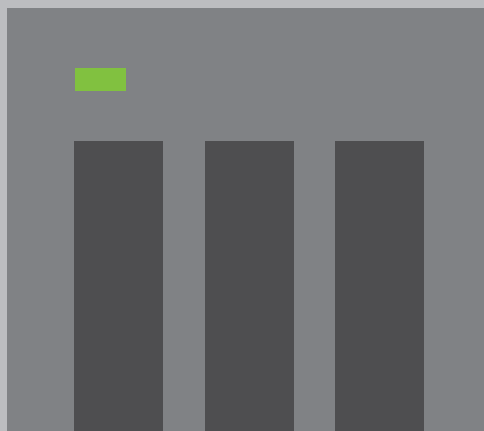


2 0 2 3

Säkerhetsguide



2 0 2 3

Säkerhetsguide

INDEX

- 1 Förord
- 2 Vanliga attacker
- 3 Grundläggande koncept för nätverksutrustning
- 4 Olika sätt att ansluta från Internet till NAS

Undvik att exponera NAS:en för Internet

- 8 Anslut NAS:en på rätt sätt
- 9 Kontrollera routerinställningar
- 12 Kontrollera NAS-inställningar
- 15 Kontrollista för nätverksrelaterade inställningar

NAS-säkerhetsinställningar

- 17 Konfigurera systemaviseringar
- 24 Aktivera automatisk uppdatering av inbyggd programvara (QTS/QuTS hero)
- 25 Inställningar för appuppdatering
- 27 Inaktivera eller ta bort onödiga funktioner
- 29 Inaktivera Telnet/SSH
- 30 Stärka systemkontosäkerheten
- 34 Ställa in lösenordsprincip
- 35 Aktivera åtkomstskydd (IP/konto)
- 36 Aktivera 2-stepsverifiering (2SV)
- 39 Ändra standardportar
- 40 Visa åtkomstloggar
- 41 Installera och aktivera säkerhetsappar
- 42 Security Counselor
- 45 Malware Remover

46 QuFirewall

51 Aktivera schemalagt snapshots

53 Ställa in princip för snapshottradering

54 Kontrollista för NAS-säkerhetsinställningar

Förord

QNAP fäster stor vikt vid säkerhet. Inför ökande hot har QNAP kontinuerligt förbättrat hårdvaru- och programvarudesign för att ge användarna lösningar som är både säkra och praktiska.

QNAP:s PSIRT (Product Security Incident Response Team) ansvarar för att hantera säkerhetsproblem som är förknippade med QNAP-produkter. Förutom att hantera incidenter som handlar om cybersäkerhet så hanterar PSIRT även rapportering, utredning, sanering och tillkännagivande av sårbarheter i olika produkter.

QNAP ser det som sitt uppdrag att förbättra produktsäkerheten. Tidigare utformades produkter för att vara behändigare och enklare för användare att installera och använda. De ökande cyberattacker mot nätverksanslutna enheter under de senaste åren har även förändrat QNAP:s perspektiv på produktdesign och därför har produktdesignen gått över till Security by Design (inbyggd säkerhet) för att fungera som en portvakt för användare och se till att användare kan hantera förekommande hot.

Självstudiekursen hjälper användare så att de konfigurerar NAS:en korrekt för förbättrad säkerhet. Om du har några frågor ber vi dig kontakta vår tekniska support för hjälp:



För information om sårbarheter och säkerhetsrelaterad incidentinformation ber vi dig ta referens från och prenumerera på QNAP:s säkerhetsråd:

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



QNAP:s kundtjänst:

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



Vanliga attacker

För att känna till hur du försvarar dig mot cyberattacker måste du känna till hur de initieras. Beträffande attacker på NAS initieras de flesta attacker via Internet. Det handlar ofta om två typer av attacker: "lösenordsknäckning" och "sårbarhetsattacker". Här kan "sårbarhetsattack" delas in i "N-dag" och "0-dag".

Begreppet "N-dag" avser att utnyttja en korrigerad sårbarhet för att initiera en attack och de flesta nuvarande aktiva attackerna hör till den kategorin. Du kan effektivt försvara dig mot sådana attacker genom att säkerställa att du alltid installerar de senaste säkerhetskorrigeringarna och uppdateringarna.

Begreppet "0-dag" avser en okänd sårbarhet utnyttjas för att initiera en attack och leverantörer kan bara utfärda säkerhetskorrigeringar efter att denna konstaterats. Det enda effektiva försvaret mot dessa attacker är att förhindra angripare från att ansluta till enheten.

Följande tabell visar svaren på olika attacker, avsedda för användares referens.

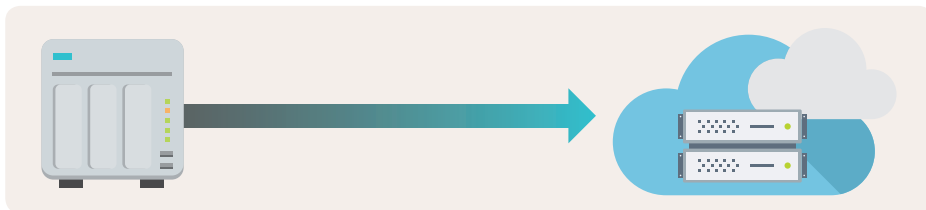
Svar	Attacker		
	Lösenordsknäckning	Sårbarhetsattack (N-dag)	Sårbarhetsattack (0-dag)
Undvik exponering för Internet	V	V	V
Uppdatera programvara (system och appar)	X	V	Δ
Aktivera automatisk uppdatering (system och appar)	X	V	Δ
Använd starka lösenord för alla konton	V	X	X
Inaktivera standardkontot "admin"	V	X	X
Aktivera 2-stegsverifiering	V	X	X
Aktivera åtkomstskydd	Δ	X	X
Aktivera brandvägg	Δ	Δ	Δ
Ta emot systemaviseringar	Δ	Δ	Δ
Ändra standardportar	Δ	Δ	Δ
Inaktivera/ta bort onödiga funktioner	Δ	Δ	Δ

V: Effektiv X: Inte effektiv Δ: Möjligen effektiv (innebär att attacken kan mildras eller att risken för att bli attackerad blir lägre)

"Undvik exponering för Internet" kan effektivt förhindra angripare från att ansluta till och initiera attacker på din enhet. Den här självstudiekursen börjar med "Undvik exponering för Internet" och tillhandahåller sedan en komplett självstudiekurs om "NAS-säkerhetsinställningar" för att förbättra defensiva funktioner på NAS:en.

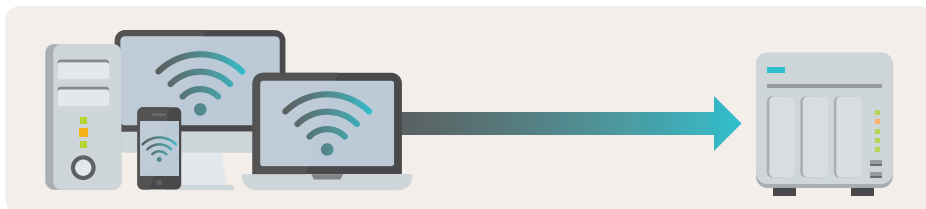
Som nätverksansluten enhet har NAS:en två anslutningsriktningar.

01 | Extern NAS-anslutning



En NAS kräver vanligtvis en extern anslutning för att fungera som avsett. Det innebär exempelvis grundläggande systemfunktioner som automatiska uppdateringar och för att skicka meddelanden. Om du dessutom behöver säkerhetskopiera data från NAS:en till ett offentligt moln eller använda NAS:en till att säkerhetskopiera data från andra enheter eller offentliga moln (exempelvis virtuella maskiner, Google Workspace eller Microsoft 365), datorer eller servrar, måste NAS:en kunna initiera utgående anslutningar.

02 | Andra enheter (exempelvis datorer, mobila enheter eller andra servrar) som ansluter till NAS:en



Om du behöver använda några funktioner eller tjänster som NAS:en tillhandahåller, inklusive åtkomst till filer och att använda inställningsgränssnittet, måste du kunna initiera anslutningar till NAS:en.

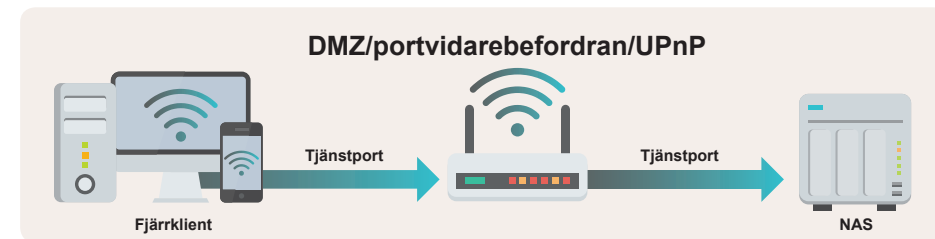
Om din router inte har en DMZ, portvidarebefordran eller UPnP så blockerar routern trafiken från Internet. Endast enheter i det lokala nätverket har åtkomst till NAS:en.

När routern är aktiverad och ovanstående funktioner är inställda, kan alla på ansluta till den öppna porten från Internet och sedan vidarebefordra till NAS:en i enlighet med reglerna på routern för att sedan logga in och använda de berörda funktionerna normalt. Dock ger det även hackare möjlighet att attackera med lösenordknäckning eller utnyttjande av programvarusårbarheter och det leder till säkerhetsrisker.

01 | Aktivera och konfigurera DMZ, portvidarebefordran eller UPnP på routern

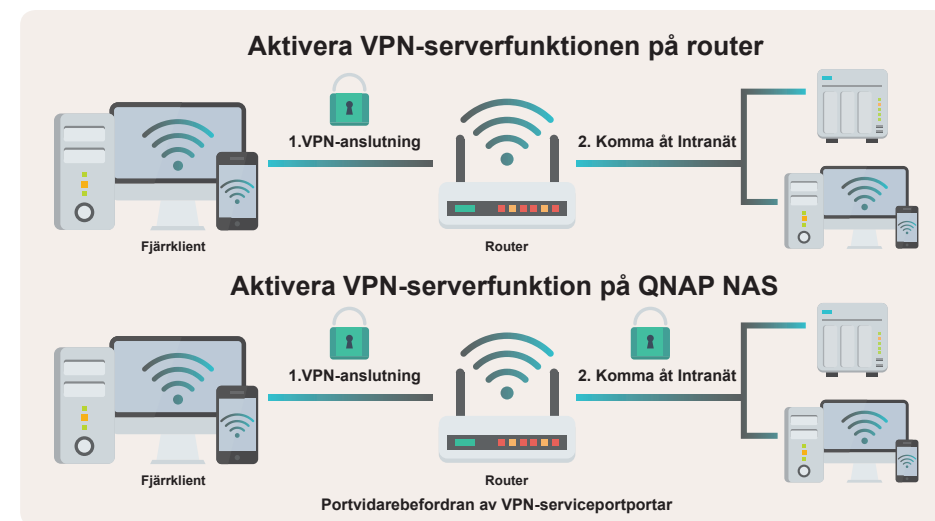
Denna metod medför säkerhetsrisker. Om du inte är expert på nätverkskonfiguration och förstår vilka risker det medför rekommenderar **QNAP inte att du använder den***. Emedan routern skickar trafik till intranätenheter kan hackare enkelt starta nätverksattacker, eftersom det inte finns någon brandvägg installerad mellan routern och NAS:en som blockerar skadlig trafik. Även om en brandvägg är installerad (genom att använda en grundläggande brandvägg eller köpa en brandvägg av företagsklass) är det dock inte någon garanti för att alla attacker blockeras.

* QNAP rekommenderar att endast de portar som har relativt låg risk öppnas för VPN-tjänster till Internet, medan andra tjänstportar som har hög risk, exempelvis systemhantering, SMB- och SSH-tjänster inte bör vara lätta att komma åt från Internet.



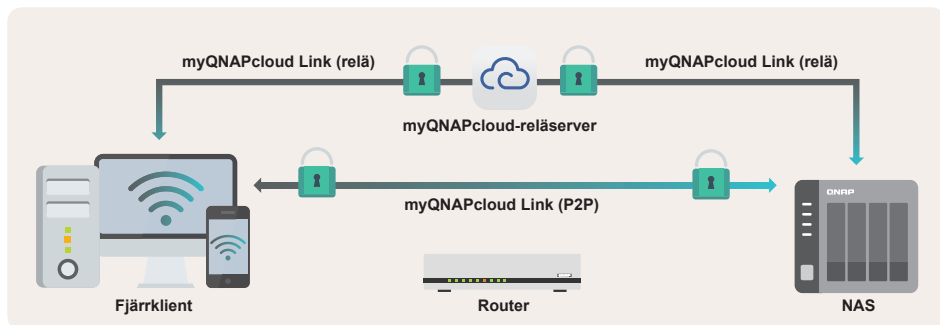
02 | Aktivera VPN-serverfunktionen på router eller QNAP NAS

Vissa routrar har stöd för VPN-serverfunktioner (exempelvis routrarna i QNAP QHora- och QMiro-serien), medan QNAP NAS även har stöd för flertalet VPN-servrar. När den är aktiverad och konfigurerad på rätt sätt kan du komma åt varje enhet på intranätet med en VPN-krypterad anslutning från Internet till VPN-servern och på så sätt få en hög säkerhetsnivå.



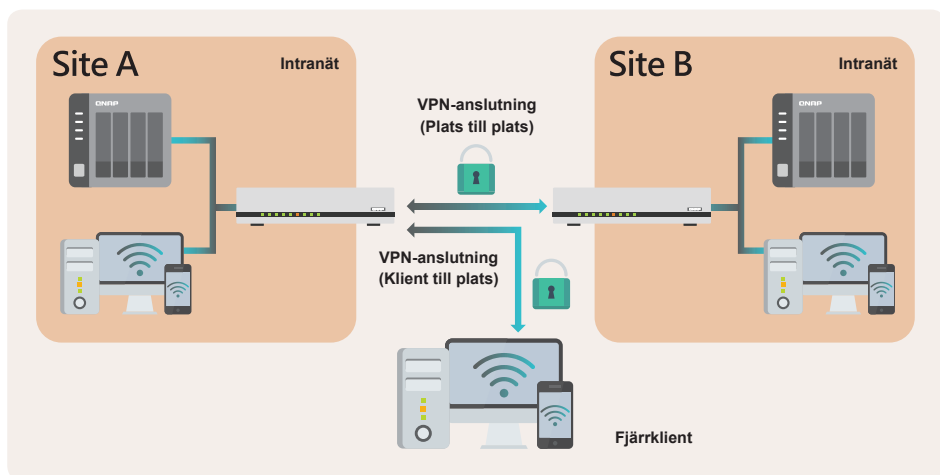
03 | Använd den säkra anslutningen myQNAPcloud Link

Det behövs inte någon routerkonfiguration om du använder myQNAPcloud Link för att ansluta till NAS, eftersom den kan öppna NAS-tjänsten direkt till Internet. myQNAPcloud Link upprättar en anslutning via en reläserver eller peer-to-peer-teknik (P2P) anpassat till nätverksmiljön. Hela anslutningen krypteras för att säkerställa säkerheten.



04 | Använd VPN-produkter med SD-WAN eller plats-till-plats

Till skillnad från VPN-serverfunktionen (VPN med klient-till-plats), som nämns här ovanför, upprättar VPN med SD-WAN eller plats-till-plats en säker krypterad VPN-anslutning mellan två eller flera routrar på olika platser. Enkelt uttryckt kan enheter på ett VPN-nätverk som är konfigurerat plats-till-plats anslutas till varandra som om de fanns på samma intranät, något som gör det idealiskt för användare som alternerar mellan flera platser. Med VPN för klient-till-plats kan du komma åt din NAS var som helst.



Du kan välja den anslutningsmetod som är lämplig för dig, enligt jämförelsetabellen. QNAP har flera säkra anslutningslösningar som möter användarnas behov.

Anslutningsmetod	Fördelar	Nackdelar	Lämpliga användare
Aktivera och konfigurera routerns DMZ/portvidarebefordran för UPnP	<ul style="list-style-type: none">• Snabbaste anslutningen	<ul style="list-style-type: none">• Sårbar för cyberattacker• Inget försvar mot 0-dag-sårbarhetsattacker	<ul style="list-style-type: none">• Ha en tydlig förståelse för vilka risker det innebär• Bekant med nätverksinställningarna• Skapa flera säkerhetskopior med viktiga data• Ha en katastrofåterställningsplan
Aktivera VPN-server på routern*	<ul style="list-style-type: none">• Relativt enkel att konfigurera	<ul style="list-style-type: none">• Ingen avisering vid inloggningsfel, automatisk blockering och brandväggsfunktion• Har stöd för färre VPN-protokoll• Prestandan begränsas av routerns hårdvara	<ul style="list-style-type: none">• Inte bekant med nätverksinställningar• Överföringshastigheten är inte viktigt
Aktivera VPN-serverfunktion på QNAP NAS*	<ul style="list-style-type: none">• Har stöd för flera VPN-protokoll• Kompatibel med NAS-brandväggen (QuFirewall)• Stöd för avisering vid inloggningsfel och automatisk blockering	<ul style="list-style-type: none">• Inställningarna är aningen mer komplicerade	<ul style="list-style-type: none">• Bekant med nätverksinställningarna• Behöver regelbundet få tillgång till många filer från Internet
Använd den säkra anslutningen myQNAPcloud Link	<ul style="list-style-type: none">• Enklast att konfigurera• Har stöd för åtkomstkontroll• NAS behöver inte exponeras för Internet	<ul style="list-style-type: none">• Långsammare anslutning	<ul style="list-style-type: none">• Inte bekant med nätverksinställningar• Sporadisk åtkomst till NAS:en från Internet• Nätverksmiljö där WAN IP-adress inte kan erhållas
Använd VPN-produkter med SD-WAN eller plats-till-plats*	<ul style="list-style-type: none">• Efter konfigurationen kan intranätanvändare använda det utan att de märker någon skillnad• Har även stöd för VPN med klient-till-plats	<ul style="list-style-type: none">• Kräver extra utrustning	<ul style="list-style-type: none">• Kräver flerpunktsåtkomst och fjärrsäkerhetskopiering• Kräver värdeskapande program

*QNAP NAS har stöd för:
myQNAPcloud Link/VPN-servrar (L2TP/IPsec, OpenVPN, WireGuard, QBelt)/QuWAN SD-WAN

* QNAP Router har stöd för:
QuWAN SD-WAN/VPN-servrar (L2TP/IPsec, OpenVPN, WireGuard, QBelt)

Avser vanliga hemroutrar

01

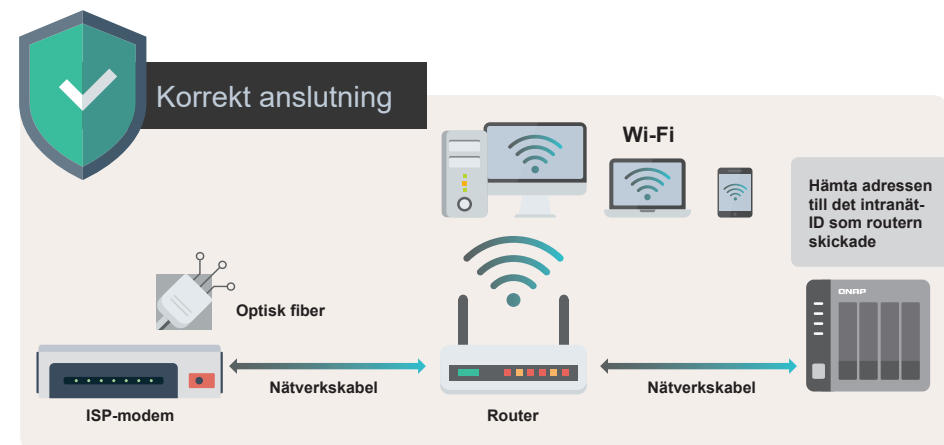
Vägledning för NAS-säkerhetsinställningar

Undvik att exponera NAS:en för Internet

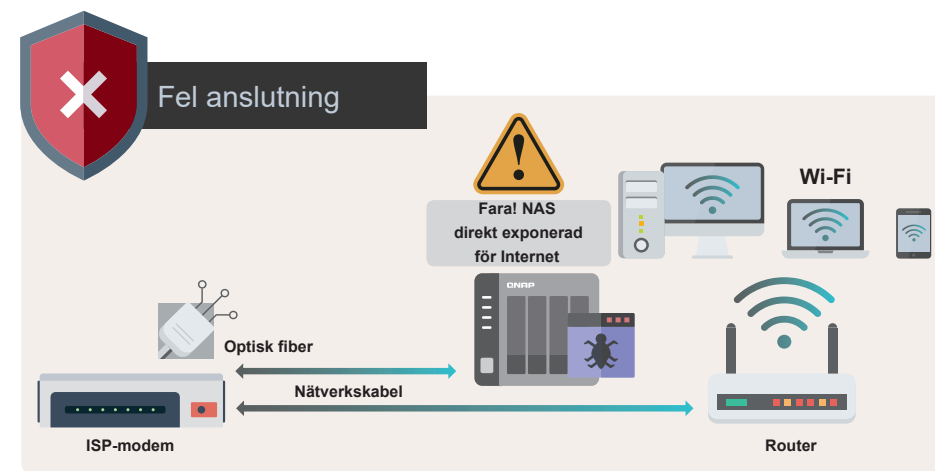


Anslut NAS:en på rätt sätt

Kontrollera att din NAS är ansluten till routern. Med rätt konfiguration kan routern blockera Internetanslutningar åt dig, så att din NAS kan vara dold från Internet och undvika cyberattacker.



