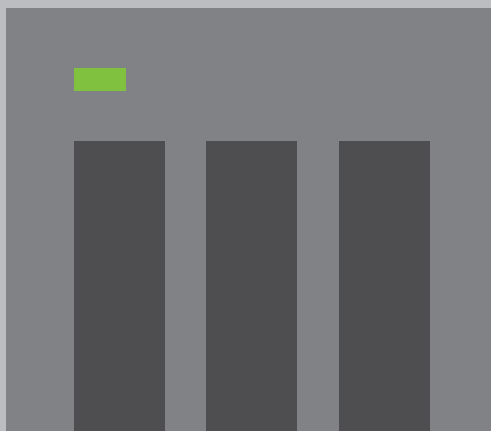


2 0 2 3

# Przewodnik po zabezpieczeniach



2 0 2 3

Przewodnik po zabezpieczeniach

# INDEKS

- 1 Wstęp
- 2 Typowe ataki
- 3 Podstawowe pojęcia dotyczące sprzętu sieciowego
- 4 Różne metody nawiązywania połączeń z serwerem NAS przez Internet

## Unikanie dostępu do serwera NAS przez Internet

- 8 Prawidłowe podłączenie serwera NAS
- 9 Sprawdzanie ustawień routera
- 12 Sprawdzanie ustawień serwera NAS
- 15 Lista kontrolna ustawień sieciowych

## Ustawienia zabezpieczeń serwera NAS

- 17 Konfigurowanie powiadomień systemowych
- 24 Włączanie automatycznej aktualizacji oprogramowania układowego (QTS / QuTS hero)
- 25 Ustawienia aktualizacji aplikacji
- 27 Wyłączanie lub usuwanie niepotrzebnych funkcji
- 29 Wyłączanie usług Telnet / SSH
- 30 Zwiększanie bezpieczeństwa konta systemowego
- 34 Ustawianie zasad zarządzania hasłami
- 35 Włączanie ochrony dostępu (do adresu IP / konta)
- 36 Włączanie weryfikacji dwuetapowej (2SV)
- 39 Zmiana domyślnych portów
- 40 Wyświetlanie dzienników dostępu
- 41 Instalowanie i włączanie aplikacji zabezpieczających
- 42 Security Counselor
- 45 Malware Remover
- 46 QuFirewall
- 51 Włączanie zaplanowanych migawek
- 53 Ustawianie zasad usuwania migawek
- 54 Lista kontrolna ustawień zabezpieczeń serwera NAS

Często zadawane pytania | 58

Firma QNAP przywiązuje dużą wagę do kwestii bezpieczeństwa. W obliczu rosnących zagrożeń QNAP stale udoskonala sprzęt i oprogramowanie, co pozwala dostarczać użytkownikom rozwiązania, które są zarówno bezpieczne, jak i wygodne.

Obsługą problemów związanych z bezpieczeństwem produktów QNAP zajmuje się zespół ds. reagowania na incydenty naruszeń bezpieczeństwa (ang. PSIRT, Product Security Incident Response Team). Oprócz obsługi incydentów związanych z cyberbezpieczeństwem zespół PSIRT zarządza zgłaszaniem, badaniem i naprawianiem luk w zabezpieczeniach różnych produktów oraz przekazuje odpowiednie informacje w tym zakresie.

Firma QNAP angażuje się również w udoskonalanie zabezpieczeń produktów. W przeszłości podczas projektowania produktów głównie skupiano się na zapewnieniu wygody ich użytkowania i łatwości konfiguracji. W ostatnich latach wzrosła liczba cyberataków na urządzenia połączone z siecią. W związku z tym zmieniała się również perspektywa projektowania produktów QNAP na rzecz zapewnienia „bezpieczeństwa od samego początku”. Obecnie nasze produkty pełnią funkcję „strażnika”, który pozwala użytkownikom radzić sobie z powiązаныmi zagrożeniami.

**Ten samouczek ułatwia prawidłowe skonfigurowanie serwera NAS pod kątem poprawy bezpieczeństwa. W przypadku jakichkolwiek pytań należy skontaktować się z naszym zespołem pomocy technicznej:**



Aby uzyskać informacje o lukach w zabezpieczeniach produktów i zdarzeniach związanych z bezpieczeństwem, należy zasubskrybować komunikaty informacyjne QNAP:

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



Obsługa klienta QNAP:

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



Aby skutecznie się bronić przed cyberatakami, należy wiedzieć, w jaki sposób są przeprowadzane. Większość ataków na serwery NAS jest przeprowadzanych przez Internet. Wyróżniamy głównie dwa typy tych ataków: „łamanie haseł” i „wykorzystywanie luk w zabezpieczeniach”. Ataki na luki w zabezpieczeniach można podzielić na kategorie „N-day” i „0-day”.

Do kategorii „N-day” należy większość obecnie przeprowadzanych ataków, w ramach których są wykorzystywane „załatane” luki w zabezpieczeniach. Skuteczna obrona przed takimi atakami polega na instalowaniu najnowszych aktualizacji i poprawek oraz stałym dbaniu o aktualność tych zabezpieczeń.

W ramach ataków „0-day” są wykorzystywane nieznanne luki w zabezpieczeniach. Dostawcy mogą udostępniać poprawki dopiero po wykryciu takich ataków. Jedyną skuteczną metodą obrony przed takimi atakami polega na uniemożliwieniu nawiązania połączenia z urządzeniem.

W poniższej tabeli przedstawiono działania użytkowników podejmowane w odpowiedzi na różne ataki.

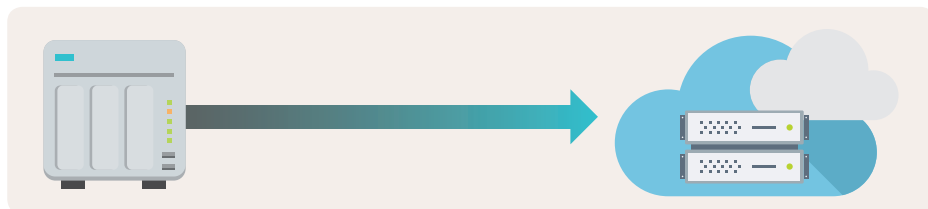
Odpowiedź	Ataki		
	Łamanie haseł	Atak na lukę w zabezpieczeniach (N-day)	Atak na lukę w zabezpieczeniach (0-day)
Unikanie dostępu przez Internet	V	V	V
Aktualizowanie oprogramowania (systemu i aplikacji)	X	V	Δ
Włączenie automatycznych aktualizacji (systemu i aplikacji)	X	V	Δ
Używanie silnych haseł do wszystkich kont	V	X	X
Wyłączenie domyślnego konta „admin”	V	X	X
Włączenie weryfikacji 2-etapowej	V	X	X
Włączenie ochrony dostępu	Δ	X	X
Włączenie zapory	Δ	Δ	Δ
Odbieranie powiadomień systemowych	Δ	Δ	Δ
Zmiana domyślnych portów	Δ	Δ	Δ
Wyłączenie/usunięcie niepotrzebnych funkcji	Δ	Δ	Δ
V: Skuteczna X: Nieskuteczna Δ: Potencjalnie skuteczna (umożliwia złagodzenie skutków lub zmniejszenie prawdopodobieństwa ataku)			

Działanie „Unikanie dostępu przez Internet” pozwala skutecznie uniemożliwić nawiązanie połączenia z urządzeniem w celu przeprowadzenia ataku. Na początku tego samouczka znajdują się informacje dotyczące działania „Unikanie dostępu przez Internet”, po których następuje wyczerpujące omówienie ustawień zabezpieczeń serwera NAS, pozwalających poprawić efektywność ochrony serwera NAS.

# Podstawowe pojęcia dotyczące sprzętu sieciowego

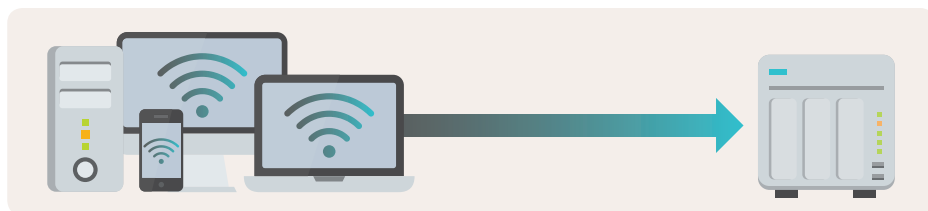
Serwer NAS jest urządzeniem sieciowym, w którym ruch danych odbywa się w dwóch kierunkach.

## 01 | Połączenie zewnętrzne z serwerem NAS



Prawidłowe działanie serwera NAS zazwyczaj wymaga połączenia zewnętrznego. Jest ono potrzebne na przykład do działania podstawowych funkcji systemu, takich jak automatyczne aktualizacje i powiadomienia. Ponadto w przypadku konieczności tworzenia kopii zapasowych danych z serwera NAS w chmurze publicznej lub używania serwera NAS do tworzenia kopii zapasowych danych z innych urządzeń, chmur publicznych (takich jak maszyny wirtualne albo usługi Google Workspace czy Microsoft 365), komputerów lub serwerów serwer NAS musi mieć możliwość inicjowania połączeń wychodzących.

## 02 | Inne urządzenia (takie jak komputery, urządzenia mobilne lub serwery), które nawiązują połączenia z serwerem NAS



Korzystanie z dowolnych funkcji lub usług udostępnianych przez serwer NAS, na przykład uzyskiwanie dostępu do plików bądź otwieranie interfejsu ustawień, wymaga zapewnienia możliwości inicjowania połączeń z serwerem NAS.

Jeśli dany router nie obsługuje funkcji DMZ lub UPnP albo funkcji przekierowania portów, ruch z Internetu będzie blokowany. Dostęp do serwera NAS będą miały tylko urządzenia znajdujące się w sieci lokalnej.

Jeśli router będzie włączony, a wyżej wymienione funkcje skonfigurowane, wszyscy użytkownicy Internetu będą mogli się połączyć z otwartym portem, skorzystać z przekierowania do serwera NAS zgodnie z regułami na routerze, a następnie się zalogować i normalnie korzystać z potrzebnych funkcji. Jednak umożliwi to również hakerom przeprowadzanie ataków polegających na łamaniu haseł lub wykorzystywaniu luk w oprogramowaniu, co wiąże się z zagrożeniem bezpieczeństwa.

# Różne metody nawiązywania połączeń zdalnych z serwerem NAS

## 01 | Włączenie i skonfigurowanie funkcji DMZ lub UPnP albo funkcji przekierowania portów na routerze

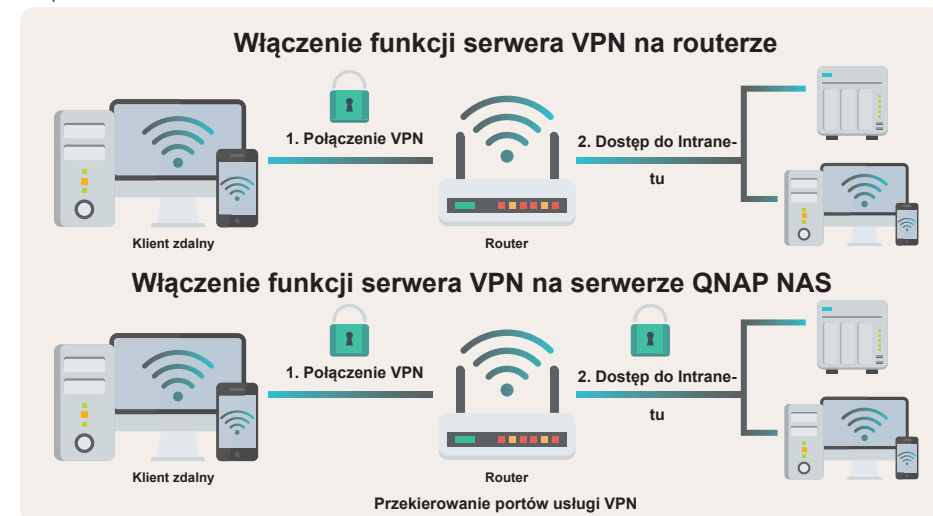
Korzystanie z tej metody wiąże się z zagrożeniami bezpieczeństwa. **QNAP odradza korzystanie z tej metody\***, chyba że użytkownik ma świadomość powiązanych zagrożeń oraz specjalistyczną wiedzę z zakresu konfiguracji sieci. Router będzie przekazywał ruch do urządzeń znajdujących się w intranecie. Jeśli między routerem a serwerem NAS nie zostanie zainstalowana zapora blokująca szkodliwy ruch, hakerzy będą mogli łatwo przeprowadzać ataki w sieci. Jednak nawet zainstalowanie zapory (czy to podstawowej zapory czy rozwiązania klasy korporacyjnej) nie gwarantuje, że każdy atak zostanie zablokowany.

\* QNAP zaleca otwarcie tylko portów usługi VPN zagrożonych w niewielkim stopniu, umożliwiających łączenie się z Internetem. Pozostałe porty usług, zagrożone w większym stopniu, takie jak usługi zarządzania systemem oraz usługi SMB i SSH, nie powinny być łatwo dostępne przez Internet.



## 02 | Włączenie funkcji serwera VPN na routerze lub serwerze QNAP NAS

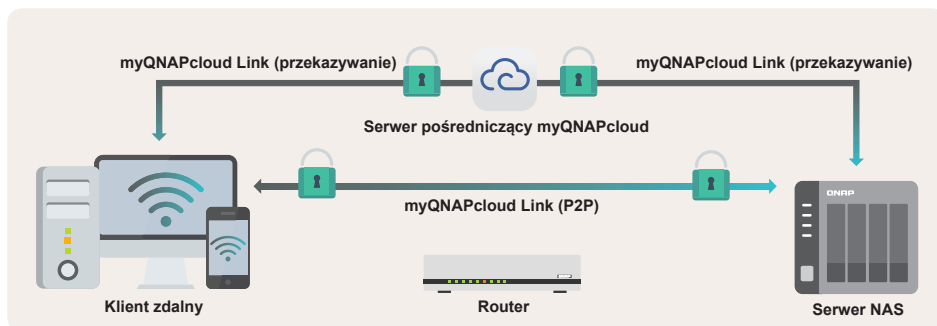
Niektóre routery obsługują funkcje serwera VPN (na przykład routery z serii QNAP QHora i QMiro). Serwer QNAP NAS również obsługuje wiele serwerów VPN. Po włączeniu i prawidłowym skonfigurowaniu tej funkcji można uzyskiwać dostęp przez Internet do wszystkich urządzeń w intranecie za pomocą szyfrowanego połączenia VPN z serwerem VPN. Takie rozwiązanie zapewnia wysoki poziom bezpieczeństwa.





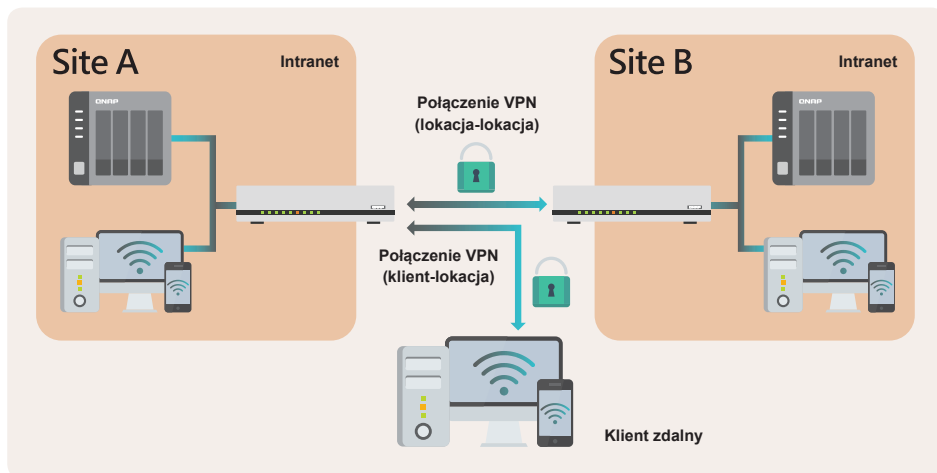
### 03 | Korzystanie z bezpiecznego połączenia myQNAPcloud Link

Usługa myQNAPcloud Link umożliwia bezpośrednie otwieranie usługi NAS w celu łączenia się przez Internet, dlatego konfiguracja routera nie jest wymagana. W zależności od środowiska sieciowego myQNAPcloud Link nawiąże połączenie za pomocą serwera pośredniczącego lub technologii peer-to-peer (P2P). Połączenie jest szyfrowane w celu zapewnienia bezpieczeństwa.




### 04 | Korzystanie z produktów VPN typu SD-WAN lub lokacja-lokacja

W przeciwieństwie do wymienionej wcześniej funkcji serwera VPN (umożliwiającej utworzenie sieci VPN typu klient-lokacja) produkt VPN typu SD-WAN lub lokacja-lokacja pozwala nawiązać bezpieczne, szyfrowane połączenie VPN między co najmniej dwoma routerami znajdującymi się w różnych lokalizacjach. Mówiąc krótko, urządzenia w sieci VPN typu lokacja-lokacja mogą łączyć się ze sobą, tak jakby znajdowały się w tym samym intranecie. Dzięki temu rozwiązanie to doskonale zaspokaja potrzeby użytkowników, którzy przebywają w różnych lokalizacjach. Sieć VPN typu klient-lokacja zapewnia dostęp do serwera NAS w dowolnym miejscu.



Poniższa tabela podsumowująca ułatwia wybór odpowiedniej metody połączenia. QNAP oferuje różne rozwiązania bezpiecznych połączeń, które pozwalają zaspokoić potrzeby użytkowników.

Metoda połączenia	Zalety	Wady	Cechy użytkowników
Włączenie i skonfigurowanie na routerze funkcji DMZ / przekierowania portów protokołu UPnP	<ul style="list-style-type: none"><li>Najszybsze połączenie</li></ul>	<ul style="list-style-type: none"><li>Podatność na cyberataki</li><li>Brak ochrony przed atakami 0-day</li></ul>	<ul style="list-style-type: none"><li>Mają pełną świadomość powiązanych zagrożeń</li><li>Są obeznani z ustawieniami sieci</li><li>Mają wiele kopii zapasowych ważnych danych</li><li>Mają plan odzyskiwania danych po awarii</li></ul>
Włączenie serwera VPN na routerze*	<ul style="list-style-type: none"><li>Względna prostota konfiguracji</li></ul>	<ul style="list-style-type: none"><li>Brak powiadomienia o niepowodzeniu logowania, funkcji automatycznego blokowania i funkcji zapory</li><li>Mniej obsługiwanych protokołów VPN</li><li>Wydajność ograniczona przez sprzęt routera</li></ul>	<ul style="list-style-type: none"><li>Nie są obeznani z ustawieniami sieci</li><li>Nie zależy im na szybkości transmisji</li></ul>
Włączenie funkcji serwera VPN na serwerze QNAP NAS*	<ul style="list-style-type: none"><li>Obsługa wielu protokołów VPN</li><li>Zgodność z zaporą NAS (QuFirewall)</li><li>Obsługa powiadamiania o niepowodzeniu logowania i automatycznego blokowania</li></ul>	<ul style="list-style-type: none"><li>Nieco bardziej skomplikowane ustawienia</li></ul>	<ul style="list-style-type: none"><li>Są obeznani z ustawieniami sieci</li><li>Często muszą uzyskiwać dostęp do wielu plików w Internecie</li></ul>
 <b>Korzystanie z bezpiecznego połączenia myQNAPcloud Link</b>	<ul style="list-style-type: none"><li>Najłatwiejsza konfiguracja</li><li>Obsługa kontroli dostępu</li><li>Serwer NAS nie musi być dostępny przez Internet</li></ul>	<ul style="list-style-type: none"><li>Wolniejsze połączenie</li></ul>	<ul style="list-style-type: none"><li>Nie są obeznani z ustawieniami sieci</li><li>Rzadko korzystają z serwera NAS przez Internet</li><li>Środowisko sieciowe, w którym nie można uzyskać adresu IP WAN</li></ul>
Korzystanie z produktów VPN typu SD-WAN lub lokacja-lokacja*	<ul style="list-style-type: none"><li>Po skonfigurowaniu tej metody użytkownicy intranetu nie odczuwają obniżenia komfortu</li><li>Obsługa sieci VPN klient-lokacja</li></ul>	<ul style="list-style-type: none"><li>Wymagane dodatkowe urządzenia</li></ul>	<ul style="list-style-type: none"><li>Wymagają dostępu w wielu punktach i zdalnego tworzenia kopii zapasowych</li><li>Korzystają z udoskonalonych aplikacji</li></ul>

\* Technologie obsługiwane przez serwer QNAP NAS:

myQNAPcloud Link / serwery VPN (L2TP/IPsec, OpenVPN, WireGuard, QBelt) / QuWAN SD-WAN

\* Technologie obsługiwane przez router QNAP:

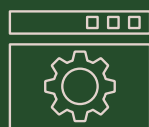
QuWAN SD-WAN / serwery VPN (L2TP/IPsec, OpenVPN, WireGuard, QBelt)

# Dotyczy typowych routerów domowych

# 01

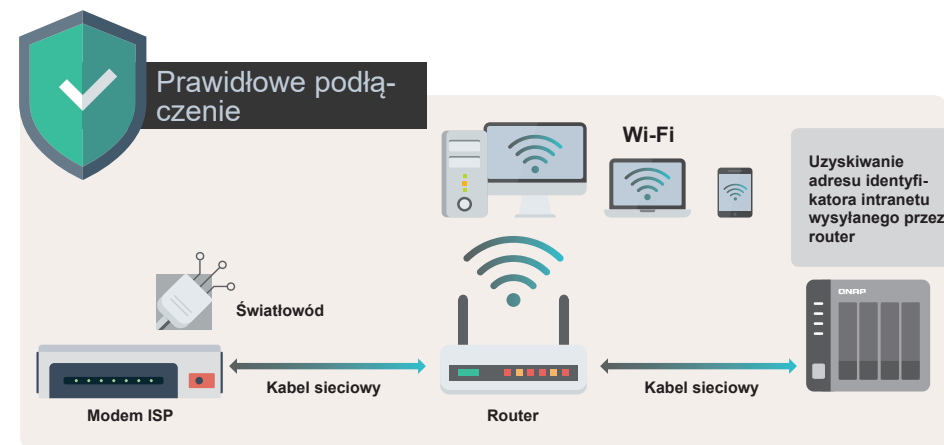
Przewodnik po ustawieniach zabezpieczeń serwera NAS

## Unikanie dostępu do serwera NAS przez Internet

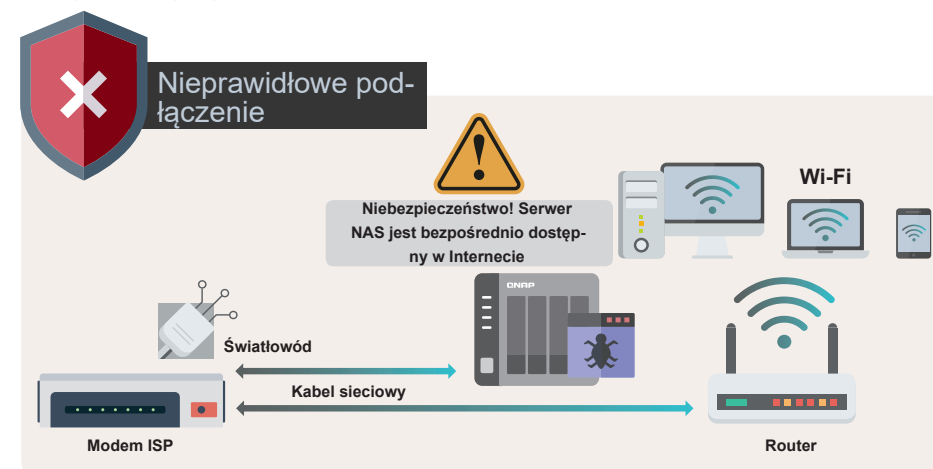


## Prawidłowe połączenie serwera NAS

Upewnij się, że serwer NAS jest połączony z routerem. Przy prawidłowej konfiguracji router może automatycznie blokować połączenia z Internetu, co pozwala ukryć serwer NAS i uniknąć cyberataków.



