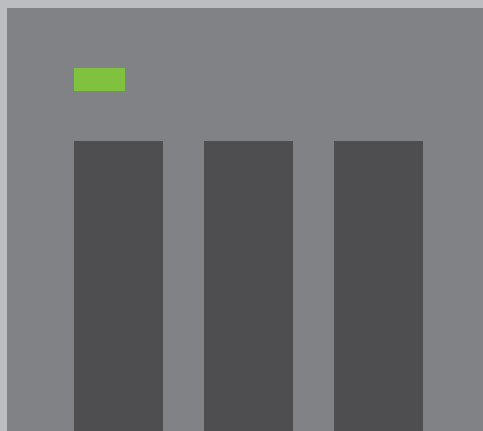


2 0 2 3

Guide de sécurité



2 0 2 3

Guide de sécurité

INDEX

- 1 Préface
- 2 Attaques courantes
- 3 Concepts de base de l'équipement réseau
- 4 Différentes façons de se connecter au NAS par Internet

Évitez d'exposer le NAS à Internet

- 8 Connecter le NAS correctement
- 9 Vérifier les paramètres du routeur
- 12 Vérifier les paramètres du NAS
- 15 Liste de contrôle des paramètres liés au réseau

Paramètres de sécurité du NAS

- 17 Configurer les notifications système
- 24 Activer la mise à jour automatique du firmware (QTS / QuTS hero)
- 25 Paramètres de mise à jour de l'application
- 27 Désactiver ou supprimer les fonctions inutiles
- 29 Désactiver Telnet/SSH
- 30 Renforcer la sécurité du compte système
- 34 Définir la stratégie de mot de passe
- 35 Activer la protection d'accès (IP / compte)
- 36 Activer la vérification en deux étapes (2SV)
- 39 Modifier les ports par défaut
- 40 Afficher les journaux d'accès
- 41 Installer et activer les applications de sécurité
- 42 Conseiller de sécurité
- 45 Malware Remover
- 46 QuFirewall
- 51 Activer les snapshots planifiés
- 53 Définir la stratégie de suppression des snapshots
- 54 Liste de contrôle des paramètres de sécurité du NAS

QNAP attache une grande importance à la sécurité. Face aux menaces de plus en plus nombreuses, QNAP a sans cesse amélioré ses conceptions matérielles et logicielles pour offrir aux utilisateurs des solutions à la fois sûres et pratiques.

L'équipe de réponse aux incidents de sécurité des produits (PSIRT pour Product Security Incident Response Team) de QNAP est responsable de la gestion des problèmes de sécurité liés aux produits QNAP. En plus de gérer les incidents liés à la cybersécurité, la PSIRT gère également le signalement, l'investigation, la correction et l'annonce des vulnérabilités dans divers produits.

QNAP s'engage également à améliorer la sécurité des produits. Dans le passé, les produits étaient conçus pour être plus pratiques et plus faciles à configurer et à utiliser pour les utilisateurs. Avec l'augmentation des cyberattaques contre les appareils en réseau ces dernières années, la perspective de conception des produits de QNAP a également changé. Ainsi, les produits intègrent l'aspect sécuritaire dès leur conception. Il s'agit d'une « Sécurité par le design » qui protège les utilisateurs et leur permet de faire face aux menaces qui les concernent.

Le didacticiel aidera les utilisateurs à configurer correctement le NAS pour améliorer la sécurité. Si vous avez des questions, contactez notre équipe de support technique pour obtenir de l'aide :



Pour les vulnérabilités des produits et les informations sur les incidents liés à la sécurité, consultez et abonnez-vous aux Avis de sécurité QNAP :

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



Service client QNAP :

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



Pour savoir comment se défendre contre les cyberattaques, il faut savoir comment elles sont lancées. En ce qui concerne les attaques sur les NAS, la plupart sont lancées via Internet. Les attaques sont principalement de deux types : « craquage de mot de passe » et « attaque de vulnérabilité ». Ici, « l'attaque de vulnérabilité » peut être divisée en « jour N » et « jour 0 ».

« jour N » fait référence à l'exploitation d'une vulnérabilité corrigée pour lancer une attaque. Il faut savoir que la plupart des attaques actives actuelles entrent dans cette catégorie. Vous pouvez vous défendre efficacement contre de telles attaques en veillant à toujours installer les derniers correctifs et mises à jour de sécurité.

« jour 0 » signifie exploiter une vulnérabilité inconnue pour lancer une attaque. En outre, les fournisseurs ne peuvent publier des correctifs de sécurité qu'après coup. Ces attaques ne peuvent être efficacement défendues qu'en empêchant les attaquants de se connecter à l'appareil.

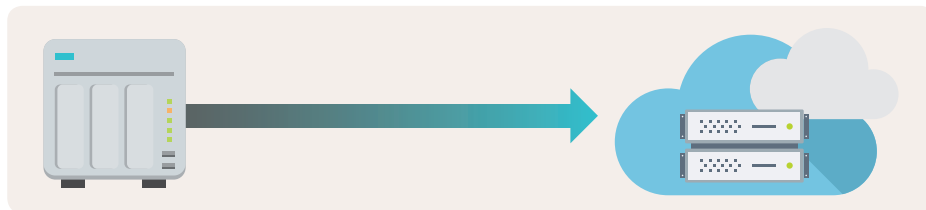
Le tableau suivant montre les réponses aux différentes attaques pour aiguiller les utilisateurs.

Réponse	Attaques		
	Craquage de mot de passe	Attaque de vulnérabilité (jour N)	Attaque de vulnérabilité (jour 0)
Éviter l'exposition à Internet	V	V	V
Mettre à jour le logiciel (système et applications)	X	V	Δ
Activer la mise à jour automatique (système et applications)	X	V	Δ
Utiliser des mots de passe forts pour tous les comptes	V	X	X
Désactiver le compte « admin » par défaut	V	X	X
Activer la vérification en 2 étapes	V	X	X
Autoriser la protection d'accès	Δ	X	X
Activer le pare-feu	Δ	Δ	Δ
Recevoir des notifications système	Δ	Δ	Δ
Modifier les ports par défaut	Δ	Δ	Δ
Désactiver/supprimer les fonctions inutiles	Δ	Δ	Δ
V : X efficace : Δ non efficace : Peut-être efficace (signifie que l'attaque peut être atténuée ou le risque d'être attaqué réduit)			

« Éviter l'exposition à Internet » peut empêcher efficacement les attaquants de se connecter et de lancer des attaques sur votre appareil. Ce didacticiel commence par « Éviter l'exposition à Internet », puis fournit un didacticiel complet « Paramètres de sécurité du NAS » pour améliorer les capacités défensives du NAS.

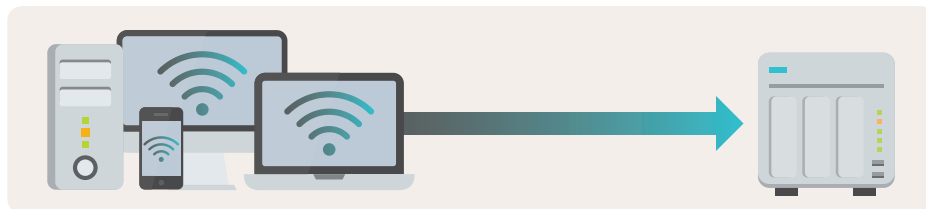
En tant que périphérique en réseau, le NAS a deux sens de connexion.

01 | Connexion externe du NAS



Un NAS nécessite généralement une connectivité externe pour fonctionner correctement. Par exemple, les fonctions système de base telles que les mises à jour automatiques et l'envoi de notifications. De plus, si vous avez besoin de sauvegarder des données du NAS sur un cloud public ou d'utiliser le NAS pour sauvegarder des données à partir d'autres appareils ou de clouds publics (tels que des machines virtuelles, Google Workspace ou Microsoft 365), des ordinateurs ou des serveurs, le NAS doit pouvoir initier des connexions sortantes.

02 | Autres appareils (tels que des ordinateurs, des mobiles ou d'autres serveurs) se connectant au NAS



Si vous avez besoin d'utiliser des fonctions ou des services fournis par le NAS, y compris l'accès aux fichiers, l'accès à l'interface des paramètres, vous devez être en mesure d'initier des connexions au NAS.

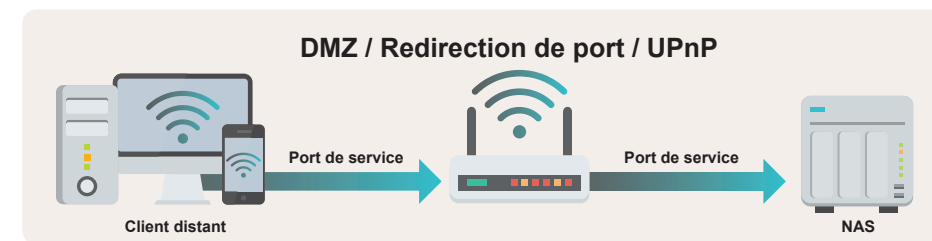
Si votre routeur n'a pas de DMZ, de redirection de port ou d'UPnP, le routeur bloquera le trafic provenant d'Internet. Seuls les appareils du réseau local pourront accéder au NAS.

Lorsque le routeur est activé et que les fonctions ci-dessus sont définies, tout le monde sur Internet peut se connecter au port ouvert, puis transférer vers le NAS conformément aux règles du routeur, puis se connecter et utiliser les fonctions associées normalement. Cependant, il fournira également aux pirates les moyens d'attaquer avec le craquage de mots de passe ou l'exploitation de vulnérabilités logicielles, posant ainsi des risques de sécurité.

01 | Activer et configurer DMZ, la redirection de port ou UPnP sur le routeur

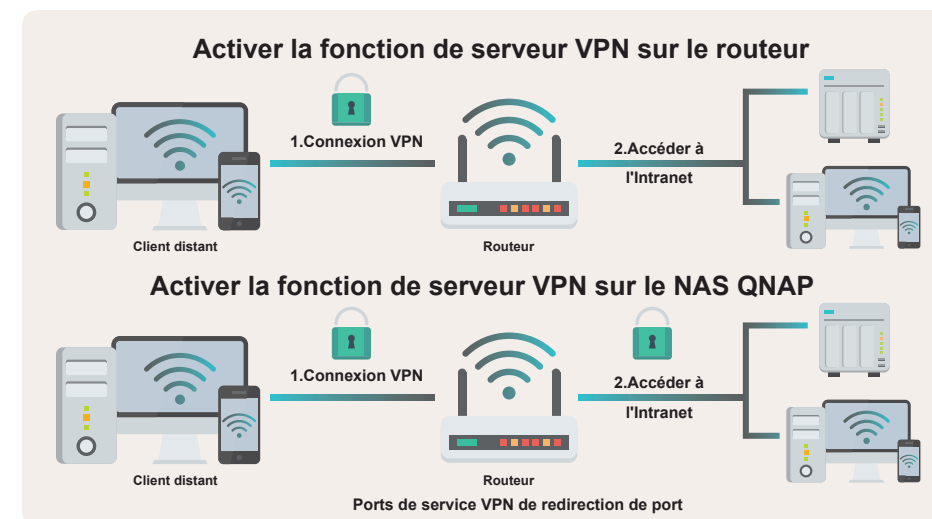
Cette méthode comporte des risques de sécurité. À moins que vous ne soyez un expert en configuration réseau et que vous compreniez les risques encourus, **QNAP vous déconseille de l'utiliser***. Étant donné que le routeur transmettra le trafic aux périphériques intranet, s'il n'y a pas de pare-feu installé entre le routeur et le NAS pour bloquer le trafic malveillant, les pirates peuvent facilement lancer des attaques réseau. Cependant, même si un pare-feu est installé (en utilisant un pare-feu de base ou en achetant un pare-feu de niveau entreprise), il n'est pas garanti qu'il bloque toutes les attaques.

* QNAP recommande uniquement d'ouvrir des ports de service VPN à risque relativement faible sur Internet, tandis que d'autres ports de service à haut risque tels que la gestion du système, les services SMB et SSH ne doivent pas être facilement accessibles depuis Internet.



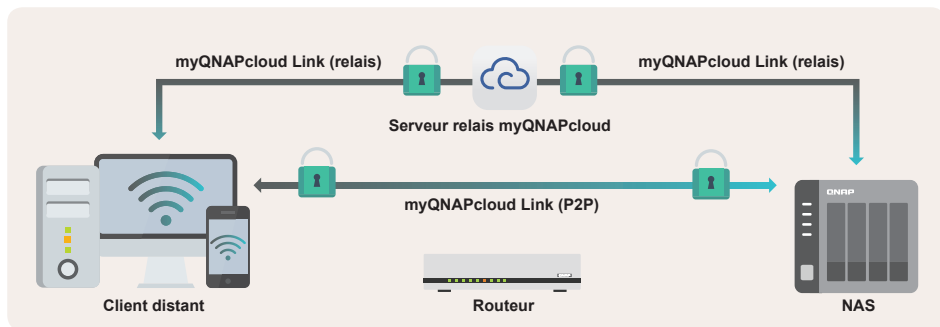
02 | Activer la fonction de serveur VPN sur le routeur ou le NAS QNAP

Certains routeurs prennent en charge les fonctions de serveur VPN (telles que les routeurs des séries QNAP QHora et QMiro), tandis que le NAS QNAP prend également en charge plusieurs serveurs VPN. Une fois activé et correctement configuré, vous pouvez accéder à chaque appareil sur l'intranet avec une connexion chiffrée VPN d'Internet au serveur VPN, offrant un haut niveau de sécurité.



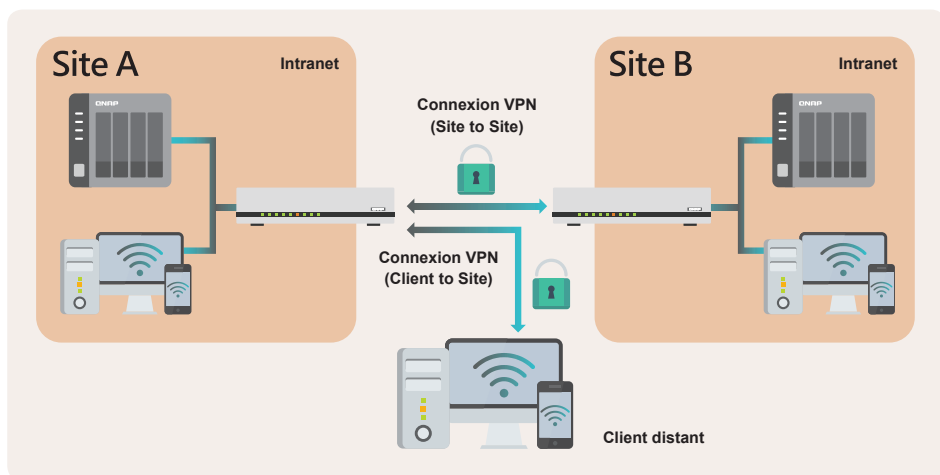
03 | Utiliser la connexion sécurisée myQNAPcloud Link

La configuration du routeur n'est pas nécessaire si vous utilisez myQNAPcloud Link pour vous connecter au NAS, car il peut ouvrir le service NAS directement sur Internet. myQNAPcloud Link établira une connexion via un serveur relais ou une technologie peer-to-peer (P2P) en fonction de l'environnement réseau. L'intégralité de la connexion sera chiffrée pour assurer la sécurité.



04 | Utiliser des produits SD-WAN ou Site-to-Site VPN

Contrairement à la fonction de serveur VPN (Client-to-Site VPN) mentionnée ci-dessus, SD-WAN ou Site-to-Site VPN établit une connexion VPN chiffrée sécurisée entre deux ou plusieurs routeurs situés à différents endroits. En termes simples, les appareils d'un réseau Site-to-Site VPN peuvent être connectés les uns aux autres comme s'ils se trouvaient sur le même intranet, ce qui le rend idéal pour les utilisateurs répartis sur plusieurs sites. Avec Client-to-Site VPN, vous pouvez accéder à votre NAS de n'importe où.



Vous pouvez choisir une méthode de connexion qui vous convient selon le tableau comparatif. QNAP dispose de plusieurs solutions de connexion sécurisée pour répondre aux besoins des utilisateurs.

Méthode de connexion	Avantages	Désavantages	Utilisateurs appropriés
Activer et configurer le routeur DMZ/Redirection de port de UPnP	<ul style="list-style-type: none">Connexion la plus rapide	<ul style="list-style-type: none">Vulnérable aux cyberattaquesAucune défense contre les attaques de vulnérabilité jour 0	<ul style="list-style-type: none">Avoir une compréhension claire des risques associésFamilier avec les paramètres réseauAvoir créé plusieurs sauvegardes pour les données importantesAvoir un plan de reprise après sinistre
Activer le serveur VPN sur le routeur*	<ul style="list-style-type: none">Relativement simple à mettre en place	<ul style="list-style-type: none">Aucune notification d'échec de connexion, blocage automatique et fonction de pare-feuMoins de protocoles VPN pris en chargePerformances limitées par le matériel du routeur	<ul style="list-style-type: none">Pas familier avec les paramètres réseauNe se soucie pas de la vitesse de transmission
Activer la fonction de serveur VPN sur le NAS QNAP*	<ul style="list-style-type: none">Prend en charge plusieurs protocoles VPNCompatible avec le pare-feu NAS (QuFirewall)Prend en charge la notification d'échec de connexion et le blocage automatique	<ul style="list-style-type: none">Les paramètres sont un peu plus compliqués	<ul style="list-style-type: none">Familier avec les paramètres réseauBesoin d'accéder fréquemment à de nombreux fichiers sur Internet
 Utiliser la connexion sécurisée myQNAPcloud Link	<ul style="list-style-type: none">Le plus simple à configurerPrise en charge du contrôle d'accèsLe NAS n'a pas besoin d'être exposé à Internet	<ul style="list-style-type: none">Connexion plus lente	<ul style="list-style-type: none">Pas familier avec les paramètres réseauAccès au NAS depuis Internet rareEnvironnement réseau où l'adresse IP WAN ne peut pas être obtenue
Utiliser des produits SD-WAN ou Site-to-Site VPN*	<ul style="list-style-type: none">Une fois configuré, les utilisateurs de l'intranet peuvent l'utiliser sans ressentir aucune différencePrend également en charge le VPN client to site	<ul style="list-style-type: none">Équipement supplémentaire requis	<ul style="list-style-type: none">Nécessite un accès multipoint et une sauvegarde à distanceNécessite des applications à valeur ajoutée

* Le NAS QNAP prend en charge :

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

* Le routeur QNAP prend en charge :

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

Fait référence aux routeurs domestiques généraux

01

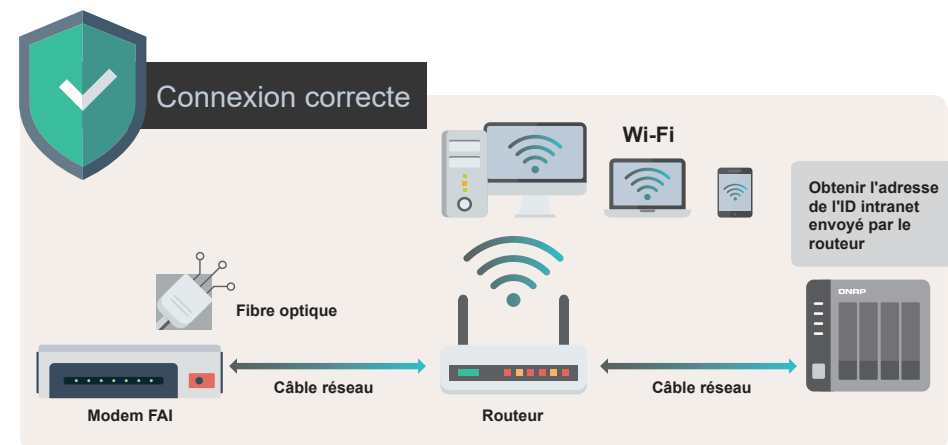
Guide des paramètres de sécurité du NAS

Évitez d'exposer le NAS à Internet

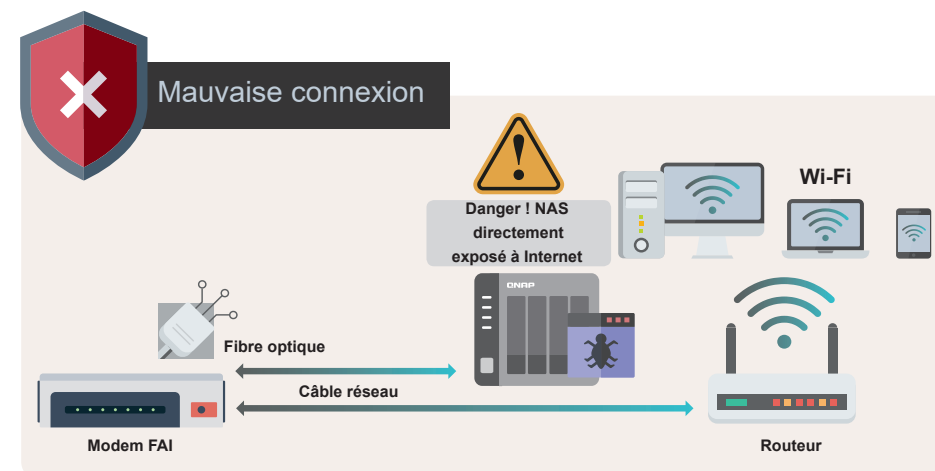


Connectez le NAS correctement

Assurez-vous que votre NAS est connecté au routeur. Avec une configuration appropriée, le routeur peut bloquer les connexions Internet pour vous, permettant à votre NAS de se cacher d'Internet et d'éviter les cyberattaques.



