# Citrix SD-WAN Orchestrator para instalaciones locales 14.4

# Contents

**Notas de la versión de SD-WAN Orchestrator para instalaciones locales versión 14.4** 5

**Notas de la versión 14.3 de SD-WAN Orchestrator for On-premises** 5

**Notas de la versión 13.2.1 de SD-WAN Orchestrator for On-premises** 9

**Notas de la versión 13.2 de SD-WAN Orchestrator for On-premises** 10

**Notas de la versión 12.3 de SD-WAN Orchestrator for On-premises** 17

**Notas de la versión 11.4.0a de SD-WAN Orchestrator for On-premises** 21

**Notas de la versión 11.1 de Citrix SD-WAN Orchestrator for On-premises** 27

**Notas de la versión 10.3 de Citrix SD-WAN Orchestrator for On-premises** 32

**Notas de la versión 9.6 de Citrix SD-WAN Orchestrator for On-premises** 37

**Notas de la versión 1.0 de Citrix SD-WAN Orchestrator for On-premises** 39

**Requisitos e instalación del sistema** 41

**Diferencia entre el servicio SD-WAN Orchestrator for On-premises y el servicio Citrix SD-WAN Orchestrator** 44

**Instalación y configuración de SD-WAN Orchestrator para entornos locales en ESXi Server** 45

**Instalación y configuración de SD-WAN Orchestrator para entornos locales en XenServer** 54

**Incorporación de SD-WAN Orchestrator para entornos locales** 62

**Citrix SD-WAN Orchestrator para inicio de sesión local** 67

**Citrix SD-WAN Orchestrator para licencias locales** 75

**Conectividad con dispositivos Citrix SD-WAN** 79

**Configuración al nivel de proveedor** 94

**Inicio de red** 99

**Diferencia de configuración** 106

**Implementación** 109

**Definiciones de servicios** **128**

**Redirección** **142**

**Comunicación entre enlaces** **160**

**Seguridad** **163**

**Grupos de sitios y IP** **181**

**Configuración y grupos de aplicaciones** **191**

**Perfiles y plantillas** **208**

**Servicio de ubicación de red** **215**

**Equilibrio de carga ECMP** **217**

**Reglas de aplicación** **222**

**HDX QoE** **228**

**Reglas de direcciones IP** **244**

**Directivas de QoS** **252**

**Configuración del sitio** **256**

**Actualización de firmware LTE** **296**

**Protocolo de resolución de direcciones** **300**

**Protocolo de descubrimiento de vecinos** **300**

**Rutas virtuales** **302**

**Redirección dinámica** **307**

**Traducción de direcciones de red** **319**

**Protocolo de configuración dinámica de host** **330**

**Redirección de multidifusión** **333**

**Protocolo de redundancia de enrutador virtual** **339**

**Configuración del sistema de nombres de dominio** **344**

**Grupos de delegación de prefijos** **349**

**Grupos de agregación de enlaces** **350**

**Configuración del dispositivo** **354**

**Administración en banda** **381**

**Ver configuración (versión preliminar)** **390**

**Panel de proveedores** **394**

**Tablero de cliente/Red** **395**

**Panel del sitio** **400**

**Solución de problemas del proveedor** **403**

**Solución de problemas de red** **405**

**Solución de problemas del sitio** **408**

**Informes de proveedores** **411**

**Informes de cliente/red** **416**

**Informes del sitio** **444**

**Diagnóstico** **479**

**Anuncios** **481**

**Administración de usuarios** **483**

**Nombre del dominio** **491**

**Certificado HTTPS** **493**

**Administración del espacio en disco** **495**

**Reemplazar un dispositivo Citrix SD-WAN afectado** **499**

**Guía de API para Citrix SD-WAN Orchestrator for On-premises** **502**

**Administración del orquestador** **504**

**Diagnóstico del orquestador** **535**

**Alarmas** **538**

# Notas de la versión de SD-WAN Orchestrator para instalaciones locales versión 14.4

December 10, 2024

Este documento de notas de la versión describe las mejoras y los cambios, los problemas corregidos y conocidos que existen para la versión Build 14.4 de Citrix SD-WAN Orchestrator for On-premises.

## Notas

Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

## Problemas conocidos

Los problemas que existen en la versión 14.4.

La publicación de software SD-WAN en Citrix SD-WAN Orchestrator for On-premises puede generar el siguiente error:

`Failed to fetch software details from Citrix cloud.`

**Solución alternativa**: Cierre sesión y vuelva a iniciar sesión en Citrix Cloud a través de Citrix SD-WAN Orchestrator for On-premises y, luego, publique el software SD-WAN.

[ SDW-24980 ]

# Notas de la versión 14.3 de SD-WAN Orchestrator for On-premises

October 31, 2022

Este documento de notas de la versión describe las mejoras y los cambios, así como los problemas solucionados y conocidos que existen para la versión 14.3 de Citrix SD-WAN Orchestrator for On-premises.

## Notas

Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

## Novedades

Las mejoras y los cambios disponibles en la compilación 14.3.

### Configuración y administración

#### Directivas de QoS

La página de directivas de QoS se ha renovado para mejorar la experiencia del usuario. Las opciones, como las reglas de aplicación personalizadas, las reglas de la aplicación, las reglas de HDX, las reglas de grupos de aplicaciones, las reglas de IP y las reglas de protocolo IP predeterminadas, se han mejorado con una nueva apariencia.

[ SDW-11029 ]

### Plataforma y sistemas

**Mejoras en la IP de administración/IP en banda**:

Las columnas **IP de administración** y **Acceso al dispositivo** de las siguientes pantallas de la interfaz de usuario se han mejorado para mostrar la dirección IP dentro de banda o la dirección IP de administración en función del tipo de dirección IP que el dispositivo utiliza para comunicarse con Citrix SD-WAN Orchestrator for On-premises:

- Proveedor > Informes > Inventario > Detalles
- Cliente > Configuración > Inicio de la red > Acciones > Ver detalles
- Cliente > Informes > Inventario > Detalles
- Sitio > Panel de control > Dispositivos

[ SDW-23353 ]

#### Exportar informe como CSV

Con la función **Exportar como CSV**, puede descargar los puntos del gráfico de rutas (ruta virtual/de miembros) para cualquier serie temporal (horaria, semanal, etc.) como un archivo de valores separados por comas (CSV) de Excel y poder trazar todos los puntos de datos distintos para un informe de sitio en particular.

[ SDW-20988 ]

### Autenticación de certificados

Citrix SD-WAN Orchestrator for On-premises admite la autenticación de dispositivos para rutas virtuales estáticas y dinámicas mediante la infraestructura de clave pública (PKI) como función de seguridad adicional. La habilitación de la función amplía el mecanismo de autenticación de ruta virtual existente mediante la distribución de certificados PKI a través de la ruta de datos, por el dispositivo que inicia el intercambio. La mejora de PKI también admite la administración de listas de revocación de certificados (CRL) para la revocación centralizada de certificados comprometidos.

[ SDW-19295 ]

#### SD-WAN Orchestrator

### Ver configuración (versión preliminar)

Citrix SD-WAN Orchestrator for On-premises presenta la página **Ver configuración** al nivel de sitio. Esta página proporciona un resumen detallado de la configuración de un sitio en varios subsistemas.

[ SDW-22284 ]

### Estadísticas entiempo real al nivel de red, estadísticasen tiempo real al nivel de sitio

La **conexión de firewall** ahora pasa a llamarse **Firewall Statistics**. Las directivas de filtro y NAT se han agregado recientemente a la lista desplegable de tipos de estadísticas. Además, las opciones de estadísticas en tiempo real están reestructuradas y divididas en las siguientes categorías:

- Estadísticas de red
- Estadísticas de aplicación
- Estadísticas de rutas

[ SDW-20966 ]

### Configuración de banda ancha móvil y estado de banda ancha móvil

Ahora puede conectar el dispositivo Citrix SD-WAN desde su sitio a una red mediante una conexión a Internet de banda ancha. Este soporte de configuración y estado de banda ancha móvil está disponible para los módems internos. También puede ver el estado de la configuración de banda ancha de tu dispositivo y de la tarjeta SIM activa.

[ SDW-10907 ]

## Problemas resueltos

Problemas que se abordan en la compilación 14.3.

#### Configuración y administración

El certificado de PKI no aparecía en la interfaz de usuario de Citrix SD-WAN Orchestrator for On-premises. Este problema se producía porque el campo **Unidad organizativa** era obligatorio en el certificado de PKI.

[ SDW-23726 ]

#### Otros

Algunos sitios no pueden conectarse a la interfaz de usuario de Citrix SD-WAN Orchestrator for On-premises.

[ SDWANHELP-2601 ]

### Problemas conocidos

Los problemas que existen en la versión 14.3.

Los gráficos de aplicaciones y categorías de aplicaciones están vacíos en la página **Informes** > **Uso** > **Aplicaciones** de la interfaz de usuario de Citrix SD-WAN Orchestrator for On-premises.

[ SDW-23817 ]

La versión de software seleccionada anteriormente en la página **Implementación** > **Configuración** > **Actualización parcial del sitio** > **Versión de software** de la interfaz de usuario no se conserva cuando los usuarios vuelven a esta página.

**Solución alternativa**: Seleccione manualmente la versión del software de actualización parcial del sitio para cada sitio haciendo clic en **Implementación** > **Seleccionar sitios**.

[ SDW-22374 ]

A veces, la interfaz de usuario muestra un error después de realizar la configuración de la interfaz de administración. Sin embargo, la configuración se ha realizado correctamente y se requiere una actualización para que la configuración actualizada aparezca en la interfaz de usuario.

[ SDW-22139 ]

En una configuración administrada por un proveedor, los anuncios agregados por los administradores del proveedor no se muestran a los clientes al iniciar sesión.

[ SDW-18491 ]

# Notas de la versión 13.2.1 de SD-WAN Orchestrator for On-premises

October 31, 2022

Este documento de notas de la versión describe las mejoras y los cambios, así como los problemas solucionados y conocidos que existen para la versión 13.2.1 de Citrix SD-WAN Orchestrator for On-premises.

## Notas

Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

## Problemas resueltos

Problemas que se abordan en la compilación 13.2.1.

### Plataforma y sistemas

Citrix SD-WAN Orchestrator for On-premises envía paquetes de sincronización TCP al punto de enlace de AWS.

[ SDW-23477 ]

## Problemas conocidos

Los problemas que existen en la versión 13.2.1.

### Otros

Algunos sitios no pueden conectarse a la interfaz de usuario de Citrix SD-WAN Orchestrator for On-premises.

**Solución alternativa**: Utilice una subred diferente a la subred 172.17.x.x.

[ SDWANHELP-2601 ]

En algunos casos, después de implementar Cloud Direct en los sitios e implementar las configuraciones (preparación y activación), el servicio Cloud Direct no aparece.

**Solución alternativa**: habilite el servicio Cloud Direct de forma manual para cada sitio.

[ SDW-22493 ]

La versión de software seleccionada anteriormente en la página **Implementación** > **Configuración** > **Actualización parcial del sitio** > **Versión de software** de la interfaz de usuario no se conserva cuando los usuarios vuelven a esta página.

**Solución alternativa**: Seleccione manualmente la versión del software de actualización parcial del sitio para cada sitio; para ello, vaya a **Implementación** > **Seleccionar sitios**.

[ SDW-22374 ]

A veces, la interfaz de usuario muestra un error después de realizar la configuración de la interfaz de administración. Sin embargo, la configuración se ha realizado correctamente y se requiere una actualización para que la configuración actualizada aparezca en la interfaz de usuario.

[ SDW-22139 ]

En una configuración administrada por un proveedor, los anuncios agregados por los administradores del proveedor no se muestran a los clientes al iniciar sesión.

[ SDW-18491 ]

#### Plataforma y sistemas

No se puede acceder a la interfaz de usuario de uno de los dispositivos Citrix SD-WAN porque el proveedor de estadísticas de red está reutilizando una sesión y esto provoca que el proceso HTTPD no se comporte correctamente (en casos excepcionales).

[ SDW-23392 ]

En el dispositivo Citrix SD-WAN 210, si elimina la licencia complementaria SE, los servicios se inhabilitan.

**Solución alternativa**: Antes de eliminar una licencia complementaria de SE (o) pasar de una licencia AE a una SE, elimine las directivas de firewall que tienen el perfil de seguridad, configure el dispositivo como administración fuera de banda (si está configurada la administración dentro de banda) y, a continuación, continúe con la etapa y el proceso de activación para convierta el dispositivo en una edición estándar.

[ SDW-18031 ]

## Notas de la versión 13.2 de SD-WAN Orchestrator for On-premises

October 31, 2022

Este documento de notas de la versión describe las mejoras y los cambios, así como los problemas solucionados y conocidos que existen para la versión 13.2 de Citrix SD-WAN Orchestrator for On-premises.

## Notas

Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

## Novedades

Las mejoras y los cambios disponibles en la compilación 13.2.

### Configuración y administración

#### Restaurar la versión anterior

Citrix SD-WAN Orchestrator for On-premises presenta la funcionalidad Restaurar la versión anterior. Cuando se selecciona la opción **Restaurar la versión anterior**, Citrix SD-WAN Orchestrator for On-premises inicia una activación en toda la red de la configuración anterior y restaura la configuración (/software) previamente activada en la red.

[ SDW-22042 ]

#### Mejoras en las licencias

Una vez recuperadas las licencias y actualizadas a producción, la etiqueta del botón **Actualizar a producción** cambia a **Actualizada a producción**, lo que indica que la actualización de la licencia ya se ha realizado.

[ SDW-20674 ]

**API: Resolución de direcciones de sitios**:

Cuando se crea un sitio mediante una API, la dirección del sitio se obtiene automáticamente mediante los valores de latitud y longitud, que se transfieren como parte de la creación del sitio, mediante la API de Google Maps.

[ SDW-20654 ]

#### Reestructura del menú de red

El menú de configuración global de Citrix SD-WAN Orchestrator for On-premises se ha reestructurado para ayudar a categorizar y descubrir mejor las funciones clave de Citrix SD-WAN. Además, cada servicio de entrega ahora está disponible tanto en los canales de entrega como en todas las páginas de

funciones clave para adaptarse a la configuración del administrador desde el contexto global o por función. Por ejemplo, un administrador puede configurar el servicio Citrix SIA de forma global en un canal de entrega el día 0 y también puede realizar las funciones del día N en Seguridad en los servicios de seguridad en la nube para realizar cualquier cambio.

Las páginas de configuración al nivel de red se mejoran de la siguiente manera:

- El nombre de**Network Config Home** pasa a llamarse **Network Home**.
- **Los servicios de entrega**, en **Configuración > Canales de entrega**, ahora pasan a llamarse **Definiciones de servicios**.
- En **Configuración > Seguridad**, la página **de cifrado de red** pasa a llamarse **Seguridad de red**.
- Las páginas de **Configuración > Seguridad** se agrupan de forma lógica de la siguiente manera para facilitar su detección:

| Grupo | Opciones de menú |
|---|---|
| Seguridad de superposición de SD-WAN | Seguridad de red |
| | Ruta virtual IPSec |
| Firewall base | Zona de firewall |
| | Valores predeterminados del firewall |
| | Directivas de firewall |
| IPsec y GRE | Certificados |
| | Perfiles de cifrado IPSec |
| | Servicio IPsec |
| | Servicio GRE |
| Seguridad de Wi-Fi | Perfiles RADIUS |
| | Perfiles SSID |

- Puede configurar los siguientes servicios desde **Configuración > Canales de entrega > Definición del servicio** o desde **Configuración > Seguridad**:
  - IPsec
  - GRE
- La página **Grupos de ECMP** se mueve a **Configuración > Enrutamiento**.
- Puede configurar **BGP, OSPF, grupos de multidifusión y VRRP** al nivel de red en **Configuración > Enrutamiento**. Puede seleccionar un sitio y hacer clic en **Ir**. Le lleva a la página de

configuración específica al nivel de sitio. Anteriormente, estas configuraciones solo estaban disponibles al nivel de sitio.

- Puede configurar el servicio Cloud Direct desde **Configuración > Canales de entrega > Definición del servicio** o desde **Configuración > Enrutamiento > SaaS y Cloud On Ramp**
- La página de **configuración de aplicaciones y DNS** pasa a llamarse **Configuración y grupos de aplicaciones**.
- Los ajustes relacionados con el DPI que antes estaban en **Configuración > Ajustes de aplicaciones y DNS > Ajustes de la aplicación** se han movido a **Configuración > Ajustes y grupos de aplicaciones > Ajustes de DPI**.
- La página**Servicio de ubicación de red**, que estaba en **Configuración > Servicios de entrega**, se encuentra directamente en **Configuración.**

[ SDW-14698 ]

### Reversión en caso de error

Durante la implementación de la red (activación), los sitios que no se pueden conectar a Citrix SD-WAN Orchestrator for On-premises vuelven a la versión anterior para intentar restaurar la conectividad. La reversión en dichos sitios consiste en que la publicación se inicia sin conexión durante un tiempo específico (actualmente 30 minutos).

Si alguno de los sitios de la red está intentando revertir, aparece un cuadro emergente con dos opciones para deshacer toda la red o ignorarlos y finalizar la implementación.

La función de reversión en caso de error debe estar habilitada antes de iniciar una implementación de red.

[ SDW-11153 ]

## Otros

### Reglas de IP

La opción Anular servicio se agrega en la sección **Reglas IP > Directiva de tráfico de rutas virtuales**. Cuando la **Directiva de tráfico** se selecciona como **Servicio de anulación**, puede seleccionar el tipo de servicio (Intranet, Internet, transferencia o descarte) que el servicio de rutas virtuales anula.

[ SDW-22213 ]

### Diferencia de configuración

Se ha agregado recientemente una función **Config Diff** al nivel de red, en **Configuración**. La función **Config Diff** le ayuda a revisar la diferencia entre dos versiones de los puntos de control de configuración. También puede ver las configuraciones a nivel global y de sitio.

[ SDW-4563 ]

### Configuración del dispositivo

Citrix SD-WAN Orchestrator for On-premises presenta una opción para configurar la prioridad de la red de administración. Puede seleccionar Dentro de banda o Fuera de banda como interfaz de administración de la red. Esta opción solo está disponible si el dispositivo SD-WAN ejecuta una versión de software 11.4.2 o una posterior.

[ NSSDW-35774 ]

## Plataforma y sistemas

### Autenticación de certificados

Citrix SD-WAN Orchestrator for On-premises admite la autenticación de dispositivos para rutas virtuales estáticas y dinámicas mediante la infraestructura de clave pública (PKI) como función de seguridad adicional. La habilitación de la función amplía el mecanismo de autenticación de ruta virtual existente mediante la distribución de certificados PKI a través de la ruta de datos, por el dispositivo que inicia el intercambio. La mejora de PKI también admite la administración de listas de revocación de certificados (CRL) para la revocación centralizada de certificados comprometidos.

[ SDW-19295 ]

Mejoras en elregistro de auditoría de proveedoresy el registro de auditoría

Las páginas de **registros de auditoría de proveedores** y **registros de auditoría de red** se han mejorado con las siguientes opciones:

- **IP de origen**: Este campo muestra la dirección IP del punto final desde el que se configura una función de SD-WAN. Este campo se muestra en la página **Registros de auditoría** y en la página **Información de auditoría**.
- **Exportar como CSV**: Esta opción le permite exportar los registros de auditoría a un formato CSV.
- **Qué ha cambiado**: Esta sección muestra los registros de todos los cambios realizados en las funciones a través de la interfaz de usuario. Active el botón **Registrar cargas útiles** para ver esta sección en la página de **información de auditoría**. Actualmente, esta sección está disponible en la página de información de auditoría de red.

[ SDW-19219 ]

### Puertos personalizados, configuración de protocolos para aplicaciones basadas en nombres de dominio

Las aplicaciones basadas en nombres de dominio ahora admiten puertos y protocolos configurables en Citrix SD-WAN Orchestrator for On-premises. Si selecciona la casilla **Configurar puerto**, puede modificar, agregar o eliminar cualquier puerto o el intervalo de puertos según sea necesario. Además,

puede cambiar/seleccionar el protocolo como TCP, UDP o Cualquiera. Antes (y con la casilla Configurar puerto desmarcada), solo se admitían los puertos 80 y 443 y el protocolo **Cualquiera** para los dominios agrupados en una aplicación.

[ NSSDW-29930 ]

## Problemas resueltos

Problemas que se abordan en la compilación 13.2.

### Otros

No se puede acceder a la interfaz de usuario de Citrix SD-WAN Orchestrator for on-premises. Este problema se produce cuando los servicios que se ejecutan en {page.productname}} no responden a las solicitudes de latidos y se supera el límite de reinicios.

[ SDWANHELP-2544 ]

Se produce un error al cargar el paquete de actualización de software en Citrix SD-WAN Orchestrator for On-premises. Este problema se produce cuando un usuario se aleja de la página de carga cuando se está cargando el paquete de software.

[ SDWANHELP-2495 ]

### Plataforma y sistemas

Un dispositivo SD-WAN que ejecute una versión de software de 11.4.1 pasa al modo Grace cuando se asignan licencias al dispositivo desde Citrix SD-WAN Orchestrator for On-premises.

[ SDW-23171 ]

## Problemas conocidos

Los problemas que existen en la versión 13.2.

### Configuración y administración

En una instancia de Citrix SD-WAN Orchestrator for On-premises recién importada, el almacenamiento provisional queda atascado en el estado **Preparando el paquete**. Este problema se produce cuando el proceso de preparación se inicia poco después de crear una nueva máquina virtual.

**Solución alternativa**: Vuelva a intentar el proceso de preparación.

[ SDW-20863 ]

### Otros

El estado del servicio de un dispositivo SD-WAN que ejecuta una versión de software de 11.4.2 aparece como **INCORRECTO** en la interfaz de usuario de Citrix SD-WAN Orchestrator for On-premises. El mensaje de error que aparece es **No responde de la URL de Orchestrator**. Este problema se produce cuando se configura un dominio personalizado en Citrix SD-WAN Orchestrator for On-premises.

**Solución alternativa**: Reinicie el dispositivo SD-WAN.

[ SDW-23322 ]

La operación **Restaurar la versión anterior** falla y se muestra el mensaje de error de **activación fallida (ER101)** para los sitios de la PSU cuando se modifica la lista de actualizaciones parciales del sitio y se realiza una administración de cambios (etapa y activación) en una red.

**Solución alternativa**: Realice otra ronda de administración de cambios antes de aplicar la acción **Restaurar la versión anterior**.

[ SDW-23227 ]

En algunos casos, después de implementar Cloud Direct en los sitios e implementar las configuraciones (preparar y activar), el servicio Cloud Direct no aparece.

**Solución alternativa**: habilite el servicio Cloud Direct de forma manual para cada sitio.

[ SDW-22493 ]

La versión de software seleccionada anteriormente en la página **Implementación** > **Configuración** > **Actualización parcial del sitio** > **Versión de software** de la interfaz de usuario no se conserva cuando los usuarios vuelven a esta página.

**Solución alternativa**: Seleccione manualmente la versión del software de actualización parcial del sitio para cada sitio haciendo clic en **Implementación** > **Seleccionar sitios**.

[ SDW-22374 ]

A veces, la interfaz de usuario muestra un error después de realizar la configuración de la interfaz de administración. Sin embargo, la configuración se ha realizado correctamente y se requiere una actualización para que la configuración actualizada aparezca en la interfaz de usuario.

[ SDW-22139 ]

En una configuración administrada por un proveedor, los anuncios agregados por los administradores del proveedor no se muestran a los clientes al iniciar sesión.

[ SDW-18491 ]

### Plataforma y sistemas

El cliente no puede enviar notificaciones push a su propio servidor HTTP.

[ SDW-23134 ]

## Notas de la versión 12.3 de SD-WAN Orchestrator for On-premises

July 15, 2023

Este documento de notas de la versión describe las mejoras y los cambios, así como los problemas solucionados y conocidos que existen para la versión 12.3 de Citrix SD-WAN Orchestrator for On-premises.

### Nota

Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

### Novedades

Las mejoras y los cambios disponibles en la compilación 12.3.

#### Otros

##### Configuración de purga

Citrix SD-WAN Orchestrator for On-premises le permite borrar datos históricos más antiguos que los días del intervalo de estadísticas de purga (30 días de forma predeterminada). Cuando se borran los datos, los datos históricos anteriores al número de días seleccionado se eliminan y ya no están disponibles. El proceso de purga se lleva a cabo alrededor de las 12:48 a. m., todos los días, según la zona horaria establecida en el dispositivo SD-WAN.

[ SDW-20402 ]

##### Interfaz de implementación sin interacción

Puede habilitar una interfaz de implementación sin intervención (ZTD) en Citrix SD-WAN Orchestrator for On-premises. La interfaz ZTD, que está protegida mediante la autenticación bidireccional, proporciona una interfaz de comunicación segura para los dispositivos SD-WAN y Citrix SD-WAN Orchestrator para entornos locales.

[ SDW-19152 ]

### Configuración de la ruta virtual para el enlace

Puede personalizar los anchos de banda para las rutas virtuales y las rutas virtuales dinámicas asociadas a un enlace WAN. Esta función es útil cuando algunos sitios muestran señales de degradación del rendimiento debido a problemas de ancho de banda.

[ SDW-9760 ]

#### SD-WAN Orchestrator

### Configuración del servidor Syslog

Citrix SD-WAN Orchestrator for On-premises admite la configuración del servidor Syslog para los dispositivos SD-WAN. Al habilitar la configuración de Syslog, puede enviar alertas del sistema y detalles de eventos de los dispositivos SD-WAN a un servidor syslog externo.

[ SDW-13990 ]

## Problemas resueltos

Problemas que se abordan en la compilación 12.3.

#### Otros

En determinadas condiciones, el dispositivo SD-WAN no se comunica con Citrix SD-WAN Orchestrator para la administración local a través de la administración dentro de banda cuando la administración dentro de banda está habilitada y la administración fuera de banda está conectada.

[ SDWANHELP-2368 ]

La interfaz de usuario muestra un error de forma incorrecta cuando el valor de las rutas virtuales dinámicas se establece en más de 8, aunque el límite máximo permitido es 32. Este problema se observa en los dispositivos VPXL y 4100 SE.

[ SDWANHELP-2354 ]

La lista desplegable de **versiones de software** en la configuración de actualización parcial del sitio muestra todas las versiones de software compatibles en lugar de mostrar solo las versiones publicadas en **Infraestructura** > **Administración de Orchestrator** > **Imágenes de software** > **Dispositivo**.

Si una versión de software incluida en Actualización parcial del sitio no está disponible para su publicación en **Infraestructura** > **Administración de Orchestrator** > **Imágenes de software** > **Dispositivo**, no se puede realizar una actualización parcial del sitio para esa versión.

[ SDW-20992 ]

## Problemas conocidos

Los problemas que existen en la versión 12.3.

### Configuración y administración

En una instancia de Citrix SD-WAN Orchestrator for On-premises recién importada, el almacenamiento provisional queda atascado en el estado **Preparando el paquete**. Este problema se produce cuando el proceso de preparación se inicia poco después de crear una nueva máquina virtual.

**Solución alternativa**: Vuelva a intentar el proceso de preparación.

[ SDW-20863 ]

### Otros

Citrix SD-WAN Orchestrator for On-premises que ejecuta VMware ESXi 13 no se reinicia y pasa a un estado incorrecto.

**Solución alternativa**: Utilice VMware ESXi versión 9.

[ SDWANHELP-2182 ]

En algunos casos, después de implementar Cloud Direct en los sitios e implementar las configuraciones (preparar y activar), el servicio Cloud Direct no aparece.

**Solución alternativa**: habilite el servicio Cloud Direct de forma manual para cada sitio.

[ SDW-22493 ]

El proceso de preparación falla de forma intermitente cuando los usuarios realizan una actualización parcial del sitio. La interfaz de usuario muestra el mensaje de error Error de **puesta en escena debido a una excepción**.

**Solución alternativa**: Vuelva a intentar el proceso de preparación.

[ SDW-22398 ]

La versión de software seleccionada anteriormente en la página **Implementación** > **Configuración** > **Actualización parcial del sitio** > **Versión de software** de la interfaz de usuario no se conserva cuando los usuarios vuelven a esta página.

**Solución alternativa**: Seleccione manualmente la versión del software de actualización parcial del sitio para cada sitio haciendo clic en **Implementación** > **Seleccionar sitios**.

[ SDW-22374 ]

A veces, la interfaz de usuario muestra un error después de realizar la configuración de la interfaz de administración. Sin embargo, la configuración se ha realizado correctamente y se requiere una actualización para que la configuración actualizada aparezca en la interfaz de usuario.

[ SDW-22139 ]

Los usuarios no pueden eliminar el archivo de imagen **tar.gz** de Citrix SD-WAN Orchestrator for On-premises cargado en la página **Infraestructura** > **Administración de Orchestrator** > **Imágenes de software** de la interfaz de usuario. El mensaje de error que aparece es **Se produjo un error al eliminar el paquete de software**.

**Solución alternativa**: Cargue un paquete de software nuevo. El archivo cargado anteriormente se elimina automáticamente.

[ SDW-22137 ]

En la página **principal**Configuración > Configuración**de red** de la interfaz de usuario, el estado de conectividad de Orchestrator para un dispositivo SD-WAN secundario aparece en línea inmediatamente después de cargar el archivo de configuración. Sin embargo, se muestra el estado correcto después de guardar la configuración del sitio.

[ SDW-20913 ]

En una configuración administrada por un proveedor, los anuncios agregados por los administradores del proveedor no se muestran a los clientes al iniciar sesión.

[ SDW-18491 ]

Cuando la copia de seguridad de la base de datos de un dispositivo se restaura en otro dispositivo que tenga la misma versión de Citrix SD-WAN Orchestrator for On-premises, los detalles del usuario no se restauran. En el dispositivo restaurado, si crea un usuario con el mismo nombre de usuario que en la base de datos de la copia de seguridad, aparece el siguiente error:

`User has a role already assigned`.

**Solución alternativa**: Cree un usuario con un nombre de usuario diferente que no exista en la base de datos de la que se realizó la copia de seguridad.

[ SDW-15984 ]

#### Plataforma y sistemas

En el dispositivo Citrix SD-WAN 210, si elimina la licencia complementaria, los servicios se inhabilitan.

**Solución alternativa**: Elimine la directiva de firewall que contiene el perfil de seguridad, organice y active los cambios para convertir el dispositivo a la edición estándar.

[ SDW-18031 ]

# Notas de la versión 11.4.0a de SD-WAN Orchestrator for On-premises

July 15, 2023

Este documento de notas de la versión describe las mejoras y los cambios, así como los problemas solucionados y conocidos que existen para la versión 11.4.0a de Citrix SD-WAN Orchestrator for On-premises.

## Notas

- Citrix SD-WAN Orchestrator for On-premises 11.4.0a soluciona el problema descrito en SDWANHELP-2317 y reemplaza a la versión 11.4.
- Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

## Novedades

Las mejoras y los cambios que están disponibles en la compilación 11.4.0a.

### Configuración y administración

#### Proxy HTTP

Puede configurar la configuración del proxy HTTP en Citrix SD-WAN Orchestrator for On-premises. Esta función centraliza la administración de todas las solicitudes salientes realizadas a Citrix Cloud. Los administradores pueden dirigir las solicitudes salientes desde Citrix SD-WAN Orchestrator for On-premises a Citrix Cloud a través de un servidor proxy HTTP.

[ SDW-20247 ]

#### Servicio Cloud Direct

Citrix SD-WAN Orchestrator for On-premises admite el servicio Cloud Direct.

El servicio Cloud Direct ofrece funcionalidades de SD-WAN como un servicio en la nube a través de una entrega confiable y segura de todo el tráfico con destino a Internet, independientemente del entorno de alojamiento (centro de datos, nube e Internet).

El servicio Cloud Direct mejora la visibilidad y la administración de la red. Permite a los socios ofrecer servicios gestionados de SD-WAN para aplicaciones SaaS críticas para el negocio a sus clientes finales.

[ SDW-16396 ]

### Administración del almacenamiento: Disponibilidad general

La función de administración de almacenamiento ahora admite la disponibilidad general.

Citrix SD-WAN Orchestrator for On-premises admite la migración de la configuración y los datos de un disco a otro. Puede realizar la migración del disco para aumentar el espacio en disco o para la recuperación ante desastres.

- **Agregar un disco nuevo**: Puede agregar un disco nuevo con un tamaño de almacenamiento al menos el doble del de los datos actuales consumidos por Citrix SD-WAN Orchestrator for On-premises.
- **Recuperación ante desastres**: En caso de desastre, puede conectar el disco que contiene la configuración y los datos de Citrix SD-WAN Orchestrator for On-premises a una nueva instancia de la máquina virtual Citrix SD-WAN Orchestrator for On-premises.

[ SDW-21316 ]

### Implementación sin intervención mediante la intermediación en la nube: Disponibilidad general

La función de implementación sin interacción ofrecida en la nube ahora es compatible con la disponibilidad general.

La implementación sin intervención mediante intermediación en la nube es un proceso automatizado que implica a Citrix SD-WAN Orchestrator for On-premises como agente para establecer la conectividad entre Citrix SD-WAN Orchestrator for On-premises y los dispositivos Citrix SD-WAN.

[ SDW-21312 ]

### Versión 11.4.1 de Citrix SD-WAN

La versión 11.4.1 de Citrix SD-WAN es compatible con Citrix SD-WAN Orchestrator for On-premises 11.4.

[ SDW-21082 ]

## Plataforma y sistemas

### sondeo ICMP

Citrix SD-WAN Orchestrator for On-premises admite el sondeo ICMP. Permite a los administradores determinar la accesibilidad de Internet hacia/desde el dispositivo SD-WAN y el host de destino. Se introducen los siguientes servicios de ICMP en la interfaz de usuario:

- Determine la accesibilidad a Internet desde un enlace mediante sondas ICMP
- Dirección de punto final ICMP IPv4
- Intervalo de sonda (en segundos)

- Reintentos

[ SDW-19292 ]

### Anular la configuración del nodo de tránsito global

Ahora puede anular la configuración del nodo de tránsito global y elegir habilitar o inhabilitar el desvío radio a radio y la exportación de rutas solo en los nodos de control de tránsito seleccionados.

[ SDW-19276 ]

**API de estadísticas de rutas de miembros (versión preliminar)**:

La API de estadísticas de rutas de miembros se modifica para permitir que el cliente de la API especifique los campos de interés. Los campos especificados se devuelven en la carga de respuesta.

[ SDW-18903 ]

### Informes del sitio: VRRP

El informe VRRP proporciona un informe en tiempo real de los grupos de VRRP configurados.

[ SDW-12082 ]

### Informes del sitio: IGMP

La tabla de informes de IGMP proporciona un informe en tiempo real de las estadísticas de IGMP y los grupos de proxy IGMP.

[ SDW-12077 ]

### Informes del sitio: IPSec

Los informes de IPSec proporcionan el informe en tiempo real de las configuraciones del túnel IPSec en la red.

[ SDW-12076 ]

### Informes del sitio: Protocolos de enrutamiento

El informe **de protocolos de enrutamiento** proporciona los detalles de los parámetros asociados a los protocolos de enrutamiento. Puede elegir el protocolo de la lista desplegable **Ver** un dominio de enrutamiento de la lista desplegable **Dominio de enrutamiento**, según sea necesario. Para ver los datos actuales, haga clic en **Recuperar datos más recientes**.

[ SDW-12075 ]

### Registrosde auditoría de proveedores, registros de auditoría de red

Las páginas de registro de auditoría al nivel de proveedor y de red se han mejorado con las siguientes capacidades:

- **Búsqueda**: Posibilidad de buscar una actividad de auditoría basada en una palabra clave.

- **Filtrado**: Ejecute una búsqueda en el registro de auditoría filtrando según el usuario, la función y el intervalo de tiempo. Para los registros al nivel de red, también puede filtrar por sitio.
- **Información de auditoría**: Seleccione el icono de información en la columna **Acción** para ir a la sección **Información de auditoría**. En esta sección se proporciona la siguiente información:
- **Método: método**de solicitud HTTP de la API invocada.
- **Estado**: Resultado de la solicitud de API. Aparece un mensaje de error cuando se produce un error en la solicitud de API.
- **Mensaje de carga**: Cuerpo del mensaje de solicitud enviado a través de la API.
- **URL**: URL HTTP de la API revocada.
- **Registrar cargas útiles**: De forma predeterminada, esta opción está inhabilitada. Cuando se habilita, el cuerpo de la solicitud del mensaje de la API se muestra en la sección **Información de auditoría**.

[ SDW-18937 ]

#### componente de selección de sitios

Se ha mejorado la usabilidad del componente de selección de sitios en las siguientes configuraciones para mejorar su usabilidad:

1. Actualización parcial del sitio
2. Servicio de ubicación de red
3. Directivas de enrutamiento
4. Directivas de QoS
5. Importar filtros de ruta
6. Exportar filtros de ruta
7. Configuración automática del proxy
8. Prevención de intrusiones
9. Directivas de firewall
10. Parámetros de la aplicación

[ SDW-16895 ]

### Problemas resueltos

Problemas que se abordan en la compilación 11.4.

#### Otros

La función ZTD negociada en la nube depende del servicio SD-WAN Orchestrator para que funcione. Esto se abordará en una próxima versión de SD-WAN Orchestrator. Sin embargo, los clientes no nece-

sitan actualizar su Citrix SD-WAN Orchestrator for On-premises.

[ SDW-20307 ]

La configuración de ZTD en la nube de SD-WAN no funciona para los sitios de HA si la ZTD en la nube ya está configurada en un sitio principal.

[ SDW-20208 ]

Citrix SD-WAN Orchestrator for On-premises muestra el estado **No conectado**, aunque el dispositivo SD-WAN esté conectado a Citrix SD-WAN Orchestrator for On-premises.

[ SDW-18280 ]

## Problemas conocidos

Los problemas que existen en la versión 11.4.

### Configuración y administración

En una instancia de Citrix SD-WAN Orchestrator for On-premises recién importada, el almacenamiento provisional queda atascado en el estado **Preparando el paquete**. Este problema se produce cuando el proceso de preparación se inicia poco después de crear una nueva máquina virtual.

**Solución alternativa**: Vuelva a intentar el proceso de preparación.

[ SDW-20863 ]

### Otros

El proceso de preparación falla cuando los usuarios que ejecutan Citrix SD-WAN Orchestrator for On-premises 11.4 actualizan sus dispositivos Citrix SD-WAN a la versión 11.4.1. La interfaz de usuario muestra el **estado como Fallo de ensayo (no se pudieron descargar los archivos de script)**. Este problema se produce cuando el ancho de banda entre el dispositivo Citrix SD-WAN y Citrix SD-WAN Orchestrator for On-premises es menor.

[ SDWANHELP-2317 ]

Citrix SD-WAN Orchestrator for On-premises que ejecuta VMware ESXi 13 no se reinicia y pasa a un estado incorrecto.

**Solución alternativa**: Utilice VMware ESXi versión 9.

[ SDWANHELP-2182 ]

La interfaz de usuario muestra una versión incorrecta del software del dispositivo SD-WAN en las páginas **Configuración > Configuración** de **red Inicio** y **Configuración** > **Implementación**. Este problema se produce en las instancias locales de Citrix SD-WAN Orchestrator que se acaban de instalar y antes de que los usuarios realicen una administración de cambios.

[ SDW-21018 ]

La interfaz de usuario no muestra ningún mensaje de error cuando se produce un error en la operación del sitio de Cloud Direct.

[ SDW-21009 ]

La lista desplegable de **versiones de software** en la configuración de actualización parcial del sitio muestra todas las versiones de software compatibles en lugar de mostrar solo las versiones publicadas en **Infraestructura** > **Administración de Orchestrator** > **Imágenes de software** > **Dispositivo**.

Si una versión de software incluida en Actualización parcial del sitio no está disponible para su publicación en **Infraestructura** > **Administración de Orchestrator** > **Imágenes de software** > **Dispositivo**, no se puede realizar una actualización parcial del sitio para esa versión.

[ SDW-20992 ]

En la página **principal**Configuración > Configuración**de red** de la interfaz de usuario, el estado de conectividad de Orchestrator para un dispositivo SD-WAN secundario aparece en línea inmediatamente después de cargar el archivo de configuración. Sin embargo, se muestra el estado correcto después de guardar la configuración del sitio.

[ SDW-20913 ]

En una configuración administrada por un proveedor, los anuncios agregados por los administradores del proveedor no se muestran a los clientes al iniciar sesión.

[ SDW-18491 ]

Cuando la copia de seguridad de la base de datos de un dispositivo se restaura en otro dispositivo que tenga la misma versión de Citrix SD-WAN Orchestrator for On-premises, los detalles del usuario no se restauran. En el dispositivo restaurado, si crea un usuario con el mismo nombre de usuario que en la base de datos de la copia de seguridad, aparece el siguiente error:

```
User has a role already assigned
```

**Solución alternativa**: Cree un usuario con un nombre de usuario diferente que no exista en la base de datos de la que se realizó la copia de seguridad.

[ SDW-15984 ]

# Notas de la versión 11.1 de Citrix SD-WAN Orchestrator for On-premises

July 15, 2023

Este documento de notas de la versión describe las mejoras y los cambios, así como los problemas solucionados y conocidos que existen para la versión 11.1 de Citrix SD-WAN Orchestrator for On-premises.

## Notas

Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

## Novedades

Mejoras y cambios que están disponibles en la versión 11.1.

### Versión 11.4.0a de Citrix SD-WAN

La versión 11.4.0a de Citrix SD-WAN es compatible con Citrix SD-WAN Orchestrator for On-premises.

[ SDW-19785 ]

### Versión 11.3.2 de Citrix SD-WAN

La versión 11.3.2 de Citrix SD-WAN es compatible con Citrix SD-WAN Orchestrator for On-premises.

[ SDW-19038 ]

### Resumen de rutas

Citrix SD-WAN Orchestrator for On-premises presenta una mejora en la funcionalidad de resumen de rutas. Con esta mejora, puede agregar rutas resumidas sin especificar la dirección IP de la puerta de enlace.

[ SDW-19404 ]

### Equilibrio de carga ECMP

Los grupos de rutas múltiples de igual coste (ECMP) permiten agrupar varias rutas, con el mismo coste, destino y tipo de servicio. El equilibrio de carga ECMP garantiza:

- Distribución del tráfico a través de múltiples conexiones de igual coste.
- Uso óptimo del ancho de banda disponible.
- Transferencia dinámica de tráfico a otra ruta miembro ECMP, si una ruta se vuelve inalcanzable.

- Los grupos ECMP se pueden formar a través de rutas virtuales e intranet servicios.

[ SDW-17452 ]

### Administración del almacenamiento (versión preliminar)

Citrix SD-WAN Orchestrator for On-premises admite la migración de la configuración y los datos de un disco a otro. Puede realizar la migración del disco para aumentar el espacio en disco o para la recuperación ante desastres.

- **Agregar un disco nuevo**: Puede agregar un disco nuevo con un tamaño de almacenamiento al menos el doble del de los datos actuales consumidos por Citrix SD-WAN Orchestrator for On-premises.
- **Recuperación ante desastres**: En caso de desastre, puede conectar el disco que contiene la configuración y los datos de Citrix SD-WAN Orchestrator for On-premises a una nueva instancia de la máquina virtual Citrix SD-WAN Orchestrator for On-premises.

[ SDW-16404 ]

### Implementación sin intervención mediante intermediación en la nube (versión preliminar)

La implementación sin intervención mediante intermediación en la nube es un proceso automatizado que implica a Citrix SD-WAN Orchestrator for On-premises como agente para establecer la conectividad entre Citrix SD-WAN Orchestrator for On-premises y los dispositivos Citrix SD-WAN.

[ SDW-11614 ]

### Mejoras en los nodos de tránsito

La habilitación de la comunicación de concentrador y radio como parte de la configuración global permite que todos los sitios utilicen los nodos de control como nodos de tránsito, de forma predeterminada, para la comunicación de sitio a sitio. Las preferencias específicas del sitio para los nodos de tránsito de superposición virtual permiten anular la configuración global del nodo de tránsito de superposición virtual para todos los sitios de la red. También puede elegir un nodo que no sea control como nodo de tránsito principal de un sitio.

[ SDW-12443 ]

Soporte de plano de datos IPv6

Citrix SD-WAN Orchestrator for On-premises admite direcciones IPv6 para las siguientes configuraciones de dispositivos Citrix SD-WAN con la versión 11.3.1 o superior del software Citrix SD-WAN:

- Servidor DNS
- Flujos
- Conexiones de firewall
- Grupos IP
- Regiones

- cliente DHCP
- Reglas de propiedad intelectual y reglas de aplicación
- Traducción de direcciones de red
- Servicio GRE
- Interfaces
- Servicio de Internet
- Protocolo de descubrimiento de vecinos
- Grupo de delegación de prefijos
- Servicio IPsec
- Configuración de HA
- Rutas IP
- Administración en banda
- Configuración de DNS
- Conjunto de opciones de servidor DHCP, retransmisión DHCP y DHCP

[ SDW-19194 ]

### Problemas resueltos

Los problemas que se abordan en la versión 11.1.

Las versiones del dispositivo SD-WAN anteriores a la 11.2.0 no pueden conectarse a Citrix SD-WAN Orchestrator para versiones locales inferiores a la 11.1. La versión recomendada de Citrix SD-WAN Orchestrator for On-premises 11.1 es la versión recomendada si los usuarios desean conectar sus dispositivos SD-WAN que ejecuten una versión de software inferior a la 11.2.0.

[ SDW-20220 ]

Cuando se produce un error al actualizar la cuenta de un cliente a la de producción, la interfaz de usuario no muestra el mensaje de error.

[ SDW-19574 ]

La actualización a la producción falla en Citrix SD-WAN Orchestrator for On-premises, para los clientes de prepago que solo tienen licencias perpetuas.

[ SDW-19558 ]

La asignación de licencias perpetuas a los sitios falla en Citrix SD-WAN Orchestrator for On-premises.

[ SDW-19556 ]

Cuando se produce un error al asignar licencias, la interfaz de usuario no muestra el mensaje de error en **Administración** > **Licencias**.

[ SDW-19238 ]

Aunque el administrador del cliente no tiene acceso para eliminar los servidores de autenticación remota, la interfaz de usuario muestra el icono de eliminación. Sin embargo, cuando el administrador del cliente intenta realizar la operación de eliminación, aparece el siguiente error:

```
User is not authorized to perform this operation.
```

[ SDW-18945 ]

Desde la página **Administración** > **Anuncios** al nivel de proveedor, si elige un cliente en la barra de menú superior, se muestra una página en blanco con **Administración de redes** como encabezado.

[ SDW-18944 ]

Tras importar los derechos de producción válidos, la opción **Actualizar a producción** está disponible en **Licencias** incluso antes de asignar la licencia al dispositivo.

[ SDW-18721 ]

## Problemas conocidos

Los problemas que existen en la versión 11.1.

La función ZTD negociada en la nube depende del servicio SD-WAN Orchestrator para que funcione. Esto se abordará en una próxima versión del servicio SD-WAN Orchestrator. Sin embargo, los clientes no necesitan actualizar su Citrix SD-WAN Orchestrator for On-premises.

[ SDW-20307 ]

Cuando Citrix SD-WAN Orchestrator for On-premises se actualiza a la versión 11.1, los registros de auditoría recopilados durante las versiones anteriores muestran **sdwan-onprem-sp** como usuario y el botón de registro de cargas útiles está habilitado en la interfaz de usuario. Estos registros se borran después de 92 días.

[ SDW-20305 ]

La configuración de ZTD en la nube de SD-WAN no funciona para los sitios de HA si la ZTD en la nube ya está configurada en un sitio principal.

**Solución temporal**:

1. Elimine la configuración de ZTD en la nube del sitio principal yendo a **Administración** > **Configuración de ZTD** > **Cloud Brokered ZTD**.
2. Vuelva a configurar el sitio ZTD en la nube para los sitios principales y secundarios al mismo tiempo.

[ SDW-20208 ]

La función de licencias no se admite en la configuración administrada por el proveedor de Citrix SD-WAN Orchestrator for On-premises. Los proveedores pueden continuar con las licencias de prueba. Se proporciona un período de gracia de 60 días.

[ SDW-18831 ]

Cuando un dispositivo pierde la conectividad con Citrix SD-WAN Orchestrator for On-premises durante más de 20 minutos y entra en la fase de reinscripción, envía un número de serie incorrecto en la solicitud de registro.

**Solución temporal**: Reinicie el dispositivo.

[ SDW-18781 ]

En una configuración administrada por un proveedor, los anuncios agregados por los administradores del proveedor no se muestran a los clientes al iniciar sesión.

[ SDW-18491 ]

Citrix SD-WAN Orchestrator for On-premises muestra el estado **No conectado**, aunque el dispositivo SD-WAN esté conectado a Citrix SD-WAN Orchestrator for On-premises.

**Solución alternativa**: Vaya a **Configuración** > **Página principal de Configuración de red** y compruebe el estado de conectividad del dispositivo en la interfaz de usuario de Citrix SD-WAN Orchestrator for On-premises.

[ SDW-18280 ]

Cuando la copia de seguridad de la base de datos de un dispositivo se restaura en otro dispositivo que tenga la misma versión de Citrix SD-WAN Orchestrator for On-premises, los detalles del usuario no se restauran. En el dispositivo restaurado, si crea un usuario con el mismo nombre de usuario que en la base de datos de la copia de seguridad, aparece el siguiente error:

```
User has a role already assigned
```

**Solución alternativa**: Cree un usuario con un nombre de usuario diferente que no exista en la base de datos de la que se realizó la copia de seguridad.

[ SDW-15984 ]

Citrix SD-WAN Orchestrator for On-premises que ejecuta VMware ESXi 13 no se reinicia y pasa a un estado incorrecto.

**Solución alternativa**: Utilice VMware ESXi versión 9.

[ SDWANHELP-2182 ]

# Notas de la versión 10.3 de Citrix SD-WAN Orchestrator for On-premises

October 31, 2022

Este documento de notas de la versión describe las mejoras y los cambios, así como los problemas solucionados y conocidos que existen para la versión 10.3 de Citrix SD-WAN Orchestrator for On-premises.

## Notas

Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

## Novedades

Mejoras y cambios que están disponibles en la versión 10.3.

### Configuración y administración

#### Redirección dinámica

A partir de la versión 11.3.1 de Citrix SD-WAN, puede configurar un ID de enrutador para todo el protocolo y también un ID de enrutador por dominio de enrutamiento. Con esta mejora, puede habilitar un enrutamiento dinámico estable en varias instancias con diferentes ID de enrutador que convergen de manera estable.

[ SDW-17097 ]

#### Reintentar la puesta en escena

La opción Reintentar la puesta en escena ahora está disponible para reiniciar la puesta en escena en los sitios en los que el proceso de preparación ha fallado.

[ SDW-16538 ]

#### Aplicación personalizada

La casilla de verificación **Habilitar informes** se ha agregado recientemente para las aplicaciones personalizadas basadas en el protocolo IP. Ahora también puede ver el tráfico definido por la aplicación personalizado basado en el protocolo IP y el nombre de dominio en la página **Informes > Uso**. La opción de aplicación personalizada también se agrega como un tipo en la página de **configuración de la calidad de la aplicación**.

[ SDW-10862 ]

### Otros

#### Configuración de reserva

La configuración de reserva garantiza que el dispositivo permanezca conectado al servicio de implementación sin contacto si hay un error de vínculo, falta de configuración o falta de software. La configuración de reserva está habilitada de forma predeterminada en los dispositivos que tienen un perfil de configuración predeterminado. Si la configuración alternativa está inhabilitada en un sitio, puede habilitarla a través de Citrix SD-WAN Orchestrator for On-premises.

[ SDW-13978 ]

#### Flujos

Ahora puede utilizar la sección **Flujos** de configuración del dispositivo para realizar la siguiente acción:

- Activar/desactivar el servicio Citrix Virtual WAN
- Reiniciar el enrutamiento dinámico
- Activar/desactivar rutas virtuales
- Activar/desactivar los enlaces WAN

[ SDW-13977 ]

#### Funciones de administrador de red y administrador de seguridad (versión preliminar)

Citrix SD-WAN Orchestrator for On-premises admite las siguientes funciones:

- **Provide-Network-Admin**: Un administrador que solo puede ver y modificar la información relacionada con la red.
- **Provider-Security-Admin**: Un administrador que solo puede ver y modificar la información relacionada con la seguridad.
- **Customer-Network-Admin**: Un administrador de clientes que solo puede ver y modificar la información relacionada con la red.
- Administrador**de seguridad del cliente: Administrador**de clientes que solo puede ver y modificar la información relacionada con la seguridad.

[ SDW-13845 ]

#### Configuración del dispositivo

Ahora puede configurar la fecha y la hora, al nivel de sitio, a través de Citrix SD-WAN Orchestrator for On-premises. Puede configurar la fecha y la hora manualmente o mediante un servidor NTP y también configurar la zona horaria.

[ SDW-13321 ]

### Soporte al nivel de proveedor

Citrix SD-WAN Orchestrator for On-premises admite la multitenencia. Con la función multiusuario, se pueden administrar varias cuentas de clientes mediante una única instancia de Citrix SD-WAN Orchestrator for On-premises. Puede tener uno de los siguientes tipos de configuraciones.

- **Configuración administrada por el proveedor**: Los clientes consumen un servicio administrado de Citrix SD-WAN Orchestrator for On-premise de los socios de Citrix mediante la función de multitenencia.
- **Configuración gestionada por el cliente**: Los clientes administran su Citrix SD-WAN Orchestrator for On-premises como un servicio autogestionado para su empresa.

Como parte del soporte de configuración administrada por el proveedor, se presentan las siguientes capacidades:

- **Funciones**: Se agregan las siguientes funciones al nivel de proveedor:
  - Provider-Master-Admin-All
  - Provider-Master-Admin-Tenant
  - Provider-Master - Solo lectura - Todo
- **Panel de control**: Se ha agregado una nueva página de interfaz de usuario que ofrece una vista panorámica de todos los clientes de SD-WAN gestionados por un proveedor.
- **Conectividad con dispositivos SD-WAN**: En una configuración administrada por un proveedor, solo los proveedores tienen la capacidad de habilitar el tipo de autenticación y regenerar el certificado Citrix SD-WAN Orchestrator for On-premises. Los clientes pueden cargar el certificado del dispositivo.
- **Plantillas de perfil de sitio y plantillas de enlaces WAN**: Las plantillas permiten la creación de **perfiles de sitio** y **perfiles de enlaces WAN** al nivel de cliente.
- **Publicar software**: Citrix SD-WAN Orchestrator for On-premises permite a los administradores de proveedores descargar la versión de software del dispositivo Citrix SD-WAN requerida para todos los dispositivos de la red. Los proveedores pueden publicar la versión de software descargada. El software publicado se descarga y almacena en Citrix SD-WAN Orchestrator for On-premises. Los administradores de clientes pueden implementar el software publicado en todos los dispositivos administrados por Citrix SD-WAN Orchestrator for On-premises.
- **Administración**: Los administradores de los proveedores pueden configurar la IP de administración, el DNS, los servidores NTP y los servidores de autenticación remota.
- **Anuncios**: Los proveedores pueden usar la opción **Anuncios** para enviar anuncios o notificaciones a sus clientes.
- **Informes: Losinformes de proveedores** proporcionan visibilidad de las alertas, las tendencias de uso y el inventario agregado de todos los clientes gestionados por un proveedor.

[ SDW-12589 ]

#### Implementación sin intervención: Sitios por lotes

Ahora puede importar un archivo CSV para agregar varios sitios simultáneamente para Zero Touch Deployment. Hay disponible una plantilla descargable de muestra en la interfaz de usuario, descárgala y proporciona todos los detalles del sitio.

[ SDW-12249 ]

### Plataforma y sistemas

#### Informes del sitio: Medición de enlaces WAN

Los informes de **medición de enlaces WAN** proporcionan detalles sobre el uso del enlace WAN medido. Puede ver los informes para obtener información sobre el consumo de datos de los enlaces WAN medidos.

[ SDW-8892 ]

## Problemas conocidos

Los problemas que existen en la versión 10.3.

### Configuración y administración

Para la HA dentro de banda, la GUI no tiene la opción de seleccionar la dirección de la regla de destino con el tipo de servicio como Cualquiera, lo que provoca un error en las reglas de salida. El mensaje de error [ EC818 ] En el nombre del sitio: El tipo de servicio "cualquiera"no se puede usar cuando la dirección es de salida.

[ SDW-16968 ]

### Otros

Aunque el administrador del cliente no tiene acceso para eliminar los servidores de autenticación remota, la GUI muestra el icono de eliminación. Sin embargo, cuando se intenta realizar la operación de eliminación, aparece el siguiente error:

```
User is not authorized to perform this operation
```

[ SDW-18945 ]

Desde la página **Administración > Anuncios** al nivel de proveedor, si elige un cliente en la barra de menú superior, se muestra una página en blanco con **Administración de redes** como encabezado.

[ SDW-18944 ]

No puede restaurar la copia de seguridad de la base de datos realizada en una configuración administrada por el proveedor en una configuración administrada por el Del mismo modo, no puede restaurar la copia de seguridad de la base de datos realizada en una configuración administrada por el cliente en una configuración administrada por

[ SDW-18904 ]

Cuando el rol de administrador de seguridad del cliente que tiene acceso de solo lectura a la configuración del sitio intenta modificar la configuración, en lugar de mostrar el acceso no autorizado, aparece una pancarta roja con un mensaje de error.

[ SDW-18840 ]

La función de licencias no se admite en la configuración administrada por el proveedor de Citrix SD-WAN Orchestrator for On-premises. Los proveedores pueden continuar con las licencias de prueba. Se proporcionará un período de gracia de 60 días.

[ SDW-18831 ]

Cuando un dispositivo pierde la conectividad con Citrix SD-WAN Orchestrator for On-premises durante más de 20 minutos y entra en la fase de reinscripción, envía un número de serie incorrecto en la solicitud de registro.

Solución temporal: Reinicie el dispositivo.

[ SDW-18781 ]

Tras importar los derechos de producción válidos, **la opción Actualizar a producción** está disponible en Licencias incluso antes de asignar la licencia al dispositivo.

Solución alternativa: haga clic en **Actualizar a producción** solo después de asignar la licencia al dispositivo.

[ SDW-18721 ]

No se admite la traducción de direcciones de red (NAT) entre Citrix SD-WAN Orchestrator for On-premises y el dispositivo.

[ SDW-18703 ]

En una configuración administrada por un proveedor, los anuncios agregados por los administradores del proveedor no se muestran a los clientes al iniciar sesión.

[ SDW-18491 ]

La CLI permite a los usuarios crear una contraseña fuera del rango de longitud permitido de 8 a 128, pero el inicio de sesión de la GUI falla si la longitud de la contraseña está fuera del rango permitido.

Solución alternativa: Al iniciar sesión en la GUI, el usuario se ve obligado a cambiar la longitud de la contraseña al rango permitido.

[ SDW-16068 ]

Cuando un usuario intenta iniciar sesión, es posible que aparezca un banner rojo en la parte superior de la página durante una fracción de segundo antes de que aparezca la página de inicio de sesión.

[ SDW-16024 ]

Cuando la copia de seguridad de la base de datos de un dispositivo se restaura en otro dispositivo que tenga la misma versión de Citrix SD-WAN Orchestrator for On-premises, los detalles del usuario no se restauran. En el dispositivo restaurado, si crea un usuario con el mismo nombre de usuario que en la base de datos de la copia de seguridad, aparece el siguiente error:

```
User has a role already assigned
```

Solución alternativa: Cree un usuario con un nombre de usuario diferente que no exista en la base de datos de la que se realizó la copia de seguridad.

[ SDW-15984 ]

## Notas de la versión 9.6 de Citrix SD-WAN Orchestrator for On-premises

July 15, 2023

Este documento de notas de la versión describe las mejoras y los cambios, así como los problemas solucionados y conocidos que existen para la versión 9.6 de Citrix SD-WAN Orchestrator for On-premises.

> **Nota**
>
> Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

### Novedades

Mejoras y cambios que están disponibles en la versión 9.6.

#### Configuración y administración

##### Redirección dinámica

A partir de la versión 11.3.1 de Citrix SD-WAN, puede configurar un ID de enrutador para todo el protocolo y también un ID de enrutador por dominio de enrutamiento. Con esta mejora, puede habilitar

un enrutamiento dinámico estable en varias instancias con diferentes ID de enrutador que convergen de manera estable.

[ SDW-17097 ]

#### Otros

##### Certificado HTTPS

El certificado HTTPS es necesario para establecer una conexión HTTPS de administración segura con Citrix SD-WAN Orchestrator for On-premises. Puede usar el certificado predeterminado disponible en la GUI de Citrix SD-WAN Orchestrator for On-premises o cargar un certificado HTTPS personalizado generado desde cualquier otro marco, como OpenSSL. El certificado HTTPS personalizado le permite tener control sobre la seguridad y los demás parámetros del tema relacionados con el certificado.

[ SDW-16359 ]

##### Interfaces

A partir de la versión 11.3.1 de Citrix SD-WAN, puede habilitar o inhabilitar una interfaz virtual mediante la casilla **Activado**.

[ SDW-15993 ]

### Problemas resueltos

Los problemas que se abordan en la versión 9.6.

#### Configuración y administración

Para el dispositivo Citrix SD-WAN 6100 SE, la interfaz de usuario no muestra la página **LAG** en **Configuración > Configuración avanzada**.

[ SDWANHELP-1895 ]

#### Otros

La GUI de Citrix SD-WAN Orchestrator for On-premises solicita a los usuarios que inicien sesión cada hora, incluso cuando la GUI está en uso continuo y no se deja inactiva.

[ SDWANHELP-1902 ]

Al crear un sitio clonando un sitio existente, se produce un error en **Deploy Config/Software > Verify Config**.

[ SDW-16103 ]

### Problemas conocidos

Los problemas que existen en la versión 9.6.

#### Otros

Si abre la GUI de Citrix SD-WAN Orchestrator for On-premises en una ficha nueva mientras se actualiza el token de autenticación, se cierra la sesión de todas las sesiones existentes en el navegador.

[ SDW-17719 ]

Si el disco se redimensiona a más de 1,8 TB, no se redimensionará el disco.

[ SDW-16404 ]

La CLI permite a los usuarios crear una contraseña dentro del rango de longitud permitido de 8 a 128. Sin embargo, el inicio de sesión de la GUI falla si la longitud de la contraseña está fuera del rango permitido.

Solución alternativa: Al iniciar sesión en la GUI, el usuario se ve obligado a cambiar la longitud de la contraseña al rango permitido.

[ SDW-16068 ]

Cuando un usuario intenta iniciar sesión, es posible que aparezca un banner rojo en la parte superior de la página durante una fracción de segundo antes de que aparezca la página de inicio de sesión.

[ SDW-16024 ]

Cuando la copia de seguridad de la base de datos de un dispositivo se restaura en otro dispositivo que tenga la misma versión de Citrix SD-WAN Orchestrator for On-premises, los detalles del usuario no se restauran. En el dispositivo restaurado, si crea un usuario con el mismo nombre de usuario que en la base de datos de la copia de seguridad, aparece el siguiente error:

```
User has a role already assigned
```

Solución alternativa: Cree un usuario con un nombre de usuario diferente que no exista en la base de datos de la que se realizó la copia de seguridad.

[ SDW-15984 ]

## Notas de la versión 1.0 de Citrix SD-WAN Orchestrator for On-premises

October 31, 2022

Citrix SD-WAN Orchestrator local es un servicio de administración autoalojado disponible como instancia independiente para cada cliente. Proporciona una plataforma de administración de vidrio de un solo panel que le permite configurar, supervisar y analizar todos los dispositivos SD-WAN de su red SD-WAN.

Citrix SD-WAN Orchestrator local se recomienda para clientes con estrictos requisitos reglamentarios en torno a la soberanía de los datos y la privacidad de los datos.

Las siguientes son algunas de las capacidades clave:

- **Autenticación: Admite la autenticación**local y RADIUS/TACACS+.
- **Configuración centralizada**: Configuración centralizada de redes SD-WAN, con flujos de trabajo guiados, ayudas visuales y perfiles.
- **Aprovisionamiento**sin intervención: Acceso ininterrumpido a la red y las conexiones.
- **Directivas centradas en las aplicaciones: Directivas**de direccionamiento del tráfico basadas en aplicaciones, calidad de servicio (QoS) y firewall, configurables a nivel mundial o por sitio.
- **Resumen jerárquico del estado**: Capacidad de supervisar de forma centralizada el estado, el uso, la calidad y el rendimiento de una red en su conjunto, con la capacidad de desglosar los sitios individuales y las conexiones asociadas.
- **Solución de problemas**: Registros de dispositivos y auditorías, utilidades de diagnóstico como Ping, Traceroute o Packet Capture para solucionar problemas de conectividad de red.

## Requisitos previos

- **Dispositivos**: Un mínimo de dos dispositivos. Cada dispositivo SD-WAN o instancia virtual debe tener una dirección IP configurada.
- **Cuenta de servicio Citrix SD-WAN Orchestrator**: Para utilizar Citrix SD-WAN Orchestrator para entornos locales, debe tener una cuenta en el servicio Citrix SD-WAN Orchestrator. Para obtener más información, consulte Incorporación del servicio Citrix SD-WAN Orchestrator.

## Citrix SD-WAN Orchestrator para entornos locales 1.0.1

### Problemas resueltos

- **SDW-16456**: Citrix SD-WAN Orchestrator for On-premises no admite ningún dominio de enrutamiento hacia ningún dominio.
- **SDW-16063**: A nivel de red, los informes resumidos de Wi-Fi no están disponibles.
- **SDW-16054**: Si se crea una cuenta de cliente fuera de la región de EE. UU. en el servicio Citrix SD-WAN Orchestrator, el token de API obtenido por la página Identity and Management (IDAM) de Citrix Cloud no funciona. El inicio de sesión del cliente en Citrix SD-WAN Orchestrator for

On-premises falla y aparece el siguiente mensaje de error: "ID de cliente, ID de cliente o secreto de cliente no válidos".

Ahora puede seleccionar el **POP** en el que estaba integrada su cuenta de nube al iniciar Citrix SD-WAN Orchestrator for On-premises por primera vez.

### Problemas conocidos

- **SDW-16068**: La CLI permite a los usuarios crear una contraseña fuera del rango de longitud permitido de 8 a 128, pero el inicio de sesión de la GUI falla si la longitud de la contraseña está fuera del rango permitido.
  - **Solución alternativa**: Al iniciar sesión en la GUI, el usuario se ve obligado a cambiar la longitud de la contraseña al rango permitido.
- **SDW-16024**: Cuando un usuario inicia sesión en la interfaz de usuario, es posible que aparezca una pancarta roja en la parte superior de la página durante una fracción de segundo antes de que aparezca la página de inicio de sesión.
- **SDW-15984**: Cuando se restaura la copia de seguridad de la base de datos de un dispositivo en otro dispositivo que tenga la misma versión de Citrix SD-WAN Orchestrator for On-premises, los detalles del usuario no se restauran. En el dispositivo restaurado, si crea un usuario con el mismo nombre de usuario que en la base de datos de la copia de seguridad, aparece el siguiente error:

  *El usuario ya tiene un rol asignado*

  - **Solución alternativa**: Cree un usuario con un nombre de usuario diferente que no exista en la base de datos de la que se realizó la copia de seguridad.
- **SDW-16103**: Al crear un sitio mediante la clonación de un sitio existente, se produce un error en **Deploy Config/Software > Verify Config**.
  - **Solución alternativa**: No cree un sitio clonando uno existente.
- **SDW-16404**: Si se cambia el tamaño del disco a más de 1,8 TB, no se cambia el tamaño del disco.

## Requisitos e instalación del sistema

October 31, 2022

Antes de instalar Citrix SD-WAN Orchestrator for On-premises en una máquina virtual (VM), asegúrese de comprender los requisitos de hardware y software y de cumplir con los requisitos previos.

> **Nota**
>
> Los requisitos del sistema son comunes tanto para la red de una sola región como para la red multirregional.

## Requisitos de hardware

Los siguientes son los requisitos de hardware para que Citrix SD-WAN Orchestrator for On-premises almacene datos de 1 mes o estadísticas de dos enlaces WAN por sitio en promedio:

| Número de sitios | Procesador | RAM | Almacenamiento |
|---|---|---|---|
| 2000 | 256 vCPUs de 3 GHz o más | 512 GB | 2 TB |
| 1000 | 128 vCPUs de 3 GHz o más | 256 GB | 1 CUCHARADA |
| 500 | 64 vCPU de 3 GHz o más | 128 GB | 500 GB |
| 256 | 32 vCPU de 3 GHz o superior | 64 GB | 256 GB |
| 128 | 8 vCPU de 3 GHz o más | 16 GB | 256 GB |

## Software

Citrix SD-WAN Orchestrator para VPX local se puede configurar en las siguientes plataformas:

Hipervisor

- Actualización 1 de VMware ESXi 7.0.
- Servidor VMware ESXi, versión 6.5.
- Citrix XenServer 6.5 o superior.

Los exploradores deben tener habilitadas las cookies y JavaScript instalado y habilitado.

La interfaz web local de Citrix SD-WAN Orchestrator es compatible con los siguientes navegadores:

- Google Chrome 40.0+
- Microsoft Internet Explorer 11+
- Mozilla Firefox 41.0+

### Requisitos previos

Los siguientes son los requisitos previos para instalar e implementar Citrix SD-WAN Orchestrator for On-premises:

- El nodo de control maestro (MCN) de SD-WAN y los nodos de cliente existentes deben actualizarse a la versión más reciente del software Citrix SD-WAN.
- Se recomienda tener un servidor DHCP disponible y configurado en la red SD-WAN.
- Debe tener los archivos de instalación local de Citrix SD-WAN Orchestrator.

> **Nota**
>
> No puede personalizar ni instalar ningún software de terceros en Citrix SD-WAN Orchestrator for On-premises. Sin embargo, puede modificar la configuración de la vCPU, la memoria y el almacenamiento.

### Descargue Citrix SD-WAN Orchestrator para software local

Descargue los archivos de instalación del software Citrix SD-WAN Orchestrator for On-premises Management Console, para la versión y la plataforma requeridas, desde la página de descargas.

Los archivos de instalación de Citrix SD-WAN Orchestrator for On-premises utilizan la siguiente convención de nomenclatura:

- extensión ctx-sdw-onprem-build.extension
- extensión ctx-onprem-build.extension
- extensión ctx-onprem-build.extension

| Plataforma | Extensión |
|---|---|
| Citrix XenServer | .xva |
| VMware ESXi | -vmware.ova |

### Lista de verificación de la Instalación y la configuración

En esta sección se proporciona una lista de verificación con la información que necesita para completar la instalación e implementación de Citrix SD-WAN Orchestrator for On-premises.

Recopile o determine la siguiente información:

- La dirección IP del servidor ESXi y XenServer que aloja el Citrix SD-WAN Orchestrator para máquinas virtuales (VM) locales.

- Un nombre único para asignar a la máquina virtual Citrix SD-WAN Orchestrator for On-premises.
- La cantidad de memoria que se debe asignar a la máquina virtual Citrix SD-WAN Orchestrator for On-premises.
- La cantidad de capacidad de disco que se va a asignar al disco virtual de la máquina virtual.
- La dirección IP de la puerta de enlace que utiliza Citrix SD-WAN Orchestrator para entornos locales para comunicarse con redes externas.
- La máscara de subred de la red en la que está instalado el Citrix SD-WAN Orchestrator para máquinas virtuales locales.

> **Nota**
>
> Citrix recomienda tomar instantáneas de las configuraciones de VM y SD-WAN periódicamente.

## Diferencia entre el servicio SD-WAN Orchestrator for On-premises y el servicio Citrix SD-WAN Orchestrator

October 31, 2022

### Funciones

| Funciones | Servicio Citrix SD-WAN Orchestrator | Citrix SD-WAN Orchestrator para locales |
|---|---|---|
| Plataforma de edición avanzada | Sí | No |
| Plataforma de edición premium | Sí | No |
| Servicio Zscaler | Sí | No |
| Servicio Azure Virtual WAN | Sí | No |
| Servicio de acceso seguro a Internet de Citrix | Sí | No |
| Firewall hospedado | Sí | No |
| Enrutamiento de aplicaciones en aplicaciones DPI preestablecidas y aplicaciones personalizadas (basadas en FQDN o IP) | Sí | Sí |

| Funciones | Servicio Citrix SD-WAN Orchestrator | Citrix SD-WAN Orchestrator para locales |
|---|---|---|
| Enrutamiento de aplicaciones en aplicaciones que requieren actualizaciones de firmas dinámicas (como Office 365, Citrix Cloud y aplicaciones recientemente compatibles). | Sí | No |
| Orchestrator: Alta disponibilidad | Sí | No |

### Requisitos

| Requisitos | Servicio Citrix SD-WAN Orchestrator | SD-WAN Orchestrator para locales |
|---|---|---|
| Se requiere imagen de fábrica de SD-WAN | Todo (versión de envío de fábrica) | Citrix SD-WAN 10.2.7, 11.1.1, 11.2.0, 11.2.2, 11.3.0 y versiones posteriores.. |
| Dispositivo desplegado en la red | Todas | Citrix SD-WAN 11.2.2, 11.3.0 y versiones posteriores.. |
| Conectividad a Internet del dispositivo SD-WAN | Si son necesarias | No se requiere |
| Los puertos del firewall deben estar abiertos | 443 | 443, 22, ICMP |
| Licencias | Modelos de pospago y prepago | Solo modelo prepago |

- La versión del software Citrix SD-WAN compatible depende de la versión de software SD-WAN Orchestrator for On-premises.

## Instalación y configuración de SD-WAN Orchestrator para entornos locales en ESXi Server

October 31, 2022

### Instale el cliente VMware vSphere

Las siguientes son las instrucciones básicas para descargar e instalar el cliente VMware vSphere que utiliza para crear e implementar el Citrix SD-WAN Orchestrator para máquinas virtuales (VM) locales.

Para descargar e instalar VMware vSphere Client, haga lo siguiente:

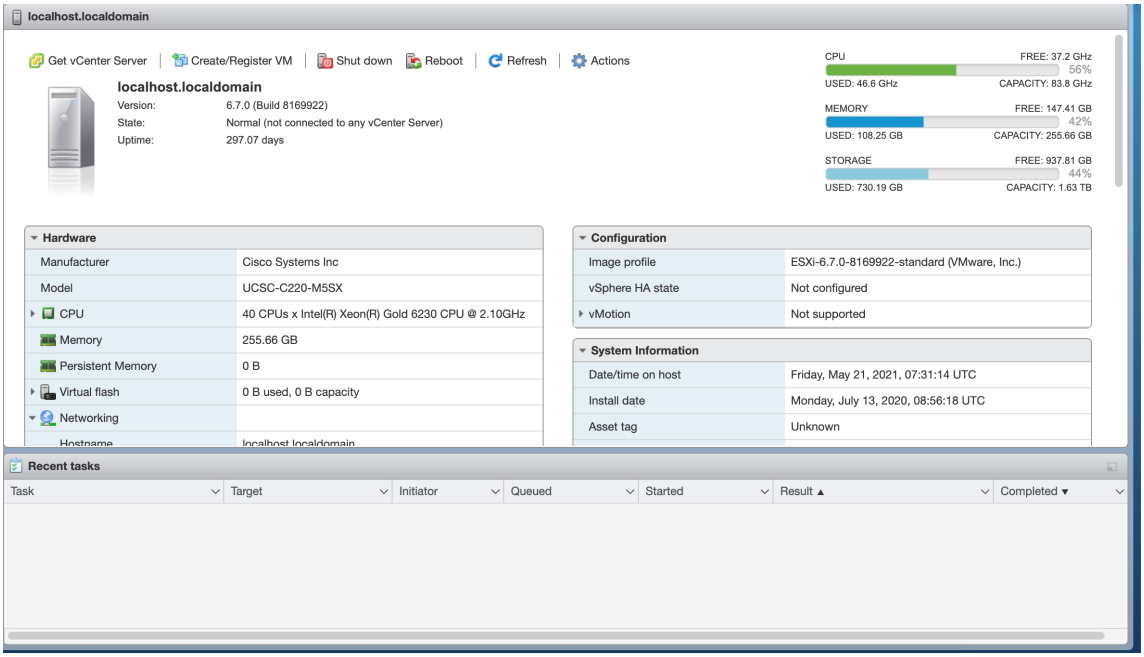
1. Abra un navegador y navegue hasta el servidor ESXi que aloja su instancia de máquina virtual vSphere Client y Citrix SD-WAN Orchestrator for On-premises. Aparece la página de bienvenida de VMware ESXi.
2. Haga clic en el enlace **Descargar vSphere Client** para descargar el archivo de instalación de vSphere Cli
3. Instale vSphere Client.

   Ejecute el archivo de instalación de vSphere Client que descargó y acepte cada una de las opciones predeterminadas cuando se le solicite.
4. Una vez completada la instalación, inicie el programa vSphere Client.

   Aparece la página de inicio de sesión de VMware vSphere Client en la que se le solicitan las credenciales de inicio de sesión del servidor
5. Introduzca las credenciales de inicio de sesión del servidor ESXi:

   - **Dirección IP/nombre**: introduzca la dirección IP o el nombre de dominio completo (FQDN) del servidor ESXi que aloja su instancia de máquina virtual Citrix SD-WAN Orchestrator for On-premises.
   - **Nombre de usuario**: introduzca el nombre de la cuenta del administrador del servidor. El valor predeterminado es raíz.
   - **Contraseña**: introduzca la contraseña asociada a esta cuenta de administrador.
6. Haga clic en **Login**.
   Aparece la página principal de vSphere Client.




## Creación de la máquina virtual Citrix SD-WAN Orchestrator para locales mediante la plantilla OVF

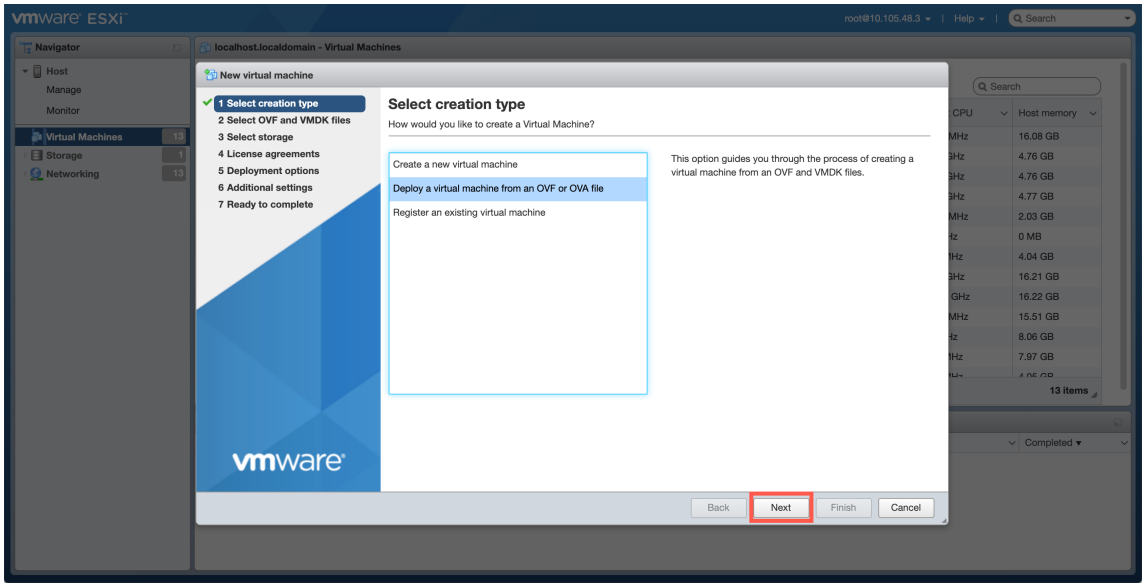
Tras instalar el cliente VMware vSphere, cree la máquina virtual Citrix SD-WAN Orchestrator for On-premises.

1. Si aún no lo ha hecho, descargue el archivo de plantilla OVF (archivo.ova) de Citrix SD-WAN Orchestrator for On-premises al PC local.

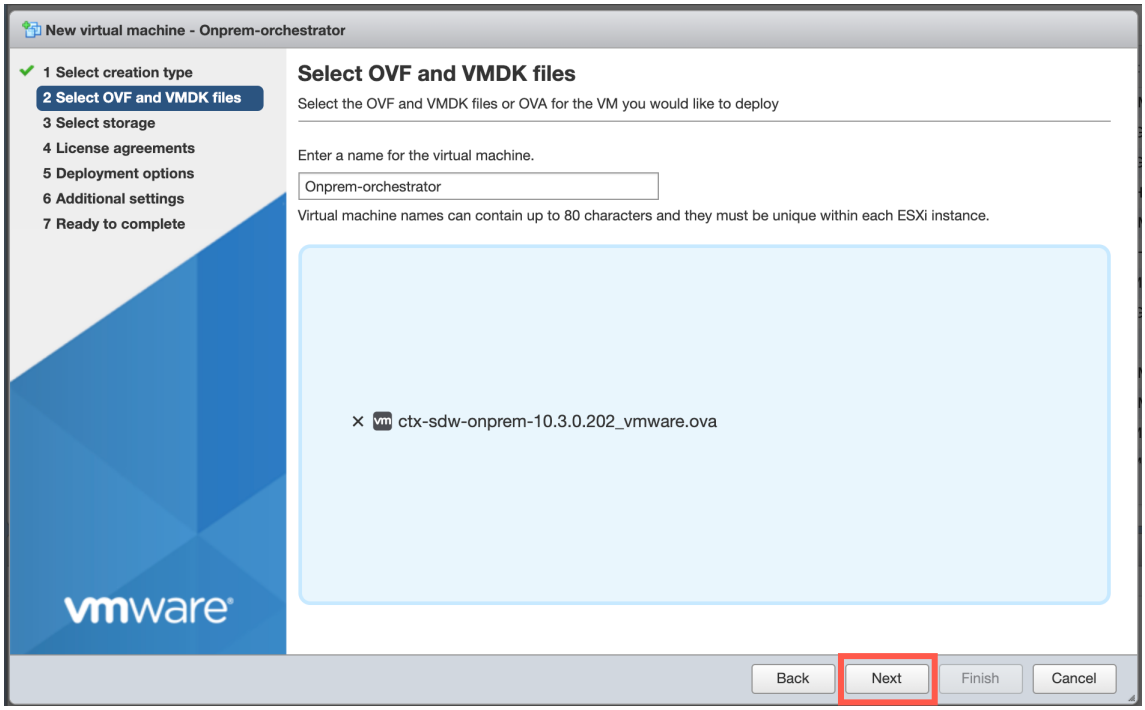
   Para obtener más información, consulte Requisitos e instalación del sistema.

2. En vSphere Client, haga clic en **Crear/Registrar máquina virtual**y, a continuación, seleccione **Implementar una máquina virtual desde un archivo OVF u OVA** de la lista. Haga clic en **Siguiente**.



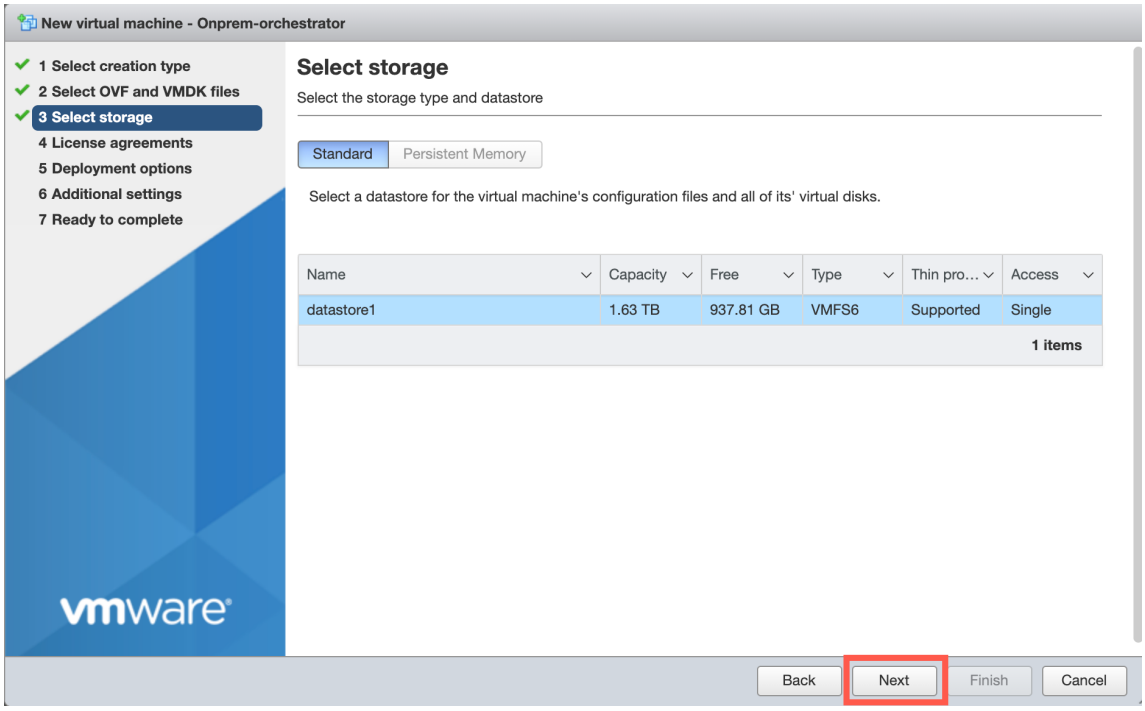

3. Introduzca un nombre único para la nueva máquina virtual.
4. Haga clic dentro del cuadro y seleccione la plantilla OVF de Citrix SD-WAN Orchestrator for On-premises (archivo.ova) que quiere instalar o puede arrastrar el archivo dentro del cuadro.
5. Haga clic en **Siguiente**.



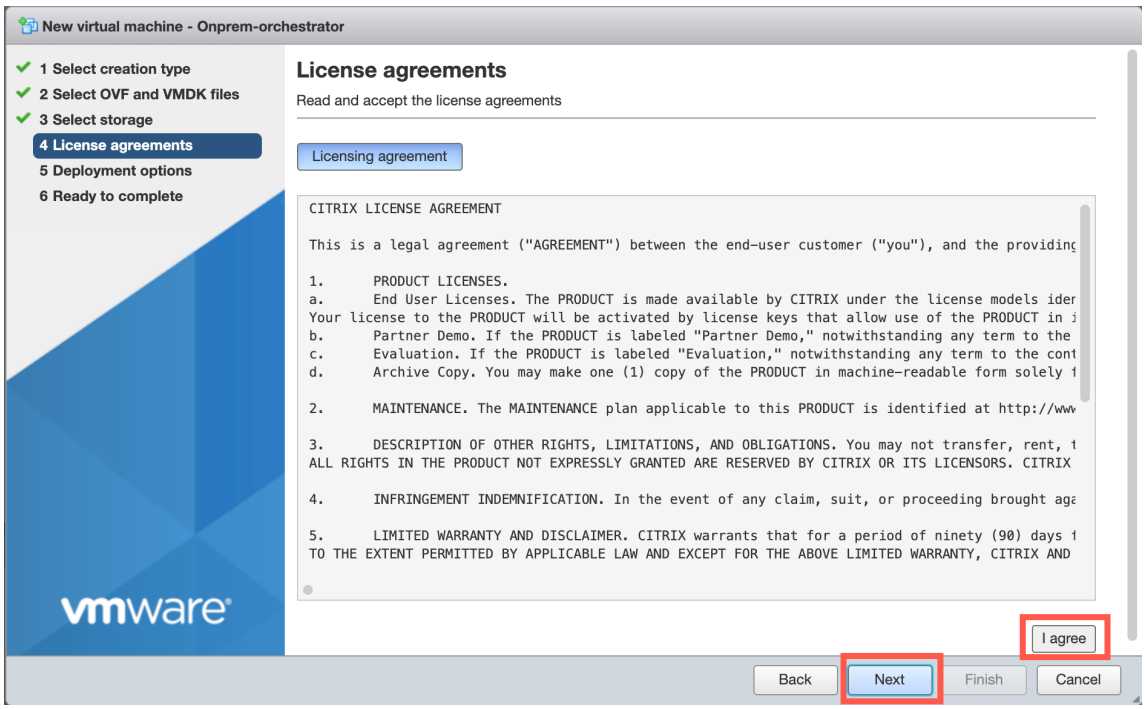

6. Haga clic en **Siguiente**.

   Aparece la página Almacenamiento.
7. Acepte el recurso de almacenamiento predeterminado haciendo clic en **Siguiente**.

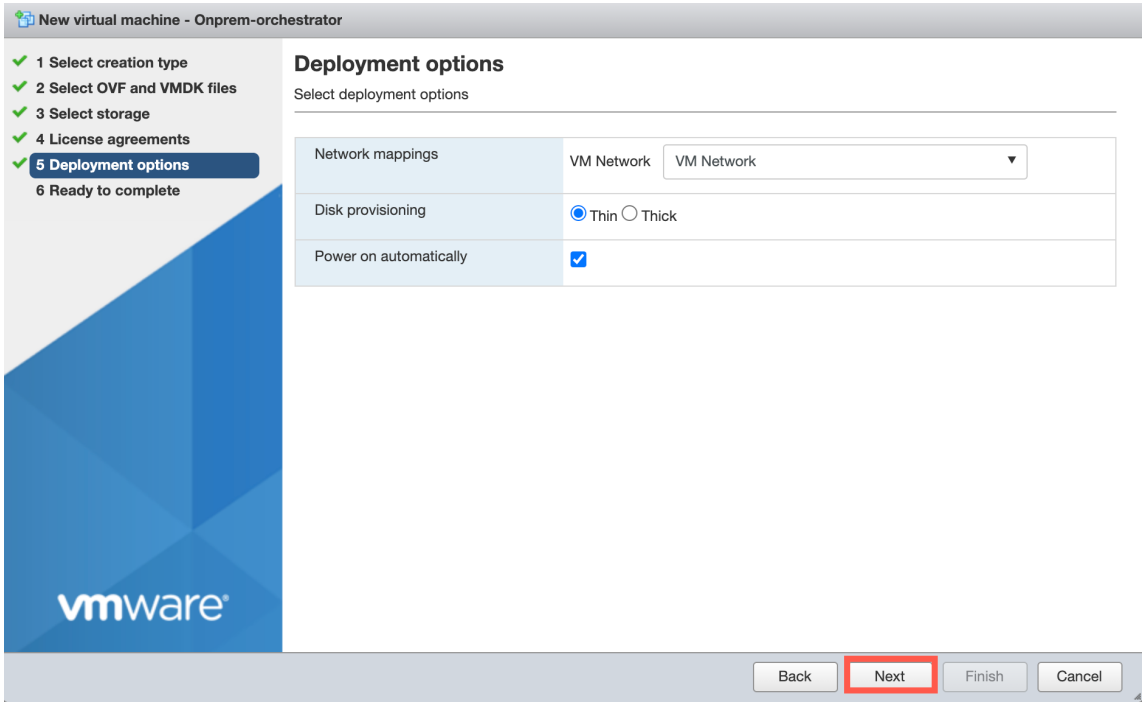



8. En la página del EULA, haga clic en **Acepto**y, a continuación, en **Siguiente**.



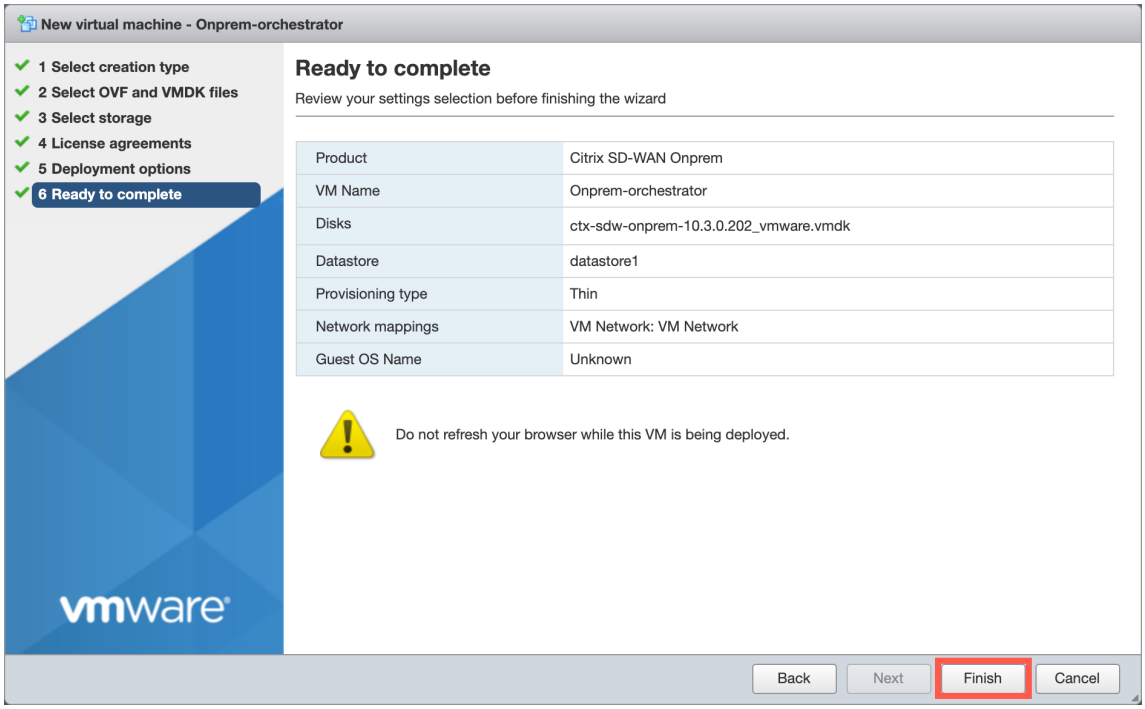

9. En la página de opciones de implementación, seleccione la red de máquinas virtuales en la lista desplegable y acepte la configuración predeterminada de los demás campos. Haga clic en **Siguiente**.




10. En la página Listo para completar, haga clic en **Finalizar** para crear la máquina virtual.

> **Nota**
>
> La descompresión de la imagen del disco en el servidor puede tardar varios minutos.



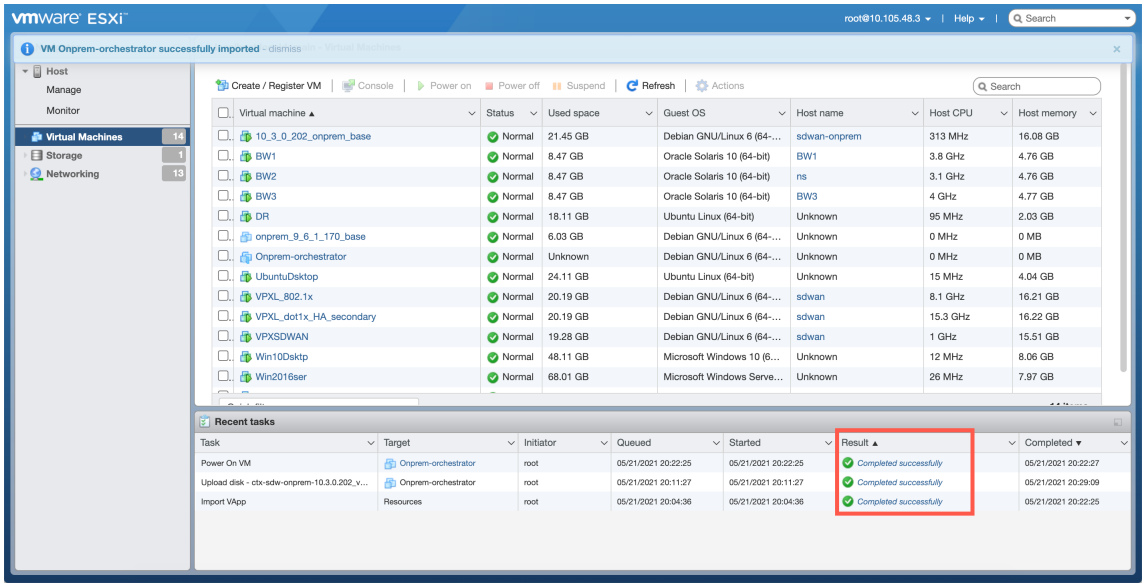

 

## Ver y registrar la dirección IP de administración en el servidor ESXi

La dirección IP de administración es la dirección IP de la máquina virtual Citrix SD-WAN Orchestrator for On-premises. Utilice esta dirección IP para iniciar sesión en la interfaz de usuario web de Citrix SD-WAN Orchestrator for On-premises.

Para mostrar la dirección IP de administración, haga lo siguiente:

1. En la página Inventario del cliente de vSphere, seleccione la nueva máquina virtual Citrix SD-WAN Orchestrator for On-premises.
2. En la página Citrix SD-WAN Orchestrator for On-premises, en Tareas recientes, espere a que el resultado aparezca completado.

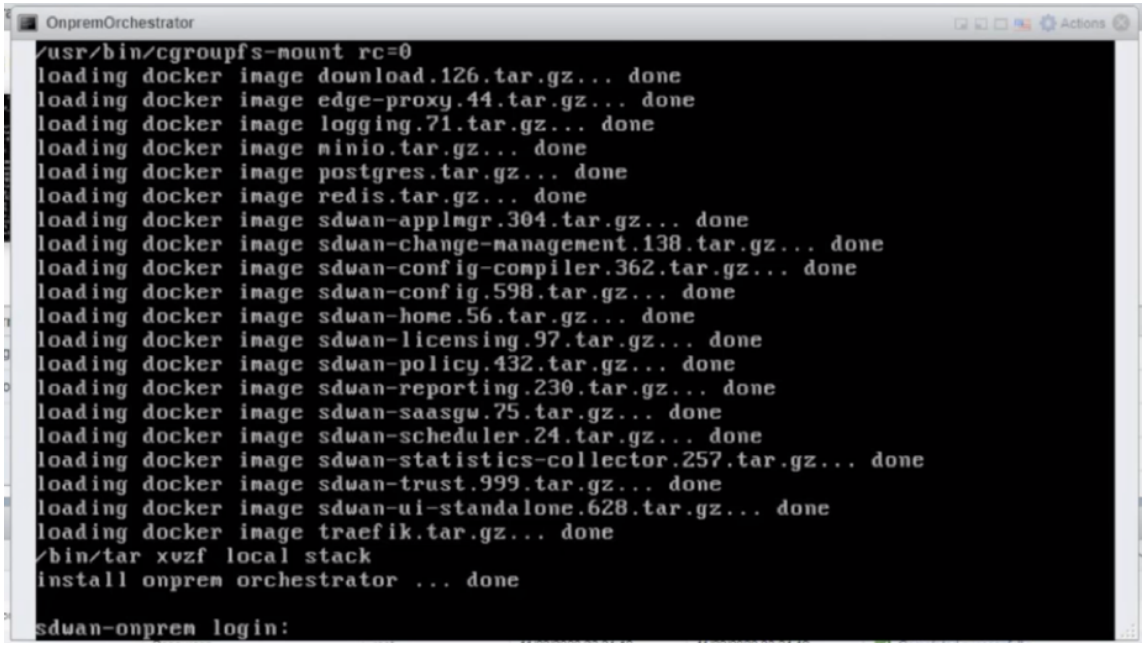



3. Seleccione la ficha **Consola** y, a continuación, haga clic en cualquier parte del área de la consola para acceder al modo consola.

> **Nota**
>
> Para liberar el control del cursor desde la consola, pulse simultáneamente las teclas <Ctrl> y <Alt>.

4. Pulse **Intro** para mostrar el mensaje de inicio de sesión de la consola.

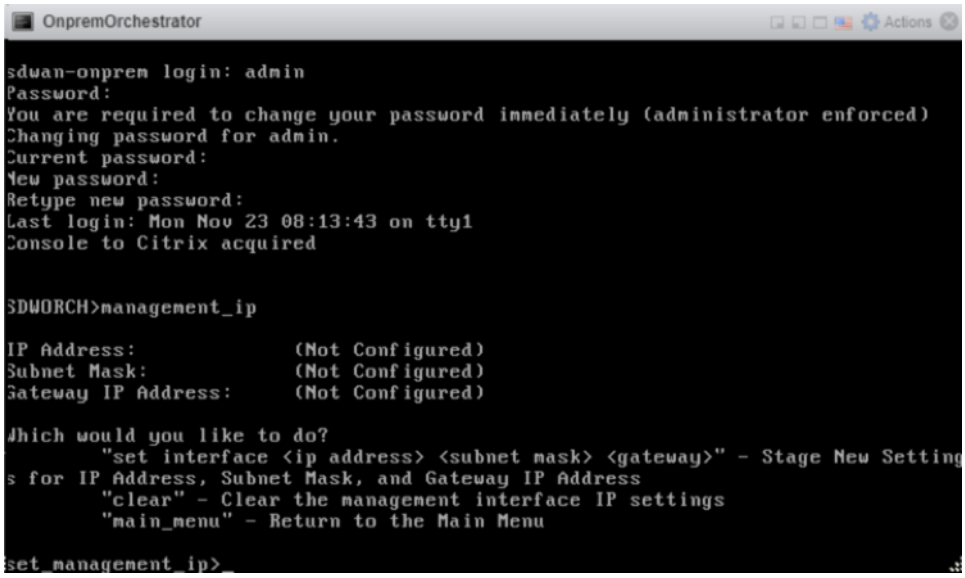



5. Inicie sesión en la consola de la máquina virtual.

   Las credenciales de inicio de sesión predeterminadas para la nueva máquina virtual Citrix SD-WAN Orchestrator for On-premises son las siguientes:

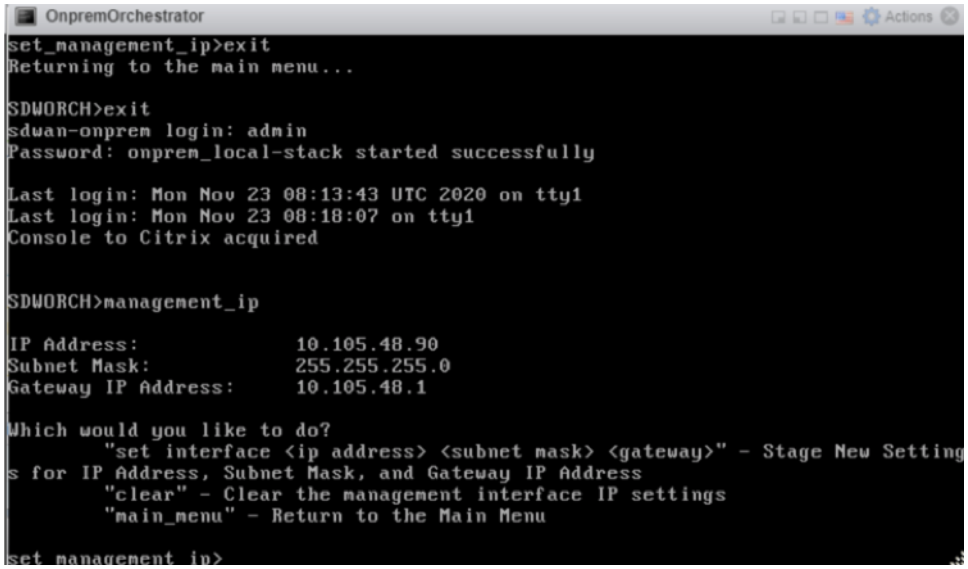
   - **Inicio de sesión**: Admin
   - **Contraseña**: Contraseña

   > **Nota**
   >
   > Es obligatorio cambiar la contraseña predeterminada de la cuenta de usuario administrador al iniciar sesión por primera vez. Este cambio se aplica mediante la CLI y la interfaz de usuario.



6. Registre la dirección IP de administración de la máquina virtual Citrix SD-WAN Orchestrator for On-premises, que se muestra como la dirección IP del host en un mensaje de bienvenida que aparece al iniciar sesión.




> **Nota**
>
> - El servidor DHCP debe estar presente y disponible en la red SD-WAN, o este paso no se puede completar.
> - En la consola, introduzca el comando CLI `set_dns` para confirmar la configuración actual del servidor DNS y volver a configurar el servidor DNS si el servidor DNS existente no puede proporcionar el servicio DNS. Para obtener más información sobre el uso del comando `set_dns`, consulte Citrix SD-WAN Orchestrator para el inicio de sesión local.

Si el servidor DHCP no está configurado en la red SD-WAN, debe introducir manualmente una dirección IP estática.

Para configurar una dirección IP estática como dirección IP de administración:

1. Cuando se inicie la máquina virtual, haga clic en la ficha **Consola**.
2. Inicie sesión en la máquina virtual. Las credenciales de inicio de sesión predeterminadas para la nueva máquina virtual Citrix SD-WAN Orchestrator for On-premises son las siguientes:
   - **Inicio de sesión**: Admin
   - **Contraseña**: Contraseña
3. En la consola, introduzca el comando CLI `management_ip`.
4. Introduzca el comando `set interface <ipaddress> <subnetmask> <gateway>` para configurar la IP de administración.

5. ¿Confirma que quiere cambiar la configuración IP de la interfaz de administración?

   Puede perder la conectividad con el dispositivo. <y/n>?

   Pulse “y”para cambiar la IP y acceder a la nueva IP de administración configurada después de casi 6 a 7 minutos.

# Instalación y configuración de SD-WAN Orchestrator para entornos locales en XenServer

October 31, 2022

Antes de instalar la máquina virtual Citrix SD-WAN Orchestrator for On-premises en un servidor XenServer, recopile la información necesaria tal como se describe en la lista de verificación de instalación y configuración.

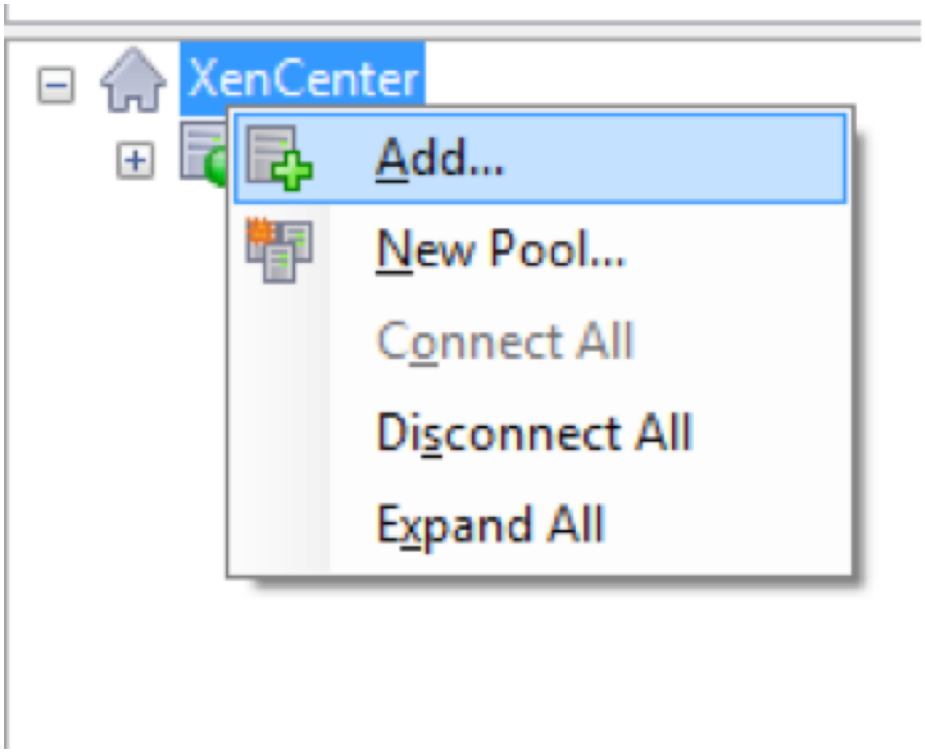
## Instalación del servidor XenServer

Para instalar el servidor Citrix XenServer en el que implementa la máquina virtual Citrix SD-WAN Orchestrator for On-premises, debe tener XenCenter instalado en su equipo. Si aún no lo ha hecho, descargue e instale XenCenter.

Para instalar un servidor XenServer:

1. Abra la aplicación XenCenter en su computadora.
2. En el panel de árbol izquierdo, haga clic con el botón secundario en **XenCenter** y seleccione **Agregar**.

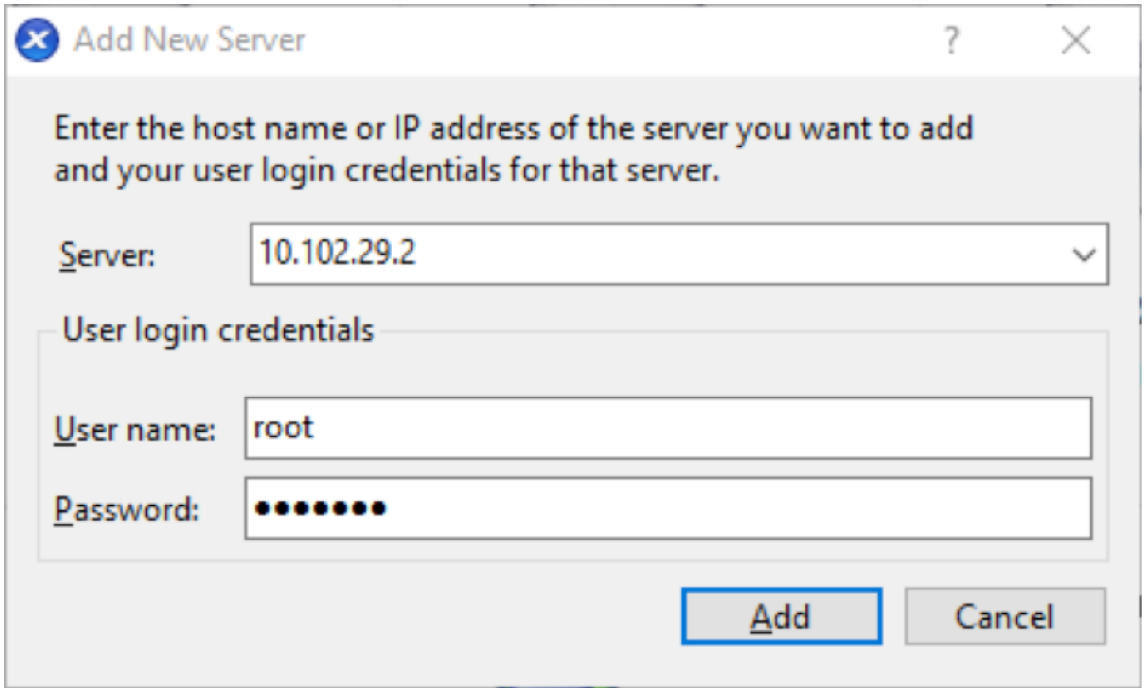
 




3. En la ventana **Agregar nuevo servidor**, introduzca la información requerida en los siguientes campos:

    - **Servidor**: introduzca la dirección IP o el nombre de dominio completo (FQDN) del servidor XenServer que aloja la instancia de máquina virtual Citrix SD-WAN Orchestrator for On-premises.
    - **Nombre de usuario**: introduzca el nombre de la cuenta del administrador del servidor. El valor predeterminado es raíz.
    - **Contraseña**: introduzca la contraseña asociada a esta cuenta de administrador.




4. Haga clic en **Agregar**.

La dirección IP del nuevo servidor aparece en el panel izquierdo.

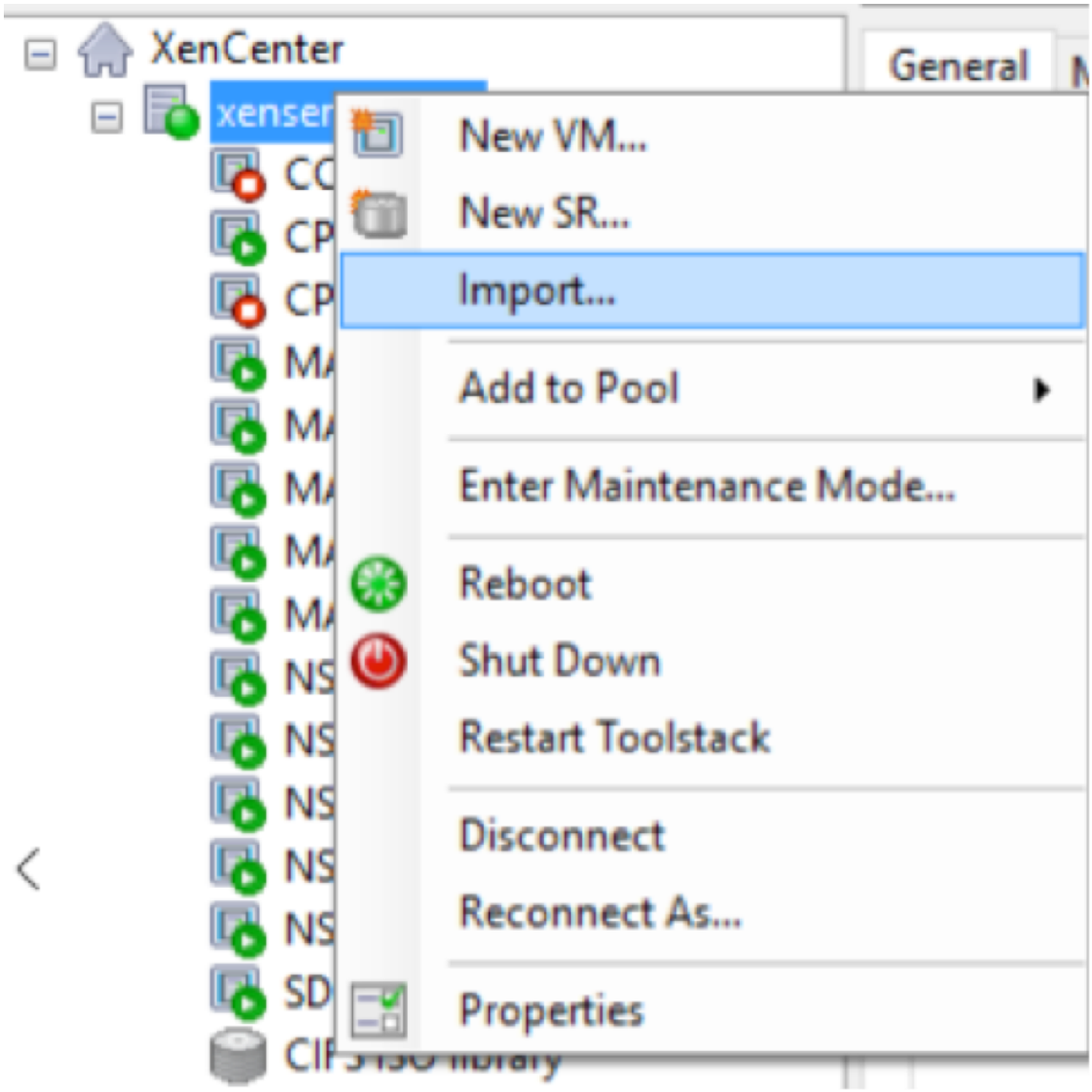
### Cree la máquina virtual Citrix SD-WAN Orchestrator para locales mediante el archivo XVA

El software Citrix SD-WAN Orchestrator para máquinas virtuales locales se distribuye como un archivo XVA. Si aún no lo ha hecho, descargue el archivo.xva. Para obtener más información, consulte Requisitos e instalación del sistema.

Para crear la máquina virtual Citrix SD-WAN Orchestrator for On-premises:

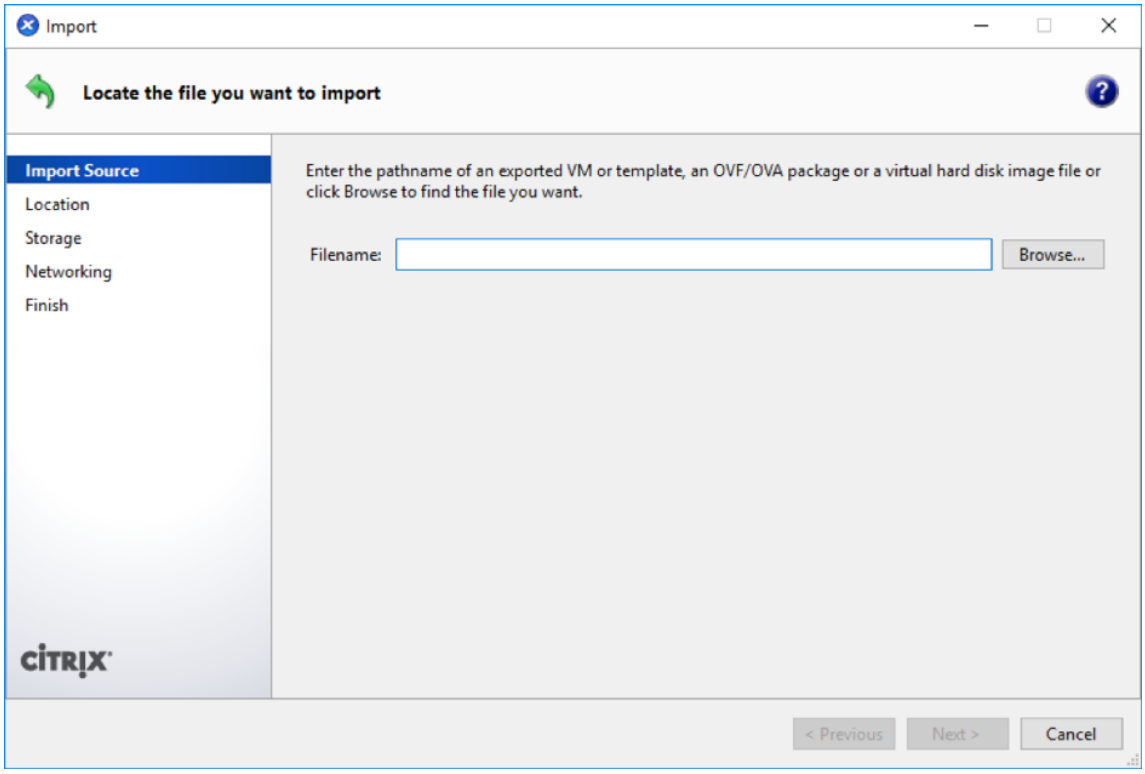
1. En XenCenter, haga clic con el botón secundario en **XenServer** y haga clic en **Importar**.

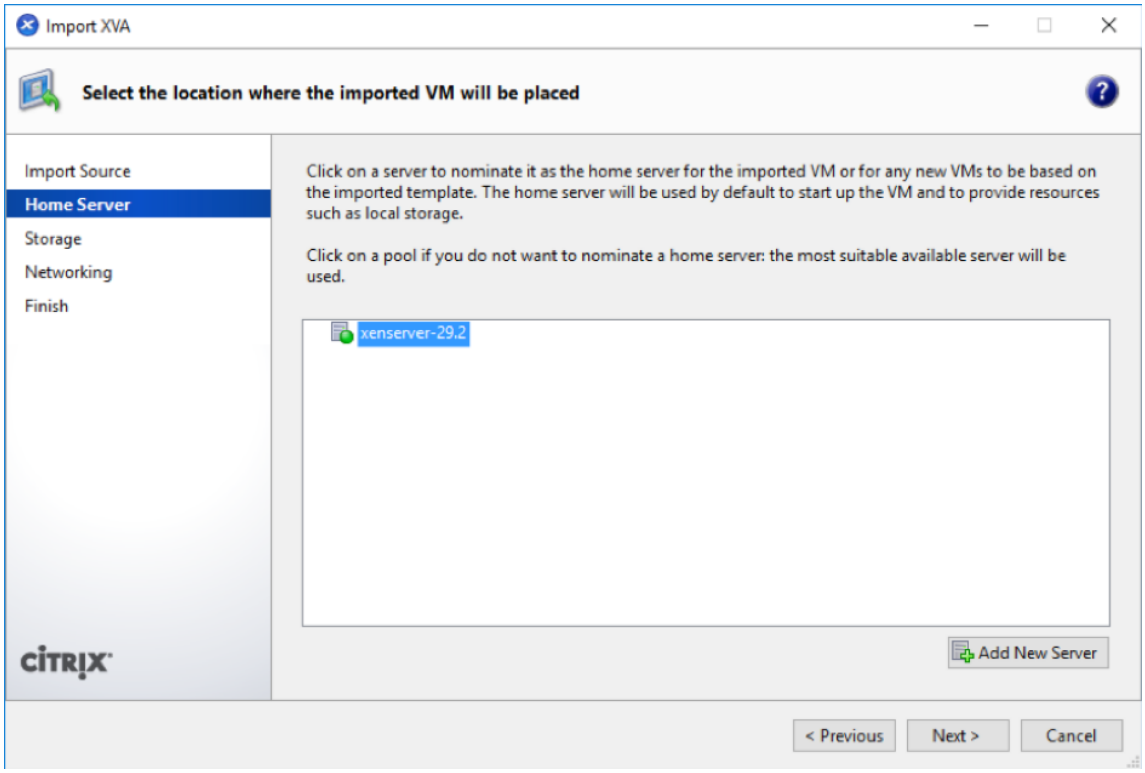



2. Busque el archivo .xva descargado, selecciónelo y haga clic en **Siguiente**.




3. Seleccione un servidor XenServer creado anteriormente como la ubicación a la que quiere importar la máquina virtual y haga clic en **Siguiente**.

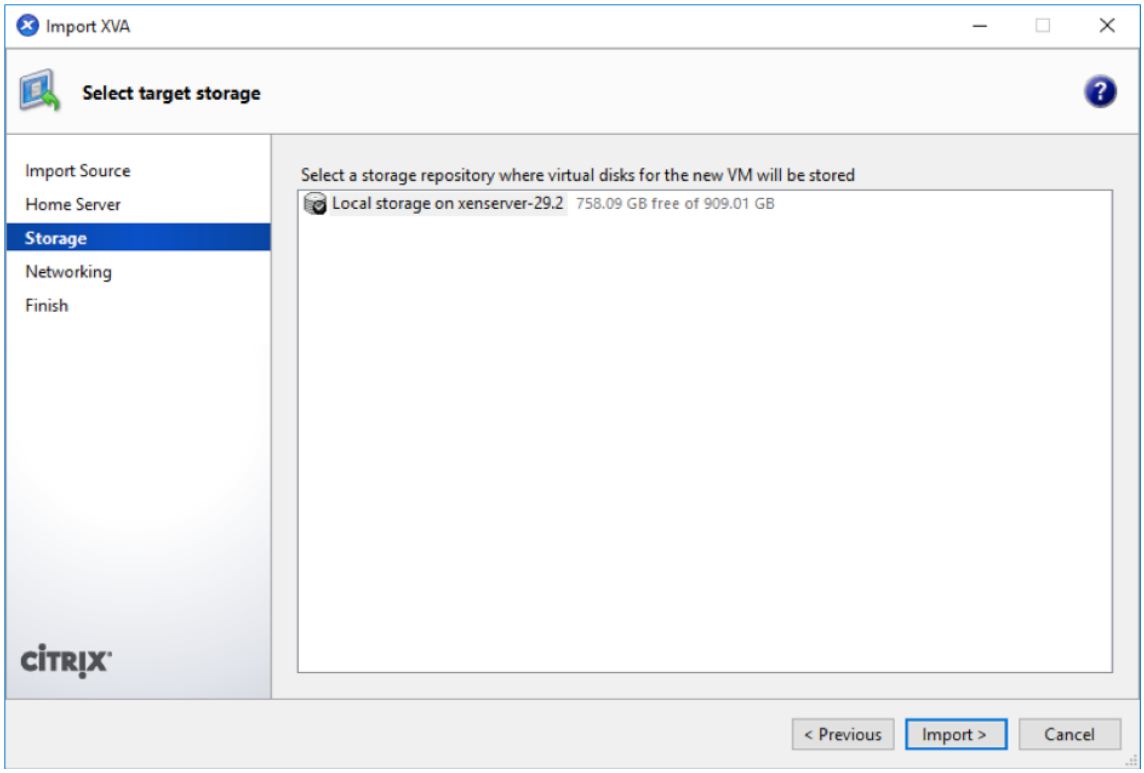



4. Seleccione un repositorio de almacenamiento en el que esté almacenado el disco virtual de la

nueva máquina virtual y haga clic en **Importar**.

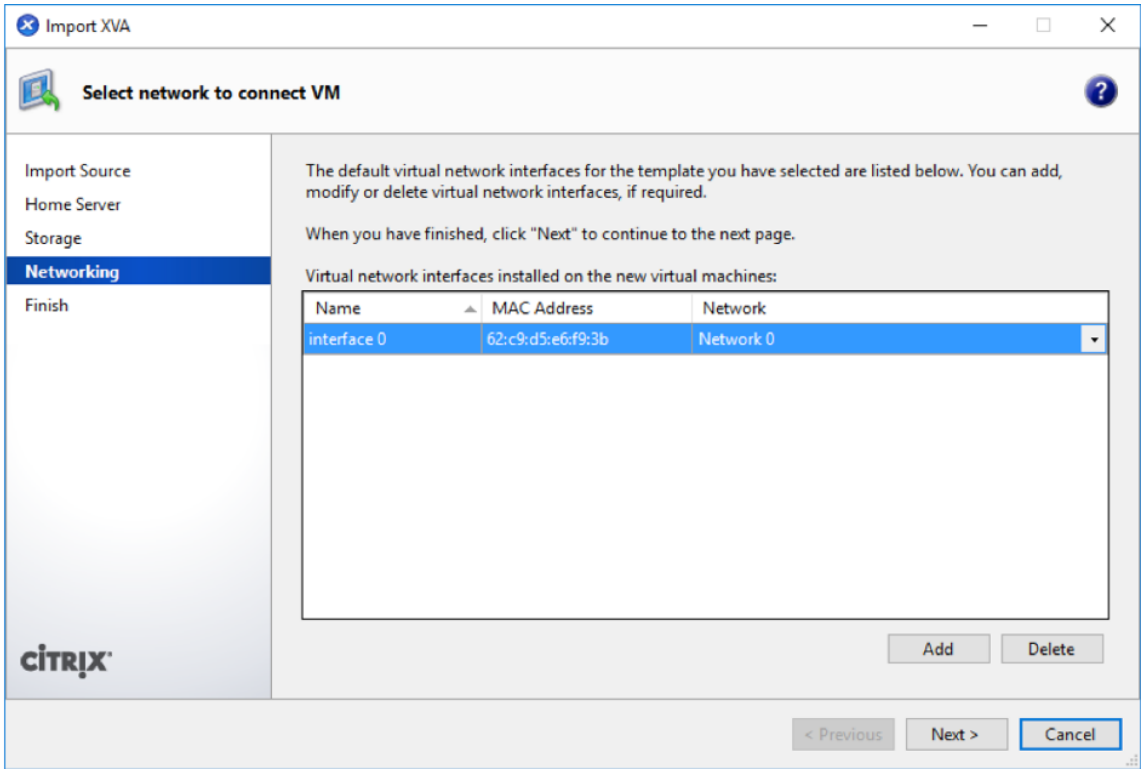
Por ahora, puede aceptar el recurso de almacenamiento predeterminado. También puede configurar el almacén de datos.




La máquina virtual Citrix SD-WAN Orchestrator for On-premises importada aparece en el panel izquierdo.

5. Seleccione la red a la que quiere conectar la máquina virtual y haga clic en **Siguiente**.




6. Haga clic en **Finalizar**.

## Ver y registrar la dirección IP de administración en XenServer

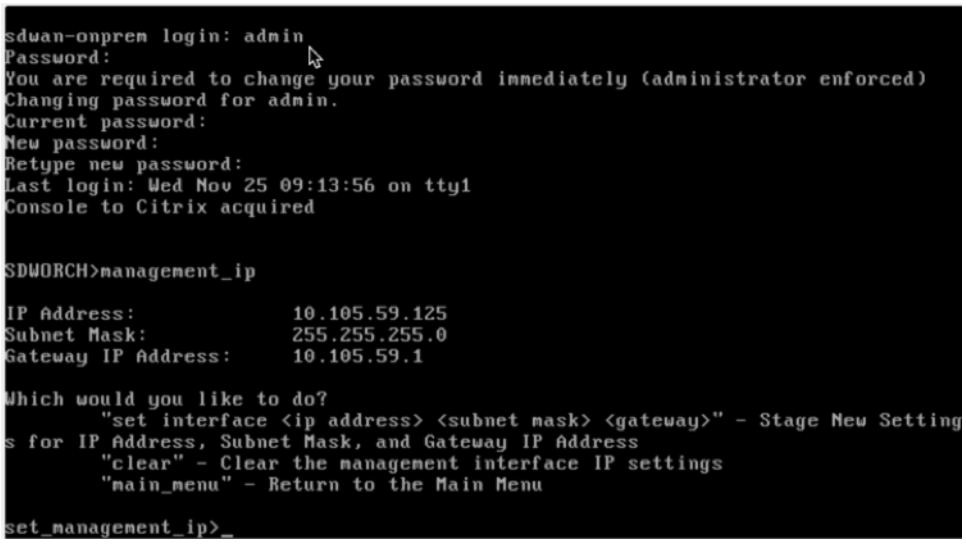
La dirección IP de administración es la dirección IP de la máquina virtual Citrix SD-WAN Orchestrator for On-premises. Utilice esta dirección IP para iniciar sesión en la interfaz de usuario web de Citrix SD-WAN Orchestrator for On-premises.

> **Nota**
>
> El servidor DHCP debe estar presente y disponible en la red SD-WAN.

Para mostrar la dirección IP de administración:

1. En la interfaz de XenCenter, en el panel izquierdo, haga clic con el botón secundario en la nueva máquina virtual de Citrix SD-WAN Orchestrator for On-premises y seleccione **Iniciar**.
2. Cuando se inicie la máquina virtual, haga clic en la ficha **Consola**.




3. Anote la dirección IP de administración.

> **Nota**
>
> El servidor DHCP debe estar presente y disponible en la red SD-WAN; de lo contrario, este paso no se puede completar.

4. Inicie sesión en la máquina virtual. Las credenciales de inicio de sesión predeterminadas para la nueva máquina virtual Citrix SD-WAN Orchestrator for On-premises son las siguientes:

   **Inicio de sesión**: Admin

   **Contraseña**: Contraseña

   > **Nota**
   >
   > Es obligatorio cambiar la contraseña predeterminada de la cuenta de usuario administrador al iniciar sesión por primera vez. Este cambio se aplica mediante la CLI y la interfaz de usuario.

   Si el servidor DHCP no está configurado en la red Citrix SD-WAN, debe introducir manualmente una dirección IP estática.

Para configurar una dirección IP estática como dirección IP de administración:

1. Cuando se inicie la máquina virtual, haga clic en la ficha Consola.
2. Inicie sesión en la máquina virtual. Las credenciales de inicio de sesión predeterminadas para la nueva máquina virtual Citrix SD-WAN Orchestrator for On-premises son las siguientes:

   **Inicio de sesión**: Admin

   **Contraseña**: Contraseña

3. En la consola, introduzca el comando CLI `management_ip`.

4. Introduzca el comando `set interface <ipaddress> <subnetmask> <gateway>` para configurar la IP de administración.
5. ¿Confirma que quiere cambiar la configuración IP de la interfaz de administración?

   Puede perder la conectividad con el dispositivo. <y/n>?

   Pulse "y"para cambiar la IP y acceder a la IP de administración configurada después de casi 6 a 7 minutos.

## Incorporación de SD-WAN Orchestrator para entornos locales

October 31, 2022

A continuación, se muestra una descripción general del proceso de incorporación de Citrix SD-WAN Orchestrator for On-premises:

- Proveedor de incorporación e arrendatarios: Nuestros clientes pueden consumir un servicio SD-WAN administrado de los socios de Citrix, habilitado por el servicio Citrix SD-WAN Orchestrator multiusuario.
- Incorporación de empresas "hágalo usted mismo"(DIY): El servicio Citrix SD-WAN Orchestrator también está disponible como un servicio autogestionado para las empresas.

### Proveedor de incorporación y arrendatarios

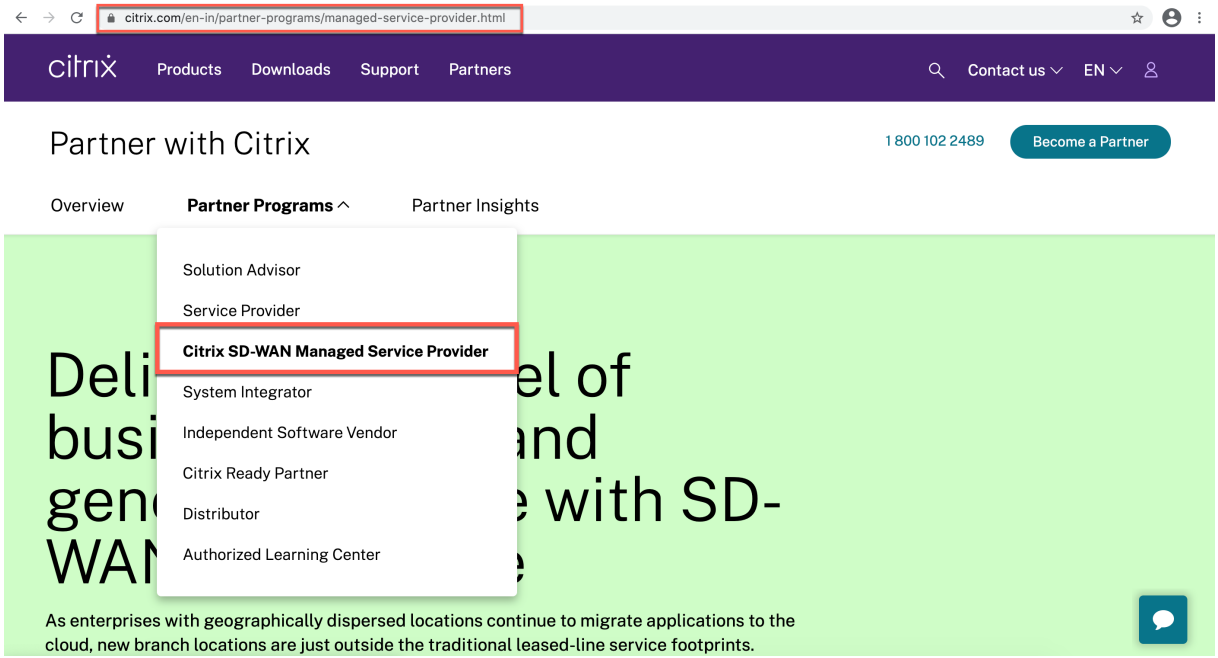
En esta sección se describe el proceso de incorporación de socios de Citrix y sus arrendatarios.
A continuación se muestra un resumen del proceso de incorporación:

1. Un posible socio se inscribe como Citrix Partner.
2. Citrix Partner se registra como revendedor de Citrix SD-WAN.

#### El socio se suscribe a un programa de asociación de Citrix

Un posible socio tendría que inscribirse en el Programa de proveedores de servicios (CSP) de Citrix: Suscripción a CSP.
Un socio también puede inscribirse en el programa de proveedores de servicios gestionados Citrix SD-WAN, que se ha creado especialmente para los socios de Citrix SD-WAN: SD-WAN MSP Sign Up.

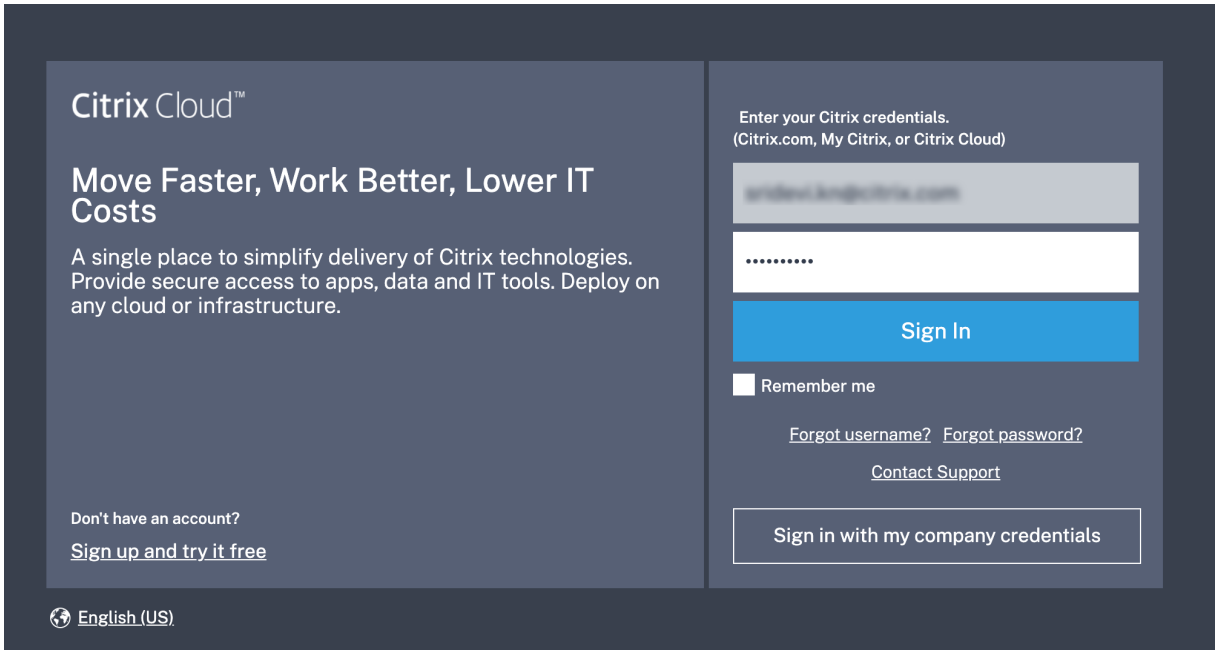
 




Se crea una cuenta de Citrix Cloud (CC) para el socio como parte del proceso de registro. Para obtener más información, consulte Registrarse en Citrix Cloud.

**El socio se registra como distribuidor de Citrix SD-WAN**

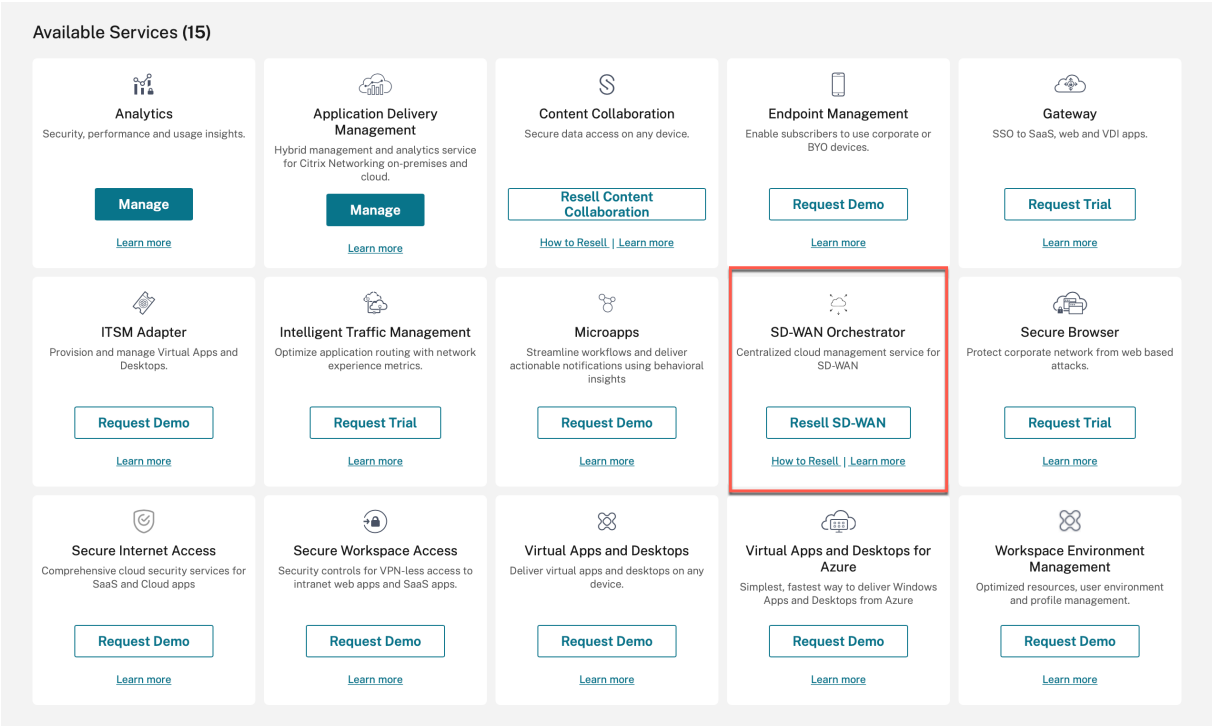
El socio inicia sesión en la cuenta de Citrix Cloud.

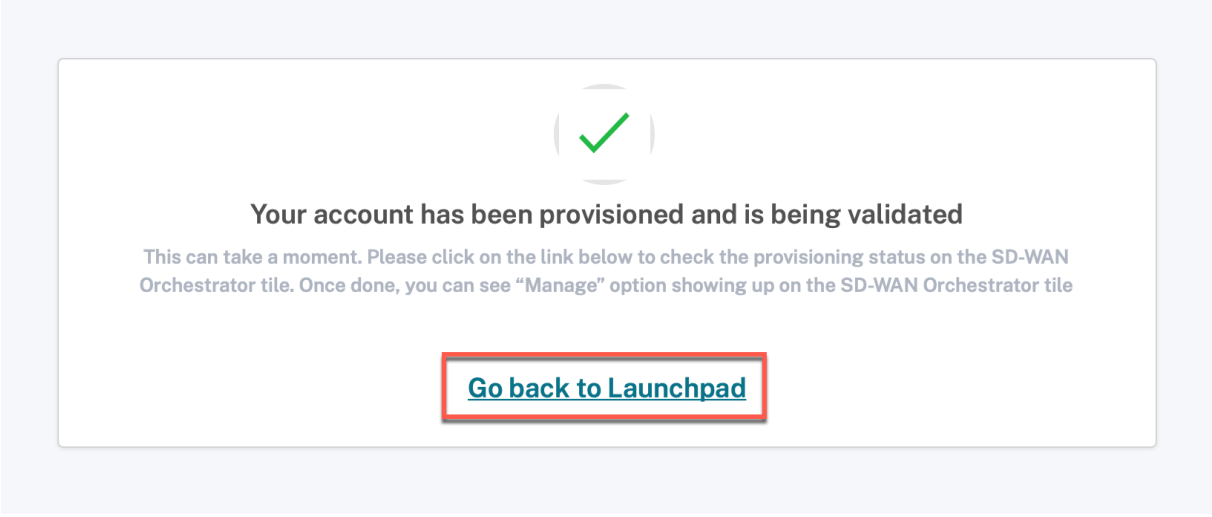



En la página principal se muestra un menú con todos los servicios disponibles ofrecidos en Citrix Cloud. El icono del **servicio Citrix SD-WAN Orchestrator** se encuentra en la sección **Servicios**

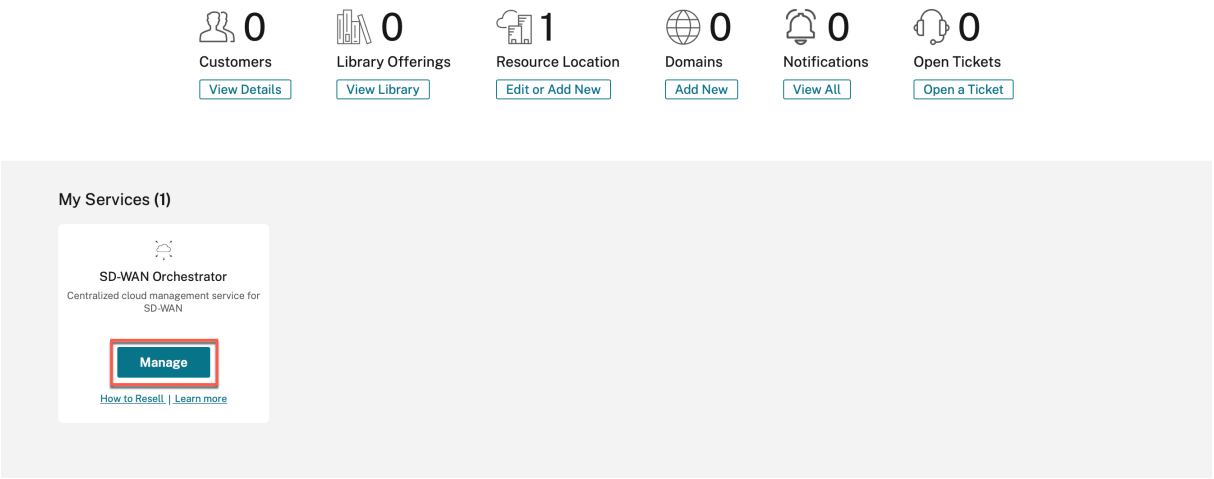
**disponibles**. El partner hace clic en **Resell SD-WAN** en el cuadro para registrarse como revendedor o proveedor de servicios de Citrix SD-WAN.




El icono del **servicio Citrix SD-WAN Orchestrator** ahora aparece en **Mis servicios**.

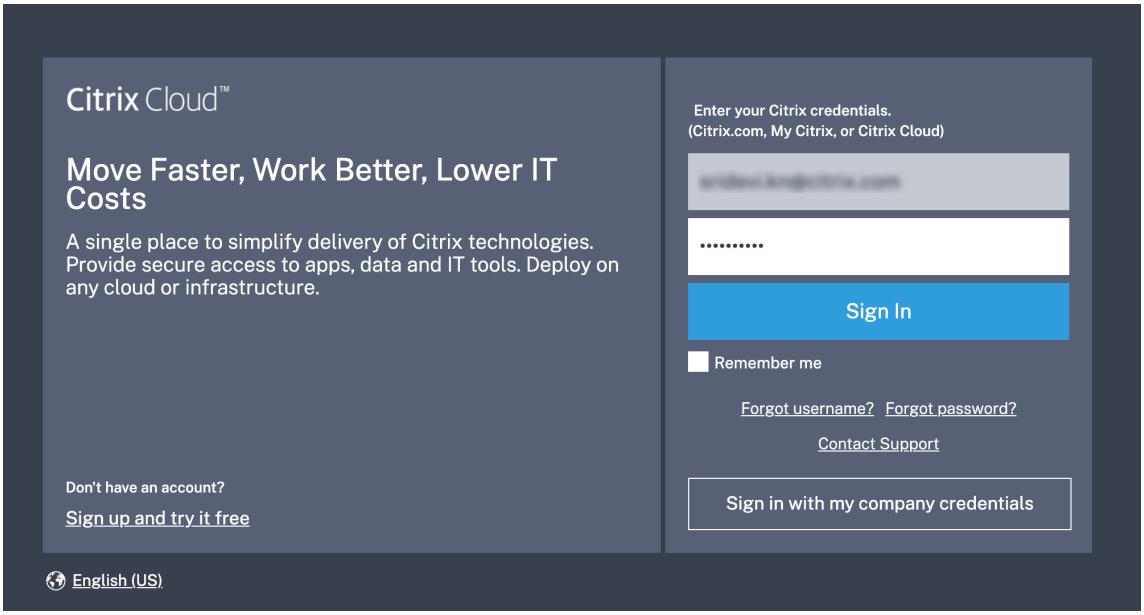



## Incorporación de clientes de empresas DIY

En esta sección se describe el proceso para incorporar clientes de empresas DIY y el procedimiento para invitar a administradores a administrar su red SD-WAN.

### Incorporación de clientes DIY

1. El cliente inicia sesión en la cuenta de Citrix Cloud.

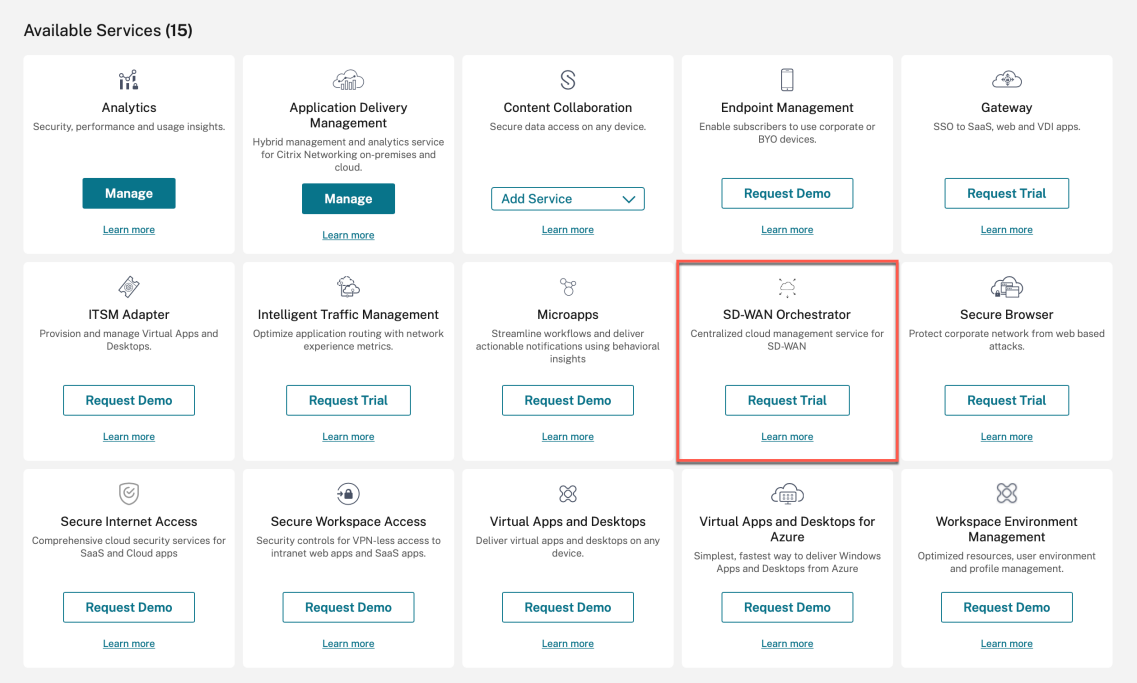



   En la página principal se muestra un menú con todos los servicios disponibles ofrecidos en Citrix Cloud. El icono del **servicio Citrix SD-WAN Orchestrator** se encuentra en la sección **Servicios disponibles**.

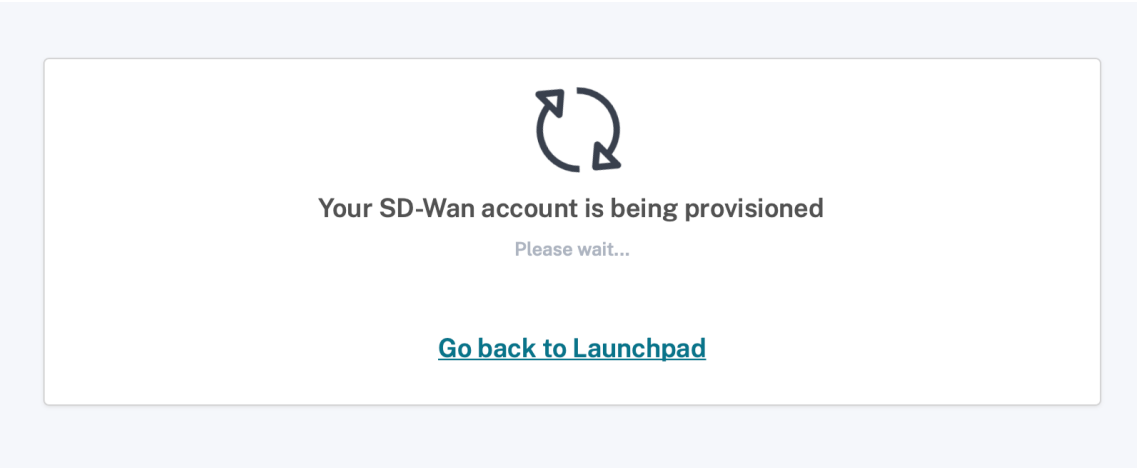
 

> **Nota**
>
> Asegúrese de registrarse en Citrix Cloud con una sola cuenta oficial. El nombre de la empresa y el ID de correo electrónico utilizados deben estar asociados a una sola cuenta de Citrix Cloud.

2. El cliente hace clic en **Solicitar prueba**.

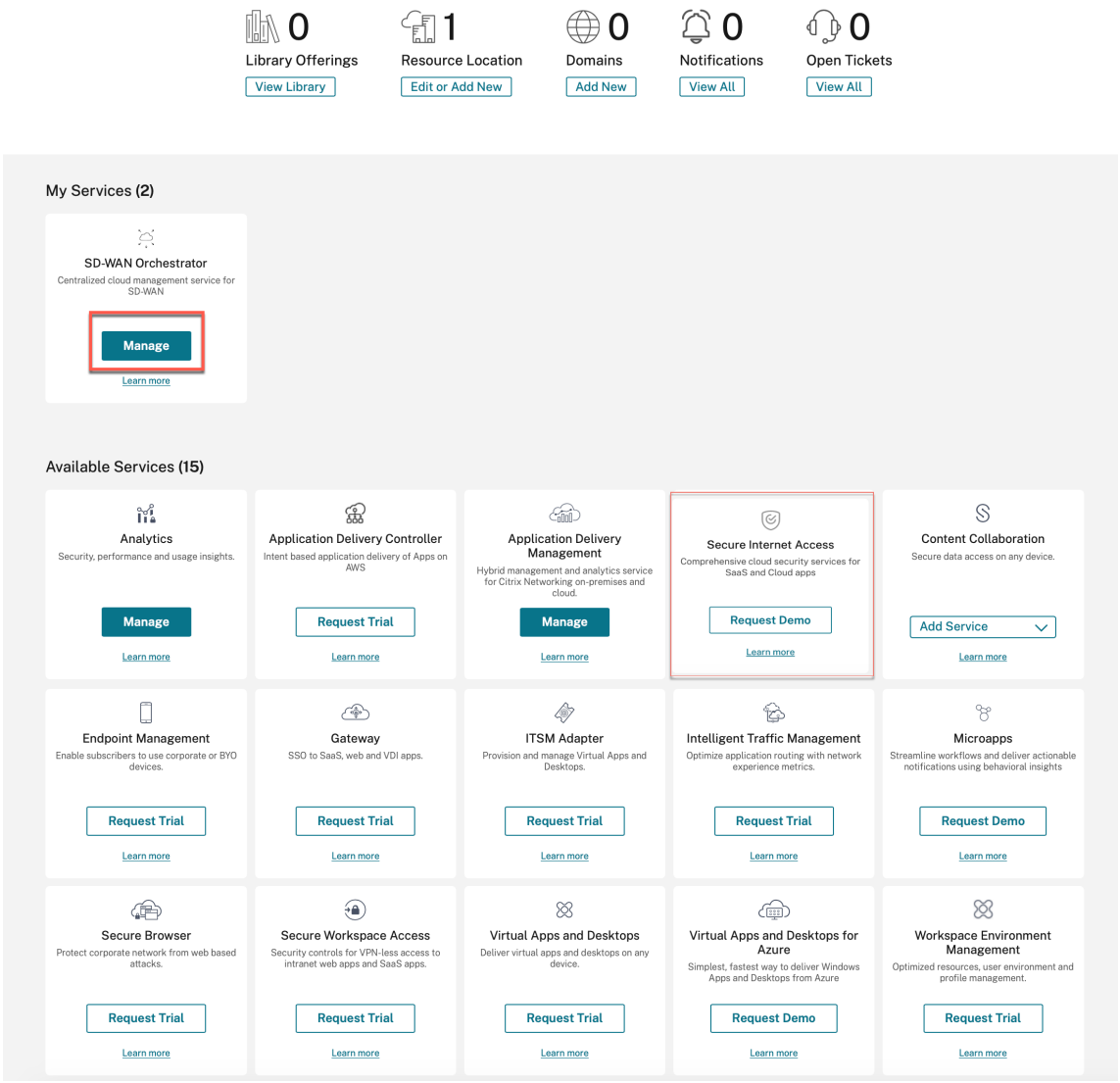



La cuenta SD-WAN del cliente se aprovisiona.




3. El icono del **servicio Citrix SD-WAN Orchestrator** ahora aparece en **Mis servicios**.




# Citrix SD-WAN Orchestrator para inicio de sesión local

July 15, 2023

Este artículo describe cómo un cliente puede iniciar sesión por primera vez en Citrix SD-WAN Orchestrator for On-premises.

Los siguientes son los requisitos previos que debe cumplir antes de iniciar sesión en Citrix SD-WAN Orchestrator for On-premises:

- Debe tener una cuenta de Citrix Cloud.  Para obtener más información, consulte El cliente accede a SD-WAN Orchestrator.