Jeśli serwer NAS zostanie połączony z modemem dostarczanym przez dostawcę usług internetowych, będzie bezpośrednio uzyskiwać adres IP WAN. W takim przypadku wszyscy użytkownicy (w tym hakerzy) będą mogli się połączyć z serwerem NAS przez Internet, a nawet próbować złamać zabezpieczenia i przeprowadzić atak.

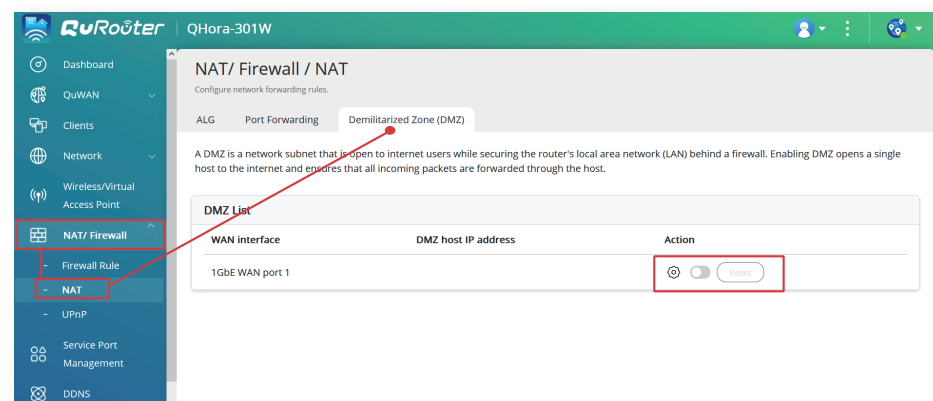
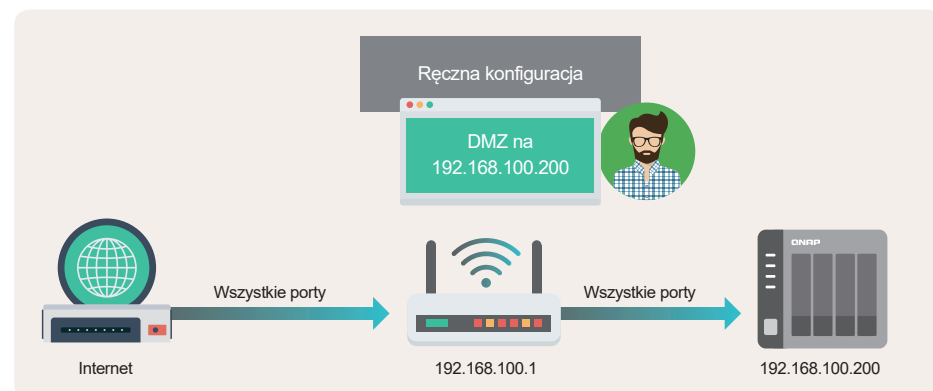


# Sprawdzanie ustawień routera

Teoretycznie w Internecie nie można się połączyć bezpośrednio z urządzeniem znajdującym się za routerem. Jednak po włączeniu funkcji „DMZ” (Strefa zdemilitaryzowana), „Przekierowanie portów” lub „UPnP” (Universal Plug and Play) router będzie przekierowywać pakiety do wybranego urządzenia zgodnie z ustawionymi regułami, co spowoduje ujawnienie urządzenia w Internecie. Jeśli następujące funkcje nie są potrzebne, należy je **wyłączyć**.

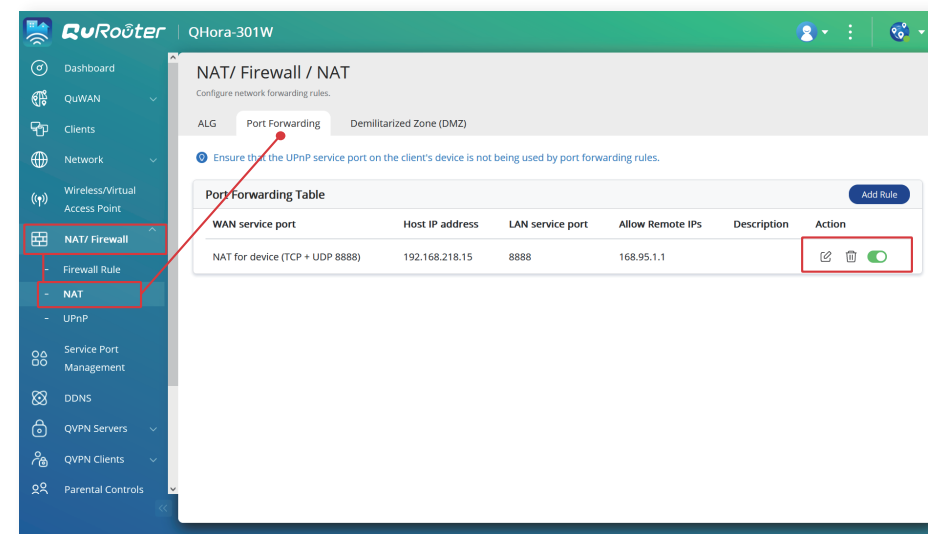
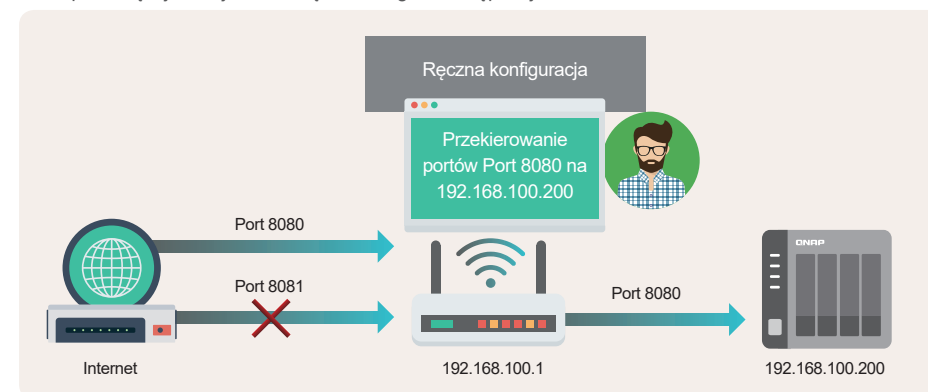
## 01 | Sprawdzanie funkcji DMZ (Strefa zdemilitaryzowana)

Włączenie tej funkcji powoduje bezpośrednie otwarcie wszystkich portów usług na wybranym urządzeniu. Można wtedy uzyskać pełny dostęp do tych portów przez Internet. Aby zmniejszyć zagrożenie bezpieczeństwa, wyłączyć tę funkcję.



## 02 | Sprawdzanie przekierowania portów

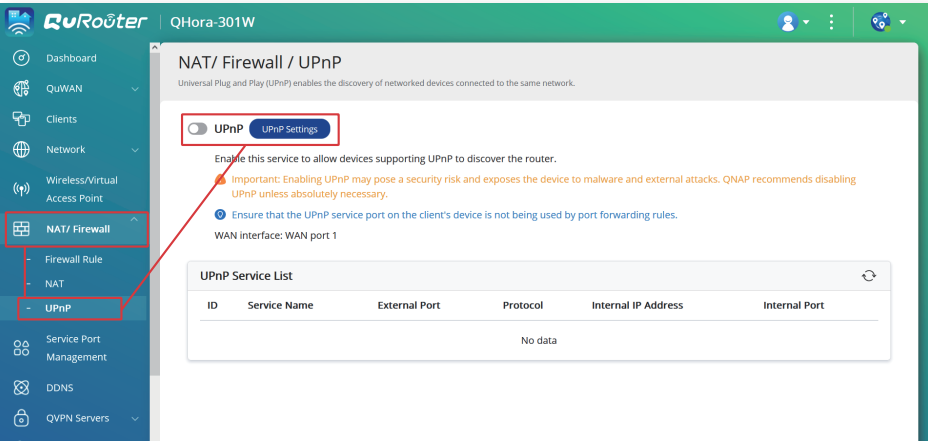
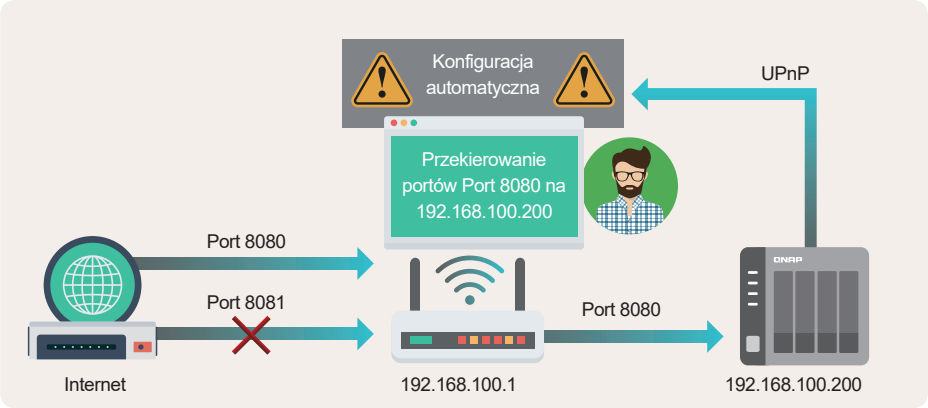
Ta funkcja umożliwia otwarcie w Internecie określonego portu usługi na urządzeniu, co umożliwia wszystkim użytkownikom uzyskiwanie dostępu do odpowiednich usług przez Internet. Jednak pozwala to również hakerom przeprowadzać ataki na otwarte usługi. Z tego względu zaleca się, aby najpierw wyłączyć wszystkie reguły przekierowania portów, a następnie skonfigurować ustawienia zabezpieczeń serwera NAS, po czym wykonać kopię zapasową ważnych danych. W dalszej kolejności można utworzyć — za pomocą tej funkcji — niezbędne usługi i udostępnić je w Internecie.





## 03 | Sprawdzanie funkcji UPnP (Universal Plug and Play)

Ta funkcja działa tak jak automatyczne przekierowanie portów. Po włączeniu tej funkcji można automatycznie skonfigurować na urządzeniu przekierowanie portów przy użyciu odpowiedniego protokołu. Korzystanie z tej funkcji wiąże się z poważnymi zagrożeniami, ponieważ może ona ujawnić usługi w Internecie bez wiedzy użytkownika lub zostać wykorzystana przez hakerów, którzy mogą włączyć ukryte możliwości dostępu. W celu zwiększenia bezpieczeństwa należy wyłączyć tę funkcję.



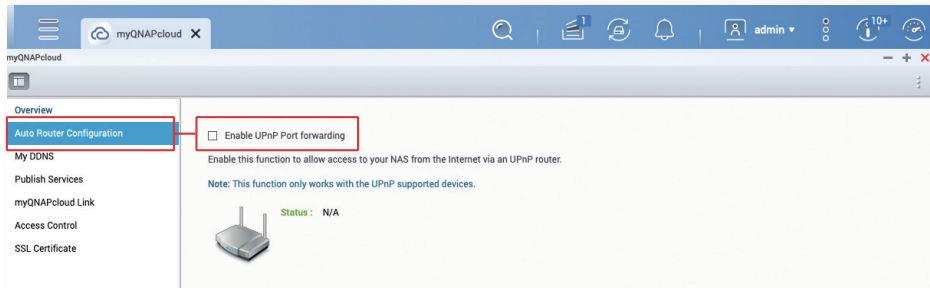
## 01 | Automatyczna konfiguracja routera, przekierowanie portów UPnP

Niektóre routery nie umożliwiają wyłączania funkcji UPnP, dlatego należy sprawdzić ustawienie „Automatyczna konfiguracja routera” na serwerze NAS, aby upewnić się, że ta funkcja jest wyłączona.

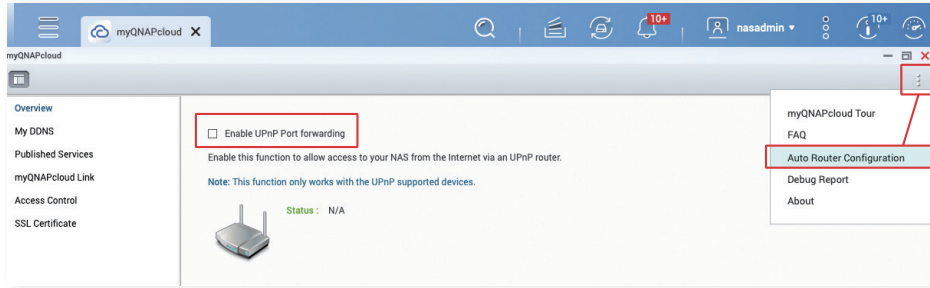
**\* Ta funkcja jest domyślnie wyłączona w systemie QTS 4.5.0 / QuTS hero h4.5.3 i nowszych wersjach.**

### Aby wyłączyć funkcję „Automatyczna konfiguracja routera”:

1. Zaloguj się do internetowego interfejsu zarządzania systemem QTS / QuTS hero, używając konta administratora.
2. Otwórz menu w lewym górnym rogu i kliknij opcję „myQNAPcloud”.
3. **QTS 5.0.0 / QuTS hero h5.0.0 i starsze wersje:** Kliknij opcję „Automatyczna konfiguracja routera” w menu po lewej stronie



**QTS 5.0.1 / QuTS hero h5.0.1 i nowsze wersje:** Kliknij ikonę menu w prawym górnym rogu i wybierz opcję „Automatyczna konfiguracja routera”.



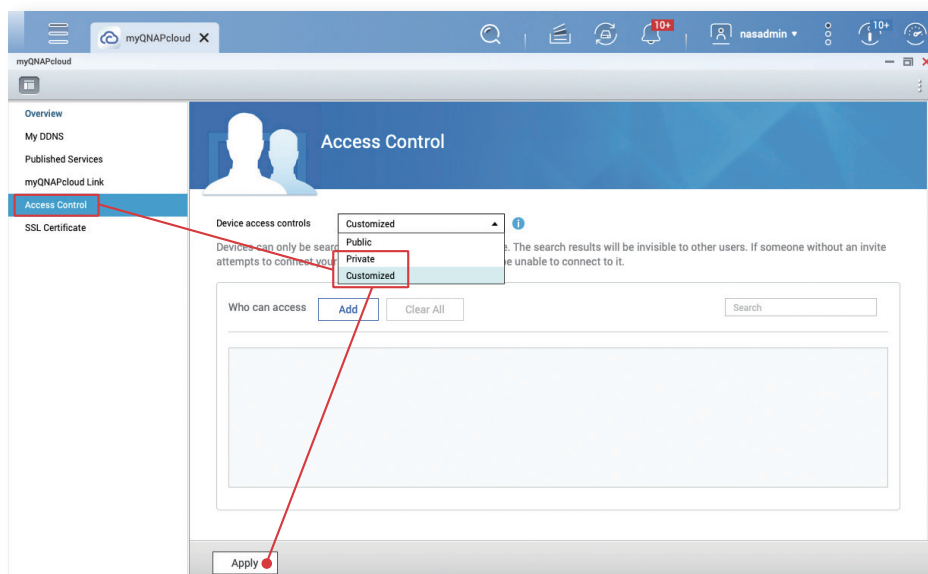
4. Na stronie ustawień „Automatyczna konfiguracja routera” usuń zaznaczenie opcji „Włącz przekierowanie portów UPnP” i kliknij opcję „Zastosuj”.

## 02 | Kontrola dostępu za pomocą usługi myQNAPcloud Link

myQNAPcloud Link to usługa w chmurze oferowana przez firmę QNAP, która pozwala korzystać z bezpiecznego połączenia. Użytkownicy mogą łączyć się z serwerem QNAP NAS za pośrednictwem wybranej nazwy urządzenia myQNAPcloud. W usłudze myQNAPcloud Link są dostępne ustawienia kontroli dostępu. Jeśli poziom dostępu jest ustawiony na wartość „Publiczny”, wszyscy użytkownicy, którzy znają nazwę urządzenia, mogą połączyć się z serwerem NAS za pomocą usługi myQNAPcloud Link. Z tego względu **zalecamy ustawienie poziomu dostępu na wartość „Prywatny” lub „Niestandardowy”**. W obu trybach użytkownicy muszą się zalogować za pomocą identyfikatora QNAP ID znajdującego się na liście dozwolonych, zanim będą mogli się bezpiecznie łączyć z usługami w chmurze przy użyciu usługi myQNAPcloud Link.

★ W systemie QTS 4.5.0 / QuTS hero h4.5.3 (i nowszych wersjach) domyślne ustawienie to „Niestandardowy”

1. Zaloguj się do internetowego interfejsu zarządzania systemem QTS / QuTS hero, używając konta administratora.
2. Kliknij menu w lewym górnym rogu i kliknij opcję „myQNAPcloud”.
3. Kliknij opcję „Kontrola dostępu” w menu po lewej stronie.
4. Na stronie ustawień „Kontrola dostępu” w obszarze „Kontrola dostępu do urządzenia” wybierz ustawienie „Prywatny” lub „Niestandardowy”, a następnie kliknij opcję „Zastosuj”.



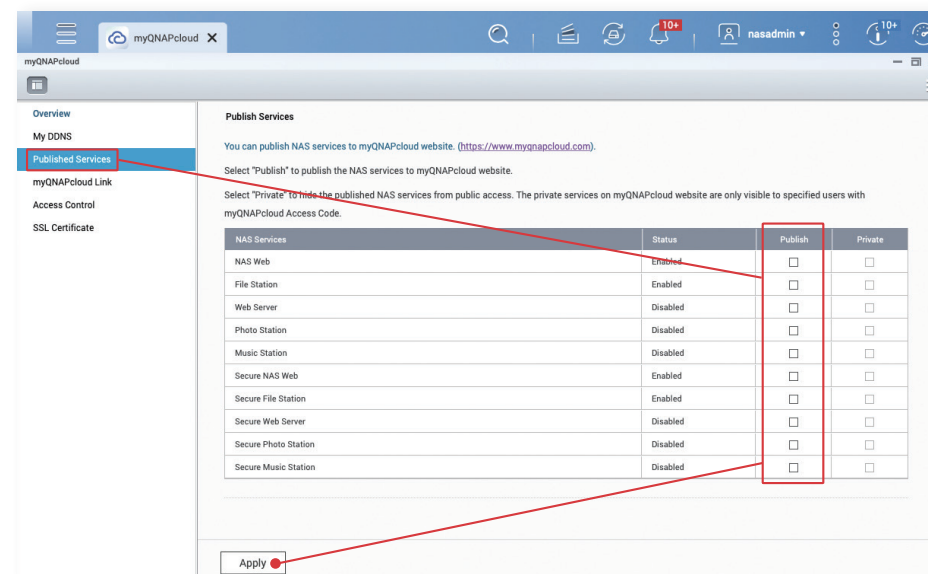
## 03 | Opublikowane usługi

Opublikowane usługi ułatwiają użytkownikom korzystanie z potrzebnych funkcji w witrynie myQNAPcloud, jednak stanowią również zagrożenie bezpieczeństwa. Jeśli używanie tej funkcji nie jest wymagane, zaleca się jej wyłączenie w celu zwiększenia bezpieczeństwa.

★ Ta funkcja jest domyślnie wyłączona w systemie QTS 4.5.0 / QuTS hero h4.5.3 i nowszych wersjach.

### Funkcja „Opublikowane usługi”:

1. Zaloguj się do internetowego interfejsu zarządzania systemem QTS / QuTS hero, używając konta administratora.
2. Kliknij menu w lewym górnym rogu i kliknij opcję „myQNAPcloud”.
3. Kliknij opcję „Opublikowane usługi” w menu po lewej stronie.
4. W polu „Opublikuj” wyczyść zaznaczenie wszystkich opcji i kliknij przycisk „Zastosuj”.



# Lista kontrolna ustawień sieciowych

## Powiązane ze sprzętem

- ☐ Połączony serwer NAS znajduje się za routerem
- ☐ Serwer NAS uzyskuje adres IP intranetu







## Router

- ☐ Wyłącz funkcję „DMZ” routera
- ☐ Wyłącz regułę „Przekierowanie portów” routera
- ☐ Wyłącz funkcję „UPnP” routera

## Serwer NAS

- ☐ Wyłącz funkcję „Automatyczna konfiguracja routera (przekierowanie portów UPnP)” na serwerze NAS
- ☐ W obszarze „Kontrola dostępu za pomocą usługi myQNAPcloud Link” wybierz ustawienie „Prywatny” lub „Niestandardowy”
- ☐ Wyłącz funkcję „Opublikowane usługi”  
Po sprawdzeniu i zastosowaniu powyższych ustawień serwer QNAP NAS nie będzie widoczny w Internecie, a ryzyko ataków hakerów znacznie się zmniejszy. Zapoznaj się z kolejnymi częściami i sprawdź pozostałe ustawienia, które pozwalają podnieść poziom bezpieczeństwa serwera QNAP NAS.

