Průvodce zabezpečením

Pokyny pro ochranu, aby byl váš NAS bezpečný a zabezpečený

Bezpečnostní list - Základní věci, které nemůžete ignorovat

Při prvním spuštění NAS

Administrátor
Nepoužívejte výchozí nastavení!
Vytvořte nového administrátora

Hesla
Používejte zásady zadávání hesel

Dvoufázové ověřování
Zvyšuje bezpečnost uživatelských účtů

UPnP
Vypněte funkci Plug and Play, abyste se vyhnuli útočníkům

Každodenní / pravidelné úkoly

Záloha
Více než jedno místo pro zálohování!
Použijte strategii zálohování 3-2-1

Snímky
Průběžné zaznamenání dat pro obnovení v případě ztráty

Aktualizace
Udržujte software automaticky aktualizovaný

VPN
Vytvořte připojení VPN pro vzdálený přístup

Jednorázové úlohy - ochrana napořád

QuFirewall
Stáhněte si z APP centra a aktivujte

Security Counselor
Stáhněte si z APP centra a aktivujte

Bezpečnostní list - Rozšířená nastavení pro IT

Pro pokročilé uživatele

Úvod

Bezpečnostní průvodce

V tomto krátkém průvodci zabezpečením najdete několik užitečných vysvětlení, jaká nastavení můžete použít k zajištění optimální ochrany svých dat.
Vždy existuje kompromis mezi pohodlím a bezpečností, o kterém musí každý uživatel rozhodnout sám.
Tento průvodce poskytuje stručný přehled nejdůležitějších témat.
Podrobné informace a pokyny naleznete na adrese: https://www.qnap.com/cs-cz/

Co je ransomware?

Ransomware jsou škodlivé programy, které uzamknou počítač nebo zašifrují soubory a zablokují vám přístup k vlastním datům.
Oběti budou donuceni zaplatit výkupné za dešifrování napadených souborů, jinak nebudou moci napadené soubory již nikdy otevřít.

Jak se můžete chránit před ransomwarem?

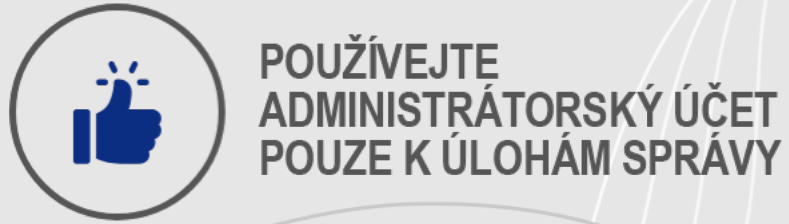
Ransomware je rostoucí hrozbou pro firemní i domácí uživatele, která se zaměřuje na počítače a síťová zařízení. Hackeři neustále hledají nové způsoby, jak umístit škodlivý software.
Společnost QNAP si je vědoma tohoto rostoucího nebezpečí a neustále pracuje na zajištění co nejlepší ochrany proti škodlivému softwaru.
Následující příklady vám mají ukázat, jak se můžete nejlépe chránit podle svých potřeb.

Při prvním spuštění NAS

Účet administrátora

Účet správce v systému QTS je ve výchozím nastavení "admin". Z bezpečnostních důvodů se nedoporučuje volit pro kritický účet systému obecné a snadno uhodnutelné jméno, protože tak případnému hackerovi stačí uhodnout správné heslo, aby získal úplnou kontrolu nad systémem. Chcete-li se před takovým scénářem ochránit, důrazně doporučujeme vytvořit jiný účet správce systému a zakázat výchozí účet "admin". Účet správce by navíc měl být používán pouze pro úkoly správy, jako jsou například úkoly údržby. Pro skutečné používání QNAP NAS se doporučuje striktně oddělit funkce správce a uživatelské funkce.

Poznámka: Možnost zakázat účet "admin" je k dispozici pouze ve verzi QTS 4.1.2 a novější.