Om du ansluter NAS:en till det modem som Internetleverantören tillhandahåller så får din NAS WAN IP-adressen direkt. I det här fallet kan vem som helst (inklusive hackare) ansluta till din NAS via Internet och till och med försöka attackera och göra intrång.

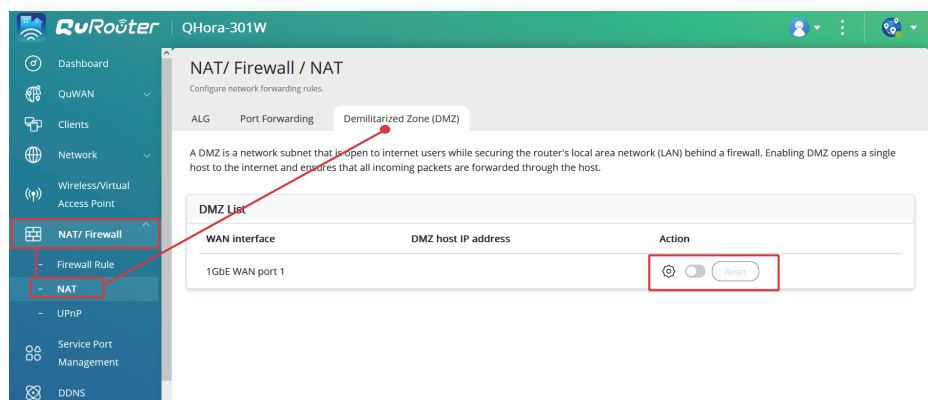
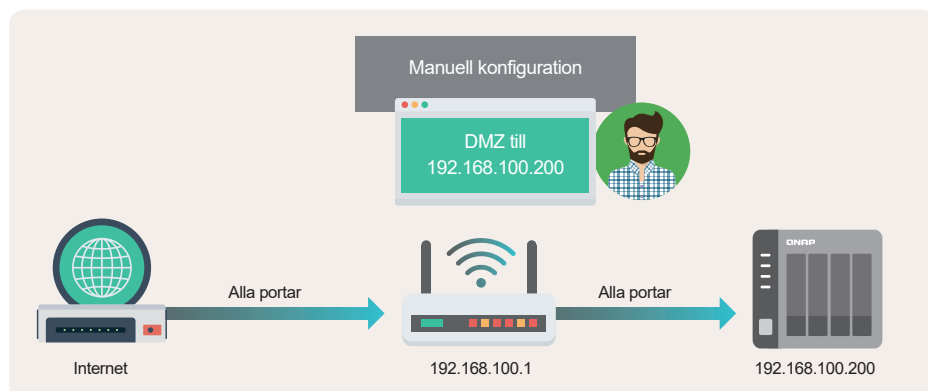


Kontrollera routerinställningar

Som standard och i teorin kan ingen ansluta direkt från Internet till din enhet bakom routern. Men om du aktiverar "DMZ (demilitariserad zon)", "Portvidarebefordran" eller "UPnP (Universal Plug and Play)" vidarebefordrar routern paket till den enhet du valt, enligt de regler du ställt in, vilket exponerar enheten för Internet. Om de inte behövs bör du kontrollera och säkerställa att följande funktioner är **inaktiverade**.

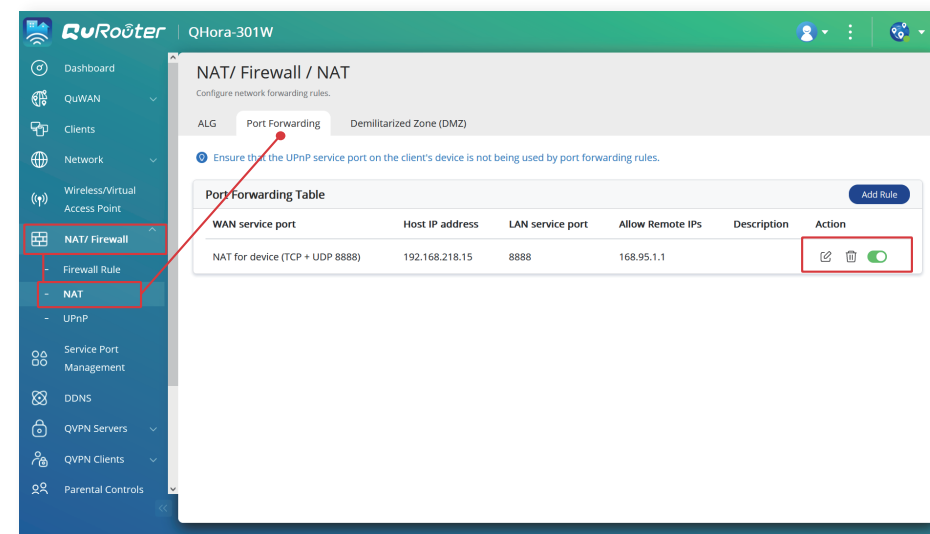
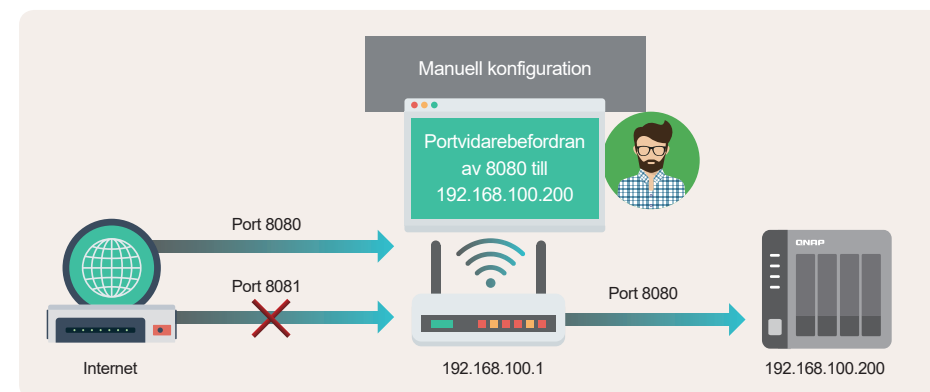
01 | Kontrollera DMZ (demilitariserad zon)

När du har aktiverat den här funktionen är alla serviceportar på den enhet du valt direkt öppna för Internet, kort sagt helt exponerade för Internet. Minska säkerhetsriskerna genom att inaktivera den här funktionen.



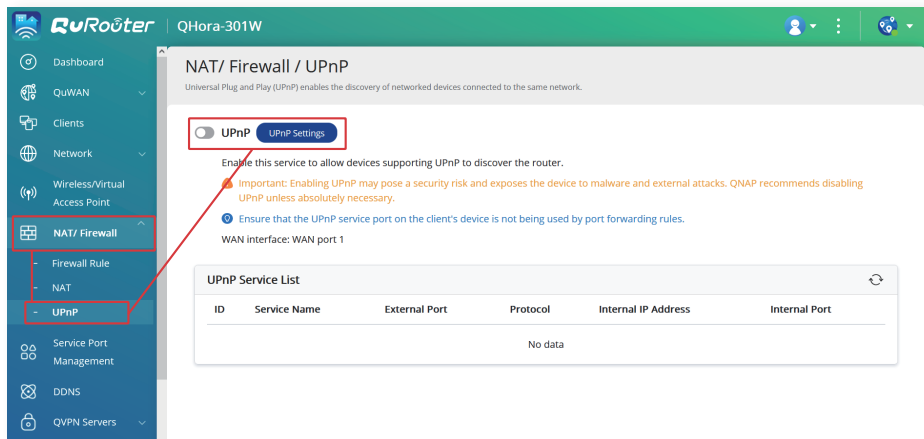
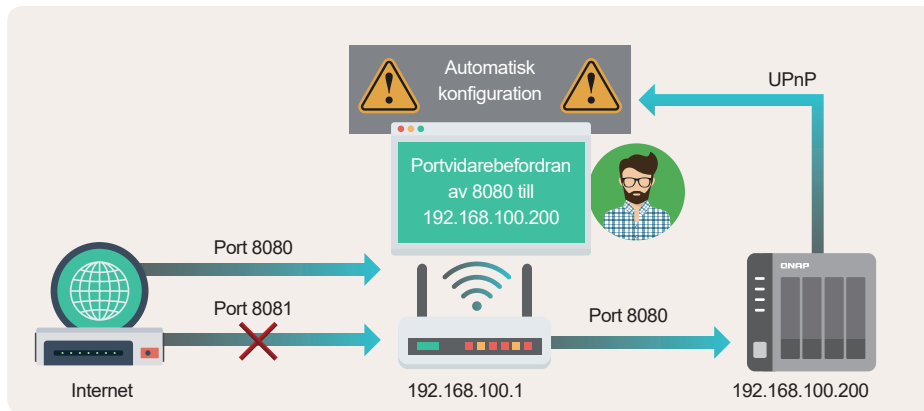
02 | Kontrollera portvidarebefordran

Med den här funktionen kan du öppna en specifik tjänstport på en enhet för Internet och på så vis kan alla komma åt tillhörande tjänster via Internet. Dock kan även hackare också initiera attacker mot öppna tjänster från Internet. Därför är vår rekommendation att du först inaktiverar alla regler för portvidarebefordran och därefter konfigurerar NAS-säkerhetsinställningarna för att sedan säkerhetskopiera viktiga data innan den här funktionen används till att öppna några viktiga tjänster på Internet.



03 | Kontrollera UPnP (Universal Plug and Play)

Den här funktionen motsvarar automatisk portvidarebefordran. När den här funktionen aktiverats kan din enhet automatiskt konfigurera portvidarebefordran genom att använda det relevanta protokollet. Den här funktionen har allvarliga säkerhetsrisker eftersom den kan exponera dina tjänster för Internet utan din vetskap eller så kan den utnyttjas av hackare till att öppna bakdörrar, därför bör du inaktivera denna funktion i och med att det förbättrar säkerheten.



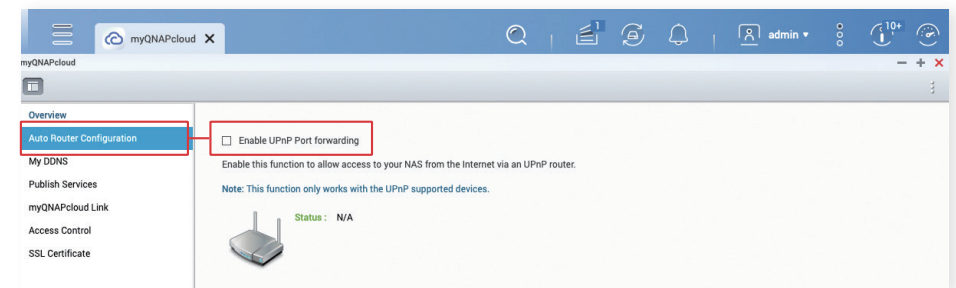
01 | Automatisk routerkonfiguration, UPnP-portvidarebefordran

Eftersom vissa routrar inte har stöd för inaktivering av UPnP-funktionen behöver du samtidigt markera inställningen "Automatisk routerkonfiguration" på NAS:en för att säkerställa att den här funktionen är inaktiverad.

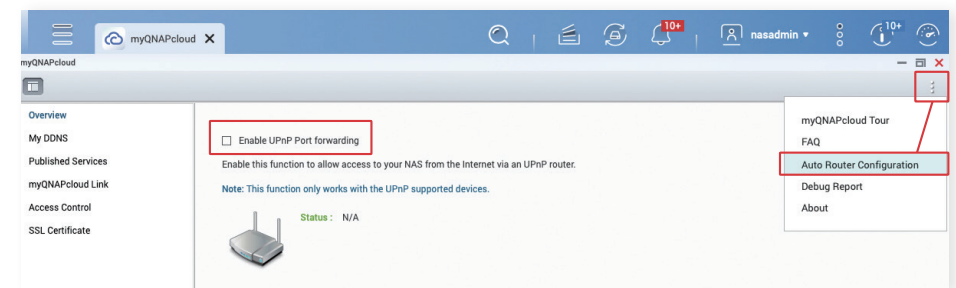
* Den här funktionen är som standard inaktiverad från QTS 4.5.0/QuTS hero h4.5.3 och framåt.

Inaktivera funktionen för automatisk routerkonfiguration:

1. Logga in på webbhanteringsgränssnittet till QTS/QuTS hero med ett administratörskonto.
2. Öppna menyn i det övre vänstra hörnet av hanteringsgränssnittet och klicka på myQNAPcloud
3. **QTS 5.0.0/QuTS hero h5.0.0** eller **tidigare**: Klicka på "Automatisk routerkonfiguration" i den vänstra menyn



QTS 5.0.1/QuTS hero h5.0.1 eller **senare**: Klicka på menyikonen i det övre högra hörnet och välj "Automatisk routerkonfiguration"



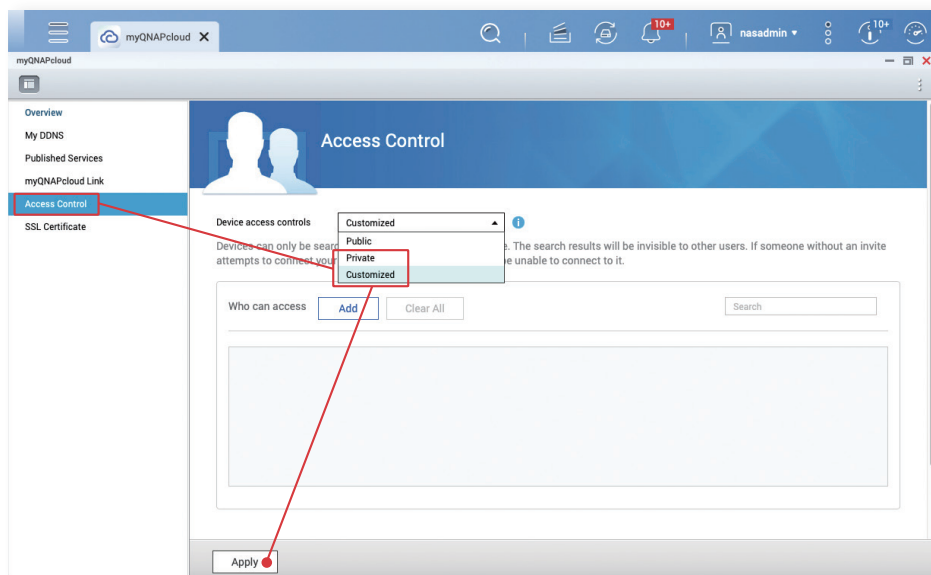
4. På sidan "Automatisk routerkonfiguration"; avmarkera "Aktivera vidarebefordran av UPnP-port" och klicka på "Tillämpa".

02 | Åtkomstkontroll till myQNAPcloud Link

myQNAPcloud Link är en tjänst för säker molnanslutning som tillhandahålls av QNAP. Användare kan ansluta till sin QNAP NAS genom deras valda myQNAPcloud-enhetsnamn. myQNAPcloud Link tillhandahåller inställningar för åtkomstkontroll. När åtkomstkontrollen är inställd till "Offentlig" kan alla som känner till enhetens namn använda myQNAPcloud Link för att ansluta till din NAS. Därför rekommenderar vi att åtkomstkontrollen ställs in till "Privat" eller "Anpassad". I båda lägena måste användarna logga in på sitt QNAP ID i listan över tillåten åtkomst innan de kan använda myQNAPcloud Link för att ansluta till molntjänster på ett säkert sätt.

* Standardinställningen i QTS 4.5.0/QuTS hero h4.5.3 (eller senare) är "Anpassad"

1. Logga in på webbhanteringsgränssnittet till QTS/QuTS hero med ett administratörskonto
2. Klicka på menyn i det övre vänstra hörnet av hanteringsgränssnittet och klicka på "myQNAPcloud"
3. Klicka på "Åtkomstkontroll" i den vänstra menyn
4. På inställningssidan för "Åtkomstkontroll"; ställ in "Enhetsåtkomstkontroller" till "Privat" eller "Anpassad" och klicka sedan på "Tillämpa".



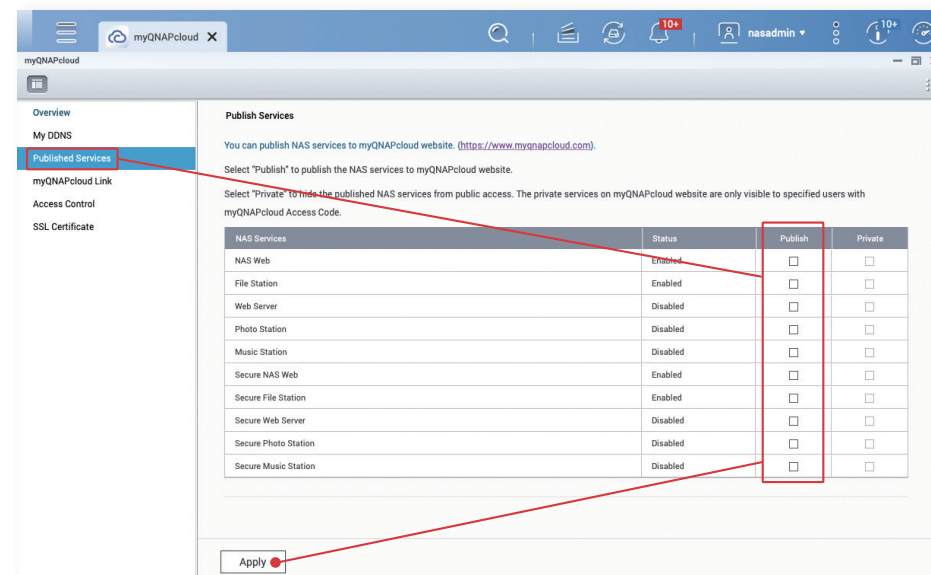
03 | Publicerade tjänster

Publicerade tjänster kan göra det enklare för användare att använda tillhörande funktioner på myQNAPcloud-webbplatsen men det ökar även säkerhetsriskerna. Om du inte behöver använda den här funktionen rekommenderar vi att du inaktiverar den för att förbättra säkerheten.

* Den här funktionen är som standard inaktiverad från QTS 4.5.0/QuTS hero h4.5.3 och framåt

Funktionen "Publicerade tjänster":

1. Logga in på webbhanteringsgränssnittet till QTS/QuTS hero med ett administratörskonto
2. Klicka på menyn i det övre vänstra hörnet av hanteringsgränssnittet och klicka på "myQNAPcloud"
3. Klicka på "Publicerade tjänster" i den vänstra menyn
4. I fältet "Publicera"; avmarkera alla och klicka på "Tillämpa".



Kontrollista för nätverksinställningar

Hårdvarurelaterat

- NAS är ansluten bakom en router
- NAS hämtar IP-adress för intranätet

Router



- Inaktivera routerns "DMZ"-funktion
- Inaktivera regeln för routerns portvidarebefordran
- Inaktivera routerns UPnP-funktion



NAS



- Inaktivera NAS-funktionen "Automatisk routerkonfiguration, UPnP-portvidarebefordran"
- Ställ in NAS:ens "Åtkomstkontroll till myQNAPcloud Link" till "Privat" eller "Anpassad".
- Inaktivera funktionen "Publicerade tjänster"

Efter att ha kontrollerat och tillämpat ovanstående inställningar är din QNAP NAS inte exponerad för Internet och riskerna för att bli attackerad av hackare har avsevärt minskats. Läs vidare och kontrollera de återstående inställningarna för att stärka din QNAP NAS.