Si vous connectez le NAS au modem fourni par le FAI, votre NAS obtiendra directement l'adresse IP WAN. Dans ce cas, n'importe qui (y compris les pirates) peut se connecter à votre NAS via Internet, et même essayer d'attaquer et de s'introduire.

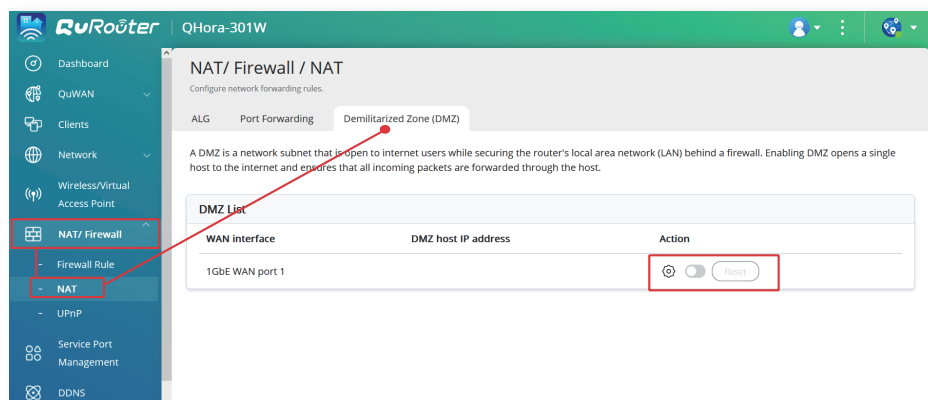
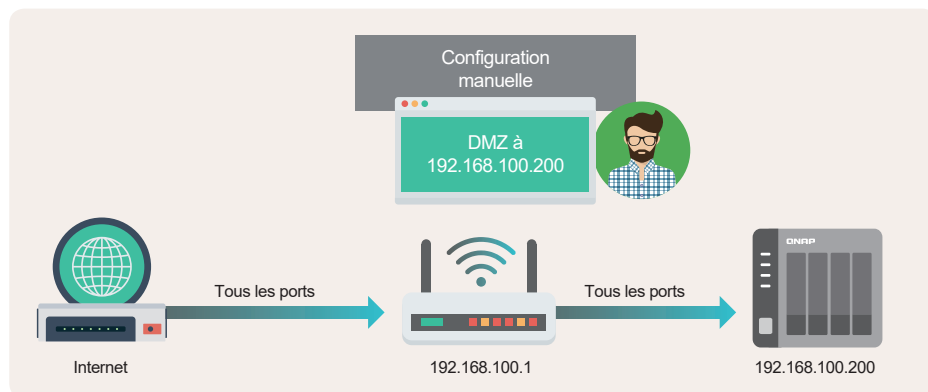


Vérifiez les paramètres du routeur

Par défaut, personne ne peut théoriquement se connecter directement depuis Internet à votre appareil derrière le routeur, mais si vous activez « DMZ (Demilitarized Zone) », « Redirection de port » ou « UPnP (Universal Plug and Play) », votre routeur transmettra paquets vers votre appareil sélectionné selon les règles que vous avez définies, exposant ainsi votre appareil à Internet. Si ce n'est pas nécessaire, vous devez vérifier et vous assurer que les fonctions suivantes sont **désactivées**.

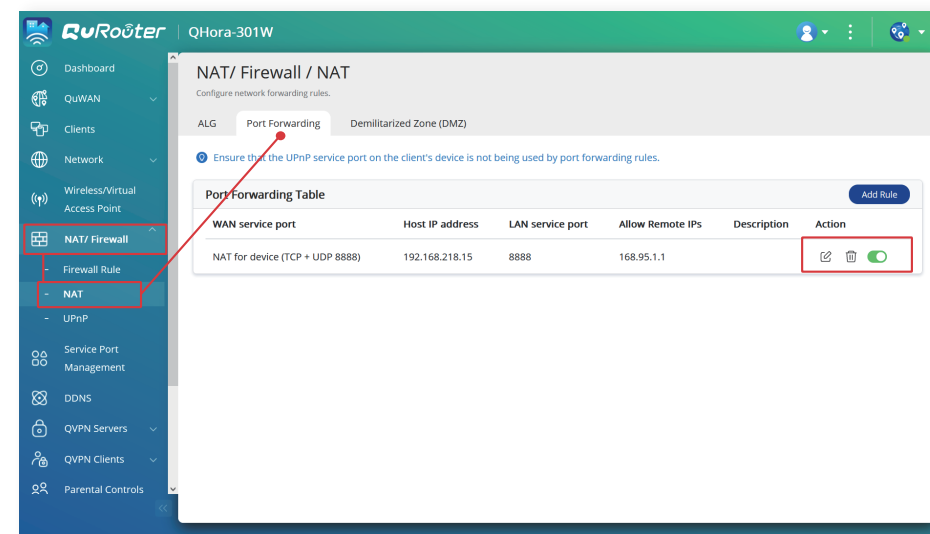
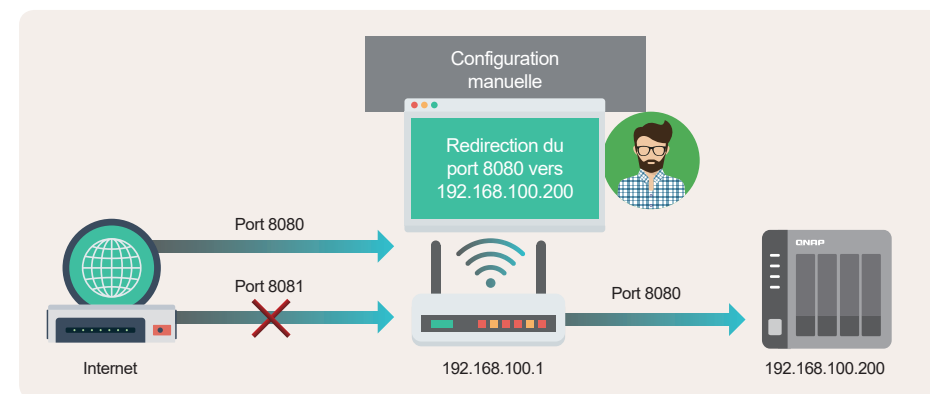
01 | Activer la DMZ (Demilitarized Zone)

Après avoir activé cette fonction, tous les ports de service de l'appareil que vous avez sélectionné seront directement ouverts sur Internet, c'est-à-dire entièrement exposés à Internet. Pour réduire les risques de sécurité, désactivez cette fonction.



02 | Activer la redirection de port

Cette fonction vous permet d'ouvrir un port de service spécifique sur un appareil vers Internet, permettant à quiconque d'accéder à des services connexes via Internet. Cependant, les pirates peuvent également lancer des attaques contre des services ouverts à partir d'Internet. Par conséquent, il est recommandé de désactiver d'abord toutes les règles de redirection de port, puis de configurer les paramètres de sécurité du NAS, puis de sauvegarder les données importantes avant d'utiliser cette fonction pour ouvrir certains services essentiels sur Internet.

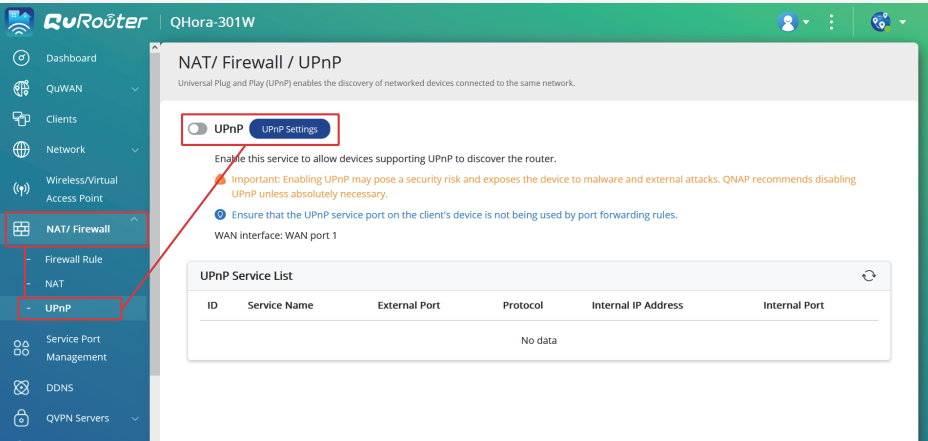
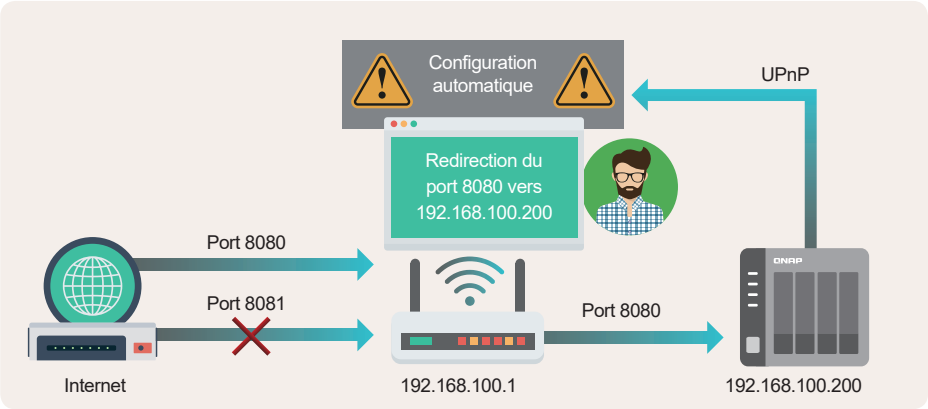




Vérifier les paramètres du NAS

03 | Activer UPnP (Universal Plug and Play)

Cette fonction est équivalente à la redirection de port automatique. Après avoir activé cette fonction, votre appareil peut configurer automatiquement la redirection de port en utilisant le protocole approprié. Cette fonction présente de sérieux risques de sécurité car elle peut exposer vos services à Internet à votre insu, ou être exploitée par des pirates pour ouvrir des portes dérobées, vous devez donc désactiver cette fonction pour améliorer la sécurité.



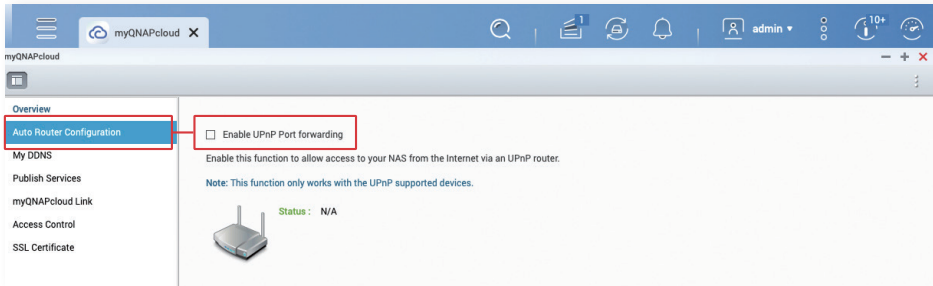
01 | Configuration automatique du routeur, redirection de port UPnP

Étant donné que certains routeurs ne prennent pas en charge la désactivation de la fonction UPnP, veuillez vérifier le paramètre « Configuration automatique du routeur » sur le NAS en même temps pour vous assurer que cette fonction est désactivée.

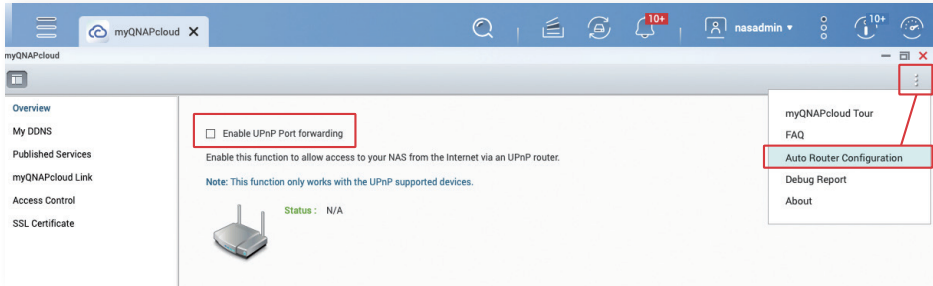
*** Cette fonction est désactivée par défaut à partir de QTS 4.5.0 / QuTS hero h4.5.3.**

Pour désactiver la fonction « Configuration automatique du routeur » :

1. Connectez-vous à l'interface de gestion Web QTS / QuTS hero à l'aide d'un compte administrateur.
2. Ouvrez le menu dans le coin supérieur gauche de l'interface de gestion et cliquez sur « myQNAPcloud »
3. **QTS 5.0.0 / QuTS hero h5.0.0** ou version **antérieure** : Cliquez sur « Configuration automatique du routeur » dans le menu de gauche



QTS 5.0.1 / QuTS hero h5.0.1 ou version **ultérieure** : Cliquez sur l'icône de menu dans le coin supérieur droit et sélectionnez « Configuration automatique du routeur »



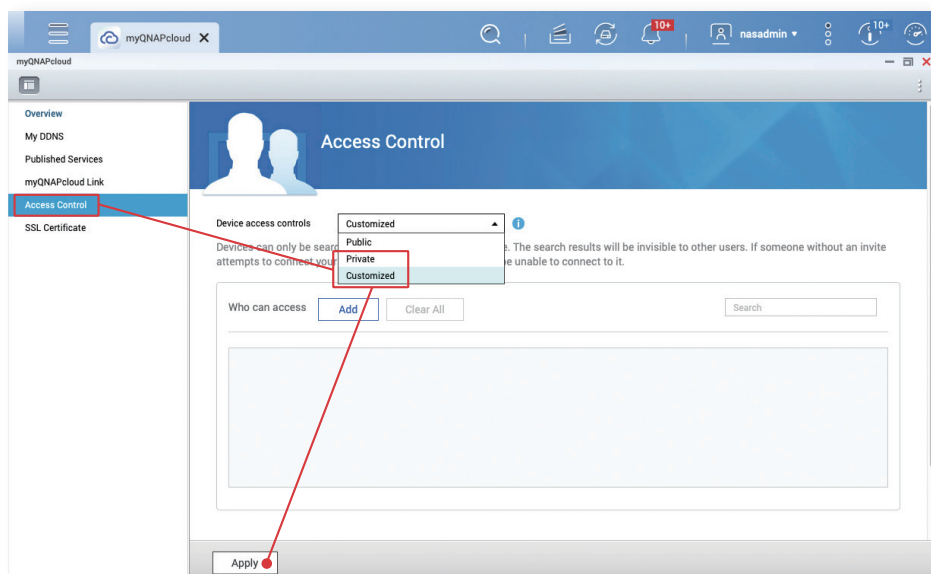
4. Sur la page des paramètres « Configuration automatique du routeur », décochez « Activer la redirection de port UPnP » et cliquez sur « Appliquer ».

02 | Contrôle d'accès à myQNAPcloud Link

myQNAPcloud Link est un service cloud de connexion sécurisée fourni par QNAP. Les utilisateurs peuvent se connecter à leur NAS QNAP via le nom d'appareil myQNAPcloud de leur choix. myQNAPcloud Link fournit des paramètres de contrôle d'accès. Lorsque le contrôle d'accès est défini sur « Public », toute personne connaissant le nom de votre appareil peut utiliser myQNAPcloud Link pour se connecter à votre NAS. Par conséquent, **nous vous recommandons de définir le contrôle d'accès sur « Privé » ou « Personnalisé »**. Dans les deux modes, les utilisateurs doivent se connecter à leur QNAP ID dans la liste d'accès autorisés avant de pouvoir utiliser myQNAPcloud Link pour se connecter en toute sécurité aux services cloud.

* Le paramètre par défaut dans Q TS 4.5.0 / Qu TS hero h4.5.3 (ou version ultérieure) est « Personnalisé »

1. Connectez-vous à l'interface de gestion Web QTS / QuTS hero à l'aide d'un compte administrateur
2. Cliquez sur le menu dans le coin supérieur gauche de l'interface de gestion, cliquez sur « myQNAPcloud »
3. Cliquez sur « Contrôle d'accès » dans le menu de gauche
4. Sur la page des paramètres « Contrôle d'accès », définissez « Contrôles d'accès aux appareils » sur « Privé » ou « Personnalisé », puis cliquez sur « Appliquer ».



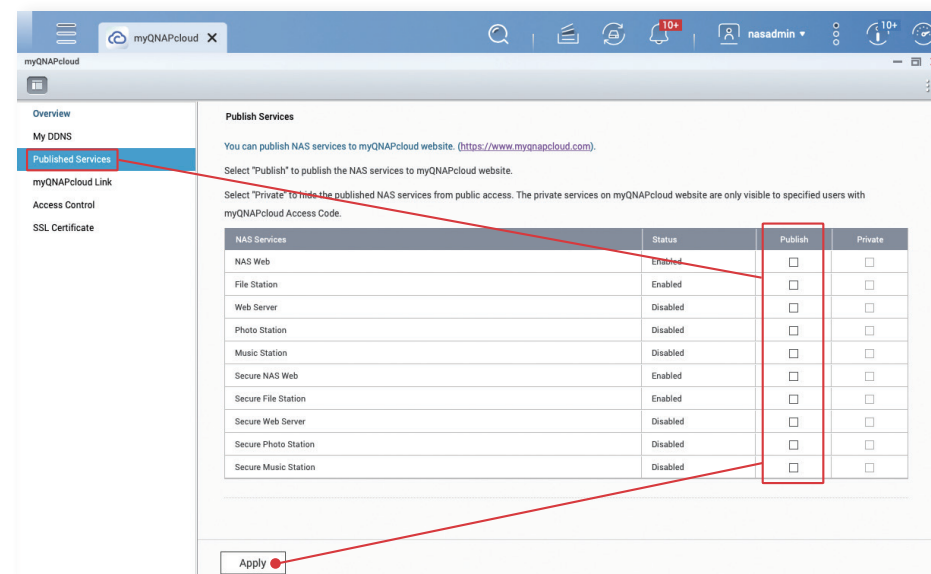
03 | Services publiés

Les services publiés peuvent faciliter l'utilisation des fonctions associées sur le site Web myQNAPcloud par les utilisateurs, mais cela augmente également les risques de sécurité. Si vous n'avez pas besoin d'utiliser cette fonction, il est recommandé de la désactiver pour améliorer la sécurité.

* Cette fonction est désactivée par défaut à partir de QTS 4.5.0 / QuTS hero h4.5.3

Fonction « Services publiés » :

1. Connectez-vous à l'interface de gestion Web QTS / QuTS hero à l'aide d'un compte administrateur
2. Cliquez sur le menu dans le coin supérieur gauche de l'interface de gestion, cliquez sur « myQNAPcloud »
3. Cliquez sur « Services publiés » dans le menu de gauche
4. Dans le champ « Publier », décochez tout et cliquez sur « Appliquer ».



Liste de contrôle des paramètres réseau

Considération matérielle

- ☐ Le NAS est connecté derrière un routeur
- ☐ Le NAS obtient l'adresse IP intranet

Routeur







- ☐ Désactiver la fonction « DMZ » du routeur
- ☐ Désactiver la règle « Redirection de port » du routeur
- ☐ Désactiver la fonction « UPnP » du routeur

NAS

- ☐ Désactiver la fonction « Configuration automatique de la redirection de port UPnP du routeur » du NAS
- ☐ Définir « Contrôle d'accès myQNAPcloud Link » du NAS sur « Privé » ou « Personnalisé »
- ☐ Désactiver la fonction « Services publiés »

Après avoir vérifié et appliqué les paramètres ci-dessus, votre NAS QNAP ne sera pas exposé à Internet et les risques d'être attaqué par des pirates sont considérablement réduits. Veuillez continuer à lire et vérifier le reste des paramètres pour renforcer le NAS QNAP.

