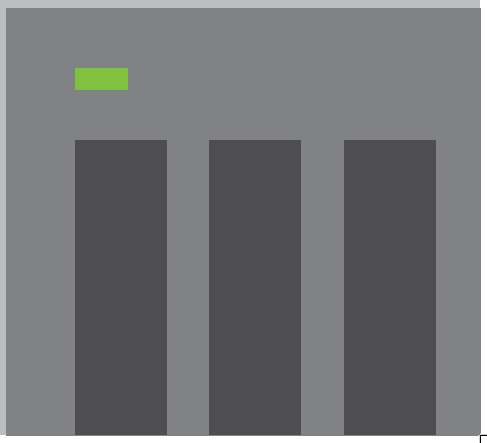
QNAP

2023

보안 가이드



2023

보안 가이드

색인

인터넷에 NAS 노출 피하기

NAS 보안 설정

서문

QNAP 은 보안을 매우 중시합니다 . 보안 위협이 증가하는 가운데 QNAP 은 사용자에게 보안과 편의성 모두를 갖춘 솔루션을 제공하기 위해 지속적으로 하드웨어 및 소프트웨어 설계를 개선해오고 있습니다 .

QNAP 의 제품 보안 사고 대응팀 (PSIRT) 은 QNAP 제품에 관련된 보안 문제 처리를 담당하고 있습니다 . 사이버 보안 관련 사건을 처리하는 것 이외에 , PSIRT 는 또한 다양한 제품에서의 취약성 보고 , 조사 , 조치 및 공지를 맡고있습니다 .

QNAP 은 제품 보안 향상을 위해 최선의 노력을 다합니다 . 과거에는 제품들이 사용자가 보다 편리하고 손쉽게 설치하여 사용할 수 있도록 설계되었습니다 . 최근 몇 년 동안 네트워크로 연결된 장치에 대한 사이버 공격이 증가함에 따라 QNAP 제품 설계 관점 역시 변화하였으며 , 사용자의 게이트키퍼 역할을 하고 사용자가 관련 위협을 효과적으로 해결할 수 있도록 Security by Design 형태로 제품 설계가 바뀌고 있습니다 .

이 튜토리얼은 사용자가 보안을 개선하기 위해 NAS 를 올바로 설정하는 데 도움이 됩니다 . 질문이 있는 경우 , 기술 지원팀에 연락해서 도움을 요청하십시오 .

제품 취약성 및 보안 관련 사건 정보에 대해서는 QNAP Security Advisories 를 구독하고 해당 자료를 참조하시기 바랍니다 .

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

QNAP 고객 서비스 :

https://service.qnap.com/

일반적인 공격

사이버 공격에 방어하는 방법을 알기 위해서는 그러한 공격이 어떻게 시작되는지를 파악해야 합니다 . NAS 에 대한 공격의 대부분은 인터넷을 통해 이루어집니다 . 주로 공격은 " 암호 크래킹 " 과 " 취약성 공격 " 의 두 가지 형태로 나타납니다 . 여기서 " 취약성 공격 " 은 " 엔데이 (N-Day)" 와 " 제로 데이 (Zero-Day)" 로 나뉠 수 있습니다 .

" 엔데이 (N-Day)" 는 이미 패치 완료된 취약성을 이용해 공격을 시작함을 뜻하며 , 대부분 현재 나타나고 있는 공격이 이 범주에 속합니다 . 이러한 공격은 항상 최신 보안 패치와 업데이트를 설치함으로써 효과적으로 방어할 수 있습니다 .

" 제로 데이 (Zero-Day)" 는 미확인된 취약성을 이용해 공격을 시작함을 뜻하며 , 제조사는 사후에만 보안 패치를 발행할 수 있습니다 . 이러한 공격은 공격자의 장치 접속을 막아 사전에 예방 및 방어할 수 있습니다 .

다음 표는 사용자가 참조할 수 있도록 다양한 공격에 대한 대응을 보여줍니다 .

대응	공격		
	암호 크래킹	취약성 공격 (엔데이)	취약성 공격 (제로데이)
인터넷에 노출 피하기	V	V	V
소프트웨어 업데이트 (시스템 및 앱)	X	V	Δ
자동 업데이트 활성화 (시스템 및 앱)	X	V	Δ
모든 계정에 강력한 암호 사용	V	X	X
기본 "admin" 계정 비활성화	V	X	X
2 단계 인증 활성화	V	X	X
액세스 보호 활성화	Δ	X	X
방화벽 활성화	Δ	Δ	Δ
시스템 알림 받기	Δ	Δ	Δ
기본 포트 변경	Δ	Δ	Δ
불필요한 기능 비활성화 / 제거	Δ	Δ	Δ

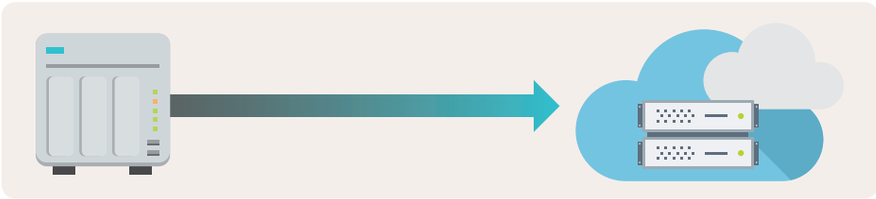
V: 효과적인 X: 효과적이지 않은 Δ : 효과적일 수 있는 (공격을 완화하거나 공격 위험을 낮출 수 있음)

" 인터넷에 노출 피하기 " 는 효과적으로 공격자의 장치 접속을 막아 공격시도를 저지하는 최선의 방법입니다 . 이 튜토리얼은 " 인터넷에 노출 피하기 " 부터 시작한 다음 , NAS 예방 및 방어 기능을 향상시키기 위한 전체 "NAS 보안 설정 " 튜토리얼을 제공합니다 .

기본 네트워크 장비 개념

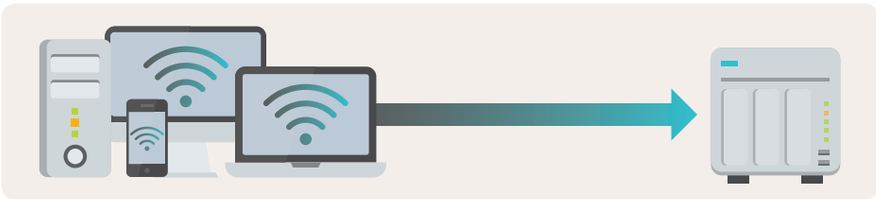
네트워크로 연결된 장치인 NAS 는 두 가지 연결 방향을 지원합니다 .

01 | NAS 외부 연결



NAS 는 일반적으로 외부 연결을 사용합니다 . 예를 들어 , 자동 업데이트 , 알림 전송과 같은 기본 시스템 기능이 해당됩니다 . 또한 NAS 데이터를 인터넷상의 퍼블릭 클라우드에 백업해야 하거나 NAS 를 사용해 다른 장치나 퍼블릭 클라우드 (예 : 가상 머신 , Google Workspace, Microsoft 365), 컴퓨터 또는 서버로부터 데이터를 백업해야 할 경우 , NAS 에 외부연결이 활성화되어 있어야 합니다 .

02 | NAS 에 연결하는 기타 장치 (예 : 컴퓨터 , 모바일 , 기타 서버)



NAS 가 제공하는 파일 엑세스 및 GUI 와 애플리케이션 서비스를 이용해야 할 경우 , NAS 에 연결이 필수입니다 .

라우터의 DMZ, 포트포워딩 또는 UPnP 기능을 사용자가 비활성화 시킨 경우 , 라우터는 인터넷과 연결을 위한 모든 트래픽을 차단합니다 . 로컬 네트워크상의 장치만 NAS 에 액세스할 수 있습니다 .

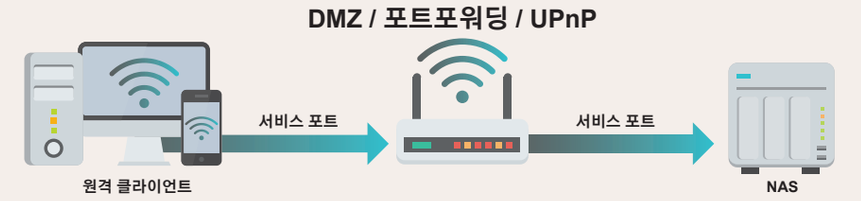
라우터의 위의 기능이 사용자가 활성화시키면 인터넷상의 불특정 다수를 포함한 모든 사람들이 개방된 포트를 통해 라우터의 표준화된 접근방법에 따라 NAS 에 접근하고 , 로그인을 위한 아이디와 비밀번호를 사용해서 사용자가 원하는 NAS 의 기능을 정상적으로 사용할 수 있습니다 . 그러나 해커들도 인터넷에 공개된 라우터를 찾아 , NAS 의 위치를 특정할 수 있으며 , 아이디와 비밀번호 크래킹이나 소프트웨어 취약성을 이용해 공격할 수 있으므로 보안 위험이 제기됩니다 .

원격으로 NAS 에 연결하는 다양한 방법

01 | 라우터의 DMZ, 포트포워딩 또는 UPnP 활성화 및 구성

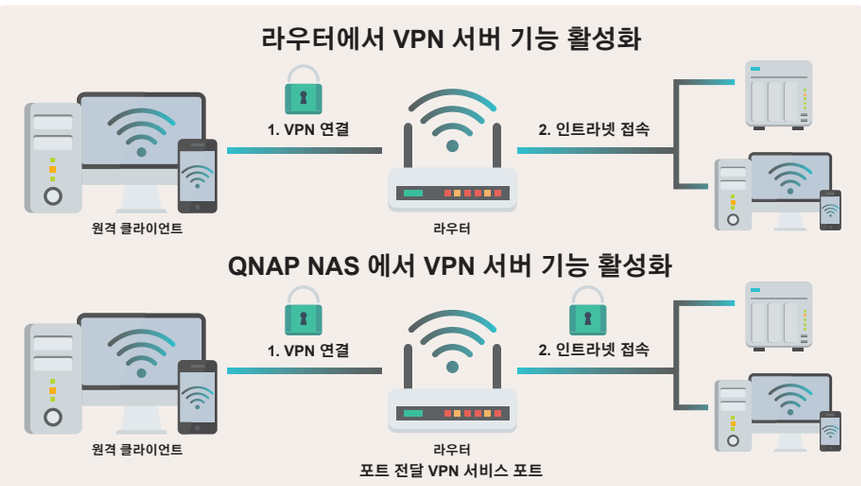
라우터의 이 기능들은 보안 위험이 있습니다 . 네트워크 구성에 관한 전문가가 아니거나 수반되는 위험을 숙지하고 있지 않은 일반 사용자는 **이 방법의 사용을 권장하지 않습니다** *. 라우터는 인트라넷 장치로 트래픽을 통과시키기 때문에 라우터와 NAS 사이에 악성 트래픽을 차단하기 위한 방화벽이 설치되어 있지 않으면 해커가 손쉽게 네트워크 주도권을 탈취하여 공격을 실행할 수 있습니다 . 그러나 방화벽이 설치되었더라도 (기본 방화벽을 사용하거나 엔터프라이즈급의 방화벽을 구매) 모든 공격의 완전한 예방과 차단이 보장되지 않습니다 .

* QNAP 은 상대적으로 위험이 낮은 VPN 서비스 포트를 사용한 인터넷 연결과 시스템 관리 , SMB, SSH 서비스와 같이 고위험 서비스 포트는 인터넷에서 손쉽게 액세스할 수 없게 조치할 것을 권장합니다 .



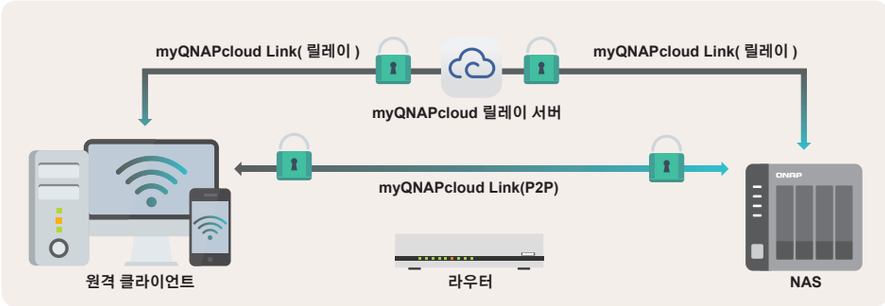
02 | 라우터 또는 QNAP NAS 에서 VPN 서버 기능 활성화

최신 라우터는 VPN 기능을 지원하고 (예 : QNAP QHora 및 QMiro 서비스 라우터), QNAP NAS 는 다중 VPN 서버기능도 지원합니다 . 활성화 및 올바른 설정이 구성된 경우 , 인터넷에서 VPN 서버까지 기기간 엔드포인트 VPN 암호화 연결을 사용해 인트라넷의 각 장치에 액세스할 수 있으며 이는 높은 수준의 보안을 제공합니다 .



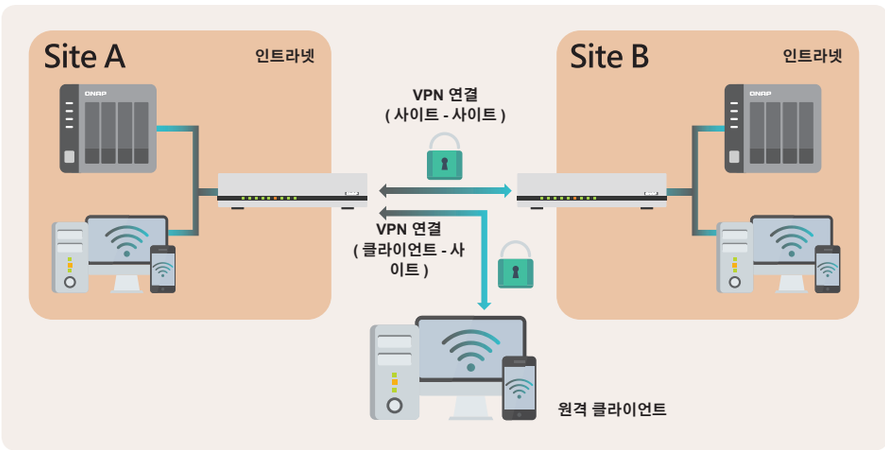
03 | myQNAPcloud Link 를 사용한 보안 연결

myQNAPcloud Link 기능을 사용하면 라우터의 설정 변경 없이도 NAS 를 인터넷에 연결할 수 있습니다 . myQNAPcloud Link 는 네트워크 환경에 따라 릴레이 서버 또는 P2P 기술을 통해 인터넷 연결을 설정합니다 . 모든 연결이 암호화되어 강력한 보안을 제공합니다 .



04 | SD-WAN 또는 Site-to-Site VPN 제품 사용

위에서 언급한 VPN 서버 기능 (Client-to-Site VPN) 과 달리 , SD-WAN 또는 Site-to-Site VPN 은 서로 다른 위치에 있는 둘 이상의 라우터 사이에 안전하게 암호화된 VPN 연결을 설정합니다 . 요약하면 , Site-to-Site VPN 네트워크상의 장치가 1 개의 동일한 인트라넷에 있는 것처럼 서로 연결될 수 있어 본사 / 지점과 같이 여러 장소를 관리하기에 적합합니다 . Client-to-Site VPN 기능은 불특정 장소에서 특정 NAS 에 액세스하기에 적합합니다 .



비교 표에 따라 적합한 연결 방법을 선택할 수 있습니다 . QNAP 는 사용자의 필요를 충족하는 여러 가지의 보안 연결 솔루션을 보유하고 있습니다 .

연결 방법	장점	단점	적합한 사용자
라우터 DMZ/ 포트포워딩 활성화 및 구성 UpnP 구성 UPnP	• 가장 빠른 연결	• 사이버 공격에 취약할 수 있음 • 0 일 취약성 공격에 대한 방어 기재 없음	• 관련 위험에 대한 명확한 이해 확보 • 네트워크 설정을 잘 알고 있음 • 중요 데이터의 여러 백업을 작성했음 • 재해 복구 계획이 있음
라우터에서 VPN 서버 활성화 *	• 상대적으로 설치가 간편함	• 로그인 오류 알림 , 자동 차단 및 방화벽 기능 없음 • 특정 VPN 프로토콜만 지원 • 라우터 하드웨어 성능에 따라 보안성능이 제한됨	• 네트워크 설정에 익숙하지 않음 • 전송 속도를 신경쓰지 않음
QNAP NAS 에서 VPN 서버 기능 활성화 *	• 여러 개의 다양한 VPN 프로토콜 지원 • NAS 방화벽 (QuFirewall) 과 호환 • 로그인 오류 알림 및 자동 차단 기능 지원	• 설정이 약간 더 복잡함 , 사용 설명서에 기준한 설정이 필요함	• 네트워크 설정을 잘 알고 있음 • 인터넷을 통한 다수의 파일에 자주 액세스해야 함
myQNAPcloud Link 보안 연결 사용	• 설치가 가장 쉬움 • 액세스 제어 지원 • NAS 가 인터넷에 노출될 필요가 없음	• 연결이 포트포워딩 적용보다 더 느림	• 네트워크 설정에 익숙하지 않음 • 인터넷에서 NAS 에 자주 액세스하지 않음 • WAN IP 주소를 획득할 수 없는 네트워크 환경
SD-WAN 또는 Site-to-Site VPN 제품 사용 *	• 설치 후 인트라넷 사용자가 어려움 없이 사용할 수 있음 • Client-to-Site VPN 도 지원함	• 추가 장비 필요	• 다중 지점 액세스 및 원격 백업 필요 • 부가가치 애플리케이션 필요

*** QNAP NAS 지원기능 및 프로토콜 :**
myQNAPcloud Link / VPN 서버 (L2TP/IPsec, OpenVPN, WireGuard, QBelt) /QuWAN SD-WAN

*** QNAP 라우터 지원 :**
QuWAN SD-WAN / VPN 서버 (L2TP/IPsec, OpenVPN, WireGuard, QBelt)

일반 가정용 /SOHO 라우터 기준

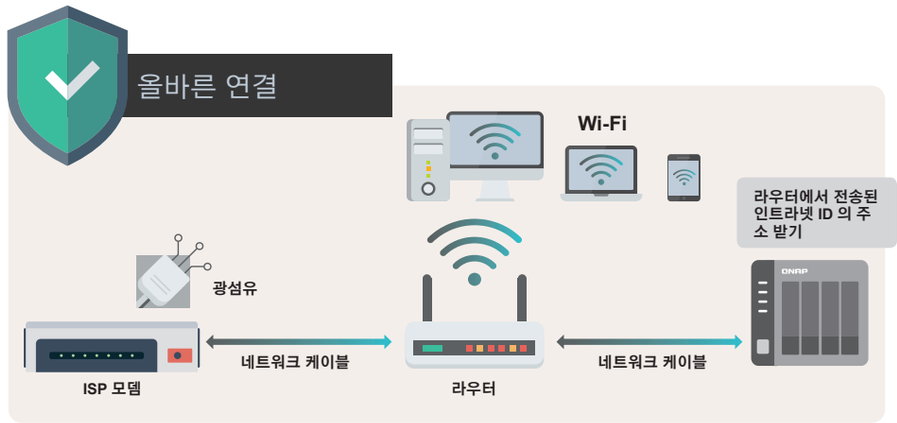
01

NAS 보안 설정 가이드

인터넷에 NAS 노출 방지

올바르게 NAS 연결

NAS 가 라우터에 연결되었는지 확인하십시오 . 올바른 설정을 적용하면 라우터가 NAS 의 인터넷 연결을 차단 및 NAS 의 직접적인 인터넷 노출을 방지하여 사이버 공격을 예방할 수 있습니다 .



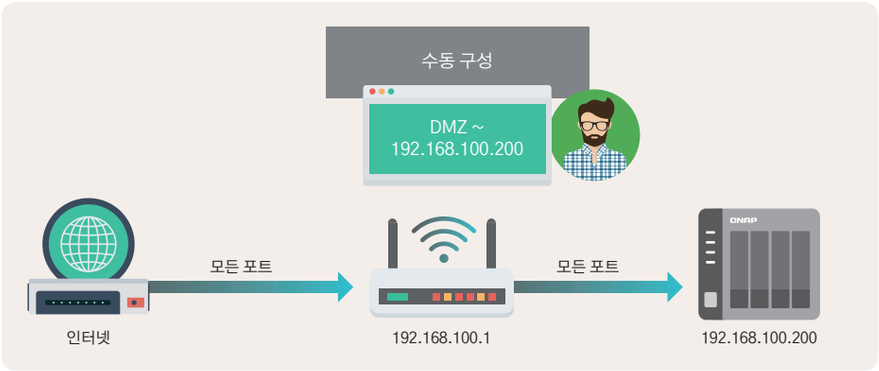
NAS 를 ISP 에서 제공한 모뎀에 직렬연결하면 WAN IP 주소는 NAS 에 직접 할당됩니다 . 이 경우 , (해커를 포함한) 누구나 인터넷을 통해 NAS 에 연결할 수 있고 공격과 침입을 시도할 수도 있습니다 .