W przypadku potrzeby uzyskiwania dostępu do serwera NAS przez Internet warto rozważyć trzy poniższe bezpieczne rozwiązania:

		
myQNAPcloud Link	QVPN Service	QuWAN SD-WAN
		
Dowiedz się więcej	Dowiedz się więcej	Dowiedz się więcej

# 02

Przewodnik po ustawieniach zabezpieczeń serwera NAS



## Ustawienia zabezpieczeń serwera NAS



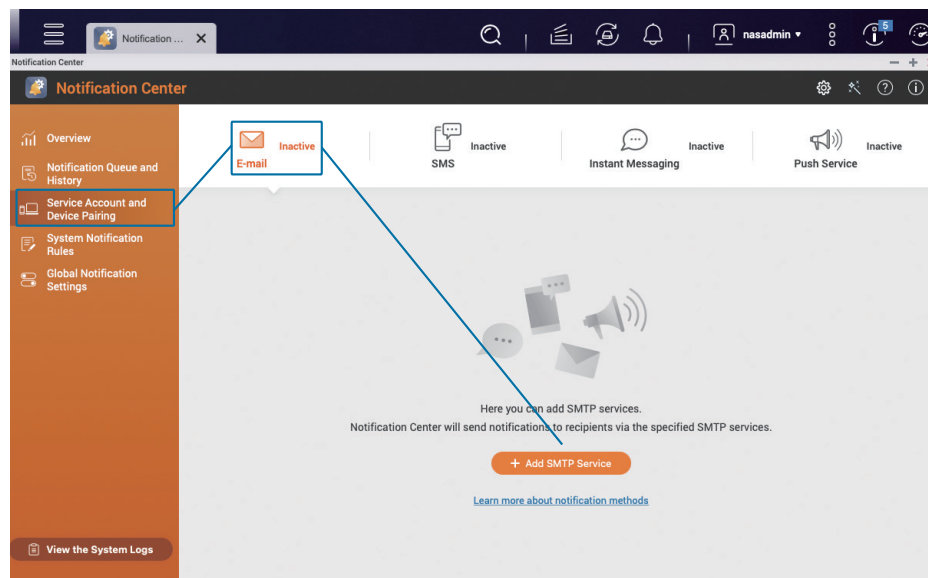
# Konfigurowanie powiadomień systemowych

Wbudowane Centrum powiadomień umożliwia wysyłanie powiadomień wypychanych, co pozwala użytkownikom monitorować status serwera NAS i sprawnie reagować na wykryte nieprawidłowości.

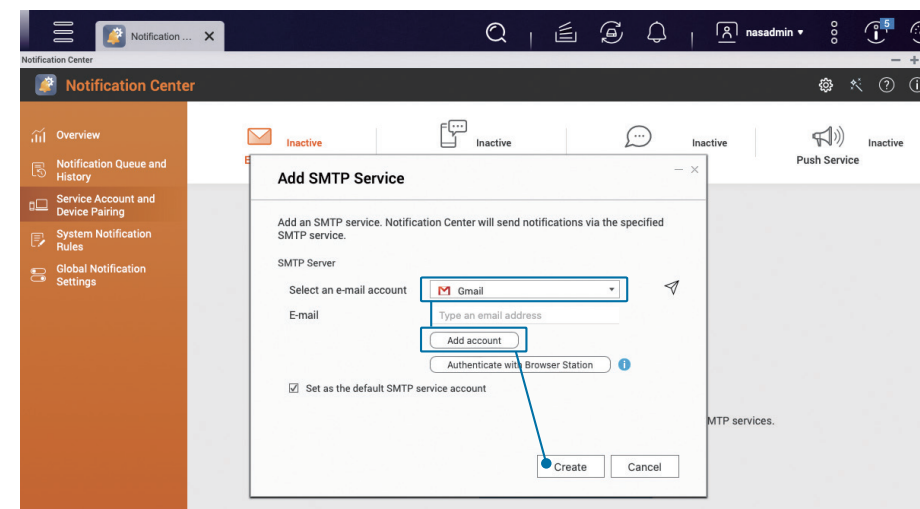
Poniższe sekcje samouczka zawierają instrukcje dotyczące tworzenia dwóch podstawowych reguł typu „E-mail”, umożliwiających wysyłanie powiadomień o alertach i aktualizacjach oprogramowania układowego. W razie potrzeby można dodać kolejne reguły.

## 01 | Dodawanie metody powiadamiania „E-mail”

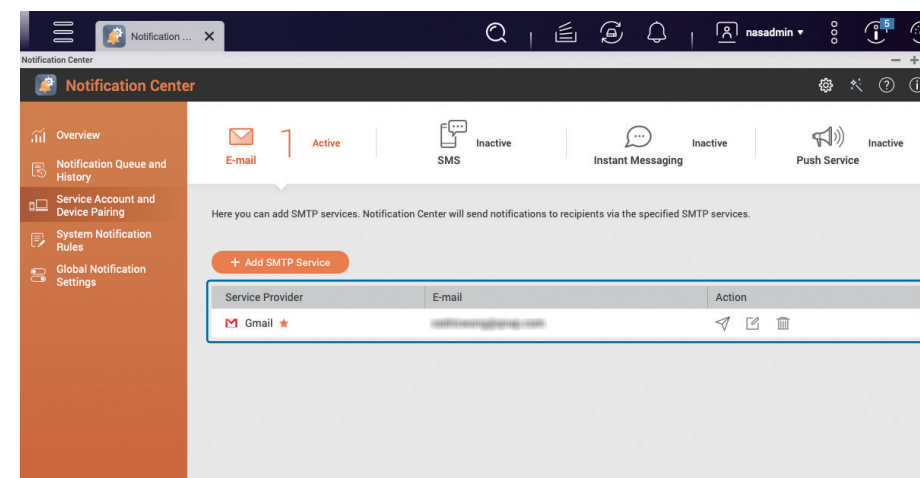
Otwórz obszar „Centrum powiadomień”, kliknij opcję „Konto usługi i parowanie urządzeń” w menu po lewej stronie, wybierz opcję „E-mail”, a następnie kliknij opcję „Dodaj usługę SMTP”.



Wybierz konto e-mail (w poniższym przykładzie użyto konta Gmail), kliknij opcję „Dodaj konto”, postępuj zgodnie z instrukcjami w procesie weryfikacji, a następnie kliknij opcję „Utwórz”.



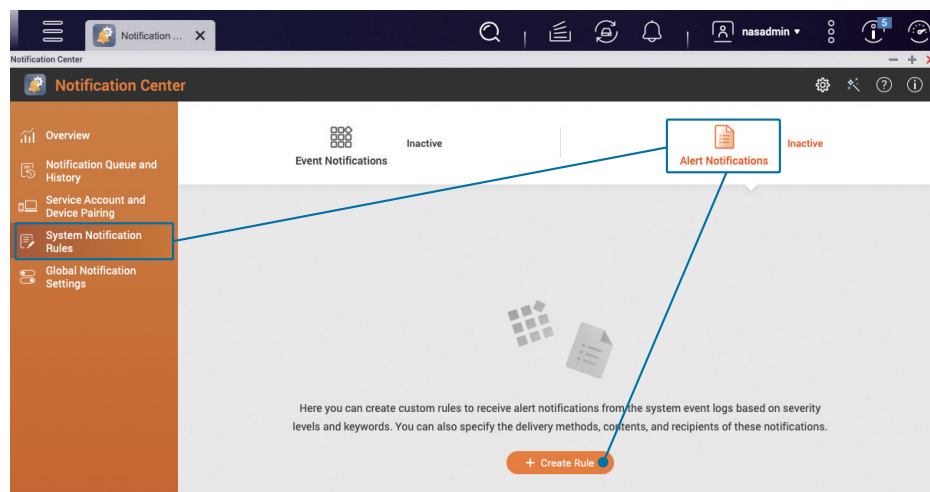
↓ Po wykonaniu tych czynności dodane konto e-mail zostanie wyświetlone na liście.



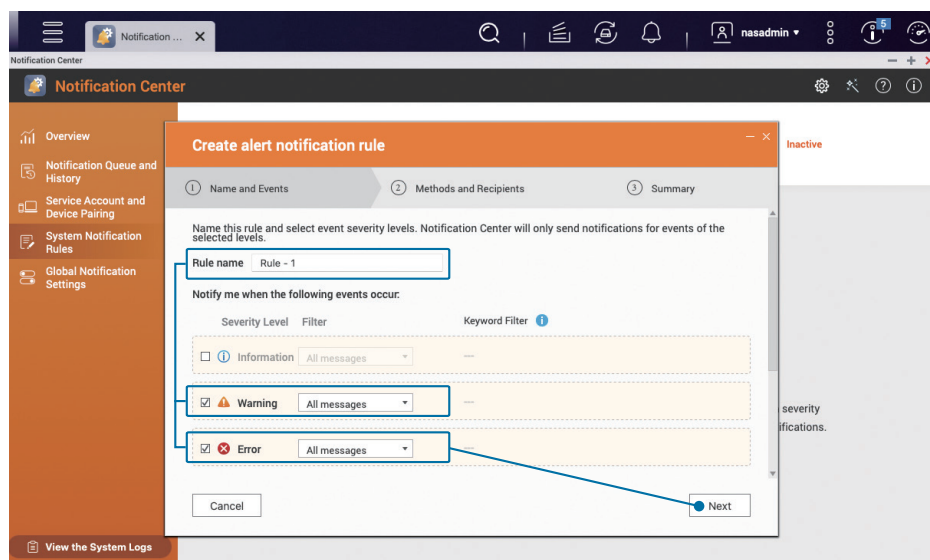


## 02 | Konfigurowanie „powiadomień o alertach”

W obszarze „Centrum powiadomień” w menu po lewej stronie kliknij opcję „Reguły powiadomień systemowych”, wybierz opcję „Powiadomienia o alertach” i kliknij opcję „Utwórz regułę”.

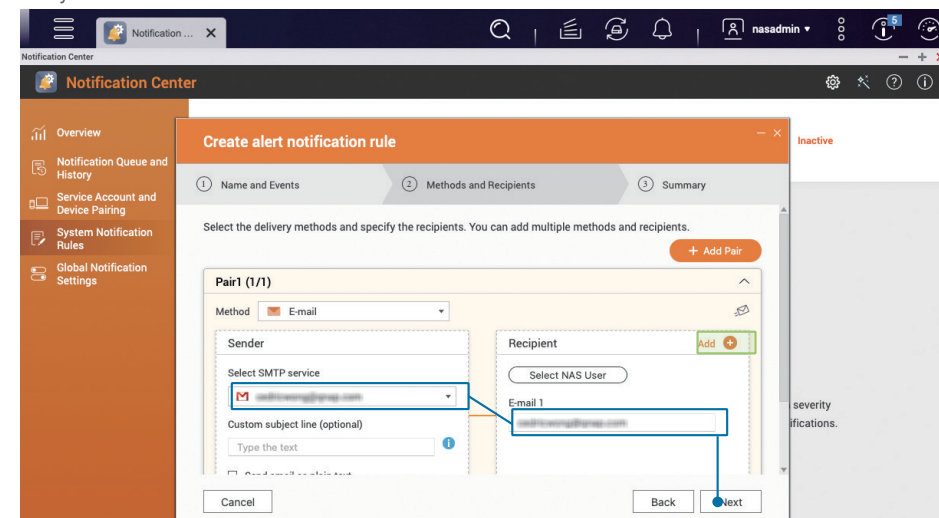


Odpowiednio zmodyfikuj nazwę w polu „Nazwa reguły”, zaznacz poziomy istotności „Ostrzeżenie” i „Błąd” i kliknij przycisk „Dalej”.

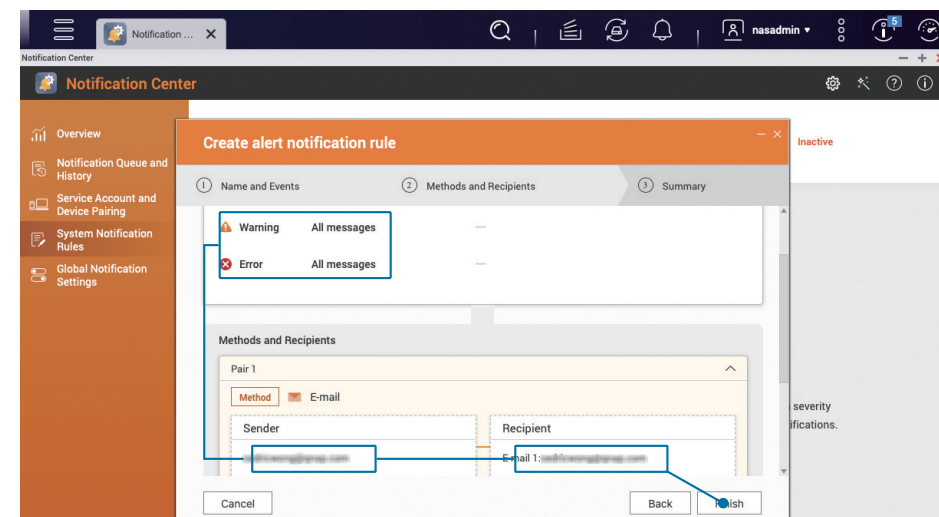


Ustaw metodę dostarczania i wybierz odbiorcę. W polu „Nadawca” w obszarze parowania wybierz dodane konto e-mail. Wprowadź adres e-mail w polu „Adres e-mail” w obszarze „Odbiorca”, a następnie kliknij przycisk „Dalej”.

W razie potrzeby możesz wprowadzić wielu odbiorców, klikając opcję „Dodaj +” w obszarze „Odbiorca”. Możesz także wybrać opcję „Dodaj parę”, aby skonfigurować równoczesne wysyłanie powiadomień różnymi metodami.



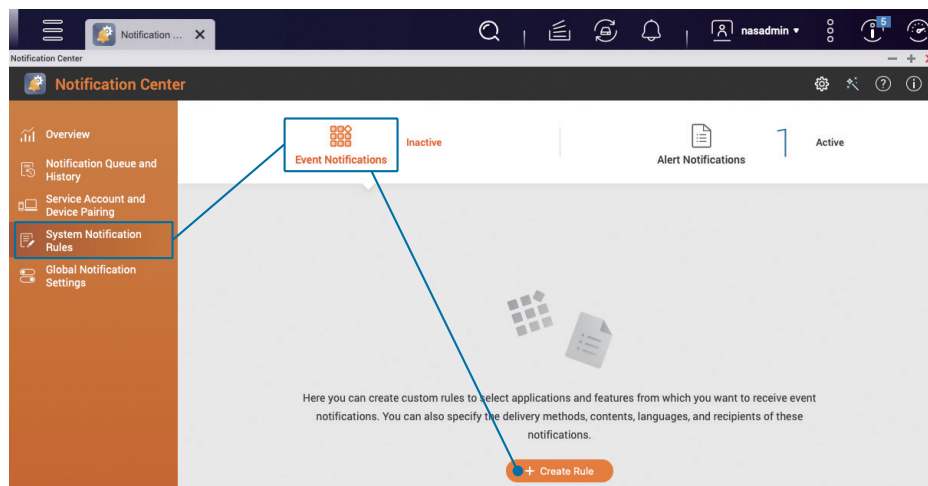
Sprawdź poprawność ustawień i kliknij opcję „Zakończ”. Konfigurowanie ustawień „Powiadomienia o alertach” zostanie zakończone.



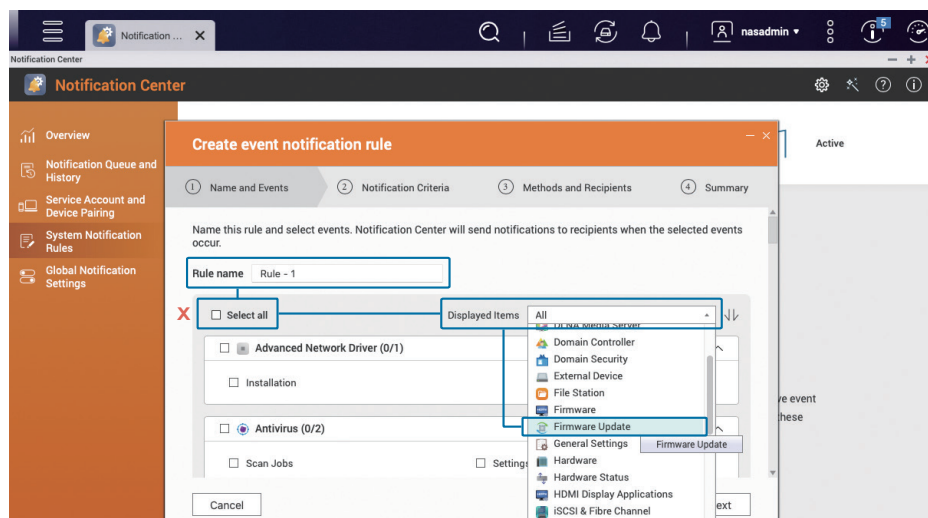


### 03 | Konfigurowanie „powiadomień o aktualizacjach oprogramowania układowego”

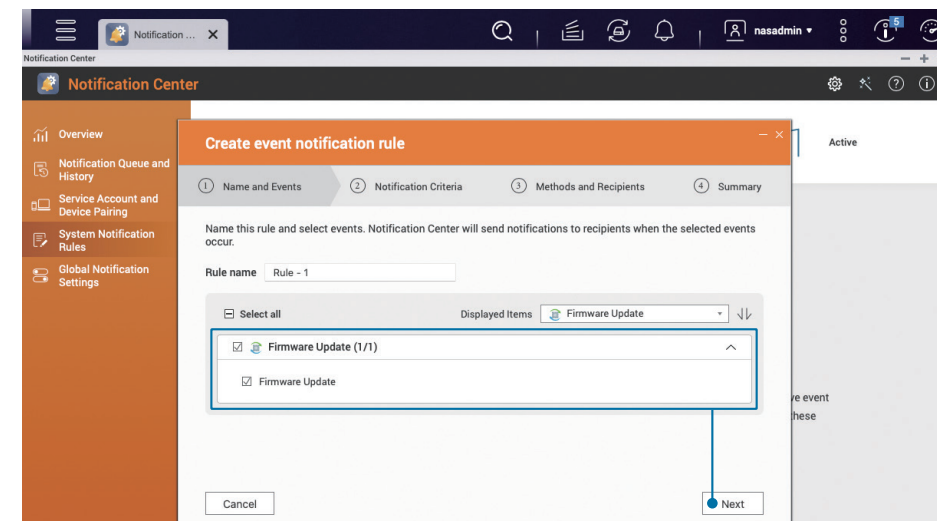
W obszarze „Centrum powiadomień” w menu po lewej stronie kliknij opcję „Reguły powiadomień systemowych”, wybierz opcję „Powiadomienia o zdarzeniach”, a następnie kliknij opcję „Utwórz regułę”.



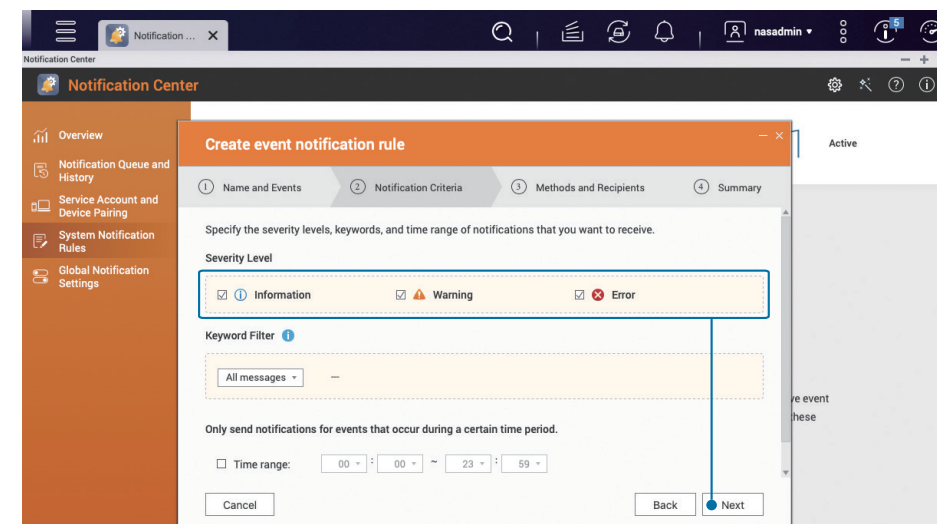
Odpowiednio zmodyfikuj nazwę w polu „Nazwa reguły”, usuń zaznaczenie opcji „Wybierz wszystkie”, wybierz opcję „Aktualizacja oprogramowania układowego” w obszarze „Wyświetlane elementy” po lewej stronie, a następnie wybierz opcję „Aktualizacja oprogramowania układowego” poniżej.



Zaznacz opcję „Aktualizacja oprogramowania układowego” i kliknij przycisk „Dalej”.

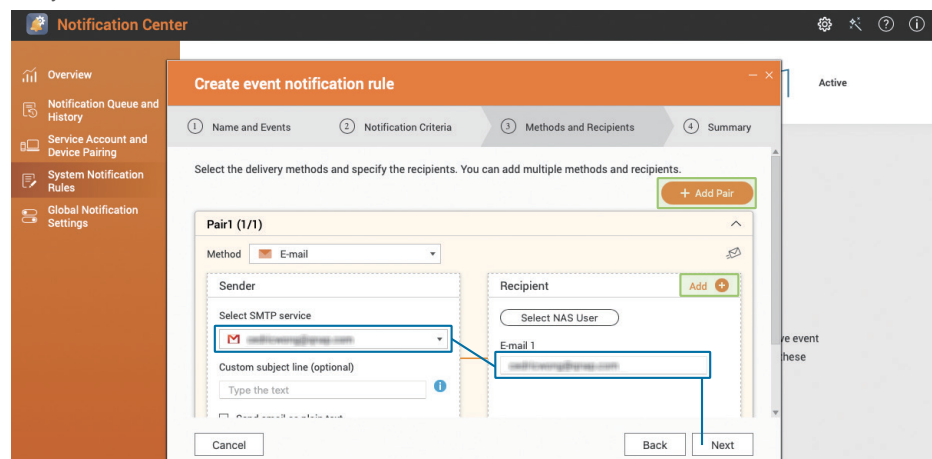


Zaznacz wszystkie poziomy istotności, w tym „Informacje”, „Ostrzeżenie” i „Błąd”, a następnie kliknij przycisk „Dalej”.

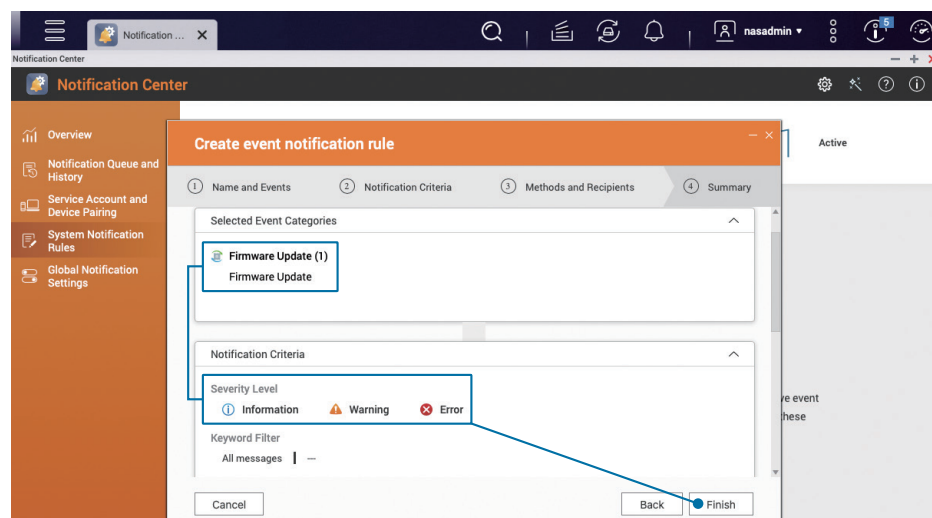


Ustaw metodę dostarczania i wybierz odbiorcę. Aktualnie jest ustawione tylko powiadomienie „E-mail”. W polu „Nadawca” w obszarze parowania wybierz dodane konto e-mail. Wprowadź adres e-mail w polu „Adres e-mail” w obszarze „Odbiorca”, a następnie kliknij przycisk „Dalej”.

