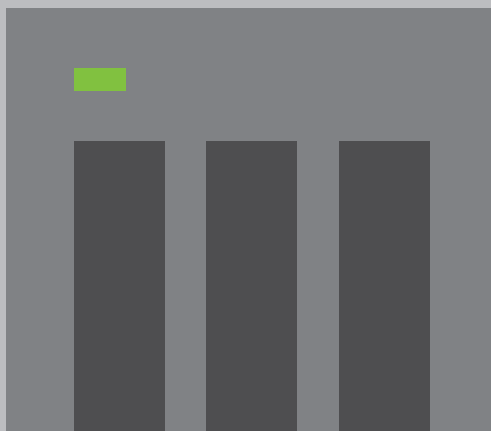


2 0 2 3

Guía de seguridad



2 0 2 3

Guía de seguridad

ÍNDICE

- 1 Prefacio
- 2 Ataques más frecuentes
- 3 Conceptos básicos de los equipos de red
- 4 Diversas formas de conexión de Internet al NAS

Evite exponer el NAS a Internet

- 8 Conexión correcta del NAS
- 9 Comprobar la configuración del enrutador
- 12 Comprobar la configuración del NAS
- 15 Lista de verificación de la configuración relacionada con la red

Configuración de seguridad del NAS

- 17 Configurar notificaciones del sistema
- 24 Habilitar la actualización automática del firmware (QTS/QuTS hero)
- 25 Configuración de la actualización de aplicaciones
- 27 Deshabilitar o eliminar las funciones innecesarias
- 29 Deshabilitar Telnet/SSH
- 30 Reforzar la seguridad de las cuentas del sistema
- 34 Establecer la política de contraseñas
- 35 Habilitar protección de acceso (IP/cuenta)
- 36 Habilitar la verificación en dos pasos (2SV)
- 39 Cambiar los puertos predeterminados
- 40 Ver los registros de acceso
- 41 Instalar y habilitar aplicaciones de seguridad
- 42 Security Counselor
- 45 Malware Remover

- 46 QuFirewall
- 51 Habilitar instantáneas programadas
- 53 Establecer una política de eliminación de instantáneas
- 54 Lista de comprobación de la configuración de seguridad del NAS

Preguntas frecuentes | 58

Prefacio

QNAP concede gran importancia a la seguridad. Ante las crecientes amenazas, QNAP sigue mejorado continuamente los diseños de hardware y software para brindar a los usuarios soluciones seguras y prácticas.

El Equipo de respuesta a incidentes de seguridad de productos (PSIRT) de QNAP es el responsable de gestionar los problemas de seguridad relacionados con los productos de QNAP. Además de gestionar los incidentes relacionados con la ciberseguridad, el PSIRT también gestiona los informes, la investigación, la reparación y el anuncio de vulnerabilidades en diversos productos.

QNAP también está comprometido con las mejoras de seguridad de los productos. En el pasado, los productos se diseñaron para ser más prácticos y fáciles de configurar y usar para los usuarios. Con el aumento de los ciberataques contra dispositivos en red en los últimos años, la perspectiva del diseño de productos de QNAP también ha cambiado, y el diseño de productos se ha desplazado a Seguridad por Diseño para proteger a los usuarios y garantizar que los puedan hacer frente a las amenazas relacionadas.

Este tutorial ayudará a los usuarios a configurar correctamente el NAS para mejorar la seguridad. Si tiene alguna duda, comuníquese con nuestro equipo de soporte técnico para obtener ayuda:



Para conocer las vulnerabilidades de los productos y la información sobre incidentes relacionados con la seguridad, consulte y suscríbase a los Avisos de seguridad de QNAP:

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



Servicio al cliente de QNAP:

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



Ataques más frecuentes

Para saber cómo defenderse de los ciberataques hay que conocer cómo se lanzan. En lo que respecta a los ataques a NAS, la mayoría de los ataques se lanzan a través de Internet. Los ataques son en su mayoría de dos tipos: "descifrado de contraseñas" y "ataque a vulnerabilidades". El "ataque a vulnerabilidades" se puede dividir en "de día N" y "de día 0".

"De día N" se refiere a la explotación de una vulnerabilidad parcheada para lanzar un ataque, y la mayoría de los ataques activos actuales pertenecen a esta categoría. Puede defenderse de manera eficaz contra tales ataques asegurándose de tener siempre instalados los últimos parches y actualizaciones de seguridad.

"De día 0" significa explotar una vulnerabilidad desconocida para lanzar un ataque, y los proveedores solo pueden emitir parches de seguridad después del hecho. Estos ataques solo se pueden defender de manera eficaz evitando que los atacantes se conecten al dispositivo.

La siguiente tabla muestra las respuestas a diferentes ataques como referencia para los usuarios.

Respuesta	Ataques		
	Descifrado de contraseñas	Ataque a vulnerabilidades (de día N)	Ataque a vulnerabilidades (de día 0)
Evitar la exposición a Internet	V	V	V
Actualizar el software (sistema y aplicaciones)	X	V	Δ
Habilitar actualizaciones automáticas (sistema y aplicaciones)	X	V	Δ
Utilizar contraseñas seguras para todas las cuentas	V	X	X
Deshabilitar la cuenta "admin" predeterminada	V	X	X
Habilitar la verificación de 2 pasos	V	X	X
Habilitar la protección de acceso	Δ	X	X
Habilitar el cortafuegos	Δ	Δ	Δ
Recibir notificaciones del sistema	Δ	Δ	Δ
Cambiar los puertos predeterminados	Δ	Δ	Δ
Deshabilitar o eliminar funciones innecesarias	Δ	Δ	Δ

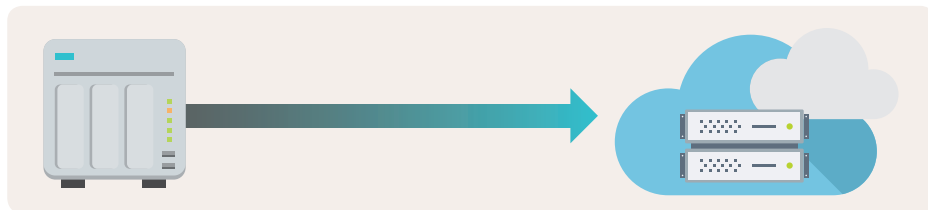
V: Eficaz X: No eficaz Δ: Posiblemente eficaz (significa que el ataque puede ser mitigado o el riesgo de ser atacado, reducido)

"Evitar la exposición a Internet" puede evitar que los atacantes se conecten y lancen ataques en su dispositivo. Este tutorial comienza por "Evitar la exposición a Internet" y posteriormente proporciona un tutorial completo de "Configuración de seguridad del NAS" para mejorar las capacidades defensivas del NAS.

Conceptos básicos de los equipos de red

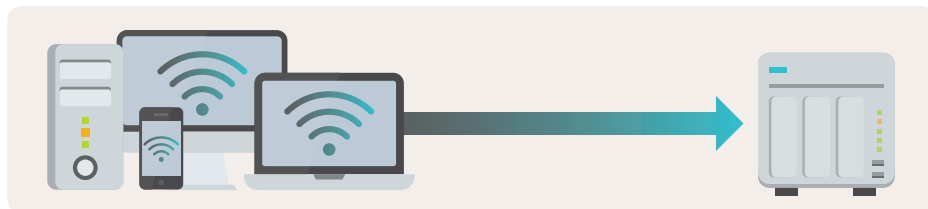
Como dispositivos conectados en red, los NAS tienen dos direcciones de conexión.

01 | Conexión externa del NAS



Un NAS generalmente requiere conectividad externa para que funcione correctamente. Por ejemplo, funciones básicas del sistema como actualizaciones automáticas y envío de notificaciones. Además, si necesita hacer una copia de seguridad de los datos del NAS en una nube pública, o usar el NAS para hacer una copia de seguridad de los datos de otros dispositivos o nubes públicas (como máquinas virtuales, Google Workspace o Microsoft 365), ordenadores o servidores, el NAS deberá poder iniciar conexiones salientes.

02 | Otros dispositivos (como ordenadores, teléfonos móviles u otros servidores) que se conecten al NAS



Si necesita usar cualquier función o servicio proporcionado por el NAS, incluido el acceso a archivos o a la interfaz de configuración, debe poder iniciar conexiones con el NAS.

Si el enrutador no tiene DMZ, reenvío de puertos o UPnP, bloqueará el tráfico de Internet. Solo los dispositivos de la red local podrán acceder al NAS.

Cuando el enrutador está habilitado y las funciones anteriores están configuradas, todos los usuarios de Internet pueden conectarse al puerto abierto y después reenviar al NAS de acuerdo con las reglas del enrutador, y posteriormente iniciar sesión y usar las funciones relacionadas normalmente. Sin embargo, esto también proporcionará a los hackers la posibilidad de atacar con el descifrado de contraseñas o la explotación de vulnerabilidades de software, lo que plantea riesgos para la seguridad.

Diversas formas de conectarse de forma remota al NAS

01 | Habilitar y configurar DMZ, reenvío de puertos o UPnP en el enrutador

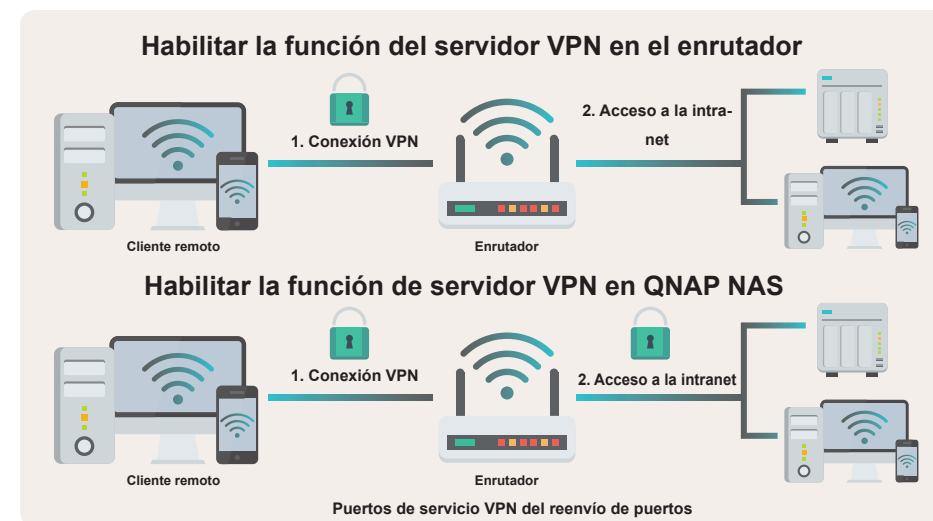
Este método supone riesgos de seguridad. A menos que sea un experto en configuración de redes y comprenda los riesgos involucrados, **QNAP no recomienda su uso***. Dado que el enrutador pasará el tráfico a los dispositivos de la intranet, si no hay un firewall instalado entre el enrutador y el NAS para bloquear el tráfico malicioso, los hackers pueden lanzar fácilmente ataques a la red. Sin embargo, aunque se instale un firewall (mediante el uso de un firewall básico o la compra de un firewall de nivel empresarial), no se garantiza que bloquee todos los ataques.

* QNAP solo recomienda abrir los puertos de servicio VPN de riesgo relativamente bajo a Internet, mientras que otros puertos de servicio de alto riesgo, como la administración del sistema, SMB y SSH, no deberían estar fácilmente accesibles desde Internet.



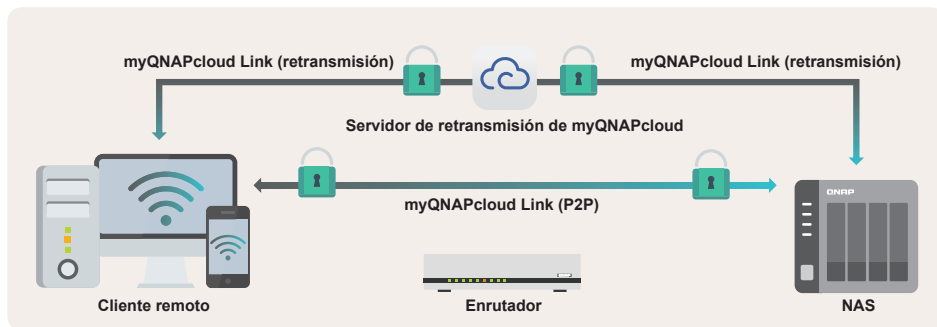
02 | Habilitar la función de servidor VPN en el enrutador o QNAP NAS

Algunos enrutadores admiten funciones de servidor VPN (como los enrutadores de las series QHora y QMiro de QNAP), mientras que el QNAP NAS también admite varios servidores VPN. Una vez habilitado y configurado correctamente, puede acceder a cada dispositivo en la intranet con una conexión encriptada de VPN desde Internet al servidor VPN, lo que brinda un alto nivel de seguridad.



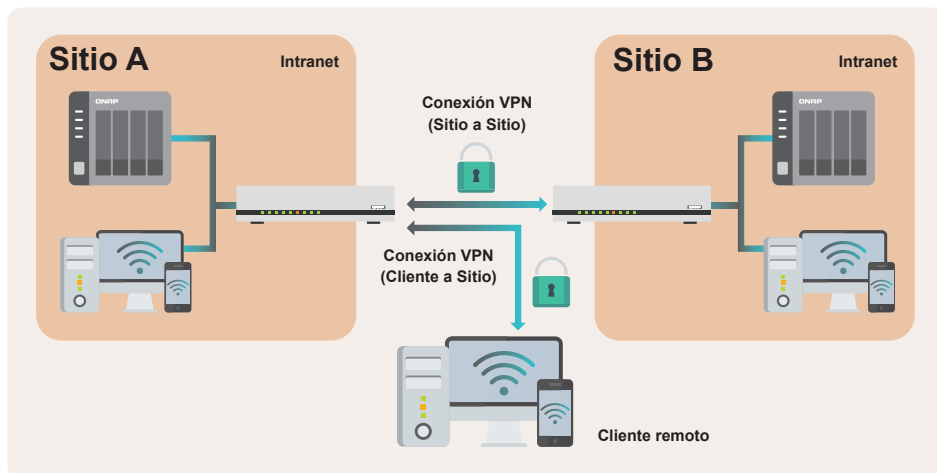
03 | Usar la conexión segura de myQNAPcloud Link

Si se usa myQNAPcloud Link para conectarse al NAS no se requiere la configuración del enrutador, ya que este puede abrir el servicio del NAS directamente a Internet. myQNAPcloud Link establecerá una conexión a través de un servidor de retransmisión o tecnología punto a punto (P2P) según el entorno de red. Toda la conexión se cifrará para garantizar la seguridad.



04 | Usar productos de VPN Sitio a Sitio o SD-WAN

A diferencia de la función de servidor VPN (VPN Cliente a Sitio) mencionada anteriormente, VPN Sitio a Sitio o SD-WAN establece una conexión VPN cifrada segura entre dos o más enrutadores en diferentes ubicaciones. En pocas palabras, los dispositivos en una red VPN Sitio a Sitio se pueden conectar entre sí como si estuvieran en la misma intranet, lo que resulta ideal para usuarios con múltiples ubicaciones. Con VPN Sitio a Sitio, podrá acceder a su NAS desde cualquier lugar.



Puede elegir el método de conexión que más le convenga según la tabla de comparación. QNAP tiene múltiples soluciones de conexión segura para satisfacer las necesidades de los usuarios.

Método de conexión	Ventajas	Desventajas	Usuarios adecuados
Habilitar y configurar el enrutador DMZ/ Reenvío de puertos de UPnP	<ul style="list-style-type: none">La conexión más rápida	<ul style="list-style-type: none">Vulnerable a ciberataquesSin defensa contra ataques a vulnerabilidades de día cero	<ul style="list-style-type: none">Tener una comprensión clara de los riesgos asociadosFamiliarizado con la configuración de la redHaber creado múltiples copias de seguridad para los datos importantesTener un plan de recuperación ante desastres
Habilitar el servidor VPN en el enrutador*	<ul style="list-style-type: none">Relativamente sencillo de configurar	<ul style="list-style-type: none">Sin notificación de errores de inicio de sesión, bloqueo automático y función de firewallSe admiten menos protocolos VPNRendimiento limitado por el hardware del enrutador	<ul style="list-style-type: none">No familiarizado con la configuración de redNo importa la velocidad de transmisión
Habilitar la función de servidor VPN en QNAP NAS*	<ul style="list-style-type: none">Admite múltiples protocolos de VPNCompatible con cortafuegos NAS (QuFirewall)Admite la notificación de errores de inicio de sesión y bloqueo automático	<ul style="list-style-type: none">La configuración es un poco más compleja	<ul style="list-style-type: none">Familiarizado con la configuración de la redNecesidad de acceder con frecuencia a muchos archivos de Internet
 Usar la conexión segura de myQNAPcloud Link	<ul style="list-style-type: none">La más fácil de configurarAdmite el control de accesoEl NAS no tiene que estar expuesto a Internet	<ul style="list-style-type: none">Conexión más lenta	<ul style="list-style-type: none">No familiarizado con la configuración de redAcceso poco frecuente al NAS desde InternetEntorno de red donde no se puede obtener la dirección IP de WAN
Usar productos de VPN Sitio a Sitio o SD-WAN*	<ul style="list-style-type: none">Una vez configurado, los usuarios de la intranet pueden usarlo sin notar ninguna diferenciaTambién es compatible con VPN Cliente a Sitio	<ul style="list-style-type: none">Se requieren equipos adicionales	<ul style="list-style-type: none">Requiere acceso multipunto y copia de seguridad remotaRequiere aplicaciones de valor añadido

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

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

Hace referencia a enrutadores domésticos generales

01

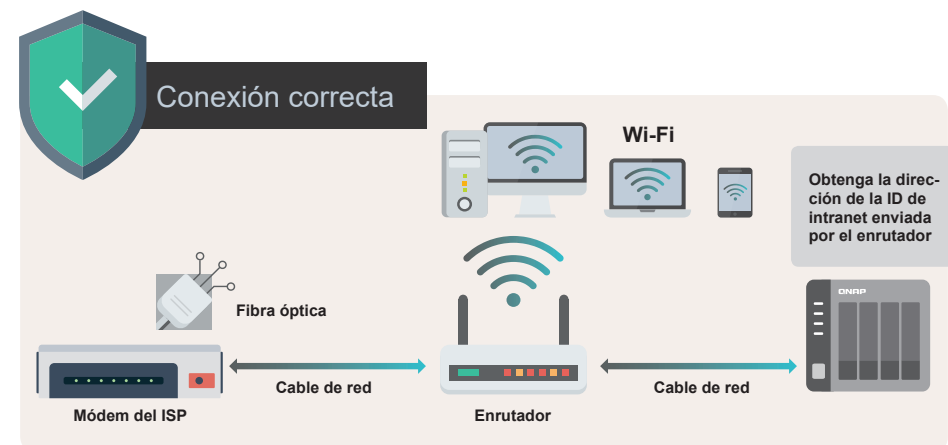
Guía de configuración de seguridad del NAS

Evite exponer el NAS a Internet

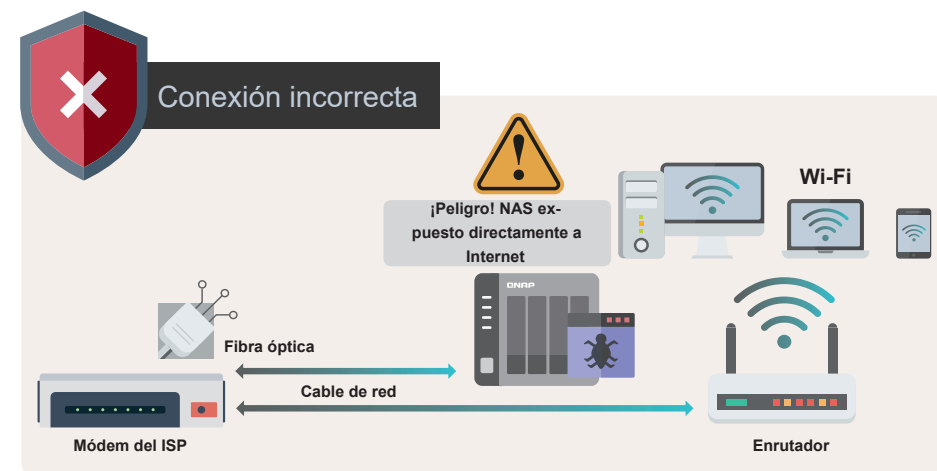


Conexión correcta del NAS

Asegúrese de que el NAS esté conectado al enrutador. Con la configuración adecuada, el enrutador puede bloquear automáticamente las conexiones de Internet, lo que permite al NAS ocultarse de Internet y evitar ciberataques.