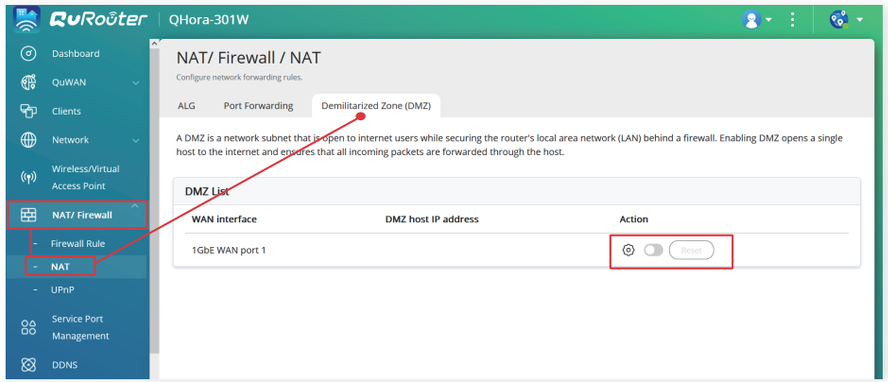
라우터 설정 확인

기술적인 이론기준으로는 누구도 인터넷에서 라우터 뒤에 있는 장치에 직접 연결할 수 없습니다 . 그러나 라우터 사용자가 "DMZ", " 포트포워딩 " 또는 "UPnP(Universal Plug and Play)" 를 활성화시키면 라우터가 설정된 규칙에 따라 패킷을 선택한 장치로 전달하므로 장치가 인터넷에 노출됩니다 . 필요하지 않으면 다음의 기능을 확인하고 비활성화되었는지 확인해야 합니다 .

01 | DMZ 설정 확인

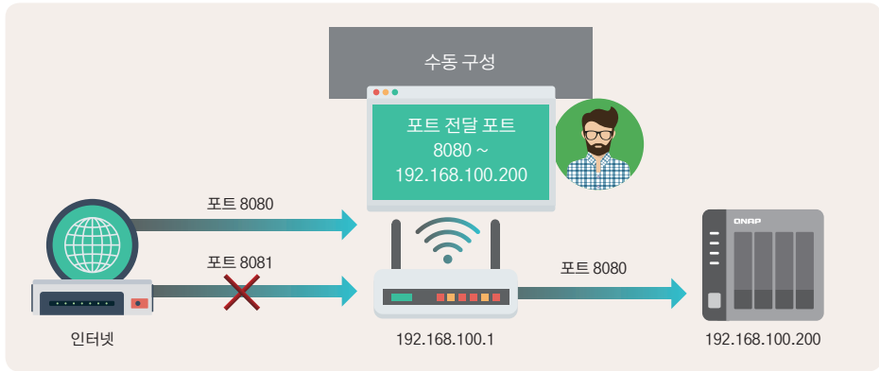
이 기능을 사용자가 활성화하면 라우터의 모든 서비스 포트가 인터넷에 직접 열립니다 . 즉 , 인터넷에 완전히 노출되게 됩니다 . 보안 위험을 줄이려면 이 기능을 반드시 비활성화하십시오 .

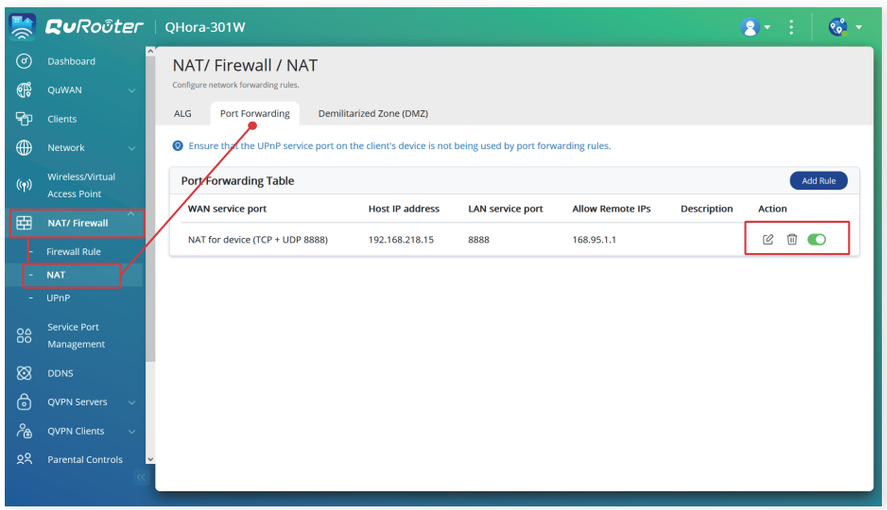




02 | 포트포워딩 확인

이 기능을 통해 라우터의 특정 서비스 포트를 인터넷에 열고 누구나 인터넷을 통해 내부망의 장치 및 관련 서비스에 액세스할 수 있게 됩니다 . 그러나 해커들도 인터넷으로부터 개방된 포트를 통해 해당 서비스에 접근 및 연결을 위한 공격을 실행할 수 있습니다 . 따라서 제일 먼저 라우터의 모든 포트포워딩 규칙을 비활성화한 다음 , NAS 보안 설정을 지정 및 완료하고 중요 데이터를 백업한 후에 일부 필수 NAS 서비스만 인터넷에 개방하는 것을 권장됩니다 .

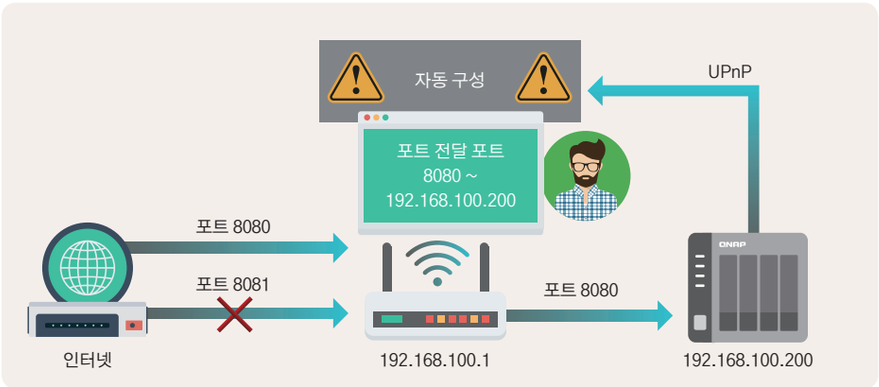


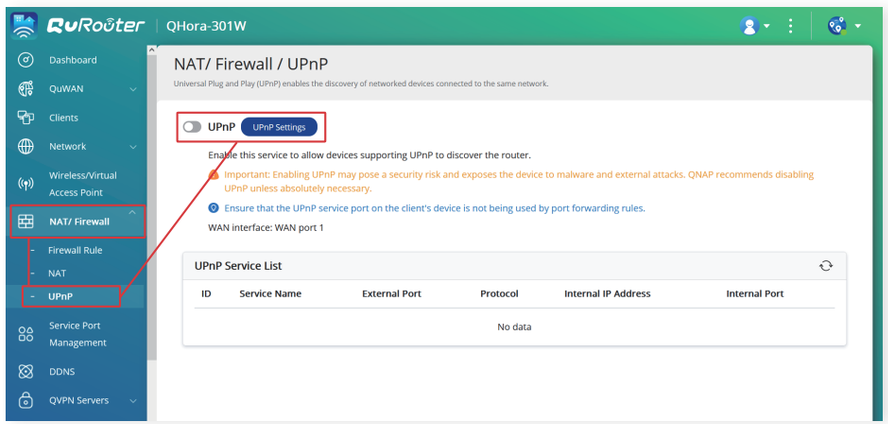


NAS 설정 확인

03 | UPnP(Universal Plug and Play) 확인

이 기능은 자동 포트포워딩과 같습니다 . 이 기능을 활성화하면 라우터가 자동으로 해당 프로토콜을 사용해 포트포워딩을 구성합니다 . 이 기능은 사용자가 알지 못하는 사이에 내부망의 기기와 모든 서비스를 인터넷에 노출시켜서 불특정 다수 또는 해커가 침입할 수 있기 때문에 심각한 보안 위험을 갖고 있는 비권장되는 기술입니다 . 따라서 보안 강화를 위해서는 이 기능을 반드시 비활성화해야 합니다 .





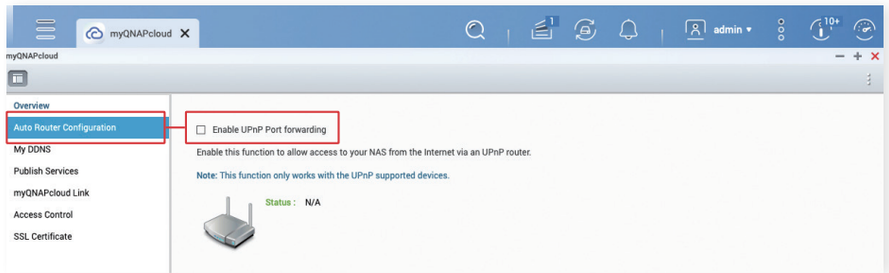
01 | 자동 라우터 구성 , UPnP 포트포워딩

일부 라우터는 UPnP 기능 비활성화를 지원하지 않기 때문에 NAS 에서도 " 자동 라우터 구성 " 설정을 확인하여 이 기능이 비활성화되었는지 확인하십시오 .

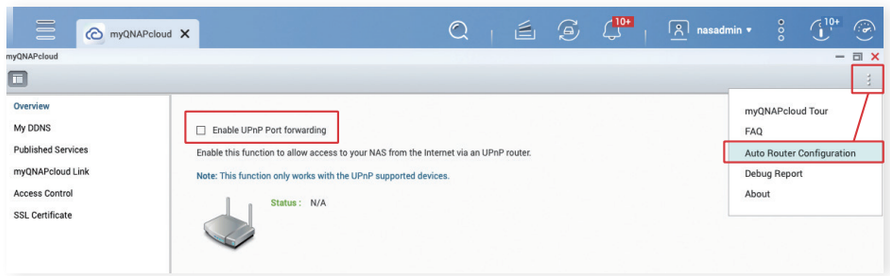
* **QTS 4.5.0 / QuTS hero h4.5.3 이후 버전부터는 이 기능이 기본적으로 비활성화되어 있습니다 .**

" 자동 라우터 구성 " 기능을 비활성화하려면 :

1. 관리자 계정을 사용하여 QTS / QuTS hero 웹 관리 인터페이스에 로그인합니다 .
2. 관리 인터페이스의 상단 왼쪽 모서리에 있는 메뉴를 열고 "myQNAPcloud" 를 클릭합니다 .
3. **QTS 5.0.0 / QuTS hero h5.0.0** 또는 **이전 버전 :** 메뉴의 왼쪽에서 " 자동 라우터 구성 " 을 클릭합니다 .



QTS 5.0.1 / QuTS hero h5.0.1 또는 **이후 버전 :** 상단 오른쪽 모서리에서 메뉴 아이콘을 클릭하고 " 자동 라우터 구성 " 을 선택합니다 .



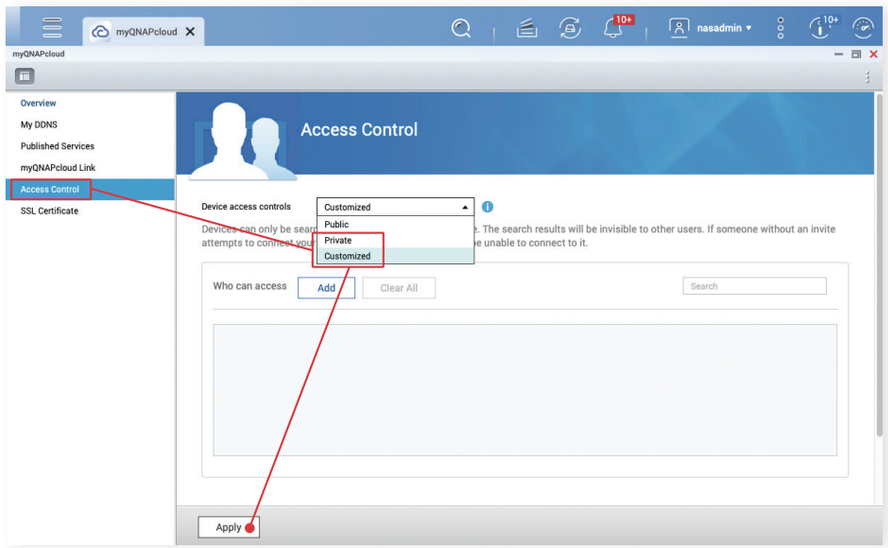
4. " 자동 라우터 구성 " 설정에서 "UPnP 포트포워딩 활성화 " 의 선택을 취소하고 " 적용 " 을 클릭합니다 .

02 | myQNAPcloud Link 액세스 제어

myQNAPcloud Link 는 QNAP 에서 제공하는 보안 연결 클라우드 서비스입니다 . 사용자가 지정한 myQNAPcloud 장치 이름을 통해 QNAP NAS 에 엑세스할 수 있습니다 . myQNAPcloud Link 는 액세스 제어 설정을 제공합니다 . 액세스 제어가 " 공개 " 로 설정된 경우 , 장치 이름을 알고 있는 사람이면 누구나 myQNAPcloud Link 를 사용해 사용자의 NAS 에 연결할 수 있습니다 . 따라서 액세스 제어를 " 비공개 " 또는 " 사용자 지정 " 으로 설정할 것을 권장합니다 . 두 모드에서는 사용자가 반드시 허용된 액세스 목록에서 QNAP ID 에 로그인해야 myQNAPcloud Link 를 사용해 안전하게 클라우드 서비스에 연결할 수 있습니다 .

* **Q TS 4.5.0 / Qu TS hero h4.5.3(이상) 에서 기본 설정은 " 사용자 지정 " 입니다 .**

1. 관리자 계정을 사용하여 QTS / QuTS hero 웹 관리 인터페이스에 로그인합니다 .
2. 관리 인터페이스의 상단 왼쪽 모서리에 있는 메뉴를 클릭하고 "myQNAPcloud" 를 클릭합니다 .
3. 왼쪽 메뉴에서 " 액세스 제어 " 를 클릭합니다 .
4. " 액세스 제어 " 설정 페이지에서 " 장치 액세스 제어 " 를 " 비공개 " 또는 " 사용자 지정 " 으로 설정한 다음 , " 적용 " 을 클릭합니다 .



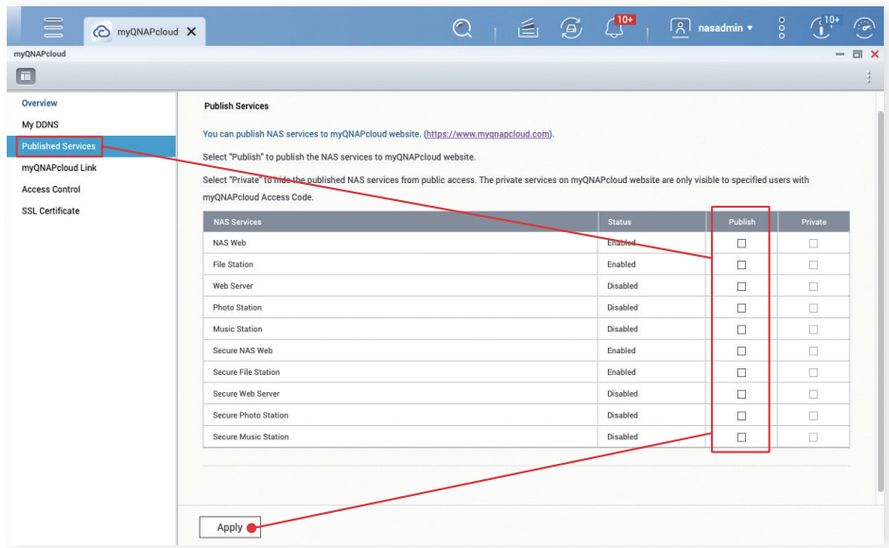
03 | 게시된 서비스

게시된 서비스를 통해 사용자가 myQNAPcloud 웹사이트에 있는 관련 기능을 보다 쉽게 사용할 수 있지만 , 동시에 보안 위험도 증가하게 됩니다 . 이 기능의 사용이 필요하지 않으면 보안을 개선하기 위해 비활성화하는 것이 권장됩니다 .

* **QTS 4.5.0 / QuTS hero h4.5.3 이후 버전부터는 이 기능이 기본적으로 비활성화 되어 있습니다 .**

" 게시된 서비스 " 기능 :

1. 관리자 계정을 사용하여 QTS / QuTS hero 웹 관리 인터페이스에 로그인합니다 .
2. 관리 인터페이스의 상단 왼쪽 모서리에 있는 메뉴를 클릭하고 "myQNAPcloud" 를 클릭합니다 .
3. 왼쪽 메뉴에서 " 게시된 서비스 " 를 클릭합니다 .
4. " 게시 " 필드에서 모든 항목의 선택을 취소하고 " 적용 " 을 클릭합니다 .



네트워크 설정 체크리스트

하드웨어 관련

☐ NAS 가 라우터 뒤에 연결되어 있습니다 .

☐ NAS 가 인트라넷 IP 주소를 획득합니다 .

라우터

☐ 라우터 "DMZ" 기능을 비활성화합니다 .

☐ 라우터 " 포트포워딩 " 규칙을 비활성화합니다 .

☐ 라우터 "UPnP" 기능을 비활성화합니다 .

NAS

☐ NAS " 자동 라우터 구성 UPnP 포트포워딩 " 기능을 비활성화합니다 .

☐ NAS "myQNAPcloud Link 액세스 제어 " 를 " 비공개 " 또는 " 사용자 지정 " 으로 설정합니다 .

☐ " 게시된 서비스 " 기능을 비활성화합니다 .

위의 설정을 확인하고 적용한 후에는 QNAP NAS 가 인터넷에 노출되지 않고 해커의 공격을 당할 위험도 크게 감소됩니다 . 나머지 설정도 확인 및 적용해서 QNAP NAS 의 보안을 강화하십시오 .

인터넷을 통해 NAS 에 액세스해야 할 경우 , 다음의 안전한 3 가지 대안을 고려할 수 있습니다 .

myQNAPcloud Link

자세한 정보

QVPN Service

자세한 정보

QuWAN SD-WAN

자세한 정보

02

NAS 보안 설정 가이드

NAS 보안 설정

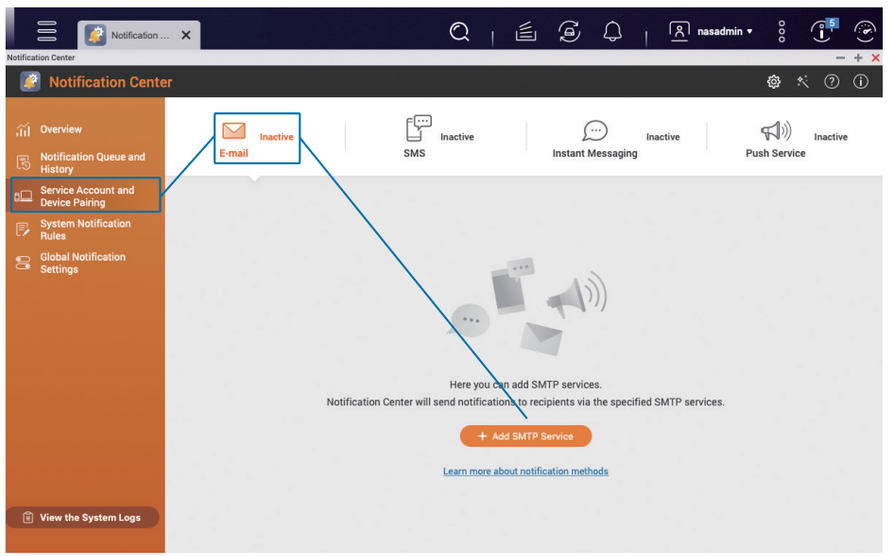
시스템 알림 설정

내장된 알림 센터 (Notification Center) 는 설정에 따라 푸시 알림을 보낼 수 있어 사용자가 NAS 상태를 계속해서 조회하고 비정상적인 활동이 감지되는 즉시 대응할 수 있습니다 .

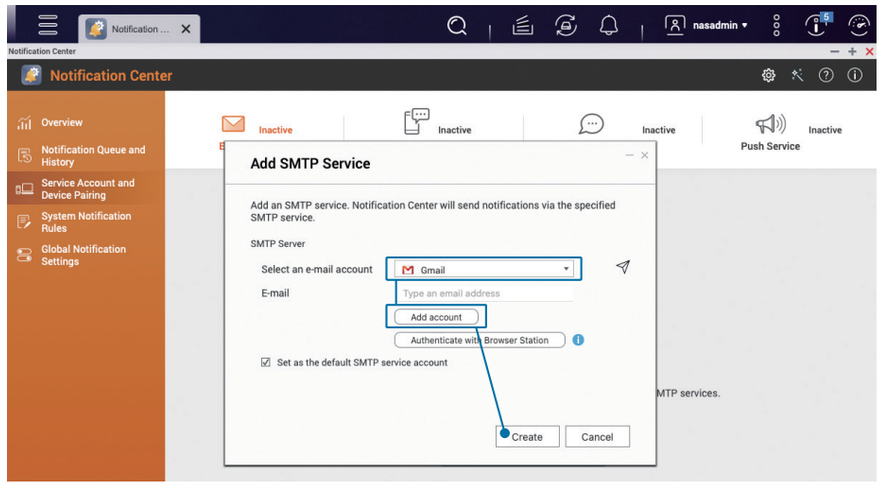
다음의 튜토리얼은 이메일 보내는 2 개의 기본 규칙의 생성 방법을 안내하여 " 경고 알림 " 및 " 펌웨어 업데이트 " 를 설정하고 추가 규칙을 생성하는 것을 안내합니다 .

