten salasanojen perusperiaatteet ovat yksinkertaiset:





Uuden järjestelmänvalvojatilin luominen

1. Kirjaudu sisään QTS:ään käyttämällä ”admin”-tiliä.

2. Valitse Control Panel (Ohjauspaneeli) > Users (Käyttäjät).

3. Luo käyttäjätili (tässä esimerkissä ”Ben”) ja lisää se Administrators (Järjestelmänvalvojat) -käyttäjäryhmään.

”Admin”-tilin poistaminen käytöstä

1. Kirjaudu sisään QTS:ään Ben-käyttäjätilillä.

2. Valitse Control Panel (Ohjauspaneeli) > Users (Käyttäjät) ja muokkaa ”admin”-tilin profiilia.

3. Napsauta Disable this account (Poista tämä tili käytöstä) -painiketta ja valitse OK.

NAS-laitteen ensimmäisellä käyttökerralla

Salasanakäytännöt

QNAP NAS -laite tarjoaa muutamia salasanoihin liittyviä asetuksia, jotka parantavat järjestelmän tietoturvaa huomattavasti.
On hyvä muistaa, että jos QNAP NAS -laite on pelkästään henkilökohtaisessa käytössä, suositeltujen salasanasääntöjen noudattaminen on yksinomaan käyttäjän vastuulla. Turvallisten salasanojen perusperiaatteet ovat yksinkertaiset:

Riittävän pitkä

Erikoismerkit

Isot ja pienet kirjaimet

Samaa salasanaa ei koskaan saa käyttää eri sovelluksissa

Vaihda salasana säännöllisesti

Jos QNAP NAS -laitteella on useita käyttäjiä, järjestelmänvalvojan on hyvä asettaa salasanoille tietyt säännöt, joiden noudattamista laite valvoo. Näin varmistetaan, että kaikki seuraavat yllä mainittuja sääntöjä. Seuraavalla sivulla on tästä lisätietoja.

NAS-laitteen ensimmäisellä käyttökerralla

Salasanakäytännöt

1. Valitse Control Panel (Ohjauspaneeli) > System (Järjestelmä) > Security (Tietoturva) > Password Policy (Salasanakäytäntö).

2. Valitse ehdot Password strength (Salasanan vahvuus) -kohdassa.

1. Uudessa salasanassa on oltava merkkejä vähintään kolmesta eri luokasta: pienet kirjaimet, isot kirjaimet, numerot ja erikoismerkit.

2. Samaa merkkiä ei saa toistaa salasanassa kolmesti tai useammin (esim. ”AAA”).

3. Käyttäjänimeä (edes takaperin kirjoitettuna) ei saa käyttää salasanana.

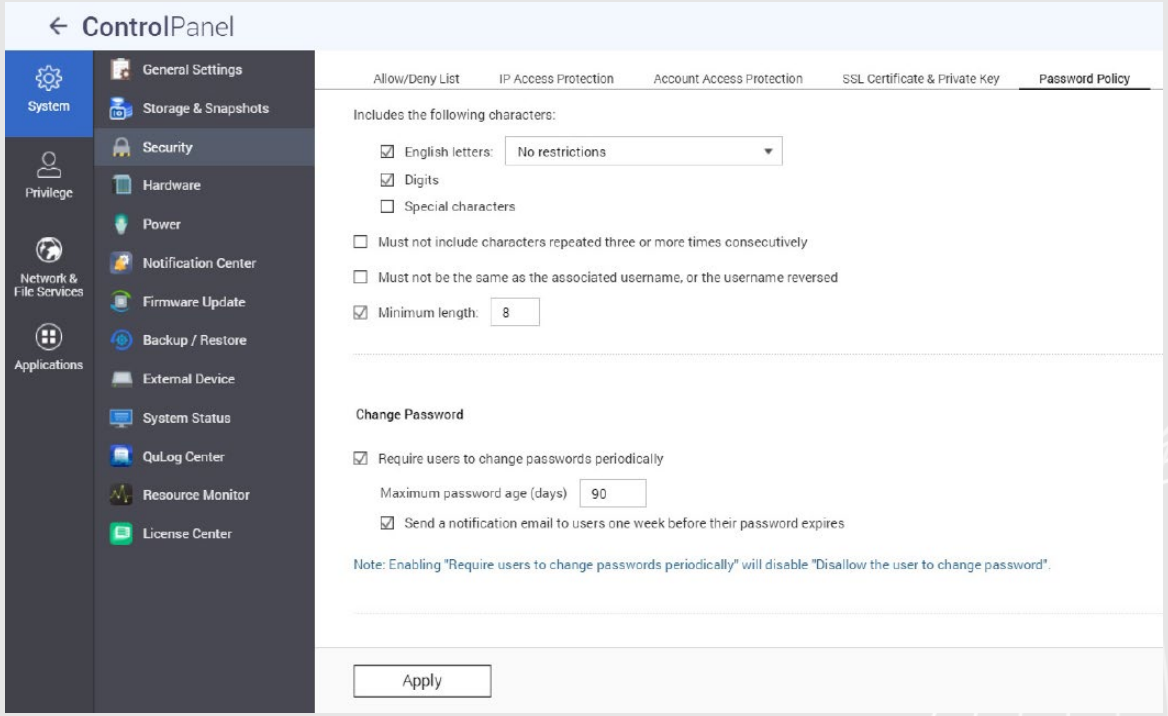
3. Ota Change Password (Vaihda salasana) -kohdassa käyttöön Require users to change passwords periodically (Vaadi käyttäjiä vaihtamaan salasana ajoittain) -asetus.