W razie potrzeby możesz wprowadzić wielu odbiorców, klikając opcję „Dodaj +” w obszarze „Odbiorca”. Możesz także wybrać opcję „Dodaj parę”, aby skonfigurować równoczesne wysyłanie powiadomień różnymi metodami.



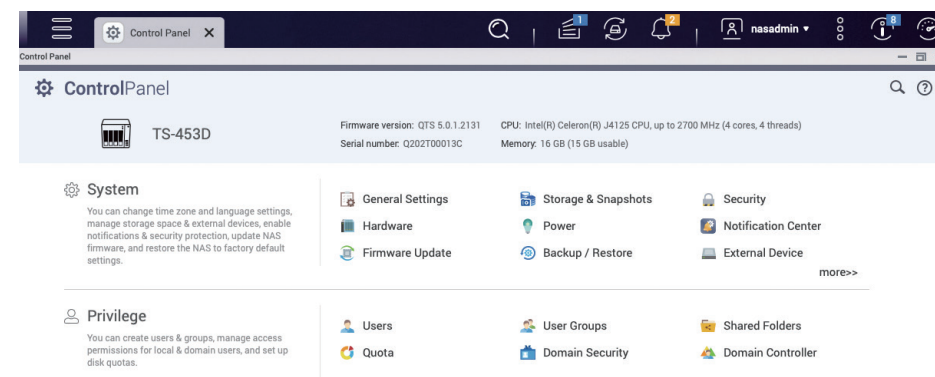
Sprawdź poprawność ustawień i kliknij opcję „Zakończ”, aby zakończyć konfigurowanie ustawień powiadomień „Aktualizacja oprogramowania układowego”.



# Włączanie automatycznej aktualizacji oprogramowania układowego (QTS / QuTS hero)

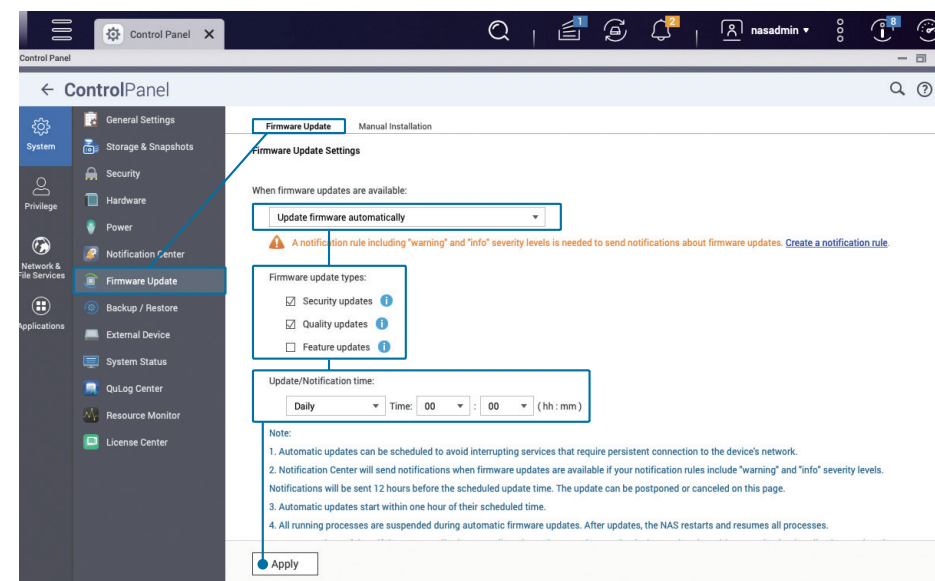
Funkcja automatycznej aktualizacji ułatwia instalowanie aktualizacji funkcji oraz poprawek błędów i luk w zabezpieczeniach.

Otwórz ekran „Panel sterowania” i kliknij opcję „Aktualizacja oprogramowania układowego”.




W obszarze „Ustawienia aktualizacji oprogramowania układowego” wybierz opcję „Automatycznie aktualizuj oprogramowanie układowe” i zaznacz opcję „Aktualizacje zabezpieczeń” i „Aktualizacje dotyczące jakości”. W obszarze „Czas aktualizacji/powiadomienia” zaleca się wybranie pory spoza godzin szczytowego wykorzystania, np. „00: 00”. Kliknij przycisk Zastosuj.

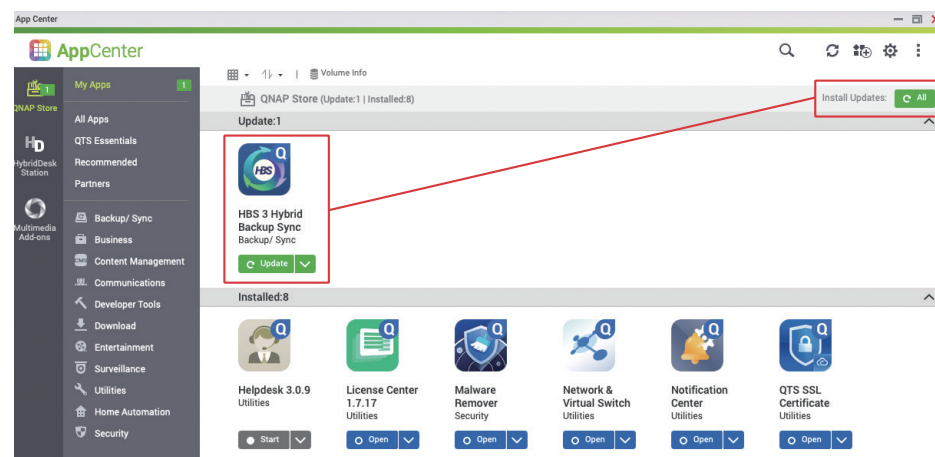
**\* Użytkownicy systemu QTS 5.0.0 / QuTS hero h5.0.0 (lub starszych wersji) powinni zaznaczyć opcję „Zalecana wersja” na stronie „Automatyczna aktualizacja”**



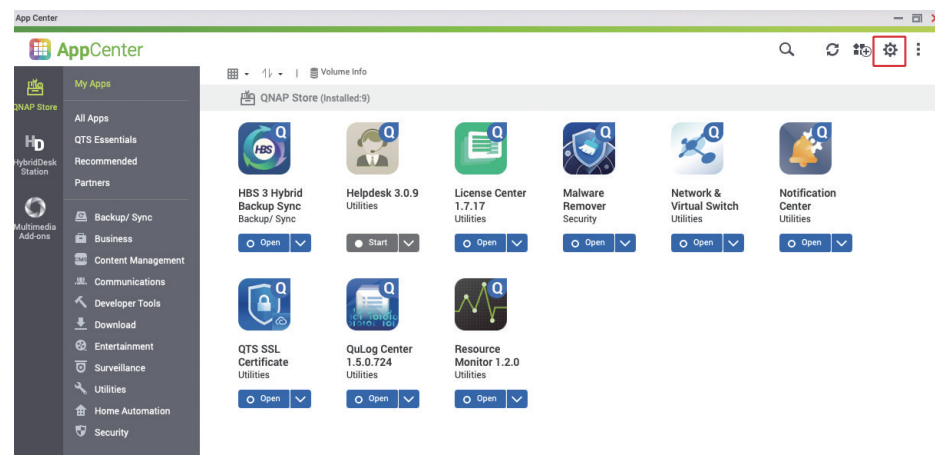
# Ustawienia aktualizacji aplikacji

Ekran App Center udostępnia różne aplikacje, które pozwalają dodawać kolejne funkcje do serwera QNAP NAS. Te aplikacje również wymagają aktualizacji, umożliwiających rozszerzenie zakresu funkcji, usunięcie problemów i luk w zabezpieczeniach oraz zwiększenie komfortu użytkowania.

Otwórz ekran „App Center”, aby sprawdzić, czy jakieś aplikacje wymagają aktualizacji. Jeśli tak, kliknij przycisk „Wszystkie”  „All” w prawym górnym rogu, aby zaktualizować wszystkie aplikacje.

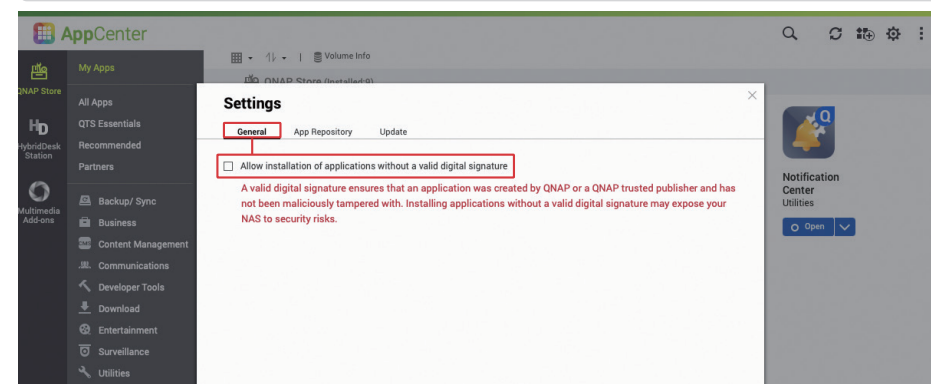


Po zakończeniu aktualizacji kliknij ikonę „Ustawienia”  w prawym górnym rogu, aby wyświetlić stronę ustawień aplikacji App Center.



Aplikacje zawierają podpisy cyfrowe, dodane przez firmę QNAP lub deweloperów współpracujących z firmą QNAP, które świadczą o autentyczności tych aplikacji. W celu zwiększenia bezpieczeństwa zaleca się usunięcie zaznaczenia opcji „Zezwalaj na instalację aplikacji bez ważnego podpisu cyfrowego”.

**\* Domyślnie nie jest ona zaznaczona, co uniemożliwia instalowanie aplikacji bez ważnego podpisu cyfrowego**

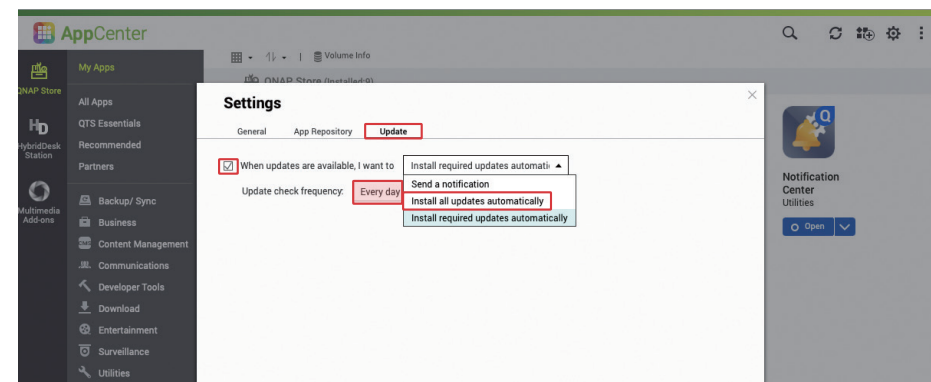


Kliknij kartę Aktualizacja. Jeśli okoliczności na to pozwalają, zaleca się wybranie opcji „Instaluj wszystkie aktualizacje automatycznie”, wybranie ustawienia „Codziennie” w obszarze częstotliwości i kliknięcie przycisku Zastosuj.

⇒ Opcja „Wymagane aktualizacje” służy przede wszystkim do spełniania wymagań związanych z zależnościami aplikacji i oprogramowania układowego. Obejmuje ona też „aktualizacje głównych luk w zabezpieczeniach”.

⇒ Opcja „Wszystkie aktualizacje” obejmuje udoskonalenia wszystkich funkcji, poprawki błędów i wszystkie poprawki luk w zabezpieczeniach. Wybranie tej opcji spowoduje, że aktualizacje będą uruchamiane częściej.

**\* Ustawienie domyślne to „Instaluj wszystkie aktualizacje automatycznie”**




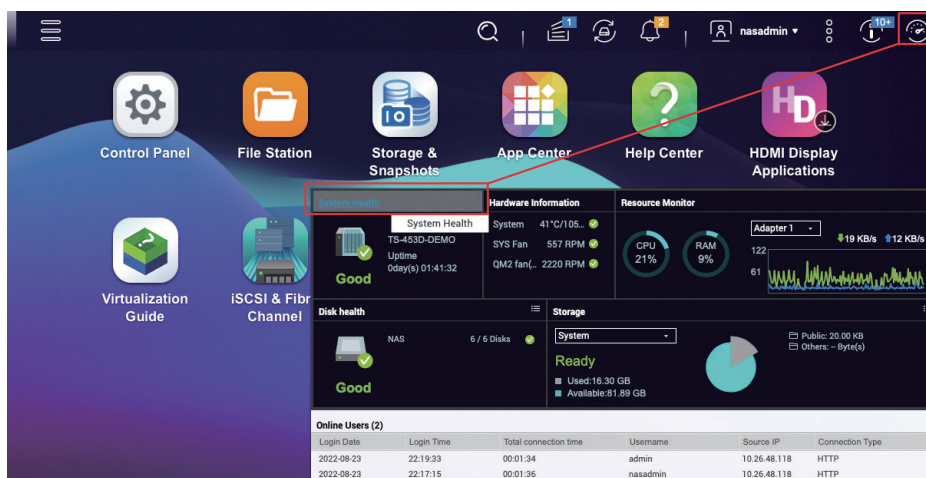


# Wyłączanie lub usuwanie niepotrzebnych funkcji

Serwer QNAP NAS udostępnia wiele funkcji i aplikacji, jednak im więcej funkcji jest włączonych, tym więcej jest potencjalnych wektorów ataków. Należy regularnie sprawdzać, które funkcje nie są potrzebne, i je wyłączać (lub usuwać). Pozwala to zwiększyć bezpieczeństwo i płynność działania systemu.

★ W celu zwiększenia bezpieczeństwa w systemie **QTS 5.0.0 / QuTS hero h5.0.0** (i nowszych wersjach) funkcje, które nie są niezbędne, są domyślnie wyłączone podczas inicjacji systemu, a mniej ważne aplikacje w obszarze **App Center** nie są domyślnie instalowane. Jeśli system został zainicjowany przed aktualizacją do wersji **QTS 5.0.0 / QuTS hero h5.0.0**, należy sprawdzić, jakie aplikacje zostały zainstalowane.

Kliknij przycisk „” w prawym górnym rogu, aby otworzyć ekran „Pulpit nawigacyjny”, a następnie kliknij opcję „Stan systemu”, aby otworzyć okno „Status systemu”.



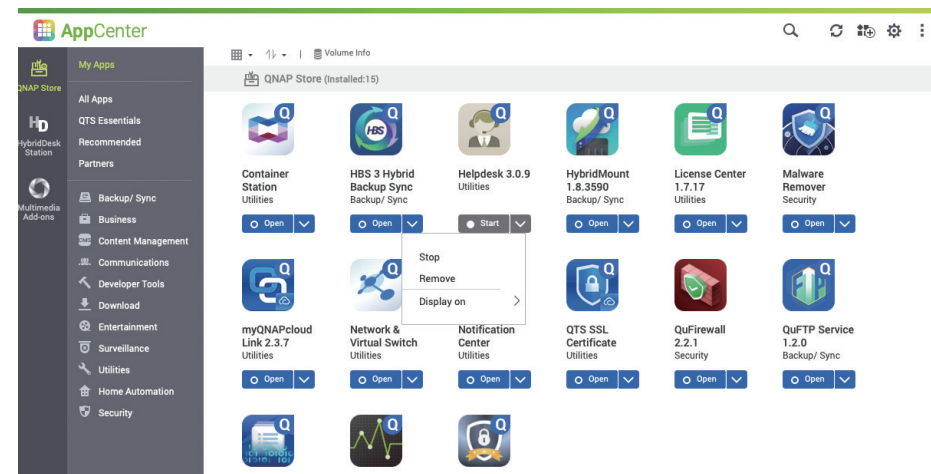
Kliknij opcję „Usługi systemowe”, aby wyświetlić włączone funkcje systemowe. Niepotrzebne funkcje systemowe można wyłączyć na ekranie Panel sterowania.

**System Status**

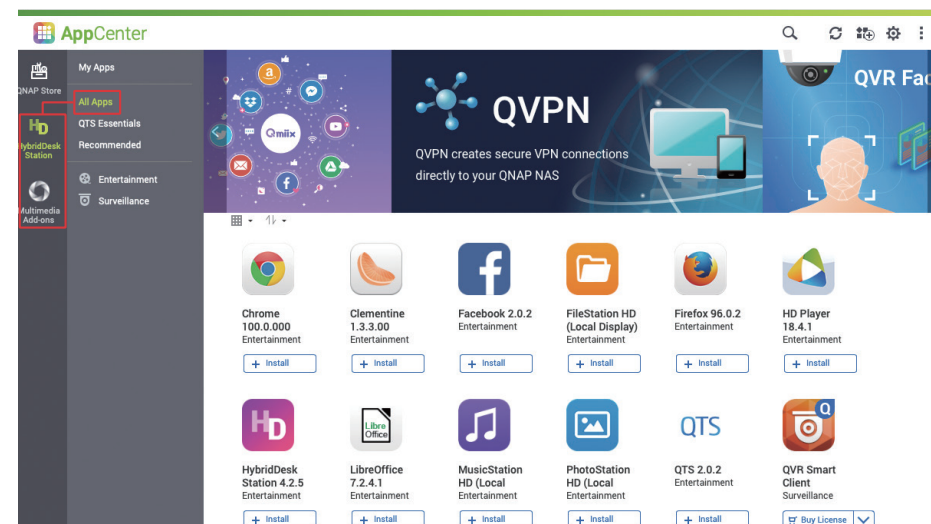
System Information   Network Status   **System Service**   Hardware Information

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

Oprócz wbudowanych funkcji systemowych należy również sprawdzić, jakie aplikacje są zainstalowane w obszarze App Center.



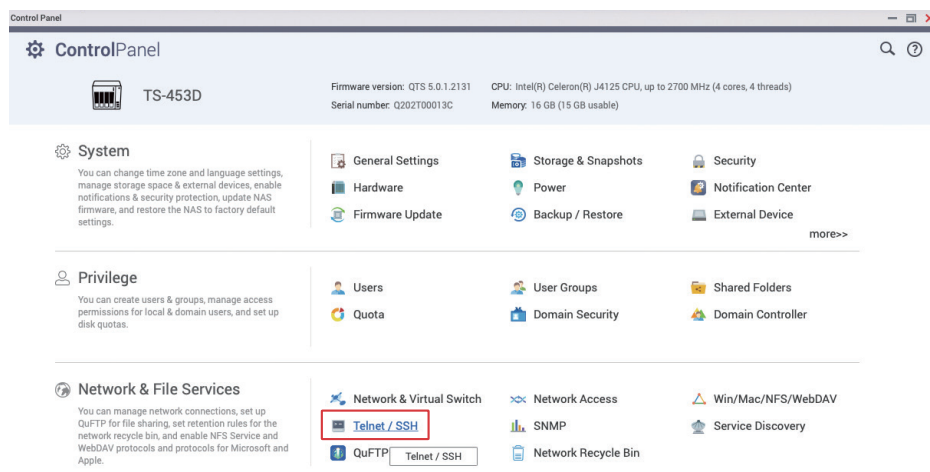
Po lewej stronie kliknij opcję „HybridDesk Station” i „Dodatki multimedialne”, aby sprawdzić status odpowiednich aplikacji.



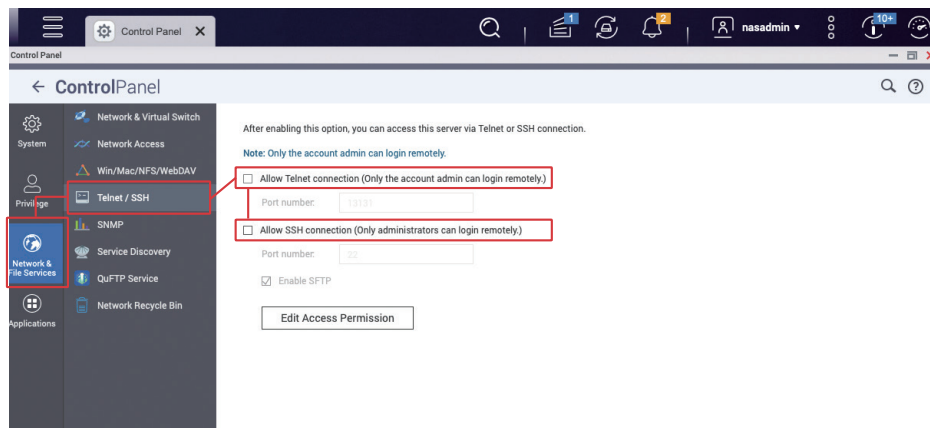
# Wyłączanie usług Telnet / SSH

Zdecydowanie zaleca się **wyłączenie usług Telnet i SSH**, jeśli nie są używane. Te dwie funkcje są zwykle używane przez pracowników działu obsługi klienta firmy QNAP oraz członków personelu informatycznego, którzy zajmują się konserwacją systemu. Użytkownicy raczej ich nie potrzebują, dlatego zaleca się ich wyłączenie.

Otwórz ekran „Panel sterowania” i kliknij opcję „Telnet / SSH”.



Usuń zaznaczenie opcji „Zezwól na połączenie Telnet” i „Zezwól na połączenie SSH”, a następnie kliknij przycisk „Zastosuj”.

