# Citrix Gateway 12.1

**Machine translated content**

## Disclaimer

La versión oficial de este contenido está en inglés. Para mayor comodidad, parte del contenido de la documentación de Cloud Software Group solo tiene traducción automática. Cloud Software Group no puede controlar el contenido con traducción automática, que puede contener errores, imprecisiones o un lenguaje inadecuado. No se ofrece ninguna garantía, ni implícita ni explícita, en cuanto a la exactitud, la fiabilidad, la idoneidad o la precisión de las traducciones realizadas del original en inglés a cualquier otro idioma, o que su producto o servicio de Cloud Software Group se ajusten a cualquier contenido con traducción automática, y cualquier garantía provista bajo el contrato de licencia del usuario final o las condiciones de servicio, o cualquier otro contrato con Cloud Software Group, de que el producto o el servicio se ajusten a la documentación no se aplicará en cuanto dicha documentación se ha traducido automáticamente. Cloud Software Group no se hace responsable de los daños o los problemas que puedan surgir del uso del contenido traducido automáticamente.

# Contents



# Notas de versión de NetScaler Gateway

January 26, 2024

Las notas de la versión describen cómo ha cambiado el software en una compilación concreta y los problemas conocidos que existen en esa compilación.

El documento de notas de la versión incluye todas o algunas de las secciones siguientes:

- **Novedades**: Las mejoras y otros cambios publicados en la compilación.
- **Problemas solucionados**: Los problemas que se han solucionado en la compilación.
- **Problemas conocidos**: Los problemas que existen en la compilación.
- **Puntos a tener en cuenta**: los aspectos importantes a tener en cuenta al usar la compilación.
- **Limitaciones**: Las limitaciones que existen en la compilación.

> **Importante:** Las notas de la versión de NetScaler Gateway se tratan como parte de las notas de la versión de NetScaler ADC. Para obtener información detallada sobre las mejoras, los problemas conocidos y las correcciones de errores de Citrix Gateway 12.1, consulte la página de notas de la versión .

**Nota:**

- Las etiquetas [ # XXXXXX] en las descripciones de los problemas son identificadores de seguimiento internos que utiliza el equipo de NetScaler ADC.
- Estas notas de la versión no documentan las correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

# Acerca de NetScaler Gateway

January 26, 2024

NetScaler Gateway es fácil de implementar y administrar. La configuración de implementación más típica consiste en localizar el dispositivo NetScaler Gateway en la DMZ. Puede instalar varios dispositivos NetScaler Gateway en la red para implementaciones más complejas.

La primera vez que inicie NetScaler Gateway, puede realizar la configuración inicial mediante una consola serie, el Asistente de configuración de la utilidad de configuración o el Protocolo de configuración dinámica de host (DHCP). En el dispositivo MPX, puede utilizar el teclado LCD del panel frontal del dispositivo para realizar la configuración inicial. Puede configurar ajustes básicos específicos de su red

interna, como la dirección IP, la máscara de subred, la dirección IP de la puerta de enlace predeterminada y la dirección del sistema de nombres de dominio (DNS). Después de configurar la configuración básica de la red, configure la configuración específica de la operación de NetScaler Gateway, como las opciones de autenticación, autorización, recursos de red, servidores virtuales, directivas de sesión y directivas de dispositivos de punto final.

Antes de instalar y configurar NetScaler Gateway, consulte los temas de esta sección para obtener información sobre cómo planificar la implementación. La planificación de la implementación puede incluir determinar dónde instalar el dispositivo, comprender cómo instalar varios dispositivos en la DMZ y los requisitos de licencia. Puede instalar NetScaler Gateway en cualquier infraestructura de red sin necesidad de realizar cambios en el hardware o software existente que se ejecuta en la red segura. NetScaler Gateway admite otros productos de red, como equilibradores de carga de servidores, motores de caché, firewalls, enrutadores y dispositivos inalámbricos IEEE 802.11.

Puede escribir la configuración en la lista de comprobación previa a la instalación para tenerlo a mano antes de configurar NetScaler Gateway.

| | |
|---|---|
| Dispositivos NetScaler Gateway | Proporciona información sobre los dispositivos NetScaler Gateway y las instrucciones de instalación del dispositivo. |
| Lista de verificación de la instalación | Proporciona información de planificación para revisar y una lista de tareas que deben realizarse antes de instalar NetScaler Gateway en la red. |
| Implementaciones comunes | Proporciona información sobre la implementación de Citrix Gateway en la DMZ de la red, en una red segura sin una DMZ y con más dispositivos para admitir el equilibrio de carga y la conmutación por error. También proporciona información sobre la implementación de NetScaler Gateway con Citrix Virtual Apps and Desktops. |
| Licensing | Proporciona información sobre la instalación de licencias en el dispositivo. También proporciona información sobre la instalación de licencias en varios dispositivos NetScaler Gateway. |

# Arquitectura de NetScaler Gateway

January 26, 2024

Los componentes principales de NetScaler Gateway son:

- Servidores virtuales. El servidor virtual de NetScaler Gateway es una entidad interna que representa todos los servicios configurados disponibles para los usuarios. El servidor virtual es también el punto de acceso a través del cual los usuarios acceden a estos servicios. Puede configurar varios servidores virtuales en un solo dispositivo, lo que permite que un dispositivo NetScaler Gateway atienda a varias comunidades de usuarios con distintos requisitos de autenticación y acceso a los recursos.
- Autenticación, autorización y contabilidad. Puede configurar la autenticación, la autorización y la contabilidad para permitir a los usuarios iniciar sesión en NetScaler Gateway con credenciales que reconocen NetScaler Gateway o los servidores de autenticación ubicados en la red segura, como LDAP o RADIUS. Las directivas de autorización definen los permisos de usuario y determinan a qué recursos tiene autorización para acceder un usuario determinado. Para obtener más información sobre la autenticación y la autorización, consulte Configuración de la autenticación y la autorización. Los servidores de cuentas mantienen datos sobre la actividad de NetScaler Gateway, incluidos los sucesos de inicio de sesión de los usuarios, las instancias de acceso a recursos y los errores operativos Esta información se almacena en NetScaler Gateway o en un servidor externo. Para obtener más información sobre la contabilidad, consulte Configuración de auditorías en NetScaler Gateway
- Conexiones de usuarios. Los usuarios pueden iniciar sesión en NetScaler Gateway mediante los siguientes métodos de acceso:
  - El plug-in de NetScaler Gateway para Windows es software instalado en un equipo basado en Windows. Los usuarios inician sesión haciendo clic con el botón derecho en un icono del área de notificación de un equipo basado en Windows. Si los usuarios utilizan un equipo en el que el plug-in de NetScaler Gateway no está instalado, pueden iniciar sesión con un explorador Web para descargar e instalar el complemento. Si los usuarios tienen instalado Citrix Receiver, los usuarios inician sesión con el plug-in de NetScaler Gateway desde Receiver. Cuando Receiver y el plug-in de NetScaler Gateway están instalados en el dispositivo de usuario, Receiver agrega el plug-in de NetScaler Gateway automáticamente.
  - El plug-in de NetScaler Gateway para macOS X que permite a los usuarios que ejecutan macOS X iniciar sesión. Tiene las mismas funciones y funciones que el plug-in de NetScaler Gateway para Windows. Puede proporcionar soporte de análisis de dispositivos de punto

final para esta versión del complemento instalando NetScaler ADC Gateway 10.1, compilación 120.1316.e.

- Complemento de NetScaler Gateway para Java que permite a los usuarios de macOS X, Linux y, opcionalmente, iniciar sesión mediante un explorador web.
- Receiver que permite conexiones de usuario a aplicaciones publicadas y escritorios virtuales en una comunidad de servidores mediante la Interfaz Web o Citrix StoreFront.
- Receiver, Secure Hub, WorxMail y WorxWeb, que permiten a los usuarios acceder a aplicaciones web y SaaS, aplicaciones móviles iOS y Android y a datos de ShareFile alojados en Citrix Endpoint Management.
- Los usuarios pueden conectarse desde un dispositivo Android que utiliza la dirección web de NetScaler Gateway. Cuando los usuarios inician una aplicación, la conexión utiliza Micro VPN para dirigir el tráfico de red a la red interna. Si los usuarios se conectan desde un dispositivo Android, debe configurar la configuración de DNS en NetScaler Gateway. Para obtener más información, consulte Compatibilidad con consultas DNS mediante sufijos DNS para dispositivos Android.
- Los usuarios pueden conectarse desde un dispositivo iOS que utiliza la dirección web de NetScaler Gateway. Puede configurar Secure Browse de forma global o en un perfil de sesión. Cuando los usuarios inician una aplicación en su dispositivo iOS, se inicia una conexión VPN y la conexión se enruta a través de NetScaler Gateway.
- Acceso sin cliente que proporciona a los usuarios el acceso que necesitan sin instalar software en el dispositivo del usuario.

  Al configurar NetScaler Gateway, puede crear directivas para configurar cómo inician sesión los usuarios. También puede restringir el inicio de sesión de los usuarios mediante la creación de directivas de análisis de sesiones y endpoints.

- Recursos de red. Estos incluyen todos los servicios de red a los que los usuarios acceden a través de NetScaler Gateway, como servidores de archivos, aplicaciones y sitios web.
- Adaptador virtual. El adaptador virtual Citrix Gateway admite aplicaciones que requieren suplantación de IP. El adaptador virtual se instala en el dispositivo de usuario cuando se instala el plug-in de NetScaler Gateway. Cuando los usuarios se conectan a la red interna, la conexión saliente entre NetScaler Gateway y los servidores internos utiliza la dirección IP de la intranet como dirección IP de origen. El plug-in de NetScaler Gateway recibe esta dirección IP del servidor como parte de la configuración.

  Si habilita la tunelización dividida en NetScaler Gateway, todo el tráfico de la intranet se enruta a través del adaptador virtual. Al interceptar el tráfico vinculado a la intranet, el adaptador virtual interceptará consultas DNS de tipo de registro A y AAAA mientras deja intactas todas las demás consultas DNS. El tráfico de red que no está vinculado a la red interna se enruta a través

del adaptador de red instalado en el dispositivo del usuario. Las conexiones a Internet y LAN privada (LAN) permanecen abiertas y conectadas. Si inhabilita la tunelización dividida, todas las conexiones se enrutan a través del adaptador virtual. Todas las conexiones existentes se desconectan y el usuario debe restablecer la sesión.

Si configura una dirección IP de intranet, el tráfico hacia la red interna se falsificará con la dirección IP de la intranet a través del adaptador virtual.

## Cómo funcionan las conexiones de usuario

January 26, 2024

Los usuarios pueden conectarse a sus correos electrónicos, recursos compartidos de archivos y otros recursos de red desde una ubicación remota. Los usuarios pueden conectarse a los recursos de la red interna con el siguiente software:

- Plug-in de NetScaler Gateway
- Citrix Receiver
- WorxMail y WorxWeb
- Dispositivos móviles Android e iOS

### Conexión con el plug-in de NetScaler Gateway

El plug-in de NetScaler Gateway permite el acceso de los usuarios a los recursos de la red interna mediante los siguientes pasos:

1. Un usuario se conecta a NetScaler Gateway por primera vez escribiendo la dirección web en un explorador web. Aparece la página de inicio de sesión y se solicita al usuario que introduzca un nombre de usuario y una contraseña. Si se configuran servidores de autenticación externos, NetScaler Gateway se pone en contacto con el servidor y los servidores de autenticación verifican las credenciales del usuario. Si se configura la autenticación local, NetScaler Gateway realiza la autenticación de usuarios.
2. Si configura una directiva de autenticación previa, cuando el usuario escriba la dirección web de Citrix Gateway en un explorador web de un equipo basado en Windows o Mac OS X, Citrix Gateway comprueba si hay políticas de seguridad basadas en el cliente antes de que aparezca la página de inicio de sesión. Las comprobaciones de seguridad comprueban que el dispositivo del usuario cumple las condiciones relacionadas con la seguridad, como actualizaciones del sistema operativo, protección antivirus y un firewall configurado correctamente. Si el dispositivo del usuario no supera la comprobación de seguridad, NetScaler Gateway impide que el usuario

inicie sesión. Un usuario que no pueda iniciar sesión debe descargar las actualizaciones o paquetes necesarios e instalarlos en el dispositivo del usuario. Cuando el dispositivo de usuario pasa la política de autenticación previa, aparece la página de inicio de sesión y el usuario puede introducir sus credenciales. Puede utilizar Advanced Endpoint Analysis en un equipo Mac OS X si instala NetScaler Gateway 10.1, compilación 120.1316.e.

3. Cuando NetScaler Gateway autentica correctamente al usuario, NetScaler Gateway inicia el túnel VPN. NetScaler Gateway solicita al usuario que descargue e instale el plug-in de NetScaler Gateway para Windows o NetScaler Gateway para Mac OS X. Si utiliza el complemento Network Gateway para Java, el dispositivo de usuario también se inicializa con una lista de direcciones IP de recursos preconfigurados y números de puerto.
4. Si configura un análisis posterior a la autenticación, después de que un usuario inicie sesión correctamente, NetScaler Gateway explora el dispositivo del usuario en busca de las directivas de seguridad del cliente necesarias. Puede exigir las mismas condiciones relacionadas con la seguridad que para una directiva de autenticación previa. Si el dispositivo del usuario no supera el análisis, la directiva no se aplica o el usuario se coloca en un grupo de cuarentena y el acceso del usuario a los recursos de red es limitado.
5. Cuando se establece la sesión, se dirige al usuario a una página principal de NetScaler Gateway, donde el usuario puede seleccionar los recursos a los que acceder. La página principal incluida en NetScaler Gateway se denomina Interfaz de acceso. Si el usuario inicia sesión con el plug-in de NetScaler Gateway para Windows, un icono en el área de notificación del escritorio de Windows muestra que el dispositivo de usuario está conectado y el usuario recibe un mensaje indicando que la conexión está establecida. El usuario también puede acceder a los recursos de la red sin utilizar la interfaz de acceso, como abrir Microsoft Outlook y recuperar correo electrónico.
6. Si la solicitud de usuario pasa las comprobaciones de seguridad previas y versiones posteriores a la autenticación, NetScaler Gateway se pone en contacto con el recurso solicitado e inicia una conexión segura entre el dispositivo de usuario y ese recurso.
7. El usuario puede cerrar una sesión activa haciendo clic con el botón secundario en el icono de NetScaler Gateway del área de notificación de un equipo basado en Windows y, a continuación, haciendo clic en Cerrar sesión. La sesión también puede agotarse debido a la inactividad. Cuando se cierra la sesión, el túnel se cierra y el usuario ya no tiene acceso a los recursos internos. El usuario también puede escribir la dirección web de NetScaler Gateway en un explorador. Cuando el usuario presiona Intro, aparece la interfaz de acceso desde la que los usuarios pueden cerrar la sesión.

Nota: Si implementa Citrix Endpoint Management en su red interna, un usuario que se conecte desde fuera de la red interna debe conectarse primero a NetScaler Gateway. Cuando el usuario establece la conexión, el usuario puede acceder a aplicaciones web y SaaS, aplicaciones móviles Android e iOS y datos de ShareFile alojados en Citrix Endpoint Management. Un usuario puede conectarse con el plug-in de NetScaler Gateway a través de acceso sin cliente o mediante Citrix Receiver o Secure Hub.

### Conexión con Citrix Receiver

Los usuarios pueden conectarse a Receiver para acceder a sus escritorios virtuales y aplicaciones basadas en Windows. Los usuarios también pueden acceder a las aplicaciones desde Endpoint Management. Para conectarse desde una ubicación remota, los usuarios también instalan el plug-in de NetScaler Gateway en su dispositivo. Receiver agrega automáticamente el plug-in de NetScaler Gateway a su lista de complementos. Cuando los usuarios inician sesión en Receiver, también pueden iniciar sesión en el plug-in de NetScaler Gateway. También puede configurar NetScaler Gateway para que realice el inicio de sesión único en el plug-in de NetScaler Gateway cuando los usuarios inicien sesión en Receiver.

### Conexión con dispositivos iOS y Android

Los usuarios pueden conectarse desde un dispositivo iOS o Android mediante Secure Hub. Los usuarios pueden acceder a su correo electrónico mediante Secure Mail y conectarse a sitios web con WorxWeb.

Cuando los usuarios se conectan desde el dispositivo móvil, las conexiones se dirigen a través de NetScaler Gateway para acceder a los recursos internos. Si los usuarios se conectan con iOS, habilita Secure Browse como parte del perfil de sesión. Si los usuarios se conectan con Android, la conexión utiliza Micro VPN automáticamente. Además,
Secure Mail y WorxWeb utilizan Micro VPN para establecer conexiones a través de NetScaler Gateway. No es necesario configurar Micro VPN en NetScaler Gateway.

## Implementaciones comunes

January 26, 2024

Puede implementar NetScaler Gateway en el perímetro de la red interna (o intranet) de su organización para proporcionar un único punto de acceso seguro a los servidores, las aplicaciones y otros recursos de red que residen en la red interna. Todos los usuarios remotos deben conectarse a NetScaler Gateway para poder acceder a los recursos de la red interna.

NetScaler Gateway suele instalarse en las siguientes ubicaciones de una red:

- En la red DMZ
- En una red segura que no tiene DMZ<

También puede implementar NetScaler Gateway con Citrix Virtual Apps, Citrix Virtual Desktops, StoreFront y Citrix Endpoint Management para permitir a los usuarios acceder a sus aplicaciones Windows,

web, móviles y SaaS. Si su implementación incluye Citrix Virtual Apps, StoreFront y Desktops 7, puede implementar NetScaler Gateway en una configuración DMZ de salto único o doble salto. Las implementaciones de doble salto no son compatibles con versiones anteriores de Citrix Virtual Desktops ni Citrix Endpoint Management.

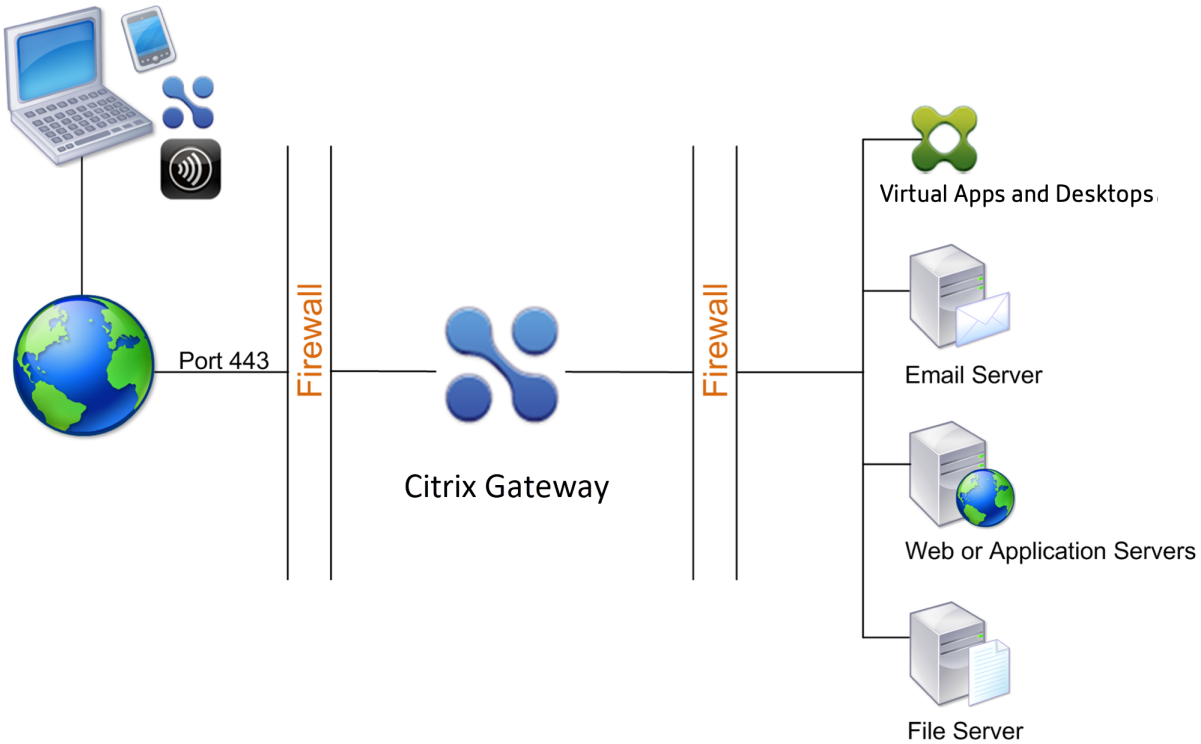
Para obtener más información sobre cómo ampliar la instalación de NetScaler Gateway con estas y otras soluciones Citrix compatibles, consulte el tema Integración con productos Citrix.

## Implementación en la DMZ

January 26, 2024

Muchas organizaciones protegen su red interna con una DMZ. Una DMZ es una subred que se encuentra entre la red interna segura de una organización e Internet (o cualquier red externa). Al implementar NetScaler Gateway en la DMZ, los usuarios se conectan con el plug-in de NetScaler Gateway o Citrix Receiver.

Figura 1. NetScaler Gateway implementado en la DMZ




En la configuración que se muestra en la ilustración anterior, se instala NetScaler Gateway en la DMZ y se configura para que se conecte tanto a Internet como a la red interna.

### Conectividad de Citrix Gateway en la DMZ

Al implementar NetScaler Gateway en la DMZ, las conexiones de usuario deben atravesar el primer firewall para conectarse a NetScaler Gateway. De forma predeterminada, las conexiones de usuario utilizan SSL en el puerto 443 para establecer esta conexión. Para permitir que las conexiones de usuario lleguen a la red interna, debe permitir SSL en el puerto 443 a través del primer firewall.

NetScaler Gateway descifra las conexiones SSL del dispositivo del usuario y establece una conexión en nombre del usuario con los recursos de red detrás del segundo firewall. Los puertos que deben abrirse a través del segundo firewall dependen de los recursos de red a los que autoriza el acceso de los usuarios externos.

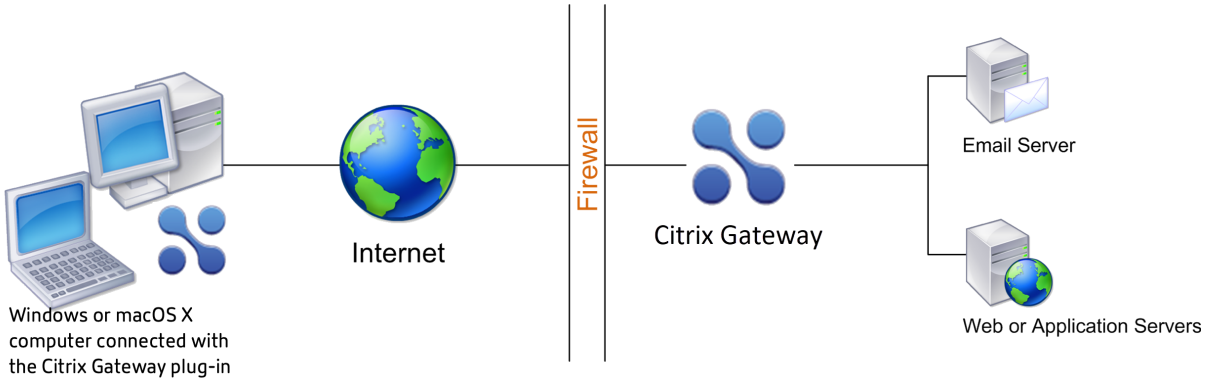
Por ejemplo, si autoriza a los usuarios externos a acceder a un servidor web de la red interna y este servidor escucha conexiones HTTP en el puerto 80, debe permitir HTTP en el puerto 80 a través del segundo firewall. NetScaler Gateway establece la conexión a través del segundo firewall con el servidor HTTP de la red interna en nombre de los dispositivos de usuario externos.

## Despliegue en la red segura

January 26, 2024

Puede instalar NetScaler Gateway en la red segura. En este caso, un firewall se interpone entre Internet y la red segura. NetScaler Gateway reside en el firewall para controlar el acceso a los recursos de la red.

Figura 1. NetScaler Gateway implementado en la red segura




Al implementar NetScaler Gateway en la red segura, conecte una interfaz de NetScaler Gateway a Internet y la otra interfaz a los servidores que se ejecutan en la red segura. La colocación de NetScaler Gateway en la red segura proporciona acceso a los usuarios locales y remotos. Sin embargo, debido a que esta configuración solo tiene un firewall, la implementación es menos segura para los usuarios que se conectan desde una ubicación remota. Aunque NetScaler Gateway intercepta el tráfico de

Internet, el tráfico entra en la red segura antes de que los usuarios se autentiquen. Cuando NetScaler Gateway se implementa en una DMZ, los usuarios se autentican antes de que el tráfico de red llegue a la red segura.

Cuando NetScaler Gateway se implementa en la red segura, las conexiones de plug-ins de NetScaler Gateway deben atravesar el firewall para conectarse a NetScaler Gateway. De forma predeterminada, las conexiones de usuario utilizan el protocolo SSL del puerto 443 para establecer esta conexión. Para admitir esta conectividad, debe abrir el puerto 443 en el firewall.

## Requisitos de software cliente

January 26, 2024

En esta sección se describen los requisitos del sistema para el software cliente Citrix Gateway.

NetScaler Gateway admite conexiones de usuario mediante el plug-in de NetScaler Gateway. Cuando los usuarios inician sesión con el complemento, se establece un túnel VPN completo. Con el plug-in de NetScaler Gateway, los usuarios pueden conectarse y trabajar con los recursos de red a los que se permite el acceso.

Si configura las políticas de punto final en Citrix Gateway, cuando los usuarios inicien sesión, Citrix Gateway descarga e instala automáticamente el complemento Endpoint Analysis en el dispositivo del usuario.

## Requisitos del sistema del complemento Citrix Gateway

January 26, 2024

El plug-in de NetScaler Gateway establece una conexión segura desde el equipo cliente al dispositivo NetScaler Gateway.

El complemento se distribuye como aplicación de escritorio para los sistemas operativos Microsoft Windows, macOS X y Linux. Después de autenticarse en la URL segura del dispositivo NetScaler Gateway con el explorador web, el complemento se descarga e instala automáticamente en el equipo.

El plug-in se aprovisiona como aplicación móvil para dispositivos Android e iOS.

> **Nota:**
>
> - Para instalar el plug-in, se necesitan privilegios de administrador y root en el sistema operativo.

> - Los exploradores compatibles con el plug-in de NetScaler Gateway también admiten VPN sin cliente.

El plug-in de NetScaler Gateway como aplicación de escritorio es compatible con los siguientes sistemas operativos y exploradores Web.

| Sistema operativo | Exploradores Web compatibles |
|---|---|
| macOS X (10.9 y posteriores) | Safari 7.1 o posterior; Google Chrome versión 30 o posterior; Mozilla Firefox versión 30 o posterior |
| Windows 10 (x86 y x64) | Internet Explorer 11; Google Chrome versión 30 o posterior; Mozilla Firefox versión 24 o posterior; Edge Chromium |
| Windows 8.1 | Internet Explorer 11; Google Chrome versión 30 o posterior; Mozilla Firefox versión 24 o posterior; Edge Chromium |
| Windows 8 | Internet Explorer 9 y 10; Google Chrome versión 30 o posterior; Mozilla Firefox versión 24 o posterior; Edge Chromium |
| Linux; Ubuntu 18.04 LTS, 16.04 LTS, 14.04 LTS y 12.04 LTS. Se admite SO de 32 y 64 bits. | Mozilla Firefox versión 44 y superior; Google Chrome 50 y superior |

> **Importante:**
>
> - Debido a un error (1573408) en Ubuntu 16.04 LTS, la instalación del complemento VPN falla. La solución alternativa para el mismo se muestra a continuación.
> - Windows 10 y Windows 11 en los modos S no admiten el complemento Citrix Gateway.
> - Actualmente, el cliente Citrix Secure Access para Ubuntu solo admite el administrador de pantalla GNOME predeterminado.

Escriba el siguiente comando mediante la interfaz de línea de comandos:

```
sudo dpkg -i nsgclient*.deb
<!--NeedCopy-->
```

Si faltan los paquetes de dependencias necesarios, el comando los enumera y se produce un error en la instalación del complemento. Estos paquetes de dependencias se deben instalar manualmente. Los administradores pueden instalar un paquete que falta escribiendo el siguiente comando mediante la interfaz de línea de comandos.

```
apt-get install <dependency package>
<!--NeedCopy-->
```

El plug-in de NetScaler Gateway como aplicación móvil es compatible con los siguientes sistemas operativos.

| Aplicación VPN | Sistemas operativos compatibles |
|---|---|
| Android | Android 7.0 y versiones posteriores |
| iOS | iOS 12.0 y versiones posteriores |

> **Nota:**
>
> Si utiliza las versiones más recientes de Apple OS, como macOS 14/iOS 17 y versiones posteriores, le recomendamos que actualice a Citrix Secure Access Client/Citrix SSO versión 23.09.1 o posterior.

## Requisitos de Endpoint Analysis

January 26, 2024

NetScaler Gateway instala el complemento Endpoint Analysis en el dispositivo del usuario. El complemento Endpoint Analysis explora el dispositivo del usuario en busca de los requisitos de seguridad de dispositivos de punto final que ha configurado en NetScaler Gateway. Los requisitos incluyen información, como el sistema operativo, el antivirus o las versiones del explorador web.

Cuando los usuarios de Windows se conectan a NetScaler Gateway mediante el explorador por primera vez, el portal solicita la instalación del complemento Endpoint Analysis. En los siguientes intentos de inicio de sesión, el complemento comprueba la configuración del control de actualización para comprobar si es necesaria la actualización del complemento de análisis de endpoint del cliente. Si es necesario, el usuario recibe una solicitud para descargar e instalar el nuevo complemento Endpoint Analysis. El complemento Endpoint Analysis para Windows se instala como una aplicación Windows de 32 bits. No se necesitan privilegios especiales para instalarlo o utilizarlo.

Para macOS, el usuario debe instalar el complemento Endpoint Analysis. El complemento para macOS se instala como una aplicación de 64 bits. No se necesitan privilegios especiales para instalarlo. En los siguientes intentos de inicio de sesión, si las versiones del complemento no coinciden, se solicita al usuario que descargue e instale el complemento.

La información sobre herramientas de la consola de la interfaz de usuario de administración explica los análisis en detalle. Para obtener más información sobre las bibliotecas de EPA, consulte https://www.citrix.com/en-in/downloads/citrix-gateway/epa-libraries/.

> **Importante:**
>
> - Los exploradores compatibles con EPA también admiten VPN sin cliente.
> - En el análisis de endpoint previo a la autenticación, el usuario no puede iniciar sesión con el plug-in de NetScaler Gateway si el usuario no instala el complemento Endpoint Analysis u omite el análisis.
> - En el análisis de endpoint posterior a la autenticación, el usuario puede acceder a los recursos para los que no es necesario realizar un análisis mediante el acceso sin cliente o mediante la aplicación Citrix Workspace.
> - Para los análisis relacionados con OPSWAT, debe instalar el paquete binario `epaPackage.exe` en el equipo cliente.

Se necesita el siguiente software en los dispositivos de usuario para utilizar el complemento Endpoint Analysis:

| Sistema operativo | Exploradores Web compatibles |
|---|---|
| macOS (10.9 y posteriores) | Safari 7.1 o posterior; Google Chrome versión 30 o posterior; Mozilla Firefox versión 30 o posterior |
| Windows 10 | Internet Explorer 11; Google Chrome versión 30 o posterior; Mozilla Firefox versión 24 o posterior; Edge Chromium |
| Windows 8.1 | Internet Explorer 11; Google Chrome versión 30 o posterior; Mozilla Firefox versión 24 o posterior; Edge Chromium |
| Windows 8 | Internet Explorer 9 y 10; Google Chrome versión 30 o posterior; Mozilla Firefox versión 24 o posterior; Edge Chromium |
| Windows 7 | Internet Explorer 9 y 10 y 11; Google Chrome versión 30 o posterior; Mozilla Firefox versión 24 o posterior; Edge Chromium |
| Windows Vista | Internet Explorer 9; Mozilla Firefox versiones 9 y 10 |
| Linux; Ubuntu 12.04 LTS, 14.04 LTS y 16.04 LTS. Se admiten sistemas operativos de 32 bits y 64 bits. Se admiten sistemas operativos de 32 bits y 64 bits. | Mozilla Firefox versión 44 y posteriores; Google Chrome 50 y versiones posteriores |

**Nota:**

- Todas las ediciones de las variantes del sistema operativo mencionadas anteriormente son compatibles.
- Para las ediciones de Windows, se deben instalar todos los service packs y las actualizaciones críticas.
- Para las versiones de Internet Explorer, las cookies deben estar habilitadas. La versión mínima requerida es 7.0.
- Para las versiones de Mozilla Firefox, Endpoint Analysis debe tener habilitados los complementos y la versión mínima requerida es la 3.0.
- Actualmente, el cliente Citrix EPA para Ubuntu solo admite el administrador de pantalla GNOME predeterminado.

## Compatibilidad con productos Citrix

January 26, 2024

En la tabla siguiente se muestran los productos y las versiones de Citrix con los que es compatible NetScaler Gateway 12.1.

> **Nota:**Las funciones de Citrix Gateway están disponibles en Citrix ADC VPX.

### Productos Citrix y versiones compatibles

| Producto Citrix | Versión de lanzamiento |
|---|---|
| Citrix SD-WAN | 10.2, 11.0 |
| Plataformas NetScaler ADC | Todos los modelos MPX y VPX actuales, incluidos los dispositivos compatibles con FIPS. |
| StoreFront | Todas las versiones de StoreFront compatibles actualmente. |
| Citrix Virtual Apps and Desktops | 7.15, 1808, 1811, 1903, 1906, 1909, 2003, 2009 |
| XenMobile | 10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12 |

> **Nota:**

> - La versión 7.6 de Citrix Virtual Apps and Desktops se admite a partir de la versión 12.1, compilación 52.xx.

### Aplicación Citrix Workspace, aplicaciones móviles de productividad de Citrix y complementos

*La primera compilación compatible para cada versión de software se indica en la tabla siguiente.Se admiten todas las compilaciones posteriores, a menos que se especifique lo contrario. Para obtener más información sobre el ciclo de vida de las versiones, consulte lamatriz de productos.

| Aplicación o complemento Citrix Workspace | Versión mínima compatible* |
|---|---|
| Plug-in de NetScaler Gateway para macOS X | 3.1.8 |
| Plug-in de NetScaler Gateway para Windows | 12.0 |
| Plug-in de NetScaler Gateway para iOS | 3.1.4 |
| Plug-in de NetScaler Gateway para Android | 2.0.14 |
| Aplicación Citrix Workspace para Android | 3.11 |
| Aplicación Citrix Workspace para iOS | 7.1.3 |
| Aplicación Citrix Workspace para Mac | 12.4 |
| Aplicación Citrix Workspace para Windows | 4.4 |
| Aplicación Citrix Workspace para Linux | 13.4 |
| Aplicación Citrix Workspace para HTML5 | 2.3 |
| Aplicación Citrix Workspace para Chrome | 2.3 |
| Secure Hub para iOS | 10.5 |
| Secure Hub para Android | 10.5 |
| Secure Mail para iOS | 10.5 |
| SecureWeb para iOS | 10.5 |
| Secure Mail para Android | 10.5 |
| SecureWeb para Android | 10.5 |

### Funciones compatibles de Citrix Gateway para el complemento Windows Gateway

| Función | Versión mínima de complemento admitida |
| --- | --- |
| Soporte de protección de dispositivos | 12.1 compilación 48.x y versiones posteriores;<br>12.0 compilación 58.x y versiones posteriores |
| Soporte nFactor | 12.1 compilación 48.x y versiones posteriores |
| Soporte para Opswat v4 | 12.1 compilación 48.x y versiones posteriores;<br>12.0 compilación 57.x y versiones posteriores |
| Soporte SAML | Compatible como parte de nFactor y no de forma independiente |
| Siempre en servicio | 12.1 compilación 51.x y versiones posteriores |

> **Nota:**Para obtener más información sobre algunas de las funciones de uso común compatibles con cada cliente VPN, consulte Clientes VPN de Citrix Gateway y funciones compatibles .

## Licencias

January 26, 2024

Antes de poder implementar Citrix Gateway para admitir las conexiones de usuarios, el dispositivo debe tener la licencia adecuada.

> **Importante:**Citrix recomienda conservar una copia local de todos los archivos de licencias que reciba. Al guardar una copia de seguridad del archivo de configuración, todos los archivos de licencia cargados se incluyen en la copia de seguridad. Si necesita volver a instalar el software del dispositivo Citrix Gateway y no tiene una copia de seguridad de la configuración, necesitará los archivos de licencia originales.

Antes de instalar licencias en NetScaler Gateway, establezca el nombre de host del dispositivo y, a continuación, reinicie NetScaler Gateway. Utilice el Asistente de configuración para configurar el nombre de host. Al generar la licencia universal para NetScaler Gateway, el nombre de host se utiliza en la licencia.

## Tipos de licencias de Citrix Gateway

March 27, 2024

NetScaler Gateway requiere una licencia de plataforma. La licencia de plataforma permite un número ilimitado de conexiones a Citrix Virtual Apps, Citrix Virtual Desktops o StoreFront mediante ICA Proxy. Para permitir conexiones VPN a la red desde el plug-in de NetScaler Gateway, un punto de inicio de sesión de SmartAccess o Secure Hub, WorxWeb o Secure Mail, también debe agregar una licencia universal. NetScaler Gateway VPX incluye la licencia Platform.

La licencia de plataforma es compatible con las siguientes versiones de NetScaler Gateway:

- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1
- NetScaler Gateway 11.0
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10
- Citrix ADC VPX

> **Importante:** Citrix recomienda conservar una copia local de todos los archivos de licencia que reciba. Al guardar una copia de seguridad del archivo de configuración, todos los archivos de licencia cargados se incluyen en la copia de seguridad. Si necesita volver a instalar el software del dispositivo NetScaler Gateway y no tiene una copia de seguridad de la configuración, necesitará los archivos de licencia originales.

### La licencia de plataforma

La licencia Platform permite conexiones ilimitadas de usuarios a aplicaciones publicadas en Citrix Virtual Apps o escritorios virtuales de Citrix Virtual Desktops. Las conexiones mediante Citrix Receiver no utilizan una licencia universal de NetScaler Gateway. Estas conexiones solo necesitan la licencia Platform. La licencia de plataforma se entrega electrónicamente con todos los pedidos nuevos de NetScaler Gateway, ya sean físicos o virtuales. Si ya posee un dispositivo cubierto por una garantía o un acuerdo de mantenimiento, puede obtener la licencia de plataforma en el sitio web de Citrix.

### La licencia universal

La licencia universal de NetScaler Gateway limita el número de sesiones de usuario simultáneas al número de licencias adquiridas. Si compra 100 licencias, puede tener 100 sesiones simultáneas en cualquier momento. Si adquiere una licencia de modificación estándar, puede tener 500 sesiones simultáneas en cualquier momento. Cuando un usuario finaliza una sesión, esa licencia se libera para el siguiente usuario. Un usuario que inicia sesión en NetScaler Gateway desde más de un equipo ocupa una licencia para cada sesión.

Si todas las licencias están ocupadas, no se pueden abrir conexiones adicionales hasta que un usuario finaliza una sesión o el administrador finaliza la sesión mediante la utilidad de configuración. Cuando se cierra una conexión, la licencia se libera y se puede utilizar para un nuevo usuario.

Cuando recibe el dispositivo NetScaler Gateway, la licencia se realiza en el siguiente orden:

- Recibirá el código de acceso a la licencia (clave de licencia) en un correo electrónico.
- Utilice el Asistente de configuración para configurar NetScaler Gateway con el nombre de host.
- Las licencias de NetScaler Gateway se asignan desde el sitio web de Citrix. Utilice el nombre de host para enlazar las licencias al dispositivo durante el proceso de asignación.
- Instale el archivo de licencia en NetScaler Gateway.

La licencia Universal admite las siguientes funciones:

- Túnel VPN completo
- Micro VPN
- Análisis de dispositivos de punto final
- SmartAccess basado en directivas
- Acceso sin cliente a sitios web y recursos compartidos de archivos

#### Obtención de la licencia universal

Necesita la siguiente información antes de ir al sitio web de Citrix para obtener la licencia universal.

- El ID de usuario y la contraseña de su cuenta Citrix.

  Regístrese en el sitio web de Citrix (https://www.citrix.com/welcome/create-account/) para recibir su ID de usuario y contraseña.
  Nota: Si no encuentra el código de licencia ni el ID de usuario y la contraseña, póngase en contacto con el servicio de atención al cliente de Citrix.

- El nombre de host de
  NetScaler Gateway

  El campo de entrada de este nombre en el sitio web de Citrix distingue entre mayúsculas y minúsculas, así que asegúrese de copiar el nombre de host exactamente como está configurado en el dispositivo NetScaler ADC.

- Número de licencias que quiere incluir en el archivo de licencia

  No es necesario descargar todas las licencias a las que se tiene derecho de una sola vez. Por ejemplo, si su empresa ha adquirido 100 licencias, puede elegir descargar 50. Puede asignar el resto en otro archivo de licencia más adelante. Se pueden instalar varios archivos de licencia en
  NetScaler Gateway.

**Nota:** Antes de obtener las licencias, asegúrese de configurar el nombre de host del dispositivo NetScaler ADC mediante el Asistente de configuración y, a continuación, reinicie el dispositivo.

#### Para obtener la licencia universal

1. Inicie sesión en el sitio web de Citrix (https://www.citrix.com/en-in/account/) con sus credenciales de Citrix.
2. En **Citrix Manage Licenses está aquí**, siga las instrucciones para obtener su archivo de licencia.

#### Instalación de la licencia universal

Para instalar la licencia, consulte "Instalación de la licencia". Después de la instalación, compruebe que la licencia se instaló correctamente.

#### Verificar la instalación de la licencia universal

Antes de continuar, compruebe que la licencia universal está instalada correctamente.

#### Para verificar la instalación de la licencia universal mediante la CLI

1. Abra una conexión SSH con el dispositivo NetScaler ADC mediante un cliente SSH, como PuTTY.
2. Inicie sesión en el dispositivo NetScaler ADC con las credenciales de administrador.
3. Utilice el comando show license para verificar que "SSL VPN = SÍ"y que el número máximo de usuarios ha aumentado de 5 al número esperado de usuarios simultáneos.

#### Para verificar la instalación de la licencia universal mediante la interfaz gráfica de usuario

1. En un explorador web, escriba la dirección IP del dispositivo NetScaler ADC, como `http://192.168.100.1`.
2. En Nombre de usuario y Contraseña, introduzca las credenciales de administrador.
3. En el panel de navegación, expanda Sistemay, a continuación, haga clic en Licencias.
4. En el panel Licencias, aparece una marca de verificación verde junto a **NetScaler Gateway**. El campo Máximo de usuarios de NetScaler Gateway permitidos muestra el número de sesiones de usuario simultáneas con licencia en el dispositivo NetScaler ADC.

## Obtener su plataforma o sus archivos de licencia universal

January 26, 2024

Tras instalar Citrix Gateway, estará listo para obtener los archivos de licencia universal o de plataforma de Citrix. Inicie sesión en el sitio web de Citrix para acceder a las licencias disponibles y generar un archivo de licencia. Una vez generado el archivo de licencia, lo descarga en un equipo. Cuando el archivo de licencia está en el equipo, lo carga en NetScaler Gateway. Para obtener más información sobre las licencias de Citrix, consulte Citrix Licensing System.

Antes de obtener los archivos de licencia, asegúrese de configurar el nombre de host del dispositivo mediante el Asistente de configuración y, a continuación, reinicie el dispositivo.

**Importante**: Debe instalar las licencias en Citrix Gateway. El dispositivo no obtiene licencias de Citrix License Server.

Para obtener sus licencias, vaya a la página web Activar, actualizar y administrar licencias de Citrix. En esta página, puede obtener su nueva licencia y activar, actualizar y administrar licencias de Citrix.

## Para instalar una licencia en Citrix Gateway

March 27, 2024

Después de descargar correctamente el archivo de licencia en su equipo, podrá instalar la licencia en NetScaler Gateway. La licencia se instala en el directorio /nsconfig/licence/.

Si utilizó el Asistente de configuración para configurar la configuración inicial de NetScaler Gateway, el archivo de licencia se instala al ejecutar el asistente. Si asigna parte de las licencias y, posteriormente, asigna un número adicional, puede instalar las licencias sin utilizar el asistente de configuración.

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Licencias .
2. En el panel de detalles, haga clic en Administrar licencias.
3. Haga clic en Agregar nueva licencia, luego en Examinar, navegue hasta el archivo de licencia y, a continuación, haga clic en Aceptar.

   Aparece un mensaje en la utilidad de configuración que indica que debe reiniciar Citrix Gateway. Haga clic en Reiniciar.

### Para establecer el número máximo de usuarios

Después de instalar la licencia en el dispositivo, debe establecer el número máximo de usuarios que pueden conectarse al dispositivo. Establezca el máximo de usuarios en la directiva de autenticación global.

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Settings, haga clic en Change Authentication AAA Settings.
3. En Número máximo de usuarios, escriba la cantidad total de usuarios y, a continuación, haga clic en Aceptar.

   El número de este campo corresponde a la cantidad de licencias que contiene el archivo de licencias. Este número debe ser menor o igual al total de licencias instaladas en el dispositivo. Por ejemplo, instale una licencia que contenga 100 licencias de usuario y otra que contenga 400 licencias de usuario. El total de licencias es igual a 500. El máximo de usuarios que pueden iniciar sesión es igual o inferior a 500. Si 500 usuarios han iniciado sesión, a todos los usuarios que intenten iniciar sesión más allá de ese número se les deniega el acceso hasta que un usuario cierra la sesión o finaliza una sesión.

## Verificar la instalación de la licencia universal

March 27, 2024

Antes de continuar, compruebe que la licencia Universal está instalada correctamente.

### Para verificar la instalación de la licencia universal mediante la utilidad de configuración

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Licencias .

   En el panel Licencias, verá una marca de verificación verde junto a Citrix Gateway. El campo Número máximo de usuarios de NetScaler Gateway permitidos muestra el número de sesiones de usuario simultáneas con licencia en el dispositivo.

### Para verificar la instalación de la licencia universal mediante la línea de comandos

1. Abra una conexión de Secure Shell (SSH) con el dispositivo mediante un cliente SSH, como PuTTY.
2. Inicie sesión en el dispositivo con las credenciales de administrador.
3. En la línea de comandos, escriba: show license La licencia está instalada correctamente si el parámetro SSL VPN es igual a Sí y el parámetro máximo de usuarios es igual al número de licencias.

# Preguntas frecuentes sobre licencias

March 27, 2024

## ¿Cómo puedo obtener ayuda con las licencias de prueba o demo?

Muchos de los productos Citrix se ofrecen ahora como experiencias de demostración completas, privadas, personalizadas y dirigidas por expertos. Nuestros expertos de Citrix personalizan la demostración para adaptarla a sus necesidades, casos de uso y proyectos activos. No se requieren descargas, licencias ni instalación. Necesitas una configuración mínima para ver una demostración instantánea. Después de la demostración, para proceder con una prueba de concepto o prueba de una solución Citrix aplicable a sus servicios, póngase en contacto con los expertos de Citrix. Para ver demostraciones, haga clic en https://demo.citrix.com/.

## ¿Cómo instalar licencias?

Para obtener más información sobre la instalación de licencias, consulte Para instalar una licencia en NetScaler Gateway.

## ¿Cuáles son los distintos tipos de licencias de Gateway?

La licencia de plataforma permite un número ilimitado de conexiones a Citrix Virtual Apps, Citrix Virtual Desktops o StoreFront mediante ICA Proxy.
La licencia universal es una licencia complementaria a las licencias de la plataforma NetScaler ADC. Esto permite conexiones VPN a la red desde el plug-in de NetScaler Gateway, un punto de inicio de sesión de SmartAccess o Secure Hub, Secure Web o Secure Mail. Para obtener más información, consulte Tipos de licencia de NetScaler Gateway.

## ¿Cuántas sesiones de usuario simultáneas se admiten?

Las sesiones admitidas dependen del tipo de licencia de puerta de enlace. Para obtener más información, consulte Tipos de licencia de NetScaler Gateway.

Otro factor a tener en cuenta es la capacidad del propio hardware subyacente. Consulte la hoja de datos de NetScaler ADC MPX/SDX o la hoja de datos de NetScaler ADC VPX para obtener información sobre el rendimiento.

### ¿Cómo comprobar las sesiones de usuario simultáneas actuales con licencia?

En la utilidad de configuración de la ficha Configuración, expanda **Sistema** y, a continuación, haga clic en **Licencias**.
En el panel **Licencias** , aparece una marca de verificación verde junto a Citrix Gateway. El campo **Número máximo de usuarios permitidos de Citrix Gateway** muestra el número de sesiones de usuario simultáneas con licencia en el dispositivo.

### ¿Cómo comprobar si se alcanza el límite de rendimiento de la licencia?

Puede extraer el rendimiento en tiempo real mediante `newnslog`. Por ejemplo, si el rendimiento de la licencia es de 500 Mbps, puede extraer el rendimiento en tiempo real superior a 500 mediante el siguiente comando.

```
nsconmsg -K newnslog -g mbits -d past -s disptime=1 -s ratecount=500 |
    more
<!--NeedCopy-->
```

```
reltime:mili second between two records Mon Feb  5 13:47:13 2018
 Index    rtime totalcount-val      delta rate/sec symbol-name&device-no&time
    12     7000      801130681       3701      528 allnic_tot_rx_mbits  Mon Feb  5 13:47:55 2018
    13        0      460776045       3682      526 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:47:55 2018
    14     7000      801134437       3756      536 allnic_tot_rx_mbits  Mon Feb  5 13:48:02 2018
    15        0      460779784       3739      534 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:02 2018
    16     7000      801138166       3729      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:09 2018
    17        0      460783497       3713      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:09 2018
    18     7000      801141896       3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:16 2018
    19        0      460787213       3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:16 2018
    20     7000      801145623       3727      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:23 2018
    21        0      460790929       3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:23 2018
    22     7000      801149353       3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:30 2018
    23        0      460794646       3717      531 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:30 2018
    24     7000      801153067       3714      530 allnic_tot_rx_mbits  Mon Feb  5 13:48:37 2018
    25        0      460798342       3696      528 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:37 2018
```

### ¿Cómo comprobar si los paquetes se pierden al alcanzar el rendimiento de las licencias?

Puede utilizar el siguiente comando para comprobar si se descartan paquetes.

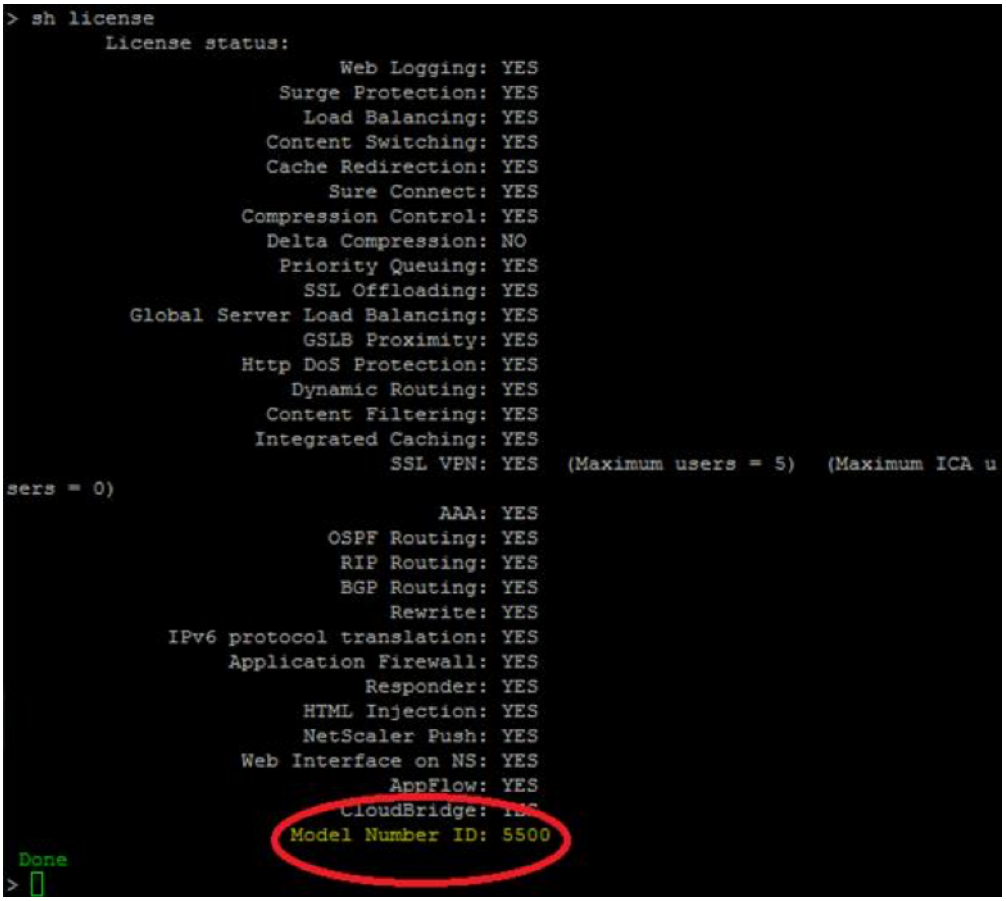
```
nsconmsg -K newnslog -d current -g nic_err_rl_pkt_drops -s disptime=1 |
    more
<!--NeedCopy-->
```

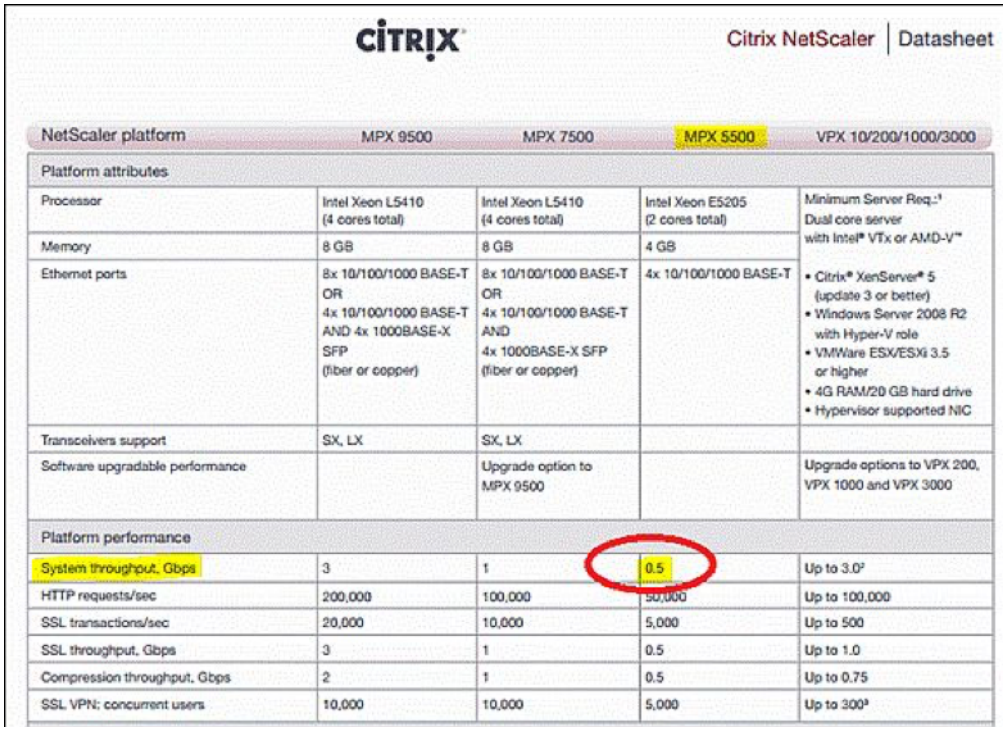
```
reltime:mili second between two records Fri Feb  2 00:12:38 2018
  Index    rtime    totalcount-val      delta rate/sec symbol-name&device-no&time
      0  1966993          23723602        478       68 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:38 2018
      1        0          48048402        465       66 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:38 2018
      2        0        8307679782     145475    20782 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:38 2018
      3     7000          23723933        331       47 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:45 2018
      4        0          48048712        310       44 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:45 2018
      5        0        8307787105     107323    15331 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:45 2018
      6     7000          23723941          8        1 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:52 2018
      7        0          48048735         23        3 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:52 2018
      8        0        8307811163      24058     3436 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:52 2018
```

## ¿Cómo puedo averiguar cuál es el rendimiento con licencia de un dispositivo NetScaler ADC?

Ejecute el comando `show license` desde la CLI y, a continuación, utilice el número de modelo para obtener el rendimiento de la hoja de datos de MPX, SDX y VPX de ADC o gateway.





CITRIX Citrix NetScaler | Datasheet

| NetScaler platform | MPX 9500 | MPX 7500 | MPX 5500 | VPX 10/200/1000/3000 |
|---|---|---|---|---|
| **Platform attributes** | | | | |
| Processor | Intel Xeon L5410 (4 cores total) | Intel Xeon L5410 (4 cores total) | Intel Xeon E5205 (2 cores total) | Minimum Server Req.:[1] Dual core server with Intel® VTx or AMD-V™ |
| Memory | 8 GB | 8 GB | 4 GB | |
| Ethernet ports | 8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper) | 8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper) | 4x 10/100/1000 BASE-T | • Citrix® XenServer® 5 (update 3 or better)<br>• Windows Server 2008 R2 with Hyper-V role<br>• VMWare ESX/ESXi 3.5 or higher<br>• 4G RAM/20 GB hard drive<br>• Hypervisor supported NIC |
| Transceivers support | SX, LX | SX, LX | | |
| Software upgradable performance | | Upgrade option to MPX 9500 | | Upgrade options to VPX 200, VPX 1000 and VPX 3000 |
| **Platform performance** | | | | |
| System throughput, Gbps | 3 | 1 | 0.5 | Up to 3.0[2] |
| HTTP requests/sec | 200,000 | 100,000 | 50,000 | Up to 100,000 |
| SSL transactions/sec | 20,000 | 10,000 | 5,000 | Up to 500 |
| SSL throughput, Gbps | 3 | 1 | 0.5 | Up to 1.0 |
| Compression throughput, Gbps | 2 | 1 | 0.5 | Up to 0.75 |
| SSL VPN: concurrent users | 10,000 | 10,000 | 5,000 | Up to 300[3] |

### ¿Cómo agregar más usuarios a las licencias de Gateway existentes?

Puede instalar una licencia universal adicional. Por ejemplo, supongamos que ha instalado una licencia universal que contiene 100 licencias de usuario. Si instala la segunda licencia universal que contiene 400 licencias de usuario, el número total de licencias de usuario es igual a 500.

## Antes de empezar

January 26, 2024

Antes de instalar Citrix Gateway, debe evaluar la infraestructura y recopilar información para planificar una estrategia de acceso que satisfaga las necesidades específicas de su organización. Cuando defina su estrategia de acceso, debe tener en cuenta las implicaciones de seguridad y completar un análisis de riesgos. También debe determinar las redes a las que los usuarios pueden conectarse y decidir las directivas que permiten las conexiones de los usuarios.

Además de planificar los recursos disponibles para los usuarios, también debe planificar el caso de implementación. Citrix Gateway funciona con los siguientes productos Citrix:

- Citrix Endpoint Management
- Citrix Virtual Apps

- Citrix Virtual Desktops
- StoreFront
- Interfaz Web
- CloudBridge

Para obtener más información sobre la implementación de NetScaler Gateway, consulte Implementaciones comunese integración con productos Citrix

Al preparar la estrategia de acceso, realice los siguientes pasos preliminares:

- Identificar recursos. Enumere los recursos de red a los que desea proporcionar acceso, como aplicaciones web, SaaS, móviles o publicadas, escritorios virtuales, servicios y datos que definió en su análisis de riesgos.
- Desarrolle casos de acceso. Cree casos de acceso que describan cómo los usuarios acceden a los recursos de la red. Un caso de acceso lo define el servidor virtual utilizado para acceder a la red, los resultados del análisis de puntos finales, el tipo de autenticación o una combinación de los mismos. También puede definir cómo los usuarios inician sesión en la red.
- Identificar el software cliente. Puede proporcionar acceso VPN completo con el plug-in de NetScaler Gateway, lo que requiere que los usuarios inicien sesión con Citrix Receiver, Secure Hub o mediante el acceso sin cliente. También puede restringir el acceso al correo electrónico a Outlook Web App o WorxMail. Estos casos de acceso también determinan las acciones que los usuarios pueden realizar cuando obtienen acceso. Por ejemplo, puede especificar si los usuarios pueden modificar documentos mediante una aplicación publicada o conectándose a un recurso compartido de archivos.
- Asocie directivas a usuarios, grupos o servidores virtuales. Las directivas que crea en NetScaler Gateway se aplican cuando la persona o el conjunto de usuarios cumplen las condiciones especificadas. Las condiciones se determinan en función de los casos de acceso que cree. A continuación, crea directivas que amplían la seguridad de la red mediante el control de los recursos a los que pueden acceder los usuarios y las acciones que los usuarios pueden realizar en esos recursos. Las directivas se asocian a los usuarios, grupos, servidores virtuales adecuados o de forma global.

En esta sección se incluyen los siguientes temas para ayudarle a planificar su estrategia de acceso:

- Planning for Security incluye información sobre autenticación y certificados.
- Requisitos previos que definen el hardware y el software de red que puede necesitar.
- Lista de comprobación previa a la instalación que puede utilizar para anotar la configuración antes de configurar NetScaler Gateway.

# Planificar la seguridad

January 26, 2024

Al planificar la implementación de Citrix Gateway, debe comprender los problemas de seguridad básicos asociados con los certificados y con la autenticación y la autorización.

## Configuración de la administración segura de certificados

De forma predeterminada, NetScaler Gateway incluye un certificado de servidor Secure Sockets Layer (SSL) autofirmado que permite al dispositivo completar las conexiones SSL. Los certificados autofirmados son adecuados para pruebas o implementaciones de muestra, pero Citrix no recomienda usarlos en entornos de producción. Antes de implementar NetScaler Gateway en un entorno de producción, Citrix recomienda solicitar y recibir un certificado de servidor SSL firmado de una entidad de certificación (CA) conocida y cargarlo en NetScaler Gateway.

Si implementa NetScaler Gateway en cualquier entorno en el que NetScaler Gateway deba funcionar como cliente en un protocolo de enlace SSL (iniciar conexiones cifradas con otro servidor), también debe instalar un certificado raíz de confianza en NetScaler Gateway. Por ejemplo, si implementa NetScaler Gateway con Citrix Virtual Apps y la Interfaz Web, puede cifrar las conexiones de NetScaler Gateway a la Interfaz Web con SSL. En esta configuración, debe instalar un certificado raíz de confianza en NetScaler Gateway.

## Soporte de autenticación

Puede configurar NetScaler Gateway para autenticar a los usuarios y controlar el nivel de acceso (o autorización) que tienen los usuarios a los recursos de red de la red interna.

Antes de implementar Citrix Gateway, su entorno de red debe tener los directorios y servidores de autenticación instalados para admitir uno de los siguientes tipos de autenticación:

- LDAP
- RADIUS
- TACACS+
- Certificado de cliente compatible con auditoría y tarjeta inteligente
- Configuración de RSA con RADIUS
- Autenticación SAML

Si su entorno no admite ninguno de los tipos de autenticación de la lista anterior, o si tiene un número reducido de usuarios remotos, puede crear una lista de usuarios locales en Citrix Gateway. A continuación, puede configurar NetScaler Gateway para autenticar a los usuarios en esta lista local. Con

esta configuración, no es necesario mantener las cuentas de usuario en un directorio externo independiente.

## Requisitos previos

January 26, 2024

Antes de configurar la configuración en NetScaler Gateway, revise los siguientes requisitos previos:

- NetScaler Gateway está instalado físicamente en la red y tiene acceso a la red. NetScaler Gateway se implementa en la DMZ o en la red interna detrás de un firewall. También puede configurar NetScaler Gateway en una DMZ de doble salto y configurar conexiones a una comunidad de servidores. Citrix recomienda implementar el dispositivo en la DMZ.
- Puede configurar NetScaler Gateway con una puerta de enlace predeterminada o con rutas estáticas a la red interna para que los usuarios puedan acceder a los recursos de la red. NetScaler Gateway está configurado para usar rutas estáticas de forma predeterminada.
- Los servidores externos utilizados para la autenticación y autorización están configurados y en ejecución. Para obtener más información, consulte Autenticación y autorización.
- La red tiene un servidor de nombres de dominio (DNS) o un servidor del Servicio de nombres de Internet (WINS) de Windows para la resolución de nombres a fin de proporcionar la funcionalidad de usuario correcta de NetScaler Gateway.
- Ha descargado las licencias universales para conexiones de usuario con el plug-in de NetScaler Gateway del sitio web de Citrix y las licencias están listas para instalarse en NetScaler Gateway.
- NetScaler Gateway tiene un certificado firmado por una entidad de certificación (CA) de confianza. Para obtener más información, consulte Instalar y administrar certificados.

Antes de instalar NetScaler Gateway, utilice la lista de comprobación previa a la instalación para anotar la configuración.

## Lista de verificación de la instalación

January 26, 2024

La lista de verificación consiste en una lista de tareas e información de planificación que debe completar antes de instalar Citrix Gateway.

Se proporciona espacio para que puedas marcar cada tarea a medida que la completes y hagas notas. Citrix recomienda tomar nota de los valores de configuración que debe introducir durante el proceso de instalación y durante la configuración de NetScaler Gateway.

Para ver los pasos para instalar y configurar NetScaler Gateway, consulte Instalación de NetScaler Gateway.

### Dispositivos de usuario

- Asegúrese de que los dispositivos de usuario cumplan los requisitos previos de instalación descritos en Requisitos del sistema del plug-in de NetScaler Gateway
- Identificar los dispositivos móviles con los que se conectan los usuarios. **Nota**: Si los usuarios se conectan con un dispositivo iOS, debe habilitar Secure Browse en un perfil de sesión.

### Conectividad de red básica de Citrix Gateway

Citrix recomienda obtener licencias y certificados de servidor firmados antes de empezar a configurar el dispositivo.

- Identifique y anote el nombre de host de NetScaler Gateway. **Nota**: Este no es el nombre de dominio completo (FQDN). El FQDN está contenido en el certificado de servidor firmado vinculado al servidor virtual.
- Obtenga licencias universales desde el sitio web de Citrix
- Genere una solicitud de firma de certificado (CSR) y envíela a una entidad de certificación (CA). Introduzca la fecha en la que envía la CSR a la CA.
- Anote la dirección IP del sistema y la máscara de subred.
- Anote la dirección IP de la subred y la máscara de subred.
- Anote la contraseña de administrador. La contraseña predeterminada que viene con Citrix Gateway es nsroot.
- Anota el número de puerto. Este es el puerto en el que Citrix Gateway escucha las conexiones de usuario seguras. El valor predeterminado es el puerto TCP 443. Este puerto debe estar abierto en el firewall entre la red no segura (Internet) y la DMZ.
- Anote la dirección IP de la puerta de enlace predeterminada.
- Anote la dirección IP y el número de puerto del servidor DNS. El número de puerto predeterminado es 53. Además, si va a agregar el servidor DNS directamente, también debe configurar ICMP (ping) en el dispositivo.
- Anote la dirección IP y el nombre de host del primer servidor virtual.
- Anote la dirección IP y el nombre de host del segundo servidor virtual (si procede).
- Anote la dirección IP del servidor WINS (si procede).

### Redes internas accesibles a través de Citrix Gateway

- Anote las redes internas a las que los usuarios pueden acceder a través de NetScaler Gateway. Ejemplo: 10.10.0.0/24.

- Introduzca todas las redes internas y segmentos de red a los que los usuarios necesitan acceso cuando se conectan a través de NetScaler Gateway mediante el plug-in de NetScaler Gateway.

### Alta disponibilidad

Si tiene dos dispositivos NetScaler Gateway, puede implementarlos en una configuración de alta disponibilidad en la que un NetScaler Gateway acepta y administra las conexiones, mientras que un segundo NetScaler Gateway supervisa el primer dispositivo. Si el primer NetScaler Gateway deja de aceptar conexiones por cualquier motivo, el segundo NetScaler Gateway se hace cargo y comienza a aceptar conexiones de forma activa.

- Anote el número de versión del software de NetScaler Gateway.
- El número de versión debe ser el mismo en ambos dispositivos NetScaler Gateway.
- Anota la contraseña de administrador (nsroot). La contraseña debe ser la misma en ambos dispositivos.
- Anote la dirección IP y el ID principales de NetScaler Gateway. El número de identificación máximo es 64.
- Anote la dirección IP y el ID secundarios de NetScaler Gateway.
- Obtenga e instale la licencia universal en ambos dispositivos.
- Debe instalar la misma licencia universal en ambos dispositivos.
- Anote la contraseña del nodo RPC.

### Autenticación y autorización

Citrix Gateway admite varios tipos de autenticación y autorización diferentes que se pueden usar en una variedad de combinaciones. Para obtener información detallada sobre la autenticación y la autorización, consulte Autenticación y autorización.

#### Autenticación LDAP

Si su entorno incluye un servidor LDAP, puede utilizar LDAP para la autenticación.

- Anote la dirección IP y el puerto del servidor LDAP.

  Si permite conexiones no seguras al servidor LDAP, el puerto predeterminado es 389. Si se cifran las conexiones al servidor LDAP con SSL, el puerto predeterminado es 636.

- Anota el tipo de seguridad.

  Puede configurar la seguridad con o sin cifrado.

- Anote el DN de enlace de administrador.

  Si el servidor LDAP requiere autenticación, introduzca el DN de administrador que Citrix Gateway debe usar para autenticarse al realizar consultas en el directorio LDAP. Un ejemplo es cn=administrator, cn=Users, dc=ace, dc=com.

- Anote la contraseña de administrador.

  Esta es la contraseña asociada al DN de enlace de administrador.

- Anote el DN base.

  DN (o nivel de directorio) en el que se encuentran los usuarios; por ejemplo, ou=users, dc=ace, dc=com.

- Anote el atributo de nombre de inicio de sesión del servidor.

  Introduzca el atributo de objeto persona del directorio LDAP que especifica el nombre de inicio de sesión de un usuario. El valor predeterminado es sAMAccountName. Si no usa Active Directory, los valores comunes para esta configuración son cn o uid.
  Para obtener más información sobre la configuración del directorio LDAP, consulte Configuración de la autenticación LDAP

- Anota el atributo group.
  Introduzca el atributo de objeto persona del directorio LDAP que especifica los grupos a los que pertenece un usuario. El valor predeterminado es memberOf. Este atributo permite a NetScaler Gateway identificar los grupos de directorios a los que pertenece un usuario.

- Anote el nombre del subatributo.

#### Autenticación y autorización RADIUS

Si su entorno incluye un servidor RADIUS, puede utilizar RADIUS para la autenticación.
La autenticación RADIUS incluye productos RSA SecurID, SafeWord y Gemalto Protiva.

- Anote la dirección IP y el puerto del servidor RADIUS principal. El puerto predeterminado es 1812.
- Anote el secreto del servidor RADIUS principal (secreto compartido).
- Anote la dirección IP y el puerto del servidor RADIUS secundario. El puerto predeterminado es 1812.
- Anote el secreto del servidor RADIUS secundario (secreto compartido).
- Anote el tipo de codificación de contraseña (PAP, CHAP, MS-CHAP v1, MSCHAP v2).

### Autenticación SAML

El lenguaje de marcado de aserciones de seguridad (SAML) es un estándar basado en XML para intercambiar autenticación y autorización entre proveedores de identidad (IdP) y proveedores de servicios.

- Obtenga e instale en NetScaler Gateway un certificado de proveedor de identidad seguro.
- Anota la URL de redireccionamiento.
- Anota el campo de usuario.
- Anote el nombre del certificado de firma.
- Anote el nombre del emisor de SAML.
- Anote el grupo de autenticación predeterminado.

### Apertura de puertos a través de los firewalls (DMZ de un solo salto)

Si su organización protege la red interna con una única DMZ e implementa NetScaler Gateway en la DMZ, abra los siguientes puertos a través de los firewalls. Si va a instalar dos dispositivos NetScaler Gateway en una implementación DMZ de doble salto, consulte Abrir los puertos apropiados en los firewalls.

#### Sobre el firewall entre la red no segura y la DMZ

- Abra un puerto TCP/SSL (predeterminado 443) en el firewall entre Internet y NetScaler Gateway. Los dispositivos de usuario se conectan a NetScaler Gateway en este puerto.

#### En el firewall entre la red segura

- Abra uno o más puertos apropiados en el firewall entre la DMZ y la red segura. NetScaler Gateway se conecta a uno o varios servidores de autenticación o a equipos que ejecutan Citrix Virtual Apps and Desktops en la red segura de estos puertos.
- Anote los puertos de autenticación.

  Abra solo el puerto adecuado para la configuración de NetScaler Gateway.

  - Para las conexiones LDAP, el valor predeterminado es el puerto TCP 389.
  - Para una conexión RADIUS, el valor predeterminado es el puerto UDP 1812. Anote los puertos de Citrix Virtual Apps and Desktops.
- Si utiliza NetScaler Gateway con Citrix Virtual Apps and Desktops, abra el puerto TCP 1494. Si habilita la fiabilidad de la sesión, abra el puerto TCP 2598 en lugar del 1494. Citrix recomienda mantener abiertos estos dos puertos.

### Citrix Virtual Desktops, Citrix Virtual Apps, la Interfaz Web o StoreFront

Realice las siguientes tareas si va a implementar NetScaler Gateway para proporcionar acceso a Citrix Virtual Apps and Desktops a través de la Interfaz Web o StoreFront. El plug-in de NetScaler Gateway no es necesario para esta implementación. Los usuarios acceden a aplicaciones y escritorios publicados a través de NetScaler Gateway mediante únicamente exploradores web y Citrix Receiver.

- Anote el FQDN o la dirección IP del servidor que ejecuta la Interfaz Web o StoreFront.
- Anote el FQDN o la dirección IP del servidor que ejecuta Secure Ticket Authority (STA) (solo para Interfaz Web).

### Citrix Endpoint Management

Realice las siguientes tareas si implementa Citrix Endpoint Management en su red interna. Si los usuarios se conectan a Endpoint Management desde una red externa, como Internet, los usuarios deben conectarse a NetScaler Gateway antes de acceder a las aplicaciones móviles, web y SaaS.

- Anote el FQDN o la dirección IP de Endpoint Management.
- Identificar aplicaciones web, SaaS y móviles iOS o Android a las que pueden acceder los usuarios.

### Implementación de DMZ de doble salto con Citrix Virtual Apps

Realice las siguientes tareas si va a implementar dos dispositivos NetScaler Gateway en una configuración DMZ de doble salto para admitir el acceso a los servidores que ejecutan Citrix Virtual Apps.

#### Citrix Gateway en la primera DMZ

La primera DMZ es la DMZ en el extremo exterior de la red interna (la más cercana a Internet o la red no segura). Los clientes se conectan a NetScaler Gateway en la primera DMZ a través del firewall que separa Internet de la DMZ. Recopile esta información antes de instalar NetScaler Gateway en la primera DMZ.

- Complete los elementos de la sección Conectividad de red básica de NetScaler Gateway de esta lista de comprobación para NetScaler Gateway.

  Al completar esos elementos, tenga en cuenta que la Interfaz 0 conecta este Citrix Gateway a Internet y la Interfaz 1 conecta este Citrix Gateway a Citrix Gateway en la segunda DMZ.

- Configure la información del segundo dispositivo DMZ en el dispositivo principal.

  Para configurar NetScaler Gateway como primer salto de la DMZ de doble salto, debe especificar el nombre de host o la dirección IP de NetScaler Gateway en la segunda DMZ del dispositivo en

la primera DMZ. Después de especificar cuándo se configura el proxy de NetScaler Gateway en el dispositivo en el primer salto, enlaza a NetScaler Gateway de forma global o a un servidor virtual.

- Anote el protocolo de conexión y el puerto entre dispositivos.

  Para configurar Citrix Gateway como el primer salto en la DMZ doble, debe especificar el protocolo de conexión y el puerto en el que Citrix Gateway, en la segunda DMZ, escucha las conexiones. El protocolo de conexión y el puerto son SOCKS con SSL (puerto predeterminado 443). El protocolo y el puerto deben estar abiertos a través del firewall que separa la primera DMZ y la segunda DMZ.

#### Citrix Gateway en la segunda DMZ

La segunda DMZ es la DMZ más cercana a su red interna y segura. NetScaler Gateway implementado en la segunda DMZ sirve como proxy para el tráfico ICA, atravesando la segunda DMZ entre los dispositivos de usuario externos y los servidores de la red interna.

- Complete las tareas de la sección Conectividad de red básica de NetScaler Gateway de esta lista de comprobación para NetScaler Gateway.

  Al completar esos elementos, tenga en cuenta que la Interfaz 0 conecta este Citrix Gateway a Citrix Gateway en la primera DMZ. La interfaz 1 conecta este NetScaler Gateway a la red segura.

## Actualización

January 26, 2024

Puede actualizar el software que reside en NetScaler Gateway cuando haya nuevas versiones disponibles. Puede buscar actualizaciones en el sitio web de Citrix. Solo puede actualizar a una nueva versión si sus licencias de NetScaler Gateway están bajo el programa Subscription Advantage cuando se publique la actualización. Puede renovar Subscription Advantage en cualquier momento. Para obtener más información, consulte el sitio web de Citrix Support.

La ruta de actualización y la información de productos compatibles también están disponibles en la Guía de actualización de Citrix.

Para obtener información sobre la última versión de mantenimiento de NetScaler Gateway, consulte Citrix Knowledge Center.

### Para comprobar si hay actualizaciones de software

1. Vaya al sitio Web de Citrix.
2. Haga clic en **My Account** e inicie sesión.
3. Haga clic en **Descargas**.
4. En Buscar descargas, seleccione **NetScaler Gateway**.
5. En **Seleccionar tipo de descarga**, seleccione **Software del producto** y, a continuación, haga clic en **Buscar**.
   También puede seleccionar **Virtual Appliances** para descargar NetScaler ADC VPX. Cuando se selecciona esta opción, se recibe una lista de software para la máquina virtual para cada hipervisor.
6. En la página NetScaler Gateway, expanda **NetScaler ADC Gateway o Access Gateway**.
7. Haga clic en la versión del software de dispositivo que quiere descargar.
8. En la página del software del dispositivo de la versión que desea descargar, seleccione el dispositivo virtual y, a continuación, haga clic en **Descargar** .
9. Siga las instrucciones en pantalla para descargar el software.

Cuando se descarga el software en el equipo, puede utilizar el Asistente de actualización o el símbolo del sistema para instalar el software.

### Para actualizar Citrix Gateway mediante el asistente de actualización

1. En la utilidad de configuración, en la **ficha Configuración**, en el panel de navegación, haga clic en Sistema.
2. En el panel de detalles, haga clic en **Asistente de actualización**.
3. Haga clic en **Next** y siga las instrucciones del asistente.

### Para actualizar Citrix Gateway mediante una línea de comandos

1. Para cargar el software en NetScaler Gateway, utilice un cliente FTP seguro, como WinSCP, para conectarse al dispositivo.
2. Copie el software de su equipo al directorio /var/nsinstall del dispositivo.
3. Utilice un cliente de Secure Shell (SSH), como PuTTY, para abrir una conexión SSH con el dispositivo.
4. Inicie sesión en NetScaler Gateway.
5. En una línea de comandos, escriba: `shell`
6. Para cambiar al directorio nsinstall, en una línea de comandos, escriba: `cd /var/nsinstall`

7. Para ver el contenido del directorio, escriba: `ls`
8. Para desempaquetar el software, escriba: tar -xvzf build_X_XX.tgz

   donde build_x_xx.tgz es el nombre de la compilación a la que quiere actualizar el software.
9. Para iniciar la instalación, en el símbolo del sistema, escriba: `./installns`
10. Cuando finalice la instalación, reinicie NetScaler Gateway.

Después de reiniciar NetScaler Gateway, para comprobar que la instalación se ha realizado correctamente, inicie la utilidad de configuración. La versión de NetScaler Gateway que se encuentra en el dispositivo aparece en la esquina superior derecha.

## Instale el sistema

January 26, 2024

Cuando recibe el dispositivo NetScaler Gateway, desempaqueta el dispositivo y prepara el sitio y el bastidor. Una vez que determine que la ubicación en la que instala el dispositivo cumple con los estándares medioambientales y que el bastidor de servidores está instalado de acuerdo con las instrucciones, instale el hardware. Después de montar el dispositivo, lo conecta a la red, a una fuente de alimentación y al terminal de consola que utiliza para la configuración inicial. Después de encender el dispositivo, realiza la configuración inicial y asigna direcciones IP de administración y de red. Asegúrese de observar las precauciones y advertencias enumeradas con las instrucciones de instalación.

Al instalar un dispositivo virtual NetScaler ADC VPX, primero debe adquirir la imagen del dispositivo virtual e instalarla en un hipervisor u otro monitor de máquina virtual.

Citrix recomienda utilizar el tema Lista de comprobación previa a la instalación de NetScaler Gateway para que pueda tomar nota de la configuración antes de intentar configurar un dispositivo NetScaler Gateway. La lista de comprobación incluye información sobre la instalación de NetScaler Gateway y un dispositivo.

## Configurar Citrix Gateway

January 26, 2024

Después de configurar la configuración de red básica en NetScaler Gateway, configure la configuración detallada para que los usuarios puedan conectarse a los recursos de red de la red segura. Esta configuración incluye:

- Servidores virtuales. Puede configurar varios servidores virtuales en Citrix Gateway, lo que le permite crear diferentes políticas según el escenario de usuario que necesite implementar. Cada servidor virtual tiene su propia dirección IP, certificado y conjunto de directivas. Por ejemplo, puede configurar un servidor virtual y restringir a los usuarios a los recursos de red de la red interna en función de su pertenencia a grupos y de las directivas que vincule a los servidores virtuales. Puede crear servidores virtuales mediante los métodos siguientes:
  - Asistente de configuración rápida
  - Asistente de NetScaler Gateway
  - Utilidad de configuración
- Alta disponibilidad. Puede configurar la alta disponibilidad cuando implementa dos dispositivos NetScaler Gateway en la red. Si el dispositivo principal falla, el dispositivo secundario puede tomar el control sin afectar a las sesiones de usuario.
- Certificados. Puede utilizar certificados para proteger las conexiones de los usuarios con NetScaler Gateway. Al crear una solicitud de firma de certificado (CSR), agrega el nombre de dominio completo al certificado. Puede enlazar certificados a servidores virtuales.
- Autenticación. NetScaler Gateway admite varios tipos de autenticación, incluidos LDAP local, RADIUS, SAML, certificados de cliente y TACACS+. Además, puede configurar la autenticación en cascada y en dos fases.
  Nota: Si utiliza RSA, Safeword o Gemalto Protiva para la autenticación, configure estos tipos mediante RADIUS.
- Conexiones de usuarios. Puede configurar las conexiones de usuario mediante perfiles de sesión. Dentro del perfil, puede determinar los plug-ins con los que los usuarios pueden iniciar sesión, junto con cualquier restricción que los usuarios puedan necesitar. A continuación, puede crear una directiva con un perfil. Puede enlazar directivas de sesión a usuarios, grupos y servidores virtuales.
- Página de inicio. Puede utilizar la interfaz de acceso predeterminada como página de inicio o crear una página principal personalizada. La página principal aparece después de que los usuarios inicien sesión correctamente en NetScaler Gateway.
- Análisis de endpoints. Puede configurar directivas en NetScaler Gateway que comprueban el dispositivo del usuario en busca de software, archivos, entradas de registro, procesos y sistemas operativos cuando los usuarios inician sesión. El análisis de puntos finales le permite aumentar la seguridad de su red al exigir que el dispositivo del usuario cuente con el software necesario.

## Usar la utilidad de configuración

January 26, 2024

La utilidad de configuración permite configurar la mayoría de los parámetros de NetScaler Gateway. Utiliza un explorador web para acceder a la utilidad de configuración.

### Para iniciar sesión en la utilidad de configuración

1. En un explorador web, escriba la dirección IP del sistema de NetScaler Gateway, como `http://192.168.100.1`.
   Nota: NetScaler Gateway está preconfigurado con una dirección IP predeterminada de 192.168.100.1 y una máscara de subred
   255.255.0.0.
2. En Nombre de usuario y contraseña, escriba nsroot
3. En Tipo de implementación, seleccione NetScaler Gateway y luego haga clic en Iniciar sesión.

Al iniciar sesión en la utilidad de configuración por primera vez, el panel se abre de forma predeterminada en la ficha Inicio. En la ficha Inicio, puede utilizar el Asistente de configuración rápida para configurar la configuración de un servidor virtual, autenticación, certificados y Citrix Endpoint Management. También puede configurar los valores de StoreFront o de Interfaz Web en el Asistente de configuración rápida.

Para obtener más información sobre la configuración de NetScaler Gateway, consulte:

- Configuración de los ajustes iniciales mediante el Asistente de configuración.
- Configurar parámetros con el Asistente de configuración rápida
- Configuración de los ajustes mediante el Asistente de NetScaler Gateway.

## Directivas y perfiles en Citrix Gateway

January 26, 2024

Las directivas y los perfiles de NetScaler Gateway permiten administrar e implementar los valores de configuración en situaciones o condiciones específicas. Una política individual establece o define los ajustes de configuración que entran en vigor cuando se cumple un conjunto específico de condiciones. Cada directiva tiene un nombre único y puede tener un perfil vinculado a la directiva.

Para obtener más información acerca de las políticas con Citrix Gateway, consulte los siguientes temas:

## Cómo funcionan las políticas

January 26, 2024

Una directiva consiste en una condición booleana y un conjunto de ajustes denominados perfil. La condición se evalúa en tiempo de ejecución para determinar si se debe aplicar la política.

Un perfil es un conjunto de configuraciones que utilizan parámetros específicos. El perfil puede tener cualquier nombre y puede reutilizarlo en más de una directiva. Puede configurar varias opciones dentro del perfil, pero solo puede incluir un perfil por directiva.

Puede enlazar directivas, con las condiciones y los perfiles configurados, a servidores virtuales, grupos, usuarios o de forma global. Las directivas se denominan por el tipo de configuración que controlan. Por ejemplo, en una política de sesión, puede controlar la forma en que los usuarios inician sesión y la cantidad de tiempo que los usuarios pueden permanecer conectados.

Si utiliza NetScaler Gateway con Citrix Virtual Apps, los nombres de directiva de NetScaler Gateway se envían a Citrix Virtual Apps como filtros. Al configurar Citrix Gateway para que funcione con Citrix Virtual Apps y SmartAccess, se configuran los siguientes parámetros en Citrix Virtual Apps:

- Nombre del servidor virtual configurado en el dispositivo. El nombre se envía a Citrix Virtual Apps como nombre de comunidad de NetScaler Gateway.
- Los nombres de las directivas de sesión o autenticación previa se envían como nombres de filtro.

Para obtener más información sobre la configuración de Citrix Gateway para que funcione con Citrix Endpoint Management, consulte Configuración de los parámetros de su entorno de Citrix Endpoint Management .

Para obtener más información sobre la configuración de Citrix Gateway para que funcione con Citrix Virtual Apps and Desktops, consulte Acceso a los recursos de Citrix Virtual Apps y Citrix Virtual Desktops con la interfaz web e Integración con Citrix Endpoint Management o StoreFront.

Para obtener más información sobre las directivas de autenticación previa, consulte Configuración de directivas de endpoint.

## Definir las prioridades de las directivas

January 26, 2024

Las directivas se priorizan y evalúan en el orden en que está vinculada la directiva.

Los dos métodos siguientes determinan la prioridad de la directiva:

- Nivel al que está vinculada la directiva: globalmente, servidor virtual, grupo o usuario. Los niveles de directivas se clasifican del más alto al más bajo de la siguiente manera:
  - Usuario (prioridad máxima)
  - Grupo
  - Servidor virtual
  - Global (prioridad más baja)
- La prioridad numérica tiene prioridad independientemente del nivel al que esté vinculada la directiva. Si una directiva vinculada globalmente tiene un número de prioridad de uno y otra directiva vinculada a un usuario tiene un número de prioridad de dos, la directiva global tiene prioridad. Un número de prioridad más bajo otorga a la directiva una mayor prioridad.

## Configurar directivas condicionales

January 26, 2024

Al configurar directivas, puede utilizar cualquier expresión booleana para expresar la condición de cuándo se aplica la directiva. Al configurar directivas condicionales, puede utilizar cualquiera de las expresiones del sistema disponibles, como las siguientes:

- Cadenas de seguridad del cliente
- Información de red
- Encabezados HTTP y cookies
- Hora del día
- Valores de certificados de cliente

También puede crear directivas para aplicarlas solo cuando el dispositivo de usuario cumpla criterios específicos, como una directiva de sesión para SmartAccess.

Otro ejemplo de configuración de una directiva condicional es la variación de la directiva de autenticación para los usuarios. Por ejemplo, puede exigir que los usuarios que se conectan con el complemento Citrix Gateway desde fuera de la red interna, como desde el ordenador de su casa o mediante Micro VPN desde un dispositivo móvil, se autentiquen mediante LDAP y que los usuarios que se conectan a través de una WAN se autentiquen mediante RADIUS.

**Nota**: No puede usar condiciones de política basadas en los resultados del análisis de terminales si la regla de política está configurada como parte de la configuración de seguridad de un perfil de sesión.

## Crear directivas en NetScaler Gateway

January 26, 2024

Puede utilizar la utilidad de configuración para crear directivas. Después de crear una directiva, la vincula al nivel adecuado: usuario, grupo, servidor virtual o global. Cuando vincula una directiva a uno de estos niveles, los usuarios reciben la configuración dentro del perfil si se cumplen las condiciones de la directiva. Cada directiva y perfil tiene un nombre único.

Si tiene Citrix Endpoint Management o StoreFront como parte de la implementación, puede utilizar el Asistente de configuración rápida para configurar los ajustes de esta implementación. Para obtener más información sobre el asistente, consulte Configuración de los ajustes con el Asistente de configuración rápida.

## Configurar expresiones del sistema

January 26, 2024

Una expresión del sistema especifica las condiciones en las que se aplica la directiva. Por ejemplo, las expresiones de una directiva de autenticación previa se aplican mientras un usuario inicia sesión. Las expresiones de una directiva de sesión se evalúan y aplican después de autenticar al usuario e iniciar sesión en NetScaler Gateway.

Las expresiones de NetScaler Gateway incluyen:

- Expresiones generales que limitan los objetos que los usuarios pueden utilizar al establecer una conexión con NetScaler Gateway
- Expresiones de seguridad del cliente que definen el software, los archivos, los procesos o los valores del registro que deben instalarse y ejecutarse en el dispositivo del usuario
- Expresiones basadas en red que restringen el acceso según la configuración de red

NetScaler Gateway también se puede utilizar como dispositivo NetScaler ADC. Algunas expresiones del dispositivo son más aplicables a NetScaler ADC. Las expresiones generales y basadas en red se utilizan habitualmente con NetScaler ADC y no suelen utilizarse con NetScaler Gateway. Las expresiones de seguridad del cliente se utilizan en NetScaler Gateway para determinar que los elementos correctos están instalados en el dispositivo del usuario.

### Configuración de expresiones de seguridad de clientes

Las expresiones son un componente de una directiva. Una expresión representa una condición única que se evalúa con respecto a una solicitud o una respuesta. Puede crear una cadena de seguridad de expresión sencilla para comprobar si hay condiciones, tales como:

- Sistema operativo del dispositivo de usuario, incluidos los service packs
- Definiciones de virus y versión del software antivirus
- Archivos
- Procesos
- Valores de registro
- Certificados de usuario

## Crear expresiones simples y compuestas

January 26, 2024

Las expresiones simples comprueban una sola condición. Un ejemplo de una expresión simple es:

REQ.HTTP.URL == `HTTP://www.mycompany.com`

---

Las expresiones compuestas comprueban si hay varias condiciones. Las expresiones compuestas se crean conectándose a uno o más nombres de expresión mediante los operadores lógicos && y

---

Las expresiones compuestas se pueden clasificar de la siguiente manera:

- Expresiones con nombre. Como entidad independiente, otras políticas pueden reutilizar una expresión con nombre y formar parte de la política. Las expresiones con nombre se configuran a nivel del sistema en la utilidad de configuración. Puede usar una expresión con nombre predefinida en la política o crear una propia.
- Expresiones en línea. Una expresión en línea es aquella que se crea dentro de la política que es específica de la política.

### Para crear una expresión con nombre

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda AppExpert y, a continuación, haga clic en Expresiones.
2. En el panel de detalles, haga clic en Agregar.

3. En el cuadro de diálogo Crear expresión de política, en Nombre de expresión, escriba un nombre para la expresión.
4. Para crear una expresión, haga clic en Agregar.
5. Lleve a cabo una de las siguientes acciones:

    a) En Expresión de uso frecuente, seleccione una expresión de la lista, haga clic en Aceptar, en Crear y, a continuación, en Cerrar.
    b) En Construir expresión, seleccione los parámetros de la cadena de expresión, haga clic en Aceptar, en Crear y, a continuación, en Cerrar.

## Agregar expresiones personalizadas

January 26, 2024

Si va a crear una política, puede crear una expresión personalizada mientras configura la política. Por ejemplo, está creando un perfil de sesión para permitir a los usuarios iniciar sesión con el plug-in de NetScaler Gateway, establecer un límite de tiempo para la sesión y permitir el inicio de sesión único con Windows. Después de crear el perfil de sesión, en el cuadro de diálogo Crear política de sesión, puede crear la expresión. El siguiente ejemplo muestra una expresión que comprueba si hay un proceso y una aplicación antivirus:

CLIENT.APPLICATION.PROCESS (ccapp.exe) EXISTE -frequent 5 && CLIENT.APPLICATION.AV (Symantec).VERSION==14.20.0.29 -freshness 5 && ns_true

## Usar operadores y operandos en expresiones de directiva

January 26, 2024

Un operador es un símbolo que identifica la operación (matemática, booleana o relacional, por ejemplo) que manipula uno o más objetos u operandos. La primera sección de este tema define los operadores que puede usar y proporciona una definición. En la segunda sección se enumeran los operadores que puede usar con calificadores específicos, como método, URL y consulta.

### Operadores y definiciones

En esta sección se definen los operadores que se pueden usar al crear una expresión de política y se proporciona una descripción del operador.

- ==,! =, EQ, NUEVO

  Estos operadores comprueban las coincidencias exactas. Distinguen entre mayúsculas y minúsculas («cmd.exe» NO ES IGUAL a «cMd.exe»). Estos operadores son útiles para crear permisos que permitan determinadas cadenas que cumplan una sintaxis exacta, pero para excluir otras cadenas.

- GT

  Este operador se usa para comparaciones numéricas. Se usa en la longitud de las URL y las cadenas de consulta.

- CONTIENE, NO CONTIENE

  Estos operadores comprueban el calificador especificado para determinar si la cadena especificada está contenida en el calificador. Estos operadores no distinguen entre mayúsculas y minúsculas.

- EXISTE, NO EXISTE

  Estos operadores comprueban la existencia de un calificador en particular. Por ejemplo, estos operadores se pueden aplicar a los encabezados HTTP para determinar si existe un encabezado HTTP determinado o si existe la consulta URL.

- CONTENIDOS

  Este operador comprueba si el calificador existe y si tiene contenido (es decir, si existe un encabezado y tiene un valor asociado, sin importar cuál sea el valor).

### Calificadores, operadores, operandos, acciones y ejemplos

En esta sección se muestran los parámetros que puede usar para los operadores y operandos. Cada elemento comienza con el calificador y, a continuación, muestra el operador y el operando asociados, describe la acción que lleva a cabo la expresión y proporciona un ejemplo.

- Método

  Operador: EQ, NEQ
  Operandos: Obligatorio:

  - Métodos HTTP estándar
  - Métodos compatibles
  - **Acciones GET, HEAD, POST, PUT, DELETE OPTIONS, TRACE, CONNECT** verifica el método de solicitud entrante con el método configurado.
    Ejemplo: Método EQ GET

URL

- Operador: EQ, NEQ
  Operandos: Obligatorio: URL (Formato:/[prefix] [*] [.suffix])
  Acciones: verifica la URL entrante con la URL configurada.
  Ejemplo:
  URL EQ/foo*.asp
  URL EQ /foo *
  URL EQ /*.asp
  URL EQ /foo.asp

- Operador: CONTAINS, NOTCONTAINS
  Operandos: Obligatorio: cualquier cadena (entre comillas)
  Acciones: verifica la URL entrante para comprobar la presencia del patrón configurado. (Incluye URL y consulta de URL).
  Ejemplo: URL CONTIENE 'ZZZ'

- URL LEN

  Operador: GT
  Operandos: Obligatorio: Longitud (como valor entero)
  Acciones: Compara la longitud de la URL entrante con la longitud configurada. (Incluye URL y consulta de URL).
  Ejemplo: URLLEN GT 60

- CONSULTA DE URL

  Operador: CONTAINS, NOTCONTAINS
  Operandos: Obligatorio: cualquier cadena (entre comillas).
  Opcional: acciones de longitud y compensación
  :
  verifica la presencia del patrón configurado en la consulta URL entrante.
  Se usa de manera similar a CONTENTS.
  Si no se especifica ninguna opción, se utiliza la consulta URL completa después del patrón.
  Si las opciones están presentes, solo la longitud de la consulta después de utilizar el patrón.
  El desfase se utiliza para indicar desde dónde empezar la búsqueda del patrón.
  Ejemplo: URLQUERY CONTIENE 'ZZZ'

- LEN DE CONSULTA DE URL

  Operador: GT
  Operandos: Obligatorio: Longitud (como valor entero)
  Acciones: compara la longitud de la consulta URL entrante con la longitud configurada.
  Ejemplo: URLQUERYLN GT 60

- TOKENS DE URL

Operador: EQ, NEQ
Operandos: Requerido: tokens de URL (tokens de URL admitidos =, +,%,!, &,?).
Acciones: compara la URL entrante con la presencia de tokens configurados. Debe escribirse una barra invertida (\) delante del signo de interrogación.
Ejemplo: URLTOKENS EQ '%, +, &,\? '

- VERSIÓN

  Operador: EQ, NEQ
  Operandos: Obligatorio: versiones HTTP estándar. Cadenas de versiones HTTP válidas HTTP/1.0, HTTP/1.1
  Acciones: compara la versión HTTP de la solicitud entrante con la versión HTTP configurada.
  Ejemplo: VERSION EQ HTTP/1.1

Header

- Operador: EXISTS, NOTEXISTS
  Operandos: Ninguno
  Acciones: examina la solicitud entrante para detectar la presencia del encabezado HTTP.
  Ejemplo: La cookie de encabezado EXISTE

- **Operador: CONTAINS, NOTCONTAINSOperandos: Obligatorio: cualquier cadena (entre comillas).Opci**
  verifica la solicitud entrante para detectar la presencia de un patrón configurado en el encabezado específico. Se usa de manera similar a CONTENTS. Si no se especifica ninguna opción, se utiliza todo el valor del encabezado HTTP después del patrón. Si las opciones están presentes, solo se utiliza la longitud del encabezado después del patrón. El desfase se utiliza para indicar desde dónde empezar la búsqueda del patrón.
  Ejemplo: Cookie de encabezado CONTIENE "&sid"

- Operador: CONTENTS
  Operandos: Opcional: longitud y compensación
  Acciones: utiliza el contenido del encabezado HTTP. Si no se especifica ninguna opción, se utiliza todo el valor del encabezado HTTP. Si hay opciones disponibles, solo se utiliza la longitud del encabezado empezando por el desplazamiento.
  Ejemplo: Header User-Agent CONTENTS

- SOURCEIP

  Operador: EQ, NEQ
  Operandos: Obligatorio: dirección
  IP Opcional: máscara
  de subred Acciones: verifica la dirección IP de origen de la solicitud entrante con la dirección IP configurada. Si se especifica la máscara de subred opcional, la solicitud entrante se verifica

con la dirección IP y la máscara de subred configuradas.
Ejemplo: Sourceip EQ 192.168.100.0 -netmask 255.255.255.0

- DESTIP

  Operador: EQ, NEQ
  Operandos: Obligatorio: dirección
  IP Opcional: máscara
  de subred Acciones: verifica la dirección IP de destino de la solicitud entrante con la dirección IP configurada. Si se especifica la máscara de subred opcional, la solicitud entrante se verifica con la dirección IP y la máscara de subred configuradas.
  Ejemplo: Sourceip EQ 192.168.100.0 -netmask 255.255.255.0

- SOURCEPORT

  Operador: EQ, NEQ
  Operandos: Obligatorio: número
  de puerto Opcional: rango
  de puertos Acciones: verifica el número de puerto de origen de la solicitud entrante con el número de puerto configurado.
  Ejemplo: SOURCEPORT EQ 10—20

- DESTPORT

  Operador: EQ, NEQ
  Operandos: Obligatorio: número
  de puerto Opcional: rango
  de puertos Acciones: verifica el número de puerto de destino de la solicitud entrante con el número de puerto configurado.
  Ejemplo: DESTPORT NEQ 80

- CLIENT.SSL.VERSION

  Operador: EQ, NEQ
  Operandos: Obligatorio: versión
  SSL Acciones: Comprueba la versión de la versión SSL o TLS utilizada en la conexión segura.
  Ejemplo: CLIENT.SSL.VERSION EQ SSLV3

- CLIENT.CIPHER.TYPE

  Operador: EQ, NEQ
  Operandos: Obligatorio: Tipo
  de cifrado de cliente Acciones: Comprueba el tipo de cifrado que se utiliza (exportación o no exportación).
  Ejemplo: CLIENT.CIPHER.TYPE EQ EXPORT

- CLIENT.CIPHER.BITS

  Operador: EQ, NEQ, GE, LE, GT, LT
  Operandos: Obligatorio: bits
  de cifrado del cliente Acciones: Comprueba la fortaleza de la clave del cifrado que se está utilizando.
  Ejemplo: CLIENT.CIPHER.BITS GE 40

- CLIENT.CERT

  Operador: EXISTS, NOTEXISTS
  Operandos: ninguno
  Acciones: Comprueba si el cliente envió un certificado válido durante el protocolo de enlace SSL.
  Ejemplo: CLIENT.CERT EXISTS

- CLIENT.CERT.VERSION

  Operador: EQ, NEQ, GE, LE, GT, LT
  Operandos: versión
  del certificado del cliente Acciones: Comprueba la versión del certificado del cliente.
  Ejemplo: CLIENT.CERT.VERSION EQ 2

- CLIENT.CERT.SERIALNUMBER

  Operador: EQ, NEQ
  Operandos: Obligatorio: número
  de serie del certificado de cliente Acciones: Comprueba el número de serie del certificado de cliente. El número de serie se trata como una cadena.
  Ejemplo: CLIENT.CERT.SER IALNUMBER EQ 2343323

- CLIENT.CERT.SIGALGO

  Operador: EQ, NEQ
  Operandos: Obligatorio: algoritmo de firma de certificados de cliente.
  Acciones: comprueba el algoritmo de firma utilizado en el certificado del cliente.
  Ejemplo: CLIENT.CERT.SIGALGO EQ MD5 con cifrado RSA

- CLIENT.CERT.SUBJECT

  Operador: CONTIENE, NO
  CONTIENE Operandos: Obligatorio: Asunto
  del certificado de cliente Opcional: longitud, compensación
  Acciones: Comprueba el campo de asunto del certificado de cliente.
  Ejemplo: CLIENT.CERT.SUBJECT CONTIENE CN= Access_Gateway

- CLIENT.CERT.ISSUER

  Operador: CONTIENE, NO
  CONTIENE Operandos: Obligatorio: emisor del certificado de
  cliente Opcional: longitud, compensación
  Acciones: Comprueba el campo emisor del certificado de cliente.
  Ejemplo: CLIENT.CERT.ISSUER CONTIENE O=Verisign

- CLIENT.CERT.VALIDFROM

  Operador: EQ, NEQ, GE, LE, GT, LT
  Operandos: Obligatorio: Fecha
  Acciones: Comprueba la fecha a partir de la cual el certificado de cliente es válido.
  Los formatos de fecha válidos son:
  martes, 05 de noviembre de 1994 08:12:31 GMT
  martes, 05-nov-94 08:12:31 GMT
  martes 14 de noviembre 08:12:31 1994
  Ejemplo: CLIENT.CERT.VALIDFROM GE 'Tue 14 de noviembre 08:12:31 1994'

- CLIENT.CERT.VALIDTO

  Operador: EQ, NEQ, GE, LE, GT, LT
  Operandos: Obligatorio: Fecha
  Acciones: Comprueba la fecha hasta la cual el certificado de cliente es válido.
  Los formatos de fecha válidos son:
  martes, 05 de noviembre de 1994 08:12:31 GMT
  martes, 05-nov-94 08:12:31 GMT
  martes 14 de noviembre 08:12:31 1994
  Ejemplo: CLIENT.CERT.VALIDTO GE 'Tue 14 de noviembre 08:12:31 1994'

## Ver la configuración de NetScaler Gateway

January 26, 2024

Al realizar cambios de configuración en NetScaler Gateway, los cambios se guardan en archivos de registro. Puede ver varios tipos de ajustes de configuración:

- Configuración guardada. Puede ver la configuración que ha guardado en NetScaler Gateway.
- Configuración en ejecución. Puede ver la configuración activa, como un servidor virtual o una directiva de autenticación, que ha configurado pero que no ha guardado como configuración guardada en NetScaler Gateway.

- Configuración en ejecución versus configuración guardada. Puede comparar en paralelo la configuración en ejecución y guardada en NetScaler Gateway.

También puede borrar los valores de configuración de NetScaler Gateway.

Importante: Si decide borrar la configuración de NetScaler Gateway, se quitan los certificados, los servidores virtuales y las directivas. Citrix recomienda no borrar la configuración.

## Guardar la configuración de Citrix Gateway

January 26, 2024

Puede guardar la configuración actual de NetScaler Gateway en un equipo de la red, ver la configuración actual en ejecución y comparar las configuraciones guardadas y en ejecución.

### Para guardar la configuración en NetScaler Gateway

1. En la utilidad de configuración, encima del panel de detalles, haga clic en el icono Guardar y, a continuación, haga clic en Sí.

### Para ver y guardar el archivo de configuración en NetScaler Gateway

La configuración guardada es la configuración que se guarda en un archivo de registro de NetScaler Gateway, como la configuración de servidores virtuales, directivas, direcciones IP, usuarios, grupos y certificados.

Al configurar la configuración en NetScaler Gateway, puede guardarla en un archivo del equipo. Si necesita volver a instalar el software NetScaler Gateway o si elimina accidentalmente alguna configuración, puede utilizar este archivo para restaurar la configuración. Si necesita restaurar la configuración, puede copiar el archivo en NetScaler Gateway y reiniciar el dispositivo mediante la interfaz de línea de comandos o un programa, como WinSCP, para copiar el archivo en NetScaler Gateway.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Diagnóstico.
2. En el panel de detalles, en Ver configuración, haga clic en Configuración guardada.
3. En el cuadro de diálogo Configuración guardada, haga clic en Guardar texto de salida en un archivo, asigne un nombre al archivo y, a continuación, haga clic en Guardar.
   Nota: Citrix recomienda guardar el archivo con el nombre de archivo ns.conf.

### Para ver la configuración actual en ejecución

Cualquier cambio en NetScaler Gateway que se produzca sin esfuerzo por guardarlos se denomina configuración en ejecución. Esta configuración está activa en NetScaler Gateway, pero no se guarda en el dispositivo. Si ha configurado opciones adicionales, como una directiva, un servidor virtual, usuarios o grupos, puede ver esta configuración en la configuración en ejecución.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Diagnóstico.
2. En el panel de detalles, en Ver configuración, haga clic en Configuración en ejecución.

### Para comparar la configuración guardada y en ejecución

Puede ver qué configuración se guarda en el dispositivo y compararla con la configuración en ejecución. Puede elegir guardar la configuración en ejecución o realizar cambios en la configuración.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Diagnóstico.
2. En el panel de detalles, en Ver configuración, haga clic en Guardado v/s en ejecución.

## Borrar la configuración de NetScaler Gateway

January 26, 2024

Puede borrar la configuración de NetScaler Gateway. Puede elegir entre los tres niveles de configuración siguientes para borrar:

Importante: Citrix recomienda guardar la configuración antes de borrar la configuración de NetScaler Gateway.

- Básico. Borra toda la configuración del dispositivo, excepto la dirección IP del sistema, la puerta de enlace predeterminada, las direcciones IP asignadas, las direcciones IP de subred, la configuración de DNS, la configuración de red, la configuración de alta disponibilidad, la contraseña administrativa y la configuración de funciones y modos.
- Extendida. Borra toda la configuración excepto la dirección IP del sistema, las direcciones IP asignadas, las direcciones IP de subred, la configuración DNS y las definiciones de alta disponibilidad.
- Completo. Restaura la configuración a la configuración original de fábrica, con exclusión de la dirección IP del sistema (NSIP) y la ruta predeterminada, necesarias para mantener la conectividad de red con el dispositivo.

Al borrar toda o parte de la configuración, la configuración de la función se establece en la configuración predeterminada de fábrica.

Al borrar la configuración, los archivos almacenados en NetScaler Gateway, como certificados y licencias, no se quitan. El archivo ns.conf no se modifica. Si quiere guardar la configuración antes de borrar la configuración, guarde la configuración en su equipo primero. Si guarda la configuración, puede restaurar el archivo ns.conf en NetScaler Gateway. Después de restaurar el archivo en el dispositivo y reiniciar NetScaler Gateway, se restaura cualquier configuración de ns.conf.

Las modificaciones de los archivos de configuración, como rc.conf, no se revierten.

Si tiene un par de alta disponibilidad, ambos dispositivos NetScaler Gateway se modifican de forma idéntica. Por ejemplo, si borra la configuración básica de un dispositivo, los cambios se propagan al segundo dispositivo.

### Para borrar la configuración de NetScaler Gateway

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Diagnóstico.
2. En el panel de detalles, en Mantenimiento, haga clic en Borrar configuración.
3. En Nivel de configuración, seleccione el nivel que quiere borrar y, a continuación, haga clic en Ejecutar.

## Configurar NetScaler Gateway mediante asistentes

January 26, 2024

NetScaler Gateway tiene los seis asistentes siguientes que puede utilizar para configurar los ajustes del dispositivo:

- El asistente de configuración por primera vez aparece cuando inicia sesión en el dispositivo Citrix Gateway por primera vez.
- El asistente de configuración le ayuda a configurar los parámetros básicos de Citrix Gateway por primera vez.
- La configuración integrada de Citrix Endpoint Management le ayuda a configurar el entorno de NetScaler Gateway y Citrix Endpoint Management.
- El asistente de configuración rápida le ayuda a configurar las políticas, expresiones y parámetros correctos para las conexiones a Citrix Endpoint Management, StoreFront y la Interfaz Web.
- El asistente de NetScaler Gateway le ayuda a configurar la configuración específica de NetScaler Gateway.

- El asistente de aplicaciones publicadas le ayuda a configurar los parámetros de las conexiones de usuario mediante Citrix Receiver.

### Cómo funciona el asistente de configuración inicial

Cuando termina de instalar y configurar la configuración inicial en el dispositivo NetScaler Gateway, cuando inicia sesión en la utilidad de configuración por primera vez, aparece el Asistente de configuración por primera vez si no se cumplen las siguientes condiciones:

- No ha instalado una licencia en el dispositivo.
- No ha configurado una subred ni una dirección IP asignada.
- Si la dirección IP predeterminada de los dispositivos es 192.168.100.1.

### Cómo funciona el asistente de configuración

Utilice el Asistente de configuración para configurar la siguiente configuración inicial en el dispositivo:

- Dirección IP del sistema y máscara de subred
- Dirección IP asignada y máscara de subred
- Nombre de host
- Puerta de enlace predeterminada
- Licencias

Nota: Antes de ejecutar el Asistente de configuración, descargue las licencias del sitio web de Citrix. Para obtener más información, consulte
Licencias de NetScaler Gateway

### Cómo funciona la configuración integrada de Citrix Endpoint Management

Puede implementar NetScaler Gateway con MDM de Citrix Endpoint Management, que ofrece la capacidad de escalar, garantizar la alta disponibilidad de las aplicaciones y mantener la seguridad. Para utilizar la configuración de Citrix Endpoint Management, debe instalar la versión 10.1, compilación 120.1316.e.

La configuración integrada de Citrix Endpoint Management crea lo siguiente:

- Servidores de equilibrio de carga para Device Manager.
- Servidores de equilibrio de carga para Microsoft Exchange con filtrado de correo electrónico.
- Servidores de equilibrio de carga para ShareFile.

Para obtener más información sobre cómo crear ajustes con la configuración integrada de Citrix Endpoint Management, consulte Configuración de las opciones del entorno de Citrix Endpoint Management

### Cómo funciona el asistente de configuración rápida

El asistente de configuración rápida le permite configurar varios servidores virtuales en NetScaler Gateway. Puede agregar, modificar y quitar servidores virtuales.

El asistente de configuración rápida permite una configuración perfecta para las siguientes implementaciones:

- Conexiones de la Interfaz Web a Citrix Virtual Apps and Desktops, con la capacidad de configurar varias instancias de Secure Ticket Authority (STA)
- Solo Citrix Endpoint Management
- Solo StoreFront
- Citrix Endpoint Management y StoreFront juntos

El asistente de configuración rápida le permite configurar las siguientes opciones en el dispositivo:

- Nombre del servidor virtual, dirección IP y puerto
- Redirección de un puerto no seguro a un puerto seguro
- Servidor LDAP
- Servidor RADIUS
- Certificados
- Servidor DNS
- Citrix Endpoint Management y Citrix Virtual Apps and Desktops

  **Nota**: Para habilitar el inicio de sesión único, debe habilitar manualmente la opción Inicio de **sesión único en aplicaciones web** en la ficha **Crear perfil de sesión de NetScaler Gateway > Experiencia del cliente** para la acción de sesión.

NetScaler Gateway admite conexiones de usuario directamente con Citrix Endpoint Management, lo que proporciona a los usuarios acceso a sus aplicaciones web, SaaS y móviles, además de acceso a ShareFile. También puede configurar la configuración de StoreFront, lo que permite a los usuarios acceder a sus aplicaciones y escritorios virtuales basados en Windows.

Al ejecutar el Asistente de configuración rápida, se crean las siguientes directivas en función de la configuración de Citrix Endpoint Management, StoreFront e Interfaz Web:

- Directivas de sesión, incluidas directivas y perfiles para Receiver, Receiver para Web, el plug-in de NetScaler Gateway y el agente de vecindad de programas

- Acceso sin cliente
- Autenticación LDAP y RADIUS

### Cómo funciona el asistente Citrix Gateway

Utilice el asistente de NetScaler Gateway para configurar la siguiente configuración en el dispositivo:

- Servidores virtuales
- Certificados
- Proveedores de servicios de nombres
- Autenticación
- Autorización
- Redirección de puertos
- Acceso sin cliente
- Acceso sin cliente para SharePoint

### Cómo funciona el asistente de aplicaciones publicadas

Utilice el asistente Aplicaciones publicadas para configurar NetScaler Gateway para que se conecte a los servidores que ejecutan Citrix Virtual Apps and Desktops en la red interna. Con el asistente Aplicaciones publicadas, puede:

- Seleccione un servidor virtual para las conexiones a la comunidad de servidores.
- Configure la configuración de las conexiones de usuario para la Interfaz Web o StoreFront, el inicio de sesión único y Secure Ticket Authority.
- Cree o seleccione directivas de sesión para SmartAccess.

En el asistente, también puede crear expresiones de directivas de sesión para conexiones de usuario. Para obtener más información sobre cómo configurar NetScaler Gateway para conectarse a un conjunto de servidores, consulte Proporcionar acceso a aplicaciones publicadas y escritorios virtuales a través de la Interfaz Web.

## Configurar NetScaler Gateway con el Asistente para la instalación por primera vez

January 26, 2024

Para configurar NetScaler Gateway (el dispositivo físico o el dispositivo virtual VPX) por primera vez, necesita un equipo administrativo configurado en la misma red que el dispositivo.

Asigne una dirección IP de NetScaler Gateway (NSIP) como dirección IP de administración del dispositivo y una dirección IP de subred (SNIP) a la que se puedan conectar los servidores. Asigne una máscara de subred que se aplique a las direcciones de Citrix Gateway y SNIP y también configure una zona horaria. Si asigna un nombre de host, puede acceder al dispositivo especificando su nombre en lugar de la dirección NSIP.

Hay dos secciones en el Asistente de configuración por primera vez. En la primera sección, se configuran las opciones básicas del sistema para el dispositivo NetScaler Gateway, que incluyen:

- Dirección NSIP, dirección SNIP y máscara de subred
- Nombre de host del dispositivo
- Servidores DNS
- Zona horaria
- Contraseña del administrador

En la segunda sección, se instalan las licencias. Si especifica la dirección de un servidor DNS, puede utilizar el número de serie de hardware (HSN) o la clave de licencia para asignar las licencias, en lugar de cargar las licencias desde un equipo local al dispositivo.

Nota: Citrix recomienda guardar las licencias en el equipo local.

Cuando termine de configurar estos valores, NetScaler Gateway le pedirá que reinicie el dispositivo. Cuando vuelva a iniciar sesión en el dispositivo, puede utilizar otros asistentes y la utilidad de configuración para configurar otras opciones.

## Configurar parámetros con el Asistente de configuración rápida

March 27, 2024

Puede configurar la configuración en NetScaler Gateway para habilitar la comunicación con Citrix Endpoint Management, StoreFront o la Interfaz Web mediante el Asistente de configuración rápida. Al completar la configuración, el asistente crea las directivas correctas para la comunicación entre NetScaler Gateway, Endpoint Management, StoreFront o la Interfaz Web. Estas directivas incluyen directivas de autenticación, sesión y acceso sin cliente. Cuando finaliza el asistente, las directivas se enlazan al servidor virtual.

Al completar el asistente de configuración rápida, NetScaler Gateway puede comunicarse con Endpoint Management o StoreFront, y los usuarios pueden acceder a sus aplicaciones basadas en Windows y escritorios virtuales y aplicaciones web, SaaS y móviles. Los usuarios pueden conectarse directamente a Endpoint Management.

Durante el asistente, se configuran las siguientes opciones:

- Nombre del servidor virtual, dirección IP y puerto
- Redirección de un puerto no seguro a un puerto seguro
- Certificados
- Servidor LDAP
- Servidor RADIUS
- Certificado de cliente para autenticación (solo para autenticación de dos factores)
- Endpoint Management, StoreFront o Interfaz Web

El asistente de configuración rápida admite la autenticación de certificados de cliente, LDAP y RADIUS. Puede configurar la autenticación de dos factores en el asistente siguiendo estas pautas:

- Si selecciona LDAP como tipo de autenticación principal, puede configurar RADIUS como tipo de autenticación secundaria.
- Si selecciona RADIUS como tipo de autenticación principal, puede configurar LDAP como tipo de autenticación secundaria.
- Si selecciona certificados de cliente como tipo de autenticación principal, puede configurar LDAP o RADIUS como tipo de autenticación secundaria.

No se pueden crear varias directivas de autenticación LDAP mediante el Asistente de configuración rápida. Por ejemplo, quiere configurar una directiva que utilice SAMAccountName en el campo **Atributo de nombre de inicio de sesión del servidor** y una segunda directiva LDAP que utilice el nombre principal de usuario (UPN) en el campo **Atributo de nombre de inicio de sesión del servidor**. Para configurar estas directivas independientes, utilice la utilidad de configuración de NetScaler Gateway para crear las directivas de autenticación. Para obtener más información, consulte Configuración de la autenticación LDAP.

Puede configurar certificados para NetScaler Gateway en el Asistente de configuración rápida mediante los métodos siguientes:

- Seleccione un certificado instalado en el dispositivo.
- Instale un certificado y una clave privada.
- Seleccione un certificado de prueba.
  **Nota**: Si usa un certificado de prueba, debe agregar el nombre de dominio completo (FQDN) que figura en el certificado.

Puede abrir el **Asistente de configuración rápida** de una de las dos formas siguientes:

- Cuando se encuentra en la página de inicio de sesión de NetScaler Gateway y seleccione **NetScaler Gateway** en **Tipo de implementación**, aparece la ficha **Inicio**. Si selecciona cualquier otra opción en **Tipo de implementación**, la ficha **Inicio** no aparece.

- Desde el enlace **Crear/supervisar NetScaler Gateway** del panel de detalles de NetScaler Gateway. El enlace aparece si instala una licencia que habilita las funciones de NetScaler ADC. Si otorga la licencia del dispositivo solo para NetScaler Gateway, el enlace no aparece.

Después de ejecutar el asistente por primera vez, puede volver a ejecutarlo para crear más servidores virtuales y configuraciones.

**Importante**: Si utiliza el Asistente de configuración rápida para configurar un servidor virtual NetScaler Gateway adicional, debe utilizar una dirección IP única. No se puede utilizar la misma dirección IP que se utiliza en un servidor virtual existente. Por ejemplo, tiene un servidor virtual con la dirección IP 192.168.10.5 con un número de puerto 80. Ejecute el Asistente de configuración rápida para crear un segundo servidor virtual con la dirección IP 192.168.10.5 con el número de puerto 443. Al intentar guardar la configuración, se produce un error.

### Para configurar los ajustes con el asistente de configuración rápida

1. En la utilidad de configuración, realice una de las siguientes acciones:
    a) Si el dispositivo solo tiene licencia para NetScaler Gateway, haga clic en la ficha **Inicio**.
    b) Si el dispositivo tiene licencia para incluir funciones de NetScaler ADC, en la ficha Configuración, en el panel de navegación, haga clic en **NetScaler Gateway** y, a continuación, en el panel de detalles, en **Introducción**, haga clic en **Configurar NetScaler Gateway para Enterprise Store**.
2. En el panel de control, haga clic en **Crear nuevo NetScaler Gateway**.
3. En **Configuración de NetScaler Gateway**, configure lo siguiente:
    a) En **Nombre**, escriba un nombre para el servidor virtual.
    b) En **Dirección IP**, escriba la dirección IP del servidor virtual.
    c) En **Puerto**, escriba el número de puerto. El número de puerto predeterminado es 443.
    d) Seleccione Redirigir solicitudes desde el puerto 80 al puerto seguro para permitir que las conexiones de usuario del puerto 80 vayan al puerto 443.
4. Haga clic en **Continuar**.
5. En la página Certificado, realice una de las siguientes acciones:
    a) Haga clic en **Elegir certificado** y, a continuación, en Certificado, seleccione el certificado.
    b) Haga clic en **Instalar certificado y,** a continuación, en **Elegir certificado** y en **Elegir clave**, haga clic en **Examinar** para desplazarse hasta el certificado y la clave privada.
    c) Haga clic en **Usar certificado de prueba** y, a continuación, en FQDN de certificado, introduzca el nombre de dominio completo (FQDN) contenido en el certificado de prueba.
6. Haga clic en **Continuar**.
7. En Configuración de autenticación, haga lo siguiente:

a) En **Autenticación primaria**, seleccione LDAP, RADIUS o Cert.
b) Seleccione un servidor de autenticación o configure la configuración del tipo de autenticación que seleccionó en el paso anterior. Si selecciona Cert, seleccione el certificado de cliente o instale un nuevo certificado de cliente.
c) En **Autenticación secundaria**, seleccione el tipo de autenticación y, a continuación, configure la configuración del servidor de autenticación.

8. Haga clic en **Continuar**.

Cuando termine de configurar los ajustes de red y autenticación, podrá configurar los ajustes de Citrix Endpoint Management o Citrix Virtual Apps and Desktops (StoreFront o Interfaz Web).

#### Configuración de los ajustes de Enterprise Store

NetScaler Gateway admite el acceso de los usuarios a aplicaciones web, SaaS y móviles y ShareFile solo a través de Endpoint Management. Si también implementa StoreFront o la Interfaz Web, los usuarios tienen acceso a aplicaciones y escritorios virtuales basados en Windows. Puede configurar los ajustes de las siguientes opciones:

- Solo Endpoint Management
- Solo StoreFront
- Endpoint Management y StoreFront juntos
- Solo Interfaz Web

Al hacer clic en **Continuar** del procedimiento anterior, podrá configurar los ajustes de su caso de implementación. Los siguientes procedimientos se inician en la página Configuración de integración de Citrix.

Después de crear el servidor virtual, modificar el servidor virtual en el Asistente de configuración rápida no le permite cambiar la configuración de Citrix Endpoint Management o Citrix Virtual Apps and Desktops.

Por ejemplo, si cancela la configuración de un servidor virtual en cualquier etapa antes de configurar los ajustes de **Citrix Enterprise Store**, el asistente selecciona automáticamente la Interfaz Web sin configurar ninguna configuración. Cuando se produce esta situación, puede modificar los detalles del servidor virtual para configurar la Interfaz Web, pero no puede cambiar a Citrix Endpoint Management. Para cambiar, debe crear un nuevo servidor virtual y no debe cancelar el asistente en ningún momento durante la configuración. Si no necesita el servidor virtual de Interfaz Web, puede eliminarlo mediante el Asistente de configuración rápida.

#### Para configurar las opciones solo para StoreFront

1. Haga clic en **Citrix Virtual Apps and Desktops**.

2. En **Tipo de implementación**, seleccione **StoreFront**.
3. En el **FQDN de StoreFront**, introduzca el nombre de dominio completo (FQDN) del servidor StoreFront.
4. En **Receiver para Web Path**, deje la ruta predeterminada o introduzca la suya propia.
5. Seleccione **HTTPS** para proteger las conexiones de usuario.
6. En **Dominio de inicio de sesión único**, introduzca el dominio de StoreFront.
7. En **URL de STA**, introduzca la dirección IP completa o el FQDN del servidor que ejecuta Secure Ticket Authority (STA) si implementa StoreFront y proporciona acceso a aplicaciones publicadas desde Citrix Virtual Apps o escritorios virtuales desde Citrix Virtual Desktops.
8. Haga clic en **Listo**.

Cuando los usuarios se conectan a StoreFront a través de NetScaler Gateway, los usuarios pueden iniciar sus aplicaciones y escritorios desde Receiver para Web o Receiver.

#### Para configurar valores solo para Endpoint Management

1. Haga clic en **Citrix Endpoint Management**.
2. En el **FQDN de App Controller**, introduzca el FQDN de Endpoint Management.
3. Haga clic en **Listo**.

#### Para configurar los ajustes de la Interfaz Web

1. En el asistente de configuración rápida, haga clic en **Citrix Virtual Apps and Desktops**.
2. En **Tipo de implementación**, seleccione **Interfaz web**y, a continuación, configure lo siguiente:
    a) En **URL del sitio de Citrix Virtual Apps**, escriba la dirección IP completa o el FQDN de la Interfaz Web.
    b) En la **URL del sitio de Citrix Virtual Apps Services**, escriba la dirección IP completa o el FQDN de la interfaz web con la ruta de la aplicación Citrix Workspace. Puede introducir la ruta por defecto o introducir su propia ruta.
    c) En **Dominio de inicio de sesión único**, introduzca el dominio que va a utilizar.
    d) En **URL de STA**, escriba la dirección IP completa o el FQDN del servidor que ejecuta STA.
3. Haga clic en **Listo**.

## Configurar parámetros mediante el asistente de NetScaler Gateway

March 27, 2024

Después de ejecutar el asistente de configuración, puede ejecutar el asistente de Citrix Gateway para configurar parámetros adicionales en Citrix Gateway. Ejecute el asistente de NetScaler Gateway desde la utilidad de configuración.

NetScaler Gateway incluye un certificado de prueba. Si no tiene un certificado firmado de una entidad emisora de certificados (CA), puede usar el certificado de prueba al utilizar el asistente de NetScaler Gateway. Cuando reciba el certificado firmado, puede quitar el certificado de prueba e instalar el certificado firmado. Citrix recomienda obtener el certificado firmado antes de poner NetScaler Gateway a disposición del público para los usuarios.

Nota: Puede crear una solicitud de firma de certificado (CSR) desde el asistente de NetScaler Gateway. Si utiliza el asistente de Citrix Gateway para crear la CSR, debe salir del asistente y volver a iniciarlo cuando reciba el certificado firmado de la CA. Para obtener más información sobre los certificados, consulte
Instalación y administración de certificados.

Puede configurar las conexiones de usuario para el protocolo de Internet versión 6 (IPv6) en el asistente de NetScaler Gateway cuando configura un servidor virtual. Para obtener más información sobre el uso de IPv6 para las conexiones de usuario, consulte Configuración de IPv6 para conexiones de usuario.

### Para iniciar el asistente de NetScaler Gateway

1. En la utilidad de configuración, haga clic en la pestaña Configuración y, a continuación, en el panel de navegación, haga clic en Citrix Gateway .
2. En el panel de detalles, en Introducción, haga clic en el asistente Citrix Gateway .
3. Haga clic en Next y siga las instrucciones del asistente.

## Configurar el nombre de host y el FQDN en NetScaler Gateway

January 26, 2024

El nombre de host es el nombre del dispositivo NetScaler Gateway asociado al archivo de licencia. El nombre de host es exclusivo del dispositivo y se utiliza al descargar la licencia Universal. Defina el nombre de host al ejecutar el Asistente de configuración para configurar NetScaler Gateway por primera vez.

El nombre de dominio completo (FQDN) se incluye en el certificado firmado vinculado a un servidor virtual. No se configura el FQDN en NetScaler Gateway. Un dispositivo puede tener un FQDN único asignado a cada servidor virtual configurado en NetScaler Gateway mediante certificados.

Puede encontrar el FQDN de un certificado consultando los detalles del certificado. El FQDN se encuentra en el campo de asunto del certificado.

### Para ver el FQDN de un certificado

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificados.
2. En el panel de detalles, seleccione un certificado, haga clic en Acción y, a continuación, en Detalles.
3. En el cuadro de diálogo Detalles del certificado, haga clic en Asunto. El FQDN del certificado aparece en la lista.

## Instalar y administrar certificados

January 26, 2024

En NetScaler Gateway, utiliza certificados para crear conexiones seguras y autenticar usuarios.

Para establecer una conexión segura, se requiere un certificado de servidor en un extremo de la conexión. Se requiere un certificado raíz de la entidad emisora de certificados (CA) que emitió el certificado del servidor en el otro extremo de la conexión.

- Certificado de servidor. Un certificado de servidor certifica la identidad del servidor. NetScaler Gateway requiere este tipo de certificado digital.
- Certificado raíz. Un certificado raíz identifica a la CA que firmó el certificado de servidor. El certificado raíz pertenece a la CA. Un dispositivo de usuario requiere este tipo de certificado digital para verificar el certificado del servidor.

Al establecer una conexión segura con un explorador web en el dispositivo del usuario, el servidor envía su certificado al dispositivo.

Cuando el dispositivo de usuario recibe un certificado de servidor, el explorador web, como Internet Explorer, comprueba qué CA emitió el certificado y si el dispositivo del usuario confía en la entidad emisora de certificados. Si la entidad emisora de certificados no es de confianza o si se trata de un certificado de prueba, el explorador web solicita al usuario que acepte o rechace el certificado (aceptando o rechazando efectivamente la capacidad de acceder al sitio).

NetScaler Gateway admite los tres tipos de certificados siguientes:

- Certificado de prueba enlazado a un servidor virtual y que también se puede utilizar para conexiones a una comunidad de servidores. NetScaler Gateway incluye un certificado de prueba preinstalado.

- Certificado en formato PEM o DER firmado por una entidad emisora de certificados y emparejado con una clave privada.
- Certificado en formato PKCS #12 que se utiliza para almacenar o transportar el certificado y la clave privada. El certificado PKCS #12 se exporta normalmente de un certificado de Windows existente como archivo PFX y, a continuación, se instala en NetScaler Gateway.

Citrix recomienda utilizar un certificado firmado por una entidad emisora de certificados de confianza, como Thawte o Verisign.

## Crear una solicitud de firma de certificado

January 26, 2024

Para proporcionar comunicaciones seguras mediante SSL o TLS, se requiere un certificado de servidor en NetScaler Gateway. Antes de cargar un certificado en NetScaler Gateway, debe generar una solicitud de firma de certificado (CSR) y una clave privada. Utilice la solicitud de creación de certificado incluida en el asistente de NetScaler Gateway o la utilidad de configuración para crear la CSR. La solicitud de creación de certificado crea un archivo.csr que se envía por correo electrónico a la entidad de certificación (CA) para que lo firme y una clave privada que permanece en el dispositivo. La CA firma el certificado y se lo devuelve a la dirección de correo electrónico que proporcionó. Cuando reciba el certificado firmado, podrá instalarlo en NetScaler Gateway. Cuando reciba el certificado de la entidad emisora de certificados, empareja el certificado con la clave privada.

Importante: Cuando utilice el asistente de NetScaler Gateway para crear la CSR, debe salir del asistente y esperar a que la CA le envíe el certificado firmado. Cuando reciba el certificado, puede volver a ejecutar el asistente de NetScaler Gateway para crear la configuración e instalar el certificado. Para obtener más información sobre el asistente de NetScaler Gateway, consulte Configuración de los ajustes mediante el Asistente de NetScaler Gateway.

### Para crear una CSR mediante el asistente de Citrix Gateway

1. En la utilidad de configuración, haga clic en la ficha Configuración y, a continuación, en el panel de navegación, haga clic en NetScaler ADC Gateway.
2. En el panel de detalles, en Introducción, haga clic en Asistente de NetScaler ADC Gateway.
3. Siga las instrucciones del asistente hasta llegar a la página Especificar un certificado de servidor.
4. Haga clic en Crear una solicitud de firma de certificado y complete los campos.
   Nota: El nombre de dominio completo (FQDN) no tiene por qué ser el mismo que el nombre de host de NetScaler Gateway. El FQDN se utiliza para el inicio de sesión del usuario.
5. Haga clic en Crear para guardar el certificado en su equipo y, a continuación, haga clic en Cerrar.

6. Salga del asistente de NetScaler Gateway sin guardar la configuración.

### Para crear una CSR mediante la GUI de Citrix ADC

También puede utilizar la GUI de NetScaler ADC para crear una CSR sin ejecutar el asistente de NetScaler Gateway.

1. Vaya a **Administración de tráfico** > **SSL > Archivos SSL** y seleccione **Crear solicitud de firma de certificado (CSR)**.
2. Complete la configuración del certificado y, a continuación, haga clic en **Crear**.

Después de crear el certificado y la clave privada, envíe el certificado por correo electrónico a la CA, como Thawte o Verisign.

Para obtener información detallada sobre el procedimiento, consulte Crear una solicitud de firma de certificado.

## Instalar el certificado firmado en NetScaler Gateway

March 27, 2024

Cuando reciba el certificado firmado de la entidad emisora de certificados (CA), emparéjelo con la clave privada del dispositivo y, a continuación, instale el certificado en NetScaler Gateway.

### Para vincular el certificado firmado con una clave privada

1. Copie el certificado en NetScaler Gateway en la carpeta nsconfig/ssl mediante un programa Secure Shell (SSH) como WinSCP.
2. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificados.
3. En el panel de detalles, haga clic en Instalar.
4. En Nombre del par de claves de certificado, escriba el nombre del certificado.
5. En Nombre del archivo del certificado, seleccione el cuadro de menú en Examinar y, a continuación, haga clic en Dispositivo.
6. Vaya al certificado, haga clic en Seleccionar y, a continuación, haga clic en Abrir.
7. En Nombre del archivo de clave privada, seleccione el cuadro de menú en Examinar y, a continuación, haga clic en Dispositivo. El nombre de la clave privada es el mismo que el de la solicitud de firma de certificado (CSR). La clave privada está en Citrix Gateway, en el directorio\nsconfig\ssl.

8. Elige la clave privada y, a continuación, haz clic en Abrir.
9. Si el certificado tiene formato PEM, en Contraseña, escriba la contraseña de la clave privada.
10. Si desea configurar la notificación para cuando caduque el certificado, seleccione Notificar cuando caduque.
11. En Periodo de notificación, escriba el número de días, haga clic en Crear y, a continuación, haga clic en Cerrar.

### Para vincular el certificado y la clave privada a un servidor virtual

Después de crear y vincular un par de certificados y claves privadas, enlaza a un servidor virtual.

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, en Abrir .
3. En la ficha Certificados, en Disponible, seleccione un certificado, haga clic en Agregar y, a continuación, haga clic en Aceptar.

### Para desvincular los certificados de prueba del servidor virtual

Después de instalar el certificado firmado, desvincule todos los certificados de prueba vinculados al servidor virtual. Puede desvincular certificados de prueba mediante la utilidad de configuración.

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, en Abrir .
3. En la pestaña Certificados, en Configurado, seleccione el certificado de prueba y, a continuación, haga clic en Eliminar.

## Configurar certificados intermedios

January 26, 2024

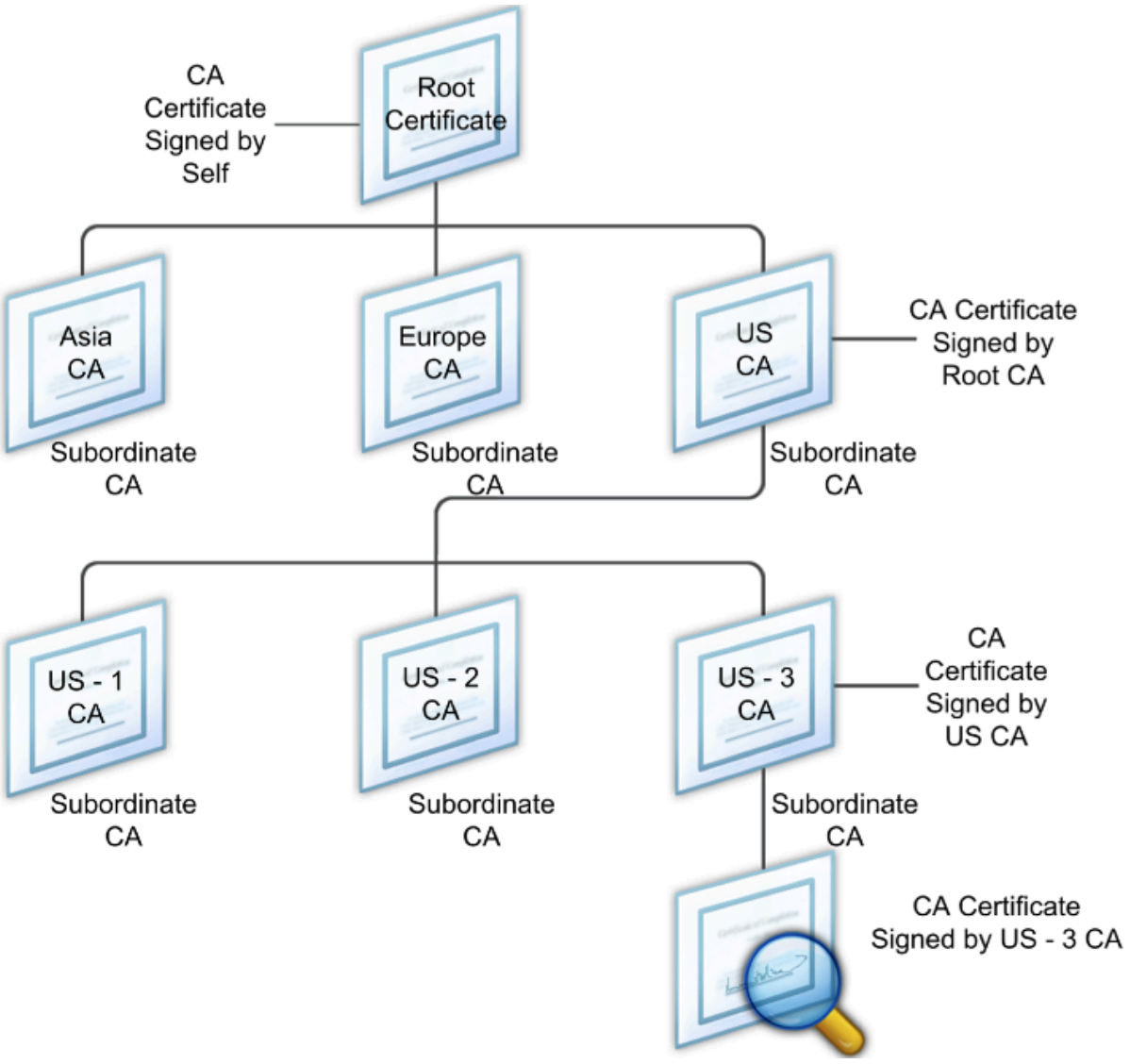
Un certificado intermedio es un certificado que va entre NetScaler Gateway (el certificado del servidor) y un certificado raíz (instalado en el dispositivo del usuario). Un certificado intermedio forma parte de una cadena.

Algunas organizaciones delegan la responsabilidad de emitir certificados para resolver el problema de la separación geográfica entre las unidades organizativas o para aplicar directivas de emisión diferentes a distintas secciones de la organización.

La responsabilidad de la emisión de certificados se puede delegar mediante la configuración de entidades de certificación (CA) subordinadas. Las CA pueden firmar sus propios certificados (es decir, están autofirmados) o pueden ser firmados por otra CA. El estándar X.509 incluye un modelo para configurar una jerarquía de CA. En este modelo, como se muestra en la siguiente figura, la CA raíz se encuentra en la parte superior de la jerarquía y es un certificado autofirmado por la CA. Las CA que están directamente subordinadas a la CA raíz tienen certificados de CA firmados por la CA raíz. Las entidades emisoras de certificados subordinadas de la jerarquía tienen sus certificados de CA firmados por las entidades emisoras de certificados subordinadas.

Figura 1. El modelo X.509 muestra la estructura jerárquica de una cadena de certificados digitales típica




Si una CA firma un certificado de servidor con un certificado autofirmado, la cadena de certificados se compone exactamente de dos certificados: el certificado de entidad final y la CA raíz. Si un certificado de usuario o servidor está firmado por una CA intermedia, la cadena de certificados es más larga.

La siguiente figura muestra que los dos primeros elementos son el certificado de la entidad final (en este caso, gwy01.company.com) y el certificado de la CA intermedia, en ese orden. El certificado de la CA intermedia va seguido del certificado de su CA. Esta lista continúa hasta que el último certificado de la lista sea para una CA raíz. Cada certificado de la cadena da fe de la identidad del certificado anterior.

Figura 2. Una cadena de certificados digitales típica


### Para instalar un certificado intermedio

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificados.
2. En el panel de detalles, haga clic en Instalar.
3. En Nombre del par de claves de certificado, escriba el nombre del certificado.
4. En Detalles, en Nombre del archivo del certificado, haga clic en Examinar (dispositivo) y, en el cuadro de menú, seleccione Local o Dispositivo.
5. Vaya a el certificado en su equipo (local) o en NetScaler Gateway (dispositivo).
6. En Formato de certificado, seleccione PEM.
7. Haga clic en Instalar y, a continuación, en Cerrar.

Al instalar un certificado intermedio en NetScaler Gateway, no es necesario especificar la clave privada ni la contraseña.

Una vez instalado el certificado en el dispositivo, el certificado debe vincularse al certificado del servidor.

### Para vincular un certificado intermedio a un certificado de servidor

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificados.
2. En el panel de detalles, seleccione el certificado de servidor y, a continuación, en Acción, haga clic en Vincular.
3. Junto a Nombre del certificado de CA, seleccione el certificado intermedio de la lista y, a continuación, haga clic en Aceptar.

# Usar certificados de dispositivo para la autenticación

March 27, 2024

NetScaler Gateway admite la comprobación de certificados de dispositivo que permite vincular la identidad del dispositivo a la clave privada de un certificado. La comprobación del certificado del dispositivo se puede configurar como parte de las directivas clásicas o avanzadas de Endpoint Analysis (EPA). En las directivas clásicas de EPA, el certificado de dispositivo solo se puede configurar para la EPA de autenticación previa.

NetScaler Gateway verifica el certificado del dispositivo antes de que se ejecute el análisis de endpoint o antes de que aparezca la página de inicio de sesión. Si configura el análisis de endpoints, el análisis de endpoints se ejecuta para verificar el dispositivo del usuario. Cuando el dispositivo pasa el análisis y después de que NetScaler Gateway verifica el certificado del dispositivo, los usuarios pueden iniciar sesión en NetScaler Gateway.

> **Importante:**
>
> - De forma predeterminada, Windows exige privilegios de administrador para acceder a los certificados de dispositivo.
> - Para agregar una comprobación de certificado de dispositivo para usuarios que no son administradores, debe instalar el complemento VPN. La versión del plug-in VPN debe ser la misma que el plug-in de la EPA del dispositivo.
> - Puede agregar varios certificados de CA a la puerta de enlace y validar el certificado de dispositivo.
> - Si instala dos o más certificados de dispositivo en NetScaler Gateway, los usuarios deben seleccionar el certificado correcto cuando empiecen a iniciar sesión en NetScaler Gateway o antes de que se ejecute el análisis de endpoint.
> - Al crear el certificado de dispositivo, debe ser un certificado X.509.
> - Si tiene un certificado de dispositivo emitido por una CA intermedia, los certificados de CA intermedia y raíz deben estar vinculados.
> - El cliente EPA necesita que el usuario tenga derechos de administrador local para poder acceder al almacén de certificados de la máquina. Esto rara vez ocurre, por lo que una solución alternativa es instalar el complemento completo de NetScaler Gateway que puede acceder al almacén local.

Para obtener más información sobre cómo crear certificados de dispositivo, consulte lo siguiente:

- Servicio de inscripción de dispositivos de red (NDES) en los Servicios de certificados de Active Directory (AD CS) en el sitio web de Microsoft.
- Ejemplo paso a paso de implementación de certificados PKI para Configuration Manager: ¿Entidad de certificación de Windows Server 2008? RedirectedFrom=MSDN) en el sitio web de Mi-

crosoft System Center.

- Cómo solicitar un certificado a una entidad emisora de certificados de Microsoft mediante DCE/RPC y la carga útil del perfil de certificados de Active Directory en el sitio web de soporte técnico de Apple.
- Emisión de certificados iPad o iPhone en el blog de soporte técnico de Microsoft Pregunte al equipo de servicios de directorio.
- Configuración del servicio de inscripción de dispositivos de red en el sitio web de TI Pro de Windows.

### Pasos para configurar certificados de dispositivo

Para configurar un certificado de dispositivo, debe completar los pasos siguientes:

- Instale el certificado de entidad emisora de certificados del dispositivo en NetScaler Gateway. Para obtener más información, consulte Instalación del certificado firmado en NetScaler Gateway.
- Enlace el certificado de entidad emisora de certificados del dispositivo al servidor virtual de NetScaler Gateway y habilite la comprobación de OCSP. Para obtener más información, consulte Instalación del certificado firmado en NetScaler Gateway.
- Cree y vincule OCSP (respondedor) en el certificado de entidad emisora de certificados del dispositivo. Para obtener más información, consulte Supervisar el estado de los certificados con OCSP.

Habilite la comprobación de certificados de dispositivo en el servidor virtual y agregue el certificado de entidad emisora de certificados de dispositivo a la lista de comprobación de certificados de dispositivo. Para obtener más información, consulte Habilitar la comprobación de certificados de dispositivo en un servidor virtual para la directiva clásica de EPA.

Complete la configuración del cliente y la verificación del certificado de dispositivo en la máquina Windows. Para obtener más información, consulte Verificación del certificado de dispositivo en un equipo Windows.

> **Nota:**
>
> Todos los clientes destinados a aprovechar la comprobación EPA del certificado de dispositivo deben tener el certificado de dispositivo instalado en el almacén de certificados del sistema de la máquina.

### Habilitar la comprobación de certificados de dispositivo en un servidor virtual para la directiva clásica de EPA

Después de crear el certificado de dispositivo, instale el certificado en NetScaler Gateway mediante el procedimiento de importación e instalación de un certificado existente en NetScaler Gateway.

1. En la ficha Configuración, vaya a **Citrix Gateway > Servidores virtuales**.
2. En la página **Servidores virtuales de Citrix Gateway** , seleccione un servidor virtual existente y haga clic en **Editar** .
3. En la página **Servidores virtuales VPN** , en la sección **Configuración básica** , haga clic en **Editar** .
4. Desactive la casilla **Habilitar autenticación** para inhabilitar la autenticación.
5. Seleccione la casilla **Habilitar certificado de dispositivo** para habilitar el certificado de dispositivo
6. Haga clic en **Agregar** para agregar a la lista el nombre del certificado de CA del emisor de un certificado de dispositivo disponible.
7. Para vincular un certificado de CA al servidor virtual, haga clic en **Certificado de CA** en la sección **CA para certificado de dispositivo**, haga clic en **Agregar**, seleccione el certificado y, a continuación, haga clic en **+**.

> **Nota:**
>
> Para obtener información sobre cómo habilitar y vincular certificados de dispositivo en un servidor virtual para directivas EPA avanzadas, consulte Certificado de dispositivo en nFactor como componente EPA.

### Verificación del certificado de dispositivo en un equipo Windows

1. Abra un explorador y acceda al FQDN de NetScaler Gateway.
2. Permita que se ejecute el cliente de Citrix End Point Analysis (EPA). Si aún no está instalado, instale la EPA.

   Citrix EPA ejecuta y valida el certificado de dispositivo y lo redirige a la página de autenticación si se aprueba la comprobación de EPA del certificado de dispositivo; de lo contrario, lo redirige a la página de error de la EPA. En caso de que tenga otras comprobaciones de la EPA, los resultados del análisis de la EPA dependen de las comprobaciones de la EPA configuradas.

Para realizar más depuraciones en el cliente, examine los siguientes registros de EPA en el cliente: C:\Users<User name>\ AppData\ Local\ Citrix\ AGEE\ nsepa.txt

> **Nota:**
>
> No se admite la verificación del certificado del dispositivo con CRL.

## Importar e instalar un certificado existente

March 27, 2024

Puede importar un certificado existente desde un equipo basado en Windows que ejecuta Internet Information Services (IIS) o desde un equipo que ejecuta Secure Gateway.

Al exportar el certificado, asegúrese de exportar también la clave privada. En algunos casos, no puede exportar la clave privada, lo que significa que no puede instalar el certificado en Citrix Gateway. Si esto ocurre, utilice la solicitud de firma de certificado (CSR) para crear un certificado nuevo. Para obtener más información, consulte Creación de una solicitud de firma de certificado.

Al exportar un certificado y una clave privada de Windows, el equipo crea un archivo de intercambio de información personal (.pfx). Este archivo se instala en NetScaler Gateway como certificado PKCS #12.

Si va a reemplazar Secure Gateway por NetScaler Gateway, puede exportar el certificado y la clave privada desde Secure Gateway. Si realiza una migración local de Secure Gateway a NetScaler Gateway, el nombre de dominio completo (FQDN) de la aplicación y del dispositivo deben ser los mismos. Al exportar el certificado desde Secure Gateway, retira inmediatamente Secure Gateway, instala el certificado en NetScaler Gateway y, a continuación, prueba la configuración. Secure Gateway y NetScaler Gateway no pueden ejecutarse en la red al mismo tiempo si tienen el mismo FQDN.

Si utiliza Windows Server 2003 o Windows Server 2008, puede utilizar Microsoft Management Console para exportar el certificado. Para obtener más información, consulte la Ayuda en línea de Windows.

Deje los valores predeterminados para todas las demás opciones, defina una contraseña y guarde el archivo.pfx en el equipo. Cuando se exporta el certificado, lo instala en NetScaler Gateway.

### Para instalar el certificado y la clave privada en NetScaler Gateway

1. En la utilidad de configuración, haga clic en la pestaña Configuración y, a continuación, en el panel de navegación, haga clic en Citrix Gateway .
2. En el panel de detalles, en Introducción, haga clic en el asistente Citrix Gateway .
3. Haga clic en Siguiente, seleccione un servidor virtual existente y, a continuación, haga clic en Siguiente.

4. En Opciones de certificado, seleccione Instalar un archivo PKCS #12 (.pfx)e.
5. En el nombre de archivo PKCS #12, haga clic en Examinar, navegue hasta el certificado y, a continuación, haga clic en Seleccionar.
6. En Contraseña, escriba la contraseña de la clave privada.

   Esta es la contraseña que utilizó al convertir el certificado al formato PEM.
7. Haga clic en Siguiente para finalizar el asistente de NetScaler Gateway sin cambiar ninguna otra configuración.

Cuando el certificado se instala en Citrix Gateway, aparece en la utilidad de configuración del nodo SSL > Certificados.

**Para crear una clave privada**

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, haga clic en SSL.
2. En el panel de detalles, enClaves SSL, haga clic enCrear clave RSA.
3. En Nombre dearchivo clave, escriba el nombre de la clave privada o haga clic en Examinar para ir a un archivo existente.
4. EnTamaño de clave (bits), escriba el tamaño de la clave privada.
5. EnValor de exponente público, seleccione F4 o 3.

   El valor del exponente público de la clave RSA. Forma parte del algoritmo de cifrado y es necesario para crear la clave RSA. Los valores son F4 (Hex: 0x10001) o 3 (Hex: 0x3). El valor predeterminado es F4.
6. EnFormato clave, seleccione PEM o DER. Citrix recomienda el formato PEM para el certificado.
7. EnAlgoritmo de codificación PEM, seleccione DES o DES3.
8. En Phrase de contraseña de PEM y verificación de frase de contraseña, escriba la contraseña, haga clic en Crear y, a continuación, en Cerrar.

   Nota: Para asignar una contraseña, el
   formato de clave debe ser PEM y debe seleccionar el algoritmo de codificación.

Para crear una clave privada DSA en la utilidad de configuración, haga clic en Crear clave DSA. Siga los mismos pasos anteriores para crear la clave privada de DSA.

# Conversión del certificado del formato PFX al formato PEM

January 26, 2024

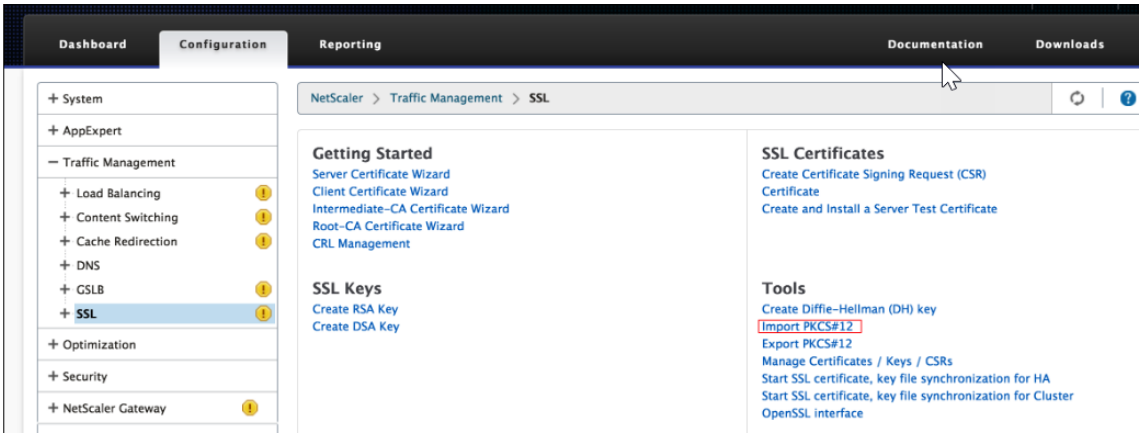
Los certificados SSL se utilizan para los servidores virtuales de equilibrio de carga SSL y los servidores virtuales NetScaler Gateway. Los certificados PEM son archivos ASCII codificados en Base64. Los certificados PEM se pueden abrir en el Editor de texto/Bloc de notas y descubre que contienen instrucciones "—BEGIN CERTIFICATE—"y "—END CERTIFICATE—".

Para obtener un acceso seguro y de confianza, debe instalar un certificado de servidor SSL en el servidor NetScaler Gateway. El archivo de certificado cargado debe tener las siguientes funciones:

- La entidad emisora de certificados (CA) en la que confían los usuarios finales debe emitir el certificado del servidor. Para obtener los mejores resultados, utilice una CA comercial como Verisign, Thawte o GeoTrust.
- El certificado debe tener el formato Privacy Enhanced Mail (PEM), un formato basado en texto que sea una codificación Base64 del formato binario Reglas de codificación distinguidas (DER).
- El archivo de certificado debe incluir una clave privada y la clave privada no debe cifrarse. No debe ser necesaria ninguna contraseña para utilizar el archivo PEM.
- Todos los certificados intermedios necesarios deben agregarse al final del archivo PEM.

Complete el procedimiento siguiente para convertir un certificado PFX al formato PEM mediante el Asistente de NetScaler Gateway:

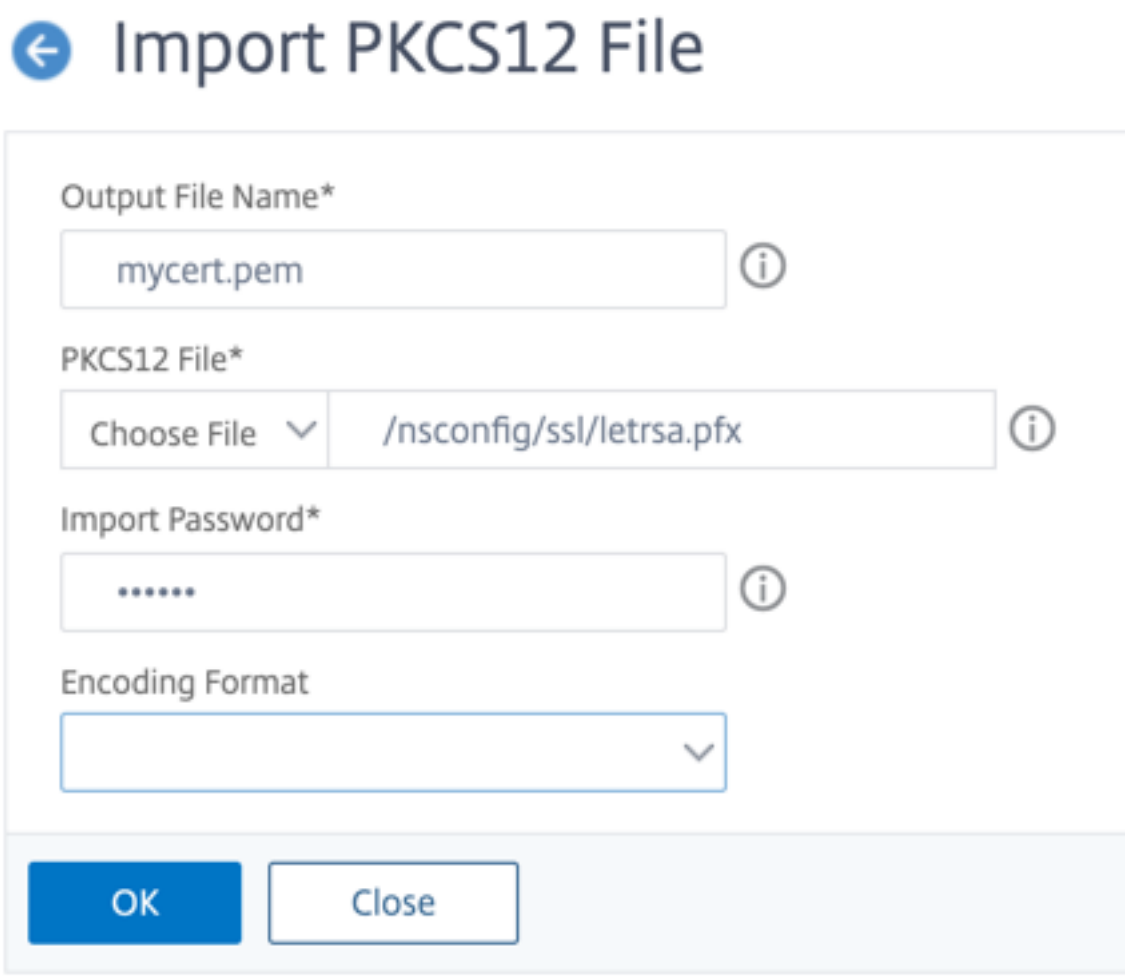
1. Vaya a **Administración del tráfico**, seleccione el nodo **SSL**.
2. Haga clic en el enlace **Importar PKCS#12**.



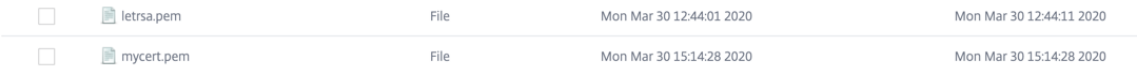

3. Especifique el nombre de archivo que quiera para el certificado PEM en el campo **Nombre del archivo de salida**.

4. Haga clic en **Examinar** y seleccione el certificado PFX que quiere convertir al formato PEM. Algunos usuarios prefieren cargar el certificado en el directorio /ncsonfig/ssl y usarlo desde allí. Si el certificado PFX está almacenado en NetScaler Gateway, elija la opción **Dispositivo y,** si está almacenado en su estación de trabajo, utilice Local.




5. Especifique la contraseña de importación.
6. Si el archivo está codificado, seleccione DES o 3DES como formato de codificación:
7. Haga clic en **Aceptar**.
8. Especifique la frase de contraseña PEM y la frase de contraseña de verificación de PEM.
9. Haga clic en el **enlace Administrar certificados/claves/CSR** para ver los archivos de certificado PEM convertidos.
10. Puede ver el archivo PFX cargado con el archivo PEM convertido.



11. Expanda el nodo **SSL**.
12. Seleccione el nodo Certificados.
13. Haga clic en **Instalar**.
14. Especifique un nombre de par de claves de **certificado en el Asistente de instalación** de certificados.
15. Busque el archivo PEM para el nombre del archivo de certificado y el nombre del archivo de clave privada.
16. Especifique la contraseña.
17. Haga clic en **Instalar**.

### OpenSSL Utility

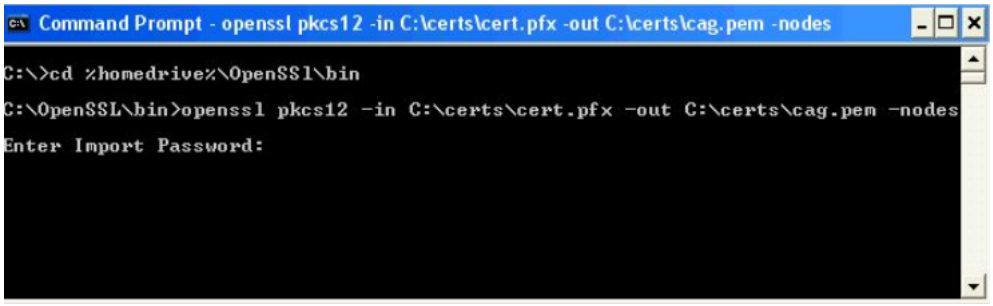
Si ha solicitado e instalado un certificado en un servidor Windows mediante el Asistente para certificados de Internet Information Service (IIS), puede exportar ese certificado con su clave privada a un archivo de intercambio de información personal (PFX). Para importar este certificado en NetScaler Gateway, debe convertir el archivo PFX a formato PEM sin cifrar.

Puede utilizar la utilidad de código abierto OpenSSL para realizar la conversión de PFX a PEM. Descargue una distribución Win32 de OpenSSL de OpenSSL Win32.

Es posible que también necesites archivos redistribuibles de C++ si quiere usarlos OpenSSL. Descargue esto desde el paquete redistribuible de Microsoft Visual C++ 2008 (x86).

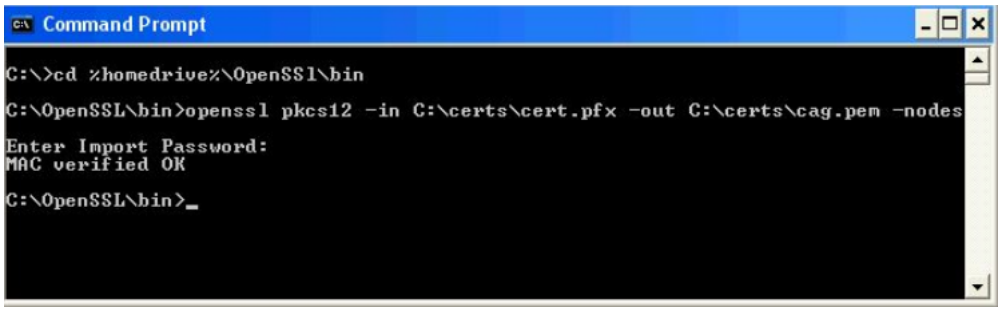
Para convertir un archivo PFX en un archivo PEM, siga los pasos siguientes en un equipo Windows:

1. Descargue e instale el paquete OpenSSL Win32 desde OpenSSL Win32.
2. Crea una carpeta c:\certs y copia el archivo yourcert.pfx en la carpeta c:\certs.
3. Abra el símbolo del sistema y cambie al directorio OpenSSL\ bin: `cd %homedrive%\OpenSSL\bin`
4. Ejecute el siguiente comando para convertir el archivo PFX en un archivo PEM sin cifrar (todo en una línea): OpenSSL pkcs12 -in c:\certs\yourcert.pfx -out c:\certs\cag.pem –nodes



5. Cuando se le solicite la contraseña de importación, introduzca la contraseña que utilizó al exportar el certificado a un archivo PFX. Debe recibir un mensaje que diga que MAC verificado OK.




6. Apunte un explorador al portal de administración de NetScaler Gateway o al puerto HTTPS 9001: `https://netscaler-gateway-server:9001`.
7. Inicie sesión como root. La contraseña predeterminada es `rootadmin`.
8. Haga clic en el enlace **Mantenimiento** en la parte superior de la página.
9. Haga clic en el botón **Examinar** junto al campo **Cargar clave privada+certificado (.pem)**. Vaya al archivo c:\certs\cag.pem y haga clic en **Cargar**.
10. Reinicie NetScaler Gateway para que se aplique el nuevo certificado SSL.

## Listas de revocación de certificados

January 26, 2024

De vez en cuando, las entidades de certificación (CA) emiten listas de revocación de certificados (CRL). Las CRL contienen información sobre certificados en los que ya no se puede confiar. Por ejemplo, supongamos que Ann deja XYZ Corporation. La empresa puede colocar el certificado de Ann en una CRL para evitar que firme mensajes con esa clave.

Del mismo modo, puede revocar un certificado si una clave privada está en peligro o si ese certificado ha caducado y se está usando una nueva. Antes de confiar en una clave pública, asegúrese de que el certificado no aparezca en una CRL.

NetScaler Gateway admite los dos tipos de CRL siguientes:

- CRL que enumeran los certificados que se han revocado o que ya no son válidos
- Protocolo de estado de certificados en línea (OSCP), protocolo de Internet utilizado para obtener el estado de revocación de los certificados X.509

### Para agregar una CRL

Antes de configurar la CRL en el dispositivo NetScaler Gateway, asegúrese de que el archivo CRL se almacena localmente en el dispositivo. En el caso de una configuración de alta disponibilidad, el archivo CRL debe estar presente en ambos dispositivos NetScaler Gateway y la ruta de acceso del directorio al archivo debe ser la misma en ambos dispositivos.

Si necesita actualizar la CRL, puede utilizar los siguientes parámetros:

- Nombre de CRL: nombre de la CRL que se agrega en NetScaler ADC. Máximo 31 caracteres.
- Archivo CRL: nombre del archivo CRL que se agrega en NetScaler ADC. NetScaler ADC busca el archivo CRL en el directorio /var/netscaler/ssl de forma predeterminada. Máximo 63 caracteres.
- URL: 127 caracteres como máximo
- DN base: 127 caracteres como máximo
- Enlazar DN: 127 caracteres como máximo
- Contraseña: 31 caracteres como máximo
- Día (s): máximo 31

1. En la utilidad de configuración, en la pestaña Configuración, expanda SSL y, a continuación, haga clic en CRL.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Agregar CRL, especifique los valores de lo siguiente:
    - Nombre de CRL
    - Archivo CRL
    - Formato (opcional)
    - Certificado CA (opcional)
4. Haga clic en **Create** y, luego, en **Close**. En el panel de detalles de la CRL, seleccione la CRL que acaba de configurar y compruebe que la configuración que aparece en la parte inferior de la pantalla es correcta.

### Para configurar la actualización automática de CRL mediante LDAP o HTTP en la utilidad de configuración

Una CA genera y publica una CRL de forma periódica o, en algunos casos, inmediatamente después de revocar un certificado determinado. Citrix recomienda actualizar periódicamente las CRL del dispositivo NetScaler Gateway para protegerse de los clientes que intentan conectarse con certificados que no son válidos.

El dispositivo NetScaler Gateway puede actualizar CRL desde una ubicación web o un directorio LDAP. Cuando especifique parámetros de actualización y una ubicación web o un servidor LDAP, la CRL no tiene que estar presente en la unidad de disco duro local en el momento de ejecutar el comando. La

primera actualización almacena una copia en la unidad de disco duro local, en la ruta especificada por el parámetro Archivo CRL. La ruta predeterminada para almacenar la CRL es /var/netscaler/ssl.

Parámetros de actualización de CRL

- **Nombre de CRL**

  Nombre de la CRL que se está actualizando en NetScaler Gateway.

- **Habilitar actualización automática de CRL**

  Habilite o inhabilite la actualización automática de CRL.

- **Certificado CA**

  Certificado de la entidad emisora de certificados que ha emitido la CRL. Este certificado de CA debe estar instalado en el dispositivo. El NetScaler ADC solo puede actualizar CRL desde CA cuyos certificados están instalados en él.

- **Método**

  Protocolo para obtener la actualización de CRL de un servidor web (HTTP) o de un servidor LDAP. Valores posibles: HTTP, LDAP. Valor predeterminado: HTTP.

- **Ámbito**

  Extensión de la operación de búsqueda en el servidor LDAP. Si el ámbito especificado es Base, la búsqueda se encuentra al mismo nivel que el DN base. Si el ámbito especificado es Uno, la búsqueda se extiende a un nivel por debajo del DN base.

- **IP de servidor**

  Dirección IP del servidor LDAP del que se recupera la CRL. Seleccione IPv6 para utilizar una dirección IP IPv6.

- **Puerto**

  Número de puerto en el que se comunica el servidor LDAP o HTTP.

- **URL**

  Dirección URL de la ubicación web de la que se recupera la CRL.

- **DN base**

  El DN base utilizado por el servidor LDAP para buscar el atributo CRL.
  Nota: Citrix recomienda utilizar el atributo DN base en lugar del nombre del emisor del certificado de CA para buscar la CRL en el servidor LDAP. Es posible que el campo Nombre del emisor no coincida exactamente con el DN de la estructura de directorios LDAP.

- **Vincular DN**

El atributo DN de enlace utilizado para acceder al objeto CRL en el repositorio LDAP. Los atributos DN de enlace son las credenciales de administrador del servidor LDAP. Configure este parámetro para restringir el acceso no autorizado a los servidores LDAP.

- **Contraseña**

  Contraseña de administrador utilizada para acceder al objeto CRL del repositorio LDAP. Esto es necesario si el acceso al repositorio LDAP está restringido, es decir, no se permite el acceso anónimo.

- **Intervalo**

  El intervalo en el que debe realizarse la actualización de la CRL. Para una actualización instantánea de CRL, especifique el intervalo como AHORA. Valores posibles: MENSUAL, DIARIO, SEMANAL, AHORA, NINGUNO.

- **Días**

  El día en el que se debe realizar la actualización de la CRL. La opción no está disponible si el intervalo está establecido en DIARIO.

- **Hora**

  La hora exacta en formato de 24 horas en la que se debe realizar la actualización de la CRL.

- **Binario**

  Establezca el modo de recuperación de CRL basado en LDAP en binario. Valores posibles: SÍ, NO. Predeterminado: NO.

1. En el panel de navegación, expanda SSL y, a continuación, haga clic en CRL.
2. Seleccione la CRL configurada para la que quiere actualizar los parámetros de actualización y, a continuación, haga clic en Abrir.
3. Seleccione la opción Habilitar actualización automática de CRL.
4. En el grupo Parámetros de actualización automática de CRL, especifique valores para los siguientes parámetros:
   Nota: Un asterisco (*) indica un parámetro obligatorio.

   - Método
   - Binario
   - Ámbito
   - IP de servidor
   - Puerto*
   - URL
   - DNS base*
   - Vincular DN
   - Contraseña

- Intervalo
- Día (s)
- Hora

5. Haga clic en Crear. En el panel CRL, seleccione la CRL que acaba de configurar y compruebe que la configuración que aparece en la parte inferior de la pantalla es correcta.

## Supervisar el estado del certificado con OCSP

January 26, 2024

El Protocolo de estado de certificados en línea (OCSP) es un protocolo de Internet que se utiliza para determinar el estado de un certificado SSL de cliente. NetScaler Gateway admite OCSP según se define en RFC 2560. OCSP ofrece ventajas significativas sobre las listas de revocación de certificados (CRL) en términos de información oportuna. El estado de revocación actualizado de un certificado de cliente es especialmente útil en transacciones que implican grandes sumas de dinero y operaciones bursátiles de alto valor. También utiliza menos recursos del sistema y de la red. La implementación de OCSP en NetScaler Gateway incluye el procesamiento por lotes de solicitudes y el almacenamiento en caché de respuestas

### Implementación de OCSP en Citrix Gateway

La validación de OCSP en un dispositivo Citrix Gateway comienza cuando Citrix Gateway recibe un certificado de cliente durante un protocolo de enlace SSL. Para validar el certificado, NetScaler Gateway crea una solicitud OCSP y la reenvía al respondedor OCSP. Para ello, NetScaler Gateway extrae la dirección URL del respondedor OCSP del certificado de cliente o utiliza una URL configurada localmente. La transacción está suspendida hasta que NetScaler Gateway evalúa la respuesta del servidor y determina si se permite o se rechaza la transacción. Si la respuesta del servidor se retrasa más allá del tiempo configurado y no hay ningún otro respondedor configurado, NetScaler Gateway permite la transacción o muestra un error, en función de si establece la comprobación de OCSP como opcional u obligatoria. NetScaler Gateway admite el procesamiento por lotes de solicitudes OCSP y el almacenamiento en caché de respuestas OCSP para reducir la carga del respondedor OCSP y proporcionar respuestas más rápidas.

### Procesamiento por lotes de solicitudes OCSP

Cada vez que NetScaler Gateway recibe un certificado de cliente, envía una solicitud al respondedor OCSP. Para evitar sobrecargar el respondedor OCSP, NetScaler Gateway puede consultar el estado

de más de un certificado de cliente en la misma solicitud. Para que el procesamiento por lotes de solicitudes funcione de forma eficiente, es necesario definir un tiempo de espera para que el procesamiento de un único certificado no se retrase mientras se espera formar un lote.

### Almacenamiento en caché de respuestas de OCSP

El almacenamiento en caché de las respuestas recibidas del respondedor OCSP permite respuestas más rápidas para el usuario y reduce la carga del respondedor OCSP. Al recibir el estado de revocación de un certificado de cliente del respondedor OCSP, NetScaler Gateway almacena en caché la respuesta localmente durante un período de tiempo predefinido. Cuando se recibe un certificado de cliente durante un protocolo de enlace SSL, NetScaler Gateway comprueba primero su caché local en busca de una entrada para este certificado. Si se encuentra una entrada que sigue siendo válida (dentro del límite de tiempo de espera de la caché), se evalúa la entrada y se acepta o rechaza el certificado de cliente. Si no se encuentra un certificado, NetScaler Gateway envía una solicitud al respondedor OCSP y almacena la respuesta en su caché local durante un período de tiempo configurado.

## Configurar el estado del certificado OCSP

January 26, 2024

La configuración del Protocolo de estado de certificados en línea (OCSP) implica agregar un respondedor OCSP, vincular el respondedor OCSP a un certificado firmado por una autoridad de certificación (CA) y vincular el certificado y la clave privada a un servidor virtual Secure Sockets Layer (SSL). Si necesita vincular un certificado y una clave privada diferentes a un respondedor OCSP que ya ha configurado, primero debe desvincular el respondedor y, a continuación, enlazar el respondedor a un certificado diferente.

### Para configurar OCSP

1. En la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Respondedor OCSP.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre , escriba un nombre para el perfil.
4. En URL, escriba la dirección web del respondedor OCSP.

   Este campo es obligatorio. La dirección web no puede superar los 32 caracteres.

5. Para almacenar en caché las respuestas de OCSP, haga clic en Caché y, en Tiempo de espera, escriba el número de minutos que NetScaler Gateway tiene la respuesta.
6. En Solicitar lote, haga clic en Habilitar.
7. En Retraso de procesamiento por lotes, especifique el tiempo, en milisegundos, permitido para agrupar por lotes un grupo de solicitudes OCSP.

   Los valores pueden ser de 0 a 10000. El valor predeterminado es 1.
8. En Producido At Time Skew, escriba la cantidad de tiempo que Citrix Gateway puede utilizar cuando el dispositivo necesita comprobar o aceptar la respuesta.
9. En Verificación de respuesta, seleccione Confiar en respuestas si quiere inhabilitar las comprobaciones de firma del respondedor de OCSP.

   Si habilita Respuestas de confianza, omita los pasos 8 y 9.
10. En Certificado, seleccione el certificado que se utiliza para firmar las respuestas de OCSP.

    Si no se selecciona un certificado, la CA a la que está vinculado el respondedor OCSP se utiliza para verificar las respuestas.
11. En Tiempo de espera de solicitud, escriba el número de milisegundos que debe esperar una respuesta de OCSP.

    Este tiempo incluye el tiempo de demora de procesamiento por lotes. Los valores pueden estar comprendidos entre 0 y 120000. El valor por defecto es 2000.
12. En Certificado de firma, seleccione el certificado y la clave privada utilizados para firmar las solicitudes de OCSP. Si no especifica un certificado ni una clave privada, las solicitudes no se firman.
13. Para habilitar la extensión número usado una vez (nonce), selecciona Nonce.
14. Para utilizar un certificado de cliente, haga clic en Inserción de certificados de cliente.
15. Haga clic en Create y, luego, en Close.

## Probar la configuración de NetScaler Gateway

January 26, 2024

Después de configurar la configuración inicial en NetScaler Gateway, puede probar la configuración conectándose al dispositivo.

Para probar la configuración de NetScaler Gateway, cree una cuenta de usuario local. A continuación, utilice la dirección IP del servidor virtual o el nombre de dominio completo (FQDN) del dispositivo, abra un explorador Web y escriba la dirección web. Por ejemplo, en la barra de direcciones, escriba`https://my.company.com` o `https://192.168.96.183`.

En la pantalla de inicio de sesión, introduzca el nombre de usuario y la contraseña de la cuenta de usuario que creó anteriormente. Después de iniciar sesión, se le pedirá que descargue e instale el plug-in de NetScaler Gateway.

Después de instalar y conectar correctamente con el plug-in de NetScaler Gateway, aparece la interfaz de acceso. La interfaz de acceso es la página principal predeterminada de NetScaler Gateway.

### Crear una nueva cuenta de usuario mediante la utilidad de configuración

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Administración de usuarios y, a continuación, haga clic en Usuarios AAA.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre de usuario, escriba el nombre de usuario.
4. Si utiliza la autenticación local, desactive la casilla Autenticación externa. La autenticación de usuarios con tipos de autenticación externa, como LDAP o RADIUS, es la opción predeterminada. Si desactiva esta casilla de verificación, NetScaler Gateway autentica a los usuarios.
5. En Contraseña y Confirmar contraseña, escriba la contraseña del usuario, haga clic en Crear y, a continuación, en Cerrar.

Al agregar usuarios mediante la utilidad de configuración, puede enlazar las siguientes directivas al usuario:

- Autorización
- Tráfico, sesión y auditoría
- Marcadores
- Aplicaciones de intranet
- Direcciones IP de intranet

Si tiene problemas para iniciar sesión con la cuenta de usuario de prueba, compruebe lo siguiente:

- Si recibe una advertencia de certificado, se instala un certificado de prueba o un certificado no válido en NetScaler Gateway. Si hay un certificado firmado por una entidad de certificación (CA) instalado en el dispositivo, asegúrese de que haya un certificado raíz correspondiente en el dispositivo del usuario.
- Si utilizó un certificado firmado por una entidad emisora de certificados, compruebe que ha generado el certificado de sitio correctamente mediante la solicitud de firma de certificado (CSR) firmada y que los datos de nombre distintivo (DN) introducidos en la CSR son correctos. El problema también puede deberse a que el nombre del host no coincide con la dirección IP que figura

en el certificado firmado. Compruebe que el nombre común del certificado configurado corresponde a la información de dirección IP del servidor virtual configurado.
- Si no aparece la pantalla de inicio de sesión o si aparece algún otro mensaje de error, revise el proceso de configuración y confirme que ha realizado todos los pasos correctamente y que ha introducido todos los parámetros correctamente.

## Creación de servidores virtuales

January 26, 2024

Un servidor virtual es un punto de acceso en el que los usuarios inician sesión. Cada servidor virtual tiene su propia dirección IP, certificado y conjunto de directivas. Un servidor virtual consiste en una combinación de dirección IP, puerto y protocolo que acepta tráfico entrante. Los servidores virtuales contienen la configuración de conexión para cuando los usuarios inician sesión en el dispositivo. Puede configurar los siguientes ajustes en los servidores virtuales:

- Certificados
- Autenticación
- Directivas
- Marcadores
- Grupos de direcciones (también conocidos como grupos de IP o IP de intranet)
- Implementación DMZ de doble salto con NetScaler Gateway
- Secure Tíquet Authority
- Transferencia de sesión proxy ICA SmartAccess

Si ejecuta el asistente de NetScaler Gateway, puede crear un servidor virtual durante el asistente. Puede configurar servidores virtuales adicionales de las siguientes maneras:

- **Desde el nodo servidores virtuales**. Este nodo se encuentra en el panel de navegación de la utilidad de configuración. Puede agregar, modificar y quitar servidores virtuales mediante la utilidad de configuración.
- **Con el asistente de configuración rápida**. Si implementa Citrix Endpoint Management, StoreFront o la Interfaz Web en su entorno, puede usar el asistente de configuración rápida para crear el servidor virtual y todas las políticas necesarias para la implementación.

Si quiere que los usuarios inicien sesión y utilicen un tipo de autenticación específico, como RADIUS, puede configurar un servidor virtual y asignar al servidor una dirección IP única. Cuando los usuarios inician sesión, se les dirige al servidor virtual y, a continuación, se les solicitan sus credenciales RADIUS.

También puede configurar las formas en que los usuarios inician sesión en NetScaler Gateway. Puede utilizar una directiva de sesión para configurar el tipo de software de usuario, el método de acceso y la página principal que ven los usuarios tras iniciar sesión.

## Para crear servidores virtuales

January 26, 2024

Puede agregar, modificar, habilitar o inhabilitar y quitar servidores virtuales mediante la GUI de NetScaler Gateway o el asistente de configuración rápida. Para obtener más información sobre cómo configurar un servidor virtual con el Asistente de configuración rápida, consulte Configuración de valores con el Asistente de configuración rápida.

### Para crear un servidor virtual mediante la interfaz gráfica de usuario

1. En la pestaña Configuración, vaya a **Citrix Gateway > Servidores virtuales** .
2. En el panel de detalles, haga clic en **Agregar**.
3. Configure los ajustes según sus necesidades.
4. Haga clic en **Create** y, luego, en **Close**.

### Para crear un servidor virtual mediante la CLI

En la línea de comandos, escriba;

```
add vpn vserver <name> <serviceType> [<IPAddress> [<port>]
<!--NeedCopy-->
```

**Ejemplo:**

```
add vpn vserver gatewayserver SSL 1.1.1.1 443
<!--NeedCopy-->
```

### Puntos a tener en cuenta al enlazar un perfil de red al servidor virtual de VPN

Puede crear perfiles de red (perfiles de red) para configurar el dispositivo de modo que utilice una dirección IP de origen especificada y vincular el perfil de red al servidor virtual de VPN. Sin embargo, tenga en cuenta lo siguiente al vincular un perfil de red al servidor virtual de VPN.

- Al enlazar un perfil de red a un servidor virtual de NetScaler Gateway, el perfil de red no selecciona un SNIP específico para que lo utilice el servidor virtual o el servicio para el tráfico a los

servidores back-end. En su lugar, el dispositivo de puerta de enlace ignora el enlace del perfil de red y utiliza el método round robin para seleccionar los SNIP.

- El perfil de red no funciona para los servicios generados dinámicamente (STA, monitor SF). Para STA y otros servicios generados dinámicamente, puede enlazar el perfil de red a esos monitores directamente y esos monitores se utilizarán en ese momento. Sin embargo, si tiene varias puertas de enlace en el mismo dispositivo, todas las puertas de enlace utilizan el mismo perfil de red para los monitores configurados.

Para obtener más información sobre el perfil de red, consulte Usar una IP de origen especificada para la comunicación back-end.

## Configurar tipos de conexión en el servidor virtual

March 27, 2024

Al crear y configurar un servidor virtual, puede configurar las siguientes opciones de conexión:

- Conexiones con Citrix Receiver solo a aplicaciones virtuales y escritorios de Citrix sin funciones de SmartAccess, análisis de endpoints o túnel de capa de red.
- Conexiones con el plug-in de NetScaler Gateway y SmartAccess, que permiten el uso de SmartAccess, análisis de extremos y funciones de túnel de capa de red.
- Conexiones con Secure Hub que establece una conexión Micro VPN desde dispositivos móviles a NetScaler Gateway.
- Conexiones paralelas realizadas a través del protocolo de sesión ICA por un usuario desde varios dispositivos. Las conexiones se migran a una sola sesión para evitar el uso de varias licencias universales.

Si quiere que los usuarios inicien sesión sin software de usuario, puede configurar una directiva de acceso sin cliente y vincularla al servidor virtual.

### Para configurar conexiones Basic o SmartAccess en un servidor virtual

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para el servidor virtual.
4. En Dirección IP y puerto, escriba la dirección IP y el número de puerto del servidor virtual.
5. Lleve a cabo una de las siguientes acciones:
    - Para permitir únicamente conexiones ICA, haga clic en Modo básico.

- Para permitir el inicio de sesión del usuario con Secure Hub, el plug-in de NetScaler Gateway y SmartAccess, haga clic en Modo SmartAccess.
- Para permitir que SmartAccess administre las sesiones de proxy ICA para conexiones de varios usuarios, haga clic en Migración de sesiones de proxy ICA.

6. Configure las demás opciones del servidor virtual, haga clic en Crear y, a continuación, en Cerrar.

## Configurar una directiva de escucha para servidores virtuales comodín

March 27, 2024

Puede configurar los servidores virtuales de NetScaler Gateway para restringir la capacidad de un servidor virtual de escuchar en una VLAN específica. Puede crear un servidor virtual comodín con una directiva de escucha que lo restrinja al procesamiento del tráfico en la VLAN especificada.

Los parámetros de configuración son los siguientes:

| Parámetro | Descripción |
|---|---|
| Nombre | Nombre del servidor virtual. El nombre es obligatorio y no se puede cambiar después de crear el servidor virtual. El nombre no puede superar los 127 caracteres y el primer carácter debe ser un número o una letra. También puede usar los siguientes caracteres: símbolo (@), guión bajo (_), guión (-), punto (.), dos puntos (:), signo de almohadilla (#) y un espacio. |
| IP | Dirección IP del servidor virtual. Para un servidor virtual comodín vinculado a la VLAN, el valor siempre es *. |
| Tipo | El comportamiento del servicio. Sus opciones son HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP y RTSP. |
| Puerto | Puerto en el que el servidor virtual escucha las conexiones de usuario. El número de puerto debe estar comprendido entre 0 y 65535. Para el servidor virtual comodín enlazado a una VLAN, el valor suele ser *. |

| Parámetro | Descripción |
| --- | --- |
| Escucha Prioridad | Prioridad asignada a la directiva de escucha. La prioridad se evalúa en orden inverso; cuanto menor sea el número, mayor será la prioridad asignada a la directiva de escucha. |
| Regla de directiva de escucha | Regla de directiva que se va a utilizar para identificar la VLAN a la que debe escuchar el servidor virtual. La regla es: CLIENT.VLAN.ID.EQ (<ipaddressat>) Por <ipaddressat>, sustituya el número de ID asignado a la VLAN. |

### Para crear un servidor virtual comodín con una directiva de escucha

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para el servidor virtual.
4. En Protocolo, seleccione el protocolo.
5. En Dirección IP, escriba la dirección IP del servidor virtual.
6. En Puerto, escriba el puerto del servidor virtual.
7. En la ficha Avanzadas, en Directiva de escucha, en Prioridad de escucha, escriba la prioridad de la directiva de escucha.
8. Junto a Regla de directiva de escucha, haga clic en Configurar.
9. En el cuadro de diálogo Crear expresión, haga clic en Agregar, configure la expresión y, a continuación, haga clic en Aceptar.
10. Haga clic en Creary, a continuación, en Cerrar.

## Configurar direcciones IP en NetScaler Gateway

January 26, 2024

Puede configurar direcciones IP para iniciar sesión en la utilidad de configuración y para las conexiones de usuario. NetScaler Gateway está configurado con una dirección IP predeterminada de 192.168.100.1 y una máscara de subred 255.255.0.0 para el acceso de administración. La dirección IP predeterminada se utiliza cuando no hay un valor configurado por el usuario para la dirección IP del sistema (NSIP).

- Dirección NSIP. Dirección IP de administración de NetScaler Gateway que se utiliza para todos los accesos relacionados con la administración al dispositivo. NetScaler Gateway también utiliza la dirección NSIP para la autenticación.
- Puerta de**enlace predeterminada**. Enrutador que reenvía el tráfico desde fuera de la red segura a NetScaler Gateway.
- **Dirección IP de subred (SNIP)**. Dirección IP que representa el dispositivo del usuario mediante la comunicación con un servidor de una red secundaria.

La dirección SNIP utiliza los puertos 1024 a 64000.

### Cómo usa Citrix Gateway las direcciones IP

NetScaler Gateway obtiene el tráfico de las direcciones IP en función de la función que se está produciendo. En la lista siguiente se describen varias funciones y la forma en que NetScaler Gateway utiliza las direcciones IP para cada una de ellas, como pauta general:

- **Autenticación.** La dirección IP que utiliza NetScaler Gateway depende del tipo de servidor de autenticación.
  - Servidores LDAP/RADIUS/TACACS. Si AAAD se comunica directamente con el servidor virtual de autenticación, se utiliza la dirección NSIP.
  - Si se utiliza un equilibrador de carga como proxy, el equilibrador de carga utiliza la dirección SNIP para la autenticación. AAAD usa la dirección NSIP para comunicarse con el balanceador de cargas. La dirección IP que utiliza NetScaler ADC depende de la entidad que se comunica con el servidor virtual de autenticación.
  - Servidores SAML/OAUTH/WEBAUTH: Estos servidores se comunican mediante la dirección SNIP.
- **Transferencias de archivos desde la página principal.** NetScaler Gateway utiliza la dirección SNIP.
- **Consultas DNS y WINS.** NetScaler Gateway utiliza la dirección SNIP.
- **Tráfico de red a los recursos de la red segura.** NetScaler Gateway utiliza la dirección SNIP o la agrupación de IP, según la configuración de NetScaler Gateway.
- **Configuración del proxy ICA.** NetScaler Gateway utiliza la dirección SNIP.

## Cambiar o eliminar direcciones IP asignadas

January 26, 2024

Citrix Gateway admite una dirección IP asignada. Si configura una dirección IP asignada en el dispositivo, no puede cambiar ni eliminar la dirección. Si necesita cambiar la dirección IP asignada, primero debe crear una nueva dirección IP asignada y, a continuación, eliminar la dirección IP asignada original.

Puede usar el asistente de configuración o el nodo Red de la utilidad de configuración para configurar direcciones IP mapeadas adicionales.

### Para crear una nueva dirección IP mapeada

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Sistema > Red y, a continuación, haga clic en IP.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear IP, en Dirección IP, escriba la dirección IP.
4. En Máscara de red, escriba la máscara de subred.
5. En Tipo de IP, selecciona IP asignada y, a continuación, haz clic en Crear.

### Para eliminar una dirección IP asignada

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Sistema > Red y, a continuación, haga clic en IP.
2. En el panel de detalles, haga clic en la dirección asignada y, a continuación, en Eliminar.

## Configurar direcciones IP de subred

January 26, 2024

La dirección IP de subred permite al usuario conectarse a NetScaler Gateway desde un host externo que reside en otra subred. Al agregar una dirección IP de subred, se realiza una entrada de ruta correspondiente en la tabla de rutas. Solo se realiza una entrada por subred. La entrada de ruta corresponde a la primera dirección IP agregada en la subred.

A diferencia de la dirección IP del sistema y la dirección IP asignada, no es obligatorio especificar la dirección IP de la subred durante la configuración inicial de Citrix Gateway.

La dirección IP asignada y las direcciones IP de subred utilizan los puertos 1024 a 64000.

### Para agregar una dirección IP de subred

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Sistema > Red y, a continuación, haga clic en IP.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Crear IP, en Dirección IP, escriba la dirección IP.
4. En Máscara de red, escriba la máscara de subred.
5. En Tipo de IP, seleccione IP de subred, haga clic en Cerrar y, a continuación, en Crear.

## Configurar IPv6 para conexiones de usuario

January 26, 2024

Puede configurar NetScaler Gateway para que escuche las conexiones de los usuarios mediante el Protocolo de Internet versión 6 (IPv6). Al configurar una de las siguientes opciones, puede activar la casilla de verificación IPv6 y, a continuación, introducir la dirección IPv6 en el cuadro de diálogo:

- Configuración global - Aplicaciones publicadas - ICA Proxy
- Autentificación global: RADIUS
- Autenticación global: LDAP
- Autenticación global - TACACS
- Perfil de sesión - Aplicaciones publicadas - ICA Proxy
- Servidores virtuales NetScaler Gateway
- Crear servidor de autenticación: RADIUS
- Crear servidor de autenticación: LDAP
- Crear servidor de autenticación - TACACS
- Crear servidor de auditoría
- Configuración de alta disponibilidad
- Enlazar o desvincular monitores de ruta para obtener alta disponibilidad
- Servidor virtual (equilibrio de carga)

Cuando configura el servidor virtual de NetScaler Gateway para que escuche en una dirección IPv6, los usuarios solo pueden conectarse con Citrix Receiver. Las conexiones de usuario con el plug-in de NetScaler Gateway no son compatibles con IPv6.

Puede utilizar las siguientes directrices para configurar IPv6 en NetScaler Gateway:

- Citrix Virtual Apps e Interfaz Web. Al configurar IPv6 para conexiones de usuario y si hay una dirección IP asignada que utiliza IPv6, los servidores de Citrix Virtual Apps e Interfaz Web también pueden usar IPv6. La Interfaz Web debe instalarse detrás de NetScaler Gateway. Cuando los

usuarios se conectan a través de NetScaler Gateway, la dirección IPv6 se traduce a IPv4. Cuando vuelve la conexión, la dirección IPv4 se traduce a IPv6.

- Servidores virtuales. Puede configurar IPv6 para un servidor virtual cuando ejecuta el asistente de NetScaler Gateway. En el asistente de NetScaler Gateway de la página Servidores virtuales, haga clic en IPv6 e introduzca la dirección IP. Solo puede utilizar la configuración de una dirección IPv6 para un servidor virtual mediante el asistente de NetScaler Gateway.
- Otros. Para configurar IPv6 para proxy ICA, autenticación, auditoría y alta disponibilidad, active la casilla de verificación IPv6 en el cuadro de diálogo y, a continuación, escriba la dirección IP.

## Resolver servidores DNS ubicados en la red segura

January 26, 2024

Si su servidor DNS se encuentra en la red segura detrás de un firewall y el firewall bloquea el tráfico ICMP, no podrá probar las conexiones con el servidor porque el firewall bloquea la solicitud. Puede resolver este problema siguiendo los siguientes pasos:

- Creación de un servicio DNS con un monitor DNS personalizado que se resuelve en un nombre de dominio completo (FQDN) conocido.
- Creación de un servidor virtual DNS no direccionable directamente en NetScaler Gateway.
- Vincular el servicio al servidor virtual.

**Nota**:

- Configure un servidor virtual DNS y un servicio DNS solo si el servidor DNS se encuentra detrás de un firewall.
- Si instala una licencia de equilibrio de carga de NetScaler ADC en el dispositivo, el nodo Servidores y servicios virtuales no aparece en el panel de navegación. Puede realizar este procedimiento expandiendo Equilibrio de carga y, a continuación, haciendo clic en Servidores virtuales.

### Para configurar un servicio DNS y un monitor DNS

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Servidores y servicios virtuales y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para el servicio.
4. En Protocolo, selecciona DNS.
5. En Dirección IP, escriba la dirección IP del servidor DNS.

6. En Puerto, escriba el número de puerto.
7. En la ficha Servicios, haga clic en Agregar.
8. En la ficha Monitores, en Disponible, seleccione DNS, haga clic en Agregar, en Crear y, a continuación, en Cerrar.
9. En el cuadro de diálogo Crear servidor virtual (equilibrio de carga), haga clic en Crear y, a continuación, en Cerrar.

A continuación, cree el servidor virtual DNS. Para obtener más información, consulte Para configurar un servidor virtual DNS y, a continuación, vincular el servicio DNS al servidor virtual.

### Para enlazar un servicio DNS a un servidor virtual DNS

1. En el cuadro de diálogo Configurar servicio virtual (equilibrio de carga), en la ficha Servicios, haga clic en Agregar, seleccione el servicio DNS, haga clic en Crear y, a continuación, haga clic en Cerrar.

## Configurar servidores virtuales DNS

January 26, 2024

Para configurar un servidor virtual DNS, especifique un nombre y una dirección IP. Al igual que el servidor virtual de NetScaler Gateway, debe asignar una dirección IP al servidor virtual DNS. Sin embargo, esta dirección IP debe estar en el lado interno de la red de destino para que los dispositivos de usuario resuelvan todas las direcciones internas. También debe especificar el puerto DNS.

**Nota**: Si instala una licencia de equilibrio de carga de NetScaler ADC en el dispositivo, el nodo Servidores y servicios
virtuales no aparece en el panel de navegación. Puede configurar esta función mediante el servidor virtual de equilibrio de carga. Para obtener más información, consulte la documentación de Citrix ADC en la documentación de productos Citrix.

### Para configurar un servidor virtual DNS

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Servidores y servicios virtuales y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para el servidor virtual.
4. En Dirección IP, escriba la dirección IP del servidor DNS.
5. En Puerto, escriba el puerto en el que escucha el servidor DNS.

6. En Protocolo, seleccione DNS y, a continuación, haga clic en Crear.

Por último, asocie el servidor virtual DNS con NetScaler Gateway mediante uno de los dos métodos siguientes, según las necesidades de la implementación:

- Enlazar el servidor globalmente a NetScaler Gateway.
- Enlazar el servidor virtual DNS por servidor virtual.

Si implementa el servidor virtual DNS de forma global, todos los usuarios tienen acceso a él. A continuación, puede restringir a los usuarios vinculando el servidor virtual DNS al servidor virtual.

## Configurar proveedores de servicios de nombres

March 27, 2024

NetScaler Gateway utiliza proveedores de servicios de nombres para convertir direcciones web en direcciones IP.

Al ejecutar el asistente de NetScaler Gateway, puede configurar un servidor DNS o un servidor WINS. Puede usar la utilidad de configuración para configurar también servidores DNS o WINS adicionales.

### Para agregar un servidor DNS a NetScaler Gateway

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Configuración de red, haga clic en Agregar.
4. En el cuadro de diálogo Insertar servidor de nombres, en Dirección IP, escriba la dirección IP del servidor DNS, haga clic en Crear y, a continuación, haga clic en Cerrar.
5. Haga clic en Aceptar en la utilidad de configuración.

### Para agregar un servidor WINS a NetScaler Gateway

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Configuración de red, en IP del servidor WINS, escriba la dirección IP del servidor WINS y, a continuación, haga clic en Aceptar.

A continuación, especifique el nombre del servidor virtual DNS y la dirección IP. Al igual que el servidor virtual de NetScaler Gateway, se debe asignar una dirección IP al servidor virtual. Sin embargo, esta dirección IP debe estar en el lado interno de la red de destino para que los dispositivos de usuario resuelvan correctamente todas las direcciones internas. También debe especificar el puerto DNS.

Si configura un servidor DNS y un servidor WINS para la resolución de nombres, puede utilizar el asistente de NetScaler Gateway para seleccionar qué servidor realiza primero la búsqueda de nombres.

### Para especificar la prioridad de búsqueda de nombres

1. En la utilidad de configuración, haga clic en la pestaña Configuración y, a continuación, en el panel de navegación, haga clic en Citrix Gateway .
2. En el panel de detalles, en Introducción, haga clic en el asistente Citrix Gateway .
3. Haga clic en Siguiente para aceptar la configuración actual hasta que acceda a la página Proveedores de servicios de nombres.
4. En Prioridad de búsqueda de nombres, seleccione WINS o DNS y, a continuación, continúe hasta el final del asistente.

## Configurar conexiones iniciadas por el servidor

January 26, 2024

Para cada usuario que inició sesión en NetScaler Gateway con direcciones IP habilitadas, el sufijo DNS se anexa al nombre de usuario y se agrega un registro de dirección DNS a la caché DNS del dispositivo. Esta técnica ayuda a proporcionar a los usuarios un nombre DNS en lugar de las direcciones IP de los usuarios.

Cuando se asigna una dirección IP a la sesión de un usuario, es posible conectarse al dispositivo del usuario desde la red interna. Por ejemplo, los usuarios que se conectan con el cliente de escritorio remoto o de computación en red virtual (VNC) pueden acceder al dispositivo de usuario para diagnosticar una aplicación problemática. También es posible que dos usuarios de NetScaler Gateway con direcciones IP de red internas que hayan iniciado sesión de forma remota se comuniquen entre sí a través de NetScaler Gateway. Permitir el descubrimiento de las direcciones IP de la red interna de los usuarios que han iniciado sesión en el dispositivo ayuda a esta comunicación.

Un usuario remoto puede utilizar el siguiente comando ping para descubrir la dirección IP de la red interna de un usuario que puede iniciar sesión en NetScaler Gateway:

ping

Un servidor puede iniciar una conexión con un dispositivo de usuario de las siguientes formas:

- Conexiones TCP o UDP. Las conexiones pueden originarse en un sistema externo de la red interna o en otro equipo que haya iniciado sesión en NetScaler Gateway. La dirección IP de red interna asignada a cada dispositivo de usuario que ha iniciado sesión en NetScaler Gateway se utiliza para estas conexiones. Los siguientes son los diferentes tipos de conexiones iniciadas por el servidor que admite Citrix Gateway:
  Para las conexiones iniciadas por el servidor TCP o UDP, el servidor tiene conocimientos previos sobre la dirección IP y el puerto del dispositivo de usuario y establece una conexión con ellos. NetScaler Gateway intercepta esta conexión.

  A continuación, el dispositivo del usuario establece una conexión inicial con el servidor y el servidor se conecta al dispositivo de usuario en un puerto conocido o derivado del primer puerto configurado.

  En este caso, el dispositivo del usuario establece una conexión inicial con el servidor y, a continuación, intercambia puertos y direcciones IP con el servidor mediante un protocolo específico de la aplicación en el que se incrusta esta información. Esto permite que NetScaler Gateway admita aplicaciones, como conexiones FTP activas.
- Comando Port. Se utiliza en un FTP activo y en determinados protocolos de voz sobre IP.
- Conexiones entre plug-ins. NetScaler Gateway admite conexiones entre complementos mediante las direcciones IP de la red interna.

  Con este tipo de conexión, dos dispositivos de usuario de NetScaler Gateway que utilizan el mismo NetScaler Gateway pueden iniciar conexiones entre sí. Un ejemplo de este tipo es el uso de aplicaciones de mensajería instantánea, como Office Communicator o Yahoo! Mensajero.

Si un usuario cierra la sesión de NetScaler Gateway y la solicitud de cierre de sesión no llega al dispositivo, el usuario puede volver a iniciar sesión con cualquier dispositivo y reemplazar la sesión anterior por una nueva. Esta función puede ser beneficiosa en implementaciones en las que se asigna una dirección IP por usuario.

Cuando un usuario inicia sesión en NetScaler Gateway por primera vez, se crea una sesión y se asigna una dirección IP al usuario. Si el usuario cierra la sesión, pero la solicitud de cierre de sesión se pierde o el dispositivo del usuario no logra cerrar la sesión sin errores, la sesión se mantiene en el sistema. Si el usuario intenta volver a iniciar sesión desde el mismo dispositivo o desde otro dispositivo, tras la autenticación correcta, aparece el cuadro de diálogo Transferir inicio de sesión. Si el usuario decide transferir el inicio de sesión, la sesión anterior de NetScaler Gateway se cierra y se crea una nueva sesión. La transferencia de inicio de sesión está activa solo dos minutos después del cierre de sesión, y si se intenta iniciar sesión desde varios dispositivos simultáneamente, el último intento de inicio de sesión reemplaza la sesión original.

# Configurar el enrutamiento en NetScaler Gateway

January 26, 2024

Para proporcionar acceso a los recursos de la red interna, Citrix Gateway debe poder redirigir los datos a sus redes internas y seguras. De forma predeterminada, NetScaler Gateway utiliza una ruta estática.

Las redes a las que NetScaler Gateway puede redirigir los datos se determinan por la forma en que se configura la tabla de redirección de NetScaler Gateway y la puerta de enlace predeterminada especificada para NetScaler Gateway.

La tabla de enrutamiento de Citrix Gateway debe contener las rutas necesarias para enrutar los datos a cualquier recurso de red interna al que un usuario pueda necesitar acceder.

NetScaler Gateway admite los siguientes protocolos de redirección:

- Protocolo de información de redirección (RIP v1 y v2)
- Abrir primero el trayecto más corto (OSPF)
- Protocolo de puerta de enlace fronteriza (BGF)

## Configuración de una ruta estática

Al configurar la comunicación con otro host o red, es posible que deba configurar una ruta estática desde Citrix Gateway al nuevo destino si no utiliza el enrutamiento dinámico.

### Para configurar una ruta estática

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema > Red > Avanzado y, a continuación, haga clic en Rutas.
2. En el panel de detalles, en la ficha Básico, haga clic en Agregar.
3. Configure los ajustes de la ruta y, a continuación, haga clic en Crear.

### Para probar una ruta estática

1. En la utilidad de configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Diagnóstico.
2. En el panel de detalles, en Utilidades, haga clic en Hacer ping.
3. En Parámetros, en Nombre de host, escriba el nombre del dispositivo.

4. En Avanzado, en Dirección IP de origen, escriba la dirección IP del dispositivo y, a continuación, haga clic en Ejecutar.

   Si se comunica correctamente con el otro dispositivo, los mensajes indican que se transmitieron y recibieron el mismo número de paquetes y que se perdieron cero paquetes.

   Si no se comunica con el otro dispositivo, los mensajes de estado indican que se han recibido cero paquetes y se han perdido todos los paquetes. Para corregir esta falta de comunicación, repita el procedimiento para agregar una ruta estática.

Para detener la prueba, en el cuadro de diálogo Ping, haga clic en Detener y, a continuación, en Cerrar.

## Configurar la negociación automática

January 26, 2024

De forma predeterminada, el dispositivo está configurado para utilizar la negociación automática, en la que NetScaler Gateway transmite el tráfico de red en ambas direcciones simultáneamente y determina la velocidad del adaptador adecuada. Si deja la configuración predeterminada en Negociación automática, NetScaler Gateway utiliza la operación de dúplex completo, en la que el adaptador de red puede enviar datos en ambas direcciones simultáneamente.

Si inhabilita la negociación automática, NetScaler Gateway utiliza la operación semidúplex, en la que el adaptador puede enviar datos en ambas direcciones entre dos nodos, pero el adaptador solo puede usar una dirección u otra a la vez.

Para la primera instalación, Citrix recomienda configurar NetScaler Gateway para que utilice la negociación automática en los puertos conectados al dispositivo. Después de iniciar sesión inicialmente y configurar NetScaler Gateway, puede inhabilitar la negociación automática. No se puede configurar la negociación automática de forma global. Debe habilitar o inhabilitar la configuración para cada interfaz.

### Para habilitar o inhabilitar la negociación automática

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Sistema > Red y, a continuación, haga clic en Interfaces.
2. En el panel de detalles, seleccione la interfaz y, a continuación, haga clic en Abrir.
3. Realice una de las siguientes acciones en el cuadro de diálogo Configurar interfaz :

   - Para habilitar la negociación automática, haga clic en Sí junto a Negociación automática y, a continuación, haga clic en Aceptar.

- Para inhabilitar la negociación automática, haga clic en No junto a Negociación automática y, a continuación, haga clic en Aceptar.

## Autenticación y autorización

January 26, 2024

NetScaler Gateway emplea un diseño de autenticación flexible que permite una amplia personalización de la autenticación de usuarios para NetScaler Gateway. Puede utilizar servidores de autenticación estándar del sector y configurar NetScaler Gateway para autenticar a los usuarios en los servidores. NetScaler Gateway también admite la autenticación basada en los atributos presentes en un certificado de cliente. La autenticación de Citrix Gateway está diseñada para adaptarse a procedimientos de autenticación sencillos que utilizan una única fuente para la autenticación de usuarios, además de procedimientos de autenticación en cascada más complejos que se basan en varios tipos de autenticación.

La autenticación de NetScaler Gateway incorpora autenticación local para la creación de usuarios y grupos locales. Este diseño se centra en el uso de directivas para controlar los procedimientos de autenticación que configura. Las directivas que cree se pueden aplicar a nivel de servidor virtual o global de NetScaler Gateway y se pueden utilizar para establecer los parámetros del servidor de autenticación de forma condicional en función de la red de origen del usuario.

Dado que las directivas están enlazadas de forma global o a un servidor virtual, también puede asignar prioridades a sus directivas para crear una cascada de varios servidores de autenticación como parte de la autenticación.

NetScaler Gateway incluye compatibilidad con los siguientes tipos de autenticación.

- Locales
- Protocolo ligero de acceso a directorios (LDAP)
- RADIUS
- SAML
- TACACS+
- Autenticación de certificado de cliente (incluida la autenticación con tarjeta inteligente)

NetScaler Gateway también admite RSA SecurID, Gemalto Protiva y SafeWord. Se utiliza un servidor RADIUS para configurar estos tipos de autenticación.

Aunque la autenticación permite a los usuarios iniciar sesión en NetScaler Gateway y conectarse a la red interna, la autorización define los recursos de la red segura a los que tienen acceso los usuarios. La autorización se configura con directivas LDAP y RADIUS.

# Configurar los tipos de autenticación global predeterminados

January 26, 2024

Al instalar NetScaler Gateway y ejecutar el asistente de NetScaler Gateway, configuró la autenticación en el asistente. Esta directiva de autenticación está vinculada automáticamente al nivel global de Citrix Gateway. El tipo de autenticación que configura en el asistente de NetScaler Gateway es el tipo de autenticación predeterminado. Puede cambiar el tipo de autorización predeterminado ejecutando de nuevo el asistente de Citrix Gateway o modificar la configuración de autenticación global en la utilidad de configuración.

Si necesita agregar tipos de autenticación adicionales, puede configurar directivas de autenticación en NetScaler Gateway y enlazar las directivas a NetScaler Gateway mediante la utilidad de configuración. Al configurar la autenticación de forma global, se define el tipo de autenticación, se configuran los valores y se establece el número máximo de usuarios que se pueden autenticar.

Después de configurar y vincular la directiva, puede establecer la prioridad para definir qué tipo de autenticación tiene prioridad. Por ejemplo, se configuran las directivas de autenticación LDAP y RADIUS. Si la directiva LDAP tiene un número de prioridad de 10 y la directiva RADIUS tiene un número de prioridad de 15, la directiva LDAP tiene prioridad, independientemente de dónde vincule cada directiva. Esto se denomina autenticación en cascada.

Puede elegir entregar páginas de inicio de sesión desde la memoria caché en memoria de Citrix Gateway o desde el servidor HTTP que se ejecuta en Citrix Gateway. Si decide entregar la página de inicio de sesión desde la memoria caché en memoria, la entrega de la página de inicio de sesión desde NetScaler Gateway es considerablemente más rápida que desde el servidor HTTP. La opción de entregar la página de inicio de sesión desde la memoria caché en memoria reduce el tiempo de espera cuando un gran número de usuarios inician sesión al mismo tiempo. Solo puede configurar la entrega de páginas de inicio de sesión desde la caché como parte de una directiva de autenticación global.

También puede configurar la dirección IP de traducción de direcciones de red (NAT) que es una dirección IP específica para la autenticación. Esta dirección IP es única para la autenticación y no es la subred de Citrix Gateway, las direcciones IP asignadas ni las direcciones IP virtuales. Este es un parámetro opcional.

**Nota**: No se puede utilizar el asistente de NetScaler Gateway para configurar la autenticación SAML.

Puede utilizar el Asistente de configuración rápida para configurar la autenticación de certificados de cliente, LDAP y RADIUS. Al ejecutar el asistente, puede seleccionar entre un servidor LDAP o RADIUS existente configurado en Citrix Gateway. También puede configurar los ajustes de LDAP o RADIUS. Si utiliza la autenticación de dos factores, Citrix recomienda utilizar LDAP como tipo de autenticación principal.

### Para configurar la autenticación de forma global

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración, haga clic en Cambiar la configuración de autenticación.
3. En Número máximo de usuarios, escriba el número de usuarios que se pueden autenticar mediante este tipo de autenticación.
4. En Dirección IP NAT, escriba la dirección IP única para la autenticación.
5. Seleccione Activar almacenamiento encaché estático para entregar las páginas de inicio de sesión más rápido.
6. Seleccione Habilitar comentarios de autenticación mejorada para enviar un mensaje a los usuarios si la autenticación falla. El mensaje que reciben los usuarios incluye errores de contraseña, cuenta inhabilitada o bloqueada, o no se encuentra al usuario, por nombrar algunos.
7. En Tipo de autenticación predeterminado, seleccione el tipo de autenticación.
8. Configure la configuración del tipo de autenticación y, a continuación, haga clic en Aceptar.

## Configurar la autenticación sin autorización

January 26, 2024

La autorización define los recursos a los que los usuarios pueden conectarse a través de NetScaler Gateway. Las directivas de autorización se configuran mediante una expresión y, a continuación, se establece que se permita o deniegue la directiva. Puede configurar NetScaler Gateway para que utilice únicamente la autenticación, sin autorización.

Al configurar la autenticación sin autorización, NetScaler Gateway no realiza ninguna comprobación de autorización de grupo. Las directivas que configura para el usuario o el grupo se asignan al usuario.

Para obtener más información sobre cómo configurar la autorización, consulte Configuración de la autorización.

## Configuración de autorización

January 26, 2024

La autorización especifica los recursos de red a los que tienen acceso los usuarios cuando inician sesión en NetScaler Gateway. La configuración predeterminada de la autorización es denegar el acceso a todos los recursos de red. Citrix recomienda utilizar la configuración global predeterminada y, a continuación, crear directivas de autorización para definir los recursos de red a los que pueden acceder los usuarios.

La autorización se configura en NetScaler Gateway mediante expresiones y directivas de autorización. Después de crear una directiva de autorización, puede vincularla a los usuarios o grupos que haya configurado en el dispositivo.

## Configuración de directivas de autorización

March 27, 2024

Al configurar una directiva de autorización, puede configurarla para permitir o denegar el acceso a los recursos de red de la red interna. Por ejemplo, para permitir que los usuarios accedan a la red 10.3.3.0, utilice la siguiente expresión:

CLIENT.IP.DST.IN_SUBNET (10.3.0.0/16)

Las directivas de autorización se aplican a usuarios y grupos. Después de autenticar a un usuario, NetScaler Gateway realiza una comprobación de autorización de grupo obteniendo la información del grupo del usuario de un servidor RADIUS, LDAP o TACACS+. Si la información del grupo está disponible para el usuario, NetScaler Gateway comprueba los recursos de red permitidos para el grupo.

Para controlar a qué recursos pueden acceder los usuarios, debe crear directivas de autorización. Si no necesita crear directivas de autorización, puede configurar la autorización global predeterminada.

Si crea una expresión dentro de la directiva de autorización que deniegue el acceso a una ruta de archivo, solo puede utilizar la ruta de acceso del subdirectorio y no el directorio raíz. Por ejemplo, use fs.path contiene "dir1dir2"en lugar de fs.path contiene "rootdirdir1dir2". Si utiliza la segunda versión de este ejemplo, se produce un error en la directiva.

Después de configurar la directiva de autorización, la vinculará a un usuario o grupo como se muestra en las tareas siguientes.

De forma predeterminada, las directivas de autorización se validan primero con las directivas vinculadas al servidor virtual y, a continuación, con las directivas vinculadas globalmente. Si vincula una directiva de forma global y quiere que la directiva global tenga prioridad sobre una directiva vinculada a un usuario, grupo o servidor virtual, puede cambiar el número de prioridad de la directiva. Los números de prioridad empiezan en cero. Un número de prioridad más bajo otorga a la directiva mayor prioridad.

Por ejemplo, si la directiva global tiene un número de prioridad de uno y el usuario tiene una prioridad de dos, la directiva de autenticación global se aplica primero.

> **Importante:**
>
> - Las directivas de autorización clásicas solo se aplican al tráfico TCP.
> - La directiva de autorización avanzada se puede aplicar a todos los tipos de tráfico (TCP/UDP/ICMP/DNS).
>   - To apply policy on UDP/ICMP/DNS traffic, policies must be bound at type UDP_REQUEST, ICMP_REQUEST, and DNS_REQUEST respectively.
>   - While binding, if "type"is not explicitly mentioned or "type"is set to REQUEST, the behavior does not change from earlier builds, that is these policies are applied only to TCP traffic.
>   - The policies bound at UDP_REQUEST do not apply for DNS traffic. For DNS, policies must be explicitly bound to DNS_REQUEST TCP_DNS is similar to other TCP requests.

Para obtener más información sobre las directivas de autorización avanzadas, consulte el artículo https://support.citrix.com/article/CTX232237.

### Para configurar una directiva de autorización mediante la interfaz gráfica de usuario

1. Vaya a **Citrix Gateway > Políticas > Autorización.**
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. En **Acción**, seleccione **Permitir** o **Denegar**.
5. En **Expresión** , haga clic en **Editor** de expresiones .
6. Para empezar a configurar la expresión, haga clic en **Seleccionar** y elija los elementos necesarios.
7. Haga clic en **Listo** cuando la expresión esté completa.
8. Haga clic en **Crear**.

### Para enlazar una directiva de autorización a un usuario mediante la interfaz gráfica de usuario

1. Vaya a **Citrix Gateway > Administración de usuarios.**
2. Haga clic en **Usuarios AAA**.
3. En el panel de detalles, seleccione un usuario y, a continuación, haga clic en **Modificar**.
4. En **Configuración avanzada**, haga clic en **Directivas de autorización**.
5. En **la página Vinculación** de directivas, seleccione una directiva o cree una directiva.

6. En **Prioridad**, defina el número de prioridad.
7. En **Tipo**, seleccione el tipo de solicitud y, a continuación, haga clic en **Aceptar**.

### Para enlazar una directiva de autorización a un grupo mediante la interfaz gráfica de usuario

1. Vaya a **Citrix Gateway > Administración de usuarios**.
2. Haga clic en **Grupos AAA**.
3. En el panel de detalles, seleccione un grupo y, a continuación, haga clic en **Modificar**.
4. En **Configuración avanzada**, haga clic en **Directivas de autorización**.
5. En **la página Vinculación** de directivas, seleccione una directiva o cree una directiva.
6. En **Prioridad**, defina el número de prioridad.
7. En **Tipo**, seleccione el tipo de solicitud y, a continuación, haga clic en **Aceptar**.

## Configuración de la autorización global predeterminada

March 27, 2024

Para definir los recursos a los que tienen acceso los usuarios en la red interna, puede configurar la autorización global predeterminada. La autorización global se configura permitiendo o denegando el acceso a los recursos de red de forma global en la red interna.

Cualquier acción de autorización global que cree se aplica a todos los usuarios que aún no tengan una directiva de autorización asociada a ellos, ya sea directamente o a través de un grupo. Una directiva de autorización de usuarios o grupos siempre anula la acción de autorización global. Si la acción de autorización predeterminada se establece en Denegar, debe aplicar directivas de autorización para todos los usuarios o grupos para que esos usuarios o grupos puedan acceder a los recursos de red. Este requisito ayuda a mejorar la seguridad.

Para establecer la autorización global predeterminada:

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Seguridad, junto a Acción de autorización predeterminada, seleccione Permitir o Denegar y, a continuación, haga clic en Aceptar.

## Inhabilitar la autenticación

March 27, 2024

Si la implementación no requiere autenticación, puede inhabilitarla. Puede inhabilitar la autenticación para cada servidor virtual que no requiera autenticación.

Importante: Citrix recomienda inhabilitar la autenticación con precaución. Si no utiliza un servidor de autenticación externo, cree usuarios y grupos locales para permitir que NetScaler Gateway autentique a los usuarios. Al inhabilitar la autenticación, se detiene el uso de funciones de autenticación, autorización y contabilidad que controlan y supervisan las conexiones a NetScaler Gateway. Cuando los usuarios escriban una dirección web para conectarse a NetScaler Gateway, la página de inicio de sesión no aparece.

### Para inhabilitar la autenticación

1. En la utilidad de configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, en Abrir .
3. En la ficha Autenticación, en Autenticación de usuario, haga clic para desactivar Habilitar autenticación

## Configurar la autenticación para horas específicas

March 27, 2024

Puede configurar una directiva de autenticación para que los usuarios tengan acceso a la red interna en momentos específicos, por ejemplo, durante el horario laboral normal. Cuando los usuarios intentan iniciar sesión en otro momento, se deniega el inicio de sesión.

Para restringir el momento en que los usuarios inician sesión en NetScaler Gateway, cree una expresión dentro de la directiva de autenticación y, a continuación, enlaza a un servidor virtual o de forma global.