Si vous avez besoin d'accéder au NAS via Internet, vous pouvez envisager ces trois alternatives sécurisées :

		
myQNAPcloud Link	QVPN Service	QuWan SD-WAN
		
En savoir plus	En savoir plus	En savoir plus

02

Guide des paramètres de sécurité du NAS



Paramètres de sécurité du NAS



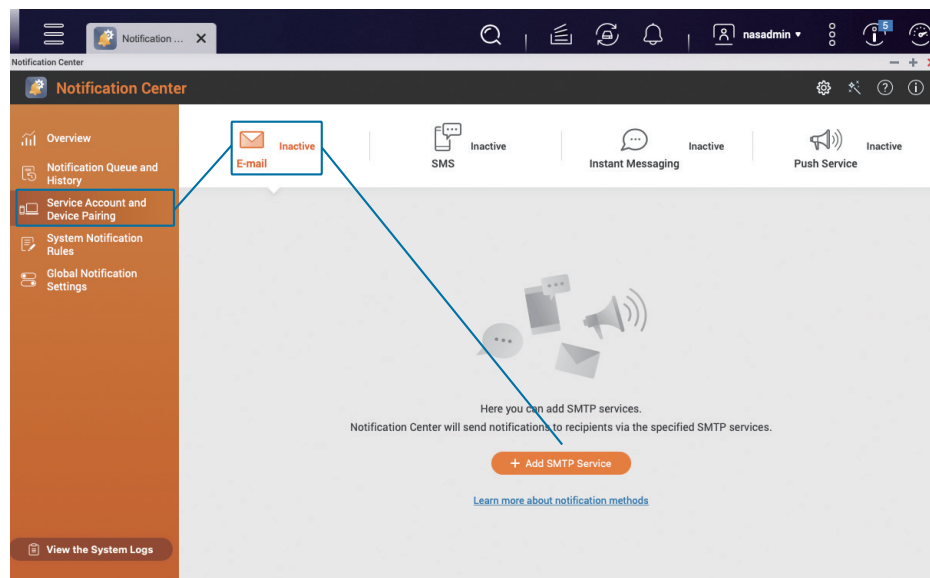
Configurer les notifications système

Le centre de notification intégré peut envoyer des notifications en fonction de vos paramètres, permettant aux utilisateurs de suivre l'état du NAS et de réagir aux anomalies dès qu'elles sont détectées.

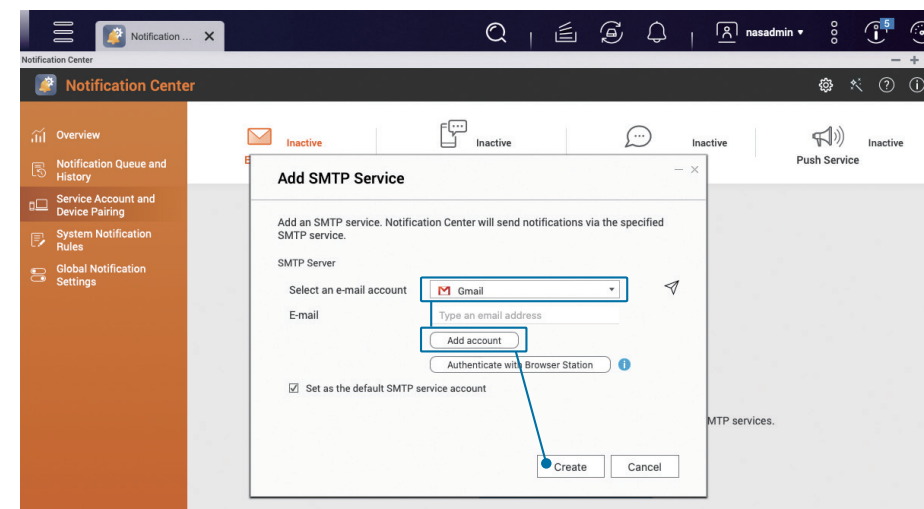
Le didacticiel suivant vous apprendra comment créer deux règles de base pour « Email » pour envoyer des « Notifications d'alerte » et « Mise à jour du firmware », et pour ajouter d'autres règles si nécessaire.

01 | Ajouter une méthode de notification par « E-mail »

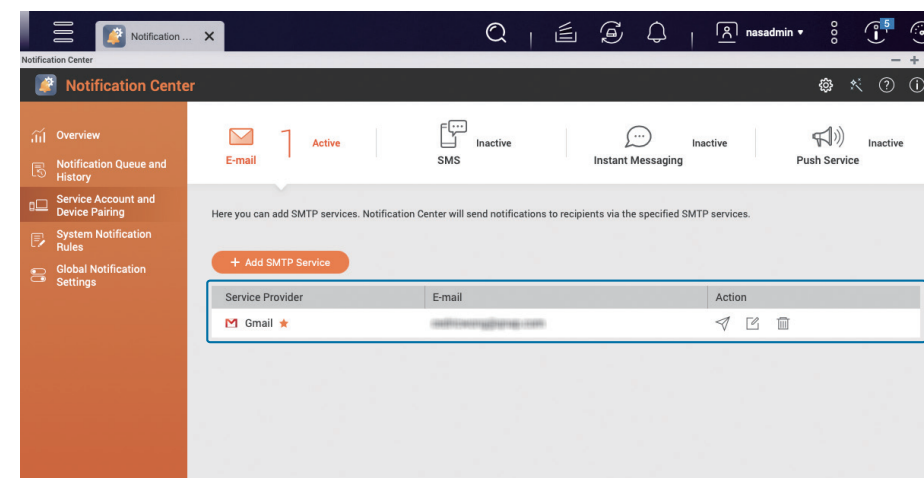
Ouvrez « Centre de notification », cliquez sur « Compte de service et couplage des appareils » dans le menu de gauche, sélectionnez « E-mail », puis cliquez sur « Ajouter un service SMTP »



Sélectionnez un compte de messagerie (ce qui suit utilise Gmail comme exemple), cliquez sur « Ajouter un compte », suivez les instructions pour terminer le processus de vérification de Gmail, puis cliquez sur « Créer » une fois la vérification terminée.

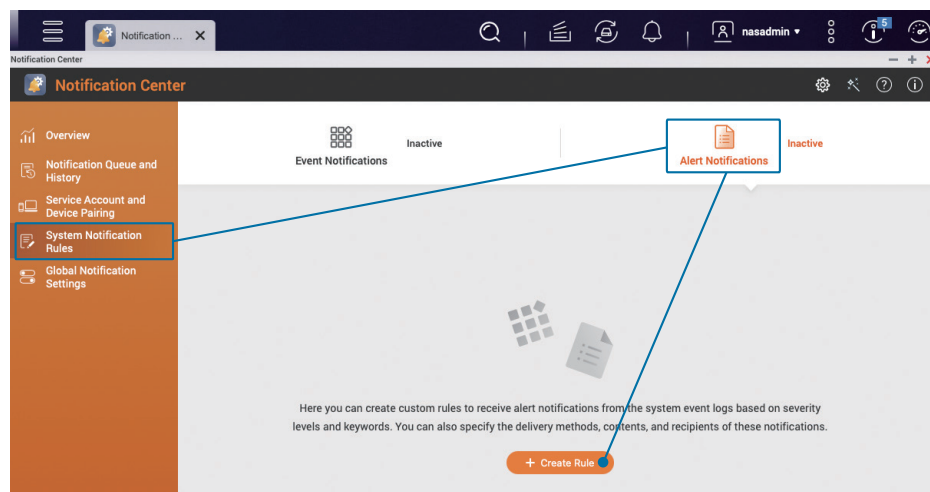


Une fois créé, vous verrez le compte de messagerie que vous avez ajouté dans la liste.

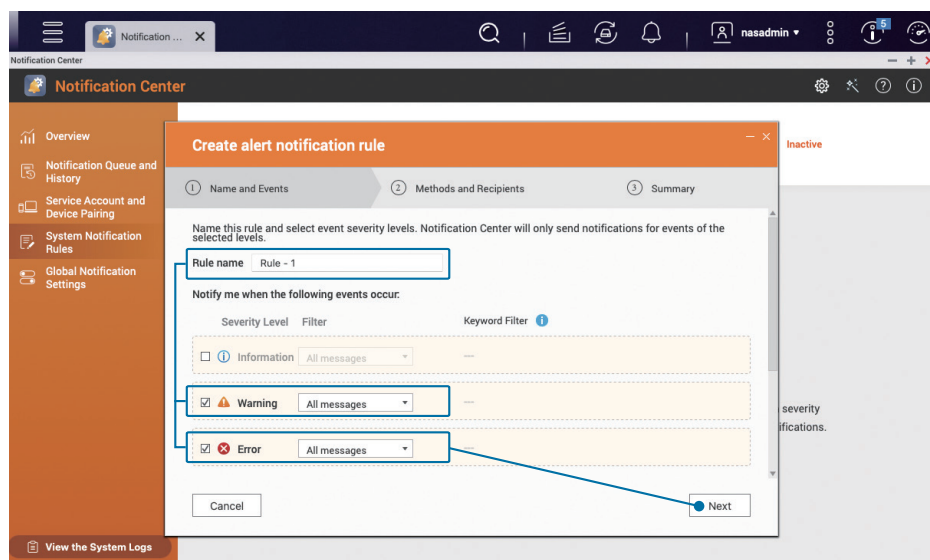


02 | Configurer les « notifications d'alerte »

Dans le menu de gauche du « Centre de notification », cliquez sur « Règles de notification système », sélectionnez « Notifications d'alerte », puis cliquez sur « Créer une règle ».

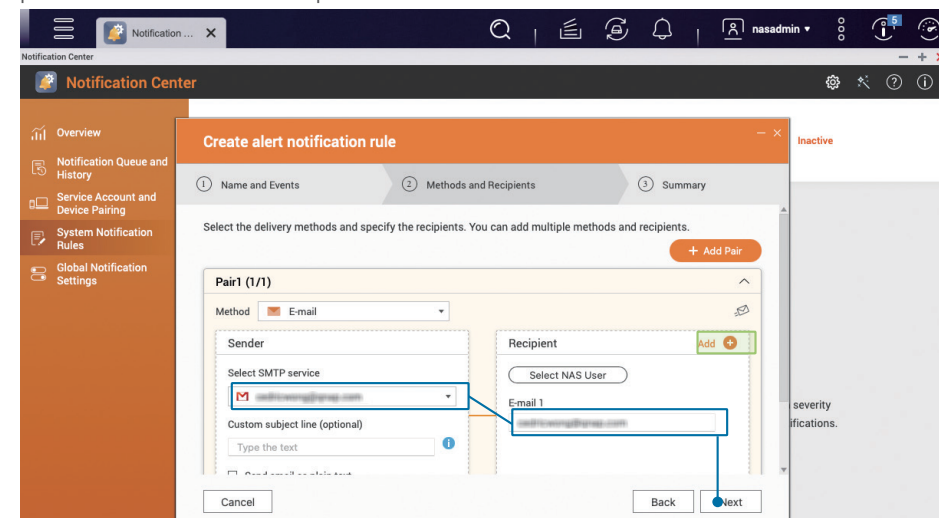


Modifiez le « Nom de la règle » selon vos besoins, vérifiez les deux niveaux de gravité « Avertissement » et « Erreur », puis cliquez sur « Suivant ».

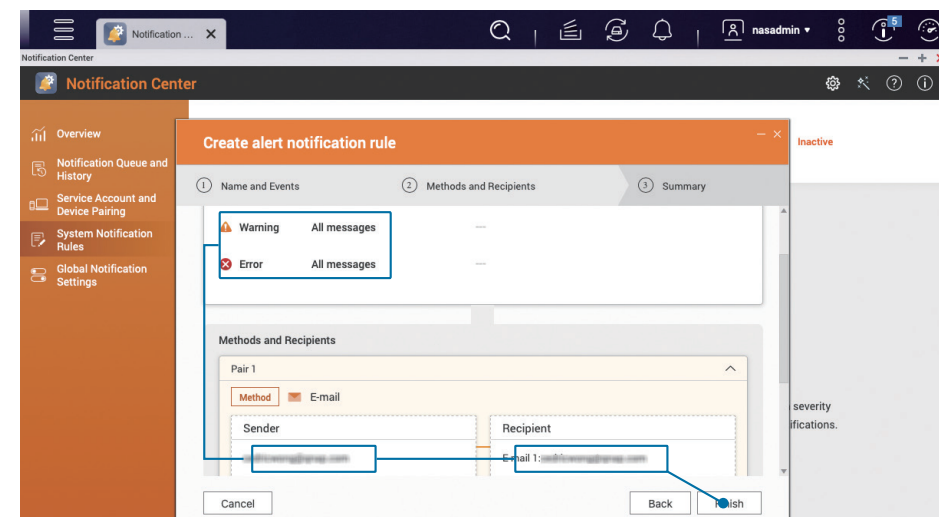


Définissez la méthode de livraison et définissez le destinataire, sélectionnez le compte de messagerie que vous venez d'ajouter comme « Expéditeur » dans le couplage, puis entrez l'« Adresse e-mail » du « Destinataire », puis cliquez sur « Suivant ».

Si nécessaire, vous pouvez saisir plusieurs destinataires en cliquant sur « Ajouter » à côté de « Destinataire ». Vous pouvez également « Ajouter un couplage » pour envoyer des notifications de plusieurs manières en même temps.

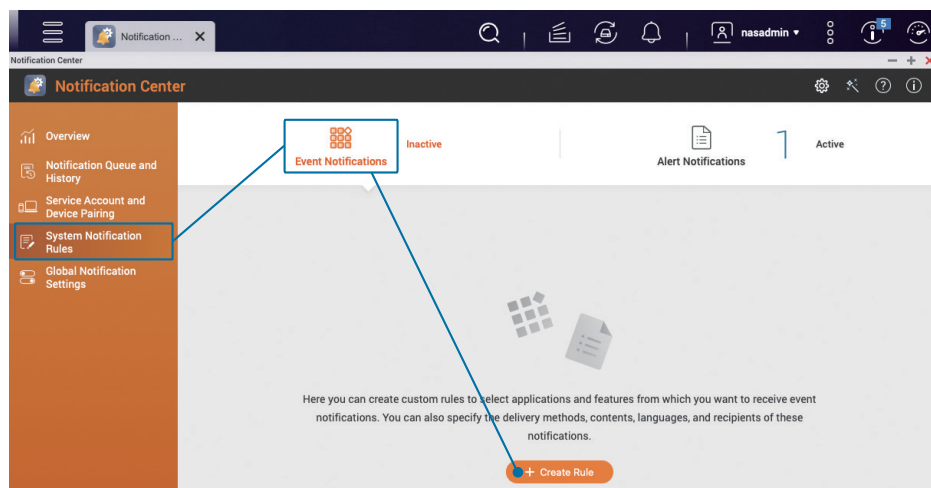


Après avoir confirmé que les paramètres sont corrects, cliquez sur « Terminer » et les paramètres « Notifications d'alerte » seront terminés.

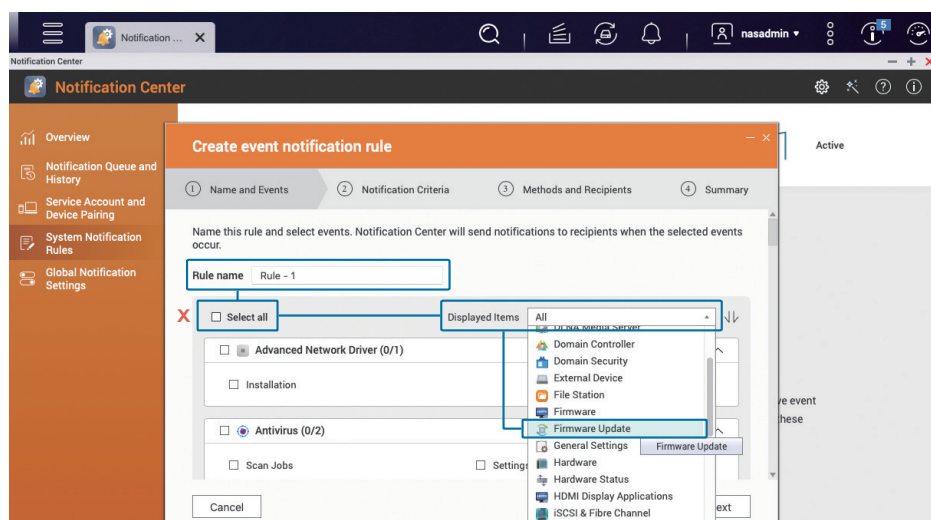


03 Configurer les notifications « Mise à jour du firmware »

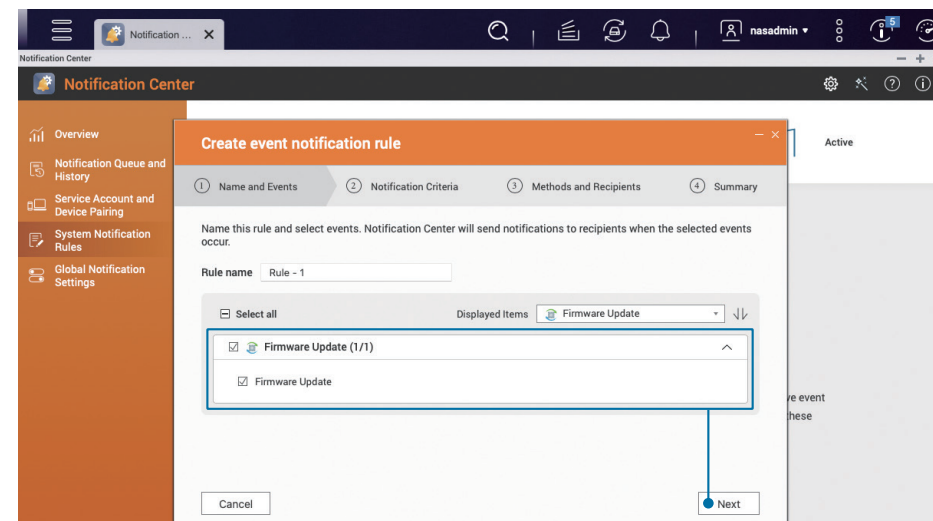
Cliquez sur « Règles de notification système » dans le menu de gauche du « Centre de notification », sélectionnez « Notifications d'événements », puis cliquez sur « Créer une règle ».



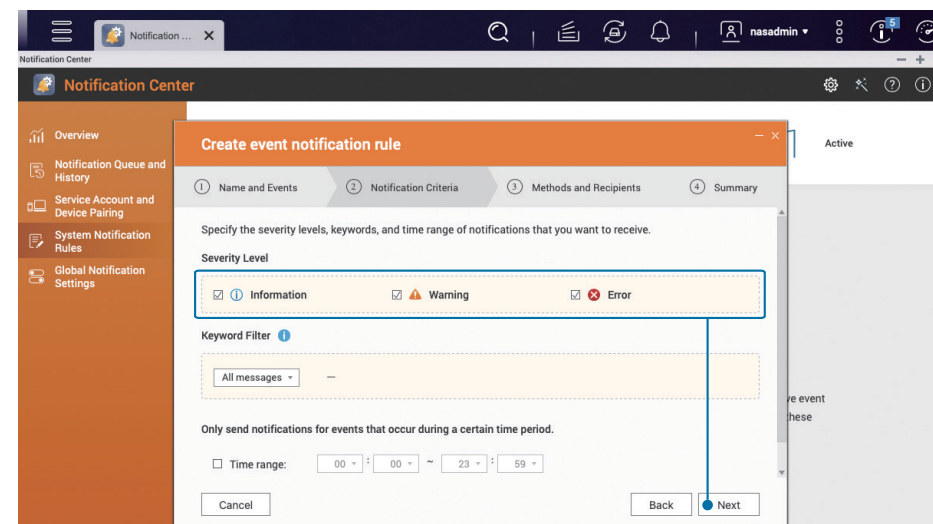
Modifiez le « Nom de la règle » en fonction de vos besoins, décochez « Sélectionner tout », puis sélectionnez « Mise à jour du firmware » dans les « Éléments affichés » à gauche, puis sélectionnez l'option « Mise à jour du firmware » ci-dessous.



Cochez l'option « Mise à jour du firmware » et cliquez sur « Suivant ».



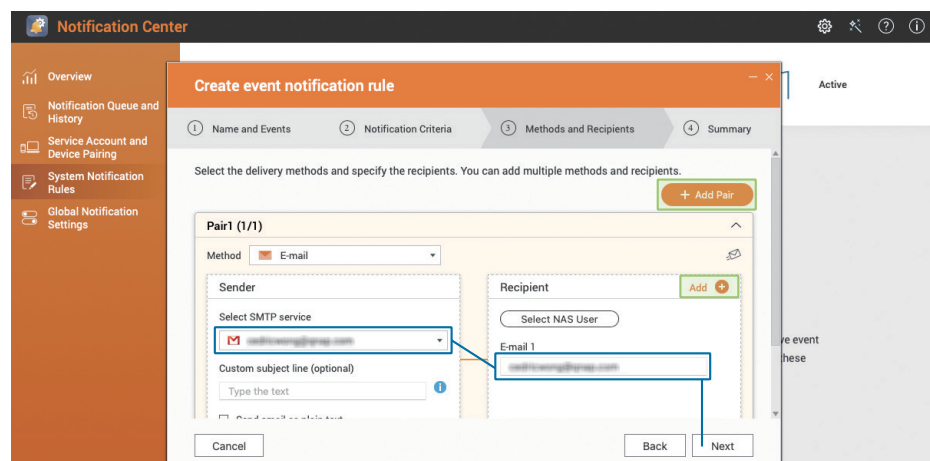
Vérifiez tous les niveaux de gravité, y compris « Information », « Avertissement » et « Erreur », cliquez sur « Suivant ».