Si conecta el NAS al módem proporcionado por el ISP, el NAS obtendrá la dirección IP WAN directamente. En este caso, cualquier persona (incluidos los hackers) puede conectarse al NAS a través de Internet e incluso intentar ataques o intrusiones.

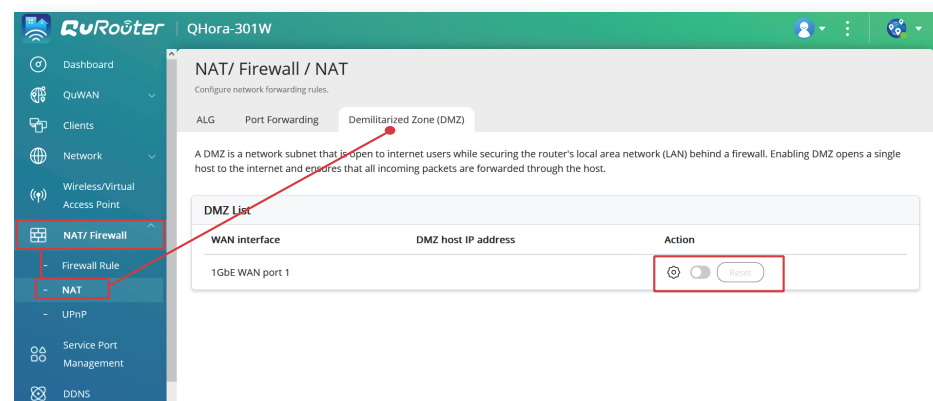
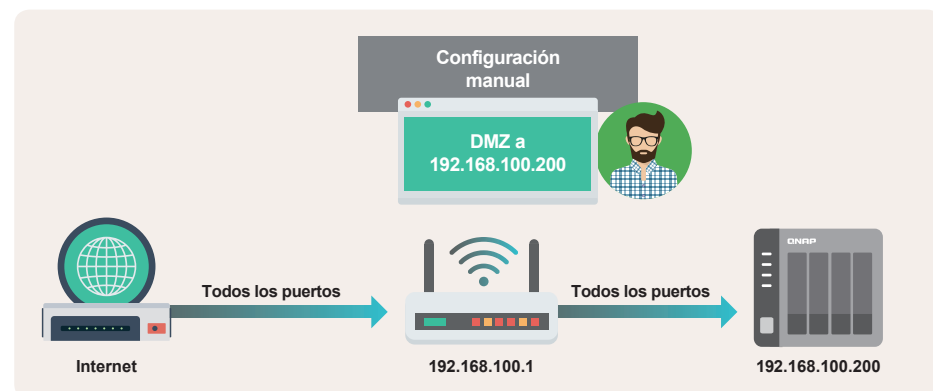


Comprobar la configuración del enrutador

De forma predeterminada, teóricamente nadie puede conectarse directamente desde Internet a su dispositivo situado detrás del enrutador, pero si habilita "DMZ (Zona desmilitarizada)", "Reenvío de puertos" o "UPnP (Universal Plug and Play)", su enrutador reenviará paquetes a su dispositivo seleccionado de acuerdo con las reglas que establezca, exponiendo así su dispositivo a Internet. Si no es necesario, debe verificar y asegurarse de que las siguientes funciones estén **deshabilitadas**.

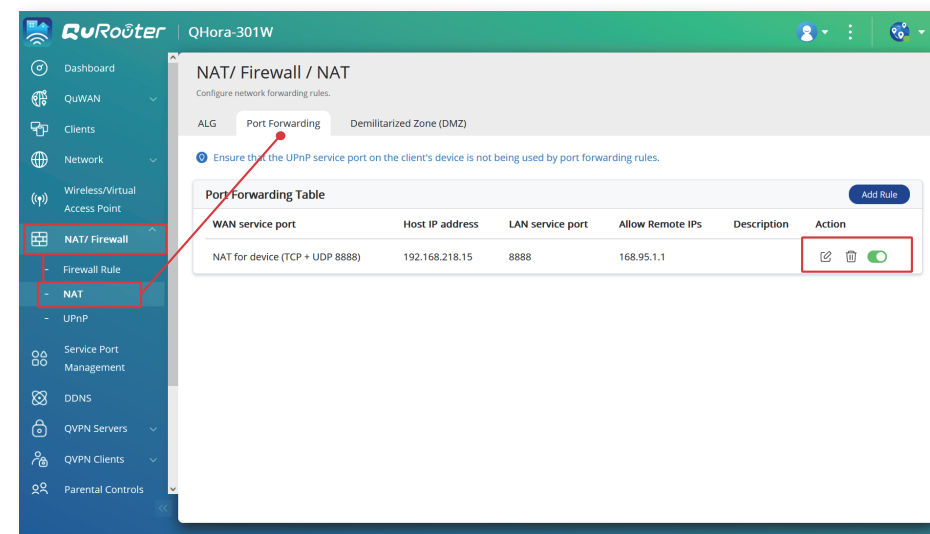
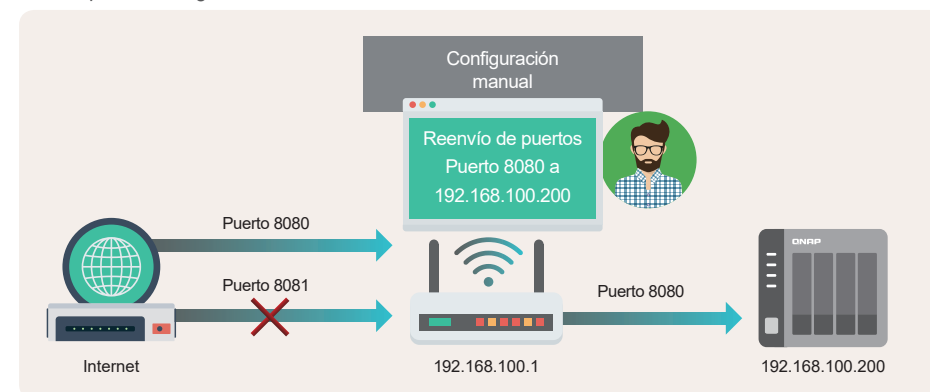
01 | Comprobar DMZ (Zona desmilitarizada)

Después de habilitar esta función, todos los puertos de servicio del dispositivo que haya seleccionado estarán directamente abiertos a Internet, es decir, completamente expuestos a Internet. Para reducir los riesgos de seguridad, deshabilite esta función.



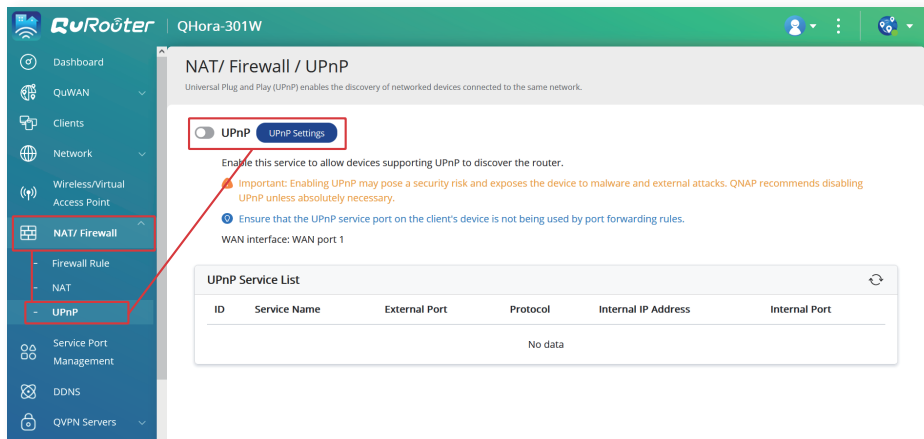
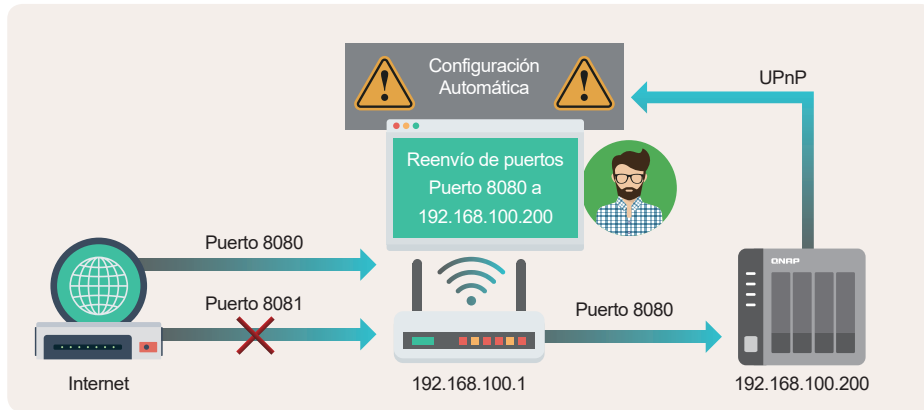
02 | Comprobar el reenvío de puertos

Esta función le permite abrir un puerto de servicio específico de un dispositivo a Internet, lo que permite que cualquier persona acceda a servicios relacionados a través de Internet. Sin embargo, los hackers también pueden lanzar ataques desde Internet contra los servicios abiertos. Por lo tanto, se recomienda deshabilitar primero todas las reglas de reenvío de puertos, luego configurar los ajustes de seguridad del NAS y posteriormente hacer una copia de seguridad de los datos importantes antes de usar esta función para abrir algunos servicios esenciales a Internet.



03 Comprobar UPnP (Universal Plug and Play)

Esta función es equivalente al reenvío automático de puertos. Después de habilitar esta función, su dispositivo puede configurar automáticamente el reenvío de puertos utilizando el protocolo correspondiente. Esta función presenta graves riesgos de seguridad, ya que puede exponer sus servicios a Internet sin su conocimiento, o ser explotada por hackers para abrir puertas traseras, por lo que debe desactivar esta función para mejorar la seguridad.



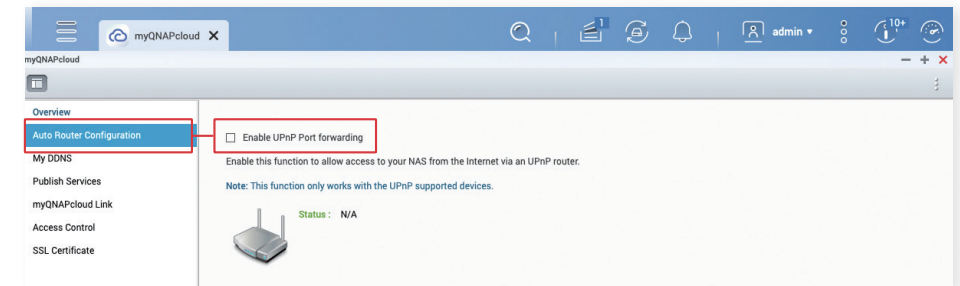
01 | Configuración automática del enrutador, reenvío de puerto UPnP

Dado que algunos enrutadores no admiten la desactivación de la función UPnP, verifique la configuración de "Configuración automática del enrutador" en el NAS al mismo tiempo para asegurarse de que esta función esté desactivada.

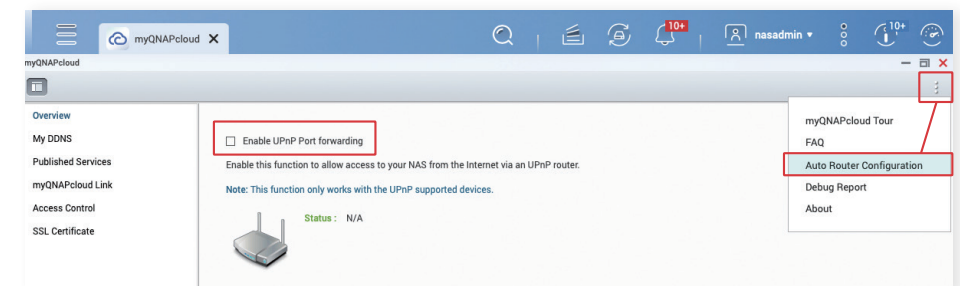
* Esta función está desactivada de forma predeterminada a partir de QTS 4.5.0/QuTS hero h4.5.3.

Para deshabilitar la función "Configuración automática del enrutador":

1. Inicie sesión en la interfaz de administración web de QTS/QuTS hero con una cuenta de administrador.
2. Abra el menú en la esquina superior izquierda de la interfaz de administración y haga clic en "myQNAPcloud".
3. **QTS 5.0.0 / QuTS hero h5.0.0 o versiones anteriores:** haga clic en "Configuración automática del enrutador" en el menú de la izquierda.



QTS 5.0.1/QuTS hero h5.0.1 o versiones posteriores: haga clic en el icono de menú en la esquina superior derecha y seleccione "Configuración automática del enrutador".



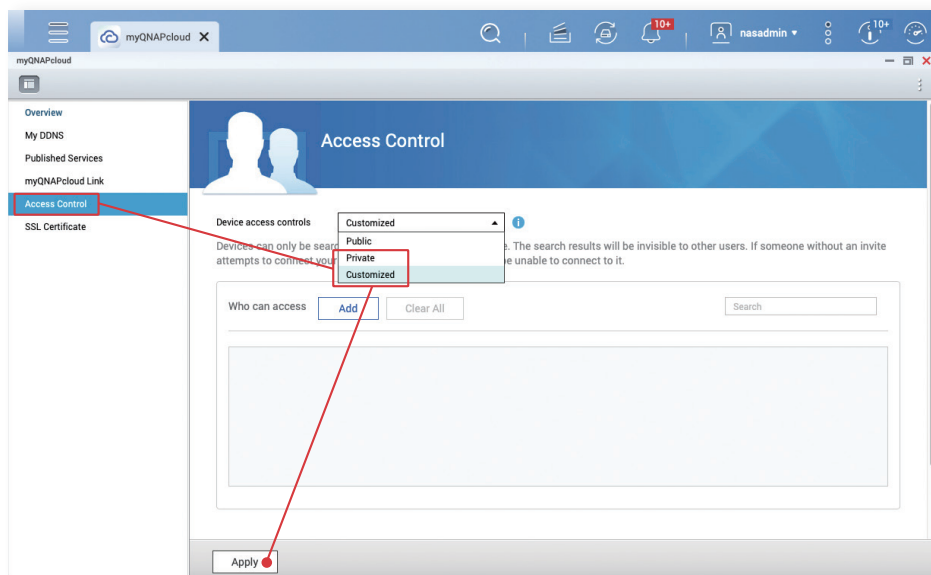
4. En la página de configuración "Configuración automática del enrutador", desactive "Habilitar el reenvío de puertos UPnP" y haga clic en "Aplicar".

02 | Control de acceso a myQNAPcloud Link

myQNAPcloud Link es un servicio en la nube de conexión segura proporcionado por QNAP. Los usuarios pueden conectarse al QNAP NAS a través del nombre de dispositivo myQNAPcloud elegido. myQNAPcloud Link proporciona ajustes de control de acceso. Cuando el control de acceso está configurado en "Público", cualquier persona que conozca el nombre del dispositivo podrá usar myQNAPcloud Link para conectarse al NAS. Por lo tanto, **recomendamos configurar el control de acceso en "Privado" o "Personalizado"**. En ambos modos, los usuarios deben iniciar sesión con su QNAP ID en la Lista de acceso permitido para poder usar myQNAPcloud Link para conectarse de forma segura a los servicios en la nube.

* La configuración predeterminada en Q TS 4.5.0/Qu TS hero h4.5.3 (o versiones posteriores) es "Personalizado"

1. Inicie sesión en la interfaz de administración web de QTS/QuTS hero con una cuenta de administrador
2. Haga clic en el menú en la esquina superior izquierda de la interfaz de administración y haga clic en "myQNAPcloud"
3. Haga clic en "Control de acceso" en el menú de la izquierda
4. En la página de configuración "Control de acceso", establezca "Controles de acceso del dispositivo" en "Privado" o "Personalizado" y luego haga clic en "Aplicar".



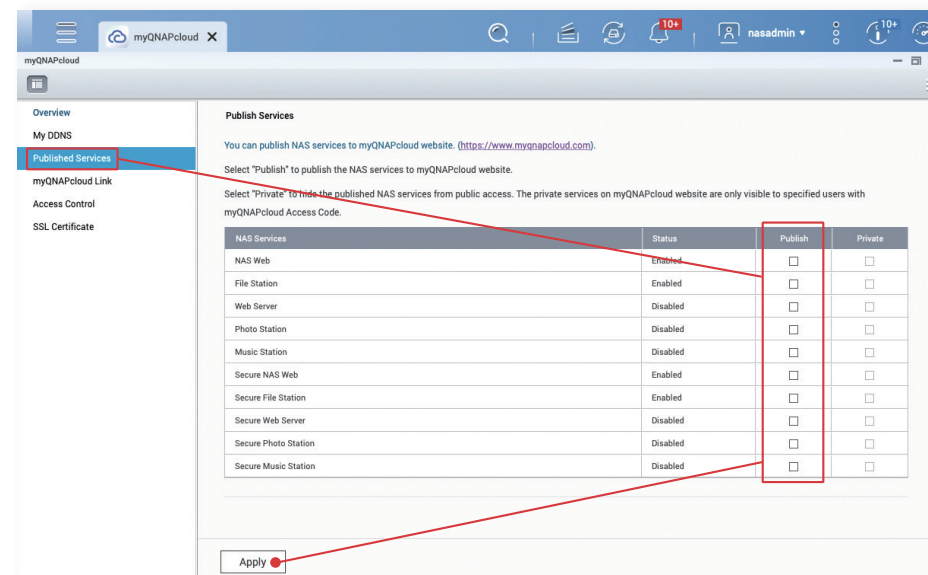
03 | Servicios publicados

Servicios publicados puede facilitar a los usuarios el uso de funciones relacionadas en el sitio web de myQNAPcloud, pero también aumentan los riesgos de seguridad. Si no necesita utilizar esta función, se recomienda desactivarla para mejorar la seguridad.

* Esta función está desactivada de forma predeterminada a partir de QTS 4.5.0/QuTS hero h4.5.3

Función "Servicios publicados":

1. Inicie sesión en la interfaz de administración web de QTS/QuTS hero con una cuenta de administrador
2. Haga clic en el menú en la esquina superior izquierda de la interfaz de administración y haga clic en "myQNAPcloud"
3. Haga clic en "Servicios publicados" en el menú de la izquierda
4. En el campo "Publicar", desactive todo y haga clic en "Aplicar".



Lista de verificación de la configuración de red

Relacionada con el hardware

- ☐ El NAS está conectado detrás de un enrutador
- ☐ El NAS obtiene la dirección IP de la intranet

Enrutador

- ☐ Deshabilite la función "DMZ" del enrutador
- ☐ Deshabilite la regla de "Reenvío de puertos" del enrutador
- ☐ Deshabilite la función "UPnP" del enrutador

NAS

- ☐ Deshabilite la función "Configuración automática del enrutador, Reenvío de puertos UPnP" del NAS
- ☐ Establezca "Control de acceso a myQNAPcloud Link" del NAS en "Privado" o "Personalizado"
- ☐ Deshabilite la función "Servicios Publicados"

Después de comprobar y aplicar la configuración anterior, el QNAP NAS no estará expuesto a Internet y los riesgos de ser atacado por hackers se reducirán considerablemente. Siga leyendo y verifique el resto de la configuración para fortalecer el QNAP NAS.

Si tiene que acceder al NAS a través de Internet, puede considerar estas tres alternativas seguras:

		
myQNAPcloud Link	QVPN Service	QuWAN SD-WAN
		
Más información	Más información	Más información

02

Guía de configuración de seguridad del NAS



Configuración de seguridad del NAS



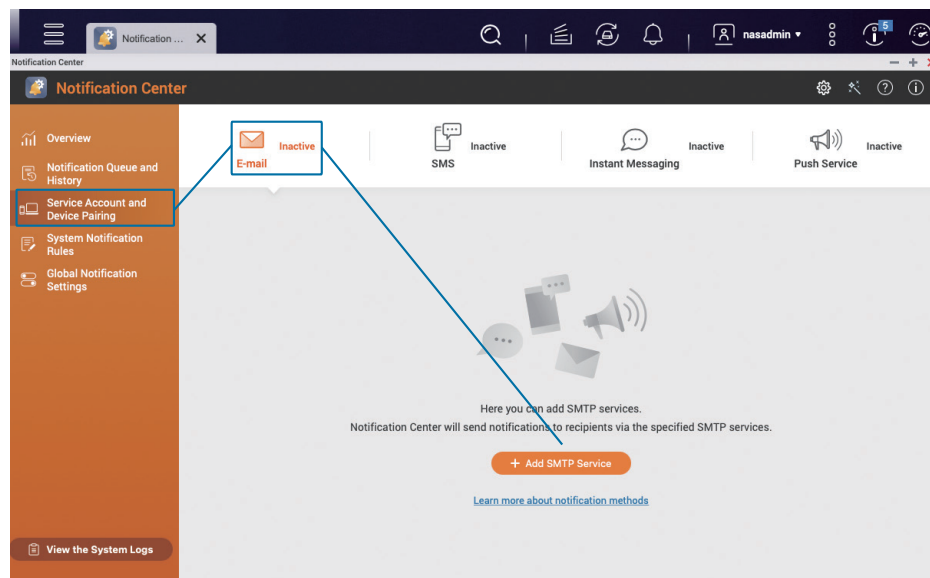
Configurar notificaciones del sistema

El Centro de notificaciones incorporado puede enviar notificaciones en función de su configuración, lo que permite a los usuarios realizar un seguimiento del estado del NAS y reaccionar ante anomalías en cuanto se detecten.

