

QNAP

2 0 2 3

Guida alla sicurezza



2 0 2 3

Guida alla sicurezza

INDICE

- 1 Prefazione
- 2 Attacchi comuni
- 3 Concetti sulle apparecchiature di rete di base
- 4 Vari modi per connettersi da Internet al NAS

Evitare di esporre il NAS a Internet

- 8 Collegare il NAS correttamente
- 9 Controllare le impostazioni del router
- 12 Controllare le impostazioni NAS
- 15 Elenco di controllo delle impostazioni relative alla rete

Impostazioni Sicurezza NAS

- 17 Impostare le notifiche di sistema
- 24 Abilitare l'aggiornamento automatico firmware (QTS / QuTS Hero)
- 25 Impostazioni aggiornamento app
- 27 Disattivare o rimuovere le funzioni non necessarie
- 29 Disattivare Telnet / SSH
- 30 Rafforzare la sicurezza degli account di sistema
- 34 Impostare il criterio password
- 35 Abilitare la protezione accesso (IP / account)
- 36 Abilitare la verifica in due fasi (2SV)
- 39 Modifiche a porte predefinite
- 40 Visualizzare il log accesso
- 41 Installare e abilitare le applicazioni di sicurezza
- 42 Security Counselor
- 45 Malware Remover
- 46 QuFirewall
- 51 Abilitare snapshot pianificate
- 53 Impostare il criterio di eliminazione delle istantanee
- 54 Elenco di controllo delle impostazioni di sicurezza NAS

QNAP attribuisce grande importanza alla sicurezza. Per far fronte alle crescenti minacce, QNAP migliora costantemente la progettazione di hardware e software per fornire agli utenti soluzioni sicure e convenienti.

Il Product Security Incident Response Team (PSIRT) di QNAP è responsabile della gestione dei problemi di sicurezza relativi ai prodotti QNAP. Oltre a gestire gli incidenti legati alla sicurezza informatica, il PSIRT gestisce anche la segnalazione, l'indagine, la correzione e l'annuncio delle vulnerabilità in vari prodotti.

QNAP si impegna inoltre a migliorare la sicurezza dei prodotti. In passato, i prodotti sono stati progettati per essere più comodi e facili da configurare e utilizzare per gli utenti. Con l'aumento degli attacchi informatici contro i dispositivi di rete, negli ultimi anni, anche la prospettiva di progettazione dei prodotti QNAP è cambiata e la progettazione dei prodotti è passata a Security by Design per fungere da gatekeeper per gli utenti e garantire che gli utenti possano affrontare le minacce correlate.

Il tutorial aiuterà gli utenti a configurare correttamente il NAS per migliorare la sicurezza. In caso di domande, contattare l'assistenza tecnica per ottenere maggiori informazioni:



Per informazioni sulle vulnerabilità del prodotto e sugli incidenti correlati alla sicurezza, fare riferimento a e sottoscrivere gli avvisi sulla sicurezza QNAP:

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



Servizio clienti QNAP:

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



Per sapere come difendersi dagli attacchi informatici, è necessario comprendere come vengono lanciati. Per quanto riguarda gli attacchi al NAS, la maggior parte di questi sono lanciati attraverso Internet. Gli attacchi sono principalmente di due tipi: "violazione della password" e "attacco alla vulnerabilità". In questo caso, l'"attacco alla vulnerabilità" può essere suddiviso in "N-day" e "0-day".

"N-day" si riferisce allo sfruttamento di una vulnerabilità con patch per lanciare un attacco e la maggior parte degli attacchi attivi attualmente in uso rientra in questa categoria. È possibile difendersi efficacemente da tali attacchi installando sempre le patch e gli aggiornamenti di sicurezza più recenti.

"0-day" si riferisce allo sfruttamento di una vulnerabilità sconosciuta per lanciare un attacco e i fornitori possono emettere patch di sicurezza solo dopo l'evento. Questi attacchi possono essere contrastati in modo efficace solo impedendo agli utenti malintenzionati di connettersi al dispositivo.

La tabella seguente mostra le risposte ai diversi attacchi come riferimento per gli utenti.

Risposta	Attacchi		
	Violazione della password	Attacco alla vulnerabilità (N-day)	Attacco alla vulnerabilità (0-day)
Evitare l'esposizione a Internet	V	V	V
Aggiornare software (sistema e applicazioni)	X	V	Δ
Abilitare l'aggiornamento automatico (sistema e applicazioni)	X	V	Δ
Utilizzare password complesse per tutti gli account	V	X	X
Disabilitare l'account "admin" predefinito	V	X	X
Abilitare verifica in 2 fasi	V	X	X
Abilitare la protezione di accesso	Δ	X	X
Abilitare il firewall	Δ	Δ	Δ
Ricevere notifiche di sistema	Δ	Δ	Δ
Modificare porte predefinite	Δ	Δ	Δ
Disabilitare/rimuovere funzioni non necessarie	Δ	Δ	Δ

V: Effettivo X: Non effettivo Δ: Potenzialmente efficace (significa che l'attacco può essere mitigato o che il rischio di essere attaccato diminuisce)

"Evita esposizione a Internet" può impedire efficacemente agli utenti malintenzionati di connettersi al dispositivo e di lanciare attacchi. Questo tutorial inizia con l'argomento "Evitare l'esposizione a Internet", quindi fornisce un tutorial completo sulle "Impostazioni di sicurezza NAS" per migliorare le capacità difensive del NAS.

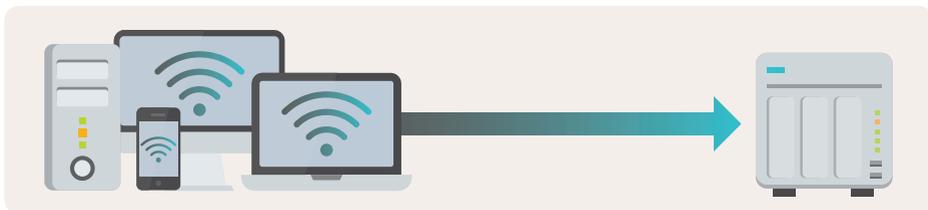
Come dispositivo di rete, il NAS ha due direzioni di connessione.

01 | Connessione esterna NAS



Un NAS richiede generalmente una connettività esterna per funzionare correttamente. Ad esempio, le funzioni di base del sistema, come gli aggiornamenti automatici e l'invio di notifiche. Inoltre, se è necessario eseguire il backup dei dati NAS su un cloud pubblico o utilizzare il NAS per eseguire il backup dei dati da altri dispositivi o cloud pubblici (ad esempio macchine virtuali, Google Workspace o Microsoft 365), computer o server, il NAS deve essere in grado di avviare connessioni in uscita.

02 | Altri dispositivi (come computer, cellulari o altri server) che si connettono al NAS



Se è necessario utilizzare qualsiasi funzione o servizio fornito dal NAS, incluso l'accesso ai file, l'accesso all'interfaccia delle impostazioni, è necessario essere in grado di avviare le connessioni al NAS.

Se il router non dispone di DMZ, Port Forwarding o UPnP, il traffico proveniente da Internet verrà bloccato. Solo i dispositivi sulla rete locale potranno accedere al NAS.

Quando il router è abilitato e le funzioni sopra indicate sono impostate, tutti gli utenti di Internet possono connettersi alla porta aperta, quindi inoltrare al NAS in base alle regole del router, quindi accedere e utilizzare le funzioni correlate normalmente. Tuttavia, fornirà anche agli hacker anche i mezzi per attaccare attraverso la violazione delle password o lo sfruttamento delle vulnerabilità del software, mettendo così a rischio la sicurezza.

01 | Abilitare e configurare DMZ, Port Forwarding o UPnP sul router

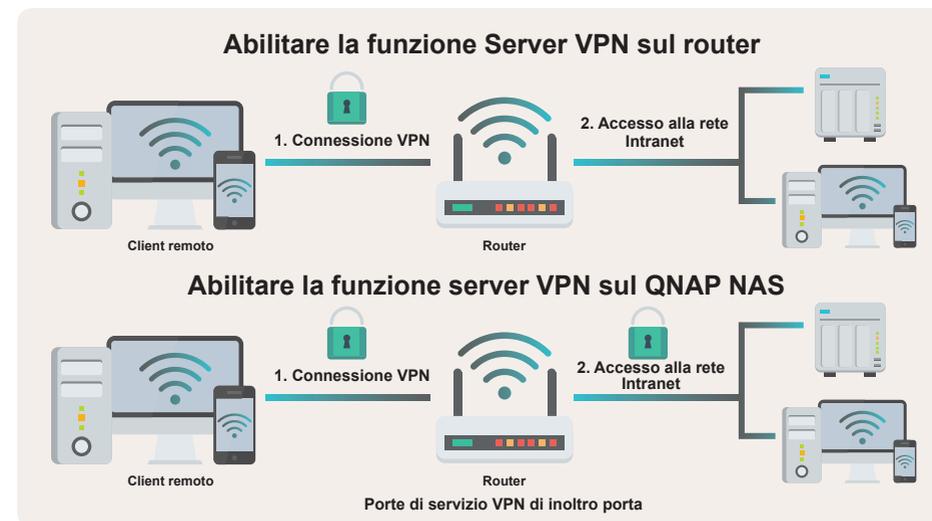
Questo metodo presenta rischi di protezione. A meno che non si sia esperti nella configurazione di rete e non si comprendano i rischi associati, **QNAP non consiglia di utilizzarlo***. Poiché il router trasmette il traffico ai dispositivi Intranet, se non è installato alcun firewall tra il router e il NAS per bloccare il traffico dannoso, gli hacker possono facilmente lanciare attacchi alla rete. Tuttavia, anche se è installato un firewall (utilizzando un firewall di base o acquistando un firewall di livello aziendale), il blocco di ogni attacco non è garantito.

* QNAP consiglia solo di aprire porte di servizio VPN a basso rischio su Internet, mentre altre porte di servizio ad alto rischio, come la gestione del sistema, i servizi SMB e SSH, non dovrebbero essere facilmente accessibili da Internet.



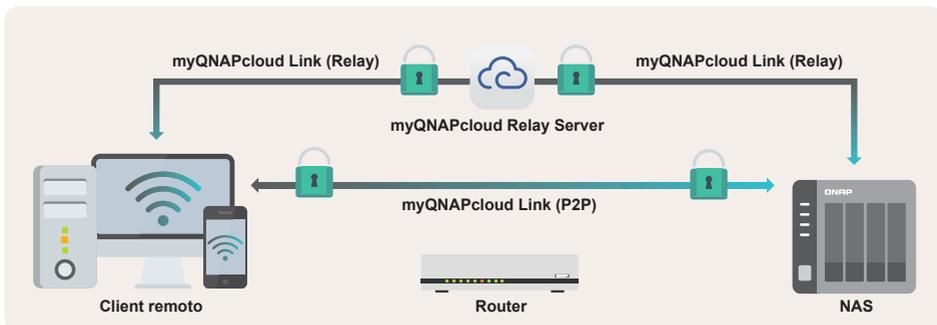
02 | Abilitare la funzione Server VPN sul router o sul NAS QNAP

Alcuni router supportano le funzioni del server VPN (come i router QNAP QHora e QMiro), mentre QNAP NAS supporta anche più server VPN. Una volta attivato e configurato correttamente, è possibile accedere a ciascun dispositivo sulla rete Intranet con una connessione crittografata VPN da Internet al server VPN, fornendo un elevato livello di protezione.



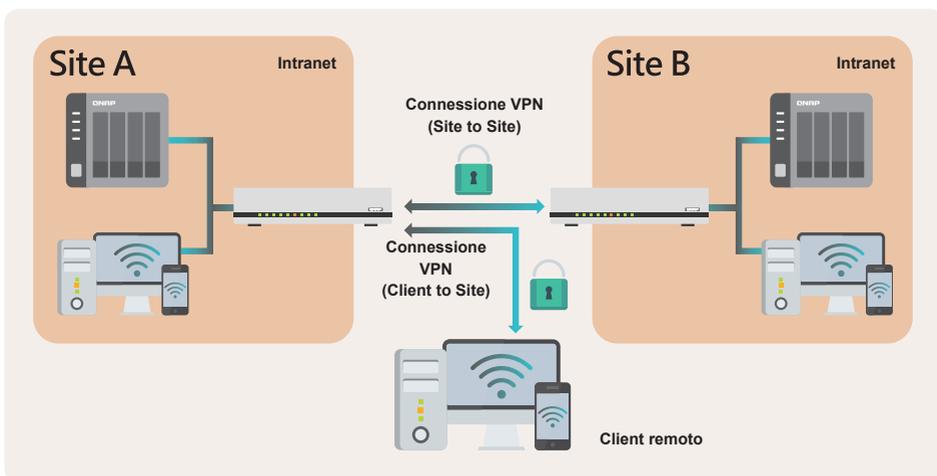
03 | Utilizzare myQNAPcloud Link Secure Connection

La configurazione del router non è necessaria se si utilizza myQNAPcloud Link per connettersi al NAS, in quanto può aprire il servizio NAS direttamente a Internet. myQNAPcloud Link stabilisce una connessione tramite un relay server o una tecnologia peer-to-peer (P2P) in base all'ambiente di rete. L'intera connessione verrà crittografata per garantire la sicurezza.



04 | Utilizzare prodotti VPN SD-WAN o Site-to-Site

A differenza della funzione del server VPN (VPN Client-to-Site) menzionata in precedenza, la VPN SD-WAN o Site-to-Site stabilisce una connessione VPN crittografata sicura tra due o più router in posizioni diverse. In poche parole, i dispositivi di una rete VPN Site-to-Site possono essere collegati tra loro come se si trovassero sulla stessa intranet, il che lo rende ideale per gli utenti con più sedi. Con la VPN Client-to-Site, è possibile accedere al proprio NAS da qualsiasi luogo.



È possibile scegliere il metodo di connessione più adatto alle proprie esigenze in base alla tabella di confronto. QNAP dispone di più soluzioni di connessione sicura per soddisfare le esigenze degli utenti.

Metodo di connessione	Vantaggi	Svantaggi	Utenti idonei
Abilitare e configurare il router DMZ/Port Forwarding di UPnP	<ul style="list-style-type: none"> Connessione più veloce 	<ul style="list-style-type: none"> Vulnerabile agli attacchi informatici Nessuna difesa contro gli attacchi alla vulnerabilità di tipo 0-Day 	<ul style="list-style-type: none"> Chiara comprensione dei rischi associati Familiarità con le impostazioni di rete Creazione più backup per i dati importanti Disporre di un piano di ripristino di emergenza
Abilitare il server VPN sul router*	<ul style="list-style-type: none"> Relativamente semplice da installare 	<ul style="list-style-type: none"> Nessuna notifica di errore di accesso, blocco automatico e funzione firewall Supporto di un numero inferiore di protocolli VPN Prestazioni limitate dall'hardware del router 	<ul style="list-style-type: none"> Nessuna familiarità con le impostazioni di rete Non importa la velocità della trasmissione
Abilitare la funzione server VPN sul QNAP NAS*	<ul style="list-style-type: none"> Supporto di più protocolli VPN Compatibilità con firewall NAS (QuFirewall) Supporto della notifica di errori di accesso e di blocco automatico 	<ul style="list-style-type: none"> Le impostazioni sono leggermente più complesse 	<ul style="list-style-type: none"> Familiarità con le impostazioni di rete Necessità di accedere frequentemente a molti file da Internet
Utilizzare myQNAPcloud Link Secure Connection	<ul style="list-style-type: none"> Facile da configurare Controllo di accesso al supporto Il NAS non deve essere esposto a Internet 	<ul style="list-style-type: none"> Connessione più lenta 	<ul style="list-style-type: none"> Nessuna familiarità con le impostazioni di rete Accesso al NAS da Internet non frequente Ambiente di rete in cui non è possibile ottenere l'indirizzo IP WAN
Utilizzare prodotti VPN SD-WAN o Site-to-Site*	<ul style="list-style-type: none"> Dopo la configurazione, la rete Intranet può essere utilizzata senza alcuna differenza Supporta anche VPN Client-to-Site 	<ul style="list-style-type: none"> Apparecchiature extra richieste 	<ul style="list-style-type: none"> Richiede l'accesso multi-point e il backup remoto Richiede applicazioni a valore aggiunto

*QNAP NAS supporta:
myQNAPcloud Link / Server VPN (L2TP/IPsec, OpenVPN, WireGuard, QBelt) /QuWAN SD-WAN

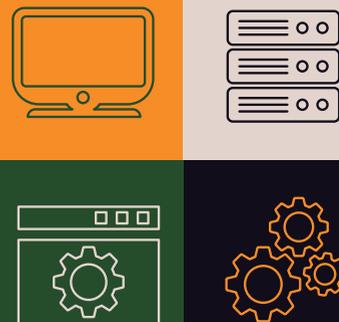
* QNAP Router supporta:
Server QuWAN SD-WAN / VPN (L2TP/IPsec, OpenVPN, WireGuard, QBelt)

Si riferisce ai router domestici generici

01

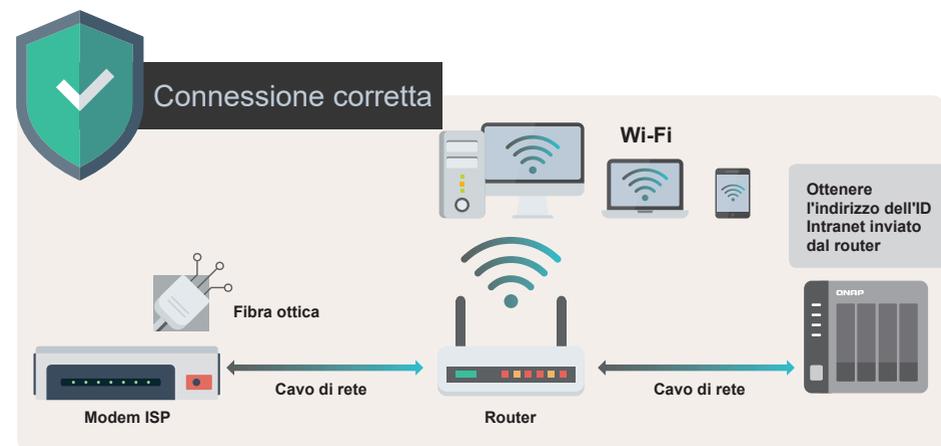
Guida delle impostazioni di sicurezza NAS

Evitare di esporre il NAS a Internet

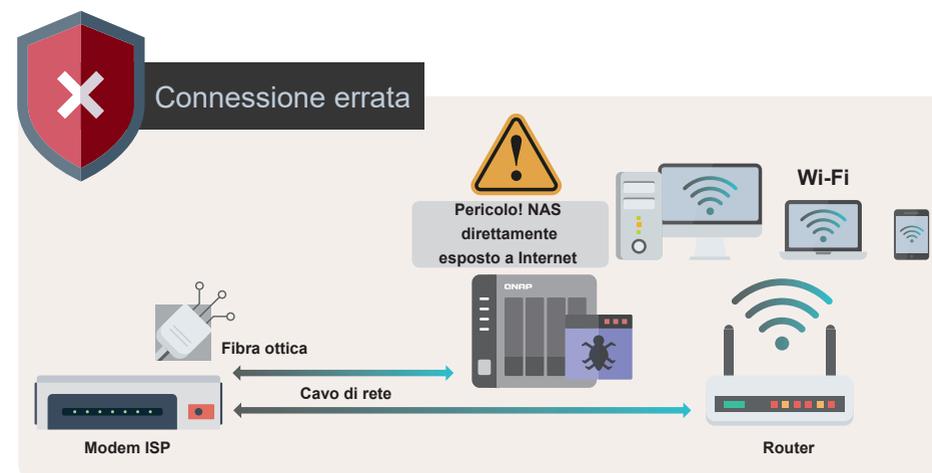


Collegare il NAS correttamente

Verificare che il NAS sia connesso al router. Con una configurazione corretta, il router può bloccare le connessioni da Internet, consentendo al NAS di nascondersi da Internet ed evitare attacchi informatici.



Se si collega il NAS al modem fornito dall'ISP, il NAS otterrà direttamente l'indirizzo IP WAN. In questo caso, chiunque (compresi gli hacker) può connettersi al NAS tramite Internet, e anche cercare di attaccare e accedere.