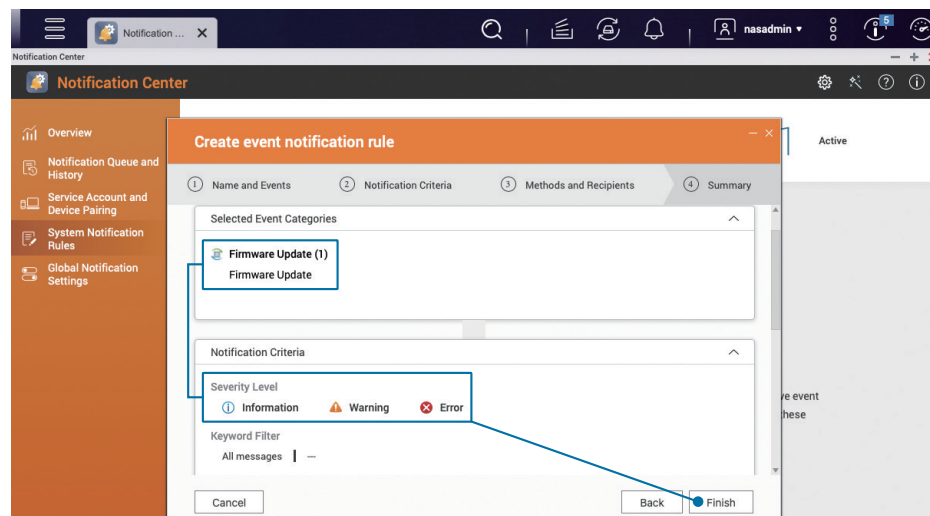
Activer la mise à jour automatique du firmware (QTS / QuTS hero)

Définissez la méthode de livraison et définissez le destinataire. Étant donné que seule la notification « E-mail » est actuellement définie, sélectionnez le compte de messagerie que vous venez d'ajouter comme « Expéditeur » dans le couplage, puis entrez l'« Adresse e-mail » du « Destinataire » et cliquez sur « Suivant ».

Si nécessaire, vous pouvez saisir plusieurs destinataires en cliquant sur « Ajouter + » à côté de « Destinataire ». Vous pouvez également « Ajouter un couplage » pour envoyer des notifications de plusieurs manières en même temps.

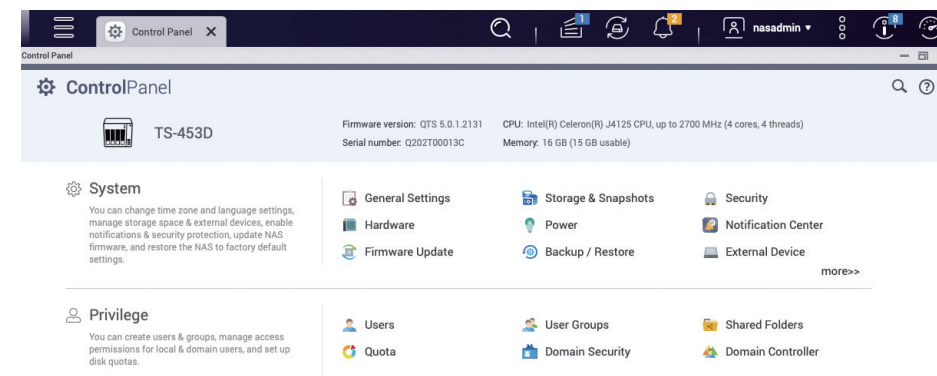


Après avoir confirmé que les paramètres sont corrects, cliquez sur « Terminer » pour terminer le réglage de « Mise à jour du firmware ».



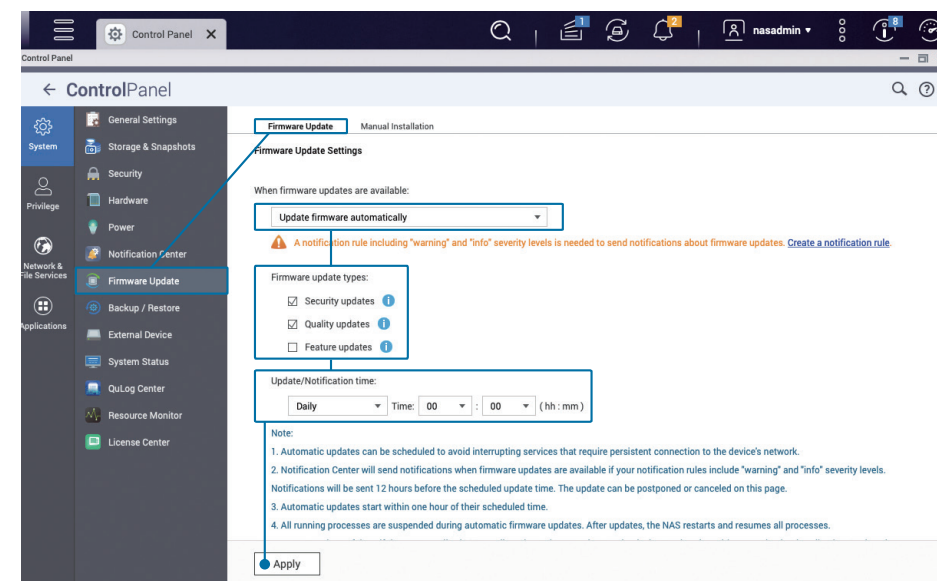
La fonction de mise à jour automatique facilite l'installation des mises à jour pour les nouvelles fonctionnalités, les corrections de bogues et les vulnérabilités.

Ouvrez « Panneau de configuration » et cliquez sur « Mise à jour du firmware ».



Dans « Paramètres de mise à jour du firmware », sélectionnez « Mettre à jour le firmware automatiquement » et cochez « Mises à jour de sécurité » et « Mises à jour de qualité » ; pour « Heure de mise à jour/notification », il est recommandé de définir une heure creuse telle que « 00 h 00 », puis de cliquer sur Appliquer.

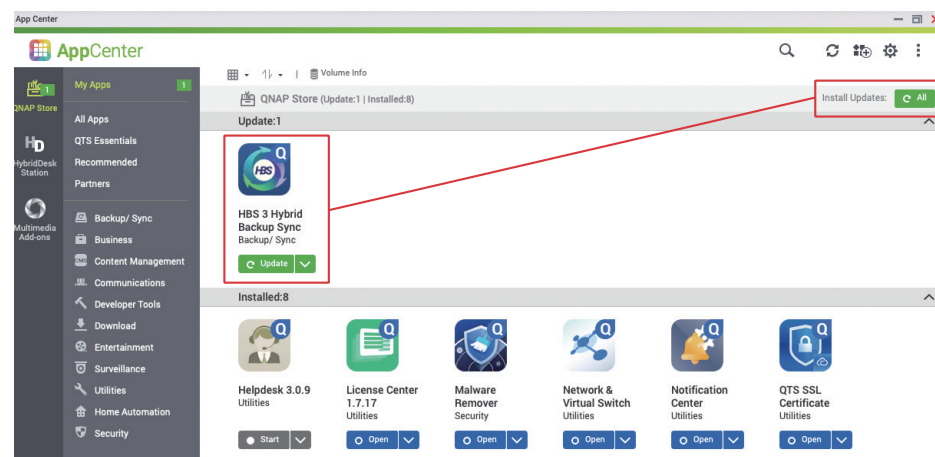
*** Pour QTS 5.0.0 / QuTS hero h5.0.0 (ou version antérieure), cochez « Version recommandée » sur la page « Mise à jour automatique »**




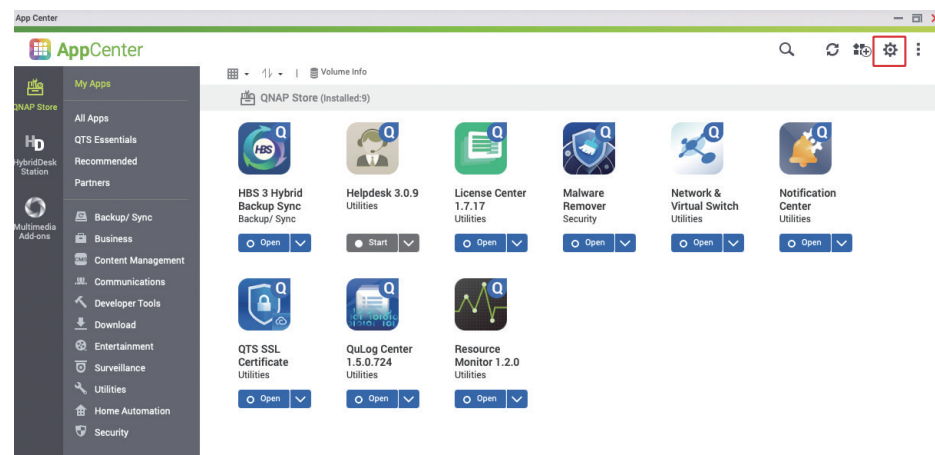
Paramètres de mise à jour des applications

L'App Center fournit plusieurs applications pour ajouter plus de fonctions à votre NAS QNAP, mais les applications doivent également être mises à jour pour améliorer les fonctions de l'application, résoudre les problèmes et les vulnérabilités et améliorer l'expérience utilisateur.

Ouvrez « App Center » pour voir s'il y a des applications qui doivent être mises à jour. Si tel est le cas, cliquez sur le bouton « Tous  All » en haut à droite pour mettre à jour toutes les applications.

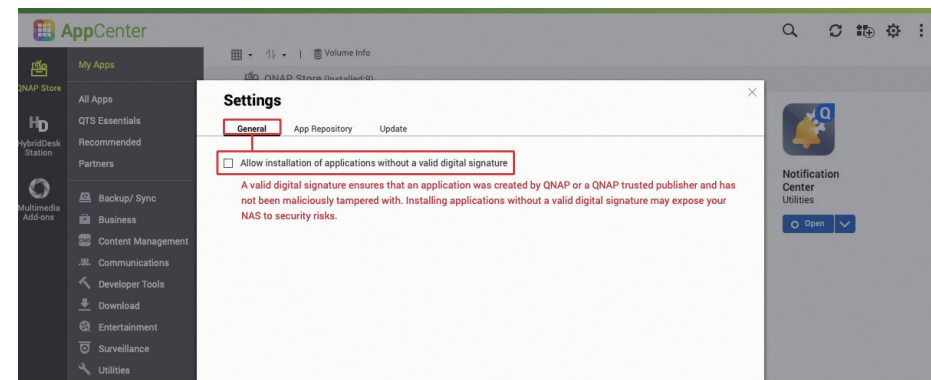


Une fois la mise à jour terminée, cliquez sur l'icône « Paramètres  » dans le coin supérieur droit pour accéder à la page des paramètres de l'App Center.



QNAP ou les développeurs approuvés par QNAP ajouteront une signature numérique à l'application pour s'assurer qu'elle est authentique. Il est recommandé de décocher « Autoriser l'installation d'applications sans signature numérique valide » pour renforcer la sécurité.

***L'option est décochée par défaut, ce qui rend impossible l'installation d'applications sans signature numérique valide**

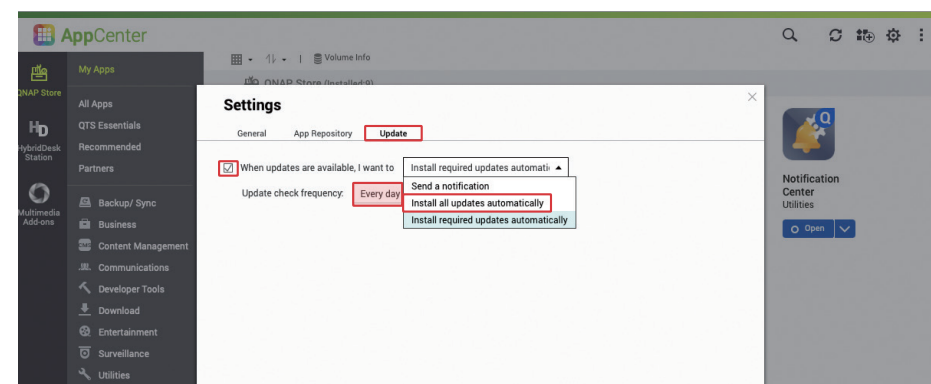


Cliquez sur l'onglet Mise à jour, s'il n'y a pas de besoin particulier, il est recommandé de sélectionner « Installer toutes les mises à jour automatiquement », de définir la fréquence sur « Tous les jours » et de cliquer sur Appliquer pour terminer le réglage.

⇒ Les « Mises à jour requises » sont principalement utilisées pour répondre aux dépendances des applications et des firmwares, et incluront également les « mises à jour des vulnérabilités majeures ».

⇒ « Toutes les mises à jour » inclut toutes les améliorations de fonctionnalités, les corrections de bogues et tous les correctifs de vulnérabilité. La mise à jour sera plus fréquente.


*** La valeur par défaut est « Installer toutes les mises à jour automatiquement »**

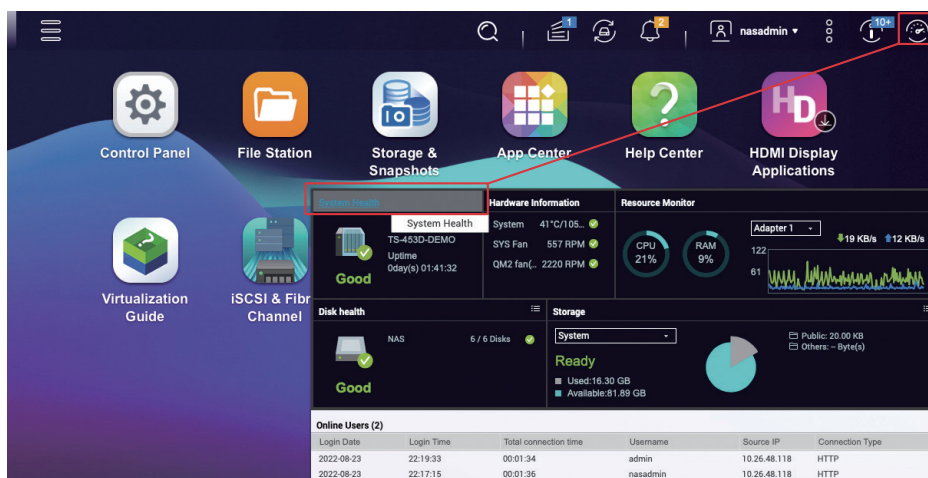


Désactiver ou supprimer les fonctions inutiles

Le NAS QNAP fournit une variété de fonctions et d'applications, mais plus il y a de fonctions activées, plus il y a de vecteurs d'attaque potentiels. Vous devez régulièrement vérifier et désactiver (ou supprimer) les fonctions inutiles pour améliorer la sécurité et rendre le système plus fluide.

★ Pour améliorer la sécurité du produit, à partir de **QTS 5.0.0 / QuTS hero h5.0.0**, les fonctions non essentielles sont désactivées par défaut lors de l'initialisation du système. En outre, l'**App Center** n'installera aucune application non essentielle par défaut. Si le système a été initialisé avant la mise à jour vers **QTS 5.0.0 / QuTS hero h5.0.0**, veuillez vérifier quelles applications ont été installées.

Cliquez sur le bouton «  » dans le coin supérieur droit pour ouvrir le « Tableau de bord » du système, cliquez sur « Santé du système » pour ouvrir la fenêtre « État du système ».

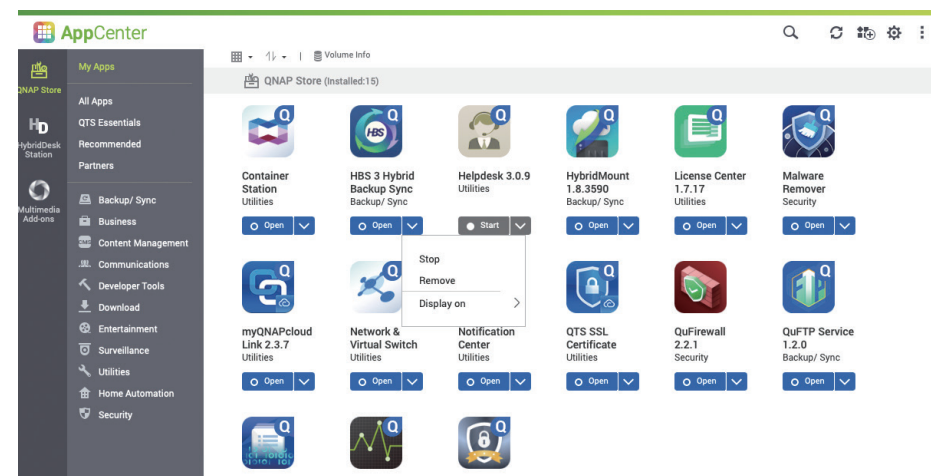


Cliquez sur « Service système » pour afficher les fonctions système activées. Vous pouvez accéder au Panneau de configuration pour désactiver les fonctions système inutiles.

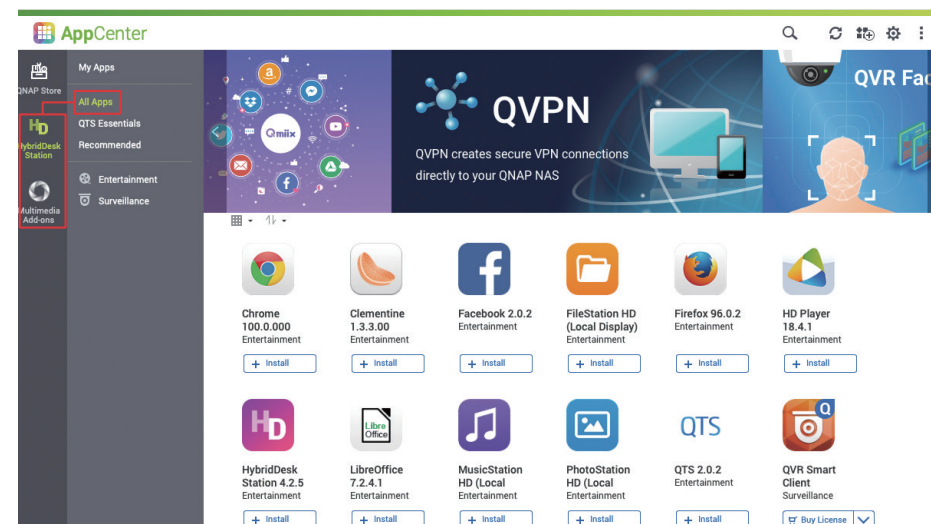
System Status

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

En plus des fonctions intégrées au système, vous devez également vérifier ce qui est installé dans l'App Center.



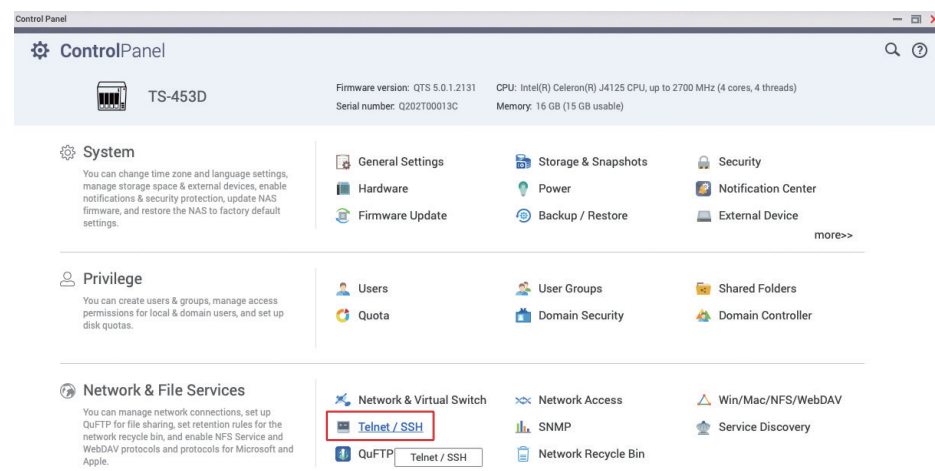
À l'extrême gauche, cliquez sur « HybridDesk Station » et « Add-ons multimédia » pour voir l'état des applications correspondantes,



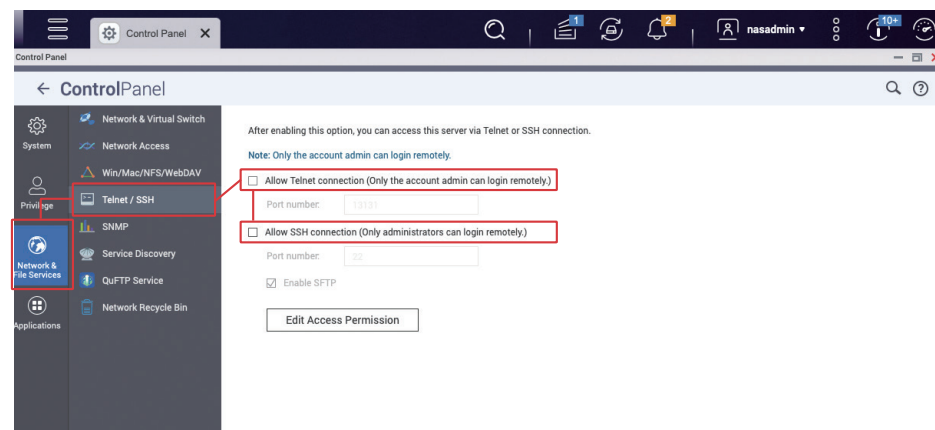
Désactiver Telnet / SSH

Sauf si vous les utilisez, il est fortement recommandé de **désactiver Telnet et SSH**. Ces deux fonctions sont généralement utilisées par le service client de QNAP ou le personnel informatique professionnel pour entretenir le système. Les utilisateurs généraux ne devraient pas en avoir besoin, il est donc recommandé de les désactiver.