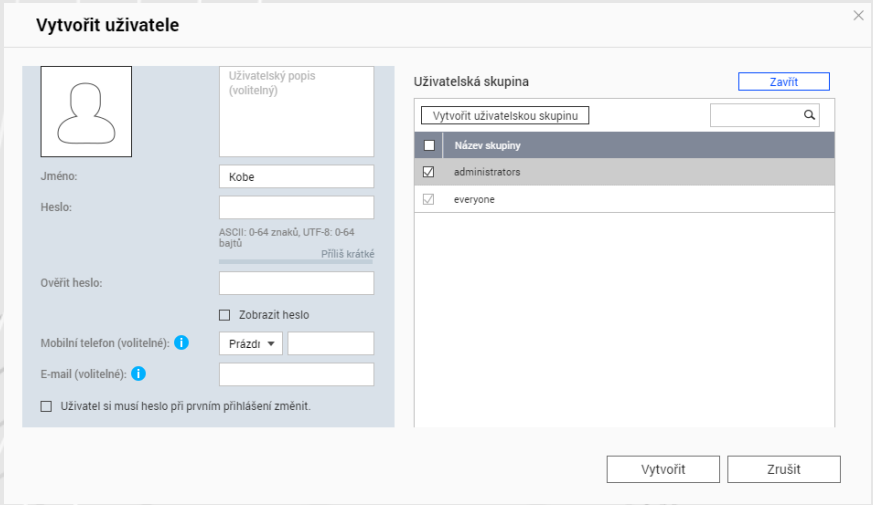
Při prvním spuštění NAS

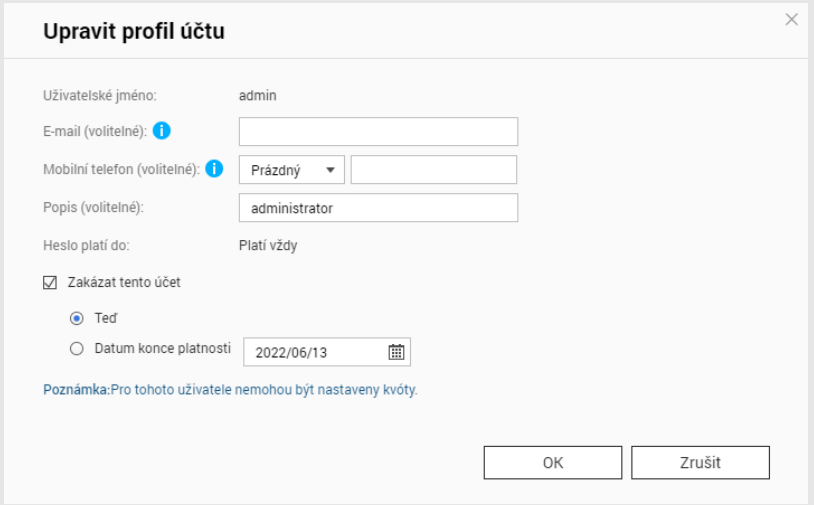
Jak deaktivovat uživatelský účet "Admin"

Pro hesla na QNAP NAS existuje několik možností nastavení, které výrazně zvýší zabezpečení vašeho systému.

Pokud používáte QNAP NAS výhradně sami, jste samozřejmě za zavedení doporučených pravidel pro hesla zodpovědní pouze vy.

Základní pravidla pro bezpečné heslo jsou jednoduchá:





Vytvoření nového účtu správce

1. Přihlaste se do systému QTS pomocí účtu "admin".
2. Vyberte možnost Ovládací panely > Uživatelé.
3. Vytvořte uživatele (v tomto příkladu „Kobe") a přiřaďte ho do skupiny uživatelů "Administrators".

Zakázání účtu "Admin"

1. Přihlaste se do systému QTS jako Kobe.
2. Vyberte možnost Ovládací panely > Uživatelé a upravte profil účtu "admin".
3. Klikněte na položku "Zakázat tento účet" a vyberte možnost "OK".

Při prvním spuštění NAS

Zásady pro zadávání hesel

Pokud jde o hesla na QNAP NAS, existuje několik možností nastavení, které výrazně zvýší zabezpečení vašeho systému.Pokud používáte QNAP NAS výhradně sami, jste samozřejmě za zavedení doporučených pravidel pro hesla zodpovědní pouze vy. Základní pravidla pro bezpečné heslo jsou jednoduchá:

Dostatečně dlouhé

Speciální znaky

Velká a malá písmena

Nikdy nepoužívejte stejné heslo pro různé aplikace

Pravidelná změna hesla

Pokud je QNAP NAS dostupný i pro jiné uživatele, měl by správce nastavit určitá pravidla pro hesla a nechat je QNAP NAS vynucovat. Tím se zajistí, že výše uvedená pravidla budou dodržována. Stručné vysvětlení naleznete na následující stránce.