### Para configurar la autenticación por hora, fecha o día de la semana

1. En la utilidad de configuración, en la pestaña Configuración, expanda Citrix Gateway > Directivas > Autenticación .

2. En Autenticación, seleccione el tipo de autenticación.
3. En el panel de detalles, haga clic en la ficha Directivas, seleccione una directiva de autenticación y, a continuación, haga clic en Abrir.
4. En el cuadro de diálogo Configurar directiva de autenticación, en Expresión, junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione Fecha/hora.
6. En Qualifier, selecciona una de las siguientes opciones:

   - TIME para configurar el momento en que los usuarios no pueden iniciar sesión.
   - DATE para configurar la fecha en que los usuarios no pueden iniciar sesión.
   - DAYOFWEEK para configurar el día en que los usuarios no pueden iniciar sesión.

   Ejemplo: TIME: 2020-10-12-02:30:00GMT DATE: 2020-10-12 DAYOFWEEK: Lunes
7. En Operador, seleccione el valor.
8. En Valor, haga clic en el calendario junto al cuadro de texto y, a continuación, seleccione el día, la fecha u hora.
9. Haga clic en Aceptar dos veces, en Cerrar y haga clic en Aceptar.

## Cómo funcionan las directivas de autenticación

January 26, 2024

Cuando los usuarios inician sesión en NetScaler Gateway, se autentican según una directiva creada por el usuario. La directiva define el tipo de autenticación. Una única directiva de autenticación se puede utilizar para necesidades de autenticación sencillas y suele estar vinculada a nivel global. También puede utilizar el tipo de autenticación predeterminado, que es local. Si configura la autenticación local, también debe configurar usuarios y grupos en NetScaler Gateway.

Puede configurar varias directivas de autenticación y vincularlas para crear un procedimiento de autenticación detallado y servidores virtuales. Por ejemplo, puede configurar la autenticación en cascada y en dos fases mediante la configuración de varias directivas. También puede establecer la prioridad de las directivas de autenticación para determinar qué servidores y el orden en que NetScaler Gateway comprueba las credenciales de usuario. Una directiva de autenticación incluye una expresión y una acción. Por ejemplo, si establece la expresión en True value, cuando los usuarios inician sesión, la acción evalúa el inicio de sesión del usuario como true y, a continuación, los usuarios tienen acceso a los recursos de red.

Después de crear una directiva de autenticación, la vincula a nivel global o a servidores virtuales. Al enlazar al menos una directiva de autenticación a un servidor virtual, las directivas de autenticación vinculadas al nivel global no se utilizan cuando los usuarios inician sesión en el servidor virtual, a menos que el tipo de autenticación global tenga una prioridad superior a la directiva vinculada al servidor virtual.

Cuando un usuario inicia sesión en NetScaler Gateway, la autenticación se evalúa en el siguiente orden:

- Se comprueba si hay directivas de autenticación vinculadas en el servidor virtual.
- Si las directivas de autenticación no están vinculadas al servidor virtual, NetScaler Gateway comprueba si hay directivas de autenticación globales.
- Si una directiva de autenticación no está vinculada a un servidor virtual ni de forma global, el usuario se autentica mediante el tipo de autenticación predeterminado.

Si configura directivas de autenticación LDAP y RADIUS y quiere enlazar las directivas de forma global para la autenticación de dos factores, puede seleccionar la directiva en la utilidad de configuración y, a continuación, seleccionar si la directiva es el tipo de autenticación principal o secundaria. También puede configurar una directiva de extracción de grupos.

## Configurar perfiles de autenticación

March 27, 2024

Puede crear un perfil de autenticación mediante el asistente de NetScaler Gateway o la utilidad de configuración. El perfil contiene toda la configuración de la directiva de autenticación. El perfil se configura al crear la directiva de autenticación.

Con el asistente de NetScaler Gateway, puede utilizar el tipo de autenticación elegido para configurar la autenticación. Si quiere configurar directivas de autenticación adicionales después de ejecutar el asistente, puede utilizar la utilidad de configuración. Para obtener más información sobre el asistente de NetScaler Gateway, consulte Configuración de los ajustes mediante el Asistente de NetScaler Gateway.

### Para crear una directiva de autenticación mediante la utilidad de configuración

1. En la utilidad de configuración, en la pestaña Configuración, expanda Citrix Gateway > Directivas > Autenticación .
2. En el panel de navegación, en Autenticación, seleccione un tipo de autenticación.
3. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .

4. Si utiliza un tipo de autenticación externa, junto a Servidor, haga clic en Nuevo.
5. En el cuadro de diálogo Crear servidor de autenticación, configure la configuración del tipo de autenticación, haga clic en Crear y, a continuación, haga clic en Cerrar.
6. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione Valor verdadero, haga clic en Agregar expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.
   Nota: Al seleccionar un tipo de autenticación y guardar el perfil de autenticación, no se puede cambiar el tipo de autenticación. Para utilizar un tipo de autenticación diferente, debe crear una nueva directiva.

### Para modificar una directiva de autenticación mediante la utilidad de configuración

Puede modificar las directivas y los perfiles de autenticación configurados, como la dirección IP del servidor de autenticación o la expresión.

1. En la utilidad de configuración, en la pestaña Configuración, expanda Citrix Gateway > Directivas > Autenticación .
2. En el panel de navegación, en Autenticación, seleccione un tipo de autenticación.
3. En el panel de detalles, en la ficha Servidores, seleccione un servidor y, a continuación, haga clic en Abrir.

### Para quitar una directiva de autenticación

Si ha cambiado o quitado un servidor de autenticación de la red, quite la directiva de autenticación correspondiente de NetScaler Gateway.

1. En la utilidad de configuración, en la pestaña Configuración, expanda Citrix Gateway > Directivas > Autenticación .
2. En el panel de navegación, en Autenticación, seleccione un tipo de autenticación.
3. En el panel de detalles, en la ficha Directivas, seleccione una directiva y, a continuación, haga clic en Quitar.

## Binding Authentication Policies

March 27, 2024

Después de configurar las directivas de autenticación, la vincula de forma global o a un servidor virtual. Puede usar cualquiera de las dos utilidades de configuración para vincular una directiva de autenticación.

Para vincular una directiva de autenticación de forma global mediante la utilidad de configuración:

1. En la utilidad de configuración, en la pestaña Configuración, expanda Citrix Gateway > Directivas > Autenticación .
2. Haga clic en un tipo de autenticación.
3. En el panel de detalles, en la ficha Directivas, haga clic en un servidor y, a continuación, en Acción, haga clic en Enlaces globales.
4. En la ficha Principal o Secundaria, en Detalles, haga clic en Insertar directiva.
5. En Nombre de directiva, seleccione la directiva y, a continuación, haga clic en Aceptar.

   **Nota:** Al seleccionar la directiva, NetScaler Gateway establece la expresión en True value automáticamente.

Para desvincular una directiva de autenticación global mediante la utilidad de configuración:

1. En la utilidad de configuración, en la pestaña Configuración, expanda Citrix Gateway > Directivas > Autenticación .
2. En la pestaña Políticas , en Acción , haga clic en Enlaces globales .
3. En el cuadro de diálogo Vincular o desvincular políticas de autenticación a políticas globales, en la pestaña Principal o Secundaria, en Nombre de la directiva, seleccione la política, haga clic en Desvincular directiva y, a continuación, haga clic en Aceptar.

## Definir prioridades para directivas de autenticación

March 27, 2024

De forma predeterminada, las directivas de autenticación se validan primero con respecto a las directivas vinculadas al servidor virtual y, a continuación, con las directivas vinculadas globalmente. Si vincula una directiva de autenticación de forma global y quiere que la directiva global tenga prioridad sobre una directiva vinculada a un servidor virtual, puede cambiar el número de prioridad de la directiva. Los números de prioridad empiezan en cero. Un número de prioridad inferior otorga mayor prioridad a la directiva de autenticación.

Por ejemplo, si la directiva global tiene un número de prioridad de uno y el servidor virtual tiene una prioridad de dos, la directiva de autenticación global se aplica primero.

### Para establecer o cambiar la prioridad de las directivas de autenticación global

1. En la utilidad de configuración, en la pestaña Configuración, expanda Citrix Gateway > Directivas > Autenticación .

2. En la pestaña Políticas , en Acción , haga clic en Enlaces globales .
3. En el cuadro de diálogo Vincular o desvincular directivas globales de autenticación, en la ficha Principal o Secundaria, en Prioridad, escriba el número y, a continuación, haga clic en Aceptar.

### Para cambiar la prioridad de una directiva de autenticación vinculada a un servidor virtual

También puede modificar una directiva de autenticación vinculada a un servidor virtual.

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. Seleccione un servidor virtual y, a continuación, haga clic en Abrir.
3. Haga clic en la ficha Autenticación y seleccione Primaria o Secundaria.
4. Seleccione la directiva y, en Prioridad, escriba el número de la prioridad y, a continuación, haga clic en Aceptar.

## Configurar usuarios locales

March 27, 2024

Puede crear cuentas de usuario localmente en NetScaler Gateway para complementar a los usuarios de los servidores de autenticación. Por ejemplo, puede que quiera crear cuentas de usuario locales para usuarios temporales, como consultores o visitantes, sin crear una entrada para esos usuarios en el servidor de autenticación.

Si utiliza la autenticación local, cree usuarios y, a continuación, agréguelos a los grupos que cree en NetScaler Gateway. Tras configurar usuarios y grupos, puede aplicar directivas de autorización y sesión, crear marcadores, especificar aplicaciones y especificar la dirección IP de los recursos compartidos de archivos y los servidores a los que los usuarios tienen acceso.

### Para crear usuarios locales

1. En la utilidad de configuración, haga clic en la ficha Configuración y, en el panel de navegación, expanda **Citrix Gateway > Administración de usuarios** y, a continuación, haga clic en **Usuarios AAA**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En Nombre de usuario, escriba el nombre de usuario.

4. Si utiliza la autenticación local, desactive **Autenticación externa**.
   **Nota**: Seleccione **Autenticación externa** para que los usuarios se autentiquen en un servidor de autenticación externo, como LDAP o RADIUS. Desactive la casilla de verificación para que NetScaler Gateway se autentique en la base de datos de usuarios local.
5. En Contraseña y Confirmar contraseña, escriba la contraseña del usuario, haga clic en **Crear y,** a continuación, en **Cerrar** .

### Para cambiar la contraseña de un usuario

Tras crear un usuario local, puede cambiar la contraseña del usuario o configurar la cuenta de usuario para que se autentique en un servidor de autenticación externo.

1. En la utilidad de configuración, haga clic en la ficha Configuración y, en el panel de navegación, expanda **Citrix Gateway > Administración de usuarios** y, a continuación, haga clic en **Usuarios AAA**.
2. En el panel de detalles, seleccione un usuario y, a continuación, haga clic en **Abrir** .
3. En Contraseña y Confirmar contraseña, escriba la nueva contraseña del usuario y, a continuación, haga clic **en**Aceptar .

### Para cambiar el método de autenticación de un usuario

Si tiene usuarios configurados para la autenticación local, puede cambiar la autenticación por un servidor de autenticación externo. Para ello, habilite la autenticación externa.

1. En la utilidad de configuración, haga clic en la ficha Configuración y, en el panel de navegación, expanda **Citrix Gateway > Administración de usuarios** y, a continuación, haga clic en **Usuarios AAA**.
2. En el panel de detalles, seleccione un usuario y, a continuación, haga clic en **Abrir** .
3. Seleccione **Autenticación externa y,** a continuación, haga clic **en**Aceptar .

### Para quitar un usuario

También puede quitar un usuario de NetScaler Gateway.

1. En la utilidad de configuración, haga clic en la ficha Configuración y, en el panel de navegación, expanda **Citrix Gateway > Administración de usuarios** y, a continuación, haga clic en **Usuarios AAA**.
2. En el panel de detalles, seleccione un usuario y, a continuación, haga clic en **Quitar**.

Al quitar un usuario de NetScaler Gateway, todas las directivas asociadas también se quitan del perfil de usuario.

# Configurar grupos

March 27, 2024

Puede tener grupos en NetScaler Gateway que sean grupos locales y que puedan autenticar a los usuarios con autenticación local. Si utiliza servidores externos para la autenticación, los grupos de NetScaler Gateway se configuran para que coincidan con los grupos configurados en los servidores de autenticación de la red interna. Cuando un usuario inicia sesión y se autentica, si el nombre de un grupo coincide con un grupo de un servidor de autenticación, el usuario hereda la configuración del grupo en NetScaler Gateway.

Una vez configurados los grupos, puede aplicar directivas de autorización y sesión, crear marcadores, especificar aplicaciones y especificar la dirección IP de los recursos compartidos de archivos y los servidores a los que el usuario tiene acceso.

Si utiliza la autenticación local, cree usuarios y agréguelos a grupos configurados en NetScaler Gateway. A continuación, los usuarios heredan la configuración de ese grupo.

**Importante**: Si los usuarios son miembros de un grupo de Active Directory, el nombre del grupo de NetScaler Gateway debe ser el mismo que el del grupo de Active Directory.

### Para crear un grupo

1. En la utilidad de configuración, haga clic en la pestaña Configuración y, en el panel de navegación, expanda **Citrix Gateway > Administración de usuarios** y, a continuación, haga clic en **Grupos AAA** .
2. En el panel de detalles, haga clic en **Agregar**.
3. En Nombre del grupo, escriba un nombre para el grupo, haga clic en **Crear y,** a continuación, en **Cerrar**.

### Para eliminar un grupo

También puede eliminar grupos de usuarios de NetScaler Gateway.

1. En la utilidad de configuración, haga clic en la pestaña Configuración y, en el panel de navegación, expanda **Citrix Gateway > Administración de usuarios y,** a continuación, haga clic en **Grupos AAA** .
2. En el panel de detalles, seleccione el grupo y, a continuación, haga clic en **Eliminar**.

## Agregar usuarios a grupos

January 26, 2024

Puede agregar usuarios a un grupo durante la creación del grupo o posteriormente. Puede agregar usuarios a varios grupos para que los usuarios puedan heredar las directivas y la configuración vinculadas a esos grupos.

Para agregar usuarios a grupos:

1. En la utilidad de configuración, haga clic en la pestaña Configuración y, en el panel de navegación, expanda **Citrix Gateway > Administración de usuarios y,** a continuación, haga clic en **Grupos AAA** .
2. En el panel de detalles, seleccione un grupo y, a continuación, haga clic en **Abrir**.
3. En la pestaña Usuarios, en Usuarios disponibles, seleccione los usuarios, haga clic en **Agregar**y**,** a continuación, en Aceptar .

## Configurar directivas con grupos

January 26, 2024

Después de configurar los grupos, puede usar el cuadro de diálogo Grupo para aplicar directivas y configuraciones que especifiquen el acceso de los usuarios. Si utiliza la autenticación local, crea usuarios y los agrega a grupos configurados en NetScaler Gateway. A continuación, los usuarios heredan la configuración de ese grupo.

Puede configurar las siguientes directivas o ajustes para un grupo de usuarios en el cuadro de diálogo Grupo :

- Usuarios
- Directivas de autorización
- Directivas de auditoría
- Directivas de sesión
- Directivas de tráfico
- Marcadores
- Aplicaciones de intranet
- Direcciones IP de intranet

En la configuración, es posible que haya usuarios que pertenezcan a más de un grupo. Además, cada grupo puede tener una o más directivas de sesión vinculada, con parámetros diferentes configurados.

Los usuarios que pertenecen a más de un grupo heredan las directivas de sesión asignadas a todos los grupos a los que pertenece el usuario. Para asegurarse de que la evaluación de directivas de sesión tiene prioridad sobre la otra, debe establecer la prioridad de la directiva de sesión.

Por ejemplo, tiene grupo1 enlazado con una directiva de sesión configurada con la página principal www.homepage1.com. Group2 está vinculado a una directiva de sesión configurada con la página principal www.homepage2.com. Cuando estas directivas están enlazadas a grupos respectivos sin un número de prioridad o con el mismo número de prioridad, la página principal que aparece a los usuarios que pertenecen a ambos grupos depende de la directiva que se procese primero. Al establecer un número de prioridad inferior, que otorga mayor prioridad, para la directiva de sesión con la página principal www.homepage1.com, puede asegurarse de que los usuarios que pertenecen a ambos grupos reciban la página principal www.homepage1.com.

Si las directivas de sesión no tienen asignado un número de prioridad o tienen el mismo número de prioridad, la prioridad se evalúa en el siguiente orden:

- Usuario
- Grupo
- Servidor virtual
- Global

Si las directivas están vinculadas al mismo nivel, sin número de prioridad o si las directivas tienen el mismo número de prioridad, el orden de evaluación es según el orden de vinculación de directivas. Las directivas vinculadas primero a un nivel tienen prioridad sobre las directivas vinculadas posteriormente.

Si tenemos un usuario vinculado a varios grupos con cada grupo enlazado a IIP, el usuario puede obtener IP libre de cualquiera de los grupos enlazados.

## Configurar la autenticación LDAP

January 26, 2024

Puede configurar NetScaler Gateway para autenticar el acceso de los usuarios con uno o varios servidores LDAP.

La autorización LDAP requiere nombres de grupo idénticos en Active Directory, en el servidor LDAP y en Citrix Gateway. Los caracteres y la caja también deben coincidir.

De forma predeterminada, la autenticación LDAP es segura mediante la Secure Sockets Layer (SSL) o la Transport Layer Security (TLS). Existen dos tipos de conexiones LDAP seguras. Con un tipo, el servidor LDAP acepta las conexiones SSL o TLS en un puerto independiente del puerto que utiliza el

servidor LDAP para aceptar conexiones LDAP claras. Una vez que los usuarios establecen las conexiones SSL o TLS, el tráfico LDAP se puede enviar a través de la conexión.

Los números de puerto de las conexiones LDAP son:

- 389 para conexiones LDAP no seguras
- 636 para conexiones LDAP seguras
- 3268 para conexiones LDAP no seguras de Microsoft
- 3269 para conexiones LDAP seguras de Microsoft

El segundo tipo de conexiones LDAP seguras usa el comando StartTLS y usa el número de puerto 389. Si configura los números de puerto 389 o 3268 en NetScaler Gateway, el servidor intenta usar StartTLS para establecer la conexión. Si utiliza cualquier otro número de puerto, el servidor intenta establecer conexiones mediante SSL o TLS. Si el servidor no puede utilizar StartTLS, SSL o TLS, la conexión falla.

Si especifica el directorio raíz del servidor LDAP, Citrix Gateway busca el atributo de usuario en todos los subdirectorios. En directorios grandes, este enfoque puede afectar al rendimiento. Por este motivo, Citrix recomienda utilizar una unidad organizativa (OU) específica.

La tabla siguiente contiene ejemplos de campos de atributos de usuario para servidores LDAP:

| Servidor LDAP | atributo de usuario | Sensible a may |
|---|---|---|
| Servidor Microsoft Active Directory | sAMAccountName | No |
| Directorio electrónico de Novell | ou | Sí |
| Servidor IBM Directory | uid | Sí |
| Lotus Domino | CN | Sí |
| Directorio Sun ONE (anteriormente iPlanet) | uid o cn | Sí |

Esta tabla contiene ejemplos del DN base:

| Servidor LDAP | DN base |
|---|---|
| Servidor Microsoft Active Directory | DC=citrix, DC = local |
| Directorio electrónico de Novell | ou=users, ou=dev |
| Servidor IBM Directory | cn=usuarios |
| Lotus Domino | OU=ciudad, O=Citrix, C=EE. UU. |

| Servidor LDAP | DN base |
| --- | --- |
| Directorio Sun ONE (anteriormente iPlanet) | ou=Personas, dc=citrix, dc=com |

La tabla siguiente contiene ejemplos de DN de enlace:

| Servidor LDAP | Vincular DN |
| --- | --- |
| Servidor Microsoft Active Directory | CN=Administrador, CN=Usuarios, DC=citrix, DC=local |
| Directorio electrónico de Novell | cn=admin, o=citrix |
| Servidor IBM Directory | LDAP_dn |
| Lotus Domino | CN=Notes Administrator, O=Citrix, C=US |
| Directorio Sun ONE (anteriormente iPlanet) | uid=admin, ou=Administradores, ou=topologyManagement, o=netscaperoot |

**Nota**: Para obtener más información sobre la configuración del servidor LDAP, consulte Determinación de atributos en el directorio LDAP.

## Para configurar la autenticación LDAP mediante la utilidad de configuración

January 26, 2024

1. Vaya a **Citrix Gateway** > **Directivas** > **Autenticación/autorización** > **Autenticación** .
2. Haga clic en **LDAP**.
3. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
4. En **Nombre**, escriba un nombre para la directiva.
5. Junto a **Servidor** , haz clic en **Nuevo** .
6. En **Nombre**, escriba el nombre del servidor.
7. En **Servidor**, en **Dirección IP y puerto**, escriba la dirección IP y el número de puerto del servidor LDAP.
8. En **Tipo**, seleccione **AD** para Active Directory o **NDS** para Novell Directory Services.

9. En **Configuración de conexión**, complete lo siguiente:

   a) En **DN base (ubicación de los usuarios)**, escriba el DN base en el que se encuentran los usuarios.

   El DN base normalmente se deriva del DN de Bind eliminando el nombre de usuario y especificando el grupo en el que se encuentran los usuarios. Algunos ejemplos de sintaxis para el DN base son:

   ```
   ou=users,dc=ace,dc=com
   cn=Users,dc=ace,dc=com
   <!--NeedCopy-->
   ```

   b) En **Administrator Vincular DN**, escriba el DN de enlace de administrador para las consultas al directorio LDAP. Algunos ejemplos de sintaxis de bind DN son:

   ```
   domain/user name
   ou=administrator,dc=ace,dc=com
   user@domain.name (for Active Directory)
   cn=Administrator,cn=Users,dc=ace,dc=com
   <!--NeedCopy-->
   ```

   Para Active Directory, se requiere el nombre del grupo especificado como cn=groupname. El nombre del grupo definido en NetScaler Gateway y el nombre del grupo en el servidor LDAP deben ser idénticos.

   Para otros directorios LDAP, el nombre del grupo no es obligatorio o, si es necesario, se especifica como ou=groupname.

   NetScaler Gateway se vincula al servidor LDAP mediante las credenciales de administrador y, a continuación, busca al usuario. Tras localizar al usuario, NetScaler Gateway desvincula las credenciales de administrador y vuelve a enlazar con las credenciales de usuario.

   c) En **Contraseña de administrador y Confirmar contraseña**de administrador, escriba la contraseña de administrador del servidor LDAP.

10. Para recuperar automáticamente la configuración adicional de LDAP, haga clic en **Recuperar atributos**.

    Al hacer clic en **Recuperar atributos**, los campos de Otros ajustes se rellenan automáticamente. Si no quieres hacerlo, continúa con los pasos 12 y 13. De lo contrario, vaya al paso 14.

11. En **Otras configuraciones** , en Atributo de nombre de inicio de sesión del servidor, escriba el atributo con el que Citrix Gateway debe buscar los nombres de inicio de sesión de los usuarios para el servidor LDAP que está configurando. El valor predeterminado es `samAccountName`.

12. En **Atributo de grupo**, deje el memberOf predeterminado para Active Directory o cambie el atributo por el atributo del tipo de servidor LDAP que está usando. Este atributo permite a

NetScaler Gateway obtener los grupos asociados a un usuario durante la autorización.

13. En Tipo **de seguridad**, seleccione el tipo de seguridad y, a continuación, haga clic en **Crear**.
14. Para permitir a los usuarios cambiar su contraseña LDAP, seleccione **Permitir cambio de contraseña**.

    **Nota:**

    - Si selecciona **TEXTO SIN FORMATO** como tipo de seguridad, no se admite la posibilidad de que los usuarios cambien sus contraseñas.
    - Si selecciona **PLAINTTEXT** o **TLS por motivos** de seguridad, utilice el número de puerto 389. Si selecciona **SSL**, utilice el número de puerto 636.

## Determine los atributos de su directorio LDAP

March 27, 2024

Si necesita ayuda para determinar los atributos de su directorio LDAP para poder configurar los ajustes de autenticación en NetScaler Gateway, puede buscarlos fácilmente con el explorador LDAP gratuito de Softerra.

Puede descargar el explorador LDAP desde el sitio web de Softerra LDAP Administrator. Después de instalar el explorador, defina los siguientes atributos:

- El nombre de host o la dirección IP del servidor LDAP.
- El puerto del servidor LDAP. El valor por defecto es 389.
- El campo DN base, que puede dejar en blanco. La información proporcionada por el explorador LDAP puede ayudarle a determinar el DN base que debe configurar esta opción en NetScaler Gateway.
- La comprobación Enlace anónimo determina si el servidor LDAP requiere credenciales de usuario para conectarse a él. Si el servidor LDAP requiere credenciales, deje la casilla de verificación desactivada.

Después de completar la configuración, el explorador LDAP muestra el nombre del perfil en el panel izquierdo y se conecta al servidor LDAP.

## Configurar la extracción de grupos LDAP

January 26, 2024

Si utiliza la autenticación de dos factores, los grupos extraídos de las fuentes de autenticación principal y secundaria se concatenan. Las directivas de autorización se pueden aplicar al grupo que se extrae del servidor de autenticación principal o secundario.

Los nombres de grupo obtenidos del servidor LDAP se comparan con los nombres de grupo creados localmente en NetScaler Gateway. Si los nombres de los dos grupos coinciden, las propiedades del grupo local se aplican al grupo obtenido de los servidores LDAP.

Si los usuarios pertenecen a más de un grupo LDAP, NetScaler Gateway extrae información de usuarios de todos los grupos a los que pertenecen los usuarios. Si un usuario es miembro de dos grupos en NetScaler Gateway y cada grupo tiene una directiva de sesión vinculada, el usuario hereda las directivas de sesión de ambos grupos. Para asegurarse de que los usuarios reciben la directiva de sesión correcta, establezca la prioridad de la directiva de sesión.

Para obtener más información sobre los atributos de pertenencia a grupos LDAP que funcionan y no funcionan con la autorización de Citrix Gateway, consulte lo siguiente:

- Cómo funciona la extracción de grupos LDAP directamente desde el objeto de usuario
- Cómo funciona indirectamente la extracción de grupos LDAP desde el objeto de grupo

## Cómo funciona la extracción de grupos LDAP directamente desde el objeto de usuario

January 26, 2024

Los servidores LDAP que evalúan la pertenencia a grupos a partir de objetos de grupo funcionan con la autorización de Citrix Gateway.

Algunos servidores LDAP permiten que los objetos de usuario contengan información sobre los grupos a los que pertenecen los objetos, como Active Directory (mediante el atributo memberOf) o IBM eDirectory (mediante el atributo groupMembership). La pertenencia al grupo de un usuario puede ser atributos del objeto de usuario, como IBM Directory Server (mediante IBM-AllGroups) o el servidor de directorios Sun ONE (mediante NSRole). Ambos tipos de servidores LDAP funcionan con la extracción de grupos de Citrix Gateway.

Por ejemplo, en IBM Directory Server, todas las pertenencias a grupos, incluidos los grupos estáticos, dinámicos y anidados, se pueden devolver mediante el uso del atributo IBM-AllGroups. En Sun ONE, todos los roles, incluidos los administrados, filtrados y anidados, se calculan mediante el uso del atributo nsRole.

## Cómo funciona indirectamente la extracción de grupos LDAP desde el objeto de grupo

January 26, 2024

Los servidores LDAP que evalúan la pertenencia a grupos a partir de objetos de grupo de forma indirecta no funcionarán con la autorización de Citrix Gateway.

Algunos servidores LDAP, como Lotus Domino, permiten que los objetos de grupo solo contengan información sobre los usuarios. Estos servidores LDAP no permiten que el objeto de usuario contenga información sobre grupos y, por lo tanto, no funcionarán con la extracción de grupos de Citrix Gateway. Para este tipo de servidor LDAP, las búsquedas de pertenencia a grupos se realizan localizando al usuario en la lista de miembros de grupos.

## Campos de atributo de grupo de autorización LDAP

January 26, 2024

En la tabla siguiente se incluyen ejemplos de campos de atributos de grupo LDAP:

| Servidores LDAP | atributo LDAP |
|---|---|
| Servidor Microsoft Active Directory | Miembro de |
| Directorio electrónico de Novell | Pertenencia a |
| Servidor IBM Directory | IBM - Todos los grupos |
| Directorio Sun ONE (anteriormente iPlanet) | NSrol |

## Para configurar la autorización LDAP

March 27, 2024

Para configurar la autorización LDAP en la directiva de autenticación, defina el nombre del atributo de grupo y el subatributo.

1. En la utilidad de configuración, en la pestaña Configuración, expanda Citrix Gateway > Directivas > Autenticación .

2. En Autenticación, haga clic en un tipo de autenticación.
3. En el panel de detalles, haga clic en Agregar.
4. En Nombre, escriba un nombre para la directiva.
5. Junto a Servidor , haz clic en Nuevo .
6. En Nombre, escriba el nombre del servidor.
7. En Servidor, escriba la dirección IP y el puerto del servidor LDAP.
8. En Atributo de grupo, escriba memberOf.
9. En Nombre de subatributo, escriba CN y, a continuación, haga clic en Crear.
10. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione la expresión, haga clic en Agregar expresión, en Crear y, a continuación, en Cerrar.

## Configurar la extracción de grupos anidados LDAP

March 27, 2024

NetScaler Gateway puede consultar grupos LDAP y extraer información de grupos y usuarios de grupos antiguos configurados en el servidor de autenticación. Por ejemplo, creaste grupo1 y dentro de ese grupo creaste grupo2 y grupo3. Si el usuario pertenece al grupo3, NetScaler Gateway extrae información de todos los grupos antiguos anidados (grupo2, grupo1) hasta el nivel especificado.

Puede utilizar una directiva de autenticación para configurar la extracción de grupos anidados de LDAP. Cuando se ejecuta la consulta, NetScaler Gateway busca en los grupos hasta que alcanza el nivel máximo de anidamiento o hasta que busca en todos los grupos disponibles.

### Para configurar la extracción de grupos anidados de LDAP

1. En la utilidad de configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas > Autenticación/autorización > Autenticación > Autenticación** y, a continuación, haga clic en **LDAP**.
2. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Servidor, haga clic en **Nuevo**.
5. En Nombre, escriba el nombre del servidor.
6. Configure los ajustes del servidor LDAP.
7. Expanda **Extracción de grupos anidados**y haga clic en **Habilitar**.
8. En **Nivel máximo de anidamiento**, escriba el número de niveles que comprueba NetScaler Gateway.
9. En **Identificador de nombre de grupo**, escriba el nombre del atributo LDAP que identifica de forma exclusiva un nombre de grupo en el servidor LDAP, como `sAMAccountName`.

10. En **Atributo de búsqueda de grupo**, escriba el nombre del atributo LDAP que se va a obtener en la respuesta de búsqueda para determinar los grupos principales de cualquier grupo. Por ejemplo: `memberOf`.
11. En **Subatributo de búsqueda de grupos**, escriba el nombre del subatributo LDAP que se va a buscar como parte del atributo de búsqueda de grupos para determinar los grupos principales de cualquier grupo. Por ejemplo, escriba CN.
12. En **Filtro de búsqueda de grupo**, escriba la cadena de consulta. Por ejemplo, el filtro puede ser `&(samaccountname=test)(objectClass=\*)`.
13. Haga clic en **Crear**y, a continuación, en **Cerrar**.
14. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione la expresión, haga clic en **Agregar expresión**, en **Crear** y, a continuación, en **Cerrar**.

## Configurar la extracción de grupos LDAP para varios dominios

January 26, 2024

Si tiene varios dominios para la autenticación y utiliza StoreFront o la Interfaz Web, puede configurar NetScaler Gateway para que utilice la extracción de grupos para enviar el nombre de dominio correcto a la interfaz web.

En Active Directory, debe crear un grupo para cada dominio de la red. Después de crear el grupo, agrega usuarios que pertenecen al grupo y al dominio especificado. Una vez configurados los grupos en Active Directory, debe configurar la extracción de grupos LDAP para varios dominios en NetScaler Gateway.

Para configurar Citrix Gateway para la extracción de grupos para varios dominios, debe crear el mismo número de políticas de sesión y autenticación que el número de dominios de la red. Por ejemplo, tiene dos dominios, denominados Sampa y Child. Cada dominio recibe una directiva de sesión y una directiva de autenticación.

Después de crear las directivas, crea grupos en NetScaler Gateway y vincula las directivas de sesión al grupo. A continuación, vincula las directivas de autenticación a un servidor virtual.

Si implementa StoreFront en varios dominios, debe haber una relación de confianza entre los dominios.

Si implementa Citrix Endpoint Management o la interfaz web en varios dominios, no es necesario que los dominios confíen entre sí.

# Crear directivas de sesión para la extracción de grupos

March 27, 2024

El primer paso al crear directivas de sesión para la extracción de grupos consiste en crear dos perfiles de sesión y establecer los siguientes parámetros:

- Habilite el proxy ICA.
- Agregue la dirección web de la interfaz Web.
- Agregue el dominio de Windows.
- Agregue el perfil a una directiva de sesión y defina la expresión en true.

## Para crear los perfiles de sesión para la extracción grupal

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, haga clic en la pestaña Perfiles y, a continuación, en Agregar .
3. En Nombre , escriba un nombre para el perfil. Por ejemplo, escriba Sampa.
4. En la ficha Aplicaciones publicadas, haga lo siguiente:
    a) Junto a Proxy ICA, haga clic en Supedición global y, a continuación, selecciona ACTIVADO.
    b) Junto a Dirección de interfaz web, haga clic en Anular global y, a continuación, escriba la dirección web de la interfaz web.
    c) Junto a Dominio de inicio de sesión único, haga clic enSobrescribir global, escribe el nombre del dominio de Windows y, a continuación, haga clic en Crear.
5. En Nombre, borre el nombre del primer dominio y escriba el nombre del segundo dominio, como Secundario.
6. Junto a Dominio de inicio de sesión único, borre el nombre del primer dominio de Windows y escriba el nombre del segundo dominio, haga clic en Crear y, a continuación, en Cerrar.

Después de crear los perfiles de sesión, crea dos directivas de sesión. Cada directiva de sesión utiliza uno de los perfiles.

## Para crear una directiva de sesión

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. En Solicitar perfil, seleccione el perfil del primer dominio.

5. Junto a Expresiones con nombre, haga clic en General, seleccione Valor verdadero, haga clic en Agregar expresión y, a continuación, en Crear.
6. En Nombre, cambie el nombre por el segundo dominio.
7. En Solicitar perfil, seleccione el perfil del segundo dominio, haga clic en Crear y, a continuación, en Cerrar.

## Crear directivas de autenticación LDAP para varios dominios

March 27, 2024

Después de crear directivas de sesión en NetScaler Gateway, crea directivas de autenticación LDAP casi idénticas. Al configurar la directiva de autenticación, el campo importante es Filtro de búsqueda. En este campo, debe escribir el nombre del grupo que creó en Active Directory.

Cree primero los perfiles de autenticación y, a continuación, cree la directiva de autenticación.

### Para crear perfiles de autenticación para la extracción de varios grupos de dominios

1. En la utilidad de configuración, en la pestaña Configuración, expanda Citrix Gateway > Directivas > Autenticación .
2. En el panel de navegación, haga clic en LDAP.
3. En el panel de detalles, haga clic en la ficha Servidores y, a continuación, haga clic en Agregar.
4. En Nombre, escriba el nombre del primer dominio, como Sampa.
5. Configure los ajustes del servidor LDAP y, a continuación, haga clic en Crear.
6. Repita los pasos 3, 4 y 5 para configurar el perfil de autenticación del segundo dominio y, a continuación, haga clic en Cerrar.

Después de crear y guardar los perfiles, cree las directivas de autenticación.

### Para crear políticas de autenticación para la extracción de varios grupos de dominios

1. En la utilidad de configuración, en la pestaña Configuración, expanda Citrix Gateway > Directivas > Autenticación .
2. En el panel de detalles, haga clic en la ficha Directivas y, a continuación, haga clic en Agregar.
3. En Nombre, escriba el nombre del primer dominio.
4. En Tipo de autenticación, seleccione LDAP.
5. En Servidor, seleccione el perfil de autenticación del primer dominio.
6. Junto a Expresiones con nombre, haga clic en General, seleccione Valor verdadero, haga clic en Agregar expresión y, a continuación, en Crear.

7. En Nombre, escriba el nombre del segundo dominio.
8. En Servidor, seleccione el perfil de autenticación para el segundo dominio, haga clic en Crear y, a continuación, en Cerrar.

## Crear grupos y directivas de enlace para la extracción de grupos LDAP para varios dominios

March 27, 2024

Después de crear directivas de autenticación, crea grupos en NetScaler Gateway. Después de crear los grupos, vincula la directiva de autenticación a un servidor virtual.

### Para crear grupos en NetScaler Gateway

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Citrix Gateway > Administración de usuarios** y, a continuación, haga clic en **Grupos AAA**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En Nombre del grupo, escriba el nombre del primer grupo de Active Directory.
   **Importante**: Al crear grupos en Citrix Gateway para la extracción de grupos de varios dominios, los nombres de los grupos deben ser los mismos que los de los grupos que definió en Active Directory. Los nombres de los grupos también distinguen entre mayúsculas y minúsculas y deben coincidir con las mayúsculas y minúsculas que escribió en Active Directory.
4. En la pestaña Políticas, haga clic en **Sesión y,** a continuación, en **Insertar política** .
5. En Nombre de la política, haga doble clic en la política y, a continuación, haga clic en **Crear** .

### Para enlazar las directivas de autenticación a un servidor virtual

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la pestaña Autenticación, haga clic en **Principal** , en Nombre de la política, haga doble clic en **Insertar política y,** a continuación, seleccione la primera política de autenticación.
4. En Nombre de la directiva, haga clic en **Insertar directiva** , haga doble clic en la segunda directiva de autenticación y, a continuación, haga clic **en**Aceptar .

# Configuración de la autenticación con certificados del cliente

January 26, 2024

Los usuarios que inician sesión en un servidor virtual de NetScaler Gateway también se pueden autenticar en función de los atributos de certificado de cliente presentados en el servidor virtual. La autenticación de certificados de cliente también se puede utilizar con otros tipos de autenticación, como LDAP o RADIUS, para proporcionar autenticación de dos factores.

Para autenticar a los usuarios en función de los atributos del certificado del lado del cliente, la autenticación del cliente debe estar habilitada en el servidor virtual y se debe solicitar el certificado de cliente. Es necesario vincular un certificado raíz al servidor virtual en NetScaler Gateway.

Cuando los usuarios inician sesión en el servidor virtual de NetScaler Gateway, tras la autenticación, la información del nombre de usuario se extrae del campo especificado del certificado. Normalmente, este campo es Sujeto:CN. Si el nombre de usuario se extrae correctamente, se puede autenticar al usuario con éxito. La autenticación falla en los siguientes casos.

- Si el usuario no proporciona un certificado válido durante el enlace de Secure Sockets Layer (SSL).
- La extracción del nombre de usuario falla, la autenticación falla.

Se puede autenticar usuarios basándose en el certificado del cliente, definiendo el tipo de autenticación predeterminado para que use el certificado del cliente. También se puede crear una acción de certificado que defina lo que hay que hacer durante la autenticación basada en un certificado SSL del cliente.

## Para configurar el certificado de cliente como el tipo de autenticación predeterminado mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > NetScaler Gateway y,** a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración de autenticación**, haga clic en **Cambiar la configuración de CERT de autenticación**.
3. Seleccione **ACTIVADO** para habilitar la autenticación de dos factores mediante el certificado según sus necesidades.
4. En **Campo Nombre de usuario**, seleccione el tipo de campo de certificado que contiene los nombres de usuario.
5. En **Campo Nombre de Grupo**, seleccione el tipo de campo de certificado que contiene el nombre del grupo.

6. En **Grupo de autorización predeterminado**, escriba el nombre del grupo predeterminado y, a continuación, haga clic en **Aceptar**.

### Extracción del nombre de usuario del certificado de cliente

Si la autenticación de certificados del cliente está habilitada en NetScaler Gateway, los usuarios se autenticarán basándose en ciertos atributos del certificado del cliente. Una vez que la autenticación se realiza correctamente, el nombre de usuario o el nombre de usuario y grupo del usuario se extraen del certificado. Además, se aplican las directivas especificadas para ese usuario.

## Configuring and Binding a Client Certificate Authentication Policy

March 27, 2024

Puede crear una directiva de autenticación de certificados de cliente y vincularla a un servidor virtual. Puede utilizar la directiva para restringir el acceso a grupos o usuarios específicos. Esta directiva tiene prioridad sobre la directiva global.

Para configurar una directiva de autenticación de certificados de cliente:

1. En la utilidad de configuración, en la pestaña Configuración, expanda **Citrix Gateway > Directivas > Autenticación** .
2. En el panel de navegación, en **Autenticación**, haga clic en **CERT**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En **el campo Nombre**, escriba un nombre para la directiva.
5. Junto a **Servidor** , haz clic en **Nuevo** .
6. En **Nombre**, escriba un nombre para el perfil.
7. Junto a **Dos factores**, selecciona **DESACTIVADO**.
8. En Campo de **nombre de usuario y Campo** de **nombre de grupo** , seleccione los valores y, a continuación, haga clic en **Crear** .

> **Nota**
>
> Si anteriormente configuró los certificados de cliente como el tipo de autenticación predeterminado, use los mismos nombres que usó para la política. Si ha completado los campos Nombre de usuario y Nombre de grupo para el tipo de autenticación predeterminado, utilice los mismos valores para el perfil.

9. En el cuadro de diálogo **Crear directiva de autenticación**, junto a **Expresiones con nombre**, seleccione la expresión, haga clic en **Agregar expresión**, en **Crear** y, a continuación, en **Cerrar**.

Para enlazar una directiva de certificados de cliente a un servidor virtual:

Después de configurar la directiva de autenticación de certificados de cliente, puede vincularla a un servidor virtual.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, en **Abrir** .
3. En el cuadro de diálogo Configurar el **servidor virtual Citrix Gateway** , haga clic en la pestaña **Autenticación** .
4. Haga clic en **Primaria** o **Secundaria**
5. En **Detalles**, haga clic en **Insertar directiva**.
6. En **Nombre de la política** , seleccione la política y, a continuación, haga clic **en**Aceptar .

Para configurar un servidor virtual de modo que solicite el certificado de cliente:

Si quiere utilizar un certificado de cliente para la autenticación, debe configurar el servidor virtual para que se soliciten certificados de cliente durante el enlace SSL.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, haga clic en un **servidor virtual** y, a continuación, haga clic en **Abrir**.
3. En la ficha **Certificados**, haga clic en **Parámetro SSL**.
4. En **Otros**, haga clic en **Autenticación de cliente**
5. En **Certificado de cliente**, seleccione **Opcional** u **Obligatorio** y haga clic en Aceptar dos veces. Seleccione **Opcional** si quiere permitir otros tipos de autenticación en el mismo servidor virtual y no requiere el uso de certificados de cliente.

> **Nota**
>
> - Para obtener más información sobre la URL de devolución de llamada, consulte Importar un NetScaler Gateway.
> - Para obtener más información sobre los certificados, consulte Instalar, vincular y actualizar certificados.

## Configurar la autenticación de certificados de cliente de dos factores

January 26, 2024

Puede configurar un certificado de cliente para autenticar primero a los usuarios y, a continuación, solicitar a los usuarios que inicien sesión con un tipo de autenticación secundario, como LDAP o RADIUS. En este caso, el certificado de cliente autentica primero a los usuarios. A continuación, aparece una página de inicio de sesión en la que pueden introducir su nombre de usuario y contraseña. Cuando se completa el enlace de Secure Sockets Layer (SSL), la secuencia de inicio de sesión puede tomar una de las dos rutas siguientes:

- Ni el nombre de usuario ni el grupo se extraen del certificado. La página de inicio de sesión aparece al usuario con un mensaje para que introduzca credenciales de inicio de sesión válidas. NetScaler Gateway autentica las credenciales de usuario como en el caso de la autenticación de contraseña normal.
- El nombre de usuario y el nombre del grupo se extraen del certificado de cliente. Si solo se extrae el nombre de usuario, aparece una página de inicio de sesión para el usuario en el que está presente el nombre de inicio de sesión y el usuario no puede modificar el nombre. Solo el campo de contraseña está en blanco.

La información de grupo que NetScaler Gateway extrae durante la segunda ronda de autenticación se anexa a la información del grupo, si la hay, que NetScaler Gateway extrajo del certificado.

## Configurar la autenticación con tarjeta inteligente

March 27, 2024

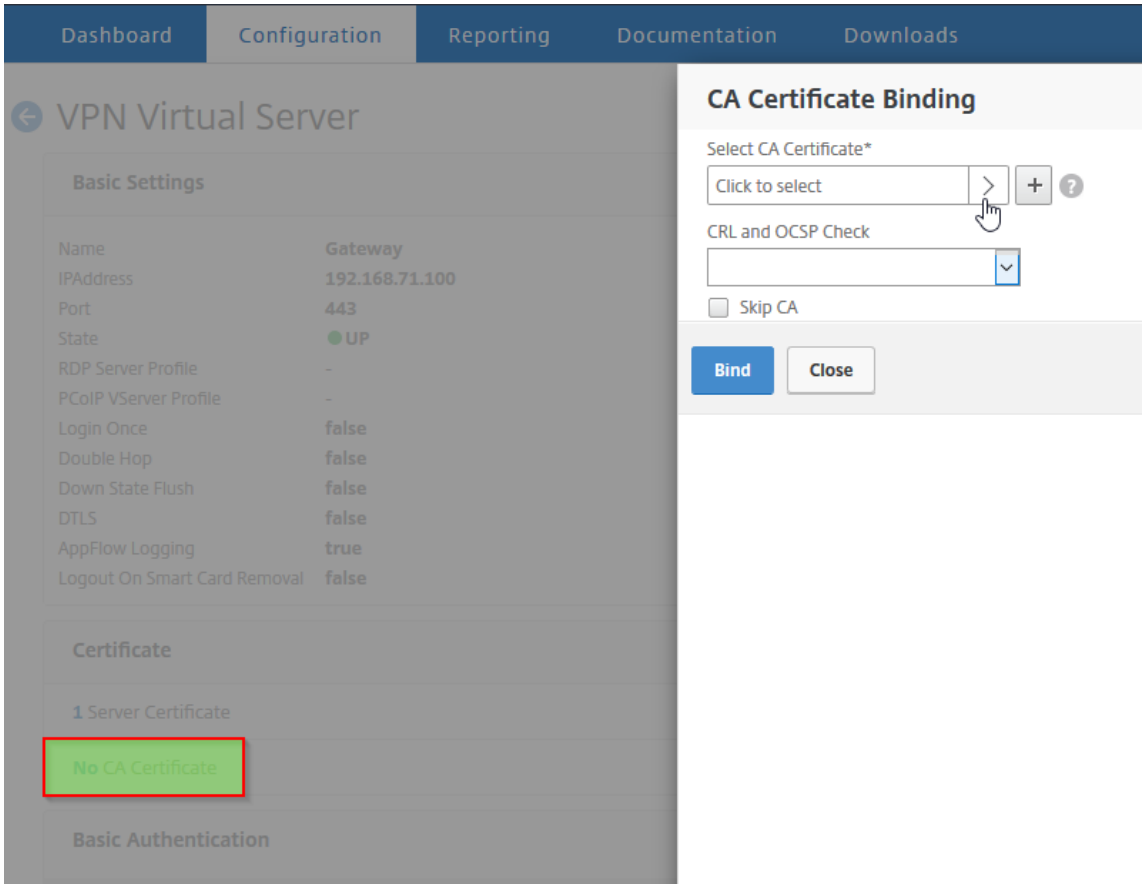
Puede configurar NetScaler Gateway para que utilice una tarjeta inteligente criptográfica para autenticar a los usuarios.

Para configurar una tarjeta inteligente para que funcione con Citrix Gateway, debe hacer lo siguiente:

- Cree una directiva de autenticación de certificados. Para obtener más información, consulte Configuración de la autenticación de certificados de cliente.
- Enlazar la directiva de autenticación a un servidor virtual.
- Agregue el certificado raíz de la entidad emisora de certificados (CA) que emite los certificados de cliente a NetScaler Gateway. Para obtener más información, consulte Para instalar un certificado raíz en Citrix Gateway.

  **Importante**: Al agregar el certificado raíz al servidor virtual para la autenticación con tarjeta inteligente, debe seleccionar el certificado en el cuadro desplegable **Seleccionar certificado de CA** , como se muestra en la siguiente figura.
  Figura 1. Agregar un certificado raíz para la autenticación con tarjeta inteligente




Después de crear el certificado de cliente, puede escribir el certificado, conocido como flash, en la tarjeta inteligente. Cuando complete este paso, podrá probar la tarjeta inteligente.

Si configura la interfaz web para la autenticación de acceso directo con tarjeta inteligente, si se da alguna de las siguientes condiciones, se produce un error en el inicio de sesión único en la interfaz web:

- Si configuras el dominio de la pestaña Aplicaciones publicadas como mydomain.com en lugar de mydomain.
- Si no establece el nombre de dominio en la pestaña Aplicaciones publicadas y si ejecuta el comando wi-sso-split-upn estableciendo el valor en 1. En este caso, UserPrincipalName contiene el nombre de dominio “midominio.com. “

Puede utilizar la autenticación con tarjeta inteligente para optimizar el proceso de inicio de sesión de sus usuarios y, al mismo tiempo, mejorar la seguridad del acceso de los usuarios a su infraestructura. El acceso a la red corporativa interna está protegido por la autenticación de dos fases basada en un certificado con infraestructura de clave pública. Las claves privadas están protegidas por controles de hardware y nunca salen de la tarjeta inteligente. Los usuarios obtienen la comodidad de acceder a sus escritorios y aplicaciones desde una serie de dispositivos de la empresa con sus tarjetas inteligentes y sus PIN.

Puede usar tarjetas inteligentes para la autenticación de usuarios a través de StoreFront en los escritorios y las aplicaciones que proporcionan Citrix Virtual Apps and Desktops. Los usuarios de tarjetas inteligentes que inician sesión en StoreFront también pueden acceder a las aplicaciones proporcionadas por Citrix Endpoint Management. Sin embargo, los usuarios deben autenticarse de nuevo para acceder a las aplicaciones web de Endpoint Management que utilizan la autenticación de certificados de cliente.

Para obtener más información, consulte Configurar la autenticación con tarjeta inteligente en la documentación de StoreFront.

### Configuración de la autenticación de tarjeta inteligente con conexiones ICA seguras

Los usuarios que inician sesión y establecen una conexión ICA segura mediante una tarjeta inteligente con inicio de sesión único configurada en Citrix Gateway pueden recibir solicitudes para su número de identificación personal (PIN) en dos momentos diferentes: al iniciar sesión y al intentar iniciar un recurso publicado. Esta situación se produce si el explorador web y Citrix Receiver utilizan el mismo servidor virtual que está configurado para usar certificados de cliente. Citrix Receiver no comparte un proceso ni una conexión SSL (Secure Sockets Layer) con el explorador web. Por lo tanto, cuando la conexión ICA completa el protocolo de enlace SSL con NetScaler Gateway, se requiere el certificado de cliente por segunda vez.

Para evitar que los usuarios reciban la segunda solicitud de PIN, tiene que cambiar dos configuraciones:

- La autenticación de cliente en el servidor virtual de VPN debe estar inhabilitada.
- La renegociación SSL debe estar habilitada.

Después de configurar el servidor virtual, vincule uno o varios servidores STA al servidor virtual, como se describe en Configuración de los parámetros de NetScaler Gateway en la Interfaz Web 5.3.

Es posible que también quieras probar la autenticación con tarjeta inteligente.

Para inhabilitar la autenticación de cliente:

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. Seleccione el servidor virtual correspondiente en el panel de detalles principal y, a continuación, haga clic en Modificar.
3. En el panel Opciones avanzadas, haga clic en Parámetros SSL.
4. Desactive la casilla Autenticación de cliente.
5. Haga clic en Listo.

Para habilitar la renegociación SSL:

1. Con la utilidad de configuración, en la ficha Configuración, vaya a Administración del tráfico y, a continuación, haga clic en SSL.
2. En el panel principal, haga clic en Cambiar la configuración avanzada de SSL.
3. En el menú Denegar renegociación de SSL, seleccione NO.

Para probar la autenticación con tarjeta inteligente:

1. Conecte la tarjeta inteligente al dispositivo del usuario.
2. Abra el explorador web e inicie sesión en NetScaler Gateway.

## Configurar la autenticación RADIUS

January 26, 2024

Puede configurar NetScaler Gateway para autenticar el acceso de los usuarios con uno o varios servidores RADIUS. Si utiliza los productos RSA SecurID, SafeWord o Protiva de Gemalto, cada uno de ellos se configura mediante un servidor RADIUS.

Es posible que su configuración requiera el uso de una dirección IP del servidor de acceso a la red (IP del NAS) o un identificador del servidor de acceso a la red (ID del NAS). Al configurar NetScaler Gateway para utilizar un servidor de autenticación RADIUS, siga las siguientes pautas:

- Si habilita el uso de la IP del NAS, el dispositivo envía su dirección IP configurada al servidor RADIUS, en lugar de la dirección IP de origen utilizada para establecer la conexión RADIUS.
- Si configura el ID del NAS, el dispositivo envía el identificador al servidor RADIUS. Si no configura el ID del NAS, el dispositivo envía su nombre de host al servidor RADIUS.
- Al habilitar la IP del NAS, el dispositivo ignora cualquier ID del NAS configurado mediante la IP del NAS para comunicarse con el servidor RADIUS.

### Configuración de Gemalto Protiva

Protiva es una sólida plataforma de autenticación desarrollada por Gemalto para utilizar los puntos fuertes de la autenticación con tarjeta inteligente de Gemalto. Con Protiva, los usuarios inician sesión con un nombre de usuario, una contraseña y una contraseña de un solo uso que genera el dispositivo Protiva. Al igual que RSA SecurID, la solicitud de autenticación se envía al servidor de autenticación de Protiva y el servidor valida o rechaza la contraseña. Para configurar Gemalto Protiva para que funcione con Citrix Gateway, siga las siguientes pautas:

- Instale el servidor Protiva.

- Instale el software Protiva SAS Agent, que amplía el servidor de autenticación de Internet (IAS), en un servidor RADIUS de Microsoft IAS. Asegúrese de anotar la dirección IP y el número de puerto del servidor IAS.
- Configure un perfil de autenticación RADIUS en NetScaler Gateway e introduzca la configuración del servidor Protiva.

### Configuración de SafeWord

La línea de productos SafeWord proporciona autenticación segura mediante un código de acceso basado en tokens. Una vez que el usuario introduce el código, SafeWord invalida inmediatamente el código de acceso y no se puede volver a utilizar. Al configurar el servidor SafeWord, necesita la siguiente información:

- Dirección IP de Citrix Gateway. Debe ser la misma dirección IP que configuró en la configuración del cliente del servidor RADIUS. NetScaler Gateway utiliza la dirección IP interna para comunicarse con el servidor RADIUS. Al configurar el secreto compartido, utilice la dirección IP interna. Si configura dos dispositivos para obtener alta disponibilidad, utilice la dirección IP interna virtual.
- Un secreto compartido.
- La dirección IP y el puerto del servidor SafeWord. El número de puerto predeterminado es 1812.

## Para configurar la autenticación RADIUS

March 27, 2024

1. En la utilidad de configuración, en la pestaña Configuración, expanda Citrix Gateway > Directivas > Autenticación .
2. Haga clic en RADIUS y, a continuación, en el panel de detalles, en la ficha Directivas, haga clic en Agregar.
3. En el cuadro de diálogo Crear política de autenticación , en Nombre, escriba un nombre para la política.
4. En Nombre, escriba un nombre para la directiva.
5. Junto a Servidor , haz clic en Nuevo .
6. En el cuadro de diálogo Crear directiva de autenticación, en Nombre, escriba un nombre para el servidor.
7. En Servidor, en Dirección IP, escriba la dirección IP del servidor RADIUS.
8. En Puerto, escriba el puerto. El valor por defecto es 1812.
9. En Detalles, en Clave secreta y Confirmar clave secreta, escriba el secreto del servidor RADIUS.

10. En ID de NAS, escriba el número de identificador y, a continuación, haga clic en Crear.
11. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione la expresión, haga clic en Agregar expresión, en Crear y, a continuación, en Cerrar.

## Seleccionar protocolos de autenticación RADIUS

January 26, 2024

NetScaler Gateway admite implementaciones de RADIUS configuradas para utilizar varios protocolos de autenticación de usuarios, entre ellos:

- Protocolo de autenticación de contraseñas (PAP)
- Protocolo de autenticación por desafío mutuo (CHAP)
- Protocolo de autenticación Challenge Handshake de Microsoft (MS-CHAP versión 1 y versión 2)

Si la implementación de NetScaler Gateway está configurada para utilizar la autenticación RADIUS y el servidor RADIUS está configurado para usar PAP, puede reforzar la autenticación de usuarios asignando un secreto compartido fuerte al servidor RADIUS. Los secretos compartidos de RADIUS fuertes consisten en secuencias aleatorias de letras mayúsculas y minúsculas, números y signos de puntuación y tienen al menos 22 caracteres. Si es posible, utilice un programa de generación de caracteres aleatorios para determinar los secretos compartidos RADIUS.

Para proteger aún más el tráfico RADIUS, asigne un secreto compartido diferente a cada dispositivo o servidor virtual de NetScaler Gateway. Al definir clientes en el servidor RADIUS, también puede asignar un secreto compartido independiente a cada cliente. Si lo hace, debe configurar por separado cada directiva de NetScaler Gateway que utiliza la autenticación RADIUS.

Al crear una directiva RADIUS, configura secretos compartidos en NetScaler Gateway como parte de la directiva.

## Configurar la extracción de direcciones IP

March 27, 2024

Puede configurar NetScaler Gateway para extraer la dirección IP de un servidor RADIUS. Cuando un usuario se autentica en el servidor RADIUS, el servidor devuelve una dirección IP enmarcada (también denominada dirección IP enmarcada del atributo 8 de RADIUS en las solicitudes de acceso) que se asigna al usuario. Los siguientes son componentes para la extracción de direcciones IP:

- Permite que un servidor RADIUS remoto proporcione una dirección IP de la red interna a un usuario que ha iniciado sesión en NetScaler Gateway.
- Permite la configuración de cualquier atributo RADIUS mediante el tipo **ipaddress**, incluidos los atributos codificados por proveedor.

Al configurar el servidor RADIUS para la extracción de direcciones IP, configure el identificador de proveedor y el tipo de atributo. El ID de proveedor y los atributos se utilizan para establecer la asociación entre el cliente RADIUS y el servidor RADIUS.

- El identificador de proveedor (ID) permite al servidor RADIUS asignar una dirección IP al cliente desde un grupo de direcciones IP configuradas en el servidor RADIUS. El ID de proveedor es el atributo de la respuesta RADIUS que proporciona la dirección IP de la red interna. Un valor cero indica que el atributo no está codificado por el proveedor
- El tipo de atributo es el atributo de dirección IP remota de una respuesta RADIUS. El valor mínimo es 1 y el valor máximo es 255.

Una configuración común consiste en extraer la **dirección IP enmarcada**del atributo RADIUS. El ID de proveedor está establecido en 0 o no se ha especificado. El tipo de atributo se establece en 8.

Para configurar la extracción de direcciones IP de un servidor RADIUS:

1. En la utilidad de configuración, en la pestaña Configuración, expanda Citrix Gateway > Directivas > Autenticación .
2. Haga clic en RADIUS y, a continuación, en el panel de detalles, en la pestaña Políticas, seleccione una política RADIUS y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar la política de autenticación , junto a Servidor, haga clic en Modificar .
4. En Detalles, en Identificador de proveedor de grupo, escriba el valor.
5. En Tipo de atributo de grupo, escriba el valor y, a continuación, haga clic dos veces en Aceptar.

## Configurar la extracción de grupos RADIUS

January 26, 2024

Puede configurar la autorización RADIUS mediante un método denominado extracción de grupos. La configuración de la extracción de grupos permite administrar usuarios en el servidor RADIUS en lugar de agregarlos a NetScaler Gateway.

Para configurar la autorización RADIUS, utilice una directiva de autenticación y configure el identificador (ID) del proveedor del grupo, el tipo de atributo de grupo, el prefijo de grupo y un separador de grupos. Al configurar la directiva, agrega una expresión y, a continuación, la vincula de forma global o a un servidor virtual.

### Configuración de RADIUS en Windows Server 2003

Si utiliza Microsoft Internet Authentication Service (IAS) para la autorización RADIUS en Windows Server 2003, durante la configuración de NetScaler Gateway, debe proporcionar la siguiente información:

- El identificador de proveedor es el código específico del proveedor que ha introducido en IAS.
- Type es el número de atributo asignado por el proveedor.
- Nombre de atributo es el tipo de nombre de atributo definido en IAS. El nombre predeterminado es CTXSUserGroups=

Si IAS no está instalado en el servidor RADIUS, puede instalarlo desde Agregar o quitar programas del Panel de control. Para obtener más información, consulte la Ayuda en línea de Windows.

Para configurar IAS, utilice Microsoft Management Console (MMC) e instale el complemento para IAS. Siga el asistente y asegúrese de seleccionar la siguiente configuración:

- Seleccione equipo local.
- Seleccione Directivas de acceso remoto y cree una directiva personalizada.
- Seleccione Grupos de Windows para la directiva.
- Seleccione uno de los protocolos siguientes:
  - Protocolo de autenticación por desafío mutuo de Microsoft versión 2 (MS-CHAP v2)
  - Protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP)
  - Protocolo de autenticación por desafío mutuo (CHAP)
  - Autenticación sin cifrar (PAP, SPAP)
- Seleccione el atributo específico del proveedor.

  El atributo específico del proveedor debe hacer coincidir los usuarios definidos en el grupo del servidor con los usuarios de NetScaler Gateway. Para cumplir con este requisito, debe enviar los atributos específicos del proveedor a NetScaler Gateway. Asegúrese de seleccionar RADIUS=STANDARD.
- El valor predeterminado de RADIUS es 0. Utilice este número para el código de proveedor.
- El número de atributo asignado por el proveedor es 0.

  Número asignado al atributo Grupo de usuarios. El atributo está en formato de cadena.
- Seleccione Cadena para el formato de atributo.

  El valor Attribute requiere el nombre del atributo y los grupos.

  Para Access Gateway, el valor del atributo es CTXSUserGroups=groupname. Si se definen dos grupos, como ventas y finanzas, el valor del atributo es CTXSUserGroups=Sales; finance. Separe cada grupo con un punto y coma.

- Elimine todas las demás entradas del cuadro de diálogo Modificar perfil de marcado, dejando la que dice Específico del proveedor.

Después de configurar la directiva de acceso remoto en IAS, debe configurar la autenticación y autorización RADIUS en NetScaler Gateway.

Al configurar la autenticación RADIUS, utilice la configuración configurada en el servidor IAS.

### Configuración de RADIUS para la autenticación en Windows Server 2008

En Windows Server 2008, se configura la autenticación y autorización RADIUS mediante el Servidor de directivas de red (NPS), que sustituye al Servicio de autenticación de Internet (IAS). Es posible utilizar el Administrador de servidores y agregar NPS como una función para instalar NPS.

Al instalar NPS, seleccione el Servicio de directivas de red. Después de la instalación, puede configurar la configuración de RADIUS para su red iniciando el NPS desde Servicios administrativos en el menú Inicio. Al abrir el NPS, agrega NetScaler Gateway como cliente RADIUS y, a continuación, configura los grupos de servidores.

Al configurar el cliente RADIUS, asegúrese de seleccionar la siguiente configuración:

- Para el nombre del proveedor, seleccione RADIUS Standard.
- Anote el secreto compartido porque tendrá que configurar el mismo secreto compartido en NetScaler Gateway.

Para los grupos RADIUS, necesita la dirección IP o el nombre de host del servidor RADIUS. No cambie la configuración predeterminada.

Después de configurar el cliente y los grupos RADIUS, configure la configuración en las dos directivas siguientes:

- Directivas de solicitud de conexión en las que se configuran los valores de la conexión de NetScaler Gateway, incluidos el tipo de servidor de red, las condiciones de la directiva de red y la configuración de la directiva.
- Directivas de red en las que se configura la autenticación del Protocolo de autenticación extensible (EAP) y los atributos específicos del proveedor.

Al configurar la directiva de solicitud de conexión, seleccione Sin especificar para el tipo de servidor de red. A continuación, configure su condición seleccionando Tipo de puerto NAS como condición y Virtual (VPN) como valor.

Al configurar una directiva de red, debe configurar los siguientes ajustes:

- Seleccione Servidor de acceso remoto (acceso telefónico VPN) como tipo de servidor de acceso a la red.

- Seleccione Autenticación cifrada (CHAP) y Autenticación sin cifrar (PAP y SPAP) para el EAP.
- Seleccione Estándar RADIUS para el atributo específico del proveedor.

  El número de atributo predeterminado es 26. Este atributo se utiliza para la autorización RADIUS.

  NetScaler Gateway necesita el atributo específico del proveedor para que los usuarios definidos en el grupo del servidor coincidan con los de NetScaler Gateway. Para ello, se envían los atributos específicos del proveedor a NetScaler Gateway.
- Seleccione Cadena para el formato de atributo.

  El valor Attribute requiere el nombre del atributo y los grupos.

  Para NetScaler Gateway, el valor del atributo es CTXSUserGroups= groupname. Si se definen dos grupos, como ventas y finanzas, el valor del atributo es CTXSUserGroups=Sales; finance. Separe cada grupo con un punto y coma.
- El separador es el que utilizó en el NPS para separar grupos, como un punto y coma, dos puntos, un espacio o un punto.

Cuando haya terminado de configurar la directiva de acceso remoto en IAS, podrá configurar la autenticación y autorización RADIUS en NetScaler Gateway.

## Para configurar la autorización RADIUS

March 27, 2024

1. En la utilidad de configuración, en la pestaña Configuración, expanda Citrix Gateway > Directivas > Autenticación .
2. Haga clic en RADIUS.
3. En la ficha Directivas, haga clic en Agregar.
4. En Nombre, escriba un nombre para la directiva.
5. Debajo del servidor* haga clic en +
6. En Nombre, escriba el nombre del servidor RADIUS.
7. En Servidor, escriba la dirección IP y el puerto del servidor RADIUS.
8. En Detalles, introduzca los valores de Identificador de proveedor de grupo y Tipo de atributo de grupo.
9. En Codificación de contraseña, seleccione el protocolo de autenticación y, a continuación, haga clic en Crear.
10. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione la expresión, haga clic en Agregar expresión, en Crear y, a continuación, en Cerrar.

# Configurar cuentas de usuario RADIUS

March 27, 2024

NetScaler Gateway puede enviar mensajes de inicio y detención de la sesión de usuario al servidor de cuentas RADIUS. Los mensajes, que se envían para cada sesión de usuario, incluyen un subconjunto de los atributos definidos en RFC2866. En la tabla 1 se enumeran los atributos admitidos y los tipos de mensajes de cuentas RADIUS (RAD_START y RAD_STOP) en los que se envían. En la tabla 2 se enumeran los valores predefinidos que se pueden asignar al atributo Acct-Terminate-Cause y los eventos de Citrix Gateway correspondientes.

Tabla 1. Atributos RADIUS compatibles

| Atributo | Significado | RAD_START | RAD_STOP |
|---|---|---|---|
| User-Name | Nombre del usuario asociado a la sesión. | X | X |
| Session-Id | El identificador de sesión de Citrix ADC. | X | X |
| Acct-Session-Time | Duración de la sesión segundos. | | X |
| Acct-Terminate-Cause | Motivo de la cancelación de la cuenta (consulte la tabla siguiente). | | X |

Tabla 2. Causas de la terminación

| Método de cierre de sesión de Citrix ADC | Causa de terminación RADIUS |
|---|---|
| LOGOUT_SESSN_TIMEDOUT | RAD_TERM_SESSION_TIMEOUT |
| LOGOUT_SESSN_INITIATEDBYUSER | RAD_TERM_USER_REQUEST |
| LOGOUT_SESSN_KILLEDBYADMIN | RAD_TERM_ADMIN_RESET |
| LOGOUT_SESSN_TLOGIN | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_MAXLICRCHD | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_CLISECCHK_FAILED | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_PREAUTH_CHANGED | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_COOKIE_MISMATCH | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSS_DHT | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSS_2FACTOR_FAIL | RAD_TERM_NAS_REQUEST |

| Método de cierre de sesión de Citrix ADC | Causa de terminación RADIUS |
|---|---|
| LOGOUT_SESSN_ICALIC | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_INTERNALERR | RAD_TERM_NAS_ERROR |
| Otros | RAD_TERM_NAS_ERROR |

La configuración de la contabilidad de usuario RADIUS requiere la creación de un par de directivas. La primera directiva es una directiva de autenticación RADIUS que designa un servidor RADIUS al que enviar mensajes de cuentas. La segunda es una directiva de sesión que utiliza la directiva de contabilidad RADIUS como acción.

Para configurar la contabilidad de usuarios RADIUS, debe:

1. Cree una directiva RADIUS para definir el servidor de cuentas RADIUS. El servidor de cuentas puede ser el mismo servidor que utiliza para la autenticación RADIUS.
2. Cree una directiva de sesión, mediante la directiva RADIUS como acción que especifica el servidor de cuentas de usuarios RADIUS.
3. Enlazar la directiva de sesión de forma global, de modo que se aplique a todo el tráfico o a un servidor virtual NetScaler Gateway, de modo que solo se aplique al tráfico que fluye a través de ese servidor virtual.

### Para crear una directiva RADIUS

1. En la utilidad de configuración, en el panel de navegación, expanda el nodo NetScaler Gateway y, a continuación, Directivas.
2. Expanda Autenticación y seleccione RADI
3. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
4. Introduzca un nombre para la directiva.
5. Seleccione un servidor en el menú Servidor o haga clic en el icono + y siga las instrucciones para agregar un servidor RADIUS.
6. En el panel Expresión, en el menú Expresiones de directivas guardadas, seleccione ns_true.
7. Haga clic en Crear.

### Para crear una directiva de sesión

Después de configurar una directiva RADIUS que especifica el servidor de cuentas RADIUS, cree una directiva de sesión que aplique este servidor de cuentas en una acción, como se indica a continuación:

1. En la utilidad de configuración, en el panel de navegación, expanda el nodo NetScaler Gateway y, a continuación, Directivas.
2. Selecciona Sesión .
3. En el panel de detalles principal, selecciona Agregar.
4. Introduzca un nombre para la directiva.
5. En el menú Acción, haga clic en el icono + para añadir una acción de sesión.
6. Escriba un nombre para la acción de sesión.
7. Haga clic en la ficha Experiencia del cliente.
8. En el menú Directiva contable, seleccione la directiva RADIUS que creó anteriormente.
9. Haga clic en Crear.
10. En el panel Expresión, en el menú Expresiones de directivas guardadas, seleccione ns_true.
11. Haga clic en Crear.

### Para enlazar la directiva de sesión de forma global

1. En la utilidad de configuración, en el panel de navegación, expanda el nodo NetScaler Gateway y, a continuación, Directivas.
2. Selecciona Sesión .
3. En el menú Acción del panel de detalles principal, seleccione Enlaces globales.
4. Haga clic en Bind.
5. En el panel Directivas, seleccione la directiva de sesión que creó anteriormente y, a continuación, haga clic en Insertar.
6. En la lista Directivas, haga clic en la entrada Prioridad de la directiva de sesión e introduzca un valor comprendido entre 0 y 64000.
7. Haga clic en Aceptar.

### Para enlazar la directiva de sesión a un servidor virtual de NetScaler Gateway

1. En la utilidad de configuración, en el panel de navegación, expanda el nodo NetScaler Gateway y, a continuación, seleccione Servidores virtuales.
2. En el panel de detalles principal, seleccione un servidor virtual y, a continuación, haga clic en Modificar.
3. En el panel Directivas, haga clic en el icono + para seleccionar una directiva.
4. En el menú Elegir directiva, seleccione Sesión y asegúrese de que la opción Solicitud esté seleccionada en el menú Elegir tipo.
5. Haga clic en Continuar.
6. Haga clic en Bind.
7. En el panel Directivas, seleccione la directiva de sesión que creó anteriormente y, a continuación, haga clic en Insertar.

8. Haga clic en Aceptar.

## Configurar la autenticación SAML

January 26, 2024

El lenguaje de marcado de aserciones de seguridad (SAML) es un estándar basado en XML para intercambiar autenticación y autorización entre proveedores de identidad (IdP) y proveedores de servicios. NetScaler Gateway admite la autenticación SAML.

Al configurar la autenticación SAML, crea la siguiente configuración:

- Nombre del certificado del IdP. Esta es la clave pública que corresponde a la clave privada del IdP.
- URL de redireccionamiento. Esta es la dirección URL del IdP de autenticación. Los usuarios que no están autenticados se redirigen a esta URL.
- Campo de usuario. Puede utilizar este campo para extraer el nombre de usuario si el IdP envía el nombre de usuario en un formato diferente al de la etiqueta NameIdentifier de la etiqueta Subject. Este es un parámetro opcional.
- Nombre del certificado de firma. Es la clave privada del servidor NetScaler Gateway que se utiliza para firmar la solicitud de autenticación al IdP. Si no configura un nombre de certificado, la aserción se envía sin firmar o se rechaza la solicitud de autenticación.
- Nombre del emisor SAML. Este valor se utiliza cuando se envía la solicitud de autenticación. Debe haber un nombre único en el campo emisor para indicar la autoridad desde la que se envía la afirmación. Este campo es opcional.
- Grupo de autenticación predeterminado. Es el grupo del servidor de autenticación desde el que se autentican los usuarios.
- Dos factores. Esta configuración habilita o inhabilita la autenticación de dos factores.
- Rechazar afirmaciones sin firmar. Si se habilita, NetScaler Gateway rechaza la autenticación de usuarios si el nombre del certificado de firma no está configurado.

NetScaler Gateway admite el enlace posterior a HTTP. En este enlace, el remitente responde al usuario con 200 OK que contiene una publicación automática de formulario con la información requerida. En concreto, el formulario predeterminado debe contener dos campos ocultos denominados `SAMLRequest`y `SAMLResponse`en función de si el formulario es una solicitud o una respuesta. El formulario también incluye RelayState, que es un estado o información utilizada por la parte que envía para enviar información arbitraria que no es procesada por la parte que confía. La parte que confía devuelve la información para que, cuando la parte remitente reciba la afirmación junto con RelayState, la parte remitente sepa qué hacer a continuación. Se recomienda cifrar u ofuscar RelayState.

> **Nota**
>
> - Cuando NetScaler Gateway se usa como IdP para Citrix Cloud, no es necesario configurar la regla **RelayState** en NetScaler Gateway.
> - En caso de encadenamiento de IdP, basta con configurar la regla **RelayState** solo en la primera directiva de SAML. En este contexto, el encadenamiento de IdP es un casos en el que una acción de SAML configurada hace referencia a un IdP de servidor virtual de autenticación que contiene otra acción de SAML.

### Configuración de Servicios de federación de Active Directory 2.0

Puede configurar los Servicios de federación de Active Directory (AD FS) 2.0 en cualquier equipo con Windows Server 2008 o Windows Server 2012 que utilice en un rol de servidor federado. Al configurar el servidor AD FS para que funcione con Citrix Gateway, debe configurar los siguientes parámetros mediante el asistente Relying Party Trust en Windows Server 2008 o Windows Server 2012.

Parámetros de Windows Server 2008:

- Confianza del partido. Proporciona la ubicación del archivo de metadatos de NetScaler Gateway `https://vserver.fqdn.com/ns.metadata.xml`, por ejemplo, donde vserver.fqdn.com es el nombre de dominio completo (FQDN) del servidor virtual de NetScaler Gateway. Puede encontrar el FQDN en el certificado de servidor vinculado al servidor virtual.
- Reglas de autorización. Puede permitir o denegar a los usuarios el acceso a la parte que confía.

Parámetros de Windows Server 2012:

- Confianza del partido. Proporciona la ubicación del archivo de metadatos de NetScaler Gateway `https://vserver.fqdn.com/ns.metadata.xml`, por ejemplo, donde vserver.fqdn.com es el nombre de dominio completo (FQDN) del servidor virtual de NetScaler Gateway. Puede encontrar el FQDN en el certificado de servidor vinculado al servidor virtual.
- Perfil AD FS. Seleccione el perfil de AD FS.
- Certificado. NetScaler Gateway no admite el cifrado. No es necesario seleccionar un certificado.
- Habilite la compatibilidad con el protocolo WebSSO SAML 2.0. Esto permite admitir el inicio de sesión único de SAML 2.0. Proporciona la URL del servidor virtual de NetScaler Gateway, como https:netScaler.virtualServerName.com/cgi/samlauth.

  Esta URL es la URL de Assertion Consumer Service del dispositivo NetScaler Gateway. Se trata de un parámetro constante y NetScaler Gateway espera una respuesta SAML en esta URL.
- Identificador de confianza de parte que confía Escriba el nombre NetScaler Gateway. Esta es una URL que identifica a las partes que confían, por ejemplo `https://netscalerGateway.virtualServerName.com/adfs/services/trust`.

- Reglas de autorización. Puede permitir o denegar a los usuarios el acceso a la parte que confía.
- Configurar reglas de notificación. Puede configurar los valores de los atributos LDAP mediante Reglas de transformación de emisión y utilizar la plantilla Enviar atributos LDAP como notificaciones. A continuación, configure los ajustes de LDAP que incluyen:
  - Direcciones de correo
  - sAMAccountName
  - Nombre principal de usuario (UPN)
  - Miembro de
- Firma de certificado. Puede especificar los certificados de verificación de firma seleccionando las propiedades de una parte retransmitiendo y, a continuación, agregando el certificado.

  Si el certificado de firma tiene menos de 2048 bits, aparece un mensaje de advertencia. Puede ignorar la advertencia para continuar. Si está configurando una implementación de prueba, inhabilite la Lista de revocación de certificados (CRL) en la Parte de transmisión. Si no inhabilita la comprobación, AD FS intenta la CRL para validar el certificado.

  Puede inhabilitar la CRL ejecutando el siguiente comando: Set-ADFWrelayingPartyTrust - SigningCertFicateRevocatonCheck None-TargetName NetScaler

Después de configurar la configuración, compruebe los datos de la parte que confía antes de completar el Asistente para confianza de la parte de retransmisión. Comprueba el certificado del servidor virtual de NetScaler Gateway con la URL del endpoint, como `https://vserver.fqdn.com/cgi/samlauth`.

Una vez que haya terminado de configurar los ajustes en el Asistente para confianza de la parte de retransmisión, seleccione la confianza configurada y, a continuación, modifique las propiedades. Debe hacer lo siguiente:

- Establezca el algoritmo hash seguro en SHA-1.

  Nota: Citrix solo admite SHA-1.
- Elimine el certificado de cifrado. Las afirmaciones cifradas no son compatibles.
- Modifique las reglas de notificación, incluidas las siguientes:
  - Seleccionar regla de transformación
  - Agregar regla de notificación
  - Seleccionar plantilla de reglas de notificación: enviar atributos LDAP como notificaciones
  - Dar un nombre
  - Seleccionar almacén de atributos: Active Directory
  - Seleccione el atributo LDAP: <Active Directory parameters>
  - Seleccione Regla de reclamo en marcha fuera como “ID de nombre”

Nota: Las etiquetas XML de nombre de atributo no son compatibles.

- Configure la URL de cierre de sesión para el cierre de sesión único. La regla de notificación es Enviar URL de cierre de sesión. La regla personalizada debe ser la siguiente:

```
pre codeblock => issue(Type = "logoutURL", Value = "https://<adfs
.fqdn.com>/adfs/ls/", Properties["http://schemas.xmlsoap.org/ws
/2005/05/identity/claimproperties/attributename"] = "urn:oasis:
names:tc:SAML:2.0:attrname-format:unspecified"); <!--NeedCopy-->
```

Después de configurar la configuración de AD FS, descargue el certificado de firma de AD FS y, a continuación, cree una clave de certificado en NetScaler Gateway. A continuación, puede configurar la autenticación SAML en NetScaler Gateway mediante el certificado y la clave.

### Configuración de la autenticación de dos factores SAML

Puede configurar la autenticación de dos factores SAML. Al configurar la autenticación SAML con autenticación LDAP, siga las siguientes pautas:

- Si SAML es el tipo de autenticación principal, inhabilite la autenticación en la directiva LDAP y configure la extracción de grupo. A continuación, vincule la directiva LDAP como tipo de autenticación secundaria.
- La autenticación SAML no utiliza una contraseña y solo utiliza el nombre de usuario. Además, la autenticación SAML solo informa a los usuarios cuando la autenticación se realiza correctamente. Si se produce un error en la autenticación SAML, no se notifica a los usuarios. Dado que no se envía una respuesta de error, SAML tiene que ser la última directiva de la cascada o la única directiva.
- Se recomienda configurar nombres de usuario reales en lugar de cadenas opacas.
- SAML no se puede enlazar como tipo de autenticación secundaria.

## Para configurar la autenticación SAML

March 27, 2024

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas\ > Autenticación**.
2. En el panel de navegación, haga clic en SAML.
3. En el panel de detalles, haga clic en Agregar.

4. En el cuadro de diálogo Crear política de autenticación , en Nombre, escriba un nombre para la política.
5. Junto a Servidor , haz clic en Nuevo .
6. En Nombre, escriba un nombre para el perfil del servidor.
7. En Nombre del certificado del IdP, seleccione un certificado o haga clic en Instalar. Este es el certificado instalado en el servidor SAML o IdP.

   Si hace clic en Instalar, agregue el certificado y la clave privada. Para obtener más información, consulte Instalar y administrar certificados.
8. En la URL de redireccionamiento, introduzca la URL del proveedor de identidad (IdP) de autenticación.

   Esta es la dirección URL del inicio de sesión del usuario en el servidor SAML. Este es el servidor al que NetScaler Gateway redirige la solicitud inicial.
9. En Campo de usuario, introduzca el nombre de usuario que quiere extraer.
10. En Nombre del certificado de firma, seleccione la clave privada del certificado que seleccionó en el paso 9.

    Este es el certificado que está enlazado a la dirección IP virtual AAA de Citrix ADC. El nombre del emisor SAML es el nombre de dominio completo (FQDN) en el que los usuarios inician sesión, como lb.example.com o ng.example.com.
11. En Nombre del emisor de SAML, introduzca el FQDN de la dirección IP virtual de Citrix Gateway o de equilibrio de carga a la que el dispositivo envía la solicitud de autenticación inicial (GET).
12. En el grupo de autenticación predeterminado, introduzca el nombre del grupo.
13. Para habilitar la autenticación de dos factores, en Dos factores, haga clic en.
14. Inhabilitar Rechazar aserción sin firmar. Habilite esta configuración solo si el servidor SAML o IdP firma la respuesta SAML.
15. Haga clic en Create y, luego, en Close.
16. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione General, Valor verdadero, haga clic en Agregar expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

## Usar la autenticación SAML para iniciar sesión en NetScaler Gateway

January 26, 2024

Puede usar la autenticación SAML para iniciar sesión en NetScaler Gateway mediante clientes VPN de Citrix y la aplicación Workspace. El complemento admite la autenticación SAML solo a través de directivas SAML avanzadas vinculadas al servidor virtual de autenticación, es decir, la autenticación nfactor.

**Importante**: El complemento no admite la autenticación SAML cuando las políticas SAML están enlazadas directamente al servidor virtual VPN, es decir, la autenticación sin factor.

### Plataformas y aplicaciones compatibles

En la tabla siguiente se enumeran las plataformas y aplicaciones que admiten la autenticación SAML para iniciar sesión en NetScaler Gateway.

| Producto | Versión |
|---|---|
| Citrix Gateway | Versión 12.0, compilación 41.16 y versiones posteriores |
| cliente VPN | Versión 12.1, compilación 49.37 y versiones posteriores. **Plataformas compatibles**: Windows 7, Windows 8, Windows 8.1, Windows 10 |
| Versiones de la aplicación Workspace | Ventanas: 1808; Mac: 1808 |

### Configurar la autenticación SAML mediante directivas SAML avanzadas

Para obtener más información sobre cómo configurar la autenticación SAML mediante directivas SAML avanzadas, consulte NetScaler ADC como proveedor de identidades SAML.

## Mejoras de autenticación para la autenticación SAML

March 27, 2024

Esta función es para aquellos que tienen conocimiento de SAML, y se requiere un conocimiento fundamental de autenticación para usar esta información. El lector debe entender FIPS para usar esta información.

Las siguientes funciones de NetScaler ADC se pueden utilizar con aplicaciones/servidores de terceros compatibles con la especificación SAML 2.0:

- Proveedor de servicios SAML (SP)
- Proveedor de identidad (IdP) SAML

El SP y el IdP permiten un inicio de sesión único (SSO) entre servicios en la nube. La función SAML SP proporciona una forma de abordar las reclamaciones de los usuarios de un IdP. El IdP puede ser un servicio de terceros u otro dispositivo NetScaler ADC. La función de proveedor de identidades SAML se utiliza para confirmar los inicios de sesión de los usuarios y proporcionar notificaciones consumidas por los SP.

Como parte de la compatibilidad con SAML, tanto el IdP como los módulos SP firman digitalmente los datos que se envían a los pares. La firma digital incluye una solicitud de autenticación de SP, aserción del IdP y mensajes de cierre de sesión entre estas dos entidades. La firma digital valida la autenticidad del mensaje.

La implementación actual de SAML SP e IdP realiza el cálculo de la firma en un motor de paquetes. Estos módulos utilizan certificados SSL para firmar los datos. En un NetScaler ADC compatible con FIPS, la clave privada del certificado SSL no está disponible en el motor de paquetes ni en el espacio de usuario, por lo que el módulo SAML de hoy no está preparado para hardware FIPS.

En este documento se describe el mecanismo para descargar los cálculos de firma a la tarjeta FIPS. La verificación de la firma se realiza en el software, ya que la clave pública está disponible.

### Solución

El conjunto de funciones SAML se ha mejorado para utilizar una API SSL para la descarga de firmas. Consulte docs.citrix.com para obtener más información sobre estas subfunciones de SAML afectadas:

1. Enlace posterior a SAML SP: firma de AuthnRequest
2. Enlace posterior a IdP de SAML: firma de aserción/respuesta/ambos
3. Casos de cierre de sesión único de SAML SP: firma de logoutRequest en el modelo iniciado por SP y firma de LogoutResponse en el modelo iniciado por el IdP
4. Enlace de artefactos de SAML SP: firma de la solicitud ArtifactResolve
5. Enlace de redireccionamiento de SAML SP: firma de AuthnRequest
6. Enlace de redireccionamiento de IdP de SAML: firma de respuesta/aserción/ambos
7. Compatibilidad con cifrado SAML SP: descifrado de aserción

### Plataforma

La API solo se puede descargar a una plataforma FIPS.

### Configuración

La configuración de descarga se realiza automáticamente en la plataforma FIPS.

Sin embargo, dado que las claves privadas SSL no están disponibles para el espacio de usuario en el hardware FIPS, hay un ligero cambio de configuración al crear el certificado SSL en hardware FIPS.

Esta es la información de configuración:

- `add ssl fipsKey fips-key`

  Cree una CSR y utilícelo en el servidor de CA para generar un certificado. A continuación, puede copiar ese certificado en /nsconfig/ssl. Supongamos que el archivo es fips3cert.cer.

- `add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key`

  A continuación, especifique este certificado en la acción SAML del módulo SP SAML.

- `set samlAction \<name\> -samlSigningCertName fips-cert`

  Úselo en SAMLIDPProfile para el módulo IdP de SAML

- `set samlidpprofile fipstest –samlIdpCertName fips-cert`

La clave FIPS no está disponible la primera vez. Si no hay ninguna clave FIPS, cree una tal y como se describe en Crear una clave FIPS.

- `create ssl fipskey \<fipsKeyName\> -modulus \<positive\\_integer \> \[-exponent ( 3 | F4 )\]`
- `create certreq \<reqFileName\> -fipskeyName \<string\>`

## Configurar la autenticación TACACS+

January 26, 2024

Puede configurar un servidor TACACS+ para la autenticación. De forma similar a la autenticación RADIUS, TACACS+ utiliza una clave secreta, una dirección IP y el número de puerto. El número de puerto predeterminado es 49.

Para configurar NetScaler Gateway para que utilice un servidor TACACS+, proporcione la dirección IP del servidor y el secreto TACACS+. Debe especificar el puerto solo cuando el número de puerto del servidor en uso es algo distinto del número de puerto predeterminado de 49.

Para configurar la autenticación TACACS+ mediante la interfaz de usuario, lleve a cabo los siguientes pasos.

1. En la utilidad de configuración, en la pestaña Configuración, expanda **Citrix Gateway > Directivas > Autenticación** .
2. Haga clic en **TACACS**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En **el campo Nombre**, escriba un nombre para la directiva.
5. Junto al campo **Servidor**, haga clic en **Agregar** para crear un nuevo servidor TACACS o haga clic en **Modificar** para realizar cambios en un servidor TACACS existente.
6. En **el campo Nombre**, escriba un nombre para el servidor.
7. En **Dirección IP**, escriba la dirección IP.
8. En **Puerto**, utilice el número de puerto predeterminado 49.
9. En el campo **Clave TACACS**, escriba la clave. En el campo **Confirmar clave TACACS**, escriba la misma clave para confirmar.
10. Haga clic en **Más**.
11. En **Autorización**, seleccione **ACTIVADO** y, a continuación, haga clic en **Crear**.
12. En el cuadro de diálogo **Crear directiva TACACS de autenticación**, seleccione la expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

Para configurar la autenticación TACACS+ mediante la interfaz de línea de comandos, escriba el siguiente comando.

```
add authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr
    |*>][-serverPort <port>] [-authTimeout <positive_integer>] {
 -tacacsSecret  }

[-authorization ( ON | OFF )] [-accounting ( ON | OFF )][-
    auditFailedCmds ( ON | OFF )] [-groupAttrName <string>][-
    defaultAuthenticationGroup <string>] [-Attribute1 <string>] [-
    Attribute2 <string>] [-Attribute3 <string>] [-Attribute4 <string>]
[-Attribute5 <string>] [-Attribute6 <string>] [-Attribute7 <string>] [-
    Attribute8 <string>] [-Attribute9 <string>] [-Attribute10 <string>]
[-Attribute11 <string>] [-Attribute12 <string>] [-Attribute13 <string>]
     [-Attribute14 <string>] [-Attribute15 <string>] [-Attribute16 <
    string>]
<!--NeedCopy-->
```

Después de configurar la configuración del servidor TACACS+ en NetScaler Gateway, vincule la directiva para activarla. Puede enlazar la directiva a nivel de servidor global o virtual. Para obtener más información sobre las directivas de autenticación vinculantes, consulte Directivas de autenticación vinculantes.

# El nivel básico de clear config no debería borrar la configuración de TACACS

March 27, 2024

## Información general

Esta mejora se centra en NO BORRAR todas las configuraciones relacionadas con el RBA (acceso basado en funciones) cuando se ejecuta el comando clear config.

El comando clear config actual se ejecuta en uno de los tres niveles:

• Básica

• Extendida

• Completo

Según el nivel elegido, las configuraciones de NetScaler se borran y se restablecen a los valores predeterminados de fábrica.

El comando usado es:

```
clear ns config \[-force\] \<level\>
```

El nuevo comando agrega un mando para permitir/denegar la eliminación de todas las configuraciones relacionadas con RBA.

## Nuevo comando

Se describen las funciones de Clear RBAConfig:

1. Mando SÍ/NO con valor predeterminado: SÍ.

   El administrador decide si quiere conservar la configuración de RBA o no.

2. SOLO se admite el NIVEL BÁSICO de clear config.
3. Las siguientes configuraciones no se han borrado:

   - Agregar/enlazar usuario/grupo del sistema.
   - Agregar directiva cmd.
   - Comandos TACACS. (añada la acción/política del TACACS).
   - Sistema de enlace global

**Nota:**La configuración relacionada con el TACACS (acción/política) se conserva si la política está vinculada al sistema global o si se borra

### Configuración CLI

El comando usado

```
clear config [ – force] <level> [–RBAconfig]
```

De forma predeterminada, se establece en SÍ y borra las configuraciones en función del nivel especificado.

Si —RBAConfig se establece en NO, se conserva la configuración relacionada con el RBA. Se incluye lo siguiente:

- Agregar /bind usuario del sistema /group
- Sistema de enlace global
- comandos relacionados con tacacs (agregar acción/política de tacacs)
- Agregar directiva cmd

## Configurar la autenticación multifactor

January 26, 2024

Puede configurar dos tipos de autenticación multifactor en NetScaler Gateway:

- Autenticación en cascada que establece el nivel de prioridad de autenticación
- Autenticación de dos factores que requiere que los usuarios inicien sesión mediante dos tipos de autenticación

Si tiene varios servidores de autenticación, puede establecer la prioridad de sus directivas de autenticación. Los niveles de prioridad que establezca determinan el orden en que el servidor de autenticación valida las credenciales de los usuarios. Una directiva con un número de prioridad inferior tiene prioridad sobre una directiva con un número mayor.

Puede hacer que los usuarios se autentiquen en dos servidores de autenticación diferentes. Por ejemplo, puede configurar una directiva de autenticación LDAP y una directiva de autenticación RSA. Cuando los usuarios inician sesión, se autentican primero con su nombre de usuario y contraseña. A continuación, se autentican con un número de identificación personal (PIN) y el código del token RSA.

# Configurar la autenticación en cascada

March 27, 2024

La autenticación le permite crear una cascada de varios servidores de autenticación mediante la priorización de directivas. Al configurar una cascada, el sistema atraviesa cada servidor de autenticación, según lo definido por las directivas en cascada, para validar las credenciales de un usuario. Las directivas de autenticación priorizadas se ponen en cascada en orden ascendente y pueden tener valores de prioridad comprendidos entre 1 y 9999. Defina estas prioridades al vincular sus directivas a nivel de servidor global o virtual.

Durante la autenticación, cuando un usuario inicia sesión, primero se comprueba el servidor virtual y, a continuación, se comprueban las directivas de autenticación global. Si un usuario pertenece a una directiva de autenticación tanto del servidor virtual como de forma global, la directiva del servidor virtual se aplica primero y, a continuación, la directiva de autenticación global. Si quiere que los usuarios reciban la directiva de autenticación vinculada globalmente, cambie la prioridad de la directiva. Cuando una directiva de autenticación global tiene un número de prioridad de uno y una directiva de autenticación vinculada a un servidor virtual tiene prioridad número dos, la directiva de autenticación global tiene prioridad. Por ejemplo, puede tener tres directivas de autenticación vinculadas al servidor virtual y establecer la prioridad de cada directiva.

Si un usuario no se autentica con una directiva de la cascada principal o si el usuario logra autenticarse con éxito en una directiva de la cascada principal pero no se autentica con una directiva en la cascada secundaria, el proceso de autenticación se detiene y se redirige al usuario a una página de error.

Nota: Citrix recomienda que cuando vincule varias directivas a un servidor virtual o de forma global, defina prioridades únicas para todas las directivas de autenticación.

## Para establecer la prioridad de las directivas de autenticación global

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas\ > Autenticación**.
2. Seleccione la directiva vinculada globalmente y, a continuación, en Acción, haga clic en Enlaces globales.
3. En el cuadro de diálogo Vincular o desvincular políticas globales de autenticación, en Prioridad, escriba el número y, a continuación, haga clic en Aceptar.

## Para cambiar la prioridad de una directiva de autenticación vinculada a un servidor virtual

También puede modificar una directiva de autenticación vinculada a un servidor virtual.

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en Abrir .
3. Haga clic en la pestaña Autenticación y, a continuación, en Principal o Secundaria.
4. Junto a la política de autenticación, en Prioridad, escriba el número y, a continuación, haga clic en Aceptar.

## Configurar la autenticación de dos factores

March 27, 2024

NetScaler Gateway admite la autenticación de dos factores. Normalmente, al autenticar usuarios, NetScaler Gateway detiene el proceso de autenticación en cuanto autentica correctamente a un usuario mediante cualquiera de los métodos de autenticación configurados. En algunos casos, es posible que necesite autenticar a un usuario en un servidor, pero extraer grupos de otro servidor. Por ejemplo, si la red autentica a los usuarios en un servidor RADIUS, pero también utiliza la autenticación de token de RSA SecurID y los grupos de usuarios se almacenan en ese servidor, es posible que deba autenticar a los usuarios en ese servidor para poder extraer los grupos.

Si los usuarios se autentican mediante dos tipos de autenticación y si uno de ellos es la autenticación de certificados de cliente, puede configurar la directiva de autenticación de certificados como segundo método de autenticación. Por ejemplo, utiliza LDAP como tipo de autenticación principal y el certificado de cliente como autenticación secundaria. Cuando los usuarios inician sesión con su nombre de usuario y contraseña, tienen acceso a los recursos de red.

Al configurar la autenticación de dos factores, selecciona si el tipo de autenticación es el tipo principal o secundario.

### Para configurar la autenticación de dos factores

1. En la utilidad de configuración, en la pestaña Configuración, expanda Citrix Gateway > Directivas > Autenticación .
2. En la ficha Directivas, haga clic en Vinculaciones globales.
3. En el cuadro de diálogo Vincular o desvincular directivas de autenticación a globales, haga clic en Principal.
4. Haga clic en Insertar directiva.
5. En Nombre de directiva, seleccione la directiva de autenticación.
6. Haga clic en Secundaria, repita los pasos 4 y 5 y haga clic en Aceptar.

## Seleccionar el tipo de autenticación para Single Sign-On

March 27, 2024

Si ha configurado el inicio de sesión único y la autenticación de dos factores en NetScaler Gateway, puede seleccionar qué contraseña usar para el inicio de sesión único. Por ejemplo, ha configurado LDAP como tipo de autenticación principal y RADIUS configurado como tipo de autenticación secundaria. Cuando los usuarios acceden a recursos que requieren inicio de sesión único, el nombre de usuario y la contraseña principal se envían de forma predeterminada. Usted establece la contraseña que se debe usar para el inicio de sesión único en las aplicaciones web dentro de un perfil de sesión.

### Para configurar la autenticación para el inicio de sesión único

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, haga clic en la ficha Perfiles y, a continuación, realice una de las siguientes acciones:
    - Para crear un nuevo perfil, haga clic en Agregar.
    - Para modificar un perfil existente, haga clic en Abrir.
3. En la ficha Experiencia del cliente, junto a Índice de credenciales, haga clic en Supedición globaly seleccione Primaria o Secundaria.
4. Si se trata de un perfil nuevo, haga clic en Crear y, a continuación, en Cerrar.
5. Si va a modificar un perfil existente, haga clic en Aceptar.

## Configurar certificados de cliente y autenticación de dos factores LDAP

March 27, 2024

Puede utilizar un certificado de cliente seguro con autenticación y autorización LDAP, por ejemplo, mediante autenticación de tarjeta inteligente con LDAP. El usuario inicie sesión y, a continuación, se extrae el nombre de usuario del certificado de cliente. El certificado de cliente es la forma principal de autenticación y LDAP es el formulario secundario. La autenticación de certificados de cliente debe tener prioridad sobre la directiva de autenticación LDAP. Al establecer la prioridad de las directivas, asigne un número inferior a la directiva de autenticación de certificados de cliente que el número que asigna a la directiva de autenticación LDAP.

Para usar un certificado de cliente, debe tener una entidad de certificación (CA) de empresa, como Servicios de certificados de Windows Server 2008, ejecutándose en el mismo equipo que ejecuta Active Directory. Puede utilizar la entidad emisora de certificados para crear un certificado de cliente.

Para utilizar un certificado de cliente con autenticación y autorización LDAP, debe ser un certificado seguro que utilice la Secure Sockets Layer (SSL). Para utilizar certificados de cliente seguros para LDAP, instale el certificado de cliente en el dispositivo de usuario e instale el certificado raíz correspondiente en NetScaler Gateway.

Antes de configurar un certificado de cliente, haga lo siguiente:

- Cree un servidor virtual.
- Cree una directiva de autenticación LDAP para el servidor LDAP.
- Defina la expresión de la directiva LDAP en Valor verdadero.

### Para configurar la autenticación de certificados de cliente con LDAP

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas\ > Autenticación**.
2. En el panel de navegación, en Autenticación, haga clic en Certificado.
3. En el panel de detalles, haga clic en Agregar.
4. En Nombre, escriba un nombre para la directiva.
5. En Tipo de autenticación, seleccione Certificado.
6. Junto a Servidor , haz clic en Nuevo .
7. En Nombre, escriba un nombre para el servidor y, a continuación, haga clic en Crear.
8. En el cuadro de diálogo Crear servidor de autenticación, en Nombre, escriba el nombre del servidor.
9. Junto a Dos factores, selecciona ON.
10. En el campo Nombre de usuario, seleccione Asunto:CN y, a continuación, haga clic en Crear.
11. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione Valor verdadero, haga clic en Agregar expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

Después de crear la directiva de autenticación de certificados, enlaza la directiva al servidor virtual. Después de vincular la directiva de autenticación de certificados, vincule la directiva de autenticación LDAP al servidor virtual.

**Importante**: Enlazar la directiva de autenticación de certificados al servidor virtual antes de vincular la directiva de autenticación LDAP al servidor virtual.

### Para instalar un certificado raíz en NetScaler Gateway

Después de crear la directiva de autenticación de certificados, descarga e instala un certificado raíz de la CA en formato Base64 y lo guarda en el equipo. A continuación, puede cargar el certificado raíz en NetScaler Gateway.

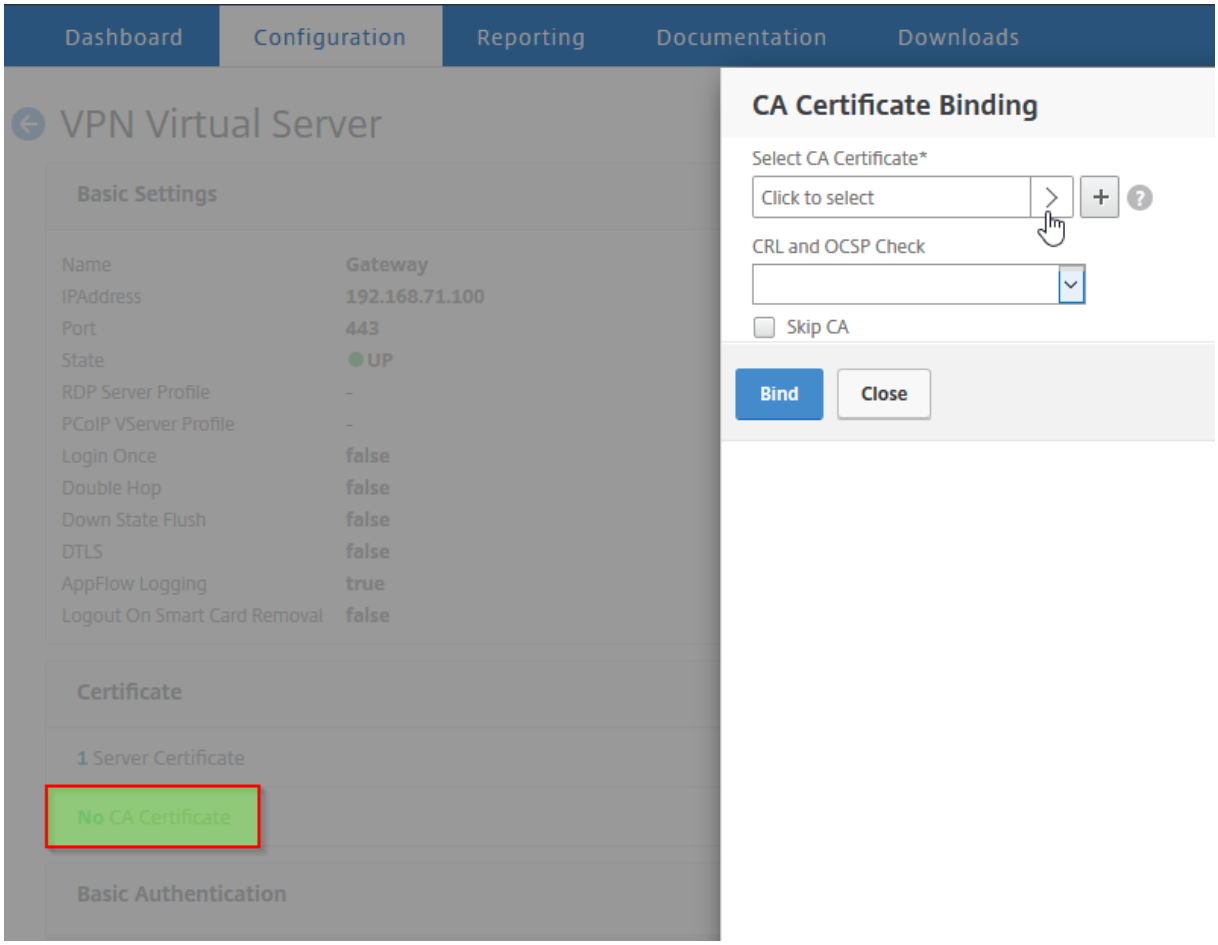
1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificados.
2. En el panel de detalles, haga clic en Instalar.
3. En Certificado: nombre del par de claves, escriba un nombre para el certificado.
4. En Nombre del archivo del certificado, haga clic en Examinar y, en el menú, seleccione Dispositivo o Local.
5. Vaya a el certificado raíz, haga clic en Abrir y, a continuación, haga clic en Instalar.

### Para agregar un certificado raíz a un servidor virtual

Después de instalar el certificado raíz en NetScaler Gateway, agregue el certificado al almacén de certificados del servidor virtual.

**Importante**: Al agregar el certificado raíz al servidor virtual para la autenticación con tarjeta inteligente, debe seleccionar el certificado en el menú **Seleccionar certificado de CA** , como se muestra en la siguiente figura.




1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en Abrir .
3. En la pestaña Certificados, en Disponible, seleccione el certificado, junto a Agregar, en el menú, haga clic como CA y, a continuación, haga clic en Aceptar.
4. Repita el paso 2.
5. En la ficha Certificados, haga clic en Parámetros SSL.
6. En Otros, seleccione Autenticación de cliente.
7. En Otros, junto a Certificado de cliente, seleccione Opcional y, a continuación, haga clic en Aceptar dos veces.
8. Después de configurar el certificado de cliente, pruebe la autenticación iniciando sesión en NetScaler Gateway con el plug-in de NetScaler Gateway. Si tiene más de un certificado instalado, recibirá un mensaje en el que se le pedirá que seleccione el certificado correcto. Después de seleccionar el certificado, aparece la pantalla de inicio de sesión con el nombre de usuario

rellenado con la información obtenida del certificado. Escriba la contraseña y, a continuación, haga clic en Login.

Si no ve el nombre de usuario correcto en el campo Nombre de usuario de la pantalla de inicio de sesión, compruebe las cuentas de usuario y los grupos del directorio LDAP. Los grupos definidos en NetScaler Gateway deben ser los mismos que los del directorio LDAP. En Active Directory, configure grupos en el nivel raíz del dominio. Si crea grupos de Active Directory que no están en el nivel raíz del dominio, puede producirse una lectura incorrecta del certificado de cliente.

Si los usuarios y los grupos no están en el nivel raíz del dominio, la página de inicio de sesión de Citrix Gateway muestra el nombre de usuario configurado en Active Directory. Por ejemplo, en Active Directory, tiene una carpeta denominada Usuarios y el certificado dice CN=Users. En la página de inicio de sesión, en Nombre de usuario, aparece la palabra Usuarios.

Si no quiere mover sus cuentas de grupo y usuario al nivel de dominio raíz, cuando configure el servidor de autenticación de certificados en NetScaler Gateway, deje en blanco el campo de nombre de usuario y el campo de nombre de grupo.

## Configurar Single Sign-On

January 26, 2024

Puede configurar NetScaler Gateway para que admita el inicio de sesión único con Windows, aplicaciones web (como SharePoint), recursos compartidos de archivos y la Interfaz Web. El inicio de sesión único también se aplica a los recursos compartidos de archivos a los que los usuarios pueden acceder mediante la utilidad de transferencia de archivos de la interfaz de acceso o desde el menú de iconos de NetScaler Gateway en el área de notificación.

Si configura el inicio de sesión único cuando los usuarios inician sesión, vuelven a iniciar sesión automáticamente sin tener que introducir sus credenciales por segunda vez.

## Configurar Single Sign-On con Windows

March 27, 2024

Los usuarios abren una conexión iniciando el plug-in de NetScaler Gateway desde el escritorio. Puede especificar que el plug-in de NetScaler Gateway se inicie automáticamente cuando el usuario inicie sesión en Windows habilitando el inicio de sesión único. Al configurar el inicio de sesión único, las credenciales de inicio de sesión de Windows de los usuarios se transfieren a Citrix Gateway para su

autenticación. Habilitar el inicio de sesión único para el plug-in de NetScaler Gateway facilita las operaciones en el dispositivo del usuario, como scripts de instalación y asignación automática de unidades.

Habilita el inicio de sesión único solo si los dispositivos de usuario inician sesión en el dominio de su organización. Si el inicio de sesión único está habilitado y un usuario se conecta desde un dispositivo que no está en su dominio, se le pedirá al usuario que inicie sesión.

El inicio de sesión único se configura con Windows de forma global o mediante un perfil de sesión asociado a una directiva de sesión.

### Para configurar el inicio de sesión único con Windows de forma global

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la pestaña Experiencia del cliente, haga clic en Inicio de sesión único con Windows y, a continuación, en Aceptar.

### Para configurar el inicio de sesión único con Windows mediante una directiva de sesión

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En Nombre , escriba un nombre para el perfil.
6. En la pestaña Experiencia del cliente, junto a Inicio de sesión único con Windows, haga clic en Anular global, en Inicio de sesión único con Windows y, a continuación, en Aceptar.
7. En el cuadro de diálogo Crear política de sesión , junto a Expresiones con nombre , seleccione General, seleccione Valor verdadero , haga clic en Agregar expresión , en Crear y, a continuación, en Cerrar .

## Configuración de Single Sign-On en Aplicaciones web

March 27, 2024

Puede configurar NetScaler Gateway para proporcionar inicio de sesión único a los servidores de la red interna que utilizan autenticación basada en web. Con el inicio de sesión único, puede rediri-

gir al usuario a una página principal personalizada, como un sitio de SharePoint o a la Interfaz Web. También puede configurar el inicio de sesión único en los recursos mediante el plug-in de NetScaler Gateway desde un marcador configurado en la página principal o una dirección web que los usuarios escriben en el explorador web.

Si va a redirigir la página principal a un sitio de SharePoint o a una Interfaz Web, proporcione la dirección web del sitio. Cuando los usuarios se autentican, ya sea mediante NetScaler Gateway o un servidor de autenticación externo, los usuarios se redirigen a la página principal especificada. Las credenciales de usuario se transfieren de forma transparente al servidor web. Si el servidor web acepta las credenciales, los usuarios inician sesión automáticamente. Si el servidor web deniega las credenciales, los usuarios reciben un mensaje de autenticación en el que se les pide su nombre de usuario y contraseña.

Puede configurar el inicio de sesión único en aplicaciones web de forma global o mediante una directiva de sesión.

### Para configurar el inicio de sesión único en aplicaciones web de forma global

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Experiencia del cliente, haga clic en Inicio de sesión único en aplicaciones web y, a continuación, haga clic en Aceptar.

### Para configurar el inicio de sesión único en aplicaciones web mediante una directiva de sesión

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la ficha Directivas, seleccione una directiva de sesión y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar política de sesión , junto a Solicitar perfil , haga clic en Modificar .
4. En la ficha Experiencia del cliente, junto a Inicio de sesión único en aplicaciones web, haga clic en Invalidación global, haga clic en Inicio de sesión único en aplicaciones web y, a continuación, haga clic en Aceptar.

### Para definir el puerto HTTP para Single Sign-On en aplicaciones web

El inicio de sesión único solo se intenta para el tráfico de red en el que el puerto de destino se considera un puerto HTTP. Para permitir el inicio de sesión único en aplicaciones que utilizan un puerto distinto del puerto 80 para el tráfico HTTP, agregue uno o varios números de puerto en NetScaler Gateway. Puede habilitar varios puertos. Los puertos se configuran globalmente.

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Configuración de red, haga clic en Configuración avanzada.
4. En Puertos HTTP, escriba el número de puerto, haga clic en Agregar y, a continuación, haga clic en Aceptar dos veces.

   Puede repetir el paso 4 para cada puerto que quiera agregar.

**Nota**: Si las aplicaciones web de la red interna utilizan direcciones IP públicas, el inicio de sesión único no funciona. Para habilitar el inicio de sesión único, la tunelización dividida debe habilitarse como parte de la configuración de directiva global, independientemente de si se utiliza el acceso sin cliente o el plug-in de NetScaler Gateway para las conexiones de dispositivos de usuario. Si no es posible habilitar la tunelización dividida a nivel global, cree un servidor virtual que utilice un intervalo de direcciones privadas.

## Configuración del inicio de sesión único en aplicaciones web mediante LDAP

March 27, 2024

Cuando configura el inicio de sesión único y los usuarios inician sesión con el nombre principal de usuario (UPN) con el formato
username@domain.com, el inicio de sesión único falla de forma predeterminada y los usuarios deben autenticarse dos veces. Si necesita utilizar este formato para el inicio de sesión de usuario, modifique la directiva de autenticación LDAP para aceptar esta forma de nombre de usuario.

### Para configurar el inicio de sesión único en aplicaciones web

1. En la utilidad de configuración, en la pestaña Configuración, expanda **Citrix Gateway > Directivas > Autenticación** .

2. En el panel de detalles, en la ficha **Directivas**, seleccione una directiva LDAP y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar la directiva de autenticación**, junto a **Servidor**, haga clic en **Modificar**.
4. En **Configuración de conexión**, en DN base (ubicación de los usuarios), escriba DC=nombredominio, DC=com.
5. En **Administrator Vincular DN**, escriba LDAPaccount@domainname.com, donde nombredominio.com es el nombre de su dominio.
6. En **Contraseña** de **administrador y Confirmar contraseña**de administrador, escriba la contraseña.
7. En **Otra configuración**, en **Atributo de nombre de inicio de sesión del servidor**, escriba UserPrincipalName.
8. En **Atributo de grupo**, escriba memberOf.
9. En **Nombre de subatributo**, escriba CN.
10. En **Atributo de nombre de SSO** , escriba el formato con el que los usuarios inician sesión y, a continuación, haga clic **dos**veces en Aceptar . Este valor es `SamAccountName` o `UserPrincipalName`.

## Configurar Single Sign-On en un dominio

March 27, 2024

Si los usuarios se conectan a servidores que ejecutan Citrix Virtual Apps y utilizan SmartAccess, puede configurar el inicio de sesión único para los usuarios que se conectan a la comunidad de servidores. Cuando configure el acceso a aplicaciones publicadas mediante una directiva y un perfil de sesión, utilice el nombre de dominio para la comunidad de servidores.

También puede configurar el inicio de sesión único para compartir archivos en la red.

### Para configurar el inicio de sesión único en un dominio

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la ficha Directivas, seleccione una directiva de sesión y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar política de sesión , junto a Solicitar perfil , haga clic en Modificar .

4. En el cuadro de diálogo Configurar perfil de sesión, en la ficha Aplicaciones publicadas, en Dominio de inicio de sesión único, haga clic en Supeditación global, escriba el nombre del dominio y, a continuación, haga clic en Aceptar dos veces.

Para obtener más información sobre cómo configurar NetScaler Gateway con Citrix Virtual Apps, consulte Integración de NetScaler Gateway con Citrix Virtual Apps and Desktops.

## Configurar el uso único de la contraseña

January 26, 2024

Puede configurar NetScaler Gateway para que utilice contraseñas de un solo uso, como un número de identificación personal (PIN) de token o un código de acceso. Una vez que un usuario introduce el código de acceso o el PIN, el servidor de autenticación invalida inmediatamente la contraseña de un solo uso y el usuario no puede volver a introducir el mismo PIN o contraseña.

Los productos que incluyen el uso de una contraseña de un solo uso incluyen:

- RSA SecurID
- Imprivata OneSign
- SafeWord
- Gemalto Protiva
- Nordic SMS PASSCODE

Para utilizar cada uno de estos productos, configure el servidor de autenticación de la red interna para que utilice RADIUS. Para obtener más información, consulte Configuración de la autenticación RADIUS.

Si configura la autenticación en NetScaler Gateway para que utilice una contraseña de un solo uso con RADIUS, tal como lo proporciona un token de RSA SecurID, por ejemplo, NetScaler Gateway intenta volver a autenticar a los usuarios mediante la contraseña almacenada en caché. Esta reautenticación se produce cuando se realizan cambios en NetScaler Gateway o si se interrumpe la conexión entre el plug-in de NetScaler Gateway y NetScaler Gateway y, a continuación, se restaura.

También se puede intentar volver a autenticar cuando las conexiones están configuradas para usar Citrix Receiver y los usuarios se conectan a la Interfaz Web mediante RADIUS o LDAP. Cuando un usuario inicia una aplicación y la usa y, a continuación, vuelve a Receiver para iniciar otra aplicación, NetScaler Gateway utiliza la información almacenada en caché para autenticar al usuario.

# Configurar RSA SecurID Authentication

January 26, 2024

Al configurar el servidor RSA/ACE para la autenticación RSA SecureID, debe completar los siguientes pasos:

Configure el cliente RADIUS con la siguiente información:

- Proporcione el nombre del dispositivo NetScaler Gateway.
- Proporciona una descripción (no es obligatorio).
- Proporcione la dirección IP del sistema.
- Proporcione el secreto compartido entre NetScaler Gateway y el servidor RADIUS.
- Configure la marca/modelo como RADIUS estándar.

En la configuración del host del agente, necesita la siguiente información:

- Proporcione el nombre de dominio completo (FQDN) de NetScaler Gateway (tal y como aparece en el certificado vinculado al servidor virtual). Después de proporcionar el FQDN, haga clic en la tecla Tabulador y se rellenará la ventana Dirección de red.

  Después de introducir el FQDN, la dirección de red aparece automáticamente. Si no lo hace, introduzca la dirección IP del sistema.
- Proporcione el tipo de agente mediante Communication Server.
- Configúrelo para importar todos los usuarios o un conjunto de usuarios a los que se les permite autenticarse a través de NetScaler Gateway.

Si aún no está configurada, cree una entrada Host de agente para el servidor RADIUS, que incluya la siguiente información:

- Proporcione el FQDN del servidor RSA.

  Después de introducir el FQDN, la dirección de red aparece automáticamente. Si no es así, proporcione la dirección IP del servidor RSA.
- Proporcione el tipo de agente, que es el servidor RADIUS.

Para obtener más información sobre la configuración de un servidor RADIUS RSA, consulte la documentación del fabricante.

Para configurar RSA SecurID, cree un perfil y una directiva de autenticación y, a continuación, vincule la directiva de forma global o a un servidor virtual. Para crear una directiva RADIUS para utilizar RSA SecurID, consulte Configuración de la autenticación RADIUS.

Después de crear la directiva de autenticación, enlaza la directiva a un servidor virtual o de forma global. Para obtener más información, consulte Directivas de autenticación vinculantes.

# Configurar la devolución de contraseña con RADIUS

March 27, 2024

Puede reemplazar las contraseñas de dominio por una contraseña de un solo uso que genera un token desde un servidor RADIUS. Cuando los usuarios inician sesión en NetScaler Gateway, introducen un número de identificación personal (PIN) y el código de acceso del token. Una vez que NetScaler Gateway valida sus credenciales, el servidor RADIUS devuelve la contraseña de Windows del usuario a NetScaler Gateway. Citrix Gateway acepta la respuesta del servidor y, a continuación, utiliza la contraseña devuelta para un inicio de sesión único en lugar de utilizar el código de acceso que los usuarios escribieron durante el inicio de sesión. Esta devolución de contraseña con la función RADIUS permite configurar el inicio de sesión único sin que los usuarios tengan que recuperar su contraseña de Windows.

Cuando los usuarios inician sesión con la devolución de contraseña, pueden acceder a todos los recursos de red permitidos en la red interna, incluidos Citrix Endpoint Management, StoreFront y la interfaz web.

Para habilitar el inicio de sesión único mediante contraseñas devueltas, configure una directiva de autenticación RADIUS en NetScaler Gateway mediante los parámetros Identificador de proveedor de contraseña y Tipo de atributo de contraseña. Estos dos parámetros devuelven la contraseña de Windows del usuario a NetScaler Gateway.

NetScaler Gateway admite Imprivata OneSign. La versión mínima requerida de Imprivata OneSign es 4.0 con service pack 3. El identificador de proveedor de contraseñas predeterminado para Imprivata OneSign es 398. El código de tipo de atributo de contraseña predeterminado para Imprivata OneSign es 5.

Puede utilizar otros servidores RADIUS para devolver contraseñas, como RSA, Cisco o Microsoft. Configure el servidor RADIUS para que devuelva la contraseña de inicio de sesión único del usuario en un par de valores de atributos específicos del proveedor. En una directiva de autenticación de NetScaler Gateway, debe agregar los parámetros Identificador de proveedor de contraseña y Tipo de atributo de contraseña para estos servidores.

Puede encontrar una lista completa de identificadores de proveedores en el sitio web de la Autoridad de Números Asignados de Internet (IANA). Por ejemplo, el identificador de proveedor para la seguridad RSA es 2197, para Microsoft es 311 y para Cisco Systems es 9. El atributo específico del proveedor que admite un proveedor debe confirmarse con el proveedor. Por ejemplo, Microsoft ha publicado una lista de atributos específicos del proveedor en Atributos RADIUS específicos del proveedor de Microsoft.

Puede seleccionar cualquiera de los atributos específicos del proveedor para almacenar la contraseña de inicio de sesión único de los usuarios en el servidor RADIUS del proveedor. Si configura NetScaler

Gateway con el identificador de proveedor y el atributo donde se almacena la contraseña de usuario en el servidor RADIUS, NetScaler Gateway solicita el valor del atributo en el paquete de solicitud de acceso que se envía al servidor RADIUS. Si el servidor RADIUS responde con el par atributo-valor correspondiente en el paquete de aceptación de acceso, la devolución de contraseña funciona independientemente del servidor RADIUS que utilice.

Para configurar el inicio de sesión único mediante contraseñas devueltas:

1. En la utilidad de configuración, en la pestaña Configuración, expanda **Citrix Gateway > Directivas > Autenticación** .
2. En el panel de navegación, haga clic en **RADIUS**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En el cuadro de diálogo Crear política de autenticación , en Nombre, escriba un nombre para la política.
5. Junto a Servidor, haga clic en **Nuevo**.
6. En Nombre, escriba el nombre del servidor.
7. Configure los ajustes del servidor RADIUS.
8. En Identificador de proveedor de contraseña, escriba el identificador de proveedor que devuelve el servidor RADIUS. Este identificador debe tener un valor mínimo de 1.
9. En Tipo de atributo de contraseña, escriba el tipo de atributo que devuelve el servidor RADIUS en el código AVP específico del proveedor. El valor puede oscilar entre 1 y 255.
10. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione la expresión, haga clic en **Agregar expresión**, en **Crear** y, a continuación, en **Cerrar**.

## Configurar la autenticación de SafeWord

January 26, 2024

La línea de productos SafeWord ayuda a proporcionar una autenticación segura mediante el uso de un código de acceso basado en un token. Una vez que los usuarios introducen un código de acceso, SafeWord lo invalida inmediatamente y no se puede volver a utilizar.

Si Access Gateway sustituye a Secure Gateway en una implementación de Secure Gateway e Interfaz Web, puede optar por no configurar la autenticación en Access Gateway y seguir permitiendo que la interfaz web proporcione autenticación de SafeWord para el tráfico HTTP entrante.

Access Gateway admite la autenticación SafeWord para los siguientes productos:

- SafeWord 2008
- Acceso a SafeWord Premier
- SafeWord para Citrix

- Acceso remoto SafeWord

Puede configurar Access Gateway para que se autentique mediante productos SafeWord de las siguientes maneras:

- Configure la autenticación para utilizar un servidor RADIUS de PremierAccess instalado como parte de SafeWord PremierAccess y permita que gestione la autenticación.
- Configure la autenticación para utilizar el agente IAS de SafeWord, que es un componente de SafeWord RemoteAccess, SafeWord para Citrix y SafeWord PremierAccess 4.0.
- Instale el agente de interfaz web SafeWord para que funcione con la interfaz web de Citrix. La autenticación no tiene que configurarse en Access Gateway y puede gestionarla la Interfaz Web de Citrix. Esta configuración no utiliza el servidor RADIUS de PremierAccess ni el agente IAS de SafeWord.

Al configurar el servidor RADIUS de SafeWord, necesita la siguiente información:

- Dirección IP de Access Gateway. Al configurar la configuración del cliente en el servidor RADIUS, utilice la dirección IP de Access Gateway.
- Un secreto compartido.
- La dirección IP y el puerto del servidor SafeWord.

## Configurar la autenticación de Gemalto Protiva

January 26, 2024

Protiva es una plataforma de autenticación sólida que se desarrolló para utilizar los puntos fuertes de la autenticación con tarjeta inteligente de Gemalto. Con Protiva, los usuarios inician sesión con un nombre de usuario, una contraseña y una contraseña de un solo uso generados por el dispositivo Protiva. Al igual que RSA SecurID, la solicitud de autenticación se envía al servidor de autenticación de Protiva y la contraseña se valida o se rechaza.

Para configurar Gemalto Protiva para que funcione con Citrix Gateway, siga las siguientes pautas:

- Instale el servidor Protiva.
- Instale el complemento del agente Protiva Internet Authentication Server (IAS) en un servidor RADIUS de Microsoft IAS. Asegúrese de anotar la dirección IP y el número de puerto del servidor IAS.

# nFactor para la autenticación de Gateway

January 26, 2024

La autenticación nFactor permite un conjunto completamente nuevo de posibilidades de autenticación. Los administradores que utilizan nFactor disfrutan de la flexibilidad de autenticación, autorización y auditoría (Citrix ADC AAA) al configurar los factores de autenticación para los servidores virtuales.

Dos bancos de directivas o dos factores ya no restringen a un administrador. El número de bancos de directivas puede ampliarse para adaptarse a diferentes necesidades. En función de factores anteriores, nFactor determina un método de autenticación. Los formularios de inicio de sesión dinámicos y las acciones en caso de fallo son posibles mediante nFactor.

> **Nota:**
>
> nFactor no es compatible con la edición estándar de Citrix ADC. Es compatible con Citrix ADC Enterprise Edition y Citrix ADC Platinum Edition.

## Casos de uso

La autenticación nFactor permite flujos de autenticación dinámicos basados en el perfil de usuario. A veces, estos pueden ser flujos simples para ser intuitivos para el usuario. En otros casos, se pueden combinar con la protección de active directory u otros servidores de autenticación. A continuación se indican algunos requisitos específicos de Gateway:

1. **Selección dinámica de nombre de usuario y contraseña.** Tradicionalmente, los clientes Citrix (incluidos los navegadores y los receptores) utilizan la contraseña de Active Directory (AD) como primer campo de contraseña. La segunda contraseña está reservada para la contraseña de un solo tiempo (OTP). Sin embargo, para proteger los servidores de AD, es necesario validar primero OTP. nFactor puede hacerlo sin necesidad de modificaciones del cliente.
2. **Punto**final de autenticación multiinquilino . Algunas organizaciones utilizan distintos servidores de puerta de enlace para usuarios certificados y no certificados. Dado que los usuarios utilizan sus propios dispositivos para iniciar sesión, los niveles de acceso de los usuarios varían según el dispositivo NetScaler ADC según el dispositivo que se utilice. Gateway puede satisfacer diferentes necesidades de autenticación.
3. **Autenticación basada en la pertenencia**a un grupo . Algunas organizaciones obtienen propiedades de usuario de los servidores de AD para determinar los requisitos de autenticación. Los requisitos de autenticación pueden variar para cada usuario.

4. **Cofactores**de autenticación . En ocasiones, se utilizan diferentes pares de directivas de autenticación para autenticar distintos conjuntos de usuarios. La provisión de directivas de pares aumenta la autenticación efectiva. Las directivas dependientes se pueden crear a partir de un flujo. Por lo tanto, los conjuntos independientes de políticas se convierten en flujos propios que aumentan la eficiencia y reducen la complejidad.

### Gestión de respuestas de autenticación

Los registros de devolución de llamada de NetScaler Gateway gestionan las respuestas de autenticación. Las respuestas AAAD (daemon de autenticación) y los códigos de éxito/fallo/error/diálogo se alimentan al gestor de devolución de llamada. Los códigos de éxito/fracaso/error/diálogo dirigen a Gateway a tomar las medidas adecuadas.

### Asistencia del cliente

En la tabla siguiente se detallan los detalles de configuración.

| Cliente | Soporte nFactor | Punto de enlace de directiva de autenticación | EPA |
|---|---|---|---|
| Exploradores web | Sí | Autenticación | Sí |
| Aplicación Citrix Workspace | Sí | VPN | Sí |
| Plug-in de Gateway | Sí | VPN | Sí |

**Nota:**

- El complemento Citrix Gateway admite la autenticación nFactor a partir de la versión 12.1 49.37.
- La aplicación Citrix Workspace admite la autenticación nFactor para los sistemas operativos compatibles de las siguientes versiones de la lista.
  - Windows 4.12
  - Linux 13.10
  - Mac 1808
  - iOS 2007
  - Android 1808
  - HTML5: compatible con Store Web
  - Chrome: compatible con Store Web

### Configuración de línea de comandos

El servidor virtual de puerta de enlace necesita un servidor virtual de autenticación denominado como atributo. Esta es la única configuración requerida para este modelo.

```
add authnProfile <name-of-profile> -authnVsName <name-of-auth-vserver>
<!--NeedCopy-->
```

authnVsName es el nombre del servidor virtual de autenticación. Este servidor virtual debe configurarse con políticas de autenticación avanzadas y se usa para la autenticación nFactor.

```
add vpn vserver <name> <serviceType> <IP> <PORT> -authnProfile <name-of
   -profile>

set vpn vserver <name> -authnProfile <name-of-profile>
<!--NeedCopy-->
```

Donde authnProfile es el perfil de autenticación creado anteriormente.

### Desafíos de interoperación

La mayoría de los clientes de Legacy Gateway y los clientes de RFWeb se basan en las respuestas enviadas por Gateway. Por ejemplo, se espera una respuesta 302 a /vpn/index.html para muchos clientes. Además, estos clientes dependen de varias cookies de Gateway , como pwcount«NSC_CERT», etc.

### Análisis de punto final (EPA)

EPA en nFactor no es compatible con el módulo de autenticación, autorización y auditoría de NetScaler ADC. Por lo tanto, el servidor virtual de NetScaler Gateway lleva a cabo la EPA. Después de EPA, las credenciales de inicio de sesión se envían al servidor virtual de autenticación mediante la API mencionada anteriormente. Una vez finalizada la autenticación, Gateway continúa con el proceso posterior a la autenticación y establece la sesión de usuario.

### Consideraciones de configuración errónea

El cliente Gateway envía las credenciales de usuario solo una vez. Gateway obtiene una o dos credenciales del cliente con la solicitud de inicio de sesión. En el modo heredado, hay un máximo de dos factores. Las contraseñas obtenidas se utilizan para estos factores. Sin embargo, con nFactor el número de factores que se pueden configurar es prácticamente ilimitado. Las contraseñas obtenidas del cliente Gateway se reutilizan (según la configuración) para los factores configurados. Debe tenerse cuidado de que la contraseña de un solo uso (OTP) no se reutilice varias veces. Del mismo modo, un administrador debe asegurarse de que la contraseña reutilizada en un factor sea aplicable a ese factor.

### Definición de clientes Citrix

La opción de configuración se proporciona para ayudar a NetScaler ADC a determinar los clientes del explorador frente a los clientes gruesos como Receiver.

Se proporciona un conjunto de patrones, ns_vpn_client_useragents, para que el administrador configure patrones para todos los clientes Citrix.

Del mismo modo, vincular la cadena "Citrix Receiver"`patset` a lo anterior para ignorar todos los clientes Citrix que tengan "Citrix Receiver"en el agente de usuario.

### Restricción de nFactor para Gateway

La autenticación de nFactor for Gateway no ocurre si se dan las siguientes condiciones.

1. AuthnProfile no está configurado en NetScaler Gateway.
2. Las directivas de autenticación avanzada no están enlazadas al servidor virtual de autenticación y el mismo servidor virtual de autenticación se menciona en AuthnProfile.
3. La cadena User-Agent de la solicitud HTTP coincide con los User-Agent configurados en`patset ns_vpn_client_useragents`.

Si no se cumplen estas condiciones, se utiliza la directiva de autenticación clásica vinculada a Gateway.

Si un agente de usuario, o parte de él, está vinculado a lo mencionado anteriormente `patset`, las solicitudes procedentes de esos agentes de usuario no participan en el flujo de nFactor. Por ejemplo, el siguiente comando restringe la configuración de todos los exploradores (suponiendo que todos los exploradores contengan "Mozilla"en la cadena user-agent):

```
bind patset ns_vpn_client_useragents Mozilla
<!--NeedCopy-->
```

### LoginSchema

LoginSchema es una representación lógica del formulario de inicio de sesión. El lenguaje XML lo define. La sintaxis de LoginSchema cumple con la especificación Common Forms Protocol de Citrix.

LoginSchema define la "vista"del producto. Un administrador puede proporcionar una descripción personalizada, texto de ayuda, etc. del formulario. Esto incluye las etiquetas del propio formulario. Un cliente puede proporcionar el mensaje de éxito o error que describe el formulario presentado en un momento determinado.

### Se requieren conocimientos de LoginSchema y nFactor

Los archivos loginSchema precompilados se encuentran en la siguiente ubicación de NetScaler ADC /NSConfig/loginSchema/loginSchema/. Estos archivos de loginSchema prediseñados se adaptan a casos de uso comunes y se pueden modificar para obtener ligeras variaciones si es necesario.

Además, la mayoría de los casos de uso de un solo factor con pocas personalizaciones no necesitan la configuración del esquema de inicio de sesión.

Se recomienda al administrador que consulte la documentación del producto Citrix para ver otras opciones de configuración que permitan a Citrix ADC descubrir los factores. Una vez que el usuario envía las credenciales, el administrador puede configurar más de un factor para elegir y procesar de forma flexible los factores de autenticación.

### Configuración de la autenticación de doble factor sin utilizar LoginSchema

NetScaler ADC determina automáticamente los requisitos de doble factor según la configuración. Una vez que el usuario presenta estas credenciales, el administrador puede configurar el primer conjunto de directivas en el servidor virtual. En cada directiva puede haber un "NextFactor"configurado como un "passthrough". Una «transferencia» implica que el dispositivo Citrix ADC debe procesar el inicio de sesión con el conjunto de credenciales existente sin acudir al usuario. Mediante el uso de factores de "paso a través", un administrador puede dirigir mediante programación el flujo de autenticación. Se recomienda a los administradores que lean la especificación nFactor o las guías de implementación para obtener más detalles. Consulte https://docs.citrix.com/en-us/netscaler/12-1/aaa-tm/multi-factor-nfactor-authentication.html.

### Nombre de usuario: Contraseña y expresiones

Para procesar las credenciales de inicio de sesión, el administrador debe configurar LoginSchema. Los casos de uso de factor único o doble factor con pocas personalizaciones de LoginSchema no necesitan una definición XML específica. LoginSchema tiene otras propiedades, como userExpression y passwd-Expression, que se pueden utilizar para modificar el nombre de usuario o la contraseña que presenta el usuario. Estas son expresiones de política avanzadas y también se pueden usar para anular la entrada del usuario.

### Pasos de alto nivel en la configuración de n

El siguiente diagrama ilustra los pasos de alto nivel implicados en la configuración de nFactor.


## Configuración GUI

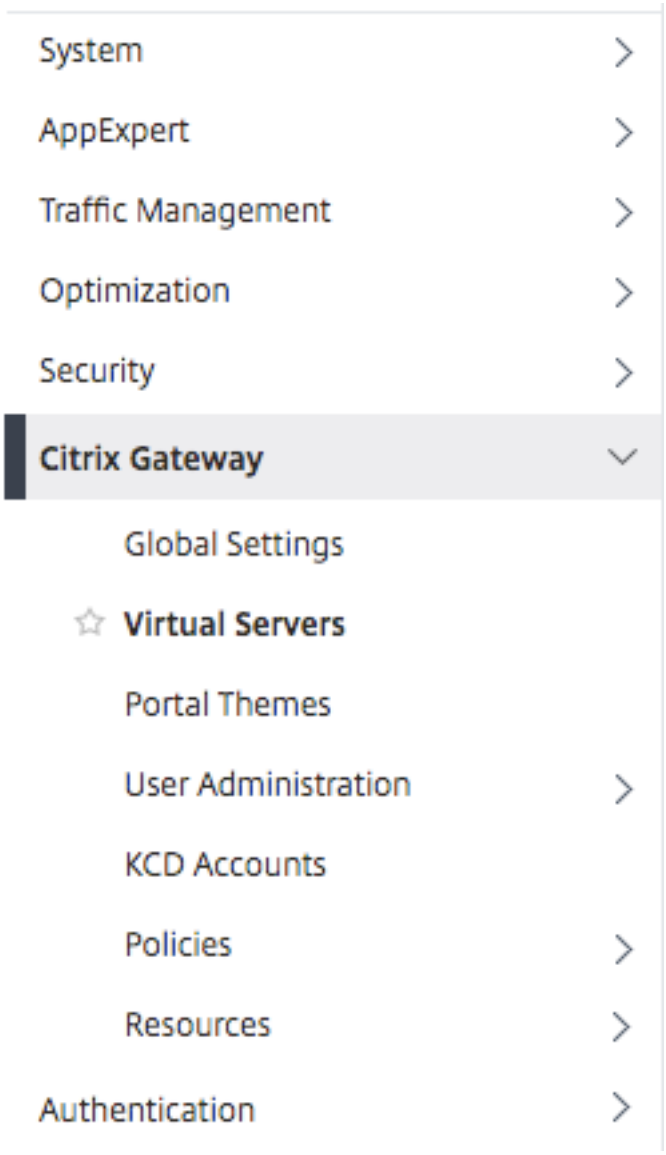
En esta sección se describen los temas siguientes:

- Creación de un servidor virtual
- Crear servidor virtual de autenticación
- Crear perfil CERT de autenticación
- Creación de una directiva de autenticación
- Agregar un servidor de autenticación LDAP
- Agregar una directiva de autenticación LDAP
- Agregar un servidor de autenticación RADIUS
- Agregar una directiva de autenticación RADIUS
- Crear un esquema de inicio de sesión de autenticación
- Creación de una etiqueta de directiva

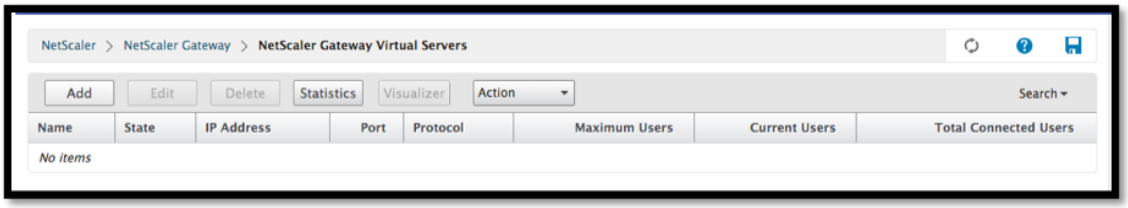
## Creación de un servidor virtual

1. Vaya a **NetScaler Gateway -> Servidores virtuales.**




2. Haga clic en el botón **Agregar** para crear un servidor virtual de puerta de enlace.




3. Introduzca la siguiente información.

| Nombre del parámetro | Descripción del parámetro |
| --- | --- |
| Escriba el nombre del servidor virtual. | Nombre del servidor virtual de NetScaler Gateway. Debe comenzar con un carácter alfabético ASCII o de subrayado (_) y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). Se puede cambiar una vez creado el servidor virtual. El siguiente requisito solo se aplica a la CLI de NetScaler ADC: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, "mi servidor"o "mi servidor"). |
| Introduzca el tipo de dirección IP del servidor virtual | Seleccione una opción Dirección IP o No direccionable del menú desplegable. |
| Introduzca la dirección IP del servidor virtual. | Una dirección de protocolo de Internet (dirección IP) es una etiqueta numérica asignada a cada dispositivo que participa en la red informática que utiliza el protocolo de Internet para la comunicación. |
| Introduzca el número de puerto del servidor virtual. | Introduzca el número de puerto. |
| Introduzca el perfil de autenticación. | Entidad de perfil de autenticación en el servidor virtual. Esta entidad se puede utilizar para transferir la autenticación al servidor virtual Citrix ADC AAA para la autenticación multifactor (nFactor) |
| Introduzca el perfil del servidor RDP. | Nombre del perfil del servidor RDP asociado al servidor virtual. |
| Introduzca el número máximo de usuarios. | Número máximo de sesiones de usuario simultáneas permitidas en este servidor virtual. El número real de usuarios permitidos para iniciar sesión en este servidor virtual depende del número total de licencias de usuario. |
| Introduzca el número máximo de intentos de inicio | Número máximo de intentos de inicio de sesión. |
| Escriba el tiempo de espera de inicio de sesión fallido. | Número de minutos que se bloquea una cuenta si el usuario supera el número máximo de intentos permitidos. |

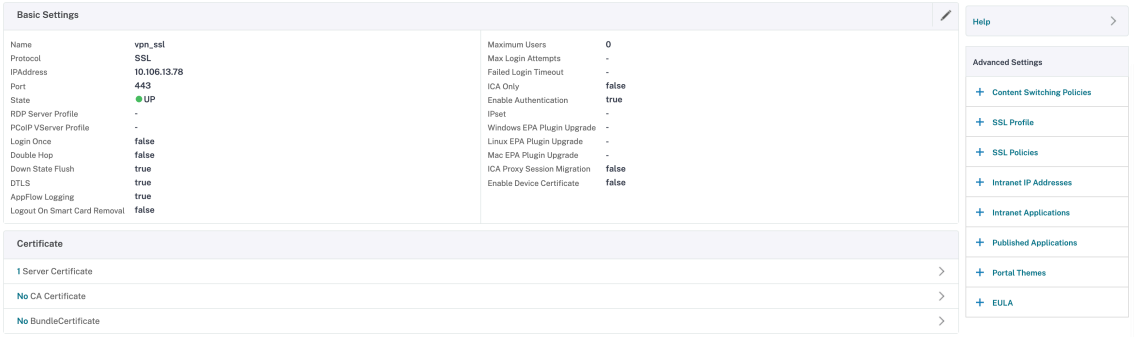
| Nombre del parámetro | Descripción del parámetro |
| --- | --- |
| Introduzca la actualización del complemento EPA de Windows. | Opción para establecer el comportamiento de actualización de plug-ins para Win. |
| Introduzca la actualización del complemento EPA de Linux. | Opción para establecer el comportamiento de actualización de plug-ins para Linux. |
| Introduzca la actualización del plug-in MAC EPA | Opción para establecer el comportamiento de actualización de plug-ins para Mac. |
| Login Once | Esta opción habilita o inhabilita el SSO sin interrupciones para este servidor virtual. |
| Solo ICA | Cuando se establece en ON, implica el modo Básico, en el que el usuario puede iniciar sesión mediante la aplicación Citrix Workspace o un explorador y acceder a las aplicaciones publicadas configuradas en el entorno Citrix Virtual Apps and Desktops indicado en el `Wihome`parámetro. No se permite a los usuarios conectarse mediante el plug-in de NetScaler Gateway y no se pueden configurar los análisis de punto final. El número de usuarios que pueden iniciar sesión y acceder a las aplicaciones no está limitado por la licencia de este modo. - Cuando está desactivado, implica el modo SmartAccess, en el que el usuario puede iniciar sesión mediante la aplicación Citrix Workspace, un explorador o un complemento de Citrix Gateway. El administrador puede configurar los análisis de puntos finales para que se ejecuten en los sistemas cliente y, a continuación, utilizar los resultados para controlar el acceso a las aplicaciones publicadas. En este modo, el cliente puede conectarse a la puerta de enlace en otros modos de cliente, como VPN y VPN sin cliente. El número de usuarios que pueden iniciar sesión y acceder a los recursos está limitado por las licencias de la CCU en este modo. |
| Habilitar autenticación | Requiere autenticación para los usuarios que se conectan a NetScaler Gateway. |

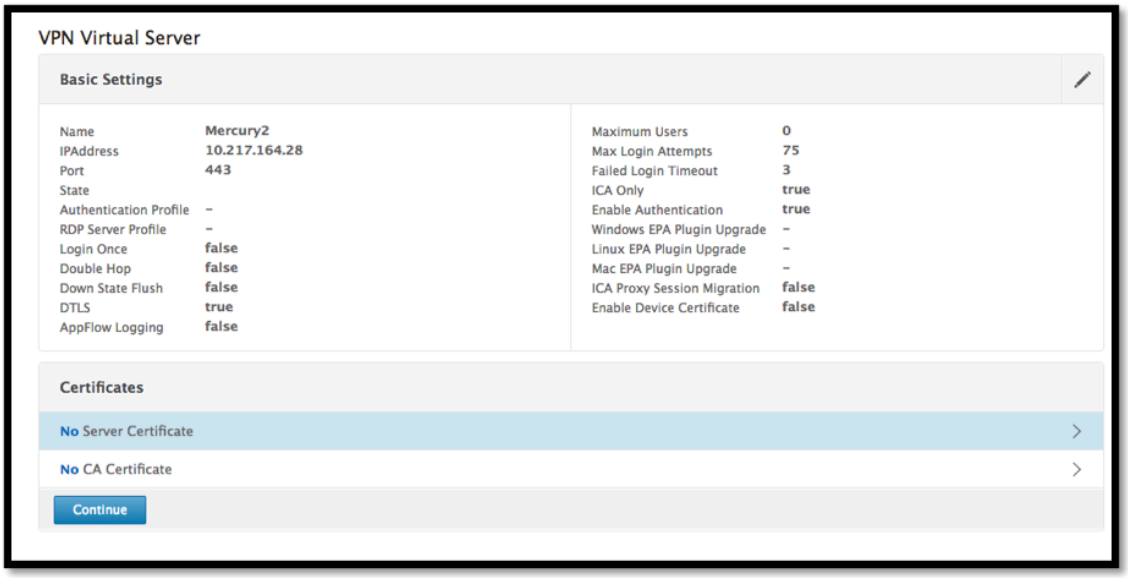
| Nombre del parámetro | Descripción del parámetro |
| --- | --- |
| Doble salto | Utilice el dispositivo NetScaler Gateway en una configuración de doble salto. Una implementación de doble salto proporciona una capa adicional de seguridad para la red interna mediante el uso de tres firewalls para dividir la DMZ en dos etapas. Dicha implementación puede tener un dispositivo en la DMZ y un dispositivo en la red segura. |
| Flush de estado descendente | Cierre las conexiones existentes cuando el servidor virtual esté marcado como DOWN, lo que significa que es posible que el servidor haya agotado el tiempo de espera. La desconexión de las conexiones existentes libera recursos y, en algunos casos, acelera la recuperación de configuraciones de equilibrio de carga sobrecargadas. Habilite este ajuste en los servidores en los que las conexiones se puedan cerrar de forma segura cuando estén marcadas como DOWN. No habilite el vaciado de estado DOWN en los servidores que deben completar sus transacciones. |
| DTLS | Esta opción inicie/detiene el servicio de turno en el servidor virtual |
| Registro de AppFlow | Registre registros de AppFlow que contienen información estándar de NetFlow o IPFIX, como marcas de tiempo para el inicio y el final de un flujo, recuento de paquetes y recuento de bytes. También registra registros que contienen información a nivel de aplicación, como direcciones web HTTP, métodos de solicitud HTTP y códigos de estado de respuesta, tiempo de respuesta del servidor y latencia. |
| Migración de sesión proxy ICA | Esta opción determina si se transfiere una sesión de proxy ICA existente cuando el usuario inicie sesión desde otro dispositivo. |
| State | El estado actual del servidor virtual, como UP, DOWN, BUSY, etc. |

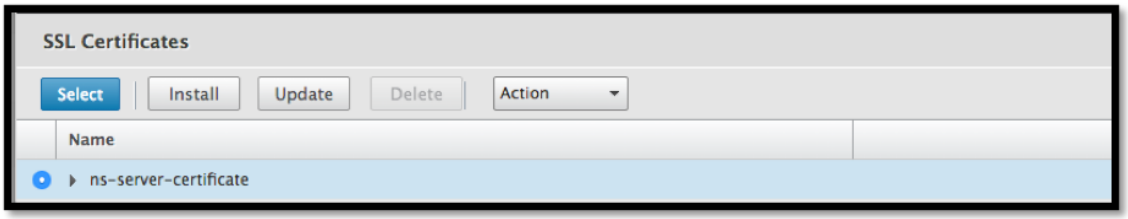
| Nombre del parámetro | Descripción del parámetro |
| --- | --- |
| Habilitar certificado de dispositivo | Indica si la comprobación del certificado de dispositivo como parte de EPA está activada o desactivada. |




4. Seleccione la sección **Sin certificado de servidor** de la página.

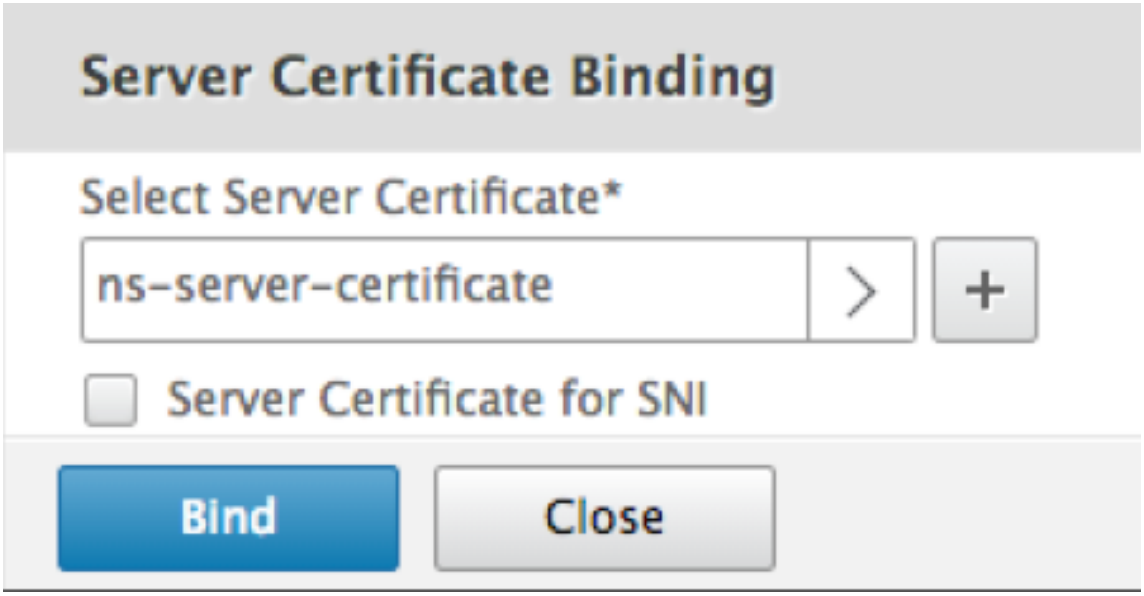



5. Haga clic en > para seleccionar el certificado del servidor.
6. Seleccione el Certificado SSL y haga clic en el botón **Seleccionar**.




7. Haga clic en **Bind**.



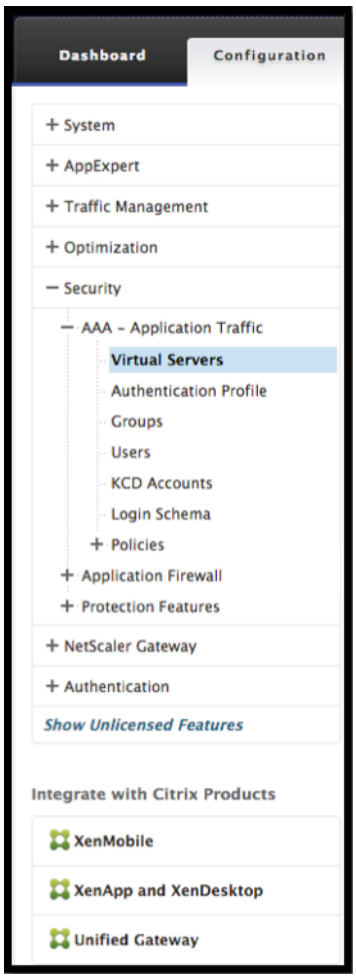

8. Si aparece una advertencia sobre **No hay cifrados utilizables**, haga clic en **Aceptar**
9. Haga clic en el botón **Continuar**.


10. En la sección Autenticación, haga clic en el icono **+** en la parte superior derecha.

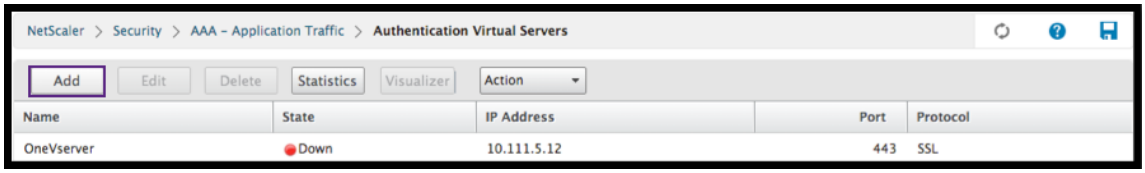

### Crear servidor virtual de autenticación

1. Vaya a **Seguridad -> AAA —Tráfico de aplicaciones -> Servidores virtuales.**




2. Haga clic en el botón **Add**.




3. Complete la siguiente configuración básica para crear el servidor virtual de autenticación.

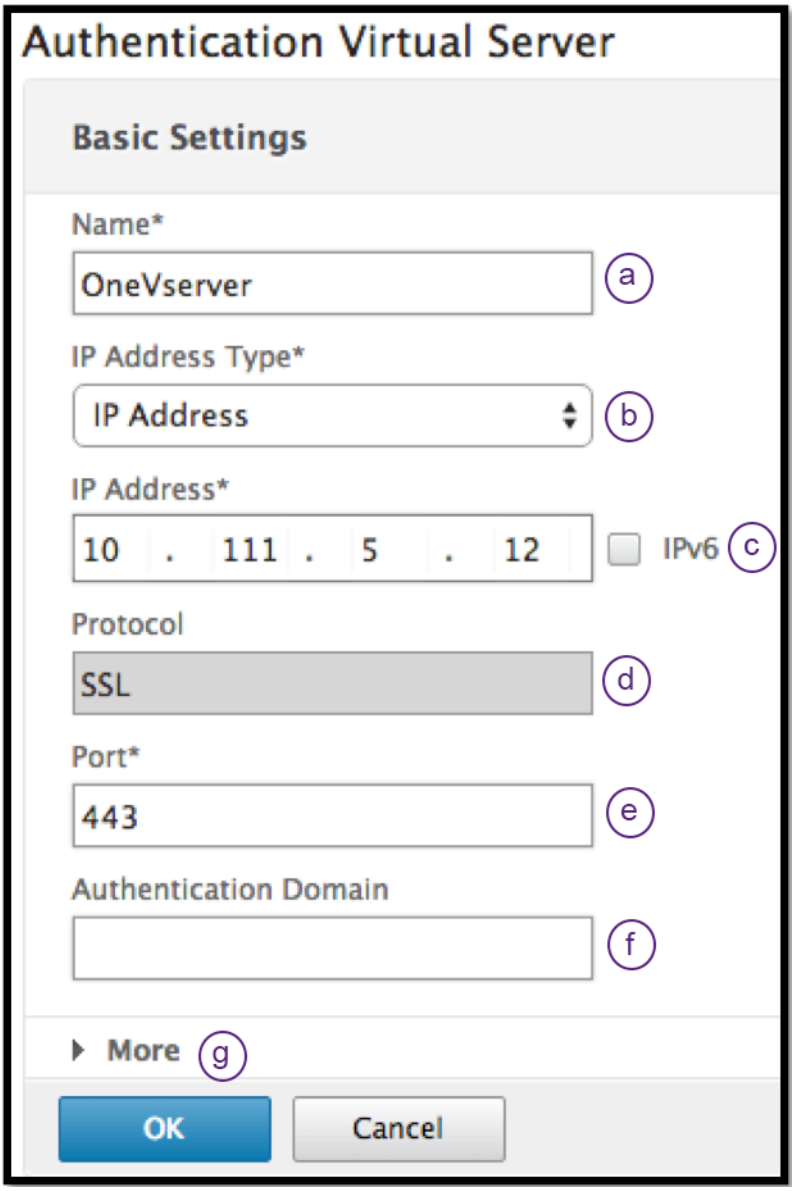
   **Nota:** El signo * situado a la derecha del nombre de la configuración indica campos obligatorios.

   - Introduzca el **nombre** del nuevo servidor virtual de autenticación.
   - Introduzca el **tipo de dirección IP**. El tipo de dirección IP se puede configurar como no direccionable.
   - Introduzca la **dirección IP**. La dirección IP puede ser cero.
   - Introduzca el tipo de **protocolo** del servidor virtual de autenticación.
   - Introduzca el **puerto TCP** en el que el servidor virtual acepta conexiones.

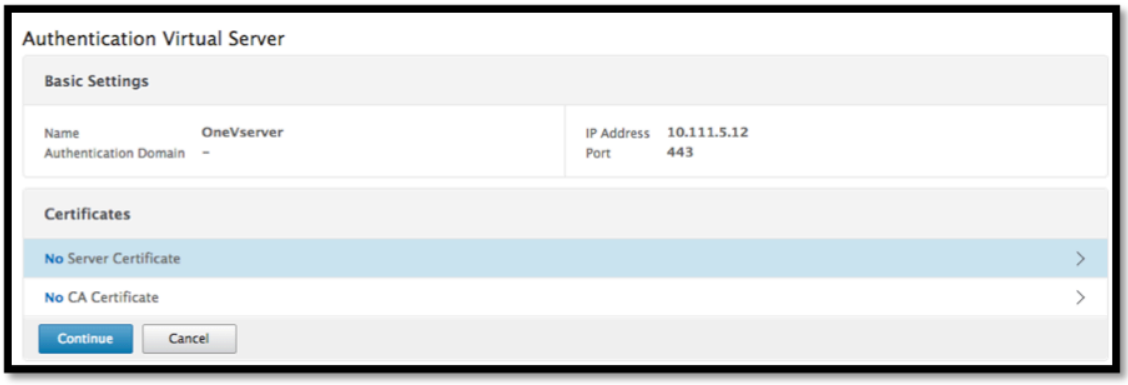
- Introduzca el **dominio** de la cookie de autenticación establecida por el servidor virtual de autenticación.

4. Haga clic en **Aceptar**.

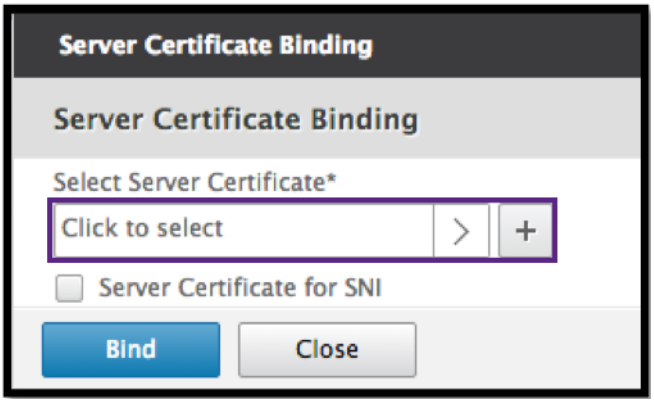



5. Haga clic en **Sin certificado de servidor**.

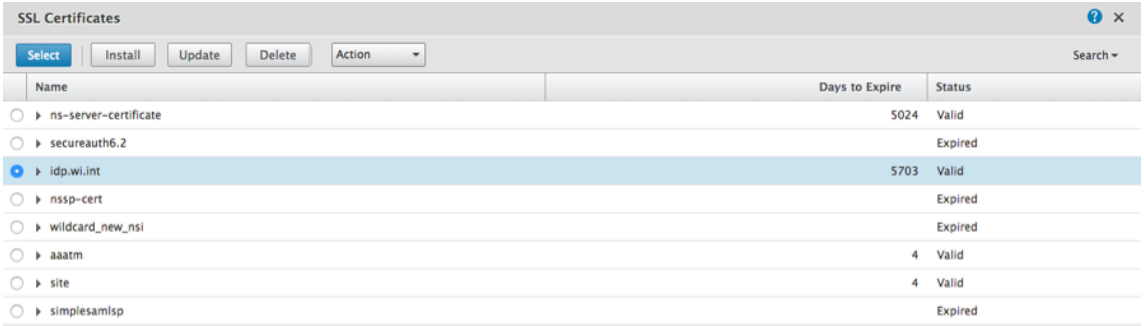



6. Seleccione el certificado de servidor deseado de la lista.




7. Elija el certificado SSL deseado y haga clic en el botón **Seleccionar**.

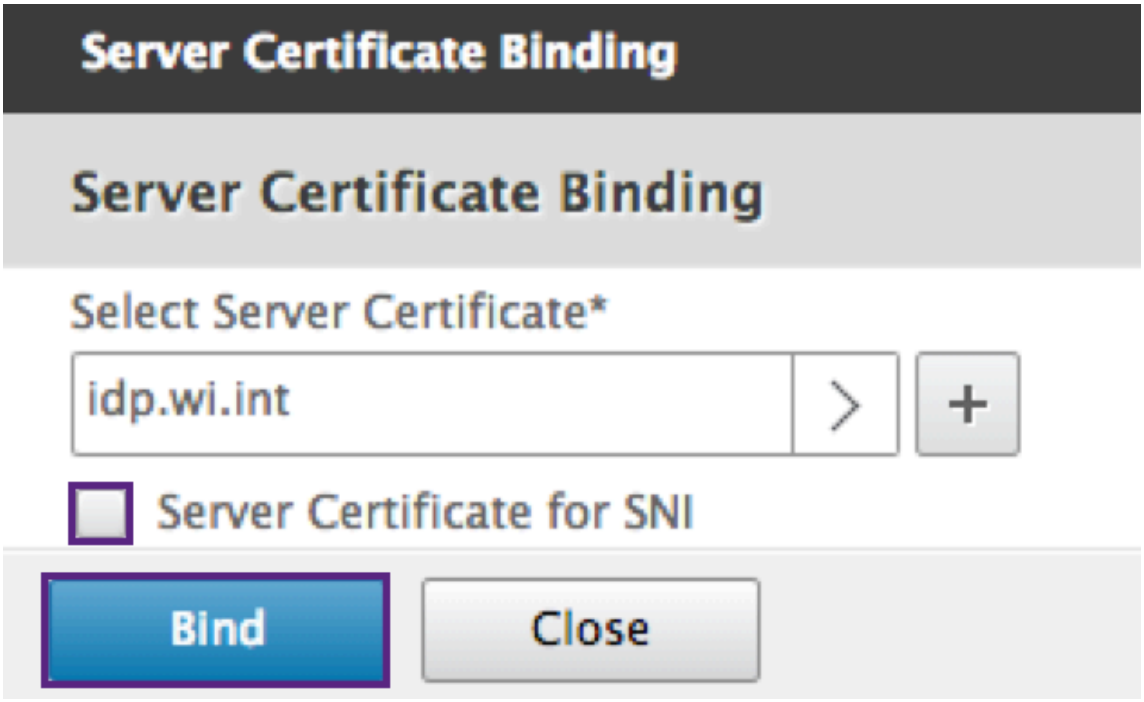
   **Nota**: El servidor virtual de autenticación no necesita un certificado vinculado a él.




8. Configure el **enlace de certificados de servidor**.

   - Marque la casilla **Certificado de servidor para SNI** para enlazar una o más claves de certificado utilizadas para el procesamiento de SNI.
   - Haga clic en el botón **Vincular**.

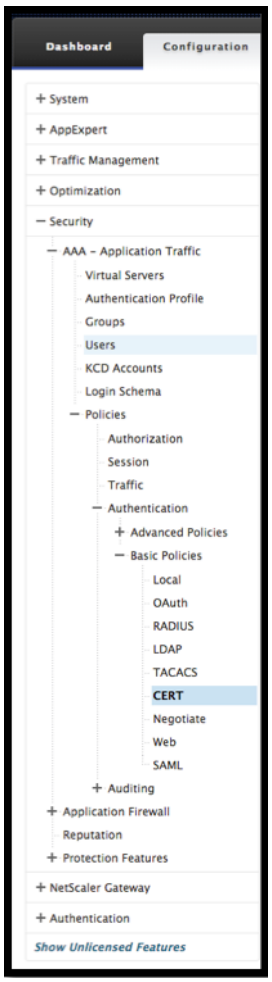
 




**Crear perfil CERT de autenticación**

1. Vaya a **Seguridad -> AAA —Tráfico de aplicaciones -> Políticas -> Autenticación -> Políticas básicas -> CERT.**




2. Seleccione la ficha Perfiles y, a continuación, seleccione **Agregar**.


3. Complete los campos siguientes para crear el perfil CERT de autenticación. El signo * situado a la derecha del nombre de la configuración indica campos obligatorios.

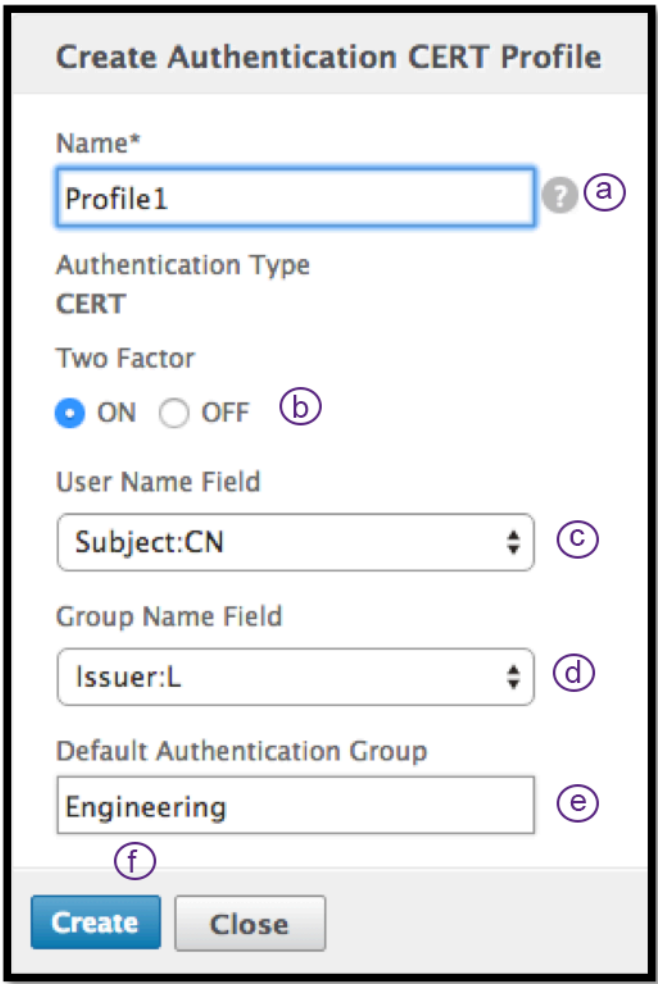
   - **Nombre**: Nombre del perfil del servidor de autenticación del certificado del cliente (acción).
   - **Dos factores**: En este caso, la opción de autenticación de dos factores es NOOP.
   - **Campo Nombre de usuario**: Introduzca el campo client-cert del que se extrae el nombre de usuario. Debe establecerse como “Subject”o “”Emisor “”(incluya ambos conjuntos de comillas dobles).
   - **Campo de nombre de grupo**: Introduzca el campo cliente-cert del que se extrae el grupo.

Debe establecerse como “Subject”o “”Emisor “”(incluya ambos conjuntos de comillas dobles).

- **Grupo de autenticación predeterminado**: Es el grupo predeterminado que se elige cuando la autenticación se realiza correctamente además de los grupos extraídos.

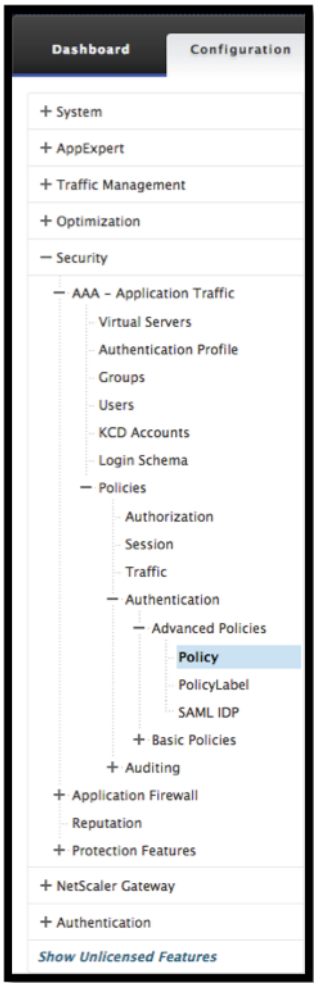
4. Haga clic en **Crear**.



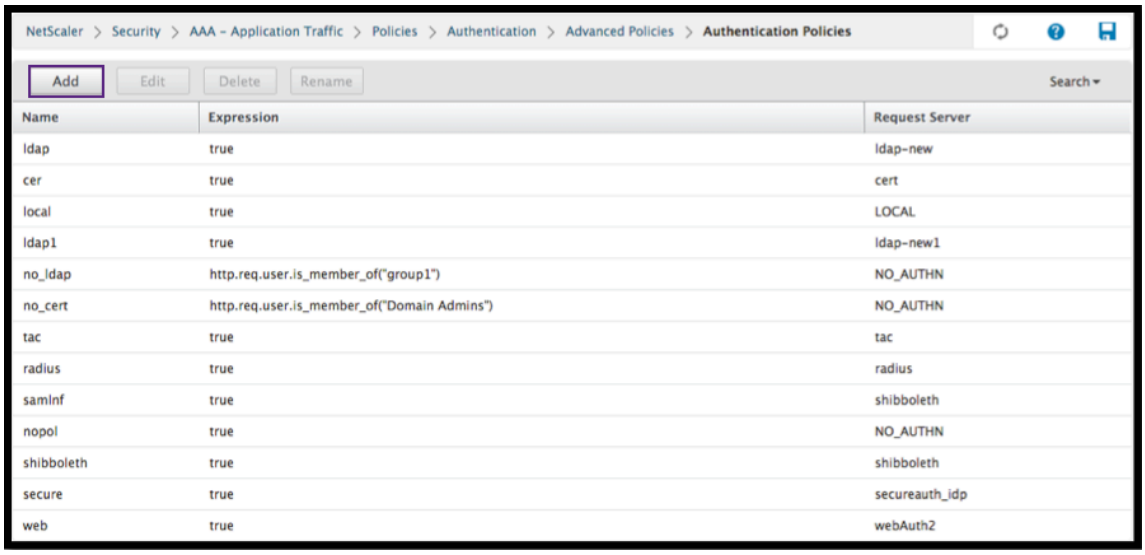

## Creación de una directiva de autenticación

1. Vaya a **Seguridad -> AAA —Tráfico de aplicaciones -> Políticas -> Autenticación -> Políticas avanzadas -> Política.**




2. Seleccione el botón **Agregar**




3. Complete la siguiente información para crear una directiva de autenticación. El signo * situado a la derecha del nombre de la configuración indica campos obligatorios.

a) **Nombre** : introduzca el nombre de la política de autenticación avanzada. Debe comenzar con una letra, un número o un carácter de guión bajo (_) y debe contener solo letras, números y guión (-), punto (.) almohadilla (#), espacio (), en (@), igual a (=), dos puntos (:) y guión bajo. No se puede cambiar una vez creada la directiva de autenticación.

El siguiente requisito solo se aplica a la CLI de NetScaler ADC: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, "mi directiva de autenticación"o "mi directiva de autenticación").

b) **Tipo de acción**: Introduzca el tipo de acción de autenticación.

c) **Acción**: Introduzca el nombre de la acción de autenticación que se realizará si la directiva coincide.

d) **Acción de registro**: Introduzca el nombre de la acción de registro de mensajes que se utilizará cuando una solicitud coincida con esta directiva.

e) **Expresión**: Introduzca el nombre de la regla con nombre de NetScaler ADC, o una expresión de sintaxis predeterminada, que la directiva utiliza para determinar si se intenta autenticar al usuario con el servidor AUTHENTICATION.

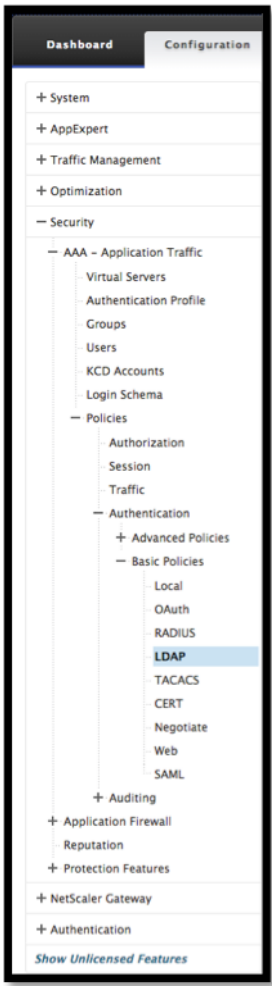
f) **Comentarios**: Introduzca cualquier comentario para conservar la información sobre esta directiva.

4. Haga clic en **Crear**.

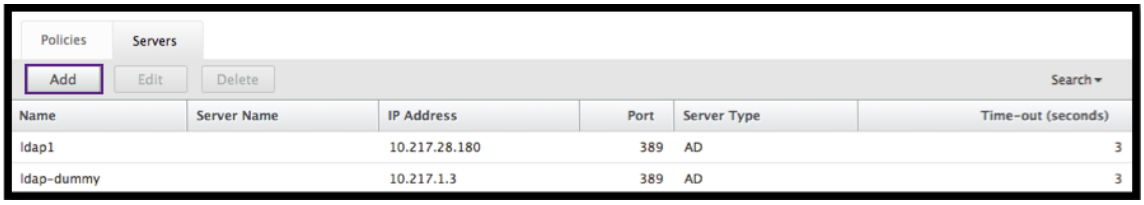

## Agregar un servidor de autenticación LDAP

1. Vaya a **Seguridad -> AAA —Tráfico de aplicaciones -> Políticas -> Autenticación -> Políticas básicas -> LDAP .**



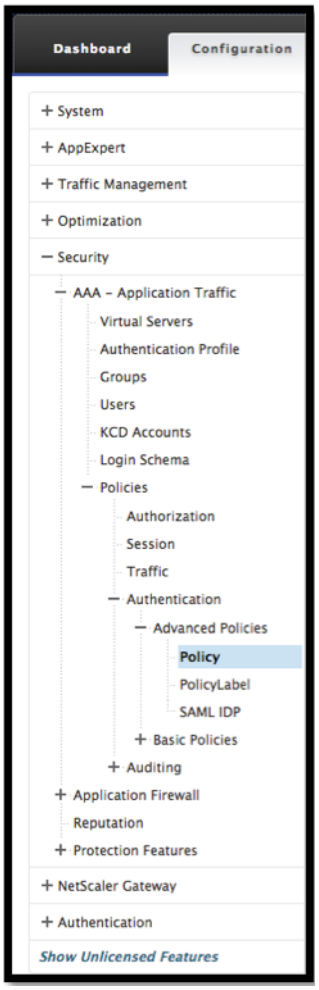

2. Agregue un servidor LDAP seleccionando la ficha **Servidor** y seleccionando el botón **Agregar**.



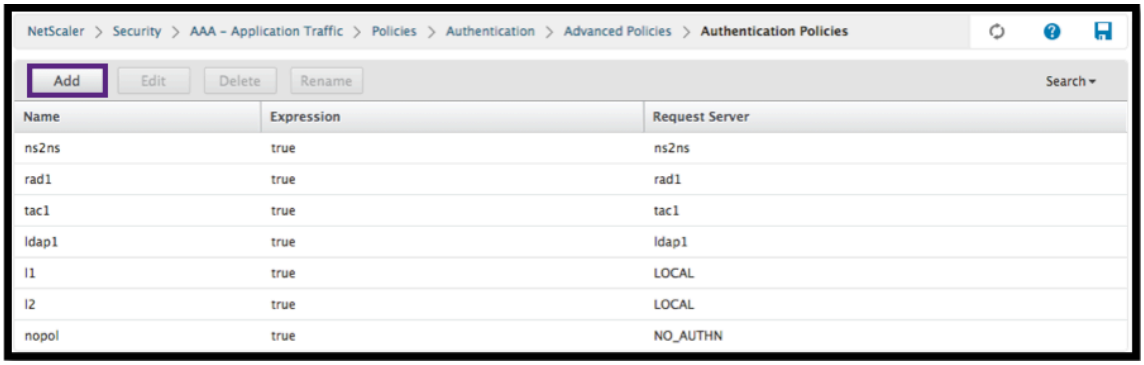

## Agregar una directiva de autenticación LDAP

1. Vaya a **Seguridad -> AAA —Tráfico de aplicaciones -> Políticas -> Autenticación -> Políticas avanzadas -> Política.**




2. Haga clic en **Agregar** para agregar una directiva de autenticación.




3. Complete la siguiente información para crear una directiva de autenticación. El signo * situado a la derecha del nombre de la configuración indica campos obligatorios.

   a) **Nombre** : nombre de la política de autenticación avanzada.
   Debe comenzar con una letra, un número o un carácter de guión bajo (_) y debe contener solo letras, números y guión (-), punto (.) almohadilla (#), espacio (), en (@), igual a (=), dos puntos (:) y guión bajo. No se puede cambiar una vez creada la directiva de autenticación.

El siguiente requisito solo se aplica a la CLI de NetScaler ADC: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “mi directiva de autenticación”o “mi directiva de autenticación”).

b) **Tipo de acción**: Tipo de acción de autenticación.

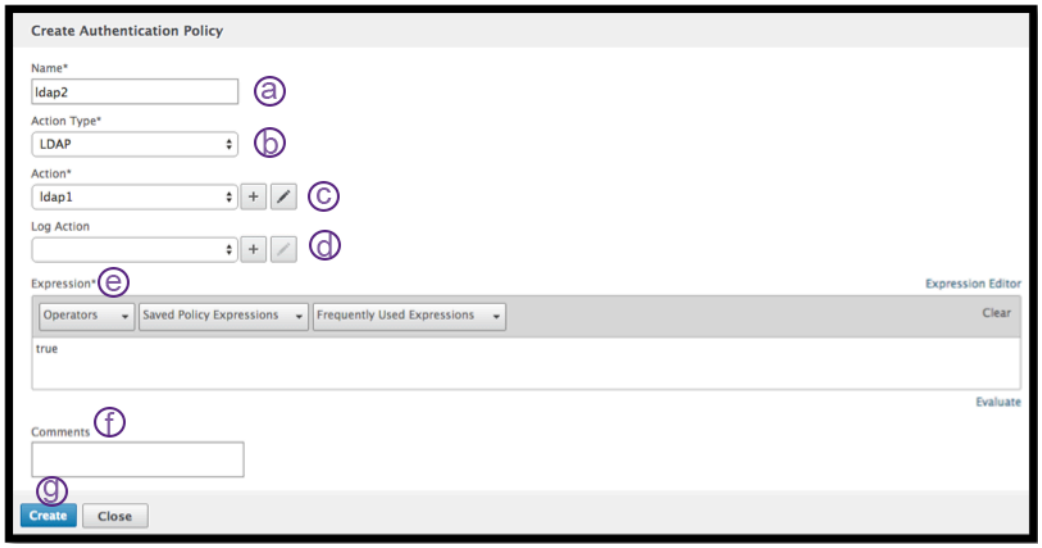
c) **Acción**: Nombre de la acción de autenticación que se va a realizar si la directiva coincide.

d) **Acción de registro**: Nombre de la acción de registro de mensajes que se utilizará cuando una solicitud coincida con esta directiva.

e) **Expresión**: Nombre de la regla con nombre de NetScaler ADC, o una expresión de sintaxis predeterminada, que la directiva utiliza para determinar si se intenta autenticar al usuario con el servidor AUTHENTICATION.

f) **Comentarios**: Cualquier comentario para preservar la información sobre esta directiva.

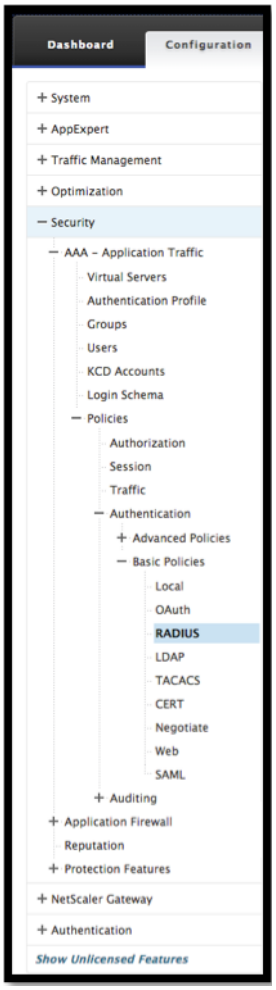
4. Haga clic en **Crear**.




## Agregar un servidor de autenticación RADIUS

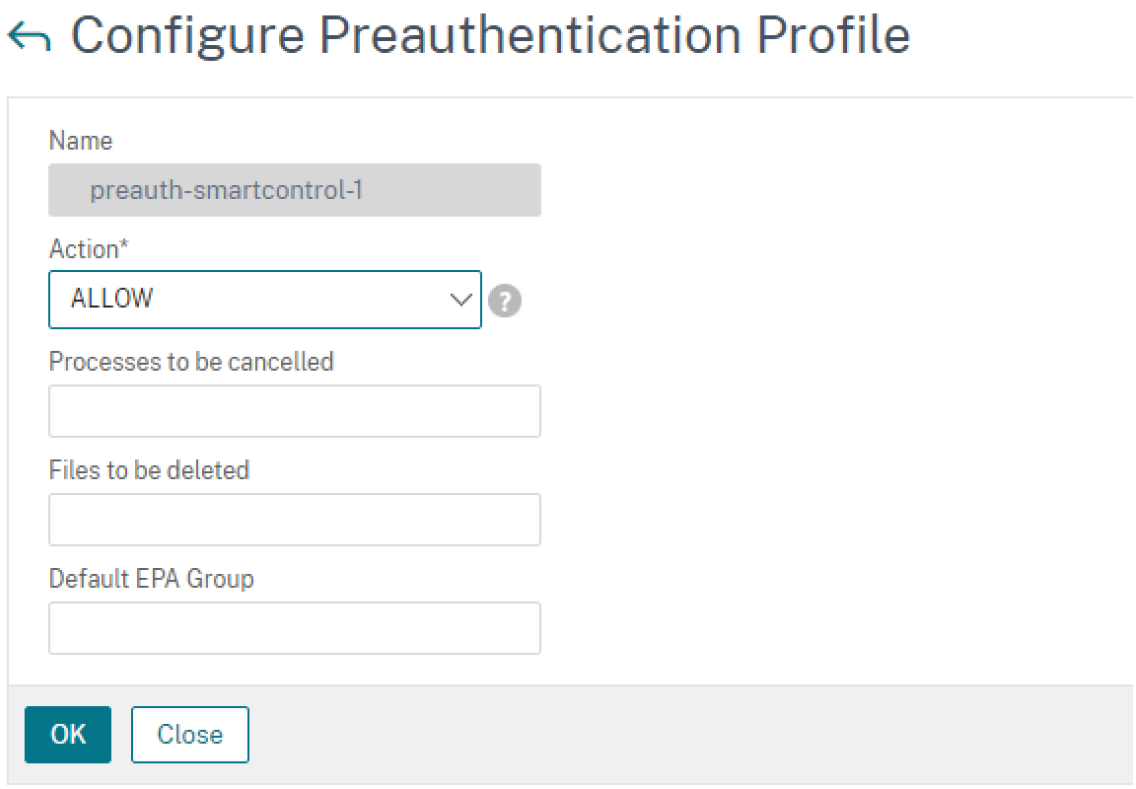
1. Vaya a **Seguridad -> AAA —Tráfico de aplicaciones -> Políticas -> Autenticación -> Políticas básicas -> RADIUS.**




2. Para agregar un servidor, seleccione la ficha **Servidores** y seleccione el botón **Agregar**.




3. Introduzca lo siguiente para crear un servidor RADIUS de autenticación. El signo * situado a la derecha del nombre de la configuración indica campos obligatorios.

   a) Introduzca un **nombre** para la acción RADIUS.

   b) Introduzca el **nombre del servidor** o la dirección **IP** del servidor asignados al servidor RADIUS.

   c) Introduzca el número de **puerto** en el que el servidor RADIUS escucha las conexiones.

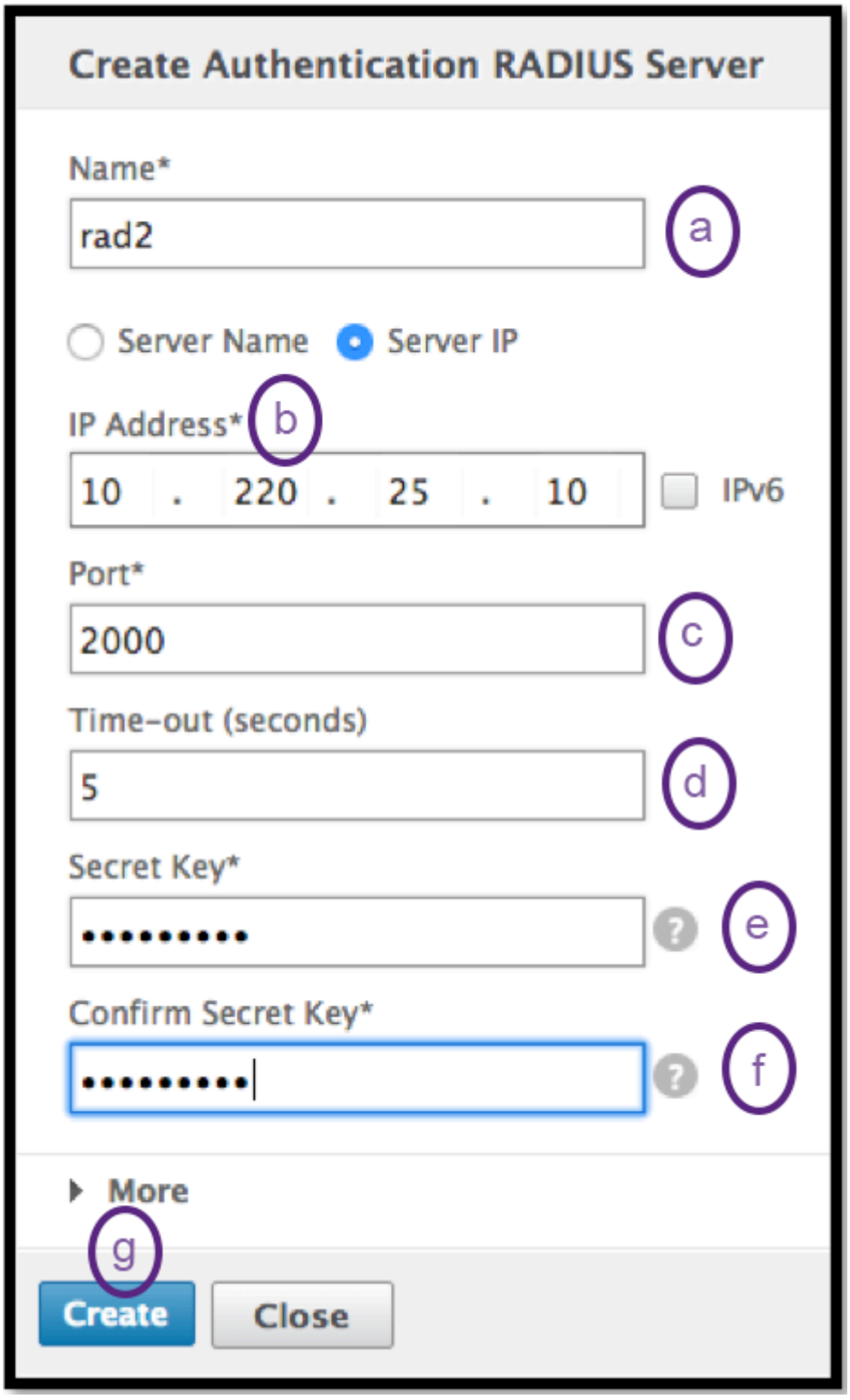
   d) Introduzca el valor de **tiempo** de espera en unos segundos. Este es el valor por el que el dispositivo Citrix ADC espera una respuesta del servidor RADIUS.

   e) Introduzca la **clave secreta** que se comparte entre el servidor RADIUS y el dispositivo Citrix ADC. La clave secreta es necesaria para permitir que el dispositivo NetScaler ADC se comunique con el servidor RADIUS.

   f) **Confirme la clave secreta** .

4. Haga clic en **Crear**.

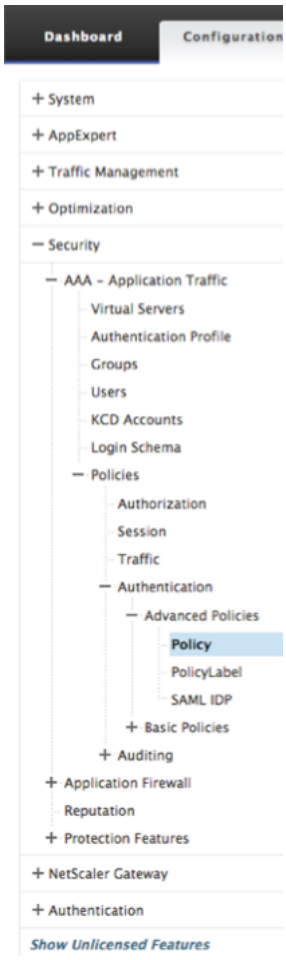
 



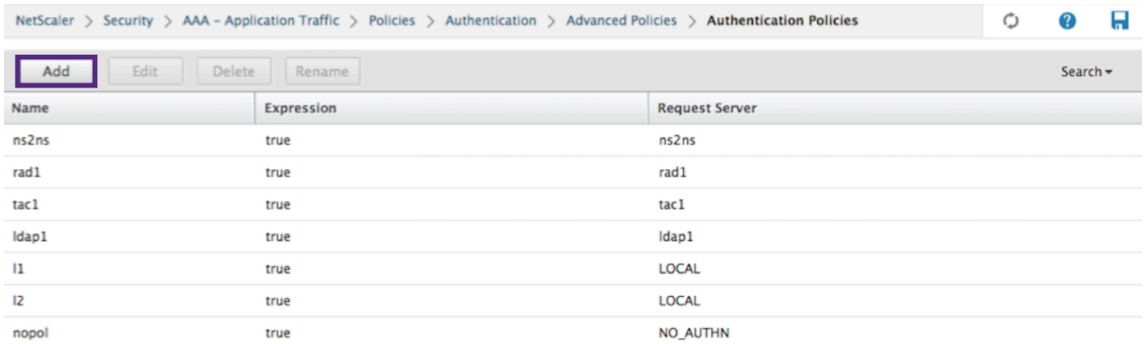

 

## Agregar una directiva de autenticación RADIUS

1. Vaya a **Seguridad -> AAA —Tráfico de aplicaciones -> Políticas -> Autenticación -> Políticas avanzadas -> Política.**




2. Haga clic en **Agregar** para crear una directiva de autenticación.




3. Complete la siguiente información para crear una directiva de autenticación. El signo * situado a la derecha del nombre de la configuración indica campos obligatorios.

   a) **Nombre** : nombre de la política de autenticación avanzada.

Debe comenzar con una letra, un número o un carácter de guión bajo (_) y debe contener solo letras, números y guión (-), punto (.) almohadilla (#), espacio (), en (@), igual a (=), dos puntos (:) y guión bajo. No se puede cambiar una vez creada la directiva de autenticación.

El siguiente requisito solo se aplica a la CLI de NetScaler ADC: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “mi directiva de autenticación”o “mi directiva de autenticación”).

b) **Tipo de acción**: Tipo de acción de autenticación.

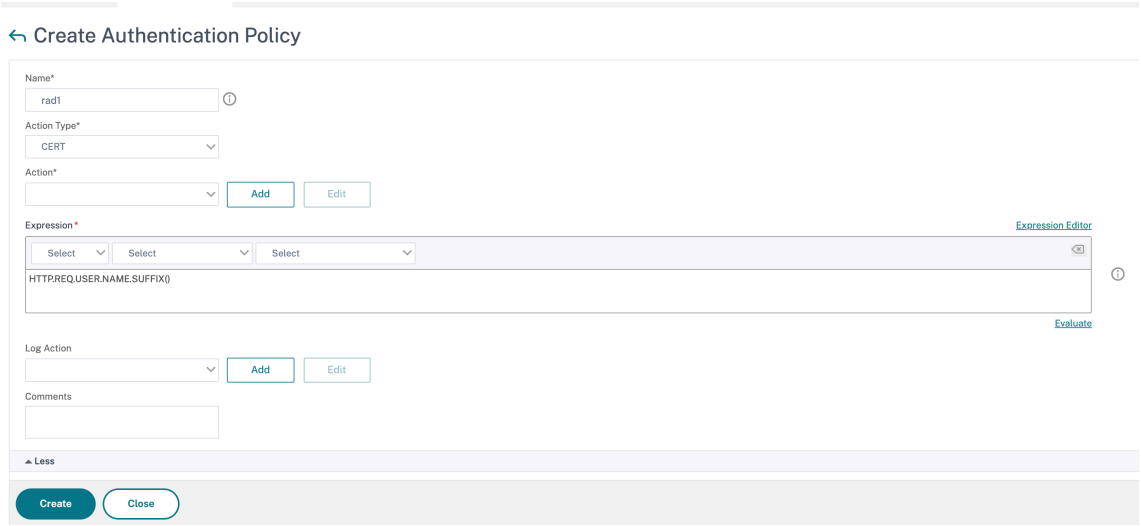
c) **Acción**: Nombre de la acción de autenticación que se va a realizar si la directiva coincide.

d) **Acción de registro**: Nombre de la acción de registro de mensajes que se utilizará cuando una solicitud coincida con esta directiva.

e) **Expresión**: Nombre de la regla con nombre de NetScaler ADC, o una expresión de sintaxis predeterminada, que la directiva utiliza para determinar si se intenta autenticar al usuario con el servidor AUTHENTICATION.

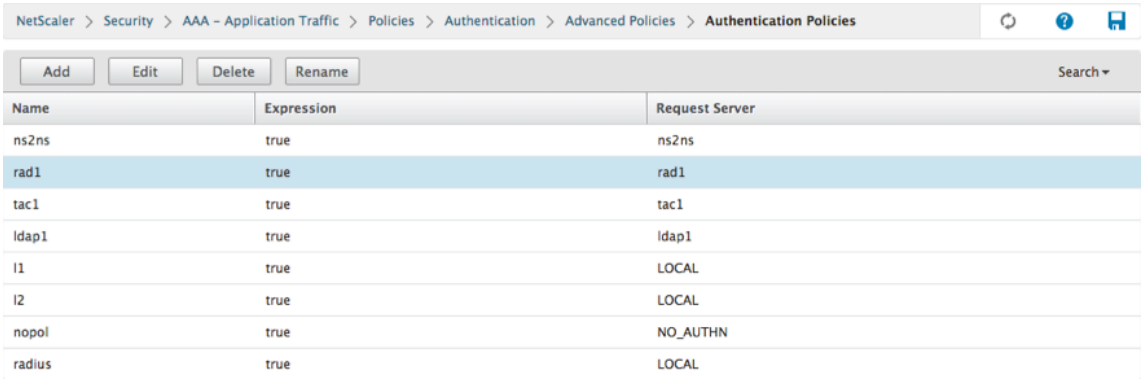
f) **Comentarios**: Cualquier comentario para preservar la información sobre esta directiva.

4. Haga clic en **OK**.




5. Compruebe que la directiva de autenticación aparezca en la lista.

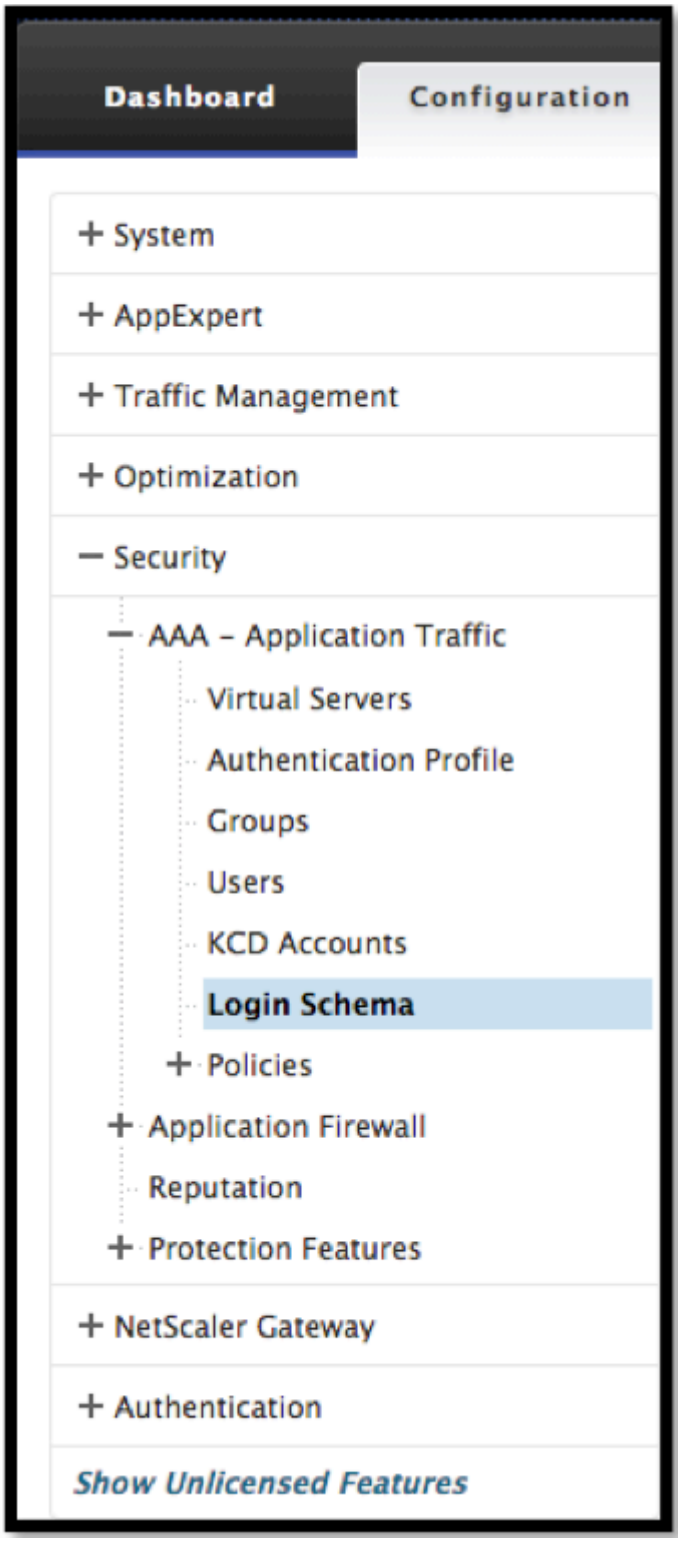
 




## Crear un esquema de inicio de sesión de autenticación

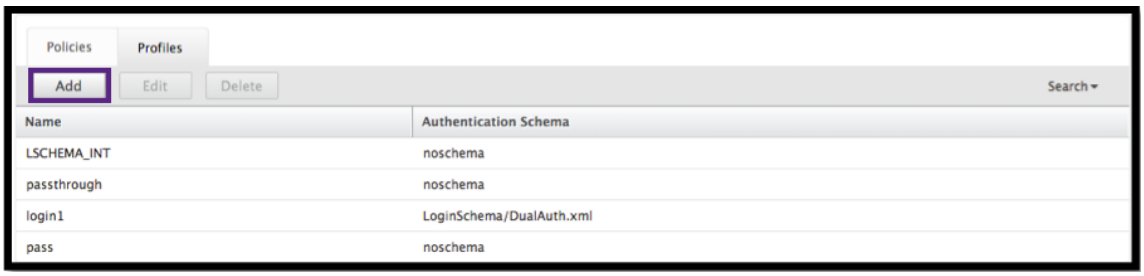
1. Vaya a **Seguridad -> AAA —Tráfico de aplicaciones -> Esquema de inicio de sesión.**




2. Seleccione la ficha Perfiles y haga clic en el botón **Agregar**.




3. Complete los campos siguientes para crear un esquema de inicio de sesión de autenticación:

   a) Introduzca el **nombre** : este es el nombre del nuevo esquema de inicio de sesión.

   b) Introduzca el **esquema de autenticación** : este es el nombre del archivo para leer un esquema de autenticación que se enviará a la interfaz de usuario de la página de inicio de sesión. Este archivo debe contener la definición xml de los elementos según el Protocolo de autenticación de Citrix Forms para poder procesar el formulario de inicio de sesión. Si un administrador no desea solicitar a los usuarios otras credenciales, sino continuar con las credenciales obtenidas anteriormente, se `noschema`puede dar como argumento. Esto solo se aplica a los loginSchemas que se utilizan con factores definidos por el usuario y no al factor de servidor virtual

   c) Introduzca la **expresión de usuario** : la expresión para la extracción del nombre de usuario durante el inicio de sesión

   d) Introduzca la **expresión de contraseña**: Esta es la expresión para la extracción de contraseña durante el inicio de sesión

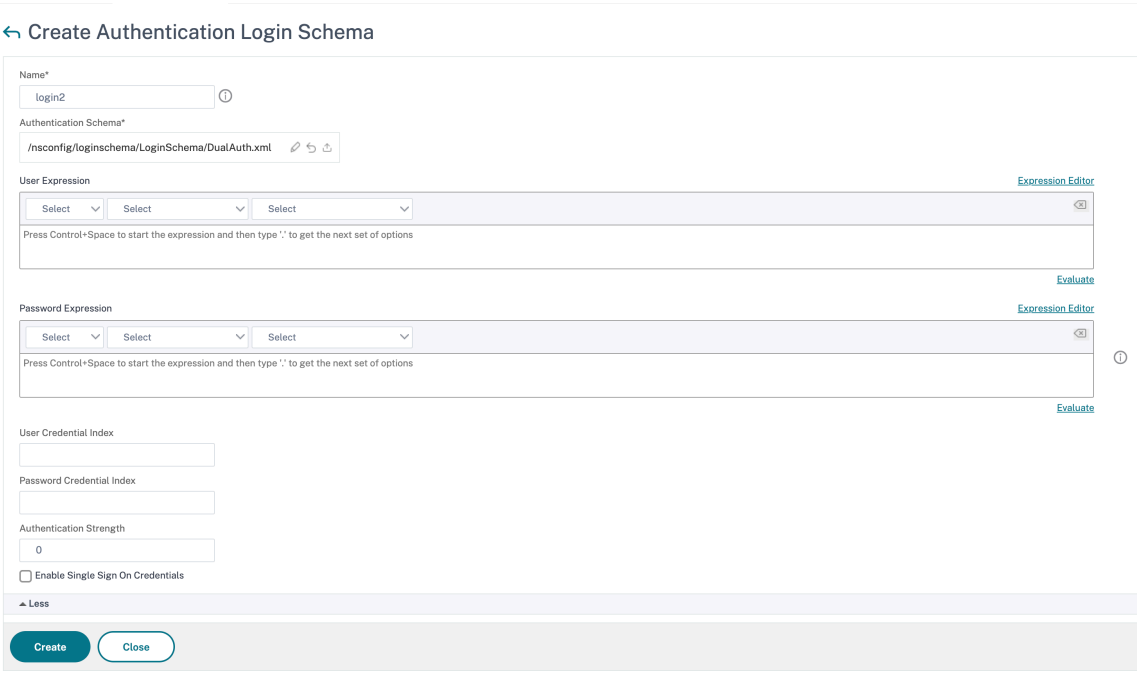
   e) Introduzca el **índice de credenciales de usuario** : este es el índice en el que el nombre de usuario introducido por el usuario debe almacenarse durante la sesión.

   f) Introduzca el **índice de credenciales de contraseña** : este es el índice en el que se debe almacenar la contraseña introducida por el usuario durante la sesión.

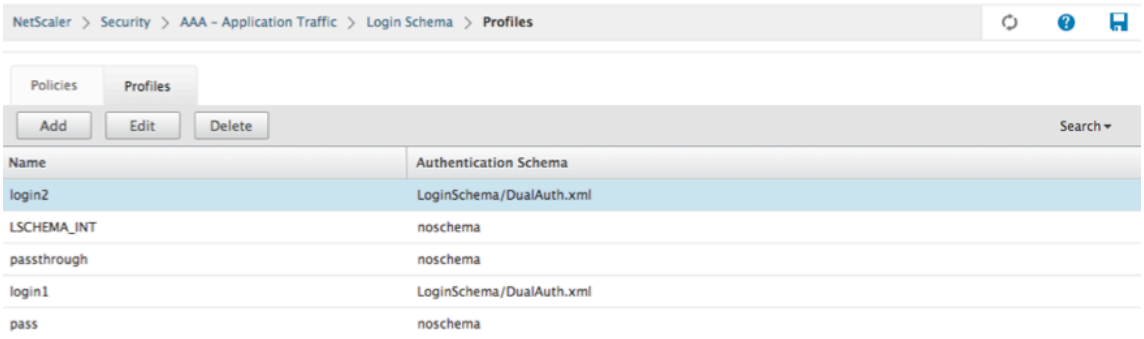
   g) Introduzca **la fuerza de autenticación**: Este es el peso de la autenticación actual.

4. Haga clic en **Crear**.




a) Compruebe que su perfil de esquema de inicio de sesión aparezca en la lista.

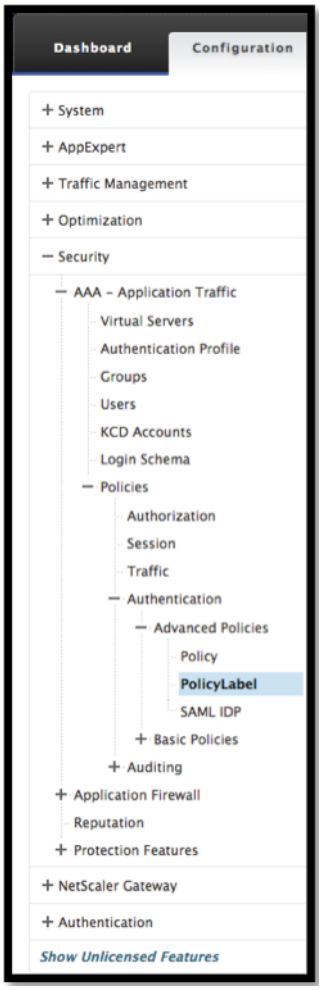



## Creación de una etiqueta de directiva

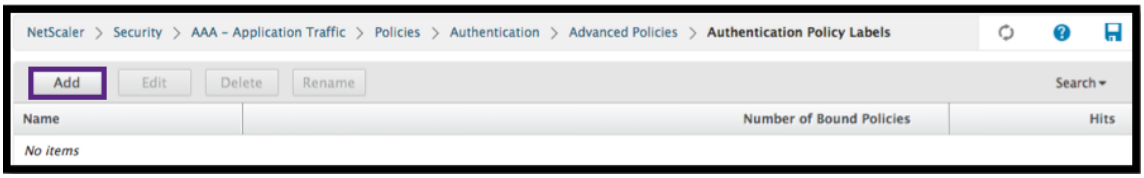
Una etiqueta de directiva especifica las directivas de autenticación de un factor concreto. Cada etiqueta de directiva corresponde a un único factor. La etiqueta de directiva especifica el formulario de inicio de sesión que debe presentarse al usuario. La etiqueta de directiva debe estar vinculada como el siguiente factor de una directiva de autenticación o de otra etiqueta de directiva de autenticación. Normalmente, una etiqueta de directiva incluye directivas de autenticación para un mecanismo de autenticación específico. Sin embargo, también puede tener una etiqueta de directiva que tenga directivas de autenticación para distintos mecanismos de autenticación.

1. Vaya a **Seguridad -> AAA —Tráfico de aplicaciones -> Políticas -> Autenticación -> Políticas avanzadas -> Etiqueta de política.**




2. Haga clic en el botón **Add**.



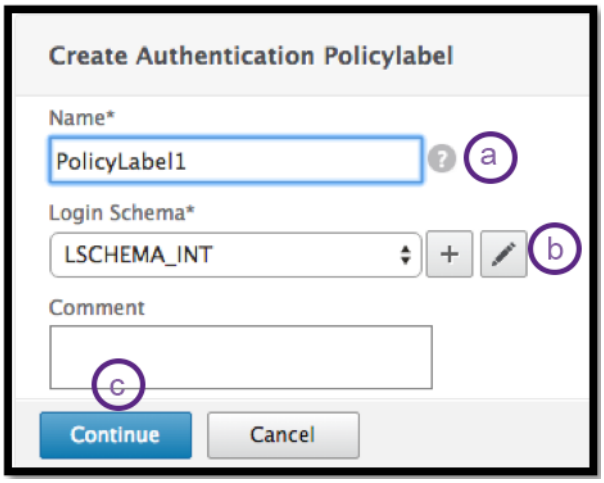

3. Complete los campos siguientes para crear una etiqueta de directiva de autenticación:

   a) Introduzca el **nombre** de la nueva etiqueta de directiva de autenticación.

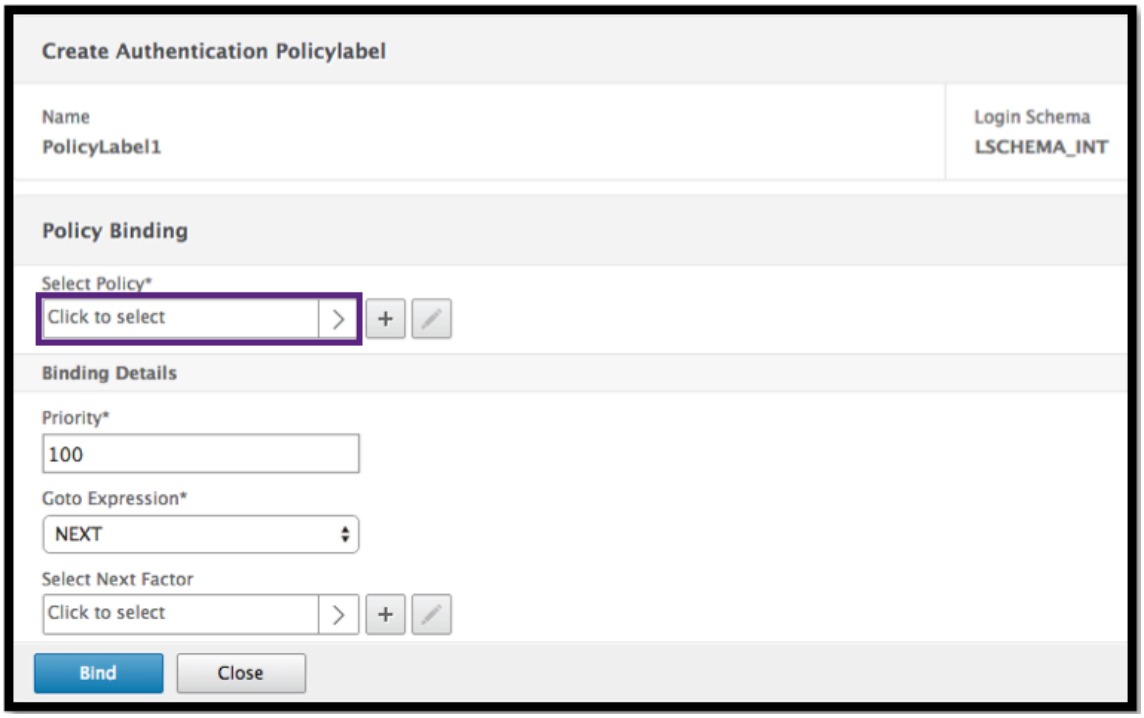
   b) Introduzca el **esquema** de inicio de sesión asociado a la etiqueta de la política de autenticación.

   c) Haga clic en **Continuar**.

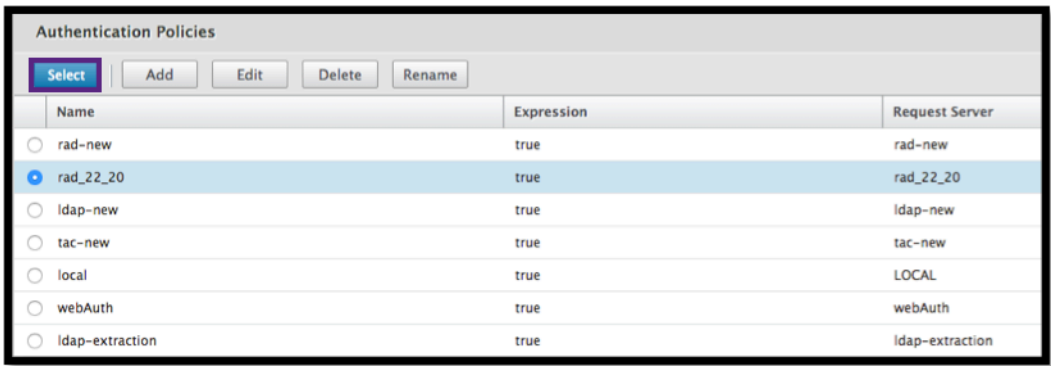
 




4. **Seleccione una directiva** en el menú desplegable.




5. Elija la **directiva de autenticación** deseada y haga clic en el botón **Seleccionar**.

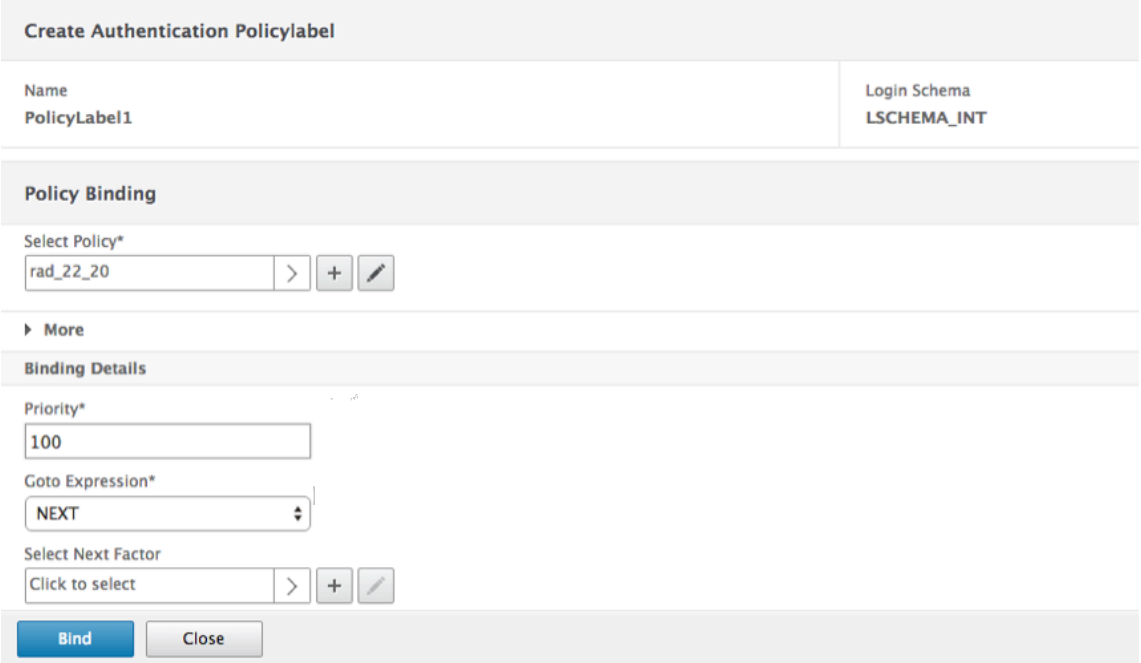


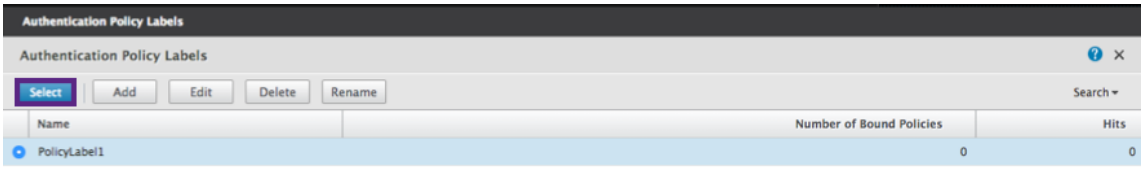
6. Rellene los campos siguientes:

   a) Introduzca la **prioridad** de la vinculación de la directiva.

   b) Introduzca la **expresión Goto**: La expresión especifica la prioridad de la siguiente política que se evaluará si la regla de política actual se evalúa como TRUE.

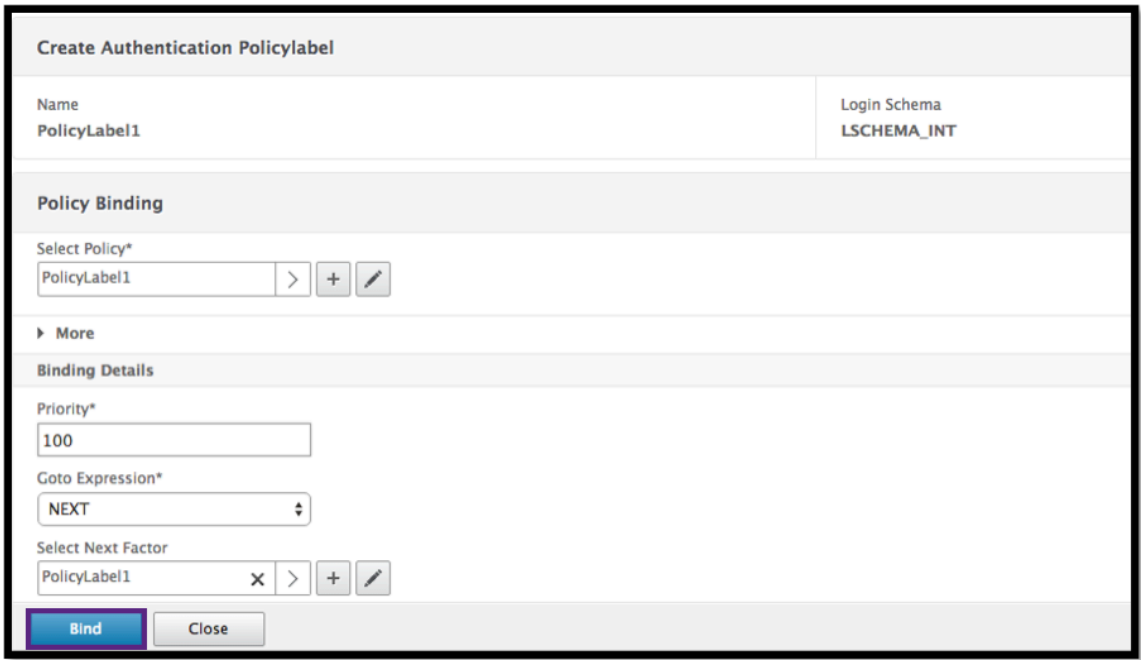



7. Seleccione la directiva de autenticación deseada y haga clic en el botón **Seleccionar**.

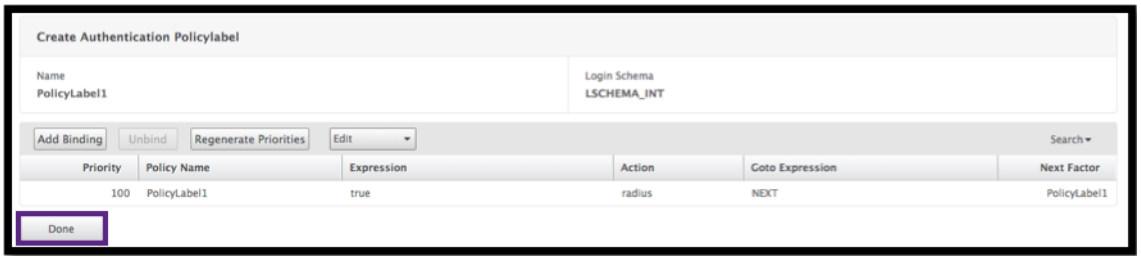



8. Haga clic en el botón **Vincular**.

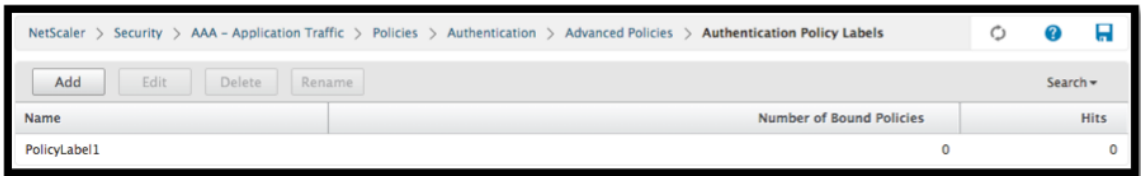
 




9. Haga clic en **Listo**.




10. Revise la etiqueta de directiva de autenticación.




## Visualizador de Unified Gateway

March 27, 2024

### Información general

El visualizador de Unified Gateway proporciona una representación visual de las configuraciones mediante el Asistente de Unified Gateway. El visualizador de Unified Gateway se utiliza para agregar y

modificar la configuración y diagnosticar un problema de back-end.