Om du behöver komma åt NAS via Internet kan du överväga dessa tre säkra alternativ:


myQNAPcloud Link

Lär dig mer

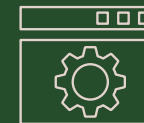

QVPN Service

Lär dig mer


QuWAN SD-WAN

Lär dig mer

02

Vägledning för NAS-säkerhetsinställningar

NAS-säkerhetsinställningar



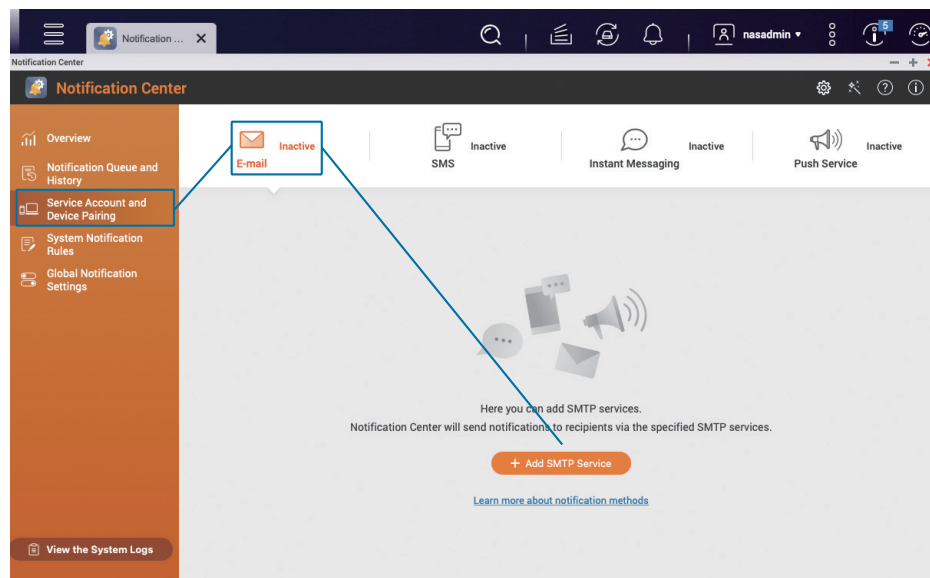
Konfigurera systemaviseringar

Aviseringscenter är inbyggt och kan skicka push-meddelanden utifrån dina inställningar, så att användarna kan ha NAS-statusen överskådlig och reagera på avvikelser så snart de upptäcks.

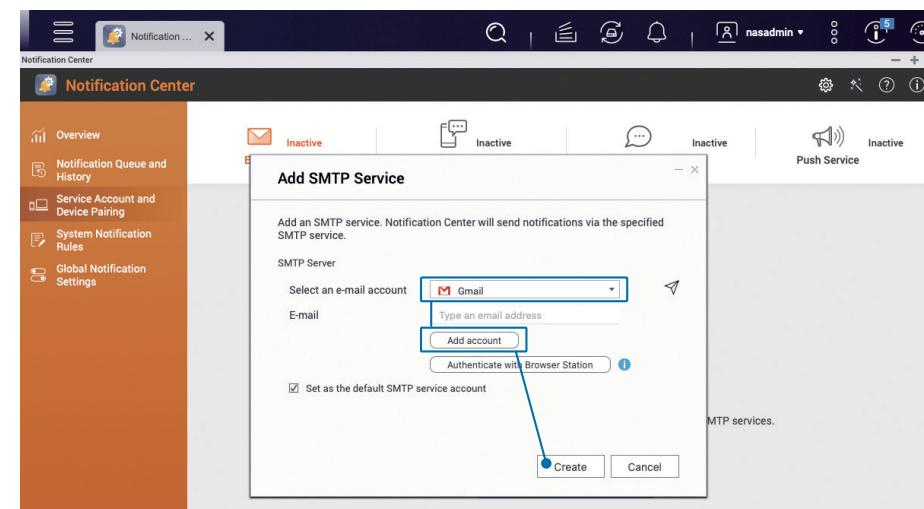
Följande självstudie lär dig hur du skapar två grundläggande regler för "E-postmeddelande" för att skicka "Larmmeddelanden" och "Uppdatering av inbyggd programvara" samt för att lägga till fler regler om det behövs.

01 | Lägg till aviseringsmetoden "E-postmeddelande"

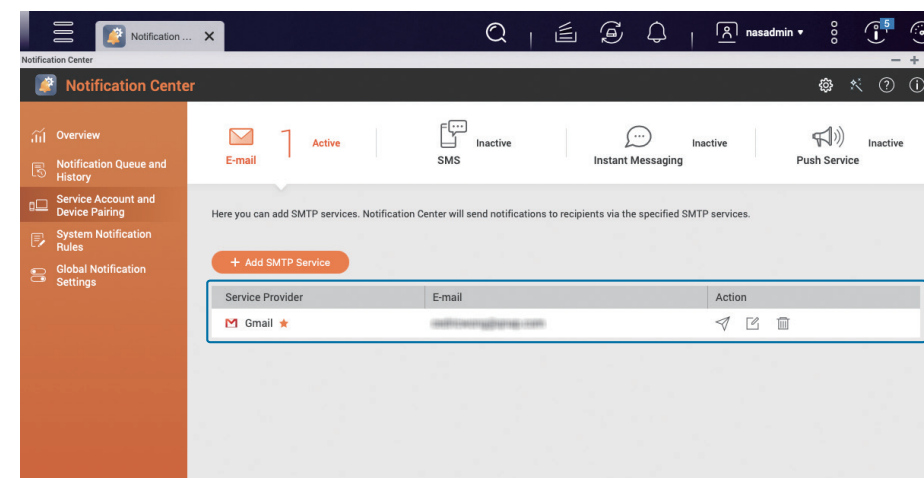
Öppna "Aviseringscenter" och klicka på "Servicekonto och enhet ihopkoppling" i den vänstra menyn, välj "E-postmeddelande" och klicka sedan på "Lägg till SMTP-tjänst"



Välj ett e-postkonto (i följande exempel används Gmail) och klicka på "Lägg till konto", följ sedan instruktionerna för att slutföra Gmail-verifieringsprocessen och klicka på "Skapa" när verifieringen är klar.

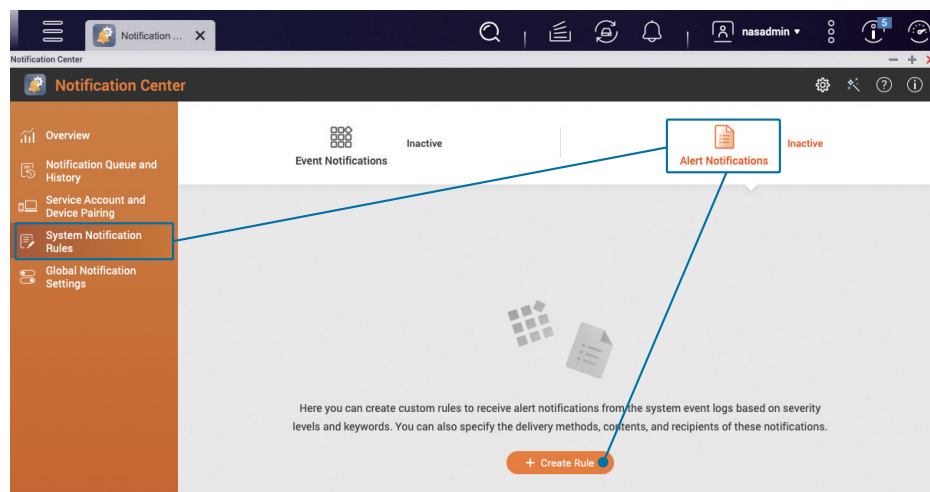


⇓ När det väl skapats ser du det e-postkonto som du har lagt till i listan.

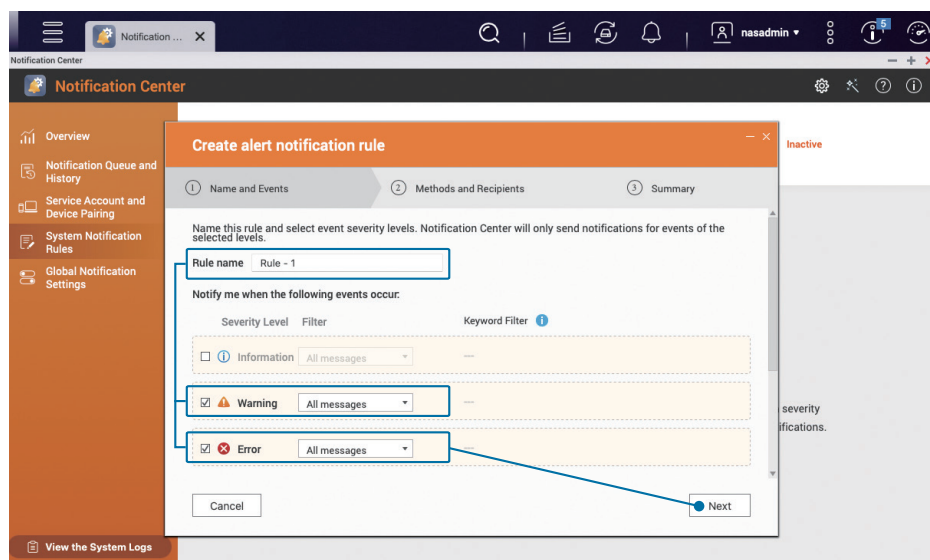


02 | Konfigurera "Larmmeddelanden"

I den vänstra sidan meny i "Aviseringscenter"; klicka på "Systemaviseringsregler" och välj "Larmmeddelanden" och klicka på "Skapa regel".

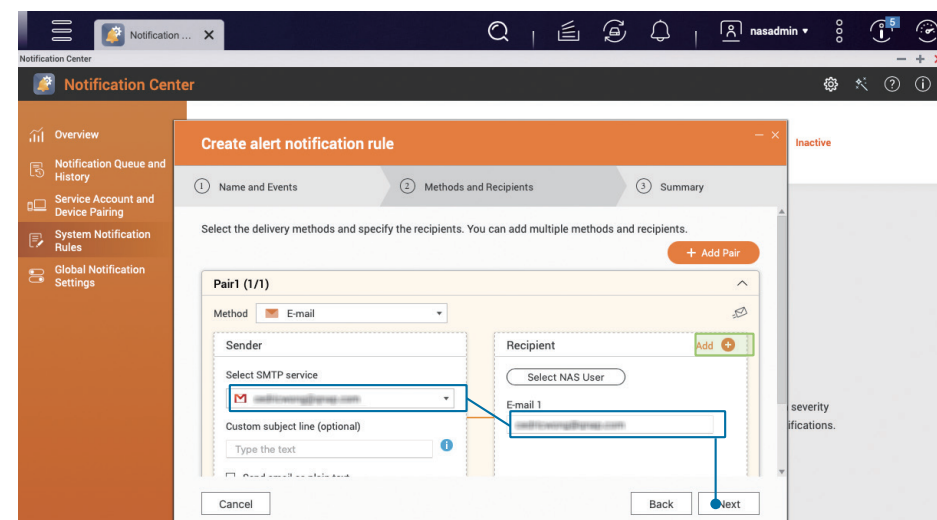


Ändra "Regelnamn" enligt dina behov och markera de två allvarighetsnivåerna "Varning" och "Fel", klicka därefter på "Nästa".

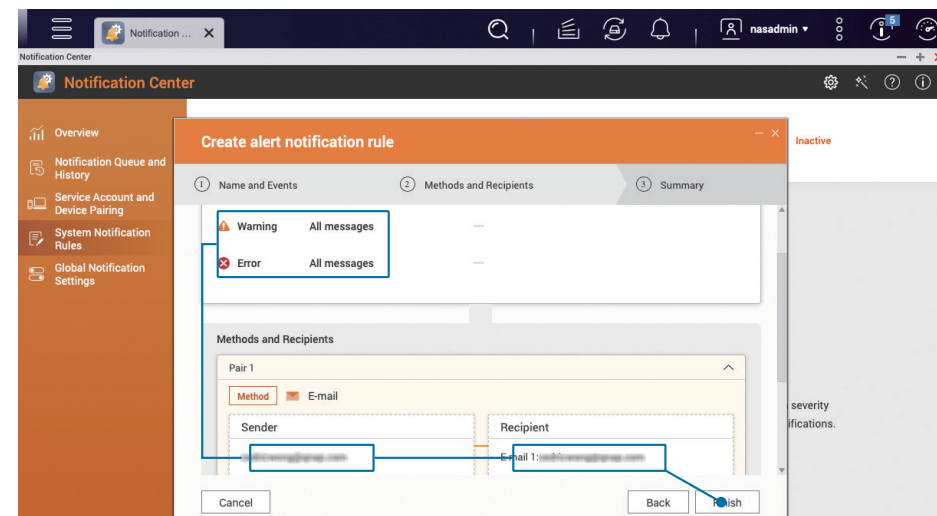


Ställ in leveransmetoden och ställ in mottagaren, välj det e-postkonto som du just lagt till som "Avsändare" i parkopplingen och ange sedan "E-postadress" till "Mottagare" och klicka sedan på "Nästa".

Om det behövs kan du ange flera mottagare genom att klicka på "Lägg till +" bredvid "Mottagare". Du kan också använda "Lägg till par" för att skicka meddelanden på flera sätt samtidigt.

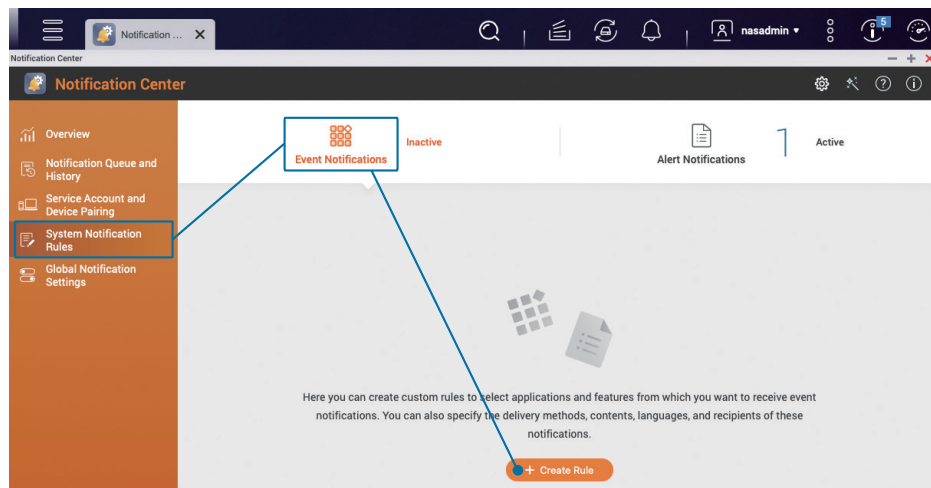


När inställningarna bekräftat är korrekta; klicka på "Slutför" så slutförs inställningarna för "Larmmeddelanden".

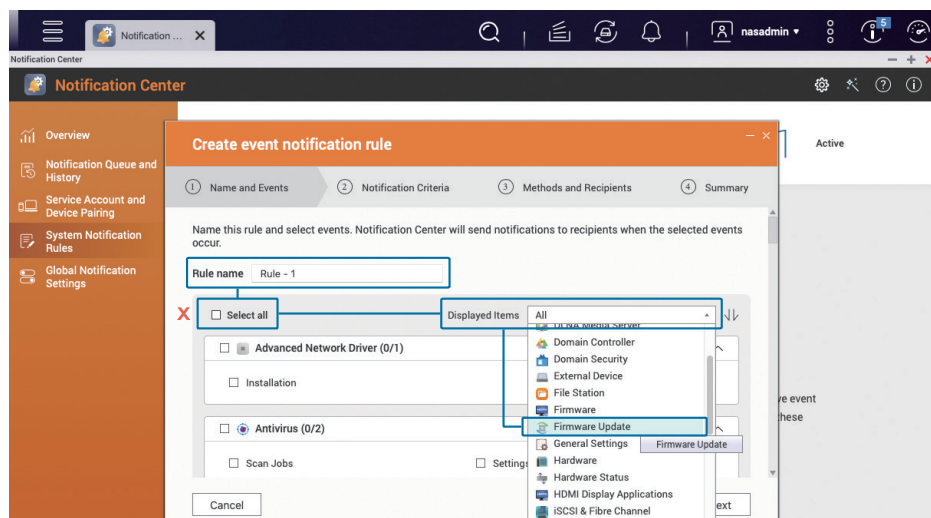


03 Konfigurera aviseringar om "Uppdatering av inbyggd programvara"

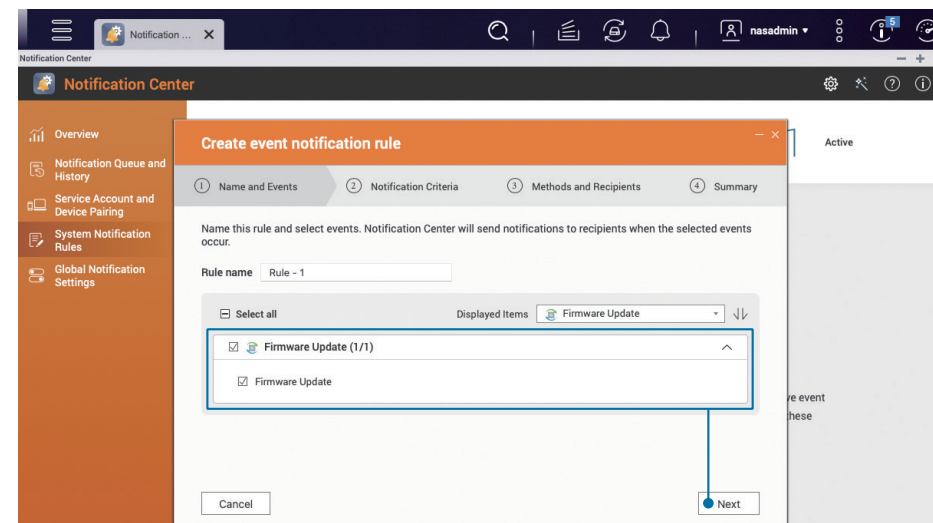
Klicka på "Systemaviseringsregler" i den vänstra menyn i "Aviseringscenter" och välj "Händelseaviseringar", klicka sedan på "Skapa regel".



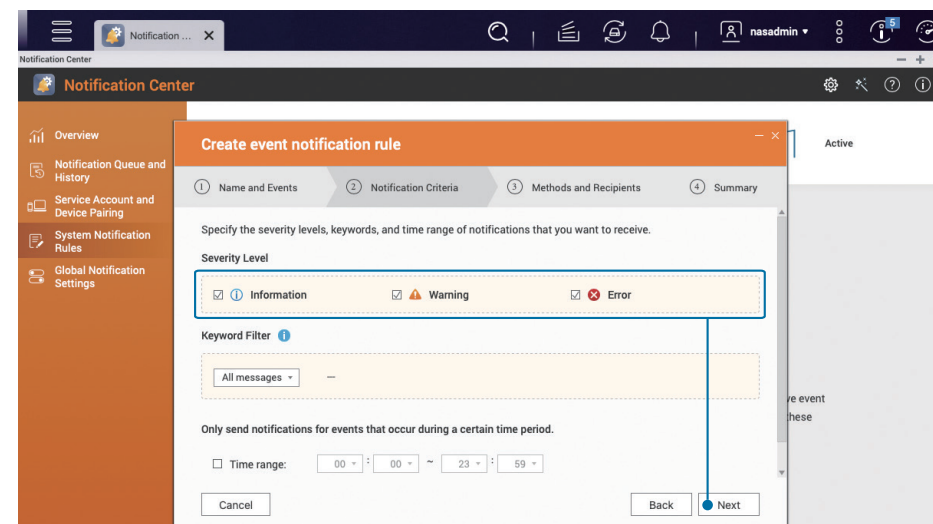
Ändra "Regelnamn" enligt dina behov, avmarkera "Markera alla" och välj sedan "Uppdatering av inbyggd programvara" i de "Visade objekt" till vänster och välj därefter alternativet "Uppdatering av inbyggd programvara" här nedanför.




Markera alternativet "Uppdatering av inbyggd programvara" och klicka på "Nästa".

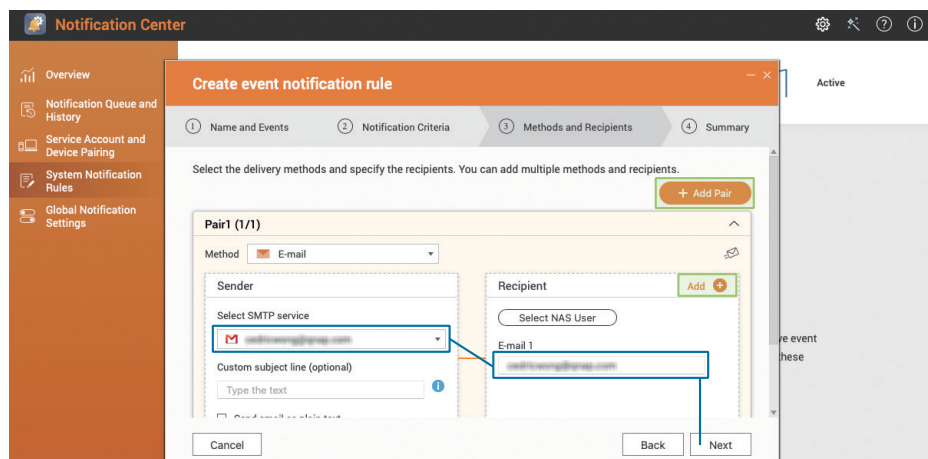


Markera alla allvarighetsnivåer, inklusive "Information", "Varning" och "Fel" och klicka på "Nästa".