Při prvním spuštění NAS

Zásady pro zadávání hesel

1. Přejděte na Ovládací panely > Systém > Zabezpečení > Zásady hesla.

2. V části Síla hesla vyberte kritéria

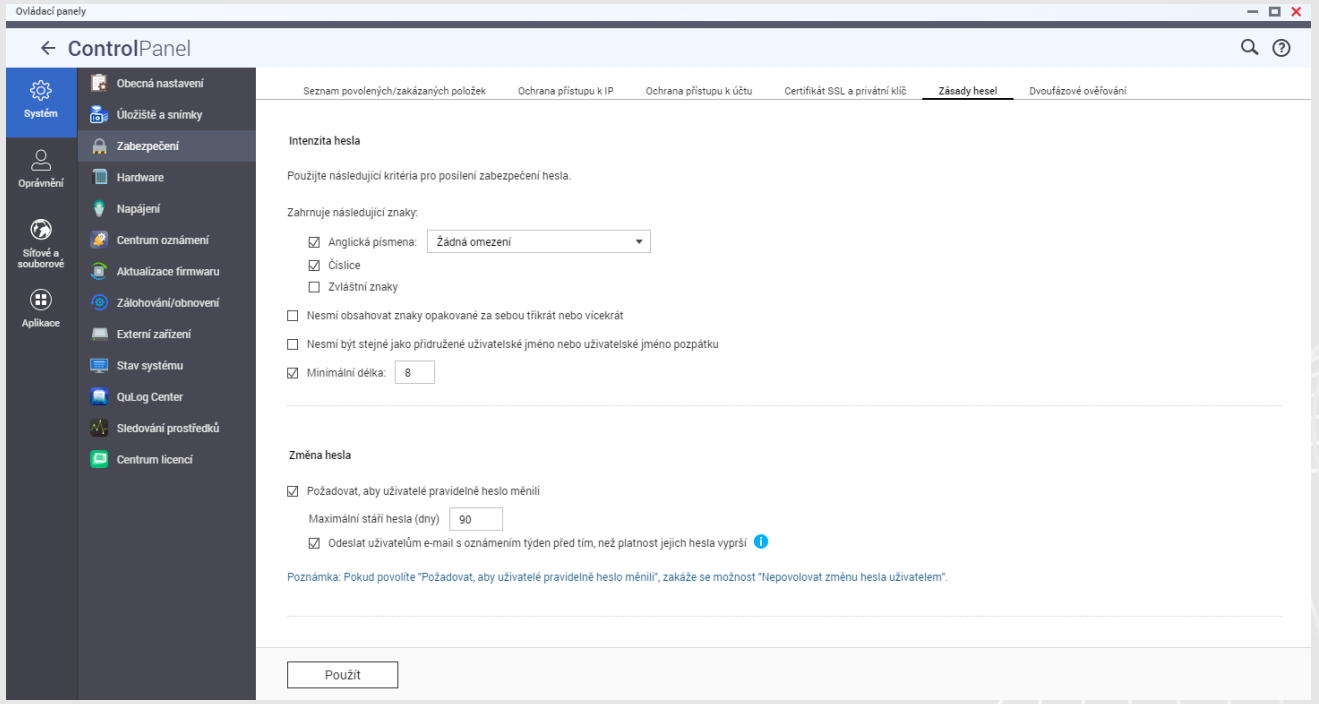
1. Nové heslo obsahuje alespoň tři znaky z následujících tříd: Malá písmena, velká písmena, číslice a speciální znaky.
2. Žádný znak v novém hesle se nesmí opakovat třikrát (nebo vícekrát) (příklad: AAA).
3. Heslo nesmí být stejné jako odpovídající uživatelské jméno, a to ani pozpátku.

3. V části Změna hesla vyberte možnost Vyžadovat od uživatelů pravidelnou změnu hesla.

Důležité: Povolením tohoto nastavení deaktivujete nastavení Zakázat uživatelům měnit heslo

1. Zadejte maximální počet dní, po které je heslo platné.
2. Nepovinné: Nastavte heslo: Zvolte možnost Odeslat uživatelům e-mail s oznámením týden před vypršením platnosti jejich hesla

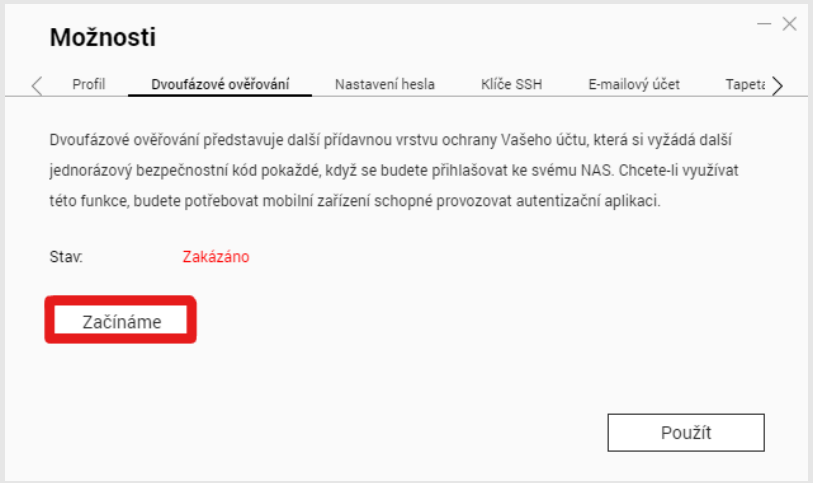
4. Klikněte na tlačítko Použít.

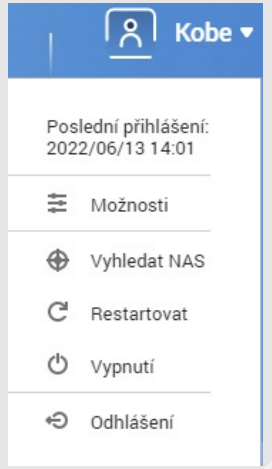


Při prvním spuštění NAS

Dvoufázové ověřování

Dvoufázové ověření zvyšuje zabezpečení uživatelských účtů. Po jeho aktivaci budete muset při každém přihlášení k NAS zadat kromě hesla také jednorázový bezpečnostní kód (6 číslic). Dvoufázové ověření vyžaduje mobilní zařízení s autentizační aplikací, která podporuje protokol TOTP (Time-based One-Time Password). Mezi podporované aplikace patří Google Authenticator (Android/iPhone/BlackBerry) nebo Authenticator (Windows Phone).Chcete-li tuto funkci používat, postupujte podle následujících kroků:





1. Nainstalujte aplikaci Authenticator do mobilního zařízení.
2. V části Síla hesla vyberte kritéria
3. Přejděte do nabídky "Možnosti" > "Dvoufázové ověření" a klikněte na tlačítko "Začínáme".
    1. Nakonfigurujte aplikaci autentizátoru naskenováním QR kódu nebo zadáním tajného klíče do aplikace.
    2. Zadejte kód vygenerovaný z aplikace do NAS a ověřte správnou konfiguraci.
    3. Pokud nemůžete použít mobilní zařízení, zvolte alternativní způsob ověření zasláním bezpečnostního kódu e-mailem nebo zodpovězením bezpečnostní otázky. Chcete-li zaslat bezpečnostní kód e-mailem, musí být server SMTP správně nakonfigurován v nabídce "Ovládací panel" > "Oznámení" >"E-mail".