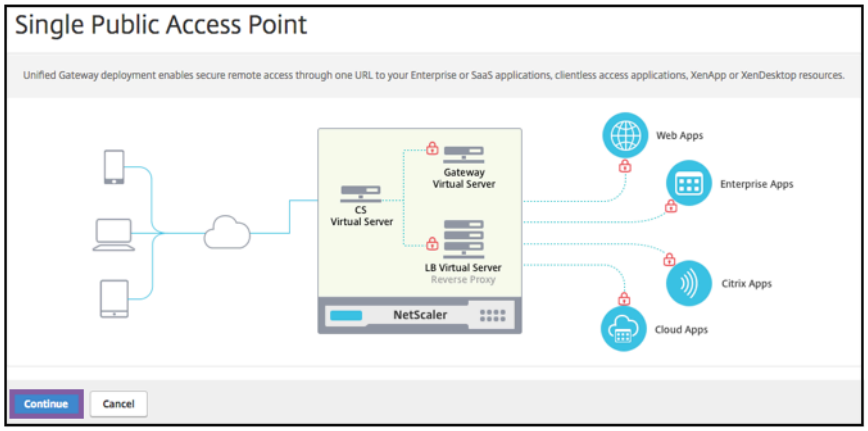
El visualizador de Unified Gateway muestra lo siguiente:

| Configuración | Configuración |
|---|---|
| Directivas de autenticación previa | Directivas de autenticación |
| Servidores virtuales CS | Servidores virtuales VPN |
| Servidores virtuales LB | Aplicaciones XA/XD |
| Aplicaciones web | Aplicaciones SaaS |

La implementación de Unified Gateway permite un acceso remoto seguro mediante una URL a sus aplicaciones empresariales o SaaS, aplicaciones de acceso sin cliente, recursos de Citrix Virtual Apps y Desktops.

### Configurar Unified Gateway

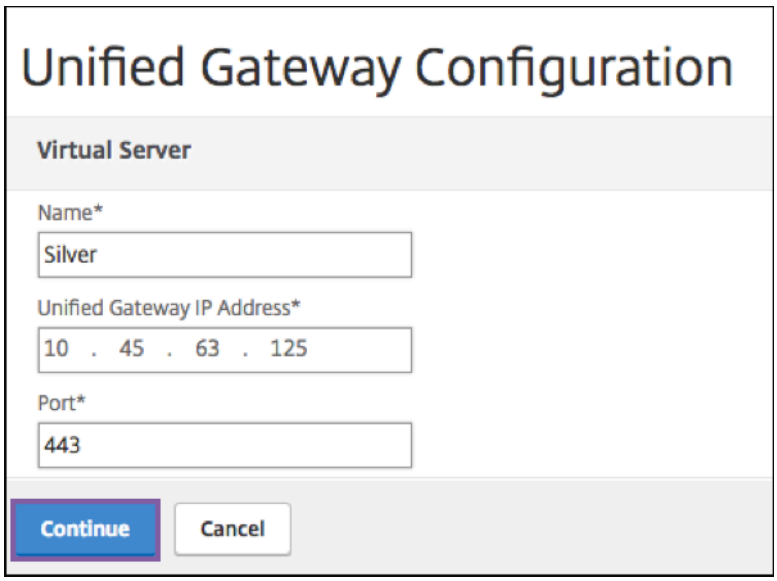
1. Seleccione Unified Gateway en el menú.
2. En la siguiente pantalla, compruebe que dispone de la siguiente información y, a continuación, haga clic en **Comenzar**:
    - Dirección IP pública de Unified Gateway.
    - Cadena de certificados de servidor (.PFX o.PEM) con certificado Root-CA opcional.
    - Detalles de autenticación basada en LDAP/RADIUS/certificado de cliente.
    - Detalles de la aplicación (URL de aplicaciones SaaS o detalles del servidor Citrix Virtual Apps and Desktops).
3. Haga clic en el botón **Continuar**.




**Cree un servidor virtual de configuración de Unified Gateway.**

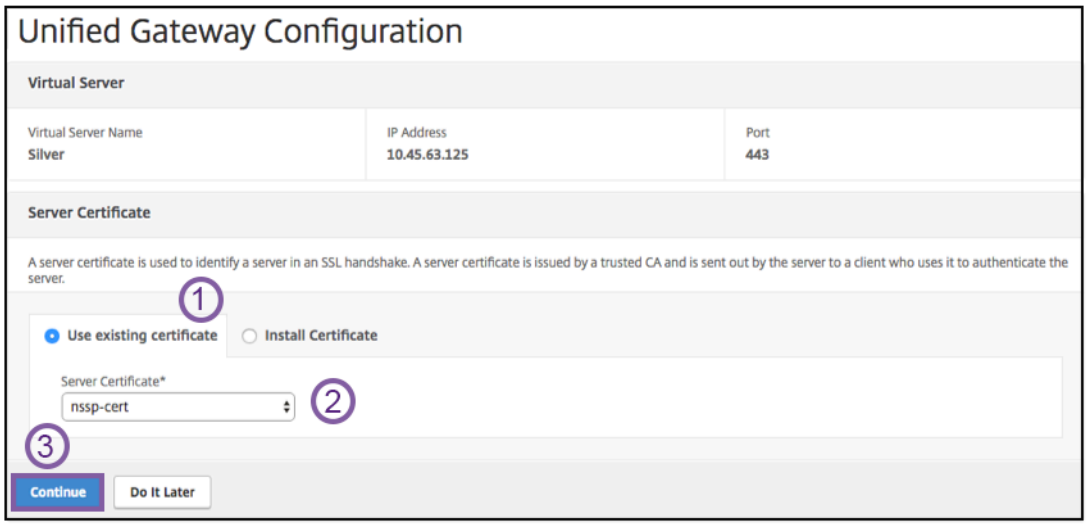
 

1. Introduzca el **nombre** de configuración del servidor virtual.
2. Introduzca la **dirección IP pública de Unified Gateway** para la implementación de Unified Gateway.
3. Introduzca el número de **puerto**. El intervalo de números de puerto es del 1 al 65535.
4. Haga clic en **Continuar**.




**Complete la siguiente información para especificar el certificado de servidor.**

1. Seleccione los botones de opción **Usar certificado existente** o **Instalar certificado**.
2. Seleccione un **certificado de servidor** en el menú.
3. Haga clic en el botón **Continuar**.

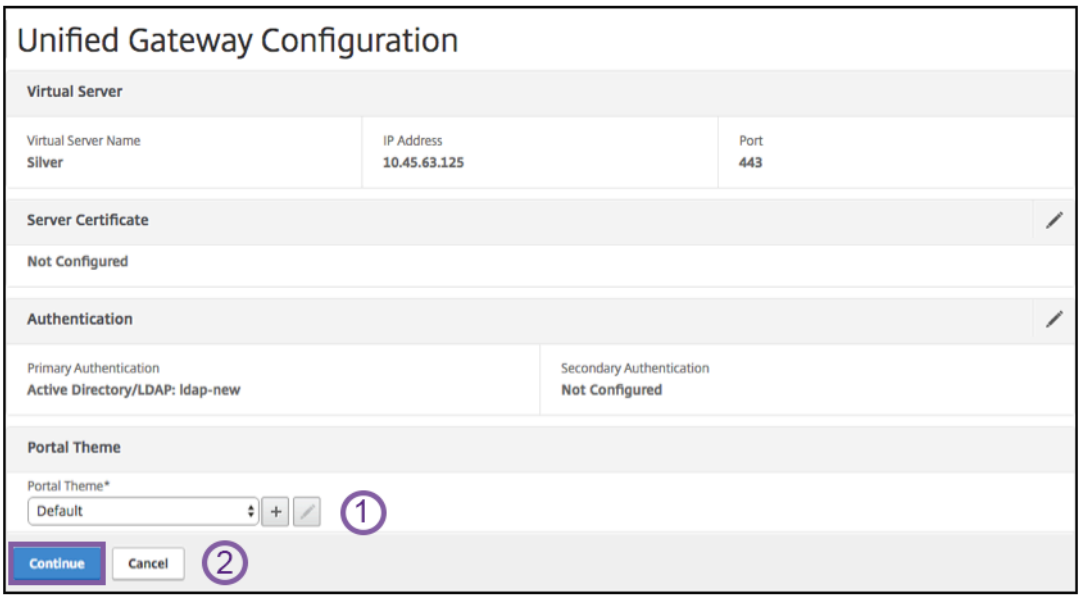



**Complete la siguiente información para especificar la autenticación.**

1. Seleccione un **método de autenticación principal** en el menú.

2. Seleccione los botones de opción **Usar servidor existente** o **Agregar nuevo servidor**.
3. Haga clic en el botón **Continuar**.
4. Selecciona el **tema del portal** en el menú.
5. Haga clic en **Continuar**.
6. Seleccione los botones de opción **Aplicación web** o **Escritorios de Citrix Virtual Apps**.
7. Haga clic en **Continuar**.




## Seleccionar aplicación

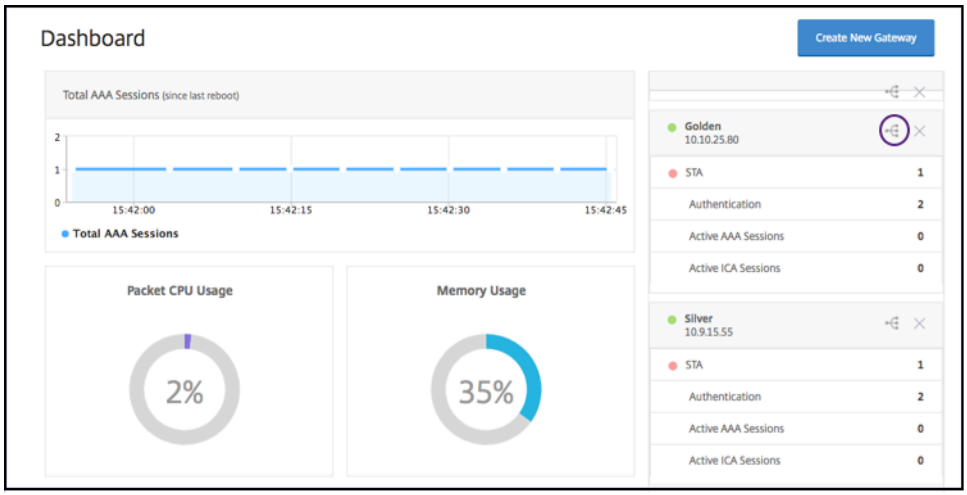
**Complete la siguiente información para especificar la aplicación web.**

1. Introduzca el nombre del enlace del marcador.
2. Seleccione el tipo de aplicación que representa la URL de VPN. Los valores posibles son:
   - Aplicación de intranet
   - Acceso sin cliente
   - SaaS
   - Aplicación preconfigurada en este NetScaler ADC
3. Marque esta casilla para que esta aplicación sea accesible a través de la URL de Unified Gateway.
4. Introduzca la URL del enlace del marcador.
5. En la URL del icono, elige un archivo para obtener un archivo de íconos. MaxLength = 255
6. Haga clic en el botón **Continuar**.
7. Haga clic en **Listo**.
8. Haga clic en **Continuar**.
9. Haga clic en **Listo**.

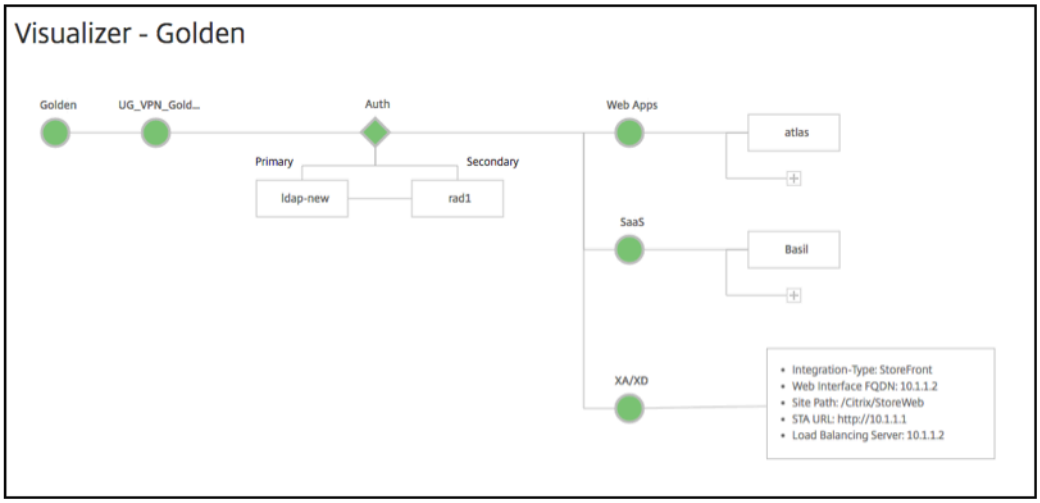
 

### Configuración GUI

1. Seleccione Unified Gateway en el menú.
2. Haga clic en el icono del **visualizador de Unified Gateway** para acceder a instancias configuradas de Gateway.

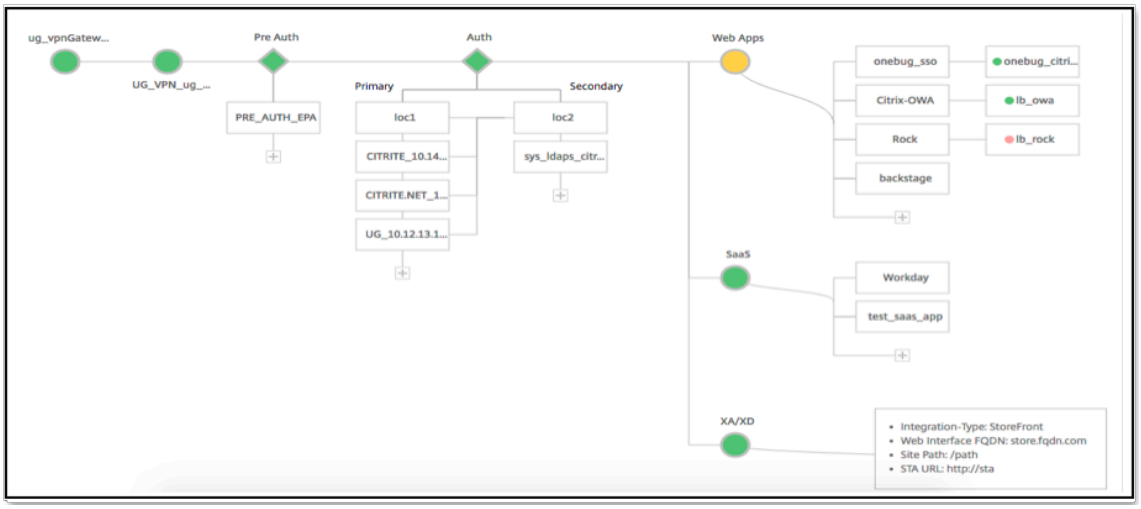



El visualizador de Unified Gateway tiene el aspecto de un diagrama de flujo, como se muestra en la siguiente imagen:




El visualizador de Unified Gateway tiene PreAuth y una sección de aplicaciones. `Auth` Si el servidor virtual de VPN tiene una directiva de autenticación previa, solo entonces `pre-auth` se muestra en el visualizador de Unified Gateway.




El visualizador de Unified Gateway utiliza un esquema de codificación de colores para el equilibrio de carga y los servidores virtuales VPN para indicar su estado.

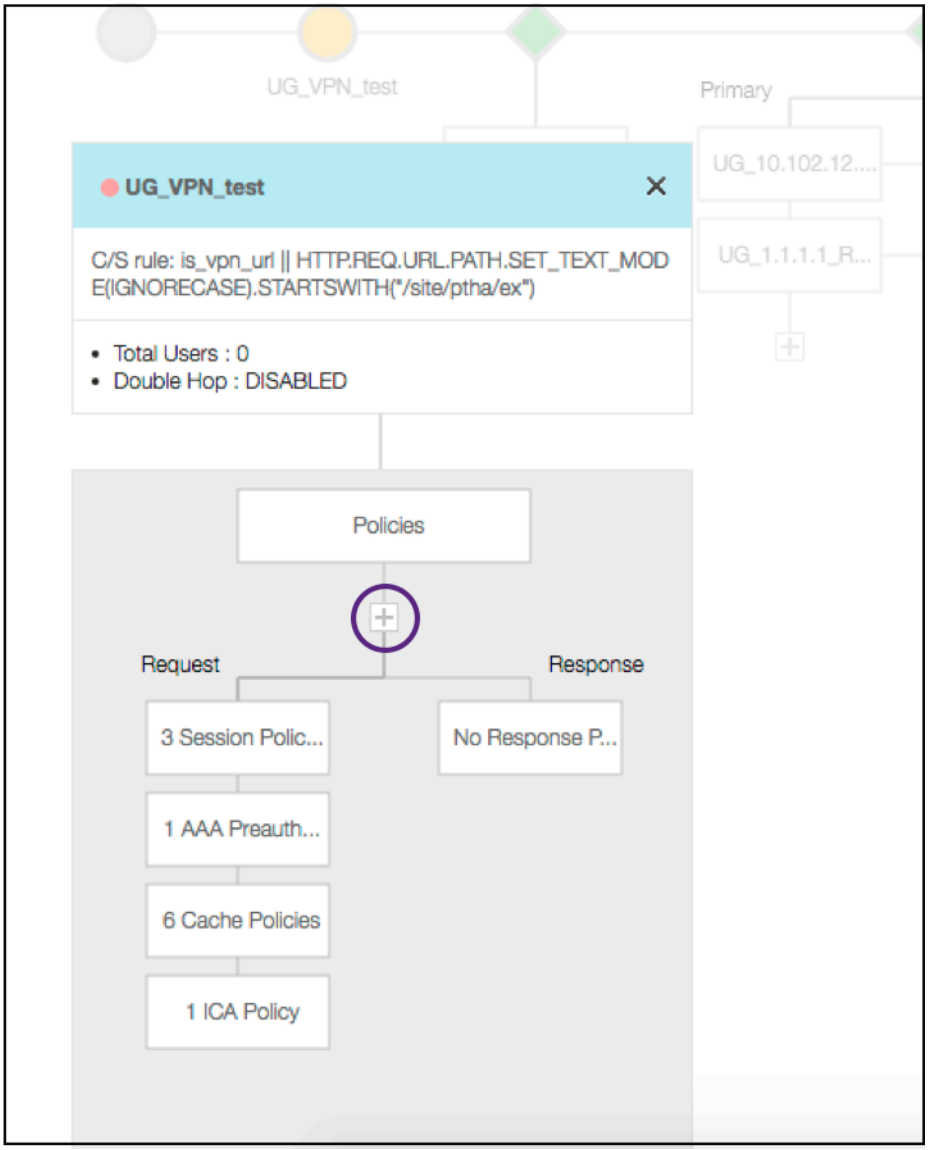
| Color | Descripción |
|---|---|
| Rojo | significa que el servidor está caído. |
| Gris | significa que las aplicaciones web/Citrix Virtual Apps no se han configurado. |
| Verde | significa que todo va bien con el servidor virtual. |
| Naranja | significa que uno de los servicios de servidor virtual de equilibrio de carga. está inactivo, pero sigue funcionando correctamente. |

### Detalles de los servidores virtuales VPN

Para obtener los detalles de los servidores virtuales VPN, haga clic en el **nodo Servidores virtuales VPN**. La ventana emergente representa detalles como la regla C/S y todas las directivas.

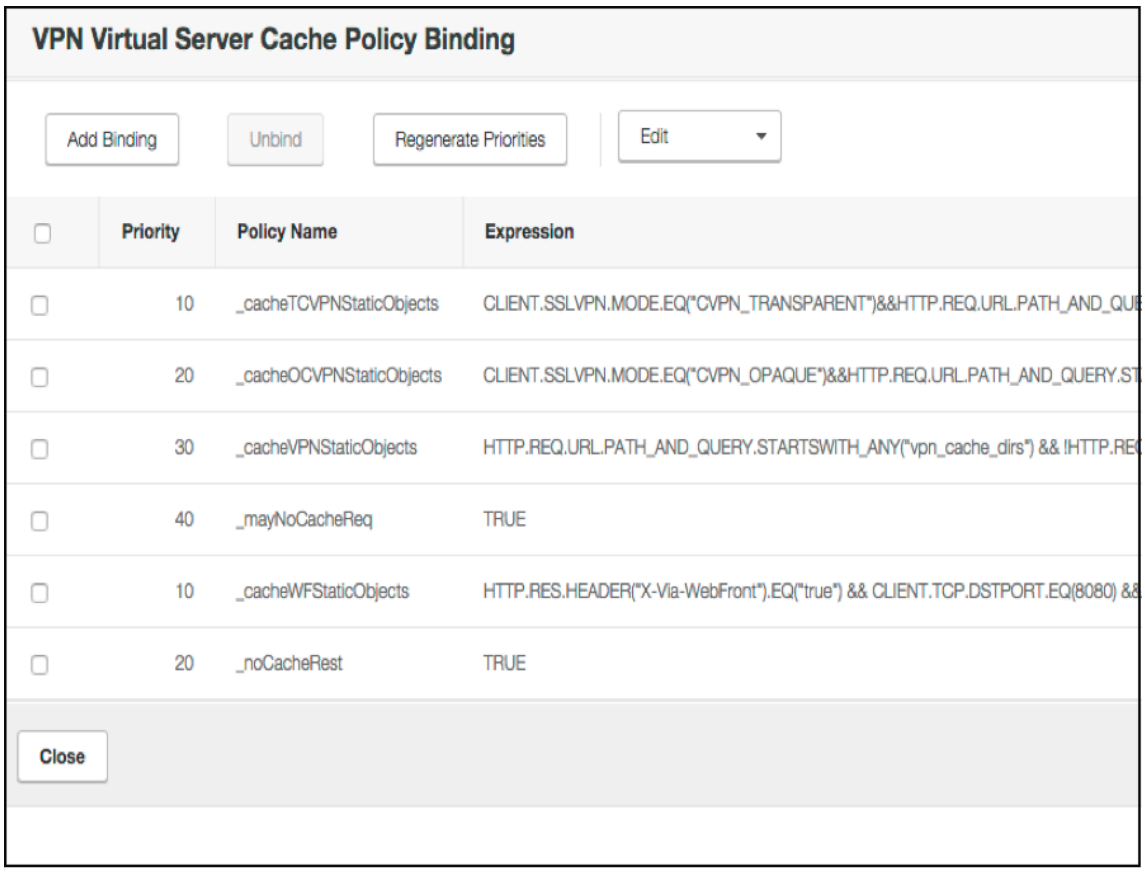
1. Agregue directivas a la entidad VPN haciendo clic en el icono (+).

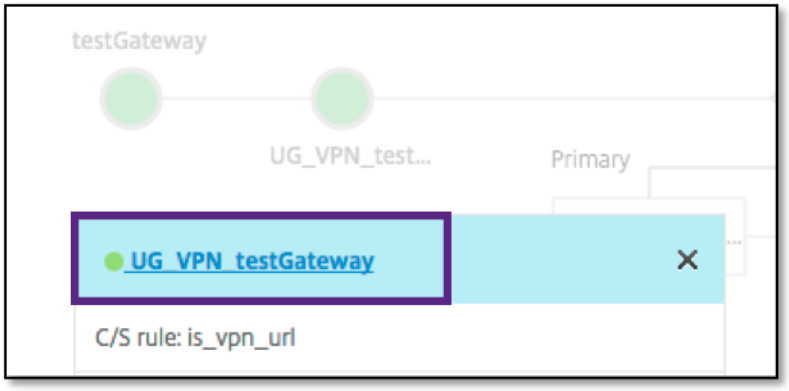



2. Haga clic en el nodo deseado para obtener detalles de las directivas ya configuradas.

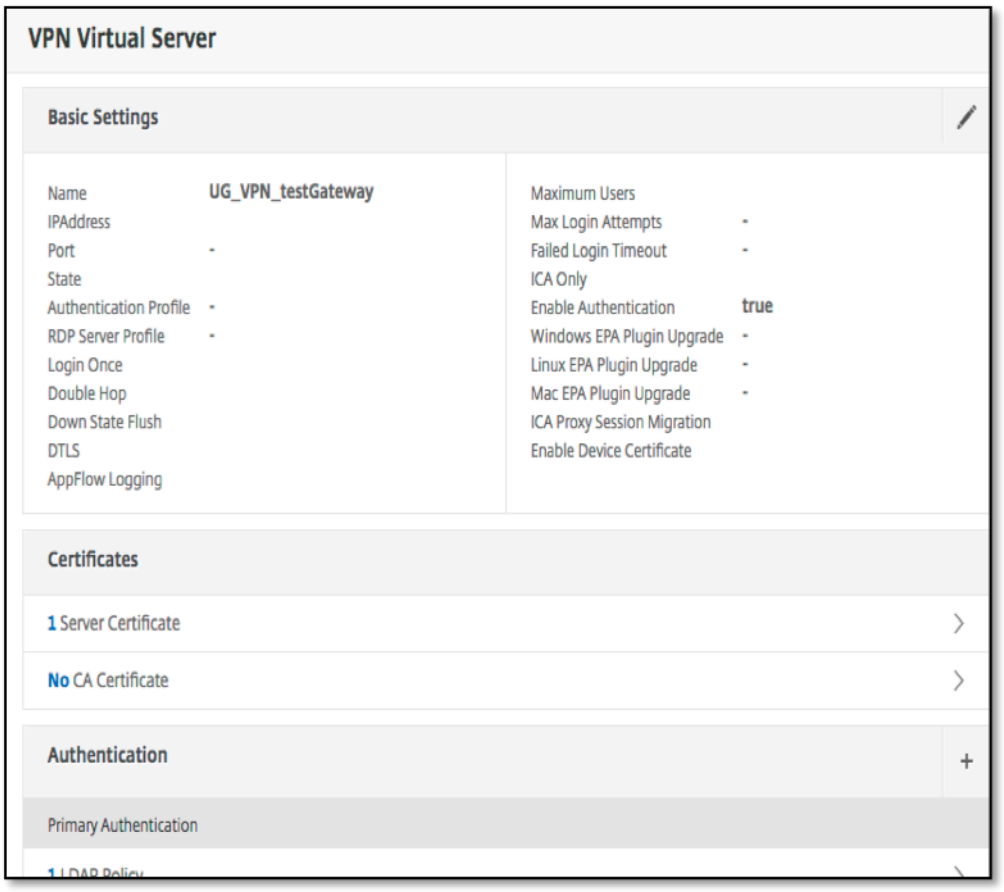



Para obtener información sobre el servidor virtual de VPN, el título de VPN en la ventana emergente es una entidad en la que se puede hacer clic y que va a un control deslizante que detalla el servidor virtual de VPN.




Los detalles del servidor VPN se muestran aquí.

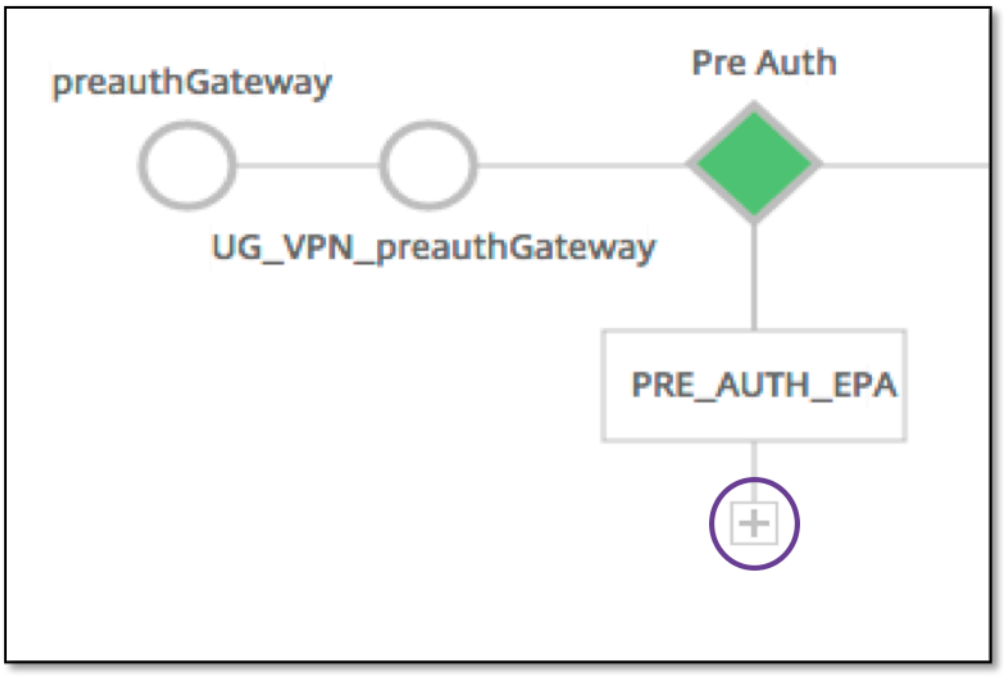



### The Pre Auth Block

Si un servidor virtual de VPN tiene directivas de autenticación previa asociadas, el visualizador de Unified Gateway muestra un bloque `Pre Auth`. El bloque `Pre Auth` muestra las directivas y ofrece una opción para agregar directivas de autenticación previa a la VPN.

1. Haga clic en el signo **+** para agregar una directiva `preauth`.



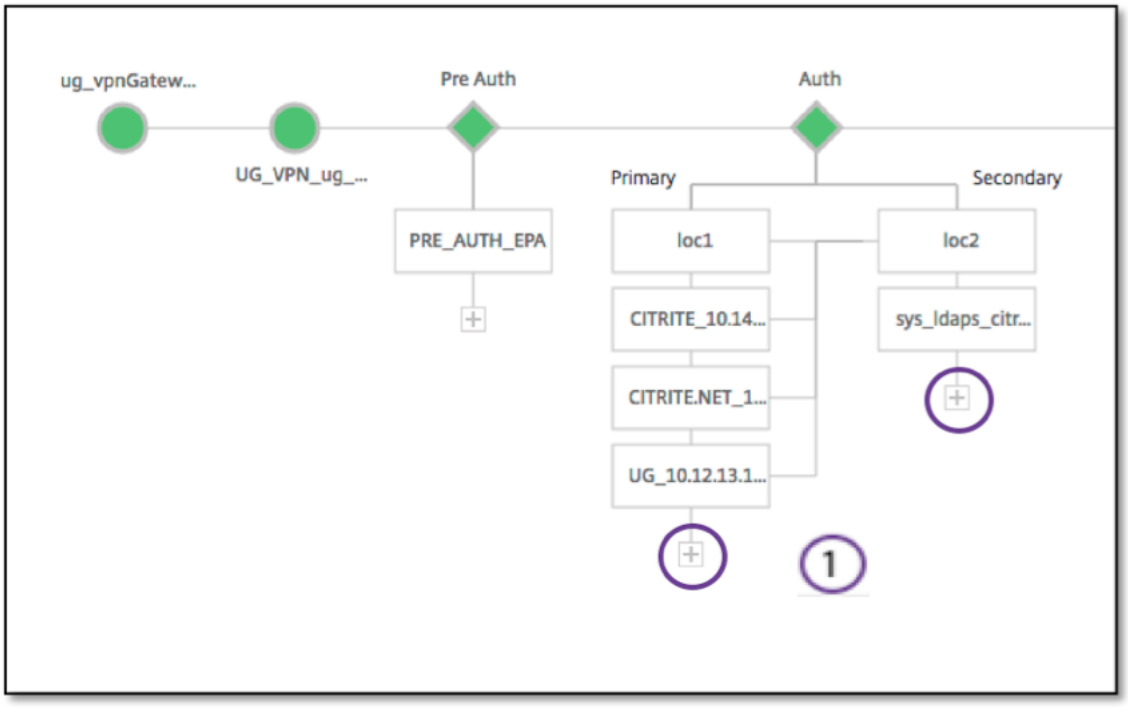

En caso de que no haya directivas de autenticación previa asociadas, este bloque se ocultaría de la vista.

### The Auth Block

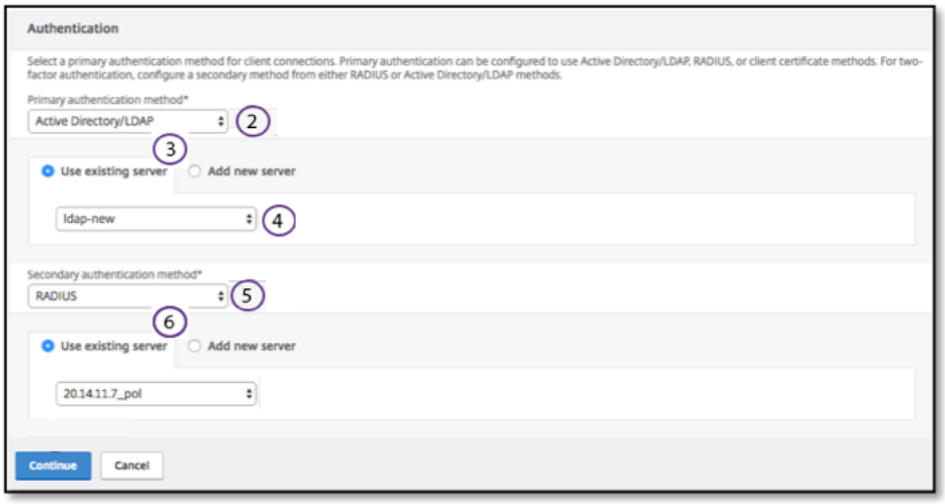
El bloque `Auth` enumera las directivas principales y secundarias. El bloque `Auth` proporciona una opción para agregar directivas.

1. Haga clic en **+** en la lista Principal para agregar un enlace de autenticación principal o haga clic en + en la lista Secundaria para agregar un enlace de autenticación secundaria.



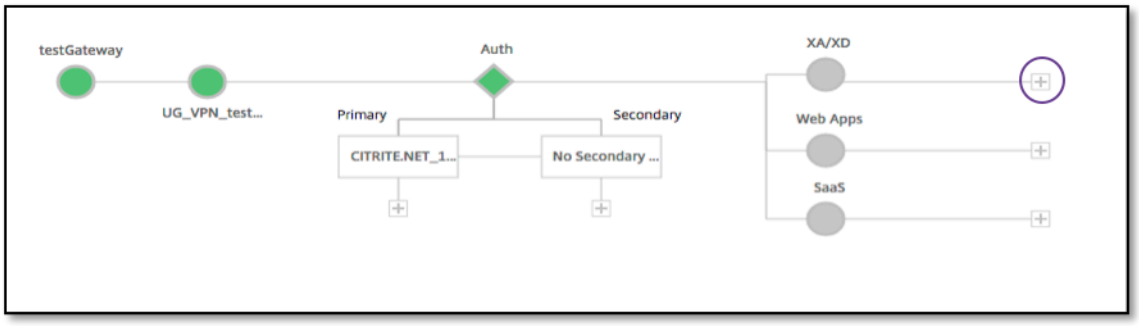

2. Seleccione una opción del menú **Método de autenticación principal**.
3. Especifique si es un **servidor existente** o **Agregar nuevo servidor** seleccionando el botón de opción.
4. Seleccione una opción del menú **Nombre de directiva LDAP**.
5. Seleccione **RADIUS** en el menú **Método de autenticación secundaria**.
6. Especifique si desea**utilizar el servidor existente** o **Agregar nuevo servidor** seleccionando el botón de opción.
7. Haga clic en **Continuar**.



### Agregar StoreFront

1. Haga clic en **+** cerca de la XA/XD y le llevará a agregar aplicaciones "XA/XD".




Puede elegir su punto de integración. Las opciones son StoreFront, WI o WionNS. Haga clic en **Continuar**.

1. Complete los siguientes campos para configurar StoreFront:

   |**Campo**|**Descripción**|
   |—|—|
   |FQDN* de StoreFront|Introduzca el FQDN del servidor de StoreFront. Longitud máxima: 255 char.Ejemplo: //storefront.xendt.net|
   |Ruta del sitio*|Introduzca la ruta de acceso a Receiver para el sitio web ya configurado en StoreFront.|
   |Dominio de inicio de sesión único*|Introduzca el dominio predeterminado para la autenticación de usuarios|
   |Nombre del almacén*|Escriba el nombre de los monitores StoreFront.
   STORENAME es un argumento que define el nombre del almacén de servicios de StoreFront para sondear el estado de los servidores StoreFront. Aplicable a monitores StoreFront. Longitud máxima: 31|
   |Servidor Secure Ticket Authority Server|*Introduzca la URL de Secure Ticket Authority, que normalmente aparece en el controlador de entrega.*
   *Ejemplo:*`http://sta`|
   |*StoreFront Server*|Introduzca la dirección IP del servidor de StoreFront |
   |Protocolo|*Introduzca el protocolo utilizado por el servidor.* |
   |*Puerto*|Introduzca el puerto utilizado por el servidor. |
   |Equilibrio de carga|Introduzca la configuración de equilibrio de carga para los servidores de StoreFront. |
   |Servidor virtual*|Introduzca la dirección IP pública para la implementación de Unified Gateway. | |

2. Haga clic en **Continuar**.

### Adición de SaaS

1. Haga clic en **+** para agregar aplicaciones SaaS y le llevará a la página Agregar SaaS. Complete los campos siguientes para configurar SaaS. Los campos que requieren información obligatoria se indican con el *.

| Campo | Descripción |
|---|---|
| Nombre* | Introduzca el nombre del enlace del marcador. |
| Tipo de aplicación | Introduzca el tipo de aplicación que representa esta URL de VPN.Los valores posibles son: Aplicación de intranet/acceso sin cliente/SaaS/aplicación preconfigurada en este NetScaler ADC |
| Introduzca la URL* | Introduzca la URL de la aplicación de intranet. |
| Elegir **archivo** | Introduzca la URL para obtener el archivo de iconos para mostrar este recurso. MaxLength = 255 |

### Incorporación de aplicaciones web

1. Haga clic en **+** para agregar aplicaciones web y le llevará a la página Agregar aplicaciones web. Complete los siguientes campos para configurar una aplicación web. Los campos que requieren información obligatoria se indican con el *.

| Campo | Descripción |
|---|---|
| Nombre* | Introduzca el nombre del enlace del marcador. |
| Tipo de aplicación | Introduzca el tipo de aplicación que representa esta URL de VPN.Los valores posibles son: Aplicación de intranet/acceso sin cliente/SaaS/aplicación preconfigurada en este NetScaler ADC |
| Introduzca la URL* | Introduzca la URL de la aplicación de intranet. |
| Elegir **archivo** | Introduzca la URL para obtener el archivo de iconos para mostrar este parámetro resource.maxLength = 255 |

Si se puede acceder a una aplicación a través de la URL de Unified Gateway, se puede acceder a los detalles del servidor de equilibrio de carga haciendo clic en la aplicación:


Se pueden agregar nuevas directivas haciendo clic en (+) y todas las directivas vinculadas se pueden ver haciendo clic en el nodo que muestra la información de la directiva.

También se muestra el número de servicios vinculados al equilibrador de carga, junto con la información general del estado. Haga clic en una lista de todos los servicios. Se pueden agregar nuevos servicios al equilibrador de carga.

Para obtener más información sobre el equilibrador de carga, se puede hacer clic en el título de la ventana emergente que llega a la página de detalles del servidor virtual de equilibrio de carga.

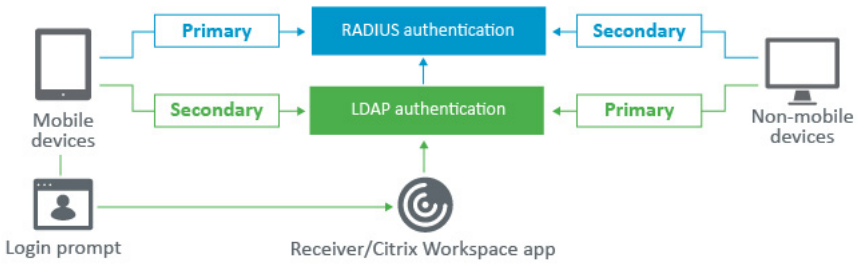
# Configurar NetScaler Gateway para utilizar la autenticación RADIUS y LDAP con dispositivos móviles/tabletas

January 26, 2024

En esta sección se describe cómo configurar el dispositivo Citrix Gateway para que utilice la autenticación RADIUS como principal y la autenticación LDAP como secundaria en dispositivos móviles o tabletas.

La configuración que se muestra en la sección permite que todas las demás conexiones utilicen primero LDAP y RADIUS en segundo lugar.

Al configurar la autenticación de dos factores en Citrix Receiver para su uso con dispositivos móviles o tabletas, debe agregar el RSA SecureID (autenticación RADIUS) como autenticación principal. Sin embargo, cuando a los usuarios se les pida el nombre de usuario y la contraseña y el código de acceso en Receiver, pondrán LDAP en primer lugar y RADIUS como segunda credencial. Desde el punto de vista del administrador, es una configuración diferente en comparación con la configuración no móvil.




Complete el siguiente procedimiento para configurar el dispositivo Citrix Gateway de modo que utilice la autenticación RADIUS como principal y la autenticación LDAP como secundaria en dispositivos móviles o tabletas.

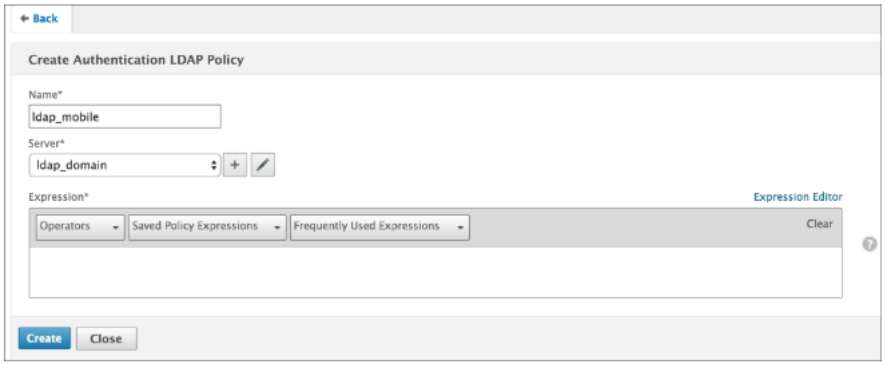
1. En la Utilidad de configuración, seleccione NetScaler Gateway > Directivas > Autenticación y cree una directiva de autenticación para LDAP y RSA para dispositivos móviles y no móviles. Esto es necesario para evitar una condición lógica que podría permitir a los usuarios eludir la autenticación RADIUS.
2. Introduzca los detalles del servidor LDAP después de hacer clic en la opción Agregar en la pestaña Servidores para LDAP.

   Para obtener más detalles sobre cómo configurar el servidor de autenticación, consulte la sección "Creación del servidor de autenticación"de Cómo configurar la autenticación LDAP en NetScaler
3. Cree una política LDAP para los dispositivos móviles seleccionando el servidor LDAP requerido.

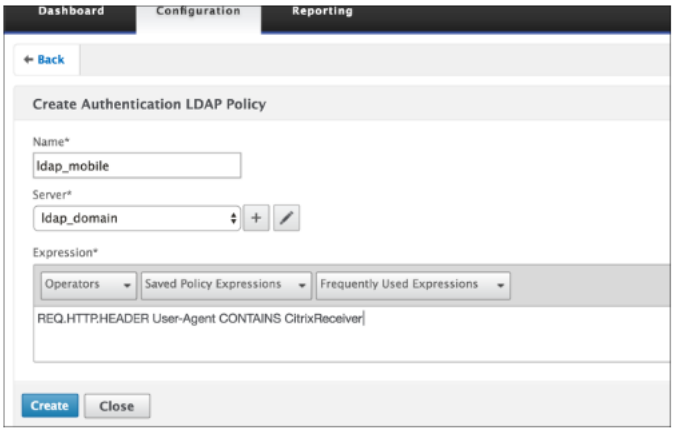
   Para vincular esta directiva solo a dispositivos móviles, utilice la siguiente expresión:

```
`REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver`
```




4. Haga clic en Editor de expresiones para crear una directiva:

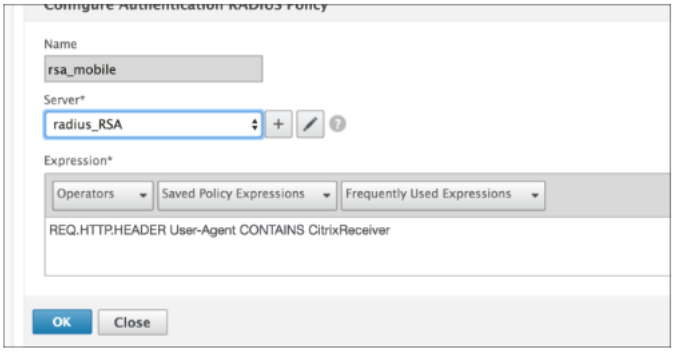

5. Cree una directiva RADIUS y un servidor RADIUS para los dispositivos móviles.

(a) Vaya a la opción RADIUS desde Citrix Gateway > Directivas > Autenticación > RADIUS. Haga clic en Agregar en la ficha Servidor.

(b) Agregue los detalles requeridos. El puerto predeterminado para la autenticación RADIUS es 1812.

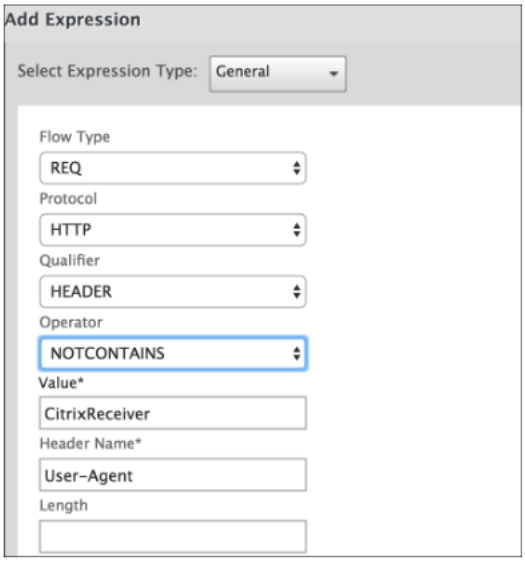

(c) Para vincular esta política solo a dispositivos móviles, utilice la siguiente expresión:

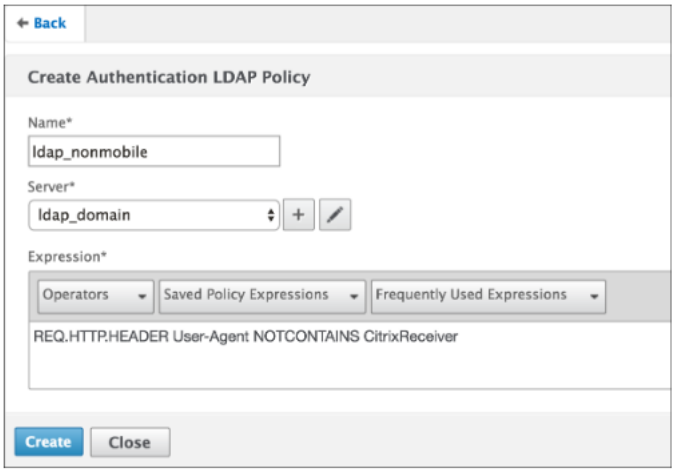



6. Siga el mismo paso para crear una directiva LDAP para dispositivos no móviles. Para vincular esta directiva solo a dispositivos no móviles, utilice la siguiente expresión:

```
1 `REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver`
```



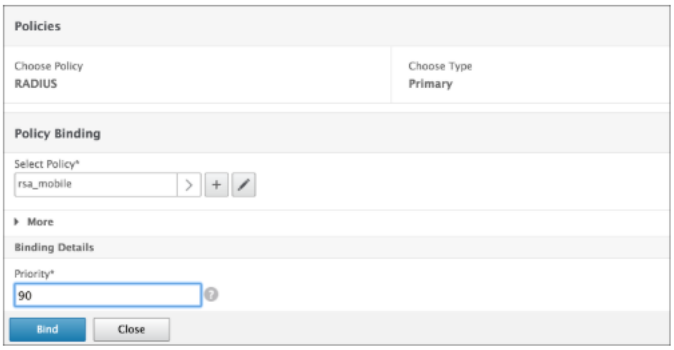



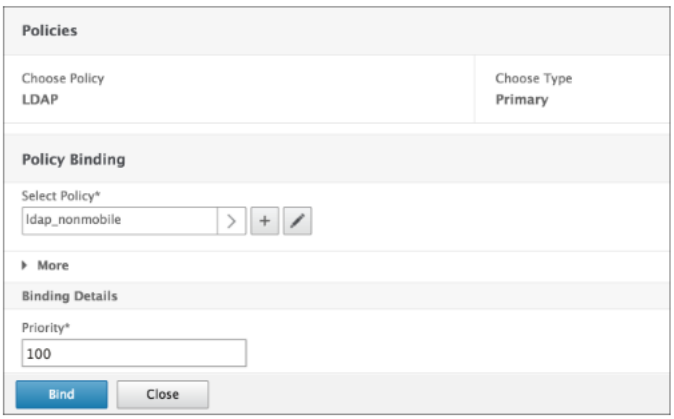

7. Cree una directiva RADIUS para dispositivos no móviles. Para vincular esta directiva solo a dispositivos no móviles, utilice la siguiente expresión:

```
`REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver`
```

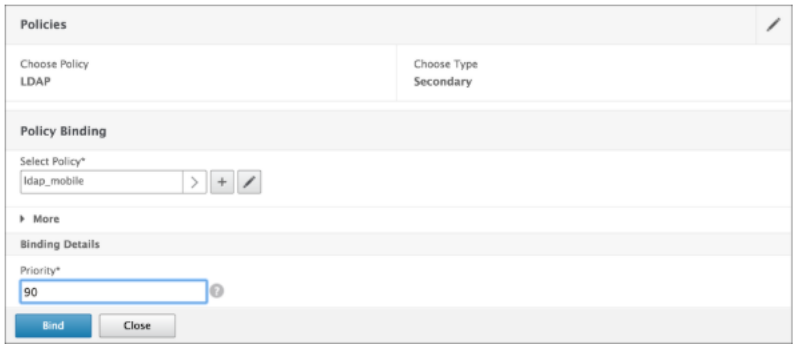

 

8. Vaya a Propiedades del servidor virtual de NetScaler Gateway y haga clic en la ficha Autenticación. En las directivas de autenticación principal, agregue la directiva RSA_mobile como prioridad máxima y la directiva LDAP_NonMobile como prioridad secundaria:




9. En las políticas de autenticación secundarias, agregue la política LDAP_Mobile como máxima prioridad, seguida de la política RSA_NonMobile como prioridad secundaria:

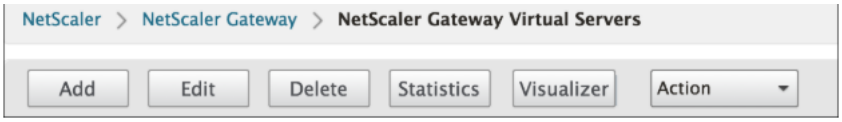


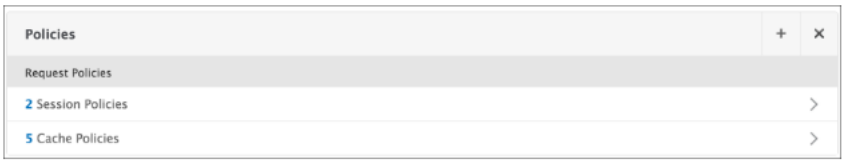

> La política de sesión debe tener el índice de credenciales de inicio de sesión único correcto, es decir, deben ser las credenciales LDAP. Para dispositivos móviles, el índice de credenciales en Perfil de sesión > Experiencia del cliente debe configurarse en Secundario, que es LDAP.

Por lo tanto, necesita dos directivas de sesión, una para dispositivos móviles y otra para dispositivos no móviles.

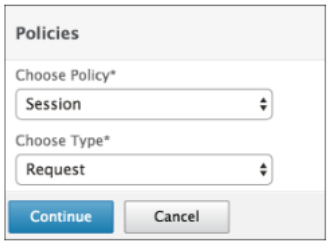
 

(a) En el caso de los dispositivos móviles, la política de sesión y el perfil de sesión tendrán el aspecto que se muestra en la siguiente captura de pantalla.
Para crear una política de sesión, navegue hasta el servidor virtual requerido y, a continuación, haga clic en Editar, vaya a la sección **Políticas** y haga clic en el signo +:




(b) Elija la opción Sesión en el menú desplegable.

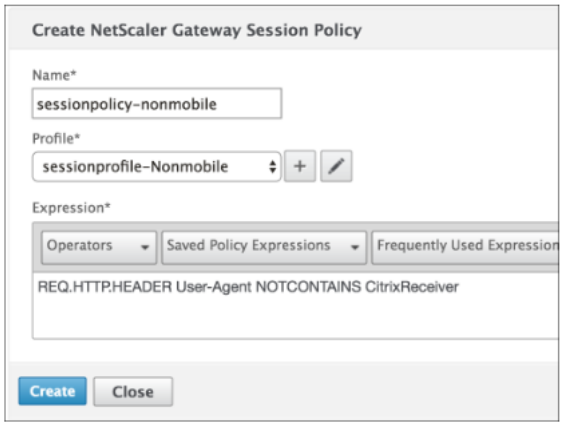



(c) Introduzca el nombre de la política de sesión que desee y haga clic en + para crear un perfil nuevo. Para dispositivos móviles, el índice de credenciales en Perfil de sesión > Experiencia del cliente debe configurarse en Secundario, que es LDAP.

(d) Para dispositivos no móviles, siga los mismos pasos. El índice de credenciales en Perfil de sesión > Experiencia del cliente debe configurarse en Principal, que es LDAP.

La expresión debe cambiarse por:

```
1 `REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver`
```

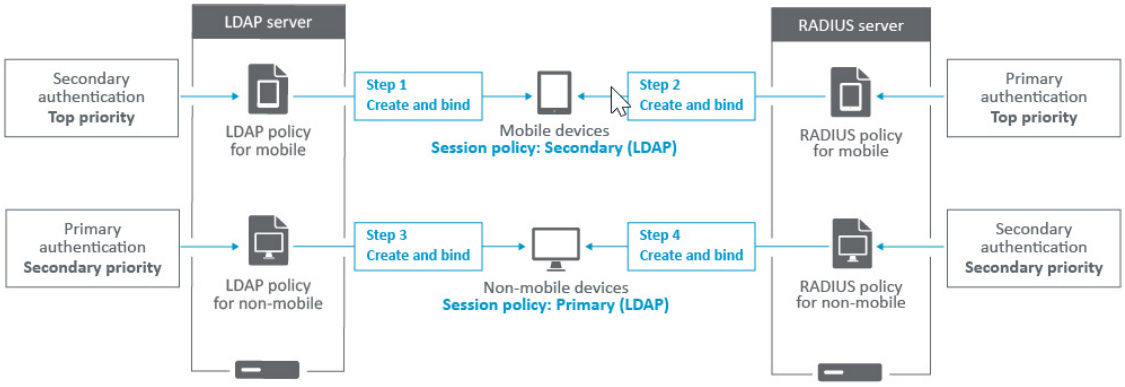


(e) Para crear un nuevo perfil para usuarios que no utilizan dispositivos móviles, haga clic en el signo +.

1. Las políticas y los perfiles del servidor virtual requerido tendrán un aspecto similar al de la siguiente captura de pantalla:
2. Además, en StoreFront, en la configuración de NetScaler Gateway establecida para usar "Tipo de inicio de sesión"= "Token de dominio y seguridad"

   imagen




## Restringir el acceso a NetScaler Gateway para los miembros de un grupo de Active Directory

March 27, 2024

NetScaler Gateway admite dos métodos para restringir el acceso de inicio de sesión.

- Filtro de búsqueda LDAP: solo los nombres de usuario que coinciden con el filtro de búsqueda LDAP (por ejemplo, pertenencia a grupos de Active Directory) pueden iniciar sesión en NetScaler Gateway.
- Grupos con permiso para iniciar sesión en un perfil o directiva de sesión de NetScaler Gateway: este método admite varios grupos de Active Directory. Para obtener información detallada, consulte https://support.citrix.com/article/CTX125797.

En este artículo se describe el método del filtro de búsqueda LDAP.

### Información general

Cuando un usuario introduce las credenciales en la página de inicio de sesión del servidor virtual de NetScaler Gateway y presiona ENTRAR, el dispositivo busca primero el nombre de usuario en Active

Directory (LDAP). Si no se ha definido un filtro de búsqueda LDAP en la directiva LDAP ni en el servidor, el dispositivo busca una coincidencia en todos los nombres de usuario de Active Directory. Una vez que se encuentra una coincidencia, el dispositivo extrae el nombre distintivo (DN) completo del usuario y utiliza el DN y la contraseña del usuario para autenticarse en Active Directory.

Si se define un filtro de búsqueda LDAP, solo se buscarán coincidencias de nombres de usuario que coincidan con el filtro de búsqueda LDAP. Por ejemplo, si el filtro de búsqueda LDAP se crea para buscar solo miembros de un grupo de Active Directory, el nombre de usuario introducido por el usuario debe coincidir con los miembros del grupo.

### Requisitos previos

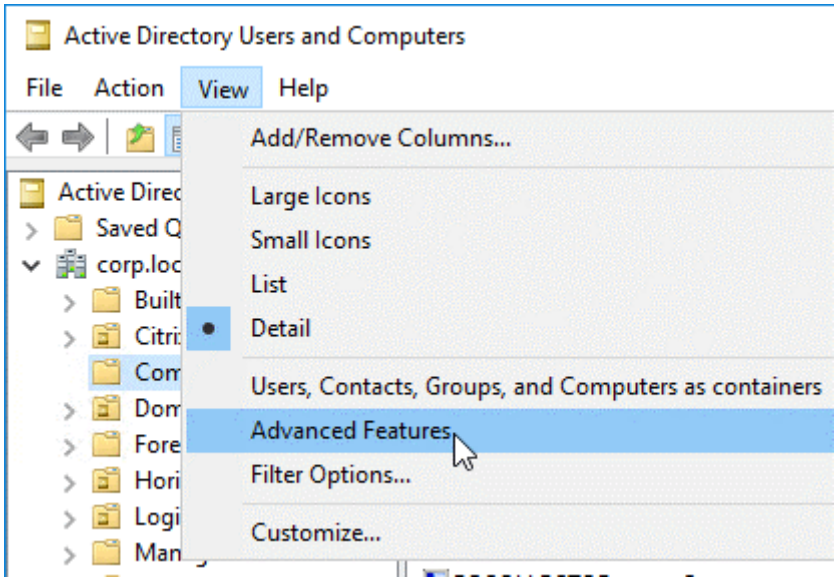
El servidor virtual NetScaler Gateway debe estar configurado para la autenticación LDAP.

### Pasos para configurar un filtro de búsqueda LDAP para los miembros de un grupo de Active Directory

1. Determine el grupo de Active Directory que tiene permiso de acceso y obtenga su nombre distintivo completo.

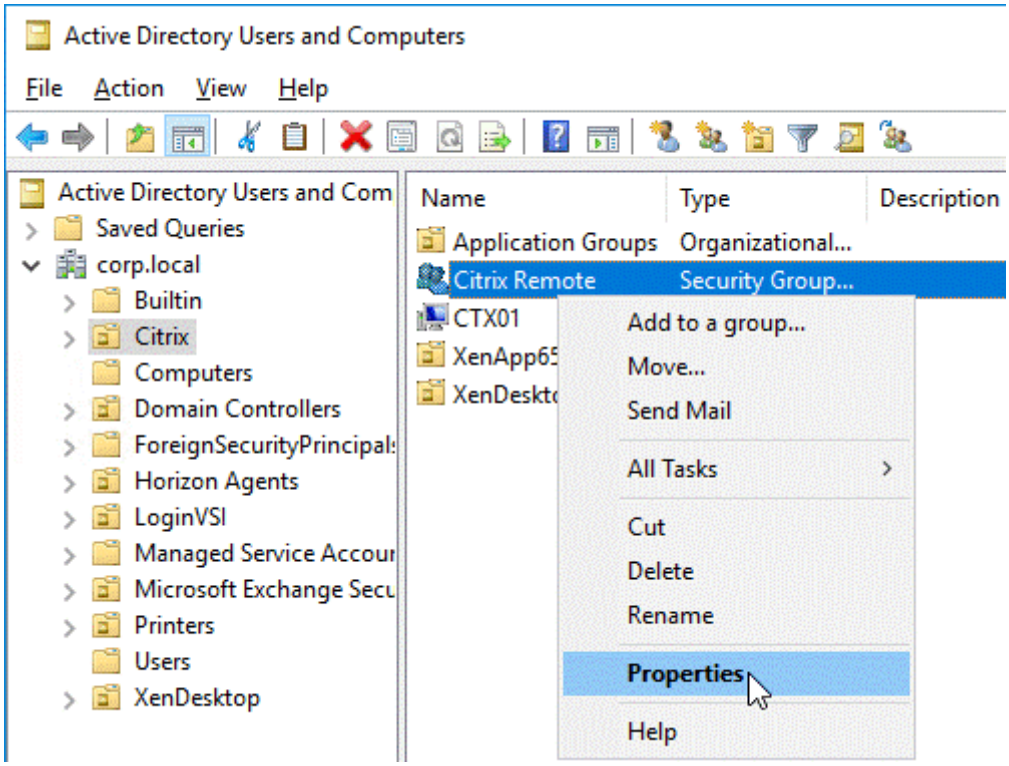
   Una forma sencilla de obtener el nombre distintivo completo del grupo es a través de Usuarios y equipos de Active Directory.

2. En Usuarios y equipos de Active Directory, en el menú **Ver**, active **Funciones avanzadas**.

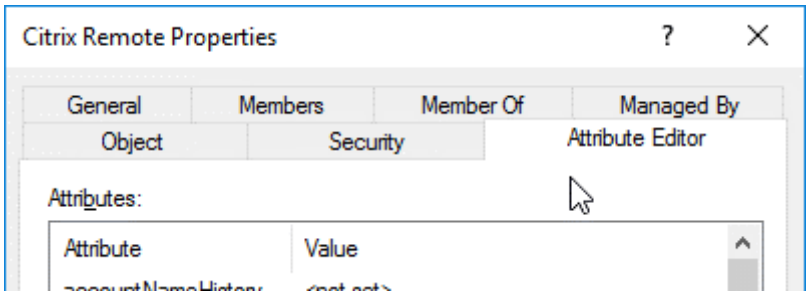



3. Examine el árbol hasta el objeto de grupo, haga clic con el botón secundario del mouse y, a continuación, haga clic en **Propiedades**.
   **Nota:** No puede usar **Buscar**. En su lugar, debe navegar por el árbol para encontrar el objeto.



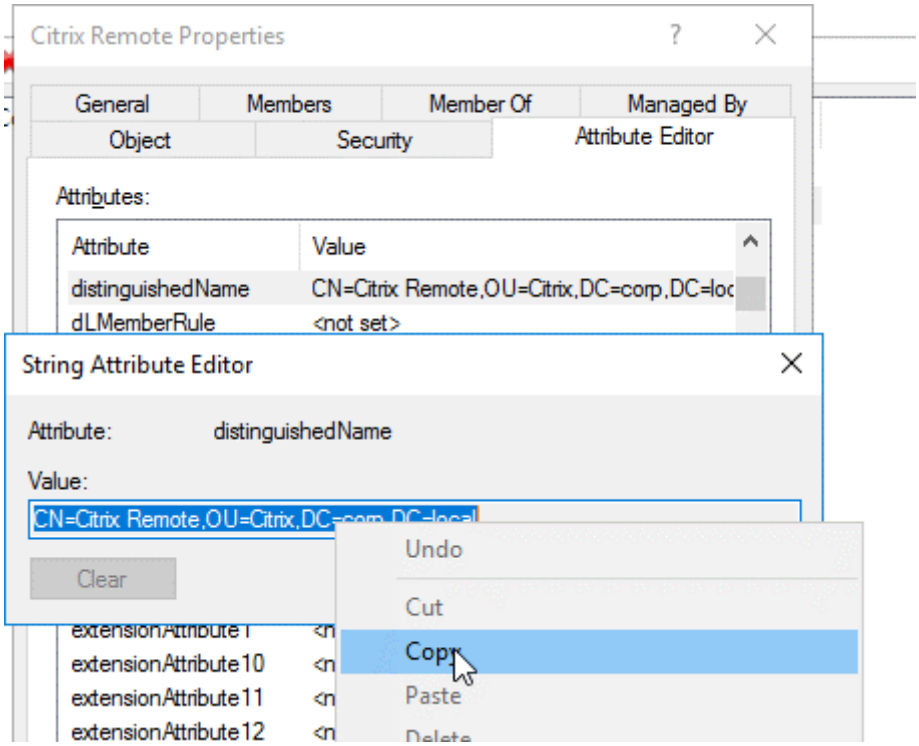

4. A la derecha, cambia a la ficha **Editor de atributos**.



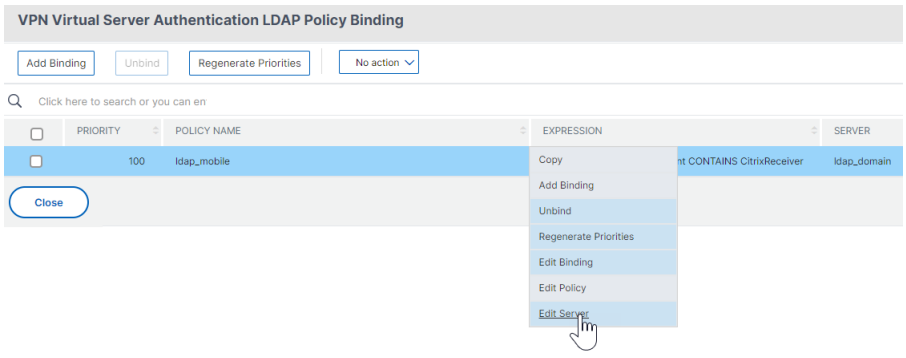

   Esta ficha solo está visible si **las funciones avanzadas** están habilitadas y si no ha utilizado la función **Buscar**.

5. Vaya hacia abajo hasta **distinguishedName**, haga doble clic en él y, a continuación, cópielo en el portapapeles.

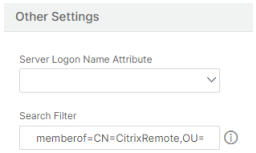
 




6. En la GUI de NetScaler Gateway, vaya a **NetScaler Gateway > Servidores virtuales**.
7. Seleccione un servidor virtual NetScaler Gateway existente y haga clic en **Modificar**.
8. En la sección Autenticación básica, haga clic en **Directivas LDAP**.
9. Haga clic con el botón secundario del mouse en una directiva LDAP existente y haga clic en **Modificar servidor**.




10. En la sección **Otros ajustes**, en el campo **Filtro de búsqueda**, escriba **memberOf=** y, a continuación, pegue el nombre distintivo del grupo de Active Directory después del signo igual (=).




Un ejemplo de filtro de búsqueda es el siguiente:

memberOf=CN=Citrix Remote, OU=Citrix, DC=corp, DC=local
**Nota:** De forma predeterminada, NetScaler solo busca nombres de usuario que sean miembros directos del grupo de Active Directory. Si quiere buscar grupos anidados, agregue Microsoft OID al filtro de búsqueda LDAP. El OID se inserta entre memberOf y =.

**Ejemplo:** memberOf:1.2.840.113556.1.4.1941:=CN=Citrix Remote, OU=Citrix, DC=corp, DC=local

11. Haga clic en **Aceptar**.

## Compatibilidad de configuración para el atributo de cookie SameSite

January 26, 2024

El atributo SameSite indica al navegador si la cookie se puede usar para el contexto entre sitios o solo para el contexto del mismo sitio. Además, si se pretende acceder a una aplicación en un contexto entre sitios, solo puede hacerlo a través de una conexión HTTPS. Para obtener más información, consulte RFC6265.

Hasta febrero de 2020, el atributo SameSite no estaba establecido explícitamente en Citrix ADC. El explorador tomó el valor predeterminado (Ninguno). La no configuración del atributo SameSite no afectó a las implementaciones AAA de Citrix Gateway y Citrix ADC.

Con la actualización de ciertos exploradores, como Google Chrome 80, se produce un cambio en el comportamiento predeterminado entre dominios de las cookies. El atributo SameSite se puede establecer en uno de los siguientes valores. El valor predeterminado para Google Chrome se establece en Lax. Para ciertas versiones de otros navegadores, es posible que el valor predeterminado del atributo SameSite siga siendo Ninguno.

- **Ninguno**: indica que el explorador debe utilizar cookie en contexto entre sitios solo en conexiones seguras.
- **Lax**: indica que el navegador debe usar cookies para las solicitudes en el contexto del mismo sitio. En el contexto entre sitios, solo los métodos HTTP seguros, como la solicitud GET, pueden usar la cookie.
- **Estricto**: utiliza la cookie solo en el mismo contexto del sitio.

Si no hay ningún atributo SameSite en la cookie, Google Chrome asume la funcionalidad de SameSite = Lax.
Como resultado, para las implementaciones dentro de un iframe con contexto entre sitios que requieren que el explorador inserte cookies, Google Chrome no comparte cookies entre sitios. Como resultado, es posible que el iframe del sitio web no se cargue.

## Configurar el atributo de cookie SameSite

Se agrega un nuevo atributo de cookie denominado SameSite a los servidores virtuales AAA de Citrix ADC y VPN. Este atributo se puede establecer a nivel global y a nivel de servidor virtual.

Para configurar el atributo SameSite, debe realizar lo siguiente:

1. Establecer el atributo SameSite para el servidor virtual
2. Enlazar las cookies al conjunto de patentes (si el navegador descarta, las cookies entre sitios, el navegador descarta las cookies de varios sitios)

### Configuración del atributo SameSite mediante la CLI

Para establecer el atributo SameSite en el nivel del servidor virtual, utilice los siguientes comandos.

```
set vpn vserver VP1 -SameSite  [ STRICT | LAX | None ]
set aaa vserver VP1 -SameSite  [ STRICT | LAX | None ]
<!--NeedCopy-->
```

Para establecer el atributo SameSite a nivel global, utilice los siguientes comandos.

```
set vpn param VP1 -SameSite  [ STRICT | LAX | None ]
set aaa param VP1 -SameSite  [ STRICT | LAX | None ]
<!--NeedCopy-->
```

**Nota**: La configuración del nivel del servidor virtual tiene preferencia sobre la configuración de nivel global. Citrix recomienda configurar el atributo de cookie SameSite en el nivel del servidor virtual.

### Enlazar cookies al patset mediante la CLI

Si el explorador descarta las cookies entre sitios, puede vincular esa cadena de cookie al conjunto de parches NS_Cookies_SameSite existente para que se agregue el atributo SameSite a la cookie.

**Ejemplo:**

```
bind patset ns_cookies_SameSite "NSC_TASS"
bind patset ns_cookies_SameSite "NSC_TMAS"
<!--NeedCopy-->
```

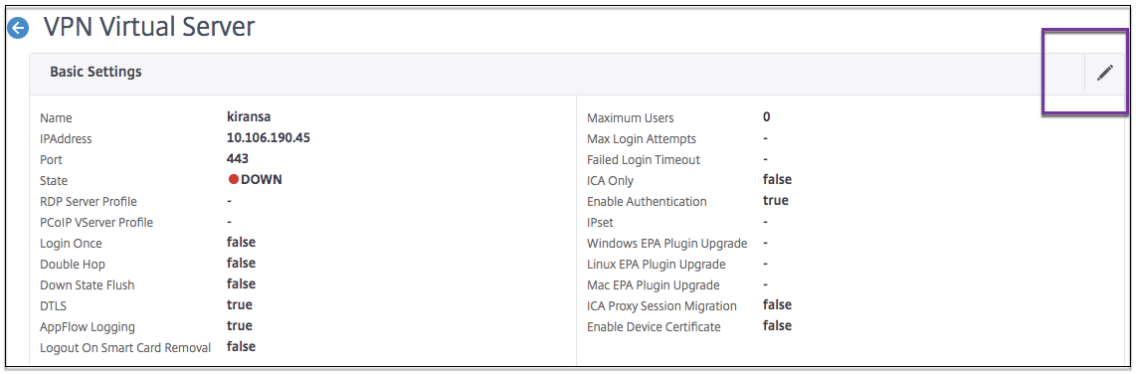
### Configuración del atributo sameSite mediante la interfaz gráfica de usuario

**Para establecer el atributo SameSite en el nivel del servidor virtual:**

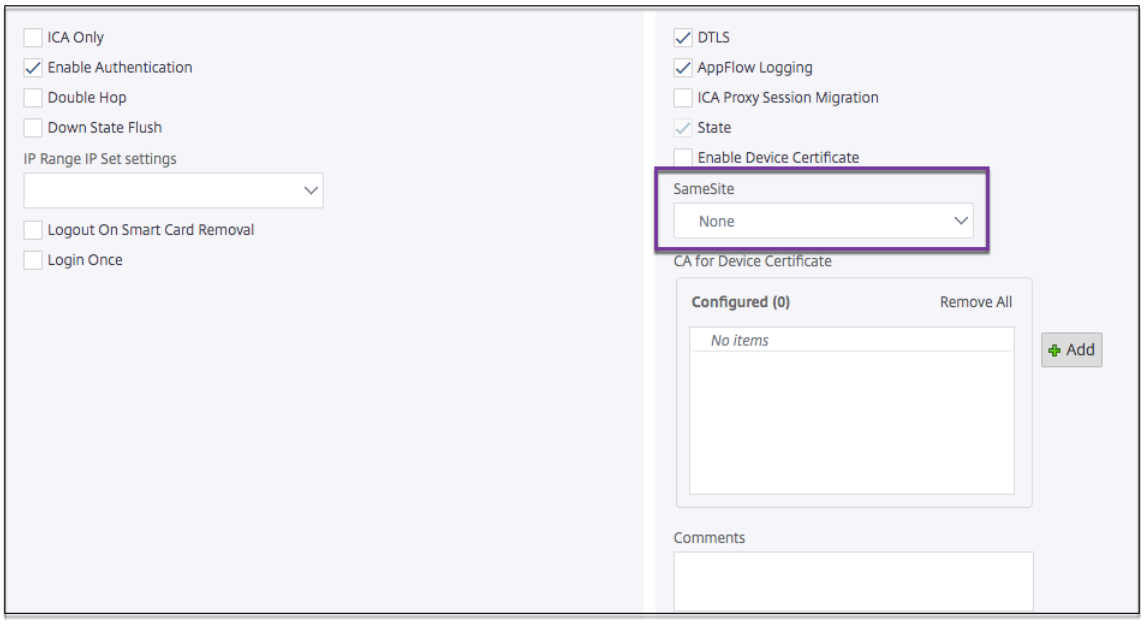
1. Vaya a **NetScaler Gateway > Servidores virtuales**.
2. Seleccione un servidor virtual y haga clic en **Modificar**.

3. Selecciona el icono de modificación en la sección **Configuración básica** y haga clic en **Más**.



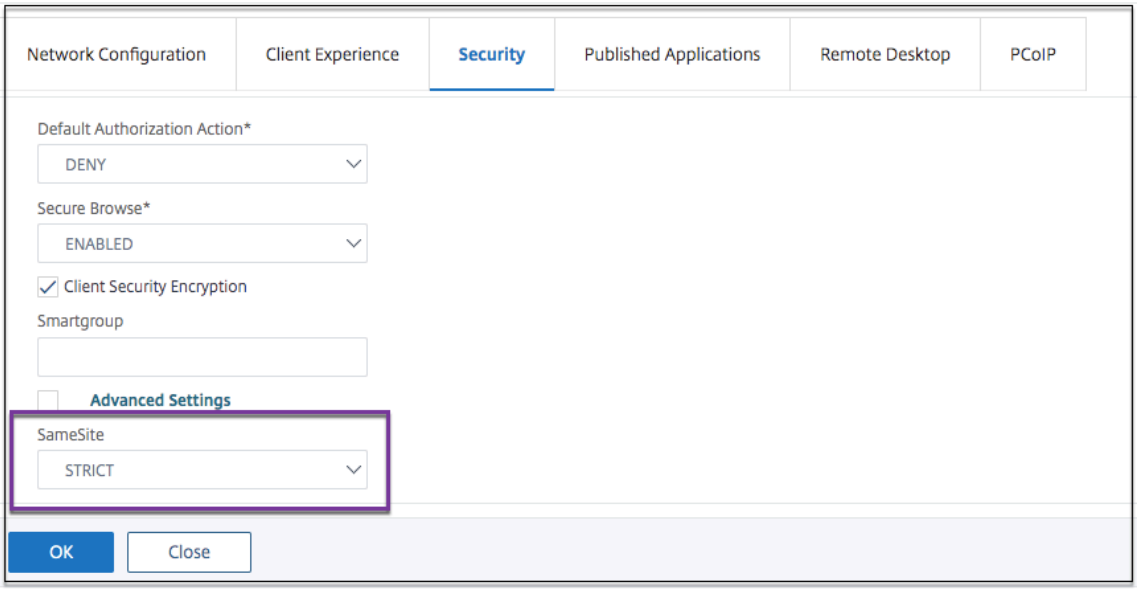

4. En **SameSite**, seleccione la opción según sea necesario.




**Para establecer el atributo SameSite a nivel global:**

1. Vaya a **Citrix Gateway > Configuración global > Cambiar configuración global.**
2. Haga clic en la ficha **Seguridad**.
3. En **SameSite**, seleccione la opción según sea necesario.




## Optimización del túnel dividido VPN de NetScaler Gateway para Office365

March 27, 2024

Dado que las organizaciones se están adaptando a las opciones de trabajo remoto con mayor rapidez que antes, la infraestructura de acceso remoto debe optimizarse para facilitar una conectividad perfecta durante condiciones de mayor carga de tráfico.

*Microsoft recomienda excluir el tráfico destinado a los servicios clave de Office 365 del alcance de la conexión VPN mediante la configuración de túneles divididos con los intervalos de direcciones IPv4 e IPv6 publicados. Para obtener el mejor rendimiento y un uso más eficiente de la capacidad de la VPN, el tráfico a estos rangos de direcciones IP dedicadas asociados a Office 365 Exchange Online, SharePoint Online y Microsoft Teams (denominados categoría Optimizar en la documentación de Microsoft) se debe enrutar directamente, fuera del túnel VPN. Consulte [Guía de Microsoft] https://docs.microsoft.com/en-us/Office365/Enterprise/office-365-vpn-split-tunnelpara obtener información más detallada sobre esta recomendación.*

La recomendación de Microsoft en NetScaler Gateway se logra mediante la redirección de la lista de direcciones IP proporcionada por Microsoft directamente a Internet para el tráfico de O365 mediante la configuración inversa del túnel dividido.

La configuración incluye lo siguiente que se puede realizar manualmente mediante los comandos **GUI o CLI**.

- Configurar túnel dividido para configuración inversa

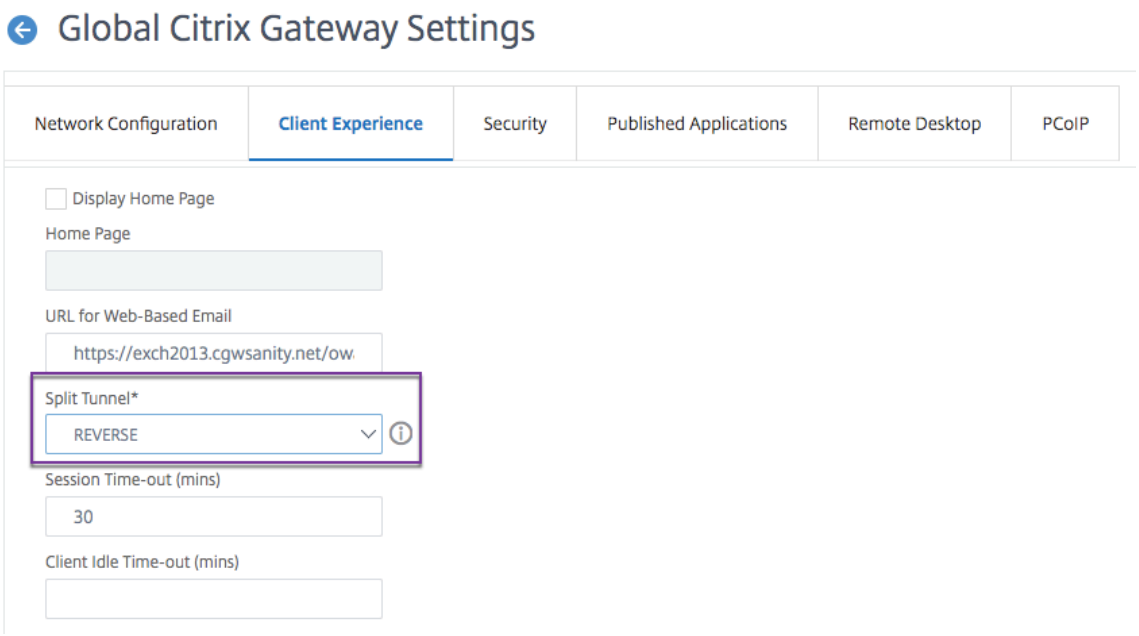
 

- Configurar aplicaciones de intranet para el acceso de los usuarios a los recursos

## Configuración mediante la interfaz gráfica de usuario

### Para configurar la tunelización dividida mediante la interfaz gráfica de usuario

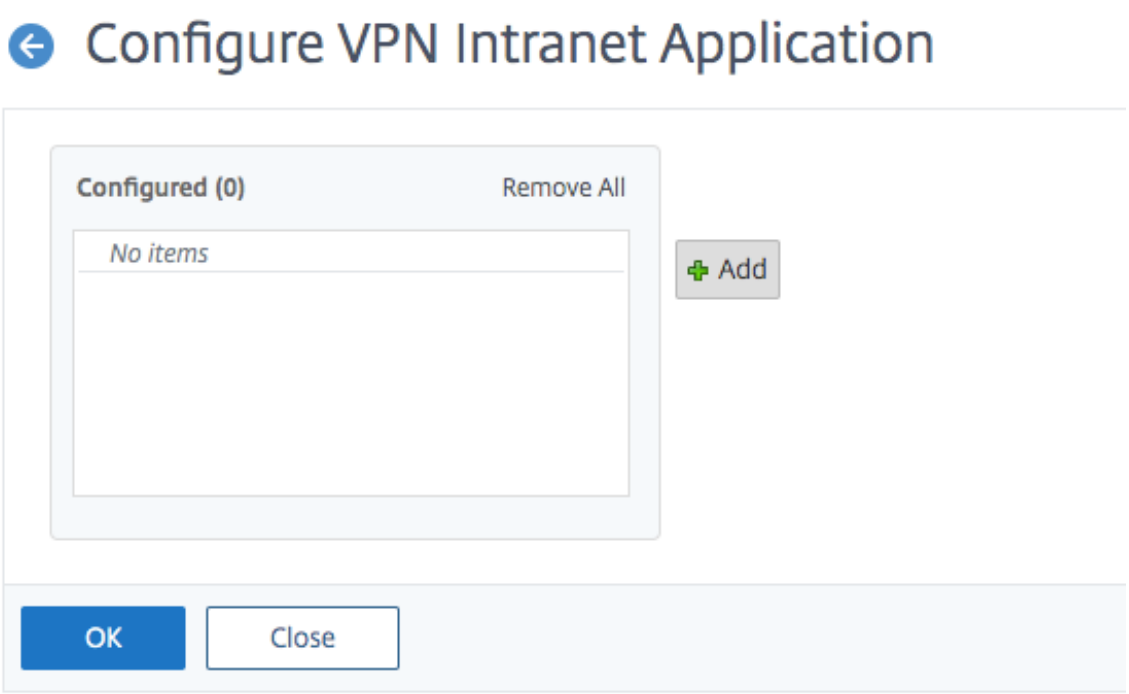
1. En la pestaña Configuración, vaya a **Citrix Gateway > Configuración global** .
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar configuración global**.
3. En la ficha **Experiencia del cliente**, en **Túnel dividido**, seleccione **Revertir**.
4. Haga clic en **Aceptar**.

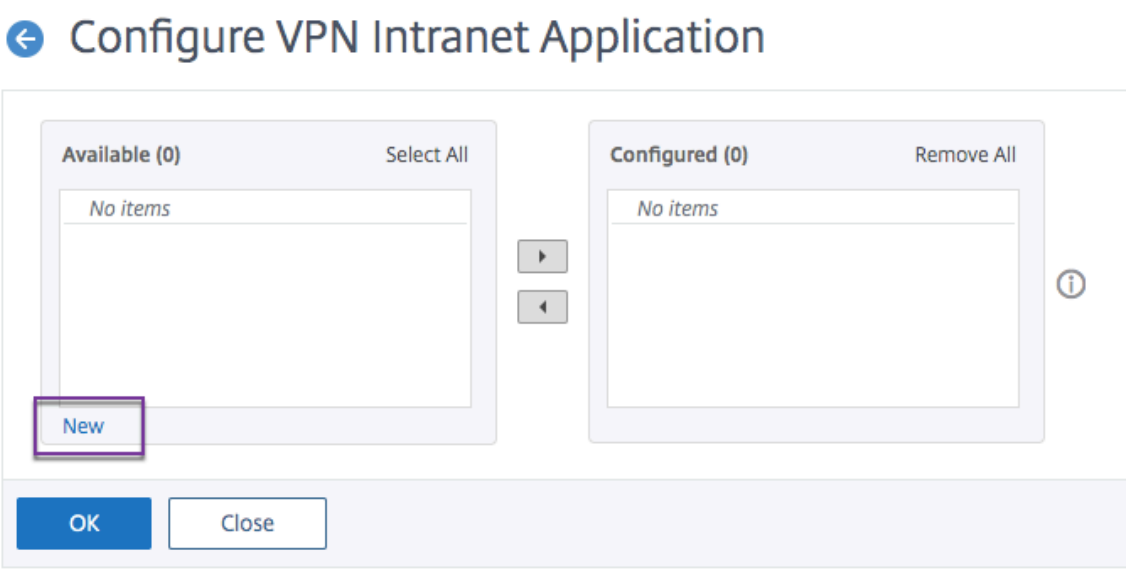



### Para crear una aplicación de intranet VPN mediante la GUI

1. En la ficha Configuración, vaya a**Citrix Gateway > Configuración global**.
2. En el panel de detalles, en **Aplicaciones de intranet**, haga clic en el enlace.
3. En la página **Configurar aplicación de intranet VPN**, haga clic en **Agregar** y, a continuación, en **Nueva**.

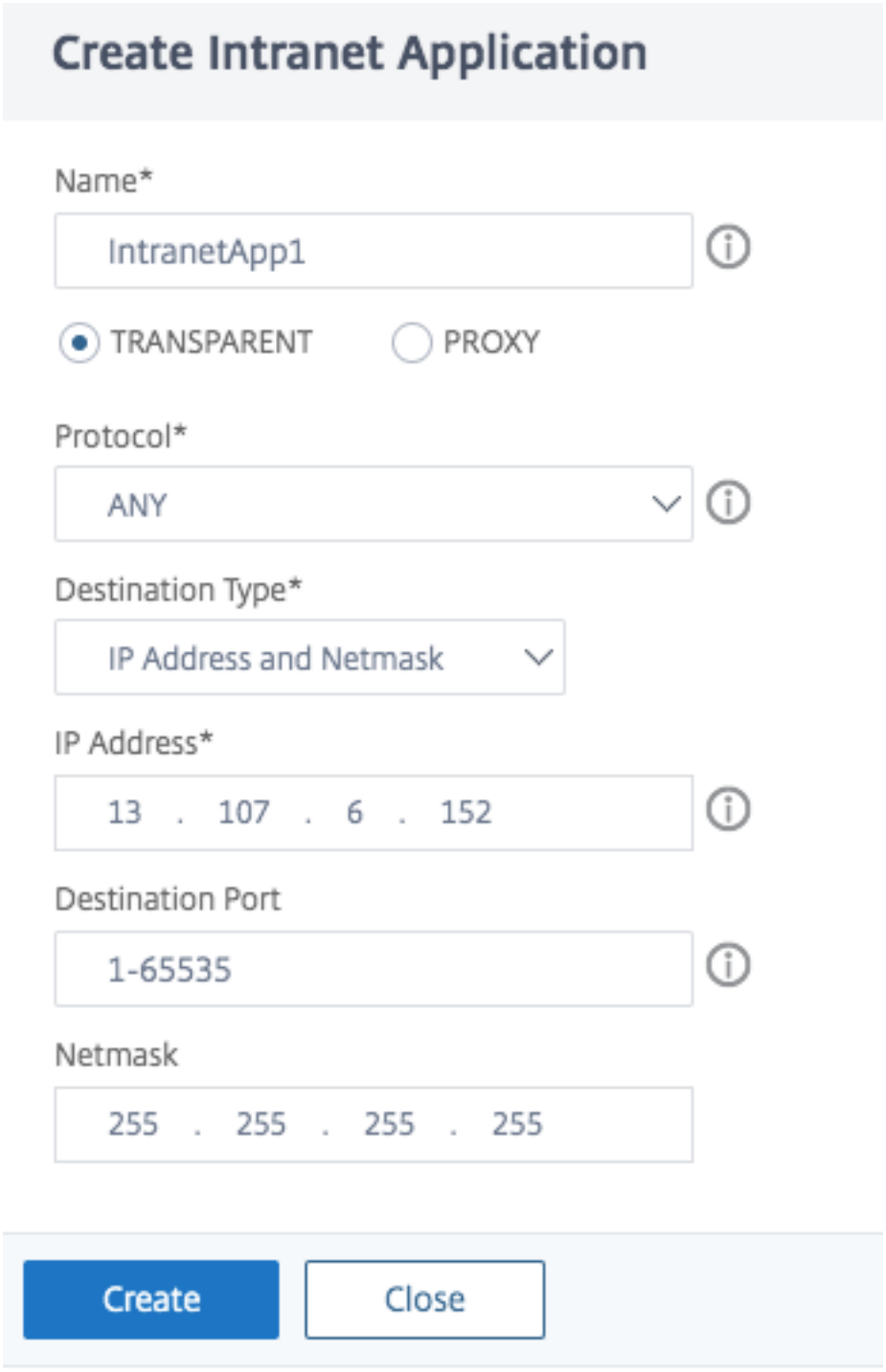
 




4. En **Nombre**, escriba un nombre para el perfil.
5. En **Protocolo**, seleccione el protocolo que se aplica al recurso de red.
6. En **Tipo de destino**, seleccione **Dirección IP y máscara de red**.
7. En **Dirección IP**, introduzca la dirección IP que debe redirigirse directamente a Internet para el tráfico de O365. Para obtener la lista de direcciones IP, consulte Lista de direcciones IP.
8. En **Máscara de red**, introduzca la dirección IP de la máscara de red.




9. Haga clic en **Create** y, luego, en **Close**.

**Nota:** Repita este procedimiento para todas las direcciones IP.

### Configuración mediante la CLI

- Para configurar el túnel dividido para que se invierta, en el símbolo del sistema, escriba;

```
set vpn parameter -splitTunnel REVERSE
<!--NeedCopy-->
```

- Para agregar una aplicación de intranet VPN, en el símbolo del sistema, escriba;

```
add vpn intranetApplication intranetapp1 ANY 13.107.6.152 -netmask
   255.255.255.254 -destPort 1-65535 -interception TRANSPARENT
<!--NeedCopy-->
```

**Nota:** Repita este procedimiento para todas las direcciones IP.

- Para enlazar la aplicación de intranet, en el símbolo del sistema, escriba;

```
bind vpn global -intranetApplication intranetapp1
<!--NeedCopy-->
```

### Lista de direcciones IP de los servicios de Office 365 (EXO, SPO y Teams)

Referencia: https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges

**Nota de Microsoft:**
*Como parte de la respuesta de Microsoft a la situación de la COVID-19, Microsoft ha declarado una moratoria temporal sobre algunos cambios de URL y direcciones IP planificados. Esta moratoria tiene por objeto proporcionar a los equipos de TI de los clientes confianza y simplicidad a la hora de implementar las optimizaciones de red recomendadas para los casos de Office 365 de trabajo desde casa. Desde el 24 de marzo de 2020 hasta el 30 de junio de 2020, esta moratoria detendrá los cambios de los servicios clave de Office 365 (Exchange Online, SharePoint Online y Microsoft Teams) en los rangos de IP y las URL incluidas en la categoría Optimize.*

#### Intervalo de direcciones IPv4

104.146.128.0/17
13.107.128.0/22
13.107.136.0/22
13.107.18.10/31
13.107.6.152/31
13.107.64.0/18
131.253.33.215/32
132.245.0.0/16

150.171.32.0/22
150.171.40.0/22
191.234.140.0/22
204.79.197.215/32
23.103.160.0/20
40.104.0.0/15
40.108.128.0/17
40.96.0.0/13
52.104.0.0/14
52.112.0.0/14
52.96.0.0/14
52.120.0.0/14

**Intervalo de direcciones IPv6**

2603:1006: :/40
2603:1016: :/36
2603:1026: :/36
2603:1036: :/
36
2603:1046: :/36
2603:1096: :/38
2603:1096:400: :/40
2603:1096:600: :/40
2603:1096:a00: :/39
2603:1096:c00: :/40
2603:10 a 6:200: :/40
2603:10 a 6:400: :/
40
2603:10 a 6:600: :/40
2603:10 a 6:800: :/40
2603:10 d 6:200: :/40
2620:1 ec:4:152/128
2620:1 ec:4:153/128
26201 ec:10/128 262:201 ec:11/128
262:01 ecd:10/128
262:01 ec:11/128
262:01 ec:8f0: :/46
262:01 ec:900:/46

2620:1 ec:29:152/128
262:01 ec:92:153/128
2a 01:111:f400: :/48
2620:1 ec:8f8: :/46
2620:1 ec:908: :/46
2a 01:111:f402: :/48

## Configurar la experiencia de usuario VPN

January 26, 2024

> **Importante:**
>
> Las capturas de pantalla de esta sección se mantienen en escala de grises por los siguientes motivos:
>
> - Ayude a los lectores con discapacidad visual, especialmente a aquellos con daltonismo o deficiencia de color.
> - El uso de una imagen en escala de grises representa la imagen de forma genérica que no muestra ningún impacto en la personalización del código de colores que podría haberse realizado en el explorador del usuario o en el sistema operativo.

Los usuarios pueden utilizar los siguientes métodos para conectarse a los recursos de red de la organización a través de Citrix Gateway:

- Citrix Receiver que contiene todos los complementos de Citrix instalados en el dispositivo del usuario.
- Receiver para Web que permite a los usuarios conectarse a aplicaciones, escritorios y ShareFile mediante un explorador web.
- Secure Hub para permitir a los usuarios acceder a Secure Mail, WorxWeb y aplicaciones móviles desde sus dispositivos iOS y Android.
- Plug-in de NetScaler Gateway para Windows, macOS X o Linux.
- Aplicación Citrix Gateway para iOS y Android.
- Plug-in de NetScaler Gateway para Java.
- Acceso sin cliente que proporciona a los usuarios el acceso que necesitan sin instalar software de usuario.
- Interoperabilidad con el complemento Citrix SD-WAN.

Si los usuarios instalan el plug-in de NetScaler Gateway y, a continuación, instalan Receiver desde Citrix Virtual Apps 6.5 para Windows Server 2008 (incluidos Feature Pack y Feature Pack 2), Citrix Virtual Desktops 7.0 o posterior, Receiver agrega automáticamente el plug-in de NetScaler Gateway. Los

usuarios pueden conectarse con el plug-in de NetScaler Gateway desde un explorador Web o desde Receiver.

SmartAccess determina automáticamente los métodos de acceso permitidos para un dispositivo de usuario en función de los resultados de un análisis de puntos finales. Para obtener más información sobre SmartAccess, consulte Configuración de SmartAccess.

Citrix Gateway admite las aplicaciones Citrix Endpoint Management Worx para dispositivos móviles iOS y Android. Citrix Gateway contiene Secure Browse, que permite las conexiones a Citrix Gateway desde dispositivos móviles iOS que establecen el túnel Micro VPN. Los dispositivos Android que se conectan con Secure Hub también establecen automáticamente un túnel micro VPN que proporciona un acceso seguro a nivel de aplicación web y móvil a los recursos de su red interna. Si los usuarios se conectan desde un dispositivo Android con aplicaciones Worx, debe configurar los parámetros de DNS en Citrix Gateway. Para obtener más información, consulte el tema Cómo admitir consultas de DNS mediante sufijos de DNS para dispositivos Android .

## Cómo funcionan las conexiones de usuario con el plug-in de NetScaler Gateway

January 26, 2024

NetScaler Gateway funciona de la siguiente manera:

- Cuando los usuarios intentan acceder a los recursos de red a través del túnel VPN, el plug-in de NetScaler Gateway cifra todo el tráfico de red destinado a la red interna de la organización y reenvía los paquetes a NetScaler Gateway.
- NetScaler Gateway finaliza el túnel SSL, acepta cualquier tráfico entrante destinado a la red privada y reenvía el tráfico a la red privada. NetScaler Gateway devuelve el tráfico al equipo remoto a través de un túnel seguro.

Cuando los usuarios escriben la dirección web, reciben una página de inicio de sesión en la que introducen sus credenciales e inician sesión. Si las credenciales son correctas, NetScaler Gateway finaliza el enlace con el dispositivo del usuario.

Si el usuario se conecta a través de un servidor proxy, puede especificar tanto el servidor proxy como las credenciales de autenticación. Para obtener más información, consulte Habilitación de la compatibilidad con proxy para conexiones de usuario.

El plug-in de NetScaler Gateway se instala en el dispositivo del usuario. Tras la primera conexión, si los usuarios inician sesión con un equipo basado en Windows, pueden usar el icono del área de notificación para establecer la conexión.

# Establecer el túnel seguro

January 26, 2024

Cuando los usuarios se conectan con el plug-in de NetScaler Gateway, Secure Hub o Citrix Receiver, el software cliente establece un túnel seguro a través del puerto 443 (o cualquier puerto configurado en NetScaler Gateway) y envía información de autenticación. Cuando se establece el túnel, NetScaler Gateway envía información de configuración al plug-in de NetScaler Gateway, Secure Hub o Receiver, describiendo las redes que se van a proteger y que contiene una dirección IP si habilita grupos de direcciones.

## Tunelización del tráfico de redes privadas a través de conexiones seguras

Cuando se inicia el plug-in de NetScaler Gateway y el usuario se autentica, todo el tráfico de red destinado a redes privadas especificadas se captura y se redirige a través del túnel seguro a NetScaler Gateway. Receiver debe admitir el plug-in de NetScaler Gateway para establecer la conexión a través del túnel seguro cuando los usuarios inician sesión.

Secure Hub, Secure Mail y WorxWeb utilizan Micro VPN para establecer el túnel seguro para dispositivos móviles iOS y Android.

NetScaler Gateway intercepta todas las conexiones de red que realiza el dispositivo del usuario y las multiplexa a través de Secure Sockets Layer (SSL) a NetScaler Gateway, donde el tráfico se demultiplexa y las conexiones se reenvían a la combinación correcta de host y puerto.

Las conexiones están sujetas a directivas de seguridad administrativas que se aplican a una única aplicación, a un subconjunto de aplicaciones o a toda una intranet. Especifica los recursos (intervalos de pares de direcciones IP/subred) a los que los usuarios remotos pueden acceder a través de la conexión VPN.

El plug-in de NetScaler Gateway intercepta y tunea los siguientes protocolos para las aplicaciones de intranet definidas:

- TCP (todos los puertos)
- UDP (todos los puertos)
- ICMP (tipos 8 y 0 - solicitud/respuesta de eco)

Las conexiones de las aplicaciones locales del dispositivo del usuario se tunelizan de forma segura a NetScaler Gateway, que restablece las conexiones con el servidor de destino. Los servidores de destino consideran que las conexiones se originan en el NetScaler Gateway local de la red privada, ocultando así el dispositivo del usuario. Esto también se denomina traducción inversa de direcciones de red (NAT). Ocultar direcciones IP agrega seguridad a las ubicaciones de origen.

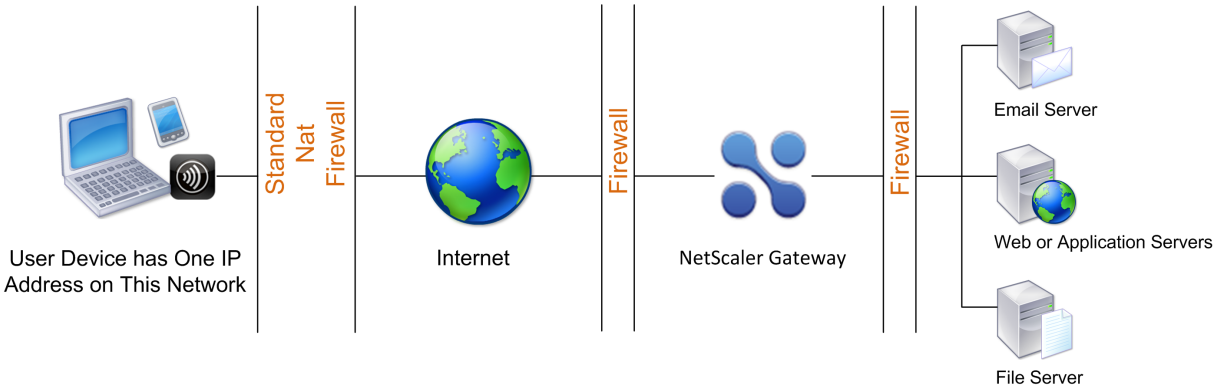
Localmente, en el dispositivo del usuario, el plug-in de NetScaler Gateway vuelve a crear todo el tráfico relacionado con la conexión, como paquetes SYN-ACK, PUSH, ACK y FIN, para que aparezca desde el servidor privado.

## Funcionamiento a través de firewalls

January 26, 2024

Los usuarios del plug-in de NetScaler Gateway se encuentran a veces dentro del firewall de otra organización, como se muestra en la siguiente ilustración:

Figura 1. Conexión desde el dispositivo del usuario a través de dos firewalls internos




Los firewalls NAT mantienen una tabla que les permite redirigir paquetes seguros desde NetScaler Gateway de vuelta al dispositivo del usuario. Para las conexiones orientadas a circuitos, NetScaler Gateway mantiene una tabla de traducción NAT inversa asignada a puertos. La tabla de traducción NAT inversa permite a NetScaler Gateway hacer coincidir las conexiones y enviar paquetes de vuelta por el túnel al dispositivo de usuario con los números de puerto correctos para que los paquetes regresen a la aplicación correcta.

## Control de actualización del plug-in de NetScaler Gateway

March 27, 2024

Los administradores del sistema controlan el rendimiento del plug-in de NetScaler ADC cuando su versión no coincide con la revisión de NetScaler Gateway. Las nuevas opciones controlan el comportamiento de actualización de plug-ins para Mac y Windows o sistemas operativos.

En el caso de los plug-ins VPN, la opción de actualización se puede establecer en dos lugares de la interfaz de usuario del dispositivo NetScaler ADC:

- En la configuración global
- En el nivel de perfil de sesión

### Comportamientos de complementos

Para cada tipo de cliente, NetScaler Gateway permite las tres opciones siguientes para controlar el comportamiento de actualización de plug-ins:

- **Siempre**

El complemento siempre se actualiza cuando la versión del complemento del usuario final no coincide con el complemento suministrado con el dispositivo NetScaler ADC. Este es el comportamiento predeterminado. Elija esta opción si no quiere que se ejecuten varias versiones de plug-ins en su empresa.

- **Esencial** (y seguridad)

El plug-in solo se actualiza cuando se considera necesario. Los ascensos de clase se consideran necesarios en las dos circunstancias siguientes:

- El complemento instalado no es compatible con la versión actual del dispositivo NetScaler ADC.
- El complemento instalado debe actualizarse para obtener la solución de seguridad necesaria.

Elija esta opción si quiere minimizar el número de actualizaciones de plug-ins, pero no quiere perderse ninguna actualización de seguridad de plug-ins

- **Nunca**

El plug-in no se actualiza.

### Parámetros de la CLI para controlar la actualización del complemento VPN

NetScaler Gateway admite dos tipos de complementos (EPA y VPN) para sistemas operativos Windows y Mac. Para admitir el control de actualización de plug-ins VPN a nivel de sesión, NetScaler Gateway admite dos parámetros de perfil de sesión denominados WindowsInPluginUpgrade y MacPluginUpgrade.

Estos parámetros están disponibles a nivel global, servidor virtual, grupo y usuario. Cada parámetro puede tener el valor Always, Essential o Never. Para obtener una descripción de estos parámetros, consulte Comportamientos de plug-ins.

### Parámetros de la CLI para controlar la actualización del complemento de la EPA

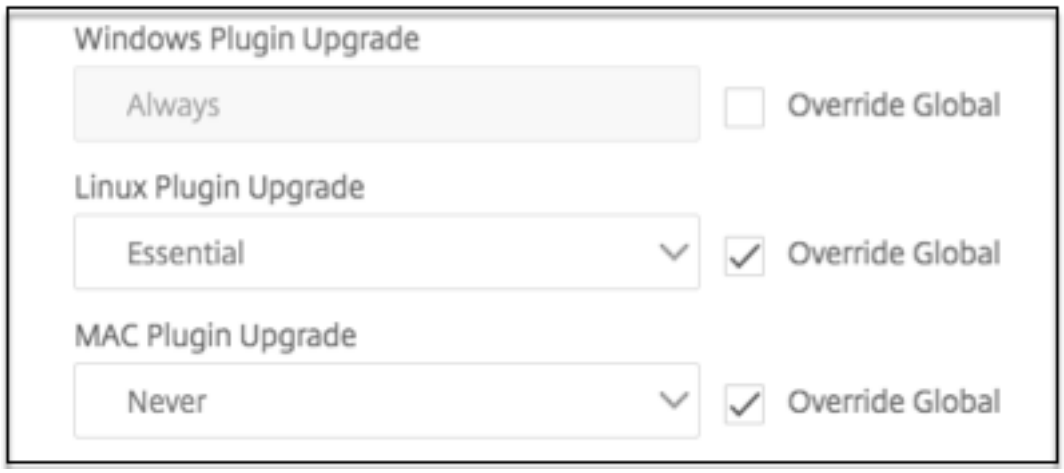
NetScaler Gateway admite complementos EPA para sistemas operativos Windows y Mac. Para admitir el control de actualización de plug-ins de EPA a nivel de servidor virtual, NetScaler Gateway admite dos parámetros de servidor virtual denominados windowsEPAPluginUpgrade y macEPAPluginUpgrade.

Los parámetros están disponibles en el nivel del servidor virtual. Cada parámetro puede tener el valor Always, Essential o Never. Para obtener una descripción de estos parámetros, consulte Comportamientos de plug-in

### Configuración de VPN

Siga estos pasos para la configuración de VPN de los complementos de Windows, Linux y Mac.

1. Vaya a **NetScaler ADC > Directivas > Sesión.**
2. Seleccione la directiva de sesión deseada y, a continuación, haga clic en **Modificar**.
3. Seleccione la ficha **Experiencia del cliente**.
4. Estas opciones de cuadros de diálogo afectan al comportamiento de actualización.
   - Siempre
   - Esencial
   - Nunca
     El valor predeterminado es Siempre.
5. Seleccione la casilla de verificación situada a la derecha de cada opción. Seleccione la frecuencia para aplicar el comportamiento de actualización.



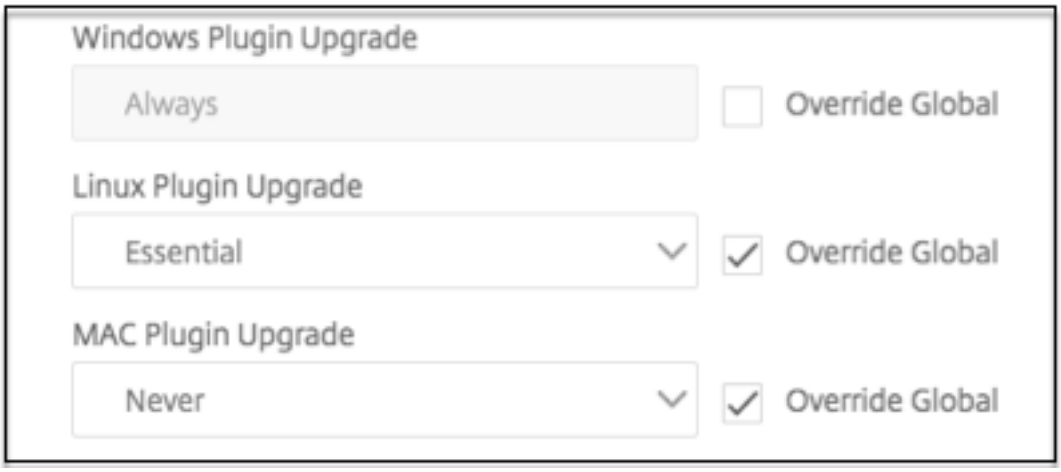
## Configuración EPA

Siga estos pasos para la configuración de la EPA de los complementos de Windows, Linux y Apple.

1. Vaya a **NetScaler Gateway > Servidores virtuales**.
2. Seleccione un servidor y haga clic en el botón **Editar**.
3. Haga clic en el icono del **lápiz**.


4. Haga clic en **Más**
5. Los cuadros de diálogo que aparecen afectan al comportamiento de la actualización. Las opciones disponibles son:

   - Siempre
   - Esencial
   - Nunca




## Requisitos

- La versión del complemento VPN y EPA de Windows debe ser superior a 11.0.0.0

- La versión del complemento EPA para Mac debe ser superior a 3.0.0.31
- La versión del complemento VPN para Mac debe ser superior a la 3.1.4 (357)

> **Nota:** Si el dispositivo NetScaler ADC se actualiza a la versión 11.0, todos los complementos VPN (y EPA) anteriores se actualizan a la versión más reciente independientemente de la configuración del control de actualización. Para las actualizaciones posteriores, respetan la configuración de control de actualización anterior.

## Configurar la configuración completa de VPN en Citrix Gateway

March 27, 2024

En esta sección se describe cómo configurar la configuración completa de VPN en un dispositivo NetScaler Gateway. Contiene consideraciones sobre redes y el enfoque ideal para resolver problemas desde la perspectiva de la red.

### Requisitos previos

- Instale un certificado SSL y vincúlelo al servidor virtual VPN.
  - CTX109260: Cómo generar e instalar un certificado SSL público en un dispositivo NetScaler
  - CTX122521: Cómo reemplazar el certificado predeterminado de un dispositivo NetScaler por un certificado de CA de confianza que coincida con el nombre de host del dispositivo
  - Documentación de Citrix: Vinculación del par de claves de certificado al servidor virtual basado en SSL
- Cree un perfil de autenticación para NetScaler Gateway.
  - Para obtener información adicional, consulte Documentación de Citrix - Configuración de la autenticación de usuarios externos
  - Para obtener información adicional, consulte Lista de comprobación: Uso de AD FS para implementar y administrar el inicio de sesión único
- Descargue Citrix VPN Client.
- Cree una directiva de sesión que permita conexiones VPN completas.

Cuando los usuarios se conectan con el plug-in de NetScaler Gateway, Secure Hub o Citrix Receiver, el software cliente establece un túnel seguro a través del puerto 443 (o cualquier puerto configurado

en NetScaler Gateway) y envía información de autenticación. Una vez establecido el túnel, NetScaler Gateway envía información de configuración al plug-in de NetScaler Gateway, Secure Hub o Receiver que se describen las redes que se van a proteger. Esta información también contiene una dirección IP si habilita las IP de la intranet.

Las conexiones de dispositivos de usuario se configuran definiendo los recursos a los que los usuarios pueden acceder en la red interna. La configuración de conexiones de dispositivos de usuario incluye lo siguiente:

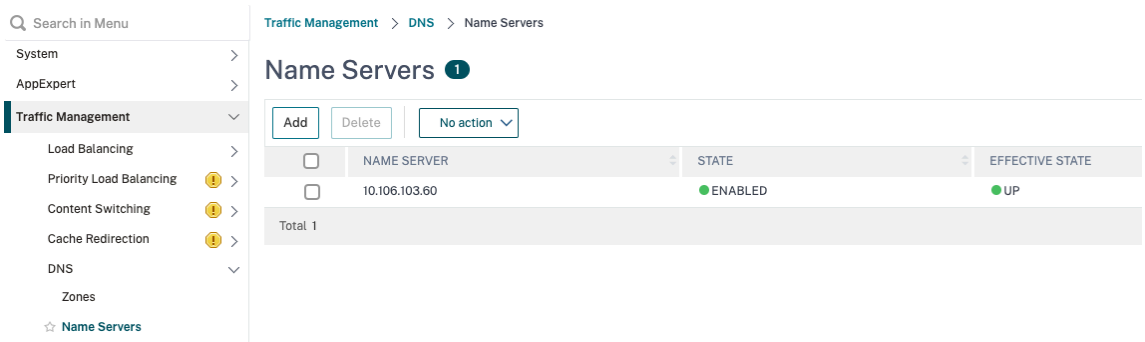
- Túneles divididos
- Direcciones IP de usuarios, incluidos grupos de direcciones (IP de intranet)
- Conexiones a través de un servidor proxy
- Definición de los dominios a los que se permite el acceso de los usuarios
- Configuración de tiempo de espera
- Single Sign-On
- Software de usuario que se conecta a través de NetScaler Gateway
- Acceso para dispositivos móviles

La mayoría de las conexiones de dispositivos de usuario se configuran mediante un perfil que forma parte de una directiva de sesión. También puede definir la configuración de conexión del dispositivo de usuario mediante directivas de autenticación, tráfico y autorización. También se pueden configurar mediante aplicaciones de intranet.

### Configurar una configuración VPN completa en un dispositivo Citrix Gateway

Para configurar una configuración de VPN en un dispositivo Citrix Gateway, complete el siguiente procedimiento:

1. Vaya a **Administración del tráfico > DNS**.
2. Seleccione el nodo Servidores de nombres, como se muestra en la siguiente captura de pantalla. Asegúrese de que el servidor de nombres DNS esté en la lista. Si no está disponible, agregue un servidor de nombres DNS.

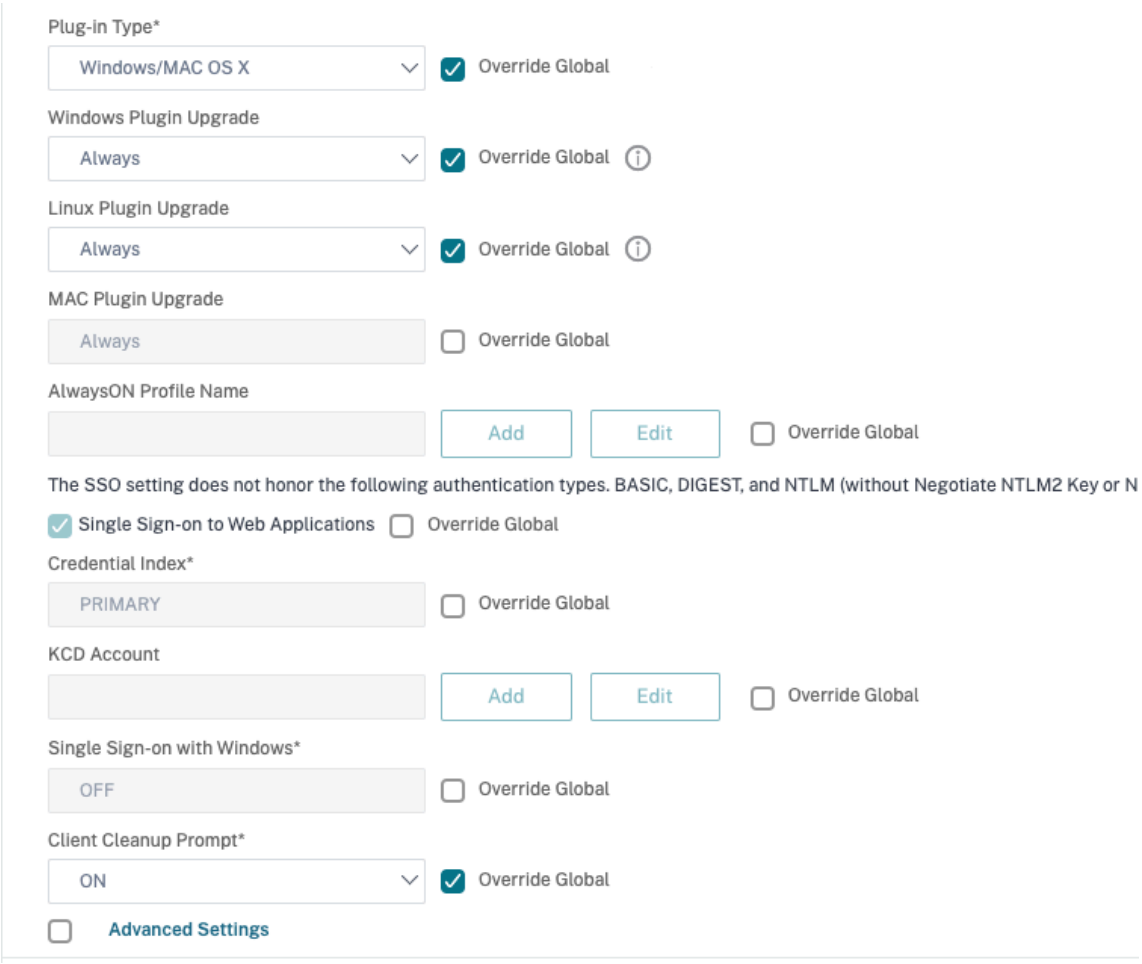



3. Expanda **NetScaler Gateway > Directivas**.

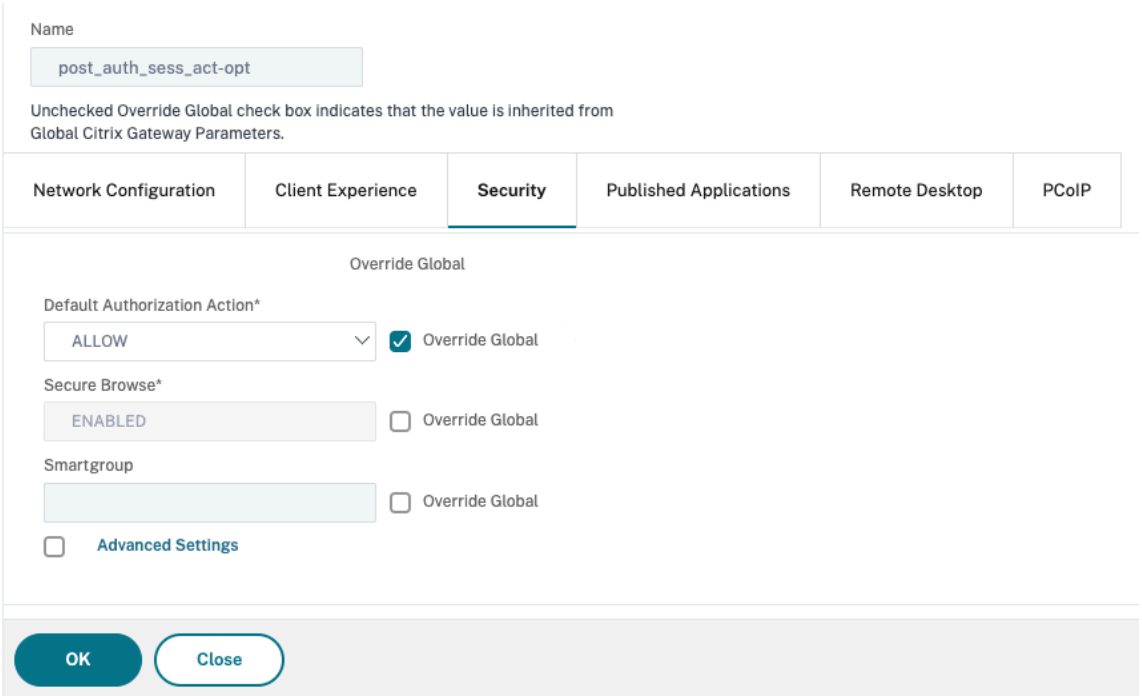
4. Seleccione el nodo **Sesión**.
5. En la página Perfiles y directivas de sesión de NetScaler Gateway, haga clic en la ficha **Perfiles** y haga clic en **Agregar**.
   Para cada componente que configure en el cuadro de diálogo Configurar perfil de sesión de NetScaler Gateway, asegúrese de seleccionar la opción **Supedición global** para el componente correspondiente.
6. Haga clic en la ficha **Experiencia del cliente**.
7. Escriba la URL del portal de la intranet en el campo Página de inicio si quiere presentar cualquier URL cuando el usuario inicie sesión en la VPN. Si el parámetro de página de inicio se establece en "nohomepage.html", la página principal no se muestra. Cuando se inicia el plug-in, se inicia una instancia del explorador y se mata automáticamente.
8. Asegúrese de seleccionar la configuración deseada de la lista Túnel dividido.
9. Selecciona **DESACTIVADO** en la lista **Acceso sin cliente** si quieres FullVPN.
10. Asegúrese de que **Windows/Mac OS X** esté seleccionado en la lista **Tipo de plug-in**.
11. Seleccione la opción **Single Sign-On en aplicaciones web** si lo quiere.
12. Asegúrese de que la opción **Mensaje de limpieza del cliente** esté seleccionada si es necesario, como se muestra en la siguiente captura de pantalla:

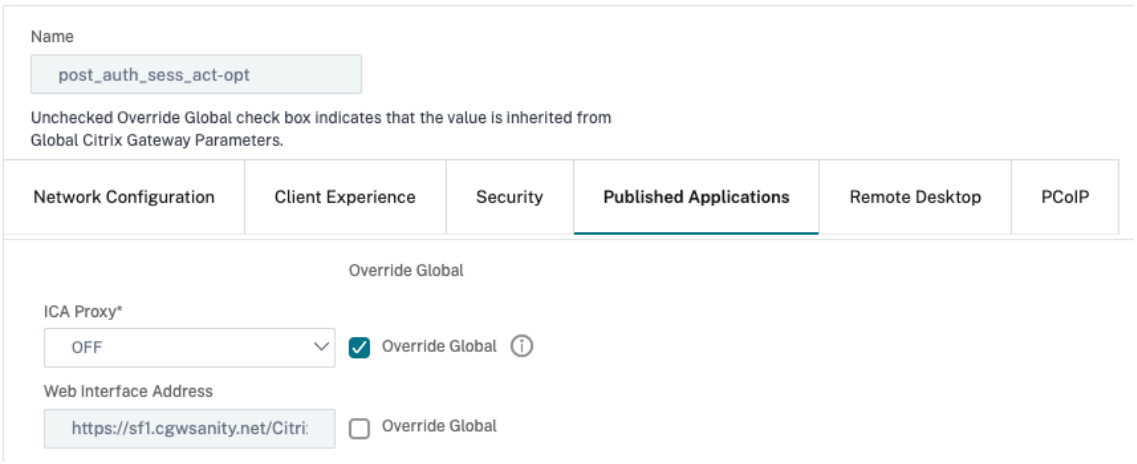



13. Haga clic en la ficha **Seguridad**.
14. Asegúrese de que **ALLOW** esté seleccionado en la lista **Acción de autorización predeterminada**, como se muestra en la siguiente captura de pantalla:

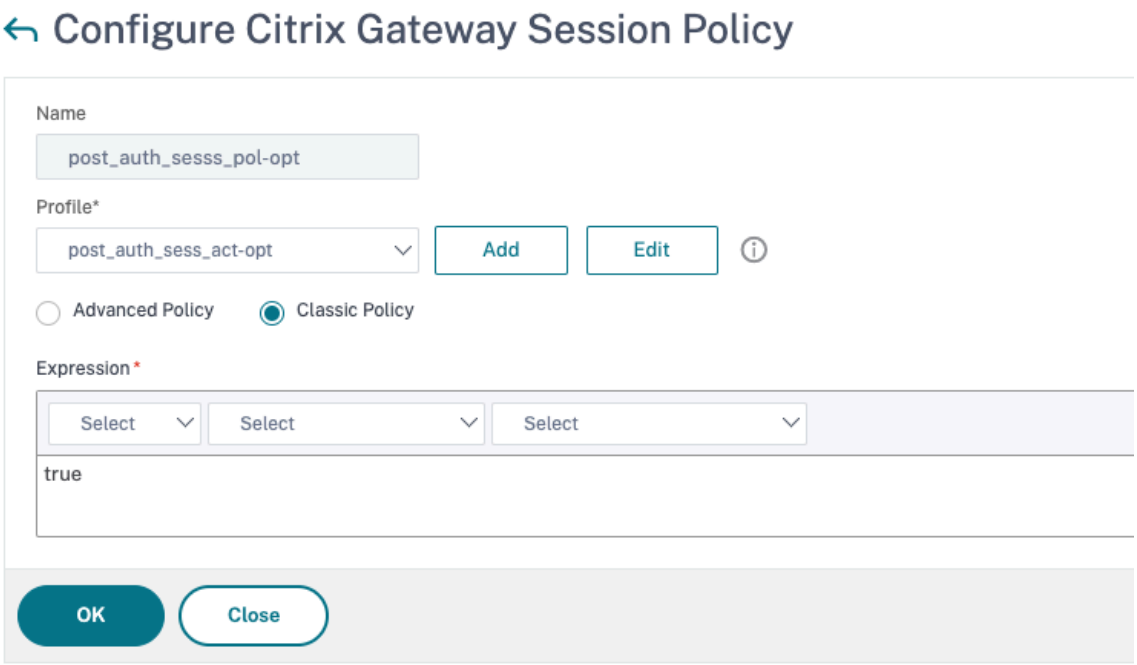



15. Haga clic en la ficha **Published Applications**.
16. Asegúrese de que está seleccionado **DESACTIVADO** en la lista **Proxy ICA** de la opción **Aplicaciones publicadas**.



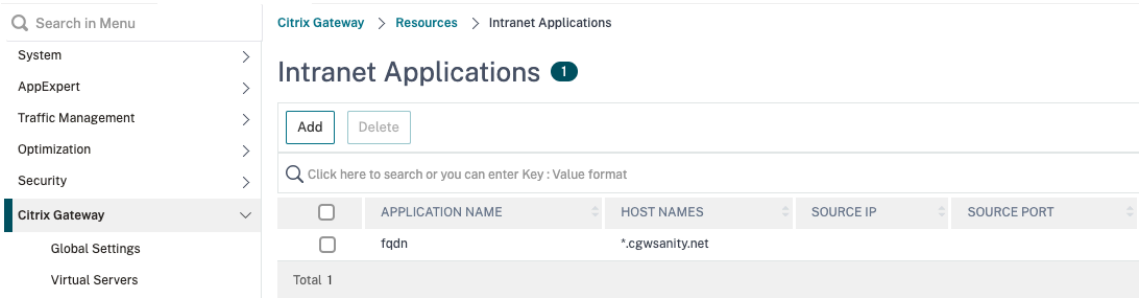

17. Haga clic en **Crear**.
18. Haga clic en **Cerrar**.
19. Haga clic en la ficha **Directivas** de la página Perfiles y directivas de sesión de NetScaler Gateway del servidor virtual o active las Directivas de sesión a nivel de GRUPO/USUARIO según sea necesario.
20. Cree una directiva de sesión con una expresión obligatoria o ns_true, como se muestra en la siguiente captura de pantalla:




21. Enlazar la directiva de sesión al servidor virtual VPN. Para obtener más información, consulte Vinculación de directivas de sesión.

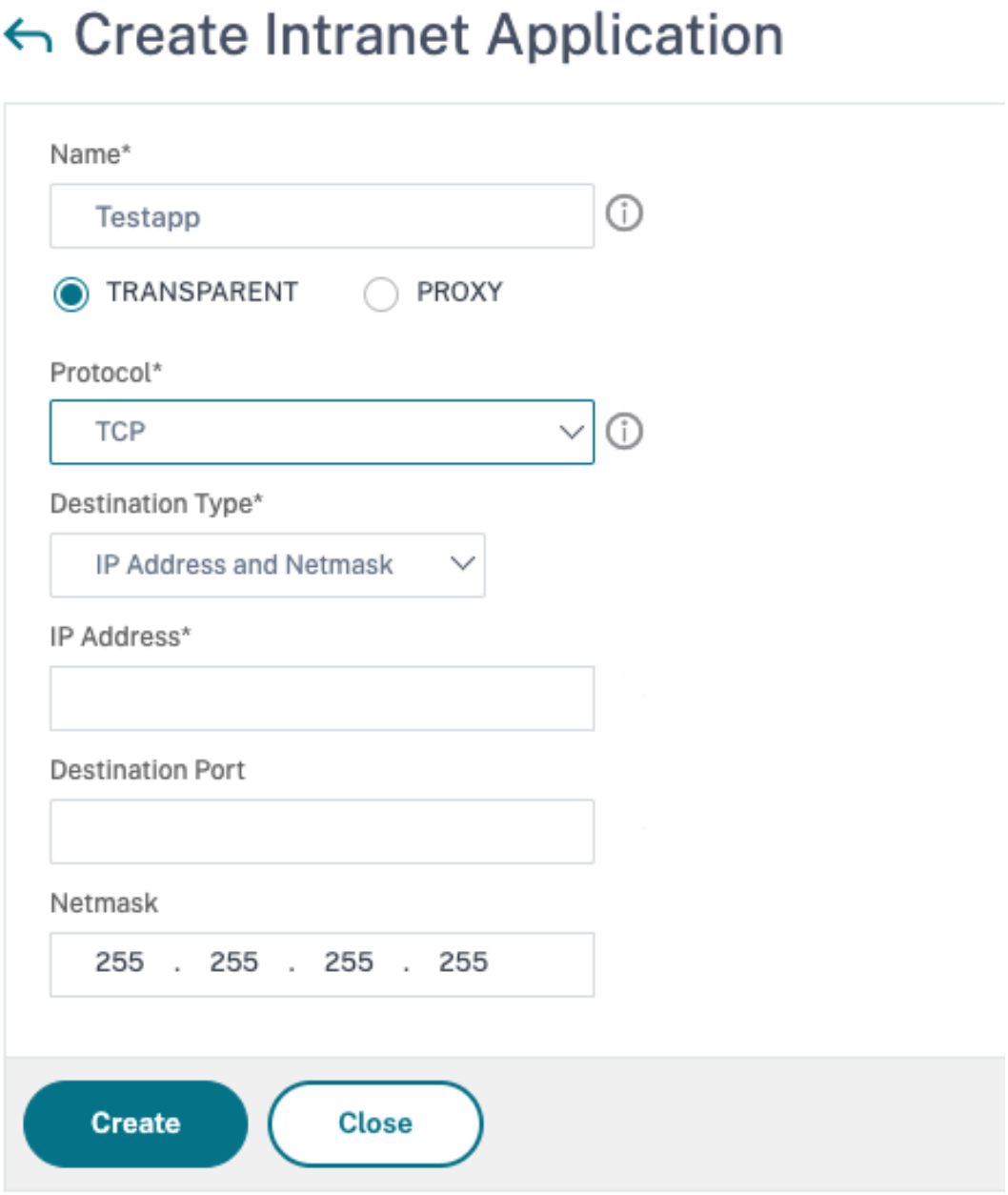
    Si el Túnel dividido se activó, debe configurar las aplicaciones de intranet a las que quiere que accedan los usuarios cuando estén conectados a la VPN. Para obtener más información sobre las aplicaciones de intranet, consulte Configuración de aplicaciones de intranet para el plug-in de NetScaler Gateway.




    a) Vaya a **NetScaler Gateway > Recursos > Aplicaciones de intranet**.

    b) Cree una aplicación de intranet. Seleccione Transparente para FullVPN con cliente Windows. Seleccione el protocolo que quiere permitir (TCP, UDP o ANY), el tipo de destino (dirección IP y máscara, intervalo de direcciones IP o nombre de host).



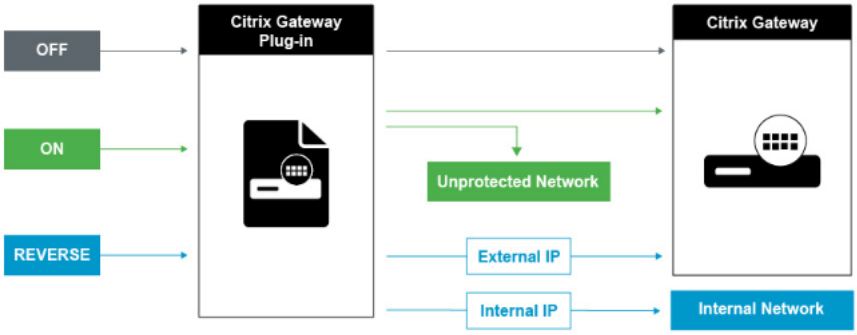

c) Si es necesario, defina una nueva directiva para Citrix VPN en iOS y Android mediante la siguiente expresión:
`REQ.HTTP.HEADER("User-Agent").CONTAINS("CitrixVPN")&& (REQ.HTTP.HEADER("User-Agent").CONTAINS("NSGiOSplugin")|| REQ.HTTP.HEADER("User-Agent").CONTAINS("Android"))`

d) Enlazar las aplicaciones de intranet creadas a nivel USER/GRUPO/VSERVER según sea necesario.

### Otros parámetros

Los siguientes son algunos de los parámetros que puede configurar.




**Túnel dividido APAGADO** Cuando el túnel dividido está desactivado, el complemento de NetScaler Gateway captura todo el tráfico de red procedente de un dispositivo de usuario y envía el tráfico a través del túnel VPN a NetScaler Gateway. En otras palabras, el cliente VPN establece una ruta predeterminada desde el PC cliente que apunta al VIP de NetScaler Gateway, lo que significa que todo el tráfico debe enviarse a través del túnel para llegar al destino. Dado que todo el tráfico se va a enviar a través del túnel, las directivas de autorización deben determinar si se permite el paso del tráfico a los recursos internos de la red o si se deniega.

Si bien está configurado en "desactivado", todo el tráfico pasa por el túnel, incluido el tráfico web estándar a los sitios web. Si el objetivo es supervisar y controlar este tráfico web, debe reenviar estas solicitudes a un proxy externo mediante NetScaler. Los dispositivos de usuario también se pueden conectar a través de un servidor proxy para acceder a redes internas.
NetScaler Gateway admite los protocolos HTTP, SSL, FTP y SOCKS. Para habilitar la compatibilidad con proxy para las conexiones de usuario, debe especificar esta configuración en NetScaler Gateway. Puede especificar la dirección IP y el puerto que utiliza el servidor proxy de NetScaler Gateway. El servidor proxy se utiliza como proxy de reenvío para todas las demás conexiones a la red interna.

Para obtener más información, consulte Habilitar la compatibilidad con proxy para las conexiones de usuario

**Túnel dividido ACTIVADO** Puede habilitar la tunelización dividida para evitar que el plug-in de NetScaler Gateway envíe tráfico de red innecesario a NetScaler Gateway. Si el túnel dividido está habilitado, el plug-in de NetScaler Gateway envía solo tráfico destinado a redes protegidas (aplicaciones de intranet) por NetScaler Gateway a través del túnel VPN. El plug-in de NetScaler Gateway no envía tráfico de red destinado a redes no protegidas a NetScaler Gateway. Cuando se inicia el plug-in de NetScaler Gateway, obtiene la lista de aplicaciones de intranet de NetScaler Gateway y establece una ruta para cada subred definida en la ficha de aplicación de intranet del equipo cliente. El plug-in de NetScaler Gateway examina todos los paquetes transmitidos desde

el dispositivo del usuario y compara las direcciones de los paquetes con la lista de aplicaciones de intranet (tabla de redirección creada cuando se inició la conexión VPN). Si la dirección de destino del paquete está dentro de una de las aplicaciones de intranet, el plug-in de NetScaler Gateway envía el paquete a través del túnel VPN a NetScaler Gateway. Si la dirección de destino no se encuentra en una aplicación de intranet definida, el paquete no se cifra y el dispositivo del usuario enruta el paquete de forma adecuada mediante la redirección predeterminada definida originalmente en el equipo cliente. "Cuando habilita la tunelización dividida, las aplicaciones de intranet definen el tráfico de red que se intercepta y se envía a través del túnel".

**Túnel de división inversa** NetScaler Gateway también admite la tunelización dividida inversa, que define el tráfico de red que NetScaler Gateway no intercepta. Si establece la tunelización dividida como inversa, las aplicaciones de intranet definen el tráfico de red que NetScaler Gateway no intercepta. Cuando habilita la tunelización dividida inversa, todo el tráfico de red dirigido a direcciones IP internas omite el túnel VPN, mientras que el resto del tráfico pasa por NetScaler Gateway. La tunelización dividida inversa se puede utilizar para registrar todo el tráfico LAN no local. Por ejemplo, si los usuarios tienen una red inalámbrica doméstica y han iniciado sesión con el plug-in de NetScaler Gateway, NetScaler Gateway no interceptará el tráfico de red destinado a una impresora u otro dispositivo dentro de la red inalámbrica.

### Para configurar el túnel dividido

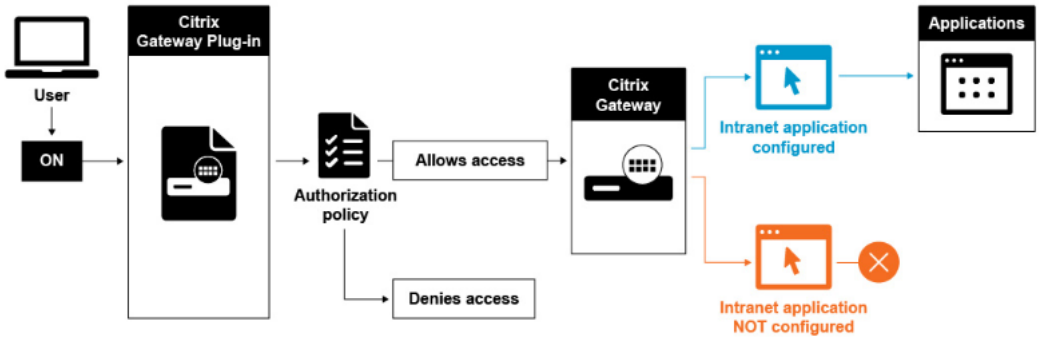
1. Vaya a **Configuración** > **Citrix Gateway > Directivas > Sesión**.
2. En el panel de detalles, en la ficha Perfiles, seleccione un perfil y, a continuación, haga clic en **Modificar**.
3. En la ficha **Experiencia del cliente**, junto a **Túnel dividido**, seleccione **Anulación global**, seleccione una opción y, a continuación, haga clic en **Aceptar**.

   Configurar la autorización y la tunelización dividida

   Al planificar la implementación de NetScaler Gateway, es importante tener en cuenta la tunelización dividida y la acción de autorización y las directivas de autorización predeterminadas.

   Por ejemplo, tiene una directiva de autorización que permite el acceso a un recurso de red. La tunelización dividida está activada y no configura las aplicaciones de intranet para enviar tráfico de red a través de NetScaler Gateway. Cuando NetScaler Gateway tiene este tipo de configuración, se permite el acceso al recurso, pero los usuarios no pueden acceder al recurso.




Si la directiva de autorización deniega el acceso a un recurso de red, tiene establecida la tunelización dividida en ON y las aplicaciones de intranet están configuradas para redirigir el tráfico de red a través de NetScaler Gateway, el plug-in de NetScaler Gateway envía tráfico a NetScaler Gateway, pero se deniega el acceso al recurso.

Para obtener más información sobre las directivas de autorización, revise lo siguiente:

- Configuración de autorización
- Configuración de directivas de autorización
- Configuración de la autorización global predeterminada

Para configurar el acceso de red a los recursos internos de la red

1. Vaya a **Configuración** > **NetScaler Gateway > Recursos > Aplicaciones de intranet**.
2. En el panel de detalles, haga clic en **Agregar**.
3. Complete los parámetros para permitir el acceso a la red, haga clic en **Crear** y, a continuación, en **Cerrar**.

Cuando no configuramos las IP de la intranet para los usuarios de VPN, el usuario envía el tráfico al Citrix Gateway VIP y, desde allí, NetScaler crea un nuevo paquete para el recurso de la aplicación de la intranet en la LAN interna. Este nuevo paquete se va a obtener desde el SNIP hacia la aplicación de intranet. Desde aquí, la aplicación de intranet obtiene el paquete, lo procesa y, a continuación, intenta responder al origen de ese paquete (el SNIP en este caso). El SNIP recibe el paquete y envía la respuesta al cliente que realizó la solicitud.

Cuando se usa la dirección IP de la intranet, el usuario envía el tráfico al VIP de Citrix Gateway y, desde allí, NetScaler asignará la IP del cliente a una de las IP de INTRANET configuradas del grupo. Tenga en cuenta que NetScaler será el propietario del grupo de IP de la intranet y, por este motivo, estos rangos no se deben usar en la red interna. El Citrix ADC asigna una IP de intranet para las conexiones VPN entrantes como lo haría un servidor DHCP. El NetScaler crea un nuevo paquete para la aplicación de intranet en la LAN a la que accedería el usuario. Este nuevo paquete se va a obtener de una de las IP de la intranet hacia la aplicación de intranet. Desde aquí, las aplicaciones de intranet obtienen el paquete, lo procesan y luego intentan responder al origen de ese paquete (la IP INTRANET). En este

caso, es necesario redirigir el paquete de respuesta al NetScaler, donde se encuentran las IP de la INTRANET (recuerde que el NetScaler es el propietario de las subredes de las IP de la intranet). Para llevar a cabo esta tarea, el administrador de red debe tener una ruta hacia la IP de INTRANET que apunte a uno de los SNIP. Se recomienda redirigir el tráfico al SNIP que contiene la ruta desde la que el paquete sale del NetScaler la primera vez para evitar cualquier tráfico asimétrico.

### Configurar resolución de servicios de nombres

Durante la instalación de NetScaler Gateway, puede utilizar el asistente de NetScaler Gateway para configurar otras opciones, incluidos los proveedores de servicios de nombres. Los proveedores de servicios de nombres traducen el nombre de dominio completo (FQDN) en una dirección IP. En el asistente de NetScaler Gateway, puede configurar un servidor DNS o WINS, establecer la prioridad de la búsqueda DNS y el número de veces que se debe volver a intentar la conexión con el servidor.

Al ejecutar el asistente de NetScaler Gateway, puede agregar un servidor DNS. Puede agregar otros servidores DNS y un servidor WINS a NetScaler Gateway mediante un perfil de sesión. A continuación, puede indicar a los usuarios y grupos que se conecten a un servidor de resolución de nombres distinto del que utilizó originalmente el asistente para configurar.

Antes de configurar otro servidor DNS en NetScaler Gateway, cree un servidor virtual que actúe como servidor DNS para la resolución de nombres.

Para agregar un servidor DNS o WINS dentro de un perfil de sesión

1. En la utilidad de configuración, ficha de configuración > **NetScaler Gateway > Directivas > Sesión**.
2. En el panel de detalles, en la ficha Perfiles, seleccione un perfil y, a continuación, haga clic en Abrir.
3. En la ficha Configuración de red, realice una de las siguientes acciones:
    - Para configurar un servidor DNS, junto a Servidor **virtual DNS** , haga clic en **Anular global** , seleccione el servidor y, a continuación, haga clic **en**Aceptar .
    - Para configurar un servidor WINS, junto a **IP del servidor WINS** , haga clic en **Anular global** , escriba la dirección IP y, a continuación, haga clic **en**Aceptar .

## Seleccionar el método de acceso de usuario

January 26, 2024

Puede configurar NetScaler Gateway para que proporcione conexiones de usuario en los siguientes casos:

- Conexiones de usuario mediante Citrix Receiver. Receiver funciona con StoreFront o la Interfaz Web para proporcionar a los usuarios acceso a aplicaciones publicadas o escritorios virtuales en una comunidad de servidores. Receiver es un software que utiliza el protocolo de red ICA para establecer las conexiones de los usuarios. Los usuarios instalan Receiver en el dispositivo del usuario. Cuando los usuarios instalan Receiver en su equipo basado en Windows o Mac, Receiver subsuma todos los complementos, incluido el plug-in de NetScaler Gateway para las conexiones de usuario. Citrix Gateway también admite conexiones desde Receiver para Android y Receiver para iOS. Los usuarios pueden conectarse a sus escritorios virtuales y aplicaciones basadas en Windows, web, móviles y SaaS a través de Citrix Endpoint Management, StoreFront o la Interfaz Web.
- Conexiones de usuario con Secure Hub. Los usuarios pueden conectarse a aplicaciones móviles, web y SaaS configuradas en Endpoint Management. Los usuarios instalan Secure Hub en su dispositivo móvil (Android o iOS). Cuando los usuarios inician sesión en Secure Hub, pueden instalar WorxMail y WorxWeb, junto con cualquier otra aplicación móvil que haya instalado en Endpoint Management. Secure Hub, Secure Mail y WorxWeb utilizan la tecnología Micro VPN para establecer conexiones a través de NetScaler Gateway.
- Conexiones de usuario mediante el plug-in de NetScaler Gateway como aplicación independiente. El plug-in de NetScaler Gateway es un software que los usuarios pueden descargar e instalar en un dispositivo de usuario. Cuando los usuarios inician sesión con el complemento, los usuarios pueden acceder a los recursos de la red segura como si estuvieran en la oficina. Los recursos incluyen servidores de correo electrónico, recursos compartidos de archivos y sitios web de intranet.
- Conexiones de usuario mediante acceso sin cliente. El acceso sin cliente proporciona a los usuarios el acceso que necesitan sin necesidad de instalar software, como el plug-in de NetScaler Gateway o Receiver, en el dispositivo del usuario. El acceso sin cliente permite conexiones a un conjunto limitado de recursos web, como Outlook Web Access o SharePoint, aplicaciones publicadas en Citrix Virtual Apps, escritorios virtuales de Citrix Virtual Apps and Desktops y recursos compartidos de archivos en la red segura a través de la interfaz de acceso. Los usuarios se conectan introduciendo la dirección web de NetScaler Gateway en un explorador web y, a continuación, seleccionan el acceso sin cliente en la página de opciones.
- Conexiones de usuario si se produce un error en el análisis de autenticación previa o posterior a la autenticación. Este caso se denomina respaldo del caso de acceso. El respaldo de escenario de Access permite que un dispositivo de usuario retroceda del plug-in de NetScaler Gateway a StoreFront o a la Interfaz Web, mediante Receiver, si el dispositivo de usuario no pasa el análisis inicial de análisis de endpoint.

Si los usuarios inician sesión en Citrix Gateway a través de Receiver, el análisis previo a la autenticación no funciona. Los análisis posteriores a la autenticación funcionan cuando NetScaler Gateway establece el túnel VPN.

Los usuarios pueden descargar e instalar el plug-in de NetScaler Gateway mediante los siguientes métodos:

- Conexión a NetScaler Gateway mediante un explorador web.
- Conexión a StoreFront configurada para aceptar conexiones de NetScaler Gateway.
- Instalación del complemento mediante un objeto de directiva de grupo (GPO).
- Carga del plug-in de NetScaler ADC en Merchandising Server.

## Implementación de complementos de Citrix Gateway para el acceso de los usuarios

January 26, 2024

NetScaler Gateway incluye los siguientes complementos para el acceso de los usuarios:

- Plug-in de NetScaler Gateway para Windows
- Plug-in de NetScaler Gateway para Mac
- Plug-in de NetScaler Gateway para Java

Cuando los usuarios inician sesión en NetScaler Gateway por primera vez, descargan e instalan el plug-in de NetScaler Gateway desde una página web. Los usuarios inician sesión haciendo clic en el icono de NetScaler Gateway del área de notificación de un equipo basado en Windows. En un equipo macOS X, los usuarios pueden iniciar sesión desde el **Dock o el menú Aplicaciones**. Si actualiza NetScaler Gateway a una nueva versión de software, el plug-in de NetScaler Gateway se actualiza automáticamente en el dispositivo del usuario.

El plug-in de NetScaler Gateway para Java se puede utilizar en cualquier dispositivo de usuario que admita Java. El plug-in de NetScaler Gateway para Java es compatible con la mayoría de las aplicaciones basadas en TCP, pero solo proporciona algunas de las funciones del complemento NetScaler Gateway para Windows o del complemento NetScaler Gateway para macOS X. El complemento NetScaler Gateway para Java proporciona acceso limitado a los recursos de red que defina. Para obtener más información sobre el complemento Java, consulte [Conexión con el complemento Citrix Gateway para Java.] (./ng-plugin-select-type/ng-connect-ng-plugin-java-configure-tsk.html)

### Implementación del complemento Citrix Gateway mediante el paquete de instalación MSI

Puede implementar el plug-in de NetScaler Gateway mediante una infraestructura de Microsoft Active Directory o una herramienta de implementación MSI estándar de terceros, como Windows Server Update Services. Si utiliza una herramienta compatible con paquetes de Windows Installer, puede implementar los paquetes con cualquier herramienta que admita archivos MSI. A continuación, utiliza la herramienta de implementación para implementar e instalar el software en los dispositivos de usuario adecuados.

#### Ventajas de utilizar una herramienta de implementación centralizada

- Cumplimiento con los requisitos de seguridad. Por ejemplo, puede instalar software de usuario sin habilitar los privilegios de instalación de software para usuarios no administrativos.
- Control de versiones de software. Puede implementar una versión actualizada del software para todos los usuarios de forma simultánea.
- Escalabilidad. Una estrategia de implementación centralizada se amplía fácilmente para admitir usuarios adicionales.
- Experiencia de usuario positiva. Puede implementar, probar y solucionar problemas relacionados con la instalación sin involucrar a los usuarios en este proceso.

Citrix recomienda esta opción cuando se prefiere el control administrativo sobre la instalación del software de usuario y el acceso a los dispositivos del usuario está disponible fácilmente.

Para obtener más información, consulte Implementación del plug-in de NetScaler Gateway desde Active Directory.

### Determinar qué complemento de software implementar

Si la implementación de NetScaler Gateway no requiere ningún complemento de software en los dispositivos de usuario, se considera que la implementación proporciona acceso sin cliente. En este caso, los usuarios solo necesitan un explorador Web para tener acceso a los recursos de red. Sin embargo, ciertas funciones requieren el software del complemento en el dispositivo del usuario.

## Selección del plug-in de NetScaler Gateway para usuarios

March 27, 2024

Al configurar NetScaler Gateway, puede elegir cómo inician sesión los usuarios. Los usuarios pueden iniciar sesión con uno de los siguientes plug-ins:

- Plug-in de NetScaler Gateway para Windows
- Plug-in de NetScaler Gateway para Mac OS X
- Plug-in de NetScaler Gateway para Java

Para completar la configuración, cree una directiva de sesión y, a continuación, vincular la directiva a usuarios, grupos o servidores virtuales. También puede habilitar plug-ins configurando los ajustes globales. En el perfil global o de sesión, seleccione Windows/Mac OS X o Java como tipo de complemento. Cuando los usuarios inician sesión, reciben el plug-in tal y como se define globalmente o en el perfil y la directiva de la sesión. Debe crear perfiles independientes para el tipo de complemento. Solo puede elegir Windows/Mac OS X o Java en el perfil de sesión. Para configurar el plug-in de NetScaler Gateway para Java, consulte Conexión con el plug-in de NetScaler Gateway para Java.

### Para configurar el complemento de forma global

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Experiencia del cliente, junto a Tipo de complemento, seleccione Windows/Mac OS X y, a continuación, haga clic en Aceptar.

### Para configurar el tipo de complemento para Windows o Mac OS X en un perfil de sesión

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. Lleve a cabo una de las siguientes acciones:
   - Si va a crear una nueva directiva de sesión, en el panel de detalles, haga clic en Agregar.
   - Si va a cambiar una directiva existente, selecciónela y, a continuación, haga clic en Abrir.
3. Cree un perfil nuevo o modifique un perfil existente. Para hacerlo, realice una de las siguientes acciones:
   - Junto a Solicitar perfil, haz clic en Nuevo .
   - Junto a Solicitar perfil , haz clic en Modificar .
4. En la pestaña Experiencia del cliente, junto a Tipo de complemento, haga clic en Anular global y, a continuación, seleccione Windows/Mac OS X.
5. Lleve a cabo una de las siguientes acciones:
   - Si va a crear un perfil nuevo, haga clic en Crear, defina la expresión en el cuadro de diálogo de la política, haga clic en Crear y, a continuación, en Cerrar.

- Si está modificando un perfil existente, después de realizar la selección, pulse Aceptar dos veces.

### Para establecer el modo de interceptación para el plug-in de NetScaler Gateway para Windows

Si está configurando el plug-in de NetScaler Gateway para Windows, también debe configurar el modo de interceptación y configurarlo en transparente.

1. En la utilidad de configuración, haga clic en la pestaña Configuración, expanda Citrix Gateway > Recursos y, a continuación, haga clic en Aplicaciones de intranet.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para la directiva.
4. Pulse en Transparente.
5. En Protocolo, seleccione CUALQUIERA.
6. En Tipo de destino, seleccione Dirección IP y máscara de red.
7. en dirección IP, escriba la dirección IP.
8. En Máscara de red, escriba la máscara de subred, haga clic en Crear y, a continuación, en Cerrar.

## Instalación del plug-in de NetScaler Gateway para Windows

January 26, 2024

Cuando los usuarios inician sesión en NetScaler Gateway, descargan e instalan el plug-in de NetScaler Gateway en el dispositivo del usuario.

Para instalar el plug-in, los usuarios deben ser administradores locales o miembros del grupo Administradores. Esta restricción se aplica solo para la instalación por primera vez. Las actualizaciones de complementos no requieren acceso a nivel de administrador.

Para permitir que los usuarios se conecten y utilicen NetScaler Gateway, debe proporcionarles la siguiente información:

- Dirección web de NetScaler Gateway, como https://NetScalerGatewayFQDN/
- Cualquier requisito del sistema para ejecutar el plug-in de NetScaler Gateway si ha configurado recursos y directivas de endpoint

En función de la configuración del dispositivo de usuario, es posible que también deba proporcionar la siguiente información:

- Si los usuarios ejecutan un firewall en su equipo, es posible que tengan que cambiar la configuración del firewall para que el firewall no bloquee el tráfico hacia o desde las direcciones IP correspondientes a los recursos a los que usted concedió acceso. El plug-in de NetScaler Gateway maneja automáticamente el Firewall de conexión a Internet en Windows XP y Firewall de Windows en Windows XP Service Pack 2, Windows Vista, Windows 7, Windows 8 o Windows 8.1.
- Los usuarios que deseen enviar tráfico a FTP a través de una conexión de Citrix Gateway deben configurar su aplicación FTP para realizar transferencias pasivas. Una transferencia pasiva significa que el equipo remoto establece la conexión de datos con el servidor FTP, en lugar de que el servidor FTP establezca la conexión de datos con el equipo remoto.
- Los usuarios que deseen ejecutar aplicaciones cliente X a través de la conexión deben ejecutar un servidor X, como XManager, en sus equipos.
- Los usuarios que instalen Receiver para Windows o Receiver para Mac pueden iniciar el plug-in de NetScaler Gateway desde Receiver o mediante un explorador Web. Proporcione instrucciones a los usuarios acerca de cómo iniciar sesión con el plug-in de NetScaler Gateway a través de Receiver o un explorador Web.

Como los usuarios trabajan con los archivos y las aplicaciones como si fueran locales en la red de la organización, no es necesario volver a capacitar a los usuarios ni configurar las aplicaciones.

Para establecer una conexión segura por primera vez, inicie sesión en NetScaler Gateway mediante la página de inicio de sesión web. El formato típico de una dirección web es.https://companyname.com Cuando los usuarios inician sesión, pueden descargar e instalar el plug-in de NetScaler Gateway en su equipo.

### Para instalar el plug-in de NetScaler Gateway para Windows

1. En un explorador web, escriba la dirección web de NetScaler Gateway.
2. Escriba el nombre de usuario y la contraseña y, a continuación, haga clic en Inicio de sesión.
3. Seleccione Acceso a red y, a continuación, haga clic en Descargar.
4. Siga las instrucciones para instalar el plug-in.

Una vez finalizada la descarga, el plug-in de NetScaler Gateway se conecta y muestra un mensaje en el área de notificación de un equipo basado en Windows.

Si quiere que los usuarios se conecten con el complemento de NetScaler Gateway sin utilizar un explorador web, puede configurarlo para que muestre el cuadro de diálogo de inicio de sesión cuando los usuarios hagan clic con el botón secundario en el icono de NetScaler Gateway en el área de notificación de un equipo basado en Windows o inicien el complemento desde el menú Inicio.

### Para configurar el cuadro de diálogo de inicio de sesión para el plug-in de NetScaler Gateway para Windows

Para configurar el plug-in de NetScaler Gateway para que utilice el cuadro de diálogo de inicio de sesión, los usuarios deben iniciar sesión para completar este procedimiento.

1. En un equipo con Windows, en el área de notificación, haga clic con el botón secundario en el icono de NetScaler Gateway y, a continuación, haga clic en Configurar NetScaler Gateway.
2. Haga clic en la ficha Perfil y, a continuación, haga clic en Cambiar perfil.
3. En la ficha Opciones, haga clic en Usar el plug-in de NetScaler Gateway para iniciar sesión.
   Nota: Si los usuarios abren el cuadro de diálogo
   Configurar NetScaler Gateway desde Receiver, la ficha
   Opciones no está disponible.

## Implementación del plug-in de NetScaler Gateway desde Active Directory

January 26, 2024

Si los usuarios no tienen privilegios administrativos para instalar el plug-in de NetScaler Gateway en el dispositivo de usuario, puede implementarlo para los usuarios desde Active Directory.

Cuando utiliza este método para implementar el plug-in de NetScaler Gateway, puede extraer el programa de instalación y, a continuación, utilizar una directiva de grupo para implementar el programa. Los pasos generales para este tipo de implementación son los siguientes:

- Extracción del paquete MSI.
- Distribución del plug-in mediante una directiva de grupo.
- Creación de un punto de distribución.
- Asignación del paquete de plug-ins de NetScaler Gateway mediante un objeto de directiva de grupo.

  **Nota:**La distribución del complemento Citrix Gateway desde Active Directory solo se admite en Windows XP, Windows Vista, Windows 7 y Windows 8.

Puede descargar el paquete MSI desde la utilidad de configuración o desde el sitio web de Citrix.

### Para descargar el paquete MSI del plug-in de NetScaler Gateway desde la utilidad de configuración

1. En la utilidad de configuración, haga clic en **Descargas**.
2. En Plug-in de NetScaler Gateway, haga clic en **Descargar complemento de NetScaler Gateway para Windows** y, a continuación, guarde el archivo **nsvpnc_setup.exe** en el servidor Windows.

   **Nota:**

   - Para equipos de 64 bits, debe guardar el archivo Agee_setup.exe en el servidor Windows.
   - Si no aparece el cuadro de diálogo **Descarga de archivos**, presione la tecla CTRL al hacer clic en el vínculo **Descargar plug-in de NetScaler Gateway para Windows**.

3. En el símbolo del sistema, vaya a la carpeta en la que guardó **nsvpnc_setup.exe** y, a continuación, escriba:

   ```
   nsvpnc_setup /c
   <!--NeedCopy-->
   ```

   Esto extrae el archivo agee.msi.

   **Nota:** Para equipos de 64 bits, vaya a la carpeta en la que guardó **Agee_setup.exe** y, a continuación, escriba:

   ```
   Agee_setup.exe /c
   <!--NeedCopy-->
   ```

   Esto extrae el archivo agee64.msi.

4. Guarde el archivo extraído en una carpeta del servidor Windows.

Después de extraer el archivo, utilice una directiva de grupo en Windows Server para distribuirlo.

Antes de iniciar la distribución, instale la Consola de administración de directivas de grupo en Windows Server 2003, Windows Server 2008 o Windows Server 2012. Para obtener más información, consulte la ayuda en línea de Windows.

**Nota:** Cuando utiliza una directiva de grupo para publicar el complemento de NetScaler Gateway, Citrix recomienda asignar el paquete al dispositivo del usuario. El paquete MSI se instala por dispositivo.

Antes de poder distribuir el software, cree un punto de distribución en un recurso compartido de red de un servidor de publicación, como Microsoft Internet Security and Acceleration (ISA) Server.

### Para crear un punto de distribución

1. Inicie sesión en el servidor de publicación como administrador.

2. Cree una carpeta y compártala en la red con permiso de lectura para todas las cuentas que necesiten acceso al paquete de distribución.
3. En el símbolo del sistema, vaya a la carpeta en la que guarde el archivo extraído y, a continuación, escriba: msiexec -a agee.msi
4. En la pantalla **Ubicación de red**, haga clic en **Cambiar** y, a continuación, vaya a la carpeta compartida en la que quiere crear la instalación administrativa del plug-in de NetScaler Gateway.
5. Haga clic en **Aceptar** y luego en **Instalar**.

Después de colocar el paquete extraído en el recurso compartido de red, asigne el paquete a un objeto de directiva de grupo en Windows.

Después de configurar correctamente el plug-in de NetScaler Gateway como un paquete de software administrado, el complemento se instala automáticamente la próxima vez que se inicie el dispositivo de usuario.

> **Nota:** Cuando el paquete de instalación se asigna a un equipo, el usuario debe reiniciarlo.

Cuando se inicia la instalación, los usuarios reciben un mensaje de que el plug-in de NetScaler Gateway está instalando.

## Actualización y eliminación del plug-in de NetScaler Gateway mediante Active Directory

January 26, 2024

Cada versión del plug-in de NetScaler Gateway se empaqueta como una instalación completa del producto, en lugar de como una revisión. Cuando los usuarios inician sesión y el plug-in de NetScaler Gateway detecta una nueva versión del complemento, el complemento se actualiza automáticamente. También puede implementar el plug-in de NetScaler Gateway para actualizar mediante Active Directory.

Para ello, cree un nuevo punto de distribución para el plug-in de NetScaler Gateway. Cree un nuevo objeto de política de grupo y asígnele la nueva versión del complemento. A continuación, cree un vínculo entre el nuevo paquete y el paquete existente. Después de crear el vínculo, se actualiza el plug-in de NetScaler Gateway.

### Eliminación del plug-in de NetScaler Gateway de dispositivos de usuario

Para quitar el plug-in de NetScaler Gateway de los dispositivos de usuario, quite el paquete asignado del Editor de objetos de directiva de grupo.

Cuando se quita el complemento del dispositivo del usuario, los usuarios reciben un mensaje que indica que el complemento se está desinstalando.

## Solución de problemas de la instalación del plug-in de NetScaler Gateway mediante Active Directory

January 26, 2024

Si el paquete asignado no se instala cuando se inicia el dispositivo del usuario, es posible que aparezca la siguiente advertencia en el registro de sucesos de la aplicación:

No se han podido aplicar los cambios a la configuración de instalación del software. La aplicación de directivas de instalación de software se ha retrasado hasta el siguiente inicio de sesión porque un administrador ha habilitado la optimización de inicios de sesión para la directiva de grupo. El error fue: el marco de políticas de grupo debería llamar a la extensión en la actualización sincrónica de políticas en primer plano.

Este error se debe a la optimización del inicio de sesión rápido en Windows XP, en la que los usuarios pueden iniciar sesión antes de que el sistema operativo inicialice todos los componentes de red, incluido el procesamiento de objetos de directiva de grupo. Algunas directivas pueden requerir más de un reinicio para que surtan efecto. Para resolver este problema, inhabilite la optimización de inicio de sesión rápido en Active Directory.

Para solucionar otros problemas de instalación del software administrado, Citrix recomienda utilizar una directiva de grupo para habilitar el registro de Windows Installer.

## Conexión con el plug-in de NetScaler Gateway para Java

March 27, 2024

El plug-in de NetScaler Gateway para Java se puede utilizar en cualquier dispositivo de usuario que admita Java.

> **Nota:**Los siguientes sistemas operativos y navegadores web requieren la versión 1.4.2 de Java Runtime Environment (JRE) hasta la versión más reciente de JRE.

- Mac OS X
- Linux
- Windows XP (todas las versiones), Windows Vista, Windows 7 y Windows 8
- Internet Explorer

- Firefox
- Safari 1.2 hasta la versión más reciente del explorador web

El plug-in de NetScaler Gateway para Java admite la mayoría de las aplicaciones basadas en TCP, pero solo proporciona algunas de las funciones del plug-in de NetScaler Gateway para Windows o del plug-in de NetScaler Gateway para Mac OS X.

Los usuarios no requieren privilegios administrativos en el dispositivo de usuario para utilizar el plug-in de NetScaler Gateway para Java. Por motivos de seguridad, es posible que quiera utilizar esta versión del complemento para un servidor virtual, grupo o usuario en particular, independientemente del dispositivo de usuario que se utilice.

Para configurar NetScaler Gateway para que instale el plug-in de NetScaler Gateway para Java en dispositivos de usuario, configure una directiva de sesión y, a continuación, enlaza con el servidor virtual, el grupo o el usuario.

Si los usuarios inician sesión desde un equipo con Windows 7, la información del servidor proxy no se establece automáticamente en Internet Explorer. Los usuarios deben configurar manualmente el servidor proxy en el equipo que ejecuta Windows 7.

### Para configurar el plug-in de NetScaler Gateway para Java

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, haga clic en la ficha Perfiles .
3. Seleccione un perfil de sesión y, a continuación, haga clic en Abrir .
4. En la pestaña Experiencia del cliente, junto a Tipo de complemento, haga clic en Anular global, seleccione Java y, a continuación, haga clic en Aceptar.

### Para establecer el modo de interceptación

Después de crear la directiva de sesión, cree una aplicación de intranet para definir el modo de interceptación para los usuarios que inician sesión con el plug-in de NetScaler Gateway para Java.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway > Recursos y, a continuación, haga clic en Aplicaciones de intranet.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre.
4. Haz clic en Proxy .
5. En Dirección IP de destino, escriba la dirección IP.
6. En Puerto de destino, escriba el número de puerto.
7. En Dirección IP de origen, escriba la dirección IP.

8. En Puerto de origen, escriba el número de puerto, haga clic en Crear y, a continuación, haga clic en Cerrar.

Si no especifica una dirección IP ni un número de puerto de origen, NetScaler Gateway utiliza automáticamente 127.0.0.1 para la dirección IP y 0 para el puerto.

### Actualización del archivo HOSTS en equipos basados en Windows

Cuando los usuarios inician sesión con el plug-in de NetScaler Gateway para Java en un equipo que ejecuta Windows Vista, Windows 7 o Windows 8, el tráfico de red para aplicaciones de intranet TCP no se tuneliza. El archivo HOSTS no se actualiza automáticamente en los equipos que ejecutan Vista y Windows 7. Debe agregar las aplicaciones de intranet manualmente al archivo HOSTS.

En un equipo basado en Windows, puede modificar el archivo HOSTS en el Bloc de notas u otro editor de texto. Si modifica el archivo HOSTS en el Bloc de notas, debe ejecutar el Bloc de notas como administrador. Agregue las entradas de asignación para la aplicación de intranet para el plug-in de NetScaler Gateway para Java y, a continuación, guarde el archivo.

## Integración del plug-in de NetScaler Gateway con Citrix Receiver

January 26, 2024

Citrix Gateway es compatible con Receiver. El sistema orquestado consta de los siguientes componentes:

- Receiver para Windows 3.4 o posterior
- Receiver para Mac
- Receiver para Android
- Receiver para iOS
- StoreFront 2.1 o posterior
- AppController 2.8 y versiones más recientes o Citrix Endpoint Management 10
- Citrix Update Service alojado en el sitio web de Citrix

Para obtener más información sobre la compatibilidad de NetScaler Gateway con los productos Citrix, consulte Compatibilidad con productos Citrix.

Puede configurar NetScaler Gateway para que cuando los usuarios inicien sesión en el dispositivo, el plug-in de NetScaler Gateway abra un explorador Web que permita el inicio de sesión único en la página principal de Receiver. Los usuarios pueden descargar Receiver desde la página de inicio.

Cuando los usuarios inician sesión en Receiver, las conexiones de los usuarios pueden enrutarse a través de Citrix Gateway de la siguiente manera:

- Directamente a Endpoint Management
- Directamente a StoreFront
- A StoreFront y, a continuación, a Endpoint Management si no configura las aplicaciones móviles MDX en Endpoint Management
- A Endpoint Management y luego a StoreFront si configura aplicaciones móviles MDX en Endpoint Management

**Nota:**Las conexiones que se dirigen directamente a Endpoint Management solo son compatibles con AppController 2.0, AppController 2.5, AppController 2.6, App Controller 2.8 y App Controller 2.9. Si tiene AppController 1.1 implementado en la red, las conexiones de usuario deben enrutarse a través de StoreFront.

## Cómo funcionan las conexiones de usuario con Citrix Receive

January 26, 2024

Los usuarios pueden conectarse a las siguientes aplicaciones, escritorios y datos desde Citrix Receiver:

- Aplicaciones basadas en Windows y escritorios virtuales publicados en StoreFront y en la interfaz web
- Acceso a los datos de ShareFile mediante Citrix Endpoint Management

Los usuarios pueden iniciar sesión mediante cualquiera de los siguientes Receivers:

- Receiver para Web
- Receiver para Windows
- Receiver para Mac
- Receiver para iOS
- Receiver para Android

Los usuarios pueden iniciar sesión en Receiver para Web mediante un explorador web o desde el icono de Receiver del dispositivo del usuario.

Cuando los usuarios inician sesión con cualquier versión de Receiver, las aplicaciones, los datos de ShareFile y los escritorios aparecen en el explorador o en la ventana de Receiver.

## Desacoplamiento del icono de la aplicación Citrix Workspace

January 26, 2024

Cuando se configura una implementación de Citrix Virtual Apps and Desktops con el plug-in de NetScaler Gateway integrado en la aplicación Citrix Workspace, el icono del complemento no está visible para un usuario conectado a la VPN. El icono del **plug-in de NetScaler Gateway** suele estar en la bandeja del sistema de Windows o en la barra de menús de macOS X Finder. Este icono es la interfaz de los ajustes y controles del plug-in. Para los usuarios de Windows, cuando la aplicación Citrix Workspace y el plug-in de NetScaler Gateway están integrados, el cuadro de diálogo **Acerca de** de la aplicación Citrix Workspace muestra los controles del plug-in de NetScaler Gateway. Para los usuarios de macOS X, no hay controles disponibles para el plug-in de NetScaler Gateway tras la integración.

Algunas implementaciones integradas pueden presentar la necesidad de exponer los controles del plug-in sin perder la integración de la funcionalidad subyacente. Para ello, utilice el siguiente comando de CLI o la tarea de la utilidad de configuración de NetScaler ADC para alternar la integración de iconos para clientes VPN.

### Configuración de la integración de iconos mediante la CLI

En la línea de comandos, escriba;

```
set vpn parameter [-iconWithReceiver (ON/OFF)]

<!--NeedCopy-->
```

### Configuración de la integración de iconos mediante la GUI

1. En la ficha Configuración, vaya a **NetScaler Gateway > Configuración global**.
2. Haga clic en **Cambiar configuración global** y, a continuación, seleccione la ficha **Experiencia del cliente**.
3. Haga clic en **Configuración avanzada.**
4. Seleccione **Mostrar el icono del complemento VPN con la aplicación Citrix Workspace.**

> **Importante:**
>
> Esta configuración surtirá efecto una vez que se reinicie el proceso del complemento VPN de Windows.

## Configurar IPv6 para conexiones ICA

March 27, 2024

NetScaler Gateway admite direcciones IPv6 para conexiones ICA. Las conexiones con IPv6 a la interfaz web o StoreFront funcionan igual que las conexiones IPv4. Cuando los usuarios se conectan mediante la dirección web de NetScaler Gateway, NetScaler Gateway envía como proxy la conexión a la interfaz web o StoreFront.

Puede configurar IPv6 para NetScaler Gateway implementado en una DMZ o implementado en una DMZ de doble salto.

Puede habilitar IPv6 en NetScaler Gateway mediante la línea de comandos. Puede usar las siguientes pautas:

- Habilite IPv6 en el dispositivo.
- Configure las direcciones IP de subred.
- Defina el orden de resolución de DNS.
- Defina la interfaz web o la dirección web de StoreFront.
- Vincule Secure Ticket Authority (STA) a NetScaler Gateway.

De forma predeterminada, la dirección IP asignada no admite direcciones IPv6. Para redirigir las comunicaciones de los usuarios a la red interna, debe crear direcciones IP de subred y, a continuación, configurar NetScaler Gateway para que utilice las direcciones IP de subred.

Si implementa varias subredes IPv6 en la red, cree varias direcciones IP de subred IPv6 en NetScaler Gateway, para cada subred de la red. La redirección de red envía los paquetes IPv6 a las subredes respectivas mediante las direcciones IP de subred.

### Para configurar IPv6 para el proxy ICA

Para configurar IPv6 para el proxy ICA:

1. Inicie sesión en NetScaler Gateway mediante una conexión de Secure Shell (SSH), como desde PuTTY.
2. En la línea de comandos, escriba enable ns feature IPv6pt. Esto habilita IPv6.
3. En la línea de comandos, escriba enable ns mode USNIP. Esto permite el uso de las direcciones IP de subred.
4. En la línea de comandos, escriba: **set dns parameter** —**ResolutionOrder AAAAAthenaQuery AthenAAAQuery OnlyAAAQuery OnlyAquery**
5. En la línea de comandos, escriba: **set vpn parameter -wihome**`http://XD_domain/Citrix/StoreWeb`.

Donde es el nombre de dominio o la dirección IP de StoreFront.

Por ejemplo, defina el **parámetro vpn -wihome `http://storefront.domain.com/Citrix/StoreWeb`.**

o bien

**establecer el parámetro vpn -wihome `http://[1000:2000::3000]/Citrix/StoreWeb`**

> Si utiliza la dirección IPv6 para configurar este parámetro, la dirección IP debe estar entre corchetes.

## Configuración de la página principal de Receiver en Citrix Gateway

March 27, 2024

Puede configurar la página de inicio de Receiver de forma global o como parte de un perfil de sesión. Si desea configurar Receiver para Web y versiones anteriores de Receiver que no reconozcan StoreFront a través de Citrix Gateway, debe crear dos perfiles de sesión independientes. El campo Página principal de Citrix Receiver debe tener la dirección web correcta para cada perfil para que los usuarios puedan iniciar sesión correctamente.

Para los Receivers que reconocen StoreFront a través de Citrix Gateway, puede hacer que Receiver para Web y Receiver compartan un perfil. Sin embargo, Citrix recomienda configurar un perfil de sesión para Receiver para Web y un perfil de sesión independiente para todos los demás Receivers.

### Para configurar la página de inicio de Receiver de forma global

Para configurar la página de inicio de Receiver de forma global:

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En el cuadro de diálogo Configuración global de NetScaler Gateway, haga clic en la ficha Aplicaciones publicadas.
4. En la página principal de Citrix Receiver, escriba la dirección web de Receiver o la página principal de Receiver para Web y, a continuación, haga clic en Aceptar.

### Para configurar la página principal de Receiver en un perfil de sesión

Para configurar la página principal de Receiver en un perfil de sesión:

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la pestaña **Perfiles** , haga clic en **Agregar** .
3. En el cuadro de diálogo **Crear perfil de sesión de NetScaler Gateway**, en la ficha **Aplicación publicada**, junto a la Página **inicial de Citrix Receiver**, haga clic en **Supedición global**.
4. En la página principal de Citrix Receiver, escriba la dirección web de la página principal de Receiver o Receiver para Web y, a continuación, haga clic en **Crear** .

## Aplicar el tema de Receiver a la página de inicio de sesión

March 27, 2024

Puede usar la utilidad de configuración para aplicar el tema de Receiver a la página de inicio de sesión de Citrix Gateway. Puede cambiar entre el tema de Receiver, el tema predeterminado o un tema personalizado que cree. La función está disponible en las siguientes versiones de Citrix Gateway:

- Citrix Gateway 10.1 o posterior.
- Access Gateway 10, compilación 71.6014.e
- Access Gateway 10, compilación 73.5002.e

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En el cuadro de diálogo Configuración global de NetScaler Gateway, haga clic en la ficha Experiencia del cliente.
4. Junto a Tema de la interfaz de usuario, haga clic en Green Bubble y, a continuación, en Aceptar.

   Este comando sobrescribe la página de inicio de sesión original con el tema de Receiver. Nota: Después de aplicar un tema diferente, aconseja a los usuarios que borren la caché del explorador para evitar que aparezcan páginas almacenadas en caché.

# Crear un tema personalizado para la página de inicio de sesión

January 26, 2024

Puede usar la utilidad de configuración para crear un tema personalizado para la página de inicio de sesión de Citrix Gateway. También puede dejar el tema predeterminado o usar el tema de Citrix Receiver. Cuando elige aplicar un tema personalizado a la página de inicio de sesión, utiliza la línea de comandos de NetScaler Gateway para crear e implementar el tema. A continuación, utilice la utilidad de configuración para configurar la página de tema personalizada.

La página de temas personalizados se configura mediante la configuración global de NetScaler Gateway.

Puede utilizar esta función con las siguientes versiones de NetScaler Gateway:

- NetScaler Gateway 10.1
- Access Gateway 10, compilación 73.5002.e (debe instalar esta compilación después de la compilación 71.6104.e para usar esta función con las versiones 2.5, 2.6 o 2.8 de AppController)
- Access Gateway 10, compilación 71.6104.e

## Crear e implementar el tema personalizado mediante la línea de comandos

Para crear e implementar el tema personalizado mediante la línea de comandos:

1. Inicie sesión en la línea de comandos de NetScaler Gateway.
2. En una línea de comandos, escriba shell.
3. En la línea de comandos, escriba mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*.
4. Utilice la utilidad de configuración para cambiar al tema personalizado y, a continuación, realizar cambios de personalización en /var/ns_gui_custom/ns_gui/vpn. Puede hacer lo siguiente:
    - Realice ediciones en el archivo css/ctx.authentication.css.
    - Copie un logotipo personalizado en la carpeta /var/ns_gui_custom/ns_gui/vpn/media. **Nota:** Puede utilizar WinSCP para transferir los archivos.
5. Si tiene varios dispositivos NetScaler Gateway, repita los pasos 3 y 4 para todos los dispositivos.

# Personalizar el portal de usuario

March 27, 2024

Las instalaciones de NetScaler Gateway que ofrecen el portal a los usuarios de VPN incluyen la opción de seleccionar un tema del portal para crear un aspecto personalizado para las páginas del portal. Puede seleccionar entre un conjunto de temas suministrado o puede usar un tema como plantilla para crear un portal personalizado o de marca. Con la utilidad de configuración, puede modificar un tema agregando nuevos logotipos, imágenes de fondo, etiquetas de cuadro de entrada personalizadas y otros atributos del diseño del portal basado en CSS. Los temas integrados del portal incluyen contenido para cinco idiomas: inglés, francés, español, alemán y japonés. Se atiende a diferentes usuarios en distintos idiomas, según las configuraciones regionales indicadas por sus exploradores web.

Tiene la opción de crear un acuerdo de licencia de usuario final (EULA) personalizado que se presente a los usuarios de VPN antes de que se les permita iniciar sesión. La función EULA admite versiones específicas de la configuración regional de un CLUF, que se presentan a los usuarios en función de las configuraciones regionales informadas de sus exploradores web.

Tanto los temas del portal como las configuraciones de EULA se pueden enlazar de forma independiente en el servidor virtual VPN y a nivel global de VPN.

> **Importante:**Citrix no admite la personalización que requiera modificaciones en el código y no ofrece soporte para resolver problemas más allá de volver a un tema predeterminado.

## Aplicación de un tema de portal

De forma predeterminada, el portal VPN está configurado para usar el tema Caxton. El tema de Caxton se llama Predeterminado.

#### Tema Caxton

Citrix Gateway incluye dos temas adicionales que se pueden aplicar al portal: los temas Greenbubble y X1.

#### Tema Greenbubble

#### Tema X1

Puede aplicar cualquiera de los temas suministrados directamente a un servidor virtual VPN o como enlace VPN global.

## Vincular un tema de portal a un servidor virtual VPN

Puede enlazar un tema de portal en un servidor virtual existente o al crear un nuevo servidor virtual.

### Uso de la línea de comandos para vincular un tema de portal a un servidor virtual VPN existente

En la línea de comandos, escriba;

```
bind vpn vserver <name> -portaltheme <name>
<!--NeedCopy-->
```

### Uso de la utilidad de configuración para vincular un tema de portal a un servidor virtual VPN existente

1. En la ficha **Configuración**, vaya a **NetScaler Gateway** y haga clic en **Servidores virtuales.**
2. Seleccione un servidor virtual y, a continuación, haga clic en **Modificar**.
3. Si un tema del portal aún no se ha enlazado al servidor virtual, haga clic en **Tema del portal** en **Configuración avanzada** en el panel de detalles. De lo contrario, la opción **Tema del portal**ya está expandida en el panel de detalles.
4. En el panel de detalles, en **Temas del portal**, haga clic en **Sin tema del portal**para expandir la ventana de enlace Tema del portal.
5. Haga clic **en Haga clic para seleccionar**.
6. En la ventana **Temas del portal**, haga clic en un nombre de tema y, a continuación, haga clic en **Seleccionar**.
7. Haga clic en **Bind**.
8. Haga clic en **Listo**.

Si está creando un servidor virtual VPN, puede seguir los pasos anteriores empezando por el paso 3 mientras se encuentra en el panel de edición del servidor virtual VPN para vincular un tema de portal.

## Vincular un tema de portal a VPN Global

### Uso de la línea de comandos para vincular un tema del portal al ámbito global de la VPN

En la línea de comando, escriba;

```
bind vpn global portaltheme <name>
<!--NeedCopy-->
```

#### Usar la utilidad de configuración para enlazar un tema de portal al ámbito global de VPN

1. En la ficha **Configuración**, vaya a **NetScaler Gateway.**
2. En el panel de detalles principal, haga clic en **NetScaler Gateway Policy Manager**.
3. Haga clic en el icono "**+**".
4. En la lista **Punto de enlace**, seleccione **Recursos**.
5. En la lista**Tipo de conexión**, seleccione**Tema del portal.**
6. Haga clic en **Continuar**.
7. En la pantalla **Punto de enlace**, haga clic en **Agregar enlace**.
8. Haga clic **en Haga clic para seleccionar**.
9. En la ventana **Temas del portal**, haga clic en un nombre de tema y, a continuación, haga clic en **Seleccionar**.
10. Haga clic en **Bind**.
11. Haga clic en **Cerrar**.
12. Haga clic en **Listo.**

> **Consejo:**Cuando haya completado una serie de cambios, utilice el comando «guardar ns config» en la línea de comandos o haga clic en el icono de guardar de la utilidad de configuración para asegurarse de que los cambios se guardan en el archivo de configuración de Citrix ADC.

### Creación de un tema de portal

Para crear un diseño de portal personalizado, utilice uno de los temas del portal suministrados como plantilla. El sistema hace una copia del tema de plantilla seleccionado con el nombre que especifique.

### Uso de un tema de portal estándar como plantilla para un tema de portal personalizado

Para crear un tema del portal, puede utilizar la utilidad de configuración o la línea de comandos para crear la entidad del tema. Sin embargo, los controles de personalización detallados solo están disponibles en la utilidad de configuración.

#### Uso de la línea de comandos para crear un tema de portal

En la línea de comandos, escriba;

```
add portaltheme <name> basetheme <name>
<!--NeedCopy-->
```

#### Uso de la utilidad de configuración para crear un tema de portal

1. En la ficha **Configuración**, vaya a **NetScaler Gateway** y haga clic en **Temas del portal**.
2. En el panel de detalles principal, haga clic en **Agregar**.
3. Introduzca un nombre para el tema, seleccione una plantilla en el menú de plantillas y, a continuación, haga clic **en**Aceptar .
4. En este punto, se le presenta la primera vista de la ventana de modificación del tema del portal. Haga clic en **Aceptar** para salir.

Puede proceder a personalizar el nuevo tema del portal con la primera vista. Sin embargo, debe leer la siguiente sección sobre la personalización del tema del portal sobre la interfaz y las descripciones emergentes de los atributos personalizables del portal dentro de la interfaz antes de continuar con la edición de un tema del portal.

Una vez creado un tema nuevo, puede vincularlo como se describe en Vincular un tema de portal a un servidor virtual VPN o Vincular un tema de portal a VPN Global . Puede enlazar un nuevo tema inmediatamente después de crearlo o después de completar tus personalizaciones.

### Personalización del tema del portal

Para personalizar un tema del portal, utilice la interfaz Tema del portal en la utilidad de configuración. Para obtener los mejores resultados, debe comprender los distintos elementos de esta interfaz antes de usarla.

### Acerca de la interfaz de temas del portal

Para abrir la interfaz de temas del portal en la utilidad de configuración de Citrix Gateway, en la pestaña **Configuración** , vaya a **Citrix Gateway** y haga clic en **Temas del portal** . Puede crear un tema como se describe en *Creación de un tema de portal* o seleccionar un tema existente en el panel de detalles principal y hacer clic en **Editar** .

La página de personalización del tema del portal tiene cuatro paneles de componentes principales para modificar el diseño del portal: el panel Tema del portal, el panel Look & Feel, el panel **Configuración avanzada** y el panel **Idioma** .

#### Interfaz de Portal Theme

El panel **Tema del portal** en la parte superior de la página informa qué tema se carga para modificar y en qué tema de plantilla se basa. La opción de visualización aquí le permite ver sus personalizaciones sin tener que acceder a la VPN con una conexión de usuario. El uso de la opción de visualización

requiere vincular el tema a un servidor virtual VPN y el enlace permanece en vigor después de cerrar la ventana de visualización.

Con el panel **Aspecto y sensación** en el centro de la página, configura las propiedades generales de un tema, como encabezados, colores e imágenes de fondo, propiedades de fuente y logotipos. Cuando este panel está en modo de modificación, las leyendas de atributos están disponibles para obtener información sobre dónde se utilizan los atributos Aspecto y sensación en las páginas del portal.

El panel **Configuración avanzada** contiene los controles de contenido en pantalla de las páginas del portal individuales. Para cargar el contenido de una página para modificarlo, haga clic en una de las páginas de la lista. Los controles de página se abren debajo de los demás paneles centrales. Una página permanece contraída en el panel **Configuración avanzada** en todas las ediciones del tema del portal siempre y cuando la página no se haya modificado.

En el panel **Idioma** , puede seleccionar cuál de los idiomas se cargará cuando se seleccione una página para editarla desde el panel **Configuración avanzada** . Las páginas en inglés se cargan de forma predeterminada.

### Tipos de atributos de página personalizables

Al personalizar un tema del portal, puede modificar una serie de atributos en la interfaz del tema del portal. Junto con el texto y los idiomas compatibles que se pueden editar, todos los elementos gráficos del diseño del portal se pueden adaptar a sus necesidades. Cada tipo de elemento de página tiene parámetros o recomendaciones que se deben tener en cuenta antes de modificarlos.

#### *Colores*

El diseño del portal especifica los colores de los atributos como fondos de página, resaltados, texto para títulos y contenido principal, controles de botones y respuestas al pasar el ratón. Para personalizar un atributo de color, puede introducir un valor de color directamente para un artículo seleccionado o utilizar el selector de color suministrado para generar un valor de color. La interfaz admite la introducción de valores de color HTML válidos en formato RGBA, formato triplete hexadecimal HTML y nombres de colores X11. Se puede acceder al selector de color para cualquier atributo de color aplicable haciendo clic en el cuadro de color situado junto al campo de entrada del atributo.

### El selector de colores *Fuentes*

Junto con los colores de las fuentes, puede modificar el tamaño de fuente de algunos atributos de página. Para cada uno de estos atributos, un menú de lista ofrece los tamaños disponibles para cada atributo, según lo determine el diseño del portal.

#### *Imágenes*

En el caso de las imágenes, una descripción emergente disponible para cada control proporciona recomendaciones de tamaño y otros requisitos. Las descripciones varían según la ubicación de un atributo en la página y su función. Puede utilizar formatos de archivo de imagen PNG o JPEG. Para seleccionar una imagen que quiere cargar, seleccione la casilla de verificación situada debajo del nombre de archivo de un elemento y, a continuación, vaya a la ubicación de la imagen en la unidad de su equipo local.

***Etiquetas***

En la sección **Configuración avanzada**, puede seleccionar el texto de una página de portal específica para modificar. Si modifica el texto en inglés predeterminado de una página, el texto de otros idiomas no se vuelve a traducir. El contenido de la página de idioma alternativo se proporciona para su comodidad, pero requiere actualizaciones manuales para cualquier personalización. Para modificar otra versión de idioma de una página, contrae primero la ventana, si está abierta, haciendo clic en el icono **X** de la página del portal abierta. A continuación, seleccione el idioma en el panel **Idioma** y haga clic en **Aceptar**. Todas las páginas del portal que se abran desde el panel **Configuración avanzada** estarán en ese idioma hasta que seleccione otro.

> **Importante**
>
> En implementaciones de alta disponibilidad o agrupadas, los temas del portal se distribuyen a través de la configuración compartida solo cuando la configuración del tema del portal se realiza en las entidades NetScaler ADC principal o coordinador de configuración, respectivamente.

## Nota sobre las personalizaciones antiguas del portal

Para las instalaciones con un diseño de portal personalizado modificado manualmente y creado en las versiones de NetScaler Gateway o Access Gateway anteriores a la 11.0, Citrix recomienda encarecidamente comenzar con un nuevo tema del portal en la interfaz de personalización. Si no puede hacerlo, puede aplicar una personalización manualmente, pero no se proporciona soporte directo para ello.

Al utilizar un portal personalizado manualmente, debe establecer el portal personalizado como una configuración de portal global. Sin embargo, hacerlo significa que una configuración de portal global aplicada *no se puede* anular con los enlaces de tema del portal a nivel de servidor virtual VPN. Intentar crear un enlace de servidor virtual VPN en este caso con la utilidad de configuración o la línea de comandos devuelve un error.

Además, en el caso de configuraciones de clúster y alta disponibilidad, las personalizaciones manuales deben realizarse en todos los nodos de la implementación, ya que los archivos subyacentes del sistema de archivos NetScaler ADC no se distribuyen en la configuración compartida automáticamente.

### Creación manual de una configuración de portal personalizada

Para aplicar manualmente una configuración de portal personalizada anterior después de actualizar a NetScaler Gateway 11.0, debe modificar una copia de una página de portal existente, colocar los archivos de portal personalizados en el sistema de archivos NetScaler ADC y seleccionar **CUSTOM** como parámetro **UITHEME**.

Puede utilizar WinSCP o cualquier otro programa de copia segura para transferir archivos al sistema de archivos NetScaler ADC.

1. Inicie sesión en la línea de comandos de NetScaler Gateway.
2. En el símbolo del sistema, escriba**shell**
3. En el símbolo del sistema, escriba **mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*.**
4. En el símbolo del sistema, escriba **cd /var/netscaler/logon/themes/**
    - Si quieres personalizar el tema de Greenbubble, escribe **cp -r Greenbubble Custom** para hacer una copia del tema de Greenbubble.
    - Si desea personalizar el tema Predeterminado (Caxton), escriba **cp -r Default Custom.**
    - Para personalizar el tema X1, escriba**cp -r X1 Custom.**
5. Realice los cambios necesarios en los archivos copiados en**/var/NetScaler/logon/themes/custom** para personalizar el tema manualmente.
    - Realice las ediciones necesarias en **css/base.css**.
    - Copie las imágenes personalizadas en el directorio **/var/ns_gui_custom/ns_gui/vpn/media**.
    - Realice cambios en las etiquetas de los archivos presentes en el directorio **resources/**. Estos archivos corresponden a las configuraciones regionales admitidas por el portal.
    - Si también se necesitan cambios en las páginas HTML o en los archivos javascript, puede hacer lo relevante para los archivos en **/var/ns_gui_custom/ns_gui/**.
6. Una vez que se hayan completado todos los cambios de personalización, escriba: **tar —cvzf /var/ns_gui_custom/customtheme.tar.gz /var/ns_gui_custom/ns_gui/***

> **Importante**
>
> Al copiar un directorio de temas en los pasos anteriores, el nombre de carpeta copiada debe escribirse exactamente como "Personalizado", ya que los nombres de directorio distinguen entre mayúsculas y minúsculas dentro de la interfaz de shell de NetScaler ADC. Si el nombre del directorio no se introduce con precisión, la carpeta no se reconoce cuando la configuración **UITHEME** está configurada en **CUSTOM**.

#### Seleccione el tema personalizado como parámetro global de VPN

Una vez finalizada la configuración del portal personalizada manualmente y copiada en el sistema de archivos NetScaler ADC, debe aplicarse a la configuración de NetScaler Gateway. Esto se hace estableciendo el parámetro UITHEME en CUSTOM y se puede completar con la línea de comandos o la utilidad de configuración.

Para utilizar la línea de comandos, escriba el siguiente comando para establecer el parámetro **UITHEME**.

```
set vpn parameter UITHEME CUSTOM
<!--NeedCopy-->
```

Para establecer el parámetro UITHEME mediante la utilidad de configuración, utilice el procedimiento siguiente.

1. En la ficha **Configuración**, desplácese a **NetScaler Gateway > Configuración global**.
2. Haga clic en **Cambiar configuración global**.
3. Haga clic en la ficha **Experiencia del cliente**.
4. Desplázate hasta la parte inferior de la pantalla y selecciona **CUSTOM** en la lista de **temas de interfaz** de usuario.
5. Haga clic en **Aceptar**.

El portal personalizado manualmente es ahora el diseño del portal presentado a los usuarios de VPN.

### Creación de un contrato de licencia de usuario final

El sistema de portal VPN ofrece la opción de aplicar un acuerdo de licencia de usuario final (EULA) a la configuración de un portal. Una vez que un CLUF está vinculado a la configuración de NetScaler Gateway, ya sea en el ámbito global de VPN o en un servidor virtual VPN relevante, los usuarios de VPN deben aceptar el CLUF como términos y condiciones antes de que se les permita autenticarse en la VPN.

Al igual que con los temas del portal, los usuarios reciben un CLUF específico del idioma en función de la configuración regional indicada por su explorador web. En el caso de una configuración regional que no coincida con ninguno de los idiomas admitidos, el idioma predeterminado que se sirve es el inglés. Para cada EULA, puede introducir un mensaje personalizado en cada uno de los idiomas admitidos. El contenido pretraducido no se proporciona para las configuraciones del CLUF como lo es para los temas del portal. Si la configuración regional notificada de un usuario coincide con un idioma en el que no se ha introducido ningún contenido del CLUF, se le devuelve una página en blanco cuando hace clic en el enlace “Términos y condiciones”de la página de inicio de sesión de VPN.

Para crear un CLUF, puede utilizar cualquiera de los controles de la utilidad de configuración de la ficha **Configurar NetScaler Gateway**** > Configuración global > CLUF**o**NetScaler Gateway > Recursos > CLUF**. Los controles del panel**Configuración global**se utilizan para administrar los enlaces de EULA globales de VPN, mientras que el control del nodo**Recursos > EULA**se utiliza para operaciones generales en configuraciones de EULA. Puede administrar los enlaces de EULA del servidor virtual VPN editando un servidor virtual VPN en**NetScaler Gateway > Servidores virtuales**. Algunos comandos también están disponibles con la línea de comandos para administrar entidades de CLUF. Sin embargo, los controles completos de administración del CLUF solo están disponibles en la utilidad de configuración.

#### Uso de la línea de comandos para crear una entidad de EULA

En la línea de comandos, escriba;

```
add vpn eula <name>
<!--NeedCopy-->
```

#### Uso de la utilidad de configuración para crear una entidad de EULA

1. Vaya a **NetScaler Gateway > Recursos > EULA**.
2. Haga clic en **Agregar** para crear una entidad.
3. Introduzca un nombre para la entidad.
4. Para cada uno de los idiomas, pega el contenido debajo de las fichas correspondientes. Puede utilizar texto sin formato o etiquetas HTML para dar formato al contenido, incluida una etiqueta <br> para agregar saltos de línea.
5. Haga clic en **Crear**.

Una vez creada una entidad EULA, se puede enlazar globalmente a la configuración de VPN o a un servidor virtual VPN.

#### Uso de la línea de comandos para vincular un EULA a VPN Global

En la línea de comando, escriba;

```
bind vpn global eula <name>
<!--NeedCopy-->
```

#### Usar la utilidad de configuración para crear un enlace global de EULA VPN

1. En la ficha **Configuración**, desplácese a **NetScaler Gateway > Configuración global**.

2. En el panel de detalles principal, haga clic en **Configurar un contrato de licencia de usuario final**.
3. Haga clic en **Add Binding**.
4. Haga clic **en Haga clic para seleccionar**.
5. Seleccione una entidad EULA y, a continuación, haga clic en **Seleccionar**.
6. Haga clic en **Bind**.
7. Haga clic en **Cerrar**.

#### Uso de la línea de comandos para vincular un EULA a un servidor virtual VPN

En la línea de comando, escriba;

```
bind vpn vserver <name> eula <name>
<!--NeedCopy-->
```

#### Usar la utilidad de configuración para enlazar un CLUF a un servidor virtual VPN

1. En la ficha **Configuración**, vaya a **NetScaler Gateway > Servidores virtuales.**
2. En el panel de detalles principal, seleccione un servidor virtual VPN y haga clic en **Modificar**.
3. En el panel **Configuración avanzada** de la parte derecha de la página, haga clic en **CLUF**.
4. En el panel CLUF recién agregado, haga clic en **Sin EULA**.
5. Haga clic **en Haga clic para seleccionar**.
6. Seleccione una entidad EULA y haga clic en **Seleccionar**.
7. Haga clic en **Bind**.
8. Haga clic en **Listo**.

## Solicitar a los usuarios que actualicen exploradores antiguos o no compatibles mediante la creación de una página personalizada

January 26, 2024

Si un cliente se conecta a una dirección VIP de Citrix ADC mediante un cifrado no seguro como SSLv3, se le puede redirigir a una página personalizada en la que se le pide que actualice a la versión más reciente de Internet Explorer, Firefox, Chrome o Safari.

**Nota:** Según RFC6176 del Grupo de trabajo de ingeniería de Internet (ITEF), los servidores TLS no deben ser compatibles con SSLv2. Por lo tanto, el dispositivo Citrix ADC no admite SSLv2 a partir de la versión 12.1 y posteriores.

### Cómo crear una página personalizada para pedir a los usuarios que actualicen exploradores antiguos no compatibles basados en SSL

- Cree una directiva de respuesta de Citrix ADC con la regla `client.ssl.version.eq()`. La versión devuelve la versión del protocolo SSL.
  - Devuelve 0 si la transacción no está basada en SSL.
  - Devuelve 0x002 si la transacción es SSLv2.
  - Devuelve 0x300 si la transacción es SSLv3.
  - Devuelve 0x301 si la transacción es TLSv1.
- Debe habilitar SSLv3 (u otra versión anterior) para activar la directiva de respuesta.

  Por ejemplo, si SSLv3 está inhabilitado en el dispositivo Citrix ADC y un cliente con un explorador antiguo que utiliza SSLv3 intenta conectarse, se deniega el acceso.
- Si la implementación requiere SSLv3 o una versión anterior durante un período específico (uno o dos meses), configure lo siguiente:
  - Habilite el protocolo SSLv3.
  - Actualice la página personalizada para incluir información de que, transcurrido el período especificado, el explorador no puede conectarse al dispositivo.

## Configurar el acceso sin cliente

January 26, 2024

El acceso sin cliente permite a los usuarios el acceso que necesitan sin necesidad de instalar software de usuario, como el plug-in de NetScaler Gateway o Receiver. Los usuarios pueden utilizar su explorador web para conectarse a aplicaciones web, como Outlook Web Access.

Siga los pasos siguientes para configurar el acceso sin cliente:

- Habilitar el acceso sin cliente de forma global o mediante una directiva de sesión vinculada a un usuario, grupo o servidor virtual.
- Selección del método de codificación de direcciones web.

Para habilitar el acceso sin cliente solo para un servidor virtual específico, inhabilite el acceso sin cliente globalmente y, a continuación, cree una directiva de sesión para habilitarlo.

Si utiliza el asistente de NetScaler Gateway para configurar el dispositivo, tiene la opción de configurar el acceso sin cliente en el asistente. La configuración del asistente se aplica de forma global. En el asistente de NetScaler Gateway, puede configurar los siguientes métodos de conexión de clientes:

- Plug-in de NetScaler Gateway. Los usuarios solo pueden iniciar sesión mediante el plug-in de NetScaler Gateway.
- Utilice el plug-in de NetScaler Gateway y permita el respaldo del caso de acceso. Los usuarios inician sesión en NetScaler Gateway con el plug-in de NetScaler Gateway. Si el dispositivo de usuario no supera la exploración de análisis de dispositivos de punto final, los usuarios pueden iniciar sesión mediante el acceso sin cliente. Cuando esto ocurre, los usuarios tienen acceso limitado a los recursos de red.
- Permitir que los usuarios inicien sesión mediante un explorador web y acceso sin cliente. Los usuarios solo pueden iniciar sesión mediante el uso de acceso sin cliente y recibir acceso limitado a los recursos de red.

## Habilitar el acceso sin cliente

March 27, 2024

Al habilitar el acceso sin cliente a nivel global, todos los usuarios reciben la configuración del acceso sin cliente. Puede utilizar el asistente de NetScaler Gateway, una directiva global o una directiva de sesión para habilitar el acceso sin cliente.

En una configuración global o en un perfil de sesión, el acceso sin cliente tiene la siguiente configuración:

- **Enciendo**. Permite el acceso sin cliente. Si inhabilita las opciones del cliente y no configura ni inhabilita StoreFront, los usuarios inician sesión mediante el acceso sin cliente.
- **Desactivado**. El acceso sin cliente no está habilitado de forma predeterminada. El acceso sin cliente se habilita después de que los usuarios inicien sesión con el plug-in de NetScaler Gateway. Si inhabilita las opciones del cliente y no configura ni inhabilita StoreFront, los usuarios inician sesión con el plug-in de NetScaler Gateway. Si el análisis de dispositivos de punto final falla cuando los usuarios inician sesión, los usuarios reciben la página de opciones con acceso sin cliente disponible.
- **Inhabilitado**. El acceso sin cliente está inhabilitado. Al seleccionar **Inhabilitado**, los usuarios no pueden iniciar sesión mediante el acceso sin cliente y el icono de acceso sin cliente no aparece en la página de opciones.

Si no habilita el acceso sin cliente mediante el asistente de NetScaler Gateway, puede habilitarlo globalmente o en una directiva de sesión mediante la utilidad de configuración.

### Para habilitar el acceso sin cliente de forma global

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En la ficha **Experiencia del cliente**, junto a **Acceso sin cliente**, seleccione ACTIVADO y **, a continuación,** haga clic en **Aceptar**.

### Para habilitar el acceso sin cliente mediante una directiva de sesión

Si quiere que solo un grupo selecto de usuarios, grupos o servidores virtuales utilice el acceso sin cliente, desactive o borre el acceso sin cliente de forma global. A continuación, mediante una directiva de sesión, habilite el acceso sin cliente y vincúlelo a usuarios, grupos o servidores virtuales.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas > Sesión**.
2. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En la pestaña **Experiencia del cliente** , junto a Acceso sin cliente, haga clic en **Anular global** , seleccione Activado y**,** a continuación , haga clic en **Crear**.
7. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresiones con nombre**, seleccione General, seleccione Valor verdadero, haga clic en Agregar expresión, en **Crear** y, a continuación, en **Cerrar**.
8. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Después de crear la directiva de sesión que permite el acceso sin cliente, la vincula a un usuario, grupo o servidor virtual.

## Cifrar la dirección web

March 27, 2024

Al habilitar el acceso sin cliente, puede optar por codificar las direcciones de las aplicaciones web internas o dejar la dirección como texto sin cifrar. Los ajustes son los siguientes:

- Oscuro. Utiliza mecanismos de codificación estándar para ocultar la parte del dominio y el protocolo del recurso.
- Claro. La dirección web no está codificada y es visible para los usuarios.

- Cifrar. El dominio y el protocolo se cifran mediante una clave de sesión. Cuando la dirección web está cifrada, la URL es diferente para cada sesión de usuario del mismo recurso web. Si los usuarios marcan la dirección web codificada como marcador, la guardan en el explorador web y luego cierras la sesión, cuando los usuarios inician sesión e intentan conectarse de nuevo a la dirección web mediante el marcador, no podrán conectarse a la dirección web.
  Nota: Si los usuarios guardan el marcador cifrado en la interfaz de acceso durante su sesión, el marcador funciona cada vez que el usuario inicia sesión.

Puede configurar esta configuración de forma global o como parte de una directiva de sesión. Si configura la codificación como parte de la directiva de sesión, puede vincularla a los usuarios, grupos o un servidor virtual.

### Para configurar la codificación de direcciones web de forma global

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Experiencia del cliente, junto a Codificación URL de acceso sin cliente, seleccione el nivel de codificación y, a continuación, haga clic en Aceptar.

### Para configurar la codificación de direcciones web mediante la creación de una política de sesión

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En Nombre , escriba un nombre para el perfil.
6. En la pestaña Experiencia del cliente, junto a Codificación de URL de acceso sin cliente, haga clic en Anular global, seleccione el nivel de codificación y, a continuación, haga clic en Aceptar.
7. En el cuadro de diálogo Crear política de sesión , junto a Expresiones con nombre , seleccione General, seleccione Valor verdadero , haga clic en Agregar expresión , en Crear y, a continuación, en Cerrar .

## Cómo funcionan las políticas de acceso sin cliente

January 26, 2024

El acceso sin cliente a las aplicaciones web se configura mediante la creación de directivas. Puede configurar la configuración de una directiva de acceso sin cliente en la utilidad de configuración. Una directiva de acceso sin cliente se compone de una regla y un perfil. Puede utilizar las directivas de acceso sin cliente preconfiguradas que vienen con NetScaler Gateway. También puede crear sus propias directivas de acceso sin cliente personalizadas.

NetScaler Gateway proporciona directivas preconfiguradas para lo siguiente:

- Outlook Web Access y Outlook Web App
- SharePoint 2007
- Todas las demás aplicaciones web

> **Nota:**
>
> OWA 2016 y SharePoint 2016 solo son compatibles con el acceso avanzado sin cliente.

Tenga en cuenta las siguientes funciones de las directivas de acceso sin cliente preconfiguradas:

- Se configuran automáticamente y no se pueden cambiar.
- Cada directiva está vinculada a nivel global.
- Cada directiva no se aplica a menos que habilite el acceso sin cliente de forma global o mediante la creación de una directiva de sesión.
- No puede quitar ni modificar los enlaces globales, aunque no habilite el acceso sin cliente.

La compatibilidad con otras aplicaciones web depende de las directivas de reescritura configuradas en NetScaler Gateway. Citrix recomienda probar todas las directivas personalizadas que cree para asegurarse de que todos los componentes de la aplicación se reescriban correctamente.

Si permite conexiones desde Receiver para Android, Receiver para iOS o Citrix Secure Hub, debe habilitar el acceso sin cliente. Para Citrix Secure Hub que se ejecuta en un dispositivo iOS, también debe habilitar Secure Browse en el perfil de sesión. Secure Browse y el acceso sin cliente funcionan conjuntamente para permitir conexiones desde dispositivos iOS. No tiene que habilitar Secure Browse si los usuarios no se conectan con dispositivos iOS.

El asistente de configuración rápida configura las directivas y la configuración de acceso sin cliente correctas para los dispositivos móviles. Citrix recomienda ejecutar el Asistente de configuración rápida para configurar las directivas correctas para las conexiones a StoreFront y Citrix Endpoint Management.

Puede enlazar directivas de acceso sin cliente personalizadas de forma global o a un servidor virtual. Si quiere vincular directivas de acceso sin cliente a un servidor virtual, debe crear una directiva personalizada y, a continuación, vincularla. Para aplicar directivas diferentes para el acceso sin cliente, ya sea de forma global o para un servidor virtual, cambie el número de prioridad de la directiva personalizada para que tenga un número inferior al de las directivas preconfiguradas, dando así mayor

prioridad a la directiva personalizada. Si no hay ninguna otra directiva de acceso sin cliente vinculada al servidor virtual, las directivas globales preconfiguradas tienen prioridad.

Nota: No puede cambiar los números de prioridad de las políticas de acceso sin cliente preconfiguradas.

## Crear nuevas directivas de acceso sin cliente

March 27, 2024

Si quiere utilizar la misma configuración que para las directivas de acceso sin cliente predeterminadas pero quiere enlazar la directiva a un servidor virtual, puede copiar las directivas predeterminadas y proporcionar un nuevo nombre para la directiva. Puede utilizar la utilidad de configuración para copiar las directivas predeterminadas.

Después de vincular la nueva directiva al servidor virtual, puede establecer la prioridad de la directiva para que se ejecute primero cuando un usuario inicie sesión.

### Para crear una nueva política de acceso sin cliente mediante la configuración predeterminada

1. En la utilidad de configuración, en el panel de navegación, expanda NetScaler Gateway > Directivas y, a continuación, haga clic en Acceso sin cliente.
2. En el panel de detalles, en la ficha Directivas, haga clic en una directiva predeterminada y, a continuación, haga clic en Agregar.
3. En Nombre, escriba un nombre nuevo para la política, haga clic en Crear y, a continuación, en Cerrar.

### Para enlazar una directiva de acceso sin cliente a un servidor virtual

Después de crear la nueva directiva, vincúlala al servidor virtual.

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en Abrir .
3. En el cuadro de diálogo configurar el servidor virtual de NetScaler Gateway, haga clic en la ficha Directivas y, a continuación, haga clic en Sin cliente.
4. Haga clic en Insertar política, seleccione una política de la lista y, a continuación, haga clic en Aceptar.

### Creación y evaluación de expresiones de política de acceso sin cliente

Al crear una nueva política para el acceso sin cliente, puede crear su propia expresión para la política. Cuando haya terminado de crear la expresión, podrá evaluar la exactitud de la expresión.

1. En la utilidad de configuración, en el panel de navegación, expanda NetScaler Gateway > Directivas y, a continuación, haga clic en Acceso sin cliente.
2. En el panel de detalles, en la ficha Directivas, haga clic en una directiva predeterminada y, a continuación, haga clic en Agregar.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Perfil, haz clic en Nuevo .
5. En Nombre , escriba un nombre para el perfil.
6. Configure los ajustes de reescritura y, a continuación, haga clic en Crear.
7. En el cuadro de diálogo Crear directiva de acceso sin cliente, en Expresión, haga clic en Agregar.
8. En el cuadro de diálogo Agregar expresión, cree la expresión y, a continuación, haga clic en Aceptar.
9. En el cuadro de diálogo Crear directiva de acceso sin cliente, haga clic en Evaluar y, si la expresión es correcta, haga clic en Crear.

## Acceso VPN avanzado sin cliente con NetScaler Gateway

January 26, 2024

La VPN sin cliente ve una forma de proporcionar acceso remoto a los recursos de la intranet de la empresa a través de NetScaler Gateway sin una aplicación cliente VPN en el equipo cliente. La VPN sin cliente proporciona acceso remoto a aplicaciones web empresariales, portales y otros recursos mediante un explorador web en el extremo del cliente.
La solución avanzada de VPN sin cliente elimina las siguientes limitaciones relacionadas con la VPN sin cliente:

- Las URL relativas no se pueden identificar a veces.
- Las URL relativas generadas dinámicamente no se pueden identificar.

Advanced Clientless VPN identifica la URL absoluta y los nombres de host y los reescribe de una manera nueva y única en lugar de intentar reescribir las URL relativas presentes en las respuestas HTTP o en las páginas web. SharePoint ya no necesita usar la carpeta predeterminada para reescribir direcciones URL y se admite un acceso personalizado a SharePoint.

### Requisitos previos

Los siguientes son los requisitos previos para configurar la VPN avanzada sin cliente.

- **Certificado**de servidor Wildcard : la VPN avanzada sin cliente reescribe las URL de una manera única. Esta singularidad se mantiene para cada URL por usuario. Por ejemplo, si la aplicación web está alojada en `https://webapp.customer.com`, y el servidor virtual VPN está alojado en `https://vpn.customer.com`, la VPN avanzada sin cliente la reescribe como `https://cvpneqwerty.vpn.customer.com`. Esto significa que cada URL se reescribe como subdominio del servidor virtual VPN. En esta nueva URL, `cvpneqwerty` se puede descifrar de vuelta a `https://webapp.customer.com`. La cadena `cvpneqwerty` es dinámica y, por lo tanto, para SSL, debe vincular el servidor virtual VPN con un certificado comodín.

  Si el servidor está alojado en `https://vpn.customer.com`, el certificado del servidor debe tener entradas para (vpn.customer.com y .vpn.customer.com) como parte de los certificados CN o SAN (donde CN = nombre común, SAN= nombre alternativo del sujeto). El proceso de vinculación de este certificado sigue siendo el mismo en NetScaler Gateway.
  **Nota:** Los certificados comodín solo admiten un nivel (es decir, ..cliente.com no está permitido). Si ya utiliza un certificado comodín (para *.customer.com) y alojamiento `https://vpn.customer.com`, esto no funciona para la VPN avanzada sin cliente. Debe obtener un nuevo certificado con `*.vpn.customer.com`.

- **Entrada DNS comodín**: Los clientes (exploradores web) deben resolver el FQDN de la aplicación VPN avanzada sin cliente. Al configurar el servidor NetScaler Gateway, debe haber configurado una entrada DNS para resolver vpn.customer.com. Esto permite que el explorador resuelva vpn.customer.com en la dirección IP de su servidor virtual VPN. Para resolver direcciones URL como `https://cvpnqwerty.vpn.customer.com` en la misma IP (dirección IP del servidor virtual VPN), debe agregar un nuevo registro para el dominio de `vpn.customer.com`. Busque la configuración del dominio en su servidor DNS y añada un registro de host para «*» con la misma dirección IP que antes. Después de agregar el registro de host, debe ver las respuestas ping correctas para `https://cpvnanything.vpn.customer.com`.

### Configurar el acceso VPN avanzado sin cliente

**Para configurar el acceso VPN avanzado sin cliente mediante la interfaz de línea de comandos, en el símbolo del sistema, escriba:**

```
set vpn parameter -clientlessVpnMode ON
set vpn parameter -advancedClientlessVpnMode ENABLED
<!--NeedCopy-->
```

Si una acción de sesión está vinculada al servidor virtual, debe habilitar también la opción Modo VPN avanzado sin cliente para esa acción de sesión.

**Ejemplo:**

```
set vpn sessionaction SessionActionName -advancedclientlessvpn ENABLED
<!--NeedCopy-->
```

**Para configurar el acceso VPN sin cliente avanzado mediante la GUI de Citrix ADC:**

1. En la GUI de NetScaler, vaya a **Configuración > Citrix NetScaler > Configuración global.**
2. En la **página Configuración global**, haga clic en **Cambiar configuración global** y, a continuación, seleccione la ficha **Experiencia del cliente**.
3. En la ficha **Experiencia del cliente**, en la lista **Acceso sin cliente**, haga clic **en On**.
4. En la ficha **Experiencia del cliente**, en la lista **Modo VPN sin cliente avanzado**, haga clic en **Habilitado**.

   Si selecciona **STRICT** en la lista del **modo VPN sin cliente avanzado** , el dispositivo Citrix ADC solo responde a las URL de StoreFront en el formato clásico de VPN sin cliente y bloquea todas las demás solicitudes clásicas de VPN sin cliente. Esta opción proporciona una configuración más segura en el dispositivo para entregar recursos web internos.

> **Nota:**
>
> - Si una acción de sesión está enlazada al servidor virtual, debe habilitar la opción **Modo VPN sin cliente avanzado** para esa acción de sesión también desde la ficha **Experiencia del cliente** en la página **Configurar perfil de sesión de NetScaler Gateway**.
> - Puede seleccionar la opción **Supedición global** para anular la configuración global.
> - También puede configurar la función VPN avanzada sin cliente a nivel de sesión.

## Advertencias

La VPN avanzada sin cliente tiene como objetivo proporcionar acceso a las aplicaciones web empresariales. Estas aplicaciones solo tienen un FQDN para cada tipo de recurso que necesitan (JavaScript, css, imágenes, etc.). Dado que codificamos el FQDN completo de las aplicaciones internas en un solo octeto (VPN sin cliente), perdemos la relación de subdominio. Como resultado, cada vez que se configura una aplicación web empresarial con CORS, a veces se observan problemas al acceder a ella a través de la VPN avanzada sin cliente.

# Configurar acceso de dominio para usuarios

March 27, 2024

Si los usuarios se conectan mediante el acceso sin cliente, puede restringir los recursos de red, los dominios y los sitios web a los que pueden acceder los usuarios. Puede utilizar el asistente de NetScaler Gateway o la configuración global para crear listas para incluir o excluir el acceso a los dominios.

Puede permitir el acceso a todos los recursos de red, dominios y sitios web y, a continuación, crear una lista de exclusión. La lista de exclusión cita un conjunto específico de recursos al que los usuarios no pueden acceder. Los usuarios no pueden acceder a los dominios incluidos en la lista de exclusión.

También puede denegar el acceso a todos los recursos de red, dominios y sitios web y, a continuación, crear una lista de inclusión específica. En la lista de inclusión se citan los recursos a los que pueden acceder los usuarios. Los usuarios no pueden acceder a ningún dominio que no aparezca en la lista.

Nota: Si configura directivas de acceso sin cliente para Citrix Endpoint Management o StoreFront y los usuarios se conectan con Receiver para Web, debe permitir los dominios a los que puede acceder Receiver para Web. Esto es necesario para que NetScaler Gateway pueda reescribir el tráfico de red de StoreFront y Endpoint Management.

### Para configurar el acceso al dominio mediante el asistente de NetScaler Gateway

1. En la utilidad de configuración, haga clic en la pestaña Configuración y, a continuación, en el panel de navegación, haga clic en Citrix Gateway .
2. En el panel de detalles, en Introducción, haga clic en el asistente Citrix Gateway .
3. Haga clic en Siguiente y, a continuación, siga las instrucciones del asistente hasta llegar a la página Configurar acceso sin cliente.
4. Haga clic en Configurar dominios para acceso sin cliente y realice una de las siguientes acciones:
    - Para crear una lista de dominios excluidos, haga clic en Excluir dominios.
    - Para crear una lista de dominios incluidos, haga clic en Permitir dominios.
5. En Nombres de dominio, escriba el nombre de dominio y, a continuación, haga clic en Agregar.
6. Repita el paso 5 para cada dominio que quiera agregar a la lista y, a continuación, haga clic en Aceptar cuando haya terminado.
7. Siga configurando el dispositivo mediante el asistente de NetScaler Gateway.

### Para configurar la configuración del dominio mediante la utilidad de configuración

También puede crear o modificar la lista de dominios mediante la configuración global de la utilidad de configuración.

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Acceso sin cliente, haga clic en Configurar dominios para acceso sin cliente.
3. Lleve a cabo una de las siguientes acciones:
   - Para crear una lista de dominios excluidos, haga clic en Excluir dominios.
   - Para crear una lista de dominios incluidos, haga clic en Permitir dominios.
4. En Nombres de dominio, escriba el nombre de dominio y, a continuación, haga clic en Agregar.
5. Repita el paso 4 para cada dominio que quiera agregar a la lista y, a continuación, haga clic en Aceptar cuando haya terminado.

## Configurar el acceso sin cliente para SharePoint 2003, SharePoint 2007 y SharePoint 2013

January 26, 2024

NetScaler Gateway puede reescribir contenido de uno o más sitios de SharePoint 2003, SharePoint 2007 o SharePoint 2013 para que el contenido esté disponible para los usuarios sin necesidad del plug-in de NetScaler Gateway. Para que el proceso de reescritura se complete correctamente, debe configurar NetScaler Gateway con el nombre de host de cada servidor SharePoint de la red.

Puede utilizar el asistente de NetScaler Gateway o la utilidad de configuración para configurar el nombre de host de los sitios de SharePoint.

En el asistente de NetScaler Gateway, avance por el asistente para configurar la configuración. Cuando llegue a la página Configurar el acceso sin cliente, escriba la dirección web del sitio de SharePoint y, a continuación, haga clic en **Agregar**.

Para agregar sitios web adicionales o configurar SharePoint por primera vez después de ejecutar el asistente de Citrix Gateway, utilice la utilidad de configuración.

> **Importante:**Classic Clientless Access admite versiones hasta SharePoint 2013 y OWA13. Advanced Clientless Access admite versiones posteriores.

### Para configurar el acceso sin cliente para SharePoint mediante la GUI de Citrix ADC

1. Vaya a **NetScaler Gateway** > **Configuración global**.
2. En el panel de detalles, en Acceso sin cliente, haga clic en **Configurar acceso sin cliente para SharePoint**.

3. En Acceso sin cliente para SharePoint, en Nombre de host del servidor de SharePoint, escriba el nombre de host del sitio de SharePoint y, a continuación, haga clic en **Agregar**.
4. Repita el paso 3 para cada sitio de SharePoint que quiera agregar a la lista y, a continuación, haga clic en **Aceptar** cuando haya terminado.

## Configuración de un sitio de SharePoint como página de inicio

March 27, 2024

Si quiere establecer un sitio de SharePoint como página principal de los usuarios, configure un perfil de sesión e introduzca el nombre de host del sitio de SharePoint.

### Para configurar un sitio de SharePoint como página principal

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **Citrix Gateway > Directivas y, a continuación,** haga clic en **Sesión** .
2. En el panel de detalles, haga clic en **Agregar**.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en **Nuevo** .
5. En Nombre , escriba un nombre para el perfil.
6. En la pestaña Experiencia del cliente, junto a la página de inicio, haga clic en **Anular global** y, a continuación, escriba el nombre del sitio de SharePoint.
7. Junto a Acceso sin cliente, haga clic en **Sobrescribir global**, seleccione **Activado y,** a continuación, haga clic en **Crear**.
8. En el cuadro de diálogo Crear directiva de sesión, junto a Expresiones con nombre, seleccione **General**, seleccione **Valor verdadero**, haga clic en **Agregar expresión**, en **Crear** y, a continuación, en **Cerrar**.

Después de completar la directiva de sesión, enlaza a usuarios, grupos, servidores virtuales o de forma global. Cuando los usuarios inician sesión, ven el sitio web de SharePoint como su página principal.

## Habilitar la resolución de nombres para servidores de SharePoint 2007

January 26, 2024

Los servidores de SharePoint 2007 envían el nombre del servidor configurado como nombre de host dentro de varias URL como parte de la respuesta. Si un nombre de servidor de SharePoint configu-

rado no es el nombre de dominio completo (FQDN), NetScaler Gateway no puede resolver la dirección IP mediante el nombre del servidor de SharePoint y algunas funciones de usuario se agotan con el mensaje de error "HTT:1.1 Tiempo de espera de puerta de enlace". Estas funciones pueden incluir la entrada y salida de archivos, ver el espacio de trabajo y cargar varios archivos cuando los usuarios inician sesión mediante el acceso sin cliente.

Para resolver este problema, puede probar una de las siguientes opciones:

- Configure un sufijo DNS en NetScaler Gateway para que el nombre de host de SharePoint se convierta en un FQDN antes de la resolución de nombres.
- Configure una entrada DNS local en NetScaler Gateway para cada nombre de servidor de SharePoint.
- Cambie todos los nombres de servidor de SharePoint para usar el FQDN, como SharePoint.intranetdomain en lugar de SharePoint.