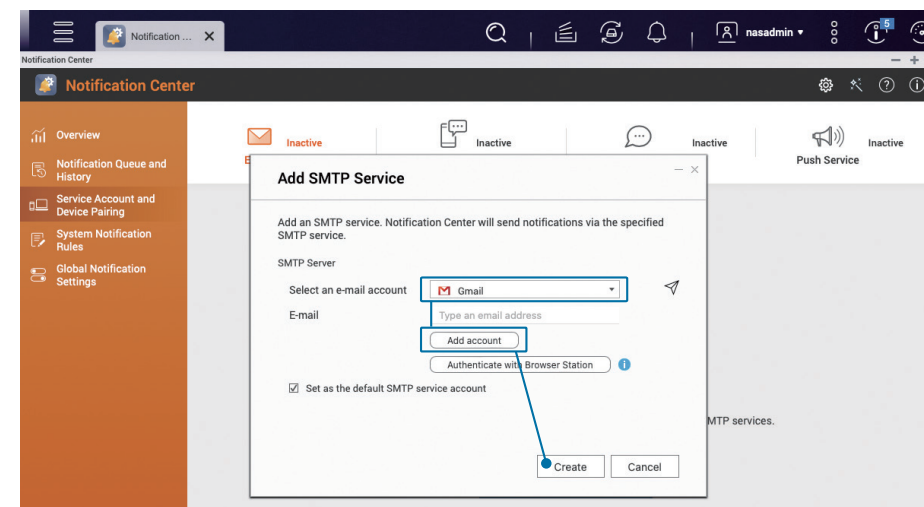
El siguiente tutorial le enseñará cómo crear dos reglas básicas para que "Correo electrónico" envíe "Notificaciones de alerta" y "Actualización de firmware", y cómo añadir más reglas si fuera necesario.

01 | Añadir el método de notificación "Correo electrónico"

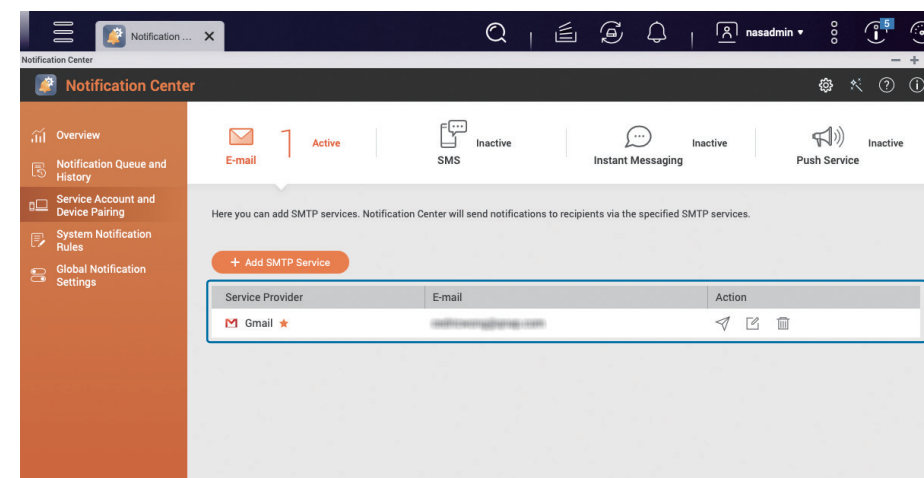
Abra el "Centro de notificaciones", haga clic en "Cuenta de servicio y sincronización de dispositivos" en el menú de la izquierda, seleccione "Correo electrónico" y luego haga clic en "Añadir servicio SMTP"



Seleccione una cuenta de correo electrónico (a continuación se usa Gmail como ejemplo), haga clic en "Añadir cuenta", siga las instrucciones para completar el proceso de verificación de Gmail y haga clic en "Crear" una vez finalizada la verificación.

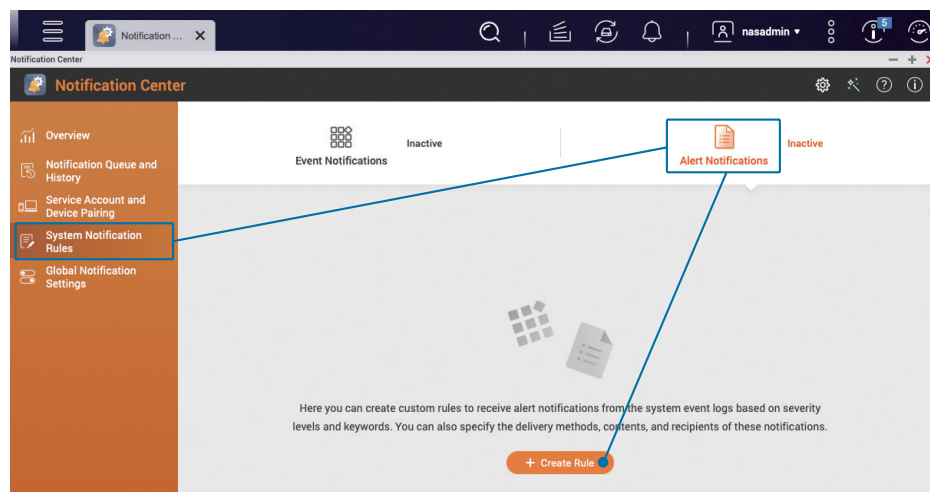


Una vez creada, verá en la lista la cuenta de correo electrónico que ha añadido.

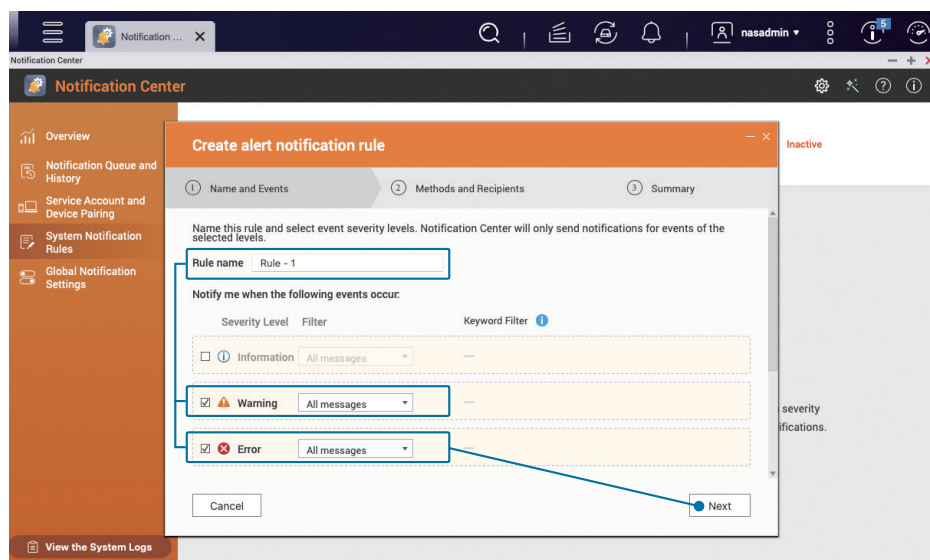


02 | Configurar "Notificaciones de alerta"

En el menú de la izquierda del "Centro de notificaciones", haga clic en "Reglas de notificación del sistema", seleccione "Notificaciones de alerta" y haga clic en "Crear regla".

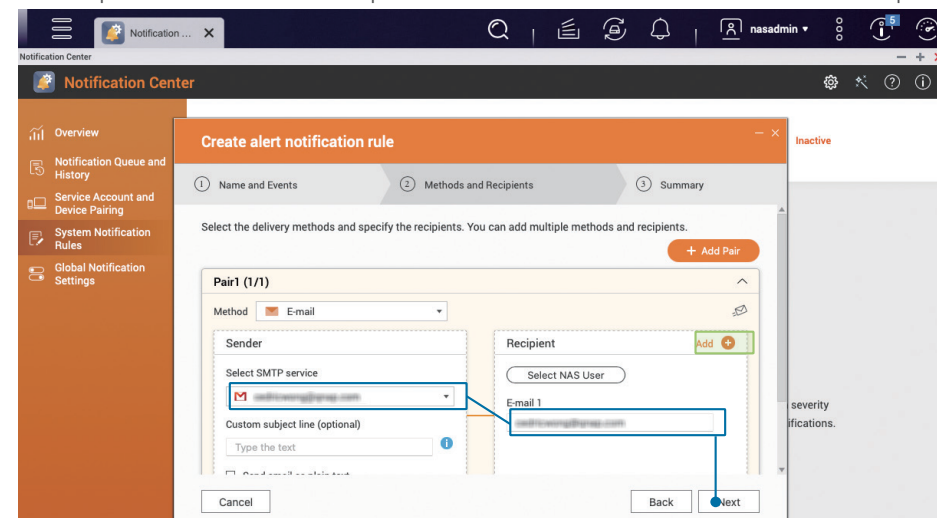


Modifique el "Nombre de la regla" según sus necesidades, verifique los dos niveles de gravedad de "Advertencia" y "Error" y haga clic en "Siguiente".

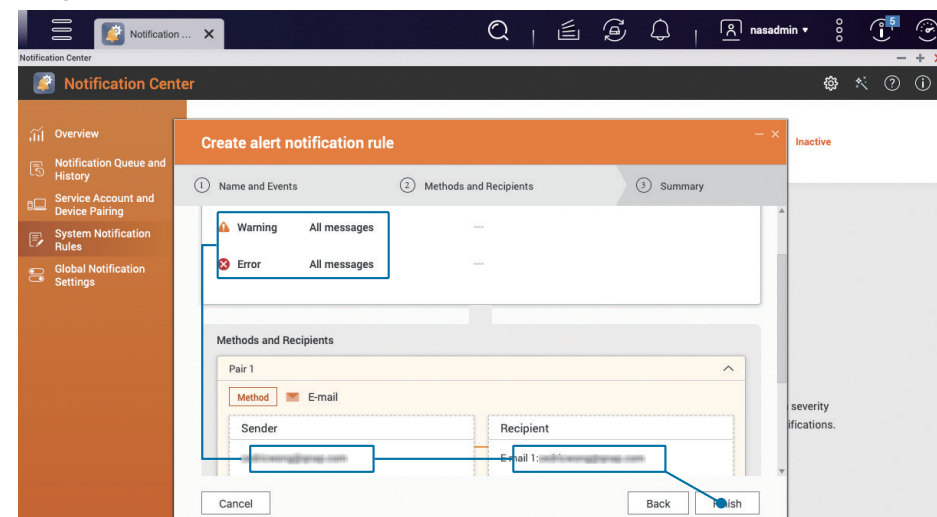


Configure el método de entrega y el destinatario, seleccione la cuenta de correo electrónico que acaba de agregar como "Remitente" en la sincronización, posteriormente introduzca la "Dirección de correo electrónico" del "Destinatario" y finalmente haga clic en "Siguiente".

Si es necesario, puede introducir varios destinatarios haciendo clic en "Añadir +" junto a "Destinatario". También puede "Añadir sincronización" para enviar notificaciones de varias maneras al mismo tiempo.

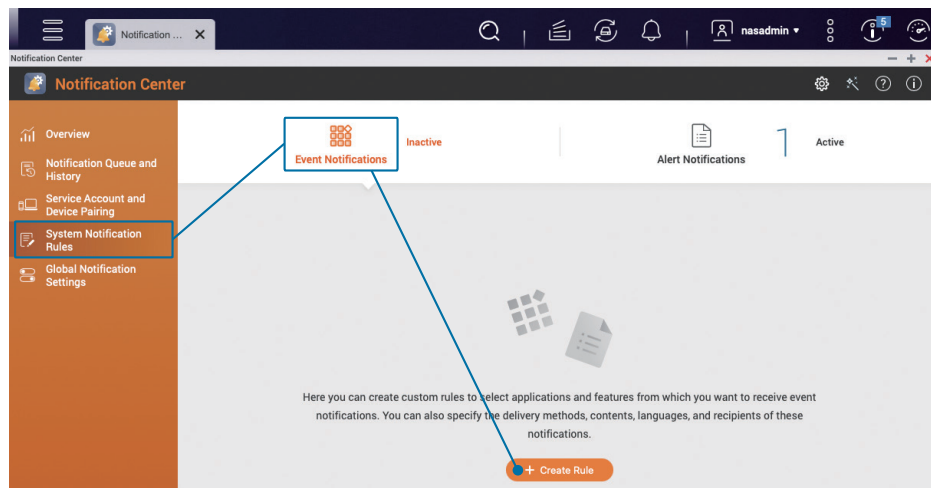


Después de confirmar que la configuración es correcta, haga clic en "Finalizar" y habrá finalizado la configuración de "Notificaciones de alerta".

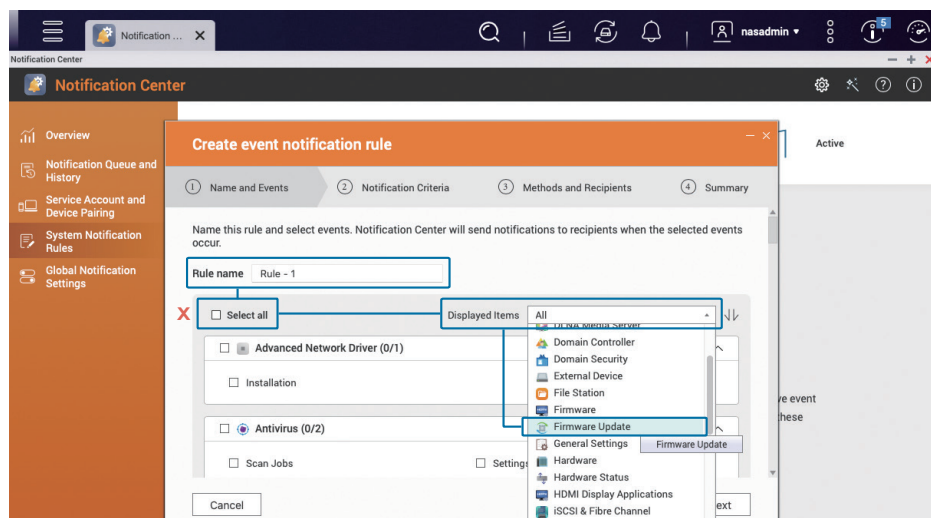


03 | Configurar notificaciones de "Actualización de firmware"

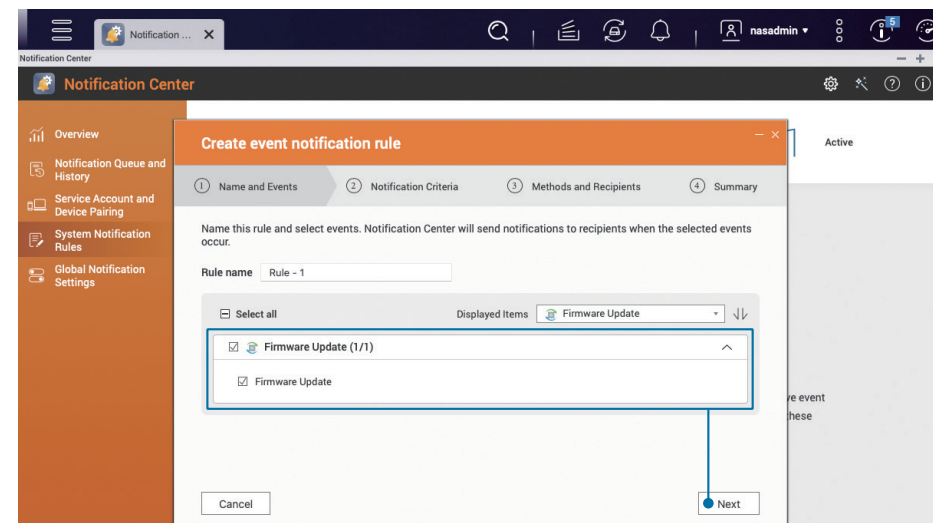
Haga clic en "Reglas de notificación del sistema" en el menú de la izquierda del "Centro de notificaciones", seleccione "Notificaciones de eventos" y haga clic en "Crear regla".



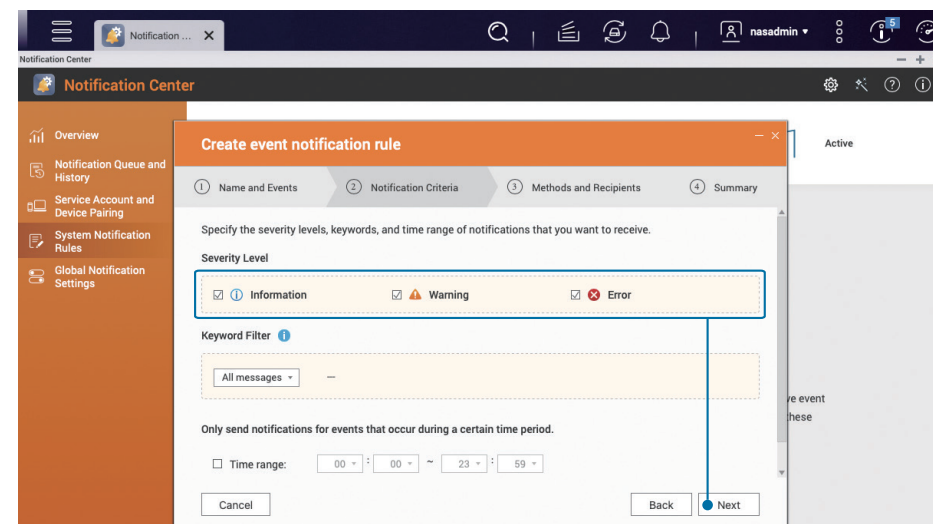
Modifique el "Nombre de la regla" según sus necesidades, desactive "Seleccionar todo", luego seleccione "Actualización de firmware" en los "Elementos mostrados" a la izquierda y finalmente seleccione la opción "Actualización de firmware" situada debajo.



Marque la opción "Actualización de firmware" y haga clic en "Siguiente".

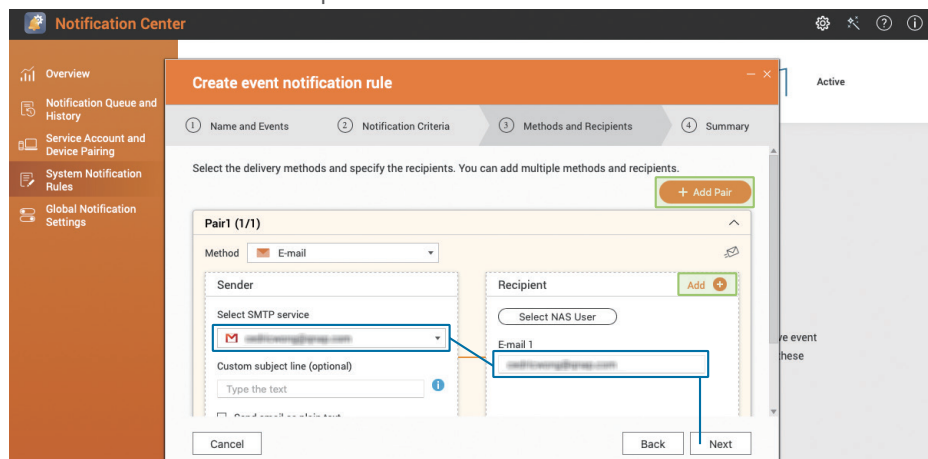


Verifique todos los niveles de gravedad, incluidos "Información", "Advertencia" y "Error"; haga clic en "Siguiente".