Tärkeää: Kun tämä asetus otetaan käyttöön, Prohibit users from changing the password (Estä käyttäjiä vaihtamasta salasanaa) -asetus poistetaan käytöstä.

1. Valitse enimmäisaika, jonka jälkeen salasana on vaihdettava.

2. Valinnainen: Valitse Send a notification email to users one week before their password expires (Lähetä käyttäjille sähköposti-ilmoitus viikkoa ennen salasanan vanhentumista) -asetus.

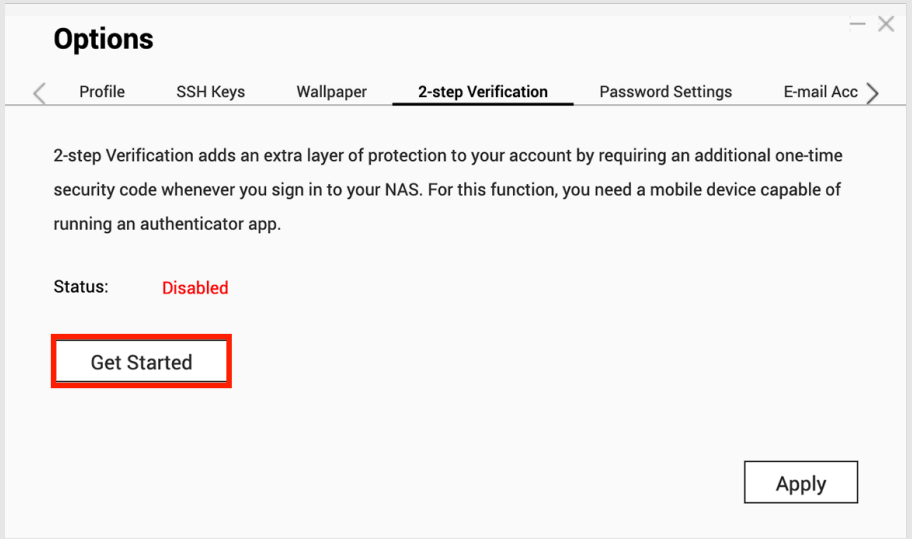
4. Napsauta Apply (Ota käyttöön).

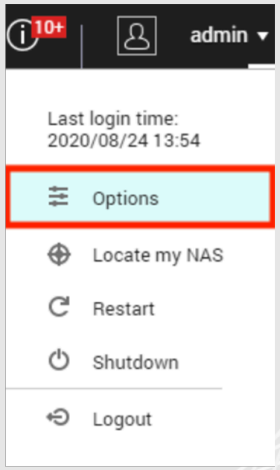


NAS-laitteen ensimmäisellä käyttökerralla

Kaksivaiheinen vahvistus

Kaksivaiheinen vahvistus parantaa käyttäjätilien tietoturvaa. Kun se on käytössä, kirjautuminen NAS-laitteelle edellyttää salasanan lisäksi kertakäyttöistä kuusinumeroista turvakoodia. Kaksivaiheisen vahvistuksen käyttöön tarvitaan mobiililaite sekä todennussovellus,
joka tukee Time-based one-time password (TOTP) -protokollaa. Yhteensopiviin sovelluksiin kuuluvat Google Authenticator (Android/iPhone/BlackBerry)
tai Authenticator (Windows Phone). Tämä toiminto voidaan ottaa käyttöön seuraavasti:





1. Asenna todennussovellus mobiililaitteelle.

2. Valitse ehdot Password strength (Salasanan vahvuus) -kohdassa.

3. Valitse Options (Asetukset) > 2-step Verification (Kaksivaiheinen vahvistus) ja napsauta Get Started (Aloita).

1. Määritä todennussovelluksen asetukset skannaamalla QR-koodi tai syöttämällä Secret Key (Salainen avain) -tunnus sovellukseen.

2. Vahvista asetukset syöttämällä sovelluksen luoma koodi NAS-laitteeseen.

3. Valitse vaihtoehtoinen vahvistustapa siltä varalta, että et voi käyttää mobiililaitettasi: sähköpostiin lähetettävä turvakoodi tai vastaaminen turvakysymykseen. Turvakoodin lähettäminen sähköpostiin edellyttää, että SMTP-palvelimen asetukset on määritetty oikein kohdassa Control Panel (Ohjauspaneeli) > Notification (Ilmoitus) > E-mail (Sähköposti).