### Para configurar un sufijo DNS

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda DNS y, a continuación, haga clic en Sufijo DNS.
2. En el panel de detalles, haga clic en Agregar.
3. En Sufijo DNS, escriba el nombre de dominio de la intranet como sufijo, haga clic en Crear y, a continuación, en Cerrar.

Puede repetir el paso 3 para cada dominio que quieras agregar.

### Para configurar un registro DNS local para cada nombre de servidor de SharePoint en NetScaler Gateway

1. En la utilidad de configuración, en el panel de navegación, expanda DNS > Registros y, a continuación, haga clic en Registros de direcciones.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre de host, escriba el nombre de host de SharePoint para el registro de direcciones DNS.
4. En Dirección IP, escriba la dirección IP del servidor de SharePoint, haga clic en Agregar, en Crear y, a continuación, en Cerrar.

El nombre de host para el que se agrega un registro A no debe tener un registro CNAME. Además, no puede haber registros A duplicados en el dispositivo.

## Habilitar cookies persistentes de acceso sin cliente

January 26, 2024

Las cookies persistentes son necesarias para acceder a determinadas funciones de SharePoint, como abrir y modificar documentos de Microsoft Word, Excel y PowerPoint alojados en el servidor de SharePoint.

Una cookie persistente permanece en el dispositivo del usuario y se envía con cada solicitud HTTP. NetScaler Gateway cifra la cookie persistente antes de enviarla al complemento del dispositivo del usuario y la actualiza periódicamente mientras exista la sesión. La cookie se vuelve obsoleta si finaliza la sesión.

En el asistente de NetScaler Gateway, los administradores pueden habilitar las cookies persistentes de forma global. También puede crear una directiva de sesión para habilitar las cookies persistentes por usuario, grupo o servidor virtual.

Las siguientes opciones están disponibles para las cookies persistentes:

- Permitir habilita las cookies persistentes y los usuarios pueden abrir y modificar documentos de Microsoft almacenados en SharePoint.
- Denegar inhabilita las cookies persistentes y los usuarios no pueden abrir y modificar documentos de Microsoft almacenados en SharePoint.
- Prompt solicita a los usuarios que permitan o rechacen las cookies persistentes durante la sesión.

Las cookies persistentes no son necesarias para el acceso sin cliente si los usuarios no se conectan a SharePoint.

## Configurar cookies persistentes para acceso sin cliente para SharePoint

March 27, 2024

Puede configurar cookies persistentes para el acceso sin cliente de SharePoint de forma global o como parte de una directiva de sesión.

### Para configurar las cookies persistentes de forma global

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.

2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Experiencia del cliente, junto a Cookies persistentes de acceso sin cliente, seleccione una opción y, a continuación, haga clic en Aceptar.

### Para configurar las cookies persistentes como parte de una directiva de sesión

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En Nombre , escriba un nombre para el perfil.
6. En la pestaña Experiencia del cliente, junto a Cookies persistentes de acceso sin cliente, haga clic en Anular global, seleccione una opción y, a continuación, haga clic en Crear.
7. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione General, Valor verdadero, haga clic en Agregar expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

## Guardar la configuración de usuario para el acceso sin cliente a través de la Interfaz Web

March 27, 2024

Cuando los usuarios inician y citan sesión en la interfaz web mediante el acceso sin cliente, NetScaler Gateway no reenvía el conjunto de cookie consumidas por el cliente de la sesión anterior, incluso si las cookies son persistentes cuando los usuarios inician sesión varias veces. Puede usar la utilidad de configuración o la línea de comandos para vincular las cookies a un conjunto de patrones de cookies de cliente a fin de conservar la configuración de la Interfaz Web entre sesiones.

### Para enlazar cookies para la persistencia de la interfaz web mediante la utilidad de configuración

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway > Directivas y, a continuación, haga clic en Acceso sin cliente.
2. En el panel derecho, en la ficha Directivas, haga clic en Agregar.
3. En el cuadro de diálogo Crear directiva de acceso sin cliente, en Nombre, escriba un nombre para la directiva.

4. Junto a Perfil, haz clic en Nuevo .
5. En Nombre , escriba un nombre para el perfil.
6. En la ficha Cookies de cliente, en Cookies de cliente, seleccione ns_cvpn_default_client_cookies y, a continuación, haga clic en Modificar.
7. En el cuadro de diálogo Configurar conjunto de patrones, en Especificar patrón, en Patrón, introduzca los siguientes parámetros:
    - WiUser y, a continuación, haga clic en Agregar.
    - WingDevice y, a continuación, haga clic en Agregar.
    - WingSession y, a continuación, haga clic en Agregar.
8. Haga clic en Aceptar y, a continuación, en Crear
9. En el cuadro de diálogo Crear directiva de acceso sin cliente, en Expresión, escriba true, haga clic en Crear y, a continuación, haga clic en Cerrar.

### Para enlazar cookies para la persistencia de la interfaz web mediante la línea de comandos

1. Inicie sesión en la línea de comandos de NetScaler Gateway mediante una conexión Secure Shell (SSH), como PuTTY.
2. En el símbolo del sistema, escriba shell.
3. En el símbolo del sistema, introduzca los siguientes comandos:
    - vincule la política patset ns_cvpn_default_client_cookies WiUser y, a continuación, presione ENTER.
    - vincule la política patset ns_cvpn_default_client_cookies WingDevice y, a continuación, presione ENTRAR.
    - enlace la política patset ns_cvpn_default_client_cookies WingSession y, a continuación, presione ENTRAR.

## Cliente VPN de Citrix SSO para dispositivos móviles

January 26, 2024

Citrix SSO es el cliente VPN para dispositivos móviles (macOS, iOS e iOS). Citrix SSO proporciona compatibilidad completa con la administración de dispositivos móviles (MDM) en macOS, iOS y Android. Con un servidor MDM, un administrador puede configurar y administrar de forma remota perfiles VPN a nivel de dispositivo y perfiles VPN por aplicación.
Citrix SSO también admite la mayoría de las funciones de uso común.

### Referencias

- Clientes de NetScaler Gateway
- Clientes VPN de NetScaler Gateway y funciones compatibles

## Página Configurar selección de cliente

January 26, 2024

Puede configurar NetScaler Gateway para que proporcione a los usuarios varias opciones de inicio de sesión. Al configurar la página de opciones del cliente, los usuarios tienen la opción de iniciar sesión desde una ubicación con las siguientes opciones:

- Plug-in de NetScaler Gateway para Windows
- Plug-in de NetScaler Gateway para Mac OS X
- Plug-in de NetScaler Gateway para Java
- StoreFront
- Interfaz Web
- Acceso sin cliente

Los usuarios inician sesión en NetScaler Gateway mediante la dirección web del certificado vinculado a NetScaler Gateway o al servidor virtual. Al crear una directiva y un perfil de sesión, puede determinar las opciones de inicio de sesión que reciben los usuarios. Según cómo configure NetScaler Gateway, la página de opciones del cliente muestra hasta tres iconos que representan las siguientes opciones de inicio de sesión:

- Acceso a la red. Cuando los usuarios inician sesión en NetScaler Gateway por primera vez mediante un explorador web y, a continuación, seleccionan Acceso a la red, aparece la página de descarga. Cuando los usuarios hacen clic en Descargar, el complemento se descarga e instala en el dispositivo del usuario. Cuando finaliza la descarga y la instalación, aparece la interfaz de acceso. Si instala una versión más reciente o vuelve a una versión anterior de NetScaler Gateway, el plug-in de NetScaler Gateway para Windows actualiza o reduce de forma silenciosa la versión del dispositivo. Si los usuarios se conectan mediante el plug-in de NetScaler Gateway para Mac, el complemento se actualiza de forma silenciosa si se detecta una nueva versión del dispositivo cuando los usuarios inician sesión. Esta versión del plug-in no baja de forma silenciosa.
- Interfaz web o StoreFront. Si los usuarios seleccionan la Interfaz Web para iniciar sesión, aparece la página Interfaz Web. Los usuarios pueden acceder a sus aplicaciones publicadas o escritorios virtuales. Si los usuarios seleccionan StoreFront para iniciar sesión, Receiver se abre y los usuarios pueden acceder a las aplicaciones y los escritorios.

Nota: Si configura StoreFront como opción del cliente, las aplicaciones y los escritorios no aparecen en el panel izquierdo de la interfaz de acceso.

- Acceso sin cliente. Si los usuarios seleccionan el acceso sin cliente para iniciar sesión, aparece la interfaz de acceso o la página principal personalizada. En la interfaz de acceso, los usuarios pueden navegar a recursos compartidos de archivos, sitios web y usar Outlook Web Access.

Si los usuarios seleccionan el plug-in de NetScaler Gateway para Java, el complemento se inicia y los usuarios inician sesión. La página de opciones no aparece.

Secure Browse permite a los usuarios conectarse a través de NetScaler Gateway desde un dispositivo iOS. Si habilita Secure Browse, cuando los usuarios inician sesión con Secure Hub, Secure Browse inhabilita la página de opciones del cliente.

## Mostrar la página Selección de cliente al iniciar sesión

March 27, 2024

Al habilitar la opción de opciones de cliente, los usuarios pueden iniciar sesión con el plug-in de NetScaler Gateway, la interfaz web, Receiver o el acceso sin cliente desde una página web tras la autenticación correcta en NetScaler Gateway. Cuando el inicio de sesión se realiza correctamente, aparecen iconos en la página web desde los que los usuarios pueden elegir el método para establecer una conexión. También puede configurar el plug-in de NetScaler Gateway para Java para que aparezca en la página de opciones.

Puede habilitar las opciones del cliente sin utilizar el análisis de dispositivos de punto final ni implementar el respaldo de casos de acceso. Si no define una expresión de seguridad del cliente, los usuarios reciben opciones de conexión para la configuración configurada en NetScaler Gateway. Si existe una expresión de seguridad de cliente para la sesión de usuario y el dispositivo de usuario falla el análisis del punto final, la página de opciones solo ofrece la opción de utilizar la Interfaz Web si está configurada. De lo contrario, los usuarios pueden utilizar el acceso sin cliente para iniciar sesión.

Las opciones del cliente se configuran de forma global o mediante un perfil y una directiva de sesión.

> **Importante:**Al configurar las opciones del cliente, no configure los grupos de cuarentena. Los dispositivos de usuario que no superan el análisis de punto final se ponen en cuarentena y se tratan de la misma manera que los dispositivos de usuario que pasan el análisis de punto final.

### Para habilitar las opciones de elección de los clientes a nivel mundial

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.

2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la pestaña Experiencia del cliente, haga clic en Configuración avanzada .
4. En la pestaña General, haga clic en Opciones del cliente y, a continuación, en Aceptar.

### Para habilitar las opciones del cliente como parte de una política de sesión

También puede configurar las opciones de cliente como parte de una directiva de sesión y, a continuación, vincularlas a usuarios, grupos y servidores virtuales.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Citrix Gateway \ > Directivas** y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En Nombre , escriba un nombre para el perfil.
6. En la ficha Experiencia del cliente, haga clic en Avanzado.
7. En la pestaña General, junto a Opciones del cliente, haga clic en Anular global, en Opciones del cliente, en Aceptar y, a continuación, en Crear.
8. En el cuadro de diálogo Crear política de sesión , junto a Expresiones con nombre, seleccione General , seleccione Valor verdadero , haga clic en Agregar expresión , en Crear y, a continuación, en Cerrar .

## Configurar opciones de selección de cliente

March 27, 2024

Además de habilitar las opciones del cliente mediante un perfil y una directiva de sesión, debe configurar la configuración del software de usuario. Por ejemplo, quiere que los usuarios inicien sesión con el plug-in de NetScaler Gateway, StoreFront o la Interfaz Web, o con acceso sin cliente. Se crea un perfil de sesión que habilita las tres opciones y las opciones del cliente. A continuación, se crea una directiva de sesión con la expresión establecida en valor True con el perfil adjunto. A continuación, vincula la directiva de sesión a un servidor virtual.

Antes de crear la directiva y el perfil de sesión, debe crear un grupo de autorización para los usuarios.

### Para crear un grupo de autorización

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **Citrix Gateway\ > Administración de usuarios** y, a continuación, haga clic en **Grupos AAA** .
2. En el panel de detalles, haga clic en **Agregar**.
3. En Nombre del grupo, escriba el nombre del grupo.
4. En la pestaña Usuarios, seleccione los usuarios, haga clic en **Agregar** para cada uno, en **Crear y,** a continuación, en **Cerrar** .

El siguiente procedimiento es un ejemplo de perfil de sesión para las opciones de cliente con el plug-in de NetScaler Gateway, StoreFront y acceso sin cliente.

### Para crear un perfil de sesión para las opciones del cliente

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **Citrix Gateway\ > Directivas** y, a continuación, haga clic en **Sesión** .
2. En el panel de detalles, haga clic en la pestaña **Perfiles** y, a continuación, en **Agregar** .
3. En Nombre , escriba un nombre para el perfil.
4. En la ficha Experiencia del cliente, haga lo siguiente:
    a) Junto a Página de inicio, haz clic en **Anular global** y, a continuación, desmarca Mostrar página de inicio. Esto inhabilita la interfaz de acceso.
    b) Junto a Acceso sin cliente, haz clic en **Anular global** y, a continuación, selecciona DESACTIVAR.
    c) Junto a Tipo de complemento, haz clic en **Anular global** y, a continuación, selecciona Windows/Mac OS X.
    d) Haga clic en **Configuración avanzada** y, junto a **Opciones del cliente**, haga clic en **Supedición global**y haga clic en **Opciones del cliente**.
5. En la pestaña Seguridad, junto a **Acción de autorización predeterminada** , haga clic en **Anular global** y, a continuación, seleccione **PERMITIR** .
6. En la ficha Seguridad, haga clic en **Configuración avanzada**.
7. En Grupos de autorización, haga clic en **Anular global** , en **Agregar y,** a continuación, seleccione el grupo.
8. En la ficha Aplicaciones publicadas, haga lo siguiente:
    a) Junto a ICA Proxy, haga clic en **Anular global** y, a continuación, seleccione **DESACTIVAR**.
    b) Junto a Dirección de interfaz web, haga clic en **Anular global y,** a continuación, escriba la dirección web de StoreFront, comohttp://ipAddress/Citrix/.
    c) Junto al Modo portal de interfaz web, haga clic en **Anular global y,** a continuación, seleccione **COMPACT** .

d) Junto a Dominio de inicio de sesión único, haz clic en **Anular global y,** a continuación, escribe el nombre del dominio.

9. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Si desea utilizar el complemento Citrix Gateway para Java como opción de cliente, en la pestaña **Experiencia del cliente** , en Tipo de complemento, seleccione Java. Si selecciona esta opción, debe configurar una aplicación de intranet y establecer el modo de interceptación en Proxy.

Después de crear el perfil de sesión, cree una directiva de sesión. Dentro de la directiva, seleccione el perfil y defina la expresión en Valor verdadero.

Para utilizar StoreFront como opción de cliente, también debe configurar Secure Ticket Authority (STA) en NetScaler Gateway. El STA está enlazado al servidor virtual.

> **Nota:**Si el servidor que ejecuta StoreFront no está disponible, la opción Citrix Virtual Apps no aparece en la página de opciones.

### Para configurar el servidor STA de forma global

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en**Configuración global**.
2. En el panel de detalles, en Servidores, haga clic en Vincular o desvincular los **servidores STA** que utilizará Secure Ticket Authority.
3. En el cuadro de diálogo **Enlazar/desenlazar servidores STA**, haga clic en **Agregar**.
4. En el cuadro de diálogo **Configurar servidor STA**, en URL, escriba la dirección web del servidor STA y, a continuación, haga clic en **Crear**.
5. Repita los pasos 3 y 4 para agregar más servidores STA y, a continuación, haga clic en Aceptar.

### Para vincular el STA a un servidor virtual

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la pestaña **Aplicaciones publicadas** , en **Secure Ticket Authority** , en **Activo** , seleccione los servidores STA y, a continuación, haga clic **en**Aceptar .

También puede agregar servidores STA en la ficha **Aplicaciones publicadas**.

# Configurar la reserva de escenario de acceso

January 26, 2024

SmartAccess permite a NetScaler Gateway determinar automáticamente los métodos de acceso permitidos para un dispositivo de usuario en función de los resultados de un análisis de puntos finales. El respaldo del escenario de acceso amplía aún más esta capacidad al permitir que un dispositivo de usuario retroceda del plug-in de NetScaler Gateway a la Interfaz Web o StoreFront mediante Citrix Receiver si el dispositivo de usuario no pasa el análisis inicial del punto final.

Para habilitar el escenario alternativo de acceso, configure una directiva posterior a la autenticación que determine si los usuarios reciben o no un método de acceso alternativo al iniciar sesión en Citrix Gateway. Esta directiva posterior a la autenticación se define como una expresión de seguridad del cliente que se configura de forma global o como parte de un perfil de sesión. Si configura un perfil de sesión, el perfil se asocia a una directiva de sesión que, a continuación, enlaza a usuarios, grupos o servidores virtuales. Al habilitar la opción alternativa de casos de acceso, NetScaler Gateway inicia un análisis de dispositivos de punto final tras la autenticación del usuario. Los resultados de los dispositivos de usuario que no cumplen los requisitos de un análisis posterior a la autenticación de reserva son los siguientes:

- Si las opciones de cliente están habilitadas, los usuarios pueden iniciar sesión en la Interfaz Web o StoreFront utilizando solo Receiver.
- Si el acceso sin cliente y las opciones de cliente están inhabilitadas, los usuarios se pueden poner en cuarentena en un grupo que proporciona acceso solo a la Interfaz Web o a StoreFront.
- Si el acceso sin cliente y la Interfaz Web o StoreFront están habilitados en NetScaler Gateway y el proxy ICA está inhabilitado, los usuarios vuelven al acceso sin cliente.
- Si la Interfaz Web o StoreFront no están configuradas y el acceso sin cliente está configurado para permitir, los usuarios recurren al acceso sin cliente.

Cuando se inhabilita el acceso sin cliente, se debe configurar la siguiente combinación de opciones para la reserva del caso de acceso:

- Defina los parámetros de seguridad del cliente para el análisis posterior a la autenticación de reserva.
- Defina la página de inicio de la Interfaz Web.
- Inhabilitar las opciones del cliente.
- Si los dispositivos de usuario fallan en la comprobación de seguridad del cliente, los usuarios se colocan en un grupo de cuarentena que permite el acceso solo a la Interfaz Web o StoreFront y a las aplicaciones publicadas.

# Crear directivas para la reserva de escenarios de acceso

March 27, 2024

Para configurar NetScaler Gateway para la suplencia de casos de acceso, debe crear directivas y grupos de las siguientes maneras:

- Cree un grupo de cuarentena en el que se coloquen los usuarios si se produce un error en la exploración de análisis de dispositivos de punto final.
- Cree una configuración global de Interfaz Web o StoreFront que se utilice si se produce un error en la exploración de análisis de dispositivos de punto final.
- Cree una directiva de sesión que anule la configuración global y, a continuación, vincule la directiva de sesión a un grupo.
- Cree una directiva de seguridad global del cliente que se aplique si se produce un error en el análisis de dispositivos de punto final.

Al configurar el escenario alternativo de acceso, siga las siguientes pautas:

- El uso de opciones de cliente o de respaldo de casos de acceso requiere el complemento Endpoint Analysis para todos los usuarios. Si el análisis de endpoint no se puede ejecutar o si los usuarios seleccionan Omitir exploración durante el análisis, se deniega el acceso a los usuarios.
  Nota: La opción de omitir el análisis se elimina en NetScaler Gateway 10.1, compilación 120.1316.e
- Al habilitar las opciones del cliente, si el dispositivo del usuario no supera el análisis de endpoint, los usuarios se colocan en el grupo de cuarentena. Los usuarios pueden continuar iniciando sesión con el plug-in de NetScaler Gateway o Citrix Receiver en la Interfaz Web o StoreFront.
  Nota: Citrix recomienda no crear un grupo de cuarentena si habilita las opciones del cliente. Los dispositivos de usuario que no superan el análisis de punto final y se ponen en cuarentena reciben el mismo tratamiento que los dispositivos de usuario que pasan el análisis de punto final.
- Si se produce un error en el análisis de endpoint y el usuario se coloca en el grupo de cuarentena, las directivas enlazadas al grupo de cuarentena solo serán efectivas si no hay directivas vinculadas directamente al usuario que tengan un número de prioridad igual o inferior que las directivas vinculadas al grupo de cuarentena.
- Puede utilizar distintas direcciones web para la interfaz de acceso y la Interfaz Web o StoreFront. Al configurar las páginas principales, la página principal de Access Interface tiene prioridad para el plug-in de NetScaler Gateway y la página principal de Web Interface tiene prioridad para los usuarios de Web Interface. La página principal de Receiver tiene prioridad para StoreFront.

### Para crear un grupo de cuarentena

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway > Administración de usuariosy, a continuación, haga clic en Grupos AAA.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre del grupo, escriba un nombre para el grupo, haga clic en Crear y, a continuación, en Cerrar.
   Importante: El nombre del grupo de cuarentena no debe coincidir con el nombre de ningún grupo de dominio al que puedan pertenecer los usuarios. Si el grupo de cuarentena coincide con un nombre de grupo de Active Directory, los usuarios se ponen en cuarentena aunque el dispositivo del usuario supere el análisis de seguridad del análisis de endpoint.

Después de crear el grupo, configure NetScaler Gateway para que vuelva a la Interfaz Web si el dispositivo de usuario no supera la exploración de análisis de endpoint.

### Para configurar los ajustes para poner en cuarentena las conexiones de usuario

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En el cuadro de diálogo Configuración global de NetScaler Gateway, en la ficha Aplicaciones publicadas, junto a Proxy ICA, seleccione DESACTIVADO.
4. Junto a Dirección de Interfaz Web, escriba la dirección web de StoreFront o de la Interfaz Web.
5. Junto a Dominio de inicio de sesión único, escriba el nombre de su dominio de Active Directory y, a continuación, haga clic en Aceptar.

Tras configurar la configuración global, cree una política de sesión que anule la configuración global del proxy ICA y, a continuación, vincule la política de sesión al grupo de cuarentena.

### Para crear una directiva de sesión para Access Scenario Fallback

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En la pestaña Aplicaciones publicadas, junto a ICA Proxy, haga clic en Anular global, seleccione Activar y, a continuación, haga clic en Crear.
6. En el cuadro de diálogo Crear política de sesión , junto a Expresiones con nombre , seleccione General, seleccione Valor verdadero , haga clic en Agregar expresión , en Crear y, a continuación, en Cerrar .

Después de crear la directiva de sesión, enlaza la directiva a un grupo de cuarentena.

### Para enlazar la directiva de sesión al grupo de cuarentena

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway > Administración de usuariosy, a continuación, haga clic en Grupos AAA.
2. En el panel de detalles, seleccione un grupo y, a continuación, haga clic en Abrir.
3. Haga clic en Sesión.
4. En la pestaña Políticas, seleccione Sesión y, a continuación, haga clic en Insertar política.
5. En Nombre de directiva, seleccione la directiva y, a continuación, haga clic en Aceptar.

Después de crear la directiva de sesión y el perfil que habilita la Interfaz Web o StoreFront en NetScaler Gateway, cree una directiva de seguridad global del cliente.

### Para crear una directiva de seguridad de cliente global

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la pestaña Seguridad , haz clic en Configuración avanzada .
4. En Seguridad del cliente, introduzca la expresión. Para obtener más información sobre la configuración de expresiones del sistema, consulte Configuración de expresiones de sistema y Configuración de expresiones de seguridad de cliente compuestas
5. En Quarantine Group, seleccione el grupo que configuró en el procedimiento de grupo y, a continuación, haga clic en Aceptar dos veces.

## Configuración de conexiones para el plug-in de NetScaler Gateway

January 26, 2024

Las conexiones de dispositivos de usuario se configuran definiendo los recursos a los que los usuarios pueden acceder en la red interna. La configuración de conexiones de dispositivos de usuario incluye:

- Definir los dominios a los que se permite el acceso de los usuarios.
- Configuración de direcciones IP para los usuarios, incluidos los grupos de direcciones (IP de intranet).
- Configuración de los ajustes de tiempo de espera.

- Configuración del inicio de sesión único.
- Configuración de la interceptación de clientes.
- Configuración de túneles divididos.
- Configuración de conexiones a través de un servidor proxy.
- Configuración del software de usuario para conectarse a través de NetScaler Gateway.
- Configuración del acceso para dispositivos móviles.

La mayoría de las conexiones de dispositivos de usuario se configuran mediante un perfil que forma parte de una directiva de sesión. También puede definir la configuración de conexión del dispositivo de usuario mediante aplicaciones de intranet, autenticación previa y directivas de tráfico.

## Configurar el número de sesiones de usuario

March 27, 2024

Puede configurar el número máximo de usuarios a los que se les permite conectarse a NetScaler Gateway en un momento determinado, ya sea a nivel global o a nivel de servidor virtual. Las sesiones no se crean en NetScaler Gateway cuando el número de usuarios que se conectan al dispositivo supera el valor configurado. Si el número de usuarios supera el número permitido, los usuarios reciben un mensaje de error.

### Para establecer el límite global de usuarios

Al configurar el límite de usuarios de forma global, la restricción se aplica a todos los usuarios que establecen sesiones en distintos servidores virtuales del sistema. Cuando el número de sesiones de usuario alcanza el valor establecido, no se pueden establecer nuevas sesiones en ningún servidor virtual presente en NetScaler Gateway.

Establece el número máximo de usuarios a nivel global al establecer el tipo de autenticación predeterminado para NetScaler Gateway.

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración, haga clic en Cambiar la configuración de autenticación.
3. En el cuadro de diálogo Configuración de autenticación global, en Número máximo de usuarios, escriba el número de usuarios y, a continuación, haga clic en Aceptar.

### Para establecer el límite de usuarios por servidor virtual

También puede aplicar el límite de usuarios a cada servidor virtual del sistema. Al configurar el límite de usuario por servidor virtual, la restricción se aplica solo a los usuarios que establecen sesiones con el servidor virtual concreto. Los usuarios que establecen sesiones con otros servidores virtuales no se ven afectados por este límite.

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, en Abrir .
3. En Usuarios máximos, escriba el número de usuarios y, a continuación, haga clic en Aceptar.

## Configurar los parámetros de tiempo de espera

January 26, 2024

Puede configurar NetScaler Gateway para forzar una desconexión si no hay actividad en la conexión durante un número de minutos especificado. Un minuto antes de que se acabe el tiempo de espera de una sesión (se desconecte), el usuario recibe una alerta que indica que la sesión se cierra. Si la sesión se cierra, el usuario debe volver a iniciar sesión.

**Hay tres opciones de tiempo de espera:**

- **Tiempo muerto forzado.** Si habilita esta configuración, Citrix Gateway desconecta la sesión una vez transcurrido el intervalo de tiempo de espera, independientemente de lo que esté haciendo el usuario. El usuario no puede realizar ninguna acción para evitar que se produzca la desconexión cuando transcurra el intervalo de tiempo de espera. Esta configuración se aplica a los usuarios que se conectan con el complemento NetScaler Gateway, la aplicación Citrix Workspace, Secure Hub o mediante un explorador web. El valor mínimo es 1 y el valor máximo es 65535.
- **Tiempo de espera de sesión.** Si habilita esta configuración, NetScaler Gateway desconecta la sesión si no se detecta actividad de red durante el intervalo especificado. Esta configuración se aplica a los usuarios que se conectan con el complemento NetScaler Gateway, la aplicación Citrix Workspace, Citrix Secure Hub o mediante un explorador web. El tiempo de espera predeterminado es de 30 minutos. El valor mínimo es 1 y el valor máximo es 65535.
- Tiempo de**espera de la sesión inactiva.** Duración después de la cual el plug-in de NetScaler Gateway finaliza una sesión inactiva si no hay actividad del usuario, como desde el mouse, el teclado o el tacto durante el intervalo especificado. Esta configuración se aplica únicamente a los usuarios que se conectan con el plug-in de NetScaler Gateway. El valor mínimo es 1 y el valor máximo es 9999.

> **Nota:**
>
> - La configuración del tiempo de espera no se aplica a Always On VPN.
> - Algunas aplicaciones, como Microsoft Outlook, envían automáticamente sondeos de tráfico de red a servidores de correo electrónico sin intervención del usuario. Citrix recomienda configurar el tiempo de espera de la sesión inactiva con el tiempo de espera de la sesión para garantizar que una sesión que se deja desatendida en un dispositivo de usuario caduque en un tiempo razonable.

Puede habilitar cualquiera de los ajustes de tiempo de espera introduciendo un valor entre 1 y 65536 para especificar los minutos del intervalo de tiempo de espera. Si habilita más de una de estas configuraciones, el primer intervalo de tiempo de espera que transcurriera cierra la conexión del dispositivo del usuario.

La configuración del tiempo de espera se establece mediante la configuración global o mediante un perfil de sesión. Al agregar el perfil a una directiva de sesión, la directiva se envuelve a un usuario, grupo o servidor virtual. Al configurar la configuración del tiempo de espera de forma global, la configuración se aplica a todas las sesiones de usuario.

## Configurar tiempos de espera forzados

March 27, 2024

Un tiempo de espera forzado desconecta automáticamente el plug-in de NetScaler Gateway después de un período de tiempo especificado. Puede configurar un tiempo de espera forzado de forma global o como parte de una directiva de sesión.

### Para configurar un tiempo de espera forzado global

1. En la utilidad de configuración, en la pestaña **Configuración** , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Configuración **global** .
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En la ficha **Configuración de red**, haga clic en **Configuración avanzada**.
4. En Tiempo de espera forzado (minutos), escriba el número de minutos que los usuarios pueden permanecer conectados.
5. En Advertencia de tiempo de espera forzado (minutos), escriba el número de minutos antes de que se avise a los usuarios de que la conexión se va a desconectar y, a continuación, haga clic en **Aceptar**.

### Para configurar un tiempo de espera forzado dentro de una política de sesión

Si quiere tener más control sobre quién recibe el tiempo de espera forzado, cree una directiva de sesión y, a continuación, aplíquela a un usuario o grupo.

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway** > **Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en **Nuevo** .
5. En Nombre , escriba un nombre para el perfil.
6. En la ficha **Configuración de red**, haga clic en **Avanzadas**.
7. En Tiempos de espera, haga clic en Supeditar global y, en Tiempo de espera forzado (minutos), escriba el número de minutos que los usuarios pueden permanecer conectados.
8. Junto a Advertencia de tiempo de espera forzado (minutos), haga clic en **Anular global** e introduzca el número de minutos durante los que se avisa a los usuarios de que la conexión se va a desconectar. Haga clic en **Aceptar** dos veces.
9. En el cuadro de diálogo **Crear política de sesión** , junto a **Expresiones con nombre** , seleccione General, seleccione **Valor verdadero** , haga clic en **Agregar expresión** , en **Crear** y, a continuación, en **Cerrar** .

## Configurar los tiempos de espera de sesión o de inactividad

March 27, 2024

Puede utilizar la GUI de NetScaler ADC para configurar los valores de tiempo de espera de sesión y cliente de forma global o para crear una directiva de sesión. Al crear un perfil y una directiva de sesión, establezca la expresión en True.

### Para configurar el tiempo de espera por inactividad de una sesión o cliente de forma global mediante la interfaz gráfica de usuario

1. En la pestaña **Configuración** , en el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en Configuración **global** .
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En la ficha **Experiencia del cliente**, realice una o ambas de las acciones siguientes:
    - En Tiempo de **espera de sesión (minutos)**, escriba el número de minutos.
    - En Tiempo de **espera inactivo del cliente (minutos)**, escriba el número de minutos y, a continuación, haga clic en **Aceptar**.

### Para configurar la configuración del tiempo de espera por inactividad de la sesión o del cliente mediante una directiva de sesión mediante la interfaz gráfica de usuario

1. En la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** > **Directivas** y, a continuación, haga clic en **Sesión**
2. En la página **Perfiles y directivas de sesión de NetScaler Gateway**, haga clic en **Perfiles de sesión**y, a continuación, haga clic en **Agregar**.
3. En Nombre , escriba un nombre para el perfil.
4. En la ficha **Experiencia del cliente**, realice una o ambas de las acciones siguientes:
    - Junto a Tiempo de **espera de sesión (minutos)**, haga clic en **Supedición global** y, a continuación, escriba el número de minutos y, a continuación, haga clic en **Crear**.
    - Junto a Tiempo de **espera inactivo del cliente (minutos)**, haga clic en **Supedición global**, escriba el número de minutos y, a continuación, haga clic en **Crear**.
5. a) En la página **Perfiles y directivas de sesión de NetScaler Gateway**, haga clic en **Directivas de sesión**y, a continuación, en **Agregar**.
6. En la **directiva Crear sesión de NetScaler Gateway**,
    - En **Nombre**, introduzca el nombre de la directiva.
    - En **Perfil**, seleccione el perfil que especifica la acción que aplicará la nueva directiva de sesión si se cumplen los criterios de la regla.
    - seleccione **Política avanzada** .
    - En el campo **Expresión**, agregue la expresión o el nombre de una expresión con nombre y especifique el tráfico que coincide con la directiva.
    - Haga clic en **Crear**y, a continuación, en **Cerrar**.

## Conectarse a recursos de la red interna

January 26, 2024

Puede configurar NetScaler Gateway para que los usuarios puedan acceder a los recursos de la red interna. Si inhabilita la tunelización dividida, todo el tráfico de red del dispositivo de usuario se envía a NetScaler Gateway y las directivas de autorización determinan si el tráfico puede pasar a través de recursos de red internos. Cuando habilita el túnel dividido, solo el tráfico destinado a la red interna es interceptado por el dispositivo del usuario y enviado a NetScaler Gateway. Puede configurar qué direcciones IP intercepta NetScaler Gateway mediante aplicaciones de intranet.

Si utiliza el plug-in de NetScaler Gateway para Windows, establezca el modo de interceptación en transparente. Si está usando el plug-in de NetScaler Gateway para Java, establezca el modo de inter-

cepción en proxy. Si establece el modo de interceptación en transparente, puede permitir el acceso a los recursos de red mediante:

- Una única dirección IP y máscara de subred
- Una serie de direcciones IP

Si establece el modo de interceptación en proxy, puede configurar las direcciones IP de destino y origen y los números de puerto.

### Para configurar el acceso de red a los recursos internos de la red

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda NetScaler Gateway, expanda Recursos y, a continuación, haga clic en **Aplicaciones de intranet.**
2. En el panel de detalles, haga clic en **Agregar.**
3. Complete los parámetros para permitir el acceso a la red, haga clic en **Crear** y, a continuación, en **Cerrar.**

## Configurar el túnel dividido

March 27, 2024

Puede habilitar la tunelización dividida para evitar que el plug-in de NetScaler Gateway envíe tráfico de red innecesario a NetScaler Gateway.

Cuando no habilita la creación de túneles divididos, el plug-in de NetScaler Gateway captura todo el tráfico de red que se origina desde un dispositivo de usuario y envía el tráfico a través del túnel VPN a NetScaler Gateway.

Si habilita la creación de túneles divididos, el plug-in de NetScaler Gateway envía solo tráfico destinado a redes protegidas por NetScaler Gateway a través del túnel VPN. El plug-in de NetScaler Gateway no envía tráfico de red destinado a redes no protegidas a NetScaler Gateway.

Cuando se inicia el plug-in de NetScaler Gateway, obtiene la lista de aplicaciones de intranet de NetScaler Gateway. El plug-in de NetScaler Gateway examina todos los paquetes transmitidos en la red desde el dispositivo del usuario y compara las direcciones de los paquetes con la lista de aplicaciones de intranet. Si la dirección de destino del paquete está dentro de una de las aplicaciones de intranet, el plug-in de NetScaler Gateway envía el paquete a través del túnel VPN a NetScaler Gateway. Si la dirección de destino no se encuentra en una aplicación de intranet definida, el paquete no se cifra y el dispositivo del usuario enruta el paquete de forma adecuada. Al habilitar la tunelización dividida, las aplicaciones de intranet definen el tráfico de red que se intercepta.

> **Nota:** Si los usuarios se conectan a aplicaciones publicadas en una comunidad de servidores mediante Citrix Receiver, no es necesario configurar la tunelización dividida.

NetScaler Gateway también admite la tunelización dividida inversa, que define el tráfico de red que NetScaler Gateway no intercepta. Si establece la tunelización dividida como inversa, las aplicaciones de intranet definen el tráfico de red que NetScaler Gateway no intercepta. Cuando habilita la tunelización dividida inversa, todo el tráfico de red dirigido a direcciones IP internas omite el túnel VPN, mientras que el resto del tráfico pasa por NetScaler Gateway. La tunelización dividida inversa se puede utilizar para registrar todo el tráfico LAN no local. Por ejemplo, si los usuarios tienen una red inalámbrica doméstica y han iniciado sesión con el plug-in de NetScaler Gateway, NetScaler Gateway no interceptará el tráfico de red destinado a una impresora u otro dispositivo dentro de la red inalámbrica.

Para obtener más información sobre las aplicaciones de intranet, consulte Configuración de la interceptación de clientes.

Configure la tunelización dividida como parte de la directiva de sesión.

### Para configurar el túnel dividido

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Directivas de Citrix Gateway** y, a continuación, haga clic en **Sesión.**
2. En el panel de detalles, en la ficha **Perfiles**, seleccione un perfil y, a continuación, haga clic en **Abrir.**
3. En la ficha **Experiencia del cliente**, junto a **Dividir túnel**, seleccione **Anulación global**, seleccione una opción y, a continuación, haga clic dos veces en **Aceptar**.

### Configurar la autorización y la tunelización dividida

Al planificar la implementación de NetScaler Gateway, es importante tener en cuenta la tunelización dividida y la acción de autorización y las directivas de autorización predeterminadas.

Por ejemplo, tiene una directiva de autorización que permite el acceso a un recurso de red. La tunelización dividida está activada y no configura las aplicaciones de intranet para enviar tráfico de red a través de NetScaler Gateway. Cuando NetScaler Gateway tiene este tipo de configuración, se permite el acceso al recurso, pero los usuarios no pueden acceder al recurso.

Si la directiva de autorización deniega el acceso a un recurso de red, tiene establecida la tunelización dividida en ON y las aplicaciones de intranet están configuradas para redirigir el tráfico de red a través de NetScaler Gateway, el plug-in de NetScaler Gateway envía tráfico a NetScaler Gateway, pero se deniega el acceso al recurso.

# Configurar la intercepción de clientes

January 26, 2024

Las reglas de interceptación para las conexiones de usuario en NetScaler Gateway se configuran mediante aplicaciones de intranet. De forma predeterminada, cuando configura la dirección IP del sistema, una dirección IP asignada o una dirección IP de subred en el dispositivo, las rutas de subred se crean en función de estas direcciones IP. Las aplicaciones de intranet se crean automáticamente en función de estas rutas y se pueden enlazar a un servidor virtual. Si habilita la tunelización dividida, debe definir las aplicaciones de intranet para que se produzca la interceptación del cliente.

Puede configurar aplicaciones de intranet mediante la utilidad de configuración. Puede enlazar aplicaciones de intranet a usuarios, grupos o servidores virtuales.

Si habilita la tunelización dividida y los usuarios se conectan mediante WorxWeb o WorxMail, al configurar la interceptación de clientes, debe agregar las direcciones IP de Citrix Endpoint Management y del servidor Exchange. Si no habilita la tunelización dividida, no es necesario configurar las direcciones IP de Endpoint Management y Exchange en aplicaciones de intranet.

## Configuración de aplicaciones de intranet para el plug-in de NetScaler Gateway

March 27, 2024

Para crear aplicaciones de intranet para el acceso de los usuarios a los recursos, defina lo siguiente:

- Una dirección IP
- Una serie de direcciones IP

Cuando define una aplicación de intranet en NetScaler Gateway, el plug-in de NetScaler Gateway para Windows intercepta el tráfico de usuario destinado al recurso y envía el tráfico a través de NetScaler Gateway.

Al configurar aplicaciones de intranet, tenga en cuenta lo siguiente:

- No es necesario definir las aplicaciones de intranet si se cumplen las siguientes condiciones:
  - El modo de intercepción está configurado como transparente
  - Los usuarios se están conectando a NetScaler Gateway con el plug-in de NetScaler Gateway para Windows
  - La tunelización dividida está desactivada

- Si los usuarios se conectan a NetScaler Gateway mediante el plug-in de NetScaler Gateway para Java, debe definir aplicaciones de intranet. El plug-in de NetScaler Gateway para Java intercepta el tráfico solo a los recursos de red definidos por las aplicaciones de intranet. Si los usuarios se conectan con este complemento, establezca el modo de intercepción en proxy.

Al configurar una aplicación de intranet, debe seleccionar un modo de interceptación que se corresponda con el tipo de software de plug-in utilizado para establecer conexiones.

Nota: No se puede configurar una aplicación de intranet para interceptación proxy y transparente. Para configurar un recurso de red que utilizarán el plug-in de NetScaler Gateway para Windows y el plug-in de NetScaler Gateway para Java, configure dos directivas de aplicación de intranet y vincule las directivas al usuario, grupo, servidor virtual o global de NetScaler Gateway.

### Para crear una aplicación de intranet para una dirección IP

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **Citrix Gateway Resources** y, a continuación, haga clic en **Aplicaciones de intranet**.
2. En el panel de detalles, haga clic en **Agregar.**
3. En Nombre , escriba un nombre para el perfil.
4. En el cuadro de diálogo **Crear aplicación de intranet**, seleccione **Transparente.**
5. En **Tipo de destino** , seleccione **Dirección IP** y máscara de red **.**
6. En Protocolo, seleccione el protocolo que se aplica al recurso de red.
7. En **Dirección IP**, escriba la dirección IP.
8. En **Máscara de red**, escriba máscara de subred, haga clic en **Crear** y, a continuación, haga clic en **Cerrar.**

### Para configurar un intervalo de direcciones IP

Si tiene varios servidores en la red, como la web, el correo electrónico y los recursos compartidos de archivos, puede configurar un recurso de red que incluya el rango de IP de los recursos de red. Esta configuración permite a los usuarios acceder a los recursos de red incluidos en el intervalo de direcciones IP.

1. En la utilidad de configuración, en la pestaña **Configuración** , en el panel de navegación, expanda **Citrix Gateway Resources** y, a continuación, haga clic en **Aplicaciones de intranet .**
2. En el panel de detalles, haga clic en **Agregar.**
3. En **Nombre**, escriba un nombre para el perfil.
4. En Protocolo, seleccione el protocolo que se aplica al recurso de red.
5. En el cuadro de diálogo Crear aplicación de intranet, seleccione Transparente.
6. En **Tipo de destino**, seleccione **Intervalo de direcciones IP.**

7. En **Inicio IP**, escriba la dirección IP inicial y, en Fin IP, escriba la dirección IP final, haga clic en **Crear** y, a continuación, haga clic en **Cerrar.**

## Configuración de aplicaciones de intranet para el plug-in de NetScaler Gateway para Java

March 27, 2024

Si los usuarios se conectan con el plug-in de NetScaler Gateway para Java, debe configurar una aplicación de intranet y establecer el modo de interceptación en proxy. El plug-in de NetScaler Gateway para Java intercepta el tráfico mediante la dirección IP de loopback del dispositivo de usuario y el número de puerto especificados en el perfil.

Si los usuarios se conectan desde un dispositivo basado en Windows, el plug-in de NetScaler Gateway para Java intenta modificar el archivo HOST estableciendo el nombre HOST de la aplicación para acceder a la dirección IP de bucle invertido y al puerto especificados en el perfil. Los usuarios deben tener privilegios administrativos en el dispositivo de usuario para modificar el archivo HOST.

Si los usuarios se conectan desde un dispositivo que no es Windows, debe configurar las aplicaciones manualmente mediante la dirección IP de origen y los valores de puerto especificados en el perfil de aplicación de la intranet.

### Para configurar una aplicación de intranet para el plug-in de NetScaler Gateway para Java

1. En la utilidad de configuración, en la pestaña **Configuración** , en el panel de navegación, expanda **Citrix Gateway Resources** y, a continuación, haga clic en **Aplicaciones de intranet .**
2. En el panel de detalles, haga clic en **Agregar.**
3. En **Nombre**, escriba un nombre para el perfil.
4. Haga clic en **Proxy.**
5. En **Dirección IP de destino** y **Puerto de destino**, escriba la dirección IP y el puerto de destino.
6. En **Dirección IP de** origen y **Puerto de origen**, escriba la dirección IP y el puerto de origen.

> **Nota:**Debe establecer la dirección IP de origen en la dirección IP de bucle invertido 127.0.0.1. Si no especifica una dirección IP, se utiliza la dirección IP de bucle innecesario. Si no introduce ningún valor de puerto, se utiliza el valor del puerto de destino.

## Configurar la resolución del servicio de nombres

January 26, 2024

Durante la instalación de NetScaler Gateway, puede utilizar el asistente de NetScaler Gateway para configurar otras opciones, incluidos los proveedores de servicios de nombres. Los proveedores de servicios de nombres traducen el nombre de dominio completo (FQDN) en una dirección IP. En el asistente de NetScaler Gateway, puede configurar un servidor DNS o WINS, establecer la prioridad de la búsqueda DNS y el número de veces que se debe volver a intentar la conexión con el servidor.

Al ejecutar el asistente de NetScaler Gateway, puede agregar un servidor DNS. Puede agregar servidores DNS adicionales y un servidor WINS a Citrix Gateway mediante un perfil de sesión. A continuación, puede indicar a los usuarios y grupos que se conecten a un servidor de resolución de nombres distinto del que utilizó originalmente el asistente para configurar.

Antes de configurar un servidor DNS adicional en Citrix Gateway, cree un servidor virtual que actúe como servidor DNS para la resolución de nombres.

### Para agregar un servidor DNS o WINS dentro de un perfil de sesión

1. En la utilidad de configuración, en la pestaña **Configuración** , en el panel de navegación, expanda **Políticas de Citrix Gateway** y, a continuación, haga clic en **Sesión.**
2. En el panel de detalles, en la ficha Perfiles, seleccione un perfil y, a continuación, haga clic en Abrir.
3. En la ficha Configuración de red, realice una de las siguientes acciones:
    - Para configurar un servidor DNS, junto a Servidor virtual DNS, haga clic en **Supeditación global**, seleccione el servidor y, a continuación, haga clic en **Aceptar**.
    - Para configurar un servidor WINS, junto a IP del servidor WINS, haga clic en **Supeditación global**, escriba la dirección IP y, a continuación, haga clic en **Aceptar**.

> **Importante:**
>
> Las directivas de respuesta no se evalúan para servidores virtuales DNS no direccionables conectados al perfil de sesión VPN.

## Habilitación del soporte proxy para conexiones de usuario

March 27, 2024

Los dispositivos de usuario se pueden conectar a través de un servidor proxy para acceder a redes internas. NetScaler Gateway admite los protocolos HTTP, SSL, FTP y SOCKS. Para habilitar la compatibilidad con proxy para las conexiones de usuario, especifique la configuración en NetScaler Gateway. Puede especificar la dirección IP y el puerto que utiliza el servidor proxy de NetScaler Gateway. El servidor proxy se utiliza como proxy de reenvío para todas las demás conexiones a la red interna.

### Configuración de proxy

Puede configurar la configuración del proxy en el explorador o en el dispositivo NetScaler ADC. Para configurar la configuración del proxy en el explorador o el dispositivo, vaya a **Configuración global de NetScaler Gateway > ficha Experiencia del cliente > Configuración avanzada > Proxy**y, a continuación, seleccione **Explorador** o **NS**, según corresponda.

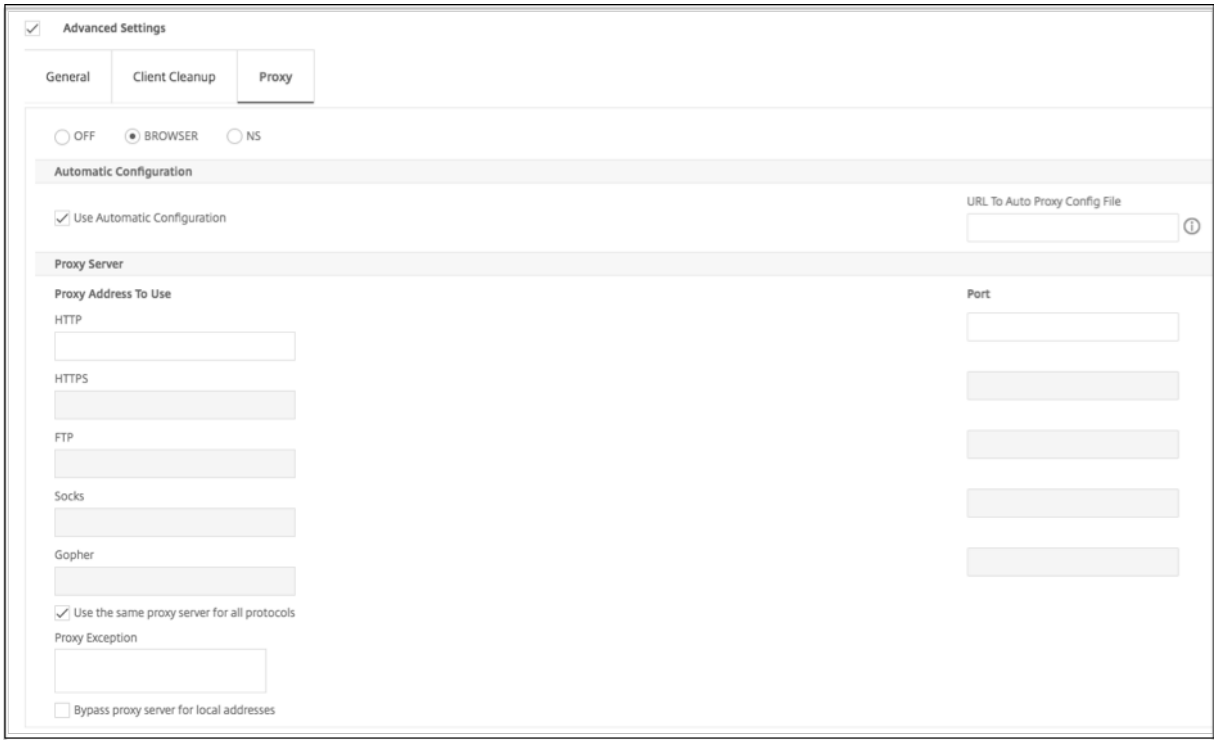
- **Explorador**: Cuando elige configurar los ajustes del proxy en el explorador, puede utilizar la opción de configuración automática proporcionando un enlace al archivo de configuración automática del proxy. La configuración automática podría sobrescribir la configuración manual.

  Además, al seleccionar **Browser**, puede omitir los proxies configurados previamente seleccionando la opción de excepción de proxy.

  **Nota:** Los diferentes tipos de clientes tienen capacidades diferentes en cuanto a la configuración **del proxy del explorador**. Para obtener más información, consulte Clientes VPN de NetScaler Gateway y funciones compatibles.

- **NS**: No puede utilizar la opción de configuración automática si configura la configuración del proxy en el dispositivo NetScaler ADC. No se pueden omitir los proxies configurados previamente cuando configura la configuración del proxy en el dispositivo.




### Para configurar la compatibilidad de proxy para conexiones de usuario

1. En el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global.**
2. En el panel de detalles, en **Configuración** , haga clic en Cambiar la configuración global.
3. En la pestaña Experiencia del cliente, haga clic en **Configuración avanzada** .
4. En la **ficha Proxy**, en **Configuración de proxy**, seleccione **Navegador.**
5. Para los protocolos, escriba la dirección IP y el número de puerto y, a continuación, haga clic en **Aceptar.**

> **Nota:**
>
> - Si selecciona NS, puede configurar servidores proxy que admitan únicamente conexiones HTTP seguras y no seguras.
> - Después de habilitar la compatibilidad con proxy en NetScaler Gateway, especifique los detalles de configuración del dispositivo de usuario del servidor proxy correspondiente al protocolo.
> - Después de habilitar la compatibilidad con proxy, NetScaler Gateway envía los detalles del servidor proxy al explorador web del cliente y cambia la configuración del proxy en el explorador.

> – When the user device connects to Citrix Gateway, the user device can communicate with the proxy server directly for connection to the user's network.
> – When the user device disconnects from Citrix Gateway, the proxy settings are restored to the previous default settings, that was present before connecting to the VPN plug-in.

### Para configurar un servidor proxy para que use todos los protocolos de NetScaler Gateway

Puede configurar un servidor proxy para que admita todos los protocolos que utiliza NetScaler Gateway. Esta configuración proporciona una combinación de dirección IP y puerto para todos los protocolos.

1. En el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global** .
2. En el panel de detalles, en **Configuración** , haga clic en Cambiar la configuración global.
3. En la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada.**
4. En la pestaña **Proxy** , en **Configuración** de proxy , selecciona **Navegador.**
5. Para los protocolos, escriba la dirección IP y el número de puerto.
6. Haga clic en Usar el mismo servidor proxy para todos los protocolos y, a continuación, haga clic en **Aceptar.**

Cuando inhabilita la tunelización dividida y establece toda la configuración del proxy en Activado, la configuración del proxy se propaga a los dispositivos del usuario. Si la configuración del proxy se establece en Equipo, la configuración no se propaga a los dispositivos de usuario.

NetScaler Gateway establece conexiones con el servidor proxy en nombre del dispositivo del usuario. La configuración del proxy no se propaga al explorador del usuario, por lo que no es posible la comunicación directa entre el dispositivo del usuario y el servidor proxy.

### Para configurar NetScaler Gateway para que sea un servidor proxy

Al configurar NetScaler Gateway como servidor proxy, HTTP no seguro y seguro es el único protocolo compatible.

1. En el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global.**
2. En el panel de detalles, en **Configuración** , haga clic en Cambiar la configuración global.
3. En la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada.**
4. En la ficha **Proxy**, en **Configuración del proxy**, seleccione **NS**.
5. Para los protocolos, escriba la dirección IP y el número de puerto y, a continuación, haga clic en **Aceptar.**

# Configurar grupos de direcciones

January 26, 2024

En algunas situaciones, los usuarios que se conectan con el plug-in de NetScaler Gateway necesitan una dirección IP única para NetScaler Gateway. Por ejemplo, en un entorno Samba, cada usuario que se conecta a una unidad de red asignada debe parecer originario de una dirección IP diferente. Al habilitar los grupos de direcciones (también conocidos como agrupación de IP) para un grupo, NetScaler Gateway puede asignar un alias de dirección IP único a cada usuario.

Los grupos de direcciones se configuran mediante direcciones IP de intranet. Es posible que los siguientes tipos de aplicaciones necesiten utilizar una dirección IP única que se extrae del grupo de direcciones IP:

- Voz sobre IP
- FTP activo
- Mensajería instantánea
- Shell seguro (SSH)
- Informática de red virtual (VNC) para conectarse al escritorio de un equipo
- Escritorio remoto (RDP) para conectarse a un escritorio cliente

Puede configurar NetScaler Gateway para asignar una dirección IP interna a los usuarios que se conectan a NetScaler Gateway. Las direcciones IP estáticas se pueden asignar a los usuarios o se puede asignar un rango de direcciones IP a un grupo, servidor virtual o al sistema de forma global.

NetScaler Gateway permite asignar direcciones IP de la red interna a los usuarios remotos. Se puede direccionar a un usuario remoto mediante una dirección IP en la red interna. Si elige utilizar un rango de direcciones IP, el sistema asigna dinámicamente una dirección IP de ese rango a un usuario remoto a petición.

Al configurar grupos de direcciones, tenga en cuenta lo siguiente:

- Las direcciones IP asignadas deben redirigirse correctamente. Para garantizar la redirección correcta, tenga en cuenta lo siguiente:
  - Si no habilita la tunelización dividida, asegúrese de que las direcciones IP se puedan redirigir a través de dispositivos de traducción de direcciones de red (NAT).
  - Todos los servidores a los que se accede mediante conexiones de usuario con direcciones IP de intranet deben tener las puertas de enlace adecuadas configuradas para llegar a esas redes.
  - Configure puertas de enlace o una ruta estática en NetScaler Gateway para que el tráfico de red del software de usuario se enrute a la red interna.

- Solo se pueden utilizar máscaras de subred contiguas al asignar rangos de direcciones IP. Se puede asignar un subconjunto de un rango a una entidad de nivel inferior. Por ejemplo, si un intervalo de direcciones IP está enlazado a un servidor virtual, vincule un subconjunto del rango a un grupo.
- Los intervalos de direcciones IP no se pueden enlazar a varias entidades dentro de un nivel de enlace. Por ejemplo, un subconjunto de un intervalo de direcciones enlazado a un grupo no se puede enlazar a un segundo grupo.
- NetScaler Gateway no permite quitar ni desvincular direcciones IP mientras las utiliza activamente una sesión de usuario.
- Las direcciones IP de la red interna se asignan a los usuarios mediante la siguiente jerarquía:
  - Vinculación directa del usuario
  - Grupo de direcciones asignadas
  - Grupo de direcciones asignadas a servidores virtuales
  - Rango global de direcciones
- Solo se pueden utilizar máscaras de subred contiguas para asignar rangos de direcciones. Sin embargo, un subconjunto de un rango asignado podría asignarse a una entidad de nivel inferior. Un intervalo de direcciones globales enlazado puede tener un rango vinculado a lo siguiente:
  - Servidor virtual
  - Grupo
  - Usuario
- Un intervalo de direcciones de servidor virtual enlazado puede tener un subconjunto enlazado a lo siguiente:
  - Grupo
  - Usuario

Un intervalo de direcciones de grupo enlazado puede tener un subconjunto enlazado a un usuario.

Cuando se asigna una dirección IP a un usuario, la dirección se reserva para el próximo inicio de sesión del usuario hasta que se agote el intervalo del grupo de direcciones. Cuando se agotan las direcciones, NetScaler Gateway recupera la dirección IP del usuario que más tiempo ha desconectado de NetScaler Gateway.

Si no se puede recuperar una dirección y todas las direcciones están en uso activo, NetScaler Gateway no permite que el usuario inicie sesión. Puede evitar esta situación permitiendo que NetScaler Gateway utilice la dirección IP asignada como dirección IP de intranet cuando el resto de direcciones IP no estén disponibles.

### Registro DNS IP de intranet

Si se asigna una IP de intranet a una máquina cliente y, una vez establecido el túnel VIP, el complemento VPN comprueba si esa máquina cliente está unida a un dominio. Si la máquina cliente es una máquina unida a un dominio, el complemento VPN inicia el proceso de registro de DNS para vincular la intranet del nombre de host de la máquina con la dirección IP de la intranet asignada. Este registro se revierte antes de la retirada del túnel.

Para que el registro de DNS se realice correctamente, asegúrese de que estén configurados los siguientes botones nsapimgr. Asegúrese también de que el servidor DNS autorizado esté configurado para permitir actualizaciones DNS "no seguras".

- **nsapimgr -ys enable_vpn_dns_override=1**: este indicador se envía al cliente VPN de NetScaler Gateway junto con los demás parámetros de configuración. Si este indicador está desconfigurado y cuando el cliente VPN intercepta una solicitud DNS/WINS, envía una solicitud http-request "GET /DNS"correspondiente al servidor virtual NetScaler Gateway a través del túnel para obtener la dirección IP resuelta. Sin embargo, si se establece el indicador 'enable_vpn_dnstruncate_fix', el cliente VPN reenvía las solicitudes DNS/WINS de forma transparente al servidor virtual de NetScaler Gateway. En este caso, el paquete DNS se envía tal cual al servidor virtual de NetScaler Gateway a través del túnel VPN. Esto ayuda en los casos en que los registros DNS procedentes de los servidores de nombres configurados en NetScaler Gateway son enormes y no caben en el paquete de respuesta UPD. En este caso, cuando el cliente vuelve a usar TCP-DNS, este paquete TCP-DNS llega al servidor de NetScaler Gateway tal cual y, por lo tanto, el servidor de NetScaler Gateway realiza una consulta TCP-DNS a un servidor DNS.
- **nsapimgr -ys enable_vpn_dnstruncate_fix=1**: Este indicador lo utiliza el propio servidor de NetScaler Gateway. Si se establece este indicador, NetScaler Gateway reemplaza el destino de las "conexiones TCP en el puerto DNS"a los servidores DNS configurados en NetScaler Gateway (en lugar de intentar enviarlos a la IP del servidor DNS presente originalmente en el paquete TCP-DNS entrante). Para las solicitudes DNS UDP, el valor predeterminado es utilizar los servidores DNS configurados para la resolución DNS.

Para obtener más información sobre cómo configurar estos mandos, consulte.https://support.citrix.com/article/CTX200243

## Configurar grupos de direcciones

March 27, 2024

La utilidad de configuración se usa para configurar los grupos de direcciones en el nivel al que desea vincular la política. Por ejemplo, si desea crear un grupo de direcciones para un servidor virtual, configure las direcciones IP de la intranet en ese nodo. Después de configurar el grupo de direcciones, la política se enlaza a la entidad en la que está configurada. También puede crear un grupo de direcciones y vincularlo globalmente en Citrix Gateway.

### Para configurar grupos de direcciones para un usuario, un grupo o un servidor virtual

1. En la utilidad de configuración, en el panel de navegación, expanda **NetScaler Gateway**y realice una de las siguientes acciones:
   - Amplíe Administración de usuarios de Citrix Gateway y, a continuación, haga clic en **Usuarios AAA** .
   - Expanda **NetScaler Gateway** > **Administración de usuarios** y, a continuación, haga clic en **Grupos AAA**.
   - Amplíe **Citrix Gateway** y, a continuación, haga clic en **Servidores virtuales** .
2. En el panel de detalles, haga clic en un usuario, grupo o servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la ficha IP **de intranet**, en Dirección IP y máscara de red, escriba la dirección IP y la máscara de subred y, a continuación, haga clic en **Agregar**.
4. Repita el paso 3 para cada dirección IP que quiera agregar al grupo y, a continuación, haga clic en **Aceptar**.

### Para configurar grupos de direcciones de forma global

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **IP de intranet**, haga clic en Para asignar una dirección IP estática única o un grupo de direcciones IP para que las usen todas las sesiones de cliente de NetScaler Gateway, configure las IP de intranet.
3. En el cuadro de diálogo **Vincular direcciones IP de intranet**, haga clic en **Acción** y, a continuación, haga clic en **Insertar**.
4. En Dirección IP y máscara de red, escriba la dirección IP y la máscara de subred y, a continuación, haga clic en **Agregar**.
5. Repita los pasos 3 y 4 para cada dirección IP que quiera agregar al grupo y, a continuación, haga clic en **Aceptar**.

# Definir las opciones del grupo de direcciones

March 27, 2024

Puede usar una directiva de sesión o la configuración global de Citrix Gateway para controlar si las direcciones IP de la intranet se asignan o no durante una sesión de usuario. La definición de opciones de grupo de direcciones le permite asignar direcciones IP de intranet a NetScaler Gateway, al tiempo que inhabilita el uso de direcciones IP de intranet para un grupo determinado de usuarios.

Puede configurar grupos de direcciones mediante una directiva de sesión de una de las tres formas siguientes:

- Nospillover: cuando configuras grupos de direcciones para la dirección IP de la intranet, obtienes una sesión con una IP disponible en el grupo. Para los usuarios que han utilizado todas las direcciones IP de intranet disponibles, aparece la página Transferir inicio de sesión.
- Spillover: Cuando configura grupos de direcciones y la IP asignada se utiliza como dirección IP de intranet, la dirección IP asignada se utiliza para los usuarios que han utilizado todas las direcciones IP de intranet disponibles.
- Desactivado: Los grupos de direcciones no están configurados.

> **Nota:**Si la dirección IP asignada no está configurada, se utiliza SNIP.

### Para configurar grupos de direcciones

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo**.
5. En Nombre , escriba un nombre para el perfil.
6. En la ficha **Configuración de red**, haga clic en **Avanzadas**.
7. Junto a IP de intranet, haga clic en **Sobrescribir global** y, a continuación, selecciona una opción.
8. Si selecciona **SPILLOVER** en el paso 9, junto a IP asignada, haga clic en **Sustituir global**, seleccione el nombre de host del dispositivo, haga clic en **Aceptar** y, a continuación, haga clic en **Crear**.
9. En el cuadro de diálogo **Crear directiva de sesión**, cree una expresión, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

### Configuración de la página de inicio de sesión de transferencia

Si un usuario no tiene disponible una dirección IP de intranet y, a continuación, intenta establecer otra sesión con NetScaler Gateway, aparece la página Transferir inicio de sesión. La página Transferir inicio de sesión permite a los usuarios reemplazar su sesión existente de NetScaler Gateway por una nueva sesión.

La página Transferir inicio de sesión también se puede utilizar si se pierde la solicitud de cierre de sesión o si el usuario no realiza un cierre de sesión limpio. Por ejemplo:

- A un usuario se le asigna una dirección IP de intranet estática y ya tiene una sesión de NetScaler Gateway. Si el usuario intenta establecer una segunda sesión desde otro dispositivo, aparece la página Transferir inicio de sesión y el usuario puede transferir la sesión al nuevo dispositivo.
- A un usuario se le asignan cinco direcciones IP de intranet y tiene cinco sesiones a través de NetScaler Gateway. Si el usuario intenta establecer una sexta sesión, aparece la página Transferir inicio de sesión y el usuario puede elegir reemplazar una sesión existente por una nueva.

> **Nota**: Si el usuario no tiene disponible una >dirección IP asignada y no se puede establecer una nueva >sesión mediante la página >Transferir inicio de sesión, el usuario recibirá un >mensaje de error.

La página Transferir inicio de sesión solo aparece si configura grupos de direcciones y inhabilita el desbordamiento.

### Configuración de un sufijo DNS

Cuando un usuario inicia sesión en NetScaler Gateway y se le asigna una dirección IP, se agrega un registro DNS para la combinación de nombre de usuario y dirección IP a la caché DNS de NetScaler Gateway. Puede configurar un sufijo DNS para que se agregue al nombre de usuario cuando se agregue el registro DNS a la caché. Esto permite hacer referencia a los usuarios mediante el nombre DNS, que puede ser más fácil de recordar que una dirección IP. Cuando el usuario cierra sesión en NetScaler Gateway, el registro se elimina de la caché DNS.

### Para configurar un sufijo DNS

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, seleccione una directiva de sesión y, a continuación, haga clic en **Abrir**.
3. Junto a Solicitar perfil, haga clic en **Modificar**.
4. En la ficha **Configuración de red**, haga clic en **Avanzadas**.

5. Junto a Sufijo DNS de IP de intranet, haga clic en **Supeditación global**, escriba el sufijo DNS y, a continuación, haga clic en **Aceptar** tres veces.

## Compatibilidad con teléfonos VoIP

January 26, 2024

Cuando instala Citrix Gateway como un dispositivo independiente y los usuarios se conectan con el complemento Citrix Gateway, Citrix Gateway admite la comunicación bidireccional con los softphones de voz sobre IP (VoIP).

NetScaler Gateway admite los siguientes softphones VoIP.

- Softphone de Cisco
- Softphone IP Avaya

Se admite la tunelización segura entre la centralita IP y el software softphone que se ejecuta en el dispositivo del usuario. Para permitir que el tráfico VoIP atraviese el túnel seguro, debe instalar el plug-in de NetScaler Gateway y uno de los softphones compatibles en el mismo dispositivo de usuario. Cuando el tráfico VoIP se envía a través del túnel seguro, se admiten las siguientes funciones del softphone:

- Llamadas salientes que se realizan desde el softphone IP
- Llamadas entrantes que se colocan en el softphone IP
- Tráfico de voz bidireccional

La compatibilidad con softphones VoIP se configura mediante direcciones IP de intranet. Configure una dirección IP de intranet para cada usuario. Si utiliza Cisco Softphone Communication, después de configurar la dirección IP de la intranet y vincularla a un usuario, no se requiere ninguna configuración adicional. Para obtener más información sobre cómo configurar una dirección IP de intranet, consulte Configuración de grupos de direcciones.

Si habilita la tunelización dividida, cree una aplicación de intranet y especifique la aplicación Avaya Softphone. Además, debe habilitar la interceptación transparente.

## Configuración del acceso a aplicaciones para el plug-in de NetScaler Gateway para Java

January 26, 2024

Puede configurar el nivel de acceso y las aplicaciones a las que los usuarios pueden acceder en la red segura. Si los usuarios inician sesión mediante el complemento NetScaler Gateway para Java, en el cuadro de diálogo Sesión remota de acceso seguro, los usuarios pueden hacer clic en Aplicaciones. Aparece el cuadro de diálogo Aplicaciones de intranet, en el que se enumeran todas las aplicaciones a las que el usuario está autorizado a acceder.

Cuando los usuarios están conectados con el plug-in de NetScaler Gateway para Java, puede configurar uno de los dos métodos que permiten a los usuarios acceder a las aplicaciones.

- Método de modificación de archivos HOSTS
- Método SourceIP y SourcePort

### Acceso a aplicaciones mediante el método de modificación de archivos HOSTS

Cuando utiliza el método de modificación de archivos HOSTS, el plug-in de NetScaler Gateway para Java agrega una entrada que corresponde a las aplicaciones que configura en el archivo HOSTS. Para modificar este archivo en un dispositivo basado en Windows, debe haber iniciado sesión como administrador o tener privilegios de administrador. Si no ha iniciado sesión con privilegios de administrador, modifique manualmente el archivo HOSTS y agregue las entradas adecuadas.

Nota: En un equipo basado en Windows, el archivo HOSTS se encuentra en la siguiente ruta de directorio:
%systemroot%\ system32\ drivers\ etc. En un equipo Macintosh o Linux, el archivo HOSTS se encuentra en
/etc/hosts.

Por ejemplo, quiere utilizar Telnet para conectarse a un equipo de la red segura. Utiliza el equipo remoto para trabajar tanto dentro de la red segura como de forma remota, por ejemplo, desde casa. La dirección IP debe ser la dirección IP del host local, 127.0.0.1. En el archivo HOSTS, agrega la dirección IP y el nombre de la aplicación, por ejemplo:

127.0.0.1 telnet1

Cuando el archivo HOSTS se modifica y guarda en el dispositivo del usuario, prueba la conexión. Puede probar la conexión abriendo un símbolo del sistema y mediante Telnet para conectarse. Si los usuarios utilizan un dispositivo de usuario que no está dentro de la red segura, inicie sesión en NetScaler Gateway antes de iniciar Telnet.

Para conectarse a un equipo de la red segura:

1. Inicie una sesión Telnet con el software disponible para su equipo.
2. En el símbolo del sistema, escriba: Abrir telnet

   Aparece el mensaje de inicio de sesión del equipo remoto.

### Acceso a aplicaciones mediante el método SourceIP y SourcePort

Si los usuarios necesitan acceder a una aplicación de la red segura y no tienen derechos administrativos en el dispositivo del usuario, configure el archivo HOSTS mediante la dirección IP de origen y el número de puerto que se encuentran en el cuadro de diálogo Aplicaciones de intranet.

Para abrir el cuadro de diálogo Aplicaciones de intranet y localizar la dirección IP y el número de puerto

1. Cuando los usuarios inicien sesión con el complemento, en el cuadro de diálogo Acceso remoto seguro, haga clic en Aplicaciones.
2. Busque la aplicación en la lista y anote la dirección IP de origen y el número de puerto de origen.

Cuando tenga la dirección IP y el número de puerto, inicie una sesión Telnet para conectarse al equipo de la red remota.

## Configurar la interfaz de acceso

January 26, 2024

Citrix Gateway incluye una página principal predeterminada, que es una página web que aparece después de que los usuarios inician sesión. La página principal predeterminada se denomina Interfaz de acceso. Utilice la interfaz de acceso como página principal o configure la interfaz web como página principal o como página principal personalizada.

La interfaz de acceso contiene tres paneles. Si tiene la interfaz web en la implementación, los usuarios pueden iniciar sesión en Receiver en el panel izquierdo de la interfaz de acceso. Si tiene StoreFront en la implementación, los usuarios no pueden iniciar sesión en Receiver desde el panel izquierdo.

La interfaz de acceso se utiliza para proporcionar enlaces a sitios web, tanto internos como externos, y enlaces a recursos compartidos de archivos en la red interna. Puede personalizar la interfaz de acceso de las siguientes formas:

- Cambiar la interfaz de acceso.
- Creación de vínculos de interfaz de acceso.

Los usuarios también pueden personalizar la interfaz de acceso agregando sus propios enlaces a sitios web y recursos compartidos de archivos. Los usuarios también pueden utilizar la página de inicio para transferir archivos de la red interna a su dispositivo.

> **Nota:** Cuando los usuarios inician sesión e intentan abrir recursos compartidos de archivos desde la interfaz de acceso, el recurso compartido de archivos no se abre y los usuarios reciben el mensaje de error "Error al realizar la conexión TCP al servidor". Para resolver este problema,

> configure el firewall para permitir el tráfico desde la dirección IP del sistema NetScaler Gateway a la dirección IP del servidor de archivos en los puertos TCP 445 y 139.

## Sustituir la interfaz de acceso por una página principal personalizada

March 27, 2024

Puede utilizar la configuración global o una directiva de sesión y un perfil para configurar una página principal personalizada que sustituya a la página principal predeterminada, la interfaz de acceso. Después de configurar la directiva, puede vincularla a un usuario, grupo, servidor virtual o de forma global. Al configurar una página principal personalizada, la interfaz de acceso no aparece cuando los usuarios inician sesión.

### Para configurar la página de inicio personalizada de forma global

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global.**
2. En el panel de detalles, en **Configuración** , haga clic en Cambiar la configuración global.
3. En la ficha **Experiencia del cliente**, en **Página principal**, haga clic en **Mostrar página principal** y, a continuación, escriba la dirección web de la página principal personalizada.
4. Haga clic en **Aceptar** y luego en **Cerrar.**

### Para configurar una página principal personalizada en un perfil de sesión

1. En la utilidad de configuración, en la pestaña **Configuración** , en el panel de navegación, expanda **Políticas de Citrix Gateway** y, a continuación, haga clic en **Sesión.**
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar.**
3. En Nombre, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo.**
5. En **Nombre**, escriba un nombre para el perfil.
6. En la ficha **Experiencia del cliente**, junto a **Página principal**, haga clic en **Modificar global**, haga clic en **Mostrar página principal** y, a continuación, escriba la dirección web de la página principal.
7. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresiones con nombre**, seleccione **General**, seleccione Valor verdadero, haga clic en **Agregar expresión**, en **Crear** y, a continuación, en **Cerrar**.

## Cambiar la interfaz de acceso

March 27, 2024

Es posible que quiera dirigir a los usuarios a una página principal personalizada, en lugar de depender de la interfaz de acceso. Para ello, instale la página principal en NetScaler Gateway y, a continuación, configure la directiva de sesión para que utilice la nueva página principal.

### Para instalar una página de inicio personalizada

1. En la utilidad de configuración, haga clic en la ficha **Configuración** y, a continuación, en el panel de navegación, haga clic en **Citrix Gateway.**
2. En el panel de detalles, en **Personalizar interfaz de acceso**, haga clic en **Cargar**la **interfaz de acceso.**
3. Para instalar la página principal desde un archivo en un equipo de la red, en Archivo local, haga clic en **Examinar**, desplácese hasta el archivo y, a continuación, haga clic en **Seleccionar.**
4. Para utilizar una página principal instalada en NetScaler Gateway, en Ruta de acceso remota, haga clic en **Examinar**, seleccione el archivo y, a continuación, haga clic en **Seleccionar.**
5. Haga clic en **Cargar** y, a continuación, en **Cerrar.**

## Crear y aplicar vínculos web y de recursos compartidos de archivos

March 27, 2024

Puede configurar la interfaz de acceso para mostrar un conjunto de vínculos a los recursos internos disponibles para los usuarios. Para crear estos vínculos es necesario definir primero los vínculos como recursos. A continuación, los vincula a un usuario, grupo, servidor virtual o globalmente para activarlos en la interfaz de acceso. Los enlaces que cree aparecen en los paneles **Sitios web y recursos compartidos de archivos** , en
**Sitios web empresariales** y Recursos **compartidos de archivos empresariales** . Si los usuarios agregan sus propios enlaces, estos enlaces aparecen en **Sitios web personales** y Recursos **compartidos de archivos personales** .

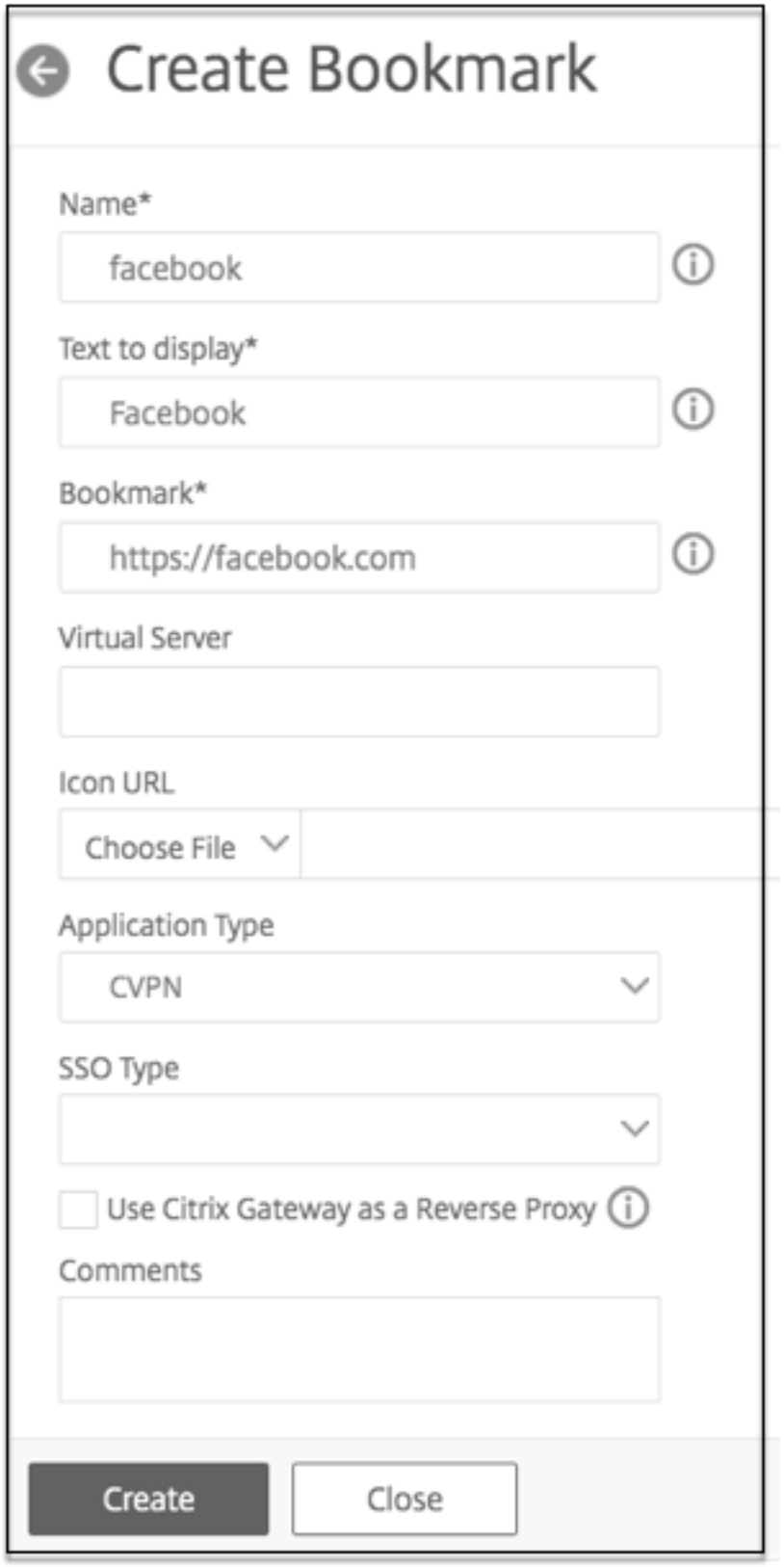
 

## Creación de marcadores de empresa

### Para crear un vínculo de interfaz de acceso en una directiva de sesión

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Recursos** y, a continuación, haga clic en **Marcadores del portal.**
2. En el panel de detalles, haga clic en **Agregar.**




3. En **Nombre**, escriba un nombre para el marcador.

4. En **Texto** para mostrar, escriba la descripción del enlace. La descripción aparece en la **interfaz de acceso.**
5. En **Marcador**, escriba la dirección web, haga clic en **Crear** y, a continuación, haga clic en **Cerrar.**

Si habilita el acceso sin cliente, puede asegurarse de que las solicitudes a los sitios web pasan por NetScaler Gateway. Por ejemplo, ha agregado un marcador para Google. En el cuadro de diálogo **Crear marcador**, active la casilla **Usar NetScaler Gateway como proxy inverso**. Al seleccionar esta casilla de verificación, las solicitudes del sitio web van del dispositivo del usuario a NetScaler Gateway y, a continuación, al sitio web. Al desactivar la casilla de verificación, las solicitudes van del dispositivo del usuario al sitio web. Esta casilla de verificación solo está disponible si habilita el acceso sin cliente.

#### Para enlazar un enlace de interfaz de acceso

Puede enlazar vínculos de la interfaz de acceso a las siguientes ubicaciones:

- Usuarios
- Grupos
- Servidores virtuales

Después de guardar la configuración, los vínculos están disponibles para los usuarios en la interfaz de acceso de la ficha **Inicio**, que es la primera página que ven los usuarios después de iniciar sesión correctamente. Los enlaces se organizan en la página según el tipo, como enlaces a sitios web o como enlaces para compartir archivos.

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:
   - Amplíe **Administración de usuarios de Citrix Gateway** y, a continuación, haga clic en **Usuarios AAA.**
   - Expanda **Administración de usuarios de NetScaler Gateway** y, a continuación, haga clic en **Grupos AAA.**
   - Amplíe **Citrix Gateway** y, a continuación, haga clic en **Servidores virtuales.**
2. En el panel de detalles, realice una de las acciones siguientes:
   - Seleccione un usuario y, a continuación, haga clic en Abrir.
   - Seleccione un grupo y, a continuación, haga clic en Abrir.
   - Seleccione un servidor virtual y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo, haga clic en la ficha **Marcadores**.
4. En **Marcadores disponibles**, selecciona uno o varios marcadores, haga clic en la flecha derecha para mover los marcadores en Marcadores configurados y, a continuación, en **Aceptar.**

**Para enlazar marcadores de forma global mediante la interfaz gráfica de usuario**

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global.**
2. En el panel de detalles, en **Marcadores**, haga clic en **Crear vínculos a las aplicaciones HTTP y de uso compartido de archivos de Windows a las que quiere que se pueda acceder en la página del portal de NetScaler Gateway**.


3. En el cuadro de diálogo **Configurar enlace global de VPN***, haga clic en **Agregar.**
4. En **Disponible**, seleccione uno o varios marcadores, haga clic en la flecha derecha para mover los marcadores en Configurado y, a continuación, en **Aceptar**.

**Para agregar un marcador Enterprise mediante la CLI**

En la línea de comandos, escriba:

```
add vpn url <urlName> <linkName> <actualURL>  [-ssotype <ssotype>]
<!--NeedCopy-->
```

**Ejemplo:**

Marcador web

```
add vpn url google google "https://www.google.com"
<!--NeedCopy-->
```

Marcador para compartir archivos

```
add vpn url fileshare fileshare \fileshare.abc.com/shares
<!--NeedCopy-->
```

#### Para enlazar un marcador Enterprise mediante la CLI

Puede enlazar marcadores de empresa a usuario, grupo, servidor virtual y nivel global.

```
bind aaa user <userName> -urlName <string>
bind aaa group <groupName> -urlName <string>
bind vpn vserver <vserverName> -urlName <string>
bind vpn global  – urlName <string>
<!--NeedCopy-->
```

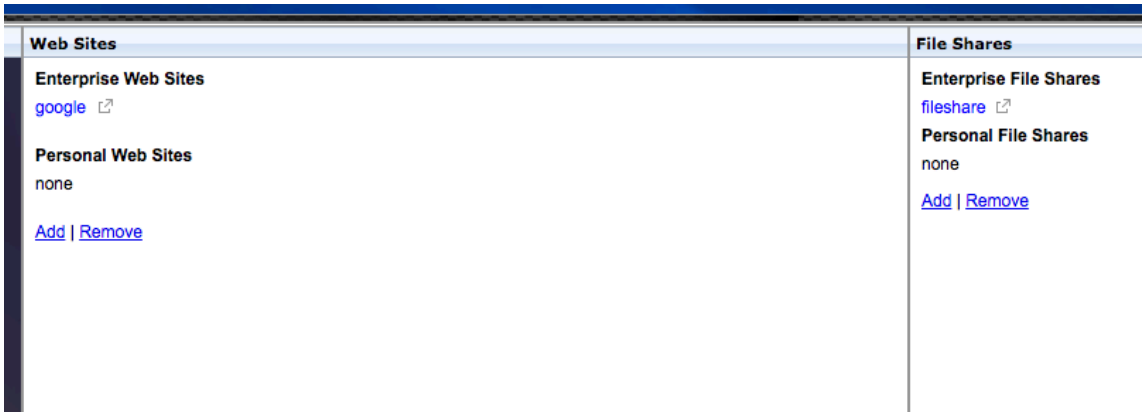
**Ejemplo:**

```
bind vpn global -urlName google
bind vpn global  – urlName fileshare
<!--NeedCopy-->
```

### Creación de marcadores personales

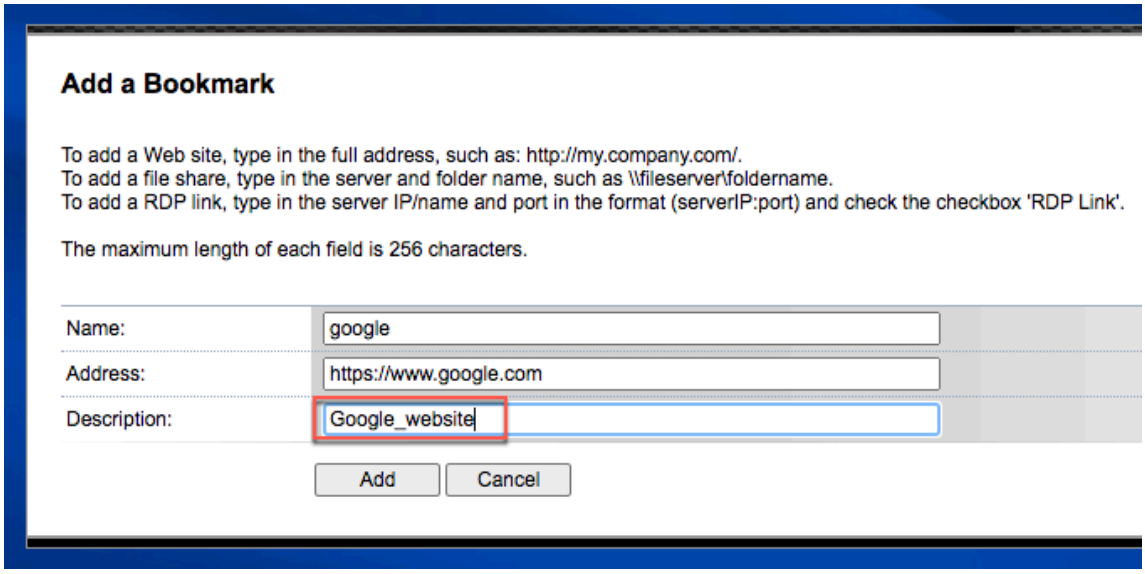
Puede crear sitios web personales y compartir archivos únicamente desde el servidor virtual VPN. No existe una interfaz gráfica de usuario de administración de NetScaler Gateway para agregar marcadores personales.

1. Inicie sesión en un servidor virtual VPN.
2. Haga clic en **Acceso de red** o **Acceso sin cliente** para agregar un marcador o compartir archivos.
3. Haga clic en **Agregar**.



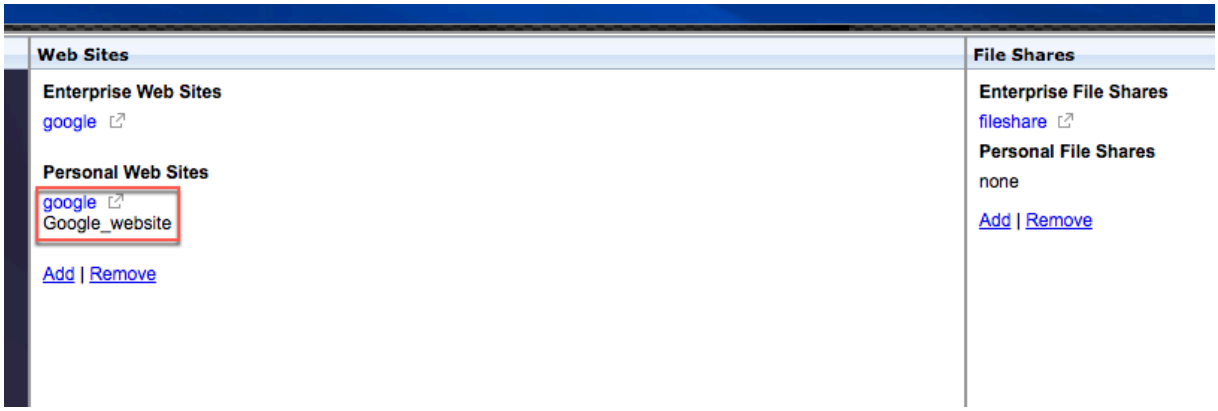

4. Introduzca los detalles del marcador, como el nombre del sitio web, la dirección y la descripción.




5. Haga clic en **Agregar**.

Los sitios web o los archivos compartidos que ha agregado aparecen en las pestañas correspondientes.




## Configurar tokens de nombre de usuario en marcadores

January 26, 2024

Puede configurar las URL de marcadores y recursos compartidos de archivos mediante un token especial,%username%. Cuando los usuarios inician sesión, el token se sustituye por el nombre de inicio de sesión de cada usuario. Por ejemplo, crea un marcador para un empleado llamado Jack para una carpeta como\\ EmployeeServer\%username%\. Cuando Jack inicia sesión, la URL del recurso compartido de archivos se asigna a\\ EmployeeServer\ Jack\. Al configurar tokens de nombre de usuario en los marcadores, tenga en cuenta las siguientes situaciones:

- Si utiliza un tipo de autenticación, el nombre de usuario sustituye al token%username%.
- Si utiliza la autenticación de dos factores, el nombre de usuario del tipo de autenticación principal se utiliza para reemplazar el tokenusername%%.
- Si utiliza la autenticación de certificados de cliente, el campo de nombre de usuario del perfil de autenticación de certificados de cliente se utiliza para reemplazar el tokenusername%%.

## Crear y aplicar enlaces web

March 27, 2024

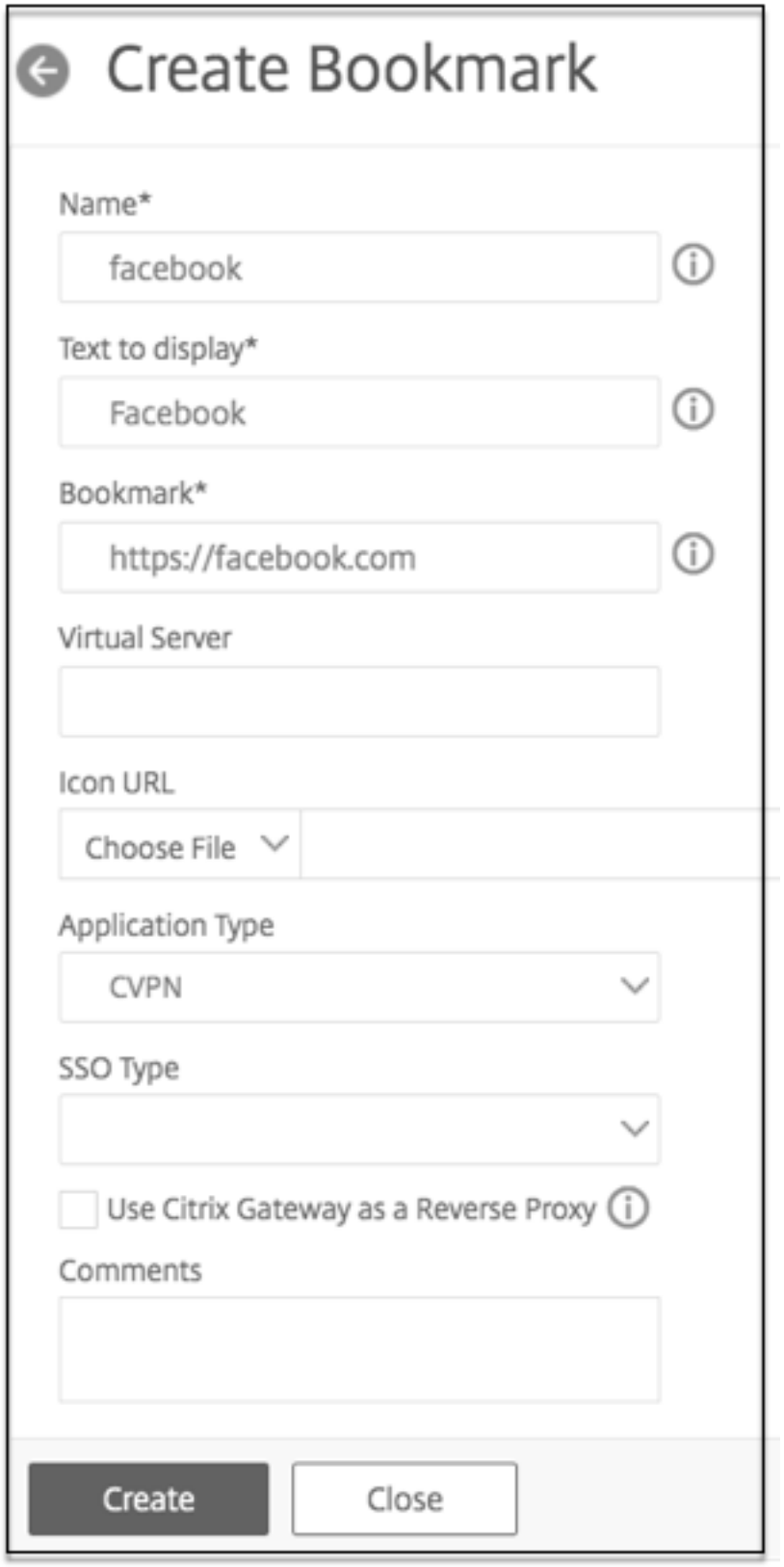
Puede configurar la interfaz de acceso para mostrar un conjunto de vínculos a los recursos internos disponibles para los usuarios. Para crear estos vínculos es necesario definir primero los vínculos como recursos. A continuación, los vincula a un usuario, grupo, servidor virtual o globalmente para activarlos en la interfaz de acceso. Los vínculos que cree aparecen en los paneles **Sitios web** de **Sitios web de empresa**.

### Creación de marcadores de empresa

#### Para crear un vínculo de interfaz de acceso en una directiva de sesión

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Recursos** y, a continuación, haga clic en **Marcadores del portal.**
2. En el panel de detalles, haga clic en **Agregar.**




3. En **Nombre**, escriba un nombre para el marcador.

4. En **Texto para mostrar**, escriba la descripción del enlace. La descripción aparece en la **interfaz de acceso.**
5. En **Marcar como favorito**, escriba la dirección web de la aplicación.
6. En **Servidor virtual**, escriba el nombre del servidor virtual de equilibrio de carga/conmutación de contenido asociado. Este campo es opcional.
7. En **URL del icono**, los iconos cargados son compatibles con todos los temas, excepto el tema predeterminado. El tamaño máximo recomendado es de 70 x 70 píxeles. Le recomendamos que utilice imágenes transparentes. Este campo es opcional.
8. En **Tipo de aplicación**, seleccione el tipo de aplicación (VPN, VPN sin cliente o SaaS) que representa la URL. Este campo es opcional.
9. En **Tipo de SSO**, seleccione el tipo de SSO que quiera configurar para el marcador. Cuando se configura SSO, los usuarios pueden acceder a las aplicaciones sin tener que introducir sus credenciales en los inicios de sesión posteriores. Se admiten los siguientes tipos de SSO:

    - Puerta de enlace unificada: Esta configuración de SSO permite el acceso remoto seguro a varios recursos de una aplicación a través de una única URL.
    - Autenticación automática: En esta configuración de SSO, se pide a los usuarios de NetScaler Gateway que proporcionen las credenciales de inicio de sesión para acceder a la aplicación.
    - Autenticación basada en SAML: En esta configuración de SSO, NetScaler Gateway utiliza un IdP para validar los detalles del usuario, genera una afirmación de SAML y la envía al SP. Si se aprueba la validación, el SSO se ha realizado correctamente.

    > **Nota:**
    >
    > Si habilita el acceso sin cliente, puede asegurarse de que las solicitudes a los sitios web pasen por Citrix Gateway. Por ejemplo, ha agregado un marcador para Google. Seleccione la casilla **Usar NetScaler Gateway como proxy inverso**. Al seleccionar esta casilla de verificación, las solicitudes del sitio web van del dispositivo del usuario a NetScaler Gateway y, a continuación, al sitio web. Al desactivar la casilla de verificación, las solicitudes van del dispositivo del usuario al sitio web. Esta casilla de verificación solo está disponible si habilita el acceso sin cliente.

10. Haga clic en **Crear** y, a continuación, en **Cerrar.**

#### Para enlazar un enlace de interfaz de acceso

Puede enlazar vínculos de la interfaz de acceso a las siguientes ubicaciones:

- Usuarios

- Grupos
- Servidores virtuales

Después de guardar la configuración, los vínculos están disponibles para los usuarios en la interfaz de acceso de la ficha **Inicio**, que es la primera página que ven los usuarios después de iniciar sesión correctamente.

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:
    - Amplíe **Administración de usuarios de Citrix Gateway** y, a continuación, haga clic en **Usuarios AAA.**
    - Expanda **Administración de usuarios de NetScaler Gateway** y, a continuación, haga clic en **Grupos AAA.**
    - Amplíe **Citrix Gateway** y, a continuación, haga clic en **Servidores virtuales.**
2. En el panel de detalles, realice una de las acciones siguientes:
    - Seleccione un usuario y, a continuación, haga clic en Abrir.
    - Seleccione un grupo y, a continuación, haga clic en Abrir.
    - Seleccione un servidor virtual y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo, haga clic en la ficha **Marcadores**.
4. En **Marcadores disponibles**, selecciona uno o varios marcadores, haga clic en la flecha derecha para mover los marcadores en Marcadores configurados y, a continuación, en **Aceptar.**

**Para enlazar marcadores de forma global mediante la interfaz gráfica de usuario**

1. En la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global.**
2. En el panel de detalles, en **Marcadores**, haga clic en **Crear vínculos a las aplicaciones HTTP y de uso compartido de archivos de Windows a las que quiere que se pueda acceder en la página del portal de NetScaler Gateway**.


3. En el cuadro de diálogo **Configurar enlace global de VPN***, haga clic en **Agregar.**
4. En **Disponible**, seleccione uno o varios marcadores, haga clic en la flecha derecha para mover los marcadores en Configurado y, a continuación, en **Aceptar**.

#### Para agregar un marcador Enterprise mediante la CLI

En la línea de comandos, escriba:

```
add vpn url <urlName> <linkName> <actualURL>  [-ssotype <ssotype>]
<!--NeedCopy-->
```

**Ejemplo:**

Marcador web

```
add vpn url google google "https://www.google.com"
<!--NeedCopy-->
```

#### Para enlazar un marcador Enterprise mediante la CLI

Puede enlazar marcadores de empresa a usuario, grupo, servidor virtual y nivel global.

```
bind aaa user <userName> -urlName <string>
bind aaa group <groupName> -urlName <string>
bind vpn vserver <vserverName> -urlName <string>
bind vpn global  – urlName <string>
<!--NeedCopy-->
```

**Ejemplo:**

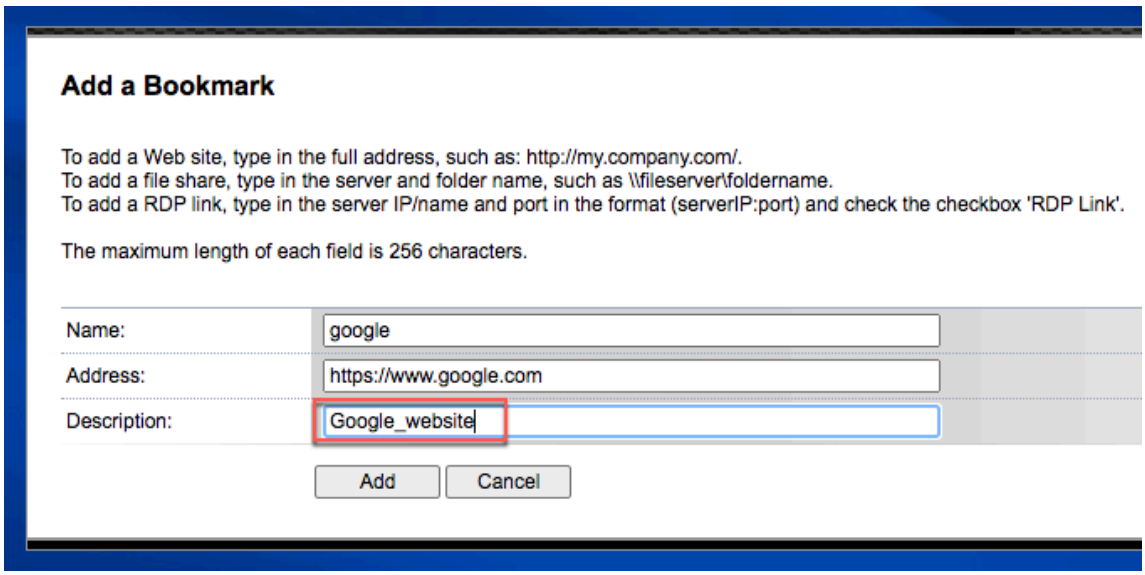
```
bind vpn global -urlName google
<!--NeedCopy-->
```

### Creación de marcadores personales

Solo puede crear sitios web personales desde el servidor virtual VPN. No existe una interfaz gráfica de usuario de administración de NetScaler Gateway para agregar marcadores personales.

1. Inicie sesión en un servidor virtual VPN.
2. Haga clic en **Acceso a red** o **Acceso sin cliente** para agregar un marcador.
3. Haga clic en **Agregar**.


4. Introduzca los detalles del marcador, como el nombre del sitio web, la dirección y la descripción.



5. Haga clic en **Agregar**.

Los sitios web que ha agregado aparecen en las fichas respectivas.


### Configurar tokens de nombre de usuario en marcadores

Puede configurar las URL de marcadores y recursos compartidos de archivos mediante un token especial,%username%. Cuando los usuarios inician sesión, el token se sustituye por el nombre de inicio de sesión de cada usuario. Por ejemplo, crea un marcador para un empleado llamado Jack para una carpeta como\\ EmployeeServer\%username%\. Cuando Jack inicia sesión, la URL del recurso compartido de archivos se asigna a\\ EmployeeServer\ Jack\. Al configurar tokens de nombre de usuario en los marcadores, tenga en cuenta las siguientes situaciones:

- Si utiliza un tipo de autenticación, el nombre de usuario sustituye al token%username%.

- Si utiliza la autenticación de dos factores, el nombre de usuario del tipo de autenticación principal se utiliza para reemplazar el token`username`%%.
- Si utiliza la autenticación de certificados de cliente, el campo de nombre de usuario del perfil de autenticación de certificados de cliente se utiliza para reemplazar el token`username`%%.

## Cómo funciona una directiva de tráfico

January 26, 2024

Las directivas de tráfico permiten configurar los siguientes ajustes para las conexiones de usuario:

- Aplicar tiempos de espera más cortos para aplicaciones sensibles a las que se accede desde redes que no son de confianza.
- Cambiar el tráfico de red para utilizar TCP en algunas aplicaciones. Si selecciona TCP, debe habilitar o inhabilitar el inicio de sesión único para determinadas aplicaciones.
- Identificar situaciones en las que quiere utilizar otras funciones HTTP para el tráfico de complementos de NetScaler Gateway.
- Definición de las extensiones de nombre de archivo que se utilizan con la asociación de tipos de archivo.

## Crear una directiva de tráfico

March 27, 2024

Para configurar una directiva de tráfico, crea un perfil y configura los siguientes parámetros:

- Protocolo (HTTP o TCP)
- Tiempo de espera de aplicación
- Inicio de sesión único en aplicaciones web
- Formulario de inicio de sesión único
- Asociación de tipos de archivos
- Plug-in repetidor
- Cuentas Kerberos Constrained Delegated (KCD)

Después de crear la directiva de tráfico, puede vincularla a servidores virtuales, usuarios, grupos o de forma global.

Por ejemplo, tiene la aplicación web PeopleSoft Human Resources instalada en un servidor de la red interna. Puede crear una directiva de tráfico para esta aplicación que defina la dirección IP de destino,

el puerto de destino y puede establecer la cantidad de tiempo que un usuario puede permanecer conectado a la aplicación, por ejemplo, 15 minutos.

Si quiere configurar otras funciones, como la compresión HTTP en una aplicación, puede utilizar una directiva de tráfico para configurar la configuración. Al crear la directiva, utilice el parámetro HTTP para la acción. En la expresión, cree la dirección de destino del servidor que ejecuta la aplicación.

### Para configurar una política de tráfico

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **Citrix Gateway > Directivas y, a continuación,** haga clic en **Tráfico** .
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear directiva de tráfico**, en **Nombre**, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En **Protocolo**, seleccione **HTTP** o **TCP**.

   > **Nota:** Si selecciona TCP como protocolo, no podrá configurar el inicio de sesión único y la configuración se inhabilitará en el cuadro de diálogo del perfil.

7. En **AppTimeout (minutos)**, escriba el número de minutos. Esta configuración limita el tiempo que los usuarios pueden permanecer conectados a la aplicación web.
8. Para habilitar el inicio de sesión único en la aplicación web, en Inicio de **sesión único**, seleccione **ACTIVADO**.

   **Nota**: Si quieres usar el inicio de sesión único basado en formularios, puedes configurar los ajustes en el perfil de tráfico. Para obtener más información, consulte Configuración del inicio de sesión único basado en formularios.
9. Para especificar una asociación de tipos de archivo, en Asociación de **tipos de archivo**, seleccione **ACTIVADA**.
10. Para utilizar el complemento Repeater para optimizar el tráfico de red, en Citrix SD-WAN, seleccione Activado, haga clic **enCrear**y, a continuación, en**Cerrar**.
11. Si configura KCD en el dispositivo, en Cuenta KCD, seleccione la cuenta.

    Para obtener más información sobre cómo configurar KCD en el dispositivo, consulte Configuración de la delegación restringida de Kerberos en un dispositivo NetScaler.
12. En el cuadro de diálogo **Crear política de tráfico** , cree o agregue una expresión, haga clic en **Crear y,** a continuación, en **Cerrar** .

# Configurar Single Sign-On basado en formularios

March 27, 2024

El inicio de sesión único basado en formularios permite a los usuarios iniciar sesión una vez en todas las aplicaciones protegidas de la red. Al configurar el inicio de sesión único basado en formularios en NetScaler Gateway, los usuarios pueden acceder a aplicaciones web que requieren un inicio de sesión basado en formularios HTML sin tener que volver a escribir la contraseña. Sin el inicio de sesión único, los usuarios deben iniciar sesión por separado para acceder a cada aplicación.

Después de crear el perfil de inicio de sesión único del formulario, creará un perfil de tráfico y una directiva que incluya el perfil de inicio de sesión único del formulario. Para obtener más información, consulte Creación de una directiva de tráfico.

## Para configurar el inicio de sesión único basado en formularios

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Tráfico.
2. En el panel de detalles, haga clic en la ficha Perfiles de SSO de formulario y, a continuación, haga clic en Agregar.
3. En Nombre , escriba un nombre para el perfil.
4. En URL de acción, escriba la URL a la que se envía el formulario completado.

   > **Nota:** La URL es la URL relativa raíz.

5. En Campo de nombre de usuario, escriba el nombre del atributo para el campo de nombre de usuario.
6. En Campo de contraseña, escriba el nombre del atributo para el campo de contraseña.
7. En Regla de éxito de SSO, cree una expresión que describa la acción que realiza este perfil cuando lo invoca una directiva. También puede crear la expresión mediante los botones Prefijo, Agregar y Operador de este campo.

   Esta regla comprueba si el inicio de sesión único se ha realizado correctamente o no.
8. En Pareja de valores de nombre, escriba el valor del campo de nombre de usuario, seguido de una y comercial (&) y, a continuación, el valor del campo de contraseña.

   Los nombres de los valores están separados por una y comercial (&), como name1=value1&name2=value2.
9. En Tamaño de respuesta, escriba el número de bytes para permitir el tamaño de respuesta completo. Escriba el número de bytes de la respuesta que se analizará para extraer los formularios.

10. En Extracción, seleccione si el par nombre/valor es estático o dinámico. La configuración predeterminada es Dinámica.
11. En Método de envío, seleccione el método HTTP utilizado por el formulario de inicio de sesión único para enviar las credenciales de inicio de sesión al servidor de inicio de sesión. El valor predeterminado es Get.
12. Haga clic en Create y, luego, en Close.

## Configurar SAML Single Sign-On

March 27, 2024

Puede crear un perfil SAML 1.1 o SAML 2.0 para el inicio de sesión único (SSO). Los usuarios pueden conectarse a aplicaciones web compatibles con el protocolo SAML para el inicio de sesión único. NetScaler Gateway admite el inicio de sesión único del proveedor de identidades (IdP) para aplicaciones web SAML.

### Para configurar el inicio de sesión único de SAML

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Tráfico.
2. En el panel de detalles, haga clic en la ficha Perfil de inicio de sesión único de SAML.
3. En el panel de detalles, haga clic en Agregar.
4. En Nombre , escriba un nombre para el perfil.
5. En Nombre del certificado de firma, introduzca el nombre del certificado X.509.
6. En ACS URL, introduzca el servicio de aserción de consumidor del proveedor de identidad o de servicio. AssertionConsumerServiceURL (URL ACS) proporciona capacidad de inicio de sesión único para los usuarios.
7. En Regla de estado de retransmisión, cree la expresión de la directiva a partir de expresiones de directiva guardadas y expresiones de uso frecuente. Seleccione en la lista Operador para definir cómo se evalúa la expresión. Para probar la expresión, haga clic en Evaluar.
8. En Enviar contraseña, selecciona ACTIVAR o DESACTIVAR.
9. En Nombre del emisor, introduzca la identidad de la aplicación SAML.
10. Haga clic en Create y, luego, en Close.

## Vincular una directiva de tráfico

March 27, 2024

Puede enlazar directivas de tráfico a servidores virtuales, grupos, usuarios y a NetScaler Gateway Global. Puede utilizar la utilidad de configuración para enlazar una directiva de tráfico.

### Para vincular una política de tráfico globalmente mediante la utilidad de configuración

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Tráfico.
2. En el panel de detalles, seleccione una directiva y, a continuación, en Acción, haga clic en Enlaces globales.
3. En el cuadro de diálogo Vincular o desvincular directivas de tráfico, en Detalles, haga clic en Insertar directiva.
4. En Nombre de directiva, seleccione la directiva y, a continuación, haga clic en Aceptar.

## Eliminar directivas de tráfico

March 27, 2024

Puede utilizar la utilidad de configuración para quitar las directivas de tráfico de NetScaler Gateway. Si utiliza la utilidad de configuración para quitar una directiva de tráfico y la directiva está vinculada al nivel de usuario, grupo o servidor virtual, primero debe desvincular la directiva. A continuación, puede quitar la directiva.

### Para desvincular una política de tráfico mediante la utilidad de configuración

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:
    - Amplíe Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
    - **Amplíe Citrix Gateway > Administración**de usuarios y, a continuación, haga clic en **Grupos AAA** .
    - **Amplíe Citrix Gateway > Administración**de usuarios y, a continuación, haga clic en **Usuarios AAA** .

2. En el panel de detalles, seleccione un servidor virtual, grupo o usuario y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar el **servidor virtual Citrix Gateway, Configurar el grupo AAA o Configurar el usuario** AAA , haga clic en la pestaña **Directivas** .
4. Haz clic en **Tráfico** , selecciona la política y, a continuación, haz clic en **Desvincular política** .
5. Haga clic en **Aceptar** y, a continuación, en **Cerrar**.

Una vez que la directiva de tráfico no esté vinculada, puede quitarla.

### Para eliminar una política de tráfico mediante la utilidad de configuración

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **Citrix Gateway > Directivas** y, a continuación, haga clic en Tráfico.
2. En el panel de detalles, en la pestaña Políticas, seleccione la política de tráfico y, a continuación, haga clic en Eliminar.

## Configurar directivas de sesión

March 27, 2024

Una directiva de sesión es un conjunto de expresiones y configuraciones que se aplican a usuarios, grupos, servidores virtuales y de forma global.

Se utiliza una directiva de sesión para configurar la configuración de las conexiones de usuario. Puede definir opciones para configurar el software con el que los usuarios inician sesión, como el plug-in de NetScaler Gateway para Windows o el plug-in de NetScaler Gateway para Mac. También puede configurar los parámetros para exigir a los usuarios que inicien sesión con Citrix Receiver o Secure Hub. Las directivas de sesión se evalúan y aplican después de autenticar al usuario.

Las directivas de sesión se aplican según las reglas siguientes:

- Las directivas de sesión siempre anulan la configuración global de la configuración.
- Los atributos o parámetros que no se establecen mediante una directiva de sesión se establecen en las directivas establecidas para el servidor virtual.
- Cualquier otro atributo que no esté establecido por una directiva de sesión o por el servidor virtual se establece en la configuración global.

> **Importante**: Las siguientes instrucciones son directrices generales para crear políticas de sesión. Existen instrucciones específicas para configurar directivas de sesión para distintas configuraciones, como el acceso sin cliente o el acceso a aplicaciones publicadas. Las instrucciones

> pueden contener instrucciones para configurar una configuración específica; sin embargo, esa configuración puede ser una de las muchas opciones incluidas en un perfil y una directiva de sesión. Las instrucciones le indican que cree una configuración dentro de un perfil de sesión y, a continuación, aplique el perfil a una directiva de sesión. Puede cambiar la configuración de un perfil y una directiva sin crear una nueva directiva de sesión. Además, puede crear toda la configuración a nivel global y, a continuación, crear una directiva de sesión para anular la configuración global.

Si implementa Citrix Endpoint Management o StoreFront en su red, Citrix recomienda utilizar el Asistente de configuración rápida para configurar perfiles y directivas de sesión. Al ejecutar el asistente, define la configuración de su implementación. A continuación, NetScaler Gateway crea las directivas de autenticación, sesión y acceso sin cliente necesarias.

### Para crear una directiva de sesión

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En Nombre , escriba un nombre para el perfil.
6. Complete la configuración del perfil de sesión y, a continuación, haga clic en Crear.
7. En el cuadro de diálogo Crear perfil de sesión, agregue una expresión para la directiva, haga clic en Crear y, a continuación, haga clic en Cerrar.
   Nota: En la expresión, seleccione Valor
   verdadero para que la directiva se aplique siempre al nivel al que está vinculada.

## Crear un perfil de sesión

March 27, 2024

Un perfil de sesión contiene la configuración de las conexiones de usuario.

Los perfiles de sesión especifican las acciones que se aplican a una sesión de usuario si el dispositivo de usuario cumple las condiciones de expresión de la directiva. Los perfiles se utilizan con directivas de sesión. Puede utilizar la utilidad de configuración para crear perfiles de sesión por separado de una directiva de sesión y, a continuación, utilizarlo para varias directivas. Solo puede utilizar un perfil con una directiva.

### Configuración de los ajustes de red para las conexiones de usuario en un perfil de sesión

Puede utilizar la ficha Configuración de red del perfil de sesión para configurar las siguientes opciones de red para las conexiones de usuario:

- Servidor DNS
- Dirección IP del servidor WINS
- Dirección IP asignada que puede utilizar como dirección IP de intranet
- Configuración de desbordamiento para grupos de direcciones (direcciones IP de intranet)
- Sufijo DNS IP de intranet
- Puertos HTTP
- Configuración de tiempo de espera forzado

### Configuración de los ajustes de conexión en un perfil de sesión

Puede utilizar la ficha Experiencia del cliente del perfil de sesión para configurar los siguientes ajustes de conexión:

- Interfaz de acceso o página de inicio personalizada
- Dirección web para correo electrónico basado en web, como Outlook Web Access
- tipo de complemento (plug-in de NetScaler Gateway para Windows, plug-in de NetScaler Gateway para Mac OS X o plug-in de NetScaler Gateway para Java)
- Túneles divididos
- Configuración de tiempo de espera de sesión e inactividad
- Acceso sin cliente
- Codificación URL de acceso sin cliente
- tipo de plug-in (Windows, Mac o Java)
- Inicio de sesión único en aplicaciones web
- Índice de credenciales para autenticación
- Inicio de sesión único con Windows
- Comportamiento de limpieza de clientes
- Scripts de inicio de sesión
- Configuración de depuración del cliente
- DNS dividido
- Acceso a direcciones IP de redes privadas y acceso LAN local
- Opciones del cliente
- Configuración de proxy

Para obtener más información sobre cómo configurar los valores de las conexiones de usuario, consulte Configuración de conexiones para el plug-in de NetScaler Gateway.

### Configuración de los ajustes de seguridad en un perfil de sesión

Puede utilizar la ficha Seguridad de un perfil de sesión para configurar las siguientes opciones de seguridad:

- Acción de autorización predeterminada (permitir o denegar)
- Secure Browse para conexiones desde dispositivos iOS
- Grupos de cuarentena
- Grupos de autorización

Para obtener más información sobre cómo configurar la autorización en NetScaler Gateway, consulte Configuración de la autorización.

### Configuración de los parámetros de Citrix Virtual Apps and Desktops en un perfil de sesión

Puede utilizar la ficha Aplicaciones publicadas de un perfil de sesión para configurar las siguientes opciones de conexión a servidores que ejecutan Citrix Virtual Apps and Desktops:

- Proxy ICA, que son conexiones de cliente mediante Citrix Receiver
- Dirección de Interfaz Web
- Modo portal de Interfaz Web
- Inicio de sesión único en el dominio de la comunidad de servidores
- Página principal de Receiver
- Dirección de servicios de cuenta

Para obtener más información sobre cómo configurar los valores para conectarse a aplicaciones publicadas en un conjunto de servidores, consulte Proporcionar acceso a aplicaciones publicadas y escritorios virtuales a través de la Interfaz Web.

Puede crear perfiles de sesión independientemente de una directiva de sesión. Al crear la directiva, puede seleccionar el perfil que quiere asociar a la directiva.

### Para crear un perfil de sesión mediante la utilidad de configuración

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, haga clic en la pestaña Perfiles y, a continuación, en Agregar .
3. Configure los ajustes del perfil, haga clic en Crear y, a continuación, en Cerrar.

Después de crear un perfil, puede incluirlo en una directiva de sesión.

### Para agregar un perfil a una política de sesión mediante la utilidad de configuración

1. En la utilidad de configuración, en el panel de navegación, expanda Access Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En la ficha Directivas, realice una de las siguientes acciones:
   - Haga clic en Agregar para crear una nueva directiva de sesión.
   - Seleccione una directiva y, a continuación, haga clic en Abrir.
3. En Solicitar perfil, seleccione un perfil de la lista.
4. Termine de configurar la política de sesión y, a continuación, realice una de las siguientes acciones:
   a) Haga clic en Crear y, a continuación, en Cerrar para crear la directiva.
   b) Haga clic en Aceptar y, a continuación, en Cerrar para modificar la política.

## Vincular directivas de sesión

January 26, 2024

Después de crear una directiva de sesión, enlaza a un usuario, grupo, servidor virtual o globalmente. Las directivas de sesión se aplican como jerarquía en el siguiente orden:

- Usuarios
- Grupos
- Servidores virtuales
- Globalmente

### Para vincular una directiva de sesión a un servidor virtual mediante la GUI

1. Vaya a **NetScaler Gateway > Servidores virtuales**.
2. Seleccione un servidor virtual y haga clic en **Modificar**. También puede crear un nuevo servidor virtual.
3. Desplácese hacia abajo hasta la sección **Directivas** y haga clic en el icono **+**.
4. En **Elegir directiva**, seleccione **Sesión**.
5. En **Elegir tipo**, seleccione **Solicitud**y haga clic en **Continuar**.
6. En **Seleccionar directiva**, seleccione la directiva que quiere enlazar a este servidor virtual.
7. En **Prioridad**, introduzca el número de prioridad de la directiva.
8. Haga clic en **Bind**.

### Para vincular una directiva de sesión a un grupo AAA de Citrix ADC mediante la GUI

1. Vaya a **NetScaler Gateway > Administración de usuarios > Grupos AAA**.
2. Seleccione un grupo NetScaler ADC AAA existente y haga clic en **Modificar**. También puede crear un grupo AAA de NetScaler ADC.
3. En **Configuración avanzada**, haga clic en **Directivas y,** a continuación, en el icono **+**.
4. En **Elegir directiva**, seleccione **Sesión**y haga clic en **Continuar**.
5. En **Seleccionar directiva**, seleccione la directiva que quiere enlazar a este grupo AAA de NetScaler ADC.
6. En **Prioridad**, introduzca el número de prioridad de la directiva.
7. Haga clic en **Bind**.

### Para vincular una directiva de sesión a un usuario AAA de Citrix ADC mediante la GUI

1. Vaya a **NetScaler Gateway > Administración de usuarios > Usuarios AAA**.
2. Seleccione un usuario de NetScaler ADC existente y haga clic en **Modificar**. También puede crear un usuario AAA de NetScaler ADC.
3. En **Configuración avanzada**, haga clic en **Directivas y,** a continuación, en el icono **+**.
4. En **Elegir directiva**, seleccione **Sesión**y haga clic en **Continuar**.
5. En **Seleccionar directiva**, seleccione la directiva que quiere enlazar a este usuario AAA de NetScaler ADC.
6. En **Prioridad**, introduzca el número de prioridad de la directiva.
7. Haga clic en **Bind**.

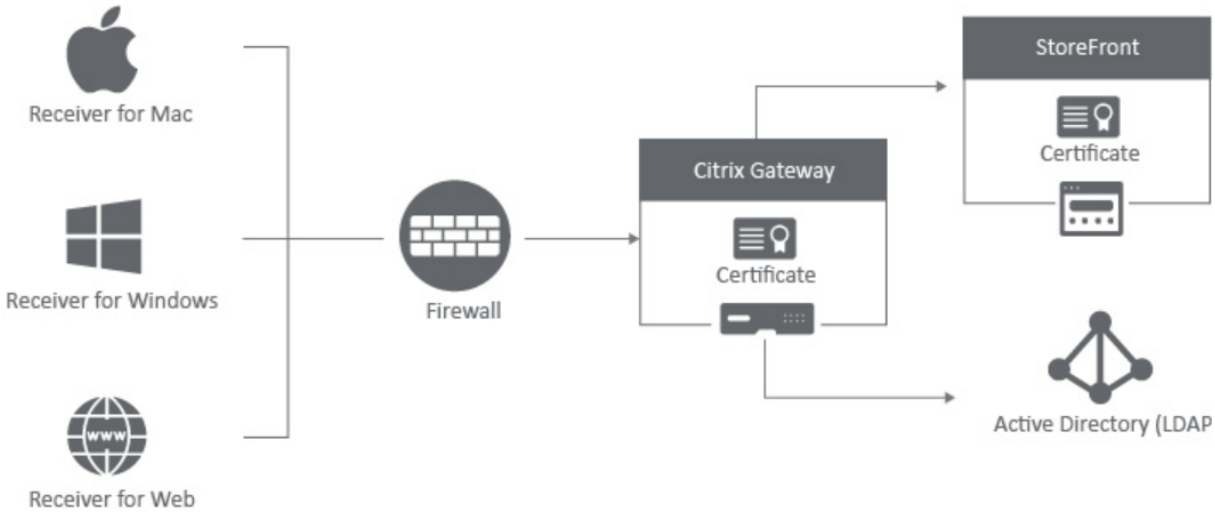
**Nota**: Para obtener más información sobre la prioridad, consulte https://support.citrix.com/article/CTX214588.

## Configuración de directivas de sesión de NetScaler Gateway para StoreFront

March 27, 2024

En este artículo se describe cómo configurar una autenticación de solo dominio de NetScaler Gateway con StoreFront para los usuarios que utilizan la aplicación Citrix Workspace o un explorador web.



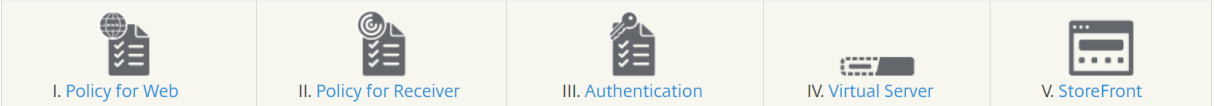

## Requisitos mínimos

- Citrix StoreFront 2.x o 3.0
- NetScaler ADC 10.5 y versiones posteriores
- Aplicación Citrix Workspace para Windows 4.x
- Aplicación Citrix Workspace para Mac 11.8
- Explorador web (aplicación Citrix Workspace para Web)
- Autenticación configurada en el dispositivo NetScaler ADC como se describe en CTX108876: cómo configurar la autenticación LDAP en un dispositivo NetScaler ADC
- Certificados SSL configurados para StoreFront Server y NetScaler Gateway. Para obtener información detallada sobre los temas siguientes, consulte la documentación de StoreFront.

  - Instalación y configuración de StoreFront 2.6

    - Certificados de Windows 2012 Server
    - Para agregar un enlace SSL a un sitio
    - Instalación y administración de certificados para el dispositivo NetScaler ADC 10.5

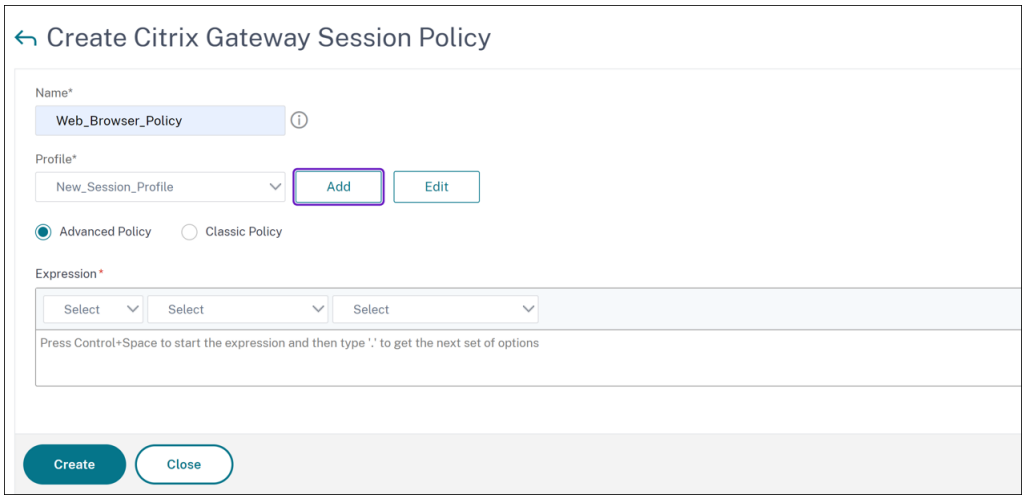
## Configuración de NetScaler Gateway con StoreFront



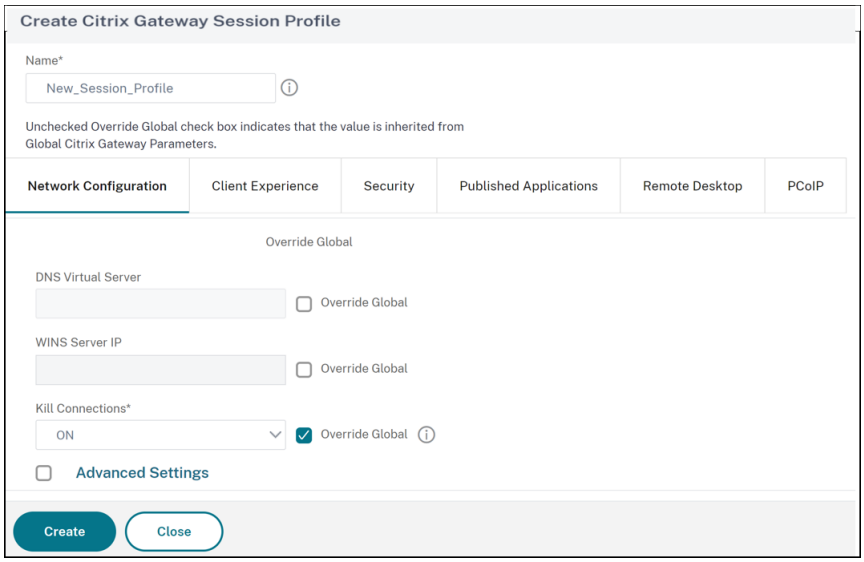

 

### Crear una directiva de sesión para el acceso basado en explorador web

1. Para crear una directiva de sesión, vaya a **NetScaler Gateway > Directivas > Sesión**.
2. En el campo **Directivas de sesión**, haga clic en **Agregar**.
3. En el campo **Nombre**, escriba el nombre de la directiva de sesión. Por ejemplo, Web_Browser_Policy.




4. Escriba el nombre del nuevo perfil de sesión en la ventana **Configurar perfil de sesión de NetScaler Gateway**.



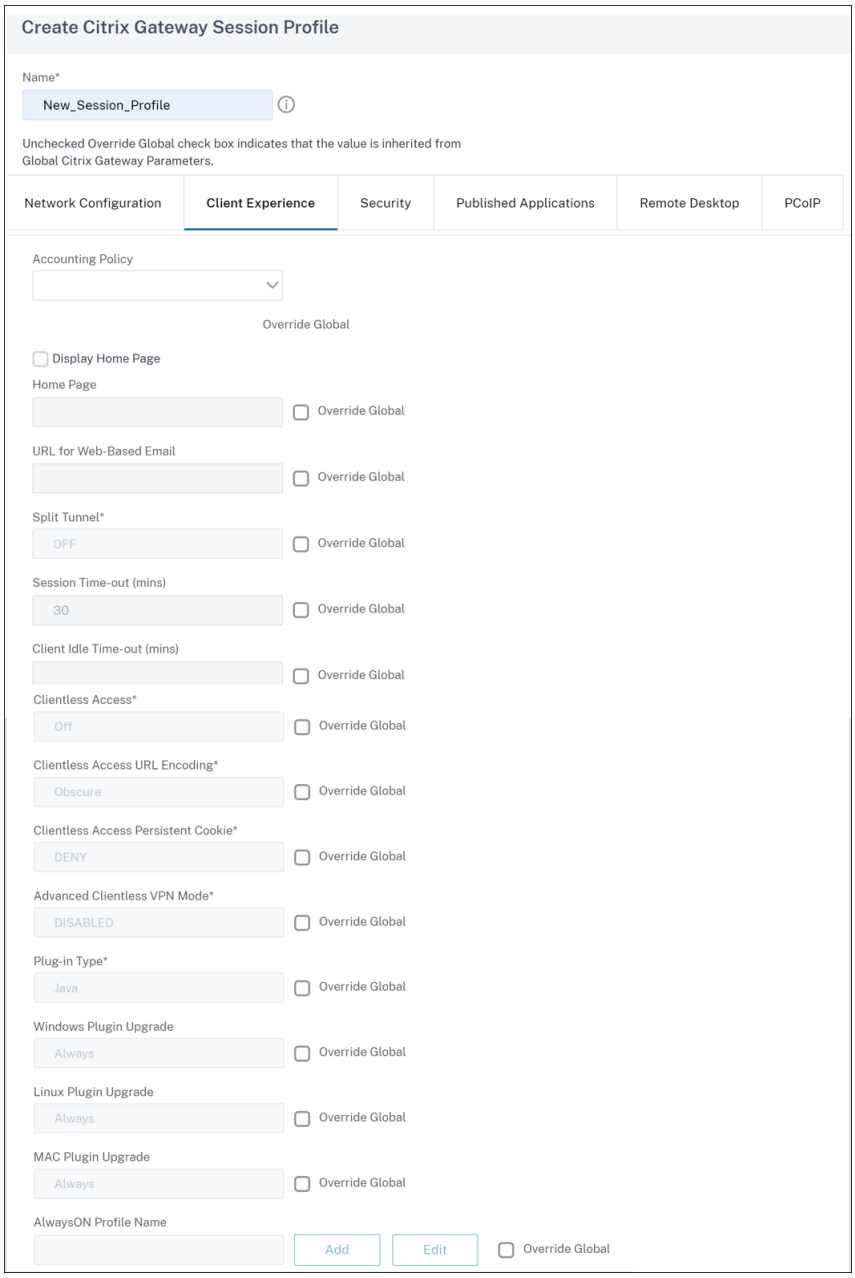

Puede marcar las casillas de verificación **Override Global** en todas las fichas para sobrescribir los valores heredados de los parámetros globales de NetScaler Gateway.
En el ejemplo de configuración, solo se incluyen detalles sobre los parámetros obligatorios.

5. En la ficha **Experiencia del cliente**, active la siguiente configuración:

   - **Acceso sin cliente**: configurado **en On**

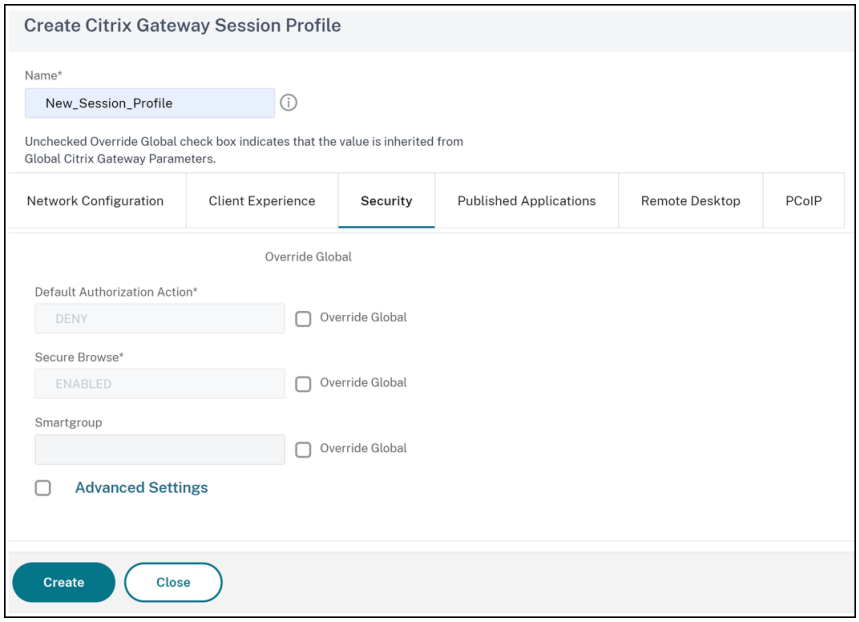
 

- **Inicio de sesión único en la aplicación**web : seleccione la casilla
- **Tipo de complemento: configurado enWindows/Mac OS X**




6. En la ficha **Seguridad**, active **Acciones de autorización predeterminadas** y defina el valor **PERMITIR**.

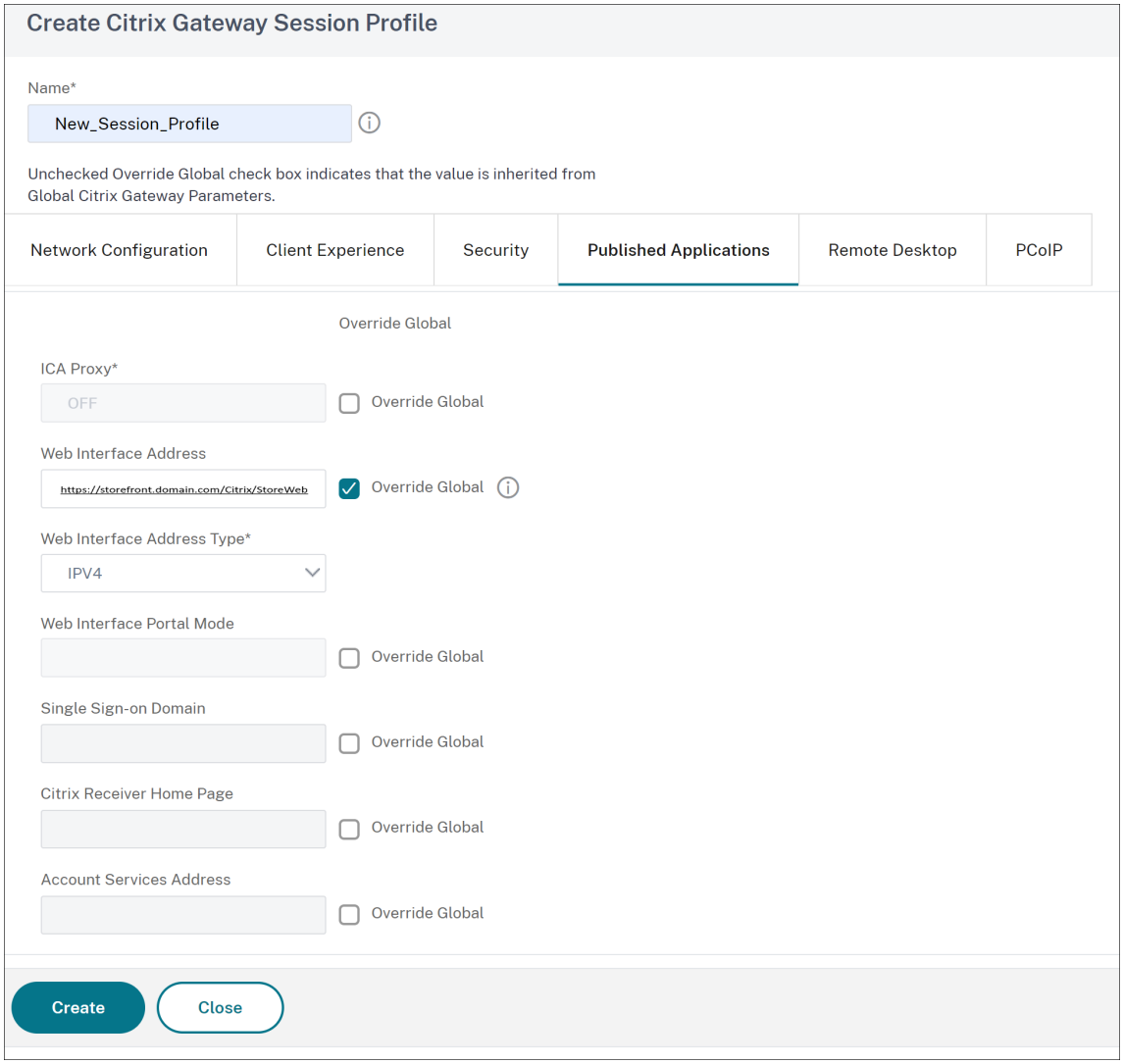
 




7. En la ficha **Aplicación publicada**, active la siguiente configuración:

   - **Proxy ICA**: establecido en ON.
   - **Dirección de la interfaz web**: FQDN del servidor StoreFront seguido de la ruta a la tienda para Internet
   - **Dominio de inicio de sesión único**: Nombre NetBIOS del dominio



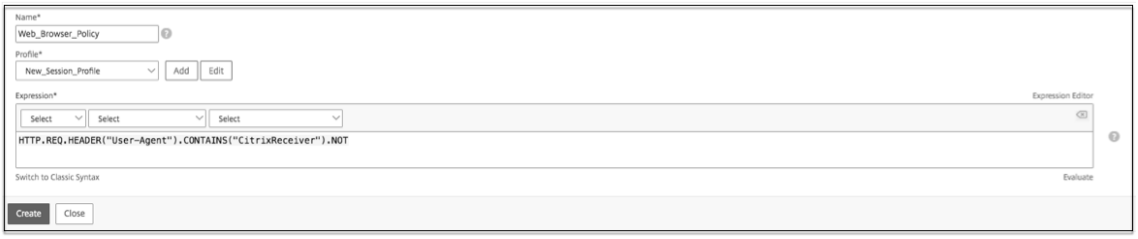

8. Haga clic en **Crear**.
9. Si utiliza una expresión de directiva clásica, en el campo **Expresión**, agregue la siguiente información y haga clic en **Crear**.

```
1 REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```


10. Si utiliza una expresión de directiva avanzada, en el campo **Expresión**, agregue la siguiente información y haga clic en **Crear**.

```
1 HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```



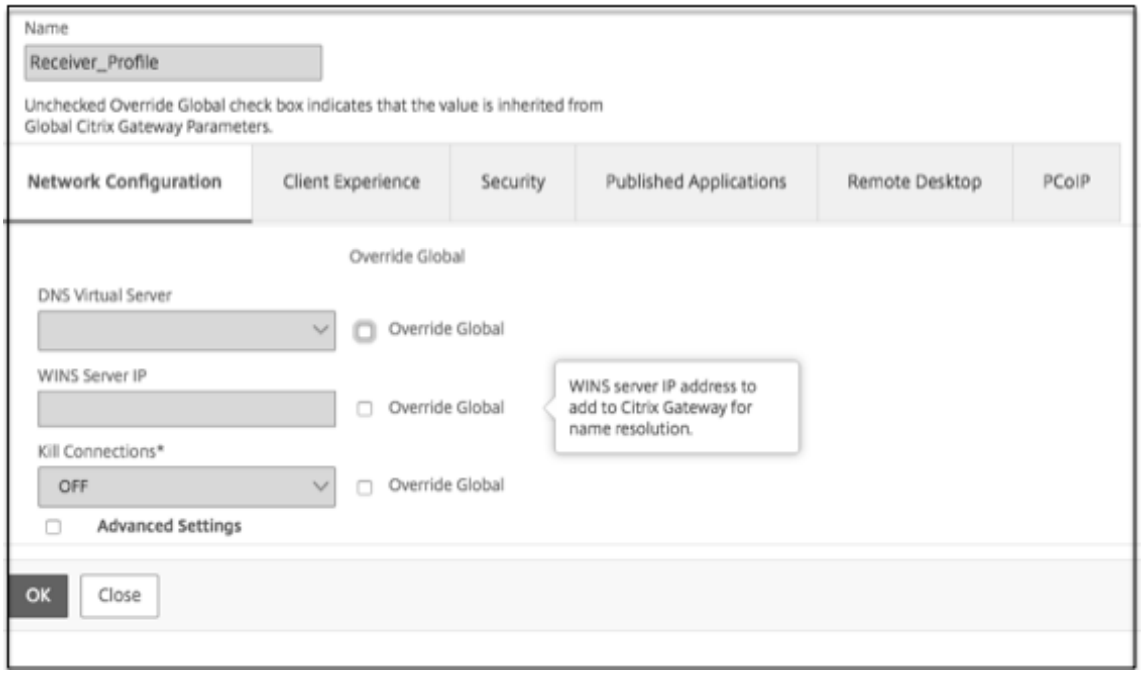

Esta directiva es necesaria para que NetScaler ADC distinga entre conexiones basadas en explorador web y conexiones basadas en aplicaciones Citrix Workspace. Esta directiva se aplica a las conexiones basadas en exploradores web.

**Crear una directiva de sesión para la aplicación Citrix Workspace para Windows o Mac y para dispositivos móviles en NetScaler Gateway**

1. Vaya a **NetScaler Gateway > Directivas > Sesión**.
2. En el campo **Directivas de sesión**, haga clic en **Agregar**.
3. En el campo **Nombre**, escriba el nombre de la directiva de sesión. Por ejemplo, Receiver_Policy.


4. Escriba el nombre del nuevo perfil de sesión en la ventana **Configurar perfil de sesión de NetScaler Gateway**.

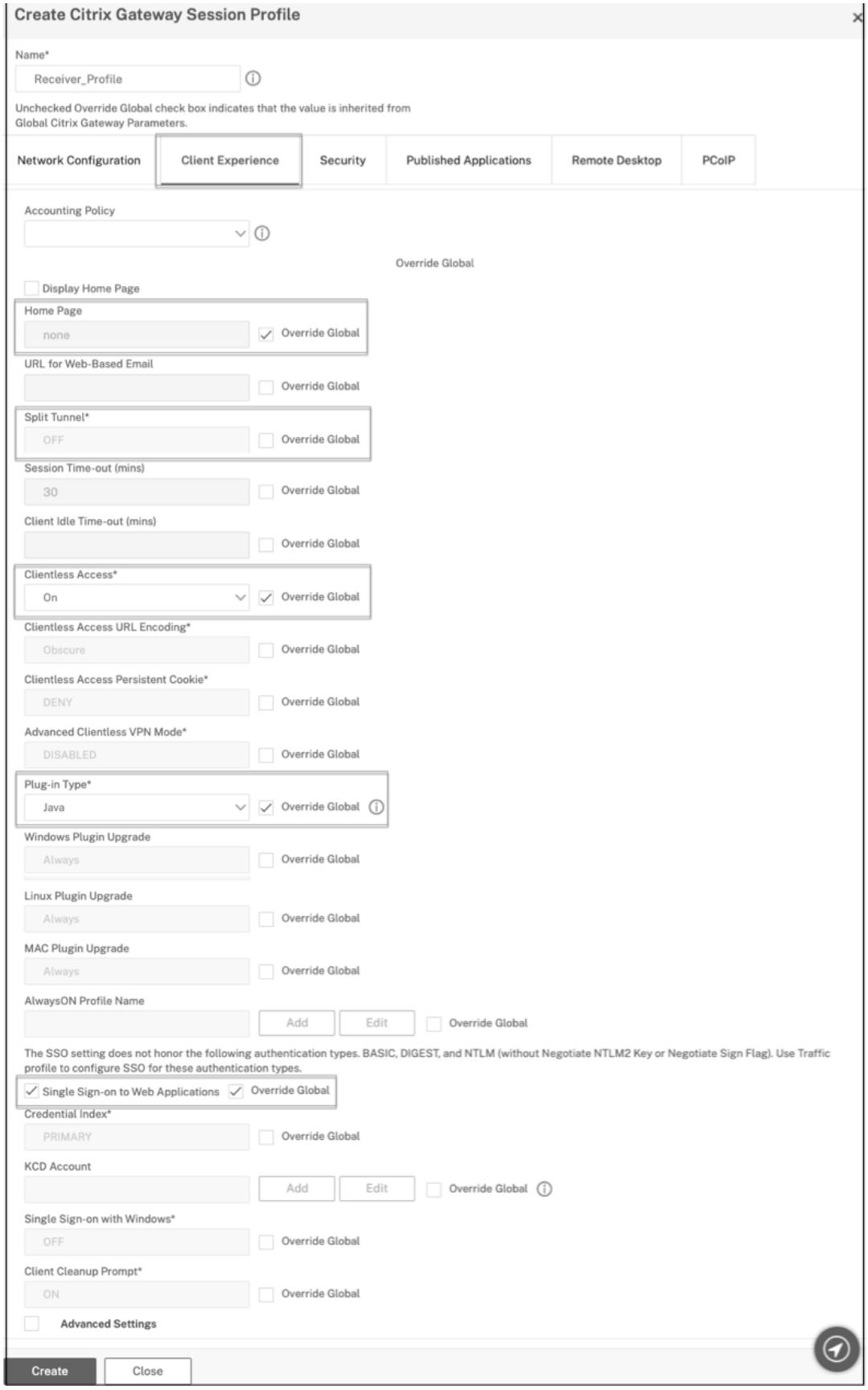
 




5. En la ficha **Experiencia del cliente**, active la siguiente configuración:

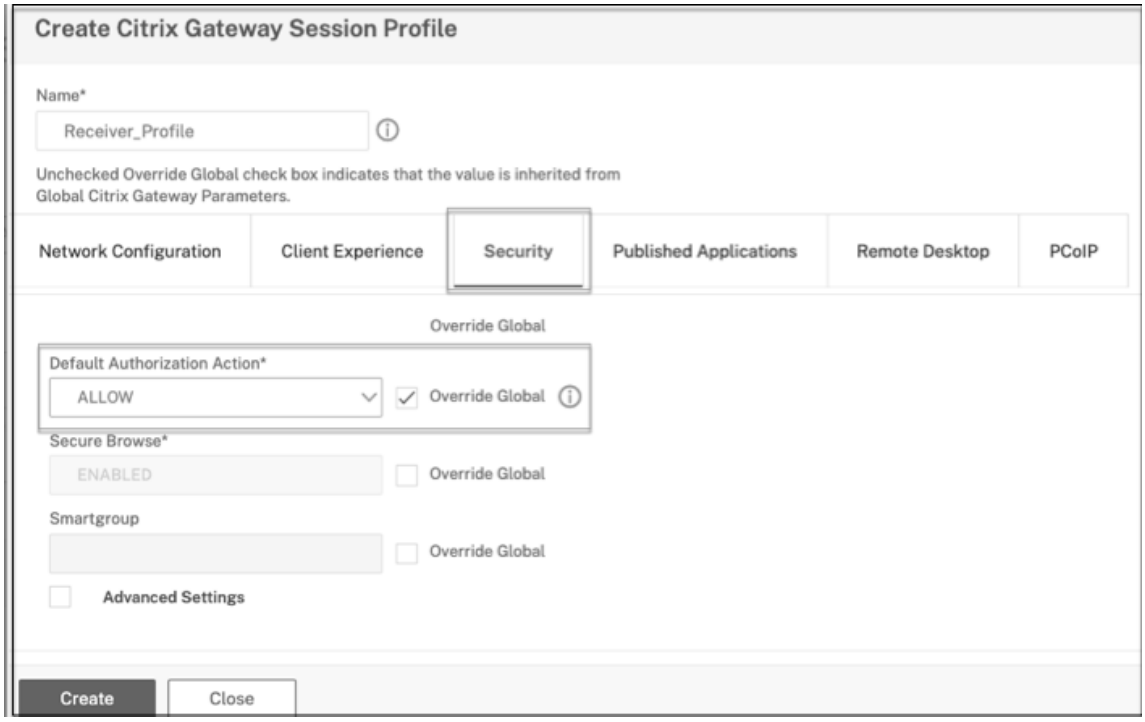
   - **Página**de inicio: Establecer en **Ninguno**
   - **Túnel dividido**: **desactivado**
   - **Acceso **sin cliente : activado **
   - Inicio de**sesión único en aplicación web**: seleccione la casilla de verificación
   - **Tipo de complemento**: Configurado en **Java**



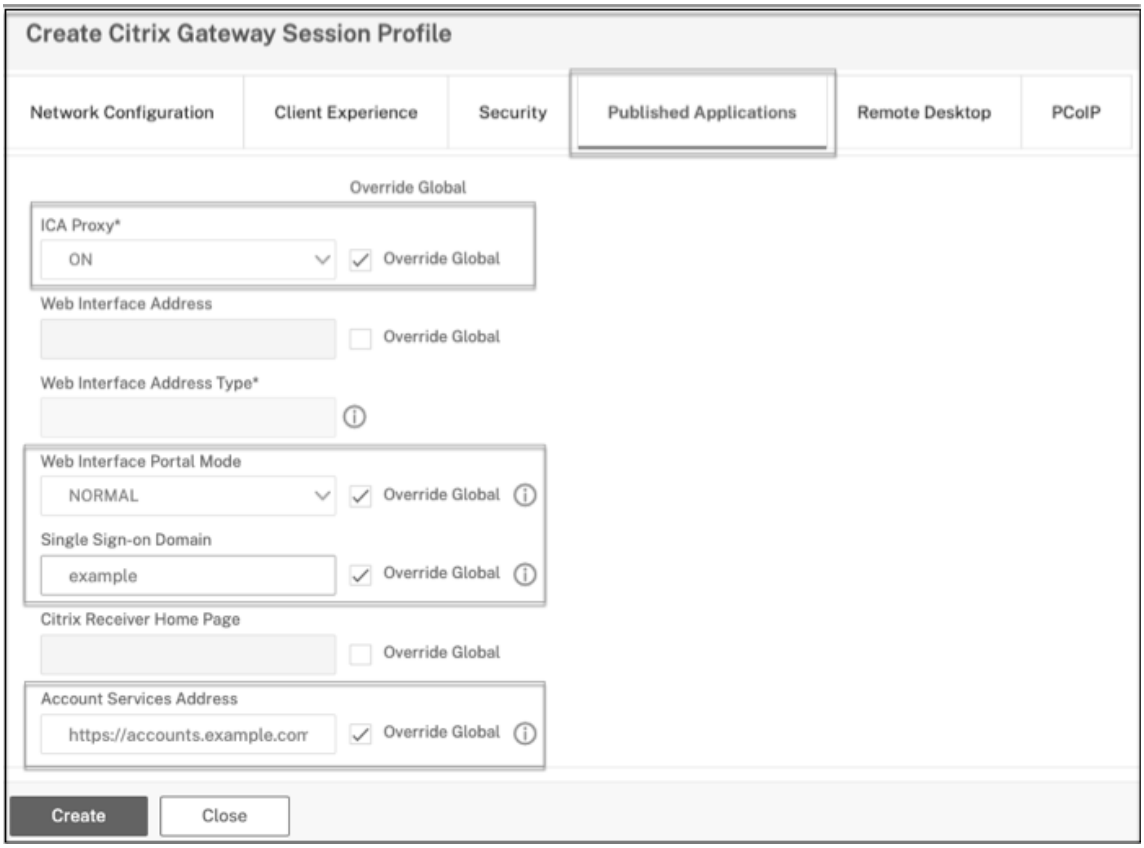
6. En la ficha **Seguridad**, establezca **Acciones de autorización predeterminadas** en **PERMITIR**.




7. En la ficha **Aplicación publicada**, active la siguiente configuración:

   - **Proxy ICA**: establecido en ON.
   - **Dirección de interfaz web:** FQDN del servidor de StoreFront seguido de la ruta de acceso al almacén para web
   - **Dominio de inicio de sesión único:** nombre NetBIOS del dominio
   - **Dirección de servicios de cuenta:**introduzca la dirección de servicios de cuenta. La última barra invertida es importante. Por ejemplo, `https://accounts.example.com/Citrix/Roaming/Accounts`




8. Haga clic en **Crear**.
9. Si utiliza una expresión de directiva clásica, en el campo **Expresión**, agregue la siguiente información y haga clic en **Crear**.

```
1 REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
```


10. Si utiliza una expresión de directiva avanzada, en el campo **Expresión**, agregue la siguiente información y haga clic en **Crear**.

```
1 HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
```


Esta directiva es necesaria para que NetScaler ADC diferencie entre las conexiones basadas en explorador web y las basadas en la aplicación Citrix Workspace. Esta directiva se aplica a las conexiones basadas en aplicaciones Citrix Workspace.

#### Configurar la autenticación en el dispositivo NetScaler ADC

Para obtener información sobre cómo configurar la autenticación LDAP en un dispositivo NetScaler ADC, consulte Configuración de la autenticación LDAP.

#### Crear servidor virtual NetScaler Gateway y enlazar las directivas de sesión

1. Vaya a **NetScaler Gateway > Servidor virtual** y haga clic en **Agregar** para agregar un nuevo servidor virtual.
2. Una vez creado el servidor virtual, vincule la directiva de sesión específica al servidor virtual en función de los requisitos de su empresa.

### Configurar la autenticación para StoreFront

1. Habilite la autenticación PassThrough desde NetScaler Gateway en StoreFront. Para obtener más información, consulte Configurar el servicio de autenticación.

   StoreFront debe confiar en el emisor del certificado vinculado del servidor virtual de NetScaler Gateway (certificados raíz o intermedio) para el servicio de devolución de llamada de autenticación.

2. Agregue NetScaler Gateway a StoreFront. Para obtener más información, consulte Agregar una conexión de NetScaler Gateway.

   La URL de la puerta de enlace debe coincidir exactamente con lo que los usuarios escriben en la barra de direcciones del explorador web.

3. Habilite el acceso remoto en el almacén de StoreFront. Para obtener más información, consulte Administrar el acceso remoto a almacenes a través de NetScaler Gateway.

## Configuración de directivas de dispositivos de punto final

January 26, 2024

El análisis de terminales es un proceso que escanea el dispositivo de un usuario y detecta información, como la presencia y el nivel de versión de un sistema operativo y del software antivirus, firewall o navegador web. Puede utilizar el análisis de puntos finales para verificar que el dispositivo de usuario cumple sus requisitos antes de permitir que se conecte a la red o que permanezca conectado después de que los usuarios inicien sesión. Puede supervisar los archivos, los procesos y las entradas del registro en el dispositivo de usuario durante la sesión de usuario para asegurarse de que el dispositivo sigue cumpliendo los requisitos.

## Cómo funcionan las directivas de dispositivos de punto final

January 26, 2024

Puede configurar NetScaler Gateway para comprobar si un dispositivo de usuario cumple determinados requisitos de seguridad antes de que un usuario inicie sesión. Esto se denomina directiva de autenticación previa. Puede configurar NetScaler Gateway para que compruebe si un dispositivo de usuario tiene antivirus, firewall, antispam, procesos, archivos, entradas de registro, seguridad de Internet o sistemas operativos que especifique en la directiva. Si el dispositivo de usuario no supera el análisis de autenticación previa, los usuarios no pueden iniciar sesión.

Si necesita configurar requisitos de seguridad adicionales que no se usen en una directiva de autenticación previa, configure una directiva de sesión y la vincule a un usuario o grupo. Este tipo de directiva se denomina directiva posterior a la autenticación, que se ejecuta durante la sesión del usuario para garantizar que los elementos necesarios, como un software antivirus o un proceso, sigan siendo verdaderos.

Al configurar una directiva de autenticación previa o posterior a la autenticación, NetScaler Gateway descarga el complemento Endpoint Analysis y, a continuación, ejecuta el análisis. Cada vez que un usuario inicia sesión, el complemento Endpoint Analysis se ejecuta automáticamente.

Utilice los tres tipos de directivas siguientes para configurar las directivas de dispositivos de punto final:

- Directiva de autenticación previa que utiliza un parámetro sí o no. El análisis determina si el dispositivo del usuario cumple los requisitos especificados. Si se produce un error en el análisis, el usuario no puede introducir las credenciales en la página de inicio de sesión.
- Directiva de sesión condicional y que se puede utilizar para SmartAccess.
- Expresión de seguridad del cliente dentro de una directiva de sesión. Si el dispositivo de usuario no cumple los requisitos de la expresión de seguridad del cliente, puede configurar a los usuarios para que se coloquen en un grupo de cuarentena. Si el dispositivo del usuario supera el escaneo, los usuarios se pueden colocar en un grupo diferente que podría requerir comprobaciones adicionales.

Puede incorporar la información detectada en las políticas, lo que le permite conceder diferentes niveles de acceso según el dispositivo del usuario. Por ejemplo, puede proporcionar acceso completo con permiso de descarga a los usuarios que se conectan de forma remota desde dispositivos de usuario que tienen requisitos actuales de software antivirus y firewall. Para los usuarios que se conectan desde equipos que no son de confianza, puede proporcionar un nivel de acceso más restringido que permite a los usuarios modificar documentos en servidores remotos sin descargarlos.

El análisis de puntos finales lleva a cabo los siguientes pasos básicos:

- Examina un conjunto inicial de información sobre el dispositivo del usuario para determinar qué análisis se deben aplicar.
- Ejecuta todos los escaneos aplicables. Cuando los usuarios intentan conectarse, el complemento Endpoint Analysis comprueba los requisitos especificados en la directiva de sesión o autenticación previa en el dispositivo del usuario. Si el dispositivo del usuario supera el análisis, los usuarios pueden iniciar sesión. Si el dispositivo del usuario no supera el análisis, los usuarios no pueden iniciar sesión.
  Nota: Los escaneos de Endpoint Analysis se completan antes de que la sesión de usuario utilice una licencia.
- Compara los valores de propiedad detectados en el dispositivo del usuario con los valores de propiedad deseados enumerados en los análisis configurados.
- Genera una salida que verifica si se encuentran o no los valores de propiedad deseados.

> **Atención:**Las instrucciones para crear políticas de análisis de puntos finales son directrices generales. Puede tener muchas opciones de configuración dentro de una directiva de sesión. Las instrucciones específicas para configurar las políticas de sesión pueden contener instrucciones para configurar una configuración específica; sin embargo, esa configuración puede ser una de las muchas opciones que se incluyen en un perfil y una política de sesión.

# Evaluar las opciones de inicio de sesión de usuario

January 26, 2024

Cuando los usuarios inician sesión, pueden optar por omitir el análisis del punto final. Si los usuarios omiten el análisis, Citrix Gateway procesa esta acción como un análisis de punto final fallido. Cuando los usuarios no superan el análisis, solo pueden tener acceso a la Interfaz Web o a través del acceso sin cliente.

Por ejemplo, quiere proporcionar acceso a los usuarios mediante el plug-in de NetScaler Gateway. Para iniciar sesión en NetScaler Gateway con el complemento, los usuarios deben estar ejecutando una aplicación antivirus, como Norton Antivirus. Si el dispositivo de usuario no ejecuta la aplicación, los usuarios solo pueden iniciar sesión con Receiver y utilizar aplicaciones publicadas. También puede configurar el acceso sin cliente, que restringe el acceso a aplicaciones específicas, como Outlook Web Access.

Para configurar NetScaler Gateway para lograr este caso de inicio de sesión, asigne una directiva de sesión restrictiva como directiva predeterminada. A continuación, configure los ajustes para actualizar a los usuarios a una política de sesión privilegiada cuando el dispositivo de usuario pase el análisis de puntos finales. En ese momento, los usuarios tienen acceso a la capa de red y pueden iniciar sesión con el plug-in de NetScaler Gateway.

Para configurar NetScaler Gateway para que aplique primero la directiva de sesión restrictiva, lleve a cabo los siguientes pasos:

- Configure los ajustes globales con el proxy ICA habilitado y todos los demás ajustes necesarios si la aplicación especificada no se está ejecutando en el dispositivo del usuario.
- Cree una directiva y un perfil de sesión que habilite el plug-in de NetScaler Gateway.
- Cree una expresión dentro de la parte de regla de la directiva de sesión para especificar la aplicación, por ejemplo:

  (existe client.application.process (symantec.exe))

Cuando los usuarios inician sesión, la directiva de sesión se aplica primero. Si el análisis de terminales falla o el usuario omite el análisis, Citrix Gateway ignora la configuración de la directiva de sesión (la expresión de la directiva de sesión se considera falsa). Como resultado, los usuarios tienen acceso restringido mediante la Interfaz Web o el acceso sin cliente. Si se aprueba el análisis de endpoints, NetScaler Gateway aplica la directiva de sesión y los usuarios tienen acceso completo con el plug-in de NetScaler Gateway.

## Definir la prioridad de las directivas de autenticación previa

March 27, 2024

Puede tener varias directivas de preautenticación vinculadas a distintos niveles. Por ejemplo, tiene una directiva que comprueba si hay una aplicación antivirus específica vinculada a NetScaler ADC AAA Global y una directiva de firewall vinculada al servidor virtual. Cuando los usuarios inician sesión, se aplica primero la directiva vinculada al servidor virtual. La directiva vinculada a NetScaler ADC AAA Global se aplica en segundo lugar.

Puede cambiar el orden en que se realizan los análisis de preautenticación. Para que NetScaler Gateway aplique primero la directiva global, cambie el número de prioridad de la directiva vinculada al servidor virtual, asignándole un número de prioridad superior al de la directiva vinculada globalmente. Por ejemplo, establezca el número de prioridad de la directiva global en uno y la directiva del servidor virtual en dos. Cuando los usuarios inician sesión, NetScaler Gateway ejecuta primero el análisis de directivas globales y, en segundo lugar, el análisis de directivas del servidor virtual.

### Para cambiar la prioridad de una política de autenticación previa

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en Abrir .
3. En la ficha Directivas, haga clic en Preautenticación.
4. En Prioridad, escriba el número de prioridad de la política y, a continuación, haga clic en Aceptar.

## Configurar directivas y perfiles de autenticación previa

March 27, 2024

> **Advertencia:**
>
> La directiva de autenticación, autorización y auditoría previa a la autenticación está obsoleta a partir de NetScaler 12.0 build 56.20 y , como alternativa, Citrix recomienda utilizar la autenticación nFactor. Para obtener más información, consulte el tema Autenticación multifactor (nFactor)] (/en-us/netscaler/12/aaa-tm/multi-factor-nfactor-authentication.html).

Puede configurar NetScaler Gateway para que compruebe la seguridad del lado del cliente antes de autenticar a los usuarios. Este método garantiza que el dispositivo del usuario que establece una

sesión con NetScaler Gateway cumpla sus requisitos de seguridad. Las comprobaciones de seguridad del lado del cliente se configuran mediante directivas de autenticación previa específicas de un servidor virtual o de forma global, como se describe en los dos procedimientos siguientes.

Las directivas de preautenticación consisten en un perfil y una expresión. El perfil se configura para que utilice una acción para permitir o denegar la ejecución de un proceso en el dispositivo del usuario. Por ejemplo, el archivo de texto, clienttext.txt, se está ejecutando en el dispositivo del usuario. Cuando el usuario inicia sesión en NetScaler Gateway, puede permitir o denegar el acceso si el archivo de texto se está ejecutando. Si no quiere permitir que los usuarios inicien sesión si el proceso se está ejecutando, configure el perfil para que el proceso se detenga antes de que los usuarios inicien sesión.

Puede configurar los siguientes ajustes para las directivas de preautenticación:

- Expresión. Incluye la siguiente configuración para ayudarle a crear expresiones:
  - Expresión. Muestra todas las expresiones creadas.
  - Haga coincidir cualquier expresión. Configura la directiva para que coincida con cualquiera de las expresiones presentes en la lista de expresiones seleccionadas.
  - Coincidir con todas las expresiones. Configura la directiva para que coincida con todas las expresiones presentes en la lista de expresiones seleccionadas.
  - Expresiones tabulares. Crea una expresión compuesta con las expresiones existentes mediante el `OR (||)or AND (&&)operators`.
  - Formato libre avanzado. Crea expresiones compuestas personalizadas mediante los nombres de las `OR (||)and AND (&&)operators`expresiones y . Elija solo las expresiones que necesite y omita otras expresiones de la lista de expresiones seleccionadas.
  - Add: Crea una expresión.
  - Modificar. Modifica una expresión existente.
  - Remove: Elimina la expresión seleccionada de la lista de expresiones compuestas.
  - Expresiones con nombre. Seleccione una expresión con nombre configurada. Puede seleccionar expresiones con nombre en la lista desplegable de expresiones que ya están presentes en Citrix Gateway.
  - Agregar expresión. Agrega la expresión con nombre seleccionada a la directiva.
  - Reemplazar expresión. Reemplaza la expresión con nombre seleccionada en la directiva.
  - Vista previa de expresión. Muestra la cadena de seguridad de cliente detallada que se configura en NetScaler Gateway al seleccionar una expresión con nombre.

### Para configurar un perfil de autenticación previa de forma global mediante la utilidad de configuración

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.

2. En el panel de detalles, en Configuración, haga clic en Cambiar la configuración de preautenticación.
3. En el cuadro de diálogo Configuración de preautenticación global, configure la configuración:
   a) En Acción , selecciona Permitir o Denegar .
      Deniega o permite que los usuarios inicien sesión después de que se haya realizado el análisis del punto final.
   b) En Procesos que se van a cancelar, introduzca el proceso.
      Esto especifica los procesos que debe detener el complemento Endpoint Analysis.
   c) En Archivos que se van a eliminar, introduzca el nombre del archivo.
      Esto especifica los archivos que debe eliminar el complemento Endpoint Analysis.
4. En Expression, puede dejar la expresión ns_true o crear una expresión para una aplicación específica, como antivirus o software de seguridad y, a continuación, hacer clic en Aceptar.

### Para configurar un perfil de autenticación previa mediante la utilidad de configuración

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas > Autenticación/autorización y, a continuación, haga clic en Pre-Authentication EPA.
2. En el panel de detalles, en la pestaña Perfiles , haga clic en Agregar .
3. En Nombre, escriba el nombre de la aplicación que se va a comprobar.
4. En Acción, selecciona PERMITIR o DENEGAR.
5. En Procesos que se van a cancelar, escriba el nombre del proceso que se va a detener.
6. En Archivos que se van a eliminar, escriba el nombre del archivo que se va a eliminar, por ejemplo, c:\clientext.txt, haga clic en Crear y, a continuación, en Cerrar.

   > Nota:
   >
   > Si se va a eliminar un archivo o se detiene un proceso, los usuarios reciben un mensaje en el que se les pide confirmación. Los pasos 5 y 6 son parámetros opcionales.

Si utiliza la utilidad de configuración para configurar un perfil de autenticación previa, cree la directiva de autenticación previa haciendo clic en Agregar en la ficha Directivas. En el cuadro de diálogo Crear política de autenticación previa, seleccione el perfil en la lista desplegable Solicitar perfil.

## Configurar expresiones de Endpoint Analysis

March 27, 2024

Las directivas de sesión de seguridad de cliente y autenticación previa incluyen un perfil y una expresión. La directiva puede tener un perfil y varias expresiones. Para explorar un dispositivo de usuario en busca de una aplicación, archivo, proceso o entrada de registro, debe crear una expresión o expresiones compuestas dentro de la directiva.

### Tipos de expresiones

La expresión consiste en un tipo de expresión y los parámetros de la expresión. Los tipos de expresión incluyen:

- General
- Seguridad del cliente
- Basado en red

### Agregar expresiones preconfiguradas a una política de autenticación previa

NetScaler Gateway incluye expresiones preconfiguradas, denominadas expresiones con nombre. Al configurar una directiva, puede utilizar una expresión con nombre para la directiva. Por ejemplo, desea que la política de autenticación previa compruebe si Symantec AntiVirus 10 tiene definiciones de virus actualizadas. Cree una directiva de preautenticación y agregue la expresión tal y como se describe en el procedimiento siguiente.

Al crear una directiva de sesión o preautenticación, puede crear la expresión al crear la directiva. A continuación, puede aplicar la directiva, con la expresión, a servidores virtuales o de forma global.

En el procedimiento siguiente se describe cómo agregar una expresión antivirus preconfigurada a una directiva mediante la utilidad de configuración.

### Para agregar una expresión con nombre a una política de autenticación previa

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas > Autenticación/autorización y, a continuación, haga clic en Pre-Authentication EPA.
2. En el panel de detalles, seleccione una directiva y, a continuación, haga clic en Abrir.
3. Junto a Expresiones con nombre, seleccione Antivirus, seleccione el producto antivirus de la lista, haga clic en Agregar expresión, en Crear y, a continuación, en Cerrar.

# Configurar expresiones personalizadas

March 27, 2024

Una expresión personalizada es aquella que se crea dentro de la directiva. Al crear una expresión, configura los parámetros de la expresión.

También puede crear expresiones de seguridad de cliente personalizadas para hacer referencia a cadenas de seguridad de cliente de uso común. Esto facilita el proceso de configuración de directivas de preautenticación y también el mantenimiento de las expresiones configuradas.

Por ejemplo, desea crear una expresión de seguridad de cliente personalizada para Symantec AntiVirus 10 y asegurarse de que las definiciones de virus no tengan más de tres días de antigüedad. Cree una nueva política y, a continuación, configure la expresión para especificar las definiciones de virus.

En el procedimiento siguiente se muestra cómo crear una directiva de seguridad de cliente en una directiva de autenticación previa. Puede seguir los mismos pasos en una directiva de sesión.

### Para crear una política de autenticación previa y una expresión de seguridad de cliente personalizada

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas > Autenticación/autorización y, a continuación, haga clic en Pre-Authentication EPA.
2. En el panel de detalles, haga clic en Agregar. Se abre el cuadro de diálogo Crear directiva de autenticación previa.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En el cuadro de diálogo Crear perfil de autenticación, en Nombre, escriba un nombre para el perfil y, en Acción, seleccione Permitir y, a continuación, haga clic en Crear.
6. En el cuadro de diálogo Crear directiva de preautenticación, junto a Ajustarcualquier expresión, haga clic en Agregar.
7. En Tipo de expresión, seleccione Seguridad del cliente.
8. Configure las siguientes opciones:

    a) En Componente, seleccione Antivirus.
    b) En Nombre, escriba un nombre para la aplicación.
    c) En Qualifier, selecciona Versión .
    d) En Operador, seleccione ==.
    e) En Valor, escriba el valor.

f) En Freshness, escriba 3 y, a continuación, haga clic en Aceptar.

9. En el cuadro de diálogo Crear política de autenticación previa, haga clic en Crear y, a continuación, en Cerrar.

Al configurar una expresión personalizada, se agrega al cuadro Expresión del cuadro de diálogo de directiva.

## Configurar expresiones compuestas

January 26, 2024

Una directiva de preautenticación puede tener un perfil y varias expresiones. Si configura expresiones compuestas, utiliza operadores para especificar las condiciones de la expresión. Por ejemplo, puede configurar expresiones compuestas para exigir que el dispositivo del usuario ejecute una de las siguientes aplicaciones antivirus:

- Symantec Antivirus 10
- McAfee Antivirus 11
- Sophos Antivirus 4

La expresión se configura con el operador OR para comprobar las tres aplicaciones anteriores. Si NetScaler Gateway detecta la versión correcta de alguna de las aplicaciones del dispositivo del usuario, los usuarios pueden iniciar sesión. La expresión del cuadro de diálogo de directivas aparece de la siguiente manera:

| | |
|---|---|
| AV_5_Symantec 10 | AV_5_McAfeeVirusScan_11 |

Para obtener más información sobre las expresiones compuestas, consulte Configuración de expresiones compuestas.

## Políticas vinculantes de autenticación previa

March 27, 2024

Después de crear la directiva de sesión de preautenticación o seguridad del cliente, vincule la directiva al nivel al que se aplica. Puede enlazar las directivas de preautenticación a servidores virtuales o de forma global.

### Para crear y vincular una directiva de autenticación previa de forma global

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, haga clic en Cambiar la configuración de preautenticación.
3. En el cuadro de diálogo Configuración global de preautenticación, en Acción, seleccione Permitir o Denegar.
4. En Nombre, escriba un nombre para la directiva.
5. En el cuadro de diálogo Configuración global previa a la autenticación, junto a Expresiones con nombre, seleccione General, seleccione Valor verdadero, haga clic en Agregar expresión, en Crear y, a continuación, en Cerrar.

### Para vincular una directiva de autenticación previa a un servidor virtual

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en Abrir .
3. En el cuadro de diálogo Configurar el servidor virtual Citrix Gateway, haga clic en la pestaña Directivas y, a continuación, en Autenticación previa.
4. En Detalles, haga clic en Insertar política y, a continuación, en Nombre de la política, seleccione la política de autenticación previa.
5. Haga clic en Aceptar.

## Desvincular y eliminar políticas de autenticación previa

March 27, 2024

Si es necesario, puede quitar una directiva de preautenticación de NetScaler Gateway. Antes de quitar una directiva de preautenticación, desvincúlelo del servidor virtual o de forma global.

### Para desvincular una política global de autenticación previa

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas > Autenticación/autorización y, a continuación, haga clic en Pre-Authentication EPA.
2. En el panel de detalles, seleccione una directiva y, a continuación, en Acción, haga clic en Enlaces globales.

3. En el cuadro de diálogo Vincular o desvincular políticas de autenticación previa a políticas globales, seleccione una política, haga clic en Desvincular política y, a continuación, haga clic en Aceptar.

### Para desvincular una directiva de autenticación previa de un servidor virtual

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. En el cuadro de diálogo Configurar el servidor virtual Citrix Gateway, haga clic en la pestaña Directivas y, a continuación, en Autenticación previa.
3. Seleccione la directiva y, a continuación, haga clic en Desvincular directiva.

Cuando la directiva de preautenticación es independiente, puede quitarla de NetScaler Gateway.

### Para eliminar una política de autenticación previa

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas > Autenticación/autorización y, a continuación, haga clic en Pre-Authentication EPA.
2. en el panel de detalles, seleccione una directiva y, a continuación, haga clic en Quitar.

## Configurar directivas posteriores a la autenticación

January 26, 2024

Una directiva posterior a la autenticación es un conjunto de reglas genéricas que el dispositivo del usuario debe cumplir para mantener activa la sesión. Si se produce un error en la directiva, finaliza la conexión con NetScaler Gateway. Al configurar la directiva posterior a la autenticación, puede configurar cualquier configuración para las conexiones de usuario que se puedan hacer condicionales.

> **Nota:** Esta funcionalidad solo funciona con el plug-in de NetScaler Gateway. Si los usuarios inician sesión con Citrix Receiver, el análisis de análisis de endpoint se ejecuta solo al iniciar sesión.

Las directivas de sesión se utilizan para configurar directivas posteriores a la autenticación. En primer lugar, crea los usuarios a los que se aplica la directiva. A continuación, agregará los usuarios a un grupo. A continuación, enlazará las aplicaciones de sesión, directivas de tráfico e intranet al grupo.

También puede especificar que los grupos sean grupos de autorización. Este tipo de grupo le permite asignar usuarios a grupos en función de una expresión de seguridad del cliente incluida en la política de sesión.

También puede configurar una directiva posterior a la autenticación para poner a los usuarios en un grupo de cuarentena si el dispositivo de usuario no cumple los requisitos de la directiva. Una directiva sencilla incluye una expresión de seguridad del cliente y un mensaje de seguridad del cliente. Cuando los usuarios están en el grupo de cuarentena, los usuarios pueden iniciar sesión en NetScaler Gateway; sin embargo, tienen acceso limitado a los recursos de red.

No se puede crear un grupo de autorización ni un grupo de cuarentena mediante el mismo perfil y directiva de sesión. Los pasos para crear la directiva posterior a la autenticación son los mismos. Al crear la directiva de sesión, selecciona un grupo de autorización o un grupo de cuarentena. Puede crear dos directivas de sesión y vincular cada directiva al grupo.

Las directivas posteriores a la autenticación también se utilizan con SmartAccess. Para obtener más información sobre SmartAccess, consulte Configuración de SmartAccess en NetScaler Gateway.

## Configurar una directiva posterior a la autenticación

March 27, 2024

Se utiliza una directiva de sesión para configurar una directiva posterior a la autenticación. Una directiva sencilla incluye una expresión de seguridad del cliente y un mensaje de seguridad del cliente.

### Para configurar una política posterior a la autenticación

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En Nombre , escriba un nombre para el perfil.
6. En la pestaña Seguridad , haz clic en Configuración avanzada .
7. En Seguridad del cliente, haga clic en Supedición global y, a continuación, haga clic en Nuevo
8. Configure la expresión de seguridad del cliente y, a continuación, haga clic en Crear.
9. En Seguridad del cliente, en Grupo de cuarentena, seleccione un grupo.
10. En Mensaje de error, escriba el mensaje que quiere que reciban los usuarios si se produce un error en el análisis posterior a la autenticación.
11. En Grupos de autorización, haga clic en Anular global, seleccione un grupo, haga clic en Agregar, en Aceptar y, a continuación, en Crear.
12. En el cuadro de diálogo Crear política de sesión , junto a Expresiones con nombre , seleccione General, seleccione Valor verdadero , haga clic en Agregar expresión , en Crear y, a continuación, en Cerrar .

## Configurar la frecuencia de los análisis posteriores a la autenticación

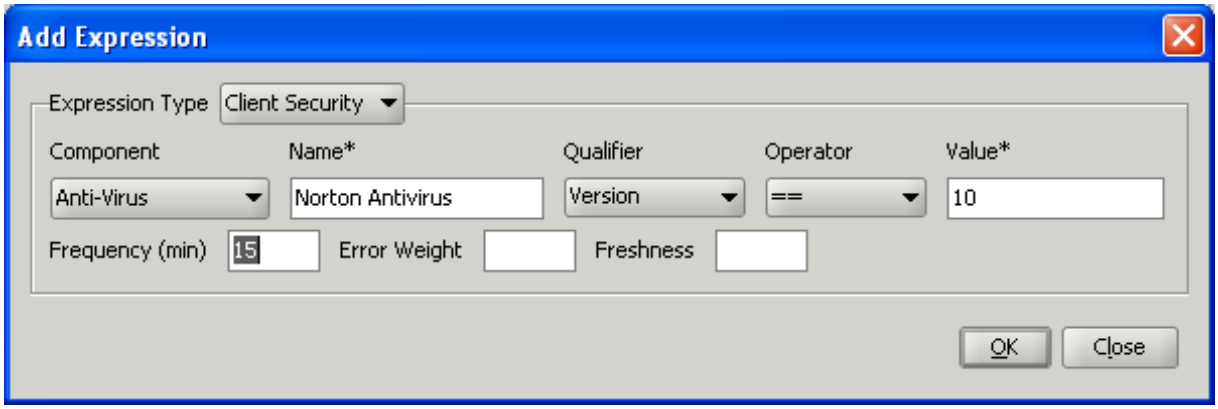
January 26, 2024

Puede configurar NetScaler Gateway para que ejecute la directiva posterior a la autenticación a intervalos especificados. Por ejemplo, ha configurado una directiva de seguridad del cliente y quiere que se ejecute en el dispositivo del usuario cada 10 minutos. Puede configurar esta frecuencia mediante la creación de una expresión personalizada dentro de la directiva.

> **Nota:** La funcionalidad de comprobación de frecuencia para las directivas posteriores a la autenticación solo funciona con el plug-in de NetScaler Gateway. Si los usuarios inician sesión con Citrix Receiver, el análisis de análisis de endpoint se ejecuta solo al iniciar sesión.

Puede establecer la frecuencia (en minutos) al configurar la directiva de seguridad del cliente siguiendo el procedimiento Configuración de una directiva posterior a la autenticación. En la siguiente ilustración se muestra dónde se puede introducir un valor de frecuencia en el cuadro de diálogo Agregar expresión.

Figura 1. Cuadro de diálogo para configurar la frecuencia de los análisis posteriores a la autenticación




## Configurar grupos de cuarentena y autorización

January 26, 2024

Cuando los usuarios inician sesión en NetScaler Gateway, los asigna a un grupo que configura en NetScaler Gateway o en un servidor de autenticación de la red segura. Si un usuario falla un análisis posterior a la autenticación, puede asignarlo a un grupo restringido, denominado grupo de cuarentena, que restringe el acceso a los recursos de red.

También puede utilizar grupos de autorización para restringir el acceso de los usuarios a los recursos de red. Por ejemplo, es posible que tenga un grupo de personal contratado que solo tenga acceso al servidor de correo electrónico y a un recurso compartido de archivos. Cuando los dispositivos de usuario superan los requisitos de seguridad definidos en NetScaler Gateway, los usuarios pueden convertirse en miembros de grupos de forma dinámica.

Utilice la configuración global o las directivas de sesión para configurar grupos de cuarentena y autorización vinculados a un usuario, grupo o servidor virtual. Puede asignar usuarios a grupos en función de una expresión de seguridad del cliente dentro de la política de sesión. Cuando el usuario es miembro de un grupo, NetScaler Gateway aplica la directiva de sesión basada en la pertenencia al grupo.

## Configurar grupos de cuarentena

March 27, 2024

Al configurar un grupo de cuarentena, se configura la expresión de seguridad del cliente mediante el cuadro de diálogo Configuración de seguridad - Configuración avanzada de un perfil de sesión.

### Para configurar la expresión de seguridad del cliente para un grupo de cuarentena

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En Nombre , escriba un nombre para el perfil.
6. En la pestaña Seguridad , haz clic en Configuración avanzada .
7. En Seguridad del cliente, haga clic en Supedición global y, a continuación, haga clic en Nuevo
8. En el cuadro de diálogo Expresión de cliente, configure la expresión de seguridad del cliente y, a continuación, haga clic en Crear.
9. En Grupo de cuarentena, seleccione el grupo.
10. En Mensaje de error, escriba un mensaje que describa el problema para los usuarios y, a continuación, haga clic en Crear.
11. En el cuadro de diálogo Crear política de sesión , junto a Expresiones con nombre , seleccione General, seleccione Valor verdadero , haga clic en Agregar expresión , en Crear y, a continuación, en Cerrar .

Después de crear la directiva de sesión, enlaza a un usuario, grupo o servidor virtual.

> **Nota**
>
> Si se produce un error en el análisis de endpoint y el usuario se coloca en el grupo de cuarentena, las directivas enlazadas al grupo de cuarentena solo serán efectivas si no hay directivas vinculadas directamente al usuario que tengan un número de prioridad igual o inferior que las directivas vinculadas al grupo de cuarentena.

### Para configurar un grupo de cuarentena global

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la pestaña Seguridad , haz clic en Configuración avanzada .
4. En Seguridad del cliente, configure la expresión de seguridad del cliente.
5. En Grupo de cuarentena, seleccione el grupo.
6. En Mensaje de error, escriba un mensaje que describa el problema para los usuarios y, a continuación, haga clic en Aceptar.

## Configurar grupos de autorización

March 27, 2024

Al configurar un análisis de punto final, puede agregar usuarios de forma dinámica a un grupo de autorización cuando el dispositivo del usuario pase el escaneo. Por ejemplo, puede crear un análisis de punto final que compruebe la pertenencia al dominio del dispositivo del usuario. En NetScaler Gateway, cree un grupo local denominado Equipos unidos a un dominio y agréguelo como grupo de autorización para cualquier persona que supere el análisis. Cuando los usuarios se unen al grupo, los usuarios heredan las directivas asociadas al grupo.

No se pueden enlazar directivas de autorización de forma global ni a un servidor virtual. Puede utilizar grupos de autorización para proporcionar un conjunto predeterminado de directivas de autorización cuando los usuarios no están configurados para ser miembros de otro grupo en NetScaler Gateway.

### Para configurar un grupo de autorización mediante una directiva de sesión

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.

4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En Nombre , escriba un nombre para el perfil.
6. En la pestaña Seguridad , haz clic en Configuración avanzada .
7. En Grupos de autorización, haga clic en Supedición global, seleccione un grupo de la lista desplegable, haga clic en Agregar, haga clic en Aceptar y, a continuación, haga clic en Crear.
8. En el cuadro de diálogo Crear política de sesión , junto a Expresiones con nombre , seleccione General, seleccione Valor verdadero , haga clic en Agregar expresión , en Crear y, a continuación, en Cerrar .

Después de crear la directiva de sesión, puede vincularla a un usuario, grupo o servidor virtual.

### Para configurar un grupo de autorización global

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la pestaña Seguridad , haz clic en Configuración avanzada .
4. En Grupo de autorización, seleccione un grupo de la lista desplegable, haga clic en Agregar y, a continuación, haga clic en Aceptar dos veces.

Si quiere eliminar un grupo de autorización de forma global o de la directiva de sesión, en el cuadro de diálogo Configuración de seguridad: avanzada, seleccione el grupo de autorización de la lista y, a continuación, haga clic en Eliminar.

## Configurar expresiones de autenticación previa de seguridad para dispositivos de usuario

January 26, 2024

NetScaler Gateway proporciona varias comprobaciones de seguridad de dispositivos de punto final durante el inicio de sesión del usuario o en otros momentos configurados durante una sesión que ayudan a mejorar la seguridad. Solo los dispositivos de usuario que pasan estas comprobaciones de seguridad pueden establecer una sesión de NetScaler Gateway.

A continuación se indican los tipos de comprobaciones de seguridad de los dispositivos de usuario que se pueden configurar en NetScaler Gateway:

- Antispam
- Antivirus
- Directivas de archivos

- Seguridad en Internet
- Sistema operativo
- Firewall personal
- Directivas de procesos
- Directivas de registro
- Directivas de servicio

Si se produce un error en una comprobación de seguridad en el dispositivo del usuario, no se establece ninguna conexión nueva hasta que se realice una comprobación posterior (en el caso de las comprobaciones que se realizan a intervalos regulares); sin embargo, el tráfico que fluye a través de las conexiones existentes sigue pasando por un túnel a través de Citrix Gateway.

Puede utilizar la utilidad de configuración para configurar directivas de autenticación previa o expresiones de seguridad dentro de las directivas de sesión diseñadas para llevar a cabo comprobaciones de seguridad en los dispositivos de los usuarios.

## Configurar expresiones antivirus, cortafuegos, seguridad de Internet o antispam

March 27, 2024

La configuración de las directivas antivirus, firewall, seguridad de Internet y antispam se configura en el cuadro de diálogo Agregar expresión. La configuración de cada directiva es la misma: las diferencias son los valores que selecciona. Por ejemplo, si desea comprobar si Norton AntiVirus versión 10 y ZoneAlarm Pro están en el dispositivo del usuario, debe crear dos expresiones en la política de sesión o autenticación previa que especifiquen el nombre y el número de versión de cada aplicación.

Al seleccionar Seguridad del cliente como tipo de expresión, puede configurar lo siguiente:

- Componente: tipo de seguridad del cliente, como antivirus, firewall o entrada de registro.
- Nombre: Nombre de la aplicación, proceso, archivo, entrada de registro o sistema operativo.
- Calificador: la versión o el valor del componente que comprueba la expresión.
- Operador: comprueba si el valor existe o es igual al valor.
- Valor: versión de la aplicación para antivirus, firewall, seguridad de Internet o software antispam en el dispositivo del usuario.
- Frecuencia: Frecuencia con la que se ejecuta un análisis posterior a la autenticación, en minutos.
- Peso del error: ponderación asignada a cada mensaje de error contenido en una expresión anidada cuando varias expresiones tienen cadenas de error diferentes. El peso determina qué mensaje de error aparece.

- Frescura: define la antigüedad de una definición de virus. Por ejemplo, puede configurar la expresión para que las definiciones de virus no tengan más de tres días.

### Para agregar una directiva de seguridad de cliente a una directiva de sesión o de autenticación previa

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:
    a) En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
    b) En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas > Autenticación/autorización y, a continuación, haga clic en Pre-Authentication EPA.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione Seguridad del cliente.
6. Configure los ajustes para lo siguiente:
    a) En Componente, seleccione el elemento que quiere escanear.
    b) En Nombre, escriba el nombre de la aplicación.
    c) En Qualifier, selecciona Versión .
    d) En Operador, seleccione el valor.
    e) En Valor, escriba la cadena de seguridad del cliente, haga clic en Aceptar, en Crear y, a continuación, en Cerrar.

## Configurar directivas de servicio

March 27, 2024

Un servicio es un programa que se ejecuta de forma silenciosa en el dispositivo del usuario. Al crear una directiva de sesión o de autenticación previa, puede crear una expresión que garantice que los dispositivos de usuario ejecuten un servicio determinado cuando se establece la sesión.

### Para configurar una directiva de servicio

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:
    a) En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
    b) En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas > Autenticación/autorización y, a continuación, haga clic en Pre-Authentication EPA.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione Seguridad del cliente.
6. Configure los ajustes para lo siguiente:
    a) En Componente, seleccione Servicio.
    b) En Nombre, escriba el nombre del servicio.
    c) En Calificador, déjalo en blanco o selecciona Versión.
    d) En función de su selección en Qualifier, realiza una de las siguientes acciones:
        - Si se deja en blanco, en Operador, seleccione == o! =
        - Si ha seleccionado Versión, en Operador, en Valor, escriba el valor, haga clic en Aceptar y, a continuación, en Cerrar.

Puede consultar una lista de todos los servicios disponibles y el estado de cada uno de ellos en un equipo basado en Windows en la siguiente ubicación:

Panel de control > Herramientas administrativas > Servicios

> **Nota:**El nombre del servicio de cada servicio es diferente del nombre que aparece en la lista. Compruebe el nombre del servicio en el cuadro de diálogo
> Propiedades.

## Configurar directivas de proceso

March 27, 2024

Al crear una directiva de sesión o de autenticación previa, puede definir una regla que exija que todos los dispositivos de usuario tengan un proceso concreto ejecutándose cuando los usuarios inicien sesión. El proceso puede ser cualquier aplicación y puede incluir aplicaciones personalizadas.

Nota: La lista de todos los procesos que se ejecutan en un equipo basado en Windows aparece en la pestaña Procesos del
Administrador de tareas de Windows.

### Para configurar una directiva de procesos

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:
    a) En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
    b) En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas > Autenticación/autorización y, a continuación, haga clic en Pre-Authentication EPA.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione Seguridad del cliente.
6. Configure los ajustes para lo siguiente:
    a) En Componente, seleccione Proceso.
    b) En Nombre, escriba el nombre de la aplicación.
    c) En Operador, seleccione EXISTS o NOTEXISTS, haga clic en Aceptar y, a continuación, en Cerrar.

Al configurar una política de análisis de terminales (autenticación previa o posterior a la autenticación) para comprobar si hay un proceso, puede configurar una suma de comprobación MD5.

Al crear la expresión de la directiva, puede agregar la suma de comprobación MD5 al proceso que está buscando. Por ejemplo, si está comprobando si notepad.exe se está ejecutando en el dispositivo del usuario, la expresión es:
CLIENT.APPLICATION.PROCESS (notepad.exe_md5_388b8fbc36a8558587afc90fb23a3b00) EXISTS

## Configurar directivas del sistema operativo

March 27, 2024

Al crear una directiva de sesión o de autenticación previa, puede configurar cadenas de seguridad del cliente para determinar si el dispositivo de usuario ejecuta un sistema operativo concreto cuando los

usuarios inician sesión. También puede configurar la expresión para que busque un service pack o una revisión concretos.

Los valores de Windows y Macintosh son:

| Sistema operativo | Valor |
|---|---|
| macOS X | macOS |
| Windows 8.1 | win8.1 |
| Windows 8 | win8 |
| Windows 7 | win7 |
| Windows Vista | vista |
| Windows XP | winxp |
| Windows Server 2008 | win2008 |
| Windows Server 2003 | win2003 |
| Servidor Windows 2000 | win2000 |
| Plataforma Windows de 64 bits | win64 |

### Para configurar una directiva del sistema operativo mediante la interfaz gráfica de usuario

1. En el panel de navegación, realice una de las siguientes acciones:
    a) Vaya a **Citrix Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
    b) Vaya a **NetScaler Gateway > Directivas > Autenticación previa**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. En **Solicitar acción**, seleccione una acción existente o cree una.
5. Haga clic en **Editor de expresiones**.
6. En **Seleccionar tipo de expresión**, seleccione **Seguridad del cliente**.
7. Configure los ajustes para lo siguiente:
    a) En **Componente**, seleccione **Sistema operativo**.
    b) En **Nombre**, escriba el nombre del sistema operativo.
    c) En Qualifier, realiza una de las siguientes acciones:
        - Deja el campo en blanco
        - Seleccione **Service Pack**
        - Seleccionar **revisión**

- Seleccionar **versión** (solo para macOS)

d) Según lo que haya seleccionado en el paso 7, en Operador, realice una de las siguientes acciones:
   - Si Qualifier está en blanco, en Operador, seleccione EQUAL (= =), NOTEQUAL (!=), EXISTS o NOTEXISTS.
   - Si ha seleccionado Service Pack o Hotfix, seleccione el operador y, en Valor, escriba el valor.

8. Haga clic en **Listo** y luego en **Cerrar**.

Si está configurando un service pack, como client.os (winxp) .sp, si no hay un número en el campo **Valor** , Citrix Gateway devuelve un mensaje de error porque la expresión no es válida.

Si el sistema operativo tiene Service Pack presentes, como Service Pack 3 y Service Pack 4, puede configurar una comprobación solo para Service Pack 4, ya que la presencia de Service Pack 4 indica automáticamente que los Service Pack anteriores están presentes.

## Configurar directivas del Registro

March 27, 2024

Al crear una directiva de sesión o de autenticación previa, puede comprobar la existencia y el valor de las entradas del registro en el dispositivo del usuario. La sesión se establece solo si la entrada en particular existe o tiene el valor configurado o superior.

Al configurar una expresión de registro, siga las siguientes pautas:

- Se utilizan cuatro barras diagonales inversas para separar claves y subclaves, como

  HKEY_LOCAL_MACHINE\\\\ SOFTWARE

- Los guiones bajos se utilizan para separar la subclave y el nombre del valor asociado, como

  HKEY_LOCAL_MACHINE\\\\ SOFTWARE\\\\ VIRUSSOFTWARE_VERSION

- Se utiliza una barra diagonal inversa (\) para indicar un espacio, como en los dos ejemplos siguientes:

  HKEY_LOCAL_MACHINE\\\\ SOFTWARE\\ Citrix\\\\ Secure\ Access\ Client_ProductVersion

  CLIENT.REG (HKEY_LOCAL_MACHINESOftwareSymantecNorton Antivirus_Version).VALUE == 12.8.0.4 -frecuencia 5

La siguiente es una expresión del Registro que busca la clave del Registro del plug-in de NetScaler Gateway cuando los usuarios inician sesión:

CLIENT.REG (secureaccess).VALU==HKEY_LOCAL_MACHINESOftwareCitRIXSecureAccessClient_ProductVersion

> **Nota:** Si está buscando claves y valores del Registro y seleccione Forma libre avanzada en el cuadro de diálogo
> Expresión, la expresión debe comenzar por
> CLIENT.REG

Las comprobaciones de registro se admiten en los cinco tipos más comunes siguientes:

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

Los valores de registro que se van a comprobar utilizan los siguientes tipos:

- Cadena

  Para el tipo de valor de cadena, se comprueba que se distinga entre mayúsculas

- DWORD

  Para el tipo DWORD, el valor se compara y debe ser igual.

- Cadena expandida

  Otros tipos, como binario y multicadena, no son compatibles.

- Solo se admite el operador de comparación '=='.
- No se admiten otros operadores de comparación, como <, > y comparaciones que distinguen mayúsculas y minúsculas.
- La longitud total de la cadena de registro debe ser inferior a 256 bytes.

Puede agregar un valor a la expresión. El valor puede ser una versión de software, una versión del service pack o cualquier otro valor que aparezca en el registro. Si el valor de datos del registro no coincide con el valor con el que se realiza la prueba, se deniega el inicio de sesión a los usuarios.

> **Nota:**No puede buscar un valor dentro de una subclave. El análisis debe coincidir con el valor nombrado y el valor de datos asociado.

### Para configurar una directiva de registro

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:

   a) En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.

b) En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas > Autenticación/autorización y, a continuación, haga clic en Pre-Authentication EPA.

2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione Seguridad del cliente.
6. Configure los ajustes para lo siguiente:

   a) En Componente, seleccione Registro.
   b) En Nombre, escriba el nombre de la clave de registro.
   c) En Calificador, déjalo en blanco o selecciona Valor.
   d) En Operador, realice una de las siguientes acciones:
      - Si el calificador se deja en blanco, seleccione EXISTS o NOTEXISTS
      - Si ha seleccionado Valor en Calificador, seleccione == o !==
   e) En Valor, escriba el valor tal y como aparece en el editor del registro, haga clic en Aceptar y, a continuación, haga clic en Cerrar.

## Configurar expresiones de seguridad de cliente compuestas

March 27, 2024

Puede combinar cadenas de seguridad del cliente para formar expresiones de seguridad de cliente compuestas.

Los operadores booleanos compatibles con NetScaler Gateway son:

- Y (&&)

---

O bien (

---

-

- No (!)

Para mayor precisión, puede agrupar las cadenas entre paréntesis.

> **Nota:** Si utiliza la línea de comandos para configurar expresiones, utilice paréntesis para agrupar las expresiones de seguridad cuando forme una expresión compuesta. El uso de paréntesis mejora la comprensión y depuración de la expresión del cliente.

### Configuración de políticas con el operador AND (&&)

El operador AND (&&) funciona combinando dos cadenas de seguridad de cliente para que la comprobación compuesta pase solo cuando ambas comprobaciones son verdaderas. La expresión se evalúa de izquierda a derecha y, si la primera comprobación falla, no se lleva a cabo la segunda comprobación.

Puede configurar el operador AND (&&) mediante la palabra clave "AND"o los símbolos "&&".

Ejemplo:

A continuación se muestra una comprobación de seguridad del cliente que determina si el dispositivo del usuario tiene la versión 7.0 del antivirus Sophos instalada y en ejecución. También comprueba si el servicio Inicio de sesión en red se está ejecutando en el mismo equipo.

```
1 CLIENT.APPLICATION.AV(sophos).version==7.0 AND CLIENT.SVC(netlogon)
     EXISTS
2 <!--NeedCopy-->
```

Esta cadena también se puede configurar como:

```
1 CLIENT.APPLICATION.AV(sophos).version==7.0 && CLIENT.SVC(netlogon)
     EXISTS
2 <!--NeedCopy-->
```

### Configuración de políticas con el operador OR (||)

El operador OR (

Puede configurar el OR ( ) mediante la palabra clave "OR"o los símbolos '

Ejemplo:

La siguiente es una comprobación de seguridad del cliente que determina si el dispositivo del usuario tiene el archivo c:\file.txt o el proceso putty.exe ejecutándose en él.

```
1 client.file(c:\\\\file.txt) EXISTS) OR (client.proc(putty.exe) EXISTS
2 <!--NeedCopy-->
```

Esta cadena también se puede configurar como

```
client.file(c:\\\\file.txt) EXISTS) || (client.proc(putty.exe) EXISTS
<!--NeedCopy-->
```

### Configuración de políticas mediante el comando NOT (! ) Operador

El NOT (!) o el operador de negación niega la cadena de seguridad del cliente.

Ejemplo:

La siguiente comprobación de seguridad del cliente `c:\\sophos\\_virus\\_defs.dat`pasa si el archivo NO tiene más de dos días de antigüedad:

```
!(client.file(c:\\\\sophos_virus_defs.dat).timestamp==2dy)
<!--NeedCopy-->
```

## Exploraciones de Advanced Endpoint Analysis

January 26, 2024

El análisis avanzado de punto final (EPA) se utiliza para analizar los dispositivos de los usuarios en busca de los requisitos de seguridad de los terminales configurados en un dispositivo Citrix Gateway. Si un dispositivo de usuario intenta acceder al dispositivo NetScaler Gateway, se analiza el dispositivo en busca de información de seguridad, como el sistema operativo, el antivirus, las versiones del explorador web, etc., antes de que un administrador pueda conceder acceso al dispositivo NetScaler Gateway.

El análisis avanzado de EPA es un análisis basado en directivas que se puede configurar en un dispositivo NetScaler Gateway para sesiones de autenticación previa y versiones posteriores. La directiva realiza una comprobación del registro en un dispositivo de usuario y, en función de la evaluación, permite o deniega el acceso a la red NetScaler ADC.

Puede realizar dos tipos de escaneo EPA: exploración OPSWAT y exploración del sistema. En la sección siguiente se explican los tipos de análisis y sus detalles.

**Escaneo OPSWAT.** El mecanismo de análisis proporciona seguridad a distintos niveles, tales como:

- Escaneo específico del producto
- Análisis específico del proveedor
- Exploración genérica

Análisis específico del producto: puede configurar los criterios de análisis para un producto concreto (por ejemplo, **Avast! Antivirus**gratuito ) ofrecido por un proveedor determinado (por ejemplo, **AVAST**

**Software a.s** .) para una categoría (por ejemplo, **Antivirus** ). El acceso solo se concede a los equipos que cumplen los criterios especificados.**

Análisis específico del proveedor: puede configurar los criterios de análisis para un proveedor determinado (por ejemplo, **AVAST Software a.s**. ) De una categoría (por ejemplo, **Antivirus** ). El análisis configurado comprueba los criterios especificados en todos los productos ofrecidos por el proveedor. El acceso solo se concede a los equipos que cumplen los criterios especificados.

Análisis genérico: puede configurar los criterios de exploración para una categoría concreta (por ejemplo, **Antivirus**). El análisis configurado comprueba los criterios especificados en todos los proveedores y los productos ofrecidos por los proveedores. El acceso solo se concede a los equipos que cumplen los criterios especificados.

**Análisis del sistema.** El análisis del sistema proporciona seguridad para los atributos de nivel del sistema, como la dirección MAC. Puede configurar los criterios de exploración para un atributo del sistema (por ejemplo, **dirección MAC**). El acceso solo se concede a los equipos que cumplen los criterios especificados.

## Configurar exploraciones de Advanced Endpoint Analysis

March 27, 2024

Puede configurar dos tipos de exploración EPA, exploración OPSWAT y exploración del sistema.

### Configuración de OPSWAT Scan

Las siguientes exploraciones OPSWAT se configuran en un dispositivo NetScaler Gateway.

- Escaneo específico del producto
- Análisis específico del proveedor
- Exploración genérica

**Nota:**Analiza si se muestra el soporte de un producto en particular en la GUI. Además, la siguiente configuración de análisis OPSWAT toma como ejemplo la EPA previa a la autenticación. El escaneo OPSWAT también se puede configurar para EPA posterior a la autenticación.

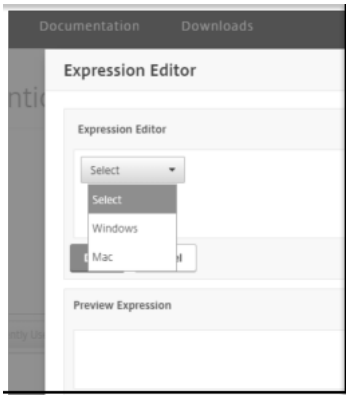
#### Configuración del escaneo OPSWAT específico del producto

Para utilizar la GUI de NetScaler para configurar el análisis OPSWAT específico del producto:

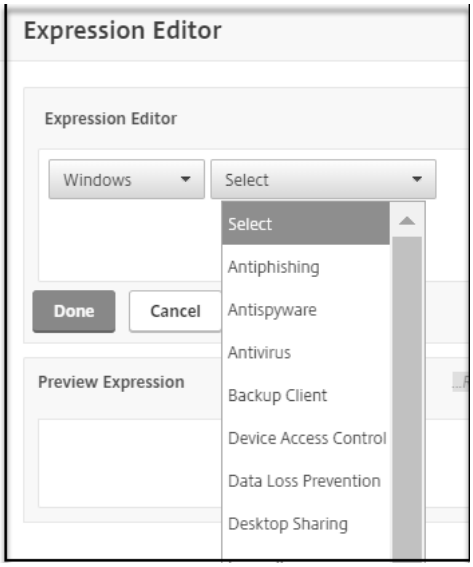
1. Vaya a **Configuración > NetScaler Gateway > Configuración global**.

2. En la página **Configuración global**, haga clic en **el vínculo Cambiar configuración de autenticación previa**.
3. En la página **Configurar el parámetro de preautenticación AAA**, haga clic en el enlace **OPSWAT EPA Editor**.
4. En el área **Editor de expresiones**, seleccione el sistema operativo.

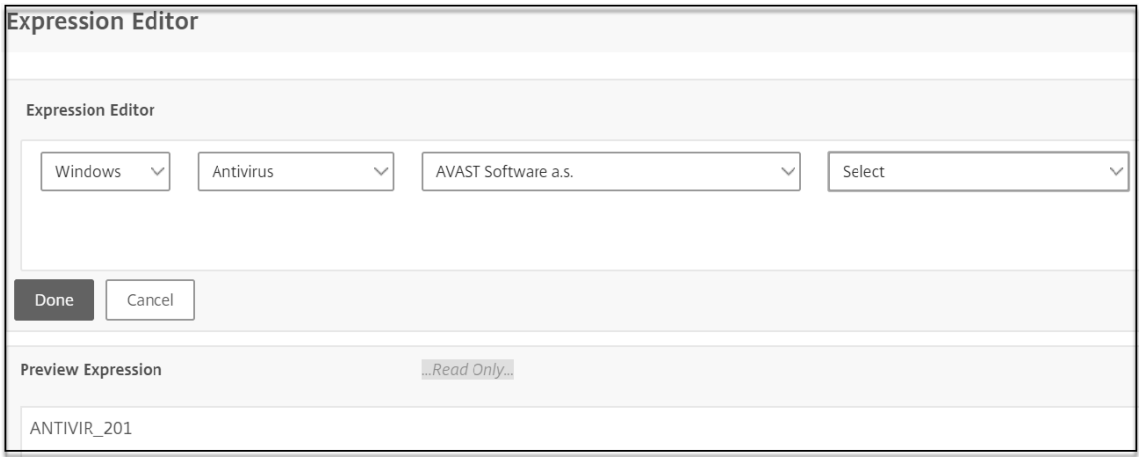



5. Seleccione la categoría, por ejemplo, **Antivirus**.

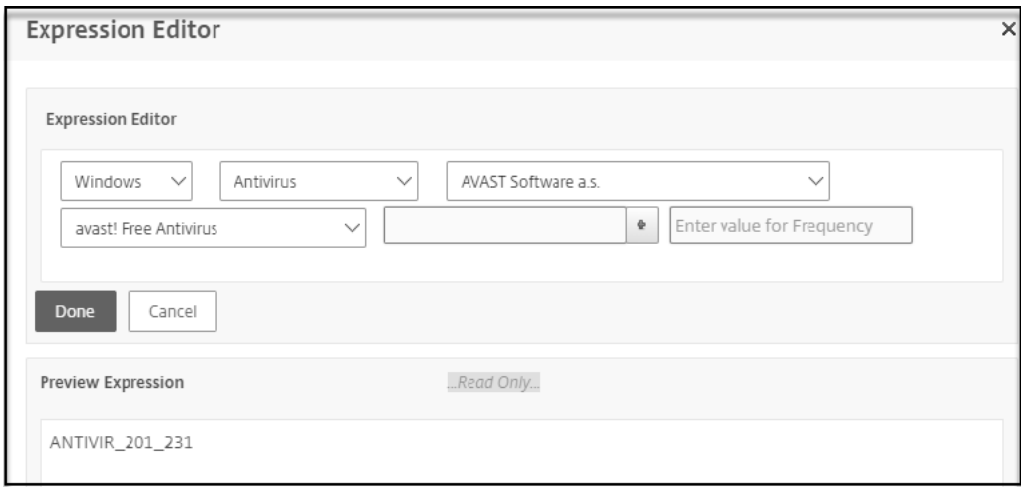



6. Seleccione el proveedor, por ejemplo **AVAST Software a.s**.

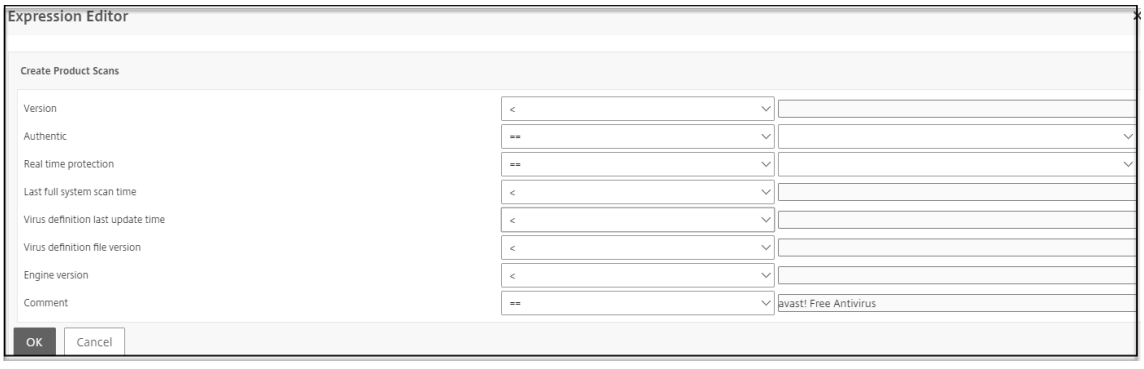
 




7. Seleccione el producto, por ejemplo **Avast! Antivirus gratuito**.

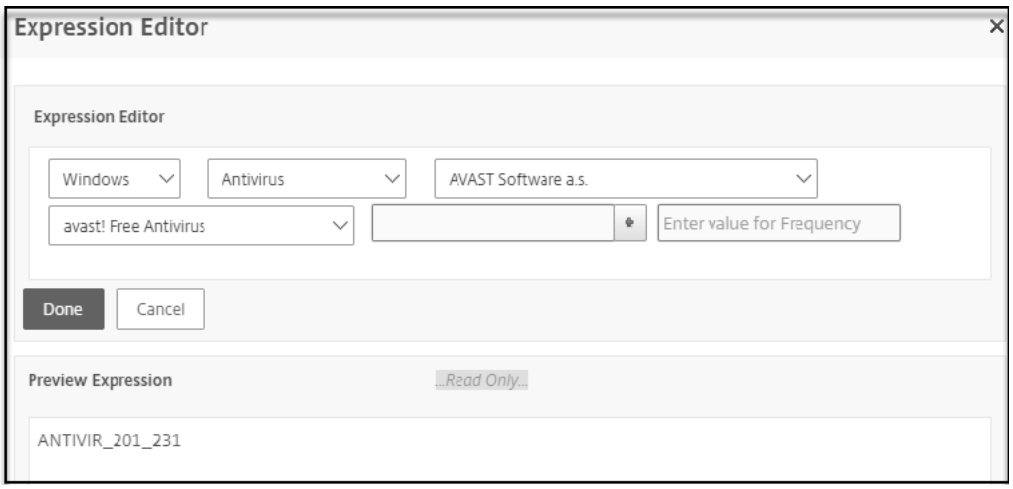



8. Haga clic en el signo **+** junto al menú del producto para configurar el escaneo del producto.




9. Si lo quiere, introduzca un valor para la frecuencia del análisis si quiere realizar un análisis periódico.



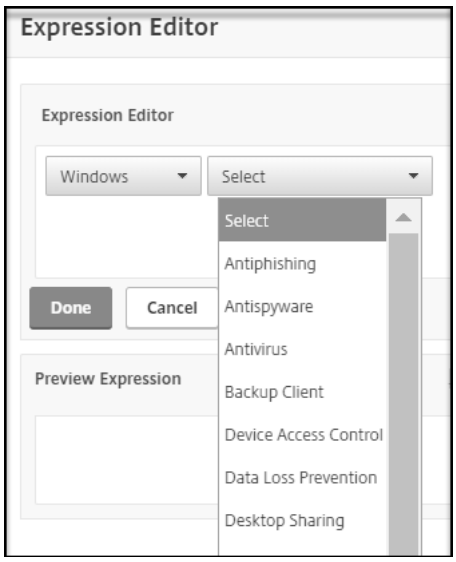

### Configuración del escaneo OPSWAT específico del proveedor

Para utilizar la GUI de NetScaler para configurar el análisis OPSWAT específico del proveedor:

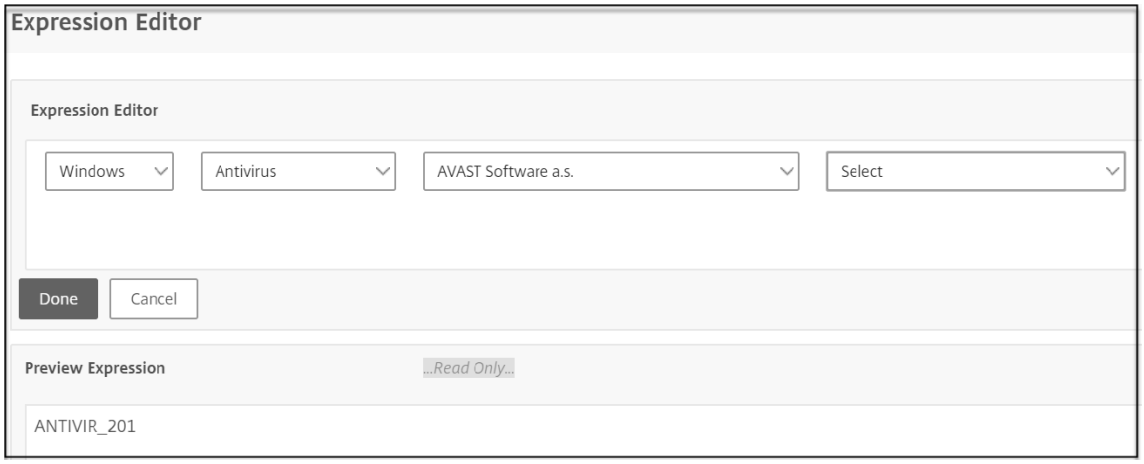
1. Vaya a **Configuración > NetScaler Gateway > Configuración global**.
2. En la página **Configuración global**, haga clic en **el vínculo Cambiar configuración de autenticación previa**.
3. En la página **Configurar el parámetro de preautenticación AAA**, haga clic en el enlace **OPSWAT EPA Editor**.
4. En el área **Editor de expresiones**, seleccione el sistema operativo.


5. Seleccione la categoría, por ejemplo, **Antivirus**.

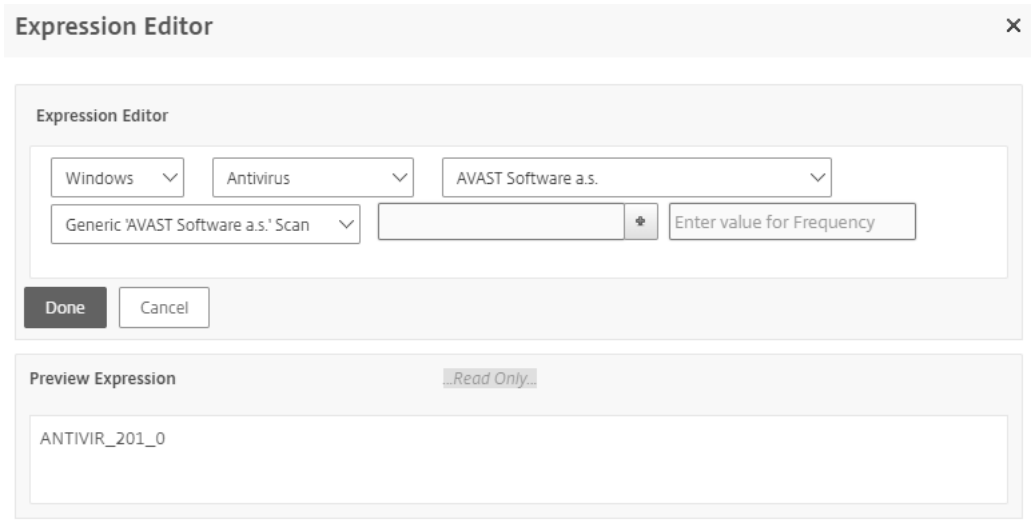
 




6. Seleccione el proveedor, por ejemplo **AVAST Software a.s.**

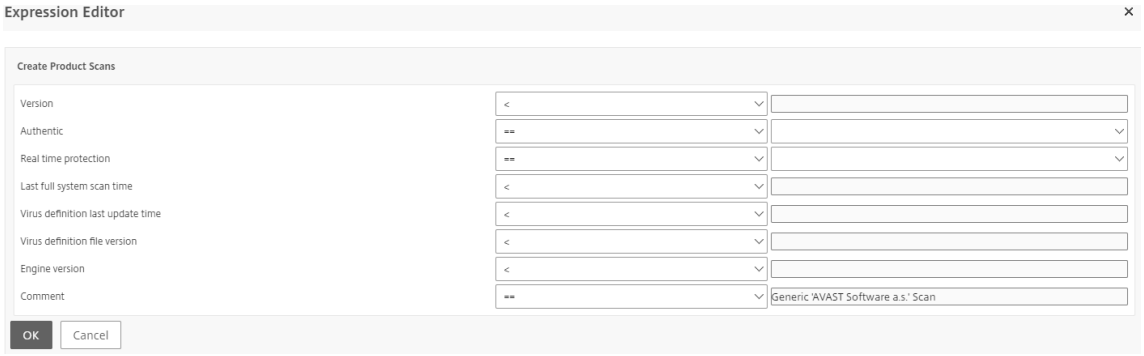



7. Seleccione Análisis **genérico "AVAST Software as"Análisis** específico del proveedor.

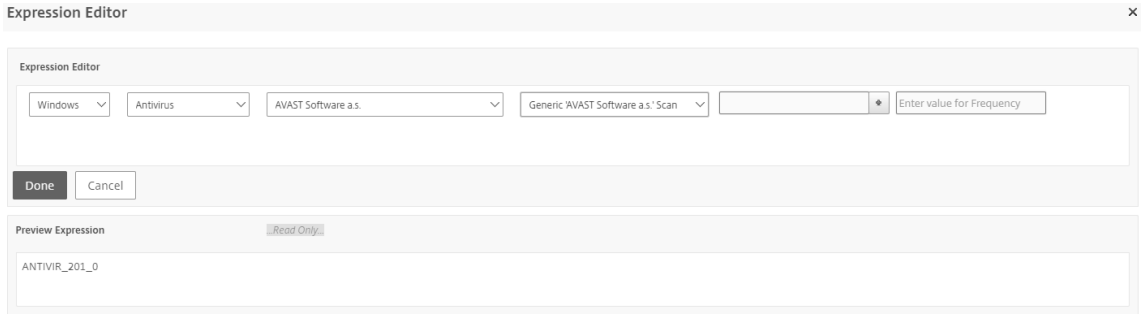


8. Haga clic en el signo **+** junto al menú del producto para configurar el escaneo.




9. Si lo quiere, introduzca un valor para la frecuencia del análisis si quiere realizar un análisis periódico.



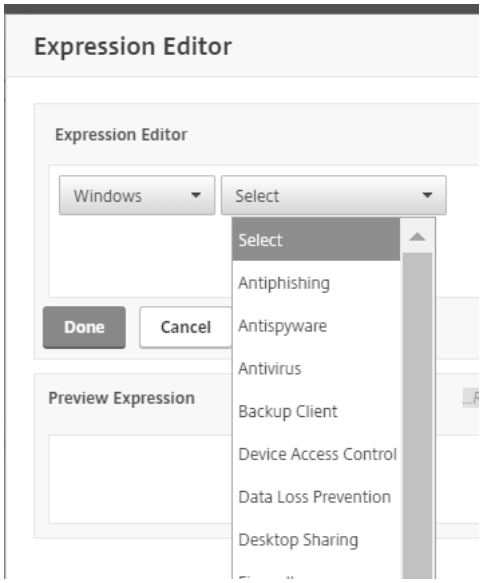

### Configuración del escaneo OPSWAT genérico

Para utilizar la GUI de NetScaler para configurar el análisis OPSWAT genérico:

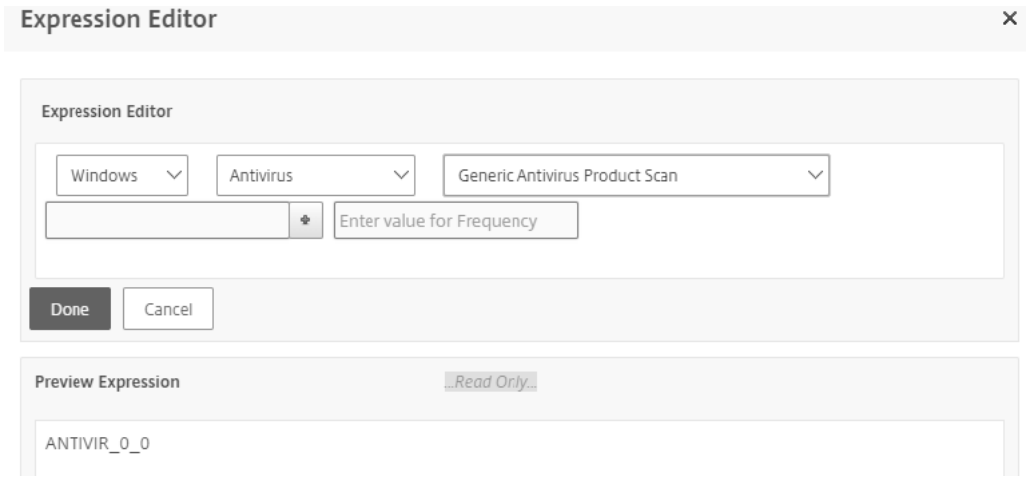
1. Vaya a **Configuración > NetScaler Gateway > Configuración global**.
2. En la página Configuración global, haga clic en el enlace **Cambiar la configuración de autenticación** previa .
3. En la página Configurar el **parámetro de preautenticación AAA** , haga clic en el enlace **OPSWAT EPA Editor** .
4. En el área **Editor de expresiones**, seleccione el sistema operativo.