Ouvrez « Panneau de configuration » et cliquez sur « Telnet / SSH »



Décochez « Autoriser la connexion Telnet » et « Autoriser la connexion SSH », puis cliquez sur « Appliquer ».

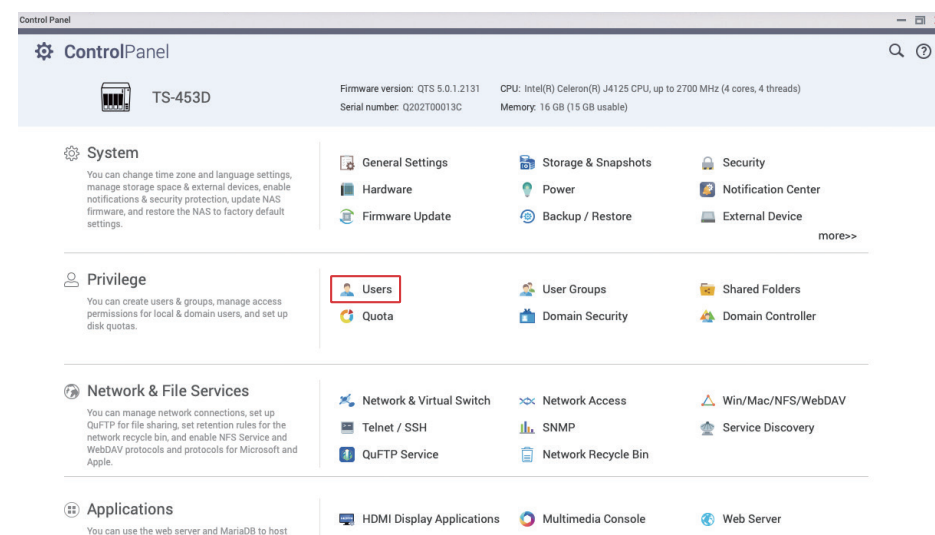


Renforcer la sécurité du compte système

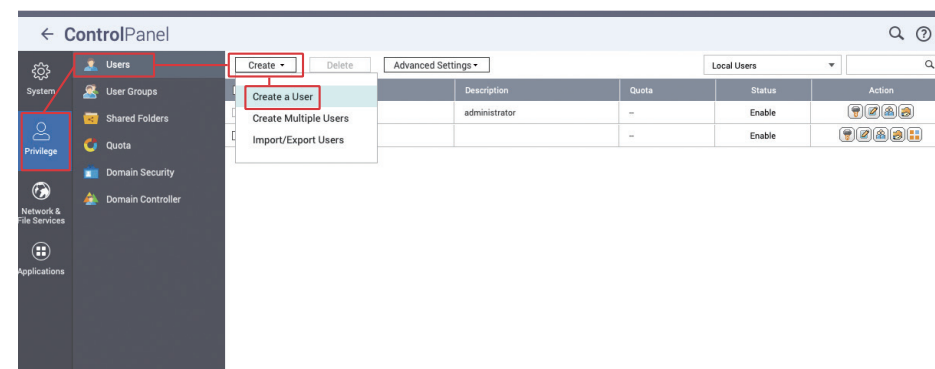
Désactiver le compte administrateur par défaut « admin »

Les pirates qui utilisent le craquage de mot de passe par force brute ciblent généralement le compte administrateur par défaut « admin ». Si le système a été initialisé avec QTS 4.5.4 / QuTS hero h4.5.4 (ou une version antérieure), le compte administrateur par défaut « admin » sera actif. Suivez ces étapes pour créer un nouveau compte administrateur et désactiver le compte « admin ».

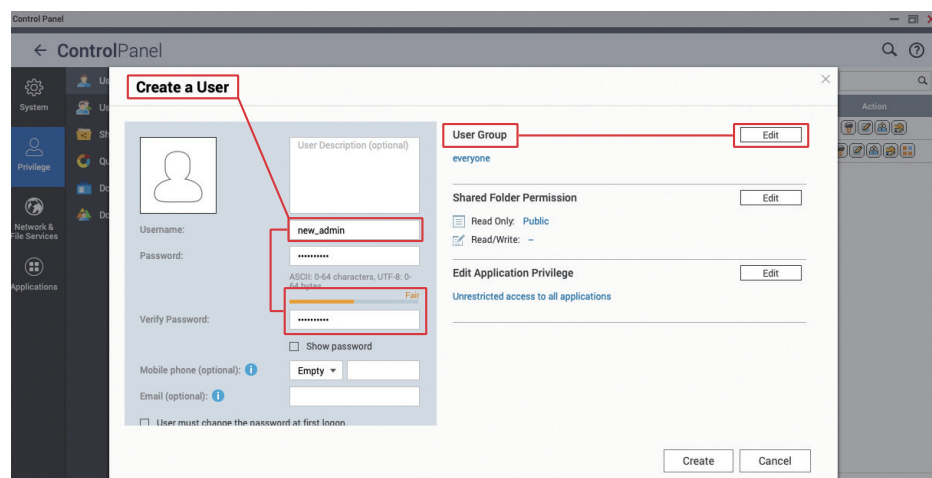
Ouvrez « Panneau de configuration » et cliquez sur « Utilisateurs »



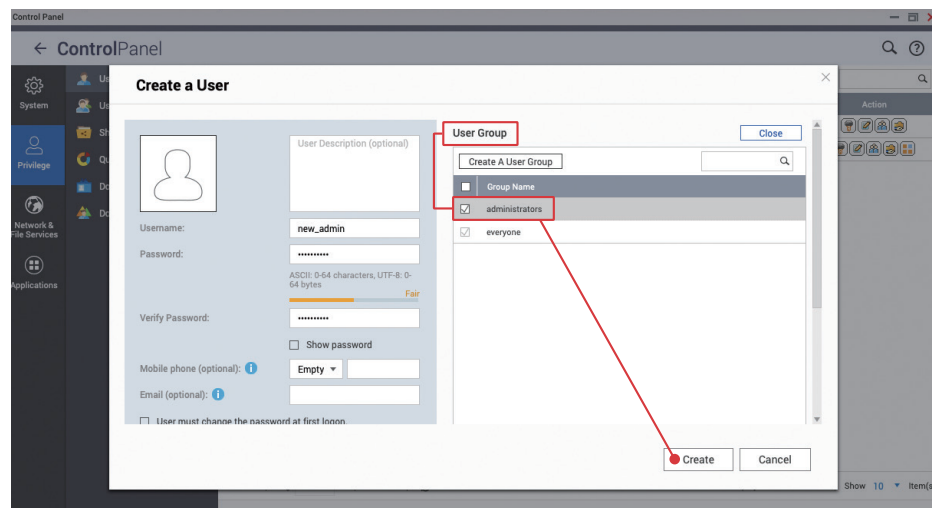
Cliquez sur « Créer » > « Créer un utilisateur »



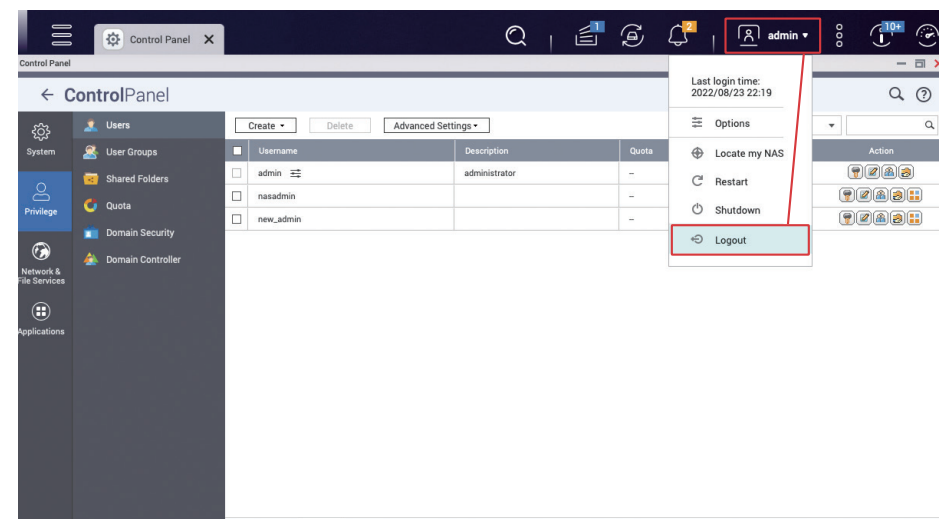
Entrez le nom d'utilisateur du compte administrateur, tel que « new_admin », et définissez un mot de passe fort.



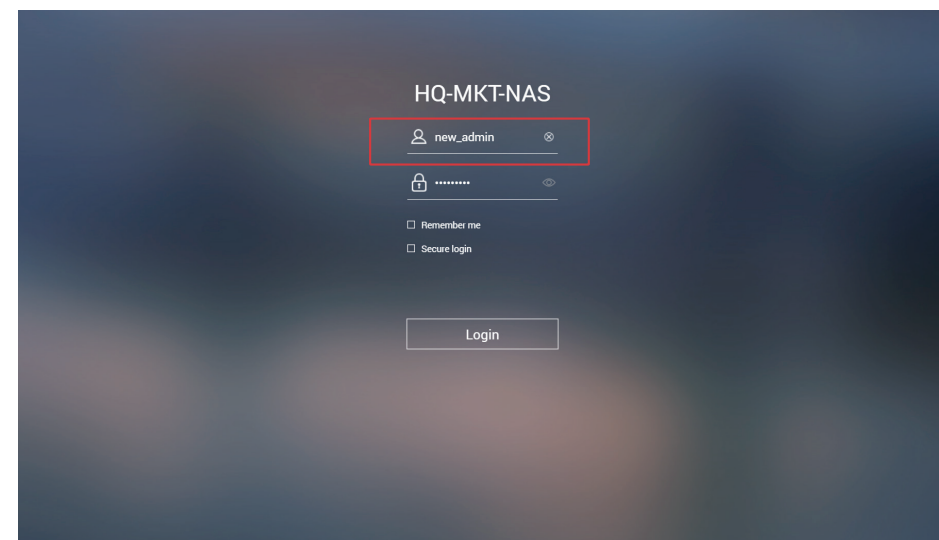
Dans la section « Groupe d'utilisateurs », cliquez sur « Modifier », cochez le groupe « administrateurs », puis cliquez sur « Créer » pour ajouter un nouvel utilisateur.



Cliquez sur « admin » en haut, ouvrez le menu et cliquez sur « Déconnexion » pour vous déconnecter de l'interface de gestion Web de QTS.

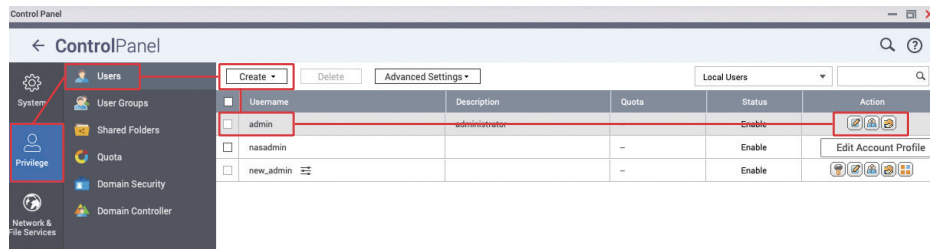


Utilisez le « compte administrateur » que vous venez de créer pour vous connecter à l'interface de gestion Web de QTS.

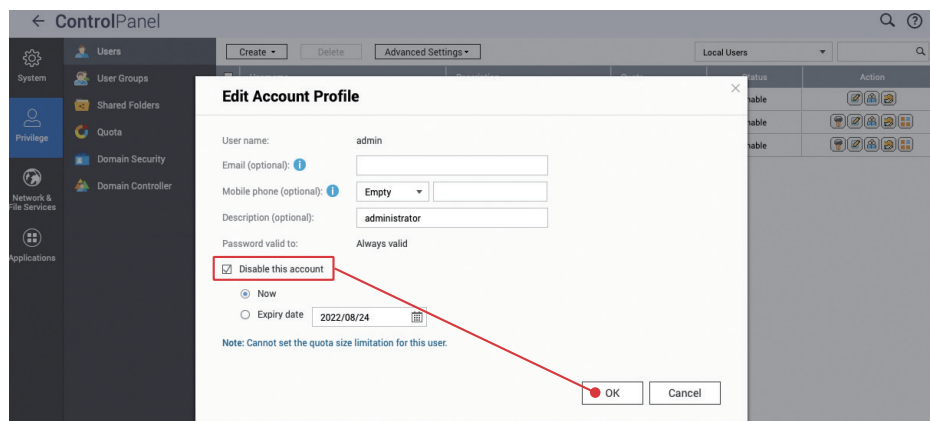


Définir la stratégie de sécurité

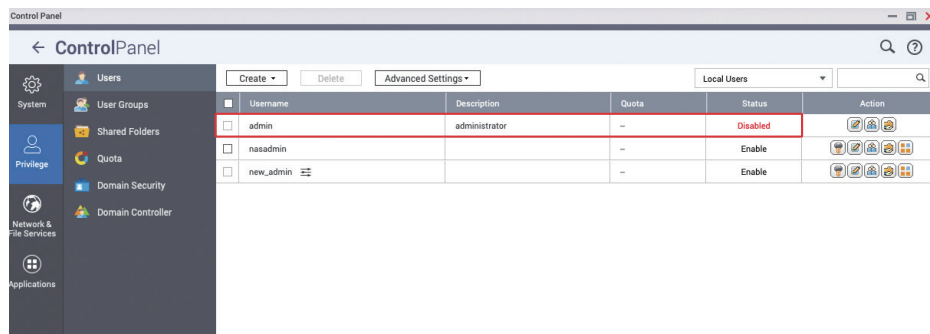
Ouvrez à nouveau le « Panneau de configuration », cliquez sur « Utilisateurs », dans la ligne « admin », cliquez sur « Modifier le profil du compte »



Cochez « Désactiver ce compte » et cliquez sur « OK » pour terminer

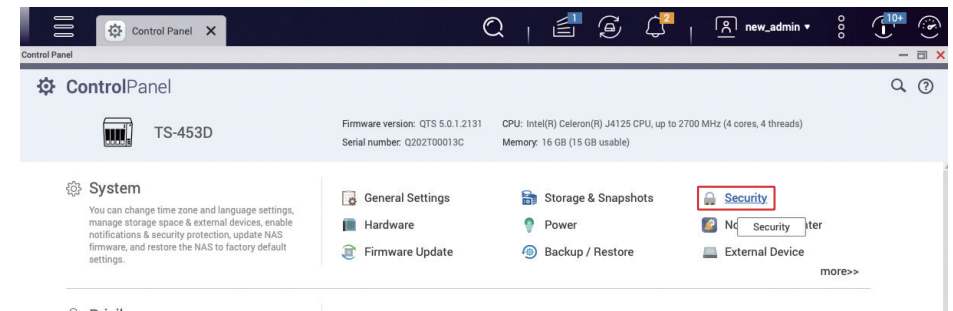


Une fois terminé, vous pouvez voir que le statut « admin » est « Désactivé »

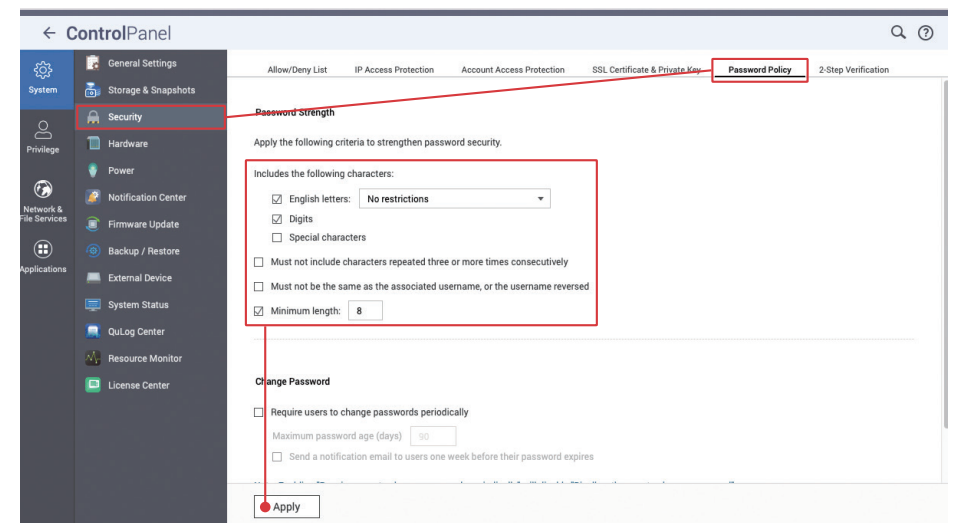


En plus de désactiver le compte administrateur par défaut « admin », vous devez également vous assurer que tous les comptes ont des mots de passe forts. Combiné à « Protection d'accès », cela peut vous aider à bloquer les tentatives de connexion malveillantes. Pour plus de sécurité, vous pouvez appliquer la « vérification en deux étapes (2SV) » pour tous les comptes afin d'empêcher le piratage des mots de passe et les connexions malveillantes.

Ouvrez « Panneau de configuration » et cliquez sur « Paramètres de sécurité »



Cliquez sur « Stratégie de mot de passe » pour accéder à la page de configuration. Si le système a été initialisé dans QTS 5.0.0 / QuTS hero h5.0.0 (ou version ultérieure), les conditions de base de la force du mot de passe sont activées par défaut. Vous pouvez définir les conditions de mot de passe fort en fonction de vos besoins. Le mot de passe peut être défini pour contenir des « lettres anglaises majuscules et minuscules » et des « chiffres », et la longueur **recommandée du mot de passe doit être d'au moins « 10 caractères »**. Cliquez sur « Appliquer » lorsque vous avez terminé.



Activer la protection d'accès (IP / compte)

« Protection d'accès IP » et « Protection d'accès au compte » peuvent aider à empêcher que les mots de passe ne soient piratés par la force brute. Lorsqu'une adresse IP ou un compte spécifique ne se connecte pas trop souvent, cela déclenche le blocage de l'adresse IP ou la désactivation du compte, empêchant les attaquants d'essayer à plusieurs reprises les mots de passe.

Cliquez sur « Protection d'accès IP » pour accéder à la page de configuration, vérifiez tous les services, définissez « Intervalle de temps », « Tentatives de connexion échouées » et « Longueur de bloc IP » en fonction de vos besoins, puis cliquez sur « Appliquer » pour terminer les paramètres.

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 [QutFirewall](#).

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

★ Si l'adresse IP d'un utilisateur normal est bloquée par erreur, vous pouvez ajuster la liste de blocage en :

- vous connectant à l'interface de gestion de QTS/QuTS hero depuis un autre ordinateur
- modifiant l'adresse IP et en vous connectant à l'interface de gestion QTS /QuTS hero
- vous connectant à l'interface de gestion QTS /QuTS hero avec un navigateur mobile
- utilisant l'application QManager

Apply

Cliquez sur « Protection d'accès au compte » pour accéder à la page de configuration, activez les services pertinents, définissez l'« Intervalle de temps » et les « Tentatives de connexion échouées » en fonction de vos besoins, puis cliquez sur « Appliquer » pour terminer la configuration.

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

★ Si « Protection d'accès au compte » est activé pour le compte administrateur, il est possible que tous les comptes administrateur soient désactivés en raison d'attaques de craquage de mot de passe. À ce moment-là, le compte « admin » ne peut être réactivé que via la fonction de réinitialisation, et le mot de passe du compte « admin » sera également réinitialisé. N'oubliez pas de changer votre mot de passe après la réinitialisation.