Podrobné vysvětlení nastavení, naleznete na našich webových stránkách s návody: https://www.qnap.com/en/how-to/tutorial/article/how-to-enhance-account-security-using-2-step-verification.

Při prvním spuštění NAS

Universal Plug and Play (UPnP)

Technologie UPnP (Universal Plug and Play) se používá k ovládání zařízení (audio zařízení, směrovače, tiskárny, chytré televizory) různých výrobců. Umožňuje, aby si zařízení v síti navzájem rozuměla a aby se některé funkce spouštěly automaticky, aniž by se uživatel musel aktivovat. V tomto případě může například QNAP NAS pomocí UPnP instruovat směrovač, aby jednoduše propustil určité příchozí požadavky na připojení. Opět je na vás, abyste vyvažovali mezi pohodlím a bezpečností. Méně zkušeným uživatelům doporučujeme funkci UPnP na směrovači a v zařízení QNAP NAS zakázat. Informace o tom, jak provést tato nastavení ve směrovači, získáte od výrobce směrovače.

Důležité:

Pokud je ve vašem směrovači povolena funkce UPnP, bude jakýkoli software a zařízení ve vaší domácí síti možnost směrovač nastavit podle potřeby. Je tedy možné, že některé porty budou otevřeny v bráně firewall. Ty to porty slouží jako vstup pro útoky zvenčí.

Nepřipojujte NAS k síti WAN z modemu, důrazně doporučujeme umístit NAS za směrovačem.

Zakázání předávání UPnP na QNAP NAS

1. Přejděte na myQNAPcloud > Automatická konfigurace směrovače
2. Zrušte zaškrtnutí políčka "Povolit předávání portů UPnP" a stiskněte tlačítko Použít

Každodenní / pravidelné úkoly

Strategie zálohování 3-2-1

Záloha

Je individuální otázkou, kde, jak a jak často zálohovat data. Rozhodujícími faktory jsou přitom bezpečnostní potřeby, důležitost dat a dostupné možnosti.

Existuje však pravidlo, které je třeba dodržovat, abyste spolehlivě zálohovali důležitá data.

Důležité: RAID není zálohování, chrání vás před selháním pevného disku. Snímky vás chrání před útoky ransomwaru z místního počítače.

Strategie zálohování 3-2-1

Zatímco první linií obrany proti napadení škodlivým softwarem je opatrnost a dodržování rozumných návyků při používání (pravidelná aktualizace softwaru, neotevírání nedůvěryhodných e-mailů, nenavštěvování neznámých webových stránek atd), vždy byste měli pamatovat na zálohování dat.

Žádný zálohovací plán není dokonalý, ale Strategie zálohování 3-2-1 je dobrý začátek. Uchovávejte 3 kopie důležitých souborů, soubory uchovávejte alespoň na 2 typech paměťových médií a 1 kopii uložte mimo pracoviště.

Důležitá data by měla být zálohována alespoň ve **3 kopiích**: 1 hlavní soubor a 2 záložní soubory.

Jedna ze záloh se ukládá mimo pracoviště (mimo domov nebo firmu).

Archivy jsou uloženy na **dvou různých** zálohovacích médiích, aby byly chráněny před různými typy nebezpečí.

Každodenní / pravidelné úkoly

Snímky

Co jsou snímky?

Snímky jsou obrazy dat uložených na vašem QNAP NAS. Při prvním pořízení snímku je zachyceno celé vaše úložiště. Všechny následující snímky pak zaznamenávají pouze obsah, který se od posledního snímku změnil. Snímky velmi šetří místo, protože jsou založeny na blocích.

Důležité:

Snímek není záloha. Umožňuje přístup k předchozím verzím pro případ, že byly omylem odstraněny nebo byl omylem změněn obsah.

Podrobný popis tohoto tématu najdete na našich webových stránkách:
https://www.qnap.com/cs-cz/software/snapshots