5. Seleccione la categoría, por ejemplo, **Antivirus**.

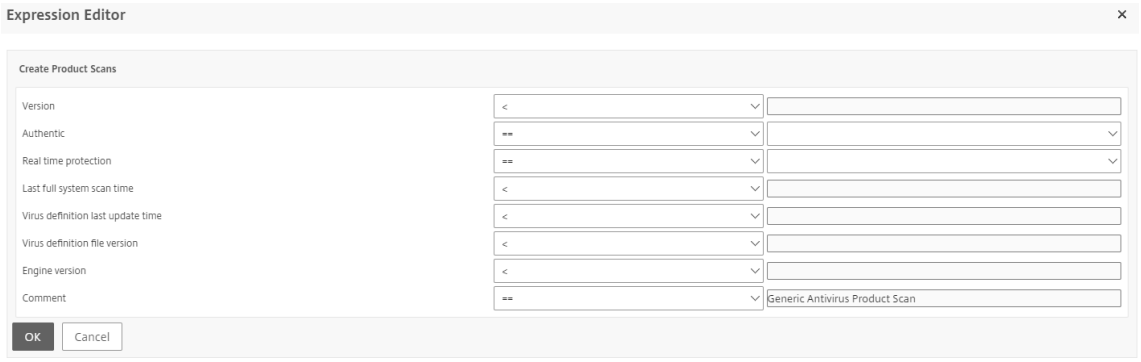



6. Seleccione el análisis específico de categoría "Genérico", por ejemplo, Análisis de **producto antivirus genérico**.




7. Haga clic en el signo **+** junto al menú del producto para configurar el escaneo.




8. Si lo quiere, introduzca un valor para la frecuencia de la exploración si quiere realizar un análisis periódico.


## Configuración de System Scan

Los siguientes análisis del sistema se configuran en un dispositivo NetScaler Gateway.

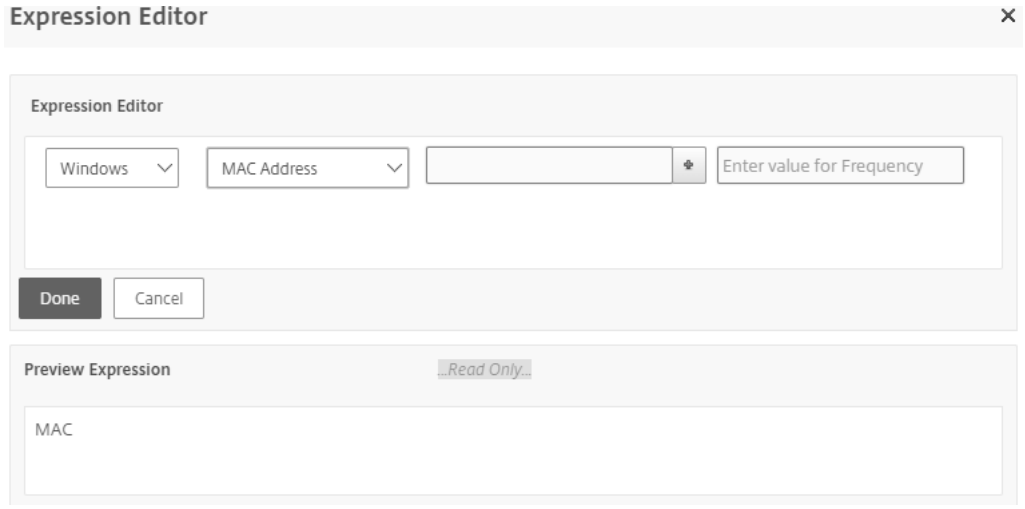
- Dirección MAC
- Comprobación de dominio
- Registro numérico
- Registro no numérico
- Windows Update

Para utilizar la GUI de NetScaler para configurar el análisis del sistema OPSWAT:

1. Vaya a **Configuración > NetScaler Gateway > Configuración global**.
2. En la página **Configuración global**, haga clic en **el vínculo Cambiar configuración de autenticación previa**.
3. En la página **Configurar el parámetro de preautenticación AAA**, haga clic en el enlace **OPSWAT EPA Editor**.
4. En el área **Editor de expresiones**, seleccione el sistema operativo.


5. Seleccione el análisis del sistema deseado en el menú. Por ejemplo, **dirección MAC**.




6. Haga clic en el signo **+** situado junto al menú del producto para configurar el escaneo.


7. Si lo quiere, introduzca un valor para la frecuencia de la exploración si quiere realizar un análisis periódico.


## Actualización de bibliotecas EPA

Para utilizar la GUI de NetScaler para actualizar las bibliotecas EPA:

1. Vaya a**Configuración > NetScaler Gateway > Actualizar componentes de cliente**.
2. En **Actualizar componentes de cliente,** haga clic en el enlace **Actualizar bibliotecas de EPA**.
3. Elija el archivo necesario y haga clic en **Actualizar**.

Para obtener la lista de aplicaciones compatibles con Windows y MAC por OPSWAT para exploraciones de NetScaler ADC, consulte https://support.citrix.com/article/CTX234466.

### Para configurar un perfil de autenticación previa mediante expresiones de Advanced Endpoint Analysis

1. Vaya a **NetScaler Gateway > Directivas**.
2. Seleccione **Autenticación previa**.
3. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
4. Escriba un nombre para el perfil.
5. Selecciona una acción.
6. Si lo quiere, introduzca los nombres de los procesos que se van a detener o los archivos que se van a eliminar en el sistema de endpoint cliente.
7. Haga clic en **Crear**.

Su perfil ahora está disponible para su uso en una política de autenticación previa como acción de solicitud

### Para configurar una política de autenticación previa mediante expresiones de Advanced Endpoint Analysis

1. Vaya a **NetScaler Gateway > Directivas**.
2. Seleccione **Autenticación previa**.

3. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
4. Introduzca un nombre para la directiva.
5. En el menú **Solicitar acción**, seleccione el perfil deseado.
6. En el panel Expresión, seleccione **OPSWAT EPA Editor**.
7. En el primer menú, selecciona un sistema operativo cliente.
8. En el segundo menú, seleccione un tipo de escaneo.
9. Cuando termine de crear la directiva, haga clic en **Crear**.

Enlace la directiva de autenticación previa de Advanced Endpoint Analysis para habilitarla.

**Para enlazar una directiva de autenticación previa**

1. Vaya a **NetScaler Gateway > Directivas**.
2. Seleccione **Autenticación previa**.
3. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
4. En el menú **Acción**, selecciona **Enlaces globales**.
5. Haga clic en **Bind**.
6. En el panel de detalles Directivas que aparece, seleccione la casilla de verificación situada junto a la directiva deseada.
7. Haga clic en **Insertar**.
8. A la directiva se le asigna automáticamente una prioridad (peso). Haga clic en la entrada Prioridad para modificarla según sea necesario.
9. Haga clic en **Aceptar** para enlazar la directiva.

**Para configurar una política de análisis avanzado de terminales para sesiones específicas**

1. Vaya a **NetScaler Gateway > Directivas**.
2. Selecciona **Sesión** .
3. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
4. Introduzca un nombre para la directiva.
5. En el menú **Acción**, realice una de las siguientes acciones:
    - a. Seleccione una acción existente.
    - b. Haga clic en el icono más para mostrar los parámetros de configuración que puede establecer la directiva de sesión. Haga clic en la casilla de verificación **Supedición global** a la derecha de una opción de configuración para activarla. Seleccione **Create**.
6. En el panel Expresión, seleccione **OPSWAT EPA Editor**.
7. En el menú, seleccione un sistema operativo cliente.
8. En el segundo menú de extracción, seleccione un tipo de escaneo.
9. Cuando termine de crear la directiva, haga clic en **Crear**.

Enlace la directiva de sesión de Advanced Endpoint Analysis para habilitarla.

**Para enlazar una directiva de sesión**

1. Vaya a **NetScaler Gateway > Directivas**.
2. Selecciona **Sesión** .
3. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
4. En el menú **Acción**, selecciona **Enlaces globales**.
5. Haga clic en **Bind**.
6. En el panel de detalles Directivas que aparece, seleccione la casilla de verificación situada junto a la directiva deseada.
7. Haga clic en **Insertar**.
8. A la directiva se le asigna automáticamente una prioridad (peso). Haga clic en la entrada Prioridad para modificarla según sea necesario.
9. Haga clic en **Aceptar** para enlazar la directiva.

## Referencia de expresiones de directiva para Advanced Endpoint Analysis

January 26, 2024

En esta referencia se describe el formato y la construcción de las expresiones de Advanced Endpoint Analysis. La utilidad de configuración de Citrix Gateway crea automáticamente los elementos de expresión que se incluyen aquí y no requieren configuración manual.

### Formato de expresión

Una expresión de análisis avanzado de puntos finales tiene el siguiente formato:

```
CLIENT.APPLICATION (SCAN-type_ Product-id_ Method-name _ Method-comparator_ Method-param _...)
```

Donde:

El tipo de escaneo es el tipo de aplicación que se analiza.

Product-ID es la identificación del producto para la aplicación analizada.

El nombre del método es el atributo del producto o del sistema que se está analizando.

El comparador de métodos es el comparador elegido para el análisis.

method-param es el valor o valores de atributo que se analizan.

Por ejemplo:

client.application(ANTIVIR_2600*RTP*==_TRUE)

> **Nota:**Para los tipos de análisis que no son de aplicaciones, el prefijo de expresión es CLIENT.SYSTEM en lugar de CLIENT.APPLICATION.

### Cadenas de expresión

Cada uno de los tipos de análisis compatibles en Advanced Endpoint Analysis utiliza un identificador único en las expresiones. En la tabla siguiente se enumeran las cadenas de cada tipo de análisis.

| Tipo de escaneo | Cadena de expresión tipo escaneo |
|---|---|
| Antiphishing | ANTIPHI |
| Antispyware | ANTISPY |
| Antivirus | ANTIVIR |
| Cliente de backup | BACKUP |
| Control de acceso a dispositivos | DEV-CONT |
| Prevención de pérdida de datos | DATA-PREV |
| Uso compartido de escritorio | DESK-SHARE |
| Firewall | FIREWALL |
| Agente de salud | HEALTH |
| Cifrado de disco duro | HD-ENC |
| Mensajería instantánea | IM |
| Explorador web | BROWSER |
| P2P | P2P |
| Administración de parches | PATCH |
| Filtrado de URL | URL-FILT |
| Dirección MAC | MAC |
| Comprobación de dominio | DOMAIN |
| Análisis numérico del registro | REG-NUM |
| Escaneo de registro no numérico | REGISTRO NO NUMÉRICO |

> **Nota:**Para los escaneos específicos de macOS X, las expresiones incluyen el prefijo MAC- antes del tipo de método. Por lo tanto, para los análisis antivirus y antisuplantación de identidad, los métodos son
> MAC-ANTIVIR y
> MAC-ANTIPHI, respectivamente. Por ejemplo:

```
client.application(MAC-ANTIVIR_2600_RTP_==_TRUE)
<!--NeedCopy-->
```

### Métodos de escaneo de aplicaciones

Al configurar expresiones de análisis avanzado de endpoints, se utilizan métodos para definir los parámetros de los análisis de endpoints. Estos métodos incluyen un nombre de método, un comparador y un valor. En las tablas siguientes se enumeran todos los métodos disponibles para su uso en expresiones.

**Métodos de exploración comunes:**

Los métodos siguientes se utilizan para varios tipos de análisis de aplicaciones.

| Método | Descripción | Comparador | Valores posibles |
|---|---|---|---|
| VERSIÓN* | Especifica la versión de la aplicación. | <, <=, >, >=, !=, == | Cadena de versión |
| AUTHENTIC** | Compruebe si la solicitud dada es auténtica o no. | == | TRUE |
| HABILITADO | Compruebe si la aplicación está habilitada. | == | TRUE |
| EJECUTÁNDOSE | Compruebe si la aplicación se está ejecutando. | == | TRUE |
| COMENTARIO | Campo de comentario (ignorado por el análisis). Delineado por [] dentro de las expresiones. | == | Cualquier texto |

* La cadena VERSION puede especificar una cadena decimal de hasta cuatro valores, como 1.2.3.4.

** Una comprobación AUTHENTIC verifica la autenticidad de los archivos binarios de la aplicación.

> **Nota:**Puede seleccionar una versión genérica para los tipos de escaneo de aplicaciones. Cuando se seleccionan escaneos genéricos, el identificador del producto es 0.

Gateway ofrece una opción para configurar los análisis genéricos para cada tipo de software. Mediante el escaneo genérico, el administrador puede escanear la máquina cliente sin restringir la verificación del escaneo a ningún producto en particular.

Para los escaneos genéricos, los métodos de escaneo solo funcionan si el producto instalado en el sistema del usuario admite ese método de escaneo. Para saber qué productos admiten un método de escaneo en particular, póngase en contacto con el servicio de asistencia de Citrix.

**Métodos de escaneo únicos:**

Los métodos siguientes son exclusivos de los tipos de análisis especificados.

| Método | Descripción | Comparador | Valores posibles |
|---|---|---|---|
| ENABLED-FOR | Compruebe si el software antisuplantación de identidad está activado para la aplicación seleccionada. | todo, cualquiera de, ninguno de | **Para Windows**: Internet Explorer, Mozilla Firefox, Google Chrome, Opera, Safari. **Para Mac:** Safari, Mozilla Firefox, Google, Chrome, Opera |

Tabla 2. Antispyware y antivirus

| Método | Descripción | Comparador | Valores posibles |
|---|---|---|---|
| RTP | Compruebe si la protección en tiempo real está activada o no. | == | TRUE |
| SCAN-TIME | Cuántos **minutos** han transcurrido desde que se realizó un análisis completo del sistema. | <, <=, >, >=, !=, == | Cualquier número positivo |

| Método | Descripción | Comparador | Valores posibles |
|---|---|---|---|
| VIRDEF-FILE-TIME | Cuántos **minutos** han transcurrido desde que se actualizó el archivo de definición de virus (es decir, número de minutos entre la marca de archivo de definición de virus y la fecha y hora actual). | <, <=, >, >=, !=, == | Cualquier número positivo |
| VIRDEF-FILE-VERSION | Versión del archivo de definición. | <, <=, >, >=, !=, == | Cadena de versión |
| ENGINE-VERSION | Versión motor. | <, <=, >, >=, !=, == | Cadena de versión |

Tabla 3. Cliente de reserva

| Método | Descripción | Comparador | Valores posibles |
|---|---|---|---|
| LAST-BK-ACTIVITY | Cuántos **minutos** han pasado desde que se completó la última actividad de copia de seguridad. | <, <=, >, >=, !=, == | Cualquier número positivo |

Tabla 4. Prevención de pérdida de datos

| Método | Descripción | Comparador | Valores posibles |
|---|---|---|---|
| HABILITADO | Compruebe si la aplicación está habilitada o no y si la protección horaria está activada o no. | == | TRUE |

Tabla 5. Agente de chequeo de estado

| Método | Descripción | Comparador | Valores posibles |
|---|---|---|---|
| SYSTEM-COMPL | Compruebe si el sistema cumple con los requisitos. | == | TRUE |

Tabla 6. Cifrado de disco duro

| Método | Descripción | Comparador | Valores posibles |
|---|---|---|---|
| ENC-PATH | PATH para comprobar el estado del cifrado. | SIN OPERADOR | Cualquier texto |
| ENC-TYPE | Compruebe si el tipo de cifrado de la ruta especificada. | todo, cualquiera de, ninguno de | **Lista con las siguientes opciones**: SIN CIFRAR, PARCIAL, CIFRADO, VIRTUAL, SUSPENDIDO, PENDIENTE |

Tabla 7. Explorador web

| Método | Descripción | Comparador | Valores posibles |
|---|---|---|---|
| PREDETERMINADO | Compruebe si está configurado como explorador predeterminado. | == | TRUE |

Tabla 8. Gestión de parches

|Método|Descripción|Comparador|Valores posibles|
|—|—|—|—|
|SCAN-TIME|Cuántos minutos han pasado desde que se realizó la última búsqueda del parche.|<, <=, >, >=, !=, ==|Cualquier número positivo|
|MISSED-PATCH|En el sistema cliente no faltan parches de este tipo.|ninguno de, ninguno de|CUALQUIER preseleccionado (parches preseleccionados en el servidor de Patch Manager) NON|

| Método | Descripción | Comparador | Valores posibles |
|---|---|---|---|
| ADDR | Compruebe si las direcciones MAC de la máquina cliente están o no en la lista dada. | ninguno de, ninguno de | Lista modificable |

Cuadro 10. Pertenencia a

| Método | Descripción | Comparador | Valores posibles |
|---|---|---|---|
| SUFFIX | Compruebe si la máquina cliente existe o no en la lista dada. | ninguno de, ninguno de | Lista modificable |

| Método | Descripción | Comparador | Valores posibles |
|---|---|---|---|
| PATH | Ruta de acceso para la comprobación del registro. En el formato: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client\EnableAutoUpdate. No es necesario que se escapen los caracteres especiales. Todas las claves raíz del registro: HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER, HKEY_USERS, HKEY_CLASSES_ROOT, HKEY_CURRENT_CONFIG | SIN OPERADOR | Cualquier texto |

| Método | Descripción | Comparador | Valores posibles |
|---|---|---|---|
| REDIR-64 | Siga la redirección de 64 bits. Si se establece en TRUE, se seguirá la redirección de WOW (es decir, la ruta de registro se comprueba en los sistemas de 32 bits, pero la ruta redirigida de WOW se comprueba en los sistemas de 64 bits). Si no se establece, no se sigue la redirección de WOW (es decir, se comprueba la misma ruta de registro para los sistemas de 32 y 64 bits). Para las entradas del registro que no se redirigen, esta configuración no tiene ningún efecto. Consulte el siguiente artículo para obtener una lista de claves de registro que se redireccionan en sistemas de 64 bits: http://msdn.microsoft.com/en-us/library/aa384253%28v=vs.85%29.aspx | == | TRUE |

| Método | Descripción | Comparador | Valores posibles |
|---|---|---|---|
| VALOR | Valor esperado para la ruta anterior. Este análisis solo funciona para los tipos de registro de REG_DWORD y REG_QWORD. | <, <=, >, >=, !=, == | Cualquier número |

|Método|Descripción|Comparador|Valores posibles|
|—|—|—|—|
|ruta|Ruta para la comprobación del registro.
Compruebe el análisis del registro para ver el tipo numérico. |SIN OPERADOR|Cualquier texto|
|redir-64|Seguir la redirección
de 64 bits Compruebe el escaneo del registro para ver si hay un tipo numérico. |==|VERDADERO|
|VALUE|Valor esperado para la ruta anterior. Para las entradas de registro de tipo cadena, el valor del registro se compara directamente con el valor esperado. Para el tipo de entrada de registro REG_BINARY, el valor del registro se convierte en una cadena hexadecimal en mayúscula y esta cadena se compara con el valor esperado.|==,! =|Cualquier texto|

Fin

## Solucionar problemas con las exploraciones de Advanced Endpoint Analysis

January 26, 2024

Para ayudar a solucionar problemas de análisis de análisis avanzado de endpoints, los plug-ins cliente escriben información de registro en un archivo de los sistemas de endpoints cliente. Estos archivos de registro se encuentran en los siguientes directorios, según el sistema operativo del usuario.

**Windows Vista, Windows 7, Windows 8, Windows 8.1 y Windows 10:**

C:\Usuarios\<nombre_de_usuario>\AppData\Local\Citrix\AGEE\nsepa.txt

**Windows XP:**

C:\Documents and Settings\Todos los usuarios\Datos de aplicaciones\Citrix\AGEE\nsepa.txt

**Sistemas macOS X:**

~/Biblioteca/Application Support/Citrix/EPAPlugin/epaplugin.log

(Donde el símbolo ~ indica la ruta del directorio principal del usuario de macOS X correspondiente).

## Administrar sesiones de usuario

January 26, 2024

Puede administrar las sesiones de usuario en la GUI de NetScaler ADC desde el cuadro de diálogo **Sesiones de usuarios activos**. Este cuadro de diálogo muestra una lista de las sesiones de usuario activas en NetScaler Gateway. Puede ver las sesiones de usuario final o grupo mediante el nombre de usuario, el nombre del grupo o la dirección IP. También puede ver las sesiones activas en este cuadro de diálogo. La información de la sesión incluye:

- Nombre de usuario
- Dirección IP del dispositivo del usuario
- Número de puerto del dispositivo de usuario
- Dirección IP del servidor virtual
- Número de puerto del servidor virtual
- Dirección IP de intranet asignada al usuario

### Administrar las sesiones de usuario mediante la interfaz gráfica de usuario

#### Para ver las sesiones de usuario

1. En el panel de navegación de la GUI de NetScaler ADC, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Supervisar conexiones, haga clic en **Sesiones de usuario activas**.
3. En **Sesiones de usuario activas**, seleccione uno de los siguientes tipos.
    - **Usuarios activos**
    - **Grupos activos**
    - **IP de intranet**: cuando selecciona IP de intranet, debe introducir la dirección IP de la intranet y la máscara de subred.
4. Haga clic en **Continuar**.

#### Para actualizar la lista de sesiones

Puede recuperar información actualizada sobre las sesiones en NetScaler Gateway.

1. En el panel de navegación de la GUI de NetScaler ADC, haga clic en **NetScaler Gateway**.

2. En el panel de detalles, en Supervisar conexiones, haga clic en **Sesiones de usuario activas**.
3. Haga clic en **Actualizar**.

#### Para sesiones de usuario final o grupo o una sesión que tiene una dirección IP de intranet específica

Puede terminar las sesiones de usuario y grupo. También puede finalizar una sesión que tenga una dirección IP de intranet y una máscara de subred específicas.

1. En el panel de navegación de la GUI de NetScaler ADC, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Supervisar conexiones, haga clic en **Sesiones de usuario activas**.
3. En Sesiones, seleccione un usuario, grupo o sesión que tenga una dirección IP de intranet específica y, a continuación, haga clic en **Finalizar**.

### Administrar las sesiones de usuario mediante la CLI

Puede utilizar los siguientes comandos de CLI para ver las sesiones de usuario, usuario final o grupo.

- `show aaa session`- Muestra todas las conexiones VPN o de autenticación, autorización y auditoría de NetScaler ADC enlazadas al usuario, grupo, dirección IP o intervalo IP especificados.
- `show vpn icaConnection` - Muestra todas las conexiones activas que utilizan el proxy ICA.
- `show system session`: Muestra información sobre todas las sesiones actuales del sistema o sobre la sesión especificada.

## Always On

January 26, 2024

La función Always On de NetScaler Gateway garantiza que los usuarios estén siempre conectados a la red empresarial. Esta conectividad VPN persistente se consigue mediante el establecimiento automático de un túnel VPN.

> **Nota**
>
> La función Always On admite portales cautivos para NetScaler ADC 12.0 compilación 51.24 y versiones posteriores.

### Cuándo usar Always On

Utilice Always On cuando necesite proporcionar conectividad VPN fluida basada en la ubicación del usuario y tenga que impedir el acceso a la red de un usuario que no está conectado a una VPN.

En los siguientes casos se ilustra el uso de Always On.

- Un empleado inicia el portátil fuera de la red empresarial y necesita ayuda para establecer la conectividad VPN.
  **Solución:** Cuando el portátil se inicia fuera de la red empresarial, Always On establece sin problemas un túnel y proporciona conectividad VPN.
- Un empleado que utiliza conectividad VPN se traslada a la red empresarial. El empleado se cambia a una red empresarial pero permanece conectado al túnel VPN, lo cual no es un estado deseable.
  **Solución:** Cuando el empleado se traslada a la red empresarial, Always On derriba el túnel VPN y cambia sin problemas al empleado a la red empresarial.
- Un empleado se traslada fuera de la red empresarial y cierra el portátil (no lo apaga). El empleado necesita ayuda para establecer la conectividad VPN al reanudar el trabajo en el portátil.
  **Solución:**Cuando el empleado se mueve fuera de la red empresarial, Always On establece sin problemas un túnel y proporciona conectividad VPN.
- Una empresa quiere regular el acceso a la red que se proporciona a sus usuarios cuando no están conectados a un túnel VPN.
  **Solución:** Según la configuración, Always On restringe el acceso, lo que permite a los usuarios acceder únicamente a la red de puerta de enlace.

### Comprensión del marco Always On

Always On conecta automáticamente a un usuario a un túnel VPN que el cliente ha establecido previamente. La primera vez que el usuario necesita un túnel VPN, debe conectarse a la URL de NetScaler Gateway y establecer el túnel. Una vez descargada la configuración Always On en el cliente, esta configuración impulsa el establecimiento posterior del túnel.

El ejecutable del cliente de NetScaler Gateway siempre se ejecuta en el equipo cliente. Cuando el usuario inicia sesión o cambia la red, el cliente de NetScaler Gateway determina si el portátil del usuario se encuentra en la red empresarial. Según la ubicación y la configuración, el cliente de NetScaler Gateway establece un túnel o derriba un túnel existente.

El establecimiento del túnel se inicia solo después de que el usuario inicie sesión en el equipo. El cliente Citrix Gateway utiliza las credenciales de la máquina cliente para autenticarse en el servidor Gateway e intenta establecer un túnel.

### Restablecimiento automático de un túnel

El restablecimiento automático de un túnel se activa cuando NetScaler Gateway derriba un túnel VPN.

> **Nota**
>
> En el error de End-Point Analysis, el cliente de NetScaler Gateway no vuelve a intentar establecer el túnel, pero muestra un mensaje de error. Si se produce un error de autenticación, el cliente de NetScaler Gateway solicita credenciales al usuario.

### Métodos de autenticación de usuarios compatibles para establecer túneles sin problemas

Los métodos de autenticación de usuarios compatibles son los siguientes:

- Nombre de usuario + contraseña de AD: si el nombre de usuario y la contraseña de Windows se utilizan para la autenticación, el cliente de NetScaler Gateway establece el túnel sin problemas mediante estas credenciales.
- Certificado de usuario: si se utiliza un certificado de usuario para la autenticación y solo hay un certificado en la máquina, el cliente de NetScaler Gateway establece el túnel sin problemas mediante este certificado. Si hay varios certificados de cliente instalados, el túnel se establece después de que el usuario haya seleccionado el certificado preferido. El cliente Citrix Gateway usa esta preferencia para los próximos túneles establecidos.
- Certificado de usuario y nombre de usuario + Contraseña de AD: este método de autenticación es la combinación de los métodos de autenticación descritos anteriormente.

> **Nota**
>
> Se admiten todos los demás mecanismos de autenticación, pero el establecimiento del túnel no es transparente para ningún otro método de autenticación. Se requiere la intervención del usuario para todos los demás métodos de autenticación.

### Requisitos de configuración para siempre activado

El administrador empresarial debe aplicar lo siguiente para los dispositivos administrados:

- El usuario no debe poder finalizar el proceso/servicio para una configuración específica
- El usuario no debe poder desinstalar el paquete para una configuración específica
- El usuario no debe poder cambiar entradas de registro específicas

> **Nota**
>
> Es posible que la función no funcione como se esperaba si el usuario tiene privilegios de admin-

> istración, como en el caso de los dispositivos no administrados.

### Consideraciones al habilitar la función Always On

Revise la siguiente sección antes de habilitar la función Siempre activado.

Acceso a la red principal: Cuando se establece el túnel, el tráfico hacia la red empresarial se decide en función de la configuración de túnel dividido. No se proporcionan configuraciones adicionales para anular este comportamiento.

Configuración de proxy del equipo cliente: la configuración del proxy del equipo cliente se ignora para conectarse al servidor de puerta de enlace.

> **Nota**
>
> La configuración del proxy del dispositivo NetScaler ADC no se ignora. Solo se ignoran las configuraciones de proxy del equipo cliente. Los usuarios que tienen un proxy configurado en sus sistemas reciben una notificación de que el complemento VPN ha ignorado su configuración de proxy.

Cuando el valor de configuración se establece en "Denegar", se aplican los siguientes cambios:

- IU del cliente: las opciones de cierre de sesión y Salir del menú contextual del complemento y de la interfaz de usuario del complemento están inhabilitadas. Los usuarios no pueden cambiar la URL de la puerta de enlace.
- Inicio de sesión en el explorador: no se permite el inicio de sesión del explorador en una puerta de enlace diferente. Los controles de cliente están inhabilitados.

### Configuración de Always On

Para configurar Always On, cree un perfil Always On en el dispositivo NetScaler Gateway y aplíquelo.

Para crear un perfil Always On:

1. En la GUI de NetScaler ADC, vaya a **Configuración > NetScaler Gateway > Directivas > AlwaysOn.**
2. En la página Perfiles de AlwaysOn, haga clic en **Agregar** .
3. En la página Crear perfil de AlwaysOn, introduzca los siguientes detalles:
    - **Nombre**: El nombre de su perfil.
    - **VPN basada en ubicación**: Seleccione una de las siguientes opciones:
        - **Remoto**para permitir a un cliente detectar si está o no en la red empresarial y establecer el túnel si no está en la red empresarial. Esta es la opción predeterminada.

- **En todas**partes para permitir al cliente omitir la detección de ubicación y establecer el túnel independientemente de la ubicación del cliente

- **Control de cliente**: Seleccione una de las siguientes opciones:
  - **Denegar**para impedir que el usuario cierre la sesión y se conecte a otra puerta de enlace. Esta es la opción predeterminada.
  - **Permitir** que el usuario cierre la sesión y se conecte a otra puerta de enlace.
- **Acceso a la red en caso de error VPN**: Seleccione una de las siguientes opciones:
  - **Acceso completo** para permitir que el tráfico de red fluya hacia y desde el cliente cuando el túnel no está establecido. Esta es la opción predeterminada.
  - **Solo a puerta de enlace** para evitar que el tráfico de red fluya hacia o desde el cliente cuando el túnel no está establecido. Sin embargo, se permite el tráfico hacia o desde la dirección IP de la puerta de enlace.

4. Haga clic en **Crear** para terminar de crear su perfil.

Para aplicar el perfil Always On:

1. En la interfaz de NetScaler ADC, seleccione **Configuración > NetScaler Gateway > Configuración global**.
2. En la página Configuración global, haga clic en el vínculo **Cambiar configuración global** y, a continuación, seleccione la ficha **Experiencia del cliente**.
3. En el menú desplegable **Nombre de perfil AlwaysOn**, seleccione el perfil recién creado y haga clic en **Aceptar**.

> **Nota**
>
> Se puede realizar una configuración similar en el perfil de sesión para aplicar las directivas a nivel de grupo, servidor o usuario.

### Nota sobre los IIP

El túnel a nivel de máquina utiliza la autenticación basada en certificados y la sesión que se crea tiene el nombre común del certificado como nombre de usuario. Por lo tanto, si los certificados de dispositivo tienen nombres comunes únicos, las sesiones de los distintos equipos tienen un nombre de usuario diferente y, por lo tanto, diferentes IIP. Asegúrese de generar un certificado de dispositivo con nombres únicos. Idealmente, debe utilizar los nombres de las máquinas como nombre común del certificado de dispositivo.

**Resumen de comportamiento de diferentes configuraciones para usuarios administradores y usuarios no administradores**

En la tabla siguiente se resume el comportamiento de las distintas configuraciones. También detalla la posibilidad de que el usuario realice ciertas acciones, lo que puede afectar a la funcionalidad de Always On .

| Error de acceso a la red en VPN | Control de clientes | Usuario no administrador | Usuario administrador |
|---|---|---|---|
| `fullaccess` | Permitir | El túnel se establece automáticamente. El usuario puede cerrar la sesión y permanecer fuera de la red. El usuario también puede apuntar a otro NetScaler Gateway. | El túnel se establece automáticamente. El usuario puede cerrar la sesión y permanecer fuera de la red empresarial. El usuario también puede apuntar a otro NetScaler Gateway. |
| `fullaccess` | Negar | El túnel se establece automáticamente. El usuario no puede cerrar la sesión ni apuntar a otro NetScaler Gateway. | El túnel se establece automáticamente. El usuario puede desinstalar el cliente de NetScaler Gateway o trasladarse a otro NetScaler Gateway. |
| onlyToGateway | Permitir | El túnel se establece automáticamente. El usuario puede cerrar la sesión (sin acceso a la red). El usuario también puede apuntar a otro NetScaler Gateway, en cuyo caso, el acceso se otorga únicamente al NetScaler Gateway que acaba de apuntar. | El túnel se establece automáticamente. El usuario puede desinstalar el cliente de NetScaler Gateway o trasladarse a otro NetScaler Gateway. |

| Error de acceso a la red en VPN | Control de clientes | Usuario no administrador | Usuario administrador |
|---|---|---|---|
| onlyToGateway | Negar | El túnel se establece automáticamente. El usuario no puede cerrar la sesión ni apuntar a otro NetScaler Gateway. | El túnel se establece automáticamente. El usuario puede desinstalar el cliente de NetScaler Gateway o trasladarse a otro NetScaler Gateway. |

## VPN siempre activa antes del inicio de sesión en Windows (formalmente siempre en servicio)

January 26, 2024

> **Importante:**
>
> Citrix recomienda actualizar a Citrix Gateway 13.0 o una versión posterior para utilizar la función Always On VPN antes de iniciar sesión en Windows.

## Configurar Citrix Gateway

January 26, 2024

### Citrix ADC con Citrix Gateway: una URL

Citrix ADC con Citrix Gateway permite un acceso seguro y simplificado a cualquier aplicación a través de una única URL para los usuarios móviles y de escritorio. Detrás de esta única URL, los administradores tienen un único punto de configuración, seguridad y control del acceso remoto a las aplicaciones. Además, los usuarios remotos tienen una experiencia mejorada con un inicio de sesión único sin interrupciones en todas las aplicaciones que necesitan, junto con el inicio de sesión/cierre de sesión una vez que son fáciles de usar.

Para ello, Citrix ADC con Gateway, junto con las capacidades de conmutación de contenido y la amplia infraestructura de autenticación de Citrix ADC, proporcionan acceso a los sitios y aplicaciones de

la organización a través de esta URL única. Además, los usuarios remotos pueden usar dispositivos móviles iOS o Android y sistemas Linux, PC o Mac con los complementos de cliente de Citrix Gateway para acceder de manera uniforme a la URL de Citrix Gateway, estén donde estén.

Una implementación de Citrix Gateway permite el acceso mediante una única URL a las siguientes categorías de aplicaciones:

- Aplicaciones de intranet.
- Aplicaciones sin cliente
- Aplicaciones de software como servicio
- Aplicaciones preconfiguradas atendidas por NetScaler ADC
- Aplicaciones publicadas de Citrix Virtual Apps and Desktops

**Las aplicaciones**de intranet pueden ser cualquier aplicación basada en la web que resida dentro de la red empresarial segura. Se trata de recursos internos como un sitio de la intranet de la organización, una aplicación de seguimiento de errores o una wiki.

Por lo general, las **aplicaciones sin cliente** a las que Citrix Gateway proporciona acceso mediante una única URL son Outlook Web Access y SharePoint, que normalmente también residen en la red empresarial segura. Estas aplicaciones proporcionan acceso al correo electrónico de Exchange y a los recursos del equipo sin software cliente dedicado que debe estar disponible para los usuarios remotos.

**Las aplicaciones**SaaS , también conocidas como aplicaciones en la nube, son aplicaciones externas basadas en la nube de las que dependen las organizaciones, como Sharefile, SalesForce o NetSuite. El inicio de sesión único basado en SAML es compatible con las aplicaciones SaaS que lo ofrecen.

Es posible que algunas organizaciones tengan **aplicaciones de NetScaler ADC preconfiguradas** implementadas en una configuración equilibrada de carga de ADC de Citrix; muchas veces esto también se conoce como una aplicación de "proxy inverso". Citrix Gateway admite estas aplicaciones cuando un servidor virtual para la implementación reside en la misma instancia o dispositivo Citrix ADC Citrix Gateway. Estas aplicaciones pueden tener su propia configuración de autenticación, que es independiente de la configuración de Citrix Gateway.

Todas las **aplicaciones publicadas de Citrix Virtual Apps and Desktops** pueden estar disponibles a través de una URL de Citrix Gateway. Las directivas de SmartAccess y SmartControl pueden aplicarse opcionalmente a directivas granulares y control de acceso a estos recursos.

### El asistente de configuración de Citrix Gateway

El método recomendado para configurar un Citrix ADC con la implementación de Citrix Gateway es utilizar el asistente de configuración de Citrix Gateway.El asistente le guía por la configuración y crea todos los servidores virtuales, directivas y expresiones necesarios, y aplica la configuración según los

detalles proporcionados. Tras la configuración inicial, el asistente se puede utilizar para administrar la implementación y supervisar su funcionamiento.

> **Nota**
> El asistente de configuración de Citrix Gateway no realiza una configuración inicial del sistema. El dispositivo Citrix Gateway o la instancia VPX deben haber completado la instalación básica antes de configurar Citrix Gateway. Consulte las instrucciones de instalación deConfiguración de NetScaler Gateway con el Asistente para configuración inicialpara completar la configuración básica.

Los elementos de Citrix Gateway configurados por el asistente son:

- El servidor virtual principal de Citrix Gateway
- Un certificado de servidor SSL para el servidor virtual Citrix Gateway
- Una configuración de autenticación primaria y otra secundaria opcional
- Selección del tema del portal y personalización opcional
- Las aplicaciones de usuario a las que se va a acceder a través del portal Citrix Gateway

Para cada uno de estos elementos, es necesario proporcionar información de configuración. Para una implementación básica de Citrix Gateway, se necesita la siguiente información.

- Para el servidor virtual Citrix Gateway principal, la dirección IP pública y el número de puerto IP para la implementación. Será la dirección IP que se resuelva en DNS en el nombre de host de la URL de Citrix Gateway. Por ejemplo, si la URL de la implementación de Citrix Gateway es `https://mycompany.com/`, la dirección IP debe resolverse en mycompany.com.
- El certificado de servidor SSL firmado para la implementación. NetScaler Gateway admite certificados con formato PEM o PFX.
- Información del servidor de autenticación principal. Los sistemas de autenticación compatibles con esta configuración de autenticación son LDAP/Active Directory, RADIUS y basados en certificados. También se puede crear una configuración de autenticación LDAP o RADIUS secundaria. Las direcciones IP del servidor de autenticación deben proporcionarse junto con las credenciales de administrador o los atributos de directorio pertinentes. Para la autenticación de certificados, se deben proporcionar los atributos del certificado de dispositivo y un certificado de CA.
- Se puede seleccionar un tema del portal. Si se desea un diseño de portal personalizado o de marca, se pueden cargar gráficos personalizados en el sistema con el asistente.
- Para las aplicaciones de usuario basadas en web, se deben especificar las URL de las aplicaciones individuales. En el caso de las aplicaciones web que van a utilizar la autenticación de inicio de sesión único de SAML, la utilidad recopila la URL de Assertion Consumer Service junto

con otros parámetros SAML opcionales. Recopile los detalles de configuración de antemano para las aplicaciones que utilizan un sistema de autenticación SAML.

- Para que los recursos publicados de Citrix Virtual Apps and Desktops estén disponibles a través de la implementación de Citrix Gateway, debe especificar el punto de integración (StoreFront, la Interfaz Web o la Interfaz Web en Citrix ADC). La utilidad requiere el nombre de dominio completo del punto de integración, la ruta del sitio, el dominio de inicio de sesión único, la URL del servidor de Secure Ticket Authority (STA) y otros, según el tipo de punto de integración.

#### Administración de configuración adicional

Para la configuración específica del sitio que no está disponible en la utilidad de configuración de Citrix Gateway, como la configuración de SSL alternativa o las políticas de sesión, puede administrar la configuración necesaria en la utilidad de configuración de Citrix Gateway. Puede modificar estos parámetros en los servidores virtuales VPN o de Content Switching una vez que los haya creado la utilidad de configuración de Citrix Gateway.

### Servidor virtual de cambio de contenido

Se trata de la entidad de configuración de NetScaler ADC detrás de la dirección IP y la URL principales de la implementación. Los certificados y parámetros del servidor SSL se administran en este servidor virtual. Dado que este servidor virtual es el host de red que responde a la implementación, la respuesta del servidor ICMP y el estado de RHI se pueden modificar en este servidor virtual, si es necesario. El servidor virtual Content Switching se encuentra en la ficha Configuración en **Traffic Management** > **Content Switching** > **Virtual Servers**.

#### Servidor virtual VPN

Todos los demás parámetros, perfiles y enlaces de políticas de VPN para la configuración de Citrix Gateway se administran en este servidor virtual, incluida la configuración de autenticación principal. Esta entidad se administra en la ficha Configurar NetScaler Gateway > Servidores virtuales. El nombre del servidor virtual VPN correspondiente incluirá el nombre dado al servidor virtual de conmutación de contenido durante la configuración inicial de Citrix Gateway.

> **Nota**
> Los servidores virtuales VPN creados para una implementación de Citrix Gateway no son direccionables y se les asigna la dirección IP 0.0.0.0.

# Preguntas frecuentes acerca Gateway unificado

January 26, 2024

¿Qué es Gateway unificado?
**

Gateway unificado es una nueva función de la versión NetScaler ADC 11.0, que proporciona la capacidad de recibir tráfico en un único servidor virtual (denominado servidor virtual de Gateway unificado) y, a continuación, dirigir internamente ese tráfico, según corresponda, a los servidores virtuales enlazados al servidor virtual de Gateway unificado.

La función de Gateway unificado permite a los usuarios finales acceder a varios servicios mediante una única dirección IP o URL (asociada con el servidor virtual de Gateway unificado). Los administradores pueden liberar direcciones IP y simplificar la configuración de la implementación de NetScaler Gateway.

Cada servidor virtual de Gateway unificado puede front-end un servidor virtual de NetScaler Gateway junto con cero o más servidores virtuales de equilibrio de carga como parte de una formación. Unified Gateway funciona aprovechando la función de conmutación de contenido del dispositivo Citrix ADC.

Algunos ejemplos de implementaciones de Gateway unificado:

- Servidor virtual de Gateway unificado -> [un servidor virtual de NetScaler Gateway]
- Servidor virtual de Gateway unificado -> [un servidor virtual de NetScaler Gateway, un servidor virtual de equilibrio de carga]
- Servidor virtual de Gateway unificado -> [un servidor virtual de NetScaler Gateway, dos servidores virtuales de equilibrio de carga]
- Servidor virtual de Gateway unificado -> [un servidor virtual de NetScaler Gateway, tres servidores virtuales de equilibrio de carga]

Cada uno de los servidores virtuales de equilibrio de carga puede ser cualquier servidor de equilibrio de carga estándar que aloje un servicio de backend, como Microsoft Exchange o Citrix ShareFile.

¿Por qué utilizar Gateway unificado?
**

La función Gateway unificado permite a los usuarios finales acceder a varios servicios mediante una única dirección IP o URL (asociada al servidor virtual de Gateway unificado). Para los administradores, la ventaja es que pueden liberar direcciones IP y simplificar la configuración de la implementación de NetScaler Gateway.

¿Puede haber más de un servidor virtual de Gateway unificado?
**

Sí. Puede haber tantos servidores virtuales de Gateway unificado como necesite.

¿Por qué es necesario cambiar de contenido para Gateway unificado?
**

La función de conmutación de contenido es necesaria porque el servidor virtual de conmutación de contenido es el que recibe tráfico y lo dirige internamente al servidor virtual apropiado. El servidor virtual de conmutación de contenido es el componente principal de la función de Gateway unificado.

En las versiones anteriores a la 11.0, la conmutación de contenido se puede utilizar para recibir tráfico de varios servidores virtuales. ¿Ese uso también se llama Gateway unificado?
**

El uso de un servidor virtual de conmutación de contenido para recibir tráfico de varios servidores virtuales se admite en las versiones anteriores a la 11.0. Sin embargo, la conmutación de contenido no podía dirigir el tráfico a un servidor virtual Citrix Gateway.

Las mejoras de la versión 11.0 permiten que un servidor virtual de conmutación de contenido dirija el tráfico a cualquier servidor virtual, incluido un servidor virtual de NetScaler Gateway.

¿Qué ha cambiado con las directivas de cambio de contenido de Gateway unificado?
**

1. Se agrega un nuevo parámetro de línea de comandos "-TargetVServer"para la acción de conmutación de contenido. El nuevo parámetro se utiliza para especificar el servidor virtual de NetScaler Gateway de destino. Ejemplo:

> añadir acción cs UG_CSACT_myug -TargetVServer UG_VPN_myug

En la utilidad de configuración de NetScaler Gateway, la acción de cambio de contenido tiene una nueva opción, Servidor virtual de destino, que puede hacer referencia a un servidor virtual de NetScaler Gateway.

2. Se puede usar una nueva expresión de directiva avanzada, is_vpn_url, para hacer coincidir las solicitudes específicas de autenticación y NetScaler Gateway.

¿Qué funciones de NetScaler Gateway no se admiten actualmente en Gateway unificado?
**

Todas las funciones son compatibles con Gateway unificado. Sin embargo, se ha informado de un problema menor (identificador de problema 544325) con el inicio de sesión nativo a través del complemento VPN. En este caso, el inicio de sesión único (SSO) transparente no funciona.

Con Gateway unificado, ¿cuál es el comportamiento de los análisis de la EPA?
**

Con Unified Gateway, el análisis de puntos finales se activa solo para los métodos de acceso de Citrix Gateway, no para el acceso AAA-TM. Si un usuario intenta acceder a un servidor virtual AAA-TM aunque

la autenticación se haya realizado en el servidor virtual Citrix Gateway, no se activa el análisis EPA. Sin embargo, si el usuario intenta obtener acceso VPN sin cliente o VPN completa, se desencadena el análisis EPA configurado. En ese caso, se realiza la autenticación o el inicio de sesión único sin interrupciones.

## Configurar

¿Cuáles son los requisitos de licencia de Gateway unificado?
**

Unified Gateway solo es compatible con las licencias Enterprise y Platinum. No estará disponible únicamente para las ediciones de licencia Standard ni para Citrix Gateway.

¿El servidor virtual de NetScaler Gateway utilizado con Gateway unificado necesita una configuración IP/puerto/SSL?
**

Para un servidor virtual Citrix Gateway utilizado con el servidor virtual Unified Gateway, no es necesaria una configuración de IP/puerto/SSL en el servidor virtual Citrix Gateway. Sin embargo, para la funcionalidad del proxy RDP, puede enlazar el mismo certificado de servidor SSL/TLS al servidor virtual de NetScaler Gateway.

¿Debo volver a aprovisionar los certificados SSL/TLS que están en el servidor virtual Citrix Gateway para usarlos con un servidor virtual de Unified Gateway?
**

No necesita volver a aprovisionar los certificados que están enlazados actualmente a su servidor virtual Citrix Gateway. Puede reutilizar cualquier certificado SSL existente y vincularlo al servidor virtual de Unified Gateway.

¿Cuál es la diferencia entre una única URL y una implementación de varios hosts? ¿Cuál necesito?
**

La URL única hace referencia a la capacidad del servidor virtual de Gateway unificado para gestionar el tráfico de un nombre de dominio completo (FQDN). Esta restricción existe cuando Gateway unificado utiliza un certificado de servidor SSL/TLS en el que el sujeto del certificado se rellena con el FQDN. Por ejemplo: ug.citrix.com

Sin embargo, si Unified Gateway utiliza un certificado de servidor comodín, puede gestionar el tráfico de varios subdominios. Por ejemplo: *.citrix.com

Otra opción es la configuración SSL/TLS con funcionalidad Indicador de nombre de servidor (SNI) para permitir el enlace de varios certificados de servidor SSL/TLS. Ejemplos: auth.citrix.com, auth.citrix.de, auth.citrix.co.uk, auth.citrix.co.jp

Un único host frente a varios hosts es similar a la forma en que los sitios web se alojan normalmente en un servidor web (por ejemplo, el servidor HTTP Apache o Microsoft Internet Information Services (IIS)). Si hay un solo host, puede usar la ruta del sitio para cambiar el tráfico de la misma manera que usa alias o "directorio virtual"en Apache. Si hay varios hosts, utiliza un encabezado de host para cambiar el tráfico de forma similar a como usa los hosts virtuales en Apache.

### Autenticación

¿Qué mecanismos de autenticación se pueden utilizar con Gateway unificado?
**

Todos los mecanismos de autenticación existentes que funcionan con Citrix Gateway funcionan con Unified Gateway.

Estos incluyen LDAP, RADIUS, SAML, Kerberos, autenticación basada en certificados, etc.

Cualquier mecanismo de autenticación que esté configurado en el servidor virtual Citrix Gateway antes de usar la actualización se usa automáticamente cuando el servidor virtual Citrix Gateway se coloca detrás del servidor virtual Unified Gateway. No se requieren pasos de configuración adicionales, aparte de asignar una dirección IP no direccionable (0.0.0.0) al servidor virtual Citrix Gateway.

¿Qué es la autenticación"SelfAuth"*?
**

SelfAuth no es un tipo de autenticación por sí solo. SelfAuth describe cómo se crea una URL. Hay un nuevo parámetro de línea de comandos, ssotype, disponible para la configuración de URL de VPN. Ejemplo:

```
\> add vpn url RGB RGB "http://blue.citrix.lab/"-vServerName Blue -
ssotype selfauth
```

SelfAuth es uno de los valores del parámetro ssotype. Este tipo de URL se puede utilizar para acceder a recursos que no están en el mismo dominio que el servidor virtual de Gateway unificado. El ajuste se puede ver en la utilidad de configuración al configurar un marcador.

¿Qué es la autenticación"StepUp"?
**

Cuando se requieren niveles de autenticación adicionales y más seguros para acceder a un recurso AAA-TM, puede usar la autenticación StepUp. En la línea de comandos, utilice un comando authnProfile para establecer el parámetro AuthenticationLevel. Ejemplo:

> agregar AuthenticationProfile AuthProfile -AuthNvsName AAATMVServer -AuthenticationHost auth.citrix.lab -AuthenticationDomain citrix.lab -AuthenticationLevel 100

Este perfil de autenticación está enlazado al servidor virtual de equilibrio de carga.

¿Se admite la autenticación StepUp para los servidores virtuales AAA-TM?
**

Sí, es compatible.

¿Qué es iniciar sesión una vez/cerrar sesión una vez?
**

Iniciar sesión una vez: los usuarios de VPN inician sesión una vez en un servidor virtual AAA-TM o Citrix Gateway. Y a partir de ese momento, los usuarios de VPN tienen acceso sin problemas a todas las aplicaciones empresariales, en la nube y web. No es necesario volver a autenticar al usuario. Sin embargo, la reautenticación se realiza en casos especiales, como AAA-TM StepUp.

Cerrar sesión una vez: después de crear la primera sesión AAA-TM o Citrix Gateway, se utiliza para crear sesiones AAA-TM o Citrix Gateway posteriores para ese usuario. Si se cierra la sesión de alguna de esas sesiones, el dispositivo NetScaler ADC también cierra la sesión de las demás aplicaciones o sesiones del usuario.

¿Se pueden especificar políticas de autenticación comunes a nivel de Unified Gateway con un enlace autenticado específico del servidor virtual de equilibrio de carga AAA-TM a nivel de servidor virtual de equilibrio de carga? ¿Cuáles son los pasos de configuración para admitir este caso de uso?
**

Si necesita especificar políticas de autenticación independientes para el servidor virtual AAA-TM detrás de Unified Gateway, necesitará tener un servidor virtual de autenticación independiente y direccionable de forma independiente (similar a la configuración AAA-TM normal). La configuración del host de autenticación en el servidor virtual de equilibrio de carga debe apuntar a este servidor virtual de autenticación.

¿Cómo se configura Unified Gateway para que los servidores virtuales AAA-TM enlazados tengan sus propias políticas de autenticación?
**

En este escenario, el servidor de equilibrio de carga debe tener la opción de FQDN de autenticación configurada para que apunte al servidor virtual AAA-TM. El servidor virtual AAA-TM debe tener una dirección IP independiente y ser accesible desde Citrix ADC y los clientes.

¿Se requiere un servidor virtual de autenticación AAA-TM para autenticar a los usuarios que acceden a un servidor virtual de Unified Gateway?
**

No. El servidor virtual Citrix Gateway autenticará incluso a los usuarios AAA-TM.

¿Dónde se especifican las directivas de autenticación de NetScaler Gateway, en el servidor virtual de Gateway unificado o en el servidor virtual de NetScaler Gateway?
**

Las directivas de autenticación deben vincularse al servidor virtual Citrix Gateway.

¿Cómo se habilita la autenticación en los servidores virtuales AAA-TM detrás de un servidor virtual de conmutación de contenido de Unified Gateway?
**

Habilite la autenticación en AAA-TM y dirija el host de autenticación al FQDN de conmutación de contenido de Unified Gateway.

## Administración de tráfico AAA

¿Cómo agrego servidores virtuales de TM para el cambio de contenido (URL única o multihost)?
**

No hay diferencia entre agregar servidores virtuales AAA-TM para una sola URL y agregarlos para varios hosts. En cualquier caso, el servidor virtual se agrega como destino en una acción de cambio de contenido. La diferencia entre una URL única y un host múltiple se implementa mediante reglas de directiva de conmutación de contenido.

¿Qué ocurre con las políticas de autenticación enlazadas a un servidor virtual de equilibrio de carga AAA-TM si ese servidor virtual se traslada a un servidor virtual de Unified Gateway?
**

Las directivas de autenticación están enlazadas al servidor virtual de autenticación y el servidor virtual de autenticación está enlazado al servidor virtual de equilibrio de carga. Para el servidor virtual de Gateway unificado, Citrix recomienda tener el servidor virtual de NetScaler Gateway como punto de autenticación único, lo que niega la necesidad de realizar la autenticación en un servidor virtual de autenticación (o incluso la necesidad de un servidor virtual de autenticación específico). Al apuntar el host de autenticación al FQDN del servidor virtual de Unified Gateway, se garantiza que el servidor virtual Citrix Gateway realice la autenticación. Si apunta el host de autenticación al cambio de contenido de Gateway unificado y sigue teniendo un servidor virtual de autenticación vinculado, se ignoran las directivas de autenticación vinculadas al servidor virtual de autenticación. Sin embargo, si apunta un host de autenticación a un servidor virtual de autenticación direccionable independiente, surten efecto las directivas de autenticación vinculadas.

¿Cómo se configuran las políticas de sesión para las sesiones AAA-TM?
**

Si, en Unified Gateway, no se especifica ningún servidor virtual de autenticación para el servidor virtual AAA-TM, las sesiones AAA-TM heredan las directivas de sesión de Citrix Gateway. Si se especifica el servidor virtual de autenticación, se aplican las políticas de sesión AAA-TM enlazadas a ese servidor virtual.

## Personalización del portal

¿Cuáles son los cambios en el portal Citrix Gateway en Citrix ADC 11.0?
**

En las versiones de NetScaler ADC anteriores a la 11.0, se puede configurar una única personalización del portal a nivel global. Todos los servidores virtuales de puerta de enlace de un dispositivo NetScaler ADC determinado utilizan la personalización del portal global.

En NetScaler ADC 11.0, con la función de temas del portal, puede configurar varios temas del portal. Los temas se pueden enlazar de forma global o a servidores virtuales específicos.

¿NetScaler ADC 11.0 admite la personalización del portal de NetScaler Gateway?
**

Con la utilidad de configuración, puede utilizar la nueva función de temas del portal para personalizar y crear los nuevos temas del portal por completo. Puede subir diferentes imágenes, establecer esquemas de color, cambiar etiquetas de texto, etc.

Las páginas del portal que se pueden personalizar son:

- Página de inicio
- Página Análisis de endpoint
- Página Error de Análisis de Endpoint
- Página Post Endpoint Analysis
- Página Conexión VPN
- Página de inicio del portal

Con esta versión, puede personalizar los servidores virtuales de NetScaler Gateway con diseños de portal únicos.

¿Los temas del portal se admiten en implementaciones de clústeres o de alta disponibilidad de NetScaler ADC?
**

Sí. Los temas del portal se admiten en implementaciones de clústeres y alta disponibilidad de NetScaler ADC.

¿Se migrarán mis personalizaciones como parte del proceso de actualización de Citrix ADC 11.0?
**

No. Las personalizaciones existentes en la página del portal de Citrix Gateway que se invoquen mediante la modificación del archivo rc.conf/rc.netscaler o mediante la funcionalidad de tema personalizado en 10.1/10.5 no se migrarán automáticamente al actualizar a Citrix ADC 11.0.

¿Hay que seguir algún paso previo a la actualización para estar preparado para los temas del portal en NetScaler ADC 11.0?
**

Todas las personalizaciones existentes deben eliminarse de los archivos rc.conf o rc.netscaler.

La otra opción es que si se utilizan temas personalizados, se les debe asignar el ajuste Predeterminado:

Vaya a **Configuración > NetScaler Gateway > Configuración global**

Haga clic en **Cambiar configuración global**. Haga clic en **Experiencia de cliente** y seleccione **Predeterminado** en **la lista desplegable Tema** de interfaz de usuario.

Tengo personalizaciones almacenadas en la instancia de NetScaler ADC, invocadas por rc.conf o rc.netscaler. ¿Cómo paso a los temas del portal?
**

El artículo CTX126206 de Citrix Knowledge Center detalla esta configuración para las versiones 9.3 y 10.0 de NetScaler ADC hasta 10.0 build 73.5001.e. Desde NetScaler ADC 10.0, compilación 10.0 73.5002.e (incluidas 10.1 y 10.5), el parámetro UITHEME CUSTOM ha estado disponible para ayudar a los clientes a conservar sus personalizaciones durante los reinicios. Si las personalizaciones están almacenadas en el disco duro Citrix ADC y desea seguir usándolas, haga una copia de seguridad de los archivos de la GUI de la versión 11.0 e insértelos en el archivo de tema personalizado existente. Si quiere pasar a los temas del portal, primero debe desactivar el parámetro UITHEME en Configuración global o en el perfil de sesión, en Experiencia del cliente. O bien puede configurarlo como DEFAULT o GREENBUBBLE. A continuación, podrá empezar a crear y enlazar un tema de portal.

¿Cómo puedo exportar mis personalizaciones actuales y guardarlas antes de actualizar a NetScaler ADC 11.0? ¿Puedo mover los archivos exportados a otro dispositivo NetScaler ADC?
**

Los archivos personalizados que se han cargado en la carpeta ns_gui_custom están en el disco y persisten durante las actualizaciones. Sin embargo, es posible que estos archivos no sean totalmente compatibles con el nuevo kernel de NetScaler ADC 11.0 y otros archivos GUI que forman parte del núcleo. Por lo tanto, Citrix recomienda hacer una copia de seguridad de los archivos GUI de la versión 11.0 y personalizar las copias de seguridad.

Además, no hay ninguna utilidad en la utilidad de configuración para exportar la carpeta ns_custom_gui a otro dispositivo NetScaler ADC. Debe utilizar SSH o una utilidad de transferencia de archivos como WinSCP para sacar los archivos de la instancia de Citrix ADC.

¿Los temas del portal son compatibles con los servidores virtuales AAA-TM?
**

Sí. Los temas del portal son compatibles con los servidores virtuales AAA-TM.

## Proxy RDP

¿Qué ha cambiado en el proxy RDP para Citrix Gateway 11.0?
**

Se han realizado muchas mejoras en RDP Proxy desde la versión de mejora de NetScaler ADC 10.5.e. En NetScaler ADC 11.0, esta función está disponible desde la primera compilación publicada.

### Cambios en las licencias

La función RDP Proxy de NetScaler ADC 11.0 solo se puede utilizar con las ediciones Platinum y Enterprise. Se deben obtener licencias de usuario simultáneo (CCU) de Citrix para cada usuario.

### Habilitar comando

En NetScaler ADC 10.5.e no había ningún comando para habilitar el proxy RDP. En NetScaler ADC 11.0, se ha agregado el comando enable:

> habilitar la función rdpproxy

La función debe tener licencia para ejecutar este comando.

### Otros cambios en el proxy RDP

Se ha convertido en obligatorio un atributo de clave previamente compartida (PSK) en el perfil del servidor.

Para migrar las configuraciones existentes de Citrix ADC 10.5.e para el proxy RDP a Citrix ADC 11.0, se deben comprender y abordar los siguientes detalles.

Si un administrador quiere agregar una configuración de proxy RDP existente a una implementación de Gateway unificado elegida:

- La dirección IP del servidor virtual de NetScaler Gateway debe modificarse y establecerse en una dirección IP no direccionable (0.0.0.0).
- Los certificados de servidor SSL/TLS y las directivas de autenticación deben estar vinculados al servidor virtual de NetScaler Gateway que forma parte de la formación de Gateway unificado elegida.

¿Cómo se migra una configuración de proxy del Protocolo de escritorio remoto (RDP) basada en NetScaler ADC 10.5.e a NetScaler ADC 11.0?
**

Opción 1: Mantenga el servidor virtual Citrix Gateway existente con la configuración de proxy RDP tal como está, con una licencia Platinum o Enterprise.

Opción 2: Mueva el servidor virtual de NetScaler Gateway existente con la configuración de proxy RDP y colóquelo detrás de un servidor virtual de Gateway unificado.

Opción 3: Agregar un servidor virtual de NetScaler Gateway independiente con configuración de proxy RDP a un dispositivo Standard Edition existente.

¿Cómo se configura la configuración del proxy de NetScaler Gateway para RDP mediante la versión NetScaler ADC 11.0?
**

Existen dos opciones para implementar el proxy RDP mediante la versión NS 11.0:

1) Utilizar un servidor virtual NetScaler Gateway externo. Esto requiere una dirección IP/FQDN visible externamente para el servidor virtual de NetScaler Gateway. Esta opción es la que está disponible en NetScaler ADC 10.5.e.

2) Uso de un servidor virtual Unified Gateway front-end del servidor virtual NetScaler Gateway.

Con la opción 2, el servidor virtual de NetScaler Gateway no necesita su propia dirección IP/FQDN, porque utiliza una dirección IP no direccionable (0.0.0.0).

## Integración con otro software de Citrix

### ¿HDX Insight es compatible con Gateway unificado?

Cuando NetScaler Gateway se implementa con Gateway unificado, se deben cumplir las siguientes condiciones:

- El servidor virtual de NetScaler Gateway debe tener un certificado SSL válido vinculado a él.
- El servidor virtual de NetScaler Gateway debe estar activo para generar registros de AppFlow en NetScaler ADM y generar informes de HDX Insight.

### ¿Cómo migro mi configuración HDX Insight existente?

No es necesaria ninguna migración. Las directivas de AppFlow vinculadas a un servidor virtual de NetScaler Gateway se trasladan si ese servidor virtual de NetScaler Gateway se coloca detrás de un servidor virtual de Gateway unificado.

Para los datos existentes en NetScaler ADM para el servidor virtual de NetScaler Gateway, hay dos posibilidades:

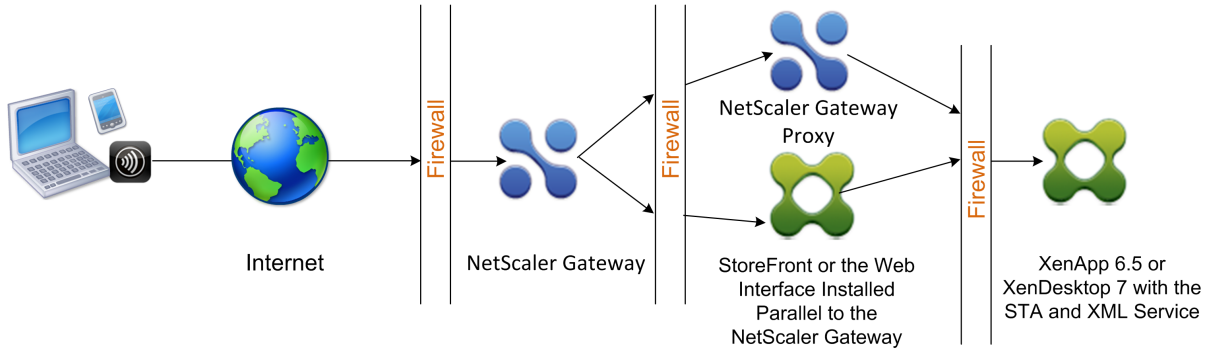
- Si la dirección IP del servidor virtual de NetScaler Gateway se asigna a un servidor virtual de Gateway unificado como parte de la migración a Gateway unificado, los datos permanecen vinculados al servidor virtual de NetScaler Gateway.
- Si al servidor virtual Unified Gateway se le asigna una dirección IP independiente, los datos de AppFlow del servidor virtual Citrix Gateway se vincularán a esa nueva dirección IP. Por lo tanto, los datos existentes no formarán parte de los nuevos datos.

## Implementación en una DMZ de doble salto

January 26, 2024

Algunas empresas usan tres firewalls para proteger sus redes internas. Esos tres firewalls dividen la zona desmilitarizada en dos niveles para ofrecer una capa extra de seguridad a la red interna. Esa configuración de red se llama "zona desmilitarizada de doble salto".

Figura 1. Dispositivos NetScaler Gateway implementados en una DMZ de doble salto




> **Nota**: Con fines ilustrativos, el ejemplo anterior describe una configuración de doble salto que utiliza tres firewalls con StoreFront, la Interfaz Web y Citrix Virtual Apps, pero también puede tener una DMZ de doble salto con un dispositivo en la DMZ y otro en la red segura. Si configura una configuración de doble salto con un dispositivo en la DMZ y otro en la red segura, puede ignorar las instrucciones para abrir puertos en el tercer firewall.

Puede configurar una DMZ de doble salto para que funcione con Citrix StoreFront o la Interfaz Web instalada en paralelo al proxy de Citrix Gateway. Los usuarios se conectan mediante Citrix Receiver.

> **Nota**: Si implementa Citrix Gateway en una DMZ de doble salto con StoreFront, la detección automática basada en correo electrónico para Receiver no funciona.

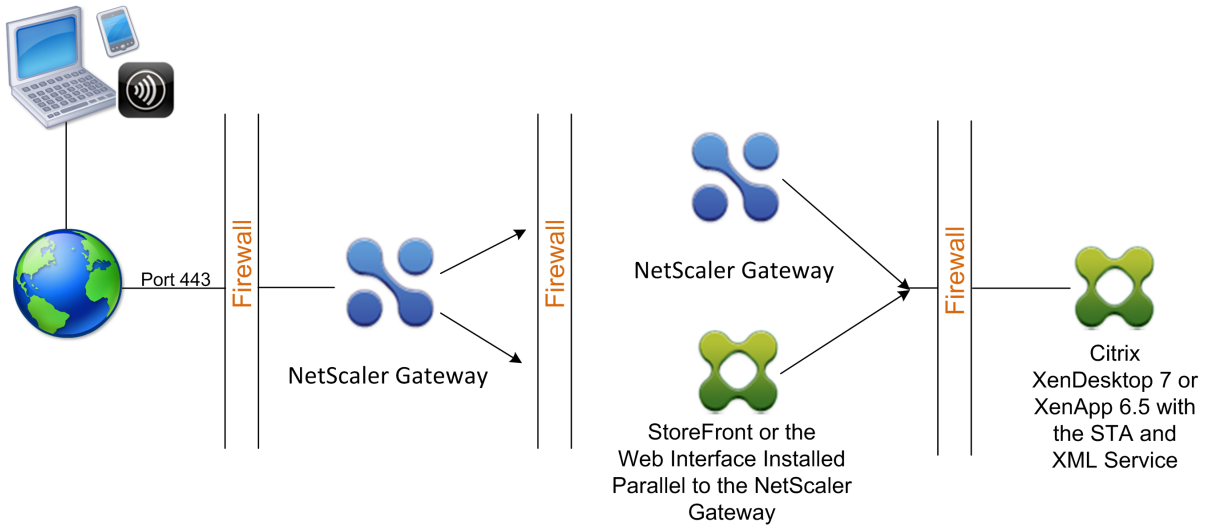
 

# Implementación de NetScaler Gateway en una DMZ de doble salto

January 26, 2024

Algunas empresas usan tres firewalls para proteger sus redes internas. Esos tres firewalls dividen la zona desmilitarizada en dos niveles para ofrecer una capa extra de seguridad a la red interna. Esa configuración de red se llama "zona desmilitarizada de doble salto". Puede implementar Citrix Gateway en una DMZ de doble salto con Citrix Virtual Apps y StoreFront.

Figura 1. Dispositivos NetScaler Gateway implementados en una DMZ de doble salto




Nota: Con fines ilustrativos, el ejemplo anterior describe una configuración de doble salto que utiliza tres firewalls y la Interfaz Web, pero también puede tener una DMZ de doble salto con un dispositivo en la DMZ y un dispositivo en la red segura. Si configura una configuración de doble salto con un dispositivo en la DMZ y otro en la red segura, puede ignorar las instrucciones para abrir puertos en el tercer firewall.

Puede configurar una DMZ de doble salto para que funcione con Citrix StoreFront o la Interfaz Web. Los usuarios se conectan mediante Citrix Receiver.

> **Nota**
>
> Si implementa Citrix Gateway en una DMZ de doble salto con StoreFront, la detección automática basada en correo electrónico para Receiver no funciona.

## Cómo funciona una implementación de doble salto

January 26, 2024

Puede implementar dispositivos NetScaler Gateway en una DMZ de doble salto para controlar el acceso a los servidores que ejecutan Citrix Virtual Apps. Las conexiones de una implementación de doble salto se producen de la siguiente manera:

- Los usuarios se conectan a Citrix Gateway en la primera DMZ mediante un explorador web y Citrix Receiver para seleccionar una aplicación publicada.
- Citrix Receiver se inicia en el dispositivo del usuario. El usuario se conecta a NetScaler Gateway para acceder a la aplicación publicada que se ejecuta en la comunidad de servidores en la red segura.

  **Nota:** Secure Hub y el plug-in de NetScaler Gateway no se admiten en una implementación DMZ de doble salto. Solo Citrix Receiver se utiliza para las conexiones de usuario.
- NetScaler Gateway en la primera DMZ gestiona las conexiones de los usuarios y realiza las funciones de seguridad de una VPN SSL. Citrix Gateway cifra las conexiones de los usuarios, determina cómo se autentican los usuarios y controla el acceso a los servidores de la red interna.
- NetScaler Gateway en la segunda DMZ funciona como dispositivo proxy de NetScaler Gateway. Este Citrix Gateway permite que el tráfico ICA atraviese la segunda DMZ para completar las conexiones de usuario a la comunidad de servidores. Las comunicaciones entre NetScaler Gateway en la primera DMZ y Secure Ticket Authority (STA) en la red interna también se realizan mediante proxy a través de NetScaler Gateway en la segunda DMZ.

NetScaler Gateway admite conexiones IPv4 e IPv6. Puede utilizar la utilidad de configuración para configurar la dirección IPv6.

En la tabla siguiente se sugiere la compatibilidad con la implementación de doble salto para las distintas funciones ICA:

| Función ICA | Soporte de doble salto |
|---|---|
| SmartAccess | Sí |
| SmartControl | Sí |
| Enlightened Data Transport (EDT) | Sí |
| HDX Insight | Sí |
| Fiabilidad de la sesión ICA (puerto 2598) | Sí |
| Migración de sesiones ICA | Sí |
| Tiempo de espera de sesión ICA | Sí |
| ICA de multisecuencia | Sí |
| Framehawk | No |

| | |
|---|---|
| Función ICA | Soporte de doble salto |
| Audio UDP | No |

## Flujo de comunicación en una implementación DMZ de doble salto

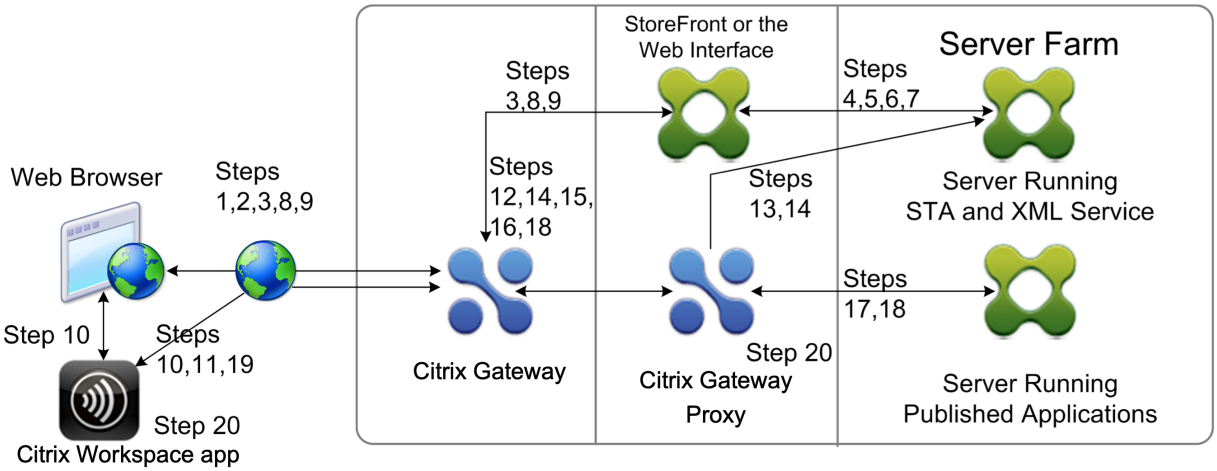
January 26, 2024

Para comprender los problemas de configuración relacionados con una implementación DMZ de doble salto, debe tener conocimientos básicos de cómo se comunican los distintos componentes de NetScaler Gateway y Citrix Virtual Apps de una implementación DMZ de doble salto para admitir una conexión de usuario. El proceso de conexión de StoreFront y la interfaz web es el mismo.

Aunque el proceso de conexión de usuario se produce en un flujo continuo, los siguientes pasos de alto nivel están implicados en el proceso.

- Autenticar usuarios
- Crear un tíquet de sesión
- Inicie la aplicación Citrix Workspace
- Completa la conexión

En la siguiente ilustración se muestran los pasos que se producen en el proceso de conexión del usuario a StoreFront o a la interfaz web. En la red segura, los equipos que ejecutan Citrix Virtual Apps también ejecutan Secure Ticket Authority (STA), XML Service y aplicaciones publicadas.

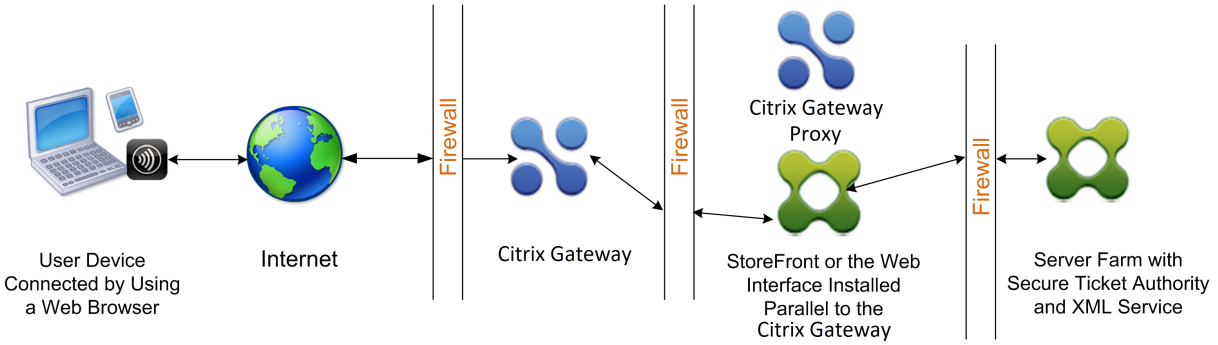


## Proceso de conexión

**La autenticación de usuarios es el primer paso del proceso de conexión de usuarios en una implementación DMZ de doble salto.**

En la siguiente ilustración se muestra el proceso de conexión de usuarios de esta implementación.




Durante la fase de autenticación de usuarios, se produce el siguiente proceso básico:

1. Un usuario escribe la dirección de NetScaler Gateway, por ejemplo, https://www.ng.wxyco.com en un explorador web para conectarse a NetScaler Gateway en la primera DMZ. Si ha habilitado la autenticación de la página de inicio de sesión en NetScaler Gateway, NetScaler Gateway autentica al usuario.
2. NetScaler Gateway en la primera DMZ recibe la solicitud.
3. NetScaler Gateway redirige la conexión del explorador web a la interfaz web.
4. La interfaz web envía las credenciales de usuario al servicio Citrix XML que se ejecuta en el conjunto de servidores de la red interna.
5. Citrix XML Service autentica al usuario.
6. El servicio XML crea una lista de las aplicaciones publicadas a las que el usuario tiene autorización para acceder y envía esta lista a la interfaz web.

   **Nota:**

   - Si habilita la autenticación en NetScaler Gateway, el dispositivo envía la página de inicio de sesión de NetScaler Gateway al usuario. El usuario introduce las credenciales de autenticación en la página de inicio de sesión y el dispositivo autentica al usuario. A continuación, NetScaler Gateway devuelve las credenciales de usuario a la interfaz web.
   - Si no habilita la autenticación, NetScaler Gateway no realiza la autenticación. El dispositivo se conecta a la interfaz web, recupera la página de inicio de sesión de la interfaz web y envía la página de inicio de sesión de la interfaz web al usuario. El usuario introduce las credenciales de autenticación en la página de inicio de sesión de la Interfaz Web y NetScaler Gateway devuelve las credenciales de usuario a la interfaz web.

**La creación del tíquet de sesión es la segunda etapa del proceso de conexión de usuario en una implementación DMZ de doble salto.**

Durante la etapa de creación del tíquet de sesión, se produce el siguiente proceso básico:

7. La interfaz web se comunica tanto con el servicio XML como con la Secure Ticket Authority (STA) de la red interna para producir tíquets de sesión para cada una de las aplicaciones publicadas a las que el usuario tiene autorización para acceder. El vale de sesión contiene una dirección de alias para el equipo que ejecuta Citrix Virtual Apps que aloja una aplicación publicada.
8. El STA guarda las direcciones IP de los servidores que alojan las aplicaciones publicadas. A continuación, el STA envía los tíquets de sesión solicitados a la interfaz web. Cada vale de sesión incluye un alias que representa la dirección IP del servidor que aloja la aplicación publicada, pero no la dirección IP real.
9. La interfaz web genera un archivo ICA para cada una de las aplicaciones publicadas. El archivo ICA contiene el tíquet emitido por la STA. A continuación, la interfaz web crea y rellena una página web con una lista de vínculos a las aplicaciones publicadas y envía esta página web al explorador web del dispositivo del usuario.

   El inicio de la aplicación Citrix Workspace es la tercera etapa del proceso de conexión de usuario en una implementación DMZ de doble salto. El proceso básico es el siguiente:

10. El usuario hace clic en un enlace a una aplicación publicada en la interfaz web. La interfaz web envía el archivo ICA de esa aplicación publicada al explorador del dispositivo del usuario.

    El archivo ICA contiene datos que indican al explorador web que inicie Receiver.

    El archivo ICA también contiene el nombre de dominio completo (FQDN) o el nombre del sistema de nombres de dominio (DNS) de NetScaler Gateway en la primera DMZ.
11. El explorador web inicia Receiver y el usuario se conecta a NetScaler Gateway en la primera DMZ mediante el nombre de NetScaler Gateway del archivo ICA. El enlace inicial de SSL/TLS se produce para establecer la identidad del servidor que ejecuta NetScaler Gateway.

    **La finalización de la conexión es la cuarta y última etapa del proceso de conexión de usuario en una implementación DMZ de doble salto.**

    Durante la fase de finalización de la conexión, se produce el siguiente proceso básico:

    - El usuario hace clic en un enlace a una aplicación publicada en la interfaz web.
    - El explorador web recibe el archivo ICA generado por la interfaz web e inicia la aplicación Citrix Workspace.
      Nota: El archivo ICA contiene código que indica al explorador web que inicie la aplicación Citrix Workspace.
    - La aplicación Citrix Workspace inicia una conexión ICA con NetScaler Gateway en la primera DMZ.

- NetScaler Gateway en la primera DMZ se comunica con Secure Ticket Authority (STA) de la red interna para resolver la dirección de alias del tíquet de sesión en la dirección IP real de un equipo que ejecuta Citrix Virtual Apps o StoreFront. Esta comunicación se transforma mediante proxy a través de la segunda DMZ por el proxy de NetScaler Gateway.
- NetScaler Gateway en la primera DMZ completa la conexión ICA a la aplicación Citrix Workspace.
- La aplicación Citrix Workspace ahora se puede comunicar a través de ambos dispositivos NetScaler Gateway con el equipo que ejecuta Citrix Virtual Apps en la red interna.

Los pasos detallados para completar el proceso de conexión de usuario son los siguientes:

12. La aplicación Citrix Workspace envía el tíquet STA de la aplicación publicada a NetScaler Gateway en la primera DMZ.
13. NetScaler Gateway en la primera DMZ se pone en contacto con el STA de la red interna para validar los tíquets. Para ponerse en contacto con STA, NetScaler Gateway establece un SOCKS o SOCKS con conexión SSL al proxy de NetScaler Gateway en la segunda DMZ.
14. El proxy de NetScaler Gateway de la segunda DMZ transfiere la solicitud de validación de tíquets al STA de la red interna. STA valida el tíquet y lo asigna al equipo que ejecuta Citrix Virtual Apps que aloja la aplicación publicada.
15. El STA envía una respuesta al proxy de NetScaler Gateway en la segunda DMZ, que se transfiere a NetScaler Gateway en la primera DMZ. Esta respuesta completa la validación del tíquet e incluye la dirección IP del equipo que aloja la aplicación publicada.
16. NetScaler Gateway en la primera DMZ incorpora la dirección del servidor Citrix Virtual Apps en el paquete de conexión de usuario y envía este paquete al proxy de NetScaler Gateway en la segunda DMZ.
17. El proxy de NetScaler Gateway de la segunda DMZ realiza una solicitud de conexión al servidor especificado en el paquete de conexión.
18. El servidor responde al proxy de NetScaler Gateway en la segunda DMZ. El proxy de NetScaler Gateway de la segunda DMZ transfiere esta respuesta a NetScaler Gateway en la primera DMZ para completar la conexión entre el servidor y NetScaler Gateway en la primera DMZ.
19. NetScaler Gateway en la primera DMZ completa el enlace SSL/TLS con el dispositivo del usuario transmitiendo el paquete de conexión final al dispositivo del usuario. Se establece la conexión del dispositivo del usuario al servidor.
20. El tráfico ICA fluye entre el dispositivo de usuario y el servidor a través de Citrix Gateway en la primera DMZ y el proxy de Citrix Gateway en la segunda DMZ.

# Preparar una implementación DMZ de doble salto

January 26, 2024

Para prepararse adecuadamente y evitar problemas innecesarios al configurar una implementación DMZ de doble salto, debe responder a las siguientes preguntas:

- ¿Quiero admitir el equilibrio de cargas?
- ¿Qué puertos debo abrir en los firewalls?
- ¿Cuántos certificados SSL necesito?
- ¿Qué componentes necesito antes de comenzar la implementación?

Los temas de esta sección contienen información que le ayudará a responder a estas preguntas según corresponda a su entorno.

### Componentes necesarios para iniciar la implementación

Antes de comenzar una implementación de DMZ de doble salto, asegúrese de que dispone de los siguientes componentes:

- Como mínimo, deben estar disponibles dos dispositivos NetScaler Gateway (uno para cada DMZ).
- Los servidores que ejecutan Citrix Virtual Apps deben estar instalados y operativos en la red interna.
- La Interfaz Web o StoreFront deben instalarse en la segunda DMZ y configurarse para funcionar con el conjunto de servidores de la red interna.
- Como mínimo, se debe instalar un certificado de servidor SSL en NetScaler Gateway en la primera DMZ. Este certificado garantiza que el explorador web y las conexiones de usuario a NetScaler Gateway estén cifradas.

  Necesita certificados adicionales si quiere cifrar las conexiones que se producen entre los demás componentes de una implementación DMZ de doble salto.

# Instalar y configurar NetScaler Gateway en una DMZ de doble salto

March 27, 2024

Debe completar varios pasos para implementar NetScaler Gateway en una DMZ de doble salto. Los pasos incluyen la instalación de dispositivos en ambas DMZ y la configuración de los dispositivos para las conexiones de dispositivos de usuario.

### Instalación de Citrix Gateway en la primera DMZ

Para instalar NetScaler Gateway en la primera DMZ, siga las instrucciones de Instalación del hardware.

Si va a instalar varios dispositivos NetScaler Gateway en la primera DMZ, puede implementar los dispositivos detrás de un equilibrador de carga.

### Configurar NetScaler Gateway en la primera DMZ

En una implementación de DMZ de doble salto, es obligatorio configurar cada NetScaler Gateway de la primera DMZ para redirigir las conexiones a StoreFront o a la interfaz web de la segunda DMZ.

La redirección a StoreFront o a la interfaz web se realiza a nivel de servidor virtual o global de NetScaler Gateway. Para conectarse a la interfaz web a través de NetScaler Gateway, un usuario debe estar asociado a un grupo de usuarios de NetScaler Gateway para el que esté habilitada la redirección a la interfaz web.

### Instalación de Citrix Gateway en la segunda DMZ

El dispositivo NetScaler Gateway de la segunda DMZ se denomina proxy de NetScaler Gateway porque dirige el tráfico ICA y Secure Ticket Authority (STA) a través de la segunda DMZ.

Siga las instrucciones de Instalar el hardware para instalar cada dispositivo Citrix Gateway en la segunda DMZ.

Puede usar este procedimiento de instalación para instalar dispositivos adicionales en la segunda DMZ.

Después de instalar los dispositivos NetScaler Gateway en la segunda DMZ, configure los siguientes valores:

- Configure un servidor virtual en el proxy de NetScaler Gateway.
- Configure los dispositivos NetScaler Gateway en la primera y la segunda DMZ para que se comuniquen entre sí.
- Enlazar NetScaler Gateway en la segunda DMZ de forma global o a un servidor virtual.
- Configure STA en el dispositivo de la primera zona desmilitarizada.
- Abra los puertos de los firewalls que separan la zona desmilitarizada.
- Instale certificados en los dispositivos.

# Configurar parámetros en los servidores virtuales del proxy de NetScaler Gateway

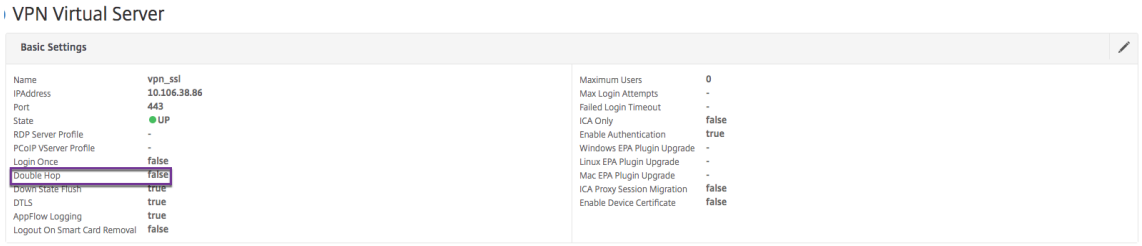
January 26, 2024

Para permitir el paso de conexiones entre los dispositivos NetScaler Gateway, habilite el doble salto en el servidor virtual del proxy NetScaler Gateway.

Cuando los usuarios se conectan, el dispositivo NetScaler Gateway autentica a los usuarios y, a continuación, envía como proxy la conexión al dispositivo proxy. En NetScaler Gateway en la primera DMZ, configure el servidor virtual para que se comunique con NetScaler Gateway en la segunda DMZ. No configure la autenticación ni las directivas en el proxy de NetScaler Gateway. Citrix recomienda inhabilitar la autenticación en el servidor virtual.

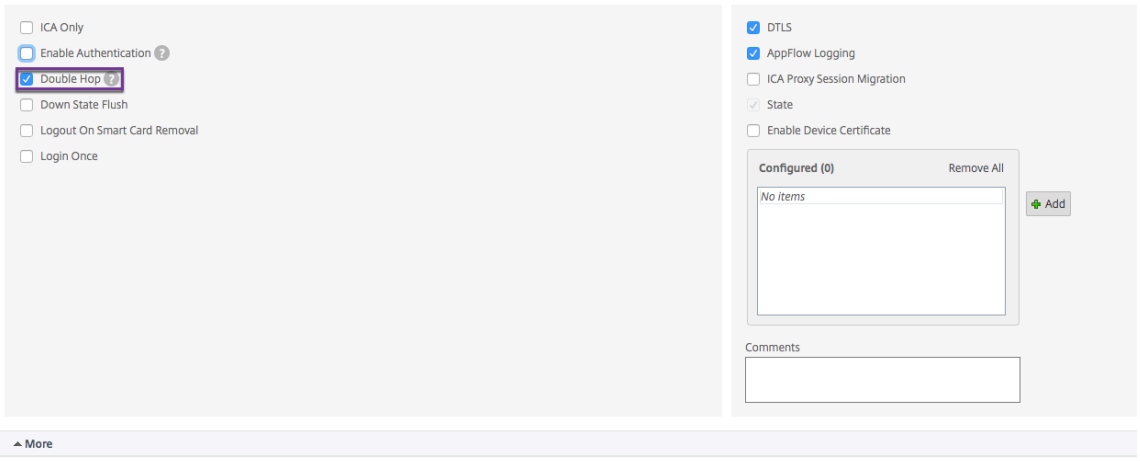
## Para habilitar el doble salto en el servidor virtual del proxy de NetScaler Gateway mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > NetScaler Gateway > Servidores virtuales**.
2. Seleccione un servidor virtual y haga clic en **Modificar**.
3. En la sección **Configuración básica**, haga clic en el icono de modificación y, a continuación, haga clic en **Más**.




4. Selecciona **Doble salto**.

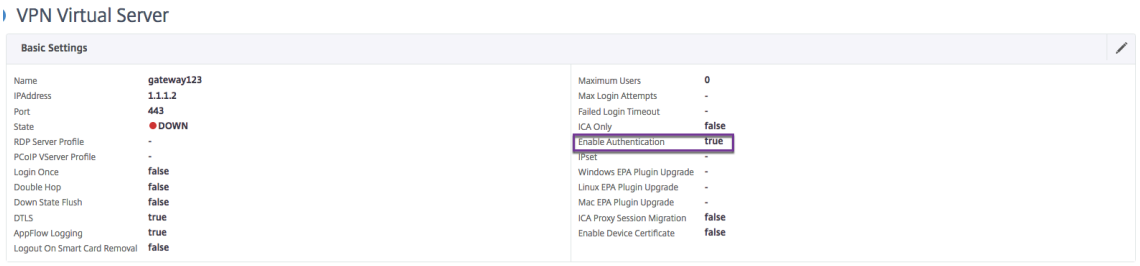
 




5. Haga clic en **Aceptar**.

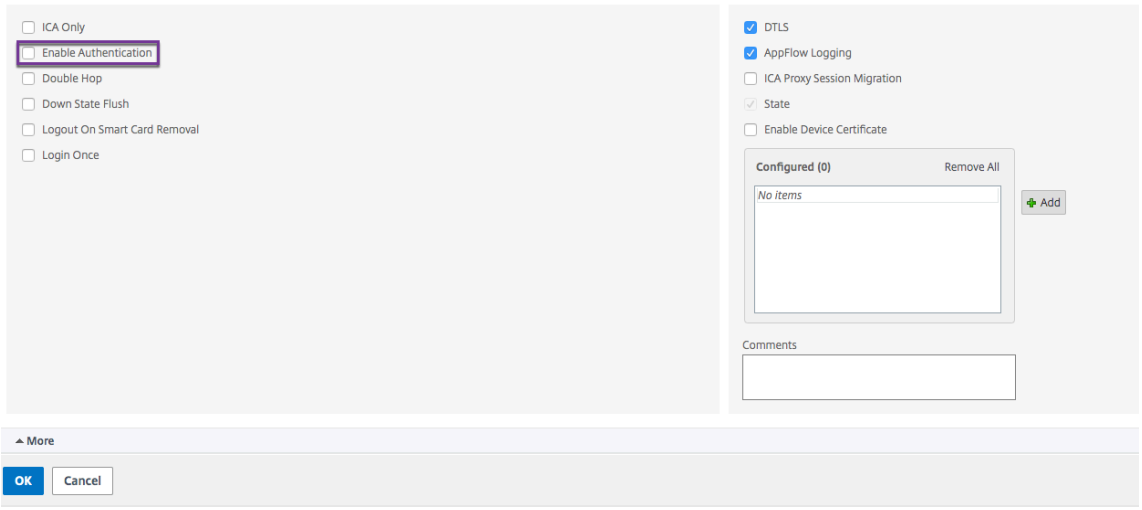
### Para inhabilitar la autenticación en el servidor virtual del proxy de NetScaler Gateway mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > NetScaler Gateway > Servidores virtuales**.
2. Seleccione un servidor virtual y haga clic en **Modificar**.
3. En la sección **Configuración básica**, haga clic en el icono de modificación y, a continuación, haga clic en **Más**.




4. Desactive la casilla de verificación **Habilitar autenticación**.




5. Haga clic en **Aceptar**.

## Configurar el dispositivo para comunicarse con el proxy del dispositivo

March 27, 2024

Al implementar NetScaler Gateway en una DMZ de doble salto, debe configurar NetScaler Gateway en la primera DMZ para que se comunique con el proxy de NetScaler Gateway en la segunda DMZ.

Si implementa varios dispositivos en la segunda DMZ, configura cada dispositivo de la primera DMZ para que se comunique con todos los dispositivos proxy de la segunda DMZ.

Nota: Si quiere utilizar IPv6, configure el servidor de salto siguiente mediante la utilidad de configuración. Para ello, expanda
Citrix Gateway > Recursos y, a continuación, haga clic en Servidores Next Hop. Siga los pasos del procedimiento siguiente y, a continuación, active la casilla de verificación
IPv6.

### Para configurar NetScaler Gateway para que se comunique con el proxy de NetScaler Gateway

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway > Recursos y, a continuación, haga clic en Servidores de salto siguiente.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para el primer NetScaler Gateway.
4. En Dirección IP, escriba la dirección IP del servidor virtual del proxy de NetScaler Gateway en la segunda DMZ.

5. En Puerto, escriba el número de puerto, haga clic en Crear y, a continuación, haga clic en Cerrar. Si utiliza un puerto seguro, como el 443, seleccione Seguro.

Debe configurar cada NetScaler Gateway instalado en la primera DMZ para que se comunique con todos los dispositivos proxy de NetScaler Gateway instalados en la segunda DMZ.

Después de configurar la configuración del proxy de NetScaler Gateway, vincule la directiva a los servidores Next Hop de NetScaler Gateway Global o a un servidor virtual.

### Para enlazar el servidor de siguiente salto de NetScaler Gateway de forma global

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway > Recursos y, a continuación, haga clic en Servidores de salto siguiente.
2. En el panel de detalles, seleccione un servidor de salto siguiente y, a continuación, en Acción, seleccione Enlaces globales.
3. En el cuadro de diálogo Configurar enlace global del servidor de salto siguiente, en Nombre del servidor de salto siguiente, seleccione el dispositivo proxy y, a continuación, haga clic en Aceptar.

### Para enlazar el servidor de siguiente salto de NetScaler Gateway a un servidor virtual

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en Abrir .
3. En la ficha Aplicaciones publicadas, en Servidores Next Hop, haga clic en un elemento y, a continuación, haga clic en Aceptar.

También puede agregar un servidor de siguiente salto desde la ficha Aplicaciones publicadas.

## Configurar NetScaler Gateway para manejar el tráfico STA e ICA

March 27, 2024

Al implementar NetScaler Gateway en una DMZ de doble salto, debe configurar NetScaler Gateway en la primera DMZ para gestionar las comunicaciones con Secure Ticket Authority (STA) y el tráfico ICA de forma adecuada. El servidor que ejecuta STA se puede enlazar de forma global o a un servidor virtual.

Después de configurar el STA, puede enlazar el STA de forma global o a un servidor virtual.

Para configurar y enlazar el STA de forma global:

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Servidores, haga clic en Vincular o desvincular los servidores STA que utilizará Secure Ticket Authority.
3. En el cuadro de diálogo Enlazar/desenlazar servidores STA, haga clic en Agregar.
4. En el cuadro de diálogo Configurar servidor STA, en URL, escriba la ruta al servidor que ejecuta STA, como http://mycompany.com o http://ipAddress y, a continuación, haga clic en Crear.

Para configurar y enlazar el STA a un servidor virtual:

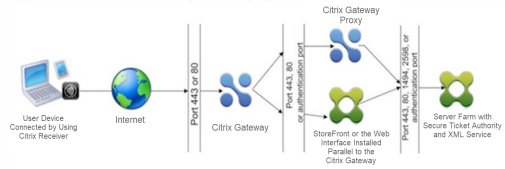
1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en Abrir .
3. En la pestaña Aplicaciones publicadas , en Secure Ticket Authority , haga clic en Agregar .
4. En el cuadro de diálogo Configurar servidor STA, en URL, escriba la ruta al servidor que ejecuta STA, como http://mycompany.com o http://ipAddress y, a continuación, haga clic en Crear.

## Abrir los puertos apropiados en los firewalls

January 26, 2024

Debe asegurarse de que los puertos adecuados estén abiertos en los firewalls para admitir las distintas conexiones que se producen entre los distintos componentes implicados en una implementación de DMZ de doble salto. Para obtener más información sobre el proceso de conexión, consulte Flujo de comunicación en una implementación DMZ de doble salto.

En la siguiente ilustración se muestran los puertos comunes que se pueden utilizar en una implementación DMZ de doble salto.




En la tabla siguiente se muestran las conexiones que se producen a través del primer firewall y los puertos que deben estar abiertos para admitir las conexiones.

| Conexiones a través del primer firewall | Puertos utilizados |
| --- | --- |
| El explorador web de Internet se conecta a NetScaler Gateway en la primera DMZ. **Nota:** NetScaler Gateway incluye una opción para redirigir las conexiones realizadas en el puerto 80 a un puerto seguro. Si habilita esta opción en NetScaler Gateway, puede abrir el puerto 80 a través del primer firewall. Cuando un usuario establece una conexión sin cifrar a NetScaler Gateway en el puerto 80, NetScaler Gateway redirige automáticamente la conexión a un puerto seguro. | Abra el puerto TCP 443 a través del primer firewall. |
| Citrix Receiver desde Internet se conecta a Citrix Gateway en la primera DMZ. | Abra el puerto TCP 443 a través del primer firewall. |

En la tabla siguiente se muestran las conexiones que se producen a través del segundo firewall y los puertos que deben estar abiertos para admitir las conexiones.

| Conexiones a través del segundo firewall | Puertos utilizados |
| --- | --- |
| NetScaler Gateway en la primera DMZ se conecta a la interfaz web en la segunda DMZ. | Abra el puerto TCP 80 para una conexión no segura o el puerto TCP 443 para una conexión segura a través del segundo firewall. |
| NetScaler Gateway en la primera DMZ se conecta a NetScaler Gateway en la segunda DMZ. | Abra el puerto TCP 443 para obtener una conexión SOCKS segura a través del segundo firewall. |
| Si ha habilitado la autenticación en NetScaler Gateway en la primera DMZ, es posible que este dispositivo deba conectarse a un servidor de autenticación de la red interna. | Abra el puerto TCP en el que el servidor de autenticación escucha las conexiones. Los ejemplos incluyen el puerto 1812 para RADIUS y el puerto 389 para LDAP. |

En la tabla siguiente se muestran las conexiones que se producen a través del tercer firewall y los puertos que deben estar abiertos para admitir las conexiones.

| Conexiones a través del tercer firewall | Puertos utilizados |
| --- | --- |
| StoreFront o la interfaz web de la segunda DMZ se conectan al servicio XML alojado en un servidor de la red interna. | Abra el puerto 80 para una conexión no segura o el puerto 443 para una conexión segura a través del tercer firewall. |
| StoreFront o la interfaz web de la segunda DMZ se conectan a la Secure Ticket Authority (STA) alojada en un servidor de la red interna. | Abra el puerto 80 para una conexión no segura o el puerto 443 para una conexión segura a través del tercer firewall. |
| NetScaler Gateway en la segunda DMZ se conecta al STA que reside en la red segura. | Abra el puerto 80 para una conexión no segura o el puerto 443 para una conexión segura a través del tercer firewall. |
| NetScaler Gateway en la segunda DMZ establece una conexión ICA con una aplicación publicada o un escritorio virtual en un servidor de la red interna. | Abra el puerto TCP 1494 para admitir conexiones ICA a través del tercer firewall. Si ha habilitado la fiabilidad de la sesión en Citrix Virtual Apps, abra el puerto TCP 2598 en lugar del 1494. |
| Si habilitó la autenticación en Citrix Gateway en la primera DMZ, es posible que este dispositivo deba conectarse a un servidor de autenticación de la red interna. | Abra el puerto TCP en el que el servidor de autenticación escucha las conexiones. Los ejemplos incluyen el puerto 1812 para RADIUS y el puerto 389 para LDAP. |

## Administrar certificados SSL en una implementación DMZ de doble salto

January 26, 2024

Debe instalar los certificados SSL necesarios para cifrar las conexiones entre los componentes de una implementación DMZ de doble salto.

En una implementación DMZ de doble salto, se producen varios tipos diferentes de conexiones entre los distintos componentes implicados en la implementación. No existe un cifrado SSL de extremo a extremo para estas conexiones. Sin embargo, cada conexión se puede cifrar individualmente.

Para cifrar una conexión es necesario instalar el certificado SSL adecuado (ya sea una raíz de confianza o un certificado de servidor) en los componentes implicados en la conexión.

En la tabla siguiente se muestran las conexiones que se producen a través del primer firewall y los certificados SSL necesarios para cifrar cada una de estas conexiones. El cifrado de las conexiones a través del primer firewall es obligatorio para proteger el tráfico enviado a través de Internet.

| Conexiones a través del primer firewall | Certificados necesarios para el cifrado |
| --- | --- |
| El explorador web de Internet se conecta a NetScaler Gateway en la primera DMZ. | NetScaler Gateway en la primera DMZ debe tener instalado un certificado de servidor SSL. El explorador web debe tener instalado un certificado raíz firmado por la misma entidad de certificación (CA) que el certificado de servidor de NetScaler Gateway. |
| Citrix Receiver desde Internet se conecta a Citrix Gateway en la primera DMZ. | La administración de certificados para esta conexión es la misma que la del explorador web a la conexión de NetScaler Gateway. Si ha instalado los certificados para cifrar la conexión del explorador web, esta conexión también se cifra con esos certificados. |

En la tabla siguiente se muestran las conexiones que se producen a través del segundo firewall y los certificados SSL necesarios para cifrar cada una de estas conexiones. El cifrado de estas conexiones mejora la seguridad pero no es obligatorio.

| Conexiones a través del segundo firewall | Certificados necesarios para el cifrado |
| --- | --- |
| NetScaler Gateway en la primera DMZ se conecta a la interfaz web en la segunda DMZ. | StoreFront o la interfaz web deben tener instalado un certificado de servidor SSL. NetScaler Gateway en la primera DMZ debe tener instalado un certificado raíz firmado por la misma entidad emisora de certificados que el certificado del servidor en la interfaz web. |
| NetScaler Gateway en la primera DMZ se conecta a NetScaler Gateway en la segunda DMZ. | NetScaler Gateway en la segunda DMZ debe tener instalado un certificado de servidor SSL. NetScaler Gateway en la primera DMZ debe tener instalado un certificado raíz firmado por la misma entidad emisora de certificados que el certificado de servidor de NetScaler Gateway en la segunda DMZ. |

En la tabla siguiente se muestran las conexiones que se producen a través del tercer firewall y los certificados SSL necesarios para cifrar cada una de estas conexiones. El cifrado de estas conexiones mejora la seguridad pero no es obligatorio.

| Conexiones a través del tercer firewall | Certificados necesarios para el cifrado |
| --- | --- |
| StoreFront o la interfaz web de la segunda DMZ se conectan al servicio XML alojado en un servidor de la red interna. | Si el servicio XML se ejecuta en el servidor Microsoft Internet Information Services (IIS) del servidor Citrix Virtual Apps, se debe instalar un certificado de servidor SSL en el servidor IIS. Si el servicio XML es un servicio estándar de Windows (no reside en IIS), se debe instalar un certificado de servidor SSL dentro de la retransmisión SSL del servidor. StoreFront o la Interfaz Web deben tener instalado un certificado raíz firmado por la misma entidad emisora de certificados que el certificado de servidor instalado en el servidor Microsoft IIS o en el SSL Relay. |
| StoreFront o la interfaz web de la segunda DMZ se conectan al STA alojado en un servidor de la red interna. | La administración de certificados para esta conexión es la misma que la conexión de la interfaz web al servicio XML. Puede utilizar los mismos certificados para cifrar esta conexión. (El certificado de servidor debe residir en el servidor Microsoft IIS o en el SSL Relay. Debe instalarse un certificado raíz correspondiente en la interfaz web.) |
| NetScaler Gateway en la segunda DMZ se conecta al STA alojado en un servidor de la red interna. | La administración de certificados de servidor SSL para STA en esta conexión es la misma que la descrita para las dos conexiones anteriores descritas en esta tabla. (El certificado de servidor debe residir en el servidor Microsoft IIS o en el SSL Relay). NetScaler Gateway en la segunda DMZ debe tener instalado un certificado raíz firmado por la misma CA que el certificado de servidor utilizado por el servicio STA y XML. |
| NetScaler Gateway en la segunda DMZ establece una conexión ICA con una aplicación publicada en un servidor de la red interna. | Se debe instalar un certificado de servidor SSL dentro del relé SSL en el servidor que aloja la aplicación publicada. El proxy de NetScaler Gateway de la segunda DMZ debe tener instalado un certificado raíz firmado por la misma entidad emisora de certificados que el certificado de servidor instalado en la retransmisión SSL. |

# Usar la alta disponibilidad

January 26, 2024

Una implementación de alta disponibilidad de dos dispositivos NetScaler Gateway puede proporcionar un funcionamiento ininterrumpido en cualquier transacción. Al configurar un dispositivo como nodo principal y el otro como nodo secundario, el nodo principal acepta conexiones y administra los servidores, mientras que el nodo secundario supervisa el principal. Si, por cualquier motivo, el nodo principal no puede aceptar conexiones, el nodo secundario asume el control.

El nodo secundario supervisa el principal mediante el envío de mensajes periódicos (a menudo denominados mensajes de latidos o comprobaciones de estado) para determinar si el nodo principal acepta conexiones. Si se produce un error en una comprobación de estado, el nodo secundario vuelve a intentar la conexión durante un período especificado, tras el cual determina que el nodo principal no funciona con normalidad. A continuación, el nodo secundario asume el control del principal (un proceso denominado conmutación por error).

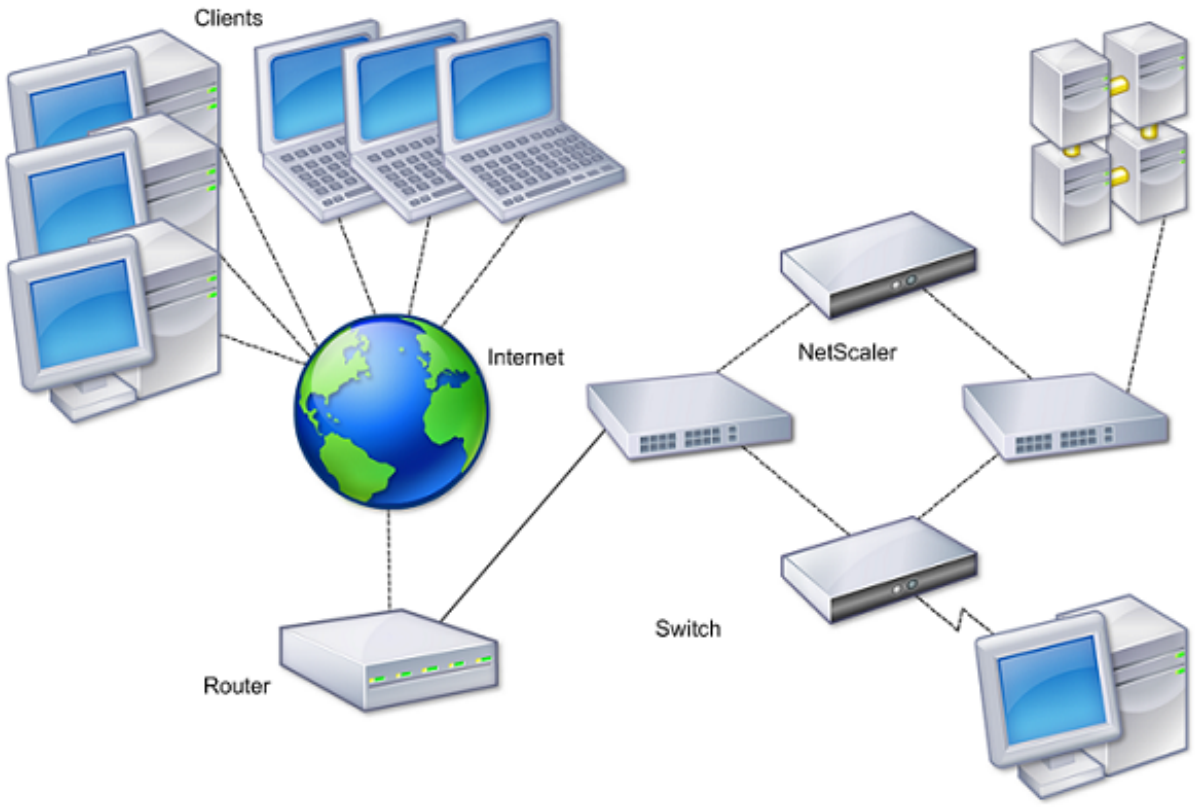
Tras una conmutación por error, todos los clientes deben restablecer sus conexiones con los servidores administrados, pero las reglas de persistencia de sesiones se mantienen como antes de la conmutación por error.

Con la persistencia de registro del servidor web habilitada, no se pierden datos de registro debido a la conmutación por error. Para habilitar la persistencia de registros, la configuración del servidor de registros debe incluir entradas para ambos sistemas en el archivo log.conf.

En la siguiente ilustración se muestra una configuración de red con un par de alta disponibilidad.

Figura 1. Dispositivos NetScaler Gateway en una configuración de alta disponibilidad




Los pasos básicos para configurar la alta disponibilidad son los siguientes:

1. Cree una configuración básica, con ambos nodos en la misma subred.
2. Personalice los intervalos en los que los nodos comunican información de comprobación de estado.
3. Personalice el proceso mediante el cual los nodos mantienen la sincronización.
4. Personaliza la propagación de comandos del principal al secundario.
5. De forma opcional, configure el modo a prueba de fallos para evitar una situación en la que ninguno de los nodos sea principal.
6. Configure direcciones MAC virtuales si su entorno incluye dispositivos que no aceptan mensajes ARP gratuitos de NetScaler Gateway.

Cuando esté preparado para una configuración más compleja, puede configurar nodos de alta disponibilidad en distintas subredes.

Para mejorar la fiabilidad de su configuración de alta disponibilidad, puede configurar monitores de rutas y crear enlaces redundantes. En algunas situaciones, como cuando se solucionan problemas o se realizan tareas de mantenimiento, es posible que quiera forzar la conmutación por error de un nodo (asignar el estado principal al otro nodo), o forzar que el nodo secundario permanezca secundario o que el nodo principal permanezca como principal.

# Cómo funciona la alta disponibilidad

January 26, 2024

Al configurar NetScaler Gateway en un par de alta disponibilidad, el NetScaler Gateway secundario supervisa el primer dispositivo mediante el envío de mensajes periódicos, también denominados mensaje de latido o comprobación de estado, para determinar si el primer dispositivo acepta conexiones. Si se produce un error en la comprobación de estado, el NetScaler Gateway secundario vuelve a intentar la conexión durante un período de tiempo especificado hasta que determina que el dispositivo principal no funciona. Si el dispositivo secundario confirma el error de comprobación de estado, el NetScaler Gateway secundario se hace cargo del NetScaler Gateway principal. Esto se denomina conmutación por error.

Los siguientes puertos se utilizan para intercambiar información relacionada con la alta disponibilidad entre dispositivos NetScaler Gateway:

- El puerto UDP 3003 se utiliza para intercambiar paquetes de saludo para comunicar el estado de los intervalos.
- El puerto TCP 3010 se utiliza para la sincronización de la configuración de alta disponibilidad.
- El puerto TCP 3011 se utiliza para sincronizar los valores de configuración.

## Directrices para configurar la alta disponibilidad

Antes de configurar un par de alta disponibilidad, debe revisar estas directrices:

- Cada dispositivo NetScaler Gateway debe ejecutar la misma versión del software NetScaler Gateway. Encontrará el número de versión en la parte superior de la página de la utilidad de configuración.
- NetScaler Gateway no sincroniza automáticamente contraseñas entre dos dispositivos. Puede configurar cada NetScaler Gateway con el nombre de usuario y la contraseña del otro dispositivo del par.
- Las entradas del archivo de configuración, ns.conf, tanto en el NetScaler Gateway principal como en el secundario deben coincidir, con las siguientes excepciones:
  - El dispositivo NetScaler Gateway principal y secundario deben configurarse con su propia dirección IP exclusiva del sistema. Utilice el Asistente de configuración para configurar o modificar la dirección IP del sistema en NetScaler Gateway.
  - En un par de alta disponibilidad, el ID de NetScaler Gateway y la dirección IP asociada deben apuntar al otro NetScaler Gateway.

Por ejemplo, si tiene dos dispositivos, denominados AG1 y AG2, debe configurar AG1 con el ID y la dirección IP exclusivos de NetScaler Gateway de AG2. Debe configurar AG2 con el ID y la dirección IP exclusivos de NetScaler Gateway de AG1.

Nota: Cada dispositivo Citrix Gateway siempre se identifica como nodo 0. Configure cada dispositivo con un ID de nodo único.

- Cada dispositivo del par de alta disponibilidad debe tener la misma licencia. Para obtener más información sobre las licencias, consulte Licencias.
- Si crea un archivo de configuración en cualquiera de los nodos mediante un método que no pasa directamente por la utilidad de configuración o la interfaz de línea de comandos (por ejemplo, importar certificados SSL o cambiar a los scripts de inicio), debe copiar el archivo de configuración en el otro nodo o crear un archivo idéntico en ese nodo.
- Al configurar un par de alta disponibilidad, asegúrese de que las direcciones IP asignadas y la dirección de puerta de enlace predeterminada del dispositivo principal y del dispositivo secundario sean idénticas. Si es necesario, puede cambiar la dirección IP asignada en cualquier momento ejecutando el Asistente de configuración.

Puede usar la lista de verificación previa a la instalación para ver una lista de los ajustes específicos que necesita configurar en una implementación de alta disponibilidad. Para obtener más información, consulte Lista de verificación previa a la instalación.

## Configuración de los ajustes de alta disponibilidad

January 26, 2024

Para configurar una configuración de alta disponibilidad, debe crear dos nodos, cada uno de los cuales define la dirección IP de NetScaler Gateway del otro como nodo remoto. Para empezar, inicie sesión en uno de los dos dispositivos NetScaler ADC que quiera configurar para obtener alta disponibilidad y agregar un nodo. Especifique la dirección IP de NetScaler Gateway del otro dispositivo como dirección del nuevo nodo. A continuación, inicie sesión en el otro dispositivo y agregue un nodo que tenga la dirección IP de NetScaler Gateway del primer dispositivo. Un algoritmo determina qué nodo pasa a ser primario y cuál se convierte en secundario.

Antes de configurar los dispositivos, agregue un nodo de alta disponibilidad. Este nodo representa el primer o el segundo NetScaler Gateway del par de alta disponibilidad. Para configurar la alta disponibilidad, primero debe crear el nodo y, a continuación, configurar la configuración de alta disponibilidad.

### Para agregar un nodo de alta disponibilidad

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, haga clic en Agregar.
3. En el cuadro de diálogo Configuración de alta disponibilidad, en el cuadro de diálogo Configuración de alta disponibilidad, en el cuadro de texto Dirección IP del nodo remoto, escriba la dirección NSIP del Citrix ADC que se va a agregar como nodo remoto. Si la dirección IP de NetScaler Gateway es una dirección IPv6, active la casilla de verificación IPv6 antes de introducir la dirección.
4. Si quiere agregar el nodo local al nodo remoto automáticamente, seleccione Configurar sistema remoto para participar en la configuración de alta disponibilidad. Si no selecciona esta opción, debe iniciar sesión en el dispositivo representado por el nodo remoto y agregar el nodo que está configurando actualmente.
5. Haga clic para habilitar Desactivar el monitor HA en las interfaces/canales que están inactivos.
6. Si el dispositivo remoto tiene un nombre de usuario y una contraseña diferentes, en Credenciales de inicio de sesión del sistema remoto, haga clic en Las credenciales de inicio de sesión del sistema remoto son diferentes de las del nodo propio.
7. En Nombre de usuario, escriba el nombre de usuario del dispositivo remoto.
8. En Contraseña, escriba la contraseña del dispositivo remoto.
9. Haga clic en Aceptar.

### Para habilitar o inhabilitar el nodo secundario

Solo puede inhabilitar o habilitar el nodo secundario. Cuando inhabilita un nodo secundario, deja de enviar mensajes de latido al nodo principal y, por lo tanto, el nodo principal ya no puede comprobar el estado del nodo secundario. Al habilitar un nodo, el nodo forma parte de la configuración de alta disponibilidad.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione el nodo local y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configuración de nodo de HA, en Estado de alta disponibilidad, seleccione ACTIVADO (No participar en HA).
4. Haga clic en Aceptar. Aparece un mensaje en la barra de estado que indica que el nodo se ha configurado correctamente.

### Para configurar los ajustes de alta disponibilidad

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.
3. En el cuadro de diálogo Configuración de nodo de alta disponibilidad, en ID, escriba el número del identificador de nodo. ID especifica el número de nodo exclusivo del otro dispositivo.
4. En Dirección IP, escriba la dirección IP del sistema y, a continuación, haga clic en Aceptar. La dirección IP especifica la dirección IP del otro dispositivo.

Nota: El identificador máximo para los nodos de un par de alta disponibilidad es 64.

## Cambio de la contraseña de un nodo RPC

January 26, 2024

Para comunicarse con otros dispositivos NetScaler Gateway, cada dispositivo requiere conocer los demás dispositivos, incluido cómo autenticarse en NetScaler Gateway. Los nodos RPC son entidades internas del sistema utilizadas para la comunicación de información de configuración y sesión de sistema a sistema. Existe un nodo RPC en cada NetScaler Gateway y almacena información, como las direcciones IP del otro dispositivo NetScaler Gateway y las contraseñas utilizadas para la autenticación. El NetScaler Gateway que establece contacto con otro NetScaler Gateway comprueba la contraseña dentro del nodo RPC.

NetScaler Gateway requiere contraseñas de nodo RPC en ambos dispositivos en un par de alta disponibilidad. Inicialmente, cada NetScaler Gateway se configura con la misma contraseña de nodo RPC. Para mejorar la seguridad, debe cambiar las contraseñas predeterminadas de los nodos RPC. La utilidad de configuración se usa para configurar y cambiar los nodos RPC.

Los nodos RPC se crean implícitamente al agregar un nodo o agregar un sitio de equilibrio de carga de servidor global (GSLB). No se pueden crear ni eliminar nodos RPC manualmente.

**Importante:** También debe proteger la conexión de red entre los dispositivos. Puede configurar la seguridad al configurar la contraseña del nodo RPC seleccionando la casilla de verificación **Proteger**.

### Para cambiar la contraseña de un nodo RPC y habilitar una conexión segura

1. Vaya a **Sistema > Red > RPC.**
2. En el panel de detalles, seleccione el nodo y, a continuación, haga clic en **Modificar**.

3. En **Contraseña** y **Confirmar contraseña**, escriba la nueva contraseña.
4. En **Dirección IP de origen**, escriba la dirección IP del sistema del otro dispositivo NetScaler Gateway.
5. Haga clic en **Seguro** y, a continuación, en **Aceptar**

## Configuración de los dispositivos primarios y secundarios para obtener alta disponibilidad

January 26, 2024

Después de cambiar la contraseña del nodo RPC y habilitar la comunicación segura, utilice la utilidad de configuración para configurar los nodos de alta disponibilidad de NetScaler Gateway principal y secundario.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.
3. En Estado de alta disponibilidad, haga clic en Habilitado (participar activamente en HA) y, a continuación, haga clic en Aceptar.

## Configuración de intervalos de comunicación

January 26, 2024

Al configurar NetScaler Gateway como un par de alta disponibilidad, puede configurar el NetScaler Gateway secundario para que escuche a intervalos específicos, medidos en milisegundos (mseg). Estos intervalos se conocen como intervalos de saludo e intervalos muertos.

El intervalo de saludo es el intervalo en el que se envían los mensajes de latidos al nodo del mismo nivel. El intervalo muerto es el intervalo de tiempo tras el cual el nodo del par se marca como DOWN si no se reciben paquetes de latidos. Los mensajes de latido son paquetes UDP enviados al puerto 3003 del otro nodo en un par de alta disponibilidad.

Cuando configuras el intervalo de saludo, puede usar los valores 200 a 1000. El valor por defecto es 200. Los valores de intervalo muerto son de 3 a 60. El valor por defecto es 3.

> **Nota**
>
> El intervalo muerto debe establecerse como múltiplo del intervalo de saludo.

### Para configurar los intervalos de comunicación para el NetScaler Gateway secundario

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.
3. En Intervalos, realice una o ambas de las acciones siguientes:
    - En Intervalo de saludo (msec), escriba el valor y, a continuación, haga clic en Aceptar. El valor predeterminado es 200 milisegundos.
    - En Intervalo muerto (segundos), escriba el valor y, a continuación, haga clic en Aceptar. El valor predeterminado es de tres segundos.

## Sincronizar dispositivos NetScaler Gateway

January 26, 2024

La sincronización automática de los dispositivos NetScaler Gateway en un par de alta disponibilidad está habilitada de forma predeterminada. Con la sincronización automática, puede realizar cambios en un dispositivo y permitir que los cambios se propaguen automáticamente al segundo dispositivo. La sincronización utiliza el puerto 3010.

La sincronización se inicia cuando ocurre lo siguiente:

- El nodo secundario se reinicia.
- El nodo principal pasa a ser secundario tras una conmutación por error.

Puede inhabilitar la sincronización, lo que impide que NetScaler Gateway secundario sincronice su configuración con la puerta de enlace principal cuando se produce un cambio en el dispositivo principal. También puede forzar la sincronización.

Habilita o inhabilita la sincronización de alta disponibilidad en el nodo secundario del par.

### Para habilitar o inhabilitar la sincronización de alta disponibilidad

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.

2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.
3. En el cuadro de diálogo Configurar nodo, en Sincronización de alta disponibilidad, realice una de las siguientes acciones:
    - Para inhabilitar la sincronización, desactive la casilla de verificación El nodo secundario buscará la configuración de Principal.
    - Para habilitar la sincronización, seleccione la casilla de verificación Nodo secundario obtendrá la configuración del nodo principal.
4. Haga clic en Aceptar. Aparece un mensaje en la barra de estado que indica que la configuración del nodo se ha realizado correctamente.

### Para forzar la sincronización entre dispositivos

Además de la sincronización automática, NetScaler Gateway admite la sincronización forzada entre los dos nodos en un par de alta disponibilidad.

Puede forzar la sincronización en los dispositivos NetScaler Gateway principal y secundario. Sin embargo, si la sincronización ya está en curso, el comando falla y NetScaler Gateway muestra una advertencia. La sincronización forzada también falla en las siguientes circunstancias:

- La sincronización se fuerza en un sistema independiente.
- El nodo secundario está inhabilitado.
- Inhabilitar la sincronización de alta disponibilidad en el nodo secundario.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En la ficha Nodos, haga clic en Forzar sincronización.

## Sincronización de archivos de configuración en una configuración de alta disponibilidad

January 26, 2024

En una configuración de alta disponibilidad, puede sincronizar varios archivos de configuración del nodo principal al nodo secundario.

### Parámetros para sincronizar archivos en una configuración de alta disponibilidad

- Modo

  Tipo de sincronización que se va a realizar. Las descripciones siguientes incluyen, entre paréntesis, el argumento de línea de comandos que especifica la opción.

  - **Todo excepto licencias y rc.conf** (todo). Sincroniza archivos relacionados con la configuración del sistema, marcadores de NetScaler Gateway, certificados SSL, listas de CRL SSL, scripts de inyección HTML y objetos XML de Application Firewall.
  - **Marcadores** (marcadores). Sincroniza todos los marcadores de NetScaler Gateway.
  - **Certificados y claves**SSL (ssl). Sincroniza todos los certificados, claves y CRL de la función SSL.
  - **Licencias y rc.conf** (misc). Sincroniza todos los archivos de licencia y el archivo rc.conf.
  - **Todo, incluidas las licencias y rc.conf** (all_plus_misc). Sincroniza archivos relacionados con la configuración del sistema, marcadores de NetScaler Gateway, certificados SSL, listas de CRL SSL, scripts de inyección HTML, objetos XML de Application Firewall, licencias y el archivo rc.conf.

Nota: Hay más opciones disponibles si instala una licencia NetScaler ADC en el dispositivo.

### Para sincronizar archivos en una configuración de alta disponibilidad mediante la utilidad de configuración

1. En el panel de navegación, expanda Sistema y, a continuación, haga clic en Diagnóstico.
2. En el panel de detalles, en Utilidades, haga clic en Iniciar sincronización de archivos HA.
3. En el cuadro de diálogo Iniciar sincronización de archivos, en la lista desplegable Modo, seleccione el tipo de sincronización adecuado (por ejemplo, Todo excepto licencias y rc.conf) y, a continuación, haga clic en Aceptar.

## Configuración de la propagación de comandos

January 26, 2024

En una configuración de alta disponibilidad, cualquier comando emitido en el nodo principal se propaga automáticamente al nodo secundario y se ejecuta en él antes de que se ejecute el comando en el nodo principal. Si la propagación del comando falla o si la ejecución del comando falla en el nodo secundario, el nodo principal ejecuta el comando y registra un error. La propagación de comandos utiliza el puerto 3011.

En una configuración de pares de alta disponibilidad, la propagación de comandos está habilitada de forma predeterminada tanto en el nodo principal como en el secundario. Puede habilitar o inhabilitar la propagación de comandos en cualquiera de los nodos en un par de alta disponibilidad. Si inhabilita la propagación de comandos en el nodo principal, los comandos no se propagan al nodo secundario. Si inhabilita la propagación de comandos en el nodo secundario, los comandos propagados desde el primario no se ejecutan en el nodo secundario.

Nota: Después de volver a habilitar la propagación, recuerde forzar la sincronización.

Nota: Si se produce la sincronización mientras se inhabilita la propagación, los cambios relacionados con la configuración que se realicen antes de que surta efecto la desactivación de la propagación se sincronizarán con el nodo secundario. Esto también es cierto para los casos en los que la propagación está inhabilitada mientras la sincronización está en curso.

### Para habilitar o inhabilitar la propagación en el nodo principal

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.
3. En Propagación HA, realice una de las siguientes acciones:
    - Para inhabilitar la propagación de alta disponibilidad, desactive la casilla de verificación El nodo principal propagará la configuración a la casilla Secundaria.
    - Para habilitar la propagación de alta disponibilidad, seleccione la casilla de verificación El nodo principal propagará la configuración a la secundaria.
4. Haga clic en Aceptar.

## Solución de problemas de propagación de comandos

January 26, 2024

En la lista siguiente se describen los motivos por los que puede fallar la propagación de comandos y las soluciones para restaurar la configuración:

- La conectividad de red no está activa. Si se produce un error en la propagación de un comando, compruebe la conexión de red entre los dispositivos NetScaler Gateway principal y secundario.
- Faltan recursos en NetScaler Gateway secundario. Si la ejecución de un comando se ejecuta correctamente en el NetScaler Gateway principal pero no se propaga al NetScaler Gateway secundario, ejecute el comando directamente en el NetScaler Gateway secundario para ver el

mensaje de error. Es posible que el error se haya producido porque los recursos requeridos por el comando están presentes en el NetScaler Gateway principal y no están disponibles en el NetScaler Gateway secundario. Además, compruebe que los archivos de licencia de cada dispositivo coinciden.

Por ejemplo, compruebe que todos los certificados de Secure Sockets Layer (SSL) estén presentes en cada NetScaler Gateway. Compruebe que exista cualquier personalización del script de inicialización en ambos dispositivos NetScaler Gateway.

- Error de autenticación. Si recibe un mensaje de error de error de autenticación, compruebe la configuración del nodo RPC de cada dispositivo.

## Configurar el modo a prueba de fallos

January 26, 2024

En una configuración de alta disponibilidad, el modo a prueba de fallos garantiza que un nodo sea siempre principal cuando ambos nodos no superen la comprobación de estado. El modo a prueba de fallos garantiza que cuando un nodo solo está disponible parcialmente, los métodos de copia de seguridad se pueden activar y manejar el tráfico.

El modo a prueba de fallos de alta disponibilidad se configura de forma independiente en cada nodo.

En la tabla siguiente se muestran algunos de los casos a prueba de fallos. El estado NOT_UP significa que el nodo no ha superado la comprobación de estado y, sin embargo, el nodo está parcialmente disponible. El estado UP significa que el nodo ha superado la comprobación de estado.

Tabla 1. Fundas de modo a prueba de fallos

| Estado de salud del nodo A (primario) | Estado de salud del nodo B (secundario) | Comportamiento de alta disponibilidad predeterminado | Comportamiento de alta disponibilidad habilitado a prueba de errores | Descripción |
|---|---|---|---|---|
| NOT_UP (último error) | NOT_UP (error primero) | A (secundaria), B (secundaria) | A (primaria), B (secundaria) | Si ambos nodos fallan, uno tras otro, el nodo que fue el último nodo principal sigue siendo el principal. |
| NOT_UP (error primero) | NOT_UP (último error) | A (secundaria), B (secundaria) | A (secundaria), B (primaria) | Si ambos nodos fallan, uno tras otro, el nodo que fue el último nodo principal sigue siendo el principal. |
| UP | UP | A (primaria), B (secundaria) | A (primaria), B (secundaria) | Si ambos nodos pasan la comprobación de estado, no hay cambios en el comportamiento con la seguridad contra fallos habilitada. |
| UP | NOT_UP | A (primaria), B (secundaria) | A (primaria), B (secundaria) | Si solo falla el nodo secundario, no hay cambios en el comportamiento con la opción a prueba de fallos habilitada. |

| Estado de salud del nodo A (primario) | Estado de salud del nodo B (secundario) | Comportamiento de alta disponibilidad predeterminado | Comportamiento de alta disponibilidad habilitado a prueba de errores | Descripción |
|---|---|---|---|---|
| NOT_UP | UP | A (secundaria), B (primaria) | A (secundaria), B (primaria) | Si solo falla el primario, no hay cambios en el comportamiento con la seguridad habilitada. |
| NOT_UP | UP (STAYSEC-ONDARY) | A (secundaria), B (secundaria) | A (primaria), B (secundaria) | Si el secundario está configurado como STAYSECONDARY, el primario sigue siendo primario aunque falle. |

**Para configurar el modo a prueba de fallos**

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.
3. En el cuadro de diálogo Configurar nodo, en Modo a prueba de fallos, seleccione Mantener un nodo principal aunque ambos nodos no estén en buen estado y, a continuación, haga clic en Aceptar.

## Configuración de la dirección MAC virtual

January 26, 2024

La dirección MAC virtual la comparten los dispositivos NetScaler Gateway principal y secundario en una configuración de alta disponibilidad.

En una configuración de alta disponibilidad, el NetScaler Gateway principal posee todas las direcciones IP flotantes, como la dirección IP asignada o la dirección IP virtual. Responde a las solicitudes

de protocolo de resolución de direcciones (ARP) de estas direcciones IP con su propia dirección MAC. Como resultado, la tabla ARP de un dispositivo externo (como un router) se actualiza con la dirección IP flotante y la dirección MAC principal de NetScaler Gateway. Cuando se produce una conmutación por error, el NetScaler Gateway secundario se hace cargo del nuevo NetScaler Gateway principal. A continuación, utiliza el protocolo de resolución de direcciones gratuito (GARP) para anunciar las direcciones IP flotantes que adquirió del dispositivo principal. La dirección MAC, que anuncia el nuevo dispositivo principal, es la de su propia interfaz.

Algunos dispositivos no aceptan mensajes GARP generados por NetScaler Gateway. Como resultado, algunos de los dispositivos externos conservan la antigua asignación de IP a Mac anunciada por el antiguo NetScaler Gateway principal. Esta situación puede provocar que un sitio no esté disponible. Para resolver el problema, configure una dirección MAC virtual en ambos dispositivos NetScaler Gateway de un par de alta disponibilidad. Esta configuración implica que ambos dispositivos NetScaler Gateway tienen direcciones MAC idénticas. Como resultado, cuando se produce una conmutación por error, la dirección MAC del NetScaler Gateway secundario permanece sin cambios y no es necesario actualizar las tablas ARP de los dispositivos externos.

Para crear una dirección MAC virtual, cree un identificador de enrutador virtual (ID) y vincúlelo a una interfaz. En una configuración de alta disponibilidad, el usuario debe enlazar el ID a las interfaces de ambos dispositivos.

Cuando el ID del router virtual está enlazado a una interfaz, el sistema genera una dirección MAC virtual con el ID del router virtual como último octeto. Un ejemplo de la dirección MAC virtual genérica es 00:00:5 e: 00:01:\ <VRID\ >. Por ejemplo, si ha creado un ID de enrutador virtual con el valor 60 y lo vincula a una interfaz, la dirección MAC virtual resultante es 00:00:5 e: 00:01:3 c, donde 3c es la representación hexadecimal del ID del router virtual. Puede crear 255 ID de enrutador virtual que van del 1 al 254.

Puede configurar direcciones MAC virtuales para IPv4 e IPv6.

## Configurar direcciones MAC virtuales IPv4

January 26, 2024

Cuando crea una dirección MAC virtual IPv4 y la vincula a una interfaz, cualquier paquete IPv4 enviado desde la interfaz utiliza la dirección MAC virtual enlazada a la interfaz. Si no hay ninguna dirección MAC virtual IPv4 enlazada a una interfaz, se utiliza la dirección MAC física de la interfaz.

La dirección MAC virtual genérica tiene el formato 00:00:5 e: 00:01:\ <VRID\ >. Por ejemplo, si crea un VRID con un valor de 60 y lo vincula a una interfaz, la dirección MAC virtual resultante es 00:00:5 e: 00:01:3 c, donde 3c es la representación hexadecimal del VRID. Puede crear 255 VRID con valores del 1 al 255.

# Creación o modificación de una dirección MAC virtual IPv4

January 26, 2024

Cree una dirección MAC virtual IPv4 asignándole un ID de enrutador virtual. A continuación, puede enlazar la dirección MAC virtual a una interfaz. No se pueden enlazar varios ID de enrutador virtual a la misma interfaz. Para verificar la configuración de la dirección MAC virtual, debe mostrar y examinar la dirección MAC virtual y las interfaces enlazadas a la dirección MAC virtual.

## Parámetros para configurar una dirección MAC virtual

- vRID

  ID del router virtual que identifica la dirección MAC virtual. Valores posibles: De 1 a 255.

- infón

  El número de interfaz (notación de ranura/puerto) que se va a enlazar a la dirección MAC virtual.

## Para configurar una dirección MAC virtual

1. En la utilidad de configuración, en la ficha Configuración, expanda Sistema > Red y, a continuación, haga clic en VMAC.
2. En el panel de detalles, en la ficha VMAC, haga clic en Agregar.
3. En el cuadro de diálogo Crear VMAC, en ID de enrutador virtual, escriba el valor.
4. En Interfaces asociadas, en Interfaces disponibles, seleccione una interfaz de red, haga clic en Agregar, en Crear y, a continuación, en Cerrar.

Después de crear la dirección MAC virtual, aparece en la utilidad de configuración. Si ha seleccionado una interfaz de red, el ID del router virtual está enlazado a esa interfaz.

## Para eliminar una dirección MAC virtual

Para eliminar una dirección MAC virtual, debe eliminar el ID del router virtual correspondiente.

1. En la utilidad de configuración, en la ficha Configuración, expanda Sistema > Red y, a continuación, haga clic en VMAC.
2. En el panel de detalles, seleccione un elemento y, a continuación, haga clic en Quitar.

### Para enlazar y desvincular una dirección MAC virtual

Al crear el ID del enrutador virtual, seleccionó una interfaz de red en NetScaler Gateway y, a continuación, enlazó el ID del router virtual a la interfaz de red. También puede desvincular una dirección MAC virtual de la interfaz de red, pero dejar la dirección MAC configurada en NetScaler Gateway.

1. En la utilidad de configuración, en la ficha Configuración, expanda Sistema > Red y, a continuación, haga clic en VMAC.
2. En el panel de detalles, seleccione un elemento y, a continuación, haga clic en Abrir.
3. En Interfaces configuradas, seleccione una interfaz de red, haga clic en Eliminar, en Aceptar y, a continuación, en Cerrar.

## Configurar direcciones MAC virtuales IPv6

January 26, 2024

NetScaler Gateway admite direcciones MAC virtuales para paquetes IPv6. Puede enlazar cualquier interfaz a una dirección MAC virtual para IPv6, incluso si una dirección MAC virtual IPv4 está enlazada a la interfaz. Cualquier paquete IPv6 enviado desde la interfaz utiliza la dirección MAC virtual enlazada a esa interfaz. Si no hay una dirección MAC virtual enlazada a una interfaz, un paquete IPv6 utiliza la MAC física.

## Creación o modificación de una dirección MAC virtual para IPv6

January 26, 2024

Para crear una dirección MAC virtual IPv6, se le asigna un ID de enrutador virtual IPv6. A continuación, puede enlazar la dirección MAC virtual a una interfaz. No se pueden enlazar varios ID de enrutador virtual IPv6 a una interfaz. Para verificar la configuración de la dirección MAC virtual, debe mostrar y examinar las direcciones MAC virtuales y las interfaces enlazadas a la dirección MAC virtual.

### Parámetros para configurar una dirección MAC virtual para IPv6

- ID de enrutador virtual

  ID del router virtual que identifica la dirección MAC virtual. Valores posibles: De 1 a 255.

- infón

  El número de interfaz (notación de ranura/puerto) que se va a enlazar a la dirección MAC virtual.

### Para configurar una dirección MAC virtual para IPv6

1. En la utilidad de configuración, en la ficha Configuración, expanda Sistema > Red y, a continuación, haga clic en VMAC.
2. En el panel de detalles, en la ficha VMAC6, realice una de las siguientes acciones:
   - Para crear una nueva dirección MAC virtual, haga clic en Agregar.
   - Para modificar una dirección MAC virtual existente, haga clic en Abrir.
3. En el cuadro de diálogo Crear VMAC6 o Configurar VMAC6, en ID de enrutador virtual, introduzca el valor, como vRID6.
4. En Interfaces asociadas, haga clic en Agregar, en Crear y, a continuación, en Cerrar. Aparece un mensaje en la barra de estado que indica que la dirección MAC virtual está configurada.

### Para quitar una dirección MAC virtual para IPv6

1. En la utilidad de configuración, en la ficha Configuración, expanda Sistema > Red y, a continuación, haga clic en VMAC.
2. En el panel de detalles, en la ficha VMAC6, seleccione el ID del router virtual que quiere quitar y, a continuación, haga clic en Quitar. Aparece un mensaje en la barra de estado que indica que se ha eliminado la dirección MAC virtual.

## Configuración de pares de alta disponibilidad en distintas subredes

January 26, 2024

Una implementación típica de alta disponibilidad es cuando ambos dispositivos de un par de alta disponibilidad residen en la misma subred. Una implementación de alta disponibilidad también puede consistir en dos dispositivos NetScaler Gateway en los que cada dispositivo se encuentra en una red diferente. En este tema se describe esta última configuración e incluye configuraciones de ejemplo y una lista de diferencias entre las configuraciones de alta disponibilidad dentro de una red y entre redes.

También puede configurar la redundancia de enlaces y los monitores de ruta. Estas funciones de NetScaler Gateway resultan útiles en una configuración de alta disponibilidad entre redes. Las funciones también cubren el proceso de comprobación de estado utilizado por cada NetScaler Gateway para garantizar que el dispositivo asociado esté activo.

### Cómo funciona la configuración de red independiente

Los dispositivos NetScaler Gateway están conectados a distintos routers, denominados R3 y R4, en dos redes diferentes. Los dispositivos intercambian paquetes de latidos a través de estos routers. Un paquete de latidos es una señal que se produce a intervalos regulares que garantiza que la conexión siga activa. Puede ampliar esta configuración para dar cabida a implementaciones que impliquen cualquier número de interfaces.

Nota: Si utiliza redirección estática en su red, debe agregar rutas estáticas entre todos los sistemas para asegurarse de que los paquetes de latidos se envían y reciben correctamente. (Si utiliza redirección dinámica en sus sistemas, las rutas estáticas son innecesarias).

Cuando los dispositivos de un par de alta disponibilidad residen en dos redes distintas, el NetScaler Gateway secundario debe tener una configuración de red independiente. Esto significa que los dispositivos NetScaler Gateway de distintas redes no pueden compartir direcciones IP asignadas, LAN virtuales ni rutas de red. Este tipo de configuración, en la que los dispositivos NetScaler Gateway de un par de alta disponibilidad tienen parámetros configurables diferentes, se conoce como configuración de red independiente o configuración de red simétrica.

En la tabla siguiente se resumen los parámetros configurables de una configuración de red independiente y se muestra cómo debe configurarlos en cada NetScaler Gateway:

| Parámetros configurables | Comportamiento |
|---|---|
| Direcciones IP | Específico de NetScaler Gateway Activa solo en ese dispositivo. |
| Dirección IP virtual | flotante. |
| LAN virtual | Específico de NetScaler Gateway Activa solo en ese dispositivo. |
| Rutas | Específico de NetScaler Gateway Activa solo en ese dispositivo. Una ruta de equilibrio de carga de enlace (LLB) es flotante. |
| listas de control de acceso (ACL) | Flotante (común). Activo en ambos dispositivos. |
| Redirección dinámica | Específico de NetScaler Gateway Activa solo en ese dispositivo. El NetScaler Gateway secundario también debe ejecutar los protocolos de redirección e intercalar con los enrutadores ascendentes. |
| Modo L2 | Flotante (común). Activo en ambos dispositivos. |
| Modo L3 | Flotante (común). Activo en ambos dispositivos. |

| Parámetros configurables | Comportamiento |
| --- | --- |
| Traducción inversa de direcciones de red (NAT) | Específico de NetScaler Gateway Invertir NAT con una dirección IP virtual porque la dirección IP NAT es flotante. |

> **Nota:**
>
> IPSET en modo INC es compatible con direcciones IP públicas. Para obtener más información, consulte Diseño de referencia validado de IP front-end de NetScaler ADC High Availability with Azure Load Balancer.

## Agregar un nodo remoto

January 26, 2024

Cuando dos nodos de un par de alta disponibilidad residen en subredes distintas, cada nodo debe tener una configuración de red diferente. Por lo tanto, para configurar dos sistemas independientes para que funcionen como un par de alta disponibilidad, debe especificar el modo de cómputo de red independiente durante el proceso de configuración.

Cuando agrega un nodo de alta disponibilidad, debe inhabilitar el monitor de alta disponibilidad para cada interfaz que no esté conectada o que se esté usando para el tráfico.

### Para agregar un nodo remoto para el modo de cómputo de red independiente

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema > Alta disponibilidad**.
2. En el panel de detalles, haga clic en la ficha **Nodos** y, a continuación, haga clic en **Agregar**.
3. En el cuadro de diálogo Configuración de alta disponibilidad, en el cuadro de texto **Dirección IP del nodo remoto**, escriba la dirección IP de NetScaler Gateway del dispositivo que es el nodo remoto.

   Para utilizar una dirección IPv6, haga clic en la casilla de verificación **IPv6** antes de introducir la dirección IP.
4. Si quiere agregar el nodo local al nodo remoto automáticamente, seleccione Configurar sistema remoto para participar en la configuración de alta disponibilidad. Si no selecciona esta opción, debe iniciar sesión en el dispositivo representado por el nodo remoto y agregar el nodo que está configurando actualmente.

5. Haga clic para habilitar el monitor de alta disponibilidad claro en las interfaces/canales que están inactivos.
6. Haga clic para activar el modo Activar el modo INC (Configuración de red independiente) en modo automático.
7. Haga clic en **Aceptar**. La página **Nodos** muestra los nodos locales y remotos de la configuración de alta disponibilidad.

### Para quitar un nodo remoto

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema > Alta disponibilidad**.
2. En el panel de detalles, haga clic en la ficha **Nodos**.
3. Seleccione el nodo que quiere quitar, haga clic en Quitar y **, a continuación,** haga clic en **Sí**.

## Configuración de monitores de rutas

January 26, 2024

Puede usar los monitores de rutas para hacer que el estado de alta disponibilidad dependa de la tabla de enrutamiento interna, independientemente de que la tabla contenga rutas estáticas o aprendidas dinámicamente. En una configuración de alta disponibilidad, un monitor de rutas de cada nodo comprueba la tabla de enrutamiento interna para asegurarse de que siempre haya una entrada de ruta para llegar a una red en particular. Si la entrada de ruta no está presente, el estado del monitor de ruta cambia a DOWN.

Cuando un dispositivo NetScaler Gateway solo tiene rutas estáticas para llegar a una red y quiere crear un monitor de rutas para la red, debe habilitar las rutas estáticas supervisadas para las rutas estáticas. La ruta estática supervisada elimina las rutas estáticas inalcanzables de la tabla de redirección interna. Si inhabilita rutas estáticas supervisadas en rutas estáticas, una ruta estática inalcanzable puede permanecer en la tabla de redirección interno, lo que contradice el propósito de tener el monitor de ruta.

Los monitores de ruta son compatibles con la configuración de red independiente habilitada o inhabilitada. La tabla siguiente muestra lo que ocurre con los monitores de ruta en una configuración de alta disponibilidad y con Configuración de red independiente habilitada o inhabilitada.

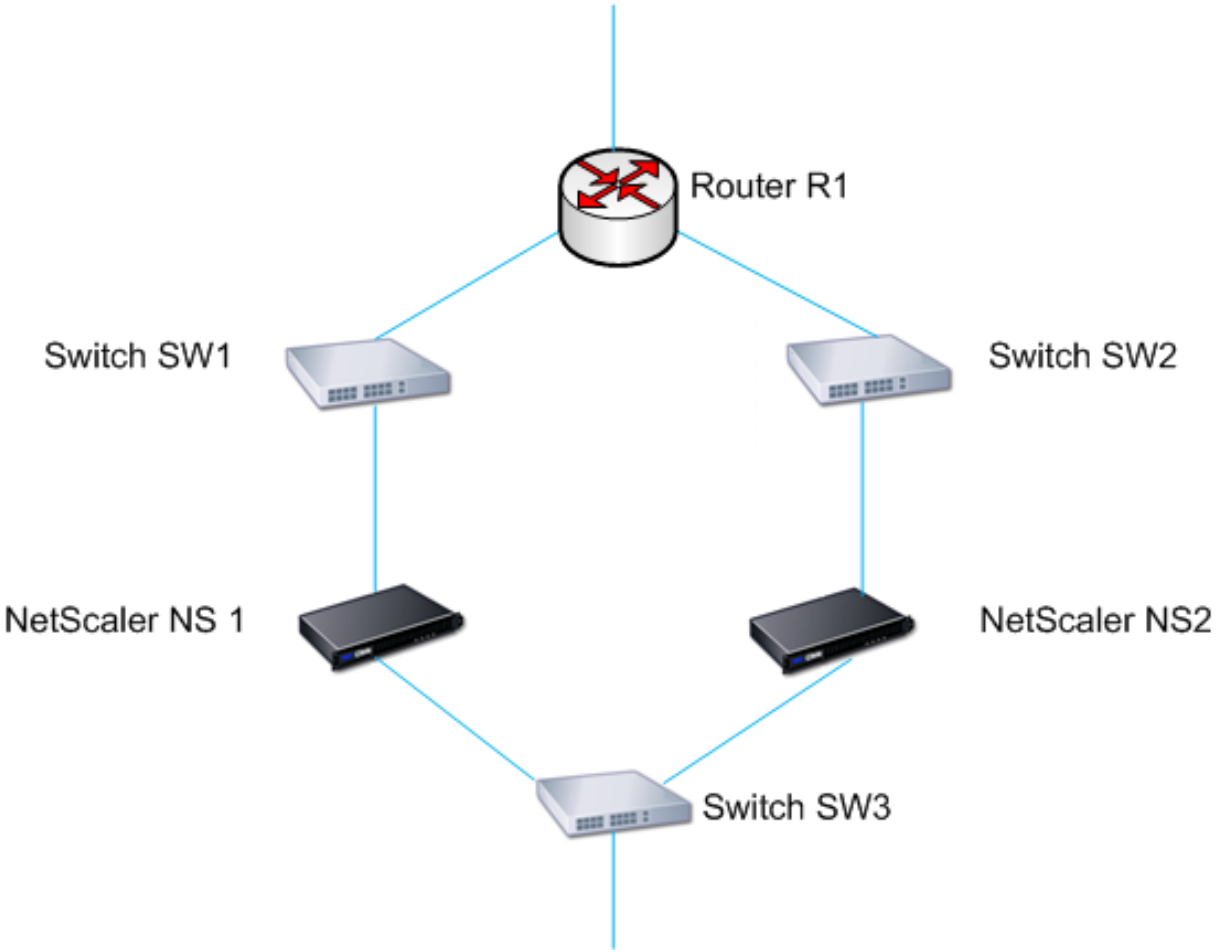
 

| Monitores de ruta en alta disponibilidad en el modo de configuración de red independiente inhabilitado | Monitores de ruta en alta disponibilidad en el modo Configuración de red independiente habilitado |
|---|---|
| Los monitores de ruta se propagan por nodos y se intercambian durante la sincronización. | Los monitores de ruta no se propagan por los nodos ni se intercambian durante la sincronización. |
| Los monitores de ruta solo están activos en el nodo principal actual. | Los monitores de ruta están activos tanto en el nodo principal como en el secundario. |
| El dispositivo Citrix Gateway siempre muestra el estado de un monitor de rutas como activo, independientemente de si la entrada de ruta está presente o no en la tabla de enrutamiento interna. | El dispositivo NetScaler Gateway muestra el estado del monitor de ruta como DOWN si la entrada de ruta correspondiente no está presente en la tabla de redirección interna. |
| Un monitor de rutas comienza a supervisar su ruta en los siguientes casos, para permitir que Citrix Gateway aprenda las rutas dinámicas, lo que puede tardar hasta 180 segundos: reinicio, conmutación por error, comando set route6 para rutas v6, comando set route msr enable/disable para rutas v4 y agregar un nuevo monitor de rutas | No aplicable. |

Los monitores de ruta son útiles cuando inhabilita el modo de configuración de red independiente y quiere que una puerta de enlace de un nodo principal sea inalcanzable como una de las condiciones para la conmutación por error de alta disponibilidad.

Por ejemplo, inhabilita la Configuración de red independiente en una configuración de alta disponibilidad en una topología de dos brazos que tiene dispositivos NetScaler Gateway NS1 y NS2 en la misma subred, con el enrutador R1 y los conmutadores SW1, SW2 y SW3, como se muestra en la siguiente ilustración. Dado que R1 es el único router de esta configuración, usted desea que la configuración de alta disponibilidad realice una conmutación por error siempre que no se pueda acceder a R1 desde el nodo principal actual. Puede configurar un monitor de ruta (por ejemplo, RM1 y RM2, respectivamente) en cada uno de los nodos para supervisar la accesibilidad de R1 desde ese nodo.




Con NS1 como nodo principal actual, el flujo de red es el siguiente:

1. El monitor de ruta RM1 en NS1 monitorea la tabla de redirección interno de NS1 para detectar la presencia de una entrada de ruta para el enrutador R1. NS1 y NS2 intercambian mensajes de latidos a través del switch SW1 o SW3 a intervalos regulares.
2. Si el conmutador SW1 falla, el protocolo de redirección de NS1 detecta que no se puede acceder a R1 y, por lo tanto, elimina la entrada de ruta para R1 de la tabla de redirección interna. NS1 y NS2 intercambian mensajes de latidos a través del switch SW3 a intervalos regulares.
3. Al detectar que la entrada de ruta para R1 no está presente en la tabla de redirección interno, RM1 inicia una conmutación por error. Si la ruta a R1 no funciona desde NS1 y NS2, la conmutación por error se produce cada 180 segundos hasta que uno de los dispositivos pueda llegar al R1 y restaurar la conexión.

## Agregar o quitar monitores de ruta

January 26, 2024

Cuando los dispositivos de un par de alta disponibilidad residen en redes diferentes, el estado de alta disponibilidad de NetScaler Gateway depende de si se puede acceder al dispositivo o no. En una configuración de alta disponibilidad entre redes, un monitor de ruta de cada NetScaler Gateway explora la tabla de redirección interna para asegurarse de que siempre haya una entrada para el otro NetScaler Gateway.

### Para agregar un monitor de ruta

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el cuadro de diálogo Enlazar/desenlazar monitores de ruta, en la ficha Supervisores de ruta, haga clic en Acción y, a continuación, en Configurar.
3. En Especificar monitor de ruta, en Red, escriba la dirección IP de la red del otro dispositivo NetScaler Gateway.

   Para configurar una dirección IPv6, haga clic en IPv6 y, a continuación, escriba la dirección IP.
4. En Máscara de red, escriba la máscara de subred de la otra red, haga clic en Agregar y, a continuación, haga clic en Aceptar.

Cuando se complete este procedimiento, el monitor de ruta se enlazará a NetScaler Gateway.

Nota: Cuando un monitor de ruta no está vinculado a un NetScaler Gateway, el estado de alta disponibilidad de cualquiera de los dispositivos viene determinado por el estado de las interfaces.

### Para quitar un monitor de ruta

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En la ficha Supervisores de ruta, haga clic en Acción y, a continuación, en Configurar.
3. En Monitores de ruta configurados, seleccione el monitor, haga clic en Eliminar y, a continuación, haga clic en Aceptar.

## Configuración de redundancia de enlaces

January 26, 2024

La redundancia de vínculos agrupa las interfaces de red para evitar la conmutación por error debido a un error en una interfaz de red de un NetScaler Gateway que tiene otras interfaces en funcionamiento.

El error de la primera interfaz del NetScaler Gateway principal desencadena la conmutación por error, aunque la primera interfaz puede seguir usando su segundo enlace para atender las solicitudes de los usuarios. Al configurar la redundancia de vínculos, puede agrupar las dos interfaces en un conjunto de interfaces de conmutación por error, lo que evita que el error de un solo enlace provoque la conmutación por error al NetScaler Gateway secundario, a menos que todas las interfaces del NetScaler Gateway principal no funcionen.

Cada interfaz de un conjunto de interfaces de conmutación por error mantiene entradas de puente independientes. Las interfaces de supervisión habilitadas y de alta disponibilidad en un NetScaler Gateway que no están vinculadas a un conjunto de interfaces con errores se conocen como interfaces críticas, porque si alguna de estas interfaces falla, se desencadena la conmutación por error.

### Para configurar la redundancia de enlaces

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En la ficha Conjunto de interfaces de conmutación por error, haga clic en Agregar.
3. En Nombre, escriba un nombre para el conjunto.
4. En Interfaces, haga clic en Agregar.
5. En Interfaces disponibles, seleccione una interfaz y, a continuación, haga clic en la flecha para mover la interfaz a Configurada.
6. Repita los pasos 4 y 5 para la segunda interfaz y, a continuación, haga clic en Crear.

Puede agregar tantas interfaces como necesite para la conmutación por error entre las interfaces.

### Para quitar interfaces del conjunto de interfaces de conmutación por error

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En la ficha Conjunto de interfaces de conmutación por error, seleccione un conjunto y, a continuación, haga clic en Quitar.

### Para quitar un conjunto de interfaces de conmutación por error

Si ya no necesita un conjunto de interfaces de conmutación por error, puede quitarlo de NetScaler Gateway.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En la ficha Conjunto de interfaces de conmutación por error, seleccione un conjunto y, a continuación, haga clic en Quitar.

## Descripción de las causas de la conmutación por error

January 26, 2024

Los siguientes eventos pueden provocar una conmutación por error en una configuración de alta disponibilidad:

1. Si el nodo secundario no recibe un paquete de latidos del nodo principal durante un período de tiempo que exceda el intervalo muerto establecido en el secundario. Para obtener más información sobre cómo establecer el intervalo muerto, consulte Configuración de intervalos de comunicación. Entre las posibles causas de que un nodo no reciba paquetes de latidos de un nodo del mismo nivel se incluyen:
    - Un problema de configuración de red impide que los latidos recorran la red entre los nodos de alta disponibilidad.
    - El nodo del mismo nivel experimenta un error de hardware o software que hace que se congele (cuelgue), se reinicie o detenga el procesamiento y el reenvío de paquetes de latidos.
2. El nodo principal experimenta un fallo de hardware en su tarjeta SSL.
3. El nodo principal no recibe paquetes de latidos en sus interfaces de red durante tres segundos.
4. En el nodo principal, se produce un error en una interfaz de red que no forma parte de un conjunto de interfaces de conmutación por error (FIS) ni de un canal de agregación de enlaces (LA) y que tiene habilitado el monitor de alta disponibilidad (HAMON). Las interfaces están habilitadas, pero pasan al estado DOWN.
5. En el nodo principal, todas las interfaces de un FIS fallan. Las interfaces están habilitadas, pero pasan al estado DOWN.
6. En el nodo principal, falla un canal LA con HAMON habilitado. Las interfaces están habilitadas, pero pasan al estado DOWN.
7. En el nodo principal, todas las interfaces fallan. En este caso, la conmutación por error se produce independientemente de la configuración de HAMON.
8. En el nodo principal, todas las interfaces se inhabilitan manualmente. En este caso, la conmutación por error se produce independientemente de la configuración de HAMON.
9. Para forzar una conmutación por error, se ejecuta el comando forzar conmutación por error en cualquiera de los nodos.
10. Un monitor de ruta enlazado al nodo principal se desactiva.

## Forzar la conmutación por error desde un nodo

January 26, 2024

Es posible que quiera forzar una conmutación por error si, por ejemplo, necesita reemplazar o actualizar el nodo principal. Puede forzar la conmutación por error desde el nodo principal o el nodo secundario. Una conmutación por error forzada no se propaga ni sincroniza. Para ver el estado de sincronización tras una conmutación por error forzada, puede ver el estado del nodo.

Una conmutación por error forzada falla en cualquiera de las siguientes circunstancias:

- Se fuerza la conmutación por error en un sistema independiente.
- El nodo secundario está inhabilitado.
- El nodo secundario está configurado para permanecer secundario.

El dispositivo NetScaler Gateway muestra un mensaje de advertencia si detecta un problema potencial al ejecutar el comando force failover. El mensaje incluye la información que ha desencadenado la advertencia y solicita confirmación antes de continuar.

## Forzar la conmutación por error en el nodo principal o secundario

January 26, 2024

Si fuerza la conmutación por error en el nodo principal, el principal se convierte en el secundario y el secundario en el principal. La conmutación por error forzada solo es posible cuando el nodo principal puede determinar que el nodo secundario está UP.

Si el nodo secundario es DOWN, el comando force failover devuelve el siguiente mensaje de error: "Operation not possible due to invalid peer state. Rectificar y volver a intentarlo."

Si el sistema secundario está en estado de reclamación o inactivo, el comando devuelve el siguiente mensaje de error: `Operation not possible now. Please wait for system to stabilize before retrying.`

Si ejecuta el comando force failover desde el nodo secundario, el nodo secundario se convierte en primario y el nodo primario se convierte en secundario. Solo se puede producir una conmutación por error forzada si el estado del nodo secundario es correcto y el nodo no está configurado para permanecer secundario.

Si el nodo secundario no puede convertirse en el nodo principal, o si el nodo secundario se configuró para permanecer secundario (mediante la opción STAYSECONDARY), el nodo muestra el siguiente mensaje de error: "Operation not possible as my state is invalid. Vea el nodo para obtener más información. "

### Para forzar la conmutación por error en el nodo principal o secundario

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione el nodo principal y, a continuación, en Acciones, haga clic en Forzar conmutación por error.
3. En el cuadro de diálogo Advertencia, haga clic en Sí.

## Obligar al nodo primario a permanecer primario

January 26, 2024

En una configuración de alta disponibilidad, puede forzar que el NetScaler Gateway principal permanezca como principal incluso después de la conmutación por error del dispositivo. Solo puede configurar esta configuración en dispositivos NetScaler Gateway independientes y en NetScaler Gateway que es el dispositivo principal en un par de alta disponibilidad.

### Para forzar que el nodo principal permanezca como principal

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.
3. En Estado de alta disponibilidad, haga clic en Mantente principal y, a continuación, en Aceptar.

Solo puede borrar esta configuración mediante el siguiente comando:

```
clear configuration full
```

Los siguientes comandos no cambian la configuración de alta disponibilidad de NetScaler Gateway:

```
clear configuration basic
```

```
clear configuration extended
```

## Obligar al nodo secundario a permanecer secundario

January 26, 2024

En una configuración de alta disponibilidad, puede forzar que el NetScaler Gateway secundario permanezca secundario, independientemente del estado del NetScaler Gateway principal. Cuando configura NetScaler Gateway para que permanezca secundario, sigue siendo secundario aunque se produzca un error en el NetScaler Gateway principal.

Por ejemplo, en una configuración de alta disponibilidad existente, supongamos que necesita actualizar el NetScaler Gateway principal y que este proceso lleva un tiempo determinado. Durante la actualización, el NetScaler Gateway principal puede dejar de estar disponible, pero no quiere que el NetScaler Gateway secundario se haga cargo. Quiere que siga siendo el NetScaler Gateway secundario, incluso si detecta un error en el NetScaler Gateway principal.

Si el estado de un NetScaler Gateway en un par de alta disponibilidad está configurado para permanecer secundario, no participa en las transiciones de máquinas de estado de alta disponibilidad. Puede comprobar el estado de NetScaler Gateway en la utilidad de configuración de la ficha Nodos.

Esta configuración funciona tanto en un NetScaler Gateway independiente como en un secundario.

Cuando se establece el nodo de alta disponibilidad, no se propaga ni sincroniza y solo afecta a NetScaler Gateway en el que se configura la configuración.

### Para forzar que el nodo secundario permanezca secundario

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.
3. En Estado de alta disponibilidad, haga clic en Permanecer en segundo plano (permanecer en modo de escucha) y, a continuación, haga clic en Aceptar.

### Para devolver NetScaler Gateway al servicio como dispositivo activo de alta disponibilidad

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la pestaña Nodos, seleccione el dispositivo que va a seguir siendo el nodo principal y, a continuación, haga clic en Abrir.
3. En Estado de alta disponibilidad, haga clic en Habilitado (participar activamente en HA) y, a continuación, haga clic en Aceptar.

# Usar clústeres

January 26, 2024

NetScaler Gateway se puede implementar en configuraciones de clúster para proporcionar un alto rendimiento, alta disponibilidad y escalabilidad para el tráfico de clientes VPN. En un clúster, un grupo de dispositivos o máquinas virtuales de NetScaler Gateway funciona como una única imagen del sistema para coordinar las sesiones de los usuarios y administrar el tráfico a los recursos de red. Se puede crear un clúster de Citrix Gateway con un mínimo de dos y un máximo de 32 dispositivos o máquinas virtuales Citrix Gateway configurados como nodos de clúster.

Lea la documentación de
NetScaler ADC Clustering antes de empezar a configurar el clúster de NetScaler Gateway. Preste especial atención a los siguientes temas de esa documentación.

- Consulte Requisitos de hardware y software para comprobar que los sistemas que piensa utilizar cumplen los requisitos.
- Consulte Cómo funciona la agrupación en clústeres para obtener una descripción de los conceptos de clustering
- Consulte Configuración de la comunicación entre nodos para planificar la implementación e identificar cualquier advertencia que pueda ser relevante para su entorno.

Un clúster de NetScaler Gateway funciona como un clúster NetScaler ADC de tipo de configuración VIP detectado.

> **Importante:** El asistente de **XenApp y XenDesktop** no es compatible con la agrupación en clústeres y, por lo tanto, no se encuentra el asistente de **XenApp y XenDesktop** en la sección **GUI > Panel de navegación > Integrar con productos Citrix**.

# Configuración de la agrupación en clústeres

January 26, 2024

Las principales tareas de configuración de clústeres de NetScaler Gateway son:

1. Decida qué dispositivo o máquina virtual Citrix Gateway será el coordinador de la configuración y cree una instancia de clúster en ese sistema (si aún no hay una).
2. Unir los sistemas NetScaler Gateway al clúster como nodos.
3. Crea un grupo de nodos en la instancia del clúster con la opción STICKY definida.

4. Enlazar un único nodo de clúster al grupo de nodos del clúster.
5. Configure un servidor virtual Citrix Gateway en el coordinador de configuración y vincúlelo al grupo de nodos del clúster.

Tenga en cuenta que hay varios métodos disponibles para configurar un clúster de Citrix ADC. El siguiente conjunto de tareas utiliza el método más directo disponible en la utilidad de configuración.

### Para crear una instancia de clúster de NetScaler Gateway mediante la utilidad de configuración

Una vez que tenga todos los detalles de implementación en orden, comience la configuración en el Citrix Gateway que será el coordinador de configuración.

Precaución: Al crear la instancia de clúster, se borra la configuración. Si necesita guardar la configuración del sistema existente como referencia, archive una copia antes de continuar con la configuración del clúster. Cualquier configuración existente que se vaya a utilizar en el clúster se puede volver a aplicar en el coordinador de configuración una vez establecido el clúster.

1. Inicie sesión en la utilidad de configuración Citrix ADC en la dirección NSIP.
2. Expanda el nodo Sistema y, a continuación, el subnodo Cluster.
3. En el panel de detalles, haga clic en Administrar clúster.
4. En el cuadro de diálogo Configuración del clúster, defina los parámetros necesarios para crear el clúster.

    a) Introduzca un ID de instancia de clúster Es el identificador numérico de la instancia de clúster. El valor predeterminado es 1 pero se puede establecer en cualquier número del 1 al 16.
    b) Introduzca la dirección IP del clúster. Será la dirección IP del coordinador de configuración del clúster, que es la dirección IP de administración del clúster.
    c) Seleccione la interfaz de plano posterior preferida. Esta es la interfaz de NetScaler Gateway que se utiliza para la comunicación entre los nodos del clúster.

5. Haga clic en Crear.
6. En el mensaje para confirmar el reinicio del sistema, haga clic en Sí.
7. Espere a que se reinicie el sistema. Cuando esté disponible, inicie sesión en la utilidad de configuración en la dirección IP del clúster configurada en el paso 4b.
8. Tenga en cuenta que, en el panel de detalles de información del sistema, el nodo local en la dirección NSIP aparece como coordinador de configuración. Esto confirma que la instancia del clúster base ya está funcionando.

El nodo local del coordinador de configuración se agrega automáticamente al clúster. Se pueden agregar más nodos en la siguiente tarea.

### Agregar nodos a un clúster de NetScaler Gateway

Una vez establecida la instancia del clúster, puede empezar a agregar otros nodos de NetScaler Gateway al clúster.

Para agregar más sistemas NetScaler Gateway al clúster, puede utilizar la utilidad de configuración para emitir de forma remota la configuración cluster-node-creation y join-cluster.

Nota: La adición de nodos al clúster debe completarse antes de configurar la configuración de Citrix Gateway. De esta forma, no tendrá que repetir la configuración de Citrix Gateway si algo va mal con la configuración del clúster y quiere eliminar el clúster y empezar de nuevo.

1. Inicie sesión en la utilidad de configuración Citrix ADC en la dirección IP del clúster.
2. Expanda el nodo Sistema y, a continuación, el subnodo Cluster.
3. En el panel de detalles, haga clic en Administrar clúster.
4. En el panel de detalles Nodos de clúster, haga clic en Agregar.
5. En el panel Crear nodo de clúster, introduzca un identificador de nodo único para este nodo.
6. Introduzca la dirección IP de NetScaler ADC del sistema que quiere agregar como nodo de clúster.
7. En el panel de credenciales del nodo de clúster, introduzca el nombre de usuario y la contraseña de Citrix Gateway para el sistema Citrix Gateway remoto.
8. En el panel Credenciales del Coordinador de configuración, introduzca la contraseña del usuario autorizado local.
9. Haga clic en Crear.
10. Cuando se le solicite, haga clic en SÍ para permitir que se guarde la configuración del sistema y realice un reinicio en caliente del NetScaler Gateway remoto.

Repita los pasos del 4 al 9 para cada sistema Citrix Gateway remoto adicional que quiera configurar como nodo de clúster.

Compruebe que los nodos del clúster estén incluidos en la lista de nodos activos del panel de detalles Nodos de clúster. Si falta algún nodo, repita los pasos 4 a 10 hasta que aparezcan todos los nodos necesarios.

### Creación de un grupo de nodos de clúster

Una vez agregados los nodos del clúster, se puede crear un grupo de nodos de clúster.

1. Inicie sesión en la utilidad de configuración Citrix ADC en la dirección IP del clúster.
2. Expanda el nodo Sistema y, a continuación, el subnodo Cluster.
3. Pulse en Grupos de nodos.
4. En el panel de detalles, haga clic en Agregar.
5. Introduzca un nombre para el grupo de nodos del clúster.

6. Selecciona la opción Adhesiva. Esto es necesario para admitir el tipo de servidor virtual Citrix Gateway.
7. Haga clic en Continuar.

El grupo de nodos del clúster ya está establecido. Antes de abandonar esta área de la utilidad de configuración, puede enlazar el nodo local de NetScaler Gateway al nuevo grupo de nodos del clúster. Este será el único nodo enlazado al grupo de clústeres.

### Vincular el nodo del clúster local al grupo de nodos del clúster

Dado que una configuración de clúster de NetScaler Gateway es de tipo detectado, solo se puede enlazar un nodo al grupo de nodos. El siguiente procedimiento vincula el nodo local del coordinador de configuración al grupo de nodos, pero cualquier nodo del clúster se puede utilizar para este enlace.

1. En el panel Opciones avanzadas, expanda Nodos de clúster.
2. En el panel central Nodos de clúster, seleccione Sin nodo de clúster.
3. En la pantalla Configuración del nodo de clúster, haga clic en Vincular.
4. Seleccione el nodo local representado por la dirección NSIP de este sistema NetScaler Gateway.
5. Haga clic en Insertar.
6. Haga clic en Aceptar.
7. Haga clic en Listo.

El clúster ya está lleno y listo para compartir un servidor virtual de NetScaler Gateway según lo configurado mediante la siguiente tarea.

### Enlace de un servidor virtual de NetScaler Gateway al grupo de nodos de clú

Con un clúster establecido, puede proceder a crear la configuración de NetScaler Gateway para la que está destinada la implementación del clúster. Para vincular la configuración al clúster, debe crear el servidor virtual de NetScaler Gateway y vincularlo a un grupo de nodos del clúster configurado en el tipo Sticky. Una vez enlazado el servidor virtual al grupo de nodos del clúster, puede seguir configurando NetScaler Gateway.

Si hay varios servidores virtuales de NetScaler Gateway configurados, estos deben estar enlazados también al grupo de nodos del clúster.

**Nota:** Si aún no se han configurado los servidores virtuales de NetScaler Gateway, es posible que tenga que habilitar primero las funciones de NetScaler Gateway y Autenticación, Autorización y Auditoría en
Sistema > Configuración > Configurar funciones básicas.

1. Inicie sesión en la utilidad de configuración Citrix ADC en la dirección IP del clúster.

2. Expanda el nodo Sistema y, a continuación, el subnodo Cluster.
3. Pulse en Grupos de nodos.
4. En el panel Grupo de nodos, seleccione el nombre del grupo de nodos deseado y, a continuación, haga clic en Modificar.
5. En el panel Avanzadas de la derecha, expanda la opción Servidores virtuales y, a continuación, haga clic en el icono + para agregar un servidor virtual.
6. Elija el tipo de servidor virtual VPN y, a continuación, haga clic en Continuar.
7. Haga clic en Bind.
8. Si aparece el servidor virtual necesario, selecciónelo, haga clic en Insertar y, a continuación, haga clic en Aceptar.
9. Si tiene que crear un nuevo servidor virtual, haga clic en Agregar. Continúe con la configuración del servidor virtual de NetScaler ADC. Como mínimo, todo lo que se necesita es crear el servidor virtual para que se pueda enlazar al grupo de nodos del clúster.
10. Una vez que el servidor virtual esté disponible en la lista Servidores virtuales de NetScaler Gateway, selecciónelo y, a continuación, haga clic en Insertar.
11. Haga clic en Aceptar.
12. Haga clic en Listo.

Nota: Si hay varios servidores virtuales de NetScaler Gateway configurados, también deben enlazarse al grupo de nodos del clúster mediante el mismo método.

## Mantener y supervisar el sistema

January 26, 2024

Una vez que haya completado la configuración de su NetScaler Gateway, deberá mantener y supervisar el dispositivo. Puede hacerlo de las siguientes maneras:

- Puede actualizar NetScaler Gateway a la versión más reciente del software. Al iniciar sesión en el sitio web de Citrix, puede ir al sitio de descargas de NetScaler Gateway y descargar el software. Puede encontrar el archivo léame de las compilaciones de mantenimiento en Citrix Knowledge Center.
- Puede asignar tareas de configuración y administración de NetScaler Gateway a distintos miembros del grupo. Con la administración delegada, puede asignar niveles de acceso a personas que les limitan a realizar tareas específicas en NetScaler Gateway.
- Puede guardar la configuración de NetScaler Gateway en el dispositivo o en un archivo del equipo. Puede comparar la configuración actual en ejecución y la configuración guardada. También puede borrar la configuración de NetScaler Gateway.

- Puede ver, actualizar y sesiones de usuario final en la utilidad de configuración de NetScaler Gateway.
- Puede configurar el registro en NetScaler Gateway. Los registros proporcionan información importante sobre el dispositivo y son útiles en caso de que se produzcan problemas.

## Configurar administradores delegados

January 26, 2024

NetScaler Gateway tiene un nombre de usuario y una contraseña de administrador predeterminados. El nombre de usuario y la contraseña predeterminados son nsroot. Al ejecutar el Asistente de configuración por primera vez, puede cambiar la contraseña de administrador.

Puede crear cuentas de administrador adicionales y asignar a cada cuenta diferentes niveles de acceso a Citrix Gateway. Estas cuentas adicionales se denominan administradores delegados. Por ejemplo, hay una persona asignada para supervisar las conexiones y los registros de Citrix Gateway y otra persona responsable de configurar parámetros específicos en Citrix Gateway. El primer administrador tiene acceso de solo lectura y el segundo administrador tiene acceso limitado al dispositivo.

Para configurar un administrador delegado, utilice directivas de comandos y usuarios y grupos del sistema.

Al configurar un administrador delegado, el proceso de configuración es:

- Agregue un usuario del sistema. Un usuario del sistema es un administrador con los privilegios especificados. Todos los administradores heredan las directivas de los grupos a los que pertenecen.
- Agregue un grupo de sistemas. Un grupo de sistemas contiene usuarios de sistemas con privilegios específicos. Los miembros del grupo del sistema heredan las directivas del grupo o grupos a los que pertenecen.
- Cree una directiva de comandos. Las directivas de comandos permiten definir qué partes de la configuración de NetScaler Gateway pueden acceder y modificar un usuario o un grupo. También puede regular qué comandos, como grupos de comandos, servidores virtuales y otros elementos que los administradores y grupos pueden configurar.
- Enlazar la directiva de comandos al usuario o grupo estableciendo la prioridad. Al configurar la administración delegada, asigne prioridades al administrador o al grupo para que NetScaler Gateway pueda determinar qué directiva tiene prioridad.

NetScaler Gateway tiene una directiva de comandos de deny system predeterminada. Las directivas de comandos no se pueden enlazar globalmente. Debe vincular las políticas directamente a los administradores del sistema (usuarios) o grupos. Si los usuarios y los grupos no tienen una directiva

de comandos asociada, se aplica la política de denegación predeterminada y los usuarios no pueden ejecutar ningún comando ni configurar Citrix Gateway.

Puede configurar directivas de comandos personalizadas para definir un mayor nivel de detalle para las asignaciones de derechos de usuario. Por ejemplo, puede dar a una persona la posibilidad de agregar directivas de sesión a NetScaler Gateway, pero no permitir que el usuario realice ninguna otra configuración.

## Configurar directivas de comandos para administradores delegados

January 26, 2024

NetScaler Gateway tiene cuatro directivas de comandos integradas que puede utilizar para la administración delegada:

- Solo lectura. Permite el acceso de solo lectura para mostrar todos los comandos excepto los comandos del grupo de comandos del sistema y ns.conf show.
- Operador. Permite el acceso de solo lectura y también permite el acceso para habilitar y inhabilitar comandos en los servicios. Esta política también permite el acceso para establecer servicios y servidores como "acceso indirecto".
- Network. Permite un acceso casi completo al sistema, excluyendo los comandos del sistema y el comando shell.
- Superusuario. Otorga todos los privilegios del sistema, como los privilegios otorgados al administrador predeterminado, nsroot.

Las directivas de comandos contienen expresiones integradas. La utilidad de configuración se utiliza para crear usuarios del sistema, grupos de sistemas, políticas de comandos y para definir los permisos.

### Para crear un usuario administrativo en NetScaler Gateway

1. En la utilidad de configuración, en el panel de navegación, en la ficha **Configuración**, expanda **Sistema** > **Administración de usuarios** y, a continuación, haga clic en **Usuarios del sistema**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre de usuario**, escriba un nombre de usuario.
4. En el campo Contraseña y Confirmar contraseña, escriba la contraseña.
5. Para agregar usuarios a un grupo, en Miembro de, haga clic en **Agregar** .
6. En **Disponible**, seleccione un grupo y, a continuación, haga clic en la flecha derecha.
7. En Políticas de comando, en Acción, haga clic en Insertar.

8. En el cuadro de diálogo Insertar políticas de comandos, seleccione el comando, haga clic en Aceptar, en Crear y, a continuación, en Cerrar.

### Creación de grupos administrativos

Los grupos administrativos contienen usuarios con privilegios administrativos en NetScaler Gateway. Puede crear grupos administrativos en la utilidad de configuración.

**Para configurar un grupo administrativo mediante la utilidad de configuración**

1. En la utilidad de configuración, en el panel de navegación, en la ficha **Configuración**, expanda **Sistema** > **Administración de usuarios** y, a continuación, haga clic en **Grupos de sistemas**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre del grupo**, escriba un nombre para el grupo.
4. Para agregar un usuario existente al grupo, en **Miembros**, haga clic en **Agregar**.
5. En **Disponible**, seleccione un usuario y, a continuación, haga clic en la flecha derecha.
6. En **Directivas de comandos**, en **Acción**, haga clic en **Insertar**, seleccione una directiva o directivas, haga clic en **Aceptar**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

## Configurar directivas de comandos personalizadas para administradores delegados

March 27, 2024

Al configurar una directiva de comandos personalizada, se proporciona un nombre de directiva y, a continuación, se configuran los componentes de la directiva para crear la especificación de comandos. Con la especificación de comandos, puede limitar los comandos que pueden usar los administradores. Por ejemplo, quiere denegar a los administradores la posibilidad de utilizar el comando remove. Al configurar la directiva, defina la acción en denegar y, a continuación, configure los parámetros.

Puede configurar una directiva de comandos sencilla o avanzada. Si configura una directiva sencilla, configura un componente del dispositivo, como Citrix Gateway y la autenticación. Si configura una política avanzada, selecciona el componente, denominado grupo de entidades, y luego selecciona los comandos que los administradores pueden ejecutar en el grupo.

### Para crear una directiva de comandos personalizada sencilla

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Sistema** > **Administración de usuario** y, a continuación, haga clic en **Directivas de comando.**
2. En el panel de detalles, haga clic en **Agregar.**
3. En **Nombre de la directiva**, escriba un nombre para la directiva.
4. En **Acción**, seleccione **Permitir** o **Denegar**.
5. En **Especificación de comandos**, haga clic en **Agregar**.
6. En el cuadro de diálogo **Agregar comando**, en la ficha **Simple**, en Operación, seleccione la acción que pueden realizar los administradores delegados.
7. En **Grupo de entidades**, seleccione uno o varios grupos.

   Puede presionar la tecla CTRL para seleccionar varios grupos.
8. Haga clic en **Create** y, luego, en **Close**.

### Para crear una directiva de comandos personalizada avanzada

1. En la utilidad de configuración, en el panel de navegación, en la ficha **Configuración**, expanda **Sistema** > **Administración de usuario** y, a continuación, haga clic en **Directivas de comando**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre de la directiva**, escriba un nombre para la directiva.
4. En **Acción**, seleccione **Permitir** o **Denegar**.
5. En **Especificación de comandos**, haga clic en **Agregar**.
6. En el cuadro de diálogo **Agregar comando**, haga clic en la ficha **Avanzadas**.
7. En **Grupo de entidades**, seleccione el grupo al que pertenece el comando, tal autenticación o alta disponibilidad.
8. En **Entidad**, seleccione la directiva.

   Puede presionar la tecla CTRL para seleccionar varios elementos de la lista.
9. En **Operación** , seleccione el comando, haga clic en **Crear** y, a continuación, en **Cerrar** .

   Puede presionar la tecla CTRL para seleccionar varios elementos de la lista.
10. Haga clic en **Create** y, luego, en **Close**.
11. En el cuadro de diálogo **Crear directiva de comandos**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Al hacer clic en Crear, la expresión aparece en Especificación de comandos del cuadro de diálogo Crear directiva de comandos.

Después de crear la directiva de comandos personalizada, puede vincularla a un usuario o a un grupo.

> **Nota:** Solo puede enlazar directivas de comandos personalizadas a los usuarios o grupos que cree. No puede vincular una política de comandos personalizada al usuario nsroot.

### Para enlazar una directiva de comandos personalizada a un usuario o grupo

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Sistema** > **Administración de usuarios** y, a continuación, haga clic en **Usuarios del sistema** o en **Grupos de sistemas**.
2. En el panel de detalles, seleccione un usuario o grupo de la lista y, a continuación, haga clic en **Abrir**.
3. En **Directivas de comandos**, seleccione la directiva y, a continuación, haga clic en **Aceptar**.

## Configurar la auditoría en NetScaler Gateway

January 26, 2024

NetScaler Gateway permite registrar los estados y la información de estado que recopila el dispositivo. Puede utilizar los registros de auditoría para ver el historial de sucesos en orden cronológico. Los mensajes de los registros contienen información sobre el suceso que generó el mensaje, una marca de tiempo, el tipo de mensaje y niveles de registro predefinidos e información del mensaje. Puede configurar ajustes que determinan la información que se registra y la ubicación en la que se almacenan los mensajes.

NetScaler Gateway admite actualmente dos formatos de registro: un formato de registro propietario para registros locales y el formato syslog para usar con servidores syslog. Puede configurar los registros de auditoría para que proporcionen la siguiente información:

| Nivel | Descripción |
|---|---|
| EMERGENCIA | Registra solo los errores principales. Las entradas del registro indican que NetScaler Gateway está experimentando un problema crítico que hace que no se pueda utilizar. |

| Nivel | Descripción |
| --- | --- |
| ALERTA | Registra problemas que pueden hacer que NetScaler Gateway funcione incorrectamente, pero que no son críticos para su funcionamiento. Se deben tomar medidas correctivas lo antes posible para evitar que Citrix Gateway experimente un problema crítico. |
| CRÍTICO | Registra las condiciones críticas que no restringen el funcionamiento de NetScaler Gateway, pero que pueden derivar a un problema mayor. |
| ERROR | Registra las entradas resultantes de una operación fallida en NetScaler Gateway. |
| ADVERTENCIA | Registra posibles problemas que pueden dar lugar a un error o a un error crítico. |
| NOTIFICACIÓN | Registra problemas más detallados que el registro de nivel de información, pero tiene el mismo propósito que la notificación. |
| INFORMACIÓN | Registra las acciones realizadas por NetScaler Gateway. Este nivel es útil para solucionar problemas. |

El registro de auditoría de NetScaler Gateway también almacena estadísticas de compresión de NetScaler Gateway si configura la compresión TCP. La relación de compresión alcanzada para los distintos datos se almacena en el archivo de registro de cada sesión de usuario.

Citrix Gateway utiliza la firma de registro SessionID, que le permite realizar un seguimiento de los registros por sesión en lugar de por usuario. Los registros que se generan como parte de una sesión tienen el mismo SessionID. Si un usuario establece dos sesiones desde el mismo dispositivo de usuario con la misma dirección IP, cada sesión tiene un ID de sesión único.

> **Importante:** Si ha escrito scripts de análisis de registros personalizados, tendrá que cambiar esta firma dentro de los scripts de análisis personalizados.

## Configurar registros en NetScaler Gateway

March 27, 2024

Al configurar el registro en NetScaler Gateway, puede elegir almacenar los registros de auditoría en NetScaler Gateway o enviarlos a un servidor syslog. La utilidad de configuración se utiliza para crear directivas de auditoría y configurar los ajustes para almacenar los registros de auditoría.

### Para crear una directiva de auditoría

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**.
2. En **Nombre**, escriba un nombre para la directiva.
3. Seleccione una de estas opciones:
   - Syslog si quiere enviar los registros a un servidor Syslog.
   - Nslog para almacenar los registros en Citrix Gateway.

     > **Nota:** Si selecciona esta opción, los registros se almacenan en la carpeta /var/log del dispositivo.
4. En el panel de detalles, haga clic en **Agregar**.
5. Escriba la siguiente información para la información del servidor en el que se almacenan los registros:
   - En Nombre, escriba el nombre del servidor.
   - En Servidor, escriba el nombre o la dirección IP del servidor de registros.
6. Haga clic en Crear y, a continuación, en Cerrar.

Después de crear la directiva de auditoría, puede vincularla a cualquier combinación de lo siguiente:

- Globalmente
- Servidores virtuales
- Grupos
- Usuarios

### Para enlazar una directiva de auditoría de forma global

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**.
2. Seleccione **Syslog** o **Nslog**.
3. En el panel de detalles, haga clic en **Acción** y, a continuación, haga clic en **Enlaces globales**.
4. En el cuadro de diálogo **Vincular o desvincular directivas de auditoría** a **global**, en **Detalles**, haga clic en **Insertar directiva**.
5. En **Nombre de directiva**, seleccione una directiva y, a continuación, haga clic en **Aceptar**.

### Para modificar una directiva de auditoría

Puede modificar una directiva de auditoría existente para cambiar el servidor al que se envían los registros.

1. En la utilidad de configuración, en la ficha **Configuración**, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**
2. Seleccione **Syslog** o **Nslog**.
3. En el panel de detalles, haga clic en una directiva y, a continuación, haga clic en **Abrir**.
4. En Servidor, seleccione el nuevo servidor y, a continuación, haga clic en **Aceptar**.

### Para quitar una directiva de auditoría

Puede quitar una directiva de auditoría de NetScaler Gateway. Al quitar una directiva de auditoría, la directiva se desvinculará automáticamente.

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**.
2. Seleccione **Syslog** o **Nslog**.
3. En el panel de detalles, haga clic en una directiva y, a continuación, en **Quitar**.

## Configurar el registro de ACL

January 26, 2024

Puede configurar NetScaler Gateway para que registre los detalles de los paquetes que coinciden con una lista de control de acceso ampliado (ACL). Además del nombre de la ACL, los detalles registrados incluyen información específica del paquete, como las direcciones IP de origen y destino. La información se almacena en un archivo syslog o nslog, según el tipo de registro (syslog o nslog) que habilite.

Puede habilitar el registro tanto a nivel global como a nivel de ACL. Sin embargo, para habilitar el registro a nivel de ACL, también debe habilitarlo a nivel global. La configuración global tiene prioridad.

Para optimizar el registro, cuando varios paquetes del mismo flujo coinciden con una ACL, solo se registran los detalles del primer paquete. El contador se incrementa para todos los demás paquetes que pertenecen al mismo flujo. Un flujo se define como un conjunto de paquetes que tienen los mismos valores para los siguientes parámetros:

- IP de origen
- IP de destino
- Puerto de origen

- Puerto de destino
- Protocolo (TCP o UDP)

Si el paquete no procede del mismo flujo o si la duración del tiempo supera el tiempo medio, se crea un nuevo flujo. El tiempo medio es el tiempo durante el cual los paquetes del mismo flujo no generan mensajes adicionales (aunque el contador se incrementa).

> **Nota:** El número total de flujos diferentes que se pueden registrar en un momento dado está limitado a 10.000.

En la tabla siguiente se describen los parámetros con los que se puede configurar el registro de ACL a nivel de regla para las ACL extendidas.

| Nombre del parámetro | Descripción |
|---|---|
| Estado de registro | Estado de la función de registro de la ACL. Valores posibles: HABILITADO y INHABILITADO. Predeterminado: DISABLED. |
| Límite de tarifa | Número de mensajes de registro que puede generar una ACL específica. Valor predeterminado: 100. |

### Para configurar el registro de ACL mediante la utilidad de configuración

Puede configurar el registro para una ACL y especificar el número de mensajes de registro que puede generar la regla.

1. En la utilidad de configuración, en el panel de navegación, expanda **Sistema** > **Red** y, a continuación, haga clic en ACL.
2. En el panel de detalles, haga clic en la ficha **ACL extendidas** y, a continuación, haga clic en Agregar.
3. En el cuadro de diálogo **Crear ACL extendida**, en Nombre, escriba un nombre para la directiva.
4. Active la casilla de verificación **Estado del registro**.
5. En el cuadro de texto **Límite de velocidad de registro**, escriba el límite de velocidad que quiere especificar para la regla y, a continuación, haga clic en **Crear**.

Después de configurar el registro de ACL, puede habilitarlo en NetScaler Gateway. Cree una directiva de auditoría y, a continuación, enlaza a un usuario, grupo, servidor virtual o de forma global.

### Para habilitar el registro ACL o TCP en NetScaler Gateway

1. En la utilidad de configuración, en el panel de navegación, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**.
2. Seleccione syslog o nslog.
3. En la ficha **Servidores**, haga clic en **Agregar**.
4. En el cuadro de diálogo **Crear servidor de auditoría**, en **Nombre**, escriba un nombre para el servidor y, a continuación, configure la configuración del servidor.
5. Haga clic en Registro **ACL o RegistroTCP**y, a continuación, haga clic en**Crear**.

## Habilitación del registro de plug-ins de NetScaler Gateway

January 26, 2024

Puede configurar el plug-in de NetScaler Gateway para registrar todos los errores en los archivos de texto almacenados en el dispositivo del usuario. Los usuarios pueden configurar el plug-in de NetScaler Gateway para establecer el nivel de registro en el dispositivo de usuario para registrar actividades específicas de usuario. Cuando los usuarios configuran el registro, el complemento crea los dos archivos siguientes en el dispositivo del usuario:

- hooklog \.txt <num\ >, que registra los mensajes de interceptación que genera el complemento de NetScaler Gateway.
- nssslvpn.txt, que enumera los errores del plug-in.

> **Nota:** Los archivos hooklog.txt no se eliminan automáticamente. Citrix recomienda eliminar los archivos periódicamente.

Los registros de usuario se encuentran en los siguientes directorios de Windows del dispositivo del usuario:

- Windows XP (todos los usuarios): %SystemDrive%:\Documents and Settings\All Users\Application Data\Citrix\AGEE
- Windows XP (para usuarios específicos): %SystemDrive%:\Documents and Settings\%username%\Local Settings\Application Data\Citrix\AGEE
- Windows Vista (todos los usuarios): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows Vista (para usuarios específicos): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGE
- Windows 7 (todos los usuarios): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 7 (para usuarios específicos): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 8 (todos los usuarios): %SystemDrive%:\ProgramData\Citrix\AGEE

- Windows 8 (para usuarios específicos): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE

Puede utilizar estos archivos de registro para solucionar problemas del plug-in de NetScaler Gateway. Los usuarios pueden enviar los archivos de registro por correo electrónico al soporte técnico.

En el cuadro de diálogo Configuración, los usuarios pueden establecer el nivel de registro del plug-in de NetScaler Gateway. Los niveles de registro son:

- Grabar mensajes de error
- Grabar mensajes de sucesos
- Registre estadísticas de plug-ins de NetScaler Gateway
- Registra todos los errores, mensajes de eventos y estadísticas

### Para habilitar el registro

1. En el dispositivo del usuario, haga clic con el botón secundario del mouse en el icono de NetScaler Gateway del área de notificación y, a continuación, haga clic en Configurar NetScaler Gateway
2. Haga clic en la ficha Seguimiento, seleccione el nivel de registro y haga clic en Aceptar.

> **Nota:** Los usuarios deben iniciar sesión con el plug-in de NetScaler Gateway para abrir el cuadro de diálogo Configuración.

## Para supervisar las conexiones ICA

January 26, 2024

Puede supervisar las sesiones de usuario activas en la comunidad de servidores mediante el cuadro de diálogo Conexiones
ICA. Este cuadro de diálogo proporciona la siguiente información:

- Nombre de usuario de la persona que se conecta a la comunidad de servidores
- Nombre de dominio de la comunidad de servidores
- Dirección IP del dispositivo del usuario
- Número de puerto del dispositivo de usuario
- Dirección IP del servidor que ejecuta Citrix Virtual Apps and Desktops
- Número de puerto del servidor que ejecuta Citrix Virtual Apps and Desktops

1. En la utilidad de configuración, en el panel de navegación, haga clic en NetScaler ADC Gateway.
2. En el panel de detalles, en Supervisar conexiones, haga clic en Conexiones ICA para ver el cuadro de diálogo de supervisión.

## Integración en productos Citrix

January 26, 2024

Si es el administrador del sistema responsable de instalar y configurar Citrix Gateway, puede configurar el dispositivo para que funcione con Citrix Endpoint Management, StoreFront y la Interfaz Web.

Los usuarios pueden conectarse directamente a Endpoint Management desde la red interna o desde una ubicación remota. Cuando los usuarios se conectan, pueden acceder a sus aplicaciones web, SaaS y móviles. También pueden trabajar con documentos ubicados en ShareFile desde cualquier dispositivo.

Para permitir las conexiones de usuarios a una comunidad de servidores a través de NetScaler Gateway, configure los valores en StoreFront o en la Interfaz Web y en NetScaler Gateway. Cuando los usuarios se conectan, tienen acceso a aplicaciones publicadas y escritorios virtuales.

Los pasos de configuración para integrar NetScaler Gateway con Endpoint Management, StoreFront y la interfaz web suponen lo siguiente:

- NetScaler Gateway reside en la DMZ y está conectado a una red existente.
- NetScaler Gateway se implementa como dispositivo independiente y los usuarios remotos se conectan directamente a NetScaler Gateway.
- StoreFront, Endpoint Management, Citrix Virtual Apps, Citrix Virtual Desktops y la interfaz web residen en la red segura.
- ShareFile se configura en Endpoint Management. Para obtener más información sobre ShareFile, consulte el tema ShareFile y el tema Configuración de ShareFile para el acceso de usuario.

La forma de implementar StoreFront y Endpoint Management depende de las aplicaciones que proporcione a los dispositivos móviles. Si los usuarios tienen acceso a aplicaciones MDX empaquetadas con MDX Toolkit, Endpoint Management reside delante de StoreFront en la red segura. Si no proporciona acceso a las aplicaciones MDX, StoreFront reside delante de Endpoint Management en la red segura.

## Cómo se conectan los usuarios a las aplicaciones, los escritorios y ShareFile

January 26, 2024

Si tiene Citrix Endpoint Management en la implementación, los usuarios pueden conectarse de las siguientes maneras:

- El plug-in de NetScaler Gateway que establece un túnel VPN completo a los recursos de la red interna. Cree un perfil de sesión para seleccionar el plug-in de NetScaler Gateway para Windows o NetScaler Gateway para Mac. Cuando los usuarios inician sesión mediante el complemento, los análisis de puntos finales se pueden ejecutar en el dispositivo del usuario.

> **Nota**: Para permitir que los análisis de puntos finales se ejecuten en ordenadores Mac, debe instalar Citrix Gateway 10.1, Build 120.1316.e o una versión posterior.

- Citrix Receiver para conectarse a aplicaciones web, SaaS y empresariales, enlaces web y documentos desde ShareFile a través de Endpoint Management. Cuando los usuarios inician sesión con Receiver, Citrix Gateway dirige la conexión a Endpoint Management. Cuando Receiver establece la conexión, las aplicaciones y los documentos de los usuarios aparecen en Receiver. Si los usuarios inician sesión con Receiver y se conectan directamente a Endpoint Management, debe habilitar el acceso sin cliente en Citrix Gateway. Esta implementación no requiere StoreFront.
- Receiver para conectarse a aplicaciones publicadas y escritorios virtuales a través de StoreFront o la Interfaz Web. Cuando los usuarios inician sesión con Receiver, Citrix Gateway enruta la conexión a StoreFront o a la Interfaz Web. Cuando Receiver establece la conexión, las aplicaciones de usuario y los escritorios aparecen en Receiver.
- Secure Hub para conectarse a aplicaciones iOS y Android, incluidas WorxMail y WorxWeb, desde dispositivos móviles a través de Endpoint Management. Cuando los usuarios inician sesión en Secure Hub, tienen acceso a las aplicaciones móviles que configura en Endpoint Management. Cuando NetScaler Gateway establece la conexión Micro VPN, las aplicaciones móviles de los usuarios aparecen en la ventana Secure Hub. Los usuarios pueden iniciar las aplicaciones desde Secure Hub. Algunas aplicaciones requieren que los usuarios descarguen e instalen la aplicación en el dispositivo móvil.

En cualquiera de los casos anteriores, si los usuarios desean conectarse a través de NetScaler Gateway, hacen lo siguiente:

- Los usuarios inician sesión mediante el plug-in de NetScaler Gateway o Receiver. Para iniciar sesión por primera vez, los usuarios abren un explorador web y escriben el nombre de dominio completo (FQDN) de Citrix Gateway o Receiver. Los usuarios con dispositivos móviles inician sesión en Secure Hub.
- En la página de inicio de sesión, los usuarios introducen sus credenciales y se autentican.
- Tras la autenticación, la sesión del usuario se redirige a StoreFront o Endpoint Management en función de la implementación.
- Si implementa StoreFront y Endpoint Management, NetScaler Gateway se pone en contacto con el primer servidor de la implementación. Por ejemplo, si configura aplicaciones móviles MDX en Endpoint Management, implementa StoreFront detrás de Endpoint Management. Si no proporciona acceso a las aplicaciones móviles MDX, implementa Endpoint Management detrás de StoreFront.

- Todos los escritorios, documentos y aplicaciones web, SaaS y basadas en Windows de los usuarios aparecen en Receiver o Secure Hub.

Si los usuarios necesitan acceder a otros recursos de la red interna, como Exchange, recursos compartidos de archivos o sitios web internos, también pueden iniciar sesión con el plug-in de NetScaler Gateway. Por ejemplo, si los usuarios desean conectarse a un servidor Microsoft Exchange de la red, inician Microsoft Outlook en su equipo. La conexión segura se realiza con el plug-in de NetScaler Gateway que se conecta a NetScaler Gateway. El túnel VPN SSL se crea en Exchange Server y los usuarios pueden acceder a su correo electrónico.

> **Importante**: Citrix recomienda configurar la autenticación en el servidor virtual de NetScaler Gateway. Cuando inhabilita la autenticación en NetScaler Gateway, las solicitudes HTTP no autenticadas se envían directamente a los servidores que ejecutan la Interfaz Web, StoreFront o Endpoint Management en la red interna.

## Implementación con Citrix Endpoint Management, Citrix Virtual Apps y escritorio

January 26, 2024

Puede hacer que los usuarios se conecten a aplicaciones Windows, web, SaaS y móviles y escritorios virtuales alojados en su red. Puede proporcionar acceso a sus aplicaciones y escritorios a usuarios remotos e internos mediante NetScaler Gateway, Citrix Endpoint Management y Citrix Virtual Apps and Desktops. Citrix Gateway autentica a los usuarios y, a continuación, les permite acceder a sus aplicaciones mediante Citrix Receiver o Secure Hub.

Los usuarios se conectan a sus aplicaciones basadas en Windows publicadas en Citrix Virtual Apps y a los escritorios virtuales publicados en Citrix Virtual Desktops mediante Receiver y StoreFront.

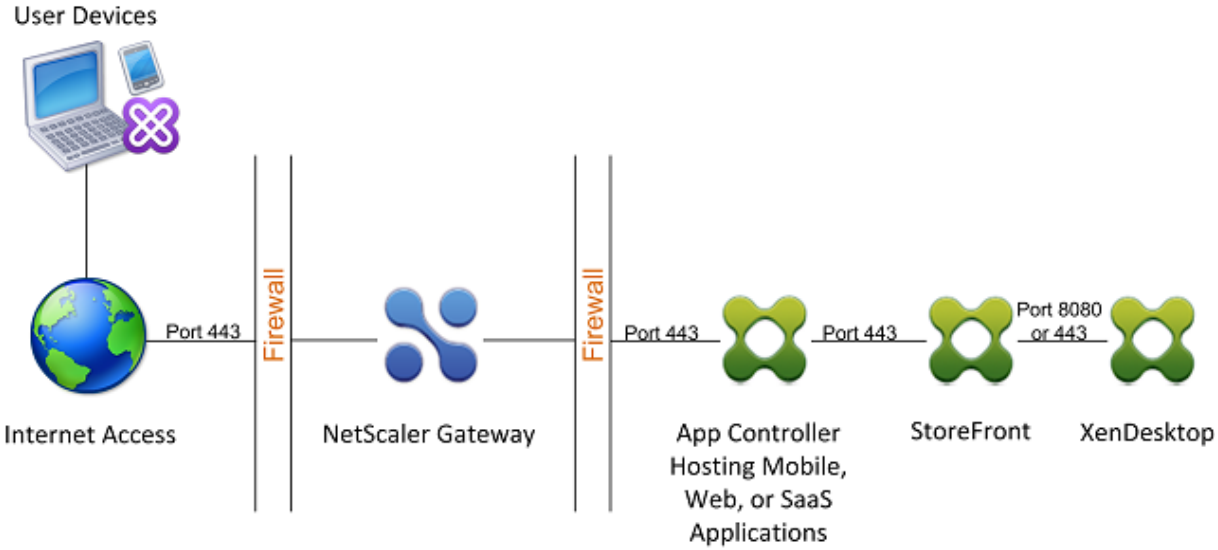
Citrix Endpoint Management contiene Citrix Endpoint Management, que permite a los usuarios conectarse a aplicaciones web, SaaS y MDX. Endpoint Management le permite administrar aplicaciones web, SaaS y MDX para el inicio de sesión único (SSO), junto con documentos de ShareFile. Instala Endpoint Management en la red interna. Los usuarios remotos se conectan a Endpoint Management a través de NetScaler Gateway para acceder a sus aplicaciones y datos de ShareFile Los usuarios remotos pueden conectarse con el plug-in de NetScaler Gateway, Receiver o Secure Hub para acceder a las aplicaciones y a ShareFile. Los usuarios que están en la red interna pueden conectarse directamente a Endpoint Management mediante Receiver. La siguiente figura muestra la implementación de Citrix Gateway con Endpoint Management y StoreFront.

Si su implementación proporciona acceso a aplicaciones MDX desde Endpoint Management y acceso

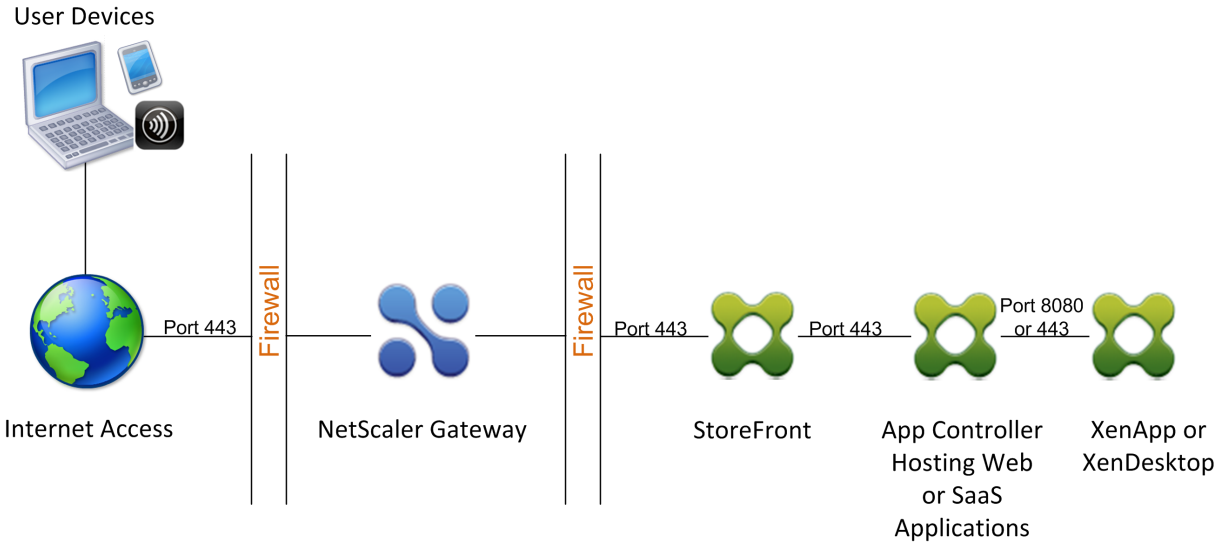
a aplicaciones basadas en Windows desde StoreFront, implemente Endpoint Management delante de StoreFront, como se muestra en la siguiente ilustración:

Figura 1. Implementación de NetScaler Gateway con Endpoint Management en frente de StoreFront




Si la implementación no proporciona acceso a las aplicaciones MDX, StoreFront reside delante de Endpoint Management, como se muestra en la siguiente ilustración:

Figura 2. Implementación de NetScaler Gateway con StoreFront frente a Endpoint Management




Con cada implementación, StoreFront y Endpoint Management deben residir en la red interna y NetScaler Gateway debe estar en la DMZ. Para obtener más información sobre la implementación de Endpoint Management, consulte el tema Instalación de Endpoint Management .
Para obtener más información sobre la implementación de StoreFront, consulte el tema StoreFront.

## Acceder a los recursos de Citrix Virtual Apps and Desktops con la Interfaz Web

January 26, 2024

Uno o más equipos que ejecutan Citrix Virtual Apps and Desktops crean una comunidad de servidores. Si la red empresarial contiene una comunidad de servidores, puede implementar NetScaler Gateway para proporcionar acceso seguro a Internet a aplicaciones publicadas o escritorios virtuales mediante la Interfaz Web.

En estas implementaciones, Citrix Gateway trabaja con la Interfaz Web y la Secure Ticket Authority (STA) para proporcionar autenticación, autorización y redirección a las aplicaciones publicadas alojadas en un equipo que ejecuta Citrix Virtual Apps o a los escritorios virtuales proporcionados por Citrix Virtual Desktops.

Esta funcionalidad se logra mediante la integración de NetScaler Gateway con la Interfaz Web, Citrix Virtual Apps y Desktops. Esta integración proporciona autenticación avanzada y una opción de control de acceso a la Interfaz Web. Para obtener más información sobre la Interfaz Web, consulte la documentación de la Interfaz Web en la biblioteca de documentación de Citrix.

La conectividad remota a una comunidad de servidores no requiere el plug-in de NetScaler Gateway. Para acceder a las aplicaciones o escritorios publicados, los usuarios se conectan mediante Citrix Receiver.

## Integrar NetScaler Gateway en Citrix Virtual Apps and Desktops

January 26, 2024

Al configurar NetScaler Gateway para conexiones de usuario, puede incluir la configuración del tráfico de red en Citrix Virtual Apps, Citrix Virtual Desktops o ambos. Para ello, debe configurar NetScaler Gateway y la Interfaz Web para que se comuniquen entre sí.

Las tareas de integración de estos productos incluyen:

- Creación de un sitio de Interfaz Web en la comunidad de Citrix Virtual Apps and Desktops.
- Configuración de la configuración en la Interfaz Web para redirigir las conexiones de usuario a través de NetScaler Gateway.
- Configurar NetScaler Gateway para comunicarse con la Interfaz Web y Secure Ticket Authority (STA).

También puede configurar NetScaler Gateway para que se comunique con una comunidad de servidores de Citrix Virtual Apps implementando NetScaler Gateway en una DMZ de doble salto. Para obtener más información, consulte Implementación de NetScaler Gateway en una DMZ de doble salto.

NetScaler Gateway y la Interfaz Web utilizan STA y Citrix XML Service para establecer conexiones de usuario. Los servicios STA y XML se ejecutan en el servidor de Citrix Virtual Apps and Desktops.

## Establecimiento de una conexión segura a la comunidad de servidores

January 26, 2024

El siguiente ejemplo muestra cómo Citrix Gateway implementado en la DMZ es compatible con la Interfaz Web para proporcionar un punto de acceso único y seguro a los recursos publicados disponibles en una red empresarial segura.

En este ejemplo, existen las condiciones siguientes:

- Los dispositivos de usuario de Internet se conectan a Citrix Gateway mediante Citrix Receiver.
- La Interfaz Web se encuentra detrás de NetScaler Gateway en la red segura. El dispositivo del usuario establece la conexión inicial con NetScaler Gateway y la conexión se transfiere a la Interfaz Web.
- La red segura contiene una comunidad de servidores. Un servidor de este conjunto de servidores ejecuta Secure Ticket Authority (STA) y Citrix XML Service. STA y XML Service se pueden ejecutar en Citrix Virtual Apps and Desktops.

### Descripción general del proceso: acceso de usuario a recursos publicados en la comunidad de servidores

1. Un usuario remoto escribe la dirección de NetScaler Gateway; por ejemplo `https://www.ag.wxyco.com`, en el campo de dirección de un explorador web. El dispositivo del usuario intenta esta conexión SSL en el puerto 443, que debe estar abierto a través del firewall para que la conexión se realice correctamente.
2. NetScaler Gateway recibe la solicitud de conexión y se solicitan sus credenciales a los usuarios. Las credenciales se devuelven a través de NetScaler Gateway, los usuarios se autentican y la conexión se transfiere a la Interfaz Web.
3. La Interfaz Web envía las credenciales de usuario al servicio XML de Citrix que se ejecuta en la comunidad de servidores.
4. El servicio XML autentica las credenciales de usuario y envía a la Interfaz Web una lista de las aplicaciones o escritorios publicados a los que el usuario tiene autorización para acceder.

5. La Interfaz Web rellena una página web con la lista de recursos publicados (aplicaciones o escritorios) a los que el usuario tiene autorización para acceder y envía esta página web al dispositivo del usuario.
6. El usuario hace clic en un enlace de escritorio o aplicación publicada. Se envía una solicitud HTTP a la Interfaz Web que indica el recurso publicado en el que ha hecho clic el usuario.
7. La Interfaz Web interactúa con el servicio XML y recibe un vale que indica el servidor en el que se ejecuta el recurso publicado.
8. La Interfaz Web envía una solicitud de tíquet de sesión al STA. Esta solicitud especifica la dirección IP del servidor en el que se ejecuta el recurso publicado. El STA guarda esta dirección IP y envía el tíquet de sesión solicitado a la Interfaz Web.
9. La Interfaz Web genera un archivo ICA que contiene el tíquet emitido por el STA y lo envía al explorador web del dispositivo del usuario. El archivo ICA generado por la Interfaz Web contiene el nombre de dominio completo (FQDN) o el nombre del sistema de nombres de dominio (DNS) de NetScaler Gateway. La dirección IP del servidor que ejecuta el recurso solicitado nunca se revela a los usuarios.
10. El archivo ICA contiene datos que indican al explorador web que inicie Citrix Receiver. El dispositivo de usuario se conecta a Citrix Gateway mediante el nombre DNS o FQDN de Citrix Gateway en el archivo ICA. El enlace inicial de SSL/TLS se produce para establecer la identidad de NetScaler Gateway.
11. El dispositivo del usuario envía el tíquet de sesión a NetScaler Gateway y, a continuación, NetScaler Gateway se pone en contacto con el STA para validar el tíquet.
12. STA devuelve a NetScaler Gateway la dirección IP del servidor en el que reside la aplicación solicitada.
13. NetScaler Gateway establece una conexión TCP con el servidor.
14. NetScaler Gateway completa el enlace de conexión con el dispositivo del usuario e indica al dispositivo del usuario que la conexión se ha establecido con el servidor. El resto del tráfico entre el dispositivo del usuario y el servidor se transforma mediante proxy a través de NetScaler Gateway. El tráfico entre el dispositivo del usuario y NetScaler Gateway está cifrado. El tráfico entre NetScaler Gateway y el servidor se puede cifrar de forma independiente, pero no se cifra de forma predeterminada.

## Implementación con la Interfaz Web

January 26, 2024

Cuando implementa NetScaler Gateway para proporcionar acceso remoto seguro a aplicaciones y escritorios virtuales de Citrix, NetScaler Gateway trabaja con la Interfaz Web y Secure Ticket Authority (STA) para proporcionar acceso a aplicaciones publicadas y escritorios alojados en una comunidad

de servidores.

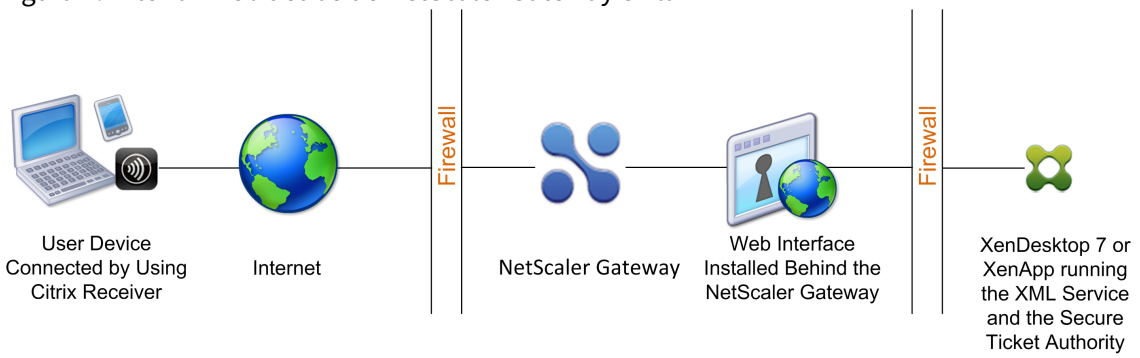
La implementación de NetScaler Gateway en la DMZ es la configuración más común cuando NetScaler Gateway opera con una comunidad de servidores. En esta configuración, Citrix Gateway proporciona un punto de acceso único y seguro para los exploradores web y Citrix Receiver que acceden a los recursos publicados a través de la Interfaz Web. En esta sección se tratan los aspectos básicos de esta opción de implementación.

La configuración de la red de su organización determina dónde se implementa NetScaler Gateway cuando funciona con una comunidad de servidores. Dispone de estas dos opciones:

- Si su organización protege la red interna con una única DMZ, implemente NetScaler Gateway en la DMZ.
- Si su organización protege la red interna con dos DMZ, implemente un NetScaler Gateway en cada uno de los dos segmentos de red en una configuración DMZ de doble salto. Para obtener más información, consulte Implementación de NetScaler Gateway en una DMZ de doble salto. Nota: También puede configurar una DMZ de doble salto con el segundo dispositivo NetScaler Gateway de la red segura.

Cuando implementa NetScaler Gateway en la DMZ para proporcionar acceso remoto a una comunidad de servidores, puede implementar una de las tres opciones de implementación siguientes:

- Implemente la Interfaz Web detrás de NetScaler Gateway en la DMZ. En esta configuración, como se muestra en la siguiente ilustración, tanto NetScaler Gateway como la Interfaz Web se implementan en la DMZ. La conexión inicial del usuario se dirige a NetScaler Gateway y, a continuación, se redirige a la Interfaz Web.
  Figura 1. Interfaz web detrás de NetScaler Gateway en la




- Implemente NetScaler Gateway en paralelo a la Interfaz Web de la DMZ. En esta configuración, tanto NetScaler Gateway como la Interfaz Web se implementan en la DMZ, pero la conexión inicial del usuario se dirige a la Interfaz Web en lugar de a NetScaler Gateway.
- Implemente NetScaler Gateway en la DMZ e implemente la Interfaz Web en la red interna. En esta configuración, NetScaler Gateway autentica las solicitudes de los usuarios antes de retransmitir la solicitud a la Interfaz Web de la red segura. La Interfaz Web no realiza la autenticación, pero interactúa con el STA y genera un archivo ICA para garantizar que el tráfico ICA se enruta a

través de NetScaler Gateway a la comunidad de servidores.

La ubicación en la que se implementa la Interfaz Web depende de varios factores, entre los que se incluyen:

- Autenticación. Cuando los usuarios inician sesión, NetScaler Gateway o la Interfaz Web pueden autenticar las credenciales de usuario. La ubicación de la Interfaz Web en la red es un factor que determina, en parte, dónde se autentican los usuarios.
- Software de usuario. Los usuarios pueden conectarse a la Interfaz Web con el plug-in de NetScaler Gateway o Citrix Receiver. Puede limitar los recursos a los que los usuarios pueden acceder utilizando únicamente Citrix Receiver o proporcionar a los usuarios un mayor acceso a la red con el plug-in de NetScaler Gateway. La forma en que se conectan los usuarios y los recursos a los que permite que los usuarios se conecten pueden ayudar a determinar dónde se implementa la Interfaz Web de la red.

## Implementar la Interfaz Web en la red segura

January 26, 2024

En esta implementación, la Interfaz Web reside en la red interna segura. NetScaler Gateway está en la zona desmilitarizada. NetScaler Gateway autentica las solicitudes de los usuarios antes de enviarlas a la Interfaz Web.

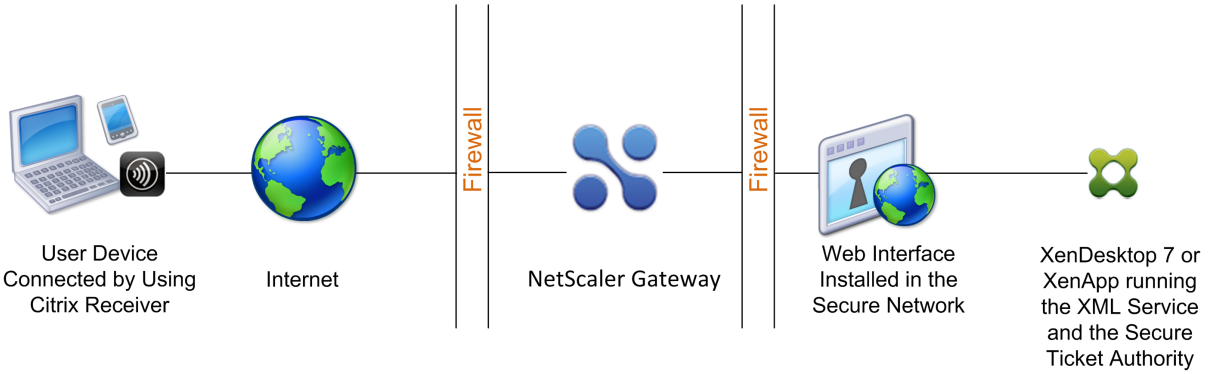
Al implementar la Interfaz Web en la red segura, debe configurar la autenticación en NetScaler Gateway.

Si implementa la Interfaz Web con Citrix Virtual Apps and Desktops, la implementación de la Interfaz Web en la red segura es el caso de implementación predeterminado. Cuando se instala Desktop Delivery Controller, también se instala una versión personalizada de la Interfaz Web.

> **Importante**:
> Cuando la Interfaz Web esté en la red segura, debe habilitar la autenticación en Citrix Gateway. Los usuarios se conectan a NetScaler Gateway, escriban sus credenciales y, a continuación, se conectan a la Interfaz Web. Cuando inhabilita la autenticación, las solicitudes HTTP no autenticadas se envían directamente al servidor que ejecuta la Interfaz Web. Se recomienda inhabilitar la autenticación en NetScaler Gateway solo cuando la Interfaz Web está en la DMZ y los usuarios se conectan directamente a la Interfaz Web.