NAS-laitteen ensimmäisellä käyttökerralla

Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) -tekniikkaa käytetään eri valmistajien laitteiden (reitittimet, audiolaitteet, tulostimet, älytelevisiot ja niin edelleen) hallitsemiseen. Sen avulla verkossa olevat laitteet voivat ymmärtää toisiaan ja tiettyjä toimintoja voidaan käyttää automaattisesti ilman käyttäjän osallistumista. UPnP:tä käyttämällä QNAP NAS -laite voi esimerkiksi käskeä reititintä hyväksymään tietyt saapuvat yhteyspyynnöt kaikissa tilanteissa. Käyttäjän on tässäkin tapauksessa löydettävä sopiva tasapaino käyttömukavuuden ja turvallisuuden väliltä. Kokemattomampia käyttäjiä suosittelemme poistamaan UPnP-ominaisuuden käytöstä reitittimen ja QNAP NAS -laitteen asetuksissa. Ohjeita reitittimen asetusten muuttamiseen on reitittimen valmistajan tarjoamissa käyttöohjeissa.

Tärkeää:

Jos UPnP on otettu käyttöön reitittimen asetuksissa, kaikki kotiverkkoon yhdistetyt ohjelmistot ja laitteet voivat määrittää reitittimen asetuksia haluamillaan tavoilla. Tämä voi johtaa esimerkiksi tiettyjen palomuurin porttien avaamiseen, mikä tarjoaa väylän ulkopuolelta tuleville hyökkäyksille.

Suosittelemme vahvasti, että NAS-laite yhdistetään verkkoon reitittimen välityks ei suoraan modeemin kautta.

UPnP-portinsiirron poistaminen käytöstä QNAP NAS -laitteen asetuksissa

1. Avaa myQNAPcloud > Auto Router Configuration (Reitittimen automaattinen määritys).

2. Poista valinta Enable UPnP Port forwarding (Ota UPnP-portinsiirto käyttöön) -ruudusta ja napsauta Apply (Ota käyttöön).

Jokapäiväiset tehtävät

3-2-1-varmuuskopiointistrategia

Varmuuskopiointi

Jokaisen käyttäjän on päätettävä itse, millä tavalla ja kuinka usein dataa varmuuskopioidaan. Tässä kysymyksessä ratkaisevassa asemassa ovat tietoturvaan liittyvät tarpeet, datan tärkeys ja saatavilla olevat vaihtoehdot.

Tärkeän datan varmuuskopiointiin on kuitenkin olemassa nyrkkisääntö, jota on hyvä noudattaa.

Tärkeää: *RAID ei ole varmuuskopio, vaan se suojaa dataa kiintolevyn ongelmilta. Tilannevedokset auttavat suojamaan tietokonetta kiristysohjelmia käyttäviltä hyökkäyksiltä.*

3-2-1-varmuuskopiointistrategia

Huolellisuus ja järkevä toiminta (ohjelmistojen päivittäminen säännöllisesti sekä epäluotettavien sähköpostien ja tuntemattomien sivustojen jättäminen avaamatta) ovat parhaat tavat suojautua haittaohjelmistoilta, mutta datan varmuuskopiointi on myös erittäin tärkeää.

Yksikään varmuuskopiointisuunnitelma ei ole aukoton, mutta 3-2-1-strategia on hyvä lähtökohta: tärkeistä tiedostoista luodaan kolme varmuuskopiota, joita säilytetään vähintään kahdella erilaisella tallennuslaitteella, ja lisäksi yhtä kopiota säilytetään toisessa sijainnissa.

Tärkeästä datasta tulee luoda vähintään **kolme kopiota:** yksi päätiedosto ja kaksi varatiedostoa.

Arkistoja suojataan erilaisilta vaaroilta tallentamalla ne **kahdelle eri** tallennusvälineelle.

Yhtä varmuuskopiota säilytetään toisessa sijainnissa (kodin tai yrityksen tilojen ulkopuolella).

Jokapäiväiset tehtävät

Tilannevedokset

Mitä ovat tilannevedokset?