01 | " 이메일 " 알림 방법 추가

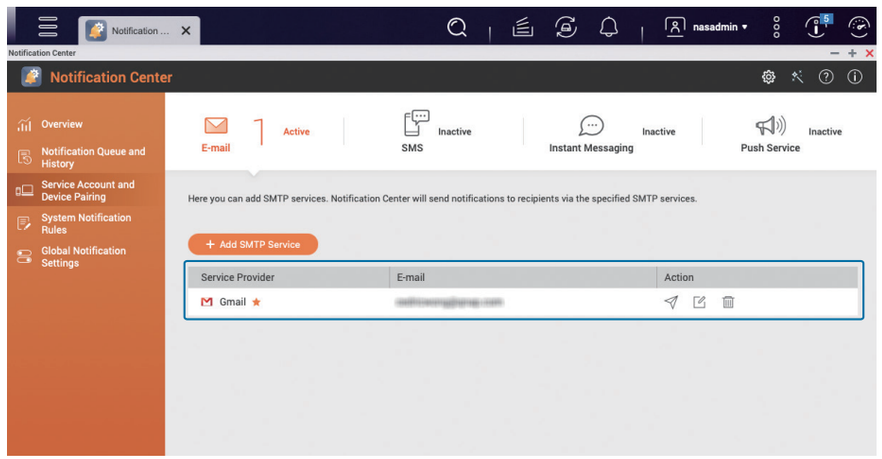
" 알림 센터 " 를 열고 왼쪽 메뉴에서 " 서비스 계정 및 장치 페어링 " 을 클릭한 다음 , " 이메일 " 을 선택하고 "SMTP 서비스 추가 " 를 클릭합니다 .



이메일 계정 (다음 예시에서는 Gmail 을 사용) 을 선택하고 " 계정 추가 " 를 클릭한 다음 , 지침을 따라 Gmail 인증 프로세스를 완료하고 인증이 완료된 후 " 만들기 " 를 클릭합니다 .

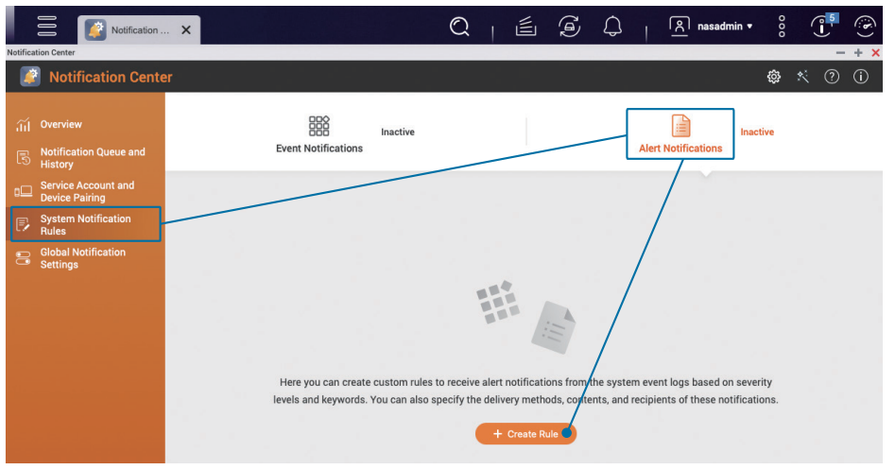


⇩⇩생성되면 방금 추가한 이메일 계정을 목록에서 볼 수 있습니다 .

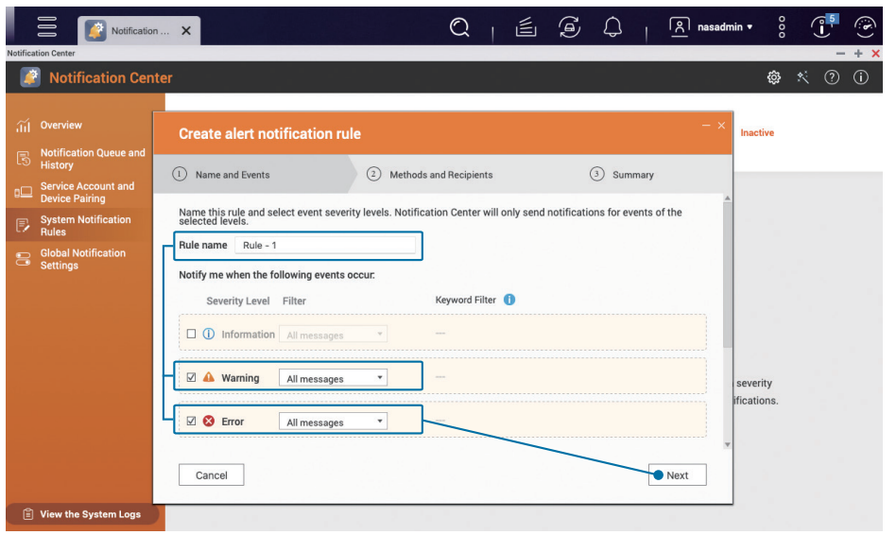


02 | " 경고 알림 " 설정

" 알림 센터 " 의 왼쪽 메뉴에서 " 시스템 알림 규칙 " 을 클릭하고 " 경고 알림 " 을 선택한 다음 , " 규칙 만들기 " 를 클릭합니다 .

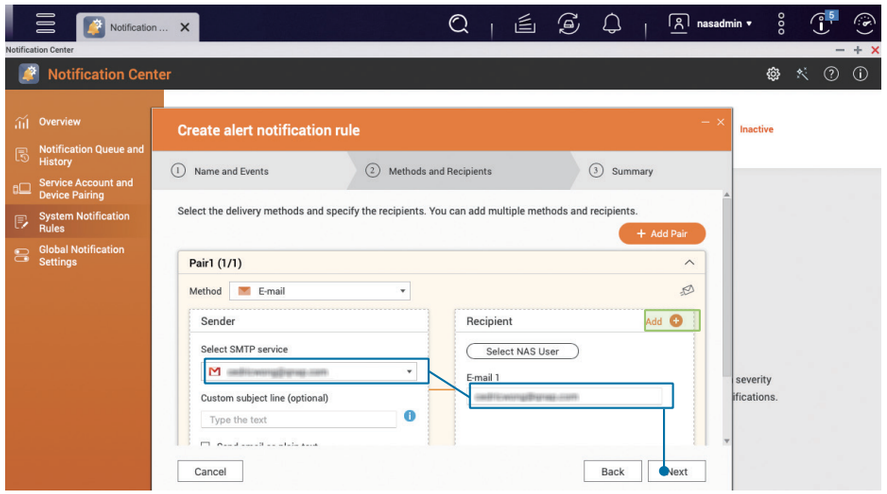


필요에 따라 " 규칙 이름 " 을 수정하고 " 경고 " 및 " 오류 " 의 두 가지 심각도 레벨을 선택한 후 , " 다음 " 을 클릭합니다 .

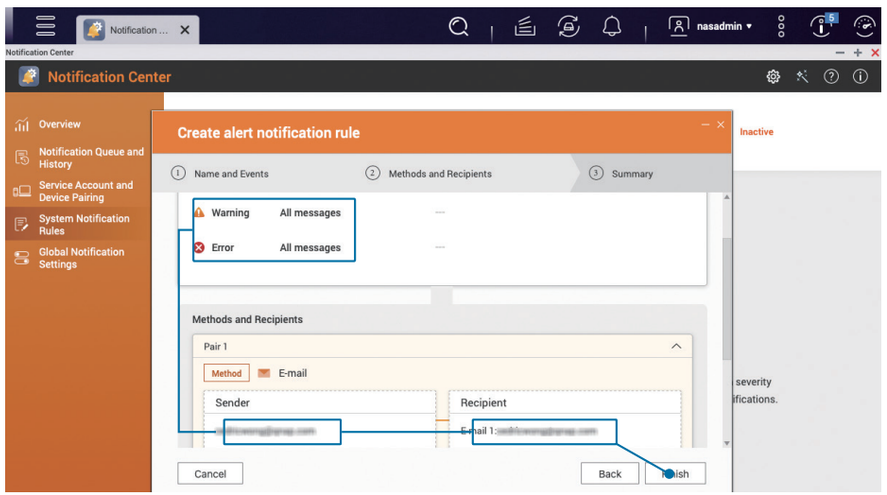


발신 방법 , 수신자를 설정하고 페어링에서 방금 " 발신자 " 로 추가한 이메일 계정을 선택한 다음 , " 수신자 " 의 " 이메일 주소 " 를 입력하고 " 다음 " 을 클릭합니다 .

필요하면 " 수신자 " 옆에 있는 " 추가 " 를 클릭해서 여러 명의 수신자를 입력할 수 있습니다 . 또는 " 페어링을 추가 " 에서 동시에 여러 방법으로 알림을 보낼 수도 있습니다 .

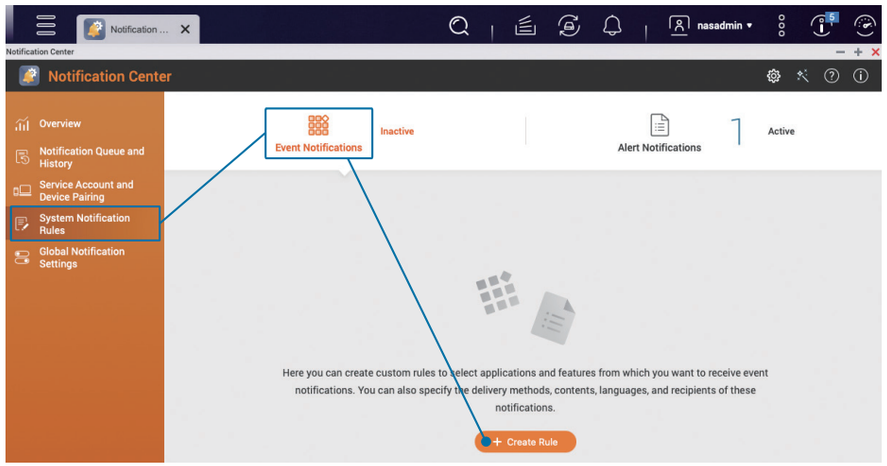


설정이 올바른지 확인한 후 " 마침 " 을 클릭합니다 . 그러면 " 경고 알림 " 설정이 완료됩니다 .

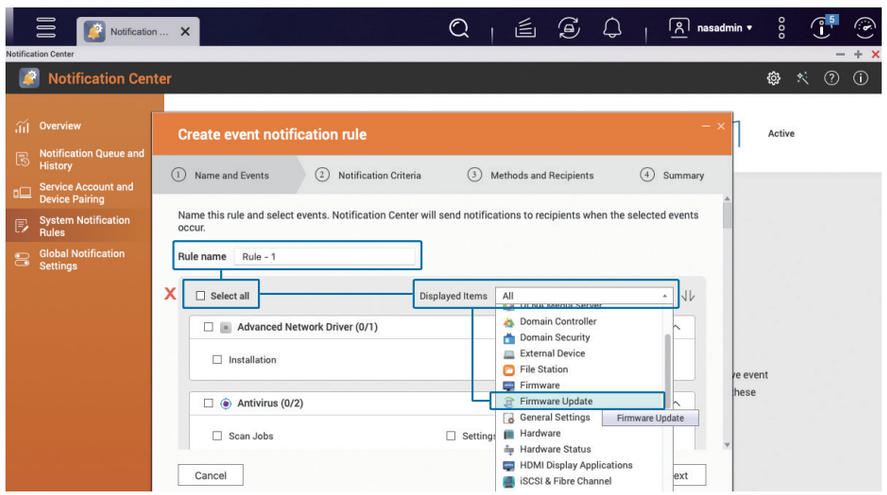


03 | " 펌웨어 업데이트 " 알림 구성

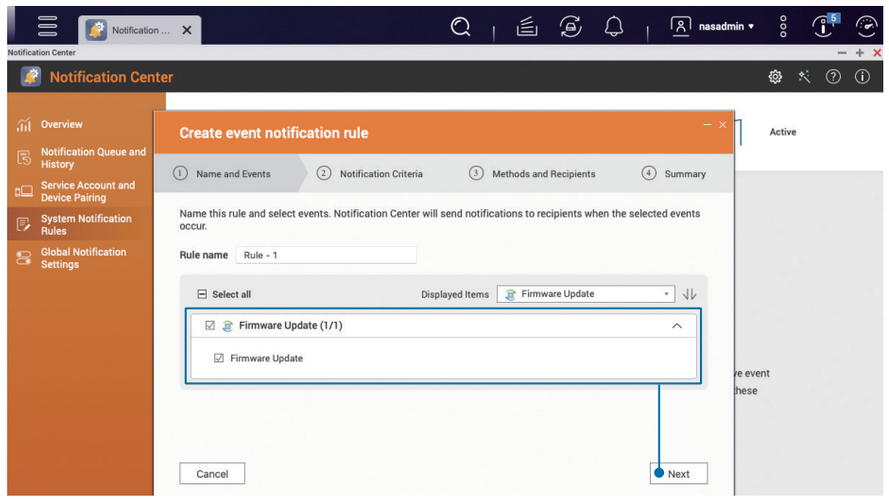
" 알림 센터 " 왼쪽 메뉴에서 " 시스템 알림 규칙 " 을 클릭하고 " 이벤트 알림 " 을 선택한 다음 , " 규칙 만들기 " 를 클릭합니다 .



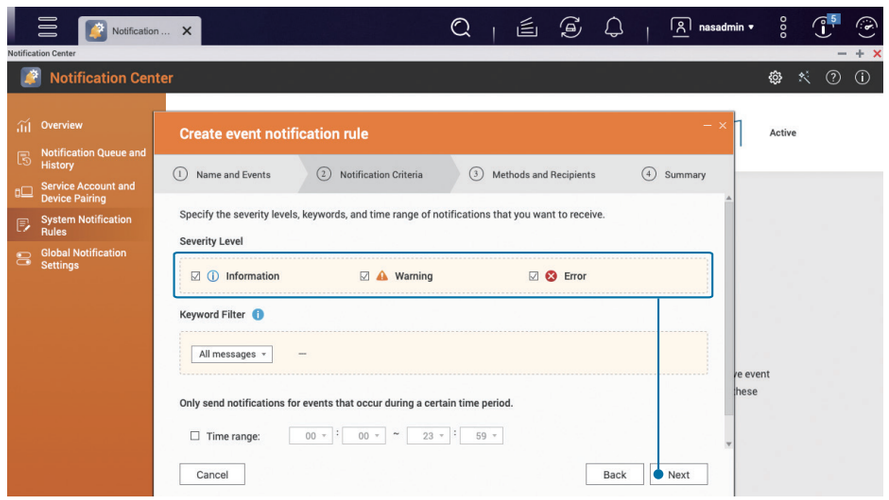
필요에 따라 " 규칙 이름 " 을 수정하고 " 모두 선택 " 의 선택을 취소한 다음 , 왼쪽의 " 표시된 항목 " 에서 " 펌웨어 업데이트 " 를 선택하고 아래의 " 펌웨어 업데이트 " 옵션을 선택합니다 .



" 펌웨어 업데이트 " 옵션을 선택하고 " 다음 " 을 클릭합니다 .



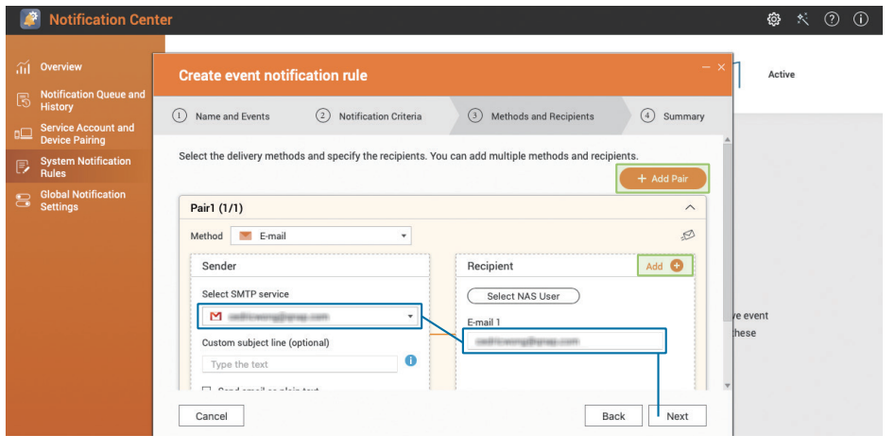
" 정보 ", " 경고 ", " 오류 " 를 포함한 모든 심각도 레벨을 선택하고 " 다음 " 을 클릭합니다 .



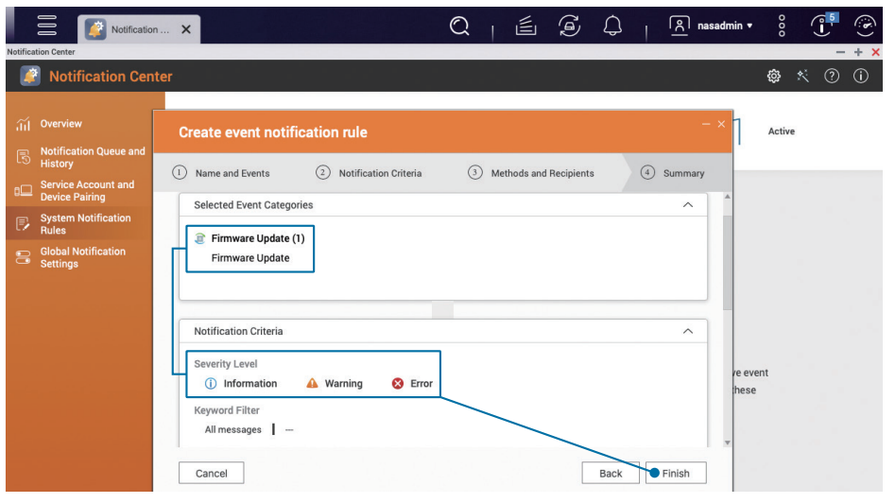
펌웨어 (QTS / QuTS hero) 자동 업데이트 활성화

발신 방법과 수신자를 설정합니다 . 현재 " 이메일 " 알림만 설정되었기 때문에 페어링에서 방금 " 발신자 " 로 추가한 이메일 계정을 선택한 다음 , " 수신자 " 의 " 이메일 주소 " 를 입력하고 " 다음 " 을 클릭합니다 .

필요하면 " 수신자 " 옆에 있는 " 추가 " 를 클릭해서 여러 명의 수신자를 입력할 수 있습니다 . 또는 " 페어링을 추가 " 애서 동시에 여러 방법으로 알림을 보낼 수도 있습니다 .

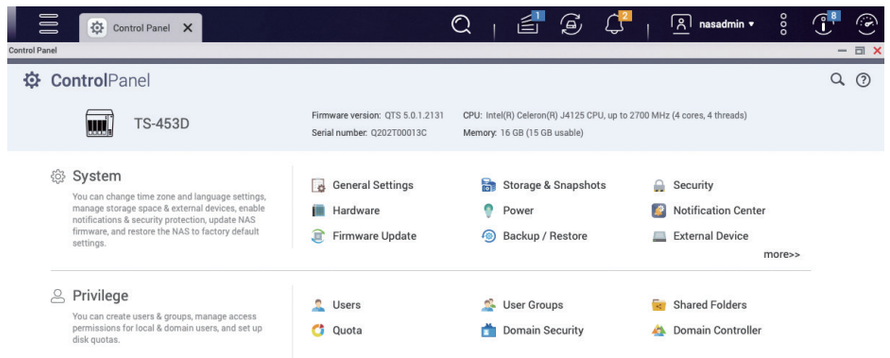


설정이 올바른지 확인한 후 " 마침 " 을 클릭하여 " 펌웨어 업데이트 " 설정을 완료합니다 .



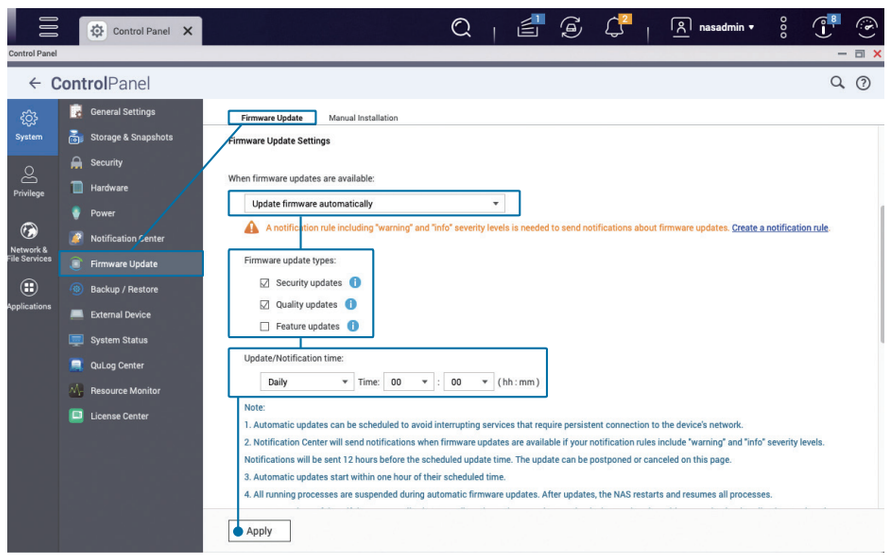
자동 업데이트 기능을 통해 새로운 기능 , 버그 수정 , 취약성에 대한 업데이트를 보다 손쉽게 설치할 수 있습니다 .

" 제어판 " 을 열고 " 펌웨어 업데이트 " 를 클릭합니다 .



" 펌웨어 업데이트 설정 " 에서 " 자동으로 펌웨어 업데이트 " 를 선택하고 " 보안 업데이트 " 및 " 품질 업데이트 " 를 선택합니다 . " 업데이트 / 알림 시간 " 의 경우 , "00 : 00" 과 같이 한산한 시간을 설정하는 것이 권장됩니다 . 적용을 클릭합니다 .