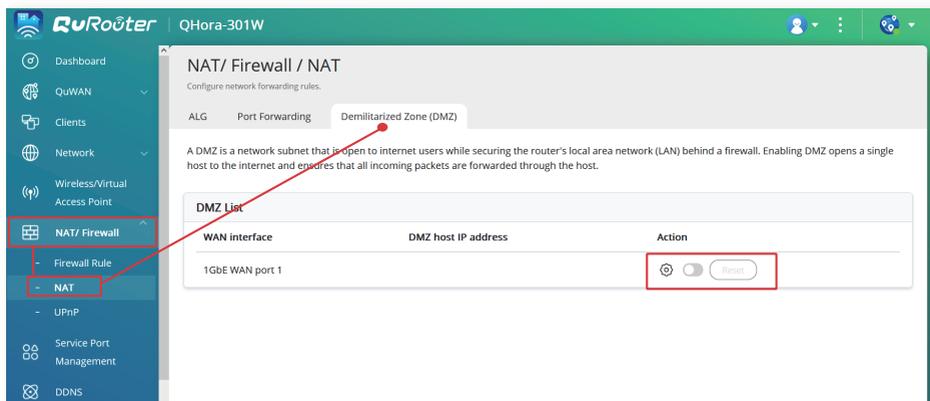
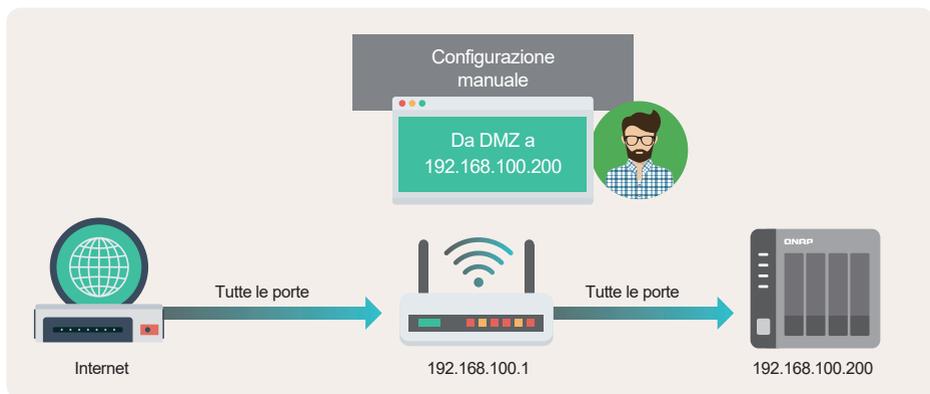


Controllare le impostazioni del router

Per impostazione predefinita, in teoria nessuno può connettersi direttamente da Internet al dispositivo dietro il router. Tuttavia, se si attivano "DMZ (zona demilitarizzata)", "Inoltro porta" o "UPnP (Universal Plug and Play)", il router inoltra i pacchetti al dispositivo selezionato in base alle regole impostate, esponendo il dispositivo a Internet. Se non è necessario, controllare e verificare che le seguenti funzioni siano **disabilitate**.

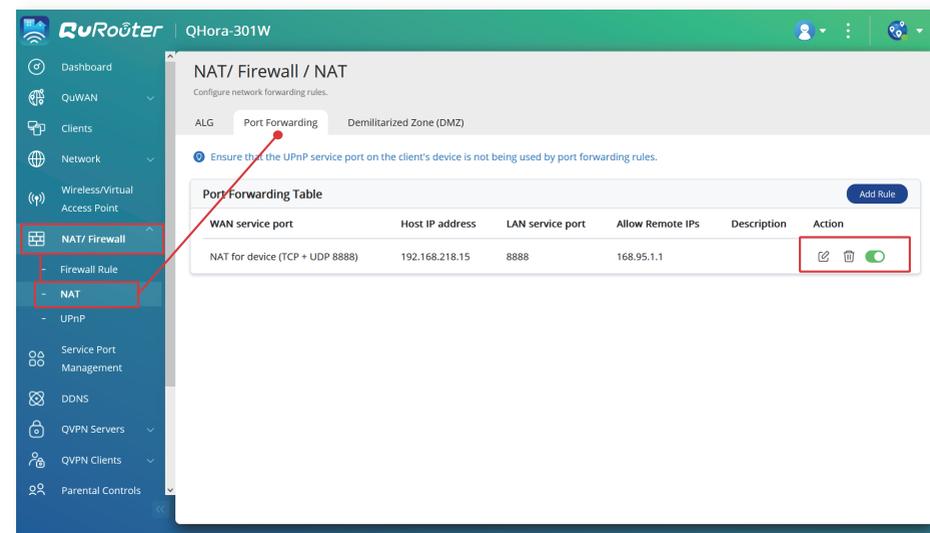
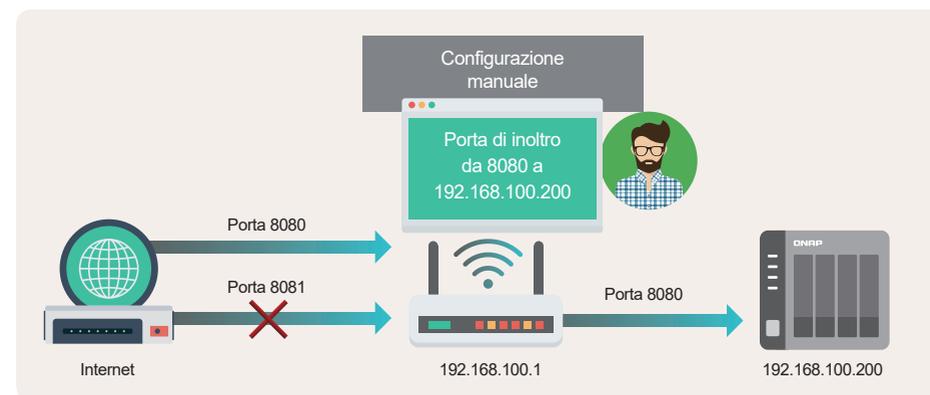
01 | Controllare DMZ (zona smilitarizzata)

Dopo aver attivato questa funzione, tutte le porte di servizio del dispositivo selezionato saranno direttamente aperte a Internet, ovvero completamente esposte a Internet. Per ridurre i rischi di protezione, disattivare questa funzione.



02 | Controllo inoltro di porta

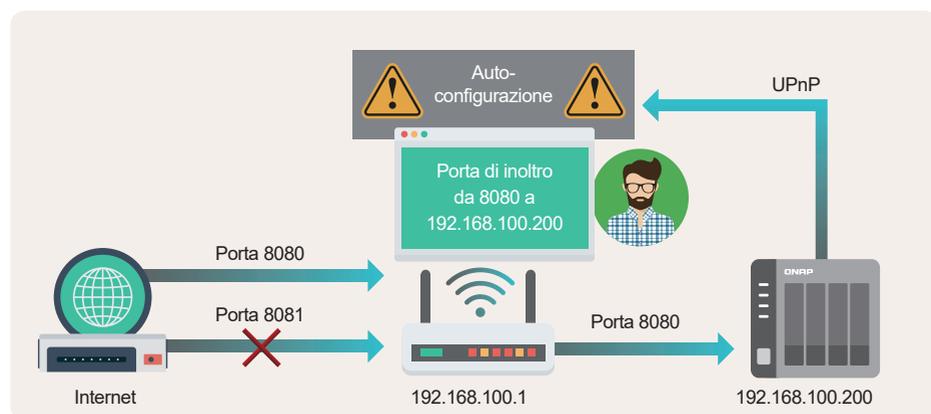
Questa funzione consente di aprire una porta di servizio specifica su un dispositivo a Internet, consentendo a chiunque di accedere ai servizi correlati tramite Internet. Tuttavia, gli hacker possono anche lanciare attacchi contro servizi aperti da Internet. Pertanto, si consiglia di disattivare prima tutte le regole di inoltro porta, quindi di configurare le impostazioni di sicurezza NAS e di eseguire il backup dei dati importanti prima di utilizzare questa funzione per aprire alcuni servizi essenziali su Internet.



Controllare le impostazioni NAS

03 | Controllare UPnP (Universal Plug and Play)

Questa funzione è equivalente all'inoltro automatico delle porte. Dopo aver attivato questa funzione, il dispositivo può configurare automaticamente l'inoltro porta utilizzando il relativo protocollo. Questa funzione presenta gravi rischi per la protezione, poiché potrebbe esporre i servizi a Internet senza che l'utente ne sia a conoscenza o essere sfruttata da hacker per aprire backdoor, pertanto è necessario disattivare questa funzione per migliorare la protezione.



ID	Service Name	External Port	Protocol	Internal IP Address	Internal Port
No data					

01 | Configurazione automatica del router (Inoltro porta UPnP)

Poiché alcuni router non supportano la disattivazione della funzione UPnP, verificare contemporaneamente l'impostazione "Configurazione automatica router" sul NAS per verificare che questa funzione sia disattivata.

* Questa funzione è disabilitata per impostazione predefinita da QTS 4.5.0 / QuTS Hero h4.5.3 in poi.

Per abilitare la funzione "Configurazione automatica router":

1. Accedere all'interfaccia di gestione Web di QTS /QuTS hero utilizzando un account amministratore.
2. Aprire il menu nell'angolo in alto a sinistra dell'interfaccia di gestione, fare clic su "myQNAPcloud"
3. **QTS 5.0.0 / QuTS Hero h5.0.0 o versioni precedenti:** Fare clic su "Configurazione automatica router" nel menu di sinistra

QTS 5.0.1 / QuTS Hero h5.0.1 o versione successiva: Fare clic sull'icona del menu nell'angolo in alto a destra, e selezionare "Configurazione automatica router"

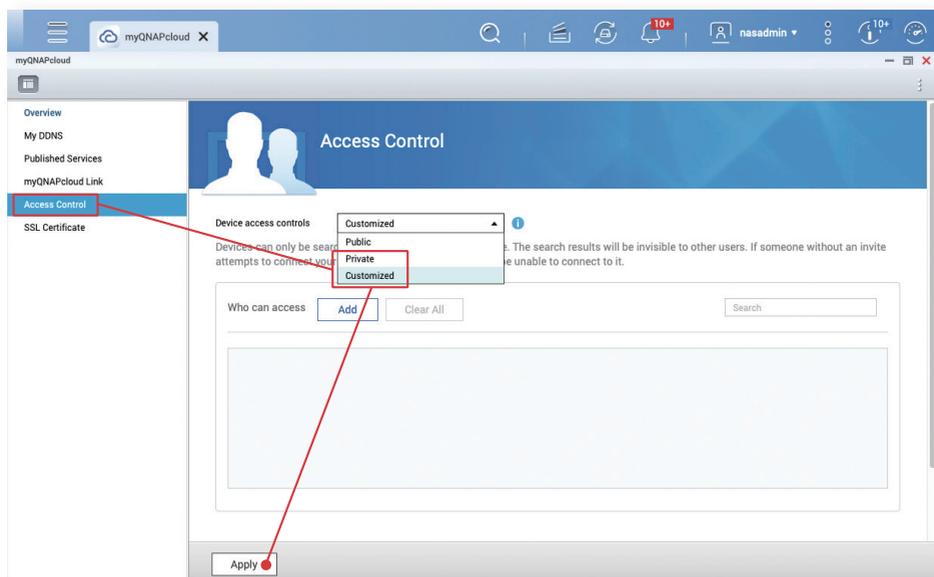
4. Nella pagina delle impostazioni "Configurazione automatica router", deselezionare "Attiva inoltro porta UPnP" e fare clic su "Applica".

02 | Controllo accesso myQNAPcloud Link

MyQNAPcloud link è un servizio cloud di connessione sicura fornito da QNAP. Gli utenti possono connettersi al proprio QNAP NAS tramite il nome del dispositivo myQNAPcloud scelto. MyQNAPcloud Link fornisce le impostazioni di controllo dell'accesso. Quando il controllo dell'accesso è impostato su "pubblico", chiunque conosca il nome del dispositivo può utilizzare myQNAPcloud Link per connettersi al NAS. Pertanto, **si consiglia di impostare il controllo di accesso su "Privato" o "Personalizzato"**. In entrambe le modalità, gli utenti devono accedere al proprio QNAP ID nell'elenco di accesso consentito prima di poter utilizzare myQNAPcloud link per connettersi in modo sicuro ai servizi cloud.

* L'impostazione predefinita in QTS 4.5.0 / Qu TS Hero h4.5.3 (o versioni successive) è "Personalizzato"

1. Accedere all'interfaccia di gestione Web di QTS /QuTS hero utilizzando un account amministratore
2. Fare clic sul menu nell'angolo in alto a sinistra dell'interfaccia di gestione, fare clic su "myQNAPcloud"
3. Fare clic su "Controllo accesso" nel menu a sinistra
4. Nella pagina delle impostazioni "Controllo accesso", impostare "Controlli accesso dispositivo" su "Privato" o "Personalizzato", quindi fare clic su "Applica".



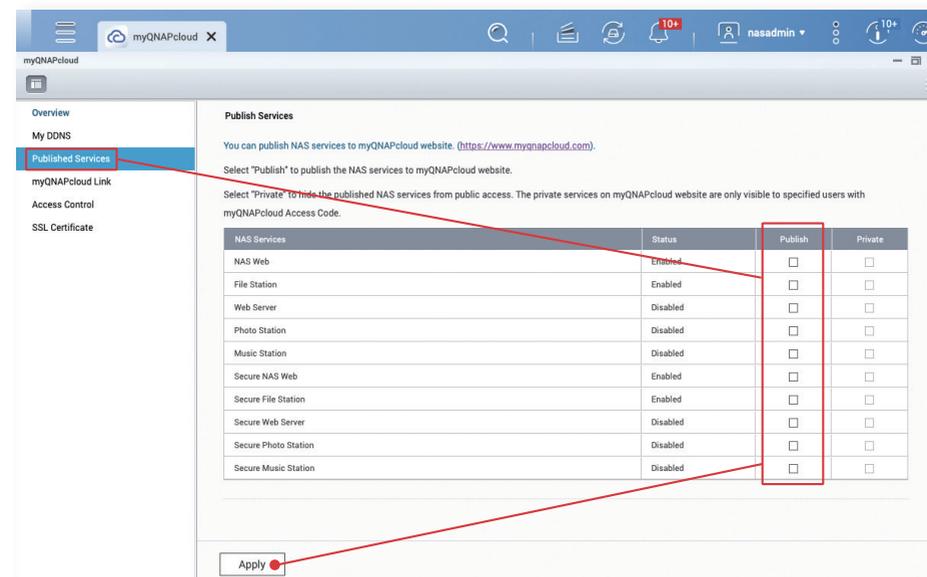
03 | Servizi pubblicati

I servizi pubblicati possono semplificare l'utilizzo delle funzioni correlate sul sito Web myQNAPcloud, ma aumentano anche i rischi per la sicurezza. Se non è necessario utilizzare questa funzione, si consiglia di disattivarla per migliorare la protezione.

* Questa funzione è disabilitata per impostazione predefinita da QTS 4.5.0 / QuTS Hero h4.5.3 in poi

Funzione "Servizi pubblicati":

1. Accedere all'interfaccia di gestione Web di QTS /QuTS hero utilizzando un account amministratore
2. Fare clic sul menu nell'angolo in alto a sinistra dell'interfaccia di gestione, fare clic su "myQNAPcloud"
3. Fare clic su "Servizi pubblicati" nel menu a sinistra
4. Nel campo "Pubblica", deseleziona tutto e fai clic su "Applica".



Checklist delle impostazioni di rete

Relativo all'hardware

- Il NAS è collegato dietro un router
- Il NAS ottiene l'indirizzo IP Intranet

Router

- Disabilitare la funzione "DMZ" del router
- Disabilitare la regola "Inoltro porta" del router
- Disabilitare la funzione "UPnP" del router

NAS

- Disabilitare la funzione "Inoltro porta UPnP configurazione router automatica" del NAS
- Impostare l'opzione "Controllo accesso myQNAPcloud Link" del NAS su "Privato" o "Personalizzato"
- Disabilitare la funzione "Servizi pubblicati"

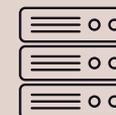
Dopo aver controllato e applicato le impostazioni di cui sopra, il QNAP NAS non sarà esposto a Internet e i rischi di essere attaccato da hacker sono notevolmente ridotti. Leggere e controllare le altre impostazioni per rafforzare il QNAP NAS.

Per accedere al NAS tramite Internet, è possibile considerare queste tre alternative sicure:

		
myQNAPcloud Link	QVPN Service	QuWAN SD-WAN
		
Ulteriori informazioni	Ulteriori informazioni	Ulteriori informazioni

02

Guida delle impostazioni di sicurezza NAS



NAS Impostazioni di sicurezza



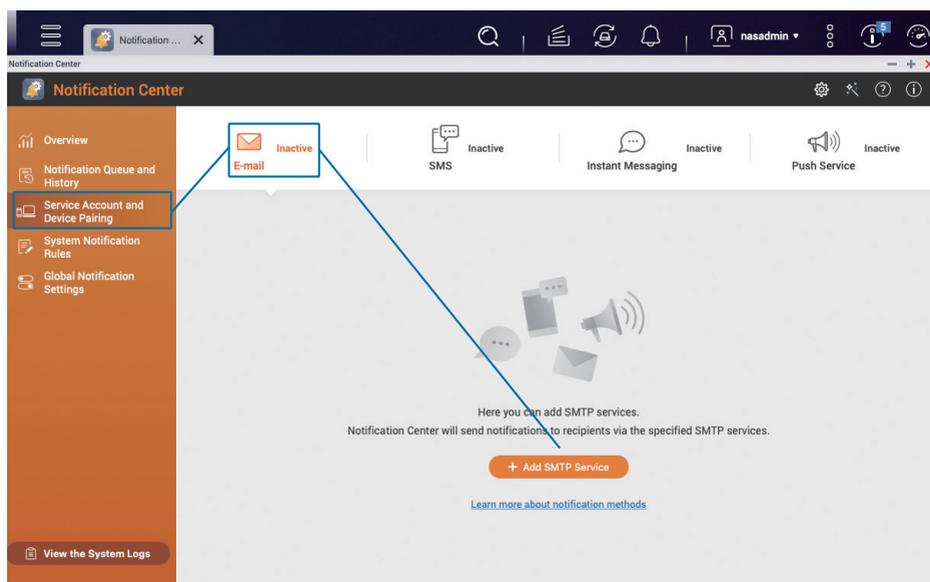
Configurare notifiche di avviso

Il Centro notifiche integrato può inviare notifiche in base alle impostazioni dell'utente, consentendo agli utenti di tenere traccia dello stato del NAS e reagire alle anomalie non appena vengono rilevate.

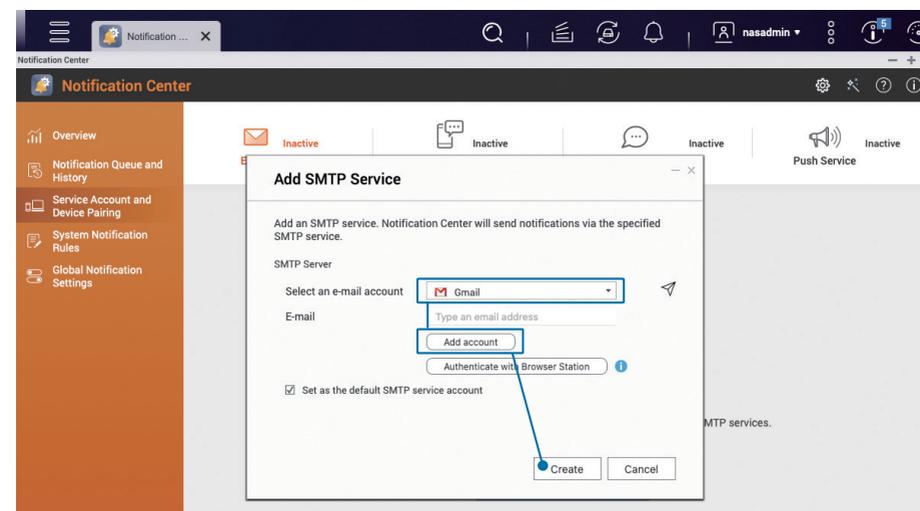
Il seguente tutorial descrive come creare due regole di base per "e-mail" per inviare "Notifiche di avviso" e "Aggiornamento firmware" e per aggiungere altre regole, se necessario.