Apply

Activer la vérification en deux étapes (2SV)

Cliquez sur « Vérification en 2 étapes » pour accéder à la page de configuration, vous pouvez imposer l'utilisation de la « vérification en 2 étapes (2SV) » pour les « utilisateurs » ou les « groupes d'utilisateurs ». Il est fortement recommandé d'activer la 2SV pour les comptes du « Groupe Administrateurs ». Pour les autres comptes, évaluez vous-même les risques et appliquez les paramètres appropriés.

Cliquez sur « Utilisateurs locaux » pour ouvrir le menu et sélectionnez « Groupes locaux ».

Control Panel

← ControlPanel

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

2-Step Verification

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

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

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

Local Users

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

Disabled

Cochez « Appliquer 2SV » dans « administrateurs » et cliquez sur « Appliquer » pour terminer le paramétrage.

Control Panel

← ControlPanel

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

2-Step Verification

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

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

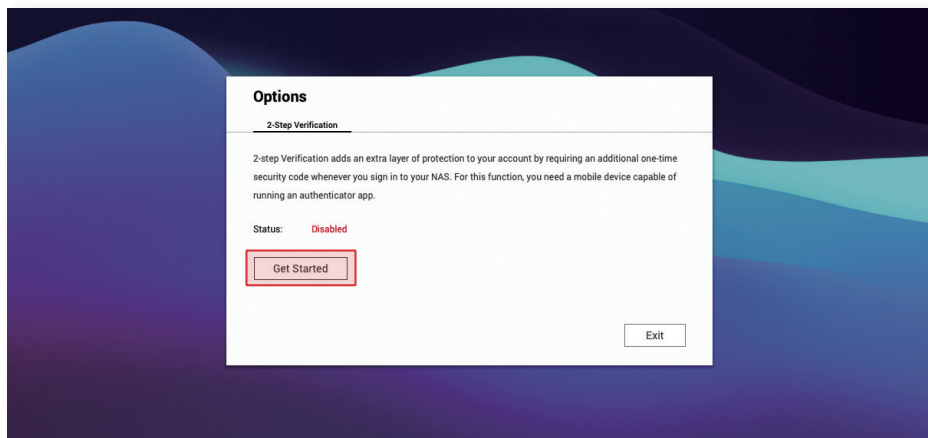
Enforce 2SV	Group Name	Description	Status
<input checked="" type="checkbox"/>	administrators		--
<input type="checkbox"/>	everyone		--

Local Groups

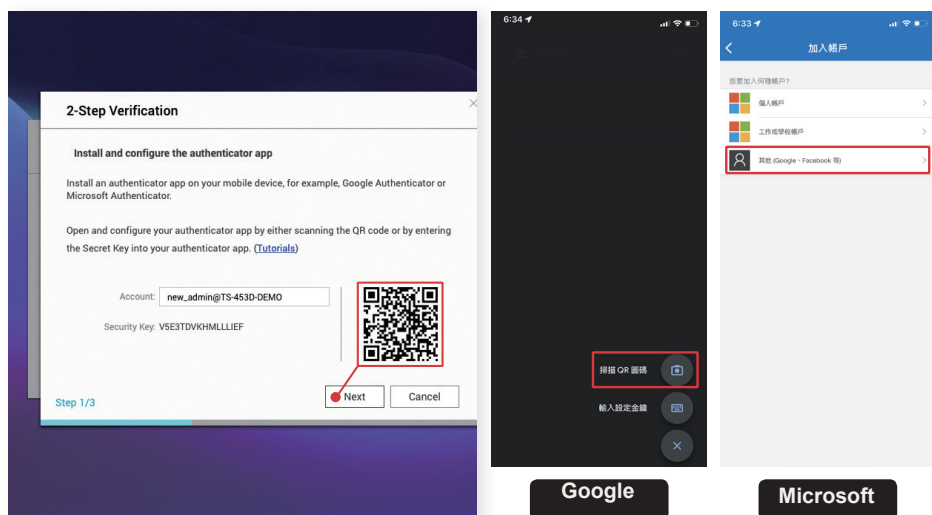
Apply

Après avoir activé « Appliquer 2SV », si le compte « Administrateur » n'a pas été configuré avec « Vérification en 2 étapes (2SV) », la prochaine fois que vous vous connecterez, vous serez dirigé de force vers la « Vérification en 2 étapes (2SV) » page de configuration pour configurer le compte.

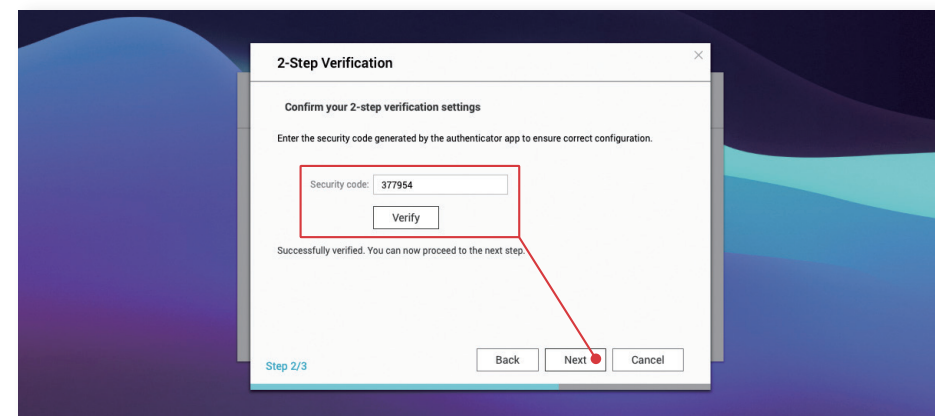
Reconnectez-vous au compte « Administrateur système » et cliquez sur « Premiers pas » pour démarrer le paramétrage.



Installez « Google Authenticator » ou « Microsoft Authenticator » sur votre appareil mobile, scannez le code QR dans le programme pour ajouter l'appareil, puis cliquez sur « Suivant ».

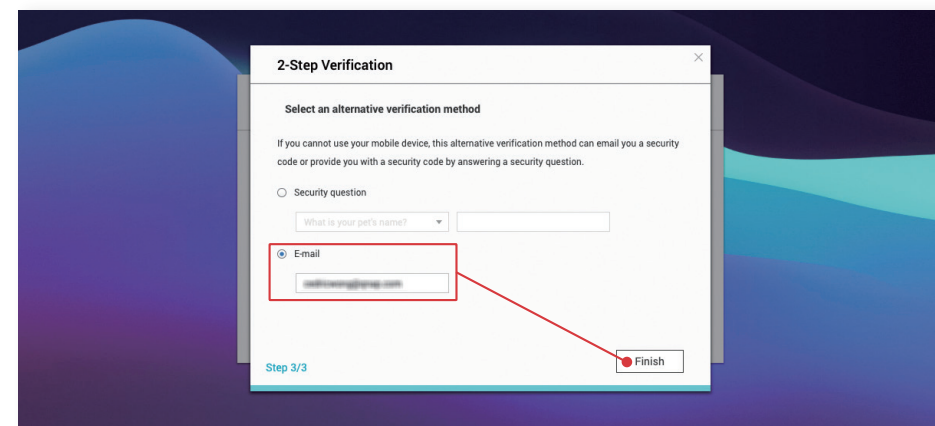


Entrez le « Code de sécurité » à six chiffres généré par « Google Authenticator » ou « Microsoft Authenticator », puis cliquez sur « Vérifier ». Après vérification, cliquez sur Suivant pour continuer.



Pour configurer une méthode de vérification alternative *, vous pouvez sélectionner « Question de sécurité » ** ou « E-mail » ***, la remplir et cliquer sur « Terminer » pour activer la « Vérification en 2 étapes (2SV) ».

- * Si vous ne pouvez pas obtenir le « Code de sécurité » d'une application d'authentification, vous pouvez recevoir un « Code de sécurité » en répondant à la « Question de sécurité » ou en utilisant « E-mail ».
- ** Répondez correctement à la « Question de sécurité » pour passer la vérification en 2 étapes. N'utilisez pas de questions et de réponses simples ou faciles à deviner.
- *** Vous devez ajouter la méthode de notification « email » dans le « Centre de notification » pour utiliser cette fonction.



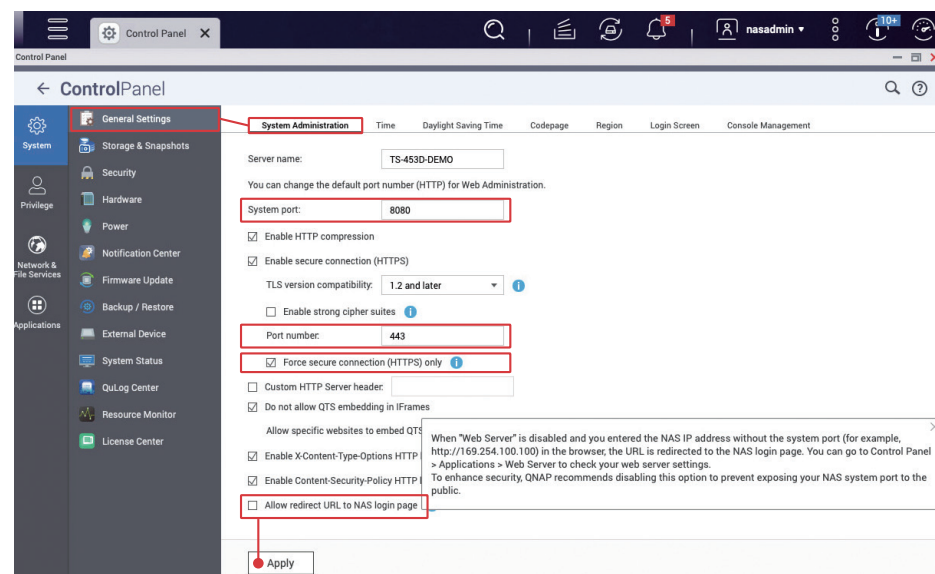
Modifier les ports par défaut

Chaque service exécuté sur le NAS a un port de service correspondant. À l'exception de certains ports de service standardisés qui ne peuvent pas être modifiés, le reste peut être défini par les utilisateurs.

Lorsqu'un pirate recherche une cible d'attaque ou utilise le moteur de recherche IoT souvent utilisé par les pirates, il essaie généralement le port par défaut en premier. Pour réduire le risque d'être attaqué, vous devez modifier les ports par défaut des services communs. En ce qui concerne les attaques contre les NAS, la cible la plus courante est le « port système ». Vous trouverez ci-après la méthode permettant de changer le « port système ». Les ports pour les autres fonctions peuvent être modifiés sur la page de paramètres correspondante. Assurez-vous de les modifier avant d'utiliser les services associés pour des raisons de sécurité.

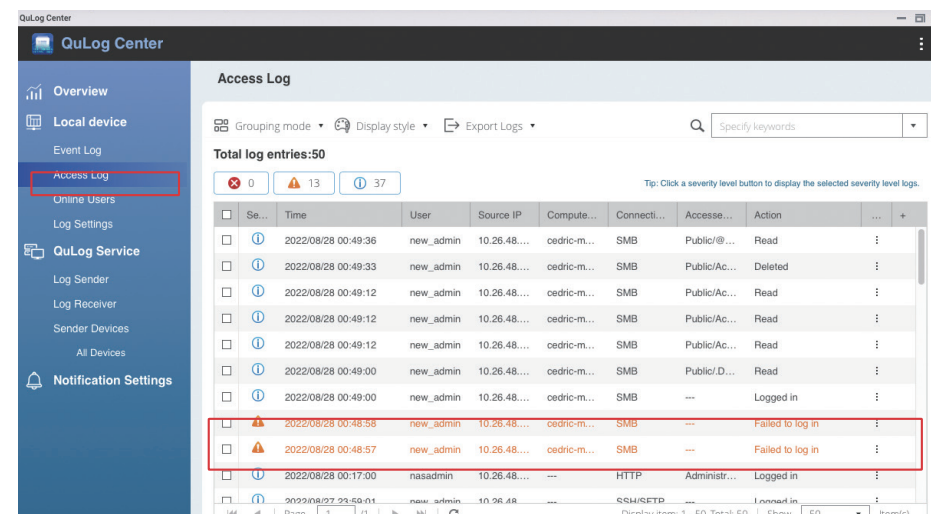
Ouvrez « Panneau de configuration », cliquez sur « Paramètres généraux », le « Port système (HTTP) » par défaut est « 8080 », vous pouvez entrer un numéro de port entre 1 et 65535 tel que « 56789 » ; pour « Port système (HTTPS) », c'est-à-dire le **port système** (la valeur par défaut est « 443 ») avec la fonction « connexion sécurisée » activée, il est également **recommandé de le changer**. Dans le même temps, il est également **recommandé de cocher « Forcer la connexion sécurisée (HTTPS) uniquement »** pour s'assurer que tous les utilisateurs transmettent des données via HTTPS, et aider à empêcher les pirates d'intercepter des informations sensibles telles que les mots de passe des comptes.

De plus, il est également **recommandé de décocher « Autoriser l'URL de redirection vers la page de connexion NAS »** pour empêcher que le « Port système » ne soit exposé en raison de la redirection automatique. Après le changement, cliquez sur « Appliquer » pour terminer le réglage.

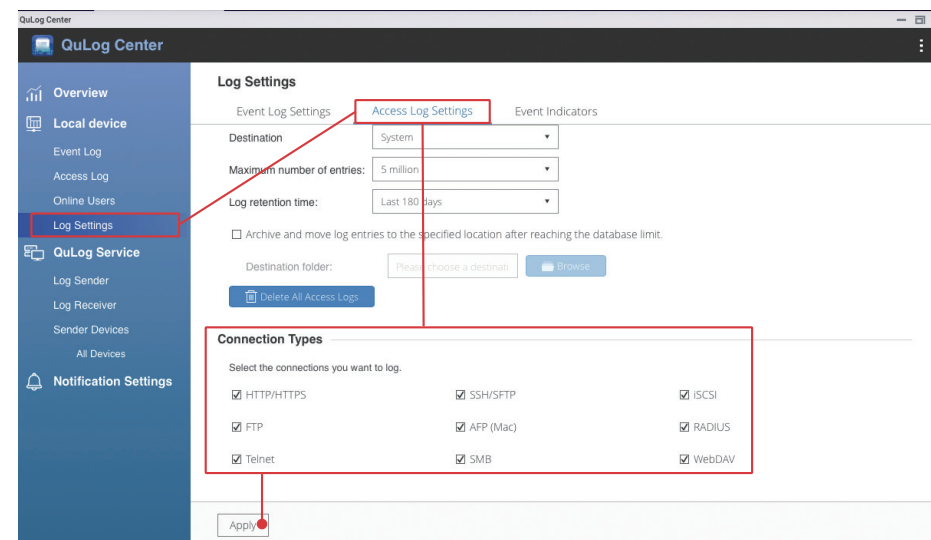


Afficher les journaux d'accès

Les journaux d'accès peuvent vous aider à afficher l'historique d'accès aux fichiers, de fonctionnement et de connexion de l'utilisateur. Lorsqu'un problème survient, la vérification des journaux d'accès doit être la première étape pour diagnostiquer les problèmes sous-jacents.



Ouvrez « QuLog Center », cliquez sur « Paramètres du journal » dans le menu de gauche, passez à la page « Paramètres du journal d'accès », dans « Types de connexion », vérifiez toutes les connexions, puis cliquez sur « Appliquer » pour terminer le réglage.



Installer et activer les applications de sécurité

QNAP fournit plusieurs applications de sécurité pour améliorer la sécurité du NAS. La configuration de ces applications peut améliorer la sécurité du NAS et permettre aux utilisateurs d'avoir l'esprit tranquille.



Conseiller de sécurité vérifie régulièrement la sécurité des paramètres de votre NAS et vous informe des risques potentiels.



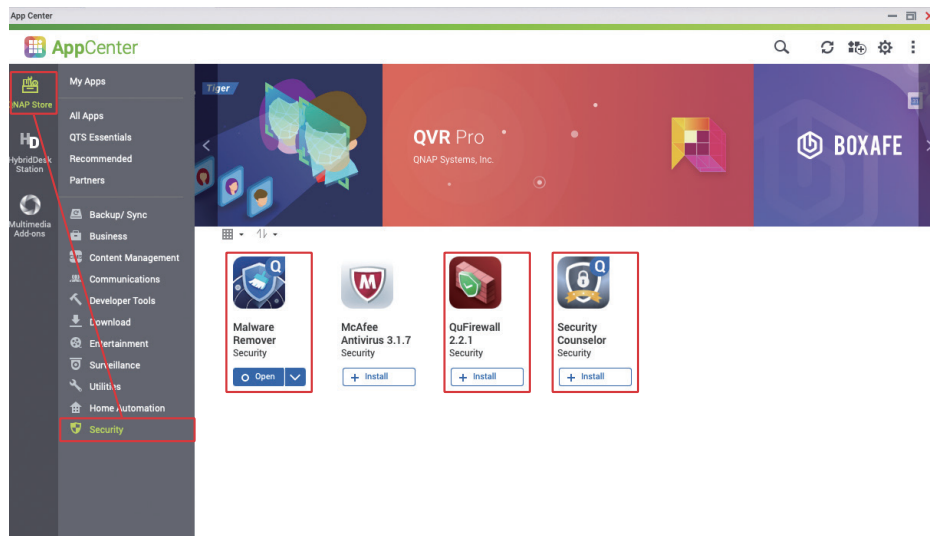
Malware Remover analyse et supprime les logiciels malveillants détectés de votre NAS.



QuFirewall fournit une fonctionnalité de pare-feu de base pour le NAS QNAP, empêchant autant de pirates que possible de se connecter à votre NAS.

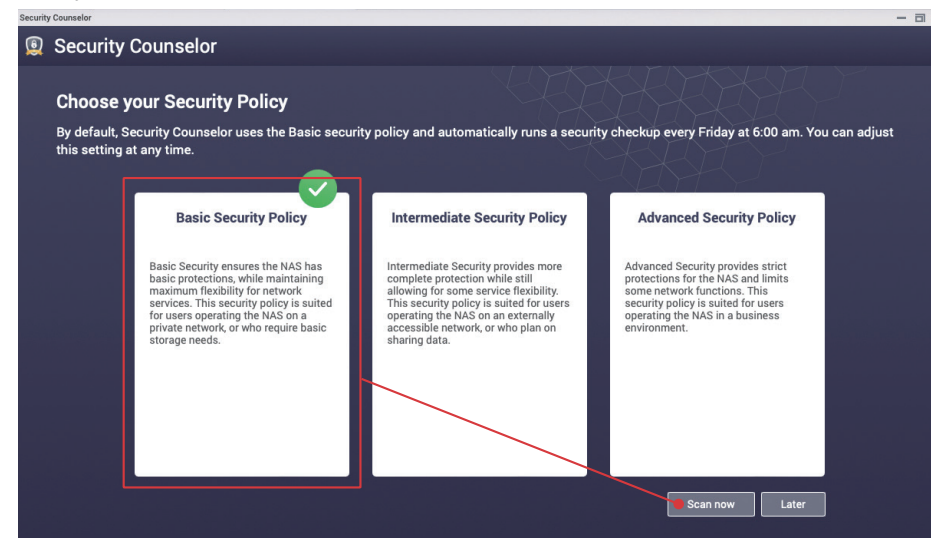
Ouvrez « App Center », cliquez sur « Sécurité » à gauche, installez « Conseiller de sécurité », « Malware Remover »* et « QuFirewall ».

* Malware Remover est préchargé sur QTS 4.4.3 (et versions ultérieures) et QuTS hero

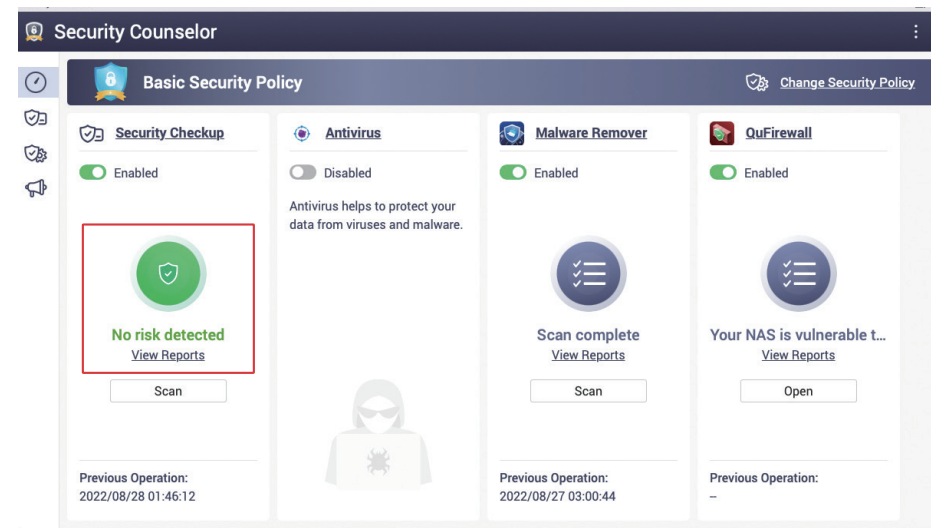


Conseiller de sécurité

Ouvrez « Conseiller de sécurité », sélectionnez « Stratégie de sécurité de base » et cliquez sur « Analyser maintenant ».