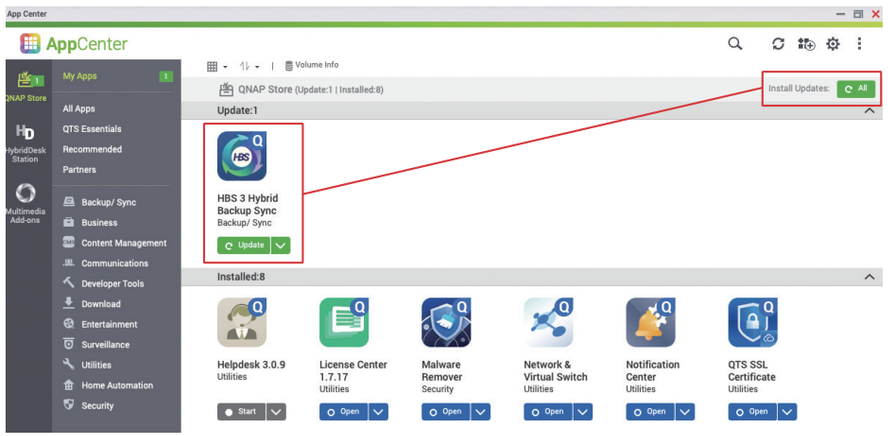
*** QTS 5.0.0 / QuTS hero h5.0.0(이전) 의 경우 , " 자동 업데이트 " 페이지에서 " 권장 버전 " 을 선택하십시오 .**



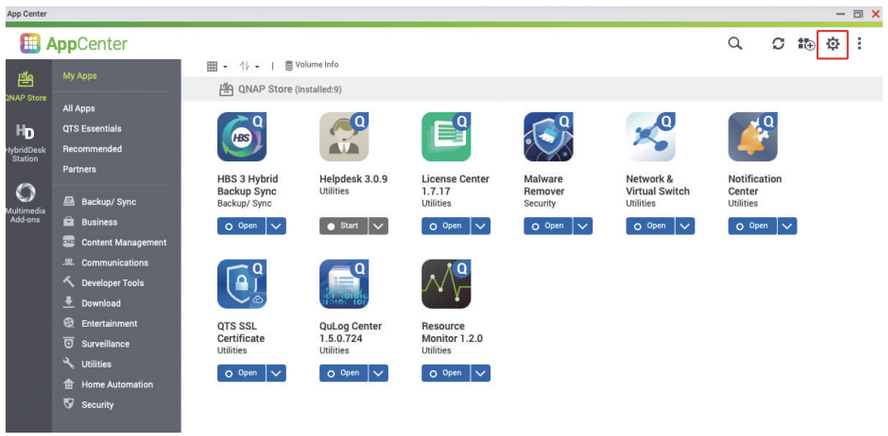
앱 업데이트 설정

App Center 는 QNAP NAS 에 다양한 앱을 제공하여 기능을 추가하고 , 설치된 앱을 위한 보안과 성능 업데이트를 통해 더 나은 사용자 경험을 제공합니다 .

"App Center" 업데이트 카테고리에 업데이트가 가능한 앱들이 표기됩니다 . 해당하는 경우 , 상단 오른쪽의 " 모두 All " 버튼을 클릭하여 모든 앱을 업데이트합니다 .

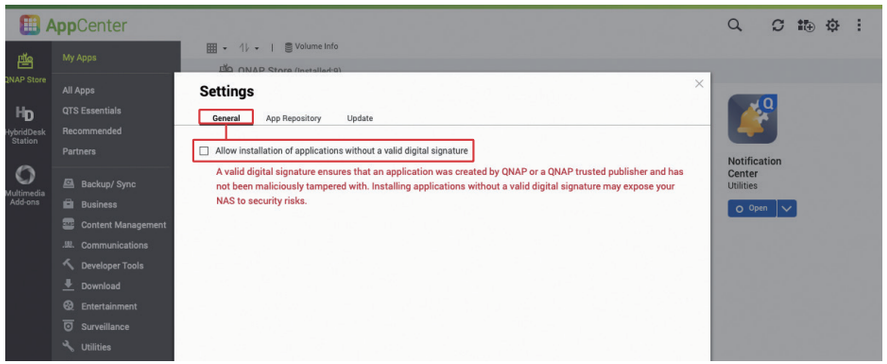


업데이트가 완료된 후 상단 오른쪽 모서리에서 " 설정 " 아이콘을 클릭하여 App Center 의 설정 페이지에 들어갑니다 .



QNAP 또는 QNAP 협업 개발자가 배포하는 앱은 정품임을 보장하기 위해 앱에 디지털 서명을 포함합니다 . 보안을 향상시키기 위해서 " 유효한 디지털 서명 없는 애플리케이션 설치 허용 " 의 선택을 취소하는 것이 권장됩니다 .

* **이 옵션은 기본적으로 비활성화되어 있어 , 유효한 디지털 서명 없는 앱의 설치가 불가능합니다 .**

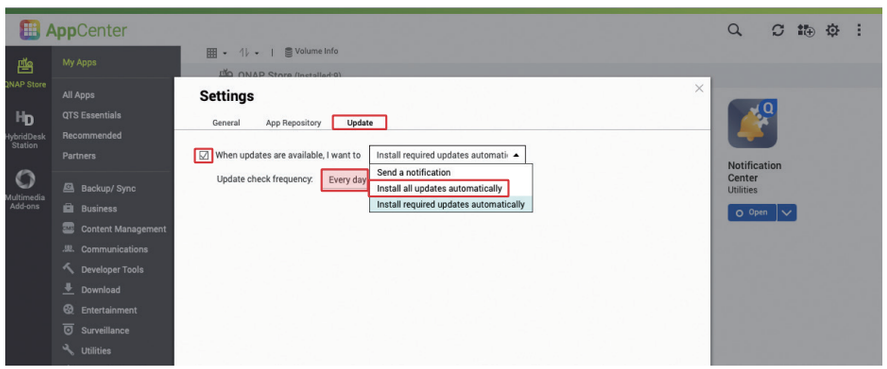


업데이트 탭을 클릭하고 , 특별한 사용조건이 없는 경우 " 모든 업데이트 자동 설치 " 를 선택하고 빈도를 " 매일로 설정하는 것을 권장합니다 . 적용을 클릭하여 설정을 완료합니다 .

⇨ " 필수 업데이트 " 는 주로 앱과 펌웨어 성능개선을 위해 사용되며 , “주요 취약성 업데이트 " 도 포함됩니다 .

⇨ " 모든 업데이트 " 에는 모든 기능 개선 사항 , 버그 수정 , 모든 취약성 개선 패치가 포함됩니다 . 업데이트가 보다 자주 있습니다 .

* **기본값은 " 모든 업데이트 자동 설치 " 입니다 .**

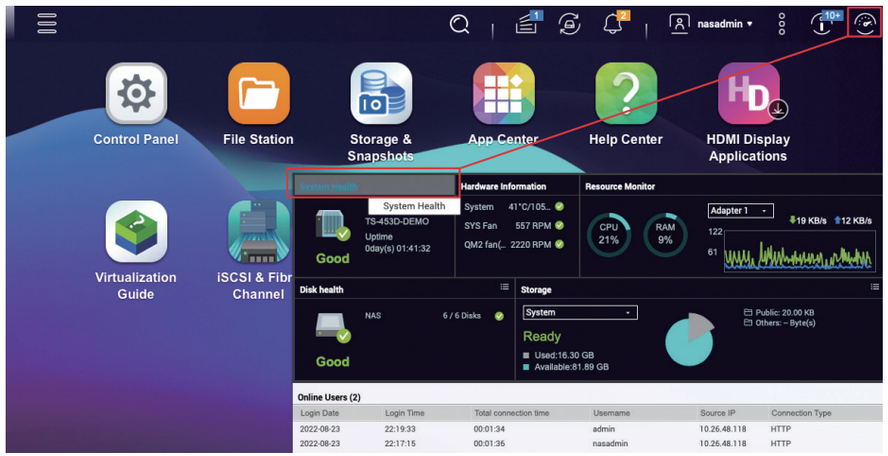


불필요한 기능 비활성화 또는 제거

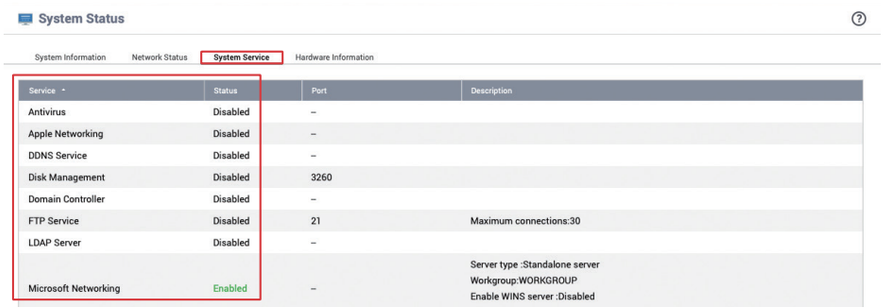
QNAP NAS 는 다양한 기능과 앱을 제공하지만 , 활성화된 기능이 많을수록 보안성 강화에 대한 관리가 요구됩니다 . 보안을 향상시키고 시스템의 원활한 사용을 위해 주기적으로 불필요한 기능을 확인하여 비활성화 (또는 제거) 를 통해 앱 관리하는 것을 권고합니다 .

* 제품 보안을 향상시키기 위해 **QTS 5.0.0 / QuTS hero h5.0.0** 버전부터는 시스템 초기화 시 필수가 아닌 기능이 기본적으로 비활성화되며 , **App Center** 가 불필요한 앱을 기본적으로 설치하지 않습니다 . **QTS 5.0.0 / QuTS hero h5.0.0** 으로 업데이트하기 전에 시스템이 초기화된 경우 , 어떤 앱이 설치되었는지 확인하십시오 .

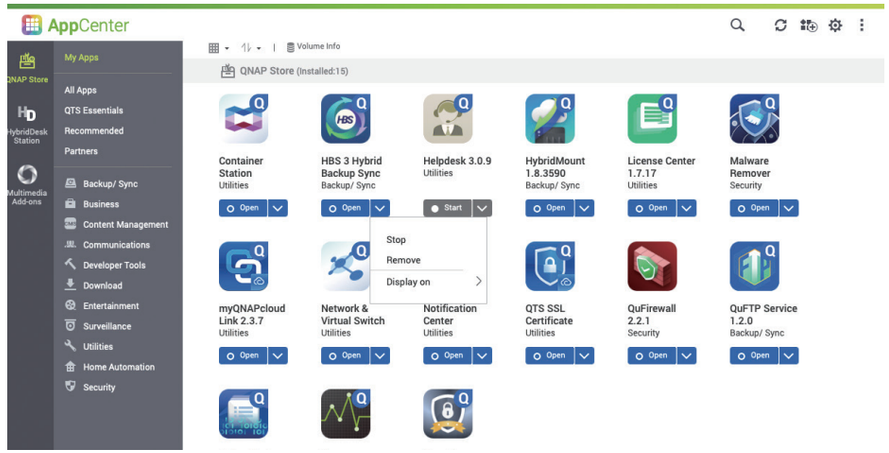
상단 오른쪽 모서리에서 " " 버튼을 클릭하여 시스템 " 대시보드 " 를 열고 , " 시스템 상태 " 를 클릭하여 " 시스템 상태 " 창을 엽니다 .



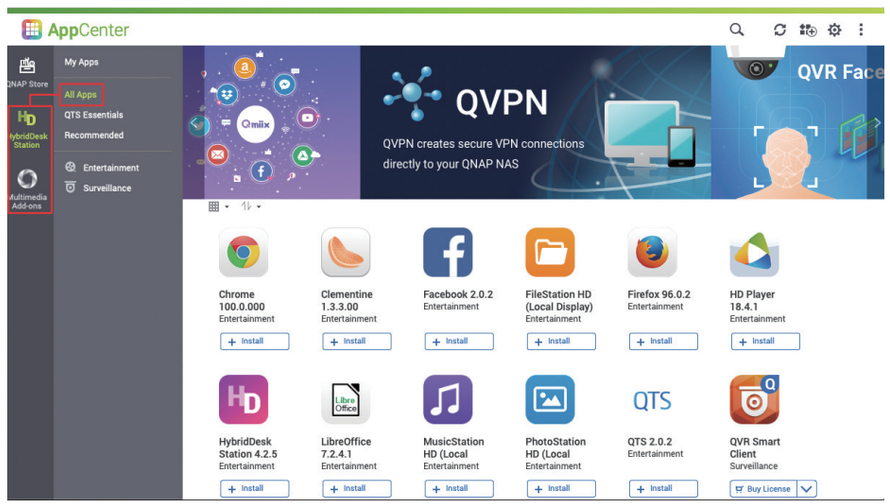
" 시스템 서비스 " 를 클릭하여 활성화된 시스템 기능을 확인합니다 . 제어판으로 가서 불필요한 시스템 기능을 비활성화할 수 있습니다 .



시스템 내장 기능 이외에도 App Center 에 설치된 항목을 확인해야 합니다 .



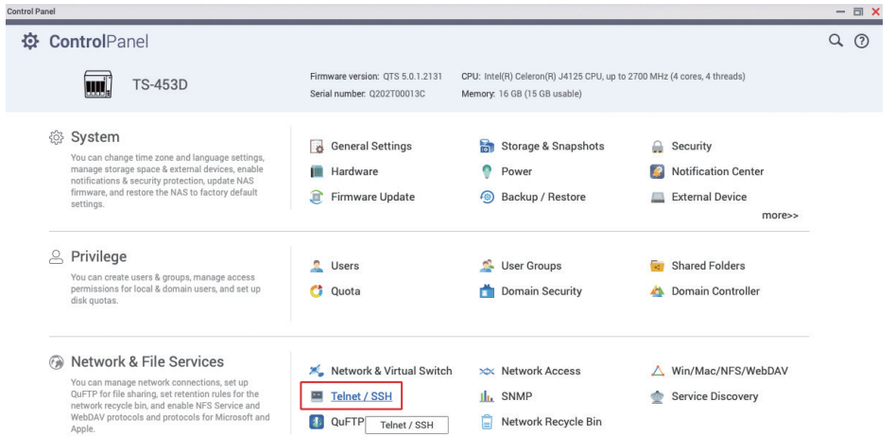
맨 왼쪽에서 "HybridDesk Station" 및 " 멀티미디어 추가 기능 " 을 클릭하여 해당하는 앱의 상태를 확인합니다 .



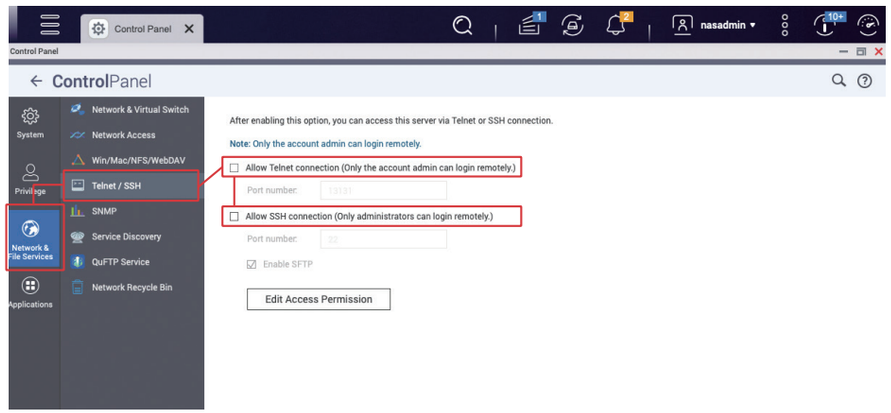
텔넷 / SSH 비활성화

이들 항목을 사용하지 않는 한 , 텔넷과 SSH 를 비활성화할 것을 강력히 권고합니다 . 이 두 기능은 일반적으로 QNAP 고객 서비스 또는 전문 IT 담당자가 시스템을 유지관리하기 위해서 사용합니다 . 일반 사용자들은 이 기능이 필요하지 않으므로 비활성화를 반드시 해야합니다 .

" 제어판 " 을 열고 " 텔넷 / SSH" 를 클릭합니다 .



" 텔넷 연결 허용 " 및 "SSH 연결 허용 " 의 선택을 취소하고 " 적용 " 을 클릭합니다 .

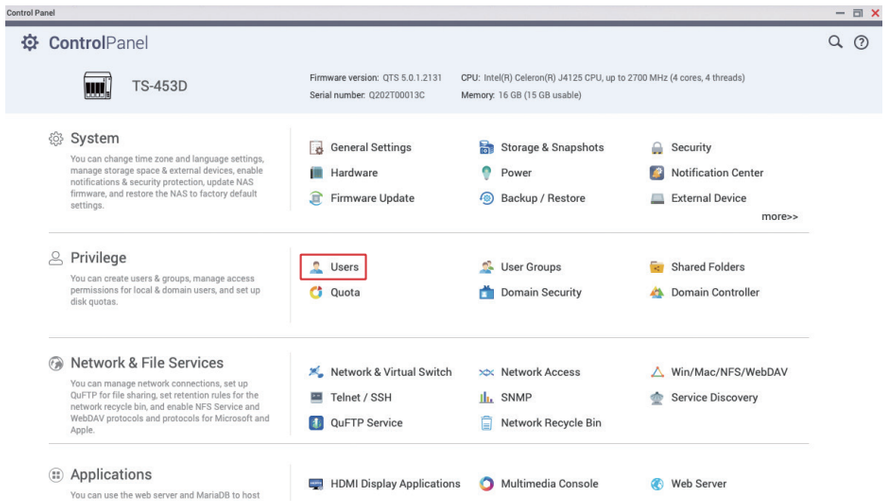


시스템 계정 보안 강화

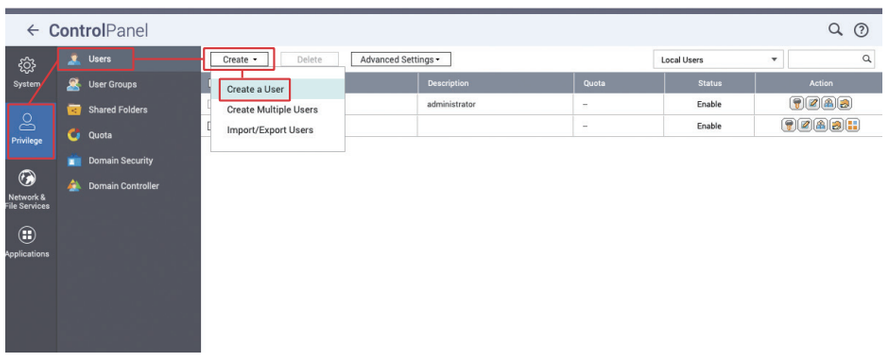
기본 관리자 계정 "admin" 비활성화

브루트 포스 공격으로 암호 크래킹을 사용하는 해커들은 일반적으로 기본 관리자 계정 "admin" 을 타겟으로 합니다 . QTS 4.5.4 / QuTS hero h4.5.4(또는 이전 버전) 를 사용해 시스템이 초기화된 경우 , 기본 관리자 계정 "admin" 이 활성 상태가 됩니다 . 다음의 단계를 따라 새로운 관리자 계정을 생성하고 "admin" 계정을 비활성화합니다 .

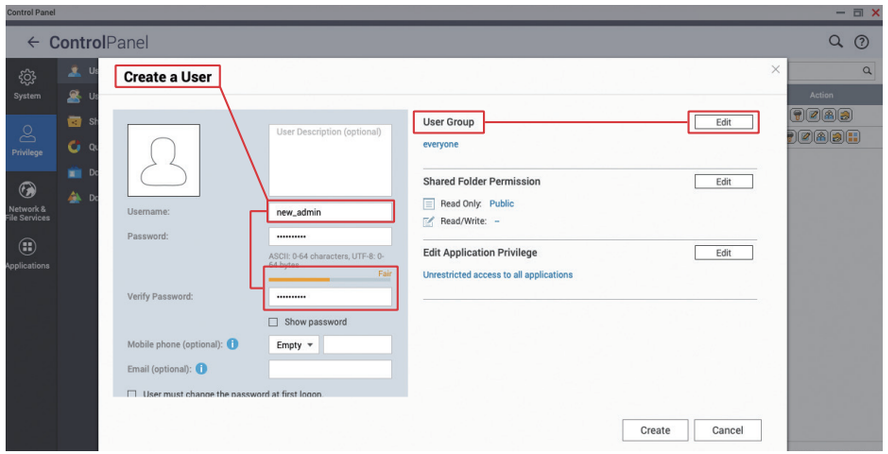
" 제어판 " 을 열고 " 사용자 " 를 클릭합니다 .



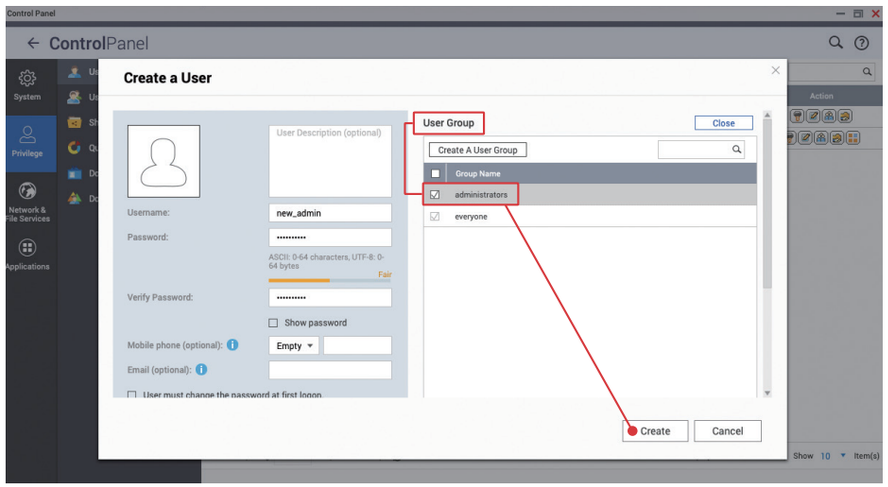
" 만들기 " > " 사용자 만들기 " 를 클릭합니다 .