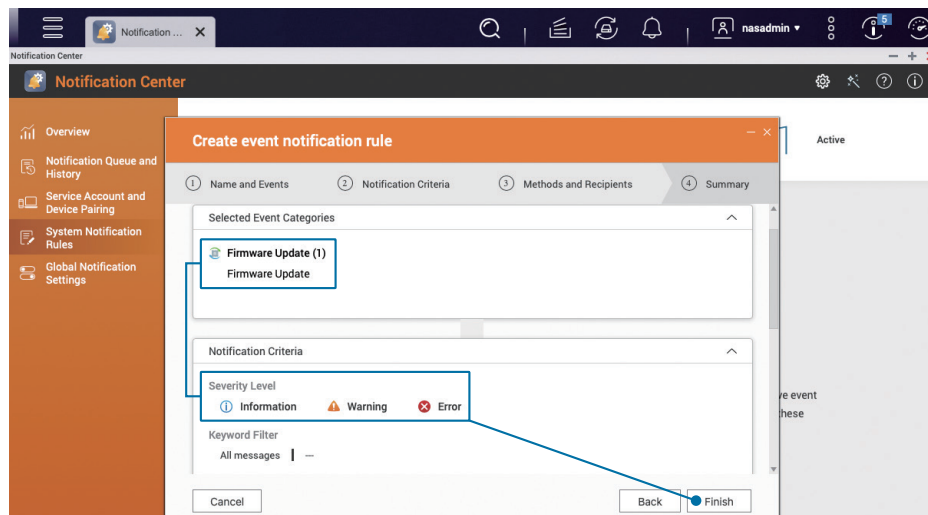


Configure el método de entrega y configure el destinatario. Dado que actualmente solo está configurada la notificación de "Correo electrónico", seleccione la cuenta de correo electrónico que acaba de agregar como "Remitente" en la sincronización, posteriormente introduzca la "Dirección de correo electrónico" del "Destinatario" y finalmente haga clic en "Siguiente".

Si es necesario, puede introducir varios destinatarios haciendo clic en "Añadir" junto a "Destinatario". También puede "Añadir sincronización" para enviar notificaciones de varias maneras al mismo tiempo.



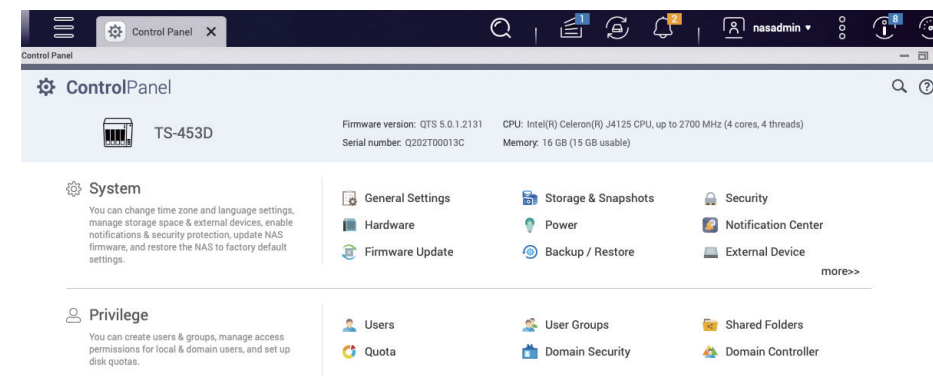
Después de confirmar que la configuración es correcta, haga clic en "Finalizar" para completar la configuración de "Actualización de firmware".



Habilitar la actualización automática de firmware (QTS/QuTS hero)

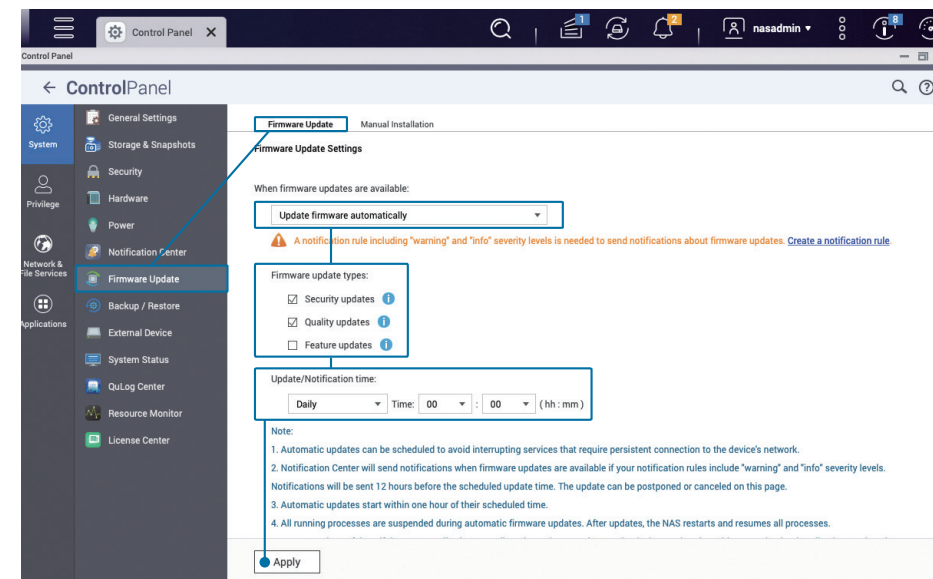
La función de actualización automática facilita la instalación de actualizaciones para nuevas funciones, correcciones de errores y vulnerabilidades.

Abra el "Panel de control" y haga clic en "Actualización de firmware".




En "Configuración de actualización de firmware", seleccione "Actualizar firmware automáticamente" y marque "Actualizaciones de seguridad" y "Actualizaciones de calidad"; para "Hora de actualización/notificación"; se recomienda establecer una hora de menor actividad, como las "00: 00". Después, haga clic en Aplicar.

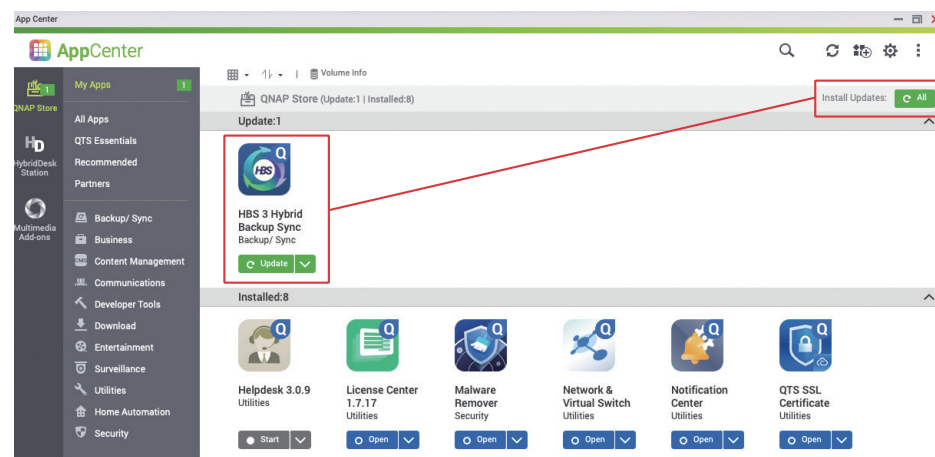
*** Para QTS 5.0.0/QuTS hero h5.0.0 (o versiones anteriores), marque "Versión recomendada" en la página "Actualización automática"**




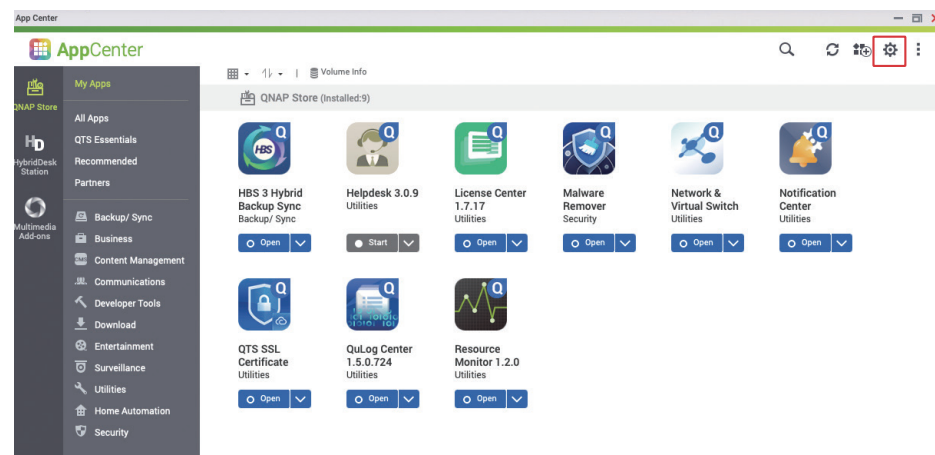
Configuración de la actualización de aplicaciones

App Center proporciona múltiples aplicaciones para agregar más funciones a su QNAP NAS, pero las aplicaciones también deben actualizarse para mejorar sus funciones, solucionar problemas y vulnerabilidades y mejorar la experiencia del usuario.

Abra "App Center" para ver si hay aplicaciones que deban ser actualizadas. Si es así, haga clic en el botón "Todo"  **All** " en la parte superior derecha para actualizar todas las aplicaciones.

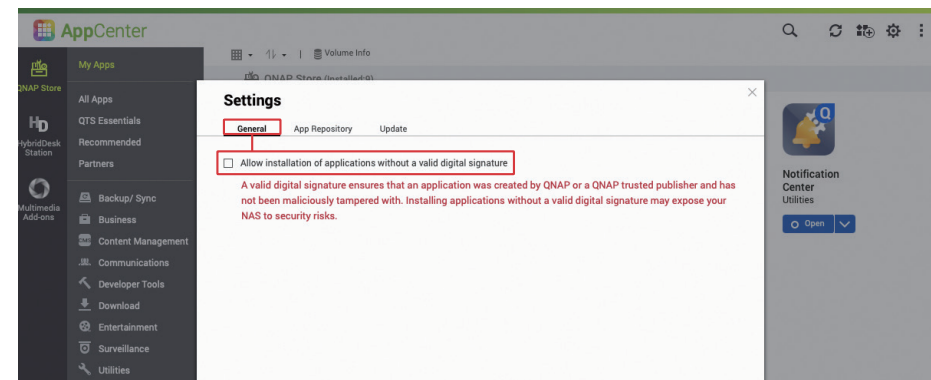


Una vez completada la actualización, haga clic en el icono "Configuración"  " en la esquina superior derecha para acceder a la página de configuración de App Center.



QNAP o los desarrolladores de confianza de QNAP agregarán una firma digital a la aplicación para garantizar que sea genuina. Se recomienda desmarcar "Permitir la instalación de aplicaciones sin una firma digital válida" para mejorar la seguridad.

*** No está marcado de forma predeterminada, lo que hace imposible instalar aplicaciones sin una firma digital válida**

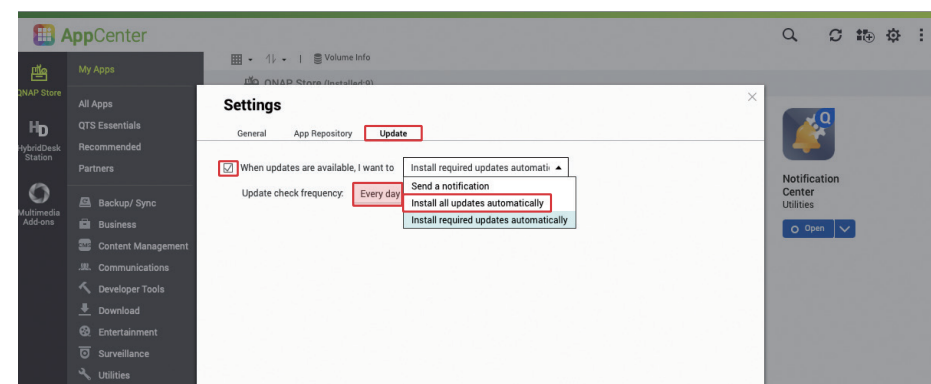


Haga clic en la pestaña Actualizar, si no hay una necesidad especial, se recomienda seleccionar "Instalar todas las actualizaciones automáticamente", establezca la frecuencia en "Todos los días" y haga clic en Aplicar para completar la configuración.

⇒ Las "Actualizaciones requeridas" se utilizan principalmente para cumplir con las dependencias de la aplicación y el firmware, y también incluirán "Actualizaciones de vulnerabilidades importantes".

⇒ "Todas las actualizaciones" incluye todas las mejoras de funciones, correcciones de errores y todos los parches de vulnerabilidad. La actualización será más frecuente.

*** La opción predeterminada es "Instalar todas las actualizaciones automáticamente"**

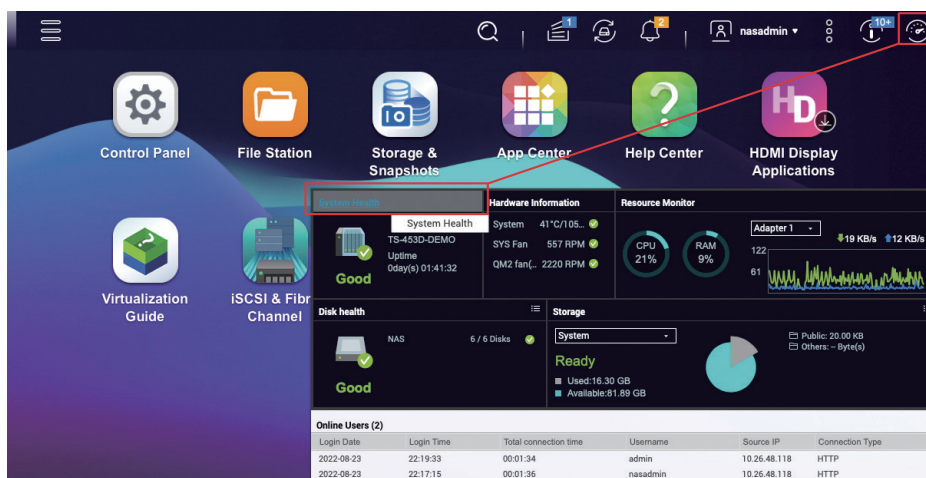


Deshabilitar o eliminar las funciones innecesarias

QNAP NAS proporciona diversas funciones y aplicaciones, pero cuantas más funciones estén habilitadas, más vectores de ataque potenciales habrá. Debe verificar y deshabilitar (o eliminar) periódicamente las funciones innecesarias para mejorar la seguridad y conseguir que el sistema funcione sin problemas.

* Para mejorar la seguridad del producto, desde **QTS 5.0.0/QuTS hero h5.0.0** en adelante, las funciones no esenciales se deshabilitan de forma predeterminada cuando se inicializa el sistema, y **App Center** no instalará ninguna aplicación no esencial de forma predeterminada. Si el sistema se inicializó antes de actualizar a **QTS 5.0.0/QuTS hero h5.0.0**, compruebe qué aplicaciones se han instalado.

Haga clic en el botón " " en la esquina superior derecha para abrir el "Panel de control" del sistema y haga clic en "Estado del sistema" para abrir la ventana "Estado del sistema".



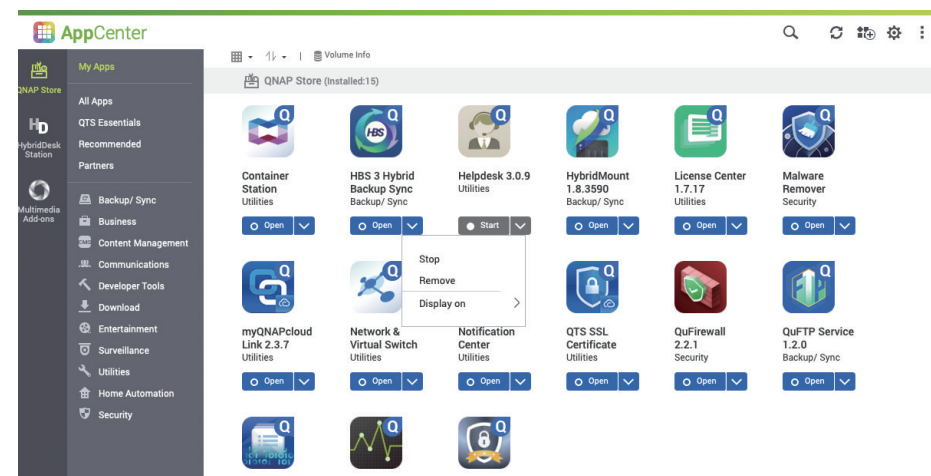
Haga clic en "Servicio del sistema" para ver las funciones habilitadas del sistema. Puede ir al Panel de control para desactivar las funciones del sistema que no necesite.

System Status

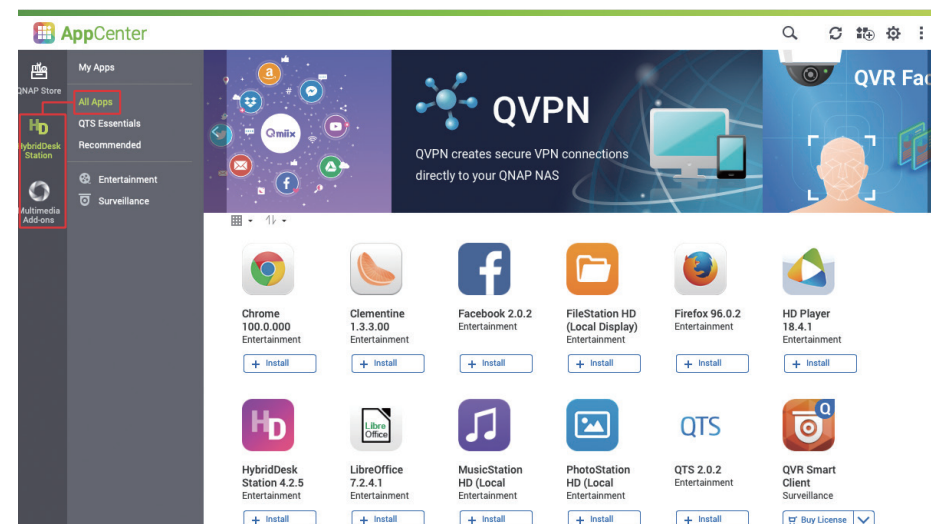
System Information Network Status **System Service** Hardware Information

Service	Status	Port	Description
Antivirus	Disabled	-	
Apple Networking	Disabled	-	
DDNS Service	Disabled	-	
Disk Management	Disabled	3260	
Domain Controller	Disabled	-	
FTP Service	Disabled	21	Maximum connections:30
LDAP Server	Disabled	-	
Microsoft Networking	Enabled	-	Server type :Standalone server Workgroup:WORKGROUP Enable WINS server:Disabled

Además de las funciones integradas del sistema, también debe verificar qué está instalado en App Center.



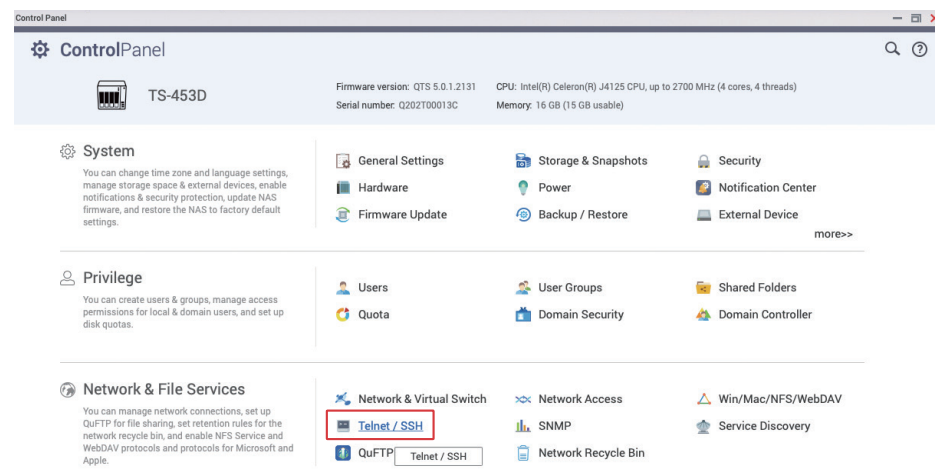
En el extremo izquierdo, haga clic en "HybridDesk Station" y "Complementos multimedia" para ver el estado de las aplicaciones correspondientes.