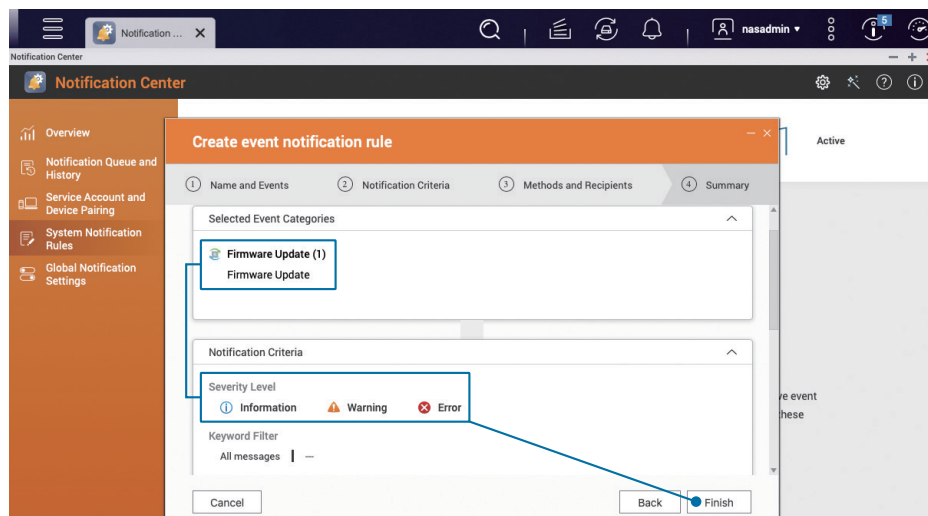


Ställ in leveransmetoden och mottagaren. Eftersom endast aviseringen "e-postmeddelande" är inställt för närvarande ska det e-postkonto som du just har lagt till väljas som "Avsändare" i ihopparningen och sedan ska "Mottagarens" e-postadress anges, klickar därefter på Nästa.

Om det behövs kan du ange flera mottagare genom att klicka på "Lägg till" bredvid "Mottagare" . Du kan också använda "Lägg till par" för att skicka meddelanden på flera sätt samtidigt.



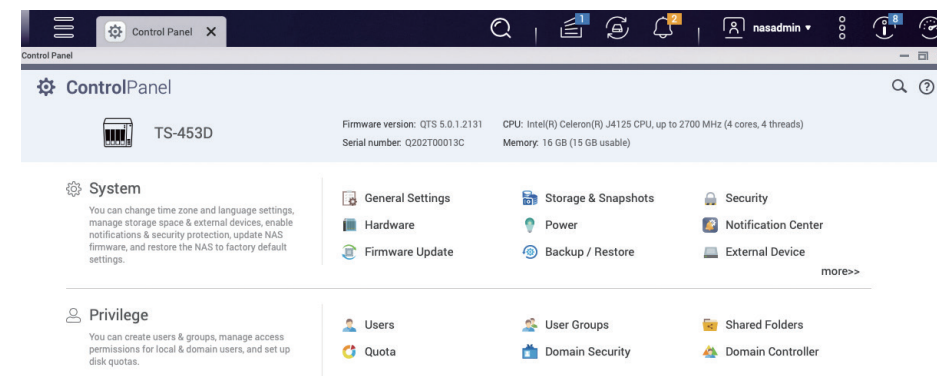
När inställningarna bekräftats vara korrekta: klicka på "Slutför" för att slutföra inställningen av "Uppdatering av inbyggd programvara".



Aktivera automatisk uppdatering av inbyggd programvara (QTS/QuTS hero)

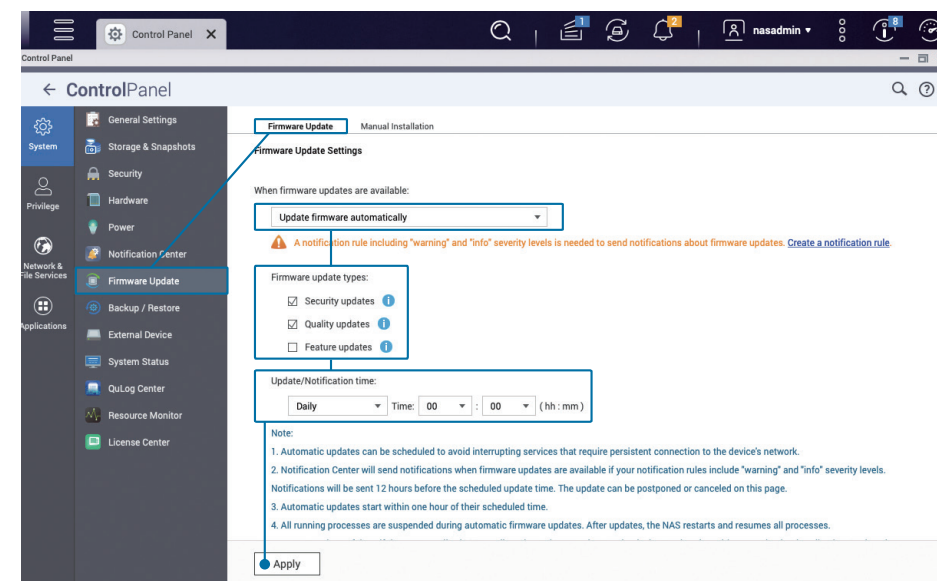
Funktionen för att uppdatera automatiskt gör det enklare att installera uppdateringar för nya funktioner, buggfixar och sårbarheter.

Öppna "Kontrollpanelen" och klicka på "Uppdatering av inbyggd programvara".




I "Inställningar för uppdatering av inbyggd programvara"; välj "Uppdatera inbyggd programvara automatiskt" och Markera "Kvalitetsuppdateringar"; för "Uppdatera/aviseringstid" är rekommendationen att ställa in en tid då aktiviteten är låg, t.ex. "00: 00" och klicka sedan på Tillämpa.

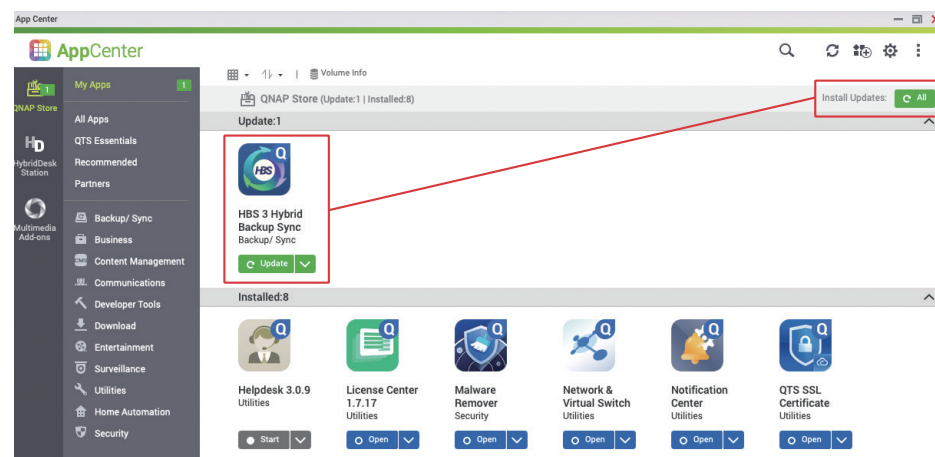
*** För QTS 5.0.0/QuTS hero h5.0.0 (eller tidigare); markera "Rekommenderad version" på sidan "Automatisk uppdatering"**




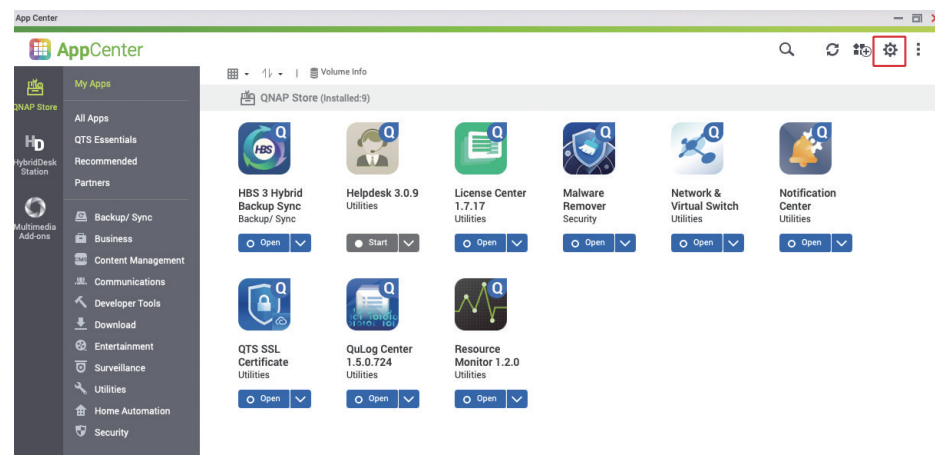
Inställningar för appuppdatering

App Center tillhandahåller flera appar som lägger till fler funktioner i din QNAP NAS men apparna måste även uppdateras för att förbättra appfunktioner, åtgärda problem och sårbarheter samt förbättra användarupplevelsen.

Öppna "App Center" för att se om det finns några appar som behöver uppdateras. Om det gör det så klickar du på knappen "Alla"  **All** " längst upp till höger för att uppdatera alla appar.

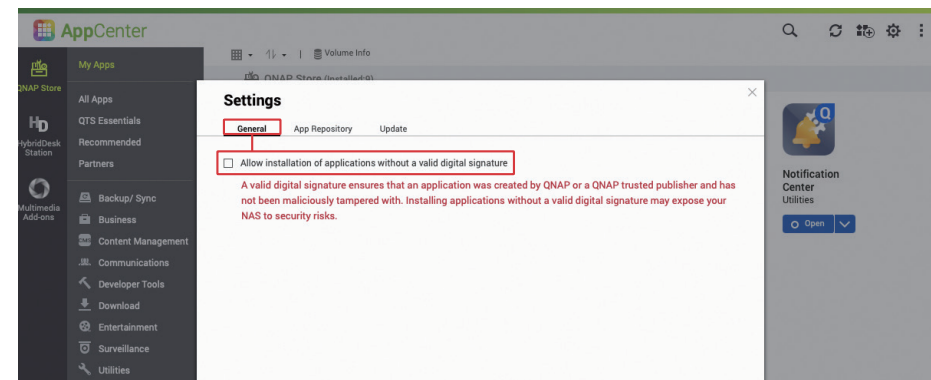


När uppdateringen är klar så klickar du på ikonen "Inställningar"  i det övre högra hörnet för att öppna inställningssidan för App Center.



QNAP eller QNAP-betrodda utvecklare lägger till en digital signatur i appen för att säkerställa att den är äkta. Vi rekommenderar "Tillåt installation av program utan en giltig digital signatur" avmarkeras i syfte att förbättra säkerheten.

*** Den är som standard avmarkerad och det innebär att det är omöjligt att installera appar som inte har en giltig digital signatur**

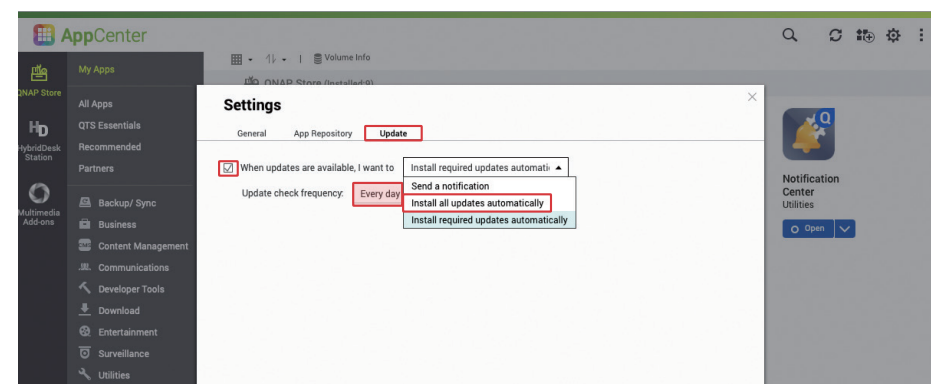


Klicka på fliken Uppdatera, om det inte finns något särskilt behov är rekommendationen att du väljer "Installera alla uppdateringar automatiskt" och ställer in att de ska göras "Varje dag" för att sedan klicka på "Tillämpa" för att slutföra inställningen.

⇒ "Nödvändiga uppdateringar" används huvudsakligen till att uppfylla beroenden för program och inbyggd programvara och innehåller även "större sårbarhetsuppdateringar".

⇒ "Alla uppdateringar" innehåller alla funktionsförbättringar, buggfixar och alla sårbarhetskorrigeringar. Uppdateringen sker oftare.

*** Standardinställningen är "Installera alla uppdateringar automatiskt"**

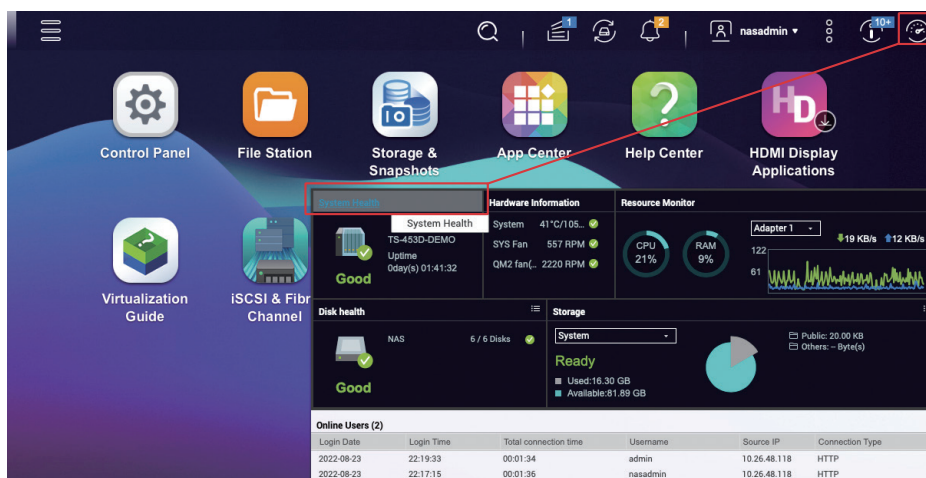


Inaktivera eller ta bort onödiga funktioner

QNAP NAS tillhandahåller en mängd olika funktioner och appar men ju fler funktioner som är aktiverade, desto fler potentiella attackvektorer finns det. Du bör regelbundet kontrollera och inaktivera (eller ta bort) onödiga funktioner, för att förbättra säkerheten och göra att systemet fungerar mer friktionsfritt.

★ För att förbättra produktsäkerheten, från **QTS 5.0.0/QuTS hero h5.0.0** och framåt har icke-väsentliga funktioner som standard inaktiverats vid systeminitiering och **App Center** installerar som standard inte några icke-väsentliga appar. Om systemet initierades innan det uppdaterades till **QTS 5.0.0/QuTS hero h5.0.0** ber vi dig kontrollera vilka appar som har installerats.

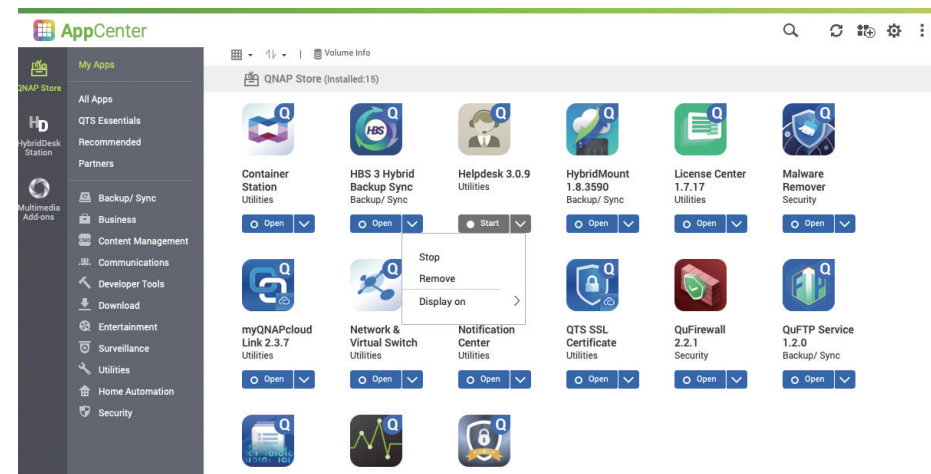
Klicka på knappen " " i det övre högra hörnet för att öppna systemets "Instrumentpanel", klicka på "Systemhälsa" för att öppna fönstret "Systemstatus".



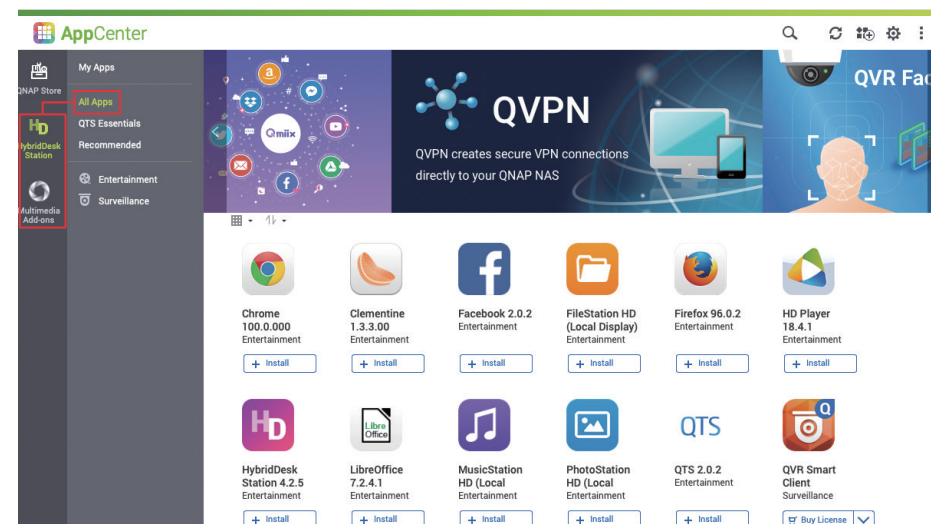
Klicka på "Systemtjänst" för att visa de aktiverade systemfunktionerna. Du kan gå till Kontrollpanelen för att inaktivera systemfunktioner som inte behövs.

System Status			
System Service			
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

Förutom de inbyggda systemfunktionerna behöver du även kontrollera vad som är installerat i "App Center".



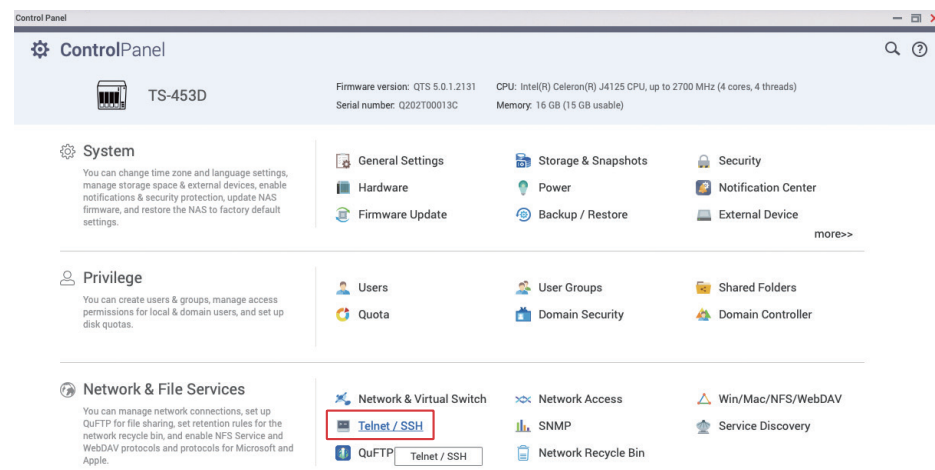
Längst till vänster; klicka på "HybridDesk Station" och "Multimedia-tillägg" för att se statusen för tillhörande appar,



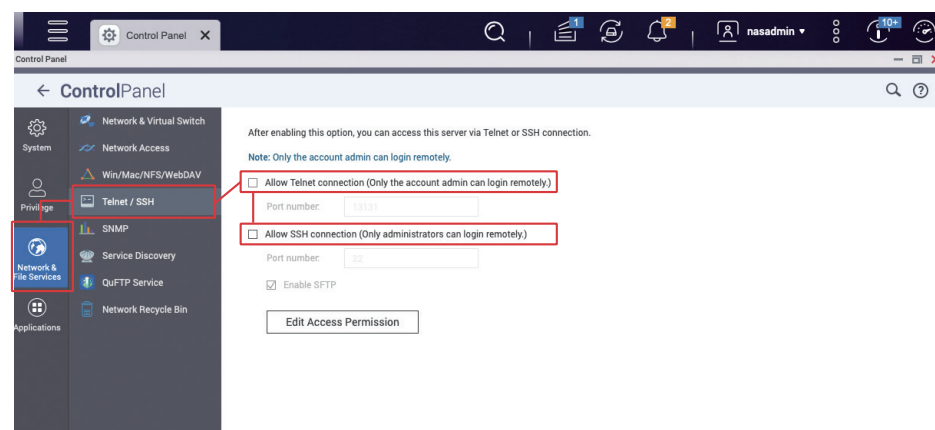
Inaktivera Telnet/SSH

Om du inte använder dem rekommenderar vi starkt att **inaktivera Telnet och SSH**. Dessa två funktioner används i allmänhet av QNAP:s kundtjänst eller professionell IT-personal när de ska underhålla systemet. Det bör inte finnas något behov för allmänna användare att använda dem och därför är rekommendationen att de inaktiveras.