Figura 1. Interfaz web ubicada dentro de la red segura



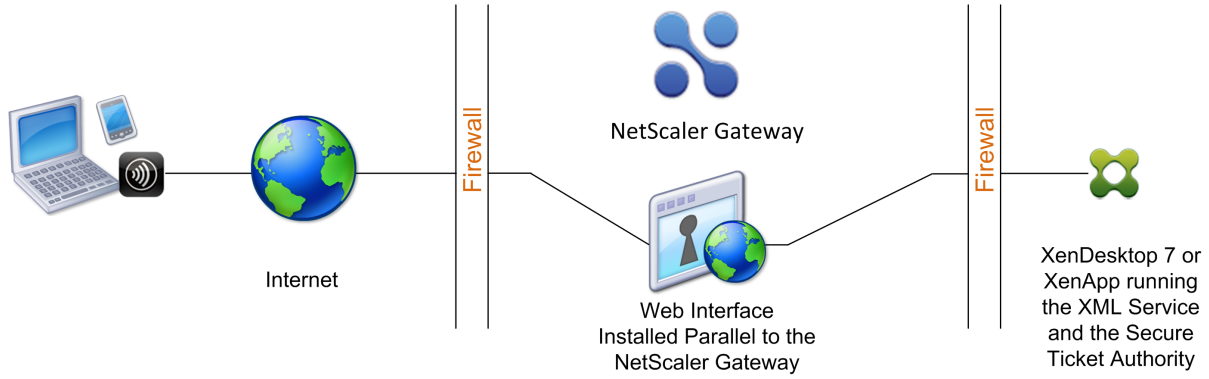

## Implementación de la interfaz web en paralelo a Citrix Gateway en la DMZ

January 26, 2024

En esta implementación, la Interfaz Web y NetScaler Gateway residen en la DMZ. Los usuarios se conectan directamente a la Interfaz Web mediante un explorador web o Citrix Receiver. Las conexiones de usuario se envían primero a la Interfaz Web para su autenticación. Tras la autenticación, las conexiones se enrutan a través de NetScaler Gateway. Después de que los usuarios inicien sesión correctamente en la Interfaz Web, pueden tener acceso a aplicaciones o escritorios publicados en la comunidad de servidores. Cuando los usuarios inician una aplicación o un escritorio, la Interfaz Web envía un archivo ICA con instrucciones para redirigir el tráfico ICA a través de NetScaler Gateway como si fuera un servidor que ejecuta Secure Gateway. El archivo ICA entregado por la Interfaz Web incluye un vale de sesión producido por Secure Ticket Authority (STA).

Cuando Citrix Receiver se conecta a Citrix Gateway, se presenta el ticket. NetScaler Gateway se pone en contacto con el STA para validar el tíquet de sesión. Si el vale sigue siendo válido, el tráfico ICA del usuario se retransmite al servidor de la comunidad de servidores. En la siguiente ilustración se muestra esta implementación.

Figura 1. La Interfaz Web instalada en paralelo a NetScaler Gateway



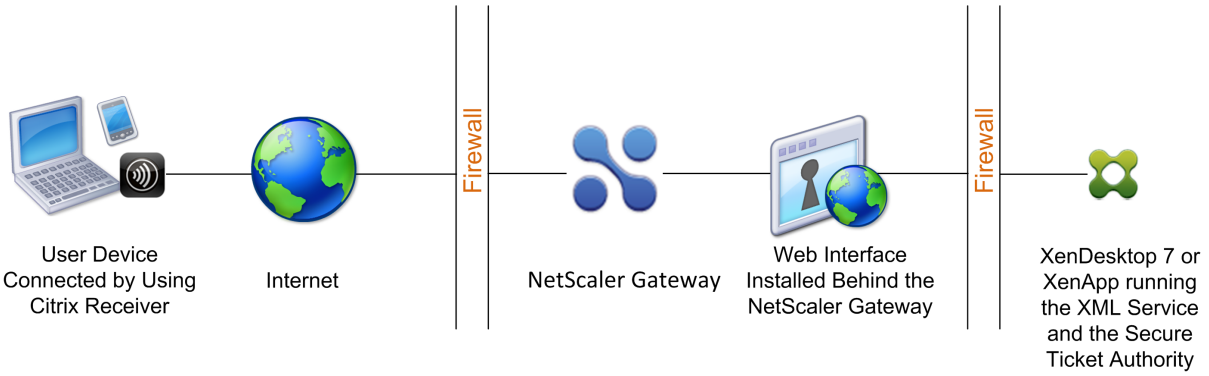
Cuando la Interfaz Web se ejecuta en paralelo a NetScaler Gateway en la DMZ, no es necesario configurar la autenticación en NetScaler Gateway. La Interfaz Web autentica a los usuarios.

## Implementación de la interfaz web detrás de Citrix Gateway en la DMZ

January 26, 2024

En esta configuración, tanto NetScaler Gateway como la Interfaz Web se implementan en la DMZ. Cuando los usuarios inician sesión con Citrix Receiver, la conexión inicial del usuario va a Citrix Gateway y, a continuación, se redirige a la Interfaz Web. Para redirigir todo el tráfico HTTPS e ICA a través de un único puerto externo y requerir el uso de un único certificado SSL, NetScaler Gateway actúa como proxy web inverso para la Interfaz Web.

Figura 1. Interfaz web ubicada detrás de NetScaler Gateway




Cuando la Interfaz Web se implementa detrás de NetScaler Gateway en la DMZ, puede configurar la autenticación en el dispositivo, pero no es necesaria. Puede hacer que Citrix Gateway o la Interfaz Web autentiquen a los usuarios, ya que ambos residen en la DMZ.

## Funciones de la Interfaz Web

January 26, 2024

Antes de configurar la Interfaz Web para que funcione con NetScaler Gateway, debe comprender las diferencias entre los sitios web de Citrix Virtual Apps y los sitios de Citrix Virtual Apps Services.

- **Sitios web de Citrix Virtual Apps.** La Interfaz Web proporciona funcionalidad para crear y administrar sitios web de Citrix Virtual Apps. Los usuarios acceden a los recursos publicados y a las aplicaciones transmitidas de forma remota mediante un explorador web y un complemento.

- **Sitios de Citrix Virtual Apps Services.** Citrix Virtual Apps es un complemento diseñado para ofrecer flexibilidad y facilidad de configuración. Al usar Citrix Virtual Apps junto con los sitios de Citrix Virtual Apps Services en la Interfaz Web, puede integrar los recursos publicados con los escritorios de los usuarios. Los usuarios acceden a las aplicaciones remotas y transmitidas por streaming, así como a los escritorios remotos y al contenido haciendo clic en los iconos de su escritorio o en el menú Inicio, o haciendo clic en el área de notificación del escritorio de su equipo. Puede determinar las opciones de configuración a las que los usuarios pueden acceder y modificar, como los ajustes de audio, pantalla e inicio de sesión.

  > **Nota**: Si selecciona esta opción, no se admite el acceso a los escritorios virtuales.

Para obtener más información, consulte la documentación de la Interfaz Web en el nodo Tecnologías de la biblioteca Citrix eDocs.

## Configuración de un sitio de la Interfaz Web

January 26, 2024

Si implementa la Interfaz Web en la red segura y configura la autenticación en NetScaler Gateway, cuando los usuarios se conectan a NetScaler Gateway, el dispositivo autentica a los usuarios.

> **Importante**: Instale y configure la Interfaz Web antes de configurar NetScaler Gateway. Para obtener más información, consulte la documentación de la Interfaz Web en el nodo Tecnologías de la documentación de productos Citrix.

Los pasos para crear un sitio de Interfaz Web incluyen:

- Seleccione cómo inician sesión los usuarios. Esto puede ser a través de un explorador web, el plug-in de NetScaler Gateway o Citrix Receiver. Para obtener más información, consulte Características de la interfaz web .
- Identifica desde dónde se autentican los usuarios. NetScaler Gateway o la Interfaz Web.

> **Nota**: Cuando la Interfaz Web se encuentra en la red segura, se habilita la autenticación en el servidor virtual de NetScaler Gateway. Cuando inhabilita la autenticación, las solicitudes HTTP no autenticadas se envían directamente al servidor que ejecuta la Interfaz Web. Se recomienda inhabilitar la autenticación en NetScaler Gateway solo cuando la Interfaz Web está en la DMZ y los usuarios se conectan directamente a la Interfaz Web.

Asegúrese de instalar un certificado de servidor válido en NetScaler Gateway. Para obtener más información sobre cómo trabajar con certificados, consulte Instalación y administración de certificados.

> **Importante**: Para que la Interfaz Web funcione correctamente con NetScaler Gateway 10.1, el servidor que ejecuta la Interfaz Web debe confiar en el certificado de NetScaler Gateway y poder resolver el nombre de dominio completo (FQDN) del servidor virtual en la dirección IP correcta.

## Crear un sitio de la Interfaz Web 5.4

January 26, 2024

La consola Citrix Web Interface Management es un complemento de Microsoft Management Console (MMC) 3.0 que permite crear y configurar sitios web de Citrix Virtual Apps y Citrix Virtual Apps Services alojados en Microsoft Internet Information Services (IIS). Los tipos de sitio de Interfaz Web se muestran en el panel izquierdo. El panel de resultados central muestra los sitios disponibles en el contenedor de tipos de sitio seleccionado en el panel izquierdo.

La consola Citrix Web Interface Management le permite realizar tareas administrativas diarias de forma rápida y sencilla. En el panel Acción se enumeran las tareas disponibles actualmente.

Al utilizar la consola, la configuración surte efecto cuando confirma los cambios mediante la consola. Como resultado, es posible que algunos ajustes de la interfaz web se inhabiliten si sus valores no son relevantes para la configuración actual y los valores correspondientes se restablecen a sus valores predeterminados en WebInterface.conf. Citrix recomienda crear copias de seguridad periódicas de los archivos WebInterface.conf y config.xml de sus sitios.

La consola Citrix Web Interface Management se instala automáticamente al instalar la Interfaz Web para Microsoft Internet Information Services. Ejecute la consola haciendo clic en **Inicio > Todos los programas > Citrix > Consolas de administración > Administración de la interfaz web de Citrix** .

> **Nota**:
> Asegúrese de que MMC 3.0 esté presente en el servidor en el que instala la Interfaz Web, ya que es un requisito previo para la instalación de la consola de administración de la Interfaz Web de Citrix. MMC 3.0 está disponible de forma predeterminada en todas las plataformas Windows compatibles con el alojamiento de la interfaz web.

### Uso de archivos de configuración

Puede modificar los siguientes archivos de configuración para configurar sitios de Interfaz Web:

- Archivo de configuración de la Interfaz Web: El archivo de configuración de la interfaz web, WebInterface.conf, permite cambiar muchas propiedades de la interfaz web. Está disponible en

los servidores de aplicaciones Microsoft Internet Information Services (IIS) y Java. Puede utilizar este archivo para realizar tareas administrativas diarias y personalizar muchos más ajustes. Modifique los valores en WebInterface.conf y guarde el archivo actualizado para aplicar los cambios. Para obtener más información sobre cómo configurar la interfaz web mediante WebInterface.conf, consulte la documentación de la interfaz web en el nodo Tecnologías de la documentación del producto Citrix.

- Archivo de configuración de plug-ins en línea de Citrix. Puede configurar el complemento en línea de Citrix mediante el archivo config.xml del servidor de Interfaz Web.

## Configurar sitios mediante la Consola de administración de la Interfaz Web de Citrix

March 27, 2024

La consola Citrix Web Interface Management es un complemento de Microsoft Management Console (MMC) 3.0 que permite crear y configurar sitios web de Citrix Virtual Apps y Citrix Virtual Apps Services alojados en Microsoft Internet Information Services (IIS). Los tipos de sitio de Interfaz Web se muestran en el panel izquierdo. El panel de resultados central muestra los sitios disponibles en el contenedor de tipos de sitio seleccionado en el panel izquierdo.

La consola Citrix Web Interface Management le permite realizar tareas administrativas diarias de forma rápida y sencilla. En el panel Acción se enumeran las tareas disponibles actualmente. Las tareas relacionadas con los elementos seleccionados en el panel izquierdo se muestran en la parte superior y las acciones disponibles para los elementos seleccionados en el panel de resultados se muestran a continuación.

Al utilizar la consola, la configuración surte efecto cuando confirma los cambios mediante la consola. Como resultado, algunas opciones de la Interfaz Web pueden estar inhabilitadas si sus valores no son relevantes para la configuración actual y los valores correspondientes se restablecen a sus valores predeterminados en WebInterface.conf. Citrix recomienda crear copias de seguridad periódicas de los archivos WebInterface.conf y config.xml de sus sitios.

La consola Citrix Web Interface Management se instala automáticamente al instalar la Interfaz Web para Microsoft IIS. Ejecute la consola haciendo clic en Inicio > Todos los programas > Citrix > Consolas de administración > Administración de la interfaz web de Citrix .

Nota: Debe asegurarse de que MMC 3.0 esté presente en el servidor en el que instala la interfaz web, ya que es un requisito previo para la instalación de la consola Citrix Web Interface Management. MMC 3.0 está disponible de forma predeterminada en todas las plataformas Windows compatibles con el alojamiento de la interfaz web.

# Configurar la configuración de NetScaler Gateway en la Interfaz Web 5.4

March 27, 2024

Para utilizar NetScaler Gateway en la implementación, debe configurar que la interfaz web admita el dispositivo. Para ello, utilice la tarea Secure Access de la consola de administración de Citrix Web Interface Management.

### Para configurar los ajustes de NetScaler Gateway en la interfaz web

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Consolas de administración > Administración de la interfaz web de Citrix.
2. En el panel izquierdo de la consola de Citrix Web Interface Management, haga clic en Sitios web de Citrix Virtual Apps o Sitios de Citrix Virtual Apps Services y, a continuación, seleccione su sitio en el panel de resultados.
3. En el panel de acciones , haga clic en Acceso seguro .
4. En la página Especificar métodos de acceso, realice una de las siguientes acciones:
    - Haga clic en Agregar para agregar una nueva ruta de acceso.
    - Seleccione una ruta existente de la lista y, a continuación, haga clic en Modificar.
5. En la lista Método de Access, seleccione una de las siguientes opciones:
    - Si quiere enviar la dirección real del servidor Citrix a NetScaler Gateway, seleccione Gateway Direct.
    - Si quiere enviar la dirección alternativa del servidor Citrix Virtual Apps a NetScaler Gateway, seleccione Gateway alternativa.
      Nota: No se puede acceder a los escritorios virtuales de Citrix Virtual Desktops si se utilizan direcciones alternativas.
    - Si quiere que la dirección asignada a NetScaler Gateway se determine mediante las asignaciones de traducción de direcciones establecidas en la interfaz web, seleccione Gateway traducida.
6. Introduzca la dirección de red y la máscara de subred que identifican a la red cliente. Utilice los botones Subir y Bajar para colocar las rutas de acceso por orden de prioridad en la tabla Direcciones de dispositivos de usuario y, a continuación, haga clic en Siguiente.
7. Si no utiliza la traducción de direcciones de puerta de enlace, continúe con el paso 10. Si utiliza la traducción de direcciones de puerta de enlace, realice una de las siguientes acciones en la página Especificar traducciones de direcciones:
    - Haga clic en Agregar para agregar una nueva traducción de direcciones.

- Seleccione una traducción de direcciones existente de la lista y, a continuación, haga clic en Editar.

8. En el área Tipo de acceso, seleccione una de las siguientes opciones:
   - Si quiere que NetScaler Gateway utilice la dirección traducida para conectarse al servidor Citrix, seleccione Traducción de rutas de puertade enlace.
   - Si ha configurado una ruta traducida del cliente en la tabla Direcciones de dispositivo de usuario y quiere que tanto el cliente Citrix como NetScaler Gateway utilicen la dirección traducida para conectarse al servidor Citrix, seleccione Conversión de ruta de puerta de enlace y dispositivo de usuario.
9. Introduzca los puertos y direcciones internos y externos (traducidos) del servidor Citrix, haga clic en Aceptar y, a continuación, haga clic en Siguiente.
   Cuando NetScaler Gateway se conecta al servidor Citrix, utiliza el número de puerto y la dirección externos. Asegúrese de que las asignaciones que cree coincidan con el tipo de direcciones que utiliza la comunidad de servidores.
10. En la página Especificar configuración de puerta de enlace, especifique el nombre de dominio completo (FQDN) y el número de puerto del dispositivo NetScaler Gateway que deben usar los clientes. El FQDN debe coincidir con el del certificado instalado en la puerta de enlace.
11. Seleccione Habilitar fiabilidad de la sesión si quiere que el servidor Citrix mantenga abiertas las sesiones desconectadas mientras el cliente intenta volver a conectarse automáticamente.
12. Seleccione Solicitar tickets de dos STA cuando estén disponibles si ha habilitado la confiabilidad de la sesión y desea usar la emisión simultánea de boletos desde dos servidores de Secure Ticket Authority (STA). Al habilitar esta opción, la Interfaz Web obtiene tickets de dos STA diferentes para que las sesiones de los usuarios no se interrumpan si una STA deja de estar disponible durante el transcurso de la sesión. Si por algún motivo la Interfaz Web no puede ponerse en contacto con dos STA, recurrirá al uso de un solo STA. Haga clic en Siguiente.
13. En la página Especificar la configuración de Secure Ticket Authority, realice una de las siguientes acciones:
    - Haga clic en Agregar para especificar la URL de una STA que puede usar la Interfaz Web.
    - Seleccione una entrada de la lista y, a continuación, haga clic en Editar.

```
1 Use the Move Up and Move Down buttons to place the STAs in order of
     priority.
2 STAs are included with the Citrix XML Service; for example, `http\[s\]:
     //servername.domain.com/scripts/ctxsta.dll`.
3
4 You can specify more than one STA for fault tolerance; however, Citrix
     recommends that you do not use an external load balancer for this
     purpose.
```

14/. Seleccione Usar para el equilibrio de carga para elegir si desea habilitar o no el equilibrio de carga entre las STA.

Habilitar el equilibrio de carga le permite distribuir uniformemente las conexiones entre los servidores para que ningún servidor se sobrecargue.

1. Seleccione Omitir servidores fallidos para especificar el tiempo durante el que se deben omitir las STA inaccesibles.

```
The Web Interface provides fault tolerance among the servers on the STA
    URLs list so that if a communication error occurs, the failed
   server is bypassed for the specified time period.
```

## Crear un sitio de la Interfaz Web 5.3

January 26, 2024

Cuando crea un sitio web Interface 5.3, puede requerir que los usuarios inicien sesión con un explorador Web, Citrix Receiver o Citrix Desktop Receiver. Puede usar la consola de administración de la Interfaz Web de Citrix para crear varios sitios de la Interfaz Web.

Solo puede habilitar el inicio de sesión único con una tarjeta inteligente en la Interfaz Web con Interfaz Web 5.3. Esta versión de la interfaz web se puede ejecutar en Citrix Virtual Apps 4.5, 5.0 y 6.0.

Web Interface 5.3 se ejecuta en los siguientes sistemas operativos:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

> **Nota**:
> Citrix Virtual Apps 6.0 solo se ejecuta en Windows Server 2008 R2.

### Para crear un sitio de la Interfaz Web, versión 5.3

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix Web Interface Management.
2. En el panel izquierdo, seleccione Sitios web de Citrix Virtual Apps. Los usuarios inician sesión en la interfaz web mediante un explorador web.
3. En el menú Acción, haga clic en Crear sitio.
4. Mantenga el sitio y la ruta predeterminados de Internet Information Services (IIS) y, a continuación, haga clic en Siguiente.

   La ruta predeterminada del sitio es /Citrix Virtual Apps o puede especificar una ruta de acceso.

> **Nota**:
> Si hay sitios web de Citrix Virtual Apps preexistentes que utilicen la ruta de acceso predeterminada, se agrega un incremento apropiado para distinguir el nuevo sitio.

5. En Especificar dónde se lleva a cabo la autenticación de usuarios, seleccione una de las siguientes opciones:

   - En la interfaz web para que los usuarios se autentiquen mediante la interfaz web.

     Seleccione esta opción si la interfaz web se implementa como un servidor independiente paralelo a NetScaler Gateway en la zona desmilitarizada (DMZ).

   - En Access Gateway para que los usuarios se autentiquen mediante el dispositivo NetScaler Gateway.

     Si selecciona esta opción, NetScaler Gateway autentica a los usuarios e inicia el inicio de sesión único en la interfaz web si está configurado en el dispositivo.

   > **Nota**:
   > Si SmartAccess está configurado en Citrix Gateway, esta configuración habilita SmartAccess en Citrix Virtual Apps and Desktops.

6. Haga clic en Siguiente.
7. en el paso 5, en Dirección URL del servicio de autenticación, escriba la dirección web en la dirección URL del servicio de autenticación de NetScaler Gateway, como`https://access.company.com/CitrixAuthService/AuthService.asmx` y, a continuación, haga clic en Siguiente.
8. En Opciones de autenticación, seleccione cómo inician sesión los usuarios.

   - Explícito. Los usuarios inician sesión mediante un explorador web.
   - Tarjeta inteligente. Los usuarios inician sesión con una tarjeta inteligente.

9. Haga clic en Siguiente.
10. Si seleccionó Tarjeta inteligente en el paso 8, seleccione una de las siguientes opciones:
    - Solicitar a los usuarios el PIN. Los usuarios introducen su número de identificación personal (PIN) cuando inician una aplicación o un escritorio publicados.
    - Los usuarios no tienen que introducir su PIN al iniciar una aplicación o un escritorio publicados.

Aparecerá una pantalla de resumen en la que se muestran los ajustes. Haga clic en Siguiente para crear el sitio de la Interfaz Web. Cuando el sitio se crea correctamente, se le pedirá que configure los ajustes restantes en la interfaz web. Siga las instrucciones en el asistente para completar la configuración.

## Configurar la configuración de NetScaler Gateway en la Interfaz Web 5.3

March 27, 2024

Después de crear el sitio web Interface 5.3, puede utilizar Citrix Web Interface Management para configurar los valores de NetScaler Gateway.

### Para configurar la configuración de la Interfaz Web 5.3 para NetScaler Gateway

1. Haga clic en **Inicio > Todos los programas > Citrix > Consolas de administración > Administración de la interfaz web de Citrix**.
2. En el panel izquierdo de Citrix Web Interface Management, haga clic en **Sitios web de Citrix Virtual Apps**.
3. En el panel de acciones, haga clic en **Acceso seguro**.
4. En el cuadro de diálogo Editar configuración de acceso seguro, haga clic en **Agregar** .
5. En el cuadro de diálogo Agregar ruta de acceso, escriba la dirección del dispositivo de usuario, la máscara de subred y, en Método de acceso, seleccione **Gateway direct** , haga clic en Aceptar **y,** a continuación, en **Siguiente** .
   Si no especifica la dirección del dispositivo del usuario ni la máscara de subred, la opción Gateway direct se aplica a todos los dispositivos de usuario. La opción Gateway direct es adecuada para dispositivos de usuario que se conectan desde fuera de la red interna, mientras que la opción Direct es adecuada para dispositivos de usuario que se conectan desde la red interna.
6. En Dirección (FQDN), escriba el nombre de dominio completo (FQDN) de NetScaler Gateway. Debe ser el mismo FQDN que se utiliza en el certificado de NetScaler Gateway.
7. En Puerto, escriba el número de puerto. El valor por defecto es 443.
8. Para habilitar la confiabilidad de la sesión, haga clic en **Habilitar la confiabilidad de la sesión y,** a continuación, haga clic en **Siguiente** .
9. En Secure Ticket Authority URLs, haz clic en **Agregar** .
10. En Secure Ticket Authority URL, escriba el nombre del servidor maestro que ejecuta el servicio XML en Citrix Virtual Apps, haga clic en Aceptar **y,** a continuación, en **Finalizar** . Por ejemplo, escriba `http://Citrix Virtual Appssrv01/Scripts/CtxSta.dll`.

Después de configurar los ajustes en la interfaz web, puede configurarlos en NetScaler Gateway.

## Agregar Citrix Virtual Apps and Desktops a un único sitio

January 26, 2024

Si ejecuta Citrix Virtual Apps and Desktops, puede agregar ambas aplicaciones a un único sitio de Interfaz Web. Esta configuración le permite utilizar el mismo servidor de Secure Ticket Authority (STA) de Citrix Virtual Apps and Desktops.

> **Nota**:
> Citrix Virtual Desktops admite la interfaz web. La versión mínima necesaria de la interfaz web es 5.0.

Si utiliza la Interfaz Web 5.3 o 5.4, combine los sitios de Citrix Virtual Apps and Desktops mediante la consola de administración de la interfaz web.

> **Nota**:
> Si las comunidades de servidores se encuentran en dominios diferentes, debe establecer una confianza bidireccional entre los dominios.

### Para agregar Citrix Virtual Apps and Desktops a un solo sitio mediante la Interfaz Web 5.3 o 5.4

1. Haga clic en **Inicio** > **Todos los programas** > **Citrix** > **Management Consolas** > **Citrix Web Interface Management**.
2. En el panel izquierdo, seleccione **Sitios web de Citrix Virtual Apps**.
3. En el panel **Acción**, haga clic con el botón secundario en un sitio y, a continuación, haga clic en **Comunidades de servidores**.
4. En el cuadro de diálogo **Administrar comunidades de servidores**, haga clic en **Agregar**.
5. Complete la configuración de la comunidad de servidores y, a continuación, haga clic en **Aceptar** dos veces.

Para obtener la mejor experiencia al utilizar Citrix Virtual Desktops, cambie la configuración UserInterfaceRanding a Escritorios en el archivo de configuración webInterface.conf.

## Redirigir conexiones de usuarios a través de NetScaler Gateway

January 26, 2024

En Citrix Virtual Apps and Desktops, puede configurar los servidores para que solo acepten conexiones redirigidas a través de NetScaler Gateway. En Citrix Virtual Apps 6.5, se configura una directiva en Citrix AppCenter para enrutar las conexiones a través de Citrix Gateway. En Citrix Virtual Desktops 7.1, utiliza Citrix Studio para configurar la configuración.

### Para configurar las propiedades del servidor Citrix Virtual Apps 6.5 para que acepten conexiones enrutadas únicamente a través de Citrix Gateway

1. Haga clic en Inicio > Herramientas administrativas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda NetScaler Resources > Citrix Virtual Apps > FarmName, donde FarmName es el nombre de la comunidad de servidores.
3. Haga clic en Directivas.
4. En el panel central, haga clic en Equipo o Usuario y, a continuación, haga clic en Nuevo.
5. En el Asistente para nueva directiva, en Nombre, escriba un nombre para la directiva y, a continuación, haga clic en Siguiente.
6. En **Categorías**, haga clic en **Configuración del servidor**.
7. En **Configuración**, junto a Control de acceso a conexiones, haga clic en **Agregar**.
8. En el cuadro de diálogo **Agregar configuración - Control de acceso a la conexión**, en **Valor, seleccione Solo conexiones de Citrix Access Gateway** y, a continuación, haga clic en **Aceptar**.
9. Haga clic en **Siguiente dos veces** y, a continuación, haga clic en **Crear**. Citrix Virtual Apps crea la directiva.

### Para configurar las propiedades del servidor de Citrix Virtual Desktops para aceptar conexiones redirigidas solo a través de NetScaler Gateway

Puede restringir el acceso a las máquinas de un grupo de entrega. Puede restringir el acceso de los usuarios mediante SmartAccess que filtra las conexiones de usuario realizadas a través de NetScaler Gateway. Puede realizar esta tarea en el nodo Directiva de Studio o mediante la configuración de directivas como se describe en la tabla de referencia rápida.

1. En Studio, en Grupos de entrega, seleccione el grupo de entrega que quiera restringir.
2. Haga clic en Modificar grupo de entrega y, a continuación, en Directiva de acceso
3. En la página Directiva de acceso, seleccione Conexiones a través de NetScaler Gateway. Solo se permiten las conexiones a través de NetScaler Gateway.
4. Para elegir un subconjunto de esas conexiones, seleccione Conexiones que cumplen cualquiera de los siguientes filtros:

    a) Defina el sitio de NetScaler Gateway.
    b) Agregue, modifique o elimine las cadenas SmartAccess que definen los casos de acceso de usuario permitidos para el grupo de entrega. Para obtener más información sobre cómo configurar SmartAccess, consulte Configuración de SmartAccess en NetScaler Gateway.

## Configurar la comunicación con la Interfaz Web

January 26, 2024

Puede configurar NetScaler Gateway para que se comunique con la interfaz web que se ejecuta en Citrix Virtual Apps and Desktops. Para ello, configure un servidor virtual en NetScaler Gateway. A continuación, vincule un certificado de servidor firmado y directivas de autenticación, sesión, autenticación previa y versiones posteriores al servidor virtual. NetScaler Gateway utiliza la dirección IP del servidor virtual para redirigir las conexiones de usuario a la interfaz web.

El Asistente para aplicaciones publicadas permite configurar NetScaler Gateway para redirigir las conexiones de usuario a la interfaz web. NetScaler Gateway utiliza Secure Ticket Authority (STA) para las conexiones de usuario.

## Configurar directivas para aplicaciones publicadas y escritorios

March 27, 2024

Para establecer comunicación con los servidores de Citrix Virtual Apps and Desktops, debe configurar NetScaler Gateway para que reconozca los servidores. Puede configurar la configuración de forma global o utilizar directivas vinculadas a usuarios, grupos o servidores virtuales.

### Para configurar la interfaz web de forma global en NetScaler Gateway

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En el cuadro de diálogo Configuración global de NetScaler Gateway, en la ficha Experiencia del cliente, haga lo siguiente:
   a) En tipo plug-in, selecciona Java.
   b) En Acceso sin cliente, selecciona Permitir.

      > **Nota**: Realice el paso 3 para admitir Citrix Receiver compatible con VPN, como Receiver para iOS o Receiver para Android. Para admitir Receiver para dispositivos móviles, debe instalar como mínimo Access Gateway 10, compilación 69.6, o Access Gateway 10, compilación 71.6014.e. Si ejecuta Access Gateway 9.3, no es necesario realizar este paso.

4. En la ficha Aplicaciones publicadas, junto a Proxy ICA, seleccione ACTIVADO.

5. Junto a Dirección de interfaz Web, escriba la dirección web de la Interfaz Web y, a continuación, haga clic en **Aceptar**.

### Para configurar una directiva de sesión para la interfaz web

Puede configurar una directiva de sesión y vincularla a un servidor virtual para limitar el acceso a la interfaz web.

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Políticas de Citrix Gateway y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En el cuadro de diálogo Crear directiva de sesión, en Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En el cuadro de diálogo Crear perfil de sesión, en Nombre, escriba un nombre para el perfil.
6. En la ficha Experiencia del cliente, haga lo siguiente:
    a) Junto al tipo de plug-in, selecciona Supedición global y, a continuación, selecciona Java.
    b) Junto a Acceso sin cliente, selecciona Sobrescribir global y, a continuación, selecciona Permitir.
7. Junto a Proxy ICA, haga clic en Supedición global y seleccione ACTIVADO.
8. Junto a Dirección de interfaz Web, haga clic en Anular Global, escriba la dirección web de la Interfaz Web y, a continuación, haga clic en Crear.
9. En el cuadro de diálogo Crear política de sesión , junto a Expresiones con nombre , seleccione General, seleccione Valor verdadero , haga clic en Agregar expresión , en Crear y, a continuación, en Cerrar .

Después de crear una directiva de sesión, enlaza la directiva a un servidor virtual.

### Para enlazar una directiva de sesión a un servidor virtual

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en Abrir .
3. En la ficha Directivas, haga clic en Sesión y, a continuación, en Insertar directiva.
4. Seleccione una directiva de sesión de la lista, introduzca el número de prioridad (opcional) y, a continuación, haga clic en Aceptar

## Configurar parámetros con el asistente de aplicaciones publicadas

March 27, 2024

Para configurar NetScaler Gateway con la interfaz web, necesita la siguiente información:

- Direcciones IP de los servidores que ejecutan Citrix Virtual Apps and Desktops.
- Nombre de dominio completo (FQDN) del servidor que ejecuta la interfaz web.
- Servidor virtual configurado en NetScaler Gateway.
- Directiva de sesión configurada para SmartAccess.
- Direcciones IP de servidores adicionales que ejecutan la interfaz web si está configurando la conmutación por error de la interfaz web.

### Para configurar la configuración de la interfaz web mediante el asistente Aplicaciones publicadas

1. En la utilidad de configuración, haga clic en la pestaña Configuración y, a continuación, en el panel de navegación, haga clic en Citrix Gateway .
2. En el panel de detalles, en Introducción, haga clic en Asistente para aplicaciones publicadas.
3. Haga clic en Siguiente y, a continuación, siga las instrucciones del asistente.

Puede configurar y activar Secure Ticket Authority (STA) desde el asistente Aplicaciones publicadas. Al completar el asistente Aplicaciones publicadas, la configuración se enlazará de forma global.

## Configurar Secure Ticket Authority en NetScaler Gateway

March 27, 2024

Secure Ticket Authority (STA) es responsable de emitir vales de sesión en respuesta a las solicitudes de conexión de aplicaciones publicadas en Citrix Virtual Apps y escritorios publicados en Citrix Virtual Desktops. Estos tíquets de sesión constituyen la base de la autenticación y autorización para acceder a los recursos publicados.

Puede enlazar el STA de forma global o a servidores virtuales. También puede agregar varios servidores que ejecutan STA cuando configura un servidor virtual.

Si está protegiendo las comunicaciones entre NetScaler Gateway y STA, asegúrese de que haya instalado un certificado de servidor en el servidor que ejecuta STA.

En una implementación típica de NetScaler Gateway GSLB, todos los servidores virtuales de puerta de enlace (en cada sitio) deben configurarse con los mismos servidores STA back-end para evitar problemas de reconexión.

### Para enlazar el STA globalmente

1. Vaya a **Citrix Gateway > Configuración global**.
2. En el panel de detalles, en Servidores, haga clic en Vincular o desvincular los **servidores STA** que utilizará Secure Ticket Authority.
3. En el cuadro de diálogo **Enlazar/desenlazar servidores STA**, haga clic en **Agregar**.
4. En el cuadro de diálogo **Configurar servidor STA**, introduzca la dirección URL del servidor STA, haga clic en **Crear** y, a continuación, haga clic en **Aceptar**.
5. En el cuadro de diálogo **Servidor STA** , en URL, escriba la dirección IP o el nombre de dominio completo (FQDN) del servidor que ejecuta STA y, a continuación, haga clic en **Crear** .

   > **Nota**:
   > Puede agregar a la lista más de un servidor que ejecute STA. Los STA que aparecen en la interfaz web deben coincidir con los STA configurados en NetScaler Gateway. Si va a configurar varios STA, no utilice el equilibrio de carga entre NetScaler Gateway y los servidores que ejecutan STA.

### Para enlazar un STA al servidor virtual

1. Vaya a **NetScaler Gateway > Servidores virtuales**.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en **Modificar**.
3. En la ficha **Aplicaciones publicadas**, en Secure Ticket Authority, haga clic en **Agregar**.
4. En el cuadro de diálogo **Configurar servidor STA**, introduzca la dirección URL del servidor STA y, a continuación, haga clic en **Crear**.
5. Repita el paso 4 para agregar servidores STA adicionales y, a continuación, haga clic en **Aceptar.**

### Referencias

- Para obtener más información sobre STA, consulte el artículo NetScaler Gateway Secure Ticket Authority.
- Para obtener más información sobre cómo configurar NetScaler Gateway para utilizar un Cloud Connector como servidor de Secure Ticket Authority (STA), consulte Cómo configuro NetScaler Gateway para que use un Cloud Connector como STA.

# Configurar opciones adicionales de la Interfaz Web en NetScaler Gateway

January 26, 2024

Si implementa NetScaler Gateway en un entorno de interfaz web, puede completar las siguientes tareas opcionales:

- Configuración de conmutación por error de la interfaz web Configure NetScaler Gateway para conmutar por error a un servidor secundario que ejecuta la interfaz web.
- Configuración del acceso mediante tarjeta inteligente con la interfazweb Configure las sesiones de usuario para iniciar sesión directamente en la interfaz web mediante Citrix Receiver y la autenticación con tarjeta inteligente.

## Configurar la conmutación por error de la Interfaz Web

March 27, 2024

Puede utilizar el Asistente para aplicaciones publicadas para configurar NetScaler Gateway para que conmute por error a un servidor secundario que ejecute la Interfaz Web.

La conmutación por error de la interfaz web permite que las conexiones de usuario permanezcan activas si falla la interfaz web principal. Al configurar la conmutación por error, define una nueva dirección IP además de la dirección IP del sistema, la dirección IP asignada o la dirección IP del servidor virtual. La nueva dirección IP debe estar en la misma subred que el sistema o la dirección IP asignada.

Al configurar la conmutación por error de la interfaz web en NetScaler Gateway, todo el tráfico de red que se envía a la nueva dirección IP se transmite a la interfaz web principal. El servidor virtual que selecciona en el asistente Aplicaciones publicadas sirve como dirección IP de traducción de direcciones de red (NAT). La dirección IP real es la de la interfaz web. Si la interfaz web principal falla, el tráfico de red se envía a la interfaz web secundaria.

### Para configurar la conmutación por error de interfaz web

1. En la utilidad de configuración, haga clic en la pestaña Configuración y, a continuación, en el panel de navegación, haga clic en Citrix Gateway .
2. En el panel de detalles, en Introducción, haga clic en Asistente para aplicaciones publicadas.
3. Haga clic en Siguiente, seleccione un servidor virtual y, a continuación, haga clic en Siguiente.

4. En la página Configurar conexiones de cliente, haga clic en Configurar conmutación por error de interfaz web.
5. En Interfaz web principal, en Servidor de interfaz web, escriba la dirección IP de la interfaz web principal.
6. En Puerto del servidor de interfaz web, escriba el número de puerto de la interfaz web principal.
7. En IP del servidor virtual, escriba la nueva dirección IP para la conmutación por error.
8. En Puerto del servidor virtual, introduzca el número de puerto del servidor virtual.
9. En Interfaz web de copia de seguridad, en Servidor de interfaz web, escriba la dirección IP del servidor que ejecuta la interfaz web o seleccione un servidor de la lista.
10. En Puerto del servidor de interfaz web, escriba el número de puerto de la interfaz web y, a continuación, haga clic en Aceptar.
11. Haga clic en Siguiente y, a continuación, siga las instrucciones para completar el asistente.

## Configurar el acceso de tarjetas inteligentes con la Interfaz Web

January 26, 2024

Al configurar la Interfaz Web para utilizar la autenticación con tarjeta inteligente, puede configurar los siguientes casos de implementación para integrar NetScaler Gateway, según cómo inicien sesión los usuarios:

- Si los usuarios inician sesión directamente en la Interfaz Web mediante Citrix Receiver y la autenticación con tarjeta inteligente, la Interfaz Web debe estar en paralelo a Citrix Gateway en la DMZ. El servidor que ejecuta la Interfaz Web también debe ser miembro del dominio.

  En este caso, tanto NetScaler Gateway como la Interfaz Web realizan la terminación de SSL. La Interfaz Web finaliza el tráfico HTTP seguro, incluida la autenticación de usuarios, la visualización de aplicaciones publicadas y el inicio de aplicaciones publicadas. NetScaler Gateway finaliza SSL para las conexiones ICA entrantes.

- Si los usuarios inician sesión con el plug-in de NetScaler Gateway, NetScaler Gateway realiza la autenticación inicial. Cuando NetScaler Gateway establece el túnel VPN, los usuarios pueden iniciar sesión en la Interfaz Web mediante la tarjeta inteligente. En este caso, puede instalar la Interfaz Web detrás de NetScaler Gateway en la DMZ o en la red segura.

> **Nota**:
> NetScaler Gateway también puede utilizar la tarjeta inteligente para la autenticación mediante un certificado de cliente.

Para obtener más información, consulte
Configuración de la autenticación de tarjeta inteligente

# Configurar el acceso a aplicaciones y escritorios virtuales en la Interfaz Web

March 27, 2024

Puede configurar NetScaler Gateway para que los usuarios tengan acceso a aplicaciones publicadas y escritorios virtuales con el plug-in de NetScaler Gateway en lugar de con Receiver. Para configurar el acceso a aplicaciones y escritorios, cambie la configuración de NetScaler Gateway de usar Receiver solo para conectarse a NetScaler Gateway, a una configuración que habilite las conexiones mediante el plug-in de NetScaler Gateway con inicio de sesión único en la Interfaz Web. Por ejemplo, puede configurar NetScaler Gateway para que todos los usuarios se conecten con el plug-in de NetScaler Gateway y utilicen la Interfaz Web como página principal. Este caso admite el inicio de sesión único en la Interfaz Web.

Además del acceso a aplicaciones y escritorios, los usuarios también pueden ejecutar aplicaciones instaladas en el dispositivo del usuario que realizan conexiones de red a través del túnel VPN.

Para iniciar la configuración, siga las siguientes pautas:

- Cree un sitio de Interfaz Web.
- Configure los ajustes de control de acceso avanzado.
- Configure SmartAccess.
- Configure el análisis de dispositivos de punto final en NetScaler Gateway.
- Configure directivas y filtros en Citrix Virtual Apps and Desktops.
- Configure NetScaler Gateway para que los usuarios inicien sesión mediante el plug-in de NetScaler Gateway para acceder a aplicaciones publicadas y escritorios virtuales.

Para obtener más información, consulte los siguientes temas de la documentación del producto Citrix:

- Configuración de un sitio de Interfaz Web.
- Cómo funciona SmartAccess para Citrix Virtual Apps and Desktops
- Configuración de directivas de dispositivos de punto final
- Configuración de directivas y filtros de Citrix Virtual Apps
- Para configurar directivas y filtros en Citrix Virtual Desktops 5
- Configuración de NetScaler Gateway para comunicarse con la Interfaz Web

Al configurar el inicio de sesión de usuario en Citrix Virtual Apps and Desktop, primero debe crear un perfil de sesión para seleccionar el plug-in de NetScaler Gateway para Windows. A continuación, crea un perfil para las aplicaciones de intranet para acceder a Citrix Virtual Apps, Citrix Virtual Desktops y la Interfaz Web.

### Para configurar la configuración global del plug-in de NetScaler Gateway para acceder a aplicaciones y escritorios

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Global Settings.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Aplicaciones publicadas, junto a Proxy ICA, seleccione DESACTIVADO.
4. En Dirección de Interfaz Web, escriba la dirección URL del sitio de Interfaz Web. Esta se convierte en la página principal de los usuarios.
5. En Dominio de inicio de sesión único, escriba el nombre de dominio de Active Directory.
6. En la ficha Experiencia del cliente, junto a Tipo de complemento, seleccione Windows/Mac OS X y, a continuación, haga clic en Aceptar.

### Para configurar la aplicación de intranet

1. En la pestaña Configuración, expanda **Citrix Gateway > Recursos y, a continuación,** haga clic en **Aplicaciones de intranet** .
2. En el panel de detalles, haga clic en **Agregar**.
3. En Nombre, escriba un nombre para la aplicación.
4. Pulse en **Transparente**.
5. En Protocolo, seleccione TCP, UDP o Cualquiera.
6. En Tipo de destino , seleccione Dirección IP y máscara de red . Por ejemplo, escriba 172.16.100.0 y la máscara de subred 255.255.255.0 para representar a todos los servidores de la subred 172.16.100.x. La dirección IP de la Interfaz Web, Citrix Virtual Apps y todos los demás servidores a los que se conectan los usuarios deben estar en una de las subredes definidas como aplicación de intranet.

   Después de crear la aplicación de intranet, puede vincularla de forma global o a un servidor virtual.
7. En Dirección IP y máscara de red, escriba la dirección IP y la máscara de subred que representan la red interna, haga clic en **Crear y,** a continuación, en **Cerrar**.

   Después de crear la aplicación de intranet, puede vincularla de forma global o a un servidor virtual.

### Para enlazar una aplicación de intranet de forma global

1. En la pestaña Configuración, expanda **Citrix Gateway > Configuración global** .

2. En el panel de detalles, en Aplicaciones de intranet, haga clic en **Crear asignaciones a aplicaciones TCP en la red segura para el complemento Citrix Gateway para Java**.
3. En el cuadro de diálogo Configurar aplicaciones de intranet VPN, haga clic en **Agregar** .
4. En Disponible, seleccione una o más aplicaciones de intranet, haga clic en la flecha para mover las aplicaciones de intranet a Configuradas y, a continuación, haga clic **en**Aceptar.

### Para enlazar una aplicación de intranet a un servidor virtual

1. En la pestaña Configuración, expanda **Citrix Gateway > Servidores virtuales** .
2. En el panel de detalles, seleccione un servidor virtual y haga clic en **Open**.
3. En el cuadro de diálogo Configurar el servidor virtual Citrix Gateway, haga clic en la pestaña **Aplicaciones de intranet** .
4. En Nombre de la aplicación disponible, seleccione las aplicaciones de intranet, haga clic en **Agregary**, a continuación, en Aceptar .

Cuando los usuarios inician sesión con el complemento Citrix Gateway, se establece el túnel VPN y se utiliza Receiver o la Interfaz Web como página principal.

## Configurar SmartAccess

January 26, 2024

Puede utilizar SmartAccess con Citrix Virtual Apps and Desktops para entregar de forma inteligente aplicaciones publicadas y escritorios virtuales a los usuarios.

SmartAccess le permite controlar el acceso a aplicaciones y escritorios publicados en un servidor mediante directivas de sesión de NetScaler Gateway. Las comprobaciones previas y versiones posteriores a la autenticación se utilizan como condición, junto con otras condiciones, para acceder a los recursos publicados. Otras condiciones incluyen todo lo que se puede controlar con una directiva de Citrix Virtual Apps and Desktops, como límites de ancho de banda de la impresora, asignación de unidades de dispositivo de usuario, portapapeles, audio y asignación de impresoras. Puede aplicar una directiva de Citrix Virtual Apps and Desktops en función de si los usuarios pasan una comprobación de NetScaler Gateway.

NetScaler Gateway puede ofrecer Citrix Virtual Desktops mediante las mismas opciones disponibles con la Interfaz Web, el acceso al proxy ICA, el acceso sin cliente y el acceso a NetScaler Gateway.

Esta funcionalidad se consigue mediante la integración de los componentes de NetScaler Gateway con la Interfaz Web y Citrix Virtual Apps and Desktops. Esta integración proporciona opciones de autenticación avanzada y control de acceso a la Interfaz Web. Para obtener más información, consulte la documentación de la Interfaz Web en el nodo Tecnologías de la documentación del producto Citrix.

La conectividad remota a una comunidad de servidores no requiere el plug-in de NetScaler Gateway. Los usuarios pueden conectarse con Citrix Receiver. Los usuarios pueden utilizar el plug-in de NetScaler Gateway para iniciar sesión y recibir sus aplicaciones publicadas y escritorios virtuales a través de Access Interface, que es la página principal predeterminada de NetScaler Gateway.

## Cómo funciona SmartAccess para Citrix Virtual Apps and Desktops

January 26, 2024

Para configurar SmartAccess, debe configurar los ajustes de NetScaler Gateway en la interfaz Web/StoreFront y configurar las directivas de sesión en NetScaler Gateway. Al ejecutar el Asistente para aplicaciones publicadas, puede seleccionar las directivas de sesión que ha creado para SmartAccess.

Después de configurar SmartAccess, la función funciona de la siguiente manera:

1. Cuando un usuario escribe la dirección web de un servidor virtual en un explorador web, todas las directivas de autenticación previa que haya configurado se descargan en el dispositivo del usuario.
2. NetScaler Gateway envía los nombres de las directivas de sesión y autenticación previa a la interfaz Web/StoreFront como filtros. Si la condición de directiva se establece en true, la directiva siempre se envía como nombre de filtro. Si no se cumple la condición de la directiva, no se envía el nombre del filtro. Esto le permite diferenciar la lista de aplicaciones y escritorios publicados y las directivas efectivas de un equipo que ejecuta Citrix Virtual Apps and Desktops, en función de los resultados del análisis de endpoints.
3. La interfaz web/StoreFront se pone en contacto con el servidor Citrix Virtual Apps and Desktops y devuelve la lista de recursos publicada al usuario. Los recursos que tienen filtros aplicados no aparecen en la lista del usuario a menos que se cumpla la condición del filtro.

Puede configurar el análisis de puntos finales de SmartAccess en NetScaler Gateway. Para configurar el análisis de terminales, cree una política de sesión que habilite la configuración del **proxy ICA** y, a continuación, configure una cadena de seguridad del cliente.

Cuando el usuario inicia sesión, la directiva de análisis de endpoints ejecuta una comprobación de seguridad del dispositivo de usuario con las cadenas de seguridad del cliente configuradas en NetScaler Gateway.

Por ejemplo, quiere comprobar si hay una versión específica de Sophos Antivirus. En el editor de expresiones, las cadenas de seguridad del cliente aparecen como:

```
client.application.av(sophos).version == 10.0.2
<!--NeedCopy-->
```

Después de configurar la directiva de sesión, enlaza a un usuario, grupo o servidor virtual. Cuando los usuarios inician sesión, se inicia la comprobación de directivas de SmartAccess y comprueba si el dispositivo del usuario tiene instalada la versión 10.0.2 o posterior de Sophos Antivirus.

Cuando la comprobación del análisis del endpoint de SmartAccess se realiza correctamente, el portal de Interfaz Web/StoreFront aparece en una sesión sin cliente. De lo contrario, aparece la interfaz de acceso.

Al crear una directiva de sesión para SmartAccess, el perfil de sesión no tiene ninguna configuración configurada, lo que crea un perfil nulo. En este caso, NetScaler Gateway utiliza la interfaz web/URL de StoreFront configurada globalmente para SmartAccess.

## Configuración de directivas y filtros de Citrix Virtual Apps

January 26, 2024

Después de crear la directiva de sesión en NetScaler Gateway, se configuran las directivas y los filtros en el equipo que ejecuta Citrix Virtual Apps. Las directivas y los filtros se aplican a los usuarios de acuerdo con la configuración del análisis de endpoint.

**Referencias:**

- Para obtener información sobre cómo restringir el acceso de los usuarios mediante expresiones y filtros de directivas de SmartAccess, consulte Administrar grupos de entrega.
- Para obtener información sobre cómo configurar las directivas y los filtros de Citrix Virtual Apps, consulte Crear directivas.

## Para configurar una directiva de sesión para SmartAccess

March 27, 2024

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En el cuadro de diálogo Crear directiva de sesión, en Nombre, escriba un nombre para la directiva, como ValidEndPoint.
4. En Perfil de solicitud, haga clic en Nuevo y, en Nombre, escriba un nombre para el perfil, como Nulo y, a continuación, haga clic en Crear.

5. En el cuadro de diálogo Crear directiva de sesión, cree una expresión de seguridad del cliente, haga clic en Crear y, a continuación, en Cerrar.

La expresión de seguridad del cliente se utiliza para diferenciar entre puntos finales válidos y no válidos. Puede proporcionar distintos niveles de acceso a aplicaciones o escritorios publicados en función de los resultados del análisis de endpoints.

Después de crear la directiva de sesión, enlaza la directiva de forma global o a un servidor virtual.

## Configurar la asignación de dispositivos de usuario en Citrix Virtual Apps

January 26, 2024

Puede utilizar filtros de NetScaler Gateway que se aplican a las directivas de un equipo que ejecuta Citrix Virtual Apps. Los filtros proporcionan a los usuarios acceso a las capacidades de Citrix Virtual Apps, como la asignación de unidades de dispositivos de usuario, asignación de impresoras o asignación del portapapeles según los resultados del análisis de endpoints.

Citrix Receiver admite la asignación de dispositivos en dispositivos de usuario para que los usuarios puedan acceder a dispositivos externos dentro de las sesiones de usuario. La asignación de dispositivos de usuario proporciona:

- Acceso a unidades y puertos locales
- Transferencia de datos de cortar y pegar entre una sesión de usuario y el portapapeles local
- Reproducción de audio (sonidos del sistema y archivos.wav) de la sesión de usuario

Durante el inicio de sesión, el dispositivo del usuario informa al servidor de las unidades de usuario y los puertos COM disponibles. En Citrix Virtual Apps 6.5, las unidades de usuario se asignan al servidor y utilizan la letra de unidad del dispositivo de usuario. Estas asignaciones están disponibles solamente para el usuario durante la sesión actual. Las asignaciones se eliminan cuando el usuario cierra la sesión y se vuelve a crear la próxima vez que el usuario inicie sesión.

Después de habilitar el servicio XML, debe configurar las directivas para la asignación de dispositivos de usuario.

Para aplicar directivas de asignación de dispositivos de usuario basadas en filtros SmartAccess, debe crear las dos directivas siguientes en el servidor:

- Una directiva ICA restrictiva que inhabilita la asignación de dispositivos de usuario y se aplica a todos los usuarios de NetScaler Gateway.

- Una directiva ICA completa que habilita la asignación de dispositivos de usuario y se aplica únicamente a los usuarios que cumplen la directiva de sesión de análisis de punto final
  Nota: La directiva ICA filtrada no restrictiva debe tener una prioridad mayor que la directiva ICA restrictiva, de modo que cuando se aplica a un usuario, la directiva no restrictiva anula la directiva que inhabilita la asignación de dispositivos de usuario.

Las directivas restrictivas y no restrictivas se configuran en Citrix Virtual Apps 6.5 mediante Citrix AppCenter.

## Para configurar una directiva restrictiva en Citrix Virtual Apps 6.5

March 27, 2024

1. Haga clic en Inicio > Herramientas administrativas > Consolas de administración > Citrix AppCenter.
2. En el panel izquierdo, expanda Citrix Virtual Apps, expanda el servidor y, a continuación, haga clic en Directivas.
3. En el panel Directivas, haga clic en la ficha Usuario y, a continuación, haga clic en Nuevo.
4. En Nombre, escriba un nombre para la directiva y, a continuación, haga clic en Siguiente.
5. En Categorías, haga clic en Toda la configuración.
6. En Configuración, en Unidades cliente de conexión automática, haga clic en Agregar.
7. En el cuadro de diálogo Agregar configuración, haga clic en Inhabilitado, haga clic en Aceptar y, a continuación, haga clic en Siguiente.
8. En Categorías, haga clic en Todos los filtros.
9. En Filtros, en Control de acceso, haga clic en Agregar.
10. En el cuadro de diálogo Nuevo filtro , haga clic en Agregar .
11. En Modo, haga clic en Denegar.
12. En Tipo de conexión, seleccione Con Access Gateway.
13. En AG Farm, escriba el nombre del servidor virtual.
14. En Condición de acceso, escriba o seleccione el nombre de la directiva de sesión configurada en NetScaler Gateway, haga clic en Aceptar dos veces, haga clic en Siguiente y, a continuación, en Crear para completar el asistente.

## Para configurar una directiva no restrictiva en Citrix Virtual Apps 6.5

March 27, 2024

1. Haga clic en Inicio > Herramientas administrativas > Consolas de administración > Citrix App-Center.
2. En el panel izquierdo, expanda Citrix Virtual Apps, expanda el servidor y, a continuación, haga clic en Directivas.
3. En el panel Directivas, haga clic en la ficha Usuario y, a continuación, haga clic en Nuevo.
4. En Nombre, escriba un nombre para la directiva y, a continuación, haga clic en Siguiente.
5. En Categorías, haga clic en Toda la configuración.
6. En Configuración, en Unidades cliente de conexión automática, haga clic en Agregar.
7. Haga clic en Activado, en Aceptar y, a continuación, en Siguiente.
8. En Categorías, haga clic en Todos los filtros.
9. En Filtros, en Control de acceso, haga clic en Agregar.
10. En el cuadro de diálogo Nuevo filtro , haga clic en Agregar .
11. En Modo, haga clic en Permitir.
12. En Tipo de conexión, seleccione Con Access Gateway.
13. En AG Farm, escriba el nombre del servidor virtual.
14. En Condición de acceso, escriba o seleccione el nombre de la directiva de sesión configurada en NetScaler Gateway, haga clic en Aceptar dos veces, haga clic en Siguiente y, a continuación, en Crear para completar el asistente.

## Habilitar Citrix Virtual Apps como método de acceso de cuarentena

January 26, 2024

Si ha configurado el análisis de dispositivos de punto final en NetScaler Gateway, los usuarios que pasan una exploración de dispositivos de punto final pueden acceder a todos los recursos que configure en NetScaler Gateway. Puede poner a los usuarios que no superen un análisis de dispositivos de punto final en un grupo de cuarentena. Estos usuarios solo pueden acceder a las aplicaciones publicadas desde Citrix Virtual Apps. El éxito o el fracaso del análisis de dispositivos de punto final determinan el método de acceso disponible para los usuarios.

Por ejemplo, crea un análisis de punto final para comprobar si el Bloc de notas se está ejecutando o no en el dispositivo del usuario cuando los usuarios inician sesión. Si el Bloc de notas se está ejecutando, los usuarios pueden iniciar sesión con el plug-in de NetScaler Gateway. Si el Bloc de notas no se está ejecutando, los usuarios solo reciben la lista de aplicaciones publicadas.

Para configurar el acceso restringido de los usuarios, cree un grupo de cuarentena en NetScaler Gateway. El grupo de cuarentena se crea dentro de un perfil de sesión y, a continuación, se agrega el perfil a una directiva de sesión.

# Crear una directiva de sesión y una exploración de Endpoint Analysis para un grupo de cuarentena

March 27, 2024

Para habilitar Citrix Virtual Apps como método de acceso a cuarentena, cree un grupo en NetScaler Gateway que utilice como grupo de cuarentena. A continuación, cree una directiva de sesión en la que seleccione el grupo.

Después de crear la directiva de sesión, enlaza la directiva al grupo de cuarentena. Después de configurar las directivas y vincularlas al grupo, pruebe los resultados. Por ejemplo, para que los usuarios inicien sesión correctamente, el Bloc de notas debe estar ejecutándose en el dispositivo del usuario. Si el Bloc de notas se está ejecutando, los usuarios pueden iniciar sesión mediante el plug-in de NetScaler Gateway. Si el Bloc de notas no está en ejecución, los usuarios pueden iniciar sesión con Citrix Receiver.

Para obtener más información sobre cómo configurar directivas de análisis de dispositivos de punto final, consulte Configuración de directivas de endpoint.

## Para crear una exploración de análisis de dispositivos de punto final y agregar un grupo de cuarentena

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Citrix Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En el cuadro de diálogo Crear directiva de sesión, en Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En el cuadro de diálogo Crear perfil de sesión, en Nombre, escriba un nombre para el perfil.
6. En la ficha Seguridad, haga clic en Avanzado.
7. En el cuadro de diálogo Configuración de seguridad - Avanzada, en Seguridad del cliente, haga clic en Supedición global y, a continuación, haga clic en Nuevo.
8. En el cuadro de diálogo Crear expresión, junto a Igualar cualquier expresión, haga clic en Agregar.
9. En Tipo de expresión, seleccione Seguridad del cliente.
10. En Componente, seleccione Proceso.
11. En Nombre, escriba notepad.exe, haga clic en Aceptar y, a continuación, haga clic en Crear.
12. En el cuadro de diálogo Configuración de seguridad - Avanzada, en Grupo de cuarentena, seleccione el grupo de cuarentena, haga clic en Crear, haga clic en Aceptar y, a continuación, haga clic en Crear.

13. En el cuadro de diálogo Crear directiva de sesión, junto a Expresiones con nombre, seleccione Valor verdadero, haga clic en Agregar expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

## Configurar Citrix Virtual Desktops para SmartAccess

January 26, 2024

NetScaler Gateway permite a Citrix Virtual Desktops entregar escritorios seguros a usuarios remotos. Citrix Virtual Desktops puede utilizar las capacidades de SmartAccess de NetScaler Gateway para entregar escritorios de forma inteligente. Cuando utiliza la consola de Delivery Services en Citrix Virtual Desktops para crear grupos de escritorios, configura directivas y filtros para el control de acceso.

Para configurar Citrix Gateway para que entregue escritorios publicados, utilice las mismas opciones que están disponibles en la Interfaz Web, el acceso mediante proxy ICA, el acceso sin cliente y el acceso a Citrix Gateway.

Al crear una directiva de sesión y configurar la configuración en la ficha Aplicaciones publicadas, utilice la dirección web del sitio de Interfaz web de Citrix Virtual Desktops. Después de crear la directiva, enlaza la directiva a un servidor virtual. A continuación, cree un perfil de sesión nula en el que no configure los ajustes. La configuración de la interfaz web se hereda de la configuración global.

## Para configurar una directiva de sesión para SmartAccess con Citrix Virtual Desktops

January 26, 2024

Configurar SmartAccess en NetScaler Gateway para acceder a Citrix Virtual Desktops mediante la creación de una directiva de sesión vinculada a un servidor virtual.

**Para configurar una directiva de sesión para SmartAccess con Citrix Virtual Desktops mediante la interfaz gráfica de usuario:**

1. En la ficha Configuración, vaya a **NetScaler Gateway > Directivas > Sesión**.
2. Haga clic en la ficha **Directivas de sesión** y, a continuación, en **Agregar**
3. En la página Crear directiva de sesión de NetScaler Gateway, introduzca un nombre para la directiva, como Citrix Virtual DesktopsPolicy.
4. En **Perfil**, haga clic en **Agregar**.

5. En la página **Crear perfil de sesión de NetScaler Gateway**, introduzca el nombre del perfil, como Citrix Virtual DesktopsProfile.
6. En la ficha **Aplicaciones publicadas**, junto a **Proxy ICA**, haga clic en **Supedición global** y, a continuación, seleccione **Activado**.
7. En **Dirección de interfaz web**, haga clic en **Supedición global** y, a continuación, escriba la dirección URL del sitio de Interfaz Web de Citrix Virtual Desktops.
8. En **Dominio de inicio de sesión único, haga clic enSupedición global**, escriba el nombre de dominio y, a continuación, haga clic en**Crear**.
9. En la página **Crear directiva de sesión de Citrix**, en **Expresión**, agregue la expresión.

También debe crear una directiva de sesión nula que esté vinculada al servidor virtual. El perfil de sesión no contiene ninguna configuración, lo que lo convierte en un perfil nulo. En la directiva de sesión, agregue la expresión True Value y, a continuación, guarde la directiva.

Después de crear ambas directivas de sesión, vincule ambas directivas al servidor virtual.

## Para configurar directivas y filtros en Citrix Virtual Desktops 5

January 26, 2024

Puede configurar los ajustes en Citrix Virtual Desktops 5 mediante Citrix Studio o el Editor de directivas de grupo. Al configurar la configuración de NetScaler Gateway en Citrix Virtual Desktops, utilice el nombre del servidor virtual de NetScaler Gateway y el nombre de la directiva de sesión. A continuación, configure el control de acceso para permitir que las conexiones cumplan los filtros definidos. También puede utilizar las directivas de SmartAccess.

1. En el servidor Citrix Virtual Desktops, haga clic en **Inicio > Todos los programas > Citrix > Citrix Studio**.
2. En el panel izquierdo, haga clic para expandir **HDX Policy y,** a continuación, haga clic en la pestaña **Usuario** del panel central.
3. En **Usuarios** , haga clic en **Nuevo** .
4. En el cuadro de diálogo **Nueva política** , en Identifique su política y, a continuación, en Nombre, escriba un nombre.
5. Haz clic en **Siguiente** dos veces.
6. En el cuadro de diálogo **Nueva política** , en la pestaña filtros, en Filtros, haga clic en **Control de acceso y,** a continuación, en **Agregar** .
7. En el cuadro de diálogo **Nuevo filtro** , haga clic en **Agregar** .

8. En el cuadro de diálogo **Nuevo elemento de filtro** , en **Tipo de conexión** , seleccione **Con Access Gateway** .

   Para aplicar la directiva a las conexiones realizadas a través de NetScaler Gateway sin tener en cuenta las directivas de NetScaler Gateway, deje las entradas predeterminadas en el nombre de la comunidad AG y en la condición de acceso.

9. Si quiere aplicar la directiva a las conexiones realizadas a través de NetScaler Gateway según las directivas existentes de NetScaler Gateway, haga lo siguiente:

   a) En **AG farm** name , escriba el nombre del servidor virtual.
   b) En **Condición de acceso** , escriba el nombre de la política de sesión o de análisis de terminales.

   > **Importante:** Citrix Virtual Desktops no valida el servidor virtual de NetScaler Gateway, la directiva de análisis de endpoint ni los nombres de directivas de sesión. Asegúrate de que la información sea correcta.

10. Haga clic **en**Aceptar dos veces, en **Siguiente** y, a continuación, en **Crear** .

## Para agregar el Desktop Delivery Controller como STA

March 27, 2024

Para establecer conexiones ICA con Citrix Virtual Desktops, debe agregar la dirección IP de Desktop Delivery Controller al servidor virtual como Secure Ticket Authority (STA).

**Para agregar un Desktop Delivery Controller como STA mediante la GUI:**

1. En la ficha Configuración, vaya a **Citrix Gateway > Servidores virtuales**.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en **Modificar**.
3. En la ficha **Aplicaciones publicadas**, en Secure Ticket Authority, haga clic en **Agregar**.
4. En el cuadro de diálogo **Configurar servidor STA**, introduzca la dirección URL del servidor STA y, a continuación, haga clic en **Crear**.
5. Repita el paso 4 para agregar servidores STA adicionales y, a continuación, haga clic **en**Aceptar .

## Configurar SmartControl

March 27, 2024

SmartControl permite a los administradores definir directivas granulares para configurar y aplicar atributos de entorno de usuario para Citrix Virtual Apps and Desktops en NetScaler Gateway. SmartControl permite a los administradores administrar estas directivas desde una única ubicación, en lugar de hacerlo en cada instancia de estos tipos de servidores.

SmartControl se implementa mediante directivas ICA en NetScaler Gateway. Cada directiva ICA es una combinación de perfiles de expresión y acceso que se puede aplicar a usuarios, grupos, servidores virtuales y de forma global. Las directivas ICA se evalúan después de que el usuario se autentica en el establecimiento de la sesión.

En la tabla siguiente se enumeran los atributos del entorno de usuario que SmartControl puede aplicar:

| | |
|---|---|
| ConnectClientDrives | Especifica la conexión predeterminada a las unidades cliente cuando el usuario inicie sesión. |
| ConnectClientLPTPorts | Especifica la conexión automática de los puertos LPT desde el cliente cuando el usuario inicie sesión. Los puertos LPT son los puertos de impresora local. |
| ClientAudioRedirection | Especifica las aplicaciones alojadas en el servidor para transmitir audio a través de un dispositivo de sonido instalado en el equipo cliente. |
| ClientClipboardRedirection | Especifica y configura el acceso al portapapeles en el dispositivo cliente y asigna el portapapeles en el servidor. |
| ClientCOMPortRedirection | Especifica la redirección del puerto COM hacia y desde el cliente. Los puertos COM son los puertos de comunicación. Los puertos COM son puertos serie. |
| ClientDriveRedirection | Especifica la redirección de unidades hacia y desde el cliente. |
| Multistream | Especifica la función multistream para los usuarios especificados. |
| ClientUSBDeviceRedirection | Especifica la redirección de dispositivos USB hacia y desde el cliente (solo hosts de estación de trabajo). |
| `Localremotedata` | Especifica la capacidad de descarga de carga de archivos HTML5 para la aplicación Citrix Workspace. |
| ClientPrinterRedirection | Especifica las impresoras cliente que se asignarán a un servidor cuando un usuario inicie sesión en una sesión. |
| Directivas | Acción | Perfiles de acceso |
| Agregar | Modificar | Eliminar |
| Mostrar vinculaciones | Administrador de directivas | Acción |

## Directivas

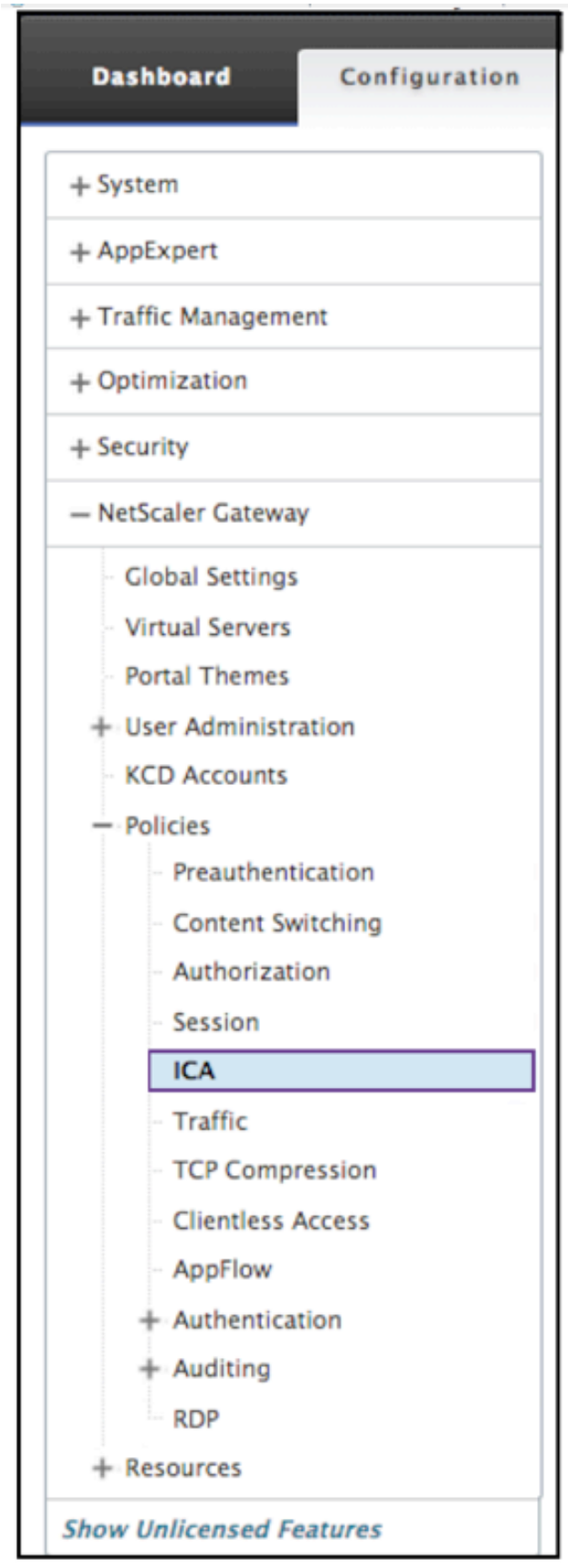
Una directiva ICA especifica una acción, un perfil de acceso, una expresión y, opcionalmente, una acción de registro. Los siguientes comandos están disponibles en la ficha **Directivas**:

- Add
- Edit (Modificar)
- Suprimir
- Mostrar vinculaciones
- Administrador de directivas
- Acción

### Add

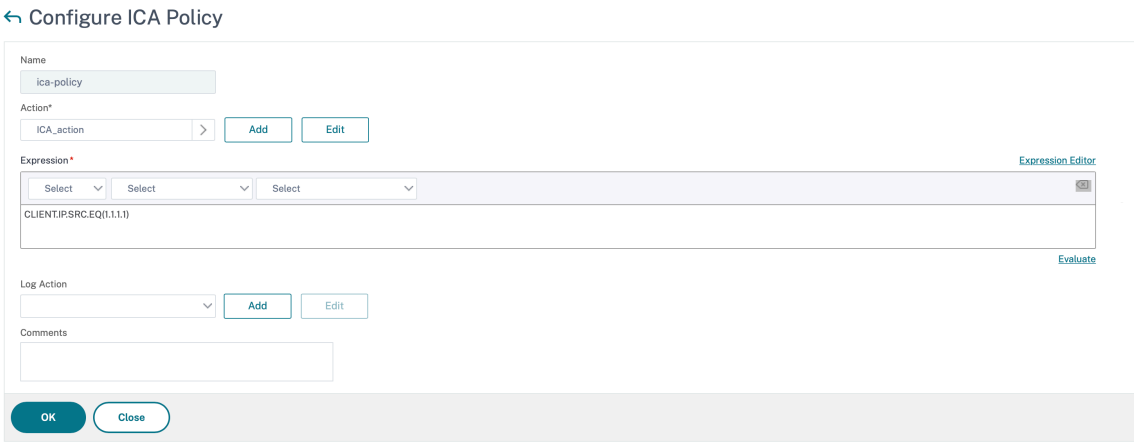
1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.



2. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
3. En el cuadro de diálogo **Nombre**, escriba un nombre para la directiva.

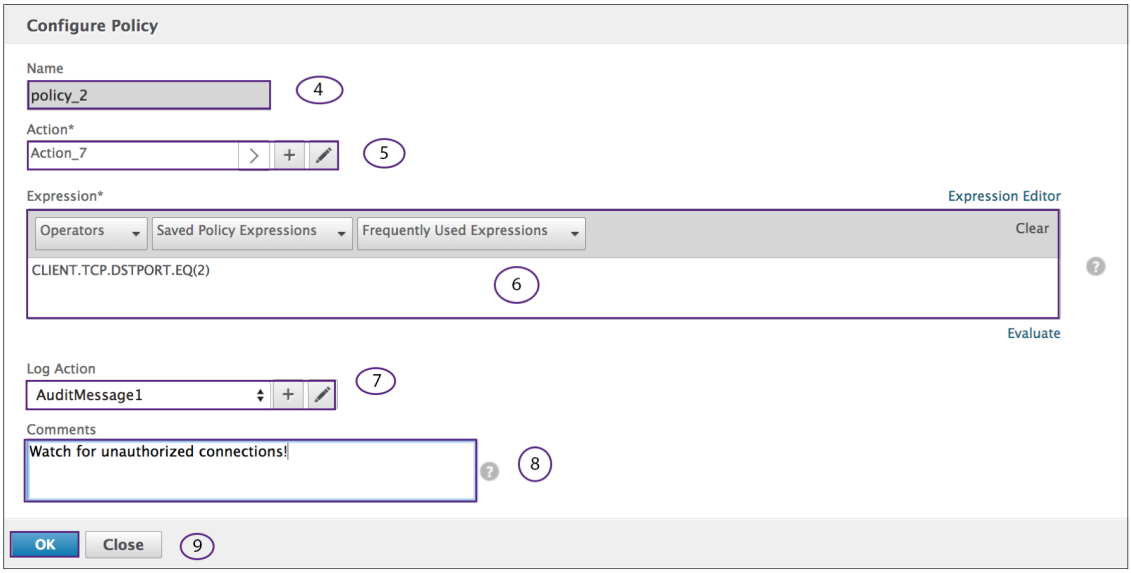



4. Junto a Acción, realiza una de las siguientes acciones:
   - Haga clic en el icono **>** para seleccionar una acción existente. Para obtener más información, consulte [Seleccione una acción] en (#common -processes).
   - Haga clic en el icono **+** para crear una acción. Para obtener más información, consulte [Crear una acción nueva] en (#common -processes).
   - El icono del **lápiz** está inhabilitado.
5. Crea una expresión.
6. Cree una **acción de registro**. Para obtener más información, consulte Crear una acción de registro.
7. Escribe un mensaje en el cuadro Comentarios. El comentario se escribe en el registro de mensajes. Este campo es opcional.
8. Haga clic en **Crear**.

### Edit (Modificar)

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.
2. Seleccione la directiva ICA de la lista.
3. En el panel de detalles, en la ficha **Directivas**, haga clic en **Modificar**.
4. Compruebe el nombre de la directiva.




5. Para revisar la **acción**, realice una de las siguientes acciones:

   - Haga clic en el icono **>** para revisar una**acción** existente. Para obtener más información, consulte [Seleccione una acción] en (#common -processes).
   - Haga clic en el icono **+** para crear una**acción**. Para obtener más información, consulte [Crear una acción nueva] en (#common -processes).
   - Haga clic en el icono del **lápiz** para revisar el [Perfil de acceso].

6. Revise la **expresión** como deba. Para obtener más información, consulte [Expresiones] en (#common -processes).
7. Para revisar la **acción de registro**, realice una de las siguientes acciones:

   - Haga clic en el signo + para crear una **acción de registro**.
   - Haga clic en el icono del **lápiz** para configurar un mensaje de auditoría.

8. Revise los comentarios según lo quiera.
9. Haga clic en **Aceptar**.

### Suprimir

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.
2. Seleccione la directiva ICA deseada de la lista.
3. En el panel de detalles, en la ficha **Directivas**, haga clic en **Eliminar**.
4. Confirme que quiere eliminar la directiva haciendo clic en**Sí**.

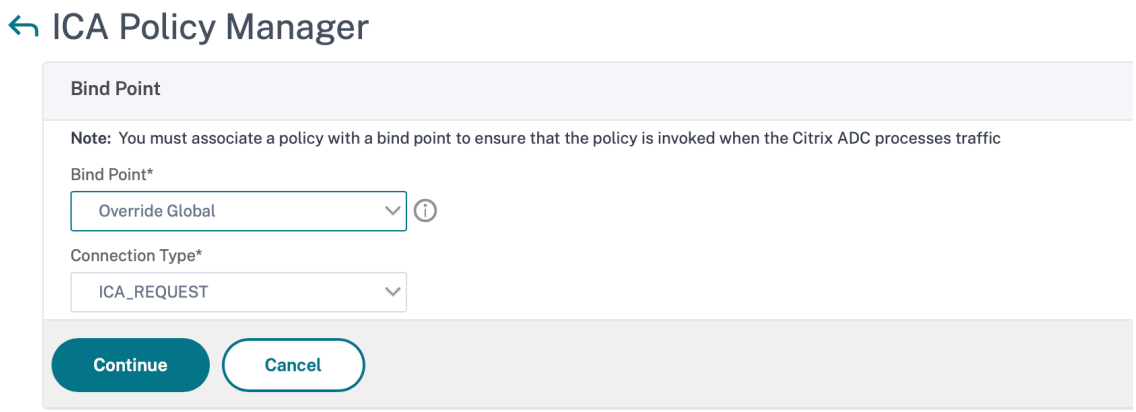
 

### Mostrar vinculación

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.
2. Seleccione la directiva ICA de la lista.
3. En el panel de detalles, en la ficha **Directivas**, haga clic en **Mostrar enlaces**.

### Administrador de directivas

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.
2. Seleccione la directiva ICA deseada de la lista.
3. En el panel de detalles, en la ficha Directivas, haga clic en **Administrador de directivas**
4. En el cuadro de diálogo **Punto de enlace**, seleccione una de las directivas siguientes.
   - Sobrescribir global
   - Servidor virtual VPN
   - Servidor virtual de redirección de caché
   - Global predeterminado
5. En el cuadro de diálogo Tipo de conexión, seleccione una directiva de enlace del menú.
6. Si selecciona el servidor virtual VPN o el servidor virtual de redirección de caché, se conecta al servidor mediante el menú.
7. Haga clic en **Continuar**.

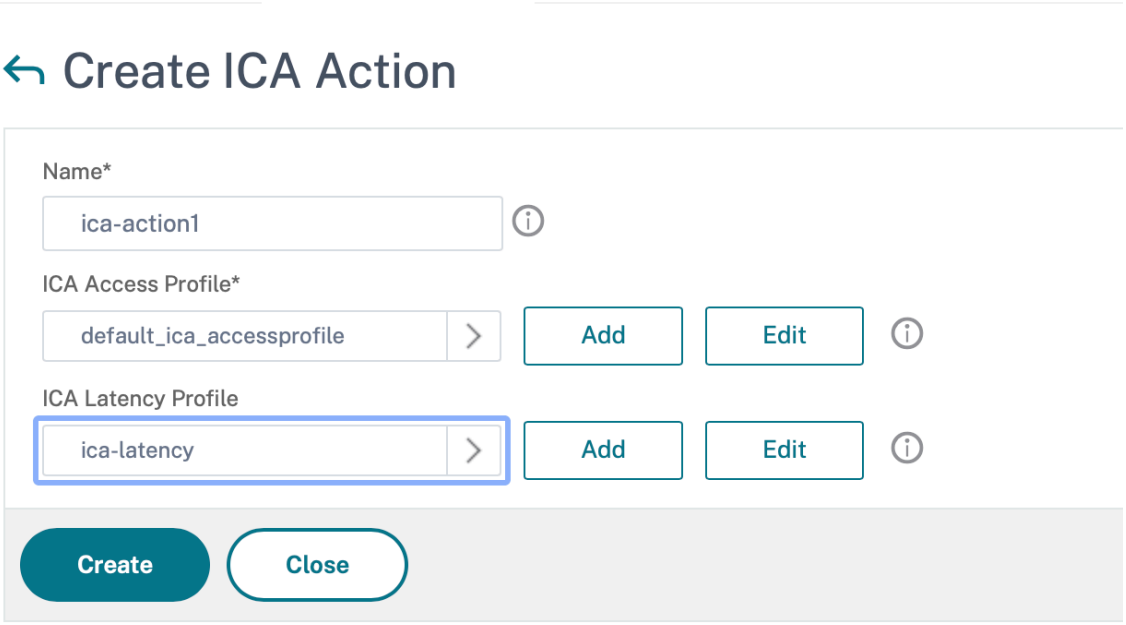



### Agregar vinculación

1. Tras seleccionar Continuar, aparece esta pantalla.
2. Seleccione una directiva para adjuntar el enlace.

3. Selecciona Agregar enlace.

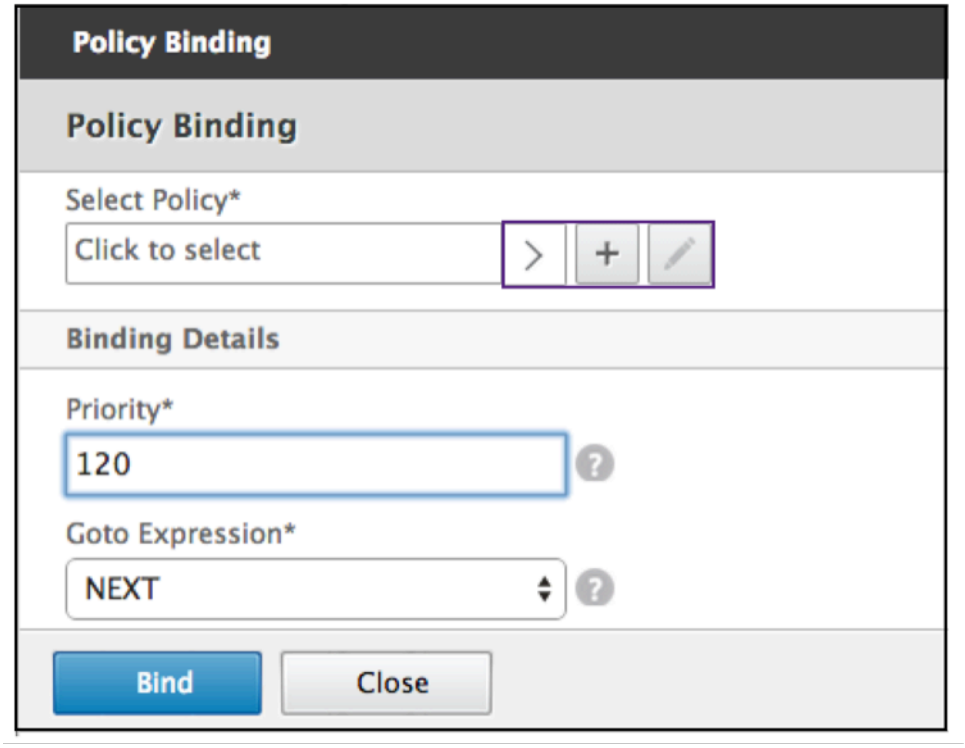



**Vinculación de directivas**

1. Después de seleccionar Listo, aparece esta pantalla.

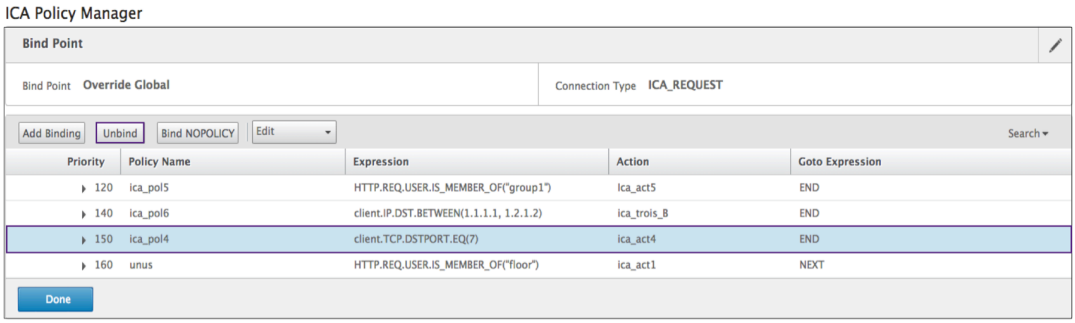
   - Haga clic en el icono**para seleccionar una directiva existente. Para obtener más información, consulteSeleccionar una directiva existente.
   - Haga clic en el icono **+** para crear una política. Para obtener información detallada, consulteCrear una directiva.




**Directiva de desvinculación**

1. Seleccione la directiva que quiere desenlazar y haga clic en el botón **Desenlazar**.

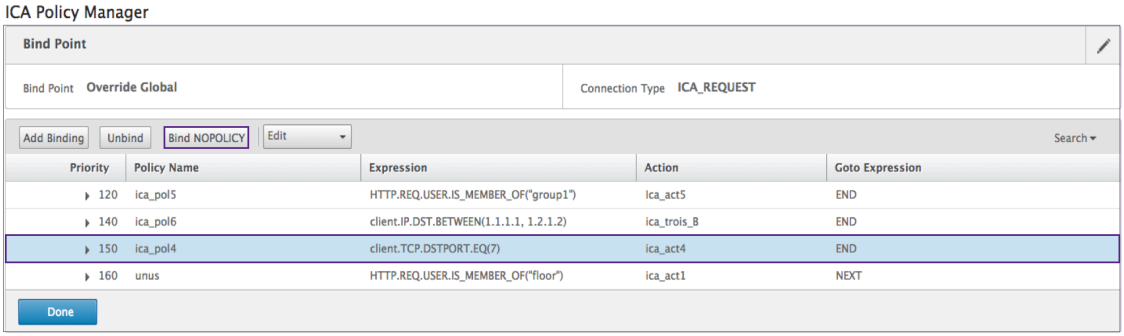



2. Haga clic en **Listo**
3. Haga clic en el botón**Sí**de la pantalla emergente para confirmar que quiere desvincular la entidad seleccionada.

**Enlazar NOPOLICY**

1. Seleccione la directiva que requiera NOPOLICY y haga clic en el botón **Vincular NOPOLICY**.

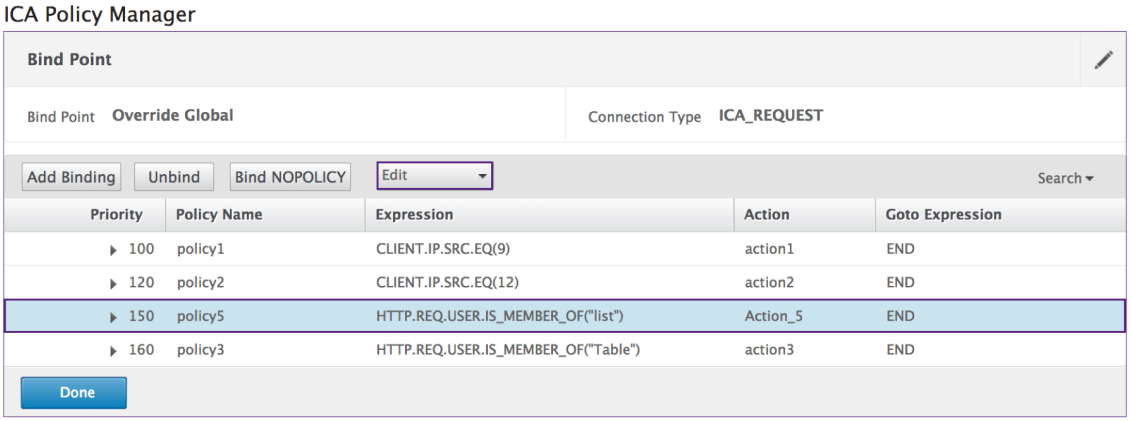



2. Haga clic en **Listo**

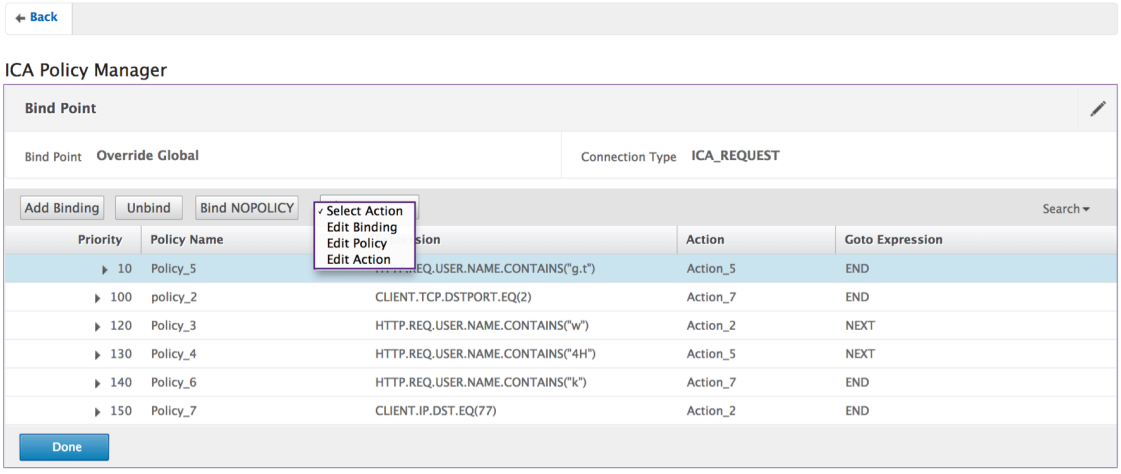
### Edit (Modificar)

Puede modificar desde el Administrador de directivas de ICA.

1. Seleccione la directiva que quiere modificar y, a continuación, seleccione **Modificar**.



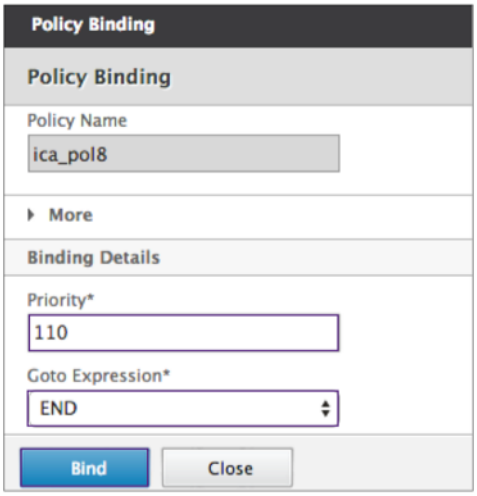

2. Puede realizar las siguientes modificaciones: [**Editar encuadernación]**,**[Editar directiva]**,**[Editar acción]**.



### Modificar enlace

1. Con la directiva seleccionada, haga clic en **Modificar enlace**.
2. Compruebe que está editando la directiva deseada. El nombre de esta directiva no se puede modificar.

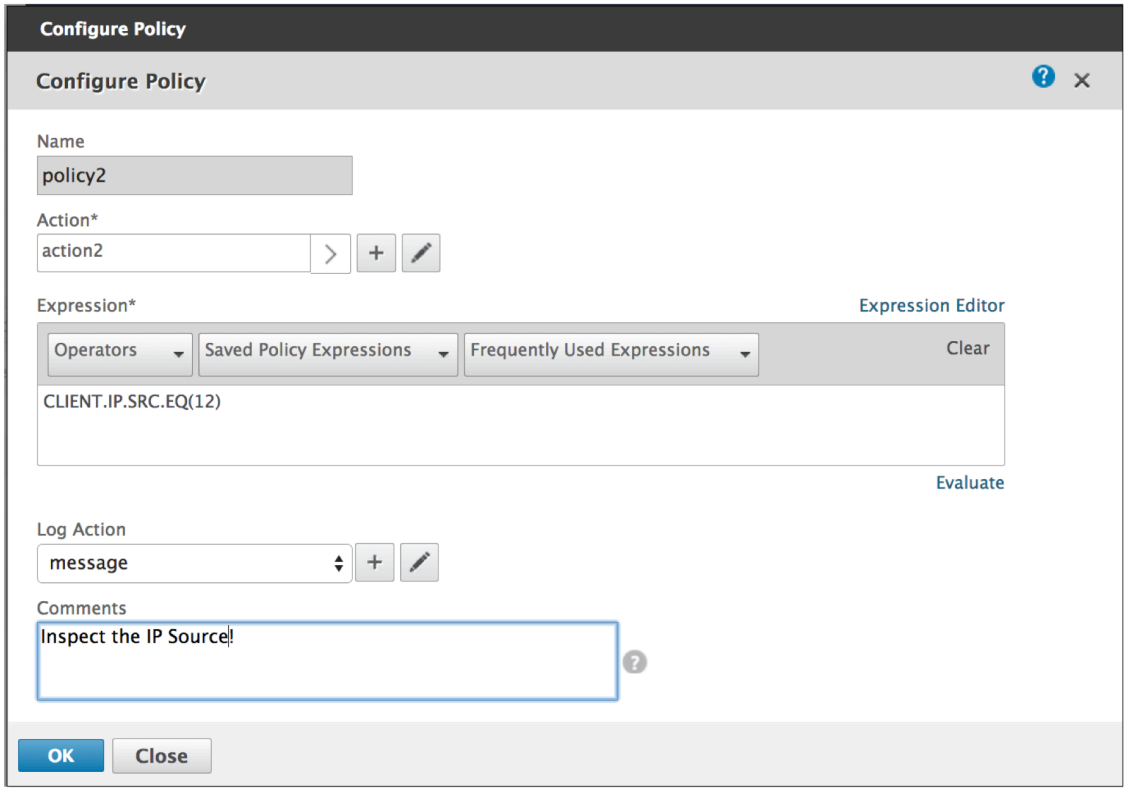



3. Establezca la prioridad según lo quiera.
4. Defina Goto Expresión como quiera.
5. Haga clic en el botón **Vincular**.

### Modificar directiva

1. Con la directiva seleccionada, haga clic en **Modificar directiva**.
2. Compruebe el nombre de la directiva para asegurarse de que está editando la directiva deseada. Este campo no se puede modificar.




3. Para revisar la directiva de acción, realice una de las siguientes acciones:

   - Haga clic en el icono **>** para seleccionar una acción existente. Para obtener más información, consulte [Seleccione una acción] en (#common -processes).
   - Haga clic en el icono **+** para crear una acción. Para obtener más información, consulte [Crear una acción nueva] en (#common -processes).
   - Haga clic en el icono del **lápiz** para revisar el perfil de acceso. Para obtener más información, consulte [Seleccione un perfil de acceso existente] en (#common -processes).

4. Revise la expresión según lo quiera. Para obtener más información, consulte [Expresiones] en (#common -processes).
5. Seleccione el tipo de mensaje deseado en el menú. Para crear una acción de registro, realice una de las siguientes acciones:

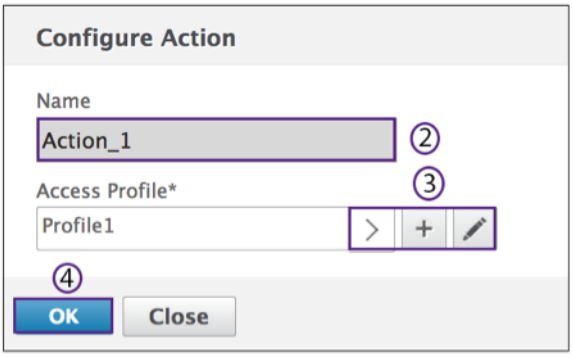
   - Haga clic en el icono **+** para crear una acción. Para obtener más información, consulte Crear una acción de registro.
   - Haga clic en el icono del **lápiz** para revisar la acción Configurar mensaje de auditoría. Para obtener más información, consulte Configurar acción de mensaje de auditoría.

6. Introduzca comentarios sobre la directiva de ICA.
7. Haga clic en **Aceptar** cuando finalice la modificación.

**Acción de modificación**

1. Con la directiva seleccionada, haga clic en**Modificar acción**.
2. Compruebe el nombre de la acción para confirmar que está editando la acción deseada. Este campo no se puede modificar.
3. Junto a Perfil de acceso, realice una de las siguientes acciones:
   - Haga clic en el icono**para seleccionar otro perfil de acceso. Para obtener más información, consulteConfigurar acción.
   - Haga clic en el icono**+**para seleccionar un nuevo perfil de canal.Cree un perfil de acceso.
   - Haga clic en el icono del **lápiz** para revisar el perfil de acceso. Para obtener más información, consulte [Seleccionar un perfil de acceso existente] en (#common-processes).
4. Haga clic en **Aceptar**.

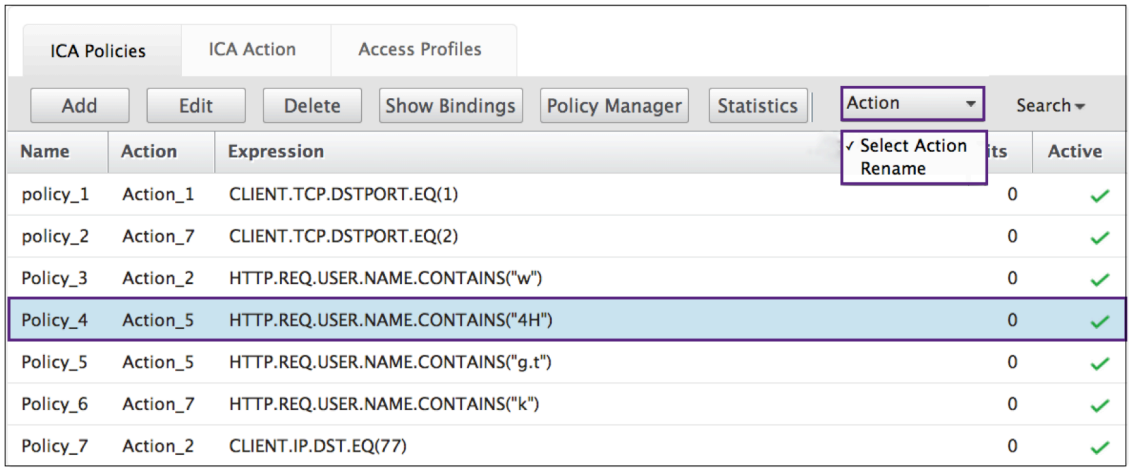



**Acción**

Los comandos **Directivas > Acción** se utilizan para cambiar el nombre de la acción.

1. Seleccione la acción ICA deseada de la lista.
2. En la ficha Directivas ICA, haga clic en **Acción**. Selecciona **Cambiar nombre** en el menú.




3. Cambie el nombre de la acción.
4. Haga clic en **OK**.

### Acción

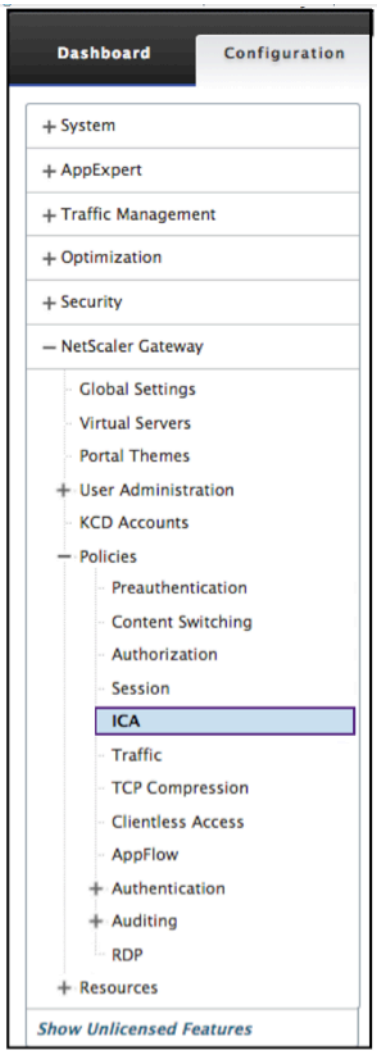
Una acción conecta una directiva con un perfil de acceso. Los siguientes comandos están disponibles en la ficha **Directivas**:

- Add
- Edit (Modificar)
- Suprimir
- Acción

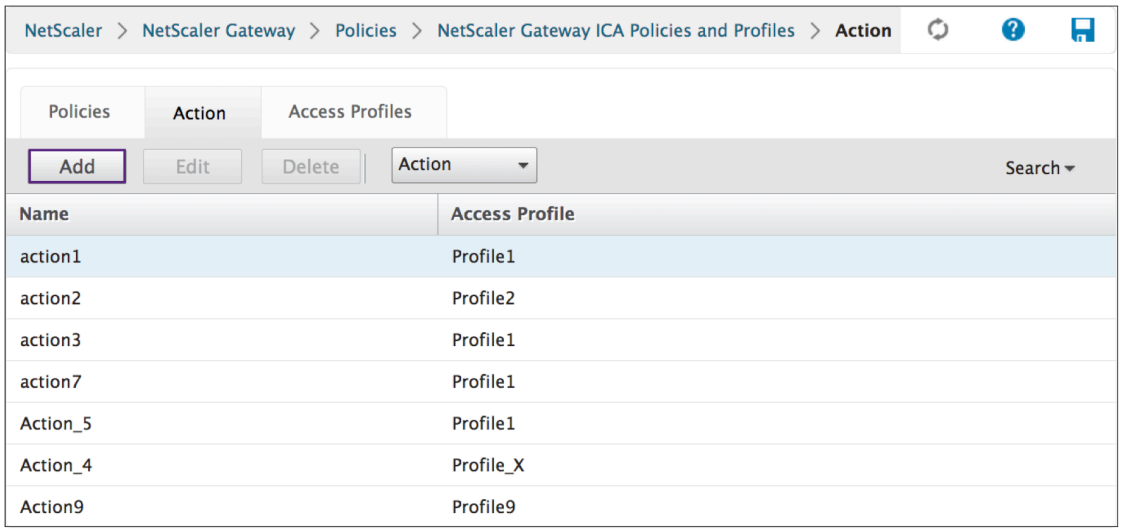
### Add

1. Vaya a **NetScaler Gateway > Acción** y, a continuación, haga clic en **ICA**.



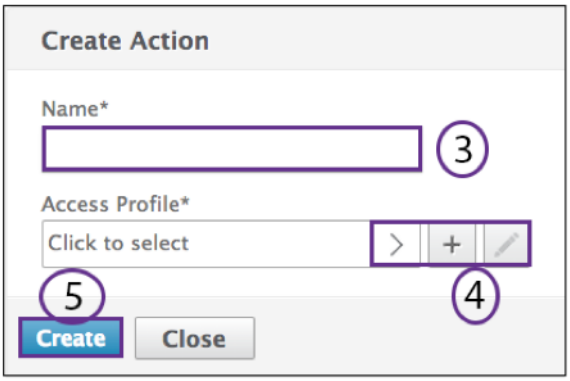

2. En el panel de detalles, en la ficha Acción, haga clic en **Agregar**.



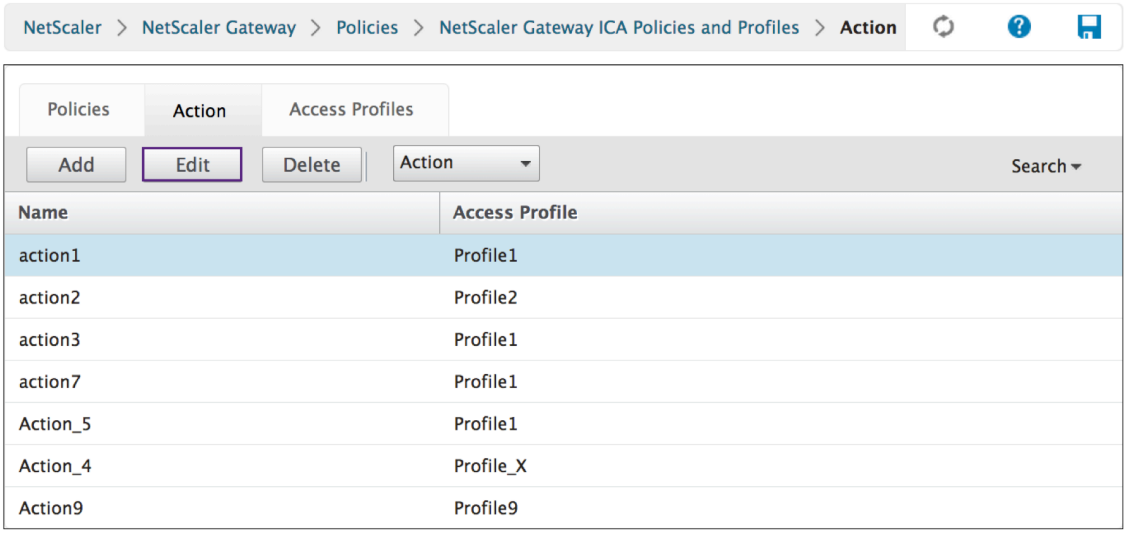
- Haga clic en el icono **para seleccionar un perfil de acceso existente. Para obtener más información, consulte [Seleccione un perfil de acceso existente] en (#common -processes).
- Haga clic en el icono **+** para crear un perfil de acceso. Para obtener más información, consulte [Crear un perfil de acceso.] (#creating-an-access-profile-with-the-gui).
- El icono del **lápiz** está inhabilitado para esta pantalla.

3. Haga clic en **Create**.




### Edit (Modificar)

1. Seleccione la directiva ICA deseada de la lista.



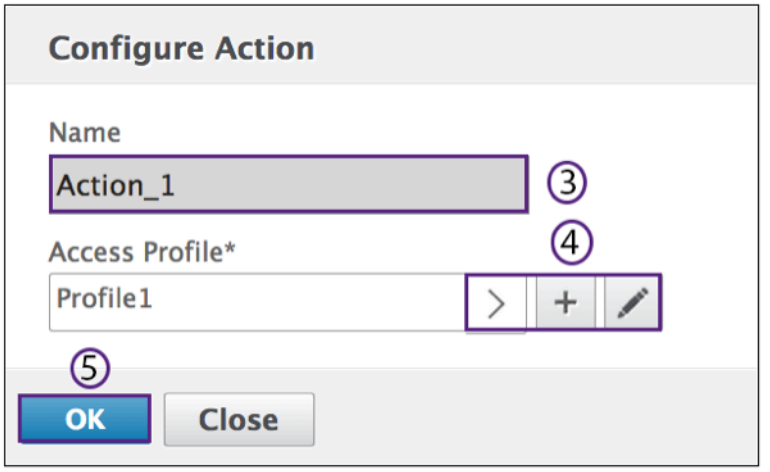

2. En el panel de detalles, en la ficha Acción, haga clic en **Modificar**.

## Configurar acción

1. Compruebe el nombre de la acción para confirmar que está editando la acción deseada. Este campo no se puede modificar.

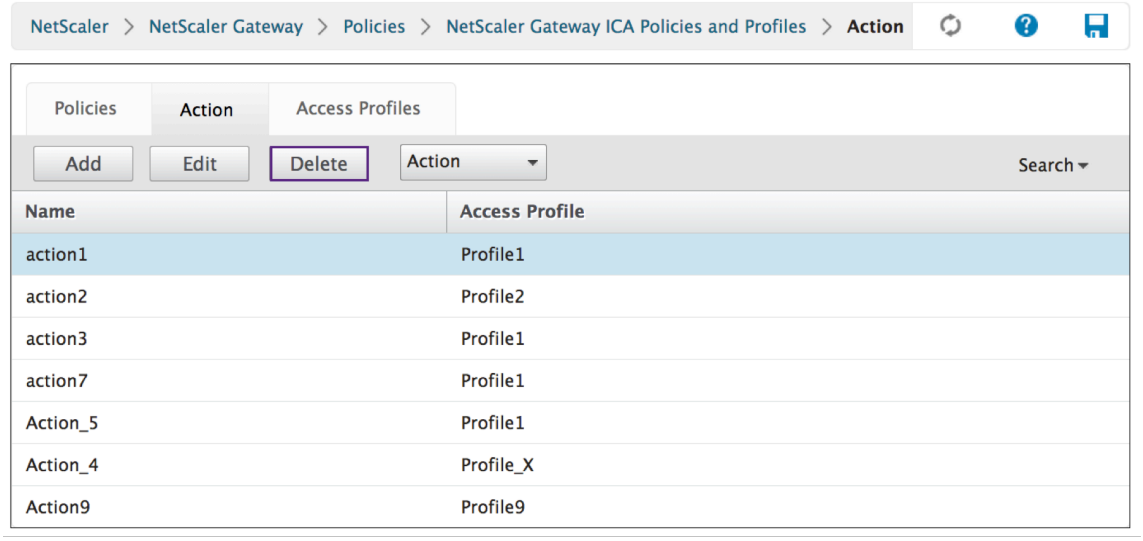
 

2. Junto a Perfil de acceso, realice una de las siguientes acciones:
   - Haga clic en **>** para seleccionar un perfil de acceso existente. Para obtener más información, consulte [Seleccionar un perfil de acceso existente] en (#common-processes).
   - Haga clic en el **signo +** para crear un perfil de acceso. Para obtener más información, consulte Crear un perfil de acceso.
   - Haga clic en el icono del **lápiz** para configurar el perfil de acceso.
3. Haga clic en **Aceptar**.




**Suprimir**

1. Vaya a **NetScaler Gateway > Acción** y, a continuación, haga clic en **ICA**.
2. Seleccione la acción ICA deseada de la lista.
3. En el panel de detalles, en la ficha Acción, haga clic en **Eliminar**.



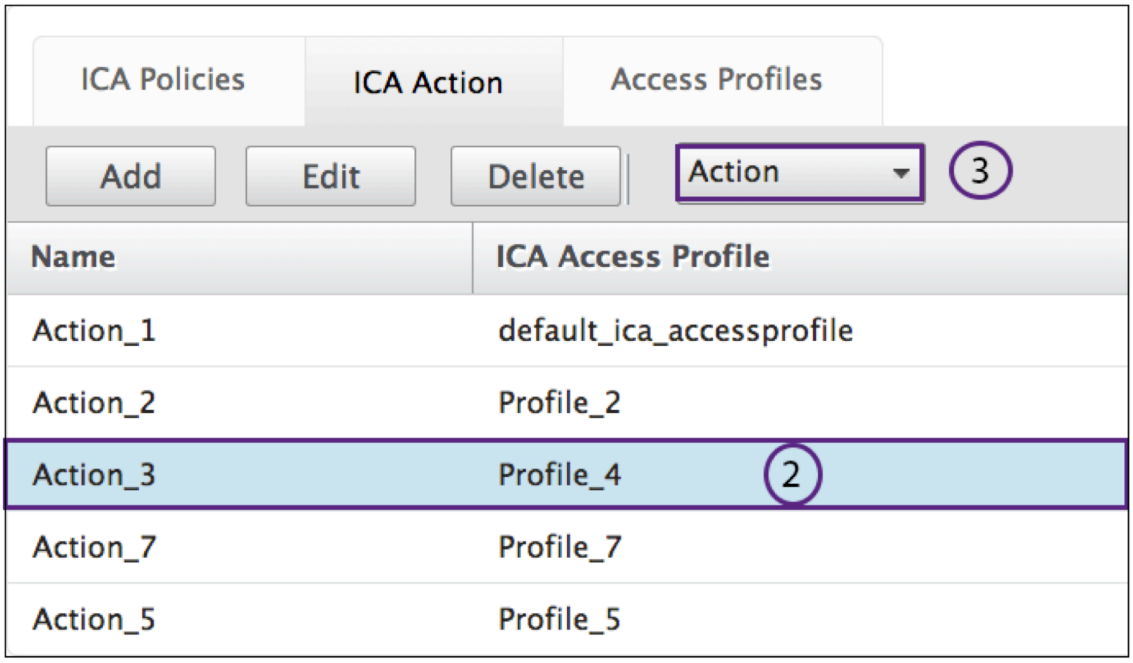

 

4. Confirme la acción en la que quiere eliminar la directiva haciendo clic en**Sí**.

### Acción

Los comandos **Acción ICA > Acción** se utilizan para cambiar el nombre de la acción.

1. Vaya a **NetScaler Gateway > Acción** y, a continuación, haga clic en **ICA**.
2. Seleccione la acción ICA deseada de la lista.
3. En el panel de detalles, en la ficha Acción, haga clic en **Acción**.




4. Seleccione **Acción > Cambiar nombre** en el menú.
5. Cambie el nombre de la acción.
6. Haga clic en **OK**.

### Perfiles de acceso

Un perfil ICA define la configuración de las conexiones de usuario.

Los perfiles de acceso especifican las acciones que se aplican al entorno ICA de Citrix Virtual Apps and Desktops de un usuario si el dispositivo del usuario cumple las condiciones de expresión de directiva. Puede utilizar la interfaz gráfica de usuario para crear perfiles ICA por separado de una directiva ICA y, a continuación, utilizarlo para varias directivas. Solo puede utilizar un perfil con una directiva.

Puede crear perfiles de acceso independientemente de una directiva ICA. Al crear la directiva, puede seleccionar el perfil de acceso que quiere asociar a la directiva. Un perfil de acceso especifica los recursos disponibles para un usuario. Los siguientes comandos están disponibles en la ficha **Directivas**:

- Add
- Edit (Modificar)
- Suprimir

### Creación de un perfil de acceso con la GUI

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.
2. En el panel de detalles, haga clic en la ficha **Perfiles de acceso** y, a continuación, haga clic en **Agregar**.
3. Configure los ajustes del perfil, haga clic en Crear y, a continuación, en **Cerrar**. Después de crear un perfil, puede incluirlo en una directiva ICA.

### Agregar un perfil de acceso a una directiva mediante la interfaz gráfica de usuario

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.
2. En la ficha Directivas, realice una de las siguientes acciones:
   - Haga clic en **Agregar** para crear una directiva ICA.
   - Seleccione una directiva y, a continuación, haga clic en **Abrir**.
3. En el menú **Acción**, seleccione un perfil de acceso de la lista.
4. Termine de configurar la directiva ICA y, a continuación, realice una de las siguientes acciones:

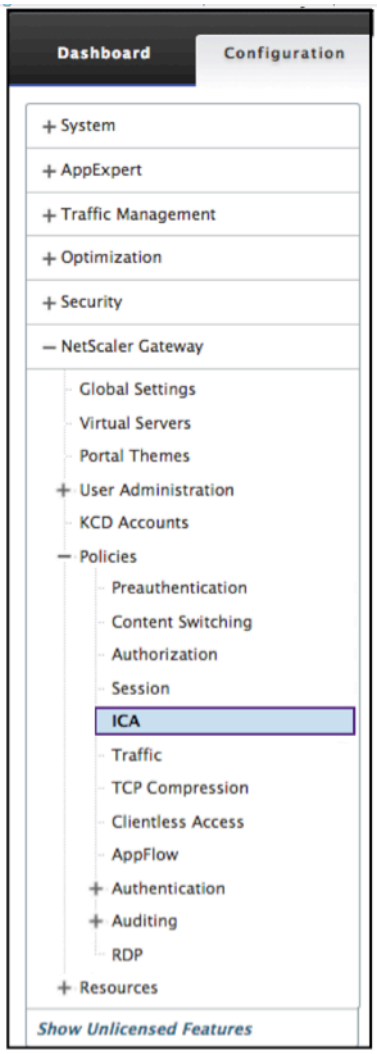
   a) Haga clic en **Crear** y, a continuación, en **Cerrar** para crear la directiva.

   1. Haga clic en **Aceptar** y, a continuación, en **Cerrar** para modificar la directiva.

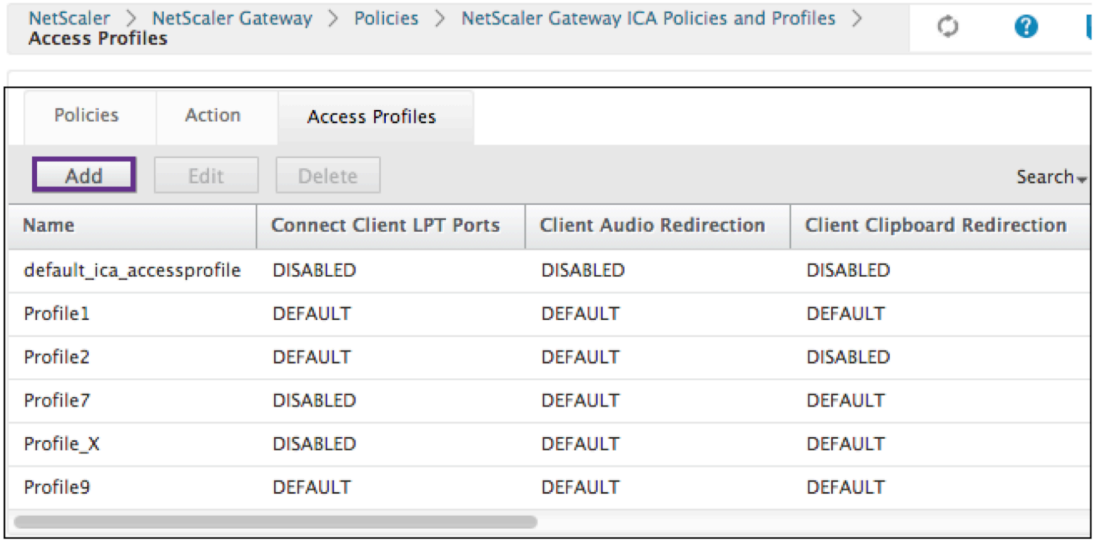
### Add

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.

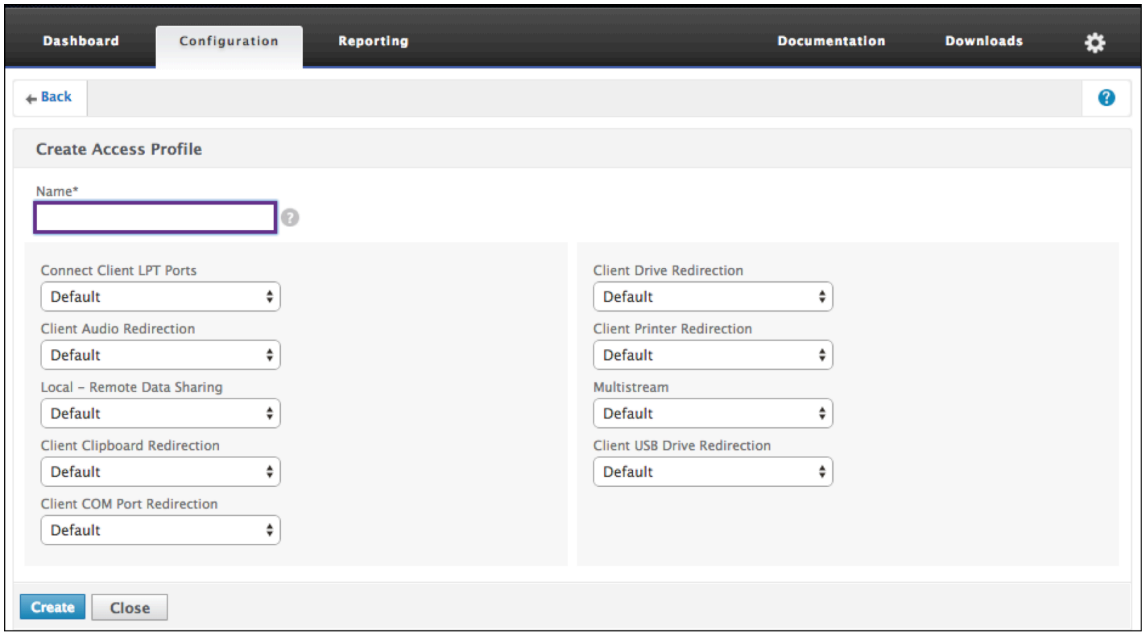



2. En el panel de detalles, en la ficha Perfiles de acceso, haga clic en**Agregar**.**



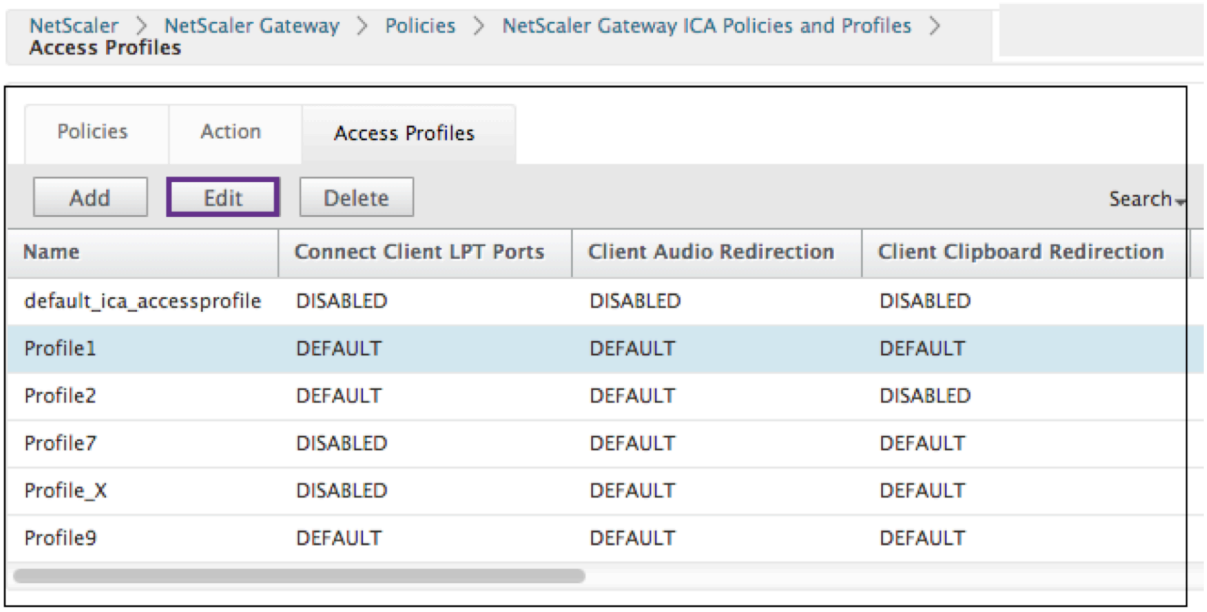
3. En Nombre, escriba un nombre para el perfil de acceso.




4. Seleccione Predeterminado o Inhabilitar en los menús mostrados para crear el perfil de acceso.
5. Haga clic en **Crear**.

## Edit (Modificar)

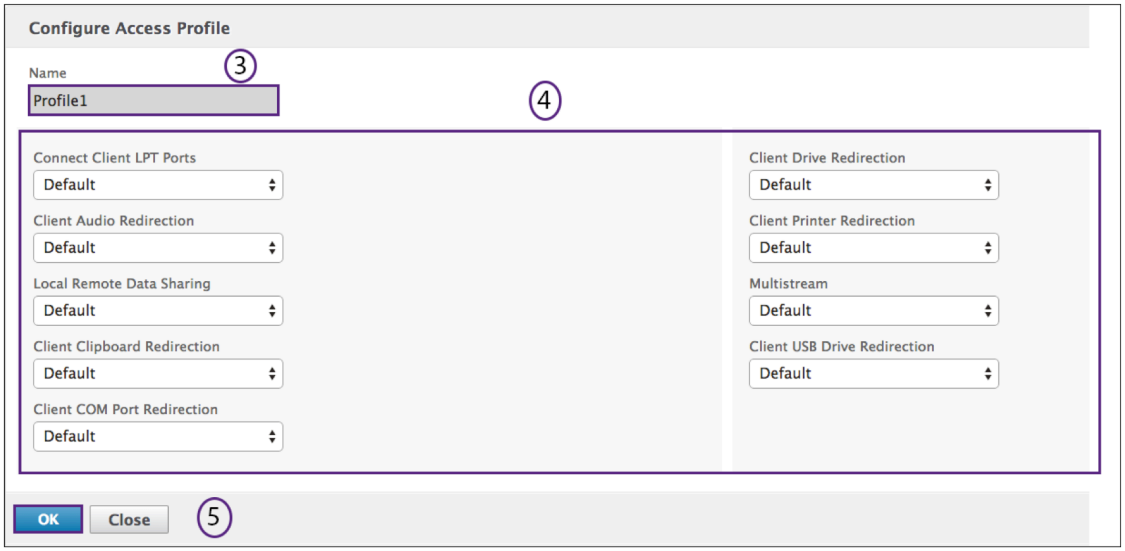
1. Seleccione el perfil de acceso que quiera modificar.
2. En el panel de detalles, en la ficha Perfiles de acceso, haga clic en **Modificar**.



## Configurar perfil de acceso

1. Compruebe que el **nombre** es el que quiere revisar.

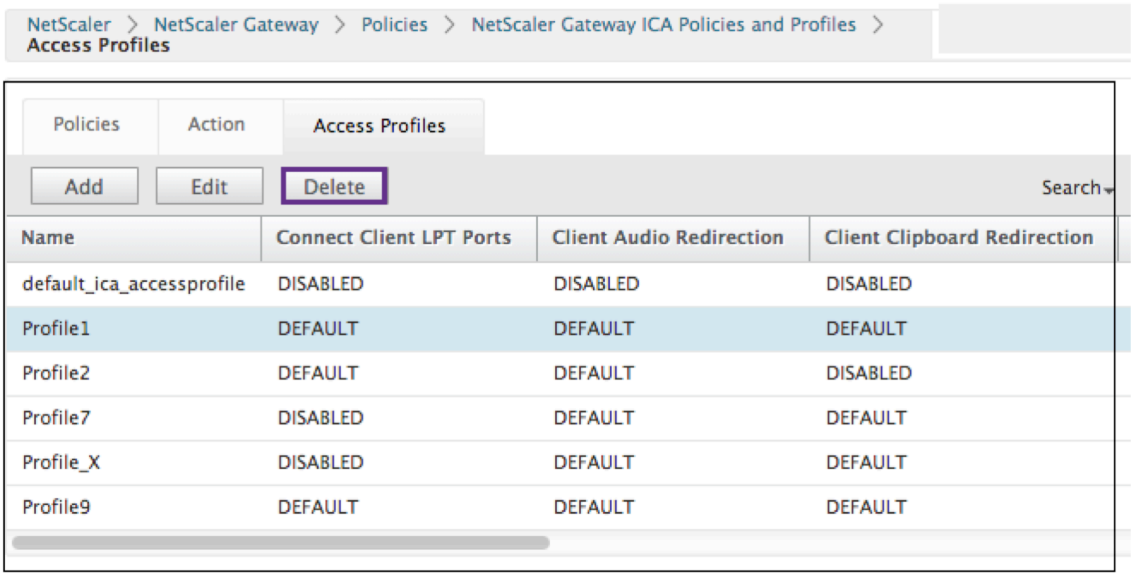



2. Seleccione **Predeterminado** o **Inhabilitar** en el menú para configurarlo según sea necesario.
3. Haga clic en **Aceptar**.

## Suprimir

1. Vaya a **Citrix Gateway > Acción y,** a continuación, haga clic en **ICA** .
2. Seleccione la acción ICA deseada de la lista.
3. En el panel de detalles, en la pestaña **Acción** , haga clic en **Eliminar** .



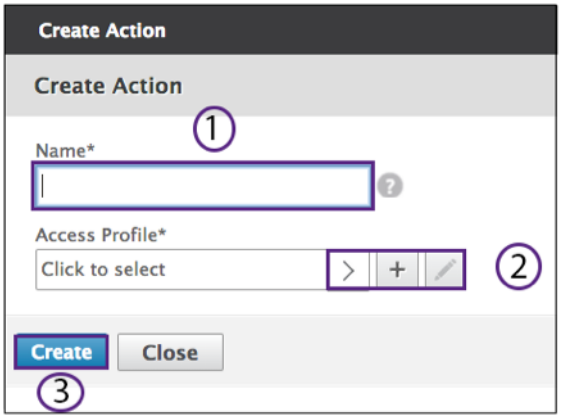

4. Confirme el perfil de acceso que quiere eliminar haciendo clic en **Sí**.

## Procesos comunes

### Crea una acción

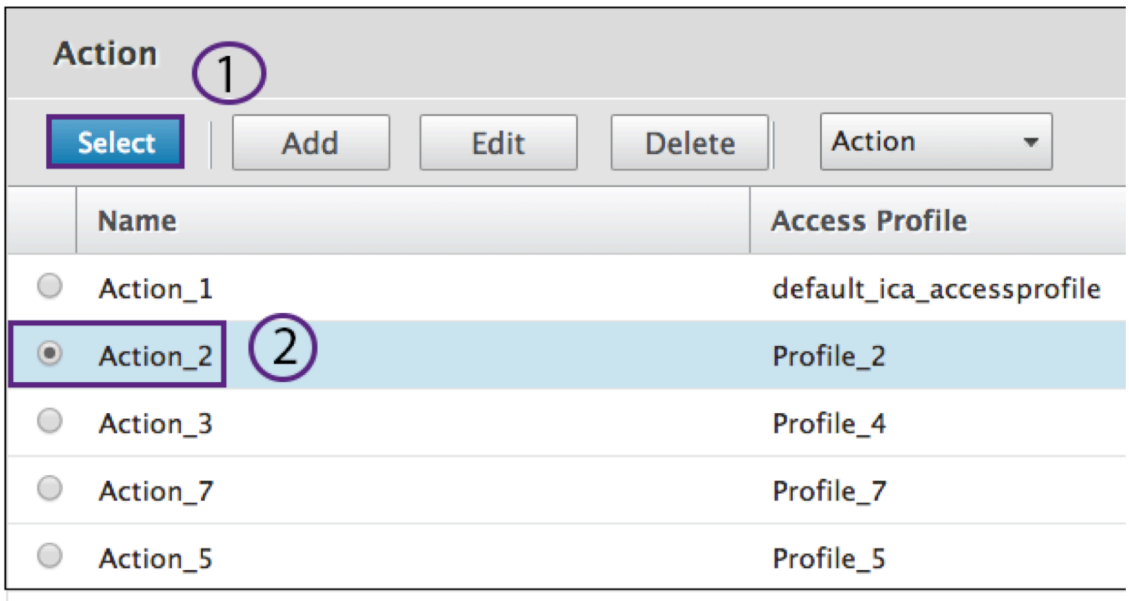
1. Escriba un nombre para la acción.
2. Seleccione una de las siguientes opciones para suministrar el perfil de acceso:
   - Haga clic en **>** para seleccionar un perfil de acceso existente. Para obtener más información, consulte [Seleccione un perfil de acceso existente] en (#common -processes).
   - Haga clic en el **signo +** para crear un perfil de acceso. Consulte para obtener más información Crear un perfil de acceso.
   - El icono del **lápiz** está inhabilitado.
3. Haga clic en **Crear**.




**Selecciona una acción**

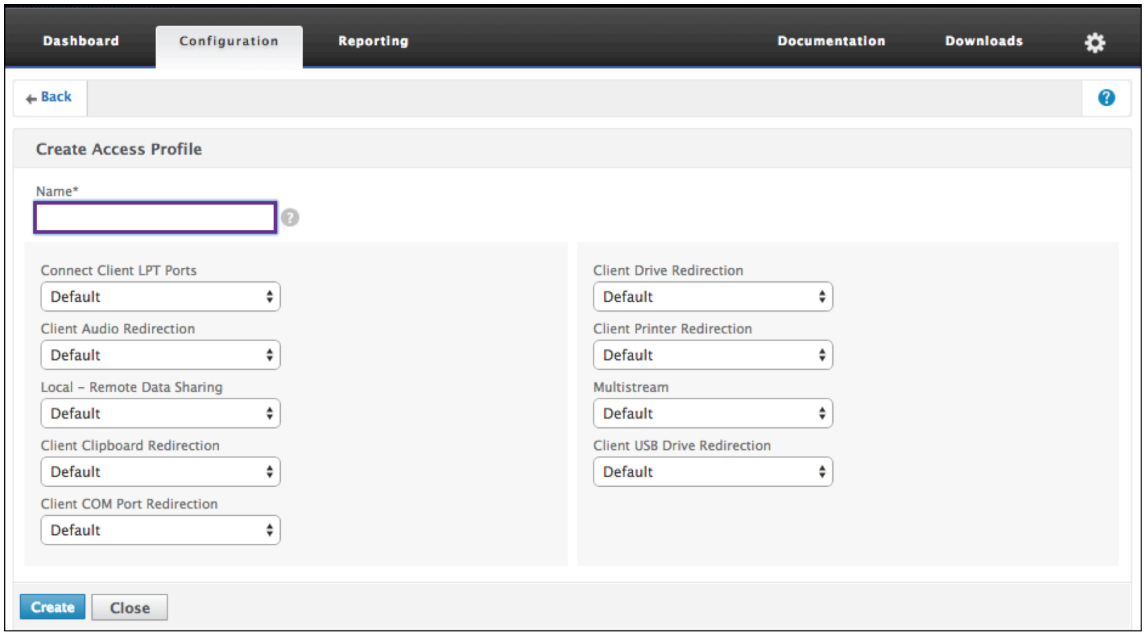
1. Seleccione una acción haciendo clic en el botón de opción situado a la izquierda de la misma. El perfil de acceso asociado especifica las funciones de usuario permitidas.
2. Haga clic en el botón **Seleccionar**.




**Crear un perfil de acceso**

1. Asigne un nombre al perfil de acceso.

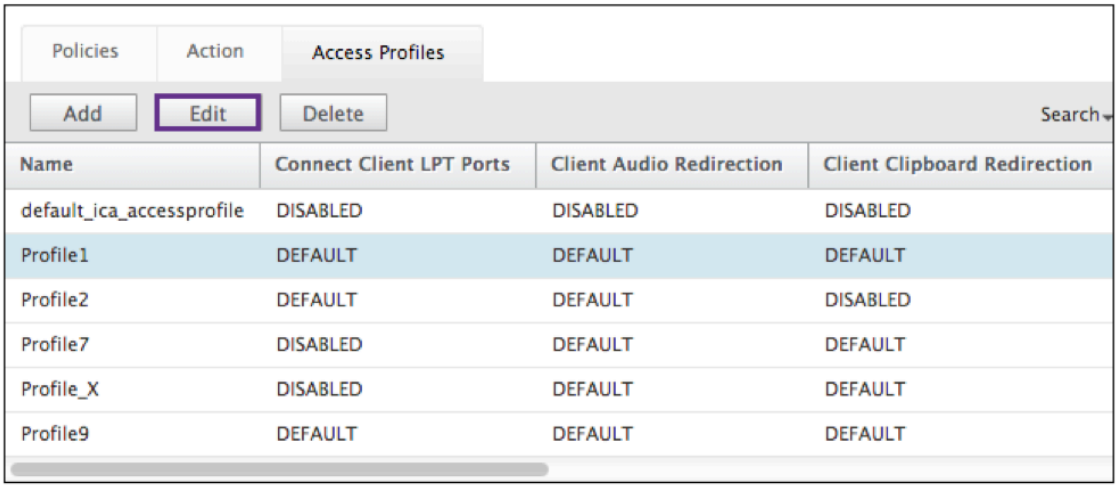
 




2. Puede configurar el perfil de acceso desde este menú.
3. Haga clic en **Crear**.

### Seleccionar un perfil de acceso existente

1. Seleccione un perfil de acceso haciendo clic en él.




2. Haga clic en Edit.
3. Configure el perfil de acceso. Para obtener más información, consulte Configurar perfil de acceso.

**Expresiones**

1. Para crear o revisar una expresión existente, seleccione Borrar.

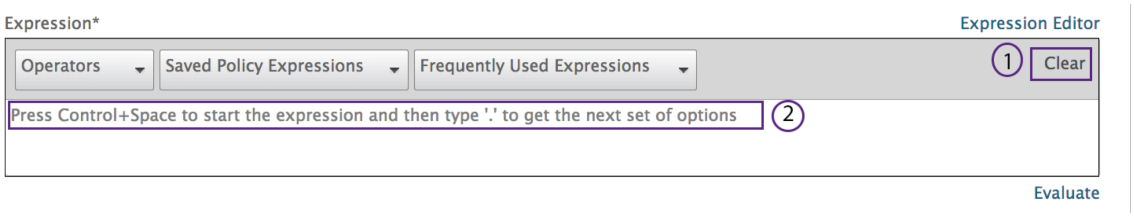
   Las expresiones son las típicas expresiones ICA. Para las expresiones HTTP, introduzca el nombre con el “”y elimine el ().

| | |
|---|---|
| ICA.SERVER.PORT | Esta expresión comprueba que el puerto especificado coincida con el número de puerto de Citrix Virtual Apps and Desktops que el usuario está intentando conectar. |
| ICA.SERVER.IP | Esta expresión comprueba que la IP especificada coincida con la dirección IP de Citrix Virtual Apps and Desktops a la que el usuario intenta conectar. |
| `HTTP.REQ.USER.IS\\_MEMBER\\_OF(“”)` .NOT | Esta expresión comprueba que un usuario que NO es miembro del nombre de grupo especificado acceda a la conexión actual. |
| HTTP.REQ.USER .IS_MEMBER_OF( “`group name`”) | Esta expresión comprueba que el usuario que accede a la conexión actual es miembro del grupo especificado. |
| HTTP.REQ.USER.NAME.CONTAINS(“”).NOT | Esta expresión comprueba que el usuario que accede a la conexión actual NO es miembro del grupo especificado. |
| HTTP.REQ.USER.NAME.CONTAINS (“enter `user name`”) Especifica los recursos de un nombre de usuario. | Esta expresión comprueba que se accede a la conexión actual mediante el nombre especificado. |
| CLIENT.IP.DST.EQ(introduzca la dirección IP aquí).NOT | Esta expresión comprueba que la IP de destino del tráfico actual NO es igual a la dirección IP especificada. |
| CLIENT.IP.DST.EQ (introduzca la dirección IP aquí) | Esta expresión comprueba que la IP de destino del tráfico actual sea igual a la dirección IP especificada. |
| CLIENT.TCP.DSTPORT.EQ (introduzca el número de puerto).NOT | Esta expresión comprueba que el puerto de destino NO es igual al número de puerto especificado. |

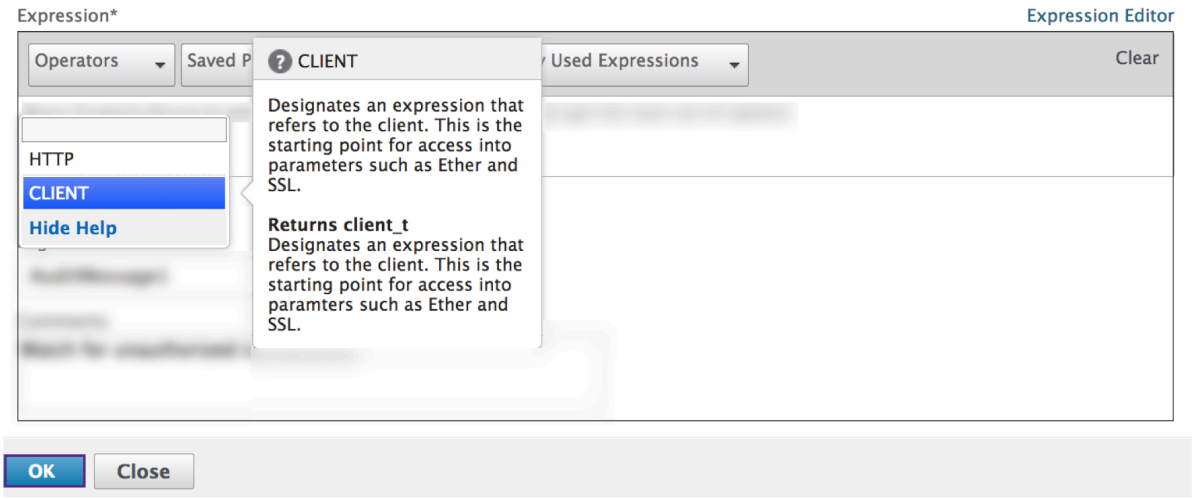
 

| | |
|---|---|
| CLIENT.TCP.DSTPORT.EQ (introduzca el número de puerto) | Esta expresión comprueba que el puerto de destino sea igual al número de puerto especificado. |

2. Al mismo tiempo, seleccione **Control** y la barra **espaciadora**. Entonces tus opciones estarán visibles.




3. Escriba el período. Haga su selección y pulse la barra **espaciadora** .
4. En cada período de la expresión de la tabla anterior, escriba el punto. Haga su selección y pulse la barra espaciadora .
5. Haga clic en **Aceptar**.




### Identificación de grupo

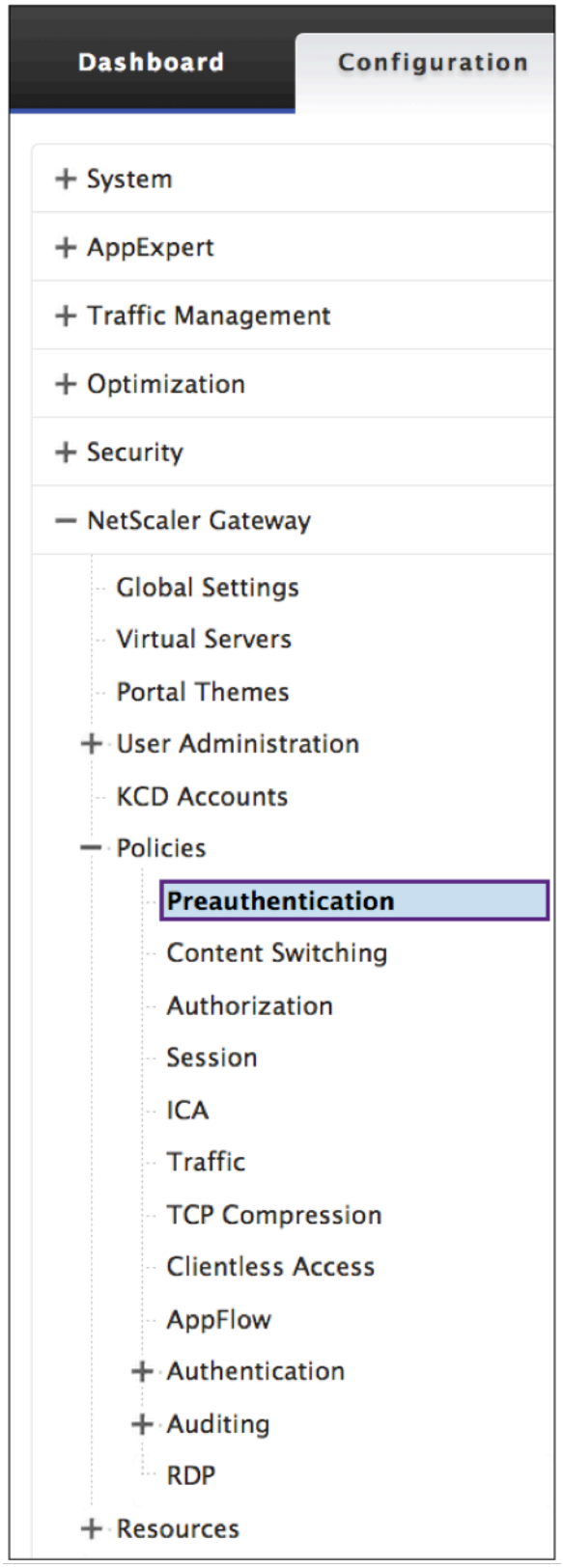
Las funciones previas a la autenticación o de sesión definen la expresión con una variable de nombre de grupo.

**Autentificación previa**

1. Seleccione Autenticación previa en el panel de configuración.

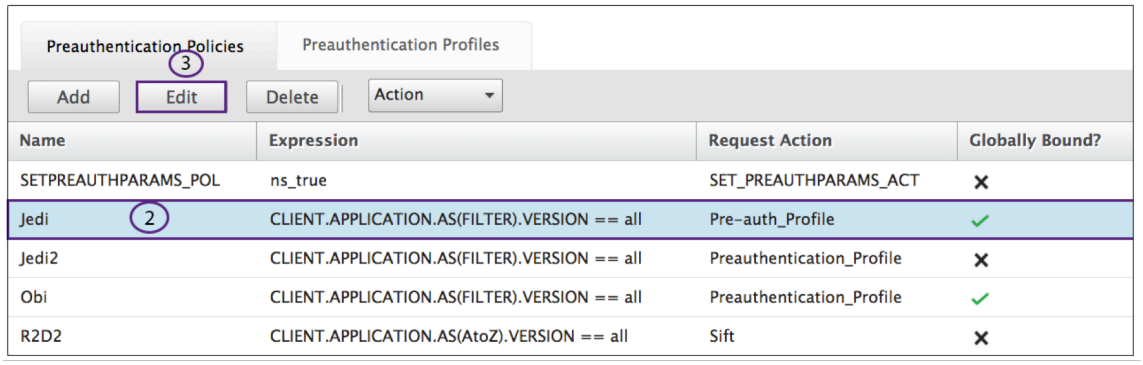
 



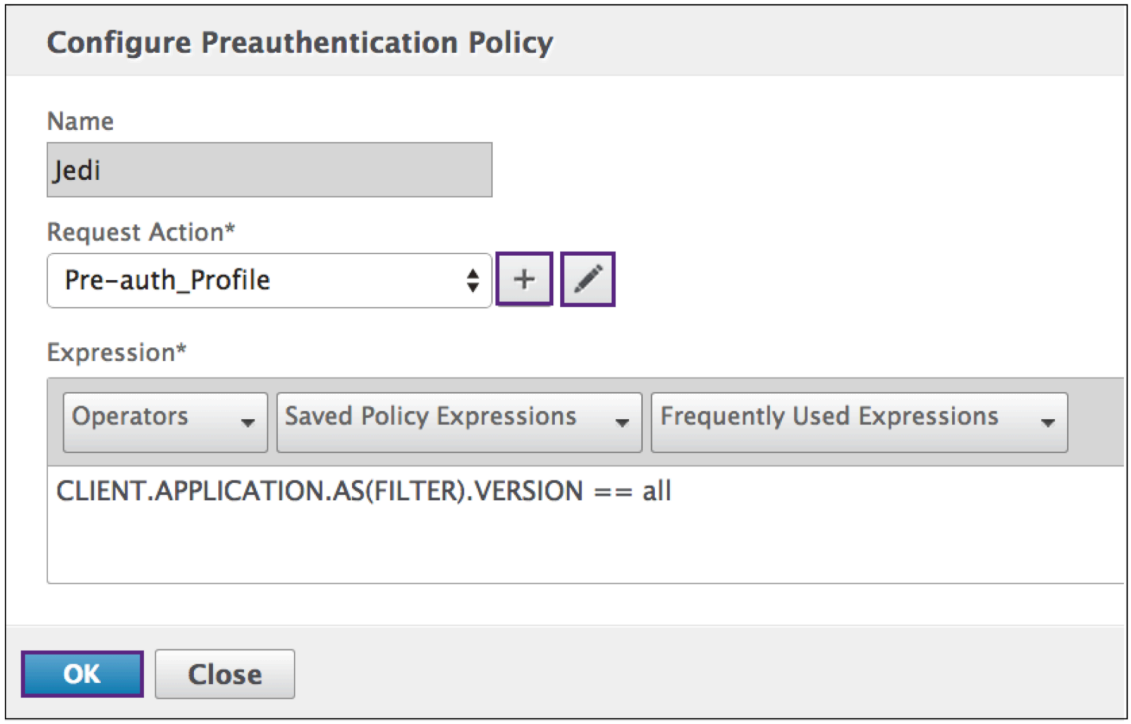

1. Seleccione un nombre de las directivas de autenticación previa.

2. Seleccione **Modificar** en la ficha Directivas de autenticación previa.

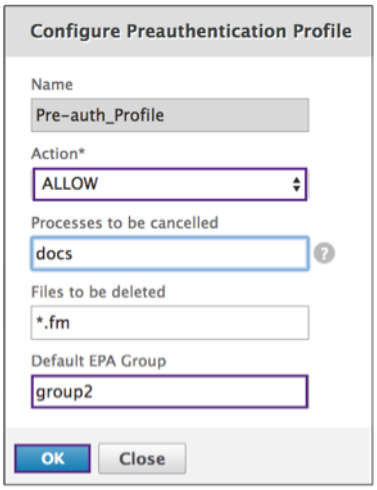



3. Seleccione el icono del **lápiz** o **+** junto al cuadro de diálogo Solicitar acción.




4. Defina ("<groupname>") en el cuadro de diálogo Grupo EPA predeterminado.

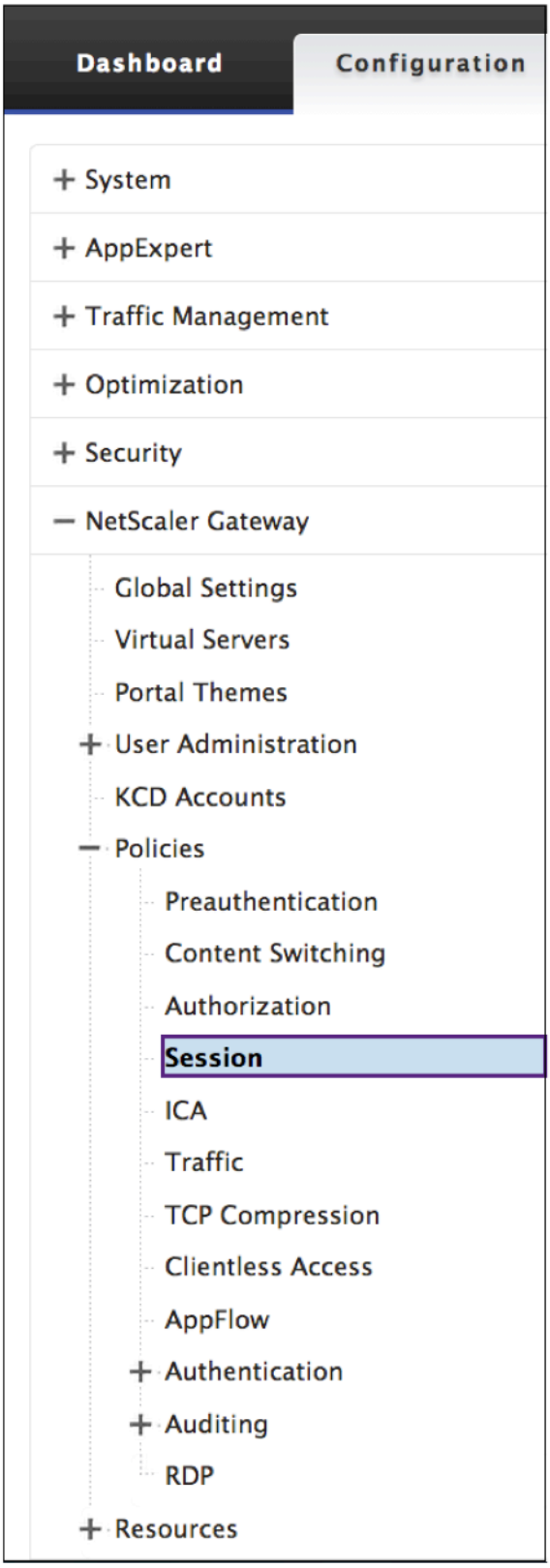
 




## Sesión

1. Seleccione **Sesión** en el panel de configuración.

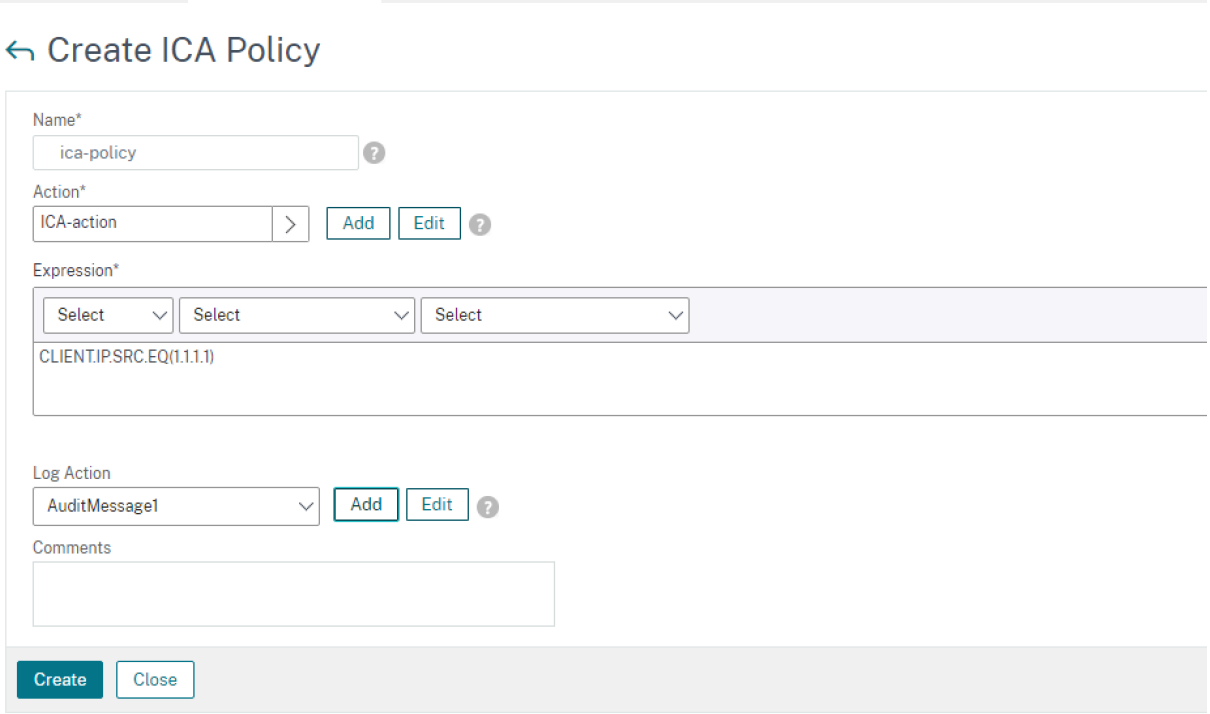
 



### Crear una acción de registro

1. En la pantalla **Configurar directiva**, junto al cuadro de diálogo **Acción de registro**, seleccione el icono **+**




### Acción Crear mensaje de auditoría

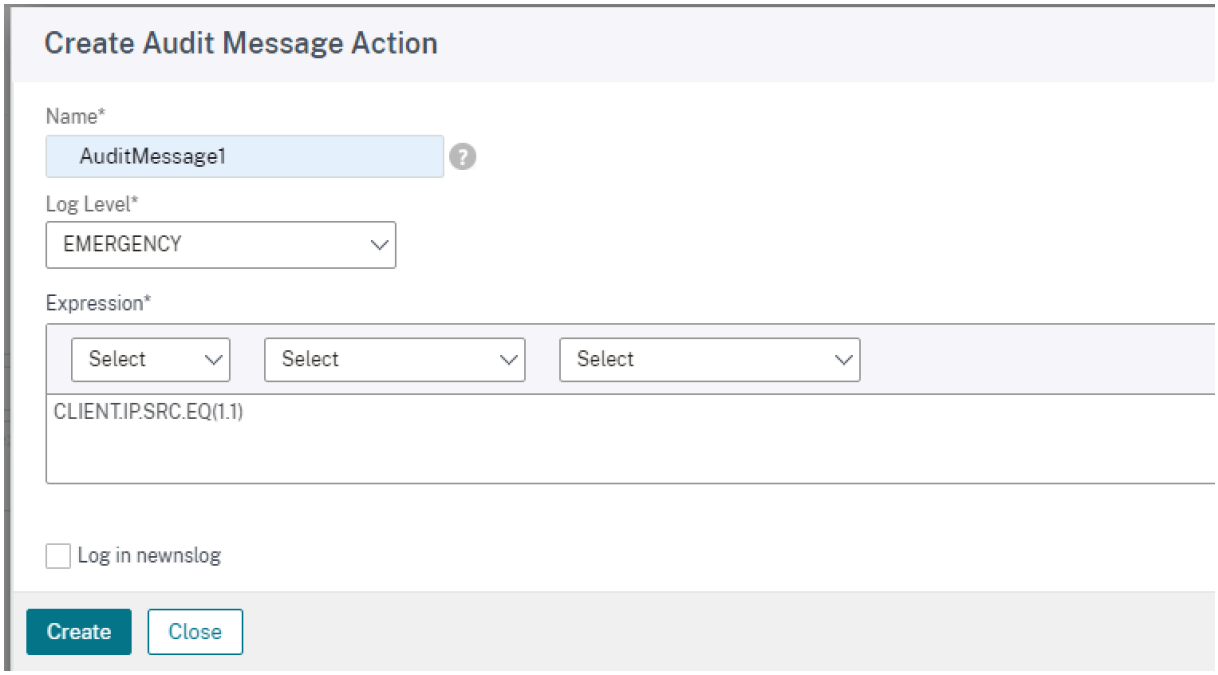
1. Aparece la pantalla **Crear acción de mensaje de auditoría**. Asigne un nombre al mensaje de auditoría. El mensaje de auditoría solo acepta números, letras o guiones bajos.
2. En el menú, especifique el nivel de registro de auditoría.

| | |
|---|---|
| Emergencia | Eventos que indican una crisis inmediata en el servidor. |
| Alerta | Eventos que podrían requerir acción. |
| Grave | Eventos que indican una crisis inminente del servidor. |
| Error | Eventos que indican algún tipo de error. |
| Advertencia | Eventos que requieren acción pronto. |
| Notificación | Eventos que el administrador debe conocer. |

| | |
|---|---|
| Informativo | Todos menos eventos de bajo nivel. |
| Depuración | Todos los eventos, con todo detalle. |

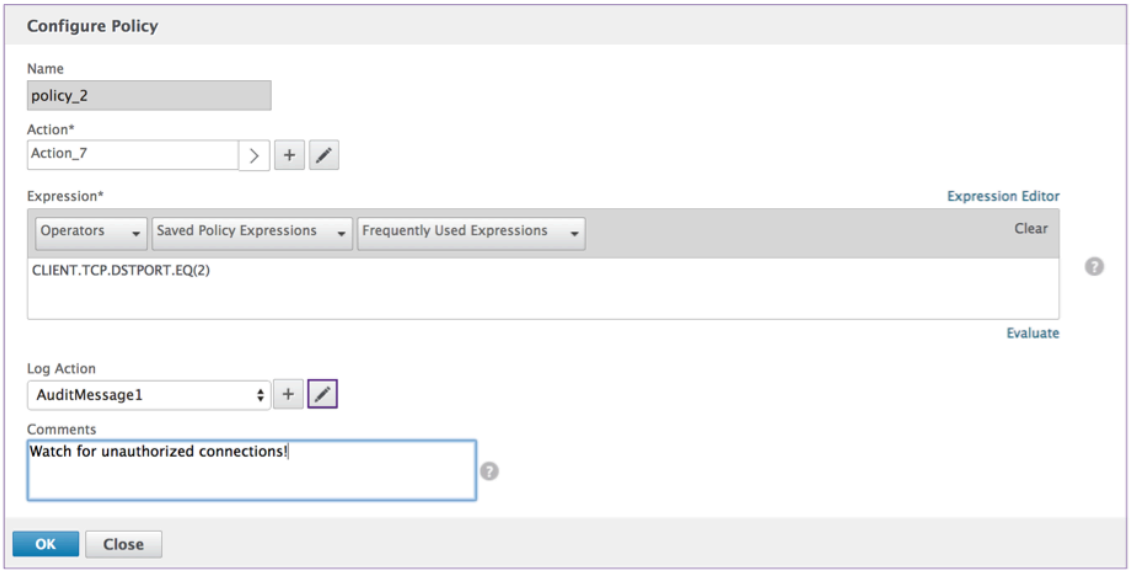
1. Introduzca una expresión. La expresión define el formato y el contenido del registro.
2. Las casillas de verificación.
   - Marque `newnslog` del inicio de sesión para enviar el mensaje a un nuevo registro ns.
   - Seleccione **Omitir comprobación de seguridad** para evitar la comprobación de seguridad. Esto permite expresiones inseguras.
3. Haga clic en **Crear**.




**Revisar una acción de registro**

1. En la pantalla Configurar directiva, junto al cuadro de diálogo Acción de registro, haga clic en el icono.

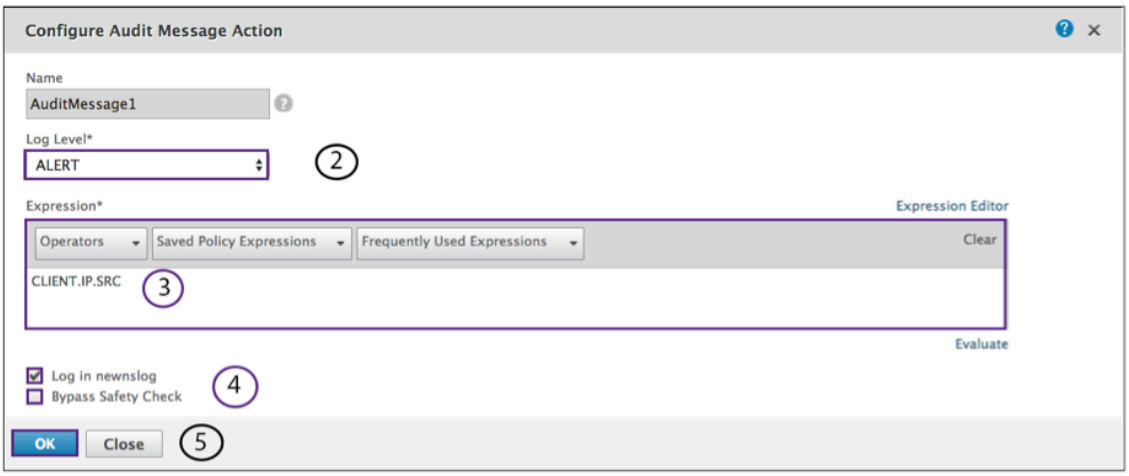
 




### Acción Configurar mensaje de auditoría

Los siguientes campos son modificables:

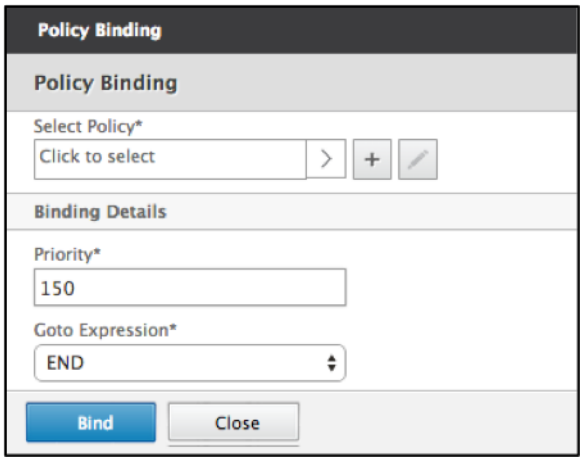
1. En el menú, especifique el nivel de registro de auditoría.
2. Introduzca una expresión. La expresión define el formato y el contenido del registro.
3. Las casillas de verificación:
   - Marque `newnslog` del inicio de sesión para enviar el mensaje a un nuevo registro ns.
   - Seleccione **Omitir comprobación de seguridad** para evitar la comprobación de seguridad. Esto permite expresiones inseguras.
4. Haga clic en **Aceptar**.



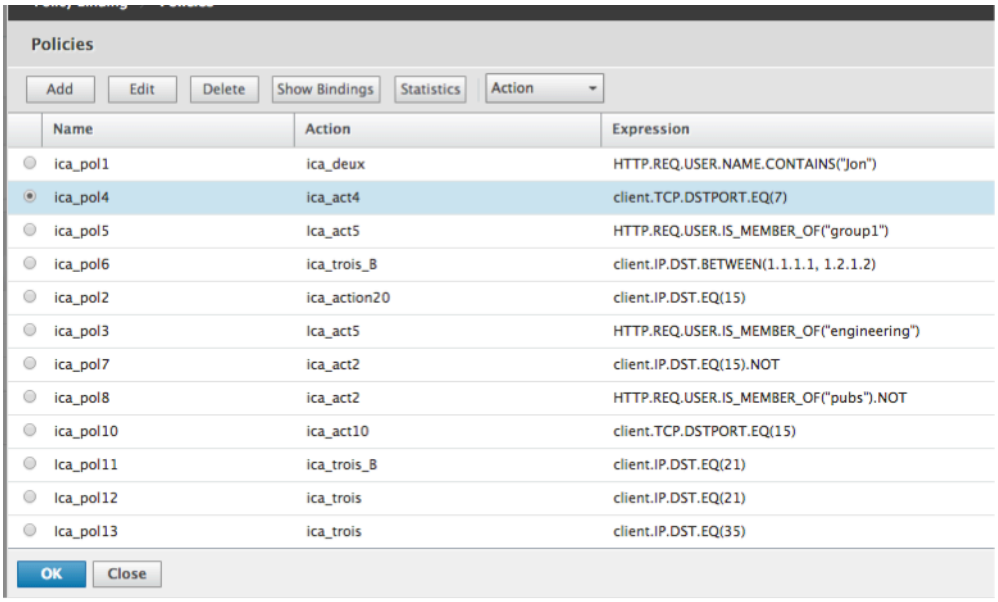

 

### Seleccione una directiva existente

1. Haga clic en **el**icono para seleccionar una política existente.



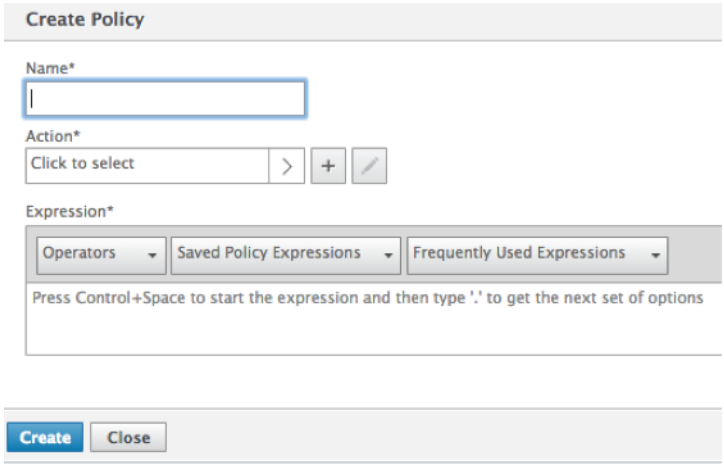

2. Seleccione el botón de opción de la directiva deseada.



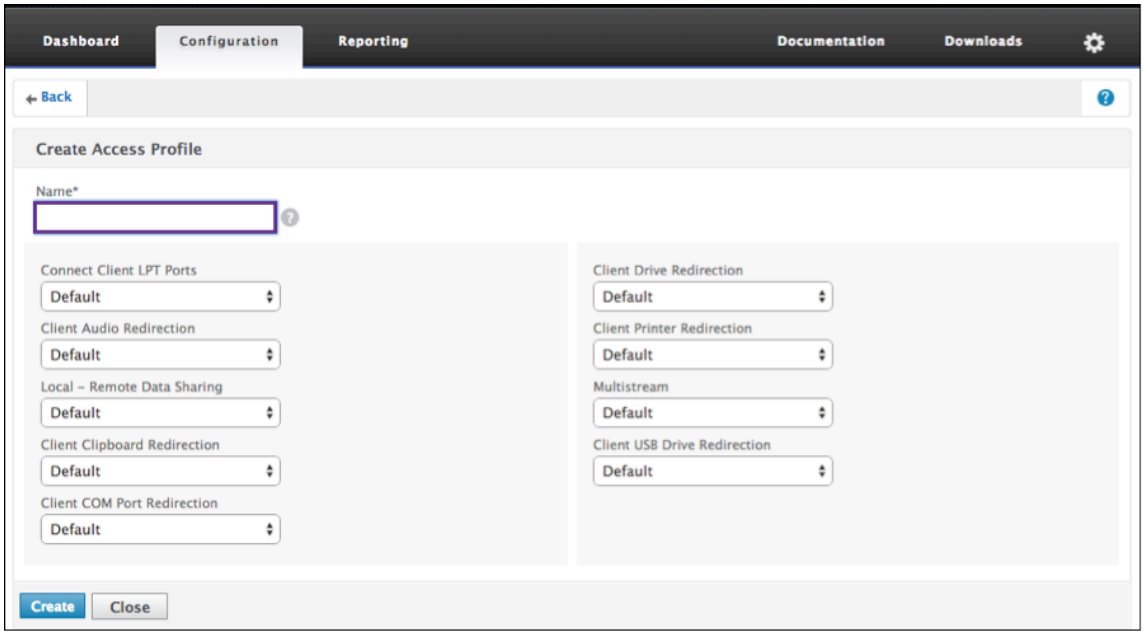

### Crear una directiva

1. En **Nombre**, escriba un nombre para la directiva.
2. Haga clic en el signo **+** para crear una política.

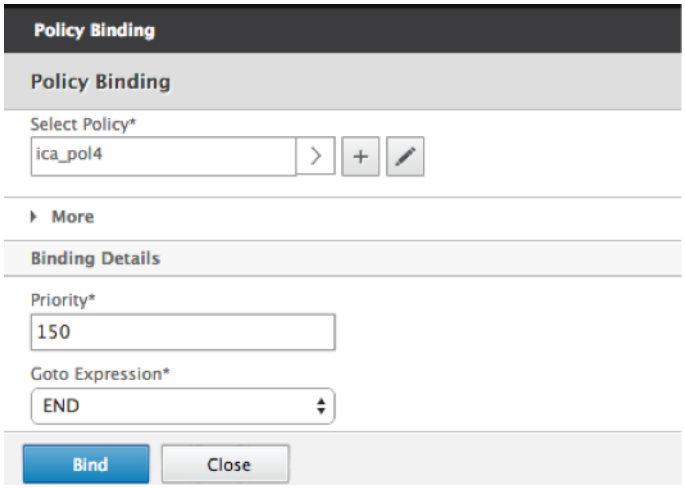



3. Crea una acción. Para obtener más información, consulte **Crear una nueva acción**.
4. Asigne un nombre al perfil de acceso.




5. Configure el perfil de acceso en este menú.
6. Haga clic en **Crear**.
7. Haga clic en **Bind**.




## Configuración del análisis de punto final de autenticación previa y versiones posteriores a la autenticación

En esta sección se describe cómo configurar el análisis de punto final (EPA) posterior a la autenticación y previa a la autenticación.

Para configurar la EPA posterior a la autenticación con SmartControl, utilice el parámetro `Smartgroup` de la acción de sesión VPN. La expresión EPA se configura en la directiva de sesión VPN.

Puede especificar un nombre de grupo para el parámetro de grupo inteligente. Este nombre de grupo puede ser cualquier cadena. No es necesario que el nombre del grupo sea un grupo existente en active directory.

Configure la directiva ICA con la expresión HTTP.REQ.IS_MEMBER_OF ("`groupname`"). Utilice el nombre del grupo especificado anteriormente para el grupo inteligente.

Para configurar la EPA previa a la autenticación con SmartControl, utilice el parámetro Grupo EPA predeterminado del perfil de autenticación previa. La expresión EPA se configura en la directiva de autenticación previa.

Puede especificar un nombre de grupo para el parámetro Grupo EPA predeterminado. Este nombre de grupo puede ser cualquier cadena. No es necesario que el nombre del grupo sea un grupo existente en active directory.

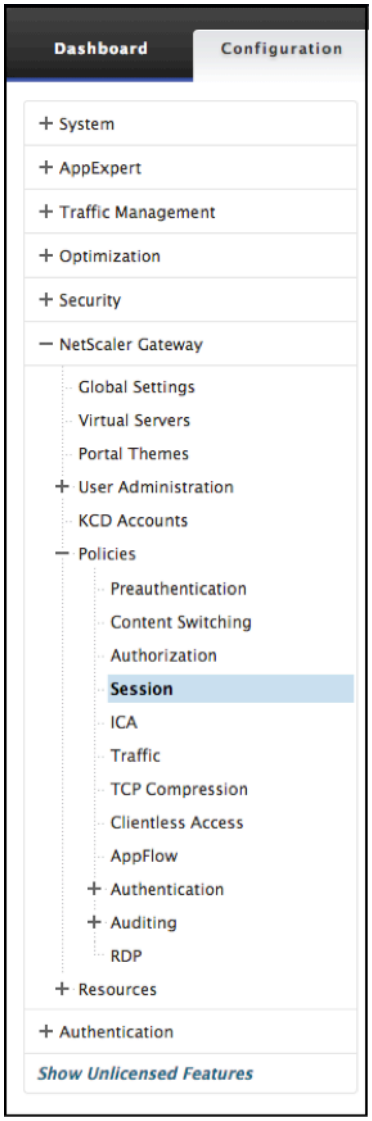
Configure la directiva ICA con la expresión HTTP.REQ.IS_MEMBER_OF ("`groupname`"), utilice el nombre de grupo especificado anteriormente para el grupo EPA predeterminado.

### Configuración posterior a la autenticación

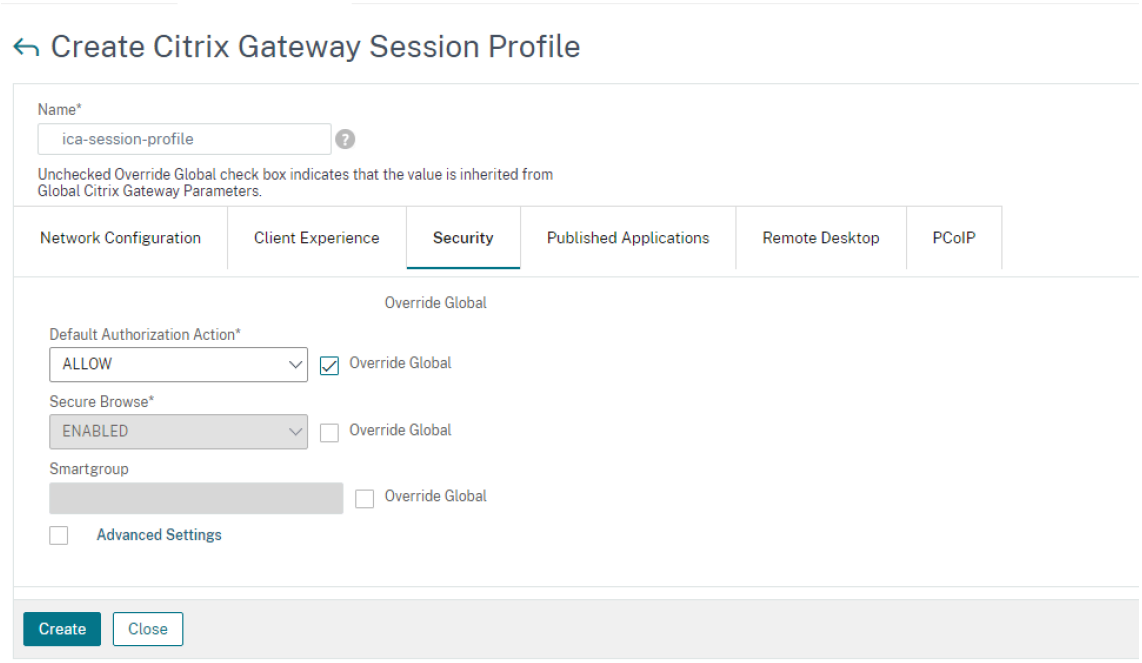
**Utilice el procedimiento siguiente para configurar grupos inteligentes para la configuración posterior a la autenticación.**

1. Vaya a **Citrix Gateway > Políticas > Sesión**.




2. Vaya a **Perfiles de sesión > Agregar**.




### Crear perfil de sesión de NetScaler Gateway

1. Seleccione la ficha **Seguridad**.
2. Introduzca un **nombre** para el perfil de NetScaler Gateway (acción).
3. Seleccione la casilla situada a la derecha del menú y seleccione la **Acción de autorización predeterminada**deseada.

   Especifique los recursos de red a los que tienen acceso los usuarios cuando inician sesión en la red interna. La configuración predeterminada de la autorización es denegar el acceso a todos los recursos de red. Citrix recomienda utilizar la configuración global predeterminada y, a continuación, crear directivas de autorización para definir los recursos de red a los que pueden acceder los usuarios. Si establece la directiva de autorización predeterminada en DENY, debe autorizar explícitamente el acceso a cualquier recurso de red, lo que mejora la seguridad.
4. Seleccione la casilla situada a la derecha del menú y seleccione la opción **Secure Browse deseada.**

   Permita que los usuarios se conecten a través de NetScaler Gateway a recursos de red desde dispositivos móviles iOS y Android con la aplicación Citrix Workspace. Los usuarios no necesitan establecer un túnel VPN completo para acceder a los recursos de la red segura.
5. Seleccione la casilla situada a la derecha del menú e introduzca el nombre `Smartgroup`.

   Este es el grupo en el que se coloca al usuario cuando la directiva de sesión asociada a esta acción de sesión tiene éxito. La directiva de sesión VPN realiza la comprobación EPA posterior a la

autenticación y, si la comprobación se realiza correctamente, el usuario se coloca en el grupo especificado con un grupo inteligente. La expresión is_member_of (http.req.user.is_member_of) se puede utilizar con directivas para comprobar si la EPA ha pasado al usuario que pertenece a este grupo inteligente.

6. Haga clic en **Crear**.
7. Vaya a **NetScaler Gateway > Directivas > Sesión**.
8. Vaya a **Directivas de sesión > Agregar**.
9. Introduzca el **nombre** de la nueva directiva de sesión que se aplica después de que el usuario inicie sesión en NetScaler Gateway.
10. Seleccione la acción **Perfil** mediante el menú.

    Acción aplicada por la nueva directiva de sesión si se cumple el criterio de regla.

    **Nota:** Si se debe crear el perfil deseado, seleccione el +. Para obtener más información, consulte Crear perfil de sesión de NetScaler Gateway.
11. Introduzca **Expresión** en este campo.

    Este campo define la expresión con nombre que especifica el tráfico que coincide con la directiva. La expresión se puede escribir en sintaxis predeterminada o clásica. La longitud máxima de una cadena literal de la expresión es de 255 caracteres. Una cadena más larga se puede dividir en cadenas más pequeñas de hasta 255 caracteres cada una y las cadenas más pequeñas se pueden concatenar con el operador +. Por ejemplo, puede crear una cadena de 500 caracteres de la siguiente manera: “”+ “”

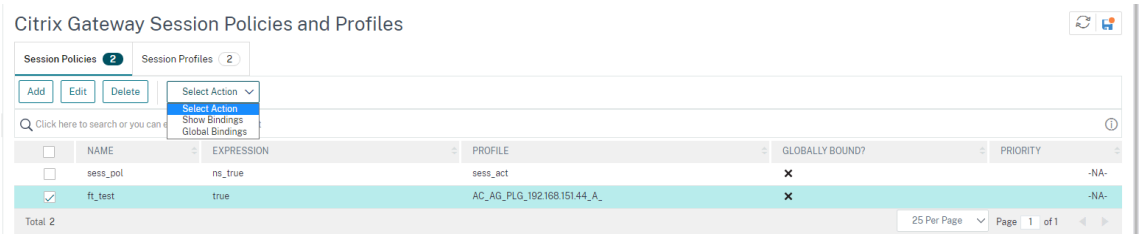
    Los siguientes requisitos solo se aplican a la CLI de NetScaler ADC:

    - Si la expresión incluye uno o varios espacios, encierre la expresión completa entre comillas dobles.
    - Si la propia expresión incluye comillas dobles, escape las comillas mediante el carácter.* Como alternativa, puede utilizar comillas simples para escribir la regla, en cuyo caso no tendrá que escapar las comillas dobles.
12. Haga clic en **Crear**.
13. Vaya a **Directivas de sesión**.
14. Seleccione el **nombre** de la directiva de sesión.
15. Seleccione **Enlaces globales** en el menú **Acción**.
16. Selecciona **Agregar enlace**.
17. Seleccione **>** para elegir una directiva existente.

    **Nota**: Seleccione + para crear una política. Para obtener más información, consulte la sección Crear perfil de sesión de NetScaler Gateway.

18. Elija un nombre de la lista y pulse el botón **Seleccionar**.
19. Introduzca la **prioridad** y haga clic en **Vincular**.
20. Haga clic en **Listo**
21. La comprobación muestra que la selección está enlazada globalmente.

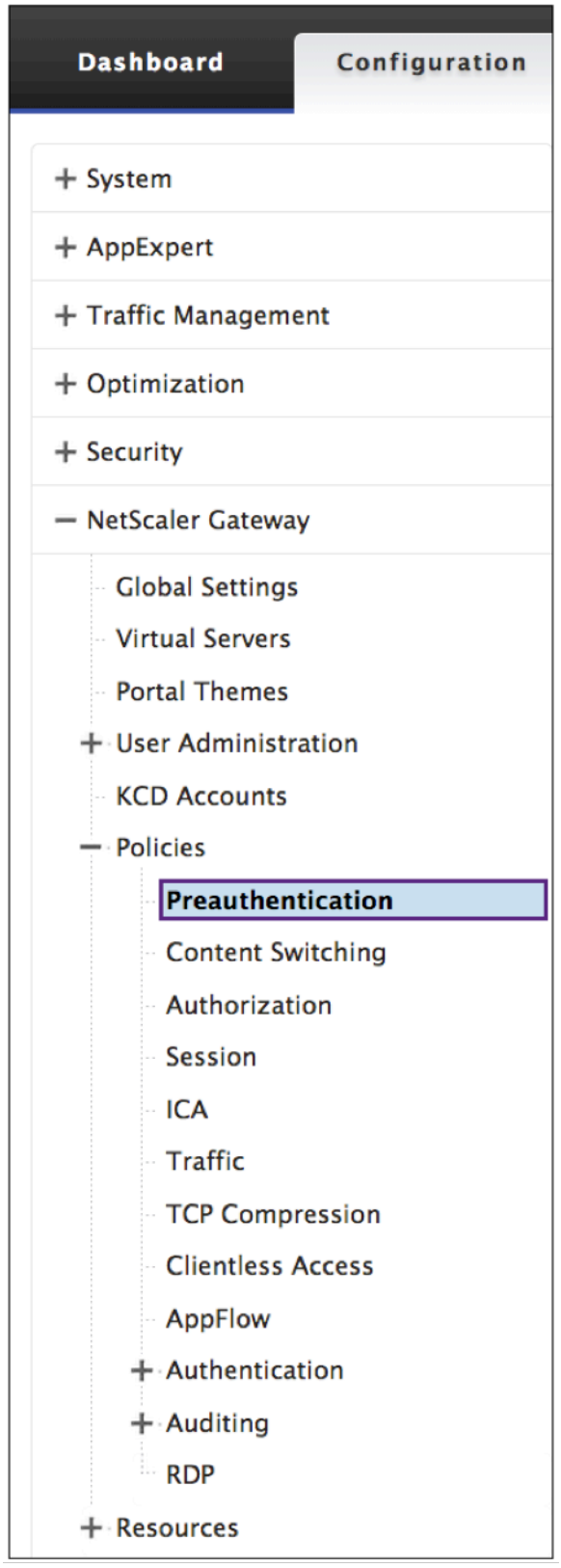



### Configuración previa a la autenticación

Utilice el procedimiento siguiente para configurar la configuración de autenticación previa.

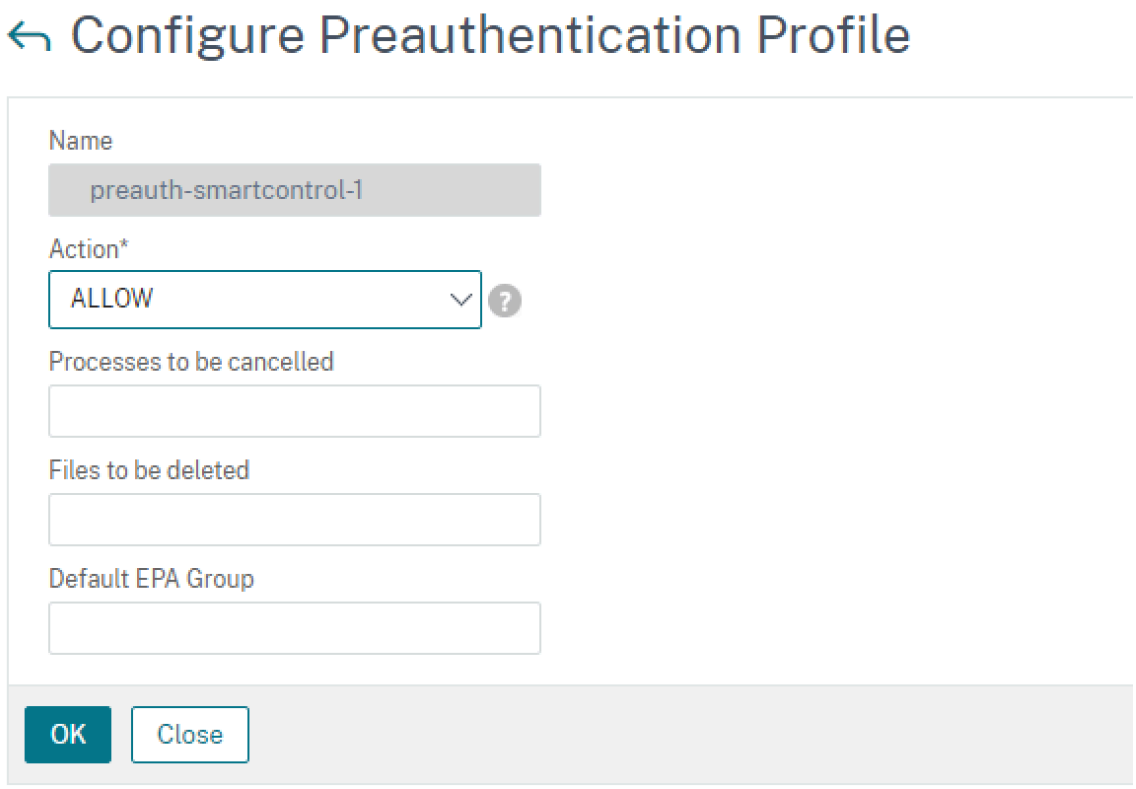
1. Vaya a Citrix NetScaler > Políticas > **Autenticación** previa.




2. Seleccione la ficha **Perfiles de autenticación previa** y seleccione **Agregar**.




3. Introduzca el **nombre** de la acción de autenticación previa.

   El nombre debe comenzar con una letra, un número o el carácter de guión bajo (_) y debe constar únicamente de letras, números y guión (-), punto (.) almohadilla (#), espacio (), en (@), igual (=), dos puntos (:) y guión bajo. No se puede cambiar una vez creada la acción de autenticación previa.

   **Nota:** El siguiente requisito se aplica únicamente a la CLI de NetScaler ADC:
   Si el nombre incluye uno o varios espacios, escriba el nombre entre comillas dobles o simples.

4. Seleccione una **acción de solicitud** que la directiva va a invocar cuando una conexión coincida con la directiva.

   **Nota:** Si quiere crear o crear un perfil de autenticación previa, seleccione el +. Para obtener más información, consulte Crear perfil de autenticación previa.

5. Introduzca una **expresión** que sea el nombre de la regla con nombre de NetScaler ADC o una expresión de sintaxis predeterminada que defina las conexiones que coinciden con la directiva.
6. Haga clic en **Crear**.
7. Vaya a la ficha **Directivas de autenticación previa** y seleccione la directiva deseada.
8. Seleccione **Enlace global** en el menú **Acción**.
9. Selecciona **Agregar vinculaciones**.

10. Seleccione para **seleccionar**una política existente.

    Seleccione + para crear una directiva. Para obtener más información, consulte Crear perfil de sesión de NetScaler Gateway.

11. **Selecciona** Directiva.
12. Introduzca la **prioridad** y haga clic en **Vincular**.
13. Haga clic en **Listo**.
14. La comprobación muestra que la **directiva de autenticación previa** está **enlazada globalmente**.

## Crear perfil de autenticación previa

1. Introduzca el **nombre** de la acción de autenticación previa

   El nombre debe comenzar con una letra, un número o el carácter de guión bajo (_) y debe constar únicamente de letras, números y guión (-), punto (.) almohadilla (#), espacio (), en (@), igual (=), dos puntos (:) y guión bajo. No se puede cambiar una vez creada la acción de autenticación previa.

   **Nota**: Si el nombre incluye uno o más espacios, escríbalo entre comillas dobles o simples. Esto solo se aplica a la CLI de Citrix ADC:

2. Introduzca a la **acción** en el menú.

   Esta opción permitirá o denegará el inicio de sesión tras los resultados del análisis de puntos finales (EPA).

3. **Procesos que se van a cancelar**

   Esta opción identifica una cadena de procesos que debe terminar la herramienta de análisis de puntos finales (EPA).

4. **Archivos que se van a eliminar**

   Esta opción identifica una cadena que especifica las rutas y los nombres de los archivos que debe eliminar la herramienta de análisis de puntos finales (EPA).

5. **Grupo EPA predeterminado**

   El grupo EPA predeterminado es el grupo que se elige cuando la comprobación de la EPA se realiza correctamente.

6. Haga clic en **Crear**.

# Configurar Single Sign-On en la Interfaz Web

January 26, 2024

Puede configurar NetScaler Gateway para proporcionar inicio de sesión único a los servidores de la red interna que utilizan autenticación basada en web. Con el inicio de sesión único, puede redirigir al usuario a una página principal personalizada, como un sitio de SharePoint o a la Interfaz Web. También puede configurar el inicio de sesión único en los recursos mediante el plug-in de NetScaler Gateway desde un marcador configurado en la interfaz de acceso o una dirección web que los usuarios escriben en el explorador web.

Si va a redirigir la Interfaz de Access a un sitio de SharePoint o a la Interfaz Web, proporcione la dirección web del sitio. Cuando los usuarios se autentican, ya sea mediante NetScaler Gateway o un servidor de autenticación externo, los usuarios se redirigen a la página principal especificada e inician sesión automáticamente. Las credenciales de usuario se transfieren de forma transparente al servidor web. Si el servidor web acepta las credenciales, los usuarios inician sesión automáticamente. Si el servidor web rechaza las credenciales, los usuarios reciben un mensaje de autenticación en el que se les pide su nombre de usuario y contraseña.

Puede configurar el inicio de sesión único en aplicaciones web de forma global o mediante una directiva de sesión.

También puede configurar el inicio de sesión único en la Interfaz Web mediante una tarjeta inteligente. Para obtener más información, consulte Configuración del inicio de sesión único en la Interfaz Web mediante una tarjeta inteligente.

Citrix Gateway funciona con las siguientes versiones de la Interfaz Web:

- Interfaz web 4.5
- Interfaz web 5.0
- Interfaz web 5.1
- Interfaz web 5.2
- Interfaz web 5.3
- Interfaz Web 5.4

Antes de configurar el inicio de sesión único, asegúrese de que la Interfaz Web ya está configurada y funciona con NetScaler Gateway.

## Para configurar el inicio de sesión único en aplicaciones web globalmente

March 27, 2024

La aplicación de inicio de sesión único de forma global permitirá a un servicio Web autenticar todas las sesiones de aplicaciones web en lugar de autenticarlas en NetScaler Gateway.

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En el cuadro de diálogo **Configuración global de NetScaler Gateway**, en la ficha **Experiencia del cliente**, haga clic en Inicio de **sesión único** en aplicaciones web y, a continuación, haga clic en **Aceptar**.

## Para configurar el inicio de sesión único en aplicaciones web mediante una directiva de sesión

March 27, 2024

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway** > **Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Perfiles**, seleccione una directiva y, a continuación, haga clic en **Agregar**.
3. En el cuadro de diálogo **Configurar política de sesión** , junto a **Solicitar perfil** , haga clic en **Modificar** .
4. En el cuadro de diálogo **Configurar perfil de sesión**, en la ficha **Experiencia del cliente**, junto a Inicio de sesión único en aplicaciones web, haga clic en **Anulación global**, Inicio de **sesión único en aplicaciones web y, a** continuación, haga clic en **Aceptar**.

## Para definir el puerto HTTP para Single Sign-On en aplicaciones web

March 27, 2024

El inicio de sesión único solo se intenta para el tráfico de red en el que el puerto de destino se considera un puerto HTTP. Para permitir el inicio de sesión único en aplicaciones que utilizan un puerto distinto

del puerto 80 para el tráfico HTTP, agregue uno o varios números de puerto en NetScaler Gateway. Puede habilitar varios puertos. Los puertos se configuran globalmente.

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En la ficha **Configuración de red**, haga clic en **Configuración avanzada**.
4. En Puertos HTTP, escriba el número de puerto, haga clic en **Agregar** y, a continuación, haga clic en **Aceptar**.

> **Nota**: Si las aplicaciones web de la red interna utilizan números de puerto diferentes, escriba el número de puerto y, a continuación, haga clic en **Agregar**. Debe definir el número de puerto HTTP para permitir el inicio de sesión único en las aplicaciones web, incluida la interfaz web.

## Pautas de configuración adicionales

January 26, 2024

Al configurar la interfaz web para el inicio de sesión único, siga las siguientes pautas:

- La dirección URL del servicio de autenticación debe comenzar por https.
- El servidor que ejecuta la interfaz web debe confiar en el certificado de NetScaler Gateway y poder resolver el nombre de dominio completo (FQDN) del certificado en la dirección IP del servidor virtual.
- La interfaz web debe poder abrir una conexión con el servidor virtual de NetScaler Gateway. Se puede utilizar cualquier servidor virtual de Citrix Gateway para este fin; no tiene que ser el servidor virtual en el que los usuarios inician sesión.
- Si hay un firewall entre la interfaz web y NetScaler Gateway, las reglas de firewall pueden impedir el acceso de los usuarios, lo que inhabilita el inicio de sesión único en la interfaz web. Para solucionar este problema, relaje las reglas de firewall o cree otro servidor virtual en NetScaler Gateway al que se pueda conectar la interfaz web. El servidor virtual debe tener una dirección IP que se encuentra en la red interna. Al conectarse a la interfaz web, utilice el puerto seguro 443 como puerto de destino.
- Si utiliza un certificado de una entidad emisora de certificados (CA) privada para el servidor virtual, en Microsoft Management Console (MMC), utilice el complemento Certificados para instalar el certificado raíz de la entidad emisora de certificados en el almacén de certificados del equipo local del servidor que ejecuta la interfaz web.

- Cuando los usuarios inician sesión y reciben un mensaje de error de acceso denegado, consulte el visor de sucesos de la interfaz web para obtener más información.
- Para que las conexiones de usuario se lleven a cabo correctamente con aplicaciones o escritorios publicados, la Secure Ticket Authority (STA) que configuró en NetScaler Gateway debe coincidir con la STA que configuró en la interfaz web.

## Para probar la conexión de Single Sign-On a la Interfaz Web

January 26, 2024

Después de configurar el inicio de sesión único para la interfaz web, desde un dispositivo cliente, abra un explorador web y compruebe si la conexión se ha realizado correctamente.

1. En un explorador web, escriba `https://NetScalerGatewayFQDN`, donde NetScalerGatewayFQDN es el nombre de dominio completo (FQDN) del certificado vinculado al servidor virtual.
2. Inicie sesión en una cuenta de usuario de dominio de Active Directory. Al iniciar sesión, se le redirigirá a la interfaz web.

Las aplicaciones aparecen automáticamente sin autenticación adicional. Cuando los usuarios inician una aplicación publicada, Citrix Receiver dirige el tráfico a través del dispositivo NetScaler Gateway a los servidores de la comunidad.

## Configurar Single Sign-On en la Interfaz Web mediante una tarjeta inteligente

March 27, 2024

Si utiliza tarjetas inteligentes para el inicio de sesión de usuario, puede configurar el inicio de sesión único en la interfaz web. Se configuran los ajustes en NetScaler Gateway y, a continuación, se configura la interfaz web para que acepte el inicio de sesión único con una tarjeta inteligente. El inicio de sesión único también se denomina autenticación de paso.

Las versiones 5.3 y 5.4 de la interfaz web admiten el inicio de sesión único en la interfaz web mediante una tarjeta inteligente. Si habilita la función Interfaz Web en Citrix ADC disponible en la versión 10 de NetScaler, también puede utilizar el inicio de sesión único con una tarjeta inteligente. Para obtener más información sobre cómo configurar esta función, consulte Uso de la autenticación de tarjeta inteligente para la interfaz web a través de NetScaler Gateway.

Los usuarios pueden estar en varios grupos de CN en Active Directory para que funcione el inicio de sesión único, siempre que la extracción del nombre de usuario en la acción del certificado sea subjectAltName:PrincipalName. Si utiliza el parámetro subject:CN, los usuarios no pueden formar parte de varios grupos CN.

Para configurar NetScaler Gateway para el inicio de sesión único en la interfaz web mediante una tarjeta inteligente, debe hacer lo siguiente:

- Instale un certificado de servidor firmado desde una entidad de certificación (CA). Para obtener más información, consulte Instalación del certificado firmado en NetScaler Gateway.
- Instale un certificado raíz en NetScaler Gateway y en el dispositivo del usuario.
- Cree un servidor virtual como punto de inicio de sesión de la interfaz web. Al configurar el servidor virtual, debe establecer el parámetro SSL del certificado de cliente en Opcional. Para obtener más información sobre cómo configurar un servidor virtual, consulte Creación de servidores virtuales.
- Cree un servidor virtual secundario en el que la autenticación de cliente esté inhabilitada en los parámetros SSL. Esta configuración impide que los usuarios reciban una solicitud secundaria de su número de identificación personal (PIN).
- Cree una directiva de autenticación de certificados de cliente. En el campo Nombre de usuario, utilice el parámetro subjectAltName:principalName para extraer usuarios de varios grupos. Deje en blanco el campo Nombre del grupo.
- Cree una directiva de sesión y un perfil en NetScaler Gateway. En el perfil de sesión, habilita el proxy ICA y especifica la interfaz web y el dominio que utiliza para el inicio de sesión único.

Puede utilizar el procedimiento siguiente para crear un perfil de sesión para el inicio de sesión único con una tarjeta inteligente.

### Para crear un perfil de sesión para el inicio de sesión único mediante una tarjeta inteligente

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Políticas de Citrix Gateway y, a continuación, haga clic en Sesión.
2. En el panel de detalles, haga clic en la pestaña Perfiles y, a continuación, en Agregar .

3. En la pestaña Experiencia del cliente, junto a la página de inicio, haga clic en Anular global y, a continuación, desactive Mostrar página de inicio.

1. Junto a Inicio de sesión único en Aplicaciones web, haga clic en Anular Global y, a continuación, haga clic en Inicio de sesión único en Aplicaciones web.
2. Haga clic en la ficha Published Applications.
3. Junto a Proxy ICA, haga clic en Supedición global y, a continuación, selecciona ACTIVADO.

4. En Dirección de interfaz web, haga clic en Sobrescribir global y, a continuación, escriba el nombre de dominio completo (FQDN) o la interfaz web.
5. En Dominio de inicio de sesión único, haga clic en Anular global y, a continuación, escriba el nombre del dominio.

   > **Nota**: Debe usar el formato dominio y no el formato domain.com.

6. Haga clic en **Create** y, luego, en **Close**.

Una vez completado el perfil de sesión, configure la directiva de sesión y utilice el perfil como parte de la directiva. A continuación, puede enlazar la directiva de sesión al servidor virtual.

## Para configurar el certificado de cliente para Single Sign-On mediante una tarjeta inteligente

March 27, 2024

Si configura el inicio de sesión único en la interfaz web mediante una tarjeta inteligente, debe seleccionar Autenticación de
cliente en el cuadro de diálogo
Certificados del servidor virtual y, a continuación, configurar el certificado de cliente como
Opcional. Si selecciona
Obligatorio, se produce un error en el inicio de sesión único en la interfaz web.

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Citrix Gateway y, a continuación, haga clic en Servidores virtuales .
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, en Abrir .
3. En el cuadro de diálogo configurar el servidor virtual de NetScaler Gateway, en la ficha Certificados, haga clic en Parámetro SSL.
4. En el cuadro de diálogo Configurar parámetros SSL, en Otros, haga clic en Autenticación de cliente.
5. En Certificado de cliente, seleccione Opcional y, a continuación, haga doble clic en Aceptar.

## Para configurar Single Sign-On para Citrix Virtual Apps y recursos compartidos de archivos

March 27, 2024

Si los usuarios se conectan a servidores que ejecutan Citrix Virtual Apps y utilizan SmartAccess, puede configurar el inicio de sesión único para los usuarios que se conectan a la comunidad de servidores. Cuando configure el acceso a aplicaciones publicadas mediante una directiva y un perfil de sesión, utilice el nombre de dominio para la comunidad de servidores.

También puede configurar el inicio de sesión único para compartir archivos en la red.

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway** > **Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, seleccione una directiva de sesión y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar directiva de sesión**, junto a **Solicitar perfil**, haga clic en **Modificar**.
4. En el cuadro de diálogo **Configurar perfil de sesión**, en la ficha **Aplicaciones publicadas**, en Dominio de inicio de sesión único, haga clic en **Supeditación global**, escriba el nombre del dominio y, a continuación, haga clic en **Aceptar dos veces**.

## Permitir asociación de tipos de archivo

January 26, 2024

La asociación de tipos de archivos permite a los usuarios abrir documentos en aplicaciones publicadas a través de Citrix Virtual Apps or Desktops 7. Puede utilizar este permiso para permitir a los usuarios abrir y modificar documentos en servidores del entorno de confianza y evitar enviar el documento al dispositivo del usuario. Puede utilizar la asociación de tipos de archivo solo para los tipos de documento asociados a una aplicación publicada y solo si configura correctamente las propiedades del servidor virtual en NetScaler Gateway.

Proporcionar la asociación de tipos de archivo como único medio para modificar documentos de recursos puede ayudar a aumentar la seguridad porque requiere que la modificación se realice en el servidor y no en el dispositivo del usuario. Por ejemplo, puede optar por conceder la asociación de tipos de archivo para un recurso compartido de archivos en el que los empleados publican informes de las reuniones de proyecto en curso, sin ofrecer la posibilidad de descargarlos o cargarlos.

Para proporcionar una asociación de tipos de archivo se requiere que:

- Los usuarios ejecutan Citrix Receiver en el dispositivo del usuario.
- Los usuarios se conectan a través de un servidor virtual que tiene una directiva de tráfico enlazada y en el que usted configura la directiva para Citrix Virtual Apps.
- Los usuarios se asignan a las aplicaciones deseadas en Citrix Virtual Apps and Desktops 7.
- Los administradores configuran Citrix Virtual Apps para que funcionen con Citrix Gateway.

Los pasos para crear una asociación de tipos de archivo incluyen:

- Creación de un sitio de interfaz web.
- Configuración de la asociación de tipos de archivo mediante una directiva de tráfico en NetScaler Gateway.
- Definir extensiones de archivos en Citrix Virtual Apps and Desktops 7.

## Crear un sitio de la Interfaz Web

March 27, 2024

Para configurar la Interfaz Web para que funcione con la asociación de tipos de archivo, primero debe crear el sitio de la Interfaz Web. El sitio de Interfaz Web puede estar en Control de acceso directo o avanzado. Copie los siguientes directorios en el sitio de Interfaz Web:

- app_data
- autenticación
- sitio

Al copiar estos directorios en el sitio de la Interfaz Web, los directorios existentes se sobrescriben.

Si utiliza la Interfaz Web 4.6 o 5.0, abra el archivo web.config en el directorio del sitio de la Interfaz Web y agregue el siguiente código. Puede descargar este código desde el sitio de Citrix Support en.http://support.citrix.com/article/ctx116253

```
pre codeblock
<location path="site/contentLaunch.ica">
<system.web>
<httpHandlers>
<add verb="*" path="*.ica" type="System.Web.UI.PageHandlerFactory"/>
</httpHandlers>
</system.web>
</location>
<location path="site/contentLaunch.rad">
<system.web>
<httpHandlers>
<add verb="*" path="*.rad" type="System.Web.UI.PageHandlerFactory"/>
</httpHandlers>
</system.web>
</location>
<!--NeedCopy-->
```

Este código debe agregarse después de la siguiente sección del archivo web.config:

```
pre codeblock
<location path="site/launch.rad">
```

```
3          <system.web>
4              <httpHandlers>
5                  <add verb="*" path="*.rad" type="System.Web.UI.
                       PageHandlerFactory"/>
6              </httpHandlers>
7          </system.web>
8      </location>
9  <!--NeedCopy-->
```

## Configurar NetScaler Gateway para la asociación de tipos de archivo

March 27, 2024

Antes de configurar la asociación de tipos de archivos en Citrix Gateway, configure un sitio de la Interfaz Web para que funcione con la asociación de tipos de archivo. Después de crear y configurar la interfaz web, debe crear la configuración en NetScaler Gateway. Los pasos incluyen:

- Creación de un nuevo servidor virtual o uso de uno existente. Para obtener más información sobre cómo crear un servidor virtual, consulte Creación de servidores virtuales.
- Crear una nueva política de sesión y un perfil que tengan configurada la Interfaz Web.
- Enlace de la directiva de sesión al servidor virtual.
- Creación de una directiva de tráfico.

Después de crear la directiva de sesión y vincularla al servidor virtual, cree la directiva de tráfico y enlaza también al servidor virtual.

Al configurar una política de tráfico para la asociación de tipos de archivo, se crea una expresión para definir las extensiones de archivo. Por ejemplo, quiere habilitar la asociación de tipos de archivo para Microsoft Word y Microsoft Excel. Un ejemplo de expresión es:

```
REQ.HTTP.URL == /\*.doc || REQ.HTTP.URL == /\*.xls
```

### Para crear una directiva de sesión y un perfil para la asociación de tipos de archivo

1. En la utilidad de configuración, haga clic en la ficha **Configuración** y, a continuación, en el panel de navegación, expanda **NetScaler Gateway** > **Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en **Nuevo** .
5. En Nombre , escriba un nombre para el perfil.
6. En la ficha **Aplicaciones publicadas**, configure los siguientes valores:

a) Junto a Dirección de interfaz web, haga clic en **Anular global** y, a continuación, escriba la dirección web de la interfaz web.
b) Junto a Modo de portal de interfaz web, haga clic en **Sobrescribir global** y, a continuación, seleccione Normal o Compacto.
c) Junto a Dominio de inicio de sesión único, haga clic en **Anular global** , escriba el nombre del dominio en el que residen las cuentas de usuario y, a continuación, haga clic en **Crear**.

7. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresión con nombre**, seleccione **Valor verdadero**, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

### Para crear un perfil de tráfico para la asociación de tipos de archivo

1. En la utilidad de configuración, en la pestaña **Configuración** , en el panel de navegación, expanda Políticas de Citrix Gateway y, a continuación, haga clic en Tráfico.
2. En el panel de detalles, haga clic en la pestaña Perfiles y, a continuación, en Agregar .
3. En Nombre , escriba un nombre para el perfil.
4. En Asociación de tipos de archivo, seleccione Activar, haga clic en Crear y, a continuación, en Cerrar.

### Para configurar la asociación de tipos de archivo en una directiva de tráfico

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Políticas de Citrix Gateway y, a continuación, haga clic en Tráfico.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. En Solicitar perfil, seleccione un perfil.
5. En el cuadro de diálogo **Crear directiva de tráfico**, en Expresiones, seleccione Forma libre avanzada y, a continuación, haga clic en **Agregar**.
6. En el cuadro de diálogo **Agregar expresión**, haga lo siguiente:

   a) En **Tipo de expresión**, haga clic en **General**.
   b) En Tipo de flujo, seleccione REQ.
   c) En Protocol, seleccione HTTP.
   d) En Calificador, selecciona URL.
   e) En Operador, seleccione = =.
   f) En Valor, escriba /*.FileExtensionType, donde.FileExtensionType es el tipo de archivo, como.doc o.xls y, a continuación, haga clic en **Aceptar**.

7. En el cuadro de diálogo **Crear directiva de tráfico**, en **Expresiones**, junto a Forma libre avanzada, haga clic en **O**.

8. Repita los pasos 4, 5 y 6 para cada extensión de archivo que desee incluir, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

## Integrar NetScaler Gateway en Citrix Virtual Apps and Desktops

January 26, 2024

Los servidores de StoreFront se implementan y se configuran para administrar el acceso a los datos y los recursos publicados. Para el acceso remoto, se recomienda agregar Citrix Gateway y colocarlo delante de StoreFront.

> **Nota**
>
> Para obtener pasos de configuración detallados sobre cómo integrar Citrix Virtual Apps and Desktops con NetScaler Gateway, consulte ladocumentación de StoreFront.

En el siguiente diagrama se muestra un ejemplo de implementación de Citrix simplificada de Citrix que incluye NetScaler Gateway. NetScaler Gateway se comunica con StoreFront para proteger las aplicaciones y los datos que entregan Citrix Virtual Apps and Desktops. Los dispositivos de usuario ejecutan Citrix Receiver para crear una conexión segura y acceder a sus aplicaciones, escritorios y archivos.


Los usuarios inician sesiones y se autentican mediante Citrix Gateway. Citrix Gateway se implementa y se protege en la zona DMZ. Se configura la autenticación de dos factores. En función de sus credenciales de usuario, los usuarios reciben los recursos y las aplicaciones que les corresponden. Las aplicaciones y los datos se encuentran en los servidores adecuados (no aparecen en el diagrama). Se utilizan servidores independientes para los datos y las aplicaciones confidenciales de seguridad.

# Integrar NetScaler Gateway en StoreFront

March 27, 2024

El asistente**Citrix Virtual Apps and Desktops** se utiliza para integrar StoreFront con NetScaler Gateway. La integración facilita el acceso a escritorios virtuales alojados (XenDesktop) y aplicaciones virtuales de Windows alojadas (XenApp) a través de NetScaler Gateway.

Para la integración de NetScaler Gateway con StoreFront, el flujo de trabajo del asistente de Citrix Virtual Apps and Desktops se ha mejorado con las siguientes capacidades.

- **Recuperación de los almacenes configurados en el StoreFront compatible:** Los almacenes configurados en StoreFront compatible se pueden recuperar con un clic. Este método de recuperación ayuda a evitar la intervención manual, evitando errores humanos (errores tipográficos).
- **Compatibilidad con la exportación del archivo de configuración de StoreFront:** Los archivos de configuración de StoreFront se pueden exportar en NetScaler Gateway. El archivo de configuración de StoreFront se puede descargar y, finalmente, importar en un servidor StoreFront compatible. Una vez importado el archivo, StoreFront completa la integración de NetScaler.
- **StoreFront** como servidor de autenticación: la**autenticación** se simplifica mediante la introducción de una acción de autenticación avanzada para utilizar StoreFront como servidor de autenticación para los servicios de autenticación.

> **Nota:**El servidor de autenticación también se puede utilizar para implementaciones que no sean de Citrix Virtual Apps and Desktops.

## Cómo configurar NetScaler Gateway para utilizarlo con StoreFront

### Requisitos previos

Debe disponer de la siguiente información para integrar NetScaler con StoreFront:

- Dirección IP del servidor virtual de NetScaler Gateway
- Nombre de dominio completo (FQDN) del servidor de StoreFront
- Un certificado de servidor para NetScaler Gateway
- Detalles del servidor de autenticación

Asegúrese también de lo siguiente:

- El puerto de firewall entre NetScaler Gateway y StoreFront está abierto
- StoreFront tiene acceso LAN

**Para integrar StoreFront con NetScaler Gateway mediante GUI de NetScaler Gateway:**

1. Haga clic en la ficha **Configuración**.
2. En **Integración con productos Citrix**, haga clic en **XenApp y XenDesktop**.
3. Haga clic en **Comenzar.**
4. Seleccione **StoreFront** y haga clic en **Continuar.**
5. Introduzca los valores de los campos siguientes en el área de NetScaler Gateway y haga clic en **Continuar.**

    - **FQDN de puerta** de enlace: FQDN de NetScaler Gateway
    - **Dirección IP de puerta** de enlace: dirección IP de NetScaler Gateway
    - **Puerto**: Puerto de NetScaler Gateway

6. Importe los siguientes archivos en el área **Certificado de servidor** y haga clic en **Continuar**. **Archivo de certificado**: Certificado de servidor para NetScaler Gateway.
7. Proporcione la siguiente información en el área de **StoreFront** y haga clic en **Continuar**.

    - **URL de StoreFront**: URL del servidor de StoreFront
    - Ruta de acceso de**Receiver para Web: ruta** de acceso a Receiver para el sitio web ya configurado en StoreFront
    - **Dominio de Active Directory predeterminado**: Dominio de inicio de sesión único que se utilizará para aplicaciones de inicio de sesión único en la red interna
    - **URL de Secure Ticket Authority**: URL de Secure Ticket Authority, normalmente presente en el controlador de entrega

    > **Nota:** Al elegir "**Recuperar almacenes**", NetScaler Gateway se pone en contacto con StoreFront y devuelve toda la información de los almacenes configurados en StoreFront. A continuación, puede seleccionar Almacén preferido en el menú desplegable. La opción "**Recuperar almacenes**"solo funciona para el servidor de StoreFront más reciente.

8. Con la nueva configuración de autenticación, un usuario puede crear una directiva de autenticación o puede usar una directiva de autenticación existente.

    Para crear una directiva de autenticación basada en dominio, introduzca los valores de los campos siguientes en y haga clic en **Continuar**.

9. **Elija Tipo de autenticación -** Seleccionar dominio en el menú desplegable
10. Seleccione **Agregar nuevo servidor** o **Usar servidor existente** según sus necesidades

    - **Dirección IP**: Dirección IP del servidor de dominio

- **Puerto**: Puerto del servidor de dominio
- **DN base**: El DN base bajo el que se encuentran los usuarios
- **Cuenta de servicio**: La cuenta utilizada para consultar Active Directory
- **Contraseña**: La contraseña necesaria para iniciar sesión en el servidor de dominio
- **Tiempo de espera**: El tiempo durante el que se busca el directorio de dominio
- **Atributo de nombre de inicio de sesión del servidor**: Atributo de nombre utilizado por el dispositivo NetScaler para consultar el servidor de dominio externo o Active Directory.

Si lo quiere, puede hacer clic en **Probar conexión** para asegurarse de que se puede acceder al servidor y de que se proporcionan credenciales válidas.

> **Nota:**Para usar una política de autenticación existente, seleccione el **tipo de autenticación** requerido en la lista **Elegir tipo de autenticación** y proporcione la información indicada anteriormente.

11. En la página Configurar NetScaler Gateway, haga clic en **Listo.**
12. Haga clic en **Descargar archivo.**

**A continuación se indican los pasos de configuración necesarios en la GUI de StoreFront:**

1. Copie el archivo Gatewayconfig.zip en StoreFront.
2. Haga clic en **Almacenes**.
3. Seleccione **Administrar Citrix Gateways** y haga clic en el enlace **Importado desde archivo** de la ventana **Administrar Citrix Gateways**.
4. En el área **Seleccionar archivo** de la ventana **Importar configuración de NetScaler**, haga clic en **Siguiente**.
5. En el área **Seleccionar tipo de inicio** de sesión, puede proporcionar una **URL de devolución** de llamada para que StoreFront se ponga en contacto con NetScaler Gateway y haga clic en **Siguiente**.
6. En Autoridades de tíquets seguros, haga clic en Siguiente.
7. En **Revisar cambios**, haga clic en **Siguiente**.
8. Haga clic en **Finalizar**.

## Configurar parámetros para el entorno de Citrix Endpoint Management

January 26, 2024

El asistente NetScaler ADC para Citrix Endpoint Management le guía a través de la configuración de las funciones de NetScaler ADC para su implementación de Citrix Endpoint Management. Puede utilizar el asistente para:

- **Configure una Micro VPN.** En este caso, los usuarios remotos pueden acceder a aplicaciones y escritorios de la red interna.
  - Para el modo solo MAM de Citrix Endpoint Management, debe usar NetScaler Gateway para la autenticación.
  - Para implementaciones MDM, Citrix recomienda NetScaler Gateway para la VPN de dispositivos móviles.
  - Para implementaciones de ENT, si un usuario opta por no inscribirse en MDM, el dispositivo funciona en el modo MAM heredado y se inscribe mediante el FQDN de NetScaler Gateway.
- **Configure la autenticación basada en certificados.** La configuración predeterminada de Citrix Endpoint Management es la autenticación de nombre de usuario y contraseña. Para agregar otra capa de seguridad para la inscripción y el acceso al entorno de Citrix Endpoint Management, considere la posibilidad de utilizar la autenticación basada en certificados.
- **Equilibrio de carga de servidores Citrix Endpoint Management.** El equilibrio de carga de NetScaler ADC es necesario para todos los modos de dispositivo de Citrix Endpoint Management si tiene varios servidores Citrix Endpoint Management o si Citrix Endpoint Management se encuentra dentro de la red DMZ o interna (y, por lo tanto, el tráfico fluye de los dispositivos a NetScaler ADC a Citrix Endpoint Management). En este caso, el dispositivo NetScaler ADC reside en la DMZ entre el dispositivo del usuario y los servidores Citrix Endpoint Management para equilibrar la carga de los datos enviados cifrados desde dispositivos móviles a los servidores de Citrix Endpoint Management.
- **Equilibrio de carga servidores Microsoft Exchange con filtrado de correo electrónico.** En este caso, el dispositivo NetScaler ADC se encuentra entre el dispositivo de usuario y NetScaler ADC Connector (XNC) de Citrix Endpoint Management y entre el dispositivo de usuario y los servidores CAS de Microsoft Exchange. Todas las solicitudes de los dispositivos de usuario van al dispositivo NetScaler Gateway, que luego se comunica con el XNC para recuperar información sobre el dispositivo. Según la respuesta del XNC, el dispositivo NetScaler ADC reenvía la solicitud desde un dispositivo de la lista de permitidos al servidor de la red interna o interrumpe la conexión desde un dispositivo de la lista de prohibidos.
- **Equilibrio de carga ShareFile StorageZones Connectors basado en el tipo de contenido solicitado.** En este escenario, se solicita información básica sobre el entorno de StorageZones Controller y, a continuación, se genera una configuración que hace lo siguiente:
  - Equilibra la carga del tráfico entre los controladores de zonas de almacenamiento.
  - Proporciona autenticación de usuario para los conectores StorageZones.
  - Valida las firmas URI para las cargas y descargas de ShareFile.
  - Termina las conexiones SSL en el dispositivo NetScaler ADC.

Para obtener más información sobre cómo configurar ShareFile, consulte Configurar NetScaler ADC para Storage Zones Controller.

> **Importante**
>
> Antes de utilizar el asistente de Citrix Endpoint Management, consulte estos artículos de Citrix Endpoint Management Deployment para obtener información y recomendaciones sobre diseño e implementación:
>
> Integración de Citrix Endpoint Management
>
> Integración en NetScaler Gateway y NetScaler ADC
>
> Consideraciones sobre SSO y proxies para aplicaciones MDX
>
> Autenticación
>
> Puede utilizar NetScaler ADC for Citrix Endpoint Management Wizard solo una vez. Si quiere varias instancias de Citrix Endpoint Management, por ejemplo, para entornos de prueba, desarrollo y producción, debe configurar NetScaler ADC para los entornos adicionales de forma manual. En los siguientes artículos de soporte se enumeran los comandos que ejecuta el asistente y se proporcionan instrucciones para ejecutarlos para crear una instancia de NetScaler ADC:
>
> Comandos generados por Citrix Endpoint Management Wizard en NetScaler ADC - SSL Bridge
>
> Comandos generados por Citrix Endpoint Management Wizard en NetScaler ADC - Descarga SSL

### Requisitos de licencia para las funciones de NetScaler ADC

Debe instalar licencias para habilitar las siguientes funciones de NetScaler ADC:

- El equilibrio de carga de MDM de Citrix Endpoint Management requiere una licencia estándar de NetScaler ADC.
- El equilibrio de carga de ShareFile con StorageZones requiere una licencia estándar de NetScaler ADC.
- El equilibrio de carga de Exchange requiere una licencia Citrix ADC o una licencia Enterprise con la adición de una licencia de almacenamiento en caché integrado.

### Asistente de NetScaler ADC para Citrix Endpoint Management

En esta sección se proporciona un ejemplo del uso del asistente NetScaler ADC para Citrix Endpoint Management para:

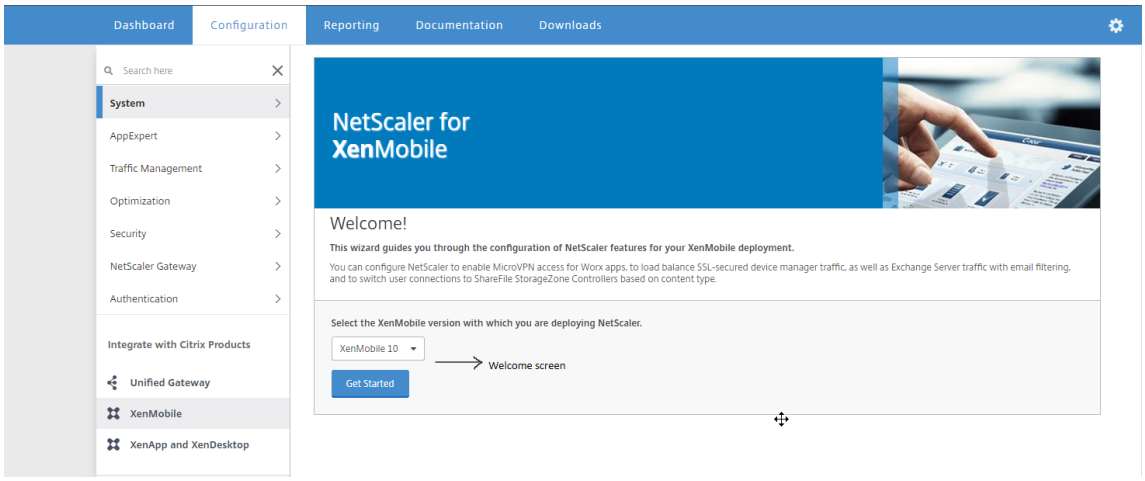
- Configurar el acceso micro VPN para conexiones de usuarios remotos a los recursos administrados por Citrix Endpoint Management en su red interna

- Configure la autenticación basada en certificados. Para obtener información sobre cómo obtener e instalar un certificado SSL público, consulte Instalación y administración de certificados.
- Configurar el equilibrio de carga para los servidores Citrix Endpoint Management.

Para utilizar el asistente:

1. En la utilidad de configuración, haga clic en la ficha **Configuración** y, a continuación, haga clic en **Citrix Endpoint Management**.




2. Seleccione su versión de Citrix Endpoint Management y, a continuación, haga clic en **Comenzar**.
3. Seleccione las casillas de verificación de las funciones que quiera configurar. Tenga en cuenta que solo puede usar este asistente una vez, por lo que debe realizar la configuración posterior de forma manual. En estas instrucciones se supone que selecciona la siguiente configuración:
   **Acceso a través de NetScaler Gateway** (para Citrix Endpoint Management ejecutándose en modos ENT o MAM)
   **Equilibrio de carga Servidores Citrix Endpoint Management**
4. En la página **Configurar NetScaler Gateway**, introduzca valores para la **dirección IP, el**puerto**y el**nombre del servidor virtual**de NetScaler Gateway** externos.
5. En la página **Certificado de servidor para NetScaler Gateway**, en el menú desplegable **Archivo de certificado**, elija el archivo de certificado en **Local** o **Appliance**. Si el certificado está en un equipo local:

   Si el certificado está en el dispositivo:
6. En la página **Configuración de autenticación**, en el campo **Método de autenticación principal**, seleccione **Certificado de cliente**.

   Esto seleccionará automáticamente **Use existing certificate policy** y **Cert Auth** en los siguientes dos campos. El siguiente procedimiento presupone que ya dispone de una directiva de certificados.