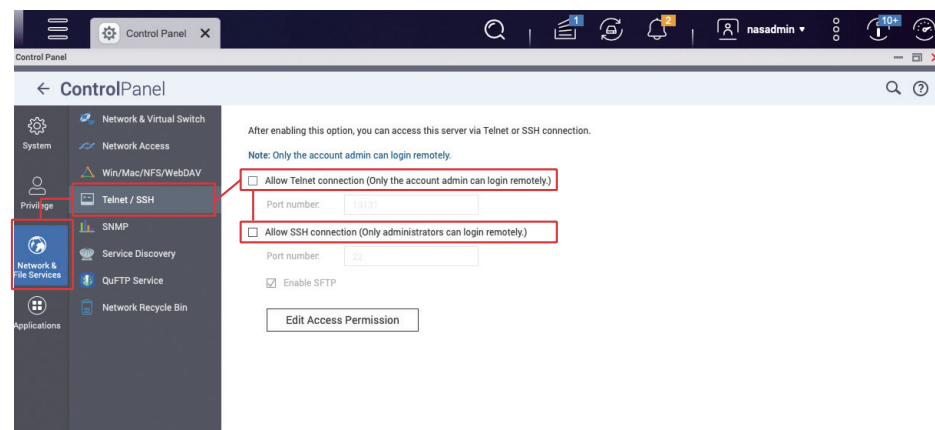
Deshabilitar Telnet/SSH

A menos que los esté utilizando, se recomienda enfáticamente **deshabilitar Telnet y SSH**. Estas dos funciones generalmente las utiliza el servicio de atención al cliente de QNAP o el personal de TI para realizar el mantenimiento del sistema. Los usuarios generales no deberían necesitarlas, por lo que se recomienda deshabilitarlas.

Abra el "Panel de control" y haga clic en "Telnet/SSH".



Desactive "Permitir conexión Telnet" y "Permitir conexión SSH" y, a continuación, haga clic en "Aplicar".

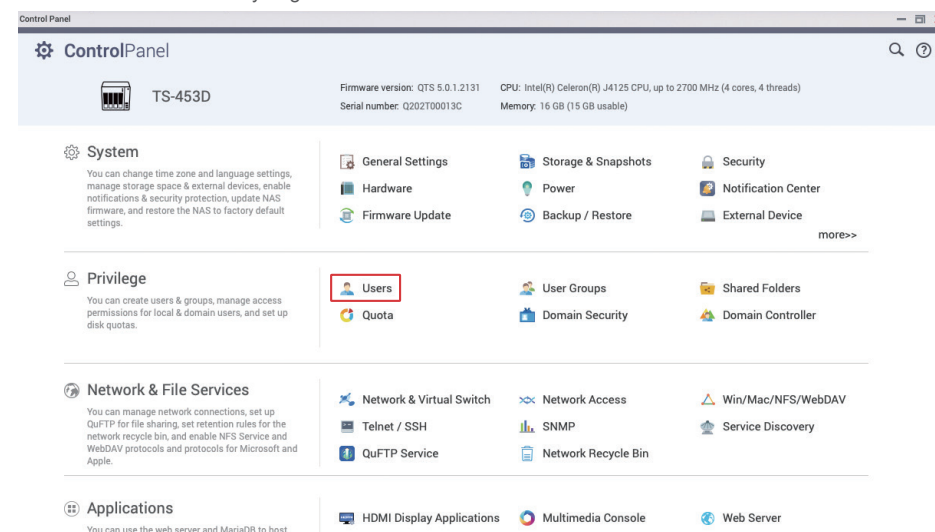


Reforzar la seguridad de las cuentas del sistema

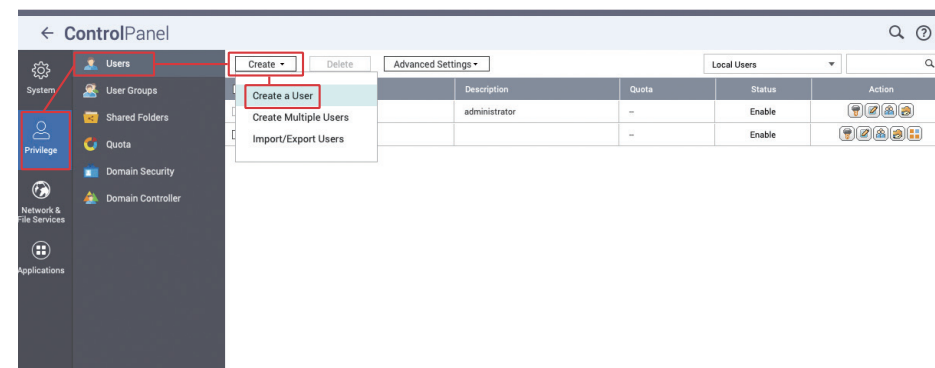
Deshabilitar la cuenta de administrador predeterminada "admin"

Los hackers que utilizan el descifrado de contraseñas por fuerza bruta generalmente se dirigen a la cuenta de administrador predeterminada "admin". Si el sistema se inicializó con QTS 4.5.4/QuTS hero h4.5.4 (o versiones anteriores), la cuenta de administrador predeterminada "admin" estará activa. Siga estos pasos para crear una nueva cuenta de administrador y deshabilitar la cuenta "admin".

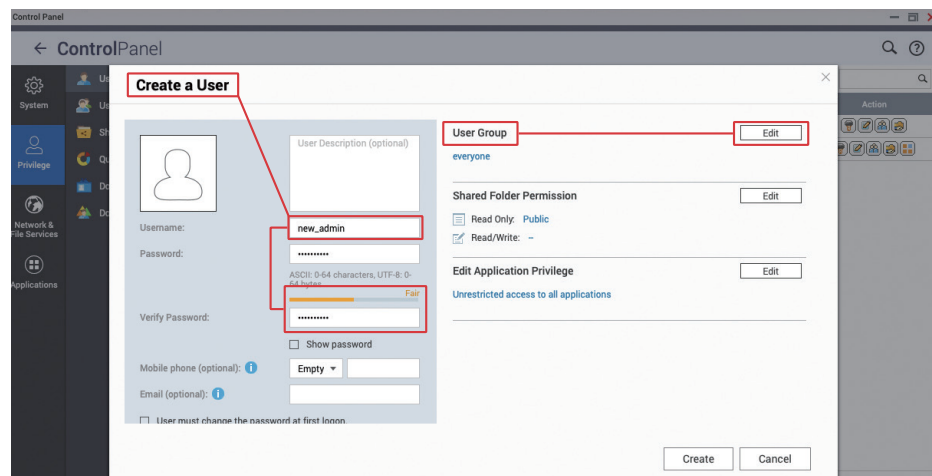
Abra el "Panel de control" y haga clic en "Usuarios".



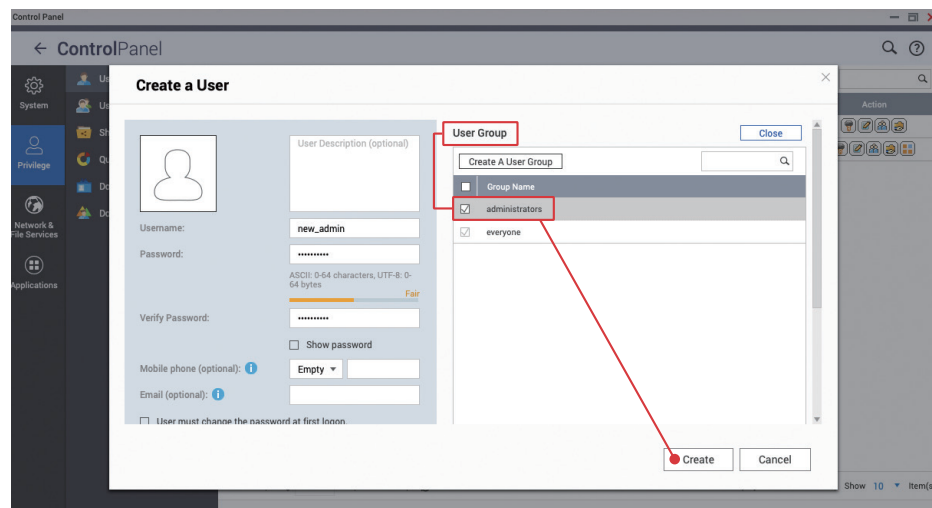
Haga clic en "Crear" > "Crear un usuario"



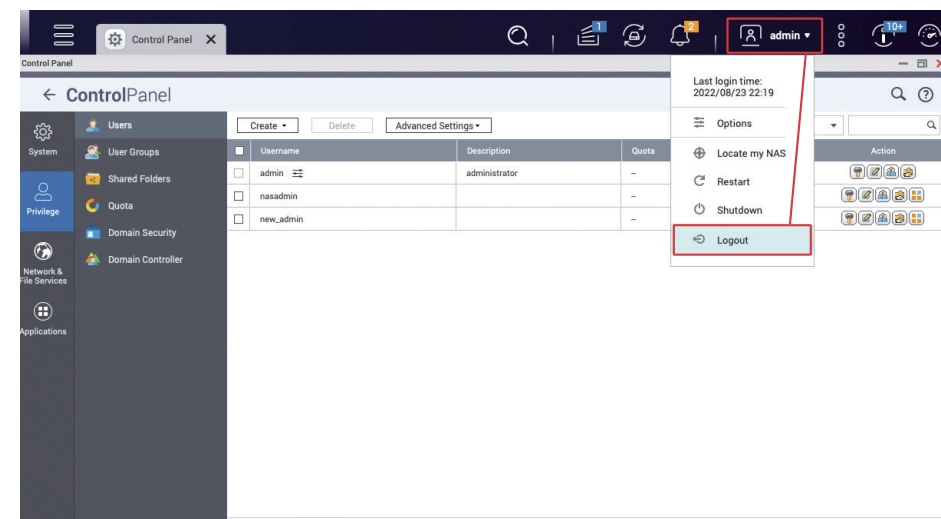
Introduzca el nombre de usuario para la cuenta de administrador, como "new_admin", y establezca una contraseña segura.



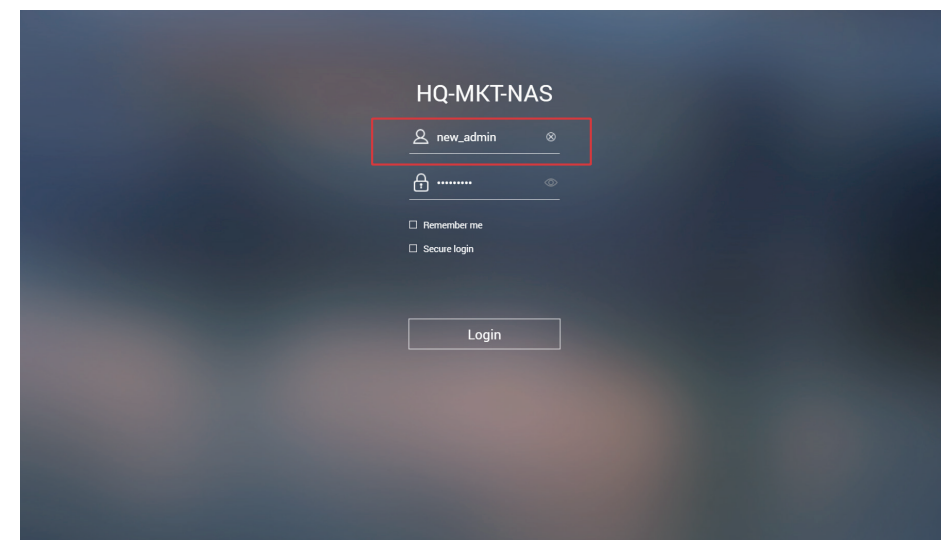
En la sección "Grupo de usuarios", haga clic en "Editar", marque el grupo "administradores" y haga clic en "Crear" para agregar un nuevo usuario.



Haga clic en "admin" en la parte superior, abra el menú y haga clic en "Cerrar sesión" para cerrar sesión en la interfaz de administración web de QTS.

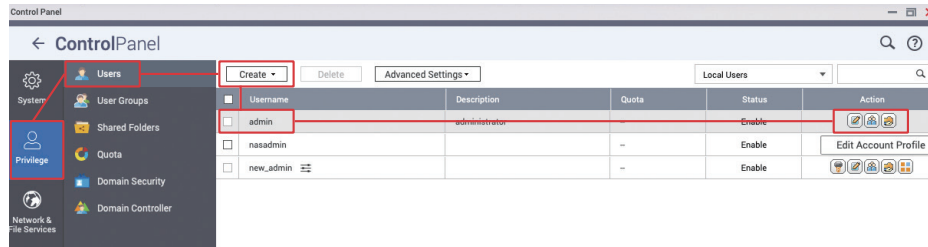


Utilice la "Cuenta de administrador" que acaba de crear para iniciar sesión en la interfaz de administración web de QTS.

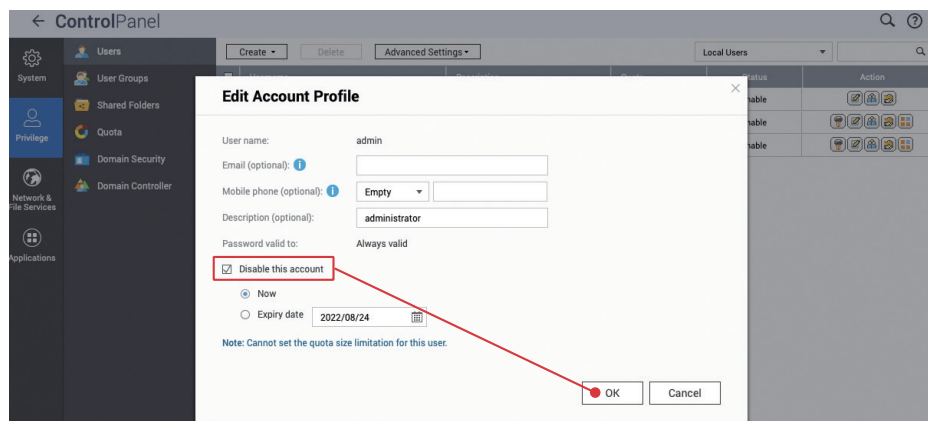


Establecer la política de contraseñas

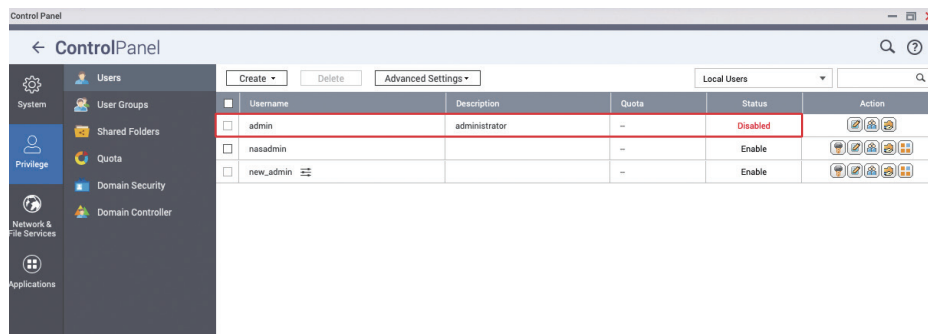
Abra el "Panel de control" nuevamente, haga clic en "Usuarios", en la fila "admin", haga clic en "Editar perfil de la cuenta"



Marque "Deshabilitar esta cuenta" y haga clic en "Aceptar" para finalizar

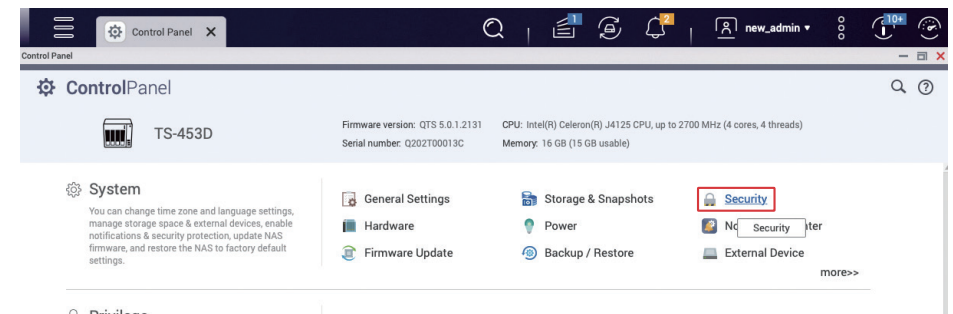


Después de completar, puede ver que el estado de "admin" es "Deshabilitado"

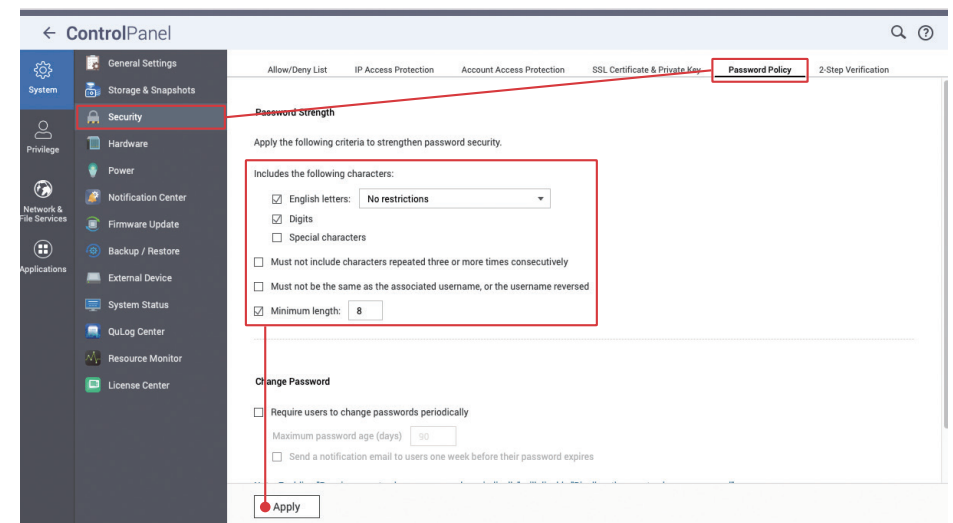


Además de deshabilitar la cuenta de administrador predeterminada "admin", también debe asegurarse de que todas las cuentas tengan contraseñas seguras. Con "Protección de acceso", puede ayudarle a bloquear los intentos de inicio de sesión maliciosos. Para mayor seguridad, puede imponer la "verificación en dos pasos (2SV)" para todas las cuentas con el fin de evitar el descifrado de contraseñas y los inicios de sesión maliciosos.

Abra el "Panel de control" y haga clic en "Configuración de seguridad"



Haga clic en "Política de contraseñas" para acceder a la página de configuración. Si el sistema se ha inicializado en QTS 5.0.0/QuTS hero h5.0.0 (o versiones posteriores), las condiciones básicas de seguridad de la contraseña están habilitadas de manera predeterminada. Puede establecer las condiciones de contraseña segura según sus necesidades. La contraseña se puede configurar para que contenga "letras mayúsculas y minúsculas" y "números", y **se recomienda que la longitud de la contraseña sea de al menos "10 caracteres"**; haga clic en "Aplicar" cuando finalice.



Habilitar protección de acceso (IP/cuenta)

La "Protección de acceso IP" y la "Protección de acceso a la cuenta" pueden ayudar a evitar que las contraseñas sean descifradas por fuerza bruta. Cuando una IP o cuenta específica no consigue iniciar sesión demasiadas veces, activará el bloqueo de IP o la desactivación de la cuenta, lo que evitará que los atacantes prueben contraseñas repetidamente.

Haga clic en "Protección de acceso de IP" para acceder a la página de configuración, verifique todos los servicios, configure el "Intervalo de tiempo", los "Intentos de inicio de sesión fallidos" y la "Duración del bloqueo de IP" según sus necesidades; a continuación, haga clic en "Aplicar" para completar la configuración.

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 [QxFirewall](#).

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

★ Si la dirección IP de un usuario normal se bloquea por error, puede ajustar la lista de bloqueo de la siguiente manera:

1. Inicie sesión en la interfaz de administración de QTS/QuTS hero desde otro ordenador
2. Cambie la dirección IP e inicie sesión en la interfaz de administración de QTS/QuTS hero
3. Inicie sesión en la interfaz de administración de QTS/QuTS hero con un navegador móvil
4. Usando la aplicación QManager

Apply

Haga clic en "Protección de acceso a cuenta" para acceder a la página de configuración, habilite los servicios relevantes, configure el "Intervalo de tiempo" y los "Intentos de inicio de sesión fallidos" según sus necesidades, y haga clic en "Aplicar" para completar la configuración.

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 la "Protección de acceso a la cuenta" está habilitada para la cuenta de administrador, existe la posibilidad de que todas las cuentas de administrador se deshabiliten debido a ataques de descifrado de contraseñas. En tal caso, la cuenta "admin" solo se puede volver a habilitar a través de la función de reinicio, y también se restablecerá la contraseña de la cuenta "admin". Recuerde cambiar la contraseña después de restablecer.