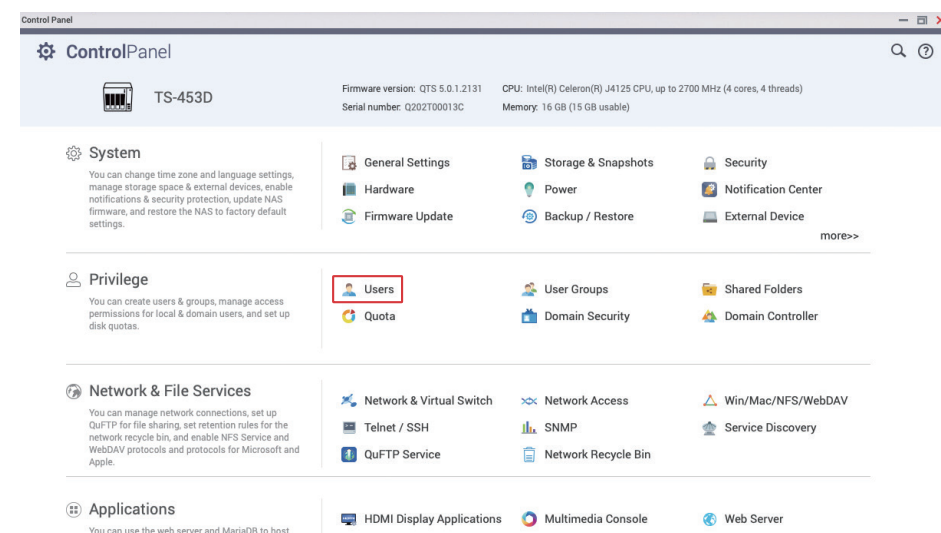


# Zwiększanie bezpieczeństwa konta systemowego

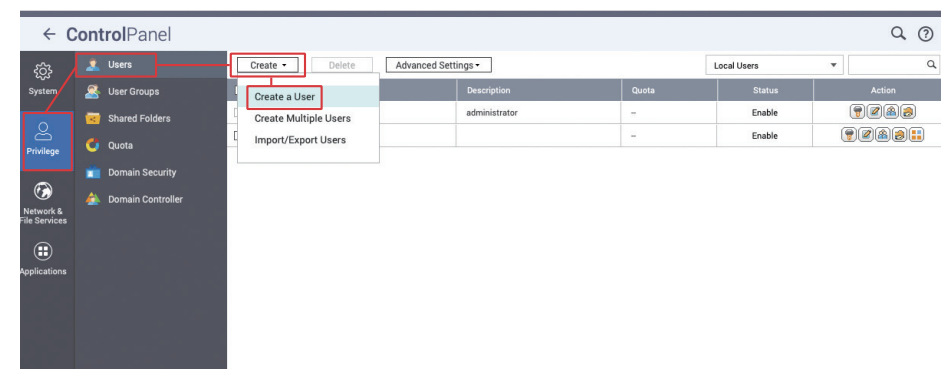
## Wyłączanie domyślnego konta administratora „admin”

Hakerzy, którzy próbują siłowo złamać hasło (w ramach ataków brute force), zwykle atakują domyślne konto administratora „admin”. Jeśli zainicjowano system w wersji QTS 4.5.4 / QuTS hero h4.5.4 (lub starszej), domyślne konto administratora „admin” jest aktywne. Wykonaj poniższe czynności, aby utworzyć nowe konto administratora i wyłączyć konto „admin”.

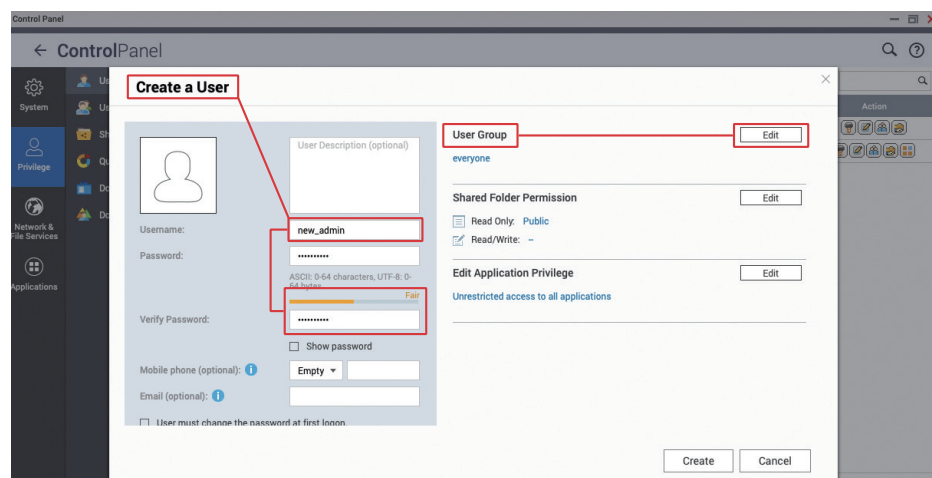
Otwórz ekran „Panel sterowania” i kliknij opcję „Użytkownicy”.



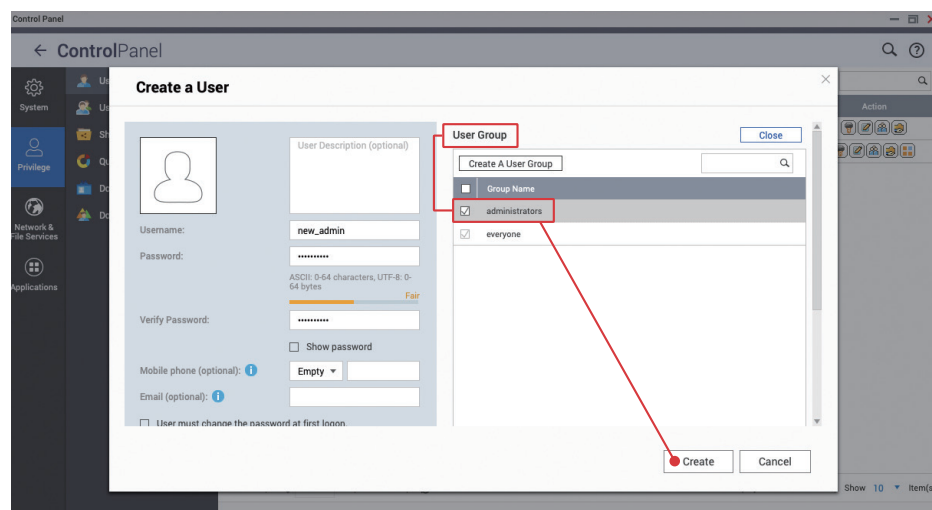
Kliknij kolejno „Utwórz” > „Utwórz użytkownika”.



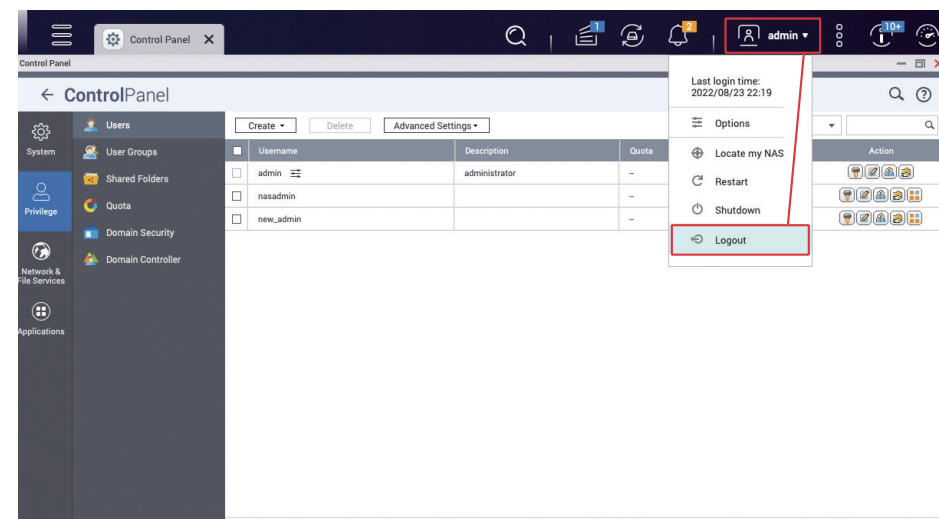
Wprowadź nazwę użytkownika konta administratora, na przykład „nowy\_admin”, i ustaw silne hasło.



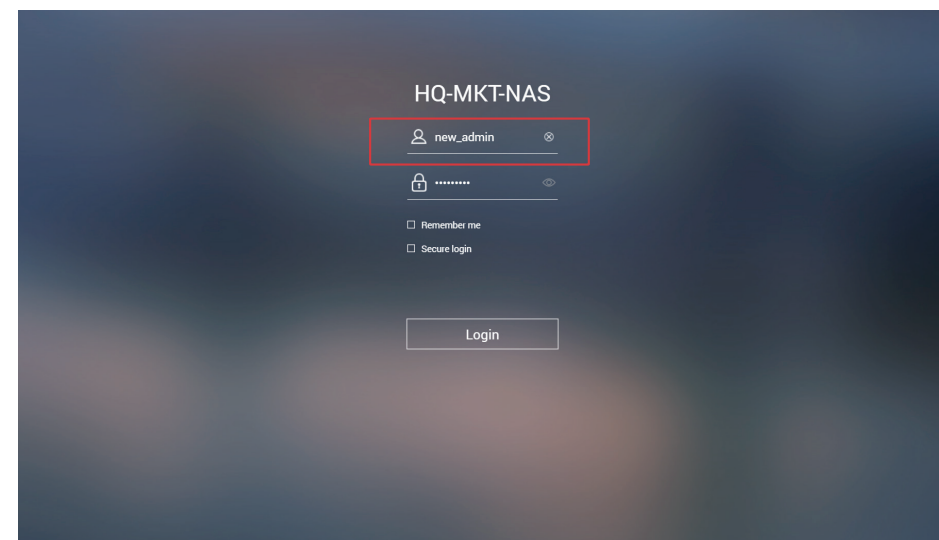
W sekcji „Grupa użytkowników” kliknij opcję „Edytuj”, zaznacz grupę „administratorzy” i kliknij opcję „Utwórz”, aby dodać nowego użytkownika.



Kliknij pozycję „admin” u góry, otwórz menu i kliknij opcję „Wyloguj się”, aby się wylogować z internetowego interfejsu zarządzania systemem QTS.

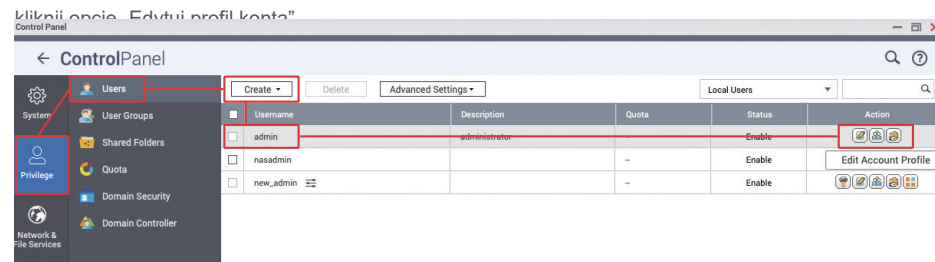


Zaloguj się do internetowego interfejsu zarządzania systemem QTS przy użyciu utworzonego konta administratora.

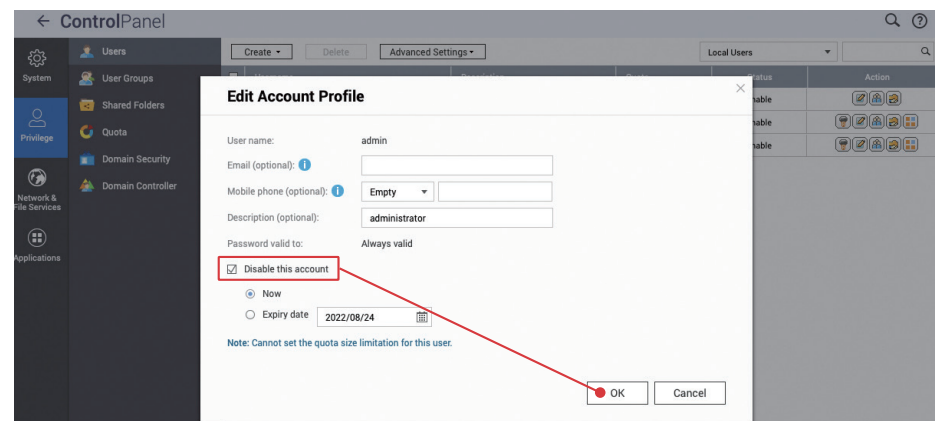


# Ustawianie zasad zarządzania hasłami

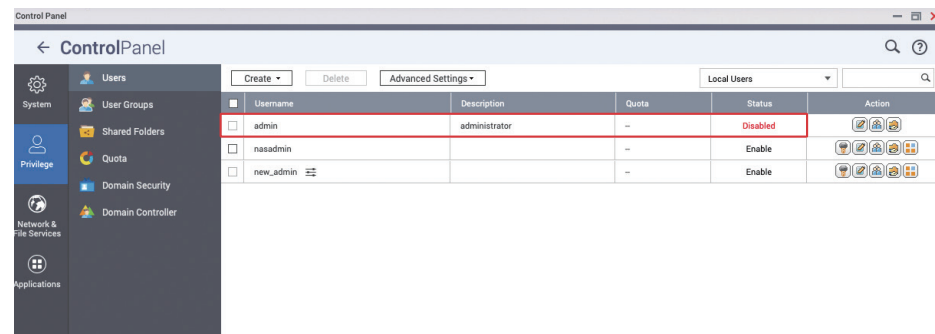
Ponownie otwórz ekran „Panel sterowania”, kliknij opcję „Użytkownicy”, a następnie w wierszu „admin”



Zaznacz opcję „Wyłącz to konto” i kliknij przycisk „OK”, aby zakończyć operację.

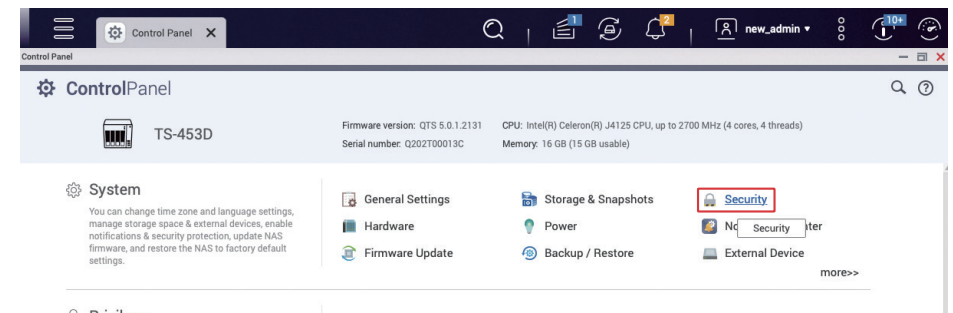


Status konta „admin” zmieni się na „Wyłączono”.

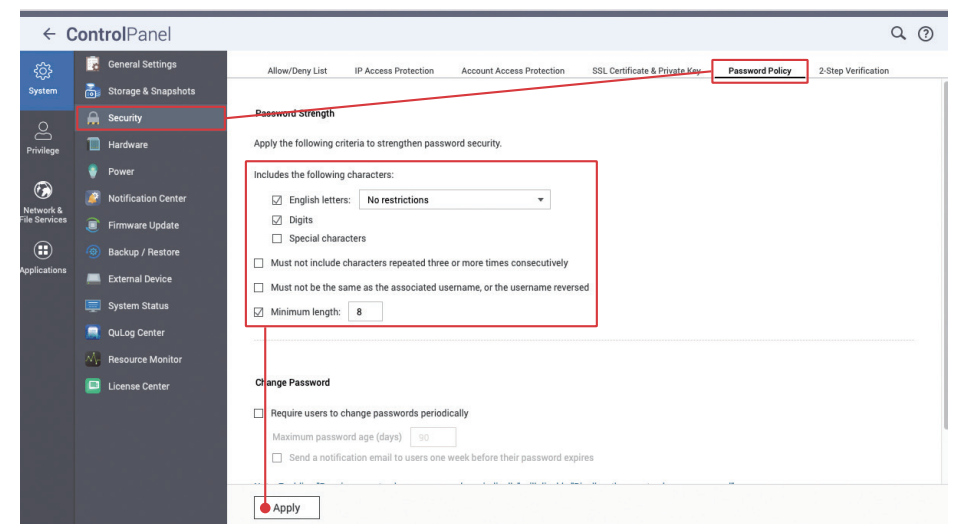


Oprócz wyłączenia domyślnego konta administratora „admin” należy też zadbać o to, aby wszystkie konta miały silne hasła. W połączeniu z korzyściami płynącymi z włączenia funkcji „Ochrona dostępu” pomoże to w blokowaniu szkodliwych prób logowania się do systemu. W celu zwiększenia bezpieczeństwa można wymusić stosowanie „weryfikacji dwuetapowej (2SV)” na wszystkich kontach, aby uniemożliwić łamanie haseł i szkodliwe logowanie się.

Otwórz ekran „Panel sterowania” i kliknij opcję „Ustawienia zabezpieczeń”.



Kliknij opcję „Zasady dotyczące haseł”, aby wyświetlić stronę ustawień. Jeśli zainicjowano system w wersji QTS 5.0.0 / QuTS hero h5.0.0 (lub nowszej), warunki stosowania hasła o minimalnej sile są domyślnie włączone. Można ustawić własne warunki dotyczące siły hasła. Można wymusić stosowanie „wielkich i małych liter alfabetu angielskiego” oraz „cyfr”. **Zaleca się, by hasło zawierało co najmniej 10 znaków.** Po ustawieniu hasła kliknij przycisk „Zastosuj”.





# Włączanie ochrony dostępu (do adresu IP / konta)

Funkcje „Ochrona dostępu adresów IP” i „Ochrona dostępu do konta” ułatwiają zabezpieczenie się przed siłowym łamaniem haseł. Wiele nieudanych prób zalogowania się z określonego adresu IP lub na dane konto spowoduje zablokowanie tego adresu IP lub dezaktywację konta, co uniemożliwi ponawianie prób złamania hasła.

Kliknij opcję „Ochrona dostępu adresów IP”, aby wyświetlić stronę ustawień. Zaznacz wszystkie usługi, odpowiednio ustaw opcje „Interwał czasu”, „Nieudane próby logowania” i „Czas blokowania adresu IP”, a następnie kliknij przycisk „Zastosuj”.

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	IP
<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

**W przypadku omyłkowego zablokowania adresu IP możesz zmienić listę zablokowanych elementów przy użyciu poniższych metod:**

1. Zaloguj się do interfejsu zarządzania systemem QTS / QuTS hero na innym komputerze
2. Zmień adres IP i zaloguj się do interfejsu zarządzania systemem QTS / QuTS hero
3. Zaloguj się do interfejsu zarządzania systemem QTS / QuTS hero za pomocą przeglądarki mobilnej
4. Użyj aplikacji QManager

**Apply**

Kliknij opcję „Ochrona dostępu do konta”, aby wyświetlić stronę ustawień, włącz odpowiednie usługi, adekwatnie ustaw opcje „Interwał czasu” i „Nieudane próby logowania”, a następnie kliknij przycisk „Zastosuj”.

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

**Jeśli opcja „Ochrona dostępu do konta” jest włączona dla konta administratora, może się zdarzyć, że w wyniku ataku mającego na celu złamanie hasła wszystkie konta administratorów zostaną wyłączone. W takim przypadku konto „admin” będzie można ponownie włączyć tylko za pomocą funkcji resetowania, a hasło do konta „admin” również zostanie zresetowane. Pamiętaj, aby po wykonaniu operacji resetowania zmienić hasło.**

**Apply**

# Włączanie weryfikacji dwuetapowej (2SV)

Kliknij opcję „Weryfikacja 2-etapowa”, aby wyświetlić stronę ustawień. Stosowanie funkcji „Weryfikacja 2-etapowa (2SV)” można wymusić w odniesieniu do użytkowników lub grup użytkowników. Zdecydowanie zaleca się włączenie funkcji 2SV dla kont należących do grupy administratorów. W przypadku innych kont należy samodzielnie ocenić ryzyko i zastosować odpowiednie ustawienia.

Kliknij opcję „Użytkownicy lokalni”, aby otworzyć menu, i wybierz opcję „Grupy lokalne”.

Control Panel

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

Allow/Deny List IP Access Protection Account Access Protection SSL Certificate & Private Key Password Policy **2-Step Verification**

**2-Step Verification**

2-Step Verification (2SV) adds an extra layer of protection to a user's account by requiring an additional one-time security code whenever a user signs in to your NAS. You can enforce 2-step verification for specific users and groups.

Note: The configuration of "Enforce 2SV" between the group and users in the group may not be consistent. See "Status" to check the final 2SV status of users.

Enforce 2SV	Username	Description
<input type="checkbox"/>	admin	administrator
<input type="checkbox"/>	nasadmin	
<input type="checkbox"/>	new_admin	

**Local Users**

Local Users  
Local Groups  
Domain Users  
Domain Groups

**Disabled**

Zaznacz opcję „Wymuszanie weryfikacji 2SV” w grupie „administratorzy” i kliknij przycisk „Zastosuj”.

Control Panel

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

Allow/Deny List IP Access Protection Account Access Protection SSL Certificate & Private Key Password Policy **2-Step Verification**

**2-Step Verification**

2-Step Verification (2SV) adds an extra layer of protection to a user's account by requiring an additional one-time security code whenever a user signs in to your NAS. You can enforce 2-step verification for specific users and groups.

Note: The configuration of "Enforce 2SV" between the group and users in the group may not be consistent. See "Status" to check the final 2SV status of users.