Si debe crear una directiva de certificados, haga clic en **Crear directiva de certificados** y complete la configuración. En la pantalla **Citrix Endpoint Management Certificate**, elija un certificado de servidor existente o instale un certificado nuevo. Si ejecuta varios servidores Citrix Endpoint Management, agregue un certificado para cada uno de ellos. **En Atributo de nombre de inicio de sesión del servidor**, especifique **userPrincipalName** o **sAMAccountName**, según sus requisitos.

- a.Seleccione **Haga clic aquí para cambiar el certificado de CA** y, a continuación, en la lista **Examinar**, vaya al certificado de CA que desee.
- b. Con el certificado de cliente como tipo de autenticación principal, tiene la opción de configurar LDPA (o RADIUS) como tipo de autenticación secundario.

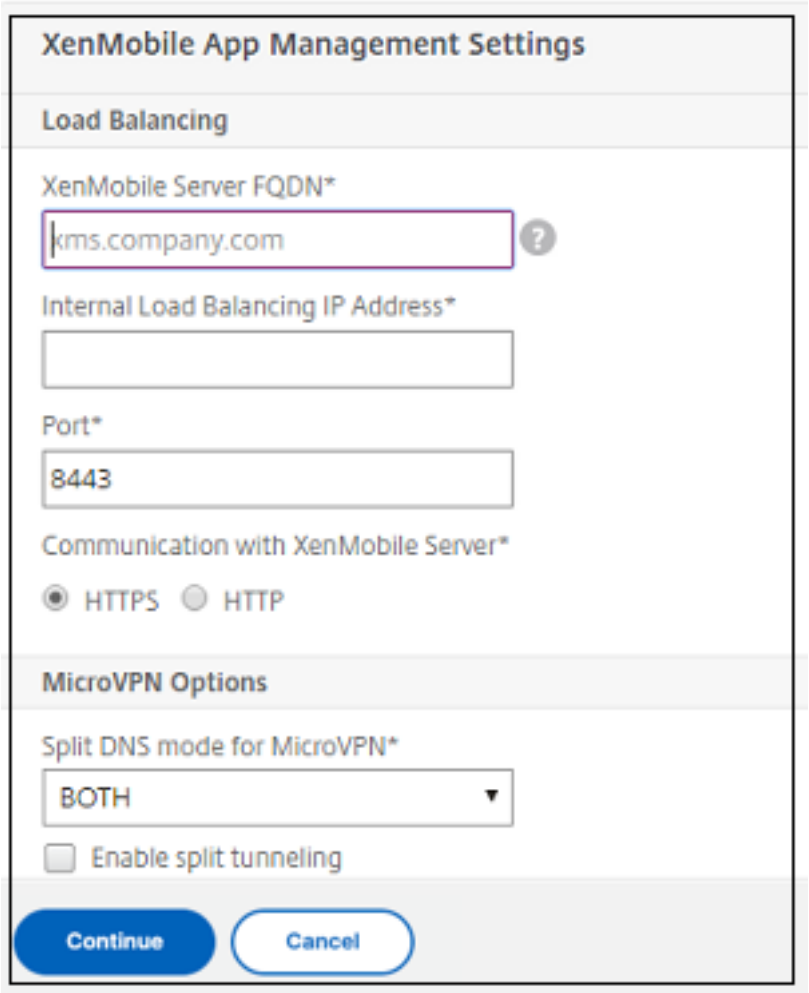
  Para utilizar solo autenticación de certificados de cliente, deje **Segundo método de autenticación** como **Ninguno** y, a continuación, haga clic en **Continuar**.

  Para utilizar la autenticación de dominio de certificado de cliente + (LDAP), cambie el **método de segunda autenticación** a **LDAP** y configure la configuración del servidor de autenticación.
- c. En la pantalla **Certificado de dispositivo**, si el certificado aún no está instalado, debe exportar este certificado desde la consola de Citrix Endpoint Management: desde la consola, haga clic en el icono de engranaje situado en la esquina superior derecha para abrir la pantalla **Configuración**.
- d. Haga clic en **Certificado** y, a continuación, seleccione el certificado de CA de la lista.
- e. Haga clic en **Exportar**.
- f. Vuelva al asistente de NetScaler ADC y seleccione el certificado que exportó (descargó) para instalarlo.
- g. Haga clic en **Continuar**.

Aparecen las direcciones IP de Citrix Endpoint Management que ha configurado.

7. Configure la configuración de **administración de aplicaciones Citrix Endpoint Management**.

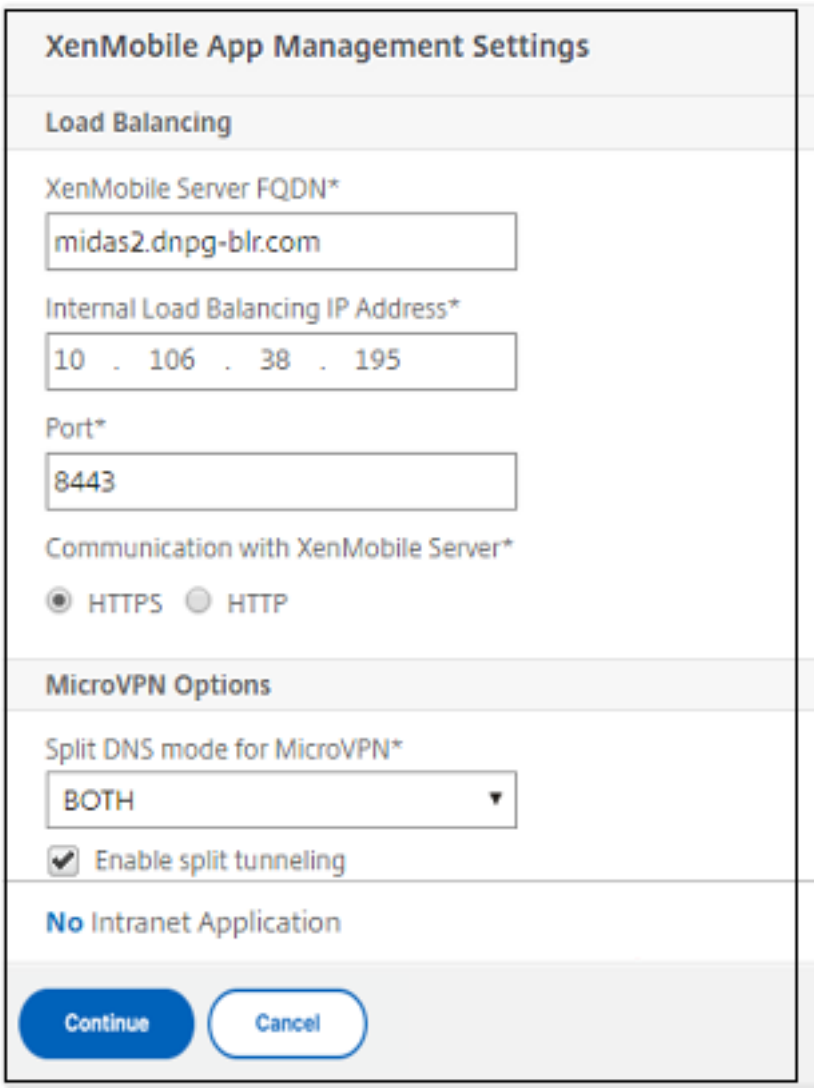



- Introduzca el **FQDN de Citrix Endpoint Management**. Este es el FQDN de equilibrio de carga para MAM.
- Introduzca una **dirección IP de equilibrio de carga interna solo para MAM** para el servidor virtual que equilibra la carga de los servidores Citrix Endpoint Management. NetScaler Gateway se comunica con Citrix Endpoint Management a través de esta IP virtual de equilibrio de carga de MAM.
- Se trata de una implementación de descarga SSL, por lo que seleccione **HTTP** en **Comunicación con Citrix Endpoint Management Server**.
- El **modo DNS dividido para el campo MicroVPN** se establece automáticamente en **AMBOS**.

Si su implementación requiere túneles divididos, seleccione **Habilitar túnel dividido**. A continuación, debe configurar el enlace de aplicaciones de intranet si habilita la tunelización dividida.

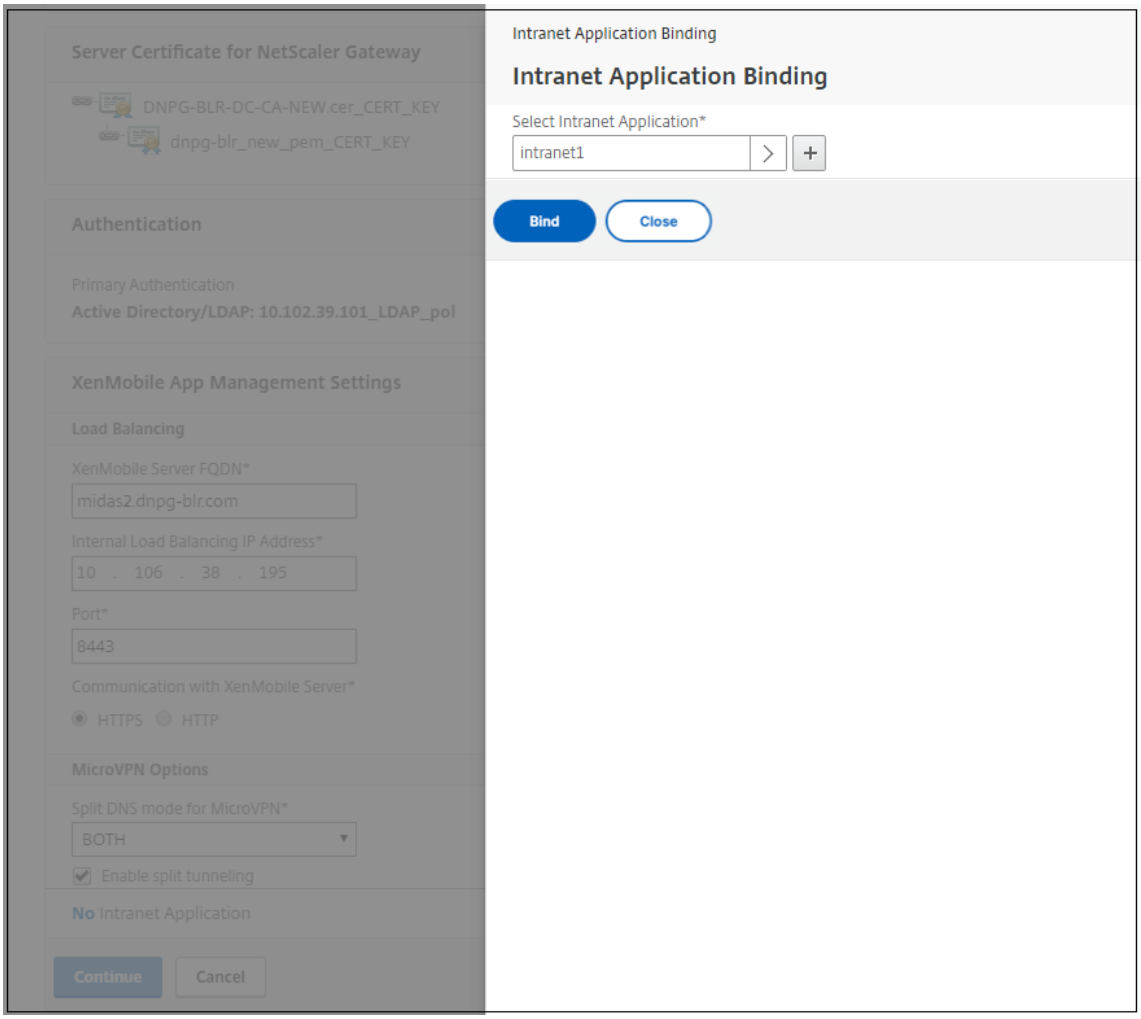
De forma predeterminada, el acceso Secure Web se tuneliza a la red interna, lo que significa que Secure Web utiliza un túnel VPN por aplicación de vuelta a la red interna para todos los accesos a la red y el dispositivo NetScaler ADC utiliza la configuración del túnel dividido.



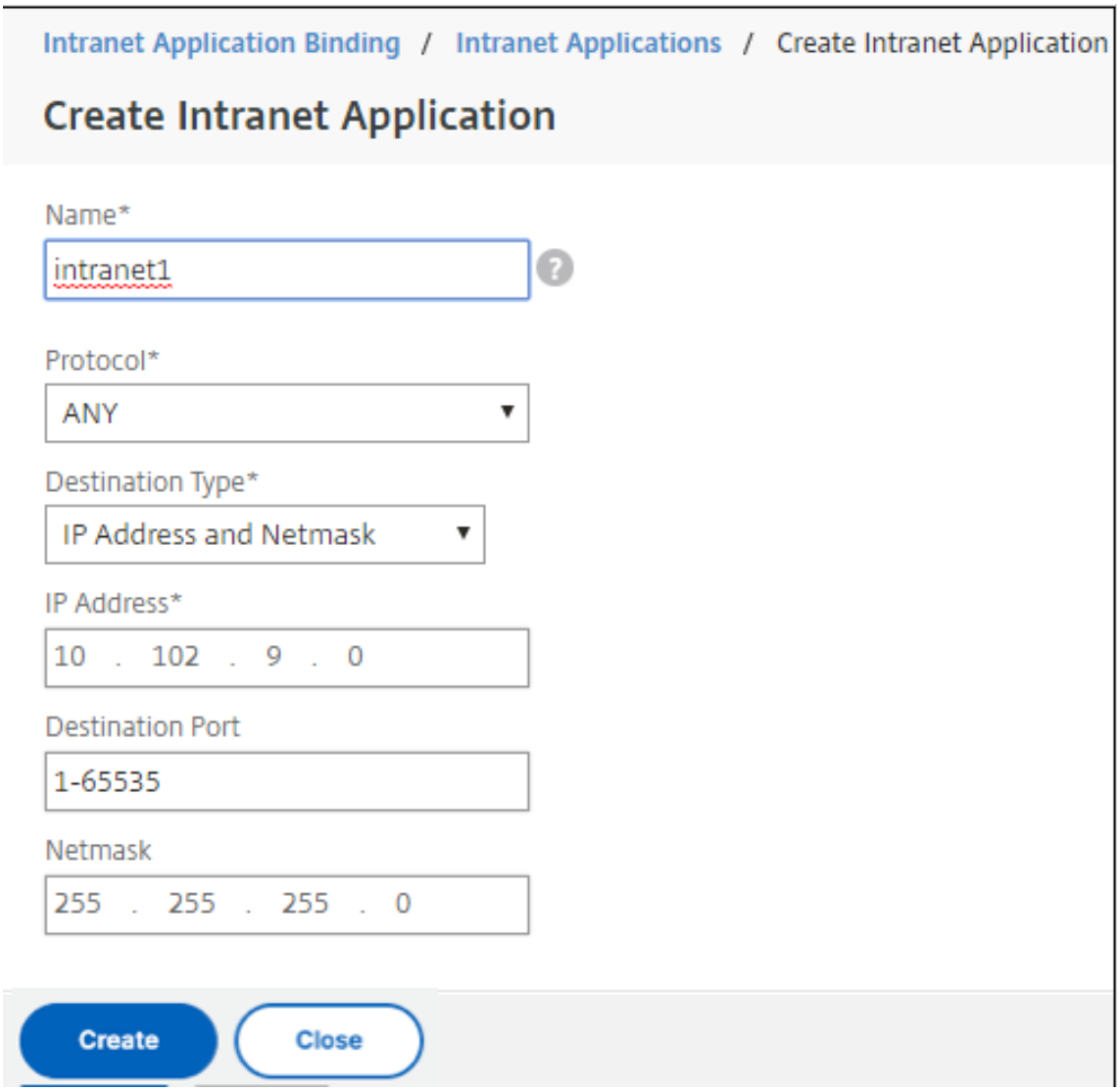

8. Para configurar reglas de interceptación para las conexiones de usuario en NetScaler Gateway, debe configurar el **enlace de aplicaciones de intranet**. Haga clic en **+** para agregar un enlace.

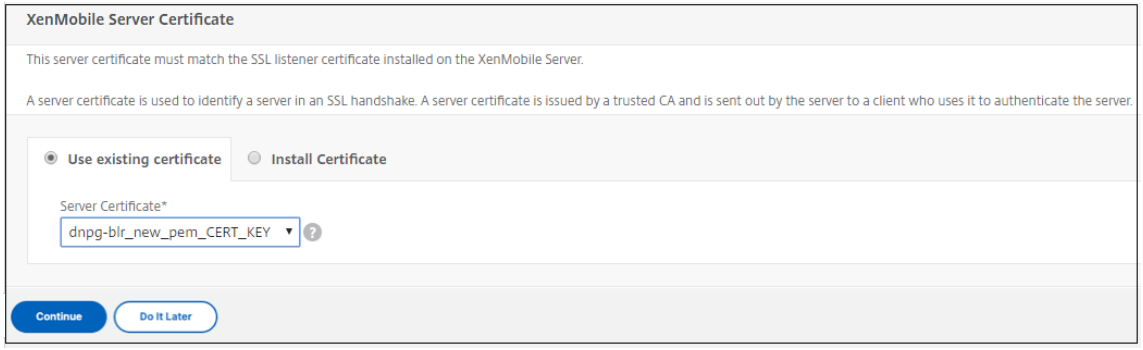



9. Complete los parámetros para permitir el acceso a la red y haga clic en **Crear**.

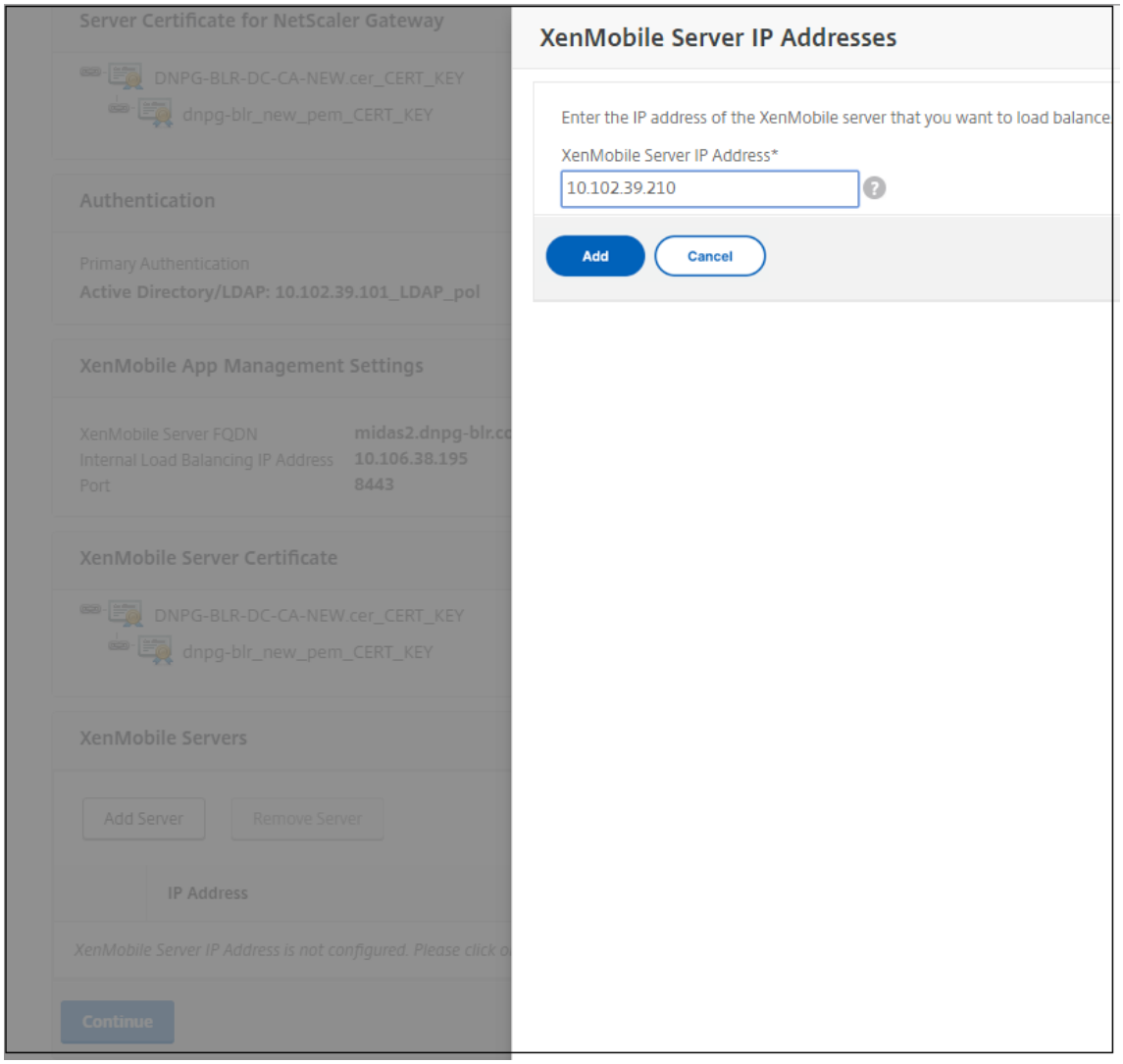



10. Agregue el certificado de Citrix Endpoint Management. Se usará para el servidor virtual de equilibrio de carga MAM.



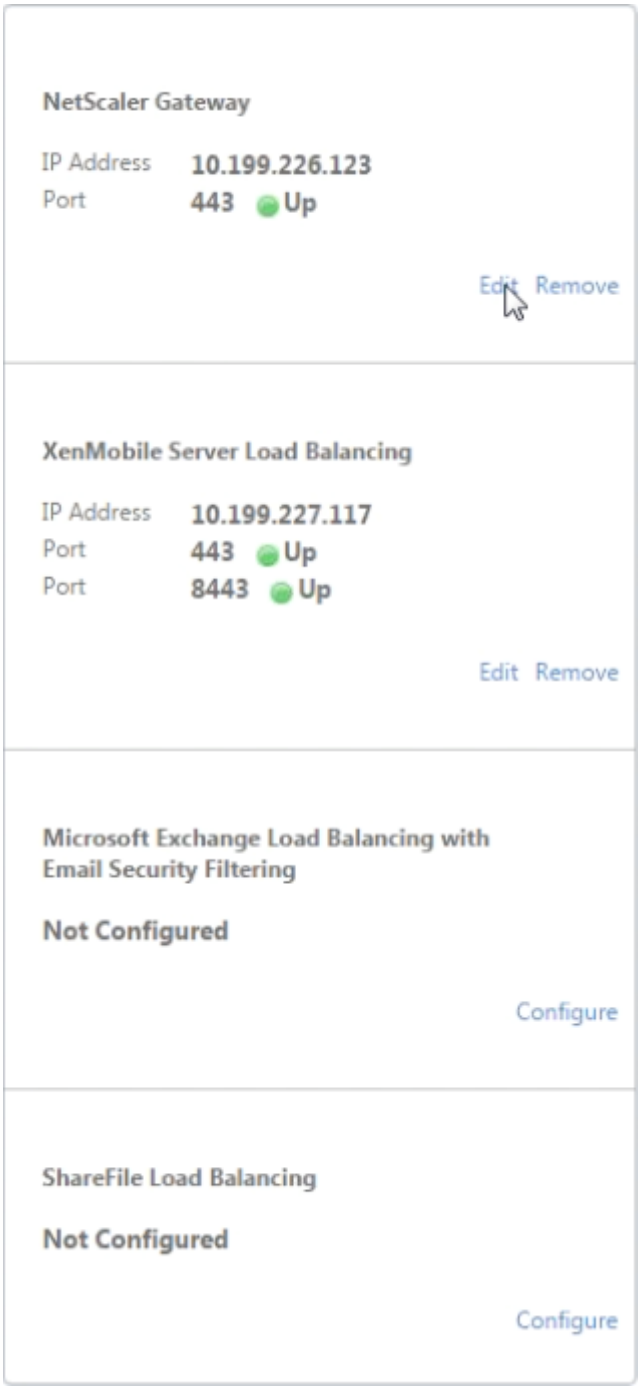

11. En **Servidores Citrix Endpoint Management**, haga clic en **Agregar servidor** para agregar la **dirección IP de Citrix Endpoint Management**para enlazar a la IP virtual de equilibrio de carga.




12. En el panel de control de NetScaler ADC, confirme que el equilibrio de carga de NetScaler Gateway y Citrix Endpoint Management está configurado de la siguiente manera.




Si va a utilizar los atributos SAMAccount en los certificados de usuario como alternativa al nombre principal de usuario (UPN), configure el perfil del certificado como se describe en Configuración manual de Citrix Gateway para la autenticación de certificados de cliente .

# Configuración de servidores de equilibrio de carga para Citrix Endpoint Management o Citrix Endpoint Management

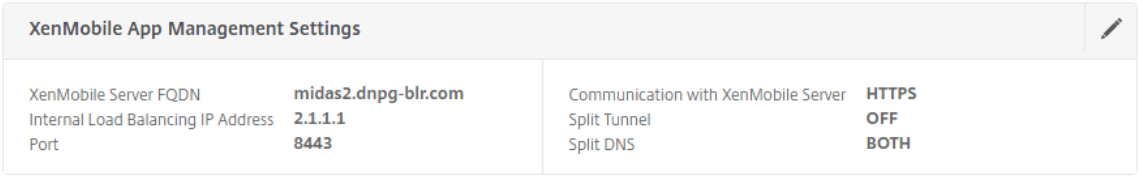
January 26, 2024

Después de utilizar el asistente de **NetScaler ADC para Citrix Endpoint Management** para la configuración inicial, utilice la utilidad de configuración de NetScaler Gateway para configurar el equilibrio de carga, como se describe en esta sección. Para Citrix Endpoint Management, utilice Descarga SSL. Para Citrix Endpoint Management Server, asegúrese de consultar las recomendaciones para los modos de equilibrio de carga en "Resumen de implementación"en Integración con NetScaler Gateway y NetScaler ADC.

## Para usar el modo Puente SSL para los VIP de Citrix ADC

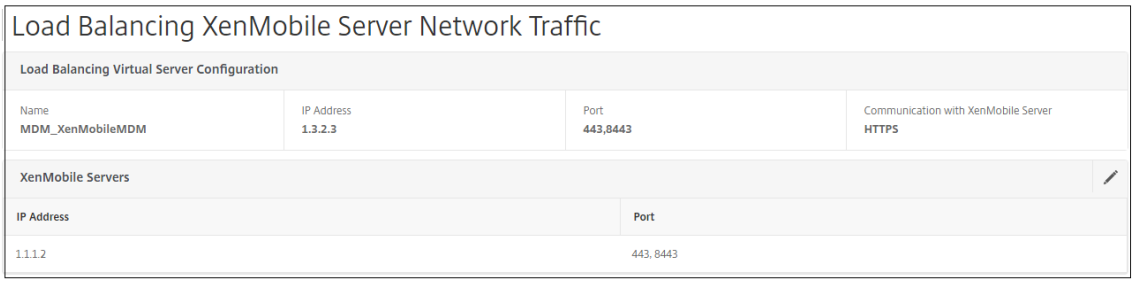
Utilice el modo Puente SSL si Citrix Endpoint Management está en la DMZ. Al equilibrar la carga de Citrix Endpoint Management con los VIP de Citrix ADC en modo SSL Bridge, el tráfico de Internet fluye directamente al servidor Citrix Endpoint Management, donde terminan las conexiones. El modo Puente SSL es el más simple de configurar. También son más fáciles de solucionar los problemas que causa.

1. Antes de configurar el modo Puente SSL, vaya a **Configuración de administración de aplicaciones Citrix Endpoint Management** y compruebe que **Comunicación con Citrix Endpoint Management Server** es **HTTPS**.

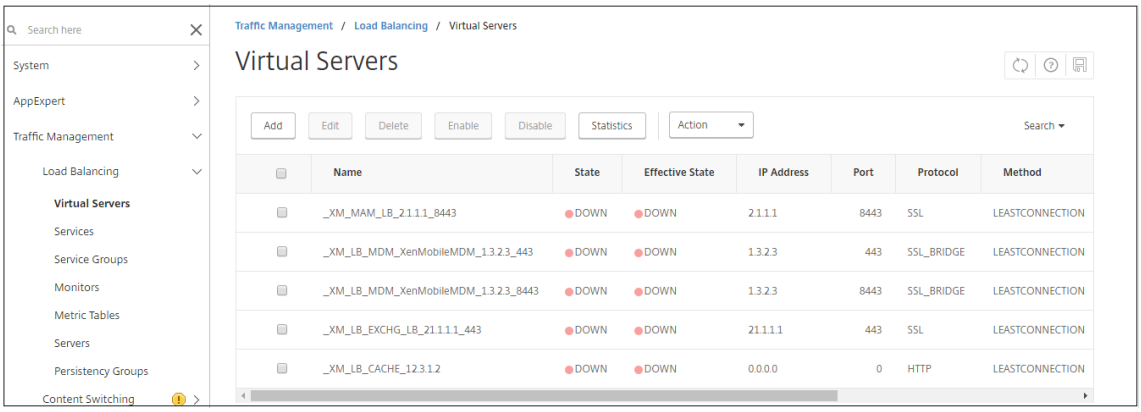



2. Después de iniciar sesión en la utilidad de configuración, en la ficha **Inicio**, en **MDM Server LB**, haga clic en **Configurar**.
3. En **Servidor virtual LB para administración de dispositivos**, en **Nombre**, escriba un nombre para el servidor.
4. En **Dirección IP**, escriba la dirección IP del servidor virtual y, a continuación, haga clic en **Continuar**.
5. En la página **Equilibrio de carga de Citrix Endpoint Management MDM Servers**, repita los pasos 3 y 4 y, a continuación, haga clic en **Crear**.
6. Compruebe que la configuración sea correcta y, a continuación, haga clic en **Listo**.




7. Para verificar la configuración del equilibrio de carga, vaya a **Administración del tráfico > Servidores virtuales**.




### To use SSL Offload mode for NetScaler ADC VIPs

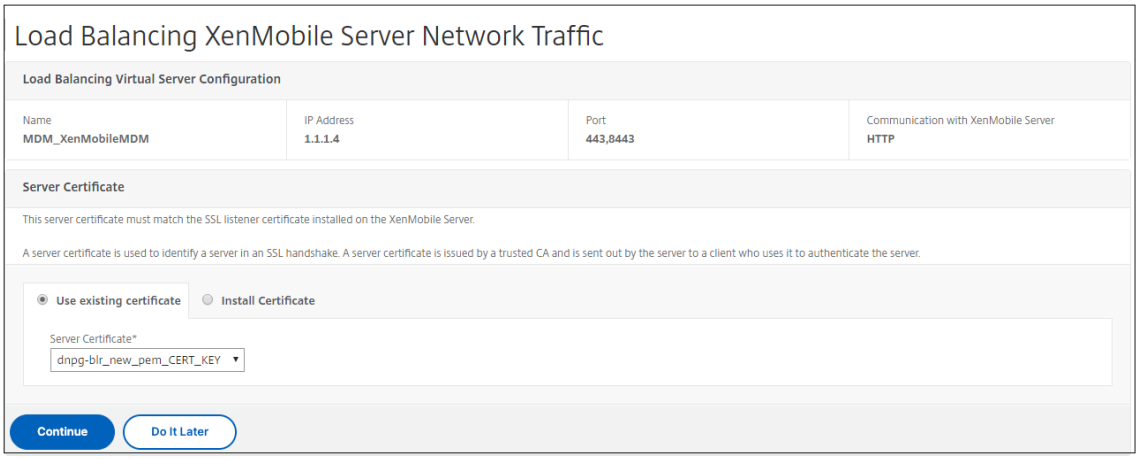
Utilice la descarga de SSL para Citrix Endpoint Management. Utilice también SSL Offload, si es necesario para cumplir con los estándares de seguridad, cuando el dispositivo Citrix Endpoint Management local esté en la red interna. Al equilibrar la carga de Citrix Endpoint Management con VIP de NetScaler ADC en modo Descarga SSL, el tráfico de Internet fluye directamente al dispositivo NetScaler ADC, donde finalizan las conexiones. A continuación, NetScaler Gateway establece nuevas sesiones desde el dispositivo a Citrix Endpoint Management. El modo Descarga de SSL implica una complejidad adicional durante la configuración y la solución de problemas.

1. Antes de configurar el modo de descarga SSL, vaya a **Citrix Endpoint Management App Management Settings** y compruebe que **Comunicación con Citrix Endpoint Management Server** es **HTTP**.

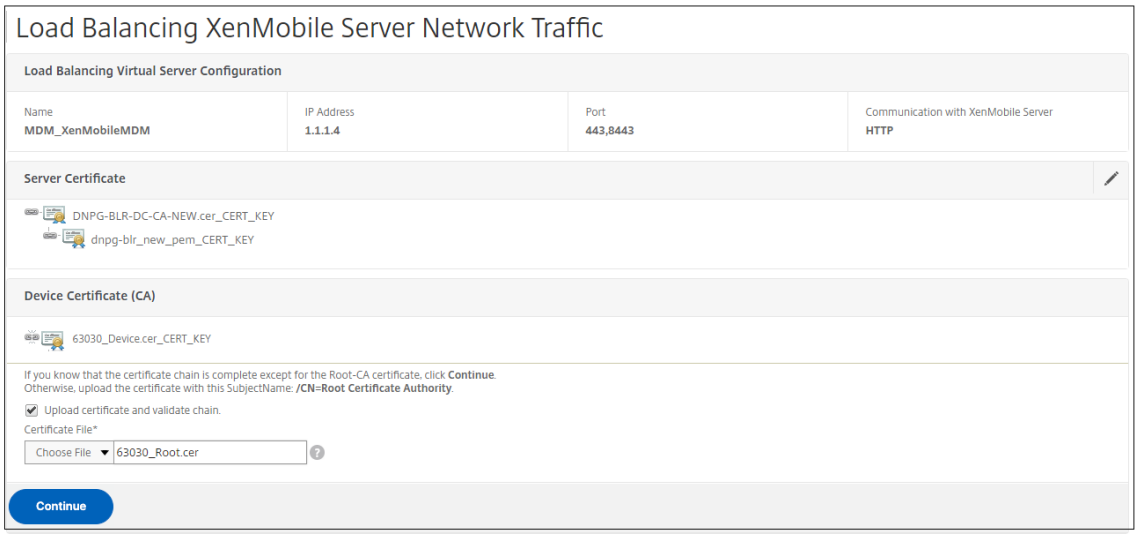

2. Inicie sesión en la utilidad de configuración. En la ficha **Inicio**, en **MDM Server LB**, haga clic en **Configurar**.

3. En **Servidor virtual LB para administración de dispositivos**, en **Nombre**, escriba un nombre para el servidor.
4. En **Dirección IP**, escriba la dirección IP del servidor virtual y, a continuación, haga clic en **Continuar**.
5. En la página **Equilibrio de carga de Citrix Endpoint Management MDM Servers**, repita los pasos 3 y 4 y, a continuación, haga clic en **Crear**.
6. Compruebe la configuración y, a continuación, haga clic en **Listo**.
7. Cuando se le pida que agregue un certificado de servidor, elija el certificado de servidor y haga clic en **Continuar**.

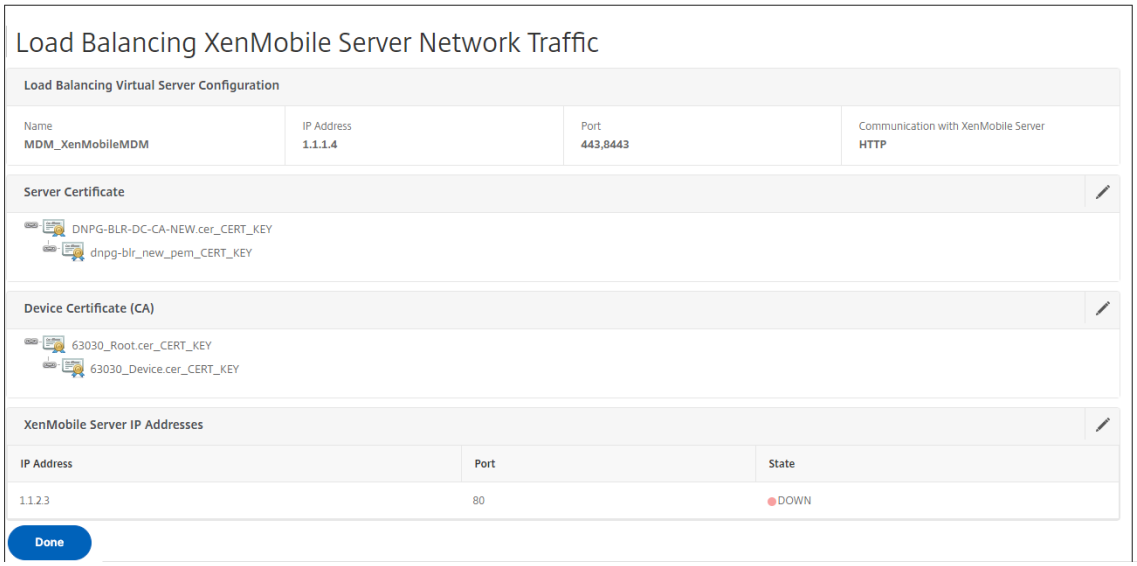



8. Especifique el certificado de CA y haga clic en **Continuar**.

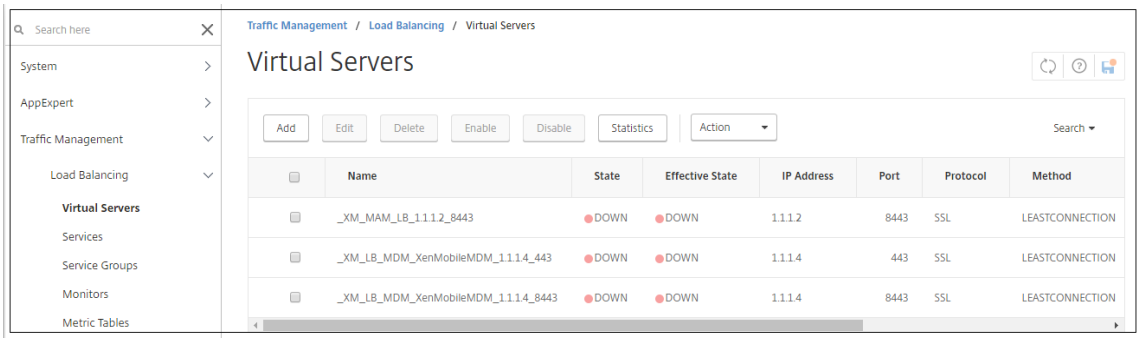



9. Mantenga la misma dirección IP de Citrix Endpoint Management. Haga clic en **Listo**.




10. Para verificar la configuración del equilibrio de carga, vaya a **Administración del tráfico > Servidores virtuales**.

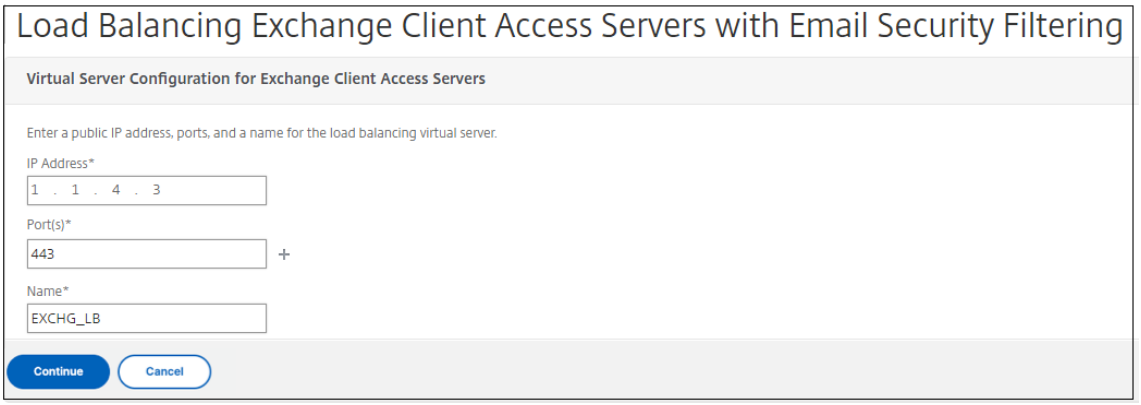



## Configuración de servidores de equilibrio de carga para Microsoft Exchange con filtrado de seguridad de correo electrónico

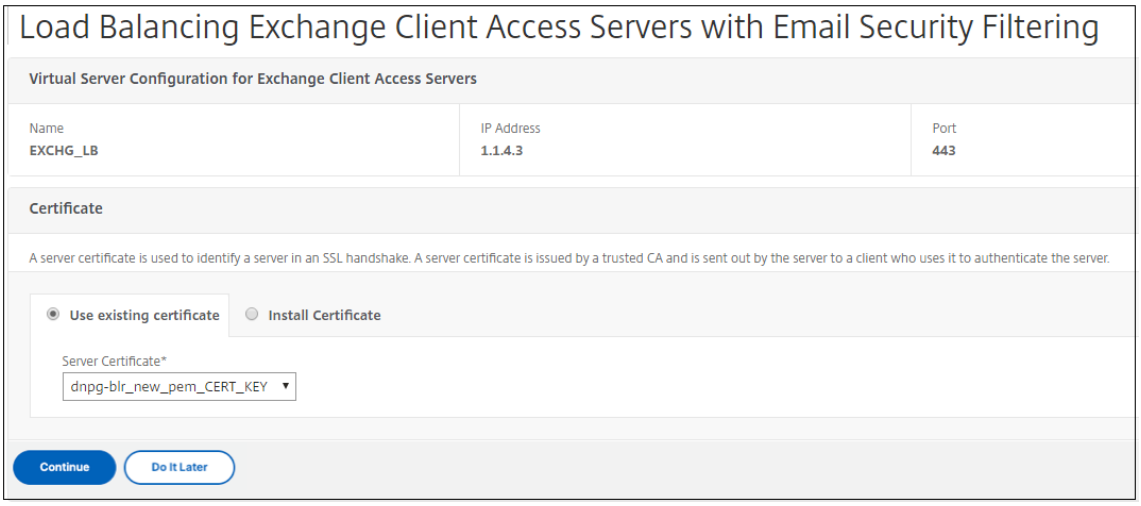
January 26, 2024

1. En la ficha **Inicio**, en **MDM Server LB**, haga clic en **Configurar**.
2. En **LB Virtual Server for Exchange CAS**, en **Nombre**, escriba un nombre para el servidor.
3. En **Dirección IP**, escriba la dirección IP del servidor virtual.
4. En **Puerto**, escriba el número de puerto. Para agregar más puertos, haga clic en el signo más (**+**) y, a continuación, escriba el número de puerto.
5. Haga clic en **Continuar**.

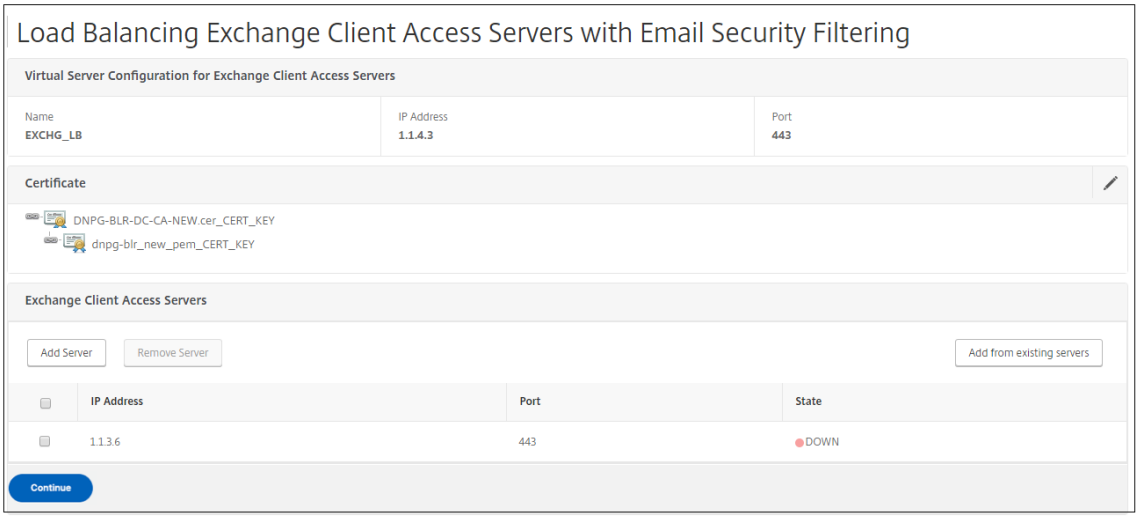
 




6. En **Certificados**, elija un certificado existente o instale uno que esté en su equipo (**local**) o en el dispositivo NetScaler ADC (**dispositivo**).
7. Haga clic en **Continuar**.




8. En **Instancias de servicio CAS de Exchange**, escriba el nombre, la dirección IP y el número de puerto del servidor virtual. A continuación, haga clic en **Agregar** y **continuar**.



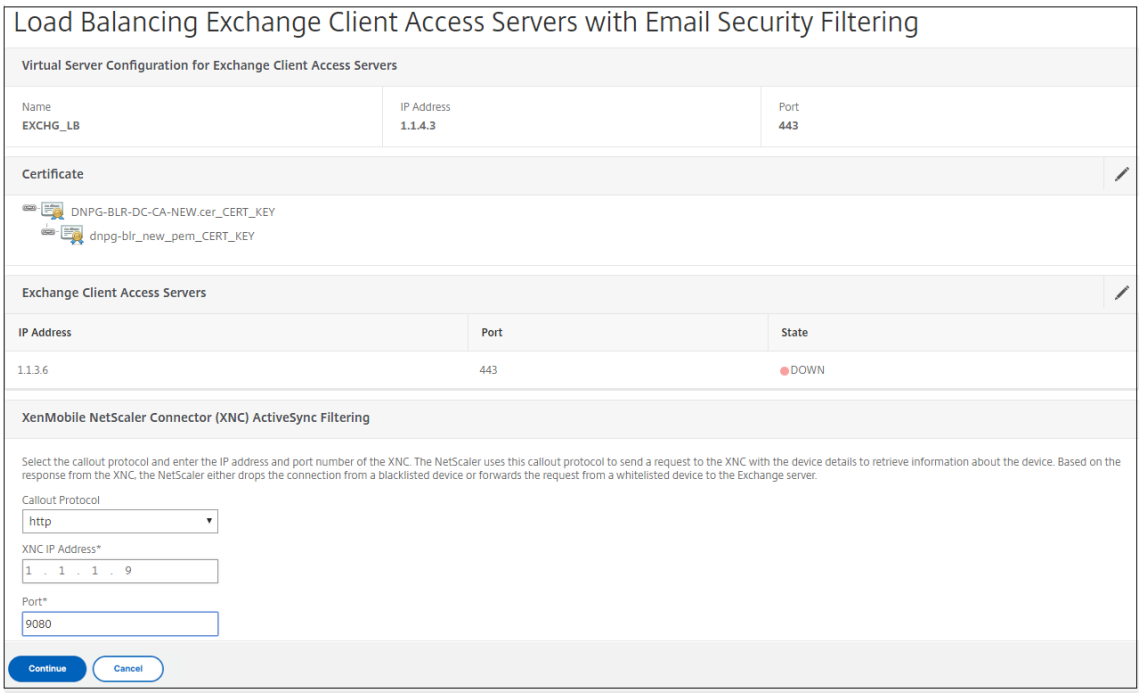
Al **hacer clic en Listo**, aparecen los campos para configurar el filtro ActiveSync de Citrix Endpoint Management de NetScaler ADC Connector (XNC).

## Configuración del filtrado ActiveSync de Citrix ADC Connector (XNC) de Citrix Endpoint Management

January 26, 2024

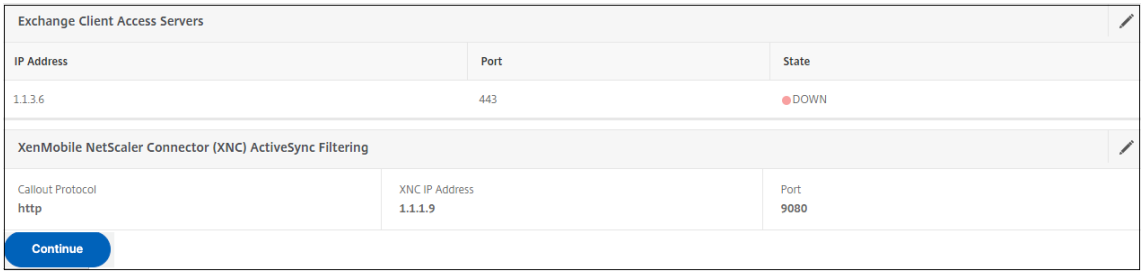
Citrix Endpoint Management NetScaler ADC Connector (XNC) proporciona un servicio de autorización a nivel de dispositivo de clientes ActiveSync a NetScaler ADC que actúa como proxy inverso para el protocolo Exchange ActiveSync. La autorización se controla mediante una combinación de políticas definidas en Citrix Endpoint Management y mediante reglas definidas localmente por el XNC.

1. En **Filtrado ActiveSync de Citrix Endpoint Management NetScaler ADC Connector (XNC)**, para **Protocolo de llamada**, seleccione **http** o **https**.
2. En **Dirección IP de XNC**, escriba la dirección IP del conector Citrix NetScaler ADC Endpoint Management.
3. En **Puerto**, escriba **9080** para el tráfico de red HTTP o **9443** para el tráfico de red HTTPS y, a continuación, haga clic en **Continuar**.




Aparecerá su configuración.




# Permitir el acceso desde dispositivos móviles con aplicaciones móviles de productividad de Citrix

March 27, 2024

El asistente de NetScaler ADC para XenMobile configura la configuración necesaria para permitir a los usuarios conectarse desde dispositivos compatibles a través de NetScaler Gateway a aplicaciones móviles y recursos de la red interna. Los usuarios se conectan mediante Secure Hub (anteriormente, Secure Hub), que establece un túnel de microVPN. Cuando los usuarios se conectan, se abre un túnel VPN a NetScaler Gateway y, a continuación, se pasa a XenMobile en la red interna. Los usuarios pueden acceder a sus aplicaciones web, móviles y SaaS desde XenMobile.

Para garantizar que los usuarios consuman una única licencia universal al conectarse a NetScaler Gateway con varios dispositivos simultáneamente, puede habilitar la transferencia de sesiones en el servidor virtual. Para obtener más información, consulte Configuración de tipos de conexión en el servidor virtual.

Si necesita cambiar la configuración después de utilizar el asistente de NetScaler ADC para XenMobile, utilice las secciones de este artículo para obtener orientación. Antes de cambiar la configuración, asegúrese de comprender las implicaciones de los cambios. Para obtener más información, consulte los artículos de XenMobile Deployment.

## Configuración de Secure Browse en Citrix Gateway

Puede cambiar Secure Browse como parte de la configuración global o como parte de un perfil de sesión. Puede enlazar la directiva de sesión a usuarios, grupos o servidores virtuales. Al configurar Secure Browse, también debe habilitar el acceso sin cliente. Sin embargo, el acceso sin cliente no requiere que habilite Secure Browse. Cuando configure el acceso sin cliente, establezca la **codificación URL de acceso sin cliente** en **Borrar**.

Para configurar Secure Browse globalmente:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En el cuadro de diálogo **Configuración global de NetScaler Gateway**, en la ficha **Seguridad**, haga clic en **Secure Browse** y, a continuación, haga clic en **Aceptar**.

Para configurar Secure Browse en un perfil y directiva de sesión:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Si va a crear una nueva directiva de sesión, haga clic en **Agregar**.
   - Si va a cambiar una directiva existente, selecciónela y, a continuación, haga clic en **Abrir**.
3. En la directiva, cree un perfil o modifique un perfil existente. Para hacerlo, realice una de las siguientes acciones:
   - Junto a **Solicitar perfil**, haga clic en **Nuevo**.
   - Junto a **Solicitar perfil** , haz clic en **Modificar** .
4. En la ficha **Seguridad**, junto a **Secure Browse**, haga clic en **Supedición global** y, a continuación, seleccione **Secure Browse**.
5. Lleve a cabo una de las siguientes acciones:
   - Si va a crear un nuevo perfil, haga clic en **Crear**, defina la expresión en el cuadro de diálogo de directivas, haga clic en **Crear y, a continuación,** haga clic en **Cerrar**.
   - Si modifica un perfil existente, después de realizar la selección, haga clic dos veces en **Aceptar**.

Para configurar directivas de tráfico para Secure Web en modo Secure Browse:

Siga estos pasos para configurar las directivas de tráfico para redirigir el tráfico de Secure Web a través de un servidor proxy en modo Secure Browse.

1. En la utilidad de configuración, en la ficha **Configuración**, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Tráfico**.
2. En el panel derecho, haga clic en la ficha **Perfiles de tráfico** y, a continuación, haga clic en **Agregar**.
3. En **Nombre**, introduzca un nombre para el perfil, seleccione **TCP** como **protocolo**y deje el resto de la configuración tal cual.
4. Haga clic en **Crear**.
5. Haga clic en la ficha **Perfiles de tráfico** y, a continuación, haga clic en **Agregar**.

6. En **Nombre**, introduzca un nombre para el perfil y, a continuación, seleccione **HTTP** como **protocolo**.
   Este perfil de tráfico es para HTTP y SSL. El tráfico VPN sin cliente es tráfico HTTP por diseño, independientemente del puerto de destino o del tipo de servicio. Por lo tanto, especifica el tráfico SSL y HTTP como **HTTP** en el perfil de tráfico.
7. En **Proxy**, introduzca la dirección IP del servidor proxy. En **Puerto**, introduzca el número de puerto del servidor proxy.
8. Haga clic en **Crear**.
9. Haga clic en la ficha **Directivas de tráfico** y, después, en **Agregar**.
10. Introduzca el **nombre** de la directiva de tráfico y, para **Solicitar perfil**, seleccione el perfil de tráfico que creó en el paso 3. Escriba la siguiente **expresión** y, a continuación, haga clic en **Crear**:

```
1 REQ.HTTP.HEADER HOST contains ActiveSyncServer || REQ.HTTP.HEADER
     User-Agent CONTAINS WorxMail || REQ.HTTP.HEADER User-Agent
     CONTAINS com.zenprise || REQ.HTTP.HEADER User-Agent CONTAINS
     Citrix Secure Hub || REQ.HTTP.URL CONTAINS AGServices || REQ.
     HTTP.URL CONTAINS StoreWeb
2 <!--NeedCopy-->
```

    Esta regla realiza una comprobación basada en el encabezado del host. Para omitir el tráfico de sincronización activa del proxy, sustituya **`ActiveSyncServer`** por el nombre del servidor de sincronización activa adecuado.
11. Haga clic en la ficha **Directivas de tráfico** y, después, en **Agregar**. Introduzca el **nombre** de la directiva de tráfico y, para **Solicitar perfil**, seleccione el perfil de tráfico creado en el paso 6. Escriba la siguiente **expresión** y, a continuación, haga clic en **Crear**:

| | |
|---|---|
| (REQ.HTTP.HEADER User-Agent CONTAINS Mozilla | REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser |

12. Haga clic en la ficha **Directivas de tráfico** y, después, en **Agregar**. Introduzca el **nombre** de la directiva de tráfico y, en **Perfil de solicitud**, seleccione el perfil de tráfico creado en el paso 6. Escriba la siguiente **expresión** y, a continuación, haga clic en **Crear**:

| | |
|---|---|
| (REQ.HTTP.HEADER User-Agent CONTAINS Mozilla | REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser |

13. Vaya a **NetScaler Gateway > Servidores virtuales**, seleccione el servidor virtual en el panel derecho y, a continuación, haga clic en **Modificar**.

14. En la fila **Directivas**, haga clic en **+**.
15. En el menú **Elegir directiva**, seleccione **Tráfico**.
16. Haga clic en **Continuar**.
17. En **Vinculación de directivas**, al lado de **Seleccionar directiva**, haga clic en **>**.
18. Seleccione la directiva que creó en el paso 10 y, a continuación, haga clic en **Aceptar**.
19. Haga clic en **Bind**.
20. En **Directivas**, haga clic en **Directiva de tráfico**.
21. En **Enlace de directivas de tráfico de servidor virtual VPN**, haga clic en **Agregar enlace**.
22. En **Vinculación de directivas**, junto al menú **Seleccionar directiva**, haga clic en **>** para ver la lista de directivas.
23. Seleccione la directiva que creó en el paso 11 y, a continuación, haga clic en **Aceptar**.
24. Haga clic en **Bind**.
25. En **Directivas**, haga clic en **Directivas de tráfico**.
26. En **Enlace de directivas de tráfico de servidor virtual VPN**, haga clic en **Agregar enlace**.
27. En **Vinculación de directivas**, junto al menú **Seleccionar directiva**, haga clic en **>** para ver la lista de directivas.
28. Seleccione la directiva que creó en el paso 12 y, a continuación, haga clic en **Aceptar**.
29. Haga clic en **Bind**.
30. Haga clic en **Cerrar**.
31. Haga clic en **Listo**.

Asegúrese de configurar la aplicación Secure Web (WorxWeb) en la consola de XenMobile. Vaya a **Configurar > Aplicaciones**, seleccione la aplicación Secure Web, haga clic en **Modificar** y, a continuación, realice los siguientes cambios:

- En la página **Información de la aplicación**, cambie el **Modo VPN inicial** a **Secure Browse**.
- En la página **iOS**, cambie el **Modo VPN inicial** a **Secure Browse**.
- En la página **Android**, cambie el **modo VPN preferido** a **Secure Browse**.

### Configurar los tiempos de espera de la aplicación y del token MDX

Cuando los usuarios inician sesión desde un dispositivo iOS o Android, se emite un token de aplicación o un token MDX. El token es similar a Secure Ticket Authority (STA).

Puede establecer el número de segundos o minutos que los tokens están activos. Si el token caduca, los usuarios no pueden acceder al recurso solicitado, como una aplicación o una página web.

Los tiempos de espera de los tokens son ajustes globales. Al configurar la configuración, se aplica a todos los usuarios que inician sesión en NetScaler Gateway.

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En el cuadro de diálogo **Configuración global de NetScaler Gateway**, en la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada**.
4. En la ficha **General**, en **Application Token Timeout (seg)** introduzca el número de segundos antes de que caduque el token. El valor predeterminado es de **100** segundos.
5. En Tiempo de **espera del token MDX (minutos)**, introduzca el número de minutos antes de que caduque el token y, a continuación, haga clic en **Aceptar**. El valor predeterminado es de **10** minutos.

### Inhabilitar Endpoint Analysis para dispositivos móviles

Si configura el análisis de dispositivos de punto final, debe configurar las expresiones de directiva para que los análisis de análisis de dispositivos de punto final no se ejecuten en dispositivos móviles Android o iOS. Las exploraciones de análisis de dispositivos de punto final no son compatibles con los dispositivos móviles.

Si vincula una directiva de análisis de dispositivos de punto final a un servidor virtual, debe crear un servidor virtual secundario para dispositivos móviles. No vincule las directivas de autenticación previa o posterior a la autenticación al servidor virtual del dispositivo móvil.

Al configurar la expresión de directiva en una directiva de autenticación previa, agrega la cadena User-Agent para excluir Android o iOS. Cuando los usuarios inician sesión desde uno de estos dispositivos y excluye el tipo de dispositivo, el análisis de endpoint no se ejecuta.

Por ejemplo, crea la siguiente expresión de directiva para comprobar si el User-Agent contiene Android, si la aplicación virus.exe no existe y para finalizar el proceso keylogger.exe si se está ejecutando mediante el perfil de autenticación previa. La expresión de directiva podría tener este aspecto:

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS Android &&
CLIENT.APPLICATION.PROCESS(keylogger.exe) contains
```

Después de crear la directiva y el perfil de autenticación previa, vincule la directiva al servidor virtual. Cuando los usuarios inician sesión desde un dispositivo Android o iOS, el análisis no se ejecuta. Si los usuarios inician sesión desde un dispositivo basado en Windows, el análisis sí se ejecuta.

Para obtener más información sobre la configuración de directivas de autenticación previa, consulte Configuración de directivas de endpoint.

### Admite consultas DNS mediante sufijos DNS para dispositivos Android

Cuando los usuarios establecen una conexión Micro VPN desde un dispositivo Android, NetScaler Gateway envía la configuración de DNS dividida al dispositivo del usuario. NetScaler Gateway admite consultas DNS divididas en función de la configuración de DNS dividida que configure. NetScaler Gateway también admite consultas DNS divididas en función de los sufijos DNS configurados en el dispositivo. Si los usuarios se conectan desde un dispositivo Android, debe configurar la configuración de DNS en NetScaler Gateway.

El DNS dividido funciona de la siguiente manera:

- Si configuras DNS dividido en **Local**, el dispositivo Android envía todas las solicitudes DNS al servidor DNS local.
- Si establece DNS dividido en **Remoto**, todas las solicitudes DNS se envían a los servidores DNS configurados en NetScaler Gateway (servidor DNS remoto) para su resolución.
- Si configuras DNS dividido en **Ambos**, el dispositivo Android comprueba el tipo de solicitud DNS.
  - Si el tipo de solicitud de DNS no es "A", envía el paquete de solicitud de DNS a los servidores DNS locales y remotos.
  - Si el tipo de solicitud de DNS es "A", el complemento de Android extrae el FQDN de la consulta y compara ese FQDN con la lista de sufijos DNS configurada en el dispositivo NetScaler ADC. Si el FQDN de la solicitud de DNS coincide, la solicitud de DNS se envía al servidor DNS remoto. Si el FQDN no coincide, la solicitud DNS se envía a los servidores DNS locales.

En la tabla siguiente se resume el trabajo de DNS dividido según el registro de tipo A y la lista de sufijos.

| Configuración DNS dividida | ¿Es un disco tipo A? | ¿Está en la lista de sufijos? | Dónde se envía la solicitud DNS |
|---|---|---|---|
| Locales | tanto sí como no | tanto sí como no | Locales |
| Remota | tanto sí como no | tanto sí como no | Remota |
| Ambos | No | NA | Ambos |
| Ambos | Sí | Sí | Remota |
| Ambos | Sí | No | Locales |

Para configurar un sufijo DNS:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, seleccione una directiva de sesión y, a continuación, haga clic en **Abrir**.
3. Junto a **Solicitar perfil** , haz clic en **Modificar** .
4. En la ficha **Configuración de red**, haga clic en **Avanzadas**.
5. Junto a **Sufijo DNS de IP de intranet** , haga clic en **Anular global** , escriba el sufijo DNS y, a continuación, haga clic **en**Aceptar tres veces.

Para configurar DNS dividido globalmente en NetScaler Gateway:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada**.
4. En la ficha **General**, en **Dividir DNS**, seleccione **Ambos**, **Remoto o**Local**y, a** continuación, haga clic en **Aceptar**.

Para configurar DNS dividido en una directiva de sesión en NetScaler Gateway:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Citrix Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada**.
7. En la ficha **General**, junto a **Dividir DNS**, haga clic en **Supedición global**, seleccione **Ambos**, **Remoto o**Local**y, a** continuación, haga clic en **Aceptar**.
8. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresiones con nombre**, seleccione **General**, **True**, haga clic en **Agregar expresión**, haga clic en **Crear y, a continuación,** haga clic en **Cerrar**.

## Configurar la autenticación de token de dominio y seguridad para Citrix Endpoint Management

January 26, 2024

Puede configurar Citrix Endpoint Management para exigir a los usuarios que se autentiquen mediante el protocolo RADIUS con sus credenciales de LDAP más una contraseña de un solo uso. En esta sección se describe la configuración necesaria de NetScaler Gateway para ese tipo de autenticación de dos factores.

### Requisitos previos

Si aún no ha ejecutado el asistente de NetScaler ADC para Citrix Endpoint Management, consulte la sección Asistente de *NetScaler ADC para Citrix Endpoint Management* en Configuración de las opciones del entorno de Citrix Endpoint Management. Asegúrese de que la configuración de NetScaler ADC incluya lo siguiente:

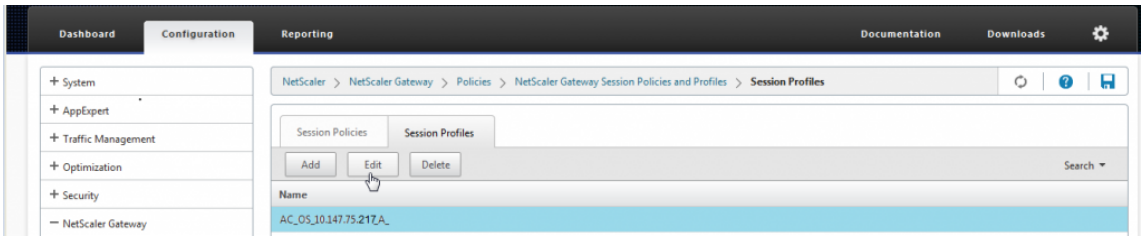
- **Número de puerto LDAP** = **636** (que es el puerto predeterminado para conexiones LDAP seguras)
- **Atributo de nombre de inicio de sesión del servidor** = **samAccountName** o **userPrincipalName** según sus requisitos

### Para configurar la autenticación de dominios y tokens de seguridad

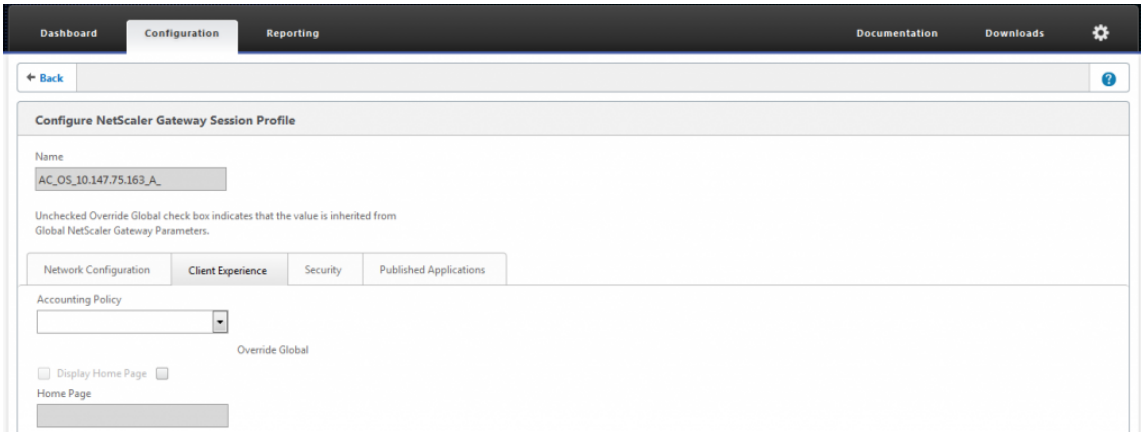
1. Vaya a **NetScaler Gateway > Servidores virtuales**. Seleccione el servidor virtual y, a continuación, haga clic en **Modificar**.
2. Haga clic en **Sin certificado de CA.**
3. En **Seleccionar certificado de CA**, elija un certificado, haga clic en **Aceptar**, en **Vincular** y, a continuación, en **Listo**.

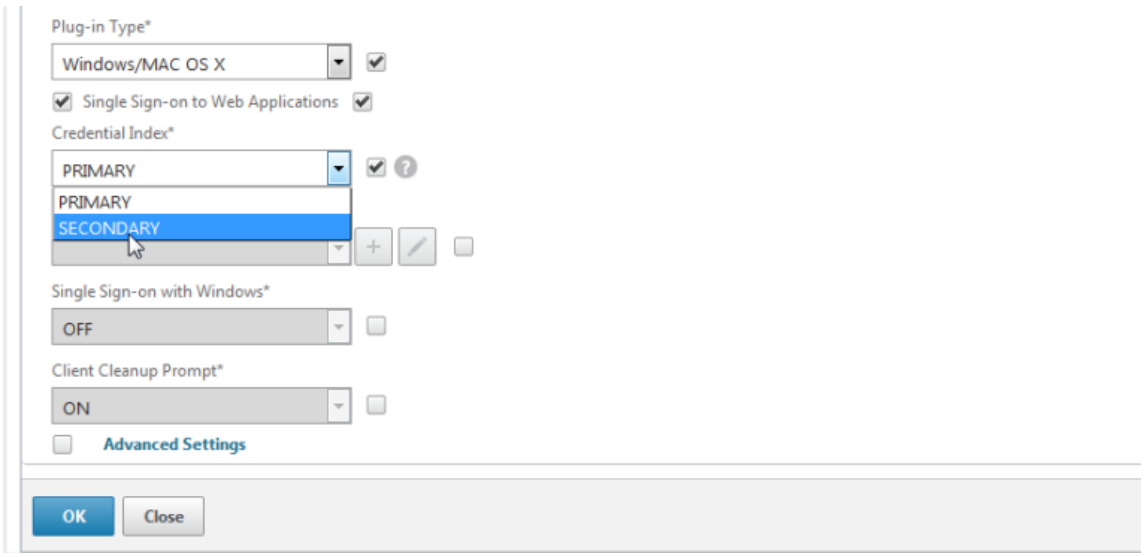
4. Vaya a **Directivas > Sesión > Perfiles de sesión**, seleccione el perfil que empieza por **AC_OS**y haga clic en **Modificar**.




5. Haga clic en la ficha **Experiencia del cliente** y vaya al final de la página.

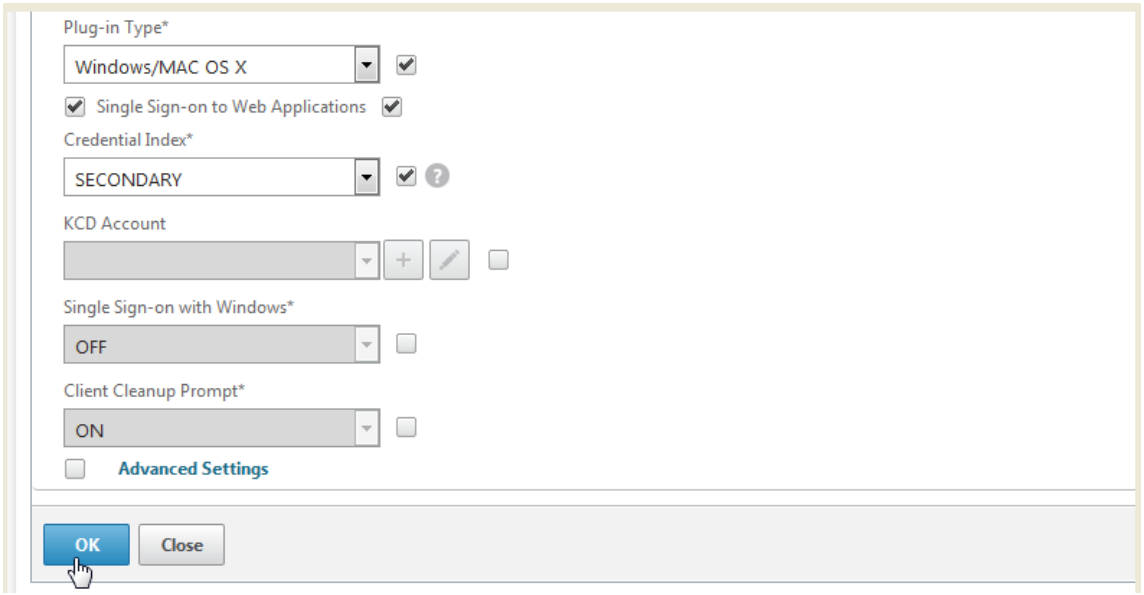



6. En **Índice de credenciales**, elija **SECUNDARIO**.

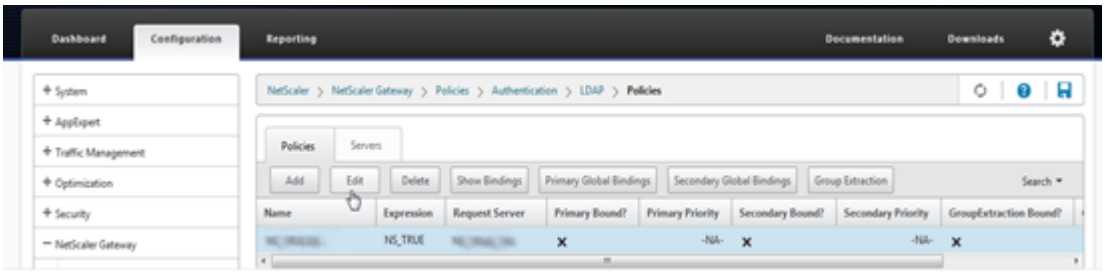



7. Haga clic en **Aceptar**.

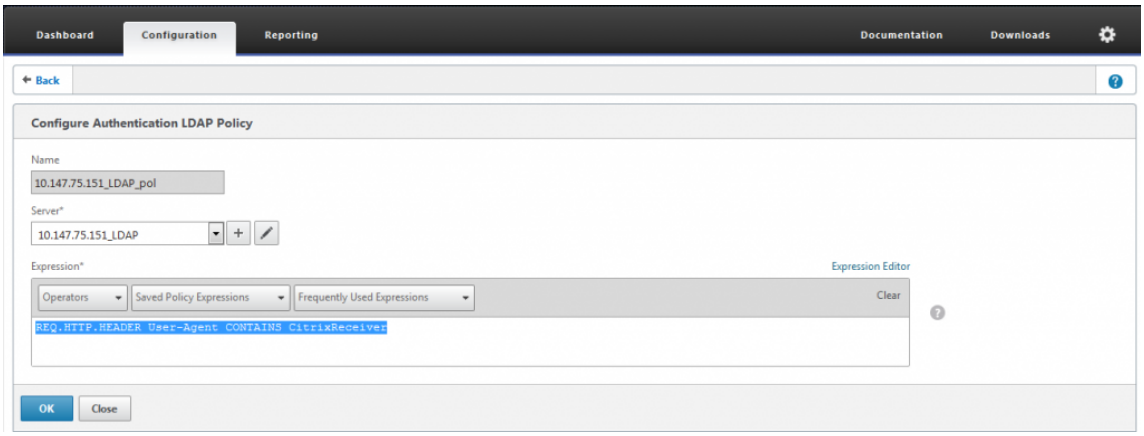



8. Vaya a **Directivas > Autenticación > LDAP**, haga clic en la ficha **Directiva LDAP** y haga clic en **Modificar**.



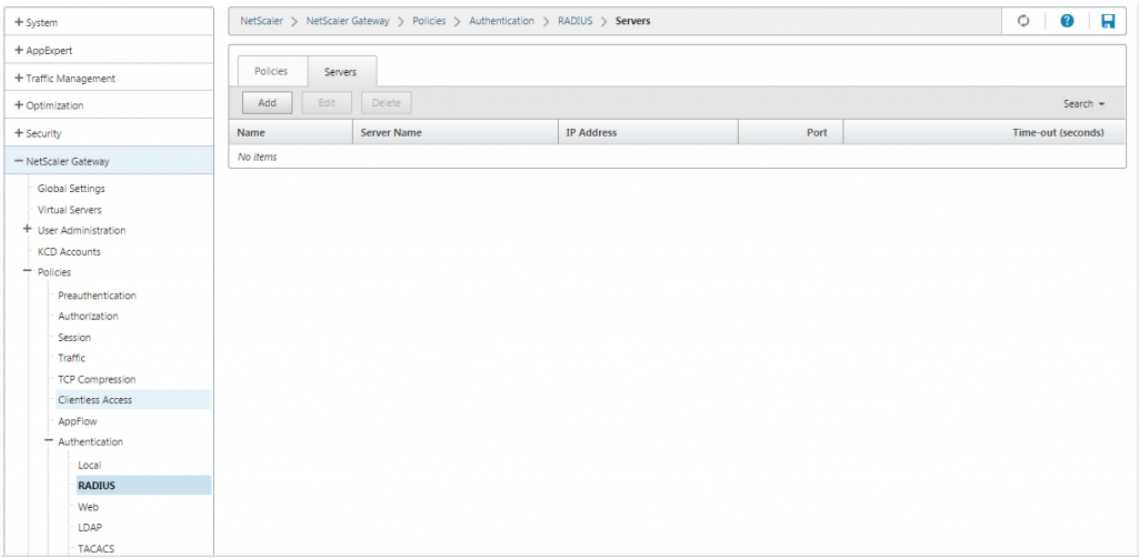

9. Para utilizar VIP independientes de NetScaler Gateway para Citrix Endpoint Management y Citrix Virtual Apps and Desktops, en **Expression**, sustituya **NS_TRUE** por lo siguiente:

   REQ.HTTP.HEADER User-Agent CONTAINS `CitrixReceiver`

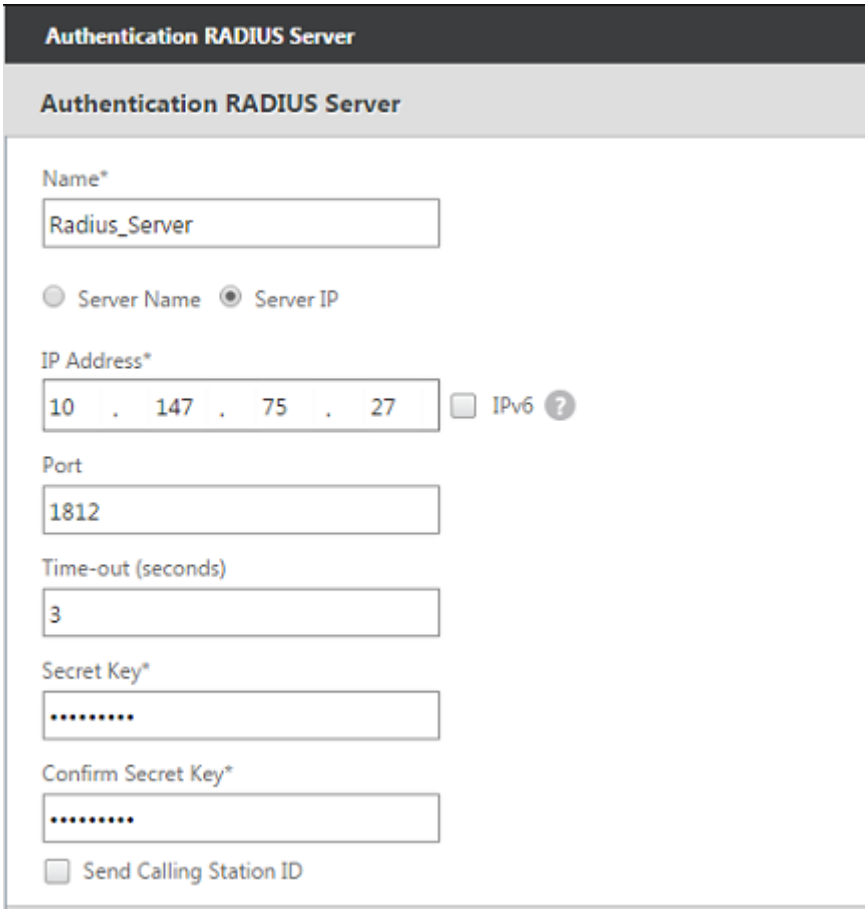



10. Vaya a **Directivas > Autenticación > RADIUS** y, a continuación, haga clic en la ficha **Servidores**.



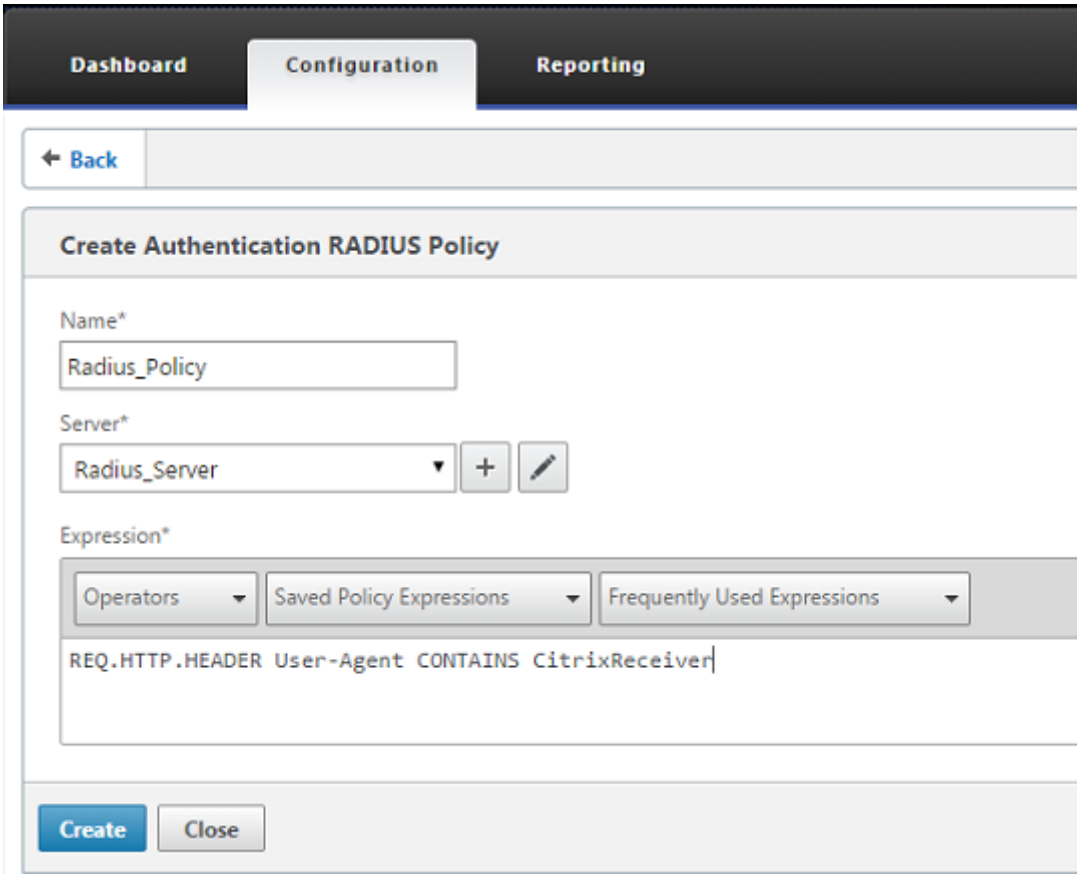

11. Haga clic en **Agregar**, introduzca los detalles del servidor RADIUS y haga clic en **Crear**.




12. Vaya a **Directivas** y, a continuación, haga clic en **Agregar**.

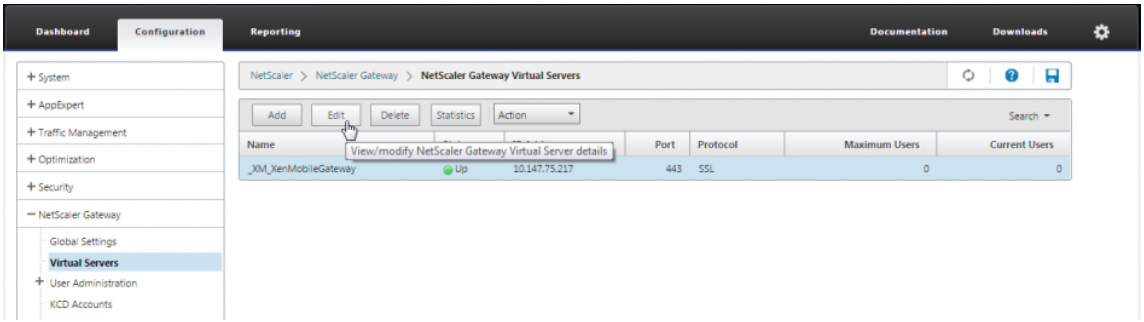
 


13. Introduzca un **nombre** para la directiva. En el menú desplegable **Servidor**, seleccione el nombre del servidor RADIUS (**Radius_Server** en nuestro ejemplo).
14. En **Expresión**, escriba **REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver** y haga clic en **Crear**.

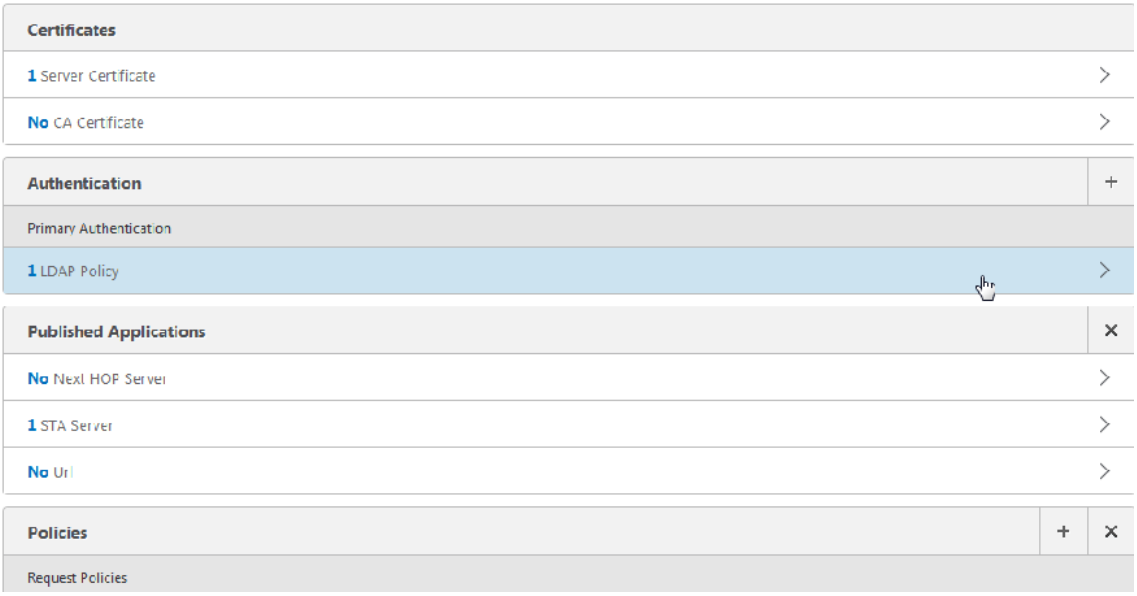



15. Seleccione el servidor virtual y, a continuación, haga clic en **Modificar**.



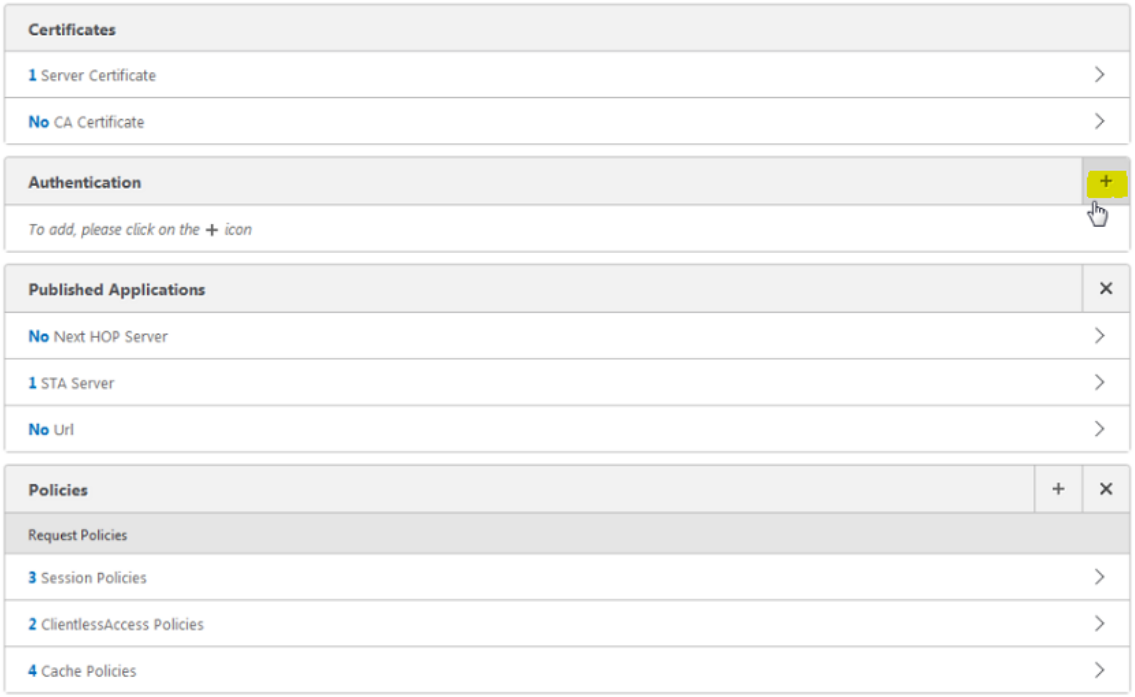

16. En **Autenticación principal**, haga clic en **Directiva LDAP**.



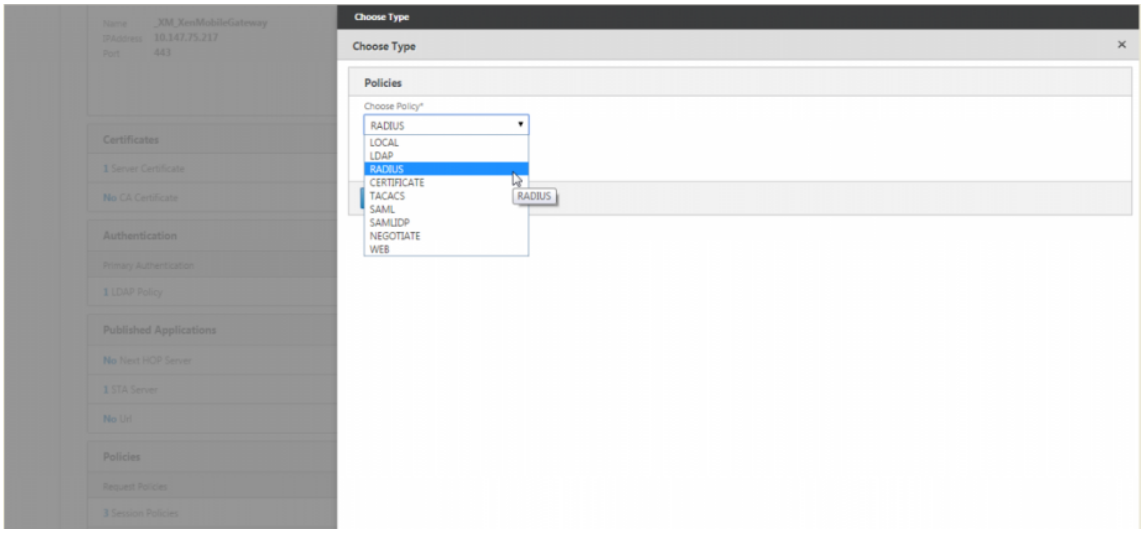

17. Seleccione la directiva, haga clic en **Desvincular**y haga clic en **Cerrar**.


18. En la fila **Autenticación**, haga clic en **+** para agregar la autenticación RADIUS.

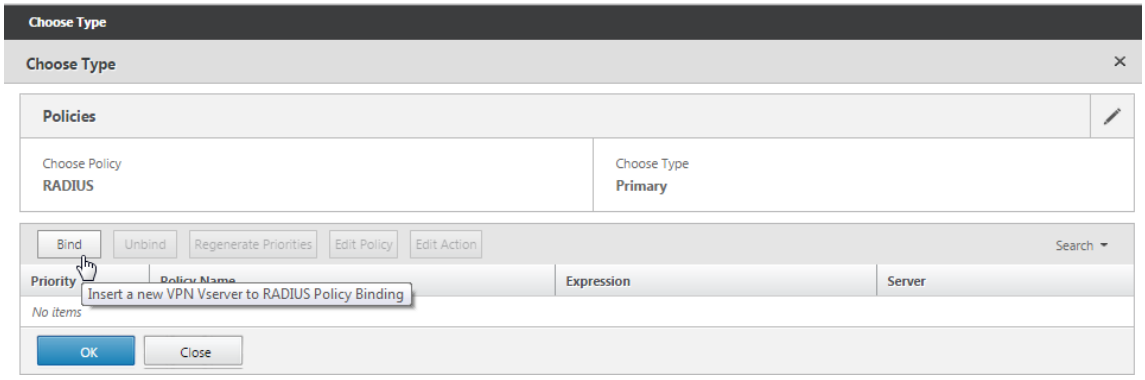



19. En **Elegir tipo**, en **Elegir directiva**, seleccione **RADIUS**.

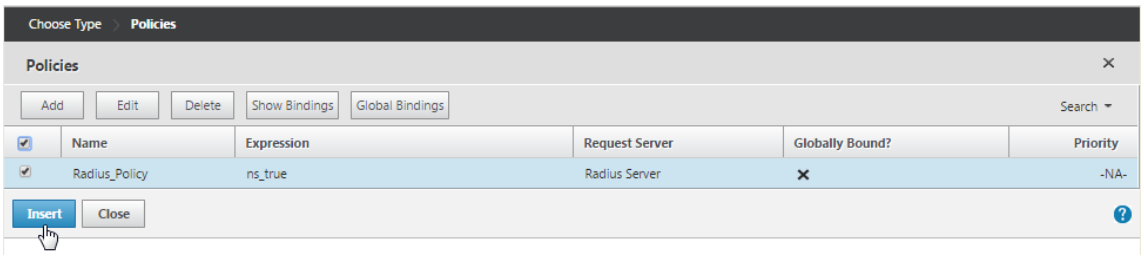



20. Haga clic en **Bind**.

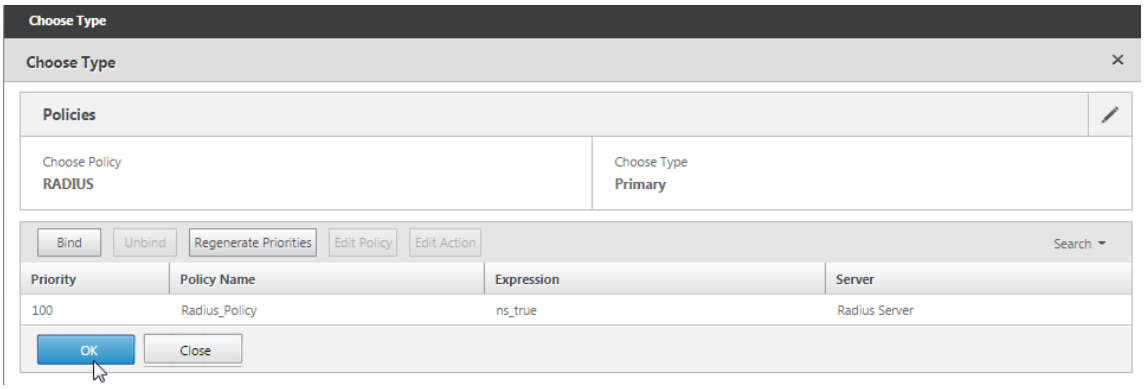
 



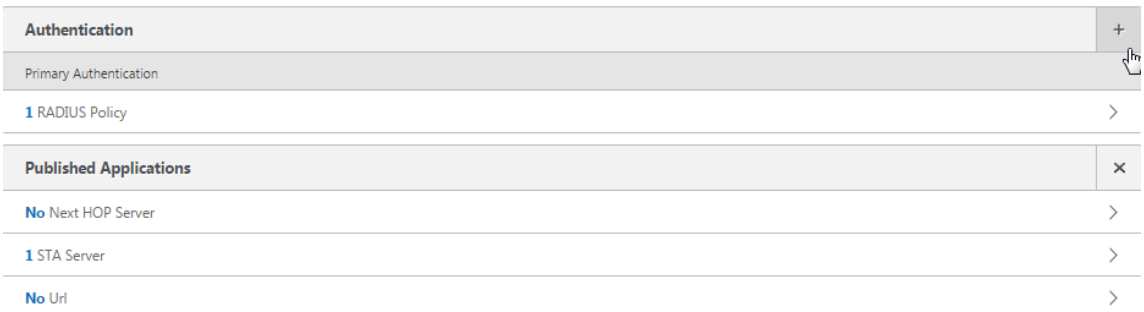

21. Seleccione la directiva de autenticación RADIUS que creó anteriormente y, a continuación, haga clic en **Insertar**.




22. Haga clic en **Aceptar**.




23. Para agregar LDAP como directiva de autenticación secundaria: en la fila **Autenticación**, haga clic en **+**.

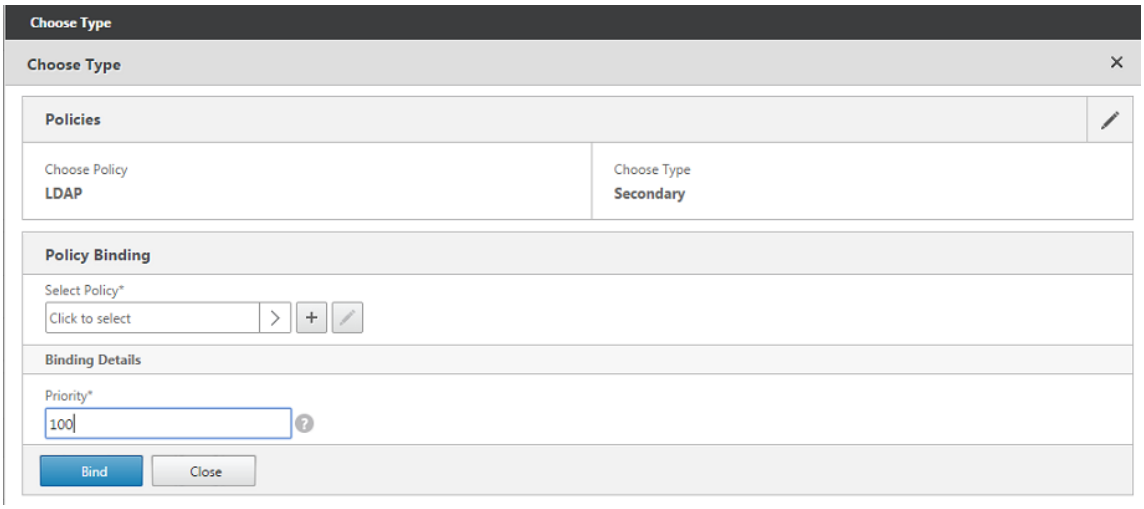



24. En **Elegir directiva**, elija **LDAP**.

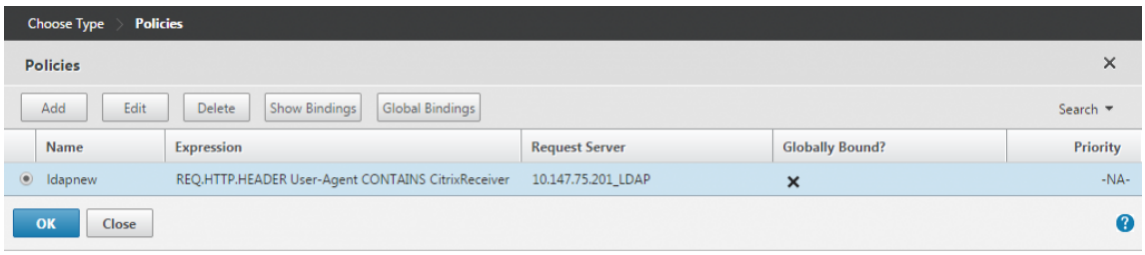
 


25. En **Elegir tipo**, elija **Secundaria**.


26. **En Seleccionar directiva**, elija la directiva LDAP.

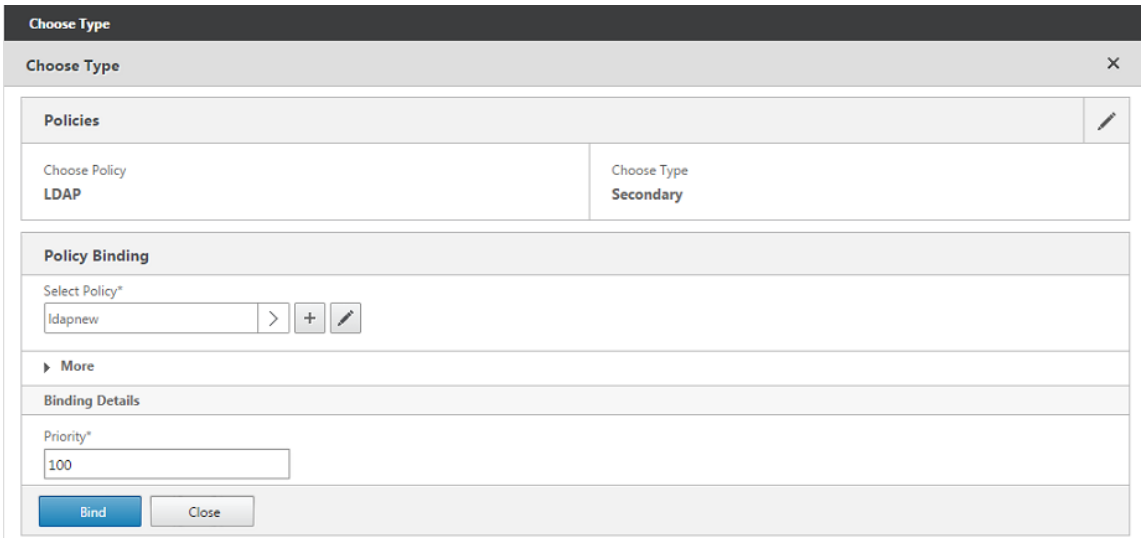



27. Seleccione la directiva y, a continuación, haga clic en **Aceptar**.



28. Haga clic en **Bind**.




29. Haga clic en **Listo**.


30. Compruebe que las directivas que ha creado tienen la máxima prioridad. Esto garantiza que tengan la máxima prioridad incluso si se agregan más directivas para usuarios que no son móviles. Para obtener más información, consulte Definición de prioridades para directivas de autenticación

# Configurar el certificado de cliente o el certificado de cliente y la autenticación de dominio

March 27, 2024

Puede utilizar el asistente de NetScaler ADC para Citrix Endpoint Management para realizar la configuración necesaria para Citrix Endpoint Management al utilizar la autenticación de solo certificado de NetScaler ADC o la autenticación de certificado más dominio. Puede ejecutar el asistente de NetScaler ADC para Citrix Endpoint Management una sola vez. Para obtener información sobre el uso del asistente, consulte Configuración de las opciones del entorno de Citrix Endpoint Management.

Si ya ha utilizado el asistente, siga las instrucciones de este artículo para la configuración adicional necesaria para la autenticación de certificados de cliente o el certificado de cliente más la autenticación de dominio.

Para asegurarse de que el usuario de un dispositivo en modo solo de MAMs no puede autenticarse con un certificado existente en el dispositivo, consulte "NetScaler ADC Certificate Revocation List (CRL)" más adelante en este artículo.

## Configurar NetScaler Gateway para la autenticación de certificados de cliente mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de tipo **SSL** y, en la sección **Parámetros SSL**, establezca **Habilitar reutilización de sesiones** como **INHABILITADO**.
3. Vaya a **NetScaler Gateway > Servidores virtuales**.
4. Seleccione el servidor virtual de tipo **SSL**y haga clic en **Modificar**.
5. En la sección **Parámetros SSL**, haga clic en el icono de modificación.
6. Seleccione **Autenticación de cliente** y en **Certificado de cliente**, seleccione **Obligatorio**.
7. Cree una directiva de certificados de autenticación para que Citrix Endpoint Management pueda extraer el **nombre principal del usuario** o la **cuenta SAMAccount** del certificado de cliente proporcionado por Secure Hub a NetScaler Gateway.
8. Vaya a **NetScaler Gateway > Directivas > Autenticación > CERT**.
9. Haga clic en la ficha **Perfiles** y, a continuación, en **Agregar**.
10. Defina los siguientes parámetros para el perfil del certificado:

    Tipo de autenticación: **CERT**

Dos factores: **DESACTIVADO** (solo para autenticación con certificado)

Campo de nombre de usuario: Asunto: **CN**

Campo de nombre de grupo: **subjectAltName:principalName**

11. Enlazar solo la directiva de autenticación de certificados como **autenticación principal** en el servidor virtual NetScaler Gateway.
12. Enlace el certificado de CA raíz para validar la confianza del certificado de cliente presentado a NetScaler Gateway.

### Configurar NetScaler Gateway para la autenticación de dominios y certificados de cliente mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de tipo **SSL** y, en la sección **Parámetros SSL**, establezca **Habilitar reutilización de sesiones** como **INHABILITADO**.
3. Vaya a **NetScaler Gateway > Directivas > Autenticación > Certificado**.
4. Haga clic en la ficha **Perfiles** y haga clic en **Agregar**.
5. Introduzca el **nombre** del perfil, establezca **Two Factoren ON y, enCampo de nombre de usuario**, seleccione **SubjetAltNamePrincipalName**.
6. Haga clic en la ficha **Directivas** y, a continuación, en **Agregar**.
7. Escriba el **nombre** de la directiva, en **Servidor** seleccione el perfil de certificado, establezca la **expresión** como **ns_true y haga** clic en **Crear**.
8. Vaya a **Servidores virtuales**, seleccione el servidor virtual de tipo **SSL**y haga clic en **Modificar**.
9. Junto a **Autenticación**, haga clic en **+** para agregar la autenticación de certificado.
10. Para seleccionar el método de autenticación, en **Elegir directiva**, seleccione **Certificado**y, en **Elegir tipo**, seleccione **Principal**. Esto vincula la autenticación de certificados como autenticación principal con la misma prioridad que el tipo de autenticación LDAP.
11. En **Enlace de directivas**, **haga clic en Haga clic para seleccionar** para seleccionar la directiva de certificados creada anteriormente.
12. Seleccione la directiva de certificados creada anteriormente y haga clic en **Aceptar**.
13. Establezca la **prioridad** en **100** y, a continuación, haga clic en **Vincular**. Utilice el mismo número de prioridad al configurar la directiva de autenticación LDAP en los pasos siguientes.
14. En la fila de **Directiva LDAP**, haga clic en **>**.

15. Seleccione la directiva y, a continuación, en el menú desplegable **Modificar**, haga clic en **Modificar enlace**.
16. Introduzca el mismo valor de **prioridad** que especificó para la directiva de certificados. Haga clic en **Bind**.
17. Haga clic en **Cerrar**.
18. Haga clic en el icono de modificación de la sección **Parámetros SSL**.
19. Active la casilla **Autenticación de cliente** y, en **Certificado de cliente**, elija **Obligatoria**y haga clic en **Aceptar**.
20. Haga clic en **Listo**.

### Lista de revocación de certificados (CRL) de Citrix ADC

Citrix Endpoint Management admite la lista de revocación de certificados (CRL) solo para una entidad emisora de certificados de terceros. Si tiene configurada una entidad emisora de certificados de Microsoft, Citrix Endpoint Management utiliza NetScaler ADC para administrar la revocación. Al configurar la autenticación por certificados de cliente, plantéese si es necesario configurar el parámetro de lista de revocación de certificados (CRL) de NetScaler ADC, **Enable CRL Auto Refresh**. Este paso garantiza que el usuario de un dispositivo en modo solo MAM no pueda autenticarse con un certificado existente en el dispositivo. Citrix Endpoint Management vuelve a emitir un nuevo certificado porque no impide que un usuario genere un certificado de usuario si se revoca uno. Este parámetro aumenta la seguridad de las entidades PKI cuando la lista de revocación de certificados comprueba si hay entidades PKI caducadas.

## Optimización del tráfico de red con CloudBridge

March 27, 2024

Cuando los usuarios inician sesión con el plug-in de NetScaler Gateway, la conexión se puede optimizar mediante el complemento CloudBridge, que se instala en el dispositivo de usuario desde CloudBridge. Cuando la conexión se optimiza mediante el uso del complemento CloudBridge, el tráfico de red se comprime y acelera a través de Citrix Gateway. Cuando CloudBridge está habilitado para una conexión, las directivas de compresión TCP en NetScaler Gateway están inhabilitadas.

El complemento CloudBridge se implementa y funciona con el plug-in de NetScaler Gateway.

Citrix Gateway admite las versiones 5.5 y 6.1 del complemento Repeater y las versiones 6.2 y 7.0 del complemento CloudBridge.

La optimización y el control de flujo de CloudBridge tienen prioridad sobre las funciones de optimización de NetScaler Gateway que requieren modificación dinámica del contenido. Si la optimización de CloudBridge está habilitada para el tráfico HTTP, las siguientes funciones de NetScaler Gateway no están disponibles:

- Inicio de sesión único en aplicaciones web
- Asociación de tipos de archivos
- Autorización HTTP

Para permitir el inicio de sesión único en aplicaciones web, puede inhabilitar la aceleración en HTTP. Para hacerlo, usa la línea de comandos. Inicie sesión en la consola serie de NetScaler Gateway y, a continuación, en el símbolo del sistema, escriba:

agregar vpn TrafficAction ssoact http -SSO ACTIVADO

El tráfico de red destinado a un puerto HTTP configurado en Citrix Gateway se excluye automáticamente de la optimización de CloudBridge. Esta es la opción predeterminada. Si configura una política de tráfico para la optimización de CloudBridge en un puerto HTTP, se respeta la política de tráfico y CloudBridge optimiza el tráfico de red. Sin embargo, las funciones de optimización de NetScaler Gateway están inhabilitadas para todo el tráfico afectado por esa directiva. CloudBridge puede acelerar el tráfico de red destinado a puertos no HTTP sin afectar a otras funciones de NetScaler Gateway.

Usa una política de tráfico para configurar las conexiones de usuario para usar el complemento CloudBridge. A continuación, puede enlazar la directiva a usuarios, grupos, servidores virtuales o de forma global. La directiva se prioriza en función de dónde vincule la directiva o según el número de prioridad que le dé a la directiva.

### Para crear una directiva de tráfico

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda Políticas de Citrix Gateway y, a continuación, haga clic en Tráfico.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en **Nuevo** .
5. En **Nombre**, escriba un nombre para el perfil.
6. En **Branch Repeater**, seleccione **ACTIVADO** y, a continuación, haga clic en **Crear**.
7. En el cuadro de diálogo **Crear directiva de tráfico**, junto a **Agregar expresión**, seleccione o escriba una expresión que represente los tipos de tráfico para habilitar la aceleración de CloudBridge, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Al agregar una expresión, elija una expresión de red para usar las mismas direcciones IP e intervalos de puertos para los que CloudBridge está configurado para acelerar. Para que se produzca la aceleración

de CloudBridge, los tipos de tráfico configurados en Citrix Gateway deben coincidir con las políticas de clase de servicio configuradas en CloudBridge.

Todo el tráfico TCP se beneficia de la aceleración de CloudBridge. Si planea utilizar el inicio de sesión único, no acelere el tráfico HTTP porque la aceleración inhabilita el inicio de sesión único.

## Configuración de RfWebUI Persona on Gateway UX

January 26, 2024

RfWebUI Persona es un tema que proporciona una nueva página de inicio de sesión y portal para los usuarios de NetScaler Gateway que inician sesión a través de NetScaler Gateway. El portal presenta a los usuarios de Receiver, StoreFront y Citrix Endpoint Management la misma interfaz gráfica de usuario que cuando acceden directamente a uno de esos productos.

### Cuándo usar RfWebUI Persona

Utilice la persona RfWebUI en NetScaler Gateway cuando necesite una vista de panel único de todas las aplicaciones proporcionadas por los diferentes productos CITRIX, como aplicaciones web y de software como servicio (SaaS), aplicaciones virtuales de Windows y escritorios.

Los siguientes casos ilustran el uso de RfWebUI Persona.

- Un usuario accede a StoreFront mediante Gateway y encuentra una interfaz gráfica de usuario diferente a la que ve al acceder al producto sin Gateway. Solución
  **:** Cuando el usuario accede a StoreFront mediante Gateway, el tema RFWebUI proporciona una interfaz de usuario similar a la que ve al acceder al producto sin utilizar Gateway.
- Un usuario accede a las aplicaciones de Receiver, StoreFront y Citrix Endpoint Management mediante Gateway y tiene dificultades para encontrar las aplicaciones deseadas porque no están agrupadas de forma lógica.
  **Solución:** La persona RfWebUI proporciona una experiencia de usuario de vista de panel único mediante la creación de un paquete lógico de aplicaciones proporcionadas por diferentes productos, como Receiver, StoreFront, Citrix Endpoint Management, etc.

### Funcionalidades proporcionadas por RfWebUI Persona

El nuevo RfWebUI ofrece las siguientes funciones:

- IR
- Agregación de aplicaciones

- Vínculos proxy RDP configurados por el usuario
- Aplicaciones favoritas

#### IR

**GO:**La función Go proporciona acceso a páginas web a través de una VPN sin cliente (CVPN). El usuario simplemente escribe la URL en la sección URL de la pestaña **Marcadores** y hace clic en **IR** .

Actualmente, la función **GO** solo admite Outlook Web Application (OWA) y direcciones URL de SharePoint.

> **Nota**
> La ficha **GO**solo está visible si el parámetro *ClientlessAccessVpnMode*de la directiva de sesión es **Habilitado**.

#### Agregación de aplicaciones

**Agregación de aplicaciones:** El tema RfWebUI proporciona una vista de panel único al agrupar las aplicaciones proporcionadas por diferentes productos bajo banners descriptivos. Por ejemplo, todas las URL de VPN configuradas por un administrador de NetScaler ADC se encuentran en un paquete denominado **Aplicaciones web y SaaS**, y los marcadores web específicos del usuario se encuentran en **Marcadores personales**. Si los paquetes de aplicaciones de Citrix Virtual Apps and Desktops están configurados en StoreFront, la vista de panel único de NetScaler Gateway también incluye estos paquetes.

#### Vínculos proxy de RDP configurados

Los usuarios pueden agregar un enlace proxy del Protocolo de escritorio remoto (RDP) como marcadores personales. Los marcadores personales aparecen en la ficha **Escritorios**.

Se admiten los siguientes modos RDP:

- Puerta de enlace única
- Puerta de enlace sin estado (doble)

> **Nota El**
> usuario solo puede agregar vínculos de proxy *RDP si se configura un RDPClientProfile*. Para obtener más información sobre las configuraciones de RDP, consulte la documentación del *proxy RDP* .

#### Aplicaciones favoritas

Los usuarios pueden agregar las aplicaciones deseadas enumeradas en **Aplicación web y SaaS** y en **Marcadores personales** a la pestaña **FAVORITOS** haciendo clic en el enlace **Agregar a favoritos** que aparece junto al nombre de la aplicación. Las aplicaciones una vez agregadas se pueden ver en la ficha **FAVORITOS**. También se puede eliminar de la pestaña **FAVORITOS** haciendo clic en el enlace **ELIMINAR** que se encuentra junto a la aplicación dentro de la pestaña **FAVORITOS** .

### Consideraciones al habilitar la persona RfWebUI

La persona de RfWebUI no es totalmente compatible con lo siguiente:

**Función de uso compartido de archivos: no se** admite la función de uso compartido de archivos SMB para acceder a recursos compartidos de archivos SMB.
**Inicio de correo electrónico:** El parámetro VPN de **correo electrónico principal** no está disponible como vista incrustada para el portal de NetScaler Gateway. Se puede acceder a él como una aplicación en el paquete de **aplicaciones web y SaaS** en la ficha **APPS** de RfWebUI.
**Cliente Java:** El cliente Java basado en explorador para establecer un túnel SSL no está disponible en este tema.

#### Configuración de RfWebUI Persona

**Para aplicar la Persona RfWebUI**:

1. En la interfaz de NetScaler ADC, vaya a **Configuración > Temas del portal de NetScaler Gateway**.
2. En la página **Temas del portal**, seleccione la casilla de verificación **RfWebUI**.
3. Haga clic en el icono **Guardar** en la esquina superior derecha de la página **Temas del portal**.
4. En el cuadro de diálogo **Guardar confirmación**, haga clic en **Sí**.

## Parámetros de configuración de RFWebUI

March 27, 2024

Dos archivos de configuración influyen en el comportamiento general del portal de NetScaler Gateway: el archivo de configuración local de NetScaler Gateway y el archivo StoreFront.

En función de la implementación, puede modificar el comportamiento del portal de NetScaler Gateway cambiando las propiedades del archivo "plugins.xml". Este fichero aparece como fichero

de configuración en el explorador del que se solicita /var/netscaler/logon/themes/<custom_theme>/plugins.xml.

Durante el inicio de sesión, se utilizan los archivos de configuración de NetScaler Gateway. Sin embargo, cuando se conecta a StoreFront, StoreFront envía una nueva configuración y se sobrescribe la configuración anterior. Este comportamiento es diferente para la VPN sin cliente y la ICA.

Para ICA, la configuración de StoreFront siempre tiene prioridad, pero algunos de los comportamientos de la VPN sin cliente en los que influye la configuración de NetScaler Gateway se conservan incluso después de actualizar la nueva configuración desde StoreFront.

En la tabla siguiente se enumeran los parámetros que describen la configuración que tiene prioridad sobre la VPN sin cliente y la ICA.

| Tipo de configuración |sub config type | Parámetro | VPN sin cliente | ICA | Descripción |
|—| —| —| —|—|—|
|Sesión para VPN sin cliente/AuthManager para ICA| - |loginFormTimeout|Citrix Gateway| - |Define el tiempo en minutos para el tiempo de espera de la página de inicio de sesión|
|Asistente de complementos | - |Habilitado|StoreFront|StoreFront|Define el tiempo en minutos para que se agote el tiempo de espera de la página de inicio de
sesión|Habilitar o inhabilitar el asistente de enchufado| |Asistente de enchufado| - |Upgradeatlogin|StoreFront|Solicitudes para la actualización del complemento al iniciar sesión |
|Asistente de plugin| - |showAfterlogin|NetScaler Gateway|StoreFront|Muestra el mensaje del complemento después de iniciar sesión |
|Asistente de enchufado| - |Mostrar solo si las aplicaciones lo requieren | NetScaler Gateway|StoreFront|Muestra el mensaje del complemento después del inicio de sesión, si lo requieren las aplicaciones | | Asistente de
enchufado| macOS/Win32 |ruta|NetScaler Gateway|StoreFront|Define la ruta de descarga de los plug-ins |
|Plug-in Assistant|ProtocolHandler|Habilitado|NetScaler Gateway|StoreFront|Alternar la página del controlador de protocolos antes de iniciar el complemento |
|Plug-in Assistant|ProtocolHandler|Plataformas|NetScaler Gateway|StoreFront|Identifica los plataforma para el complemento |
|Asistente de enchufado| - |Omitir la comprobación de doble salto cuando se inhabilita|* NetScaler Gateway|StoreFront|Alternar la comprobación de configuración de NetScaler Gateway de doble salto para el paso a través de ICA|
|Interfaz de usuario| - |Opciones de marco|NA|NA|-|
|Interfaz de usuario| |LaunchDesktop|StoreFront|StoreFront|Habilitar o inhabilitar el inicio del escritorio |
|Interfaz de usuario| WorkspaceControl|Activado|StoreFront|StoreFront|Habilitar o inhabilitar el control del espacio de
trabajo| |Interfaz de usuario|WorkspaceControl |Reconexión automática en Inicio de sesión | Store-

Front|StoreFront|Cambiar para volver a conectar automáticamente sesión anterior si está disponible |
|Interfaz de usuario| WorkspaceControl |logffaction|StoreFront|StoreFront|Define el comportamiento de cierre de sesión de Citrix Workspace|
|Interfaz de usuario| WorkspaceControl |ShowReconnectButton|StoreFront|StoreFront|Mostrar u ocultar el botón **Reconectar** |
|Interfaz de usuario| WorkspaceControl | Mostrar botón de desconexión | StoreFront|StoreFront|Mostrar u ocultar el botón **Desconectar** |
|Interfaz de usuario | WorkspaceControl | Mostrar DesktopsView|StoreFront|StoreFront|Mostrar u ocultar la vista Escritorios |
|Interfaz de usuario|Control de WorkspaceControl |showAppsView|StoreFront|StoreFront|Mostrar u ocultar la vista Aplicaciones|
|Interfaz de usuario| WorkspaceControl|DefaultView|StoreFront|StoreFront|Seleccione la vista Escritorio o la vista App|
|Interfaz de usuario|Configuración del receptor |Habilitado|StoreFront|StoreFront|Alternar la configuración del receptor |
|Interfaz de usuario| Configuración del receptor|Mostrar solo si lo requieren las aplicaciones|NetScaler Gateway|NetScaler Gateway|Mostrar el mensaje del receptor si las aplicaciones lo requieren |
|Interfaz de usuario|Configuración del receptor |URL de descarga|StoreFront|StoreFront|Descargue la URL del receptor|
|Interfaz de usuario| appShortcuts |habilitada|StoreFront|StoreFront|Habilitar o inhabilitar la ficha de acceso directo a la aplicación |
|Interfaz de usuario|Accesos directos de la aplicación |allowSessionReconnect|StoreFront|StoreFront| Permitir la reconexión de la sesión |

## Personalización del portal de puerta de enlace mediante plug-ins personalizados

March 27, 2024

El marco RfWebUI de NetScaler Gateway ofrece la posibilidad de agregar los plug-ins personalizados para personalizar su portal de puerta de enlace. Estos plug-ins personalizados se pueden utilizar para agregar una gran funcionalidad a la puerta de enlace, por ejemplo, si quiere agregar una página completamente nueva en el flujo de la puerta de enlace. Para otros casos de uso, el código se puede agregar al archivo de script personalizado proporcionado para los temas de puerta de enlace en la ubicación `/var/netscaler/logon/themes/<custom_theme>/script.js`.

1. Para agregar un plug-in personalizado, cree el archivo JavaScript en la ubicación `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/`. Por ejemplo, puede

encontrar los siguientes plug-ins en /var/netscaler/logon/LogonPoint/plugins/ns-gateway/.

- ns-nfactor.js
- nsg-epa.js
- nsg-setclient.js

Se recomienda introducir el nombre del plug-in con el formato <plugin_name>.js.

Todos estos archivos de plug-ins se obtienen mediante el marco RfWebUI requerido por la funcionalidad.

2. Después de crear el archivo de plug-in, utilice el siguiente código como ejemplo para registrar el plug-in con el marco RfWebUI.

```
1          (function ($) {
2
3                      CTXS.ExtensionAPI.addPlugin( {
4
5                                  Name : " plugin name " ,
6                                  initialize: function() {
7    }
8
9                       }
10  );
11              }
12  )(jQuery);
13 <!--NeedCopy-->
```

donde,

**name** es el nombre que se le da al plug-in. Se utiliza como identificador del plug-in.

**initialize** toma la función como parámetro que se utiliza para inicializar el plug-in.

3. Introduzca el nombre del plug-in y la función de inicialización en la función CTXS.ExtensionAPI.addPlugin() para registrar el plug-in.
El nombre y la ubicación del plug-in agregado deben estar registrados en el archivo plugins.xml de la ubicación /var/netscaler/logon/themes/<custom_theme>/plugins.xml.

4. Después de escribir el código del plug-in, el nombre y la ubicación del plug-in recién agregado deben registrarse con el archivo plugins.xml en la ubicación /var/netscaler/logon/themes/<custom_theme>/plugins.xml. El plug-in debe estar registrado con la etiqueta plug-in.

```
1 <plugins>
2 <plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js"/>
3 <plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient
     .js"/>
```

```
<plugin name="ns-nfactorn" src="plugins/ns-gateway/ns-nfactor.js"
   />
</plugins>
<!--NeedCopy-->
```

5. Introduzca un nombre y src para el plug-in para que rfWebUI pueda identificar y recuperar el plug-in.

### Ejemplo de configuración

Las configuraciones de ejemplo siguientes se pueden utilizar para agregar un plug-in personalizado para agregar un pie de página a la página de inicio de sesión de NetScaler Gateway.

1. Cree el archivo de plug-in de JavaScript en la ubicación, /var/netscaler/logon/LogonPoint/plugins/ns-gateway/.
2. Asigne al plug-in el nombre ns-footer.js /var/netscaler/logon/LogonPoint/plugins/ns-gateway/ns-footer.js
3. Agregue el siguiente código al plug-in registrado en la RfWebUI y en la función de inicialización agregue el pie de página a la puerta de enlace.

```
(function ($) {

CTXS.ExtensionAPI.addPlugin({

    name: "ns-footer", // Name of plugin - must match name sent in
        configuration
    initialize: function () {

        CTXS.Extensions.beforeLogon = function (callback) {

            $("#customExplicitAuthBottom").append("<div style='
               text-align:center;color:white;font-size:15px;'><br>
               Disclaimer<BR><BR>"+
                " Access to this website is restricted to
                   employees of Login Consultants<BR></div>");
            callback();
         }
 ;
     }

 }
 );
 }
 )(jQuery);
<!--NeedCopy-->
```

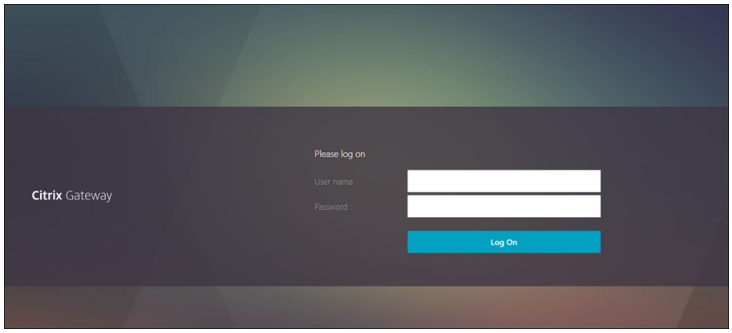
4. Guarde el archivo.

5. Agregue el nombre y src en el archivo plugins.xml de la ubicación `var/netscaler/logon/themes/<custom_theme>/plugins.xml`.

```
<plugins>
<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js" />
<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient
    .js" />
<plugin name="ns-nfactor" src="plugins/ns-gateway/ns-nfactor.js"
    />
<plugin name="ns-footer" src="plugins/ns-gateway/ns-footer.js" />
</plugins>
<!--NeedCopy-->
```

6. Configure el tema personalizado para el que se agrega el plug-in.
7. Limpia la caché con el comando `flush cache contentgroup loginstaticobjects` .
8. Vuelva a cargar la pantalla del portal.
   El pie de página se agrega a la página de inicio de sesión de NetScaler Gateway.




## Crear y personalizar el esquema de inicio de sesión

January 26, 2024

Esquema de inicio de sesión es el archivo XML que proporciona la estructura de la autenticación basada en formularios.
Los usuarios pueden utilizar una amplia gama de formularios de autenticación mediante un conjunto de construcciones de interfaz de usuario similares a los formularios HTML básicos.

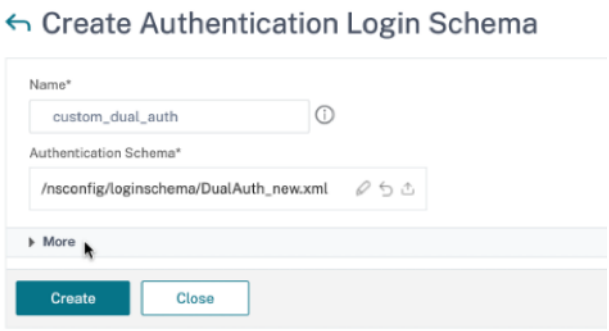
En las autenticaciones nFactor, los factores de autenticación están encadenados entre sí. Cada factor puede tener páginas o archivos de esquema de inicio de sesión diferentes. En algunos casos de autenticación, a los usuarios se les pueden presentar varias pantallas de inicio de sesión. También puede hacer que un esquema de inicio de sesión recopile la información que se puede transmitir a varios factores para que estos últimos factores no tengan que mostrar otro esquema de inicio de sesión.

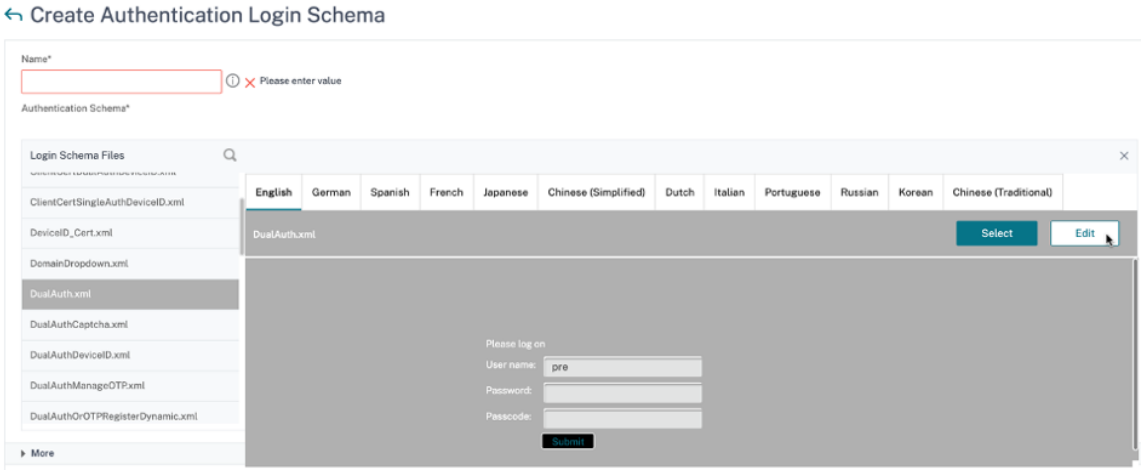
Los archivos XML del esquema de inicio de sesión se incluyen en el dispositivo NetScaler ADC de `/nsconfig/loginschema/LoginSchema`.

### Crear un perfil de esquema de inicio de sesión

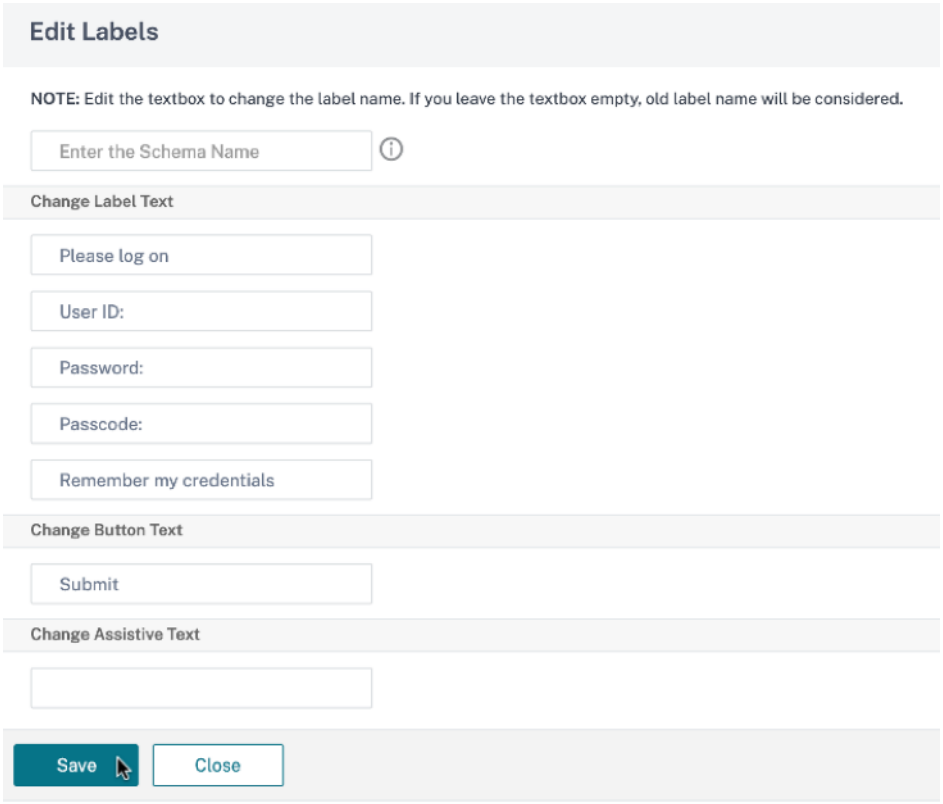
1. Vaya a **Seguridad > AAA > Esquema de inicio**de sesión.
2. Haga clic en la ficha **Perfiles** y, a continuación, haga clic en **Agregar**.
3. En **Esquema de autenticación**, haga clic en el icono del lápiz.




4. Haga clic en la carpeta **LoginSchema** para ver los archivos que contiene.
5. Seleccione uno de los archivos y realice los cambios necesarios.
   - Cambia las etiquetas haciendo clic en el botón Modificar en la parte superior derecha.
   - Modifique el esquema seleccionando el idioma.



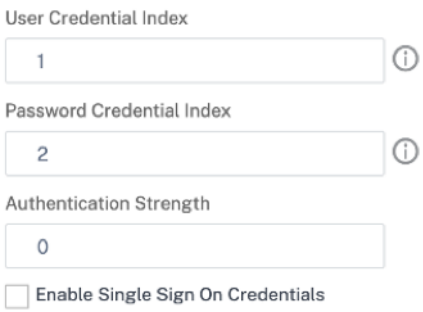

 



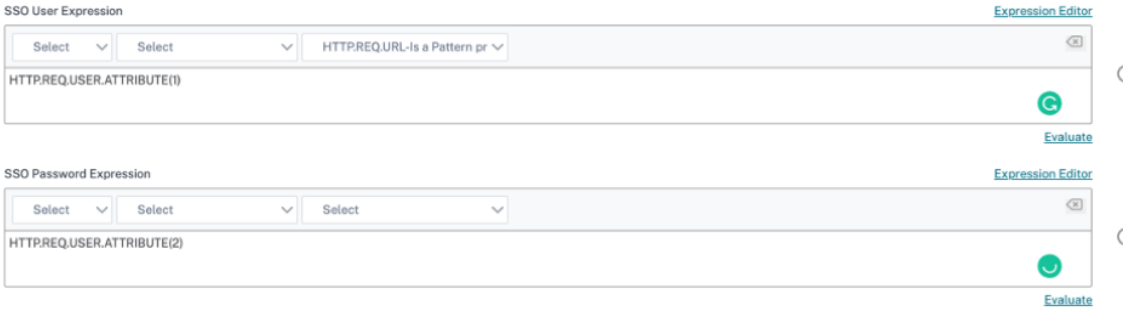

**Nota:** Al guardar los cambios tras la modificación, se crea un nuevo archivo XML de esquema con los cambios.

6. En la parte superior derecha, haga clic en **Seleccionar** para seleccionar el esquema XML modificado.
7. Introduzca un nombre de esquema de inicio de sesión y haga clic en **Más**.

   **Nota:** Puede utilizar las credenciales ya introducidas en otros lugares. Por ejemplo, puede utilizar el nombre de usuario y una de las contraseñas para el inicio de sesión único en StoreFront. Puede hacer clic en **Más** e introducir valores únicos para los índices. Estos valores pueden estar entre 1 y 16. Puede hacer referencia a estos valores de índice en una directiva de tráfico o un perfil mediante la expresión REQ.USER.ATTRIBUTE (#).






8. Haga clic en **Crear** para crear el perfil de esquema de inicio de sesión.

### Enlazar un perfil de esquema de inicio de sesión a un servidor virtual de autenticación, autorización y auditoría

Para enlazar un perfil de esquema de inicio de sesión a un servidor virtual de autenticación, autorización y auditoría, primero debe crear una directiva de esquema de inicio de sesión. Las directivas de esquema de inicio de sesión no son necesarias cuando se vincula el perfil del esquema de inicio de sesión a una etiqueta de directiva de autenticación.

Para crear y enlazar una directiva de esquema de inicio de sesión:

1. Vaya a **Seguridad > AAA > Esquema de inicio**de sesión.
2. Haga clic en la ficha **Directivas** y, a continuación, haga clic en **Agregar**.
3. En **Perfil**, seleccione el perfil de esquema de inicio de sesión creado anteriormente.
4. En **Regla**, introduzca la expresión de sintaxis predeterminada y haga clic en **Crear**.

## Personalizaciones del portal desde la interfaz de usuario de administración

January 26, 2024

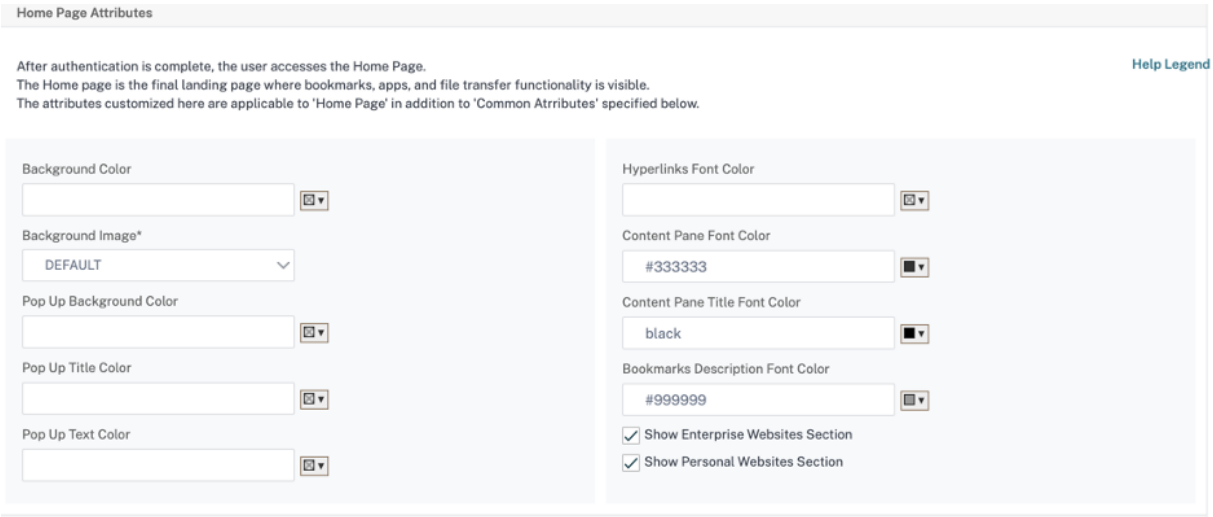
Los administradores pueden personalizar los temas del portal creando los temas personalizados para lograr la apariencia personalizada del portal del usuario. Se pueden crear temas personalizados basados en los temas RfWebUI, Default, X1 y GreenBubble.

**Para crear los temas personalizados:**

1. En la ficha Configuración, vaya a **NetScaler Gateway > Temas del portal** y haga clic en **Agregar**.
2. Introduzca un nombre para el nombre del tema personalizado.
3. En **Tema de plantilla**, seleccione el tema base, según sus necesidades. **RfWebUI** se selecciona de forma predeterminada.

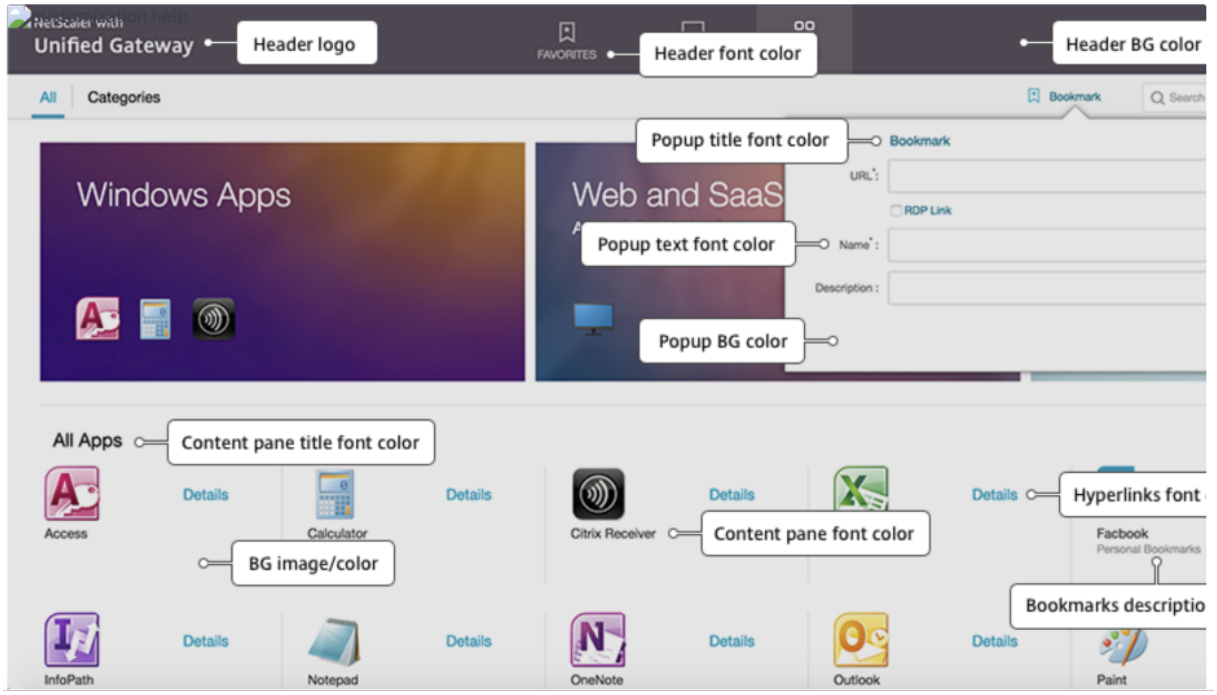
 

4. Haga clic en **Aceptar**.
5. En la sección **Apariencia**, modifique los atributos según sus requisitos para la página de inicio y haga clic en **Aceptar**.




La siguiente ilustración muestra el tema personalizado basado en RfWebUi.

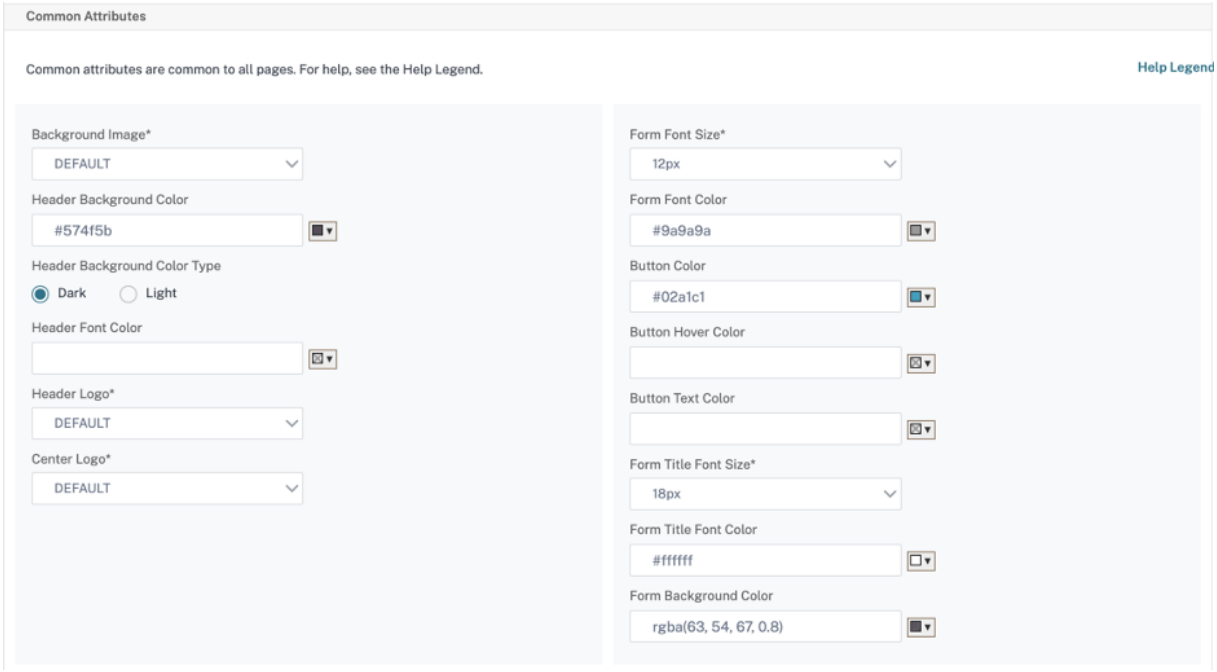
El enlace **Leyenda de ayuda** muestra la visualización gráfica de la página con los nombres de las secciones para ayudarlo a elegir lo que desea modificar.



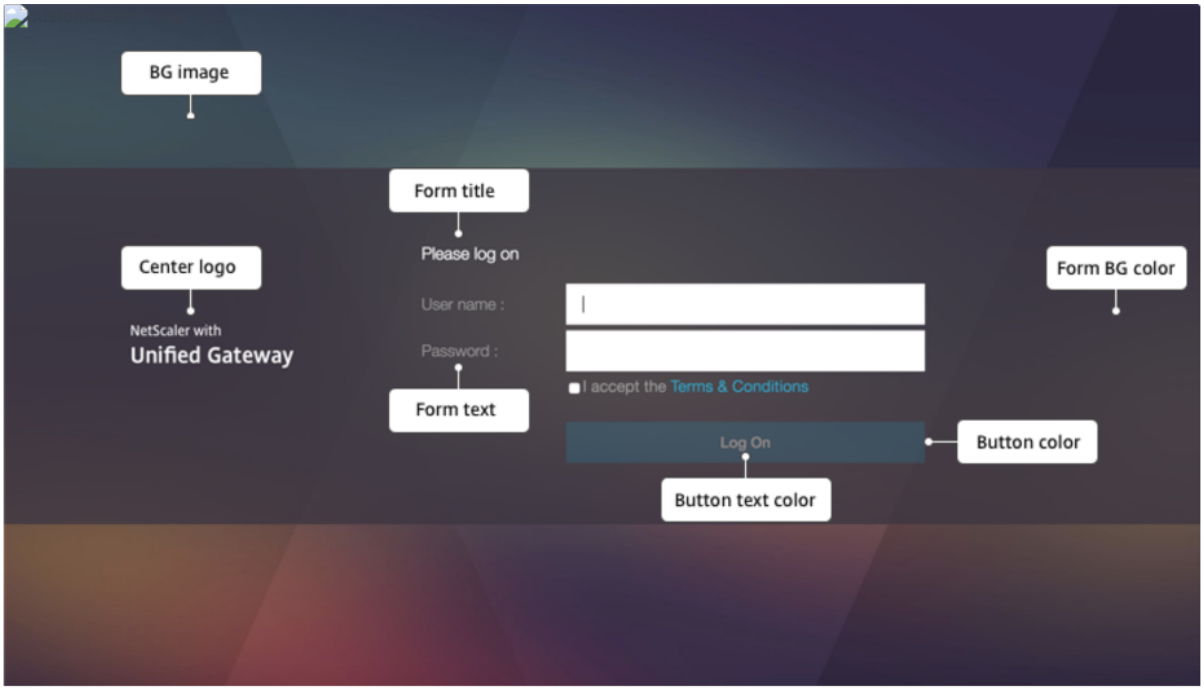

 

### Atributos comunes

La sección **Atributos comunes** proporciona los parámetros configurables que son comunes a todas las páginas de inicio de sesión de NetScaler Gateway.



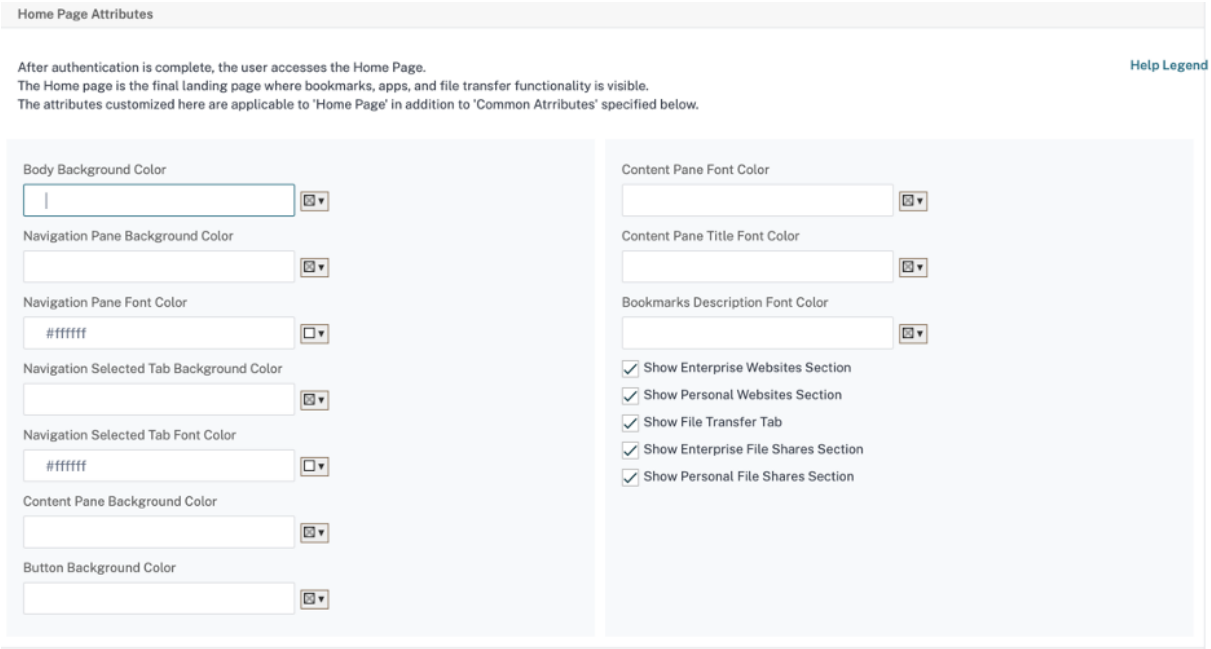

Haga clic en el enlace **Leyenda de ayuda** para ver cada parámetro configurable común.

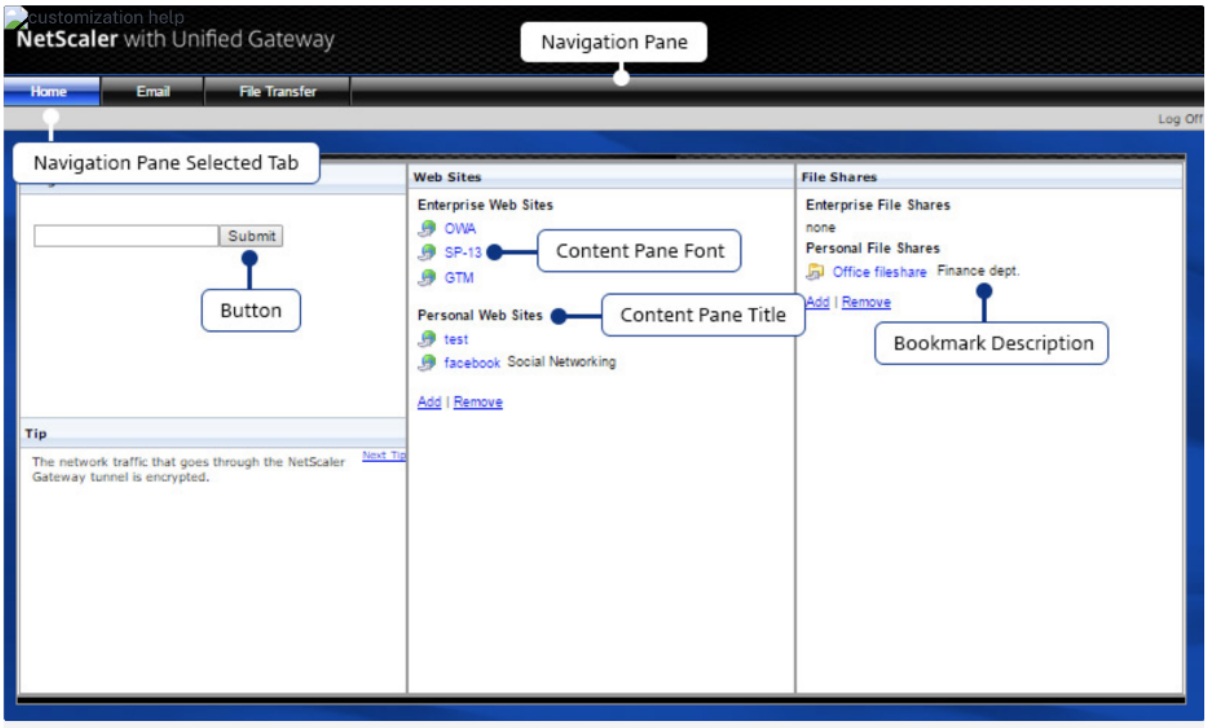



Del mismo modo, para el tema personalizado basado en **Default**, la siguiente ilustración muestra la configuración disponible para la página principal.

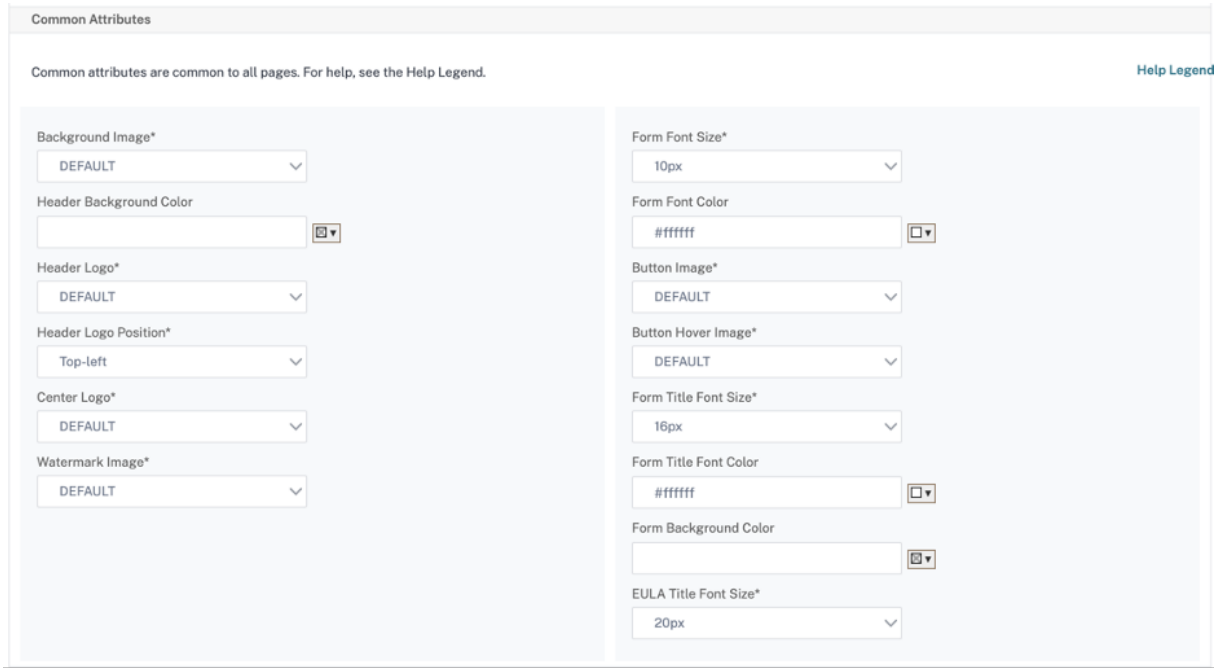
 

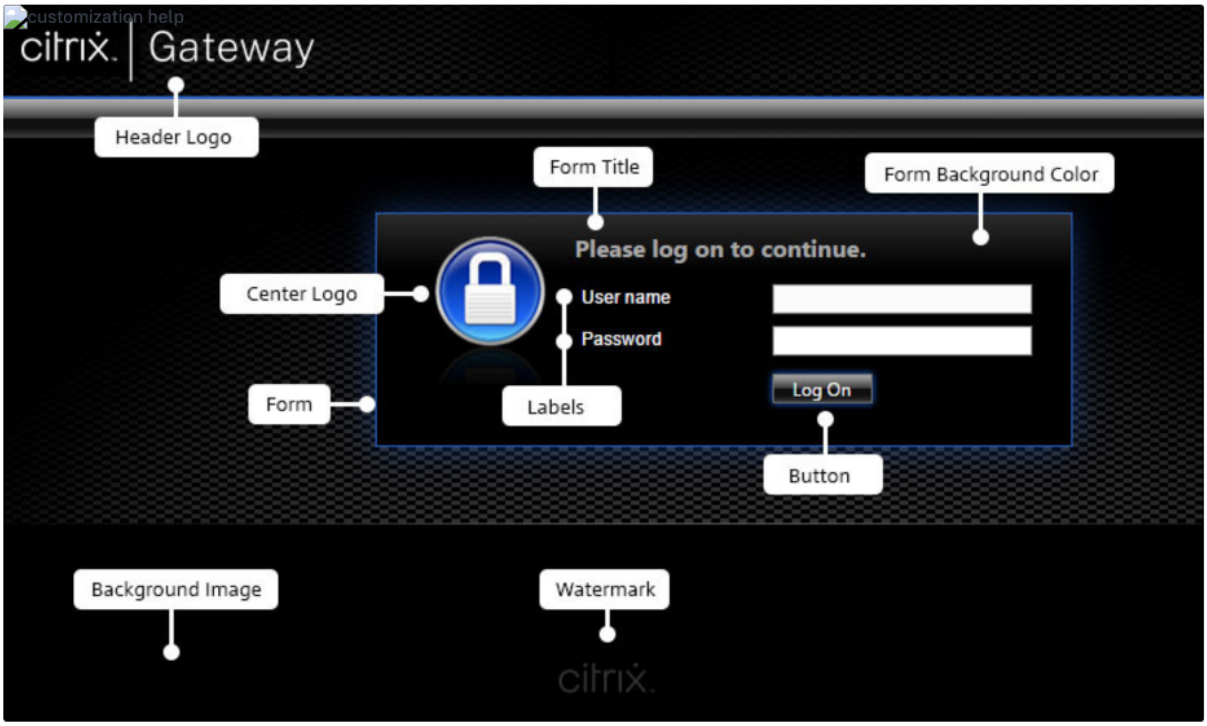
**Nota:** Esta configuración es diferente para x1 y GreenBubble.





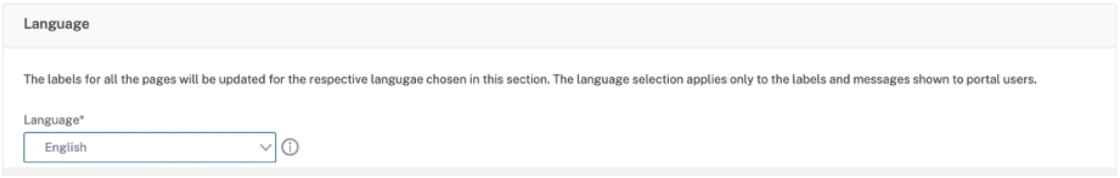

## Personalizaciones de cadenas

Además del aspecto y el aspecto de las páginas de inicio del portal de puerta de enlace, la interfaz de usuario de administración también permite la personalización de cadenas en todas las páginas.

**Realice los siguientes pasos para personalizar las cadenas:**

1. Seleccione el idioma para el que desea modificar la cadena. Las cadenas se muestran en el idioma seleccionado. El inglés está seleccionado de forma predeterminada.




   **Nota:** El idioma que seleccione no define el idioma del tema del portal. Es el idioma para el que se personalizan las cadenas.

2. A la derecha, en **Configuración avanzada**, se enumeran las páginas que están disponibles para la personalización de cadenas.

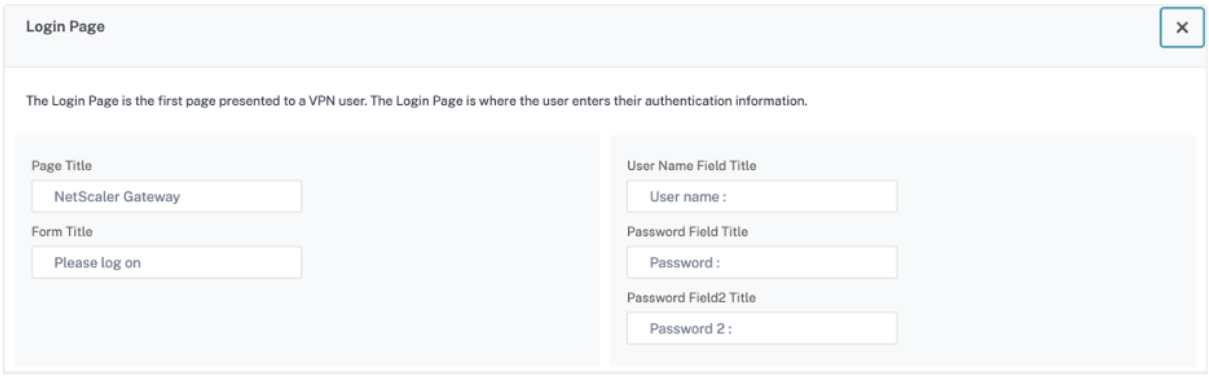
   - Página inicio de sesión
   - Página EPA
   - Página de error EPA
   - Página post-EPA
   - Página Conexión VPN
   - Página de inicio

3. Seleccione la página para la que desea personalizar las cadenas y haga clic en el icono de edición. Se muestra un formulario con personalizaciones de cadenas rellenadas previamente.
4. Seleccione el campo y agregue o modifique la cadena según sus requisitos.
5. Haga clic en **Listo** para completar la creación del tema del portal personalizado. Puede modificar los temas más adelante en **NetScaler Gateway > Temas del portal**.

**Nota:** Si la sección sigue mostrando las cadenas en el idioma seleccionado anteriormente, es posible que la sección ya estuviera abierta cuando se cambió el idioma. En este caso, cierre la sección, seleccione el idioma y vuelva a abrir la página desde **Configuración avanzada**.

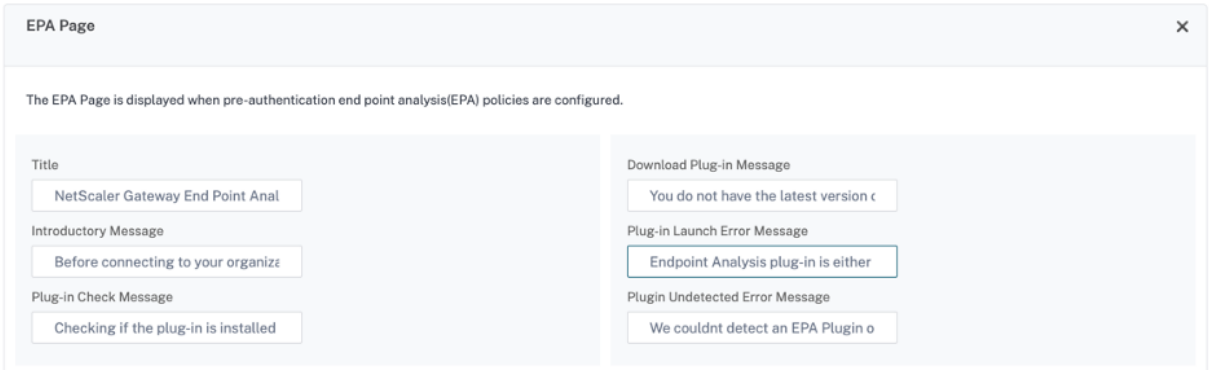
Las siguientes capturas de pantalla muestran el conjunto de cadenas personalizables disponibles para cada página.

**Página inicio de sesión:**

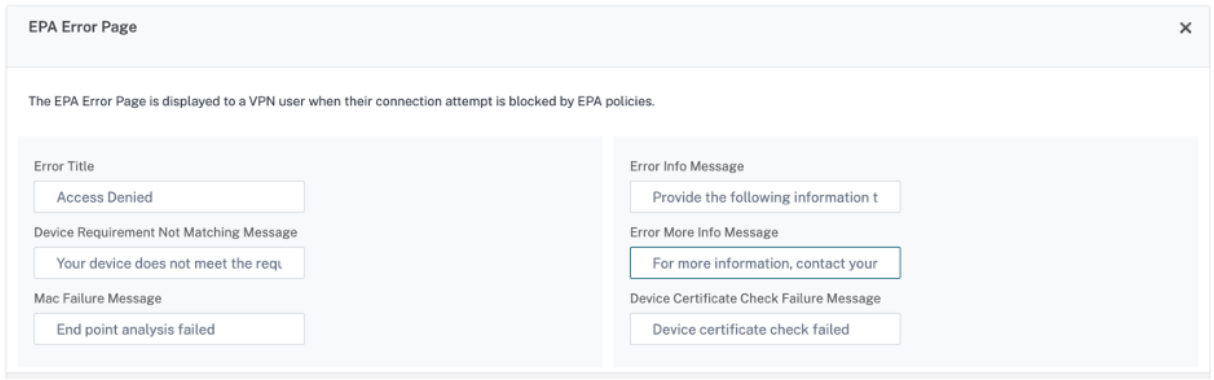


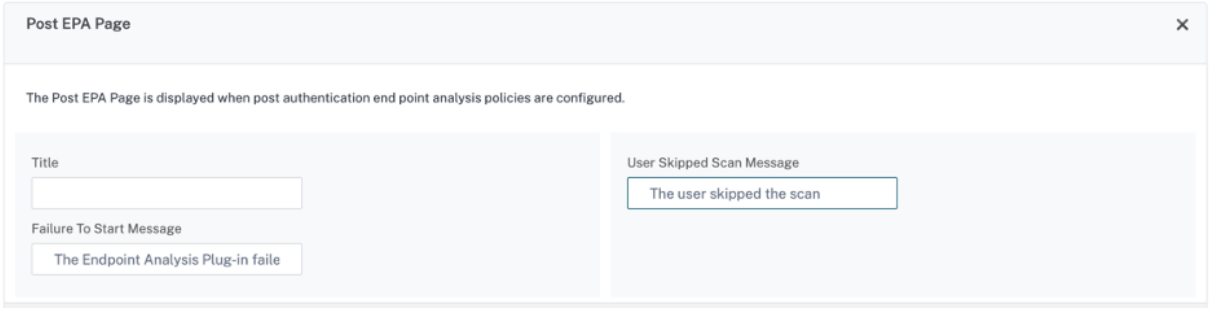
### Página EPA:



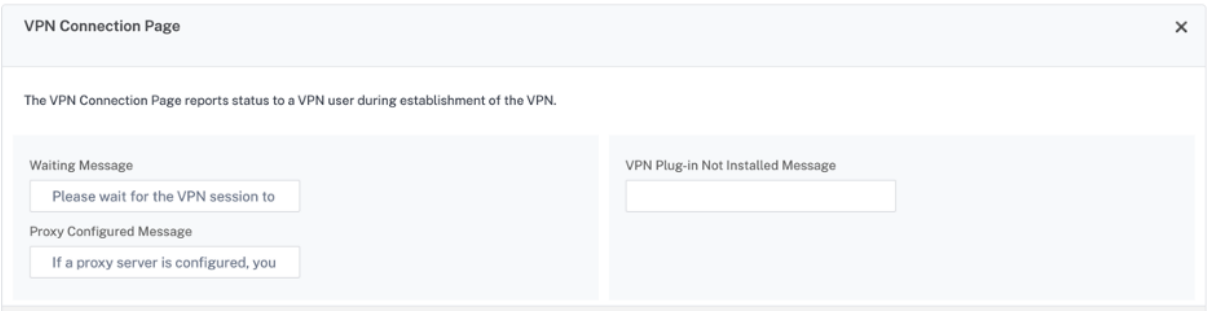

### Página Error de la EPA:




### Página posterior a la EPA:

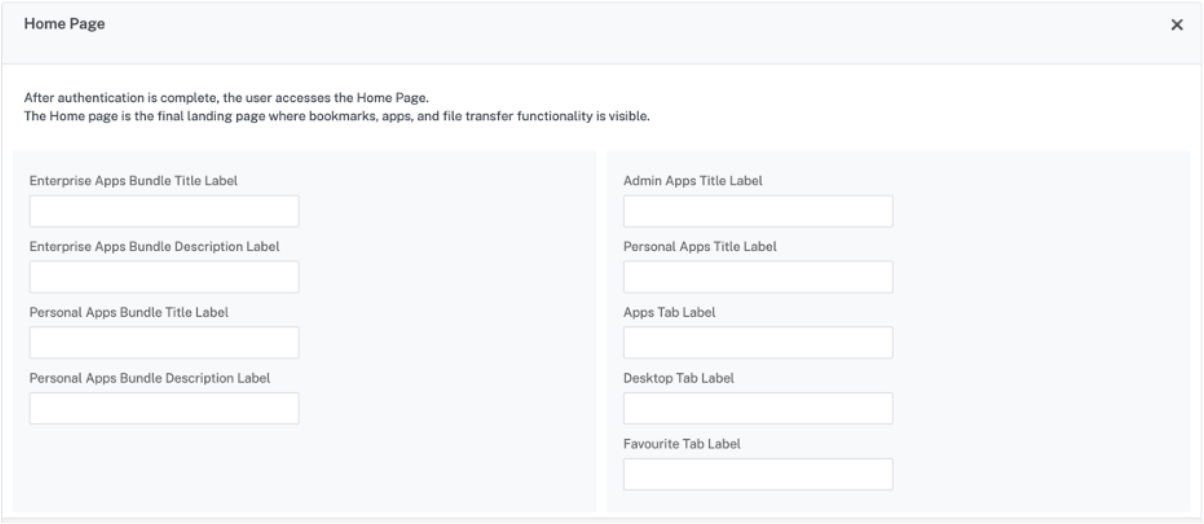



### Página Conexión VPN:



**Página de inicio:**




## Proxy RDP

March 27, 2024

La funcionalidad del proxy RDP se proporciona como parte de NetScaler Gateway. En una implementación típica, el cliente RDP se ejecuta en el equipo de un usuario remoto. El dispositivo NetScaler Gateway se implementa en la DMZ y la comunidad de servidores RDP se encuentra en la red corporativa interna.

El usuario remoto;

1. se conecta a la dirección IP pública de NetScaler Gateway
2. establece una conexión VPN SSL
3. autentica
4. accede a los escritorios remotos a través del dispositivo NetScaler Gateway

La función de proxy RDP se admite en los modos VPN sin cliente y proxy ICA.

> **Nota:**
>
> - Citrix Gateway no admite el host de sesión de escritorio remoto (RDSH), la aplicación remota, el multiusuario de RDS, las sesiones RDP ni las aplicaciones RDP.

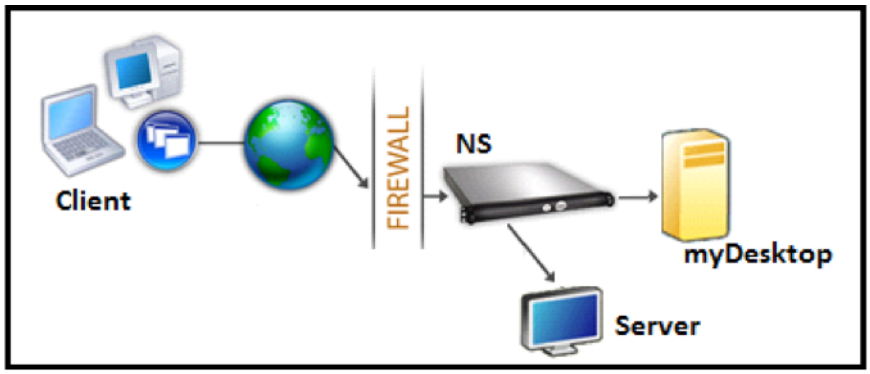
Las siguientes funciones del proxy RDP proporcionan acceso a una comunidad de escritorios remotos a través de NetScaler Gateway.

- Proteja el tráfico RDP mediante VPN sin cliente o modo Proxy ICA (sin túnel completo).

- SSO (inicio de sesión único) en servidores RDP a través de NetScaler Gateway. También proporciona una opción para inhabilitar el SSO si es necesario.
- Función de cumplimiento (SmartAccess), en la que los administradores de NetScaler ADC pueden inhabilitar determinadas capacidades de RDP mediante la configuración de NetScaler Gateway.
- Solución de puerta de enlace única o sin estado (doble) para todas las necesidades (VPN/ICA/RDP/Citrix Endpoint Management).
- Compatibilidad con el cliente MSTSC nativo de Windows para RDP sin necesidad de clientes personalizados.
- Uso del cliente RDP existente proporcionado por Microsoft en MACOSX, iOS y Android.

En la siguiente ilustración se muestra una descripción general de la implementación:




### Implementación mediante VPN sin cliente

En este modo, los vínculos RDP se publican en la página de inicio o portal de Gateway, como marcadores, a través de la configuración de `add vpn url` o mediante un portal externo. El usuario puede hacer clic en estos vínculos para obtener acceso al Escritorio remoto.

### Implementación mediante ICA Proxy

En este modo, se configura una página principal personalizada en el VIP de puerta de enlace mediante el parámetro `wihome`. Esta página principal se puede personalizar con la lista de recursos de escritorio remoto a los que el usuario puede acceder. Esta página personalizada se puede alojar en NetScaler ADC o, si es externa, puede ser un iFrame en la página del portal Gateway existente.

En cualquiera de los dos modos, después de que el usuario haga clic en el enlace o icono de RDP aprovisionado, llega a NetScaler Gateway una solicitud HTTPS del recurso correspondiente. La puerta de enlace genera el contenido del archivo RDP para la conexión solicitada y lo envía al cliente. Se invoca el cliente RDP nativo y se conecta a un agente de escucha RDP en Gateway. Gateway realiza

el SSO en el servidor RDP mediante la compatibilidad con la aplicación (SmartAccess). La puerta de enlace bloquea el acceso de los clientes a determinadas funciones de RDP, según la configuración de NetScaler ADC y, a continuación, envía el tráfico RDP entre el cliente RDP y el servidor.

## Detalles de ejecución

El administrador de NetScaler ADC puede configurar determinadas capacidades de RDP mediante la configuración de NetScaler Gateway. NetScaler Gateway proporciona la función "cumplimiento de RDP"para parámetros importantes de RDP. NetScaler ADC garantiza que el cliente no pueda habilitar los parámetros bloqueados. Si los parámetros bloqueados están habilitados, la función de aplicación RDP sustituye a los parámetros habilitados por el cliente y no se respetan.

> **Importante:** La función de cumplimiento solo se aplica si el SSO está habilitado.

### Parámetros RDP compatibles para la aplicación

Se admite la aplicación de los siguientes parámetros de redirección. Estos parámetros se pueden configurar como parte de un perfil de cliente RDP.

- Redirección del portapapeles
- Redirección de impresoras
- Redirección de unidades de disco
- Redirección de puertos COM
- Redirección de dispositivos PNP

### Flujo de conexión

El flujo de conexión se puede dividir en dos pasos:

- Enumeración de recursos RDP y descarga de archivos RDP.
- Inicio de la conexión RDP.

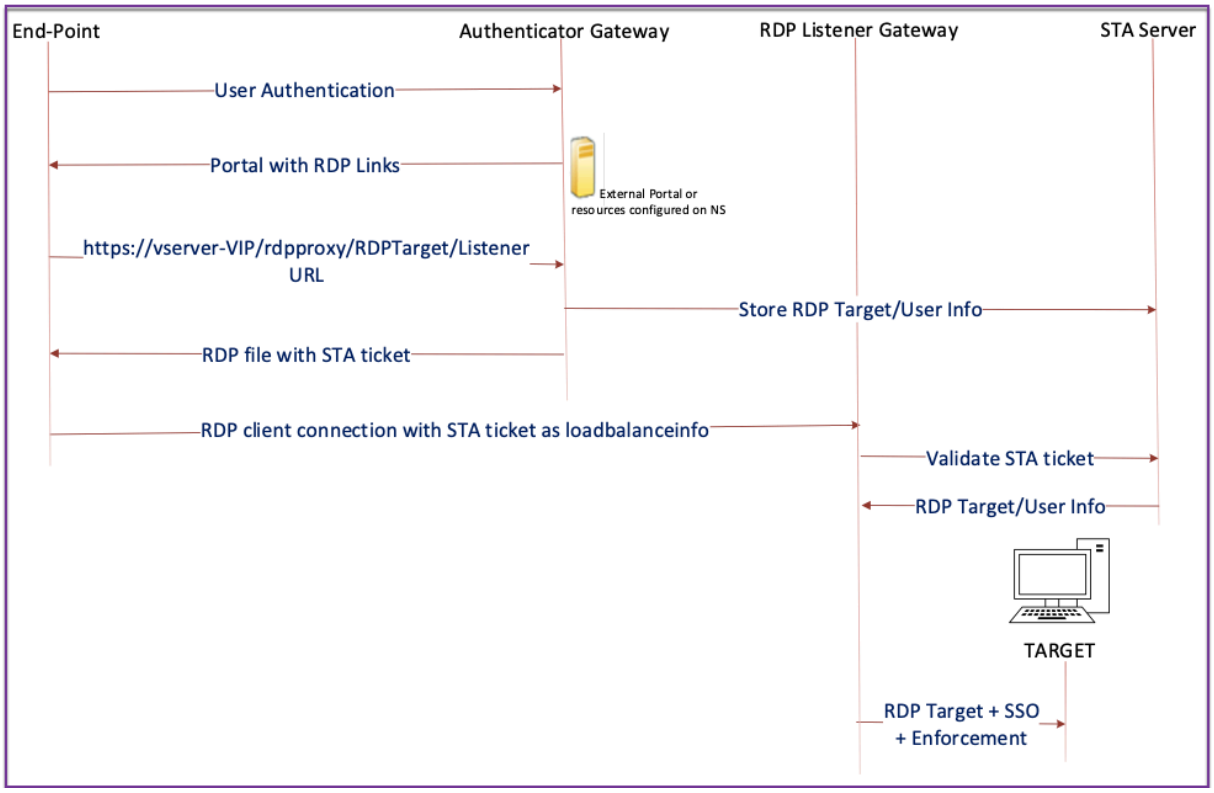
Según el flujo de conexión anterior, existen dos soluciones de implementación:

- Solución de puerta de enlace sin estado (doble): la enumeración de recursos RDP y la descarga de archivos RDP se realizan a través de la puerta de enlace del autenticador, pero el inicio de la conexión RDP se realiza a través de la puerta de enlace de escucha de
- Solución de gateway única: la enumeración de recursos RDP, la descarga de archivos RDP y el inicio de la conexión RDP se realizan a través de la misma puerta de enlace.

### Compatibilidad con gateway sin estado (dual)

En la siguiente ilustración se muestra la implementación:




- Un usuario se conecta a la VIP de puerta de enlace de autenticación y proporciona las credenciales.
- Tras iniciar sesión correctamente en la puerta de enlace, se redirige al usuario a la página principal o al portal externo, que enumera los recursos de escritorio remoto a los que puede acceder el usuario.
- Una vez que el usuario selecciona un recurso RDP, el VIP de Authenticator Gateway recibe la solicitud en el formato que `https://vserver-vip/rdpproxy/rdptarget/listener` indica el recurso publicado en el que hizo clic el usuario. Esta solicitud contiene la información sobre la dirección IP y el puerto del servidor RDP que el usuario ha seleccionado.
- La puerta de enlace de autenticación procesa la solicitud /rdpproxy/. Dado que el usuario ya está autenticado, esta solicitud incluye una cookie de puerta de enlace válida.
- La información de `RDPTarget` y `RDPUser` se almacena en el servidor STA y se genera un tíquet STA. La información almacenada en el servidor STA se cifra mediante la clave previamente compartida configurada. La puerta de enlace de autenticación utiliza uno de los servidores STA configurados en el servidor virtual de puerta de enlace.
- La información de "Listener"obtenida en la solicitud /rdpproxy/ se coloca `.rdp file` como

"fulladdress", y el tíquet STA (predefinido con el AuthID de STA) se coloca `.rdp file` como "loadbalanceinfo".

- `.rdp file` se devuelve al dispositivo de punto final del cliente.
- El cliente RDP nativo se inicia y se conecta al `RDPListener Gateway`. Envía el tíquet STA en el paquete inicial.

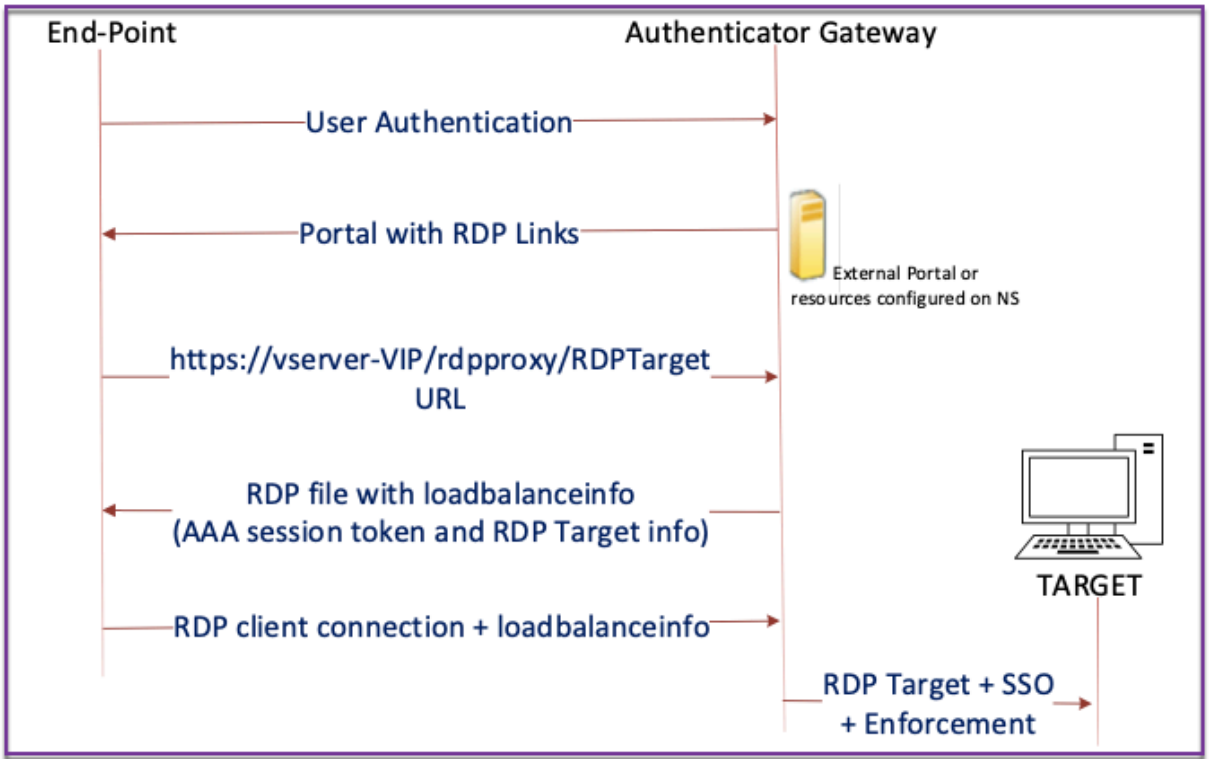
  La puerta de enlace `RDPListener` valida el tíquet de STA y obtiene la información de `RDPTarget` y `RDPUser`. El servidor STA que se va a utilizar se recupera mediante el 'authID' presente en el `loadbalanceinfo`.
- Se crea una sesión de puerta de enlace para almacenar directivas de autorización/auditoría. Si existe una sesión para el usuario, se reutiliza.
- La puerta de enlace `RDPListener` se conecta a `RDPTarget` e inicia sesión con SSO mediante CREDSSP.

> **Importante:**
>
> - Para el proxy RDP sin estado, el servidor STA valida el tíquet STA, enviado por el cliente RDP, para obtener la información de `RDPTarget`/`RDPUser`. Debe enlazar el servidor STA además del servidor virtual VPN.

### Compatibilidad con puerta de enlace única

En la siguiente ilustración se muestra la implementación:




> **Importante:**
>
> En el caso de una única implementación de puerta de enlace, el servidor STA no es necesario. La puerta de enlace del autenticador `RDPTarget` codifica la cookie de sesión de autenticación, autorización y auditoría de Citrix de forma segura y las envía como `loadbalanceinfo` en `.rdp file`. Cuando el cliente RDP envía este token en el paquete inicial, la puerta de enlace del autenticador decodifica la información de `RDPTarget`, busca la sesión y se conecta a `RDPTarget`.

### Soporte para oyente único

- Escucha única para tráfico RDP y SSL.
- La descarga de archivos RDP y el tráfico RDP se pueden gestionar a través de la misma tupla 2 (es decir, IP y puerto) en el dispositivo NetScaler ADC.

### Requisitos de licencia del proxy RDP

Edición premium, modificación avanzada

> **Nota:**
>
> La función RDP Proxy no está disponible para los clientes que solo tienen una licencia de plataforma Gateway o solo la modificación Standard.

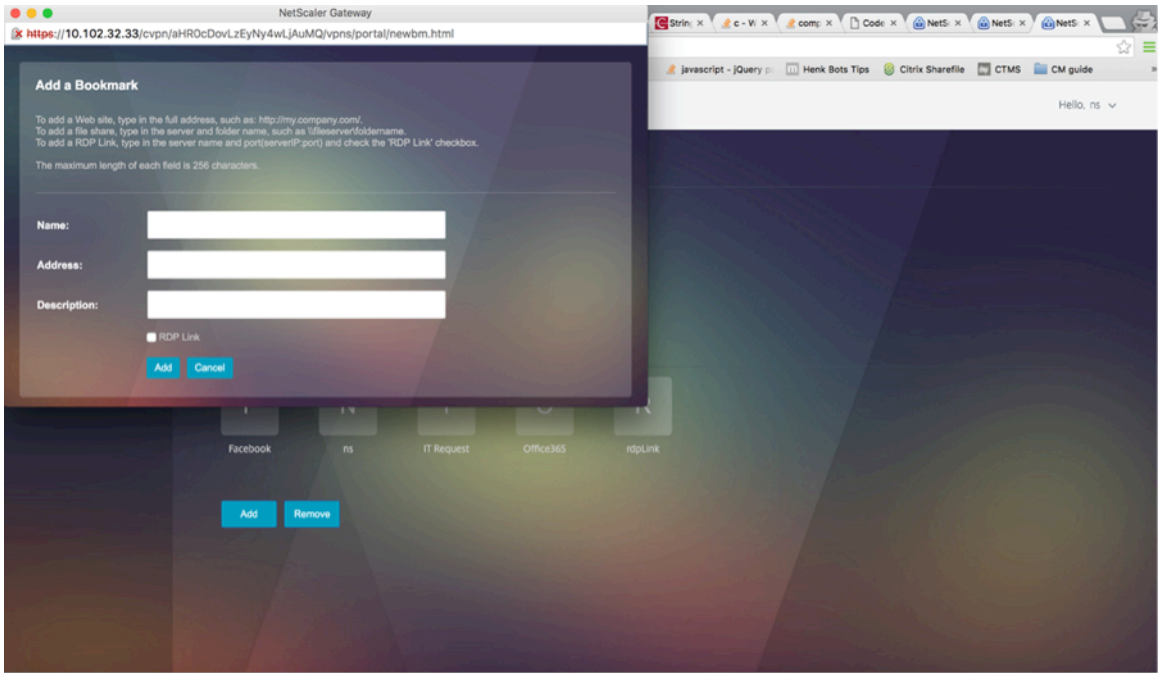
 

Puede utilizar el siguiente comando para habilitar el proxy RDP.

```
enable feature rdpProxy
<!--NeedCopy-->
```

### Marcador

**Generación de enlaces RDP mediante Portal.** En lugar de configurar los vínculos RDP para el usuario o publicar los vínculos RDP a través de un portal externo, puede dar a los usuarios la opción de generar sus propias URL proporcionando `targerIP:Port`. Para la implementación de proxy RDP sin estado, el administrador puede incluir información del listener RDP en FQDN: Formato de puerto como parte del perfil de cliente RDP. Esto se hace bajo la opción `rdpListener`. Esta configuración se utiliza para la generación de enlaces RDP a través del portal en modo de puerta de enlace dual.




#### Crear marcadores

1. Cree marcadores en la página del portal para acceder a los recursos de RDP: (ActualURL comienza por `rdp://`).
2. Agregar url de VPN `<urlName> <linkName> <actualURL>`
   - La dirección URL debe tener el siguiente formato: `rdp://<TargetIP:Port>`.
   - Para el modo proxy RDP sin estado, la URL debe tener el siguiente formato: `rdp://<TargetIP:Port>/<ListenerIP:Port>`

- La URL se publica en el portal en el formato:
  `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>`
  `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>/<ListenerIP:Port>`

3. Enlaza los marcadores al usuario, grupo, servidor virtual VPN o VPN global.

#### Funciones y modos que se habilitan para el proxy RDP

```
- enable ns feature ssl

- enable ns feature sslvpn

- enable ns feature rdpproxy

- enable mode usnip
<!--NeedCopy-->
```

### Pasos de configuración de alto nivel para el proxy

Los siguientes pasos de alto nivel implicados en la configuración del proxy RDP sin estado.

- Crear un perfil de servidor RDP
- Creación de un perfil de cliente RDP
- Crear y enlazar un servidor virtual
- Crear un marcador
- Crear o modificar un perfil o una directiva de sesión
- Enlazar un marcador

#### Configurar un perfil de cliente

Configure el perfil del cliente en la puerta de enlace del autenticador. A continuación se muestra un ejemplo de configuración:

```
add rdpClient profile <name> [-addUserNameInRdpFile ( YES | NO )] [-
    audioCaptureMode ( ENABLE | DISABLE )] [-keyboardHook <keyboardHook
    >] [-multiMonitorSupport ( ENABLE | DISABLE )] [-psk <string>] [-
    rdpCookieValidity <positive_integer>] [-rdpCustomParams <string>] [-
    rdpFileName <string>] [-rdpHost <optional FQDN that will be put in
    the RDP file as 'fulladdress>] [-rdpUrlOverride ( ENABLE | DISABLE
    )] [-redirectClipboard ( ENABLE | DISABLE )] [-redirectComPorts (
    ENABLE | DISABLE )] [-redirectDrives ( ENABLE | DISABLE )] [-
    redirectPnpDevices ( ENABLE | DISABLE )] [-redirectPrinters ( ENABLE
     | DISABLE )] [-videoPlaybackMode ( ENABLE | DISABLE )]
<!--NeedCopy-->
```

Asocie el perfil del cliente RDP al servidor virtual VPN.

Esto se puede hacer configurando una SessionAction+sessionPolicy o estableciendo el parámetro VPN global.

Ejemplo:

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <
    prioritynumber>
<!--NeedCopy-->
```

O bien

```
set vpn parameter  – rdpClientprofile <name>
<!--NeedCopy-->
```

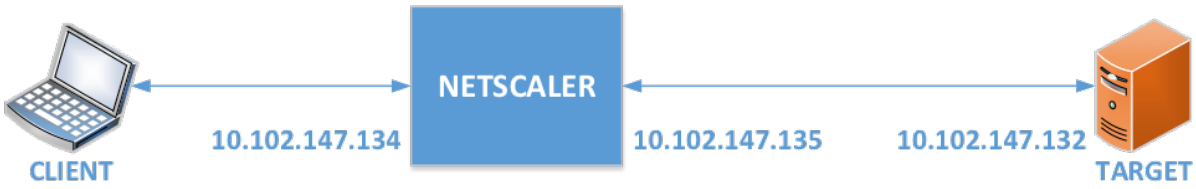
#### Configurar un perfil de servidor

Configure el perfil del servidor en la puerta de enlace del listener.

```
add rdp ServerProfile <profilename> -rdpIP <IPV4 address of the RDP
    listener> -rdpPort <port for terminating RDP client connections> -
    psk <key to decrypt RDPTarget/RDPUser information, needed while
    using STA>`
<!--NeedCopy-->
```

`rdp ServerProfile` debe configurarse en el servidor virtual VPN.

```
add vpn vserver v1 SSL <publicIP> <portforterminatingvpnconnections> -
    rdpServerProfile <rdpServer Profile>`
<!--NeedCopy-->
```




### Configuración del proxy RDP mediante la CLI

A continuación se muestra un ejemplo de configuración del proxy RDP mediante la CLI.

- Agregue la URL de VPN del usuario con la información de destino.

```
add aaa user Administrator  –password freebsd123$%^

add vpn url rdp RdpLink rdp://rdpserverinfo

add dns addrec rdpserverinfo 10.102.147.132

bind aaa user Administrator   –urlName rdp
<!--NeedCopy-->
```

- Configure el perfil de cliente y servidor RDP para la conexión VPN.

```
add rdp clientprofile p1  –psk citrix -redirectClipboard ENABLE

add rdp serverprofile p1 -rdpIP 10.102.147.134 -psk citrix

add vpn vserver mygateway SSL  10.102.147.134 443  –
   rdpserverprofile p1

set vpn parameter -clientlessVpnMode ON -
   defaultAuthorizationAction ALLOW -rdpClientProfileName p1

add ssl certKey gatewaykey -cert rdp_rootcert.pem  -key
   rdp_rootkey

bind ssl vserver mygateway -certkeyName gatewaykey
<!--NeedCopy-->
```

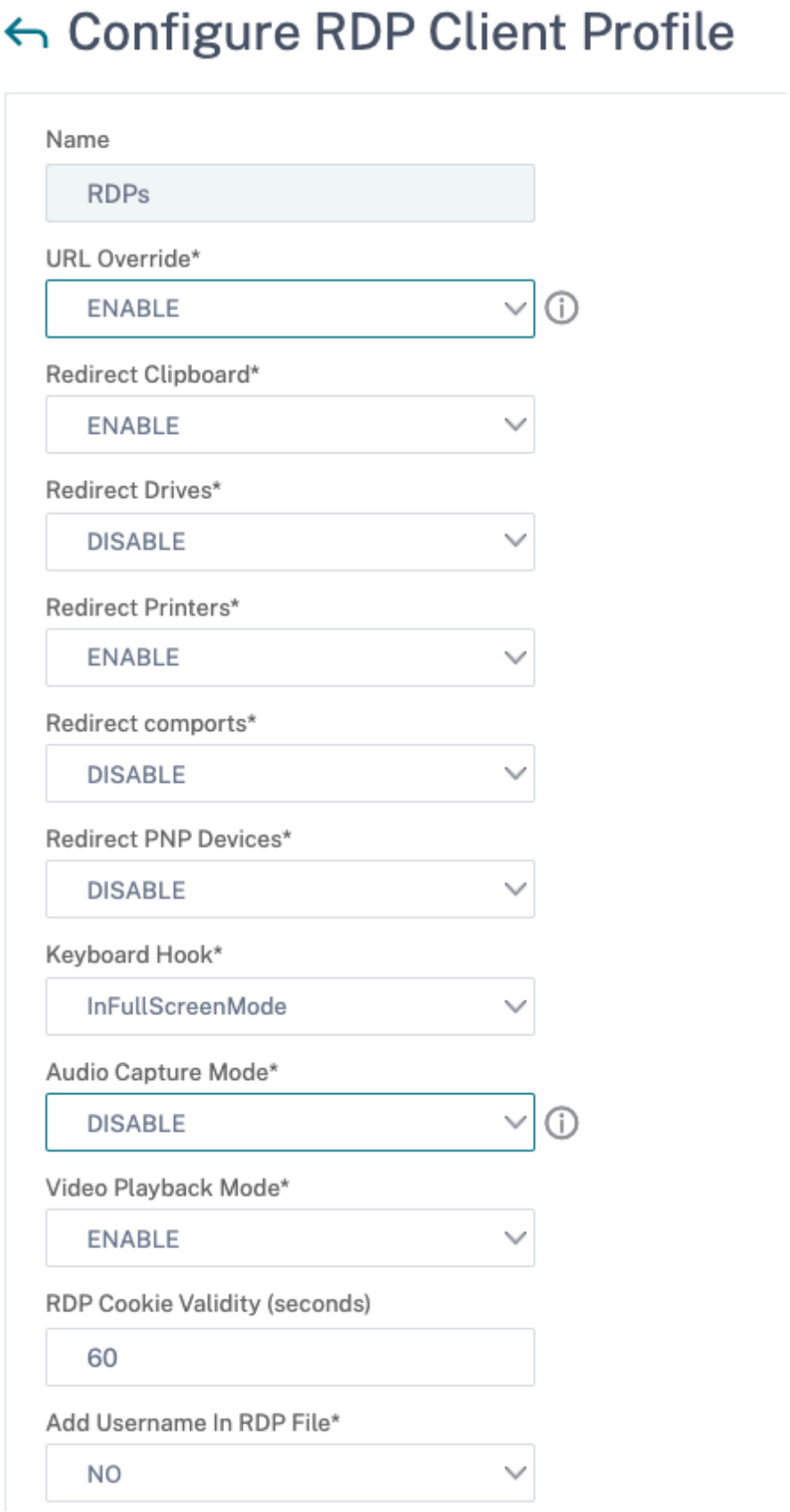
- AGREGAR SNIP para la conexión de NetScaler ADC al destino.

```
add ns ip 10.102.147.135  255.255.255.0  –type SNIP
<!--NeedCopy-->
```

### Configuración del proxy RDP mediante la interfaz gráfica de usuario

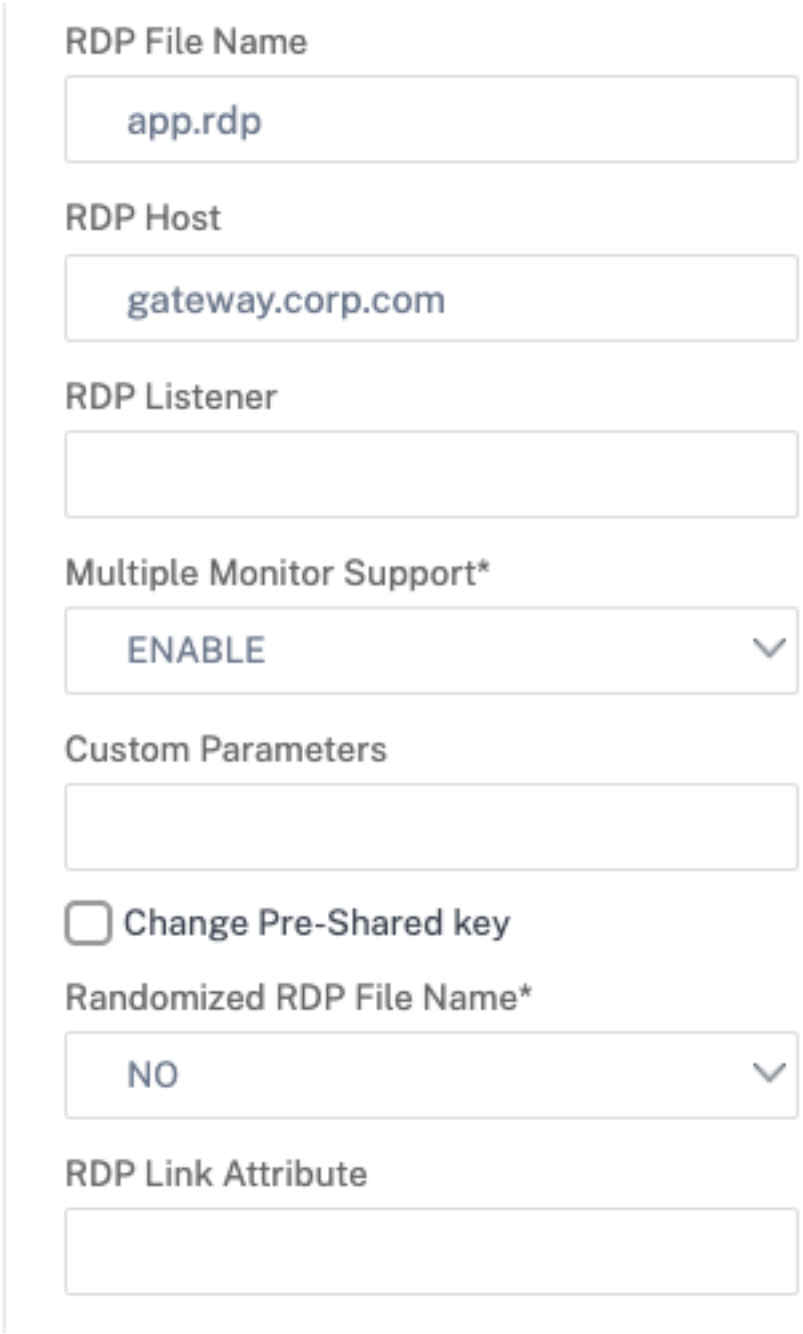
1. Vaya a **NetScaler Gateway > Directivas**, haga clic con el botón derecho en **RDP**y haga clic en **Activar función**
2. Haga clic en RDP en el panel de navegación. A la derecha, selecciona la ficha **Perfiles de cliente** y haga clic en **Agregar**.
3. Introduzca un nombre para el perfil del cliente y configúrelo.



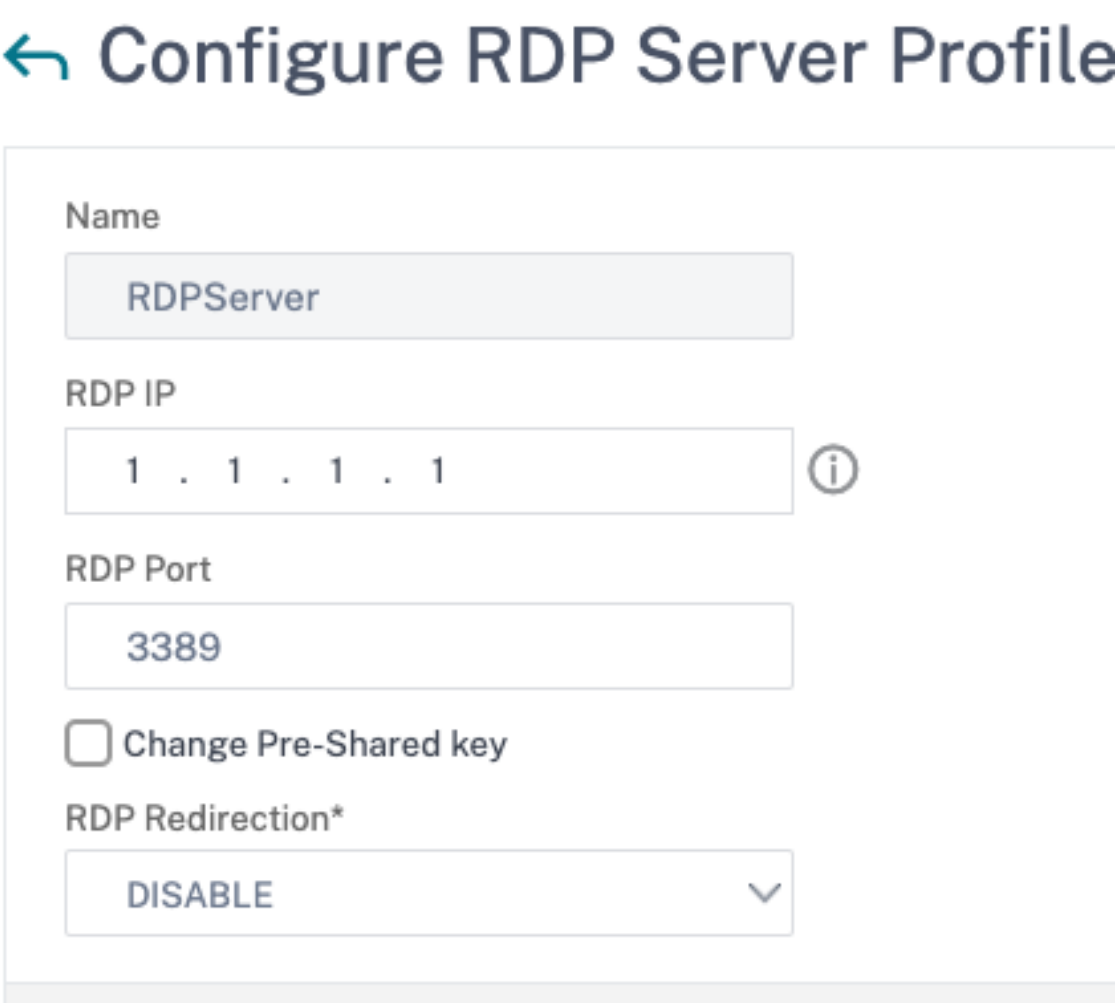

 

4. En el campo Host de RDP, introduzca el FQDN que se resuelve en la escucha del proxy RDP, que suele ser el mismo FQDN que el FQDN del dispositivo NetScaler Gateway.
5. En **Clave previamente compartida**, introduzca una contraseña y haga clic en **Aceptar**.



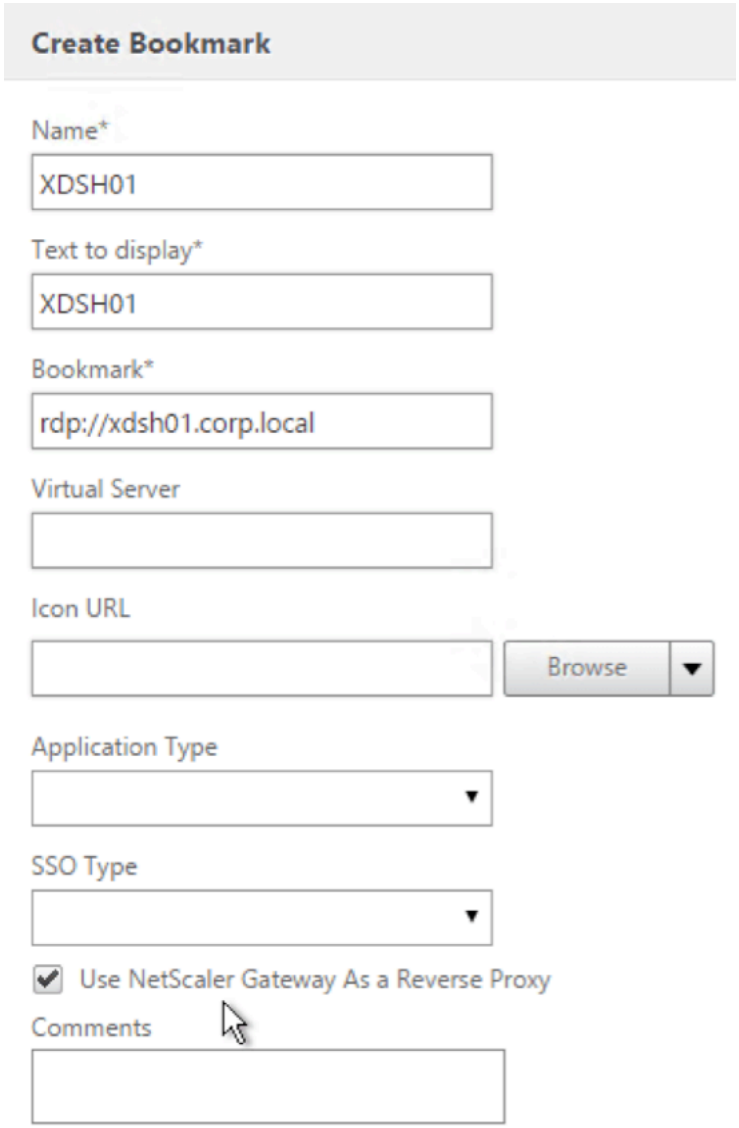

6. Introduzca un nombre en el perfil del servidor.
7. Introduzca la dirección IP del servidor virtual de puerta de enlace al que va a enlazar este perfil.
8. Introduzca la misma clave previamente compartida que configuró para el perfil de cliente RDP. Haga clic en **Crear**.



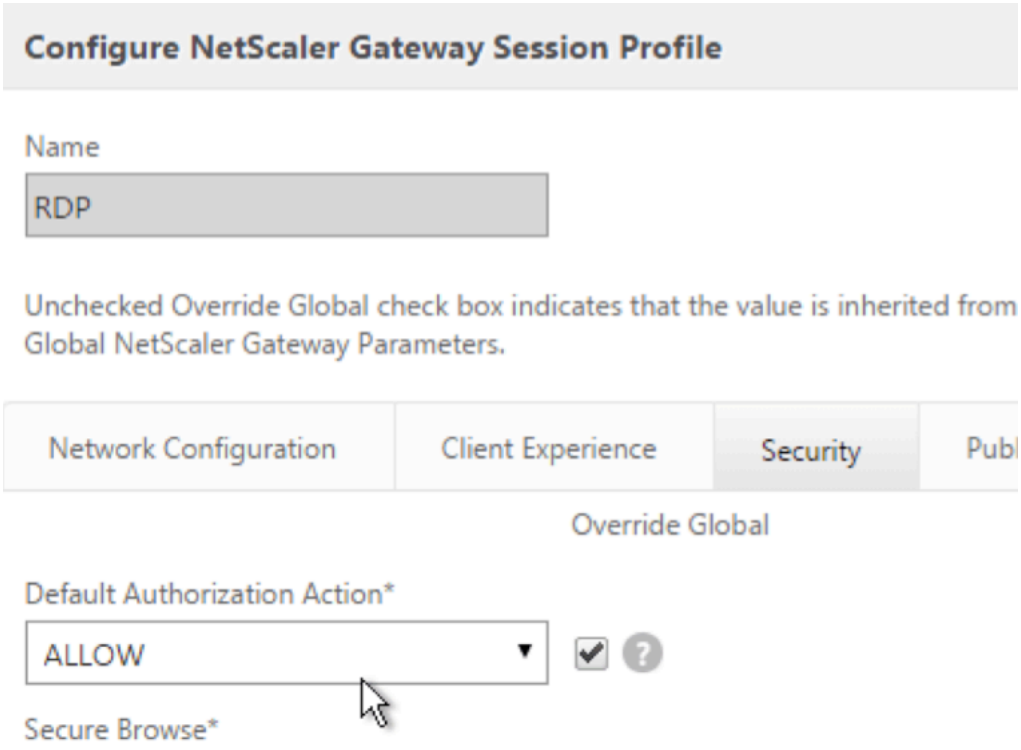

9. Si quiere agregar marcadores de RDP en la página del portal de acceso sin cliente, a la izquierda, expanda **NetScaler Gateway**, expanda **Recursos**y haga clic en **Marcadores**.
10. A la derecha, haga clic en **Agregar**.
11. Ponle un nombre al marcador.
12. Para la URL, escriba **rdp: //myRDPServer mediante IP o DNS**.
13. Seleccione Usar **NetScaler Gateway como proxy inverso** y haga clic en **Crear**.
14. Cree marcadores según sus necesidades.

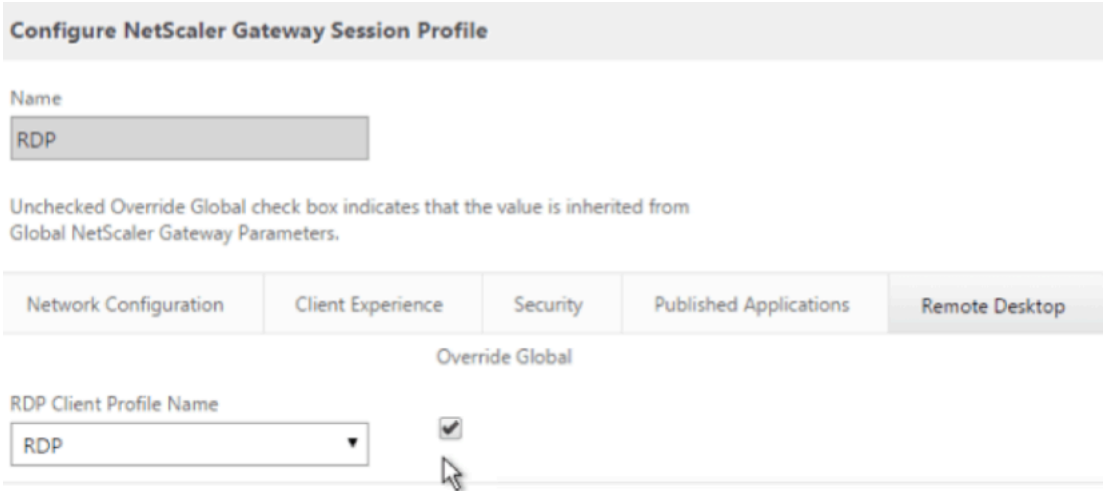



15. Crea o modifica un perfil de sesión. Vaya a **NetScaler Gateway > Directivas > Sesión**.
16. En la ficha Seguridad, establezca **Acción de autorización predeterminada** en **Permitir**. O bien, puede utilizar directivas de autorización para controlar el acceso.

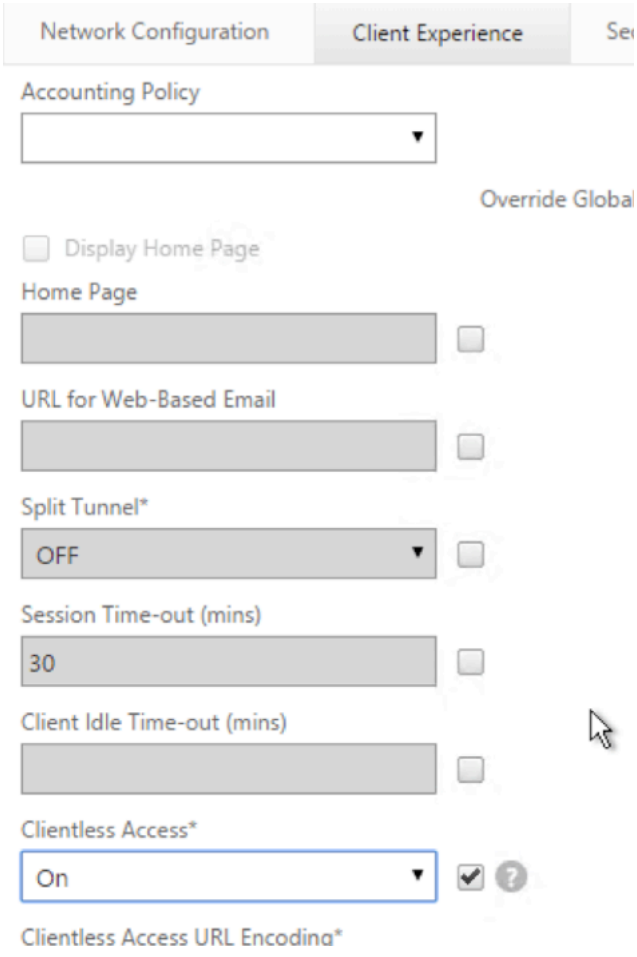



17. En la ficha Escritorio remoto, seleccione el perfil de cliente RDP que creó anteriormente.

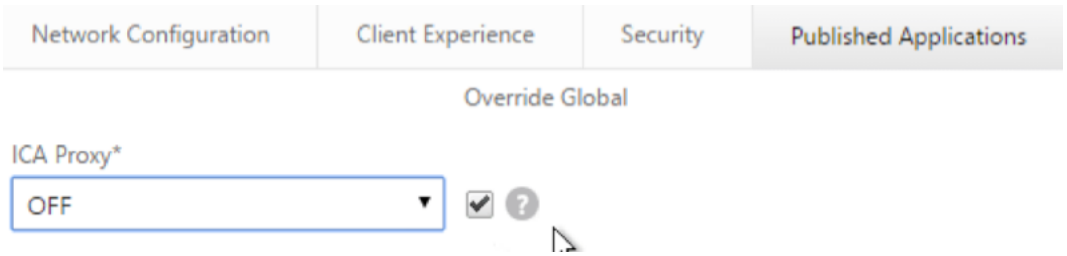



18. Si quiere utilizar marcadores, en la ficha **Experiencia del cliente**, establezca **Acceso sin clienteen On**.

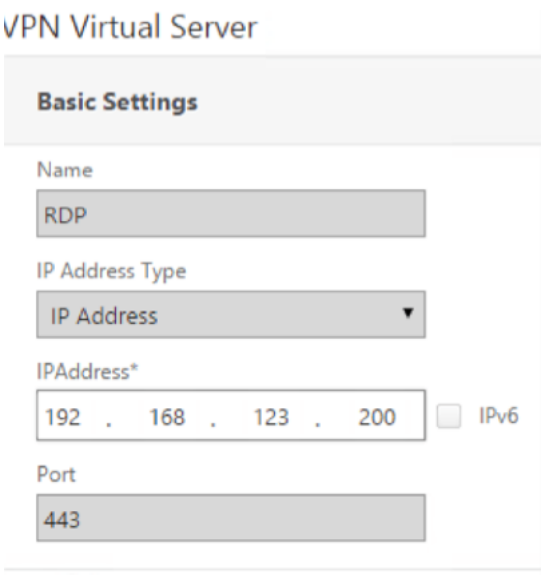



19. En la ficha **Aplicaciones publicadas**, asegúrese de que el proxy ICA esté **DESACTIVADO**.

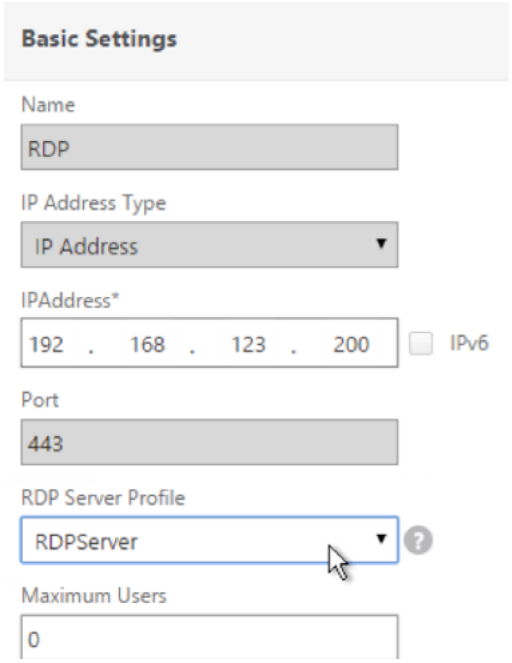



20. Modifique o cree su servidor virtual de puerta de enlace.
21. En la sección **Configuración básica**, haga clic en **Más**.

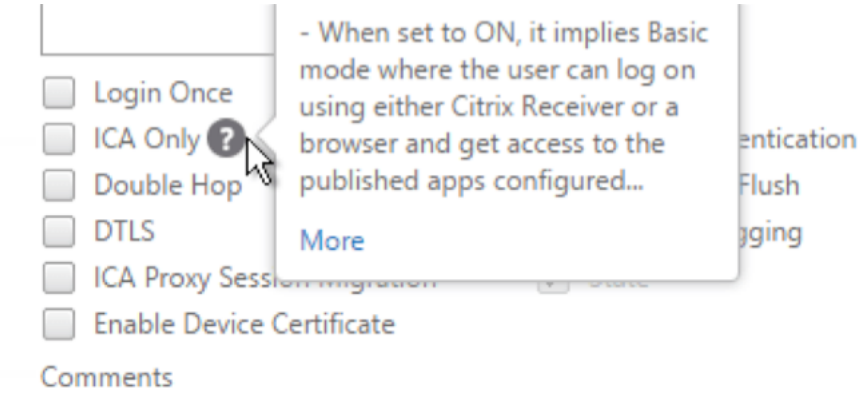



22. Utilice la lista de perfiles de servidor RDP para seleccionar el perfil de servidor RDP que creó anteriormente.

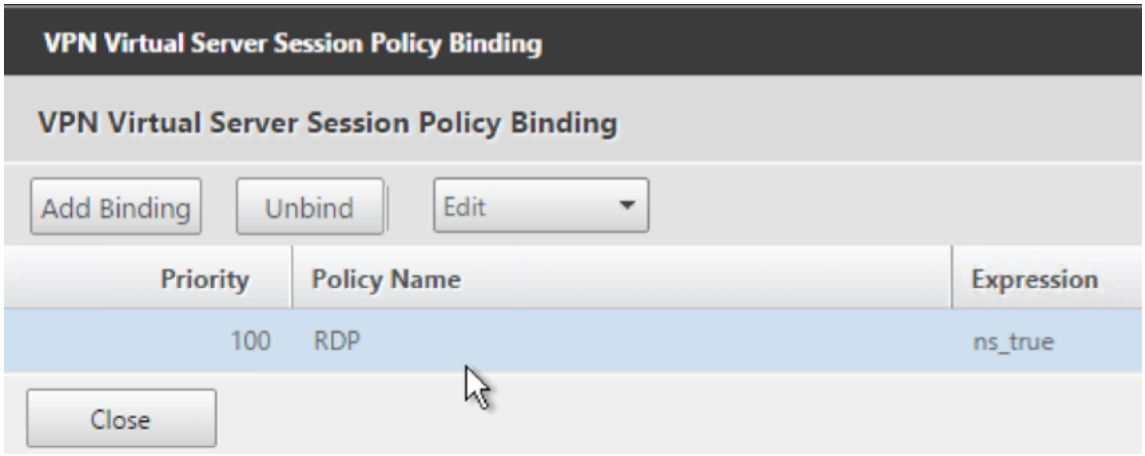



23. Desplácese hacia abajo. Asegúrese de que **solo ICA** no esté marcada.

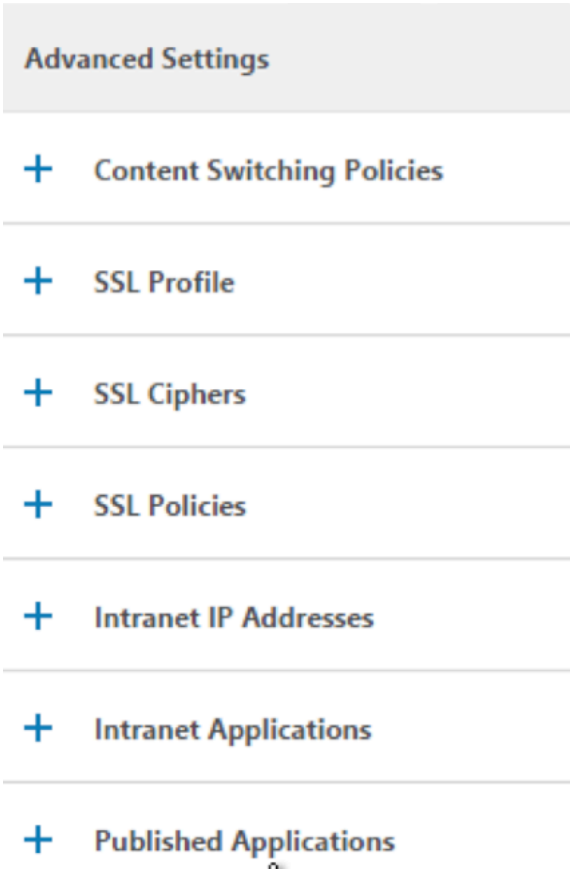



24. Enlazar un certificado.
25. Enlazar directivas de autenticación.
26. Enlazar la directiva/perfil de sesión que tiene configurado el perfil de cliente RDP.

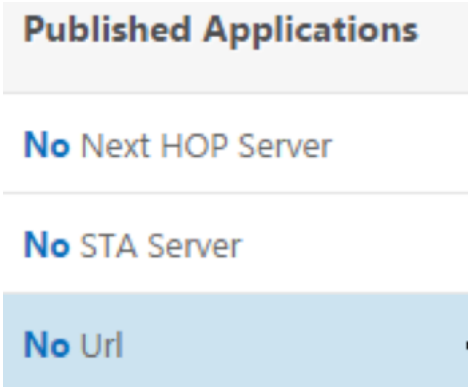



27. Puede enlazar marcadores al servidor virtual de NetScaler Gateway o a un grupo de autenticación, autorización y auditoría. Para enlazar con el servidor virtual de NetScaler Gateway, a la derecha, en la sección Configuración avanzada, haga clic en **Aplicaciones publicadas**.