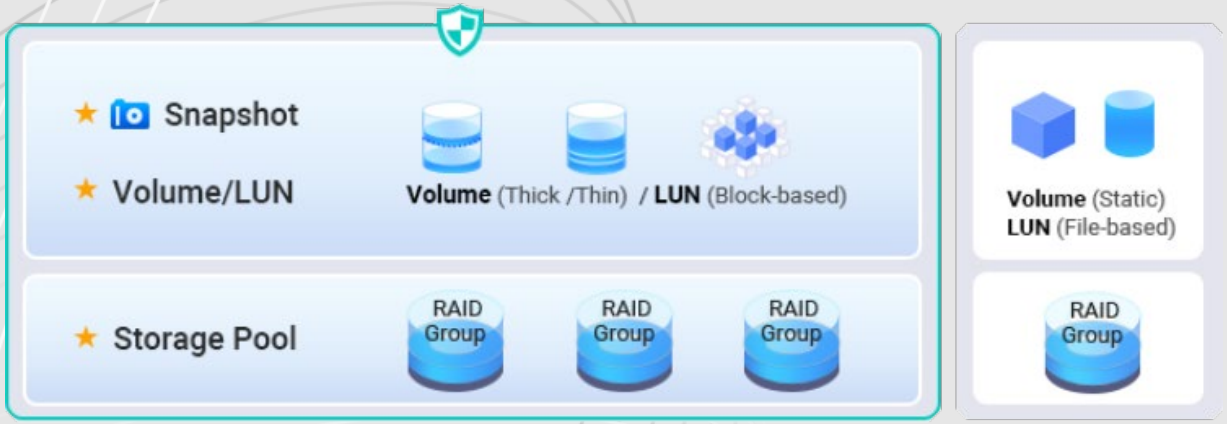
Tilannevedokset ovat QNAP NAS -laitteelle tallennetun datan näköistiedostoja. Kun tilannevedos luodaan ensimmäisen kerran, se kattaa koko tallennustilan. Sen jälkeen luotavat tilannevedokset huomioivat vain edellisen kerran jälkeen tehdyt muutokset. Tilannevedokset perustuvat lohkoihin, joten ne käyttävät tilaa erittäin tehokkaasti.

Tärkeää:

Tilannevedos ei ole varmuuskopio. Jos sisältö poistetaan tai siihen tehdään muutoksia vahingossa, tilannevedoksen avulla on mahdollista käyttää sen aiempaa versiota.

Yksityiskohtaisempia tietoja tästä aiheesta on saatavilla verkkosivustollamme:
https://www.qnap.com/solution/snapshots/en-us/

Tilannevedosten käyttöönotto



Jokapäiväiset tehtävät

Automaattiset päivitykset

Päivitykset

On tärkeää pitää NAS-laitteen laiteohjelmisto ajan tasalla. QNAP tekee jatkuvasti töitä sulkeakseen mahdolliset tietoturva-aukot ja myös lisätäkseen uusia ominaisuuksia järjestelmään. Päivitykset on siis hyvä ottaa käyttöön nopeasti, jotta data pysyy mahdollisimman tehokkaasti suojattuna. Jos QNAP NAS -laite on yhteydessä internetiin eikä oletusasetuksia ole muutettu, se tarkistaa laiteohjelmiston uusimmat päivitykset ja ilmoittaa niistä automaattisesti. Päivitysten asentamista ei saa laiminlyödä. On myös hyvä muistaa, että päivityksen yhteydessä QNAP NAS -laite on käynnistettävä uudelleen, jolloin laitetta ei voi käyttää 5–10 minuuttiin.

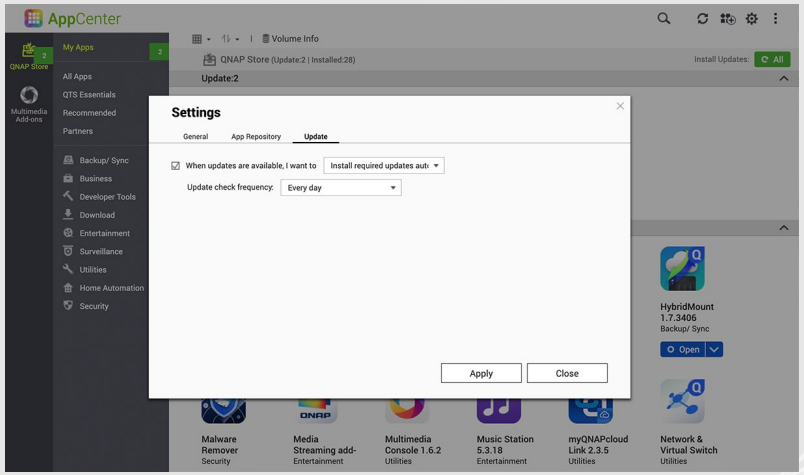
Uusimman laiteohjelmiston voi asentaa myös manuaalisesti. Tämä on tarpeen silloin, kun QNAP NAS -laite ei voi tarkistaa ja ladata päivityksiä automaattisesti, koska se ei ole yhteydessä internetiin. Mahdollisesti saatavilla olevat laiteohjelmistopäivitykset voi tarkistaa seuraavasti:

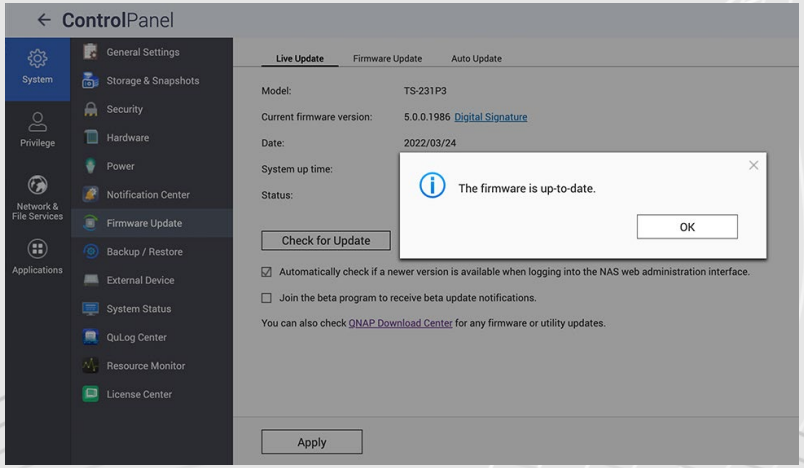
Laiteohjelmiston päivittäminen reaaliaikaisesti

1. Kirjaudu sisään järjestelmänvalvojan tilillä.
2. Avaa Control Panel (Ohjauspaneeli) > Firmware Update (Laiteohjelmiston päivitys).
3. Avaa Live Update (Reaaliaikainen päivitys).
4. Napsauta Check for update (Tarkista päivitykset).

Sovellusten päivittäminen automaattisesti

1. Avaa App Center.
2. Avaa Settings (Asetukset).
3. Avaa Update (Päivitys).
4. Valitse When updates are available… (Kun päivityksiä on saatavilla…).
5. Valitse Install all updates automatically (Asenna kaikki päivitykset automaattisesti).





Jokapäiväiset tehtävät

VPN

Mikä on VPN?

VPN (Virtual Private Network) tarkoittaa näennäistä yksityisverkkoa. Tässä tapauksessa sen avulla muodostetaan suojattu yhteys QNAP NAS -laitteeseen käyttäjän ollessa tien päällä. QNAP NAS -laite ylläpitää VPN-palvelinta, kun taas käyttäjän laitteella toimii erityinen VPN-ohjelmisto. VPN-palvelin ja -ohjelmisto yhdistetään toisiinsa tunnelilla internetin kautta. Tämän menetelmän etuna on, että yhteyttä ei voi käyttää ilman lupaa, koska sitä suojataan todennus- ja salaustekniikoilla. VPN-yhteys vastaa siis tilannetta, jossa molemmat laitteet olisi kirjattu sisään samaan verkkoon. Tällöin myös paikalliset resurssit ovat käytettävissä vaivattomasti. Kun VPN on otettu käyttöön, taatusti suojatun yhteyden muodostaminen kotiverkkoon onnistuu helposti yhä uudelleen. Suosittelemme muodostamaan etäyhteyden aina VPN:n kautta. Vaikka se heikentää tiedonsiirtonopeutta, yhteys on turvallinen.

Miten VPN otetaan käyttöön ja miten se toimii?

Yksityiskohtaiset määritysohjeet ovat saatavilla ohjesivustollamme:
https://www.qnap.com/en/how-to/tutorial/article/how-to-set-up-and-use-qvpn

Suositus etäkäyttöä varten

myQNAPcloud Link ja VPN (edellyttää portinsiirron käyttöä VPN-palveluporteille, suosittelemme QuFirewallin käyttöönottoa tietoturvan parantamiseksi)

Kertaluontoiset tehtävät

QuFirewall

Mikä on QuFirewall?

QuFirewall on QNAP-laitteelle suunniteltu palomuurin hallintaohjelmisto. Helppokäyttöisen ja tehokkaan profilointijärjestelmänsä avulla QuFirewall tukee laitteeseen muodostettavien yhteyksien hallintaa ja todennusta. QNAP suosittelee asentamaan QuFirewallin QNAP NAS -laitteelle ja sallimaan vain tietyn alueen tai aliverkon IP-osoitteet.