Öppna "Kontrollpanelen" och klicka på "Telnet/SSH"



Avmarkera "Tillåt Telnet-anslutning" och "Tillåt SSH-anslutning" och klicka sedan på Tillämpa.

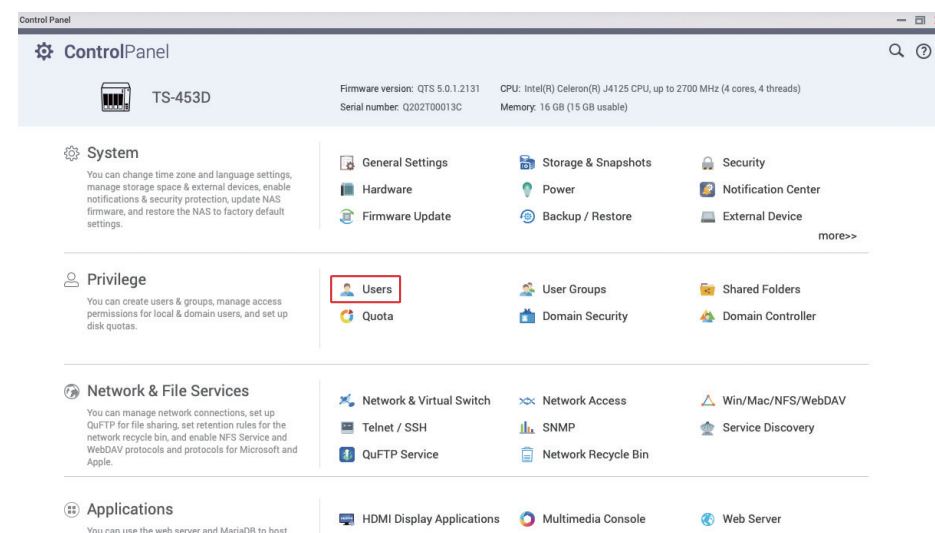


Stärk systemkontosäkerheten

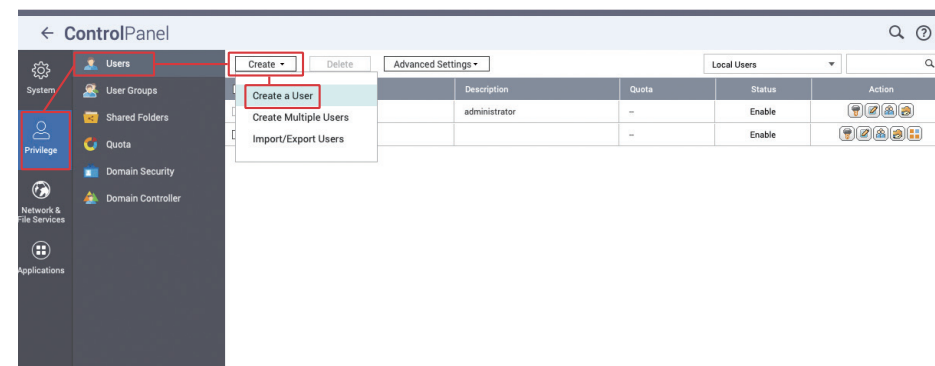
Inaktivera standardadministratörskontot "admin"

Hackare som använder lösenordsknäckning med ordlista riktar i allmänhet in sig på standardadministratörskontot "admin". Om systemet initierades med QTS 4.5.4/QuTS hero h4.5.4 (eller tidigare) är standardadministratörskontot "admin" aktivt. Följ dessa steg för att skapa ett nytt administratörskonto och inaktivera kontot "admin".

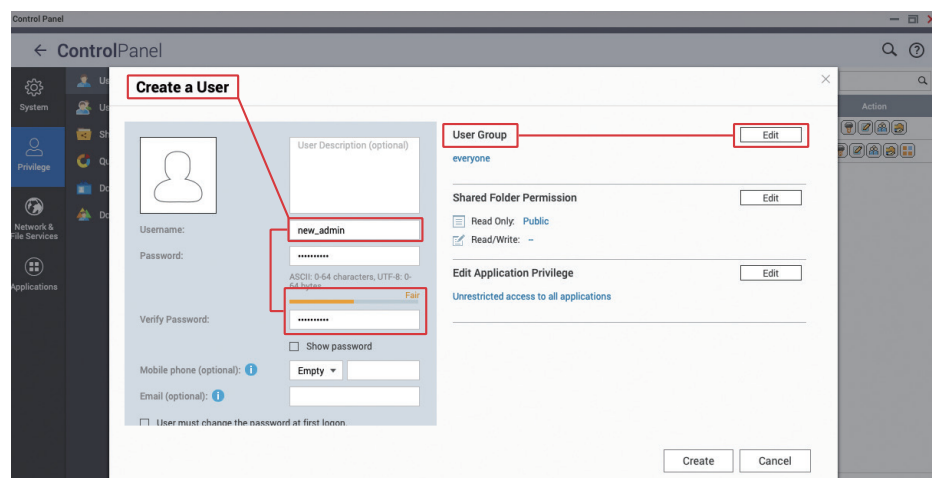
Öppna "Kontrollpanelen" och klicka på "Användare"



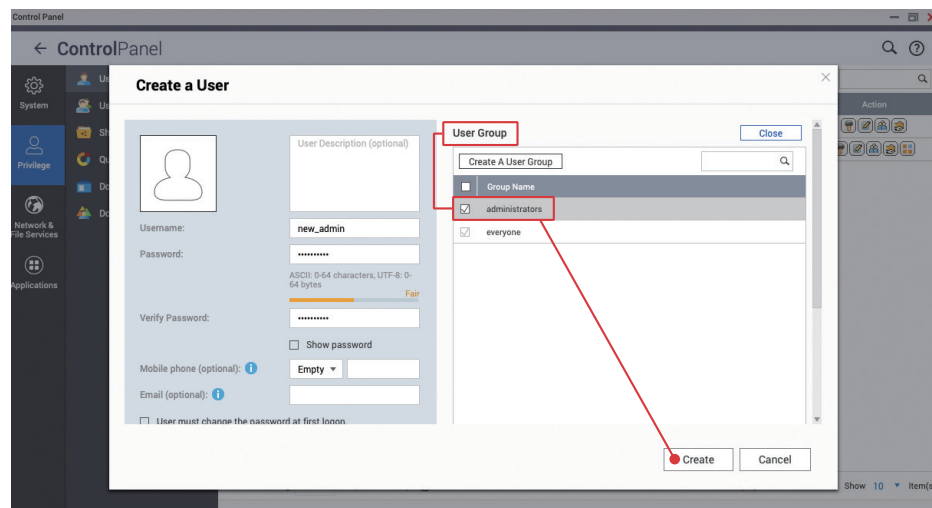
Klicka på "Skapa" > "Skapa en användare"



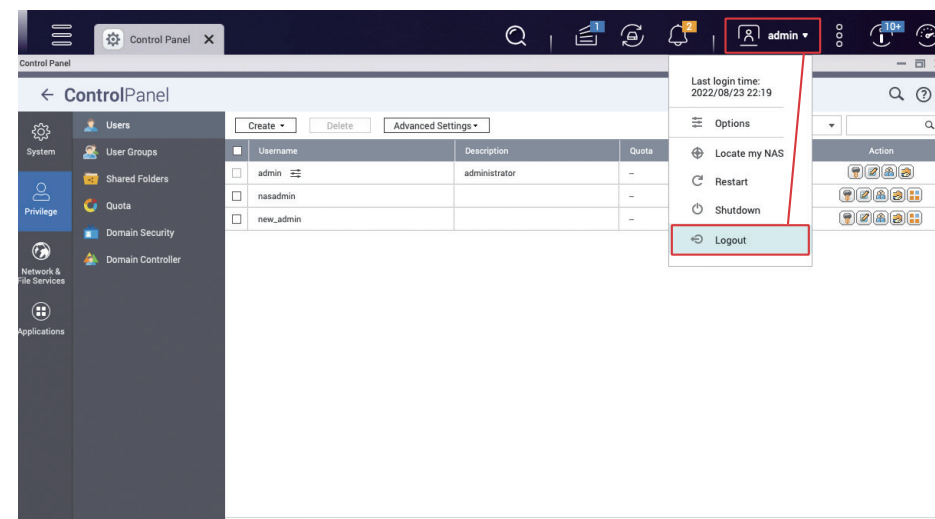
Ange användarnamnet för administratörskontot, exempelvis Ny_admin och ställ in ett starkt lösenord.



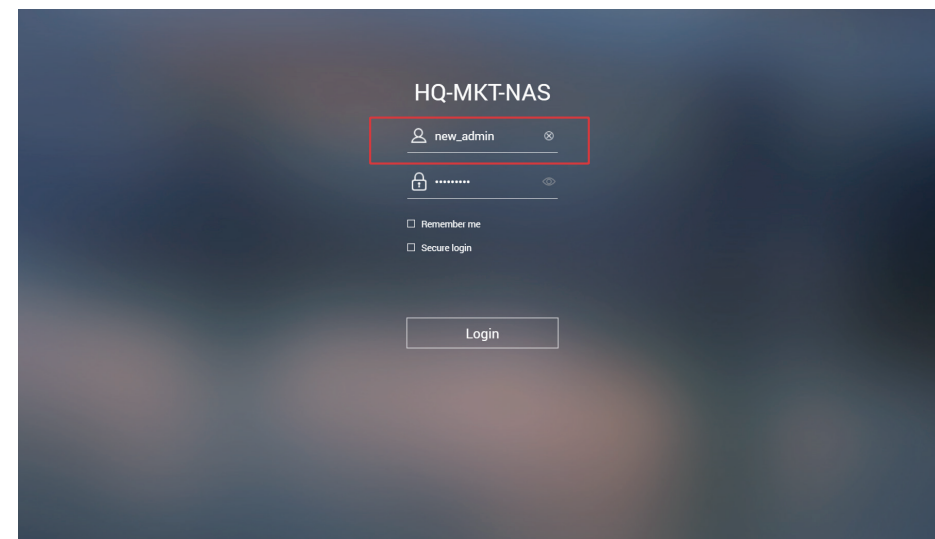
I avsnittet "Användargrupp"; klicka på "Redigera" och markera gruppen "administratörer" klicka sedan på "Skapa" för att lägga till en ny användare.



Klicka på "admin" högst upp, öppna menyn och klicka på "Logga ut" för att logga ut från QTS-webbhanteringsgränssnittet.

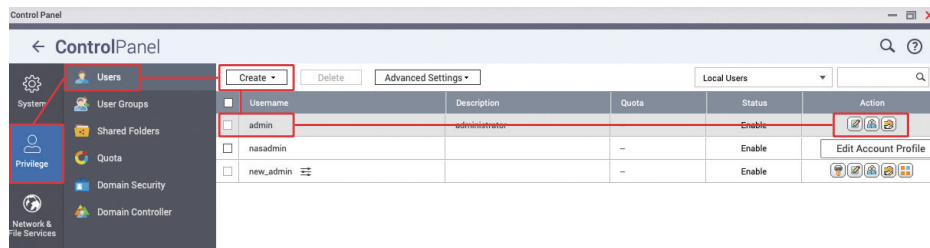


Använd det administratörskonto som du nyss skapade för att logga in på QTS-webbhanteringsgränssnittet.

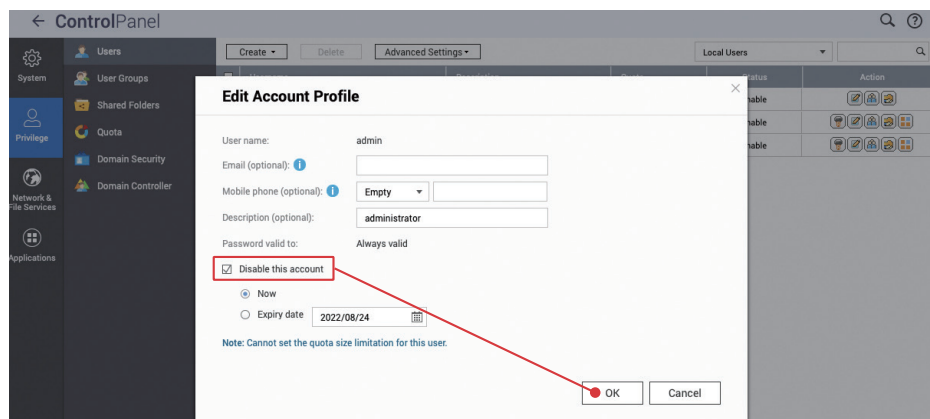


Ställ in lösenordsprincip

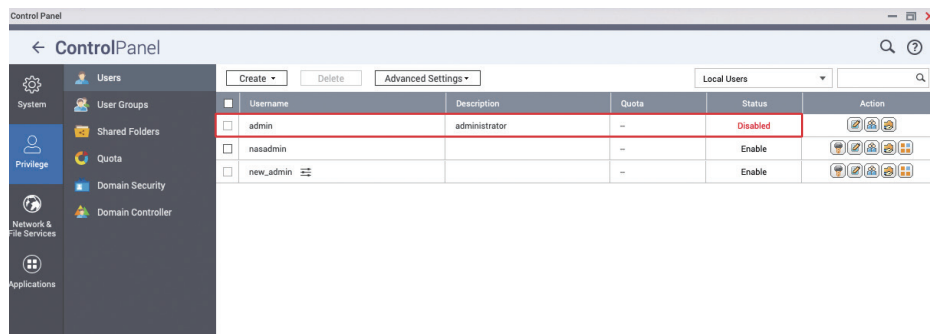
Öppna "Kontrollpanelen" igen och klicka på "Användare" på raden "admin" och klicka på "Redigera kontoprofil"



Markera "Inaktivera det här kontot" och klicka på "OK" för att slutföra

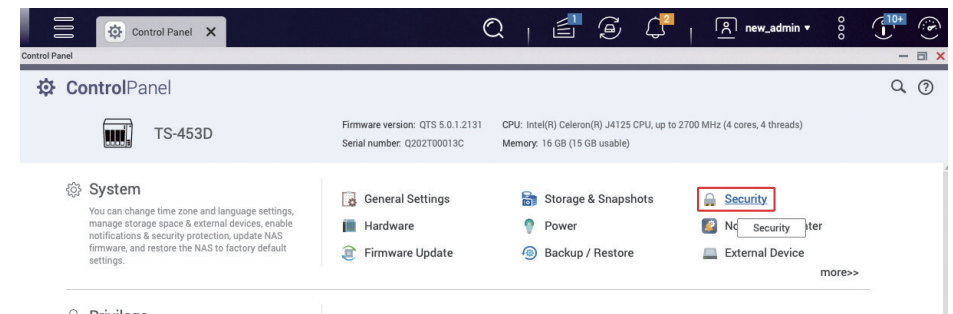


När detta är slutfört ser du att statusen för "admin" är "Inaktiverad"

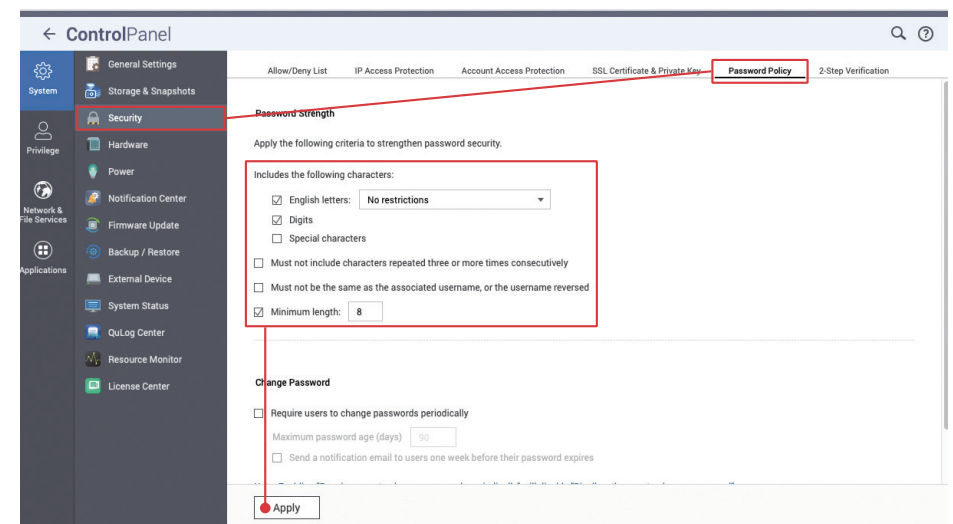


Utöver att inaktivera standardadministratörskontot "admin" måste du också vara noga med att alla konton har starka lösenord. I kombination med "Åtkomstskydd" kan det hjälpa dig att blockera skadliga inloggningsförsök. För högre säkerhet du kan framtvunga "2-stegsverifiering (2SV)" för alla konton, för att förhindra lösenordsknäckning och skadliga inloggningar.

Öppna "Kontrollpanelen" och klicka på "Säkerhetsinställningar"



Klicka på "Lösenordsprincip" för att öppna inställningssidan. Om systemet initierades i QTS 5.0.0/QuTS hero h5.0.0 (eller senare) är de grundläggande villkoren för lösenordsstyrka som standard aktiverade. Du kan ställa in villkoren för starkt lösenord efter dina behov. Lösenordet kan ställas in så att det innehåller "stora och små bokstäver och siffror från det engelska alfabetet" och lösenordslängden rekommenderas vara minst 10 tecken. Klicka på "Tillämpa" när det är slutfört.



Aktivera åtkomstskydd (IP/konto)

"Skydd mot IP-åtkomst" och "Kontoåtkomstskydd" kan bidra till att förhindra att lösenord knäcks med nyckelsökning. När en specifik IP-adress eller ett visst konto inte lyckas logga in efter för många försök aktiveras IP-blockering eller inaktivering av kontot, vilket förhindrar angripare från att försöka med nya lösenord upprepade gånger.

Klicka på "Skydd mot IP-åtkomst" för att öppna inställningssidan, markera alla tjänster och ställ in "Tidsintervall", "Misslyckade inloggningsförsök" och "IP-blockets längd" efter dina behov och klicka sedan på "Tillämpa" för att slutföra inställningarna.

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	IP block length
<input checked="" type="checkbox"/> SSH	1 minute(s)	5	5 minutes
<input checked="" type="checkbox"/> Telnet	1 minute(s)	5	5 minutes
<input checked="" type="checkbox"/> HTTP(S)	1 minute(s)	5	5 minutes
<input checked="" type="checkbox"/> FTP	1 minute(s)	5	5 minutes
<input checked="" type="checkbox"/> SAMBA	1 minute(s)	5	5 minutes
<input checked="" type="checkbox"/> AFP	1 minute(s)	5	5 minutes
<input checked="" type="checkbox"/> RTTR	1 minute(s)	5	5 minutes
<input checked="" type="checkbox"/> Rsync	1 minute(s)	5	5 minutes

Om en normal användares IP-adress blockeras av misstag kan du justera blockeringslistan genom att:

1. Logga in på hanteringsgränssnittet för QTS/QuTS hero från en annan dator
2. Ändra IP-adressen och logga in på hanteringsgränssnittet för QTS/QuTS hero
3. Logga in på hanteringsgränssnittet för QTS/QuTS hero i en mobil webbläsare
4. Använda QManager-appen

Apply

Klicka på "Kontoåtkomstskydd" för att komma till inställningssidan, aktivera relevanta tjänster, ställa in "Tidsintervall" och "Misslyckade inloggningsförsök" efter dina behov och klicka på "Tillämpa" för att slutföra inställningen.