01 | Aggiungere il metodo di notifica "E-mail"

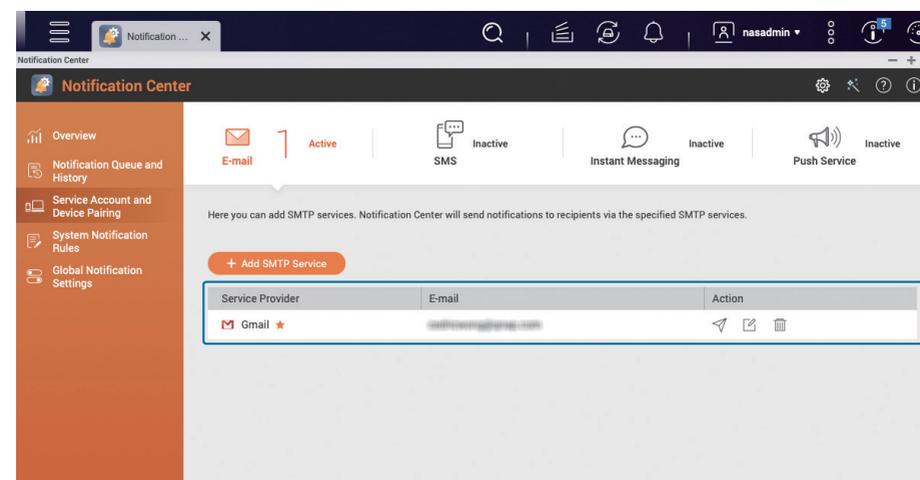
Aprire "Centro notifiche", fare clic su "Associazione account di servizio e dispositivi" nel menu a sinistra, selezionare "E-mail", quindi fare clic su "Aggiungi servizio SMTP"



Selezionare un account e-mail (il seguente utilizza Gmail come esempio), fare clic su "Aggiungi account", seguire le istruzioni per completare il processo di verifica di Gmail e fare clic su "Crea" al termine della verifica.

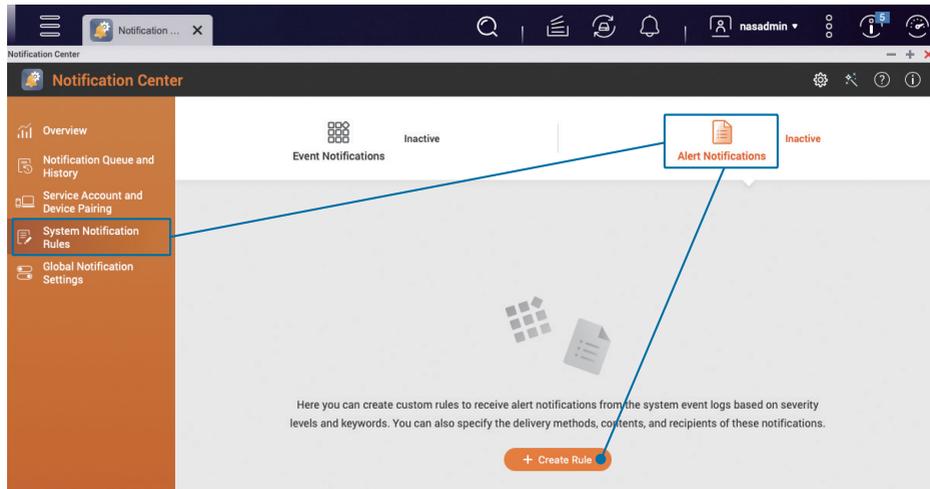


Una volta creato ↕ , verrà visualizzato l'account e-mail aggiunto nell'elenco.

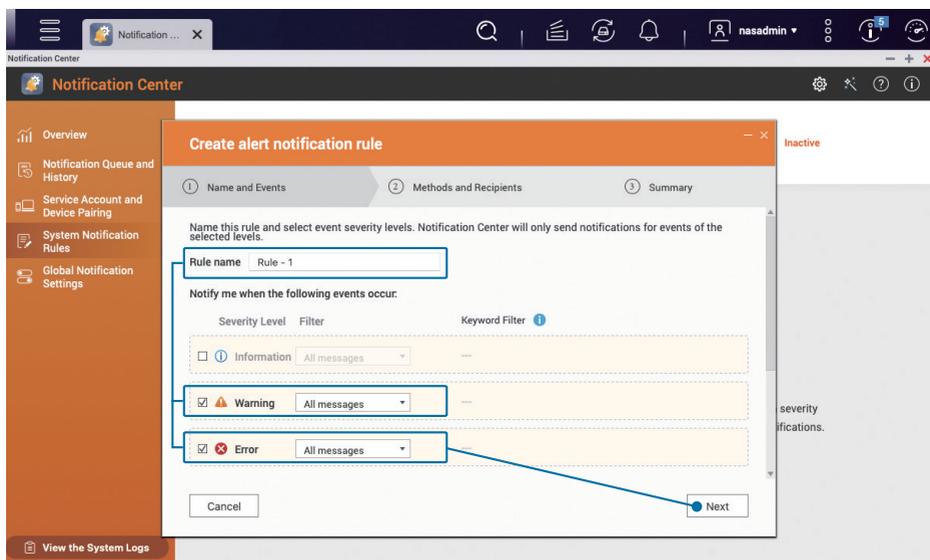


02 | Configurare "Notifiche avvisi"

Nel menu a sinistra di "Centro notifiche", fare clic su "Regole di notifica del sistema", selezionare "Notifiche avvisi" e fare clic su "Crea regola".

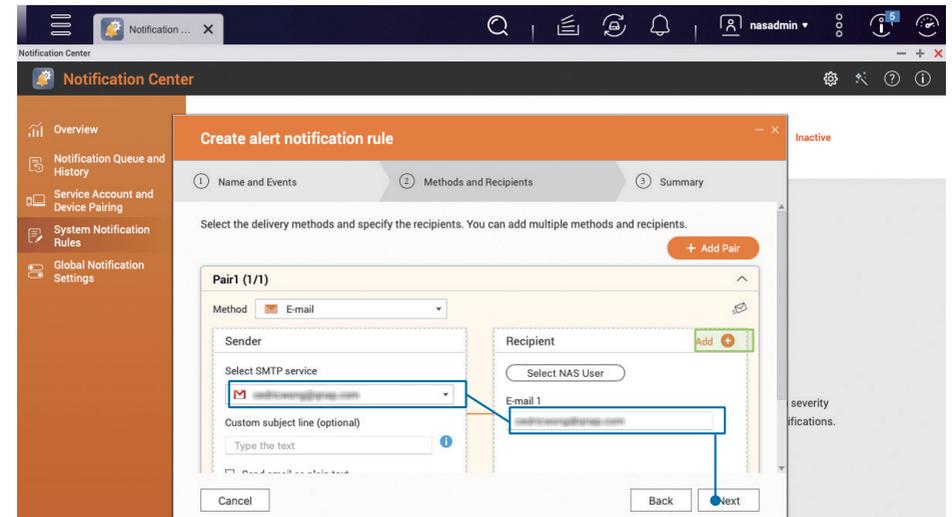


Modificare il "Nome regola" in base alle specifiche esigenze, controllare i due livelli di gravità "Avvertenza" e "Errore", quindi fare clic su "Avanti".

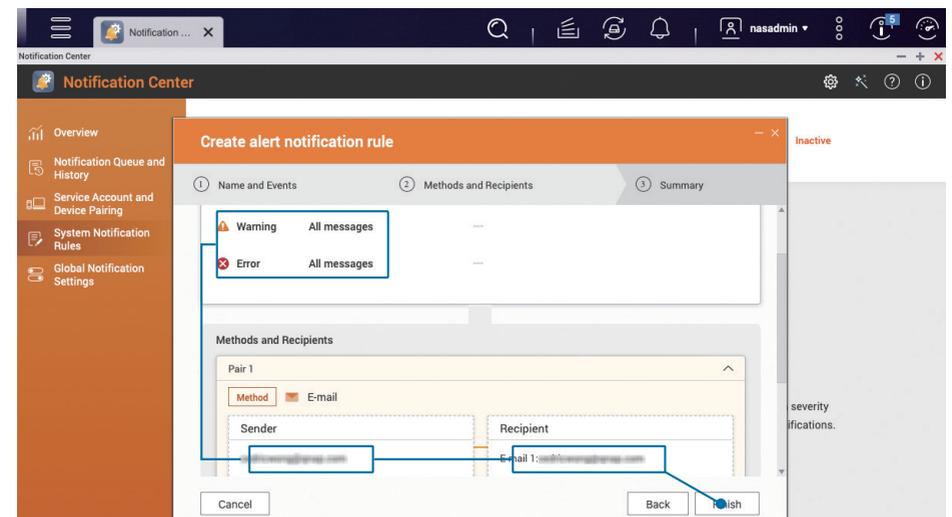


Impostare il metodo di consegna e il destinatario, selezionare l'account e-mail appena aggiunto come "Mittente" nell'associazione, quindi immettere l'Indirizzo e-mail del "Destinatario" e fare clic su "Avanti".

Se necessario, è possibile immettere più destinatari facendo clic su "Aggiungi +" accanto a "Destinatario". È possibile anche "Aggiungi coppia" per inviare notifiche in più modi contemporaneamente.

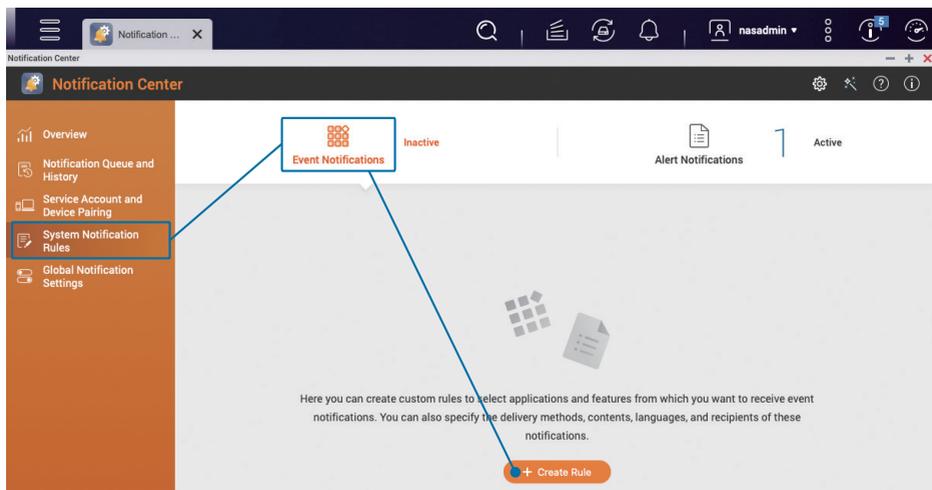


Dopo aver confermato che le impostazioni sono corrette, fare clic su "Fine" per completare le impostazioni "Notifiche di avviso".

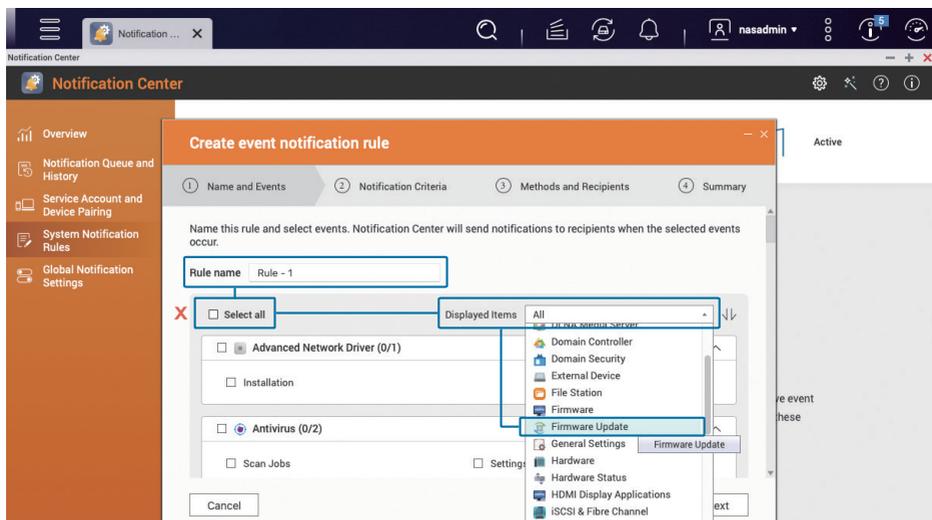


03 | Configurare notifiche "Aggiornamento firmware"

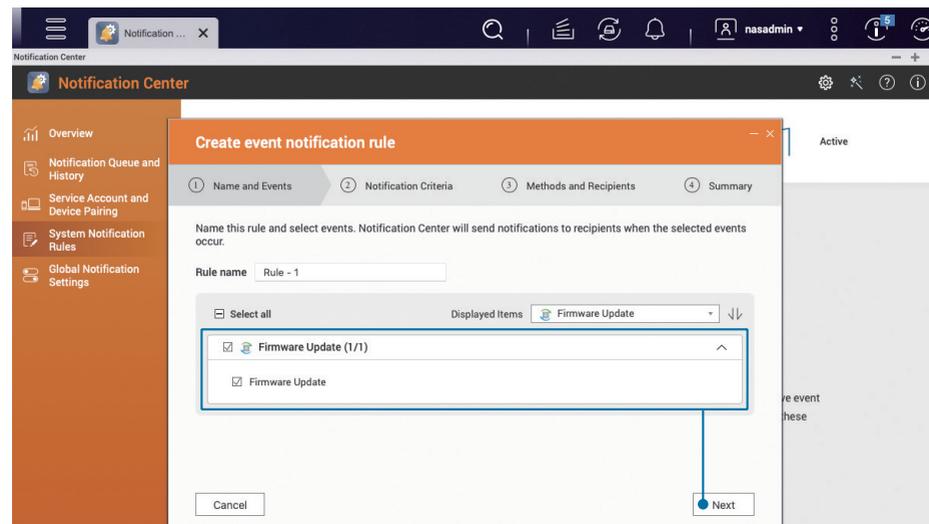
Fare clic su "Regole di notifica sistema" nel menu a sinistra di "Centro notifiche", selezionare "Notifiche eventi", quindi fare clic su "Crea regola".



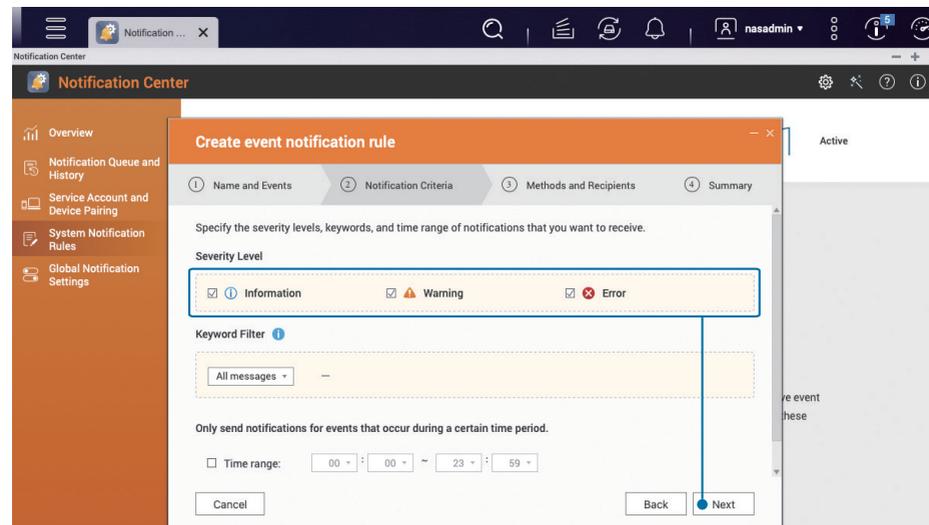
Modificare il "Nome regola" in base alle proprie esigenze, deselezionare "Seleziona tutto", quindi selezionare "Aggiornamento firmware" nelle "Voci visualizzate" a sinistra, quindi selezionare l'opzione "Aggiornamento firmware" riportata di seguito.



Selezionare l'opzione "Aggiornamento firmware" e fare clic su "Avanti".



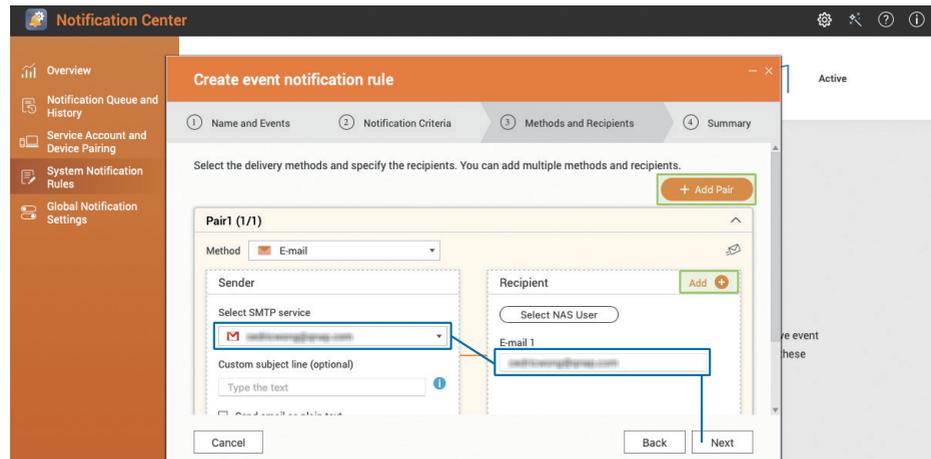
Controllare tutti i livelli di gravità, inclusi "Informazioni", "Avvertenza" e "Errore", quindi fare clic su "Avanti".



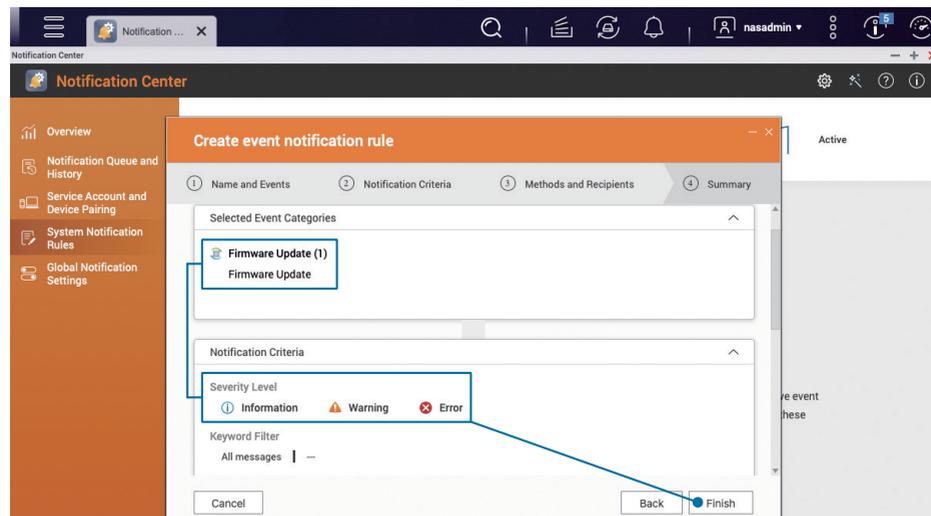
Abilitare l'aggiornamento automatico firmware (QTS / QuTS Hero)

Impostare il metodo di consegna e il destinatario. Poiché è attualmente impostata solo la notifica "E-mail", selezionare l'account e-mail appena aggiunto come "Mittente" nell'associazione, quindi immettere l'indirizzo e-mail del "Destinatario", quindi fare clic su "Avanti".

Se necessario, è possibile immettere più destinatari facendo clic su "Aggiungi +" accanto a "Destinatario". È possibile anche "Aggiungi coppia" per inviare notifiche in più modi contemporaneamente.

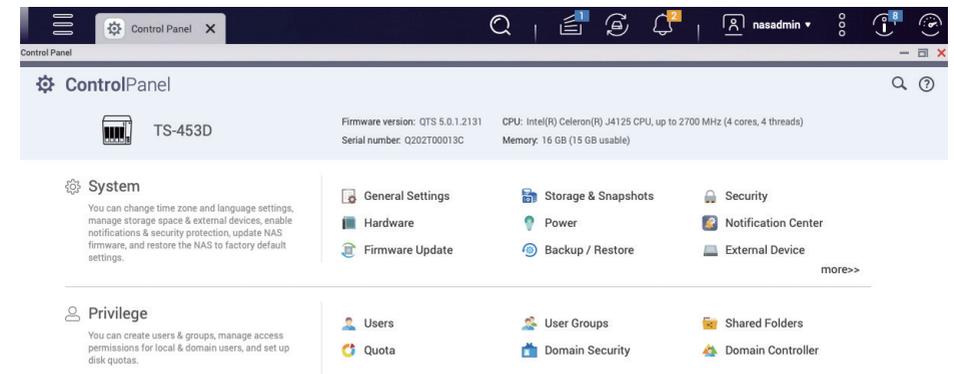


Dopo aver confermato che le impostazioni sono corrette, fare clic su "Fine" per completare l'impostazione di "Aggiornamento firmware".