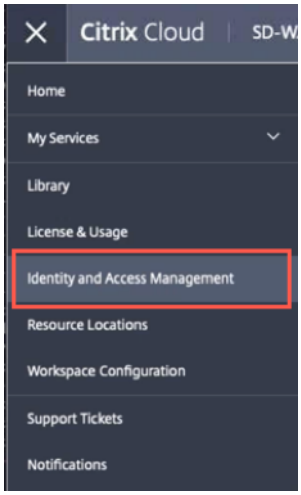
- Para utilizar Citrix SD-WAN Orchestrator for On-premises, debe tener una cuenta en el servicio Citrix SD-WAN Orchestrator. Para obtener más información, consulte Incorporación del servicio Citrix SD-WAN Orchestrator.
- Cree un administrador con privilegios personalizados.
- Cree un cliente desde la página de acceso a la API para obtener el ID del cliente, el identificador y los detalles secretos. Estos detalles son necesarios durante el inicio de sesión de Citrix SD-WAN Orchestrator for On-premises

> **Nota**
>
> Sin el inicio de sesión en la nube, no puede continuar con el inicio de sesión local.

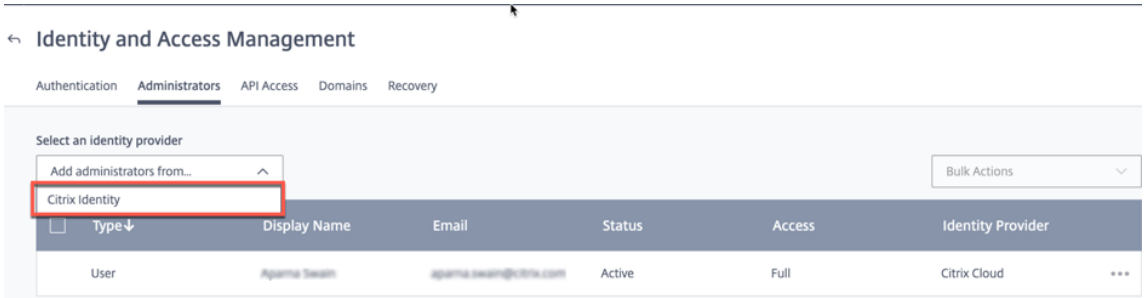
## Crear administrador

Un proveedor o un cliente empresarial pueden invitar a un administrador a administrar su red SD-WAN. Realice los siguientes pasos para invitar a un administrador:

1. Inicie sesión en Citrix Cloud y vaya a **Administración de acceso e identidad**.

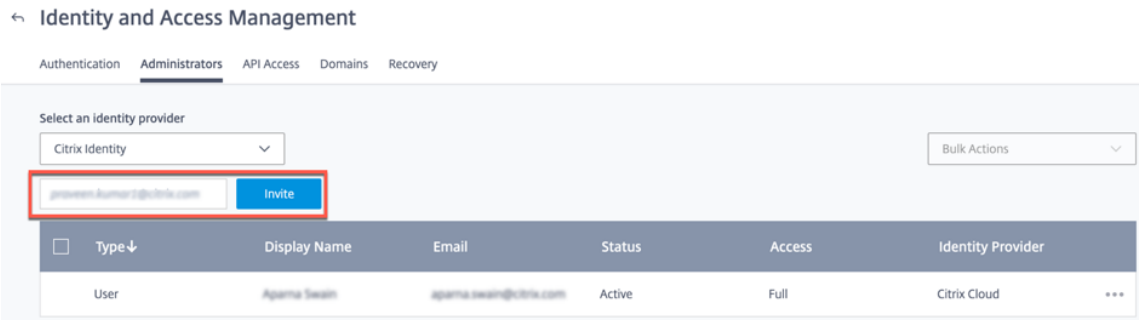



2. Vaya a la página **Administradores** y seleccione **Citrix Identity** en la lista desplegable del proveedor de identidades.



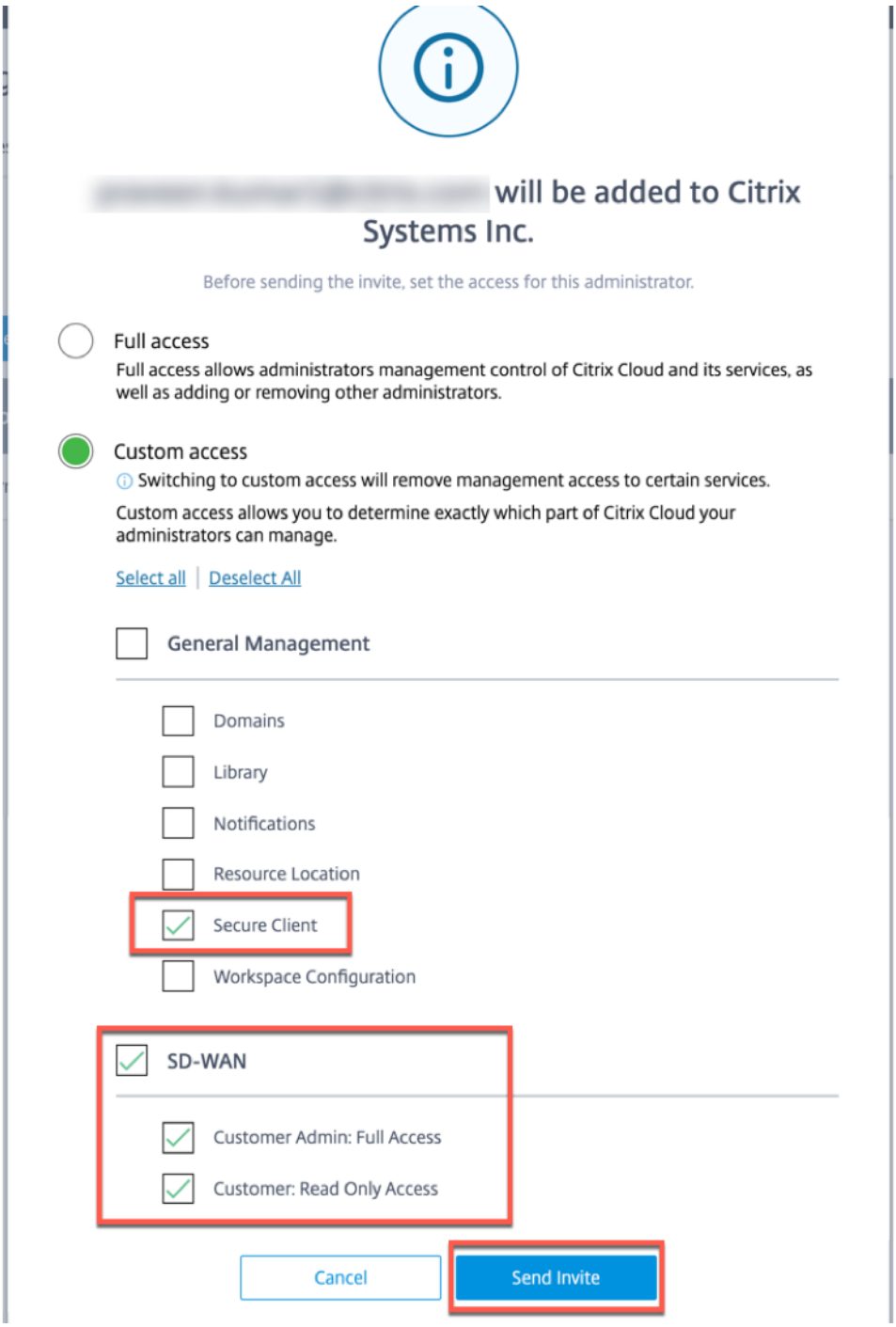

 

3. Introduzca la nueva ID de correo electrónico del administrador y haga clic en **Invitar**




4. Puede elegir entre **acceso completo** o **acceso personalizado**. Se recomienda configurar el acceso personalizado para el administrador que solo administre los servicios de SD-WAN. Cuando se selecciona el botón de opción **Acceso personalizado**, también debe seleccionar la casilla de verificación **Secure Client** en la sección **Administración general** y la casilla de verificación **SD-WAN**.




5. Haga clic en **Enviar invitación**.

Una vez que haya creado la cuenta de administrador, inicie sesión a través de la cuenta de administrador para generar las claves de **API**.

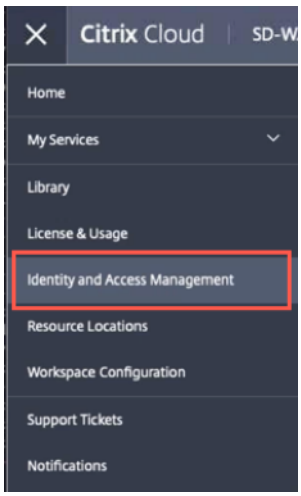
> **Nota:**
>
> Si ya tienes una función de administrador personalizada, puede usarla para crear el token de API.

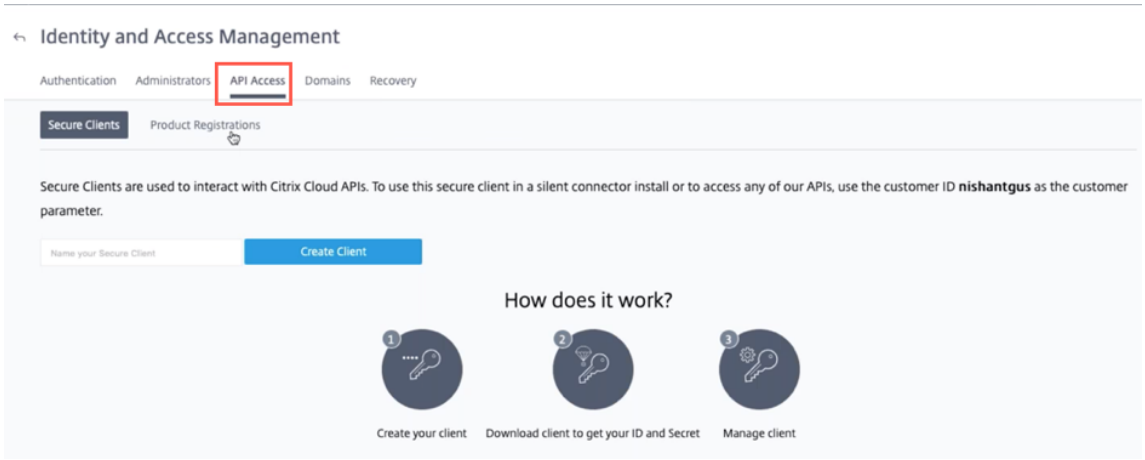
### Generar token de API

Realice los siguientes pasos para iniciar sesión en Citrix SD-WAN Orchestrator for On-premises.

1. Inicie sesión en Citrix Cloud y vaya a **Administración de acceso e identidad**.

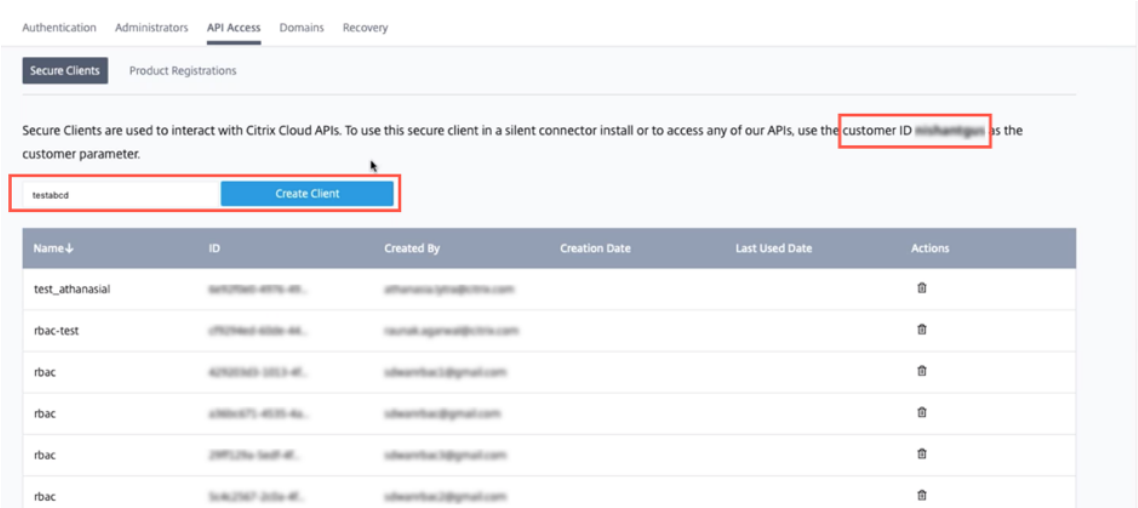



2. Ve a la página **de acceso a la API**

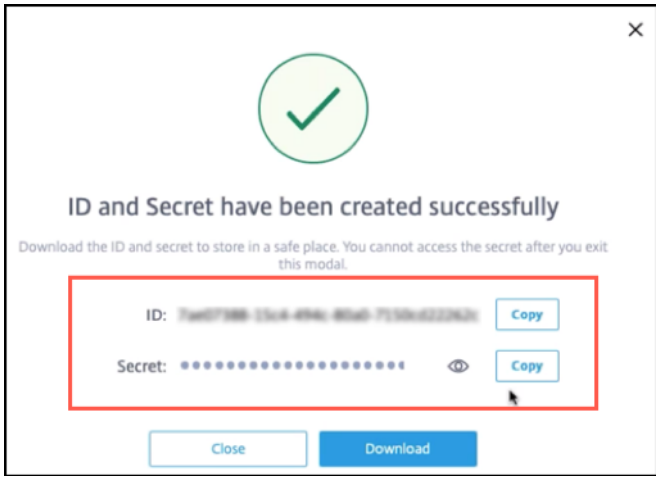



3. Crea un cliente. Anote el **ID de cliente** que necesita más adelante para iniciar sesión en Citrix SD-WAN Orchestrator for On-premises.




4. Al hacer clic en **Crear cliente**, le proporciona el **ID** y una **clave secreta** que puede copiar, guardar o descargar.




5. Vaya a su hipervisor de Citrix (XenServer/VMware) e inicie Citrix SD-WAN Orchestrator para aplicaciones locales.
6. Una vez que se inicie Citrix SD-WAN Orchestrator for On-premises, proporcione el nombre de usuario (admin) y la contraseña (contraseña) predeterminados.

> **Nota**
>
> Es obligatorio cambiar la contraseña predeterminada de la cuenta de usuario administrador al iniciar sesión por primera vez. Este cambio se aplica mediante la CLI y la interfaz de usuario.

7. Si el servidor DHCP no está configurado en la red SD-WAN, debe introducir manualmente una dirección IP estática. Para configurar una dirección IP estática como dirección IP de administración:

- En la consola, introduzca el comando CLI `management_ip`.
- Introduzca el comando `set interface <ipaddress> <subnetmask> <gateway>`.

> **Nota**
>
> - La dirección IP de administración es la dirección IP de la máquina virtual Citrix SD-WAN Orchestrator for On-premises. Utilice esta dirección IP para iniciar sesión en la interfaz de usuario web de Citrix SD-WAN Orchestrator for On-premises.
> - La interfaz de administración se puede configurar mediante dos métodos: CLI y DHCP.

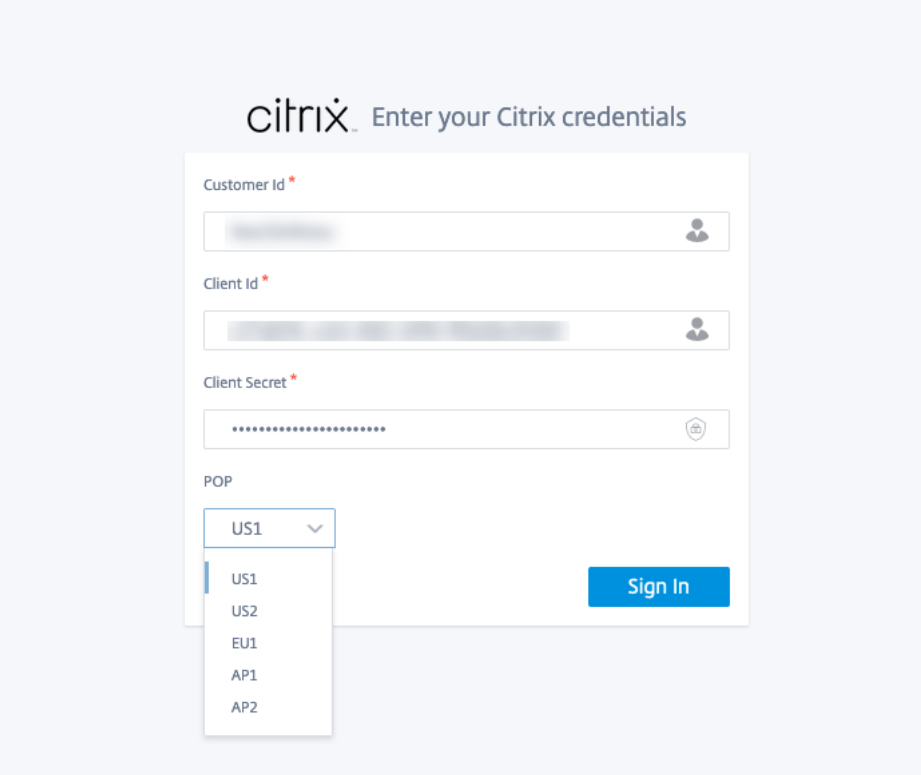
8. Una vez que se inicia Citrix SD-WAN Orchestrator for On-premises, se configura de forma predeterminada con los servidores DNS 9.9.9.9 y 149.112.112.112 como principales y secundarios, respectivamente. Si es necesario, puede cambiar la dirección IP del servidor DNS mediante los siguientes comandos:

   - En la consola, introduzca el comando CLI `set_dns`.
   - Introduzca el comando `set primary <ipaddress>` y, a continuación, introduzca `y` para confirmar el cambio.
   - Introduzca el comando `set secondary <ipaddress>` e introduzca `y` para confirmar el cambio.

```
SDWORCH>set_dns

Primary :               nameserver 9.9.9.9
Seconday :              nameserver 149.112.112.112

Which would you like to do?
        "set primary <ip address>" - Stage New Primary DNS IP Address
        "set secondary <ip address>" - Stage New Primary DNS IP Address
        "clear" - Clear all DNS IP Address
        "main_menu" - Return to the Main Menu

set_dns>set primary 8.8.8.8

Are you sure you want to change your Domain Name Server IP settings? <y/n>?
y

Primary :               nameserver 8.8.8.8
Seconday :              nameserver 149.112.112.112

Which would you like to do?
        "set primary <ip address>" - Stage New Primary DNS IP Address
        "set secondary <ip address>" - Stage New Primary DNS IP Address
        "clear" - Clear all DNS IP Address
        "main_menu" - Return to the Main Menu

set_dns>set secondary 9.9.9.9

Are you sure you want to change your Domain Name Server IP settings? <y/n>?
y

Primary :               nameserver 8.8.8.8
Seconday :              nameserver 9.9.9.9

Which would you like to do?
        "set primary <ip address>" - Stage New Primary DNS IP Address
        "set secondary <ip address>" - Stage New Primary DNS IP Address
        "clear" - Clear all DNS IP Address
        "main_menu" - Return to the Main Menu
```

9. Abra un navegador nuevo con la IP de administración. Aparece la siguiente pantalla:

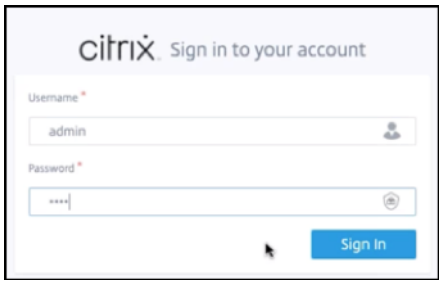
 




10. Proporcione el **ID de cliente, el ID de cliente** y el **secreto de cliente** que guardó o descargó anteriormente al crear el cliente desde la nube Orchestrator. Seleccione el POP en el que estaba incorporada su cuenta en la nube. No puede cambiar el POP después de iniciar sesión correctamente.

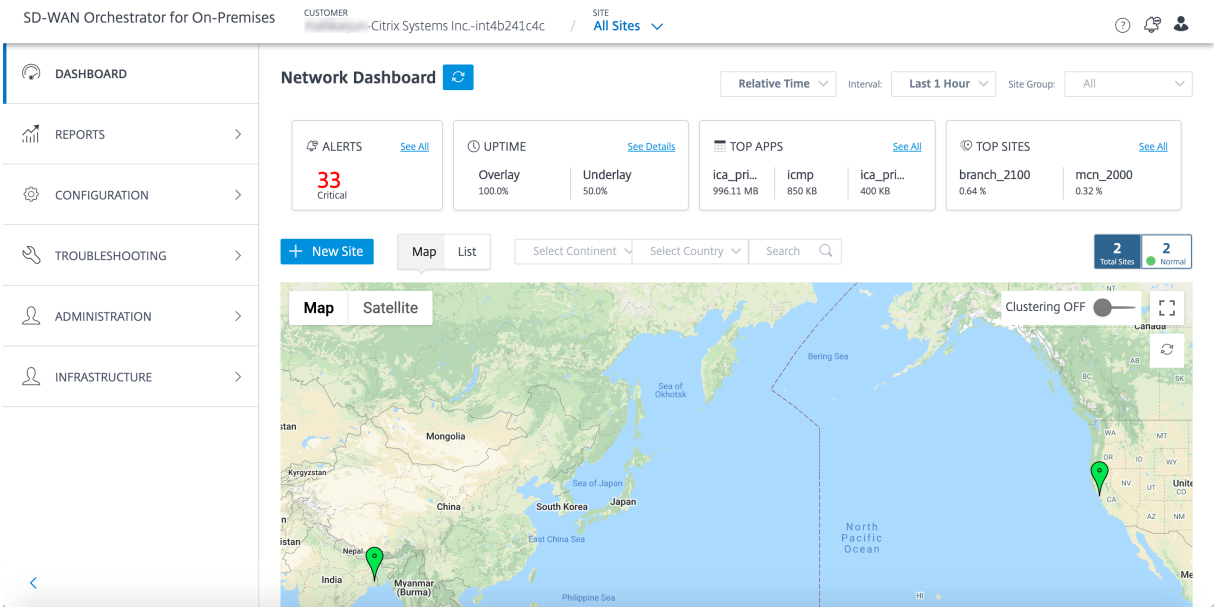
    > **Nota:**
    >
    > Esta pantalla aparece una vez cada 15 días. Para el siguiente inicio y cierre de sesión, solo verá la página de inicio de sesión local.

11. Proporcione el nombre de usuario y la contraseña predeterminados en la página de inicio de sesión local.




Puede ver que aparece la página Citrix SD-WAN Orchestrator for On-premises Dashboard.




# Citrix SD-WAN Orchestrator para licencias locales

October 31, 2022

Las licencias de Citrix SD-WAN Orchestrator for On-premises se aplican a los clientes del programa "hágalo usted mismo", es decir, a clientes empresariales directos

Como requisito previo para obtener licencias de Citrix SD-WAN Orchestrator for On-premises, asegúrese de haber iniciado sesión en Citrix Cloud. Para obtener más información, consulte Citrix SD-WAN Orchestrator para el inicio de sesión local.

La implementación local de Citrix SD-WAN Orchestrator está disponible de forma gratuita, pero el cliente debe asumir el coste de la infraestructura y el mantenimiento del servidor de administración.

## Modo de prueba

La cuenta Citrix SD-WAN Orchestrator for On-premises del cliente se aprovisiona en modo de prueba. El modo de prueba continúa durante un período predeterminado de 60 días.

Una vez que finaliza el período de prueba, se eliminan las rutas de datos del cliente. No se pueden implementar cambios adicionales hasta que se carguen licencias válidas. Los derechos de Citrix Cloud del cliente para Citrix SD-WAN Orchestrator for On-premises cambian de versión de prueba a producción cuando se aloja la primera licencia válida en él. Según el número y el tipo de licencias cargadas, un número equivalente de sitios puede obtener las autorizaciones de ancho de banda adecuadas. Un

mensaje persistente **Su periodo de prueba ha caducado. Actualice a Producción recuperando al menos un derecho de licencia válido en Orchestrator para restaurar la funcionalidad de la red y continuar con el uso.** se muestra para los clientes de prepago. Para obtener más información, consulte Recuperar y asignar derechos para el modelo de facturación prepagada.

### Modelo de facturación prepago

Se proporciona un modelo de facturación prepago para los clientes locales de Citrix SD-WAN Orchestrator. Los siguientes tres tipos de modelos de facturación prepago están disponibles:

- **Suscripción anual prepagada**: La suscripción prepaga tiene un plan de 1 año y otro de 3 años. La suscripción caduca en la fecha de caducidad. Todos los dispositivos de la red de clientes tienen una suscripción anual de prepago. Las licencias de mantenimiento se incluyen en el paquete de suscripción y permiten actualizar los dispositivos a versiones de software más recientes.
- **Prepago perpetuo**: Con el prepago perpetuo, las licencias no tienen límite de tiempo, duración restringida ni caducidad. Sin embargo, la licencia de mantenimiento de hardware está disponible como un complemento de pago y debe adquirirse por separado. Todos los dispositivos de la red del cliente tienen una suscripción permanente de prepago.

Para ver el modelo de facturación en Citrix SD-WAN Orchestrator for On-premises, al nivel de red, vaya a **Administración** > **Licencias** > **Seleccione el modelo de facturación**. El modelo de facturación se muestra como **Prepagado, anual y perpetuo**.

Cargue las licencias a todos los sitios de los clientes. Para obtener más información, consulte Recuperar y asignar derechos para el modelo de facturación prepagada.

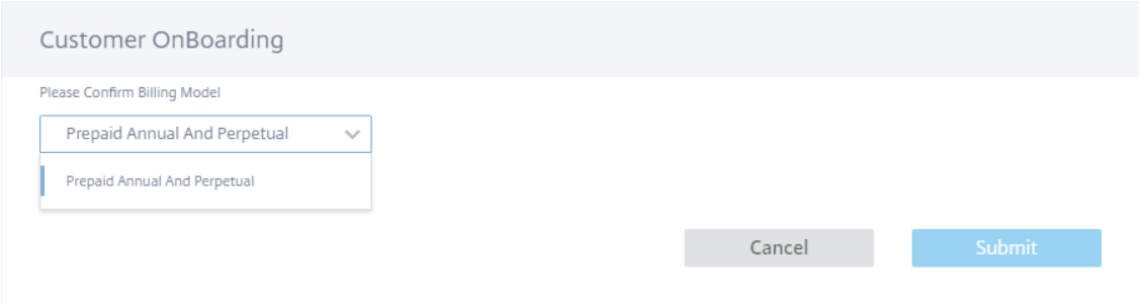
### Recuperar y asignar derechos para el modelo de facturación prepago

Puede recuperar los derechos de licencia mediante el código de acceso proporcionado por Citrix por correo electrónico. Como alternativa, el cliente también puede ver el código de acceso en el portal de administración de licencias de Citrix Cloud. El cliente puede tener un modelo de facturación de suscripción **prepaga perpetuao suscripción anual** prepagada en la red.

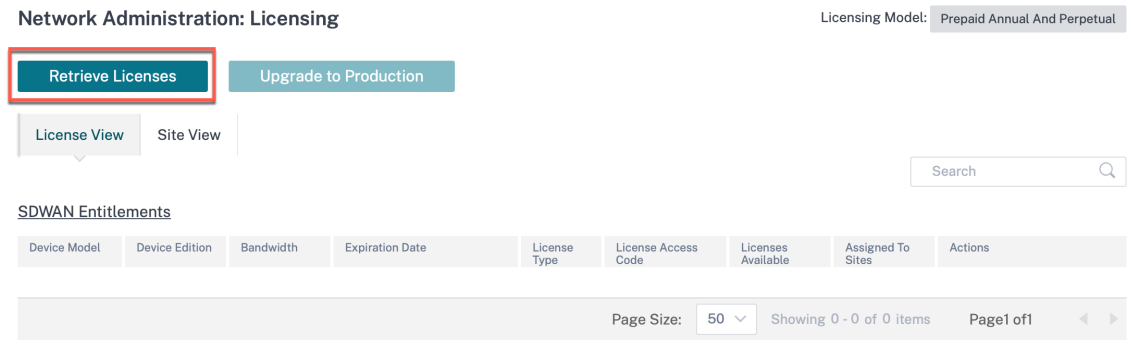
**Requisito previo**: Asegúrese de que las licencias de Citrix SD-WAN Orchestrator for On-premises no se asignen iniciando sesión en el portal de administración de licencias. Si las licencias están asignadas, libérelas o desasigne antes de usar los códigos de acceso a las licencias en el producto Citrix SD-WAN Orchestrator for On-premises.

1. En la interfaz de usuario de Citrix SD-WAN Orchestrator para locales, vaya a **Administración** > **Licencias** y haga clic en **Seleccionar modelo de facturación**. Selecciona un modelo de facturación y haga clic en **Enviar**.

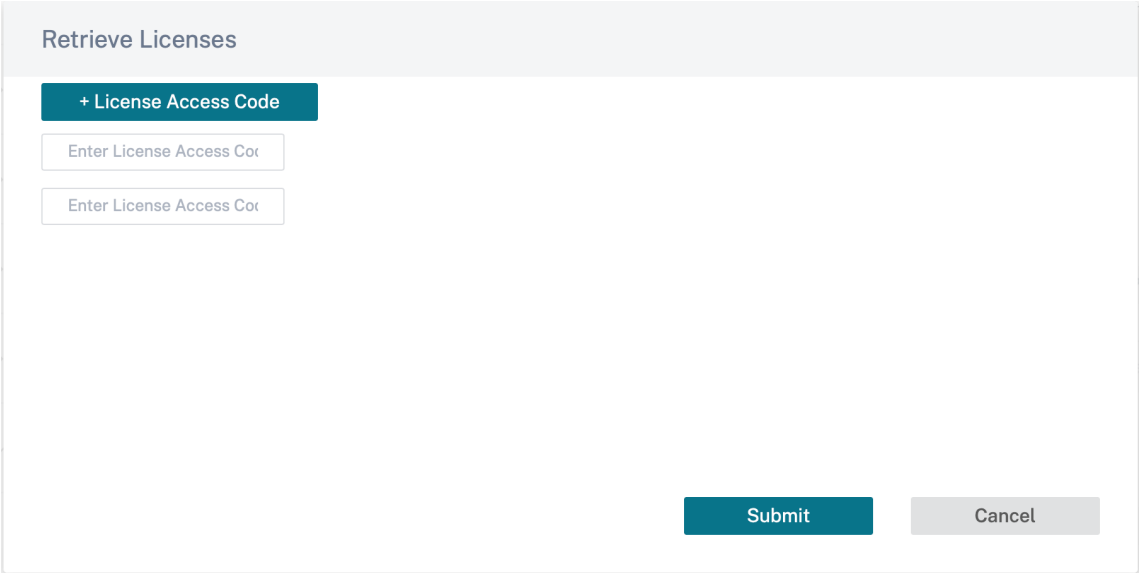
 




2. Haga clic en **Recuperar licencias**.

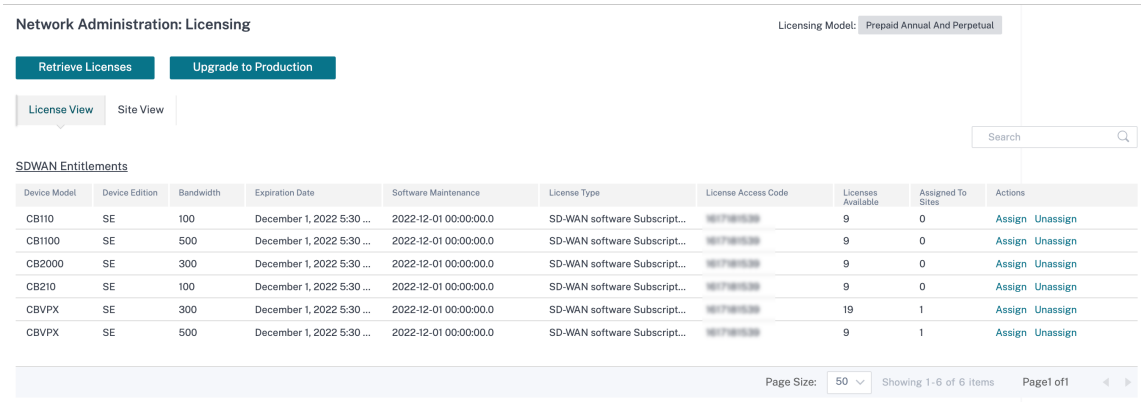



3. Haga clic en **+ Código de acceso a la licencia**, introduzca el número requerido de códigos de acceso para recuperar los derechos y haga clic en **Enviar**.

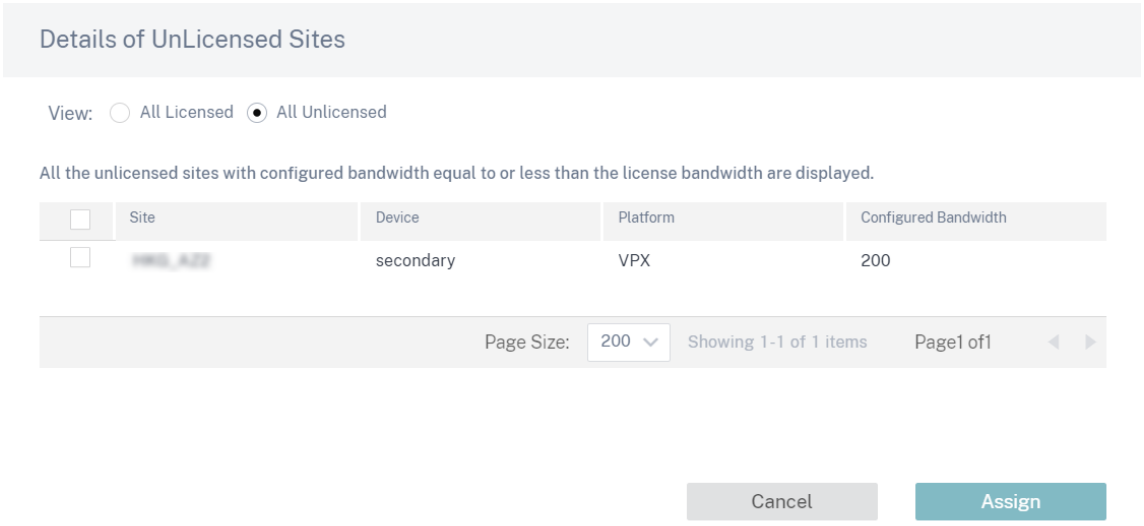



El Citrix SD-WAN Orchestrator for On-premises recupera los derechos y rellena la tabla de licencias.



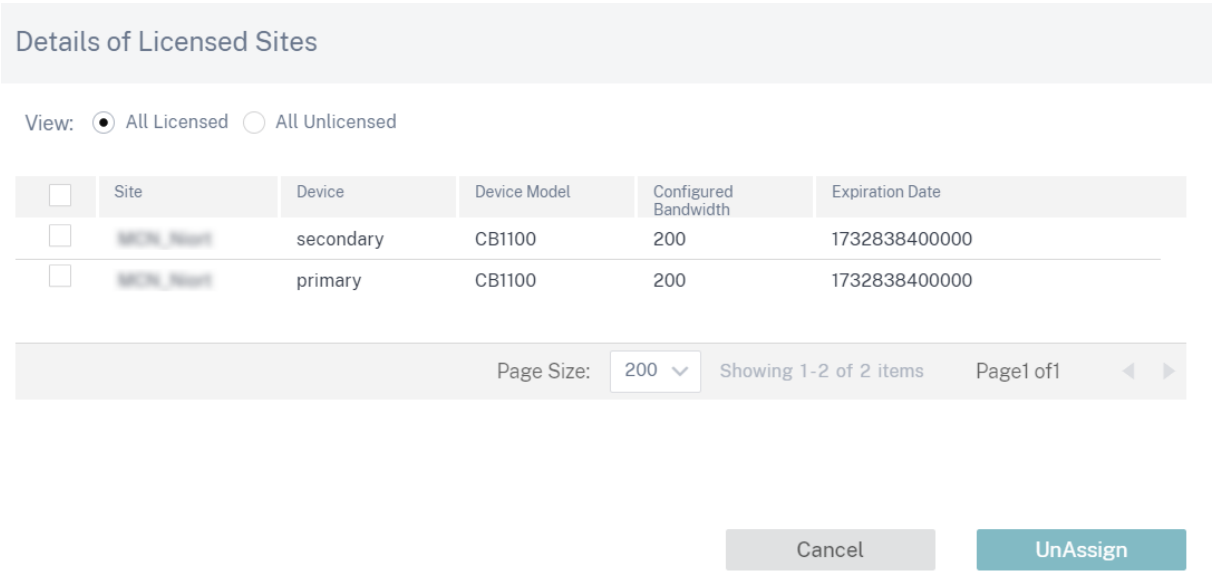

4. Haga clic en **Asignar/Desasignar** y seleccione **Todo sin licencia**. Se muestran todos los sitios sin licencia con ancho de banda configurado igual o inferior al ancho de banda de licencia.




5. Seleccione los sitios, haga clic en **Asignar** y, a continuación, en **Actualizar a producción**.

En la vista **Todas las licencias**, se muestra una lista de sitios con licencia. Puede optar por anular la asignación de las licencias y liberarlas de nuevo al grupo.




En la **vista del sitio**, los sitios se asocian automáticamente con las licencias según el ancho de banda y el ancho de banda de licencia configurados, lo que le permite asignar las licencias rápidamente.

> **Nota**
>
> Para asignar una licencia al dispositivo, un dispositivo debe tener un número de serie verificado.


### Caducidad de la licencia

Cuando la licencia caduca, se concede un período de gracia de 30 días. Se espera que el socio o cliente renueve sus licencias durante este tiempo. Una vez que finaliza el período de gracia, se eliminan las rutas de datos de red del cliente y no se pueden implementar cambios adicionales hasta que se renueven las licencias.

## Conectividad con dispositivos Citrix SD-WAN

October 31, 2022

Después de configurar los sitios en Citrix SD-WAN Orchestrator for On-premises, establezca la conectividad entre los dispositivos Citrix SD-WAN en los sitios con Citrix SD-WAN Orchestrator for On-premises. Puede establecer la conectividad de una de las siguientes maneras:

- **Autenticación unidireccional**: El dispositivo SD-WAN autentica Citrix SD-WAN Orchestrator for On-premises. Al habilitar la autenticación unidireccional, debe descargar el certificado Citrix SD-WAN Orchestrator for On-premises y cargarlo en el dispositivo SD-WAN.
- **Autenticación bidireccional**: Las SD-WAN se autentican entre sí mediante los certificados intercambiados. Al habilitar la autenticación bidireccional, debe cargar el certificado del dispositivo SD-WAN en Citrix SD-WAN Orchestrator para locales y también el certificado de Citrix SD-WAN Orchestrator para locales en el dispositivo SD-WAN.
- **Sin autenticación**: La conectividad se establece entre los dispositivos Citrix SD-WAN Orchestrator para locales y los dispositivos SD-WAN sin autenticación. No necesita usar el dispositivo SD-WAN ni el certificado Citrix SD-WAN Orchestrator for On-premises. Puede usar Sin autenticación si tiene una red segura, como MPLS.

> **Nota:**
>
> Se recomienda utilizar únicamente la **autenticación unidireccional** o bidireccional. En el caso de que no haya autenticación, debe elegir el servidor DNS seguro.

Puede configurar la conectividad con cada sitio de forma manual o utilizar la implementación automática sin intervención.

> **Nota**
>
> Citrix SD-WAN 11.3.0 es la versión de software mínima necesaria para que un dispositivo se conecte a Citrix SD-WAN Orchestrator for On-premises.

## Implementación sin contacto

La implementación sin intervención es un proceso automatizado para configurar la conectividad entre los dispositivos y Citrix SD-WAN Orchestrator for On-premises. Puede establecer la conectividad automáticamente mediante una configuración de implementación sin intervención fuera de la nube o una implementación sin intervención negociada en la nube.

### Implementación sin interacción fuera de la nube

La configuración de implementación sin intervención fuera de la nube le permite configurar Citrix SD-WAN Orchestrator para obtener información local en dispositivos SD-WAN. La API de NITRO que se ejecuta en el back-end gestiona la descarga y la carga de certificados. Descarga el certificado de Citrix

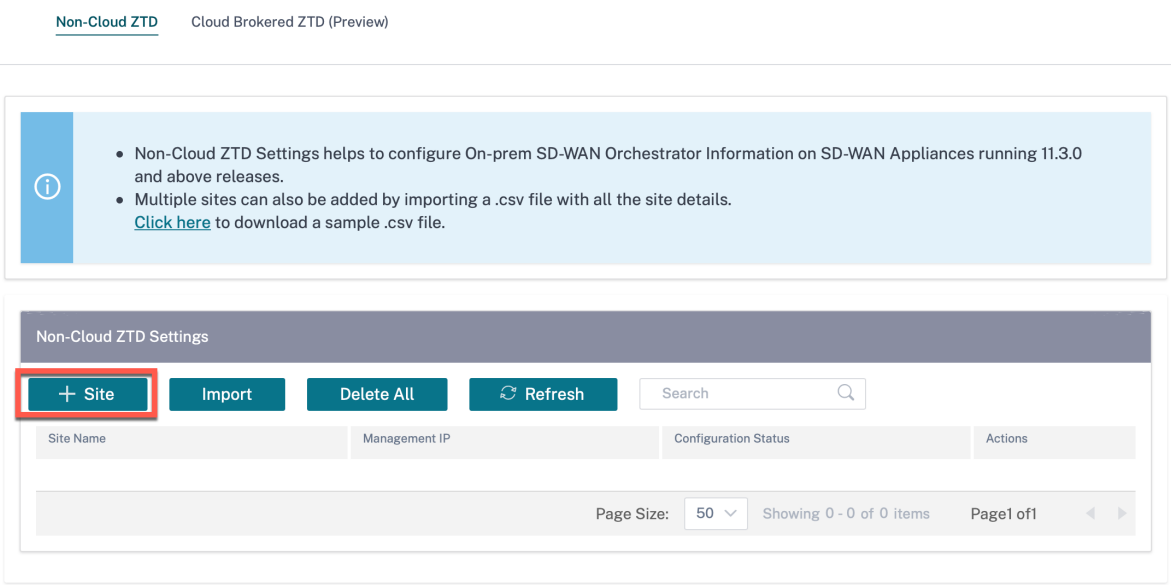
SD-WAN Orchestrator for On-premises, inicia sesión en el dispositivo SD-WAN y carga el certificado. También descarga el certificado del dispositivo SD-WAN y lo carga en Citrix SD-WAN Orchestrator for On-premises.

> **Nota**
>
> La implementación sin intervención fuera de la nube es compatible con los dispositivos SD-WAN que se ejecutan con la versión 11.3.0 o posterior.

La implementación sin intervención solo admite la **autenticación unidireccionaly la autenticación bidireccional**.**No se admite ninguna autenticación**. Si el**tipo de autenticación**está habilitado en**la página Administración > Autenticación de certificados**, se establece la autenticación bidireccional. Si el**tipo de autenticación** está inhabilitado, se establece la autenticación unidireccional.

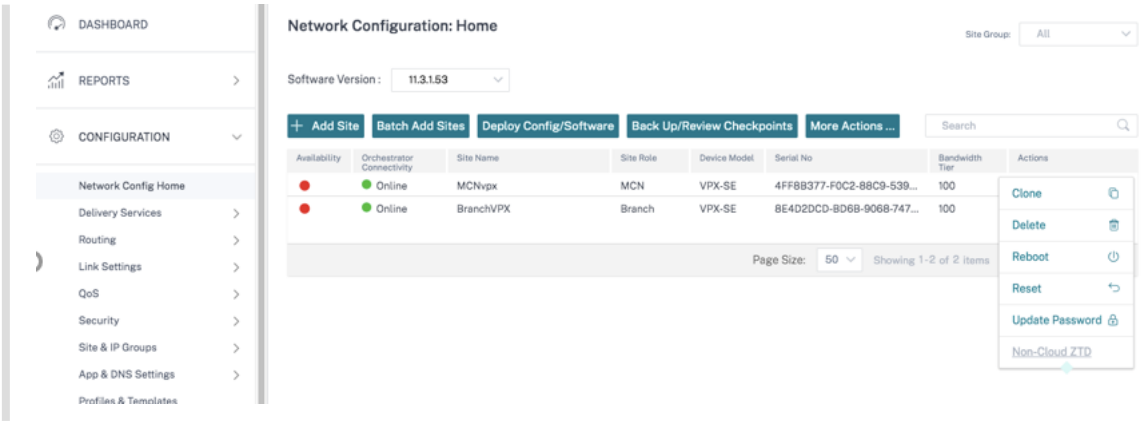
Puede agregar sitios manualmente o importar un archivo CSV para agregar varios sitios simultáneamente.

Para configurar los ajustes de implementación sin intervención en la nube, vaya a **Administración** > **Configuración de ZTD** > **ZTD fuera de la nube**y haga clic en **+ Sitio**.




> **Nota**
>
> También puede acceder a la configuración de implementación sin intervención fuera de la nube para cada sitio desde la página **principal de configuración de red**. Haga clic en el icono de acción del sitio y seleccione **ZTD que no sea de nube**.




Seleccione un sitio de la lista desplegable **Nombre del sitio** e introduzca la dirección **IP de administración** del dispositivo Citrix SD-WAN.

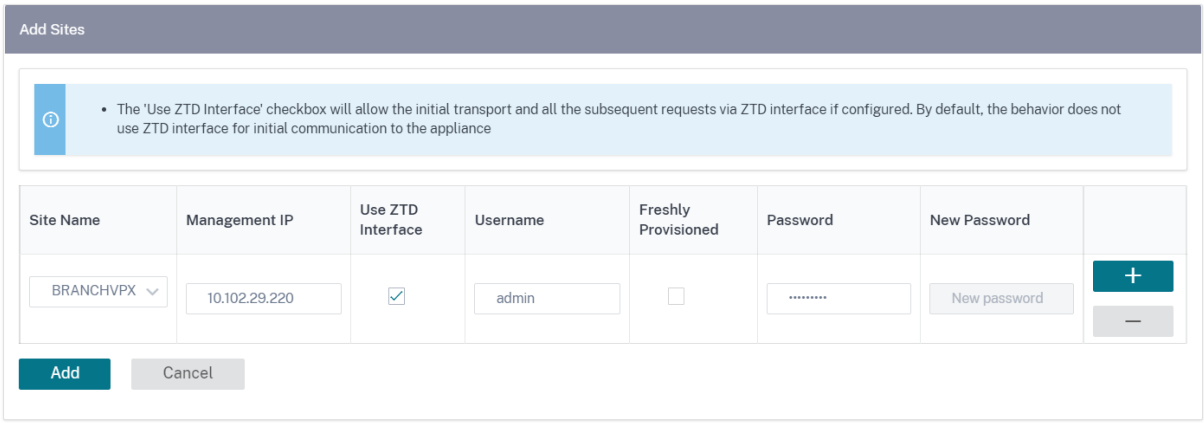
Al habilitar la opción **Usar interfaz ZTD**, se garantiza que la interfaz ZTD se utilice para ZTD que no esté en la nube, si la interfaz ZTD está habilitada en SD-WAN Orchestrator for On-premises.

> **Nota**
>
> - Ignore la opción **Use ZTD Interface** si la interfaz ZTD no está habilitada en SD-WAN Orchestrator for On-premises.
> - Active la opción **Usar interfaz ZTD** cuando el dispositivo SD-WAN pueda acceder a la dirección IP de la interfaz ZTD pero no pueda acceder a la dirección IP de administración.
> - No seleccionar la opción **Usar interfaz ZTD** después de habilitar la interfaz ZTD no significa que la dirección IP de la interfaz de administración se utilice para la comunicación entre el dispositivo SD-WAN y SD-WAN Orchestrator for On-premises. La opción **Use ZTD Interface** solo se usa para la configuración inicial del dispositivo con ZTD que no es de nube.

Proporcione el nombre de usuario y la contraseña del dispositivo. Seleccione la casilla de verificación **Recién aprovisionados** si va a agregar un sitio recientemente aprovisionado en el que no se ha cambiado la contraseña predeterminada. Introduzca la **nueva contraseña**. La contraseña predeterminada se cambia por la nueva contraseña durante este proceso de implementación sin intervención.

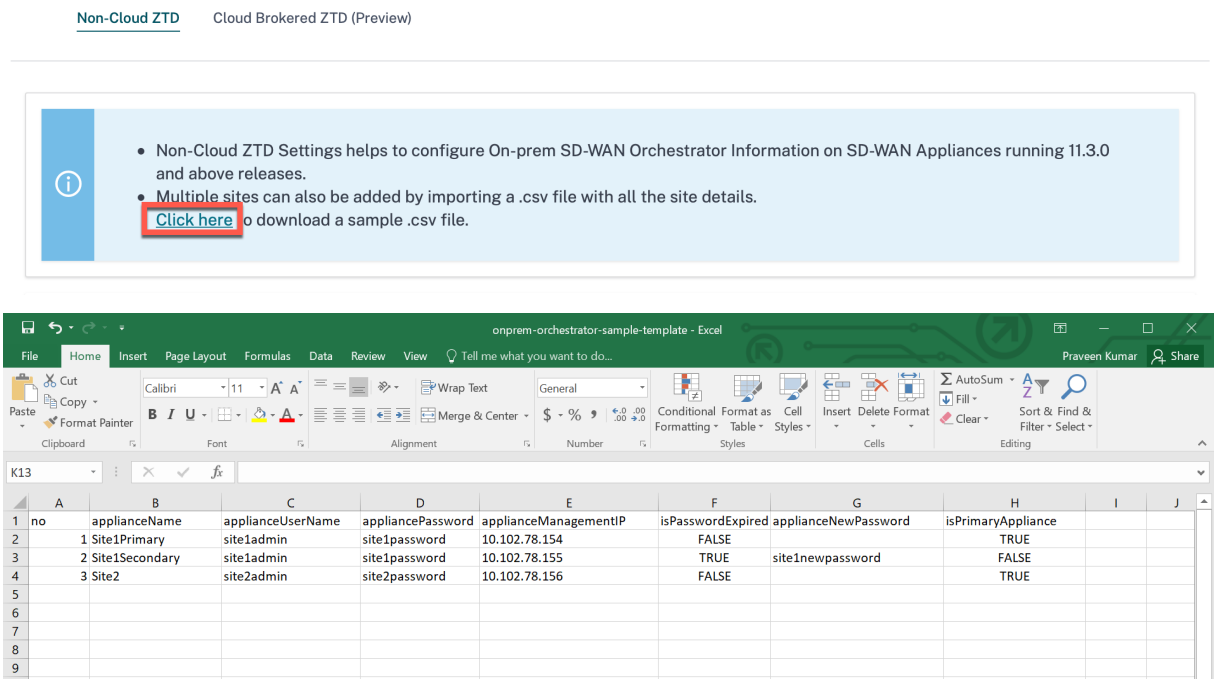
> **Nota**
>
> Para un sitio recién aprovisionado, es obligatorio cambiar la contraseña predeterminada en el momento del primer inicio de sesión.




Haga clic en **+** para seguir agregando más sitios.

También puede importar un archivo CSV para agregar varios sitios simultáneamente. Hay disponible un ejemplo de plantilla descargable en la interfaz de usuario. Descárguelo y proporcione los detalles del sitio.







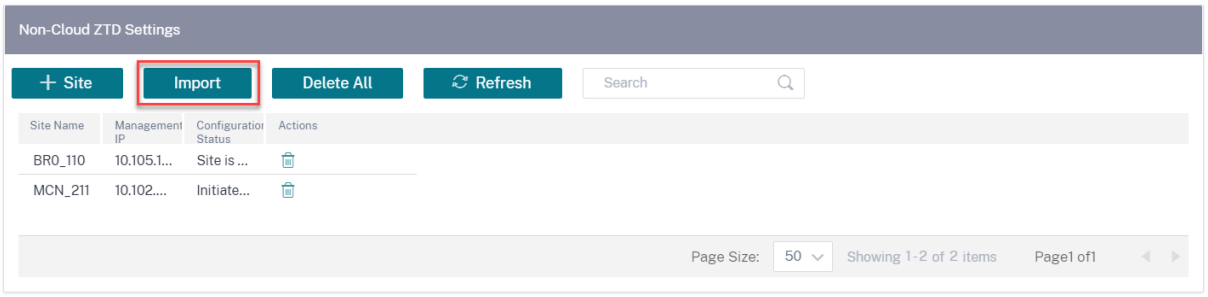
- **Nombre del dispositivo**: E l nombre del sitio configurado durante la configuración del sitio. Para obtener más información, consulte Configuración del sitio.
- **Nombre de usuario del dispositivo**: El nombre de usuario configurado en el dispositivo del sitio.
- **Contraseña del dispositivo**: La contraseña correspondiente al dispositivo del sitio.
- **¿Ha caducado la contraseña?** Determina si el dispositivo se ha aprovisionado recientemente. Si el valor es **True**, proporcione la **nueva contraseña del dispositivo**.
- **Nueva contraseña del dispositivo**: L a contraseña de los dispositivos recién aprovisionados. Si

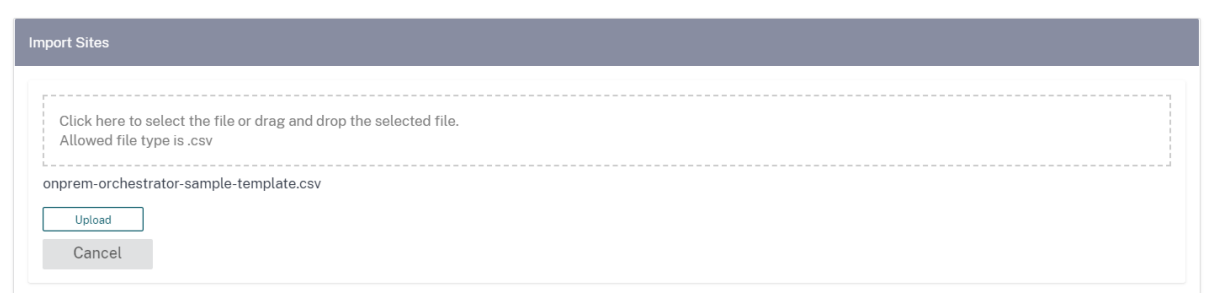
 

el valor Ha **caducado la contraseña esTrue**, proporcione la**nueva contraseña del dispositivo**.

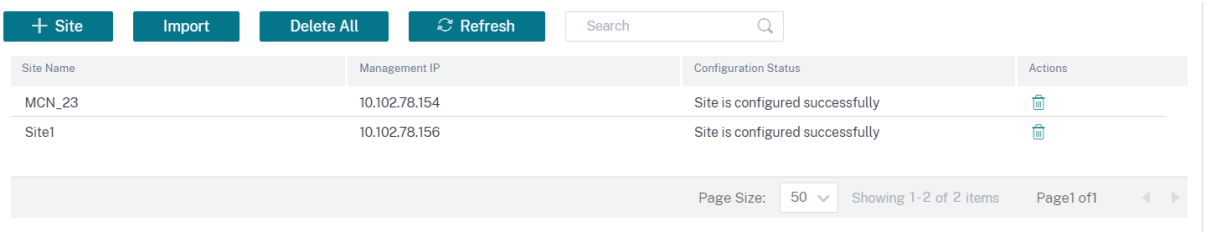
- **Es el dispositivo principal**: Si se configura la alta disponibilidad (HA), el dispositivo activo debe tener el valor True y el dispositivo en espera debe tener el valor False. Si HA no está configurado, el valor debe ser True.

Haga clic en **Importar**, selecciona el archivo CSV y haga clic en **Cargar**




Se muestra el estado de configuración de los sitios. Puede elegir eliminar los sitios de forma individual o Eliminar todos si los sitios no son necesarios para una implementación sin intervención.




### Implementación sin intervención mediante intermediación en la nube

La implementación sin intervención mediante intermediación en la nube utiliza el servicio Citrix SD-WAN Orchestrator como intermediario entre Citrix SD-WAN Orchestrator for On-premises y los dispositivos Citrix SD-WAN. Citrix SD-WAN Orchestrator for On-premises envía un paquete de configuración de implementación sin intervención en la nube al servicio Citrix SD-WAN Orchestrator. El paquete de configuración de implementación sin intervención en la nube consta de la siguiente información:

- Información de identidad local
- Tipo de autenticación

- Certificado local
- Detalles del dispositivo (lista de números de serie)

El servicio Citrix SD-WAN Orchestrator almacena la información recibida de Citrix SD-WAN Orchestrator for On-premises. Cuando un dispositivo contacta con el servicio Citrix SD-WAN Orchestrator con su número de serie, la inteligencia adquirida del servicio Citrix SD-WAN Orchestrator determina que el dispositivo debe ser administrado por Citrix SD-WAN Orchestrator for On-premises. El servicio Citrix SD-WAN Orchestrator transfiere los detalles del Citrix SD-WAN Orchestrator for On-premise al dispositivo. El dispositivo Citrix SD-WAN envía su certificado al servicio Orchestrator. El servicio Citrix SD-WAN Orchestrator recibe y almacena el certificado del dispositivo.

Citrix SD-WAN Orchestrator for On-premises obtiene periódicamente el certificado del dispositivo del servicio Citrix SD-WAN Orchestrator. Una vez que se establece una conexión segura entre Citrix SD-WAN Orchestrator for On-premises y el dispositivo, Citrix SD-WAN Orchestrator for On-premises envía la configuración y los archivos relevantes a los dispositivos.

La configuración de implementación sin intervención mediante intermediación en la nube solo está disponible para los clientes con una configuración administrada por el cliente. La configuración administrada por el proveedor no admite la configuración de implementación sin intervención mediante intermediación en la nube.

**Requisitos previos**

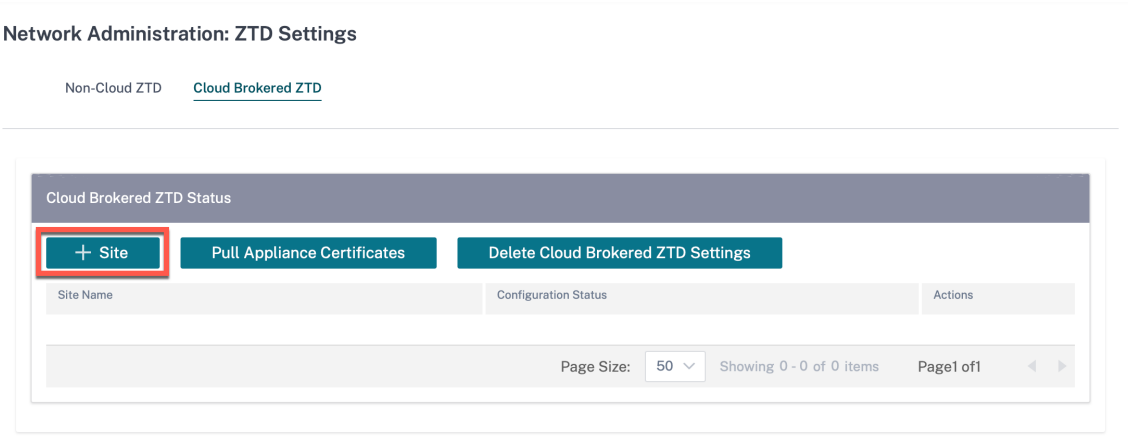
- Los dispositivos necesitan acceso a los siguientes nombres de dominio para establecer la conexión con el servicio Citrix SD-WAN Orchestrator:
  - sdwanzt.citrixnetworkapi.net
  - descargar.citrixnetworkapi.net
  - trust.citrixnetworkapi.net
  - sdwan-home.citrixnetworkapi.net
- Asegúrese de que Citrix SD-WAN Orchestrator for On-premises siempre tenga conectividad con el servicio Citrix SD-WAN Orchestrator con los dispositivos SD-WAN integrados.
- Asegúrese de que el dispositivo Citrix SD-WAN tenga conectividad con el servicio SD-WAN Orchestrator durante el proceso de incorporación inicial y si el restablecimiento de fábrica se realiza en el dispositivo SD-WAN.

Para configurar los ajustes de implementación sin intervención de Cloud Broker:

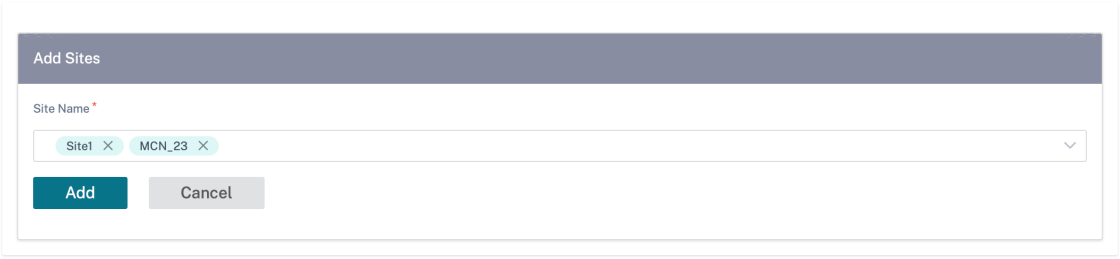
1. En Citrix SD-WAN Orchestrator for On-premises, cree y defina sitios mediante el flujo de trabajo guiado. Para obtener más información, consulte Configuración del sitio.
2. Verifique y compile la configuración mediante el rastreador de implementación. Para obtener más información, consulte la sección Deployment Tracker en el tema Configuración de red.

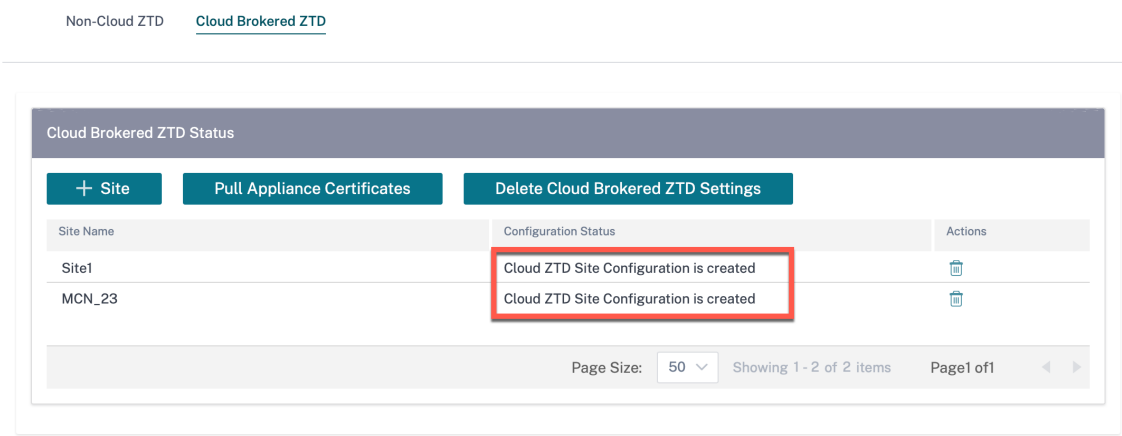
3. Vaya a **Administración > Configuración de ZTD > Cloud Brokered ZTD** y haga clic en **+ Sitio**.




4. En la lista desplegable, seleccione un nombre de sitio y haga clic en **Agregar**. Los sitios se enumeran en función de su configuración. Puede seleccionar uno o varios sitios.




5. La configuración de implementación sin intervención en la nube se crea y se envía al servicio Citrix SD-WAN Orchestrator.



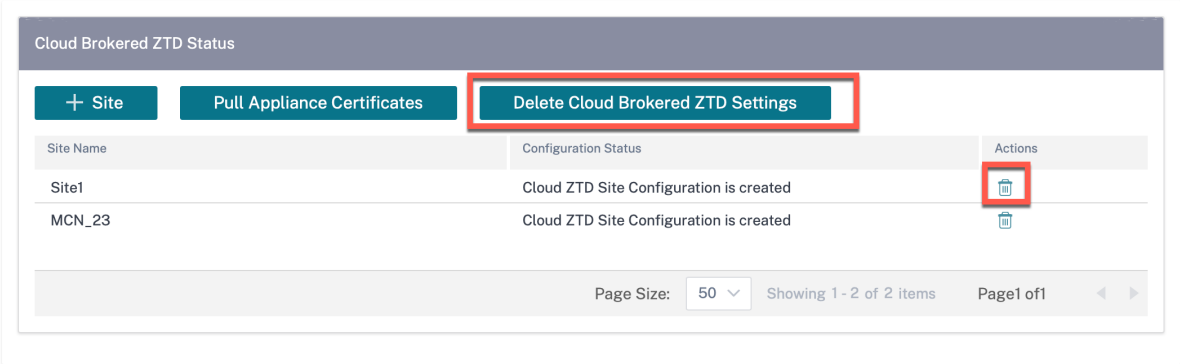

6. Conecte y encienda los dispositivos SD-WAN en el centro de datos y las sucursales.
7. Los dispositivos se ponen en contacto con el servicio Citrix SD-WAN Orchestrator con su número de serie.

8. El servicio Citrix SD-WAN Orchestrator actúa como intermediario entre Citrix SD-WAN Orchestrator for On-premises y los dispositivos. Permite el intercambio de certificados y el dispositivo Citrix SD-WAN establece una conexión segura con Citrix SD-WAN Orchestrator for On-premises. Una vez que la implementación sin interacción se haya realizado correctamente, el sitio configurado se conectará y se mostrará en la columna **Conectividad de Orchestrator**, en **Configuración > Inicio de configuración de red**.
9. **Active** y **organice** la configuración para enviar la configuración y el software a los dispositivos.
10. Una vez que se aplica la configuración o el software, se establecen las rutas virtuales y la columna **Disponibilidad**, en **Configuración > Inicio de configuración de red**, se actualiza con el estado de la ruta virtual correspondiente.

> **NOTA**
>
> Citrix SD-WAN Orchestrator for On-premises tarda unos 30 minutos en obtener el certificado del dispositivo e incorporarlos por completo. Para obtener los certificados del dispositivo inmediatamente (sin esperar 30 minutos), haga clic en **Extraer certificados del dispositivo**.

Si es necesario, puede elegir hacer clic en **Eliminar la configuración de ZTD de Cloud Brokered**. Elimina la información relacionada con todos los sitios. Si necesita eliminar la información de un sitio en particular, haga clic en el icono de eliminación correspondiente a ese sitio.




### Limitaciones

- Los dispositivos SD-WAN no pueden conectarse a varias instancias de Citrix SD-WAN Orchestrator for On-premises que compartan credenciales de inicio de sesión en la nube. Por ejemplo, un dispositivo SD-WAN permanece conectado a Citrix SD-WAN Orchestrator for On-premises configurado por primera vez. Los detalles de Citrix SD-WAN Orchestrator for On-premises que se configuran a continuación no se envían al dispositivo SD-WAN.
- Los dispositivos SD-WAN conectados a través de LTE no pueden establecer una conexión con Citrix SD-WAN Orchestrator para dispositivos locales alojados en una red privada.

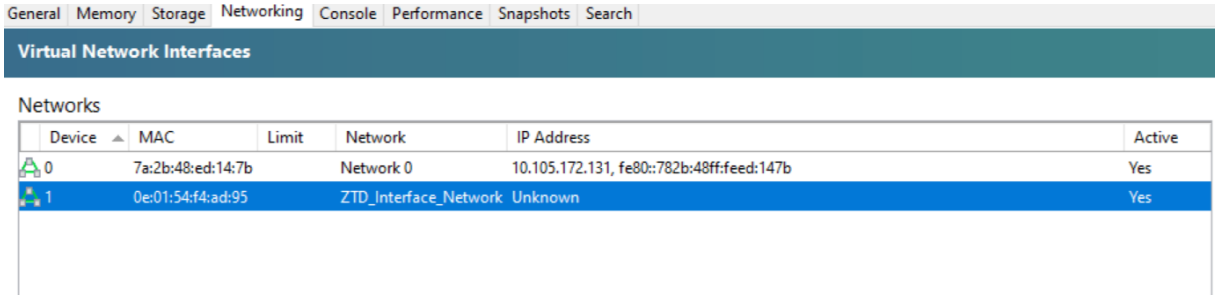
 

### Configuración de la interfaz ZTD

Puede habilitar una interfaz Zero Touch Deployment (ZTD) en SD-WAN Orchestrator for On-premises. La interfaz ZTD, que está protegida mediante la autenticación bidireccional, proporciona una interfaz de comunicación segura para los dispositivos SD-WAN y SD-WAN Orchestrator para entornos locales.

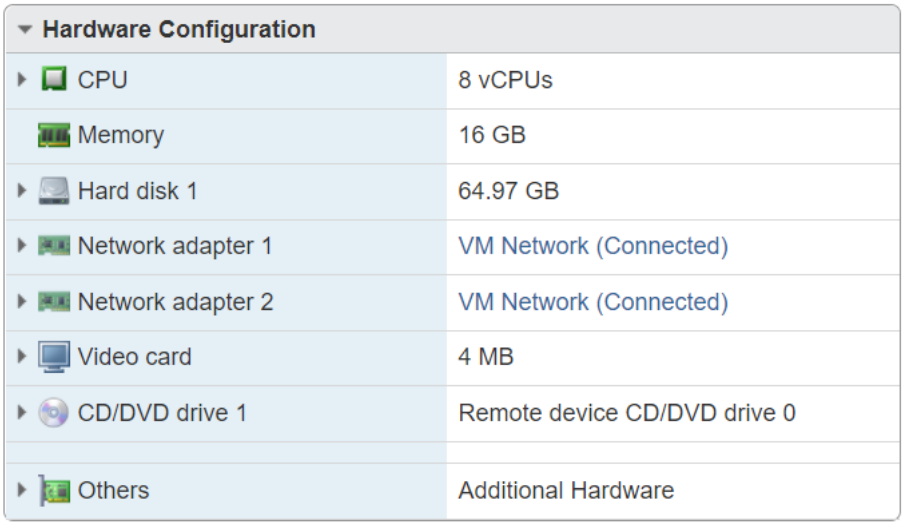
Tras habilitar la interfaz ZTD, los nuevos dispositivos D-WAN implementados a través de ZTD no en la nube y ZTD negociado en la nube utilizan la dirección IP de la interfaz ZTD para comunicarse con SD-WAN Orchestrator for On-premises.

Como requisito previo, asegúrese de que SD-WAN Orchestrator for On-premises Virtual Machine tenga una interfaz adicional, además de la interfaz de administración.




**Nota**

Para la máquina virtual VMware ESXi, asegúrese de que la máquina virtual se reinicie después de agregar una interfaz adicional para ZTD.



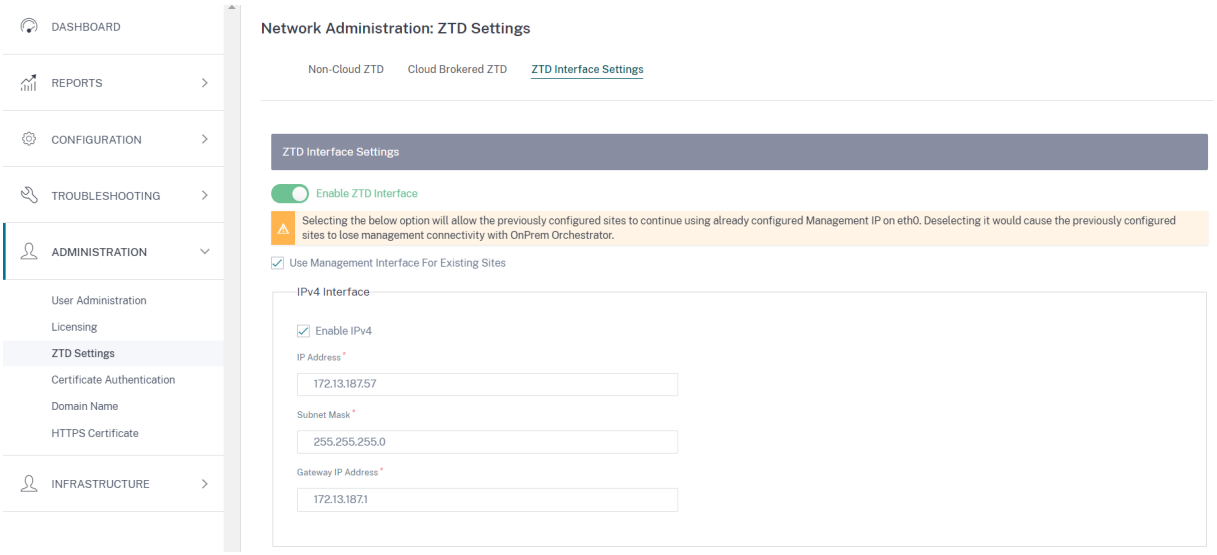

 

### Activación de la interfaz ZTD

En la GUI de SD-WAN Orchestrator for On-premises, vaya a **Administración** > **Configuración de ZTD** y seleccione **Habilitar la interfaz ZTD** para habilitar la interfaz ZTD. Proporcione la dirección IP de la interfaz ZTD, la máscara de subred y la dirección IP de la puerta de enlace.

Seleccione **Usar interfaz de administración para sitios existentes para** asegurarse de que los dispositivos SD-WAN ya implementados a través de la ZTD ajena a la nube o la ZTD de intermediación en la nube continúen conectándose con SD-WAN Orchestrator para entornos locales mediante la dirección IP de la interfaz de administración.

> **Advertencia**
>
> Si no se selecciona **Usar interfaz de administración para sitios existentes**, los dispositivos SD-WAN que ya estén implementados a través de la ZTD que no es de nube o la ZTD de Cloud Brokered-ZTD perderán la conexión con SD-WAN Orchestrator for On-premises.




**Configuración de ZTD ajeno a la nube mediante la interfaz ZTD** Si se selecciona la opción **Usar la interfaz de administración para sitios existentes**, los dispositivos que ya están implementados mediante ZTD que no es de nube seguirán utilizando la dirección IP de la interfaz de administración para conectarse con SD-WAN Orchestrator for On-premises. Inicie una ZTD que no sea de nube en los dispositivos para establecer una conexión con SD-WAN Orchestrator for On-premises mediante la dirección IP de la interfaz ZTD.

> **Nota**
>
> Puede inhabilitar la opción Usar la interfaz de administración para sitios existentes después de que todos los dispositivos SD-WAN hayan establecido una conexión con SD-WAN Orchestrator

> for On-premises a través de la dirección IP de la interfaz ZTD.

Si no se selecciona la opción **Usar la interfaz de administración para sitios existentes**, los dispositivos SD-WAN que ya se hayan desplegado mediante ZTD que no sea de nube pierden la conexión con SD-WAN Orchestrator for On-premises. Inicie ZTD fuera de la nube en dispositivos SD-WAN para restablecer la conexión con SD-WAN Orchestrator for Onpremises mediante la dirección IP de la interfaz ZTD.

**Configuración de Cloud Brokers ZTD mediante la interfaz ZTD** Si se selecciona la opción **Usar la interfaz de administración para sitios existentes**, los dispositivos que ya están implementados mediante Cloud Brokered ZTD seguirán usando la dirección IP de la interfaz de administración para conectarse con SD-WAN Orchestrator for On-premises. Para establecer una conexión con SD-WAN Orchestrator for On-premises mediante la dirección IP de la interfaz ZTD, realice una de las siguientes acciones:

- En los dispositivos SD-WAN, actualice la dirección IP y el certificado de SD-WAN Orchestrator for On-premises.

  > **Nota**
  >
  > Actualice el certificado solo si los certificados se regeneran manualmente; no es necesario que actualice el certificado si los dispositivos ya los tienen.

- Realice un restablecimiento de fábrica e inicie Cloud Brokered-ZTD en los dispositivos para establecer una conexión con SD-WAN Orchestrator for On-premises mediante la dirección IP de la interfaz ZTD.

> **Nota**
>
> Puede inhabilitar la opción **Usar la interfaz de administración para sitios existentes** después de que todos los dispositivos SD-WAN hayan establecido una conexión con SD-WAN Orchestrator for On-premises a través de la dirección IP de la interfaz ZTD.

Si no se selecciona la opción **Usar la interfaz de administración para sitios existentes**, los dispositivos SD-WAN que ya están implementados mediante ZTD negociado en la nube pierden la conexión con SD-WAN Orchestrator for On-premises. Para restablecer la conexión con SD-WAN Orchestrator for On-premises mediante la dirección IP de la interfaz ZTD, realice una de las siguientes acciones:

- En los dispositivos SD-WAN, actualice la dirección IP y el certificado de SD-WAN Orchestrator for On-premises.
- Realice un restablecimiento de fábrica e inicie Cloud Brokered-ZTD en los dispositivos para establecer una conexión con SD-WAN Orchestrator for On-premises mediante la dirección IP de la interfaz ZTD.

### Configuración de conectividad manual

Al configurar la conectividad manualmente, debe descargar el certificado Citrix SD-WAN Orchestrator for On-premises y cargarlo en cada dispositivo de la red. Implica iniciar sesión en cada dispositivo de forma manual para cargar los certificados.

Para configurar la conectividad manualmente:

1. Vaya a **Administración > Autenticación de certificados** y active el **tipo de autenticación**

   Cuando el tipo de autenticación está habilitado, el dispositivo SD-WAN puede conectarse a Citrix SD-WAN Orchestrator for On-premises solo mediante la autenticación bidireccional. Cuando el tipo de autenticación está inhabilitado, el dispositivo SD-WAN puede conectarse a Citrix SD-WAN Orchestrator for On-premise mediante la autenticación sin autenticación, la autenticación unidireccional o la autenticación bidireccional.

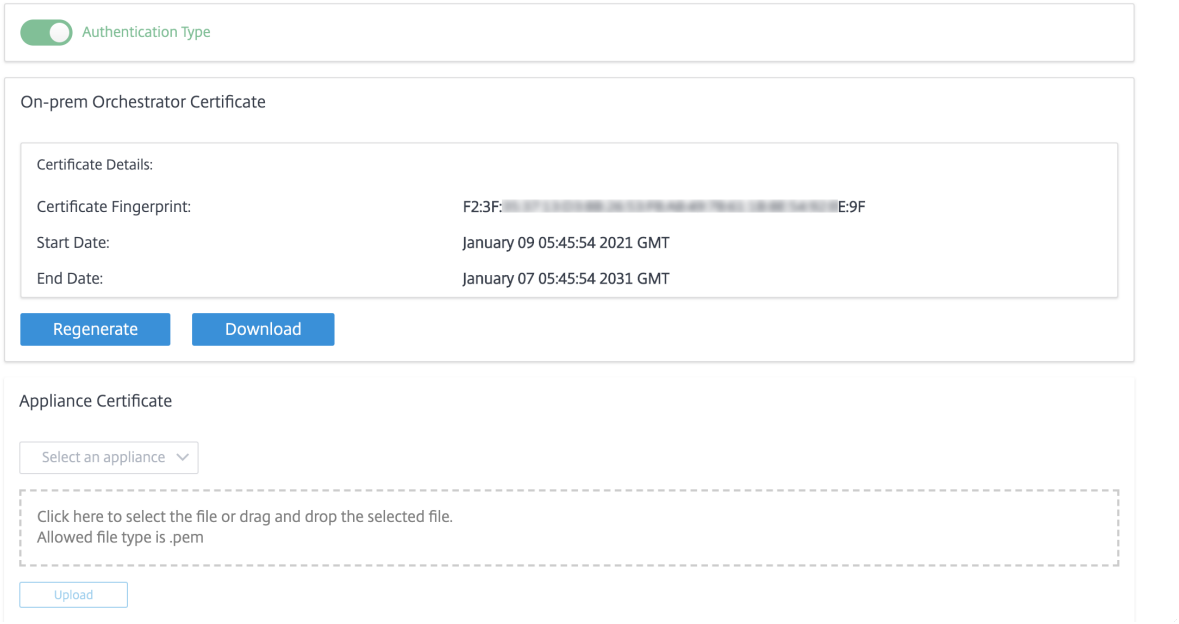
   > **Nota**
   >
   > En una configuración administrada por un proveedor, solo los proveedores pueden habilitar el tipo de autenticación y regenerar el certificado Citrix SD-WAN Orchestrator for On-premises.

2. Haga clic en **Regenerar** y **descargue** el certificado Citrix SD-WAN Orchestrator for On-premises.
3. Elija un dispositivo de la sección **Certificado de dispositivo** y cargue el certificado correspondiente descargado del dispositivo SD-WAN. Para obtener información detallada sobre la descarga del certificado del dispositivo, consulte Configuración local de Citrix SD-WAN Orchestrator en el dispositivo SD-WAN.

   > **NOTA**
   >
   > - Solo se admite el tipo de archivo .pem.
   > - Solo los administradores del cliente pueden cargar el certificado del dispositivo.

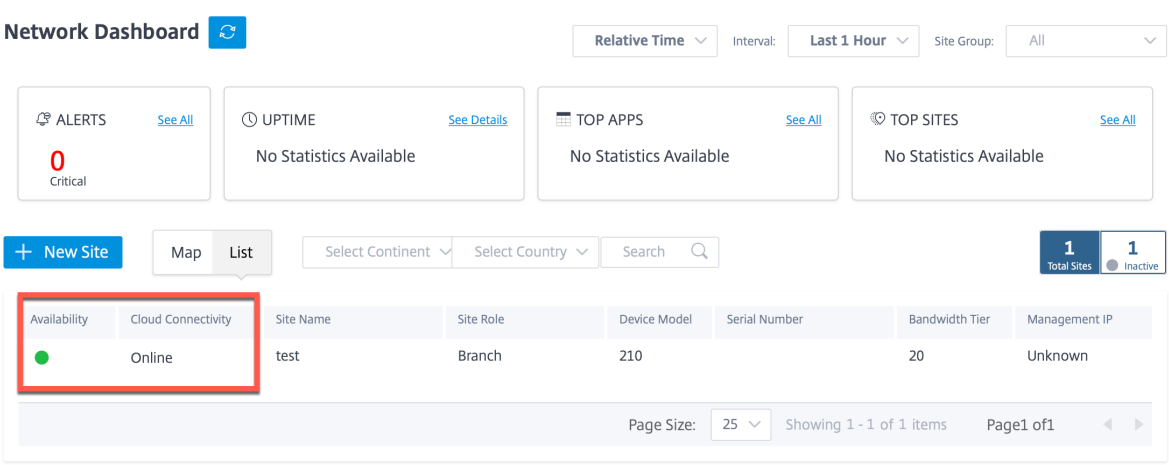
4. Inicie sesión en la interfaz de usuario del dispositivo SD-WAN y vaya a **Configuración > WAN virtual > SD-WAN Orchestrator local**. Cargue el certificado descargado de Citrix SD-WAN Orchestrator for On-premises. Para obtener información detallada, consulte Citrix SD-WAN Orchestrator para la configuración local en un dispositivo SD-WAN.




## Verificar la conectividad

Para comprobar el estado de conectividad del dispositivo, vaya a **Configuración > Configuración de red Inicio**y compruebe la columna **Conectividad a la nube** correspondiente a su sitio.



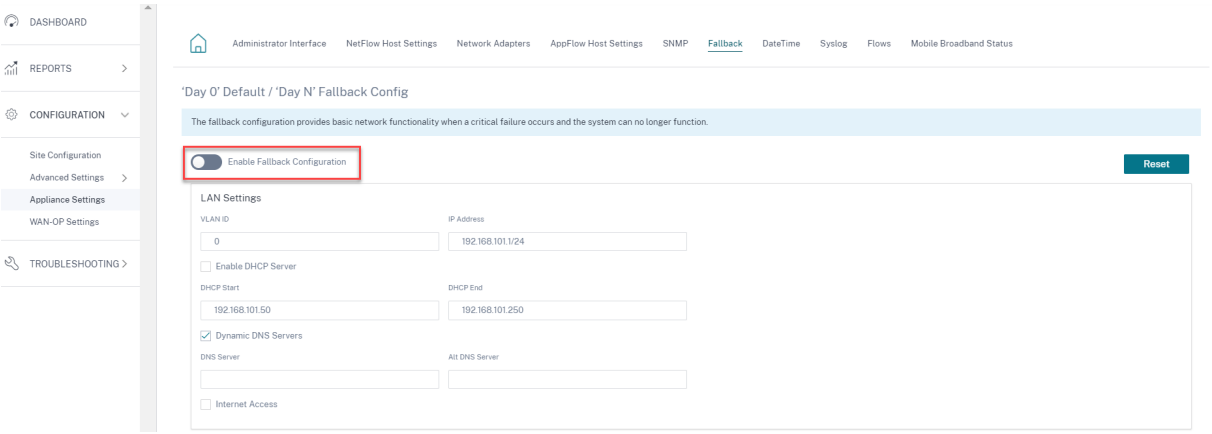

> **Nota:**
>
> Puede publicar el software deseado para actualizar los dispositivos en **Infraestructura > Administración de Orchestrator > Imágenes de software > Dispositivo**. Para obtener más información, consulte Publicar software.

## Configuración de reserva

La configuración alternativa garantiza que el Citrix SD-WAN Orchestrator para la conectividad local que ha establecido con el dispositivo Citrix SD-WAN se conserve a través de la IP de administración en banda del dispositivo.

Puede habilitar la configuración alternativa en Citrix SD-WAN Orchestrator for On-premises al nivel de sitio. Para ello, vaya a **Configuración** > **Configuración del dispositivo** > **Fallback** y haga clic en **Habilitar configuración alternativa**.



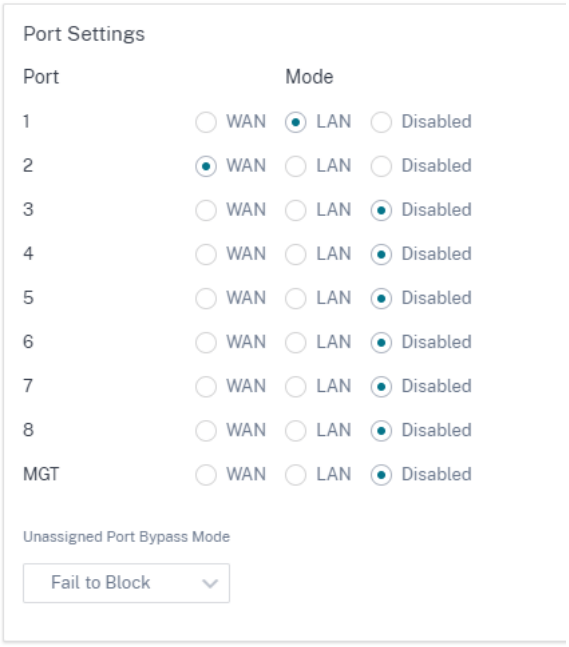

Para obtener información detallada sobre la configuración alternativa, consulte Administración dentro de banda.

> **Nota:**
>
> Si utiliza un dispositivo que no sea Citrix SD-WAN 110 SE, asegúrese de ejecutar SD-WAN 11.2 o una versión posterior para habilitar la configuración alternativa predeterminada.

La siguiente tabla proporciona los detalles de los puertos WAN y LAN designados previamente para la configuración de reserva en diferentes plataformas:

| Plataforma | Puertos WAN | Puertos LAN |
|---|---|---|
| 110 | 1/2 | 1/1 |
| 110-LTE | 1/2, LTE-1 | 1/1 |
| 210 | 1/4, 1/5 | 1/3 |
| 210-LTE | 1/4, 1/5, LTE-1 | 1/3 |
| VPX | 2 | 1 |
| 410 | 1/4, 1/5, 1/6 | 1/3 (FTB) |
| 1100 | 1/4, 1/5, 1/6 | 1/3 (FTB) |




## Configuración al nivel de proveedor

November 16, 2020

### Perfiles

Un perfil es una plantilla de configuración **activa**. Una plantilla regular está destinada a ayudar a la creación de una nueva entidad. Pero una vez creada la plantilla, los cambios posteriores en la plantilla no se aplican a las nuevas entidades creadas con la plantilla base. Un perfil sirve como entidad maestra central activa, de la que heredan todas las entidades secundarias, no solo durante la creación sino también durante toda la vida de un perfil. Todas las entidades secundarias asociadas al perfil heredan automáticamente los cambios realizados en un perfil.

Por ejemplo, un administrador crea un perfil de configuración de sitio denominado **tienda minorista pequeña** y lo aplica a todas las pequeñas tiendas minoristas propiedad de una empresa. Ahora, cualquier cambio realizado en el perfil de la tienda minorista pequeña en un momento dado se aplicaría automáticamente a todas las tiendas heredadas de este perfil. En función de lo que es común en todas las entidades, y lo que no lo es, ciertos parámetros en la configuración del perfil pueden dejarse sin definir. Estos parámetros serían personalizables y pueden variar entre las entidades que heredan el mismo perfil.

## Plantillas de perfil para proveedores de servicios

Los socios pueden crear plantillas de perfil, que sus clientes pueden utilizar al crear perfiles.

Por ejemplo, un proveedor puede crear cuatro plantillas de perfil de sitio: Sucursal pequeña, sucursal media, sucursal grande y centro de datos. Estas plantillas se ponen automáticamente a disposición de las cuentas de cliente asociadas con el socio. Los clientes pueden utilizar estas plantillas mientras crean perfiles.

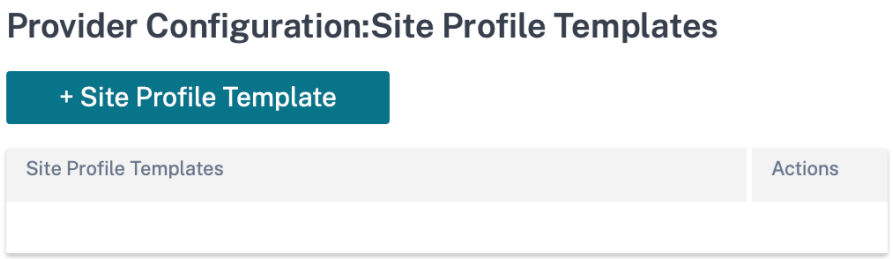
Por ejemplo, supongamos que un cliente decide crear un perfil para la configuración de sucursales pequeñas. El cliente puede seleccionar una de las plantillas compartidas por el partner, disponible a través de una lista desplegable como parte de la configuración del perfil. El cliente puede personalizarlo según sus necesidades de red antes de guardar el perfil. La plantilla de perfil no es una entidad activa. Solo ayuda a la creación de perfiles a nivel de cliente. Los perfiles solo se pueden crear a nivel de cliente y están destinados a ser entidades activas que actúan como registros de configuración maestra.

El proveedor puede crear perfiles de configuración, que se pueden compartir con algunos o todos los clientes, según sea necesario. Actualmente se admiten perfiles de sitio y WAN.

### Plantillas de perfil de

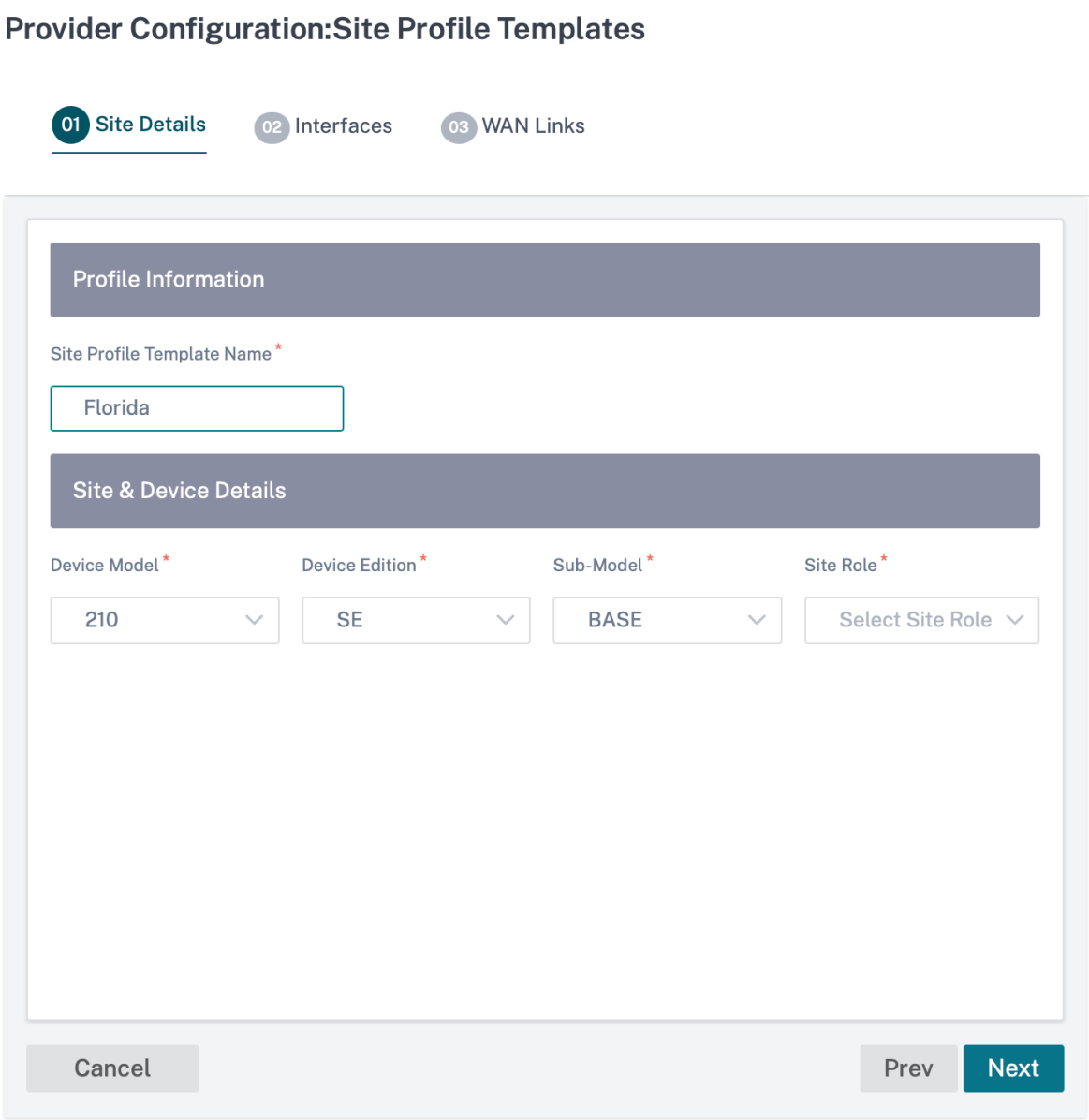
Las plantillas de perfil de sitio son plantillas de configuración de sitio creadas por proveedores de servicios para permitir la creación de perfiles de sitio a nivel de cliente.

Para crear plantillas de perfil, vaya a **Configuración** > Plantillas de perfil de **sitio** y haga clic en **+ Plantilla de perfil de sitio**.



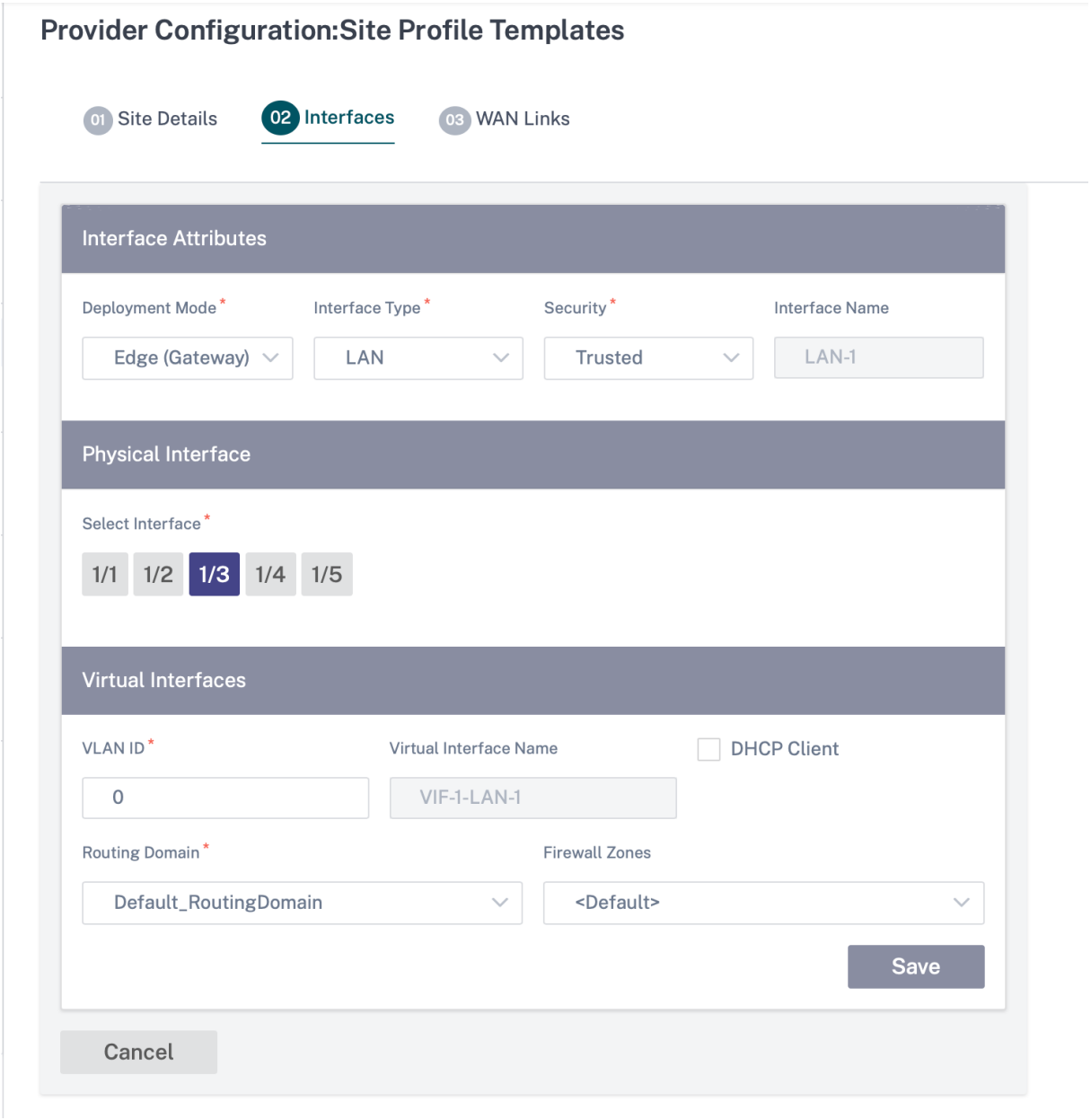

Para crear una plantilla de perfil de sitio, debe configurar los **detalles del sitio**, las **interfaces** y los **enlaces WAN**. Para obtener una descripción detallada de la configuración de sitios, consulte Detalles del sitio.



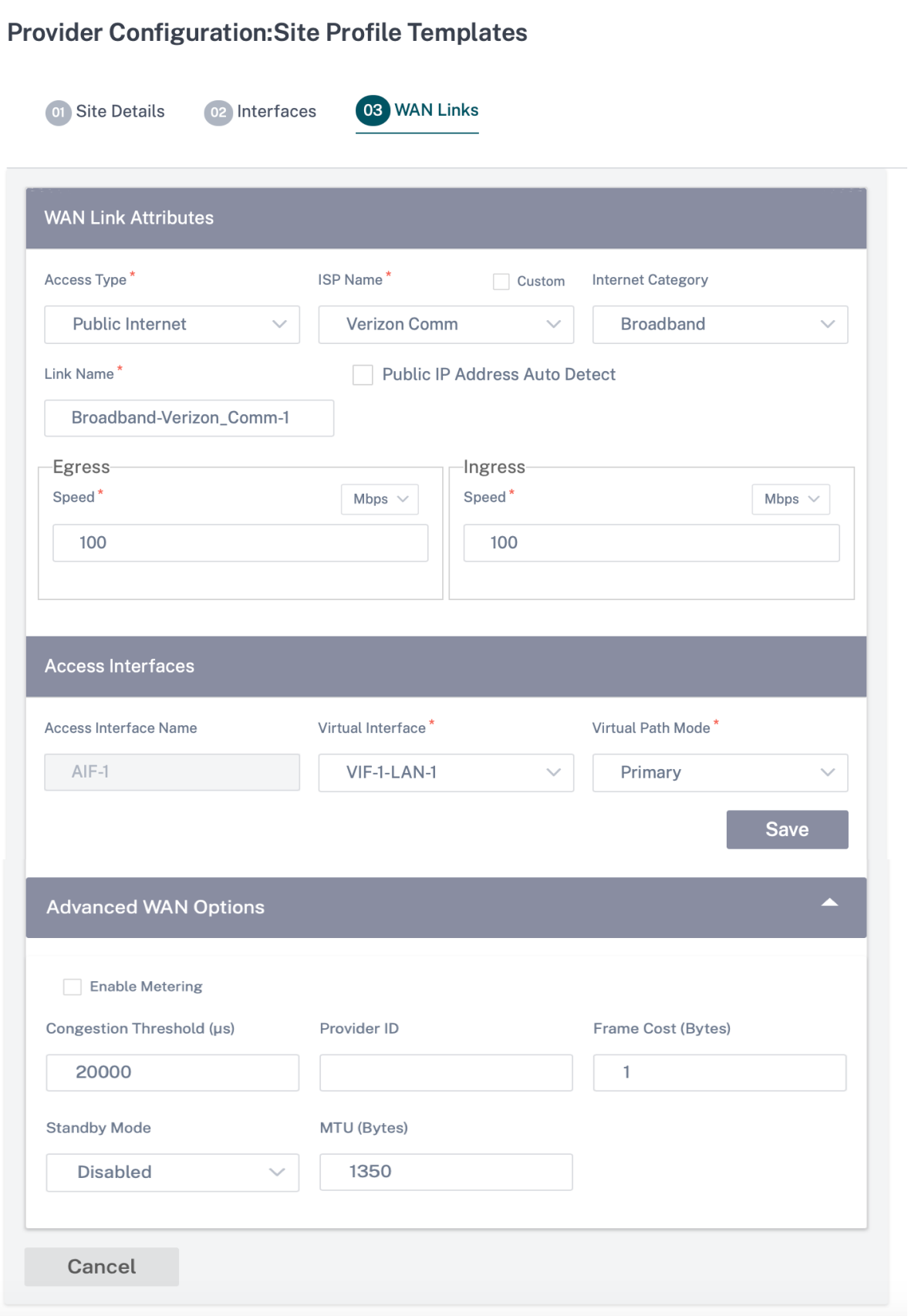

Asigne una interfaz para el sitio haciendo clic en la**opción**+ Interfaz. Para agregar una interfaz, debe rellenar los campos **Atributos de interfaz**, **Interfaz física** e **Interfaces virtuales**. Para obtener una descripción detallada de la configuración de interfaces, consulte Interfaces.




Proporcione **atributos de enlace WAN**, **interfaces de acceso** y **servicios** con **opciones avanzadas**. Para obtener una descripción detallada de la configuración de enlaces WAN, consulte Vínculos WAN.

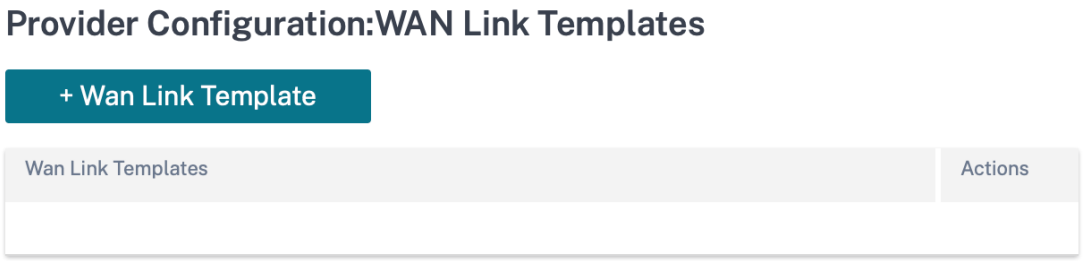
 



**Plantillas de vínculos de**

Las plantillas de perfil WAN son plantillas de configuración de enlaces WAN creadas por proveedores de servicios, para permitir la creación de perfiles de enlace WAN a nivel de cliente.




Para crear una plantilla de enlace WAN, haga clic en **+ Plantilla de enlace WAN**. Debe rellenar la información del enlace WAN, como Nombre **de perfil**, Tipo de **acceso**, Categoría de **Internet**, Velocidad**de**LAN a WAN, etc. Para obtener una descripción detallada de la configuración de enlaces WAN, consulte Vínculos WAN.

## Inicio de red

October 31, 2022

La página **principal de la red** actúa como ancla para la configuración de la red, ofrece capacidades de configuración al nivel de red empresarial y sirve como punto de partida para configurar la red SD-WAN de una empresa.

La página **principal de la red** muestra el total de sitios dentro de la red y también segrega los sitios según su estado de conectividad. Seleccione los enlaces numerados para ver los sitios según las siguientes categorías de estado:

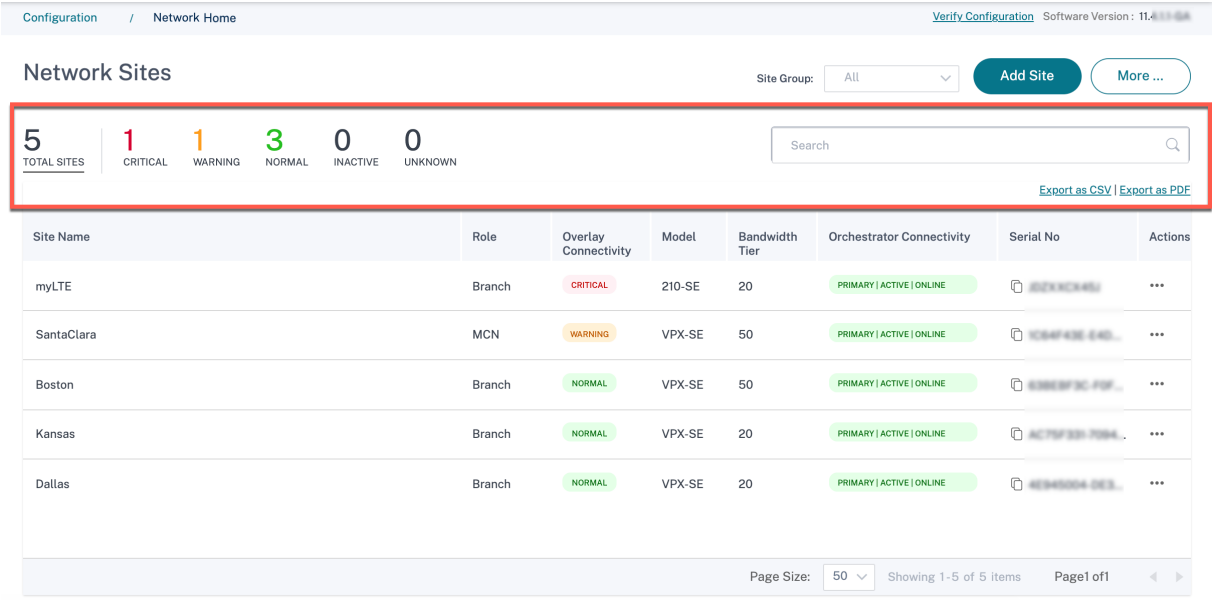
- **Crítico**: Sitios que tienen todas las rutas virtuales asociadas inactivas.
- **Advertencia**: Sitios que tienen al menos una ruta virtual de acceso.
- **Normal**: Todas las rutas virtuales y las rutas de miembros asociadas del sitio están activas.
- **Inactivo**: Los sitios se encuentran en estado no desplegado e inactivo.
- **Desconocido**: Se desconoce el estado del sitio.

Al hacer clic en el estado, se filtran los sitios según su estado y se muestran los detalles. También puede utilizar la barra de **búsqueda** para ver los detalles de un sitio en función del nombre del sitio,

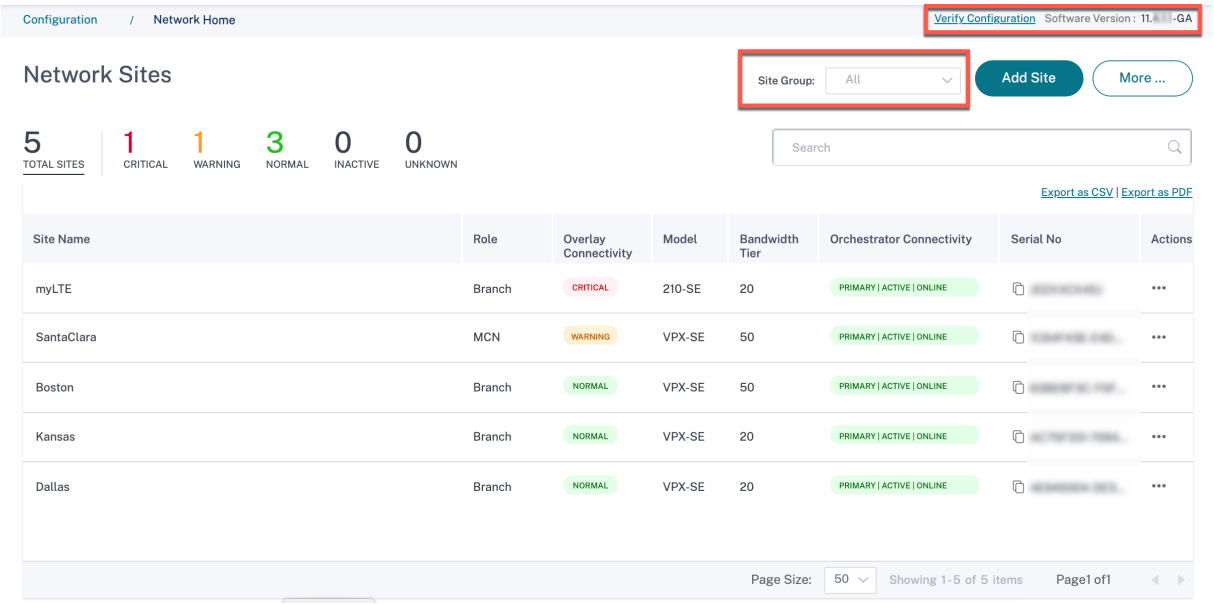
el rol, la conectividad superpuesta, el modelo, el nivel de ancho de banda y los parámetros del número de serie.

Puede exportar los resultados filtrados a un archivo CSV o PDF mediante las opciones **Exportar como CSV** y **Exportar como PDF**. El nombre del archivo CSV y PDF lleva el prefijo **SiteList** seguido de la fecha y la hora en que se exportó el archivo.




En la esquina superior derecha de la pantalla, puede ver la versión actual del software. Haga clic en **Verificar configuración** para validar cualquier error de auditoría. Para obtener más información, consulte Verificar la configuración.

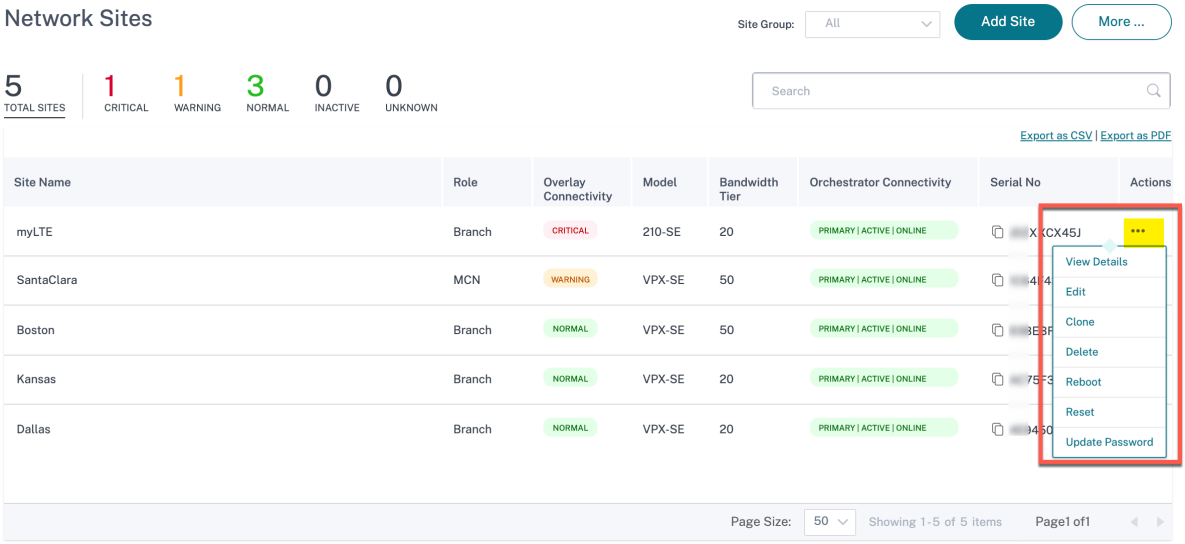
Puede filtrar los sitios según el grupo o la región a la que pertenecen mediante la lista desplegable de **grupos de sitios**.



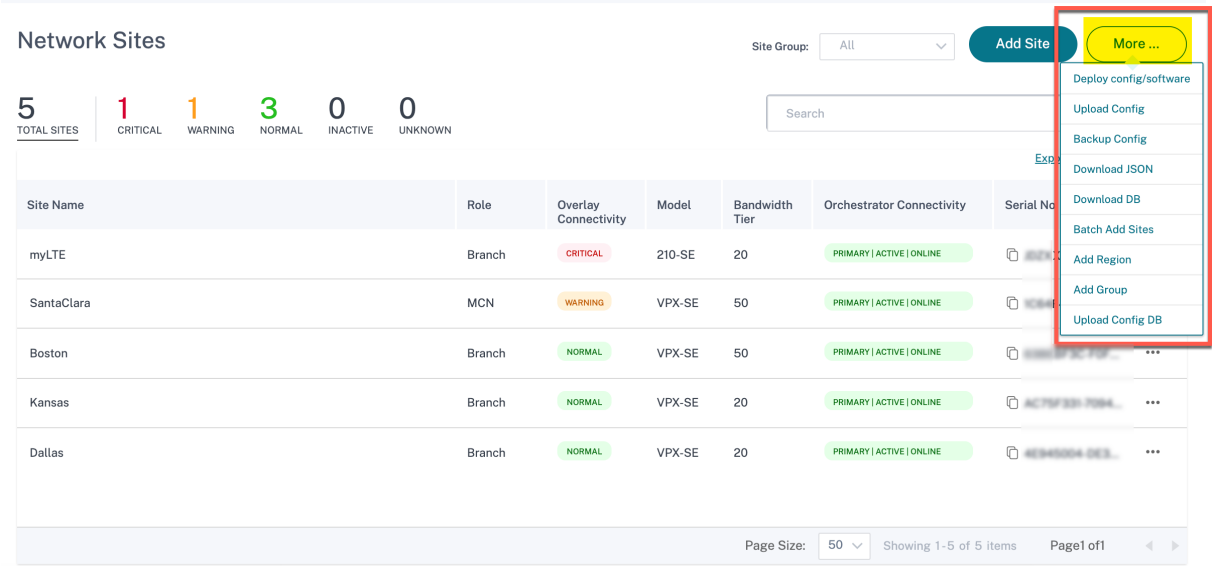

 

Al hacer clic en el nombre del sitio en el resultado filtrado, accederá a la pantalla de **configuración del sitio**. Si el sitio tiene una configuración de alta disponibilidad, la columna **Conectividad de Orchestrator** muestra el estado de los dispositivos principales y secundarios. La columna **Número de serie** muestra el número de serie del dispositivo. En una configuración de alta disponibilidad, se muestran los números de serie del dispositivo principal y secundario. Puede copiar el número de serie del dispositivo mediante el icono de copia.

Mediante la columna **Acciones**, puede ver los detalles, modificar, clonar, eliminar, restablecer y actualizar la contraseña del sitio. También puede reiniciar los dispositivos asociados a un sitio.




Puede realizar otras acciones, como cargar la configuración, agregar sitios en un lote, descargar JSON, etc., mediante la opción **Más...**



### Agregar sitio

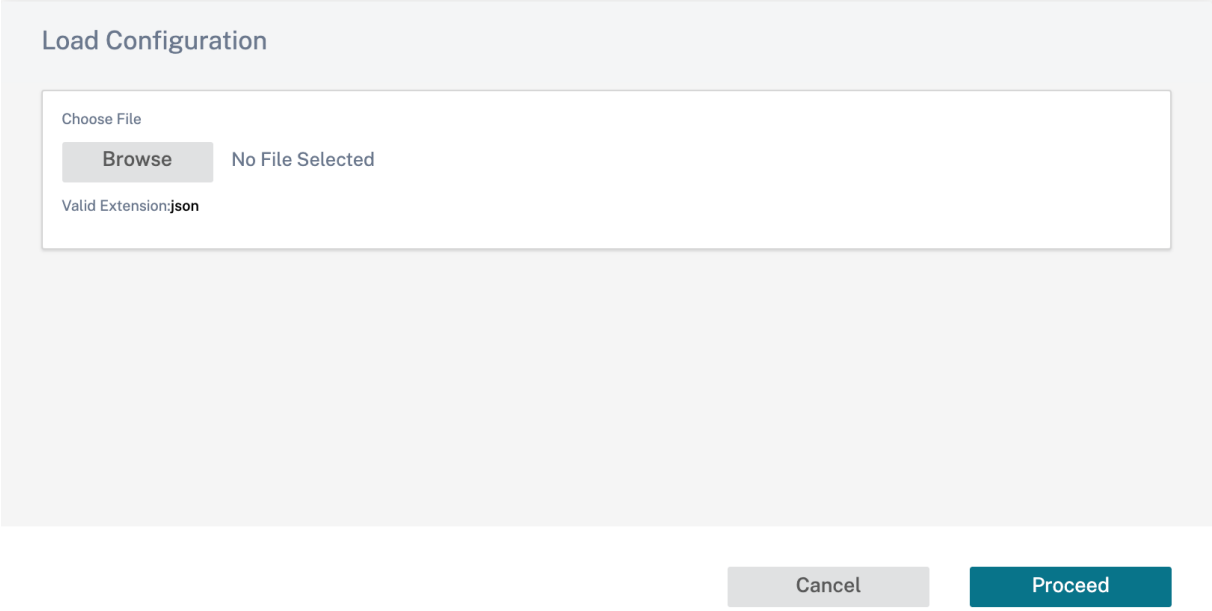
Use la opción **+ Agregar sitio** para agregar un sitio nuevo. Para obtener más información sobre el flujo de trabajo de configuración del sitio, consulte Configuración del sitio

### Implementar la configuración y el software

La opción **Más > Implementar configuración/software** lo lleva a la sección **Implementación**, que ayuda a verificar, organizar y activar la configuración en toda la red. Para obtener más información sobre la implementación de la configuración y el software, consulte Implementación.

### Configuración de carga

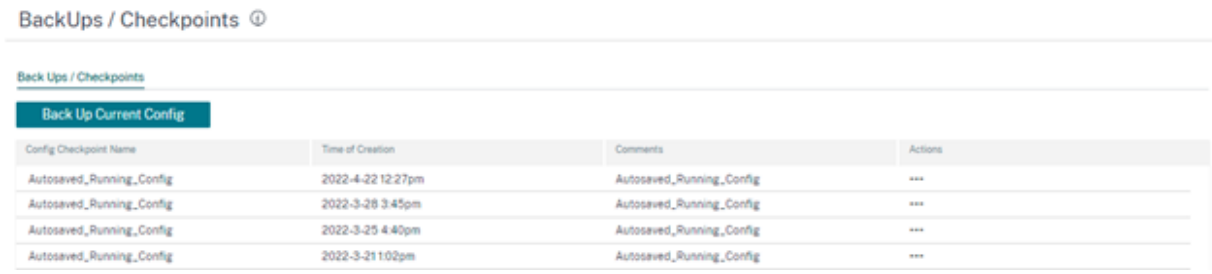
La opción **Más > Cargar configuración** le permite buscar y cargar una de las configuraciones guardadas anteriormente. La configuración recién cargada sirve como configuración activa para la red.




### Respaldos y puntos de control

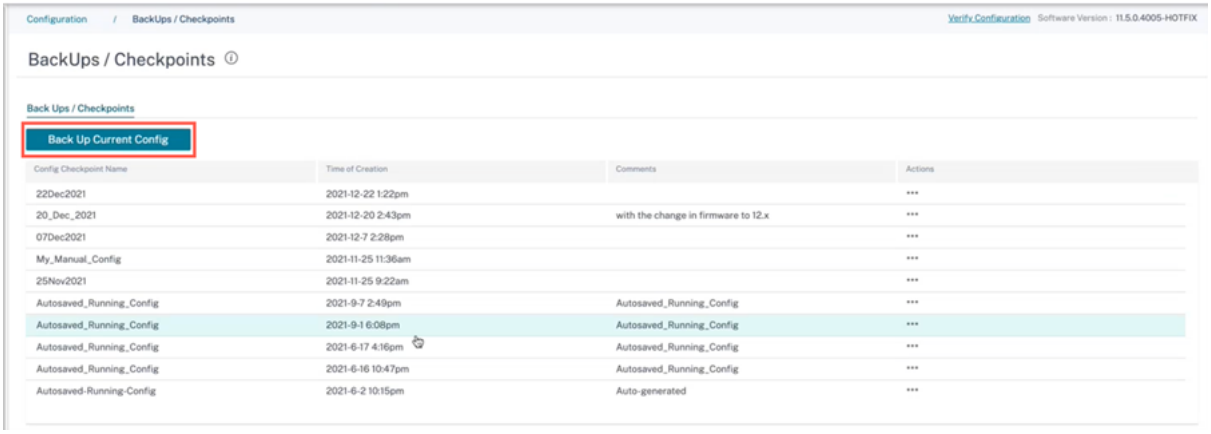
La opción **Más > Configuración de respaldo** lo lleva a la página **Copias de seguridad/Puntos de control** y permite realizar copias de seguridad y restaurar la configuración, o revisar los puntos de control guardados.

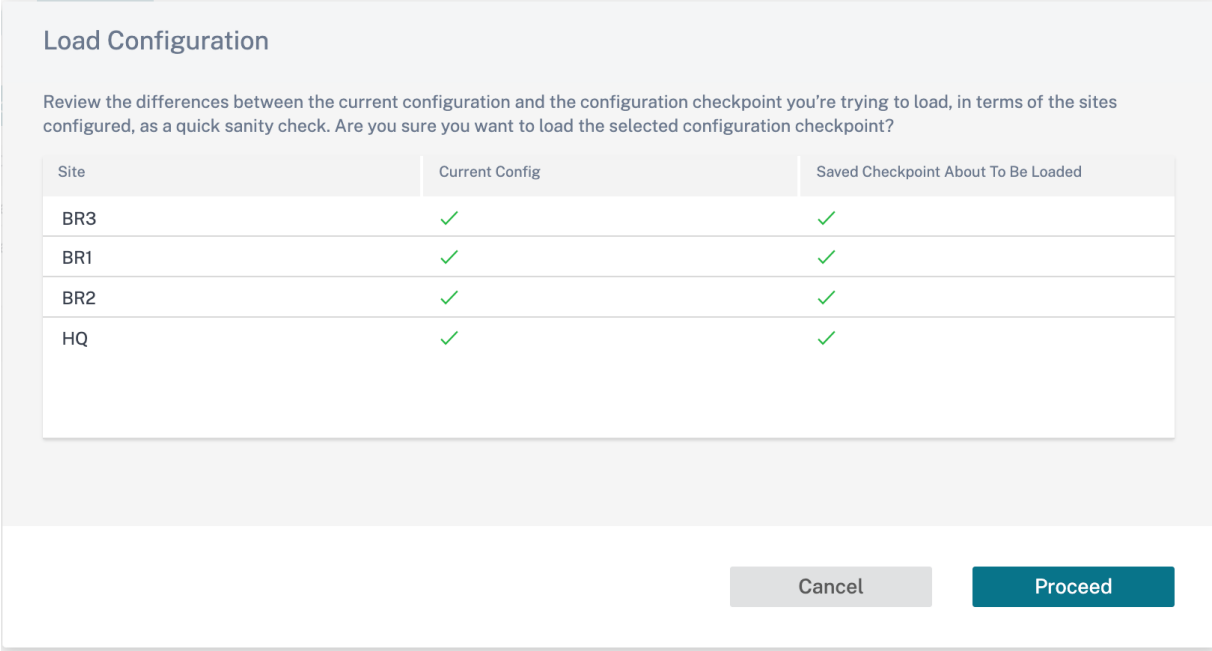



Haga clic en **Verificar configuración** para validar cualquier error de auditoría.

Haga clic en **Respaldar la configuración actual** para hacer una copia de seguridad de la configuración actual como punto de control para su uso futuro.




Haga clic en **Cargar configuración** (en **Acciones**) para cargar una configuración guardada. Haga clic en **Continuar**.




Haga clic en **Copiar** (en **Acciones**) para crear una copia similar de una configuración existente. Tam-

bién puede descargar, modificar y eliminar los puntos de control de configuración guardados. Estas operaciones están disponibles en **Acciones**.

### Descargar JSON

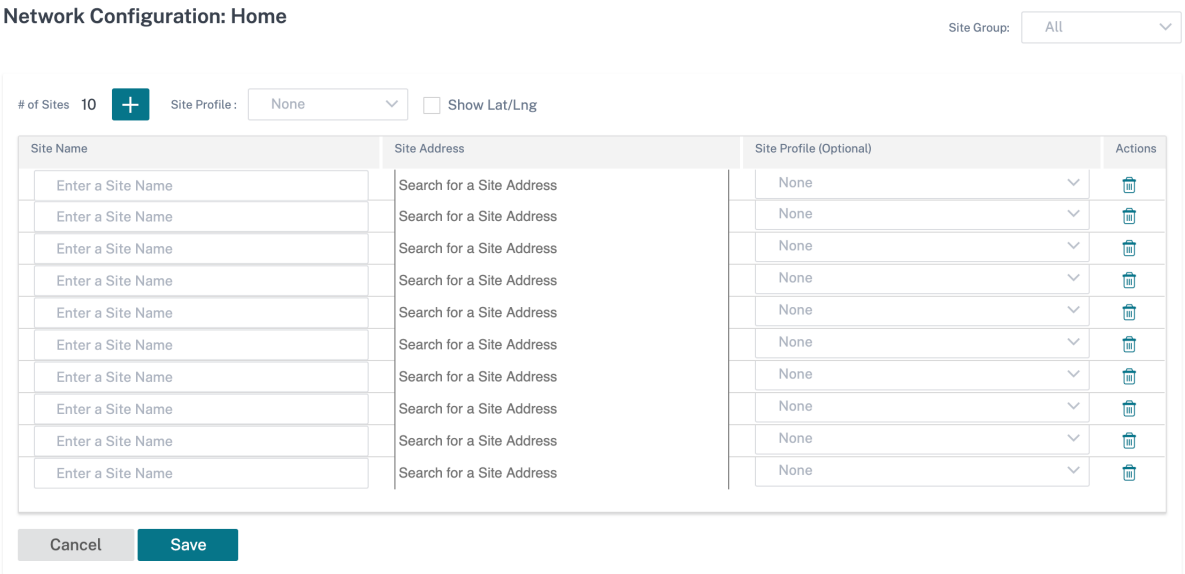
La opción **Más > Descargar JSON** le permite descargar y exportar la configuración actual en formato JSON para revisarla sin conexión.

### Descarga DB

La opción **Más > Descargar base** de datos permite descargar y exportar la configuración actual en formato de base de datos.

### Agregar sitios en un lote

La opción **Más > Agregar sitios por lotes** le permite agregar rápidamente varios sitios en un lote. También puede seleccionar un perfil de sitio que se utilizará para cada sitio, lo que le dejará solo con parámetros únicos, como direcciones IP que quedan por configurar para cada sitio.




### Agregar región

La opción **Más > Agregar región** le permite crear una región y lo lleva a la **página Sitios y grupos de IP > Regiones**. Para obtener más información, consulte Regiones.

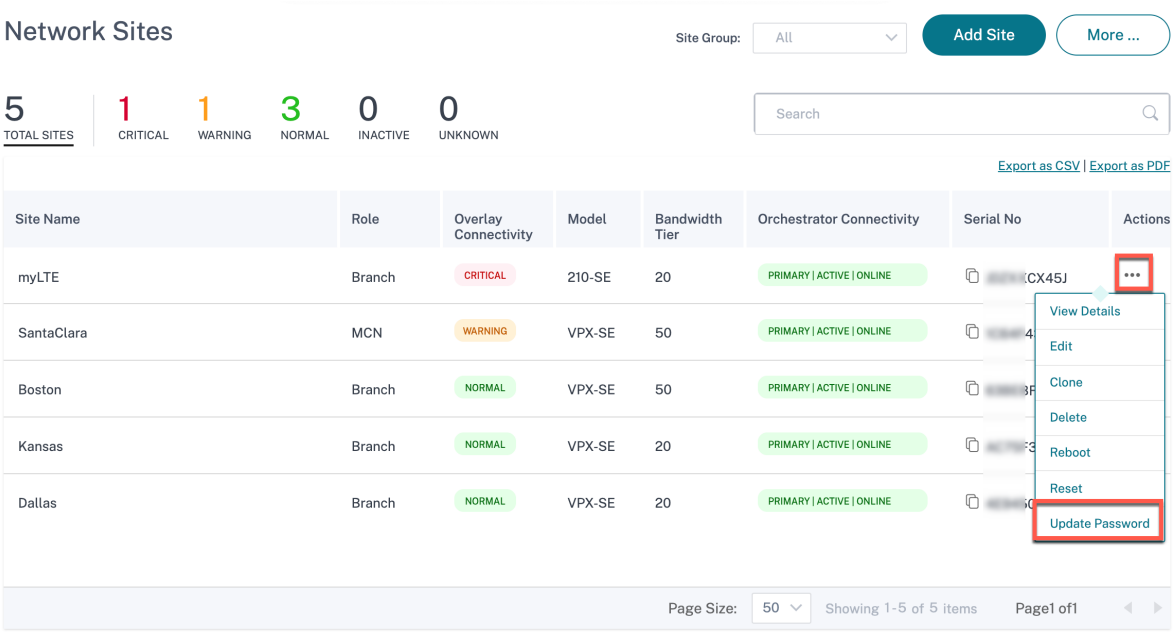
### Agregar grupo

La opción **Más > Agregar grupo** lo lleva a la **página Grupos de sitios e IP > Grupos personalizados**, donde puede crear una región. Para obtener más información, consulte Grupos personalizados.

### Actualizar contraseña

Puede cambiar la contraseña de los dispositivos SD-WAN en diferentes sitios de la red, a través del Citrix SD-WAN Orchestrator for On-premises.

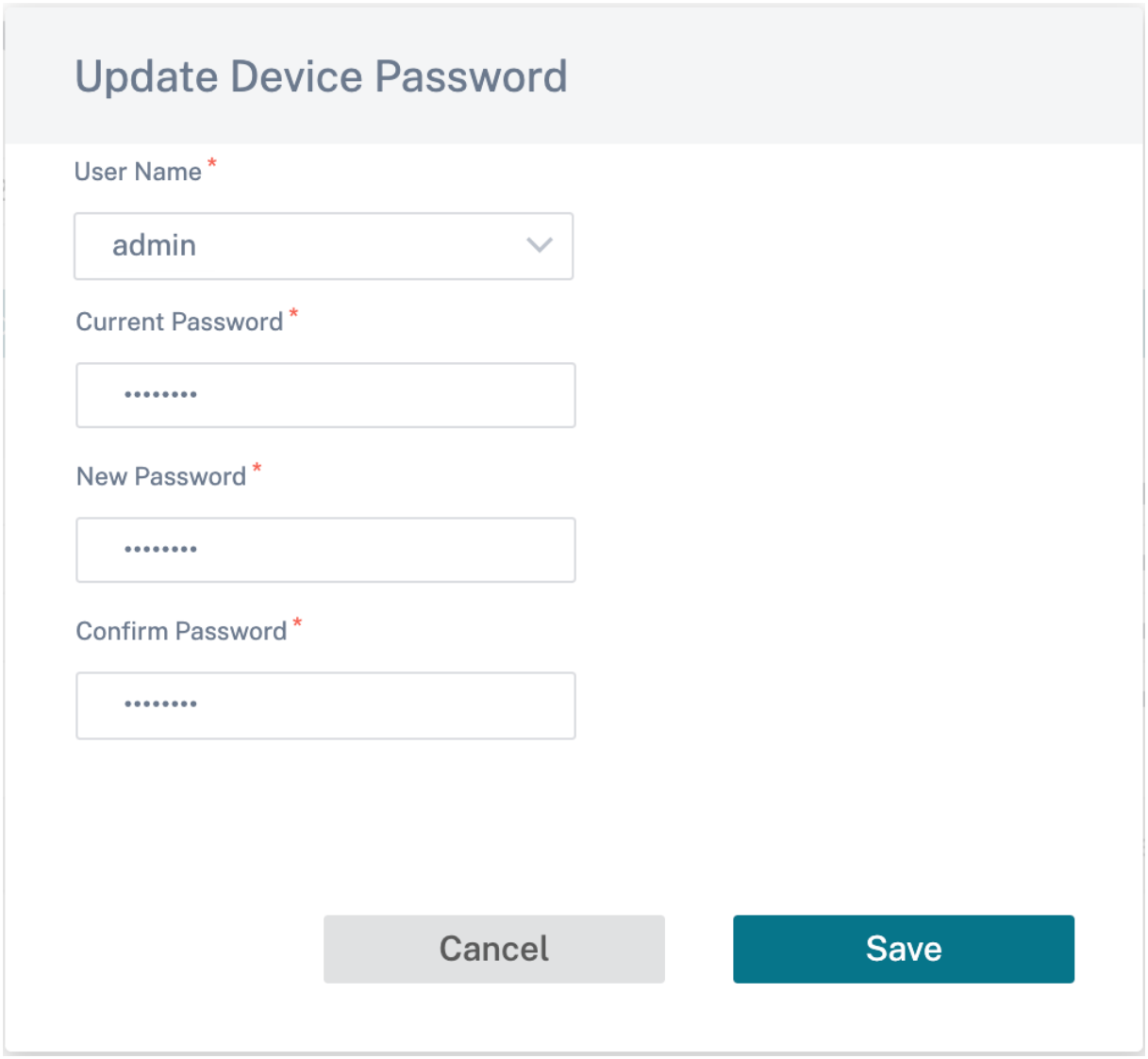
Para cambiar la contraseña, para un dispositivo que esté en línea, haga clic en el icono Más y seleccione **Actualizar contraseña**.




Proporcione los valores de los siguientes campos:

- **Nombre de usuario**: S eleccione un nombre de usuario para el que quiera cambiar la contraseña de la lista de usuarios configurada en el sitio.
- **Contraseña actual**: Introduzca la contraseña actual. Este campo es opcional para usuarios administradores.
- **Contraseña nueva**: introduzca una contraseña nueva de su elección.
- **Confirme la contraseña**: vuelva a introducir la contraseña para confirmarla.

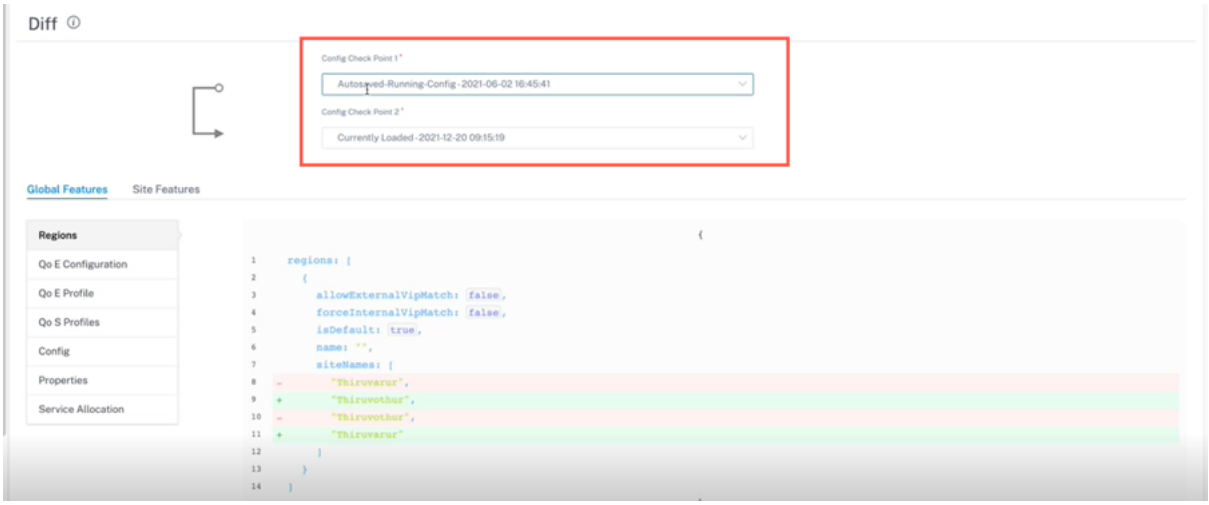



## Diferencia de configuración

October 31, 2022

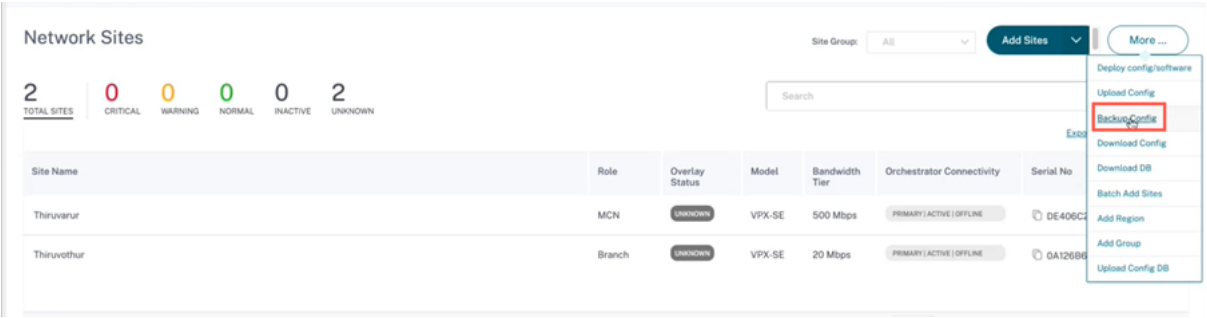
La función **Config Diff** le ayuda a revisar la diferencia entre dos versiones de los puntos de control de configuración. La opción **Config Diff** está disponible al nivel de red, en **Configuración** > **Config Diff**.

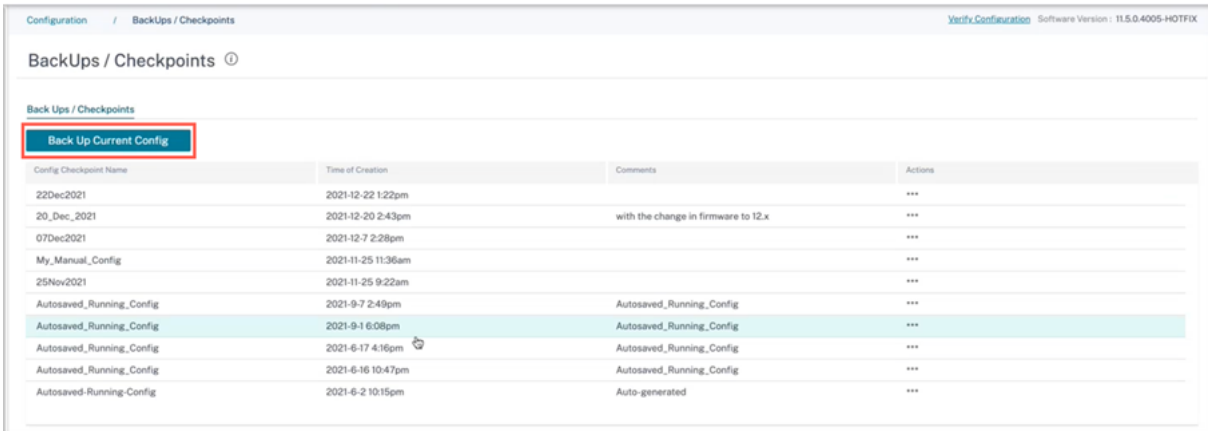



Durante la implementación, puede guardar una configuración con un nombre adecuado. Las configuraciones guardadas se conocen como puntos de control. Al comparar la diferencia entre las dos configuraciones, debe seleccionar las configuraciones necesarias en las listas desplegables de **Config Check Point 1/2**.

Puede ver la lista de copias de seguridad y puntos de control de configuraciones guardadas en **Configuración** > **Red principal** > seleccionar **Configuración de respaldo** en la lista desplegable **Más**.

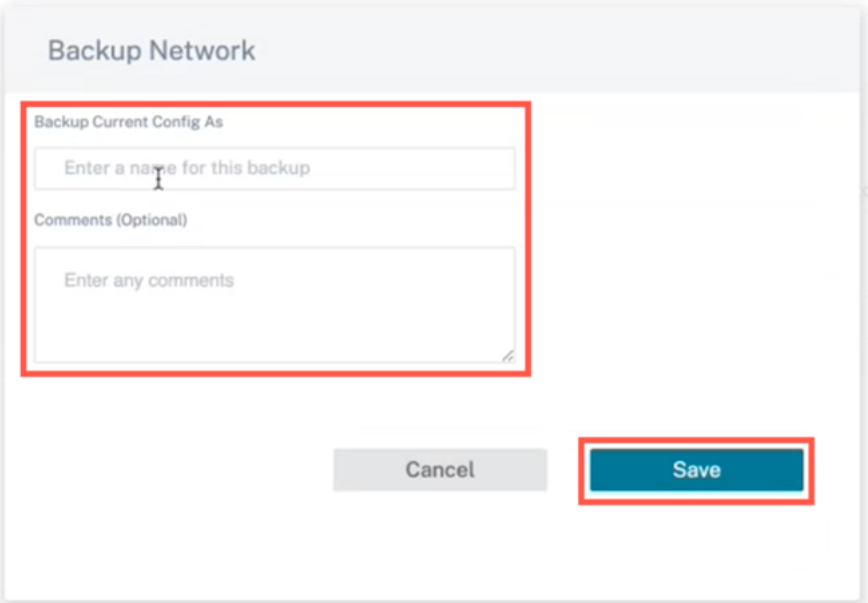



Cuando se realiza una implementación, siempre se realiza una copia de seguridad automática de la configuración. También puede hacer una copia de seguridad de la configuración actual manualmente. Para ello, haga clic en la opción Realizar **copia de seguridad de la configuración actual**.



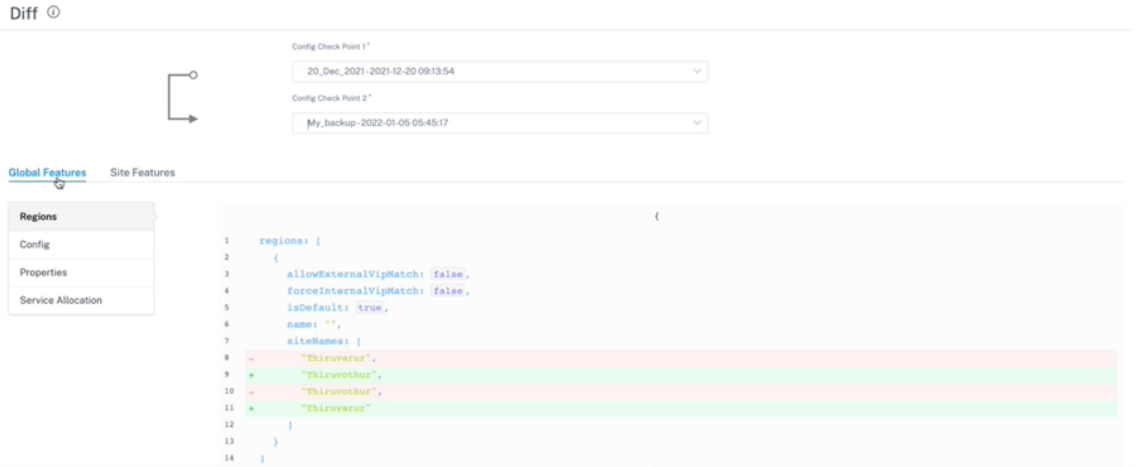
Introduzca un nombre para guardar la configuración junto con los comentarios (opcional). Haga clic en **Guardar**.




> **Nota:**
>
> Puede guardar o crear un máximo de cinco copias de seguridad de la configuración. Al crear una nueva copia de seguridad, se elimina automáticamente la configuración de respaldo más antigua.

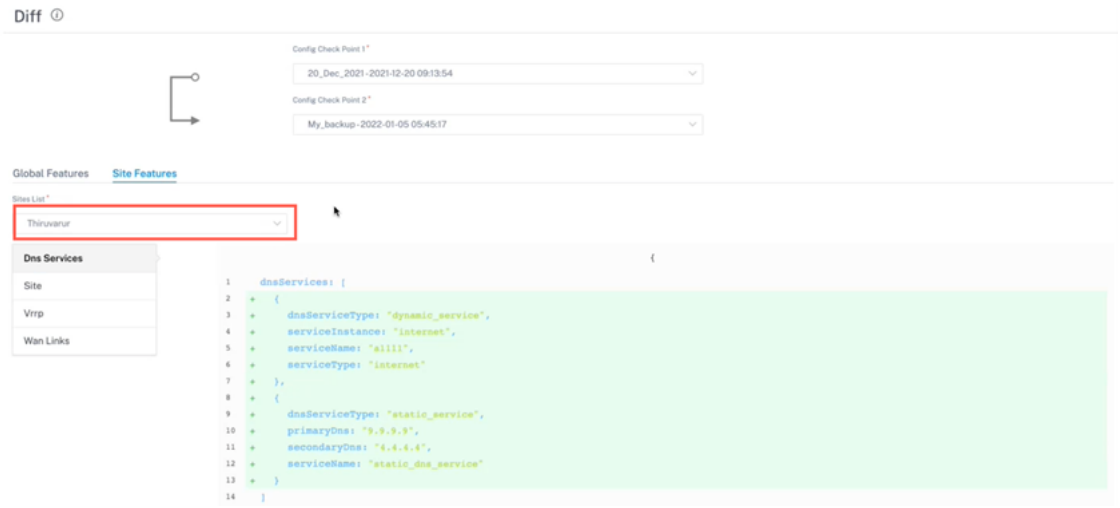
Hay dos tipos de configuraciones disponibles:

- **Nivel global**: En la categoría global, puede ver una lista de funciones globales actualizadas, como regiones, propiedades y configuración.




- **Nivel de sitio**: En la categoría de sitio, puede seleccionar el sitio en la lista desplegable y ver los detalles modificados, como el sitio, los enlaces WAN y los servicios DNS.




El valor eliminado aparece en fondo rojo con el símbolo menos y el valor actualizado o agregado aparece en fondo verde con el símbolo más.

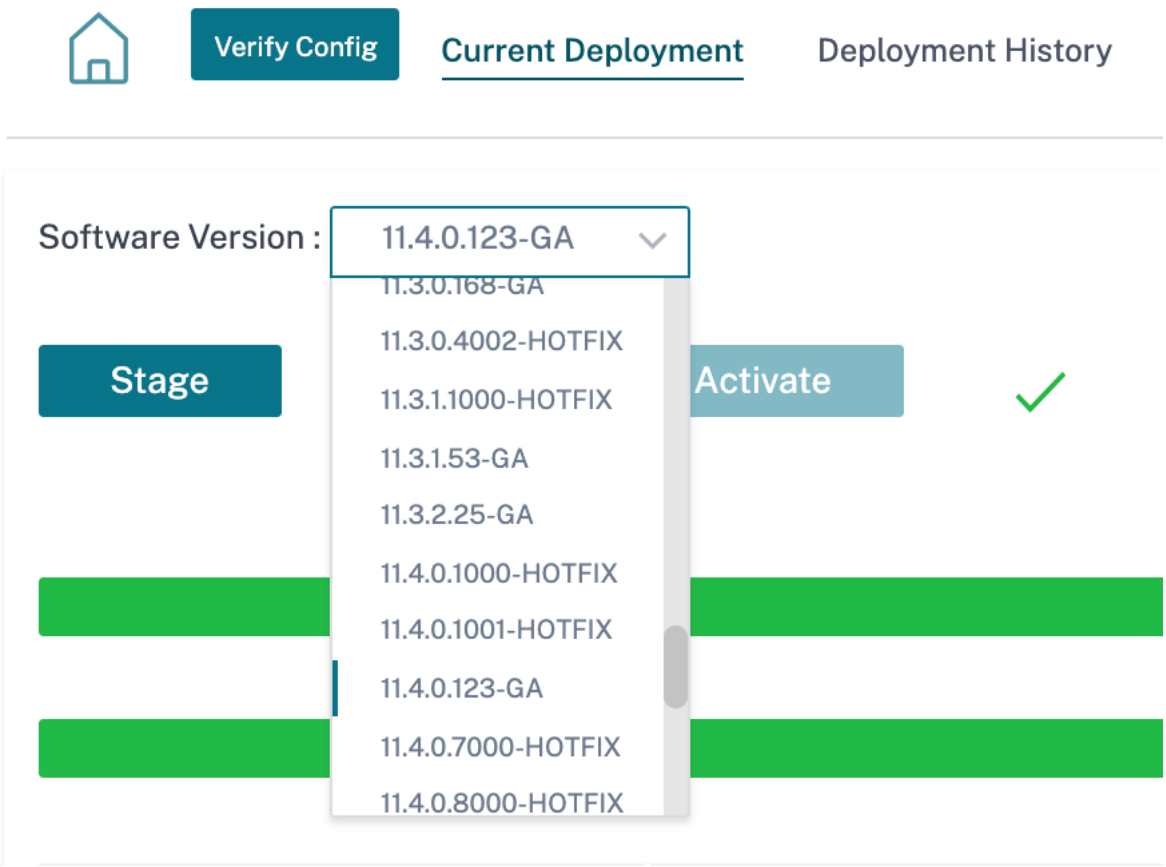

## Implementación

October 31, 2022

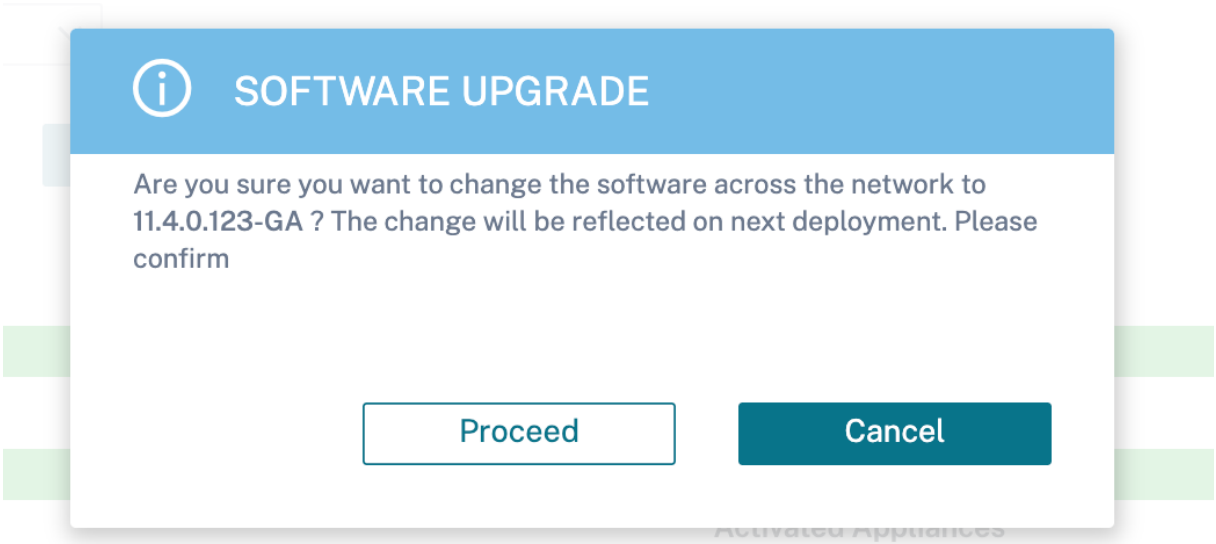
Una vez configurados los sitios, la página de **implementación** le permite cambiar la versión del software, la etapa e implementar la configuración en la red.

Para actualizar el software SD-WAN en todos los dispositivos de la red, seleccione una versión del software del dispositivo en el campo **Versión de software**.

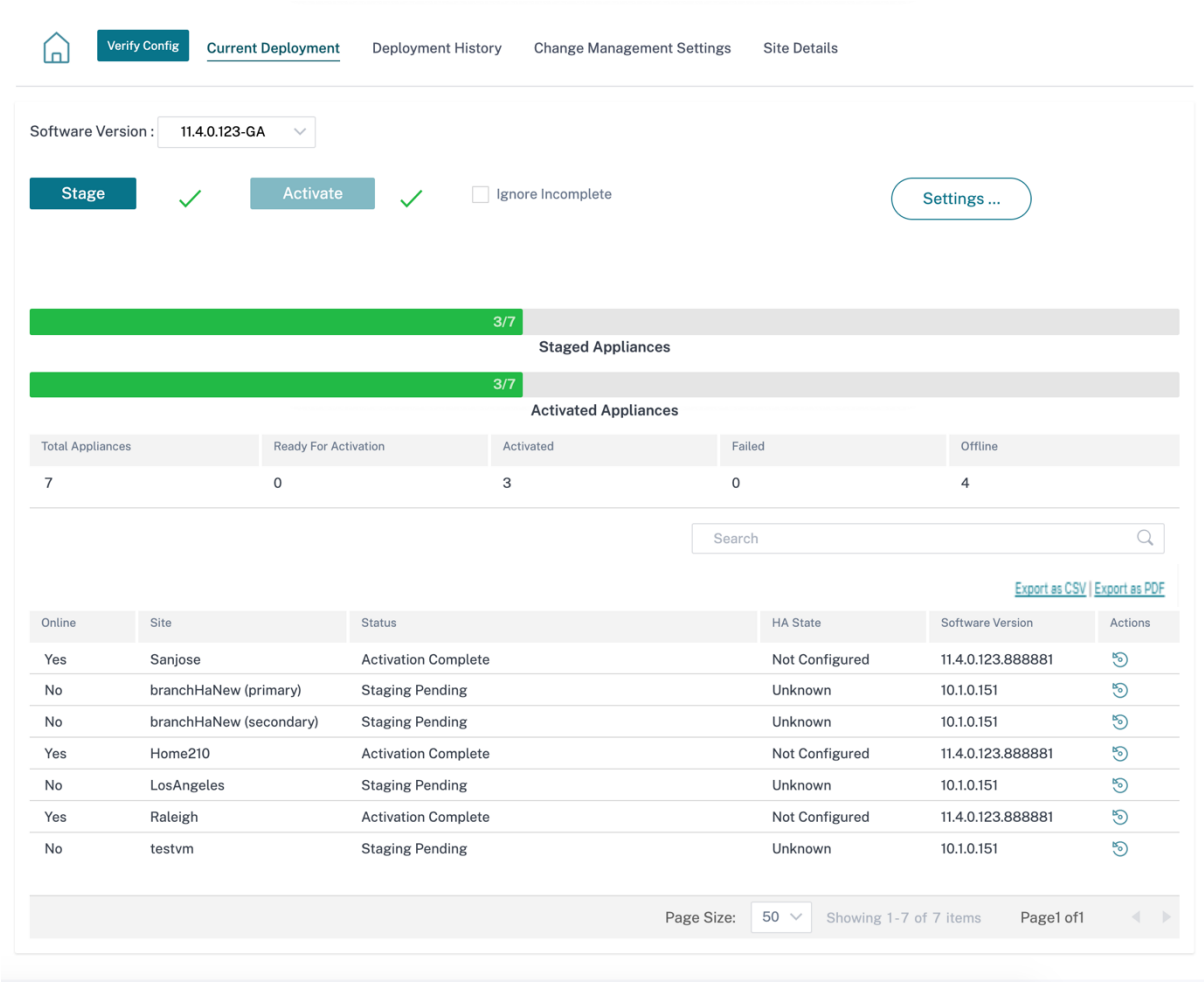
 




Aparece un mensaje de confirmación. Haga clic en **Continuar**.






## Reversión en caso de error

Con la función **Rollback on Error** habilitada, los sitios que no se conectan al servicio Citrix SD-WAN Orchestrator después de realizar la activación de la red (como parte de la implementación) activan una reversión automática a la versión anterior (paquete de última fase) para intentar restaurar la conectividad.