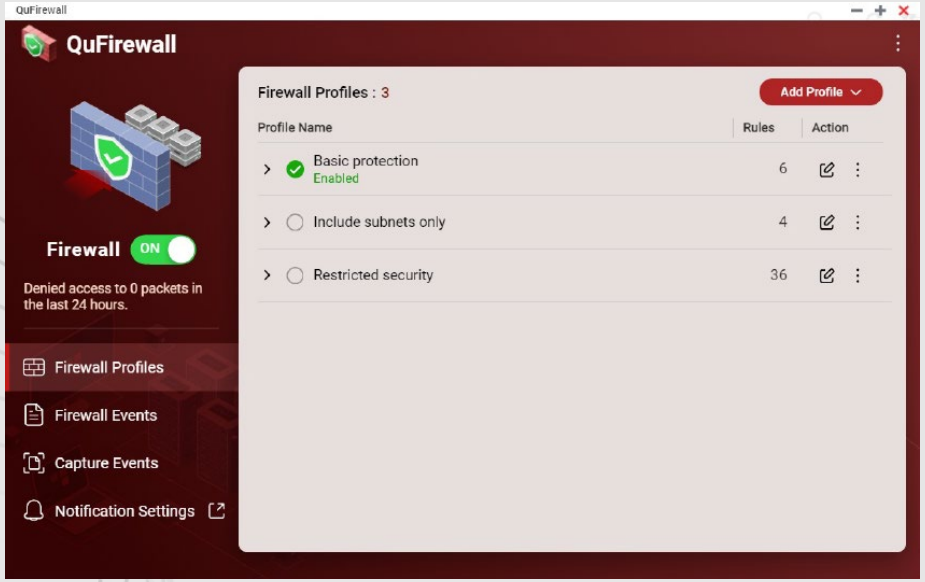
QuFirewallin käyttöönotto

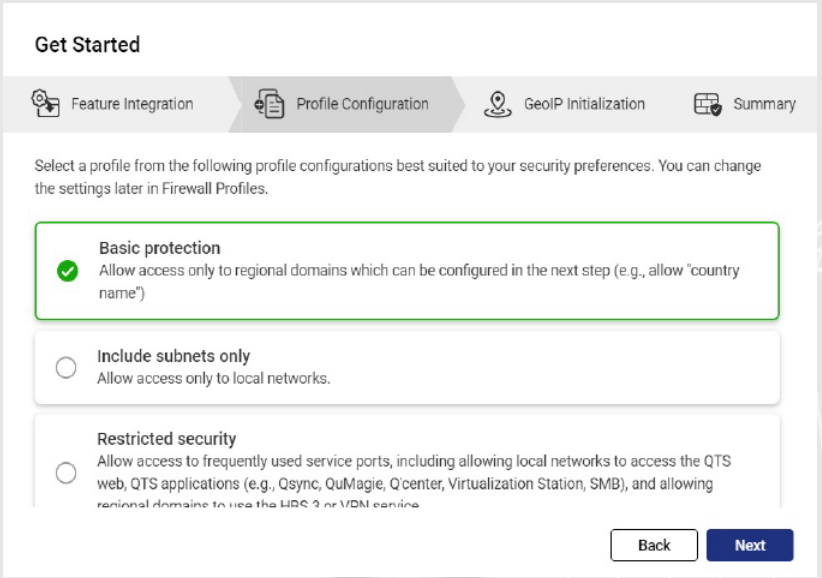
1. Avaa App Center ja asenna QuFirewall.

2. Valitse profiilimääritys.

3. Valitse alue.

4. Napsauta Finish (Valmis).





Kertaluontoiset tehtävät

Security Counselor

Mikä on Security Counselor?

Security Counselor on QNAP NAS -laitteen käyttämä tietoturvaportaali. Se tarkistaa järjestelmän heikkouksien varalta ja tarjoaa suosituksia, jotka auttavat suojaamaan dataa erilaisilta hyökkäyksiltä. Koska erilaisilla verkkoympäristöillä on erilaisia vaatimuksia, valittavissa on kolme erilaista oletustietoturvakäytäntöä: Basic (Perustaso), Intermediate (Keskitaso) ja Advanced (Edistynyt). Security Checkup (Tietoturvatarkistus) -toiminto tarkistaa järjestelmän valitun käytännön mukaisesti. Lisäksi tietoturvakäytännön asetukset voi määrittää manuaalisesti valitsemalla Custom (Mukautettu) -vaihtoehdon.

Basic (Perustaso)

Intermediate (Keskitaso)

Advanced (Edistynyt)

Custom (Mukautettu)

Tietoturvatarkistukset voi suorittaa manuaalisesti, mutta suojauksen tehostamiseksi niille voi myös määrittää säännöllisen aikataulun.

Aikataulun voi valita eri vaihtoehdoista (päivittäin, arkisin, viikonloppuisin tai tiettyinä viikonpäivinä), jotta tarkistus ei häiritse työntekoa.

Kun tarkistuksen tuloksia napsautetaan, Security Counselor auttaa avaamaan niihin liittyvän järjestelmäosion ja muuttamaan tarvittavia asetuksia NAS-laitteen suojaamiseksi.