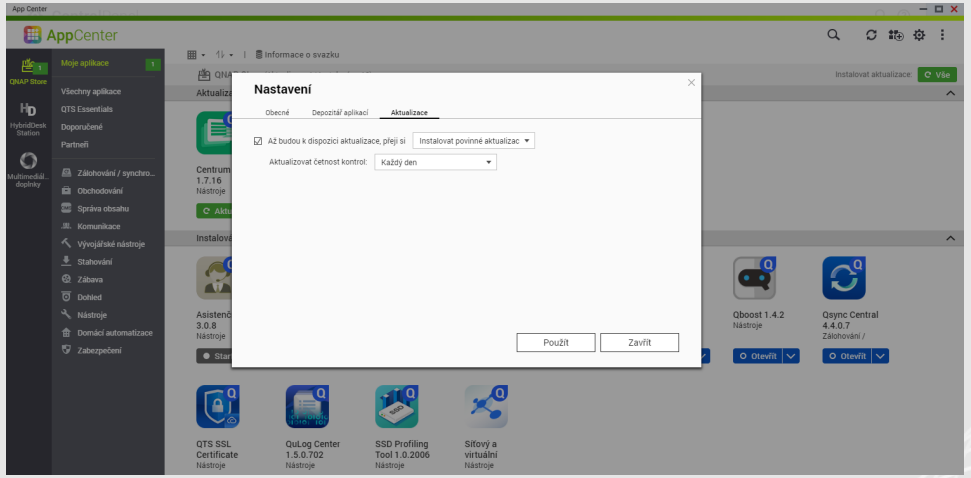
Nastavení snímků

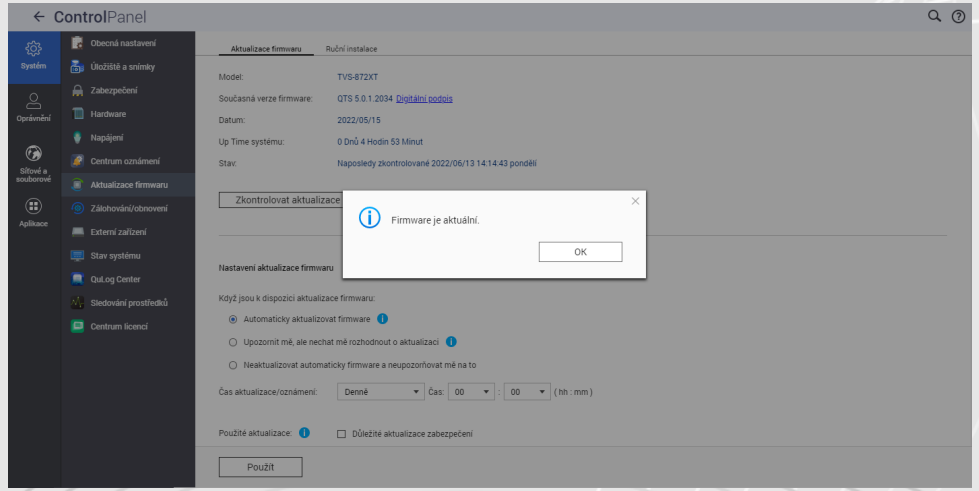
Každodenní / pravidelné úkoly

Automatické aktualizace

Aktualizace

Aktualizovaný systémový software je u vašeho NAS důležitý. Společnost QNAP neustále pracuje na uzavření bezpečnostních hrozeb a občas přidává do systému nové funkce. Aktualizace by proto měly být vždy použity neprodleně, aby byla vaše data co nejlépe chráněna. Pokud je váš QNAP NAS připojen k internetu a nezměnili jste výchozí nastavení, zařízení automaticky zkontroluje nejnovější systémový software a upozorní vás na něj.
Měli byste se pak ujistit, že jste jej aktualizovali. Uvědomte si, že zařízení QNAP NAS bude k tomu potřebovat restartovat a bude po dobu 5-10 minut nedostupný. Máte také možnost ručně nainstalovat nejnovější systémový software. To je nutné v případě, že váš QNAP NAS není připojen k internetu, a proto nemůže automaticky zkontrolovat a stáhnout aktualizace. Pokud chcete zjistit, zda je váš firmware aktuální, proveďte následující kroky.





Aktualizace firmwaru v reálném čase

1. Přihlaste se jako "Administrator".

2. Otevřete Ovládací panely > Aktualizace firmwaru

3. Otevřete Live Update

4. Klikněte na možnost Zkontrolovat aktualizaci

Automatická aktualizace aplikací

1. Přejděte do Centra aplikací

2. Přejděte do nastavení

3. Otevřete Aktualizace

4. Vyberte možnost "Když jsou k dispozici aktualizace...".

5. Vyberte možnost Instalovat všechny aktualizace automaticky

Každodenní / pravidelné úkoly

VPN

Co je VPN?

VPN je virtuální privátní síť. V našem případě je určena k vytvoření zabezpečeného přístupu k zařízení QNAP NAS pokud jste na cestách. Server VPN běží na QNAP NAS a speciální software VPN běží na zařízení, které se používá pro vzálené připojení. Mezi těmito dvěma zařízeními je vytvořen tunel přes internet. Výhodou je, že připojení je chráněno ověřováním a šifrováním a mohou ho používat pouze oprávněné osoby. Takové spojení VPN se tedy chová stejně, jako kdyby byla obě zařízení přihlášena do stejné sítě. To znamená, že k místním zdrojům je možné přistupovat bez dalšího omezení. Jednou nastavené připojení VPN lze snadno používat opakovaně a je zaručen bezpečný přístup do domácí sítě. Na cestách vždy doporučujeme navázat připojení přes VPN. Rychlost přenosu dat tím sice poněkud trpí, ale připojení je bezpečné.

Jak nastavit a používat síť VPN?

Podrobné vysvětlení nastavení, najdete na našich webových stránkách s návody:
https://www.qnap.com/en/how-to/tutorial/article/how-to-set-up-and-use-qvpn

Doporučení pro vzdálený přístup

myQNAPcloud Link a VPN (vyžadováno přesměrování portů služby VPN, pro lepší ochranu doporučujeme povolit QuFirewall).