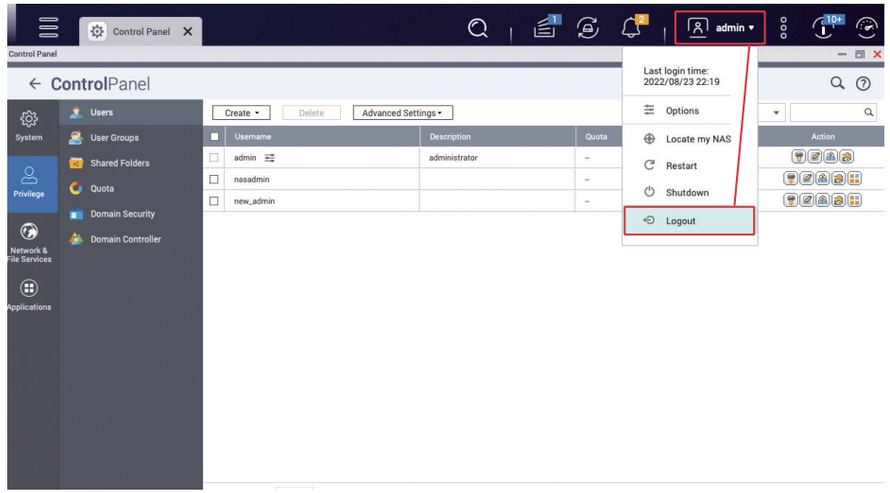
관리자 계정의 사용자 이름을 입력하고 (예 : "new_admin"), 강력한 암호를 설정합니다 .



" 사용자 그룹 " 섹션에서 " 편집 " 을 클릭하고 " 관리자 " 그룹을 선택한 다음 , " 만들기 " 를 클릭하여 새로운 사용자를 추가합니다 .



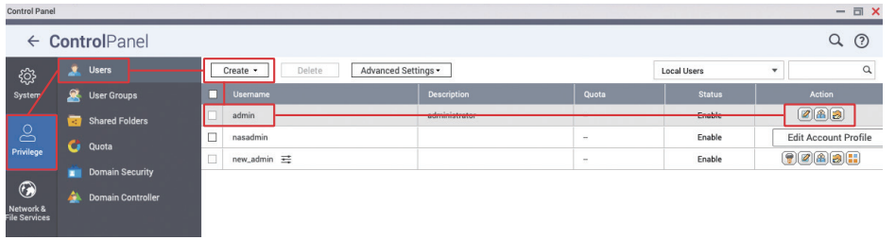
상단에서 "admin" 을 클릭하고 메뉴를 연 다음 , " 로그아웃 " 을 클릭하여 QTS 웹 관리 인터페이스에서 로그아웃합니다 .



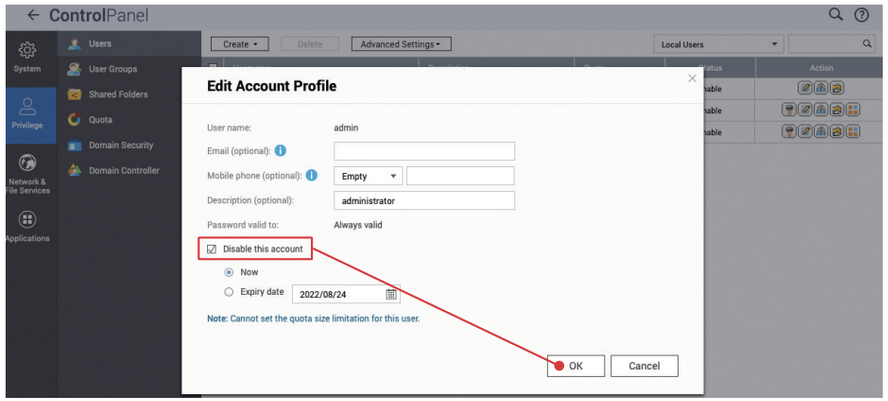
방금 만든 " 관리자 계정 " 을 사용하여 QTS 웹 관리 인터페이스에 로그인합니다 .

암호 정책 설정

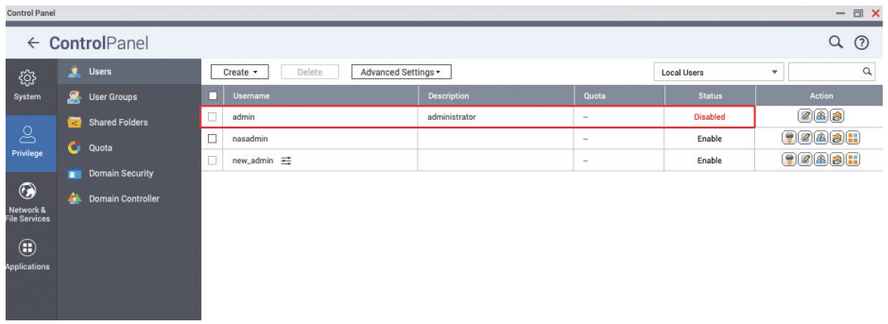
" 제어판 " 을 다시 열고 "admin" 행에서 " 사용자 " 를 클릭한 다음 , " 계정 프로필 편집 " 을 클릭합니다 .



" 이 계정 비활성화 " 를 선택하고 " 확인 " 을 클릭하여 완료합니다 .

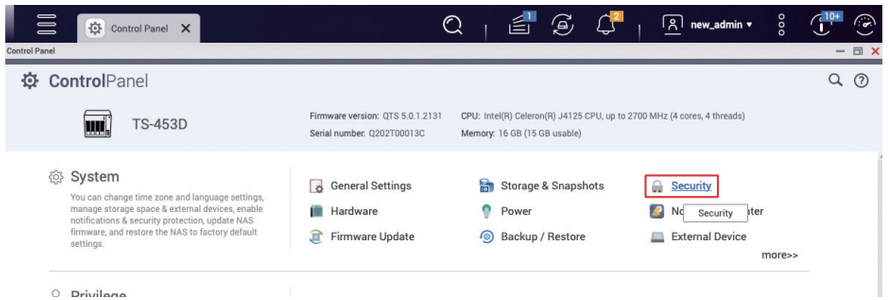


완료하면 "admin" 상태가 " 비활성화됨 " 인 것을 확인할 수 있습니다 .

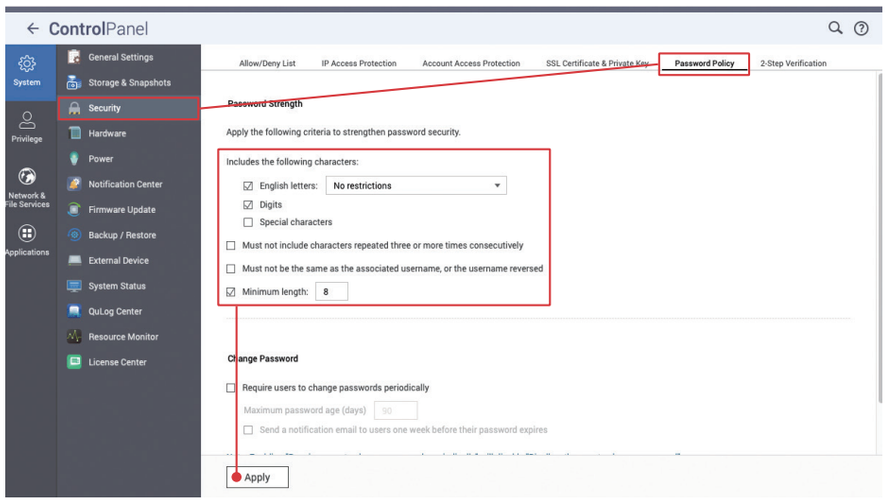


기본 관리자 계정 "admin" 을 비활성화하는 것 이외에 , 모든 계정에 강력한 암호가 설정되었는지도 확인해야 합니다 . " 액세스 보호 " 를 사용하면 악성 로그인 시도를 차단하는 데 도움이 될 수 있습니다 . 보안 향상을 위해서 모든 계정에 대해 "2 단계 인증 (2SV)" 을 실시하면 암호 크래킹과 악성 로그인을 방지할 수 있습니다 .

" 제어판 " 을 열고 " 보안 설정 " 을 클릭합니다 .



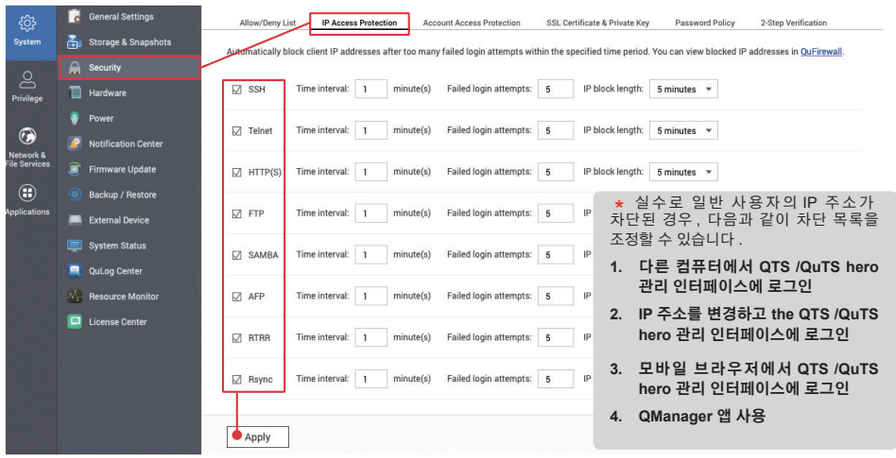
" 암호 정책 " 을 클릭하고 설정 페이지로 들어갑니다 . QTS 5.0.0 / QuTS hero h5.0.0(또는 이후 버전) 을 사용해 시스템이 초기화된 경우 , 기본 암호 정책이 기본적으로 활성화되어 있습니다 . 필요에 따라 강력한 암호 조건추가를 권장합니다 . 암호에 " 대소문자 ", " 숫자 " 가 포함되도록 설정할 수 있고 , 암호 길이는 최소 "10 자 " 이상이 권장됩니다 . 완료 후 " 적용 " 을 클릭합니다 .



액세스 보호 활성화 (IP / 계정)

"IP 액세스 보호 " 및 " 계정 액세스 보호 " 기능으로 브루트 포스 공격으로 암호가 해킹되는 것을 효과적으로 막을 수 있습니다 . 특정 IP 또는 계정의 로그인 실패 횟수가 너무 많을 경우 , IP 차단 또는계정 비활성화가 작동하여 공격자가 반복해서 암호를 입력하지 못하게 됩니다 .

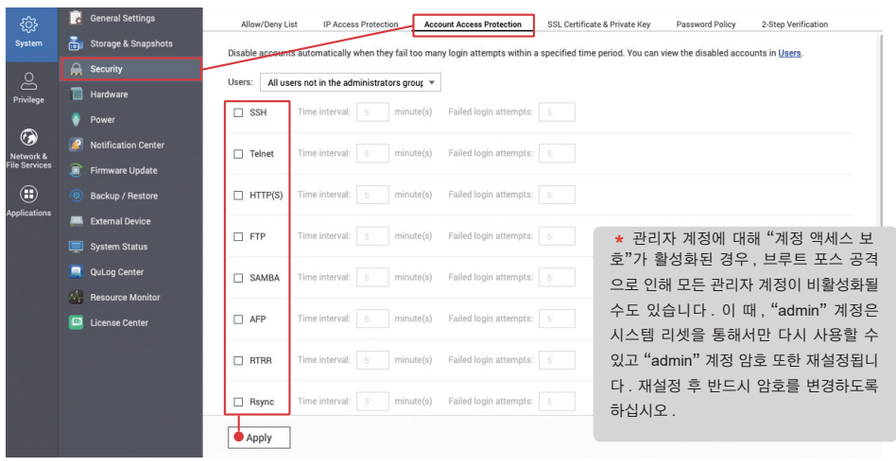
"IP 액세스 보호 " 를 클릭하여 설정 페이지로 들어갑니다 . 모든 서비스를 선택하고 필요에 따라 " 시간 간격 ", " 로그인 실패 횟수 " 및 "IP 차단 기간 " 을 설정한 다음 , " 적용 " 을 클릭하여 설정을 완료합니다 .



* 실수로 일반 사용자의 IP 주소가 차단된 경우 , 다음과 같이 차단 목록을 조정할 수 있습니다 .

1. **다른 컴퓨터에서 QTS /QuTS hero 관리 인터페이스에 로그인**
2. **IP 주소를 변경하고 the QTS /QuTS hero 관리 인터페이스에 로그인**
3. **모바일 브라우저에서 QTS /QuTS hero 관리 인터페이스에 로그인**
4. **QManager 앱 사용**

" 계정 액세스 보호 " 를 클릭하여 설정 페이지로 들어갑니다 . 관련 서비스를 활성화하고 필요에 따라 " 시간 간격 ", " 로그인 실패 횟수 " 및 "IP 차단 기간 " 을 설정한 다음 , " 적용 " 을 클릭하여 설정을 완료합니다 .

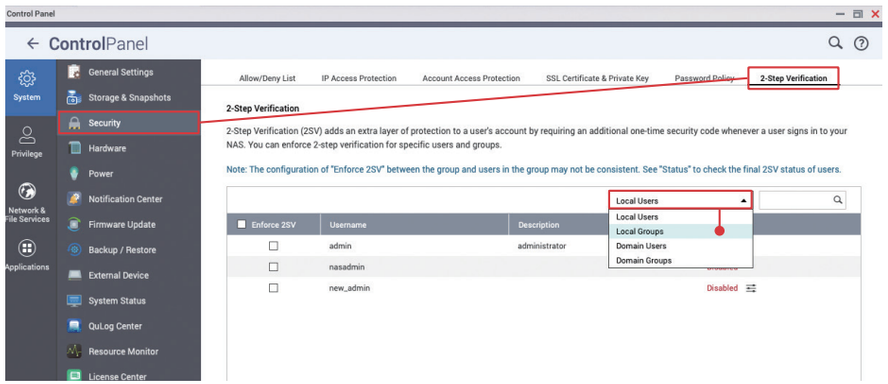


* 관리자 계정에 대해 “계정 액세스 보호”가 활성화된 경우 , 브루트 포스 공격으로 인해 모든 관리자 계정이 비활성화될 수도 있습니다 . 이 때 , “admin” 계정은 시스템 리셋을 통해서만 다시 사용할 수 있고 “admin” 계정 암호 또한 재설정됩니다 . 재설정 후 반드시 암호를 변경하도록 하십시오 .

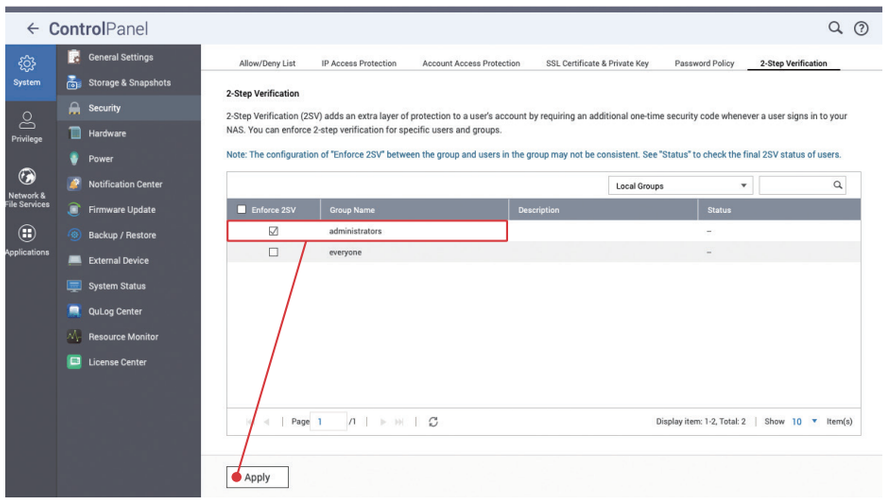
2 단계 인증 활성화 (2SV)

"2 단계 인증 " 을 클릭하여 설정 페이지로 들어갑니다 . " 사용자 " 또는 " 사용자 그룹 " 에 대해 "2 단계 인증 (2SV)" 사용을 실시할 수 있습니다 . " 관리자 그룹 " 의 계정에 대해 2SV 를 활성화할 것을 권장합니다 . 다른 계정의 경우 , 위험을 직접 평가하고 적절한 설정을 적용하십시오 .

" 로컬 사용자 " 를 클릭하여 메뉴를 열고 " 로컬 그룹 " 을 선택합니다 .

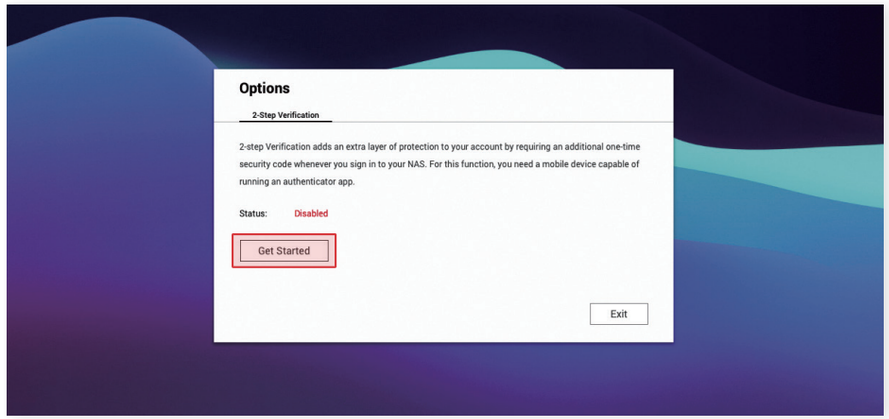


" 관리자 " 에서 "2SV 실시 " 를 선택하고 " 적용 " 을 클릭하여 설정을 완료합니다 .

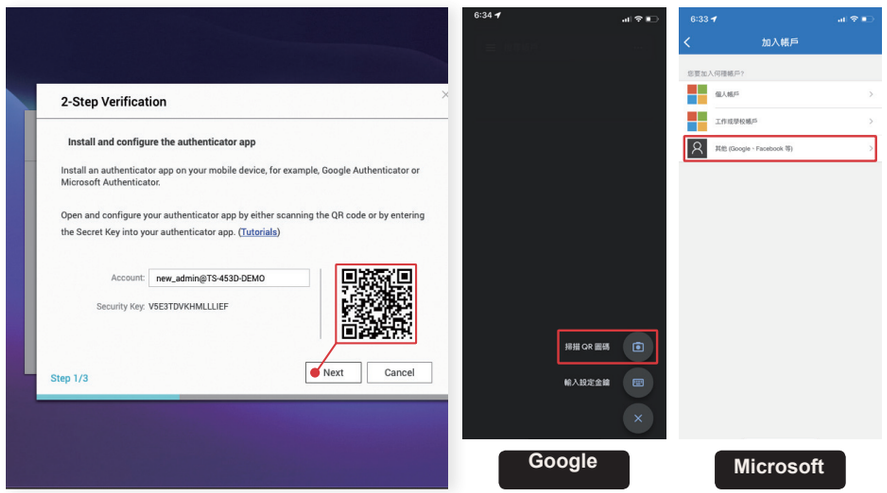


"2SV 실시 " 를 활성화한 후 , "2 단계 인증 (2SV)" 을 사용해 관리자 " 계정이 설정되지 않은 경우 다음 번 로그인할 때 계정 설정을 위해 강제로 "2 단계 인증 (2SV)" 설정 페이지로 이동됩니다 .

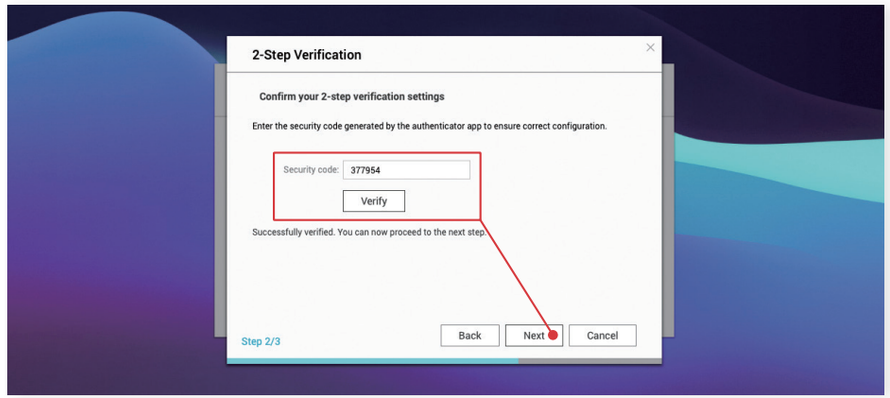
" 시스템 관리자 " 계정으로 다시 로그인하고 " 시작하기 " 를 클릭하여 설정을 시작합니다 .



모바일 기기에 "Google Authenticator" 또는 "Microsoft Authenticator" 를 설치하고 프로그램의 QR 코드를 스캔하여 장치를 추가한 후 , " 다음 " 을 클릭합니다 .



"Google Authenticator" 또는 "Microsoft Authenticator" 에서 생성된 6 자리 " 보안 코드 " 를 입력하고 " 인증 " 을 클릭합니다 . 인증이 끝나면 다음을 클릭하여 계속합니다 .

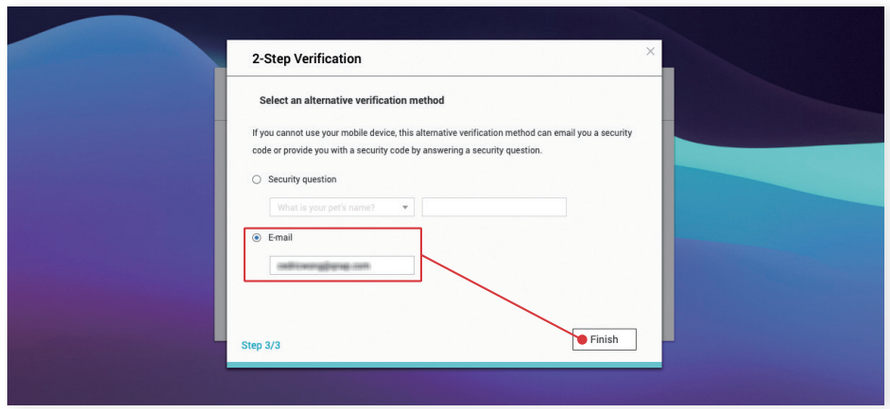


다른 인증 방법 * 을 설정하려면 " 보안 질문 "** 또는 " 이메일 "*** 을 선택하고 항목을 작성한 다음 , " 마침 " 을 클릭하여 "2 단계 인증 (2SV)" 을 활성화합니다 .