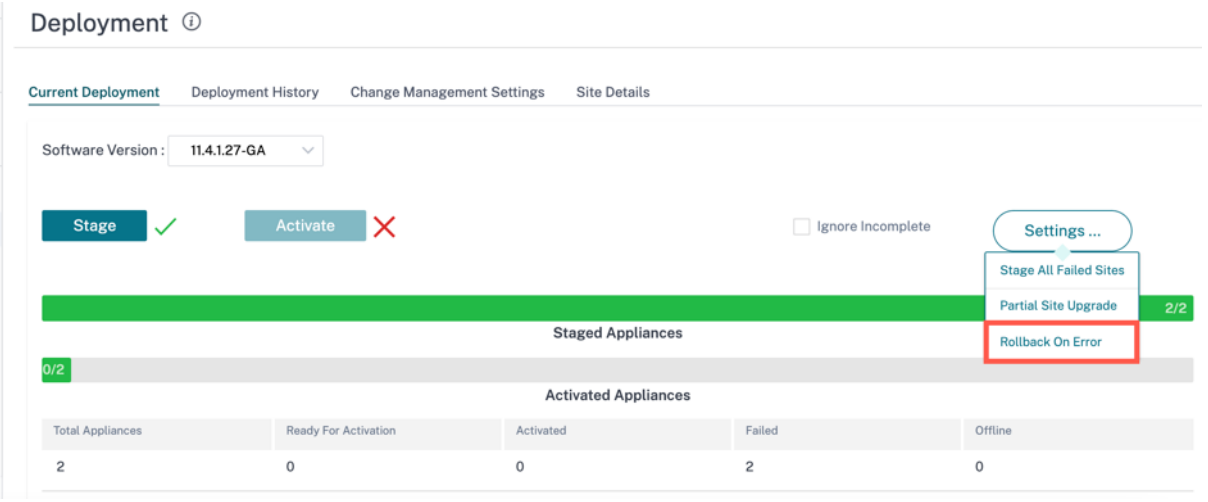
> **Nota**
>
> La reversión automática solo se aplica al sitio que no se pudo conectar al servicio Citrix SD-WAN Orchestrator y no a toda la red.

La reversión solo se activa si el dispositivo pierde la conectividad del servicio Citrix SD-WAN Orchestrator, no en otros casos, como si el estado de la ruta virtual deja de funcionar, etc.

Si al menos un sitio de la red inicia una reversión, un mensaje de advertencia muestra una lista de los sitios que están intentando hacer la reversión y una opción para iniciar una reversión en toda la red de todos los sitios en línea. Puede comprobar el progreso de estos sitios y elegir la acción adecuada.

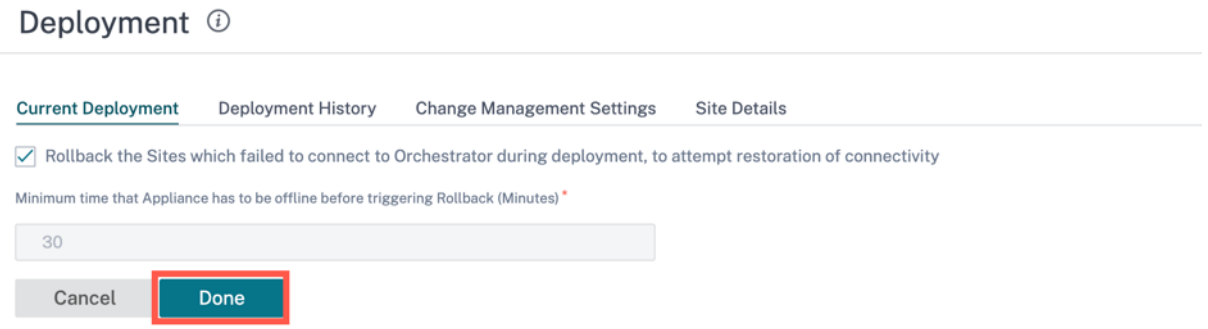
 

Para habilitar la función de reversión en caso de error, vaya a **Configuración > Implementación > Configuración > Reversión en caso de error**.




Puede seleccionar la casilla de verificación **Revertir en caso de error** para habilitar la reversión automática de los sitios que no se han podido conectar al servicio Citrix SD-WAN Orchestrator después de la activación. La función de **reversión en caso de error** debe estar habilitada antes de iniciar la implementación para habilitar su funcionalidad.

Para que un sitio active la reversión automática, debe permanecer sin conexión durante al menos 30 minutos (actualmente no se puede modificar) después de la activación. Si, en caso de que el sitio pueda conectarse al servicio Citrix SD-WAN Orchestrator en 30 minutos, la reversión no se activará.



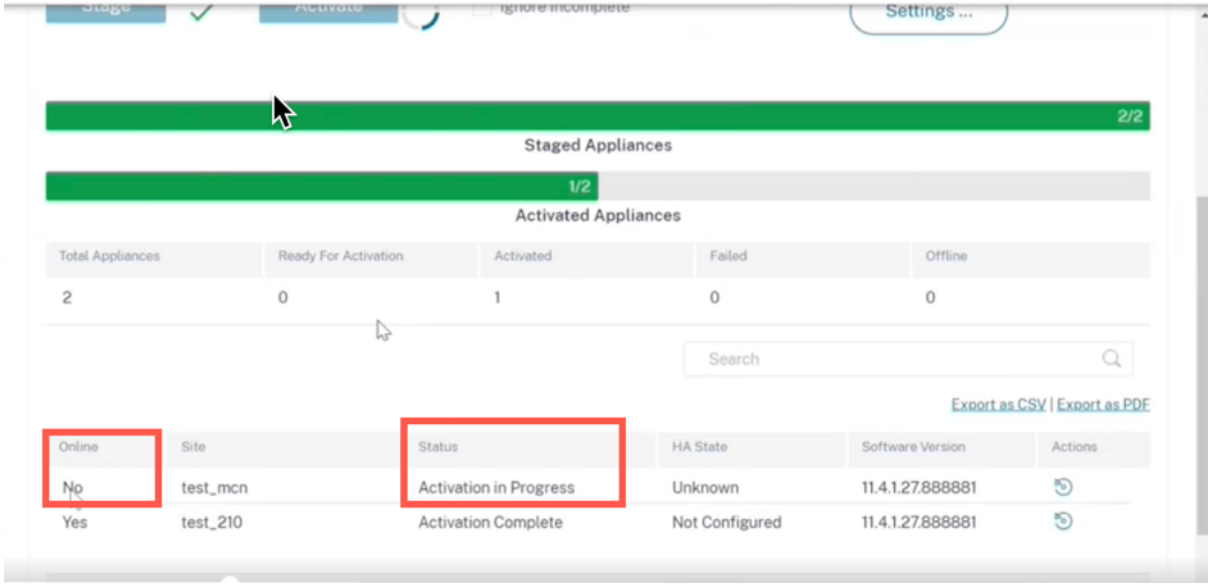

> **Nota**
> La reversión en los sitios solo se realiza cuando el sitio pierde la conectividad después de la activación. La reversión no se activa en los casos en que el sitio está en línea y la activación ha fallado.

Haga clic en **Listo** una vez que haya activado **la opción Revertir en error**.

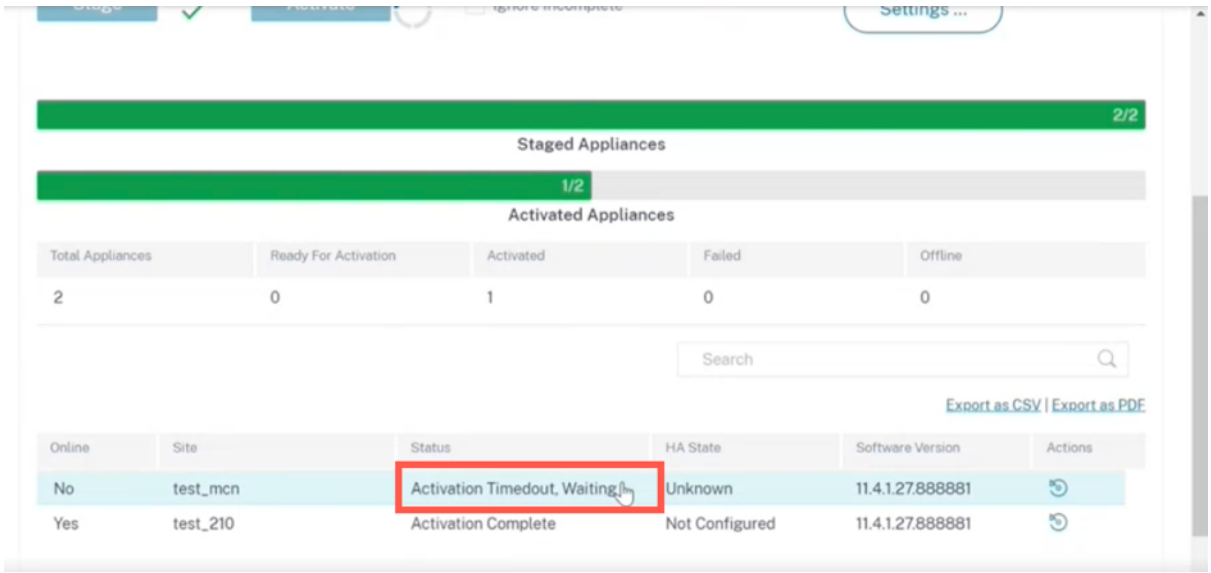
 

**Caso de uso 1: Actualización sin éxito**

Un sitio espera a que se complete la activación durante un tiempo específico con el estado **Activación en curso**.



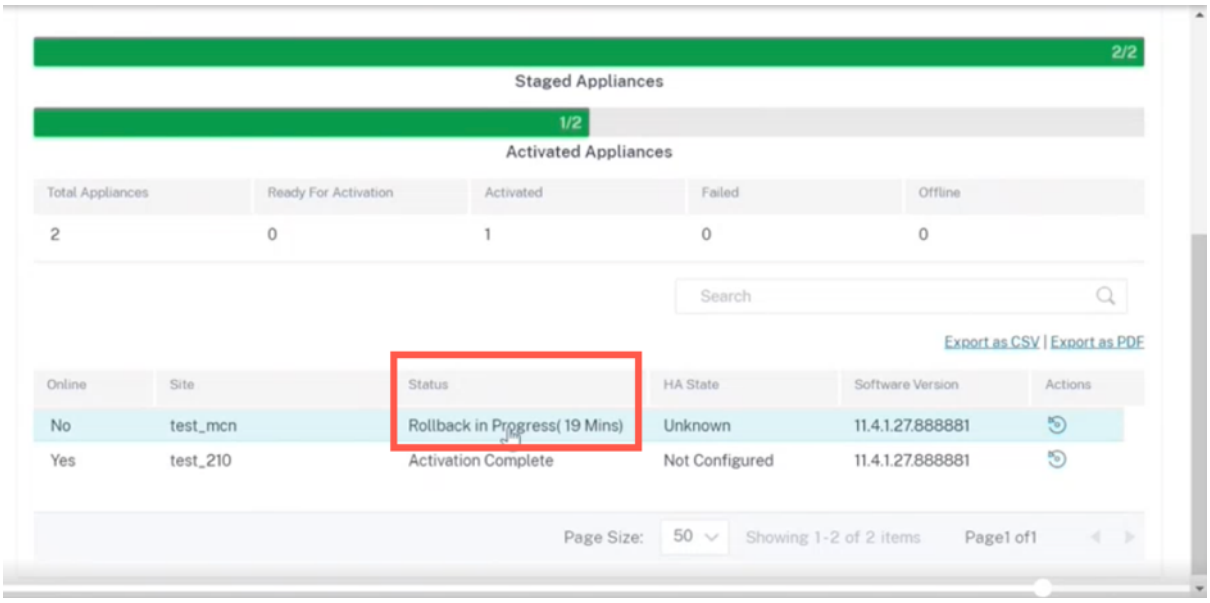

Después de ese tiempo de espera, si el sitio sigue sin conexión, el servicio Citrix SD-WAN Orchestrator espera otros 30 minutos (tiempo de espera de inicio de la reversión) para que el sitio pueda volver a conectarse. En esta etapa, el estado se muestra como **Tiempo de espera de activación, en espera para iniciar la reversión (tiempo restante en minutos)**.




Tras el período de espera de 30 minutos, el dispositivo activa una reversión automática a la configuración anterior o (y) al software para intentar restaurar la conectividad del servicio Citrix SD-WAN Orchestrator. El servicio Citrix SD-WAN Orchestrator espera 20 minutos (configuración no configurable) para que el dispositivo se conecte al servicio Citrix SD-WAN Orchestrator y, durante este período, el

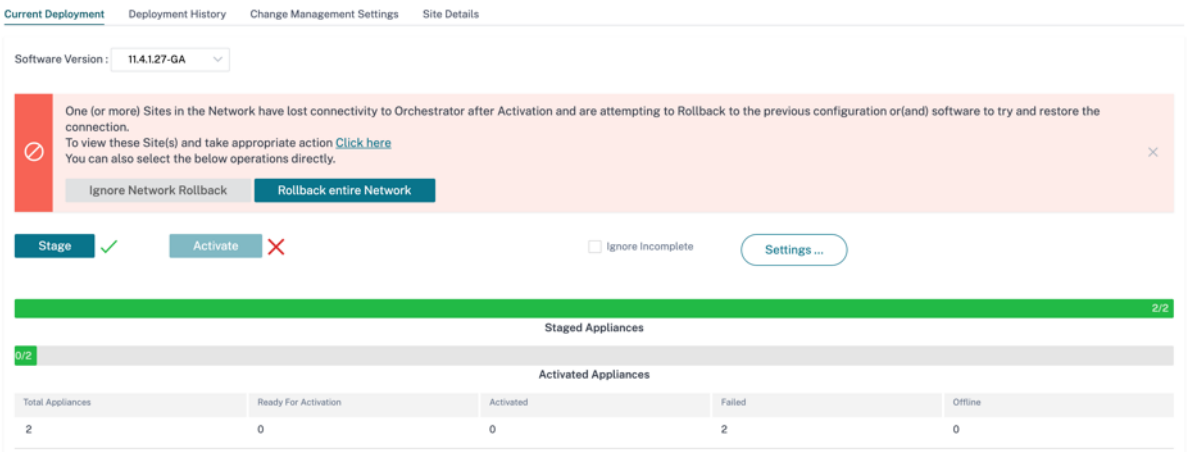
 

estado se muestra **como Reversión en curso (tiempo restante en minutos)**.




Si el dispositivo no se puede volver a conectar, en estos 20 minutos, el servicio Citrix SD-WAN Orchestrator marca la operación de reversión como fallida y el estado se muestra como **Fallo de reversión del dispositivo**.

En la red, si al menos un dispositivo ha iniciado la reversión automática, se presenta un banner al usuario de la siguiente manera:




Según la etapa de activación de la red, las opciones que se muestran realizan las siguientes operaciones:

- Ignorar la reversión de red
  - **Para un caso de actualización sin interrupciones**: finalice la implementación actual.
  - **Primer paso en el caso de actualización sin éxito**: La implementación pasa al segundo paso de la activación.

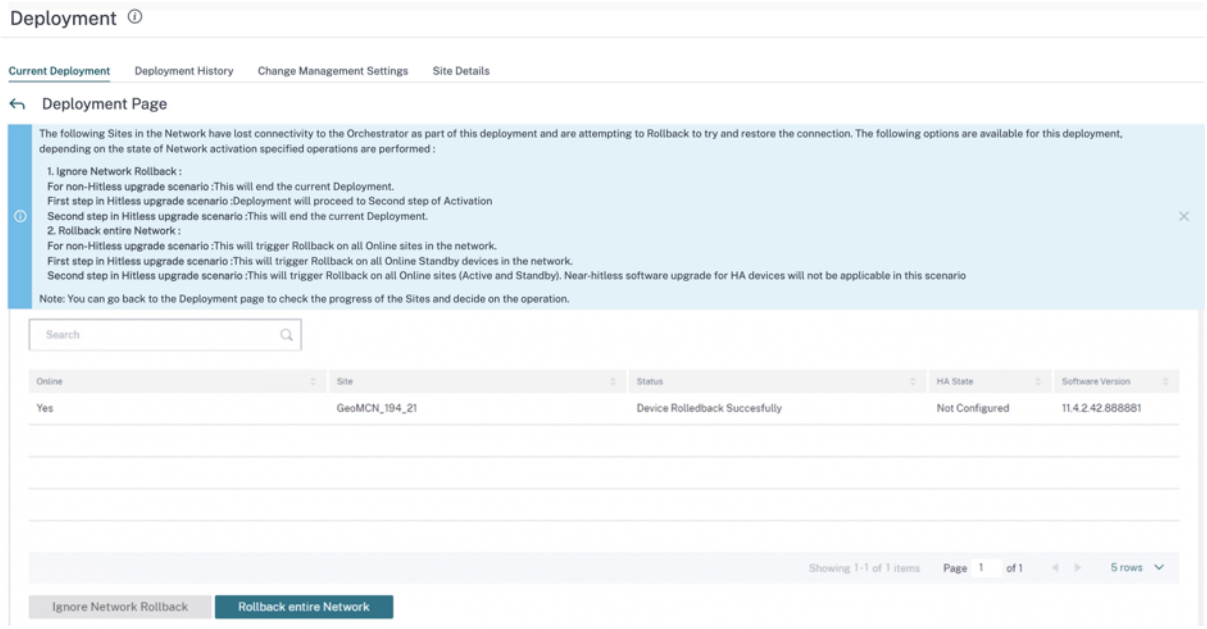
  - **Segundo paso en el caso de actualización sin éxito**: finalizar la implementación actual.

- Revertir toda la red:

  - **Para un caso de actualización sin interrupciones**: Active la reversión en todos los sitios en línea de la red.
  - **Primer paso en el caso de actualización sin interrupciones**: Active la reversión en todos los dispositivos en espera en línea de la red.
  - **Segundo paso en el caso de actualización sin éxito**: Activar la reversión en todos los sitios en línea (activos y en espera). La actualización de software prácticamente ininterrumpida para dispositivos de alta disponibilidad no es aplicable en este caso.

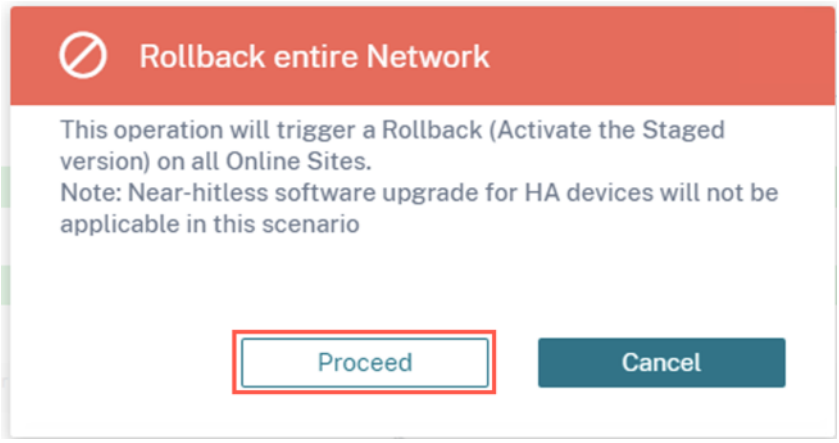
Puede hacer clic en el hipervínculo Más **clic aquí** para ver la lista de sitios para los que la reversión está en curso o se ha completado y realizar las acciones anteriores para esa página.

También puede esperar a que los sitios que han activado la reversión tengan éxito o no funcionen antes de decidir si activar la reversión en toda la red.




Si selecciona la opción **Revertir toda la red**, aparece el siguiente cuadro emergente.




> **Nota:**
> La actualización de software casi sin interrupciones para el dispositivo de alta disponibilidad no se aplica en este caso, es decir, si hay algún sitio de alta disponibilidad en la red, al desencadenar una reversión en toda la red, se activan ambos dispositivos de alta disponibilidad de ese sitio a la vez, lo que puede provocar inactividad de la red.

Haga clic en **Continuar** para iniciar la reversión de toda la red en todos los sitios en línea.

#### Caso de uso 2: Actualización sin éxito

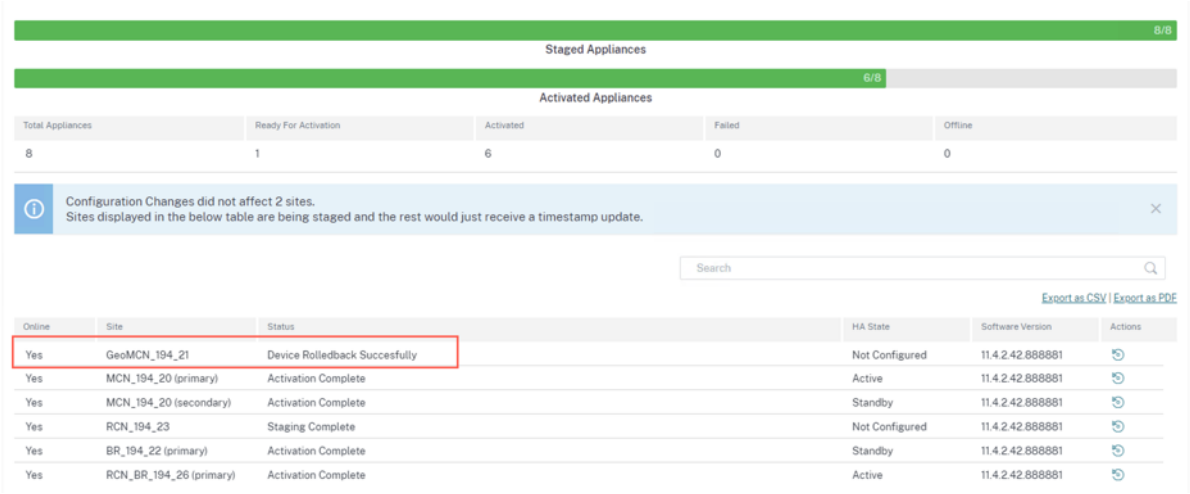
En el caso de la actualización sin impacto, los dispositivos en espera se activarían primero, seguidos de los dispositivos activos y de baja disponibilidad. Como parte del primer paso, si el dispositivo en espera se desconecta después de la activación e inicia una reversión, están disponibles las siguientes opciones:

- **Ignorar la reversión de la red**: ignore los dispositivos en espera que están fuera de línea y continúe con la activación de los dispositivos activos.
- **Reversión de toda la red**: Anule todos los dispositivos en espera en línea que hayan completado la activación y finalice la implementación en curso. En este caso, no se activa ningún dispositivo activo o que no sea de alta disponibilidad.

El siguiente paso de la actualización sin errores, que es la activación de dispositivos activos y de dispositivos que no son de alta disponibilidad, se sigue el mismo flujo de trabajo de reversión por error que se menciona en la sección de actualizaciones sin errores anterior. En este caso, si elige **Revertir toda la red**, la reversión se activa para todo el dispositivo (tanto activo como en espera).

Una vez que el sitio complete la reversión y se conecte de nuevo al servicio Citrix SD-WAN Orchestrator, el estado de ese sitio mostrará La **reversión del dispositivo se ha realizado correctamente** y los sitios están en línea.




### Limitaciones

No se admite la corrección automática de dispositivos y redes con reversión o reversión.

> **Nota**
> La reversión automática del sitio es solo un mecanismo de respaldo para intentar restaurar la conectividad perdida con el servicio Citrix SD-WAN Orchestrator. Si el dispositivo sigue sin poder conectarse al servicio Citrix SD-WAN Orchestrator, compruebe la configuración de red de este dispositivo.

Puede exportar los resultados filtrados a un archivo CSV o PDF mediante las opciones **Exportar como CSV** y **Exportar como PDF**. El nombre del archivo CSV y PDF lleva el prefijo **Lista de sitios de implementación** seguido de la fecha y la hora en que se exportó el archivo.

- **Etapa**: Una vez que la verificación de la configuración se haya realizado correctamente, haga clic en **Etapa** para distribuir los archivos de configuración a todos los dispositivos de la red. De forma predeterminada, el servicio Citrix SD-WAN Orchestrator espera a que todos los nodos de control (MCN, RCN, Geo MCN, Geo RCN) y los dispositivos de sucursal en línea se organicen antes de permitir que el usuario los active.

  Si el proceso de puesta en escena falla en algún sitio, utilice la opción **Reintentar la puesta en escena**, situada en la columna **Acciones**, para volver a iniciar el proceso de puesta en escena.

- **Activar**: haga clic en **Activar** para activar la configuración por etapas en todos los sitios de la red.

- **Ignorar lo incompleto**: Si se selecciona, la casilla **Activar** solo se activa después de que se pongan en escena todos los nodos de control en línea (MCN, RCN, Geo MCN, Geo RCN). Puede optar por activarlos incluso si algunos de los dispositivos de la sucursal en línea no están preparados. Los dispositivos de sucursal en línea que no se ponen en escena se ignoran.

- **Configuración de actualización parcialdel sitio: Se agrega la opción Actualización**parcial del sitio para actualizar o degradar los sitios seleccionados con una versión diferente. La función de**actualización parcial del sitio** permite probar una nueva versión antes de implementarla en toda la red.

Con la función de **actualización parcial del sitio**, las actualizaciones se pueden escalonar y, por lo tanto, reducir el impacto de las actualizaciones de software durante el horario laboral.

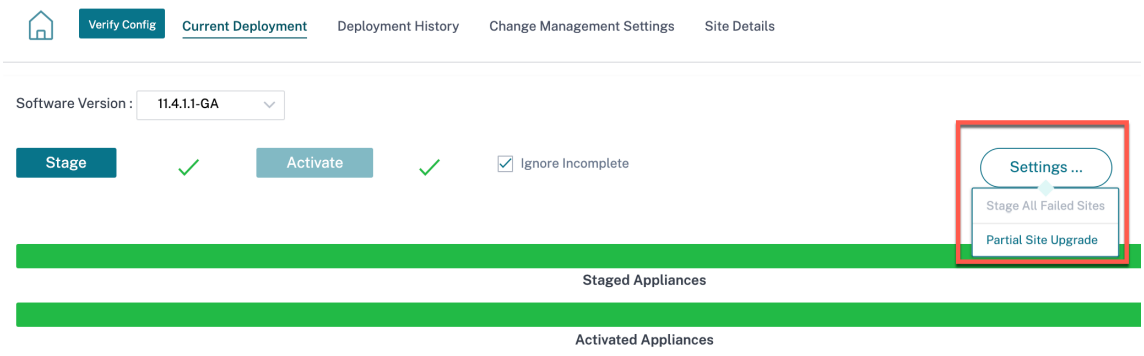
> **Nota**
>
> La actualización parcial del sitio solo se puede realizar cuando todos los sitios de la red ejecutan la versión 11.2.2 o superior del software Citrix SD-WAN.

Cualquier cambio de configuración para la **actualización parcial del sitio** necesita una administración de cambios para que los cambios surtan efecto. La **actualización parcial del sitio** elige la versión inferior y genera la configuración para la misma. No se puede probar ninguna función nueva mientras la red esté en el modo de **actualización parcial del sitio**.

Al cambiar de una versión más reciente a una anterior mediante la **actualización parcial del sitio**, si se trata de una función que solo es compatible con la versión más reciente (con una configuración similar presente tanto en la versión nueva como en la anterior), se producen errores de auditoría. Por ejemplo, si se selecciona una nueva plataforma que solo es compatible con la versión más reciente, esto generará errores de auditoría.

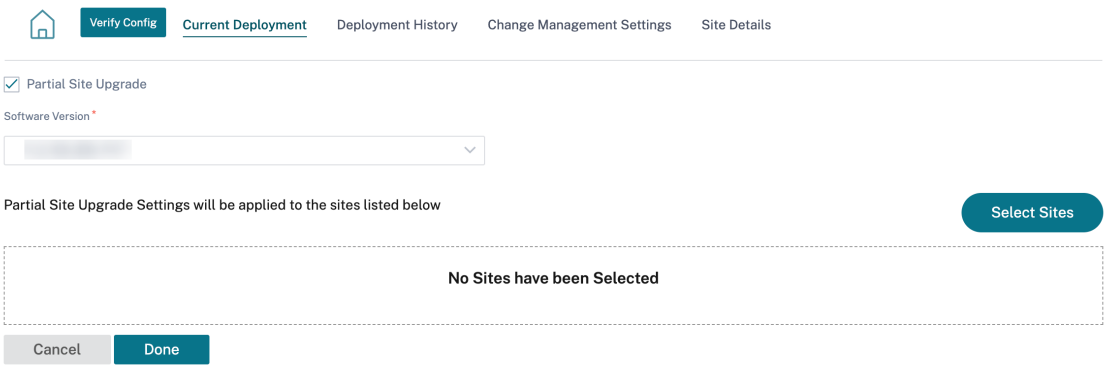
Para realizar la actualización parcial del sitio:

1. Haga clic en la **configuración...** y seleccione la opción **Actualización parcial del sitio**.



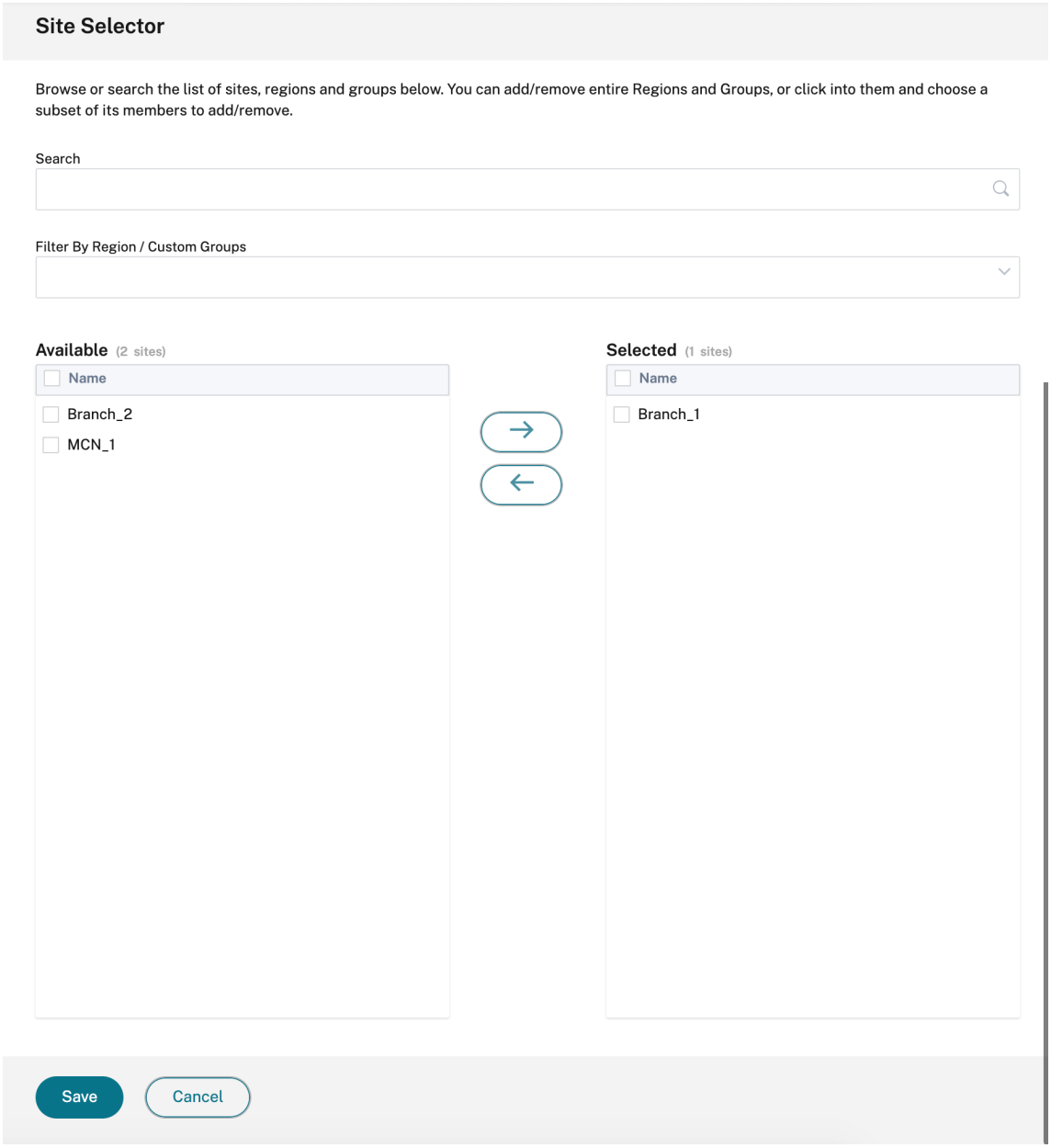

2. Seleccione la casilla Actualización parcial del sitio, elija la versión del software y haga clic en **Seleccionar sitios** para agregar nuevos sitios.

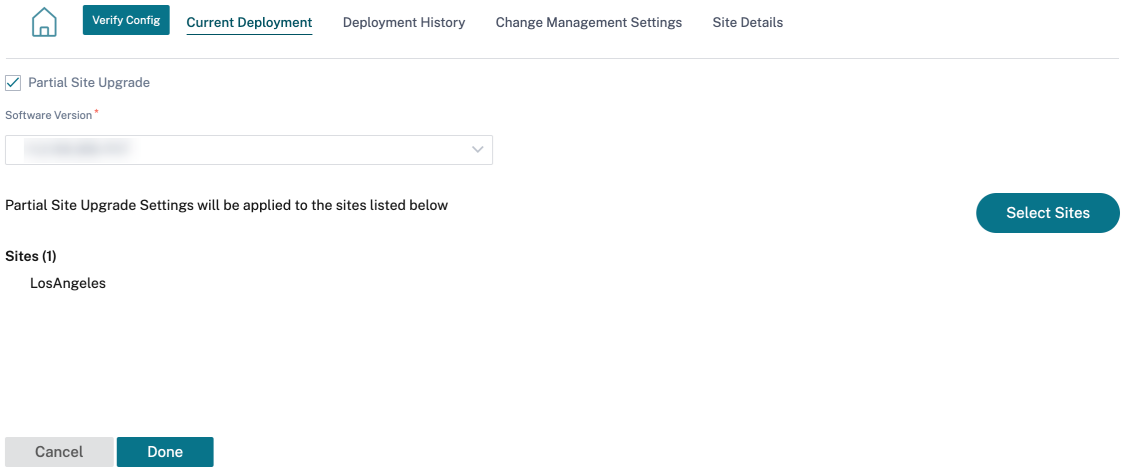



3. Seleccione los sitios y haga clic en **Guardar**.



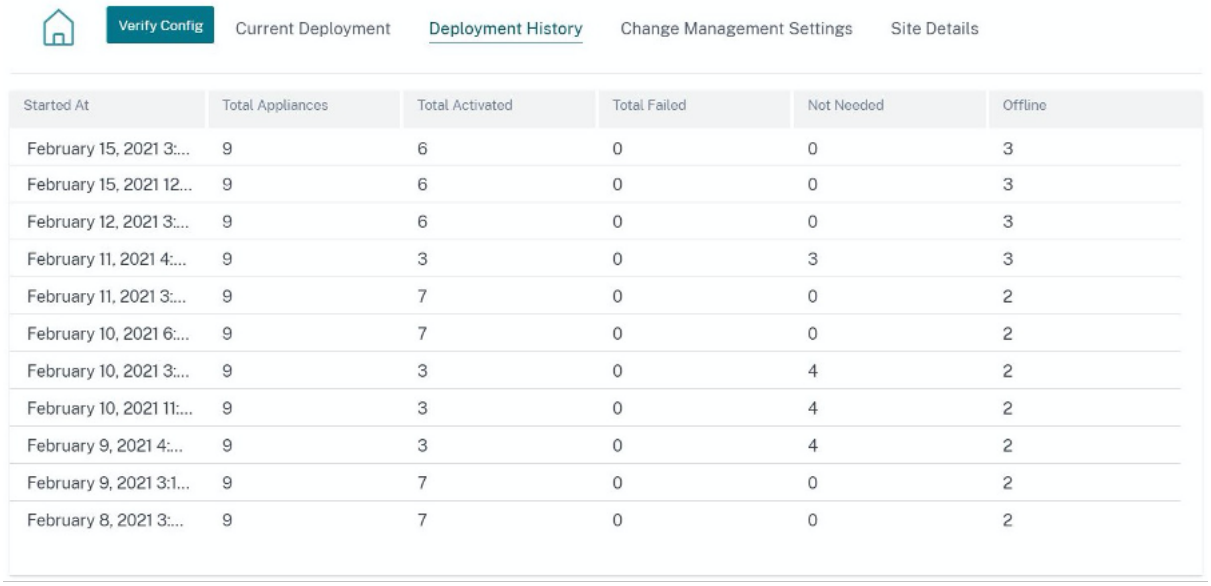

 




En el caso de una actualización solo de configuración, solo se organizan y activan los sitios que tienen cambios de configuración. Para los sitios restantes, la marca de tiempo se actualiza y procesa.

Si se cambia la versión del software, tanto la configuración como el paquete de software se almacenan y activan en todos los sitios de la red.

La sección **Historial de implementacións** ayuda a revisar las operaciones y los resultados de la implementación anterior.




| Started At | Total Appliances | Total Activated | Total Failed | Not Needed | Offline |
|---|---|---|---|---|---|
| February 15, 2021 3:... | 9 | 6 | 0 | 0 | 3 |
| February 15, 2021 12... | 9 | 6 | 0 | 0 | 3 |
| February 12, 2021 3:... | 9 | 6 | 0 | 0 | 3 |
| February 11, 2021 4:... | 9 | 3 | 0 | 3 | 3 |
| February 11, 2021 3:... | 9 | 7 | 0 | 0 | 2 |
| February 10, 2021 6:... | 9 | 7 | 0 | 0 | 2 |
| February 10, 2021 3:... | 9 | 3 | 0 | 4 | 2 |
| February 10, 2021 11:... | 9 | 3 | 0 | 4 | 2 |
| February 9, 2021 4:... | 9 | 3 | 0 | 4 | 2 |
| February 9, 2021 3:1... | 9 | 7 | 0 | 0 | 2 |
| February 8, 2021 3:... | 9 | 7 | 0 | 0 | 2 |

## Actualización de software casi sin éxito de HA

Durante la actualización del software (11.0.x y versiones anteriores), la preparación y la activación de todos los dispositivos de la red se realizan al mismo tiempo. Esto incluye el par High Availability (HA), lo que lleva al tiempo de inactividad de la red. Con la función de actualización de software de

alta disponibilidad prácticamente sin interrupciones, el servicio Citrix SD-WAN Orchestrator garantiza que el tiempo de inactividad durante el proceso de actualización del software (11.1.x y superior) no sea superior al del cambio de HA a lo largo del tiempo.

> **Nota**
>
> La actualización de software casi sin éxito de HA es aplicable para lo siguiente:
>
> - Los sitios que se implementan en modo Alta Disponibilidad (HA). No es aplicable para sitios que no sean de alta disponibilidad.
> - Solo implementaciones basadas en el servicio Citrix SD-WAN Orchestrator y no para las redes que se administran mediante el SD-WAN Center o MCN.
> - Solo actualizaciones de software y no actualizaciones de configuración. Si se produce un cambio de configuración junto con el software como parte de la actualización, el servicio Citrix SD-WAN Orchestrator no realiza una actualización de software de alta disponibilidad casi sin interrupciones y continúa actualizándose de la manera anterior (actualización en un solo paso).

Resumen de la secuencia de actualización:

1. El servicio Citrix SD-WAN Orchestrator comprueba el estado de alta disponibilidad de todos los dispositivos de la red.
2. Actualiza todos los dispositivos secundarios que están en estado de **espera**.
3. Se activa la conmutación HA y se cambia el estado de los dispositivos **activos** y **en espera**.
4. Actualiza los dispositivos principales que ahora están en estado **de espera**.

La actualización de software casi sin éxito de HA es un proceso de actualización de dos pasos:

**Paso 1**: Durante la actualización del software, después de la versión 11.1, el servicio Citrix SD-WAN Orchestrator primero realiza la actualización del software en todos los dispositivos que están en estado de **espera** en la red. La red sigue en funcionamiento con los **dispositivos Active** instalados.

Una vez que todos los dispositivos **en espera** se actualicen al software más reciente, se activa la conmutación de HA en toda la red. Los dispositivos **en espera** (con el software más reciente) pasan a estar **activos**.

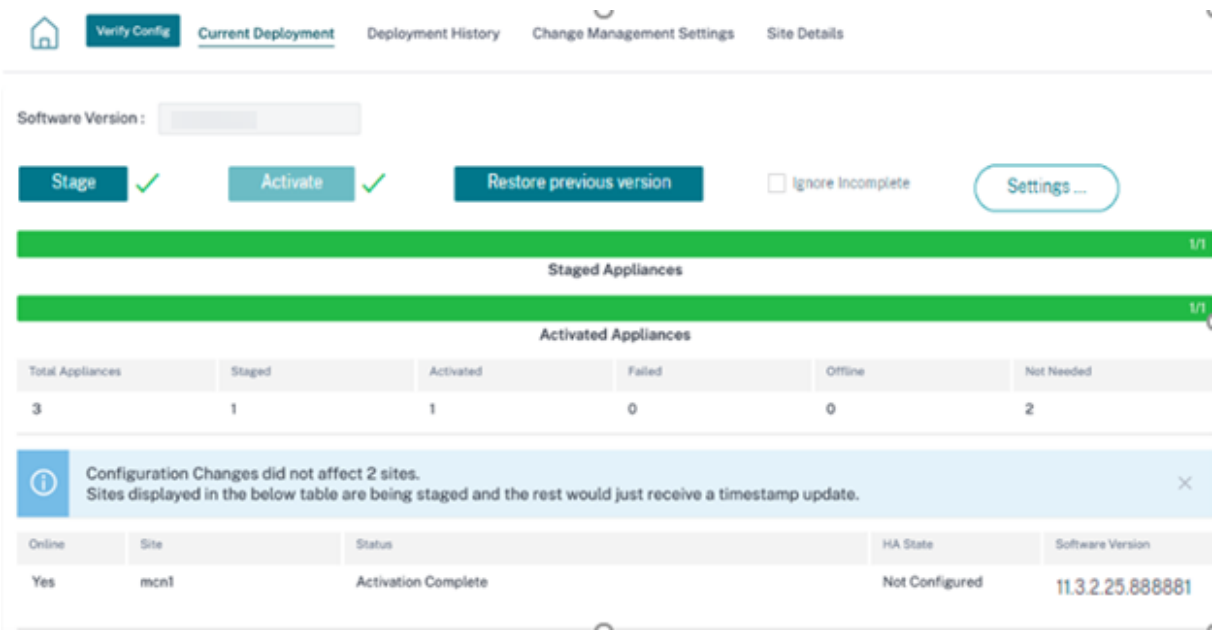
**Paso 2**: Los dispositivos **en espera** actuales con una versión de software antigua se actualizan al software más reciente y seguirán funcionando en modo de **espera**.

Durante este proceso de actualización de software, todos los demás sitios que no sean de alta disponibilidad también se activarán con el software más reciente.

Para obtener más información, consulte las preguntas frecuentes.

Para ver el estado de la actualización, vaya a **Deployment Tracker** > **Implementación actual**.




- **Etapa**: haga clic en **Etapa** para distribuir los archivos de configuración a todos los dispositivos de la red. De forma predeterminada, el servicio Citrix SD-WAN Orchestrator espera a que todos los nodos de control (MCN, RCN, Geo MCN, Geo RCN) y los dispositivos de sucursal en línea se organicen antes de permitir que el usuario los active.
- **Activar**: haga clic en **Activar** para activar la configuración por etapas en todos los sitios de la red.
- **Restaurar la versión anterior**: haga clic en **Restaurar la versión anterior** para volver a la configuración activada anteriormente en la red. La actualización del software HA casi sin interrupciones se aplica cuando se restaura la versión anterior si la versión anteriormente activa es solo un cambio de versión de software y no un cambio de configuración. Para obtener más información acerca de esta funcionalidad, consulte Restaurar la versión anterior.
- **Ignorar lo incompleto**: Si se selecciona, la casilla **Activar** solo se activa después de que se pongan en escena todos los nodos de control en línea (MCN, RCN, Geo MCN, Geo RCN). Puede optar por activarlos incluso si algunos de los dispositivos de la sucursal en línea no están preparados. Los dispositivos de sucursal en línea que no se ponen en escena se ignoran.

En el caso de una actualización solo de configuración, solo se organizan y activan los sitios que tienen cambios de configuración. Para los sitios restantes, la marca de tiempo se actualiza y procesa. La columna **No se necesita** muestra el número de sitios que no tienen ningún cambio de configuración.

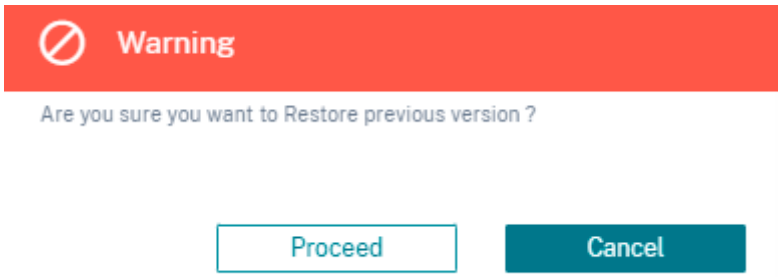
Si se cambia la versión del software, tanto la configuración como el paquete de software se almacenan y activan en todos los sitios de la red.

### Restaurar la versión anterior

En la funcionalidad de restauración de la versión anterior, el servicio Citrix SD-WAN Orchestrator inicia una activación en toda la red de la configuración anterior y restaura la configuración (y/o el software) previamente activados en la red.

Al seleccionar la opción **Restaurar la versión anterior**, aparece el siguiente mensaje de confirmación:




> **Nota:**
>
> La acción Restaurar la versión anterior se puede realizar cuando la red no está en estado preestablecido. Esta opción está inhabilitada para las redes por etapas.

### Corrección automática para configuración y actualización de software

En el servicio Citrix SD-WAN Orchestrator, la función de corrección automática se implementa en el flujo de trabajo de administración de cambios.

Cuando el ensayo falló para un sitio y si el sitio que había fallado en el ensayo es un nodo de control, debe reiniciar después de recibir el mensaje de error de ensayo. El botón **Activar** no se habilitará si se produce un error en la configuración provisional de los nodos de control. Si el sitio que falló en la puesta en escena es un nodo de sucursal, aún puede continuar con la activación. Pero para sincronizar esa rama con la red, realice otra ronda de administración de cambios.

> **Nota**
>
> - La comprobación de corrección automática comienza solo después de hacer clic en el botón **Activar** y se detiene una vez que se emite la siguiente etapa desde la interfaz de usuario del servicio Citrix SD-WAN Orchestrator.
> - La funcionalidad del modo de mantenimiento solo es aplicable a la función de corrección automática. Si inicia una **etapa y unaactivación**, el dispositivo con el modo de mantenimiento activado también se actualiza con los cambios de software y configuración.

Con la mejora de la función de corrección automática, cuando se produce un error de ensayo, el mecanismo de corrección automática empuja el software y la versión de configuración esperados

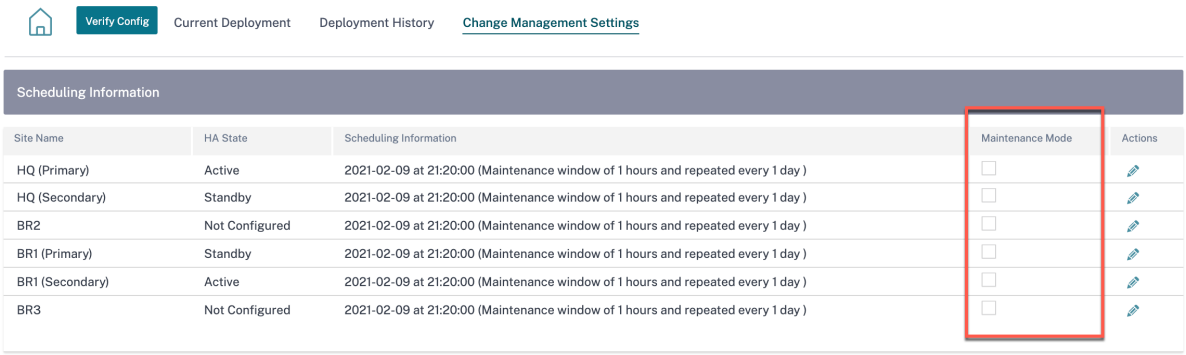
 

a la rama fallida e intenta ponerlo en sincronización con la red actual. La función de corrección automática es aplicable a fallas de ensayo en el nodo de sucursal y para errores de activación en cualquier nodo.

Los siguientes son los dos puntos de activación cuando se inicia la corrección automática:

- En la interfaz de usuario del rastreador de implementacións del servicio Citrix SD-WAN Orchestrator, una vez que aparece un mensaje de **error de**ensayo**o error de activación**, la corrección automática comienza a ejecutarse en segundo plano. La comprobación de corrección automática comienza una vez completada la activación.
- En caso de que el software y la configuración no coincidan, y el dispositivo no ha presentado el software y la versión de configuración esperados, el servicio Citrix SD-WAN Orchestrator comienza a enviar el software y la copia de configuración necesarios al dispositivo para su activación.

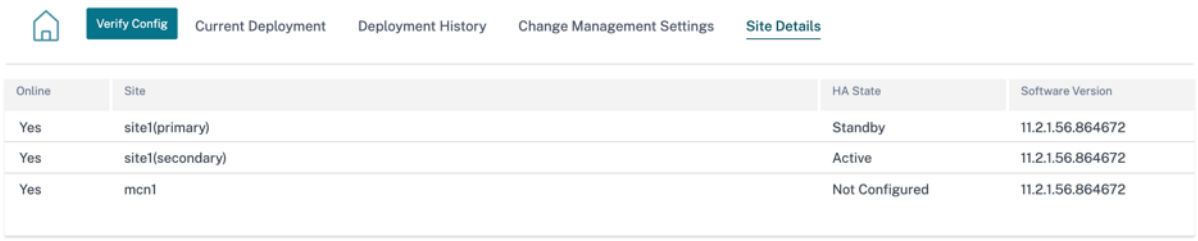
Para solucionar problemas de un dispositivo de forma manual, active la casilla de verificación del modo de mantenimiento en la **configuración de administración de cambios**. Esta casilla de verificación se utiliza para controlar si el dispositivo necesita ser marcado para corrección automática o no. Una vez desactivada la casilla de verificación Modo de mantenimiento, la corrección automática sincroniza el dispositivo con el software de red y la versión de configuración.




## Detalles del sitio

La ficha **Detalles del sitio** del Deployment Tracker proporciona información sobre todos los dispositivos de la red. La tabla contiene el nombre del dispositivo, la conectividad del servicio Citrix SD-WAN Orchestrator, el estado de alta disponibilidad (HA) y la versión de software que se está ejecutando actualmente.




## Verificar configuración

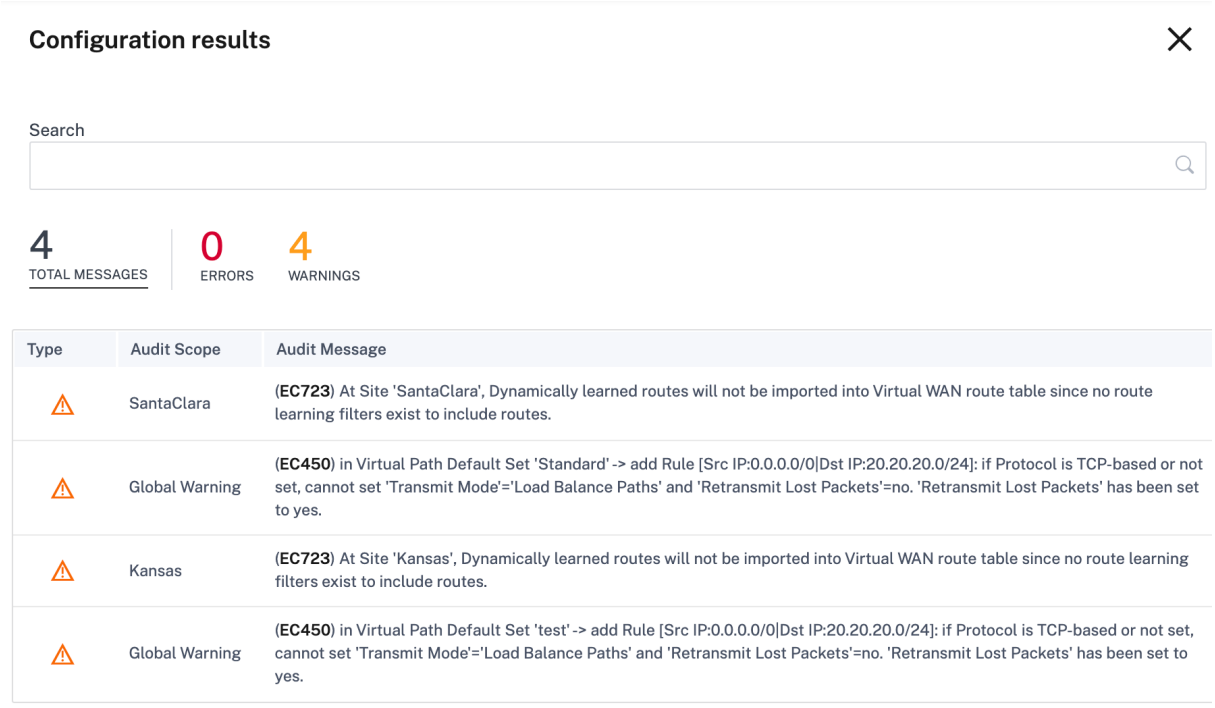
Puede hacer clic en **Verificar configuración** para validar la configuración de la red y comprobar si hay algún error o advertencia de auditoría. Al hacer clic en **Verificar configuración**, aparece la página de **resultados de la configuración**. Esta página contiene detalles de los errores y advertencias de auditoría.

Los resultados de la configuración muestran el número total de errores y advertencias de auditoría. Los resultados también se filtran según el tipo de auditoría (error o advertencia) y se muestran con diferentes códigos de colores. Puede hacer clic en los enlaces de los números para ver los resultados filtrados.

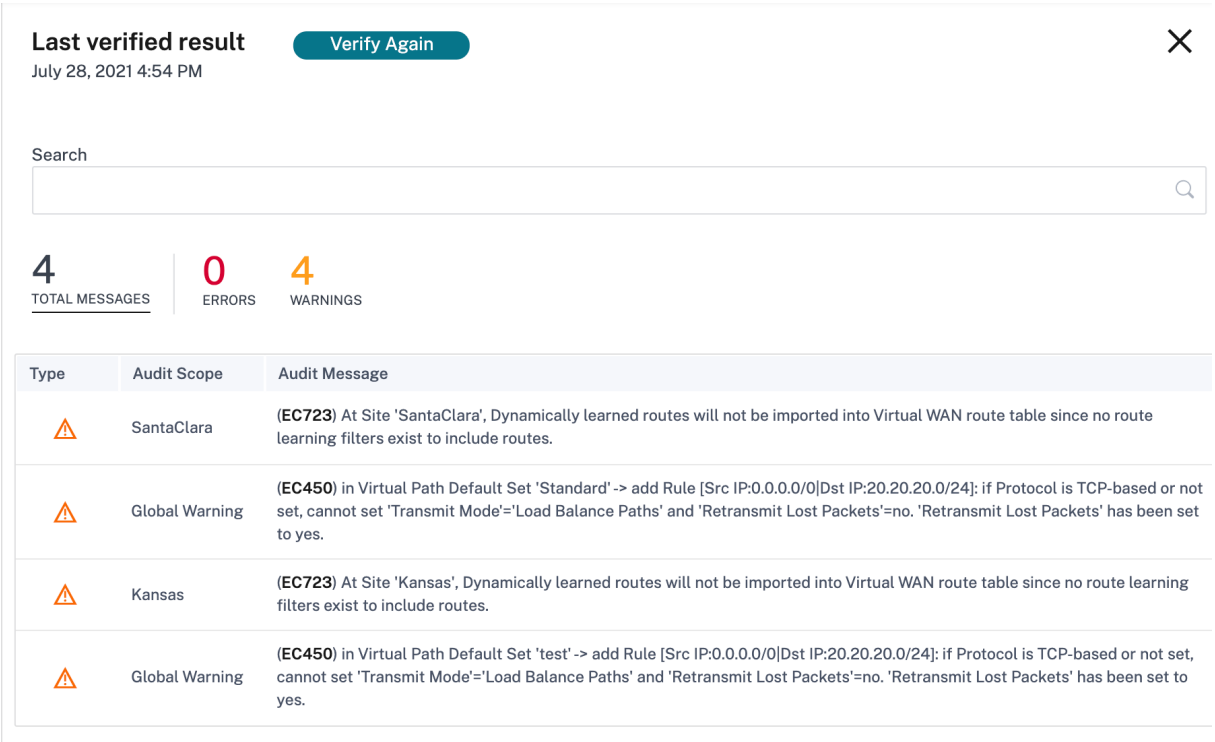
La columna **Tipo** muestra un icono para indicar si se trata de un error o de una advertencia. La columna **Alcance de la auditoría** especifica si el error o la advertencia se refieren a un sitio o al nivel de red. Si el error o la advertencia son específicos de un sitio, se muestra el nombre del sitio. Si el error o la advertencia se producen a nivel global, se muestran **Error globalo Advertencia global**, respectivamente. La columna**Mensaje de auditoría** contiene el código de error y el mensaje de error.

Puede utilizar la barra de búsqueda para buscar cualquier error o advertencia específicos en función del tipo, el código de error, el nombre del sitio o el mensaje de error.




Al hacer clic en **Verificar configuración** por segunda vez, se abre la página de **resultados de la configuración**, que muestra los mismos resultados de la última verificación de la configuración, junto con la fecha y la hora. Si es necesario, puede hacer clic en **Verificar de nuevo** para volver a ejecutar la validación.



# Definiciones de servicios

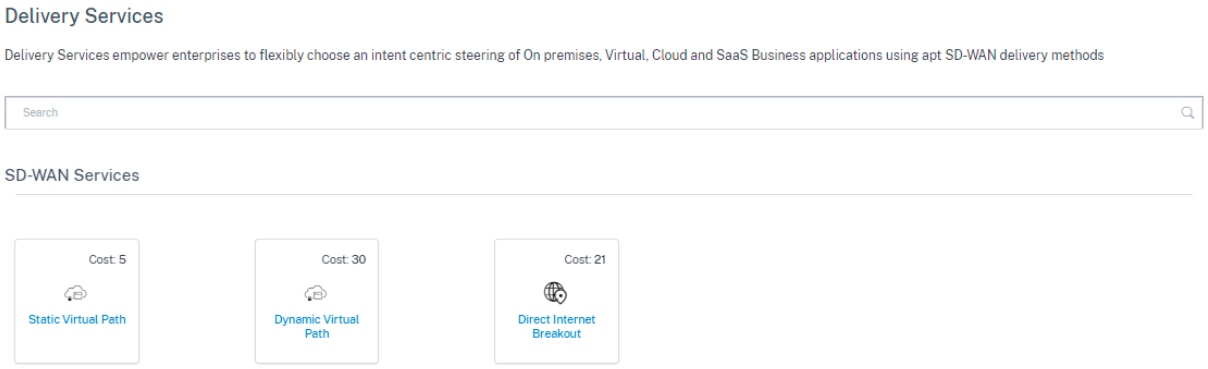
October 31, 2022

Los canales de entrega se clasifican ampliamente en definiciones de servicios y asignación de ancho de banda.

Los servicios de entrega son mecanismos de entrega disponibles en Citrix SD-WAN para dirigir diferentes aplicaciones o perfiles de tráfico mediante los métodos de entrega correctos en función de la intención empresarial. Puede configurar servicios de entrega como Internet, Intranet, rutas virtuales, IPSec y LAN GRE. Los servicios de entrega se definen globalmente y se aplican a los enlaces WAN en sitios individuales, según corresponda.

Cada enlace WAN puede aplicar todos o un subconjunto de los servicios relevantes, y configurar recursos compartidos relativos de ancho de banda (%) entre todos los servicios de entrega.

El servicio Virtual Path está disponible en todos los vínculos de forma predeterminada. Los otros servicios se pueden agregar según sea necesario.
Para configurar los servicios de entrega, al nivel de cliente, vaya a **Configuración** > **Canales de entrega** > **Definiciones de servicios**.




Los Servicios de Entrega se pueden clasificar en términos generales como los siguientes:

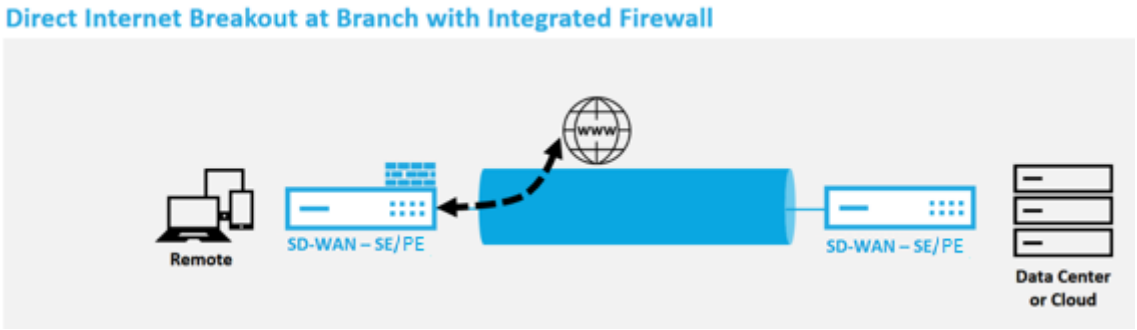
- **Servicio de ruta virtual**: El túnel SD-WAN superpuesto de dos extremos que ofrece conectividad segura, confiable y de alta calidad entre dos sitios que alojan dispositivos SD-WAN o instancias virtuales. Establezca el ancho de banda mínimo reservado para cada ruta virtual en Kbps. Esta configuración se aplica a todos los enlaces WAN de todos los sitios de la red.
- **Servicio de Internet**: Canal directo entre un sitio SD-WAN e Internet público, sin encapsulación SD-WAN involucrada. Citrix SD-WAN admite la capacidad de equilibrio de carga de sesiones para el tráfico con destino a Internet a través de varios enlaces de Internet.
- **Servicio de intranet**: Subyace la conectividad basada en enlaces desde un sitio de SD-WAN a cualquier sitio que no sea de SD-WAN. El tráfico no está encapsulado o puede utilizar cualquier

encapsulación de ruta no virtual, como IPSec, GRE. Puede configurar varios servicios de Intranet.

### Servicio de Internet

El**servicio de Internet** está disponible de forma predeterminada como parte de los servicios de entrega. Para configurar un servicio de Internet, desde el nivel de cliente, vaya a **Configuración** > **Canales de entrega** > **Definiciones de servicios**. En la sección **Servicios de SD-WAN**, seleccione el icono **Direct Internet Breakout** y, a continuación, haga clic en **Agregar**.

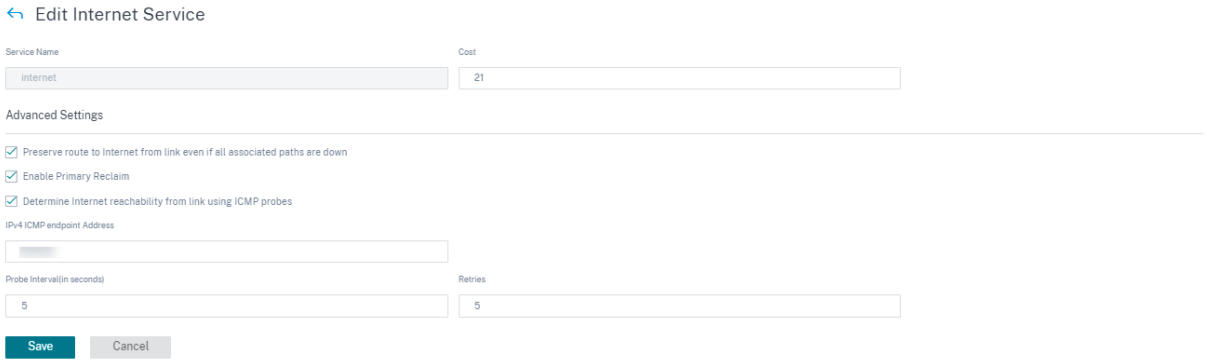




Puede configurar los siguientes servicios de Internet:

- **Preserve la ruta a Internet desde el enlace incluso si todas las rutas asociadas están inactivas**: Puede configurar el coste de la ruta del servicio de Internet en relación con otros servicios de entrega. Con este servicio, puede conservar la ruta a Internet desde el enlace, incluso si todas las rutas asociadas están inactivas. Si todas las rutas asociadas a un enlace WAN están muertas, el dispositivo SD-WAN utiliza esta ruta para enviar o recibir tráfico de Internet.
- **Determine la accesibilidad de Internet desde un enlace mediante sondas ICMP**: Puede habilitar las sondas ICMP para enlaces WAN de Internet específicos a un servidor explícito en Internet. Con la configuración de la sonda ICMP, el dispositivo SD-WAN trata el enlace a Internet como activo cuando las rutas de los miembros del enlace están activas o cuando se recibe la respuesta de la sonda ICMP del servidor.
- **Dirección de punto final ICMP de IPv4**: La dirección IPv4 de destino o la dirección del servidor.
- **Intervalo de sondeo (en segundos)**: intervalo de tiempo en el que el dispositivo SD-WAN envía los sondeos en los enlaces WAN configurados por Internet. De forma predeterminada, el dispositivo SD-WAN envía sondeos en los enlaces WAN configurados cada 5 segundos.

- **Reintentos**: Número de reintentos que puede intentar antes de determinar si el enlace WAN está activo o no. Tras 3 fallos de sonda consecutivos, el enlace WAN se considera inactivo. El máximo de reintentos permitido es de 10.




### Modos de implementación compatibles

El servicio de Internet se puede utilizar en los siguientes modos de implementación:

- Modo de implementación en línea (superposición SD-WAN)

Citrix SD-WAN se puede implementar como solución superpuesta en cualquier red. Como solución de superposición, la SD-WAN generalmente se implementa detrás de routers perimetrales o firewalls existentes. Si la SD-WAN se implementa detrás de un firewall de red, la interfaz se puede configurar como confiable y el tráfico de Internet se puede enviar al firewall como una puerta de enlace a Internet.

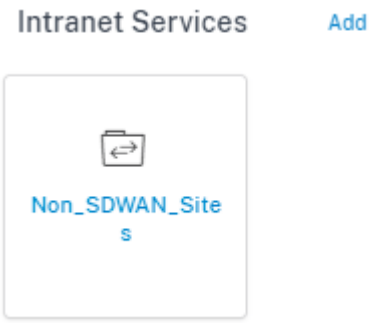
- Modo Edge o Gateway

Citrix SD-WAN se puede implementar como dispositivo perimetral, reemplazando los dispositivos de firewall o enrutador perimetral existentes. La función de firewall integrado permite que la SD-WAN proteja la red de la conectividad directa a Internet. En este modo, la interfaz conectada al vínculo público de Internet se configura como no confiable, lo que obliga a habilitar el cifrado, y las funciones de firewall y NAT dinámico están habilitadas para proteger la red.

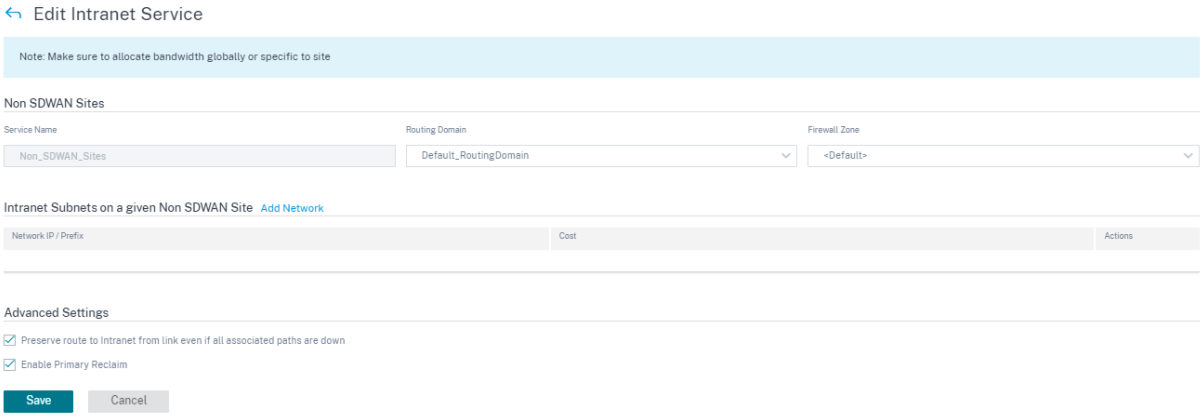
## Servicio de intranet

Puede crear varios servicios de intranet. Para agregar un servicio de Intranet, desde el nivel de cliente, vaya a **Configuración** > **Canales de entrega** > **Definiciones de servicios**. En la sección **Servicios de intranet**, haga clic en **Agregar**.




Una vez creado el servicio de Intranet en el nivel global, puede hacer referencia a él en el nivel de enlace WAN. Proporcione un **nombre de servicio**y seleccione el **dominio de enrutamiento** y la **zona de firewall**que quiera. Agregue todas las direcciones IP de la intranet a través de la red para que otros sitios de la red puedan interactuar. También puede conservar la ruta a la intranet desde el vínculo incluso si todas las rutas asociadas están incompletas.



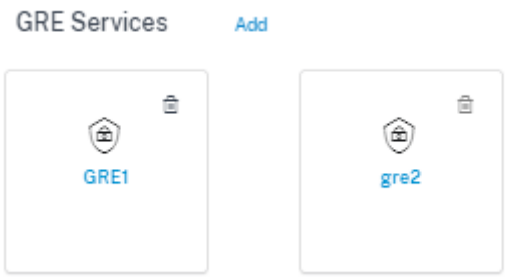

## Servicio GRE

Puede configurar los dispositivos SD-WAN para terminar túneles GRE en la LAN.

Para agregar un servicio GRE, desde el nivel de cliente, vaya a **Configuración** > **Canales de entrega** > **Definiciones de servicios**. También puede navegar a la página de configuración de **los servicios GRE** desde **Configuración > Seguridad**.

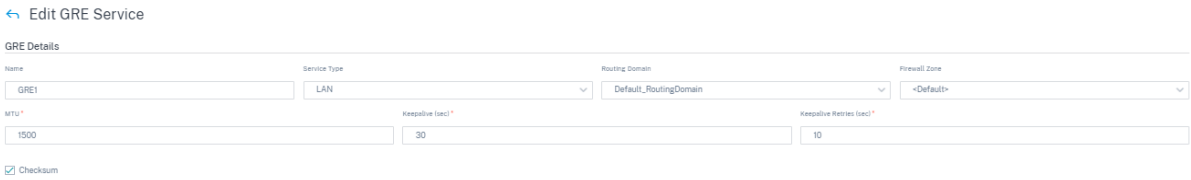
En la sección **IPSec y GRE**, vaya a **Servicios de IPSec** y haga clic en **Agregar**.




**Detalles del GRE**:

- **Tipo de servicio**: Seleccione el servicio que utiliza el túnel GRE.
- **Nombre**: Nombre del servicio GRE de LAN.
- **Dominio de redirección**: Dominio de redirección del túnel GRE.
- **Zona de firewall**: La zona de firewall elegida para el túnel. De forma predeterminada, el túnel se coloca en Default_LAN_ZONE.
- **MTU**: Unidad de transmisión máxima: El tamaño del datagrama IP más grande que se puede transferir a través de un enlace específico. El rango es de 576 a 1500. El valor predeterminado es 1500.
- **Mantener vivo**: El período transcurrido entre el envío de mensajes de mantenimiento activo. Si se configura en 0, no se envían paquetes de mantenimiento vivo, pero el túnel permanece activo.
- **Reintentos de Keep Alive**: Número de veces que el dispositivo Citrix SD-WAN envía paquetes de mantenimiento activo sin respuesta antes de que desconecte el túnel.
- **Checksum**: habilita o inhabilita Checksum para el encabezado GRE del túnel.

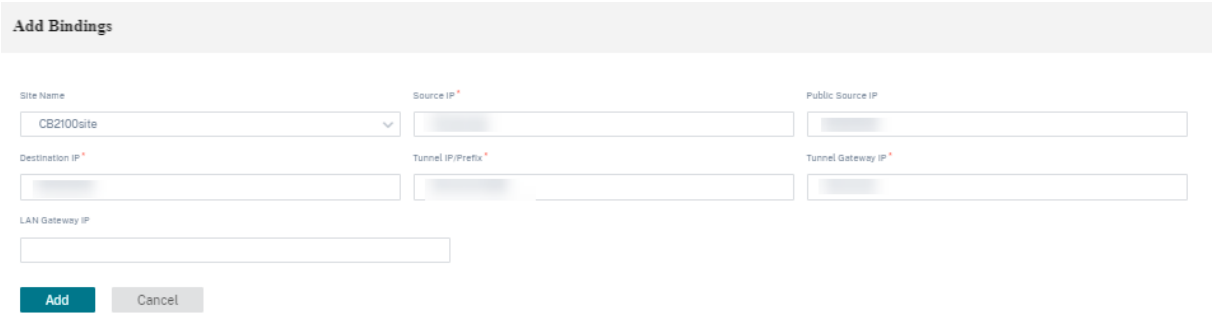



**Vinculaciones de sitios**:

- **Nombre del sitio**: El sitio para mapear el túnel GRE.
- **IP de origen**: La dirección IP de origen del túnel. Esta es una de las interfaces virtuales configuradas en este sitio. El dominio de redirección seleccionado determina las direcciones IP de origen disponibles.
- **IP de origen público**: La IP de origen si el tráfico del túnel pasa por NAT.
- **IP de destino**: La dirección IP de destino del túnel.
- **IP/prefijo del túnel**: La dirección IP y el prefijo del túnel GRE.
- **IP de puerta de enlace de túnel**: La dirección IP del siguiente salto para enrutar el tráfico del túnel.

- **IP de puerta de enlace LAN**: La dirección IP del siguiente salto para enrutar el tráfico LAN.




## Servicio IPsec

Los dispositivos Citrix SD-WAN pueden negociar túneles IPsec fijos con pares de terceros en el lado LAN o WAN. Puede definir los puntos finales del túnel y asignar los sitios a los puntos finales del túnel.

También puede seleccionar y aplicar un perfil de seguridad IPsec que defina el protocolo de seguridad y la configuración IPsec.

Para configurar la configuración de IPsec de ruta virtual:

- Habilite túneles IPsec de ruta virtual para todas las rutas virtuales en las que se requiera el cumplimiento de FIPS.
- Configure la autenticación de mensajes cambiando el modo IPsec a AH o ESP + Auth y utilice una función hash aprobada por FIPS. SHA1 es aceptado por FIPS, pero SHA256 es altamente recomendable.
- La vida útil de IPsec debe configurarse durante no más de 8 horas (28.800 segundos).

Citrix SD-WAN utiliza la versión 2 de IKE con claves previamente compartidas para negociar los túneles IPSec a través de la ruta virtual mediante la siguiente configuración:

- Grupo DH 19: ECP256 (curva elíptica de 256 bits) para negociación de claves
- Cifrado AES-CBC de 256 bits
- hash SHA256 para autenticación de mensajes
- hash SHA256 para la integridad del mensaje
- DH Group 2: MODP-1024 para un secreto directo perfecto

Para configurar el túnel IPSec para un tercero:

- Configure el grupo DH aprobado por FIPS. Los grupos 2 y 5 están permitidos bajo FIPS, sin embargo, se recomiendan encarecidamente los grupos 14 y superiores.
- Configure la función hash aprobada por FIPS. SHA1 es aceptado por FIPS, sin embargo SHA256 es altamente recomendable.

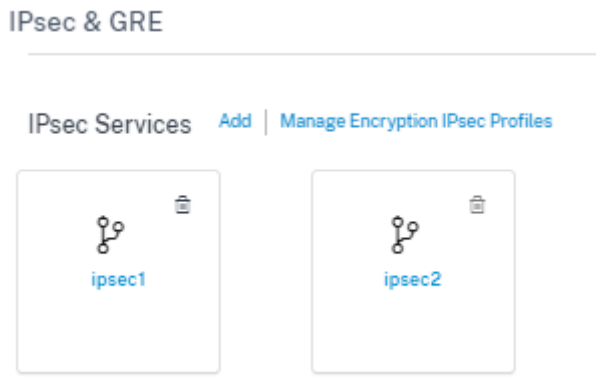
 

- Si utiliza IKEv2, configure una función de integridad aprobada por FIPS. SHA1 es aceptado por FIPS, sin embargo SHA256 es altamente recomendable.
- Configure una vida útil de IKE y una vida útil máxima de no más de 24 horas (86.400 segundos).
- Configure la autenticación de mensajes IPsec cambiando el modo IPsec a AH o ESP+Auth y utilice una función hash aprobada por FIPS. SHA1 es aceptado por FIPS, pero SHA256 es altamente recomendable.
- Configure una vida útil IPsec y una vida útil máxima de no más de ocho horas (28.800 segundos).

### Configuración de un túnel IPsec

Desde el nivel de cliente, vaya a **Configuración** > **Canales de entrega** > **Definiciones de servicios**. También puede ir a la página de **servicios de IPSec** desde **Configuración > Seguridad**.

En la sección **IPSec y GRE** > **Servicios IPSec**, haga clic en **Agregar**. Aparece la página **Modificar servicio IPSec**.




1. Especifique los detalles del servicio.
    - **Nombre del servicio**: Nombre del servicio IPsec.
    - **Tipo de servicio**: Seleccione el servicio que utiliza el túnel IPSec.
    - **Dominio de redirección**: Para túneles IPsec a través de LAN, seleccione un dominio de redirección. Si el túnel IPsec utiliza un servicio de Intranet, el servicio de Intranet determina el dominio de redirección.
    - **Zona de firewall**: La zona de firewall del túnel. De forma predeterminada, el túnel se coloca en Default_LAN_ZONE.
    - **Habilitar ECMP**: Cuando se selecciona la casilla **Habilitar ECMP**, se habilita el equilibrio de carga de ECMP para el túnel IPSec.
    - **Tipo de ECMP**: Seleccione el tipo de mecanismo de equilibrio de carga de ECMP según sea necesario. Para obtener más información sobre los tipos de ECMP, consulte Equilibrio de carga de ECMP.
2. Agregue el punto final del túnel.

- **Nombre**: Si el **tipo de servicio** es Intranet, elija un servicio de intranet que proteja el túnel. De lo contrario, introduzca un nombre para el servicio.
- **IP del mismo par**: Dirección IP del par remoto.
- Perfil**IPsec: Perfil**de seguridad IPsec que define el protocolo de seguridad y la configuración de IPsec.
- Clave**precompartida: L a clave**previamente compartida que se utiliza para la autenticación IKE.
- **Clave previamente compartida del mismo nivel: La clave**previamente compartida que se utiliza para la autenticación IKEv2.
- **Datos de identidad**: L os datos que se utilizarán como identidad local cuando se utilice la identidad manual o el tipo FQDN de usuario.
- **Datos de identidad**del mismo grupo: Los datos que se utilizarán como identidad de pares cuando se utilice identidad manual o tipo FQDN de usuario.
- **Certificado**: Si elige Certificado como autenticación IKE, elija uno de los certificados configurados.

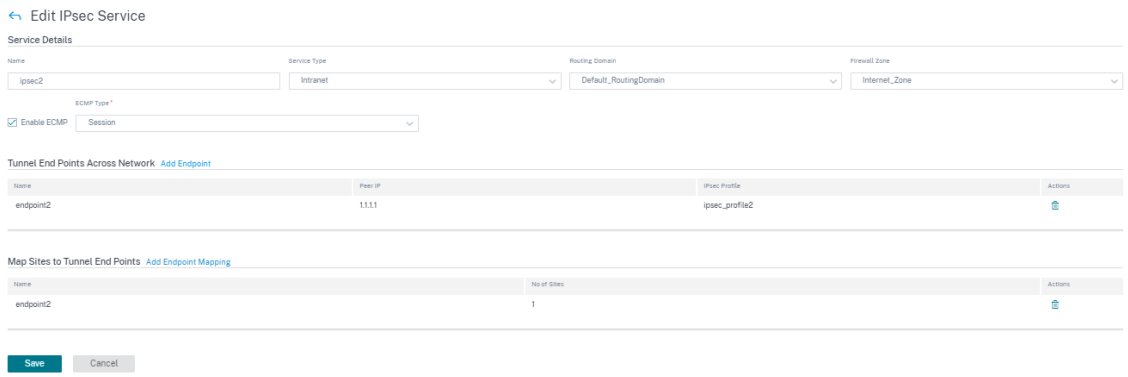
3. Asigne sitios a los puntos finales del túnel.

   - **Elija Endpoint**: El dispositivo de punto final que se va a asignar a un sitio.
   - **Nombre del sitio**: El sitio que se va a asignar al punto final.
   - **Nombre de la interfaz virtual**: La interfaz virtual del sitio que se va a utilizar como punto final.
   - **IP local**: Dirección IP virtual local que se va a utilizar como punto final del túnel local.
   - **IP de puerta**de enlace: La dirección IP del siguiente salto.

4. Cree la red protegida.

   - **IP/prefijo de la red**de origen: Dirección IP de origen y prefijo del tráfico de red que protege el túnel IPsec.
   - **IP/prefijo de red**de destino: Dirección IP de destino y prefijo del tráfico de red que protege el túnel IPsec.

5. Asegúrese de que las configuraciones IPsec estén reflejadas en el dispositivo del mismo nivel.



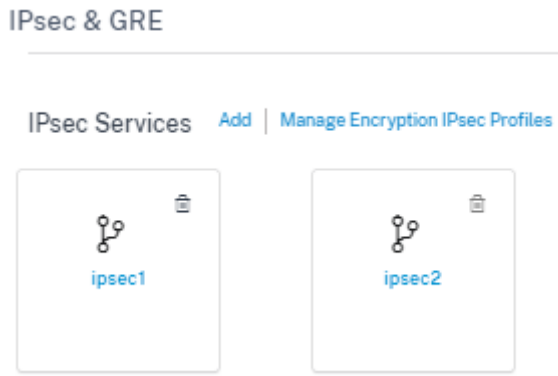
Para obtener más información sobre el cumplimiento de FIPS, consulte Seguridad de red.

> **Nota**
>
> Citrix SD-WAN Orchestrator for On-premises admite la conectividad a Oracle Cloud Infrastructure (OCI) a través de IPSec.

### Perfiles de cifrado IPSec

Para agregar un perfil de cifrado IPSec, al nivel de cliente, vaya a **Configuración** > **Canales de entrega** > **Definiciones de servicios**. También puede acceder a la página de configuración de **perfiles de cifrado de IPSec** desde **Configuración > Seguridad**.

En la sección **IPSec y GRE**, seleccione **Administrar perfiles IPSec de cifrado**.




IPsec proporciona túneles seguros. Citrix SD-WAN admite rutas virtuales IPsec, lo que permite que los dispositivos de terceros terminen túneles VPN IPsec en el lado LAN o WAN de un dispositivo Citrix SD-WAN. Puede proteger los túneles IPsec de sitio a sitio que terminan en un dispositivo SD-WAN mediante un binario criptográfico IPsec con certificación FIPS 140-2 de nivel 1.

Citrix SD-WAN también admite tunelización IPsec resistente mediante un mecanismo de túnel de ruta virtual diferenciado.

Los perfiles IPsec se utilizan al configurar los servicios IPsec como conjuntos de servicios de entrega. En la página del perfil de seguridad de IPSec, introduzca los valores necesarios para el siguiente **perfil de cifrado de IPSec, la configuración de IKE** y la **configuración de IPSec**.

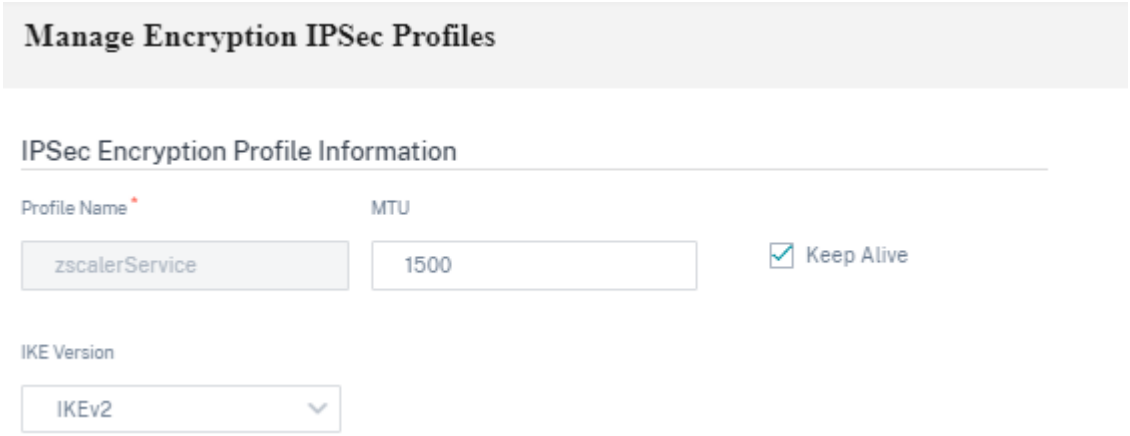
Haga clic en **Verificar configuración** para validar cualquier error de auditoría.

**Información del perfil de cifrado IPSec**:

- **Nombre de perfil**: Proporcione un nombre de perfil.
- **MTU**: Introduzca el tamaño máximo del paquete IKE o IPSec en bytes.
- **Keep Alive**: Active la casilla de verificación para mantener el túnel activo y habilitar la elegibilidad de la ruta.

- **Versión IKE**: Seleccione una versión del protocolo IKE de la lista desplegable.

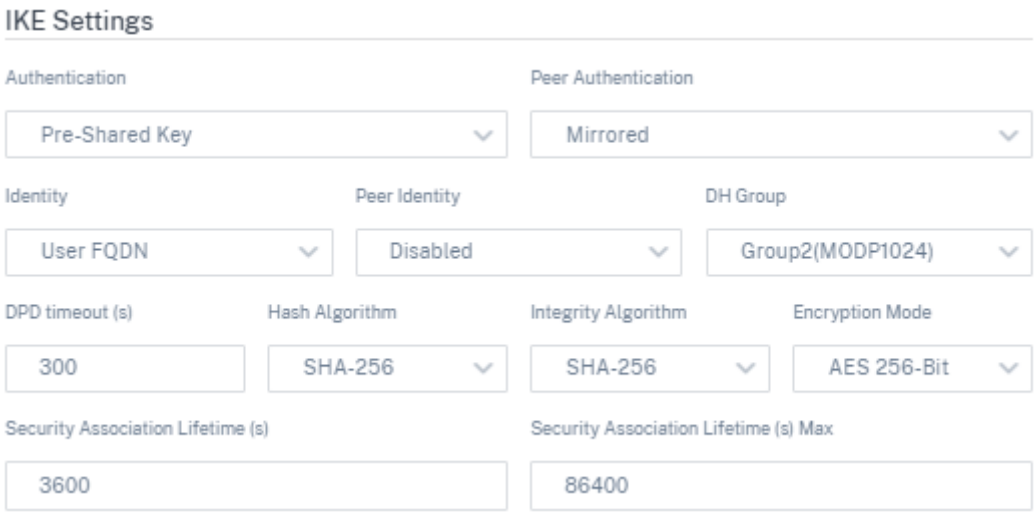



**Configuración IKE**

- **Modo**: Seleccione el modo principal o el modo agresivo en la lista desplegable del modo de negociación de la fase 1 de IKE.
  - **Principal**: No hay información expuesta a posibles atacantes durante la negociación, pero es más lenta que el modo Agresivo. **El modo principal** es compatible con FIPS.
  - **Agresivo**: Cierta información (por ejemplo, la identidad de los pares negociadores) está expuesta a posibles atacantes durante la negociación, pero es más rápida que el modo Principal. El modo**agresivo** no es compatible con FIPS.
- **Autenticación**: Elija el tipo de autenticación como certificado o clave precompartida en el menú desplegable.
- **Autenticación por**pares: Elija el tipo de autenticación de pares en la lista desplegable.
- **Identidad**: Seleccione el método de identidad en la lista desplegable.
- **Identidad de pares**: Seleccione el método de identidad del mismo nivel en la lista desplegable.
- **Grupo DH**: Seleccione el grupo Diffie-Hellman (DH) que está disponible para la generación de claves IKE.
- Tiempo de**espera de DPD**: introduzca el tiempo de espera de Dead Peer Detection (en segundos) para las conexiones VPN.
- **Algoritmo de hash**: Elija un algoritmo de hash de la lista desplegable para autenticar los mensajes IKE.
- **Algoritmo de integridad**: Elija el algoritmo de hash IKEv2 que se utilizará para la verificación de HMAC.
- **Modo de cifrado**: Elija el modo de cifrado para los mensajes IKE de la lista desplegable.
- **Duración (s) de la asociación de seguridad**: introduzca la cantidad de tiempo, en segundos, que debe transcurrir para que exista una asociación de seguridad IKE.

- **Duración máxima de la asociación de seguridad**: introduzca la cantidad máxima de tiempo, en segundos, para permitir que exista una asociación de seguridad IKE.

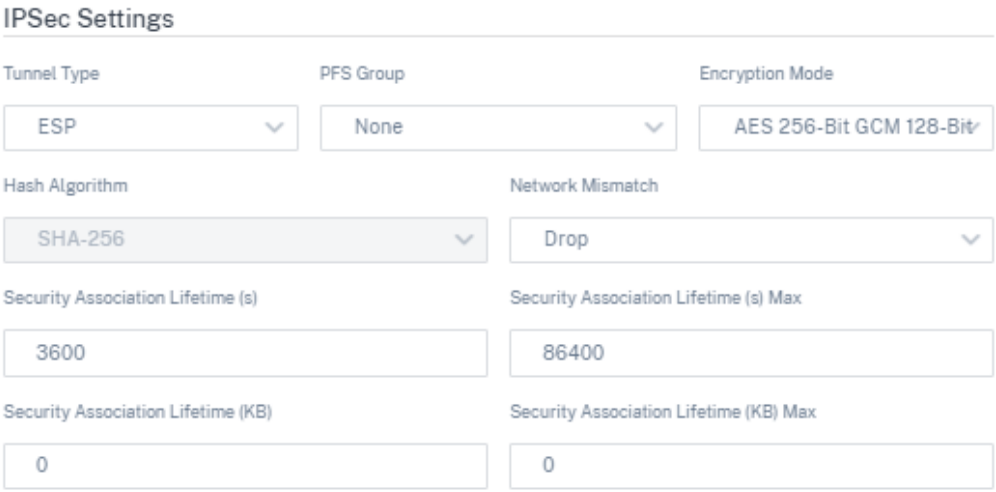



**Configuración de IPSec**

- **Tipo de túnel**: Elija **ESP**, **ESP+Auth**, **ESP+NULL**o **AH** como tipo de encapsulación de túnel en la lista desplegable. Estos se agrupan en categorías compatibles con FIPS y no conformes con FIPS.
  - **ESP**: Cifra solo los datos del usuario
  - **ESP+Auth**: Cifra los datos del usuario e incluye un HMAC
  - **ESP+NULL**: Los paquetes se autentican pero no se cifran
  - **AH**: Solo incluye un HMAC
- **Grupo PFS**: Elija el grupo Diffie-Hellman que quiere utilizar para generar claves secretas a la perfección en el menú desplegable.
- **Modo de cifrado**: Elija el modo de cifrado para los mensajes IPSec en el menú desplegable.
- **Algoritmo de hash: Los algoritmos**hash MD5, SHA1 y SHA-256 están disponibles para la verificación HMAC.
- **Discrepancia de red**: Elija la acción que quiera realizar si un paquete no coincide con las redes protegidas del túnel IPSec en el menú desplegable.
- **Duración (s) de la asociación de seguridad**: introduzca el tiempo (en segundos) que debe transcurrir para que exista una asociación de seguridad IPSec.
- **Duración máxima de la asociación de seguridad**: introduzca la cantidad máxima de tiempo (en segundos) para permitir que exista una asociación de seguridad IPSec.

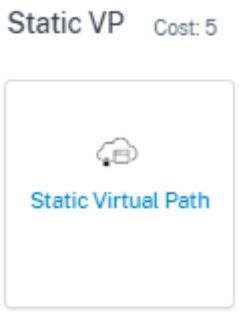
- **Duración de la asociación de seguridad (KB)**: introduzca la cantidad de datos (en kilobytes) para que exista una asociación de seguridad IPSec.
- **Duración máxima de la asociación de seguridad (KB)**: introduzca la cantidad máxima de datos (en kilobytes) para permitir que exista una asociación de seguridad IPSec.




### Ruta virtual estática

La configuración de ruta virtual se hereda de la configuración de ruta automática del vínculo wan global. Puede anular estas configuraciones y agregar o quitar la ruta de acceso del miembro. También puede filtrar las rutas virtuales según el sitio y el perfil QoS aplicado. Especifique una dirección IP de seguimiento para el enlace WAN que se puede hacer un pinging para determinar el estado del enlace WAN. También puede especificar una IP de seguimiento inverso para la ruta inversa que se puede hacer un pinging para determinar el estado de la ruta inversa.

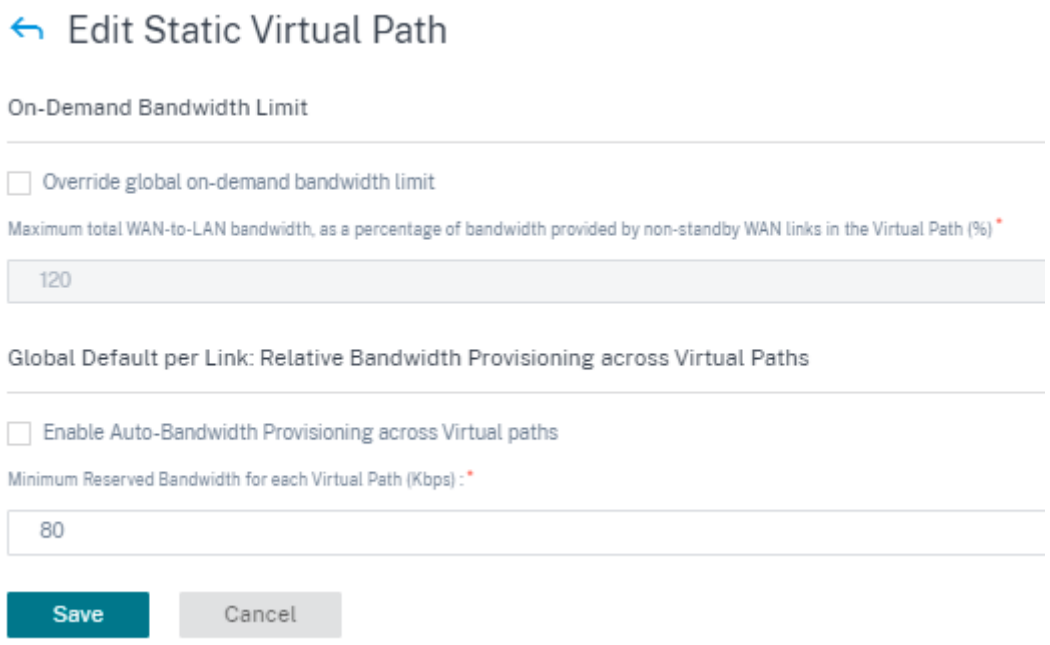
Para configurar rutas virtuales estáticas, desde el nivel de cliente, vaya a **Configuración** > **Canales de entrega**y haga clic en el icono **Ruta virtual estática**.




Las siguientes son algunas de las configuraciones admitidas:

- **Lista de ancho de banda bajo demanda**
  - **Anular el límite global de ancho de banda bajo demanda**: Cuando está habilitado, los valores límite de ancho de banda global se sustituyen por valores específicos del sitio.
  - Ancho de**banda máximo total de WAN a LAN, como porcentaje del ancho de banda proporcionado por los enlaces WAN que no están en espera en la ruta virtual (%)**: Actualice el límite máximo de ancho de banda, en%.
- **Valor predeterminado global por enlace: Provisioning de ancho de banda relativo en rutas virtuales**:
  - **Habilite el Provisioning automático del ancho de banda en las rutas virtuales**: Cuando está habilitado, el ancho de banda de todos los servicios se calcula y aplica automáticamente de acuerdo con la magnitud del ancho de banda consumido por los sitios remotos.
  - Ancho de**banda mínimo reservado para cada ruta virtual (Kbps)**: El ancho de banda máximo que se debe reservar exclusivamente para cada servicio en cada enlace WAN.




## Configuración de ruta virtual dinámica

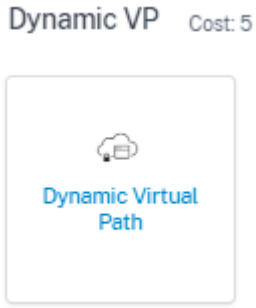
La configuración global de rutas virtuales dinámicas permite a los administradores configurar los valores predeterminados de la ruta virtual dinámica en toda la red.

Una ruta virtual dinámica se crea una instancia dinámica entre dos sitios para permitir la comunicación directa, sin saltos intermedios de nodo SD-WAN. Del mismo modo, la conexión de ruta virtual dinámica también se elimina dinámicamente. Tanto la creación como la eliminación de rutas

virtuales dinámicas se activan en función de los umbrales de ancho de banda y la configuración de tiempo.

Para configurar rutas virtuales dinámicas, desde el nivel de cliente, vaya a **Configuración** > **Canales de entrega** > **Definiciones de servicios**y haga clic en el icono **Ruta virtual dinámica**.




Las siguientes son algunas de las configuraciones admitidas:

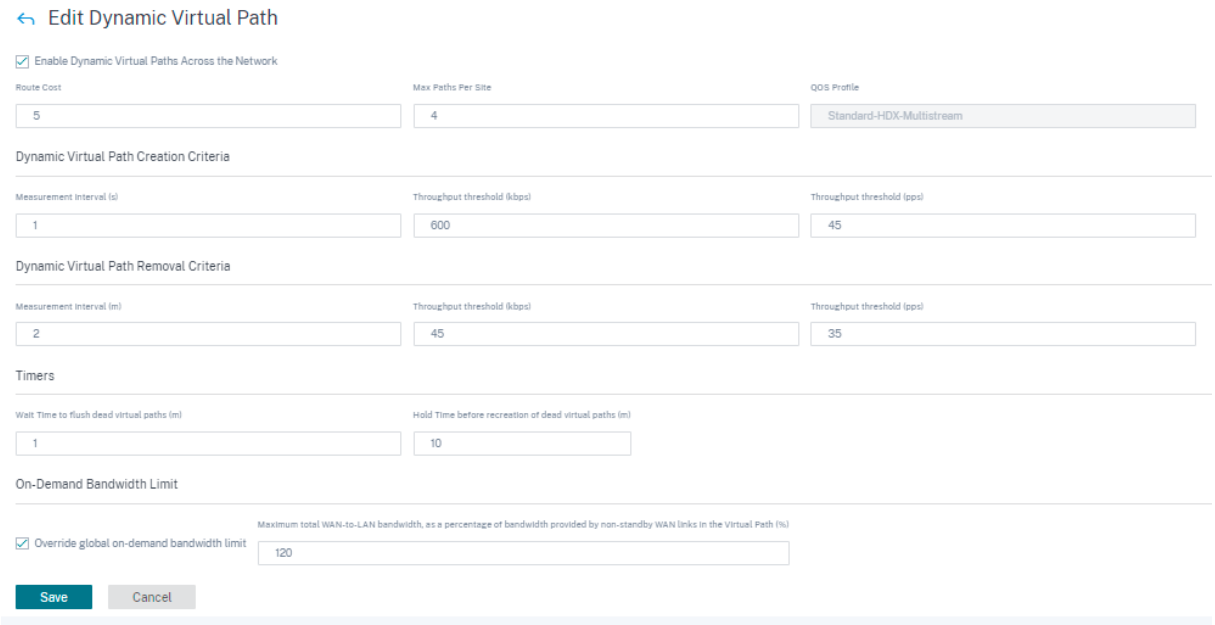
- Aprovisionamiento para habilitar o inhabilitar rutas virtuales dinámicas en toda la red
- El coste de ruta para rutas virtuales dinámicas
- El perfil de QoS que se va a utilizar es **estándar** de forma predeterminada.
- Criterios de creación de rutas virtuales dinámicas:
  - **Intervalo de medición (segundos)**: Cantidad de tiempo durante el cual se miden el recuento de paquetes y el ancho de banda para determinar si la ruta virtual dinámica debe crearse entre dos sitios, en este caso, entre una rama determinada y el nodo de control.
  - **Umbral de rendimiento (kbps)**: Umbral del rendimiento total entre dos sitios, medido durante el **intervalo de medición**, en el que se activa la ruta virtual dinámica. En este caso, el umbral se aplica al nodo de control.
  - **Umbral de rendimiento (pps)**: Umbral del rendimiento total entre dos sitios, medido durante el **intervalo de medición**, en el que se activa la ruta virtual dinámica.
- Criterios de eliminación de rutas virtuales dinámicas:
  - **Intervalo de medición (minutos)**: Cantidad de tiempo durante el cual se miden el recuento de paquetes y el ancho de banda para determinar si se debe eliminar una ruta virtual dinámica entre dos sitios, en este caso, entre una sucursal determinada y el nodo de control.
  - **Umbral de rendimiento (kbps)**: Umbral del rendimiento total entre dos sitios, medido durante el **intervalo de medición**, en el que se elimina la ruta virtual dinámica.
  - **Umbral de rendimiento (pps)**: Umbral del rendimiento total entre dos sitios, medido durante el **intervalo de medición**, en el que se elimina la ruta virtual dinámica.
- Temporizadores

  - **Tiempo de espera para vaciar las rutas virtuales muertas (m)**: Tiempo después del cual se elimina una ruta virtual dinámica MUERTA.
  - **Tiempo de espera antes de la recreación de rutas virtuales muertas (m)**: Tiempo después del cual se puede recrear una ruta virtual dinámica eliminada por estar MUERTA.

- Lista de ancho de banda

  - **Anular el límite global de ancho de banda bajo demanda**: Cuando está habilitado, los valores límite de ancho de banda global se sustituyen por valores específicos del sitio.
  - Ancho de**banda máximo total de WAN a LAN, como porcentaje del ancho de banda proporcionado por los enlaces WAN que no están en espera en la ruta virtual (%)**: Actualice el límite máximo de ancho de banda, en%.




Haga clic en **Verificar configuración** para validar cualquier error de auditoría.

## Redirección

October 31, 2022

La sección **Enrutamiento** ofrece las siguientes opciones:

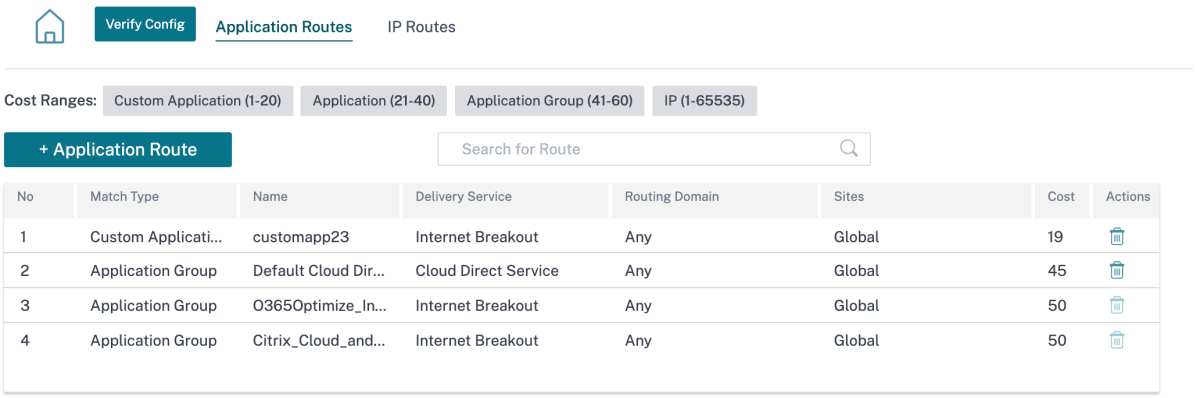
- Directivas de redirección
- Resumen de rutas
- Dominios de redirección
- Importar perfiles de ruta

- Exportar perfiles de ruta
- Nodos de tránsito

### Directivas de enrutamiento

Las directivas de enrutamiento ayudan a habilitar la dirección del tráfico. En función de la selección (Rutas de aplicación y rutas IP), puede utilizar diferentes formas de dirigir el tráfico.

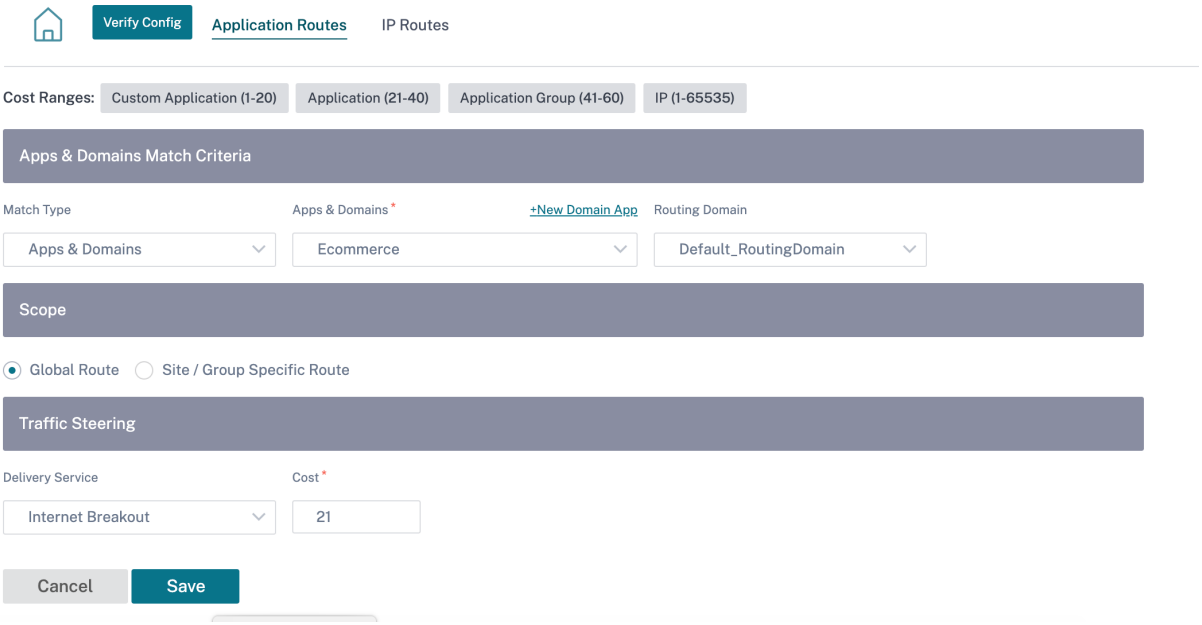



#### Rutas de aplicación

Haga clic en **+ Ruta de aplicación** para crear una ruta de aplicación.

- **Criterios de coincidencia de aplicaciones personalizados**
  - **Tipo de coincidencia**: Seleccione el tipo de coincidencia como **Aplicación/Aplicación personalizada/Grupo** de aplicaciones en la lista desplegable.
  - **Aplicación**: Seleccione una aplicación de la lista.
  - **Dominio de enrutamiento**: Seleccione un dominio de enrutamiento.
- **Alcance**: Puede definir el alcance de la ruta de la aplicación a nivel global o a nivel específico del sitio y el grupo.
- **Dirección de tráfico**;
  - **Servicio de entrega**: Elija un servicio de entrega de la lista.
  - **Coste**: Refleja la prioridad relativa de cada ruta. Reduzca el coste, mayor será la prioridad.
- **Elegibilidad basada en la ruta**:
  - **Agregar ruta**: Elija un sitio y enlaces WAN. Si la ruta elegida desaparece, entonces la ruta de la aplicación no recibe ningún tráfico.



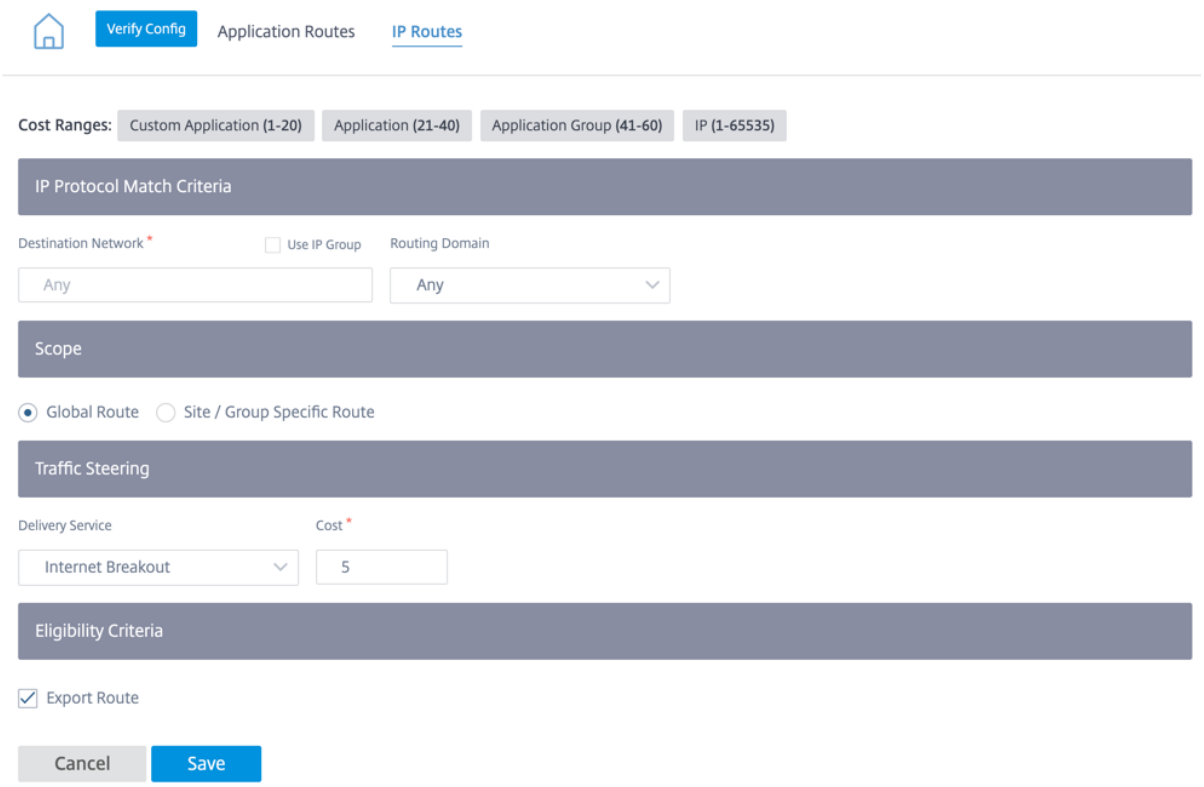

Si se agrega una nueva ruta de aplicación, el coste de la ruta debe estar en el rango siguiente:

- **Aplicación personalizada**: 1—20
- **Aplicación**: 21-40
- **Grupo de aplicaciones**: 41—60

### Rutas IP

Vaya a la ficha **Rutas IP** y haga clic en **+ Directiva de ruta IP** a ruta IP para dirigir el tráfico.




- **Criterios de coincidencia del protocolo IP**
  - **Red de destino**: Agregue la red de destino que ayuda a reenviar los paquetes.
  - **Usar grupo IP**: Puede agregar una red de destino o activar la casilla **Usar grupo IP** para seleccionar cualquier grupo de IP de la lista desplegable.
  - **Dominio de enrutamiento**: Seleccione un dominio de enrutamiento de la lista desplegable.
- **Alcance**: Puede definir el alcance de la ruta IP a nivel global o a nivel específico de sitio y grupo.
- **Dirección de tráfico**:
  - **Servicio de entrega**: Elija un servicio de entrega de la lista desplegable.
  - **Coste**: Refleja la prioridad relativa de cada ruta. Reduzca el coste, mayor será la prioridad.

  Si se agrega una nueva ruta IP, el coste de la ruta debe estar entre 1 y 20.
- **Criterios de elegibilidad**
  - **Exportar ruta**: Si se selecciona la casilla **Exportar** ruta y la ruta es una ruta local, la ruta se puede exportar de forma predeterminada. Si la ruta es una ruta basada en INTRANET/INTERNET, para que la exportación funcione, el reenvío WAN a WAN debe estar habilitado. Si la casilla **Exportar ruta** está desactivada, la ruta local no es apta para exportarse a otra SD-WAN y tiene importancia local.

- **Elegibilidad basada en la ruta**:
  - **Agregar ruta**: Elija un sitio y enlaces WAN. Si la ruta agregada desaparece, entonces la ruta IP no recibe ningún tráfico.

Haga clic en **Verificar configuración** para validar cualquier error de auditoría.

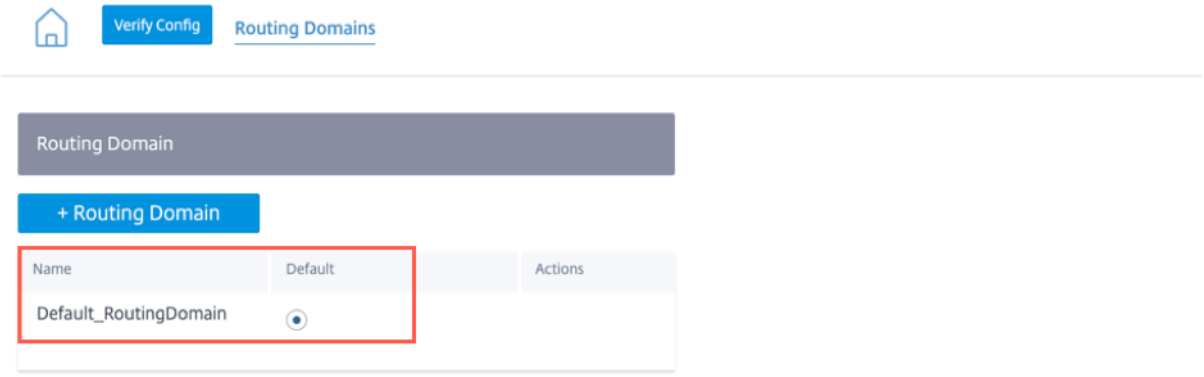
### Resumen de rutas

El resumen de rutas reduce el número de rutas que debe mantener un enrutador. Una ruta de resumen es una única ruta que se utiliza para representar varias rutas. Ahorra ancho de banda mediante el envío de un solo anuncio de ruta, lo que reduce el número de enlaces entre routers. Ahorra memoria porque solo se mantiene una dirección de ruta. Los recursos de CPU se utilizan de manera más eficiente evitando búsquedas recursivas. Puede agregar rutas resumidas sin especificar la dirección IP de la puerta de enlace.

### Dominios de redirección

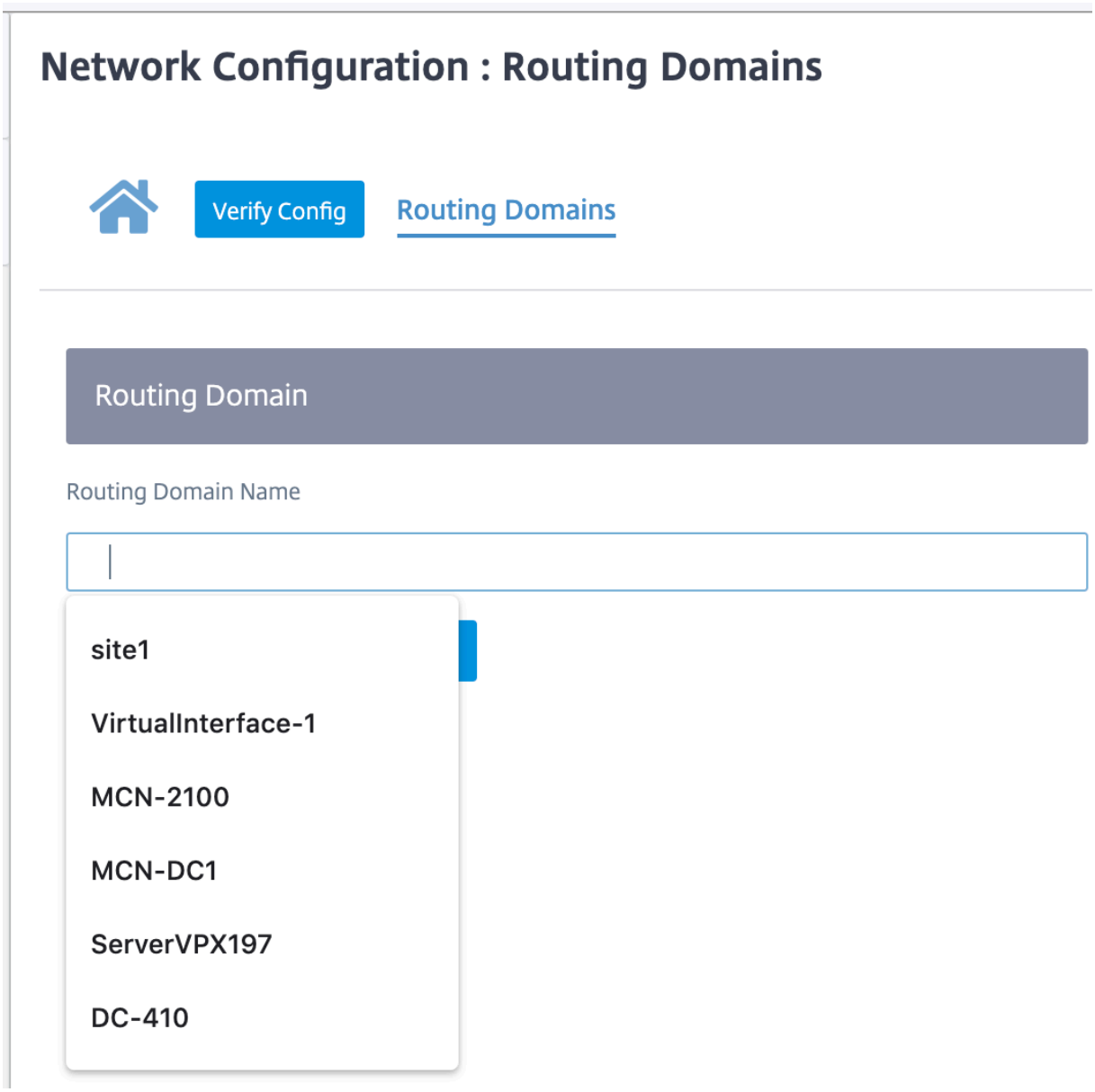
Los**dominios de enrutamiento** se utilizan para segregar el tráfico a través de VLAN Una vez creados los dominios de enrutamiento, puede hacer referencia a ellos a nivel global (para los servicios de intranet) o al nivel de interfaz.

También puede seleccionar el dominio de enrutamiento predeterminado que se aplica a todos los sitios.




Para hacer coincidir las rutas de un dominio de enrutamiento específico, haga clic en **+ Dominio de enrutamiento** y elija uno de los dominios de enrutamiento configurados en la lista desplegable. Haga clic en **Guardar**.




Haga clic en **Verificar configuración** para validar cualquier error de auditoría.

Para obtener más información, consulte Dominio de enrutamiento.

#### Servicio de dominio de interredirección

Citrix SD-WAN Orchestrator for On-premises proporciona un servicio de dominio de interen- rutamiento estático, que permite la filtración de rutas entre los dominios de enrutamiento dentro de un sitio o entre diferentes sitios. Esto elimina la necesidad de un enrutador perimetral para manejar las fugas de ruta. El servicio de enrutamiento entre VRF también se puede utilizar para configurar rutas, directivas de firewall y reglas NAT.

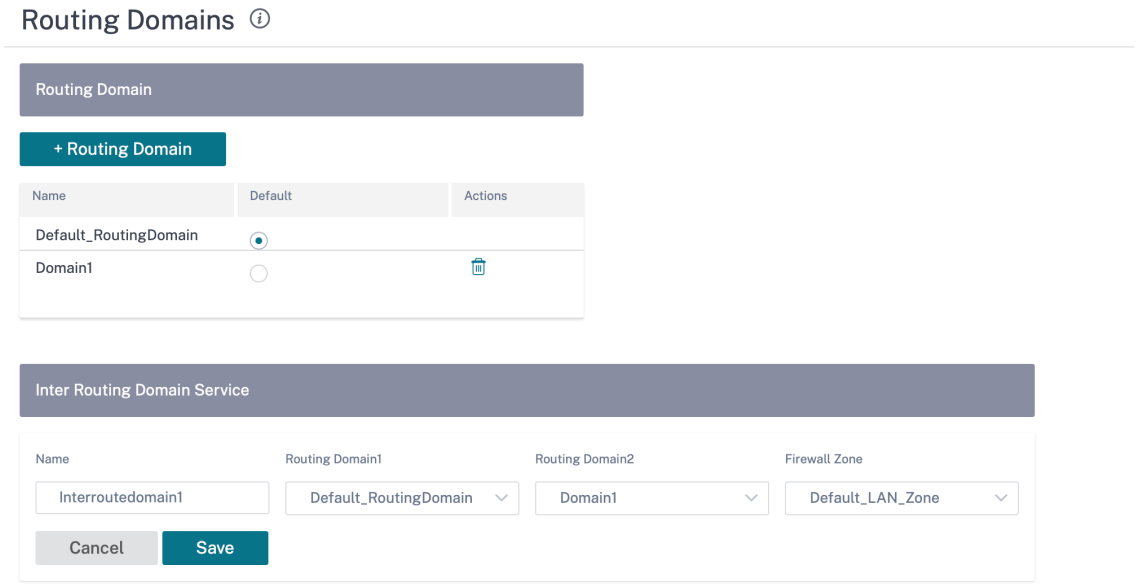
 

Para obtener más información, consulte Servicio de dominios entre rutas.

Para configurar el servicio de dominios de enrutamiento entre rutas a través del Citrix SD-WAN Orchestrator for On-premises:

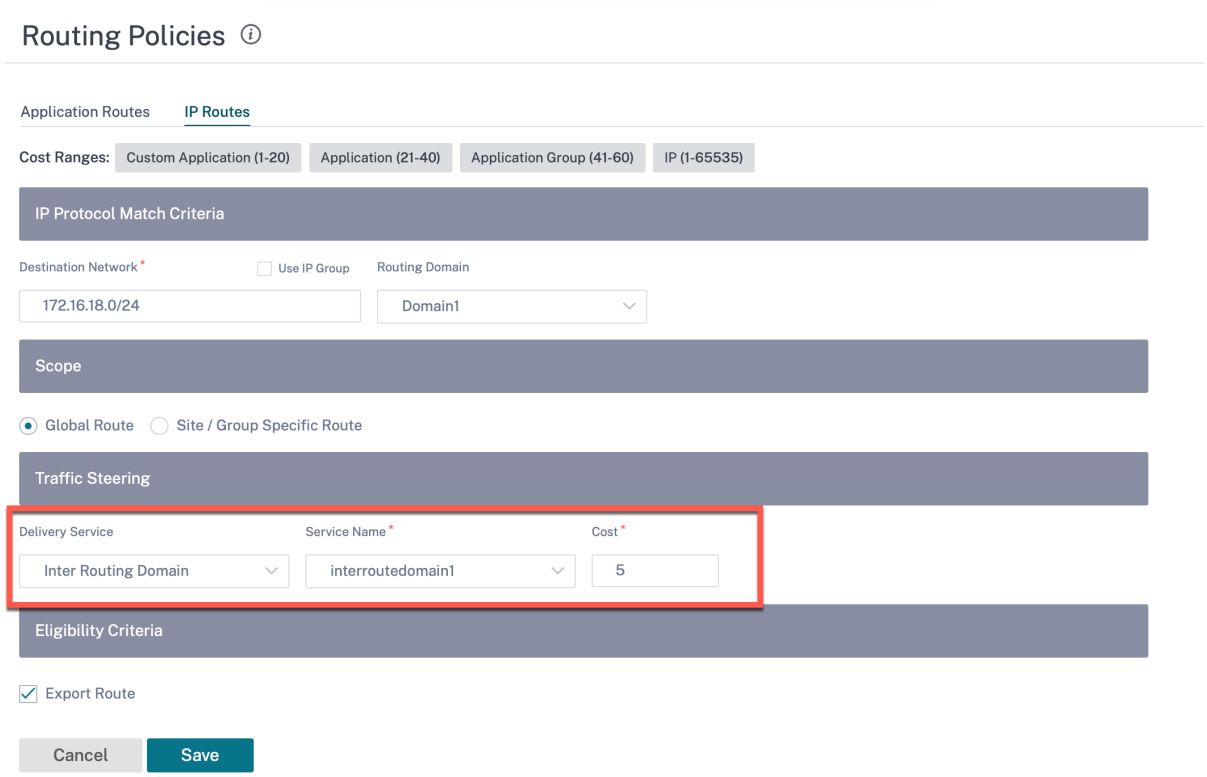
1. A nivel de red, vaya a **Configuración** > **Enrutamiento** > **Dominios de enrutamiento > Servicio de dominiosentre enrutamientos**.
2. Haga clic en **+ Dominio de interenrutamiento** e introduzca valores para los siguientes parámetros:

- **Nombre**: El nombre del servicio de dominio de interredirección.
- **Dominio de redirección 1**: E l primer dominio de redirección del par.
- **Dominio de redirección 2**: El segundo dominio de redirección del par.
- **Zona de firewall**: La zona de firewall del servicio.
  - **Predeterminado**: Se asigna la **zona de firewall Inter_Routing_Domain_Zone**.
  - **Ninguno**: E l servicio se comporta como un conducto, que no tiene zona y mantiene la zona original del paquete.
  - Es posible que se seleccionen todas las zonas configuradas en la red.




Para crear rutas mediante el servicio de dominio entre enrutamiento, cree una ruta con el tipo de servicio como Servicio de dominio entre enrutamiento y seleccione el servicio de dominio entre enrutamiento. Para obtener más información sobre la configuración de rutas, consulte Directivas de enrutamiento.

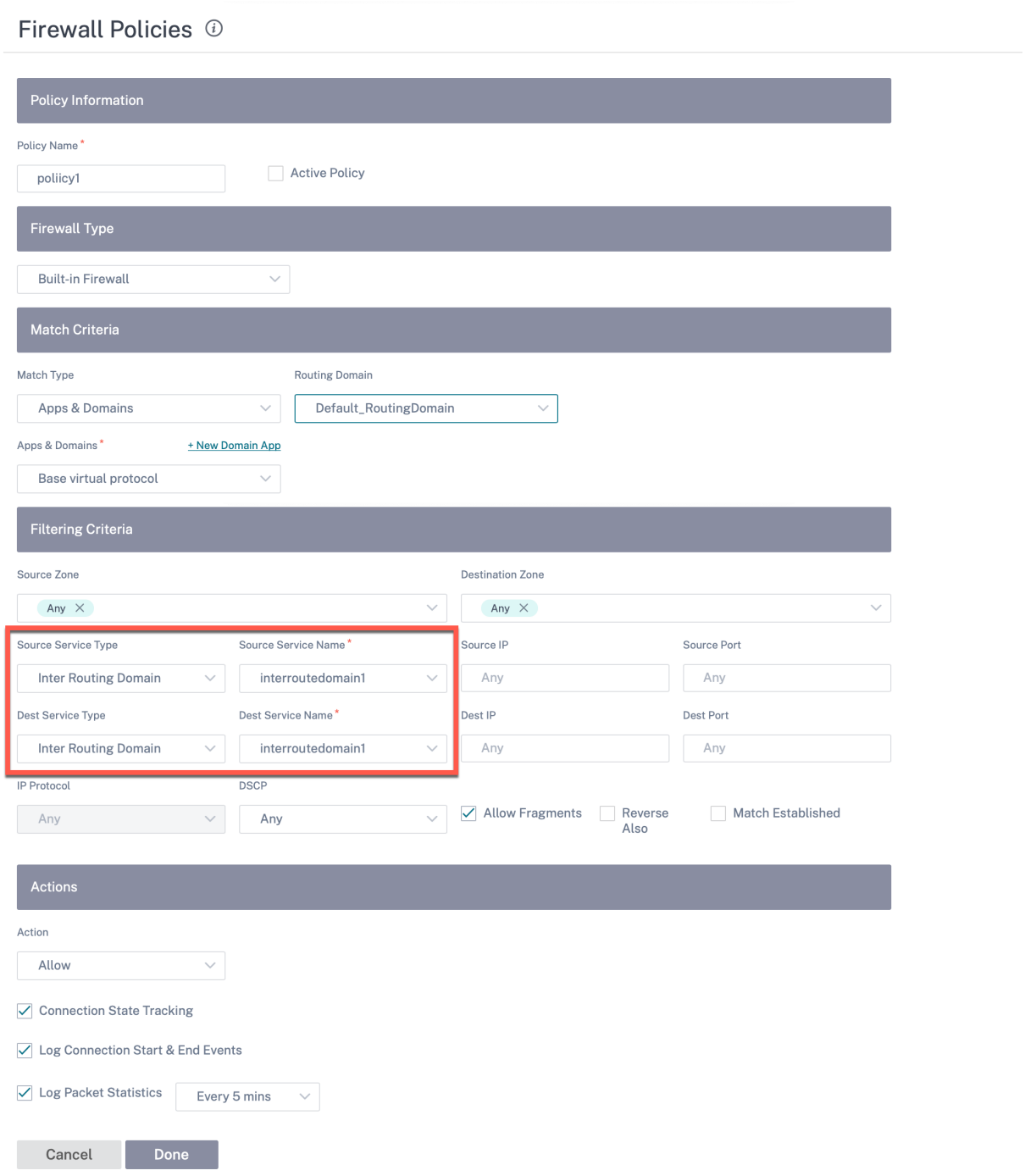
 




Agregue también una ruta del otro par Dominio de redirección, para establecer la conexión entre ambos dominios de redirección.

También puede configurar directivas de firewall para controlar el flujo de tráfico entre dominios de redirección. En las directivas de firewall, seleccione Servicio de dominio de interredirección para los servicios de origen y destino y seleccione la acción de firewall necesaria. Para obtener información sobre cómo configurar las directivas de firewall, consulte Directivas de firewall.



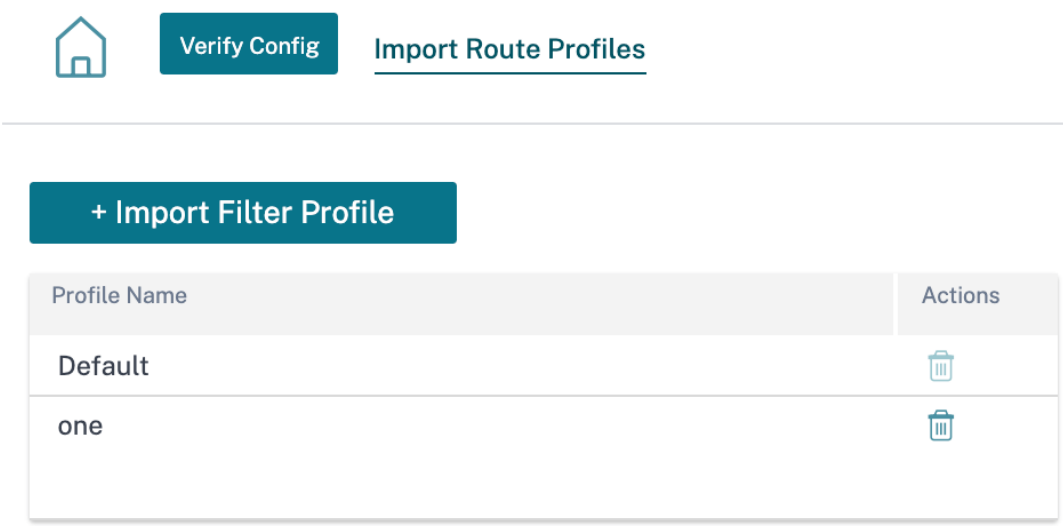

También puede elegir el tipo de servicio Intranet para configurar directivas NAT estáticas y dinámicas. Para obtener más información sobre la configuración de las directivas NAT, consulte Traducción de direcciones de red

### Importar perfiles de ruta

Puede configurar Filtros para ajustar la forma en que se lleva a cabo el aprendizaje de rutas.

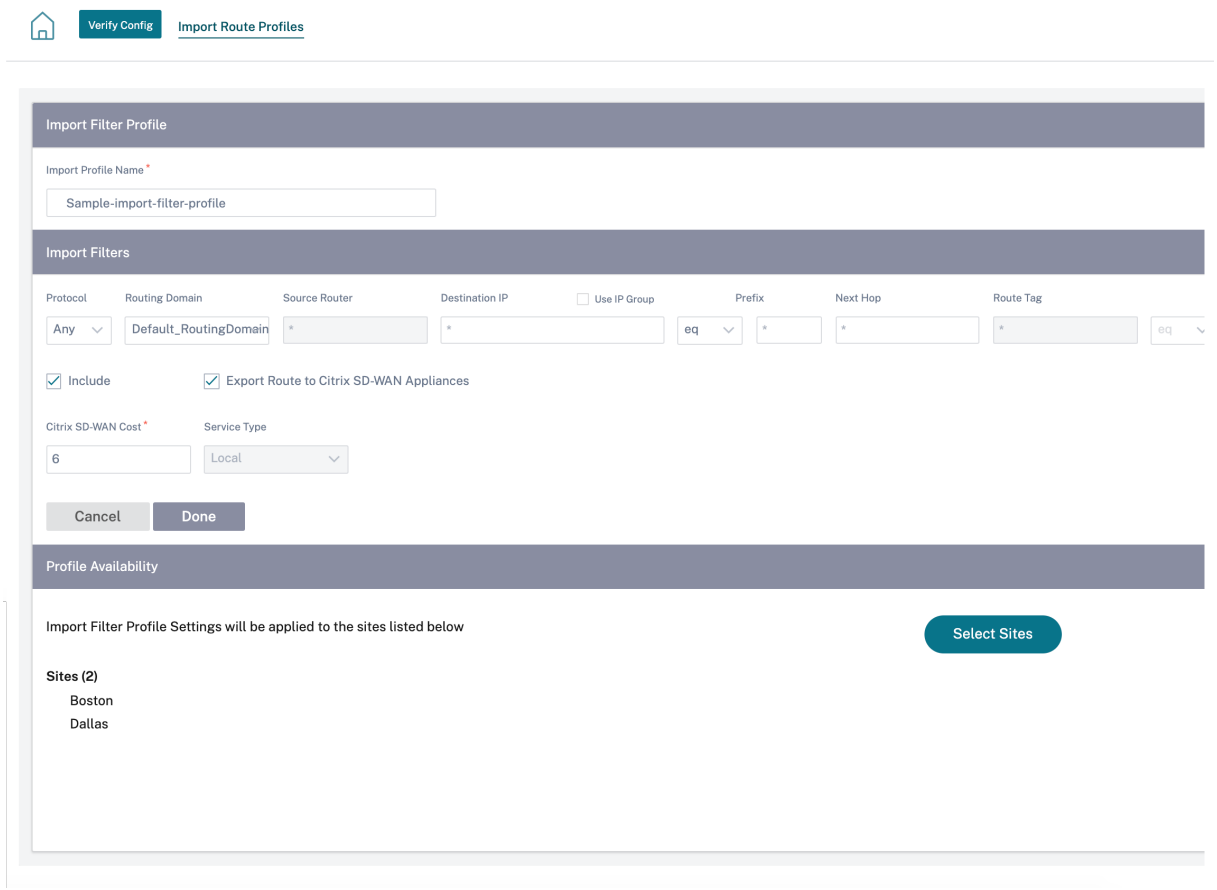
Las reglas de filtro de importación son reglas que deben cumplirse antes de importar rutas dinámicas a la base de datos de rutas SD-WAN. De forma predeterminada, no se importan rutas.




Agregue un **perfil de filtro de importación** con el **nombre del perfil de importación, la disponibilidad del perfil y**los filtros de importación**,** junto con los siguientes campos:

- **Protocolo**: Seleccione el protocolo de la lista.
- **Dominio de enrutamiento**: Para hacer coincidir las rutas de un dominio de enrutamiento específico, elija uno de los dominios de enrutamiento configurados de la lista.
- **Enrutador de origen**: Introduzca la dirección IP y la máscara de red del objeto de red configurado que describe la red de la ruta.
- **IP de destino**: Introduzca la dirección IP de destino.
- **Prefijo**: Para hacer coincidir las rutas por prefijo, elija un predicado de coincidencia de la lista e introduzca un prefijo de ruta en el campo adyacente.
- **Próximo salto**: Introduzca el destino del siguiente salto.
- **Etiqueta de ruta**: Rellena la etiqueta de ruta.
- **Coste**: El método (predicado) y el coste de la ruta SD-WAN que se utilizan para restringir la selección de rutas exportadas.

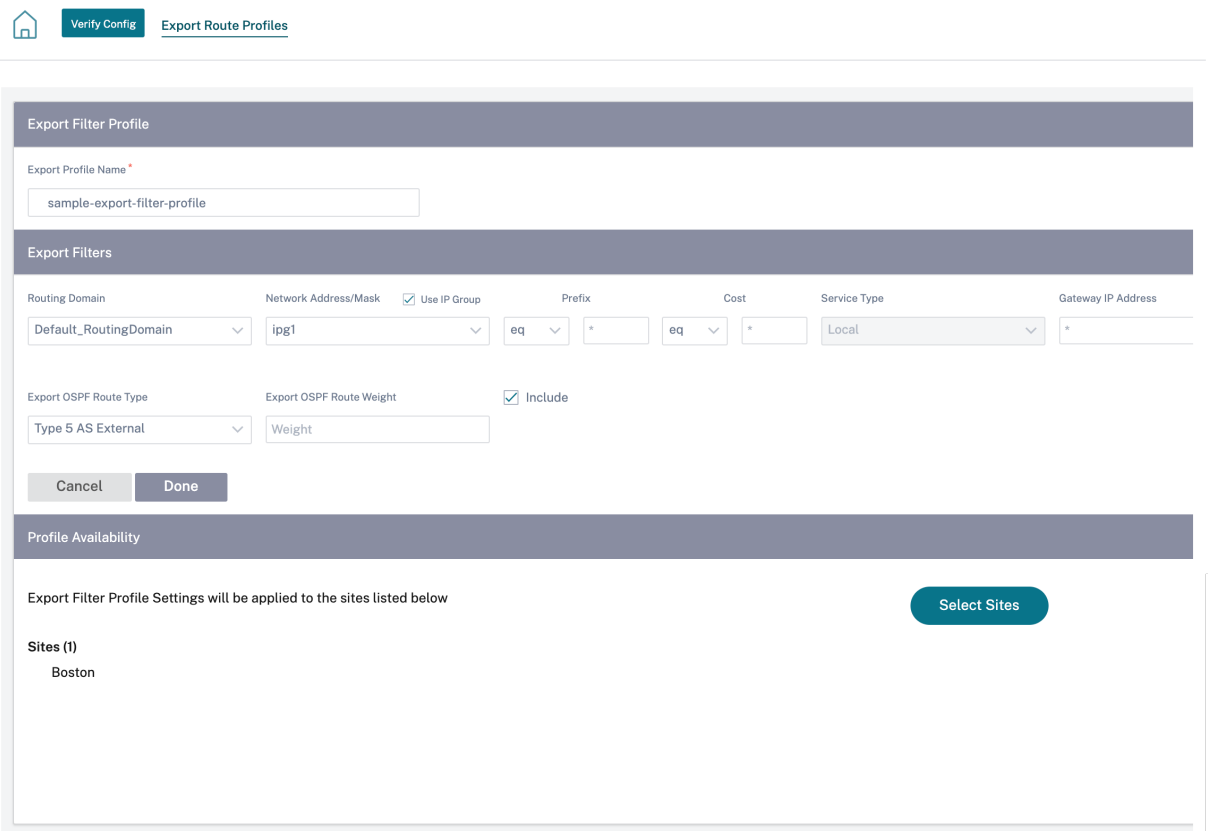



Haga clic en **Verificar configuración** para validar cualquier error de auditoría.

## Exportar perfiles de ruta

Defina las reglas que deben cumplir al anunciar rutas SD-WAN a través de protocolos de redirección dinámica. De forma predeterminada, todas las rutas se anuncian a los pares.




Haga clic en **Verificar configuración** para validar cualquier error de auditoría.

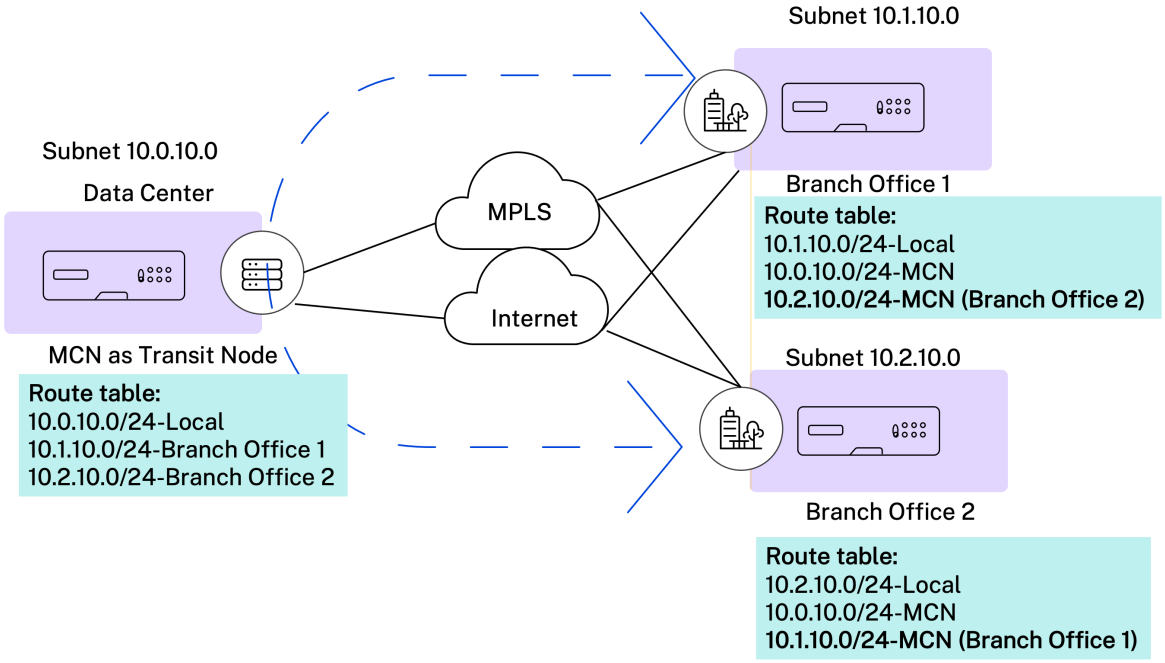
## Nodos de tránsito

### Nodo de tránsito virtual superpuesto

Los nodos de tránsito son los sitios que pueden reenviar tráfico entre una o más sucursales dentro de una región.

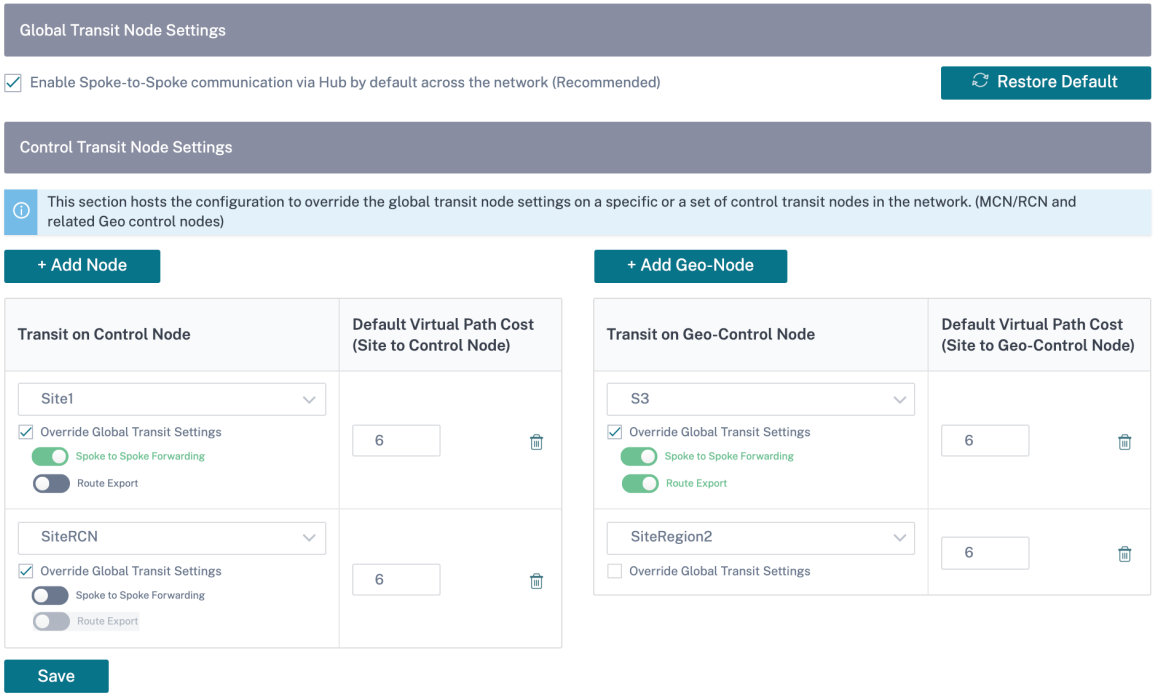
Se puede influir en el tráfico entre dos nodos para que elija el nodo de tránsito como salto intermedio ajustando el coste de la ruta. Los nodos de tránsito se utilizan para enrutar datos a nodos no adyacentes. Por ejemplo, si hay tres nodos conectados en la serie A-B-C, los datos de A a C se pueden enrutar a través de B. Puede especificar el nodo de tránsito y los sitios que se enrutarán a través del nodo de tránsito en el servicio Citrix SD-WAN Orchestrator. Las rutas virtuales se eligen en orden ascendente de coste. Disminuya el coste, mayor sea la prioridad.




**Nodos de tránsito de superposición virtual global predeterminados** Puede especificar los nodos de control (MCN/RCN) y los nodos de control geográfico (Geo-MCN/RCN) para que actúen como nodos de tránsito superpuestos virtuales globales predeterminados en una red. Al habilitar la comunicación de voz y radio a través de Hub como parte de la configuración global, todos los sitios pueden utilizar los nodos de control configurados como nodos de tránsito, de forma predeterminada, para la comunicación de sitio a sitio.




Agregue el nodo de control y los nodos de control geográfico que quiera utilizar como nodos de tránsito de superposición virtual y especifique el coste de la ruta virtual. Los nodos de control y los nodos de control geográfico tienen 6 y 7 como los costes de ruta virtual predeterminados respectivos. Puede optar por cambiar el coste de la ruta virtual según los requisitos de su red. Haga clic en **Restaurar valores predeterminados** para restablecer los costes de las rutas virtuales predeterminadas para los nodos de tránsito predeterminados.

> **Nota**
>
> Puede agregar un máximo de 3 nodos de control y 3 nodos de control geográfico como nodos de tránsito.

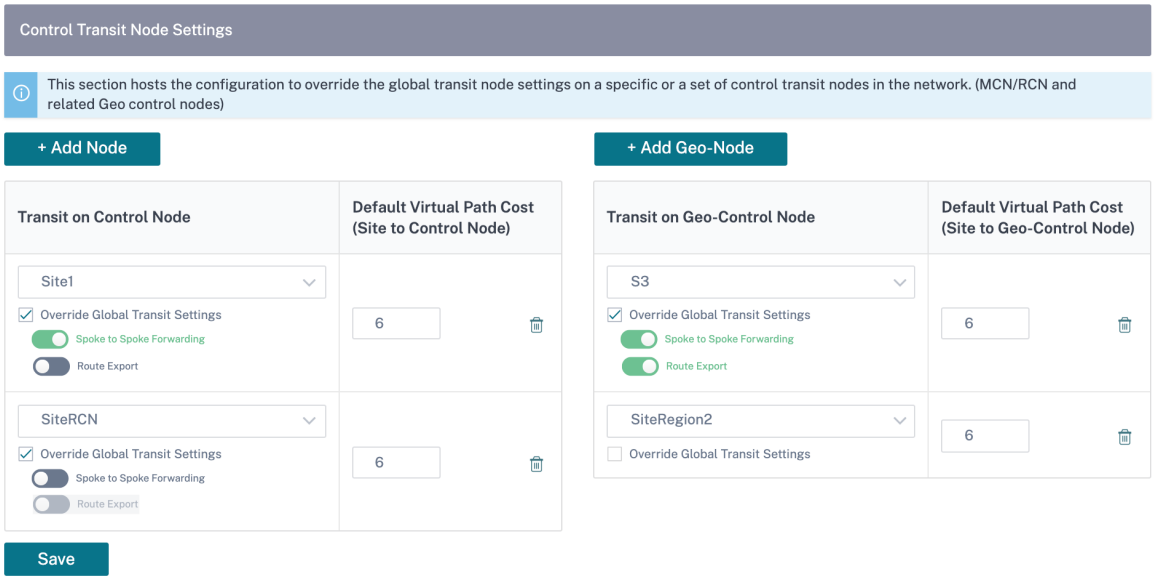
De forma predeterminada, el reenvío WAN a WAN está habilitado en todas las rutas asociadas con los nodos de control y control geográfico seleccionados. El reenvío WAN a WAN permite que un sitio actúe como un salto intermedio entre dos sitios adyacentes para cualquier tráfico de sitio a sitio, Internet o intranet y actuar como mediador para rutas virtuales dinámicas.

Puede anular la configuración del nodo de tránsito global y elegir habilitar o inhabilitar el reenvío de radio a radio solo en los nodos de control de tránsito seleccionados. Cuando la transferencia de **radio a radio está** habilitada, el nodo de control de tránsito exporta las rutas a través de los sitios conectados a él. Solo se habilitan la comunicación de sitio a sitio y la ruta virtual dinámica entre los sitios conectados al nodo de tránsito.

Al habilitar la **exportación de rutas**, se permite el reenvío virtual de rutas a rutas virtuales y la exportación de rutas (reenvío de WAN a WAN) en todas las rutas del sitio. Al inhabilitar el botón de con-

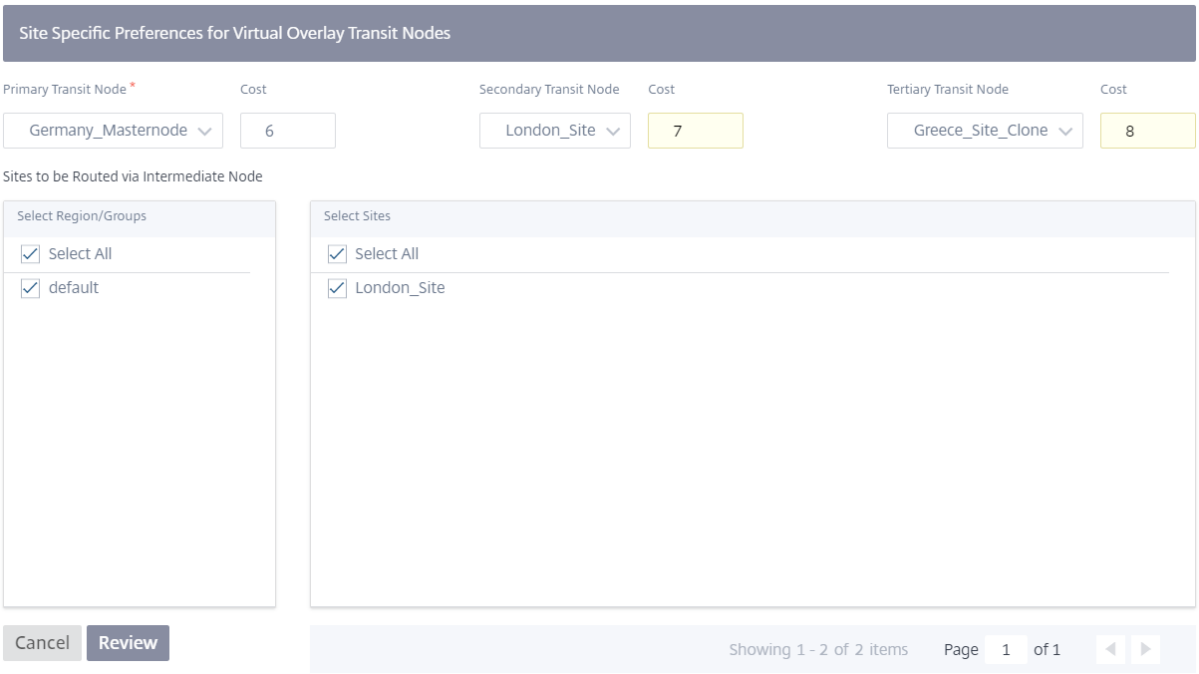
 

mutación, solo se permite el reenvío de rutas virtuales a rutas virtuales y se inhabilita la exportación de rutas en todas las rutas del sitio. La exportación de rutas solo se puede habilitar cuando la transferencia de **radio a radio** está habilitada.




**Preferencias específicas del sitio para nodos de tránsito de superposición virtual** Las preferencias específicas del sitio para los nodos de tránsito de superposición virtual permiten anular la configuración global del nodo de tránsito de superposición virtual para todos los sitios de la red. También puede elegir un nodo que no sea control como nodo de tránsito principal de un sitio. Elija un nodo de control o nodo de control geográfico como los nodos de tránsito secundario y terciario. Si el nodo de tránsito principal está inactivo, los sitios utilizan el nodo de tránsito secundario. Si ambos nodos de tránsito primarios y secundarios están inactivos, los sitios utilizan el nodo de tránsito terciario. Especifique el coste de los nodos de tránsito y seleccione los sitios a los que se aplica la configuración de nodo de tránsito de superposición virtual específica del sitio.




### Nodo de tránsito de Internet

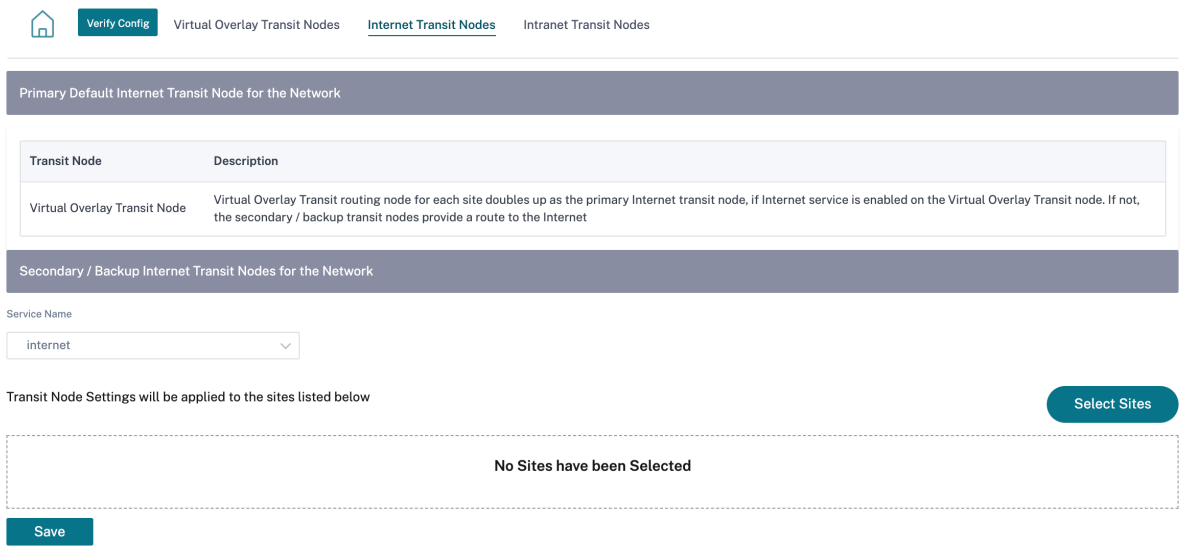
Puede agregar sitios como sitios de tránsito de Internet para habilitar el acceso a Internet a los sitios. Los sitios que necesitan conectividad directa a Internet deben tener al menos un enlace con el servicio de Internet habilitado. Esto significa que al menos un enlace establecido en un ancho de banda compartido distinto de cero%.

A cada sitio de tránsito se le puede asignar un coste de ruta. Los sitios con servicio de Internet disponible acceden a Internet directamente, ya que la ruta directa sería la ruta de menor coste. Los sitios sin servicio de Internet pueden redirigirse a Internet a través de los sitios de tránsito configurados. Cuando se configuran los sitios de tránsito de Internet, las rutas a Internet a través de estos sitios de tránsito se empujan automáticamente a todos los sitios. Los sitios de tránsito de Internet son los sitios con servicio de Internet habilitado.

Por ejemplo, si San Francisco y Nueva York están configurados como sitios de tránsito por Internet. Las rutas a Internet a través de San Francisco y Nueva York se desplazan automáticamente a todos los sitios.