Enforce 2SV	Group Name	Description	Status
<input checked="" type="checkbox"/>	administrators		--
<input type="checkbox"/>	everyone		--

Page 1 / 1

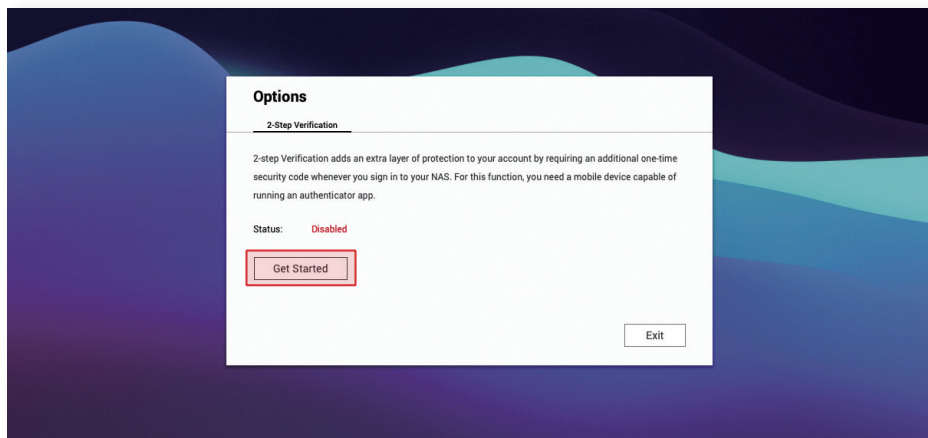
Display item: 1-2, Total: 2 | Show 10 Item(s)

**Apply**

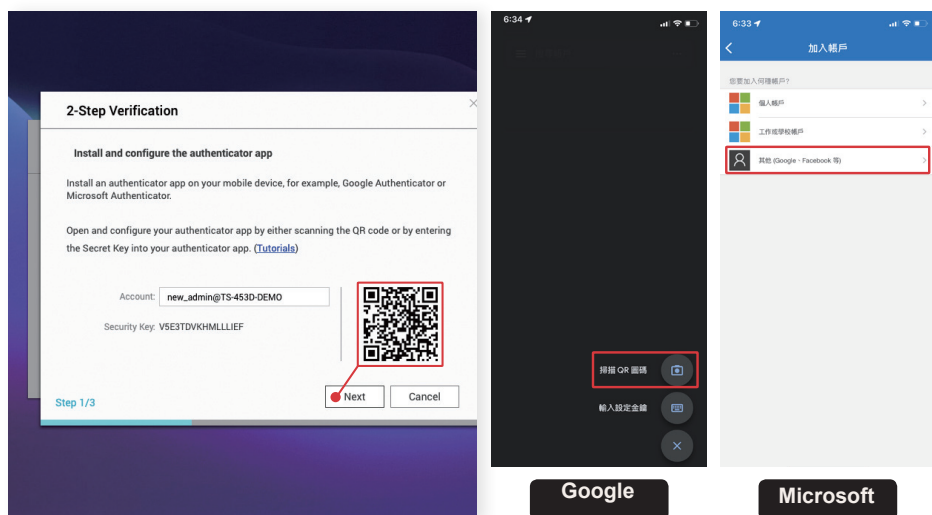


Jeśli opcja „Wymuszanie weryfikacji 2SV” została włączona, ale funkcja „Weryfikacja 2-etapowa (2SV)” nie została skonfigurowana na koncie „Administrator”, podczas kolejnego logowania nastąpi przekierowanie do strony ustawień „Weryfikacja 2-etapowa (2SV)” w celu skonfigurowania konta.

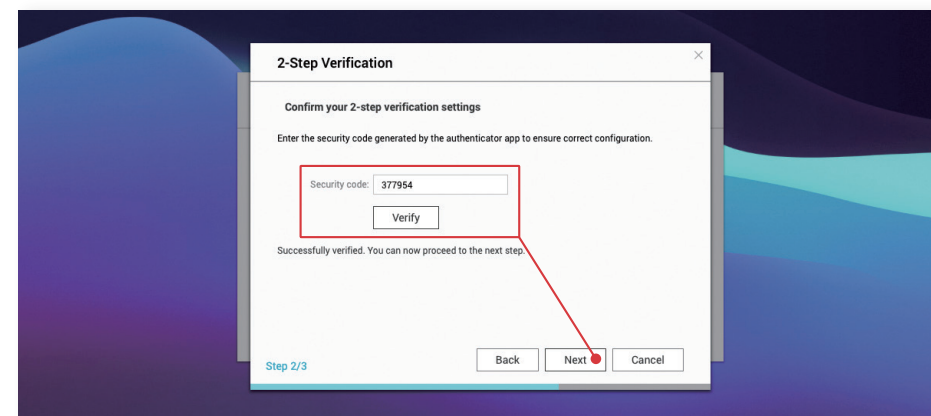
Zaloguj się ponownie na konto „Administrator systemu” i kliknij opcję „Rozpocznij”, aby rozpocząć konfigurowanie ustawień.



Zainstaluj aplikację „Google Authenticator” lub „Microsoft Authenticator” na urządzeniu mobilnym, zeskanuj kod QR w celu dodania urządzenia, a następnie kliknij przycisk „Dalej”.

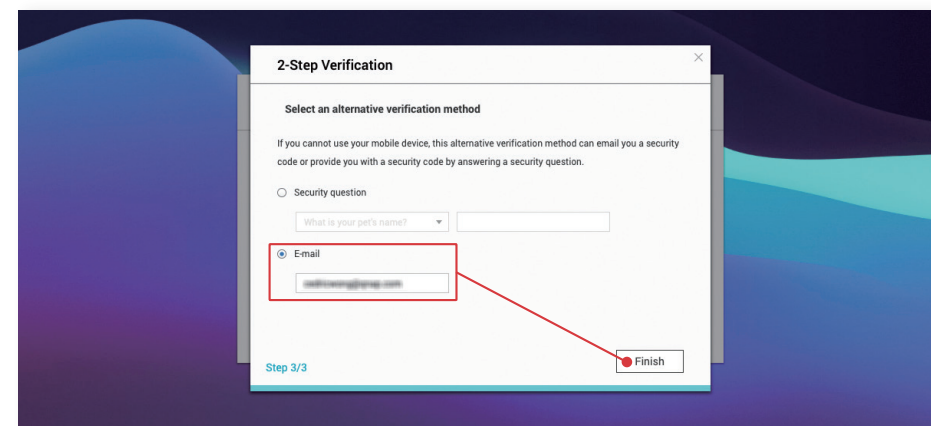


Wprowadź sześciocyfrowy kod zabezpieczający wygenerowany w aplikacji „Google Authenticator” lub „Microsoft Authenticator”, a następnie kliknij opcję „Weryfikuj”. Po zakończeniu weryfikacji kliknij przycisk Dalej.



Aby skonfigurować inną metodę weryfikacji\*, wybierz opcję „Pytanie zabezpieczające\*\*” lub „E-mail\*\*\*”, wprowadź odpowiednie informacje i kliknij opcję „Zakończ” w celu włączenia funkcji „Weryfikacja 2-etapowa (2SV)”.

- \* Jeśli nie można uzyskać kodu zabezpieczającego w aplikacji uwierzytelniającej, można rozwiązać ten problem, wybierając opcję „Pytanie zabezpieczające” lub „E-mail”.
- \*\* Aby przejść weryfikację dwuetapową, należy odpowiedzieć poprawnie na pytanie zabezpieczające. Nie należy używać prostych lub łatwych do odgadnięcia pytań i odpowiedzi.
- \*\*\* Korzystanie z tej funkcji wymaga dodania metody powiadomienia „E-mail” na ekranie „Centrum powiadomień”.



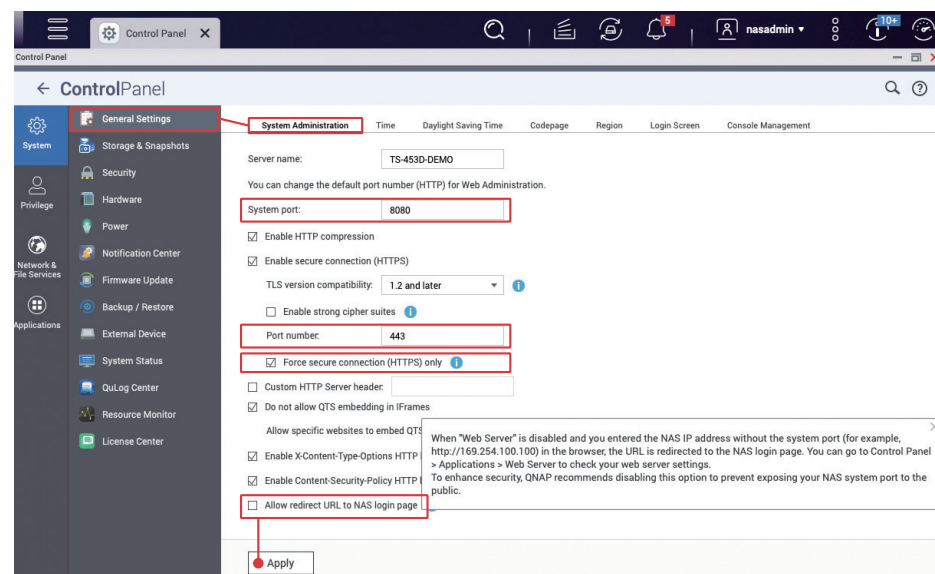
# Zmiana domyślnych portów

Z każdą usługą uruchomioną na serwerze NAS jest skojarzony odpowiedni port. Niektórych standardowych portów usług nie można modyfikować, ale pozostałe porty mogą być definiowane przez użytkowników.

Hakerzy szukający celów ataków, którzy często korzystają z wyszukiwarki urządzeń IoT, zwykle najpierw próbują uzyskać dostęp do domyślnego portu. Aby zmniejszyć ryzyko takiego ataku, należy zmienić domyślne porty typowych usług. W przypadku ataków na serwer NAS najczęstszym celem jest „port systemowy”. Poniżej przedstawiono metodę zmiany „portu systemowego”. Porty innych funkcji można zmodyfikować na odpowiedniej stronie ustawień. Aby zapewnić bezpieczeństwo systemu, pamiętaj, aby zmodyfikować te porty przed użyciem odnośnych usług.

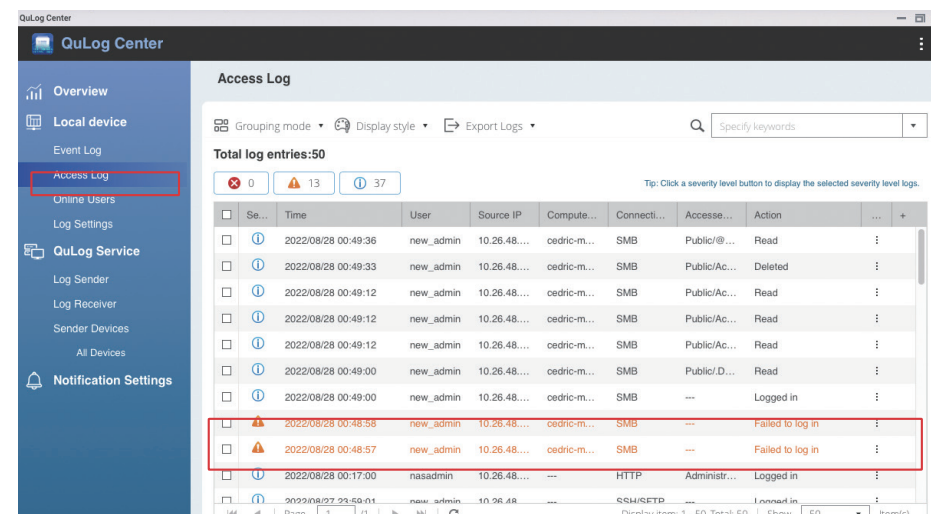
Otwórz ekran „Panel sterowania” i kliknij opcję „Ustawienia ogólne”. Wartość domyślna w obszarze „Port systemowy (HTTP)” to „8080”. Możesz wprowadzić numer portu z zakresu od 1 do 65535, na przykład „56789”. Ponadto **zaleca się zmianę** w obszarze „Port systemowy (HTTPS)” (wartość domyślna to „443”), czyli dla **portu systemowego** z włączoną funkcją bezpiecznych połączeń. Oprócz tego **zaleca się zaznaczenie opcji „Wymuszaj tylko bezpieczne połączenie (HTTPS)”**, aby wymusić przesyłanie danych przez użytkowników za pośrednictwem protokołu HTTPS i uniemożliwić hakerom przechwycenie informacji poufnych, takich jak hasła do kont.

**Zaleca się również usunięcie zaznaczenia opcji „Zezwalaj na przekierowywanie adresu URL do strony logowania NAS”, aby zapobiec ujawnianiu portu systemowego w wyniku automatycznego przekierowania. Po wprowadzeniu zmian kliknij przycisk „Zastosuj”.**

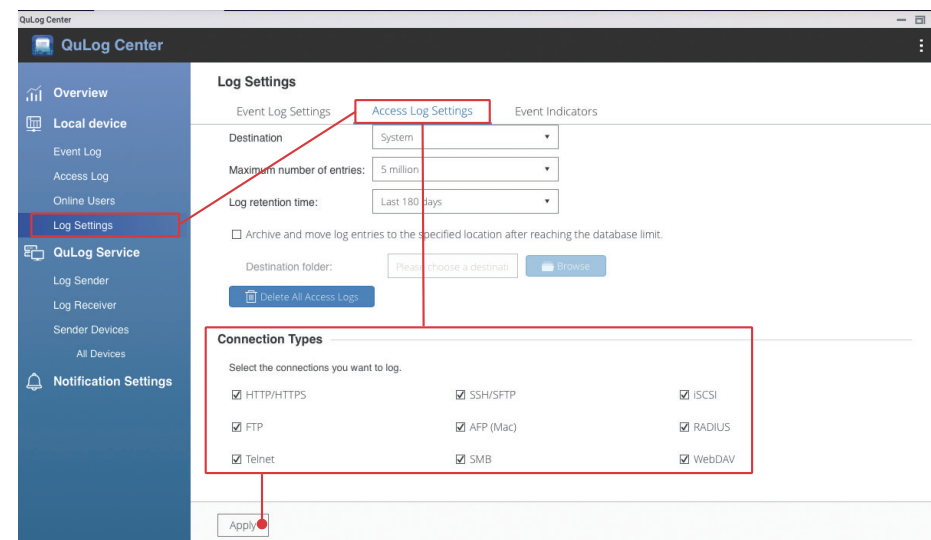


# Wyświetlanie dzienników dostępu

Dzienniki dostępu zawierają informacje na temat uzyskiwania dostępu do plików, wykonywanych operacji oraz historii logowania użytkowników. Diagnozowanie problemów powinno się rozpoczynać od sprawdzenia dzienników dostępu.



Otwórz aplikację „QuLog Center”, kliknij opcję „Ustawienia dziennika” w menu po lewej stronie, przejdź do strony „Ustawienia dziennika dostępu”, zaznacz wszystkie połączenia w obszarze „Typy połączeń”, a następnie kliknij przycisk „Zastosuj”.



# Instalowanie i włączanie aplikacji zabezpieczających

Firma QNAP udostępnia kilka aplikacji zabezpieczających, które poprawiają bezpieczeństwo serwera NAS. Skonfigurowanie tych aplikacji pozwala zwiększyć bezpieczeństwo serwera NAS i umożliwia bezproblemowe korzystanie z jego funkcji.



Security Counselor regularnie sprawdza ustawienia serwera NAS pod kątem bezpieczeństwa oraz informuje o potencjalnych zagrożeniach.



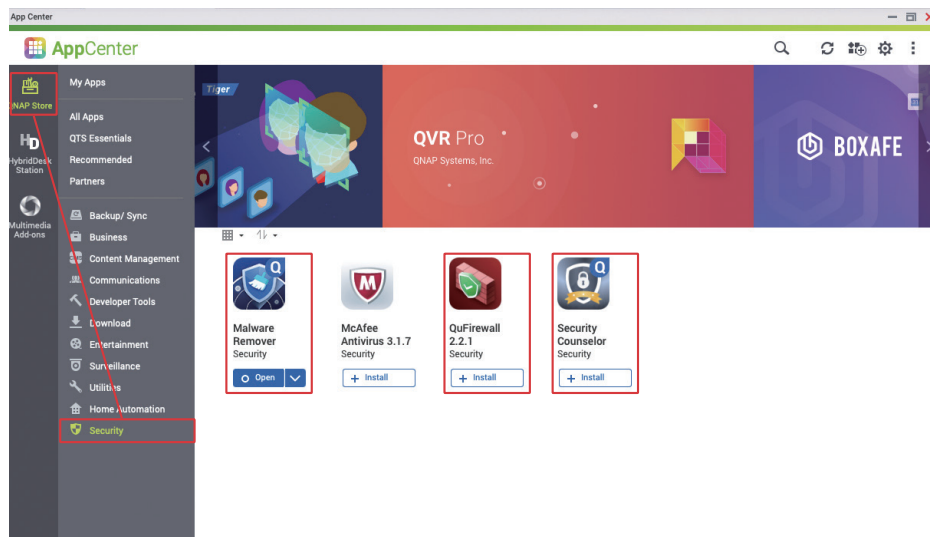
Malware Remover skanuje serwer NAS i usuwa wykryte złośliwe oprogramowanie.



QuFirewall zapewnia podstawową funkcjonalność zapory sieciowej i blokuje szkodliwe połączenia z serwerem QNAP NAS.

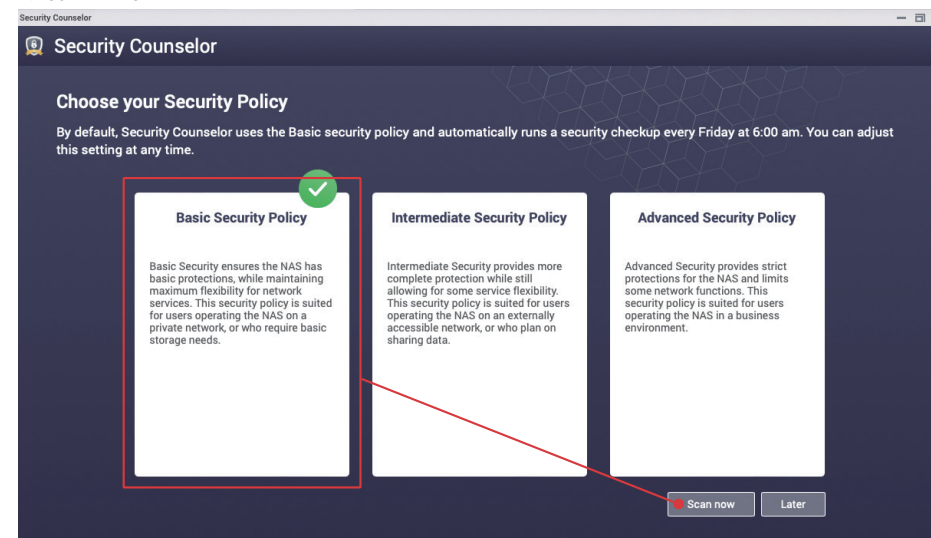
Otwórz ekran „App Center”, kliknij opcję „Zabezpieczenia” po lewej stronie, a następnie zainstaluj aplikacje „Security Counselor”, „Malware Remover” i „QuFirewall”.

★ Aplikacja Malware Remover jest fabrycznie zainstalowana w systemach QTS 4.4.3 (i nowszych wersjach) oraz QuTS hero

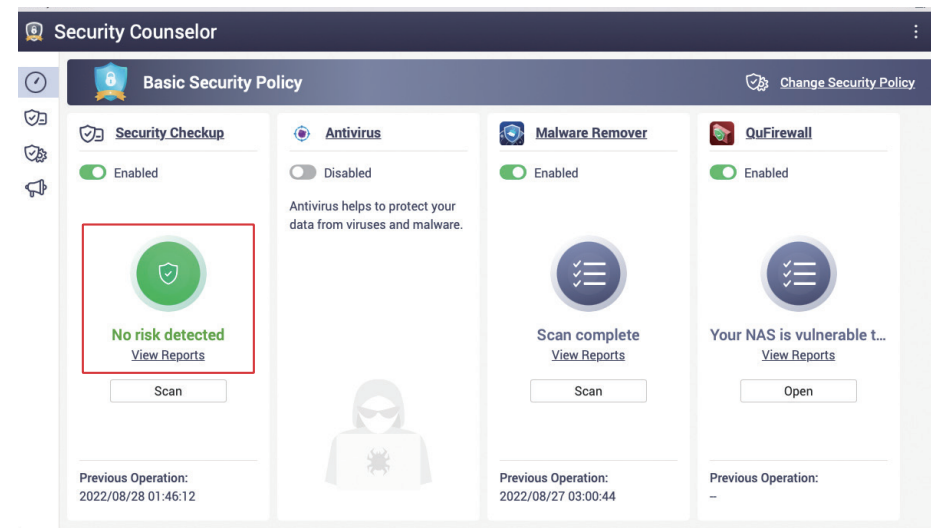


# Security Counselor

Otwórz aplikację „Security Counselor”, wybierz opcję „Podstawowe zasady bezpieczeństwa” i kliknij opcję „Skanuj teraz”.



Typowy wynik skanowania to „Nie wykryto żadnego ryzyka”. Jeśli zostanie wykryte zagrożenie, kliknij opcję „Wyświetl raporty”, aby uzyskać szczegółowe informacje, i postępuj zgodnie z instrukcjami w zakresie zmiany ustawień.





Poniżej przedstawiono wyniki skanowania po celowym wprowadzeniu błędnych ustawień. Kliknij opcję „Asystent sugerowanych ustawień”, aby ułatwić sobie dostosowywanie ustawień.

**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	<span style="color: red;">!</span>	High	Either this setting is deselected in the Password Policy screen or the current required mini...	⋮
Update	<span style="color: green;">✓</span>	High	The	⋮
Account	<span style="color: green;">✓</span>	High	The	⋮
Network	<span style="color: green;">✓</span>	High	The	⋮
Network	<span style="color: green;">✓</span>	High	The web server on your device cannot be directly accessed from the internet using the foll...	⋮
Network	<span style="color: green;">✓</span>	High	The NAS doesn't allow Telnet connections.	⋮
System	<span style="color: green;">✓</span>	High	Run user defined processes during startup is disabled.	⋮

Funkcja „Asystent sugerowanych ustawień” wyświetla listę odpowiednich sugestii. Po zapoznaniu się z nimi kliknij opcję „Zastosuj sugestie”, aby umożliwić systemowi automatyczne zastosowanie odpowiednich ustawień. Niektóre ustawienia trzeba zmodyfikować ręcznie. Kliknij kartę „Ręcznie” po lewej stronie i odpowiednio dostosuj ustawienia. Gdy zmiany zostaną zastosowane, skanowanie zostanie automatycznie uruchomione ponownie. Ponowne sprawdzenie wyników skanowania pozwoli się upewnić, że na serwerze NAS nie wykryto zagrożeń bezpieczeństwa.

**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
<span style="color: red;">!</span> Either this setting is deselected in the Password Policy screen or the current required minimum length for passwords is below 8 characters.	<span style="color: green;">✓</span> Configure the settings in the Password Policy screen and require the use of passwords with a minimum of 8 characters.

Apply suggestion Close

Kliknij opcję „Sprawdzanie zabezpieczeń” po lewej stronie, aby wyświetlić ekran wyników skanowania, a następnie kliknij opcję „Harmonogram skanowania” po prawej stronie, aby otworzyć ekran ustawień harmonogramu skanowania.

**Security Counselor**

**Basic Security Policy** Change Security Policy

**No risk detected** Last scan status: Finished Last scan time: 2022/08/28 02:08:53 Scan schedule: Friday 06: 00 Scan schedule

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

Category	Status	Risk	Result	Action
Update	<span style="color: green;">✓</span>	High	The NAS is using the most up-to-date version of firmware.	⋮
Account	<span style="color: green;">✓</span>	High	The current settings in the Password Policy screen include requiring passwords to have a ...	⋮
Account	<span style="color: green;">✓</span>	High	The default administrator password is not the default password.	⋮
Network	<span style="color: green;">✓</span>	High	The system administration service on your device cannot be directly accessed from the int...	⋮
Network	<span style="color: green;">✓</span>	High	The web server on your device cannot be directly accessed from the internet using the foll...	⋮
Network	<span style="color: green;">✓</span>	High	The NAS doesn't allow Telnet connections.	⋮
System	<span style="color: green;">✓</span>	High	Run user defined processes during startup is disabled.	⋮

Zaleca się takie ustawienie harmonogramu skanowania, aby skanowanie odbywało się **co najmniej raz w miesiącu**. Pozwoli to na regularne sprawdzanie ustawień i stanu systemu. Jeśli zostanie wykryte zagrożenie, a ustawienia na ekranie Centrum powiadomień są prawidłowe, zostanie wyświetlone powiadomienie, co umożliwi sprawną reakcję.