* 인증 앱으로부터 " 보안 코드 " 를 수신할 수 없는 경우 , " 보안 질문 " 에 답하거나 " 이메일 " 을 사용해서 " 보안 코드 " 를 받을 수 있습니다 .

** 2 단계 인증을 통과하려면 " 보안 질문 " 에 올바로 답하십시오 . 단순하거나 추측하기 쉬운 질문과 답변은 사용하지 마십시오 .

*** 이 기능을 사용하려면 " 알림 센터 " 에 " 이메일 " 알림 방법을 추가해야 합니다 .



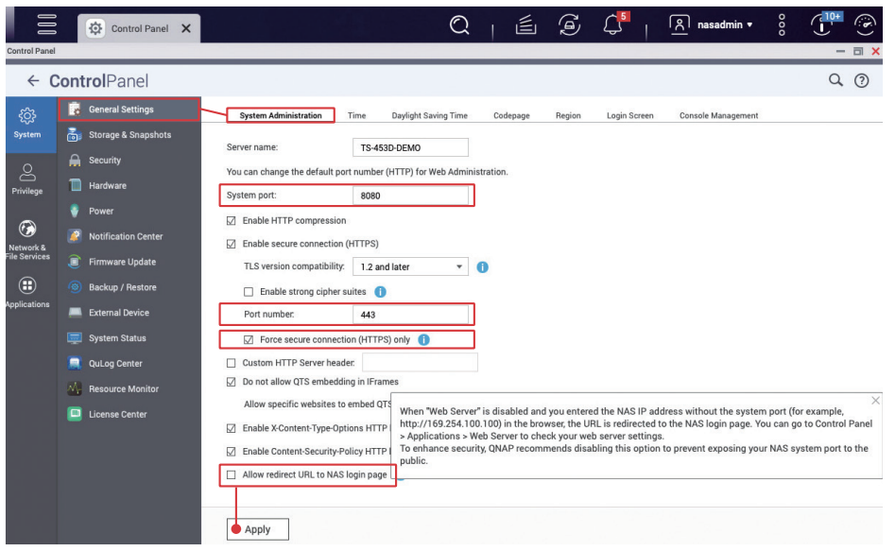
기본 포트 변경

NAS 에서 실행 중인 각 서비스는 해당하는 서비스 포트를 갖습니다 . 수정이 불가능한 일부 표준화된 서비스 포트를 제외하고 , 나머지 서비스 포트는 사용자가 정의할 수 있습니다 .

해커가 공격 타겟을 물색하거나 해커들이 종종 이용하는 IoT 검색 엔진을 사용할 경우 , 기본 포트에 대한 도입을 제일 먼저 시도합니다 . 공격 위험을 줄이기 위해서 일반 서비스의 기본 포트를 변경해야 합니다 . NAS 를 대상으로 한 공격의 경우 가장 일반적인 타겟은 " 시스템 포트 " 입니다 . 다음은 " 시스템 포트 " 를 변경하는 방법을 설명합니다 . 다른 기능의 포트는 해당 설정 페이지에서 수정할 수 있습니다 . 보안을 위해 관련 서비스를 사용하기 전에 반드시 포트를 수정하도록 하십시오 .

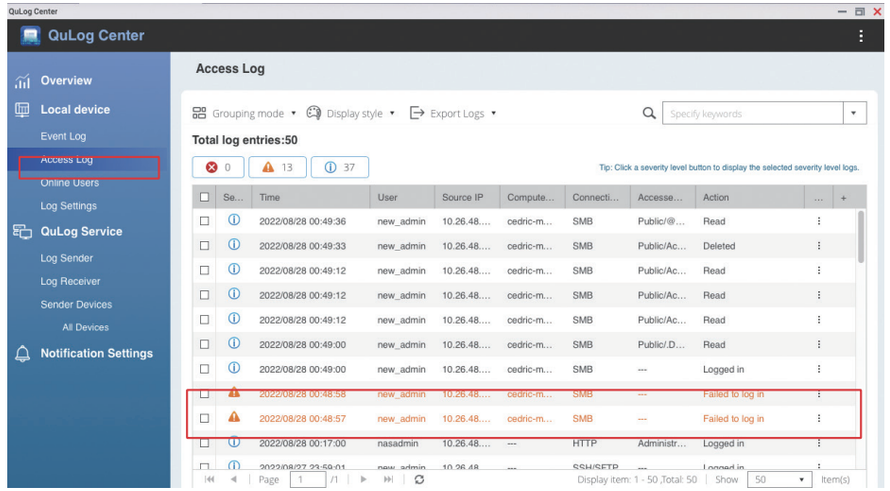
" 제어판 " 을 열고 " 일반 설정 " 을 클릭합니다 . " 시스템 포트 (HTTP)" 기본값은 "8080" 입니다 . 1 ~ 65535 사이에서 포트 번호를 입력할 수 있습니다 (예 : "56789"). " 시스템 포트 (HTTPS)" 의 경우 시스템 포트 (기본값 "443") 는 " 보안 연결 " 기능이 활성화되어 있으며 , 이 포트도 변경하는 것이 권장됩니다 . 동시에 , 모든 사용자가 HTTPS 를 통해 데이터를 전송하도록 하기 위해 " 강제 보안 연결 (HTTPS) 전용 " 을 선택하는 것을 강력히 권장합니다 . 이렇게 하면 해커들이 포트 번호 대입이 어려워져 계정 암호과 같은 민감한 정보를 쉽게 가로채지 못하게 됩니다 .

또한 자동 리디렉션으로 인해 " 시스템 포트 " 가 노출되지 않게 하기 위해서 "NAS 로그인 페이지로 URL 리디렉션 허용 " 의 선택을 취소하는 것이 권장됩니다 . 변경 후 " 적용 " 을 클릭하여 설정을 완료합니다 .

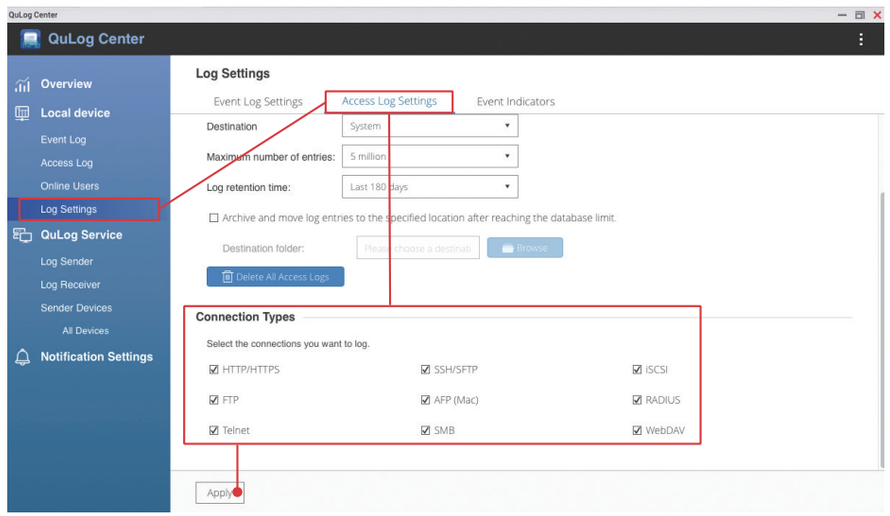


액세스 로그 보기

액세스 로그는 사용자의 파일 액세스 , 작업 , 로그인 기록을 조회하는 데 도움이 될 수 있습니다 . 문제가 발생했을 때 액세스 로그 확인이 기본적인 문제 진단을 위해 첫 번째로 취해야 할 단계입니다 .



"QuLog Center" 를 열고 왼쪽 메뉴에서 " 로그 설정 " 을 클릭한 다음 , " 액세스 로그 설정 " 페이지로 전환합니다 . " 연결 유형 " 에서 모든 연결을 선택한 다음 , " 적용 " 을 클릭하여 설정을 완료합니다 .



보안 앱 설치 및 활성화

QNAP 는 NAS 보안을개선하기 위해 여러 가지 보안 앱을 제공합니다 . 이러한 앱을 설정하면 NAS 보안을 개선하고 사용자가 안심하고 서비스를 이용할 수 있습니다 .

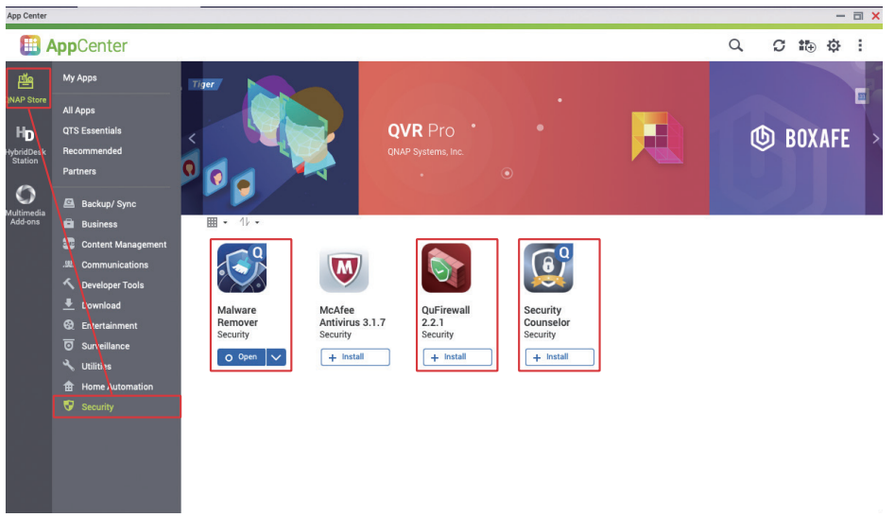
Security Counselor 는 정기적으로 NAS 설정의 보안을 점검하고 잠재적인 위험을 알립니다 .

Malware Remover 는 NAS 에서 감지된 맬웨어를 검사하여 제거합니다 .

QuFirewall 은 QNAP NAS 에 대한 기본적인 방화벽 기능을 제공하여 해커들의 접근을 차단하는 도구 중에 하나입니다 .

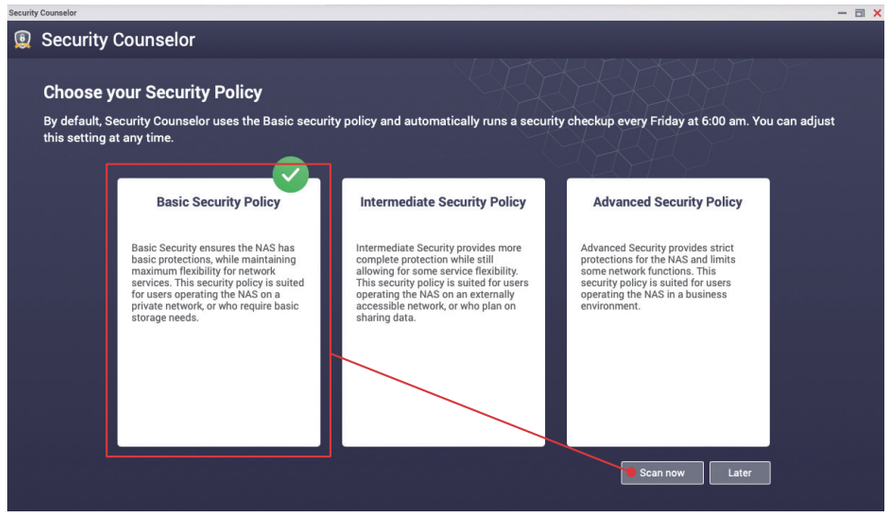
"App Center" 를 열고 왼쪽에서 " 보안 " 을 설치한 다음 , "Security Counselor", "Malware Remover"* 및 "QuFirewall" 을 설치합니다 .

* Malware Remover 는 QTS 4.4.3(이상) 및 QuTS hero 에 사전 설치되어 있습니다 .

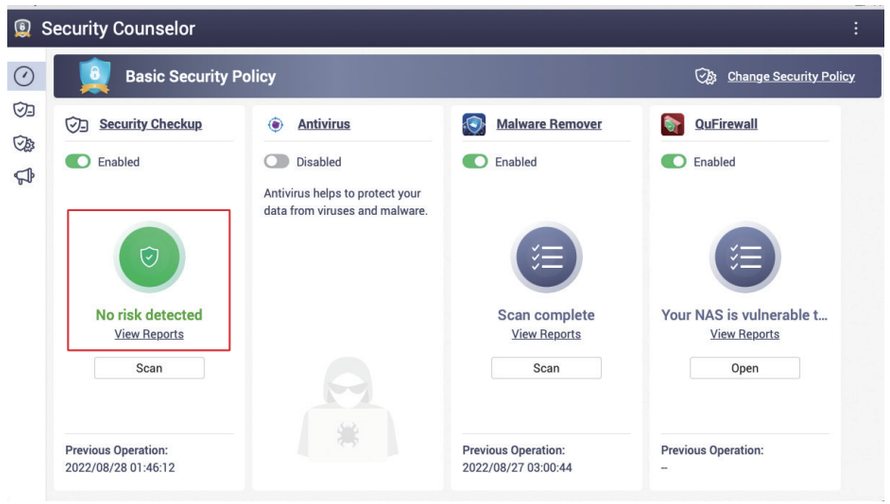


Security Counselor

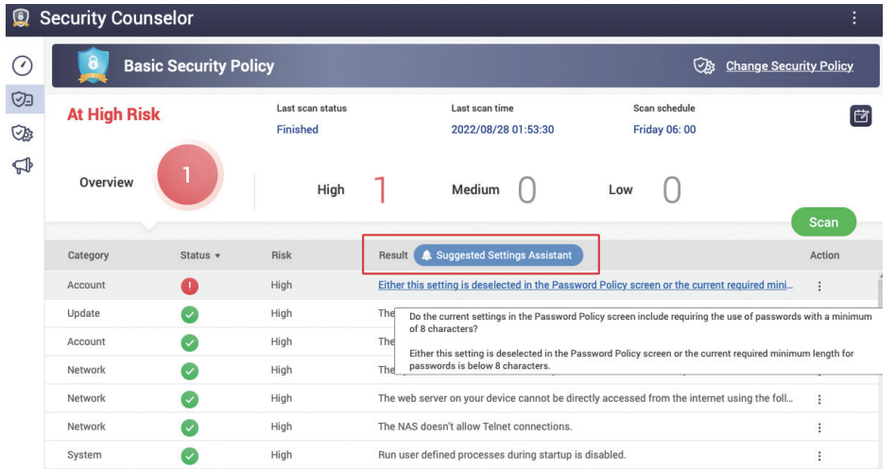
"Security Counselor" 를 열고 " 기본 보안 정책 " 을 선택한 다음 , " 지금 검사 " 를 클릭합니다 .



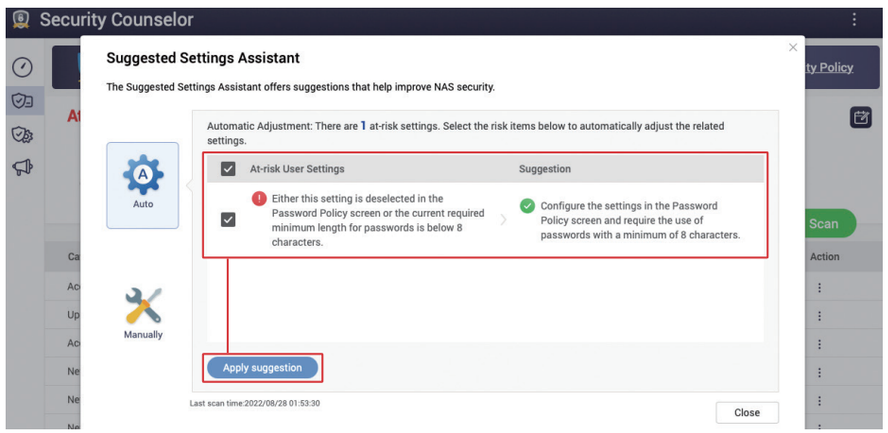
검사가 완료되면 일반적으로 결과가 " 감지된 위험 없음 " 으로 나타납니다 . 위험이 감지되면 " 보고서 보기 " 를 클릭하여 세부 내용을 확인하고 지침을 따라 설정을 수정합니다 .



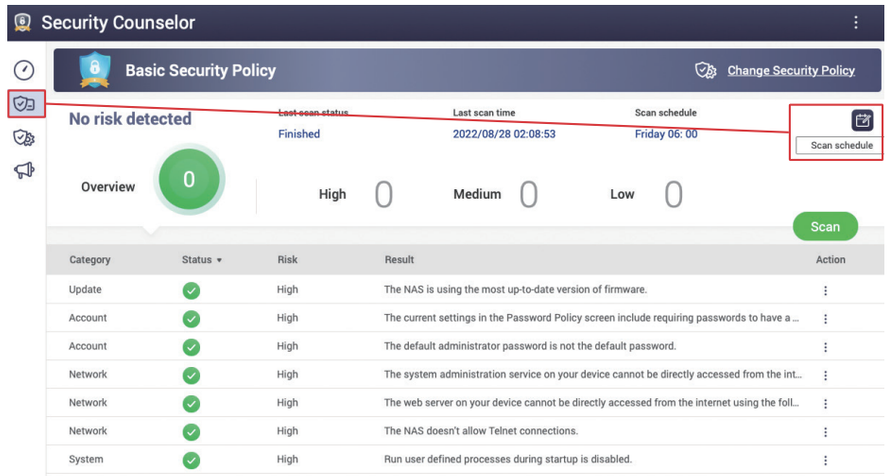
다음은 임의로 잘못된 설정을 수정하여 " 고위험 " 검사 결과가 나오도록 한 예시입니다 . " 추천 설정 도우미 " 를 클릭하면 설정을 조정하는 데 도움이 될 수 있습니다 .



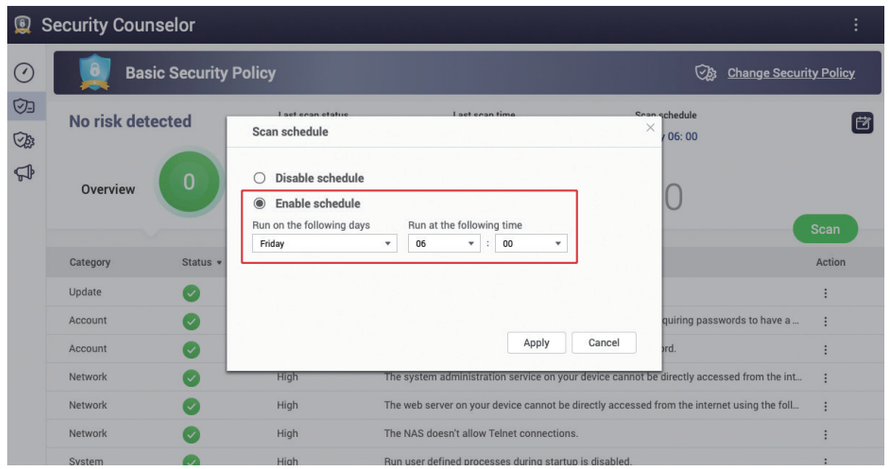
" 추천 설정 도우미 " 에는 설정 추천 사항이 표기됩니다 . 해당 내용을 확인한 후 , " 제안 적용 " 을 클릭합니다 . 그러면 시스템이 관련 설정을 자동으로 적용합니다 . 일부 설정은 수동으로 수정해야 합니다 . 왼쪽에서 " 수동 " 탭을 클릭하고 제안된 대로 설정을 조정합니다 . 변경 내용을 적용하면 검사가 자동으로 다시 시작합니다 . NAS 에 감지된 보안 위험이 없음을 보장하기 위해 검사 결과를 다시 확인할 수 있습니다 .



왼쪽에서 " 보안 점검 " 을 클릭하여 검사 결과 화면으로 들어간 다음 , 오른쪽에서 " 검사 예약 " 을 클릭하여 검사 예약 설정 화면을 엽니다 .

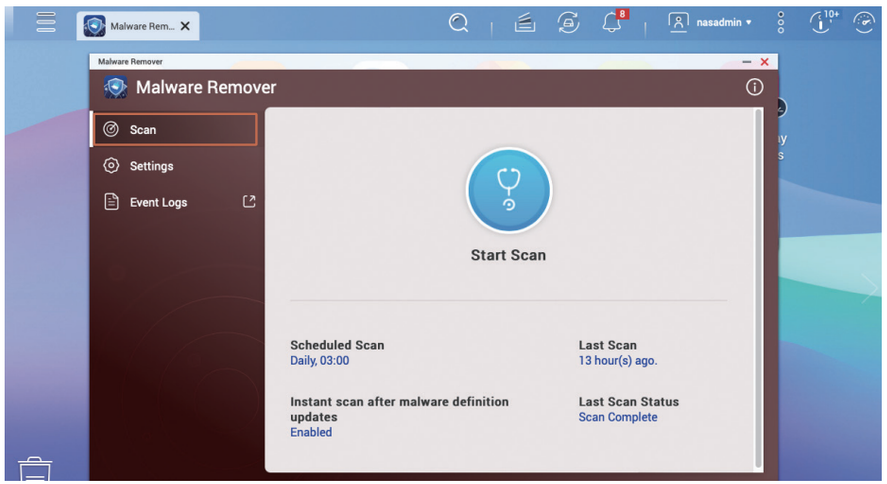


시스템이 정기적으로 설정과 시스템 상태를 확인할 수 있도록 " 검사 예약 " 을 최소한 한 달에 한 번 이상으로 설정하는 것이 권장됩니다 . 위험이 감지되고 Notification Center(알림 센터) 가 올바로 설정되면 알림이 보내지고 바로 문제를 처리할 수 있습니다 .