El nodo de tránsito de superposición virtual con servicio Internet habilitado actúa como nodo principal de tránsito de Internet. Si el servicio Internet no está habilitado en el nodo de tránsito de superposición virtual, el nodo de tránsito de Internet secundario/copia de seguridad proporciona una ruta a Internet.



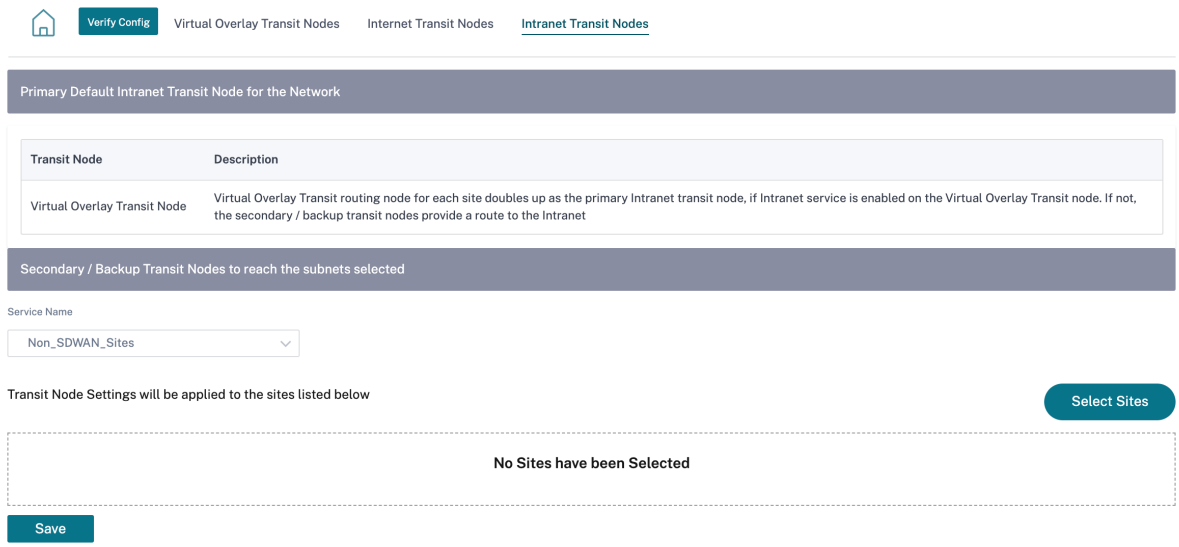

### Nodo de tránsito de la intranet

El nodo de tránsito de la intranet permite que todos los sitios que no sean de intranet tengan acceso a las redes de intranet configuradas. A cada sitio de tránsito se le puede asignar un coste de ruta. Los sitios disponibles con servicio de intranet acceden directamente a las redes de la intranet, ya que la ruta directa sería la ruta de enrutamiento más económica. Los sitios sin servicio de Intranet pueden redirigirse a las redes de Intranet a través de los sitios de tránsito configurados. Cuando se configuran los sitios de tránsito, las rutas a las redes de intranet a través de estos sitios de tránsito se insertan automáticamente a todos los sitios.

Por ejemplo, si 10.2.1.0/24 es una red de intranet y Austin y Dallas son los sitios de tránsito configurados. Las rutas a esa dirección de red a través de Austin y Dallas se desplazan automáticamente a todos los sitios.

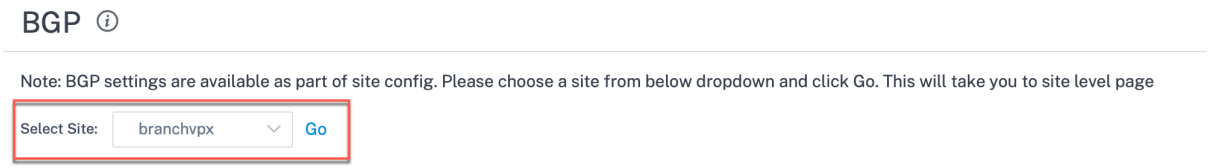
El nodo de tránsito de superposición virtual con el servicio Intranet habilitado actúa como nodo de tránsito de intranet principal. Si el servicio de intranet no está habilitado en el nodo de tránsito de superposición virtual, el nodo de tránsito de intranet secundario/copia de seguridad proporciona una ruta a la intranet.



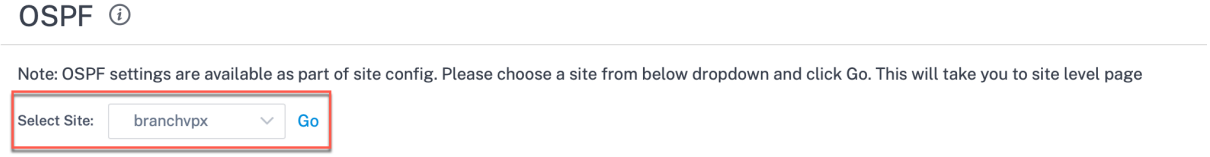

## BGP

Puede configurar los ajustes de BGP para un sitio seleccionando el sitio requerido en la lista desplegable y haciendo clic en **IR**. Esto lo llevará a la página de configuración de BGP al nivel de sitio. Para obtener información detallada sobre la configuración de BGP, consulte BGP.




## OSPF

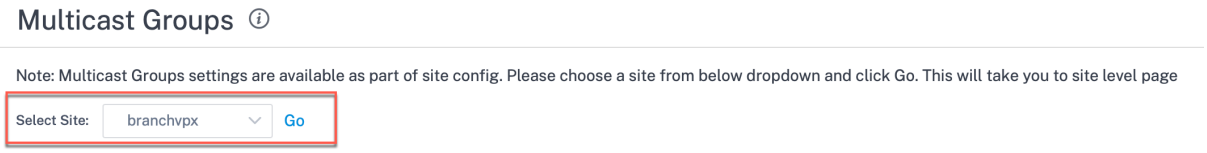
Para configurar los ajustes de OSPF de un sitio, seleccione el sitio requerido en la lista desplegable y haga clic en **IR**. Esto lo llevará a la página de configuración de OSPF al nivel de sitio. Para obtener información detallada sobre la configuración de OSPF, consulte OSPF.



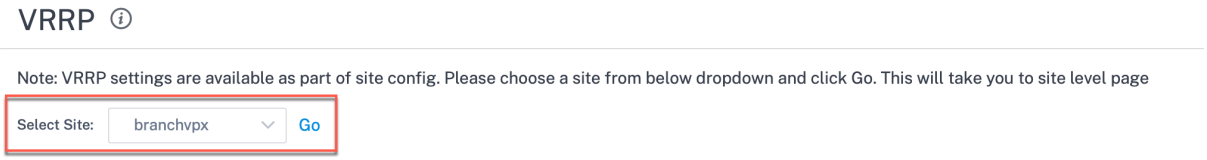
### Grupos de multidifusión

Para configurar el enrutamiento de multidifusión para un sitio, seleccione el sitio requerido en la lista desplegable y haga clic en **IR**. Esto lo llevará a la página de configuración de grupos de multidifusión al nivel de sitio. Para obtener información detallada sobre la configuración del enrutamiento de multidifusión, consulte Grupos de multidifusión.




### VRRP

Puede configurar el protocolo de redundancia del enrutador virtual (VRRP) para un sitio seleccionando el sitio requerido en la lista desplegable y haciendo clic en **IR**. Esto lo lleva a la página de configuración de VRRP al nivel de sitio. Para obtener información detallada sobre la configuración del enrutamiento de multidifusión, consulte VRRP.




## Comunicación entre enlaces

October 31, 2022

La configuración de comunicación entre vínculos se utiliza para la creación automática de rutas entre enlaces WAN compatibles. Puede anular esta configuración en Configuración del **sitio** y **rutas virtuales**, donde puede seleccionar o anular la selección de las rutas de miembros individuales de una ruta virtual determinada.

Actualmente, están disponibles las dos opciones siguientes:

- Reglas para automatizar la creación de rutas entre enlaces WAN compatibles.
- Valores predeterminados globales para rutas virtuales dinámicas

Estos valores son heredados por todos los enlaces WAN de la red del cliente.

Haga clic en **Verificar configuración** para validar cualquier error de auditoría.

### Grupos de comunicación entre vínculos predeterminados

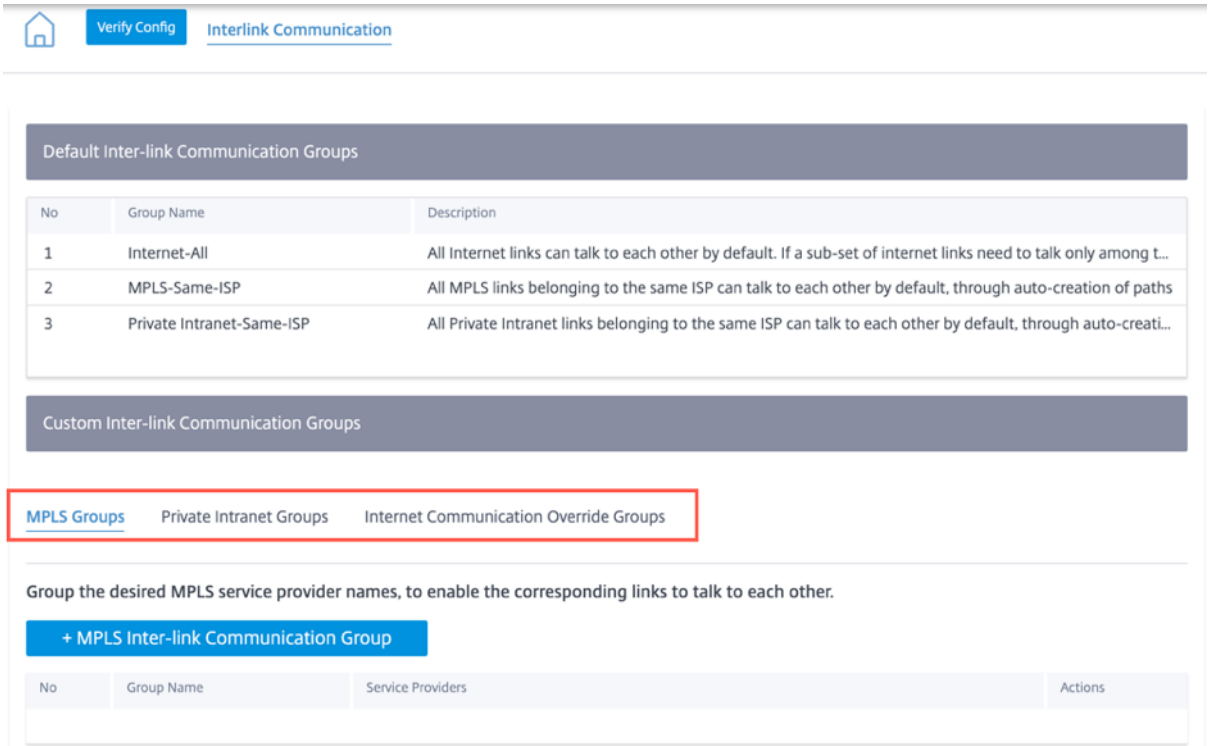
Los grupos de comunicación entre vínculos predeterminados están destinados a automatizar la creación de rutas entre:

- Dos enlaces a Internet cualesquiera
- Dos enlaces MPLS que compartan un proveedor de servicios,.
- Dos enlaces de intranet privada que compartan un proveedor de servicios

### Grupos de comunicación entre enlaces personalizados

Los grupos de comunicación entre vínculos personalizados permiten que la Intranet privada, Internet pública o los vínculos MPLS creen automáticamente rutas con otros enlaces privados de Intranet, Internet pública o MPLS a través de diversos proveedores de servicios.

Por ejemplo, considere este caso: Una empresa tiene oficinas en los EE. UU. y la India. Las oficinas estadounidenses utilizan enlaces de AT&T MPLS, mientras que las oficinas de India utilizan enlaces Airtel MPLS. Supongamos que los enlaces MPLS de AT&T y Airtel son compatibles en términos de etiquetas DSCP y parámetros relacionados, y permiten la creación de rutas entre sí. Las reglas personalizadas de comunicación entre vínculos le permiten seleccionar un par de ISP (por ejemplo, ATT-Airtel en este caso) y habilitar la creación automática de rutas entre los enlaces que pertenecen a estos ISP.



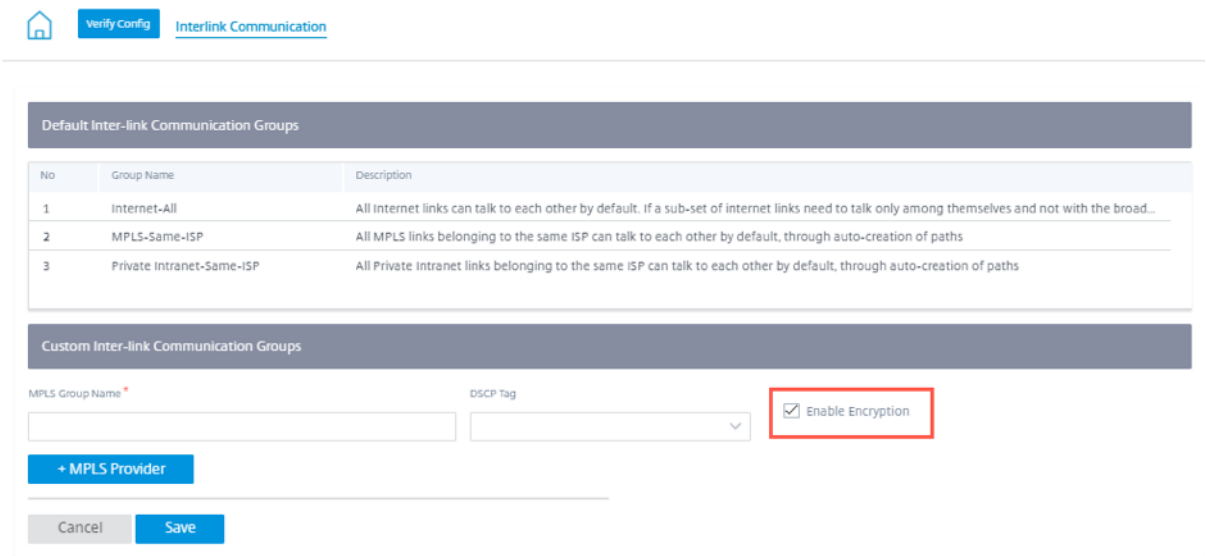

- **Grupos MPLS**: Puede agrupar los nombres de los proveedores de servicios MPLS que quiera para permitir que los enlaces correspondientes se comuniquen entre sí. Haga clic en **+ Grupo**

**de comunicación entre enlaces MPLS** y escriba un nombre de grupo MPLS. Seleccione la etiqueta DSCP en la lista desplegable. También puede agregar el proveedor MPLS seleccionando el nombre del ISP en la lista desplegable. La casilla **Habilitar el cifrado** ayuda a habilitar el cifrado para cada grupo de comunicación entre enlaces MPLS personalizado. En raras ocasiones, para eliminar la sobrecarga del cifrado, puede inhabilitar esta opción.

- **Grupos de intranet privados**: Puede agrupar los nombres de los proveedores de servicios de intranet deseados para permitir que los enlaces correspondientes se comuniquen entre sí. Haga clic en **+ Grupo de comunicación entre enlaces de intranet** privada y proporcione el nombre del grupo de intranet privada. Seleccione la etiqueta DSCP en la lista desplegable. También puede agregar el proveedor de intranet privada seleccionando el nombre del ISP en la lista desplegable. La casilla **Habilitar el cifrado** ayuda a habilitar/inhabilitar el cifrado para cada grupo de comunicación entre enlaces de intranet privado personalizado.
- **Grupos de anulación de comunicaciones de Internet**: Si un subconjunto de enlaces de Internet debe comunicarse solo entre sí y no con el resto de enlaces de Internet, puede agrupar los nombres de ISP correspondientes para permitir la exclusión del grupo predeterminado.

El resto de los enlaces de Internet todavía pueden comunicarse entre sí. Haga clic en **+ Grupo de comunicación entre enlaces de Internet público** y proporcione un nombre de grupo de Internet público. Seleccione la etiqueta DSCP en la lista desplegable. También puede agregar el proveedor de Internet público seleccionando el nombre del ISP en la lista desplegable. La opción **Habilitar el cifrado** garantiza que los paquetes del grupo de comunicación entre enlaces que se envían por las rutas virtuales estén cifrados.



# Seguridad

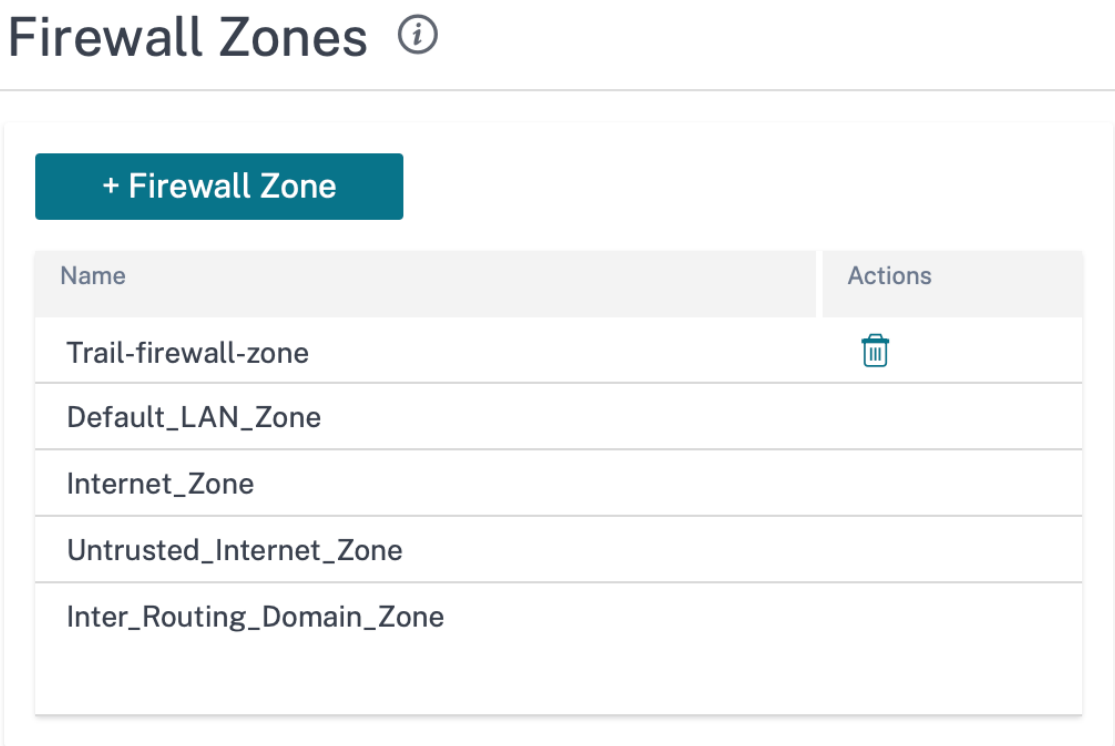
October 31, 2022

Puede configurar los ajustes de seguridad, como la seguridad de la red, la ruta virtual, IPsec, el firewall y los certificados, que se aplican a todos los dispositivos de la red.

## Zonas de firewall

Puede configurar zonas en la red y definir directivas para controlar la forma en que el tráfico entra y sale de las zonas. Las siguientes zonas están disponibles de forma predeterminada:

- **default_lan_zone**: Se aplica al tráfico hacia o desde un objeto con una zona configurable, donde la zona no se ha establecido.
- **Internet_Zone**: Se aplica al tráfico hacia o desde un servicio de Internet mediante una interfaz de confianza.
- **Untrusted_Internet_Zone**: Se aplica al tráfico hacia o desde un servicio de Internet mediante una interfaz que no es de confianza.




También puede crear sus propias zonas y asignarlas a los siguientes tipos de objetos:

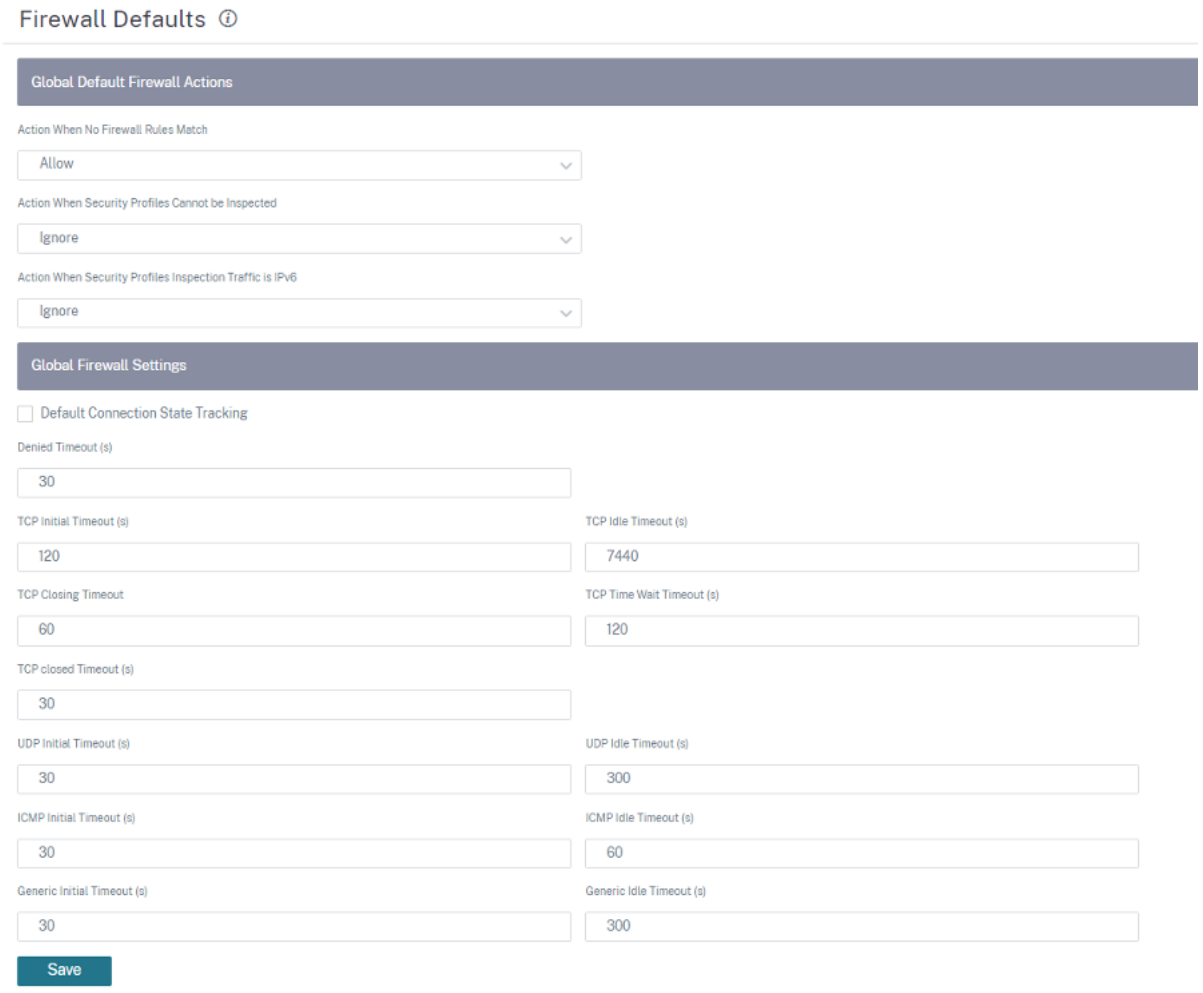
 

- Interfaces de red virtual
- Servicios de intranet
- Túneles GRE
- Túneles LAN IPsec

Haga clic en **Verificar configuración** para validar cualquier error de auditoría.

### Valores predeterminados del firewall

Puede configurar las acciones de firewall globales predeterminadas y las configuraciones globales del firewall que se pueden aplicar a todos los dispositivos de la red SD-WAN. La configuración también se puede definir en el nivel de sitio que reemplaza la configuración global.




- **Acción cuando no coincide ninguna regla de firewall**: Seleccione una acción (Permitir o eliminar) de la lista para los paquetes que no coincidan con una directiva de firewall.
- **Acción cuando no se pueden inspeccionar los perfiles de seguridad**: Seleccione una acción

(ignorar o eliminar) para los paquetes que coincidan con una regla de firewall y se conecten a un perfil de seguridad, pero que el subsistema Edge Security no pueda inspeccionar temporalmente. Si selecciona **Ignorar**, la regla de firewall correspondiente se tratará como no coincidente y se evalúa la siguiente regla de firewall en orden. Si selecciona **Cortar**, se descartan los paquetes que coinciden con la regla de firewall correspondiente.

- **Acción de firewall predeterminada**: Seleccione una acción (Permitir/eliminar) de la lista para los paquetes que no coincidan con una directiva.
- **Seguimiento del estado de conexión predeterminado**: Permite el seguimiento direccional del estado de la conexión para los flujos TCP, UDP e ICMP que no coinciden con una directiva de filtro o regla de NAT.

  > **Nota**
  >
  > Los flujos asimétricos se bloquean cuando se habilita **el seguimiento del estado de la conexión predeterminada**, incluso cuando no hay directivas de firewall definidas. Si existe la posibilidad de flujos asimétricos en un sitio, la recomendación es habilitarlos al nivel de sitio o directiva y no a nivel mundial.

- **Tiempo de espera denegado (s)**: Tiempo (en segundos) para esperar a que lleguen nuevos paquetes antes de cerrar las conexiones denegadas.
- Tiempo de**espera inicial de TCP**: Tiempo (en segundos) para esperar nuevos paquetes antes de cerrar una sesión TCP incompleta.
- Tiempo de**espera de inactividad de TCP**: Tiempo (en segundos) para esperar nuevos paquetes antes de cerrar una sesión TCP activa.
- Tiempo de**espera de cierre de TCP**: Tiempo (en segundos) para esperar nuevos paquetes antes de cerrar una sesión TCP tras una solicitud de finalización.
- **Tiempos de espera de TCP**: Tiempo (en segundos) para esperar nuevos paquetes antes de cerrar una sesión TCP finalizada.
- Tiempo de**espera de cierre de TCP**: Tiempo (en segundos) para esperar nuevos paquetes antes de cerrar una sesión TCP abortada.
- Tiempo de**espera inicial de UDP**: Tiempo (en segundos) para esperar nuevos paquetes antes de cerrar la sesión de UDP que no ha recibido tráfico en ambas direcciones.
- Tiempo de**espera de inactividad de UDP**: Tiempo (en segundos) para esperar nuevos paquetes antes de cerrar una sesión UDP activa.
- Tiempo de**espera inicial de ICMP**: Tiempo (en segundos) para esperar a que lleguen nuevos paquetes antes de cerrar una sesión de ICMP que no ha recibido tráfico en ambas direcciones
- Tiempo de espera de**inactividad de ICMP**: Tiempo (en segundos) para esperar a que lleguen nuevos paquetes antes de cerrar una sesión ICMP activa.

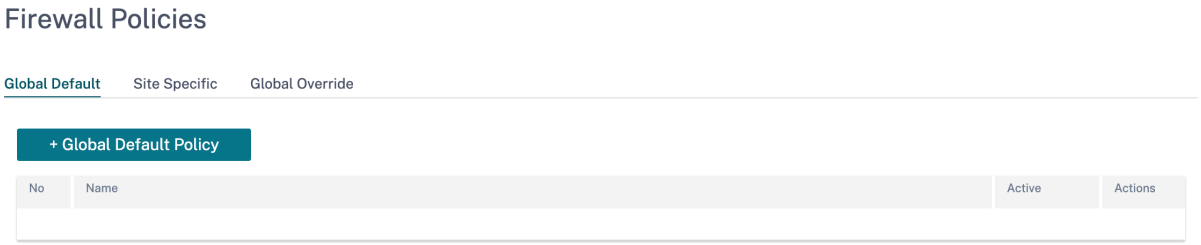
- Tiempo de**espera inicial genérico**: Tiempo (en segundos) para esperar nuevos paquetes antes de cerrar una sesión genérica que no ha recibido tráfico en ambas direcciones.
- Tiempo de**espera de inactividad genérico**: Tiempo (en segundos) para esperar nuevos paquetes antes de cerrar una sesión genérica activa.

Haga clic en **Verificar configuración** para validar cualquier error de auditoría.

### Directivas de firewall

Los perfiles de firewall proporcionan seguridad al garantizar que el tráfico de red está restringido solo a una regla de firewall específica según los criterios de coincidencia y aplicando acciones específicas. Las **directivas de firewall** contienen tres secciones.

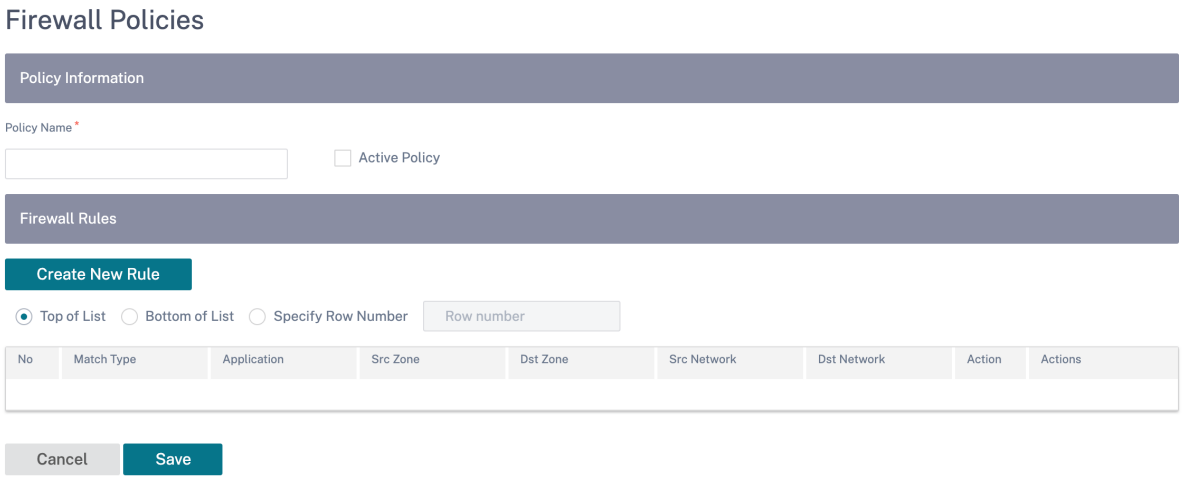
- **Predeterminado** global: La directiva predeterminada global es una agregación de un par de reglas de firewall. La directiva que cree en la sección **Predeterminado global** se aplica a todos los sitios de la red.
- **Sitio específico**: Puede aplicar las reglas de firewall definidas en ciertos sitios específicos.
- **Anulación global**: Puede anular las directivas globales y específicas del sitio mediante la **Directiva de anulación global**.




Puede definir reglas de firewall y colocarlas en función de la prioridad. Puede elegir el orden de prioridad para comenzar desde la parte superior de la lista, en la parte inferior de la lista o desde una fila específica.

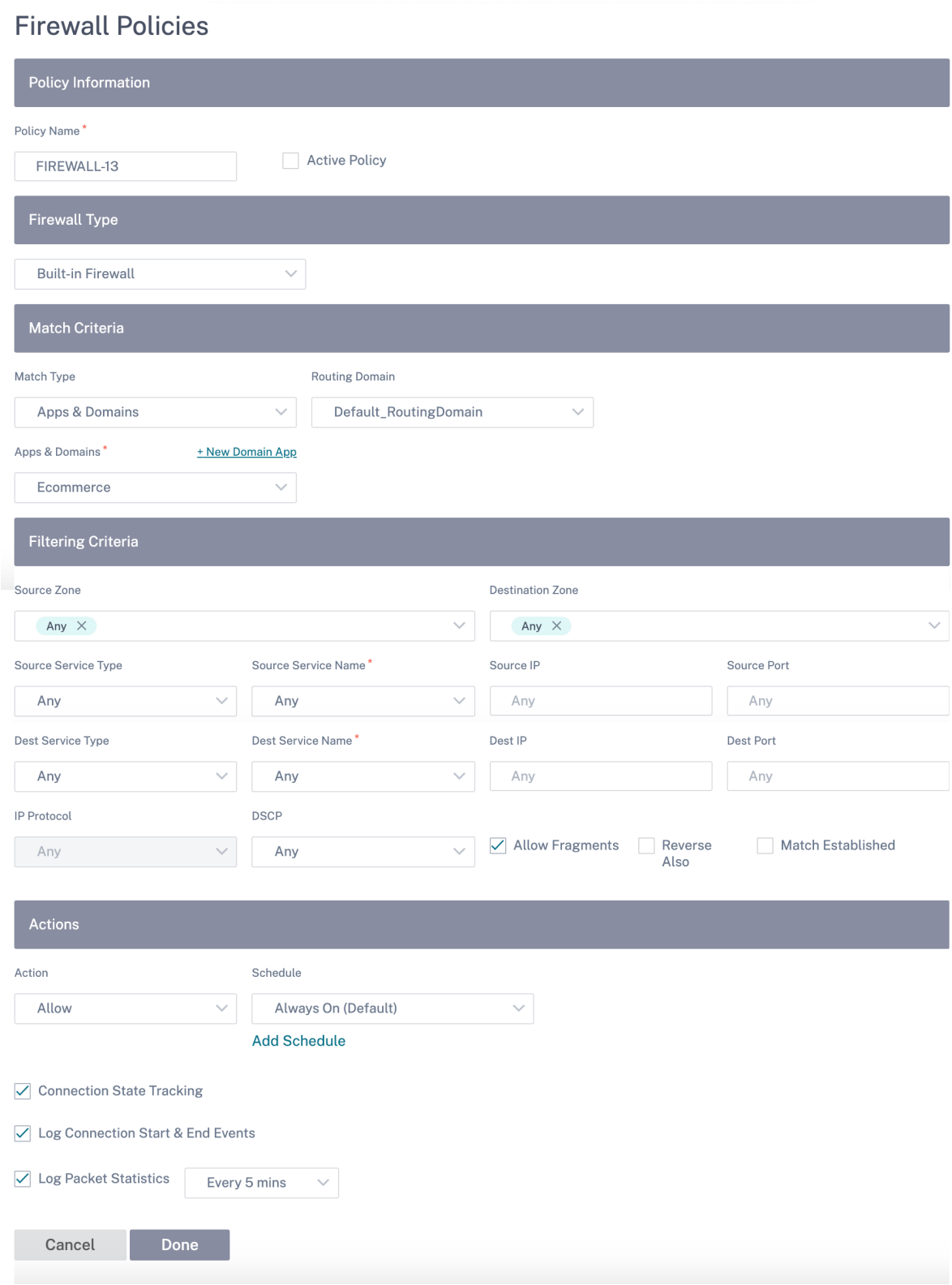
Se recomienda tener reglas más específicas para aplicaciones o subaplicaciones en la parte superior, seguidas de reglas menos específicas para las que representan un tráfico más amplio.




Para crear una regla de firewall, haga clic en **Crear nueva regla**.




- Introduzca un nombre de directiva y active la casilla de verificación **Directiva activa** si quiere aplicar todas las reglas de firewall.

- Los criterios de coincidencia definen el tráfico de la regla como, por ejemplo, una aplicación, una aplicación definida personalizada, un grupo de aplicaciones, una familia de aplicaciones o un protocolo IP basado en.
- Criterios de filtrado:
  - **Zona de origen**: La zona de firewall de origen.
  - **Zona de destino**: La zona de firewall de destino.
  - **Tipo de servicio de**origen: El tipo de servicio SD-WAN de origen (local, ruta virtual, intranet, host IP o Internet) son ejemplos de tipos de servicio.
  - **Nombre del servicio de origen**: El nombre de un servicio vinculado al tipo de servicio. Por ejemplo, si la ruta virtual está seleccionada para el tipo de servicio de origen, sería el nombre de la ruta virtual específica. Esto no siempre es necesario y depende del tipo de servicio seleccionado.
  - **IP de origen**: La dirección IP y la máscara de subred que la regla usa para hacer coincidir.
  - **Puerto de origen**: El puerto de origen que utiliza la aplicación específica.
  - **Tipo de servicio Dest**: El tipo de servicio SD-WAN de destino (local, ruta virtual, intranet, host IP o Internet) son ejemplos de tipos de servicios.
  - **Nombre del servicio Dest**: Nombre de un servicio vinculado al tipo de servicio. Esto no siempre es necesario y depende del tipo de servicio seleccionado.
  - **Dirección IP**: La dirección IP y la máscara de subred que el filtro utiliza para hacer coincidir.
  - **Puerto Dest**: E l puerto de destino que utiliza la aplicación específica (es decir, el puerto de destino HTTP 80 para el protocolo TCP).
  - **Protocolo IP**: Si se selecciona este tipo de coincidencia, seleccione un protocolo IP con el que coincida la regla. Las opciones incluyen ANY, TCP, UDP, ICMP, etc.
  - **DSCP**: Permite al usuario hacer coincidir la configuración de una etiqueta DSCP.
  - **Permitir fragmentos**: Permite los fragmentos de IP que coincidan con esta regla.
  - **Invertir también**: Agregue automáticamente una copia de esta directiva de filtros con la configuración de origen y destino invertida.
  - **Coincidencia establecida**: haga coincidir los paquetes entrantes de una conexión a la que se permitieron los paquetes salientes.
- Se pueden realizar las siguientes acciones en un flujo coincidente:
  - **Permitir**: Permitir el flujo a través del Firewall.
  - **Descartar**: Deniegue el flujo a través del firewall descartando los paquetes.

- **Rechazar**: Deniegue el flujo a través del firewall y envíe una respuesta específica del protocolo. TCP envía un restablecimiento, ICMP envía un mensaje de error.
- **Contar y continuar**: Cuente la cantidad de paquetes y bytes de este flujo y, a continuación, continúe con la lista de directivas.

Además de definir la acción que se va a realizar, también puede seleccionar los registros que se van a capturar.

## Seguridad de red

Seleccione el mecanismo de cifrado que se utilizará en toda la red. Puede configurar la configuración de seguridad global que proteja toda la red SD-WAN.

El modo de cifrado de red define el algoritmo utilizado para todas las rutas cifradas en la red SD-WAN. No es aplicable a rutas no cifradas. Puede establecer el cifrado como AES-128 o AES-256.

### Cumplimiento FIPS

El modo FIPS obliga a los usuarios a configurar los ajustes compatibles con FIPS para sus túneles de IPSec y los ajustes de IPSec para las rutas virtuales.

La activación del modo FIPS ofrece las siguientes capacidades:

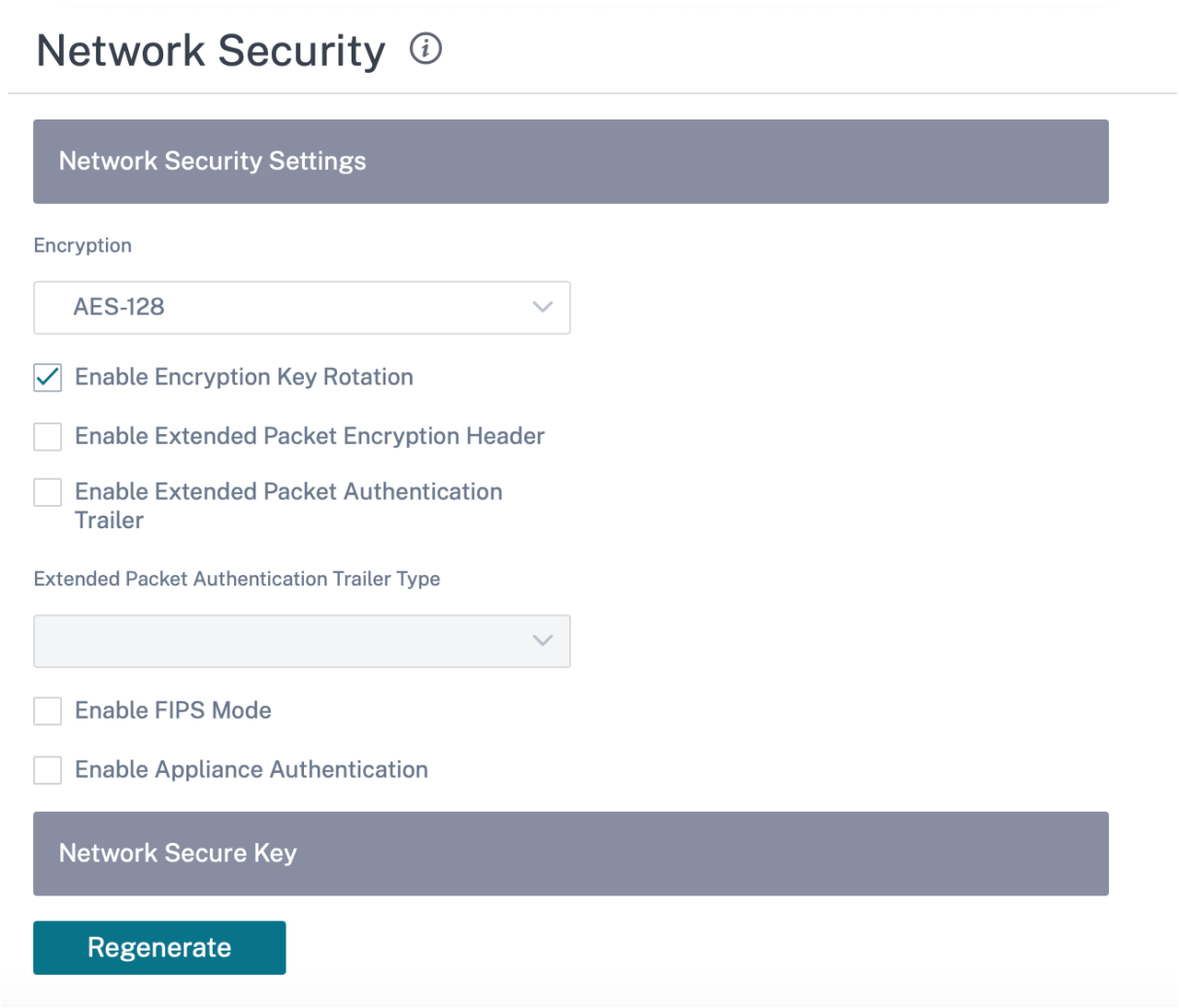
- Muestra el modo IKE compatible con FIPS.
- Muestra un grupo IKE DH compatible con FIPS desde el que los usuarios pueden seleccionar los parámetros necesarios para configurar el dispositivo en modo compatible con FIPS (2,5,14 — 21).
- Muestra el tipo de túnel IPsec compatible con FIPS en la configuración de IPsec para rutas virtuales
- Modo de integridad IKE hash e (IKEv2), modo de autenticación IPsec.
- Realiza errores de auditoría para la configuración de vida útil basada en FIPS.

Para habilitar el cumplimiento de FIPS en el servicio Citrix SD-WAN Orchestrator:

1. Vaya a **Configuración** > **Seguridad > Seguridadde la red**.
2. En la sección **Configuración de seguridad de red**, haga clic en la casilla **Habilitar el modo FIPS**.

Al habilitar el modo FIPS, se exigen comprobaciones durante la configuración para garantizar que todos los parámetros de configuración relacionados con IPsec cumplan los estándares FIPS. Se le pedirá a través de errores de auditoría y advertencias que configure IPsec.




Si la configuración de IPSec no cumple con los estándares FIPS cuando está habilitada, es posible que se produzca un error de auditoría. Los siguientes son los tipos de errores de auditoría que se muestran al hacer clic en **Verificar configuración** en la interfaz de usuario de Citrix SD-WAN Orchestrator for On-premises.

- Cuando el modo FIPS está activado y se selecciona la opción que no es compatible con FIPS.
- Cuando el modo FIPS está activado y se introduce un valor de vida incorrecto.
- Cuando el modo FIPS está habilitado y la configuración de IPSec para la ruta virtual establecida por defecto también está habilitada, y se selecciona el modo túnel incorrecto (ESP frente a ESP_Auth/AH).
- Cuando se habilita el modo FIPS, también se habilita la configuración de IPSec para el conjunto predeterminado de rutas virtuales y se introduce un valor de vida incorrecto.

**Habilitar rotación de claves**de cifrado: Cuando está activada, las claves de cifrado se rotan a intervalos de 10 a 15 minutos.

**Habilitar encabezado de cifrado de paquetes extendido**: Cuando está habilitado, se antecede un

contador cifrado de 16 bytes al tráfico cifrado para servir como vector de inicialización y cifrar paquetes aleatoriamente.

**Habilitar tráiler de autenticación de paquetes extendida**: Cuando está habilitada, se agrega un código de autenticación al contenido del tráfico cifrado para verificar que el mensaje se entrega sin alteraciones.

**Tipo de tráiler de autenticación de paquetes extendida**: Este es el tipo de tráiler utilizado para validar el contenido del paquete. Seleccione una de las siguientes opciones del menú desplegable: Suma de **comprobación de 32 bits** o **SHA-256**.

### Inspección SSL

La inspección de Secure Sockets Layer (SSL) es un proceso de interceptación, descifrado y análisis del tráfico HTTPS y SMTP seguro en busca de contenido malicioso. La inspección SSL proporciona seguridad al tráfico que entra y sale de su organización. Puede generar y cargar el certificado de CA raíz de su organización y realizar la inspección intermedia del tráfico.

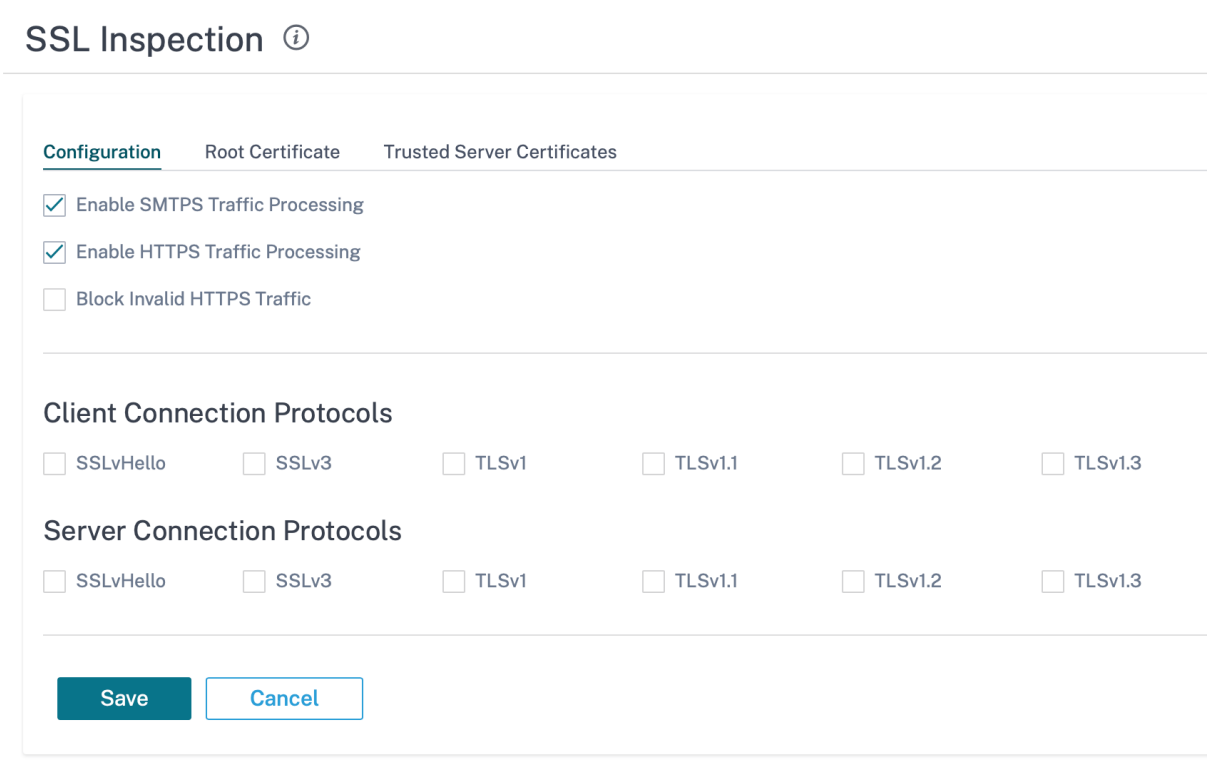
> **NOTA**
>
> La inspección SSL se admite a partir de la versión 11.3.0 de Citrix SD-WAN.

Para habilitar la inspección SSL, al nivel de red, vaya a **Configuración > Seguridad > Inspección SSL > Configuración** y defina los siguientes parámetros de configuración de SSL.

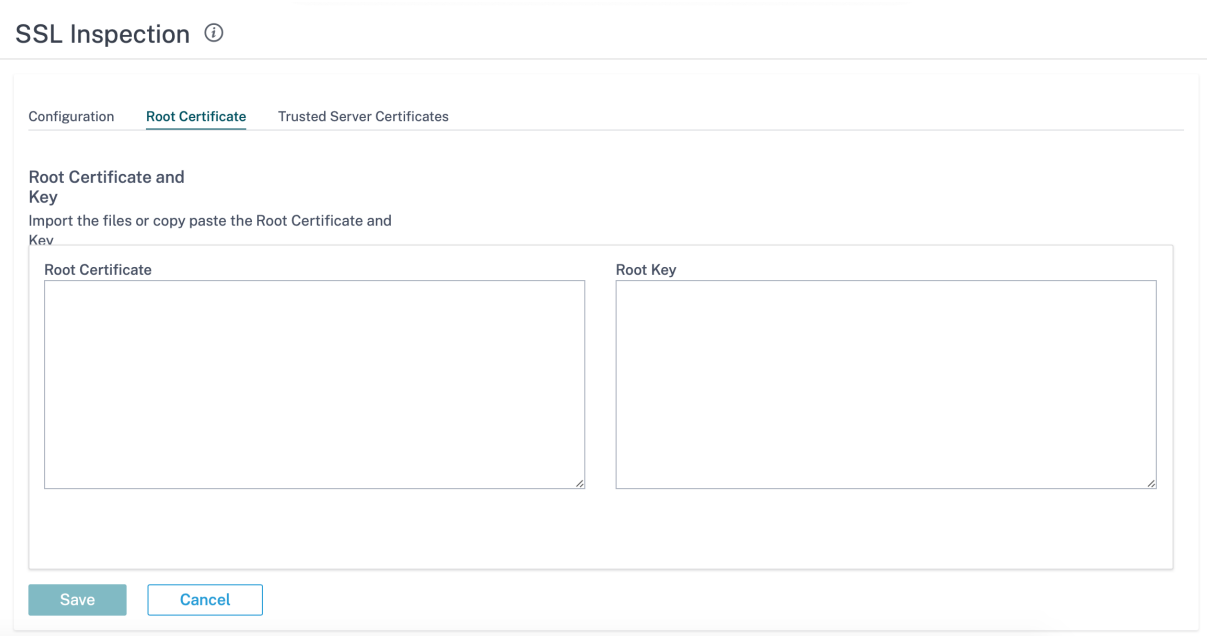
- **Habilite el procesamiento del tráfico SMTPS**: El tráfico SMTP seguro se somete a una inspección SSL.
- **Habilite el procesamiento de tráfico HTTPS**: El tráfico HTTPS se somete a una inspección SSL.
- **Bloquear tráfico HTTPS no válido**: De forma predeterminada, cuando la casilla **Bloquear tráfico HTTPS no válido** está desactivada, se ignora el tráfico que no sea HTTPS en el puerto 443 y se permite que fluya sin obstáculos. Cuando se selecciona **Bloquear tráfico HTTPS no válido**, se bloquea el tráfico que no sea HTTPS para la inspección de SSL. Al habilitar esta opción, es posible que se bloquee el tráfico que de otro modo sería legítimo, es decir, el tráfico HTTP en el puerto 443 o el tráfico HTTPS de sitios con un certificado caducado.
- **Protocolos de conexión de cliente**: Seleccione los protocolos de cliente requeridos. Los protocolos disponibles son SSLVhello, SSLv3, TLSv1, TSLv1.1, TLSv1.2 y TLSv1.3.
- **Protocolos de conexión al servidor**: Seleccione los protocolos de servidor requeridos. Los protocolos disponibles son SSLVhello, SSLv3, TLSv1, TSLv1.1, TLSv1.2 y TLSv1.3.

> **NOTA**
>
> Las versiones anteriores a TLSv1.2 se consideran vulnerables y no deben habilitarse, a menos que la compatibilidad con versiones anteriores sea importante.

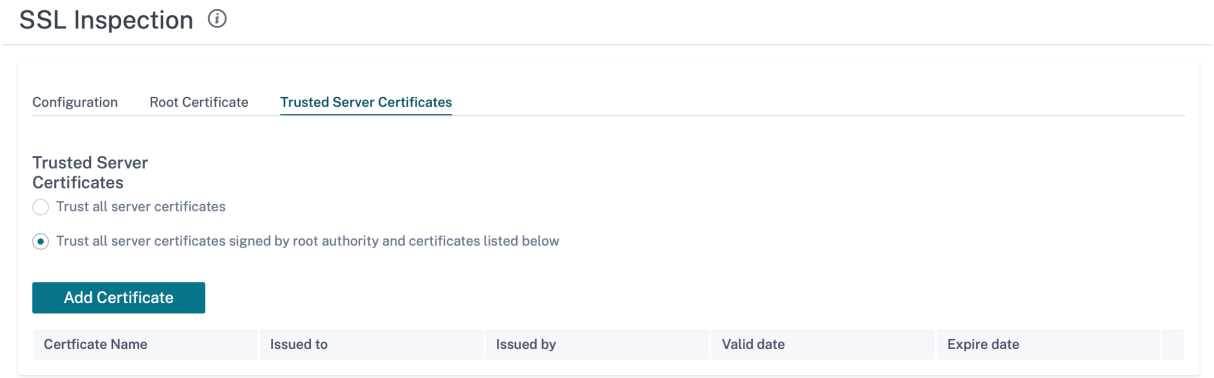



En la ficha **Certificado raíz**, copie y pegue el certificado raíz y la clave de la autoridad de certificación raíz (CA) de su organización. La CA raíz se utiliza para crear y firmar una copia falsificada de los certificados de los sitios originales, de modo que se pueda realizar la inspección de SSL. Se asume implícitamente que el certificado de CA raíz está instalado en todas las estaciones de trabajo y dispositivos del cliente a los que se les puede inspeccionar su SSL de tráfico.



La opción predeterminada, **Confiar en todos los certificados de servidor firmados por la autoridad raíz y los certificados que se enumeran a continuación**, da como resultado que SD-WAN valide todos los certificados de servidor con la lista estándar de CA raíz y la CA raíz configuradas previamente. También descarta los servidores que tienen un certificado no válido. Para anular este comportamiento, cargue el certificado SSL autofirmado de los servidores internos en la ficha **Certificados de servidor de confianza**. Haga clic en **Agregar certificado** e introduzca un nombre, busque el certificado y cárguelo. Como alternativa, si selecciona **Confiar en todos los certificados de servidor**, Citrix SD-WAN considera que todos los servidores son de confianza, independientemente del estado de validación de los certificados.




Como parte de los perfiles de seguridad, puede crear reglas SSL y habilitarlas para la inspección de SSL. Para obtener más información sobre la creación de reglas SSL para un perfil de seguridad, consulte Seguridad perimetral.

## Prevención de intrusiones

Intrusion Prevention System (IPS) detecta y evita que la actividad malintencionada entre en la red. El IPS inspecciona el tráfico de la red y toma medidas automatizadas en todos los flujos de tráfico entrante. Incluye una base de datos con más de 34 000 detecciones de firmas y firmas heurísticas para el escaneo de puertos, lo que le permite monitorear y bloquear de manera efectiva la mayoría de las solicitudes sospechosas.

IPS utiliza la detección basada en firmas, que coincide con los paquetes entrantes con una base de datos de patrones de exploit y ataque identificables de forma única. La base de datos de firmas se actualiza automáticamente diariamente. Dado que hay miles de firmas, las firmas se agrupan en tipos Categoría y Clase.

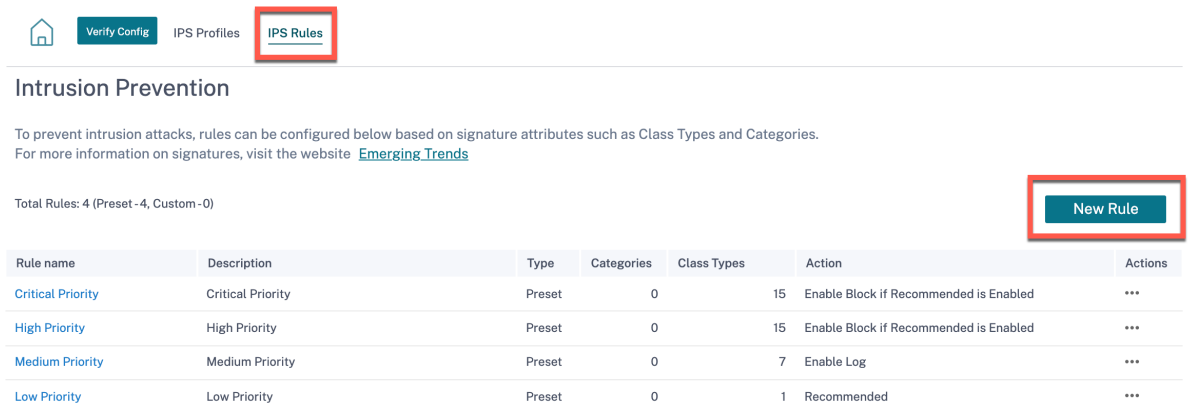
Puede crear reglas de IPS y habilitar solo las categorías de firmas o los tipos de clases que su red requiere. Dado que la prevención de intrusiones es un proceso sensible a la informática, utilice solo el conjunto mínimo de categorías de firmas o tipos de clases que sean relevantes para su red.

Puede crear un perfil de IPS y habilitar una combinación de reglas de IPS. A continuación, estos perfiles IPS se pueden asociar globalmente a toda la red o solo a sitios específicos.

Cada regla se puede asociar a varios perfiles de IPS y cada perfil de IPS se puede asociar a varios sitios. Cuando se habilita un perfil de IPS, inspecciona el tráfico de red de los sitios a los que está asociado el perfil de IPS y de las reglas de IPS habilitadas en ese perfil.

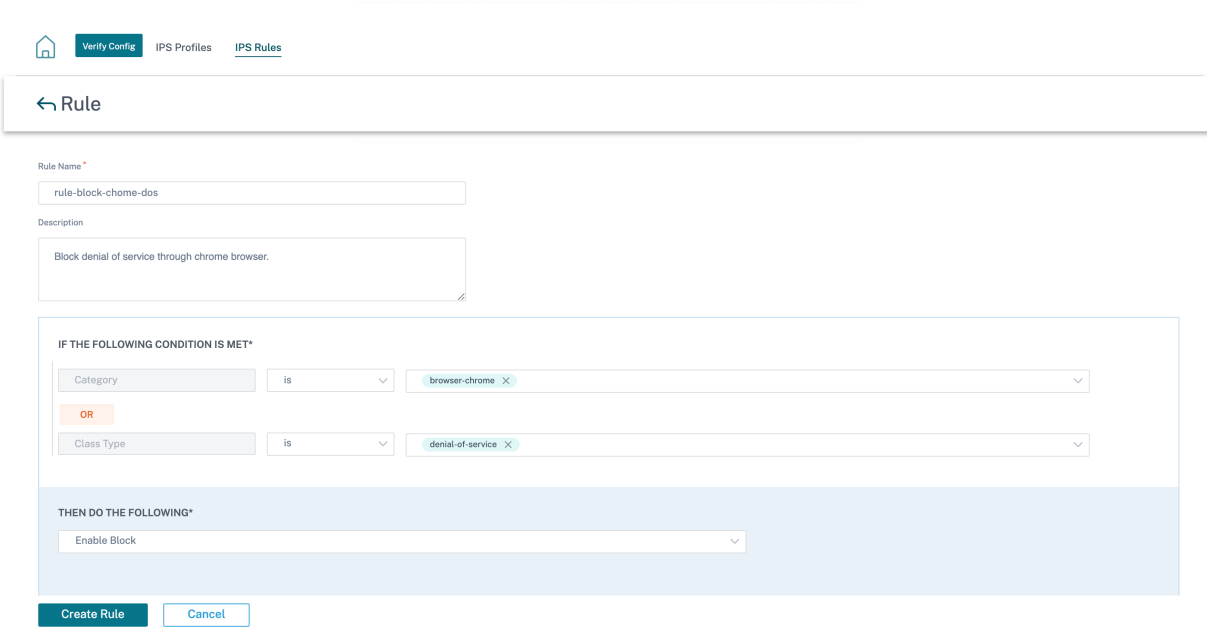
Para crear reglas de IPS, al nivel de red, vaya a **Configuración > Seguridad > Prevención de intrusiones > Reglas de IPS** y haga clic en **Nueva regla**.




Proporcione un nombre de regla y una descripción. Seleccione los atributos de firma de categoría o tipo de clase coincidentes, seleccione una acción para la regla y habilítela. Puede elegir entre las siguientes acciones de regla:

| Acción de regla | Función |
|---|---|
| Recomendado | Hay acciones recomendadas definidas para cada firma. Realice la acción recomendada para las firmas. |
| Habilitar registro | Permitir y registrar el tráfico que coincida con cualquiera de las firmas de la regla. |
| Habilitar bloque si Recomendado está habilitado | Si la acción de la regla es **Recomendada** y la acción recomendada para la firma es **Activar registro**, elimine el tráfico que coincida con cualquiera de las firmas de la regla. |
| Activar bloque | Suelte el tráfico que coincida con cualquiera de las firmas de la regla. |

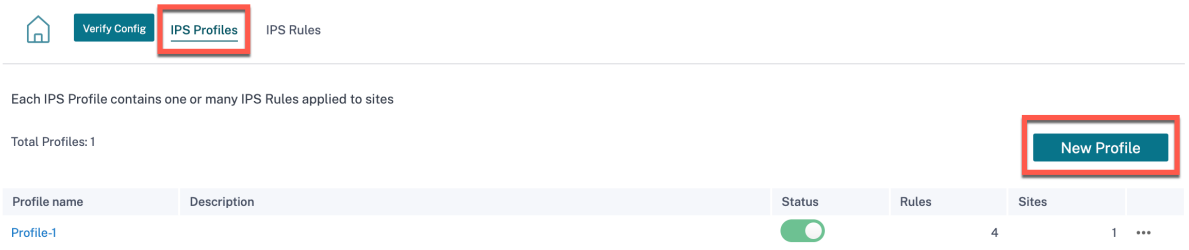
 




**Nota**

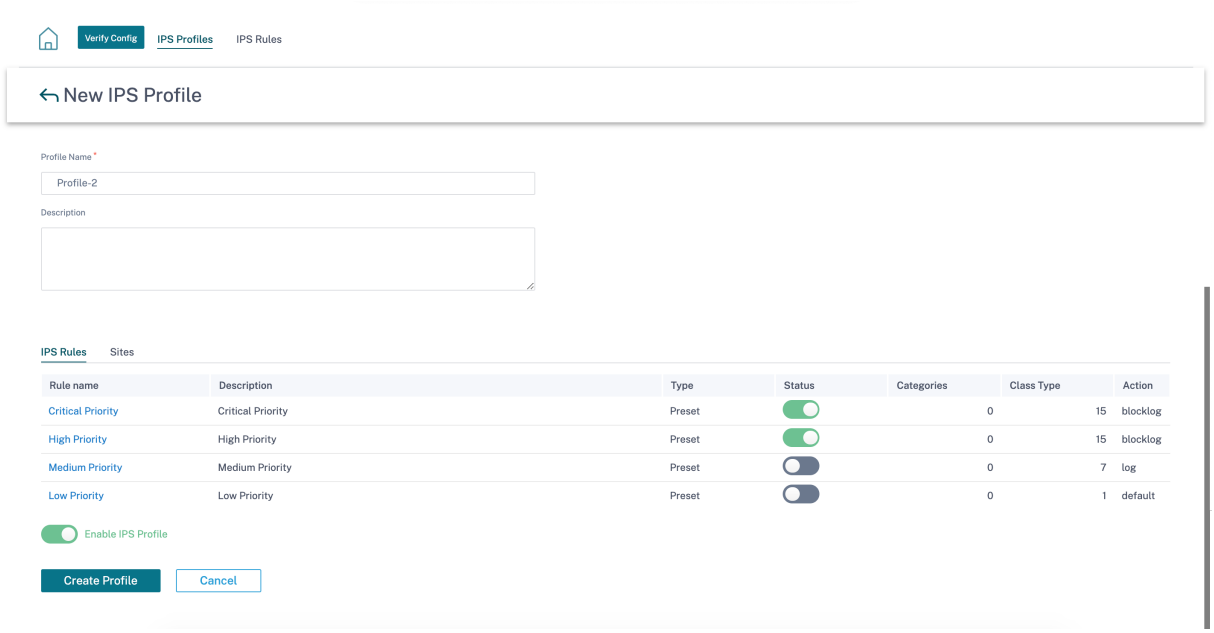
- Dado que la prevención de intrusiones es un proceso sensible a la informática, utilice solo el conjunto mínimo de categorías de firmas que sean relevantes para sus implementaciones de seguridad perimetral.
- El firewall SD-WAN elimina el tráfico en todos los puertos WAN L4 que no están reenviados por puertos y que no están visibles en el motor IPS. Esto proporciona una capa de seguridad adicional contra ataques dos triviales y análisis.

Para crear perfiles de IPS, al nivel de red, vaya a **Configuración > Seguridad > Prevención de intrusiones > Perfiles de IPS** y haga clic en **Nuevo perfil**.

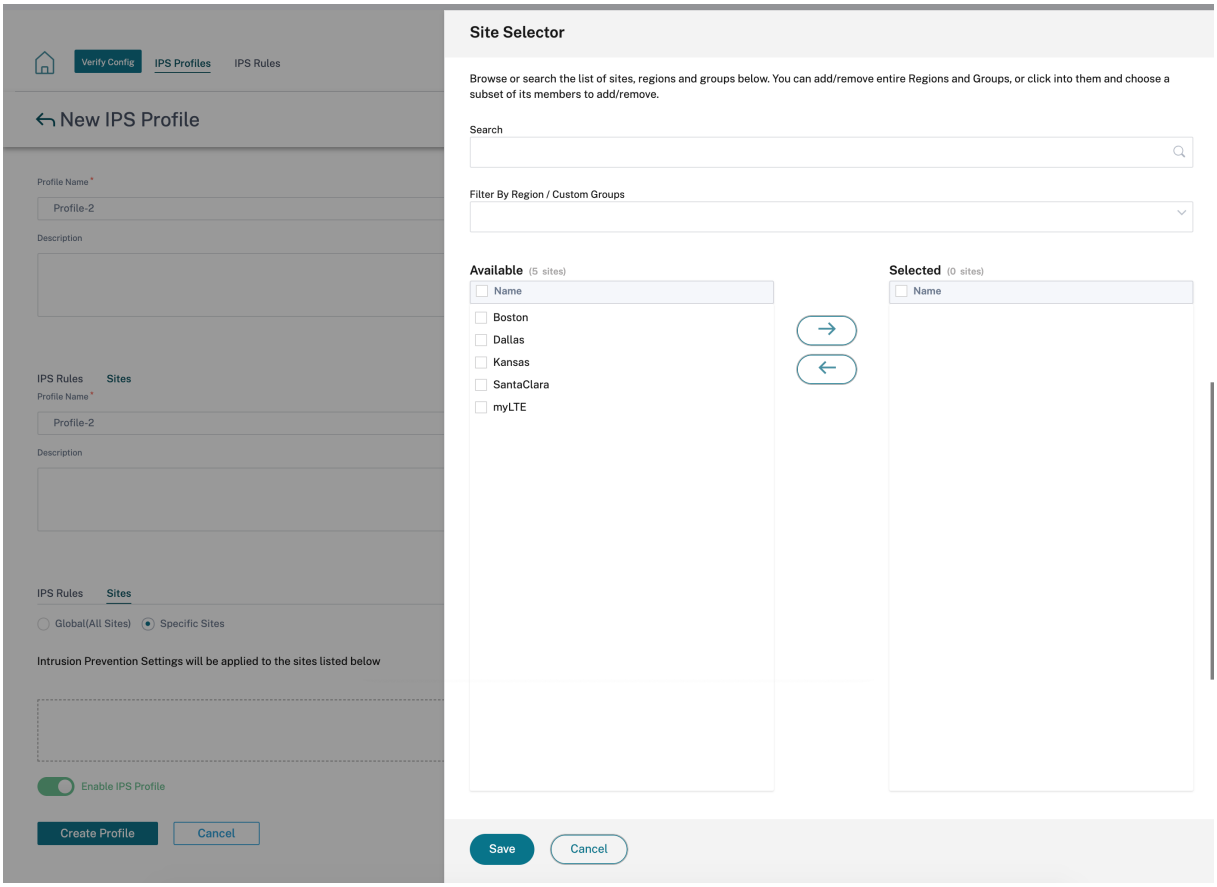



Proporcione un nombre y una descripción para el perfil de IPS. En la ficha **Reglas de IPS**, habilite las **reglas de IPS** necesarias y active **Activar perfiles de IPS**.




En la ficha **Sitios**, haga clic en **Seleccionar sitios**. Seleccione los sitios y haga clic en **Guardar**. Haga clic en **Crear perfil**.




Puede habilitar o inhabilitar estos perfiles IPS al crear perfiles de seguridad. Los perfiles de seguridad

se utilizan para crear reglas de firewall. Para obtener más información, consulte Perfil de seguridad: Prevención de intrusiones.

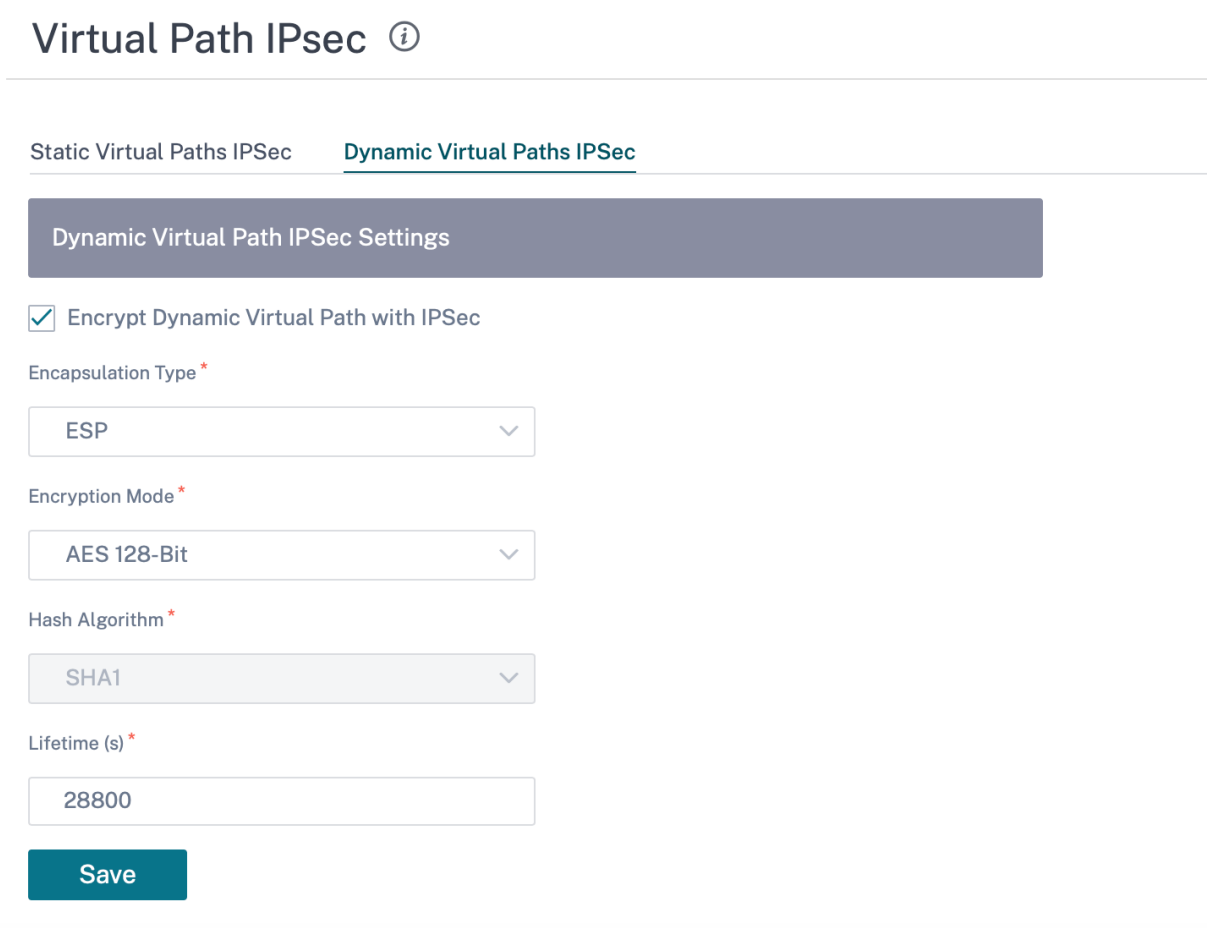
### Ruta virtual IPSec

**Ruta virtual IPSec** define la configuración del túnel IPSec para garantizar la transmisión segura de datos a través de las rutas virtuales estáticas y las rutas virtuales dinámicas. Seleccione la ficha **IPSec de rutas virtuales estáticaso IPsec de rutas virtuales dinámicas** para definir la configuración del túnel IPSec.

- **Tipo de encapsulación**: Elija uno de los siguientes tipos de seguridad:
  - **ESP**: Los datos están encapsulados y cifrados.
  - **ESP+Auth**: Los datos se encapsulan, cifran y validan con un HMAC.
  - **AH**: Los datos se validan con un HMAC.
- **Modo de cifrado**: El algoritmo de cifrado que se utiliza cuando se habilita el ESP.
- **Algoritmo**de hash: El algoritmo de hash utilizado para generar un HMAC.
- **Duración (s)**: La duración preferida, en segundos, para que exista una asociación de seguridad IPSec. Escriba 0 para ilimitado.

Para obtener información sobre la configuración del servicio IPSec, consulte Servicio IPSec.

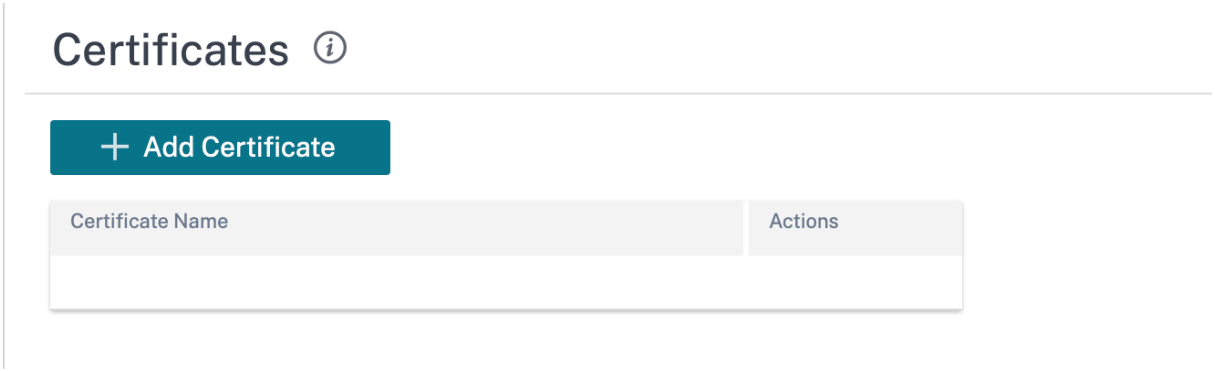



Haga clic en **Verificar configuración** para validar cualquier error de auditoría

## Certificados

Existen dos tipos de certificados: De identidad y de confianza. Los certificados de identidad se utilizan para firmar o cifrar datos para validar el contenido de un mensaje y la identidad del remitente. Los certificados de confianza se utilizan para verificar las firmas de mensajes. Los dispositivos Citrix SD-WAN aceptan certificados de identidad y certificados de confianza. Los administradores pueden administrar certificados en el Editor de configuración.

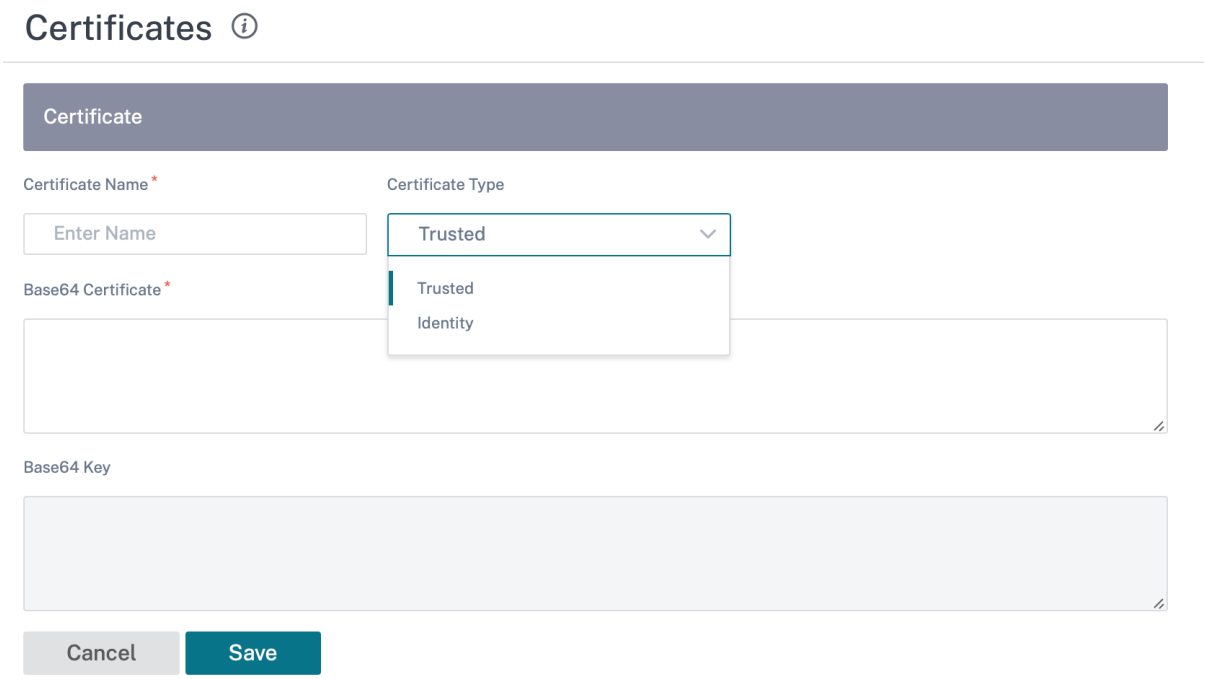



Haga clic en **Verificar configuración** para validar cualquier error de auditoría

Para agregar un certificado, haga clic en **Agregar certificado**.

- **Nombre del certificado**: Proporcione el nombre del certificado.
- **Tipo de certificado**: Seleccione el tipo de certificado en la lista desplegable.
  - **Certificados**de identidad: Los certificados de identidad requieren que la clave privada del certificado esté disponible para el firmante. Certificados de identidad o sus cadenas de certificados en las que un par confía para validar el contenido y la identidad del remitente. Los certificados de identidad configurados y sus respectivas huellas digitales se muestran en el Editor de configuración.
  - **Certificados**de confianza: Los certificados de confianza son certificados autofirmados, de autoridad de certificación (CA) intermedia o de CA raíz que se utilizan para validar la identidad de un par. No se requiere clave privada para un certificado de confianza. Los certificados de confianza configurados y sus respectivas huellas digitales se enumeran aquí.



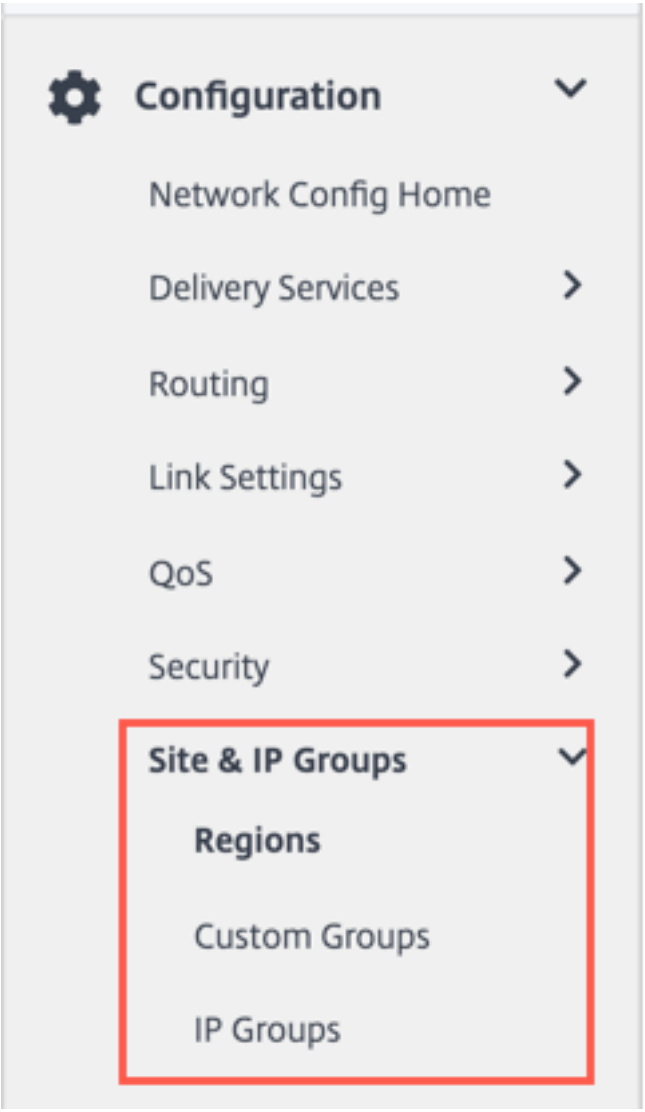

## Grupos de sitios y IP

October 31, 2022

Los administradores pueden agrupar sitios o direcciones IP para simplificar las directivas de aplicaciones comunes en varios sitios o direcciones de red, y también servir como filtros para los informes.

Para ver las regiones, los sitios y los grupos IP, vaya a **Configuración** > **Grupos de sitios e IP**.

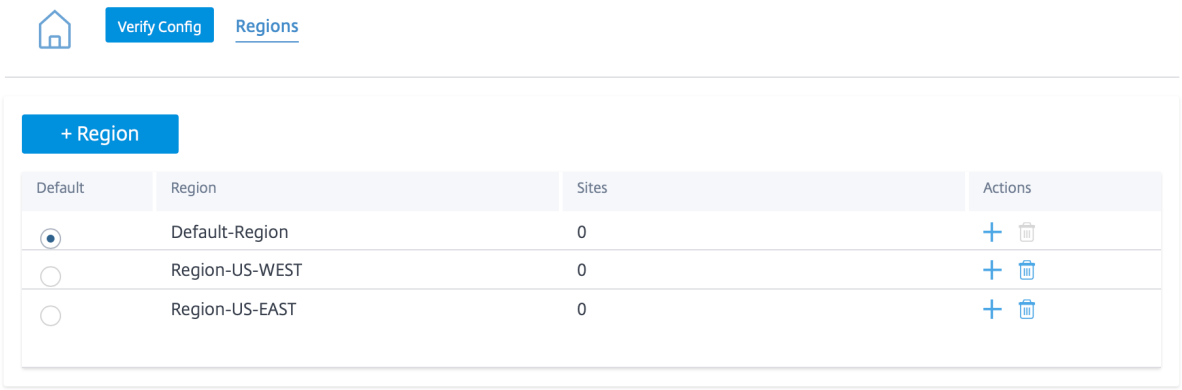
 




### Regiones

Las regiones ayudan a crear límites administrativos dentro de redes grandes que abarcan cientos a miles de sitios. Si su organización tiene una red grande que abarca varios límites administrativos (o geográficos), puede considerar la posibilidad de crear regiones para segmentar la red.




Actualmente, se admite un máximo de 1000 sitios por región. Se espera que cada región tenga un nodo de control regional (RCN), que sirve como hub y Controller para la región. Por lo tanto, normalmente consideraría una implementación de varias regiones si su red tiene más de 500 sitios. De forma predeterminada, todas las redes son redes de una sola región, donde el nodo de control maestro (MCN) sirve como concentrador y nodo de control para todos los sitios. Al agregar una o más regiones, la red se convierte en una red de varias regiones. La región asociada al MCN se denomina **región predeterminada**.

Una red multiregión admite una arquitectura jerárquica con un MCN que controla varios RCNs. Cada RCN, a su vez, controla varios sitios de sucursal. Incluso en una implementación de varias regiones, puede hacer que el MCN se doble como nodo concentrador directo para un subconjunto de los sitios mientras que el resto de los sitios utilizan sus respectivos RCNs como nodos de concentrador.

Se dice que los sitios que administra directamente el MCN, es decir, los RCN y, posiblemente, algunos otros sitios administrados directamente por el MCN se encuentran en la región **predeterminada**. La **región predeterminada** sería la única región de una red antes de que se agreguen otras regiones. Después de agregar otras regiones, puede seleccionar la opción **Predeterminada** para utilizar la región deseada como región predeterminada.

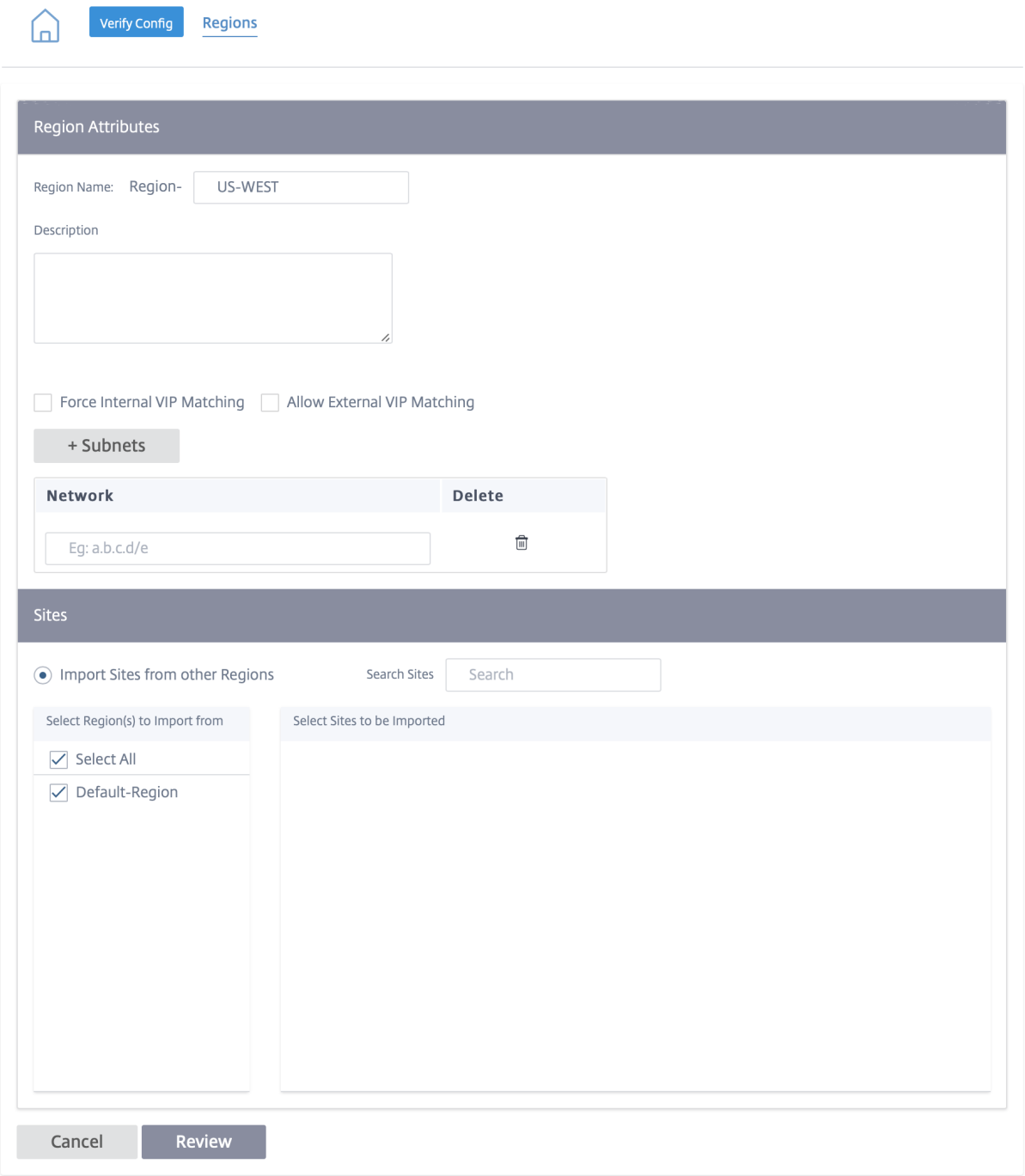
Para crear una región:

1. Haga clic en **+ Región**. Proporcione un nombre de región y una descripción.
2. Habilite la coincidencia VIP de intervalo según si quiere **Coincidencia VIP interna forzada** o **Permitir Coincidencia VIP externa**.
    - Coincidencia VIP interna forzada: Cuando está habilitada, todas las direcciones IP virtuales no privadas de la región están obligadas a coincidir con las subredes configuradas.
    - Coincidencia de VIP externa permitida: Cuando está habilitada, se permite que las direcciones IP virtuales no privadas de otras regiones coincidan con las subredes configuradas.
3. Haga clic en **+ Subredes** para agregar subredes. Introduzca una dirección **de red**. La dirección de red es la dirección IP y la máscara de la subred.

4. Seleccione los sitios.
5. Haga clic en **Revisar** y luego en **Guardar** La región recién creada se agrega a la lista de regiones existente.

> **Nota**
>
> Un cliente solo puede tener rutas virtuales estáticas o dinámicas dentro de una región.



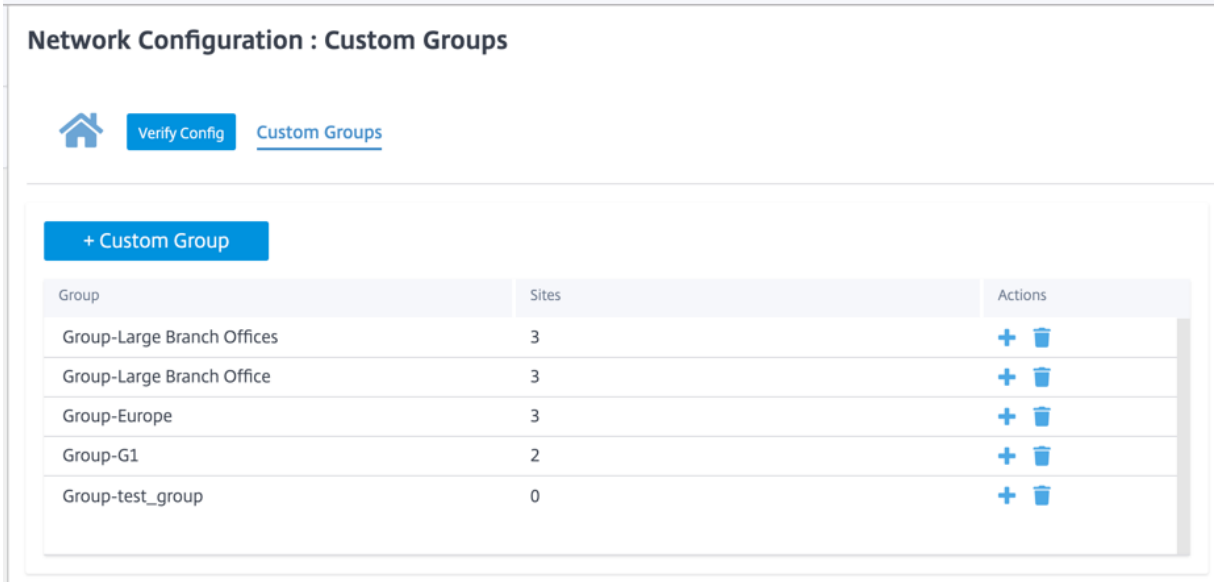
Puede colocar sitios debajo de la región una vez que se haya creado correctamente una región.

> **Nota**
>
> Las rutas virtuales dinámicas no se pueden establecer entre sucursales de diferentes regiones.

Haga clic en **Verificar configuración** para validar cualquier error de auditoría.

### Grupos personalizados

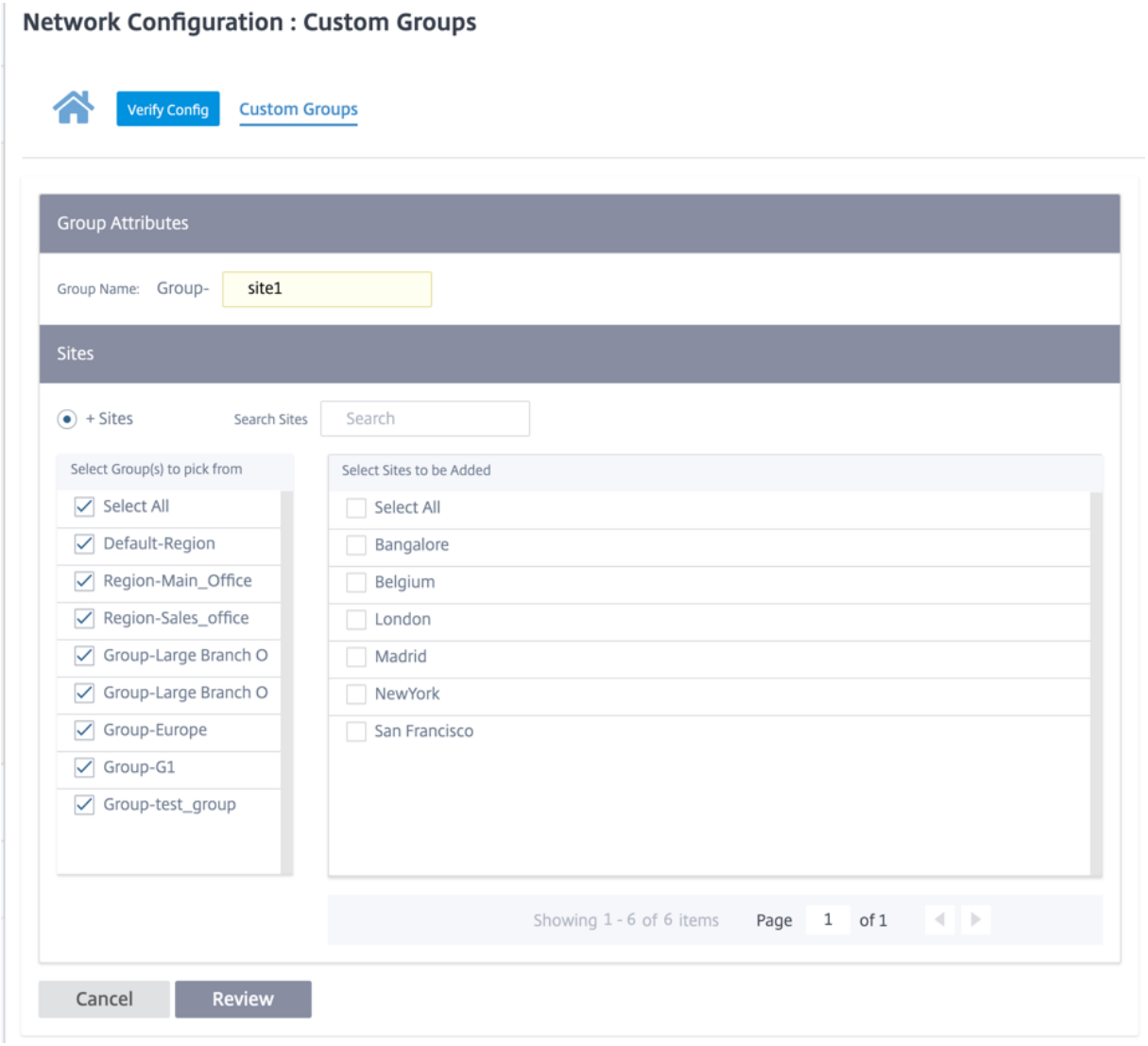
Los**grupos personalizados** ofrecen a los usuarios la flexibilidad de agrupar sitios según sea necesario. Los usuarios pueden aplicar directivas para grupos de sitios a la vez, sin tener que tratar necesariamente cada sitio de forma individual. Los grupos también pueden servir como filtros para paneles, informes o configuración de red. A diferencia de las Regiones, los grupos pueden superponerse en términos de sitios. En otras palabras, los mismos sitios pueden formar parte de varios grupos.




Por ejemplo, un usuario puede crear un grupo denominado **Business Critical Sites** para configurar directivas comunes para todos los sitios críticos para la empresa. El usuario también puede supervisar su estado y rendimiento por separado como grupo. Algunos de esos sitios también pueden formar parte de un grupo de **sucursales grandes**, por ejemplo.

**Los grupos de sitios personalizados** proporcionan una forma de agrupar sitios de forma lógica con fines de elaboración de informes. Puede crear grupos personalizados y agregar sitios a cada grupo personalizado. Para crear un grupo personalizado, haga clic en **+ Grupo personalizado**. Proporcione un nombre de grupo y seleccione o agregue sitios. Haga clic en **Revisar** y luego en **Guardar**



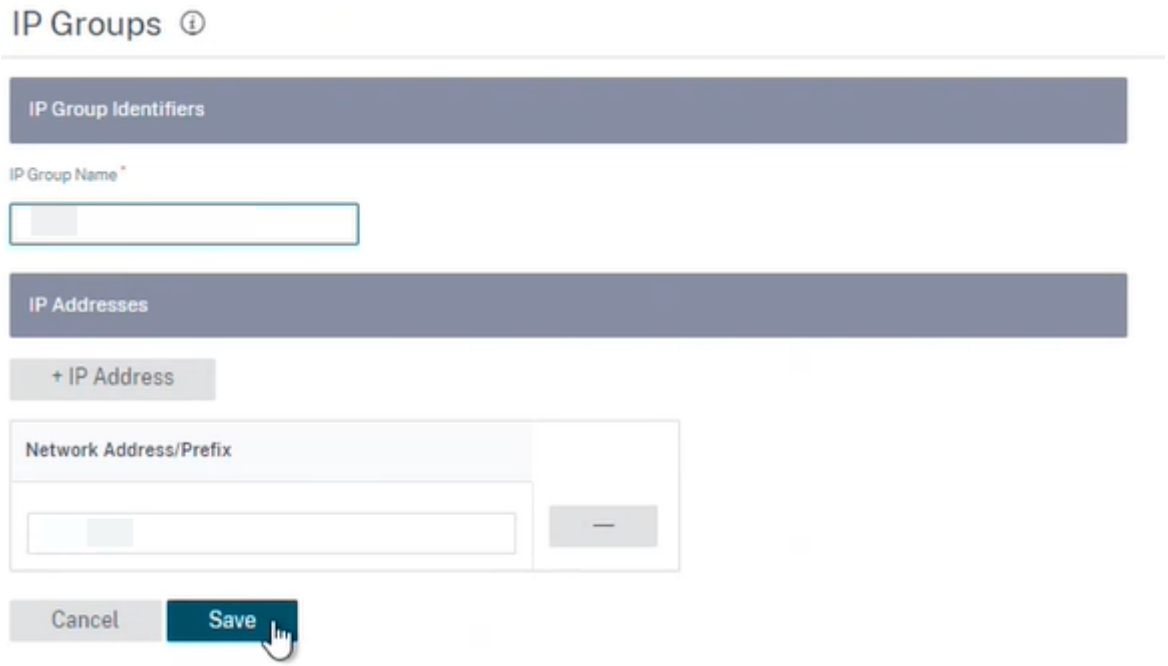

Haga clic en **Verificar configuración** para validar cualquier error de auditoría.

## Grupos IP

El servicio Citrix SD-WAN Orchestrator presenta la opción de agregar grupos IP (objetos de red). Con esta opción, puede agrupar las direcciones IP y de red mediante **grupos de IP** y, al mismo tiempo, definir un filtro de ruta en lugar de crear un filtro para cada subred. Estos grupos se pueden usar en la configuración y las directivas según sea necesario, sin tener que escribir necesariamente direcciones IP individuales cada vez.


Puede crear grupos de IP y agregar direcciones y prefijos de red. Para crear un grupo IP, seleccione **Grupos IP** y haga clic en **+ Grupo IP**. Proporcione un nombre de grupo. Haga clic en **+ Dirección IPe introduzca las direcciones IP** que quiere agregar al grupo IP.

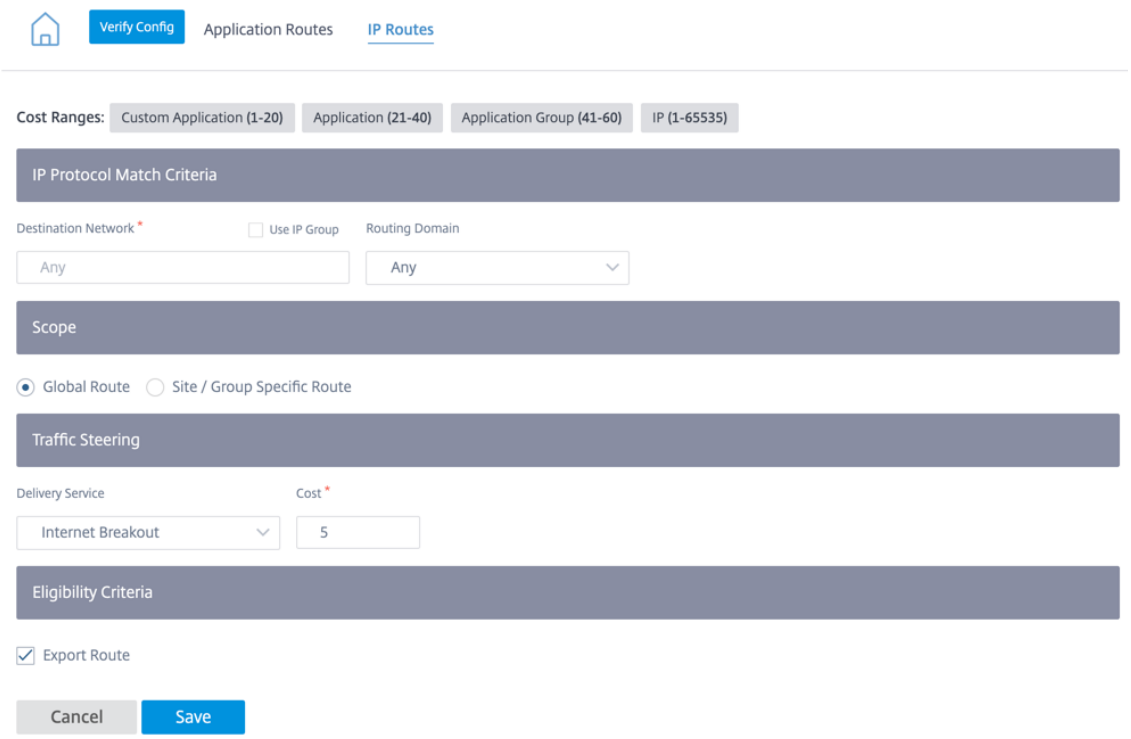



Haga clic en **Verificar configuración** para validar cualquier error de auditoría

Las siguientes funciones utilizan los grupos de IP:

- **Crear una ruta IP**: Puede agregar una red de destino o activar la casilla **Usar grupo IP** para seleccionar un grupo de IP existente. Para obtener más información, consulte Grupos de direcciones IP.

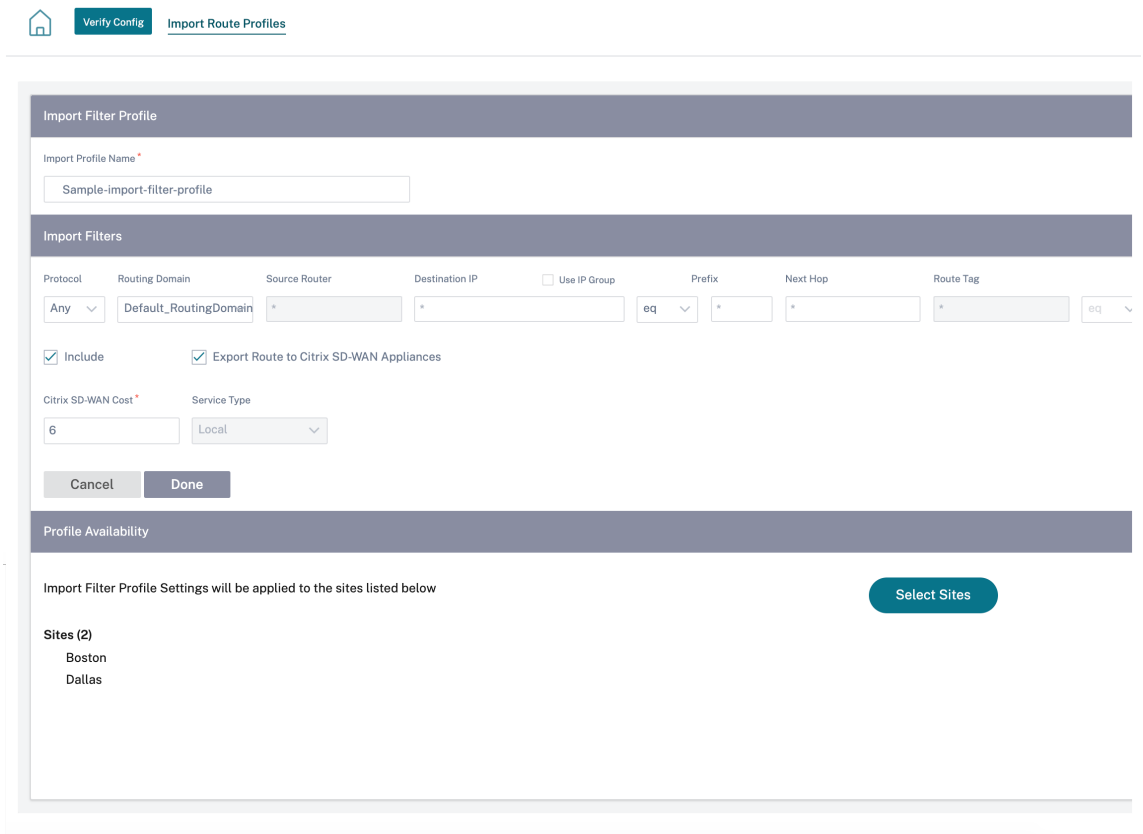



- **Importar perfiles de ruta**: Al crear un perfil de filtro de importación, puede elegir de la lista de grupos IP disponibles en su red.

  Puede agregar una red de destino o activar la casilla **Usar grupo IP** para seleccionar un grupo de IP existente.

  Para obtener más información, consulte Importar perfiles de ruta.

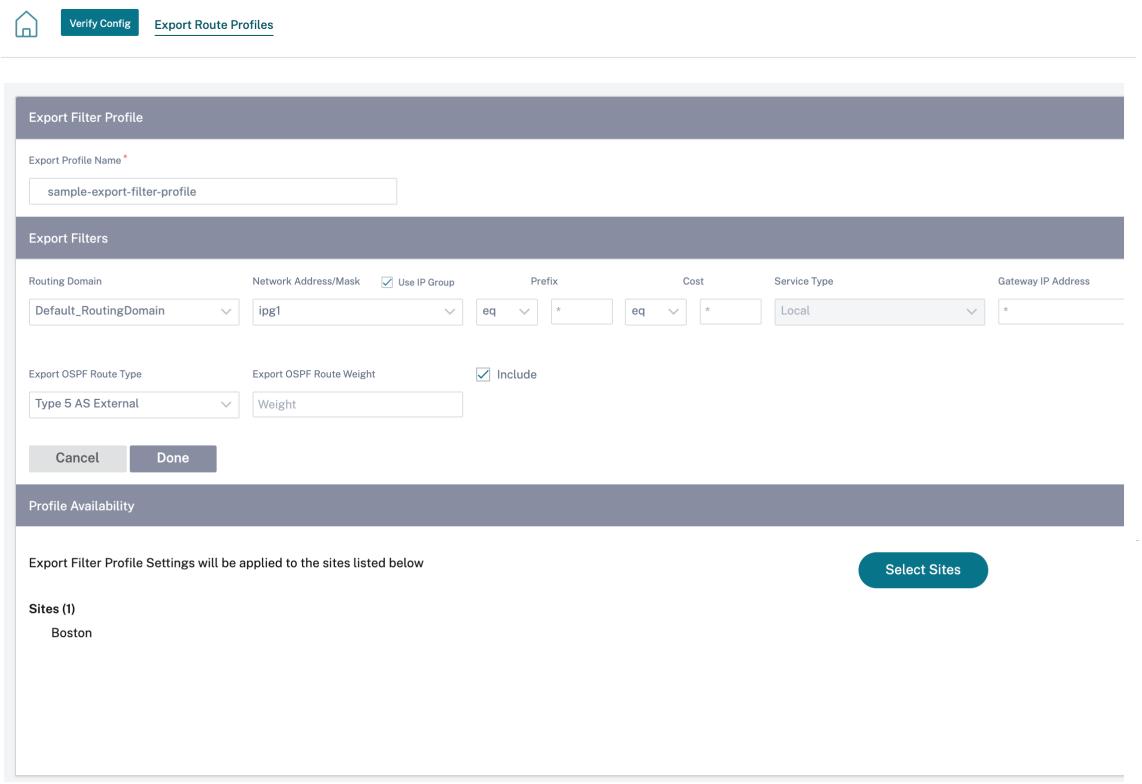
 




- **Exportar perfiles de ruta**: Al crear un perfil de filtro de exportación, puede agregar una máscara de dirección de red o activar la casilla **Usar grupo de IP** para seleccionar un grupo de IP existente.

  Para obtener más información, consulte Exportar perfiles de ruta.

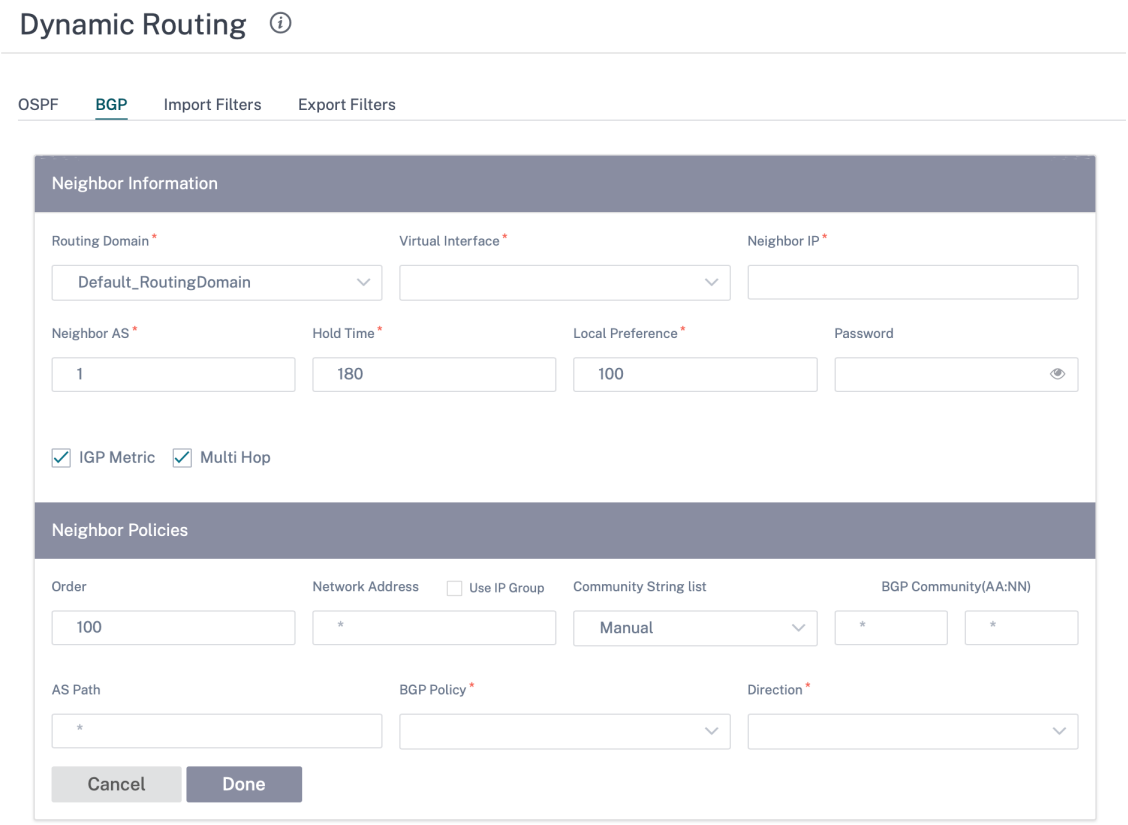
 




- **Directivas de vecinos de BGP**: Al agregar una directiva de BGP configurada para los enrutadores vecinos, puede agregar una dirección de red o activar la casilla **Usar grupo de IP** para seleccionar un grupo de IP existente.

  Para obtener más información, consulte BGP.




## Configuración y grupos de aplicaciones

October 31, 2022

Esta sección permite a los usuarios definir aplicaciones personalizadas, agrupar aplicaciones para su uso en directivas, perfiles QoS y también configuración DNS.

Puede definir un **grupo de aplicaciones** para aplicaciones predefinidas y personalizadas. Un **grupo** de aplicaciones contiene aplicaciones que necesitan un tratamiento similar al definir una directiva de seguridad.

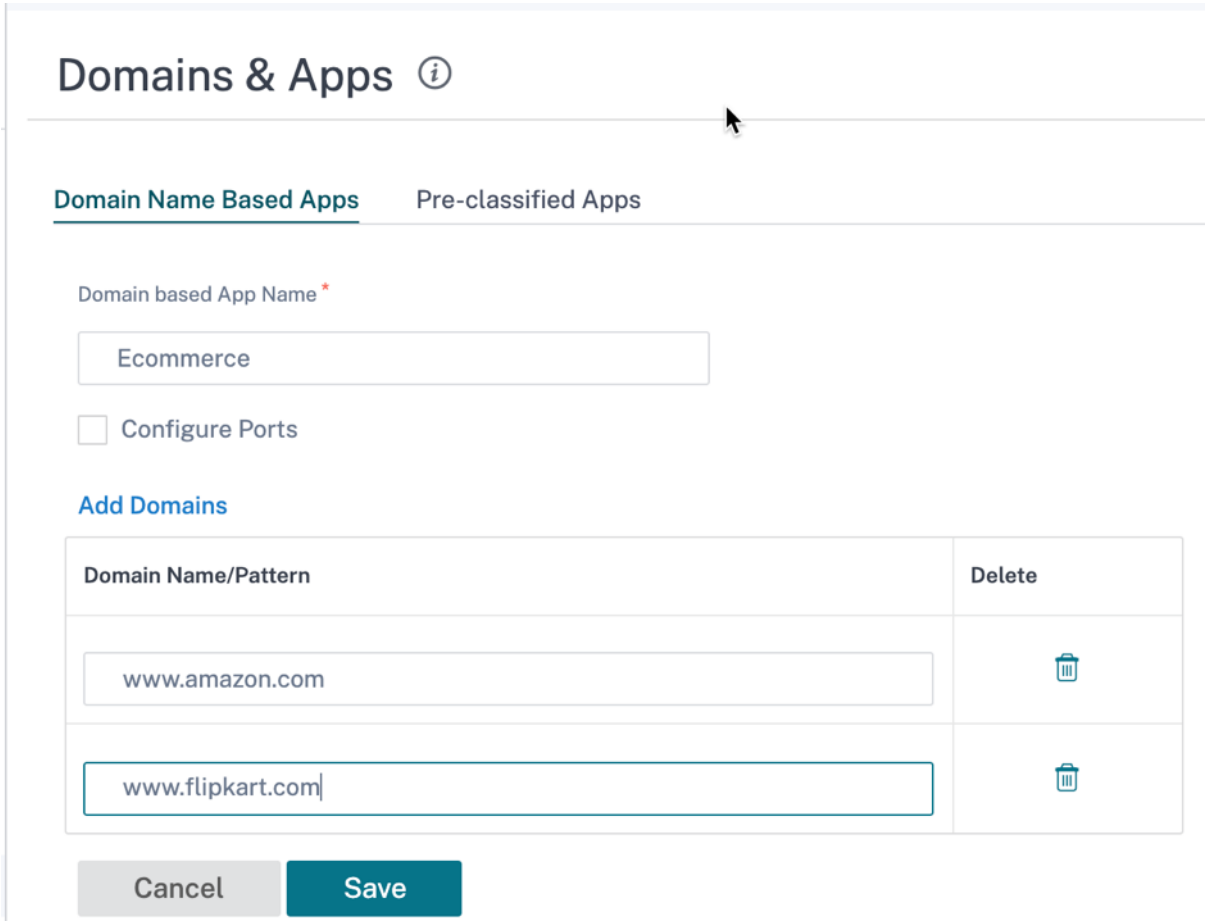
Puede reutilizar los **grupos de aplicaciones** con frecuencia al definir directivas, como la dirección de aplicaciones o las reglas de firewall. Elimina la necesidad de crear varias entradas para cada aplicación individual. Del mismo modo, al utilizar cualquier servicio de aplicaciones, los grupos de aplicaciones admiten aplicaciones comunes con un nombre único para una reutilización simplificada y coherente.

Para ver **los grupos de aplicaciones**, vaya a **Configuración > Configuración y grupos de aplicaciones**.

### Dominios y aplicaciones

Puede crear aplicaciones internas basadas en nombres de dominio que no están disponibles en la lista de aplicaciones publicadas de la página **Dominios y aplicaciones**. Para crear aplicaciones basadas en el nombre de dominio, al nivel de red, vaya a **Configuración y grupos de aplicaciones > Dominios y aplicaciones > ficha Aplicaciones basadas en nombres de dominio** y haga clic en **Nueva aplicación basada en nombres de dominio**. Introduzca el nombre de la aplicación y agregue los nombres o patrones de dominio. Puede introducir el nombre de dominio completo o utilizar comodines al principio.




Todas las aplicaciones basadas en nombres de dominio están visibles en las **directivas de**enrutamiento**de**aplicaci reglas**de aplicación y firewall**.

A partir de la versión 11.4.2 de Citrix SD-WAN, la opción **Configurar puertos** está disponible **en Aplicaciones basadas en nombres de dominio**. Cuando la casilla **Configurar puertos** está habilitada, presenta la flexibilidad de configurar un grupo de varios puertos, rangos de puertos y un protocolo (TCP/UDP/cualquiera) para la aplicación basada en el dominio.

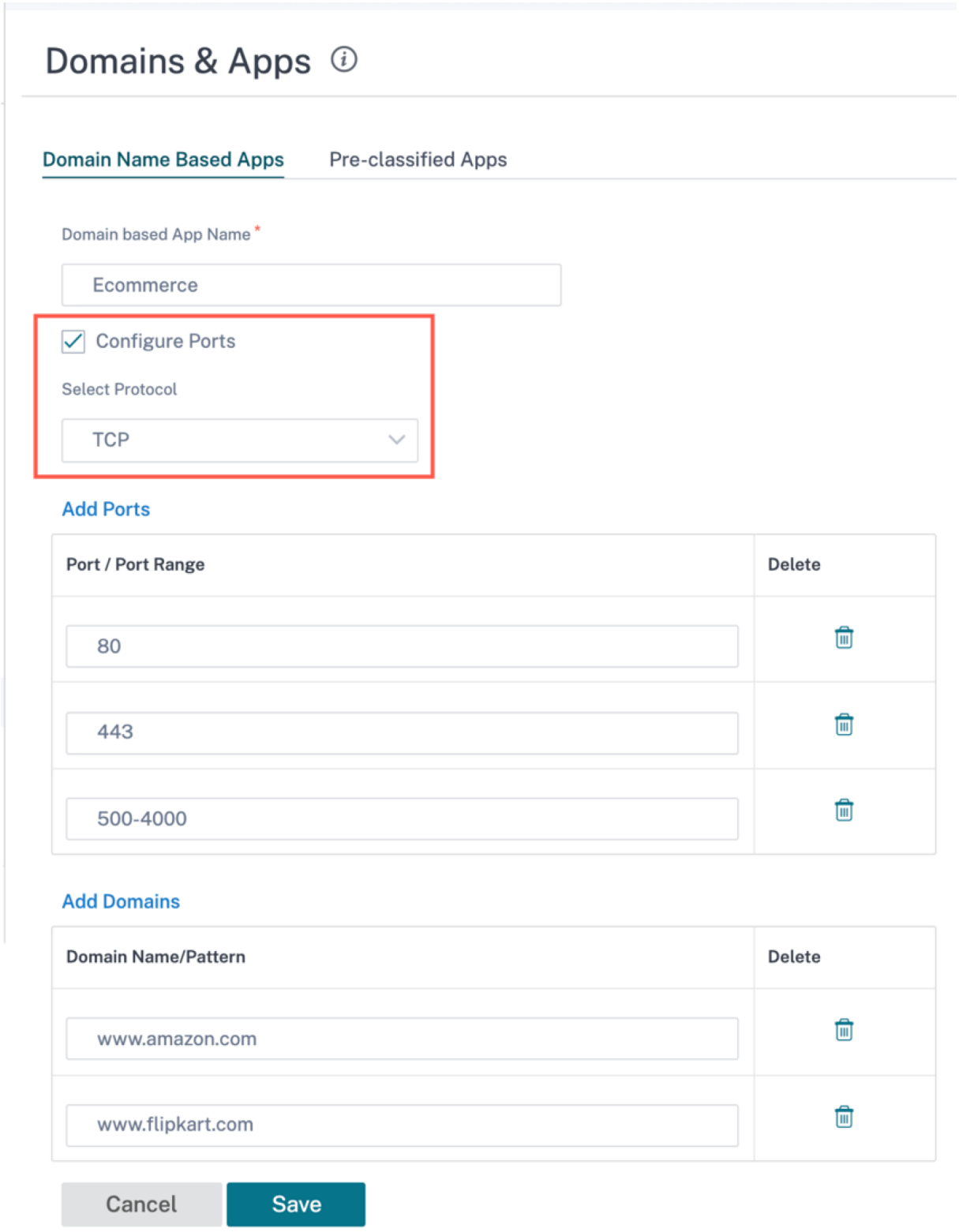
Anteriormente, los puertos **80** y **443**y el protocolo **Any** eran compatibles con los dominios agrupados en una aplicación. Puede ver el mismo comportamiento si la casilla **Configurar puertos** está desac-

tivada. De forma predeterminada, la casilla **Configurar puertos** está inhabilitada.

Al seleccionar la casilla **Configurar puerto**, puede modificar, agregar o eliminar cualquier puerto o rango de puertos según sea necesario, junto con la selección de protocolos como TCP, UDP o Cualquiera. De forma predeterminada, el valor del protocolo se establece en **Cualquiera** y los puertos se establecen en **80** y **443**.

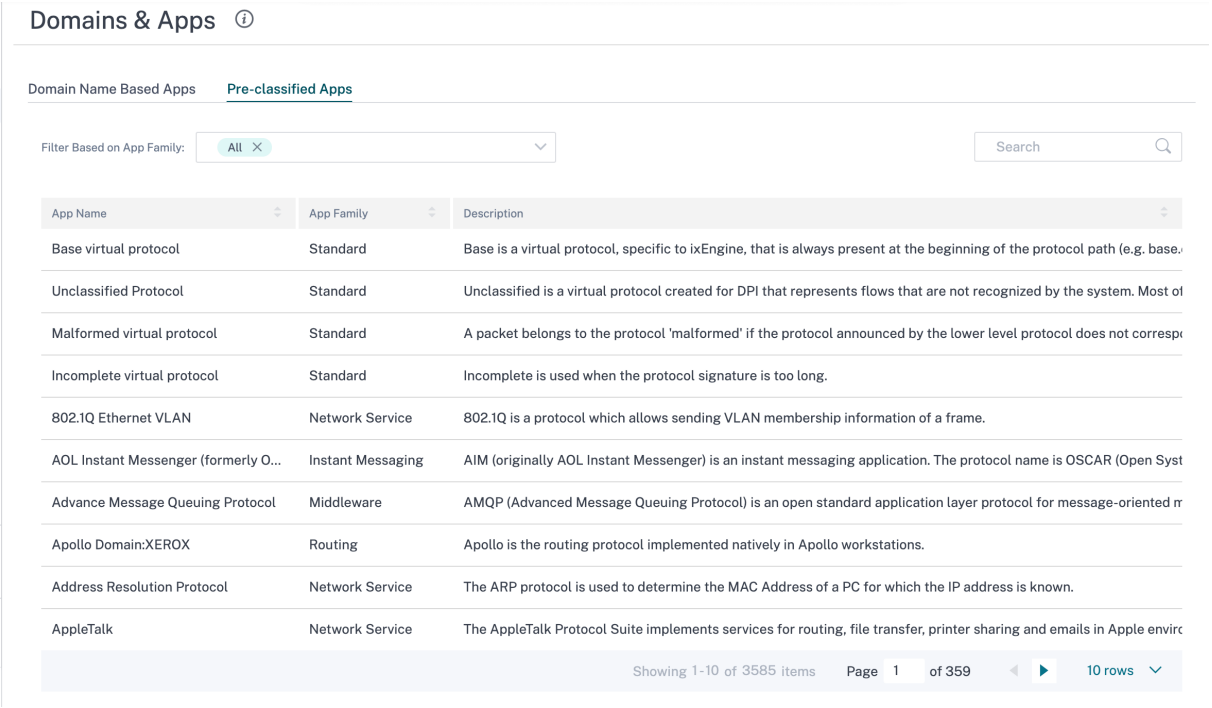
 




También puede ver la lista de aplicaciones predefinidas en la ficha **Aplicaciones preclasificadas**.

Puede buscar una aplicación específica mediante la barra de **búsqueda** o filtrar la lista según la familia de aplicaciones.

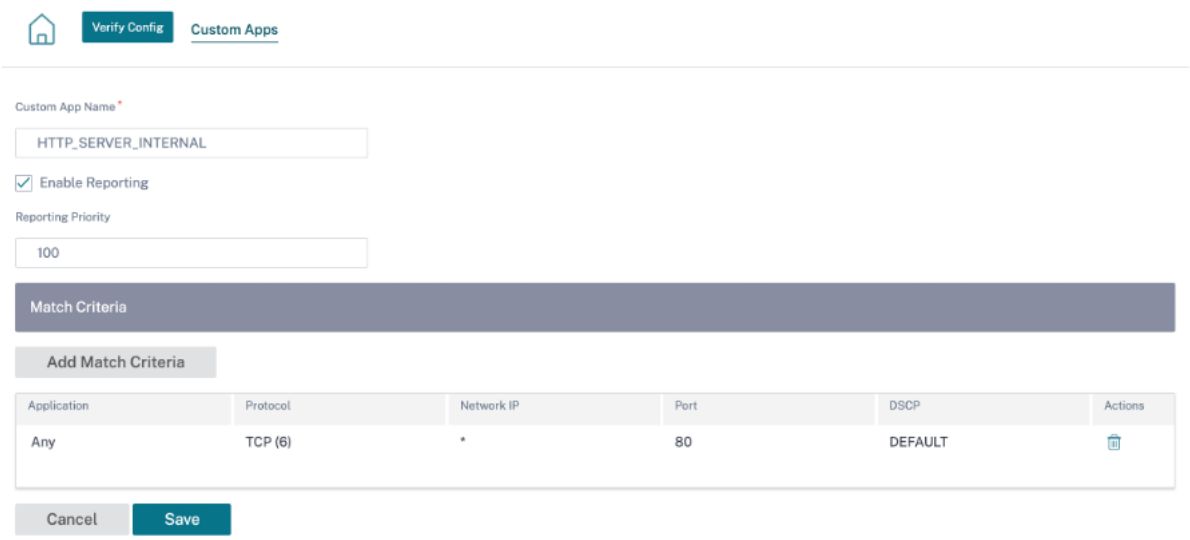



## Aplicación personalizada

**Las aplicaciones personalizadas** se utilizan para crear aplicaciones internas o combinaciones de puertos IP que no están disponibles en la lista de aplicaciones publicadas. El administrador debe definir una aplicación personalizada basada en el protocolo IP que se pueda utilizar en varias directivas según sea necesario, sin consultar los detalles de la dirección IP y el número de puerto cada vez.

Para crear una aplicación personalizada, en el nivel de red, vaya a **Configuración y grupos de aplicaciones > Aplicaciones personalizadas**, haga clic en **+ Aplicación personalizada** y escriba un nombre para la aplicación personalizada. Especifique los criterios de coincidencia, como el protocolo IP, la dirección IP de la red, el número de puerto y la etiqueta DSCP. El flujo de datos que coincide con este criterio se agrupa como la aplicación personalizada.



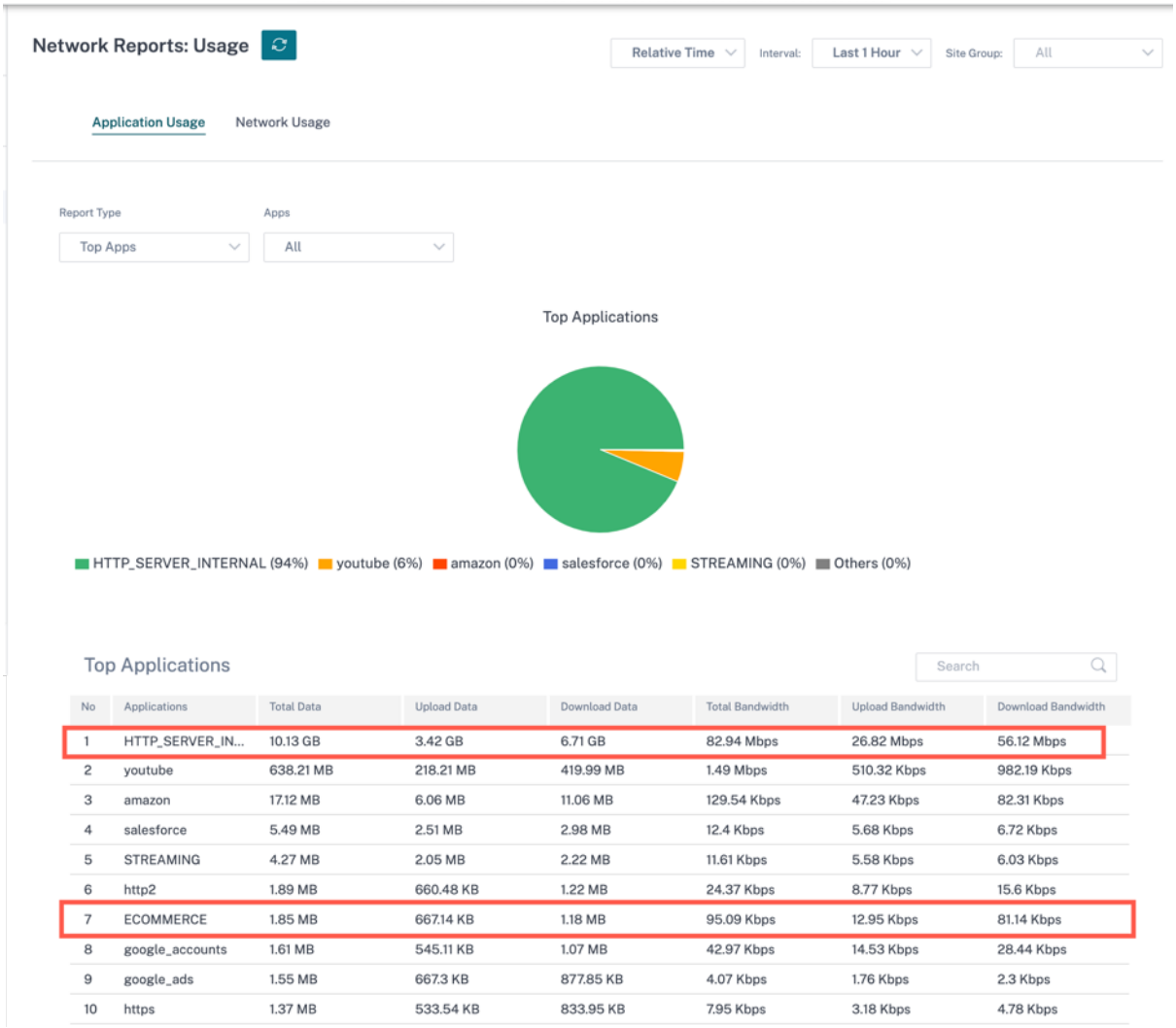

Una vez guardadas, las aplicaciones personalizadas aparecen en una lista y se pueden modificar o eliminar, según sea necesario.

Se agrega la casilla de verificación **Habilitar informes** para las aplicaciones y grupos de aplicaciones personalizados basados en el protocolo IP. Debe seleccionar la casilla **Activar informes** e indicar la prioridad de los informes.

Cuando se selecciona la casilla **Habilitar informes**, puede ver el tráfico de la aplicación IP personalizada en **Informes** > **Uso**.

La prioridad de los informes es el orden en que se seleccionan las aplicaciones o grupos de aplicaciones personalizados basados en el protocolo IP para los informes. Es útil elegir la aplicación personalizada de alta prioridad o el grupo de aplicaciones para la elaboración de informes, cuando hay varias coincidencias con la generación de informes habilitada. Por ejemplo, si la prioridad de informes de una aplicación personalizada se establece en 1, significa que la aplicación personalizada tiene la prioridad más alta en los informes. Mientras que si la prioridad de informes se establece en 100, la aplicación personalizada tiene una prioridad mucho menor en los informes.



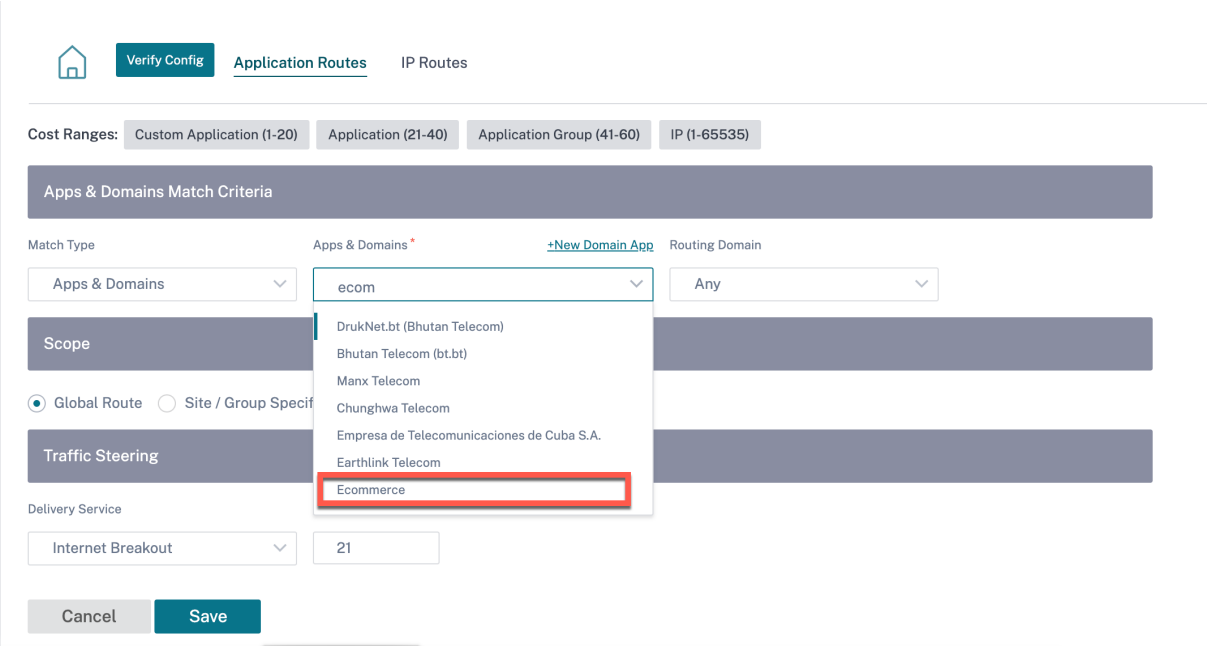

| No | Applications | Total Data | Upload Data | Download Data | Total Bandwidth | Upload Bandwidth | Download Bandwidth |
|---|---|---|---|---|---|---|---|
| 1 | HTTP_SERVER_IN... | 10.13 GB | 3.42 GB | 6.71 GB | 82.94 Mbps | 26.82 Mbps | 56.12 Mbps |
| 2 | youtube | 638.21 MB | 218.21 MB | 419.99 MB | 1.49 Mbps | 510.32 Kbps | 982.19 Kbps |
| 3 | amazon | 17.12 MB | 6.06 MB | 11.06 MB | 129.54 Kbps | 47.23 Kbps | 82.31 Kbps |
| 4 | salesforce | 5.49 MB | 2.51 MB | 2.98 MB | 12.4 Kbps | 5.68 Kbps | 6.72 Kbps |
| 5 | STREAMING | 4.27 MB | 2.05 MB | 2.22 MB | 11.61 Kbps | 5.58 Kbps | 6.03 Kbps |
| 6 | http2 | 1.89 MB | 660.48 KB | 1.22 MB | 24.37 Kbps | 8.77 Kbps | 15.6 Kbps |
| 7 | ECOMMERCE | 1.85 MB | 667.14 KB | 1.18 MB | 95.09 Kbps | 12.95 Kbps | 81.14 Kbps |
| 8 | google_accounts | 1.61 MB | 545.11 KB | 1.07 MB | 42.97 Kbps | 14.53 Kbps | 28.44 Kbps |
| 9 | google_ads | 1.55 MB | 667.3 KB | 877.85 KB | 4.07 Kbps | 1.76 Kbps | 2.3 Kbps |
| 10 | https | 1.37 MB | 533.54 KB | 833.95 KB | 7.95 Kbps | 3.18 Kbps | 4.78 Kbps |

**Nota**

- Para utilizar una aplicación basada en nombres de dominio, **las aplicaciones y los dominios** deben figurar como criterios de coincidencia al crear la ruta de la aplicación, la directiva de QoS y la directiva de firewall.
- Para utilizar una aplicación personalizada, la **aplicación personalizada** debe figurar como criterio de coincidencia al crear la ruta de la aplicación, la directiva de QoS y la directiva de firewall.

Una vez que haya creado la aplicación personalizada, para realizar el enrutamiento de la aplicación, vaya a **Enrutamiento > Directivas de enrutamiento > + Ruta de aplicación**y seleccione **Aplicación personalizada** en la lista desplegable **Tipo de coincidencia**. Del mismo modo, para la aplicación basada en nombres de dominio, seleccione **Aplicaciones y dominios** en la lista desplegable **Tipo de coincidencia**.

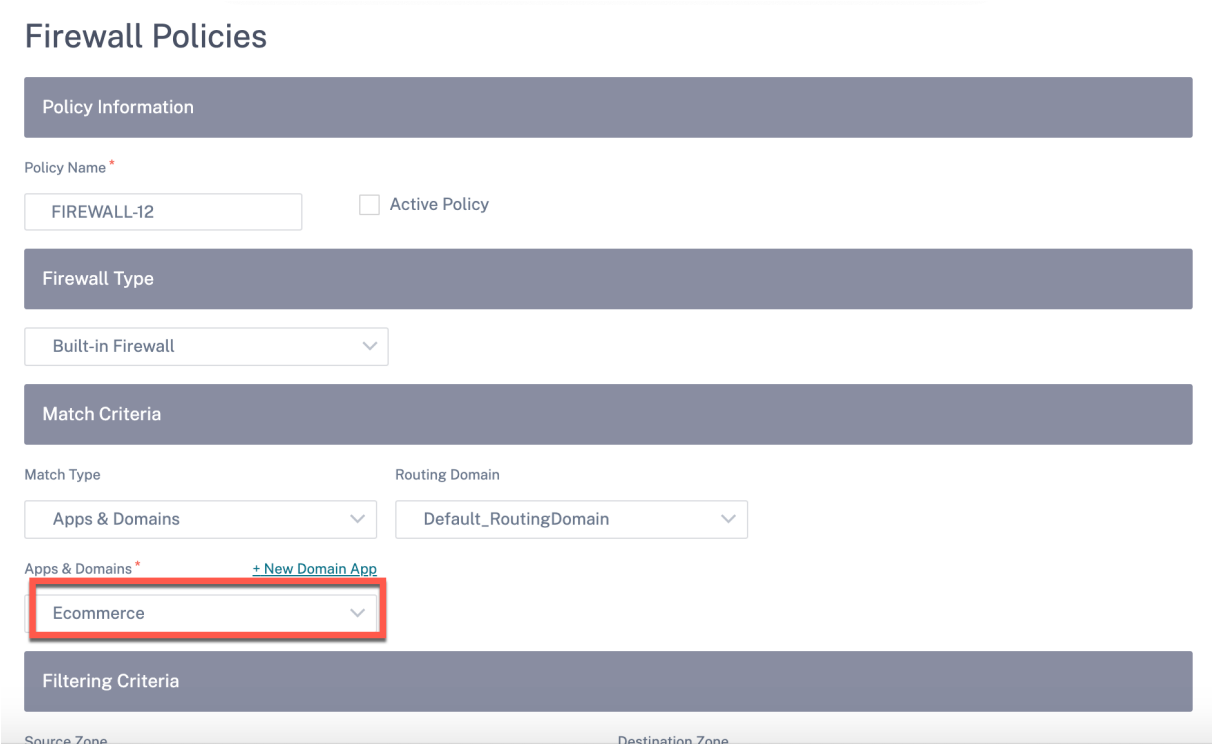
 




También puede seleccionar una aplicación basada en nombres de dominio según los criterios de coincidencia al crear una aplicación personalizada de **protocolo IP**.

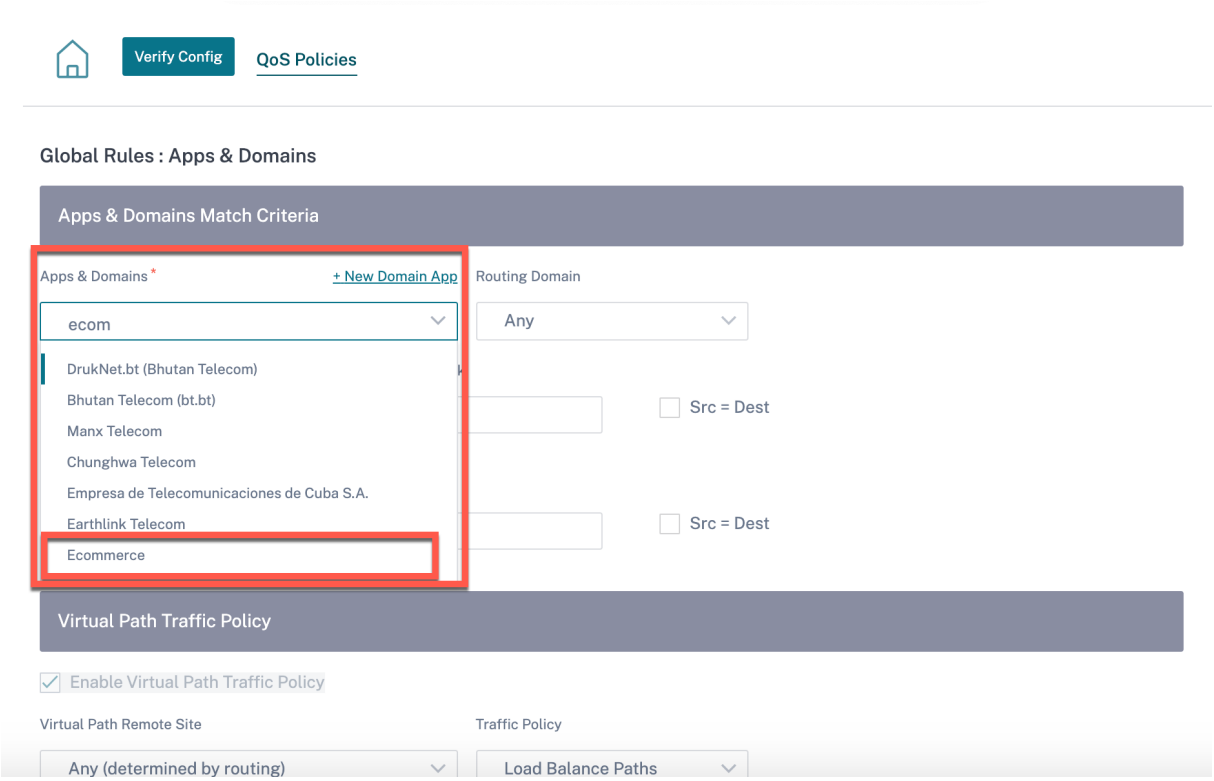

Del mismo modo, para ver la aplicación personalizada en las **Directivas de firewall**, vaya a **Seguridad > Directivas de firewall**. La aplicación se puede utilizar para cualquier tipo de directiva (anulación global/directivas específicas del sitio/directivas globales). Haga clic en **Crear nueva regla** y, en **Criterios de coincidencia**, seleccione **Aplicación personalizada** en la lista desplegable **Tipo de coincidencia**. Para ver la aplicación basada en nombres de dominio, seleccione **Aplicaciones y dominios** en la lista desplegable **Tipo de coincidencia**.




Puede ver las aplicaciones personalizadas basadas en nombres de dominio tanto en la regla **global como en la regla específica del sitio o grupo**. Para ver las aplicaciones basadas en nombres de dominio, vaya a **QoS > Directivas de QoS > Reglas globales > Regla de aplicación > + Regla**de aplicación y seleccione la aplicación basada en nombres de dominio requerida en la lista desplegable **Aplicaciones y dominios**. Para ver las aplicaciones personalizadas, vaya a **QoS > Directivas de QoS > Reglas globales > Reglas de aplicación personalizadas > + Regla de aplicación**personalizada y seleccione la aplicación personalizada requerida en la lista desplegable **Aplicaciones personalizadas**.

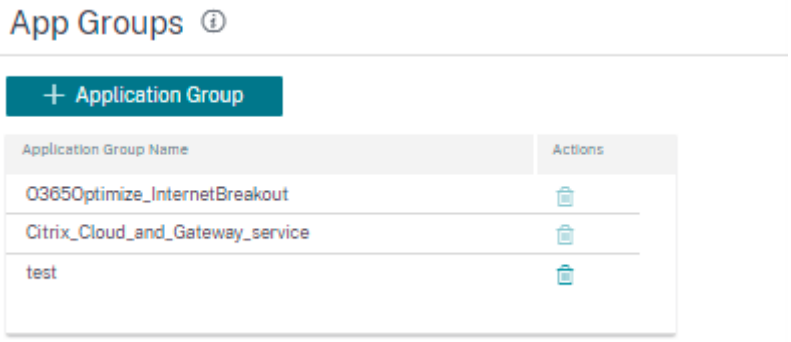
 




Haga clic en **Verificar configuración** para validar cualquier error de auditoría.

## Grupos de aplicaciones

Un **grupo de aplicaciones** ayuda a los administradores a agrupar aplicaciones similares para usarlas en directivas comunes, sin tener que crear necesariamente una directiva para cada aplicación individual.

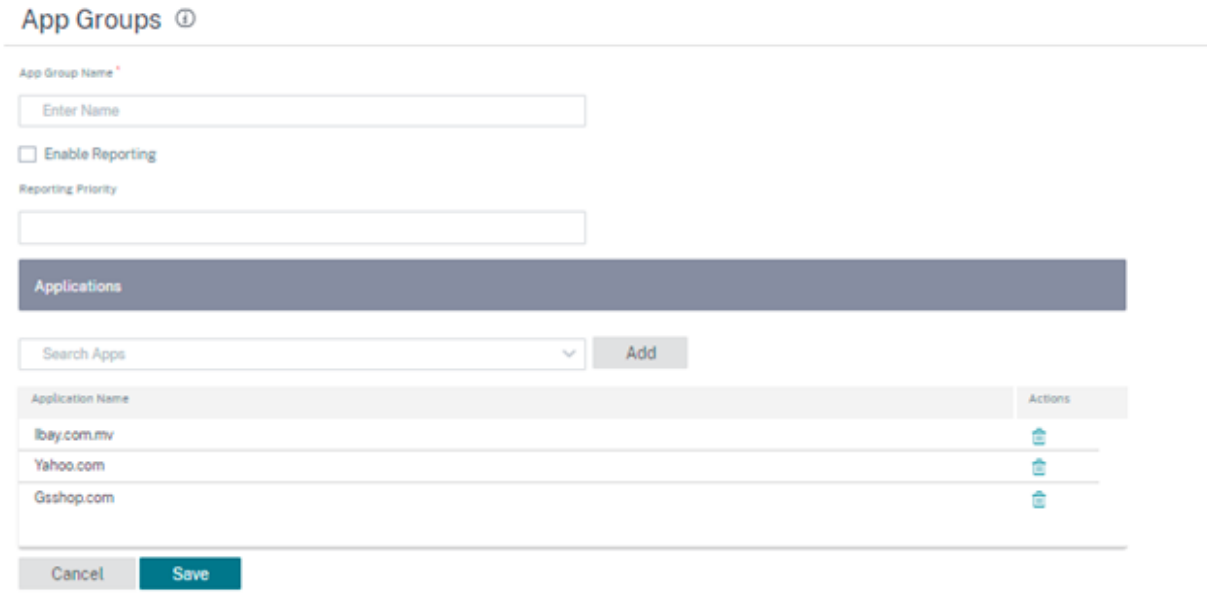



Puede crear un **grupo de aplicaciones** mediante la opción **Agregar grupos de aplicaciones**. Puede hacer referencia al mismo grupo de aplicaciones mientras crea una directiva según el rol de aplicación. La directiva que se define para el grupo en particular se aplica a cada aplicación que coincida con la categoría específica.

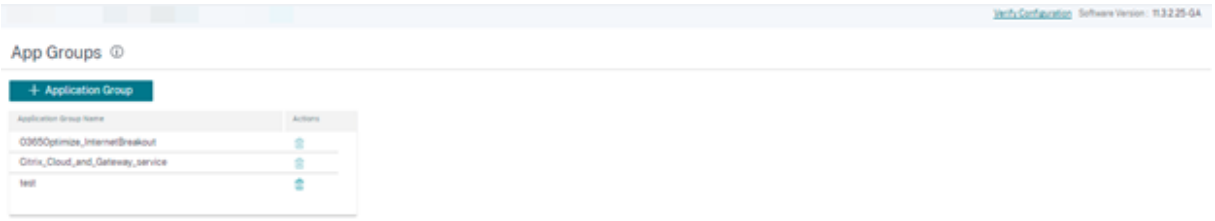
 

Por ejemplo, puede crear un **grupo de aplicaciones** como **redes sociales** y agregar redes sociales como Facebook, LinkedIn y Twitter al grupo para definir determinadas directivas para las aplicaciones de redes sociales.

Para crear un **grupo de aplicaciones**, especifique un nombre de grupo, busque y agregue aplicaciones en la lista de **aplicaciones**.
Siempre puede volver atrás y modificar su configuración o eliminar el **grupo de aplicaciones** según sea necesario.



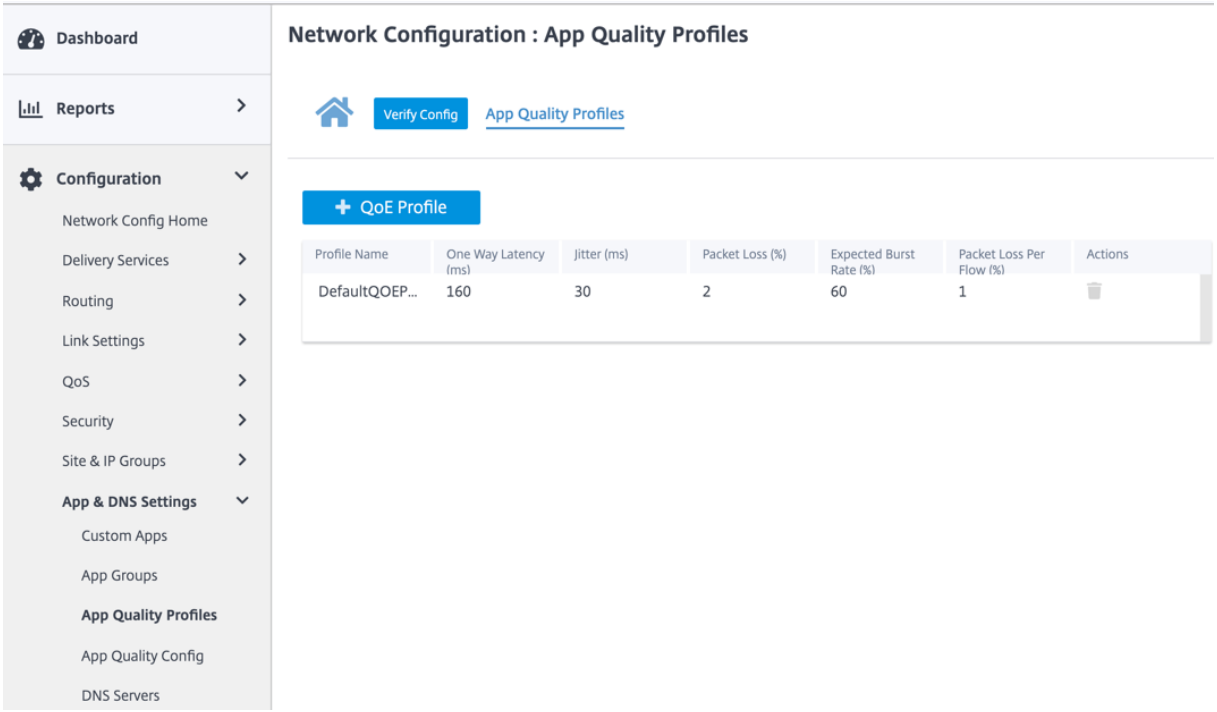

Haga clic en **Verificar configuración** en la página **Configuración** > **Configuración y grupos** de **aplicaciones > Grupos** de aplicaciones para validar cualquier error de auditoría.




## Perfiles de calidad de aplicaciones

Esta sección permite ver y crear perfiles de calidad de aplicaciones.




La**QoE de la aplicación** es una medida de calidad de experiencia de aplicaciones en la red SD-WAN. Mide la calidad de las aplicaciones que fluyen por las rutas virtuales entre dos dispositivos SD-WAN.

La puntuación QoE de la aplicación es un valor entre 0 y 10. El rango de puntuación en el que cae determina la calidad de una aplicación.

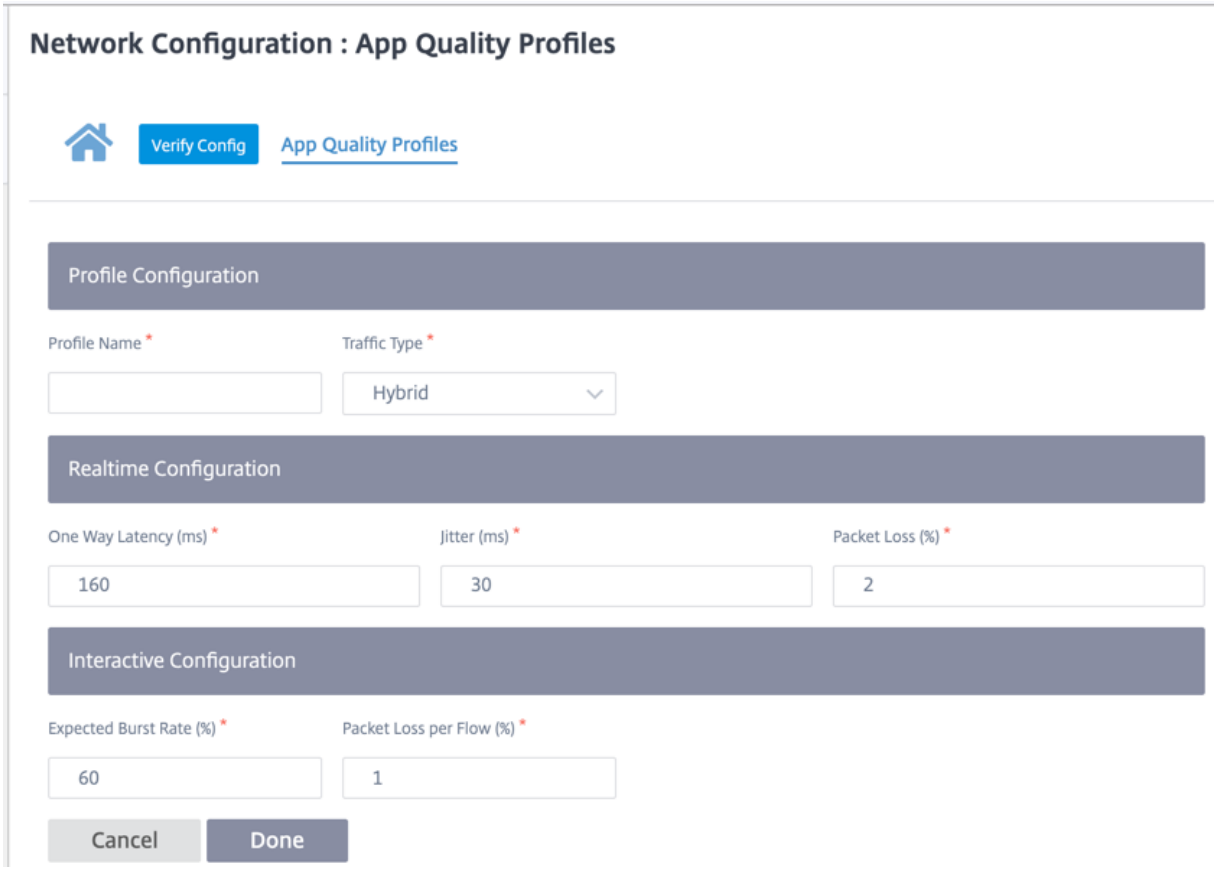
| Calidad | Rango |
|---|---|
| Bueno | 8–10 |
| Normal | 4–8 |
| Mala | 0–4 |

La puntuación QoE de la aplicación se puede utilizar para medir la calidad de las aplicaciones e identificar tendencias problemáticas.