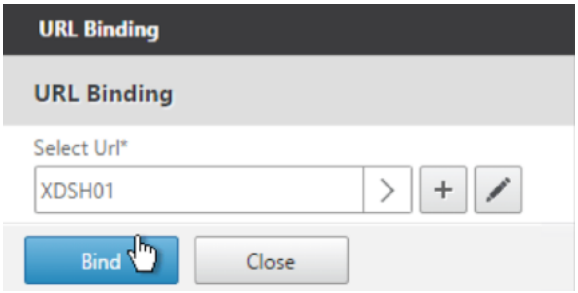
 




28. A la izquierda, en la sección **Aplicaciones publicadas**, haga clic en **Sin URL**.

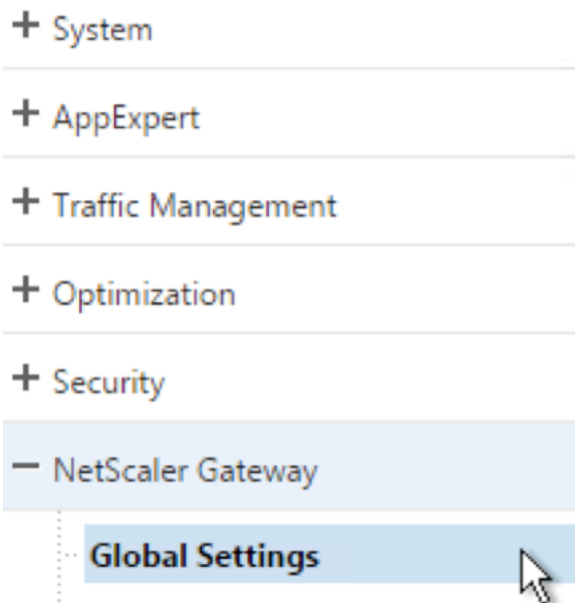



29. Enlace sus marcadores.

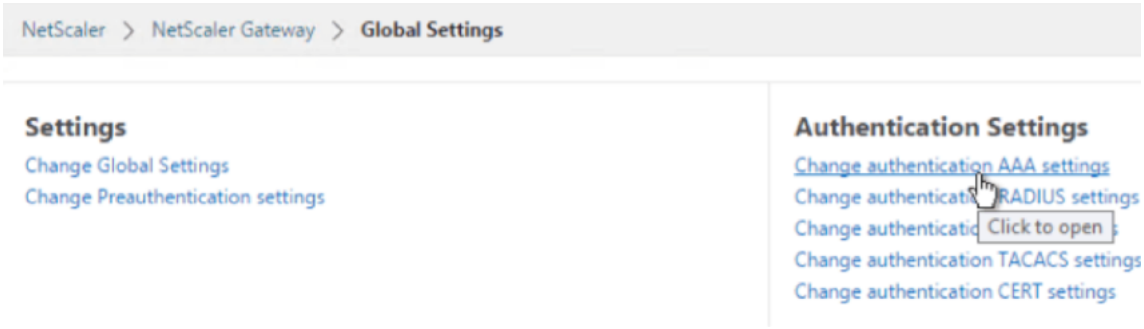


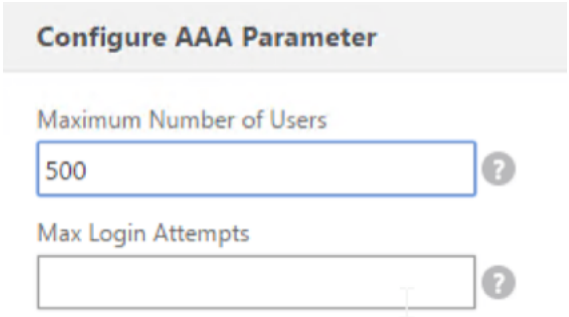
30. Dado que solo ICA no se especifica para este servidor virtual de NetScaler Gateway, asegúrese de que las licencias universales de NetScaler Gateway estén configuradas correctamente. A la izquierda, expanda **NetScaler Gateway** y haga clic en **Configuración global**.




31. A la derecha, haga clic en **Cambiar configuración de autenticación AAA**.

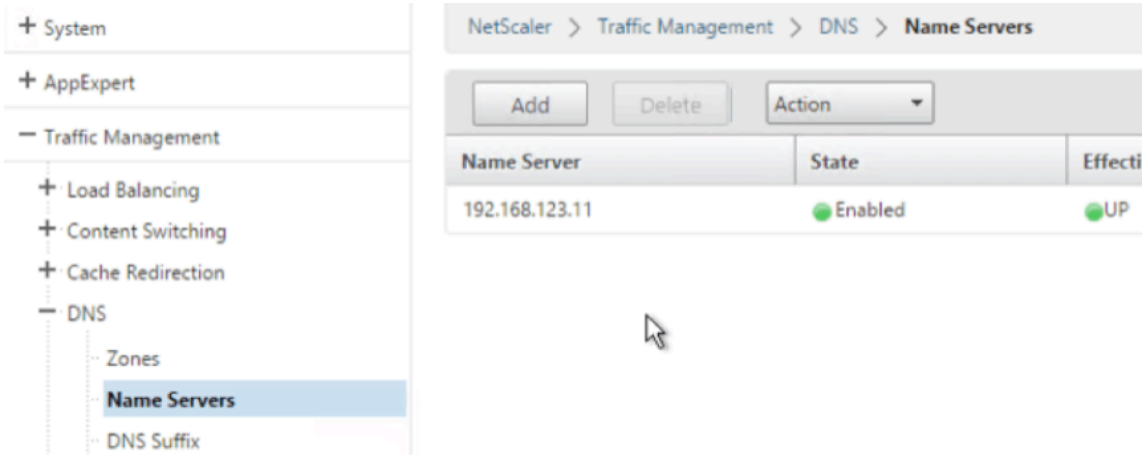



32. Cambie el **número máximo de usuarios** al límite con licencia.

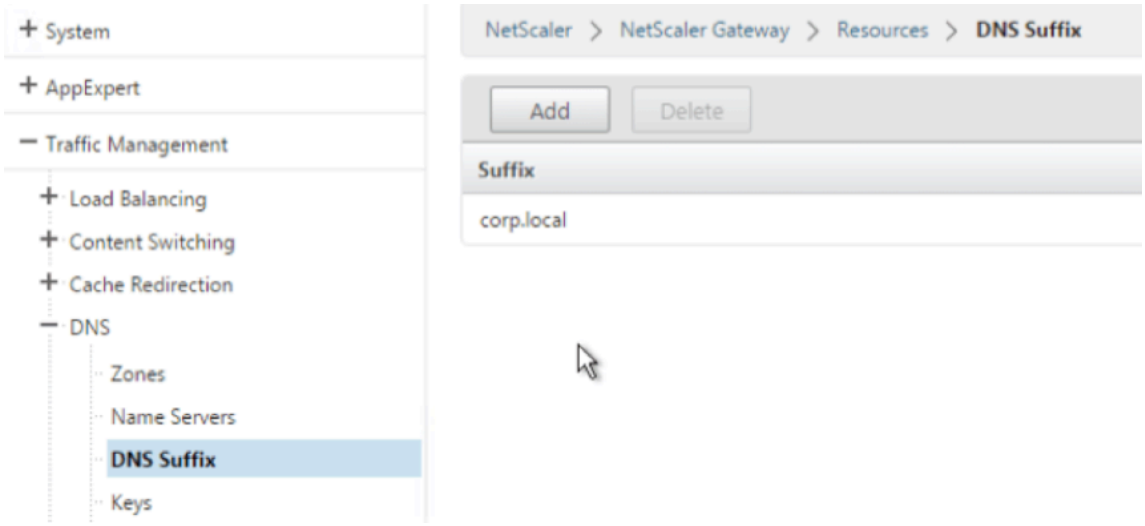



33. Si quiere conectarse a servidores RDP mediante DNS, asegúrese de que los servidores DNS estén configurados en el dispositivo (**Administración del tráfico > DNS > Servidores de nombres)**.

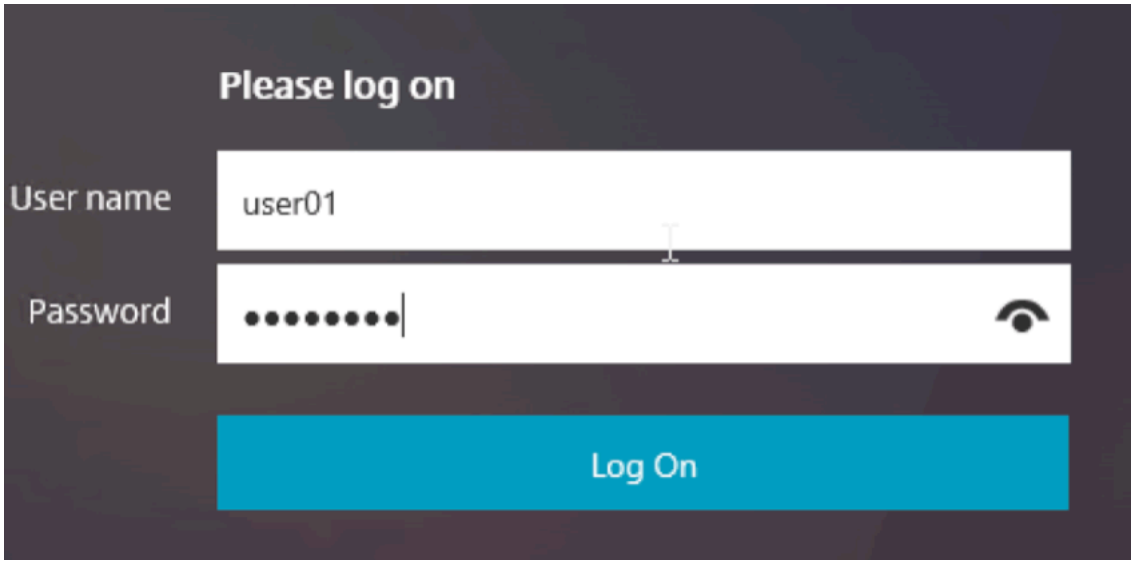



34. Si quiere utilizar los nombres cortos en lugar de los FQDN, agregue un **sufijo DNS (Administración del tráfico > DNS > Sufijo DNS)**.

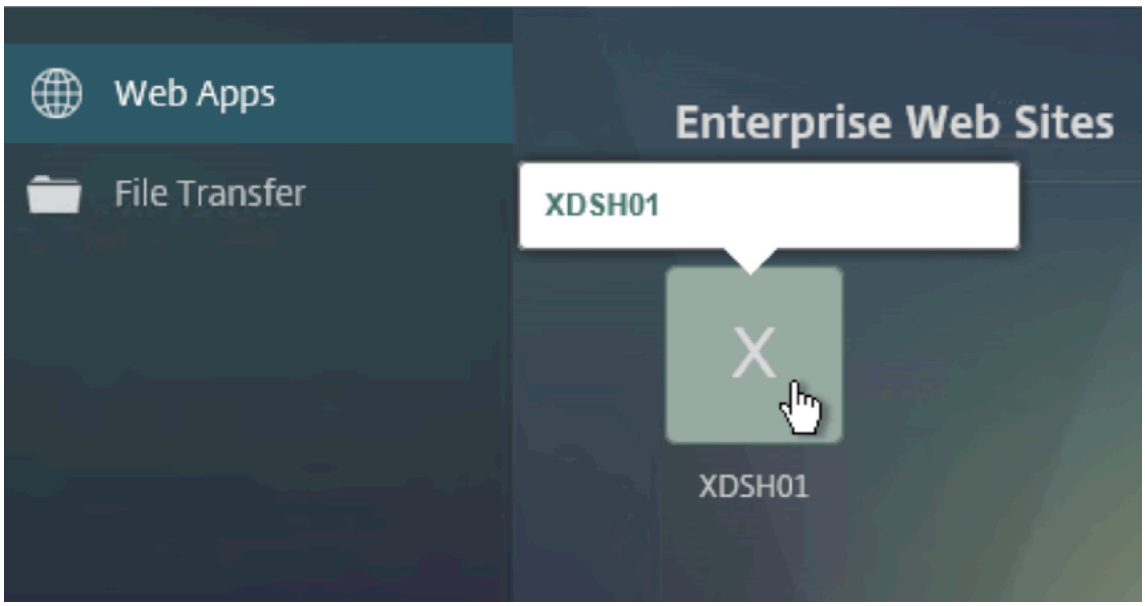



35. Conéctate a su puerta de enlace e inicia sesión.

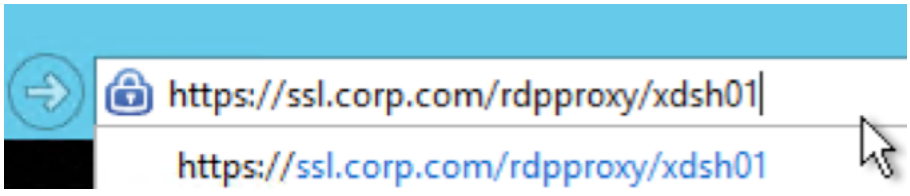
 




36. Si ha configurado **Marcadores**, haga clic en el **marcador**.



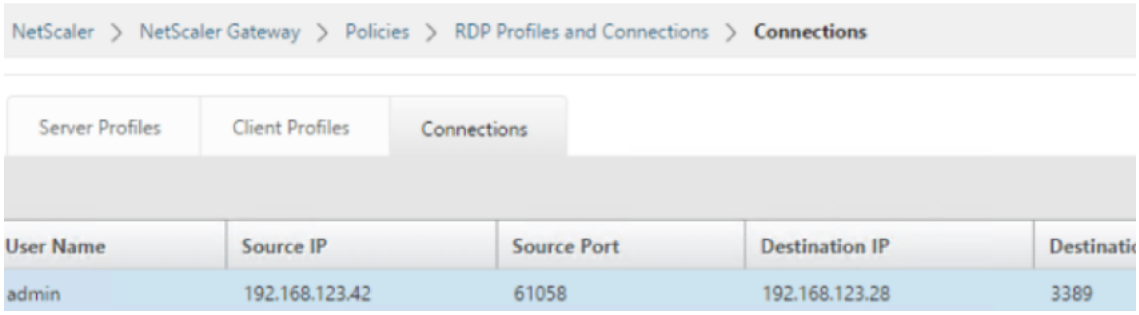

37. Puede cambiar la barra de direcciones a **/rdpProxy/myrdpServer**. Puede introducir una dirección IP (por ejemplo rdpproxy/192.168.1.50) o un nombre DNS (/rdpproxy/myserver).




38. Abre el archivo descargado `.rdp file`.

39. Para ver los usuarios conectados actualmente, vaya a **NetScaler Gateway Policies > RDP.** A la derecha está la ficha **Conexiones**.




### Opción para inhabilitar el SSO

La función SSO (inicio de sesión único) con proxy RDP se puede inhabilitar mediante la configuración de directivas de tráfico de NetScaler ADC para que siempre se pidan credenciales al usuario. Cuando el SSO está inhabilitado, la aplicación de RDP (SmartAccess) no funciona.

Ejemplo:

```
add vpn trafficaction <TrafficActionName> HTTP -SSO OFF
<!--NeedCopy-->
```

La directiva de tráfico se puede configurar según el requisito; a continuación se muestran dos ejemplos:

- Para inhabilitar el inicio de usuario único para todo el tráfico:

```
add vpn trafficpolicy <TrafficPolicyName>  "url contains rdpproxy
   " <TrafficActionName>
<!--NeedCopy-->
```

- Para inhabilitar SSO basado en IP/FQDN de origen/destino

```
add vpn trafficPolicy <TrafficPolicyName>  "HTTP.REQ.URL.CONTAINS
   ("rdpproxy") && CLIENT.IP.SRC.EQ(<IP>)" <TrafficActionName>
bind vpnvserver rdp -policy <TrafficPolicyName> -priority 10
<!--NeedCopy-->
```

## Proxy RDP sin estado

January 26, 2024

El proxy RDP sin estado accede a un host RDP. El acceso se concede a través del RDPListener en Citrix Gateway cuando el usuario se autentica en un Citrix Gateway Authenticator independiente. La información requerida por el RDPListener para Citrix Gateway se almacena de forma segura en un servidor STA.

El flujo y los nuevos botones creados para esta funcionalidad se describen aquí.

### Requisitos previos

- El usuario se autentica en Citrix Gateway Authenticator.
- La URL /rdpproxy inicial y el cliente RDP están conectados a un Citrix Gateway RDPListener diferente.
- La puerta de enlace de autenticación transfiere de forma segura la información de la puerta de enlace RDPListener mediante un servidor STA.

### Configuración

- Agregue un nuevo perfil *RDPServer*. El perfil del servidor está configurado en la puerta de enlace RDPListener.

```
1  add rdpServer Profile [profilename] -rdpIP [IPV4 address of the
      RDP listener] -rdpPort [port for terminating RDP client
      connections] -psk [key to decrypt RDPTarget/RDPUser
      information, needed while using STA].
2  <!--NeedCopy-->
```

  En el caso de un proxy RDP sin estado, el servidor STA valida el vale STA, que envía el cliente RDP, para obtener la información de destino o usuario RDP de RDP.

  El perfil del servidor RDP se configura en el servidor virtual vpn mediante el siguiente comando:

```
1  add vpn vserver v1 SSL [publicIP] [
      portforterminatingvpnconnections] -rdpServerProfile [rdpServer
       Profile]
2  <!--NeedCopy-->
```

> **Advertencia**
> Una vez que el RDPServerProfile esté configurado en el servidor virtual vpn, no se puede modificar. Además, el mismo ServerProfile no se puede reutilizar en otro servidor virtual VPN.

El comando **rdp profile** se renombró como perfil **RDPClient** y tiene parámetros nuevos. Se ha agregado el comando MultiMonitorSupport. Además, se ha agregado una opción para configurar parámetros personalizados, que no se admiten como parte del perfil del cliente RDP. Se ha eliminado el param

clientSSL, ya que la conexión siempre está protegida. El perfil del cliente se configura en la puerta de enlace del autenticador.

```
add rdpClient profile <name> -rdpHost <optional FQDN that will be put
   in the RDP file as ' fulladdress '> \[-rdpUrlOverride \( ENABLE |
   DISABLE )] \[-redirectClipboard \( ENABLE | DISABLE )] \[-
   redirectDrives \( ENABLE | DISABLE )]

      \[-redirectPrinters \( ENABLE | DISABLE )] \[-keyboardHook <
         keyboardHook>] \[-audioCaptureMode \( ENABLE | DISABLE )]
         \[-videoPlaybackMode \( ENABLE | DISABLE )]

      \[-rdpCookieValidity <positive\_integer>]\[-multiMonitorSupport
          \( ENABLE | DISABLE )] \[-rdpCustomParams <string>] La
         configuración —RDPhost se utiliza en una única implementaci
         ón de puerta de enlace.
```

- Asocie el perfil RDP con el servidor virtual vpn.

Esto se puede hacer configurando SessionAction+SessionPolicy o configurando el parámetro vpn global.

Ejemplo

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <
   prioritynumber>

OR

set vpn parameter  – rdpClientprofile <name>
```

### Contador de conexiones

Se agregó un nuevo contador de conexiones ns_rdp_tot_curr_active_conn, que mantiene el registro del número de conexiones activas en uso. Se puede ver como parte del comando nsconmsg en el shell de NetScaler. Más adelante, proporcionaremos un nuevo comando CLI para ver estos contadores.

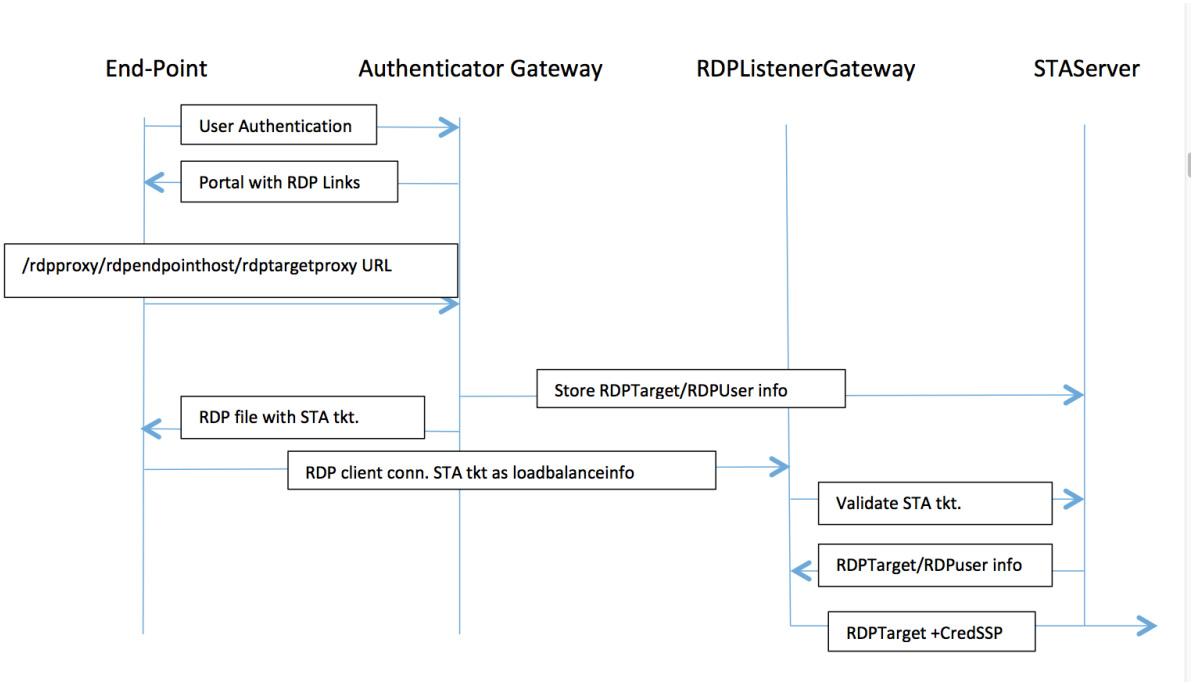
### Flujo de conexión

Hay dos conexiones involucradas en el flujo del proxy RDP. La primera conexión es la conexión VPN SSL del usuario al VIP de Citrix Gateway y la enumeración de los recursos RDP.

La segunda conexión es la conexión del cliente RDP nativo al agente de escucha RDP (se configura

mediante RDPip y RDPport) en Citrix Gateway y, posteriormente, la transmisión por proxy del cliente RDP a los paquetes del servidor de forma segura.




1. El usuario se conecta al Authenticator Gateway VIP y proporciona sus credenciales.
2. Tras iniciar sesión correctamente en Gateway, se redirige al usuario a la página de inicio o al portal externo, que enumera los recursos de escritorio remoto a los que puede acceder el usuario.
3. Una vez que el usuario selecciona un recurso RDP, el Authenticator Gateway VIP recibe una solicitud en el formato `https://AGVIP/rdpproxy/ip:port/rdptargetproxy`que indica el recurso publicado en el que el usuario hizo clic. Esta solicitud contiene la información sobre la IP y el puerto del servidor RDP que el usuario ha seleccionado.
4. La puerta de enlace de autenticación procesa la solicitud /rdpproxy/. Como el usuario ya está autenticado, esta solicitud incluye una cookie de Gateway válida.
5. La información de RDPTarget y RDPUser se almacena en el servidor STA y se genera un ticket STA. La información se almacena como un blob XML que se cifra opcionalmente mediante la clave previamente compartida configurada. Si se cifra, el blob se codifica y almacena en base64. La puerta de enlace de autenticación utilizará uno de los servidores STA que está configurado en el servidor virtual de Gateway.
6. El blob XML tendrá el siguiente formato

   <Value name=”IPAddress”>ipaddr </Value> nport<Value name=”Port”> n </Value>

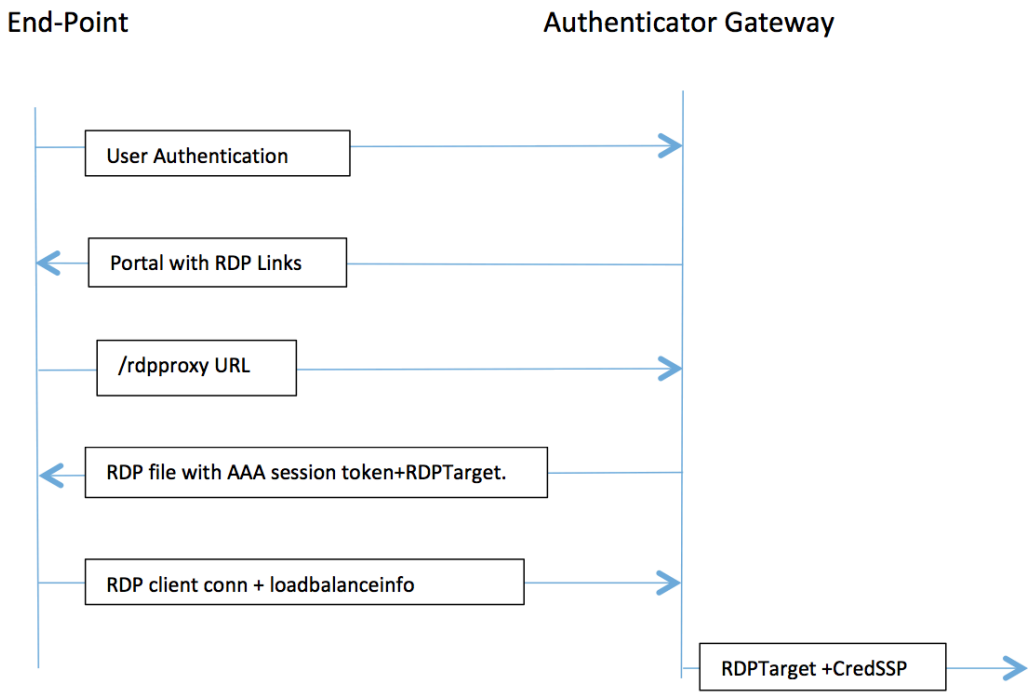
   <Value name=”Username”>nombre de usuario </Value><Value name=”Password”> npwd </Value>

7. El "rdptargetproxy"obtenido en la solicitud /rdpproxy/ se coloca como el 'fulladdress'y el ticket STA (pre-penado con el STA authID) se coloca como el 'loadbalanceinfo'en el archivo.rdp.
8. El archivo.rdp se devuelve al punto final del cliente.
9. El cliente RDP nativo se inicia y se conecta a la puerta de enlace RDPListener. Envía el tíquet STA en el paquete x.224 inicial.
10. La puerta de enlace RDPListener valida el ticket STA y obtiene la información de RDPTarget y RDPUser. El servidor STA que se va a utilizar se recupera mediante el «authID» presente en loadbalanceinfo.
11. Se crea una sesión de puerta de enlace para almacenar directivas de autorización/auditoría. Si ya existe una sesión para el usuario, se vuelve a utilizar.
12. La puerta de enlace RDPListener se conecta al RDPTarget e inicia sesión de forma única mediante CREDSSP.

### Compatibilidad con puerta de enlace única

Si el archivo RDP se genera con la URL /rdpproxy/rdptarget/rdptargetproxy, generaremos un ticket STA; de lo contrario, se utilizará el método actual de «loadbalanceinfo» que hace referencia directamente a la sesión.



En el caso de una implementación de una única puerta de enlace, la URL /rdpproxy llega a la propia puerta de enlace de autenticación. No se requiere un servidor STA. La puerta de enlace de autenticación codifica la cookie de sesión RDPTarget y AAA de forma segura y la envía como «loadbalance-info» en el archivo.rdp. Cuando el cliente RDP envía este token en el paquete x.224, la puerta de enlace del autenticador decodifica la información de RDPTarget, busca la sesión y se conecta al RDPTarget.

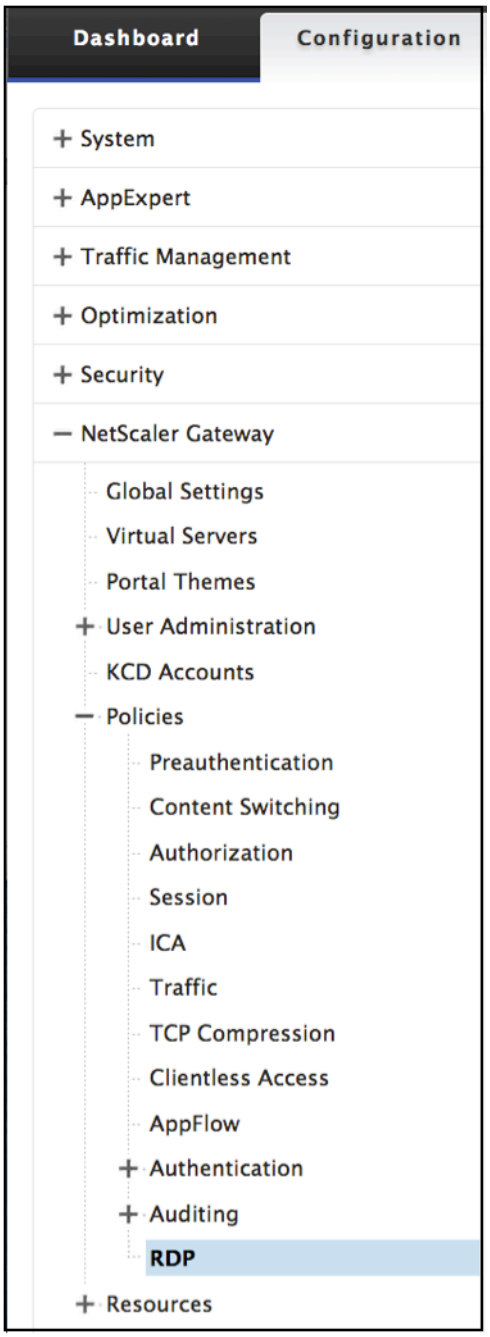
### Notas sobre la actualización

La configuración anterior no funciona con esta nueva versión, ya que los parámetros RDPip y RDP-port, que se configuraban anteriormente en vpn vserver, se han actualizado para que formen parte del RDPServerProfile y «rdp Profile» se ha renombrado como «rdp ClientProfile» y se ha eliminado el antiguo parámetro ClientSSL.

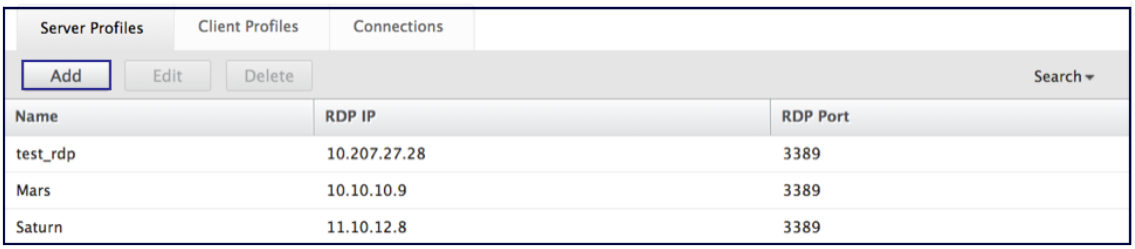
### Crear perfil de servidor RDP

1. Vaya a Citrix Gateway > Políticas > RDP.

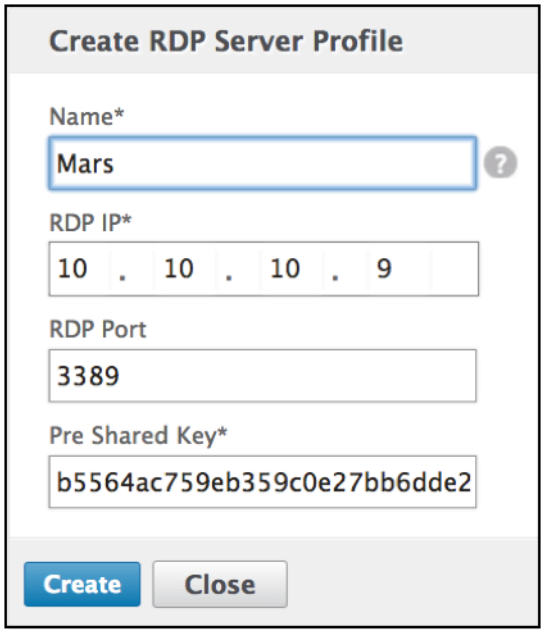



2. Vaya a la pestaña Perfiles del servidor y haga clic en **Agregar** .



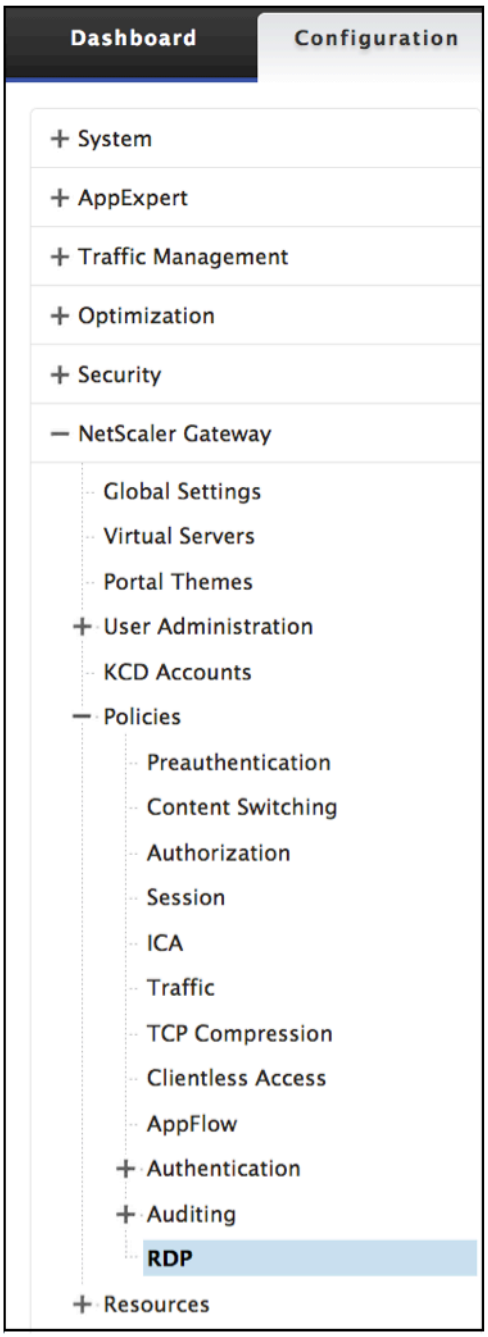
3. Introduzca la siguiente información para crear el perfil del servidor RDP.



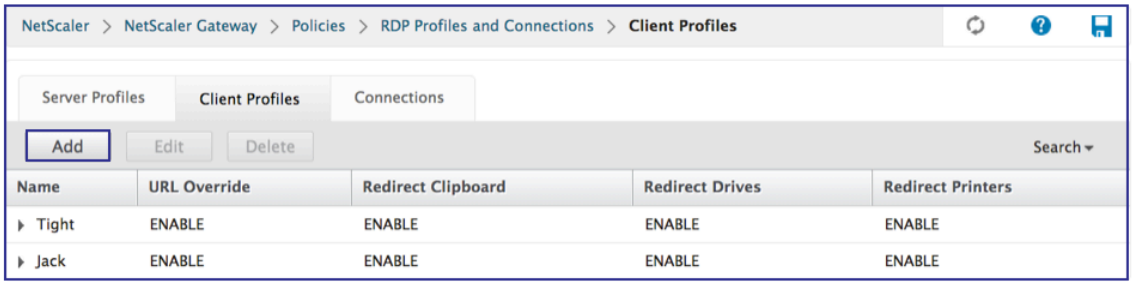

### Configurar el perfil del cliente RDP

1. Vaya a Citrix Gateway > Políticas > RDP

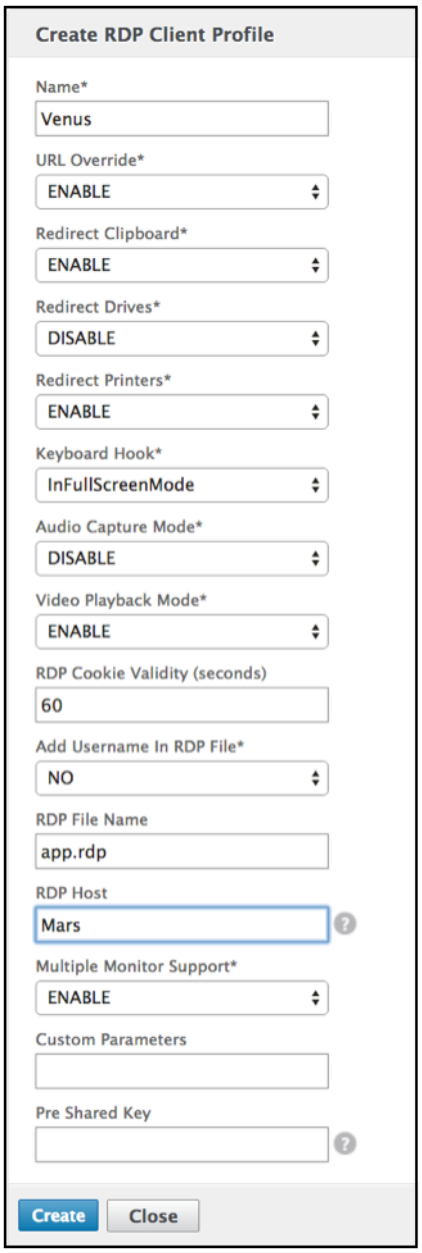



2. Vaya a la pestaña Perfiles de clientes y haga clic en **Agregar** .



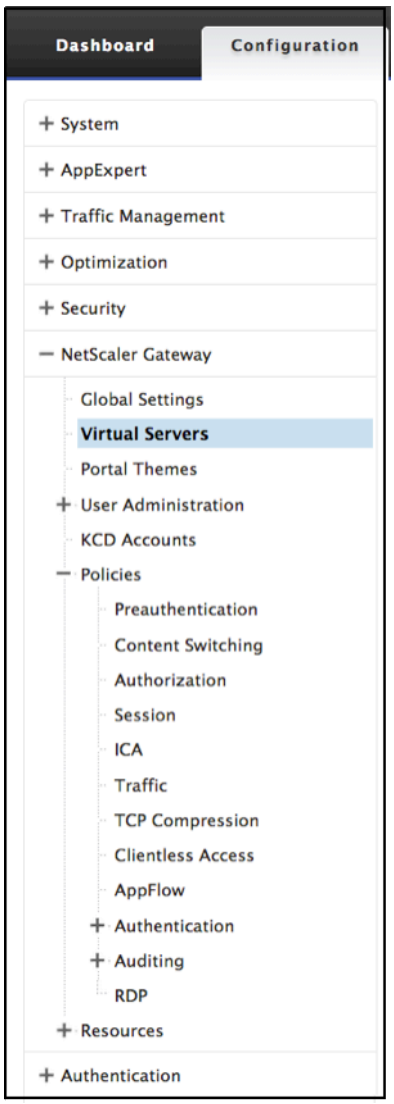
3. Introduzca la siguiente información para configurar el perfil del servidor RDP.




## Configurar un servidor virtual

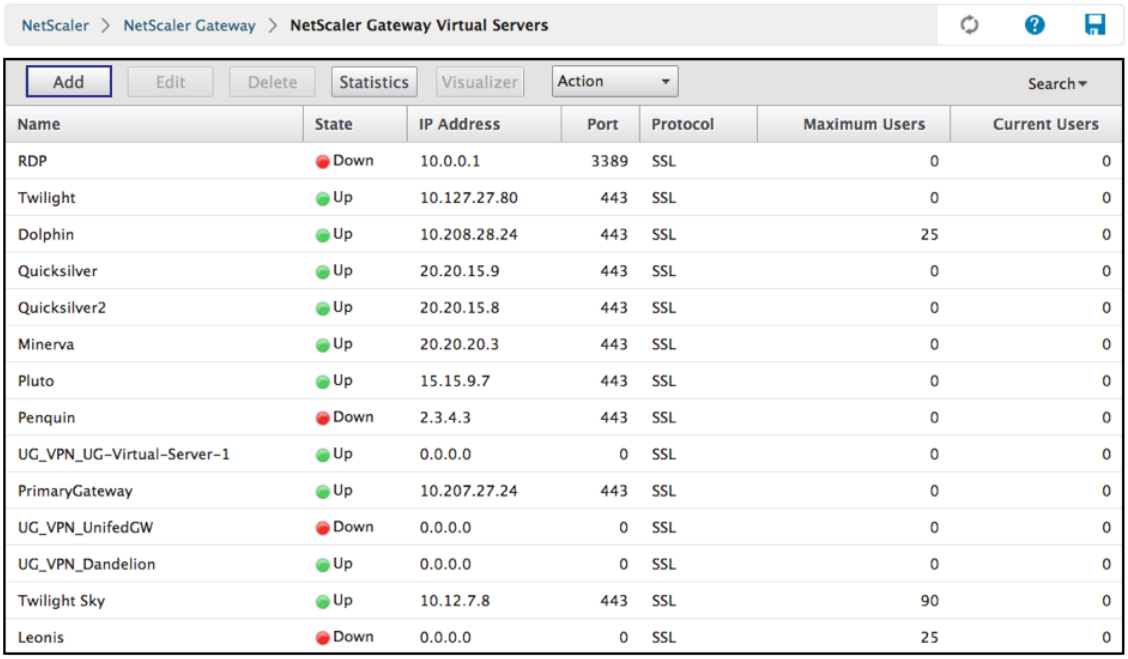
1. Vaya a Citrix Gateway > Servidor virtual.



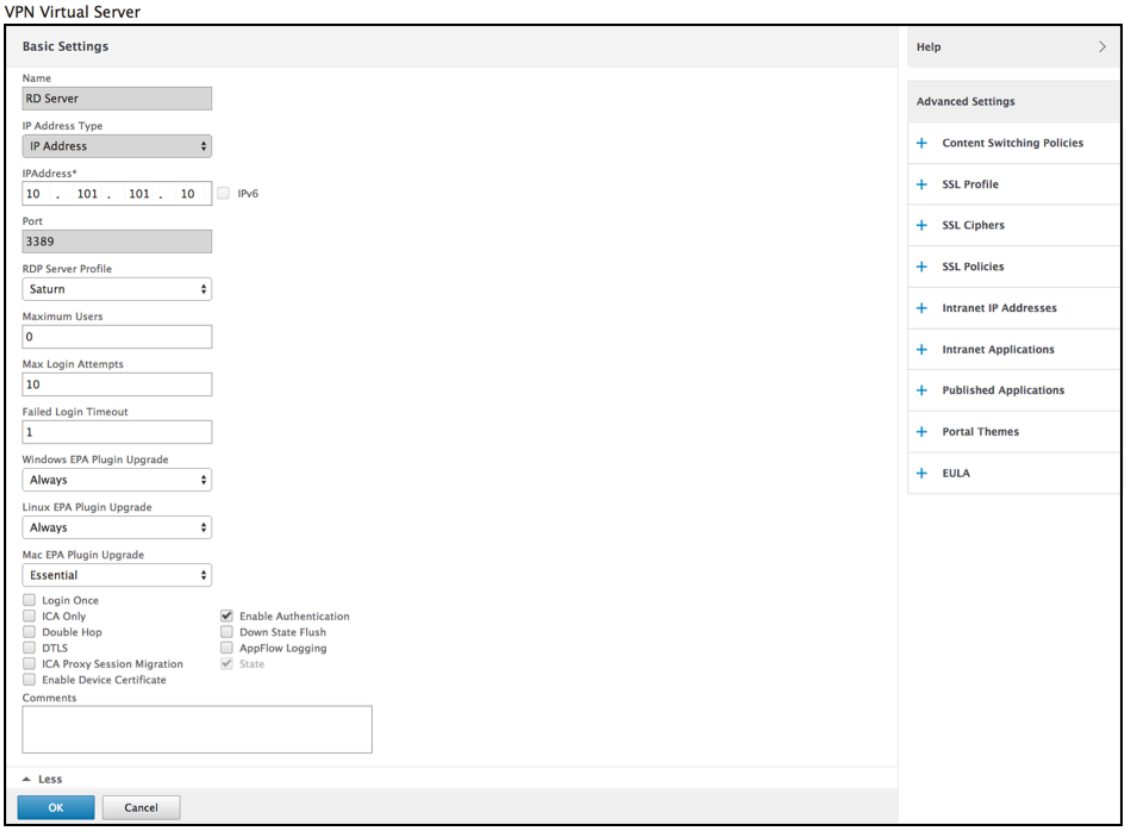

2. Haga clic en **Agregar** para crear un nuevo servidor RDP.



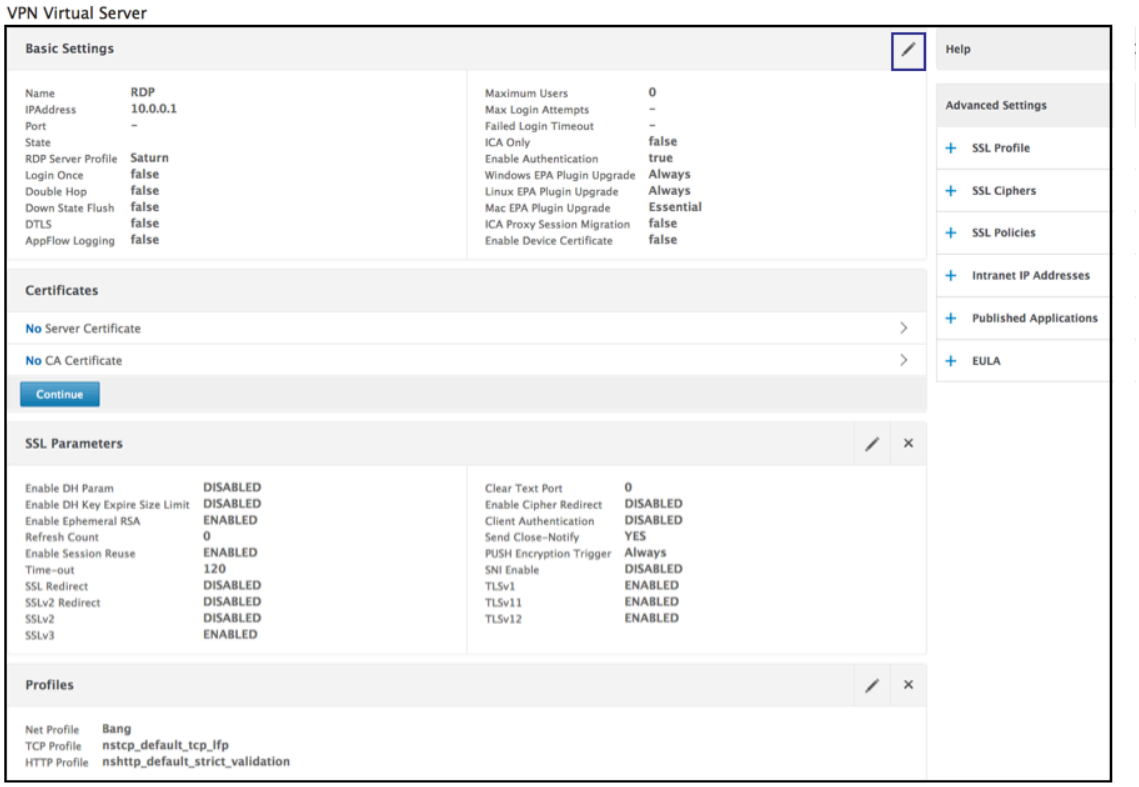

| Name | State | IP Address | Port | Protocol | Maximum Users | Current Users |
|---|---|---|---|---|---|---|
| RDP | Down | 10.0.0.1 | 3389 | SSL | 0 | 0 |
| Twilight | Up | 10.127.27.80 | 443 | SSL | 0 | 0 |
| Dolphin | Up | 10.208.28.24 | 443 | SSL | 25 | 0 |
| Quicksilver | Up | 20.20.15.9 | 443 | SSL | 0 | 0 |
| Quicksilver2 | Up | 20.20.15.8 | 443 | SSL | 0 | 0 |
| Minerva | Up | 20.20.20.3 | 443 | SSL | 0 | 0 |
| Pluto | Up | 15.15.9.7 | 443 | SSL | 0 | 0 |
| Penquin | Down | 2.3.4.3 | 443 | SSL | 0 | 0 |
| UG_VPN_UG-Virtual-Server-1 | Up | 0.0.0.0 | 0 | SSL | 0 | 0 |
| PrimaryGateway | Up | 10.207.27.24 | 443 | SSL | 0 | 0 |
| UG_VPN_UnifedGW | Down | 0.0.0.0 | 0 | SSL | 0 | 0 |
| UG_VPN_Dandelion | Up | 0.0.0.0 | 0 | SSL | 0 | 0 |
| Twilight Sky | Up | 10.12.7.8 | 443 | SSL | 90 | 0 |
| Leonis | Down | 0.0.0.0 | 0 | SSL | 25 | 0 |

3. Complete los datos de esta página de configuración básica **y** haga clic en Aceptar .




4. Haz clic en el **lápiz** para editar la página.




## Redirección de conexiones RDP

January 26, 2024

Un dispositivo Citrix Gateway ahora admite la redirección de conexiones RDP en presencia del agente de conexiones o el directorio de sesión. Una comunicación proxy RDP ya no requiere una URL exclusiva para cada conexión del cliente al servidor. En su lugar, el proxy utiliza una única URL para conectarse a una comunidad de servidores RDP, lo que reduce la sobrecarga de mantenimiento y configuración de un administrador.

**Punto a tener en cuenta**:

- La redirección de conexiones RDP solo se admite cuando el SSO está habilitado y se admite tanto en modo de puerta de enlace única como en modo de puerta de enlace sin estado o puerta de enlace doble junto con la aplicación (SmartAccess).
- La función RDP Proxy solo es compatible con la redirección basada en tokens que admite cookies IP. Los tokens de redirección basados en IP "msts="los devuelve el agente de sesiones de Windows o el agente de conexión cuando la funcionalidad **Usar redirección de direcciones IP** está inhabilitada.

- Puede inhabilitar la opción **Usar redirección de direcciones IP** para habilitar la redirección basada en tokens en la siguiente ubicación.

  `Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > RD Connection Broker`.

- Inhabilite la opción Usar redirección de direcciones IP en los equipos RDSH y no en el equipo del agente de conexiones.
- Se pueden configurar redireccionadores dedicados para la conexión de proxy RDP.

### Requisitos previos

- Cree un perfil de servidor RDP para habilitar el agente de escucha 3389 en el servidor virtual de NetScaler Gateway.
  Si la máquina que quiere RDP no es miembro de ninguna infraestructura de agente de conexiones de RDS, no necesita el agente de escucha 3389.
- Habilite la redirección de conexiones RDP en el dispositivo NetScaler Gateway para admitir el proxy RDP en presencia de un agente de conexiones.

### Implementar proxy RDP en presencia de un agente de conexión

El proxy RDP en presencia de un agente de conexión se puede implementar de las dos formas siguientes.

- Con servidores host de sesión de Escritorio remoto que participan en el equilibrio de carga del agente de conexiones de Escritorio remoto.
- En presencia de la función de equilibrio de carga de RDP.

**Con servidores host de sesión de Escritorio remoto que participan en el equilibrio de carga del agente de conexiones de Escritorio**remoto:

En este caso, el enlace URL RDP se puede configurar para que apunte a uno de los servidores RDP como servidor de destino, que actúa como redirector. Además, es posible tener uno de los servidores RDP de la granja como servidor de destino. En este caso, el servidor no acepta ninguna sesión RDP.

**En presencia de la función**de equilibrio de carga de RDP :

Cuando el equilibrio de carga del agente de conexión no está habilitado, podemos tener la función de equilibrio de carga de RDP disponible en Citrix ADC para realizar el equilibrio de carga necesario de las sesiones de RDP en presencia de un agente de conexiones. En este caso, el enlace URL de RDP debe configurarse para que tenga el balanceador de cargas de RDP como servidor de destino. El

equilibrador de carga RDP puede estar en el mismo dispositivo NetScaler Gateway que el proxy RDP. Para obtener más información, consulte Servidores RDP de equilibrio de carga.

#### Configurar el proxy RDP en presencia de un agente de conexión mediante la CLI

En la línea de comandos, escriba;

```
add rdpserverprofile <Name> -psk <string> -rdpRedirection ( ENABLE |
    DISABLE )

add rdpserverprofile serverProfileName -psk " secretString " -
    rdpRedirection ENABLE
<!--NeedCopy-->
```

#### Configurar la redirección de conexiones RDP mediante la GUI de NetScaler ADC

1. Vaya a **Citrix Gateway > Políticas > RDP**.
2. Haga clic con el botón derecho en **RDP** para **habilitaro inhabilitar** la funcionalidad de redirección RDP.

## Rellenar URL de RDP según el atributo LDAP

January 26, 2024

Puede configurar un dispositivo NetScaler Gateway para recuperar una lista de servidores RDP (IP/FQDN) de un atributo de servidor LDAP. Según la lista recuperada, el dispositivo muestra las URL de RDP de los servidores a los que puede acceder un usuario determinado.

### Para rellenar las URL de RDP según el atributo LDAP mediante la CLI

En la línea de comandos, escriba:

```
add rdpclientprofile <Name>  – rdpUrlLinkAttribute <string>

add rdpclientprofile clientProfileName  – rdpUrlLinkAttribute
    rdpServerAttribute
<!--NeedCopy-->
```

En el ejemplo anterior, RDPServerAttribute corresponde a los detalles del servidor RDP de un usuario determinado en un servidor LDAP.

**Nota**: Para obtener los detalles del atributo LDAP del servidor LDAP, la acción LDAP debe configurarse con la misma cadena que se configura `pUrlLinkAttribute` como se indica a continuación.

```
add authentication ldapAction dnpg_ldap -serverIP <IP address>-ldapBase
    <"domain name"> -ldapBindDn <username> -ldapLoginName
   sAMAccountName -ldapbindDnpassword <password>

add authentication ldapAction dnpg_ldap -serverIP 10.102.39.101 -
   ldapBase "dc=dnpg-blr,dc=com" -ldapBindDn sqladmin@dnpg-blr.com -
   ldapLoginName sAMAccountName -ldapbindDnpassword xxxx

add authentication ldapPolicy dnpg_ldap_pol ns_true dnpg_ldap

bind vpn vs vserver<name> -pol dnpg_ldap_pol

set ldapaction dnpg_ldap -attributes "rdpServerAttribute"

set rdpclientprofile ldap -rdpLinkAttribute rdpServerAttribute
<!--NeedCopy-->
```

### Configuración del servidor LDAP

En el servidor LDAP, lleve a cabo los siguientes pasos:

1. Vaya a un **usuario**concreto.
2. En **Usuarios y equipos de AD**, haga clic en **Ver** y, a continuación, en **Detalles**.
3. Haga clic con el botón derecho del ratón en el **nombre de usuarioy,**
4. Cambie el valor del atributo requerido y haga clic **en**Aceptar .

### Para rellenar las URL de RDP basadas en el atributo LDAP mediante la interfaz gráfica de usuario

1. Vaya a **Citrix Gateway > Políticas > RDP**.
2. En la página **Perfiles y conexiones de RDP**, haga clic en la ficha **Perfiles de cliente** y seleccione el perfil de cliente en el que quiere configurar el atributo de enlace RDP.
3. En la página **Configurar perfil de cliente RDP**, en **Atributo de vínculo de RDP**, introduzca el nombre del atributo LDAP.

   **Nota:** El valor del atributo LDAP puede ser una lista separada por comas.

## Aleatorizar el nombre del archivo RDP con el proxy RDP

January 26, 2024

Al hacer clic en una URL RDP, se descarga un archivo RDP. Al hacer clic de nuevo en la URL de RDP, se descarga un nuevo archivo RDP con el mismo nombre, lo que genera una ventana emergente para reemplazar el nuevo archivo por el archivo existente. Para evitar esto, el administrador puede optar por aleatorizar el nombre del archivo rdp. <outputof time ()\ >El nombre del archivo ahora se distribuye aleatoriamente añadiendo la salida de la función time () en el formato\ <rdpFileName\ >\ _ \.rdp. De este modo, el dispositivo genera un nombre de archivo RDP único cada vez que descarga un archivo.

### Configurar compatibilidad para la aleatorización de nombres de archivo RDP con proxy RDP

**Para configurar la compatibilidad con la aleatorización de nombres de archivo RDP con proxy RDP mediante la interfaz de línea de comandos del símbolo del sistema, escriba**:

```
1     add rdpclientprofile <profileName> -rdpfileName <filename> -
         randomizeRDPFilename <YES/NO>
2
3     add rdpclientprofile clientProfileName -rdpfileName testRDP -
         randomizeRDPFilename YES
4 <!--NeedCopy-->
```

**Para configurar la compatibilidad con la asignación aleatoria del nombre de archivo RDP con un proxy RDP mediante la GUI de Citrix ADC:**

1. Vaya a **NetScaler Gateway** > **Directivas** > **RDP**.
2. En la página **Perfiles y conexiones RDP**, haga clic en la ficha **Perfiles de cliente** y seleccione el perfil de cliente en el que quiere configurar aleatoriamente la funcionalidad de nombre de archivo RDP.
3. En la página **Configurar perfil de cliente de RDP**, seleccione **SÍ** en el menú desplegable junto al campo **Nombre de archivo RDP aleatorizado**.

## Compatibilidad con proxy PCoIP habilitado para NetScaler Gateway para VMware Horizon View

January 26, 2024

NetScaler Gateway 12.0 admite el protocolo PC-over-IP (PCoIP), que es el protocolo de visualización remota de varias soluciones de VDI que no son de Citrix, incluida VMware Horizon View. PCoIP es análogo al protocolo Citrix HDX/ICA y al protocolo Microsoft RDP. PCoIP utiliza el puerto UDP 4172.

Cuando PCoIP se transmite mediante proxy a través de NetScaler Gateway, NetScaler Gateway puede reemplazar las soluciones de acceso remoto PCoIP tradicionales, como View Security Server o VMware Access Point.

**En los siguientes casos se ilustra el uso de la solución VMware Horizon View habilitada para NetScaler Gateway.**

- Usuarios de PCoIP de VMware Horizon que necesitan acceder de forma remota a grupos de escritorios y grupos de aplicaciones de VMware Horizon View a través de NetScaler Gateway sin implementar un servidor de seguridad de Horizon View ni un punto de acceso de VMware.
- Los usuarios de PCoIP acceden de forma remota a otras soluciones de escritorios virtuales basadas en PCoIP a través de NetScaler Gateway.

> **Nota**
>
> NetScaler Gateway se implementa como solución de acceso remoto.

## Configuración del proxy PCoIP habilitado para NetScaler Gateway para VMware Horizon View

January 26, 2024

### Requisitos previos

**Versión**: NetScaler ADC 12.0 o superior

**Licencia universal**: PCoIP Proxy utiliza la función de acceso sin cliente de NetScaler Gateway, lo que significa que cada conexión de NetScaler Gateway debe tener licencia para NetScaler Gateway Universal. En el servidor virtual de NetScaler Gateway, asegúrese de que **ICA Only** esté desactivada.

**Infraestructura de Horizon View**: Una infraestructura interna de Horizon View funcional. Asegúrese de poder conectarse a Horizon View Agents internamente sin NetScaler Gateway. Asegúrese de que el **túnel seguro HTTP (S) de Horizon View y la SecureGateway PCoIP** no estén habilitados en los servidores de conexión de View a los que NetScaler ADC realizará conexiones proxy.
Se admiten las siguientes versiones de VMware Horizon view.

- Servidor de conexión: 7.0.1 y superior

- Horizon Client: 4.2.0 y superior (Windows y Mac)

**Puertos de firewall**:

Asegúrese de lo siguiente:

- UDP 4172 y TCP 443 deben abrirse desde los clientes de Horizon View a la VIP de NetScaler Gateway.
- UDP 4172 debe estar abierto desde el SNIP de NetScaler ADC a todos los agentes internos de Horizon View.
- El proxy PCoIP es compatible con el Citrix ADC implementado detrás de NAT. Los siguientes son los puntos importantes a tener en cuenta:
  - La compatibilidad se basa en la configuración de parámetros FQDN del servidor virtual VPN
  - Solo admite FQDN de acceso público y no IP
  - Admite solo puertos 443 y 4172
  - Debe ser una NAT estática

**Certificado: certificado** válido para el servidor virtual de NetScaler Gateway.

**Autenticación**: Una directiva/servidor de autenticación LDAP que utiliza sintaxis clásica.

**Unified Gateway (opcional)**: Si Unified Gateway, cree la Unified Gateway antes de agregar la funcionalidad PCoIP.

**Tema del portal RfWebUI**: Para el acceso del explorador web a Horizon View, el servidor virtual de NetScaler Gateway debe configurarse con el tema RfWebUI.

**Horizon View Client**: Horizon View Client debe instalarse en el dispositivo cliente, incluso si se accede a iconos publicados de Horizon mediante el portal NetScaler ADC RfWebUI.

**Para configurar NetScaler Gateway para que admita el proxy PCoIP para VMware Horizon View:**

1. Vaya a **Configuración > Directivas de NetScaler Gateway > PCoIP**.
2. Cree un perfil de servidor virtual y un perfil PCoIP en la página **Perfiles y conexiones de PCoIP**.
   a) Para crear un perfil de servidor virtual, en la ficha **Perfiles de vServer**, haga clic en **Agregar**.
   b) Escriba un nombre para el perfil del servidor virtual.
   c) Introduzca un nombre de dominio de Active Directory que se utiliza para el inicio de sesión único en el servidor de conexión de View y, a continuación, haga clic en **Crear.**
   **Nota: El** servidor virtual de NetScaler Gateway solo admite un dominio de Active Directory. Además, el nombre de dominio especificado aquí se muestra en Horizon View Client.

d) Haga clic en **Login**.

e) Para crear un perfil PCoIP, en la ficha **Perfiles**, haga clic en **Agregar**.

   i. Introduzca un nombre para el perfil PCoIP.

   ii. Introduzca la URL de conexión del servidor de conexión de VMware Horizon View interno y, a continuación, haga clic en **Crear**.

f) Vaya a **Configuración > Citrix Gateway > Políticas > Sesión** .

g) A la derecha, selecciona la ficha **Perfiles de sesión**.

h) En la página **Perfiles y directivas de sesión de NetScaler Gateway**, cree o modifique un perfil de sesión de NetScaler Gateway.

   i. Para crear un perfil de sesión de NetScaler Gateway, haga clic en **Agregar**y escriba un nombre.

   ii. Para modificar un perfil de sesión de NetScaler Gateway, selecciónelo y haga clic en **Modificar**.

i) En la ficha **Experiencia del cliente**, asegúrese de que el valor **Acceso sin cliente** esté establecido **en On**.

j) En la ficha **Seguridad**, asegúrese de que el valor **Acción de autorización predeterminada** esté establecido en **PERMITIR**.

k) En la ficha **PCoIP**, seleccione el perfil PCoIP necesario y, a continuación, haga clic en **Crear**. También puede crear o modificar perfiles PCoIP desde esta ficha.

l) Haga clic en **Crear** o en **Aceptar** para terminar de crear o modificar el perfil de sesión.

m) Si ha creado un perfil de sesión, debe crear también una directiva de sesión correspondiente.

   i. Vaya a **Configuración > Citrix Gateway > Políticas > Sesión** .

   ii. A la derecha, selecciona la ficha **Directivas de sesión**.

   iii. Haga clic en **Agregar**, introduzca un nombre para la directiva de sesión y seleccione el nombre del perfil de sesión necesario en el menú **Perfil**.

   iv. Si quiere crear la directiva de sesión con la sintaxis predeterminada, en el área Expresión, escriba “true”(sin las comillas) y, a continuación, haga clic en **Crear**. Nota: Unified Gateway tiene el valor predeterminado de Sintaxis clásica.

   v. Si quiere crear la directiva de sesión mediante la sintaxis clásica, primero haga clic en **Cambiar a sintaxis clásica**. A continuación, en el área Expresión, escriba “ns_true” (sin las comillas) y, a continuación, haga clic en **Crear**.

n) Enlazar el perfil del servidor virtual PCoIP y la directiva de sesión creados a un servidor virtual de NetScaler Gateway.

i. Vaya a **NetScaler Gateway > Servidores virtuales**.

ii. A la derecha, **agregue** un nuevo servidor virtual de NetScaler Gateway o **modifique** un servidor virtual de NetScaler Gateway existente.

iii. Si está editando un servidor virtual de NetScaler Gateway existente, en la sección **Configuración básica**, haga clic en el icono de lápiz.

iv. Para agregar y modificar, en la sección **Configuración básica**, haga clic en **Más**.

v. Utilice el menú **Perfil de vServer de PCoIP** para seleccionar el perfil de servidor virtual PCoIP necesario.

vi. Desplácese hacia abajo y asegúrate de que solo ICA esté desactivada. A continuación, haga clic en **Aceptar** para cerrar la sección **Configuración básica**.

vii. Si va a crear un nuevo servidor virtual de NetScaler Gateway, vincule un **certificado**y vincule una directiva de autenticación LDAP.

viii. Desplácese hacia abajo hasta la sección **Directivas** y haga clic en el icono más.

ix. El valor predeterminado de la página **Elegir tipo** es **Sesión** y **Solicitud**. Haga clic en **Continuar**.

x. En la sección **Vinculación de directivas**, haga clic **en Haga clic para seleccionar**.

xi. Seleccione la directiva de sesión necesaria que tiene configurado el perfil PCoIP y haga clic en **Seleccionar**.

xii. En la página **Vinculación de directivas**, haga clic en **Vincular**.

xiii. Si quiere utilizar un explorador web para conectarse a VMware Horizon View, a la derecha, en **Configuración avanzada**, agregue la sección **Temas del portal**. Si solo utiliza Horizon View Client para conectarse a NetScaler Gateway, no debe realizar este paso.

xiv. Utilice el menú **Tema del portal** para seleccionar **RfWebUI** y haga clic en **Aceptar**.

xv. Los iconos publicados de Horizon View se agregan al portal de RfWebUI.

> **Nota:** VMware utiliza dos o más protocolos cuando utiliza cualquier protocolo que no sea RDP. Esto puede hacer que las solicitudes tengan un equilibrio de carga en dos servidores back-end diferentes. Puede resolver este problema configurando un único grupo de persistencia en todos los protocolos para garantizar que todas las conexiones permanezcan en el mismo servidor virtual Citrix.

### Pasos para habilitar la redirección USB

Se puede acceder a los dispositivos USB conectados a la máquina cliente desde los escritorios virtuales y las aplicaciones. A continuación se indican los pasos para habilitar la redirección USB:

1. Inicie sesión en la consola de administrador de VMware Horizon.
2. Vaya a **Inventario > Ver servidores de configuración**.
3. Seleccione la ficha **Servidores de conexión**.
4. Seleccione un servidor de conexión de la lista y haga clic en **Modificar**.
5. En la ficha **General**, seleccione la opción **Usar conexión de túnel seguro a máquina** en **HTTP (S) Secure Tunnel**. Proporcione la URL externa de NetScaler Gateway en el campo **URL externa**.

### Actualización de la expresión de conmutación de contenido para Unified Gateway

Si el servidor virtual de NetScaler Gateway está detrás de un servidor virtual de conmutación de contenido (Unified Gateway), debe actualizar la expresión de conmutación de contenido para incluir las rutas URL de PCoIP.

1. En la GUI de NetScaler ADC, vaya a **Configuración > Administración del tráfico > Cambio de contenido > Directivas**.
2. Agregue la siguiente expresión en el área **Expresión** y, a continuación, haga clic en **Aceptar**.

| | | | |
|---|---|---|---|
| | http.req.url.path.eq (“/broker/xml”) | http.req.url.path.contains (“/broker/resources”) | http.req.url.path.eq (“/pcoip-client”) |

### Usar puerta de enlace PCoIP

1. Para conectarse, debe tener instalado Horizon View Client en el dispositivo cliente. Una vez instalada, puede utilizar la interfaz de usuario de Horizon View Client para conectarse a NetScaler Gateway o utilizar la página del portal RfWebUI de NetScaler Gateway para ver los iconos publicados desde Horizon.
2. Para ver las conexiones PCoIP activas, vaya a **NetScaler Gateway > PCoIP.**
3. A la derecha, cambia a la ficha **Conexiones**. Las sesiones activas se muestran con los siguientes datos: nombre de usuario, IP de cliente de Horizon View e IP de destino de Horizon View Agent.
4. Para terminar una conexión, haga clic con el botón derecho en la ficha **Conexión** y, a continuación, haga clic en **Matar conexión** O haga clic en **Matar todas las conexiones** para terminar todas las conexiones PCoIP.

## Configurar el servidor de conexión de VMware Horizon View

January 26, 2024

Para admitir el proxy PCoIP a través de NetScaler Gateway:

1. Inicie sesión en la **consola de administrador de VMware Horizon**.
2. Vaya a **Inventario** —> **Ver configuración** —> **Servidores**.
3. Seleccione la ficha **Servidores de conexión**.
4. Seleccione un servidor de conexión de la lista y haga clic en **Modificar**.
5. En la ficha **General**, anule la selección de la opción **Usar conexión de túnel seguro** a máquina en HTTP(S) Secure Tunnel.
6. Haga clic en **Aceptar** para cerrar la ventana **Modificar configuración del servidor de conexión**.
7. Siga los pasos del 4 al 6 en todos los servidores de conexión de la lista.

## Soporte de transporte de datos iluminado por HDX

January 26, 2024

La compatibilidad con Enlightened Data Transport (EDT) para Citrix Gateway garantiza una experiencia de usuario de alta definición durante la sesión en escritorios virtuales para los usuarios que utilizan Citrix Receiver.

Además, se facilita el cifrado de extremo a extremo con DTLS 1.0 para la terminación de EDT entre Receiver y el VDA. Para obtener más información, consulte Compatibilidad con el protocolo DTLSv1.0 .

Citrix Gateway, compatible con EDT, ofrece una buena experiencia de usuario tanto en condiciones de LAN como de WAN, sin ninguna configuración administrativa o de usuario cuando se desvía de una a otra. El beneficio es más visible en redes de alta latencia con pérdida moderada de paquetes, donde la experiencia del usuario generalmente se retrasaría con respecto a las alternativas. Para obtener más información, consulte HDX .

## Cuándo utilizar el protocolo Enlightened Data Transport

January 26, 2024

En los siguientes casos se ilustra el uso de NetScaler Gateway habilitado para EDT.

- Un usuario quiere disfrutar de una experiencia tan buena como en un entorno LAN mientras accede de forma remota a los recursos empresariales.
- Un usuario quiere una experiencia de usuario de escritorio y aplicaciones virtuales enriquecidas en redes Wi-Fi y móviles en las que la calidad de la red es deficiente debido a la congestión, la alta pérdida de paquetes y la alta latencia.

Los siguientes puntos deben tenerse en cuenta al utilizar EDT.

- El mando DTLS en el nivel del servidor virtual está habilitado de forma predeterminada.
- No se admite IPv6 con DTLS.
- A partir de la versión 12.1, compilación 51.x, las políticas de SmartControl y las políticas ICA son compatibles con las conexiones DTLS/EDT.
- El dispositivo ahora se puede configurar para la funcionalidad de doble salto para el tráfico de EDT entre Receiver y VDA. Para obtener más información, haga clic en Implementación en una DMZ de doble salto.

> **Nota:** EDT es compatible con la plataforma MPX FIPS en la versión 12.1, compilación 49.xx y versiones posteriores. En los dispositivos MPX basados en el chip SSL Intel Coleto, EDT es compatible con la versión 12.1 versión 51.16 y versiones posteriores.

## Configurar NetScaler Gateway para que admita Enlightened Data Transport y HDX Insight

March 27, 2024

El tráfico de EDT a través de Gateway ahora tiene visibilidad de extremo a extremo. La disponibilidad de datos de visibilidad histórica y en tiempo real permite a NetScaler ADM admitir una amplia variedad de casos de uso.

Se admiten los siguientes casos:

| Escenario | Compatibilidad con EDT |
|---|---|
| Citrix Gateway | Sí |
| NetScaler Gateway con alta disponibilidad (HA) | Sí |
| Optimización de NetScaler Gateway con alta disponibilidad (HA) | Sí |

| Escenario | Compatibilidad con EDT |
|---|---|
| NetScaler ADC con Unified Gateway | Sí |
| NetScaler Gateway con GSLB | Sí |
| NetScaler Gateway con clúster | Sí |
| Cifrado DTLS de Citrix Receiver a Citrix Gateway | Sí |
| Secure Ticket Authority dobles (STA) en NetScaler Gateway | Sí |
| Tiempo de espera de sesión ICA de NetScaler Gateway | Sí |
| ICA multisecuencia de NetScaler Gateway | No |
| Fiabilidad de la sesión de NetScaler Gateway (puerto 2598) | Sí |
| Doble salto de NetScaler Gateway | Sí |
| Cifrado DTLS de NetScaler ADC a VDA | Sí |
| HDX Insight | Sí |
| NetScaler Gateway en modo IPv6 | No |
| SOCKS de NetScaler Gateway (puerto 1494) | No |
| Proxy LAN puro Citrix ADC (consulte la nota) | No |

> **Nota:**
>
> EDT no se admite si el proxy LAN Citrix ADC está configurado en el modo de usuario de LAN o en el modo transparente. Sin embargo, se admite TCP. Para obtener más información, consulte:
>
> - Configuración del proxy ICA saliente
> - Recopilación de HDX Insight Analytics para usuarios de LAN con Citrix ADC mediante SOCKS

### Configurar NetScaler Gateway para admitir el Enlightened Data Transport

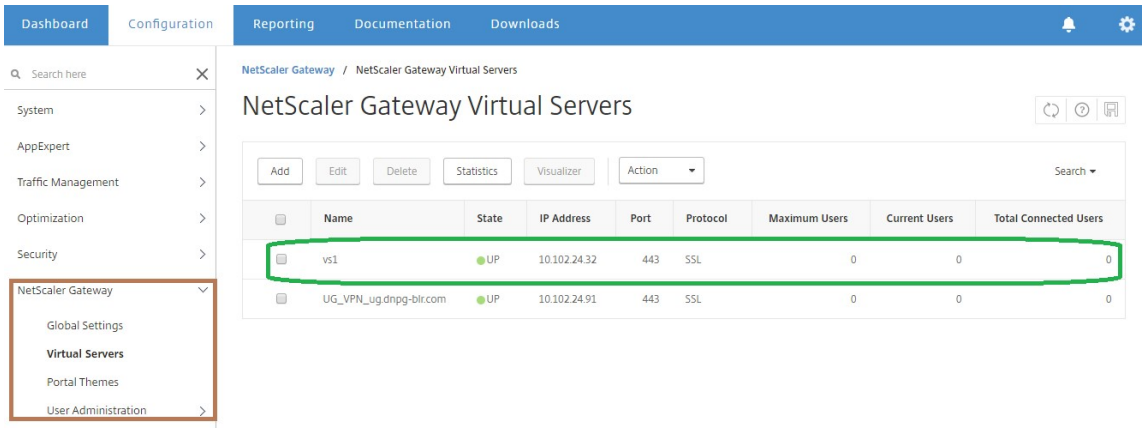
Si utiliza el Enlightened Data Transport (EDT), la Transport Layer Security de datagramas (DTLS) debe estar habilitada para cifrar la conexión UDP utilizada por EDT. El parámetro DTLS debe estar habilitado en el nivel del servidor virtual de VPN de Gateway y los componentes de Citrix Virtual Apps and Desktops deben actualizarse y configurarse correctamente para lograr un tráfico cifrado entre el servidor virtual de VPN de Gateway y el dispositivo de usuario.

> **Nota:**El puerto UDP (por ejemplo, el puerto 443) configurado para el servidor virtual frontend de Citrix Gateway debe abrirse en la DMZ para que el servidor virtual reciba las conexiones DTLS. DTLS y CGP son requisitos previos para que EDT funcione con Citrix Gateway.

**Para configurar NetScaler Gateway para que admita EDT mediante GUI**

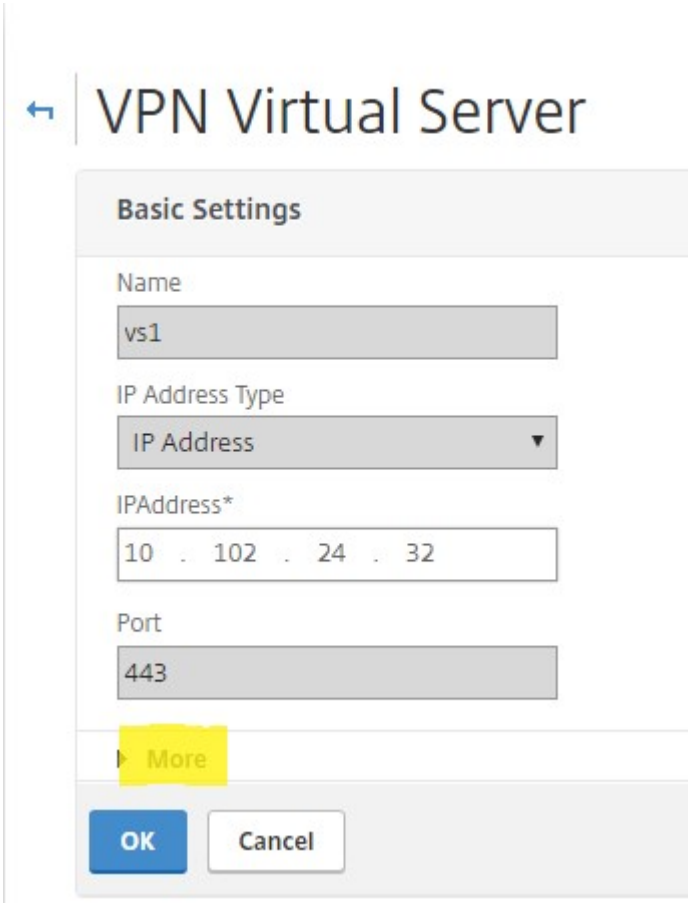
1. Implemente y configure NetScaler Gateway para comunicarse con StoreFront y autenticar a los usuarios de Citrix Virtual Apps and Desktops.
2. En la ficha Configuración de la GUI de NetScaler ADC, expanda **NetScaler Gateway** y seleccione **Servidores virtuales**.




3. Haga clic en **Modificar** para mostrar la configuración básica del servidor virtual de VPN y, a continuación, compruebe el estado de la configuración DTLS.


4. Haga clic en **Más** para mostrar la opción de configuración adicional.



5. Seleccione **DTLS** para proporcionar seguridad en las comunicaciones de los protocolos de datagramas. Haga clic en **Aceptar**. El área **Configuración básica** del servidor virtual de VPN muestra que el indicador DTLS está establecido en **True**.


**Para configurar la compatibilidad con NetScaler Gateway para EDT mediante CLI**

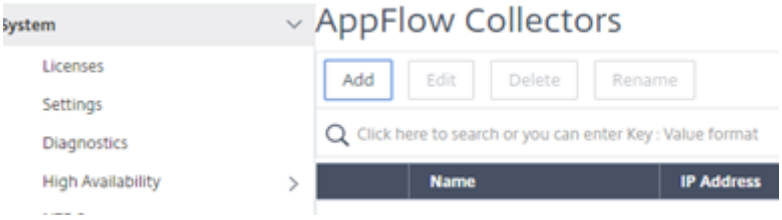
```
set vpn vserver vs1 -DTLS ON
```

## Configurar NetScaler Gateway para admitir HDX Insight

HDX Insight proporciona visibilidad integral del tráfico HDX a las aplicaciones y escritorios virtuales que pasan por NetScaler ADC. También permite a los administradores ver métricas de latencia de red y clientes en tiempo real, informes históricos, datos de rendimiento de extremo a extremo y solucionar problemas de rendimiento.

**Para configurar NetScaler Gateway para que admita HDX Insight mediante la interfaz gráfica de usuario**

1. En la ficha **Configuración**, vaya a **Sistema> AppFlow>Collectors** y haga clic en **Agregar**.




2. En la página **Crear recopilador de AppFlow**, rellene los campos siguientes y haga clic en Crear.
   Nombre: nombre del coleccionista

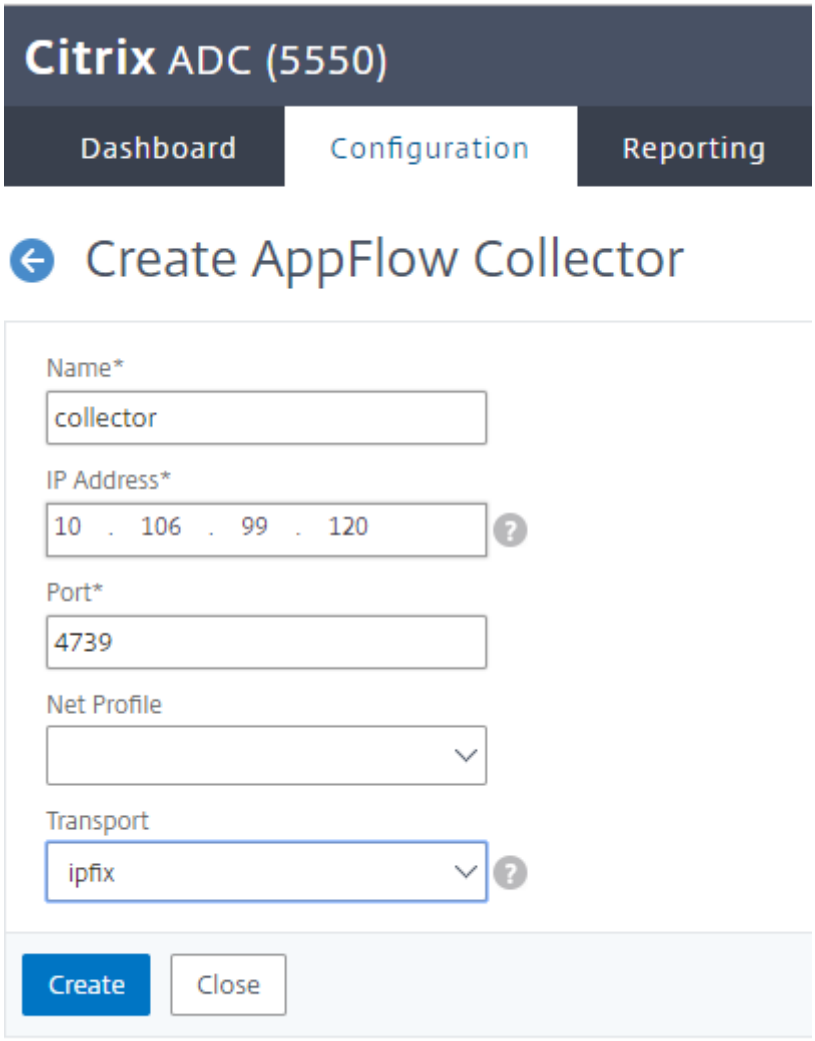
   Dirección IP: dirección IPv4 del recopilador

   Puerto: puerto en el que escucha el recopilador

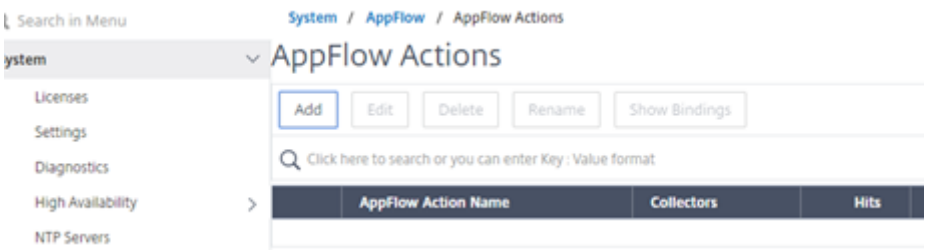
 

Perfil de red: perfil de red para asociar con el recopilador. La dirección IP definida en el perfil se utiliza como dirección IP de origen para el tráfico de AppFlow de este recopilador. Si no establece este parámetro, la dirección IP de NetScaler ADC (NSIP) se utiliza como dirección IP de origen.

Transporte: tipo de colector de transporte.




3. Vaya a **Sistema > AppFlow> Acciones**y haga clic en **Agregar**.




4. En la página **Crear acción de AppFlow**, rellene los campos siguientes y haga clic en **Crear**.

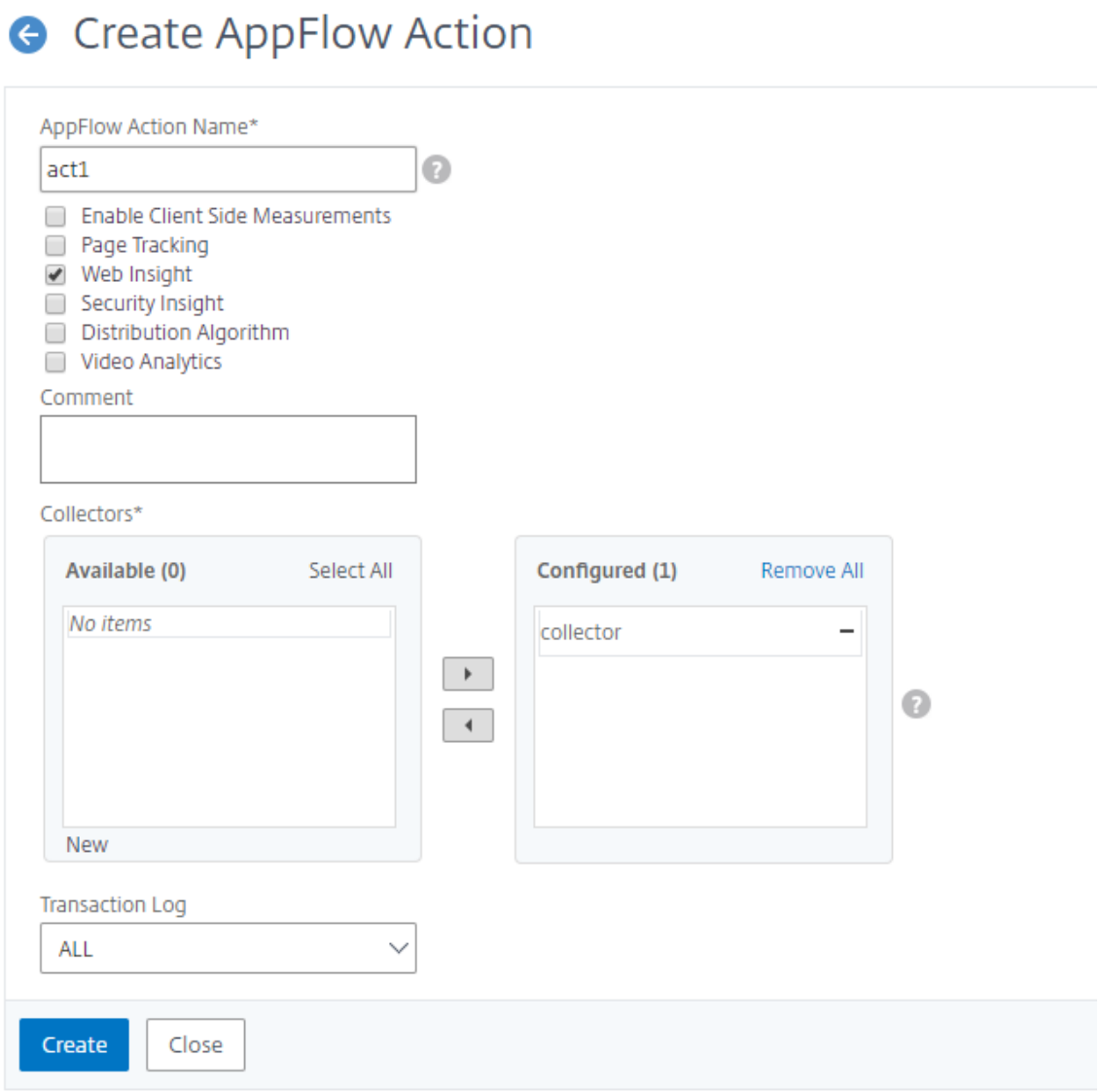
 

Nombre de acción de AppFlow: nombre de la acción

Comentario: cualquier comentario sobre la acción

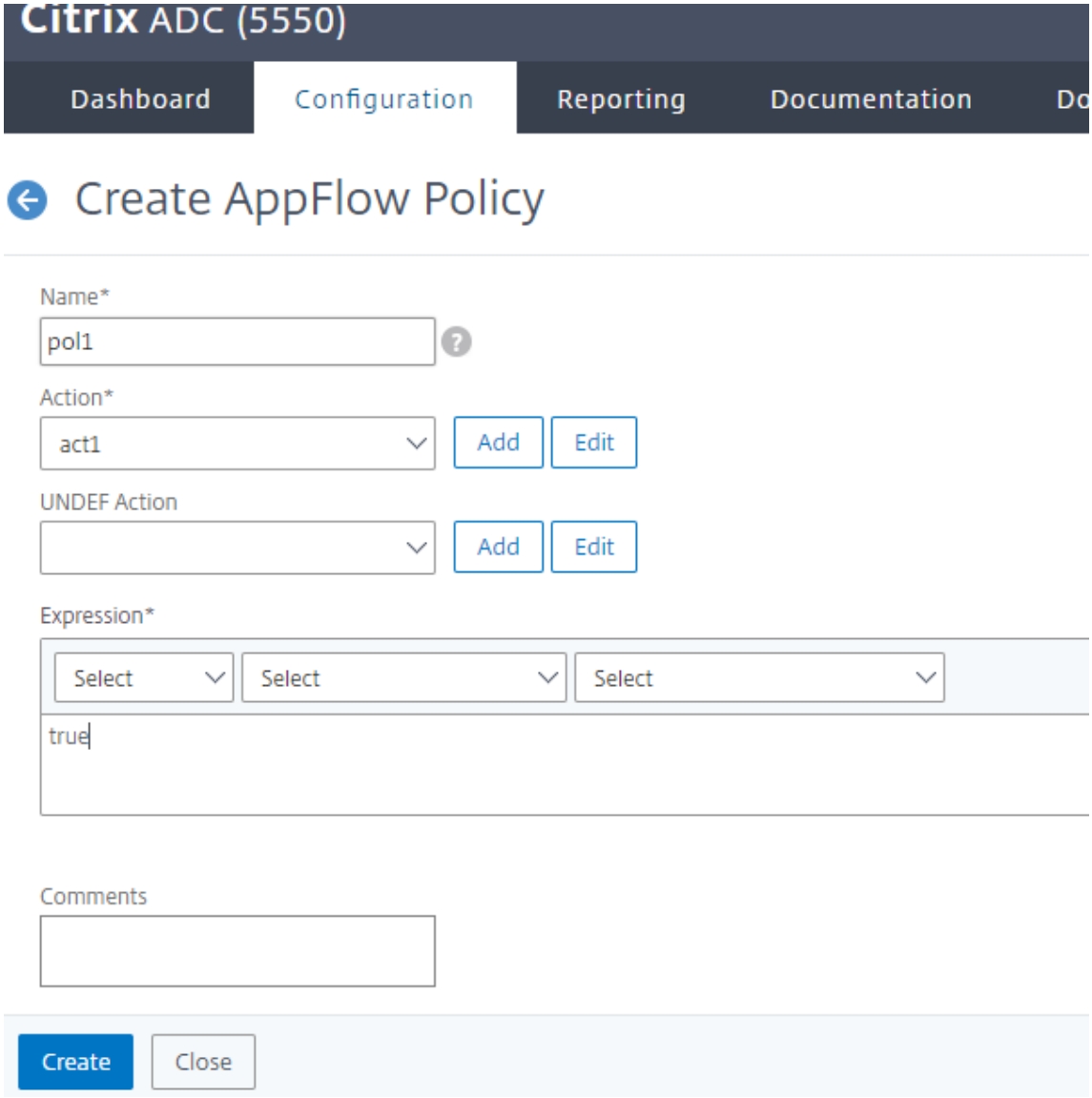
Recopilador: seleccione los nombres de los recopiladores que se asociarán a la acción de AppFlow.

Registro de transacciones: tipo de transacciones que se van a registrar.




5. Vaya a **Sistema> AppFlow>Directivas**y haga clic en **Agregar**.




6. En la página **Crear política de AppFlow** , complete los siguientes campos y haga clic en **Crear**.

   Nombre: nombre de la directiva.

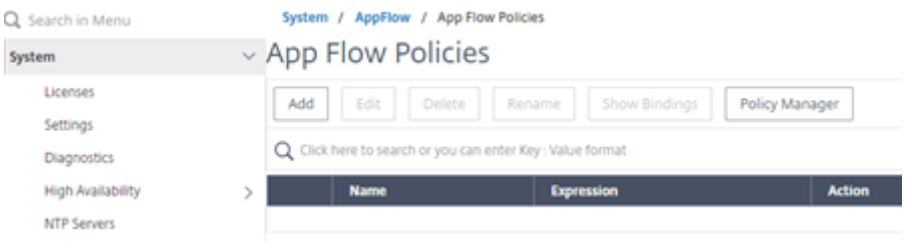
   Acción: nombre de la acción que se va a asociar a la directiva.

   UNDEF: nombre de la acción de flujo de aplicaciones que se asociará a esta política cuando se produzca un evento indefinido.

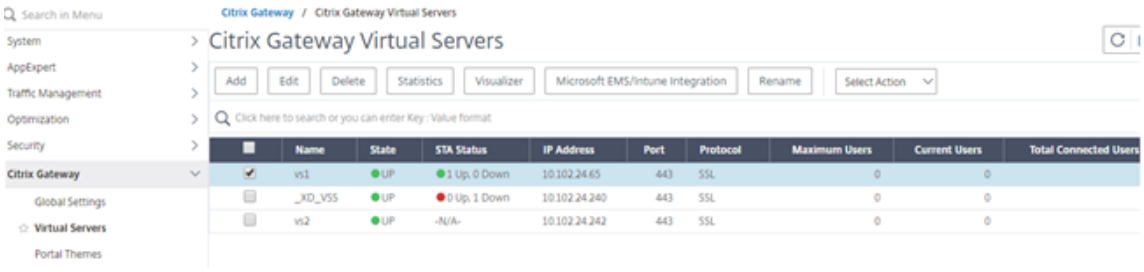
   Expresión: expresión u otro valor con el que se evalúa el tráfico. Debe ser una expresión booleana.

   Comentarios: cualquier comentario sobre esta directiva.

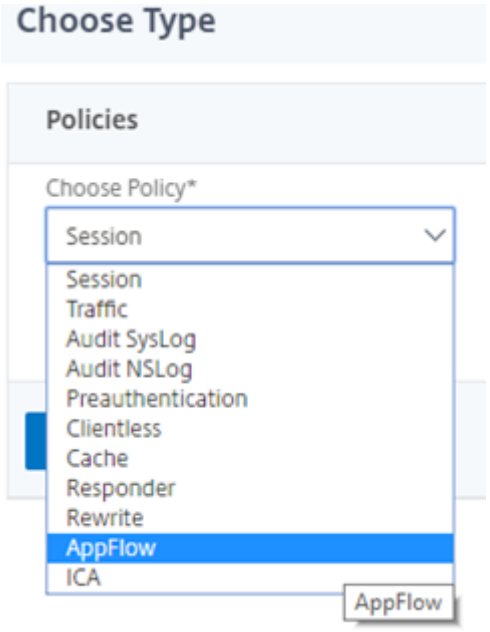



7. Vaya a **NetScaler Gateway>Servidores virtuales**, seleccione el servidor virtual y haga clic en **Modificar**.



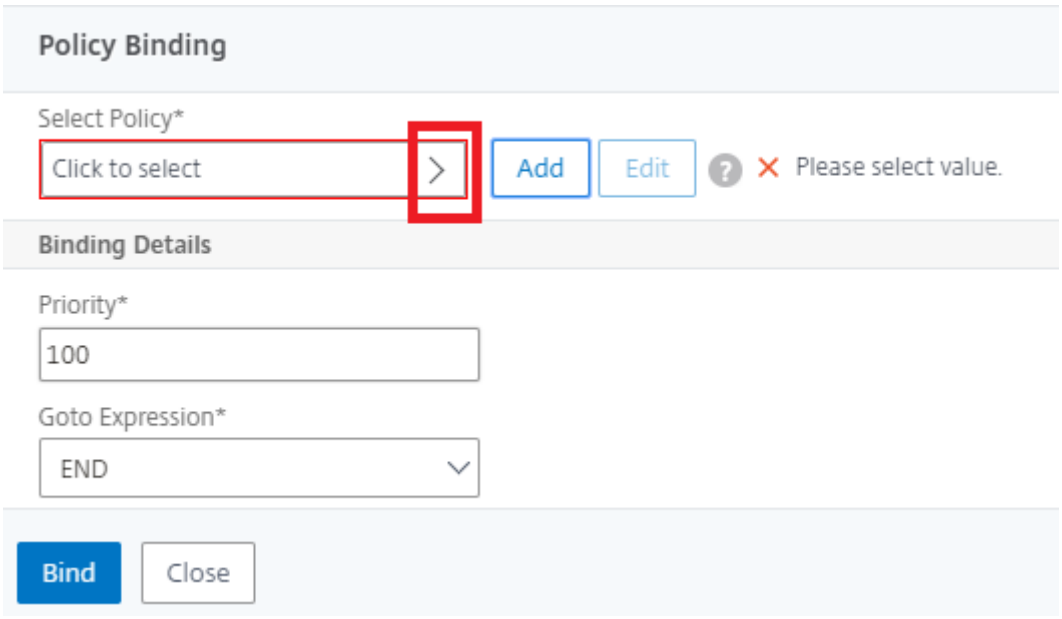

8. Desplácese hacia abajo en la página **Servidor Virtual VPN** y, en la sección **Directivas**, haga clic en **+**.


9. En la pantalla **Elegir tipo**, en el menú desplegable **Elegir directiva**, seleccione **AppFlow**. En el menú desplegable **Elegir tipo**, elija **Solicitud o SolicitudICA**y haga clic en**Continuar**.

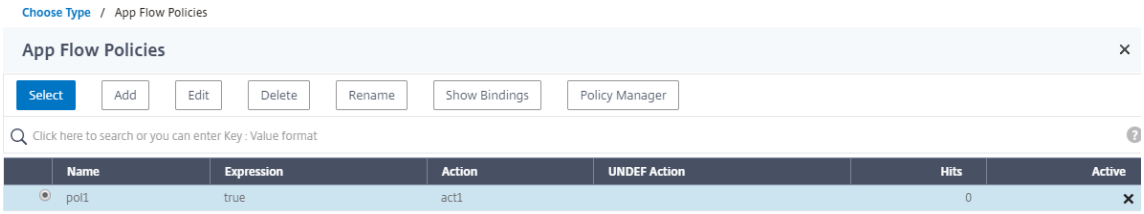


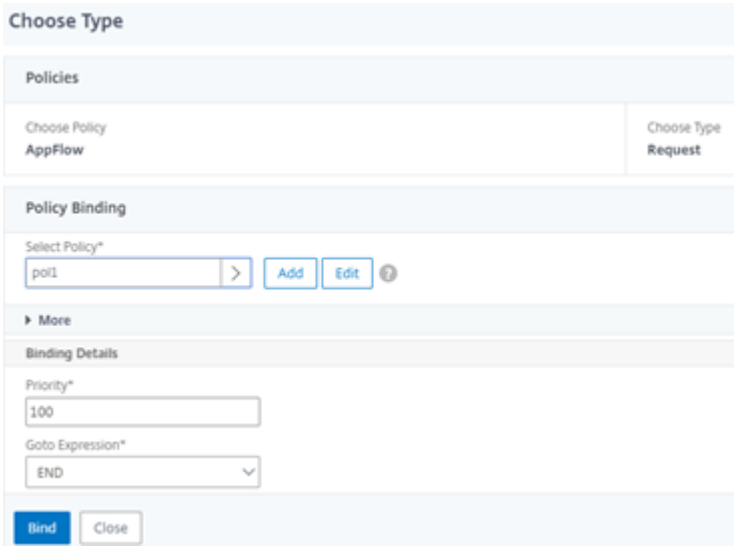
10. Haga clic en la flecha resaltada en **Seleccionar directiva**.




11. Seleccione la **directiva AppFlow** y haga clic en **Seleccionar**.




12. Por último, haga clic en **Vincular**.



**Para configurar Citrix Gateway para que sea compatible con HDX Insight mediante la CLI, escriba el siguiente comando**

```
add appflow collector col3 -IPAddress<ip_mas>
add appflow action act1 <action_name>
add appflow policy <policy_name> true <action_name>
bind vpn Vserver <vserver_name>  -pol <policy_name> - priority101 END -
   type <ICA_Request>
```

## Umbral de latencia L7

March 27, 2024

La función de umbral de latencia L7 de HDX Insight detecta de forma activa los problemas de latencia de red de extremo a extremo a nivel de aplicación y toma medidas proactivas. La función de umbral de latencia L7 realiza una supervisión de latencia en tiempo real para detectar los picos y envía notificaciones a HDX Insight si la latencia supera la latencia mínima observada.

Anteriormente, los valores promedio de latencia L7 del lado del cliente y del servidor se enviaban cada 60 segundos a HDX Insight. Cualquier pico observado dentro de este intervalo se promedió y, por lo tanto, permaneció sin ser detectado. Además, no había monitorización de latencia en vivo para detectar estos picos.

### En qué se diferencia la latencia L7 de la latencia L4

Las latencias de red también se capturan y muestran en el nivel L4. Estas latencias se calculan a partir de la capa TCP y no requieren análisis del tráfico ICA. Por lo tanto, son relativamente fáciles de obtener y consumen menos CPU. Sin embargo, el principal inconveniente de la latencia L4 es comprender la latencia de extremo a extremo. Si hay proxies TCP en la ruta, la latencia L4 captura solo la latencia del NetScaler ADC al proxy TCP. Esto puede dar lugar a información incompleta y, por lo tanto, provocar dificultades para depurar el problema.

La latencia de L7 se calcula analizando el tráfico ICA. El cálculo de latencia L7 se realiza en la capa ICA y, por lo tanto, los proxies intermedios no producen valores de latencia incompletos. Por lo tanto, proporciona detección de latencia de extremo a extremo.

En las ilustraciones siguientes se muestra un tipo de implementación con y sin proxy TCP.

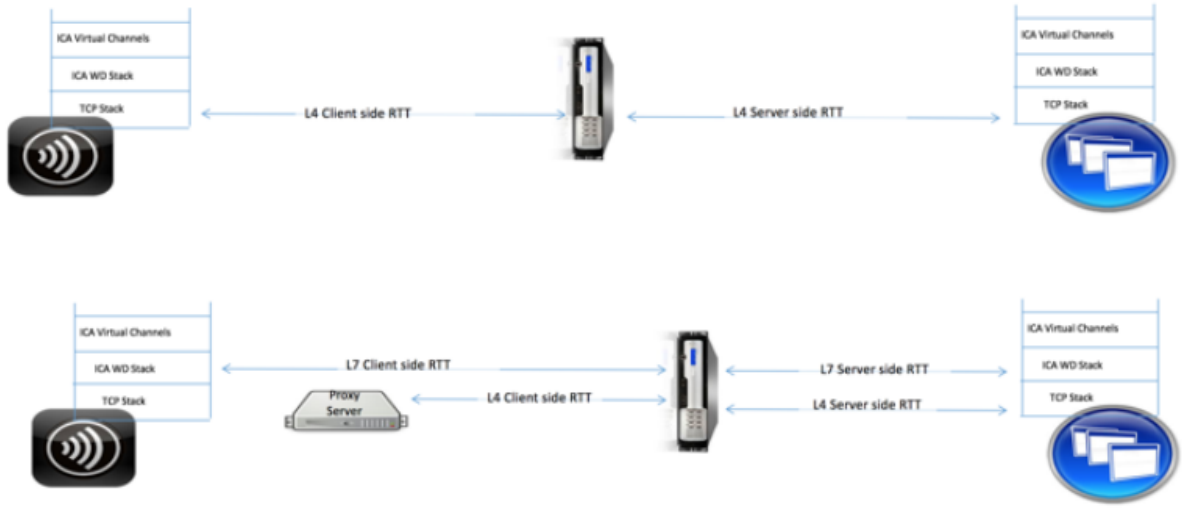



*Fig 2. Deployment with TCP Proxies*

### Diferencia entre los cálculos de latencia ICA RTT y L7

ICA RTT representa el tiempo total de ida y vuelta desde la aplicación Citrix Workspace hasta Virtual Delivery Agent (VDA). La latencia de L7 proporciona detalles detallados sobre las latencias del lado del cliente y del servidor. La latencia del cliente L7 es la latencia entre la aplicación Citrix Workspace y NetScaler Gateway. La latencia del servidor L7 es la latencia entre NetScaler Gateway y VDA.

> **Nota: El**cálculo de latencia L7 del servidor para el servidor solo se admite para las versiones 7.13 y versiones posteriores de Citrix Virtual Apps and Desktops.

### Configurar el umbral de latencia de L7 mediante la CLI

1. Agregue un perfil de latencia ICA.

```
add ica latencyprofile <name> [-l7LatencyMonitoring ( ENABLED |
    DISABLED )] [-l7LatencyThresholdFactor <positive_integer>] [-
    l7LatencyWaitTime <positive_integer>] [-l7LatencyNotifyInterval
     <positive_integer>] [-l7LatencyMaxNotifyCount <
    positive_integer>]
<!--NeedCopy-->
```

2. Agregue una acción ICA.

```
add ica action <name> [-latencyprofileName <string>]
<!--NeedCopy-->
```

3. Agregue una directiva ICA.

```
add ica policy <name> -rule <expression> -action <string> [-
    comment<string>] [-logAction <string>
<!--NeedCopy-->
```

4. Enlazar la directiva ICA al servidor VPN o al punto de enlace global ICA.

```
bind ica global -policyName <string> -priority <positive_integer>
    [-gotoPriorityExpression <expression>] [-type (
    ICA_REQ_OVERRIDE | ICA_REQ_DEFAULT )]
<!--NeedCopy-->
```

O bien

```
bind vpn vserver <name> -policy <string>  [-priority <
    positive_integer>]
<!--NeedCopy-->
```

O bien

```
bind cr vserver <name> -policy <string> [-priority <positive
    _integer>]
<!--NeedCopy-->
```

**Argumentos**

- **Monitorización de latencia**: Parámetro para habilitar o inhabilitar la supervisión de umbral L7. Cuando este parámetro está habilitado, las notificaciones se envían a HDX Insight cuando se cumplen las condiciones establecidas.

  Valor predeterminado: DESACTIVADO

- **latencyThresholdFactor**: Factor por el cual la latencia activa debe ser mayor que la latencia mínima observada para concluir que se ha superado el umbral y, por lo tanto, debe enviarse una notificación a HDX Insight.

  Valor predeterminado: 4

  Valor mínimo: 2

  Valor máximo: 65535

- **latencyWaitTime**: Tiempo en segundos para que el dispositivo espere una vez superado el umbral de latencia para enviar una notificación a HDX Insight.

  Valor por defecto: 20

  Valor mínimo: 1

  Valor máximo: 65535

- **latencyNotifyInterval**: Intervalo de tiempo en segundos para que el dispositivo envíe notificaciones posteriores a HDX Insight una vez transcurrido el tiempo de espera.

  Valor por defecto: 20

  Valor mínimo: 1

  Valor máximo: 65535

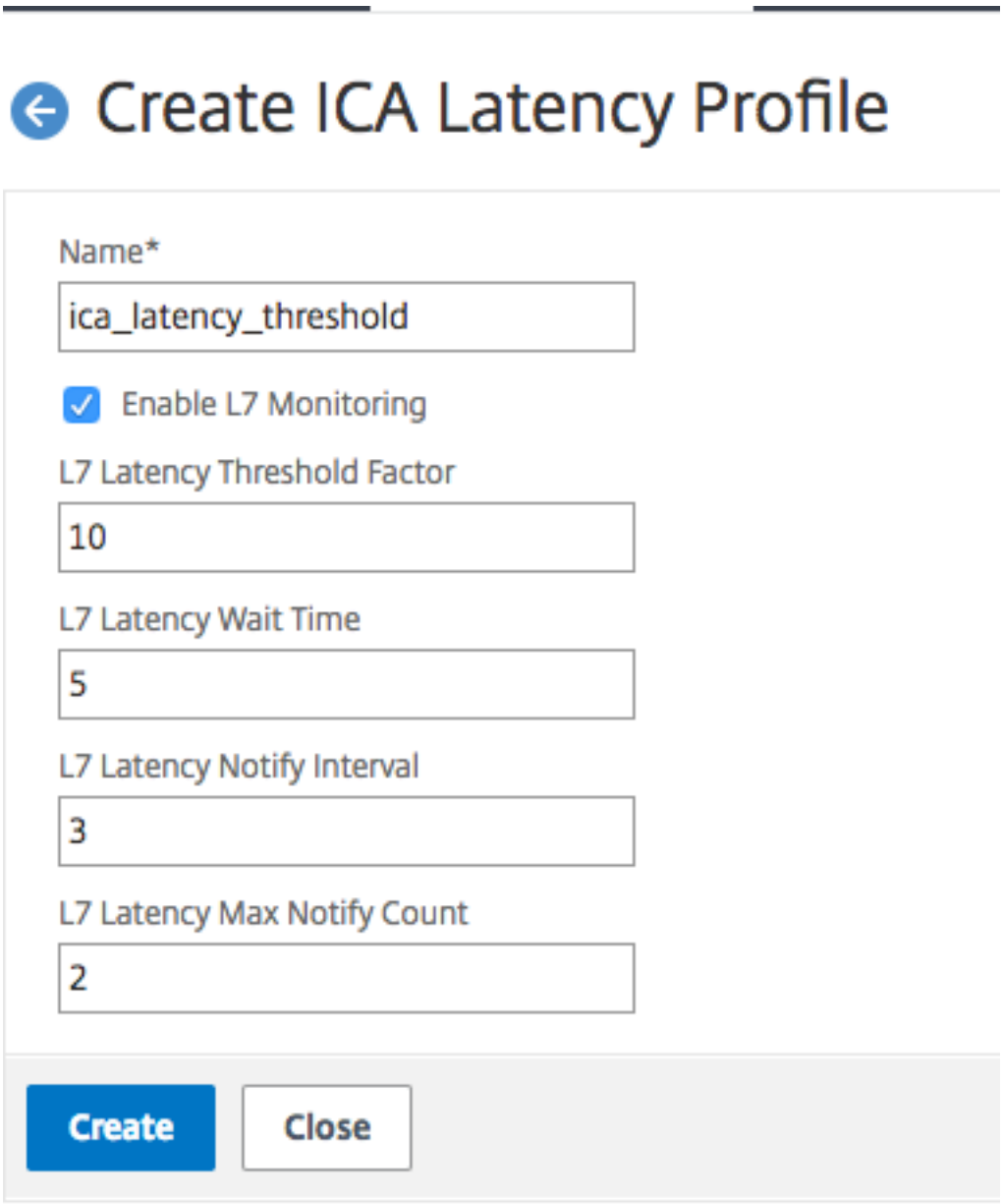
- **LatencyMaxNotifyCount**: Número máximo de notificaciones que se pueden enviar a HDX Insight dentro de un intervalo en el que la latencia está por encima del umbral.

  Valor predeterminado: 5

### Configurar el umbral de latencia de L7 mediante la GUI

1. Vaya a **Configuración** > **NetScaler Gateway** > **Directivas** > **ICA**.
2. Seleccione la ficha **Perfiles de latencia ICA** y haga clic en **Agregar**.
3. En la página **Crear Perfil de Latencia ICA**, realice lo siguiente.




- Seleccione Supervisión de **latencia de L7 para habilitar la supervisión** del umbral de nivel 7.
- En **Factor de umbral L7**, introduzca el valor en el que la latencia activa debe superar la latencia mínima observada para enviar notificaciones a HDX Insight.
- En **Tiempo de espera de latencia de L7**, introduzca el tiempo en segundos que debe esperar el dispositivo después de superar el umbral para enviar una notificación a HDX Insight.
- En **Intervalo de notificación de latencia de nivel 7**, introduzca el tiempo en segundos para que el dispositivo envíe notificaciones posteriores a HDX Insight una vez transcurrido el tiempo de espera.

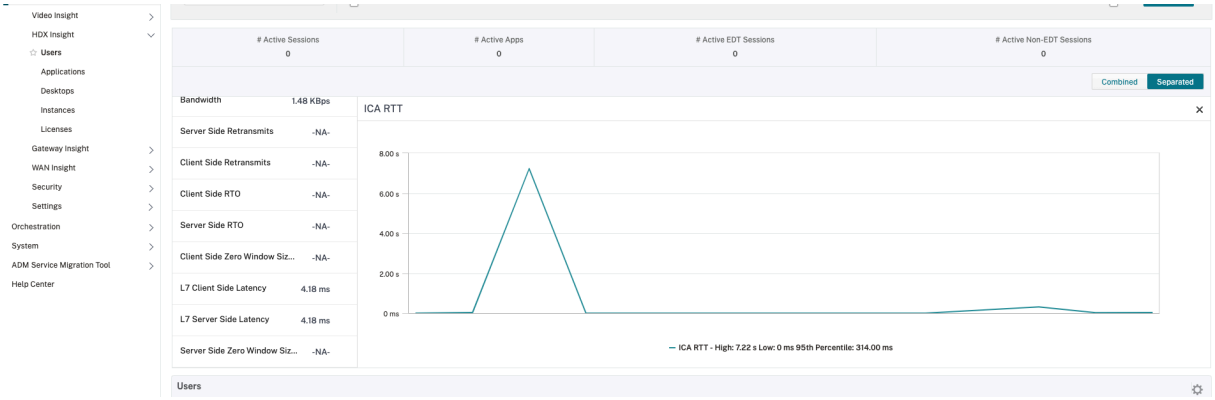
- En **Recuento máximo de notificaciones de latencia de nivel 7**, introduzca el número máximo de notificaciones que se pueden enviar a HDX Insight en un intervalo en el que la latencia esté por encima del umbral.
  **Nota:** El recuento máximo de notificaciones de latencia L7 se aplica una vez que se supera el umbral y se restablece cuando la latencia activa cae por debajo del umbral. La periodicidad de estas notificaciones se rige por el intervalo de notificación.

4. Haga clic en **Crear**.

> **Importante:**
>
> Después de configurar los parámetros del umbral de latencia de L7, debe configurar HDX Insight. Para obtener más información, consulte Configurar NetScaler Gateway para que sea compatible con HDX Insight.

#### Ver parámetros de latencia de nivel 7 en NetScaler ADM

Para ver los parámetros de latencia de L7 en NetScaler ADM, vaya a **Analytics > HDX Insight > Aplicaciones** o **análisis > HDX Insight > Usuarios**.




## Parámetro para especificar un intervalo de tiempo para el cálculo del valor de latencia del cliente L7

A partir de la versión 12.1, compilación 63.20 de Citrix ADC y posteriores, puede especificar un intervalo de tiempo, en segundos, para el que se calculará el valor de latencia del cliente L7. Esta configuración es necesaria si ha habilitado la latencia L7 y la latencia ICA de una sesión se graba incorrectamente como 64 000 ms.

#### Para establecer la frecuencia de latencia mediante la CLI

En la línea de comandos, escriba;

```
set ica parameter -L7LatencyFrequency <positive_integer>
<!--NeedCopy-->
```

Ejemplo:

```
set ica parameter -L7LatencyFrequency 5
<!--NeedCopy-->
```

Para ver la frecuencia de latencia L7, en la línea de comando, escriba;

```
show ica parameter
<!--NeedCopy-->
```

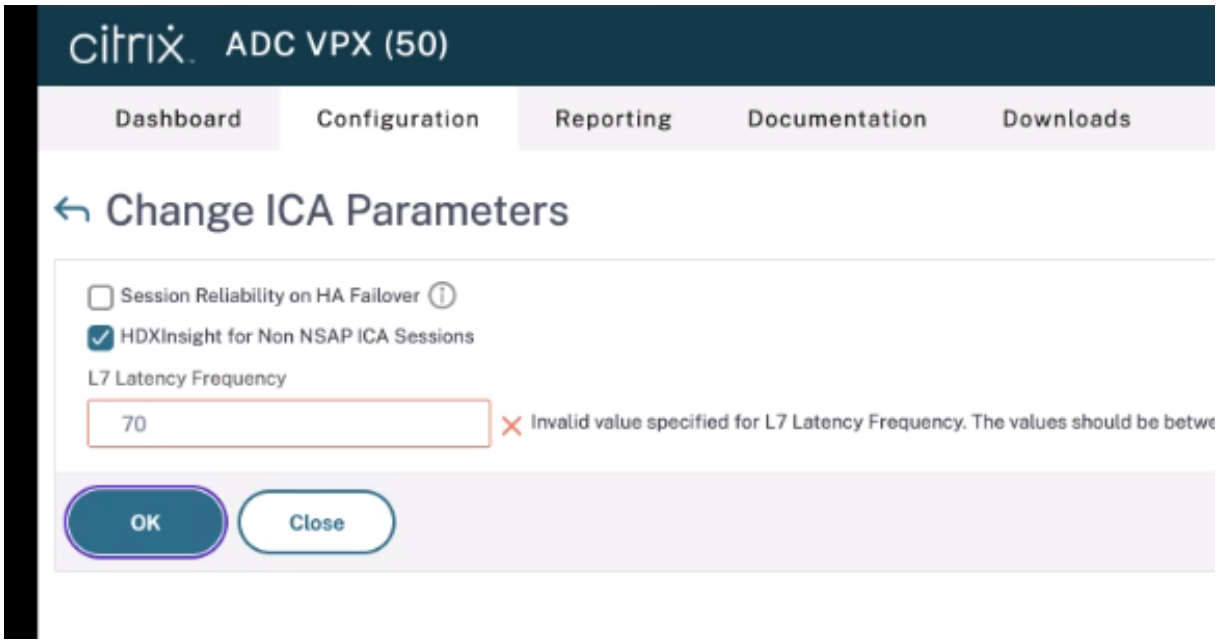
Para desactivar o desactivar la frecuencia de latencia L7, en la línea de comandos, escriba:

```
unset ica parameter -L7LatencyFrequency
<!--NeedCopy-->
```

**Nota:**De forma predeterminada, la latencia del cliente L7 se calcula para cada paquete. El valor predeterminado del `L7LatencyFrequency`parámetro es 0, el valor mínimo 0 y el valor máximo es 60.

#### Para establecer la frecuencia de latencia mediante la CLI

1. Vaya a **Sistema > Configuración > Cambiar parámetros ICA**.
2. En **Frecuencia de latencia L7** , introduzca el intervalo de tiempo para el que se calculará el valor de latencia del cliente L7.

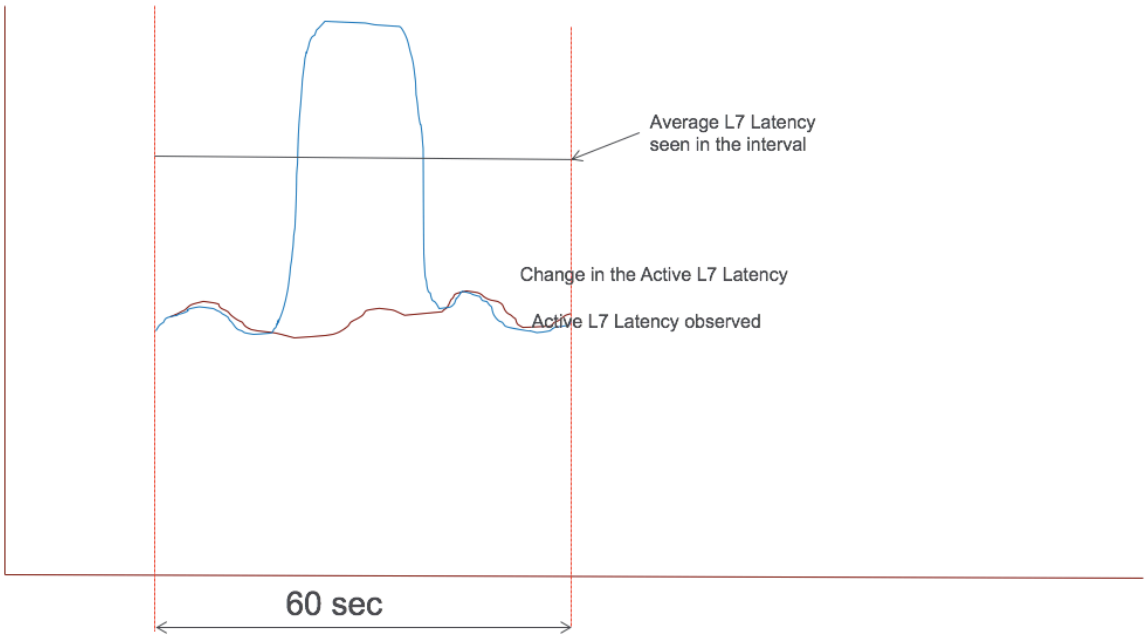


### Modelo de medición de latencia L7

En el módulo de medición de latencia L7, los valores medios de latencia L7 del lado del cliente y del servidor se envían a HDX Insight cada 60 segundos. Como resultado, los picos observados dentro de este intervalo se promedian y, por lo tanto, no se detectan. Además, el módulo de medición de latencia L7 no tiene la capacidad de supervisión de latencia en vivo.

En la siguiente ilustración se ilustra un modelo de medición de latencia L7 de muestra.



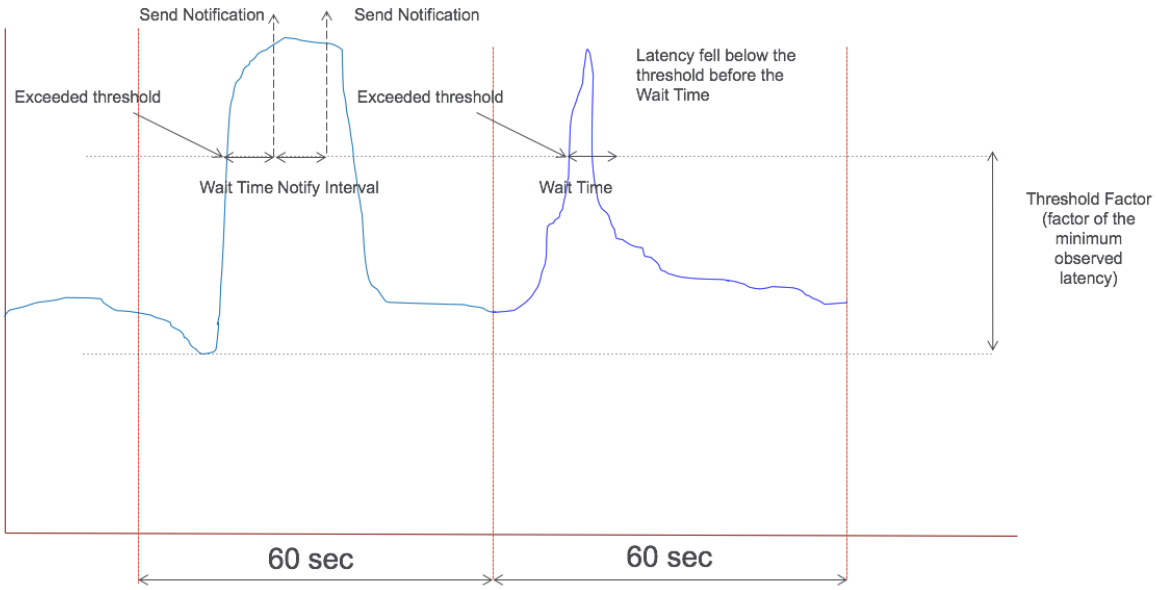

### Modelo de informes de umbral de latencia de nivel 7

El modelo de informes de umbral de latencia L7 tiene la capacidad de monitorización de latencia en tiempo real para detectar picos. Las notificaciones se envían a HDX Insight si la latencia supera la latencia mínima observada.

Siempre que se supera un factor umbral, se detecta un aumento de la latencia. Una vez que expira el tiempo de espera del umbral configurado, se envía una notificación a HDX Insight. Se envía una notificación posterior a HDX Insight después de que haya expirado el tiempo de espera y se supere el factor umbral.
En caso de que el valor de latencia caiga por debajo del factor umbral antes de que expire el tiempo de espera, no se envía ninguna notificación a HDX Insight.

En la siguiente ilustración se ilustra un modelo de informe de umbral de latencia de nivel 7 de muestra.




Los siguientes parámetros se pueden configurar en tiempo de ejecución:

- Supervisión de umbrales (ACTIVAR/DESACTIVAR)
- Factor umbral
- Tiempo de espera umbral
- Intervalo de notificación
- Recuento máximo de notificaciones

## Integración de Microsoft Intune

January 26, 2024

La integración de Microsoft Intune con NetScaler Gateway proporciona la mejor solución de protección de datos y acceso a aplicaciones de su clase ofrecida por NetScaler Gateway e Intune.

Obtienes el conjunto más completo de aplicaciones de productividad seguras, como correo electrónico, calendario, contactos, toma de notas, modificación de documentos y acceso remoto, todo lo cual se puede administrar de forma centralizada en diferentes plataformas. La integración de Intune y Citrix Gateway proporciona funcionalidades de administración de dispositivos móviles (MDM) de primera clase, mientras que la tecnología del lado del cliente de Citrix Gateway permite a estas aplicaciones avanzadas de Intune acceder a los datos y aplicaciones corporativos de forma segura a través de Citrix Gateway.

La integración permite a NetScaler Gateway extraer datos de cumplimiento de Intune, lo que permite directivas de acceso condicional. Las directivas de acceso condicional proporcionan a NetScaler

Gateway un control más preciso sobre la regulación del acceso en función de las funcionalidades del dispositivo, etc. Por ejemplo, un administrador puede crear una directiva en la que solo se conceda acceso a los dispositivos con "Cámara"inhabilitada.

NetScaler Gateway admite la autenticación de tokens de Azure Active Directory Libraries (ADAL) una vez configurado el servidor virtual de NetScaler Gateway. Tras la configuración, una aplicación móvil empaquetada con el paquete o SDK exclusivo para red de Citrix accede a Citrix Gateway mediante un token ADAL que la aplicación puede obtener directamente de AAD.

## Cuándo utilizar la solución MDM integrada de Intune

January 26, 2024

Los siguientes casos ilustran el uso de la solución MDM de Intune integrada:

- Un nuevo cliente decide incorporar Intune con la implementación local de NetScaler Gateway
- Un usuario existente de NetScaler Gateway quiere agregar la administración de dispositivos móviles con Intune
- Un usuario actual de Intune quiere permitir que los dispositivos móviles y las aplicaciones accedan a los datos ubicados dentro de una red empresarial con un dispositivo virtual o físico de Citrix Gateway en la DMZ de la empresa.

> **Nota**
>
> Solo se admiten clientes iOS y Android.

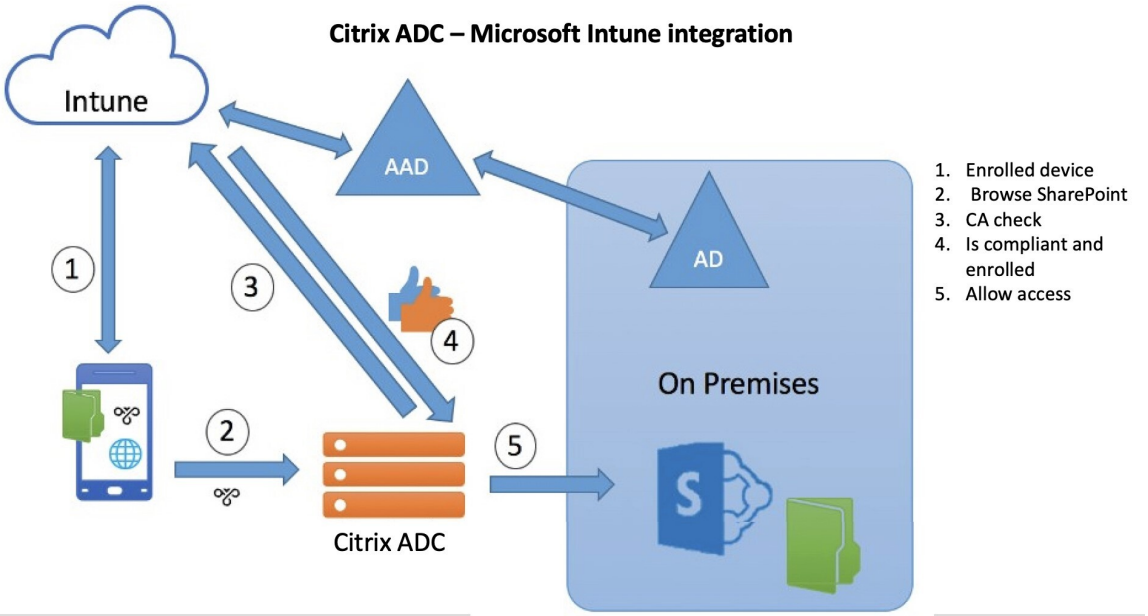
## Descripción de la integración de MDM en NetScaler Gateway-Intune

January 26, 2024

A continuación se muestra un ejemplo del flujo de eventos en una integración MDM típica de Citrix Gateway-Intune:

1. Inscribir un dispositivo móvil en Intune.
2. Las aplicaciones y políticas de dispositivo aprobadas por la empresa se envían al dispositivo.
3. Explore SharePoint (aplicación local) desde el dispositivo.
4. La solicitud del explorador va a NetScaler Gateway.
5. El dispositivo Citrix Gateway comprueba con Intune el estado de inscripción del dispositivo.
6. Si un dispositivo compatible se inscribe correctamente, se concede el acceso a SharePoint.




Cuando el dispositivo no cumple con una directiva de acceso condicional (CA), el cliente VPN de Citrix Gateway muestra un mensaje de error al usuario con un enlace a una página alojada en Intune para inscribir o corregir el estado de cumplimiento del dispositivo.

**Nota:**Los administradores deben asegurarse de lo siguiente al enviar los certificados a Intune para que los usuarios puedan diferenciar entre los distintos certificados de su dispositivo.

- Los certificados deben tener un resumen de asignaturas.
- Los resúmenes temáticas de los distintos certificados deben ser distintos.

## Configurar la comprobación del dispositivo de control de acceso a la red para el servidor virtual Citrix Gateway para la implementación de la autenticación de un solo factor

March 27, 2024

En este tema se proporciona información sobre cómo configurar NetScaler Gateway para conectarse a una red interna desde un dispositivo móvil (iOS y Android) con la seguridad de conformidad de acceso a la red (NAC) que ofrece Microsoft Intune. Cuando un usuario intenta conectarse a NetScaler Gateway desde un cliente VPN para iOS o Android, la puerta de enlace comprueba primero con el servicio Intune si el dispositivo es un dispositivo administrado y que cumple los requisitos.

- Administrado: El dispositivo se inscribe mediante el cliente del portal de empresa de Intune.
- Cumple con los requisitos: se aplican las directivas necesarias enviadas desde el servidor MDM de Intune.

Solo si el dispositivo está administrado y es compatible, se establece la sesión VPN y se proporciona acceso al usuario a los recursos internos.

> **Nota:**
>
> - En esta configuración, NetScaler Gateway en el back-end habla con el servicio Intune. Los perfiles SSL gestionan las conexiones entrantes a NetScaler Gateway. La comunicación back-end de NetScaler Gateway gestiona todos los requisitos de SNI de los servicios en la nube de back-end (Intune).
> - La comprobación de NAC de Intune, para la VPN por aplicación o incluso para la VPN de todo el dispositivo, solo se admite cuando el portal de administración de Intune aprovisiona el perfil de VPN (ahora conocido como Microsoft Endpoint Manager). Estas funciones no son compatibles con los perfiles VPN agregados por el usuario final. El administrador de Intune debe implementar el perfil VPN en su dispositivo desde Microsoft Endpoint Manager para utilizar la comprobación de NAC en el dispositivo del usuario final.

### Licencias

Se requiere una licencia de Citrix Enterprise Edition para esta funcionalidad.

### Requisitos del sistema

- NetScaler Gateway versión 11.1 compilación 51.21 o posterior
- VPN para iOS: 10.6 o posterior
- VPN para Android: 2.0.13 o posterior
- Microsoft
  - Acceso a Azure AD (con privilegios de arrendatario y administrador)
  - Tenant habilitado para Intune
- Firewall:
  Habilite reglas de firewall para todo el tráfico DNS y SSL desde la dirección IP de subred a `https://login.microsoftonline.com` y `https://graph.windows.net` (puerto 53 y puerto 443)

### Requisitos previos

- Todas las directivas de autenticación existentes deben convertirse de directivas clásicas a directivas avanzadas. Para obtener información sobre cómo convertir de directivas clásicas a directivas avanzadas, consulte https://support.citrix.com/article/CTX131024.

- Cree una aplicación NetScaler Gateway en el portal de Azure. Para obtener más información, consulte Configuración de una aplicación NetScaler Gateway en el portal de Azure.
- Configure la directiva OAuth en la aplicación NetScaler Gateway que creó mediante la siguiente información específica de la aplicación.
  - ID de cliente/ ID de aplicación
  - Secreto de cliente/clave de aplicación
  - ID de arrendatario Azure

### Referencias

- Este documento captura la configuración de configuración de NetScaler Gateway. La mayor parte de la configuración del cliente de Citrix SSO (iOS/Android) se realiza en el lado de Intune. Para obtener más información sobre la configuración de VPN de Intune para NAC, consulte https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate.
- Para configurar el perfil VPN de una aplicación iOS, consulte https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-ios.
- Para configurar la aplicación NetScaler Gateway en el portal de Azure, consulte Configuración de una aplicación NetScaler Gateway en el portal de Azure.

### Para agregar un servidor virtual Citrix Gateway con nFactor para la implementación de Gateway

1. Navegue hasta los servidores virtuales en el nodo del árbol de Citrix Gateway.
2. Proporcione la información necesaria en el área **Configuración básica** y haga clic en **Aceptar**.
3. Seleccione **Certificado de servidor**.
4. Seleccione el certificado de servidor necesario y haga clic en **Vincular**.
5. Haga clic en **Continuar**.
6. Haga clic en **Continuar**.
7. Haga clic en **Continuar**.
8. Haga clic en el icono del signo más **[+]** junto a **Directivas** y seleccione **Sesión** en la lista **Elegir directiva**, seleccione **Solicitud** en la lista **Elegir tipo** y haga clic en **Continuar**.
9. Haga clic en el icono del signo más **[+]** junto a **Seleccionar directiva**.
10. En la página **Crear directiva de sesión de NetScaler Gateway**, proporcione un nombre para la directiva de sesión.

11. Haga clic en el icono más [+] junto a **Perfil** y, en la página **Crear perfil de sesión de NetScaler Gateway**, proporcione un nombre para el perfil de sesión.
12. En la ficha **Experiencia del cliente**, haga clic en la casilla de verificación situada junto a **Acceso sin cliente** y seleccione **Desactivado** en la lista.
13. Haga clic **en la casilla de verificación situada junto a Tipo** de complemento y seleccione Windows/macOS en la lista.
14. Haga clic en **Configuración avanzada**, seleccione la casilla de verificación situada junto a **Opciones del cliente** y establezca su valor **en**ACTIVADO.
15. En la ficha **Seguridad**, haga clic en la casilla de verificación situada junto a **Acción de autorización predeterminada** y seleccione **Permitir** en la lista.
16. En la ficha **Aplicaciones publicadas**, haga clic en la casilla de verificación situada junto a **Proxy ICA** y seleccione **DESACTIVADO** en la lista.
17. Haga clic en **Crear.**
18. Escriba **NS_TRUE** en el área **Expresión** de la página **Crear directiva de sesión de NetScaler Gateway**.
19. Haga clic en **Crear**.
20. Haga clic en **Bind**.
21. Seleccione **Perfil de autenticación** en **Configuración avanzada**.
22. Haga clic en el icono más **[+]** y proporcione un nombre para el perfil de autenticación.
23. Haga clic en el icono más **[+]** para crear un servidor virtual de autenticación.
24. Especifique el nombre y el tipo de dirección IP del servidor virtual de autenticación en el área **Configuración básica** y haga clic en **Aceptar**.El tipo de dirección IP también puede **ser No direccionable**.
25. Haga clic en **Directiva de autenticación**.
26. En la vista Vinculación de directivas, haga clic en el icono más **[+]** para crear una directiva de autenticación.
27. Seleccione **OAUTH** como **tipo de acción** y haga clic en el icono más **[+]** para crear una acción de OAuth para NAC.
28. Cree una acción de OAuth mediante **ID de cliente**, **secreto de cliente**e **ID de arrendatario**.

    **El ID**de **cliente, el secreto** del cliente y el **ID de inquilino** se generan después de configurar la aplicación NetScaler Gateway en el portal de Azure.

    Asegúrese de tener un servidor de nombres DNS adecuado configurado en el dispositivo para resolver y alcanzar `https://login.microsoftonline.com/`, `https://graph.windows.net/`y *.manage.microsoft.com.

29. Crear directiva de autenticación para **OAuth Action**.

    **Regla:**

```
http.req.header("User-Agent").contains("NAC/1.0")&& ((http.req.
    header("User-Agent").contains("iOS") &&    http.req.header("
    User-Agent").contains("NSGiOSplugin")) || (http.req.header("
    User-Agent").contains("Android") &&    http.req.header("User-
    Agent").contains("CitrixVPN")))
<!--NeedCopy-->
```

30. Haga clic en el icono con el signo más **[+]** para crear la etiqueta de política NextFactor.
31. Haga clic en el icono más **[+]** para crear un esquema de inicio de sesión.
32. Seleccione **noschema** como esquema de autenticación y haga clic en **Crear** .
33. Tras seleccionar el esquema de inicio de sesión creado, haga clic en **Continuar**.
34. En **Seleccionar directiva**, seleccione una directiva de autenticación existente para el inicio de sesión de usuario o haga clic en el icono más **+** para crear una directiva de autenticación.
    Para obtener más información sobre la creación de una política de autenticación, consulte Configurar políticas de autenticación avanzadas .
35. Haga clic en **Bind**.
36. Haga clic en **Listo**.
37. Haga clic en **Bind**.
38. Haga clic en **Continuar**.
39. Haga clic en **Listo**.
40. Haga clic en **Crear**.
41. Haga clic en **Aceptar**.
42. Haga clic en **Listo**.

### Para enlazar el esquema de inicio de sesión de autenticación al servidor virtual de autenticación para indicar que los complementos VPN deben enviar el ID de dispositivo como parte de la solicitud /cgi/login

1. Vaya a **Seguridad** > **AAA - Tráfico de aplicaciones** > **Servidores virtuales**.
2. Seleccione el servidor virtual seleccionado previamente y haga clic en **Modificar**.
3. Haga clic en **Esquemas de inicio** de sesión en **Configuración avanzada**.
4. Haga clic en **Esquemas de inicio** de sesión para enlazar.

5. Haga clic en **[>]** para seleccionar y vincular las directivas de esquema de inicio de sesión integradas existentes para la verificación del dispositivo NAC.
6. Seleccione la directiva de esquema de inicio de sesión necesaria adecuada para su implementación de autenticación y haga clic en **Seleccionar**.

   En la implementación explicada, se utiliza la autenticación de factor único (LDAP) junto con la política de acción OAuth de NAC, por lo que se ha seleccionado **lschema_single_factor_deviceid**.
7. Haga clic en **Bind**.
8. Haga clic en **Listo**.

## Solución de problemas

### Problemas generales

| Problema | La resolución |
|---|---|
| El mensaje “Agregar directiva requerida”aparece cuando abres una aplicación | Agregar directivas en la API de Microsoft Graph |
| Hay conflictos de directivas | Solo se permite una única directiva por aplicación |
| Su aplicación no se puede conectar a los recursos internos | Asegúrese de que los puertos de firewall correctos estén abiertos, corrija el ID de arrendatario, etc. |

### Problemas de NetScaler Gateway

| Problema | La resolución |
|---|---|
| Los permisos necesarios para configurar la aplicación de puerta de enlace en Azure no están disponibles. | Compruebe si dispone de una licencia adecuada de Intune. Pruebe a utilizar el portal manage.windowsazure.com para ver si se puede agregar el permiso. Contacte con la asistencia de Microsoft si el problema persiste. |

| Problema | La resolución |
| --- | --- |
| NetScaler Gateway no puede contactar con `login.microsoftonline.comandgraph.windows.net`. | Desde NS Shell, comprueba si puede acceder al siguiente sitio web de Microsoft: cURL -v -k https://login.microsoftonline.com. A continuación, compruebe si el DNS está configurado en NetScaler Gateway. Compruebe también que la configuración del firewall sea correcta (en caso de que las solicitudes DNS estén protegidas por firewall). |
| Aparece un error en ns.log después de configurar OAuthAction. | Compruebe si las licencias de Intune están habilitadas y si la aplicación Azure Gateway tiene establecidos los permisos adecuados. |
| El comando Sh OAuthAction no muestra el estado de OAuth como completo. | Consulte la configuración de DNS y los permisos configurados en la aplicación de Azure Gateway. |
| El dispositivo Android o iOS no muestra la solicitud de autenticación dual. | Compruebe si el ID de dispositivo de factor dual logonSchema está vinculado al servidor virtual de autenticación. |

**Estado y condición de error de OAuth de NetScaler Gateway**

| Estado | Condición de error |
| --- | --- |
| AADFORGRAPH | Secreto no válido, URL no resuelta, tiempo de espera de la conexión agotado |
| MDMINFO | `*manage.microsoft.com`está caído o es inalcanzable |
| GRAPH | El punto final del gráfico no está accesible |
| CERTFETCH | No se puede hablar con el token del dispositivo de punto final https://login.microsoftonline.com debido a un error de DNS. Para validar esta configuración, vaya a la solicitud de Shell y escriba cURL https://login.microsoftonline.com. Este comando debe validarse. |

**Nota:** Cuando el estado de OAuth es correcto, el estado se muestra como COMPLETE.

**Comprobación de configuración de Intune**

Asegúrese de seleccionar la casilla **Acepto** en **Configuración básica de VPN para iOS para Citrix SSO > Habilitar el control de acceso a la red (NAC)**. De lo contrario, la comprobación de NAC no funciona.

## Configuración de una aplicación NetScaler Gateway en el portal de Azure

January 26, 2024

En la siguiente sección se enumeran los pasos para configurar una aplicación NetScaler Gateway en el portal de Azure.

### Requisito previo

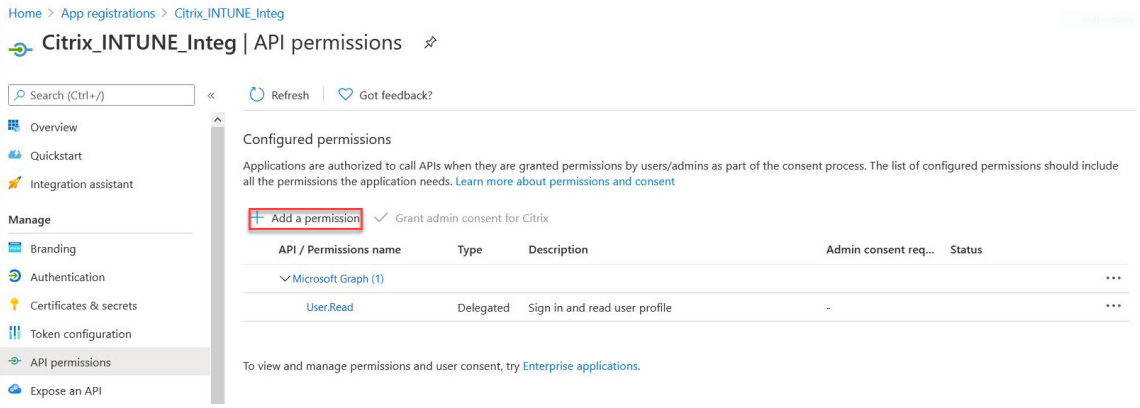
- Credenciales de administrador global de Azure
- La licencia de Intune está habilitada
- Para la integración de Intune, debe crear una aplicación Citrix Gateway en Azure Portal.
- Una vez creada la aplicación NetScaler Gateway, configure la directiva OAuth en NetScaler Gateway mediante la siguiente información específica de la aplicación:
  - ID de cliente/ ID de aplicación
  - Secreto de cliente/clave de aplicación
  - Identificador Azure arrendatario
- NetScaler Gateway utiliza el identificador de cliente de la aplicación y el secreto del cliente para comunicarse con Azure y comprobar el cumplimiento de NAC.

### Para crear la aplicación Citrix Gateway en Azure

1. Inicia sesión en portal.azure.com
2. Haga clic en **Azure Active Directory**.
3. Haga clic en **Registros de aplicaciones** y haga clic en **Nuevo registro**.
4. En la página **Registrar una aplicación**, introduzca el nombre de una aplicación y haga clic en **Registrar**.
5. Vaya a **Autenticación**, haga clic en **Agregar URI**, escriba FQDN para NetScaler Gateway y haga clic en **Guardar**.

6. Acceda a la página **Visión General** para obtener el ID de cliente, el ID de arrendatario y el ID de objeto.
7. Navega hasta **Permisos de API** y haga clic en **Agregar un permiso**.
   a) Vaya hacia abajo y seleccione **Azure AD Graph**.
   b) Elija **Permisos de aplicación**, seleccione **Aplicación.Leer todo**y, a continuación, haga clic en **Agregar permisos**.
   c) Haga clic en **Conceder consentimiento de administrador para<tenant>** y seleccione **Sí**.
   d) Compruebe que se conceden los permisos a su arrendatario.




> **Nota:**
>
> Todas las aplicaciones de Azure AD que llaman a los dispositivos de punto final de servicio `https://login.microsoftonline.com` o `https://graph.windows.net` requieren que se asigne el permiso de API para que la puerta de enlace pueda llamar a la API de NAC. Los permisos API disponibles son:
>
> - Application.Read.All
> - Application.ReadWrite.All
> - Application.OwnedBy
> - Directory.Read.All
>
> El permiso preferido es **Application.Read.All**.
>
> Para obtener más información, consulte https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/bap/2428040

8. Haga clic en el mosaico **Microsoft Graph** para configurar los permisos de API para Microsoft Graph.
9. Haga clic en el mosaico **Permisos delegados**.

10. Seleccione los permisos siguientes y haga clic en **Agregar permisos**.

    - Correo electrónico
    - `openid`
    - Profile
    - Directory.AccessAsUser.All
    - User.Read
    - User.Read.All
    - User.ReadBasic.All

    > **Permiso adicional para la comprobación de NAC de Intune:**
    >
    > todas las aplicaciones de Azure AD que llaman a los dispositivos de punto final de servicio `https://login.microsoftonline.com` o `https://graph.windows.net` requieren que se asigne el permiso de API para que la puerta de enlace pueda llamar a la API de NAC. Los permisos API disponibles son:
    >
    > - Application.Read.All
    > - Application.ReadWrite.All
    > - Application.OwnedBy
    > - Directory.Read.All
    >
    > El permiso preferido es **Application.Read.All**.
    >
    > Para obtener más información, consulte https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040

11. Haga clic en el icono de **Intune** para configurar los permisos de API para Intune.
12. Haga clic en el mosaico **Permisos de aplicación** y **Permisos delegados** para agregar permisos para get_device_compliance y get_data_warehouse respectivamente.
13. Seleccione los siguientes permisos y haga clic en **Agregar permisos**.

    - get_device_compliance - Permisos de aplicación
    - get_data_warehouse - Permisos delegados

14. En la página siguiente se enumeran los permisos de API configurados.
15. Vaya a **Certificados y secretos** y haga clic en **Nuevo secreto de cliente**.
16. En la página **Agregar un secreto de cliente**, introduzca la descripción, seleccione caducidad y haga clic en **Agregar**.
17. En la siguiente pantalla se muestra el secreto del cliente configurado.

> **Nota**
>
> El secreto del cliente solo se muestra una vez cuando se genera. Debe copiar localmente el secreto del cliente que se muestra. Utilice el mismo secreto de cliente junto con el identificador de cliente asociado a la aplicación recién registrada al configurar la acción OAuth en el dispositivo Citrix Gateway para Intune.

La configuración de la aplicación en Azure Portal ya está completa.

## Descripción de la autenticación de tokens ADAL de Azure

January 26, 2024

A continuación se muestra el flujo de eventos en una autenticación de token típica de NetScaler Gateway y Microsoft ADAL:

1. Cuando se inicia una aplicación en iOS o Android, la aplicación se pone en contacto con Azure. Se solicita al usuario que inicie sesión con sus credenciales de usuario. Tras un inicio de sesión satisfactorio, la aplicación recibe un token ADAL.

2. Este token ADAL se presenta en un NetScaler Gateway, que se ha configurado para validar el token ADAL.

3. NetScaler Gateway valida la firma del token ADAL con el certificado correspondiente de Microsoft.

4. Tras una validación satisfactoria, NetScaler Gateway extrae el nombre principal del usuario (UPN) y concede a la aplicación acceso VPN a los recursos internos.

## Configurar el servidor virtual de NetScaler Gateway para la autenticación de token ADAL de Microsoft

January 26, 2024

Para configurar un servidor virtual NetScaler Gateway para supervisar la autenticación de tokens ADAL de Microsoft, necesita la siguiente información:

- CertEndPoint: URL del punto final que contiene la clave web Json (JWK) para la verificación del token ADAL.
- Público: FQDN del servidor virtual NetScaler ADC al que la aplicación envía el token ADAL.
- Emisor: nombre del emisor de AAD. Se rellena de forma predeterminada.

- tenantID: IDde arrendatario para el registro de Azure ADAL.
- ClientID: ID único que se le da a la aplicación Gateway como parte del registro ADAL.
- ClientSecret: clave secreta proporcionada a la aplicación Gateway como parte del registro ADAL.

1. Crea una OAuthAction:

   **agregar autenticación OAuthAction**-
   **OAuthType <oauth_action_name INTUNE** —**clientid** -
   **clientsecret** -
   **audience\ -tenantid \ -issuer -**
   ****UsernameField**UPN-**Certendpoint <client_id>**
   ****<**client_secret>
   **<audience**\ > <tenantID\ > <issuer_name><certEndpoint_name>

   Ejemplo:

   agregar autenticación OAuthAction tmp_action -OAuthType INTUNE -clientid id 1204 -clientsecret a -audience “
   http://hello”-tenantid xxxx -issuer “
   https://hello”-UserNameField upn -CertendPoint
   https://login.microsoftonline.com/common/discovery/v2.0/keys

2. Crea una política de autenticación para asociarla al OAuth recién creado:

   **agregar**
   política de **autenticación** <policy_name
   **-rule true -action** <oauth intune action>

   Ejemplo:

   agregar política de autenticación oauth_intune_pol -rule true -action tmp_action

3. Enlaza el OAuth recién creado a AuthVS:

   **bind authentication vserver**<auth_vserver
   **-policy** -
   **priority 2 -GoToPriorityExpression <oauth_intune_policy>EN** D

   Ejemplo:

   vincular autenticación vserver auth_vs_for_gw1_intune -policy oauth_pol -priority 2 -goToPriorityExpression END

4. Cree un esquema de inicio de sesión:

   **agregar autenticación LoginSchema**
   **-**AuthenticationSchema <loginSchemaName\ > <authenticationSchema» location» >

**agregar autenticación LoginSchemaPolicy**\ -
**rule true -action**\ <loginSchemaPolicyName\ > <loginSchemaName\ >

Ejemplo:

agregar esquema de inicio de sesión de autenticación oauth_loginschema -AuthenticationSchema "/nsconfig/loginschema/LoginSchema/OnlyOAuthToken.xml»

agregar autenticación LoginSchemaPolicy oauth_loginschema_pol -rule true -action oauth_loginschema

5. Enlazar AuthVs con LoginSchema:

   **vincular autenticación vserver-policy -priority 2 <auth_vs> -GoToPriorityExpression <oauth_pol>END**

   Ejemplo:

   vincular autenticación vserver auth_vs_for_gw1_intune -policy oauth_loginschema_pol -priority 2 -GoToPriorityExpression END

6. Agregue un perfil de autenticación y asígnelo a un servidor virtual VPN:

   **agregar perfil**de autenticación **-AuthNvsName**\ <nfactor_profile_name><authvserver\ >

   **configurar vpn vserver**<vserverName\ \ **-authnprofile** <nfactor_profile_name>

   Ejemplo:

   agregar perfil de autenticación nfactor_prof_intune -AuthNVSName auth_vs_for_gw1_intune

   configurar vpn vserver gw1_intune-authnprofile nfactor_prof_intune

## Tipo de compatibilidad de servicio para el tráfico UDP

January 26, 2024

La compatibilidad con tipos de servicio (ToS) para UDP garantiza que una vez que un remitente configura un valor ToS para un paquete UDP, NetScaler Gateway conserva el valor hasta que el paquete llegue a su destino. Según el valor configurado y la configuración de la red de destino, la red de destino coloca el paquete UDP en una cola de salida priorizada.

> **Nota**
> Con la información de ToS, puede asignar una prioridad a cada paquete IP y solicitar un tratamiento específico, como alto rendimiento, alta fiabilidad, baja latencia, etc.

# Configuración automática de proxy para proxy saliente compatible con NetScaler Gateway

January 26, 2024

Al configurar el dispositivo NetScaler Gateway para que admita la configuración automática de proxy (PAC), la dirección URL de un archivo PAC se inserta en el explorador del cliente. El tráfico del cliente se redirige a los servidores proxy respectivos según las condiciones definidas en el archivo PAC.

A continuación se presentan algunos casos de uso comunes de PAC para proxy saliente:

- Configurar varios servidores proxy que gestionan el tráfico de clientes.
- Equilibrar la carga del tráfico del proxy en las subredes.

## Configurar los parámetros globales de NetScaler Gateway para admitir PAC para proxy saliente mediante la CLI

En la línea de comandos, escriba:

```
set vpn parameter -proxy BROWSER -autoProxyUrl <URL>
<!--NeedCopy-->
```

## Configurar NetScaler Gateway para que admita PAC en un perfil de sesión mediante la CLI

En la línea de comandos, escriba:

```
add vpn sessionAction <name> -proxy BROWSER -autoProxyUrl <URL>
<!--NeedCopy-->
```

Donde:

- **URL**: URL del servidor proxy
- **Nombre**: Nombre de la acción de sesión de VPN

## Configurar los parámetros globales de NetScaler Gateway para admitir PAC para proxy saliente mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > NetScaler Gateway > Configuración global**.
2. En la página **Configuración global**, haga clic en **Cambiar configuración global** y, a continuación, seleccione la **ficha Experiencia del cliente**.

3. En la ficha**Experiencia del cliente**, seleccione**Configuración avanzada**y, a continuación, seleccione la**ficha Proxy**.
4. En la**ficha Proxy**, seleccione **Explorador** y, a continuación, seleccione **Usar configuración automática**.
5. En el campo**URL al archivo de configuración automática del proxy**, escriba la URL del archivo PAC necesario.
6. Haga clic en **Create**.

### Configurar NetScaler Gateway para que admita PAC en el perfil de sesión mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > NetScaler Gateway > Directivas > Sesión**.
2. En la página **Perfiles y directivas de sesión**de NetScaler Gateway, cree un perfil de sesión de NetScaler Gateway.
3. Seleccione la ficha **Perfiles de sesión**, haga clic en **Agregar**e introduzca un nombre.
4. En la ficha **Experiencia del cliente**, seleccione **Configuración avanzada** y, a continuación, seleccione la ficha **Proxy**.
5. En la ficha **Proxy**, seleccione **Explorador** y, a continuación, seleccione **Usar configuración automática**.
6. En el campo**URL al archivo de configuración automática del proxy**, escriba la URL del archivo PAC necesario.
7. Haga clic en **Create**.
8. Haga clic en **Create**.

## Compatibilidad con proxies ICA salientes

January 26, 2024

La compatibilidad con proxy ICA saliente para NetScaler Gateway permite a los administradores de red aprovechar las funcionalidades de SmartControl incluso cuando Receiver y NetScaler Gateway se implementan en distintas organizaciones.

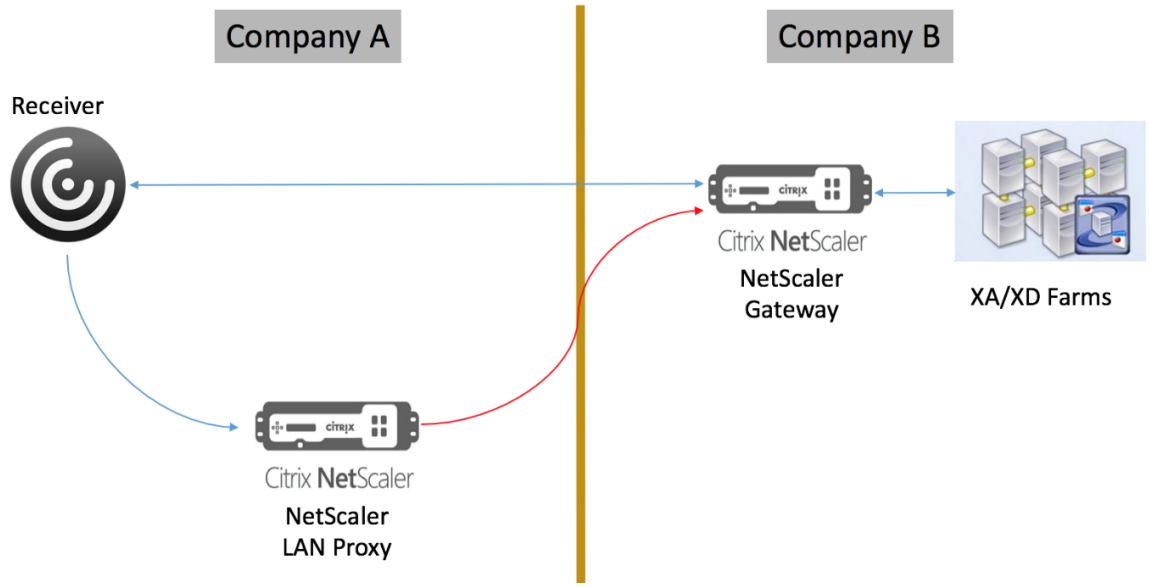
En el siguiente caso se ilustra el uso de la solución Proxy ICA saliente:

Un administrador de red necesita controlar las capacidades relacionadas con la sesión ICA cuando Receiver y NetScaler Gateway se implementan en distintas organizaciones.

### Comprensión de la compatibilidad con el proxy ICA saliente

Para llevar la funcionalidad de SmartControl a la organización empresarial, la empresa A, que tiene el receptor, necesitamos agregar un dispositivo NetScaler ADC que actúe como proxy LAN. El proxy LAN de NetScaler ADC aplica SmartControl y envía el tráfico a NetScaler Gateway de la empresa B. En este caso de implementación, Receiver reenvía el tráfico al proxy LAN de NetScaler ADC, lo que permite que el administrador de red de la empresa A aplique SmartControl. La implementación se muestra en la siguiente ilustración.




En este caso, el tráfico entre el proxy LAN y NetScaler Gateway se realiza a través de SSL.

> **Nota:** No habilite la autenticación basada en certificados de cliente en NetScaler Gateway.

## Configurar el proxy ICA saliente

January 26, 2024

Para configurar un proxy ICA saliente mediante la CLI, siga estos pasos:

1. Agregue un servidor virtual de redirección de caché:

   **agregar cr vserver**\\\ <name\ > <serviceType\ >\ <IPAddress\ > <port\ > - **CacheType** \ <cacheType\ >

   **El servicio**debe ser HDX

   **CacheType**debe ser FORWARD

**Ejemplo:**

agregar cr vserver CR_LAN_proxy HDX 10.217.208.197 8080 -CacheType FORWARD

2. Agregue un perfil ICA SmartControl:

**agregar ica accessprofile** \<name\> - **ConnectClientLPTPorts** (PREDETERMINADO) - **ClientAudioRedirection** (PREDETERMINADO) - **LocalRemoteDataSharing** (PREDETERMINADO) - **ClientClipboardRedirection** (PREDETERMINADO) - **ClientComPortRedirection** (PREDETERMINADO) - **ClientDriverRedirection** (PREDETERMINADO) - **ClientPrinterRedirection** (PREDETERMINADO) - **Multistream** (PREDETERMINADO ) - **ClientUSBDriverRedirection** (PREDETERMINADO)

**Ejemplo:**

```
add ica accessprofile disableCDM -ConnectClientLPTPorts DEFAULT -
    ClientAudioRedirection DEFAULT  – LocalRemoteDataSharing DEFAULT
     -ClientClipboardRedirection DEFAULT -ClientCOMPortRedirection
    DEFAULT  – ClientPrinterRedirection DEFAULT -Multistream DEFAULT
     -ClientUSBDriveRedirection DEFAULT
```

3. Agregue una acción ICA:

**agregar ica action** \<name\> **-AccessProfileName** \<string\>

**Ejemplo:**

```
add ica action disableCDM\_action -accessProfileName disableCDM
```

4. Agregue una política ICA:

**agregar ica policy**<string\> \ **-rule**\ -**action \ -comment**\ -**LogAction** \ <name\> <expression\> <string\> <string\>

5. Enlazar la política ICA al servidor virtual o global:

a. Enlazar a un servidor virtual

```
**bind cr vserver** \<name\> **-policyName** \<string\> **-
    priority** \<positive\_integer\>
```

**Ejemplo:**

```
bind cr vserver CR\_LAN\_Proxy –policyname disableCDM\_pol –
    priority 10
```

b. Vincularse a Global

```
**bind ica global -policyName** \<string\> -**priority** \<
    positive\_integer\>
```

**Ejemplo:**

```
bind ica global –policyName disableCDM\_pol –priority 10
```

> **Nota**
>
> Configure los puertos ICA seguros: este valor es el número de puerto del Citrix Gateway al que el proxy LAN establece una conexión saliente. De forma predeterminada, se establece en 443. Use el siguiente comando para cambiar el puerto.
>
> **establecer el parámetro ns -SecureICAports**\ <port\ >
>
> Ejemplo:
>
> establecer un parámetro ns -Secure ICAports 8443

## Integrar NetScaler Gateway en Citrix Virtual Apps and Desktops

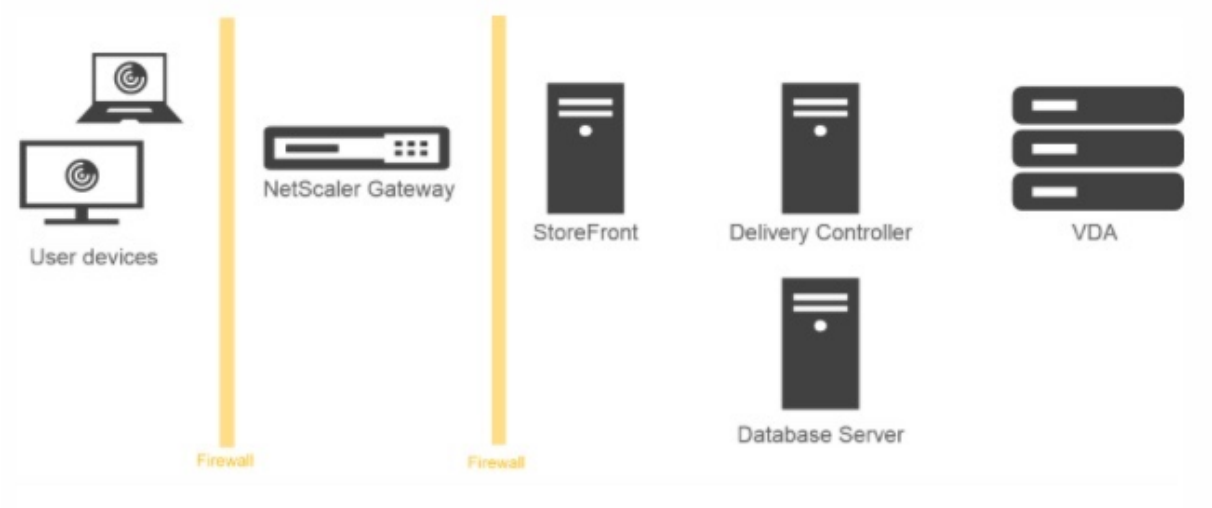
January 26, 2024

Los servidores de StoreFront se implementan y se configuran para administrar el acceso a los datos y los recursos publicados. Para el acceso remoto, se recomienda agregar NetScaler Gateway y colocarlo delante de StoreFront.

> **Nota**:
> Para ver los pasos de configuración detallados sobre cómo integrar Citrix Virtual Apps and Desktops con Citrix Gateway, consulte la documentación de StoreFront.

En el siguiente diagrama se muestra un ejemplo de implementación de Citrix simplificada de Citrix que incluye NetScaler Gateway. NetScaler Gateway se comunica con StoreFront para proteger las aplicaciones y los datos que entregan Citrix Virtual Apps and Desktops. Los dispositivos de usuario ejecutan Citrix Receiver para crear una conexión segura y acceder a sus aplicaciones, escritorios y archivos.




## Compatibilidad con OTP nativa para la autenticación

March 27, 2024

NetScaler Gateway admite contraseñas de un solo uso (OTP) sin tener que usar un servidor de terceros. La contraseña de un solo uso es una opción muy segura para autenticarse en servidores seguros, ya que el número o código de acceso generado es aleatorio. Anteriormente, firmas especializadas, como RSA con dispositivos específicos que generan números aleatorios, ofrecían los OTP. Este sistema debe estar en comunicación constante con el cliente para generar un número esperado por el servidor.

Además de reducir los gastos de capital y operativos, esta función mejora el control del administrador al mantener toda la configuración en el dispositivo Citrix ADC.

> **Nota**: Dado que ya no se necesitan servidores de terceros, el administrador de NetScaler ADC debe configurar una interfaz para administrar y validar los dispositivos de usuario.

El usuario debe estar registrado en un servidor virtual de NetScaler Gateway para utilizar la solución OTP. El registro solo es necesario una vez por dispositivo único y se puede restringir a determinados entornos. La configuración y validación de un usuario registrado es similar a la configuración de una directiva de autenticación adicional.

### Ventajas de tener función de OTP nativa

- Reduce los costes operativos al eliminar la necesidad de tener una infraestructura adicional en un servidor de autenticación además de Active Directory.

- Consolida la configuración solo en el dispositivo Citrix ADC, lo que ofrece un gran control a los administradores.
- Elimina la dependencia del cliente de un servidor de autenticación adicional para generar un número esperado por los clientes.

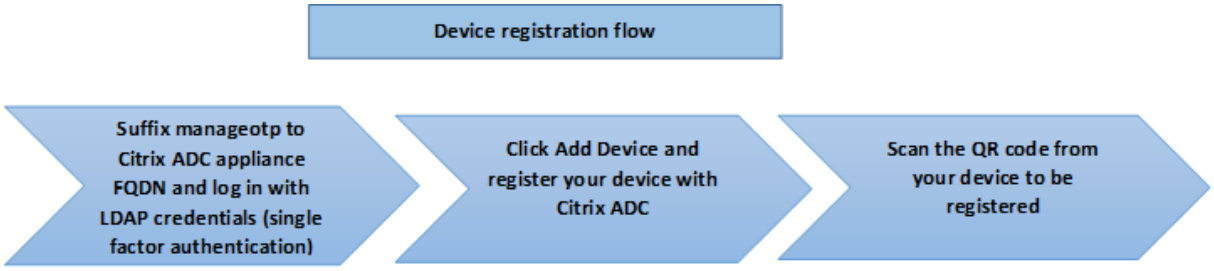
### flujo de trabajo OTP nativo

La solución OTP nativa es un proceso doble y el flujo de trabajo se clasifica de la siguiente manera:

- Registro de dispositivos
- Inicio de sesión de usuario final

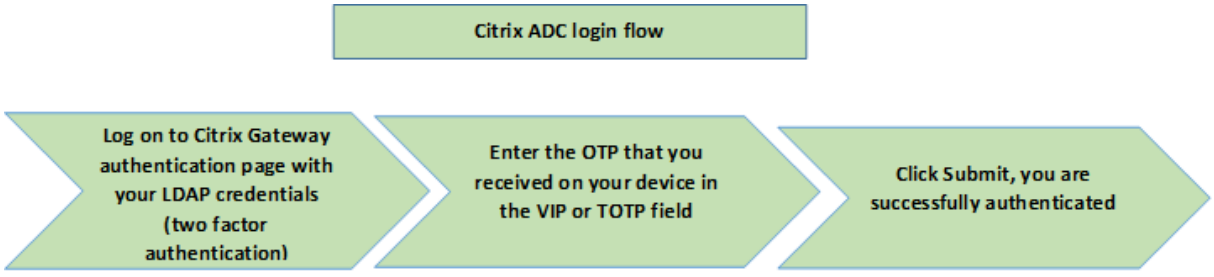
**Importante:** Puede omitir el proceso de registro si utiliza soluciones de terceros o administra otros dispositivos distintos del dispositivo NetScaler ADC. La cadena final que agregue debe tener el formato especificado por Citrix ADC.

En la siguiente ilustración se muestra el flujo de registro de dispositivos para registrar un nuevo dispositivo para recibir OTP.




**Nota:** El registro del dispositivo se puede realizar mediante cualquier número de factores. El factor único (como se especifica en la ilustración anterior) se utiliza como ejemplo para explicar el proceso de registro del dispositivo.

En la siguiente ilustración se muestra la verificación de OTP a través del dispositivo registrado.




### Requisitos previos

Para utilizar la función OTP nativa, asegúrese de que se cumplen los siguientes requisitos previos.

- La versión de la función Citrix ADC es 12.0, compilación 51.24 y versiones posteriores.
- La licencia Advanced o Premium Edition está instalada en Citrix Gateway.
- NetScaler Gateway está configurado con IP de administración y se puede acceder a la consola de administración mediante un explorador y una línea de comandos.
- Citrix ADC está configurado con un servidor virtual de autenticación, autorización y auditoría para autenticar a los usuarios.
- El dispositivo Citrix ADC se configura con Unified Gateway y el perfil de autenticación, autorización y auditoría se asigna al servidor virtual Gateway.
- La solución OTP nativa está restringida al flujo de autenticación nFactor. Se requieren directivas avanzadas para configurar la solución. Para obtener más información, consulte el artículo CTX222713.

Asegúrese también de lo siguiente para Active Directory:

- Longitud mínima de atributo de 256 caracteres.
- El tipo de atributo debe ser 'DirectoryString', como UserParameters. Estos atributos pueden contener valores de cadena.
- El tipo de cadena de atributos debe ser Unicode, si el nombre del dispositivo no está escrito en inglés.
- El administrador LDAP de Citrix ADC debe tener acceso de escritura al atributo AD seleccionado.
- El dispositivo Citrix ADC y la máquina cliente deben sincronizarse con un servidor horario de red común.

## Configurar OTP nativo mediante la GUI

El registro OTP nativo no es solo una autenticación de un solo factor. Las siguientes secciones le ayudan a configurar la autenticación de un solo factor y de segundo factor.

### Crear esquema de inicio de sesión para el primer factor

1. Vaya a **Seguridad AAA > Tráfico de aplicaciones > Esquema de inicio**de sesión.
2. Vaya a **Perfiles** y haga clic en **Agregar**.
3. En la página **Crear esquema de inicio de sesión de autenticación**, escriba *lschema_single_auth_manage_o* en el campo **Nombre** y haga clic en **Modificar** junto a **noschema**.
4. Haga clic en la carpeta **LoginSchema**.
5. Desplácese hacia abajo para seleccionar **SingleAuth.xml** y haga clic en **Seleccionar**.
6. Haga clic en **Crear**.
7. Haga clic en **Directivas** y haga clic en **Agregar**.

8. En la pantalla **Crear directiva de esquema de inicio de sesión de autenticación**, introduzca los valores siguientes.

   **Nombre:** lpol_single_auth_manage_otp_by_url
   **Perfil:** seleccione lpol_single_auth_manage_otp_by_url de la lista.
   **Regla:** HTTP.REQ.COOKIE.VALUE("NSC_TASS").EQ("`manageotp`")

**Configurar el servidor virtual de autenticación, autorización y auditoría**

1. Vaya a **Seguridad > AAA —Tráfico de aplicaciones > Servidores virtuales de autenticación**. Haga clic para modificar el servidor virtual existente.
2. Haga clic en el icono **+** situado junto a **Esquemas de inicio** de sesión en **Configuración avanzada** en el panel derecho.
3. Selecciona **Sin esquema de inicio de sesión**.
4. Haga clic en la flecha y seleccione la directiva **lpol_single_auth_manage_otp_by_url**.
5. Seleccione la directiva **lpol_single_auth_manage_otp_by_url** y haga clic en **Seleccionar**.
6. Haga clic en **Vincular**.
7. Desplácese hacia arriba y seleccione **1 Directiva de autenticación** en **Directiva de autenticación avanzada**.
8. Haga clic con el botón derecho en **la directiva nFactor** y seleccione **Modificar enlace**.
9. Haga clic en el icono **+** presente en **Seleccionar factor siguiente,** cree un factor siguiente y haga clic en **Vincular**.
10. En la pantalla **Crear autenticación `PolicyLabel`**, introduzca lo siguiente y haga clic en **Continuar**:

    **Nombre**: manage_otp_flow_label

    **Esquema de inicio de sesión**: Lschema_Int
11. En la pantalla **Etiqueta de directiva de autenticación**, haga clic en el icono **+** para crear una directiva.
12. En la pantalla **Crear directiva de autenticación**, escriba lo siguiente:

    **Nombre**: auth_pol_ldap_otp_action
13. Seleccione el tipo de acción mediante la lista **Tipo de acción**.
14. En el campo **Acción**, haga clic en el icono **+** para crear una Acción.

15. En la página **Crear servidor LDAP de autenticación**, seleccione el botón de opción **IP del servidor**, anule la selección de la casilla de verificación situada junto a **Autenticación**, introduzca los valores siguientes y seleccione **Probar conexión**.

    **Nombre**: ldap_otp_action

    **Dirección IP**: 192.168.10.11

    **DN base**: DC = formación, DC = laboratorio

    **Administrador**: Administrator@training.lab

    **Contraseña**: xxxxx

16. Desplácese hacia abajo hasta la sección **Otros ajustes**. Utilice el menú desplegable para seleccionar las siguientes opciones.
    **Atributo de nombre de inicio de sesión del servidor** como **nuevo** y escriba **userprincipalname**.

17. Utilice el menú desplegable para seleccionar **Atributo de nombre de SSO** como **Nuevo** y escriba **userprincipalname**.

18. Introduzca "UserParameters"en el campo **OTP Secret** y haga clic en **Más**.

19. Introduzca los siguientes atributos.

    **Atributo 1** = mail
    **Atributo 2** =
    **Atributo objectGUID 3** = immutableID

20. Haga clic en **Aceptar**.

21. En la página **Crear directiva de autenticación**, establezca la expresión en **true** y haga clic en **Crear**.

22. En la página **Crear etiqueta de directiva de autenticación**, haga clic en **Vincular** y haga clic en **Listo.**

23. En la página **Enlace de directivas**, haga clic en **Vincular**.

24. En la página **Directiva de autenticación**, haga clic en **Cerrar** y haga clic en **Listo**.

> **Nota**
>
> El servidor virtual de autenticación debe estar vinculado al tema del portal RFWebUI. Enlace un certificado de servidor al servidor. La IP del servidor '1.2.3.5'debe tener un FQDN correspondiente, es decir, otpauth.server.com, para su uso posterior.

**Crear esquema de inicio de sesión para OTP de segundo factor**

1. Vaya a **Seguridad > Tráfico de aplicaciones AAA > Servidores virtuales**. Seleccione el servidor virtual que va a modificar.
2. Vaya hacia abajo y seleccione **1 esquema de inicio de sesión**.
3. Haga clic en **Add Binding**.
4. En la sección **Vinculación de directivas**, haga clic en el icono **+** para agregar una directiva.
5. En la página **Crear directiva de esquema de inicio de sesión de autenticación**, escriba Nombre como OTP y haga clic en el icono **+** para crear un perfil.
6. En la página **Crear esquema de inicio de sesión de autenticación**, escriba Nombre como OTP y haga clic en el icono situado junto a **noschema**.
7. Haga clic en la carpeta **LoginSchema**, seleccione **DualAuthManageOTP.xml**y, a continuación, haga clic en **Seleccionar**.
8. Haga clic en **Crear**.
9. En la sección **Regla**, escriba **True**. Haga clic en **Crear**.
10. Haga clic en **Bind**.
11. Observe los dos factores de autenticación. Haga clic en **Cerrar** y haga clic en **Listo**.

**Configurar la directiva de cambio de contenido para administrar OTP**

Las siguientes configuraciones son necesarias si utiliza Unified Gateway.

1. Vaya a **Administración del tráfico > Cambio de contenido > Directivas**. Seleccione la directiva de cambio de contenido, haga clic con el botón derecho y seleccione **Modificar**.
2. Modifique la expresión para evaluar la siguiente instrucción OR y haga clic en **Aceptar**:

```
es_vpn_url
```

## Configurar OTP nativo mediante la CLI

Debe disponer de la siguiente información para configurar la página de administración de dispositivos OTP:

- IP asignada al servidor virtual de autenticación
- FQDN correspondiente a la IP asignada
- Certificado de servidor para servidor virtual de autenticación

> **Nota:** La OTP nativa es solo una solución basada en web.

**Para configurar la página de registro y administración de dispositivos OTP**

Crear servidor virtual de autenticación

```
add authentication vserver authvs SSL 1.2.3.5 443
bind authentication vserver authvs -portaltheme RFWebUI
bind ssl vserver authvs -certkeyname otpauthcert
<!--NeedCopy-->
```

> **Nota:** El servidor virtual de autenticación debe estar enlazado al tema del portal RFWebUI. Enlace un certificado de servidor al servidor. La IP del servidor '1.2.3.5'debe tener un FQDN correspondiente, es decir, otpauth.server.com, para su uso posterior.

**Para crear una acción de inicio de sesión LDAP**

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
    -  serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
    ldapBindDnPassword <PASSWO> -ldapLoginName <USER FORMAT>
<!--NeedCopy-->
```

**Ejemplo**:

```
add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4 -
    serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
    administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
    ldapLoginName userprincipalname
<!--NeedCopy-->
```

**Para agregar la directiva de autenticación para el inicio de sesión de LDAP**

```
add authentication Policy auth_pol_ldap_logon -rule true -action
    ldap_logon_action
<!--NeedCopy-->
```

**Para presentar la interfaz de usuario a través de LoginSchema**

Mostrar campo de nombre de usuario y campo de contraseña a los usuarios al iniciar sesión

```
add authentication loginSchema lschema_single_auth_manage_otp -
    authenticationSchema "/nsconfig/loginschema/LoginSchema/
    SingleAuthManageOTP.xml"
<!--NeedCopy-->
```

### Mostrar la página de registro y administración de dispositivos

Citrix recomienda dos formas de mostrar la pantalla de registro y administración del dispositivo: URL o nombre de host.

- **Uso de URL**

  Cuando la URL contiene '/manageotp'

  ```
  - add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_ur
    -rule "http.req.cookie.value("NSC_TASS").contains("manageotp
  ")"-action lschema_single_auth_manage_otp
  - bind authentication vserver authvs -policy lpol_single_auth_manage_otp
    -priority 10 -gotoPriorityExpression END
  ```

- **Uso del nombre de host**

  Cuando el nombre de host es 'alt.server.com'

  ```
  - add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_ho
    -rule "http.req.header("host").eq("alt.server.com")"-action
  lschema_single_auth_manage_otp
  - bind authentication vserver authvs -policy lpol_single_auth_manage_otp
    -priority 20 -gotoPriorityExpression END
  ```

#### Para configurar la página de inicio de sesión de usuario mediante la CLI

Debe disponer de la siguiente información para configurar la página Inicio de sesión de usuario:

- IP de un servidor virtual de equilibrio de carga
- FQDN correspondiente para el servidor virtual de equilibrio de carga
- Certificado de servidor para el servidor virtual de equilibrio de carga

  vincular ssl vserver lbvs_https -certkeyname lbvs_server_cert

El servicio back-end en el equilibrio de carga se representa de la siguiente manera:

```
1 add service iis_backendsso_server_com 1.2.3.210 HTTP 80
2 bind lb vserver lbvs_https iis_backendsso_server_com
3 <!--NeedCopy-->
```

#### Para crear una acción de validación de código de acceso OTP

```
1 add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
    -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
    ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT> -
    authentication DISABLED -OTPSecret <LDAP ATTRIBUTE>
```

```
<!--NeedCopy-->
```

**Ejemplo:**

```
add authentication ldapAction ldap_otp_action -serverIP 1.2.3.4 -
    serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
    administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
    ldapLoginName userprincipalname -authentication DISABLED -OTPSecret
    userParameters
<!--NeedCopy-->
```

> **Importante:** La diferencia entre el inicio de sesión LDAP y la acción OTP es la necesidad de inhabilitar la autenticación e introducir un nuevo parámetro `OTPSecret`. No utilice el valor del atributo AD.

**Para agregar directiva de autenticación para la validación de código de acceso OTP**

```
add authentication Policy auth_pol_otp_validation -rule true -action
    ldap_otp_action
<!--NeedCopy-->
```

**Para presentar la autenticación de dos factores a través de LoginSchema** Agregue la interfaz de usuario para la autenticación de dos factores.

"'add authentication loginSchema lscheme_dual_factor -authenticationSchema "/nsconfig/loginschema/LoginSchema/DualAuth.xml"
add authentication loginSchemaPolicy lpol_dual_factor -rule true -action lscheme_dual_factor

```
#### Para crear un factor de validación de código de acceso mediante la
     etiqueta de directiva

Crear una etiqueta de directiva de flujo OTP de administración para el
    siguiente factor (el primer factor es inicio de sesión LDAP)
```

add authentication loginSchema lschema_noschema -authenticationSchema noschema
add authentication policylabel manage_otp_flow_label -loginSchema lschema_noschema

```
#### Para enlazar la directiva OTP a la etiqueta de directiva
```

bind authentication policylabel manage_otp_flow_label -policyName auth_pol_otp_validation -priority 10 -gotoPriorityExpression NEXT

```
#### Para enlazar el flujo de la interfaz de usuario

Enlazar el inicio de sesión LDAP seguido de la validación OTP con el
    servidor virtual de autenticación.
```

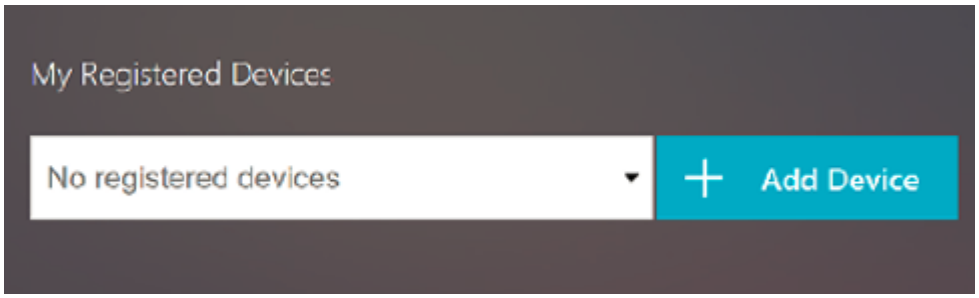
bind authentication vserver authvs -policy auth_pol_ldap_logon -priority 10 -nextFactor manage_otp_flow_label -gotoPriorityExpression NEXT

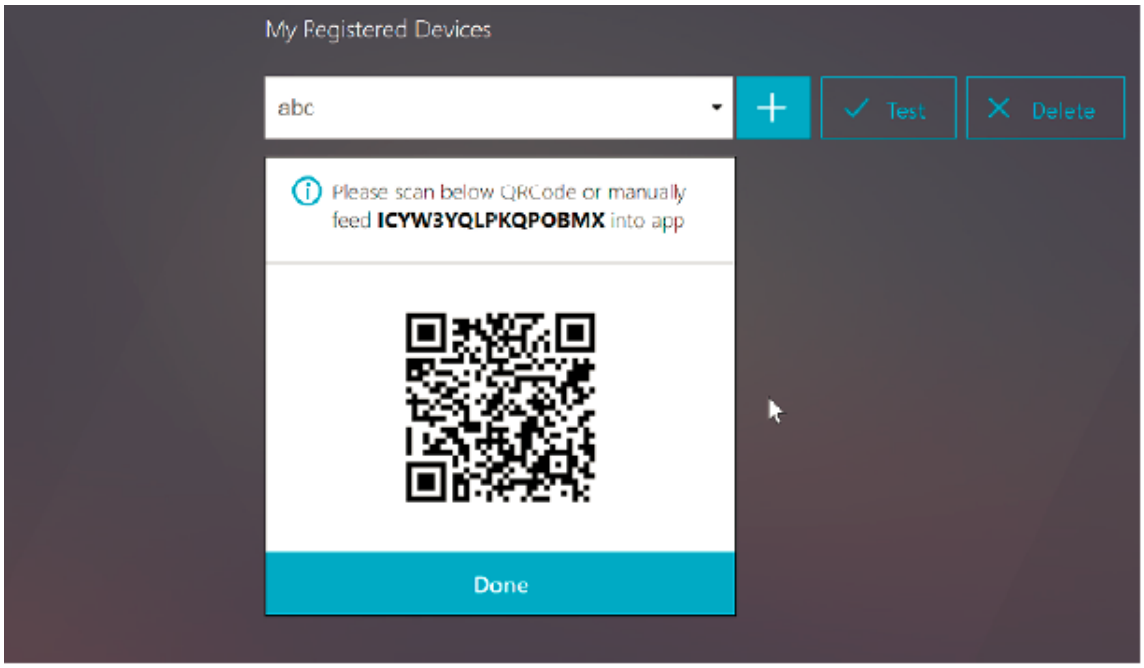
bind authentication vserver authvs -policy lpol_dual_factor -priority 30 -gotoPriorityExpression END
‘‘‘

### Registre su dispositivo con Citrix ADC

1. Vaya a el FQDN de NetScaler ADC (primera IP pública), con el sufijo /manageotp. Por ejemplo, inicie sesión en https://otpauth.server.com/manageotp con credenciales de usuario.
2. Haga clic en el ícono **+** para agregar un dispositivo.



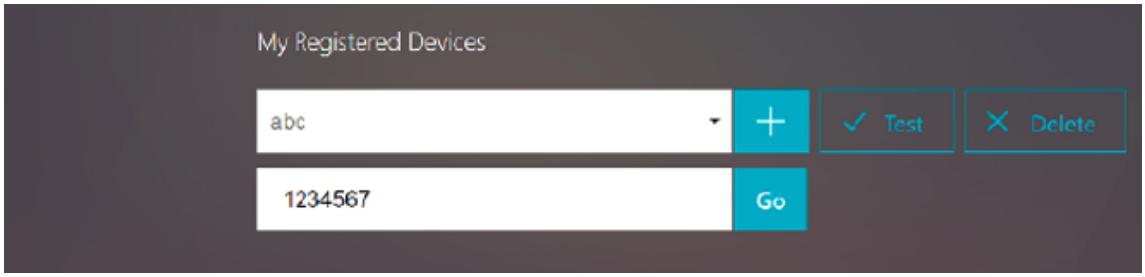

3. Introduzca el nombre de un dispositivo y presione **Ir**. Aparece un código de barras en la pantalla.
4. Haga clic en **Iniciar configuración** y luego haga clic en **Escanear código de barras**
5. Coloque la cámara del dispositivo sobre el código QR. Si lo quiere, puede introducir el código de 16 dígitos.




> **Nota**: El código QR mostrado es válido durante 3 minutos.

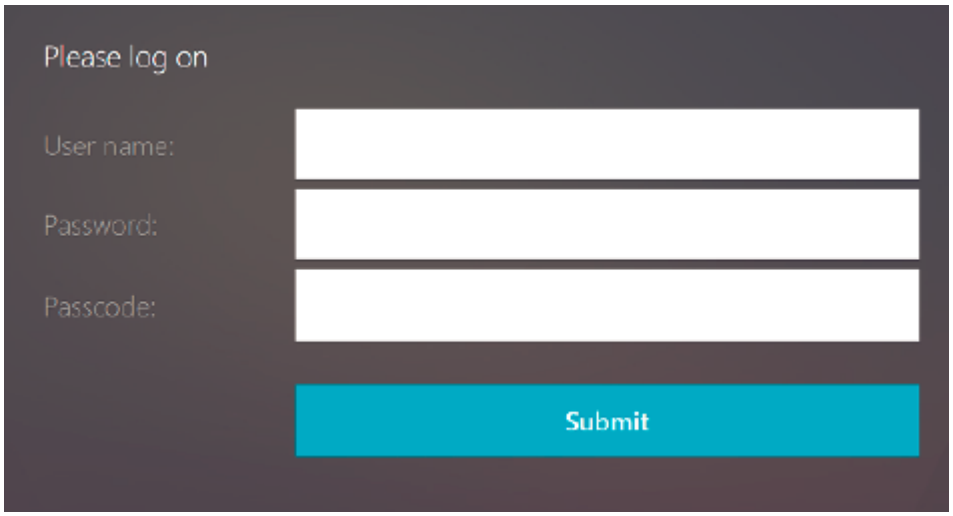
6. Una vez escaneado correctamente, se le presenta un código sensible al tiempo de 6 dígitos que se puede utilizar para iniciar sesión.




7. Para realizar la prueba, haga clic en **Listo** en la pantalla QR y, a continuación, haga clic en la marca de verificación verde de la derecha.
8. Seleccione su dispositivo en el menú desplegable e introduzca el código de Google Authenticator (debe ser azul, no rojo) y haga clic en **Ir**.
9. Asegúrate de cerrar la sesión mediante el menú desplegable de la esquina superior derecha de la página.

### Inicie sesión en Citrix ADC mediante la OTP

1. Navegue a la primera URL pública e introduzca su OTP desde Google Authenticator para iniciar sesión.
2. Autenticación en la página inicial de Citrix ADC.



## Configuración de la extensión de indicación de nombre de servidor

March 27, 2024

Ahora se puede configurar un dispositivo Citrix Gateway para incluir una extensión de indicación de nombre de servidor (SNI) en el paquete SSL de «saludo al cliente» que se envía al servidor back-end. La extensión SNI ayuda al servidor back-end a identificar el FQDN que se solicita durante el protocolo de enlace SSL y a responder con los certificados respectivos.

> **Nota**
>
> Habilita la compatibilidad con SNI cuando hay varios dominios SSL alojados en el mismo servidor.

**Para configurar NetScaler Gateway para que admita SNI mediante GUI:**

1. En la GUI de NetScaler, vaya a **Configuración > Citrix NetScaler > Configuración global.**
2. Haga clic en el enlace **Cambiar configuración global** y, en el menú **SNI del servidor backend**, seleccione **Habilitado**.

**Para configurar NetScaler Gateway para que admita SNI mediante la interfaz de línea de comandos, en el símbolo del sistema, escriba:**

```
set vpn parameter backendServerSni <ENABLED><DISABLED>
<!--NeedCopy-->
```

## Validar el certificado del servidor durante un protocolo de enlace SSL

January 26, 2024

El dispositivo NetScaler Gateway ahora se puede configurar para validar el certificado de servidor proporcionado por el servidor back-end durante un enlace SSL.

Para configurar los parámetros globales de NetScaler Gateway para admitir PAC para proxy saliente mediante la utilidad de configuración

Enlazar el certificado de CA

1. Vaya a **Configuración** > **NetScaler Gateway** > **NetScaler Gateway Policy Manager** > **Vinculaciones de certificados**.**
2. En la pantalla **Vinculaciones de certificados**, haga clic en el icono **+**.
3. En la pantalla **Enlace de certificados de CA**, haga clic en **Agregar enlace** y haga clic en **Instalar**.

4. Seleccione el nombre del archivo del certificado en el campo **Nombre del archivo del certificado** y haga clic en **Instalar**.
5. En la pantalla **Enlace de certificados de CA**, seleccione el certificado y haga clic en **Vincular**.
6. Haga clic en **Listo**.

**Habilitación de la validación de certificados:**

1. Vaya a **NetScaler Gateway > Configuración global.**
2. Haga clic en **Cambiar configuración global**.**
3. Seleccione **Habilitado** en el menú desplegable **Validación de certificados del servidor backend** y haga clic en **Aceptar**.

Para configurar los parámetros globales de NetScaler Gateway para admitir certificados de servidor con la línea de comandos

En el símbolo del sistema, escriba los comandos siguientes:

```
    bind vpn global cacert DNPGCA1

    set vpn parameter backendcertValidation ENABLED
<!--NeedCopy-->
```

## Usar la directiva avanzada para crear directivas VPN

January 26, 2024

Classic Policy Engine (PE) y Advance Policy Infrastructure (PI) son dos marcos de configuración y evaluación de directivas diferentes que NetScaler ADC admite actualmente.

La infraestructura de políticas avanzadas consiste en un lenguaje de expresión extremadamente poderoso. El lenguaje de expresiones se puede usar para definir reglas en la política, definir varias partes de la acción y otras entidades compatibles. El lenguaje de expresión puede analizar cualquier parte de la solicitud o respuesta y también le permite examinar en profundidad los encabezados y la carga útil. El mismo lenguaje de expresiones se expande y funciona en todos los módulos lógicos compatibles con NetScaler ADC.

> **Nota:**
> Le recomendamos que utilice directivas avanzadas para crear directivas.

### ¿Por qué migrar de la directiva clásica a la directiva anticipada?

Advanced Policy tiene un conjunto de expresiones enriquecido y ofrece una flexibilidad mucho mayor que la directiva clásica. A medida que Citrix ADC escala y atiende a una gran variedad de clientes, es

imperativo admitir expresiones que superen con creces las políticas avanzadas. Para obtener más información, consulte Directivas y expresiones.

A continuación se presentan las capacidades agregadas para la Directiva Anticipada.

- Posibilidad de acceder al cuerpo de los mensajes.
- Soporta muchos protocolos adicionales.
- Accede a muchas funciones adicionales del sistema.
- Tiene más funciones básicas, operadores y tipos de datos.
- Permite analizar archivos HTML, JSON y XML.
- Facilita la rápida coincidencia paralela de múltiples cadenas (conjuntos de patrones, etc.).

Ahora se pueden configurar las siguientes directivas de VPN mediante Advance Policy.

- Directiva de sesión
- Directiva de autorización
- Directiva de tráfico
- Directiva de túnel
- Directiva de auditoría

Además, el análisis de punto final (EPA) se puede configurar como una función nFactor para autenticación. La EPA se utiliza como control de acceso para los dispositivos de punto final que intentan conectarse al dispositivo Gateway. Antes de que aparezca la página de inicio de sesión de Gateway en un dispositivo de punto final, se comprueban los requisitos mínimos de hardware y software del dispositivo, según los criterios de aptitud configurados por el administrador de Gateway. El acceso a Gateway se concede en función del resultado de las comprobaciones realizadas. Anteriormente, EPA se configuraba como parte de la directiva de sesión. Ahora se puede vincular a nFactor proporcionando más flexibilidad en cuanto a cuándo se puede realizar. Para obtener más información sobre la EPA, consulte el tema Cómo funcionan las directivas de dispositivos de punto final. Para obtener más información sobre nFactor, consulte el tema Autenticación nFactor.

**Casos de uso:**

### EPA previo a la autenticación mediante EPA avanzado

El escaneo EPA previo a la autenticación se realiza antes de que el usuario proporcione las credenciales de inicio de sesión. Para obtener información sobre cómo configurar NetScaler Gateway para la autenticación nFactor con la exploración EPA previa a la autenticación como uno de los factores de autenticación, consulte el tema CTX224268.

### EPA posterior a la autenticación con EPA avanzada

El escaneo EPA posterior a la autenticación se realiza después de verificar las credenciales del usuario. En la infraestructura de políticas clásica, la EPA posterior a la autenticación se configuraba como parte de la política de sesión o la acción de sesión. En la infraestructura de políticas avanzada, el escaneo de la EPA se configurará como el factor EPA en la autenticación del factor n. Para obtener información sobre la configuración de Citrix Gateway para la autenticación de factores n con el escaneo EPA posterior a la autenticación como uno de los factores de autenticación, consulte el tema CTX224303
.

### EPA de autenticación previa y versiones posteriores a la autenticación mediante directivas avanzadas

EPA se puede realizar antes de la autenticación y versiones posteriores a la autenticación. Para obtener información sobre cómo configurar NetScaler Gateway para la autenticación nFactor con exploraciones EPA previas y posteriores a la autenticación, consulte el tema CTX231362.

### Escaneo periódico de la EPA como factor en la autenticación nFactor

En la infraestructura de políticas clásica, el escaneo periódico de la EPA se configuró como parte de la acción de la política de sesión. En una infraestructura de políticas avanzada, se puede configurar como parte de la autenticación de factor n de la EPA.

Para obtener más información sobre cómo configurar la exploración EPA periódica como factor en la autenticación nFactor, haga clic en el temaCTX231361.

**Solución de problemas:**

Los siguientes puntos deben tenerse en cuenta para la solución de problemas.

- Las directivas clásicas y avanzadas del mismo tipo (por ejemplo, directiva de sesión) no pueden vincularse a la misma entidad o punto de enlace.
- La prioridad es obligatoria para todas las políticas de PI.
- La política avanzada para VPN se puede vincular a todos los puntos de enlace.
- La política avanzada con la misma prioridad se puede vincular a un único punto de enlace.
- Si no se aplica ninguna de las políticas de autorización configuradas, se aplica la acción de autorización global configurada en el parámetro VPN.
- En la directiva de autorización, la acción de autorización no se invierte si se produce un error en la regla de autorización.

**Expresiones equivalentes de directivas avanzadas de uso común para Classic Policy:**

| Expresiones clásicas de directivas | Expresiones de directiva anticipada |
|---|---|
| ns_true | true |
| ns_false | false |
| REQ.HTTP | HTTP.REQ |
| RES.HTTP | HTTP.RES |
| HEADER “foo” | HEADER(“foo”) |
| CONTAINS ”bar” | .CONTAINS («bar») [Tenga en cuenta el uso de «.».] |
| REQ.IP | CLIENT.IP |
| RES.IP | SERVER.IP |
| SOURCEIP | SRC |
| DESTIP | DST |
| REQ.TCP | CLIENT.TCP |
| RES.TCP | SERVER.TCP |
| SOURCEPORT | SRCPORT |
| DESTPORT | DSTPORT |
| STATUSCODE | STATUS |
| REQ.SSL.CLIENT.CERT | CLIENT.SSL.CLIENT_CERT |

## Configuración simplificada de aplicaciones SaaS mediante una plantilla

January 26, 2024

La configuración de aplicaciones SaaS con inicio de sesión único en NetScaler Gateway se simplifica mediante el aprovisionamiento de un menú desplegable de plantillas para aplicaciones SaaS populares. La aplicación SaaS que se va a configurar se puede seleccionar en el menú. La plantilla rellena previamente gran parte de la información necesaria para configurar las aplicaciones. Sin embargo, se debe proporcionar la información específica del cliente.

**Nota: La siguiente sección contiene los pasos que se deben seguir en Citrix Gateway para configurar y publicar una aplicación mediante una plantilla. Los pasos de configuración que se deben realizar en el servidor de aplicaciones se presentan en la sección siguiente.**

## Configuración y publicación de aplicaciones mediante plantilla: configuración específica de NetScaler Gateway

**La siguiente configuración toma la aplicación AWS Console como ejemplo para configurar y publicar una aplicación mediante una plantilla.**

Antes de empezar, necesitas lo siguiente:

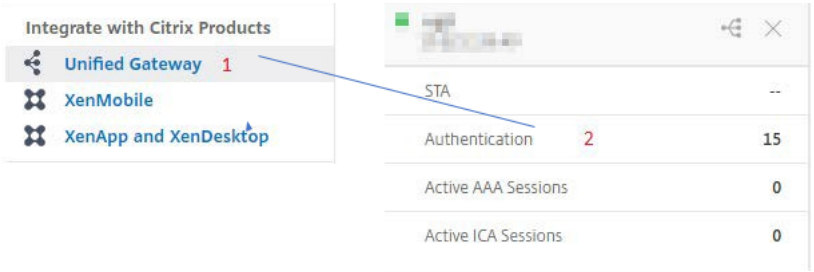
- Cuenta de administrador para la consola de AWS
- Cuenta de administrador de Citrix Gateway

**Los pasos de configuración de la consola de AWS son los siguientes:**

1. Configure la consola de AWS con el catálogo de aplicaciones.
2. Exportar metadatos de IdP de AWS Console desde NetScaler ADC.
3. Configure el IdP en la consola de AWS.

**PASO 1:**Configurar la consola de AWS con el catálogo de aplicaciones

1. Haga clic en **Unified Gateway > Autenticación** .




   Aparece la pantalla de configuración de Unified Gateway.

2. En la sección **Aplicaciones**, haga clic en el icono de edición. Ahora, haz clic en el icono con el signo más. Aparece la ventana Aplicación.

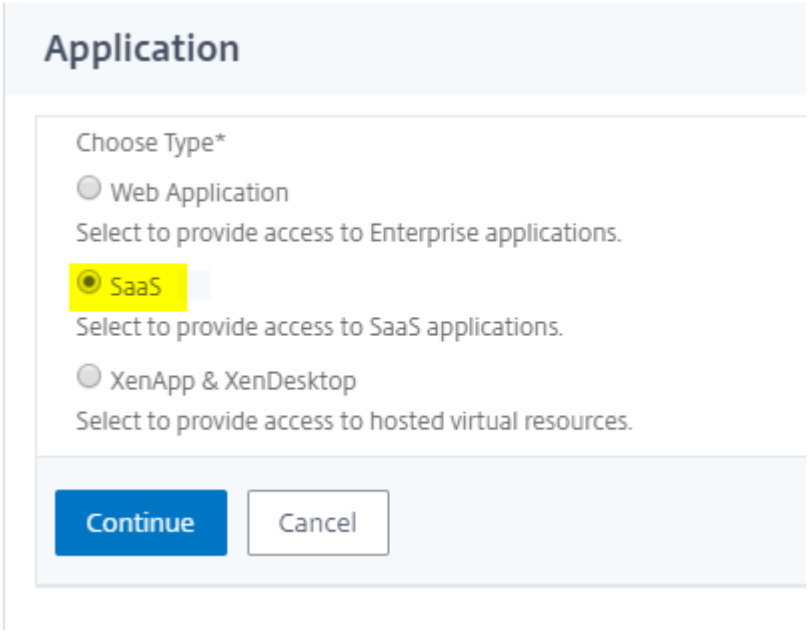
   imagen 



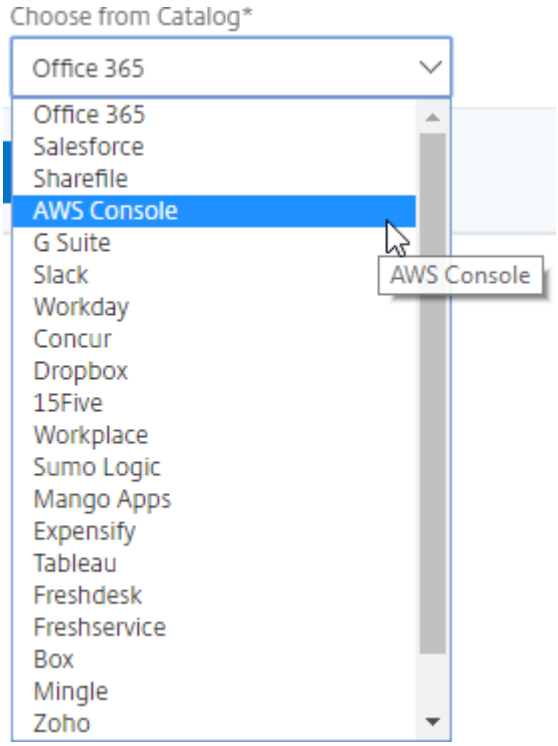


3. Seleccione **SaaS** en el tipo de aplicación.

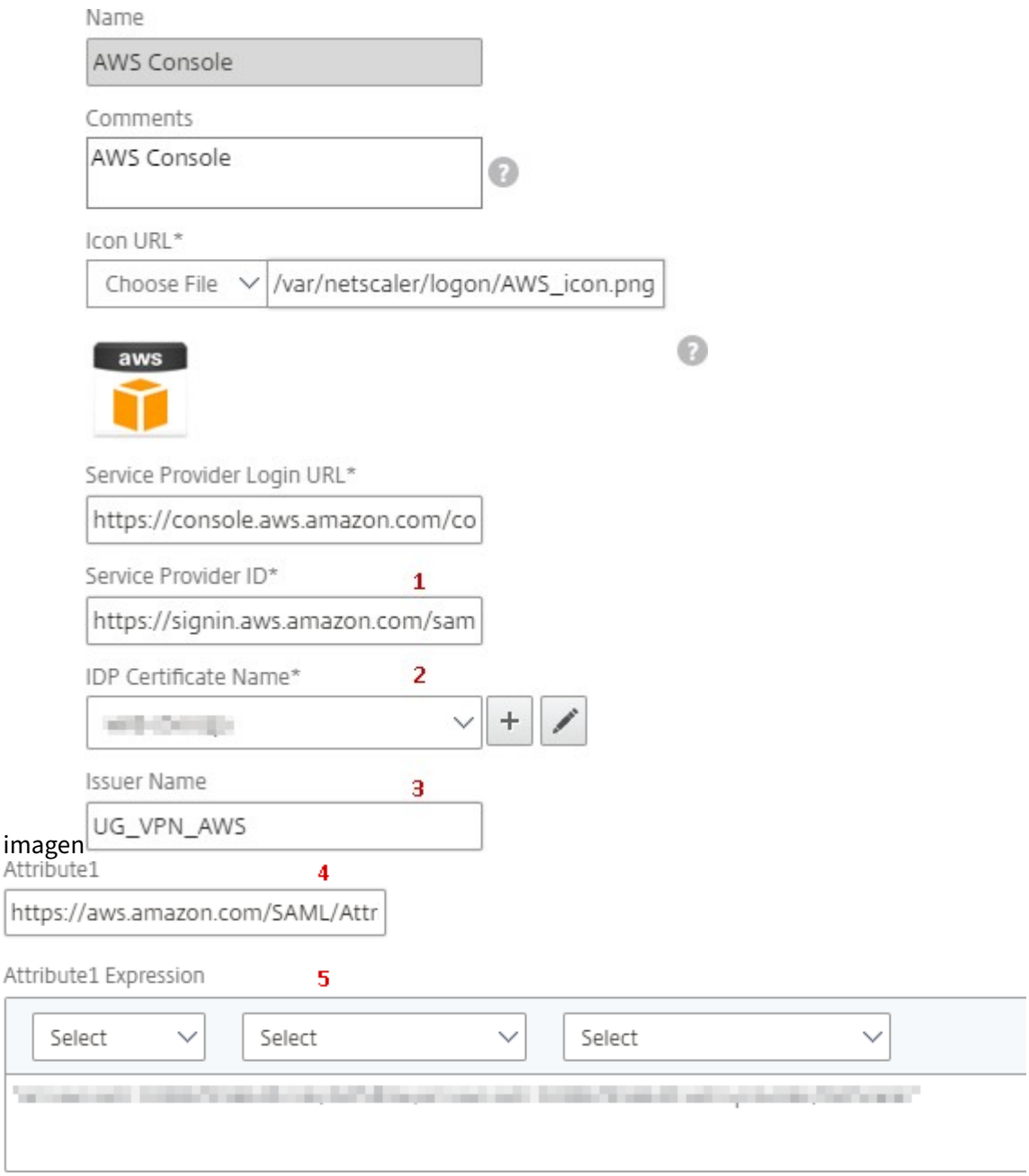



4. Seleccione **AWS Console** de la lista desplegable.




5. Rellene la plantilla de aplicación con los valores adecuados.




imagen

6. Introduzca los siguientes detalles de configuración de SAML y haga clic en **Continuar**.

   **ID de proveedor de servicios** —https://signin.aws.amazon.com/saml

   **Nombre del certificado de firma**: Debe seleccionarse el certificado del IdP

   **Nombre del emisor**: El nombre del emisor se puede rellenar según su elección

   **Atributo 1** —`https://aws.amazon.com/SAML/Attributes/Role`

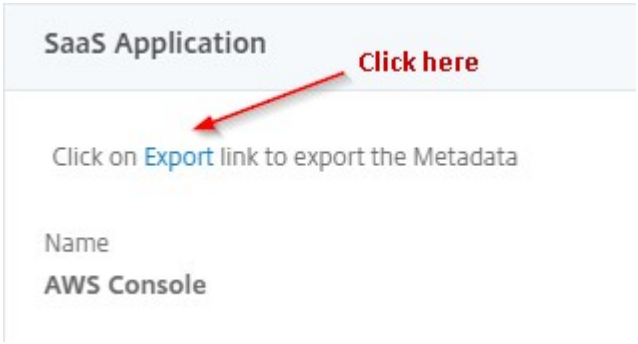
   **Expresión de atributo1**: ARN de rol, ARN de IdP, como se muestra en el paso 3

7. Haga clic en **Listo**.

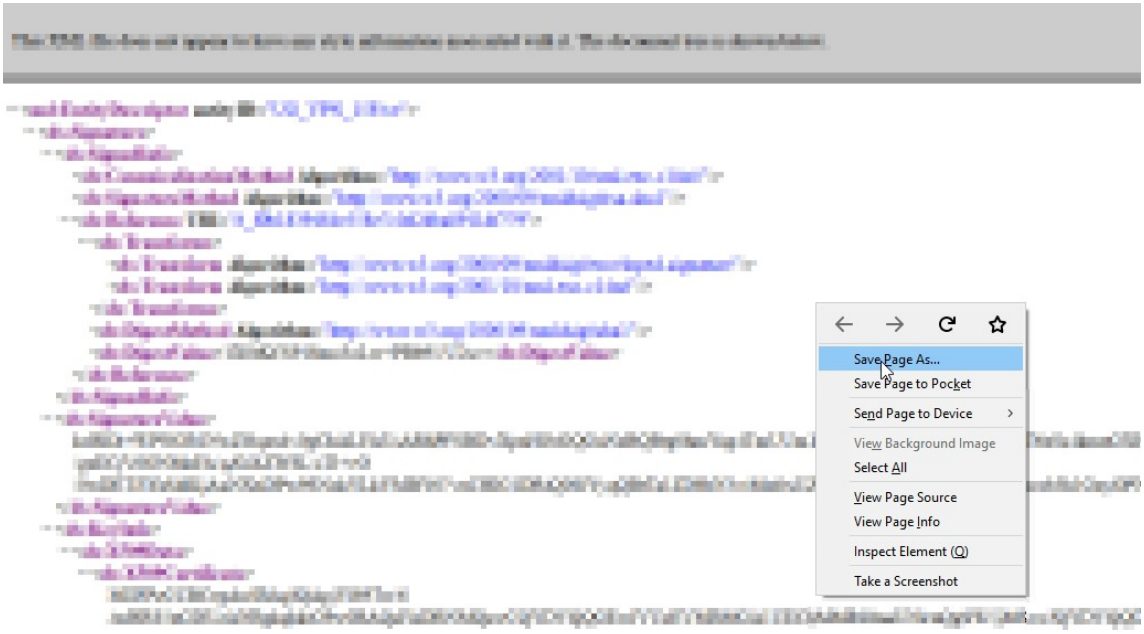
 

**PASO 2:** Exporte los metadatos del IdP de la consola de AWS desde NetScaler Gateway.

1. Haga clic en **Unified Gateway > Autenticación** .
2. Desplácese hacia abajo y haga clic en la plantilla **de AWS Console**. Aparece la ventana Aplicación SaaS. Haga clic en el enlace **Exportar**.




3. **Los metadatos** se abrirá en otra ventana. Guardar el archivo de **metadatos del IdP**




**PASO 3:** Configure el IdP en la consola de AWS.

## Configuración y publicación de aplicaciones mediante plantilla: configuración específica del servidor de aplicaciones

Los siguientes son los enlaces al pdf que contiene orientación sobre la configuración específica del servidor de aplicaciones para configurar y publicar aplicaciones SaaS populares mediante una plantilla.

- 15Five

- Absorb
- Accompa
- Adobe Captivate Prime
- Adobe Creative Cloud
- Aha
- Alertops
- Allocadia
- Ariba
- Assembla
- AWS Console
- BambooHR
- Base CRM
- BitaBIZ
- Bluejeans
- Blissbook
- Bonusly
- Box
- Bugsnag
- Buildkite
- CakeHR
- Cardboard
- Cedexis
- Celoxis
- Cisco Meraki
- ClearSlide
- CloudCheckr
- ConceptShare
- Concur
- Confluence

- Contactzilla
- Convo
- Criconus
- Dashlane
- Datadog
- Deskpro
- Deputy
- DigiCert
- Docusign
- Domo
- Dropbox
- Duo
- efront
- Ekarda
- Envoy
- ERP
- Expensify
- EZOfficeInventory
- EZRentOut
- Favro
- Federated Directory
- Feedly
- Fivetran
- Flatter Files
- Flowdock
- Freshdesk
- Front
- G-Suite
- GitHub

- GlassFrog
- GotoMeeting
- Happyfox
- Helpjuice
- Help Scout
- Hoshinplan
- Humanity
- Igloo
- Illumio
- Image Relay
- iMeet Central
- InteractGo
- iQualify One
- Jira
- Kanban Tool
- Keeper Security
- Kentik
- Kentik
- Kissflow
- KnowBe4
- KnowledgeOwl
- Kudos
- LaunchDarkly
- Lifesize
- Litmos
- LiquidPlanner
- LogDNA
- Mango
- Manuscript

- Marketo
- Mingle
- Mixpanel
- MuleSoft
- MyWebTimesheets
- New Relic
- Nmbrs
- Nuclino
- Office365
- OneDesk
- OpsGenie
- Orginio
- Pagerduty
- Panorama9
- ParkMyCloud
- Peakon
- People HR
- Pingboard
- Pipedrive
- PlanMyLeave
- PlayVox
- Podio
- ProdPad
- Proto.io
- Proxyclick
- PurelyHR
- Quandora
- Rackspace
- RealtimeBoard

- Remedyforce
- Robin
- Rollbar
- Salesforce
- Samanage
- Samepage
- Sentry
- ServiceDesk Plus
- ServiceNow
- Shufflrr
- Skeddly
- Skills Base
- Slack
- Slemma
- Sli.do
- Smartsheet
- Spoke
- Spotinst
- SproutVideo
- StatusCast
- Status Hero
- Statushub
- Statuspage
- Sumologic
- Supermood
- Syncplicity
- Tableau
- Targetprocess
- Teamphoria

- Testable
- TestFairy
- TextExpander
- TextMagic
- ThousandEyes
- Thycotic Secret Server
- Tinfoil Security
- Trisotech
- Trumba
- TwentyThree
- Unifi
- UserEcho
- UserVoice
- Velpic
- VictorOps
- Vidizmo
- Visual Paradigm
- Weekdone
- Wepow
- When I Work
- Workday
- Workpath
- Workplace
- Workstars
- Workteam
- XaitPorter
- Ximble
- XMatters
- Yodeck

- Zendesk
- Zivver
- Zoho-one
- Zivver
- Zoom

## Certificado de dispositivo en nFactor como componente de la EPA

March 27, 2024

El certificado de dispositivo se puede configurar en nFactor como componente EPA. El certificado de dispositivo puede aparecer como cualquier factor como parte de la EPA.

A continuación se presentan las ventajas de configurar el certificado de dispositivo en nFactor como componente de la EPA.

- El error en la validación del certificado de dispositivo no provoca un error de inicio de sesión. Según la configuración, el inicio de sesión puede continuar y el usuario se puede colocar en grupos con acceso limitado.
- Dado que la comprobación del certificado de dispositivo se basa en directivas, puede permitir o bloquear de forma selectiva el acceso a los recursos de la intranet corporativa en función de la autenticación del certificado de dispositivo. Por ejemplo, la autenticación de certificado de dispositivo se puede utilizar para proporcionar acceso condicional a la aplicación de Office 365 solo en los portátiles administrados corporativos.

La validación de certificados de dispositivo no puede formar parte de un análisis periódico de la EPA.

> **Importante:**
>
> - De forma predeterminada, Windows exige privilegios de administrador para acceder a los certificados de dispositivo. Para agregar la comprobación de certificados de dispositivo para usuarios que no son administradores, debe instalar el complemento VPN de la misma versión que el complemento EPA en el dispositivo.
> - Puede agregar varios certificados de CA a la puerta de enlace y validar el certificado de dispositivo.

### Configurar el certificado de dispositivo en nFactor como un componente EPA

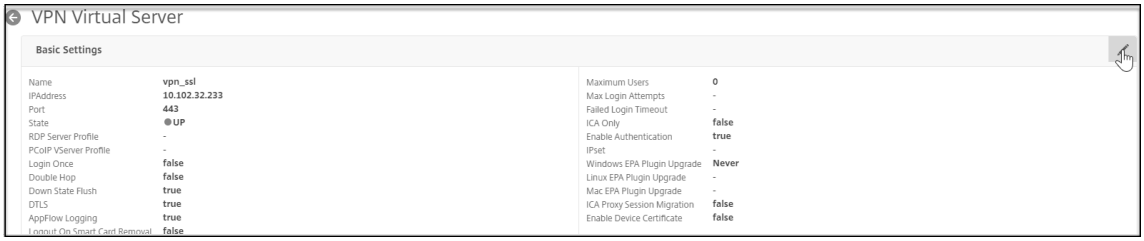
**Para configurar el certificado de dispositivo en nFactor como un componente de la EPA mediante la interfaz de línea de comandos, en la línea de comandos, escriba:**

```
add authentication epaAction epa-act -csecexpr sys.client_expr("device-cert_0_0") -defaultgroup epa_pass -quarantine_group epa_fail

<!--NeedCopy-->
```

**Para configurar el certificado de dispositivo en nFactor como un componente de la EPA para el servidor virtual VPN mediante la GUI de Citrix ADC:**

1. En la GUI de NetScaler, vaya a **Configuración > Citrix Gateway > Servidores virtuales**.
2. En la página **Servidores virtuales de Citrix Gateway**, seleccione el servidor virtual que desea modificar y haga clic en **Modificar**.
3. En la página **Servidor virtual VPN**, haga clic en el icono Modificar.

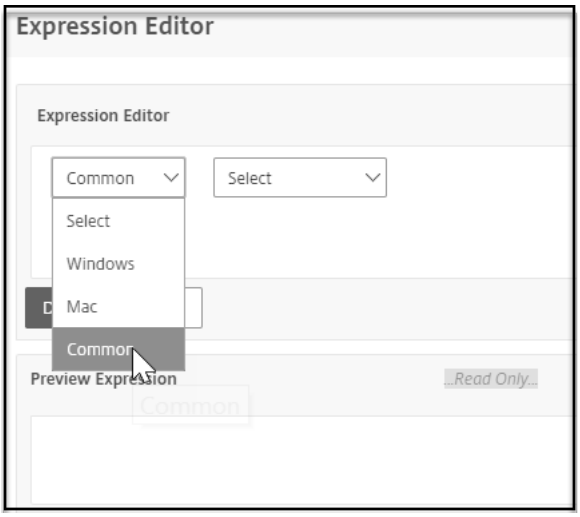



4. Haga clic en **Más**.
5. Haga clic en **Agregar** junto a la sección CA para certificado de dispositivo y, a continuación, haga clic en Aceptar.

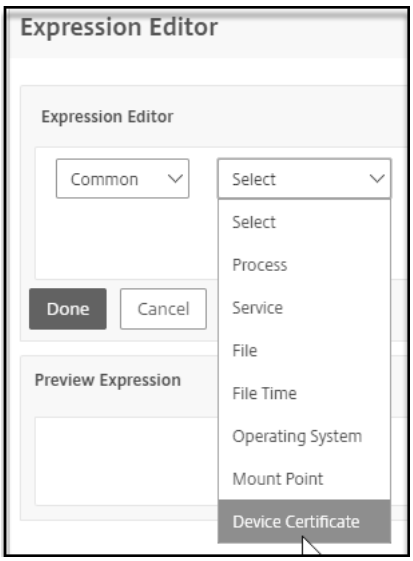

 

> No seleccione la casilla de verificación Habilitar certificado de dispositivo. Habilitarlo habilita la validación del certificado de dispositivo en la clásica EPA.

6. En la GUI de NetScaler, vaya a **Configuración > Seguridad > AAA —Tráfico de aplicaciones > Políticas > Autenticación > Políticas avanzadas > Acciones > EPA** .
7. En la página **Acción de autenticación EPA**, haga clic en **Agregar**. Puede hacer clic en **Modificar** para modificar una acción de la EPA existente.
8. En la página **Crear acción de EPA de autenticación**, proporcione los valores de los campos obligatorios para crear una acción de EPA de autenticación y haga clic en el enlace **Editor de EPA**.
9. Seleccione **Común** en el menú **Editor de expresiones**.




10. Seleccione **Certificado de dispositivo** en el menú siguiente que aparece y haga clic en **Listo** para completar la configuración.

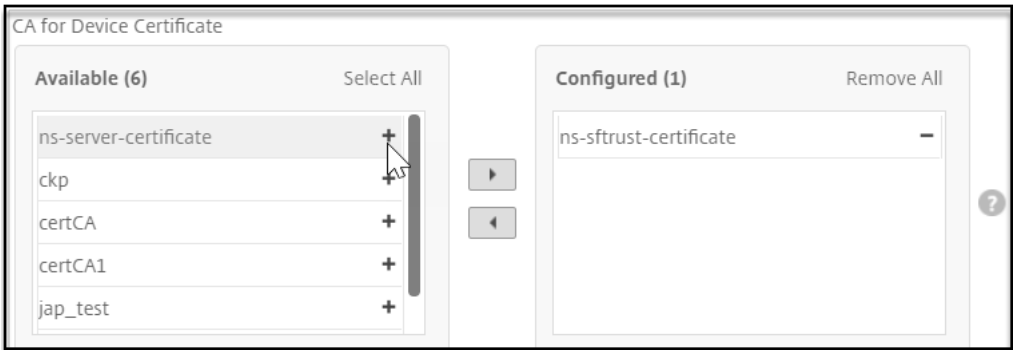


**Para configurar el certificado de dispositivo en nFactor como un componente EPA para el servidor virtual Citrix ADC AAA mediante la GUI de Citrix ADC:**

1. En la GUI de Citrix DC, vaya a **Seguridad > Tráfico de aplicaciones AAA > Servidores virtuales** .
2. En la página **Servidores virtuales de Citrix Gateway** , seleccione el servidor virtual que desea modificar y haga clic en Editar.
3. En la página **Servidor virtual de autenticación**, haga clic en el icono Modificar.
4. Haga clic en **Más**.
5. Haga clic en **Agregar** junto a la sección **CA para certificado de dispositivo**.


6. Seleccione el certificado que se va a agregar y haga clic en **Aceptar** para completar la configuración.




7. Repita el **paso 6 al paso 10** de la sección anterior para completar la configuración.