Jednorázové úlohy

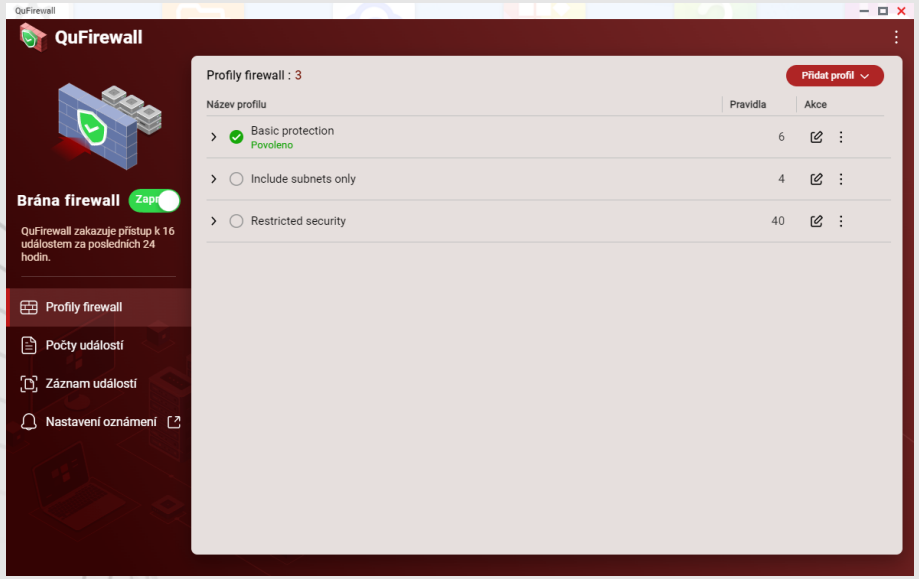
QuFirewall

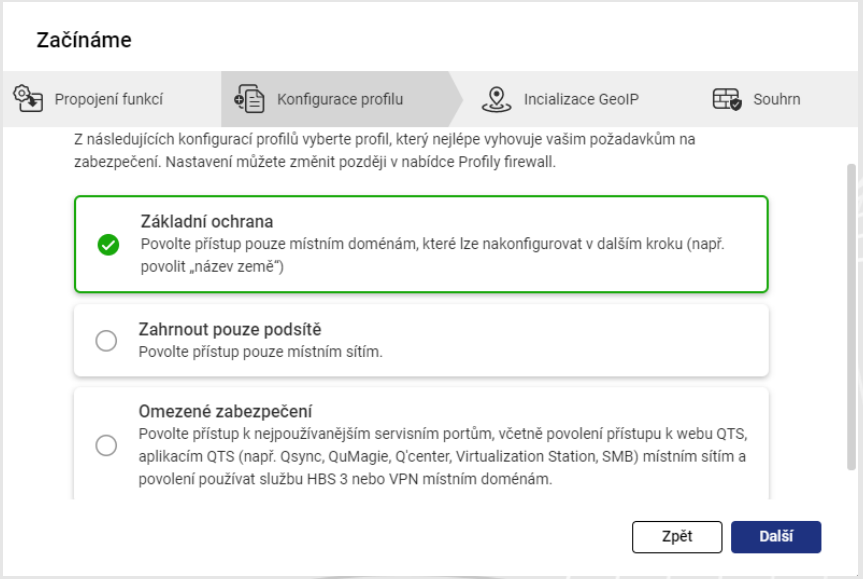
Co je QuFirewall

QuFirewall je aplikace pro správu brány firewall pro zařízení QNAP. Díky integraci výkonného a snadno použitelného systému profilování vám QuFirewall umožňuje kontrolovat a ověřovat připojení k vašemu zařízení. Společnost QNAP doporučuje nainstalovat QuFirewall na vaše QNAP NAS zařízení a omezit povolené IP adresy na určitou oblast nebo podsíť.

Nastavení QuFirewall

1. Nainstalujte QuFirewall z Centra aplikací
2. Vyberte konfiguraci profilu
3. Zvolte svůj region
4. Klikněte na tlačítko Dokončit





Jednorázové úlohy

Security Counselor

Co je to "Security Counselor"?

Security Counselor je váš bezpečnostní portál pro QNAP NAS. Prověřuje váš systém na zranitelná místa a poskytuje doporučení k ochraně vašich dat před různými způsoby útoků.

Na základě bezpečnostních požadavků vašeho síťového prostředí si můžete vybrat jednu ze tří výchozích bezpečnostních zásad (základní / středně pokročilá / pokročilá).

Funkce Kontrola zabezpečení při skenování systému použije vybranou zásadu. Můžete také nakonfigurovat vlastní zásady výběrem Vlastní bezpečnostní zásady.