### Configuración del perfil

Haga clic en **+ Perfil de QoE** para crear un perfil de QoE, especificar un nombre de perfil y seleccionar un tipo de tráfico de la lista desplegable.




**Configuración en tiempo real**

Puede definir los umbrales de calidad de los dispositivos interactivos y en tiempo real mediante perfiles QoE y asignar estos perfiles a aplicaciones u objetos de aplicaciones.

El cálculo de QoE de la aplicación para aplicaciones en tiempo real utiliza una técnica innovadora de Citrix, que se deriva de la puntuación MOS.

Los valores de umbral predeterminados son:

- Umbral de latencia (ms): 160
- Umbral de fluctuación (ms): 30
- Umbral de pérdida de paquetes (%):.

Un flujo de una aplicación en tiempo real que cumple los umbrales de latencia, pérdida y fluctuación se considera de buena calidad.

La QoE para aplicaciones en tiempo real se determina a partir del porcentaje de flujos que cumplen el umbral dividido por el número total de muestras de flujo.

QoE para tiempo real = (Número de muestras de flujo que cumplen el umbral/Número total de muestras de flujo) * 100

Se representa como puntuación QoE que va de 0 a 10.

#### Configuración interactiva

La QoE de aplicaciones para aplicaciones interactivas utiliza una técnica innovadora de Citrix basada en umbrales de pérdida de paquetes y velocidad de ráfaga.

Las aplicaciones interactivas son sensibles a la pérdida de paquetes y al rendimiento. Por lo tanto, medimos el porcentaje de pérdida de paquetes y la tasa de ráfagas del tráfico de entrada y salida en un flujo.

Los umbrales configurables son:

- Porcentaje de pérdida de paquetes.
- Porcentaje de la tasa de ráfaga de salida esperada en comparación con la tasa de ráfaga de entrada.

Los valores de umbral predeterminados son:

- Umbral de pérdida de paquetes: 1%
- Velocidad de ráfaga: 60%

Un flujo es de buena calidad si se cumplen las siguientes condiciones:

- El porcentaje de pérdida de un flujo es inferior al umbral configurado.
- La velocidad de ráfaga de salida es al menos el porcentaje configurado de la velocidad de ráfaga de entrada.

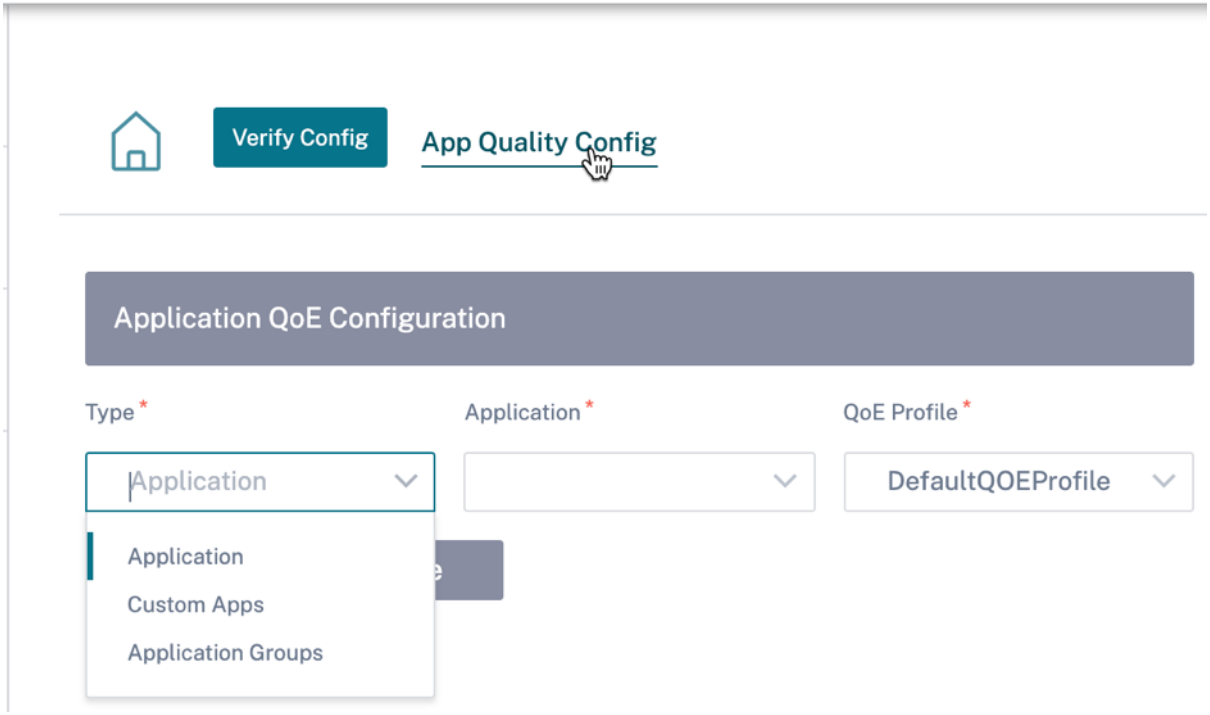
### Configuración de calidad de las aplicaciones

Asigne objetos de aplicación o aplicación a perfiles QoE predeterminados o personalizados. Puede crear perfiles de QoE personalizados para el tráfico en tiempo real e interactivo.

Haga clic en **+Configuración de QoE** para crear perfiles de QoE personalizados:

- **Tipo**: Seleccione la aplicación de DPI o un objeto de aplicación (aplicación, aplicaciones personalizadas y grupos de aplicaciones).
- **Aplicación**: busque y seleccione una aplicación u objeto de aplicación según el tipo seleccionado.
- **Perfil QoE**: Seleccione un perfil QoE para asignarlo a la aplicación o al objeto de aplicación.

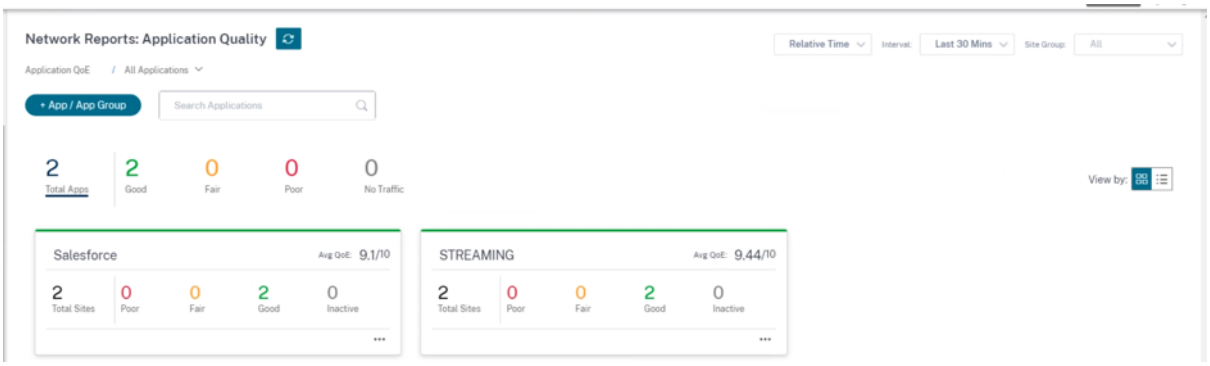
 




Haga clic en **Listo**.

Haga clic en **Verificar configuración** para validar cualquier error de auditoría.

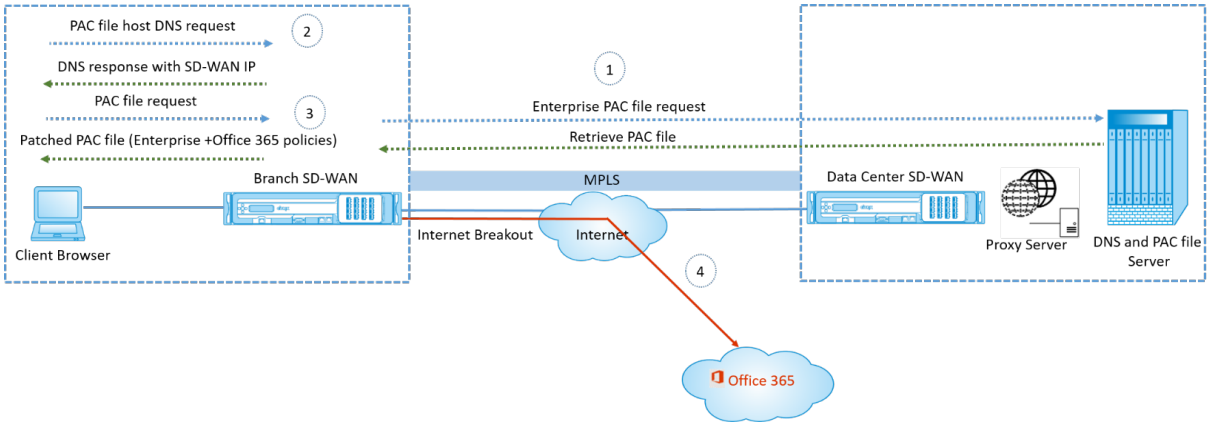
Una vez que configure la QoE de la aplicación con el tipo de aplicación personalizado, se generará automáticamente un cuadro de informe de aplicación correspondiente en **Informes > Calidad de la aplicación**. Todo el tráfico que coincida con la aplicación seleccionada pasa por la ruta virtual de la aplicación personalizada.




### Cómo funciona la personalización de archivos PAC

Idealmente, el archivo PAC del host de red empresarial en el servidor web interno, esta configuración de proxy se distribuye mediante la directiva de grupo. El explorador cliente solicita archivos PAC del servidor web empresarial. El dispositivo Citrix SD-WAN sirve los archivos PAC personalizados para los sitios en los que está habilitado el breakout de Office 365.




1. Citrix SD-WAN solicita y recupera periódicamente la última copia del archivo PAC empresarial del servidor web empresarial. El dispositivo Citrix SD-WAN parchea las URL de office 365 en el archivo PAC empresarial. Se espera que el archivo PAC empresarial tenga un marcador de posición (etiqueta específica de SD-WAN) en el que las URL de Office 365 se parchean sin problemas.
2. El explorador de cliente genera una solicitud DNS para el host de archivo PAC de empresa. Citrix SD-WAN intercepta la solicitud del FQDN del archivo de configuración del proxy y responde con el VIP de Citrix SD-WAN.
3. El explorador del cliente solicita el archivo PAC. El dispositivo Citrix SD-WAN sirve el archivo PAC parcheado localmente. El archivo PAC incluye la configuración del proxy empresarial y las directivas de exclusión de URL de Office 365.
4. Al recibir una solicitud para la aplicación Office 365, el dispositivo Citrix SD-WAN realiza una interrupción directa de Internet.

### Requisitos previos

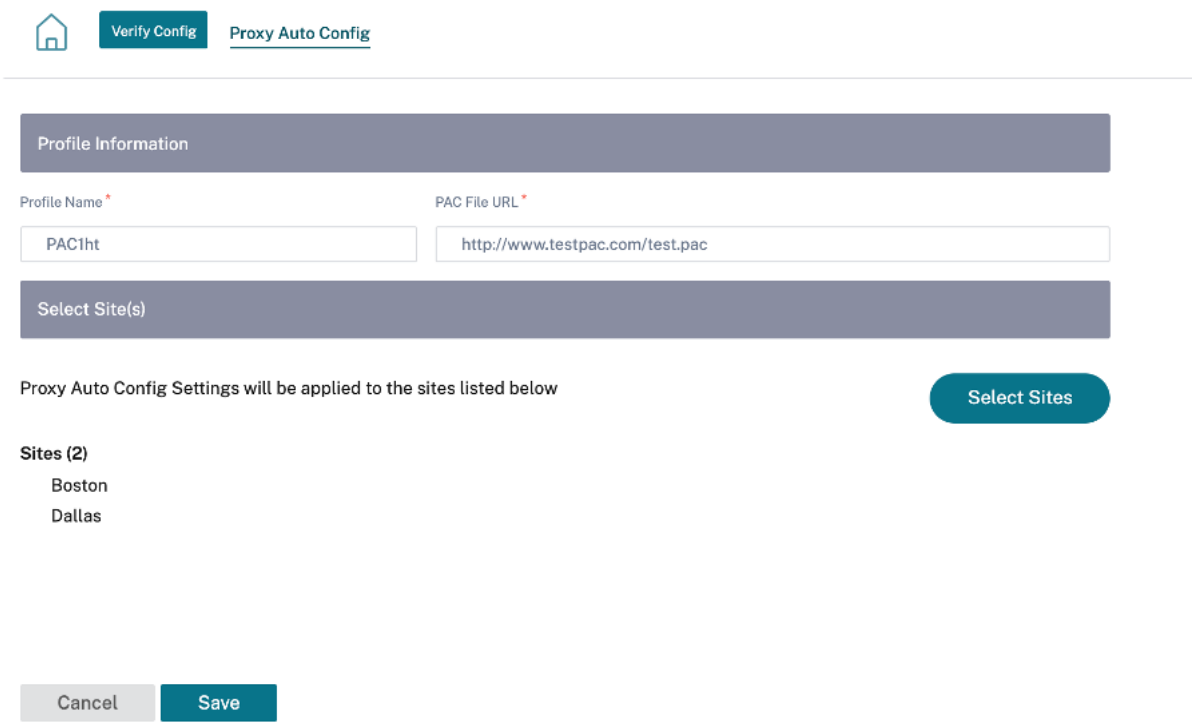
1. Las empresas deben tener un archivo PAC alojado.
2. El archivo PAC debe tener un marcador de posición *SDWAN_TAG* o una aparición de la función `findproxyforurl` para parchear las URL de Office 365.
3. La dirección URL del archivo PAC debe estar basada en dominios y no basada en IP.
4. El archivo PAC solo se sirve a través de los VIP de identidad de confianza.
5. El dispositivo Citrix SD-WAN debe poder descargar el archivo PAC empresarial a través de su interfaz de administración.

### Configurar configuración automática del proxy

En la interfaz de usuario de SD-WAN Orchestartor, al nivel de red, vaya a **Configuración > Configuración** de **aplicaciones y grupos** > **Configuración automática de proxy** y haga clic en **+ perfil de**

**archivo PAC**.




Introduzca un nombre para el perfil de archivo PAC, proporcione la dirección URL del servidor de archivos PAC de empresa. Las reglas de grupo de Office 365 se aplican de forma dinámica al archivo PAC de empresa.

Seleccione los sitios a los que se aplica el perfil del archivo PAC. Si hay direcciones URL diferentes para cada sitio, cree un perfil diferente por sitio.

### Limitaciones

- No se admiten las solicitudes del servidor de archivos HTTPS PAC.
- No se admiten varios archivos PAC de una red, incluidos los archivos PAC para dominios de redirección o zonas de seguridad.
- No se admite la generación de un archivo PAC en Citrix SD-WAN desde cero.
- WPAD a través de DHCP no es compatible.

## Parámetros de PPP

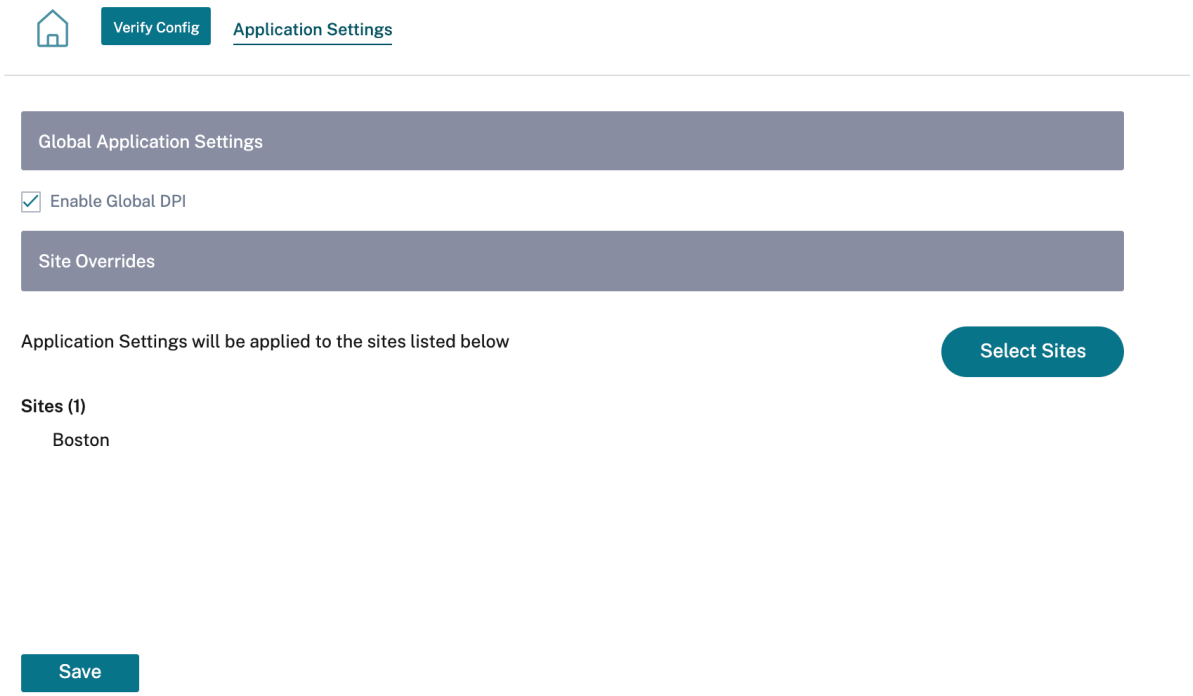
Los dispositivos Citrix SD-WAN realizan la inspección profunda de paquetes (PPP) para identificar y clasificar aplicaciones. La biblioteca del DIP reconoce miles de aplicaciones comerciales. Permite el

descubrimiento y la clasificación de aplicaciones en tiempo real. Mediante la tecnología PPP, el dispositivo SD-WAN analiza los paquetes entrantes y clasifica el tráfico como perteneciente a una aplicación o familia de aplicaciones en particular.

PPP está habilitado globalmente, de forma predeterminada, para todos los sitios de la red. La inhabilitación de PPP detiene la capacidad de clasificación de PPP en el dispositivo. Ya no puede utilizar las categorías de aplicaciones o aplicaciones clasificadas por PPP para configurar directivas de firewall, QoS y enrutamiento. Tampoco podrá ver el informe de aplicaciones y categorías de aplicaciones principales.

Para inhabilitar el DPI global, en el nivel de red, vaya a **Configuración > Configuración y grupos de aplicaciones > Configuración de DPI** y desactive la opción **Habilitar DPI global**.




También puede optar por inhabilitar PPP para determinados sitios solo si se anula la configuración global de PPP. Para inhabilitar el DPI en los sitios seleccionados, agregue los sitios a la lista de **modificaciones** de sitios.

## Perfiles y plantillas

October 31, 2022

Un perfil es una plantilla de configuración activa. Una plantilla normal ayuda a crear una nueva en-

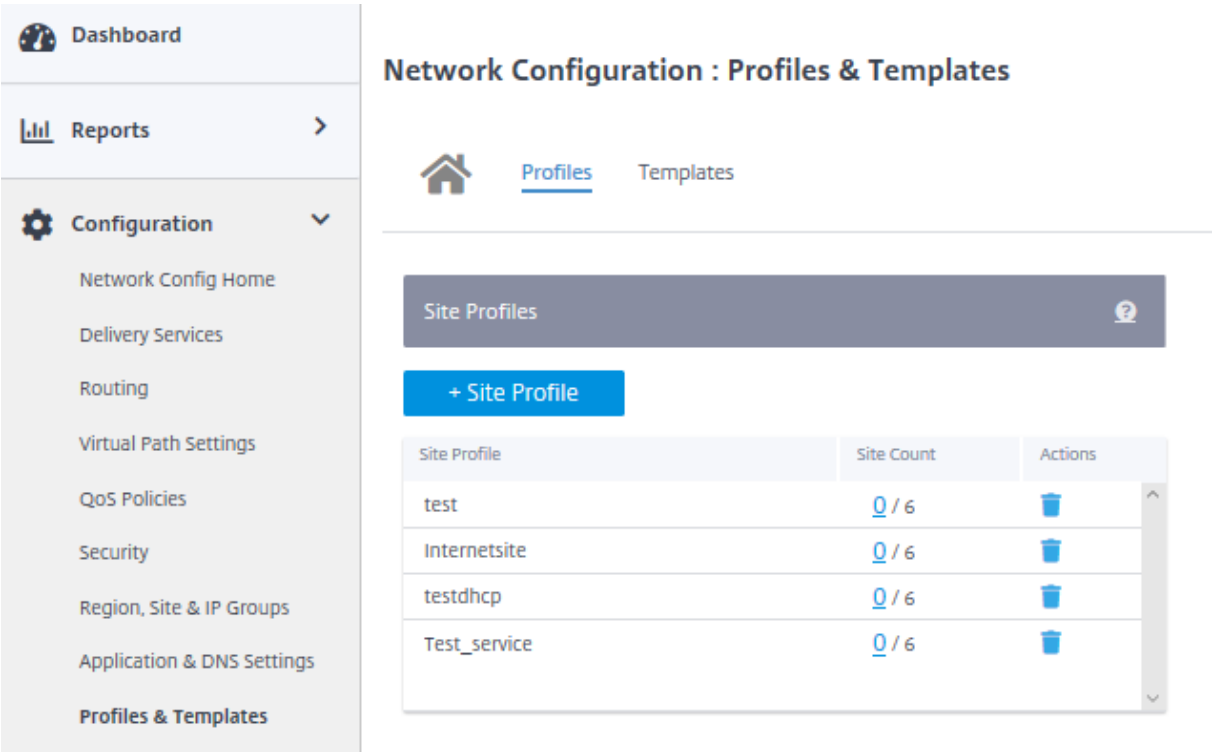
 

tidad. Sin embargo, una vez creada la plantilla, los cambios posteriores en la plantilla no se aplican a las entidades existentes creadas con la plantilla base. Un perfil sirve como entidad maestra central activa. Todas las entidades secundarias heredan del perfil, no solo durante la creación sino también durante toda la vida de un perfil. Todas las entidades secundarias asociadas al perfil heredan automáticamente los cambios realizados en un perfil.

Por ejemplo, un administrador crea un perfil de configuración de sitio llamado tienda minorista pequeña y lo aplica a todas las tiendas minoristas pequeñas propiedad de una empresa. Ahora, cualquier cambio realizado en el perfil de la tienda minorista pequeña en un momento dado se aplicaría automáticamente a todas las tiendas heredadas de este perfil. En función de lo que es común en todas las entidades, y lo que no lo es, ciertos parámetros en la configuración del perfil pueden dejarse sin definir. Estos parámetros serían personalizables y pueden variar entre las entidades que heredan el mismo perfil.

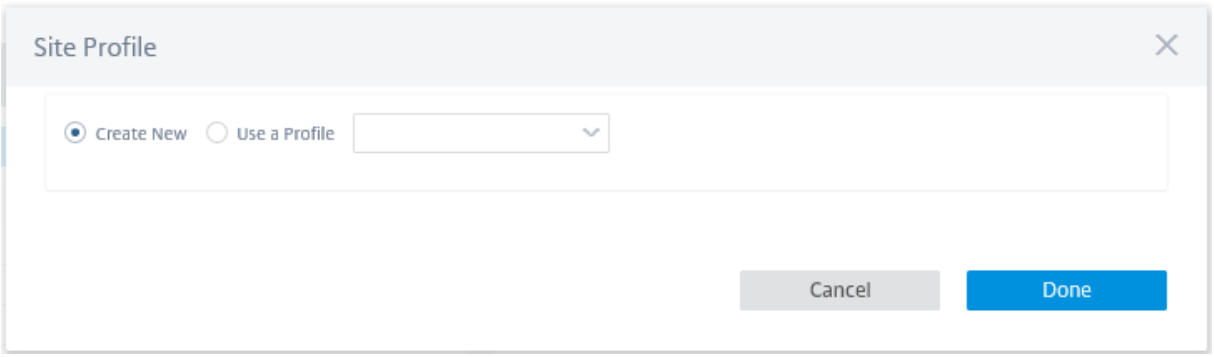
### Perfiles del sitio

Los perfiles de sitio le ayudan a configurar sitios de forma fácil y rápida. Puede crear un perfil de sitio una vez y volver a utilizarlo varias veces mientras crea sitios.



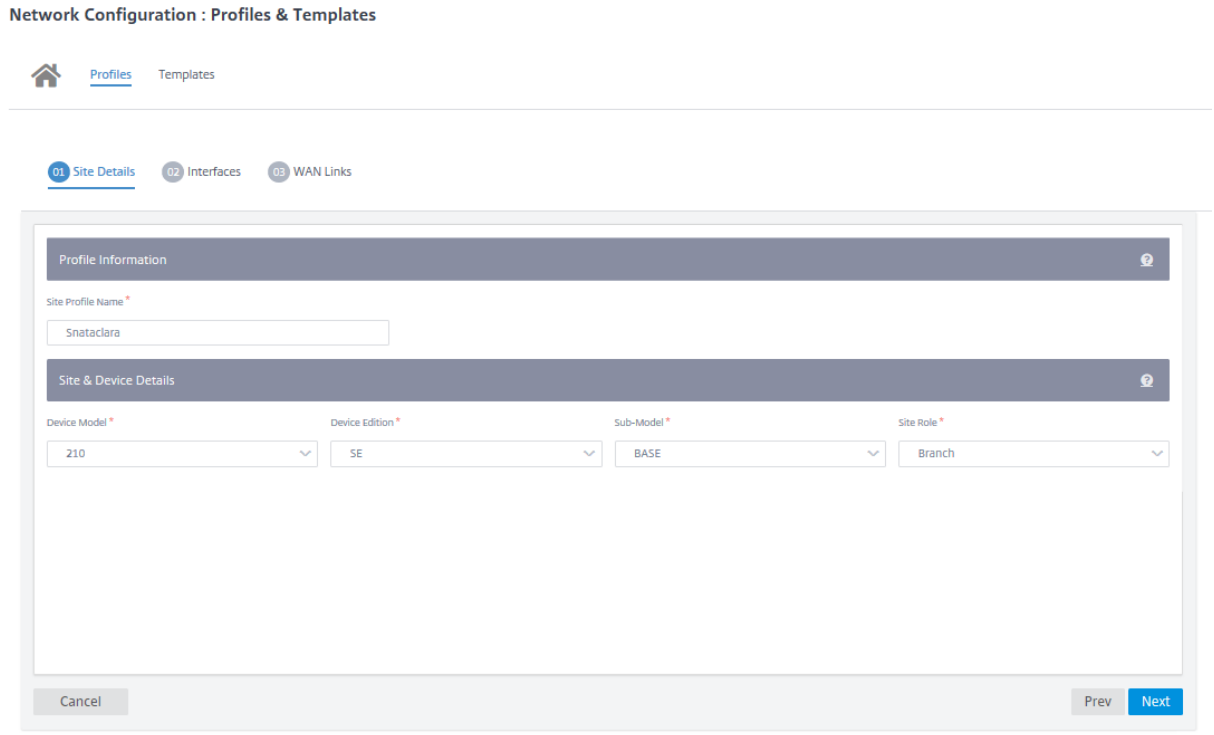

Para crear un perfil de sitio, haga clic en **+ Perfil del sitio**. Puede crear un perfil desde cero o modificar un perfil de sitio existente y guardarlo como un perfil nuevo.



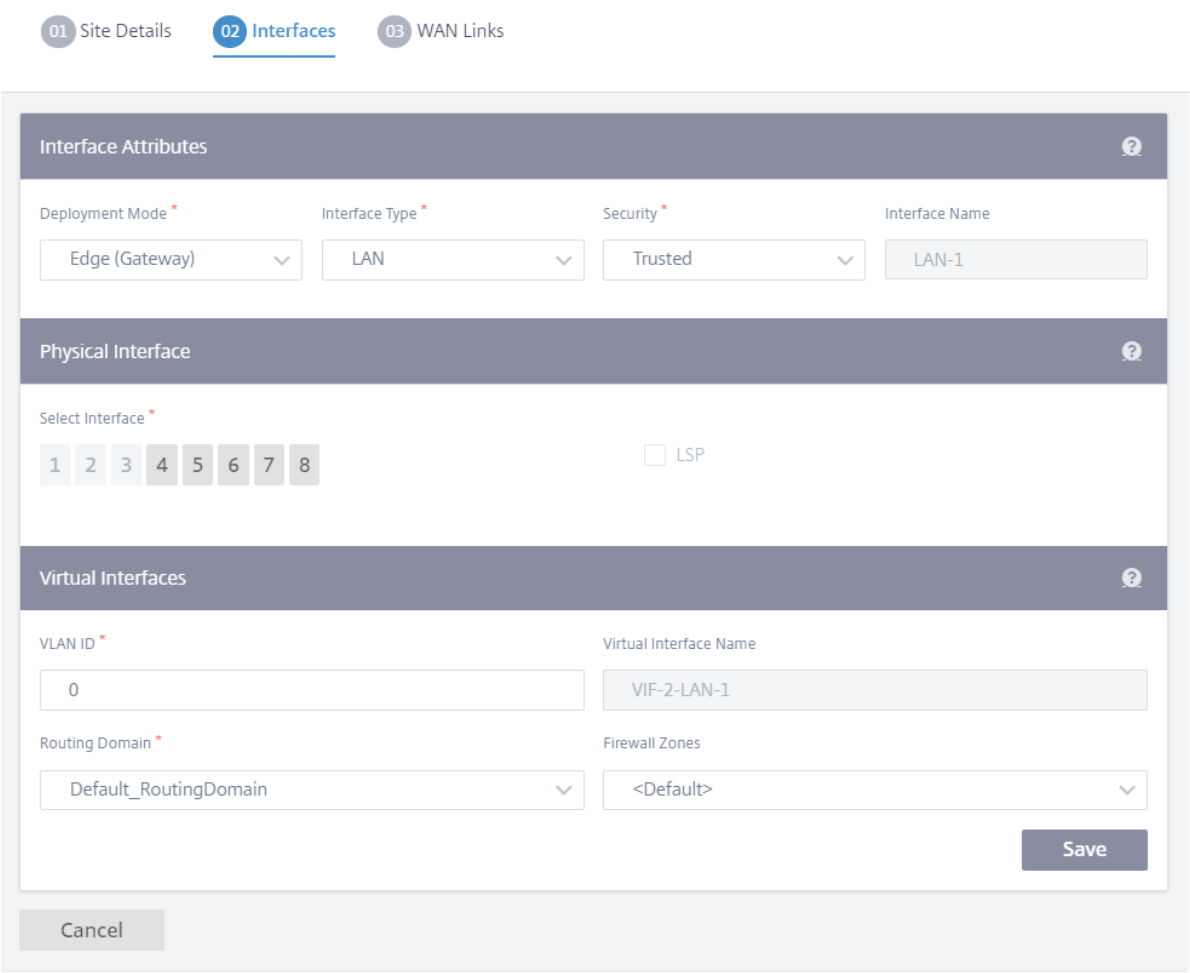

Para crear un perfil de sitio, debe configurar los **detalles del sitio**, **las interfaces**y **los enlaces WAN**. Para obtener una descripción detallada de la configuración de sitios, consulte Detalles del sitio.

Proporcione los detalles del dispositivo.




Asigne una interfaz para el sitio haciendo clic en la opción **Interfaz +**. Para agregar una interfaz, debe completar los campos **Atributos de la interfaz**, **Interfaz física**e **Interfaces virtuales**. Para obtener una descripción detallada de la configuración de interfaces, consulte Interfaces.

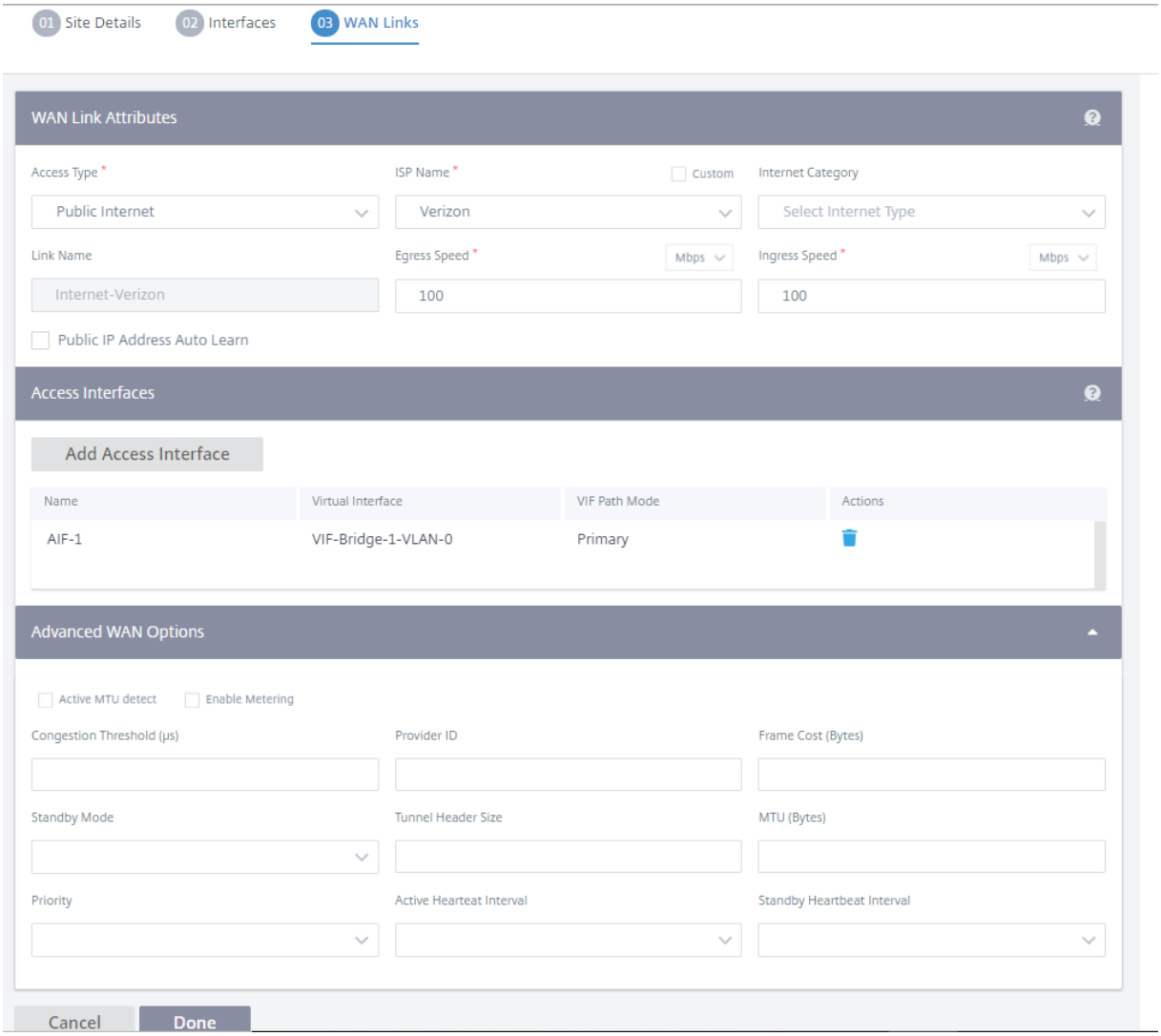
 




Complete **los atributos de enlace WAN**, **las interfaces de acceso**y **los servicios** con **opciones avanzadas**.

Para obtener una descripción detallada de la configuración de los enlaces WAN, consulte Enlaces WAN.




## Plantillas

El servicio Citrix SD-WAN Orchestrator le permite usar plantillas como un conjunto de campos predefinidos para configurar un nuevo sitio o un enlace WAN.

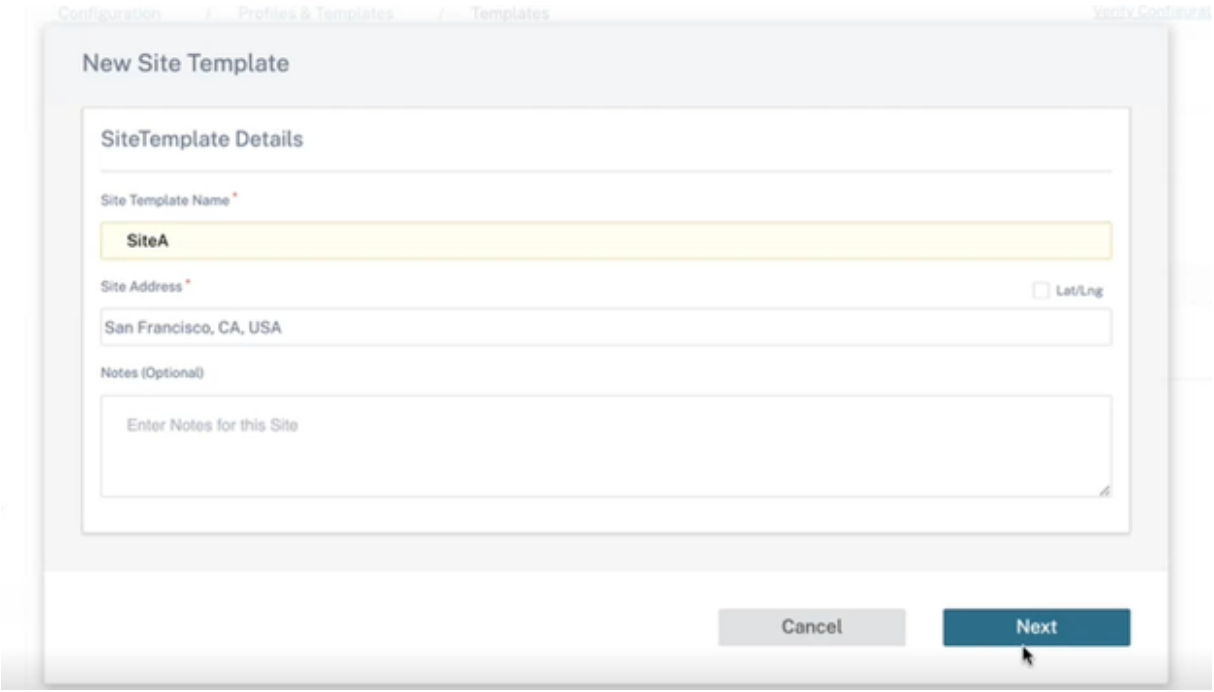
### Plantilla de sitio

Una plantilla de sitio es una plantilla predefinida que se utiliza para la creación de sitios. Para configurar un sitio con una plantilla de sitio predefinida, al nivel de cliente, vaya a **Configuración** > **Perfiles y plantillas** > **Plantillas**. En la sección **Plantilla de sitio**, haga clic en **Agregar plantilla de sitio**.

En la pantalla **Nueva plantilla de sitio** que aparece, proporcione los detalles necesarios y haga clic en **Siguiente**.

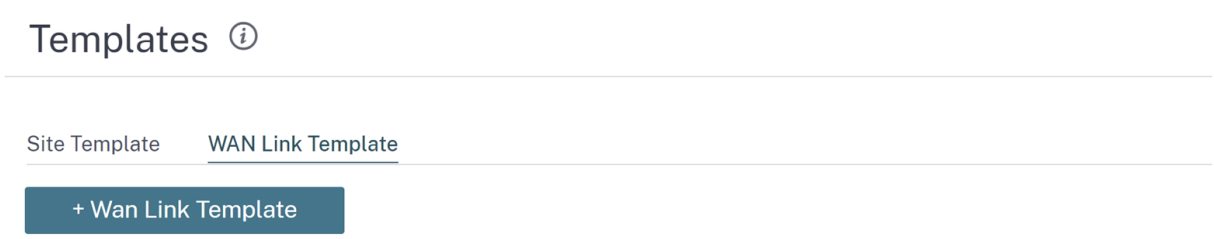
 

> **Nota**
>
> Cuando se clona un sitio o se crea un sitio con una plantilla de sitio y la fuente tiene la conexión Wi-Fi configurada, la configuración de Wi-Fi no se copia en el nuevo sitio.



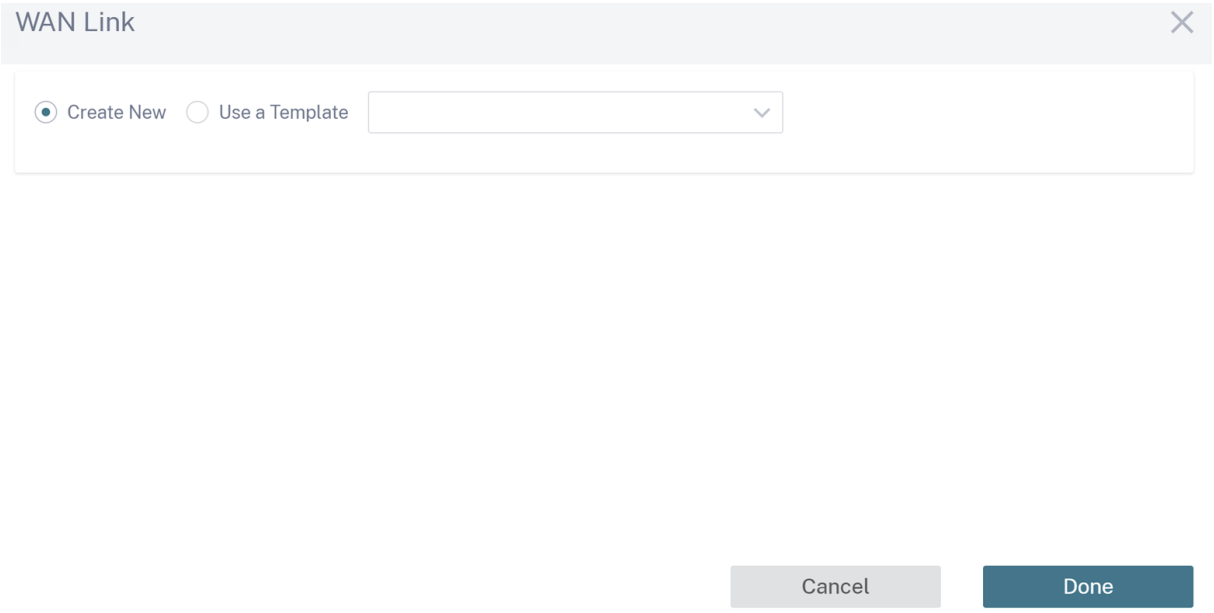

**Plantilla de vínculos WAN**

Las plantillas de enlaces WAN le ayudan a configurar los enlaces WAN fácil y rápidamente. Puede crear una plantilla de enlace WAN una vez y reutilizarla varias veces mientras configura enlaces WAN. Incluso puede copiar las configuraciones modificadas de la plantilla de enlace WAN a las configuraciones de enlace WAN del sitio creadas con la plantilla de enlace WAN.

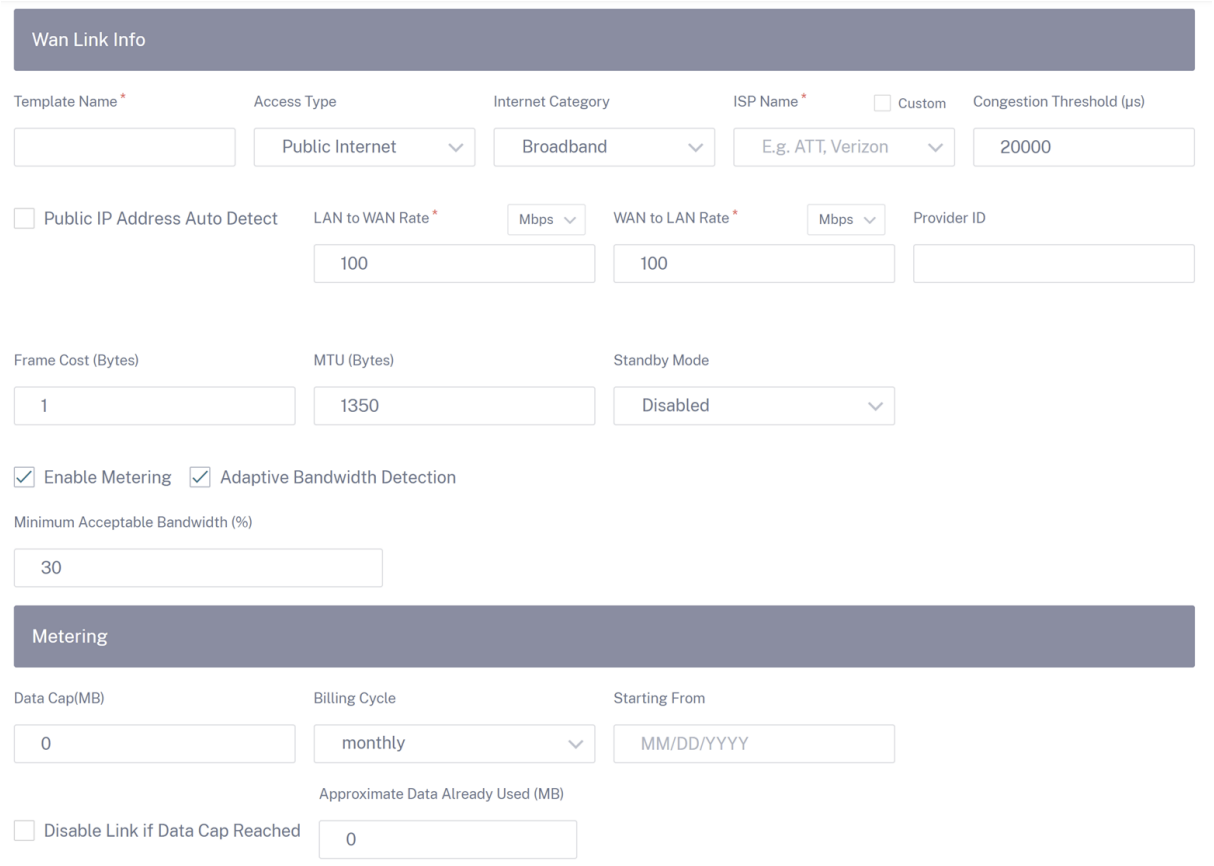



Para crear una plantilla de enlace WAN, haga clic en **+ Plantilla de enlace WAN**. Puede crear una plantilla desde cero o modificar una plantilla de enlace WAN existente y guardarla como una nueva plantilla.




Proporcione la información del enlace WAN, como el **nombre del perfil**, el **tipo de acceso**, la **categoría de Internet**, la **velocidad de LAN a WAN** (Mbps), etc., para crear un perfil WAN. Para obtener una descripción detallada de la configuración de los enlaces WAN, consulte Enlaces WAN.



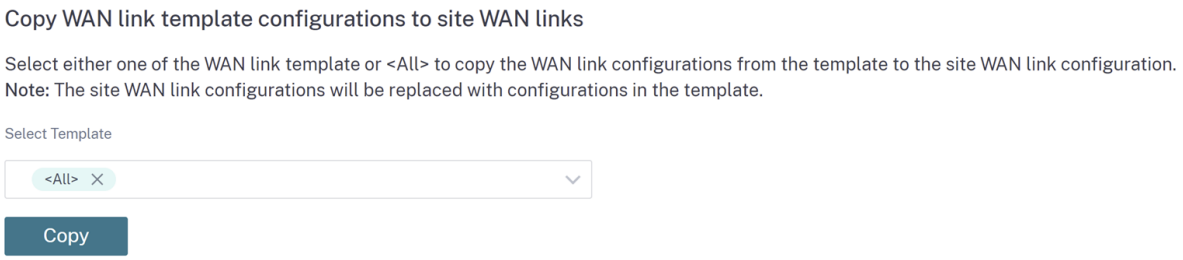

Anteriormente, la opción de copiar las configuraciones de plantillas de enlaces WAN modificadas a las

configuraciones de enlaces WAN del sitio no estaba disponible. Por ejemplo, si un usuario ya había creado varios enlaces WAN de sitios mediante una plantilla de enlaces WAN y tenía que modificar una configuración concreta (por ejemplo, la configuración del umbral de congestión), tenía que hacerlo en cada enlace WAN del sitio de forma individual. A partir de ahora, el usuario puede actualizar la plantilla de enlaces WAN con la nueva configuración del umbral de congestión y copiar las configuraciones más recientes de la plantilla de enlaces WAN a todos los enlaces WAN del sitio creados con la plantilla de enlaces WAN.

Al seleccionar una o más plantillas de enlaces WAN y hacer clic en copiar, las actualizaciones que realice en la plantilla de enlace WAN se copian a la configuración de enlace WAN del sitio creada con las plantillas seleccionadas.

> **Nota**
>
> Las configuraciones de sitios de enlaces WAN que se crean mediante la función de perfil de sitio no se actualizan.




## Servicio de ubicación de red

July 10, 2024

> **Actualización importante:**
>
> Esta función está obsoleta en la implementación del servicio Citrix SD-WAN Orchestrator. Sin embargo, puede seguir habilitando NLS mediante Citrix Cloud. Para obtener más información, consulte Optimizar la conectividad a los espacios de trabajo con Direct Workload Connection.

El servicio de ubicación de red (NLS) es un servicio de Citrix Cloud que determina si el usuario que se conecta a Citrix Virtual Apps and Desktops proviene de la red interna. Con NLS, puede evitar configurar manualmente las direcciones IP de las ubicaciones implementadas de Citrix SD-WAN mediante el script de PowerShell. Para obtener información detallada sobre NLS, consulte Citrix Workspace Network Location Service.

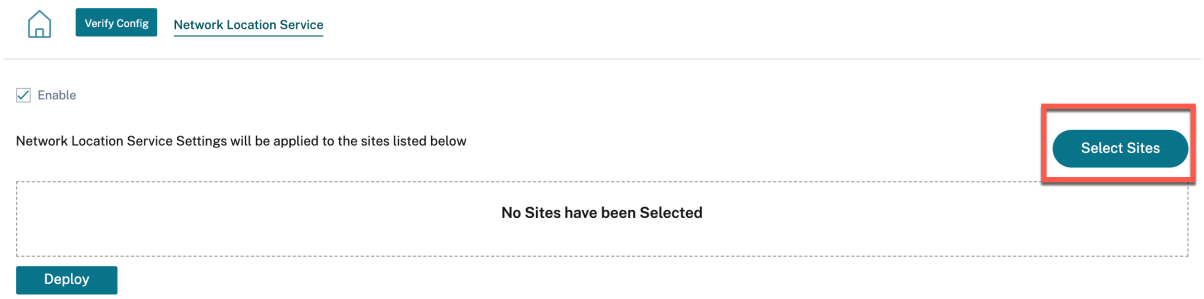
Puede habilitar el NLS para todos los sitios de la red o sitios específicos. El sitio habilitado para NLS comparte la dirección IP pública de todos sus enlaces WAN de Internet junto con otros detalles del

sitio, como la ubicación geográfica y la zona horaria, con la base de datos de NLS. Con estos detalles, el servicio de ubicación de red determina si el usuario que se conecta a Citrix Virtual Apps and Desktops se encuentra en una interfaz de red con Citrix SD-WAN.

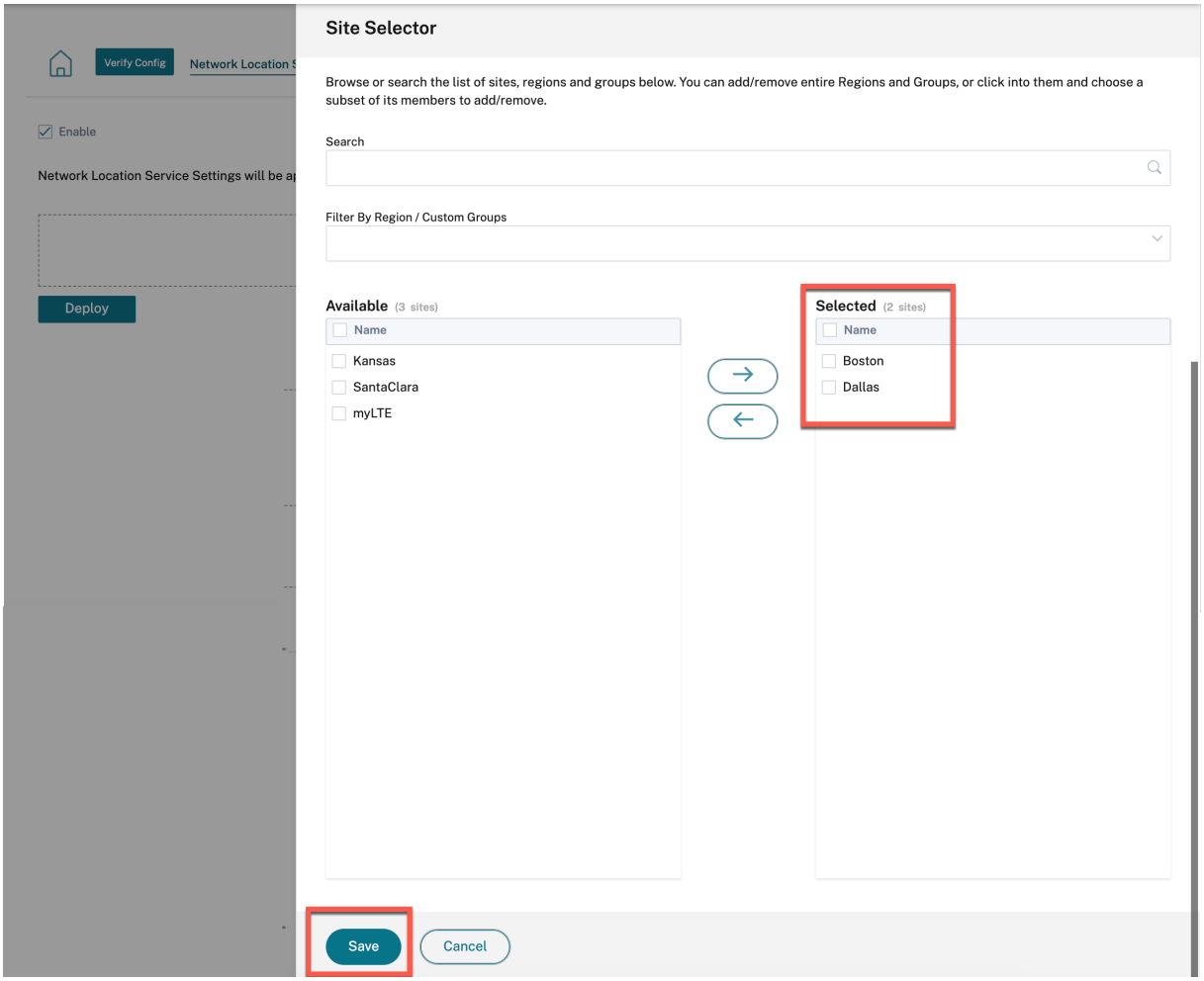
Si una solicitud de usuario proviene de una interfaz de red con Citrix SD-WAN, el usuario se conecta directamente al Virtual Delivery Agent de Citrix Virtual Apps and Desktops, evitando el servicio Citrix Gateway.

Para habilitar NLS, al nivel de cliente, vaya a **Configuración > Servicio de ubicación de red**.




Seleccione **Activar** si quiere habilitar NLS en todos los sitios de la red. Para habilitar el NLS en sitios específicos, haga clic en **Seleccionar sitios**. Elija la **región** y seleccione los sitios en consecuencia. Haga clic en **Guardar** y luego en **Implementar**




## Equilibrio de carga ECMP

October 31, 2022

Los grupos de rutas múltiples de igual coste (ECMP) permiten agrupar varias rutas con el mismo coste, destino y servicio. Las conexiones o los datos de sesión se equilibran la carga en todas las rutas del grupo ECMP dependiendo del tipo de grupo ECMP. Por ejemplo, considere una red con dos vínculos WAN entre una sucursal y un centro de datos que tenga el mismo coste de ruta. Tradicionalmente, uno de los enlaces WAN estaría activo y el otro permanece inactivo actuando como enlace de reserva. Con ECMP Groups, puede agrupar estos vínculos WAN juntos y permitir que el tráfico se equilibre la carga a través de ambos enlaces WAN. El equilibrio de carga ECMP garantiza:

- Distribución del tráfico a través de múltiples rutas de igual coste.
- Uso óptimo del ancho de banda disponible.

- Transferencia dinámica de tráfico a otra ruta miembro de ECMP, si una ruta se vuelve inalcanzable.

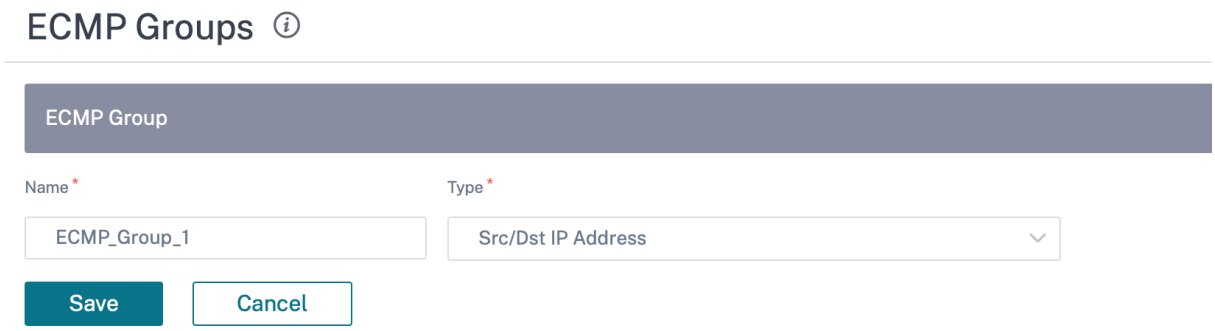
El equilibrio de carga de ECMP es compatible con los siguientes servicios:

- Rutas virtuales
- Citrix Secure Internet Access
- Zscaler
- IPsec
- GRE

Puede definir un máximo de 254 grupos ECMP en la red. El número máximo de rutas elegibles para ECMP en un grupo ECMP depende del dispositivo y del tipo de licencia. Citrix SD-WAN admite los dos tipos siguientes de grupos ECMP:

- Dirección IP de origen/destino: R edes en las que varios clientes intentan conectarse al mismo destino, las conexiones se equilibran la carga a través de enlaces WAN de igual coste.
- Sesión: Redes donde un único cliente está conectado a un destino y se generan varias sesiones. Los datos de la sesión se equilibran la carga a través de enlaces WAN de igual coste.

Para configurar un grupo ECMP, en el nivel de red, vaya a **Configuración > Enrutamiento > Grupos ECMP**. Proporcione un nombre para el grupo ECMP y seleccione el tipo como **Dirección IP Src/Dest** o **Sesión** según sea necesario.



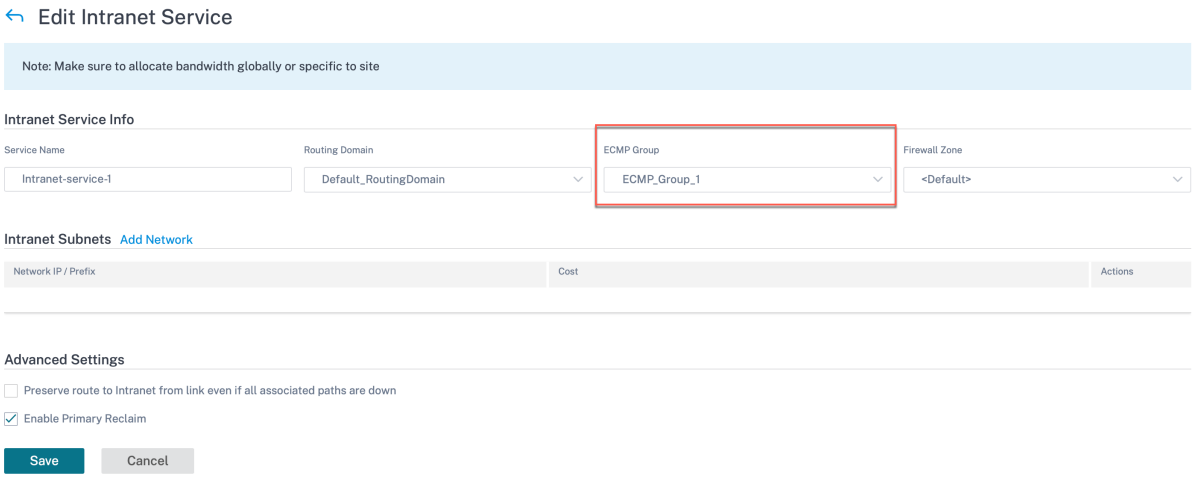

Puede asociar los grupos ECMP a los siguientes servicios:

- Rutas virtuales (al nivel de sitio)
- Citrix Secure Internet Access
- Zscaler
- IPsec
- GRE

Para habilitar la configuración de ECMP en los servicios de Intranet, en el nivel Red *, vaya a **Configuración > Canales de entrega > Asignación de ancho de banda > Intranet + Servicio** y seleccione el **tipo de servicio** como **Intranet**. Seleccione el grupo ECMP al configurar el servicio de Intranet.

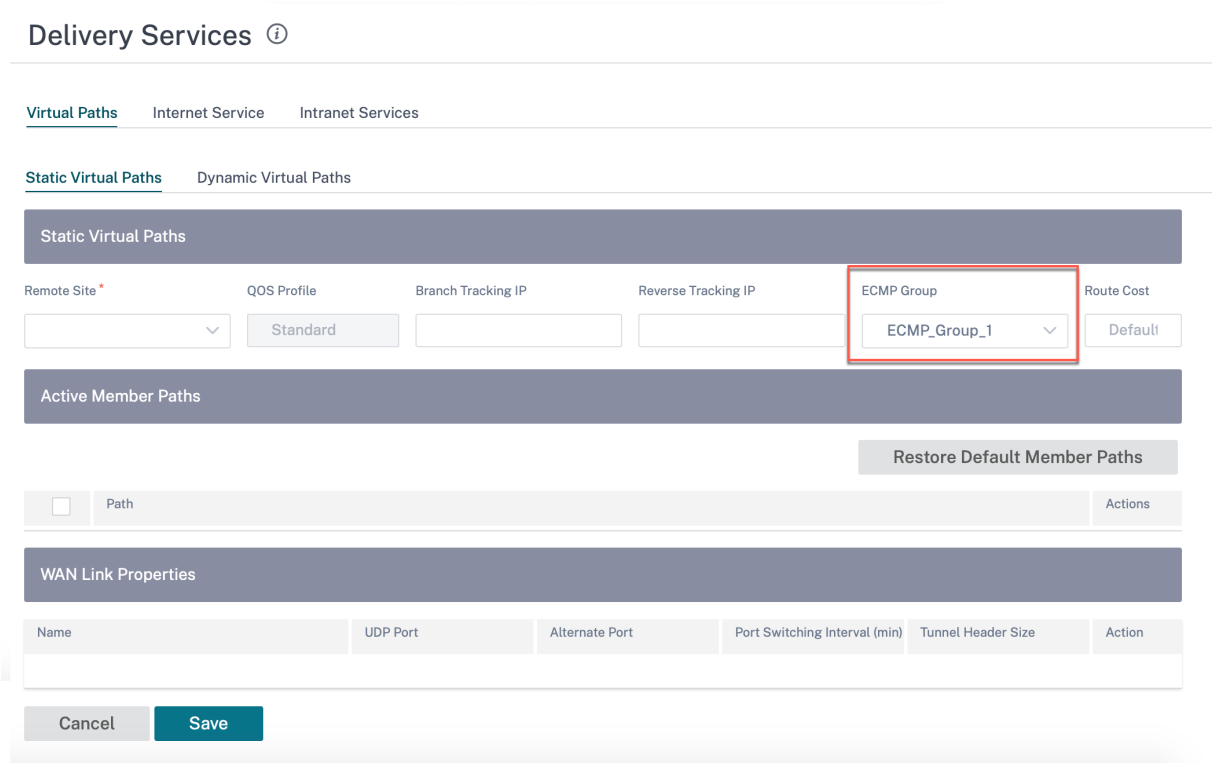
> **Nota**
>
> Si selecciona **Ninguno**, no se habilitará la configuración de ECMP en el servicio.




Para habilitar la configuración de ECMP en rutas virtuales, al nivel de sitio, vaya a **Configuración > Configuración** > **Configuración avanzada** > **Servicios de entrega** > **Rutas virtuales** > **Rutas virtuales estáticas** > **+ Rutas virtuales**. Seleccione el grupo ECMP al configurar las rutas virtuales estáticas.

> **Nota**
>
> Si selecciona **Ninguno**, no se habilitará la configuración de ECMP en el servicio.

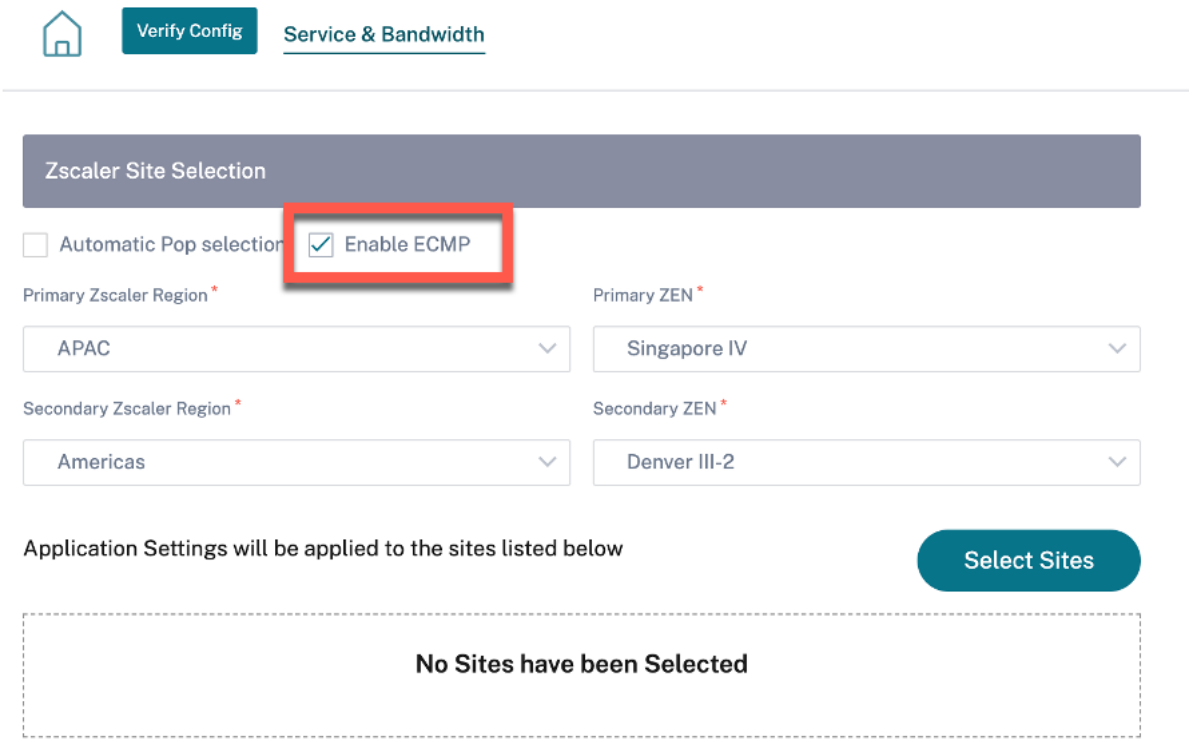
 




Para habilitar la configuración de ECMP en los servicios de Zscaler, en el nivel de red, vaya a **Configuración > Servicios y ancho de banda**. Haga clic en el icono de **configuración** situado junto a Zscaler que aparece en la columna **Servicios de entrega**. Autentica y haga clic en **+ Sitio**. Seleccione la casilla **Activar ECMP** al agregar sitios.

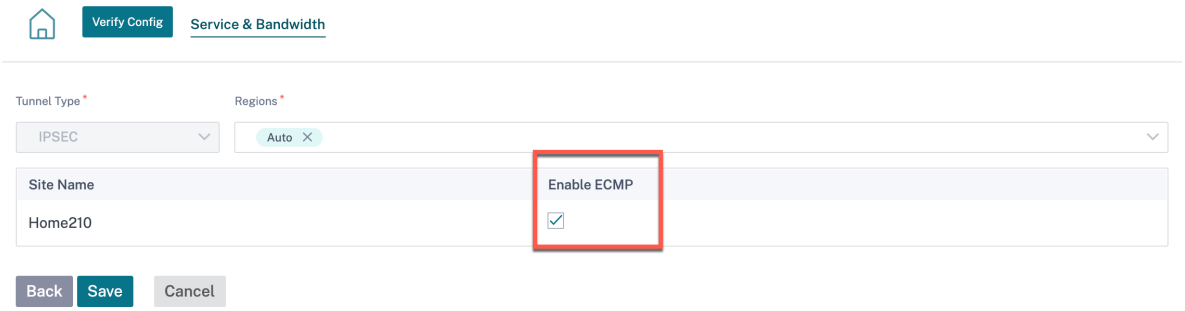
> **NOTA**
>
> El servicio Zscaler solo admite el equilibrio de carga de ECMP basado en sesiones.




Para habilitar la configuración de ECMP en el servicio Citrix Secure Internet Access, al nivel de red, vaya a **Configuración > Servicios y ancho de banda**. Haga clic en el icono de **configuración** situado junto a **Secure Internet Access Service** y haga clic en **+ Sitio**. Seleccione la casilla **Activar ECMP** después de seleccionar los sitios.

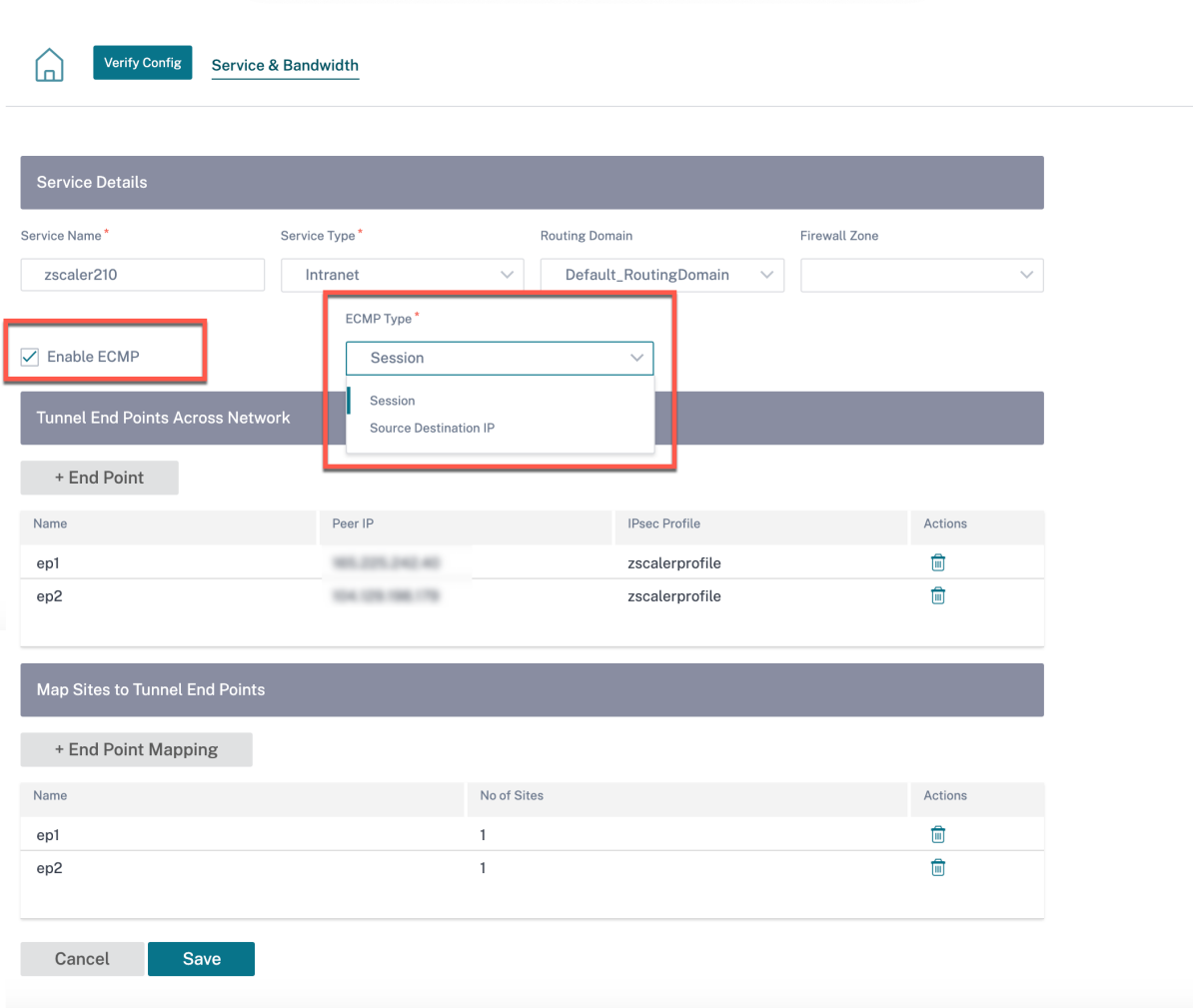
> **NOTA**
>
> El servicio Citrix Secure Internet Access solo admite el equilibrio de carga de ECMP basado en sesiones.




Para habilitar la configuración de ECMP en túneles IPSec fijos con pares de terceros en el lado de la LAN o la WAN, vaya a **Configuración > Servicios y ancho de banda > Intranet + Servicio** y seleccione el **tipo de servicio** como **IPsec**. Seleccione la casilla **Activar ECMP** y elija un tipo de la lista desplegable

de **tipos de ECMP**.




## Reglas de aplicación

October 31, 2022

Las reglas de la aplicación permiten que el dispositivo Citrix SD-WAN analice el tráfico entrante y lo clasifique como perteneciente a una aplicación o grupo de aplicaciones en particular. Esta clasificación mejora la calidad de servicio (QoS) de aplicaciones individuales o familias de aplicaciones mediante la creación y aplicación de reglas de aplicación.

Puede filtrar los flujos de tráfico en función de los tipos de coincidencia de aplicaciones, grupos de aplicaciones u objetos de aplicación y aplicarles reglas de aplicación. Las reglas de la aplicación son similares a las reglas del Protocolo de Internet (IP). Para obtener información sobre las reglas de IP, consulte Reglas de IP.

Para cada regla de aplicación, puede especificar la directiva de tráfico. Las siguientes son las directivas de tráfico disponibles:

- **Ruta de equilibrio de carga**: El tráfico de aplicaciones para el flujo se equilibra en varias rutas. El tráfico se envía a través de la mejor ruta hasta que se utiliza esa ruta. Los paquetes restantes se envían a través de la siguiente mejor ruta.
- **Ruta persistente**: El tráfico de aplicaciones permanece en la misma ruta hasta que la ruta deja de estar disponible.
- **Ruta de acceso duplicada**: El tráfico de aplicaciones se duplica en múltiples paths, lo que aumenta la fiabilidad.
  Las reglas de aplicación están asociadas a clases.

### ¿Cómo se aplican las reglas de aplicación?

En la red SD-WAN, cuando los paquetes entrantes llegan al dispositivo SD-WAN, los pocos paquetes iniciales no se clasifican por PPP. En este punto, los atributos de reglas IP como Clase, Terminación TCP se aplican a los paquetes. Tras la clasificación de DPI, los atributos de la regla de aplicación, como la clase y la directiva de tráfico, anulan los atributos de la regla

Las reglas IP tienen más atributos en comparación con las reglas de aplicación. La regla de aplicación anula solo algunos atributos de la regla IP. El resto de los atributos de la regla IP permanecen procesados en los paquetes.

Por ejemplo, supongamos que ha especificado una regla de aplicación para una aplicación de correo web, como Google Mail, que utiliza el protocolo SMTP. La regla IP establecida para el protocolo SMTP se aplica inicialmente antes de la clasificación de DPI. Tras analizar los paquetes y clasificarlos como pertenecientes a la aplicación Google Mail, se aplica la regla de aplicación especificada para la aplicación Google Mail.

### Crear reglas de aplicación

Para crear reglas de aplicación, vaya a **Configuración > QoS > Directivas de QoS** > **Reglas de aplicación**. Seleccione la ficha **Reglas globales** para crear reglas de aplicación a nivel global o **Reglas específicas de sitio/grupo** para crear reglas al nivel de sitio.

Haga clic en **Nueva regla** de **aplicación en la sección Reglas** de aplicación.

- Criterios de coincidencia de aplicaciones.
  - **Aplicaciones y dominios**: Elija una aplicación o un dominio de la lista desplegable. También puede crear una aplicación de dominio haciendo clic en **+ Nueva aplicación de dominio**. Introduzca un nombre y agregue dominios.

- **Dominio de enrutamiento**: Seleccione un dominio de enrutamiento. Puede seleccionar el dominio de enrutamiento predeterminado o seleccionar **Cualquiera**.
- **Red de origen**: Dirección IP de origen y máscara de subred para que coincidan con el tráfico.
- **Red de destino**: La dirección IP de destino y la máscara de subred para que coincidan con el tráfico.
- **Puerto de origen**: Número de puerto de origen o intervalo de puertos para que coincida con el tráfico.
- **Puerto de destino**: Número de puerto de destino o intervalo de puertos para que coincida con el tráfico.
- **Src = Dest**: S i se selecciona, el puerto de origen también se usa como puerto de destino.

- Directiva de tráfico de rutas virtuales

  Seleccione la casilla **Habilitar la directiva de tráfico de rutas virtuales**.

  - **Sitio remoto de ruta virtual**: Seleccione la ruta virtual para el sitio remoto.
  - **Directiva de tráfico**: Elija una de las siguientes directivas de tráfico según sea necesario.
    - **Rutas de equilibrio de carga**: El tráfico de aplicaciones para el flujo se equilibra en varias rutas. El tráfico se envía a través de la mejor ruta hasta que se utiliza esa ruta. Los paquetes restantes se envían a través de la siguiente mejor ruta.
    - **Ruta persistente**: El tráfico de aplicaciones permanece en la misma ruta hasta que la ruta deja de estar disponible. Seleccione una de las siguientes **directivas de persistencia**:
      - **Persistir en el enlace de origen**: El tráfico de la aplicación permanece en el enlace de origen hasta que la ruta ya no esté disponible.
      - **Persiste en el enlace MPLS si está disponible; de lo contrario, en el enlace de origen**: El tráfico de la aplicación permanece en el enlace MPLS. Si el enlace MPLS no está disponible, el tráfico permanece en el enlace de origen.
      - **Persiste en el enlace de Internet si está disponible, de lo contrario en el enlace de origen**: El tráfico de la aplicación permanece en el enlace de Internet. Si el enlace de Internet no está disponible, el tráfico permanece en el enlace de origen.
      - **Persiste en el enlace de la intranet privada si está disponible; de lo contrario, en el enlace de origen**: El tráfico de la aplicación permanece en el enlace de la intranet privada Si el enlace de la intranet privada no está disponible, el tráfico permanece en el enlace de origen.

      **La impedancia de persistencia** es el tiempo (en ms) hasta que el tráfico de la aplicación permanece en el enlace.
    - **Rutas duplicadas**: El tráfico de las aplicaciones se duplica en varias rutas, lo que aumenta la confiabilidad.

- Configuración de QoS (clase de QoS)
  - **Tipo de transferencia**: Elija uno de los siguientes tipos de transferencia:
    - **Tiempo real**: Se usa para tráfico de baja latencia, bajo ancho de banda y urgente. Las aplicaciones en tiempo real son urgentes, pero en realidad no necesitan un gran ancho de banda (por ejemplo, voz sobre IP). Las aplicaciones en tiempo real son sensibles a la latencia y la fluctuación, pero pueden tolerar algunas pérdidas
    - **Interactivo**: Se utiliza para el tráfico interactivo con requisitos de latencia baja a media y requisitos de ancho de banda bajo a medio. La interacción suele ser entre un cliente y un servidor. Es posible que la comunicación no necesite un ancho de banda alto, pero es sensible a la pérdida y la latencia.
    - **Bulk**: Se utiliza para tráfico de ancho de banda alto y aplicaciones que pueden tolerar una latencia alta. Las aplicaciones que gestionan la transferencia de archivos y necesitan un gran ancho de banda se clasifican como clases masivas. Estas aplicaciones implican poca interferencia humana y son manejadas principalmente por los propios sistemas.
  - **Prioridad**: Elija una prioridad para el tipo de transferencia seleccionado.

Parámetros avanzados

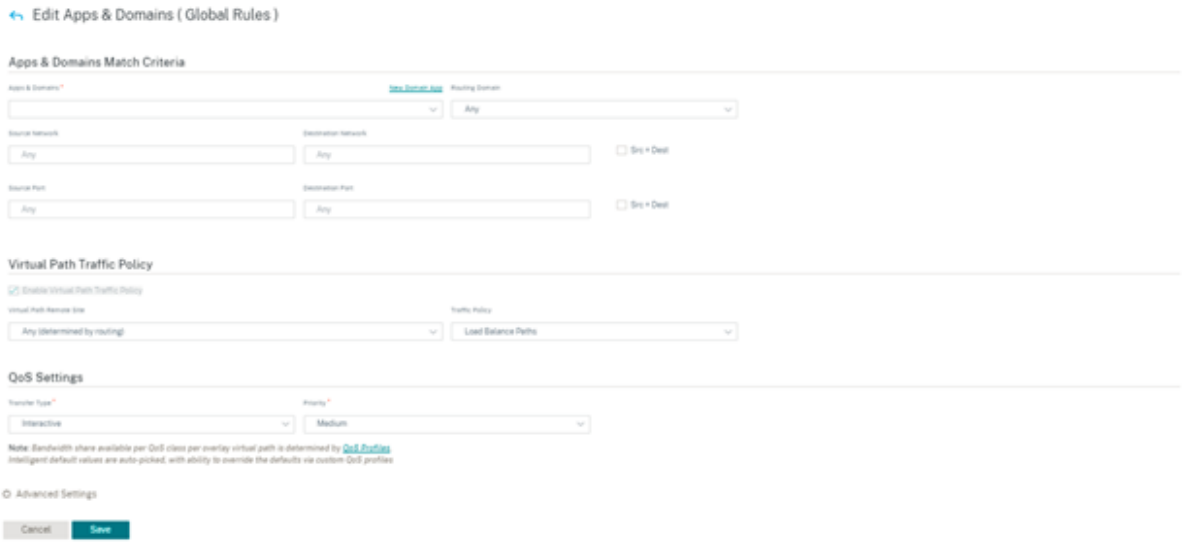
- Información general sobre WAN
  - **Retransmitir paquetes perdidos**: Envía el tráfico que coincide con esta regla al dispositivo remoto a través de un servicio confiable y retransmite los paquetes perdidos.
  - **Habilitar la agregación de paquetes**: Agrega paquetes pequeños en paquetes más grandes.
- LAN a WAN
  - **Profundidad de caída (bytes)**: Umbral de profundidad de cola tras el cual se descartan los paquetes.
  - **Límite**de descarte: Tiempo después del cual se descartan los paquetes en espera en el programador de clases. No aplicable a una clase a granel.
  - **Habilitar RED**: La detección temprana aleatoria (RED) garantiza un reparto justo de los recursos de clase al descartar paquetes cuando se produce congestión.
  - **Profundidad de desactivación de paquetes duplicados (bytes)**: La profundidad de la cola del programador de clases, momento en el que no se generan los paquetes duplicados.
  - **Límite de desactivación de paquetes duplicados: Tiempo durante el cual se puede inhabilitar**la duplicación para evitar que los paquetes duplicados consuman ancho
- WAN a LAN

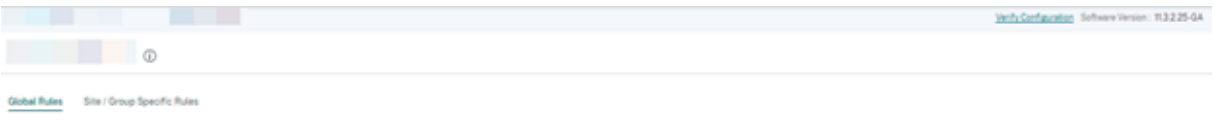
- **Etiqueta DSCP**: Etiqueta DSCP que se aplica a los paquetes que coinciden con esta regla en WAN a LAN, antes de enviarlos a la LAN.
- **Habilitar la resecuenciación de paquetes**: Los flujos de tráfico que coinciden con la regla se etiquetan según el orden de secuencia y los paquetes se reordenan (si es necesario) en el dispositivo de WAN a LAN.
- **Tiempo de espera**: intervalo de tiempo durante el cual se retienen los paquetes para volver a secuenciar, tras el cual los paquetes se envían a la LAN. Cuando el temporizador caduca, los paquetes se envían a la LAN sin esperar más a los números de secuencia necesarios.

  Si la regla tiene una directiva de tráfico como ruta duplicada, el tiempo de espera predeterminado es de 80 ms. De lo contrario, el valor predeterminado es 900 ms para las reglas TCP y 250 ms para las reglas que no son TCP.
- **Descartar paquetes de resecuenciación tardía**: Descarta los paquetes desordenados que llegaron después de que los paquetes necesarios para la resecuenciación se hayan enviado a la LAN.

Haga clic en **Guardar** para guardar los ajustes de configuración.




Haga clic en **Verificar configuración** en la página **Configuración** > **QoS> Directivas de QoS** para validar cualquier error de auditoría. Para validar cualquier error de auditoría.



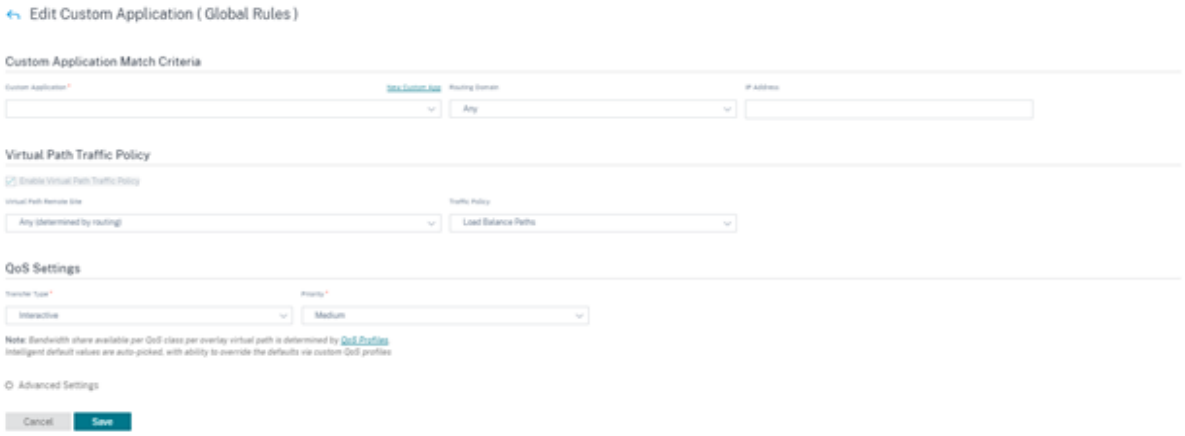

 

### Crear reglas de aplicación personalizadas

También puede crear reglas de aplicación personalizadas. Para crear una regla de aplicación personalizada, vaya a **Configuración > QoS > Directivas de QoS** > **Reglas de aplicación personalizadas**. Seleccione la ficha **Reglas globales** para crear reglas de aplicación personalizadas a nivel global o **Reglas específicas de sitio/grupo** para crear reglas al nivel de sitio.

Haga clic en **Nueva regla de aplicación personalizada** en la sección **Reglas de aplicación personalizadas**. Haga clic en **Nueva aplicación personalizada** junto al nombre del campo **Aplicación personalizada**. Introduzca un nombre para la aplicación personalizada. En la sección **Criterios de coincidencia**, seleccione la aplicación, el protocolo, la etiqueta DSCP e introduzca la IP de la red y el número de puerto. Haga clic en **Guardar**.

Introduzca los detalles en los demás campos según sea necesario. Para obtener información sobre las descripciones de los campos, consulte Crear reglas de aplicación.



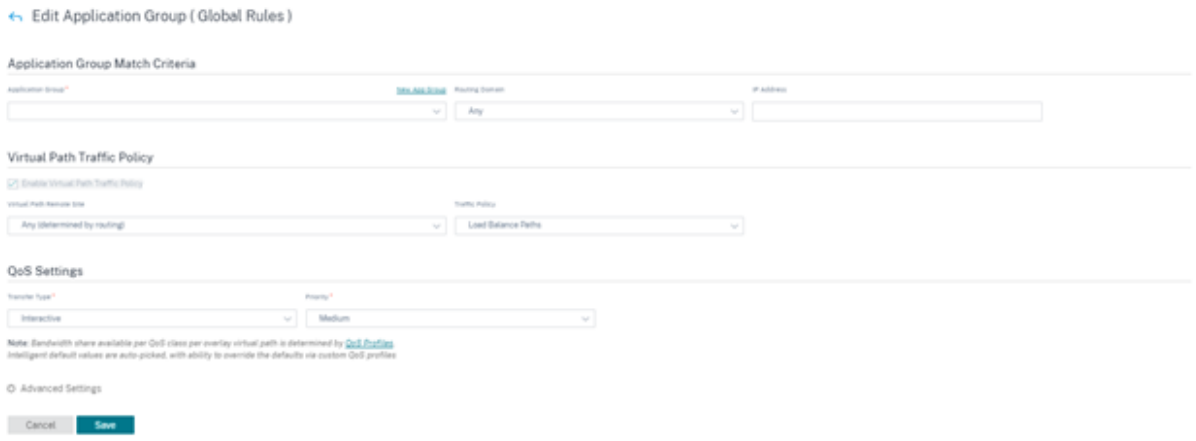

### Crear reglas de grupos de aplicaciones

Puede crear reglas para un grupo de aplicaciones. Para crear reglas de grupos de aplicaciones, vaya a **Configuración > QoS > Directivas de QoS** > **Reglas de grupos de aplicaciones**. Seleccione la ficha **Reglas globales** para crear reglas de grupos de aplicaciones a nivel global o **Reglas específicas de sitio/grupo** para crear reglas al nivel de sitio.

Haga clic en **Nueva regla de grupo** de **aplicaciones en la sección Reglas del grupo** de aplicaciones. Haga clic en **Nuevo grupo de aplicaciones** junto al nombre **del campo Grupo de aplicaciones**. Escriba un nombre para el grupo de aplicaciones. Busque y agregue aplicaciones según sea necesario. Haga clic en **Guardar**.

Introduzca los detalles en los demás campos según sea necesario. Para obtener información sobre las descripciones de los campos, consulte Crear reglas de aplicación.




### Verificar las reglas de aplicación

Para comprobar las reglas de la aplicación, vaya a **Informes > Tiempo real > Flujos**. Seleccione el sitio del que quiere ver la información de flujo y el número de flujos que quiere mostrar. Haga clic en **Personalizar columnas** y seleccione las casillas de verificación correspondientes a la información de flujo que quiere ver. Compruebe si la información de flujo se ajusta a las reglas configuradas.

Vaya a **Informes > Tiempo real > Estadísticas** y seleccione **Reglas**. Elija el sitio y haga clic en **Recuperar los datos más recientes**. Compruebe las reglas configuradas.

Para obtener más información sobre los informes, consulte Flujos.

## HDX QoE

October 31, 2022

Los parámetros de red, como la latencia, la fluctuación y la caída de paquetes, afectan a la experiencia de usuario de los usuarios de HDX. La calidad de la experiencia (QoE) ayuda a los usuarios a comprender y comprobar la calidad de la experiencia de su ICA. QoE es un índice calculado que indica el rendimiento del tráfico ICA. Los usuarios pueden ajustar las reglas y la directiva para mejorar la QoE.

La QoE es un valor numérico entre 0 y 100, cuanto mayor sea el valor, mejor será la experiencia del usuario.

Los parámetros utilizados para calcular la QoE se miden entre los dos dispositivos Citrix SD-WAN ubicados en el lado del cliente y del servidor, y no entre el cliente o los propios dispositivos del servidor. La latencia, la fluctuación y la caída de paquetes se miden en el nivel de flujo y pueden ser diferentes

de las estadísticas en el nivel de enlace. Es posible que la aplicación de host final (cliente o servidor) nunca sepa que hay una pérdida de paquetes en la WAN. Si la retransmisión se realiza correctamente, la tasa de pérdida de paquetes de nivel de flujo es inferior a la pérdida de nivel de enlace. Sin embargo, como resultado, podría aumentar un poco la latencia y la fluctuación.

Puede ver una representación gráfica de la calidad general de las aplicaciones HDX en el panel de HDX de Citrix SD-WAN Orchestrator for On-premises. Las aplicaciones HDX se clasifican en las tres categorías de calidad siguientes:

| Calidad | Rango QoE |
|---|---|
| Bueno | 71-100 |
| Normal | 51-70 |
| Mala | 0-50 |

Según la página de la interfaz de usuario seleccionada, en el panel de control de HDX se muestra una lista de los cinco sitios, cinco usuarios, cinco sesiones o todos ellos inferiores (con una calidad mínima de QoE).

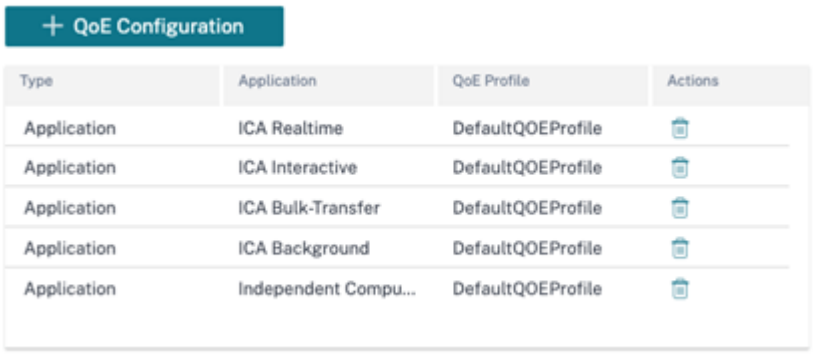
Una representación gráfica de la QoE para diferentes intervalos de tiempo le permite supervisar el rendimiento de las aplicaciones HDX en cada sitio.

### Configurar HDX QoE

1. A nivel de red, vaya a **Configuración > Configuración y grupos de aplicaciones > Configuración de calidad de la aplicación** y haga clic en **+ Configuración de QoE**. Agregue las siguientes aplicaciones mediante el perfil de QoE que quiera utilizar para calcular el comportamiento de HDX:

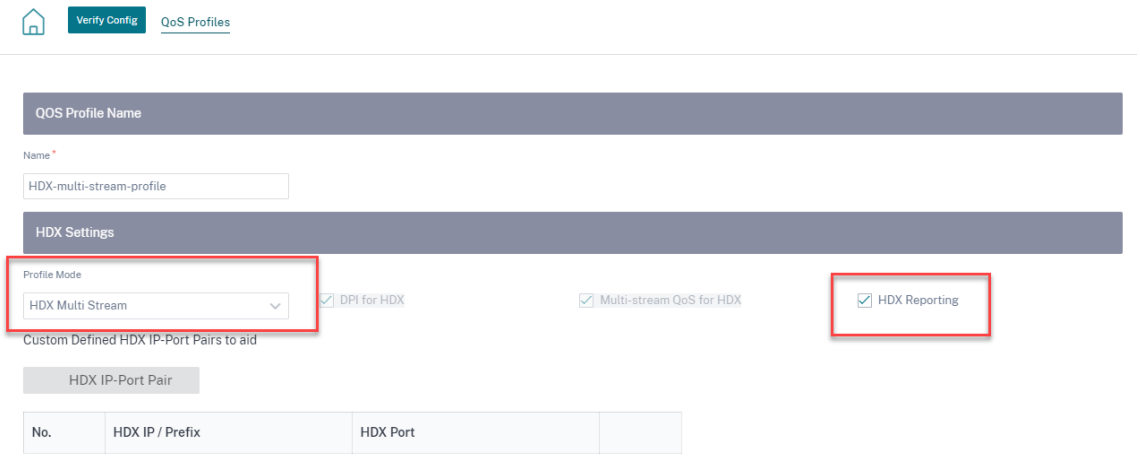
    - ICA en tiempo real (ica_priority_0)
    - ICA interactiva (ica_priority_1)
    - Transferencia masiva ICA (ica_priority_2)
    - Antecedentes ICA (ica_priority_3)
    - Arquitectura informática independiente (Citrix) (ICA)



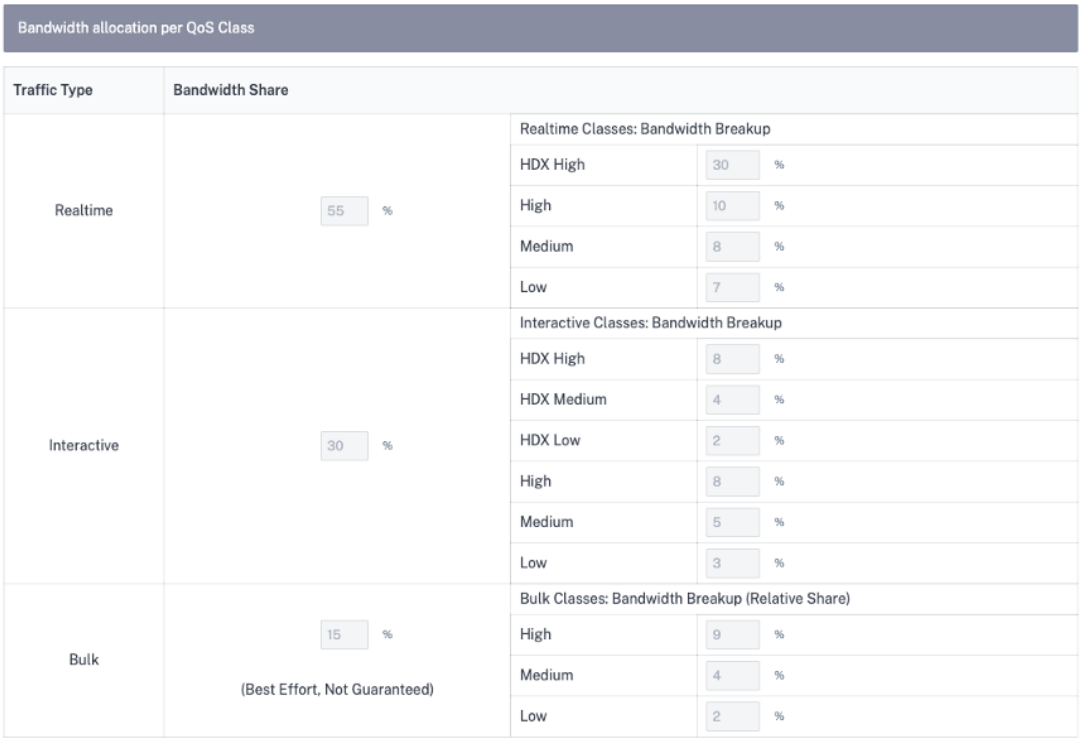

Estas configuraciones proporcionan los parámetros para medir el rendimiento de HDX utilizados en el informe HDX a través del perfil. Se requiere la configuración de ICA Real-Time, ICA Interactive, ICA Bulk-Transfer e ICA Background para las conexiones HDX Multi-Stream (MSI), y se requiere una arquitectura de computación independiente (Citrix) para las conexiones de transmisión única (SSI).

2. Vaya a **Configuración > QoS > Perfiles de QoS**. Seleccione **Standard-HDX-Multistream** como perfil de QoS predeterminado y active la casilla de verificación **HDX Reporting**. Borre los **informes de HDX** si no se requieren los informes de HDX.

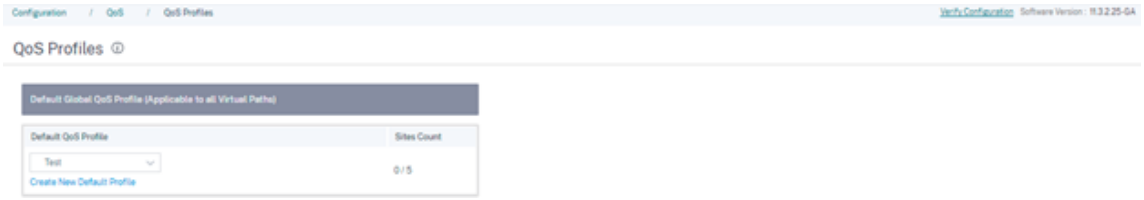



En cada perfil de QoS, hay un porcentaje de ancho de banda predefinido para cada clase. Se pueden configurar para ajustar el ancho de banda asignado a las clases que utiliza el tráfico HDX.



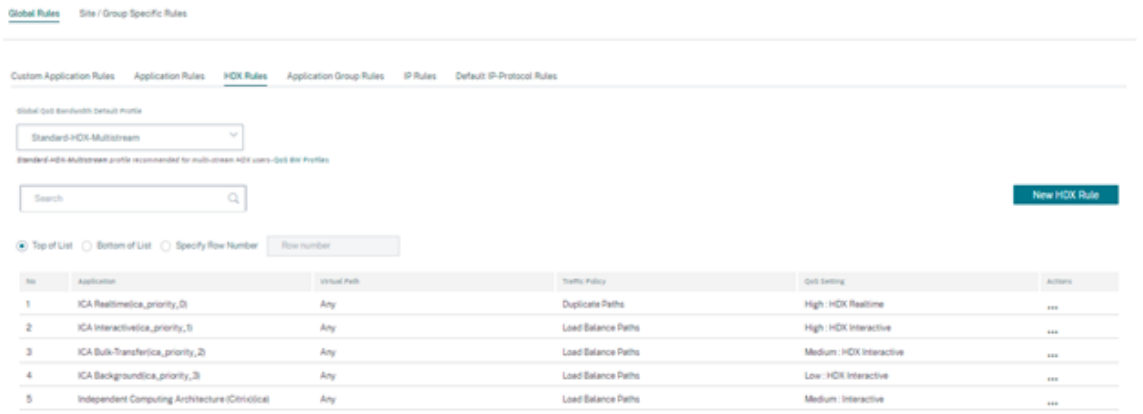

3. Asegúrese de que el nuevo perfil de QoS se utilice activamente comprobando el indicador **de recuento de sitios**.




4. Vaya a **Configuración > QoS > Directivas de QoS** > **Reglas HDX**y configure el nuevo perfil de QoS con los informes de HDX habilitados como **perfil predeterminado de ancho de banda de QoS global**.

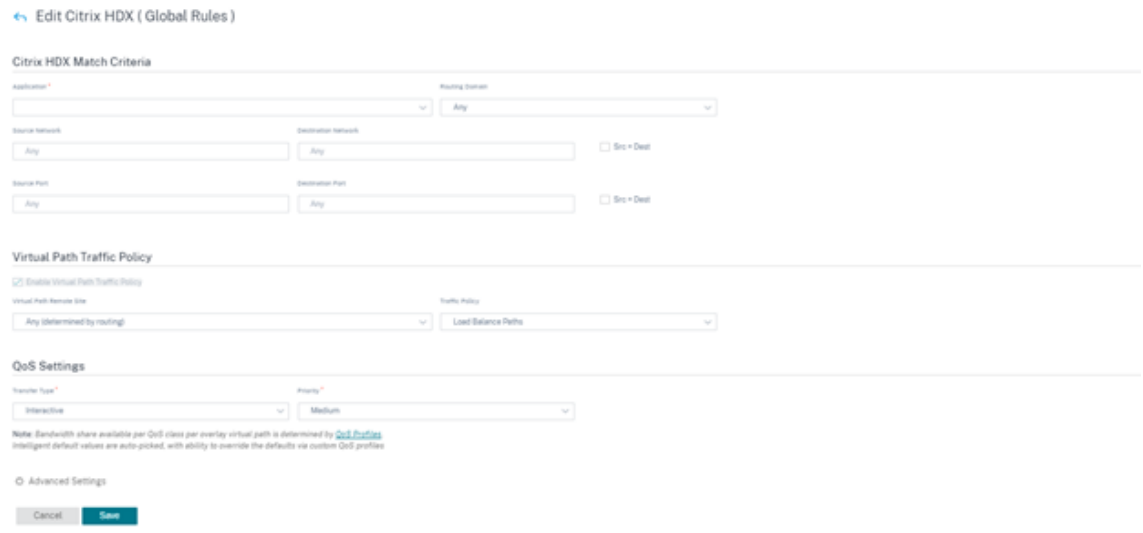

5. Agregue reglas HDX. Estas configuraciones asignan los ajustes de QoS adecuados a las conexiones HDX. Para comprobar los detalles de las reglas o editarlas, navegue hasta la sección inferior de la página de **reglas de HDX**. En la tabla Reglas, vaya a la columna **Acciones** y seleccione **Modificar**. Para cambiar la configuración de cualquier regla predeterminada, haga clic en **Clonar** y realice las modificaciones necesarias.

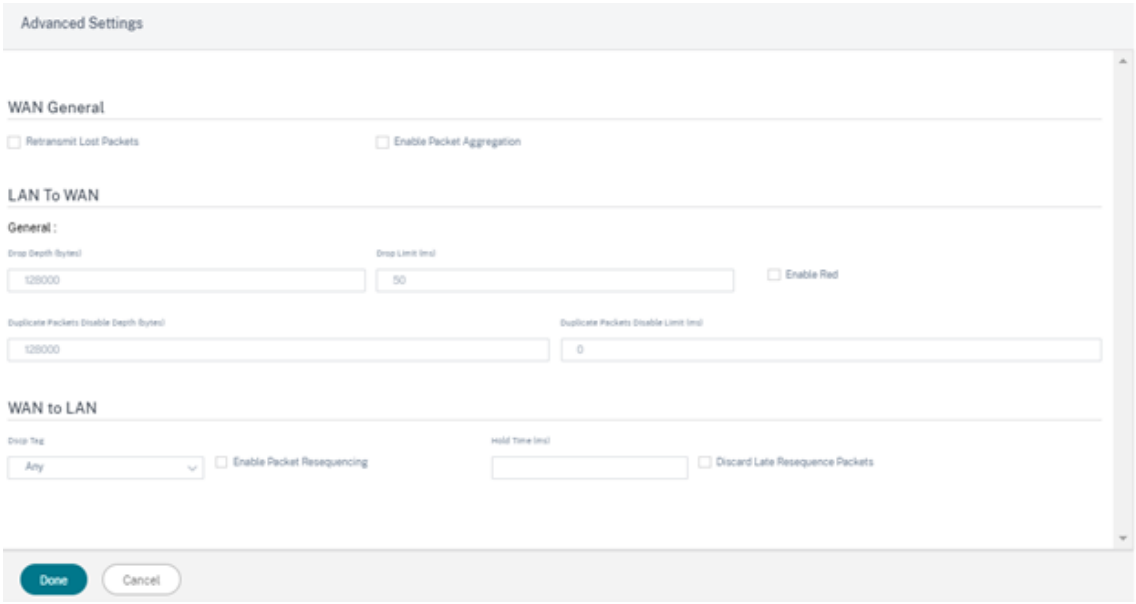



Estas configuraciones se pueden modificar:

- Clase de QoS: En tiempo real, interactiva, masiva
- Directiva de tráfico:
  - **Rutas duplicadas**: El tráfico se duplicará en varias rutas para aumentar la confiabilidad.
  - **Ruta persistente**: El tráfico de un flujo permanecerá en la misma ruta, a menos que la ruta deje de estar disponible.
  - **Rutas de equilibrio de carga**: El tráfico de un flujo se equilibra en varias rutas.
  - **Configuración avanzada**: Defina directivas de retransmisión, RED y paquetes atrasados.






## Panel e informes HDX

Citrix SD-WAN Orchestrator for On-premises proporciona el panel HDX para realizar mediciones actualizadas y detalladas de la experiencia del usuario de Citrix Virtual Applications and Desktops en la red, para cada sitio, usuario y sesión.

Hay dos tipos de sesiones HDX: Una secuencia única y multi-stream. Una sesión de flujo único solo tiene una conexión en la sesión, mientras que una sesión de varias secuencias tiene cuatro. Las sesiones de varias secuencias permiten una QoS más avanzada. La conexión en una sesión HDX de una sola secuencia predeterminada es la clase interactiva, mientras que la conexión de prioridad superior de una sesión HDX multi-stream predeterminada a clase en tiempo real y los otros tres a clase interactiva. Esto es configurable.

La puntuación de calidad de experiencia (QoE) es un valor numérico entre 0 y 100. Cuanto mayor sea el valor, mejor será la experiencia del usuario. El QoE del tráfico de clase en tiempo real se calcula en función de la fluctuación, la latencia y la tasa de pérdida. La clase interactiva QoE se calcula sobre la base de la tasa de ráfaga y la tasa de pérdida. El QoE de una sesión es el promedio de todas las conexiones de la sesión. El QoE de un usuario es el promedio de todas las sesiones iniciadas por ese usuario. El QoE de un sitio es el promedio de todas las sesiones en ese sitio.

Todas las estadísticas son métricas:

- Para el tráfico HDX en ese sitio
- Experimentado por ese usuario
- De todas las conexiones en esa sesión

No incluyen las métricas de otros tipos de tráfico. Las métricas son el promedio del período seleccionado o el total del período seleccionado.

> **Nota:**
>
> Los informes de HDX requieren versiones de software mínimas:
>
> - Citrix Virtual Apps and Desktops 7-1912 LTSR (o versión actual)
> - Aplicación Citrix Workspace para Windows 19.12 LTSR (o versión actual)
> - SD-WAN 11.2.0 (o versión actual)

Citrix siempre recomienda utilizar la versión de software más reciente para obtener las mejoras y correcciones de errores más recientes. Por ejemplo, SD-WAN requiere las versiones 11.2.3 u 11.3.1 para admitir los nuevos comandos de EDT introducidos en las versiones posteriores de Citrix Virtual Apps and Desktops LTSR.

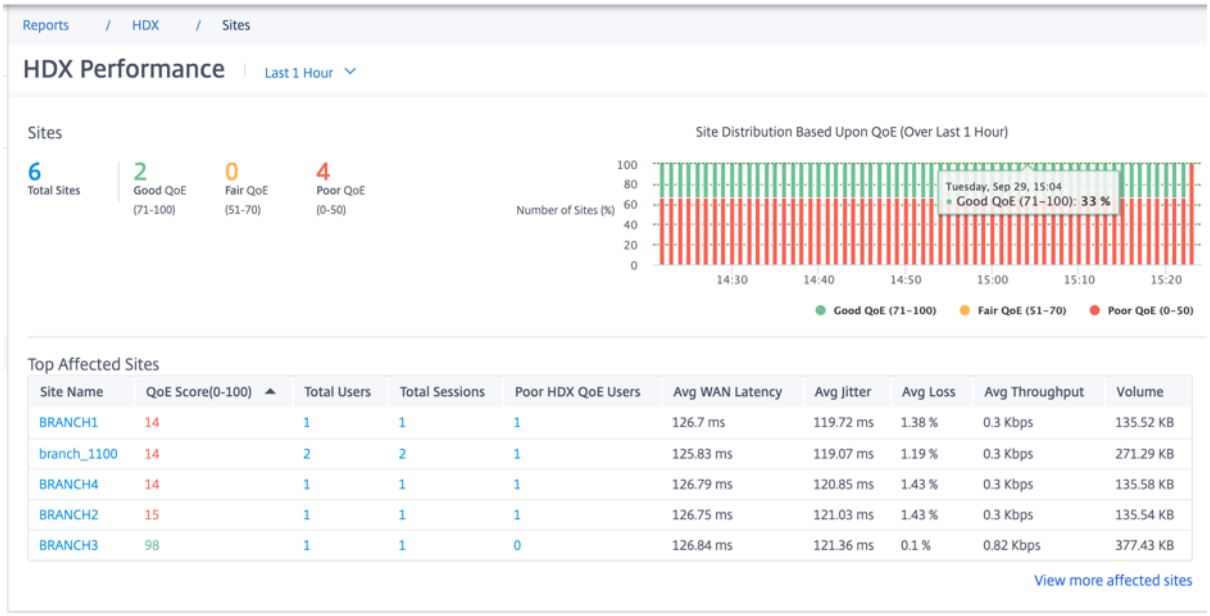
Los clientes de Mac y Linux no son totalmente compatibles con la generación de informes de múltiples flujos de ICA y HDX a través de Citrix SD-WAN. Por ejemplo, los clientes de Linux admiten múltiples transmisiones, pero carecen de detalles como el tiempo de ida y vuelta y el retraso. La tabla de funciones de CWA proporciona información sobre qué sistemas operativos admiten las funciones **ICA multipuerto** y **HDX Insight con NSAP VC**.

Los usuarios deben acceder a HDX fuera del cifrado de Citrix Gateway, ya sea mediante el acceso directo a StoreFront o mediante el uso de Beacon Points o el servicio de ubicación de red.

### Sitios

Este informe HDX proporciona datos HDX detallados por sitio. Para ver las estadísticas del sitio, vaya a **Informes** > **HDX** > **Sitios**.




El panel informa sobre el sitio con tráfico HDX ejecutándose durante el intervalo de tiempo seleccionado (por ejemplo, los últimos 5 minutos, los últimos 30 minutos, el último día, el último mes, etc.). El rendimiento del sitio se clasifica como bueno (71-100), justo (51-70) o pobre (0-50) en función del QoE del tráfico HDX del sitio. El valor de QoE de la sección de resumen y **de la tabla de sitios más afectados** es el valor promedio durante el período de tiempo seleccionado. El informe gráfico de la serie temporal muestra una historia detallada con lapso de tiempo. Cada barra muestra el porcentaje de sitios QoE buenos, justos y pobres en ese momento.

También puede ver el número de sitios en porcentaje que tienen una QoE buena, equitativa y mala en ese momento en el gráfico **Distribución de sitios basada en la QoE**. Pase el ratón sobre la barra de colores para ver el número porcentual de sitios en un estado bueno/justo/pobre.

**NOTA**

- Las estadísticas se recopilan en una dirección, desde el lado remoto hasta el sitio actual. Por ejemplo, para una sesión entre el sitio-A y el sitio-B, el informe del sitio-A se recopila sobre el tráfico procedente del sitio-B al sitio-A, mientras que el informe del sitio-B se recopila sobre el tráfico procedente del Sitio-A al sitio-B. Por lo tanto, las estadísticas de la misma sesión en el Sitio-A y el Sitio-B pueden ser diferentes.
- La **tabla de sitios más afectados** refleja solo los 5 sitios más afectados. De forma predeterminada, muestra los 5 sitios con las puntuaciones de QoE más bajas. Pero cada columna es ordenable, ascendente o descendente, y se utiliza como criterio de consulta. Por ejemplo, al hacer clic en el título de la columna **Avg Jitter**, se mostrarán los 5 sitios con la fluctuación promedio más baja o la fluctuación promedio más alta. Lo mismo para otras columnas. Para ver los detalles de todos los sitios con tráfico de HDX durante el período de tiempo

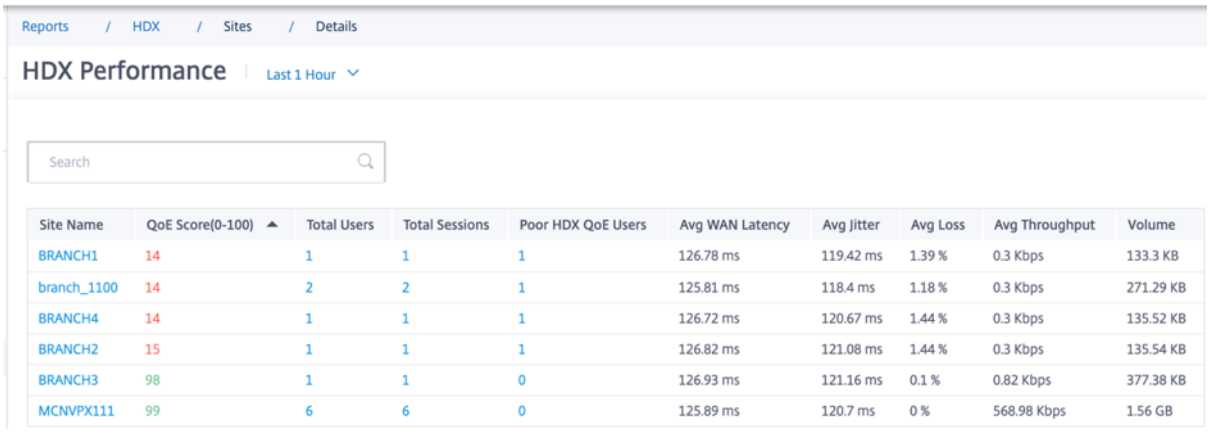
> seleccionado, haga clic en **Ver más sitios afectados**.

Los siguientes son los detalles de cada sitio:

- **Nombre del sitio**: El nombre del sitio.
- **Puntuación de QoE (0-100)**: La puntuación QoE promedio de este sitio.
- **Total de usuarios**: El número total de usuarios de HDX activos que se vieron en el sitio durante el período seleccionado.
- **Sesiones totales**: El número total de sesiones HDX vistas en el sitio durante el período seleccionado, incluidas las sesiones de transmisión única y las de transmisión múltiple.
- **Usuarios deficientes de QoE de HDX**: Número de usuarios de HDX que sufren una QoE deficiente (inferior a 50).
- **Latencia WAN**promedio: Latencia promedio en la WAN, desde el sitio remoto hasta este sitio.
- **Fluctuación**promedio: El valor de fluctuación promedio para la duración seleccionada.
- **Pérdida promedio**: El valor porcentual promedio de pérdida de paquetes durante la duración seleccionada.
- **Rendimiento promedio**: El valor promedio del rendimiento de datos durante la duración seleccionada.
- **Volumen**: El volumen total de tráfico visto en este sitio. La GUI de Citrix SD-WAN Orchestrator for On-premises puede ajustar y cambiar la unidad en función del valor numérico.

Al hacer clic en cualquier título de columna se muestra el informe ordenado en esa columna. Haga clic en **Ver más sitios afectados** para ver los informes de todos los sitios. Al hacer clic en una sola fila se muestra el informe detallado de ese sitio.

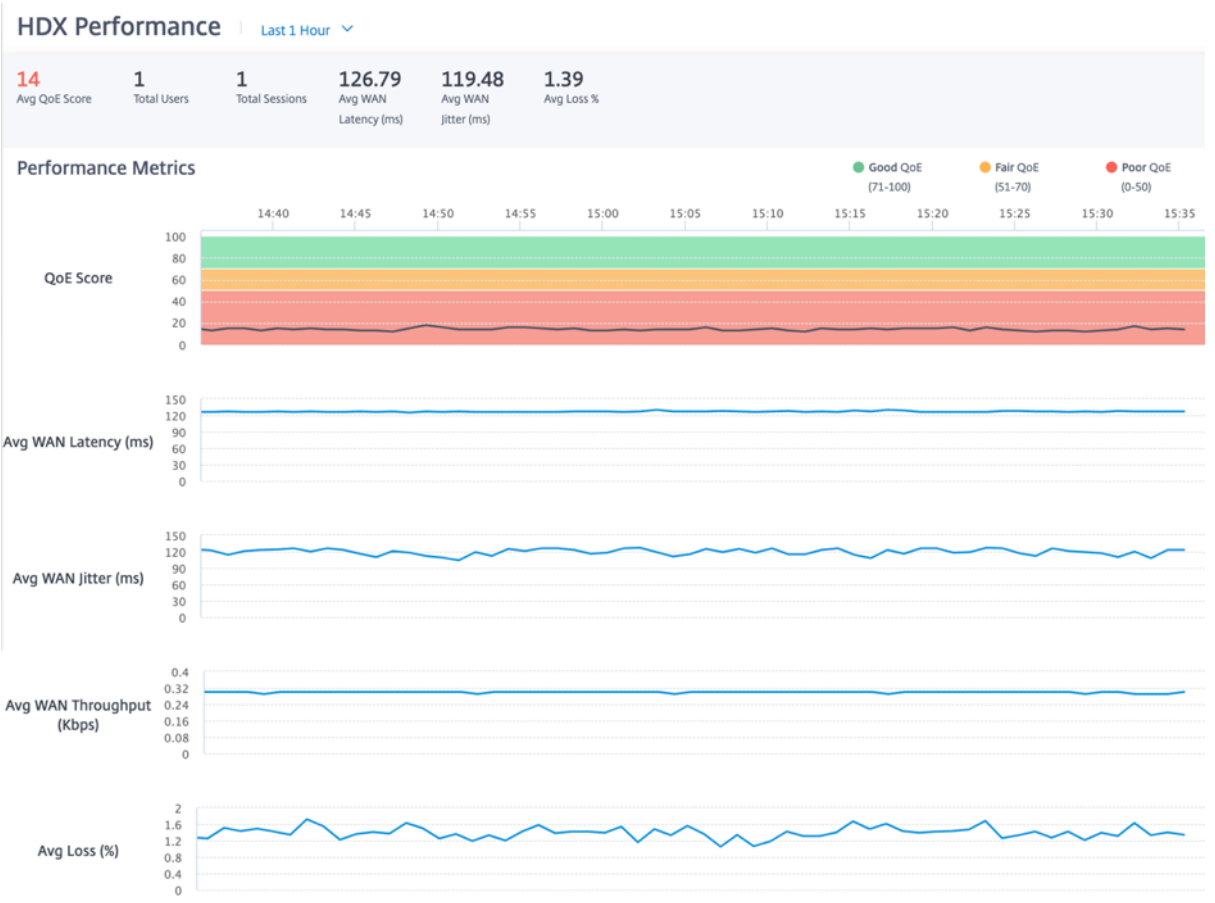
La tabla de la siguiente captura de pantalla es un ejemplo de la tabla de informes que muestra todos los sitios. Tiene las mismas columnas que la tabla de **sitios más afectados**.




| Site Name | QoE Score(0-100) | Total Users | Total Sessions | Poor HDX QoE Users | Avg WAN Latency | Avg Jitter | Avg Loss | Avg Throughput | Volume |
|---|---|---|---|---|---|---|---|---|---|
| BRANCH1 | 14 | 1 | 1 | 1 | 126.78 ms | 119.42 ms | 1.39 % | 0.3 Kbps | 133.3 KB |
| branch_1100 | 14 | 2 | 2 | 1 | 125.81 ms | 118.4 ms | 1.18 % | 0.3 Kbps | 271.29 KB |
| BRANCH4 | 14 | 1 | 1 | 1 | 126.72 ms | 120.67 ms | 1.44 % | 0.3 Kbps | 135.52 KB |
| BRANCH2 | 15 | 1 | 1 | 1 | 126.82 ms | 121.08 ms | 1.44 % | 0.3 Kbps | 135.54 KB |
| BRANCH3 | 98 | 1 | 1 | 0 | 126.93 ms | 121.16 ms | 0.1 % | 0.82 Kbps | 377.38 KB |
| MCNVPX111 | 99 | 6 | 6 | 0 | 125.89 ms | 120.7 ms | 0 % | 568.98 Kbps | 1.56 GB |

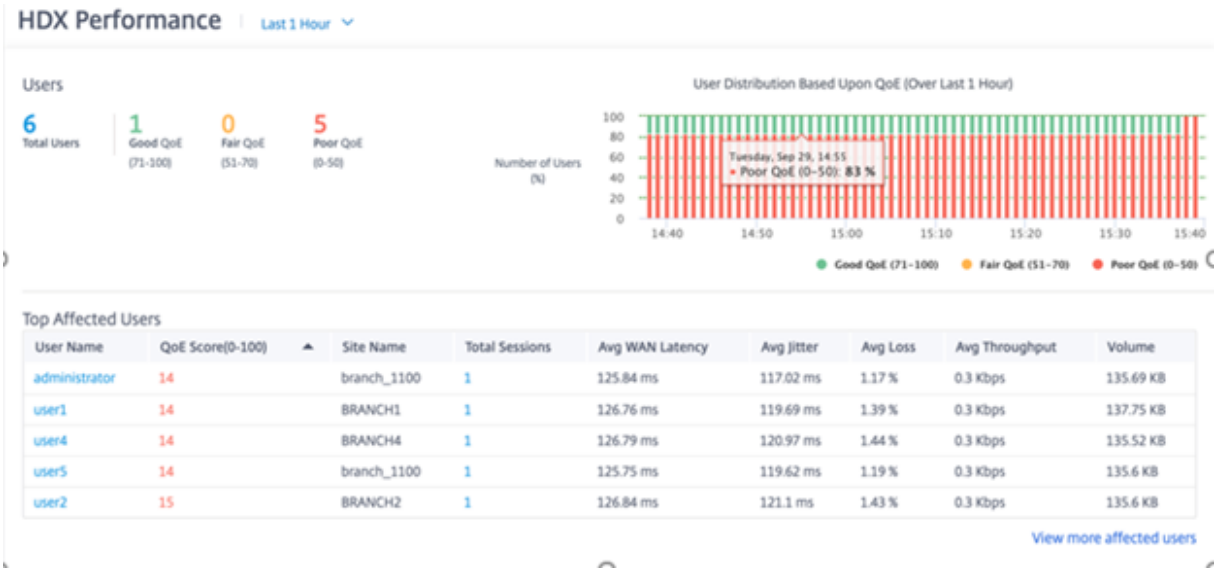
Haga clic en la fila de emplazamiento individual para ver una representación gráfica de las métricas de rendimiento. Al pasar el ratón sobre el gráfico, se proporcionan más detalles.




## Usuarios

Para ver el informe de usuarios de HDX, vaya a **Informes > HDX > Usuarios**.




El informe de usuario muestra el rendimiento experimentado por cada usuario durante el período se-

leccionado (por ejemplo, los últimos 5 minutos, los últimos 30 minutos, el último día, el último mes, etc.). Si el usuario ha estado en varios sitios durante el período seleccionado, el último sitio desde el que el usuario inició sesión se muestra en el informe. La experiencia del usuario se clasifica como buena (71-100), justa (51-70) o mala (0-50) en función de la puntuación QoE de su tráfico HDX. Los valores de QoE de la sección de resumen y de la tabla de **usuarios más afectados** son los valores promedio del período seleccionado. El informe gráfico de la serie temporal muestra una historia detallada con lapso de tiempo. Cada barra muestra el porcentaje de usuarios con QoE buena, justa y deficiente en ese momento.

También puede ver el número de usuarios en porcentaje que tienen una QoE buena, justa y mala en ese momento en el gráfico **Distribución de usuarios basada en la QoE**. Pase el ratón hacia la barra de colores para ver el porcentaje de usuarios en buen estado, justo o pobre.

**Información de identificación personal** Actualmente, los informes de QoE de HDX tienen los siguientes dos campos de información de identificación personal (PII):

- **Nombre de usuario**: muestra el nombre de usuario.
- **Dirección IP**: muestra la dirección IP del cliente.

> **NOTA**
>
> - Cuando el nombre de usuario no está disponible, la dirección IP aparece en el campo **Nombre de usuario**.
> - Los informes de usuario HDX se basan en estadísticas de la SD-WAN del lado del cliente, no de la SD-WAN del lado del Virtual Delivery Agent (VDA). Esto refleja la experiencia HDX del usuario final.
> - La **tabla de usuarios más afectados** refleja solo los 5 usuarios más afectados. De forma predeterminada, muestra los 5 mejores usuarios con el QoE más bajo. Pero cada columna es ordenable, ascendente o descendente, y se utiliza como criterio de consulta. Por ejemplo, al hacer clic en el título de la columna **Avg Jitter**, se mostrarán los 5 usuarios con la fluctuación promedio más baja o la fluctuación promedio más alta. Para ver los detalles de todos los usuarios que tienen tráfico de HDX durante el período seleccionado, haga clic en **Ver más usuarios afectados**.

Los siguientes son los detalles de cada usuario:

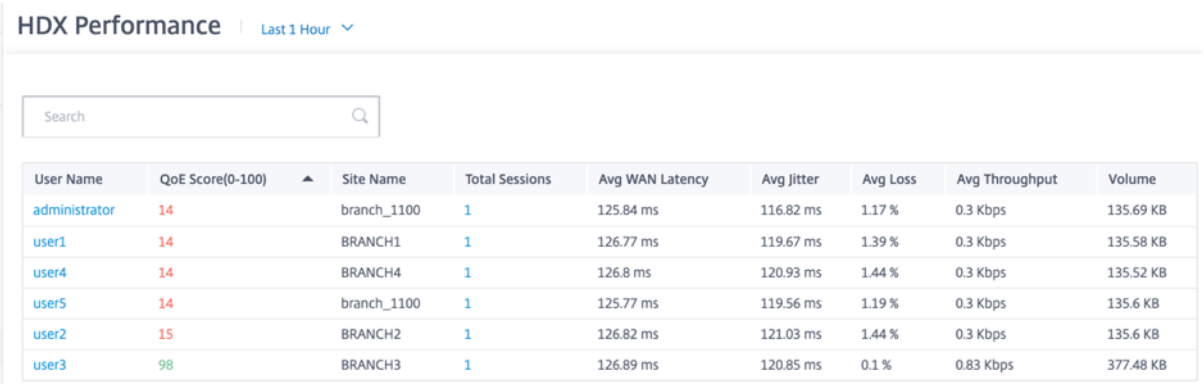
- **Nombre de usuario**: El nombre de usuario.
- **Puntuación de QoE (0-100)**: La puntuación QoE promedio de este usuario.
- **Nombre del sitio**: El nombre del sitio desde el que el usuario inició sesión.
- **Sesiones totales**: El número total de sesiones HDX activas de ese usuario, incluidas las sesiones de transmisión única y las de transmisión múltiple.

- Latencia**promedio de WAN: Latencia**promedio en la WAN, experimentada por el lado del cliente.
- **Fluctuación**promedio: El valor de fluctuación promedio para la duración seleccionada.
- **Pérdida promedio**: El valor porcentual promedio de pérdida de paquetes durante la duración seleccionada.
- **Rendimiento promedio**: El valor promedio del rendimiento de datos durante la duración seleccionada.
- **Volumen**: El volumen total de tráfico utilizado por este usuario. La GUI de Citrix SD-WAN Orchestrator for On-premises puede ajustar y cambiar la unidad en función del valor numérico.

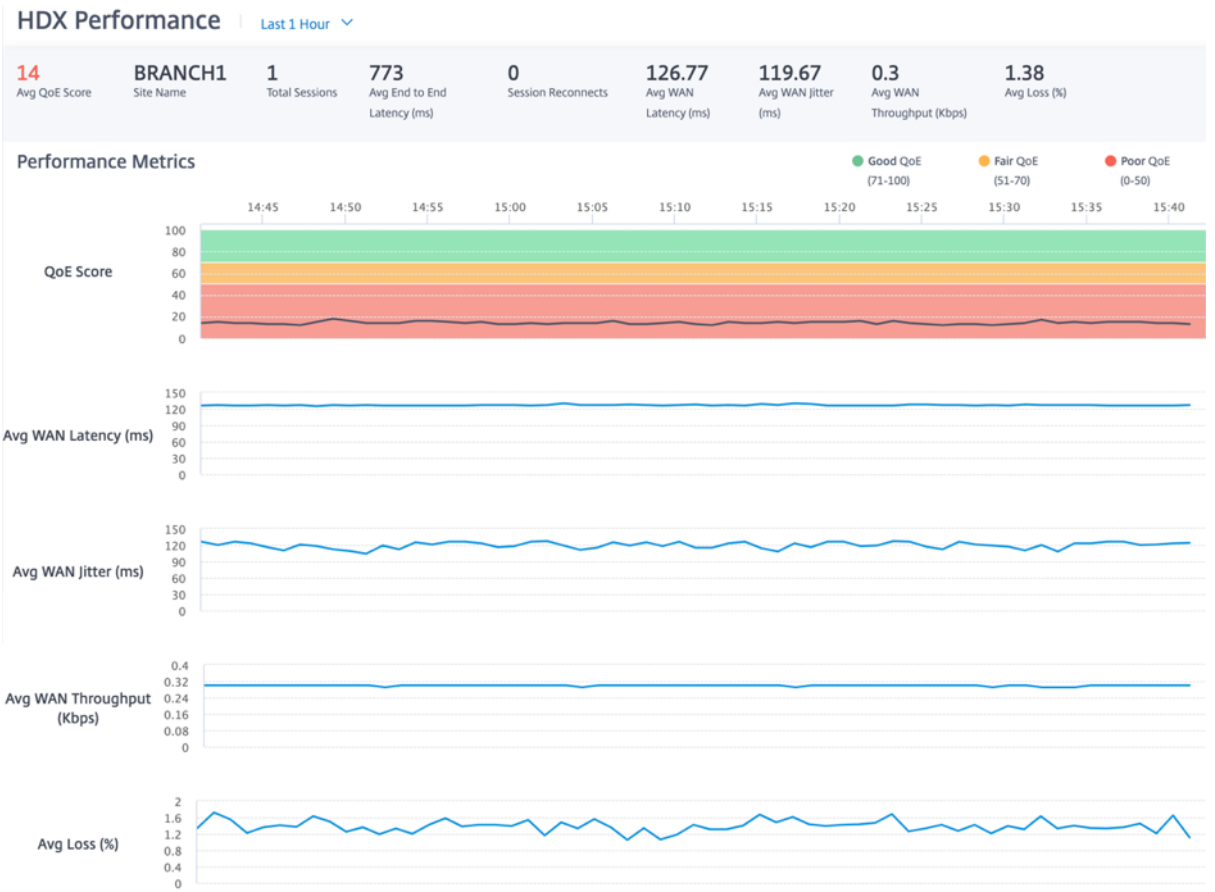
Al hacer clic en cualquier título de columna se muestra el informe ordenado en esa columna. Haga clic en **Ver más usuarios afectados** para ver los informes de todos los usuarios. Al hacer clic en una sola fila se muestra el informe detallado de ese usuario.

La siguiente captura de pantalla es un ejemplo del informe que muestra todos los usuarios. Tiene las mismas columnas que la tabla de **usuarios más afectados**.



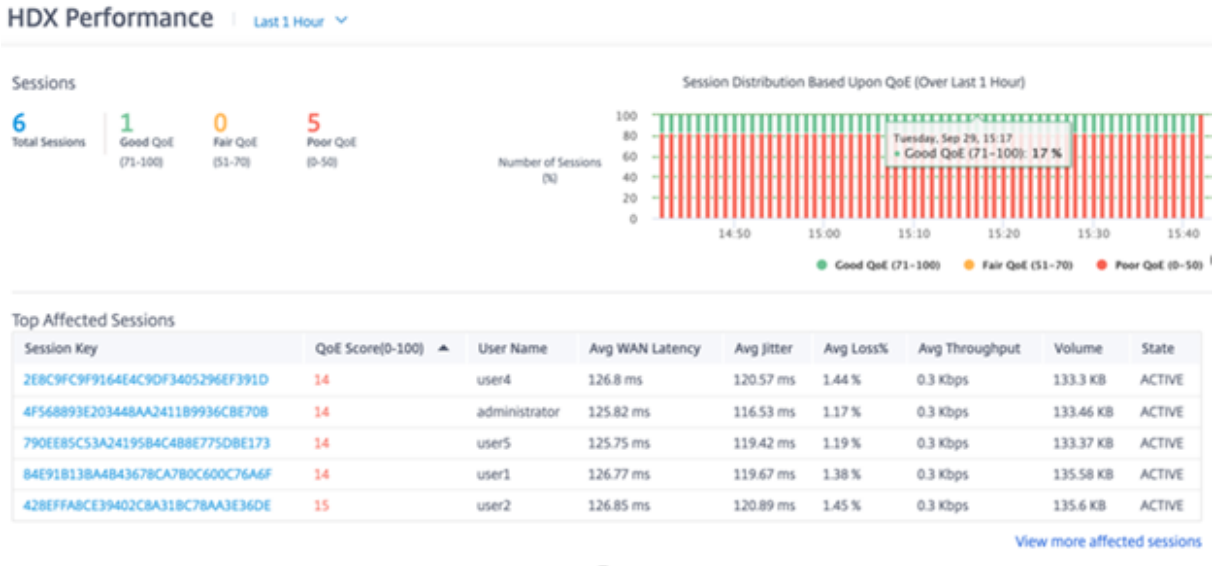

Haga clic en una fila de usuario individual para ver una representación gráfica de las métricas de rendimiento de ese usuario.




**Sesiones**

El informe Sesión proporciona detalles al nivel de sesión. Para ver el informe de la sesión, vaya a **Informes > HDX > Sesiones**.



El panel muestra los informes de las sesiones de HDX ejecutadas durante el período seleccionado (por ejemplo, los últimos 5 minutos, los últimos 30 minutos, el último día, el último mes, etc.). Las sesiones se clasifican como buenas (71-100), justas (51-70) o pobres (0-50) en función del QoE de esa sesión. El valor QoE de la sección de resumen y la tabla Principal Afectados es el valor medio a lo largo del período seleccionado. El informe gráfico de la serie temporal muestra una historia detallada con lapso de tiempo. Cada barra muestra el porcentaje de sesiones de QoE buenas, justas y deficientes en ese momento.

También puede ver el número de sesiones en porcentaje, con una QoE buena, justa y mala en ese momento en el gráfico **Distribución de sesiones basada en la QoE**. Pase el ratón hacia la barra de colores para ver el porcentaje de sesiones en buen estado, justo o pobre.

> **Nota**
>
> - Los informes de sesión HDX se basan en estadísticas de la SD-WAN del lado del cliente, no de la SD-WAN del lado VDA. Esto refleja la experiencia HDX del usuario final.
> - La **tabla Sesiones más afectadas** refleja solo las 5 sesiones más afectadas. De forma predeterminada, muestra las 5 sesiones principales con el QoE más bajo. Pero cada columna es ordenable, ascendente o descendente, y se utiliza como criterio de consulta. Por ejemplo, al hacer clic en el título de la columna **Avg Jitter**, se mostrarán las 5 sesiones con la fluctuación promedio más baja o la fluctuación promedio más alta. Para ver los detalles de todas las sesiones de HDX durante el período de tiempo seleccionado, haga clic en **Ver más sesiones afectadas**.

Los siguientes son los detalles de la parte superior de cada sesión:

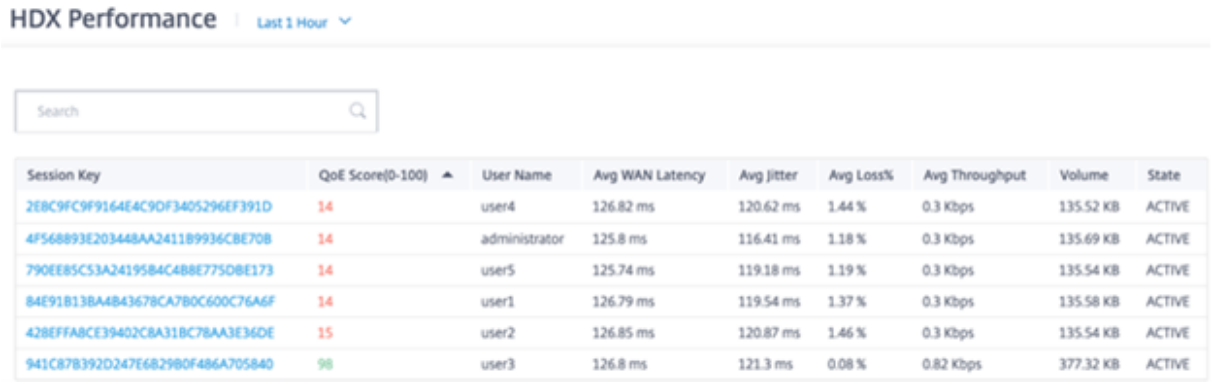
- **Clave de sesión**: La identidad única de una sesión HDX.
- **Puntuación de QoE (0-100)**: La QoE promedio de esta sesión.
- **Nombre de usuario**: El nombre de usuario.
- **Latencia WAN promedio**: La latencia WAN promedio de la sesión durante la duración seleccionada, medida en el lado del cliente.
- **Fluctuación**promedio: El valor de fluctuación promedio de la sesión durante la duración seleccionada.
- **% de pérdida**promedio: El valor porcentual de pérdidas promedio de la sesión durante la duración seleccionada.
- **Rendimiento promedio**: El valor de rendimiento promedio de la sesión durante la duración seleccionada.
- **Volumen**: El volumen total de tráfico utilizado en esta sesión. La GUI de Citrix SD-WAN Orchestrator for On-premises puede ajustar y cambiar la unidad en función del valor numérico.
- **Estado**: Estado de la sesión.

Al hacer clic en el título de cualquier columna, se muestra el informe ordenado en esa columna. Haga

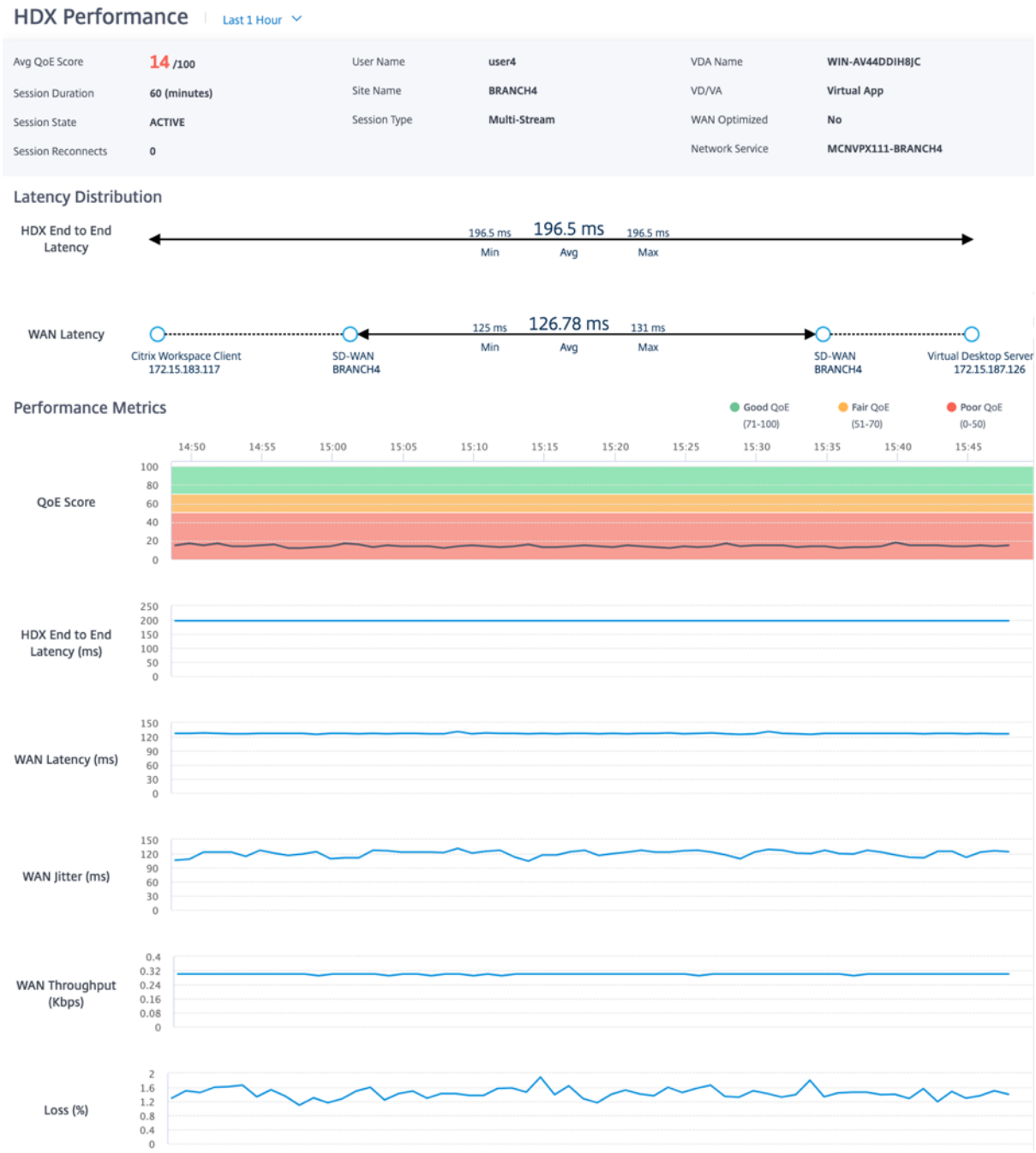
clic en **Ver más sesiones afectadas** para ver los informes de todas las sesiones. Al hacer clic en una sola fila se muestra el informe detallado de esa sesión.

La siguiente captura de pantalla es un ejemplo de la tabla de informes que muestra todas las sesiones. Tiene las mismas columnas que la tabla **Sesiones más afectadas**.




Haga clic en la clave de sesión individual para ver una representación gráfica de las métricas de rendimiento junto con los detalles sobre todas las variables que afectan a QoE.




- **Puntuación promedio de QoE**: La QoE promedio durante el período seleccionado.
- **Nombre de usuario**: El usuario que inició esta sesión.
- **Nombre del VDA**: Nombre del VDA desde el que se entrega el escritorio/la aplicación publicados.
- **Duración de la sesión**: El tiempo activo de esta sesión en el período seleccionado.
- **Nombre del sitio**: El sitio cliente del usuario cuando se inició la sesión.
- **VD/VA**: Si esta sesión es una sesión de **escritorio virtual** o una sesión de **aplicación virtual**.
- **Estado de la sesión**: El estado de la sesión al final del período seleccionado.

- **Tipo de sesión**: Si la sesión es una sesión de varios flujos o una sesión de transmisión única la última vez que se inició la sesión.
- **Optimizado para WAN**: Si esta sesión estaba optimizada para WAN. Si SD-WAN es plataforma PE, Optimización de WAN está habilitada para HDX y esta sesión está optimizada, entonces este campo muestra verdadero.
- **Reconexiones de sesión**: Si la sesión se ha desconectado y se ha vuelto a conectar automáticamente debido a un problema de red, este campo es el recuento de dichas incidencias.
- **Servicio de red**: Es el nombre del servicio a través del cual se entrega esta sesión.
- **Latencia de extremo a extremo de HDX**: La mitad del valor del tiempo de ida y vuelta entre el VDA y el cliente.
- **Latencia de WAN**: La latencia desde la SD-WAN del lado del VDA hasta la SD-WAN del lado del cliente.

## Reglas de direcciones IP

October 31, 2022

**Las reglas de IP** le ayudan a crear reglas para su red y a tomar determinadas decisiones de calidad de servicio (QoS) basadas en las reglas. Puede crear reglas personalizadas para su red. Por ejemplo, puede crear una regla como: Si la dirección IP de origen es 172.186.30.74 y la dirección IP de destino es 172.186.10.89, establezca la **directiva de tráfico** como **ruta persistente** y el **tipo de tráfico** como **tiempo real**.

Puede crear reglas para el flujo de tráfico y asociarlas con aplicaciones y clases. Puede especificar criterios para filtrar el tráfico de un flujo y aplicar el comportamiento general, el comportamiento de LAN a WAN, el comportamiento de WAN a LAN y las reglas de inspección de paquetes.

Puede crear reglas de IP globales y específicas del sitio al nivel de red. Si un sitio está asociado a la regla creada globalmente, puede crear reglas específicas para el sitio. En esos casos, las reglas específicas del sitio tienen prioridad y anulan la regla creada globalmente.

Las reglas de protocolo IP predeterminadas HTTP, HTTPS y ALTHTTPS siempre aparecen en la parte superior de la lista de la tabla de reglas. Sin embargo, las reglas IP específicas del sitio (una vez creadas) aparecen por encima de HTTP, HTTPS, ALTHTTPS y las reglas IP globales en la tabla de reglas.

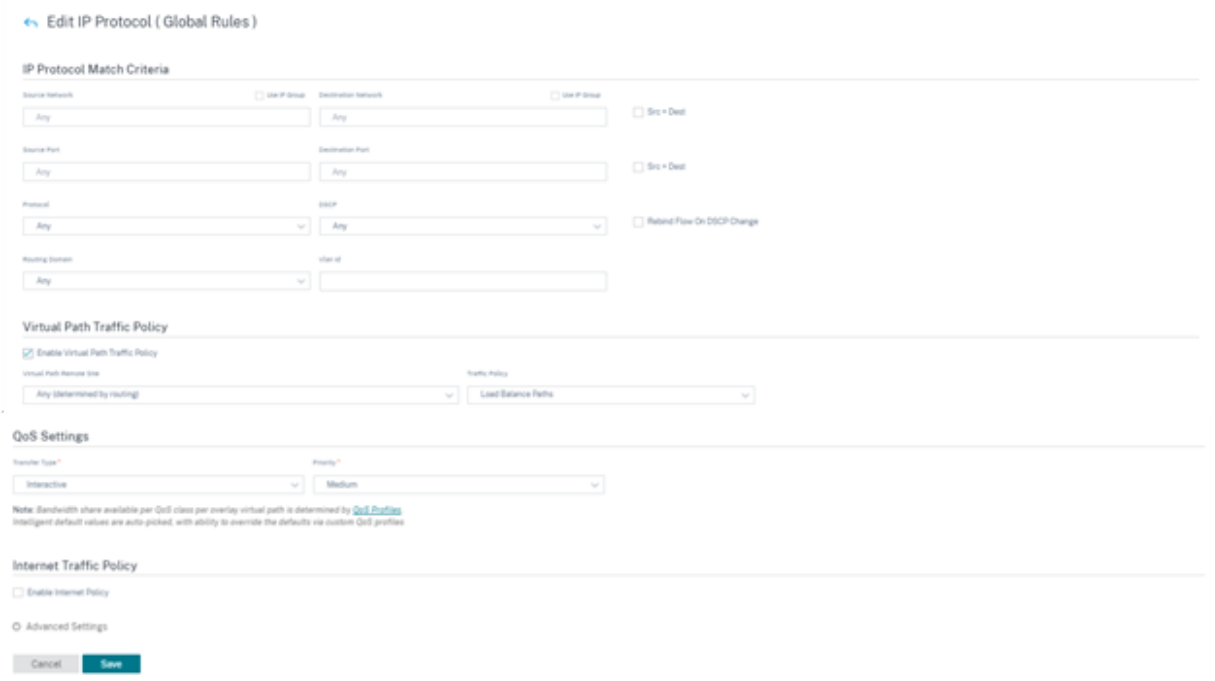
### Crear reglas de IP

Para crear reglas IP, vaya a **Configuración > QoS > Directivas de QoS** > **Reglas IP**. Seleccione la ficha **Reglas globales** para crear reglas de IP a nivel global o **Reglas específicas de sitio/grupo** para crear

reglas al nivel de sitio.

Haga clic en **Nueva regla** de **IP en la sección Reglas** de IP.




- Criterios de coincidencia del protocolo
  - **Agregar o quitar sitios**: (disponible solo al crear una regla de IP específica para el sitio) Seleccione los sitios, haga clic en **Revisar**y **listo**.
  - **Red de origen**: La dirección IP de origen y la máscara de subred con las que coincide la regla.
  - **Red de destino**: La dirección IP y la máscara de subred de destino con las que coincide la regla.
  - **Usar grupo IP**: Seleccione la casilla **Usar grupo IP** para elegir cualquier grupo IP existente de la lista desplegable.
  - **Src = Dst**: Si se selecciona, la dirección IP de origen también se utiliza como dirección IP de destino.
  - **Puerto de origen**: El puerto de origen (o el intervalo de puertos de origen) con el que coincide la regla.
  - **Puerto de destino**: El puerto de destino (o el intervalo de puertos de destino) con el que coincide la regla.
  - **Src = Dst**: Si se selecciona, el puerto de origen también se utiliza como puerto de destino.
  - **Protocolo**: El protocolo con el que coincide la regla. Puede seleccionar uno de los protocolos predefinidos o seleccionar **Cualquiera**o **Número**.
  - **Número de protocolo**: Este campo solo aparece cuando selecciona **Número** en la lista desplegable de **protocolos**. Al seleccionar un número de protocolo, el entero asociado al

protocolo se utiliza para las configuraciones de fondo.
- **DSCP**: La etiqueta DSCP del encabezado IP con la que coincide la regla.
- **Dominio de enrutamiento**: El dominio de enrutamiento con el que coincide la regla.
- **ID de VLAN**: introduzca el identificador de VLAN para la regla. El identificador de VLAN identifica el tráfico que entra y sale de la interfaz virtual. Utilice el identificador de VLAN como 0 para designar el tráfico nativo o sin etiquetar.
- **Revincular el flujo al cambiar el DSCP**: Cuando se selecciona, los flujos que por lo demás son idénticos en términos de criterios de coincidencia se tratan como separados si sus campos de DSCP son diferentes.

- Directiva de tráfico de rutas virtuales

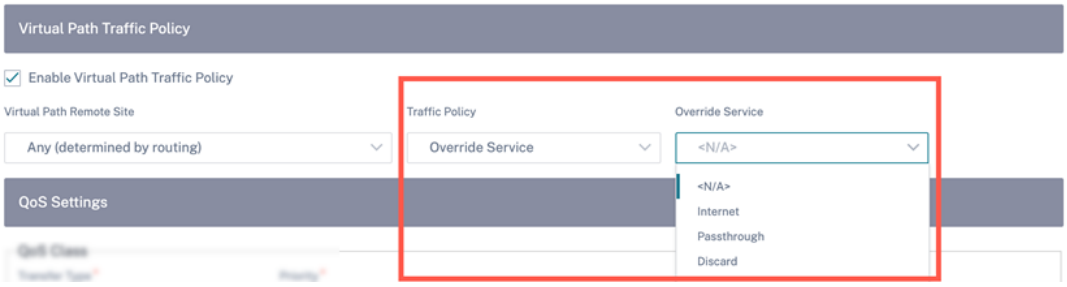
  Seleccione la casilla **Habilitar la directiva de tráfico de rutas virtuales**.

  - **Sitio remoto de ruta virtual**: Seleccione la ruta virtual para el sitio remoto.
  - **Directiva de tráfico**: Elija una de las siguientes directivas de tráfico según sea necesario.
    - **Rutas de equilibrio de carga**: El tráfico de aplicaciones para el flujo se equilibra en varias rutas. El tráfico se envía a través de la mejor ruta hasta que se utiliza esa ruta. Los paquetes restantes se envían a través de la siguiente mejor ruta.
    - **Ruta persistente**: El tráfico de aplicaciones permanece en la misma ruta hasta que la ruta deja de estar disponible. Seleccione una de las siguientes **directivas de persistencia**:
      - **Persistir en el enlace de origen**: El tráfico de la aplicación permanece en el enlace de origen hasta que la ruta ya no esté disponible.
      - **Persiste en el enlace MPLS si está disponible; de lo contrario, en el enlace de origen**: El tráfico de la aplicación permanece en el enlace MPLS. Si el enlace MPLS no está disponible, el tráfico permanece en el enlace de origen.
      - **Persiste en el enlace de Internet si está disponible, de lo contrario en el enlace de origen**: El tráfico de la aplicación permanece en el enlace de Internet. Si el enlace de Internet no está disponible, el tráfico permanece en el enlace de origen.
      - **Persiste en el enlace de la intranet privada si está disponible; de lo contrario, en el enlace de origen**: El tráfico de la aplicación permanece en el enlace de la intranet privada Si el enlace de la intranet privada no está disponible, el tráfico permanece en el enlace de origen.

      **La impedancia de persistencia** es el tiempo (en ms) hasta que el tráfico de la aplicación permanece en el enlace.
    - **Rutas duplicadas**: El tráfico de las aplicaciones se duplica en varias rutas, lo que aumenta la confiabilidad.

    * **Servicio de anulación**: El tráfico del flujo anula a un servicio diferente. Seleccione el tipo de servicio (Intranet, Internet, transferencia o descarte) que el servicio de ruta virtual anula.