Une fois l'analyse terminée, le résultat est normalement « Aucun risque détecté ». Si un risque est détecté, cliquez sur « Afficher les rapports » pour plus de détails et suivez les instructions pour modifier les paramètres.



Voici les résultats d'analyse causés par « à haut risque » avec des paramètres incorrects délibérément modifiés. Cliquez sur « l'assistant de paramètres suggérés » pour vous aider à ajuster les paramètres.

Security Counselor

Basic Security Policy Change Security Policy

At High Risk Last scan status: Finished Last scan time: 2022/08/28 01:53:30 Scan schedule: Friday 06: 00

Overview **1** High **1** Medium **0** Low **0** Scan

Category	Status	Risk	Result	Action
Account	❌	High	Either this setting is deselected in the Password Policy screen or the current required mini...	⋮
Update	✅	High	Do the current settings in the Password Policy screen include requiring the use of passwords with a minimum of 8 characters?	⋮
Account	✅	High	Either this setting is deselected in the Password Policy screen or the current required minimum length for passwords is below 8 characters.	⋮
Network	✅	High	The web server on your device cannot be directly accessed from the internet using the foll...	⋮
Network	✅	High	The NAS doesn't allow Telnet connections.	⋮
System	✅	High	Run user defined processes during startup is disabled.	⋮

L'« Assistant de configuration suggérée » répertorie les suggestions pertinentes. Après avoir lu et confirmé, cliquez sur « Appliquer la suggestion » et le système appliquera automatiquement les paramètres pertinents pour vous. Certains paramètres doivent être modifiés manuellement, cliquez sur l'onglet « Manuellement » à gauche et ajustez les paramètres comme suggéré. Après avoir appliqué les modifications, l'analyse redémarrera automatiquement. Vous pouvez vérifier à nouveau les résultats de l'analyse pour vous assurer qu'aucun risque de sécurité n'a été détecté sur le NAS.

Security Counselor

Suggested Settings Assistant

The Suggested Settings Assistant offers suggestions that help improve NAS security.

Automatic Adjustment: There are **1** at-risk settings. Select the risk items below to automatically adjust the related settings.

At-risk User Settings	Suggestion
❌ Either this setting is deselected in the Password Policy screen or the current required minimum length for passwords is below 8 characters.	✅ Configure the settings in the Password Policy screen and require the use of passwords with a minimum of 8 characters.

Apply suggestion Close

Cliquez sur « Contrôle de sécurité » sur la gauche pour accéder à l'écran des résultats de l'analyse, puis cliquez sur « Planification de l'analyse » sur la droite pour ouvrir l'écran de réglage de la planification de l'analyse.

Security Counselor

Basic Security Policy Change Security Policy

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

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

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

« Planification d'analyse » est recommandé d'être réglé sur **au moins une fois par mois**, afin que le système puisse vérifier régulièrement les paramètres et l'état du système. Si un risque est détecté et que le centre de notification est correctement configuré, vous recevrez une notification afin qu'il puisse être traité dans les meilleurs délais.

Security Counselor

Basic Security Policy Change Security Policy

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

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

Scan schedule

☐ Disable schedule

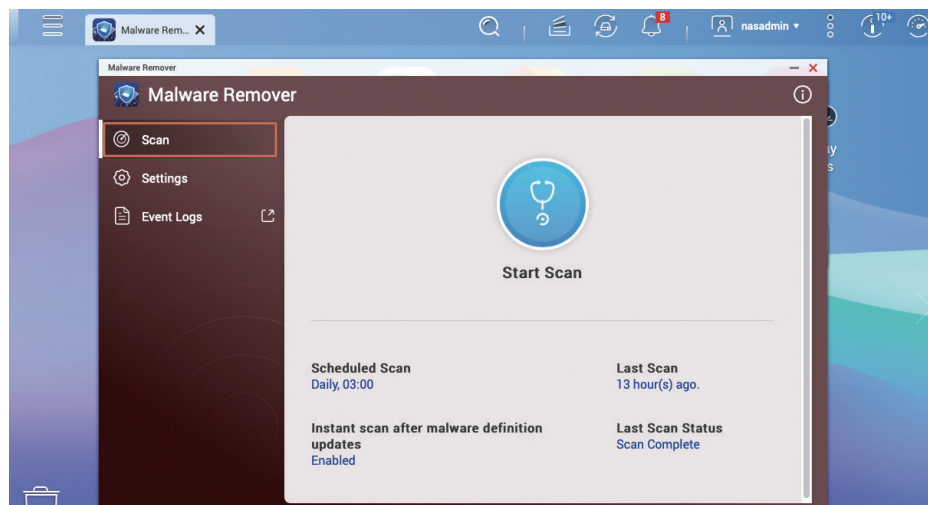
☒ Enable schedule

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

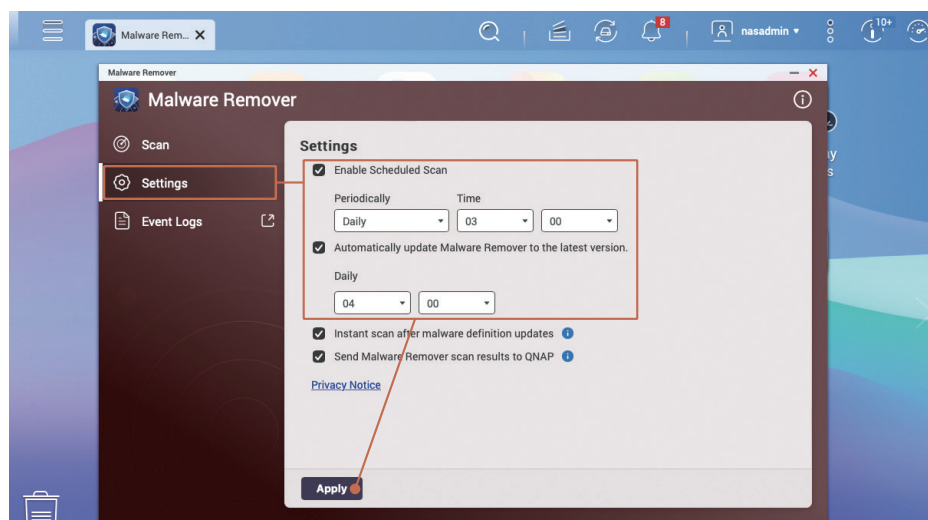
Apply Cancel

Malware Remover

Ouvrez « Malware Remover », l'état de la dernière analyse s'affiche, cliquez sur « Paramètres » à gauche.

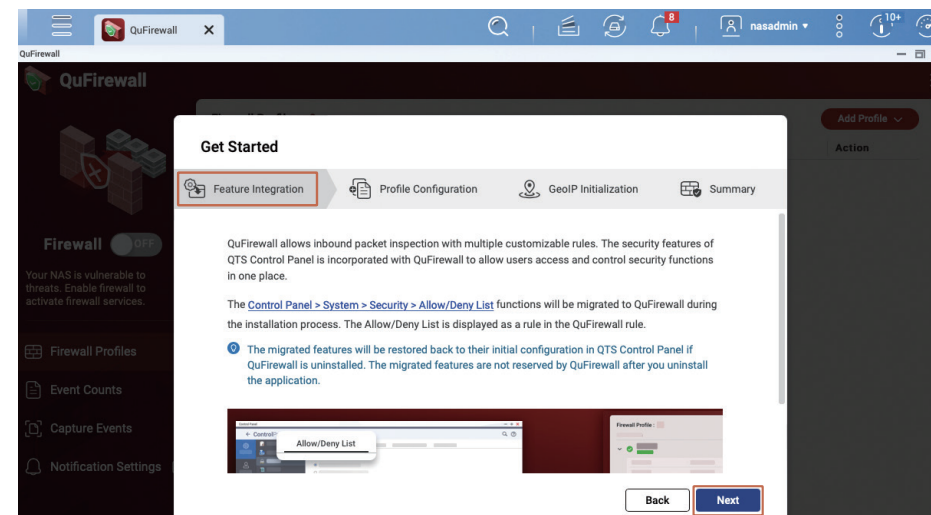


Nous recommandons de régler « Planification d'analyse » sur **une fois par jour**, afin que « Malware Remover » vérifie régulièrement l'état du système. Assurez-vous également que l'option « Mettre automatiquement à jour Malware Remover vers la dernière version » reste cochée.

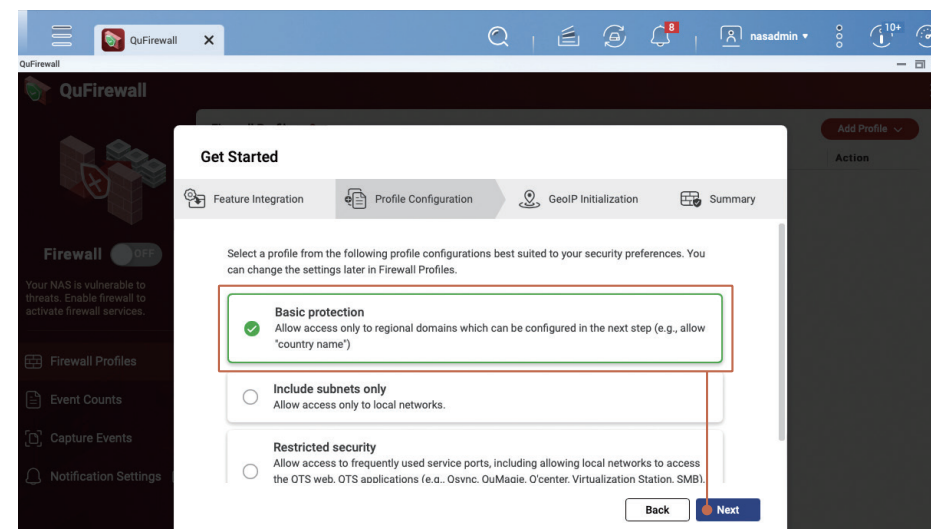


QuFirewall

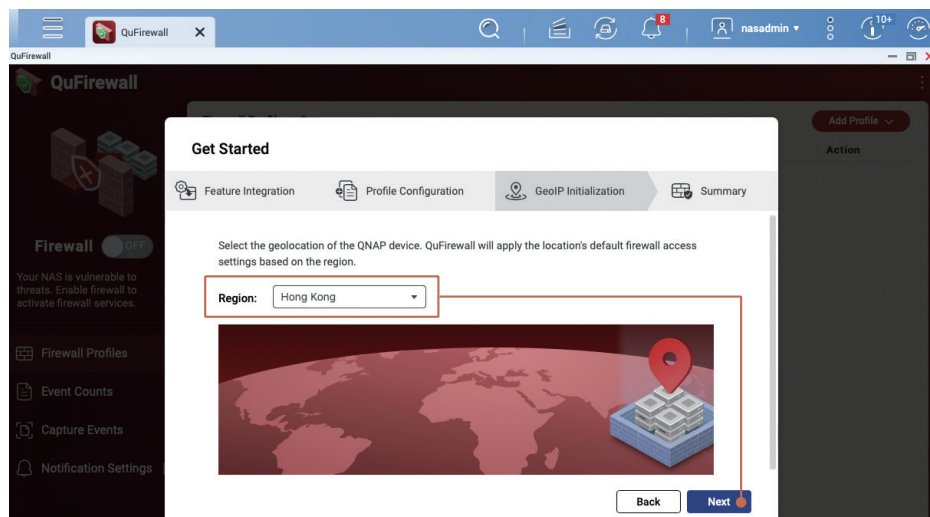
Ouvrez QuFirewall. Si c'est la première fois que vous utilisez QuFirewall, l'écran de démarrage s'affiche. Après lecture, cliquez sur « Suivant » pour continuer.



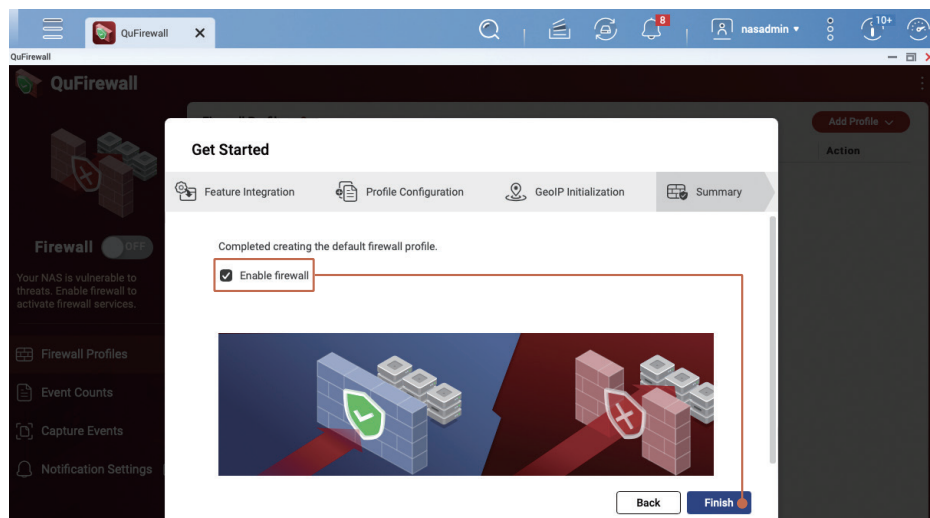
Si votre réseau n'a pas de besoins particuliers, il est recommandé de sélectionner « Protection de base », puis de cliquer sur « Suivant » pour continuer.



Définissez une région en fonction de votre emplacement. Par exemple : si vous êtes à Taïwan, sélectionnez « Taïwan » ; si vous êtes à Hong Kong, veuillez sélectionner « Hong Kong » ; si vous êtes à Macao, veuillez sélectionner « Macao ». Vous pourrez ajouter d'autres régions ultérieurement. Cliquez sur Suivant pour continuer.

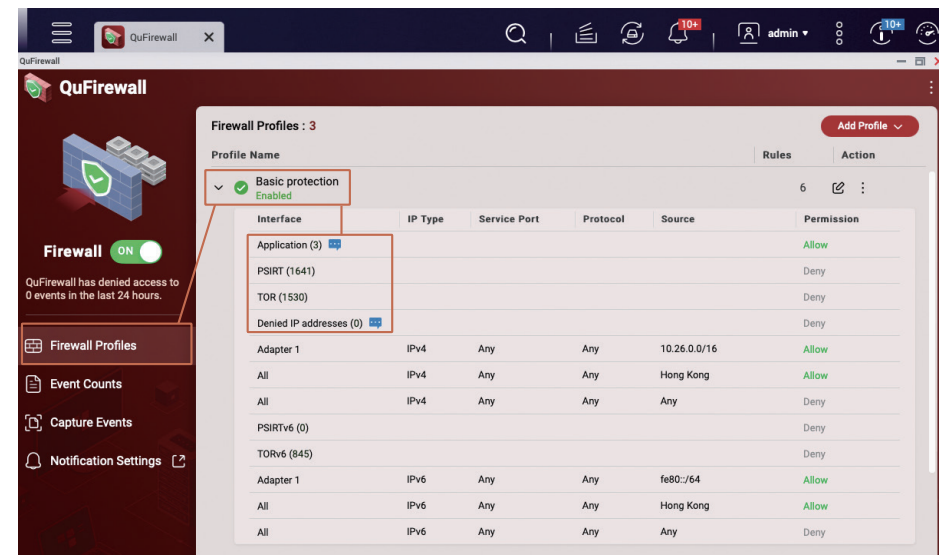


Cochez « Activer le pare-feu », puis cliquez sur « Terminer » pour appliquer les paramètres et activer le pare-feu.



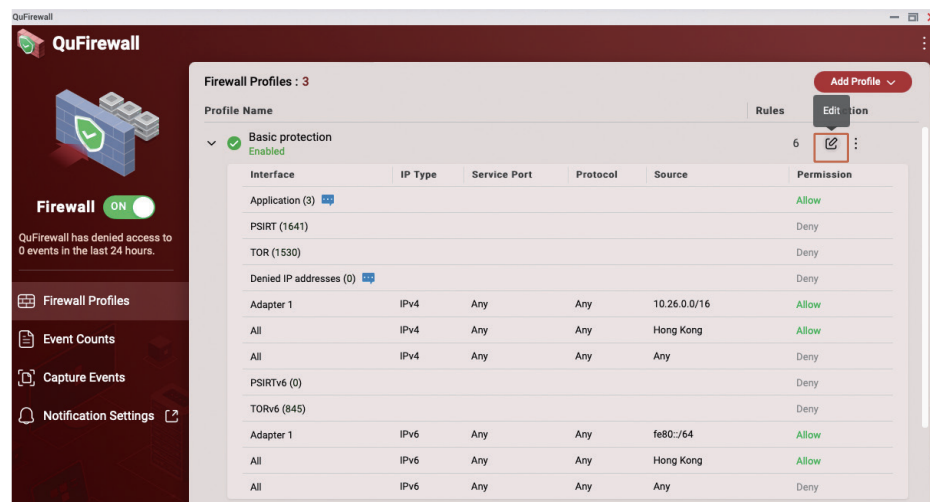
Allez sur la page Profils QuFirewall et vous verrez que la « Protection de base » est activée. Cliquez sur « Protection de base » pour développer et afficher les règles de pare-feu correspondantes. Les règles sont vérifiées par rapport aux informations contenues dans les paquets entrants, qui sont autorisés à passer ou à être bloqués selon les règles du pare-feu. Les règles de pare-feu seront exécutées dans l'ordre. Si les conditions ne sont pas remplies, la ligne de règles suivante sera vérifiée. S'ils ne sont pas respectés, ils tomberont dans la dernière règle « tout refuser » et le pare-feu bloquera les connexions concernées.

- Des règles « d'application » sont créées par le système pour assurer le bon fonctionnement du système.
- La règle « PSIRT » est une liste noire compilée par la PSIRT QNAP. Il contient des adresses IP connues pour attaquer le NAS QNAP.
- La règle « TOR » est utilisée pour bloquer les connexions du réseau TOR. Le réseau TOR est largement utilisé par les criminels en raison de son anonymat, et le bloquer peut réduire le risque d'être attaqué.
- Les « adresses IP refusées » sont des adresses IP bloquées par la fonction « Protection d'accès IP » ou la liste noire ajoutée manuellement par l'utilisateur.



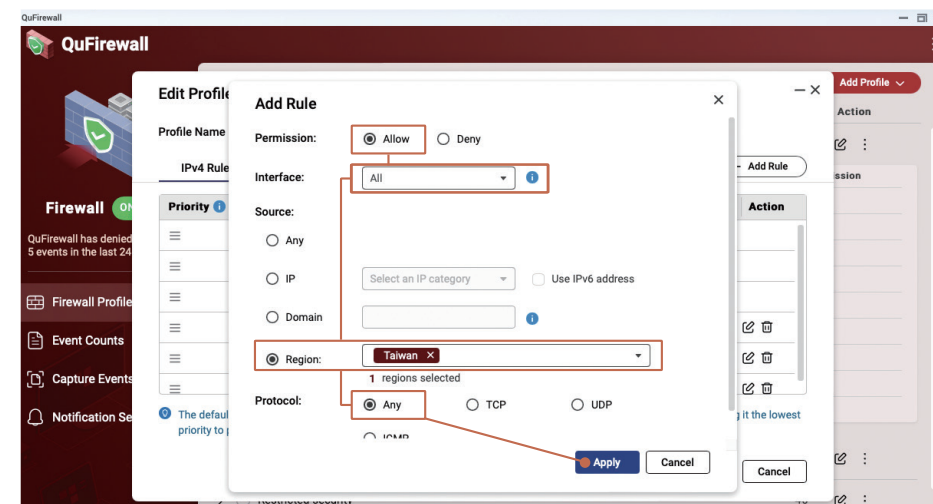
D'autres règles peuvent être personnalisées par l'utilisateur, et sous les paramètres de protection de base, seules les connexions Internet du même intranet et de la même région seront « autorisées ». QNAP recommande d'utiliser le concept de « liste blanche » pour gérer vos règles personnalisées afin de limiter strictement les adresses IP pouvant se connecter au NAS.

Ce qui suit montre comment modifier les règles de pare-feu. Cliquez sur le bouton « Modifier » pour modifier l'écran Profils de pare-feu.