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 checked="" type="checkbox"/> SSH	5 minute(s)	5
<input checked="" type="checkbox"/> Telnet	5 minute(s)	5
<input checked="" type="checkbox"/> HTTP(S)	5 minute(s)	5
<input checked="" type="checkbox"/> FTP	5 minute(s)	5
<input checked="" type="checkbox"/> SAMBA	5 minute(s)	5
<input checked="" type="checkbox"/> AFP	5 minute(s)	5
<input checked="" type="checkbox"/> RTTR	5 minute(s)	5
<input checked="" type="checkbox"/> Rsync	5 minute(s)	5

Om "Kontoåtkomstskydd" är aktiverat för administratörskontot finns det en möjlighet att alla administratörskonton inaktiveras på grund av lösenordsknäkningsattacker. I det skedet kan kontot "admin" endast återaktiveras via återgå-funktionen, och lösenordet för kontot "admin" återgår även det. Kom ihåg att byta ditt lösenord efter återgången.

Apply

Aktivera 2-stepsverifiering (2SV)

Klicka på "2-stepsverifiering" för att öppna inställningssidan, du kan framtvunga "2-stepsverifiering (2SV)" för "användare" eller "användargrupper". Vi rekommenderar starkt att du aktiverar 2SV för konton i "Administratörgruppen". För övriga konton kan du själv bedöma riskerna och tillämpa lämpliga inställningar.

Klicka på "Lokala användare" för att öppna menyn och välj "Lokala grupper".

Control Panel

General Settings Storage & Snapshots Security Hardware Power Notification Center Firmware Update Backup / Restore External Device System Status QuLog Center Resource Monitor License Center

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"/>	nasadmin	
<input type="checkbox"/>	new_admin	

Local Users

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

Disabled

Apply

Markera "Obligatorisk 2SV" i "administratörer" och klicka på "Tillämpa" för att slutföra inställningen.

Control Panel

General Settings Storage & Snapshots Security Hardware Power Notification Center Firmware Update Backup / Restore External Device System Status QuLog Center Resource Monitor License Center

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		--

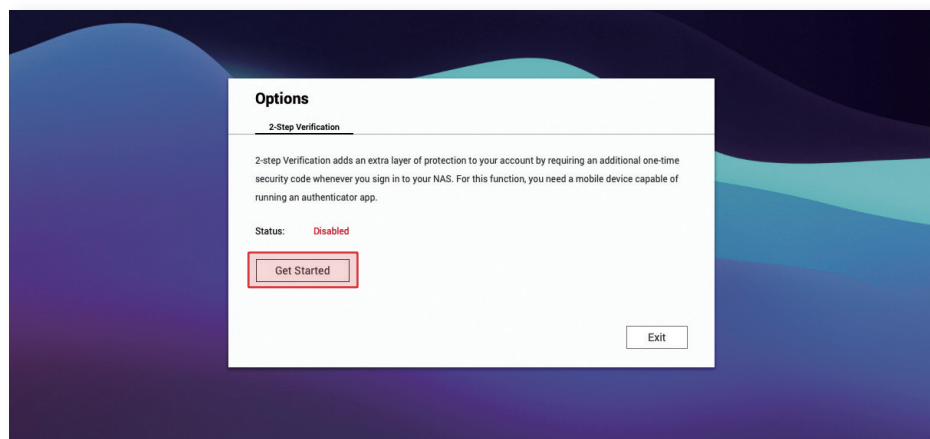
Page 1 / 1

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

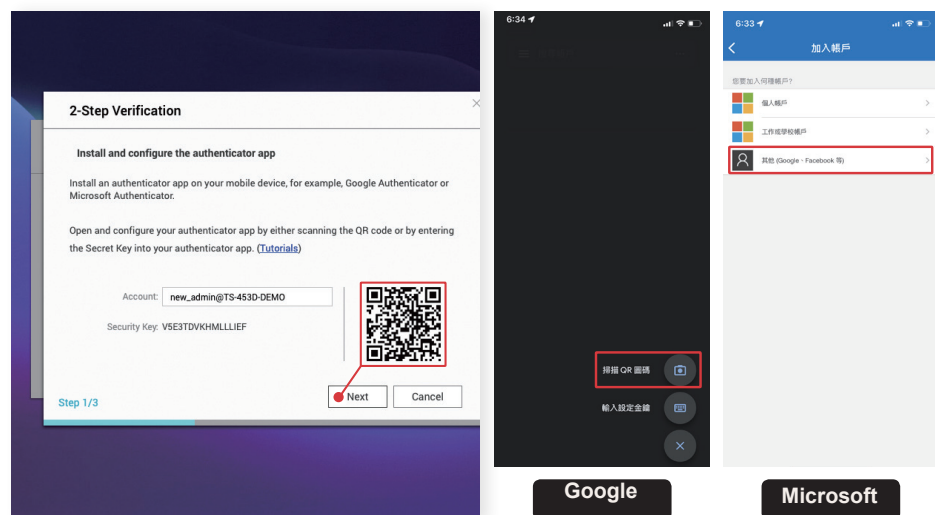
Apply

När du har aktiverat "Obligatorisk 2SV" och om kontot "Administratör" inte har ställts in med "2-stepsverifiering (2SV)" vidarebefordras du, nästa gång du loggar, till inställningssidan för "2-stepsverifiering (2SV)" för att konfigurera kontot.

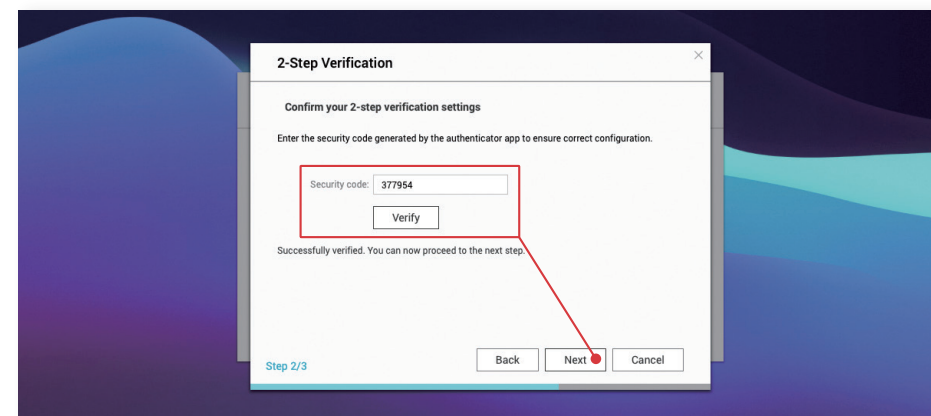
Logga in på kontot "Systemadministratör" igen och klicka på "Komma igång" för att starta inställningen.



Installera "Google Authenticator" eller "Microsoft Authenticator" på din mobila enhet, skanna QR-koden i programmet för att lägga till enheten och klicka sedan på "Nästa".

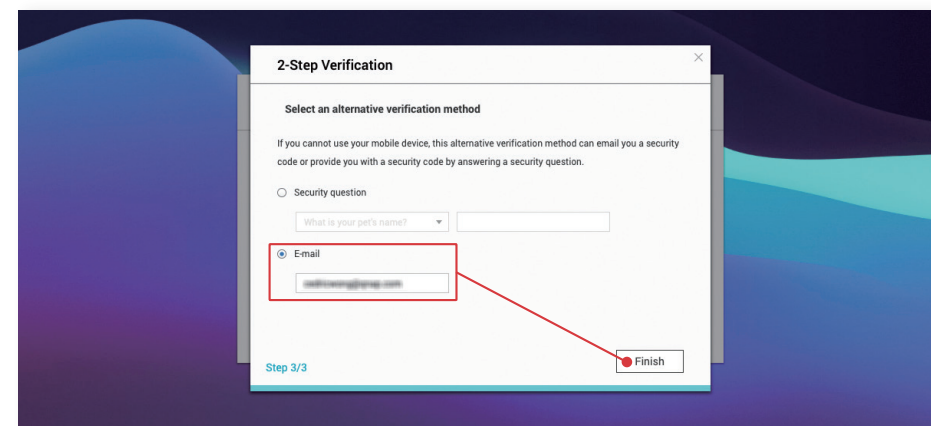


Ange den sexsiffriga "Säkerhetskoden" som genereras av "Google Authenticator" eller "Microsoft Authenticator" och klicka på "Verifiera". Efter verifieringen klickar du på Nästa för att fortsätta.



Om du vill konfigurera en alternativ verifieringsmetod* kan du välja "Säkerhetsfråga"** eller "E-postmeddelande"*** samt fylla i detta och klicka på "Slutför" för att aktivera "2-stepsverifiering (2SV)".

- * Om du inte kan få "Säkerhetskoden" från en autentiseringsapp kan du få en säkerhetskod genom att svara på "Säkerhetsfrågan" eller använda "E-post".
- ** Besvara "Säkerhetsfrågan" korrekt för att göra en godkänd 2-stepsverifiering. Använd inte frågor och svar som är okomplicerade eller lätta att gissa sig till.
- *** Du måste lägga till aviseringsmetoden "e-postmeddelande" i "Aviseringscenter" för att kunna använda den här funktionen.



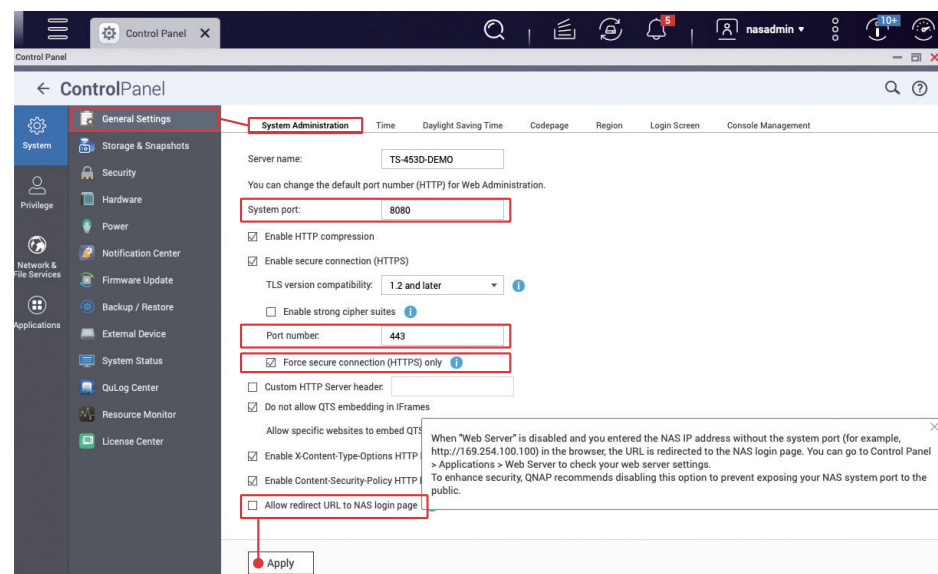
Ändra standardportar

Varje tjänst som körs på NAS:en har en motsvarande serviceport. Med undantag för vissa standardiserade tjänstportar som inte kan ändras kan resterande definieras av användarna.

När en hackare letar efter ett attackmål eller använder IoT-sökmotorn som hackare ofta använder, görs i allmänhet försök på standardporten först. För att minska risken för att bli attackerad måste du ändra standardportarna för gemensamma tjänster. När det gäller attacker mot NAS-enheter är det vanligaste målet "systemporten". Följande visar hur du ändrar "systemporten". Portarna för övriga funktioner kan ändras på den motsvarande inställningssidan. Var noga med att ändra dem innan du använder de tillhörande säkerhetstjänsterna.

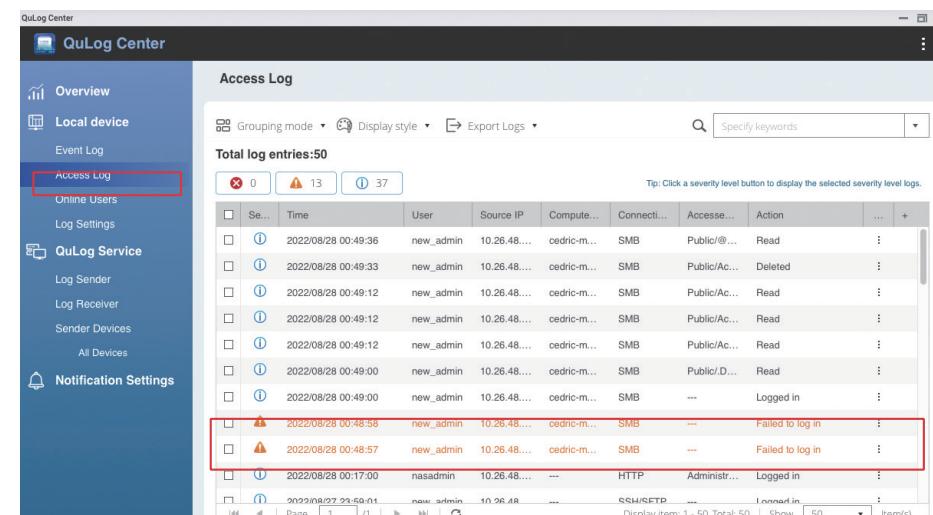
Öppna "Kontrollpanelen" och klicka på "Allmänna inställningar", "Systemporten (HTTP)" är som standard "8080", du kan ange ett portnummer mellan 1 och 65535, exempelvis "56789" för "Systemport (HTTPS)", dvs. **systemporten** (standard är "443") med funktionen "säker anslutning" aktiverad och därför är **rekommendationen att ändra den**. Samtidigt är **rekommenderas även att endast markera "Framtvinga säker anslutning (HTTPS)"** för att säkerställa att alla användare överför data via HTTPS och bidra till att förhindra hackare från att fånga upp känslig information som exempelvis kontots lösenord.

Dessutom är **rekommendationen att avmarkera "Tillåt omdirigerings-URL till NAS-inloggningssidan"** för att förhindra att "Systemporten" exponeras på grund av automatisk omdirigering. Efter ändringen; klicka på "Tillämpa" för att slutföra inställningen.

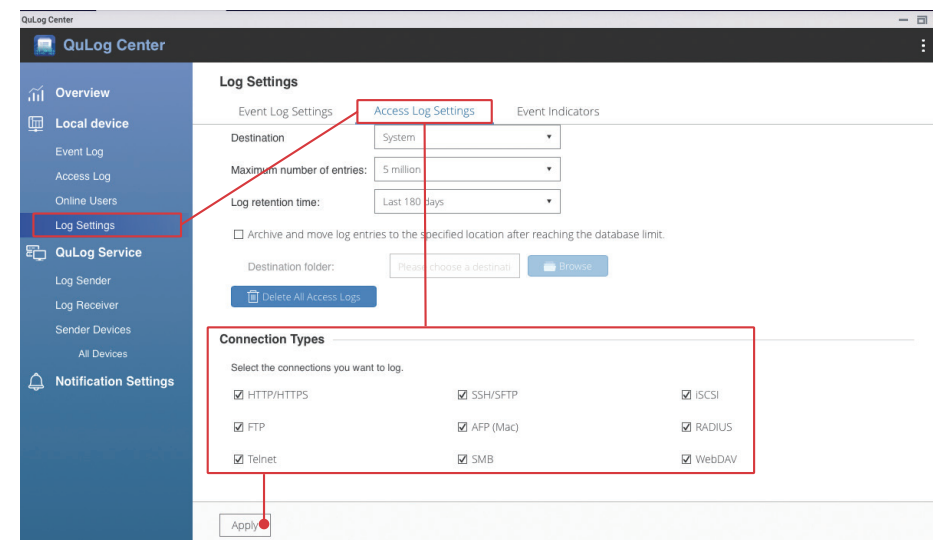


Visa åtkomstloggar

I åtkomstloggarna får du hjälp att se användarens filåtkomst, åtgärder och inloggningshistorik. När det uppstår ett problem bör kontroll av åtkomstloggar vara det första steget som tas för att diagnostisera de underliggande problemen.



Öppna "QuLog Center" och klicka på "Loggställningar" i den vänstra menyn, byt sedan till sidan för "Inställningar för åtkomstlogg", i "Anslutningstyper", kontrollera alla anslutningar och klicka sedan på "Tillämpa" för att slutföra inställningen.



Installera och aktivera säkerhetsappar

QNAP tillhandahåller flertalet säkerhetsappar som förbättrar NAS-säkerheten. Genom att konfigurera dessa appar kan NAS-säkerheten förbättras och användarna kan känna sig väl till mods.



Security Counselor kontrollerar regelbundet säkerheten för dina NAS-inställningar och informerar dig om potentiella risker.



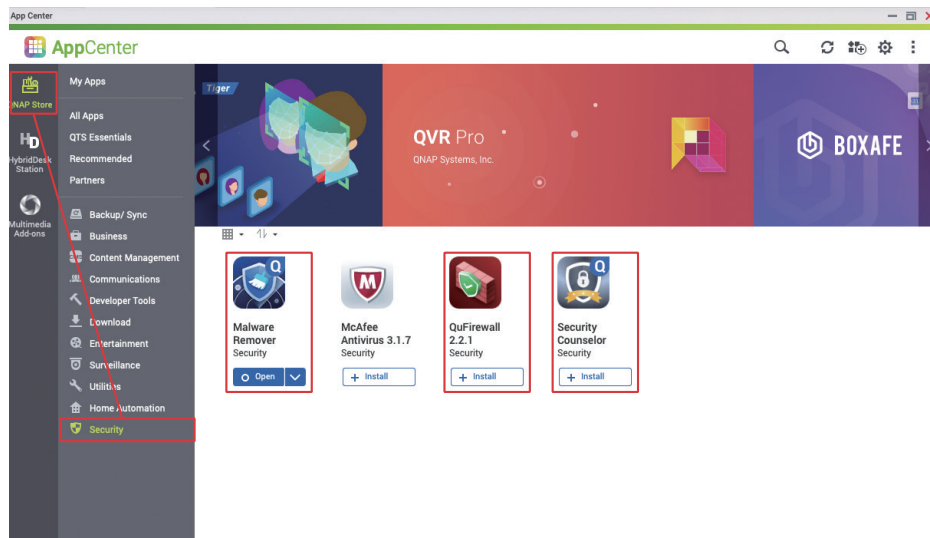
Malware Remover skannar och tar bort den skadliga programvara som upptäcks, från din NAS.



QuFirewall tillhandahåller grundläggande brandväggsfunktioner för QNAP NAS och det blockerar så många hackare som möjligt från att ansluta till din NAS.

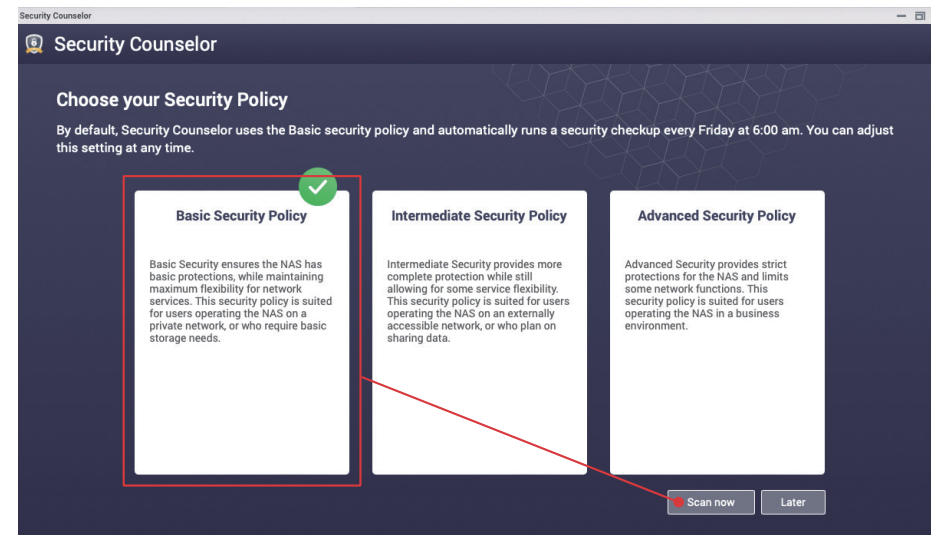
Öppna "App Center", klicka på "Säkerhet" till vänster, installera "Security Counselor", "Malware Remover"* och "QuFirewall".

* Malware Remover är förinstallerad på QTS 4.4.3 (och senare) och QuTS hero

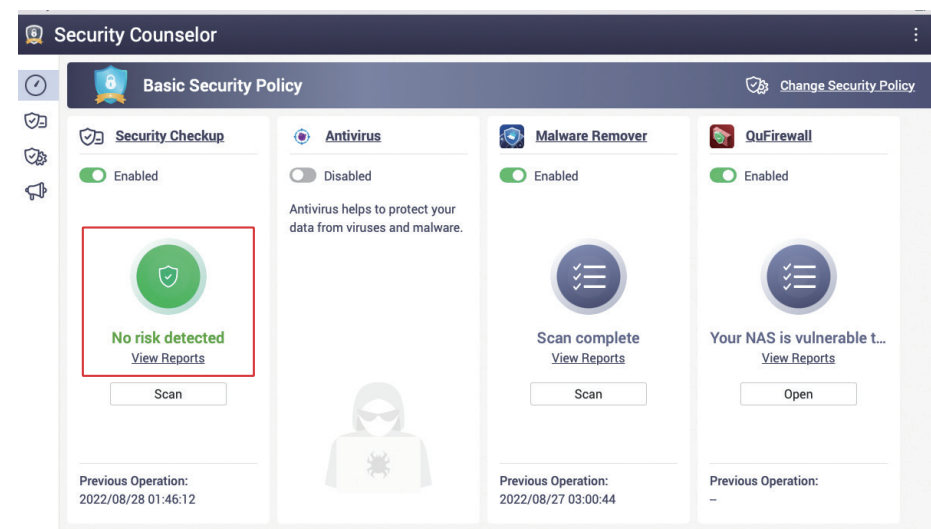


Security Counselor

Öppna "Security Counselor" och välj "Grundläggande säkerhetsprincip" och klicka på "Skanna nu".