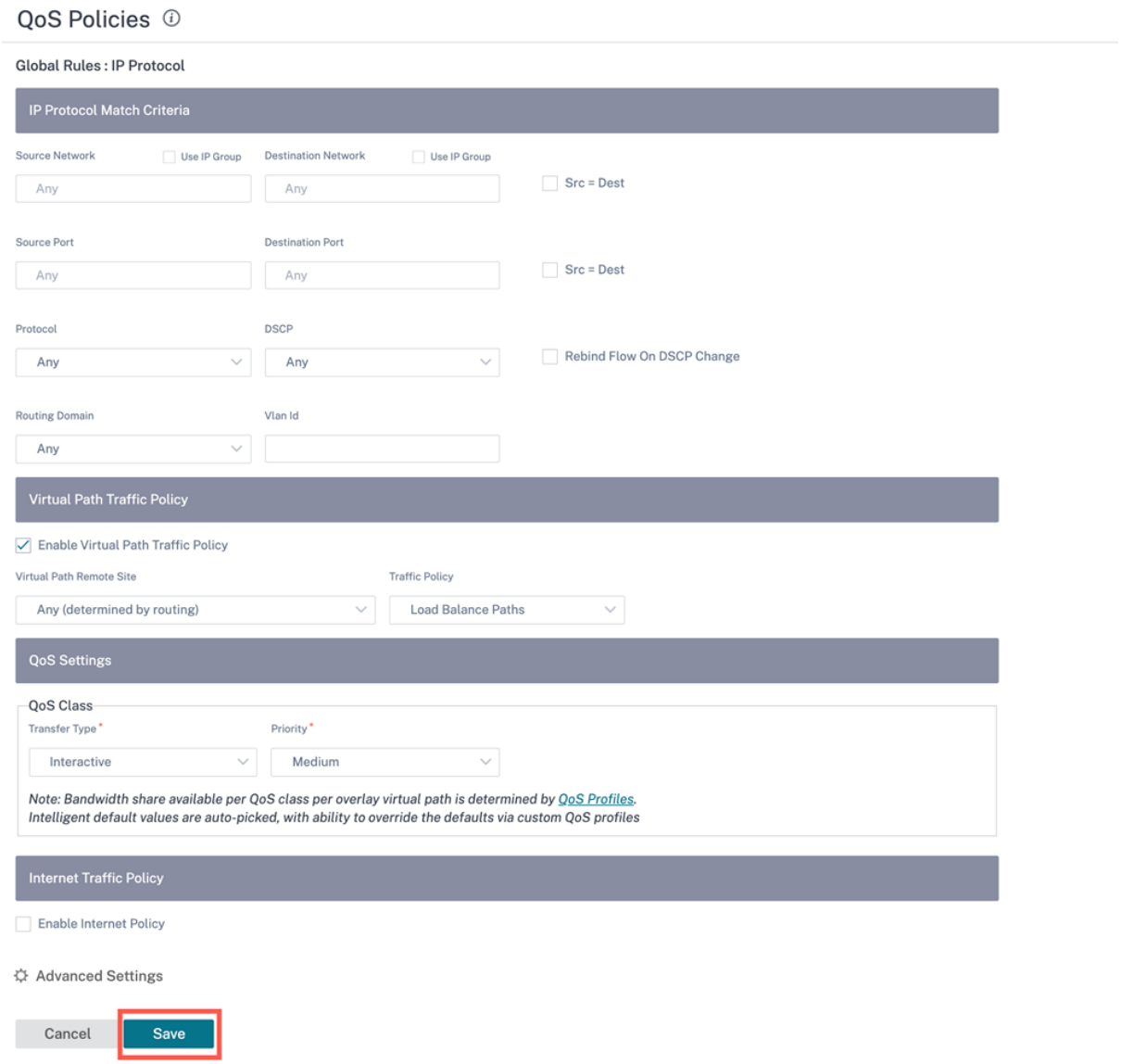



- Configuración de QoS (clase de QoS)
  - **Tipo de transferencia**: Elija uno de los siguientes tipos de transferencia:
    * **Tiempo real**: Se usa para tráfico de baja latencia, bajo ancho de banda y urgente. Las aplicaciones en tiempo real son urgentes, pero en realidad no necesitan un gran ancho de banda (por ejemplo, voz sobre IP). Las aplicaciones en tiempo real son sensibles a la latencia y la fluctuación, pero pueden tolerar algunas pérdidas
    * **Interactivo**: Se utiliza para el tráfico interactivo con requisitos de latencia baja a media y requisitos de ancho de banda bajo a medio. La interacción suele ser entre un cliente y un servidor. Es posible que la comunicación no necesite un ancho de banda alto, pero es sensible a la pérdida y la latencia.
    * **Bulk**: Se utiliza para tráfico de ancho de banda alto y aplicaciones que pueden tolerar una latencia alta. Las aplicaciones que gestionan la transferencia de archivos y necesitan un gran ancho de banda se clasifican como clases masivas. Estas aplicaciones implican poca interferencia humana y son manejadas principalmente por los propios sistemas.
  - **Prioridad**: Elija una prioridad para el tipo de transferencia seleccionado.

- Directiva de tráfico de Internet
  - Seleccione la casilla **Habilitar la directiva de Internet** para configurar la directiva de tráfico de Internet.
  - **Modo**: método de transmisión y recepción de paquetes para flujos que coinciden con la regla. Puede elegir el **servicio de anulación** o el **enlace WAN** según sea necesario.
  - **Enlace WAN**: El enlace WAN que utilizarán los flujos que coincidan con la regla cuando se habilite el equilibrio de carga de Internet.
  - **Servicio de anulación**: El servicio de destino de los flujos que coinciden con la regla.

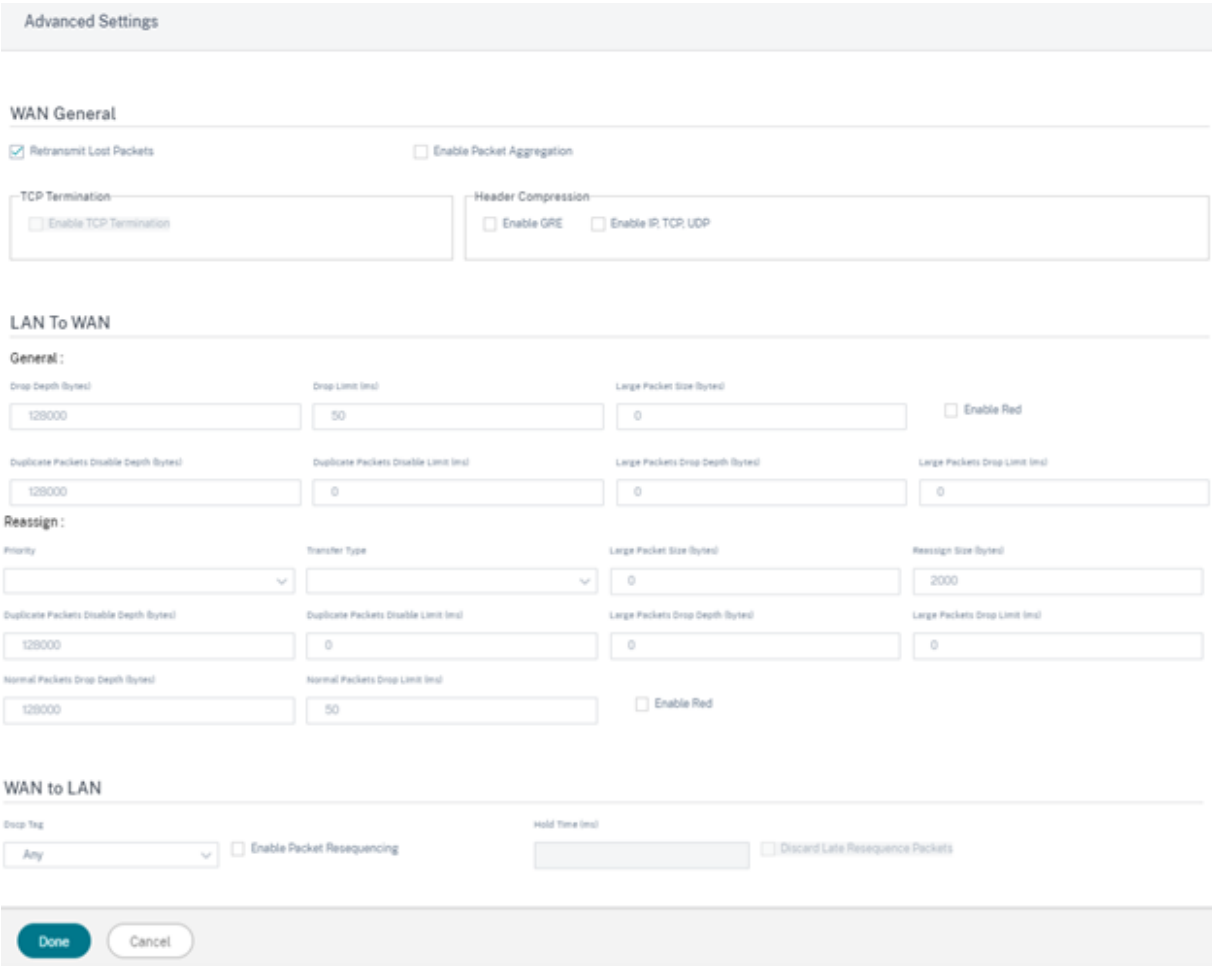
 

> **Nota**
>
> Un servicio de rutas virtuales no puede anular otro servicio de rutas virtuales.




Parámetros avanzados




- Información general sobre WAN
  - **Retransmitir paquetes perdidos**: Envía el tráfico que coincide con esta regla al dispositivo remoto a través de un servicio confiable y retransmite los paquetes perdidos.
  - **Habilitar la agregación de paquetes**: Agrega paquetes pequeños en paquetes más grandes.
  - **Habilitar la terminación**de TCP: Permite la terminación TCP del tráfico para este flujo. El tiempo de ida y vuelta para el reconocimiento de paquetes se reduce y, por lo tanto, mejora el rendimiento.
  - **Habilitar GRE**: Comprime los encabezados de los paquetes GRE.
  - **Habilitar IP, TCP y UDP**: Comprime los encabezados de los paquetes IP, TCP y UDP.

    > **Nota**
    >
    > Los paquetes IPv6 no admiten la compresión de encabezados.

- LAN a WAN

General

- **Profundidad de caída (bytes)**: Umbral de profundidad de cola tras el cual se descartan los paquetes.
- **Límite**de descarte: Tiempo después del cual se descartan los paquetes en espera en el programador de clases. No aplicable a una clase a granel.
- **Tamaño de paquete grande**: A los paquetes más pequeños o iguales a este tamaño se les asignan los valores de límite de descarte y profundidad de descarte especificados en los campos **Profundidad de caída de paquetes grandes (bytes)y Límite de caída de paquetes grandes (ms)**. A los paquetes que superen este tamaño se les asignan los valores especificados en los campos Límite de caída y Profundidad de caída predeterminados.
- **Habilitar RED**: La detección temprana aleatoria (RED) garantiza un reparto justo de los recursos de clase al descartar paquetes cuando se produce congestión.
- **Profundidad de desactivación de paquetes duplicados (bytes)**: La profundidad de la cola del programador de clases, momento en el que no se generan los paquetes duplicados.
- **Límite de desactivación de paquetes duplicados: Tiempo durante el cual se puede inhabilitar**la duplicación para evitar que los paquetes duplicados consuman ancho
- **Profundidad de caída de paquetes grandes (bytes)**: Si la profundidad de la cola supera este umbral, los paquetes se descartan y se cuentan las estadísticas.
- **Límite de descarte de paquetes grandes (ms)**: La cantidad máxima de tiempo estimada que deben esperar los paquetes mayores o iguales al tamaño de paquete grande en el programador de clases. Si el tiempo estimado supera este umbral, los paquetes se descartan y se cuentan las estadísticas. No es válido para clases masivas.

Reasignar

- **Prioridad**: Puede establecer la prioridad del enlace WAN en espera según sea necesario. La prioridad del enlace WAN en espera indica el orden en que se activa un enlace WAN en espera. Un enlace WAN en espera de alta prioridad se activa primero. Un enlace WAN de baja prioridad pasa a estar activo en último lugar.
- **Tipo de transferencia**: Seleccione el tipo de transferencia al que quiere asociar esta regla.
- **Profundidad de desactivación de paquetes duplicados (bytes)**: La profundidad de la cola del programador de clases, momento en el que no se generan los paquetes duplicados.
- **Límite de desactivación de paquetes duplicados**: Designa el tiempo que un paquete espera en la cola antes de que no se realice la duplicación, lo que evita que los paquetes duplicados consuman ancho de banda cuando el ancho de banda es limitado.
- **Profundidad de caída de paquetes grandes (bytes)**: S i la profundidad de la cola supera este umbral, los paquetes se descartan y se cuentan las estadísticas.
- **Límite de descarte de paquetes grandes (ms)**: Si el tiempo estimado supera este umbral,

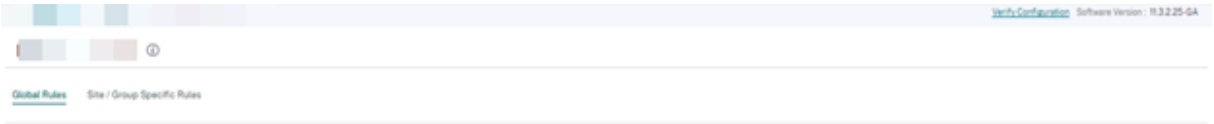
 

los paquetes se descartan y se cuentan las estadísticas. No es válido para clases masivas.
  - **Profundidad de caída de paquetes normal (bytes)**: Si la profundidad de la cola supera este umbral, los paquetes se descartan y se cuentan las estadísticas.
  - **Límite normal de descarte de paquetes (ms)**: Si el tiempo estimado supera este umbral, los paquetes se descartan y se cuentan las estadísticas. No es válido para clases masivas.

- WAN a LAN
  - Etiqueta**DSCP: Etiqueta**DSCP que se aplica a los paquetes que coinciden con esta regla en WAN a LAN, antes de enviarlos a la LAN.
  - **Habilitar la resecuenciación de paquetes**: Los flujos de tráfico que coinciden con la regla se etiquetan según el orden de secuencia y los paquetes se reordenan (si es necesario) en el dispositivo de WAN a LAN.
  - **Tiempo de espera**: intervalo de tiempo durante el cual se retienen los paquetes para volver a secuenciar, tras el cual los paquetes se envían a la LAN. Cuando el temporizador caduca, los paquetes se envían a la LAN sin esperar más a los números de secuencia necesarios.

    Si la regla tiene una directiva de tráfico como ruta duplicada, el tiempo de espera predeterminado es de 80 ms. De lo contrario, el valor predeterminado es 900 ms para las reglas TCP y 250 ms para las reglas que no son TCP.
  - **Descartar paquetes de resecuenciación tardía**: Descarta los paquetes desordenados que llegaron después de que los paquetes necesarios para la resecuenciación se hayan enviado a la LAN.

Haga clic en **Guardar** para guardar los ajustes de configuración. Haga clic en **Verificar configuración** en la página **Configuración** > **Directivas de QoS** para validar cualquier error de auditoría.



### Verifique las reglas de IP

Para verificar las reglas de IP, vaya a **Informes > Tiempo real > Flujos**. Seleccione el sitio del que quiere ver la información de flujo y el número de flujos que quiere mostrar. Haga clic en **Personalizar columnas** y seleccione las casillas de verificación correspondientes a la información de flujo que quiere ver. Compruebe si la información de flujo se ajusta a las reglas configuradas.

Vaya a **Informes > Tiempo real > Estadísticas** y seleccione **Reglas**. Elija el sitio y haga clic en **Recuperar los datos más recientes**. Compruebe las reglas configuradas. Para obtener más información, consulte Informes del sitio.

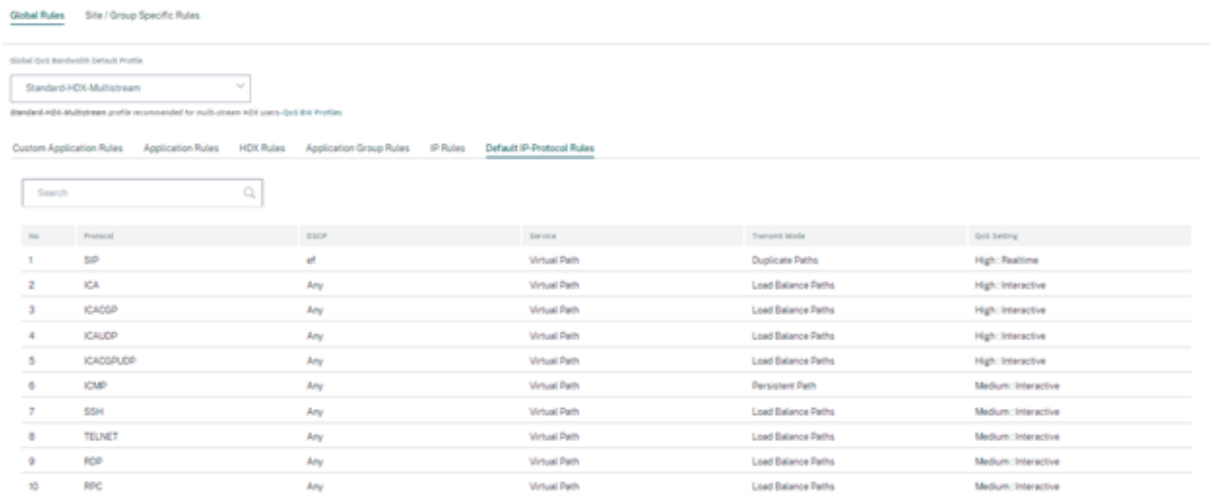
 

# Directivas de QoS

October 31, 2022

Un administrador puede definir las directivas de aplicaciones y tráfico. Estas directivas ayudan a habilitar las capacidades de direccionamiento del tráfico, calidad de servicio (QoS) y filtrado para las aplicaciones. Especifique si una regla definida se puede aplicar globalmente en todos los sitios de la red o en determinados sitios específicos.

Las directivas se definen en forma de varias reglas que se aplican en el orden definido por el usuario.




## Crear una nueva regla

El administrador debe colocar la regla definida en función de la prioridad. Las prioridades se clasifican según parámetros como la parte superior de la lista, la parte inferior de la lista o una fila específica.

Se recomienda tener reglas **más específicas** para las aplicaciones o subaplicaciones en la parte superior, seguidas de reglas **menos específicas** para las que representan un tráfico más amplio.

Por ejemplo, puede crear reglas específicas para Facebook Messenger (subaplicación) y Facebook (aplicación). Coloque una regla de Facebook Messenger encima de la regla de Facebook para que se seleccione la regla de Facebook Messenger. Si el orden se invierte, ya que Facebook Messenger es una subaplicación de la aplicación de Facebook, no se seleccionará la regla de Facebook Messenger. Es importante obtener el pedido correcto.

### Coincidir criterios

Seleccione el tráfico para una regla definida como:

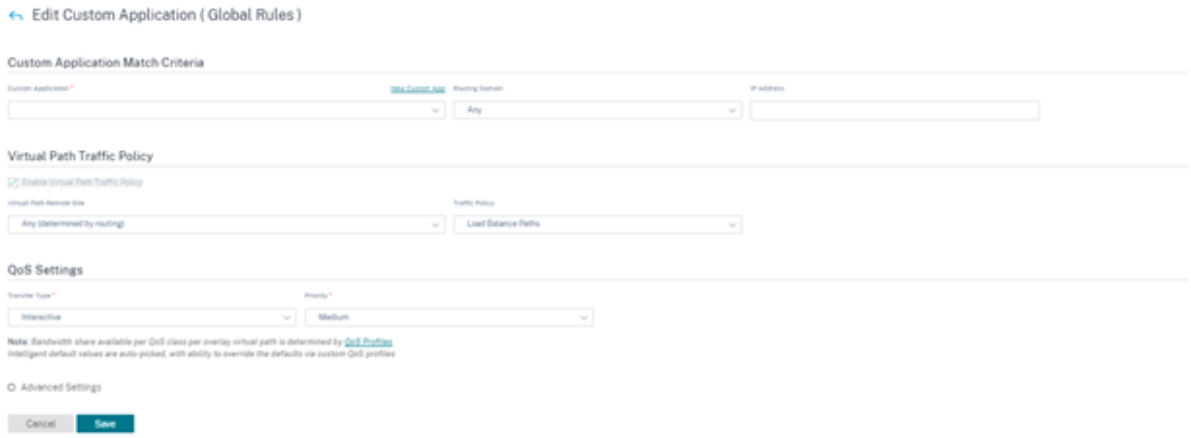
- Una aplicación
- Aplicación definida personalizada
- Grupo de aplicaciones o regla basada en protocolo IP

### Ámbito de regla

Especifique si una regla definida se puede aplicar globalmente en todos los sitios de la red o en determinados sitios específicos.

### Dirección de aplicación

Vaya a **Configuración** > **QoS** > **Reglas de aplicación personalizadas**. Especifique cómo se debe dirigir el tráfico.

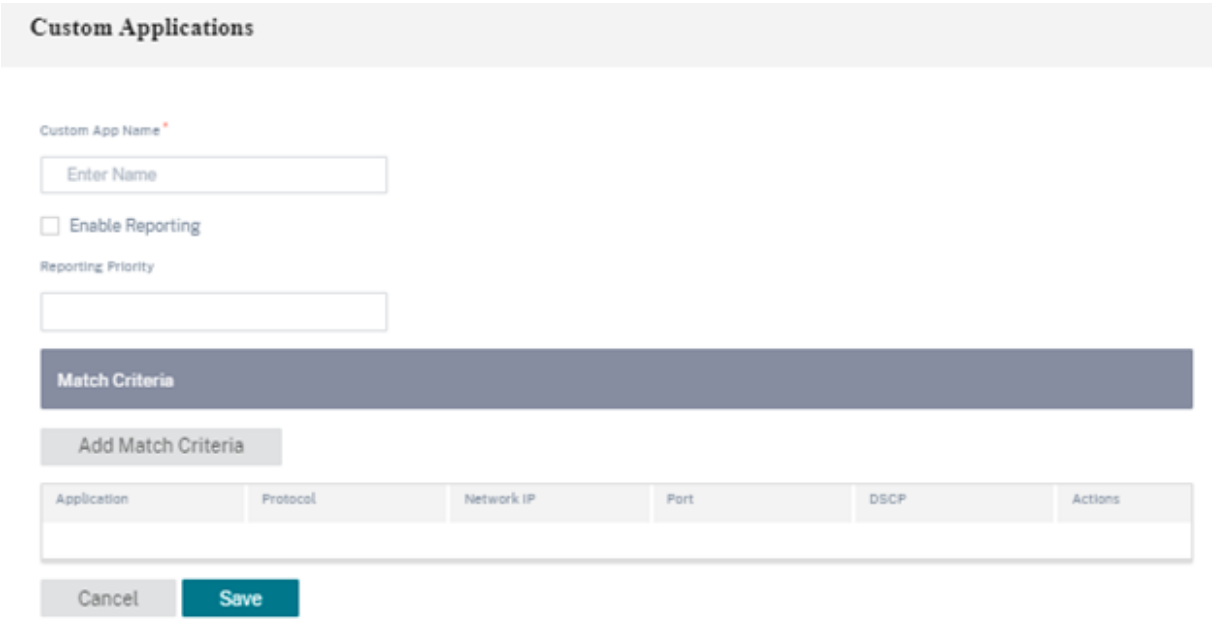



**Nueva aplicación personalizada**: Seleccione un criterio de coincidencia de la lista. El administrador puede agregar una nueva aplicación personalizada asignando un nombre a:

- Aplicación personalizada
- Protocolo (TCP, UDP, ICMP)
- IP/prefijo de red
- Puerto
- Etiqueta DSCP

También puede crear una aplicación personalizada basada en nombre de dominio.



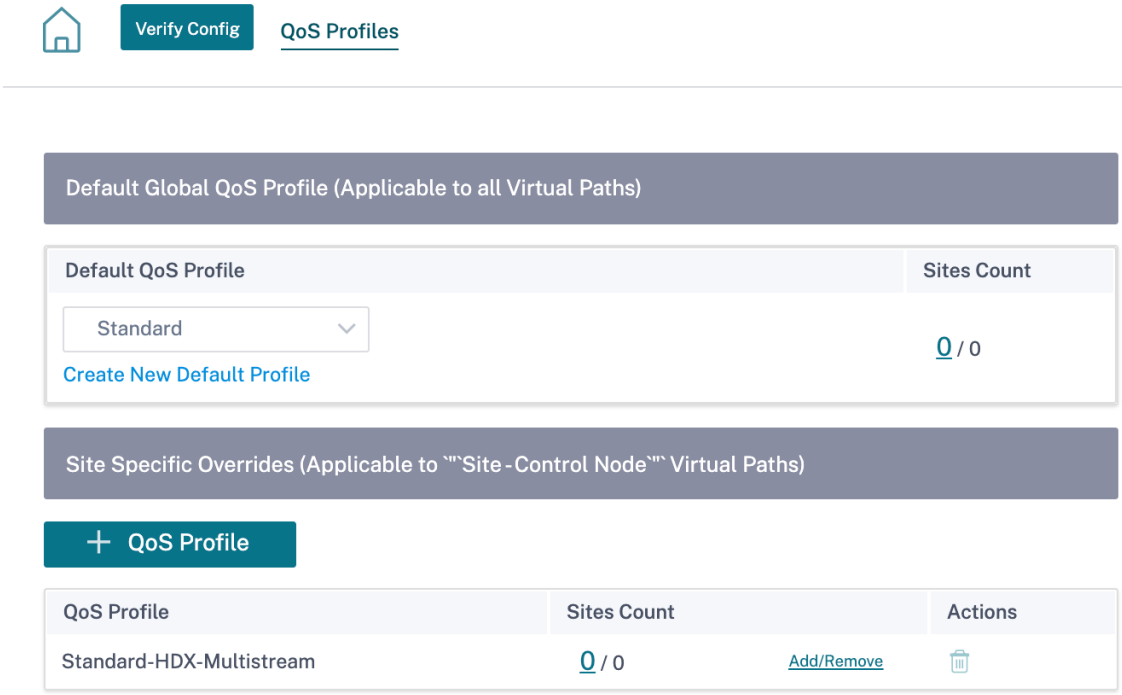

Haga clic en **Verificar configuración** en la página **Configuración** > **Directivas de QoS** para validar cualquier error de auditoría.

**Reglas de IP** **Las reglas de IP** le ayudan a crear reglas para su red y a tomar determinadas decisiones de calidad de servicio (QoS) basadas en las reglas. Para obtener más información sobre las reglas de IP, consulte Reglas de IP.

## Perfiles de QoS

La sección Calidad de servicio (QoS) ayuda a crear el perfil de QoS mediante la opción **+ Perfil de QoS**. El perfil QoS proporciona un servicio mejorado a cierto tráfico. El objetivo de QoS es proporcionar prioridad, incluyendo el tipo de tráfico (clases en tiempo real, interactivo y masivo) y ancho de banda dedicado. Las rupturas de ancho de banda están disponibles en valores de%. Esto también mejoró las funciones de pérdida.

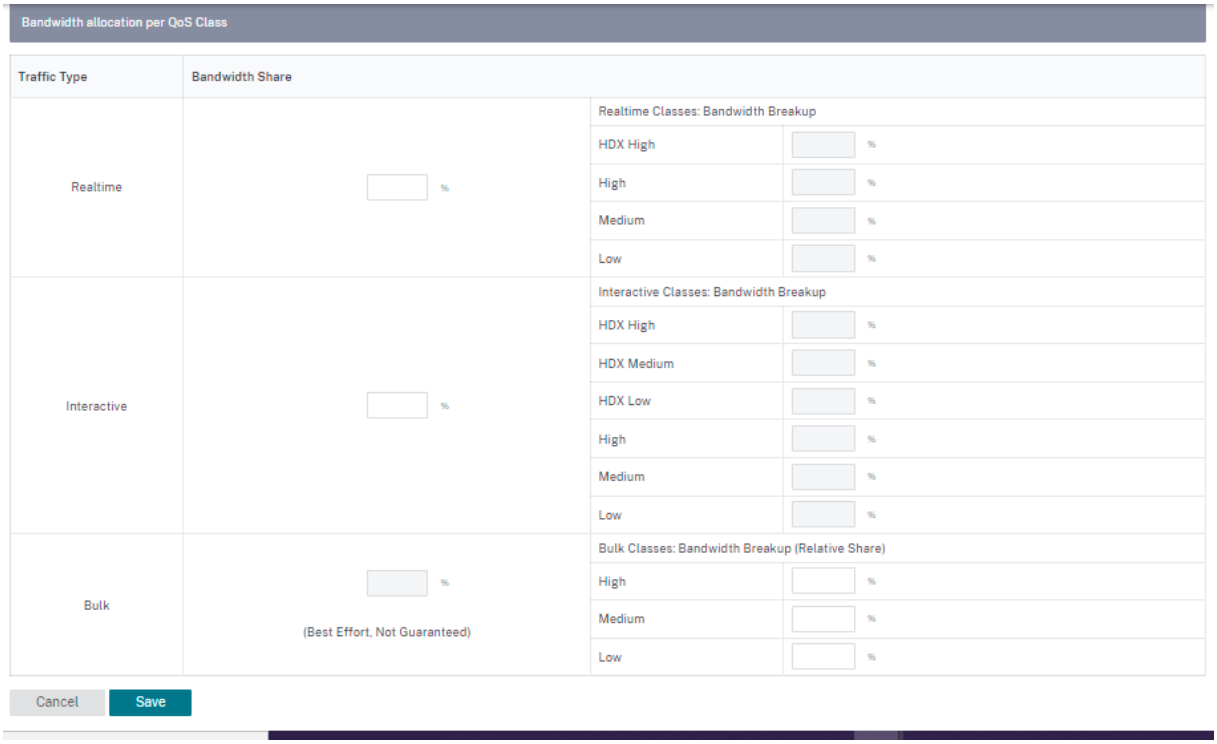



Haga clic en **Verificar configuración** en la página **Configuración** > **Directivas de QoS** para validar cualquier error de auditoría.

### Personalización de perfiles de QoS

Si se utilizan los conjuntos predeterminados de rutas virtuales, las clases se pueden modificar en **Configuración** > **QoS** > **Perfiles de QoS**. Haga clic en **Crear nuevo perfil predeterminado**, introduzca un nombre para el conjunto predeterminado, seleccione los sitios y actualice la asignación de ancho de banda para la clase de QoS. Haga clic en **Guardar**. Para obtener más información sobre las clases, consulte Clases.



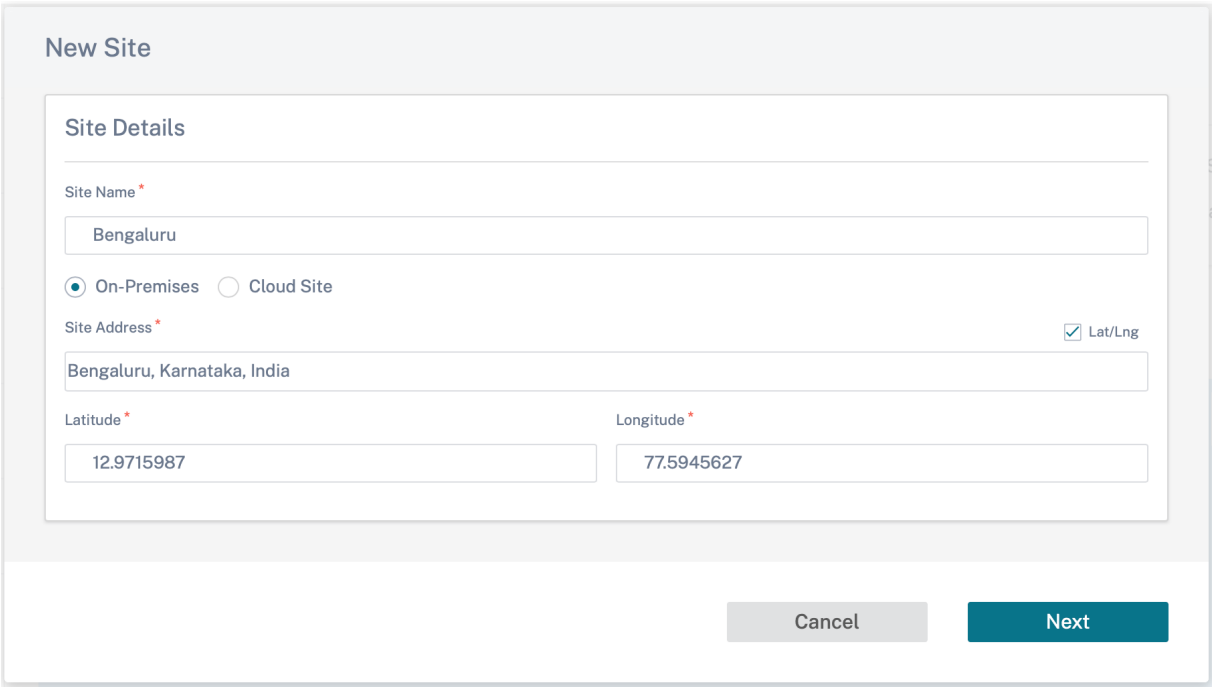

## Configuración del sitio

October 31, 2022

Puede agregar nuevos sitios desde la página **principal de la red** o desde la sección **Perfiles y plantillas** para configurar su red SD-WAN.

Para crear un sitio, haga clic en **+ Nuevo sitio** en el Panel de control de red. Proporcione un nombre y una ubicación para el sitio.

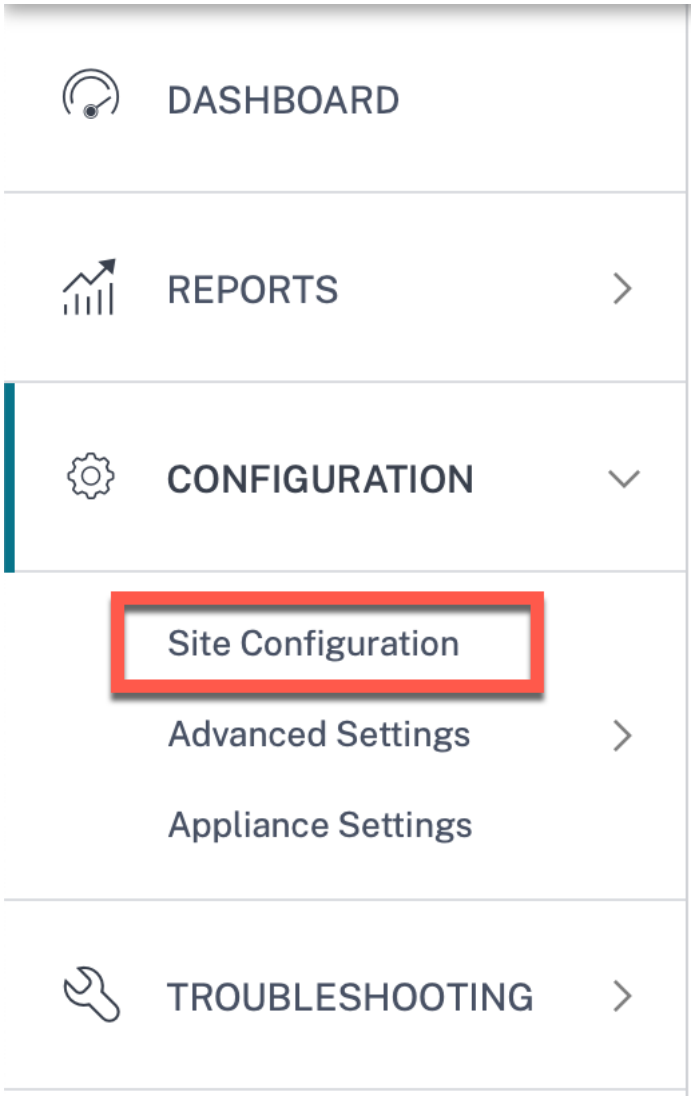



Puede crear un sitio desde cero o utilizar un perfil de sitio para configurar un sitio rápidamente.

Una pantalla gráfica a la derecha de la pantalla proporciona un diagrama de topología dinámica a medida que se continúa con la configuración.

Para ver la configuración del sitio, seleccione el sitio y vaya a **Configuración > Configuración del sitio**.

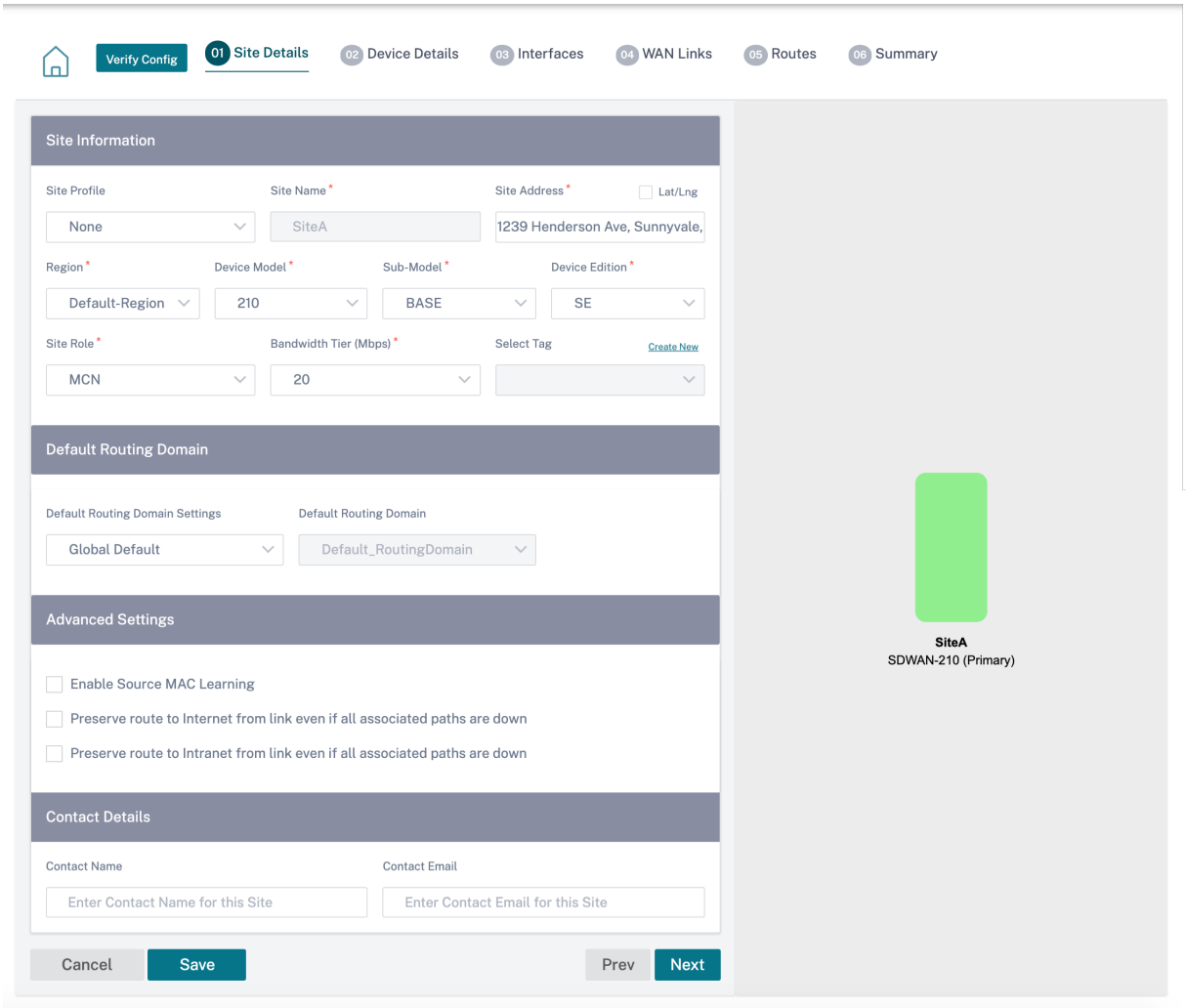
 




**Detalles del sitio**

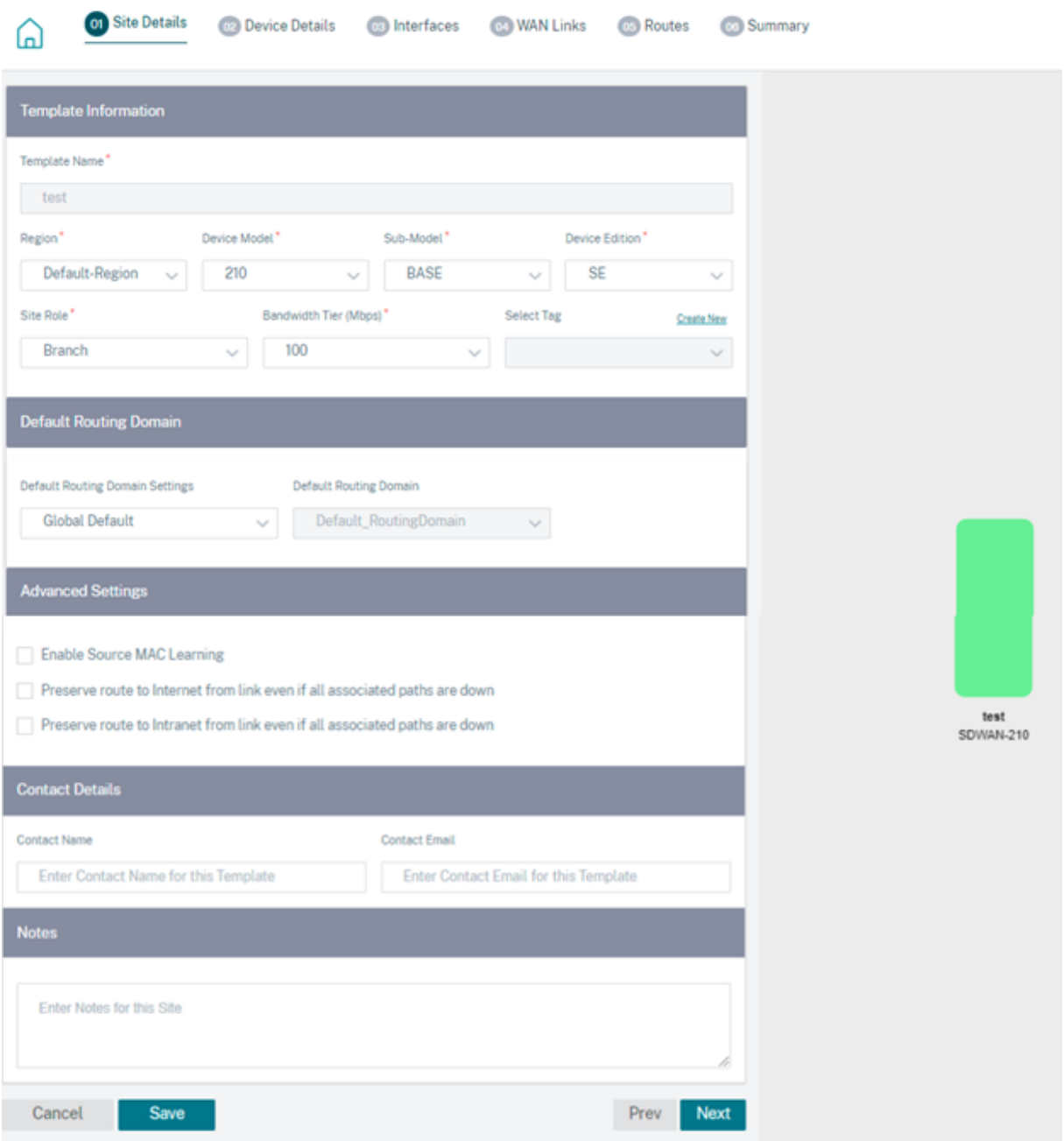
El primer paso consiste en introducir el sitio, el dispositivo, la configuración avanzada y los detalles de contacto del sitio.




Al configurar sitios mediante una plantilla de sitio, aparece la siguiente pantalla.




**Información sobre el sitio o la plantilla**

- Al elegir un **perfil de sitio**, se rellenan automáticamente los parámetros del sitio, la interfaz y los enlaces WAN según la configuración del perfil del sitio.
- **La dirección** y el **nombre del sitio** se rellenan automáticamente según los detalles proporcionados en el paso anterior.
- Active la casilla **Lat/Lng** para obtener la latitud y la longitud de un sitio.

- Seleccione la **región** en la lista desplegable.
- **El modelo y el**submodelo**del dispositivo** se pueden seleccionar según el modelo de hardware o el dispositivo virtual que se utilice en un sitio determinado.
- **Device Edition** se refleja automáticamente en función del modelo de dispositivo seleccionado. Actualmente, se admiten las ediciones Premium (PE), Advanced Edition (AE) y Standard Edition (SE). El modelo PE solo es compatible con las plataformas 1100, 2100, 5100 y 6100. El modelo AE es compatible con las plataformas 210 y 1100.

  > **Nota**
  >
  > El servicio Citrix SD-WAN Orchestrator no admite las plataformas Advanced Edition y Premium Edition.

- **El rol del sitio** define el rol del dispositivo. Puede asignar una de las siguientes funciones a un sitio:
  - **MCN**: El nodo de control maestro (MCN) actúa como controlador de la red y solo se puede designar un dispositivo activo de la red como MCN.
  - **Sucursal**: Dispositivos en las sucursales que reciben la configuración del MCN y participan en el establecimiento de las funcionalidades de WAN virtual en las sucursales. Puede haber varios sitios de sucursal.
  - **RCN**: El nodo de control regional (RCN) admite una arquitectura de red jerárquica, lo que permite la implementación de redes multirregionales. MCN controla múltiples RCNs y cada RCN, a su vez, controla múltiples sitios de sucursales.
  - **MCN con redundancia geográfica**: Un sitio en una ubicación diferente que asume las funciones de administración del MCN, si no está disponible, lo que garantiza la recuperación ante desastres. El MCN con redundancia geográfica no proporciona capacidades de alta disponibilidad ni de conmutación por error para el MCN.
  - **RCN georedundante**: Un sitio en una ubicación diferente, que asume las funciones de administración del RCN, si no está disponible, lo que garantiza la recuperación ante desastres. El RCN con redundancia geográfica no proporciona capacidades de alta disponibilidad ni de conmutación por error para el RCN.
- El**nivel de ancho** de banda es la capacidad de ancho de banda facturable que puede configurar en cualquier dispositivo, según el modelo de dispositivo. Por ejemplo, el dispositivo SD-WAN 410 Standard Edition (SE) admite niveles de ancho de banda de 20, 50, 100, 150 y 200 Mbps. Dependiendo de las necesidades de ancho de banda para un sitio determinado, puede seleccionar el nivel deseado. Cada sitio se factura por el nivel de ancho de banda configurado.

#### Dominio de redirección

La sección **Dominio de enrutamiento** le permite seleccionar el dominio de enrutamiento predeterminado para el sitio. La configuración del**dominio de enrutamiento** puede ser global o específica del sitio. Si selecciona **Valores predeterminados globales, se**selecciona automáticamente el dominio de enrutamiento predeterminado que se aplica a nivel mundial. Si selecciona **Site Specific**, puede seleccionar el dominio de enrutamiento predeterminado en la lista desplegable **Dominio de enrutamiento**.

#### Funcionalidad de redirección para la segmentación de redes LAN

Los dispositivos SD-WAN Standard y Enterprise Edition (SE/PE) implementan la segmentación de LAN en distintos sitios donde se implementa cualquiera de los dispositivos. Los dispositivos reconocen y mantienen un registro de las VLAN del lado de la LAN disponibles y configuran reglas sobre a qué otros segmentos de LAN (VLAN) se pueden conectar en una ubicación remota con otro dispositivo SE/PE de SD-WAN.

La capacidad anterior se implementa mediante una tabla de enrutamiento y reenvío virtuales (VRF) que se mantiene en el dispositivo SE/PE de SD-WAN, que realiza un seguimiento de los rangos de direcciones IP remotas accesibles a un segmento de LAN local. Este tráfico de VLAN a VLAN seguiría atravesando la WAN a través de la misma ruta virtual preestablecida entre los dos dispositivos (no es necesario crear nuevas rutas).

Un ejemplo de uso de esta funcionalidad es que un administrador de WAN podría segmentar el entorno de redes de sucursales locales a través de una VLAN y proporcionar acceso a algunos de esos segmentos (VLAN) a segmentos de LAN del lado de DC que tienen acceso a Internet, mientras que otros podrían no obtener dicho acceso. La configuración de las asociaciones de VLAN a VLAN se logra a través de la interfaz web del servicio Citrix SD-WAN Orchestrator.

#### Parámetros avanzados

- **Habilitar el aprendizaje de MAC**de origen: Almacena la dirección MAC de origen de los paquetes recibidos para que los paquetes salientes al mismo destino se puedan enviar al mismo puerto.
- **Conservar la ruta a Internet desde el enlace incluso si todas las rutas asociadas están inactivas**: Cuando se habilita, los paquetes destinados al servicio de Internet siguen eligiendo el servicio de Internet, incluso si todos los enlaces WAN para el servicio de Internet no están disponibles.
- **Conservar la ruta a la Intranet desde el enlace incluso si todas las rutas asociadas están inactivas**: Cuando se habilita, los paquetes destinados al servicio de intranet siguen eligiendo

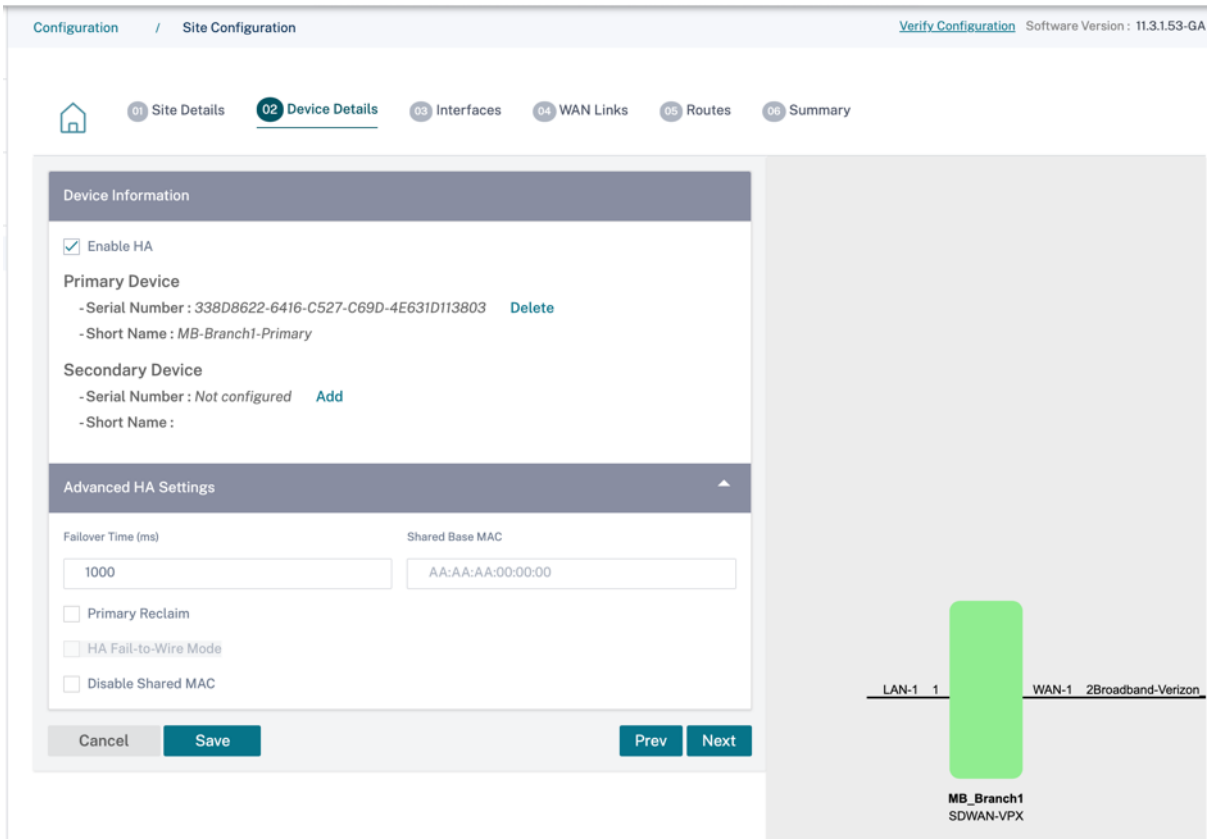
el servicio de intranet, incluso si todos los enlaces WAN para el servicio de intranet no están disponibles.

- Datos de contacto del administrador disponibles en el sitio.

Un diagrama de red dinámico a la derecha del panel de configuración proporciona retroalimentación visual de forma continua, a medida que pasa por el proceso de configuración.

### Detalles del dispositivo

La sección de detalles del dispositivo le permite configurar y habilitar Alta disponibilidad (HA) en un sitio. Con HA, se pueden implementar dos dispositivos en un sitio como primario activo y secundario pasivo. El dispositivo secundario se hace cargo cuando falla el primario. Para obtener más información, consulte Alta disponibilidad.



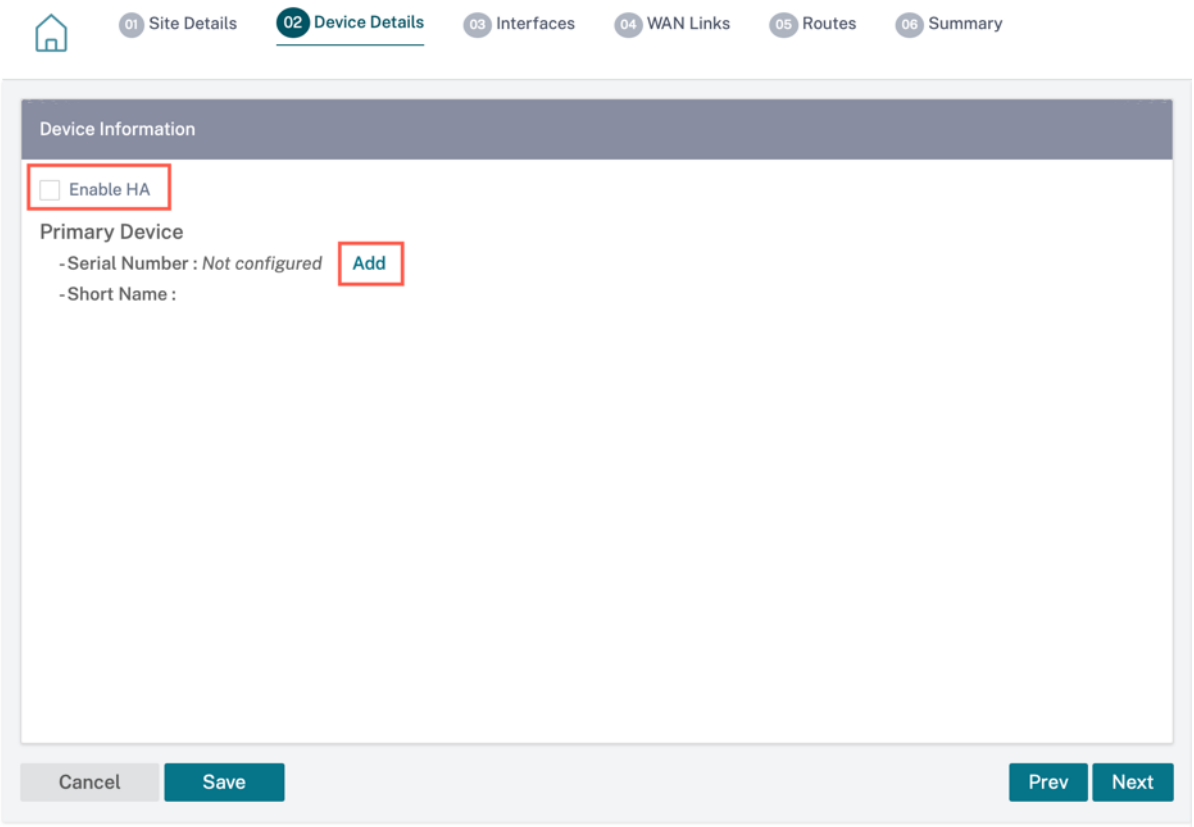

**Nota**

Los números de serie no se pueden configurar con las plantillas del sitio.

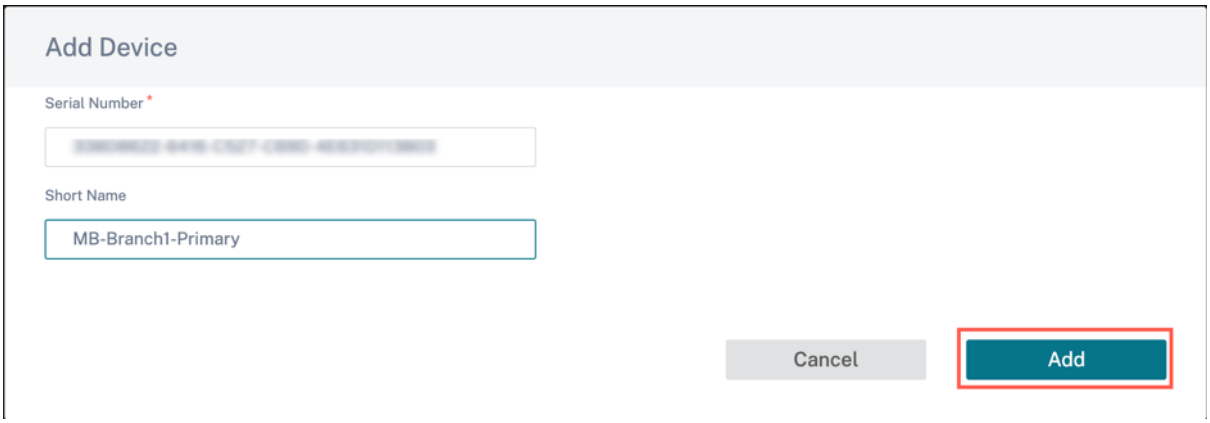
 

### Información de dispositivos

Habilite HA e introduzca el número de serie y un nombre abreviado para los dispositivos primarios y secundarios. Haga clic en **Agregar** y proporcione el número de serie junto con el nombre abreviado del sitio.

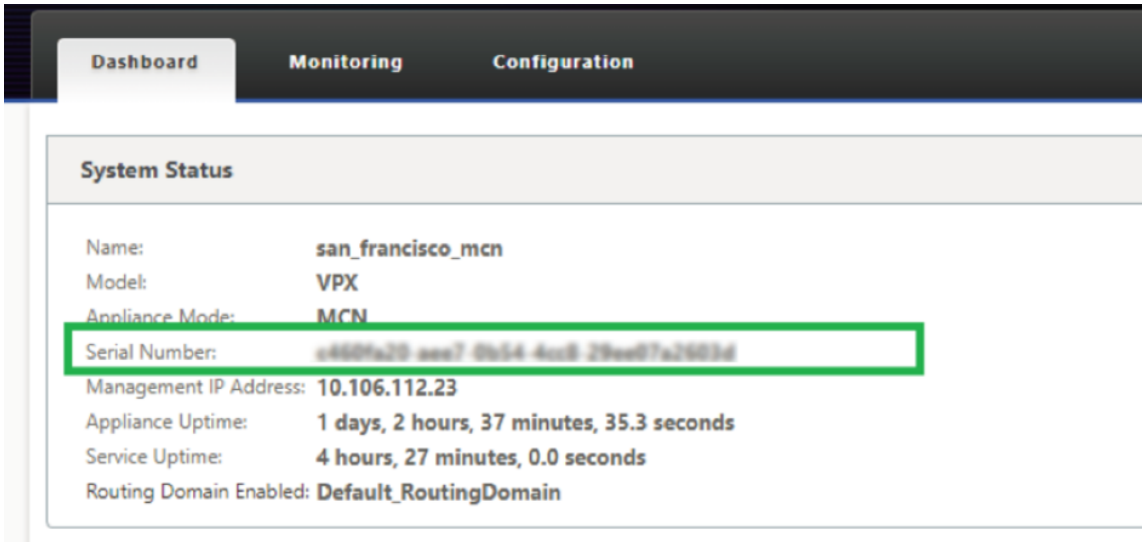



Haga clic en **Agregar**.




- **Número de serie**: Se puede acceder al **número de serie** de una instancia SD-WAN virtual (VPX) desde la consola web VPX, como se indica en la siguiente captura de pantalla. También se puede encontrar un número de serie de un dispositivo de hardware en la etiqueta del dispositivo.

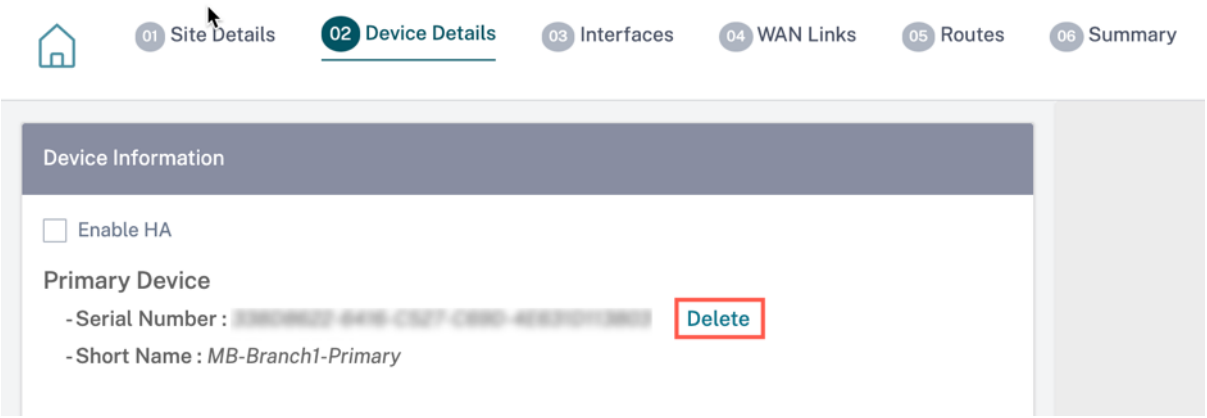
 




- **Nombre abreviado**: El campo **Nombre abreviado** se utiliza para especificar un nombre abreviado fácilmente identificable para un sitio o para etiquetarlo si se quiere.

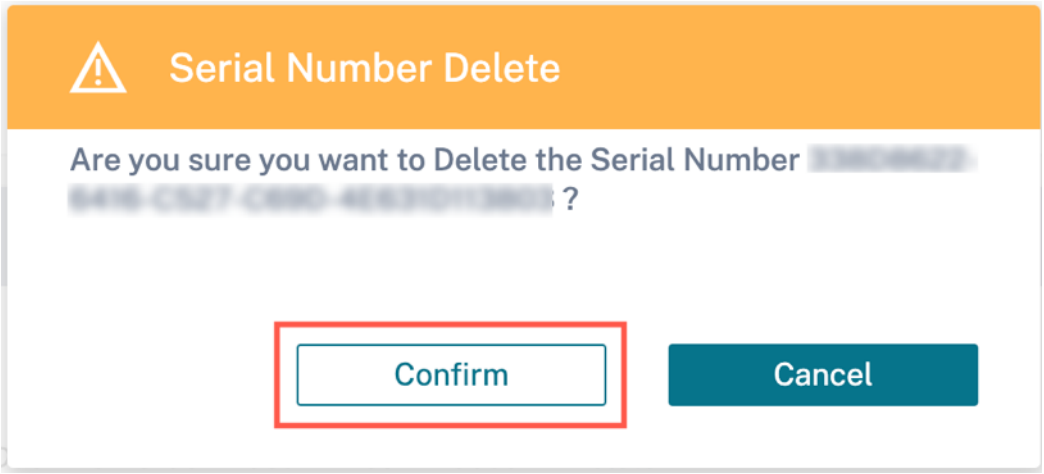
Haga clic en la opción **Eliminar** si quiere eliminar el número de serie.

> **Nota**
> Para actualizar el número de serie es necesario eliminar el número de serie existente y leer uno nuevo.




Al hacer clic en la opción **Eliminar**, aparece una ventana emergente para confirmar si quiere eliminar el número de serie o no.




### Configuración avanzada de HA

- **Tiempo de conmutación por error (ms)**: Se pierde el tiempo de espera tras el contacto con el dispositivo principal, antes de que el dispositivo en espera se active.
- **MAC base compartida**: La dirección MAC compartida para el par de dispositivos de alta disponibilidad. Cuando se produce una conmutación por error, el dispositivo secundario tiene las mismas direcciones MAC virtuales que el dispositivo principal con error.
- **Inhabilitar la MAC base compartida**: Esta opción solo está disponible en plataformas basadas en hipervisores y en la nube. Elija esta opción para inhabilitar la dirección MAC virtual compartida.
- **Reclamación principal**: El dispositivo principal designado recupera el control al reiniciarse después de un evento de conmutación por error.
- Modo**HA Fail-to-Wire: El modo**HA Fail-to-Wire está activado. Para obtener más información, consulte Modos de implementación de HA.
- **Habilite la compatibilidad con cables**en Y: Los puertos de factor de forma pequeño conectables (SFP) se pueden usar con un cable en Y de fibra óptica para habilitar la función de alta disponibilidad para la implementación del modo Edge. Esta opción solo está disponible en los dispositivos Citrix SD-WAN 1100 SE/PE. Para obtener más información, consulte Habilitar la alta disponibilidad en modo perimetral mediante cable en Y de fibra óptica.

### Detalles de Wi-Fi

Puede configurar un dispositivo Citrix SD-WAN que admita Wi-Fi como punto de acceso Wi-Fi.

Las dos variantes siguientes de la plataforma Citrix SD-WAN 110 admiten Wi-Fi y se pueden configurar como punto de acceso Wi-Fi:

- Citrix SD-WAN 110-WiFi-SE

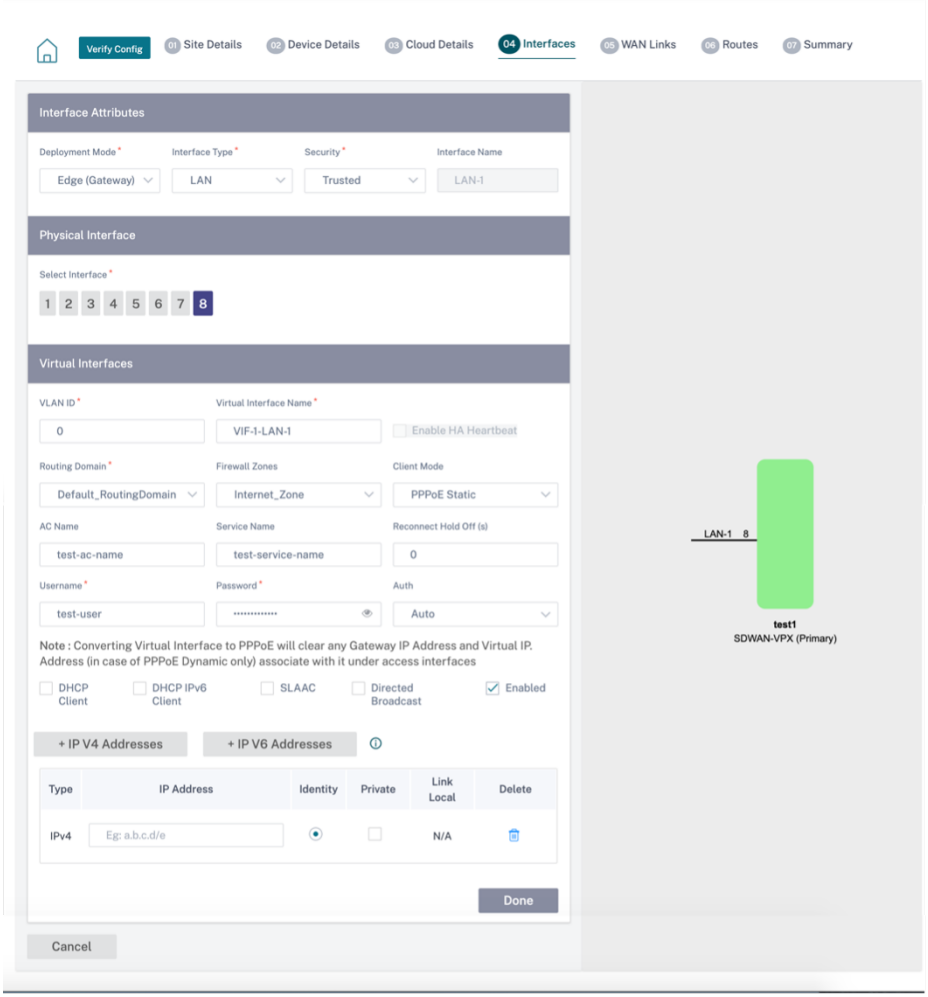
- Citrix SD-WAN 110-LTE-WiFi

Para obtener más información sobre la configuración de Wi-Fi, consulte Punto de acceso Wi-Fi

## Interfaces

El siguiente paso es agregar y configurar las interfaces. Haga clic en **+ Interfaz** para comenzar a configurar la interfaz. Haga clic en **+ HA Interface** para comenzar a configurar la interfaz HA. La opción de **interfaz + HA** solo está disponible si ha configurado un dispositivo secundario para una alta disponibilidad.

La configuración de la interfaz implica seleccionar el modo de implementación y establecer los atributos de nivel de interfaz. Esta configuración es aplicable a los enlaces LAN y WAN.



#### Administración en banda

La administración en banda le permite utilizar los puertos de datos SD-WAN para la administración. Transporta tanto tráfico de datos como de administración, sin tener que configurar una ruta de administración adicional. La administración en banda permite que las direcciones IP virtuales se conecten a servicios de administración como la interfaz de usuario web y SSH. Puede acceder a la interfaz de usuario web y SSH mediante la IP de administración y las IP virtuales en banda.

Para habilitar la administración dentro de banda, elija una dirección IPv4 de la lista desplegable **IP de administración en banda** o una dirección IPv6 de la lista desplegable **IPv6 de administración en banda**. Seleccione el **proxy DNS** al que se reenvían todas las solicitudes de DNS del plano de administración en banda y de respaldo desde la lista desplegable **DNS de administraciónen banda o DNS V6 de administración** en banda.

Para obtener más información sobre la administración dentro de banda, consulte Administración dentro de banda.

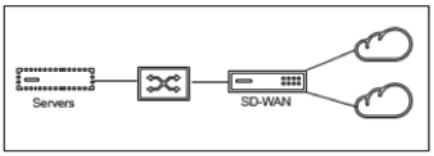
Las direcciones IP configuradas para las interfaces aparecen en la lista desplegable **IP de administración de InBand**. Los servicios de proxy DNS configurados en **Configuración avanzada > DNS** aparecen en la lista desplegable de **DNS de InBand Management**.

#### atributos de interfaz

Se admiten los siguientes modos de implementación:

1. Edge (puerta de enlace)
2. Inline: Fail-to-wire, Fail-to-block y Virtual inline.

- **Modo de implementación**: Seleccione uno de los siguientes modos de implementación.
  - **Edge (puerta de enlace)**:

    El modo Gateway implica que SD-WAN sirve como "puerta de enlace"a la WAN para todo el tráfico LAN. El **modo Gateway** es el modo predeterminado. Puede implementar el dispositivo como una Gateway en el lado LAN o en el lado WAN.
  - **En línea**:

    Cuando la SD-WAN se implementa en línea entre un conmutador LAN y un enrutador WAN, se espera que la SD-WAN "conecte"la LAN y la WAN.

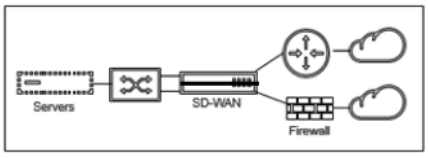
Todos los dispositivos Citrix SD-WAN tienen interfaces emparejadas de puentes predefinidas. Con la opción Bridge habilitada, la selección de cualquier interfaz en el extremo de la LAN resalta automáticamente la interfaz emparejada que está reservada para el extremo WAN del puente. Por ejemplo, las interfaces físicas 1 y 2 son un par puente.

* **Fail-to-Wire**: Permite una conexión física entre el par de interfaces puenteadas, lo que permite que el tráfico omita la SD-WAN y fluya directamente a través del puente en caso de que se reinicie o falle el dispositivo.

Anteriormente, el cliente DHCP solo era compatible con el puerto Fail-to-Block. Con la versión 11.2.0 de Citrix SD-WAN, la capacidad del cliente DHCP se amplía en el puerto de falla de conexión para el sitio de la sucursal con implementaciones de alta disponibilidad (HA) en serie. Esta mejora:

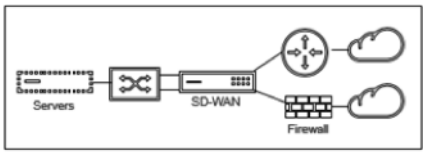
* Permite la configuración del cliente DHCP en el grupo de interfaces que no son de confianza que tiene implementaciones de pares de puentes de error a cable y de alta disponibilidad en serie.
* Permite seleccionar interfaces DHCP como parte de vínculos WAN de intranet privada.

> **Notas**
>
> * La opción Alineación (Fail-to-Wire) solo está disponible en dispositivos de hardware y no en dispositivos virtuales (VPX / VPXL).
> * Ahora se admite el cliente DHCP en el vínculo de intranet privada.
> * Una interfaz LAN no debe estar conectada al par de error a cable, ya que los paquetes pueden estar conectados entre las interfaces.



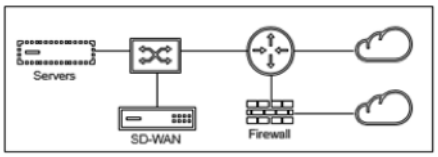

* **Error de bloqueo**: Esta opción inhabilita la conexión física entre el par de interfaces en puente en los dispositivos de hardware, lo que evita que el tráfico fluya a través del puente en caso de que se reinicie o falle el dispositivo.

> **Nota**
>
> Alineación (Fail-to-Block) es la única opción de modo puente disponible en los dispositivos virtuales (VPX / VPXL).



* **Virtual en línea (con un brazo)**:




Cuando la SD-WAN se implementa en este modo, tiene un **solo brazo** que la conecta al enrutador WAN, la LAN y la WAN que comparten la misma interfaz en la SD-WAN. Por lo tanto, la configuración de la interfaz se comparte entre los vínculos LAN y WAN.

- **Tipo de interfaz: S**eleccione el tipo de interfaz en la lista desplegable.
- **Seguridad (confiable o no confiable)**: Especifica el nivel de seguridad de la interfaz. Los segmentos de confianza están protegidos por un firewall.
- **Nombre de interfaz: S**egún el modo de implementación seleccionado, el campo **Nombre de interfaz** se rellena automáticamente.

**Interfaz física**

- **Seleccione la interfaz: S**eleccione el puerto Ethernet configurable que está disponible en el dispositivo.

**Interfaz virtual**

- **ID de VLAN**: El ID para identificar y marcar el tráfico hacia y desde la interfaz.
- **Nombre de la interfaz virtual: S**egún el modo de implementación seleccionado, el campo **Nombre de la interfaz virtual** se rellena automáticamente.
- **Activar HA Heartbeat**: habilite la sincronización de los latidos de HA a través de esta interfaz. Esta opción está habilitada si ha configurado un dispositivo secundario para HA. Seleccione esta opción para permitir que los dispositivos primarios y secundarios sincronicen los latidos de alta disponibilidad a través de esta interfaz. Especifique la dirección IP del dispositivo principal y secundario.
- **Dominio de enrutamiento**: El dominio de enrutamiento que proporciona un único punto de administración de la red de la sucursal o la red del centro de datos.
- **Zonas de firewall**: L a zona de firewall a la que pertenece la interfaz. Las zonas de firewall aseguran y controlan las interfaces en la zona lógica.
- **Modo cliente: S**eleccione **Modo cliente** en la lista desplegable. Al seleccionar PPPoE Static muestra más configuraciones.

> **Nota**
>
> Cuando el modo Sitio (en la ficha Detalles del sitio) se selecciona como **Sucursal** y el **campo Seguridad** (en la ficha **Interfaz** ) se selecciona como **No confiable**, la opción **PPPoE Dinámica** está disponible en **Modo cliente**.

Citrix SD-WAN actúa como un cliente PPPoE. Para IPv4, SD-WAN obtiene la dirección IPv4 dinámica o usa la dirección IPv4 estática. Para IPv6, obtiene la dirección local del enlace del servidor PPPoE. Para la dirección IPv6 unicast, se puede usar IP estática, DHCP o SLAAC.

- **Cliente DHCP**: Cuando se habilita en las interfaces virtuales, el servidor DHCP asigna direcciones IPv4 de forma dinámica al cliente conectado.
- **Cliente DHCP IPv6**: Cuando se habilita en las interfaces virtuales, el servidor DHCP asigna dinámicamente direcciones IPv6 al cliente conectado.
- **SLAAC**: Esta opción solo está disponible para direcciones IPv6. Cuando se selecciona, la interfaz obtiene las direcciones IPv6 mediante la configuración automática de direcciones sin estado (SLAAC).
- **Transmisión dirigida**: Cuando se selecciona la casilla de verificación **Transmisión** dirigida, las transmisiones dirigidas se envían a las subredes IP virtuales de la interfaz virtual.
- **Activado**: De forma predeterminada, la casilla **Activado** está seleccionada para todas las interfaces virtuales. Si quiere inhabilitar la interfaz virtual, desactive la casilla **Activado**.

  > **Nota**
  >
  > - La casilla **Activado** solo está disponible a partir de la versión 11.3.1 de Citrix SD-WAN.
  > - La opción para inhabilitar una interfaz virtual solo está disponible cuando no la utiliza una interfaz de acceso de enlace WAN. Si la interfaz virtual la utiliza una interfaz de acceso al enlace WAN, la casilla de verificación es de solo lectura y está seleccionada de forma predeterminada.
  > - Al configurar otras funciones, junto con las interfaces virtuales habilitadas, las interfaces virtuales inhabilitadas también aparecen en la lista, excepto en **Interfaces de acceso** para un **enlace WAN**. Incluso si selecciona una interfaz virtual inhabilitada, la interfaz virtual no se considera y no afecta a la configuración de red.

- **+ Dirección IPv4**: La dirección IPv4 virtual y la máscara de red de la interfaz.
- **+ Dirección IPv6**: La dirección IPv6 virtual y el prefijo de la interfaz.
- **Identidad**: Elija una identidad para utilizarla en los servicios de IP. Por ejemplo, la **identidad** se utiliza como la dirección IP de origen para comunicarse con los vecinos de BGP.
- **Privada**: Cuando está habilitada, la dirección IP virtual solo se puede enrutar en el dispositivo local.

**Nota**

- Los puertos LTE no admiten direcciones IP estáticas (IPv4 e IPv6).
- Los puertos LTE admiten DHCP y SLAAC. La configuración de DHCPv4 o DHCPv6 es obligatoria. SLAAC es opcional.
- En los puertos LTE, las direcciones Link-Local se pueden configurar para IPv6 o SLAAC.

### Credenciales de PPPoE

El Protocolo punto a punto sobre Ethernet (PPPoE) conecta varios usuarios de equipos en una LAN Ethernet a un sitio remoto a través de dispositivos locales comunes del cliente, por ejemplo, Citrix SD-WAN. PPPoE permite a los usuarios compartir una línea de suscriptor digital (DSL) común, un módem por cable o una conexión inalámbrica a Internet. PPPoE combina el Protocolo punto a punto (PPP), comúnmente utilizado en las conexiones de acceso telefónico, con el protocolo Ethernet, que admite varios usuarios en una LAN. La información del protocolo PPP se encapsula dentro de una trama Ethernet.

Los dispositivos Citrix SD-WAN utilizan PPPoE para permitir que los ISP tengan conexiones DSL y módem por cable continuas y continuas, a diferencia de las conexiones de acceso telefónico. PPPoE proporciona cada sesión de sitio remoto de usuario para conocer las direcciones de red de los demás mediante un intercambio inicial denominado "descubrimiento". Después de establecer una sesión entre un usuario individual y el sitio remoto, por ejemplo, un proveedor de ISP, la sesión se puede supervisar. Las empresas utilizan el acceso a Internet compartido a través de líneas DSL mediante Ethernet y PPPoE.

Citrix SD-WAN actúa como un cliente PPPoE. Para IPv4, SD-WAN obtiene la dirección IPv4 dinámica o usa la dirección IPv4 estática. Para IPv6, obtiene la dirección local del enlace del servidor PPPoE. Para la dirección IPv6 unicast, se puede usar IP estática, DHCP o SLAAC.

Se requiere lo siguiente para establecer sesiones PPPoE satisfactorias:

- Configure la interfaz de red virtual (VNI).
- Credenciales únicas para crear una sesión PPPoE.
- Configure el enlace WAN. Cada VNI solo puede tener configurado un enlace WAN.
- Configure la dirección IP virtual. Cada sesión obtiene una dirección IP única, dinámica o estática, según la configuración proporcionada.
- Implemente el dispositivo en modo puente para usar PPPoE con una dirección IP estática y configure la interfaz como "confiable"..
- Se prefiere que la IP estática tenga una configuración para forzar la IP propuesta por el servidor; si es diferente de la IP estática configurada, puede producirse un error.
- Implemente el dispositivo como un dispositivo Edge para usar PPPoE con IP dinámica y configure la interfaz como "no confiable"..

- Los protocolos de autenticación soportados son, PAP, CHAP, EAP-MD5, EAP-SRP.
- El número máximo de sesiones múltiples depende del número de VNI configuradas.
- Cree varios VNIs para admitir varias sesiones PPPoE por grupo de interfaz.

> **Nota**
>
> Se permite crear varias VNI con la misma etiqueta de VLAN 802.1Q.

Limitaciones para la configuración PPPoE:

- No se admite el etiquetado VLAN 802.1q.
- No se admite la autenticación EAP-TLS.
- Compresión de direcciones/controles.
- Compresión desinflada.
- Negociación de compresión de campo de protocolo.
- Protocolo de control de compresión.
- Compresión BSD Compress.
- Protocolos IPX.
- Enlace múltiple PPP.
- Compresión de cabecera TCP/IP estilo Van Jacobson.
- Opción de compresión de ID de conexión en compresión de encabezado TCP/IP estilo Van Jacobson.
- PPPoE no es compatible con las interfaces LTE.

Desde la versión 11.3.1 de Citrix SD-WAN, se considera un encabezado PPPoE de 8 bytes extra para ajustar el tamaño máximo de segmento (MSS) de TCP. El encabezado PPPoE adicional de 8 bytes ajusta el MSS en los paquetes de sincronización en función de la MTU. La MTU admitida oscila entre 1280 y 1492 bytes.

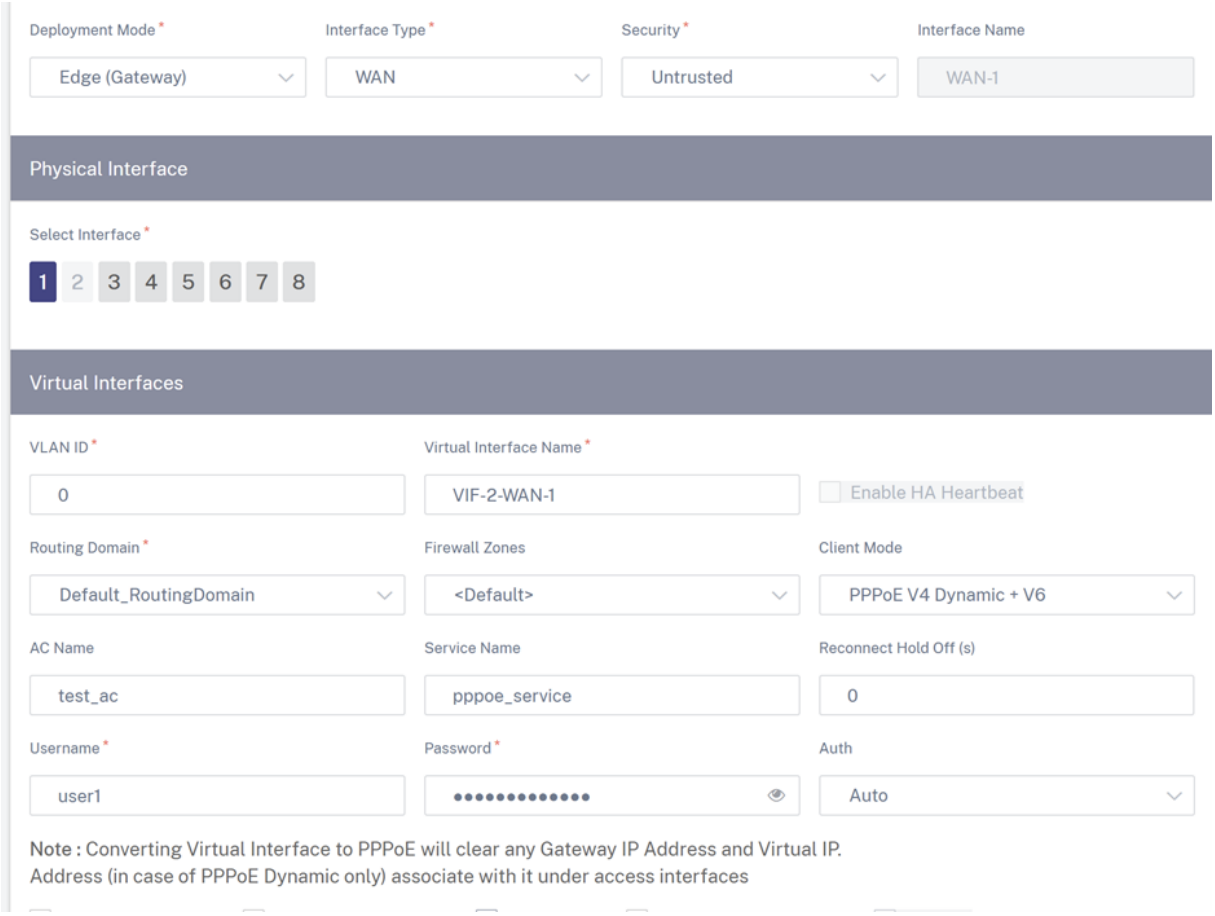
**Configuración de PPPoE** En un MCN, solo puede configurar PPPoE estático. En una sucursal, puede configurar PPPoE estático o PPPoE dinámico.

Para configurar PPPoE, en la configuración al nivel de sitio, vaya a la ficha **Configuración > Configuración del sitio > Interfaces**. En la sección **Interfaces virtuales**, seleccione la opción PPPoE adecuada de la lista desplegable del **modo cliente**.

> **Nota**
>
> - Un VNI configurado con múltiples interfaces puede tener una interfaz utilizada para la conectividad PPPoE.
> - Si una VNI configurada con varias interfaces y una conectividad PPPoE se cambia a una interfaz diferente, se puede usar la página **Informes > Tiempo real > PPPoE** para detener la sesión existente e iniciar una nueva sesión. A continuación, se puede establecer la nueva

sesión a través de la nueva interfaz.
- Si PPPoE Dynamic está seleccionado, se requiere que el VNI sea "Untrusted."




- **Nombre de CA: P**roporcione el nombre del concentrador de acceso (AC) para la configuración de PPPoE.
- **Nombre del servicio:** introduzca un nombre de servicio.
- **Retención (s) de reconexión:** introduzca el tiempo de espera del intento de reconexión.
- **Nombre de usuario:** Introduzca el nombre de usuario para la configuración de PPPoE.
- **Contraseña:** introduzca la contraseña de la configuración de PPPoE.
- **Autenticación: S**eleccione el protocolo de autorización en la lista desplegable.
  - Cuando la opción **Auth** se establece en Automática, el dispositivo SD-WAN cumple con la solicitud de protocolo de autenticación compatible recibida del servidor.
  - Cuando la opción **Auth** se establece en PAP/CHAP/EAP, solo se respetan los protocolos de autenticación específicos. Si PAP está en la configuración y el servidor envía una solicitud de autenticación con CHAP, se rechaza la solicitud de conexión. Si el servidor no negocia con PAP, se produce un error de autenticación.

Solo se permite la creación de un enlace WAN por VNI estático o dinámico PPPoE. La configuración

del enlace WAN varía en función de la selección de VNI del modo cliente.

Si el VNI está configurado con el modo de cliente dinámico PPPoE:

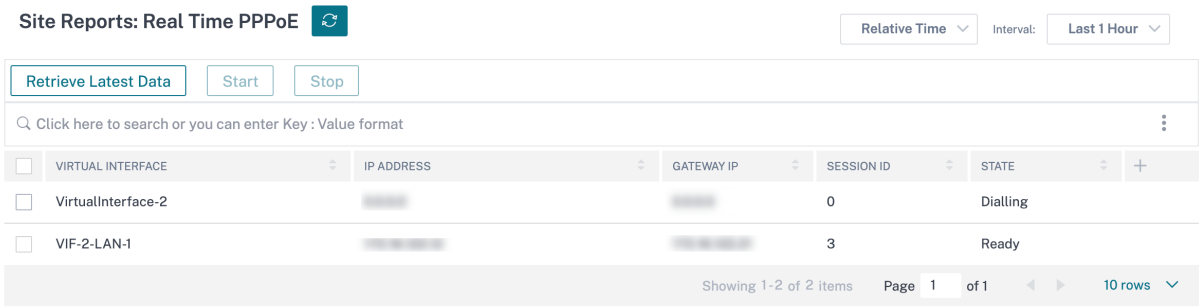
- Los campos Dirección IP y Dirección IP de puerta de enlace se vuelven inactivos.
- El modo de ruta virtual está configurado en "Primario"..
- No se puede configurar el ARP de proxy.

De forma predeterminada, se selecciona Enlace de dirección MAC de puerta de enlace.

Si la VNI está configurada con el modo de cliente estático PPPoE, configure la dirección IP.

> **Nota**
>
> Si el servidor no respeta la dirección IP estática configurada y ofrece una dirección IP diferente, se produce un error. La sesión PPPoE intenta restablecer la conexión periódicamente, hasta que el servidor acepte la dirección IP configurada.

**Supervisión y solución de problemas de PPPo** A nivel de sitio, navegue por la sección **Informes > Tiempo real > PPPoE** para ver información sobre las VNI configuradas con el modo de cliente dinámico o estático de PPPoE. Le permite iniciar o detener manualmente las sesiones para solucionar problemas.




Si hay un problema al establecer una sesión PPPoE:

- Al pasar el ratón sobre el estado fallido, se muestra el motivo del error reciente.
- Para establecer una sesión nueva o para solucionar problemas de una sesión PPPoE activa, reinicie la sesión.
- Si una sesión PPPoE se detiene manualmente, no se puede iniciar hasta que se inicie manualmente y se active un cambio de configuración, o se reinicie el servicio.

Una sesión PPPoE puede fallar por los siguientes motivos:

- Cuando la SD-WAN no se autentica ante el par debido a un nombre de usuario o contraseña incorrectos en la configuración.

- La negociación PPP falla: La negociación no llega al punto en el que se ejecuta al menos un protocolo de red.
- Problema de memoria del sistema o recursos del sistema.
- Configuración incorrecta o inválida (nombre de CA o nombre de servicio incorrecto).
- Error al abrir el puerto serie debido a un error del sistema operativo.
- No se recibió ninguna respuesta para los paquetes de eco (el enlace es incorrecto o el servidor no responde).
- Hubo varias sesiones continuas de marcación fallidas en un minuto.

Después de 10 fallas consecutivas, se observa el motivo de la falla.

- Si el fallo es normal, se reinicia inmediatamente.
- Si el error es un error, el reinicio se revierte durante 10 segundos.
- Si el error es grave, el reinicio se revierte durante 30 segundos antes de reiniciar.

Los paquetes de solicitud de eco LCP se generan desde SD-WAN cada 60 segundos y si no se reciben 5 respuestas de eco se considera un error de enlace y se restablece la sesión.

- Si el VNI está activo y listo, las columnas IP y IP de puerta de enlace muestran los valores actuales de la sesión. Indica que se trata de valores recibidos recientemente.
- Si el VNI está detenido o se encuentra en estado fallido, los valores son los últimos valores recibidos.
- Al pasar el ratón sobre la columna IP de la puerta de enlace, se muestra la dirección MAC del concentrador de acceso PPPoE desde donde se reciben la sesión y la IP.
- Al pasar el ratón sobre el valor del "estado", se muestra un mensaje, que es más útil para un estado de "Fallo".

| Tipo de sesión PPPoE | Color de estado | Descripción |
|---|---|---|
| Configurado | Amarillo | Un VNI está configurado con PPPoE. Este es un estado inicial. |
| Marcación | Amarillo | Después de configurar un VNI, el estado de la sesión PPPoE pasa al estado de marcado iniciando el descubrimiento de PPPoE. Se captura la información del paquete. |

| Tipo de sesión PPPoE | Color de estado | Descripción |
|---|---|---|
| La función de persistencia | Amarillo | El VNI pasa del estado de detección al estado de sesión, en espera de recibir la IP, si es dinámico o en espera del acuse de recibo del servidor para la IP anunciada, si es estática. |
| Listo | Verde | Se reciben los paquetes IP y el VNI y el enlace WAN asociado están listos para su uso. |
| Error | Rojo | La sesión PPP/PPPoE ha finalizado. El motivo del error puede deberse a una configuración no válida o a un error fatal. La sesión intenta volver a conectarse después de 30 segundos. |
| Detenido | Amarillo | La sesión PPP/PPPoE se detiene manualmente. |
| Terminación | Amarillo | Un estado intermedio que termina por un motivo. Este estado se inicia automáticamente después de cierto tiempo (5 segundos para un error normal o 30 segundos para un error grave). |
| Inhabilitado | Amarillo | El servicio SD-WAN está inhabilitado. |

El archivo *SDWAN_ip_learned.log* contiene registros relacionados con PPPoE. Vaya a **Solución de problemas > Registros de dispositivos** para ver o descargar el archivo *SDWAN_ip_learned.log*.

#### Configuración 802.1X cableada

El 802.1X cableado es un mecanismo de autenticación que requiere que los clientes se autentiquen antes de poder acceder a los recursos de la LAN. El servicio Citrix SD-WAN Orchestrator admite la configuración de la autenticación 802.1X cableada en interfaces LAN.

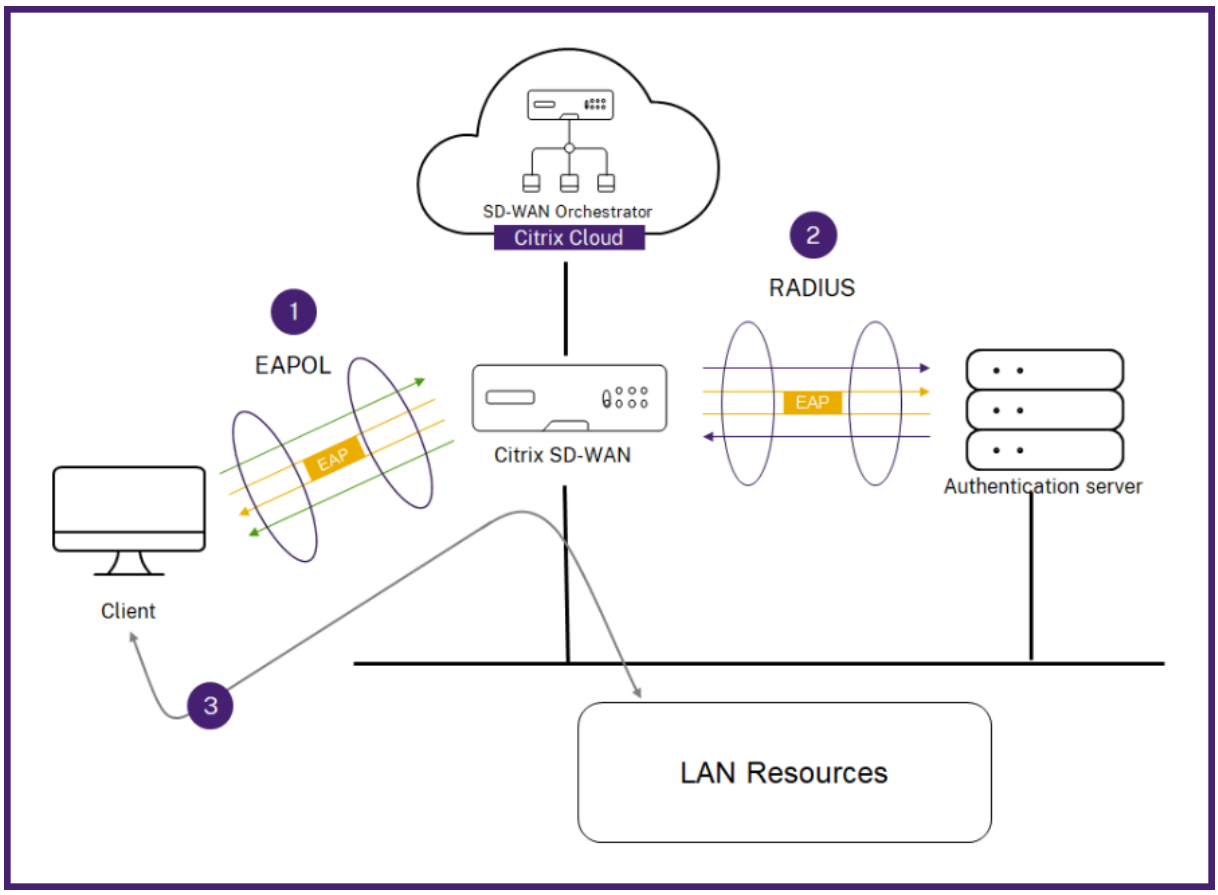
En la red Citrix SD-WAN, los clientes envían solicitudes de autenticación al dispositivo Citrix SD-WAN para tener acceso a los recursos de LAN. El dispositivo Citrix SD-WAN actúa como autenticador y envía las solicitudes de autenticación al servidor de autenticación. El servicio Citrix SD-WAN Orchestrator solo admite servidores RADIUS que se configuran como servidores de autenticación.

Al autenticarse por primera vez, solo se pueden procesar los paquetes EAPOL o los paquetes DHCP que pueden inicializar la autenticación 802.1X desde la LAN virtual predeterminada. Un cliente recién conectado debe autenticarse en un plazo de 90 segundos. Si la autenticación se realiza correctamente, obtiene acceso a los recursos de la LAN.

Si la autenticación falla, no se concede al cliente acceso a la red y se descartan todos los paquetes. Los clientes que están conectados directamente al dispositivo Citrix SD-WAN pueden volver a intentar la autenticación desconectando el cable Ethernet y volviéndolo a insertar. De manera opcional, puede definir una LAN virtual específica para conceder acceso a recursos de LAN limitados para las solicitudes de autenticación fallidas. En esos casos, las solicitudes de autenticación fallidas obtienen acceso a la LAN virtual especificada. Puede restringir el acceso al tráfico autenticado mediante diferentes dominios de enrutamiento o zonas de firewall al crear la LAN virtual.

> **Nota**
>
> - La LAN virtual predeterminada siempre debe tener 802.1X habilitado.
> - No se admiten las LAN virtuales dinámicas.




El dispositivo Citrix SD-WAN espera recibir paquetes sin una etiqueta 802.1Q (paquetes sin etiquetar). Si el dispositivo Citrix SD-WAN recibe un paquete con una etiqueta 802.1Q establecida en la LAN virtual asignada, todos los paquetes originados en el MAC deben etiquetarse. Si se recibe un paquete sin la etiqueta 802.1Q en el encabezado o con una etiqueta que no sea la LAN virtual a la que pertenece la dirección MAC, el paquete se descarta.

Cuando varios clientes conectados a un switch intentan autenticarse al mismo tiempo en un solo puerto, cada cliente se autentica de forma individual, antes de que pueda acceder a los recursos de la LAN. Los clientes que no se autentiquen pueden volver a intentar la autenticación desconectando el cable Ethernet, esperando 3 minutos y volviendo a insertar el cable Ethernet. Las plataformas Citrix SD-WAN 110, 210 y 410 admiten un máximo de 32 clientes (tanto autenticados como no autenticados). Todas las demás plataformas admiten un máximo de 64 clientes (tanto autenticados como no autenticados).

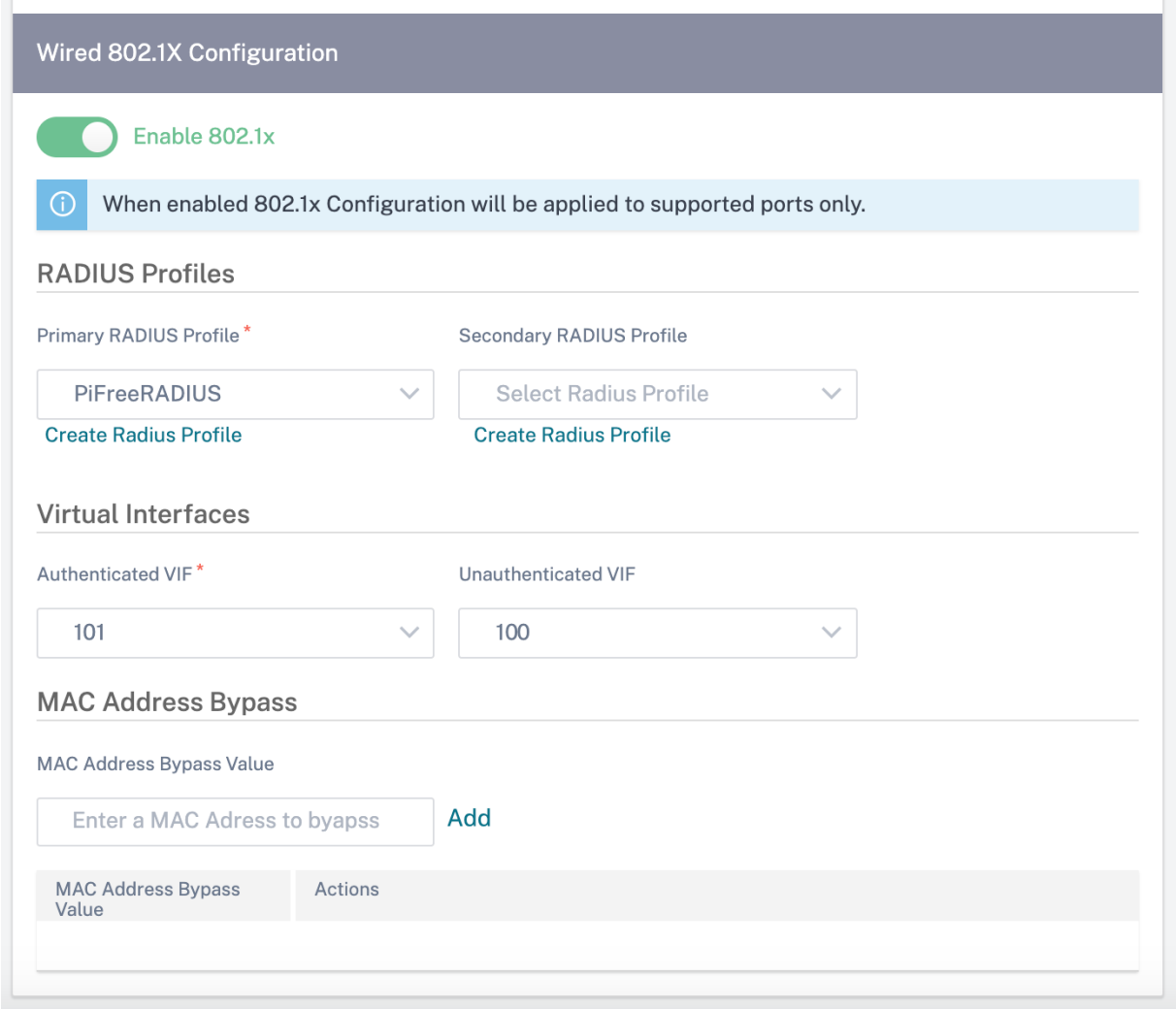
Para configurar la autenticación 802.1X, vaya a **Configuración del sitio > Interfaces** y active el botón **Activar 802.1x**. Seleccione un perfil RADIUS existente o haga clic en **Crear perfil RADIUS** para crear un perfil RADIUS. Para obtener información sobre la creación de un perfil RADIUS, consulte Perfiles de servidor RADIUS. Puede usar los mismos perfiles RADIUS para la autenticación empresarial inalámbrica 802.1x y WPA2-Enterprise inalámbrica, siempre que el dispositivo sea compatible con WPA2-Enterprise inalámbrica.

Seleccione una interfaz virtual de la lista desplegable **VIF autenticado**. La interfaz virtual seleccionada otorga acceso a los recursos de la LAN para que las solicitudes de autenticación se realicen correctamente.

Si lo quiere, puede seleccionar una interfaz de la lista desplegable **VIF sin autenticar**. La interfaz virtual seleccionada otorga acceso a un recurso LAN específico para las solicitudes autenticadas fallidas.

Puede agregar una lista de direcciones MAC que omita el proceso de autenticación. El tráfico de estas direcciones MAC se tratará implícitamente como autenticado. Estas direcciones MAC son susceptibles de sufrir ataques malintencionados. Por lo tanto, utilice esta capacidad solo en entornos físicamente seguros y para hardware heredado que no admita la autenticación 802.1x cableada.




Puede ver las alertas asociadas a las solicitudes de autenticación 802.1x cableadas en **Informes > Alertas**. Para obtener más información, consulte Alertas.

### Enlaces WAN

El siguiente paso es configurar enlaces WAN. Haga clic en **+ Enlace WAN** para empezar a configurar un enlace WAN.

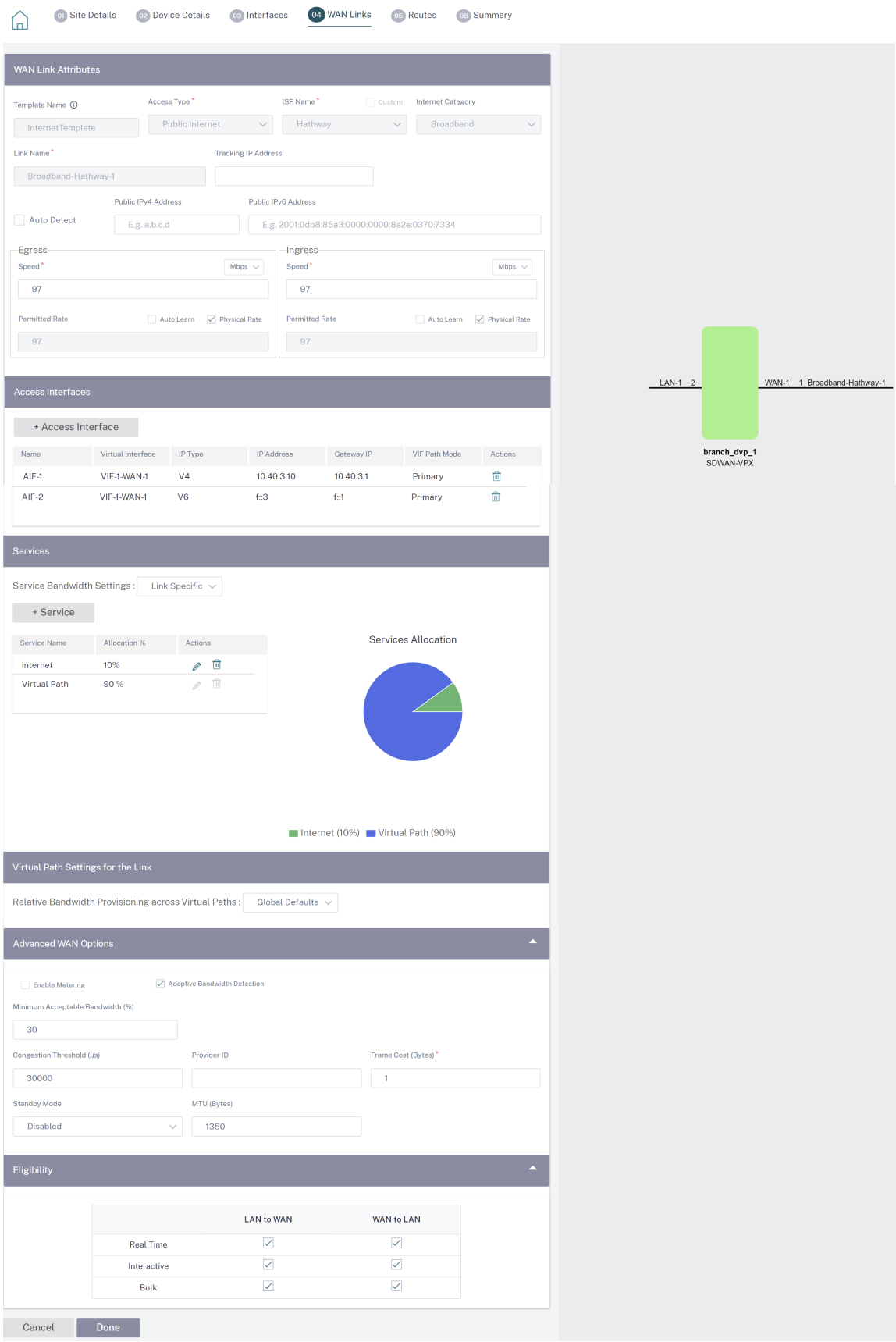
La configuración del enlace WAN implica configurar el tipo de acceso al enlace WAN y los atributos de interfaz de acceso.

Puede configurar el atributo de **enlace WAN** desde cero o utilizar una plantilla de enlace WAN para configurar rápidamente los atributos de enlace WAN. Si ya ha utilizado un perfil de sitio, los atributos del **enlace WAN** se rellenan automáticamente.

## Atributos de enlace WAN



- **Nombre de la plantilla**: El nombre de la plantilla de enlace WAN utilizada para crear el enlace WAN. El nombre de la plantilla de enlaces WAN no se puede modificar después de la creación de los enlaces WAN. Una vez creados los enlaces WAN mediante una plantilla de enlaces WAN, no podrá modificar el tipo de acceso, el nombre del ISP o la categoría de Internet.
- **Tipo de acceso**: Especifica el tipo de conexión WAN del enlace.
  - **Internet pública**: indica que el enlace está conectado a Internet a través de un ISP.
  - **Intranet privada**: indica que el enlace está conectado a uno o más sitios dentro de la red SD-WAN y no puede conectarse a ubicaciones fuera de la red SD-WAN.
  - **MPLS**: variante especializada de intranet privada. Indica que el vínculo utiliza una o más etiquetas DSCP para controlar la calidad de servicio entre dos o más puntos de una Intranet y no puede conectarse a ubicaciones fuera de la red SD-WAN.
- **Nombre del ISP**: El nombre del proveedor de servicios.
- **Categoría de Internet**: El tipo de servicio de tecnología de acceso a Internet con enlace WAN (banda ancha, satélite, fibra, LTE, etc.) habilitado en el enlace WAN.
- **Nombre del enlace**: Se rellena automáticamente según las entradas anteriores.
- **Dirección IP de seguimiento**: La dirección IP virtual de la ruta virtual a la que se puede hacer ping para determinar el estado de la ruta.
- Dirección**IPv4 pública y direcciónIPv6**pública: La dirección IP del servidor NAT o DNS. Esta dirección es aplicable y expuesta, solo cuando el tipo de acceso de enlace WAN es Internet público o Intranet privada en la implementación de HA serie. La IP pública se puede configurar manualmente o aprender automáticamente mediante la opción Aprendizaje automático.
- **Detección automática**: Cuando está habilitada, el dispositivo SD-WAN detecta automáticamente la dirección IP pública. Esta opción solo está disponible cuando la función del dispositivo es una **rama** y no el **nodo de control maestro (MCN)**.
- **Velocidad de salida**: La velocidad de WAN a LAN.
  - **Velocidad**: La velocidad disponible o permitida del tráfico de WAN a LAN en Kbps o Mbps.
  - **Velocidad permitida**: En los casos en que se supone que el dispositivo SD-WAN no debe utilizar toda la capacidad del enlace WAN, cambie la velocidad permitida en consecuencia.
  - **Aprendizaje automático**: Si no está seguro del ancho de banda y si los enlaces no son confiables, puede habilitar la función de aprendizaje automático. La función Aprendizaje automático solo aprende la capacidad del vínculo subyacente y utiliza el mismo valor en el futuro.
  - **Velocidad física**: La capacidad de ancho de banda real del enlace WAN.
- **Velocidad de ingreso**: La velocidad de LAN a WAN.
  - **Velocidad**: La velocidad disponible o permitida del tráfico de LAN a WAN en Kbps o Mbps.
  - **Velocidad permitida**: En los casos en que se supone que el dispositivo SD-WAN no debe utilizar toda la capacidad del enlace LAN, cambie la velocidad permitida en consecuencia.

  - **Aprendizaje automático**: Si no está seguro del ancho de banda y si los enlaces no son confiables, puede habilitar la función de aprendizaje automático. La función Aprendizaje automático solo aprende la capacidad del vínculo subyacente y utiliza el mismo valor en el futuro.
  - **Velocidad física**: La capacidad de ancho de banda real del enlace LAN.

#### Colas MPLS

La configuración de la **cola MPLS** solo está disponible para el tipo de acceso al enlace WAN MPLS. Esta opción tiene por objeto permitir la definición de las colas correspondientes a las colas MPLS del proveedor de servicios, en el enlace WAN MPLS. Para obtener información sobre cómo agregar colas MPLS, consulte Colas MPLS.

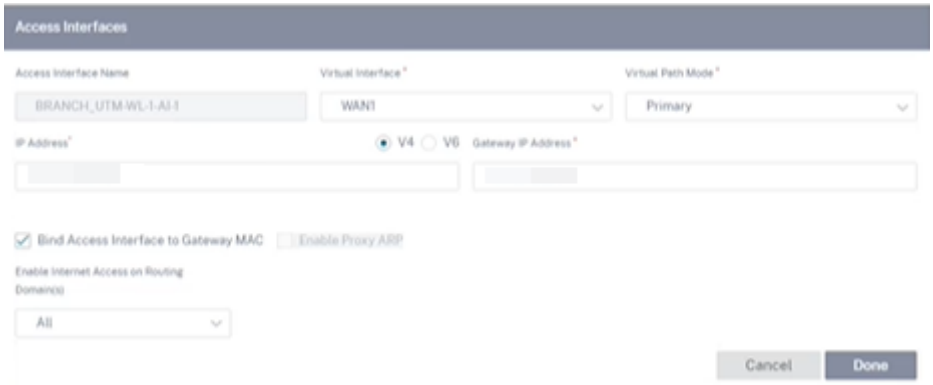
#### Interface de acceso

Una interfaz de acceso define la dirección IP y la dirección IP de la puerta de enlace de un enlace WAN. Se requiere al menos una interfaz de acceso para cada enlace WAN. Los siguientes son los parámetros de la interfaz de acceso:

- **Nombre de la interfaz de acceso**: Nombre con el que se hace referencia a la interfaz de acceso El valor predeterminado utiliza la siguiente convención de nomenclatura: WAN_LINK_NAME-AI-Number: Donde WAN_LINK_Name es el nombre del enlace WAN que está asociando a esta interfaz, y number es el número de interfaces de acceso configuradas actualmente para este vínculo, incrementadas en 1.
- **Interfaz virtual**: La interfaz virtual que utiliza la interfaz de acceso. Seleccione una entrada en el menú desplegable de Interfaces virtuales configuradas para el sitio de sucursal actual.
- **Modo de ruta virtual**: Especifica la prioridad del tráfico de ruta virtual en el enlace WAN actual. Las opciones son: Principal, Secundarioo Excluir. Si se establece en Excluir, la interfaz de acceso se usa únicamente para el tráfico de Internet e Intranet.
- **Dirección IP**: La dirección IP del punto final de la interfaz de acceso desde el dispositivo a la WAN. Seleccione V4 (IPv4) o V6 (IPv6) según sea necesario.
- **Dirección IP de puerta**de enlace: La dirección IP del router de puerta de enlace.
- **Enlazar la interfaz de acceso a la MAC de la puerta**de enlace: Si está habilitada, la dirección MAC de origen de los paquetes recibidos en los servicios de Internet o Intranet debe coincidir con la dirección MAC de la puerta de enlace Enlaces de.
- **Habilitar el ARP del proxy**: Si se habilita, el dispositivo WAN virtual responde a las solicitudes de ARP para la dirección IP de la puerta de enlace cuando no se puede acceder a la puerta de enlace.
- **Habilitar el acceso a Internet en los dominios de enrutamiento**: Crea automáticamente una ruta PREDETERMINADA (0.0.0.0/0) en todas las tablas de enrutamiento de los dominios de en-

rutamiento respectivos. Puede habilitar para TODOS los dominios de enrutamiento o NINGUNO. Evita la necesidad de crear una ruta estática exclusiva a través de todos los dominios de enrutamiento si necesitaban acceso a Internet.




### Servicios

La sección **Servicios** le permite agregar tipos de servicios y asignar el porcentaje de ancho de banda que se utilizará para cada tipo de servicio. Puede definir los tipos de servicio y configurar sus atributos en la sección Servicios de entrega. Puede optar por utilizar estos valores predeterminados globales o configurar los ajustes de ancho de banda de servicio específicos del enlace en la lista desplegable de **ajustes de ancho de banda del servicio**. Si elige el vínculo específico, introduzca los siguientes detalles:

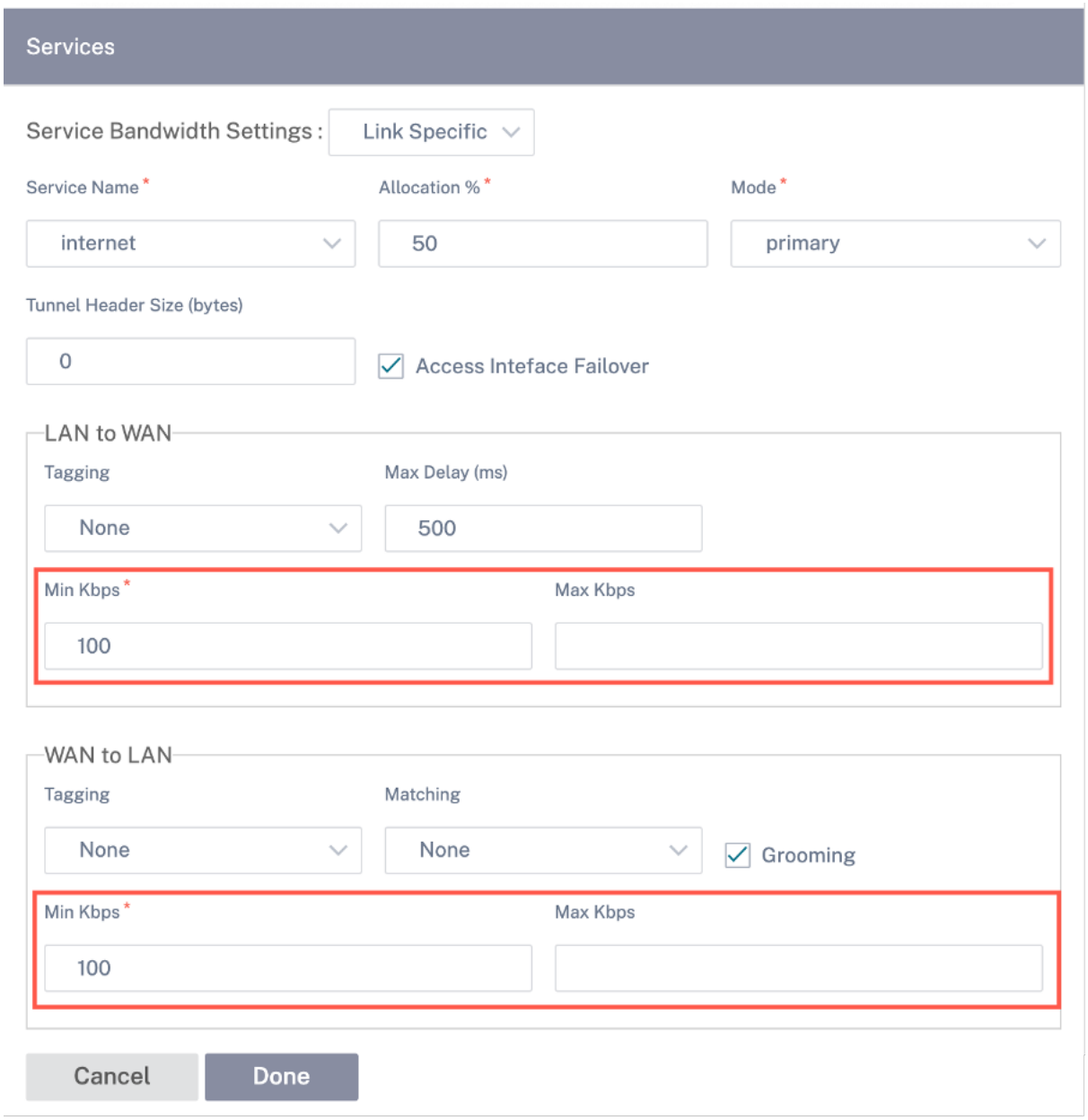
- **Nombre del servicio**: El nombre del servicio de enlace WAN.
- **% de asignación**: La parte justa garantizada del ancho de banda asignada al servicio con respecto a la capacidad total del enlace.
- **Modo**: El modo de funcionamiento del enlace WAN, según el servicio seleccionado. Para Internet, hay uno de Primaria, Secundaria y Equilibrio y para Intranet hay Primaria y Secundaria.
- **Tamaño del encabezado del túnel**: El tamaño del encabezado del túnel, en bytes.
- **Etiqueta de LAN a WAN**: La etiqueta DHCP que se aplica a los paquetes de LAN a WAN del servicio.
- **Retraso de LAN a WAN**: Tiempo máximo para almacenar paquetes en búfer cuando se supera el ancho de banda de los enlaces WAN.
- **Mínimo Kbps de LAN a WAN**: El valor mínimo de ancho de banda de carga que está reservado para el servicio. El campo **Mínimo en Kbps** es obligatorio.
- **Máximo en Kbps de LAN a WAN**: El valor máximo de ancho de banda de carga reservado para el servicio. El campo **Máximo de Kbps** es opcional y el valor no puede ser inferior al valor mínimo de ancho de banda de carga configurado. El valor debe ser igual o superior al valor mínimo del ancho de banda de carga.
- **Etiqueta WAN a LAN**: La etiqueta DHCP que se aplica a los paquetes WAN a LAN del servicio.

- **Coincidencia de WAN a LAN**: Los criterios de coincidencia para que los paquetes de Internet WAN a LAN se asignen al servicio.
- **Kbps mínimo de WAN a LAN**: El valor mínimo de ancho de banda de descarga que está reservado para el servicio. El campo **Mínimo en Kbps** es obligatorio.
- **Máximo de Kbps de WAN a LAN**: El valor máximo de ancho de banda de descarga reservado para el servicio. El campo **Máximo de Kbps** es opcional y el valor no puede ser inferior al valor mínimo de ancho de banda de descarga configurado. El valor debe ser igual o superior al valor mínimo del ancho de banda de descarga.
- Limpieza de**WAN a LAN: Si**se habilita, los paquetes se descartan aleatoriamente para evitar que el tráfico de WAN a LAN supere el ancho de banda aprovisionado por el servicio.

> **Nota**
>
> Los campos de Kbps mínimo y máximo no están disponibles para la ruta virtual.




### Configuración de la ruta virtual para el enlace

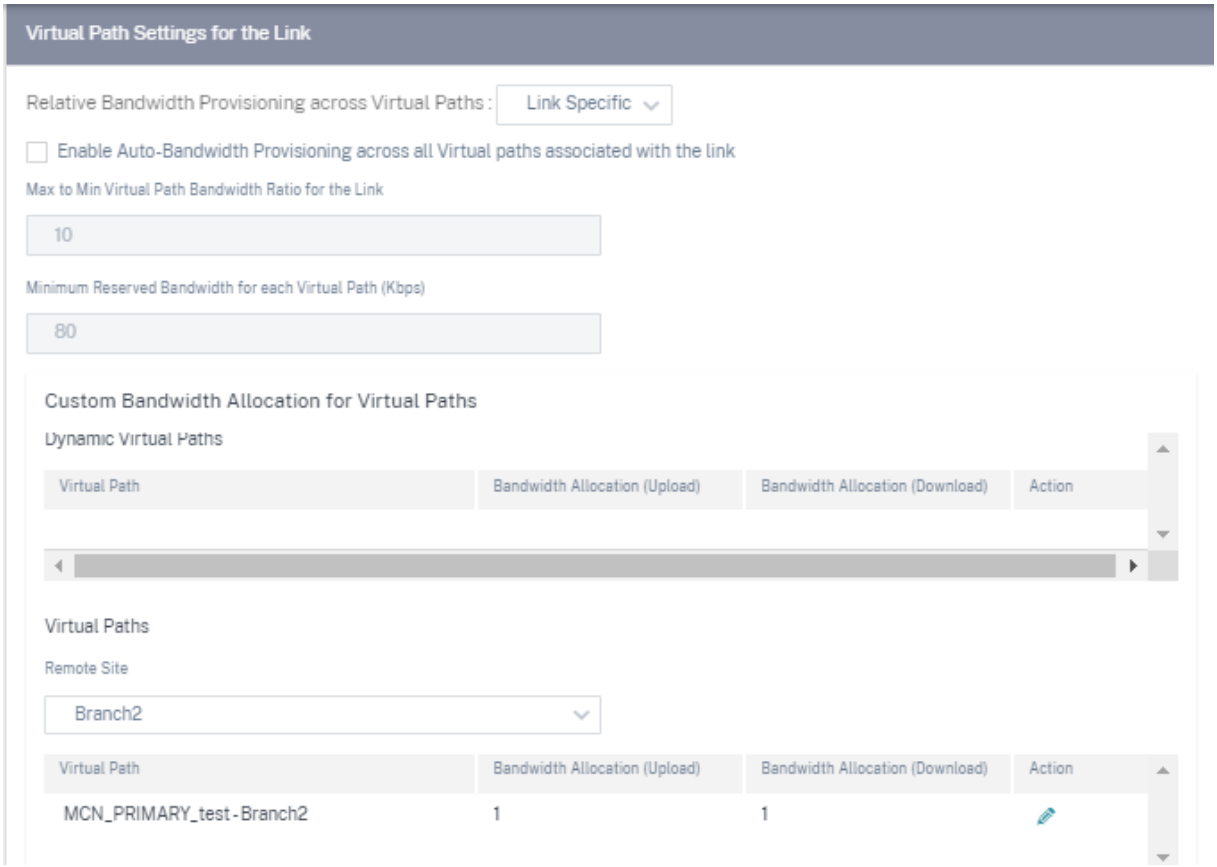
Seleccione el aprovisionamiento de ancho de banda relativo en las rutas virtuales como **predeterminado global** o **específico de enlace**, según sea necesario. Al seleccionar **Link Specific**, al habilitar el aprovisionamiento automático del ancho de banda, la parte del ancho de banda para el servicio de rutas virtuales se calcula automáticamente y se aplica en función de la magnitud del ancho de banda que pueden consumir los sitios remotos.

- **Relación de ancho de banda de ruta virtual máxima a mínima para el enlace**: Puede establecer la relación de ruta virtual máxima y mínima que se puede aplicar al enlace WAN selec-

cionado.

- Ancho de**banda mínimo reservado para cada ruta virtual (Kbps)**: Puede establecer el valor mínimo de ancho de banda reservado en Kbps para cada ruta virtual.

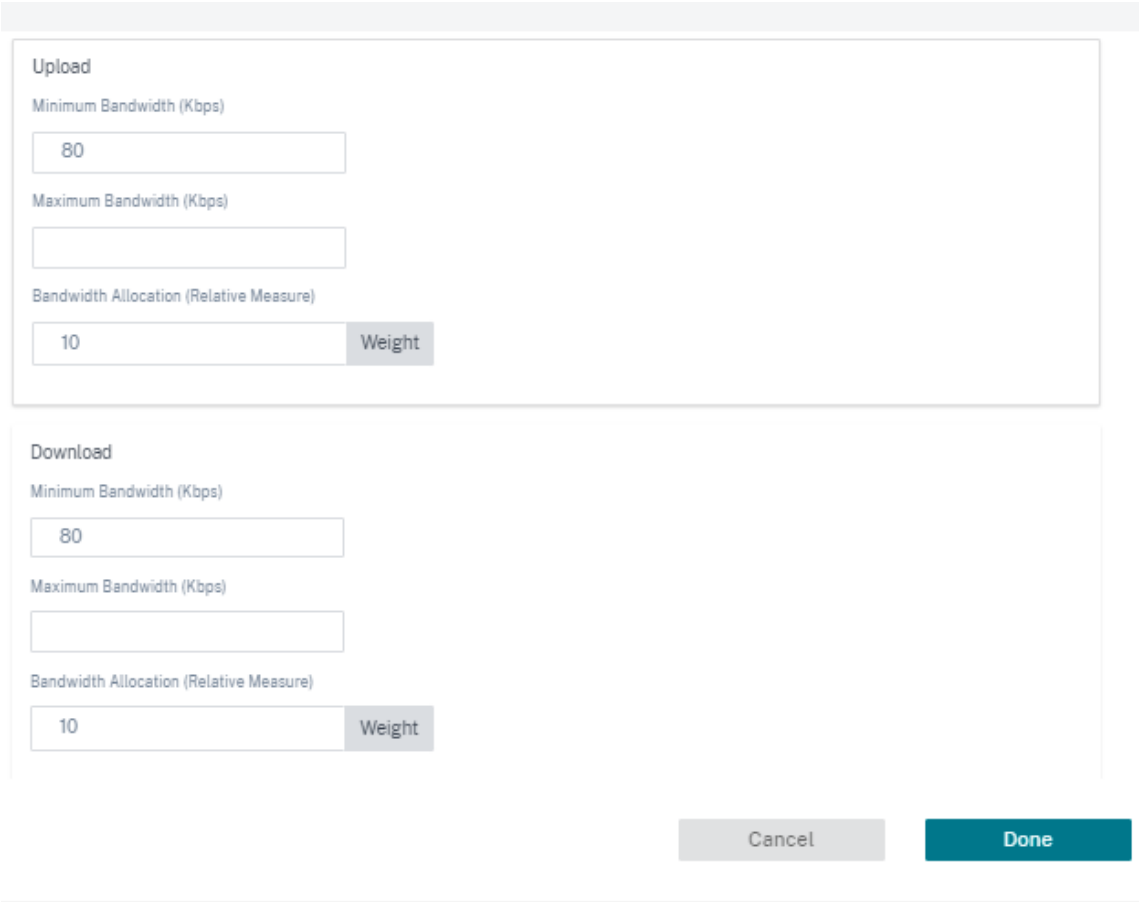



Para personalizar los anchos de banda de las rutas virtuales asociadas a un enlace WAN:

1. Desactive la casilla **Habilitar el Provisioning automático de ancho de banda en todas las rutas virtuales asociadas al enlace**.
2. En la sección **Asignación personalizada de ancho de banda para rutas virtuales**, seleccione un sitio remoto. Puede aprovisionar anchos de banda para las rutas virtuales al sitio remoto.
    - **Ancho de banda mínimo (Kbps)**: El ancho de banda mínimo reservado para la ruta virtual. El ancho de banda mínimo que puede configurar para una ruta virtual es de 80 Kbps.
    - Ancho de**banda máximo (Kbps)**: El ancho de banda máximo que la ruta virtual puede utilizar desde el enlace WAN. Si no se establece el ancho de banda máximo, el sitio utiliza todo el ancho de banda disponible.
    - **Asignación de ancho de banda (medida relativa)**: El ancho de banda compartido asignado a una ruta virtual fuera del ancho de banda elegible de su grupo. Por ejemplo, si un grupo de enlaces WAN de 3 rutas virtuales cumple los requisitos para un ancho de banda

de 30 Mbps y quiere asignar el mismo ancho de banda para cada ruta virtual, actualice 10 como asignación de ancho de banda en el sitio remoto.




3. Haga clic en **Listo**.

> **Nota**
>
> El servicio Citrix SD-WAN Orchestrator conserva la configuración de ancho de banda personalizada previamente configurada incluso después de que las rutas virtuales dinámicas configuradas anteriormente estén inhabilitadas entre dos sitios. Asegúrese de actualizar la configuración personalizada del ancho de banda de forma manual cuando vuelva a configurar las rutas virtuales dinámicas.

**Puntos a tener en cuenta para el aprovisionamiento de**

- De forma predeterminada, todas las sucursales y los servicios WAN (ruta virtual/Internet/intranet) reciben una ponderación de 1 cada uno.
- La personalización del ancho de banda es necesaria cuando hay una gran disparidad en términos de requisitos de ancho de banda.

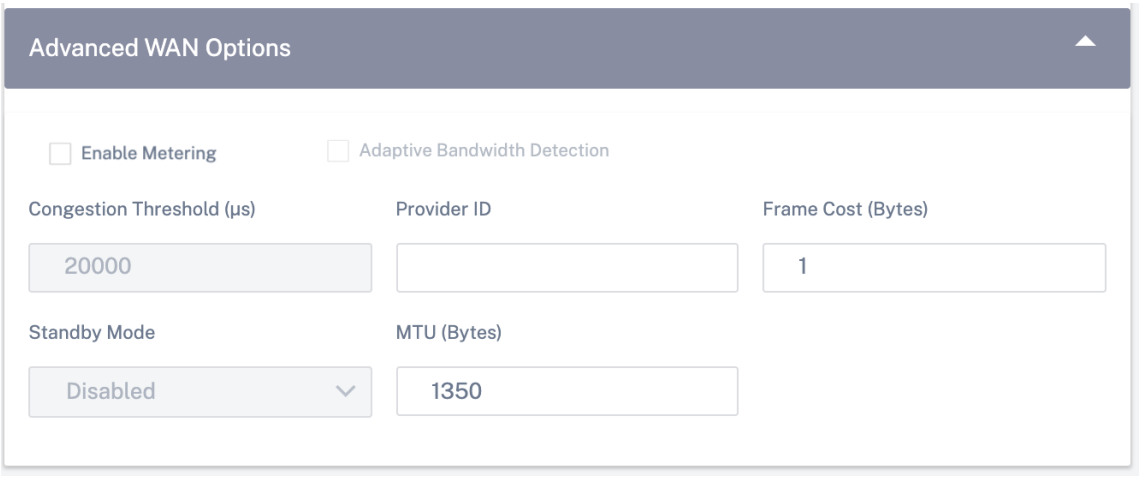
 

- Cuando se habilitan las rutas virtuales dinámicas entre los sitios disponibles, la capacidad del enlace WAN se comparte entre la ruta virtual estática al centro de datos y las rutas virtuales dinámicas.

#### Opciones WAN avanzadas

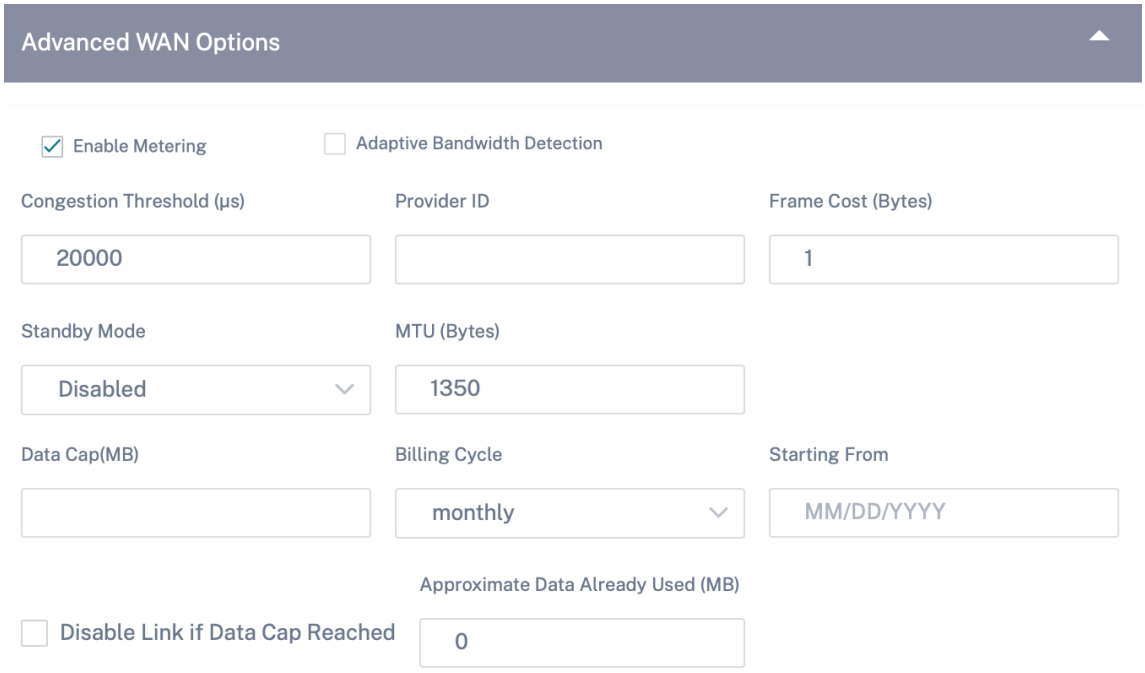
La configuración avanzada del enlace WAN permite configurar los atributos **específicos del ISP**.

- **Umbral de congestión**: Cantidad de congestión después de la cual el enlace WAN limita la transmisión de paquetes para evitar una mayor congestión.
- **ID de proveedor**: identificador único para que el proveedor diferencie las rutas al enviar paquetes duplicados.
- **Coste de trama (bytes)**: Se agregan bytes adicionales de encabezado/tráiler a cada paquete, por ejemplo, para los tráilers de Ethernet IPG o AAL5.
- **MTU (bytes)**: El tamaño de paquete sin procesar más grande en bytes, sin incluir el coste de la trama.
- **Modo de espera**: Un enlace en espera no se usa para transportar el tráfico de usuarios a menos que se active. El modo de espera de un enlace WAN está inhabilitado de forma predeterminada. Para obtener más información sobre el modo de espera, consulte Modo de espera.




- **Habilitar la medición**: Realiza un seguimiento del uso en un enlace WAN y alerta al usuario cuando el uso del enlace supera el límite de datos configurado. Para obtener información detallada sobre la medición, consulte Vínculos WAN de medición y en espera.




- **Detección de ancho de banda adaptable**: Utiliza el enlace WAN a una velocidad de ancho de banda reducida cuando se detecta una pérdida. Cuando el ancho de banda disponible esté por debajo del ancho de **banda mínimo aceptable**configurado, la ruta se marcará como INCORRECTA. Utilice Sensibilidad de pérdida errónea personalizada en el grupo Ruta o Autopath con Detección de ancho de banda adaptable.

  > **Nota**
  >
  > La detección de ancho de banda adaptable solo está disponible para el cliente y no para MCN.

  - Ancho de**banda mínimo aceptable**: Cuando hay una velocidad de ancho de banda variable, el porcentaje de velocidad permitida de WAN a LAN por debajo del cual la ruta se marca como MALA. Los kbps mínimos son diferentes en cada lado de una ruta virtual. El valor puede estar en el rango 10% -50% y el valor predeterminado es 30%.

Para obtener más información, consulte Detección de ancho de banda adaptable

### Rutas

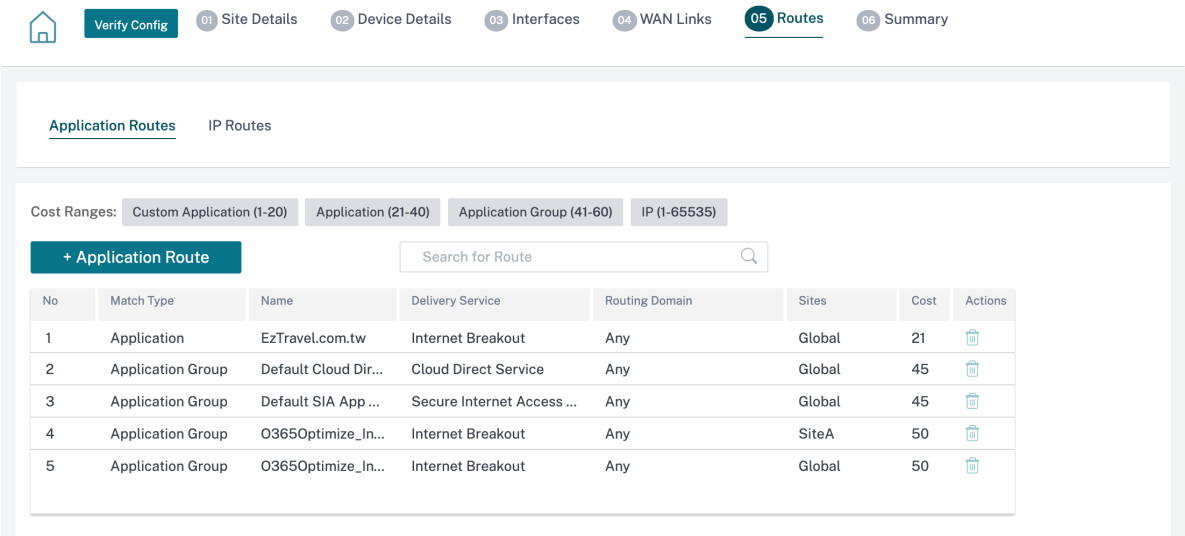
El siguiente paso en el flujo de trabajo de configuración del sitio es crear rutas. Puede crear rutas de aplicaciones e IP en función de los requisitos del sitio.

> **NOTA**
>
> Las rutas que se agregaron antes de introducir las fichas **Ruta de aplicación** y **Ruta IP** se enumeran en la ficha **Rutas IP** con el nombre de **Servicio de entrega** como Internet.

Las rutas globales y las rutas específicas del sitio que se crean al nivel de red aparecen automáticamente en las fichas **Rutas > Rutas de aplicación** y **rutas > Rutas IP**. Solo se pueden ver las rutas globales en el nivel de emplazamiento. Para modificar o eliminar una ruta global, vaya a las configuraciones de nivel de red.

También puede crear, modificar o eliminar rutas en el nivel del sitio.




### Rutas de aplicación

Haga clic en **+ Ruta de aplicación** para crear una ruta de aplicación.

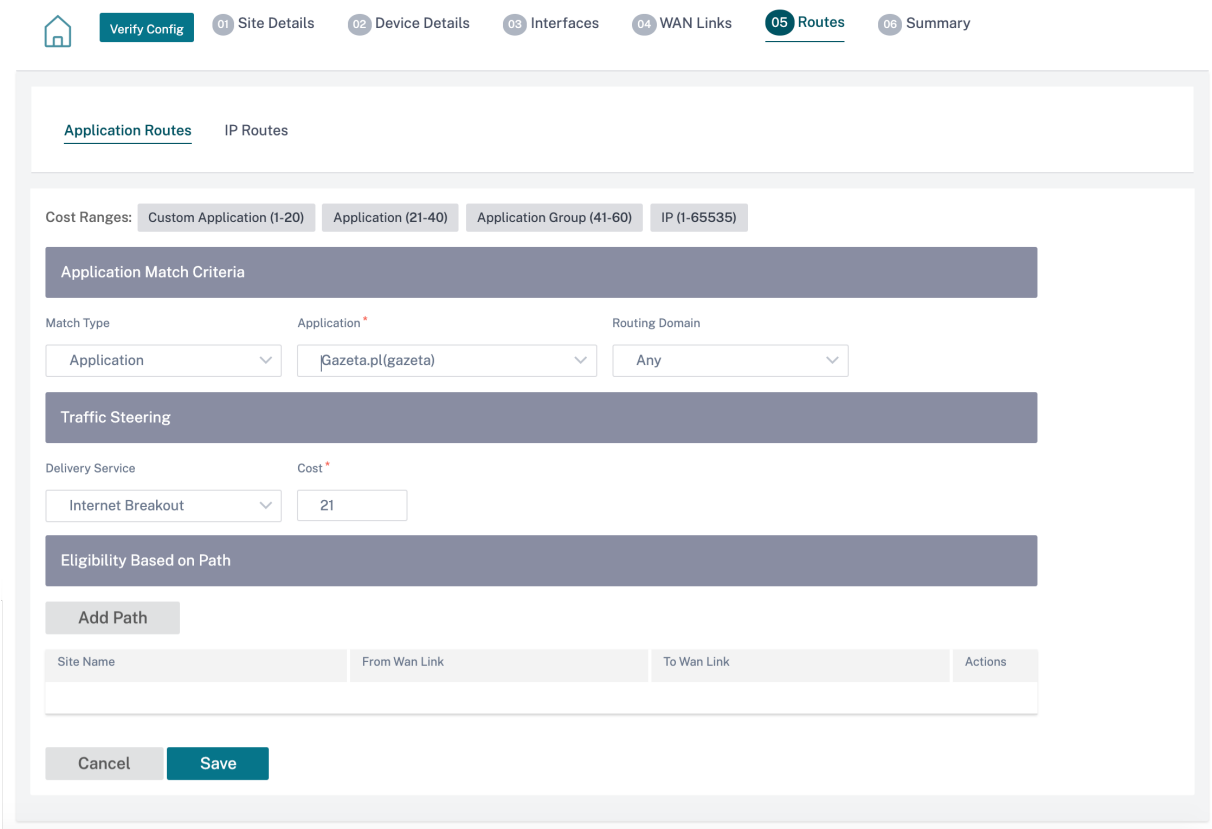
- **Criterios de coincidencia de aplicaciones personalizados**
  - **Tipo de coincidencia**: Seleccione el tipo de coincidencia como **Aplicación**/****Aplicación personalizada/Grupo**** de aplicaciones en la lista desplegable.
  - **Aplicación**: Seleccione una aplicación de la lista desplegable.
  - **Dominio de enrutamiento**: Seleccione un dominio de enrutamiento.
- **Dirección de Tráfico**
  - **Servicio de entrega**: Elija un servicio de entrega de la lista.
  - **Coste**: Refleja la prioridad relativa de cada ruta. Reduzca el coste, mayor será la prioridad.
- **Elegibilidad basada en la ruta**:

- **Agregar ruta**: Elija un sitio y enlaces WAN, tanto de origen como de destino. Si la ruta agregada desaparece, entonces la ruta de la aplicación no recibe ningún tráfico.

Si se agrega una nueva ruta de aplicación, el coste de la ruta debe estar en el rango siguiente:

- Aplicación personalizada: 1—20
- Aplicación: 21—40
- Grupo de aplicación: 41-60




### Rutas IP

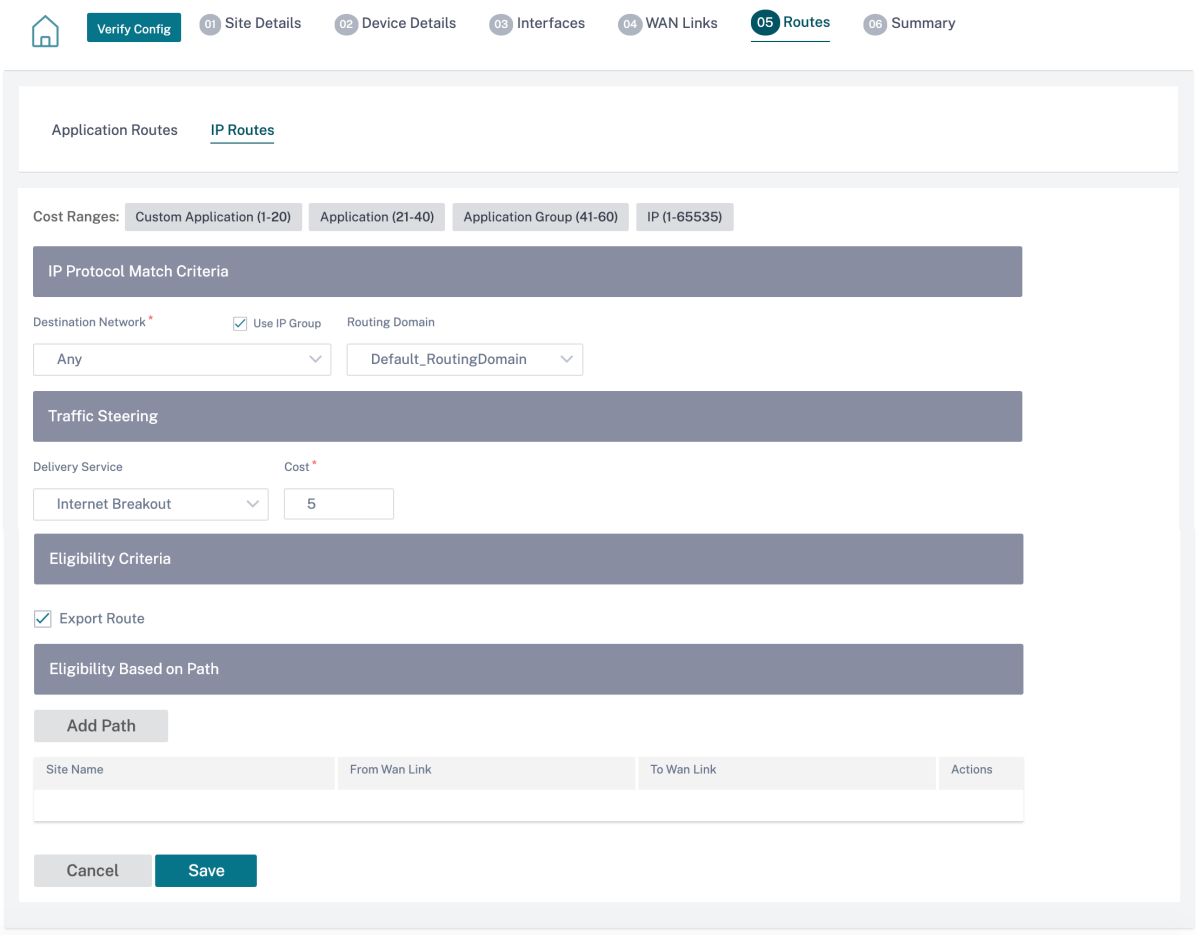
Vaya a la ficha **Rutas IP** y haga clic en **+ Ruta IP** para crear la directiva de rutas IP para dirigir el tráfico.

- **Criterios de coincidencia del protocolo IP**
  - **Red de destino**: Agregue la red de destino que ayuda a reenviar los paquetes.
  - **Usar grupo IP**: Puede agregar una red de destino o activar la casilla Usar grupo IP para seleccionar cualquier grupo de IP de la lista desplegable.
  - **Dominio de enrutamiento**: Seleccione un dominio de enrutamiento de la lista desplegable.

- **Dirección de Tráfico**
  - **Servicio de entrega**: Elija un servicio de entrega de la lista desplegable.
  - **Coste**: Refleja la prioridad relativa de cada ruta. Reduzca el coste, mayor será la prioridad.
- **Criterios de elegibilidad**
  - **Exportar ruta**: Si se selecciona la casilla Exportar ruta y la ruta es una ruta local, la ruta se puede exportar de forma predeterminada. Si la ruta es una ruta basada en INTRANET/INTERNET, para que la exportación funcione, el reenvío WAN a WAN debe estar habilitado. Si la casilla Exportar ruta está desactivada, la ruta local no puede exportarse a otra SD-WAN y tiene importancia local.
- **Elegibilidad basada en la ruta**:
  - **Agregar ruta**: Elija un sitio y enlaces WAN, tanto de origen como de destino. Si la ruta agregada desaparece, entonces la ruta IP no recibe ningún tráfico.

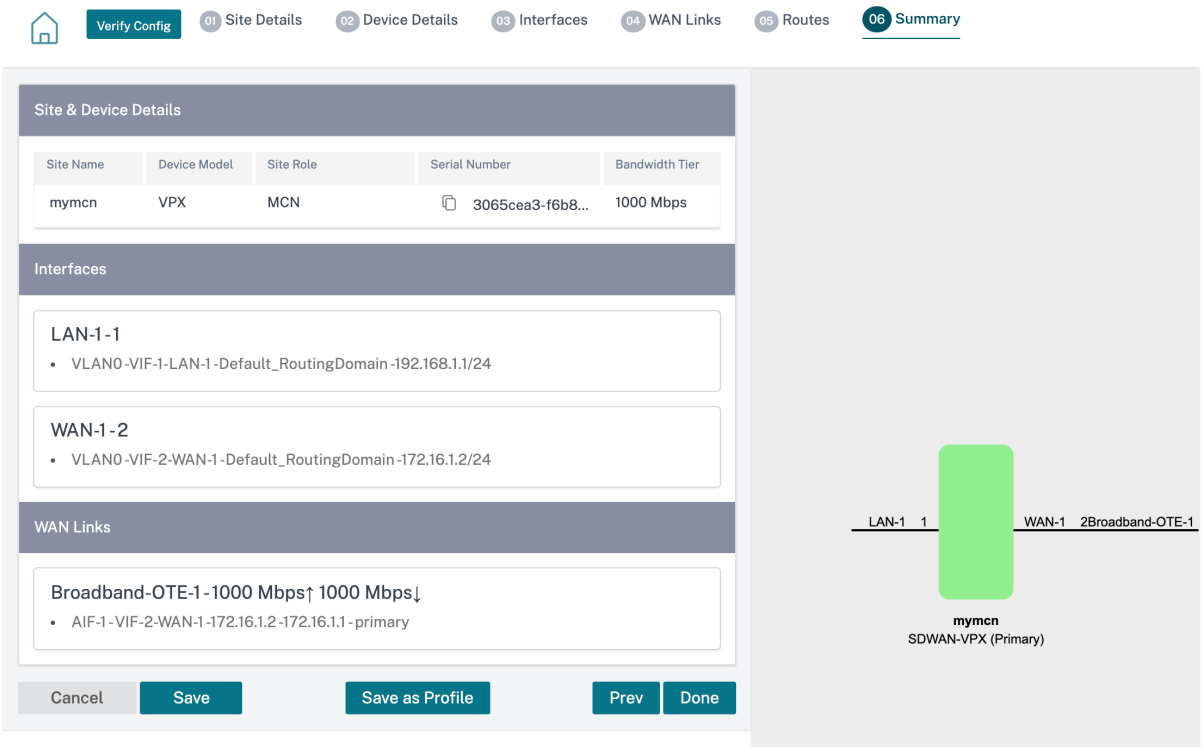
Si se agrega una nueva ruta IP, el coste de la ruta debe estar entre 1 y 20.



### Resumen

Esta sección proporciona un resumen de la configuración del sitio para permitir una revisión rápida antes de enviar el mismo.




Utilice la opción **Guardar como plantilla** para guardar la configuración del sitio como plantilla para volver a utilizarla en otros sitios. Al hacer clic en **Listo**, se completa la configuración del sitio y se accede a la página de **inicio de Configuración de red** para revisar todos los sitios configurados. Para obtener más información, consulte Configuración de red.

## Actualización de firmware LTE

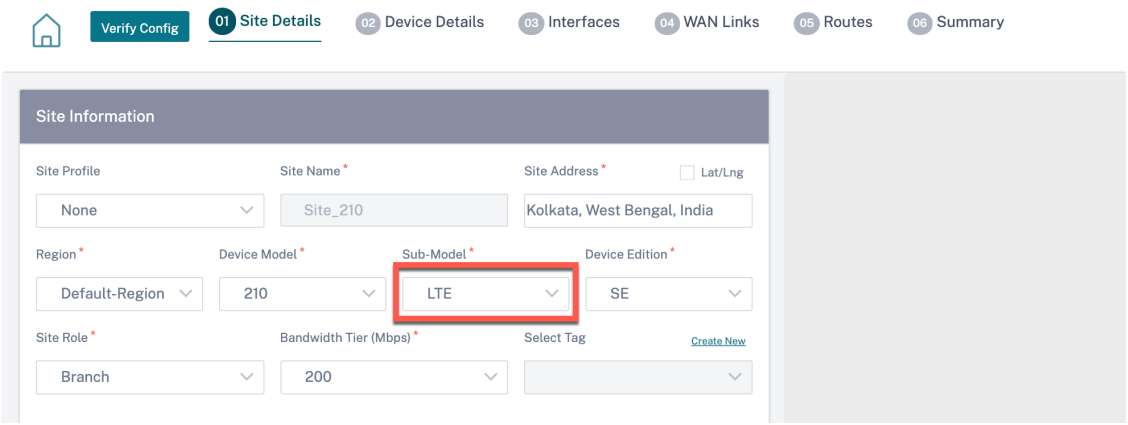
October 31, 2022

El servicio Citrix SD-WAN Orchestrator le permite configurar y administrar todos los sitios LTE de su red. Incluye dispositivos conectados a través de un módem LTE interno o un módem USB LTE externo.