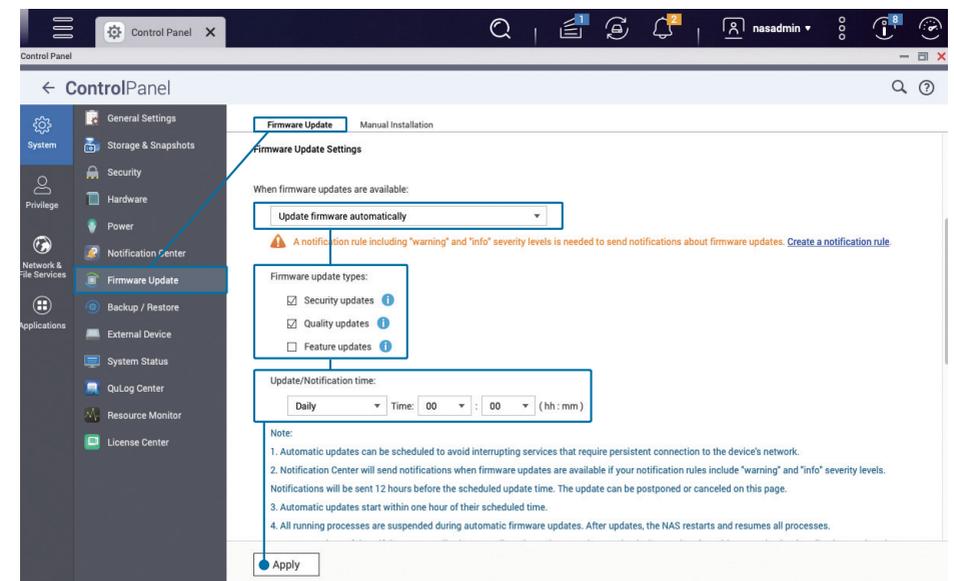
La funzione di aggiornamento automatico semplifica l'installazione di aggiornamenti per nuove funzionalità, correzioni di bug e vulnerabilità.

Aprire "Pannello di controllo" e fare clic su "Aggiornamento firmware".



In "Impostazioni aggiornamento firmware", selezionare "Aggiorna firmware automaticamente" e selezionare "Aggiornamenti di protezione" e "Aggiornamenti di qualità"; per "Ora aggiornamento/notifica", si consiglia di impostare un'ora non di punta, ad esempio "00: 00", quindi fare clic su Applica.

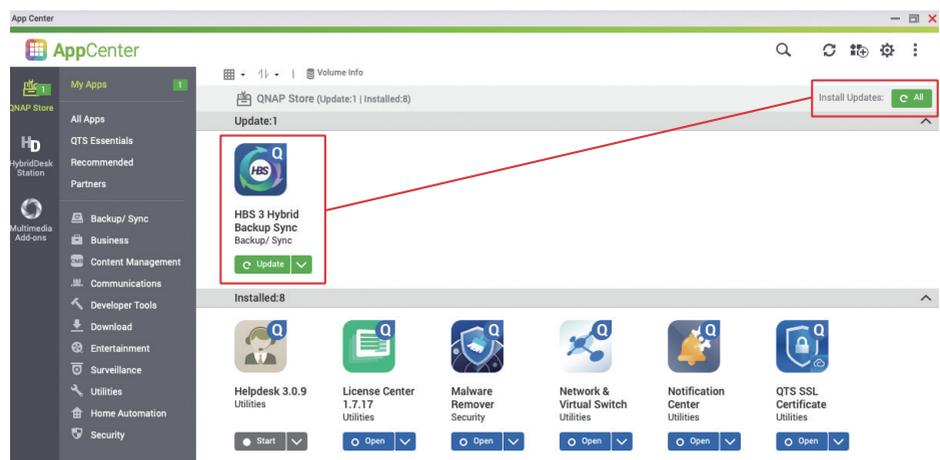
*** Per QTS 5.0.0 / QuTS Hero h5.0.0 (o versione precedente), selezionare "Versione consigliata" nella pagina "Aggiornamento automatico"**



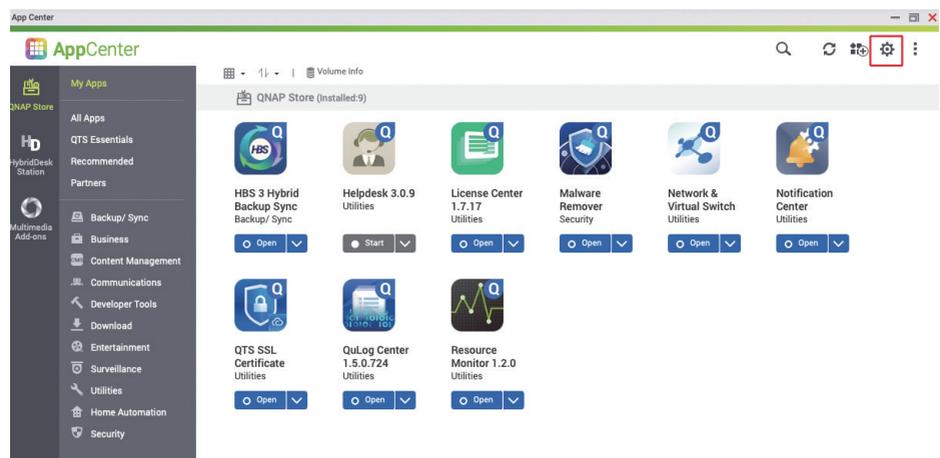
Impostazioni aggiornamento app

App Center fornisce più applicazioni per aggiungere altre funzioni al QNAP NAS, ma le applicazioni devono anche essere aggiornate per migliorare le funzioni delle applicazioni, risolvere problemi e vulnerabilità e migliorare l'esperienza utente.

Aprire "App Center" per verificare se non presenti app da aggiornare. In tal caso, fare clic sul pulsante "Tutti  All" in alto a destra per aggiornare tutte le app.

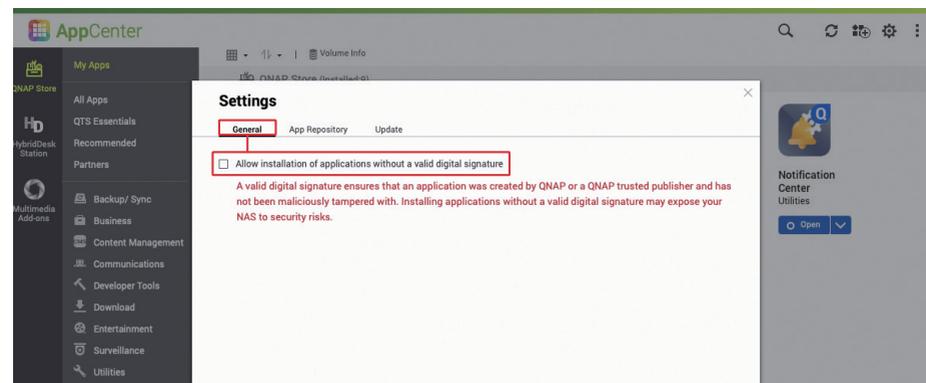


Al termine dell'aggiornamento, fare clic sull'icona "Impostazioni" , nell'angolo in alto a destra, per accedere alla pagina delle impostazioni di App Center.



Gli sviluppatori di fiducia QNAP o QNAP aggiungeranno una firma digitale all'applicazione per garantire l'originalità. Si consiglia di deselezionare "Consenti l'installazione di applicazioni senza firma digitale valida" per migliorare la protezione.

*** Opzione deselezionata per impostazione predefinita che rende impossibile installare le app senza firma digitale valida**

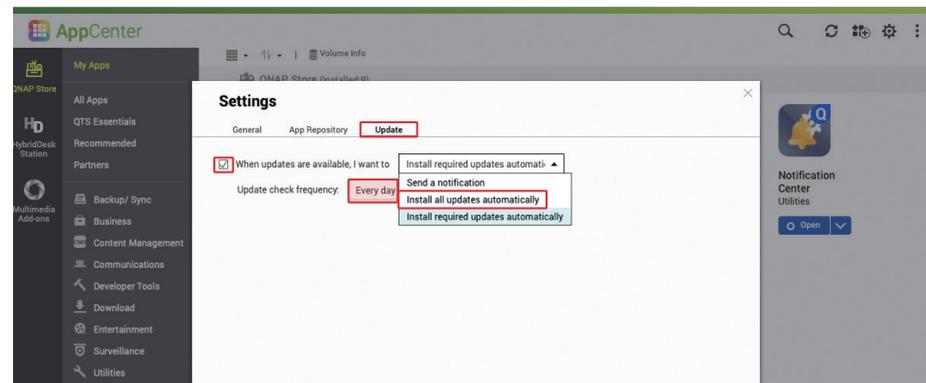


Fare clic sulla scheda Aggiorna; se non è necessario eseguire alcuna operazione, si consiglia di selezionare "Installa tutti gli aggiornamenti automaticamente", impostare la frequenza su "Ogni giorno" e fare clic su Applica per completare l'impostazione.

⇒ Gli "Aggiornamenti obbligatori" vengono utilizzati principalmente per soddisfare le dipendenze di app e firmware e includono anche "Aggiornamenti delle principali vulnerabilità".

⇒ L'opzione "Tutti gli aggiornamenti" include tutti i miglioramenti delle funzionalità, le correzioni dei bug e tutte le patch di vulnerabilità. L'aggiornamento sarà più frequente.

*** L'impostazione predefinita è "Installa tutti gli aggiornamenti automaticamente"**

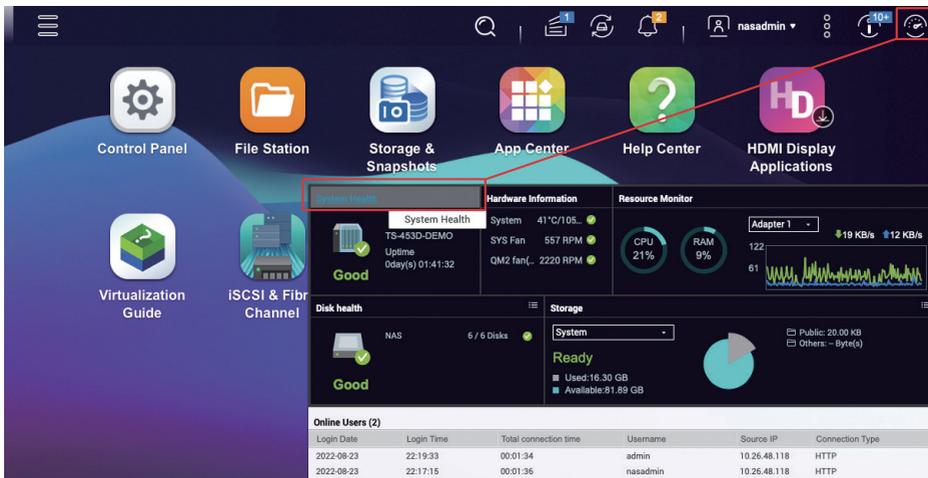


Disabilitare o rimuovere le funzioni non necessarie

QNAP NAS fornisce una varietà di funzioni e applicazioni; ma più sono le funzioni abilitate più saranno i potenziali vettori di attacco. È necessario controllare e disattivare (o rimuovere) regolarmente le funzioni non necessarie per migliorare la sicurezza e rendere il sistema più efficiente.

* Per migliorare la sicurezza del prodotto, a partire da **QTS 5.0.0 / QuTS Hero h5.0.0**, le funzioni non essenziali sono disabilitate per impostazione predefinita sull'inizializzazione del sistema e **App Center** non installerà alcuna app non essenziale per impostazione predefinita. Se il sistema è stato inizializzato prima di eseguire l'aggiornamento a **QTS 5.0.0 / QuTS Hero h5.0.0**, verificare quali applicazioni sono state installate.

Fare clic sul pulsante "🏠", nell'angolo in alto a destra, per aprire la "Dashboard" del sistema, fare clic su "Integrità sistema" per aprire la finestra "Stato sistema".



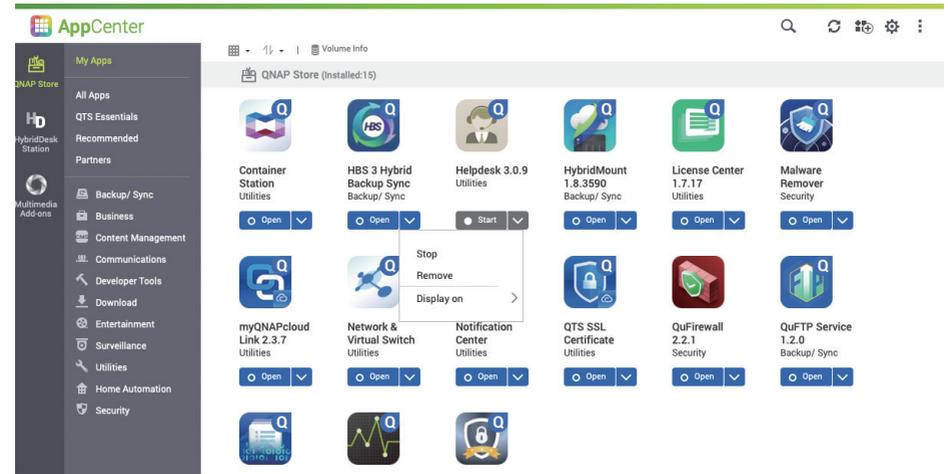
Fare clic su "Servizio di sistema" per visualizzare le funzioni di sistema abilitate. È possibile accedere al Pannello di controllo per disattivare le funzioni di sistema non necessarie.

System Status

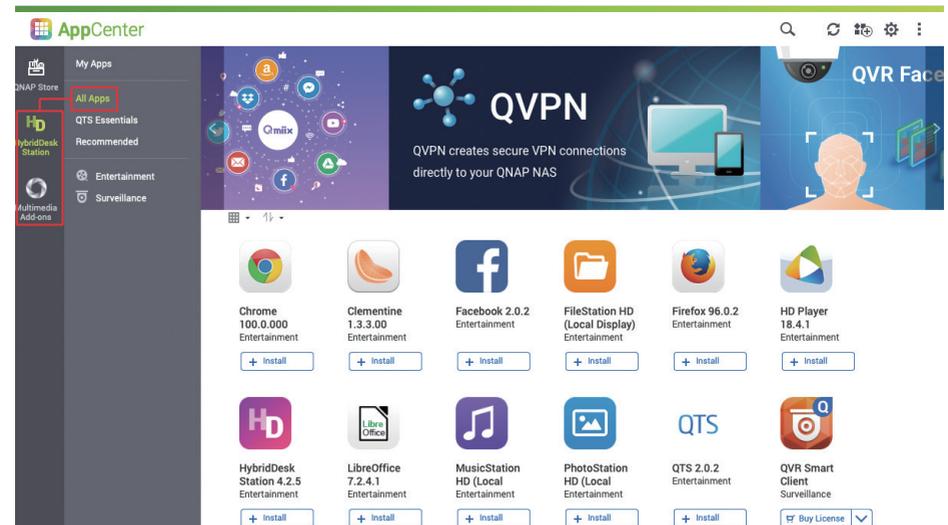
System Information Network Status **System Service** Hardware Information

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

Oltre alle funzioni integrate nel sistema, è anche necessario verificare quelle installate in App Center.



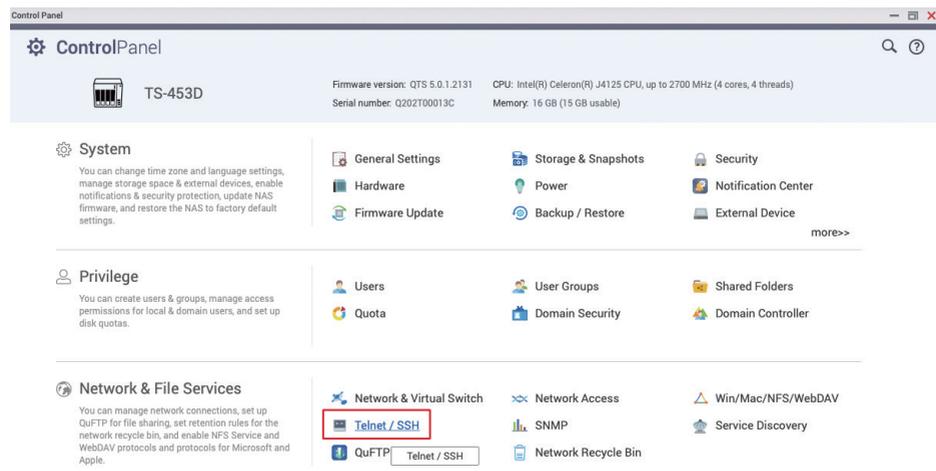
Sul lato sinistro, fare clic su "HybridDesk Station" e "Componenti aggiuntivi multimediali" per visualizzare lo stato delle applicazioni corrispondenti,



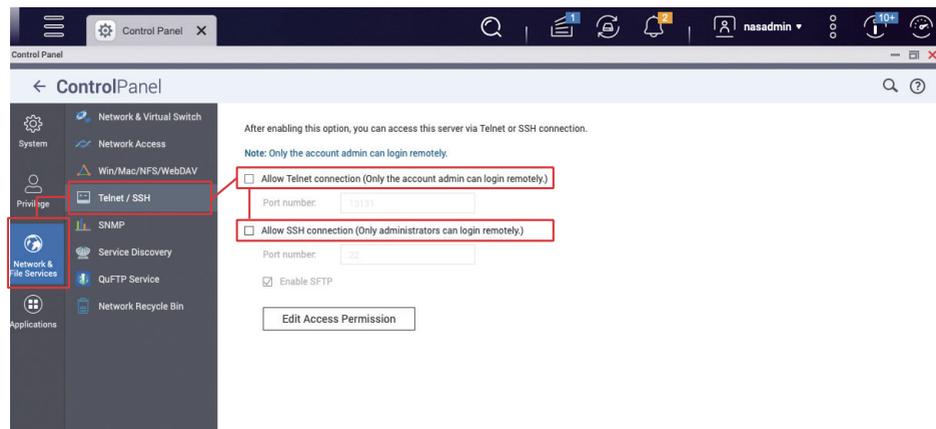
Disabilitare Telnet / SSH

Tranne se utilizzati, si consiglia di disabilitare **Telnet** e **SSH**. Queste due funzioni vengono generalmente utilizzate dal servizio clienti QNAP o dal personale IT professionale per la manutenzione del sistema. Gli utenti generici non dovrebbero necessitarne, pertanto si consiglia di disattivarle.

Aprire "Pannello di controllo" e fare clic su "Telnet / SSH"



De selezionare "Consenti connessione Telnet" e "Consenti connessione SSH", quindi fare clic su "Applica".

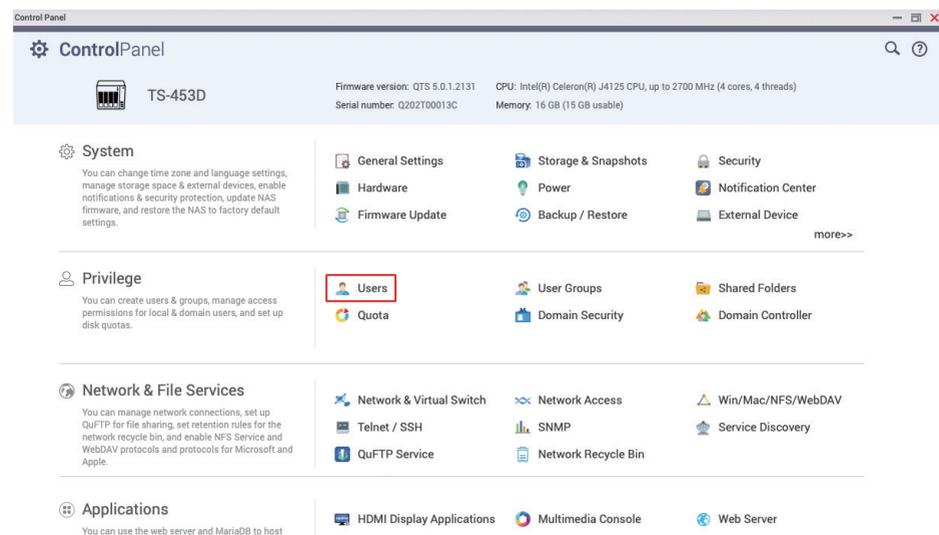


Rafforzare la sicurezza dell'account di sistema

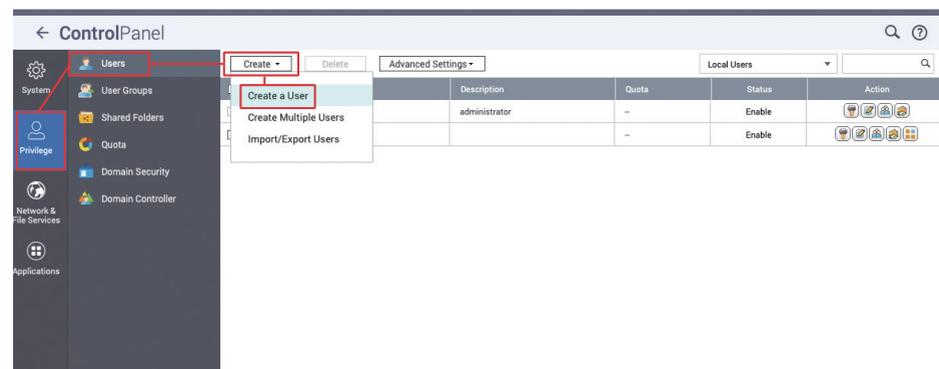
Disabilitare l'account amministratore predefinito "admin"

Gli hacker che utilizzano il cracking forzato per le password sono generalmente destinati all'account amministratore predefinito "admin". Se il sistema è stato inizializzato utilizzando QTS 4.5.4 / QuTS Hero h4.5.4 (o versione precedente), l'account amministratore predefinito "admin" sarà attivo. Per creare un nuovo account amministratore e disabilitare l'account "admin", procedere come segue.