**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

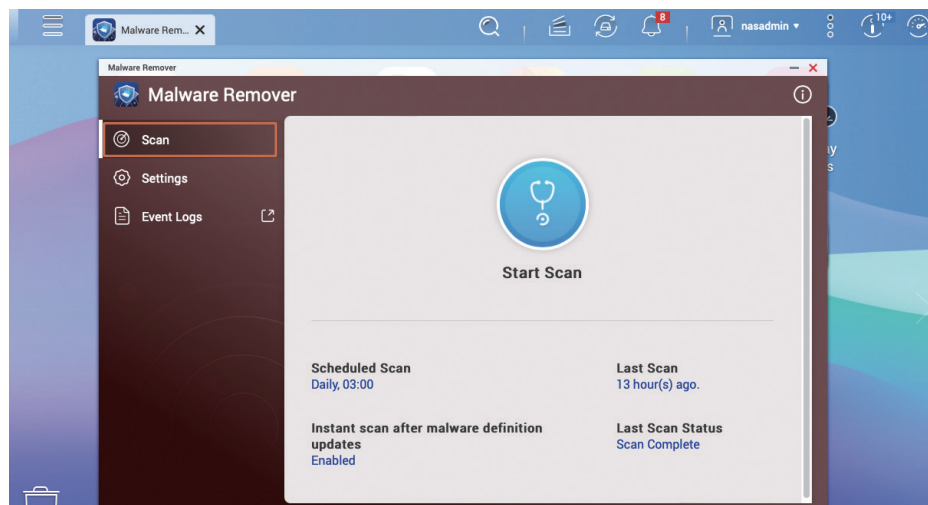
Run at the following time: 06 : 00

Apply Cancel

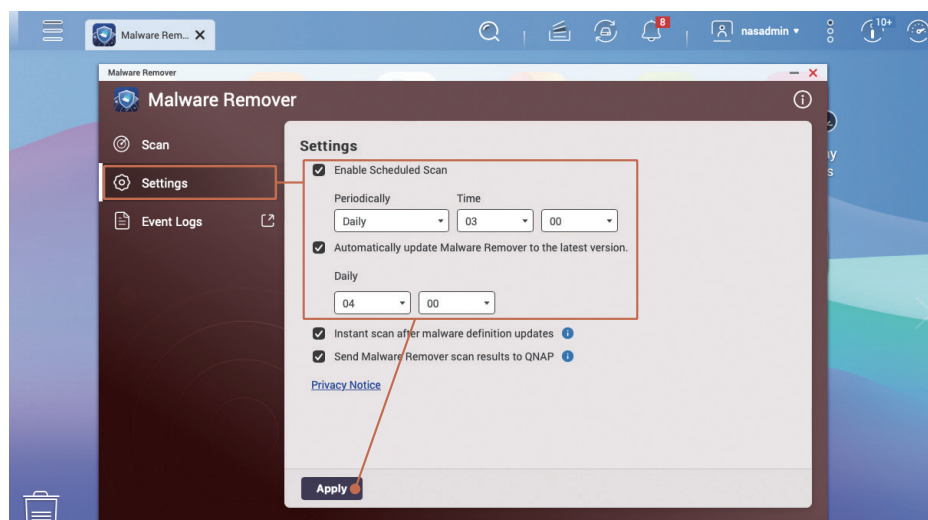
Category	Status	Risk	Result	Action
Update	<span style="color: green;">✓</span>	High	The NAS is using the most up-to-date version of firmware.	⋮
Account	<span style="color: green;">✓</span>	High	The current settings in the Password Policy screen include requiring passwords to have a ...	⋮
Account	<span style="color: green;">✓</span>	High	The default administrator password is not the default password.	⋮
Network	<span style="color: green;">✓</span>	High	The system administration service on your device cannot be directly accessed from the int...	⋮
Network	<span style="color: green;">✓</span>	High	The web server on your device cannot be directly accessed from the internet using the foll...	⋮
Network	<span style="color: green;">✓</span>	High	The NAS doesn't allow Telnet connections.	⋮
System	<span style="color: green;">✓</span>	High	Run user defined processes during startup is disabled.	⋮

# Malware Remover

Otwórz aplikację „Malware Remover”. Zostanie wyświetlony status ostatniego skanowania. Kliknij opcję „Ustawienia” po lewej stronie.

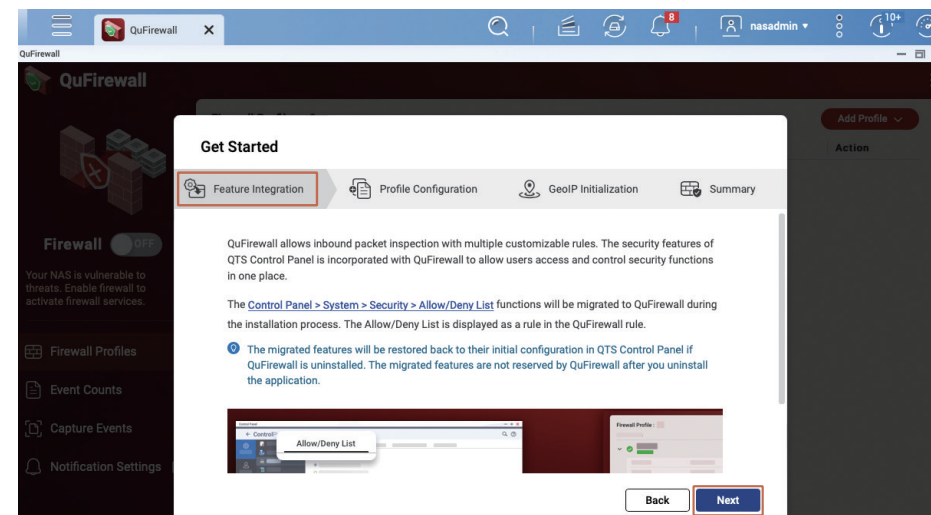


Zaleca się takie ustawienie harmonogramu skanowania, aby skanowanie odbywało się **raz dziennie**. Pozwoli to aplikacji „Malware Remover” na regularne sprawdzanie stanu systemu. Ponadto opcja „Automatycznie aktualizuj Malware Remover do najnowszej wersji” powinna być zaznaczona.

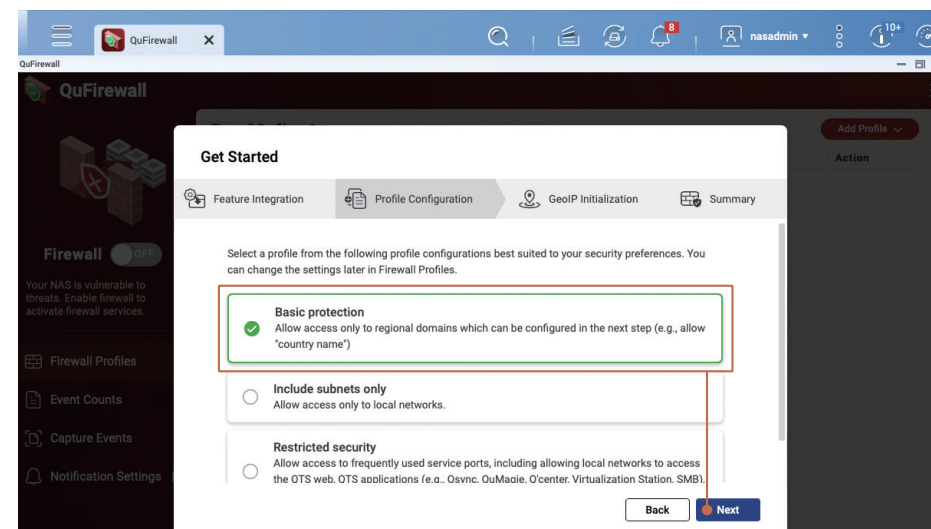


# QuFirewall

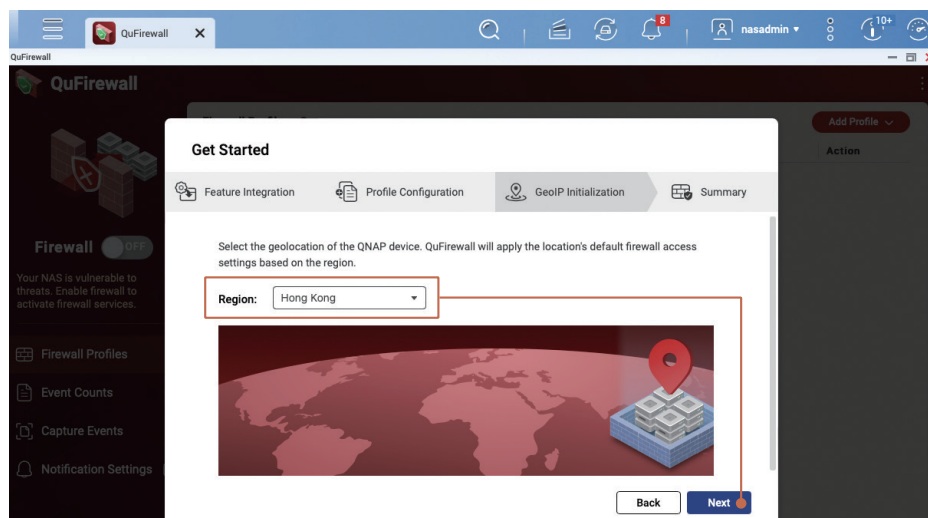
Otwórz aplikację „QuFirewall”. Przy pierwszym użyciu aplikacji QuFirewall zostanie wyświetlony ekran Rozpocznij. Po zapoznaniu się z wyświetlonym komunikatem kliknij opcję „Dalej”.



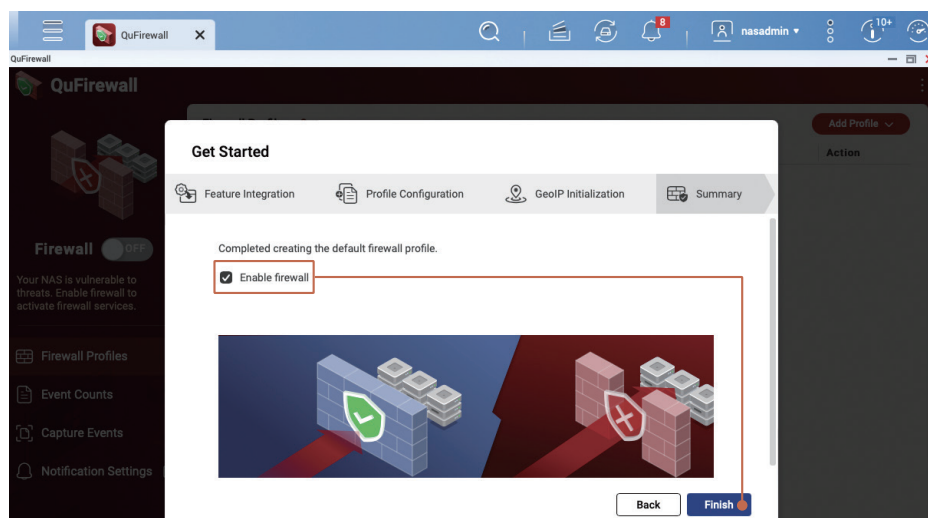
Jeśli nie występują specjalne wymagania dotyczące sieci, zaleca się wybranie opcji „Podstawowa ochrona”, a następnie kliknięcie przycisku „Dalej”.



Wybierz odpowiedni region. Jeśli na przykład przebywasz na Tajwanie, wybierz opcję „Tajwan”. Jeśli przebywasz w Hongkongu, wybierz opcję „Hongkong”. Jeśli przebywasz w Makau, wybierz opcję „Makau”. Później można dodać kolejne regiony. Aby kontynuować, kliknij przycisk „Dalej”.

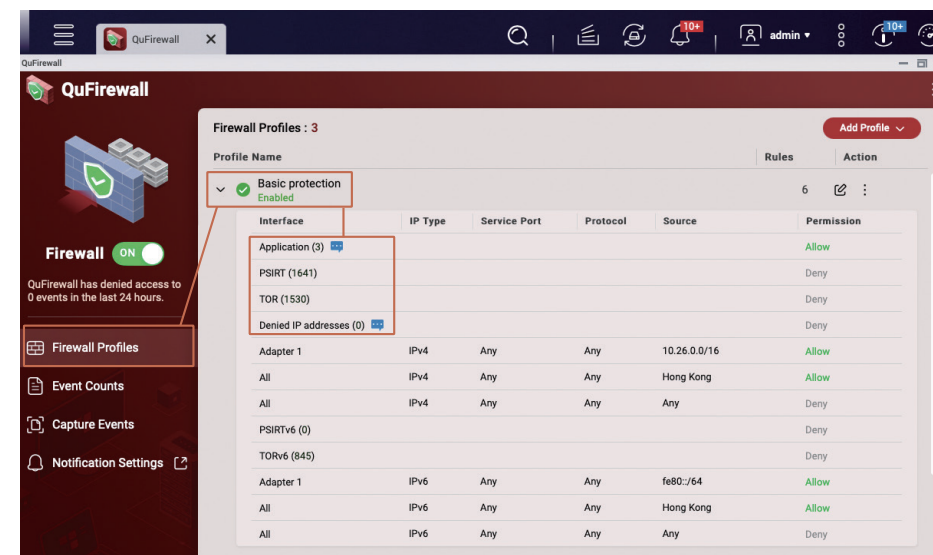


Zaznacz opcję „Włącz zaporę”, a następnie kliknij przycisk „Zakończ”, aby zastosować ustawienia i włączyć zaporę.




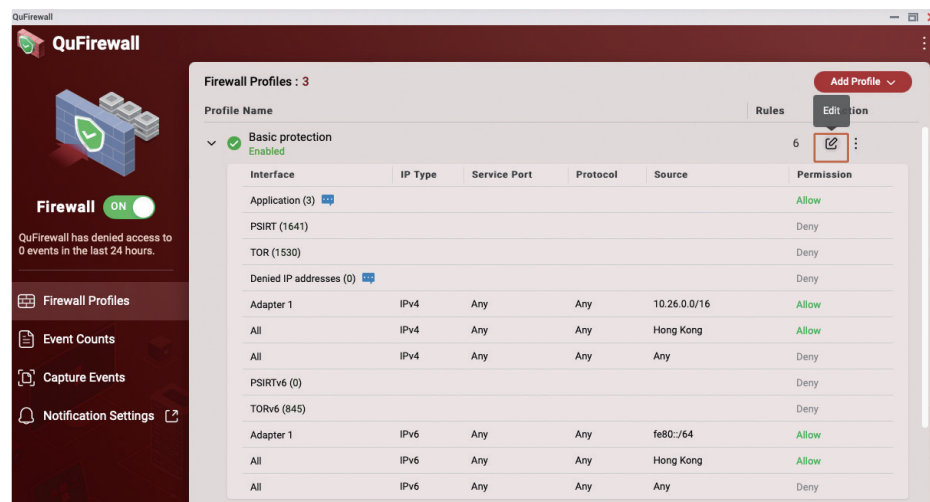
Gdy otworzysz stronę profilów zapory QuFirewall, zobaczysz, że opcja „Podstawowa ochrona” jest włączona. Kliknij opcję „Podstawowa ochrona”, aby rozwinąć i wyświetlić odpowiednie reguły zapory. Informacje w pakietach przychodzących są porównywane z regułami zapory, a same pakiety są przepuszczane lub blokowane. Reguły zapory są przetwarzane sekwencyjnie. Jeśli warunki nie są spełnione, sprawdzana jest następna grupa reguł. Jeśli te reguły również nie są spełnione, następuje przejście do ostatniej reguły „Odrzucaj wszystkie”, a zaporę blokuje odpowiednie połączenia.

- Systemowe reguły „Aplikacje” zapewniają prawidłowe działanie systemu.
- Reguła „PSIRT” to rodzaj „czarnej listy” opracowanej przez zespół QNAP PSIRT. Zawiera ona adresy IP, z których przeprowadzono ataki na serwery QNAP NAS.
- Reguła „TOR” służy do blokowania połączeń z sieci TOR. Wielu przestępców wykorzystuje sieć TOR ze względu na jej anonimowość. Zablokowanie tej sieci może zmniejszyć ryzyko ataku.
- „Odrzucone adresy IP” to adresy IP, które zostały zablokowane przez funkcję „Ochrona dostępu adresów IP” lub ręcznie dodane do czarnej listy przez użytkownika.



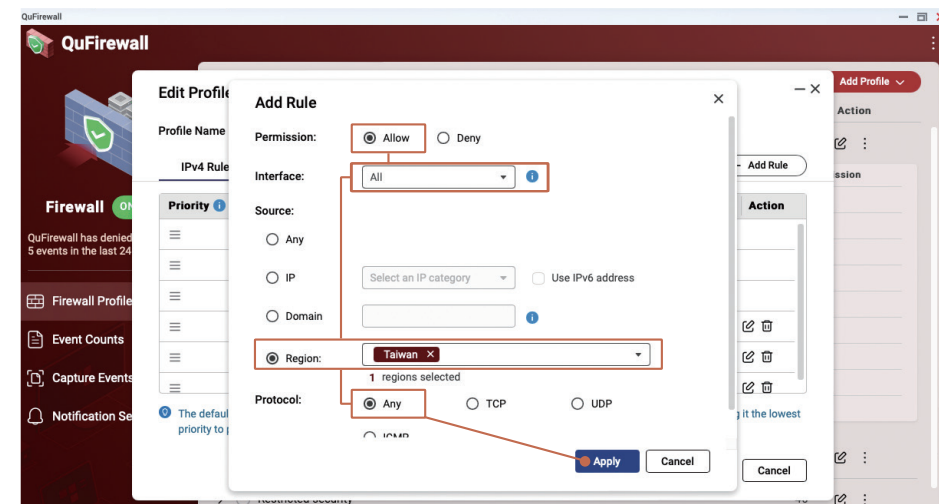
Użytkownik może dostosować inne reguły. Zgodnie z ustawieniami podstawowej ochrony dozwolone są tylko połączenia z Internetem w ramach tego samego intranetu i tego samego regionu. Firma QNAP zaleca zarządzanie niestandardowymi regułami za pomocą „białej listy” w celu ścisłego ograniczania adresów IP, które mogą nawiązywać połączenia z serwerem NAS.

Poniżej przedstawiono metodę edytowania reguł zapory. Kliknij przycisk „Edytuj” , aby edytować elementy na ekranie Profile zapory.

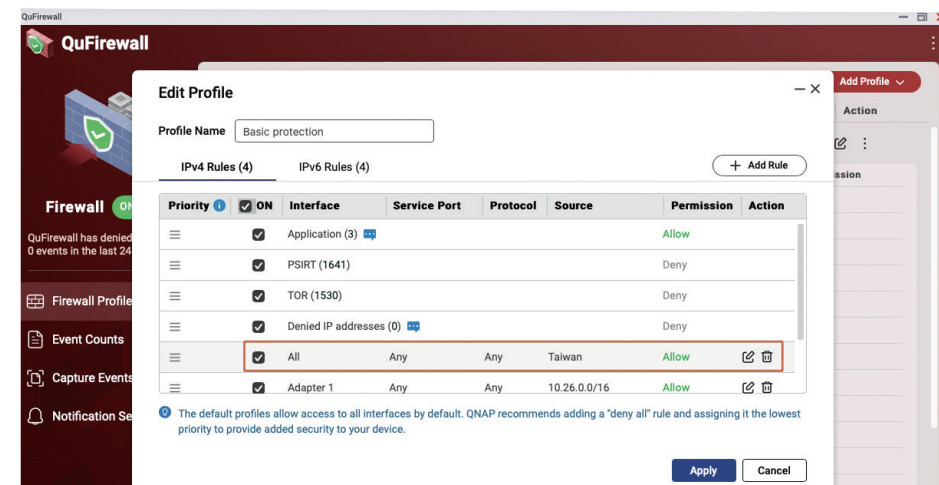
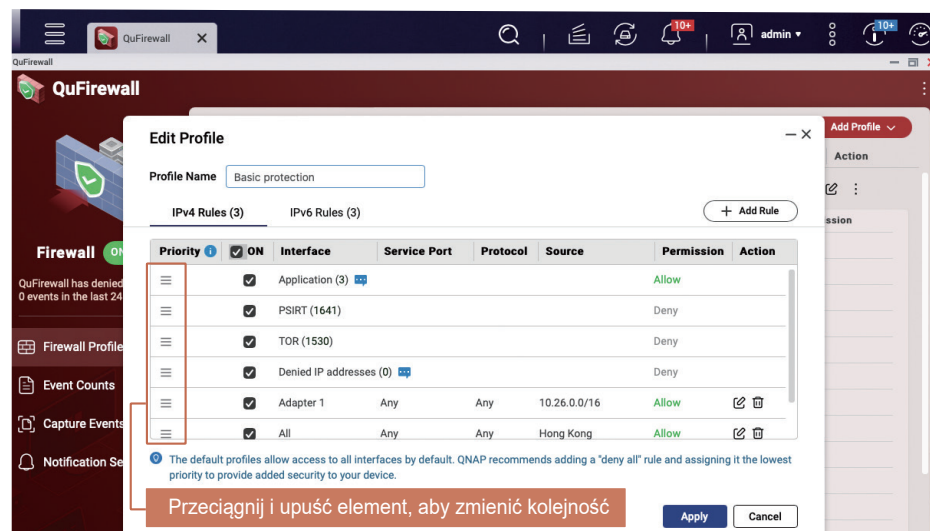


Na ekranie Edytuj profil można zmieniać kolejność reguł i dodawać nowe reguły. W poniższym przykładzie dodano kolejny region, z którego są dozwolone połączenia. Kliknij opcję „Dodaj regułę”, aby wyświetlić ekran ustawień.

Aby na przykład zezwolić na połączenia z Tajwanu, w obszarze „Uprawnienia” wybierz opcję „Zezwalaj”, w obszarze „Interfejs” wybierz opcję „Wszystkie”, w obszarze „Źródło” wybierz opcję „Region”, a następnie wybierz „Tajwan”, w obszarze „Protokół” wybierz opcję „Dowolny”, a następnie kliknij przycisk „Zastosuj”, aby dodać regułę.



Nowo dodane reguły będą wyświetlane na stronie „Edytuj profil”. W razie potrzeby można dostosować ich kolejność. Upewnij się, że reguły są prawidłowe i kliknij przycisk „Zastosuj”.