Para configurar los sitios LTE en la red:

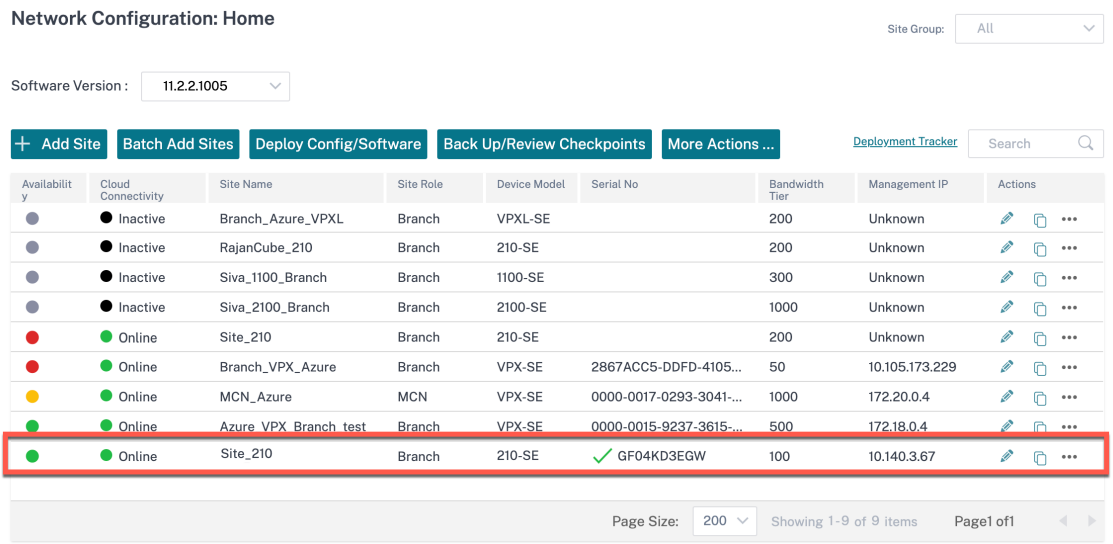
1. A nivel de sitio, vaya a **Configuración > Configuración del sitio**.




2. Seleccione el submodelo como **LTE** junto con los demás detalles necesarios y haga clic en Guardar. Para obtener más información sobre la configuración del sitio, consulte Configuración del sitio.

3. Una vez creado el sitio, vaya a la página **principal de configuración de red** y haga clic en el botón **Deploy Config/Software**.



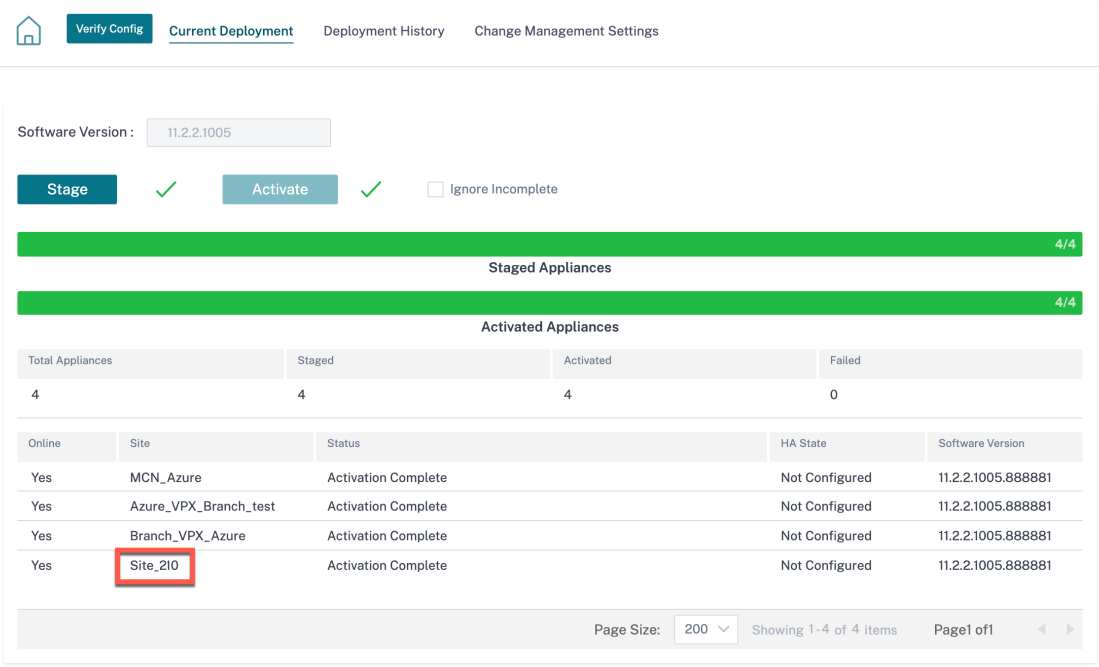

c

**Nota:**

Actualmente, la compatibilidad con LTE está disponible en los dispositivos Citrix SD-WAN 210.

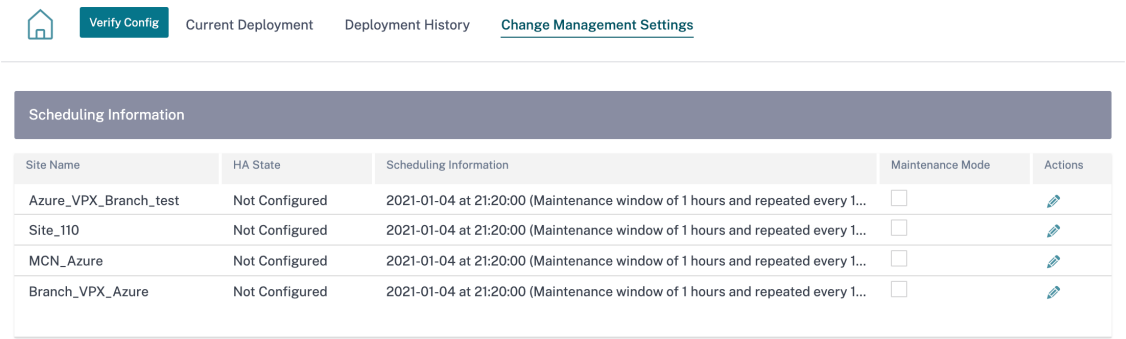
4. El campo **Versión de software** se rellena automáticamente con el paquete de la versión de software más reciente y el archivo no se puede modificar. Al hacer clic en **Stage**, se descarga todo el firmware LTE adecuado para la versión de software seleccionada.




Lleva unos minutos completar el ensayo. Puede ver el estado para realizar un seguimiento del progreso del ensayo. Inicialmente, el **estado muestra En fase pendiente**, **Descarga del software del dispositivo**y, por último, En **fase finalizada**. Puede cancelar la puesta en escena en cualquier momento haciendo clic en el botón **Cancelar etapa**.

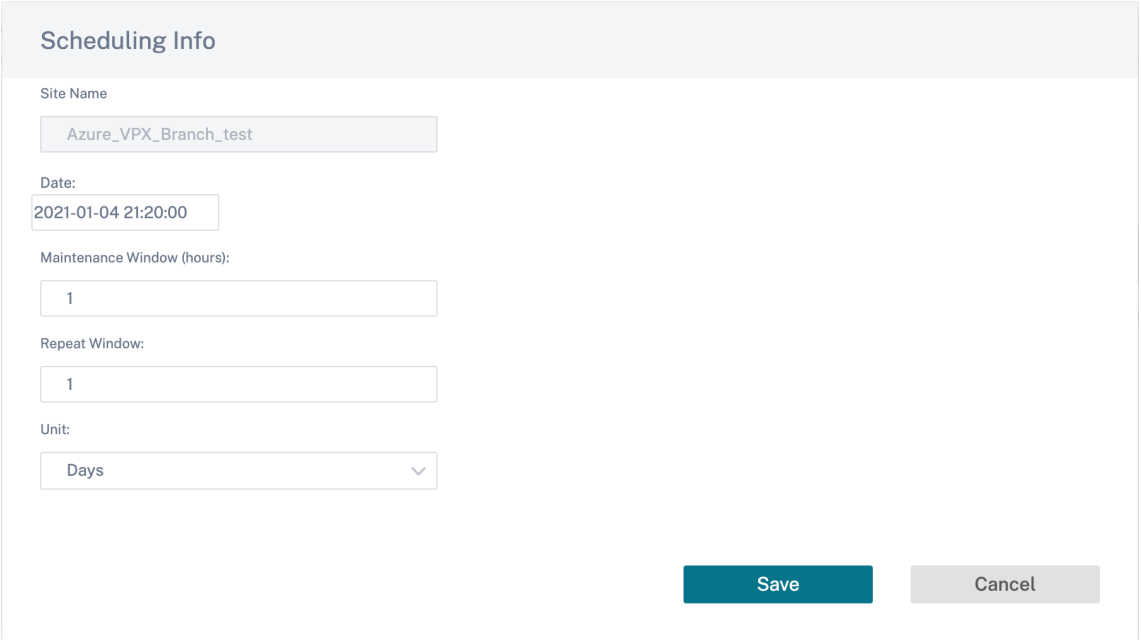
5. Una vez finalizada la puesta en escena, haga clic en el botón **Activar** para activar el software.
6. La activación del software LTE forma parte de la ventana de programación. Para actualizar el software LTE, vaya a la ficha **Configuración de administración de cambios**. Puede ver una lista de nombres de sitio con información de programación y una opción de acción.




En la ventana de programación, se especifica un período de tiempo específico para completar la actualización del software LTE.

7. Haga clic en el símbolo de acción y proporcione la información de programación: fecha con hora, duración del período de mantenimiento en horas, ventana repetida con la unidad como días/semanas/meses. Haga clic en **Guardar**.




Una vez que se establece la temporización, propaga la información al dispositivo. El firmware de LTE se actualiza cuando la hora del dispositivo coincide con la hora establecida en la ventana de programación. La ventana de programación le permite configurar una hora específica para actualizar el firmware LTE. La actualización del firmware LTE no se iniciará inmediatamente cuando establezca la ventana de programación.

> **Nota**
>
> Para todos los dispositivos, la siguiente es la información de programación predeterminada que ya está configurada:
>
> - **Ventana de programación**: 21:20:00
> - **Período de mantenimiento**: 1 hora
> - **Ventana repetida**: 1 día
>
> Por lo tanto, si no configura los ajustes de administración de cambios, la ventana de programación procesará la actualización automáticamente. Además, si establece el valor de la **ventana de mantenimiento (horas)** en **0**, la actualización del firmware de LTE se realiza inmediatamente.

A partir de 11.1.0, se agrega un nuevo mando de configuración para la configuración de administración en banda en la página del grupo de interfaz de sitio. Esta es una configuración obligatoria para cualquier dispositivo que necesite administrarse a través de una IP dentro de banda. La falta de esta configuración en el servicio Citrix SD-WAN Orchestrator puede provocar que el dispositivo se desconecte (lo que es especialmente importante cuando los 210 y 110 que se administraron a través de LTE se actualizan a la 11.1.0).

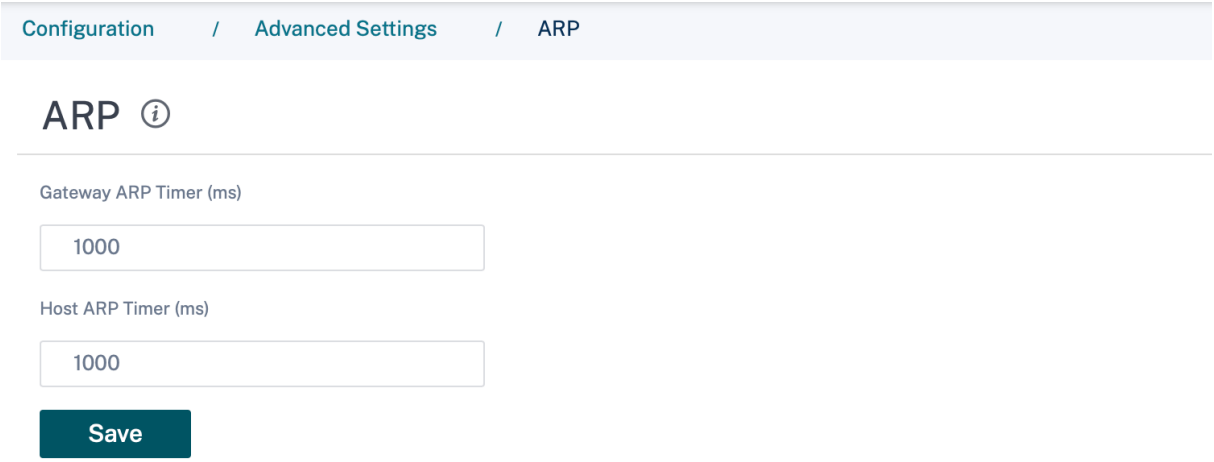
 

## Protocolo de resolución de direcciones

October 31, 2022

En las implementaciones de Citrix SD-WAN, como Gateway y One-ARM, cuando se reciben con frecuencia las solicitudes del Protocolo de resolución de direcciones (ARP), los puntos de acceso se sobrecargan y afectan al flujo de tráfico. Para superar la sobrecarga de tráfico, puede configurar los siguientes temporizadores de ARP para enviar las solicitudes de ARP con intervalos de tiempo específicos.

- **Temporizador ARP de puerta de enlace (ms)**: El tiempo (rango: 100 a 20000 milisegundos) entre las solicitudes de ARP de las direcciones IP de gateway configuradas.
- **Temporizador de ARP del host (ms)**: El tiempo (rango: De 1000 a 180000 milisegundos) entre las solicitudes de ARP de direcciones IP de host configuradas.




## Protocolo de descubrimiento de vecinos

October 31, 2022

En una red IPv6, los dispositivos Citrix SD-WAN emiten periódicamente los mensajes de publicidad del enrutador para anunciar su disponibilidad y transmitir información a los dispositivos vecinos de la red SD-WAN. Los anuncios de enrutador incluyen la información del prefijo IPv6. El protocolo NDP (NDP) que se ejecuta en los dispositivos Citrix SD-WAN utiliza estas publicaciones de enrutadores para determinar los dispositivos vecinos en el mismo enlace. El NDP también determina las direcciones de la capa de enlace de cada uno, encuentra vecinos y mantiene la información de accesibilidad de los vecinos activos.

Para configurar el anuncio del enrutador NDP, vaya a **Configuración > Configuración > Configuración avanzada > NDP** y haga clic en **+ NDP**.

Elija una de las interfaces virtuales configuradas de la lista desplegable de **interfaces virtuales**. Seleccione **Activar publicidad** para habilitar el envío periódico de anuncios de enrutadores y la respuesta a las solicitudes de enrutador para la interfaz virtual seleccionada.

Especifique los intervalos máximo, mínimo y de vida útil del router.

- **Intervalo máximo**: El tiempo máximo (en segundos) permitido entre el envío periódico de anuncios de enrutadores multidifusión no solicitados.
- **Intervalo mínimo**: El tiempo mínimo (en segundos) permitido entre el envío periódico de anuncios no solicitados de enrutador multidifusión.
- **Duración del router**: Tiempo (en segundos) durante el que los hosts consideran válido el router. El 0 indica que el router no se puede utilizar como router predeterminado

Seleccione **Managed Flag** si las direcciones IP están disponibles a través del protocolo DHCPv6. Seleccione **Otro indicador** si la información de configuración (distinta de las direcciones IP) está disponible a través del protocolo DHCPv6.

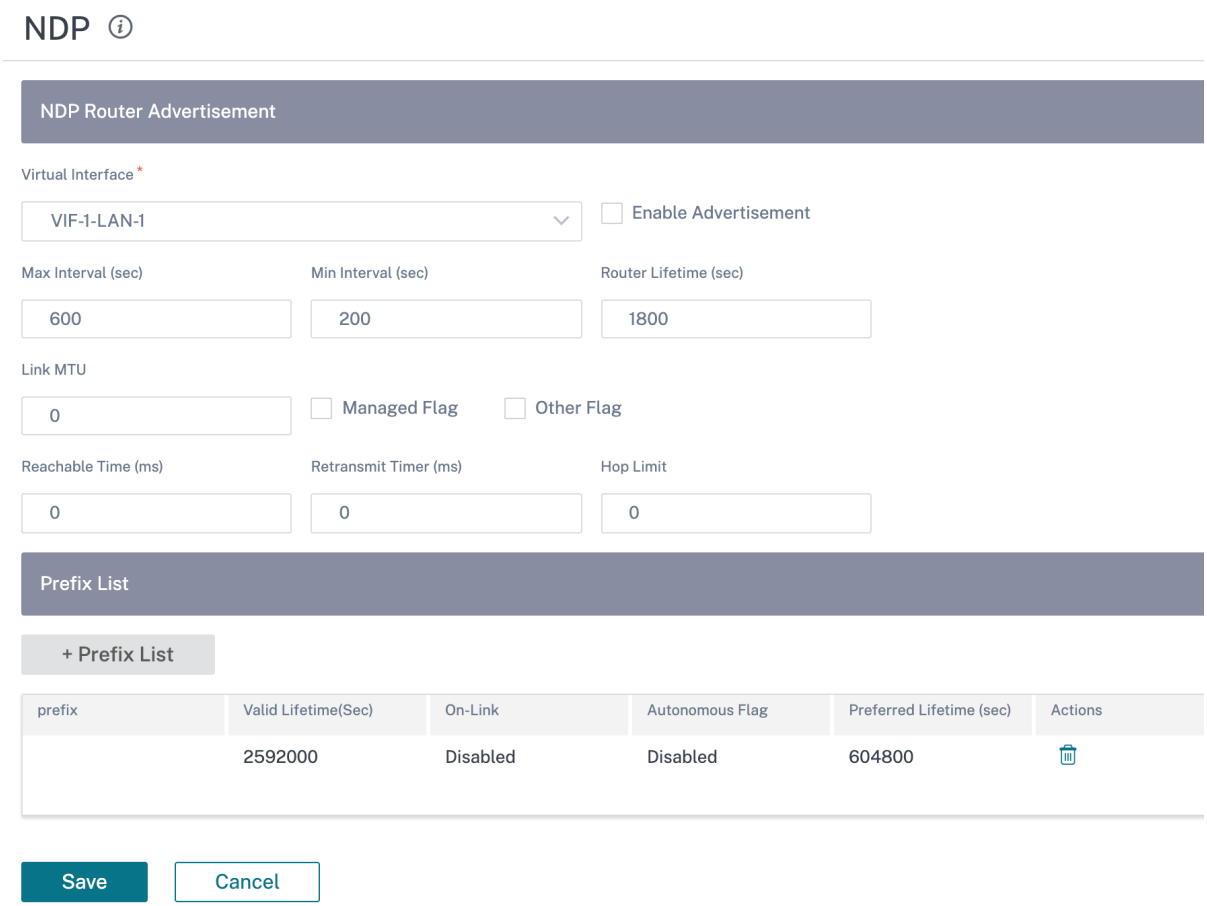
Especifique los siguientes valores para la interfaz seleccionada.

- **Link MTU**: La unidad máxima de transmisión (MTU) recomendada para la interfaz.
- **Tiempo accesible**: El tiempo (en milisegundos) en el que el protocolo NDP permanece en el estado **Accesible**.
- **Temporizador de retransmisión**: El tiempo (en milisegundos) entre la retransmisión de los mensajes de solicitud de vecino al resolver una dirección IP o sondear un vecino.
- **Límite de saltos**: El número máximo de saltos que se incluirán en el anuncio del router.

Haga clic en +Lista de prefijos e introduzca los siguientes valores:

- **Prefijo**: El prefijo y la longitud del prefijo en la notación de redirección entre dominios sin clase (CIDR).
- **Duración válida**: El tiempo en segundos hasta el que el prefijo es válido. -1 representa el infinito, lo que significa que el prefijo permanece para siempre.
- **Enlace**: Cuando se selecciona, el prefijo se considera local para la red.
- **Indicador autónomo**: Cuando está habilitado, el prefijo es utilizado por la configuración automática de direcciones sin estado (SLAAC) del host para generar la dirección IP.
- **Duración del prefijo**: El tiempo (en segundos) hasta el que se considera preferido el prefijo.




# Rutas virtuales

October 31, 2022

Una ruta virtual es un vínculo lógico entre dos enlaces WAN. Comprende una colección de rutas WAN combinadas para proporcionar comunicación de alto nivel de servicio entre dos nodos SD-WAN. Esto se logra midiendo y adaptándose constantemente a la demanda cambiante de las aplicaciones y a las condiciones de la WAN. Los dispositivos SD-WAN miden la red por ruta. Una ruta virtual puede ser estática (siempre existe) o dinámica (existe solo cuando el tráfico entre dos dispositivos SD-WAN alcanza un umbral configurado).

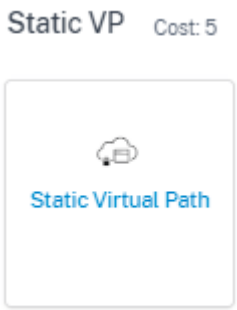
## Rutas virtuales estáticas

La configuración de ruta virtual se hereda de la configuración de ruta automática del vínculo wan global. Puede anular estas configuraciones y agregar o quitar la ruta de acceso del miembro. También

puede filtrar las rutas virtuales según el sitio y el perfil QoS aplicado. Especifique una dirección IP de seguimiento para el enlace WAN que se puede hacer un pinging para determinar el estado del enlace WAN. También puede especificar una IP de seguimiento inverso para la ruta inversa que se puede hacer un pinging para determinar el estado de la ruta inversa.

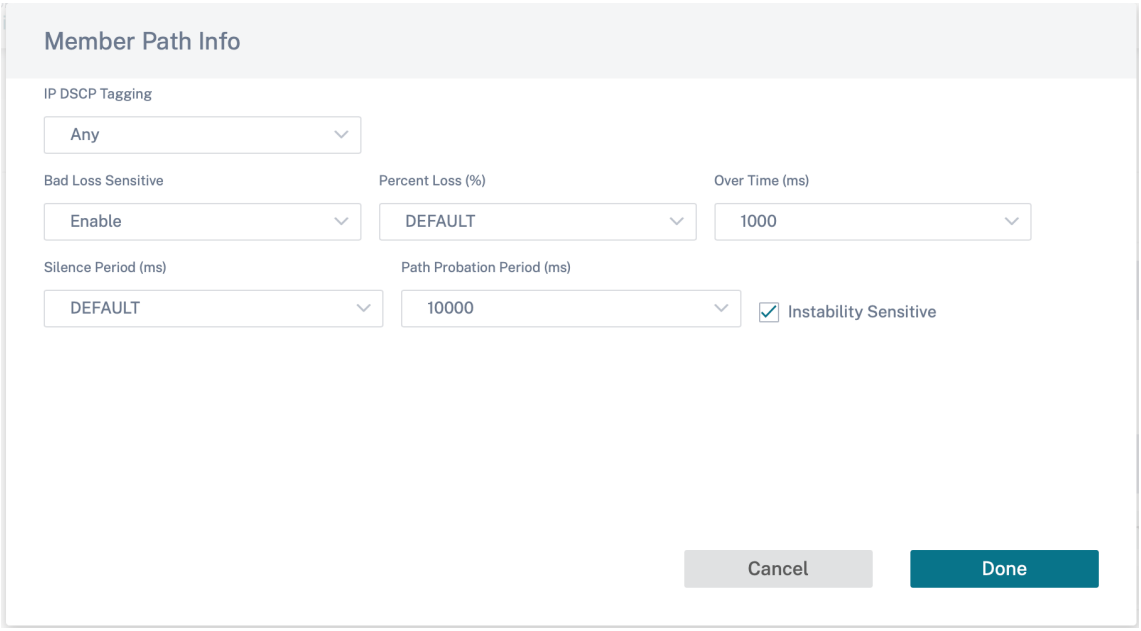
Para configurar rutas virtuales estáticas, desde el nivel del sitio, vaya a **Configuración > Configuración** > **Configuración avanzada** > **Rutas virtuales > Rutasvirtuales estáticas**.




Las rutas de los miembros activos se enumeran en la sección **Rutas de miembros activos** ; puede ver o modificar la configuración de las rutas de los miembros.

- **Etiquetado IP DSCP**: Etiqueta para el encabezado IP externo de la trama del Protocolo de control de rutas virtuales (VPCP).
- **Sensible a la pérdida**: S i se habilita, una ruta podría marcarse como MALA debido a una pérdida e incurrir en una penalización de latencia en la puntuación de la ruta. Establezca el porcentaje de pérdida durante el tiempo necesario para marcar la ruta como MALA. Inhabilite esta opción si la pérdida de ancho de banda es intolerable.
- **Porcentaje de pérdida**: Si la pérdida de paquetes supera el porcentaje establecido durante el tiempo configurado, el estado GOOD Path cambia a MALO.
- **Con el tiempo**: Si la pérdida de paquetes supera el porcentaje establecido durante este tiempo configurado, el estado de la ruta se marca como INCORRECTO.
- **Período de silencio**: El estado de la ruta pasa de BUENO a MALO cuando no se recibe ningún paquete dentro del período de tiempo especificado.
- **Período de prueba de ruta**: El período de espera antes de cambiar el estado de la ruta de MALO a BUENO.
- **Sensible a la inestabilidad**: Se tienen en cuenta las penalizaciones de latencia debidas al mal estado y otros picos de latencia.

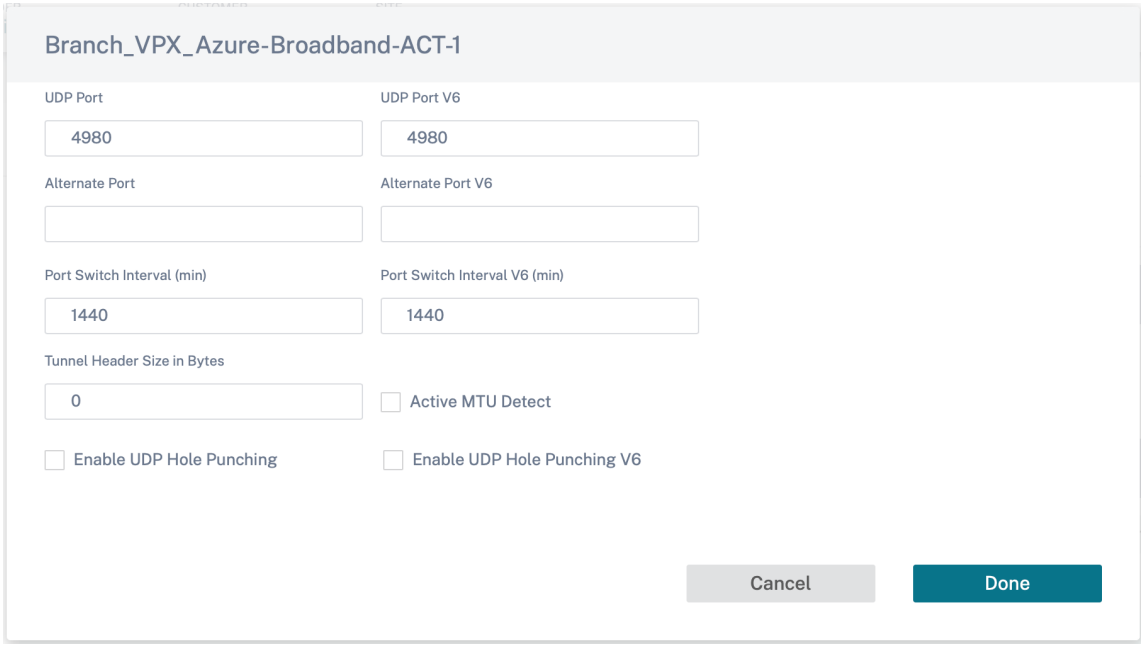
 




Se muestran los detalles del enlace WAN para las rutas de miembro activo seleccionadas, puede cambiar la configuración según sea necesario. La configuración del **puerto UDP** se puede configurar tanto para IPv4 como para IPv6.

- **Puerto UDP**: El puerto utilizado para la transferencia de paquetes de LAN a WAN y de WAN a LAN. También puede especificar.
- **Puerto alternativo: El puerto**UDP alternativo que se utilizará cuando se habilite la conmutación de puertos UDP.
- **Intervalo de conmutación de puerto**: El intervalo, en minutos, en el que el enlace WAN alterna su puerto UDP.
- **Tamaño del encabezado del túnel en bytes**: El tamaño del encabezado del túnel, en bytes, si corresponde.
- **Detección activa de MTU**: L as rutas de LAN a WAN para las rutas virtuales dinámicas se sondean activamente para detectar MTU.
- **Habilite la perforación de agujeros de UDP**: El MCN ayuda a la conectividad UDP entre sitios de clientes compatibles protegidos por NAT.



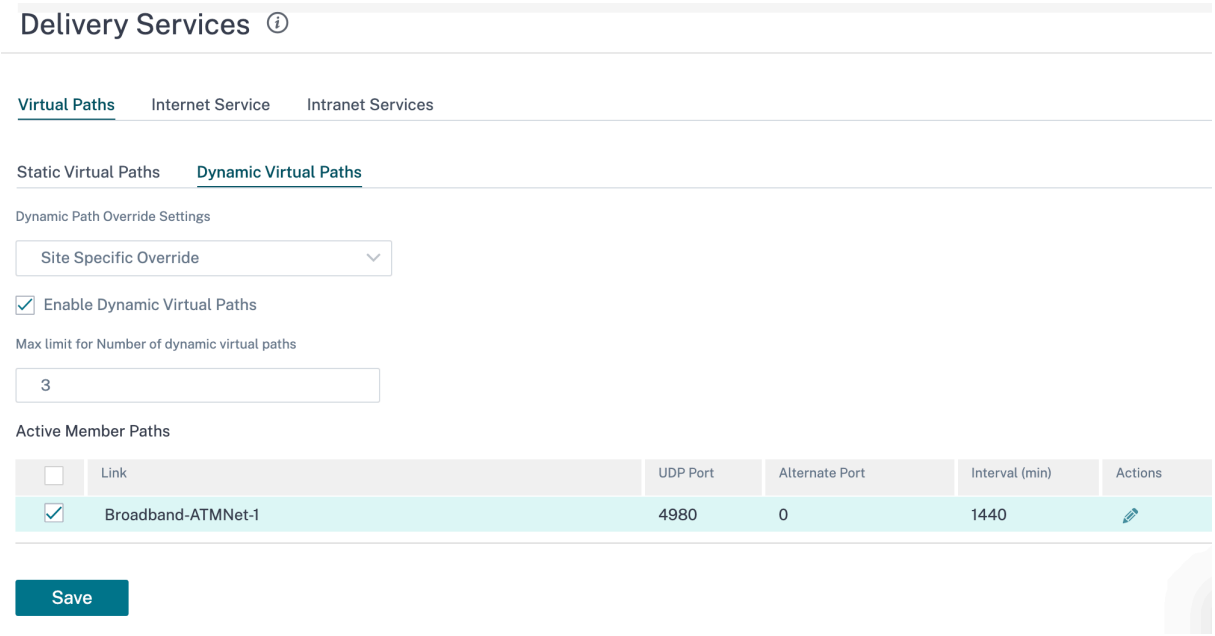

## Rutas virtuales dinámicas

Con la demanda de VoIP y videoconferencias, el tráfico entre oficinas ha aumentado. Configurar conexiones de malla completas a través de centros de datos requiere mucho tiempo e ineficiente. Con Citrix SD-WAN, puede crear automáticamente rutas entre oficinas bajo demanda mediante la función Ruta virtual dinámica. La sesión utiliza inicialmente una ruta fija existente. A medida que se cumplen el umbral de ancho de banda y tiempo, se crea una nueva ruta de acceso dinámicamente si esa nueva ruta tiene mejores funciones de rendimiento que la ruta fija. El tráfico de sesión se transmite a través de la nueva ruta, lo que resulta en un uso eficiente de los recursos. Las rutas virtuales dinámicas solo existen cuando son necesarias y reducen la cantidad de tráfico transmitido desde y hacia el centro de datos.

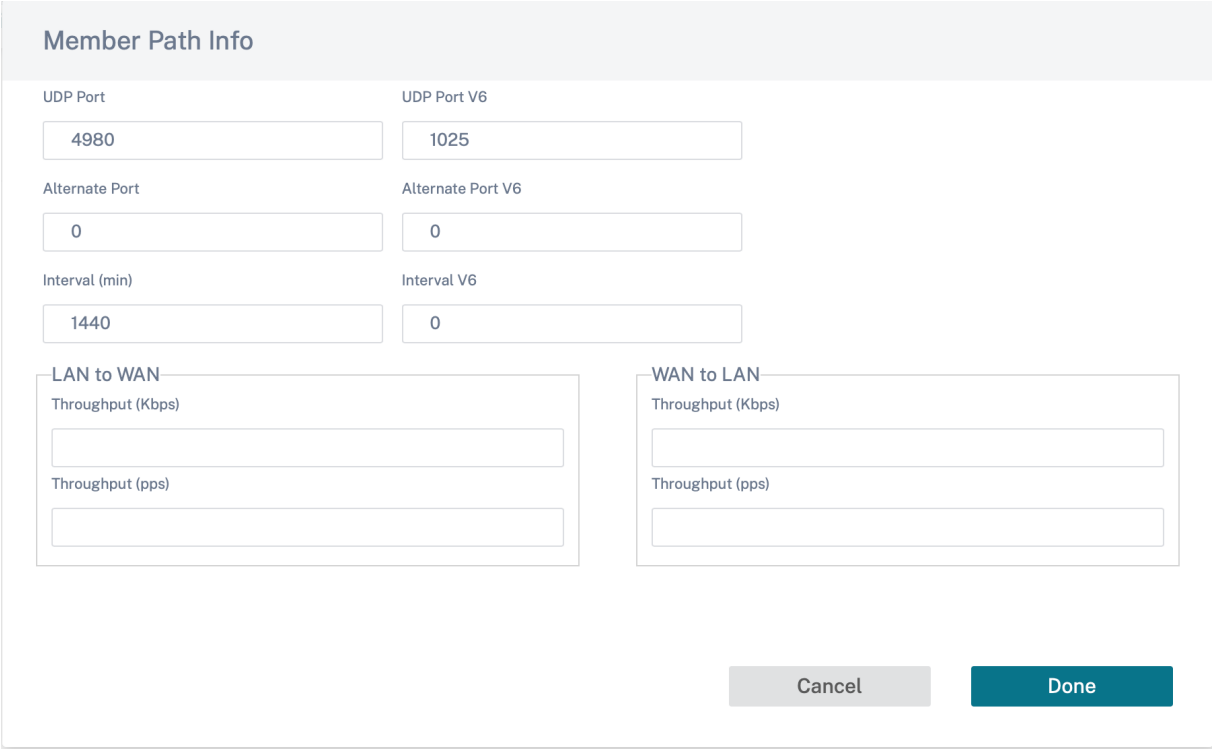
Para configurar rutas virtuales dinámicas, desde el nivel del sitio, vaya a **Configuración > Configuración** > **Configuración avanzada** > **Rutas virtuales** > **Rutas virtuales dinámicas**.

Seleccione **Anular los valores predeterminados globales** para anular la configuración de la ruta virtual heredada de la configuración de ruta automática del enlace WAN global. Seleccione **Habilitar rutas virtuales dinámicas** para permitir rutas virtuales dinámicas entre este sitio y otros sitios conectados a través de un nodo intermedio. Establezca las rutas virtuales dinámicas máximas permitidas para el sitio.




Establezca el puerto UDP y el umbral de ruta virtual dinámica. Especifique el umbral de rendimiento, en kbps o paquetes por segundo, en el sitio intermedio en el que se activan las rutas virtuales dinámicas en LAN a WAN o WAN a LAN.



# Redirección dinámica

October 31, 2022

Después de la configuración e implementación de los dispositivos SD-WAN en la red y una vez establecidas las conexiones, es importante asegurarse de que el tráfico se redirige correctamente a través de la red SD-WAN superpuesta. Puede comprobar la redirección del tráfico mediante herramientas de diagnóstico ping y traceroute. Si las pruebas de ping y traceroute indican que la conectividad se establece a través de las rutas de calco subyacente, la redirección del tráfico se puede lograr utilizando los siguientes protocolos de redirección dinámica.

- **Open Shortest Path First (OSPF)**: Es un protocolo de puerta de enlace interior que se utiliza para redirigir el tráfico dentro de un sistema autónomo, como la red empresarial. OSPF utiliza un algoritmo de enrutamiento de estado de enlace para detectar cambios en la topología de la red y redirigir los paquetes calculando primero la ruta más corta para cada ruta. Utilice este protocolo para redirigir el tráfico MPLS. Para obtener más información, consulte la sección **OSPF**.
- **Border Gateway Protocol (BGP)**: Es un protocolo de puerta de enlace exterior diseñado para redirigir la información de enrutamiento y accesibilidad del tráfico entre los diferentes sistemas autónomos de Internet. Es capaz de tomar decisiones de redirección basadas en rutas determinadas por los ISP. Utilice este protocolo para redirigir el tráfico de Internet. Para obtener más información, consulte la sección **Configurar BGP**.

Anteriormente, la capacidad de enrutamiento dinámico solo estaba disponible para un único ID de router. Pudo configurar un ID de router único de forma global para todos los dominios de enrutamiento configurados (uno para OSPF y BGP) o no proporcionar ningún ID de router. A partir de la versión 11.3.1 de Citrix SD-WAN, no solo puede configurar un ID de enrutador para todo el protocolo, sino también configurar un ID de enrutador para cada dominio de redirección. Con esta mejora, puede habilitar la redirección dinámica estable en varias instancias con diferentes ID de enrutador convergiendo de manera estable.

Si configura un ID de enrutador para un dominio de redirección específico, el ID de enrutador específico anula el dominio de redirección de nivel de protocolo.

## OSPF

Para configurar OSFF, vaya a **Configuración > Configuración > Configuración avanzada > Enrutamiento dinámico > OSPF**.

### Configuración básica de OSPF

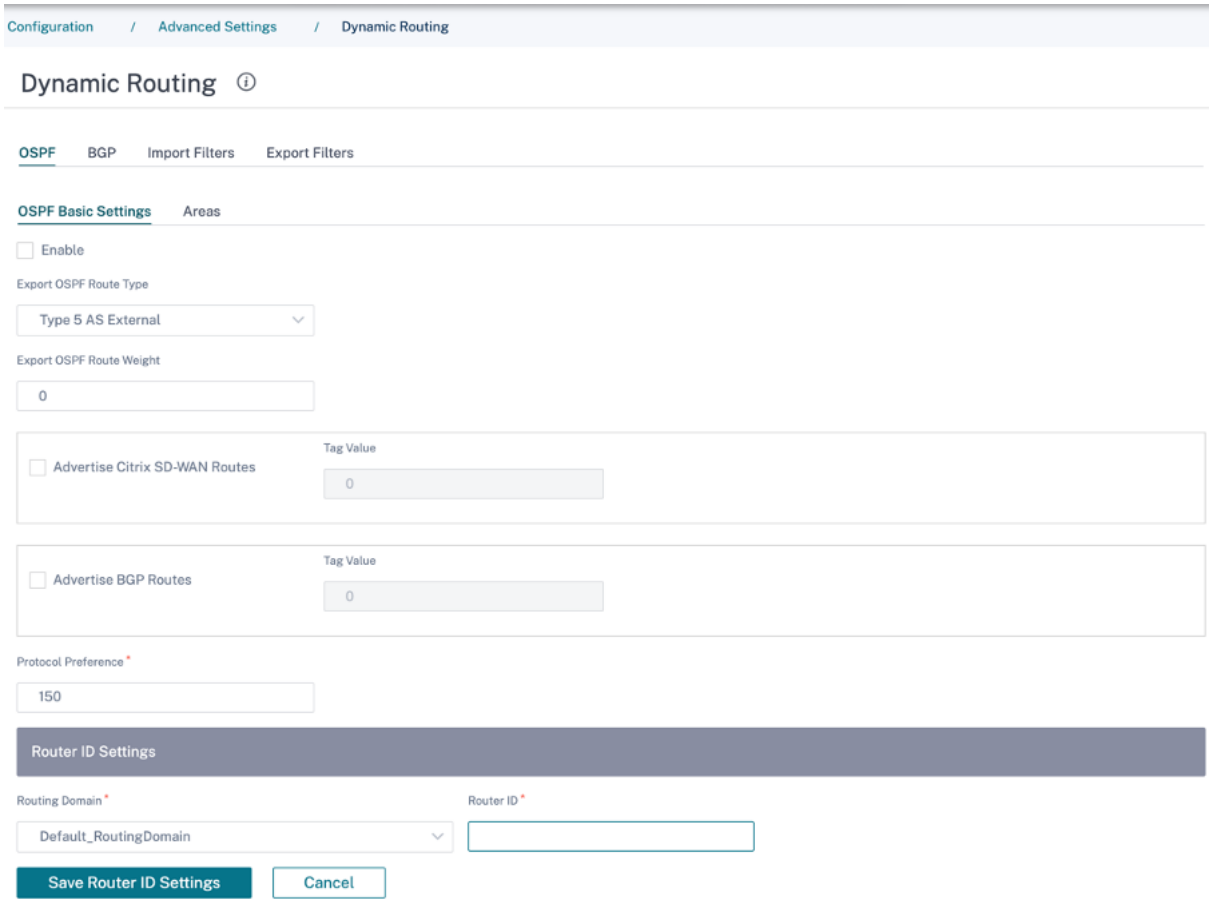
Estos son los parámetros a configurar:

- **Habilitar**: Permita que el protocolo de enrutamiento OSPF del dispositivo SD-WAN comience a intercambiar paquetes de saludo entre los enrutadores vecinos.
- **ID del router**: La dirección IPv4 que se utiliza para las publicaciones de OSPF. Este campo es opcional. Si no se especifica, se elige la dirección IPv4 virtual más baja de las interfaces virtuales que participan en el enrutamiento. Para la interfaz IPv6, es obligatorio especificar el ID del router en formato IPv4. Por ejemplo, 1.1.1.1.

  > **Nota**
  >
  > - La configuración del ID del router es opcional para una red IPv4. Sin embargo, para una red IPv6, la configuración del ID del router es obligatoria. El ID del router de una red IPv6 debe configurarse en el mismo formato IPv4 (notación de 32 bits).
  >
  >   * Debe crear enlaces IPv4 e IPv6 separados al mismo enrutador (si corresponde) para el aprendizaje y la publicidad.

- **Tipo de ruta OSPF de exportación**: Anuncie la ruta SD-WAN a los vecinos de OSPF como ruta intraárea de tipo 1 o ruta externa de tipo 5.
- **Peso de ruta OSPF de exportación**: E l coste que se anuncia a los vecinos de OSPF es el coste de la ruta original y el peso configurado aquí.
- **Anunciar rutas SD-WAN**: Para anunciar rutas SD-WAN a los elementos de la red homóloga.
- **Anunciar rutas BGP**: Para permitir la redistribución de las rutas BGP en el dominio OSPF.

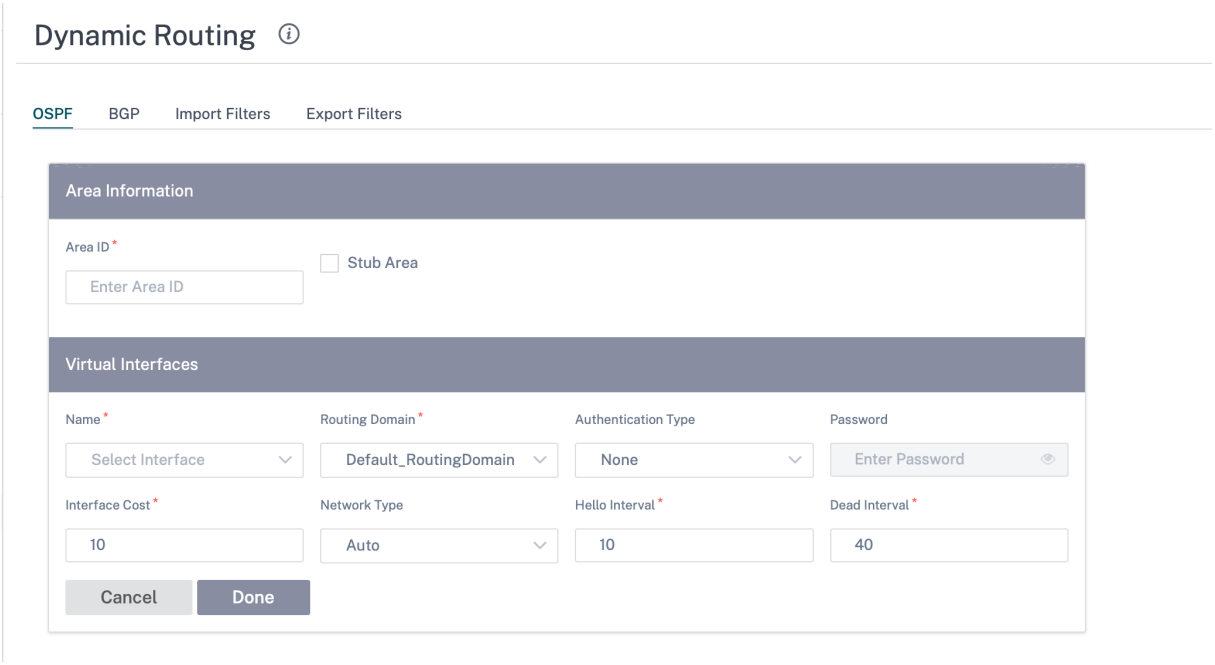
 




### Áreas

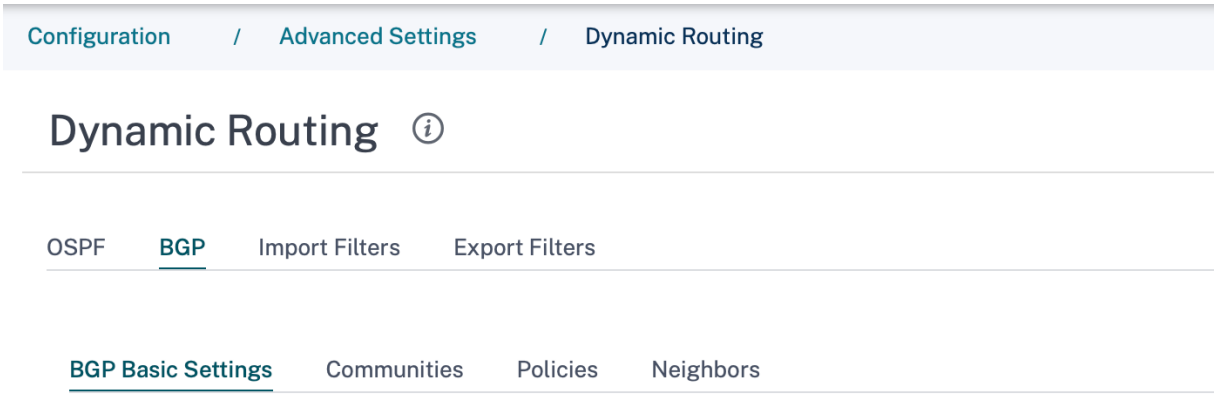
Haga clic en **+ Área** y proporcione el ID de área de la red desde la que OSPF conocerá las rutas y las anunciará. El área auxiliar garantiza que esta área no recibirá anuncios de rutas desde fuera del Sistema Autónomo designado. Configure la configuración de la interfaz virtual.




### BGP

Para configurar BGP, vaya a **Configuración > Configuración > Configuración avanzada > Enrutamiento dinámico > BGP**.




#### Configuración básica de BGP

Los parámetros que deben configurarse son los siguientes:

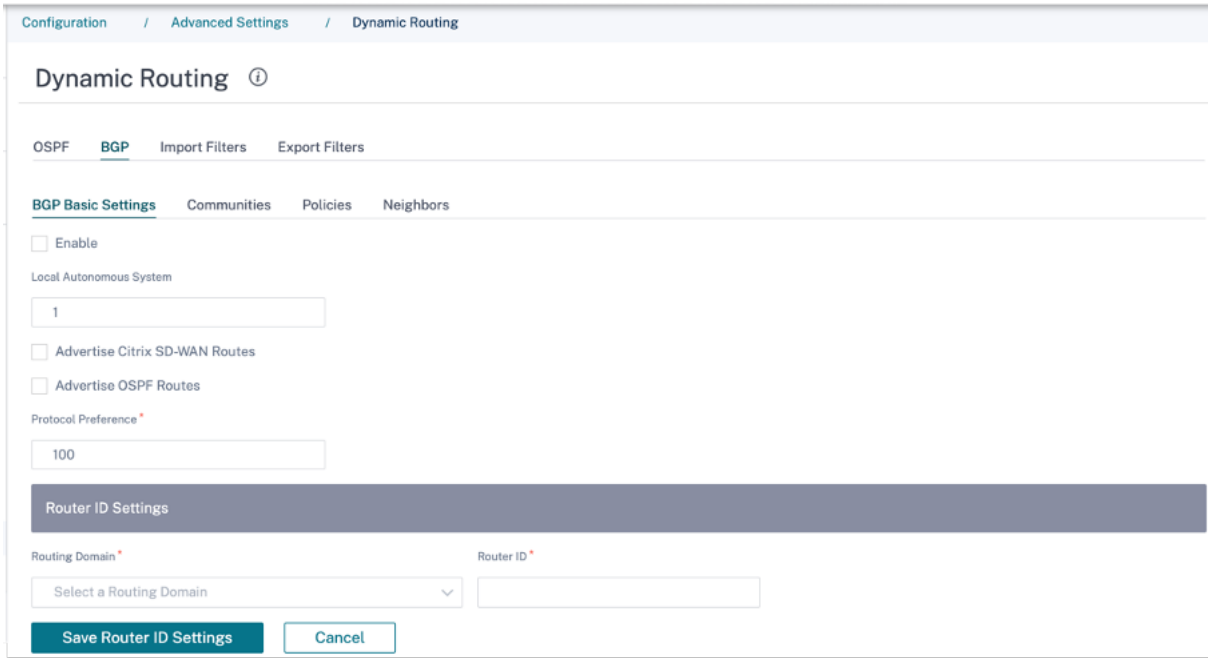
- **Habilitar**: Permita que el protocolo de enrutamiento BGP del dispositivo SD-WAN comience a enviar un mensaje abierto como parte de la interconexión de BGP.
- **ID del router**: La dirección IPv4 que se utiliza para las publicaciones de BGP. Si no se especifica el ID del router, se elige la dirección IPv4 virtual más baja de las interfaces virtuales que

participan en el enrutamiento.

> **Nota**
>
> - La configuración del ID del router es opcional para una red IPv4. Sin embargo, para una red IPv6, la configuración del ID del router es obligatoria. El ID del router de una red IPv6 debe configurarse en el mismo formato IPv4 (notación de 32 bits).
>
>  * Debe crear enlaces IPv4 e IPv6 separados al mismo enrutador (si corresponde) para el aprendizaje y la publicidad.

- **Sistema autónomo local**: Número de sistema autónomo en el que se ejecuta el protocolo BGP.
- **Anunciar rutas SD-WAN**: Para anunciar rutas SD-WAN a los elementos de la red homóloga.
- **Anunciar rutas OSPF**: Para permitir la redistribución de las rutas OSPF en el dominio BGP.



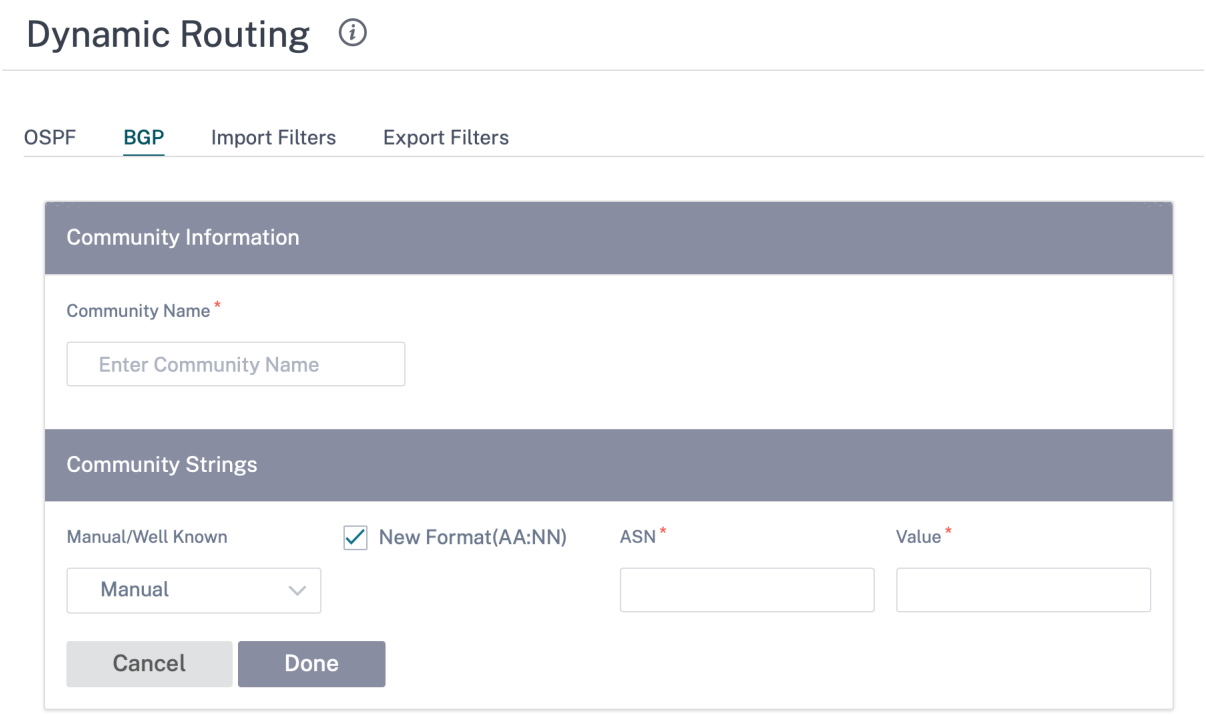

### Comunidades

Haga clic en **+ Comunidad** para agregar una comunidad. Colección de comunidades BGP que se pueden utilizar para el filtrado de rutas. La lista de comunidades también se puede utilizar para establecer o modificar las comunidades de una ruta coincidente.

Para cada directiva, los usuarios pueden configurar varias cadenas de comunidad, el atributo AS-PATH-PREPEND y **MED**. Los usuarios pueden configurar hasta 10 atributos para cada directiva.

Especifique el nombre de la comunidad e introduzca una cadena de comunidad que se anunciará.

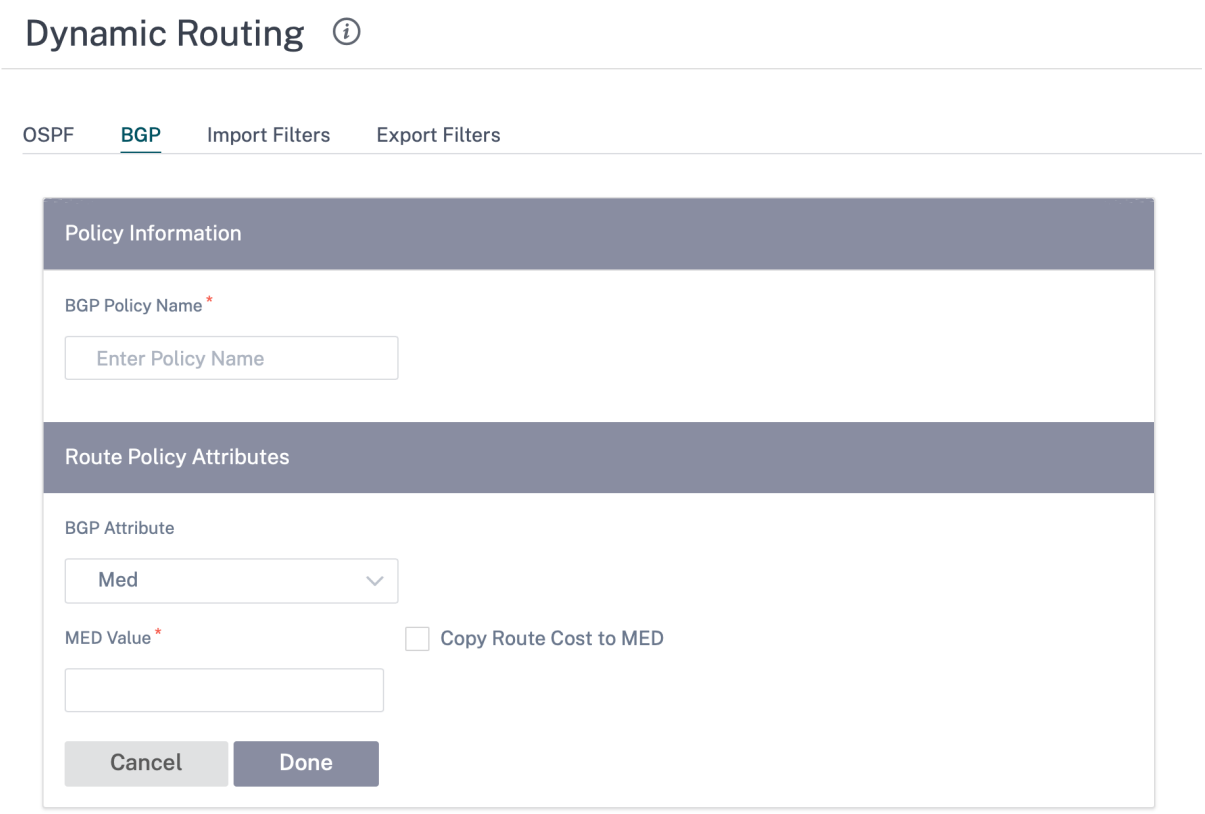



- **Nombre de la comunidad**: introduzca un nombre de comunidad.
- **Manual/Conocido**: Configure la comunidad BGP manualmente o seleccione una comunidad BGP estándar conocida de la lista.
- **Nuevo formato (AA:NN)**: Seleccione la casilla de verificación para usar el nuevo formato para configurar la comunidad BGP.
- **ASN**: Los primeros 16 dígitos de la comunidad BGP cuando se utiliza el nuevo formato de configuración.
- **Valor**: introduzca el valor de la comunidad de BGP.

### Directivas

Una colección de atributos BGP que se puede utilizar para establecer o modificar atributos de ruta para cada par BGP. Cree directivas BGP para que se apliquen selectivamente a un conjunto de redes por vecino, en cualquier dirección (importación o exportación). Un dispositivo SD-WAN admite ocho directivas por sitio, con hasta ocho objetos de red (u ocho redes) asociados a una directiva.



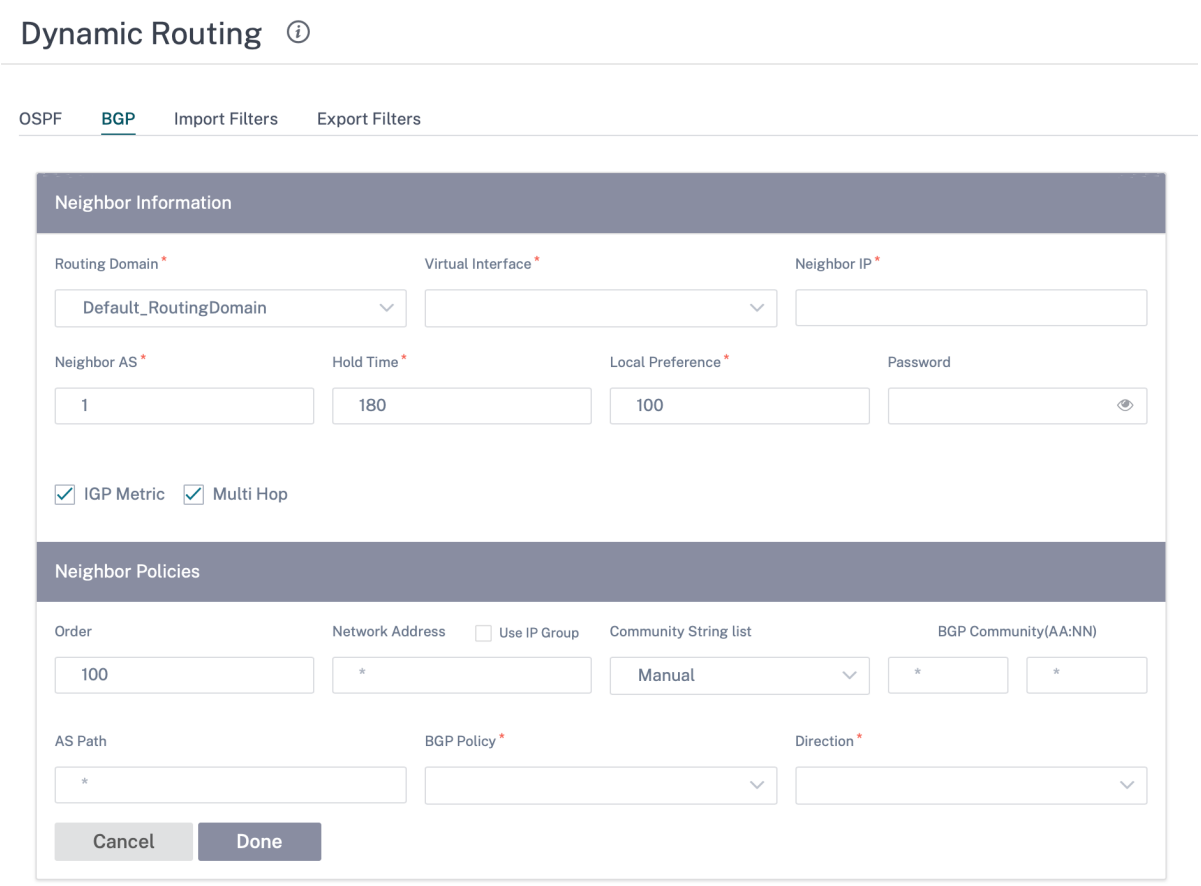

- **Nombre de la directiva de BGP**: Introduzca el nombre de la directiva de BGP.
- **Atributos de BGP**: Seleccione los atributos de BGP de la lista y proporcione la información necesaria.

### Vecinos

Los vecinos son todos los enrutadores de pares BGP configurados que se comprueban para encontrar las rutas más cortas para la redirección. Todos los vecinos deben formar parte del mismo Sistema Autónomo.

Haga clic en **+ Vecino** para agregar una directiva de BGP configurada para los enrutadores vecinos. Puede especificar la dirección para indicar si esta directiva se aplica a las rutas entrantes o salientes.




## Filtrado de rutas

Para las redes con el aprendizaje de rutas habilitado, Citrix SD-WAN Orchestrator proporciona más control sobre qué rutas SD-WAN se anuncian a los vecinos de enrutamiento y qué rutas se reciben de los vecinos de enrutamiento, en lugar de anunciar y aceptar todas o ninguna ruta.

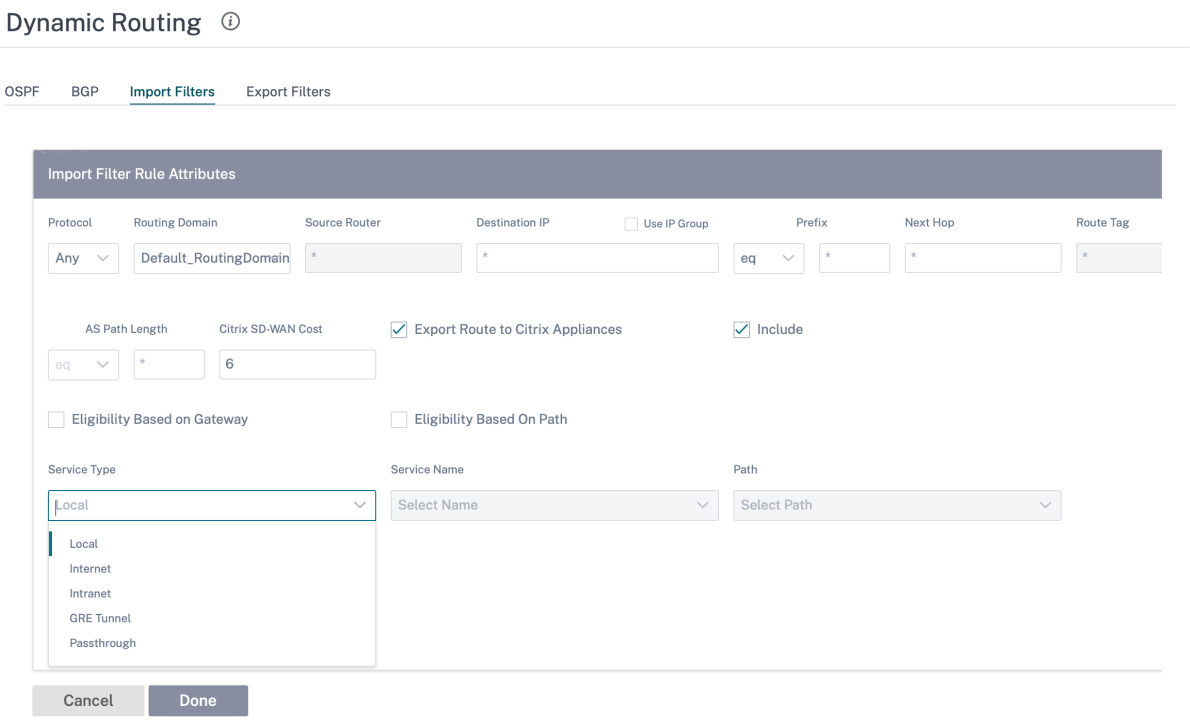
### Filtros de importación

Los filtros de importación se utilizan para aceptar o no las rutas que se reciben mediante vecinos OSPF y BGP basados en criterios de coincidencia específicos. Las reglas de filtrado de importación son las reglas que deben cumplirse antes de importar rutas dinámicas a la base de datos de rutas SD-WAN. Por defecto, no se importan rutas.

Puede configurar Filtros para ajustar la forma en que se lleva a cabo el aprendizaje de rutas.

Haga clic en **+ Importar regla**.




Utilice los siguientes criterios para crear cada filtro de exportación que quiera crear.

| Criteria de campo | Descripción | Valor |
|---|---|---|
| Protocolo | El protocolo de enrutamiento mediante el cual se aprende una ruta. Seleccione el protocolo en la lista desplegable. | Cualquiera, OSPF, BGP |
| Dominio de redirección | Introduzca el dominio de enrutamiento en la lista desplegable. | • Nombre de dominio de enrutamiento |
| Enrutador fuente | La dirección IP del enrutador de origen, es aplicable solo para iBGP | • Dirección IP |
| IP de destino | La dirección IP y la máscara de subred del destino de una ruta | • Dirección IP |
| Utilice IP Group | Seleccione la casilla **Usar grupo IP** según sea necesario. | • Grupo IP |

| Criteria de campo | Descripción | Valor |
| --- | --- | --- |
| Prefijo | Para hacer coincidir las rutas por prefijo, elija un predicado de cruce en el menú e introduzca un prefijo Ruta en el campo adyacente | • eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to |
| Siguiente salto | La dirección IP del siguiente salto | • Dirección IP |
| Etiqueta de ruta | La etiqueta Ruta OSPF con la que coincide el filtro. Las etiquetas de ruta OSPF evitan los bucles de redirección durante la redistribución mutua entre OSPF y otros protocolos | Valor numérico |
| Coste | El coste de ruta utilizado para hacer coincidir las rutas OSPF para la importación | Valor numérico |
| Longitud de ruta AS | Longitud de ruta AS utilizada para hacer coincidir las rutas BGP para la importación | Valor numérico |
| Exportar ruta a dispositivos Citrix | Seleccione la casilla de verificación para habilitar este filtro. De lo contrario, el filtro se ignora | Nada |
| Incluir | Seleccione la casilla de verificación Incluir rutas que coincidan con este filtro. De lo contrario, las rutas coincidentes se ignoran | Nada |
| Elegibilidad basada en Gateway | Seleccione esta casilla de verificación y proporcione el **tipo de servicio**, el **nombre del servicio** y la **ruta** en la lista desplegable. | Tipo de servicio (local, Internet, intranet, túnel GRE, acceso directo), nombre del servicio y ruta |

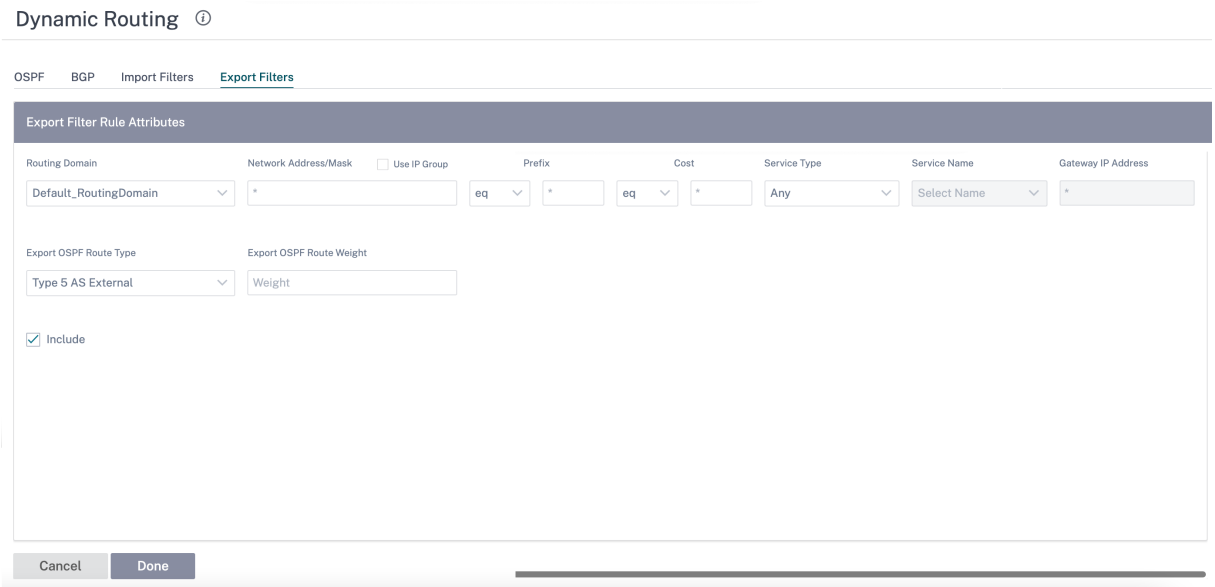
| Criteria de campo | Descripción | Valor |
|---|---|---|
| Elegibilidad basada en la ruta | Seleccione esta casilla de verificación y proporcione el **tipo de servicio**, el **nombre del servicio** y la **ruta** en la lista desplegable. | Tipo de servicio (local, Internet, intranet, túnel GRE, acceso directo), nombre del servicio y ruta |

Haga clic en **Listo** para guardar la configuración.

### Filtros de exportación

Los filtros de exportación se utilizan para incluir o excluir rutas para anuncios mediante protocolos OSPF y BGP basados en coincidencias específicas criterios. Las reglas de filtro de exportación son las reglas que deben cumplirse al anunciar rutas SD-WAN a través de protocolos de enrutamiento dinámico. Todas las rutas se anuncian a los pares de forma predeterminada.

Haga clic en **+ Exportar regla**.




Utilice los siguientes criterios para crear cada filtro de exportación que quiera crear.

| Criteria de campo | Descripción | Valor |
|---|---|---|
| Dominio de redirección | Seleccione el dominio de enrutamiento en la lista desplegable. | Dominio de redirección |

| Criteria de campo | Descripción | Valor |
| --- | --- | --- |
| Dirección o máscara de red | Introduzca la **dirección IP** y la máscara de subred del objeto de red configurado que describe la red de la ruta | • Dirección IP |
| Utilice IP Group | Seleccione la casilla de verificación si es necesario e introduzca el grupo IP en la lista desplegable. | • Grupo IP |
| Prefijo | Para hacer coincidir las rutas por prefijo, elija un predicado de cruce en el menú e introduzca un prefijo Ruta en el campo adyacente | • eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to |
| Coste | El método (predicado) y el coste de ruta de SD-WAN que se utilizan para limitar la selección de rutas exportadas | Valor numérico |
| Tipo de servicio | Seleccione los tipos de servicio asignados a rutas coincidentes de una lista de servicios Citrix SD-WAN | Cualquiera, Local, Ruta virtual, Internet, Intranet, Túnel GRE LAN, Túnel IPsec LAN |
| Nombre del sitio/servicio | Para Intranet, Túnel GRE LAN y Túnel IPsec de LAN, especifique el nombre del tipo de servicio configurado que se va a utilizar | Cadena de texto |
| Dirección IP de la puerta de enlace | Si elige Túnel GRE de LAN como tipo de servicio, introduzca la IP de la puerta de enlace para el túnel | Dirección IP |
| Exportar tipo de ruta OSPF | Publique la ruta Citrix SD-WAN a los vecinos de OSPF como ruta intraárea de tipo 1 o ruta externa de tipo 5. La ruta predeterminada siempre se anuncia como ruta externa de tipo 5 a áreas normales y ruta resumida de tipo 3 a áreas de acceso directo. | Tipo de ruta |

| Criteria de campo | Descripción | Valor |
| --- | --- | --- |
| Peso de ruta OSPF de exportación | Al exportar rutas de Citrix SD-WAN a OSPF, y el peso del coste de Citrix SD-WAN de cada ruta como coste total. | Peso |
| Incluir | Seleccione la casilla de verificación Incluir rutas que coincidan con este filtro. De lo contrario, las rutas coincidentes se ignoran | Nada |

El filtrado de rutas se implementa en rutas LAN y rutas de ruta virtual en una red SD-WAN (centro de datos/sucursal) y se anuncia a una red que no es SD-WAN mediante el uso de BGP y OSPF.

Puede configurar hasta 512 filtros de exportación y 512 filtros de importación. Este es el límite general, no por límite de dominio de redirección.

## Traducción de direcciones de red

October 31, 2022

La traducción de direcciones de red (NAT) del dispositivo SD-WAN realiza la conservación de direcciones IP para preservar el número limitado de direcciones IP registradas. Traduce las direcciones privadas de la red interna a una dirección pública legal y conecta su red SD-WAN privada con la Internet pública. La dirección IP pública se utiliza para la comunicación a través de Internet. NAT también garantiza una seguridad adicional mediante la publicidad de una sola dirección para toda la red a Internet, ocultando toda la red interna.

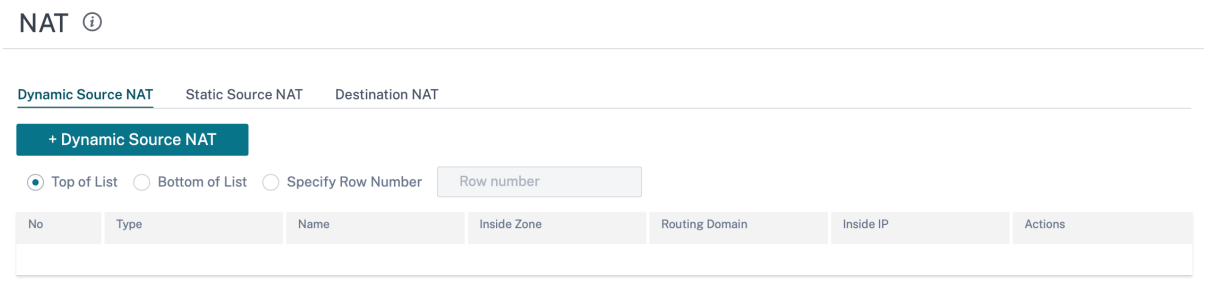
Puede configurar los siguientes tipos de NAT:

- NAT de origen dinámico
- NAT estático
- NAT de destino

> **Nota**
>
> La capacidad de NAT solo se puede configurar al nivel de sitio. No hay configuración global (plantillas) para NAT.

Para configurar NAT para un sitio mediante el servicio Citrix SD-WAN Orchestrator, desde el nivel del sitio, vaya a **Configuración > Configuración > Configuración avanzada > NAT**.




## NAT entrante y saliente

La dirección de una conexión puede ser de interior a exterior o de exterior a interior. Cuando se crea una regla NAT, puede definir la dirección mediante la casilla **de verificación Al recibir**. Cuando se selecciona la casilla de verificación, la dirección se configura como **Entrante** y, cuando la casilla de verificación está desactivada, la dirección se configura como **Salida**.

- **Entrante**: La dirección de origen se traduce para los paquetes recibidos en el servicio. La dirección de destino se traduce para los paquetes transmitidos en el servicio. Por ejemplo, servicio de Internet a servicio LAN: Para los paquetes recibidos (de Internet a LAN), la dirección IP de origen se traduce. Para los paquetes transmitidos (LAN a Internet), la dirección IP de destino se traduce.
- **Saliente**: La dirección de destino se traduce para los paquetes recibidos en el servicio. La dirección de origen se traduce para los paquetes transmitidos en el servicio. Por ejemplo, servicio LAN a servicio de Internet —para paquetes transmitidos (LAN a Internet) la dirección IP de origen se traduce. Para los paquetes recibidos (de Internet a LAN) se traduce la dirección IP de destino.

## Derivación de Zona

Las zonas de firewall de origen y destino para el tráfico entrante y saliente no deben ser las mismas. Si las zonas de firewall de origen y destino son las mismas, NAT no se realiza en el tráfico.

Para NAT saliente, la zona exterior se deriva automáticamente del servicio. Todos los servicios de SD-WAN están asociados a una zona de forma predeterminada. Por ejemplo, el servicio de Internet en un vínculo de Internet de confianza está asociado a la zona de Internet de confianza. Del mismo modo, para un NAT entrante, la zona interior se deriva del servicio.

Para un servicio de ruta virtual, la derivación de zona NAT no ocurre automáticamente, debe introducir manualmente la zona interior y externa. NAT se realiza únicamente en el tráfico que pertenece a estas zonas. No se pueden derivar zonas para rutas virtuales porque puede haber varias zonas dentro de las subredes de rutas virtuales.

### NAT de origen dinámico

La**NAT de origen dinámico** es una asignación de varias direcciones IP privadas o subredes dentro de la red SD-WAN a una dirección IP pública o subred fuera de la red SD-WAN. Permite que varios hosts traduzcan sus direcciones IP de origen a la misma dirección IP pública con diferentes números de puerto. NAT con restricción de puerto utiliza el mismo puerto externo para todas las traducciones relacionadas con una dirección IP interna y un par de puertos. El tráfico de diferentes zonas y subredes a través de direcciones IP de confianza (internas) en el segmento LAN se envía a través de una única dirección IP pública (externa).

> **Nota**
>
> Las traducciones de NAT dinámicas permiten todo el tráfico recíproco de una sesión iniciada desde la red interna. Para filtrar estas conexiones, agregue directivas de filtro para el tráfico saliente.

#### Traducción de direcciones de puertos

NAT dinámico realiza la traducción de direcciones de puerto (PAT) junto con la traducción de direcciones IP. Los números de puerto se utilizan para distinguir qué tráfico pertenece a qué dirección IP. Se utiliza una sola dirección IP pública para todas las direcciones IP privadas internas, pero se asigna un número de puerto diferente a cada dirección IP privada. PAT es una forma rentable de permitir que varios hosts se conecten a Internet mediante una única dirección IP pública.

La casilla de verificación **Simétrica** define la configuración de PAT. Al configurar las reglas de NAT, si se selecciona la casilla de verificación, se configura la NAT simétrica y, cuando se desactiva, la NAT restringida de puertos se configura en el back-end.

- **Puerto restringido**: Puerto Restringido NAT utiliza el mismo puerto externo para todas las traducciones relacionadas con un par de direcciones IP internas y puertos. Este modo se utiliza normalmente para permitir aplicaciones P2P de Internet.
- **Simétrico**: NAT simétrico utiliza el mismo puerto externo para todas las traducciones relacionadas con una tupla Dirección IP interna, Puerto interior, Dirección IP exterior y Puerto exterior. Este modo se utiliza normalmente para mejorar la seguridad o ampliar el número máximo de sesiones NAT.

#### Reenvío de puertos

La NAT dinámica con reenvío de puertos permite que el tráfico de una red externa acceda a hosts y puertos específicos de la red interna sin que la sesión se inicie desde dentro. Esto se usa normalmente para hosts internos como servidores web.

Una vez configurada la NAT dinámica, puede definir las directivas de reenvío de puertos. Configure NAT dinámico para la traducción de direcciones IP y defina la directiva de reenvío de puertos para asignar un puerto externo a un puerto interno. El reenvío dinámico de puertos NAT se suele utilizar para permitir que los hosts remotos se conecten a un host o servidor de la red privada.

#### Configurar NAT de origen dinámico

Para configurar la NAT dinámica para un sitio mediante el servicio Citrix SD-WAN Orchestrator, desde el nivel del sitio, vaya a **Configuración > Configuración > Configuración avanzada > NAT > NAT de origen dinámico**. Haga clic en **+ Fuente dinámica NAT**.

- **Tipo**: Los tipos de servicio de SD-WAN a los que se aplica la directiva de NAT. Para la NAT estática, los tipos de servicio admitidos son los servicios locales, de rutas virtuales, de Internet, de intranet y de dominio de enrutamiento intermedio.
- **Dominio de enrutamiento**: Seleccione el dominio de enrutamiento al que se aplica la traducción seleccionada.
- **Tipo de dirección IP**: Seleccione el tipo de dirección IPv4 o IPv6 según sus preferencias.
- **Servicio de destino**: Proporcione un nombre para el servicio que corresponda al tipo de servicio.
- **Zona interior**: El tipo de coincidencia de la zona del firewall interior del que debe ser el paquete para permitir la traducción.
- **IP/prefijo interno**: La dirección IP interna y el prefijo a los que se debe traducir si se cumplen los criterios de coincidencia.
- **IP externa**: La dirección IP externa y el prefijo a los que se traduce la dirección IP interna si se cumplen los criterios de coincidencia. Para el tráfico saliente que utiliza servicios de Internet e Intranet, la dirección IP del vínculo WAN configurada se elige dinámicamente como la dirección IP externa.
- **Paridad de puertos**: Si está habilitado, los puertos externos para las conexiones NAT mantienen la paridad (incluso si el puerto interior es par, impar si el puerto exterior es impar).
- **Enlazar ruta de respondedor**: Garantiza que el tráfico de respuesta se envíe a través del mismo servicio en el que se recibe, para evitar la redirección asimétrica.
- **Permitir relacionado**: P ermite que el tráfico relacionado con el flujo coincida con la regla. Por ejemplo, la redirección ICMP relacionada con el flujo específico que coincide con la directiva, si hubo algún tipo de error relacionado con el flujo.
- **Acceso directo a IPSec**: Permite traducir una sesión de IPSec (AH/ESP).
- Acceso directo de**GRE/PPTP: garantiza que el tráfico de respuesta se envíe a través**del mismo servicio en el que se recibe, para evitar el enrutamiento asimétrico.
- **Al recibir**: Cuando se selecciona esta casilla de verificación, se configura la NAT de entrada. Cuando se desactiva, se configura la NAT de salida.

- **Simétrico**: Cuando se selecciona esta casilla, se configura la NAT simétrica. Cuando está desactivada, se configura la NAT restringida de puertos

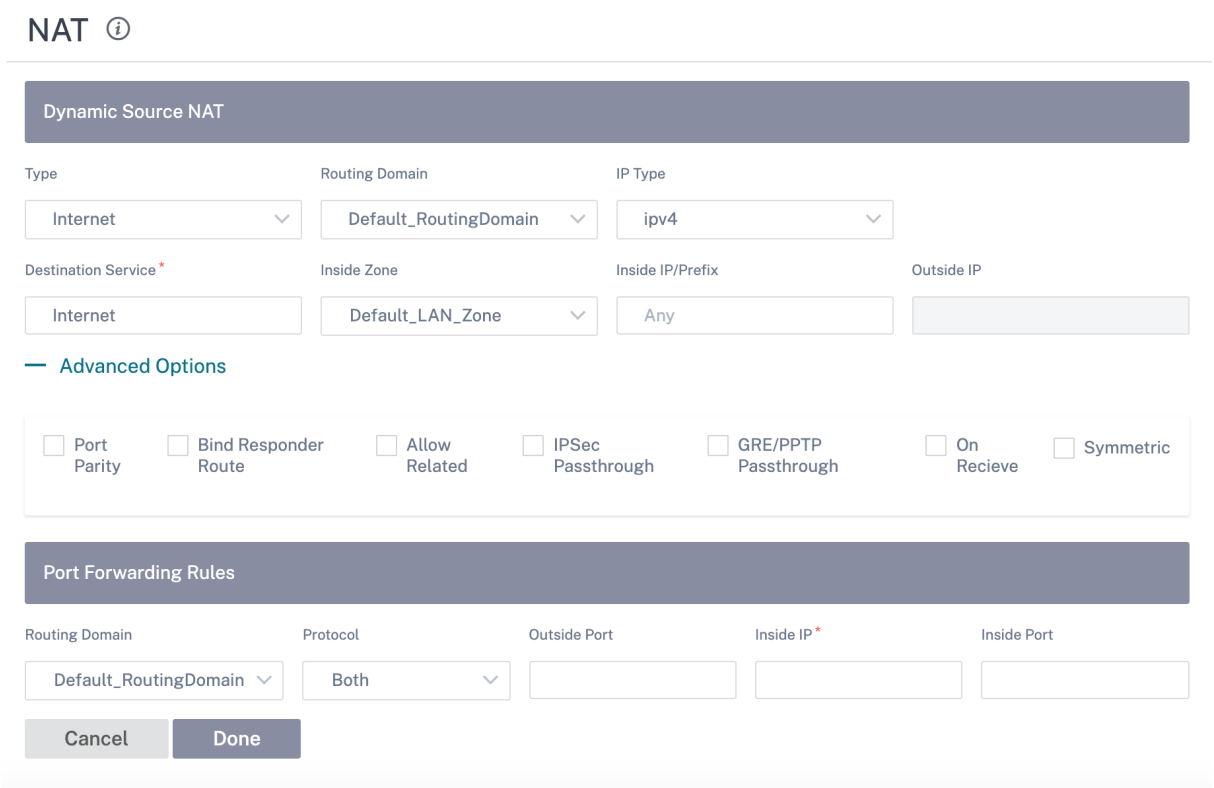
Reglas de reenvío de puertos:

- **Dominio de enrutamiento**: Seleccione el dominio de enrutamiento al que se aplica la traducción seleccionada.
- **Protocolo**: TCP, UDP o ambos.
- **Puerto exterior**: El puerto exterior que es el puerto de reenvío hacia el puerto interior.
- **IP interna**: La dirección interna para reenviar los paquetes coincidentes.
- **Puerto interior**: El puerto interior al que se reenviará el puerto exterior.

Cada regla de reenvío de puertos tiene una regla NAT principal. La dirección IP externa se toma de la regla NAT principal.

> **Nota**
>
> La interfaz de usuario del servicio Citrix SD-WAN Orchestrator muestra las reglas NAT creadas automáticamente cuando se cumplen las siguientes condiciones:
>
> - El servicio de Internet está activado en el sitio.
> - La regla NAT de fuente dinámica de Internet de salida IPv4 no está configurada en el sitio.
> - Al menos 1 enlace WAN está en una interfaz que no es de confianza o Internet está habilitada en todos los dominios de enrutamiento.




## NAT de origen estático

NAT estático es una asignación uno a uno de una dirección IP privada o subred dentro de la red SD-WAN a una dirección IP pública o subred fuera de la red SD-WAN. Configure NAT estático introduciendo manualmente la dirección IP interna y la dirección IP externa a la que debe traducir. Puede configurar NAT estático para los servicios de dominio local, rutas virtuales, Internet, Intranet y interredirección.

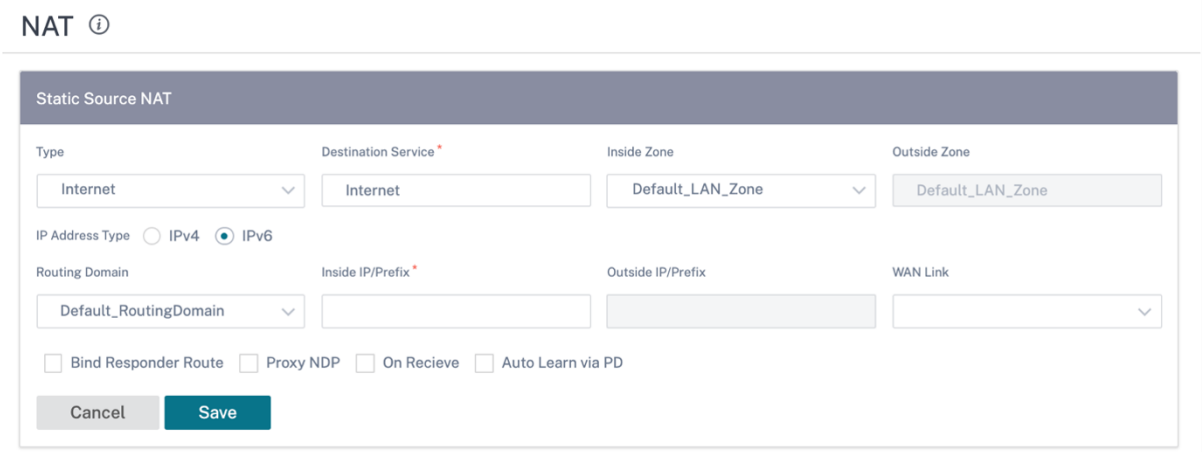
### Configurar NAT de origen estático

Para configurar la NAT estática para un sitio mediante el servicio Citrix SD-WAN Orchestrator, desde el nivel del sitio, vaya a **Configuración > Configuración > Configuración avanzada > NAT > NAT de fuente estática**. Haga clic en **+ Fuente estática NAT**.

- **Tipo**: Los tipos de servicio de SD-WAN a los que se aplica la directiva de NAT. Para NAT estático, los tipos de servicio admitidos son Local, Rutas virtuales, Internet, Intranet y servicios de dominio de interredirección
- **Servicio de destino**: Proporcione un nombre para el servicio que corresponda al tipo de servicio.

- **Zona interior**: El tipo de coincidencia de la zona del firewall interior del que debe ser el paquete para permitir la traducción.
- **Zona exterior**: Tipo de coincidencia de zona de firewall exterior del que debe ser el paquete para permitir la traducción.
- **Tipo de dirección IP**: Seleccione el tipo de dirección IPv4 o IPv6 según sus preferencias.
- **Dominio de enrutamiento**: Seleccione el dominio de enrutamiento al que se aplica la traducción seleccionada.
- **IP/prefijo interno**: La dirección IP interna y el prefijo a los que se debe traducir si se cumplen los criterios de coincidencia.
- **IP/prefijo externo**: La dirección IP externa y el prefijo al que se traduce la dirección IP interna si se cumplen los criterios de coincidencia.
- **Enlazar ruta de respondedor**: Garantiza que el tráfico de respuesta se envíe a través del mismo servicio en el que se recibe, para evitar la redirección asimétrica.
- **ARP proxy**: garantiza que el dispositivo responda a las solicitudes ARP locales para la dirección IP externa.
- **NDP proxy**: garantiza que el dispositivo responda a las solicitudes de NDP locales para la dirección IP externa.
- **Al recibir**: Cuando se selecciona esta casilla de verificación, se configura la NAT de entrada. Cuando se desactiva, se configura la NAT de salida.
- **Aprendizaje automático mediante PD**: Esta casilla de verificación solo se activa cuando se selecciona IPv6 como **tipo de dirección IP**. Cuando se selecciona, Citrix SD-WAN solicita un prefijo al enrutador de delegación ascendente y el enrutador de delegación responde con un prefijo a Citrix SD-WAN.



## Directivas NAT estáticas para el servicio de Internet IPv6

Citrix SD-WAN admite directivas NAT estáticas para el servicio de Internet IPv6 a partir de la versión 11.4.0. Una directiva de NAT estática para el servicio de Internet IPv6 especifica la asignación de un prefijo de red interna a un prefijo de red externa. El número de directivas NAT estáticas necesarias depende del número de redes internas y del número de redes externas (enlaces WAN). Si hay un número **M** de redes internas y un número **N** de enlaces WAN, el número de directivas NAT estáticas necesarias es **M x N**.

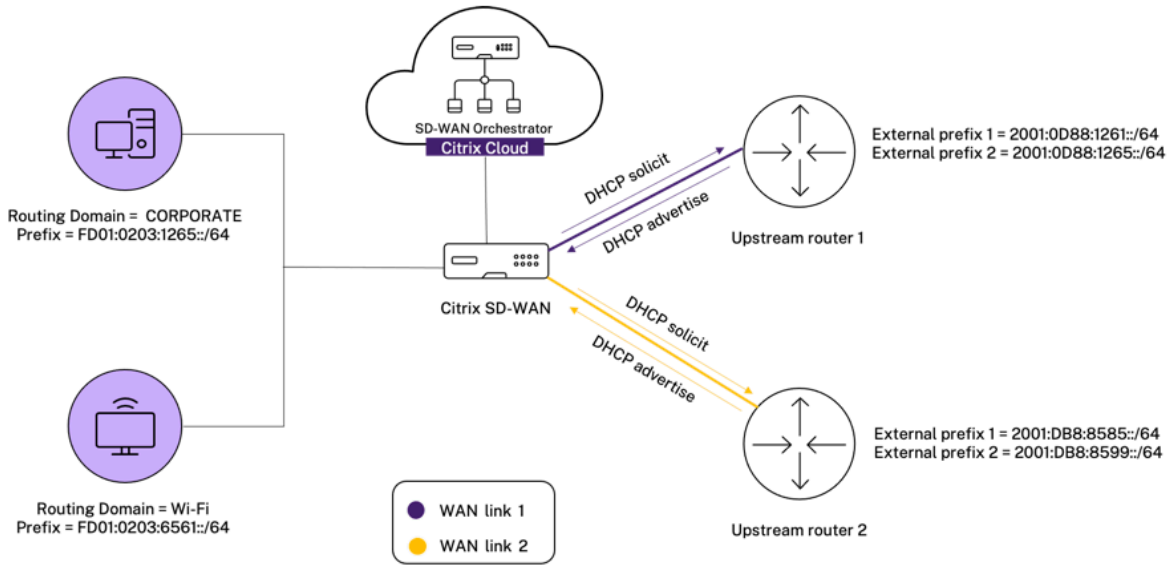
A partir de la versión 11.4.0 de Citrix SD-WAN, al crear una directiva de NAT estática, puede introducir la dirección IP externa manualmente o habilitar el **aprendizaje automático mediante PD**. Cuando se habilita el **aprendizaje automático mediante PD**, el dispositivo SD-WAN recibe prefijos delegados del enrutador de delegación ascendente a través de la delegación de prefijos de DHCPv6. Antes de la versión 11.4.0 de Citrix SD-WAN, la dirección IP externa se derivaba del servicio automáticamente y no existía la opción de introducir manualmente la dirección IP externa. Si va a actualizar un dispositivo a la versión 11.4.0 o posterior y tiene directivas NAT estáticas configuradas para el servicio de Internet IPv6, debe actualizar manualmente las directivas.

### Ejemplo de configuración

En la siguiente topología, el dispositivo Citrix SD-WAN está configurado con 2 redes internas y 2 enlaces WAN:

- Dentro de la red 1 reside en el dominio de redirección CORPORATE con el prefijo de red FD 01:0203:6561□/64
- La red interna 2 reside en el dominio de redirección Wi-Fi con el prefijo de red FD 01:0203:1265□/64
- A través del enlace WAN 1, el dispositivo SD-WAN recibe del enrutador de delegación ascendente a través de la delegación de prefijos DHCPv6, 2 prefijos delegados 2001:0D88:1261::/64 y 2001:0D88:1265::/64. Estos dos prefijos delegados se utilizan como prefijos de red externa cuando el tráfico de las redes internas transita por el enlace WAN 1.
- A través del enlace WAN 2, el dispositivo SD-WAN recibe del enrutador de delegación ascendente a través de la delegación de prefijos DHCPv6, 2 prefijos delegados 2001:DB8:8585::/64 y 2001:DB8:8599::/64. Estos dos prefijos delegados se utilizan como prefijos de red externa cuando el tráfico de las redes internas transita por el enlace WAN 2.




En este caso, hay M=2 dentro de las redes y vínculos WAN N=2. Por lo tanto, la cantidad de directivas de NAT estáticas necesarias para la implementación adecuada del servicio de Internet IPv6 es 2 x 2 = 4. Estas cuatro directivas NAT estáticas especifican la traducción de direcciones para:

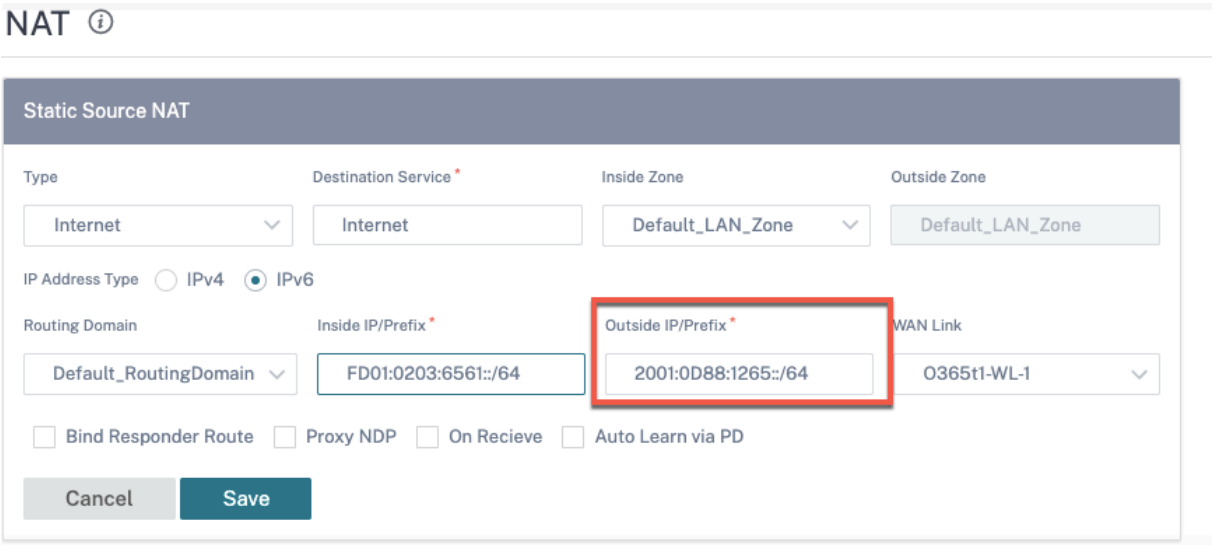
- Red interna 1 a través del enlace WAN 1
- Red interna 1 a través del enlace WAN 2
- Red interna 2 a través del enlace WAN 1
- Red interna 2 a través del enlace WAN 2

Para configurar estas directivas de NAT estáticas, desde el nivel del sitio, vaya a **Configuración > Configuración > Configuración avanzada > NAT > NAT de origen estático**. Haga clic en **+ Fuente estática NAT**.

Al crear directivas de NAT, asegúrese de seleccionar el **tipo** como **Internet** y el **tipo de dirección IP** como **IPv6**. Seleccione el enlace WAN y, en el campo **IP interior/prefijo**, introduzca el prefijo de la red interna (solo se permiten los prefijos /64). En el campo **IP/prefijo externo**, puede introducir manualmente el prefijo de la red externa o seleccionar la casilla de verificación **Aprendizaje automático mediante PD**.

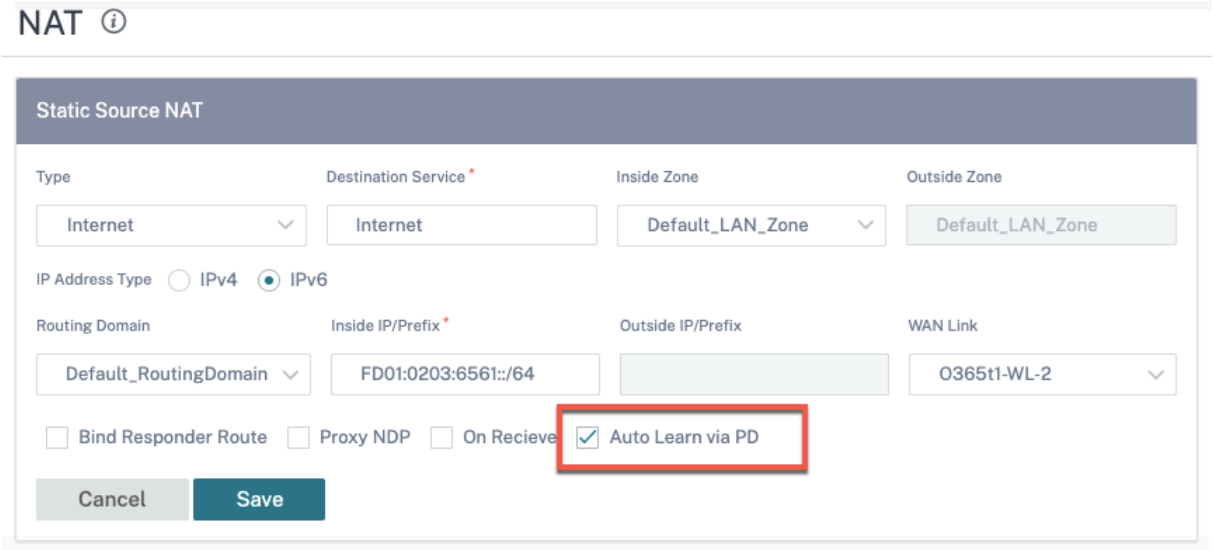
A continuación se muestra un ejemplo en el que la dirección IP externa se introduce manualmente en la directiva NAT estática.




Si selecciona la casilla de verificación **Aprendizaje automático mediante PD**, asegúrese de que el router ascendente admita la delegación de prefijos de DHCPv6. Citrix SD-WAN solicita un prefijo del enrutador delegador ascendente y el enrutador delegador responde con un prefijo a Citrix SD-WAN. Citrix SD-WAN utiliza este prefijo delegado para traducir la dirección IP interna a la dirección IP externa.

A continuación se muestra un ejemplo en el que la función **Aprendizaje automático mediante PD** está habilitada, de modo que el prefijo de red externa se obtiene mediante la delegación de prefijos DHCPv6.




### NAT de destino

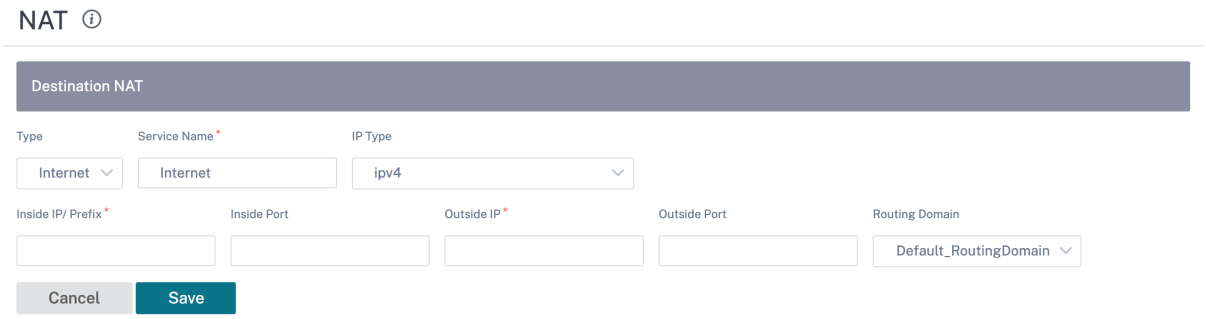
Las directivas de NAT de destino permiten la configuración de directivas de traducción de direcciones de red entre subredes o hosts individuales.

> **Nota**
>
> - Si bien las traducciones entrantes y salientes se pueden configurar simultáneamente para un servicio, solo se utilizará la primera que coincida. Se pueden realizar varias traducciones si existe una regla en el Servicio en el que se recibe un paquete y en el Servicio se envía un paquete.
> - Las traducciones de NAT de destino solo se aplican al tráfico procedente del servicio local.

Para configurar estas directivas de NAT de destino, desde el nivel de sitio, vaya a **Configuración > Configuración > Configuración avanzada > NAT > NAT de destino**. Haga clic en **+ Destination NAT**

- **Tipo**: Los tipos de servicio de SD-WAN a los que se aplica la directiva de NAT. Para NAT estático, los tipos de servicio admitidos son Local, Rutas virtuales, Internet, Intranet y servicios de dominio de interredirección
- **Nombre del servicio**: Proporcione un nombre para el servicio que corresponda al tipo de servicio.
- **Tipo de IP**: Seleccione el tipo de dirección IPv4 o IPv6 según sus preferencias.
- **Puerto interior**: El puerto interior al que se reenviará el puerto exterior.
- **IP externa**: La dirección IP externa y el prefijo a los que se traduce la dirección IP interna si se cumplen los criterios de coincidencia. Para el tráfico saliente que utiliza servicios de Internet e Intranet, la dirección IP del vínculo WAN configurada se elige dinámicamente como la dirección IP externa.
- **Puerto exterior**: El puerto exterior que es el puerto de reenvío hacia el puerto interior.
- **Dominio de enrutamiento**: Seleccione el dominio de enrutamiento al que se aplica la traducción seleccionada.
- **Al recibir**: Cuando se selecciona esta casilla de verificación, se configura la NAT de entrada. Cuando se desactiva, se configura la NAT de salida.

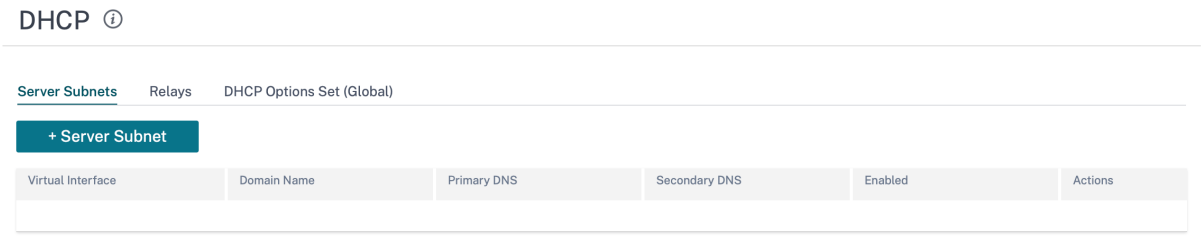


# Protocolo de configuración dinámica de host

October 31, 2022

Puede configurar sus dispositivos SD-WAN como **servidores DHCP** o **agente de retransmisión DHCP**. La función de servidor DHCP permite a los dispositivos de la misma red que la interfaz LAN/WAN del dispositivo SD-WAN obtener su configuración IP del dispositivo SD-WAN. La función de retransmisión DHCP permite a los dispositivos SD-WAN reenviar paquetes DHCP entre el cliente DHCP y el servidor.




## Servidor DHCP

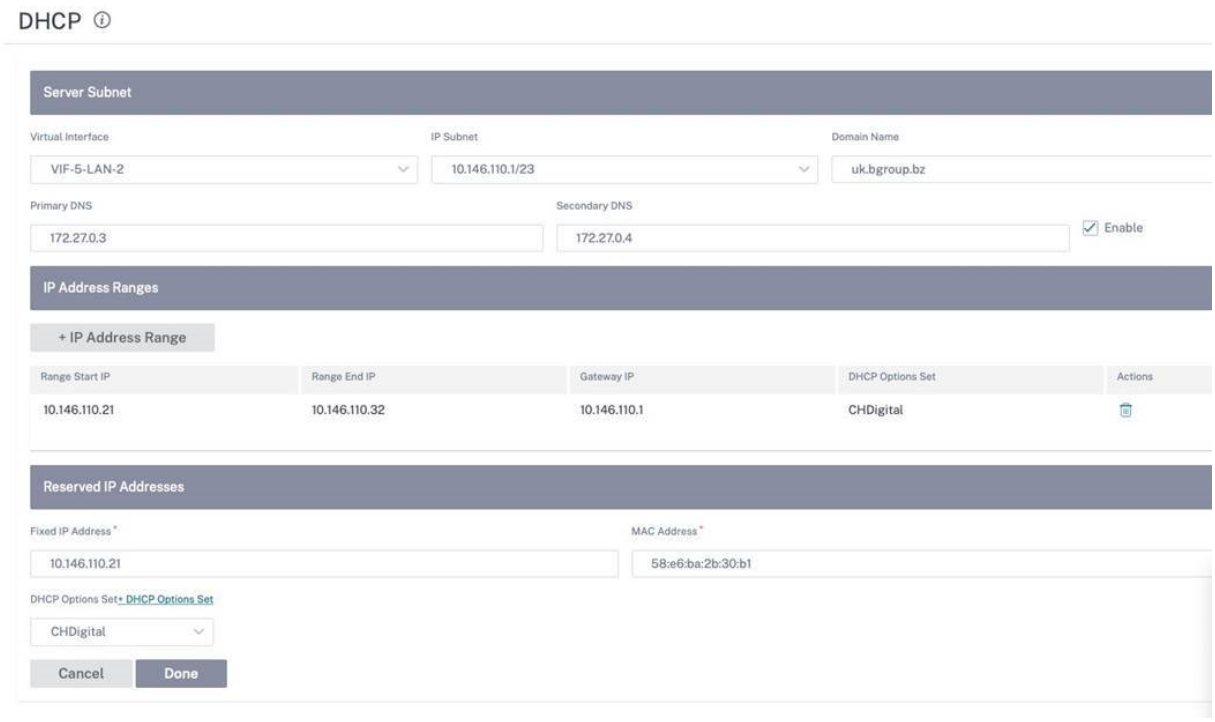
Los dispositivos Citrix SD-WAN se pueden configurar como un servidor DHCP. Puede asignar y administrar direcciones IP de grupos de direcciones especificados dentro de la red a clientes DHCP.

El servidor DHCP se puede configurar para asignar otros parámetros como la dirección IP DNS y la Gateway predeterminada. El servidor DHCP acepta solicitudes de asignación de direcciones y renovaciones. El servidor DHCP también acepta transmisiones de segmentos LAN conectados localmente o de solicitudes DHCP reenviadas por otros agentes de retransmisión DHCP dentro de la red.

Para configurar el servidor DHCP, en la página de configuración del sitio, desde el nivel del sitio, vaya a **Configuración > Configuración avanzada > DHCP > Subredes del servidor >** haga clic en **+ Subred del servidor**.

Seleccione la **interfaz virtual** que se utilizará para recibir las solicitudes DHCP. La subred IP a la que el servidor DHCP proporciona las direcciones IP se rellena automáticamente.




Introduzca el **nombre de dominio**, el **DNS principal**y el **DNS secundario**. El servidor DHCP reenvía esta información a los clientes DHCP.

Configure grupos dinámicos de direcciones IP que se utilizan para asignar direcciones IP a los clientes. Especifique la dirección IP inicial y final del rango y seleccione el **conjunto de opciones DHCP**.

> **Nota**
>
> El conjunto de opciones de DHCP consiste en grupos de configuraciones de DHCP que se pueden aplicar a intervalos de direcciones IP individuales. Para obtener más información, consulte Conjunto de opciones de DHCP.

Configure la dirección IP reservada asignando hosts individuales que requieren una dirección IP fija a su dirección MAC. Introduzca la **dirección IP fija**, la **dirección MAC**y seleccione un **conjunto de opciones de DHCP**.

> **Nota**
>
> Para las direcciones IP reservadas, la **IP de la puerta** de enlace se establece configurando la opción **Router** en el **conjunto de opciones de DHCP**.

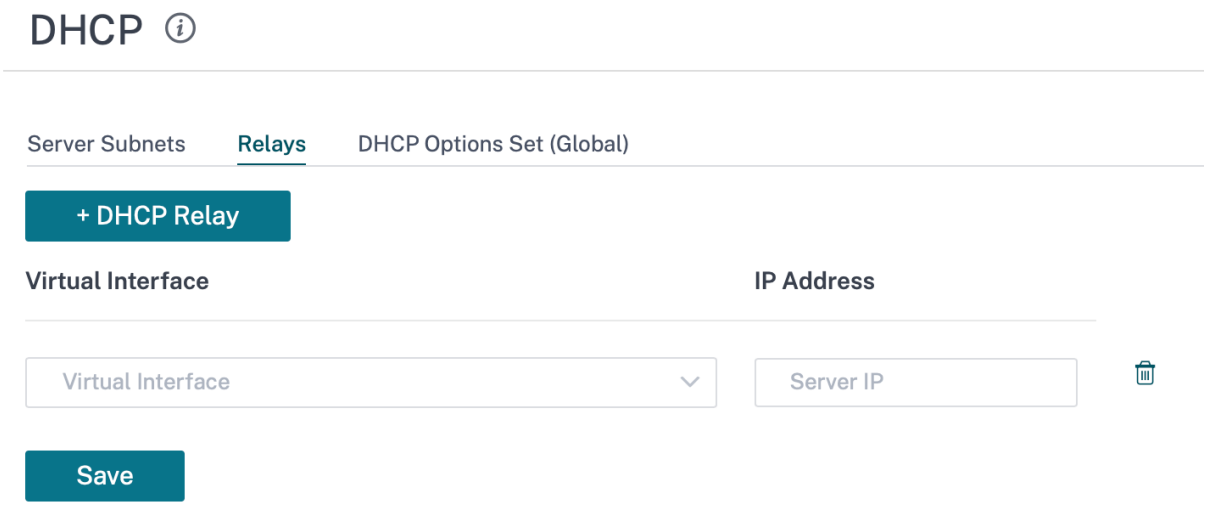
### relé DHCP

El dispositivo Citrix SD-WAN se puede configurar como una retransmisión DHCP. Retransmite solicitudes y respuestas DHCP entre los clientes DHCP locales y un servidor DHCP remoto.

Permite a los hosts locales adquirir direcciones IP dinámicas del servidor DHCP remoto. El agente de retransmisión recibe mensajes DHCP y genera un nuevo mensaje DHCP para enviarlo en otra interfaz.

Para configurar el servidor DHCP, en la página de configuración del sitio, vaya a **Configuración > Configuración > Configuración avanzada > DHCP > Relés** > haga clic en **+ Retransmisión DHCP**.




Seleccione una **interfaz virtual** que se comunique con un servidor DHCP remoto. Introduzca la **IP del servidor DHCP** que utiliza el repetidor para reenviar la solicitud y la respuesta de los clientes.

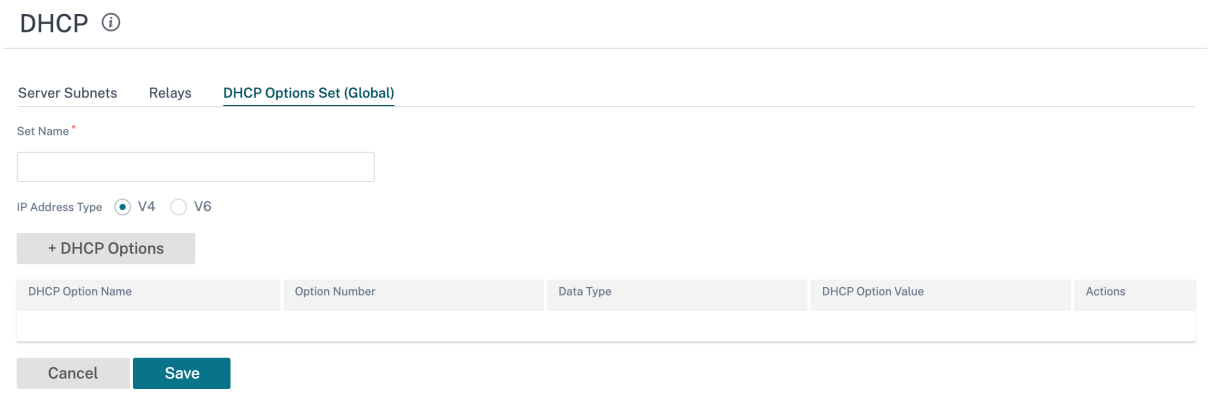
Puede configurar un único **relé DHCP** mediante una interfaz de red virtual común y dirigirlo a varios servidores DHCP.

### conjunto de opciones de DHCP

Las opciones DHCP son un grupo de configuraciones DHCP que se pueden aplicar a intervalos de direcciones IP individuales o a un único host.

Defina un nombre para el perfil de opciones de DHCP y elija el **tipo de dirección IP**. Haga clic en **+ Conjunto de opciones de DHCP** y seleccione un nombre de opción DHCP de la lista. El número de opción está preconfigurado. Para las opciones personalizadas, el rango es 224-254. Seleccione un **tipo de datos** e introduzca un **valor** para la opción.




### Aprendizaje de direcciones IP de enlace WAN a través del cliente DHCP

Los dispositivos Citrix SD-WAN admiten el aprendizaje de direcciones IP de enlace WAN a través de clientes DHCP. Esta funcionalidad reduce la cantidad de configuración manual necesaria para implementar dispositivos SD-WAN y reduce los costes de ISP al eliminar la necesidad de comprar direcciones IP estáticas. Los dispositivos SD-WAN pueden obtener direcciones IP dinámicas para los vínculos WAN en interfaces que no son de confianza. Esto elimina la necesidad de un enrutador WAN intermedio para realizar esta función.

> **Notas**
>
> - El cliente DHCP solo se puede configurar para interfaces no conectadas en puente que no sean de confianza configuradas como nodos de cliente.
> - El cliente DHCP y el puerto de datos se pueden habilitar en MCN/RCN solo si la dirección IP pública está configurada.
> - No se admite la implementación de redirección basado en directivas (PBR) en el sitio con la configuración del cliente DHCP.
> - Los eventos DHCP se registran únicamente desde la perspectiva del cliente y no se generan registros del servidor DHCP.

Para obtener información sobre la configuración de DHCP para una interfaz virtual que no es de confianza en los modos de bloqueo y error de conexión, consulte Configuración al nivel de sitio.

## Redirección de multidifusión

October 31, 2022

La redirección de multidifusión permite una distribución eficiente del tráfico de uno a varios. Una fuente de multidifusión envía tráfico de multidifusión en una sola secuencia a un grupo de multidi-

fusión. El grupo de multidifusión contiene receptores como hosts y enrutadores adyacentes que utilizan el protocolo IGMP para la comunicación de multidifusión. Voz sobre IP, Vídeo a demanda, Televisión por IP y Videoconferencias son algunas de las tecnologías comunes que utilizan redirección de multidifusión. Cuando habilita la redirección de multidifusión en el dispositivo Citrix SD-WAN, el dispositivo actúa como enrutador de multidifusión.

## Multidifusión específica de origen

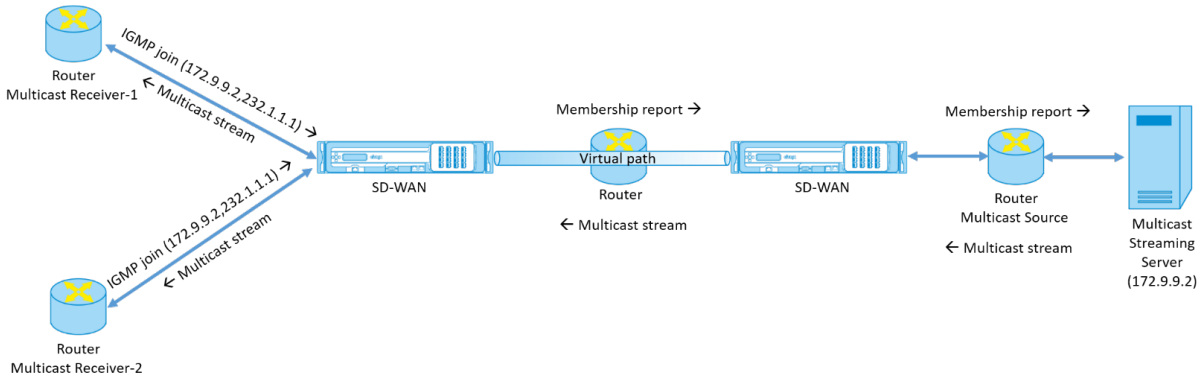
Los protocolos de multidifusión normalmente permiten a los receptores de multidifusión recibir tráfico de multidifusión desde cualquier origen.

Con la multidifusión específica de origen (SSM), puede especificar el origen desde el que los receptores reciben el tráfico de multidifusión. Garantiza que los receptores no sean oyentes abiertos a todas las fuentes que envían transmisiones de multidifusión, sino que escuchen a una fuente de multidifusión particular.

El SSM reduce el coste de los recursos utilizados para consumir tráfico de todas las fuentes posibles. El SSM también proporciona una capa de seguridad al garantizar que los receptores reciben tráfico de un remitente conocido.

La siguiente topología muestra dos receptores de multidifusión en un sitio de sucursal y un servidor de multidifusión (172.9.9.2) en el centro de datos. El servidor de multidifusión transmite tráfico a través de un grupo determinado (232.1.1.1), los receptores se unen al grupo. Cualquier tráfico transmitido en el grupo de multidifusión se retransmite a todos los receptores que se unieron al grupo.

> **Nota**
>
> Para que SSM funcione, la IP del grupo de multidifusión debe estar dentro del rango 2320.0.0/8.




1. Los receptores de multidifusión envían una solicitud de unión IGMP IP que indica que los receptores quieren unirse al grupo de multidifusión y quieren recibir la secuencia de multidifusión desde el origen.

La combinación IGMP incluye 2 atributos el origen y el grupo de multidifusión (S, G). IGMP Versión 3 se utiliza para SSM en el origen de multidifusión y el receptor para retransmitir algunas direcciones de origen específicas INCLUDE.

El SSM permite a los receptores recibir explícitamente flujos de servidores Multicast específicos, cuya dirección de origen es proporcionada explícitamente por los receptores como parte de la solicitud JOIN. En este ejemplo, se activa una solicitud de combinación IGMP v3 con una lista de origen de inclusión explícita, que contiene el origen 172.9.9.2, para que sea la dirección que envía la secuencia de multidifusión sobre el grupo 232.1.1.1.

2. Citrix SD-WAN en la sucursal escucha todas las solicitudes IGMP de estos receptores y lo convierte en un informe de pertenencia y lo envía a través de la ruta virtual al dispositivo SD-WAN del centro de datos.
3. El dispositivo Citrix SD-WAN del centro de datos recibe el informe de pertenencia a través de la ruta virtual y lo reenvía al origen de multidifusión, estableciendo un canal de control.
4. El origen de multidifusión transmite la secuencia de multidifusión a través de la ruta de acceso virtual a los receptores de multidifusión.

El tráfico del canal de control y el flujo de multidifusión fluyen a través de la ruta virtual establecida entre la rama y el centro de datos. La ruta de superposición Citrix SD-WAN asegura y aísla el tráfico de multidifusión de la degradación de WAN o de los apagones de enlaces.

### Configuración de multidifusión

Para configurar la multidifusión, realice lo siguiente en el servicio SD-WAN Orchestrator tanto en el origen como en el destino.

1. Crear un grupo de multidifusión: Proporcione un nombre y una dirección IP para el grupo de multidifusión. La IP del grupo de multidifusión debe estar dentro del rango 2320.0.0/8 para la multidifusión específica de origen.
2. Habilitar el proxy IGMP: Puede configurar el dispositivo Citrix SD-WAN como un proxy IGMP/MLD para transmitir la información del canal de control IGMP para el enrutamiento de multidifusión.
3. Definir los servicios ascendentes y descendentes: Una interfaz ascendente permite al PROXY IGMP conectarse al dispositivo SD-WAN más cerca de la fuente de multidifusión real que transmite el tráfico. Una interfaz descendente permite que el proxy IGMP se conecte a los hosts que están más lejos de la fuente de multidifusión real que transmite el tráfico.
   Los servicios ascendentes y descendentes son diferentes para el dispositivo en el origen y el dispositivo en el destino.

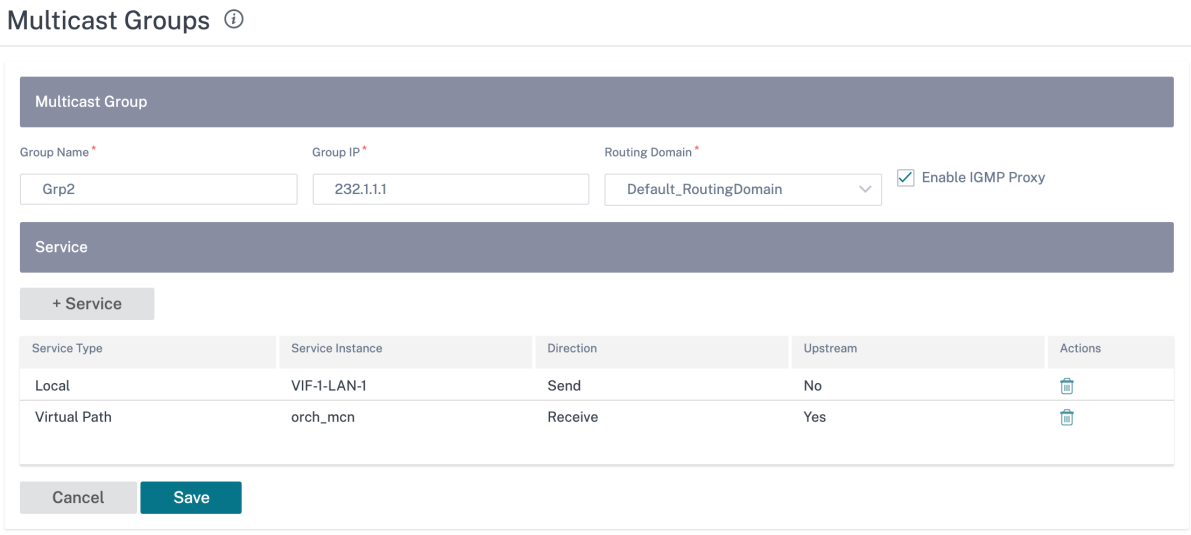
> **Nota**:
>
> Una vez que la sucursal o el MCN se configuran como ascendentes, también deben configurarse como ascendentes para los demás grupos.

Para configurar la multidifusión, al nivel de sitio, vaya a **Configuración > Configuración** > **Configuración avanzada** > **Grupos de multidifusión**. Cree un grupo de multidifusión proporcionando un nombre y una dirección IP (IPv4 o IPv6) para el grupo de multidifusión. Haga clic en **Habilitar proxy IGMP**.

Configure las rutas ascendentes y descendentes para los dispositivos de sucursal y centro de datos.

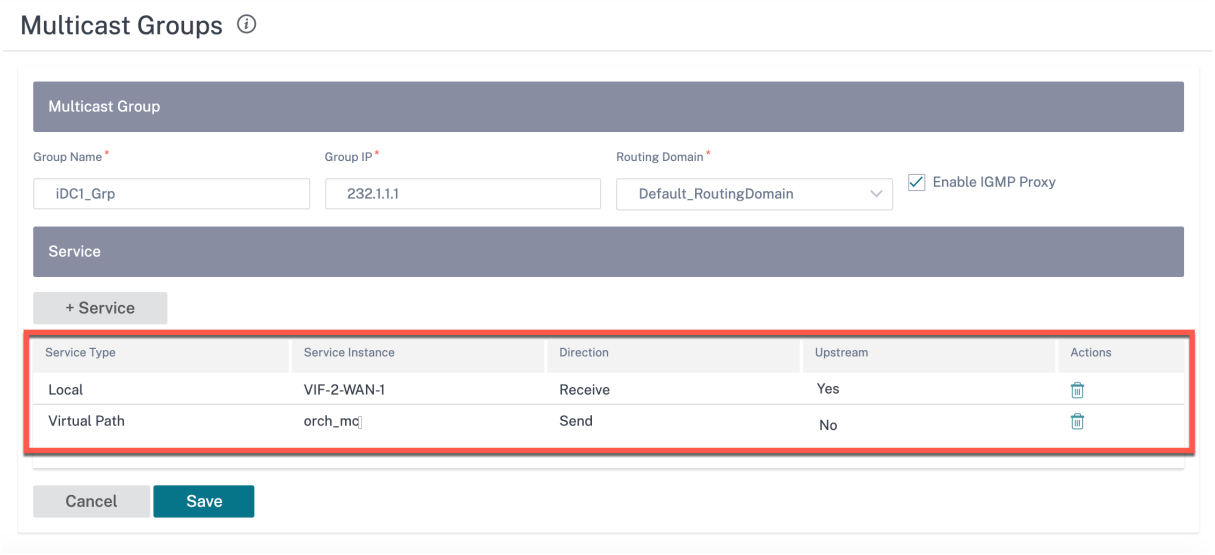
Para el dispositivo más cercano al receptor de multidifusión (Branch), el dispositivo recibe el tráfico de multidifusión en la interfaz de ruta virtual y envía el tráfico de la interfaz local hacia el receptor.

> **Nota**:
>
> - Cuando una fuente de multidifusión se configura como un servicio de intranet, la IP de origen de la transmisión de multidifusión debe tener una ruta asignada al servicio de intranet.
> - Asegúrese de crear las directivas de firewall adecuadas para permitir el tráfico de multidifusión en el dispositivo SD-WAN.




Para el dispositivo más cercano al origen de multidifusión (centro de datos), el dispositivo recibe el tráfico de multidifusión en la interfaz local y envía el tráfico en la Interfaz de ruta virtual.

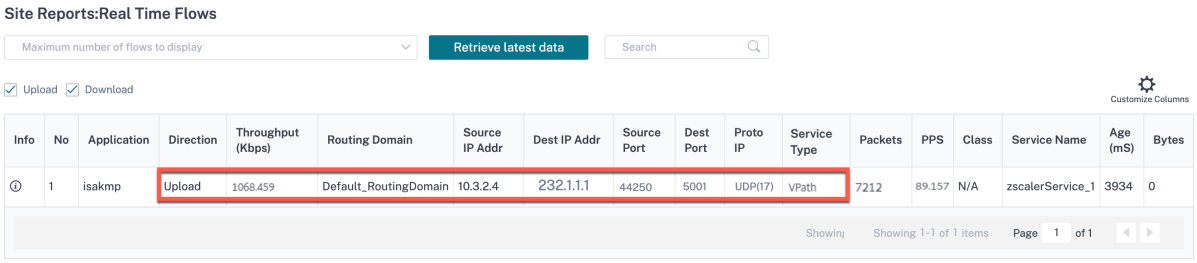



## Supervisión

### Estadísticas de flujos

Una vez establecido el canal de control de multidifusión y el origen de multidifusión comienza a transmitir, puede ver las estadísticas de flujos de multidifusión. Puede ver que el tráfico UDP de multidifusión se envió en el servicio de ruta virtual desde un receptor al grupo de multidifusión 232.1.1.1.

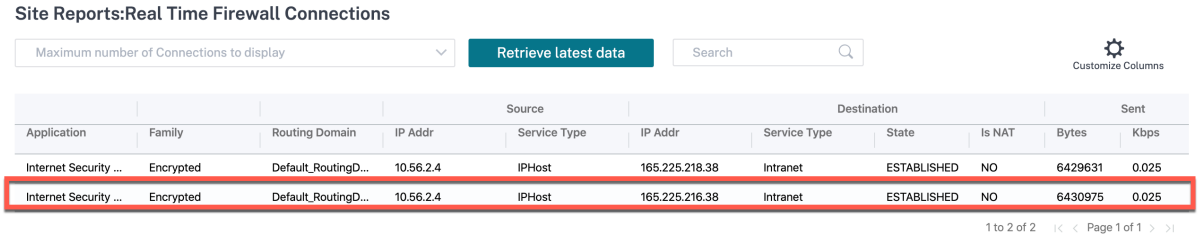
> **Nota**:
>
> Si SSM está habilitado y si el tráfico se recibe de un servidor diferente que no forma parte de la lista esperada de remitentes de origen, el dispositivo SD-WAN no tendrá datos de informes.




### Estadísticas de firewall

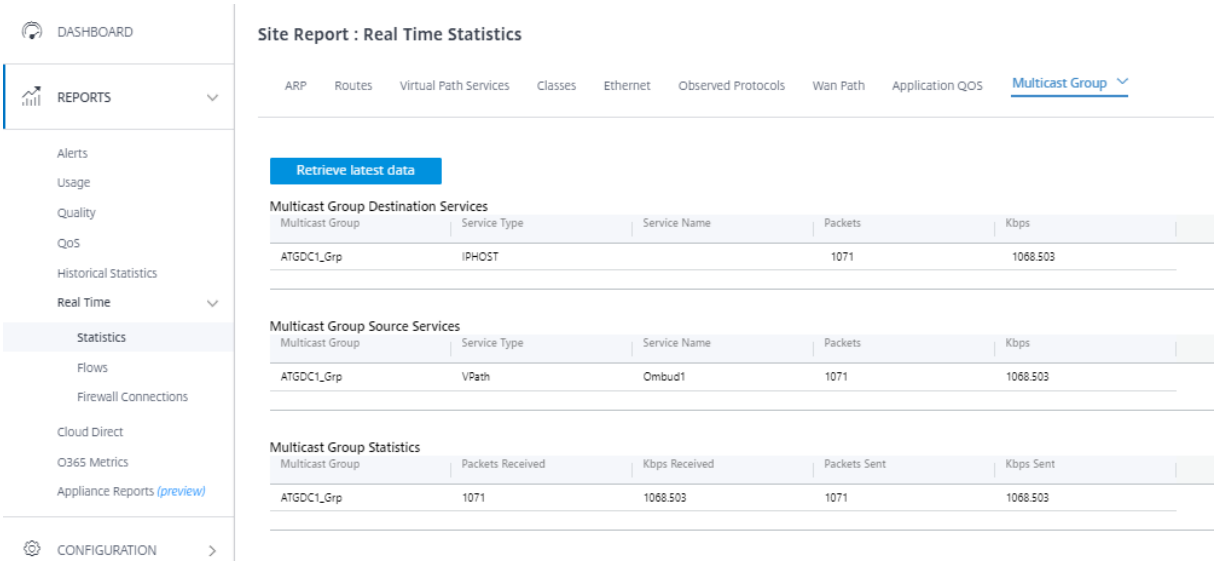
La tabla del firewall muestra el tráfico de multidifusión que llega a través de la interfaz LAN a través de la dirección IP del grupo Multicast y se envía a través de la ruta virtual.




### Estadísticas de grupos de multidifusión

La tabla de grupos de multidifusión proporciona detalles sobre el tráfico de multidifusión, como los paquetes enviados y recibidos por origen, destino y la agregación de ambos.

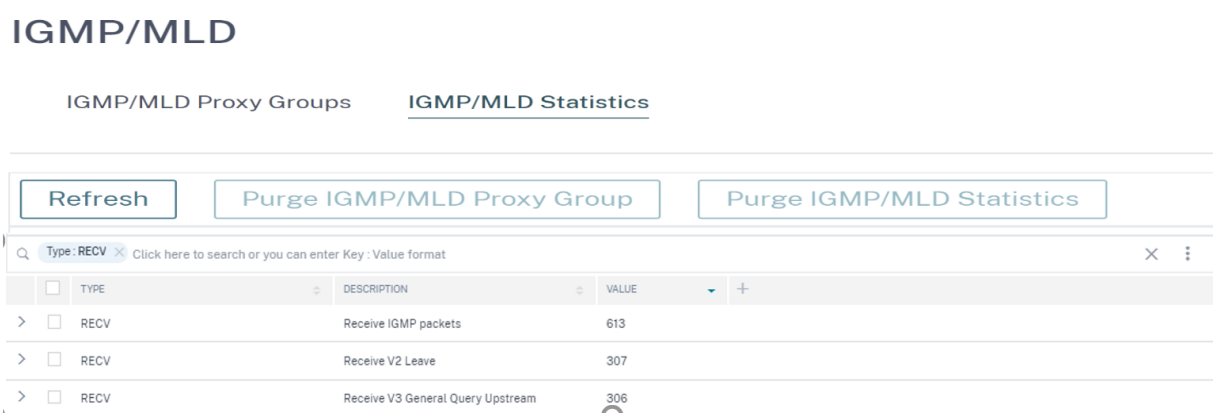



## IGMP/MLD

Cuando los receptores de multidifusión inician una solicitud de unión a un grupo, puede ver los detalles del receptor en **Informes** > **Tiempo real** > **IGMP/MLD** > **Estadísticas de IGMP/MLD**. Puede ver esta información tanto en el origen como en el destino. Haga clic en **Actualizar** para obtener los datos actuales.

La siguiente imagen muestra que los paquetes IGMP/MLD recibidos y el tipo de filtro RECV se utilizan para incluir los paquetes de recepción IGMP/MLD.




Para ver los detalles de los grupos de proxy IGMP, vaya a **Informes** > **Tiempo real** > **IGMP/MLD** > **Grupos de proxy IGMP/MLD**. Haga clic en **Actualizar** para obtener los datos actuales.

Seleccione **Purgar estadísticas de IGMP/MLD** para purgar los datos estadísticos de IGMP de la tabla de estadísticas de IGMP.

Seleccione **Purgar grupo IGMP/MLD** para purgar los datos del grupo IGMP de la tabla de grupos IGMP.

## Protocolo de redundancia de enrutador virtual

October 31, 2022

El Protocolo de redundancia de enrutador virtual (VRRP) es un protocolo ampliamente utilizado que proporciona redundancia de dispositivos para eliminar el punto único de falla inherente al entorno estático con enrutamiento predeterminado.

VRRP permite configurar dos o más routers para formar un grupo. Este grupo aparece como una única Gateway predeterminada con una dirección IP virtual y una dirección MAC virtual.

Un enrutador de respaldo se hace cargo automáticamente si el enrutador principal o principal falla. En una configuración de VRRP, el router principal envía un paquete VRRP conocido como anuncio a los enrutadores de respaldo. Cuando el enrutador principal deja de enviar el anuncio, el enrutador de respaldo establece el temporizador de intervalos. Si no se recibe ningún anuncio durante este período de espera, el router de respaldo inicia la rutina de conmutación por error.

El VRRP especifica un proceso de elección en el que el router con la prioridad más alta se convierte en el router principal. Si la prioridad es la misma entre los enrutadores, el enrutador con la dirección IP más alta se convierte en el enrutador principal. Los otros enrutadores están en estado de copia de seguridad. El proceso de elección se inicia de nuevo si el router principal falla, si un router nuevo se une al grupo o si un router existente abandona el grupo.

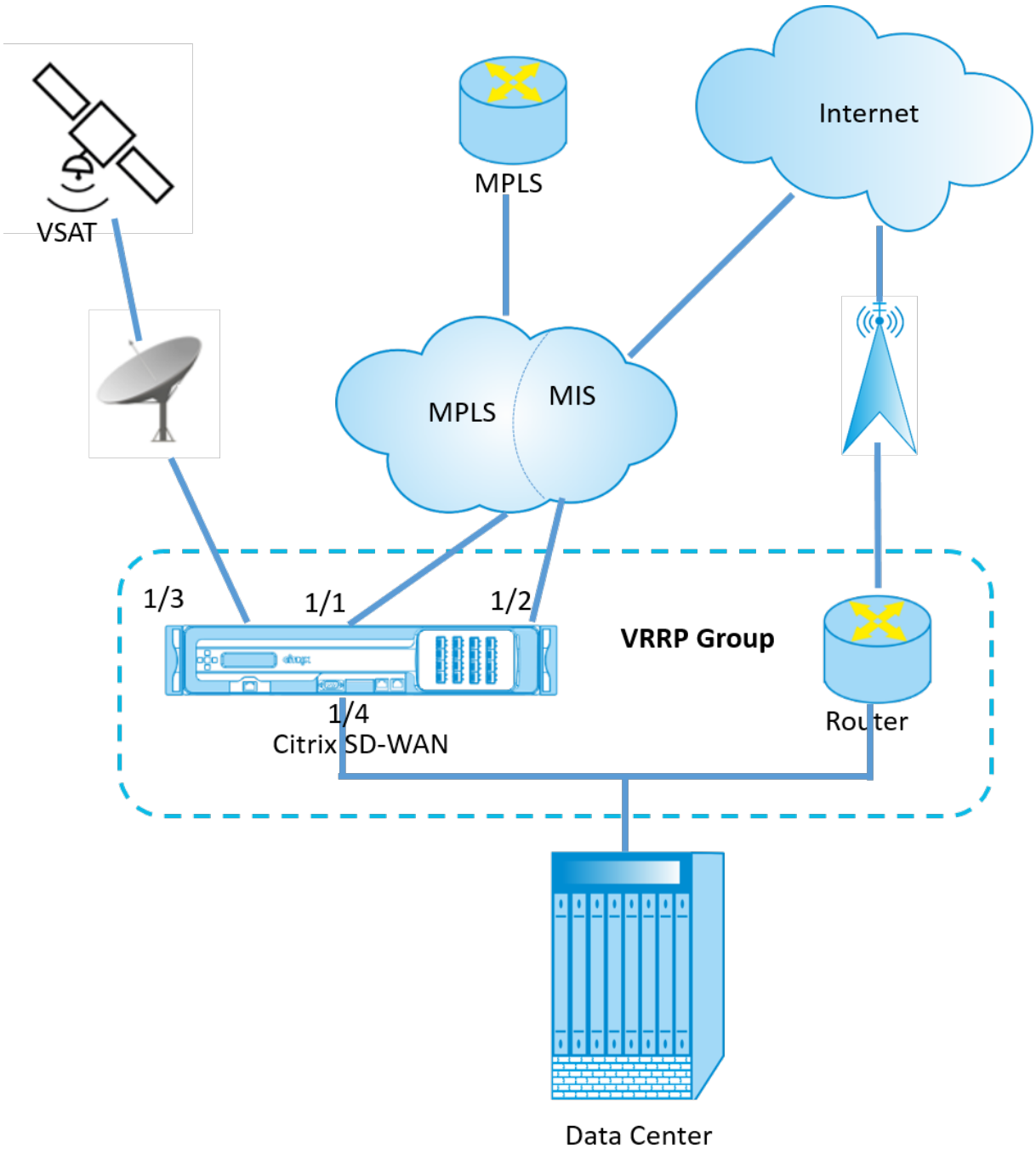
 

VRRP garantiza una ruta predeterminada de alta disponibilidad sin configurar protocolos de redirección dinámico o detección de enrutadores en todos los hosts finales.

La versión 10.1 de Citrix SD-WAN admite VRRP versión 2 y versión 3 para interoperar con enrutadores de terceros. La versión 11.5 de Citrix SD-WAN admite la versión 6. El dispositivo SD-WAN actúa como el enrutador principal y dirige el tráfico para que utilice el servicio de rutas virtuales entre los sitios. Puede configurar el dispositivo SD-WAN como enrutador principal de VRRP configurando la IP de la interfaz virtual como IP de VRRP y estableciendo manualmente la prioridad en un valor superior al de los enrutadores pares. Puede configurar el intervalo de anuncio y la opción de preferencia.

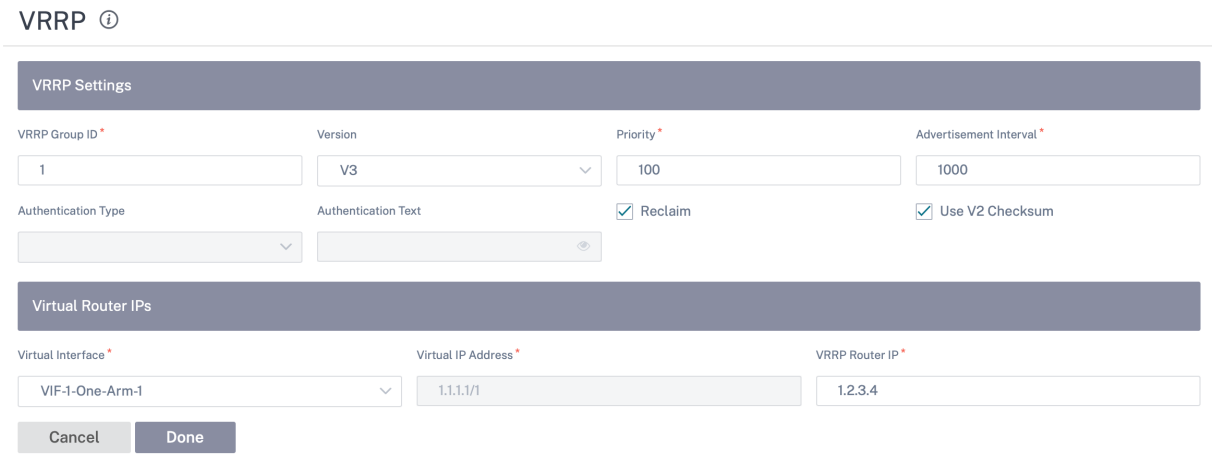
El siguiente diagrama de red muestra un dispositivo Citrix SD-WAN y un enrutador configurados como grupo VRRP. El dispositivo SD-WAN está configurado para ser el enrutador principal. Si se produce un error en el dispositivo SD-WAN, el router de copia de seguridad se llevará a cabo en milisegundos, lo que garantiza que no haya tiempo de inactividad.




Para configurar VRRP, en la página de configuración del sitio, vaya a **Configuración > Configuración** > **Configuración avanzada** > **VRRP** > haga clic en **+ Agregar VRRP**.




Puede modificar los siguientes parámetros de ruta de miembro:

- **ID de grupo VRRP**: El ID del grupo VRRP. El ID de grupo debe tener un rango de valores comprendido entre 1 y 255. También se debe configurar el mismo ID de grupo en los routers de respaldo.
- **Versión**: La versión del protocolo VRRP. Puede elegir entre el protocolo VRRP V2 y V3.
- **Prioridad**: La prioridad del dispositivo Citrix SD-WAN para el grupo VRRP. El rango de prioridad es 1-254. Establezca este valor en el máximo (254) para que el dispositivo SD-WAN sea el enrutador principal.

  > **Nota**
  >
  > Si el enrutador es el propietario de la dirección IP VRRP, la prioridad se establece en 255 de forma predeterminada.

- **Intervalo**de anuncios: La frecuencia en milisegundos con la que se envían las publicaciones de VRRP cuando el dispositivo SD-WAN es el enrutador principal. El intervalo de anuncio predeterminado es de un segundo.
- **Tipo de autenticación**: Puede elegir **Texto sin formato** para introducir una cadena de autenticación. La cadena de autenticación se envía como texto sin cifrar en los anuncios de VRRP. Elija **Ninguno**si no quiere configurar la autenticación.
- **Texto de autenticación**: La cadena de autenticación que se enviará en el anuncio de VRRP. Esta opción está activada si el **tipo de autenticación** es **texto sin formato**.

  > **Nota**
  >
  > Los parámetros **Tipo de autenticacióny Texto** de autenticación solo están habilitados para la versión 2 del protocolo VRRP.

- **Utilice V2 Checksum**: Permite la compatibilidad con dispositivos de red de terceros para VRRPv3. De forma predeterminada, VRRPv3 utiliza el método de cálculo de suma de comprobación v3. Algunos dispositivos de terceros solo pueden admitir el cálculo de suma de comprobación VRRPv2. En tales casos, habilite esta opción.
- **Interfaz virtual**: La interfaz virtual que se utilizará para VRRP. Si se usa IPv6, la interfaz virtual tendrá NDP RA habilitada de forma predeterminada. Elija una de las interfaces virtuales configuradas.
- **Dirección IP virtual: Dirección**IP virtual asignada a la interfaz virtual. Elija una de las direcciones IP virtuales configuradas para la interfaz virtual. Puede especificar la dirección IPv4 o IPv6.
- **IP del enrutador VRRP**: La dirección IP del enrutador virtual del grupo VRRP. De forma predeterminada, la dirección IP virtual del dispositivo SD-WAN se asigna como dirección IP del enrutador virtual. La IP del enrutador virtual VRRP debe ser una dirección IPv6 local de enlace.

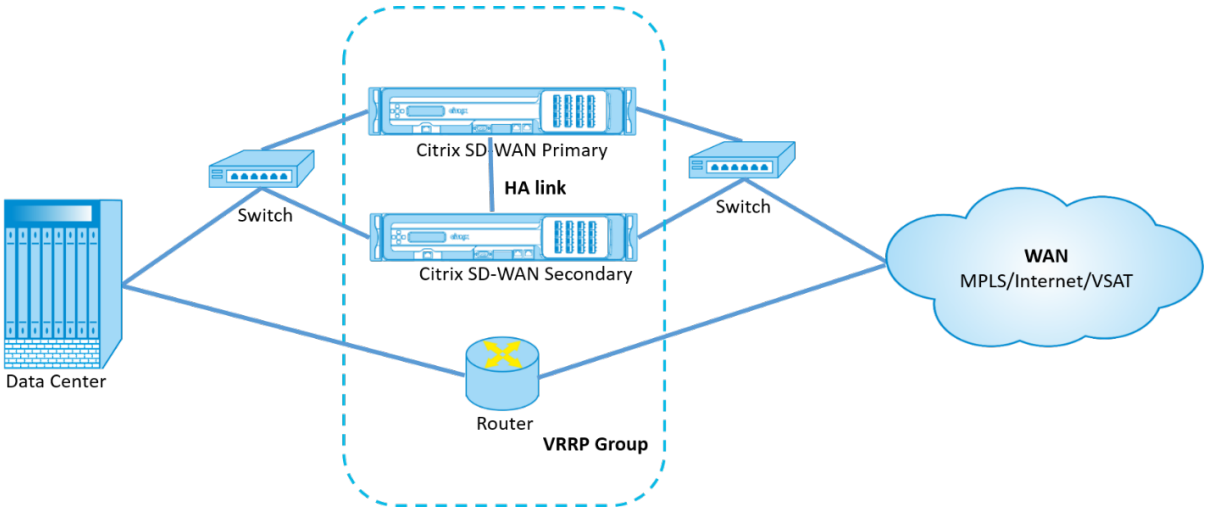
### Limitaciones

- VRRP solo se admite en la implementación en modo puerta de enlace.
- Puede configurar hasta cuatro ID de VRRP (VRID).
- En VRID pueden participar hasta 16 interfaces de red virtuales.

### Alta disponibilidad y VRRP

Puede reducir significativamente el tiempo de inactividad de la red y las interrupciones del tráfico al aplicar las funciones de alta disponibilidad y VRRP en su red SD-WAN. Implemente un par de dispositivos Citrix SD-WAN en funciones activas/en espera junto con un enrutador en espera para formar el grupo VRRP. Este grupo aparece como una única Gateway predeterminada con una dirección IP virtual y una dirección MAC virtual.




Los siguientes son dos casos de implementación de alta disponibilidad y VRRP:

**Primer caso: El temporizador de conmutación por error de alta disponibilidad en SD-WAN es igual al temporizador de conmutación por error de VRRP.**

El comportamiento esperado es la conmutación de alta disponibilidad antes de la conmutación de VRRP, es decir, el tráfico continúa fluyendo a través del nuevo dispositivo Active SD-WAN. En este caso, SD-WAN continúa con el rol Maestro VRRP.

**Segundo caso: Temporizador de conmutación por error de alta disponibilidad en SD-WAN mayor que el temporizador de conmutación por error de VRRP.**

El comportamiento esperado es que ocurre la conmutación de VRRP al enrutador, es decir, el enrutador se convierte en VRRP Master y el tráfico podría fluir momentáneamente a través del router, evitando el dispositivo SD-WAN.

Pero una vez que ocurre la conmutación de alta disponibilidad, SD-WAN vuelve a convertirse en VRRP Master, es decir, el tráfico ahora fluye a través del nuevo dispositivo SD-WAN activo.

Para obtener más información sobre los modos de implementación de alta disponibilidad, consulte Alta disponibilidad.

## Configuración del sistema de nombres de dominio

October 31, 2022

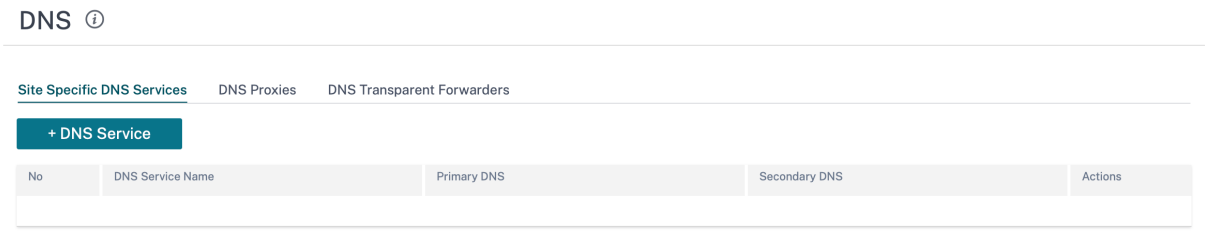
El Sistema de nombres de dominio (DNS) traduce los nombres de dominio legibles por humanos a direcciones IP legibles por máquina, y de la manera opuesta. Citrix SD-WAN proporciona las siguientes funciones DNS:

- Proxy DNS

- Reenvío transparente DNS

Para configurar los ajustes de DNS, en la página de configuración del sitio, vaya a **Configuración > Configuración avanzada** > **Configuración de DNS**.




### Servidores DNS específicos del sitio

En la ficha **Servidores DNS específicos del sitio**, haga clic en **+ Servidor DNS** para configurar los servidores DNS específicos del sitio a los que se dirigen las solicitudes de DNS. Proporcione un nombre para el servidor DNS. Elija uno de los siguientes tipos de servicio:

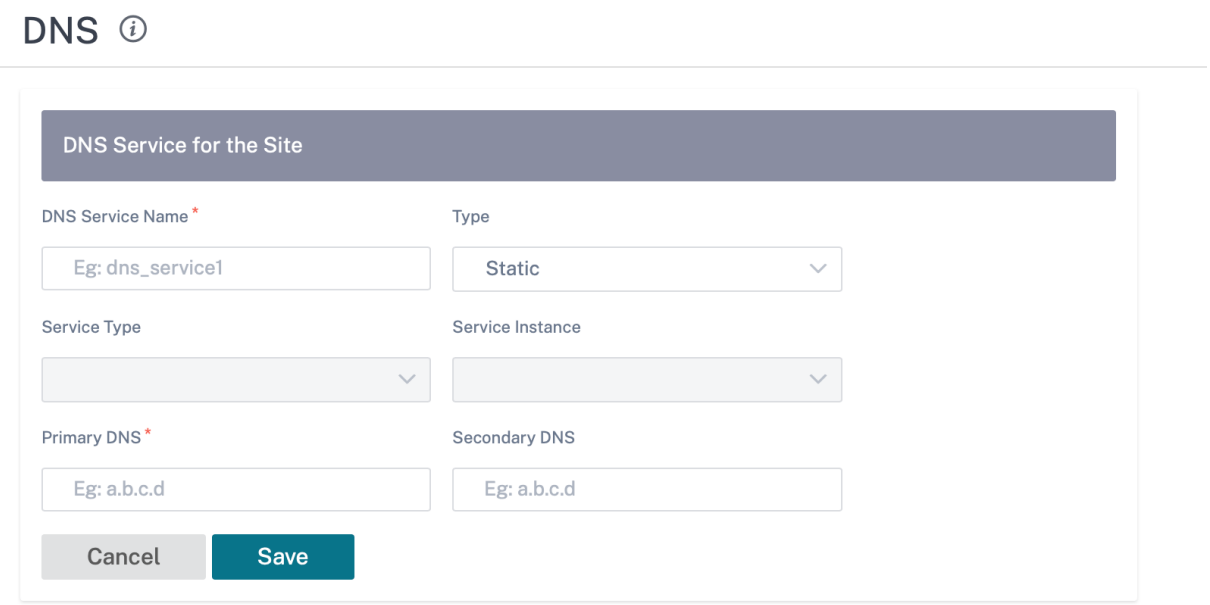
- **Estática**: intercepta las solicitudes DNS destinadas a la dirección IP SD-WAN de Citrix y las reenvía a los servidores DNS IPv4 especificados. Puede crear internos, ISP, google o cualquier otro servicio DNS de código abierto.
- **Dinámica**: intercepta las solicitudes DNS destinadas a la dirección IP SD-WAN de Citrix y las redirige a uno de los servidores DNS IPv4 aprendidos de los enlaces WAN basados en DHCP. Si el enlace WAN desaparece, se elige otro servidor DNS de enlaces WAN basado en DHCP. Esta función es útil en la implementación en la que los ISP permiten solicitudes DNS solo a los servidores DNS alojados por ellos. El servicio DNS dinámico solo se puede configurar al nivel de sitio. Solo se permite un servicio DNS dinámico por sitio.
- **Staticv6**: intercepta las solicitudes DNS destinadas a la dirección IP SD-WAN de Citrix y las reenvía a los servidores DNS IPv6 especificados. Puede crear internos, ISP, google o cualquier otro servicio DNS de código abierto.
- **Dynamicv6**: intercepta las solicitudes DNS destinadas a la dirección IP SD-WAN de Citrix y las redirige a uno de los servidores DNS IPv6 aprendidos de los enlaces WAN basados en DHCP. Si el enlace WAN desaparece, se elige otro servidor DNS de enlaces WAN basado en DHCP. Esta función es útil en la implementación en la que los ISP permiten solicitudes DNS solo a los servidores DNS alojados por ellos. El servicio DNS dinámico solo se puede configurar al nivel de sitio. Solo se permite un servicio DNS dinámico por sitio.