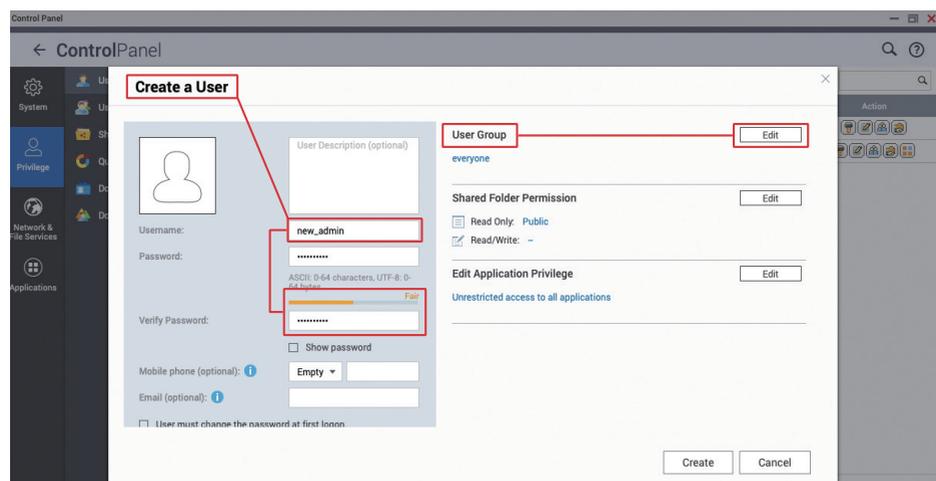
Aprire "Pannello di controllo" e fare clic su "Utenti"



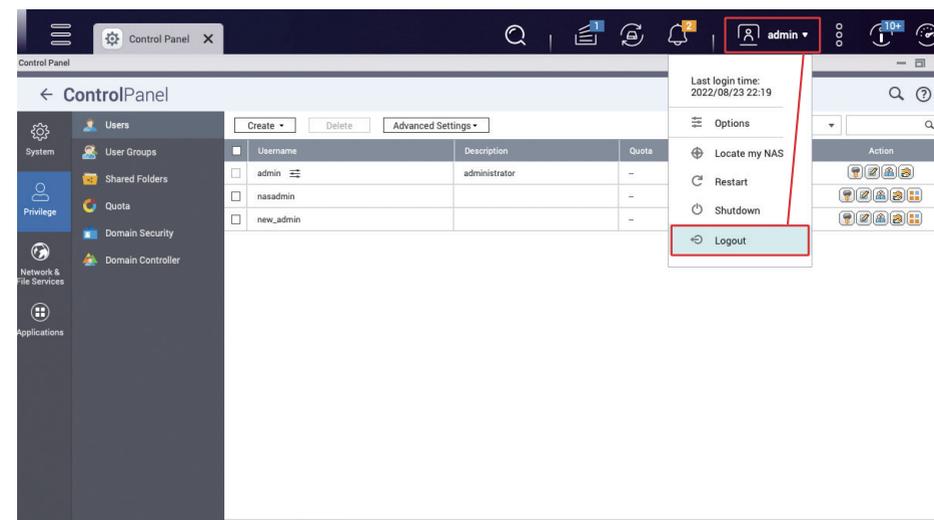
Fare clic su "Crea" > "Crea utente".



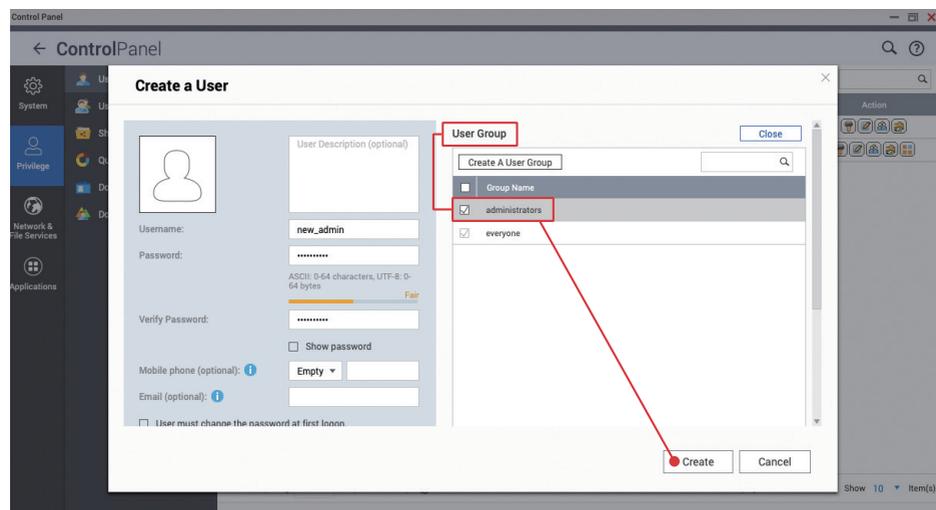
Immettere il nome utente per l'account amministratore, ad esempio "new_admin" e impostare una password complessa.



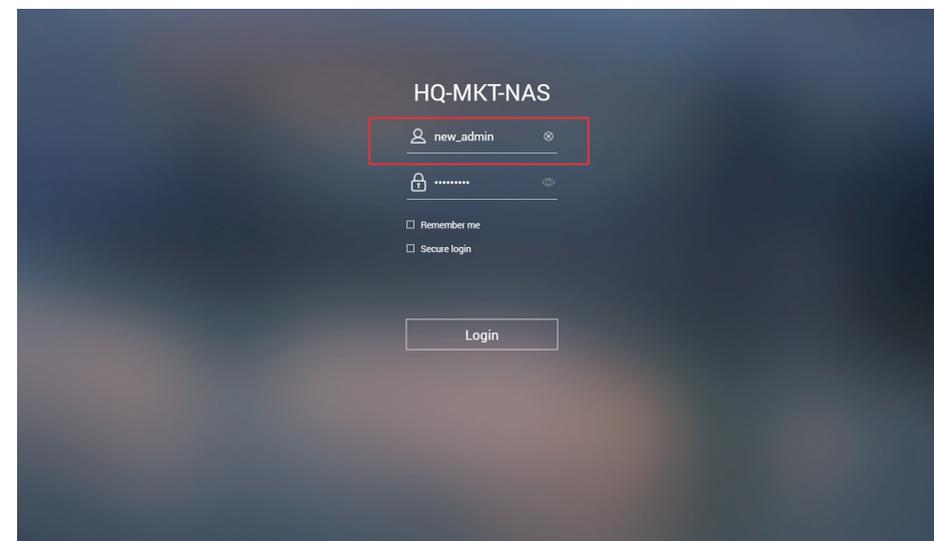
Fare clic su "admin" nella parte superiore, aprire il menu e fare clic su "Logout" per disconnettersi dall'interfaccia di gestione Web QTS.



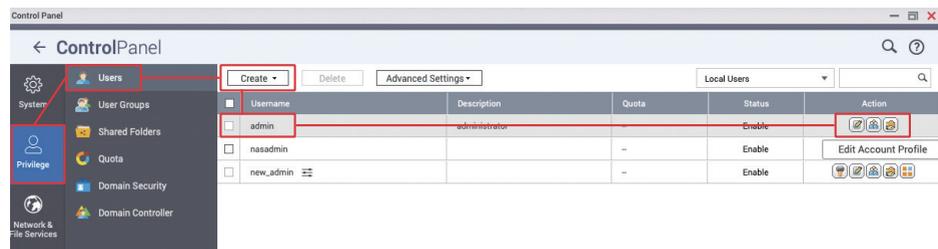
Nella sezione "Gruppo utenti", fare clic su "Modifica", selezionare il gruppo "amministratori" e fare clic su "Crea" per aggiungere un nuovo utente.



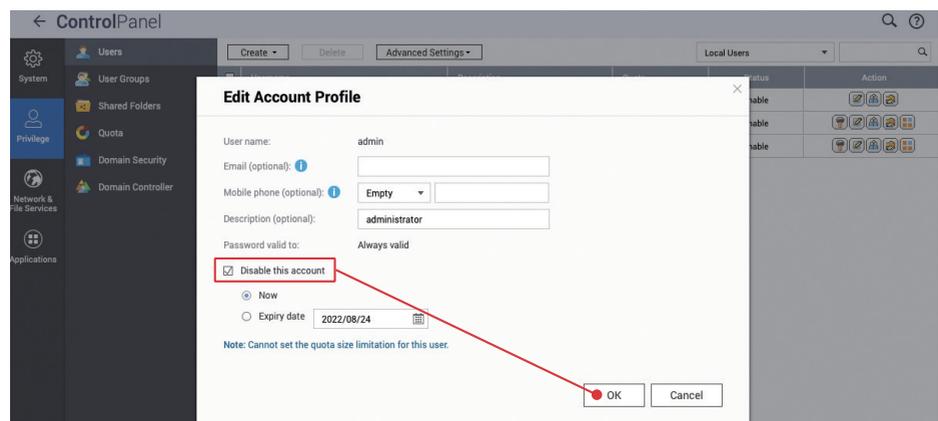
Utilizzare l'"Account amministratore" appena creato per accedere all'interfaccia di gestione Web QTS.



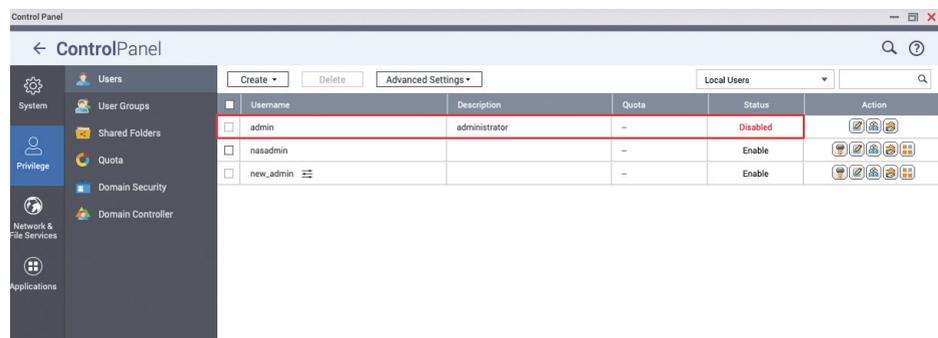
Aprire nuovamente il "Pannello di controllo", fare clic su "Utenti", nella riga "admin", fare clic su "Modifica profilo account"



Selezionare "Disattiva account" e fai clic su "OK" per terminare



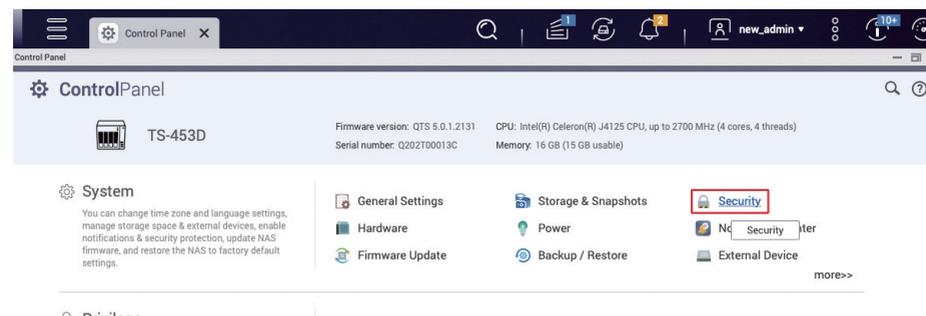
Al termine, è possibile vedere che lo stato "admin" è "Disabilitato"



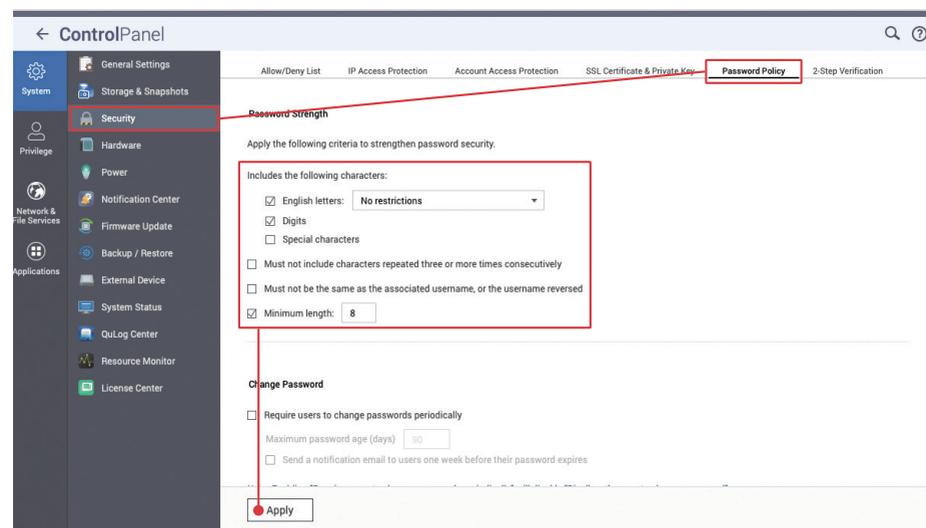
Imposta criterio password

Oltre a disattivare l'account amministratore predefinito "admin", è necessario verificare che tutti gli account siano protetti con password complesse. Con la funzione di protezione dell'accesso, è possibile bloccare i tentativi di accesso dannosi. Per una maggiore sicurezza, è possibile applicare la "verifica in due fasi (2SV)" per tutti gli account per impedire il cracking delle password e gli accessi dannosi.

Aprire "Pannello di controllo" e fare clic su "Impostazioni di sicurezza"



Fare clic su "Criterio password" per accedere alla pagina delle impostazioni. Se il sistema è stato inizializzato in QTS 5.0.0 / QuTS Hero h5.0.0 (o versione successiva), le condizioni di base per la complessità della password sono attivate per impostazione predefinita. È possibile impostare le condizioni con password complesse in base alle specifiche esigenze. La password può essere impostata in modo da contenere "lettere maiuscole e minuscole inglesi" e "numeri", mentre la lunghezza della password è **consigliata ad almeno "10 caratteri"**, fare clic su "Applica" dopo il completamento.



Abilitare la protezione di accesso (IP / account)

"Protezione accesso IP" e "Protezione accesso account" possono aiutare a impedire che le password vengano violate da attacchi. Quando un IP o un account specifico non riesce ad accedere troppe volte, attiverà il blocco IP o la disattivazione dell'account, impedendo agli utenti malintenzionati di tentare ripetutamente le password.

Fare clic su "Protezione accesso IP" per accedere alla pagina delle impostazioni, controllare tutti i servizi, impostare "Intervallo di tempo", "Tentativi di accesso non riusciti" e "Lunghezza blocco IP" in base alle proprie esigenze, quindi fare clic su "Applica" per completare le impostazioni.

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	IP
<input checked="" type="checkbox"/> FTP	1 minute(s)	5	IP
<input checked="" type="checkbox"/> SAMBA	1 minute(s)	5	IP
<input checked="" type="checkbox"/> AFP	1 minute(s)	5	IP
<input checked="" type="checkbox"/> RTTR	1 minute(s)	5	IP
<input checked="" type="checkbox"/> Rsync	1 minute(s)	5	IP

Apply

*** Se l'indirizzo IP di un utente normale è bloccato per errore, è possibile regolare l'elenco di blocco:**

1. **Accedere all'interfaccia di gestione di QTS /QuTS hero da un altro computer**
2. **Modificare l'indirizzo IP e accedere all'interfaccia di gestione QTS /QuTS hero**
3. **Accedere all'interfaccia di gestione di QTS /QuTS hero con un browser mobile**
4. **Utilizzando l'app QManager**

Fare clic su "Protezione accesso account" per accedere alla pagina delle impostazioni, abilitare i servizi, impostare "Intervallo di tempo" e "Tentativi di accesso non riusciti" in base alle specifiche esigenze, quindi fare clic su "Applica" per completare le impostazioni.

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

Apply

*** Se l'opzione "Protezione accesso account" è attivata per l'account amministratore, è possibile che tutti gli account amministratore vengano disabilitati a causa di attacchi di violazione della password. A questo punto, l'account "admin" può essere riabilitato solo tramite la funzione di ripristino e verrà reimpostata anche la password dell'account "admin". Ricordare di modificare la password dopo la reimpostazione.**

Abilitare la Verifica in due passaggi (2SV)

Fare clic su "Verifica in 2 passaggi" per accedere alla pagina delle impostazioni, è possibile applicare l'utilizzo di "Verifica in 2 passaggi (2SV)" per "Utenti" o "Gruppi di utenti". Si consiglia vivamente di abilitare 2SV per gli account nel "Gruppo amministratori". Per gli altri account, valutare personalmente i rischi e applicare le impostazioni appropriate.

Fare clic su "Utenti locali" per aprire il menu e selezionare "Gruppi locali".

Control Panel

← ControlPanel

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

Local Users

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

Apply

Selezionare "Imponi 2SV" in "administrators" e fare clic su "Applica" per completare l'impostazione.

Control Panel

← ControlPanel

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		-

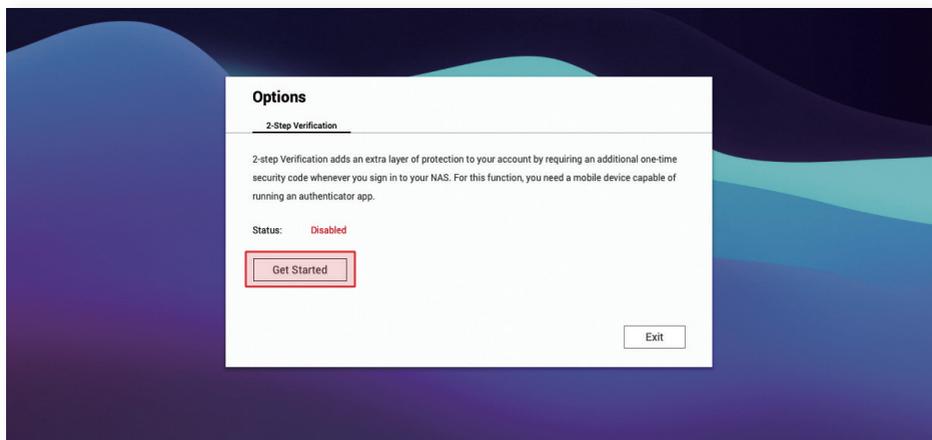
Page 1 / 1

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

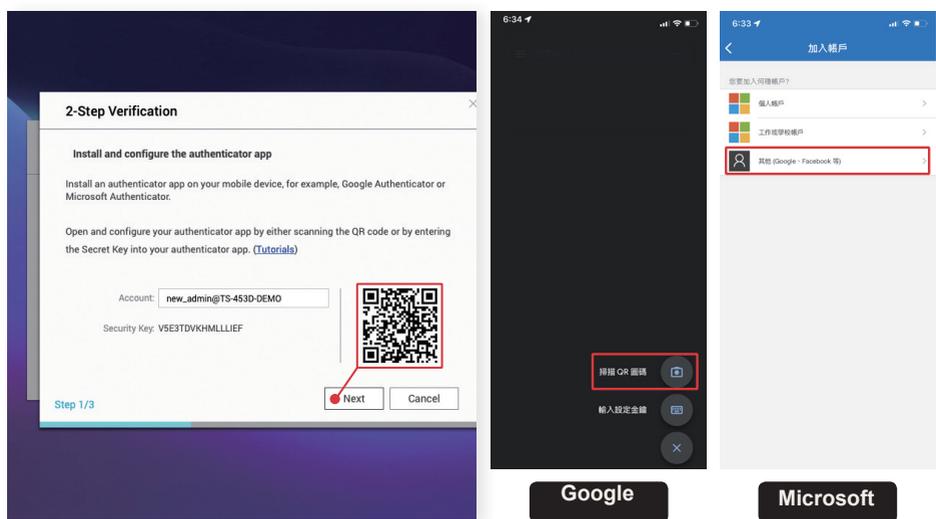
Apply

Dopo aver attivato "Imponi 2SV", se l'account "Amministratore" non è stato impostato con "Verifica in 2 passaggi (2SV)", la volta successiva che si effettua l'accesso, verrà eseguito l'indirizzamento forzato alla pagina di impostazione "Verifica in 2 passaggi (2SV)" per la configurazione dell'account.