När skanningen är klar blir resultatet vanligtvis "Ingen risk identifierad". Om en risk identifieras; klicka på "Visa rapporter" för mer utförlig information och följ instruktionerna för att ändra inställningarna.



Följande är de skanningsresultat som orsakas av "hög risk" med avsiktligt gjorda felaktiga inställningar. Klicka på "Assistenten Föreslagna inställningar" som hjälper dig att justera inställningarna.

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	The ...	⋮
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.	⋮

"Assistenten Föreslagna inställningar" ger dig en lista med relevanta förslag. När du har läst och bekräftat; klicka på "Tillämpa förslag" så tillämpar systemet automatiskt de relevanta inställningarna för dig. Vissa inställningar måste ändras manuellt, klicka på fliken "Manuellt" till vänster och justera föreslagen(slagna) inställningar. Efter att ändringarna har tillämpats startas skanningen om automatiskt. Du kan kontrollera skanningsresultaten igen för att säkerställa att inga säkerhetsrisker har identifierats på NAS:en.

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

❌ Either this setting is deselected in the Password Policy screen or the current required minimum length for passwords is below 8 characters.

✅ Configure the settings in the Password Policy screen and require the use of passwords with a minimum of 8 characters.

Apply suggestion Close

Klicka på "Säkerhetskontroll" till vänster för att komma till skärmen med skanningsresultat och klicka sedan på "Skanningsschema" till höger för att öppna skärmen för inställning av skanningsschema.

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.	⋮

Rekommendationen är att "Skanningsschema" ställs in på **minst en gång i månaden**, så att systemet regelbundet kan kontrollera inställningarna och systemstatusen. Om en risk identifieras och Aviseringscenter är korrekt konfigurerad får du en avisering så att den kan hanteras snarast möjligt.

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

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

Scan schedule

☐ Disable schedule

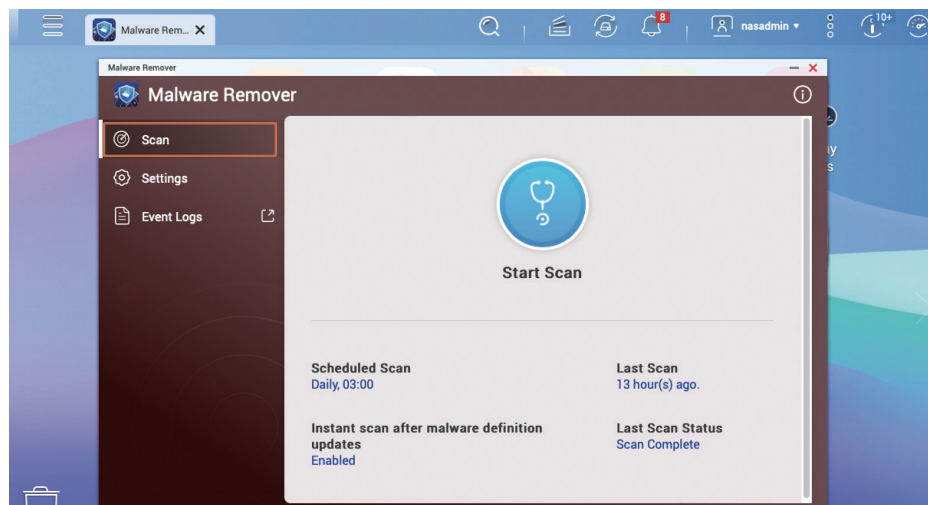
☒ Enable schedule

Run on the following days: **Friday** Run at the following time: **06 : 00**

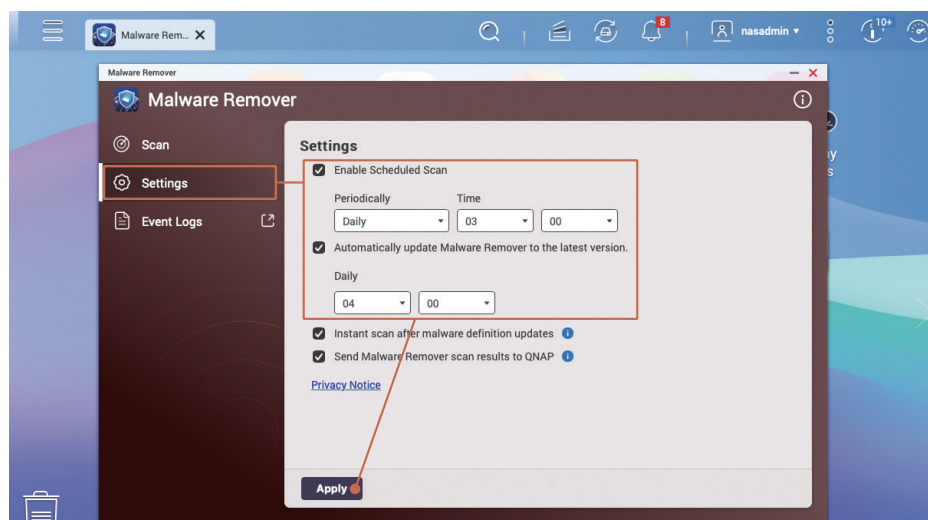
Apply Cancel

Malware Remover

Öppna "Malware Remover" som då visar statusen för den senaste skanningen, klicka sedan på "Inställningar" till vänster.

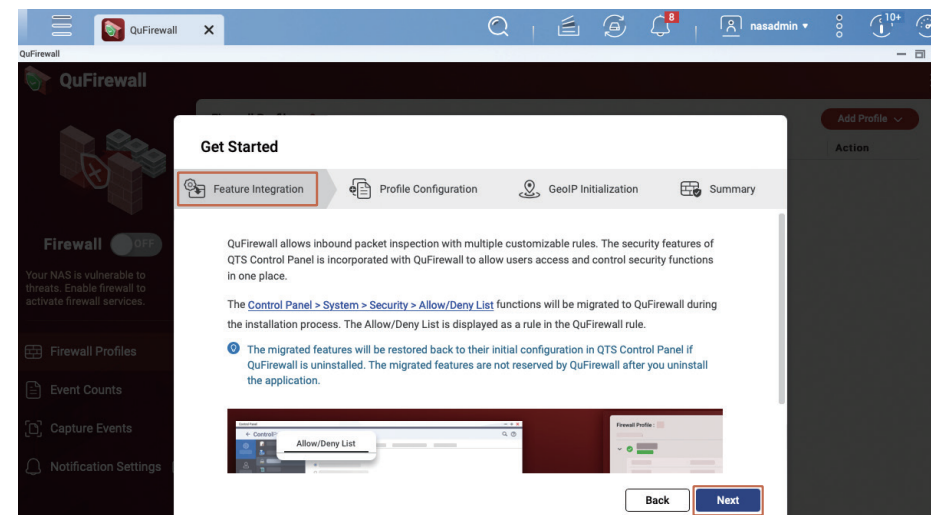


Rekommendationen är att "Skanningsschema" ställs in till **en gång per dag**, så att "Malware Remover" regelbundet kontrollerar systemstatusen. Var även noga med att "Uppdatera Malware Remover automatiskt till den senaste versionen" förblir markerad.

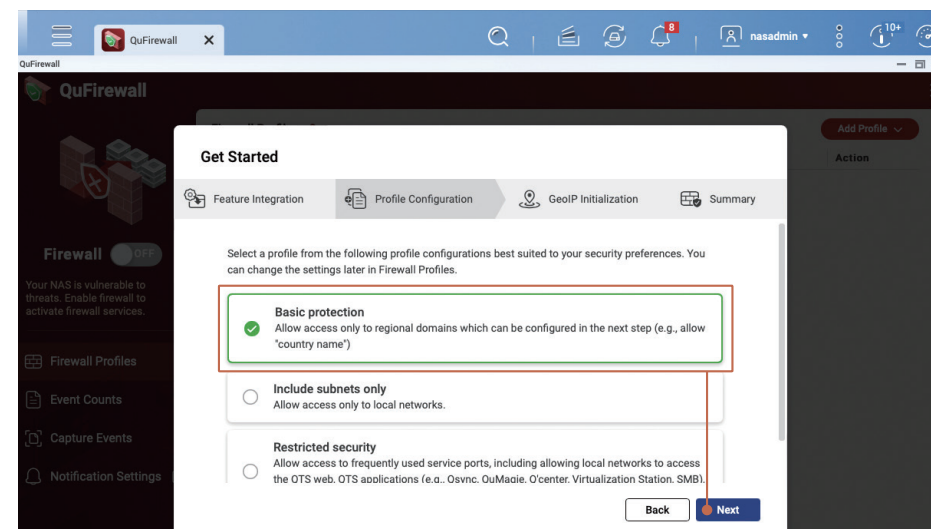


QuFirewall

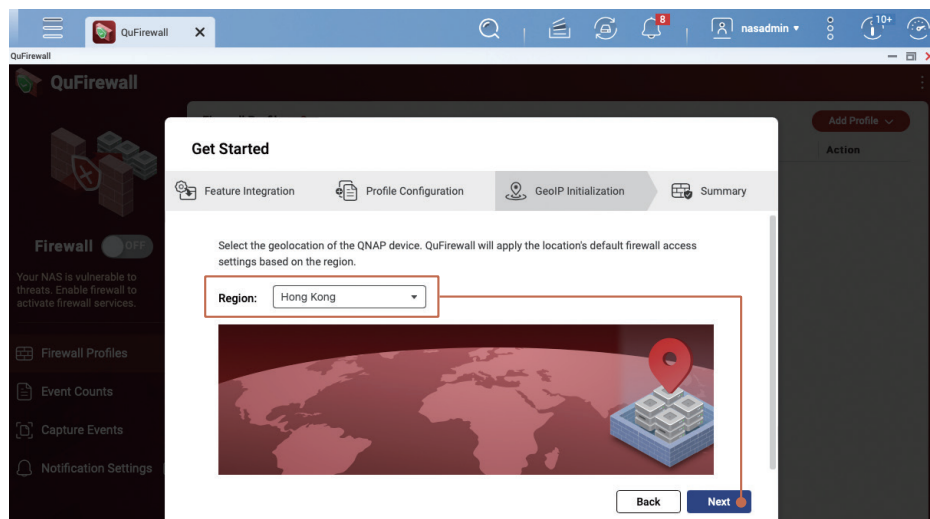
Öppna "QuFirewall". Om det här är första gången du använder QuFirewall visas skärmen Komma igång. Efter läsningen; klicka på "Nästa" för att fortsätta.



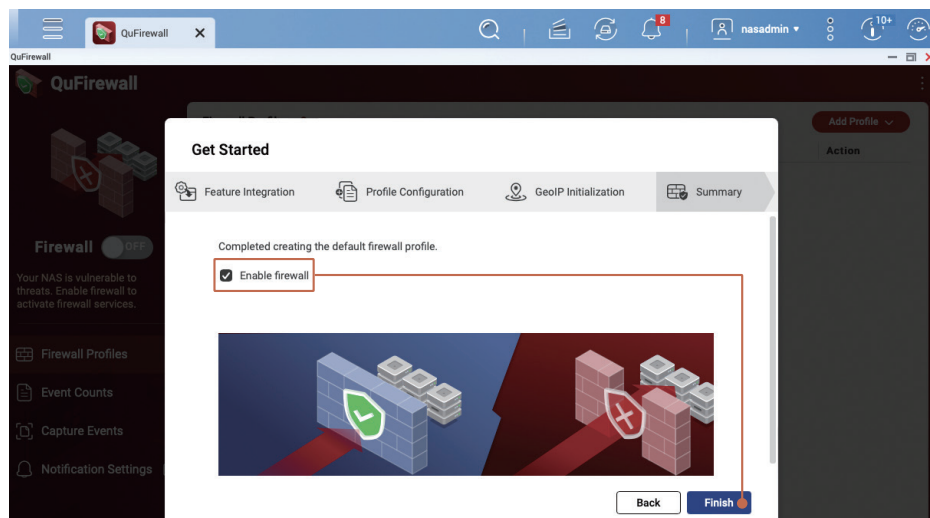
Om nätverket inte har några särskilda behov är rekommendationen att "Grundskydd" väljs, klicka sedan på "Nästa" för att fortsätta.



Ange en region enligt din plats. Om du till exempel befinner dig i Taiwan så välj "Taiwan"; om du befinner dig i Hongkong så välj "Hongkong"; om du befinner dig i Macau så välj "Macao". Du kan lägga till fler regioner senare. Klicka på "Nästa" för att fortsätta.

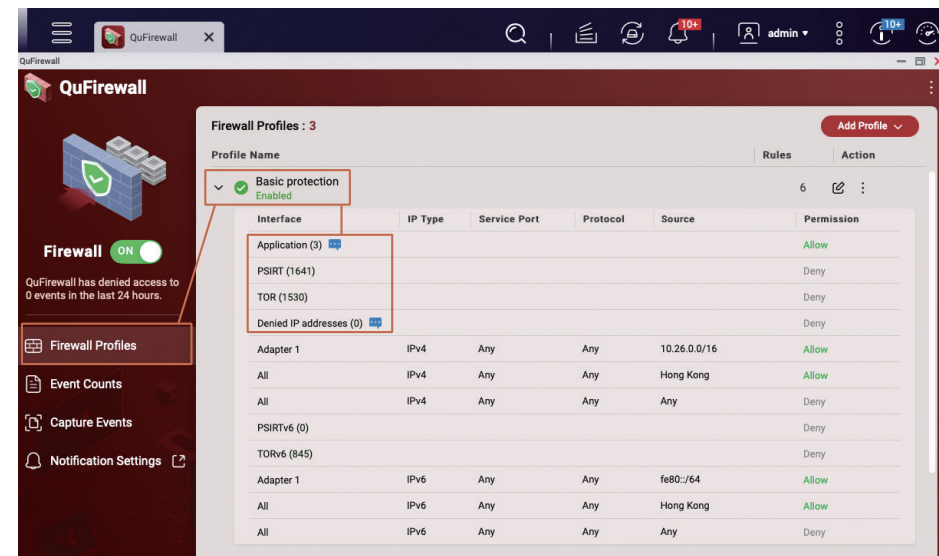


Markera "Aktivera brandvägg" och klicka sedan på "Slutför" för att tillämpa inställningarna och aktivera brandväggen.



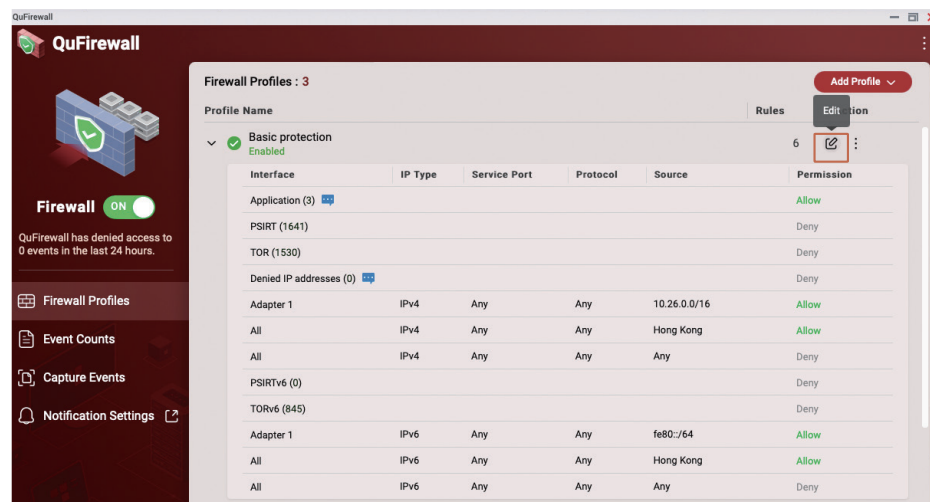
Gå till sidan QuFirewall-profiler där du ser att "Grundskydd" är aktiverat. Klicka på "Grundskydd" för att expandera och visa de motsvarande brandvägsreglerna. Informationen i de inkommande paketen kontrolleras med utgångspunkt i reglerna och tillåts passera eller blockeras enligt brandvägsreglerna. Brandvägsreglerna utförs i sekvens. Om villkoren inte uppfylls kontrolleras nästa rad med regler. Om dessa inte uppfylls hamnar de i den sista regeln "neka alla" och brandväggen blockerar relevanta anslutningar.

- Regler för "Program" skapas av systemet för att säkerställa att systemet fungerar som det ska.
- "PSIRT"-regeln är en svartlista som sammanställts av QNAP PSIRT. Den innehåller IP-adresser som är kända för att attackera QNAP NAS.
- "TOR"-regeln används för att blockera anslutningar från TOR-nätverket. TOR-nätverket används ofta av brottslingar på grund av dess anonymitet att blockera det kan minska risken för att bli attackerad.
- "Nekade IP-adresser" är IP-adresser som blockeras av funktionen "Skydd mot IP-åtkomst" eller den svarta listan som användaren lagt till manuellt.

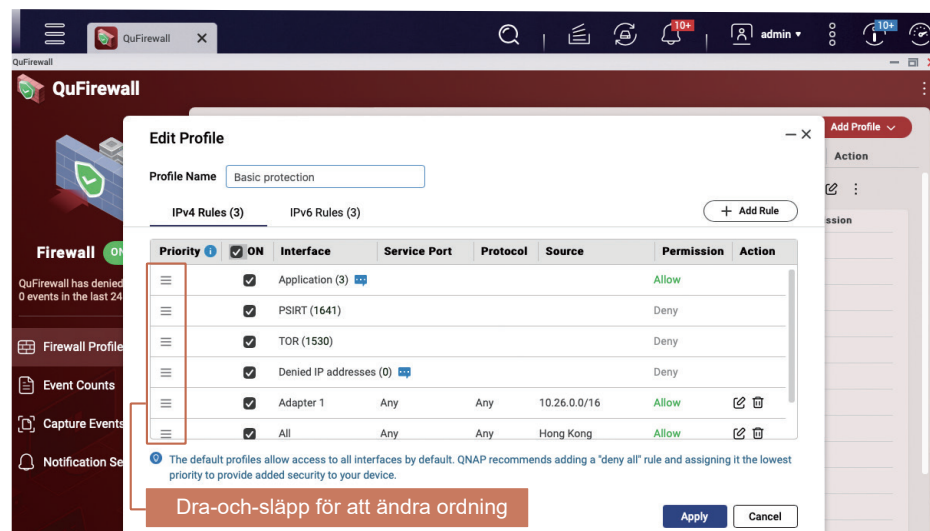


Andra regler kan anpassas av användaren och under inställningarna för grundskydd är endast Internetanslutningar från samma intranät och från samma region tillåtna. QNAP rekommenderar att du använder begreppet "vitlistning" för att hantera dina anpassade regler, dessa begränsar strikt de IP-adresser som kan ansluta till NAS-enheten.

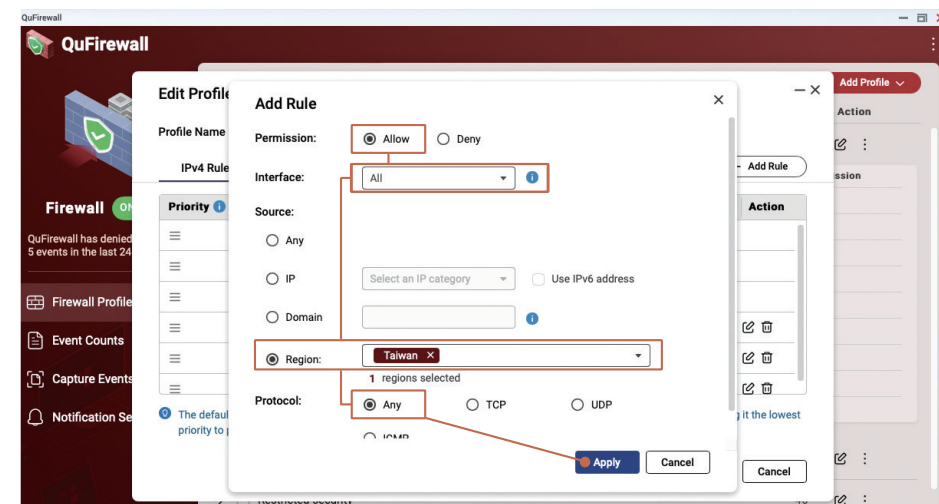
Följande visar hur du redigerar brandväggsregler. Klicka på knappen "Redigera" för att redigera på skärmen Brandväggsprofiler.