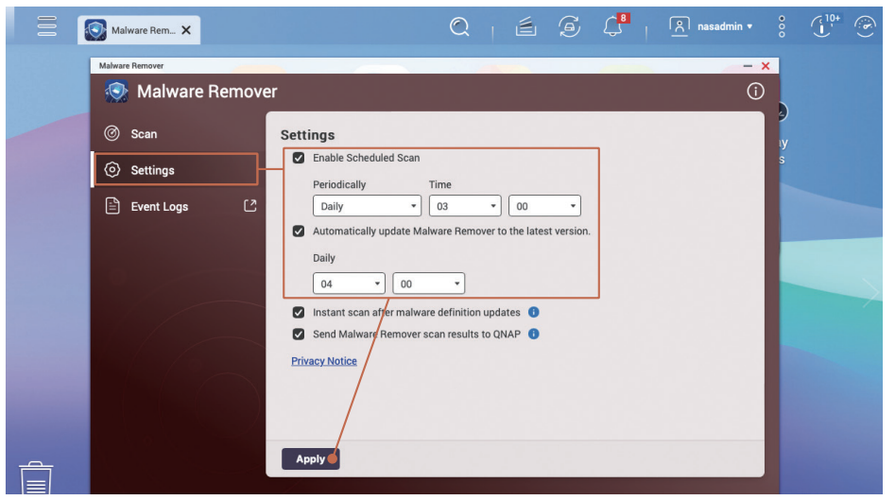


Malware Remover

"Malware Remover(맬웨어 리무버)" 를 엽니다 . 마지막 검사 상태가 표시되고 왼쪽에서 " 설정 " 을 클릭합니다 .

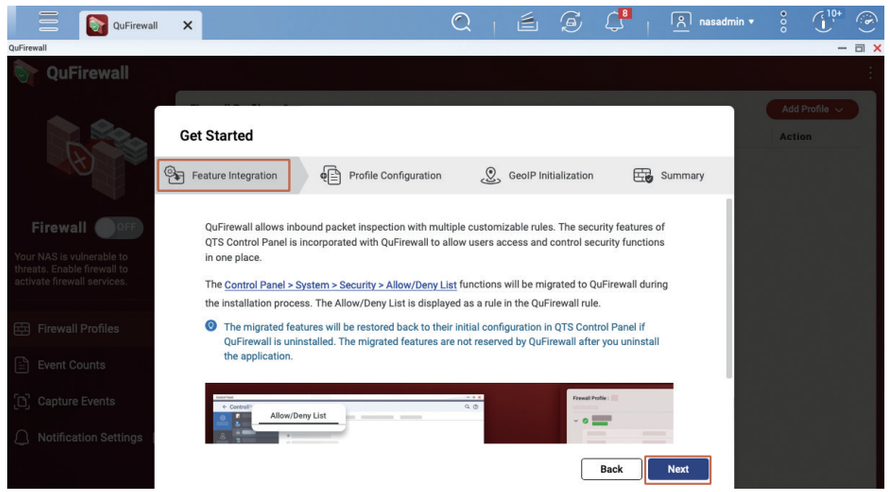


"Malware Remover" 가 정기적으로 시스템 상태를 점검할 수 있도록 " 검사 예약 " 을 하루에 한 번으로 설정하는 것이 권장됩니다 . 또한 기본값인 "Malware Remover 를 최신 버전으로 자동 업데이트합니다 " 의 유지를 바랍니다 .

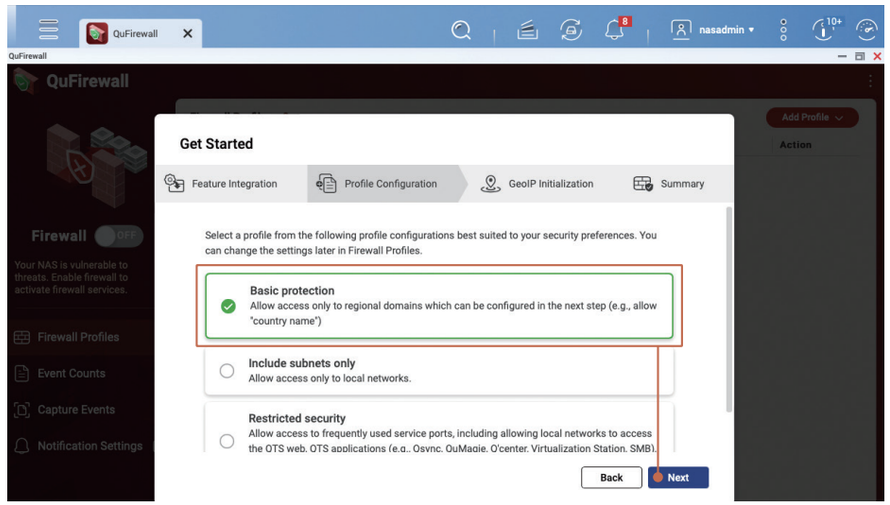


QuFirewall

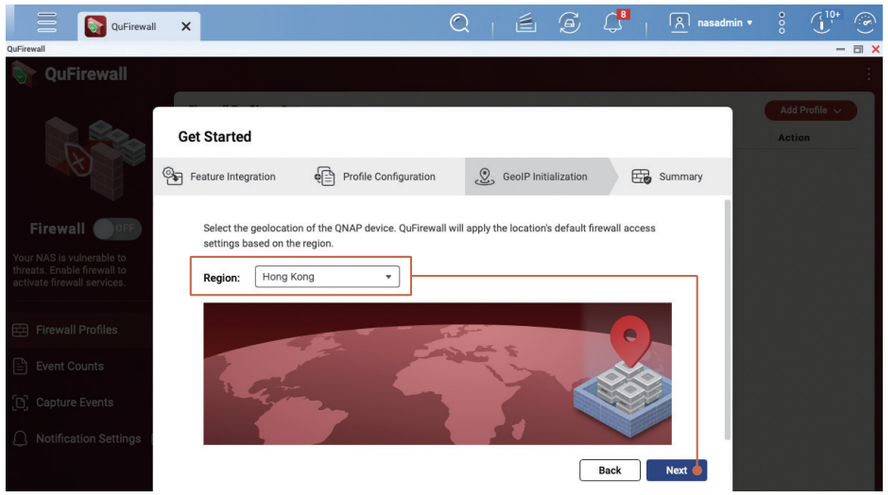
"QuFirewall(큐파이어월)" 을 엽니다 . QuFirewall 을 처음 사용하는 경우 시작하기 화면이 표시됩니다 . 화면의 내용을 읽은 후 " 다음 " 을 클릭하여 계속합니다 .



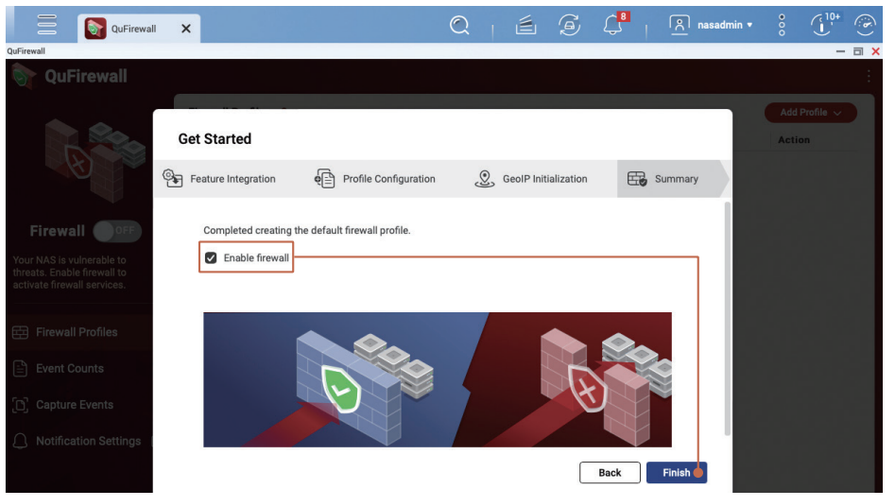
네트워크 관련 커스터마이징이 필요 없는 경우 , " 기본 보호 " 를 선택하는 것이 권장됩니다 . " 다음 " 을 클릭하여 계속합니다 .



위치에 따라 지역을 설정합니다 . 선택된 지역에서만 NAS 로 접근이 가능합니다 . 예를 들어 , 한국에 있는 경우 " 한국 " 을 선택하고 " 홍콩 " 에 있는 경우 " 홍콩 " 을 선택하십시오 . 나중에 지역을 더 추가할 수 있습니다 . " 다음 " 을 클릭하여 계속합니다 .

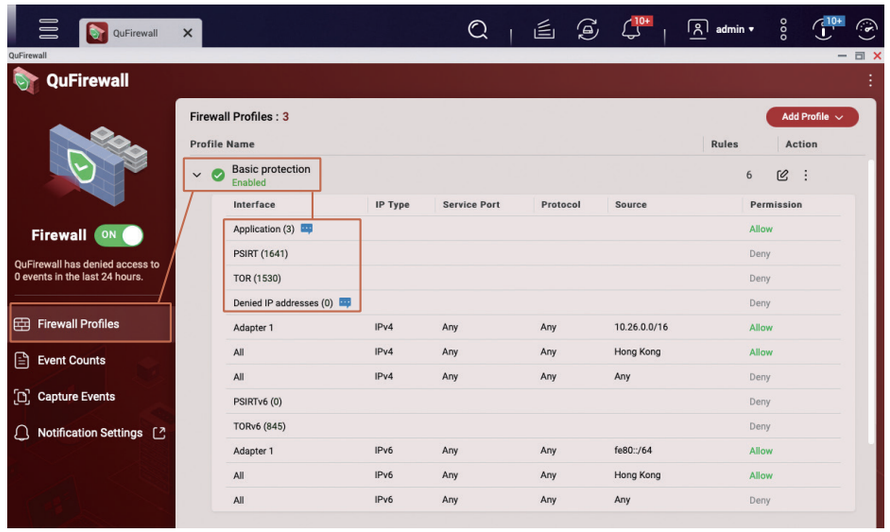


" 방화벽 활성화 " 를 선택하고 " 마침 " 을 클릭하면 설정이 적용되어 방화벽이 활성화됩니다 .



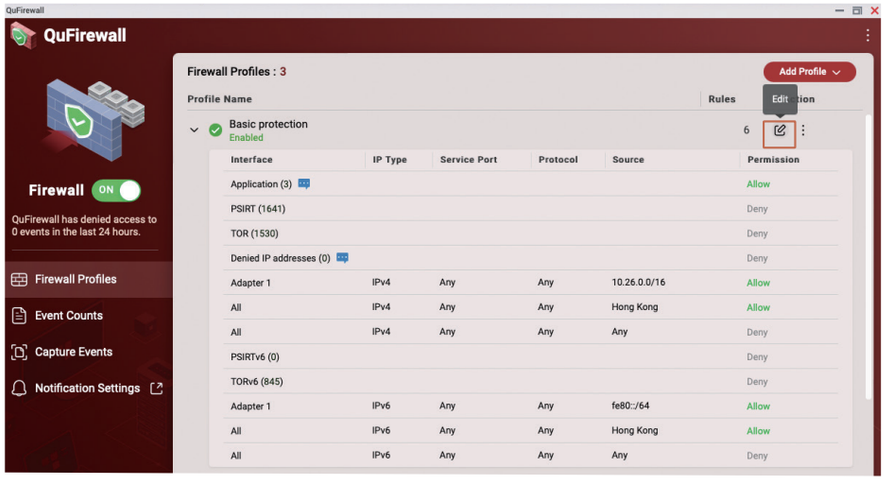
QuFirewall 프로필 페이지로 가면 " 기본 보호 " 가 활성화된 것을 확인할 수 있습니다 . " 기본 보호 " 를 클릭하여 확장하고 해당하는 방화벽 규칙을 확인합니다 . 수신되는 패킷의 정보에 대해 규칙이 선택되며 , 규칙에 따라 해당 패킷이 방화벽을 통과하거나 차단됩니다 . 방화벽 규칙은 순차적으로 실행됩니다 . 조건이 충족되지 않으면 다음 라인의 규칙이 적용됩니다 . 수신된 패킷이 해당 규칙에 충족되지 않으면 마지막의 " 모두 거부 " 규칙이 적용되어 방화벽이 해당 연결을 차단합니다 .

- " 애플리케이션 " 규칙은 시스템의 올바른 기능을 보장하기 위해 시스템에서 생성됩니다 .
- "PSIRT" 규칙은 QNAP PSIRT 에서 작성된 블랙리스트입니다 . 여기에는 QNAP NAS 를 공격한 이력이 있는 IP 주소가 포함되어 있습니다 .
- "TOR" 규칙은 TOR 네트워크로부터의 연결을 차단하는 데 사용됩니다 . TOR 네트워크는 익명성 때문에 범죄자들에게 널리 사용되며 , 이 네트워크를 차단하면 공격 위험을 줄일 수 있습니다 .
- " 거부된 IP 주소 " 는 "IP 액세스 보호 " 기능 또는 사용자가 직접 추가한 블랙리스트에서 차단된 IP 주소입니다 .

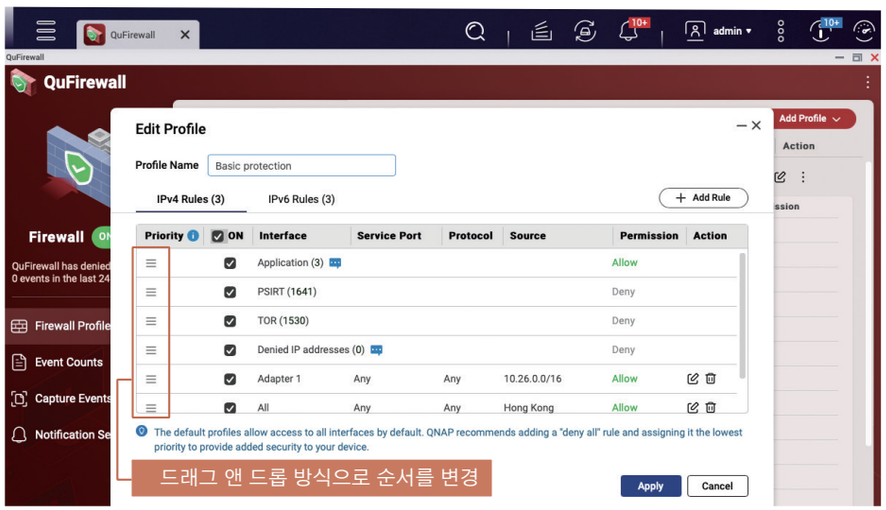


사용자는 다른 규칙을 설정할 수 있으며 , 기본 보호 설정 하에서는 동일 인트라넷 및 동일 지역의 인터넷 연결만이 " 허용 " 됩니다 . 더욱 안전한 사용을 위해 QNAP 은 NAS 관리자가 " 화이트리스트 " 를 만들어 NAS 에 연결을 허용하는 내부 / 외부 IP 주소를 사용자 지정 규칙에 사전등록 하는것을 권장합니다 .

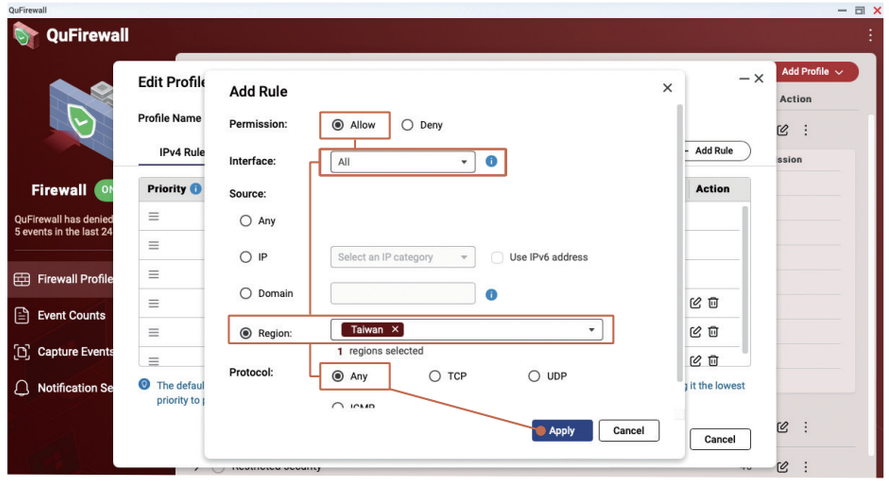
다음은 방화벽 규칙을 편집하는 방법을 보여줍니다 . " 편집 " 버튼을 클릭하여 방화벽 프로필 화면을 편집합니다 .



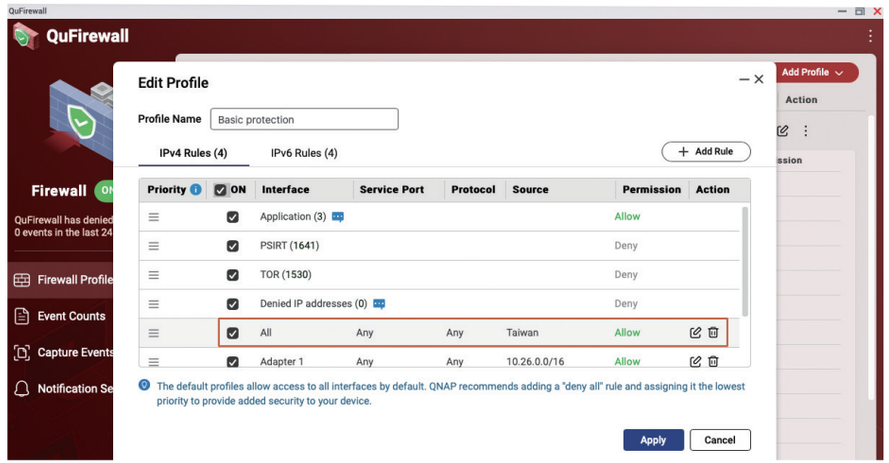
프로필 편집 화면에서 규칙의 순서를 변경하거나 새 규칙을 추가할 수 있습니다 . 다음 예시에서는 연결이 허용된 하나 이상의 지역을 추가합니다 . " 규칙 추가 " 를 클릭하여 설정 화면으로 들어갑니다 .



예를 들어 한국에서만 연결을 허용하려면 " 권한 " 을 " 허용 " 으로 설정하고 , " 인터페이스 " 를 " 모두 " 로 설정하고 , " 소스 " 에 대한 " 지역 " 에서 " 한국 " 을 선택하고 " 프로토콜 " 을 " 임의 " 로 설정해야 합니다 . 그런 다음 " 적용 " 을 클릭하여 규칙을 추가합니다 .



" 프로필 편집 " 페이지에서 새로 추가된 규칙을 볼 수 있습니다 . 필요하면 규칙의 순서를 조정할 수 있습니다 . 규칙이 올바른지 확인한 후 , " 적용 " 을 클릭합니다 .



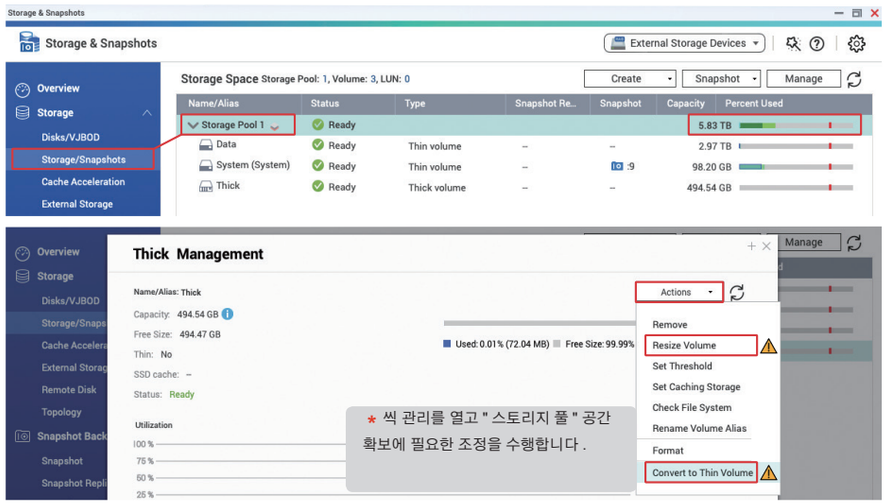
스냅샷 활성화

스냅샷 기능은 다중 버전의 복원 지점을 생성해서 중요한 데이터를 보호할 수 있습니다 . QNAP NAS 에서 스냅샷 스케줄 기능을 설정하여 , 시스템이 일정에 따라 자동으로 스냅샷을 생성하여 기본적인 데이터 보호 방법으로 사용할 수 있습니다 .

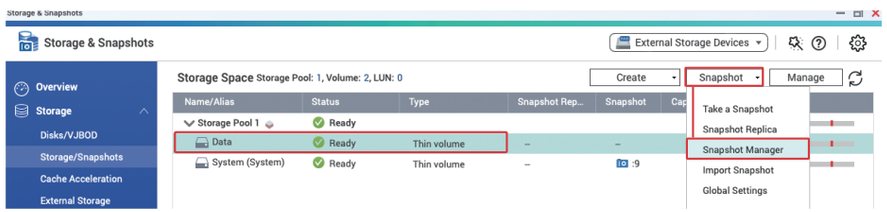
* 예약된 스냅샷은 기능은 QTS 5.0.0 에서는 " 전체 / 씬 볼륨 " 에 대해 기본 활성화되어있습니다 .
* QTS 5.0.1(이상) 에서는 기본적으로 " 씬 볼륨 " 만 예약된 스냅샷이 기본 활성화되어있습니다 .
* QuTS hero h5.0.1(이상) 에서 생성된 " 공유 폴더 " 는 기본적으로 예약된 스냅샷을 활성화합니다 .