Kertaluontoiset tehtävät

Security Counselor

Security Counselorin käyttöönotto

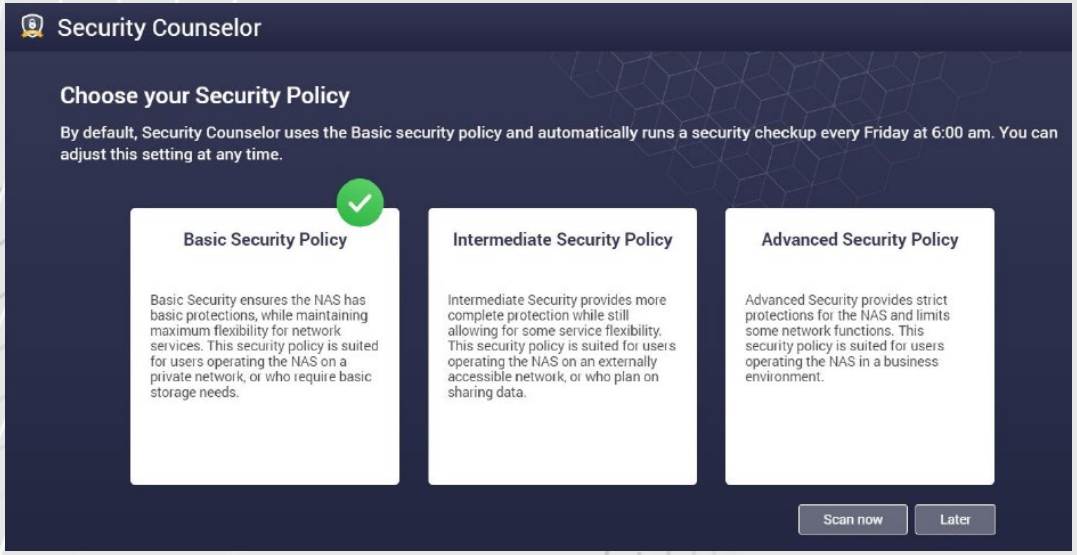
1. Avaa App Center ja lataa Security Counselor.

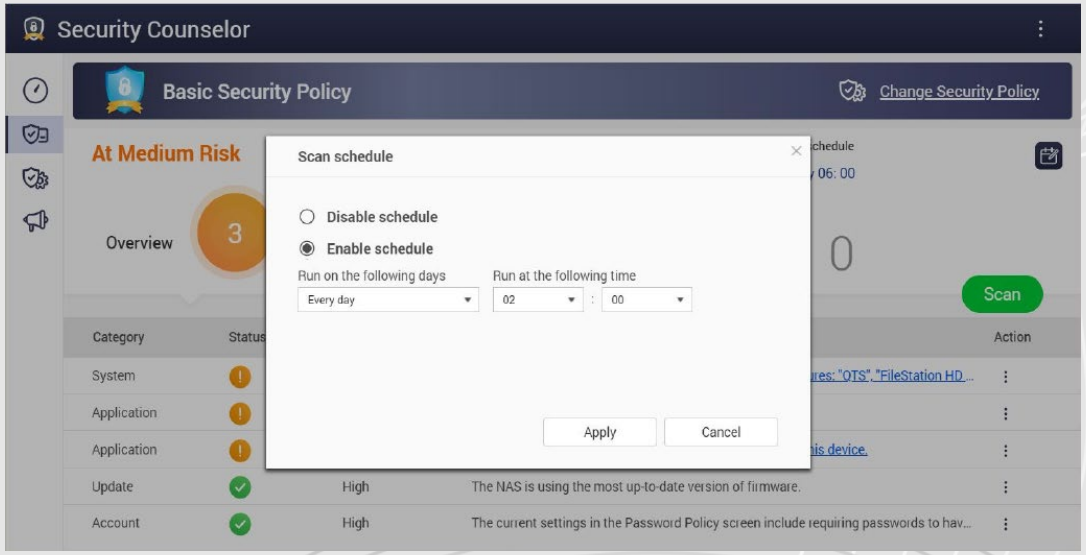
2. Valitse haluamasi Security Policy (Tietoturvakäytäntö) -asetus ja napsauta Scan now (Tarkista nyt).

3. Jos haluat luoda aikataulun, valitse Security Checkup (Tietoturvatarkistus) -kohta (vihreä).

4. Valitse Scan schedule (Tarkistusaikataulu) -kohta (punainen).

5. Valitse haluamasi ajankohta ja napsauta Apply (Ota käyttöön).





Lisäasetukset

Salattu yhteys

Salattujen HTTPS-yhteyksien käyttäminen

On suositeltavaa varmistaa, että data salataan, kun QNAP NAS -laitteeseen muodostetaan yhteys käyttäjän oman verkon ulkopuolelta. Tällä tavalla kolmannet osapuolet eivät pääse ”lukemaan” siirrettävää dataa. Tämä onnistuu käyttämällä suojattua yhteyttä, kuten HTTPS-yhteyttä HTTP:n sijaan tai FTPS-yhteyttä FTP:n sijaan. S-kirjain on lyhenne sanasta ”Secure”, joka tarkoittaa suojattua. Tiedonsiirto salataan nyt käyttämällä varmennetta, jolla vahvistetaan yhteyden muodostavan tahon henkilöllisyys.

1. Valitse Control Panel (Ohjauspaneeli) > System (Järjestelmä) > Security (Tietoturva) > SSL Certificate & Private Key (SSL-varmenne ja yksityinen avain).