Základní

Středně pokročilá

Pokročilá

Vlastní

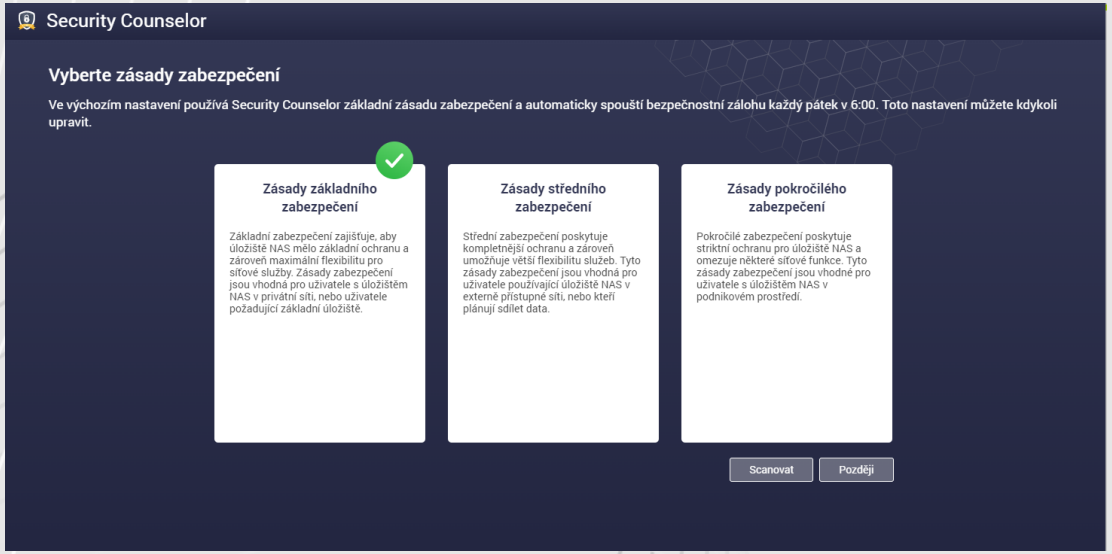
Bezpečnostní kontrolu lze provádět ručně nebo podle plánu, aby byla zajištěna maximální ochrana. Plán lze nastavit různými způsoby (denně / pracovní den / víkend / konkrétní den v týdnu), aby nebyla přerušena vaše práce. Na výsledky kontroly můžete kliknout a Security Counselor vás navede do příslušné části systému, kde můžete změnit související nastavení pro zabezpečení NAS.

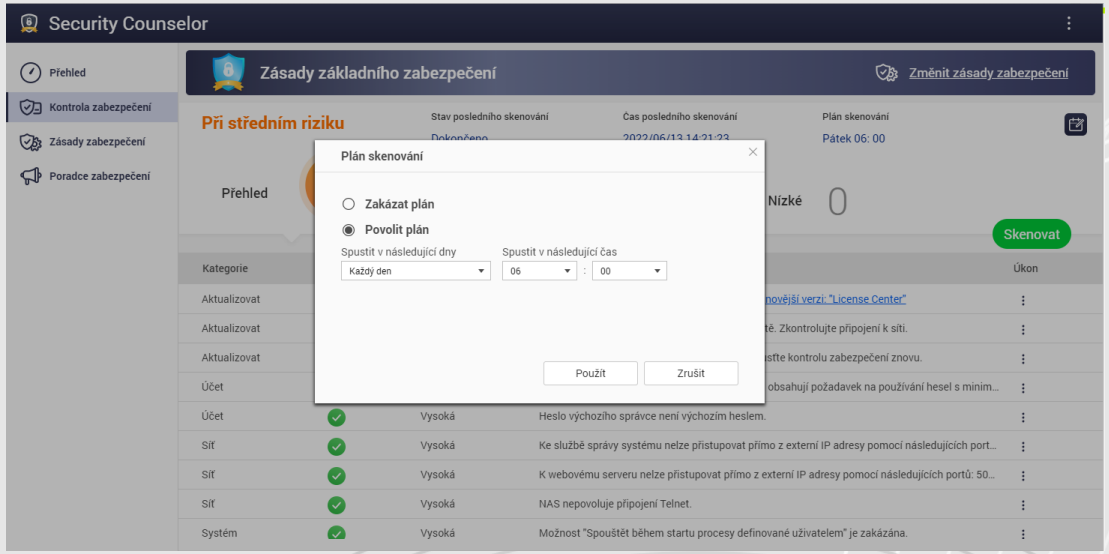
Jednorázové úlohy

Security Counselor

Nastavení služby "Security Counselor"

1. Stáhněte si aplikaci Security Counselor z Centra aplikací
2. Vyberte bezpečnostní zásady a klikněte na tlačítko Skenovat nyní
3. Chcete-li vytvořit plán, přejděte na položku Kontrola zabezpečení (zelená).
4. Přejděte na Plán skenování (ikonka)
5. Vyberte požadované časy a klepněte na tlačítko Použít





Rozšířená nastavení

Šifrované připojení

Používání šifrovaných připojení HTTPS

Pokud se chcete ke svému QNAP NAS připojit mimo vlastní síť, měli byste se ujistit, že jsou data šifrována. To vás ochrání před třetími stranami, které by mohly "číst" vaše data. To můžete zajistit použitím chráněných připojení. Jedná se například o HTTPS místo HTTP nebo FTPS místo FTP. Písmeno S znamená "Secure". Přenos dat je nyní šifrován pomocí certifikátu, takže je zajištěna pravost příslušné strany.