" 스토리지 및 스냅샷 " 을 열고 왼쪽에서 " 스토리지 / 스냅샷 " 을 클릭합니다 . " 스토리지 공간 " 이 " 스토리지 풀 " 구조이고 , " 스토리지 풀 " 이 스냅샷 기능을 적용하기 위한충분한 여유 공간이 있는지 확인합니다 . 볼륨 유형이 " 전체 볼륨 " 일 경우 , 스냅샷 기능을 위한 " 스토리지 풀 " 공간 확보를 위해 " 볼륨 크기 조정 *" 및 " 씬 볼륨으로 전환 *" 을 고려할 수 있습니다 .

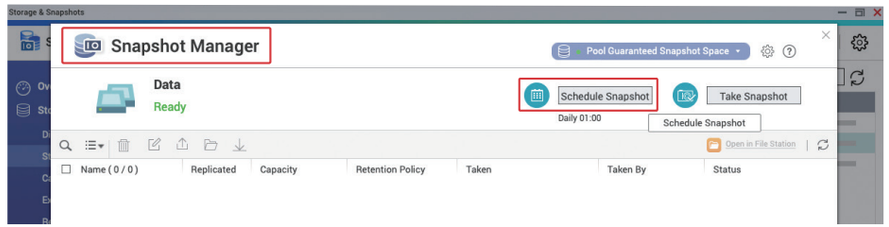
* 볼륨을 전환하기 전에 데이터를 반드시 백업하여 혹시라도 발생할 수 있는 데이터 손실에 대비를 권고드립니다 .



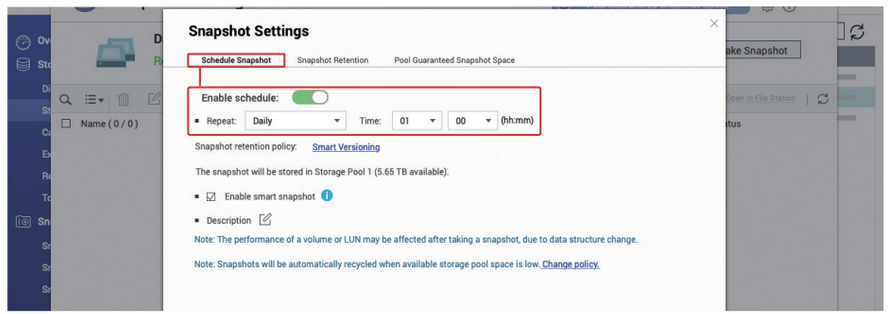
NAS 의 " 스토리지 풀 " 에 충분한 공간이 있음을 확인한 후 , 먼저 " 볼륨 " 을 클릭한 다음 상단에서 " 스냅샷 " 을 클릭하고 메뉴에서 " 스냅샷 관리자 " 를 클릭합니다 .



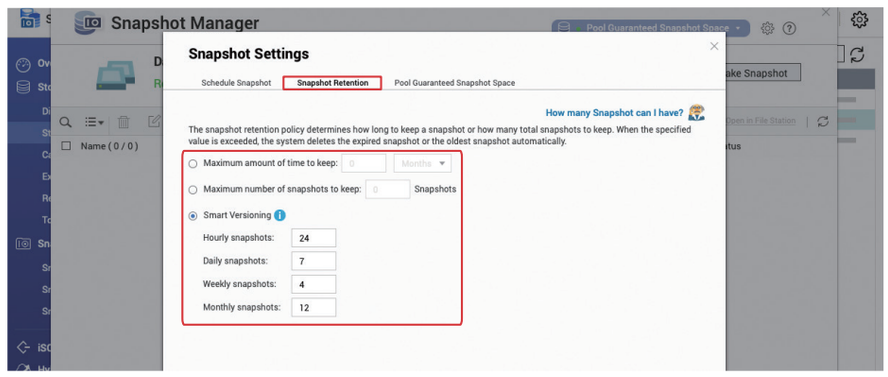
" 볼륨 " 의 " 스냅샷 관리자 " 설정 페이지로 이동하고 상단 오른쪽에서 " 스냅샷 예약 " 을 클릭합니다 .



" 예약 사용 " 을 " 활성화 " 상태로 전환한 다음 , 필요에 맞는 예약규칙을 설정합니다 .
" 매일 " 또는 " 매주 " 를 사용하는 것이 권장됩니다 .



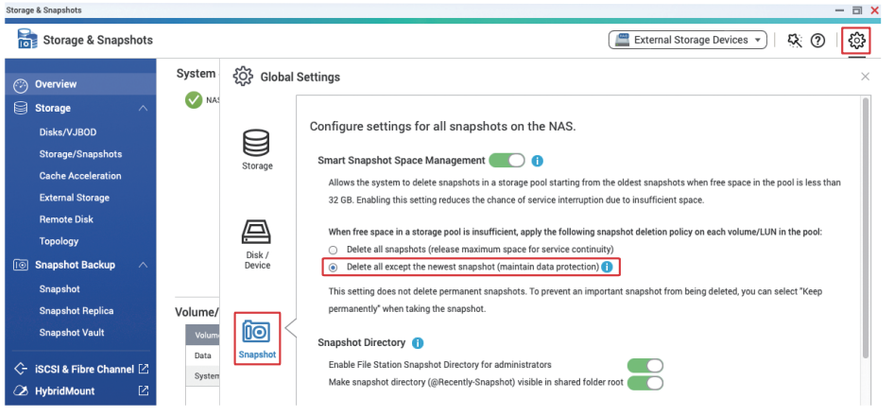
스냅샷 보관 정책을 설정하여 스냅샷이 너무 많은 공간을 차지하지 않도록 스냅샷 생성 갯수를정할 수 있습니다 .
" 스마트 버전 관리 " 설정 사용을 권장합니다 . 스마트 버전관리 기능은 GFS(Grandfather-Father-Son) 규칙으로 , 데이터 보호를 위해 한번의 스냅샷 생성 후 데이터가 변경될 때마다 새로운 버전의 스냅샷이 자동으로 생성됩니다 . 설정이 완료되면 " 확인 " 을 클릭하여 해당 설정을 적용합니다 .



스냅샷 삭제 정책 설정

사용자의 설정에 기반한 스냅샷 삭제를 통해 스토리지 풀에 공간이 부족할때 공간 부족으로 발생할 수 있는 서비스 중단을 예방하고 , 정상적인 시스템 서비스를 유지할 수 있습니다 .

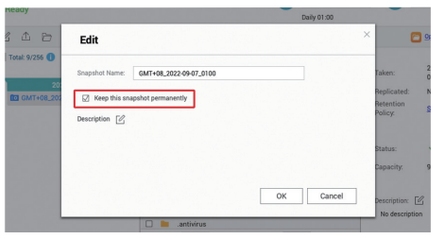
" 스토리지 및 스냅샷 " 에서 상단 오른쪽 모서리에 있는 " 설정 " 버튼을 클릭하고 " 전역 설정 " 을 열고 다음 , " 스냅샷 " 을 클릭합니다 . " 최신 스냅샷을 제외한 모든 항목 삭제"로 설정하여 공간 부족으로 인한 스냅샷 삭제시에도 최신 스냅샷을 유지하는 것을 권장합니다 .

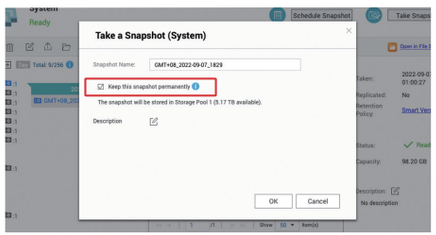


사용자의 사용 시나리오에 의거하여 " 스토리지 풀 " 의 공간이 부족해도 시스템이 모든 스냅샷의 보관이 필요한 경우 " 스마트 스냅샷 공간 관리 " 를 비활성화해야 합니다 . 이경우 " 스토리지 풀 " 공간이 부족해지면 " 스토리지 풀 " 이 " 읽기 전용 / 삭제 " 상태로 자동변경되어 쓰기가 제한된다는 점을 유념하십시오 . " 스토리지 풀 " 을 정상 작동 상태로 복원하려면 수동으로 스냅샷을 삭제해야 합니다 . 스마트 스냅샷 공간관리 기능이 비활성화한 경우 사용자가 정기적인 공간 사용량 확인이 요구됩니다 .

스냅샷 삭제 정책으로 인한 보호 기능 실패를 방지하기 위해서 , 할당된 스냅샷 공간대비 대용량의 데이터를 저장하는 경우 , 기존 스냅샷의 전부 또는 일부를 " 스냅샷을 영구적으로 보관 "* 으로 선택 / 설정하여 스냅샷이 시스템에서 삭제되지 않도록 하십시오 .

* 공간을 확보하기 위해서 반드시 수동으로 삭제해야 합니다 . 수동으로 생성하고 정기적으로 삭제하는 것이 권장됩니다 .





NAS 보안 설정 체크리스트

☐ 알림 센터 설정

- ☐ 최소 하나의 알림 설정하기
- ☐ " 경고 알림 " 규칙 만들기
- ☐ " 펌웨어 업데이트 " 알림 규칙 만들기

☐ 펌웨어 자동 업데이트 활성화 (QTS / QuTS hero)

☐ App Center 구성

- ☐ 모든 앱을 최신 버전으로 업데이트
- ☐ 유효한 디지털 서명이 없는 애플리케이션 설치 금지
- ☐ 자동 업데이트 활성화

☐ 불필요한 기능 비활성화 또는 제거

- ☐ 활성화된 서비스가 필요한지 확인
- ☐ 활성화된 **App Center** 앱이 필요한지 확인
- ☐ **SSH 비활성화**
- ☐ 텔넷 **비활성화**

☐ 시스템 계정 보안 강화

- ☐ 기본 "admin" 계정 비활성화
- ☐ 암호 정책 설정
- ☐ **IP** 액세스 보호 **활성화**
- ☐ 2 단계 인증 (**2SV**) **활성화**

☐ 기본 시스템 포트 변경

☐ 액세스 로그 활성화

☐ 보안 앱 설치 및 활성화

- ☐ **Security Counselor**
  - ☐ 예약된 검사 시작
- ☐ **Malware Remover**
  - ☐ 예약된 검사 시작
- ☐ **QuFirewall**
  - ☐ 방화벽 활성화
  - ☐ **Geo-IP** 지역 **설정**
  - ☐ **PSIRT** 규칙 활성화
  - ☐ **TOR** 규칙 활성화

☐ 예약된 스냅샷 활성화

- ☐ 정기적으로 " 스냅샷 영구 보관 " 설정

FAQ

Q 인터넷에서 NAS 로 접근을 막으면 더욱 안전해지나요 ?

A 아닙니다 . NAS 와 " 인터넷 연결 끊기 " 의 개념은 일반적으로 NAS 를 네트워크에서 차단하는 것을 지칭하며 외부에서 내부에 있는 NAS 로 연결을 막는 것을 말합니다 . 일부 맬웨어는 악성코드 실행을 위해 외부 연결이 필요하지만 , 여전히 외부 연결 없이도 악성 공격을 수행하는 맬웨어들도 존재합니다 . 따라서 단순 인터넷 연결 단절은 해커들의 불법적 행위를 차단하지 못할 뿐 아니라 자동 소프트웨어 업데이트 , 알림과 같은 안전에 도움이 되는 일부 시스템 기능도 제대로 작동하지 못하게 됩니다 . 올바른 설정방법은 불필요한 인터넷 노출을 사전에 예방하여 허용된 IP 주소만 NAS 로의 연결 및 불특정 다수의 트래픽을 제한하여 보안을 개선하는 것입니다 .

Q 내 하드 디스크는 RAID 로 구성되어 있습니다 . 이것이 백업이 필요하지 않음을 의미합니까 ?

A 아닙니다 . RAID 는 백업 방법이 아닙니다 . 레이드 0 이상의 RAID 레벨은 디스크 오류에 대한 중복성을 제공하기 위한 것뿐입니다 . 즉 , 레이드는 디스크 고장에 대비 방법일뿐 데이터 삭제 또는 암호화에 대한 보호 기능을 제공하지 않습니다 . 따라서 3-2-1 백업 규칙에 따라 데이터를 백업하는 것을 권장합니다 .

Q 이미 " 스냅샷 " 을 설정했습니다 . 이것이 백업이 필요하지 않음을 의미합니까 ?

A 아닙니다 . " 스냅샷 " 은 데이터와 동일한 하드 드라이브 세트에 저장되므로 RAID 오류가 발생하면 데이터가 여전히 손실됩니다 . 또한 해커들이 충분한 권한을 확보할 수 있는 경우 (관리자 계정이 탈취된 경우), " 스냅샷 " 또한 삭제될 수 있습니다 . 따라서 3-2-1 백업 규칙에 따라 스냅샷 파일도 백업하는 것을 권장합니다 .

Q 내 NAS 는 인터넷에 연결되지 않습니다 . 이것이 공격이 불가능함을 의미합니까 ?

A 아닙니다 . 대부분 사이버 공격이 인터넷을 통해 발생하지만 인트라넷상에서도 다른 기기를 통해 NAS 가 공격을 받을 수 있습니다 . 예를 들어 인트라넷상의 다른 컴퓨터 또는 장치가 해킹되었거나 맬웨어의 영향을 받은 경우 , 인트라넷을 통해 NAS 도 공격을 받을 수 있습니다 . 컴퓨터에 바이러스 방지 소프트웨어를 설치하고 네트워크 보안 제품을 구축하면 관련 위협을 예방 / 대응하는 데 도움이 될 수 있습니다 . 예를 들어 , QNAP ADRA NDR 은 의심스러운 인트라넷 활동을 감지하여 자동으로 격리시킬 수 있습니다 . 동시에 3-2-1 백업 규칙에 따른 데이터 백업을 권장합니다 .

Q NAS 를 오랜 기간 관리하지 않고 사용 중입니다 . 혹시 맬웨어의 감염 여부를 확인할 수 있나요 ?

A CPU 나 시스템 프로세스 부하가 비정상적으로 높거나 , 소프트웨어 업데이트가 실패하거나 , App Center 에 알 수 없는 앱이 있을 경우 악성 프로그램이 설치되었을 수 있습니다 . 즉시 최신 버전의 Malware Remover 를 설치하여 사용하는 것이 권장됩니다 . 여전히 문제를 해결할 수 없으면 QNAP 기술 지원팀에 연락해서 도움을 요청하십시오 .

Q 인터넷에 일부 서비스를 열어야 할 경우 , 보안을 위해 무엇을 해야 하나요 ?

A NAS 에 최신 버전의 펌웨어와 앱이 설치되었는지 확인하십시오 . QuFirewall 을 활성화하여 기본적인 방화벽을 적용할 수도 있으며 , "PSIRT" 및 "TOR" 규칙은 일부 해커의 연결을 차단하는 데 도움이 될 수 있습니다 . 가정 사용자는 공유기의 방화벽 기능 사용 , 비즈니스 또는 엔터프라이즈 사용자일 경우 , 상위 수준의 방화벽 솔루션을 사용하는 것을 권장합니다 . 또한 스토리지 풀 공간을이 할당하여 " 스냅샷 " 을 통한 기본적인 데이터 보호를 권장합니다 . 최악의 시나리오를 준비하고 중요한 데이터 손실 예방 / 방지를 위해서 3-2-1 백업 규칙에 따라 데이터를 백업하는 것을 권장합니다 .

Q 내 NAS 가 구형이고 최신 버전의 QTS 를 지원하지 않습니다 . 그래도 안전하게 사용할 수 있나요 ?

A 레거시 및 기술지원 중단 (EOL) 모델은 기술지원이 제한되므로 인터넷 / 인트라넷에 연결하여 사용시 위험에 노출될 가능성이 높습니다 . 따라서 인트라넷 / 오프라인에서 백업용도로만 사용을 권장합니다 .

Q NAS 로그인 실패 경고가 계속해서 나타나는 이유는 무엇입니까 ?

A 로그인의 실패한 IP 주소가 인터넷에서 접속시도인 경우 , 외부에서 암호 크래킹 공격을 통한 NAS 에 접근일 수도 있습니다 . 튜토리얼을 따라 안전한 인터넷 연결과 NAS 의 보안 설정을 강화해야 합니다 . 로그인 실패한 IP 주소가 인트라넷에서 접속시도인 경우 , 해당 IP 주소를 가진 장치에 맬웨어가 설치되었는지 또는 단순 접속실패인지 확인하여 인트라넷의 관리에도 유의하시기 바랍니다 .

Q 모든 파일이 이상한 파일 이름으로 바뀌었습니다. 왜 그런가요?

A Ransomware 감염의 증상입니다. NAS 액세스 로그를 확인하여 암호화 작업이 다른 인트라넷의 컴퓨터 / 장치나 NAS 에서 발생한 것인지 확인하십시오. NAS 가 Ransomware 의 영향을 받은 경우, 적절한 단계를 취해 감염이 번지는 일을 막아야 합니다. NAS 관련 사항은 QNAP 기술 지원팀에 연락해서 도움을 요청하십시오.

Q NAS 가 Ransomware 에 감염된 경우, 어떻게 해야 하나요?

A 대부분 Ransomware 는 고도화된 암호화 방법을 사용합니다. 정확한 Key 값이 없는 경우 파일의 암호를 풀 수 없으므로 백업 또는 스냅샷으로만 파일을 복구할 수 있습니다.

제일 먼저 이 튜토리얼을 따라 라우터 설정을 수정하여 인터넷에 NAS 노출을 피하고, 2 차 공격을 막으십시오. 두 번째로, 즉시 모든 동기화 작업을 일시 중단하고 스냅샷 설정을 영구 보관으로 변경하여 백업 파일을 잃지 않도록해야 합니다. 보유한 데이터에 대한 백업본이나 스냅샷이 있어야만 NAS 펌웨어와 앱을 업데이트하고 Malware Remover 검사를 완료한 후 파일을 복구할 수 있습니다. 데이터가 백업되지 않은 경우, Ransomware 에서 남긴 랜섬 요구 노트와 랜섬 지불 방법을 백업한 다음, 데이터 복구와 같은 방법을 시도하여 일부 데이터를 복원해 보십시오. 필요하면 QNAP 기술 지원팀에 연락해서 도움을 요청하십시오.

Q QNAP 이 새롭게 발견되는 취약성에 대해 패치적용을 완료했다는 언론 기사가 자주 보입니다. 이는 QNAP 제품이 안전하지 않음을 뜻합니까?

A 이 세상에 완벽한 소프트웨어와 하드웨어는 없습니다. 여러 제조사에서 개발한 특허 소프트웨어에건, 오픈 소스 소프트웨어이건, 심지어 하드웨어 조차도 취약성은 항상 발견되며 제조업체에서 패치 작업이 항상 이루어지고 있습니다. 다른 기술 업체와 마찬가지로 QNAP 은 계속해서 알려진 취약성에 대한 패치를 제공하고 있으며, 사용자가 장치와 데이터 보안을 위해 조속히 업데이트할 수 있도록 업데이트 파일을 제공하고 있습니다. 특히 QNAP PSIRT 팀은 사이버 보안 알림 발행을 통한 즉각적인 외부공개 및 세계 사이버 보안협회의 권고를 준수하고 있습니다. 투명한 외부공개를 통해 사용자가 발생한 문제에 적절히 대응할 수 있습니다. QNAP 는 투명하고 열린 방식으로 취약성 문제를 공개 및 대응함으로써 사용자의 알 권리를 보호하고 제품 안전을 개선할 수 있다고 믿습니다. 또한 사용자은 QNAP Security Advisories 에 참여하거나, 제품 보안관련 이메일을 구독하면 더욱 빠르고 신속하게 정확한 정보를 받으실 수 있습니다.

QNAP Security Advisories:
https://www.qnap.com/go/security-advisories/

Q 3-2-1 백업 규칙이 무엇입니까?

A 3-2-1 백업 규칙은 IT 업계에서 통용되는 데이터 백업과 복원 / 복구를 위한 규칙입니다. 이 규칙은 데이터 재난 / 재해 상황이 발생했을 때 데이터 복원 / 복구를 위해서 어떤 방식으로 파일과 데이터 복원본 준비해야 하는지를 설명합니다.

3-2-1 백업에서 "3" 는 최소 3 개의 백업 사본을 뜻합니다. "2" 는 최소 2 개의 다른 저장 매체를 사용하여, "1" 은 최소 하나의 사본이 오프사이트 백업이어야 함을 뜻합니다.

3-2-1 백업 원리에 따라 실수에 의한 수정, 삭제, 하드웨어 손상, 바이러스 감염, 화재와 홍수와 같은 재해 발생 등에 관계없이 복원 가능한 백업 파일을 확보할 수 있습니다.

이 규칙에 의거하여 QNAP NAS 는 Hybrid Backup Sync 3(HBS3), Snapshot Replica, SnapSync(QuTS hero 에서만 지원) 등 애플리케이션을 통해 NAS 의 데이터를 오프사이트 NAS, 퍼블릭 클라우드, 외부 스토리지, 기타 파일 서버 및 / 또는 기타 장치에 백업할 수 있는 다양한 기능을 제공합니다.

Hybrid Backup Sync 3(HBS3) 관련 튜토리얼 :
https://www.qnap.com/go/how-to/tutorial/article/hybridbackup-sync

스냅샷 복제 관련 튜토리얼 :
https://www.qnap.com/go/how-to/tutorial/article/savesnapshots-to-other-qnap-nas-with-snapshot-replica

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

추가 방법으로, 오프라인 백업 또는 QuTS hero 의 WORM(Write Once Read Many) 스토리지 공간을 활용한 백업방법을 적용하여 백업본에 대한 데이터 조작을 방지할 수 있습니다.

메모

2023
보안 가이드

QNAP

2023 보안 가이드

QNAP SYSTEMS, INC.

전화: +886-2-2641-2000 팩스: +886-2-2641-0555 이메일: qnapsales@qnap.com

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