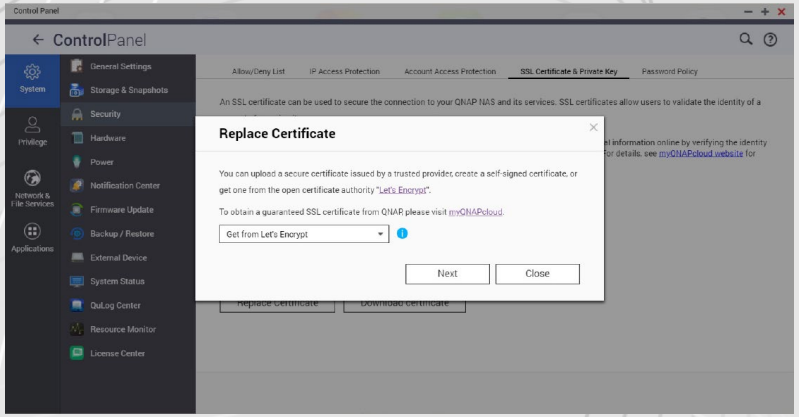
2. Napsauta Replace Certificate (Korvaa varmenne).

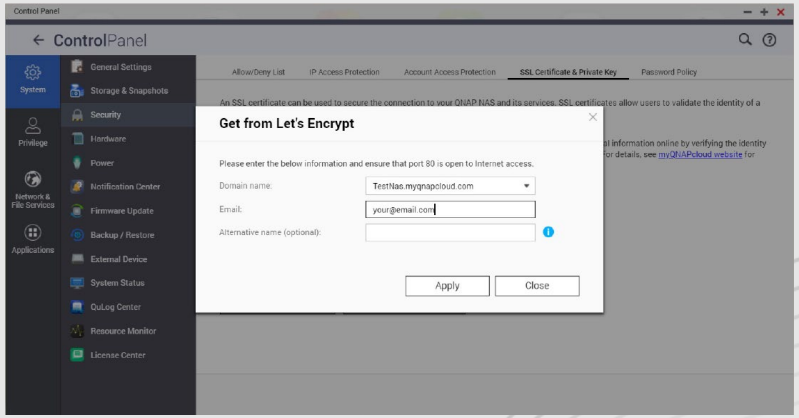
3. Valitse Get from Let’s Encrypt (Nouda Let’s Encrypt -palvelusta).

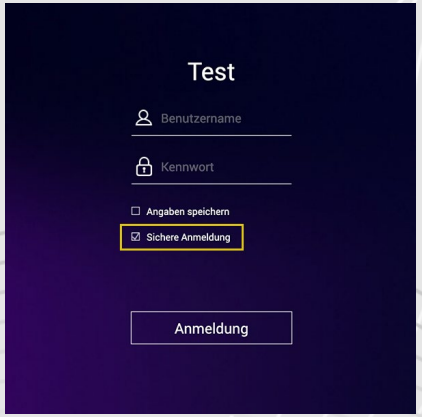
4. Syötä Domain name (Toimialuenimi) -kohdassa nimi tai DDNS-tunnus, jolla yhteys NAS-laitteeseen voidaan muodostaa.

5. Syötä sähköpostiosoite, jota käytetään Let’s Encrypt -palveluun rekisteröitymiseen.

6. Kun kirjaudut sisään verkkokäyttöliittymän kautta, valitse Secure login (Suojattu kirjautuminen).







Lisäasetukset

Portit

Mitä ovat portit?

Porttien ansiosta tietokoneet voivat olla yhteydessä toisiinsa ja internetiin. Palomuuri sulkee tarpeettomat portit, jotta tietokoneelle ei pääse haittaohjelmia niiden kautta. Portinsiirron avulla voidaan käyttää verkkopalveluja ja -sovelluksia, jotka sallivat internetistä saapuvat yhteydet. Lisäksi sen avulla internetissä olevat käyttäjät voivat hyödyntää kotiverkossa toimivia verkko- ja etäpalvelimia ja muita palveluja.

Oletusporttien muuttaminen

On suositeltavaa vaihtaa reitittimen asetuksissa määritetyt oletusportit (kuten 21, 22, 80, 443, 8080 ja 8081) satunnaisesti valittuihin porttinumeroihin. Esimerkiksi portin 8080 voisi vaihtaa portiksi 9527. Ohjeita näiden muutosten tekemiseen voi pyytää reitittimen valmistajalta.

PORTINSIIRTOA EI TULE OTTAA KÄYTTÖÖN ”järjestelmäportille” eikä tarpeettomille palveluporteille (esim. SSH tai Telnet)

Tarpeettomien palveluporttien sulkeminen portinsiirron ulkopuolelle voi ehkäistä hyökkäyksiä. Kun portinsiirto on käytössä, kuka tahansa voi muodostaa yhteyden näihin palveluportteihin internetin kautta.

Ohjeita

Varmuuskopiointi:	https://www.qnap.com/en/how-to/tutorial/article/hybrid-backup-sync
Järjestelmänvalvojatili:	https://www.qnap.com/en/how-to/faq/article/can-i-rename-the-default-admin-account
Salasanakäytäntö:	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?
Salaus:	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
Portinsiirto:	https://www.qnap.com/en/how-to/faq/article/how-do-i-set-up-port-forwarding-on-the-nas
QuFirewallin käyttö:	https://www.qnap.com/en/how-to/tutorial/article/how-to-use-qufirewall
Päivitykset:	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/