# Włączanie zaplanowanych migawek

Funkcja migawek umożliwia tworzenie punktów przywracania wielu wersji, co pozwala chronić ważne dane. Na serwerze QNAP NAS można ustawić harmonogram tworzenia migawek, aby umożliwić systemowi automatyczne tworzenie migawek w ramach podstawowej ochrony danych.

- \* Zaplanowane migawki są domyślnie włączone w przypadku woluminów pełnych/uproszczonych utworzonych w systemie QTS 5.0.0
- \* W systemie QTS 5.0.1 (i nowszych wersjach) zaplanowane migawki są domyślnie włączone tylko w przypadku woluminów uproszczonych
- \* W folderach udostępnionych utworzonych w systemie QuTS hero h5.0.1 (i nowszych wersjach) zaplanowane migawki są domyślnie włączone

Otwórz sekcję „Pamięć masowa i migawki”, kliknij opcję „Pamięć masowa/Migawki” po lewej stronie i upewnij się, że w obszarze „Przestrzeń dyskowa” wybrano strukturę „Pula pamięci” oraz że pula pamięci zawiera wystarczającą ilość wolnego miejsca do zapewnienia działania funkcji migawek. W przypadku woluminu pełnego można rozważyć użycie funkcji „Zmień rozmiar woluminu”\* i „Konwertuj na wolumin uproszczony”\*, aby zwolnić miejsce w puli pamięci wymagane do działania funkcji migawek.

- \* Przed skonwertowaniem woluminów należy wykonać kopię zapasową danych, aby uniknąć potencjalnej utraty danych.

Storage & Snapshots

Storage Space Storage Pool: 1, Volume: 3, LUN: 0

Name/Alias	Status	Type	Snapshot Re...	Snapshot	Capacity	Percent Used
Storage Pool 1	Ready				5.83 TB	
Data	Ready	Thin volume			2.97 TB	
System (System)	Ready	Thin volume		to :9	98.20 GB	
Thick	Ready	Thick volume			494.54 GB	

Thick Management

Name/Alias: Thick

Capacity: 494.54 GB

Free Size: 494.47 GB

Thin: No

SSD cache: --

Remote Disk

Status: Ready

Utilization

100%  
75%  
50%  
25%

Used: 0.01% (72.04 MB) Free Size: 99.99%

Actions

- Remove
- Resize Volume
- Set Threshold
- Set Caching Storage
- Check File System
- Rename Volume Alias
- Format
- Convert to Thin Volume

\* Otwórz sekcję zarządzania woluminami pełnymi, aby wprowadzić odpowiednie zmiany w celu zwolnienia miejsca w puli pamięci.

Gdy upewnisz się, że pula pamięci na serwerze NAS zawiera wystarczającą ilość miejsca, kliknij opcję „Wolumin”, a następnie opcję „Migawka” u góry, po czym kliknij opcję „Manager kopii migawkowych” w menu.

Storage & Snapshots

Storage Space Storage Pool: 1, Volume: 2, LUN: 0

Name/Alias	Status	Type	Snapshot Rep...	Snapshot	Cap
Storage Pool 1	Ready				
Data	Ready	Thin volume			
System (System)	Ready	Thin volume		to :9	

Snapshot Manager

Przejdź do strony ustawień „Manager kopii migawkowych” woluminu i kliknij opcję „Zaplanuj migawkę” w prawym górnym rogu.

Snapshot Manager

Pool Guaranteed Snapshot Space

Data Ready

Schedule Snapshot

Daily 01:00

Take Snapshot

Schedule Snapshot

Open in File Station

Name (0/0)	Replicated	Capacity	Retention Policy	Taken	Taken By	Status
------------	------------	----------	------------------	-------	----------	--------

W obszarze „Włącz harmonogram” wybierz stan „Włącz”, a następnie odpowiednio zmodyfikuj harmonogram. Zaleca się wybranie opcji „Codziennie” lub „Co tydzień”.

Snapshot Settings

Schedule Snapshot Snapshot Retention Pool Guaranteed Snapshot Space

Enable schedule: ☒

Repeat: Daily Time: 01:00 (h:mm)

Snapshot retention policy: Smart Versioning

The snapshot will be stored in Storage Pool 1 (5.65 TB available).

☒ Enable smart snapshot

Description

Note: The performance of a volume or LUN may be affected after taking a snapshot, due to data structure change.

Note: Snapshots will be automatically recycled when available storage pool space is low. [Change policy](#)

Odpowiednio konfiguruując zasady przechowywania migawek, można ograniczyć liczbę migawek i zajmowane przez nie miejsce.

Zaleca się włączenie funkcji „Inteligentne przechowywanie wersji”, czyli korzystanie ze schematu GFS (Grandfather-Father-Son), który pozwala zachować liczbę wersji wystarczającą do zapewnienia ochrony danych. Po wprowadzeniu ustawień kliknij przycisk „OK”, aby je zastosować.

Snapshot Settings

Schedule Snapshot Snapshot Retention Pool Guaranteed Snapshot Space

How many Snapshot can I have?

The snapshot retention policy determines how long to keep a snapshot or how many total snapshots to keep. When the specified value is exceeded, the system deletes the expired snapshot or the oldest snapshot automatically.

☐ Maximum amount of time to keep: 0 Months

☐ Maximum number of snapshots to keep: 0 Snapshots

☒ Smart Versioning

Hourly snapshots: 24

Daily snapshots: 7

Weekly snapshots: 4

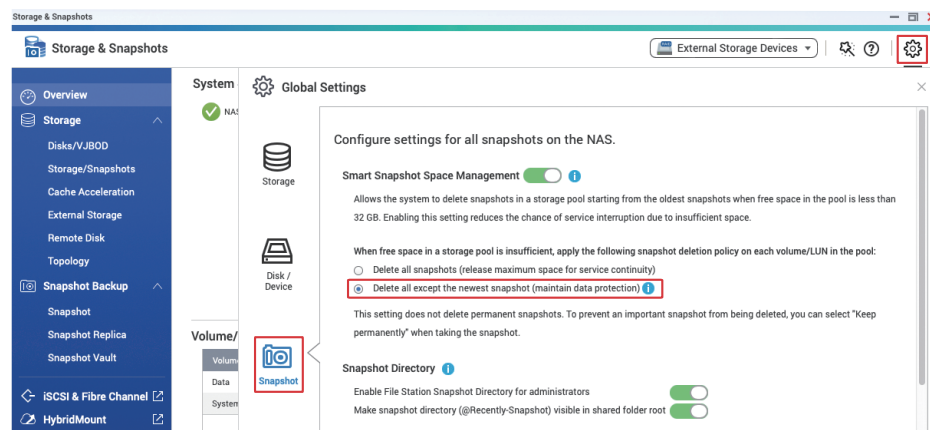
Monthly snapshots: 12



# Ustawianie zasad usuwania migawek

Jeśli ilość miejsca w puli pamięci będzie zbyt mała, migawki zostaną usunięte zgodnie z ustawieniami, aby zapewnić normalną pracę systemu i uniknąć potencjalnych przerw w działaniu usług.

W sekcji „Pamięć masowa i migawki” kliknij przycisk „Ustawienia” w prawym górnym rogu, otwórz ekran „Ustawienia globalne” i kliknij opcję „Migawka”. Zaleca się ustawienie opcji „**Usuń wszystko oprócz najnowszej migawki**”, aby uniknąć usunięcia wszystkich migawek i utraty ochrony.

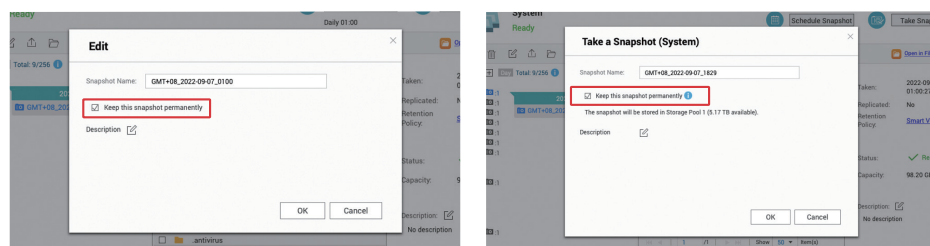


Jeśli chcesz, aby system zachowywał wszystkie migawki nawet w przypadku niewystarczającej ilości miejsca w puli pamięci, wyłącz opcję „Inteligentne zarządzanie miejscem na migawki”. Pamiętaj jednak, że jeśli ilość miejsca w puli pamięci będzie niewystarczająca, pula pamięci przejdzie w tryb „tylko do odczytu/usuwanie”. Aby przywrócić normalne działanie puli pamięci, konieczne będzie ręczne usunięcie migawki. Po wyłączeniu tej funkcji należy regularnie sprawdzać wykorzystanie miejsca.



Aby uniknąć braku ochrony spowodowanego przez zasady usuwania migawek, w przypadku przechowywania dużej ilości danych zaleca się wybranie opcji „Zachowaj tę kopię migawkową na stałe” co najmniej dla części migawek. Dzięki temu system nie będzie ich usuwać.

★ Aby zwolnić miejsce, należy ręcznie usunąć migawkę. Zaleca się ręczne tworzenie i regularne usuwanie migawek



# Lista kontrolna ustawień zabezpieczeń serwera NAS

- ❑ **Skonfigurowanie Centrum powiadomień**
  - ❑ Ustaw co najmniej jedną metodę powiadamiania
  - ❑ Utwórz reguły powiadomień o alertach
  - ❑ Utwórz reguły powiadomień o aktualizacji oprogramowania układowego
- ❑ **Włącz automatyczną aktualizację oprogramowania układowego (QTS / QuTS hero)**
- ❑ **Skonfiguruj elementy na ekranie App Center**
  - ❑ Zaktualizuj wszystkie aplikacje do najnowszych wersji
  - ❑ Zabroń instalowania aplikacji, które nie mają ważnego podpisu cyfrowego
  - ❑ Włącz automatyczne aktualizacje
- ❑ **Wyłącz lub usuń niepotrzebne funkcje**
  - ❑ Sprawdź, czy włączone usługi są potrzebne
  - ❑ Sprawdź, czy aplikacje włączone na ekranie **App Center** są potrzebne
  - ❑ Wyłącz usługę **SSH**
  - ❑ Wyłącz usługę **Telnet**
- ❑ **Zwiększ bezpieczeństwo konta systemowego**
  - ❑ Wyłącz domyślne konto „admin”
  - ❑ Ustaw zasady zarządzania hasłami
  - ❑ Włącz funkcję **Ochrona dostępu** adresów IP
  - ❑ Włącz funkcję Weryfikacja dwuetapowa (**2SV**)
- ❑ **Zmień domyślny port systemowy**
- ❑ **Włącz Dziennik dostępu**
- ❑ **Zainstaluj i włącz aplikacje zabezpieczające**
  - ❑ **Security Counselor**
    - ❑ Włącz zaplanowane skanowanie
  - ❑ **Malware Remover**
    - ❑ Włącz zaplanowane skanowanie
  - ❑ **QuFirewall**
    - ❑ Włącz zaporę
    - ❑ Ustaw region **Geo-IP**
    - ❑ Włącz reguły **PSIRT**
    - ❑ Włącz reguły **TOR**
- ❑ **Włącz zaplanowane migawki**
  - ❑ Regularnie włączaj opcję „Zachowaj tę kopię migawkową na stałe”

# Często zadawane pytania

## Q Czy odłączenie serwera NAS od Internetu zwiększa bezpieczeństwo?

A Nie. Odłączenie serwera NAS zwykle oznacza jego „odcięcie” od sieci, tak aby nawiązywanie połączeń zewnętrznych nie było możliwe. Niektóre złośliwe programy wymagają połączenia zewnętrznego, ale inne są w stanie wykonywać szkodliwe operacje bez takiego połączenia. Z tego względu działanie to nie tylko nie powstrzyma hakerów, ale także uniemożliwi prawidłowe funkcjonowanie niektórych funkcji systemu, takich jak automatyczne aktualizacje oprogramowania i powiadomienia. Właściwe podejście, które zwiększa bezpieczeństwo, polega na ograniczeniu ruchu do serwera NAS i unikaniu ujawniania go w Internecie.

## Q Dysk twardy działa w ramach konfiguracji RAID. Czy to oznacza, że kopie zapasowe nie są potrzebne?

A Nie. RAID nie jest metodą tworzenia kopii zapasowych. Poziomy RAID powyżej 0 pozwalają jedynie zapewnić nadmiarowość na wypadek awarii dysku. Konfiguracja RAID nie zabezpiecza przed usunięciem ani zaszyfrowaniem danych. Z tego względu zaleca się prawidłowe **tworzenie kopii zapasowych danych zgodnie z zasadą 3-2-1**.

## Q Migawki zostały skonfigurowane. Czy to oznacza, że kopie zapasowe nie są potrzebne?

A Nie. Migawki są przechowywane na tych samych dyskach twardych co dane, dlatego w przypadku awarii macierzy RAID dane i tak zostaną utracone. Ponadto, jeśli hakerzy uzyskają wystarczające uprawnienia (na przykład w wyniku złamania hasła do konta administratora), również mogą usunąć migawkę. Z tego względu zaleca się prawidłowe tworzenie kopii zapasowych plików migawek zgodnie z zasadą 3-2-1.

## Q Serwer NAS nie jest dostępny w Internecie. Czy to oznacza, że przeprowadzenie ataku jest niemożliwe?

A Nie. Źródłem większości cyberataków jest Internet, ale serwer NAS można zaatakować również w intranecie. Jeśli na przykład zabezpieczenia innego komputera lub jakiegoś urządzenia w intranecie zostaną naruszone, urządzenie to może posłużyć do przeprowadzenia ataku na inne urządzenia w intranecie. Zainstalowanie na komputerze oprogramowania antywirusowego i wdrożenie produktów zabezpieczających sieć może pomóc w radzeniu sobie z powiązаныmi zagrożeniami. Na przykład QNAP ADRA NDR pozwala wykrywać podejrzaną aktywność w intranecie i automatycznie ją izolować. Zaleca się także prawidłowe tworzenie kopii zapasowych danych zgodnie z zasadą 3-2-1.

## Q Serwer NAS jest używany od dawna. Jak sprawdzić, czy jest na nim zainstalowane złośliwe oprogramowanie?

A Nienormalnie wysokie obciążenie procesora, błędy aktualizacji oprogramowania lub obecność nieznanymi aplikacji na ekranie App Center mogą sugerować, że został zainstalowany złośliwy program. Zaleca się zainstalowanie i uruchomienie najnowszej wersji oprogramowania Malware Remover. Jeśli problem nadal będzie występować, skontaktuj się z zespołem pomocy technicznej QNAP.

## Q Jeśli jest konieczne udostępnienie niektórych usług w Internecie, co należy zrobić w celu zapewnienia bezpieczeństwa?

A Upewnij się, że na serwerze NAS są zainstalowane najnowsze wersje oprogramowania układowego i aplikacji. Aplikacja zapory QuFirewall zapewnia podstawową ochronę, a reguły „PSIRT” i „TOR” ułatwiają blokowanie niektórych połączeń nawiązywanych przez hakerów. Użytkownicy biznesowi i korporacyjni powinni korzystać z bardziej zaawansowanego rozwiązania zapory. Jeśli jest dostępne wolne miejsce w puli pamięci, można też tworzyć migawki w celu zapewnienia podstawowej ochrony danych. Zaleca się także prawidłowe tworzenie kopii zapasowych danych zgodnie z zasadą 3-2-1, aby się przygotować na najgorszy scenariusz i zapobiec potencjalnej utracie danych.

## Q Serwer NAS jest stary i nie obsługuje najnowszej wersji systemu QTS. Czy wciąż można bezpiecznie korzystać z tego serwera?

A W przypadku starszych modeli oraz modeli, których okres eksploatacji został zakończony, pomoc techniczna jest ograniczona. Takie serwery powinny być używane tylko do tworzenia kopii zapasowych w intranecie lub offline.

## Q Dlaczego wciąż jest wyświetlany komunikat o niepowodzeniu zalogowania do serwera NAS?

A Jeśli adres IP powiązany z nieudanym logowaniem pochodzi z Internetu, oznacza to, że trwa siłowy atak (brute force) na serwer NAS mający na celu złamanie hasła. Należy unikać udostępniania serwera NAS w Internecie i wzmocnić jego zabezpieczenia zgodnie z instrukcjami w tym samouczku. Jeśli adres IP powiązany z nieudanym logowaniem pochodzi z intranetu, sprawdź, czy na urządzeniu o tym adresie IP nie jest zainstalowane złośliwe oprogramowanie.

## Q Dlaczego wszystkie pliki mają dziwne nazwy?

**A** Jest to objaw infekcji przez oprogramowanie typu ransomware. Przejrzyj dzienniki dostępu do serwera NAS, aby ustalić, czy operacja szyfrowania została zainicjowana na serwerze NAS czy na innym komputerze. Jeśli serwer NAS został zaatakowany przez oprogramowanie typu ransomware, należy podjąć odpowiednie działania w celu powstrzymania rozprzestrzeniania się infekcji. W razie potrzeby skontaktuj się z zespołem pomocy technicznej firmy QNAP w celu uzyskania wsparcia.

## Q Co zrobić, jeśli serwer NAS został zainfekowany przez oprogramowanie typu ransomware?

**A** W większości programów typu ransomware są używane niezniszczalne metody szyfrowania. Bez prawidłowego klucza nie można odblokować plików, więc ich przywrócenie jest możliwe tylko za pomocą kopii zapasowej lub migawki.

Należy natychmiast zmodyfikować ustawienia routera zgodnie z instrukcjami w tym samouczku, aby uniknąć ujawniania serwera NAS w Internecie i zapobiec kolejnym atakom. Ponadto należy wstrzymać wszystkie zadania synchronizacji i ustawić trwałe przechowywanie migawek, aby uniknąć utraty plików kopii zapasowych. Jeśli są dostępne kopie zapasowe lub migawki danych, pliki można przywrócić po zaktualizowaniu aplikacji i oprogramowania układowego serwera NAS oraz przeprowadzeniu skanowania za pomocą aplikacji Malware Remover. Jeśli kopie zapasowe danych nie są dostępne, należy zachować informacje dotyczące żądania okupu i metody jego zapłaty, a następnie spróbować przywrócić niektóre dane przy użyciu metod takich jak odzyskiwanie danych. W razie potrzeby skontaktuj się z zespołem pomocy technicznej firmy QNAP w celu uzyskania wsparcia.

## Q Pojawiają się doniesienia medialne o łataniu luk w zabezpieczeniach produktów firmy QNAP. Czy to oznacza, że produkty QNAP nie są bezpieczne?

**A** Nie ma idealnego oprogramowania ani całkowicie niezawodnego sprzętu. Zarówno w oprogramowaniu zamkniętym (prawie zastrzeżonym), jak i oprogramowaniu typu open source, a także w urządzeniach, występują luki w zabezpieczeniach, które są wykrywane, a następnie naprawiane przez producentów. Tak jak inne duże firmy technologiczne firma QNAP stale naprawia wykryte luki, a następnie udostępnia użytkownikom odpowiednie pliki w celu jak najszybszego przeprowadzenia aktualizacji, która pozwala zapewnić bezpieczeństwo urządzeń i danych. Ponadto zespół QNAP PSIRT udostępnia powiadomienia dotyczące cyberbezpieczeństwa, aby umożliwić użytkownikom reagowanie na pojawiające się problemy. Firma QNAP traktuje kwestię luk w zabezpieczeniach w otwarty i przejrzysty sposób, ponieważ uważa, że użytkownicy mają prawo do informacji oraz że zwiększa to bezpieczeństwo produktów. Użytkownicy są również zachęceni do subskrybowania komunikatów informacyjnych QNAP, umożliwiających uzyskanie odpowiednich, dokładnych i kompletnych informacji, zanim pojawią się doniesienia medialne.

## Komunikaty informacyjne dotyczące bezpieczeństwa produktów QNAP:

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



## Q Na czym polega zasada tworzenia kopii zapasowych 3-2-1?

**A** Zasada 3-2-1 dotyczy dobrze znanej metody tworzenia kopii zapasowych w branży IT. Pozwala ona się przygotować na najgorszy scenariusz. Gwarantuje ona, że w przypadku awarii będą istnieć pliki kopii zapasowych umożliwiające przywrócenie danych i uniknięcie ich utraty.

Liczba „3” oznacza, że istnieją co najmniej trzy kopie zapasowe. „2” odpowiada minimalnej liczbie nośników pamięci masowej. Liczba „1” oznacza, że co najmniej jedna kopia jest przechowywana poza siedzibą firmy.

Z zasady 3-2-1 wynika, że dane z kopii zapasowych będzie można przywrócić niezależnie od charakteru przypadkowych zdarzeń, takich jak modyfikacja lub usunięcie danych, uszkodzenie sprzętu, infekcja wirusowa czy inne katastrofy, na przykład pożary i powodzie.

Aby spełnić wymagania tej zasady, serwer QNAP NAS udostępnia funkcje Hybrid Backup Sync 3 (HBS3), Replikacja migawek i SnapSync (obsługiwana tylko w systemie QuTS hero), które umożliwiają tworzenie kopii zapasowych danych z serwera NAS na zewnętrznym serwerze NAS lub urządzeniu pamięci masowej, innych serwerach plików i/lub urządzeniach albo w chmurze publicznej. To pozwala mieć pewność, że żadne dane nie zostaną utracone.

## Samouczki dotyczące aplikacji Hybrid Backup Sync 3 (HBS3):

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



## Samouczki dotyczące aplikacji Replikacja migawek:

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



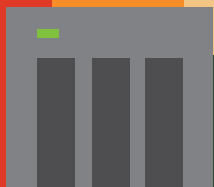
## Samouczki dotyczące aplikacji SnapSync:

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



Aby zwiększyć bezpieczeństwo i zapobiec manipulowaniu danymi, można dodać kopię zapasową offline lub kopię zapasową w pamięci masowej typu WORM (jednokrotny zapis, wielokrotny odczyt) w systemie QuTS hero.

NOTA



2 0 2 3

Przewodnik po zabezpieczeniach

# QNAP



## QNAP SYSTEMS, INC.

TEL.: +886-2-2641-2000 FAKS: +886-2-2641-0555 Adres e-mail: [qnapsales@qnap.com](mailto:qnapsales@qnap.com)

Adres: 3F, No.22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221, Tajwan

Firma QNAP może zmienić specyfikacje i opisy produktów w dowolnym czasie bez powiadomienia.

Copyright © 2023 QNAP Systems, Inc. Wszelkie prawa zastrzeżone.

QNAP® i inne nazwy produktów QNAP są znakami towarowymi lub zarejestrowanymi znakami towarowymi firmy QNAP Systems, Inc. Inne wymienione nazwy firm i produktów są znakami towarowymi ich właścicieli.