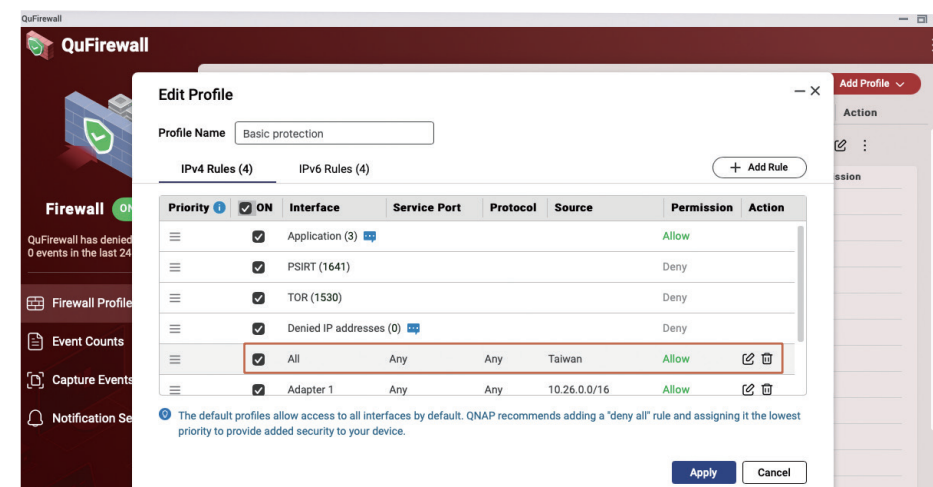
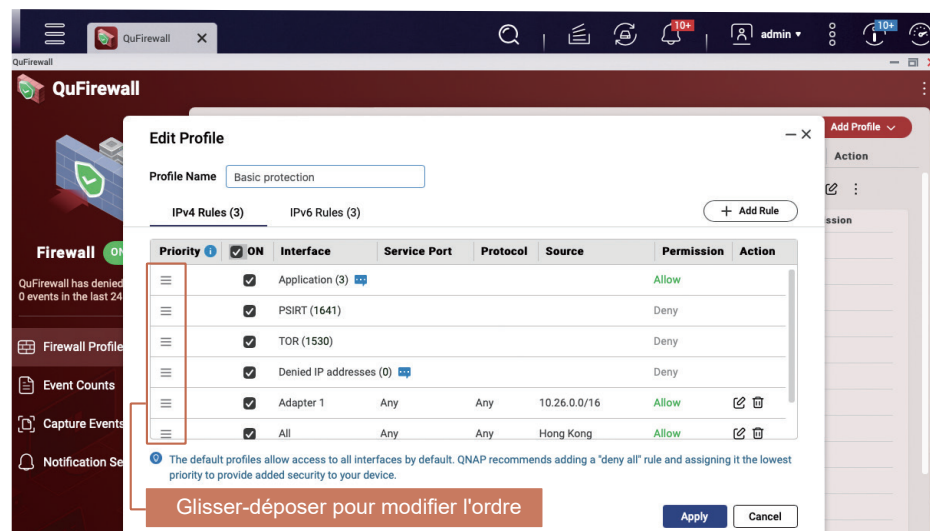


Sur l'écran Modifier le profil, vous pouvez modifier l'ordre des règles ou ajouter de nouvelles règles. L'exemple suivant ajoute une autre région autorisée à se connecter, cliquez sur « Ajouter une règle » pour accéder à l'écran de configuration.

Par exemple, pour autoriser les connexions depuis Taïwan, « Autorisation » doit être défini sur « Autoriser » ; « Interface » réglé sur « Tous » ; « Région » pour « Source », puis sélectionnez « Taïwan » ; « Protocole » défini sur « Tout », puis cliquez sur « Appliquer » pour ajouter la règle lorsque vous avez terminé.



Sur la page « Modifier le profil », vous pouvez voir les règles nouvellement ajoutées. Si nécessaire, vous pouvez ajuster l'ordre des règles. Après avoir confirmé qu'ils sont corrects, cliquez sur « Appliquer ».



Activer les snapshots planifiés

La fonction de snapshot peut protéger vos données importantes en créant des points de restauration multi-versions. Vous pouvez définir une planification de snapshots sur le NAS QNAP pour permettre au système de créer automatiquement des snapshots en fonction de la planification en tant que protection de base des données.

- * Les snapshots planifiés sont activés par défaut pour les « volumes pleins/minces » créés par QTS 5.0.0
- * Dans QTS 5.0.1 (et versions ultérieures), seuls les « volumes minces » ont des snapshots planifiés activés par défaut
- * Les « dossiers partagés » créés par QuTS hero h5.0.1 (et versions ultérieures) activeront les snapshots planifiés par défaut

Ouvrez « Stockage et snapshots », cliquez sur « Stockage/Snapshots » sur la gauche et assurez-vous que « Espace de stockage » est une structure « Pool de stockage » et que le « Pool de stockage » dispose de suffisamment d'espace libre pour que la fonction de snapshot fonctionne. Si votre type de volume est « volume plein », vous pouvez envisager « Redimensionner le volume* » et « Convertir en volume mince* » pour libérer de l'espace dans le « Pool de stockage » pour la fonction de snapshot.

- * Vous devez sauvegarder vos données avant de convertir des volumes pour éviter une perte de données potentielle.

Après avoir confirmé qu'il y a suffisamment d'espace dans le « Pool de stockage » sur le NAS, cliquez d'abord sur « Volume », puis cliquez sur « Snapshot » en haut, et cliquez sur « Gestionnaire de snapshots » dans le menu.

Accédez à la page de configuration « Gestionnaire de snapshots » de « Volume » et cliquez sur « Planifier un snapshot » en haut à droite.

Basculez « Activer la planification » sur l'état « Activer », puis modifiez la planification en fonction de vos besoins.

Il est recommandé d'utiliser « Quotidien » ou « Hebdomadaire ».

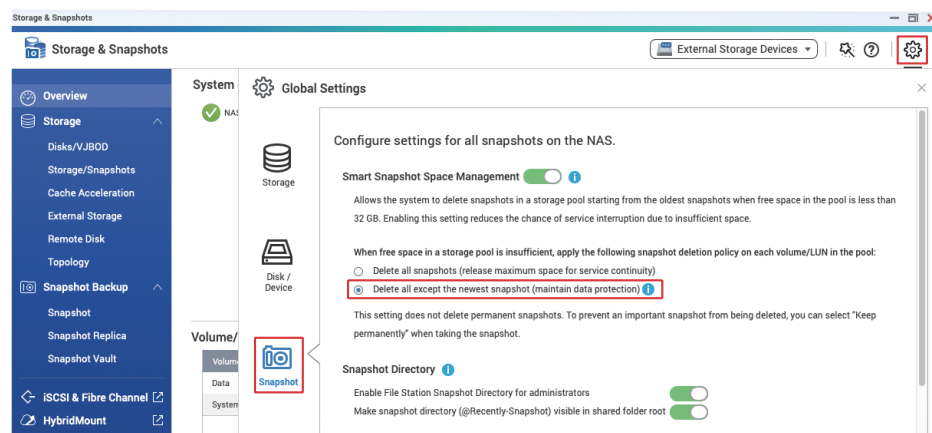
Vous pouvez définir une stratégie de rétention de snapshots pour limiter le nombre de snapshots et empêcher les snapshots d'occuper trop d'espace.

Il est recommandé de définir « Versions intelligentes », c'est-à-dire la règle Grand-père-Père-Fils (GPS), afin de conserver suffisamment de versions pour la protection des données. Une fois le réglage terminé, cliquez sur « OK » pour appliquer les paramètres.

Définir la stratégie de suppression de snapshot

Lorsque le pool de stockage dispose d'un espace insuffisant, le système supprime les snapshots en fonction de vos paramètres pour maintenir un service système normal et éviter une interruption de service potentielle causée par un espace insuffisant.

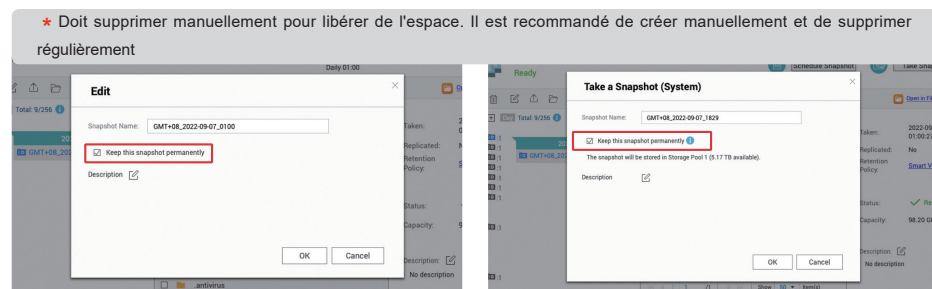
Dans « Stockage et snapshots », cliquez sur le bouton « Paramètres » dans le coin supérieur droit, ouvrez « Paramètres généraux » et cliquez sur « Snapshot ». Il est recommandé de le définir sur « **Supprimer tout sauf le dernier snapshot** » pour éviter que tous les snapshots ne soient récupérés et ne perdent leur protection.



Si vous souhaitez que le système conserve tous les snapshots même lorsque le « pool de stockage » dispose d'un espace insuffisant, désactivez la « gestion intelligente de l'espace des snapshots ». Veuillez noter que cela entraînera le passage du « Pool de stockage » à l'état « lecture seule/suppression » lorsque l'espace « Pool de stockage » est insuffisant. Vous devez supprimer manuellement le snapshot pour restaurer le « pool de stockage » en fonctionnement normal. Assurez-vous de vérifier régulièrement l'utilisation de l'espace après avoir désactivé cette fonction.



Pour éviter l'échec de la protection en raison de la stratégie de suppression des snapshots, il est recommandé de définir tout ou partie des snapshots sur « Conserver le snapshot en permanence » * après avoir stocké une grande quantité de données pour éviter que les snapshots ne soient recyclés par le système.



Liste de contrôle des paramètres de sécurité NAS

- ❑ **Configuration du centre de notification**
 - ❑ Définir au moins une méthode de notification
 - ❑ Créer des règles « Notifications d'alertes »
 - ❑ Créer des règles de notification « Mise à jour du firmware »
- ❑ **Activer la mise à jour automatique du firmware (QTS / QuTS hero)**
- ❑ **Configurer l'App Center**
 - ❑ Mettre à jour toutes les applications vers la dernière version
 - ❑ Interdire l'installation d'applications qui n'ont pas de signature numérique valide
 - ❑ Activer les mises à jour automatiques
- ❑ **Désactiver ou supprimer les fonctions inutiles**
 - ❑ Vérifier si des services activés sont nécessaires
 - ❑ Vérifier si les applications App Center activées sont nécessaires
 - ❑ Désactiver SSH
 - ❑ Désactiver Telnet
- ❑ **Renforcer la sécurité du compte système**
 - ❑ Désactiver le compte « admin » par défaut
 - ❑ Définir la stratégie de mot de passe
 - ❑ Activer **Protection d'accès IP**
 - ❑ Activer la vérification en deux étapes (2SV)
- ❑ **Modifier le port système par défaut**
- ❑ **Activer le Journal d'accès**
- ❑ **Installer et activer les applications de sécurité**
 - ❑ **Conseiller en sécurité**
 - ❑ Démarrer l'analyse planifiée
 - ❑ **Malware Remover**
 - ❑ Démarrer l'analyse planifiée
 - ❑ **QuFirewall**
 - ❑ Activer le pare-feu
 - ❑ Définir la région **Geo-IP**
 - ❑ Activer les règles **PSIRT**
 - ❑ Activer les règles **TOR**
- ❑ **Activer les snapshots planifiés**
 - ❑ Régler régulièrement « Conserver le snapshot en permanence »

Q Est-il plus sûr de déconnecter le NAS d'Internet ?

A Non. La « déconnexion » du NAS fait généralement référence à la coupure du NAS du réseau afin qu'il ne puisse pas établir de connexions avec le monde extérieur. Bien que certains logiciels malveillants nécessitent une connexion externe pour s'exécuter, il existe encore des logiciels malveillants capables d'effectuer avec succès des actions malveillantes sans connexion externe. Par conséquent, non seulement il ne parviendra pas à empêcher les pirates d'effectuer des actions illégales, mais il empêchera également certaines fonctions du système de fonctionner correctement, telles que les mises à jour logicielles automatiques et les notifications. L'approche correcte consiste à limiter le trafic vers le NAS, par exemple en évitant l'exposition à Internet, pour améliorer la sécurité.

Q Mon disque dur est configuré en RAID, cela signifie-t-il que je n'ai pas besoin de sauvegarde ?

A Non. RAID n'est pas une méthode de sauvegarde. Les niveaux RAID supérieurs à 0 sont uniquement destinés à fournir une redondance contre les pannes de disque. RAID n'offre aucune protection contre la suppression ou le chiffrement des données. Par conséquent, il est recommandé de **sauvegarder correctement les données selon le principe de sauvegarde 3-2-1**.

Q J'ai déjà configuré des « snapshots », cela signifie-t-il que je n'ai pas besoin de sauvegarde ?

A Non. Étant donné que les « snapshots » sont stockés sur le même ensemble de disques durs que vos données, les données seront toujours perdues en cas de panne RAID. De plus, si les pirates peuvent obtenir des privilèges suffisants (comme réussir à casser le compte administrateur), l'« snapshot » peut également être supprimé. Par conséquent, il est recommandé de sauvegarder correctement les fichiers de snapshot selon le principe de sauvegarde 3-2-1.

Q Mon NAS n'est pas exposé à Internet, cela signifie-t-il qu'il est impossible d'être attaqué ?

A Non. Bien que la plupart des cyberattaques proviennent d'Internet, le NAS risque toujours d'être attaqué sur l'intranet. Par exemple, si un autre ordinateur ou appareil de votre intranet est piraté ou affecté par un logiciel malveillant, il peut être utilisé pour attaquer et se propager à d'autres appareils de l'intranet. L'installation d'un logiciel antivirus et le déploiement de produits de sécurité réseau sur votre ordinateur peuvent vous aider à faire face aux menaces associées. Par exemple, QNAP ADRA NDR peut détecter les activités intranet suspectes et les isoler automatiquement. Dans le même temps, il est également recommandé de sauvegarder correctement les données selon le principe de sauvegarde 3-2-1.

Q Mon NAS est utilisé depuis longtemps, comment puis-je vérifier si un logiciel malveillant est installé ?

A Si vous remarquez que la charge du processeur est anormalement élevée, rencontrez des échecs de mise à jour logicielle ou s'il existe des applications inconnues dans l'App Center, il est possible qu'un programme malveillant ait été installé. Il est recommandé d'installer et d'utiliser la dernière version du Malware Remover. Si vous ne parvenez toujours pas à résoudre le problème, contactez l'équipe d'assistance technique de QNAP pour obtenir de l'aide.

Q Si je suis dans l'obligation d'ouvrir certains services à internet, comment garantir la sécurité ?

A Assurez-vous que le NAS dispose de la dernière version du firmware et des applications installées. Vous pouvez activer QuFirewall pour fournir une protection de base par pare-feu, et les règles « PSIRT » et « TOR » peuvent vous aider à bloquer les connexions de certains pirates. Si vous êtes un utilisateur professionnel ou d'entreprise, il est recommandé d'utiliser une solution de pare-feu de niveau supérieur. De plus, si l'espace du pool de stockage le permet, vous pouvez créer des « snapshots » pour la protection de base des données. Il est également recommandé de sauvegarder correctement les données selon le principe de sauvegarde 3-2-1 pour se préparer au pire scénario et éviter une perte de données potentielle.

Q Mon NAS est ancien et ne prend pas en charge la dernière version de QTS, peut-il encore être utilisé en toute sécurité ?

A Les modèles hérités et en fin de vie (EOL) ont une prise en charge limitée et ne doivent être utilisés que pour la sauvegarde intranet/hors ligne.

Q Pourquoi est-ce que je continue à recevoir un avertissement d'échec de connexion au NAS ?

A Si l'adresse IP de l'échec de la connexion provient d'Internet, cela signifie que votre NAS subit une attaque de craquage de mot de passe par force brute. Vous devez éviter d'exposer votre NAS à Internet et suivre ce didacticiel pour renforcer votre NAS. Si l'adresse IP de l'échec de la connexion provient de l'intranet, veuillez vérifier si l'appareil avec cette adresse IP contient un logiciel malveillant.

Q Pourquoi tous mes fichiers ont-ils des noms de fichiers étranges ?

A Ceci est un symptôme d'une infection par ransomware. Vérifiez les journaux d'accès au NAS pour déterminer si l'action de chiffrement provient d'un autre ordinateur ou du NAS lui-même. Si votre NAS a été affecté par un ransomware, vous devez prendre les mesures adéquates pour arrêter la propagation de l'infection. Si nécessaire, contactez l'équipe d'assistance technique de QNAP pour obtenir de l'aide.

Q Que dois-je faire si mon NAS est infecté par un ransomware ?

A La plupart des ransomwares utilisent des méthodes de chiffrement incassables. S'il n'y a pas de clé correcte, les fichiers ne peuvent pas être déverrouillés, de sorte que les fichiers ne peuvent être restaurés que par sauvegarde ou snapshot.

Modifiez immédiatement les paramètres du routeur conformément à ce didacticiel pour éviter d'exposer le NAS à Internet et pour empêcher les attaques secondaires. Deuxièmement, vous devez immédiatement suspendre toutes les tâches de synchronisation et définir des snapshots pour qu'ils soient conservés en permanence afin d'éviter de perdre des fichiers de sauvegarde. Si vos données contiennent des sauvegardes ou des snapshots que vous pouvez restaurer, vous pouvez restaurer les fichiers après avoir mis à jour le firmware et les applications du NAS et après avoir terminé l'analyse du Malware Remover. Si les données ne sont pas sauvegardées, veuillez sauvegarder la note de rançon laissée par le ransomware et la méthode de paiement de la rançon, puis essayez d'utiliser des méthodes telles que la récupération de données pour récupérer certaines données. Si nécessaire, contactez l'équipe d'assistance technique de QNAP pour obtenir de l'aide.

Q Je continue de voir des rapports dans la presse faisant état de correctifs de vulnérabilités sur les produits QNAP. Cela signifie-t-il que les produits QNAP ne sont pas sûrs ?

A Il n'y a pas de logiciel et de matériel parfaits dans le monde. Qu'il s'agisse de logiciels propriétaires développés par divers fabricants ou de logiciels open source, voire de matériel, les vulnérabilités sont toujours trouvées puis corrigées par les fabricants. Comme d'autres grandes entreprises technologiques, QNAP continue de corriger les vulnérabilités connues, puis publie des fichiers de mise à jour que les utilisateurs doivent mettre à jour dès que possible pour assurer la sécurité des appareils et des données des utilisateurs. La PSIRT QNAP émet également des notifications de cybersécurité pour la divulgation externe, afin que les utilisateurs puissent agir contre les problèmes qui surviennent. QNAP estime que traiter les vulnérabilités de manière ouverte et transparente peut protéger le droit des utilisateurs à savoir et contribuer à améliorer la sécurité des produits. Les utilisateurs sont également invités à s'abonner aux avis de sécurité de QNAP pour obtenir des informations pertinentes, exactes et complètes avant les reportages des médias.



Avis de sécurité QNAP :

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

Q Qu'est-ce que le principe de sauvegarde 3-2-1 ?

A Le principe de sauvegarde 3-2-1 est un principe de sauvegarde bien connu dans l'industrie informatique. Il vous prépare au pire scénario. Il garantit qu'en cas de sinistre, il existe des fichiers de sauvegarde pour restaurer les données afin d'éviter les pertes et d'assurer la sécurité.

« 3 » dans Sauvegarde 3-2-1 signifie au moins trois copies de sauvegarde ; « 2 » signifie au moins deux supports de stockage ; et « 1 » signifie qu'au moins une copie est une sauvegarde hors site.

Selon le principe de sauvegarde 3-2-1, il y aura des fichiers de sauvegarde qui pourront être restaurés indépendamment de la modification accidentelle, de la suppression, des dommages matériels, de l'infection virale et des catastrophes telles que les incendies et les inondations.

Pour satisfaire ce principe, le NAS QNAP inclut Hybrid Backup Sync 3 (HBS3), Snapshot Replica et SnapSync (pris en charge par QuTS hero uniquement) pour sauvegarder les données sur le NAS vers un NAS hors site, un cloud public, un stockage externe, d'autres serveurs de fichiers, et/ou d'autres dispositifs pour s'assurer que rien n'est perdu.

Didacticiels Hybrid Backup Sync 3 (HBS3) :

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



Didacticiels sur les répliques de snapshots :

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



Didacticiels SnapSync :

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



Pour améliorer la sécurité, vous pouvez ajouter une sauvegarde hors ligne ou une sauvegarde à l'espace de stockage WORM (Write Once Read Many) de QuTS hero pour empêcher la falsification des données.

MÉMO



2 0 2 3

Guide de sécurité



QNAP SYSTEMS, INC.

TÉL. : +886-2-2641-2000 FAX : +886-2-2641-0555 E-mail : qnapsales@qnap.com

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

QNAP peut apporter des modifications aux caractéristiques et descriptions des produits à tout moment sans préavis.

Copyright © 2023 QNAP Systems, Inc. Tous droits réservés.

QNAP® et d'autres noms de produits QNAP sont des marques propriétaires ou des marques déposées de QNAP Systems, Inc.

Les autres produits et noms de société mentionnés dans le présent document sont des marques commerciales de leurs détenteurs respectifs.