Apply

Habilitar la verificación en dos pasos (2SV)

Haga clic en "Verificación en 2 pasos" para acceder a la página de configuración; puede imponer el uso de "Verificación en 2 pasos (2SV)" para "usuarios" o para "grupos de usuarios". Se recomienda encarecidamente habilitar 2SV para las cuentas del "Grupo de administradores". Para otras cuentas, evalúe los riesgos usted mismo y aplique la configuración adecuada.

Haga clic en "Usuarios locales" para abrir el menú y seleccione "Grupos locales".

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

Marque "Aplicar 2SV" en "administradores" y haga clic en "Aplicar" para completar la configuración.

Control Panel

← ControlPanel

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

2-Step Verification

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

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

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

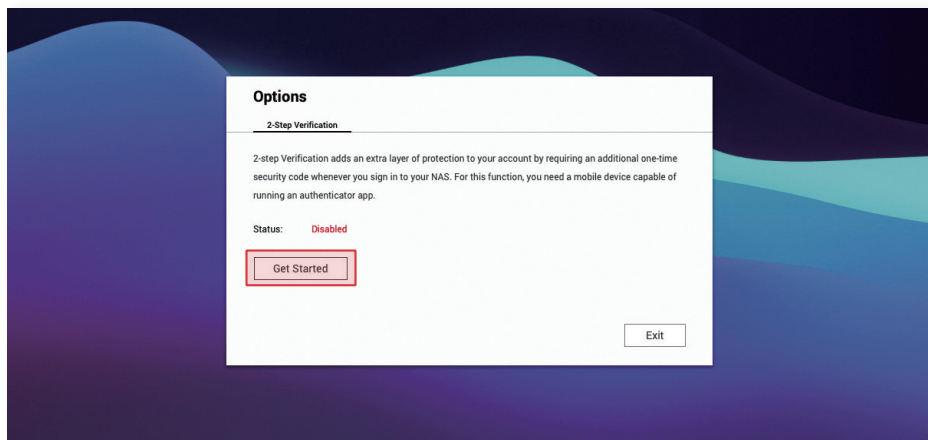
Page 1 / 1

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

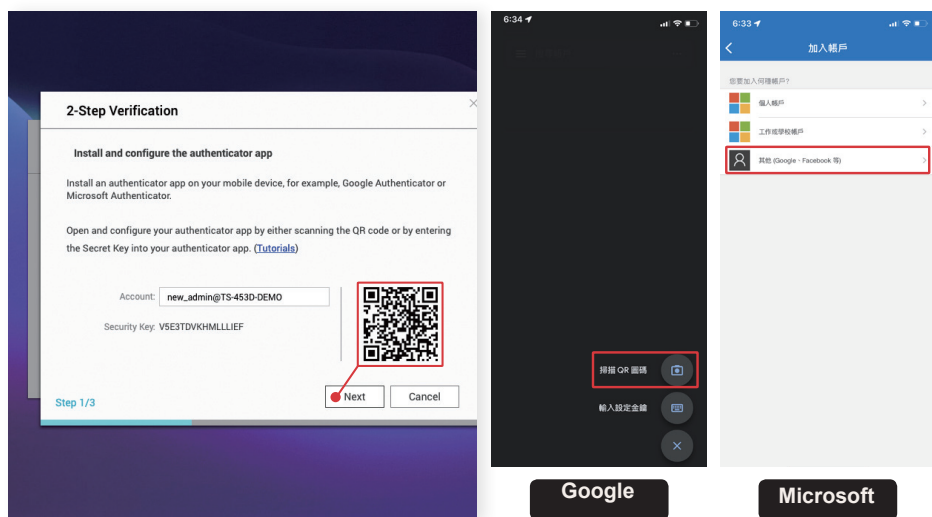
Apply

Después de habilitar "Aplicar 2SV", si la cuenta de "Administrador" no se ha configurado con "Verificación de 2 pasos (2SV)", la próxima vez que inicie sesión, se le dirigirá obligatoriamente a la página de configuración "Verificación de 2 pasos (2SV)" para configurar la cuenta.

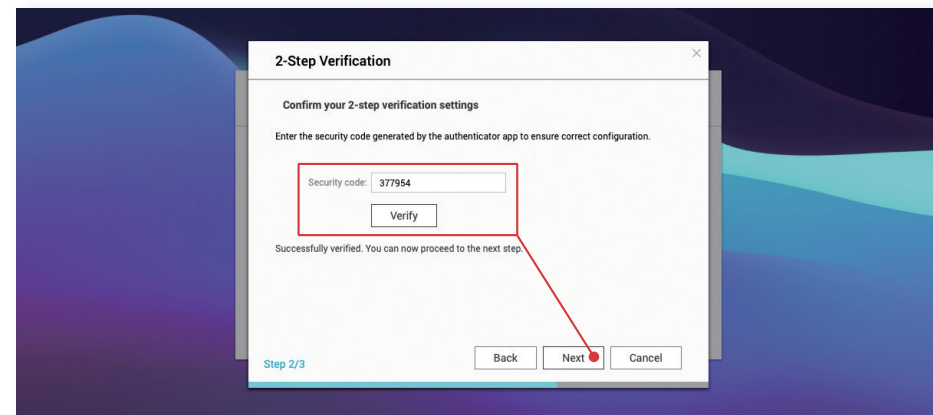
Vuelva a iniciar sesión en la cuenta de "Administrador del sistema" y haga clic en "Iniciar" para iniciar la configuración.



Instale "Google Authenticator" o "Microsoft Authenticator" en su dispositivo móvil, escanee el código QR en el programa para agregar el dispositivo y, a continuación, haga clic en "Siguiente".

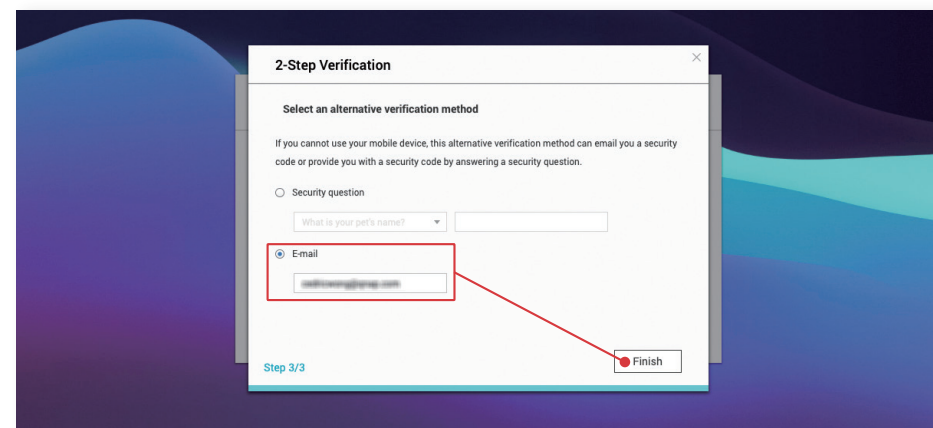


Introduzca el "Código de seguridad" de seis dígitos generado por "Google Authenticator" o "Microsoft Authenticator" y haga clic en "Verificar". Después de la verificación, haga clic en Siguiente para continuar.



Para configurar un método de verificación alternativo*, puede seleccionar "Pregunta de seguridad"*** o "Correo electrónico"***, rellenarlo y hacer clic en "Finalizar" para habilitar la "Verificación en dos pasos (2SV)".

- * Si no puede obtener el "Código de seguridad" de una aplicación de autenticación, puede recibir un "Código de seguridad" respondiendo la "Pregunta de seguridad" o usando "Correo electrónico".
- ** Responda la "Pregunta de seguridad" correctamente para superar la verificación de 2 pasos. No use preguntas y respuestas simples o fáciles de adivinar.
- *** Debe agregar el método de notificación "correo electrónico" en el "Centro de notificaciones" para usar esta función.



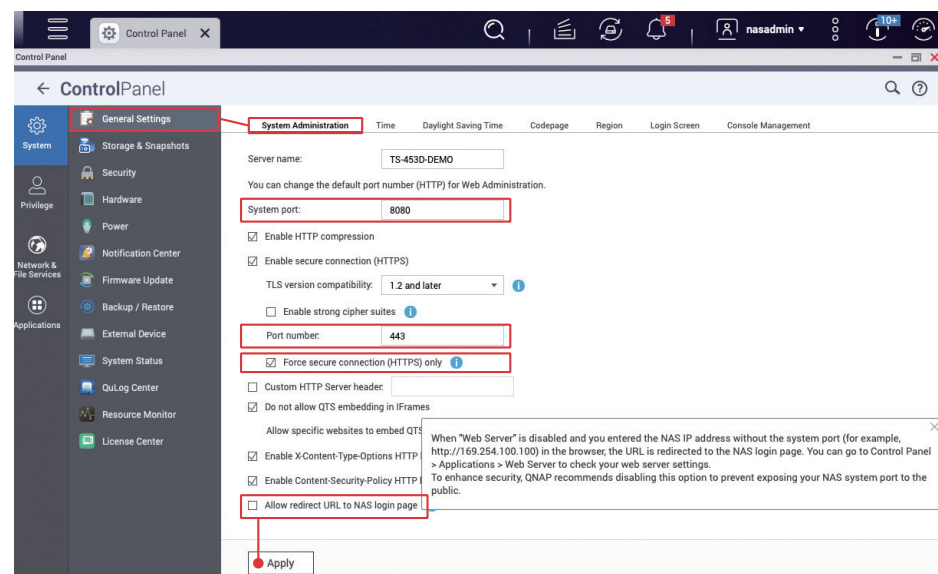
Cambiar los puertos predeterminados

Cada servicio que se ejecuta en el NAS tiene un puerto de servicio correspondiente. Salvo algunos puertos de servicio estandarizados que no se pueden modificar, el resto puede ser definido por los usuarios.

Cuando un hacker busca un objetivo de ataque, o utiliza el motor de búsqueda de IoT que suelen utilizar los hackers, generalmente se intenta primero con el puerto predeterminado. Para reducir el riesgo de ser atacado, debe cambiar los puertos predeterminados de los servicios más usados. En lo que respecta a los ataques contra el NAS, el objetivo más frecuente es el "puerto del sistema". A continuación se demostrará cómo cambiar el "puerto del sistema". Los puertos para otras funciones se pueden modificar en la página de configuración correspondiente. Por seguridad, asegúrese de modificarlos antes de usar los servicios relacionados.

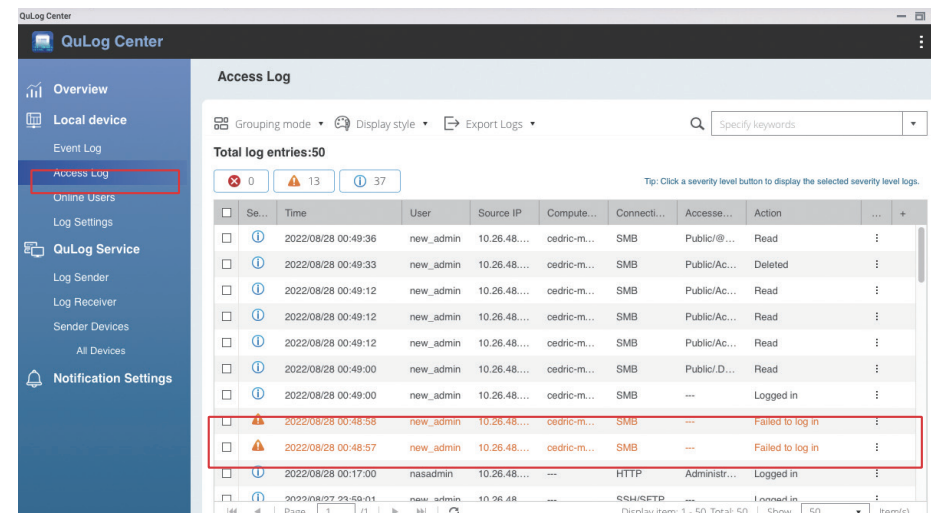
Abra el "Panel de control", haga clic en "Configuración general", el "Puerto del sistema (HTTP)" predeterminado es "8080", puede introducir un número de puerto entre 1 y 65535, como "56789"; para "Puerto del sistema (HTTPS)", es decir, el **puerto del sistema** (el valor predeterminado es "443") con la función "conexión segura" habilitada, también **se recomienda cambiarlo**. Al mismo tiempo, también **se recomienda marcar "Forzar conexión segura (HTTPS) solamente"** para garantizar que todos los usuarios transmitan datos a través de HTTPS y ayudar a evitar que los hackers intercepten información confidencial, como contraseñas de cuentas.

Además, también **se recomienda desmarcar "Permitir redirigir URL a la página de inicio de sesión de NAS"** para evitar que el "Puerto del sistema" quede expuesto debido a la redirección automática. Después del cambio, haga clic en "Aplicar" para completar la configuración.

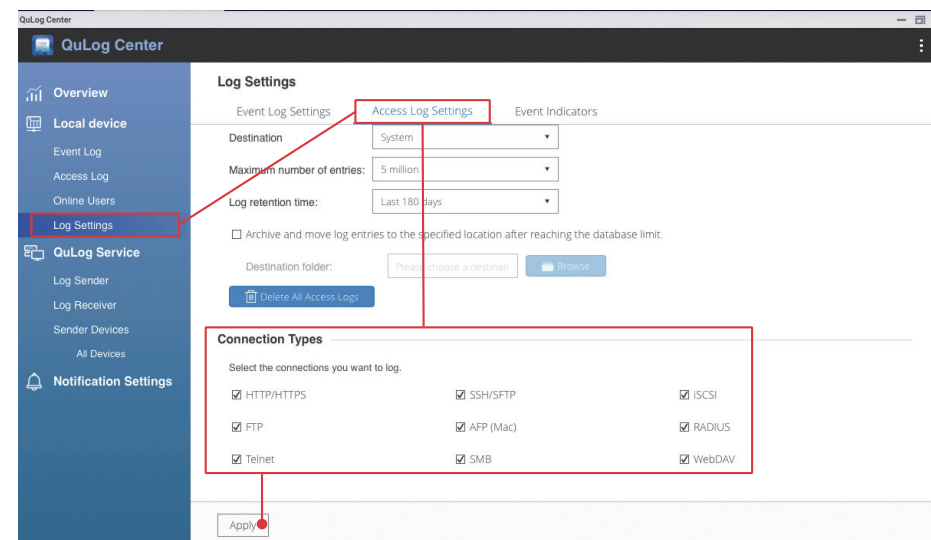


Ver registros de acceso

Los registros de acceso pueden ayudarle a ver el acceso a los archivos, las operaciones y el historial de inicio de sesión del usuario. Cuando se produce un problema, verificar los registros de acceso debe ser el primer paso para diagnosticar los problemas subyacentes.



Abra "QuLog Center", haga clic en "Configuración de registro" en el menú de la izquierda, cambie a la página "Configuración de registro de acceso", en "Tipos de conexión", verifique todas las conexiones y luego haga clic en "Aplicar" para completar la configuración.



Instalar y habilitar aplicaciones de seguridad

QNAP ofrece varias aplicaciones de seguridad para mejorar la seguridad del NAS. La configuración de estas aplicaciones puede mejorar la seguridad del NAS y aumentar la tranquilidad de los usuarios.



Security Counselor comprueba periódicamente la seguridad de la configuración del NAS y le informa sobre los riesgos potenciales.



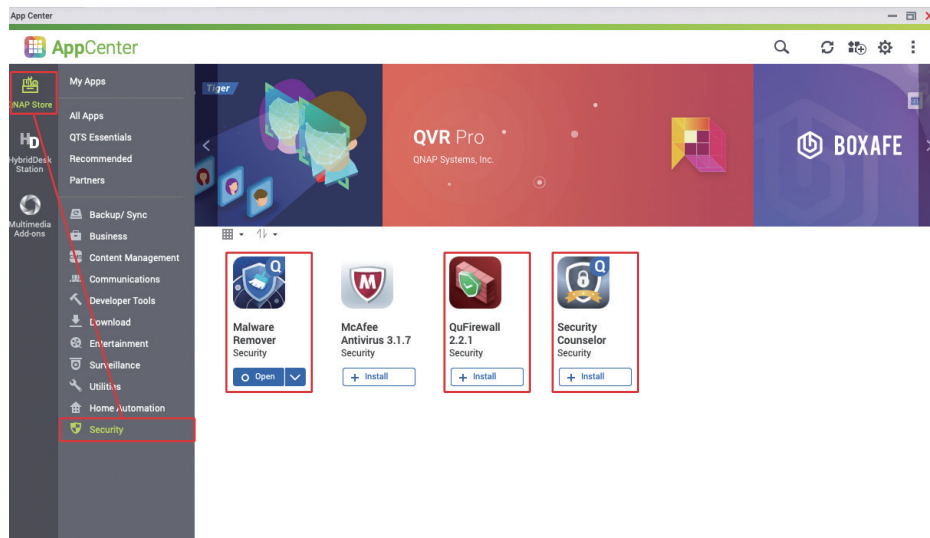
Malware Remover escanea y elimina el malware detectado del NAS.



QuFirewall proporciona funciones básicas de firewall para el QNAP NAS, bloqueando la conexión al NAS de la mayoría de los hackers.

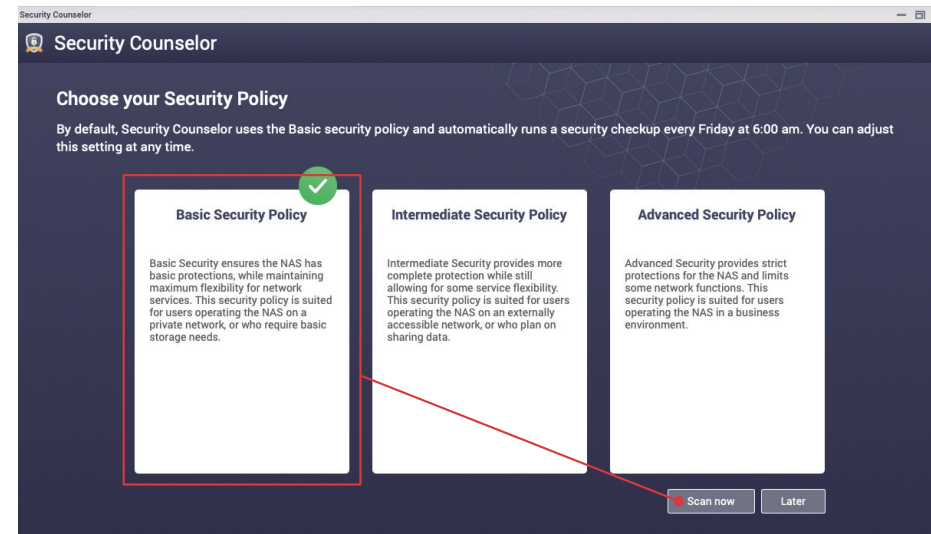
Abra "App Center", haga clic en "Seguridad" a la izquierda e instale "Security Counselor", "Malware Remover" y "QuFirewall".

★ Malware Remover está precargado en QTS 4.4.3 (y versiones posteriores) y en QuTS hero

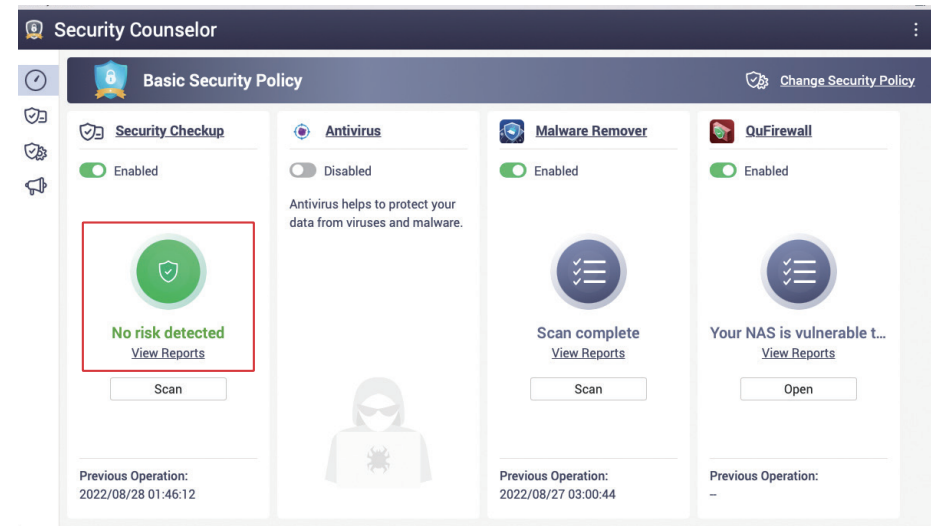


Security Counselor

Abra "Security Counselor", seleccione "Política de seguridad básica" y haga clic en "Analizar ahora".