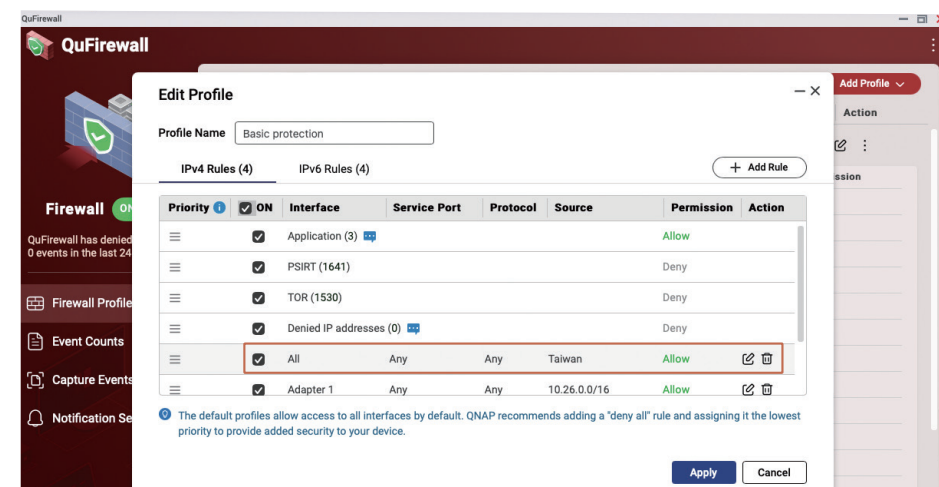
På skärmen Redigera profil kan du ändra reglernas ordning eller lägga till nya regler. Följande exempel lägger till ytterligare en region som är en tillåten anslutning; klicka på "Lägg till regel" för att öppna skärmen med inställningar.



Om du till exempel vill tillåta anslutningar från Taiwan måste "Behörighet" ställas in till "Tillåt"; "Gränssnitt" vara inställt på "Alla"; "Region" för "Källa", välj sedan "Taiwan"; "Protokoll" inställt till "Alla" och klicka sedan på "Tillämpa" för att lägga till regeln när den är slutförd.



På sidan "Redigera profil" kan du se de nyligen tillagda reglerna. Om det behövs kan du justera reglernas ordning. När de bekräftats vara korrekta; klicka på "Tillämpa".



Aktivera schemalagda snapshots

Snapshotfunktionen kan skydda dina viktiga data genom att skapa återställningspunkter i flera versioner. Du kan ställa in ett snapshotschema på QNAP NAS för att tillåta att systemet automatisk som grundskydd skapar snapshots i enlighet med schemat.

- * Schemalagda snapshots är som standard aktiverade för "fulla/tunna volymer" som skapats av QTS 5.0.0
- * I QTS 5.0.1 (och senare) har endast "tunna volymer" schemalagda snapshots aktiverade som standard
- * "Delade mappar" som skapas av QuTS hero h5.0.1 (och senare) aktiverar som standard schemalagda snapshots

Öppna "Lagring och snapshots", klicka på "Lagring/snapshots" till vänster och se till att "Lagringsutrymmet" är en "Lagringspool"-struktur och att "Lagringspoolen" har tillräckligt med ledigt utrymme för snapshotfunktionen ska fungera. Om din volymtyp är en "full volym" kan du överväga att "Ändra storlek på volym*" och "Konvertera till tunn volym*" för att frigöra utrymme för snapshotfunktion i "Lagringspool".

* Du måste säkerhetskopiera dina data innan du konverterar volymer för att undvika möjlig dataförlust.

The screenshot shows the 'Storage & Snapshots' interface. On the left, the 'Storage/Snapshots' menu is highlighted. The main area shows 'Storage Space Storage Pool: 1, Volume: 3, LUN: 0'. A table lists storage volumes: Data (5.83 TB), System (System) (2.97 TB), and Thick (98.20 GB). The 'Thick Management' window is open, showing details for the 'Thick' volume. The 'Actions' menu is open, with 'Convert to Thin Volume' highlighted. A red box highlights the 'Convert to Thin Volume' option.

* Öppna Tjock hantering för att göra relevanta justeringar som frigör utrymme i "Lagringspool"

När det är bekräftat att det finns tillräckligt med utrymme i "Lagringspool" på NAS;en; klicka först på "Volym" och sedan på "Snapshot" högst upp, klicka därefter på "Snapshothanteraren" i menyn.

The screenshot shows the 'Storage & Snapshots' interface. The 'Snapshot' menu is highlighted at the top. The 'Snapshot Manager' option is highlighted in the dropdown menu.

Gå till inställningssidan för "Snapshothanteraren" i "Volym" och klicka på "Schemalägg snapshot" längst upp till höger.

The screenshot shows the 'Snapshot Manager' interface. The 'Schedule Snapshot' button is highlighted with a red box. The 'Take Snapshot' button is also visible.

Ändra "Aktivera schema" till tillståndet "Aktivera" och ändra sedan schemat efter dina behov. Rekommendationen är att du använder "Dagligen" eller "Veckovis".

The screenshot shows the 'Snapshot Settings' window. The 'Enable schedule' toggle is turned on. The 'Repeat' dropdown is set to 'Daily' and the 'Time' is set to '01:00 (h:mm)'. The 'Snapshot retention policy' is set to 'Smart Versioning'.


Du kan ställa in en bevarandepincip för snapshots för att begränsa antalet snapshots och förhindra att snapshots använder för mycket utrymme.

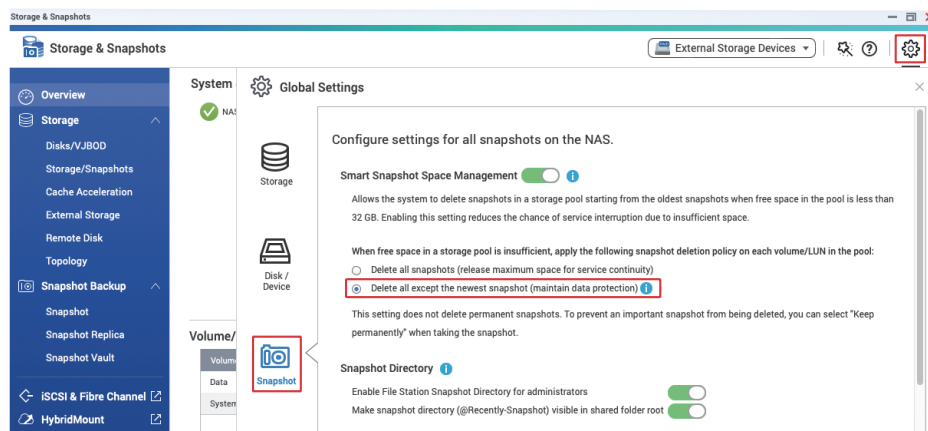
Det rekommenderas att ställa in "Smart versionshantering", det vill säga GFS-regeln (farfar-far-son (Grandfather-Father-Son)) så att det finns tillräckligt många versioner för dataskydd. När inställningen är klar; klicka på "OK" för att tillämpa inställningarna.

The screenshot shows the 'Snapshot Settings' window, specifically the 'Snapshot Retention' tab. The 'Smart Versioning' option is selected. The 'Maximum amount of time to keep' is set to '0 Months'. The 'Maximum number of snapshots to keep' is set to '0 Snapshots'. The 'Smart Versioning' section shows: Hourly snapshots: 24, Daily snapshots: 7, Weekly snapshots: 4, Monthly snapshots: 12.

Ställ in princip för snapshottradering

När lagringspoolen har otillräckligt med utrymme raderar systemet snapshots, baserat på dina inställningar, för att upprätthålla normal systemservice och undvika potentiella driftstopp på grund av otillräckligt utrymme.

I "Lagring och snapshots"; klicka på knappen "Inställningar"  högst uppe i det högra hörnet, öppna "Globala inställningar" och klicka på "Snapshot". Rekommendationen är att det ställs in till "Radera alla utom det senaste snapshotet" för att undvika att alla snapshots återställs och skyddet därigenom går förlorat.

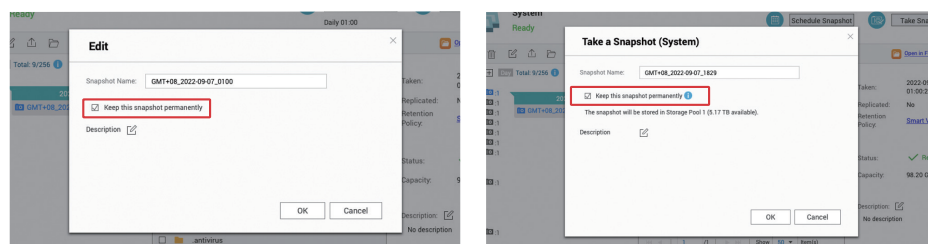


Om du vill att systemet ska behålla alla snapshots, även när "Lagringspool" har otillräckligt med utrymme inaktiverar du "Utrymmeshantering för Smart snapshot". Observera att det innebär att "Lagringspool" går över till tillståndet skrivskydd/radera när lagringsutrymme är inte räcker till. Du måste manuellt radera snapshotet för att återställa "Lagringspool" till normal drift. Var noga med att regelbundet kontrollera utrymmes användningen efter att du har inaktiverat den här funktionen.



För att undvika skyddsfel på grund av principen för snapshottradering rekommenderar vi att alla eller några av snapshoten ställs in till "Behåll snapshotet permanent" * efter att en stor mängd data lagrats, för att förhindra att snapshotsen kasseras av systemet.

* Måste raderas manuellt för att frigöra utrymme. Vi rekommenderar att regelbundet skapa och radera



Kontrollista för NAS-säkerhetsinställningar

□ Konfigurera Aviseringscenter

- Ställ in minst en aviseringsmetod
- Skapa regler för "Larmmeddelanden"
- Skapa aviseringsregler för "Uppdatering av inbyggd programvara"

□ Aktivera automatisk uppdatering av inbyggd programvara (QTS/QuTS hero)

□ Konfigurera App Center

- Uppdatera alla appar till den senaste versionen
- Förbjud installation av program som inte har en giltig digital signatur
- Aktivera automatiska uppdateringar

□ Inaktivera eller ta bort onödiga funktioner

- Kontrollera om aktiverade tjänster är nödvändiga
- Kontrollera i App Center om de appar som är aktiverade är nödvändiga
- Inaktivera SSH
- Inaktivera Telnet

□ Stärk systemkontosäkerheten

- Inaktivera standardkontot "admin"
- Ställ in lösenordsprincip
- Aktivera IP-åtkomstskydd
- Aktivera 2-stegsverifiering (2SV)

□ Ändra standardsystemport

□ Aktivera åtkomstlogg

□ Installera och aktivera säkerhetsappar

- Security Counselor
 - Starta schemalagd skanning
- Malware Remover
 - Starta schemalagd skanning
- QuFirewall
 - Aktivera brandvägg
 - Ställ in Geo-IP-region
 - aktivera PSIRT-regler
 - Aktivera TOR-regler

□ Aktivera schemalagda snapshots

- Ange regelbundet "Behåll snapshot permanent"

Vanliga frågor

Q Är det säkrare att koppla bort NAS:en från Internet?

A Nej. "Bortkoppling" av NAS-enheten avser i allmänhet att stänga ute NAS-enheten från nätverket så att den inte kan initiera anslutningar till omvärlden. Även om vissa skadliga program kräver en extern anslutning för att köras, finns det fortfarande skadlig kod som kan utföra skadliga åtgärder utan någon extern anslutning. Därför blir det inte bara ett misslyckande med att förhindra hackare från att utföra olagliga åtgärder det innebär även att vissa systemfunktioner förhindras från att fungera korrekt, exempelvis automatiska programvaruuppdateringar och aviseringar. Det rätta sättet är att begränsa trafiken till NAS:en, som att exempelvis undvika exponering för Internet, för att förbättra säkerheten.

Q Min hårddisk är konfigurerad med RAID, betyder det att jag inte behöver säkerhetskopiera?

A Nej. RAID är inte en säkerhetskopieringsmetod. RAID-nivåer över 0 är endast avsedda att ge redundans mot diskfel. RAID ger inget skydd mot radering eller kryptering av data. Därför är rekommendationen att på lämpligt sätt **säkerhetskopiera data enligt principen 3-2-1-säkerhetskopiering**.

Q Jag har redan konfigurerat snapshots, betyder det att jag inte behöver säkerhetskopiera?

A Nej. Eftersom "snapshots" lagras på samma uppsättning hårddiskar som dina data går även data förlorade om det uppstår ett RAID-fel. Om hackare dessutom kommer över tillräckliga privilegier (genom att exempelvis framgångsrikt knäcka administratörskontot) kan även snapshotbilden tas bort. Därför är rekommendationen att korrekt säkerhetskopiera snapshotsfilerna enligt 3-2-1-principen för säkerhetskopiering.

Q Min NAS är inte exponerad för Internet, betyder det att den omöjligen kan bli attackerad?

A Nej. Även om de flesta cyberattacker kommer från Internet så löper NAS:en fortfarande en att attackerats på intranätet. Om exempelvis en annan dator eller enhet på intranätet hackas eller påverkas av skadlig programvara kan den användas för att attackera och sprida sig till andra enheter på intranätet. Genom att installera antivirusprogram och distribuera nätverkssäkerhetsprodukter på datorn kan du få hjälp att hantera berörda hot. Exempelvis QNAP ADRA NDR kan identifiera misstänkta intranätaktiviteter och isolera dem automatiskt. Rekommendationen är att även säkerhetskopiera data korrekt enligt 3-2-1-principen för säkerhetskopiering.

Q Min NAS har använts under lång tid, hur kontrollerar jag om det finns skadlig programvara installerad?

A Om du ser tecken på att processorbelastningen är onormalt hög, upplever fel i programvaruuppdateringen eller om det finns okända appar i App Center, är det möjligt att ett skadligt program har installerats. Rekommendationen är att du installerar och använder den senaste versionen av Malware Remover. Om du fortfarande inte kan lösa problemet ber vi dig kontakta QNAP:s tekniska supportteam för att få hjälp.

Q Om det är nödvändigt för mig att öppna vissa tjänster på Internet, vad behöver jag göra för att garantera säkerheten?

A Se till att NAS:en har den senaste versionen av inbyggd programvara och appar installerade. Du kan aktivera QuFirewall för att få en grundläggande brandväggs-skydd och reglerna "PSIRT" och "TOR" kan bidra till att blockera vissa hackares anslutningar. Om du är en företags- eller enterpriseanvändare är rekommendationen att använda en brandväggs-lösning på hög nivå. Om lagringspoolutrymmet tillåter kan du dessutom skapa "snapshots" för grundläggande dataskydd. Rekommendationen är även att säkerhetskopiera data korrekt enligt 3-2-1-principen för säkerhetskopiering som en förberedelse för det sämsta möjliga scenariot och förhindra potentiell dataförlust.

Q Min NAS är gammal och har inte stöd för den senaste versionen av QTS, kan den fortfarande användas på ett säkert sätt?

A Äldre modeller och EOL-modeller (End of Life, uppnått livslängden) har begränsad support och bör endast användas för säkerhetskopiering på intranät/offline.

Q Varför får jag en varning om inloggningsfel på NAS-enheten?

A Om IP-adressen för den misslyckade inloggningen kommer från Internet betyder det att det pågår en attack, i form av lösenordsknäckning med ordlista, på din NAS. Du bör undvika att exponera din NAS för Internet och följa den här självstudien för att stärka din NAS. Om IP-adressen för den misslyckade inloggningen är från intranätet behöver du kontrollera om enheten med den IP-adressen har skadlig programvara installerad.

Q Varför har alla mina filer konstiga filnamn?

A Det är ett symptom på en ransomwareinfektion. Kontrollera NAS-åtkomstloggarna för att avgöra om krypteringsåtgärden är från en annan dator eller själva NAS:en. Om din NAS har påverkats av en ransomware bör du vidta lämpliga åtgärder för att stoppa infektionsspridningen. Kontakta vid behov QNAP:s tekniska supportteam för att få hjälp.

Q Vad ska jag göra om min NAS infekteras med en ransomware?

A De flesta ransomware använder oforcerbara krypteringsmetoder. Om det inte finns någon korrekt nyckel kan filerna inte låsas upp, vilket innebär att filerna bara kan återställas med säkerhetskopiering eller snapshot.

Ändra omedelbart routerinställningarna, enligt den här självstudien, för att undvika att exponera NAS:en för Internet och för att förhindra sekundära attacker. Därefter bör du omedelbart stänga av alla synkroniseringsuppgifter och snapshots som är inställda för permanent bevaring, för att undvika att förlora säkerhetskopierade filer. Om dina data har säkerhetskopior eller snapshots som du kan återställa kan du återställa filerna efter att du har uppdaterat NAS:ens inbyggda programvara och appar och efter genomsökning med Malware Remover. Om data inte säkerhetskopierats ber vi dig säkerhetskopiera utpressningsmeddelandet som lämnats av ransomware och vilken betalningsmetod som avses för att därefter försöka använda metoder som dataåterställning för att återställa vissa data. Kontakta vid behov QNAP:s tekniska supportteam för att få hjälp.

Q Jag ser hela tiden medierapporter om att QNAP korrigerar produktsårbarheter. Betyder det att QNAP-produkter inte är säkra?

A Ingenstans i världen finns det perfekt programvara och hårdvara. Det spelar ingen roll om det är egenutvecklad programvara av olika tillverkare eller programvara med öppen källkod, eller till och med hårdvara. Det finns alltid sårbarheter som hittas och vilka tillverkarna sedan korrigerar. Precis som andra stora teknikföretag fortsätter QNAP att korrigera kända sårbarheter och sedan släppa uppdateringsfiler så att användare kan uppdatera så snart som möjligt, för att säkerställa säkerheten för användarnas enheter och data. QNAP PSIRT utfärdar även cybersäkerhetsmeddelanden som blir åtkomliga externt, så att användare kan agera mot problem som uppstår. QNAP anser att hanteringen av sårbarheter på ett öppet och genomsynligt sätt kan skydda användarnas rätt att känna till och bidra till att förbättra produktsäkerheten. Användare uppmanas också att prenumerera på QNAP:s Säkerhetsråd för att få relevant, korrekt och fullständig information innan de läser om det i medierapporterna.

QNAP:s Säkerhetsråd:

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



Q Vad är 3-2-1-säkerhetskopieringsprincipen?

A 3-2-1-säkerhetsprincipen är en välkänd säkerhetsprincip inom IT-branschen. Det förbereder för det sämsta tänkbara scenariot. Det säkerställer att det i händelse av en katastrof finns säkerhetskopierade filer för att återställa data och därigenom undvika förluster och säkerställa säkerheten.

"3" i Säkerhetskopiering 3-2-1 betyder minst tre säkerhetskopior; "2" betyder minst två lagringsmedia; "1" betyder att minst en kopia finns på annan plats.

Baserat på 3-2-1-säkerhetskopieringsprincipen, kommer det att finnas säkerhetskopiefiler som kan återställas, oavsett om det behövs på grund av oavsiktlig modifiering, radering, hårdvaruskada, virusinfektion och katastrofer som bränder och översvämningar.

För att uppfylla denna princip innehåller QNAP NAS Hybrid Backup Sync 3 (HBS3), Snapshot Replica och SnapSync (stöds endast av QuTS hero) för att säkerhetskopiera data på NAS:en till en extern NAS, offentligt moln, extern lagring, andra filservrar och/eller andra enheter för att säkerställa att ingenting går förlorat.

Relaterade självstudier för Hybrid Backup Sync 3 (HBS3):

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



Relaterade självstudier för Snapshot Replica:

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



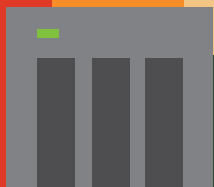
Självstudier för SnapSync:

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



För att förbättra säkerheten kan du lägga till Offline Backup eller säkerhetskopiering till QuTS heros WORM (Write Once Read Many) lagringsutrymme för att förhindra att data manipuleras.

NOTA



2 0 2 3

Guía de seguridad



QNAP SYSTEMS, INC.

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

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

QNAP kan när som helst ändra specifikationer och produktbeskrivningar utan föregående meddelande.

Copyright © 2023 QNAP Systems, Inc. Med ensamrätt.

QNAP® och andra namn på QNAP-produkter är varumärken eller registrerade varumärken som tillhör QNAP Systems, Inc.

Andra produkter och företagsnamn som nämns här är varumärken som tillhör respektive innehavare.