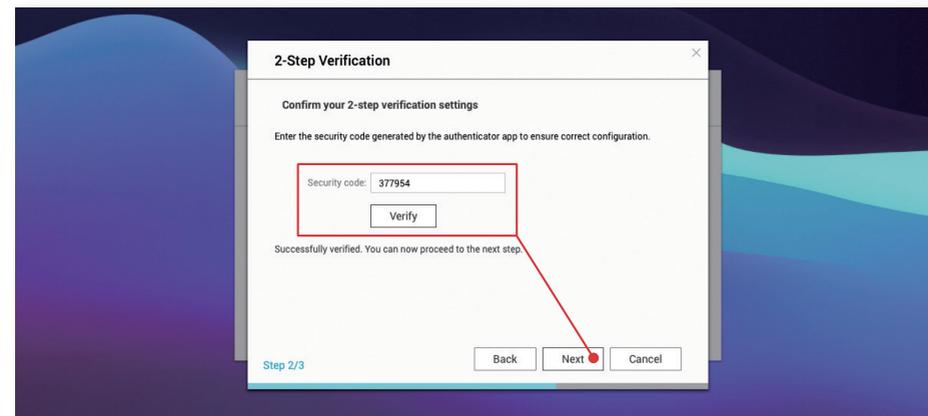
Accedere nuovamente all'account "Amministratore di sistema" e fare clic su "Inizia" per avviare l'impostazione.



Installare "Google Authenticator" o "Microsoft Authenticator" sul dispositivo mobile, eseguire la scansione del codice QR nel programma per aggiungere il dispositivo, quindi fare clic su "Avanti".

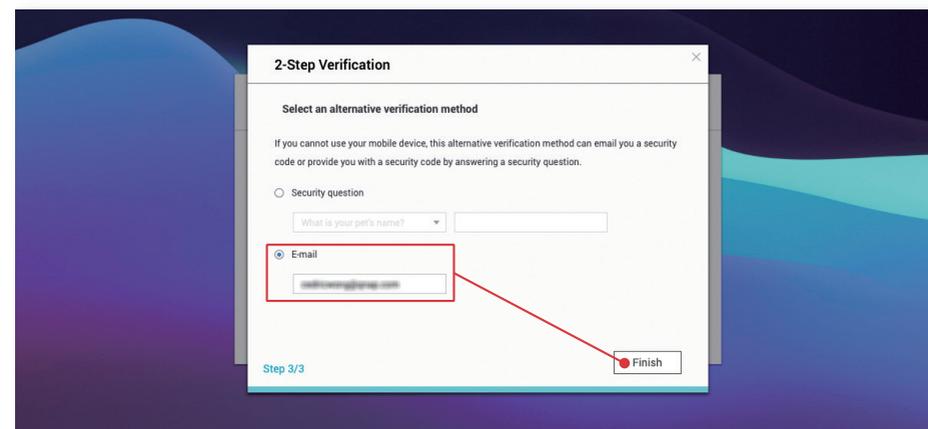


Immettere il "Codice di protezione" a sei cifre generato da "Google Authenticator" o "Microsoft Authenticator" e fare clic su "Verifica". Dopo la verifica, fare clic su Avanti per continuare.



Per configurare un metodo di verifica alternativo*, è possibile selezionare "Domanda di sicurezza"*** o "E-mail"***, compilarlo e fare clic su "Fine" per abilitare "Verifica in 2 fasi (2SV)".

- * Se non è possibile ottenere il "Codice di sicurezza" da un'applicazione di autenticazione, è possibile ricevere un "Codice di sicurezza" rispondendo alla "Domanda di sicurezza" o utilizzando "E-mail".
- ** Rispondere correttamente alla "Domanda di sicurezza" per superare la verifica in 2 passaggi. Non utilizzare domande e risposte semplici o facili da indovinare.
- *** Per utilizzare questa funzione, è necessario aggiungere il metodo di notifica "E-mail" nel "Centro notifiche".



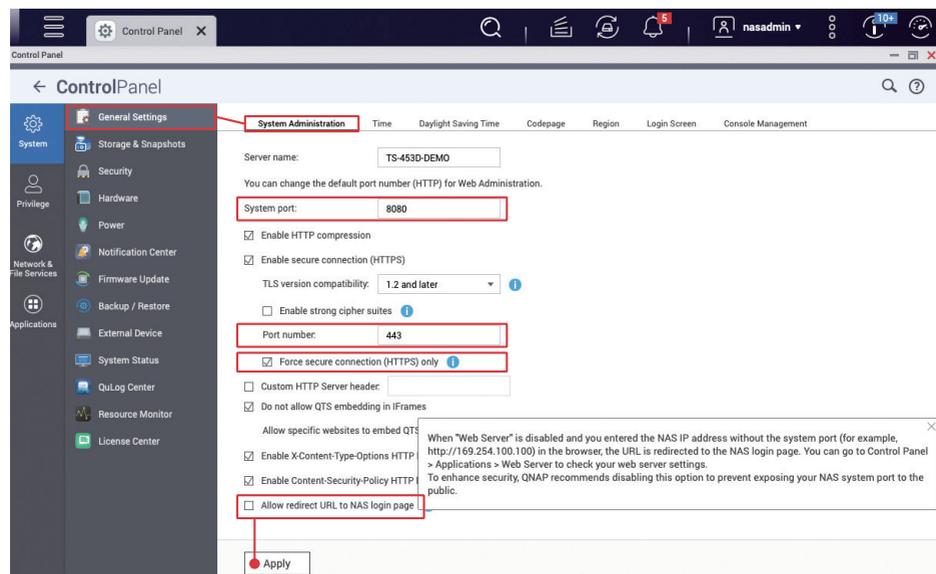
Modifiche a porte predefinite

Ogni servizio in esecuzione sul NAS ha una porta di servizio corrispondente. Ad eccezione di alcune porte di servizio standardizzate che non possono essere modificate, il resto può essere definito dagli utenti.

Quando un hacker cerca un obiettivo di attacco o utilizza il motore di ricerca IoT spesso utilizzato dagli hacker, la porta predefinita viene solitamente tentata per prima. Per ridurre il rischio di attacchi, è necessario modificare le porte predefinite dei servizi comuni. Per quanto riguarda gli attacchi al NAS, il target più comune è la "porta di sistema". Di seguito viene illustrato come modificare la "porta di sistema". Le porte per altre funzioni possono essere modificate nella pagina delle impostazioni corrispondente. Verificare di modificarli prima di utilizzare i servizi correlati per la sicurezza.

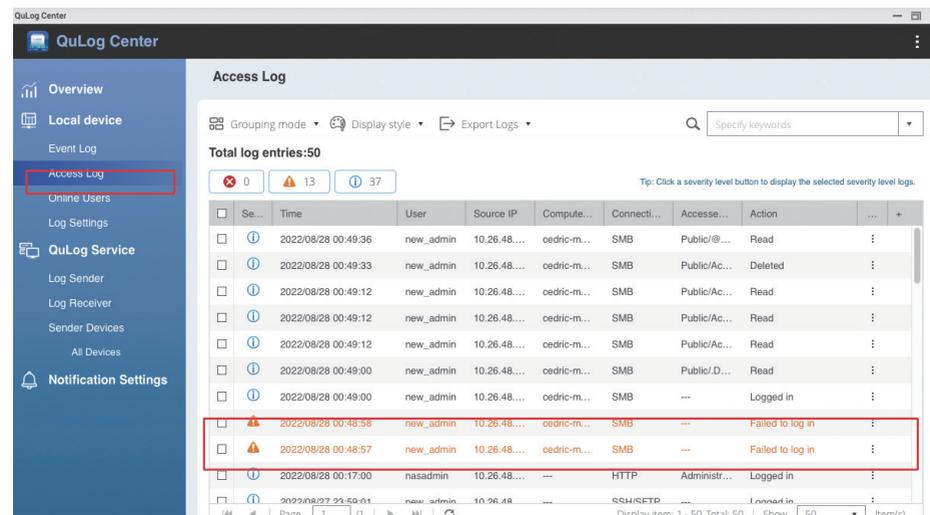
Aprire "Pannello di controllo", fare clic su "Impostazioni generali", il valore predefinito "Porta di sistema (HTTP)" è "8080", è possibile immettere un numero di porta compreso tra 1 e 65535, ad esempio "56789"; per "Porta di sistema (HTTPS)", ovvero la **porta di sistema** (valore predefinito "443") con la funzione "Connessione protetta" attivata, si **consiglia di modificarla**. Allo stesso tempo, si consiglia anche di **controllare "Forza solo connessione protetta (HTTPS)"** per garantire che tutti gli utenti trasmettano dati tramite HTTPS e per impedire agli hacker di intercettare informazioni riservate come le password degli account.

Inoltre, si consiglia di **deselezionare "Consenti reindirizzamento URL alla pagina di accesso NAS"** per evitare che la "Porta di sistema" venga esposta a causa del reindirizzamento automatico. Dopo la modifica, fare clic su "Applica" per completare l'impostazione.

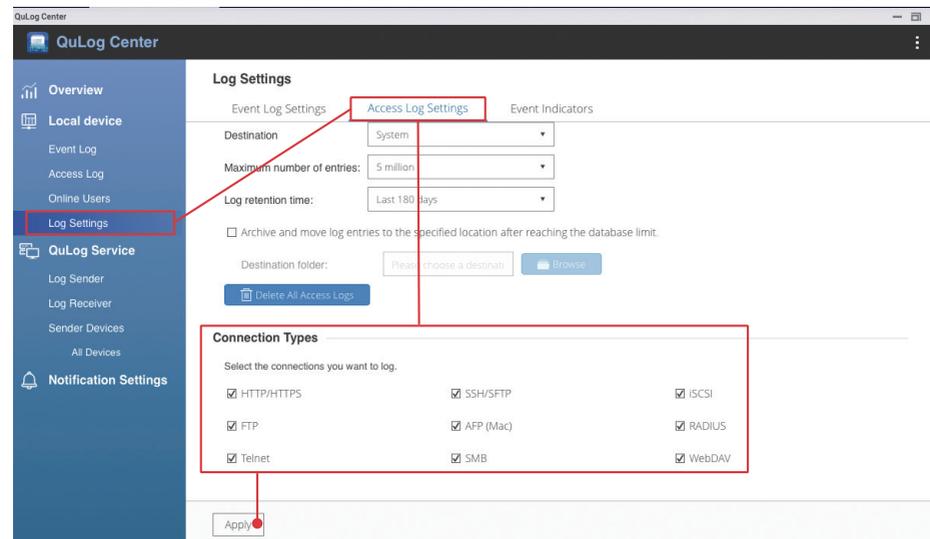


Visualizzare il log accesso

I log di accesso consentono di visualizzare l'accesso ai file, il funzionamento e la cronologia di accesso dell'utente. Quando si verifica un problema, il controllo dei log di accesso dovrebbe essere il primo passo per diagnosticare i problemi sottostanti.



Aprire "QuLog Center", fare clic su "Impostazioni registro" nel menu a sinistra, passare alla pagina "Impostazioni log di accesso", in "Tipi di connessione", controllare tutte le connessioni, quindi fare clic su "Applica" per completare l'impostazione.



Installare e abilitare app di sicurezza

QNAP fornisce diverse applicazioni di sicurezza per migliorare la sicurezza NAS. La configurazione di queste app può migliorare la sicurezza NAS e consentire agli utenti di avere tranquillità.



Security Counselor controlla regolarmente la sicurezza delle impostazioni NAS e informa l'utente di potenziali rischi.

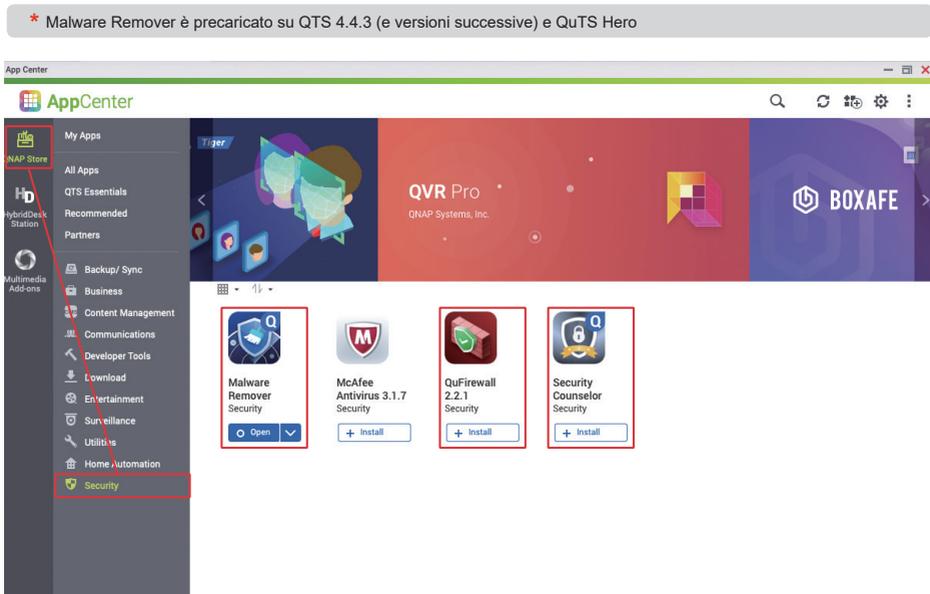


Malware Remover esegue la scansione e rimuove il malware rilevato dal NAS.



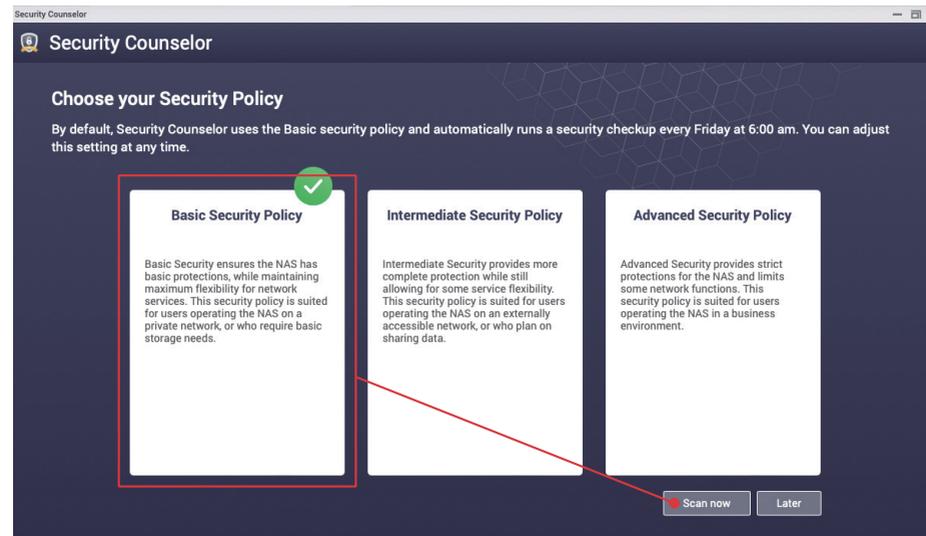
QuFirewall fornisce funzionalità firewall di base per QNAP NAS, impedendo al maggior numero possibile di hacker di connettersi al NAS.

Aprire "App Center", fare clic su "Sicurezza" a sinistra, installare "Security Counselor", "Malware Remover" e "QuFirewall".

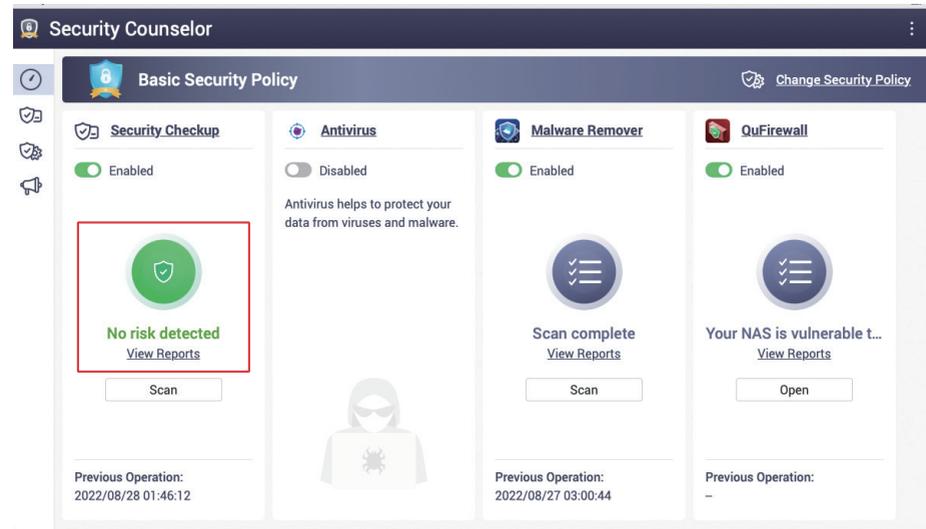


Security Counselor

Aprire "Security Counselor", selezionare "Criterio di sicurezza di base" e fare clic su "Scansiona ora".



Al termine della scansione, il risultato è normalmente "Nessun rischio rilevato". Se viene rilevato un rischio, fare clic su "Visualizza report" per ulteriori dettagli e seguire le istruzioni per modificare le impostazioni.



Di seguito sono riportati i risultati della scansione causati da "rischio elevato" con impostazioni errate deliberatamente modificate. Fare clic su "Assistente impostazioni consigliate" per regolare le impostazioni.

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

"Assistente impostazioni consigliato" elenca i suggerimenti pertinenti. Dopo la lettura e la conferma, fare clic su "Applica suggerimento"; il sistema applicherà automaticamente le impostazioni pertinenti. Alcune impostazioni devono essere modificate manualmente, fare clic sulla scheda "Manualmente" a sinistra e regolare le impostazioni come suggerito. Dopo aver applicato le modifiche, la scansione verrà riavviata automaticamente. È possibile controllare nuovamente i risultati della scansione per verificare che non siano stati rilevati rischi per la sicurezza sul NAS.

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
<input checked="" type="checkbox"/> Either this setting is deselected in the Password Policy screen or the current required minimum length for passwords is below 8 characters.	<input checked="" type="checkbox"/> Configure the settings in the Password Policy screen and require the use of passwords with a minimum of 8 characters.

Apply suggestion

Last scan time: 2022/08/28 01:53:30

Fare clic su "Controllo di sicurezza" a sinistra per accedere alla schermata dei risultati della scansione, quindi fare clic "Pianificazione scansione" a destra per aprire la schermata di impostazione della pianificazione delle scansioni.

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

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.	⋮

Si consiglia di impostare "Pianificazione scansione" su **almeno una volta al mese**, in modo che "Malware Remover" controlli regolarmente lo stato del sistema. Se viene rilevato un rischio e il Centro notifiche è impostato correttamente, si riceverà una notifica in modo che possa essere gestito il più presto possibile.