Una vez finalizado el análisis, normalmente el resultado será "No se ha detectado ningún riesgo". Si se detecta un riesgo, haga clic en "Ver informes" para obtener detalles y siga las instrucciones para modificar la configuración.



A continuación se muestran los resultados del análisis causados por "alto riesgo", con una configuración incorrecta modificada deliberadamente. Haga clic en el "Asistente de configuración sugerida" para que le ayude a ajustar la configuración.

Security Counselor

Basic Security Policy Change Security Policy

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

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

Category	Status	Risk	Result	Action
Account	❌	High	Either this setting is deselected in the Password Policy screen or the current required mini...	⋮
Update	✅	High	The	⋮
Account	✅	High	The	⋮
Network	✅	High	The	⋮
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.	⋮

El "Asistente de configuración sugerida" indica las sugerencias relevantes. Después de leer y confirmar, haga clic en "Aplicar sugerencia" y el sistema aplicará automáticamente la configuración relevante. Algunas configuraciones deben modificarse manualmente; haga clic en la pestaña "Manualmente" a la izquierda y ajuste la configuración como se sugiere. Después de aplicar los cambios, el análisis se reiniciará automáticamente. Puede verificar los resultados del análisis nuevamente para asegurarse de que no se hayan detectado riesgos de seguridad en el 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

Haga clic en "Comprobación de seguridad" a la izquierda para acceder a la pantalla de resultados del análisis y, a continuación, haga clic en "Programación de análisis" a la derecha para abrir la pantalla de configuración del programa de análisis.

Security Counselor

Basic Security Policy Change Security Policy

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

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

Category	Status	Risk	Result	Action
Update	✅	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.	⋮

Se recomienda configurar "Programación de análisis" **al menos una vez al mes**, para que el sistema pueda verificar periódicamente la configuración y el estado del sistema. Si se detecta un riesgo y el Centro de notificaciones está configurado correctamente, recibirá una notificación para que pueda ser atendida lo antes posible.

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

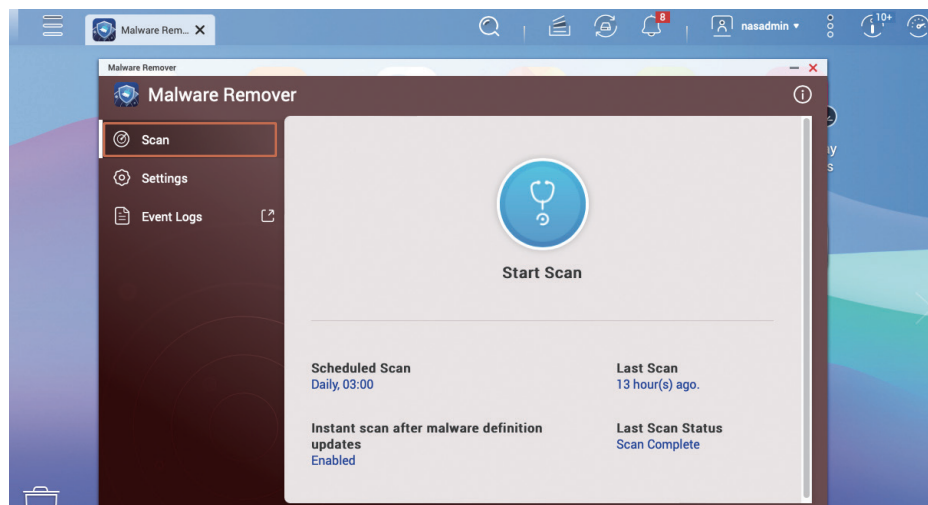
☒ Enable schedule

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

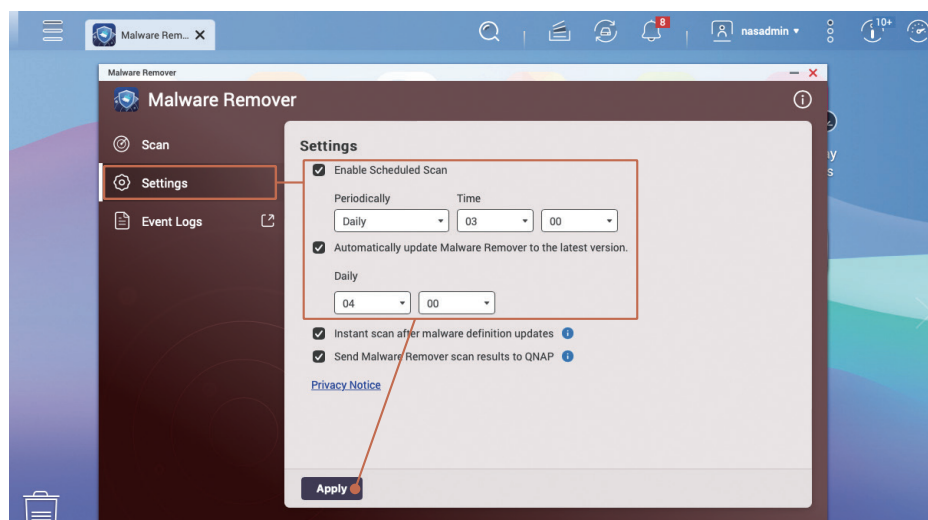
Apply Cancel

Malware Remover

Abra "Malware Remover". Se muestra el estado del último análisis; haga clic en "Configuración" a la izquierda.

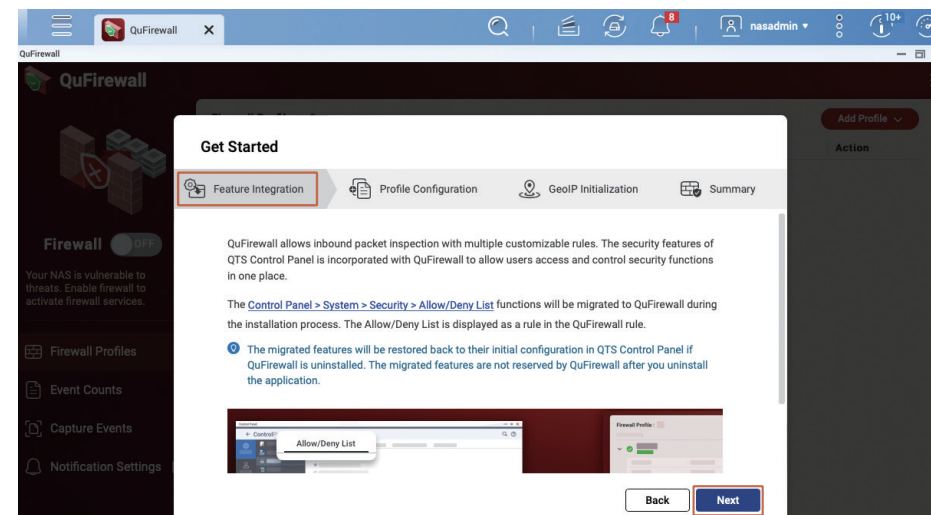


Se recomienda configurar "Programación de análisis" **una vez al día**, para que "Malware Remover" verifique periódicamente el estado del sistema. Asegúrese también de que "Actualizar el Malware Remover automáticamente a la última versión" permanezca marcado.

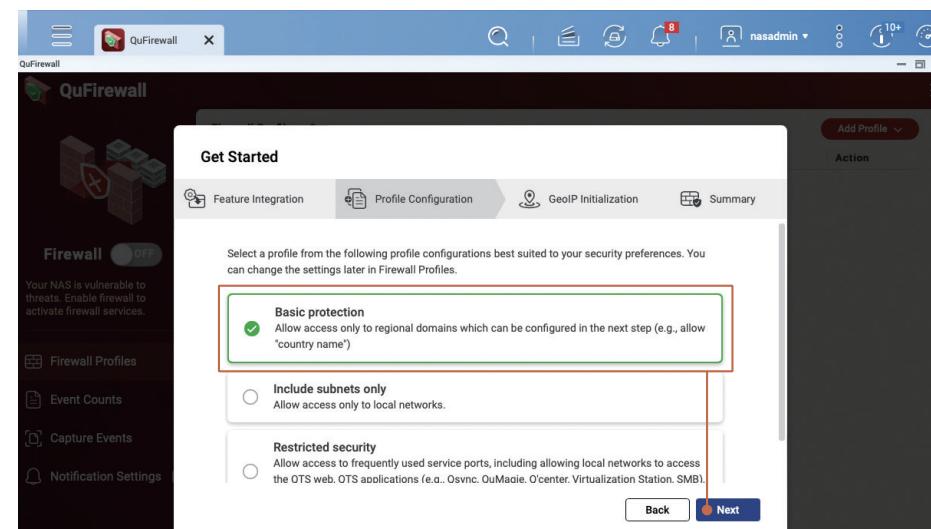


QuFirewall

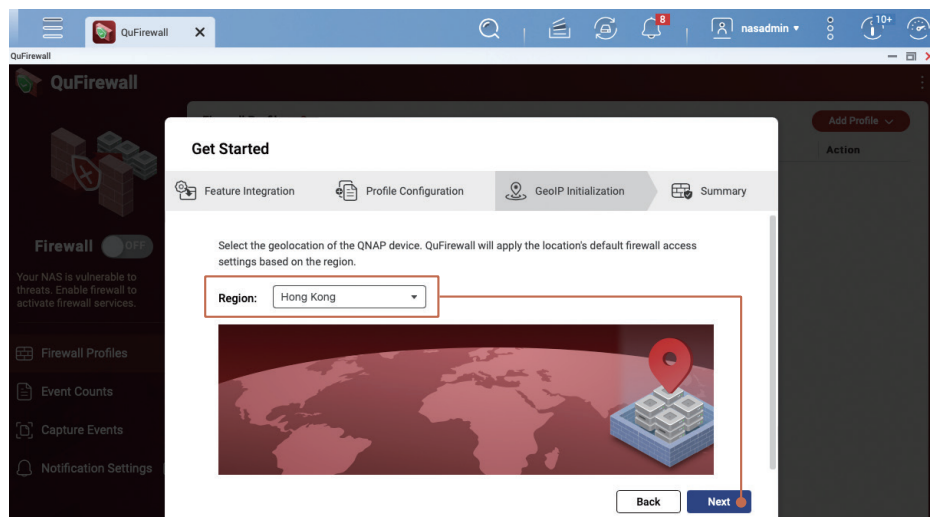
Abra "QuFirewall". Si esta es la primera vez que usa QuFirewall, se muestra la pantalla Iniciar. Después de leer, haga clic en "Siguiente" para continuar.



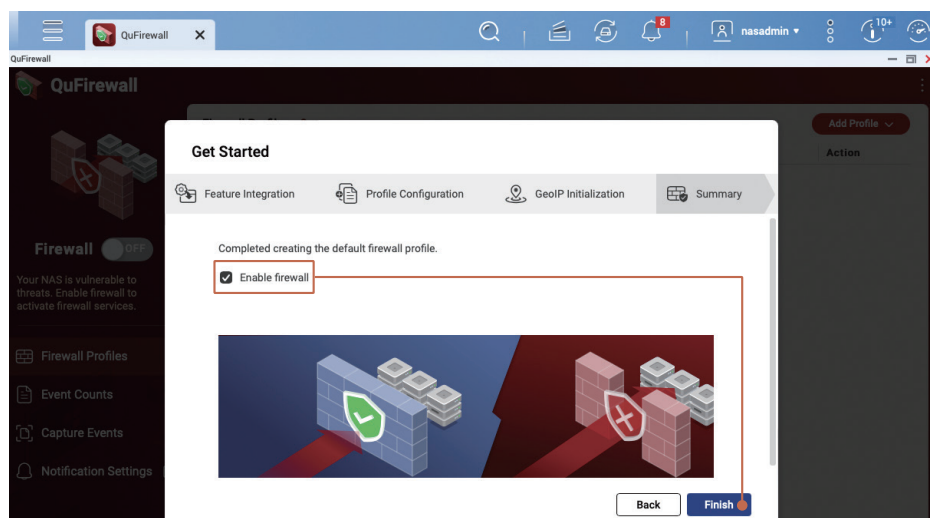
Si su red no tiene necesidades especiales, se recomienda seleccionar "Protección básica" y luego hacer clic en "Siguiente" para continuar.



Establezca una región según su ubicación. Por ejemplo: si se encuentra en Taiwán, seleccione "Taiwán"; si se encuentra en Hong Kong, seleccione "Hong Kong"; si se encuentra en Macao, seleccione "Macao". Puede agregar más regiones más tarde. Haga clic en "Siguiente" para continuar.

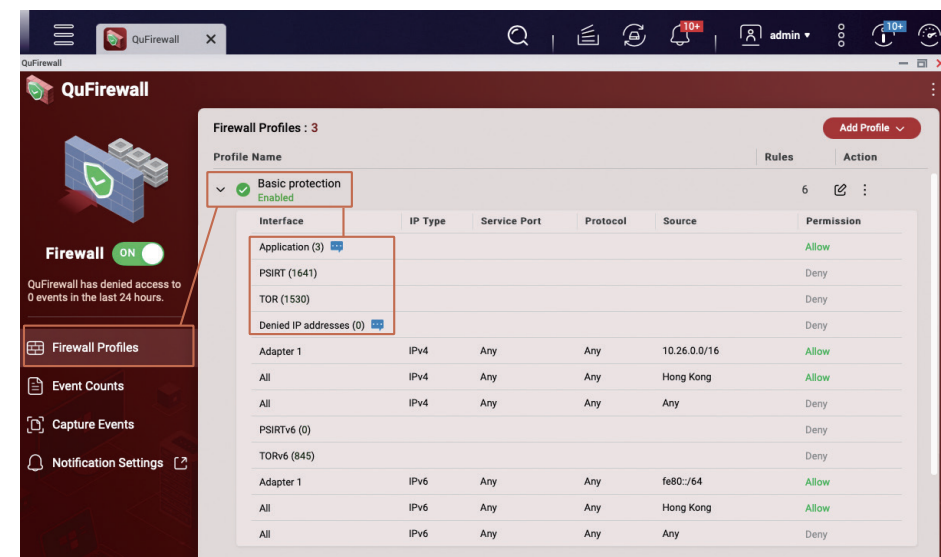


Marque "Habilitar firewall" y, a continuación, haga clic en "Finalizar" para aplicar la configuración y habilitar el firewall.




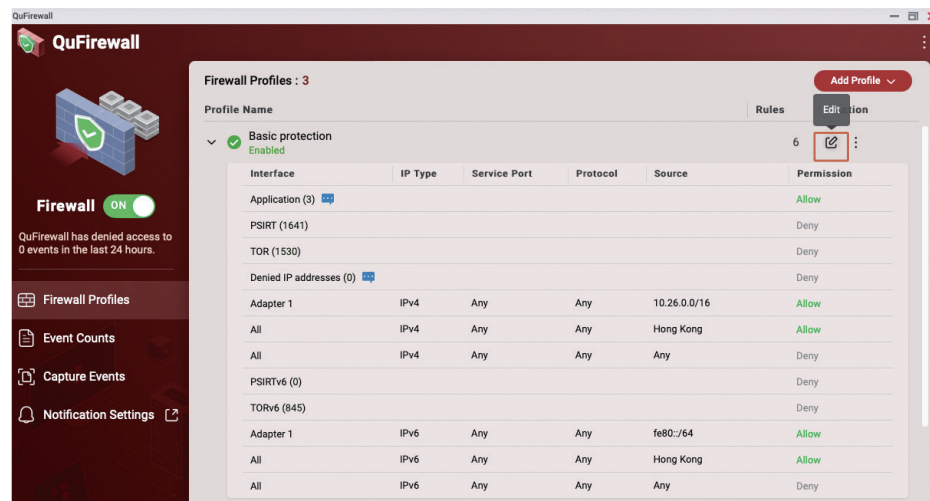
Vaya a la página Perfiles de QuFirewall y verá que la "Protección básica" está habilitado. Haga clic en "Protección básica" para expandir y ver las reglas de firewall correspondientes. Las reglas se comparan con la información de los paquetes entrantes, que pueden pasar o bloquearse de acuerdo con las reglas del firewall. Las reglas del cortafuegos se ejecutarán en secuencia. Si no se cumplen las condiciones, se comprobará la siguiente línea de reglas. Si no se cumplen, caerán en la última regla "denegar todo" y el cortafuegos bloqueará las conexiones relevantes.

- Las reglas de "aplicación" son creadas por el sistema para garantizar que el sistema funcione correctamente.
- La regla "PSIRT" es una lista negra compilada por QNAP PSIRT. Contiene direcciones IP que se sabe que atacan el QNAP NAS.
- La regla "TOR" se utiliza para bloquear las conexiones de la red TOR. La red TOR es ampliamente utilizada por los delincuentes debido a su anonimato y bloquearla puede reducir el riesgo de ser atacado.
- Las "Direcciones IP denegadas" son direcciones IP bloqueadas por la función "Protección de acceso de IP" o la lista negra agregada manualmente por el usuario.

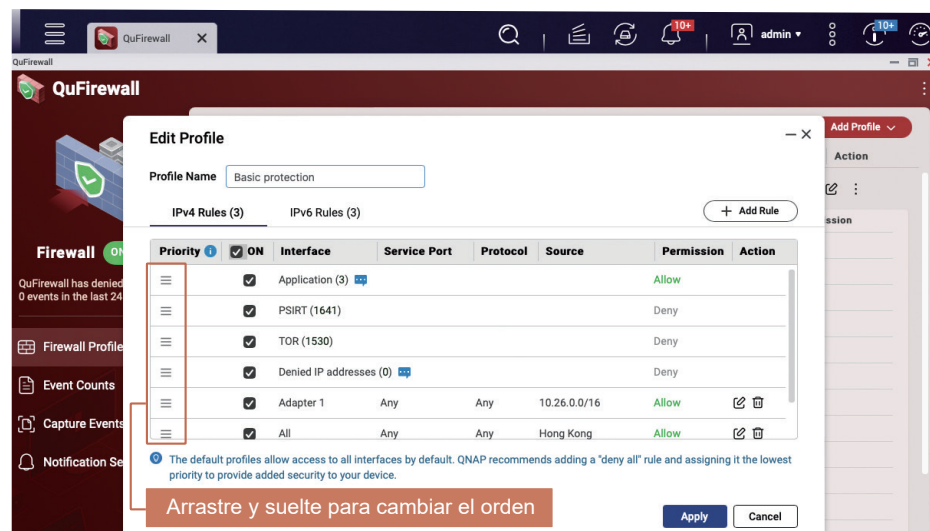


El usuario puede personalizar otras reglas y, en la configuración de protección básica, solo se "permitirán" las conexiones a Internet desde la misma intranet y desde la misma región. QNAP recomienda **usar el concepto de "lista blanca" para administrar sus reglas personalizadas** para limitar estrictamente las direcciones IP que pueden conectarse al NAS.

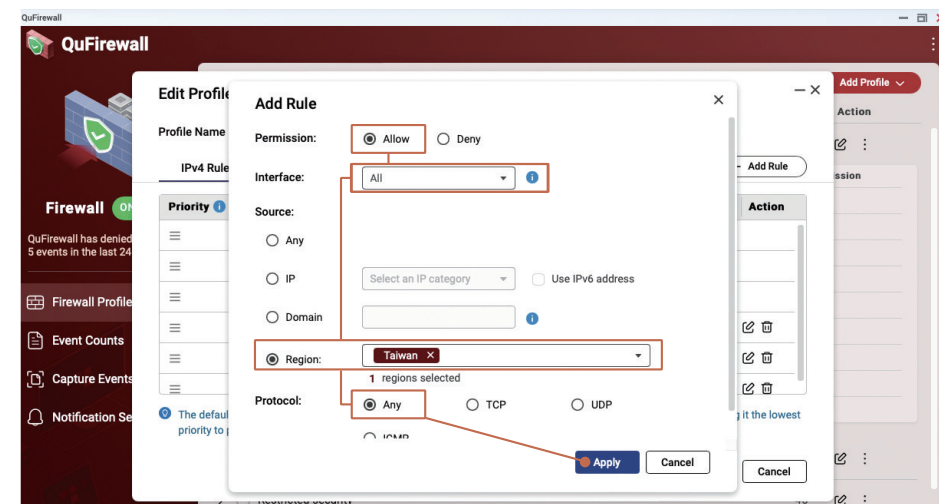
A continuación se muestra cómo editar las reglas del firewall. Haga clic en el botón "Editar"  para editar la pantalla Perfiles de firewall.