1. Otevřete Ovládací panely > Systém > Zabezpečení a přejděte do části SSL certifikát a soukromý klíč .

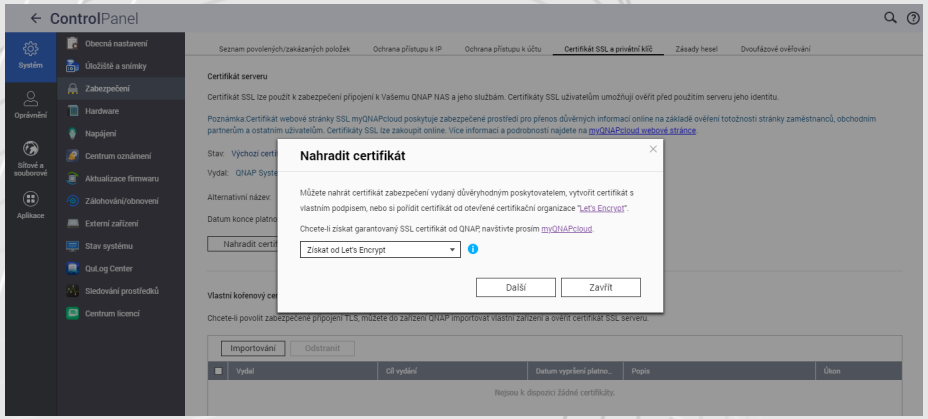
2. Klepněte na tlačítko Nahradit certifikát.

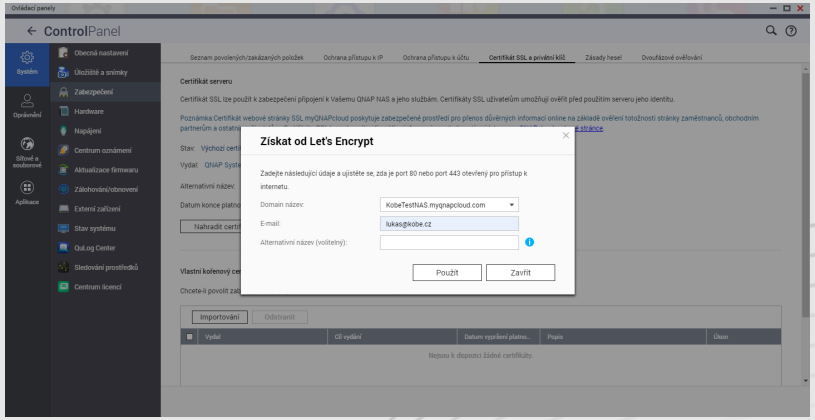
3. Vyberte možnost Získat z Let's Encrypt.

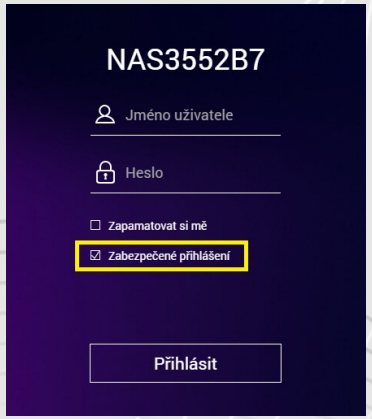
4. V části Název domény zadejte název nebo DDNS, pod kterým je NAS dostupný.

5. Zadejte svou e-mailovou adresu pro registraci u služby Lets's Encrypt.

6. Při přihlašování do webového rozhraní vyberte možnost Zabezpečené přihlášení.







Rozšířená nastavení

Porty

Co jsou to porty?

Port umožňuje komunikaci mezi vaším počítačem a jiným počítačem přes internet. Brána firewall nepoužívané porty uzavírá, aby se přes ně do počítače nedostal škodlivý software. Nastavením přesměrování portů můžete používat online služby a další internetové aplikace, které přijímají připojení z internetu, nebo umožnit uživatelům na internetu přístup k webovým a vzdáleným serverům a dalším službám ve vaší domácí síti.

Změna výchozích portů

V konfiguraci směrovače byste měli změnit výchozí porty, například 21, 22, 80. 443. 8080 a 8081 na náhodná vlastní čísla portů. Například změňte číslo portu 8080 na 9527. Informace o tom, jak to provést, získáte od výrobce směrovače.

NEPŘEDÁVEJTE "systémový port" / nepotřebné porty služeb (např. SSH, Telnet).

Zakázáním přesměrování portů na nepotřebných servisních portech můžete snížit plochu útoku. Po přesměrování portů může mít k těmto portům služeb přístup kdokoli přes internet.

Instrukce v angličtině

Zálohování:	https://www.qnap.com/en/how-to/tutorial/article/hybrid-backup-sync
Účet administrátora:	https://www.qnap.com/en/how-to/faq/article/can-i-rename-the-default-admin-account
Zásady pro zadávání hesel:	https://www.qnap.com/en/how-to/knowledge-base/article/setup-the-password-policy-to-require-the-change-periodically
UPnP:	https://docs.qnap.com/nas-outdated/QTS4.3.5/en/GUID-907F01D9-68D9-4449-A4D1-3213E19D0124.html?
Šifrování:	https://www.qnap.com/en/how-to/tutorial/article/how-to-use-ssl-certificates-to-increase-the-connection-security-to-your-qnap-nas
VPN:	https://www.qnap.com/en/how-to/tutorial/article/how-to-set-up-and-use-qvpn
Přesměrování portů:	https://www.qnap.com/en/how-to/faq/article/how-do-i-set-up-port-forwarding-on-the-nas
Jak používat QuFirewall:	https://www.qnap.com/en/how-to/tutorial/article/how-to-use-qufirewall
Aktualizace:	https://www.qnap.com/en/how-to/tutorial/article/how-to-update-your-qnap-nass-firmware
Security Counselor:	https://www.qnap.com/solution/security-counselor/cs-cz/