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

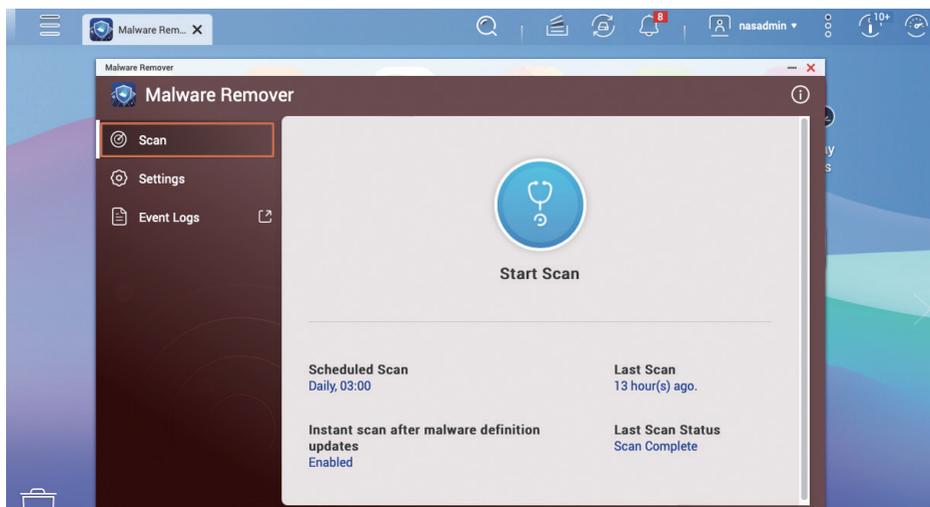
Run on the following days: Friday

Run at the following time: 06:00

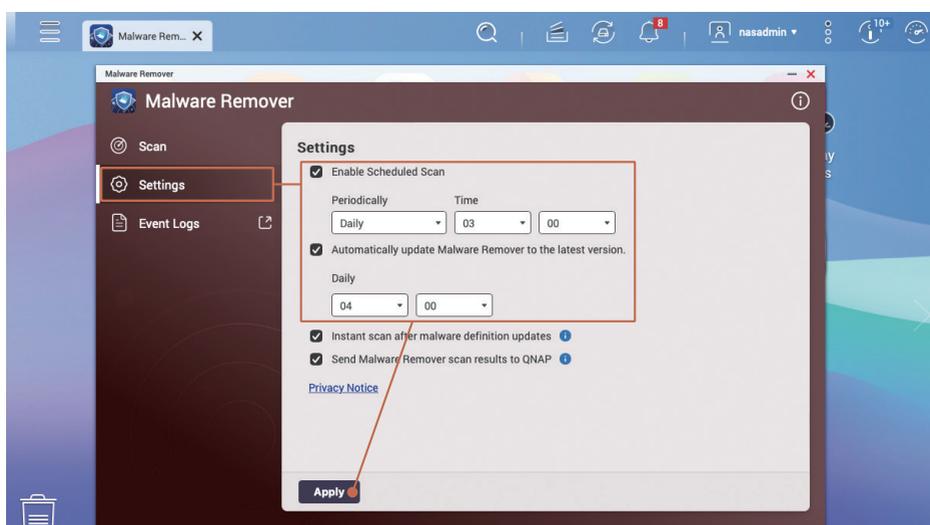
Apply Cancel

Malware Remover

Aprire "Malware Remover", viene visualizzato lo stato dell'ultima scansione, quindi fare clic su "Impostazioni" a sinistra.

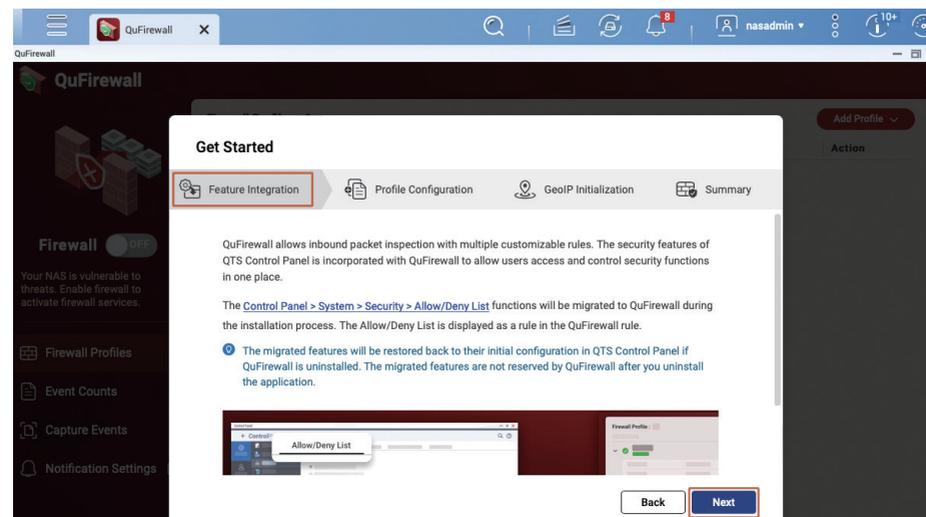


Si consiglia di impostare "Pianificazione scansioni" su **una volta al mese**, in modo che il sistema possa controllare regolarmente le impostazioni e lo stato del sistema. Verificare inoltre che l'opzione "Aggiorna automaticamente Malware Remover alla versione più recente" rimanga selezionata.

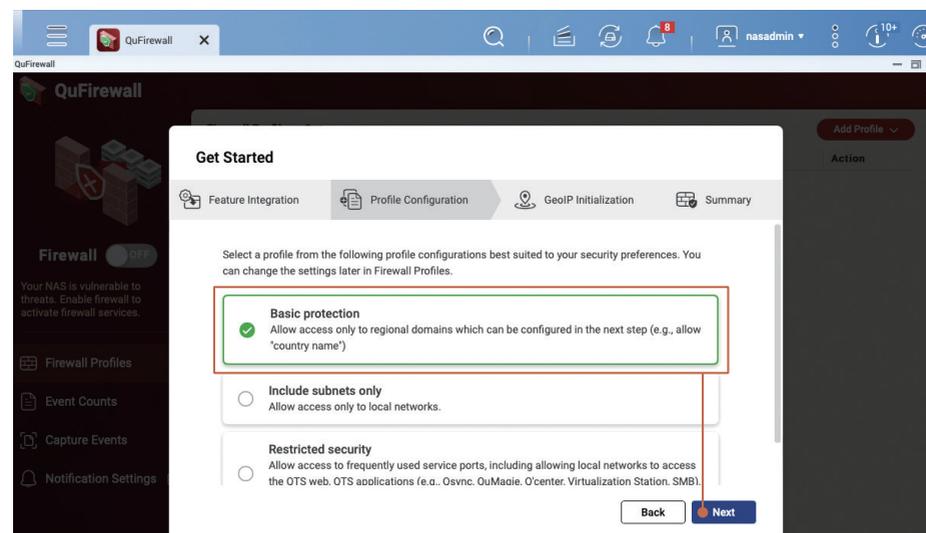


QuFirewall

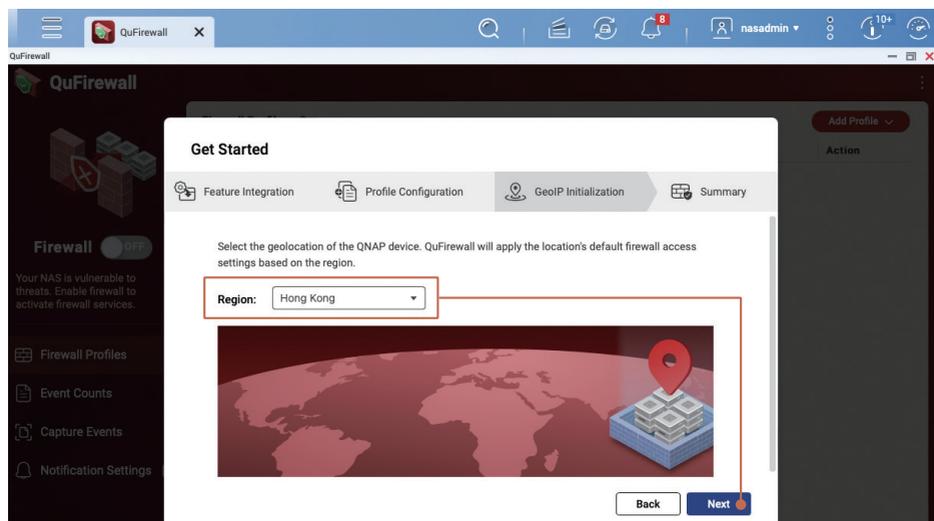
Aprire "QuFirewall". Se si utilizza QuFirewall per la prima volta, viene visualizzata la schermata di avvio. Dopo la lettura, fare clic su "Avanti" per continuare.



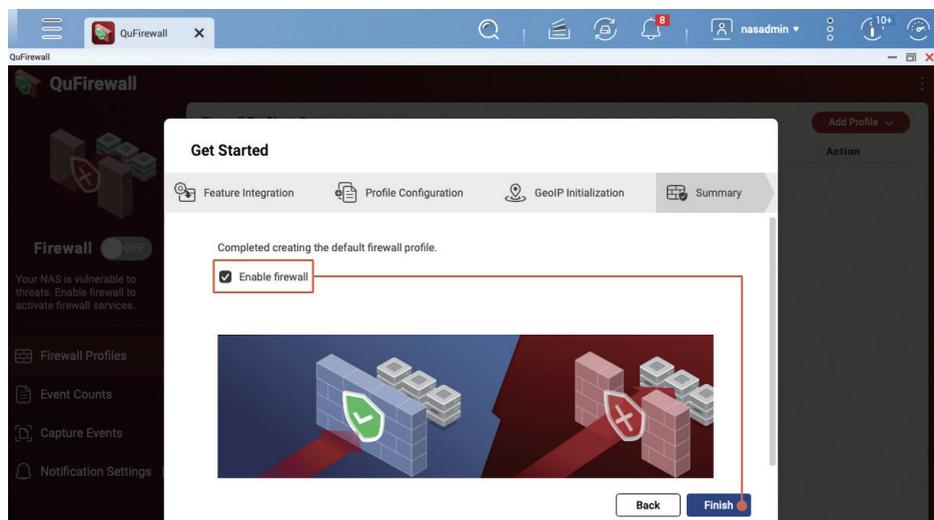
Se la rete non presenta esigenze particolari, si consiglia di selezionare "Protezione di base", quindi fare clic su "Avanti" per continuare.



Selezionare una regione in base alla posizione. Ad esempio: per Taiwan, selezionare "Taiwan"; per Hong Kong, selezionare "Hong Kong"; per Macao, selezionare "Macao". È possibile aggiungere più regioni in un secondo momento. Fare clic su "Avanti" per continuare.

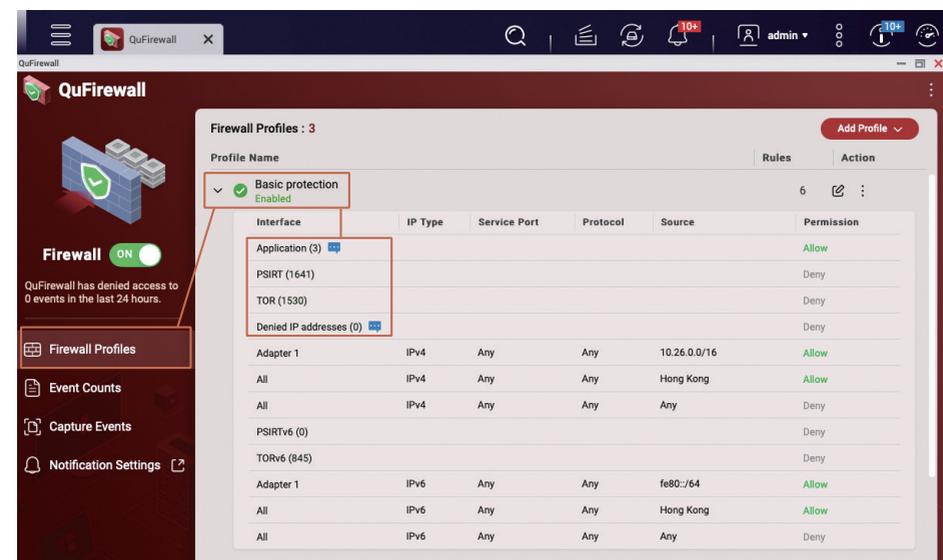


Selezionare "Abilita firewall", quindi fare clic su "Fine" per applicare le impostazioni e attivare il firewall.



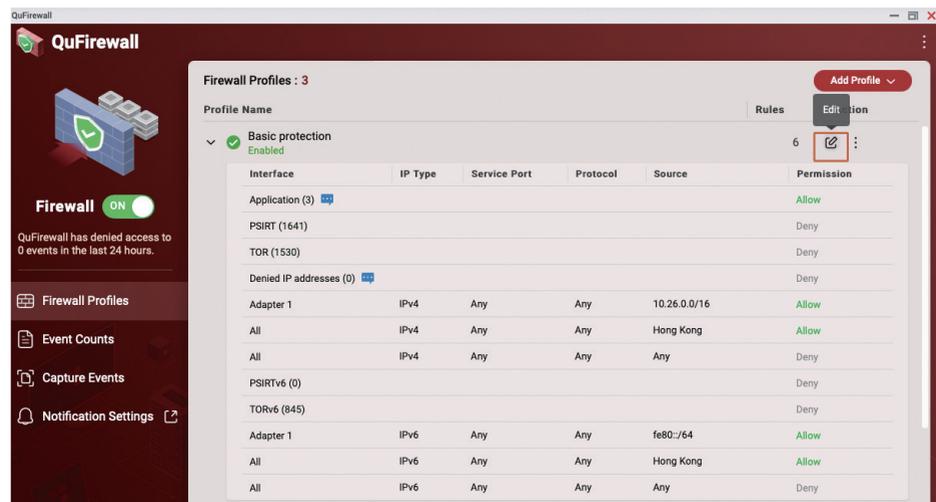
Andare alla pagina Profili di QuFirewall e l'opzione "Protezione di base" sarà visualizzata come attivata. Fare clic su "Protezione di base" per espandere e visualizzare le regole firewall corrispondenti. Le regole vengono controllate rispetto alle informazioni contenute nei pacchetti in entrata, che possono passare o essere bloccati in base alle regole del firewall. Le regole del firewall verranno eseguite in sequenza. Se le condizioni non sono soddisfatte, verrà controllata la riga successiva di regole. Se non vengono soddisfatte, rientrano nell'ultima regola "Nega tutti" e il firewall blocca le connessioni pertinenti.

- Le regole di "Applicazione" vengono create dal sistema per garantire il corretto funzionamento del sistema.
- La regola "PSIRT" è una blacklist compilata da QNAP PSIRT. Contiene indirizzi IP noti per attaccare QNAP NAS.
- La regola "TOR" viene utilizzata per bloccare le connessioni dalla rete TOR. TOR Network è ampiamente utilizzato dai criminali a causa del suo anonimato e il suo blocco può ridurre il rischio di essere attaccato.
- Gli "Indirizzi IP negati" sono indirizzi IP bloccati dalla funzione "Protezione accesso IP" o dalla blacklist aggiunta manualmente dall'utente.

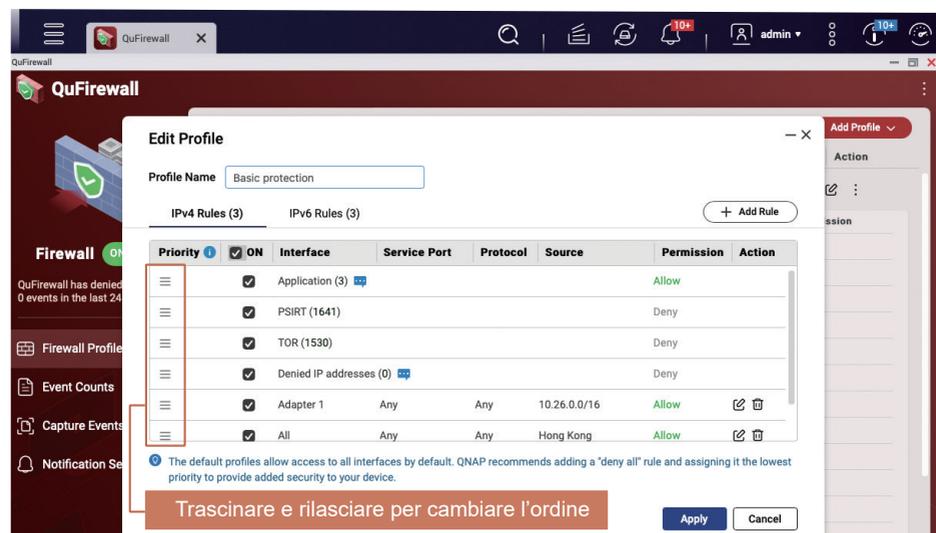


Altre regole possono essere personalizzate dall'utente e, in base alle impostazioni di protezione di base, solo le connessioni Internet dalla stessa intranet e dalla stessa regione saranno "consentite". QNAP consiglia di utilizzare il concetto di "whitelisting" per gestire le regole personalizzate per limitare rigorosamente gli indirizzi IP che possono connettersi al NAS.

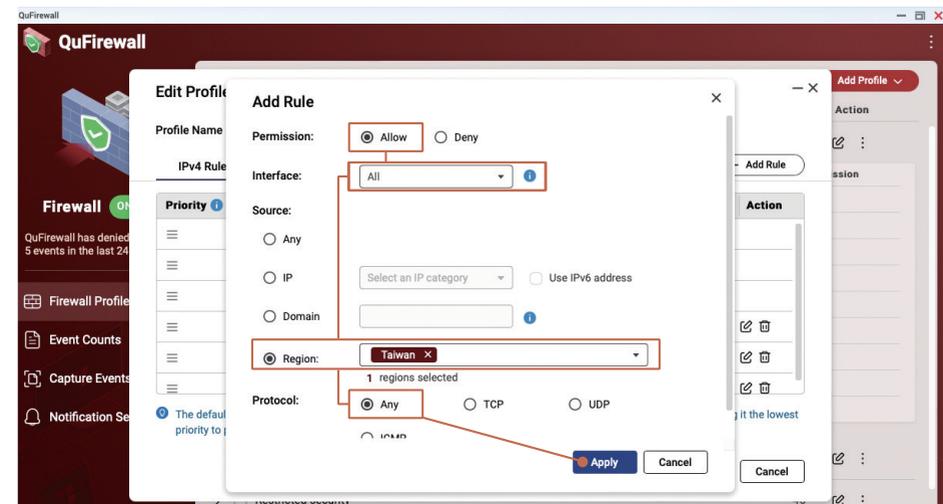
Di seguito viene illustrato come modificare le regole del firewall. Fare clic sul pulsante "Modifica" per modificare la schermata Profili firewall.



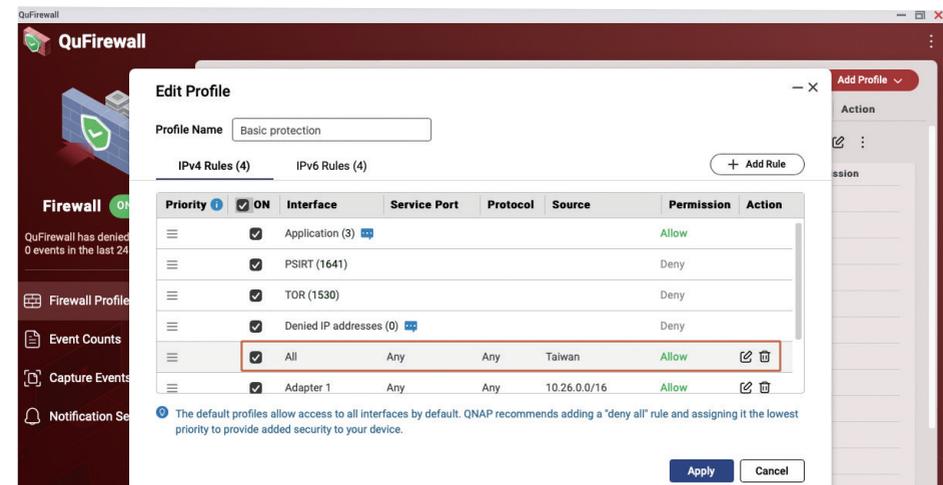
Nella schermata Modifica profilo, è possibile modificare l'ordine delle regole o aggiungere nuove regole. Nell'esempio seguente viene aggiunta un'altra regione a cui è consentita la connessione. Fare clic su "Aggiungi regola" per accedere alla schermata di impostazione.



Ad esempio, per consentire connessioni da Taiwan, è necessario impostare "Autorizzazione" su "Consenti"; "Interfaccia" su "Tutti"; "Regione" per "Origine", quindi selezionare "Taiwan"; "Protocollo" su "Qualsiasi", quindi fare clic su "Applica" per aggiungere la regola al termine.



Nella pagina "Modifica profilo", è possibile visualizzare le nuove regole aggiunte. Se necessario, è possibile modificare l'ordine delle regole. Dopo aver confermato che sono corrette, fare clic su "Applica".