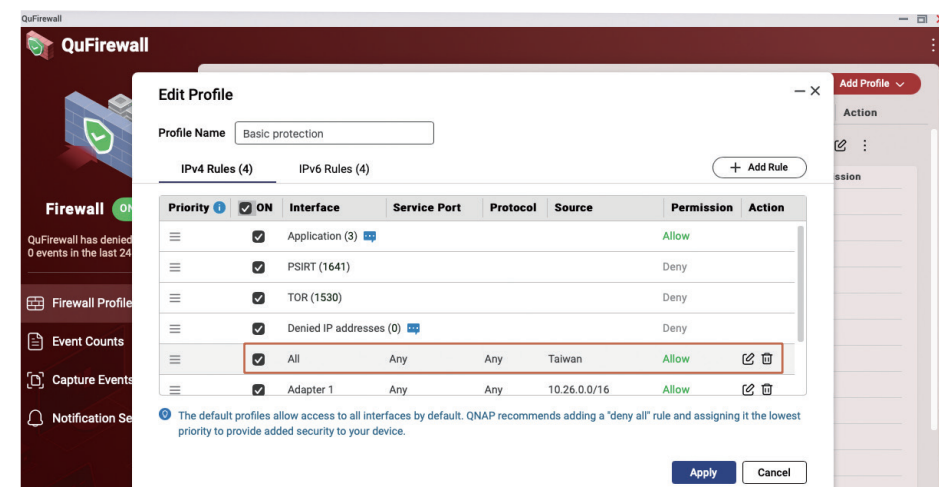
En la pantalla Editar perfil, puede cambiar el orden de las reglas o agregar reglas nuevas. El siguiente ejemplo agrega una región más a la que se permite la conexión; haga clic en "Añadir regla" para acceder a la pantalla de configuración.



Por ejemplo, para permitir conexiones desde Taiwán, "Permiso" debe establecerse en "Permitir"; "Interfaz", en "Todos"; "Región", en "Origen" y luego seleccione "Taiwán"; establezca "Protocolo" en "Cualquiera" y, a continuación, haga clic en "Aplicar" para agregar la regla cuando haya terminado.



En la página "Editar perfil", puede ver las reglas recién agregadas. Si es necesario, puede ajustar el orden de las reglas. Después de confirmar que son correctas, haga clic en "Aplicar".



Habilitar instantáneas programadas

La función de instantánea puede proteger sus datos importantes mediante la creación de puntos de restauración de varias versiones. Puede establecer una programación de instantáneas en el QNAP NAS para permitir que el sistema cree automáticamente instantáneas de acuerdo con la programación como protección básica de datos.

- Las instantáneas programadas están habilitadas de forma predeterminada para "volúmenes completos/Thin" creados por QTS 5.0.0
- En QTS 5.0.1 (y versiones posteriores), solo los "volúmenes Thin" tienen instantáneas programadas habilitadas de forma predeterminada
- Las "carpetas compartidas" creadas por QuTS hero h5.0.1 (y versiones posteriores) habilitarán instantáneas programadas de forma predeterminada

Abra "Almacenamiento e instantáneas", haga clic en "Almacenamiento/Instantáneas" a la izquierda y asegúrese de que "Espacio de almacenamiento" sea una estructura de "Conjunto de almacenamiento" y que el "Conjunto de almacenamiento" tenga suficiente espacio libre para que funcione la función de instantáneas. Si su tipo de volumen es "volumen completo", puede considerar "Redimensionar volumen*" y "Convertir a volumen Thin*" para liberar espacio del "Conjunto de almacenamiento" para la función de instantánea.

- Debe hacer una copia de seguridad de sus datos antes de convertir volúmenes para evitar posibles pérdidas de datos.

Storage & Snapshots

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

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

Thick Management

Name/Alias: Thick

Capacity: 494.54 GB

Free Size: 494.47 GB

Thin: No

SSD cache: --

Status: Ready

Utilization: 100% (72.04 MB) / 75% / 60% / 25%

Actions:

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

Abra Gestión Thick para realizar los ajustes pertinentes para liberar espacio en el "Conjunto de almacenamiento"

Después de confirmar que hay suficiente espacio en el "Conjunto de almacenamiento" en el NAS, primero haga clic en "Volumen" y, a continuación, haga clic en "Instantánea" en la parte superior y haga clic en "Administrador de instantáneas" en el menú.

Storage & Snapshots

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

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

Snapshot Manager

Snapshot Retention

How many Snapshot can I have?

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

Maximum amount of time to keep: 0 Months

Maximum number of snapshots to keep: 0 Snapshots

Smart Versioning

Hourly snapshots: 24

Daily snapshots: 7

Weekly snapshots: 4

Monthly snapshots: 12

Vaya a la página de configuración "Administrador de instantáneas" de "Volumen" y haga clic en "Programa de instantáneas" en la parte superior derecha.

Snapshot Manager

Pool Guaranteed Snapshot Space

Enable schedule: ☒

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

Snapshot retention policy: Smart Versioning

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

Enable smart snapshot

Description

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

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

Cambie el estado de "Habilitar Programación" a "Habilitar" y luego modifique la programación según sus necesidades.

Se recomienda utilizar "Diariamente" o "Semanalmente".

Snapshot Settings

Schedule Snapshot Snapshot Retention Pool Guaranteed Snapshot Space

Enable schedule: ☒

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

Snapshot retention policy: Smart Versioning

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

Enable smart snapshot

Description

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

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

Puede configurar una política de conservación de instantáneas para limitar la cantidad de instantáneas y evitar que las instantáneas ocupen demasiado espacio.

Se recomienda configurar "Creación de versiones inteligentes", es decir, la regla Abuelo-Padre-Hijo (GFS), para conservar suficientes versiones para la protección de datos. Una vez completada la configuración, haga clic en "Aceptar" para aplicar la configuración.

Snapshot Manager

Snapshot Retention

How many Snapshot can I have?

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

Maximum amount of time to keep: 0 Months

Maximum number of snapshots to keep: 0 Snapshots

Smart Versioning

Hourly snapshots: 24

Daily snapshots: 7

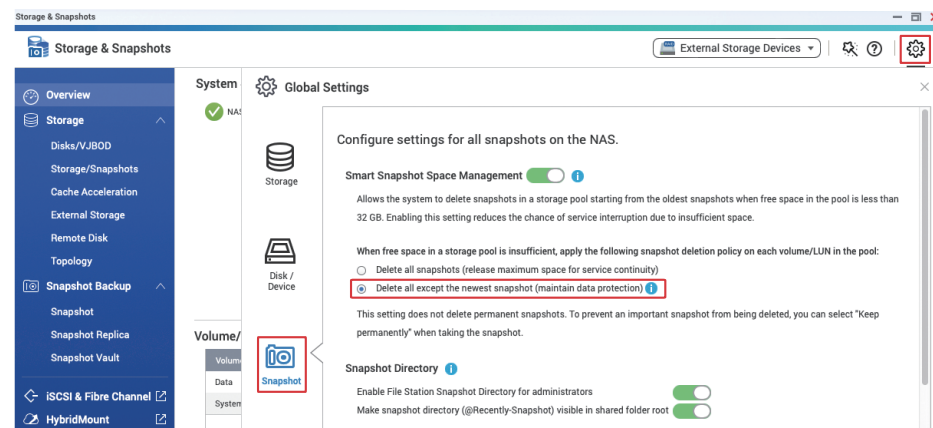
Weekly snapshots: 4

Monthly snapshots: 12

Establecer una política de eliminación de instantáneas

Cuando el conjunto de almacenamiento no tenga espacio suficiente, el sistema eliminará las instantáneas según su configuración para mantener el servicio normal del sistema y evitar posibles interrupciones del servicio causadas por ser el espacio insuficiente.

En "Almacenamiento e instantáneas", haga clic en el botón "Configuración" en la esquina superior derecha, abra "Configuración global" y haga clic en "Instantánea". Se recomienda configurarlo en "Eliminar todo excepto la instantánea más reciente" para evitar que todas las instantáneas se recuperen y pierdan la protección.

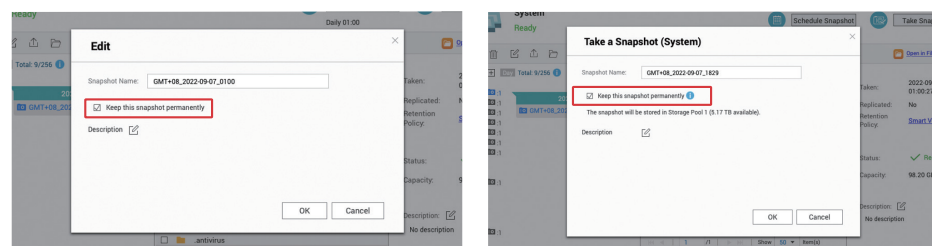


Si desea que el sistema conserve todas las instantáneas incluso cuando el "Conjunto de almacenamiento" no tiene espacio suficiente, deshabilite la "Gestión inteligente del espacio para instantáneas". Tenga en cuenta que esto hará que el "Conjunto de almacenamiento" entre en el estado "solo lectura/eliminación" cuando el espacio del "Conjunto de almacenamiento" sea insuficiente. Debe eliminar manualmente la instantánea para restaurar el "Conjunto de almacenamiento" a su funcionamiento normal. Asegúrese de comprobar periódicamente el uso del espacio después de desactivar esta función.



Para evitar fallos en la protección debido a la política de eliminación de instantáneas, se recomienda configurar todas las instantáneas o parte de ellas en "Mantener la instantánea de forma permanente" después de almacenar una gran cantidad de datos para evitar que el sistema recicle las instantáneas.

* Debe eliminar manualmente para liberar espacio. Se recomienda crear y eliminar de forma manual periódicamente



Lista de comprobación de la configuración de seguridad del NAS

- ❑ **Configuración del Centro de notificaciones**
 - ❑ Establezca al menos un método de notificación
 - ❑ Cree reglas de "Notificaciones de alerta"
 - ❑ Cree reglas de notificación de "Actualización de firmware"
- ❑ **Habilitar la actualización automática de firmware (QTS/QuTS hero)**
- ❑ **Configurar App Center**
 - ❑ Actualice todas las aplicaciones a la versión más reciente
 - ❑ Prohíba la instalación de aplicaciones que no tengan una firma digital válida
 - ❑ Habilite las actualizaciones automáticas
- ❑ **Deshabilitar o eliminar las funciones innecesarias**
 - ❑ Compruebe si los servicios habilitados son necesarios
 - ❑ Compruebe si son necesarias las aplicaciones habilitadas de App Center
 - ❑ Deshabilite SSH
 - ❑ Deshabilite Telnet
- ❑ **Reforzar la seguridad de las cuentas del sistema**
 - ❑ Deshabilite la cuenta "admin" predeterminada
 - ❑ Establezca la política de contraseñas
 - ❑ Habilite Protección de acceso de IP
 - ❑ Habilite la verificación en dos pasos (2SV)
- ❑ **Cambiar el puerto del sistema predeterminado**
- ❑ **Habilitar el registro de acceso**
- ❑ **Instalar y habilitar aplicaciones de seguridad**
 - ❑ **Security Counselor**
 - ❑ Inicie el escaneo programado
 - ❑ **Malware Remover**
 - ❑ Inicie el escaneo programado
 - ❑ **QuFirewall**
 - ❑ Habilite el cortafuegos
 - ❑ Establezca la región Geo-IP
 - ❑ Habilite reglas PSIRT
 - ❑ Habilite reglas TOR
- ❑ **Habilitar instantáneas programadas**
 - ❑ Configure periódicamente "Mantener la instantánea de forma permanente"

Preguntas frecuentes

Q ¿Es más seguro desconectar el NAS de Internet?

A No. La "desconexión" del NAS generalmente se refiere a desconectar el NAS de la red para que no pueda iniciar conexiones con el mundo exterior. Aunque algunos programas maliciosos requieren una conexión externa para ejecutarse, todavía hay programas maliciosos que pueden realizar acciones maliciosas con éxito sin una conexión externa. Por lo tanto, no solo no evitará que los hackers realicen acciones ilegales, sino que también evitará que funcionen correctamente algunas funciones del sistema, como las actualizaciones automáticas de software y las notificaciones. El enfoque correcto es limitar el tráfico al NAS, como evitar la exposición a Internet, para mejorar la seguridad.

Q Mi disco duro está configurado con RAID, ¿significa que no necesito copias de seguridad?

A No. RAID no es un método de copias de seguridad. Los niveles de RAID por encima de 0 solo están destinados a proporcionar redundancia contra fallos del disco. RAID no proporciona protección contra la eliminación o el cifrado de datos. Por lo tanto, se recomienda **realizar una copia de seguridad adecuada de los datos de acuerdo con el principio de copia de seguridad 3-2-1**.

Q Ya he configurado "instantáneas", ¿significa que no necesito copias de seguridad?

A No. Debido a que las "instantáneas" se almacenan en el mismo conjunto de discos duros que sus datos, los datos también se perderán si hay un fallo de RAID. Además, si los hackers pueden obtener suficientes privilegios (como descifrar con éxito la cuenta del administrador), también se podría eliminar la "instantánea". Por lo tanto, se recomienda realizar una copia de seguridad adecuada de los archivos de instantáneas de acuerdo con el principio de copia de seguridad 3-2-1.

Q Mi NAS no está expuesto a Internet, ¿significa que es imposible que lo ataquen?

A No. Aunque la mayoría de los ciberataques provienen de Internet, el NAS aún corre el riesgo de ser atacado en la intranet. Por ejemplo, si otra computadora o dispositivo en su intranet es pirateado o afectado por malware, puede usarse para atacar y propagarse a otros dispositivos de la intranet. La instalación de software antivirus y la implementación de productos de seguridad de red en su ordenador pueden ayudarle a lidiar con las amenazas relacionadas. Por ejemplo, QNAP ADRA NDR puede detectar actividades sospechosas en la intranet y aislarlas automáticamente. Al mismo tiempo, también se recomienda realizar una copia de seguridad adecuada de los datos de acuerdo con el principio de copia de seguridad 3-2-1.

Q Mi NAS lleva mucho tiempo en uso, ¿cómo compruebo si hay malware instalado?

A Si nota que la carga del procesador es anormalmente alta, observa fallos en la actualización del software o hay aplicaciones desconocidas en App Center, es posible que se haya instalado un programa malicioso. Se recomienda instalar y utilizar la última versión de Malware Remover. Si aun así no consigue resolver el problema, comuníquese con el equipo de soporte técnico de QNAP para obtener ayuda.

Q Si es necesario que abra algunos servicios a Internet, ¿qué debo hacer para garantizar la seguridad?

A Asegúrese de que el NAS tenga instalada la última versión de firmware y aplicaciones. Puede habilitar QuFirewall para proporcionar una protección de firewall básica, y las reglas "PSIRT" y "TOR" pueden ayudarle a bloquear las conexiones de algunos hackers. Si es un usuario comercial o empresarial, se recomienda utilizar una solución de firewall de nivel superior. Además, si el espacio del conjunto de almacenamiento lo permite, puede crear "instantáneas" para la protección básica de datos. También se recomienda realizar una copia de seguridad adecuada de los datos de acuerdo con el principio de copia de seguridad 3-2-1 para prepararse para el peor de los casos y evitar la posible pérdida de datos.

Q Mi NAS es antiguo y no es compatible con la última versión de QTS, ¿se puede seguir utilizando de forma segura?

A Los modelos Legacy y End of Life (EOL) tienen soporte limitado y solo deben usarse para copias de seguridad fuera de línea/intranet.

Q ¿Por qué sigo recibiendo una advertencia de error al iniciar sesión en el NAS?

A Si la dirección IP del inicio de sesión con errores proviene de Internet, significa que su NAS está bajo un ataque de descifrado de contraseñas por fuerza bruta. Debe evitar exponer su NAS a Internet y seguir este tutorial para protegerlo. Si la dirección IP del inicio de sesión con errores es de la intranet, verifique si el dispositivo con esa dirección IP tiene malware instalado.

Q ¿Por qué todos mis archivos tienen nombres de archivo extraños?

A Este es un síntoma de una infección por ransomware. Verifique los registros de acceso del NAS para determinar si la acción de encriptación proviene de otro ordenador o del mismo NAS. Si su NAS se ha visto afectado por ransomware, debe tomar las medidas adecuadas para detener la propagación de la infección. En caso necesario, comuníquese con el equipo de soporte técnico de QNAP para obtener ayuda.

Q ¿Qué debo hacer si mi NAS está infectado con ransomware?

A La mayoría de ransomware utiliza métodos de cifrado irrompibles. Si no se proporciona la clave correcta, los archivos no se pueden desbloquear, por lo que los archivos solo se pueden restaurar mediante una copia de seguridad o una instantánea.

Modifique de inmediato la configuración del enrutador de acuerdo con este tutorial para evitar exponer el NAS a Internet y para prevenir ataques secundarios. En segundo lugar, debe suspender inmediatamente todas las tareas de sincronización y configurar las instantáneas para que se conserven de forma permanente, con el fin de evitar la pérdida de los archivos de copia de seguridad. Si sus datos tienen copias de seguridad o instantáneas que puede restaurar, puede restaurar los archivos después de actualizar el firmware y las aplicaciones del NAS y después de completar el análisis de Malware Remover. Si no tiene una copia de seguridad de los datos, realice una copia de seguridad de la nota de rescate que dejó el ransomware y el método de pago del rescate, y luego intente utilizar métodos como la recuperación de datos para recuperar algunos datos. En caso necesario, comuníquese con el equipo de soporte técnico de QNAP para obtener ayuda.

Q Continúo viendo informes en los medios sobre vulnerabilidades en los productos de parches de QNAP. ¿Significa esto que los productos de QNAP no son seguros?

A No existe ningún software ni hardware que sean perfectos. Tanto si es software propio desarrollado por diversos fabricantes como si se trata de software de código abierto, o incluso de hardware, siempre se encuentran vulnerabilidades para las cuales los fabricantes posteriormente desarrollan parches. Al igual que las principales empresas de tecnología, QNAP continúa desarrollando parches para las vulnerabilidades conocidas y posteriormente publica archivos de actualización para que los usuarios se actualicen lo antes posible con el fin de garantizar la seguridad de los dispositivos y los datos de los usuarios. QNAP PSIRT también emite notificaciones de ciberseguridad para divulgación externa, de modo que los usuarios puedan actuar contra los problemas que surjan. QNAP considera que tratar con las vulnerabilidades de manera abierta y transparente puede proteger el derecho de los usuarios a conocer y ayudar a mejorar la seguridad de los productos. También se invita a los usuarios a suscribirse a los Avisos de seguridad de QNAP para obtener información relevante, precisa y completa antes de los informes de los medios.

Avisos de seguridad de QNAP:

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



Q ¿Qué es el principio de copia de seguridad 3-2-1?

A El principio de copia de seguridad 3-2-1 es un principio de copia de seguridad bien conocido en la industria de TI. Se prepara para el peor de los casos. Garantiza que, en caso de desastre, haya archivos de copia de seguridad para restaurar los datos con el fin de evitar pérdidas y garantizar la seguridad.

"3" en Copia de seguridad 3-2-1 significa al menos tres copias de seguridad; "2" significa al menos dos soportes de almacenamiento; y "1" significa que al menos una copia de seguridad se guarda fuera de las instalaciones.

Según el principio de copia de seguridad 3-2-1, habrá archivos de copia de seguridad que se pueden restaurar independientemente de la modificación accidental, la eliminación, el daño del hardware, la infección por virus y los desastres tales como incendios o inundaciones.

Para satisfacer este principio, el QNAP NAS incluye Hybrid Backup Sync 3 (HBS3), Snapshot Replica y SnapSync (compatible solo con QuTS hero) para realizar copias de seguridad de los datos del NAS en un NAS externo, una nube pública, un almacenamiento externo, otros servidores de archivos, y/u otros dispositivos para asegurar que no se pierda nada.

Tutoriales relacionados con Hybrid Backup Sync 3 (HBS3):

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



Tutoriales relacionados con la réplica de instantáneas:

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



Tutoriales de SnapSync:

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



Para mejorar la seguridad, puede añadir una copia de seguridad fuera de línea o una copia de seguridad en el espacio de almacenamiento WORM (Write Once Read Many) de QuTS hero con el fin de evitar la manipulación de los datos.

NOTA



2 0 2 3

Guía de seguridad



QNAP SYSTEMS, INC.

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

Dirección: 3F, No.22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221, Taiwán (China)

QNAP puede realizar cambios en las especificaciones y en las descripciones de los productos sin previo aviso.

Copyright © 2023 QNAP Systems, Inc. Todos los derechos reservados.

QNAP® y otros nombres de productos QNAP son marcas comerciales o marcas comerciales registradas de QNAP Systems, Inc. Otros productos y nombres de empresas aquí mencionados son marcas comerciales de sus respectivos propietarios.