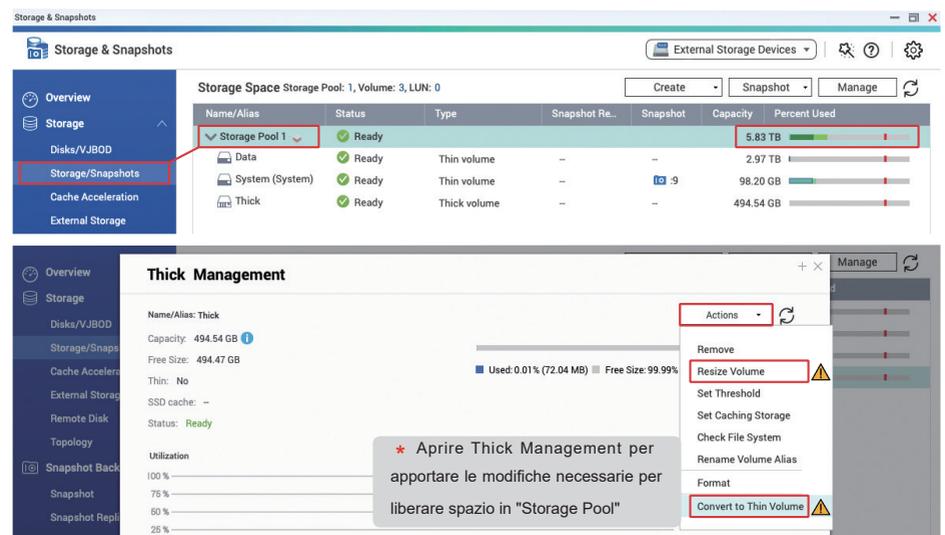
Abilitare snapshot pianificate

La funzione snapshot consente di proteggere i dati importanti creando punti di ripristino multiversione. È possibile impostare una pianificazione snapshot sul QNAP NAS per consentire al sistema di creare automaticamente snapshot in base alla pianificazione come protezione dati di base.

- * Le snapshot pianificate sono abilitate per impostazione predefinita per i "volumi completi/thin" creati da QTS 5.0.0
- * In QTS 5.0.1 (e versioni successive) solo i "volumi thin" con snapshot pianificate abilitate per impostazione predefinita
- * Le "Cartelle condivise" create da QuTS Hero h5.0.1 (e versioni successive) abilitano gli snapshot pianificate per impostazione predefinita

Aprire "Archiviazione e snapshot", fare clic su "Archiviazione/Snapshot" a sinistra e verificare che "Spazio di archiviazione" sia una struttura "Storage Pool" e che lo "Storage Pool" disponga di spazio libero sufficiente per il funzionamento della funzione di snapshot. Se il tipo di volume è "volume pieno", è possibile considerare "Ridimensiona volume*" e "Converti in volume thin*" per liberare spazio di "Storage Pool" per la funzione di snapshot.

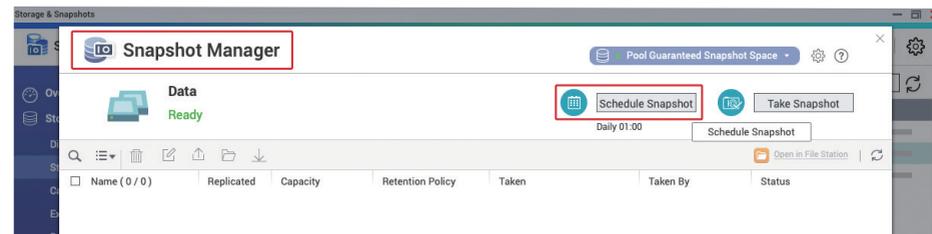
- * È necessario eseguire il backup dei dati prima di convertire i volumi per evitare potenziali perdite di dati.



Dopo aver confermato lo spazio sufficiente in "Storage Pool" sul NAS, fare clic su "Volume", quindi su "Snapshot" nella parte superiore e fare clic su "Snapshot Manager" nel menu.

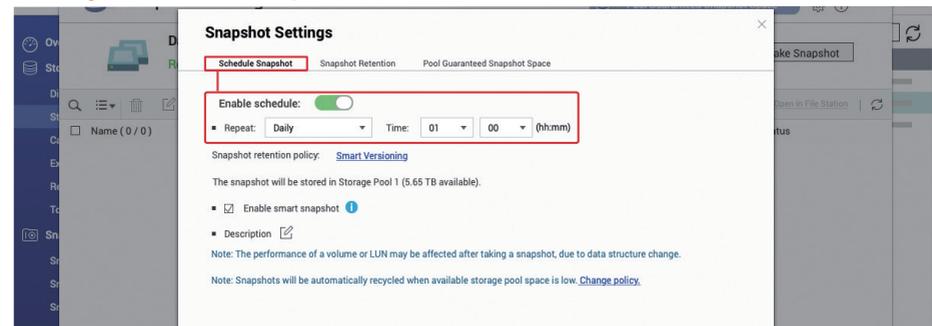


Andare alla pagina di impostazione "Snapshot Manager" di "Volume" e fare clic su "Pianifica snapshot", in alto a destra.



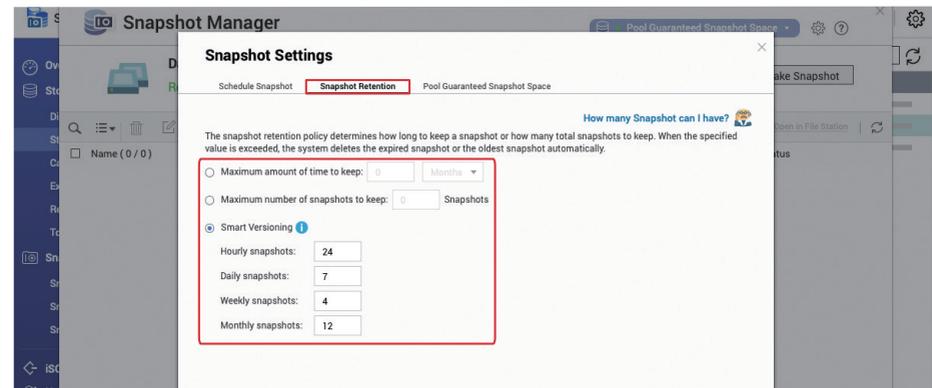
Impostare lo stato "Abilita pianificazione" su "Abilita", quindi modificare la pianificazione in base alle specifiche esigenze.

Si consiglia di utilizzare i valori predefiniti.



È possibile impostare un criterio di conservazione delle snapshot per limitare il numero di snapshot ed evitare che occupino troppo spazio.

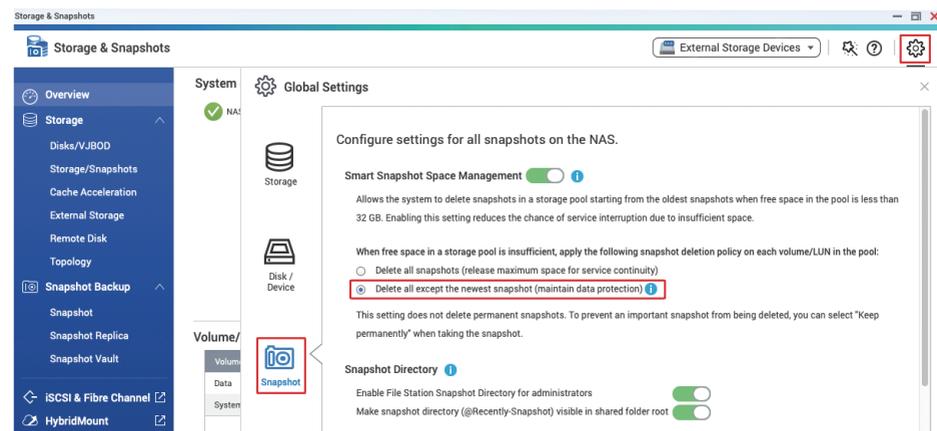
Si consiglia di impostare "Smart Versioning", cioè la regola del GFS (Grandfather-Father-Son), per mantenere un numero sufficiente di versioni per la protezione dei dati. Dopo avere completato l'impostazione, fare clic su "OK" per applicarla.



Impostare il criterio di eliminazione snapshot

Quando lo spazio dello storage pool non è sufficiente, il sistema elimina le snapshot in base alle impostazioni per mantenere il normale servizio di sistema ed evitare potenziali interruzioni del servizio causate da spazio insufficiente.

In "Archiviazione e snapshot", fare clic su "Impostazioni" , nell'angolo in alto a destra, aprire "Impostazioni globali" e fare clic su "Snapshot". Si consiglia di impostarlo su "Elimina tutto tranne snapshot più recente" per evitare che tutte le snapshot vengano recuperate e perdano la protezione.

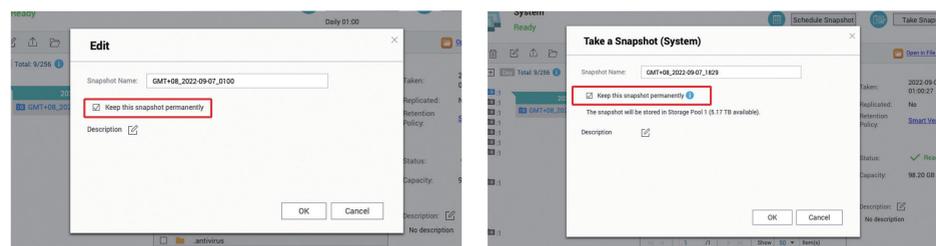


Per far sì che il sistema conservi tutte le snapshot anche quando lo "Storage Pool" non dispone di spazio sufficiente, disabilitare "Smart Snapshot Space Management". In questo modo lo "Storage Pool" entrerà nello stato di sola lettura/eliminazione quando lo spazio "Storage Pool" sarà insufficiente. È necessario eliminare manualmente la snapshot per ripristinare lo "Storage Pool" al normale funzionamento. Controllare regolarmente l'utilizzo dello spazio dopo aver disattivato questa funzione.



Per evitare errori di protezione dovuti ai criteri di eliminazione delle snapshot, si consiglia di impostare tutte o parte delle snapshot su "Mantieni snapshot in modo permanente"* dopo aver memorizzato una grande quantità di dati per evitare che le snapshot vengano riciclate dal sistema.

* Deve essere eliminata manualmente per liberare spazio. Si consiglia di creare ed eliminare manualmente regolarmente



Elenco di controllo delle impostazioni di sicurezza NAS

- Configurare il Centro notifiche**
 - Impostare almeno un metodo di notifica
 - Creare una regola "Notifiche avvisi"
 - Creare regole di notifica "Aggiornamento firmware"
- Abilitare l'aggiornamento automatico firmware (QTS / QuTS Hero)**
- Configurare App Center**
 - Aggiornare tutte le app alla versione più recente
 - Impedire l'installazione di applicazioni che non dispongono di una firma digitale valida
 - Abilitare aggiornamenti automatici
- Disabilitare o rimuovere le funzioni non necessarie**
 - Verificare se sono necessari servizi abilitati
 - Verificare se le app App Center abilitate sono necessarie
 - Disabilitare SSH
 - Disabilitare Telnet
- Rafforzare la sicurezza account di sistema**
 - Disabilitare l'account "admin" predefinito
 - Impostare il criterio password
 - Abilitare la protezione di accesso IP
 - Abilitare la Verifica in due passaggi (2SV)
- Modificare la porta predefinita di sistema**
- Abilitare il log di accesso**
- Installare e abilitare app di sicurezza**
 - Security Counselor**
 - Abilitare la scansione pianificata
 - Malware Remover**
 - Abilitare la scansione pianificata
 - QuFirewall**
 - Abilitare il firewall
 - Impostare la regione Geo-IP
 - Abilitare regole PSIRT
 - Abilitare regole TOR
- Abilitare snapshot pianificate**
 - Impostare regolarmente "Mantieni snapshot definitivamente"

Q È più sicuro scollegare il NAS da Internet?

A No. Generalmente, la "disconnessione" del NAS fa riferimento alla rimozione del NAS dalla rete in modo da non consentire l'iniziazione di connessioni nell'ambiente esterno. Sebbene alcuni malware richiedono l'esecuzione di una connessione esterna, esistono ancora malware in grado di eseguire azioni pericolose senza connessione esterna. Pertanto, non solo gli hacker non potranno eseguire azioni illegali, ma alcune funzioni di sistema non potranno funzionare correttamente, ad esempio gli aggiornamenti e le notifiche software automatici. L'approccio corretto è limitare il traffico nel NAS in modo da evitare l'esposizione su Internet, per migliorare la sicurezza.

Q Il disco rigido è configurato con RAID, quindi non è necessario il backup?

A No. Il RAID non è un metodo di backup. Il livelli RAID superiori a 0 sono intesi solo a fornire ridondanza da errori disco. RAID non fornisce alcuna protezione dal rilevamento o dalla crittografia dati. Pertanto, si consiglia di eseguire correttamente il [backup di dati in base al principio di backup 3-2-1](#).

Q Le "snapshot" sono state già configurate, quindi non è necessario il backup?

A No. Le "snapshot" sono memorizzate nello stesso set di dischi rigidi dei dati, quindi in caso di errore RAID i dati saranno persi. Inoltre, se gli hacker sono in grado di ottenere privilegi sufficienti (ad esempio, il cracking dell'account amministratore), anche la "snapshot" potrebbe essere eliminata. Pertanto, si consiglia di eseguire correttamente il backup dei file snapshot in base al principio di backup 3-2-1.

Q Il NAS non è esposto a Internet, significa che non è possibile che venga attaccato?

A No. Sebbene la maggior parte degli attacchi informatici provengano da Internet, il NAS rischia comunque di essere attaccato tramite intranet. Ad esempio, se un altro computer o dispositivo della rete Intranet viene violato o interessato da malware, può essere utilizzato per attaccare e danneggiare altri dispositivi della rete Intranet. L'installazione di software antivirus e la distribuzione di prodotti per la protezione di rete sul computer possono aiutare a gestire le minacce correlate. Ad esempio, QNAP ADRA NDR è in grado di rilevare attività Intranet sospette e di isolarle automaticamente. Nel contempo, si consiglia anche di eseguire correttamente il backup di dati in base al principio di backup 3-2-1.

Q Il NAS è stato utilizzato per molto tempo, come verificare se è installato un malware?

A Se si nota che il carico del processore è eccessivamente elevato, si verificano errori di aggiornamento del software o se sono presenti applicazioni sconosciute in App Center, è possibile che sia stato installato un programma dannoso. Si consiglia installare ed utilizzare la versione più recente di Malware Remover. Se non è ancora possibile risolvere il problema, contattare il team di supporto tecnico QNAP per assistenza.

Q Se è necessario aprire alcuni servizi a Internet, cosa occorre fare per garantire la sicurezza?

A Verificare che sul NAS sia installata la versione più recente del firmware e delle applicazioni. È possibile abilitare QuFirewall per fornire una protezione firewall di base e le regole "PSIRT" e "TOR" possono aiutare a bloccare le connessioni di alcuni hacker. Per il ruolo di utente aziendale o aziendale, si consiglia di utilizzare una soluzione firewall di livello superiore. Inoltre, se lo spazio dello storage pool lo consente, è possibile creare "snapshot" per la protezione dei dati di base. Si consiglia inoltre di eseguire correttamente il backup dei dati in base al principio di backup 3-2-1 per prepararsi allo scenario peggiore e prevenire la potenziale perdita di dati.

Q Il NAS è obsoleto e non supporta la versione più recente di QTS, può ancora essere utilizzato in modo sicuro?

A I modelli legacy e EOL (End of Life) hanno un supporto limitato e devono essere utilizzati solo per il backup intranet/offline.

Q Perché continuo a ricevere un avviso di errore di accesso al NAS?

A Se l'indirizzo IP del login non riuscito proviene da Internet, significa che il NAS è sotto attacco di cracking password forzato. Occorre evitare di esporre il NAS a Internet e seguire questo tutorial per rafforzare il proprio NAS. Se l'indirizzo IP dell'accesso non riuscito proviene dalla rete Intranet, verificare se il dispositivo con tale indirizzo IP dispone di malware installato.

Q Perché tutti i miei file hanno nomi file strani?

A Questo è un sintomo di un'infezione ransomware. Controllare i log di accesso NAS per determinare se l'azione di crittografia proviene da un altro computer o dal NAS stesso. Se il vostro NAS è stato influenzato da ransomware, allora occorre adottare misure adeguate per arrestare la diffusione dell'infezione. Se necessario, contattare il team di supporto tecnico QNAP per assistenza.

Q Cosa fare se il NAS viene infettato da un ransomware?

A La maggior parte dei ransomware utilizza metodi di crittografia infrangibili. Se non è presente alcuna chiave corretta, i file non possono essere sbloccati, quindi i file possono essere ripristinati solo tramite backup o snapshot.

Modificare immediatamente le impostazioni del router in base a questo tutorial per evitare di esporre il NAS a Internet e per prevenire attacchi secondari. In secondo luogo, è necessario sospendere immediatamente tutte le attività di sincronizzazione e impostare le snapshot in modo che vengano conservate definitivamente per evitare di perdere i file di backup. Se i dati contengono backup o snapshot ripristinabili, è possibile ripristinare i file dopo aver aggiornato il firmware e le applicazioni NAS e dopo aver completato la scansione di Malware Remover. Se i dati non vengono sottoposti a backup, eseguire il backup della nota di riscatto lasciata dal ransomware e dal metodo di pagamento del riscatto, quindi provare a utilizzare metodi come il recupero dei dati per recuperare alcuni dati. Se necessario, contattare il team di supporto tecnico QNAP per assistenza.

Q Sono visualizzati continuamente report multimediali sulle vulnerabilità del prodotto QNAP con patch. Significa che i prodotti QNAP non sono sicuri?

A Non esistono software e hardware perfetti al mondo. Che si tratti di software proprietario sviluppato da vari produttori o di software open source, o anche di hardware, le vulnerabilità vengono sempre individuate e quindi applicate alle patch dai produttori. Come altre importanti aziende tecnologiche, QNAP continua a applicare patch alle vulnerabilità note e rilascia i file di aggiornamento per consentire agli utenti di aggiornare il prima possibile per garantire la protezione dei dispositivi e dei dati degli utenti. QNAP PSIRT emette inoltre notifiche di cybersicurezza per la divulgazione esterna, in modo che gli utenti possano agire contro i problemi che si presentano. QNAP ritiene che affrontare le vulnerabilità in modo aperto e trasparente possa proteggere il diritto degli utenti a conoscere e contribuire a migliorare la sicurezza dei prodotti. Gli utenti sono inoltre invitati a iscriversi agli avvisi di sicurezza QNAP per ottenere informazioni pertinenti, accurate e complete prima dei report multimediali.

Avvisi sulla sicurezza QNAP:

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



Q Qual è il principio di backup 3-2-1?

A Il principio di backup 3-2-1 è un principio di backup noto nel settore IT. È concepito in base allo scenario peggiore. Garantisce che in caso di emergenza siano presenti file di backup per ripristinare i dati al fine di evitare perdite e garantire la sicurezza.

Il "3" in Backup 3-2-1 indica almeno tre copie di backup; il "2" indica almeno due supporti di archiviazione; e l'"1" indica almeno che una copia è un backup offsite.

In base al principio di backup 3-2-1, saranno presenti file di backup che possono essere ripristinati indipendentemente da modifiche accidentali, cancellazione, danni all'hardware, infezioni da virus e disastri come incendi e inondazioni.

Per soddisfare questo principio, QNAP NAS include Hybrid Backup Sync 3 (HBS3), Snapshot Replica e SnapSync (supportato solo da QuTS Hero) per eseguire il backup dei dati sul NAS su un NAS esterno, cloud pubblico, storage esterno, altri file server e/o altri dispositivi per garantire che non venga perso nulla.

Esercitazioni correlate a Hybrid Backup Sync 3 (HBS3):

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



Tutorial relativi a Snapshot Replica:

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



Tutorial SnapSync:

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



Per migliorare la sicurezza, è possibile aggiungere il backup o il backup offline allo spazio di archiviazione WORM (Write Once Read Many) di QuTS Hero per evitare che i dati vengano manomessi.

MEMO



2 0 2 3

Guida alla sicurezza

QNAP



QNAP SYSTEMS, INC.

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

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

QNAP potrebbe modificare le specifiche e le descrizioni del prodotto in qualsiasi momento senza preavviso.
Copyright © 2023 QNAP Systems, Inc. Tutti i diritti riservati.

QNAP® e altri nomi dei prodotti QNAP sono marchi di proprietà o marchi registrati di QNAP Systems, Inc.
Altri prodotti e nomi societari riportati qui possono essere marchi registrati dei rispettivi proprietari.