Para configurar el servicio DNS estático, seleccione **Tipo** como **estático** (para la dirección IPv4) o **Estático** (para la dirección IPv6) e introduzca un par de direcciones IP del servidor **DNS principal** y del servidor **DNS secundario**.

Para configurar el servicio DNS dinámico, seleccione **Tipo** como **dinámico** (para la dirección IPv4) o **Dynamicv6** (para la dirección IPv6) y seleccione **Internet** para el **tipo de servicio** y la **instancia de servicio**.

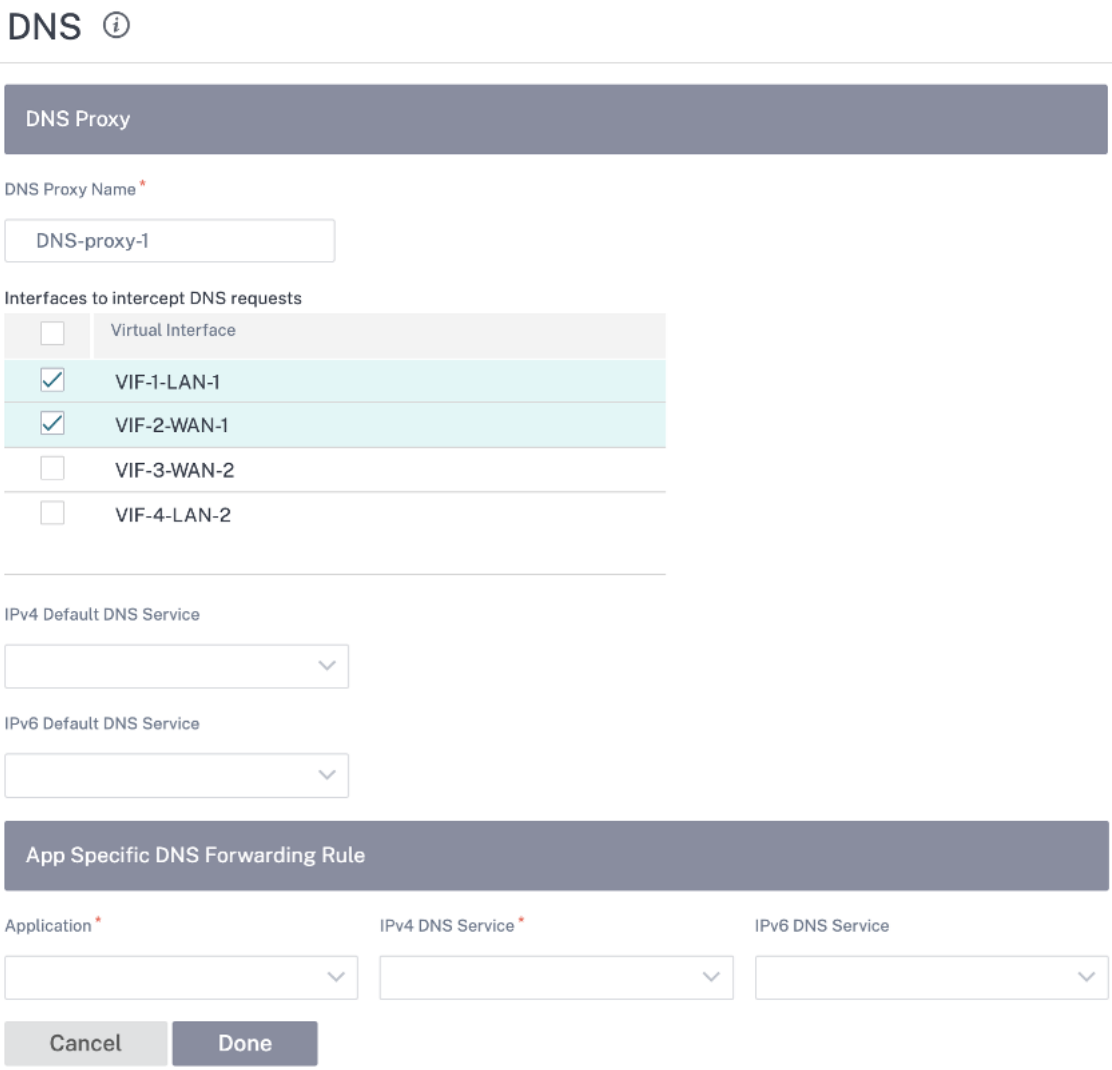
Los servicios de proxy DNS correspondientes aparecen en la lista desplegable **DNS de administración de InBand**, en **Configuración del sitio > Interfaces**.




### Proxy DNS

El proxy DNS intercepta las solicitudes DNS destinadas a la dirección IP SD-WAN y las reenvía a los servidores DNS seleccionados. Puede configurar un proxy con varios reenviadores que ayuden a dirigir las solicitudes DNS en función de los nombres de dominio de la aplicación.



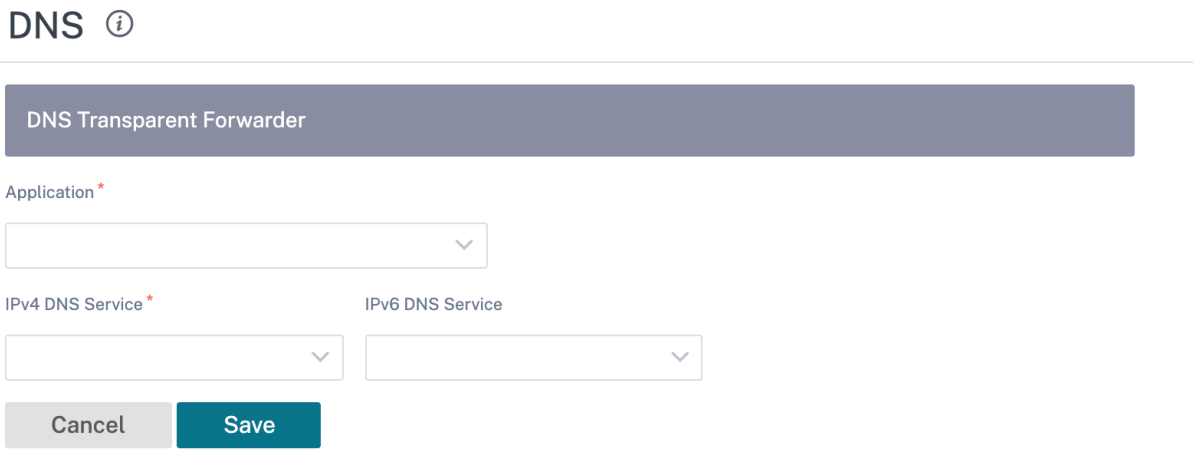

- Configuración del proxy DNS:
  - **Nombre del proxy DNS**: Nombre del proxy DNS.
  - **Interfaces para interceptar las solicitudes de DNS**: Las interfaces en las que se interceptan las solicitudes de DNS. Solo se permiten las interfaces de confianza.
  - **Servidor DNS predeterminado para todo el tráfico**: El servidor DNS predeterminado al que se reenvían las solicitudes de DNS, si ninguna de las aplicaciones coincide en la búsqueda del reenviador DNS.
  - **Servicio DNS predeterminado de IPv4: El servicio**DNS predeterminado de IPv4 al que se reenvían las solicitudes de DNS, si ninguna de las aplicaciones coincide en la búsqueda del reenviador de DNS.
  - **Servicio DNS predeterminado de IPv6: El servicio**DNS predeterminado de IPv6 al que se reenvían las solicitudes de DNS, si ninguna de las aplicaciones coincide en la búsqueda del reenviador de DNS.

- Reglas de reenvío DNS específicas de la aplicación:
  - **Aplicación**: Aplicaciones para las que las solicitudes de DNS deben reenviarse al servidor DNS seleccionado.
  - **Servicio DNS IPv4: El servicio**DNS IPv4 al que se reenvía la solicitud de DNS para la aplicación especificada.
  - **Servicio DNS IPv6: El servicio**DNS IPv6 al que se reenvía la solicitud de DNS para la aplicación especificada.

### Reenviadores transparentes DNS

Citrix SD-WAN se puede configurar como un reenviador DNS transparente. En este modo, SD-WAN puede interceptar solicitudes DNS que no están destinadas a su dirección IP y reenviarlas a los servidores DNS especificados. Solo se interceptan las solicitudes DNS procedentes del servicio local en interfaces de confianza. Si las solicitudes DNS coinciden con cualquier aplicación de la lista de reenviadores DNS, se reenvía al servicio DNS configurado.




- **Aplicación**: Aplicaciones para las que las solicitudes de DNS deben reenviarse al servidor DNS seleccionado.
- **Servicio DNS IPv4: El servicio**DNS IPv4 al que se reenvía la solicitud de DNS para la aplicación especificada.
- **Servicio DNS IPv6: El servicio**DNS IPv6 al que se reenvía la solicitud de DNS para la aplicación especificada.

# Grupos de delegación de prefijos

October 31, 2022

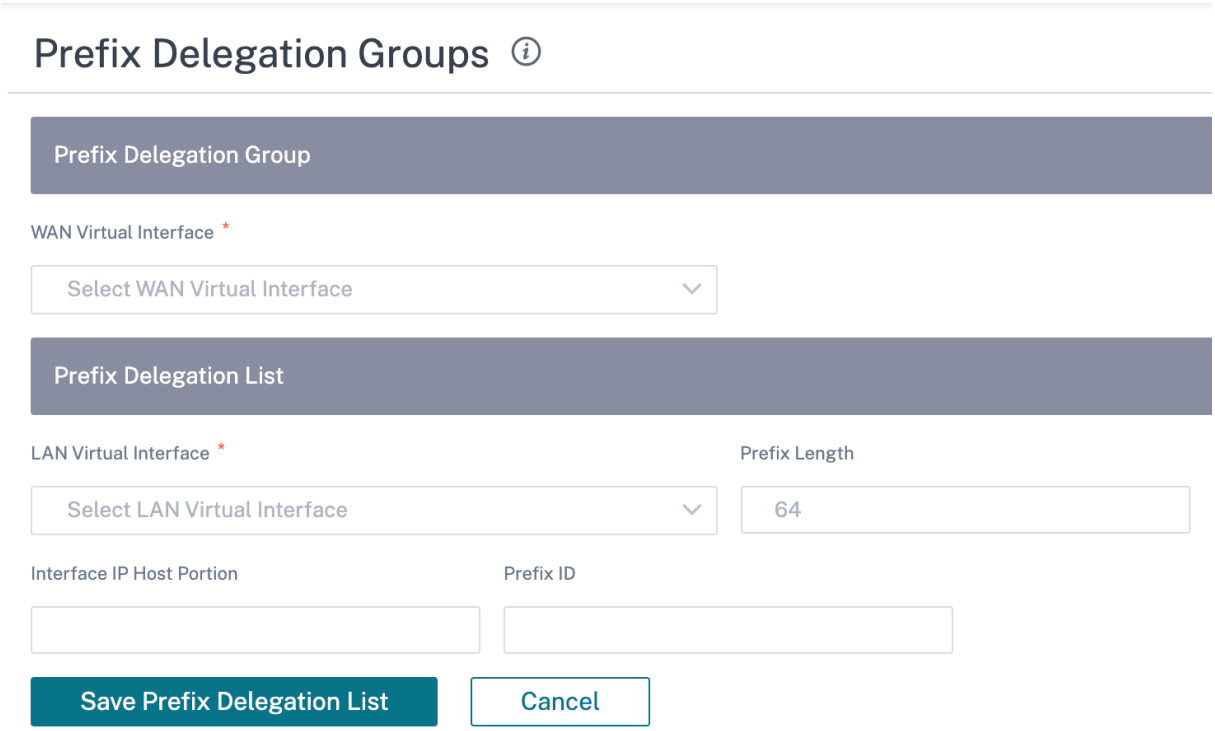
Los dispositivos Citrix SD-WAN se pueden configurar como un cliente DHCPv6 para solicitar un prefijo del ISP mediante el puerto WAN configurado. Una vez que el dispositivo Citrix SD-WAN recibe el prefijo, lo usa para crear un grupo de direcciones IP para atender a los clientes LAN. A continuación, el dispositivo Citrix SD-WAN se comporta como un servidor DHCP y anuncia el prefijo en los puertos LAN a los clientes de la LAN.

Para configurar la delegación de prefijos, vaya a **Configuración > Configuración > Configuración avanzada > Grupos de delegación de prefijos** y haga clic en **+ Grupos de delegación de prefijos**.

Elija una interfaz virtual WAN configurada en la que se solicite el prefijo al ISP y proporcione los siguientes detalles:

- **Interfaz Virtual LAN**: Seleccione una de las interfaces virtuales LAN configuradas para las que se solicita el prefijo.
- **Longitud de prefijo**: Número de bits de una dirección IPv6 de unidifusión global que forman parte del prefijo.
- **Parte de host IP de interfaz**: La parte del host que se va a utilizar para la dirección IP de la interfaz.
- **Id. de prefijo**: identificador único para identificar las solicitudes de delegación de prefijos para la interfaz LAN.




## Grupos de agregación de enlaces

October 31, 2022

La funcionalidad de grupos de agregación de vínculos (LAG) permite agrupar dos o más puertos en el dispositivo SD-WAN para que funcionen juntos como un solo puerto. Esto garantiza una mayor disponibilidad, redundancia de enlaces y performance mejorado.

Citrix SD-WAN Orchestrator para entornos locales admite grupos de agregación de enlaces simples (ACTIVE-BACKUP). Las negociaciones basadas en el protocolo 802.3ad LACP no se admiten en la versión actual. En cualquier momento, solo un puerto está activo y los otros puertos están en modo de copia de seguridad. Los soportes activos y de copia de seguridad se basan en el paquete Kit de desarrollo de planos de datos (DPDK) para la funcionalidad de LAG.

La funcionalidad LAG solo está disponible en las siguientes plataformas:

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 410 SE
- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 2100 SE/PE

- Citrix SD-WAN 4100 SE
- Citrix SD-WAN 5100 SE/PE
- Citrix SD-WAN 6100 SE/PE

> Nota
>
> - La funcionalidad LAG no es compatible con las plataformas VPX/VPXL.
> - Se admiten un mínimo de dos puertos y un máximo de cuatro puertos por LAG.
> - Todos los miembros de LAG deben ser del mismo tipo, por ejemplo, 1/1 o 1/2. 1/1 y 10/1 no son compatibles con la configuración de LAG.
> - La función de propagación del estado del enlace (LSP) no es compatible si los LAG se utilizan como interfaces Ethernet en los grupos de interfaces.

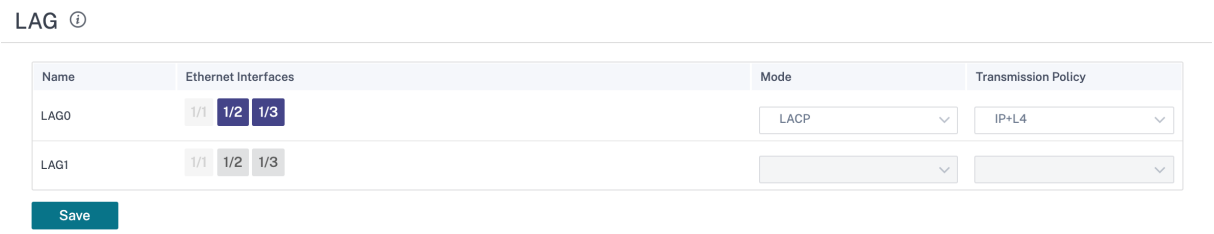
| Plataforma | Cantidad máxima de LAG admitidos | Puertos compatibles con LACP |
|---|---|---|
| 110 | 1 | 1/1 |
| 210 | 2 | 1/1 o 1/2 |
| 410 | 1 | 1/1 o 1/2 |
| 1100 | 3 | 1/1 o 1/2 |
| 2100 | 3 | 1/1 o 1/2 |

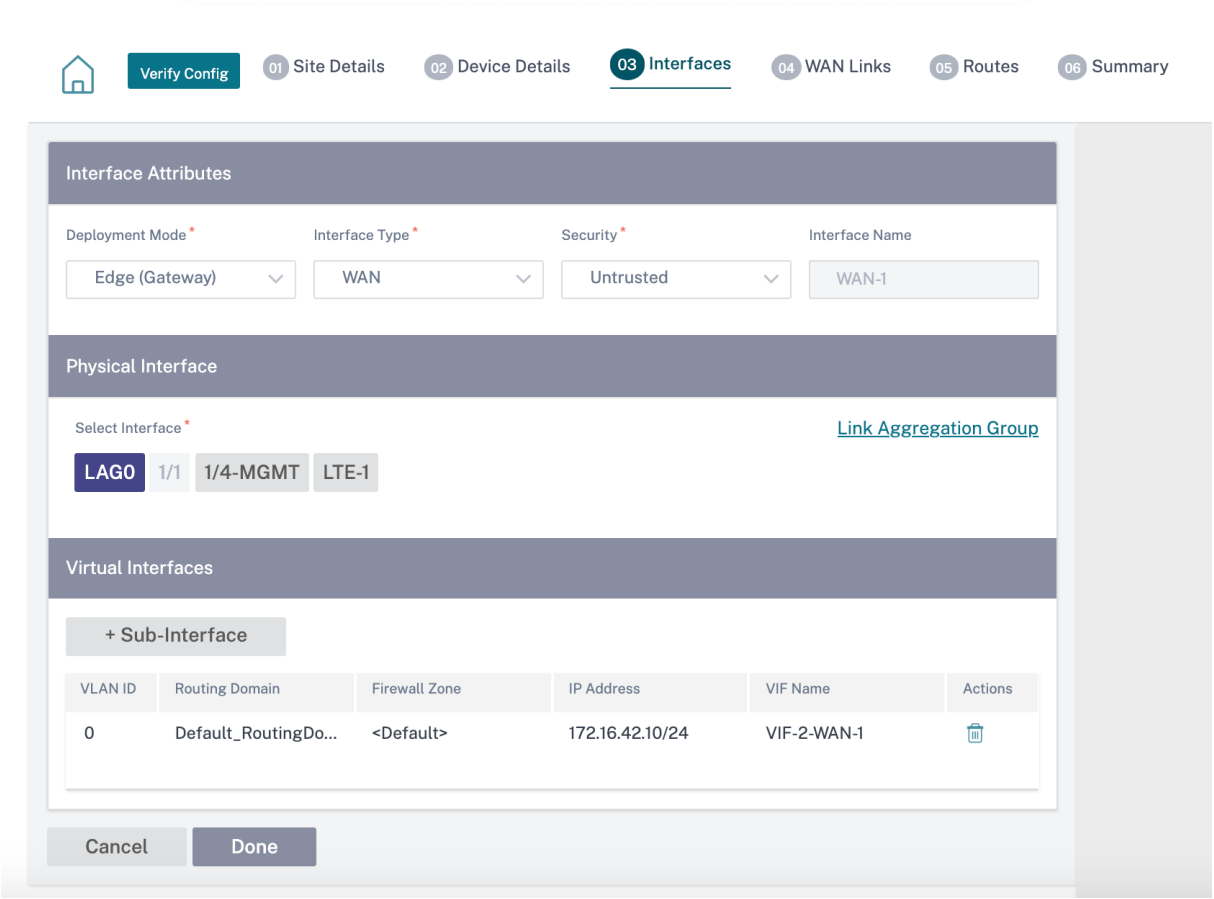
| Plataforma | Cantidad máxima de LAG admitidos | Puertos compatibles con LACP |
|---|---|---|
| 4100 | 4 | 1/1 o 1/2 |
| 5100 | 3 | 10/1 o 10/2 |
| 6100 | 4 | 1/1 o 1/2 |

Para configurar los grupos de agregación de enlaces, al nivel de sitio, vaya a **Configuración > Configuración > Configuración avanzada > LAG** y seleccione las interfaces Ethernet miembros para formar un grupo de agregación de enlaces.

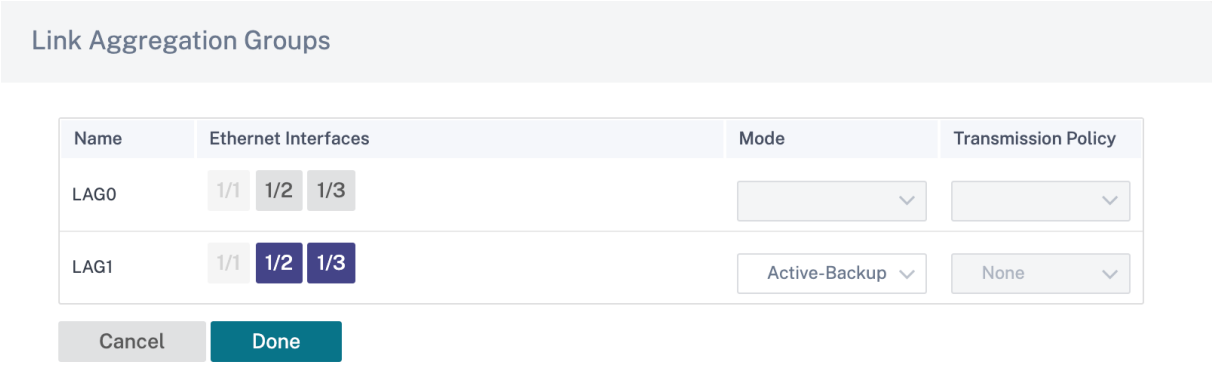



Una vez que los puertos se agreguen al LAG, puede seleccionar los LAG para configurar las interfaces en **Configuración del sitio**. Estas interfaces se utilizan además para configurar enlaces LAN/WAN y HA. No puede cambiar la configuración de los puertos miembros individuales, los cambios de configuración realizados en el LAG se envían automáticamente a los puertos miembros.




En la sección **Interfaces**, haga clic en **Grupo de agregación de enlaces** para cambiar rápidamente la configuración de LAG si es necesario.




Puede ver los detalles de las interfaces que están configuradas con LAG y LACP en **Informes > Informes de dispositivos > Grupo LAG LACP**. Para obtener más información, consulte Informesde dispositivos.

## Configuración del dispositivo

October 31, 2022

El servicio Citrix SD-WAN Orchestrator le permite configurar los ajustes del dispositivo al nivel de sitio y enviarlos a los dispositivos remotos.

Puede configurar el usuario, los adaptadores de red, NetFlow, AppFlow, SNMP, la configuración de respaldo y los ajustes del flujo de purga.

> **Nota**
>
> La opción de configurar los ajustes del dispositivo no está disponible al crear o modificar una plantilla de sitio.

Si ha configurado HA, seleccione el dispositivo principal o secundario para el que quiere cambiar la configuración del dispositivo.

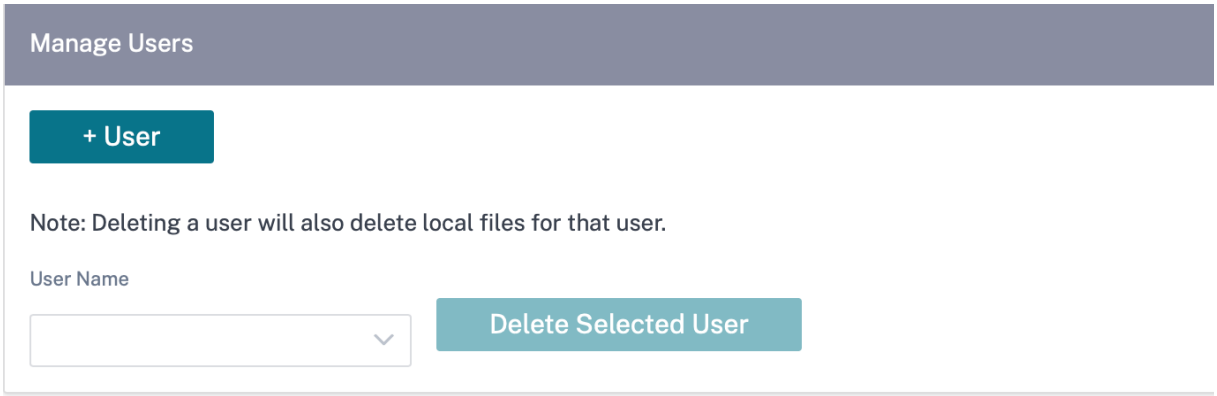

 

## Interfaz administrativa

La interfaz administrativa le permite agregar y administrar las cuentas de usuario locales y remotas. Las cuentas de usuario remoto se autentican a través de los servidores de autenticación RADIUS o TACACS+.

### Administrar usuarios

Puede agregar nuevas cuentas de usuario para el sitio. Para agregar un nuevo usuario, vaya a **Configuración > Configuracióndel dispositivo**>**Interfaz de administración**>**Administrar usuarios**y haga clic en**+Usuario**.

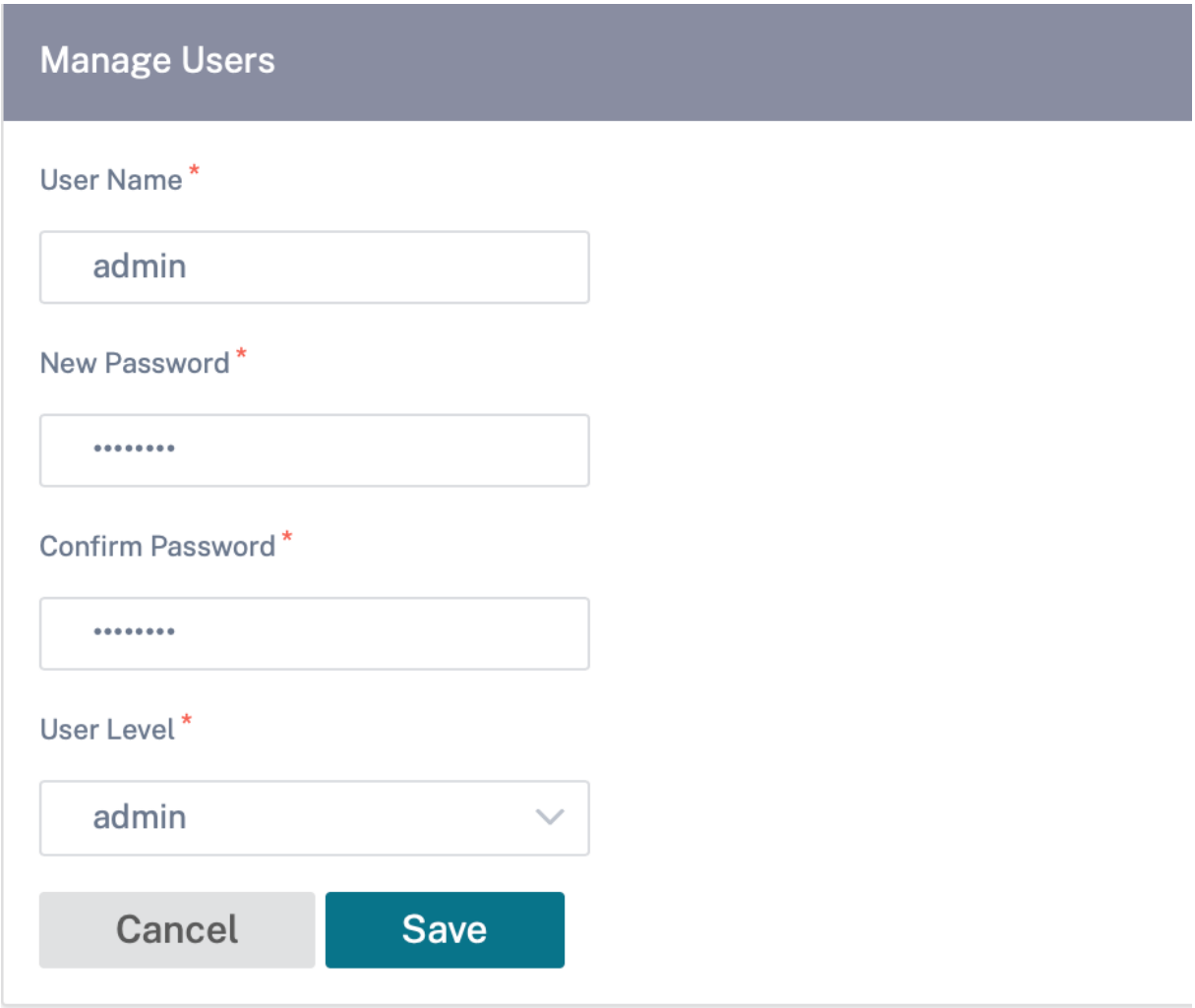



Proporcione los siguientes detalles:

- **Nombre de usuario**: El nombre de usuario de la cuenta de usuario.
- **Nueva contraseña**: La contraseña de la cuenta de usuario.
- **Confirme la contraseña**: vuelva a introducir la contraseña para confirmarla.
- **Nivel de usuario**: Seleccione uno de los siguientes privilegios de cuenta:
  - **Administrador**: Una cuenta de administrador tiene acceso de lectura y escritura a todos los ajustes. Un administrador puede realizar la configuración y la actualización de software en la red.
  - **Visor**: Una cuenta de espectador es una cuenta de solo lectura con acceso a las secciones Panel, Informes y Supervisión.
  - Administrador de**red**: Un administrador de red tiene acceso de lectura y escritura a la configuración de red y acceso de solo lectura para otros ajustes.
  - Administrador**de seguridad**: Un administrador de seguridad tiene acceso de lectura y escritura para la configuración relacionada con el firewall o la seguridad, acceso de solo lectura para otras configuraciones.

> **Nota**
>
> El administrador de seguridad tiene la autoridad para inhabilitar el acceso de escritura al firewall para otros usuarios (administrador/visor).




Para eliminar un usuario, seleccione un nombre de usuario y haga clic en **Eliminar usuario seleccionado**. Se eliminan la cuenta de usuario y los archivos locales.

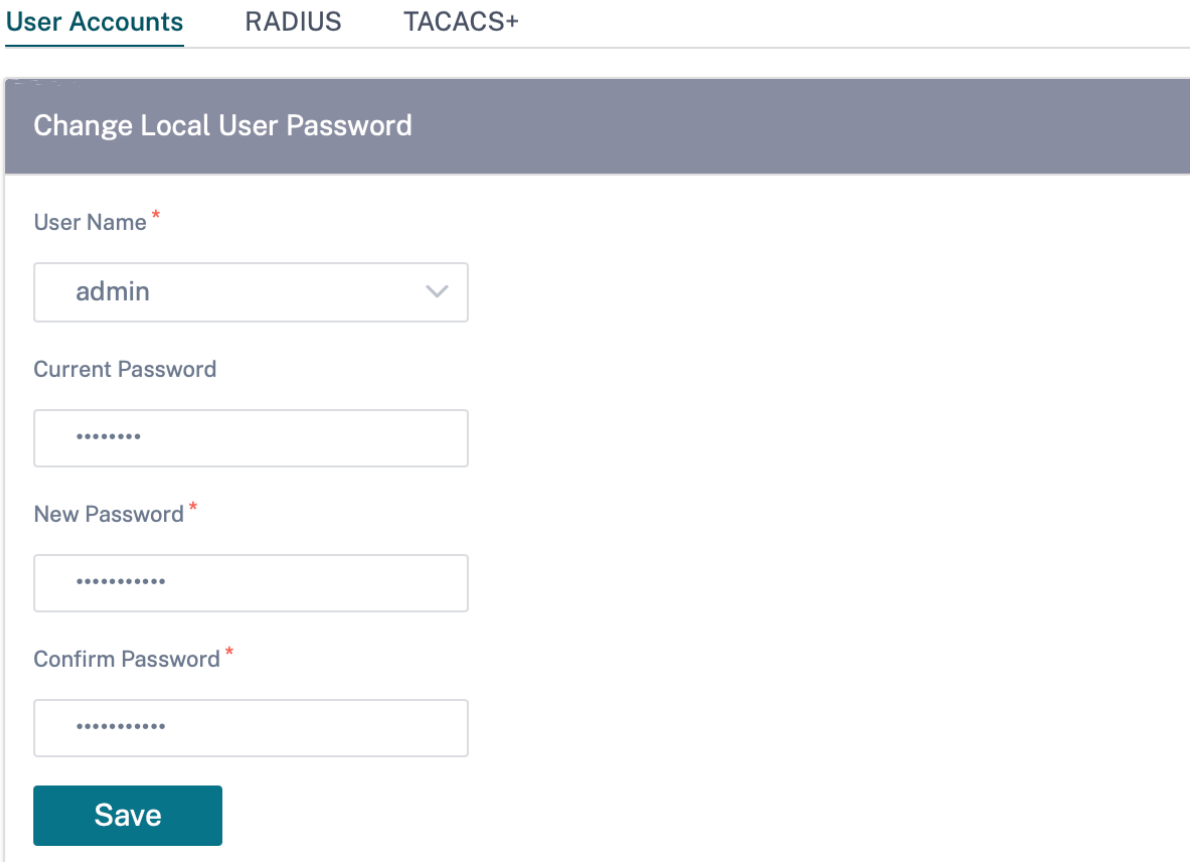
#### Cambiar contraseña de usuario local

Para cambiar la contraseña del usuario local, vaya a **Configuración** > **Configuración del dispositivo** > **Interfaz administrativa** > **Cuentas de usuario** > **Cambiar contraseña de usuario local** e introduzca los siguientes valores:

- **Nombre de usuario**: S eleccione un nombre de usuario para el que quiera cambiar la contraseña de la lista de usuarios configurada en el sitio.

- **Contraseña actual**: Introduzca la contraseña actual. Este campo es opcional para usuarios administradores.
- **Contraseña nueva**: introduzca una contraseña nueva de su elección.
- **Confirme la contraseña**: vuelva a introducir la contraseña para confirmarla.




### Servidor de autenticación RADIUS

RADIUS habilita la autenticación remota de usuarios en el dispositivo. Para utilizar la autenticación RADIUS, debe especificar y configurar al menos un servidor RADIUS. Opcionalmente, puede configurar servidores RADIUS de copia de seguridad redundantes, hasta un máximo de tres. Los servidores se comprueban secuencialmente. Asegúrese de que las cuentas de usuario necesarias se crean en el servidor de autenticación RADIUS.

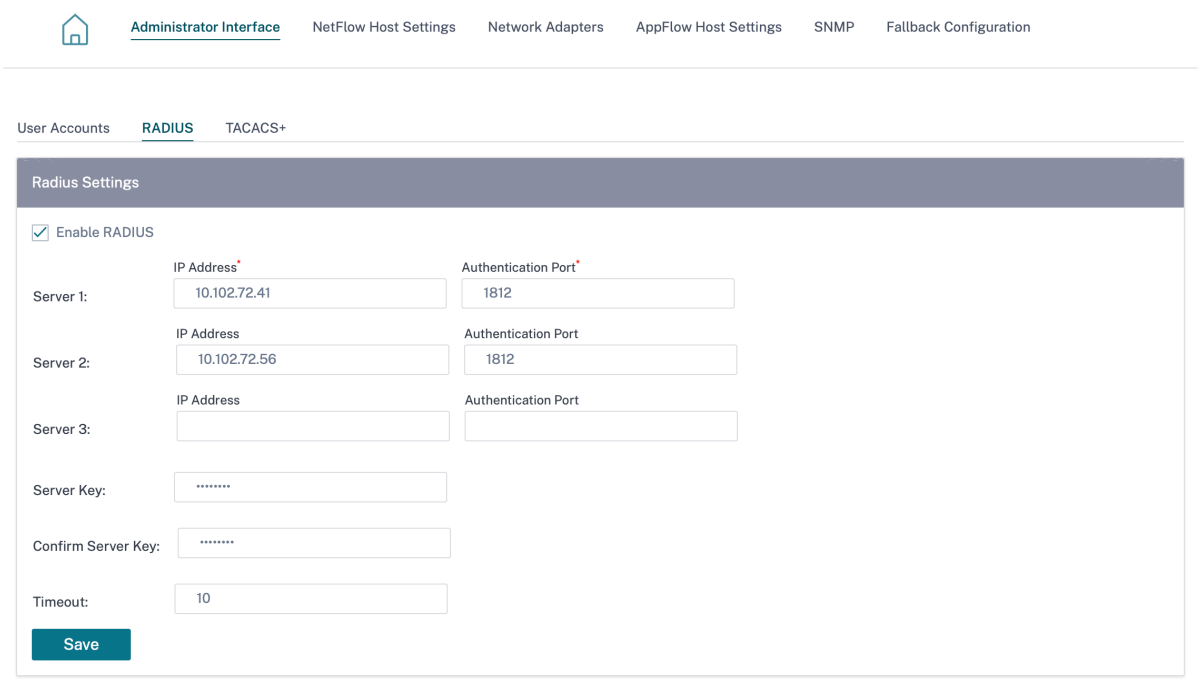
Para configurar la autenticación RADIUS, vaya a **Configuración** > **Configuración del dispositivo** > **Interfaz administrativa** > **RADIUS**y haga clic en **Habilitar RADIUS**.

> **Nota**
>
> Puede habilitar la autenticación RADIUS o TACACS+ en un sitio. No se pueden habilitar ambos al mismo tiempo.

Proporcione la dirección IP del host del servidor RADIUS y el número de puerto de autenticación. El número de puerto predeterminado es 1812. Introduzca una clave de servidor y confirme que es una clave secreta utilizada para conectarse al servidor RADIUS. Especifique el intervalo de tiempo a esperar una respuesta de autenticación del servidor RADIUS. El valor de tiempo de espera debe ser menor o igual a 60 segundos.

> **Nota**
>
> La configuración de **clave de servidor** y **tiempo** de espera se aplica a todos los servidores configurados.




## Servidor de autenticación TACACS+

TACACS+ habilita la autenticación remota de usuarios en el dispositivo. Para utilizar la autenticación TACACS+, debe especificar y configurar al menos un servidor TACACS+. Opcionalmente, puede configurar servidores TACACS+ de copia de seguridad redundantes, hasta un máximo de tres. Los servidores se comprueban secuencialmente. Asegúrese de que las cuentas de usuario necesarias se crean en el servidor de autenticación TACACS+.

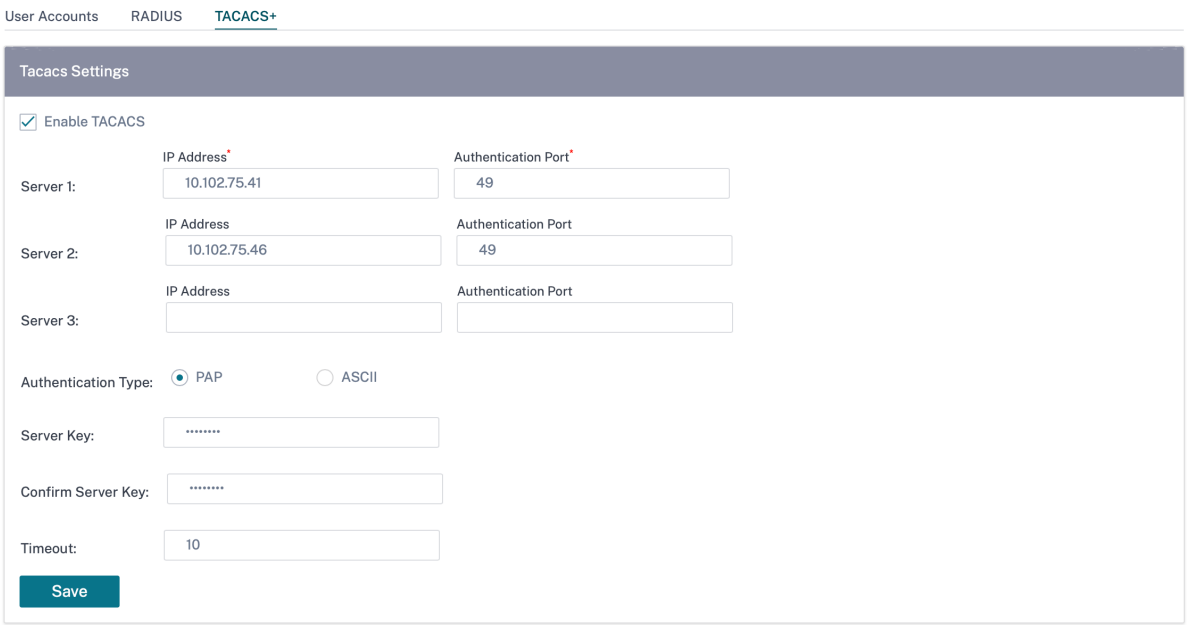
 

Para configurar la autenticación TACACS+, vaya a **Configuración > Configuracióndel dispositivo**>**Interfaz administrativa**>**TACACS+**y haga clic en**Habilitar TACACS+**.

> **Nota**
>
> Puede habilitar la autenticación RADIUS o TACACS+ en un sitio. No se pueden habilitar ambos al mismo tiempo.

1. Seleccione el método de cifrado para enviar el nombre de usuario y la contraseña al servidor TACACS+.
2. Proporcione la dirección IP del host del servidor TACACS+ y el número de puerto de autenticación. El número de puerto predeterminado es 49.
3. Introduzca una clave de servidor y confírmela. Es una clave secreta que se utiliza para conectarse al servidor TACACS+.
4. Especifique el intervalo de tiempo a esperar una respuesta de autenticación desde el servidor TACACS+. El valor de tiempo de espera debe ser menor o igual a 60 segundos.

> **Nota**
>
> La **configuración del**tipo de autenticación**, la**clave del servidor**y el tiempo** de espera se aplican a todos los servidores configurados.




## Configuración del host de NetFlow

Los recopiladores de NetFlow recopilan el tráfico de red IP a medida que entra o sale de una interfaz SD-WAN. Puede determinar el origen y el destino del tráfico, la clase de servicio y las causas de la con-

gestión del tráfico mediante los datos de NetFlow. Para obtener más información, consulte Multiple NetFlow Collector.

Puede configurar hasta tres hosts NetFlow. Para configurar los ajustes del host de NetFlow, vaya a **Configuración > Configuracióndel dispositivo > Configuración delhost de NetFlow**. Seleccione **Activar NetFlow** y proporcione la dirección IP y el número de puerto del host de NetFlow.

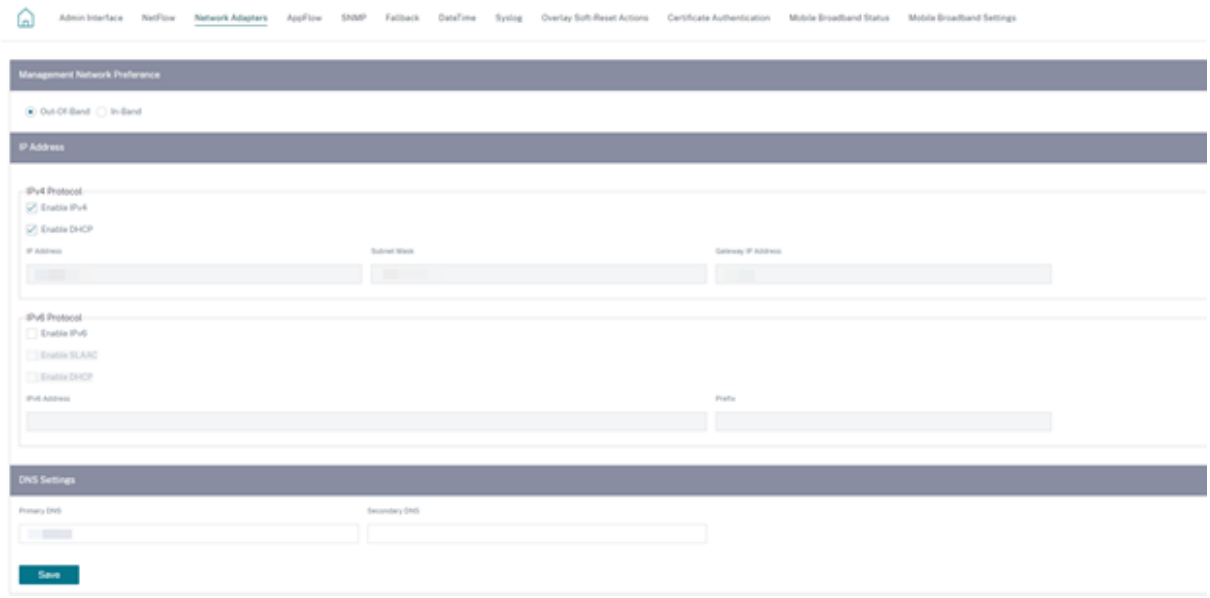

## Adaptadores de red

Para los dispositivos Citrix SD-WAN, puede cambiar manualmente las preferencias de la red de administración, la dirección IP de administración y otros parámetros de la red. Puede cambiar la dirección IPv4, la máscara de subred, la dirección IP de la puerta de enlace, la dirección IPv6 y el prefijo del dispositivo u obtener la dirección IP automáticamente habilitando DHCP o SLAAC (solo para direcciones IPv6). Para obtener más información, consulte Protocolo de configuración de host dinámico.

> **Nota**
>
> - No puede cambiar la dirección IP si la interfaz se utiliza para la administración dentro de banda. Para obtener más información sobre la administración dentro de banda, consulte Administración dentro de banda.
> - La opción Dentro de banda solo funciona si ha configurado un puerto de datos como puerto de administración en banda y si está configurado el servicio de Internet. Asegúrese de que tiene la configuración necesaria para admitir la administración en banda del dispositivo SD-WAN antes de configurar la preferencia de administración.
> - La sección Preferencias de red de administración (dentro y fuera de banda) está visible si el dispositivo ejecuta una versión de software de 11.4.2 o posterior.

Para configurar los ajustes del adaptador de red, vaya a **Configuración > Configuracióndel dispositivo**>**Adaptador de red**.



### Configuración del host de AppFlow

AppFlow e IPFIX son estándares de exportación de flujos utilizados para identificar y recopilar datos de aplicaciones y transacciones en la infraestructura de red. Estos datos ofrecen una mejor visibilidad de la utilización y el rendimiento del tráfico de aplicaciones.

Los datos recopilados, denominados registros de flujo, se transmiten a uno o más recopiladores IPv4. Los recopiladores agregan los registros de flujo y generan informes históricos o en tiempo real. Para obtener más información, consulte AppFlow e IPFIX.

### SNMP

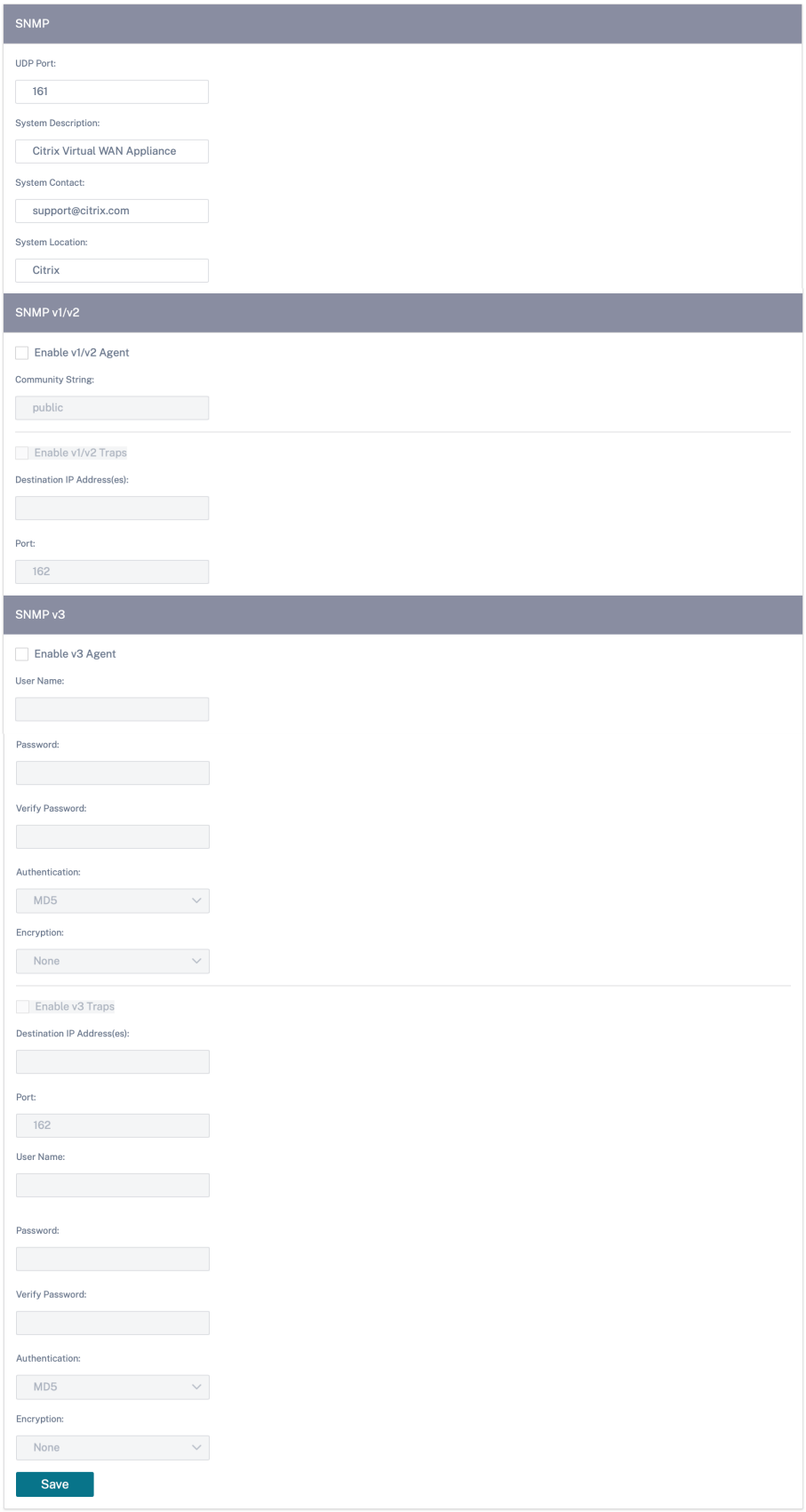
SNMP se utiliza para intercambiar información de administración entre dispositivos de red. SNMPv1 es la primera versión del protocolo SNMP. SNMPv2 es el protocolo revisado, que incluye mejoras en los tipos de paquetes de protocolo, asignaciones de transporte y elementos de estructura MIB. SNMPv3 define la versión segura del SNMP. El protocolo SNMPv3 también facilita la configuración remota de las entidades SNMP.

El agente SNMP recopila la información de administración del dispositivo localmente y la envía al administrador de SNMP cada vez que se consulta. Si el agente detecta un evento de emergencia en el dispositivo, envía un mensaje de advertencia al administrador sin esperar a que se le consulte los datos. Este mensaje de emergencia se llama trampa. Habilite los agentes de versión SNMP necesarios, las capturas correspondientes, y proporcione la información requerida. Para obtener más información, consulte SNMP.

Para configurar los ajustes de SNMP, vaya a **Configuración** > **Configuración del dispositivo** > **SNMP**



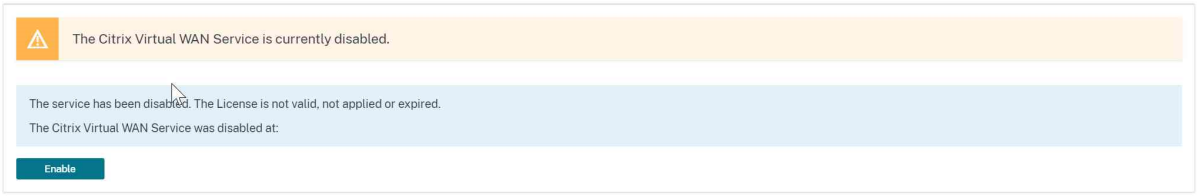

 

### Configuración de reserva

La configuración de reserva garantiza que el dispositivo permanezca conectado al servicio de implementación sin contacto si hay un error de vínculo, falta de configuración o falta de software. La configuración de reserva está habilitada de forma predeterminada en los dispositivos que tienen un perfil de configuración predeterminado. También puede modificar la configuración de reserva según la configuración de red LAN existente. Para obtener más información, consulte Configuración alternativa.

### Flujos

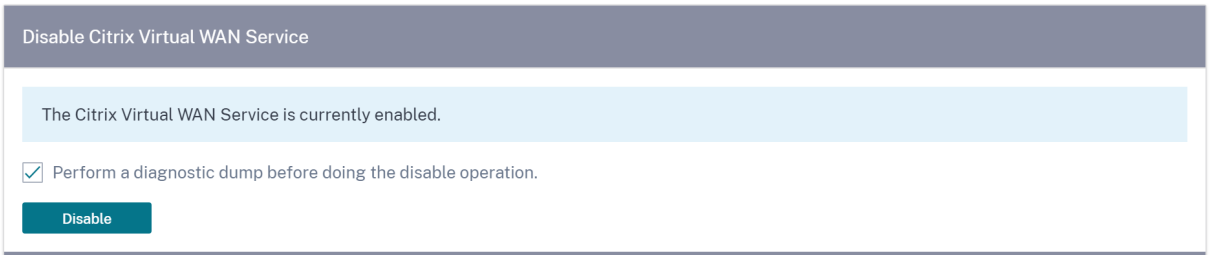
La sección de flujos le permite habilitar o inhabilitar el servicio Citrix Virtual WAN en el dispositivo. Al habilitar el servicio se habilita e inicia el daemon de la WAN virtual. Hay una opción para habilitar el servicio Citrix Virtual Wan si el servicio está inhabilitado.




#### Inhabilitar el servicio Citrix Virtual WAN

La opción **Inhabilitar el servicio Citrix Virtual WAN** está disponible si el servicio está habilitado. Al inhabilitar el servicio, se detiene el daemon WAN virtual en el dispositivo.

Puede optar por recopilar un volcado de diagnóstico de la red WAN virtual antes de inhabilitar el servicio Citrix Virtual WAN.

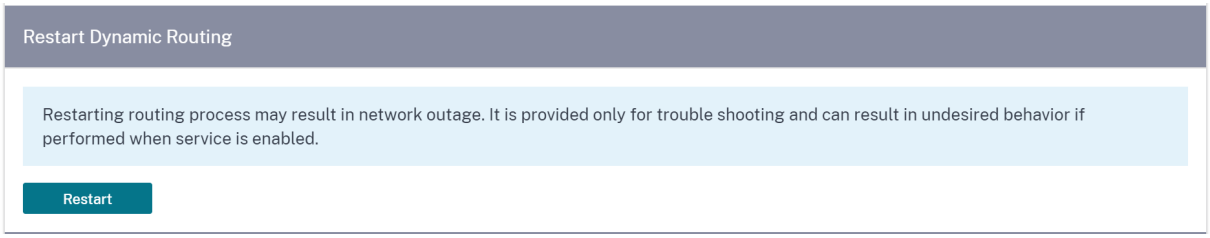



#### Reiniciar el enrutamiento dinámico

Puede reiniciar el proceso de aprendizaje dinámico de rutas mediante los protocolos de enrutamiento OSPF y BGP. La opción de reinicio del enrutamiento dinámico se proporciona únicamente para solucionar problemas.

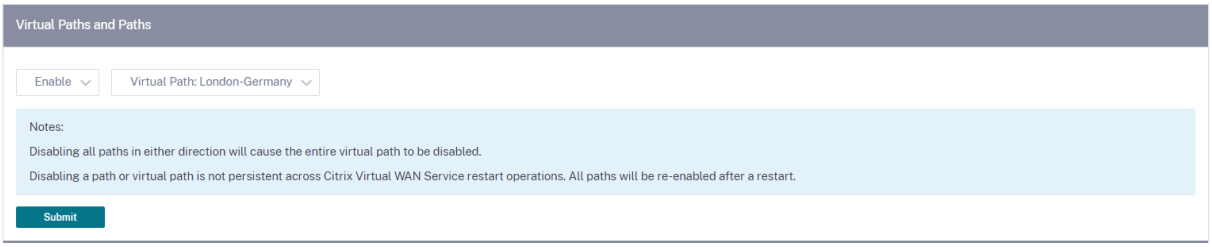
> **Advertencia**
>
> El reinicio del enrutamiento dinámico podría provocar una interrupción de la red.




### Rutas virtuales

Puede optar por habilitar o inhabilitar la ruta virtual entre dos sitios. Puede elegir las rutas individuales subyacentes, en cualquier dirección, o la ruta virtual superpuesta. Al inhabilitar las rutas individuales, se inhabilita toda la ruta virtual.

> **Nota**
>
> Todas las rutas se vuelven a habilitar después de reiniciar el servicio Citrix Virtual WAN.

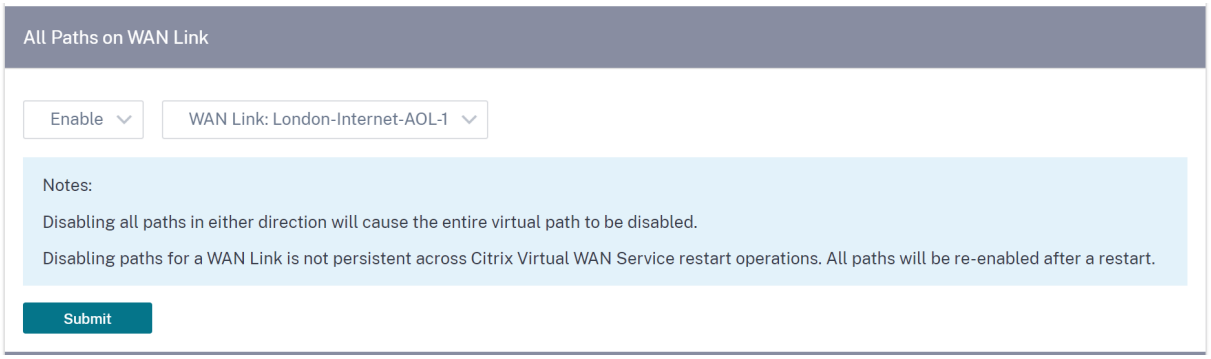



### Todas las rutas en el enlace WAN

Puede optar por habilitar o inhabilitar los enlaces WAN entre dos sitios. Al inhabilitar todos los enlaces WAN, se inhabilita la ruta virtual.

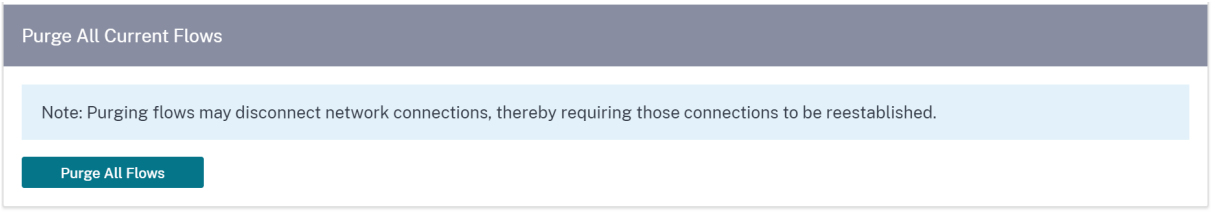
> **Nota**
>
> Todos los enlaces WAN se vuelven a habilitar después de reiniciar el servicio Citrix Virtual WAN.




### Purgar todos los flujos de corriente

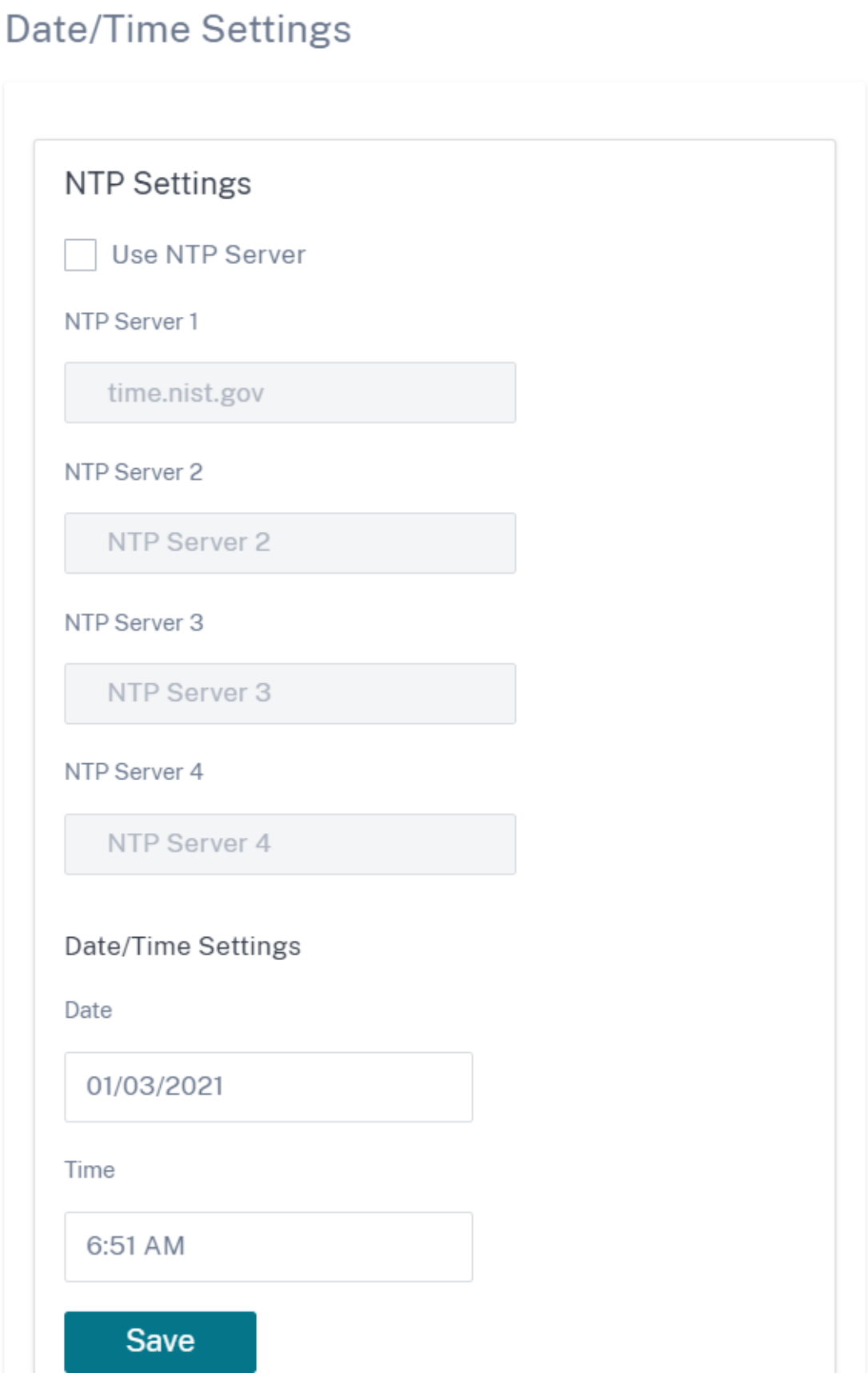
Al purgar los flujos, se finalizan todos los flujos actuales, se borran las tablas de flujo, se restablecen las conexiones de flujo y se vuelve a rellenar la tabla de flujo.




### Fecha y hora

Puede cambiar la fecha y la hora del dispositivo de forma manual o mediante un servidor NTP. Para configurar la fecha y la hora manualmente, asegúrese de que la opción **Usar servidor NTP** no esté seleccionada y proporcione la fecha y la hora.

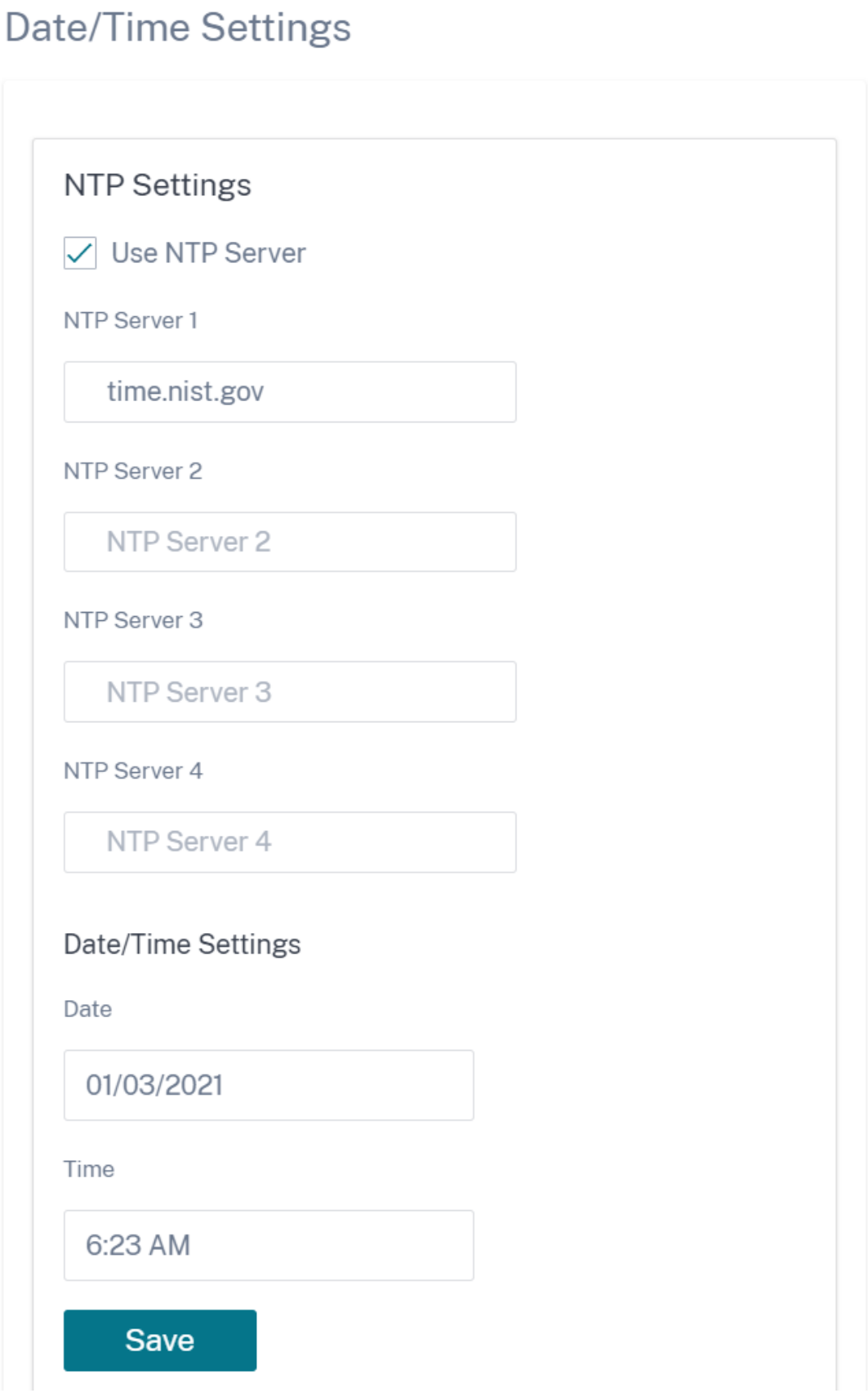
 



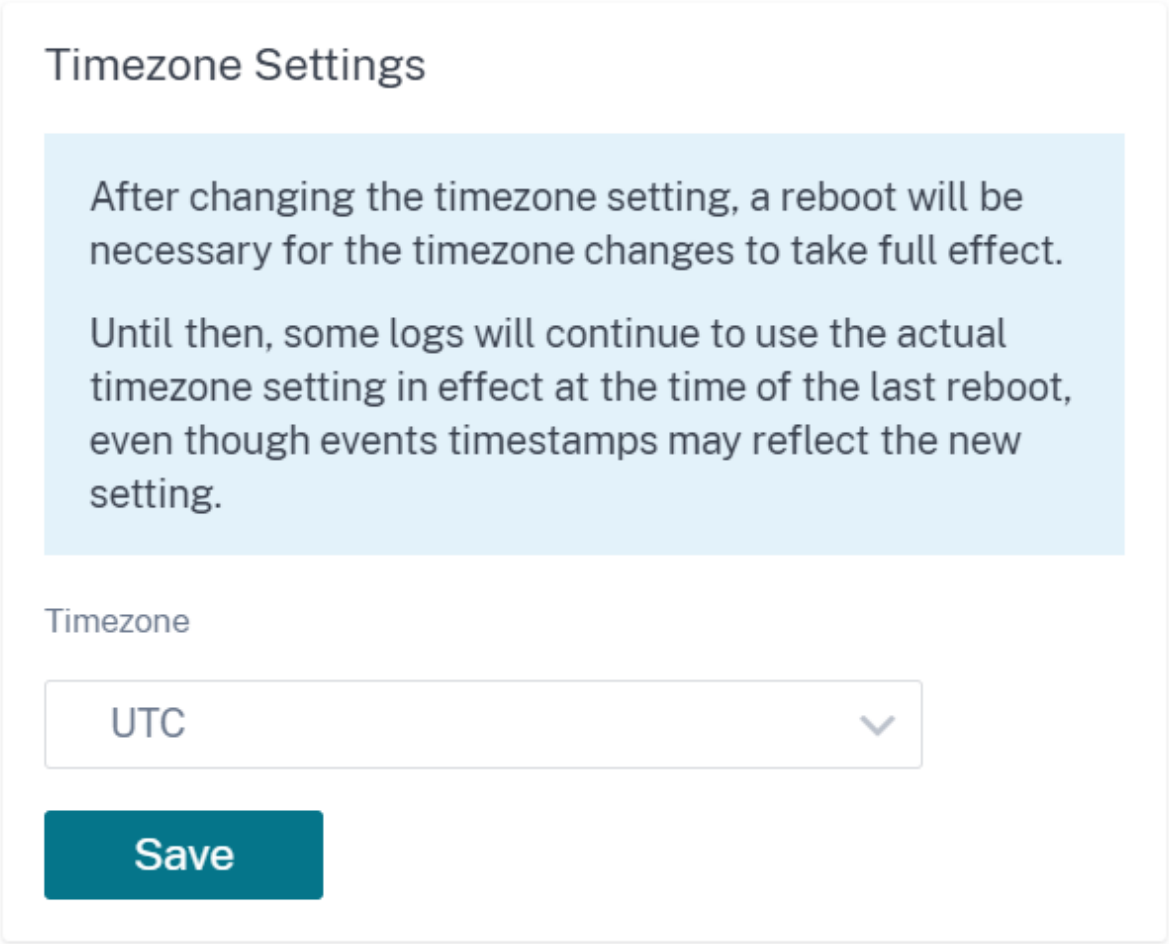
Si selecciona la opción **Usar servidor NTP**, no podrá introducir manualmente la fecha y la hora actuales. Puede especificar hasta 4 servidores NTP, pero debe especificar al menos uno. Actúan como servidores NTP de respaldo. Si un servidor está inactivo, el dispositivo se sincroniza automáticamente con el otro servidor NTP. Si especifica un nombre de dominio para un servidor NTP, también debe configurar un servidor DNS a menos que ya lo haya hecho.



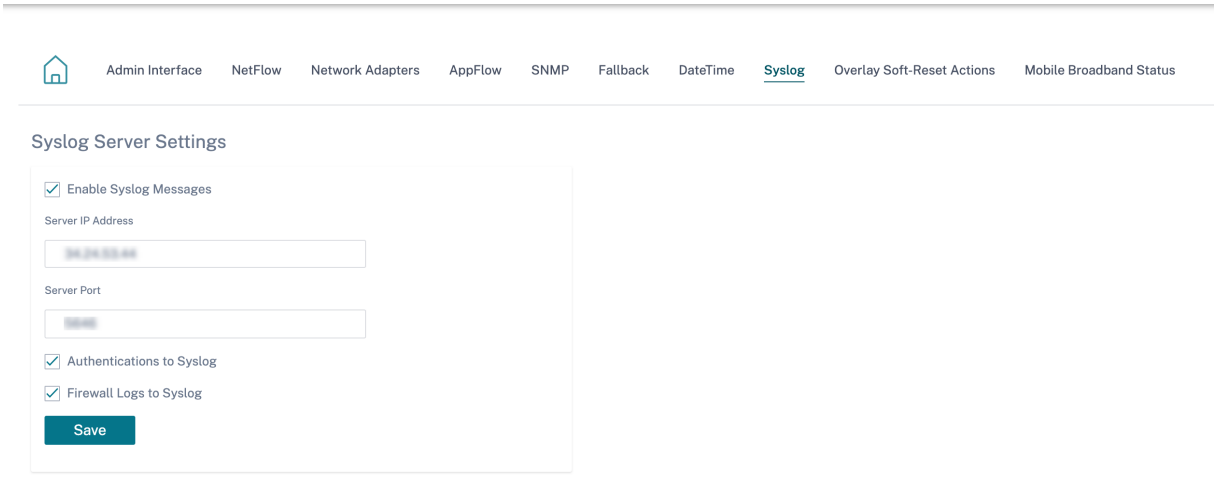
Si es necesario cambiar la zona horaria, cámbiela antes de configurar la fecha y la hora o, de lo contrario, la configuración no se mantendrá. Reinicie el dispositivo después de cambiar la zona horaria.




### Configuración del servidor Syslog

Puede configurar los ajustes del servidor Syslog de los dispositivos SD-WAN mediante el servicio Citrix SD-WAN Orchestrator. Al habilitar la configuración de Syslog, puede enviar alertas del sistema y detalles de eventos de los dispositivos SD-WAN a un servidor Syslog externo. Sin embargo, debe seleccionar el tipo de evento en la interfaz de usuario del dispositivo SD-WAN yendo a **Configuración** > **Configuración del dispositivo** > **Registración/supervisión** > **Opciones de alarma**. Para obtener más información, consulte Configurar alarmas.




Los siguientes ajustes del servidor Syslog se pueden configurar mediante el servicio Citrix SD-WAN Orchestrator:

- **Habilitar los mensajes de Syslog**: habilite o inhabilite el envío de registros o mensajes de eventos al servidor Syslog.
- **Dirección IP del servidor**: Dirección IP del servidor Syslog.
- **Puerto del servidor**: Número de puerto del servidor Syslog.
- **Autenticación en Syslog**: habilite o inhabilite el envío de registros de autenticación o mensajes de eventos al servidor Syslog.
- **Registros de firewall en Syslog**: habilite o inhabilite el envío de registros de firewall al servidor Syslog.

## Autenticación de certificados

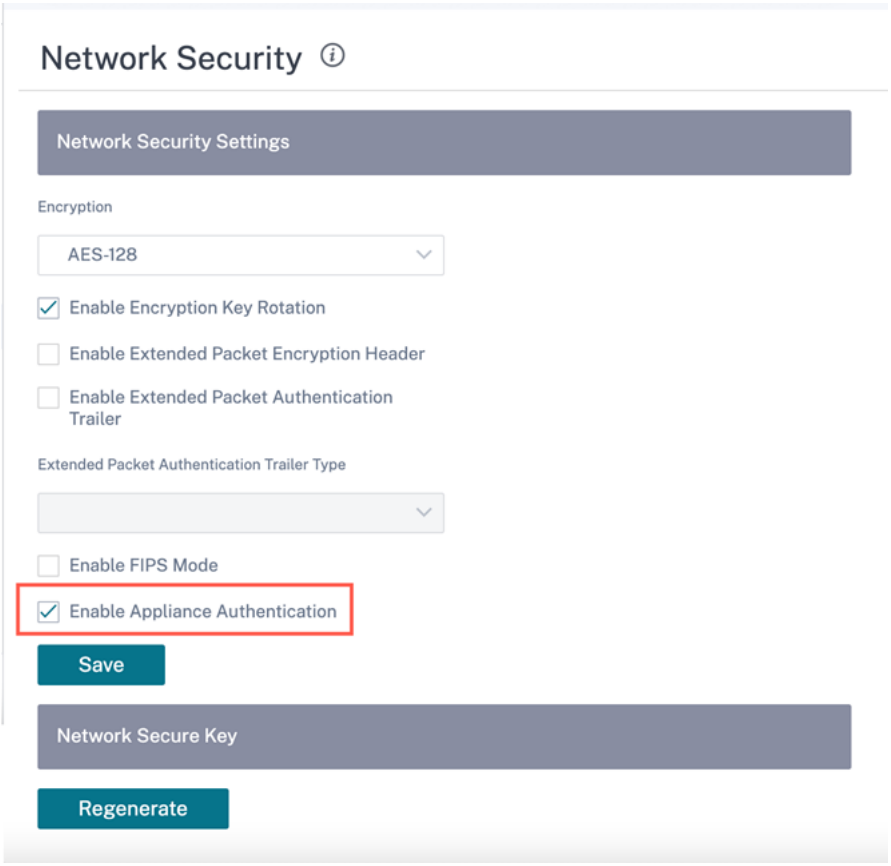
El servicio Citrix SD-WAN Orchestrator garantiza que se establezcan rutas seguras entre los dispositivos de la red SD-WAN mediante el uso de técnicas de seguridad como el cifrado de red y los túneles IPSec de rutas virtuales. Además de las medidas de seguridad existentes, la autenticación basada en certificados se introduce en el servicio Citrix SD-WAN Orchestrator.

La autenticación de certificados permite a las organizaciones usar certificados emitidos por su autoridad de certificación (CA) privada para autenticar los dispositivos. Los dispositivos se autentican antes de establecer las rutas virtuales. Por ejemplo, si un dispositivo de sucursal intenta conectarse al centro de datos y el certificado de la sucursal no coincide con el certificado que espera el centro de datos, no se establece la ruta virtual.

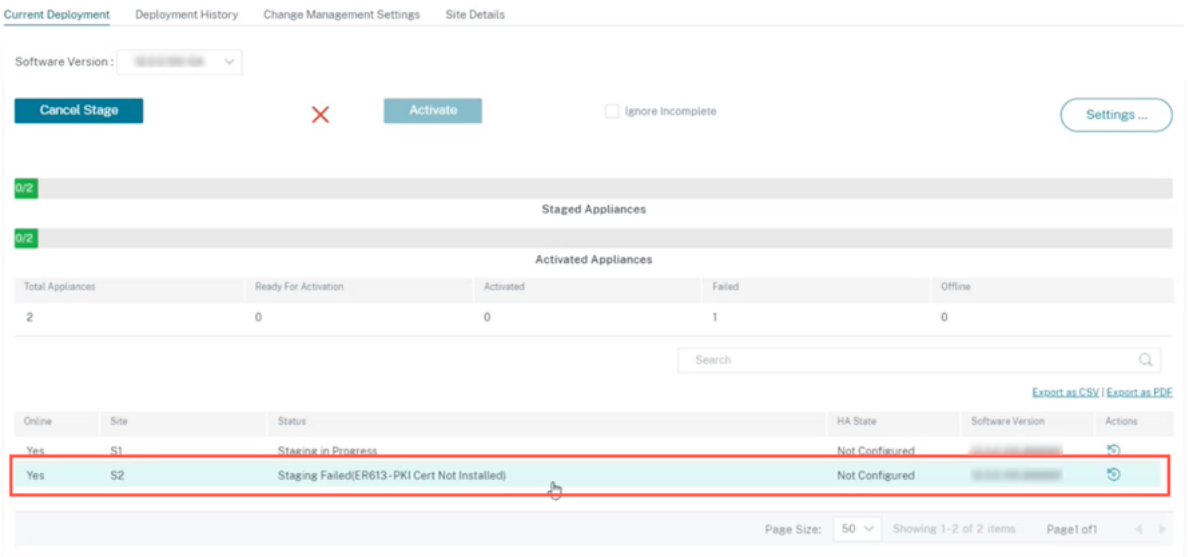
El certificado emitido por la entidad emisora de certificados vincula una clave pública al nombre del dispositivo. La clave pública funciona con la clave privada correspondiente que posee el dispositivo identificado por el certificado.

Para habilitar la autenticación del dispositivo, al nivel de red, vaya a **Configuración** > **Seguridad** > **Seguridad** de **red** y seleccione **Habilitar la autenticación del dispositivo**. Haga clic en **Guardar**.



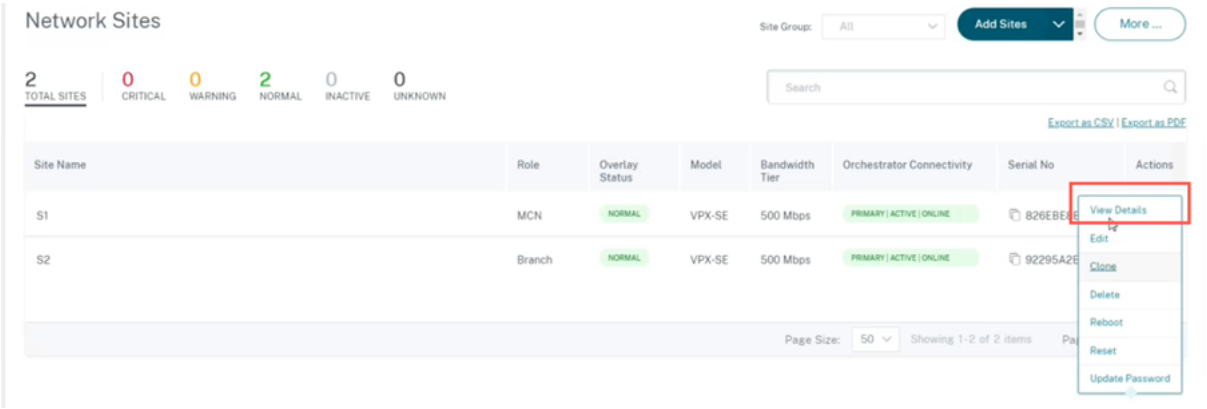

Durante la implementación, si la autenticación del dispositivo está habilitada pero no hay ningún certificado de PKI instalado en el dispositivo, la configuración provisional muestra el estado de error.



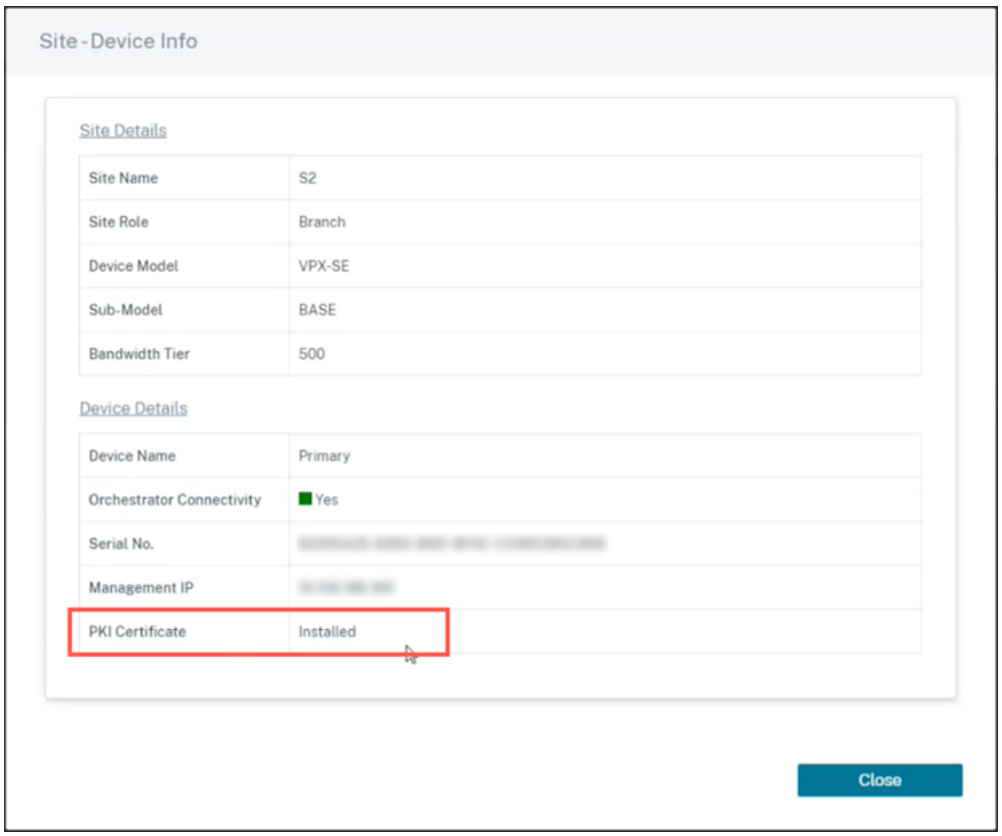

 

### Ver certificado

Puede ir a la página de detalles del dispositivo para comprobar si el certificado de PKI está instalado o no. Para hacerlo, vaya a **Configuración** > **Red principal** > haga clic en el símbolo de **acción** del sitio en el que quiere verificar el certificado > haga clic en **Ver detalles**.




La siguiente pantalla se completa con los detalles del sitio y del dispositivo:

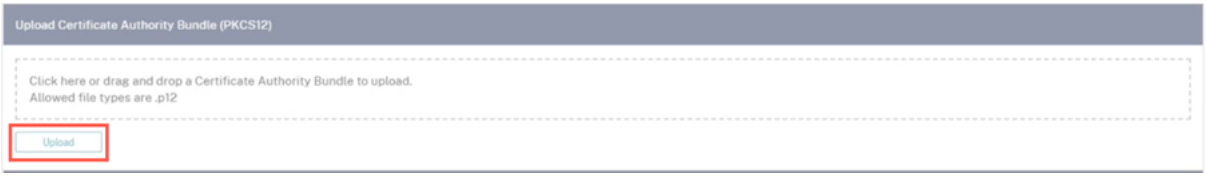



En la sección **Detalles del dispositivo**, puede ver el estado de instalación del certificado PKI.

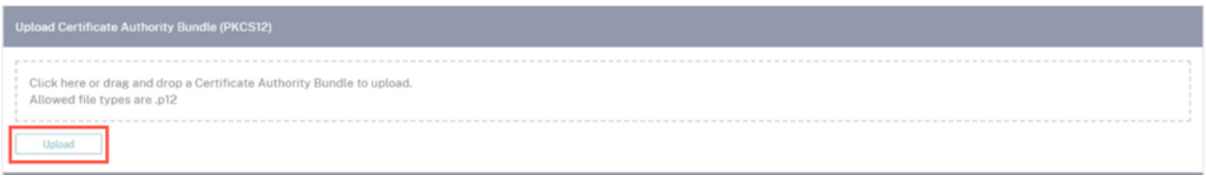
### Cargar paquete de identidad

El paquete Identidad incluye una clave privada y el certificado asociado a la clave privada. Puede cargar el certificado del dispositivo emitido por la CA en el dispositivo. El paquete de certificados es un archivo PKCS12 con la extensión.p12. Puede elegir protegerlo con una contraseña. Arrastre y suelte el archivo PKCS12, introduzca una contraseña y haga clic en **Cargar**. Si deja el campo de contraseña en blanco, se considerará que no está protegido por contraseña.




### Subir paquete de entidad emisora de certificados

Cargue el paquete PKCS12 que corresponde a la autoridad de firma del certificado. El paquete de la autoridad de certificación incluye la cadena completa de firmas, la autoridad raíz y toda la autoridad signataria intermedia. Arrastre el paquete PKCS12 y haga clic en **Cargar**




### Crear solicitud de firma de certificación

El dispositivo puede generar un certificado sin firmar y crear una solicitud de firma de certificados (CSR). Para crear una CSR para un dispositivo, proporcione el nombre de la organización, la unidad, el pueblo o la ciudad, la provincia/región/condado/ciudad, el país y la dirección de correo electrónico. El nombre común del dispositivo es el nombre del sitio que se rellena automáticamente y no se puede modificar. Haga clic en **Crear CSR**.

### Administrar la solicitud de firma de certificados

Una vez que la CSR se haya generado correctamente desde el servidor, debe descargar la CSR del dispositivo y conseguir que su CA la firme y volver a cargarla en el dispositivo en formatos PEM o DER. Se utiliza como certificado de identidad para el dispositivo. En primer lugar, cargue la CA para firmar el certificado.


Una vez cargada la CA, suba la CSR firmada.


### Administrador de listas de revocación de certificados

Una lista de revocación de certificados (CRL) es una lista publicada de números de serie de certificados que ya no son válidos en la red. El archivo CRL se descarga periódicamente y se almacena localmente en todo el dispositivo. Cuando se autentica un certificado, el respondedor examina la CRL para ver si el certificado de iniciadores ya se revocó. Citrix SD-WAN admite actualmente CRL de la versión 1 en formato PEM y DER.

Para habilitar la CRL, active la casilla de verificación CRL habilitada. Indique la ubicación en la que se mantiene el archivo CRL. Se admiten ubicaciones HTTP, HTTPS y FTP. Especifique el intervalo de tiempo para comprobar y descargar el archivo CRL, el intervalo es de 1 a 1440 minutos. Haga clic en **Configuración de carga**.

> **Nota**
>
> El período de reautenticación de una ruta virtua1 puede oscilar entre 10 y 15 minutos. Si el intervalo de actualización de la CRL se establece en una duración más corta, la lista de CRL actualizada puede incluir un número de serie actualmente activo. Haga que un certificado revocado activamente esté disponible en su red por un período breve.

## Configuración de banda ancha móvil

El servicio Citrix SD-WAN Orchestrator le permite conectar un dispositivo Citrix SD-WAN desde su sucursal a una red mediante una conexión de banda ancha móvil.

Para configurar los ajustes de banda ancha móvil, al nivel de sitio, vaya a **Configuración > Configuracióndel dispositivo > Configuración**de**banda ancha móvil**.

Actualmente, los ajustes de banda ancha móvil se pueden configurar en los dispositivos Citrix SD-WAN 110 y Citrix SD-WAN-210.

Puede configurar los siguientes ajustes de banda ancha móvil en el servicio Citrix SD-WAN Orchestrator.

### Estado PIN de la SIM

Si ha insertado una tarjeta SIM que está bloqueada con un PIN, el estado de la SIM es **Habilitada**. No puede usar la tarjeta SIM hasta que se verifique con el PIN de la SIM. Puede obtener el PIN de la tarjeta SIM del operador. Haga clic en **Verificar**.

Introduzca el PIN de la SIM proporcionado por el operador y haga clic en **Verificar**.

**Inhabilitar PIN de la SIM** Puede inhabilitar la función del PIN de la SIM para una tarjeta SIM para la que el PIN de la SIM esté activado y verificado. Haga clic en **Inhabilitar**. Introduzca el PIN de la SIM y haga clic en **Desactivar**

**Habilitar PIN de la SIM** Para habilitar el PIN de la SIM, haga clic en **Activar**. Introduzca el PIN de la tarjeta SIM proporcionado por el operador y haga clic en **Habilitar**.

Si el estado del PIN de la SIM cambia a **Activado y No verificado**, significa que el PIN no está verificado y que no puede realizar ninguna operación hasta que se verifique el PIN.

Haga clic en **Verificar PIN**. Introduzca el PIN de la SIM proporcionado por el operador y haga clic en **Verificar PIN**.

**Modificar PIN de la SIM** Una vez que el PIN esté en estado **Habilitado y Verificado**, puede elegir cambiar el PIN.

Haga clic en **Modificar**. Introduzca el PIN de la tarjeta SIM proporcionado por el operador. Introduzca el nuevo PIN de la SIM y confírmelo. Haga clic en **Modificar**.

**Desbloquear SIM** Si olvida el PIN de la SIM, puede restablecer el PIN de la SIM mediante el PUK de la SIM obtenido del operador.

Para desbloquear una SIM, haga clic en **Desbloquear**. Introduzca el PIN de la SIM y el PUK de la SIM obtenidos del operador y haga clic en **Desbloquear**.

> **Nota**
>
> La tarjeta SIM se bloquea permanentemente con 10 intentos fallidos de PUK, mientras desbloquea la SIM. Póngase en contacto con el proveedor de servicios del operador para obtener una nueva tarjeta SIM.

#### Configuración de APN

Para configurar los ajustes de APN, introduzca el APN, el nombre de usuario, la contraseña y la autenticación proporcionados por el operador. Puede elegir entre los protocolos de autenticación **PAP**, **CHAPo PAPCHAP**. Si el transportista no ha proporcionado ningún tipo de autenticación, establezca en**Ninguno**.

#### Configuración de la red

Puede seleccionar la red móvil en los dispositivos Citrix SD-WAN que admiten módems internos.

#### Itinerancia

La opción de roaming está habilitada de forma predeterminada en tus dispositivos. Puede optar por inhabilitarlo.

#### Administrar firmware

Cada equipo que tenga habilitado LTE dispondrá de un conjunto de firmware disponible. Puede seleccionar de la lista existente de firmware o cargar un firmware y aplicarlo. Si no está seguro del firmware que debe utilizar, seleccione la opción AUTO-SIM para permitir que el módem LTE elija el firmware más adecuado en función de la tarjeta SIM insertada en el dispositivo.

> **Nota**
>
> Actualmente, el firmware solo se puede aplicar a los dispositivos SD-WAN SE 210 LTE.

**Activar/desactivar módem**

Activa o desactiva el módem en función de tu intención de utilizar la funcionalidad de banda ancha. De forma predeterminada, el módem está activado.

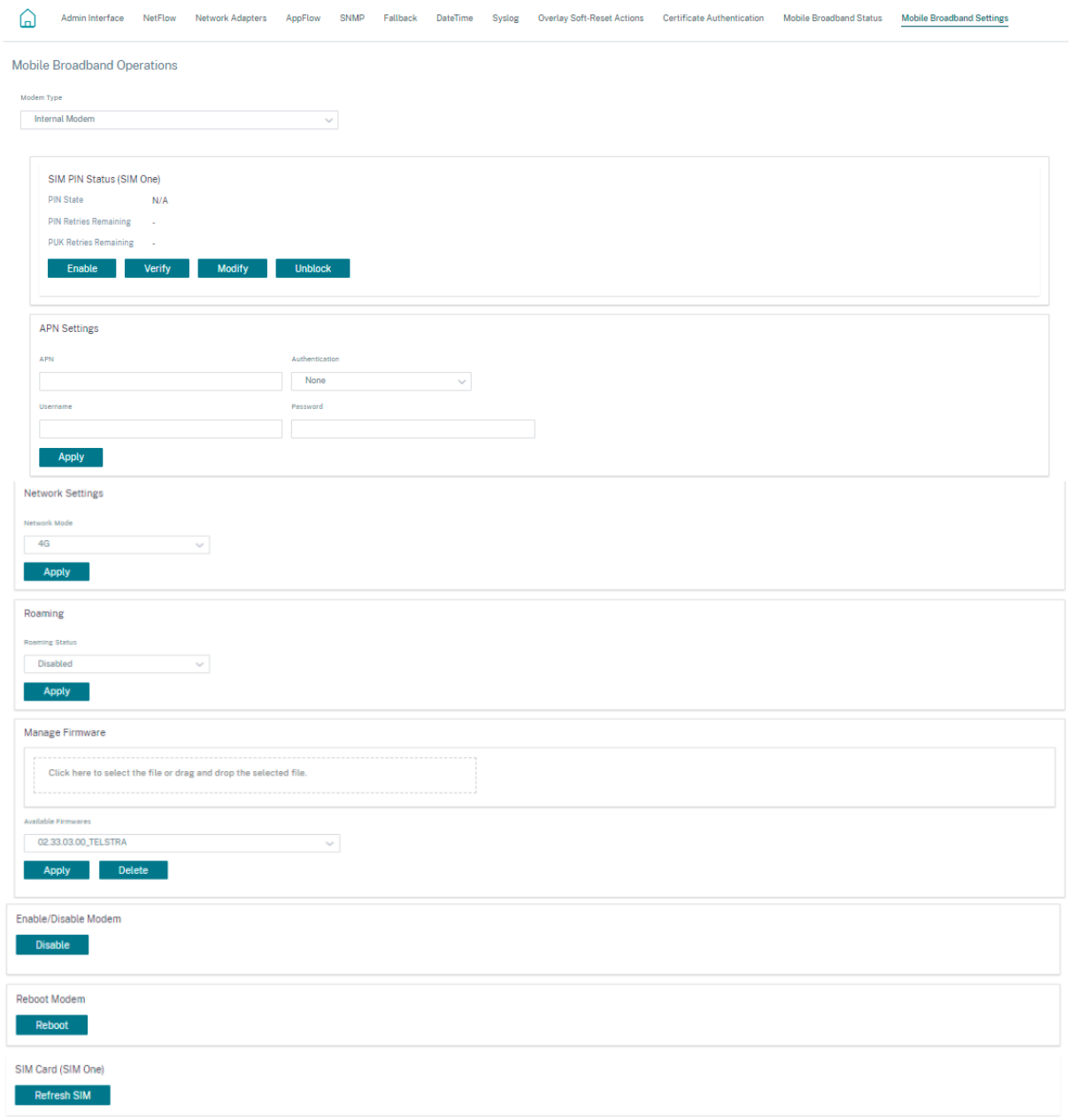
**Reiniciar el módem**

Reinicia el módem. La operación de reinicio puede tardar entre 3 y 5 minutos en completarse.

**Actualizar SIM**

Utilice esta opción cuando cambie en caliente la tarjeta SIM para detectar una nueva.

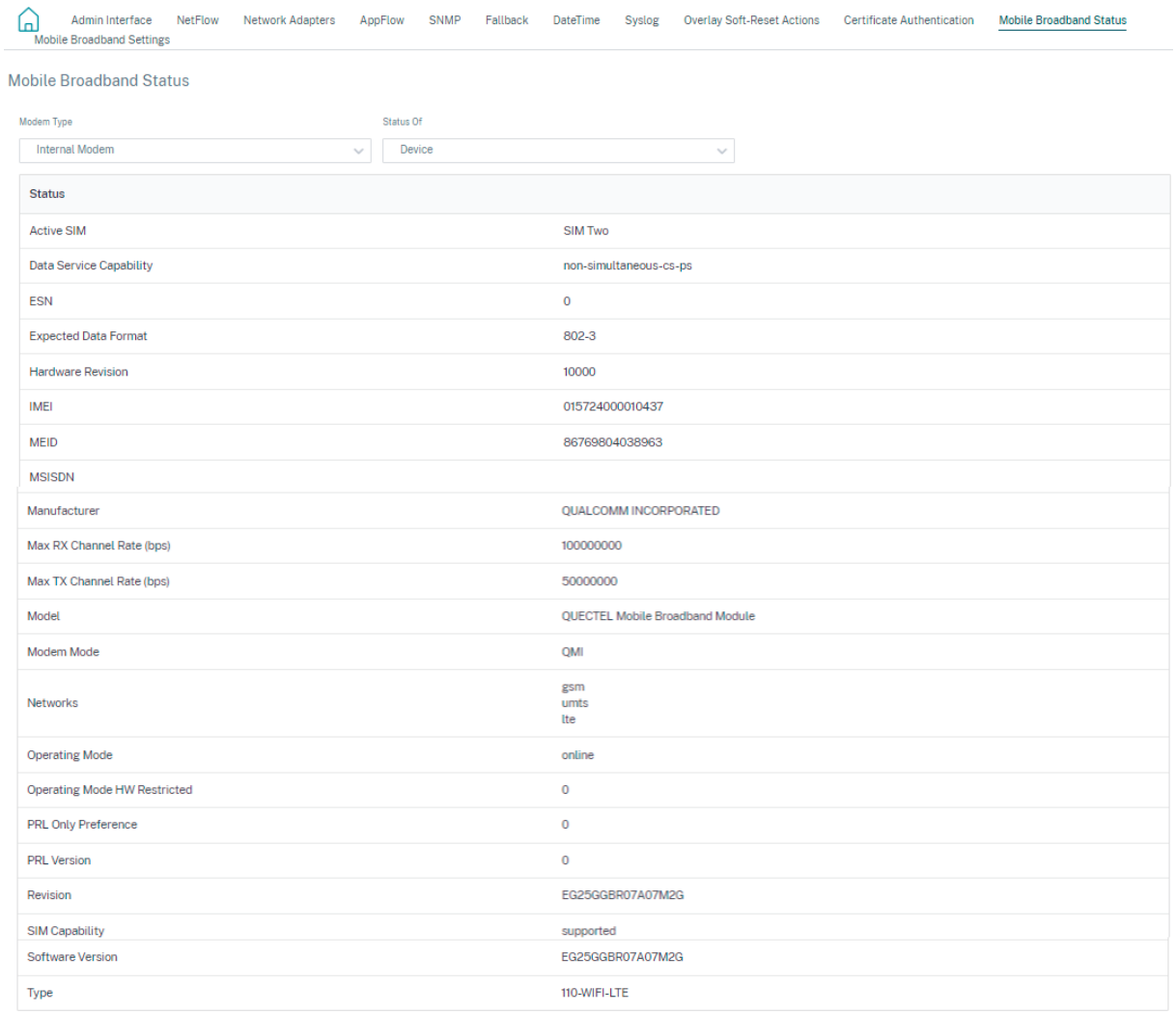
 




## Estado de banda ancha móvil

La sección Estado de la banda ancha móvil muestra el estado de los ajustes de configuración de banda ancha. Para ver el estado de la banda ancha móvil, al nivel de sitio, vaya a **Configuración > Configuración > Configuracióndel dispositivo**>**Estado de la banda ancha móvil**. Puede ver el estado del dispositivo y de la SIM activa.

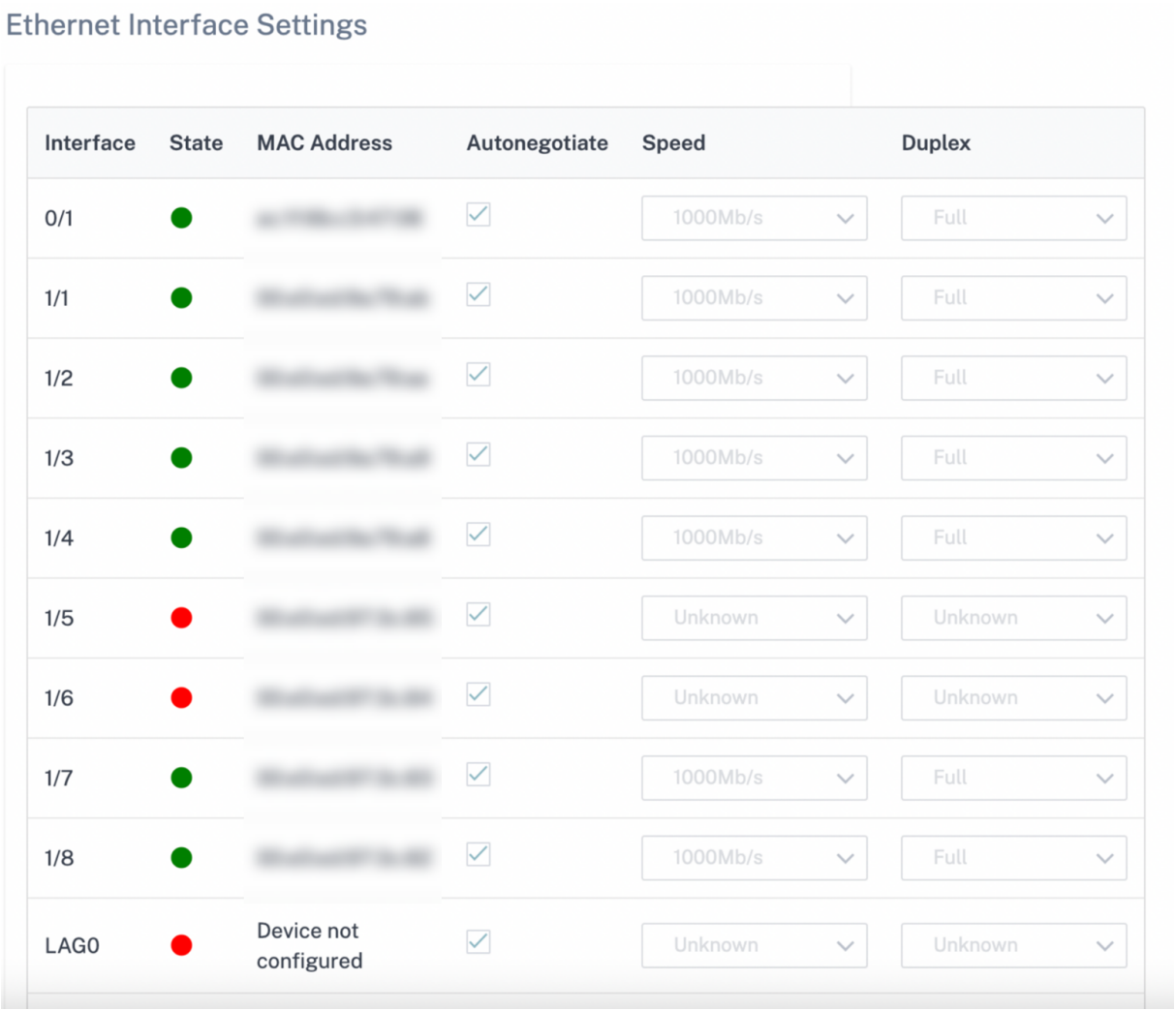



## Configuración de la interfaz Ethernet

La sección de estado de la interfaz Ethernet muestra el estado de conectividad de los puertos ethernet, el tipo de interfaz, la dirección MAC, la negociación automática y la información de configuración del dúplex. Para ver la configuración de la interfaz ethernet, al nivel de sitio, vaya a **Configuración > Configuracióndel dispositivo > Configuración**de la**interfaz Ethernet**. Los puertos que están inactivos administrativamente se indican en rojo.

> **Nota:**
>
> Esta configuración está disponible actualmente en modo de solo lectura en la interfaz de usuario del servicio Citrix SD-WAN Orchestrator. Si quiere modificar la configuración de la interfaz Ethernet, puede hacerlo mediante la nueva interfaz de usuario para los dispositivos SD-WAN.




## Administración en banda

October 31, 2022

El servicio Citrix SD-WAN Orchestrator le permite administrar el dispositivo SD-WAN de dos maneras: Administración fuera de banda y administración dentro de banda. La administración fuera de banda le permite crear una dirección IP de administración mediante un puerto reservado para la administración, que solo transporta tráfico de administración. La administración en banda le permite utilizar los puertos de datos SD-WAN para la administración. Lleva tanto tráfico de datos como de administración, sin tener que configurar una ruta de administración de adiciones.

La administración en banda permite que las direcciones IP virtuales se conecten a servicios de administración como la interfaz de usuario web y SSH. Puede habilitar la administración en banda en

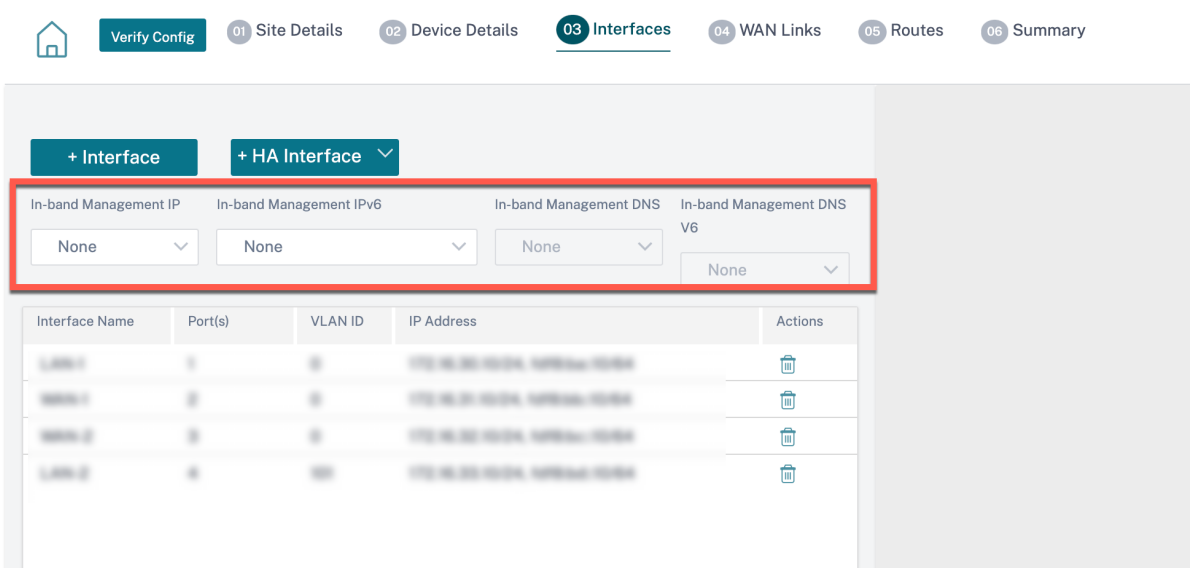
 

una interfaz de confianza habilitada para ser utilizada para servicios IP. Puede acceder a la interfaz de usuario web y SSH mediante la IP de administración y las IP virtuales en banda.

> **Nota**
>
> La administración dentro de banda en el servicio Citrix SD-WAN Orchestrator es compatible con Citrix SD-WAN 11.1.1 y versiones posteriores.

Para habilitar la administración dentro de banda en una IP virtual, al nivel de sitio, vaya a **Configuración > Configuracióndel sitio**>**Interfaces**. Seleccione la IP virtual que se utilizará como puerto de administración en banda. Puede usar la**IP de administración en banda**o el**IPv6 de administración en banda** para acceder a la interfaz de usuario web y a SSH.

> **Nota**
>
> La administración en banda solo se admite en puertos LAN.




Para obtener información detallada sobre el procedimiento de configuración de una dirección IP virtual, consulte Interfaces.

La IP de administración en banda también actúa como IP de gestión de copias de seguridad. Se utiliza como dirección IP de administración si el puerto de administración no está configurado con una Gateway predeterminada. Seleccione el **proxy DNS** al que se reenvían todas las solicitudes de DNS a través del plano de administración en banda. Para obtener información sobre la configuración del proxy DNS, consulte Proxy DNS.

En los casos de uso en los que la conectividad del dispositivo con el servicio Citrix SD-WAN Orchestrator cambia entre los puertos de administración y los puertos dentro de banda, configure el **DNS de**

**administraciónen banda o el DNS V6 de administración** en banda para garantizar una conectividad ininterrumpida del servicio Citrix SD-WAN Orchestrator.

### Aprovisionamiento en banda

La necesidad de implementar dispositivos SD-WAN en entornos más sencillos como el hogar o las sucursales pequeñas ha aumentado significativamente. Configurar un acceso de administración independiente para implementaciones más sencillas es una sobrecarga adicional. La implementación sin táctiles junto con la función de administración en banda permite el Provisioning y la administración de la configuración a través de puertos de datos designados. La implementación sin táctiles es compatible con los puertos de datos designados y no es necesario utilizar un puerto de administración independiente para la implementación sin contacto.

Puede aprovisionar un dispositivo en el estado enviado de fábrica, que admita el Provisioning en banda conectando el puerto de administración o de datos a Internet. Los dispositivos que admiten el Provisioning en banda tienen puertos específicos para LAN y WAN. El dispositivo en estado de restablecimiento de fábrica tiene una configuración predeterminada que permite establecer una conexión con el servicio de implementación sin contacto. El puerto LAN actúa como servidor DHCP y asigna una IP dinámica al puerto WAN que actúa como cliente DHCP. Los enlaces WAN supervisan el servicio DNS Quad 9 para determinar la conectividad WAN.

Una vez que se obtiene la dirección IP y se establece una conexión con el servicio de implementación sin contacto, los paquetes de configuración se descargan e instalan en el dispositivo. Para obtener información sobre la implementación sin intervención a través del servicio Citrix SD-WAN Orchestrator, consulte Zero Touch Deployment.

> **Nota**
>
> - El Provisioning en banda es aplicable a todas las plataformas. Sin embargo, la configuración predeterminada solo se habilita en las plataformas Citrix SD-WAN 110 y VPX porque las demás plataformas se suministran con una versión de software anterior.
> - Para el Provisioning del día 0 de los dispositivos SD-WAN a través de los puertos de datos, la versión del software del dispositivo debe ser Citrix SD-WAN 11.1.1 o superior.

La configuración predeterminada de un dispositivo en estado de restablecimiento de fábrica incluye las siguientes configuraciones:

- Servidor DHCP en puerto LAN
- Cliente DHCP en el puerto WAN
- Configuración de QUAD9 para DNS
- La IP LAN predeterminada es 192.168.101.1/24 para los dispositivos Citrix SD-WAN con imagen de fábrica 11.1.1.39.

- La IP LAN predeterminada es 192.168.0.1/24 para el dispositivo Citrix SD-WAN 110 con imagen de fábrica 11.0.4.
- Licencia Grace de 35 días.

Una vez aprovisionado el dispositivo, la configuración predeterminada se inhabilita y anula por la configuración recibida del servicio de implementación sin contacto. Si caduca una licencia de dispositivo o licencia de gracia, se activa la configuración predeterminada, lo que garantiza que el dispositivo permanece conectado al servicio de implementación sin contacto y recibe el servicio administrado de licencias.

### Configuración de reserva

La configuración de reserva garantiza que el dispositivo permanezca conectado al servicio de implementación sin contacto si hay un error de vínculo, falta de configuración o falta de software. La configuración de reserva está habilitada de forma predeterminada en los dispositivos que tienen un perfil de configuración predeterminado. También puede modificar la configuración de reserva según la configuración de red LAN existente.

La configuración alternativa conserva la conectividad con el dispositivo a través de la IP de administración en banda del dispositivo y el servicio Citrix SD-WAN Orchestrator en los siguientes casos:

- Dónde se bloquea la t2_app
- intenta realizar el restablecimiento de la configuración

En un caso en el que un dispositivo tiene configurada la administración en banda y usted realiza un restablecimiento manual de la configuración o la t2_app se bloquea más de cuatro veces en 120 segundos debido a la configuración del usuario. En este marco, el servicio se inhabilita y, por lo tanto, se pierde la conectividad con el servicio Citrix SD-WAN Orchestrator y el dispositivo.

Pero si tenía habilitada la configuración alternativa, obtendrá las siguientes funciones:

- Acceso básico dentro de banda a las funciones de administración (Web UI/SSH/SNMP)
- Capacidad para que el dispositivo se conecte a servicios externos a través de un puerto en banda (Citrix SD-WAN Orchestrator Service/ZTD)

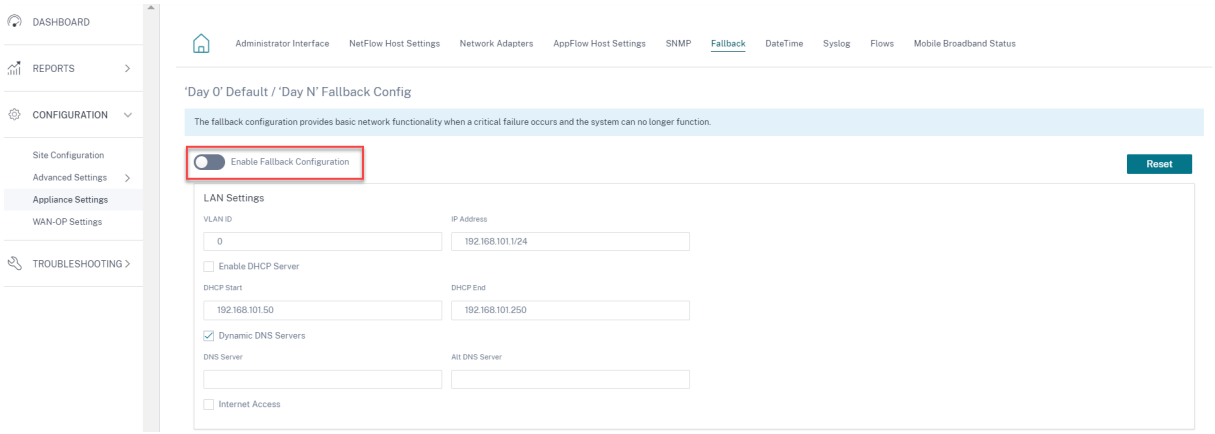
Para estos casos, en lugar de inhabilitar el dispositivo de servicio, vuelve con una configuración alternativa con el servicio habilitado. La conectividad con el servicio Citrix SD-WAN Orchestrator y el dispositivo a través de la IP de administración en banda permanece intacta mientras el enlace tenga conectividad a Internet.

> **Nota**

> Tras el aprovisionamiento inicial del dispositivo, asegúrese de que la configuración alternativa esté habilitada para la conectividad del servicio de implementación sin interacción.

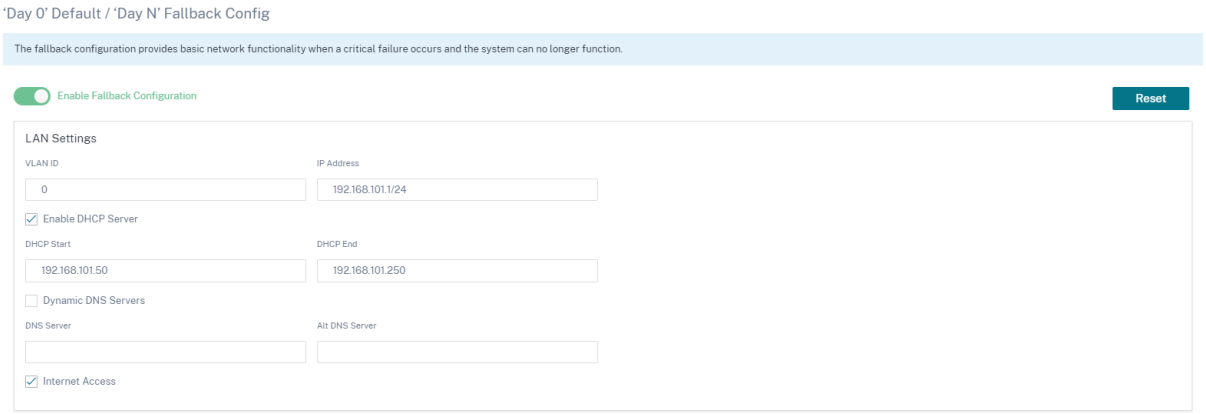
Si la configuración alternativa está inhabilitada, puede habilitarla a través del servicio Citrix SD-WAN Orchestrator al nivel de sitio. Para ello, vaya a **Configuración** > **Configuración del dispositivo** > **Alternativa** y haga clic en **Habilitar configuración alternativa**.




Para personalizar la configuración alternativa según su red LAN, modifique los valores de las siguientes configuraciones de LAN según los requisitos de la red. Esta es la configuración mínima necesaria para establecer una conexión con el servicio de implementación sin contacto.

- **ID de VLAN**: El ID de VLAN en el que se debe agrupar el puerto LAN.
- **Dirección IP**: La dirección IP virtual asignada al puerto LAN.
- **Habilitar servidor DHCP**: habilita el puerto LAN como servidor DHCP. El servidor DHCP asigna direcciones IP dinámicas al puerto WAN.
- **Inicio y finalización de DHCP**: Rango de direcciones IP que DHCP utiliza para asignar una IP al puerto WAN de forma dinámica.
- **Servidor DNS dinámico**: habilita el puerto LAN como servidor de nombres de dominio.
- **Servidor DNS**: La dirección IP del servidor DNS principal.
- **Servidor DNS Alt**: La dirección IP del servidor DNS secundario.
- **Acceso a Internet**: Permita el acceso a Internet a todos los clientes LAN sin ningún otro filtrado.

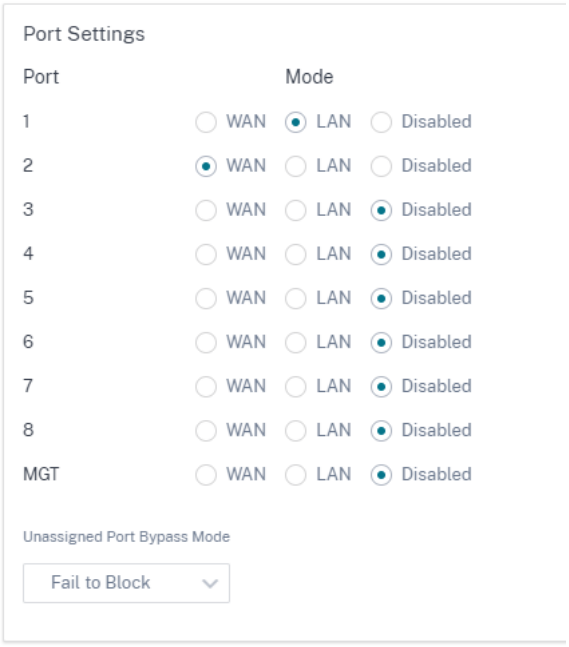



Configure el modo para cada puerto. El puerto puede ser un puerto LAN o un puerto WAN o puede inhabilitarse. Los puertos mostrados dependen del modelo del dispositivo. Además, configure el modo de derivación de puerto en **Fail-to-Block** o **Fail-to-Wire**.

La siguiente tabla proporciona los detalles de los puertos WAN y LAN designados previamente para la configuración de reserva en diferentes plataformas:

| Plataforma | Puertos WAN | Puertos LAN |
|---|---|---|
| 110 | 1/2 | 1/1 |
| 110-LTE | 1/2, LTE-1 | 1/1 |
| 210 | 1/4, 1/5 | 1/3 |
| 210-LTE | 1/4, 1/5, LTE-1 | 1/3 |
| VPX | 2 | 1 |
| 410 | 1/4, 1/5, 1/6 | 1/3 (FTB) |
| 1100 | 1/4, 1/5, 1/6 | 1/3 (FTB) |

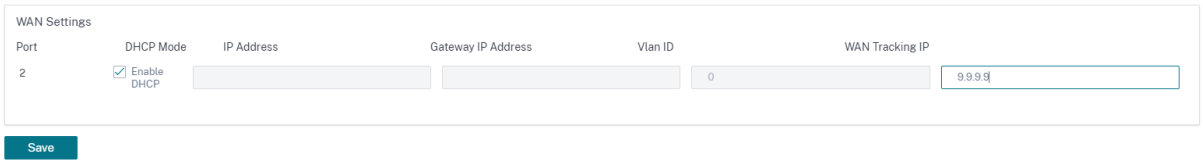
 




Los puertos WAN se pueden configurar como enlaces WAN independientes mediante el cliente DHCP y supervisar el servicio DNS Quad9 para determinar la conectividad WAN. Puede configurar IP/IP estáticas WAN para los puertos WAN en ausencia de DHCP para utilizar la administración en banda para el aprovisionamiento inicial.

> **Nota**
>
> Solo puede configurar los puertos Ethernet con las IP estáticas. Las IP estáticas no se pueden configurar con los puertos LTE-1 y LTE-E1. Aunque puede agregar los puertos LTE-1 y LTE-E1 como WAN, los campos de configuración permanecen no modificables.

Al agregar un puerto WAN, se agrega en la sección **Configuración WAN (puerto: 2)** con la casilla **Habilitar DHCP** seleccionada de forma predeterminada. Si se selecciona la casilla **Modo DHCP**, los campos de texto **Dirección IP**, **Dirección IP de puerta**de enlace e **ID de VLAN** aparecen atenuados. Desactive la casilla **Activar DHCP** si quiere configurar una IP estática.




De forma predeterminada, el campo **Dirección IP de seguimiento de WAN** se rellena automáticamente con 9.9.9.9. Puede cambiar la dirección según sea necesario.

> **Nota**
>
> Si selecciona la casilla **Servidores DNS dinámicos**, asegúrese de agregar o configurar al menos

> un puerto WAN con el **modo DHCP** seleccionado.

Para restablecer la configuración de reserva a la configuración predeterminada en cualquier momento, haga clic en **Restablecer**.

> **Nota**
>
> Se recomienda habilitar la configuración alternativa en todos los dispositivos que estén conectados a Orchestrator a través del puerto de administración o en banda conectado a la subred LAN. Asegúrese de que la configuración alternativa predeterminada esté configurada según los requisitos de subred de la red.

### Failover de puerto

El servicio Citrix SD-WAN Orchestrator también permite conmutar por error el tráfico de administración sin problemas al puerto de administración cuando el puerto de datos deja de funcionar y viceversa. Si un dispositivo puede conectarse a Internet a través de los puertos de administración y en banda, se elige el puerto de administración para la implementación sin contacto.

Al reiniciar el dispositivo, si Internet está disponible a través del puerto en banda y no en el puerto de administración, el dispositivo se conecta inmediatamente al servicio Citrix SD-WAN Orchestrator.

Una vez establecida la conexión, un agente de servicio que se ejecuta en el dispositivo envía la información de los latidos al servicio Citrix SD-WAN Orchestrator cada 10 segundos. Si el servicio Citrix SD-WAN Orchestrator no recibe el latido durante 5 minutos, se activa la conmutación por error del puerto en banda. El servicio Citrix SD-WAN Orchestrator informa que el dispositivo está fuera de línea durante este período.

Al reiniciar el dispositivo, si Internet no está disponible tanto en el puerto de administración como en banda y una vez restablecida la conexión a Internet, el agente de servicio tarda unos 5 minutos en reiniciar y establecer una conexión.

Asegúrese de que la opción **Preservar ruta a Internet desde el enlace incluso si todas las rutas asociadas están inactivas** esté habilitada al nivel de red, **Configuración** > **Servicios de entrega** > **Internet**. Garantizar que la conectividad con el servicio Citrix SD-WAN Orchestrator se mantenga incluso si la ruta virtual está inactiva.


## Puerto de datos o administración configurable

La administración en banda permite que los puertos de datos transporten tanto tráfico de datos como de administración, eliminando la necesidad de un puerto de administración dedicado. Deja el puerto de administración sin utilizar en los dispositivos de gama baja, que ya tienen baja densidad de puertos. Citrix SD-WAN permite configurar el puerto de administración para que funcione como puerto de datos o como puerto de administración.

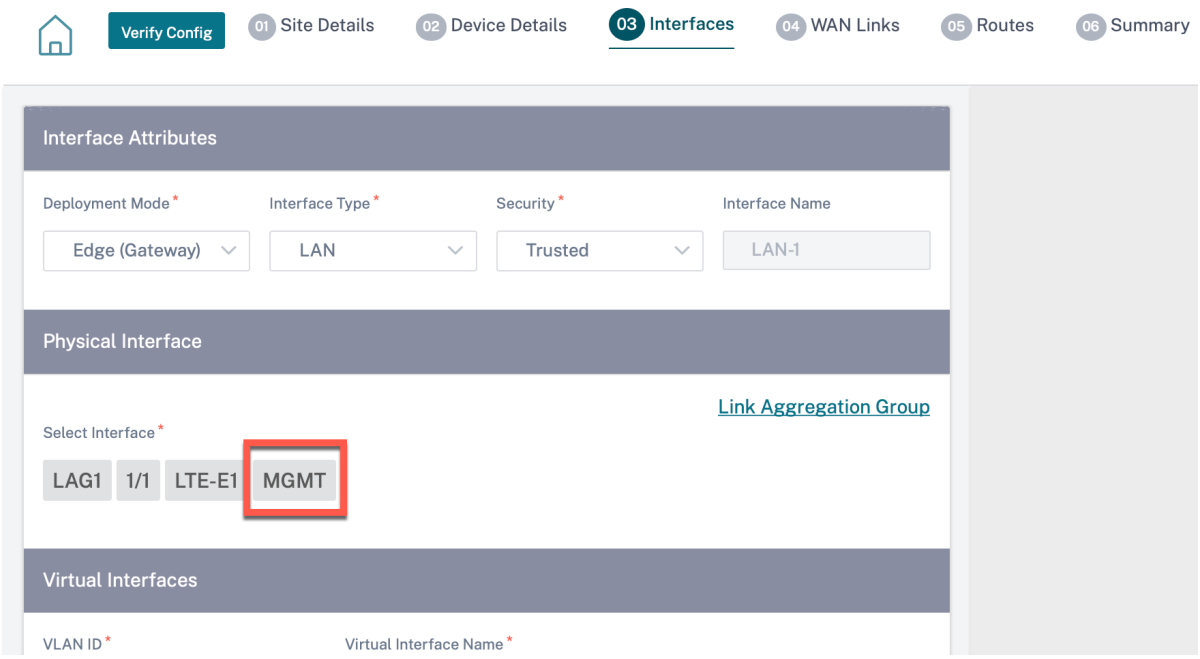
> **Nota**
>
> Puede convertir el puerto de administración en puerto de datos solo en las siguientes plataformas.
>
> - Citrix SD-WAN 110 SE/LTE
> - Citrix SD-WAN 210 SE/LTE

Mientras configura un sitio, utilice el puerto de administración en la configuración. Después de activar la configuración, el puerto de administración se convierte en un puerto de datos.

> **Nota**
>
> Solo puede configurar un puerto de administración cuando la administración en banda está habilitada en otras interfaces de confianza del dispositivo.

Para configurar una interfaz de administración, al nivel de sitio, vaya a **Configuración > Configuracióndel sitio**>**Interfaces** y seleccione la interfaz de administración. Para obtener más información sobre la configuración de grupos de interfaces, consulte Interfaces.




Para volver a configurar el puerto de administración para realizar la funcionalidad de administración, quite la configuración. Cree una configuración sin utilizar el puerto de administración y actívelo.

## Ver configuración (versión preliminar)

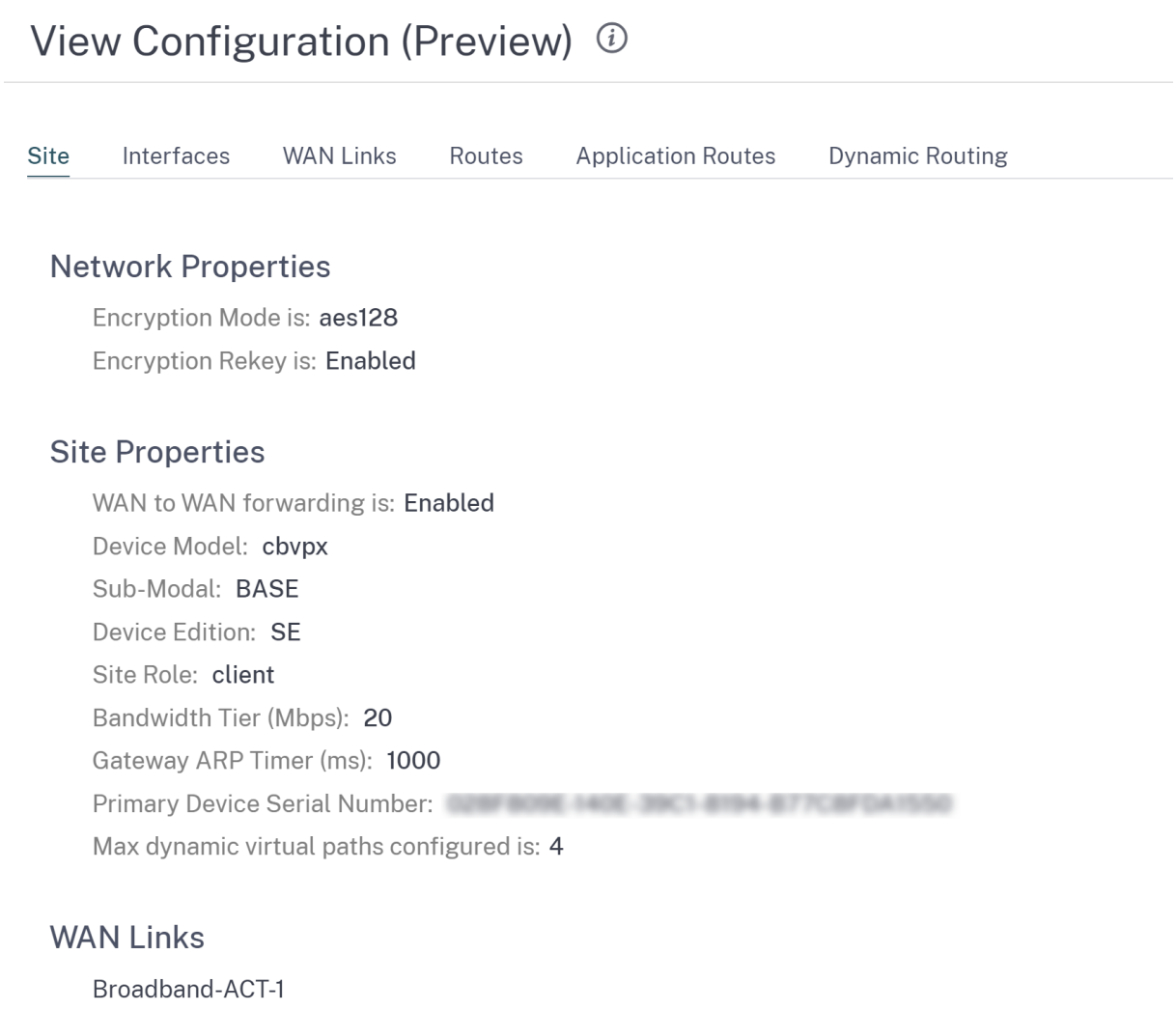
October 31, 2022

La página **Ver configuración** proporciona un resumen consolidado de los ajustes de configuración de un sitio. Para ver las configuraciones, al nivel de sitio, vaya a **Configuración** > **Ver configuración**. Para obtener más información sobre la configuración del sitio, consulte Configuración del sitio.

### Sitios

La página **Sitios** muestra un resumen de los detalles del sitio. El resumen del sitio incluye las propiedades de la red, las propiedades del sitio y el estado del enlace WAN. Para ver los detalles de configuración del sitio, vaya a **Configuración** > **Ver configuración** > **Sitio**.

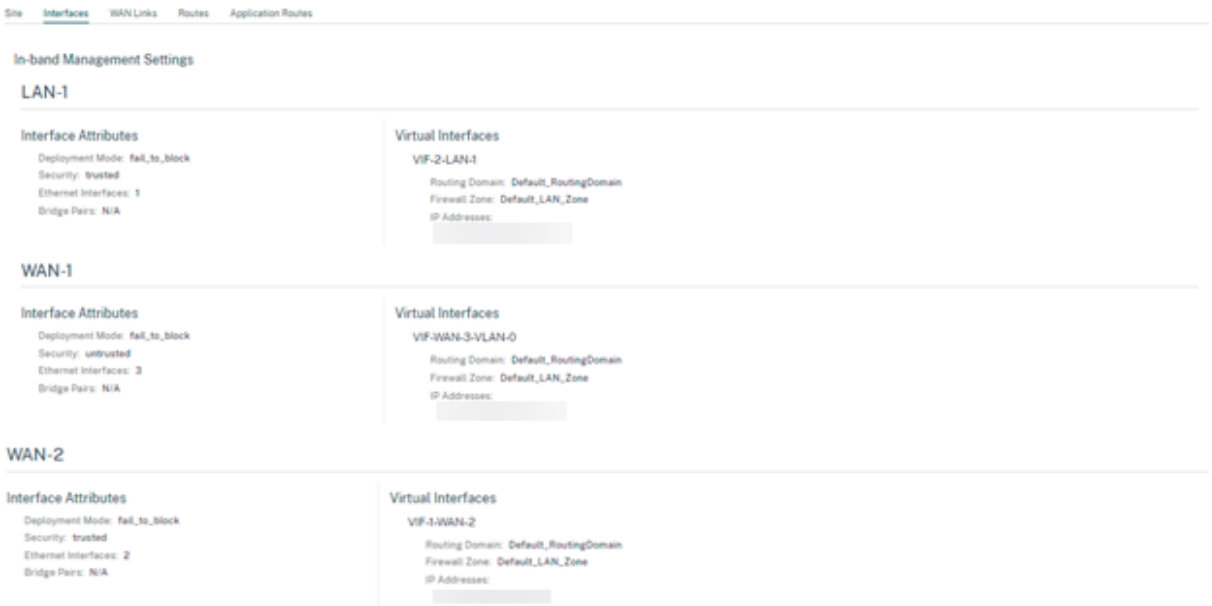
 




### Interfaces

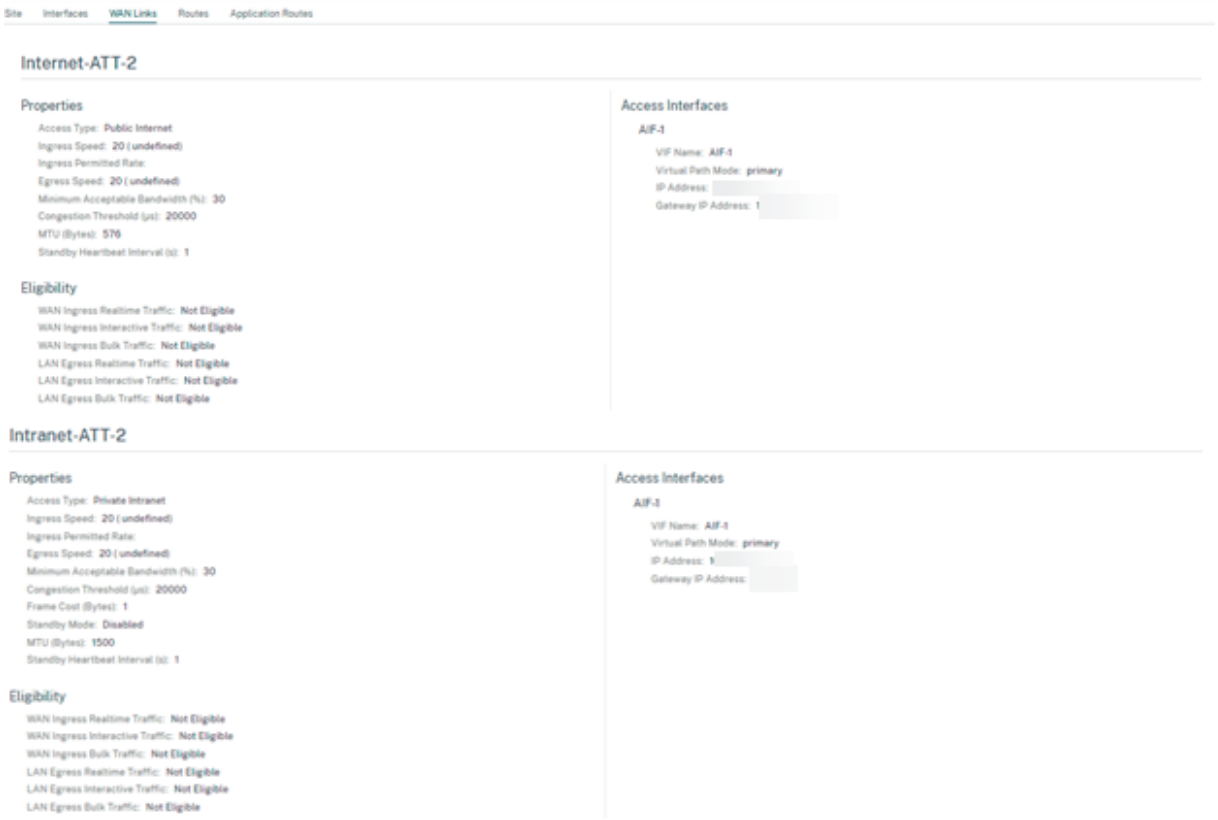
La página **Interfaces** muestra un resumen de las interfaces configuradas. Para ver los detalles de configuración de las interfaces virtuales, vaya a **Configuración** > **Ver configuración** > **Interfaces**.




## Enlaces WAN

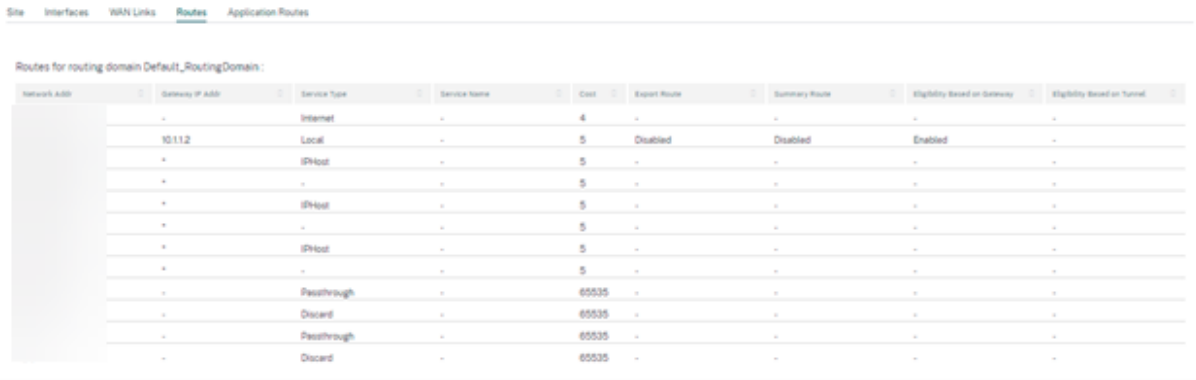
Para ver los detalles de configuración de los enlaces WAN configurados, vaya a **Configuración** > **Ver configuración** > **Enlaces WAN**.



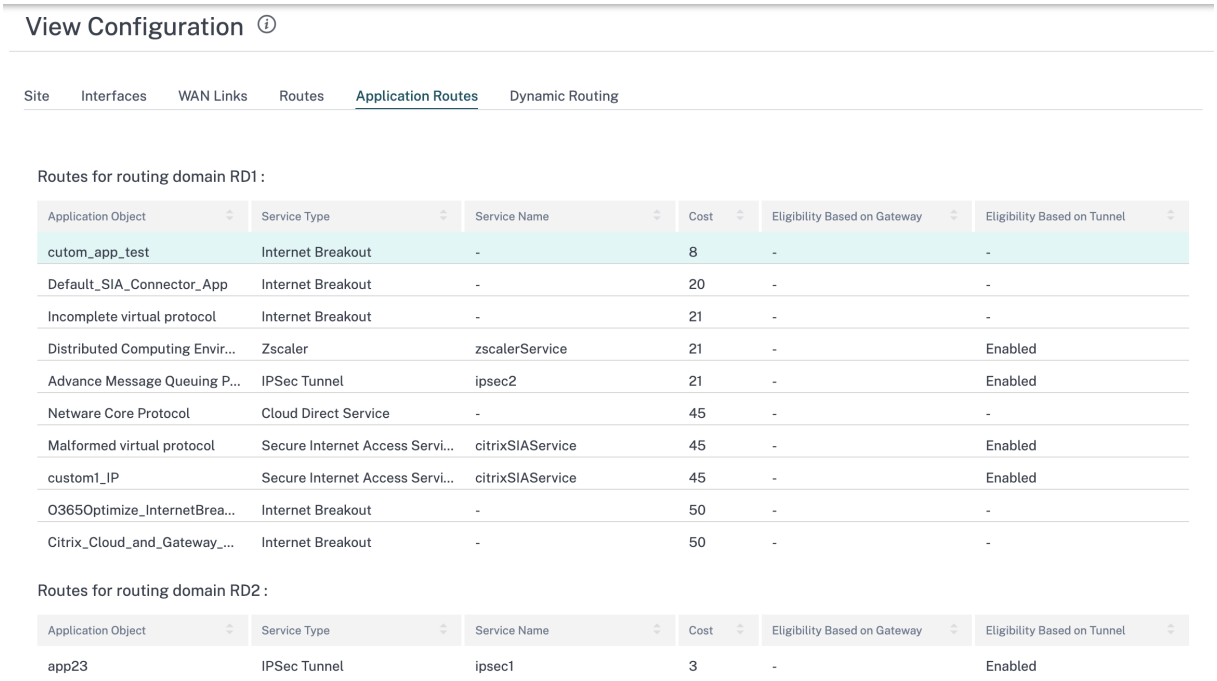
## Rutas

Para ver la información de ruta de las rutas IP creadas, vaya a **Configuración** > **Ver configuración** > **Rutas**.



## Rutas de aplicación

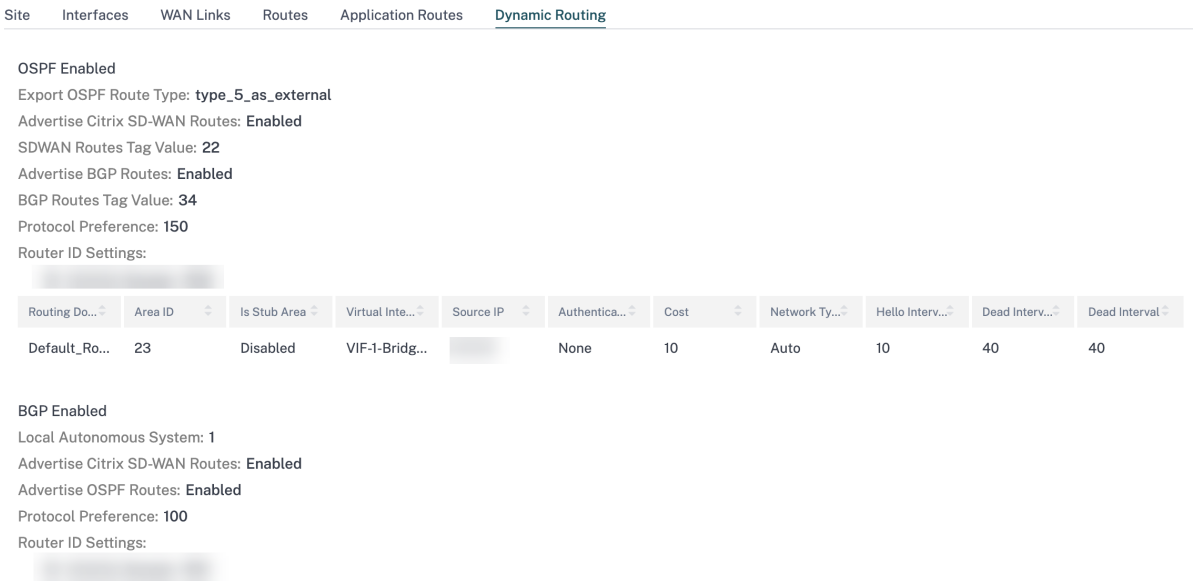
Para ver un resumen de las rutas de aplicación específicas, vaya a **Configuración** > **Ver configuración** > **Rutas de aplicación**.




## Redirección dinámica

Para ver un resumen de las configuraciones de OSPF, BGP, filtro de importación y filtro de exportación, vaya a **Configuración** > **Ver configuración** > **Enrutamiento dinámico**.

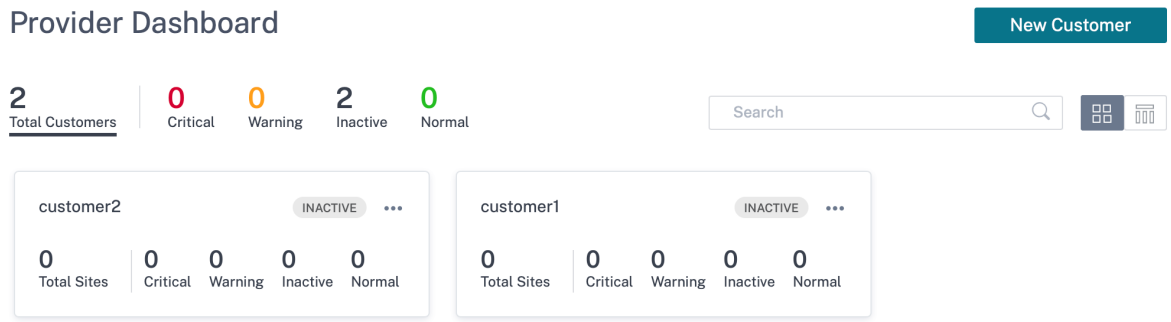
 




## Panel de proveedores

November 16, 2020

Cuando inicia sesión como asociado de Citrix,**aparece el Panel de**proveedores. Ofrece una vista de pájaro de todos los clientes de SD-WAN gestionados por un proveedor de servicios.




Se proporciona una instantánea de estado codificada por colores de la red SD-WAN de cada cliente, con una provisión para profundizar en cualquiera de ellas para obtener detalles específicos del cliente. El panel está disponible tanto en la vista de **icono como en** la vista **de lista**.

Los criterios de codificación de colores utilizados para la red del cliente son:

- Crítico (rojo): Uno o más sitios están indisponibles
- Advertencia (naranja): No hay sitios inactivados, pero hay una o más alertas críticas.

- Normal (verde): No hay sitios inactivados y no hay alertas críticas.
- Inactivo (gris): La red se está configurando, pero aún no se ha implementado.

Los criterios de codificación de colores permiten a los administradores centrarse en los clientes que necesitan su atención.

## Tablero de cliente/Red

July 10, 2024

El panel de control de red ofrece una vista panorámica de la red SD-WAN de una organización en términos de salud y uso en todos los sitios. El panel captura un resumen de las alertas de toda la red, el tiempo de actividad de las rutas de superposición y calco subyacente, resalta las tendencias de uso y proporciona una vista global de la red.

El panel resume los siguientes aspectos de una red, con una provisión para profundizar para obtener más detalles.

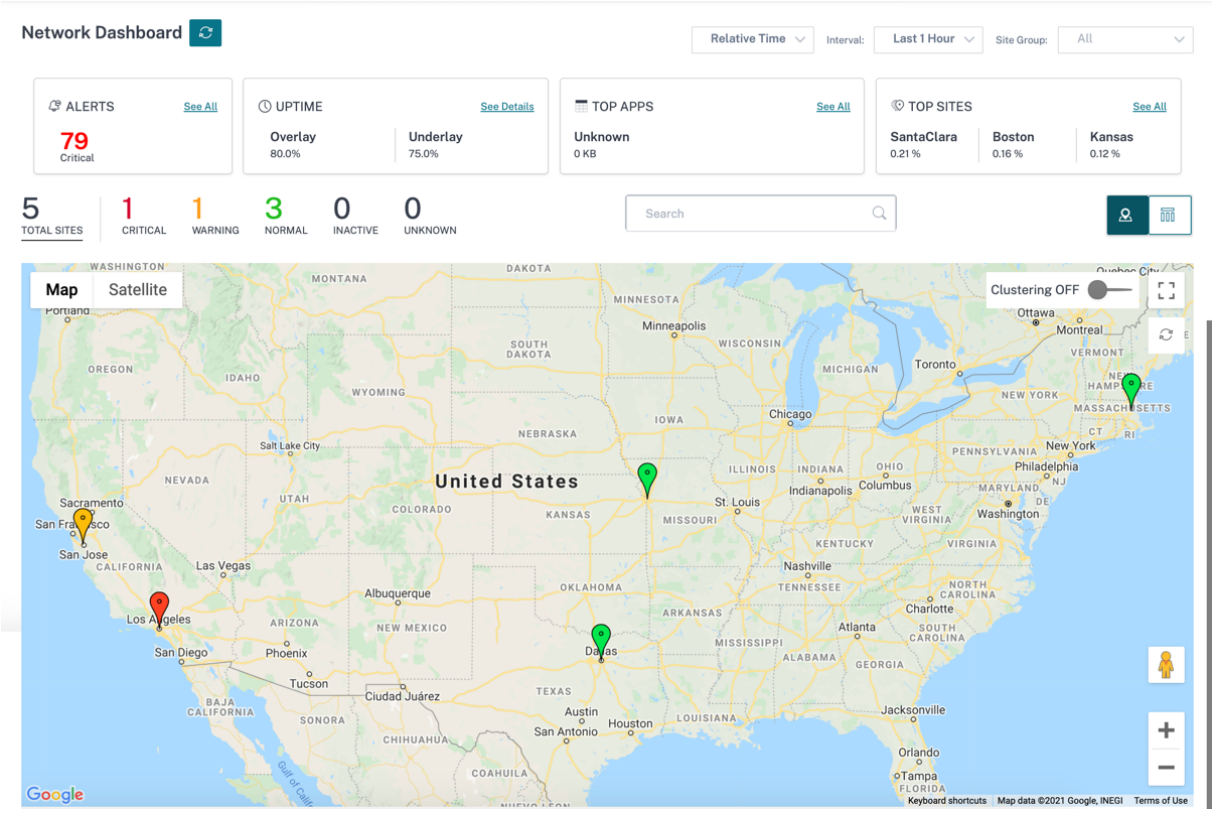
- **Alertas críticas**: Recuento continuo de las alertas de salud críticas, si las hay, que aparecen en la red.
- **Tiempo de actividad**: Comparación en paralelo del tiempo de actividad promedio que ofrece la red superpuesta virtual SD-WAN frente a la red subyacente física
- **Tendencias de uso**: Aplicaciones principales, según el volumen de tráfico y sitios principales, según la utilización de la capacidad.
- **Vista de red**: Representación visual de todos los sitios de una red, disponible tanto en la vista de mapa como en la vista de lista.

El panel muestra el número total de sitios de la red y también segrega los sitios según su estado de conectividad. Seleccione los enlaces numerados para ver los sitios según las siguientes categorías de estado:

- **Crítico**: Sitios que tienen todas las rutas virtuales asociadas inactivas.
- **Advertencia**: Sitios que tienen al menos una ruta virtual de acceso.
- **Normal**: Todas las rutas virtuales y las rutas de miembros asociadas del sitio están activas.
- **Inactivo**: Sitios que se encuentran en estado no desplegado e inactivo.
- **Desconocido**: Se desconoce el estado del sitio.

Al hacer clic en el estado, se filtran los sitios según su estado y se muestran los detalles. También puede utilizar la barra de **búsqueda** para ver los detalles de un sitio en función del nombre del sitio, el rol, la conectividad superpuesta, el modelo, el nivel de ancho de banda y los parámetros del número de serie.




El mapa proporciona una vista en tiempo real de la red global con todos los sitios de la organización representados en un mapa mundial, según su ubicación. El color de cada sitio refleja su estado actual.

A continuación se presentan los criterios de codificación de colores utilizados para cada sitio:

- **Crítico (rojo)**: Al menos una ruta virtual superpuesta asociada a un sitio está INACTIVO.
- **Advertencia (naranja)**: Al menos una ruta de miembro subyacente está DESACTIVADA, pero todas las rutas virtuales superpuestas están ARRIBA.
- **Normal (verde)**: Todas las rutas virtuales superpuestas y las rutas de los miembros subyacentes asociadas están activas.
- **Inactivo (gris)**: El sitio está subconfigurado y aún no se ha implementado.

Al pasar el cursor sobre cualquier sitio, se muestran algunos de los detalles clave específicos del sitio, como el rol de sitio, el modelo de dispositivo y el nivel de ancho de banda. Las rutas virtuales asociadas a un sitio aparecen con códigos de color adecuados que reflejan su estado. La **vista de lista** proporciona los mismos detalles para cada sitio, resumidos como entradas de una tabla.

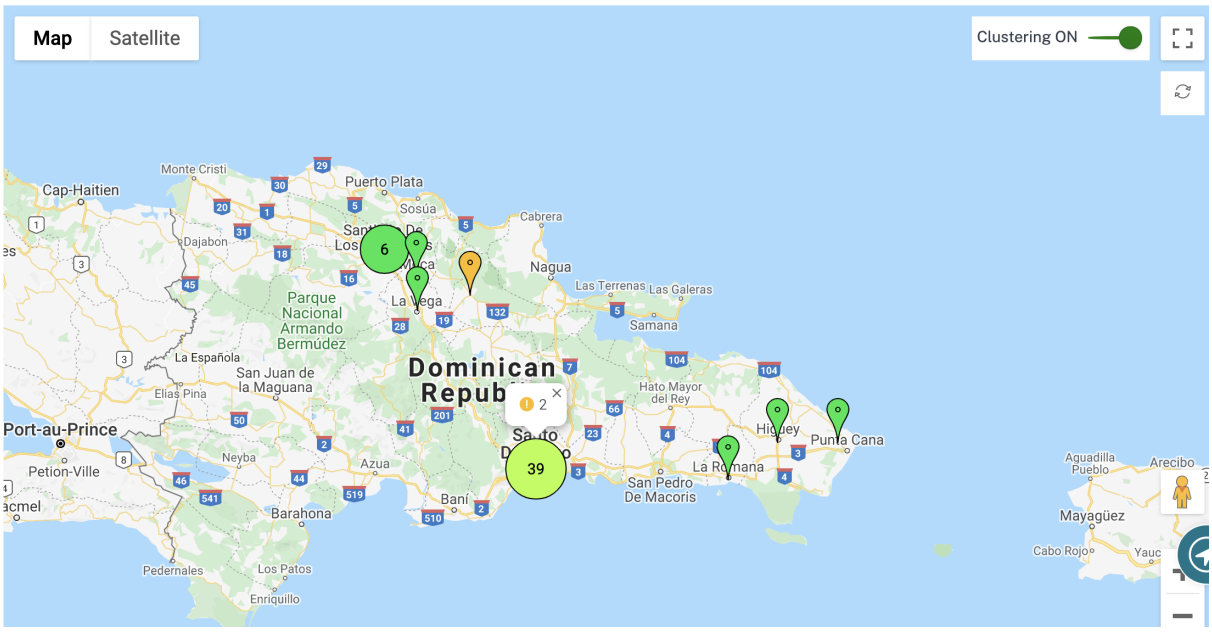
### Agrupar en clústeres

La función **Clustering ON** supervisa la consistencia, el estado y el estado de varios sitios de un clúster o una combinación de clústeres. El servicio Clustering ON proporciona una vista en tiempo real de los

sitios que ayudan a supervisar la conmutación por error y el estado actual del sitio.

Esta función **Clustering ON** se introdujo para administrar la alta densidad de sitios. No se recomienda utilizar la opción Clustering OFF cuando hay miles de sitios y también reduce el rendimiento.




En la tabla siguiente se describe el tono de cinco colores que se utiliza para los clústeres para representar el estado de los sitios:

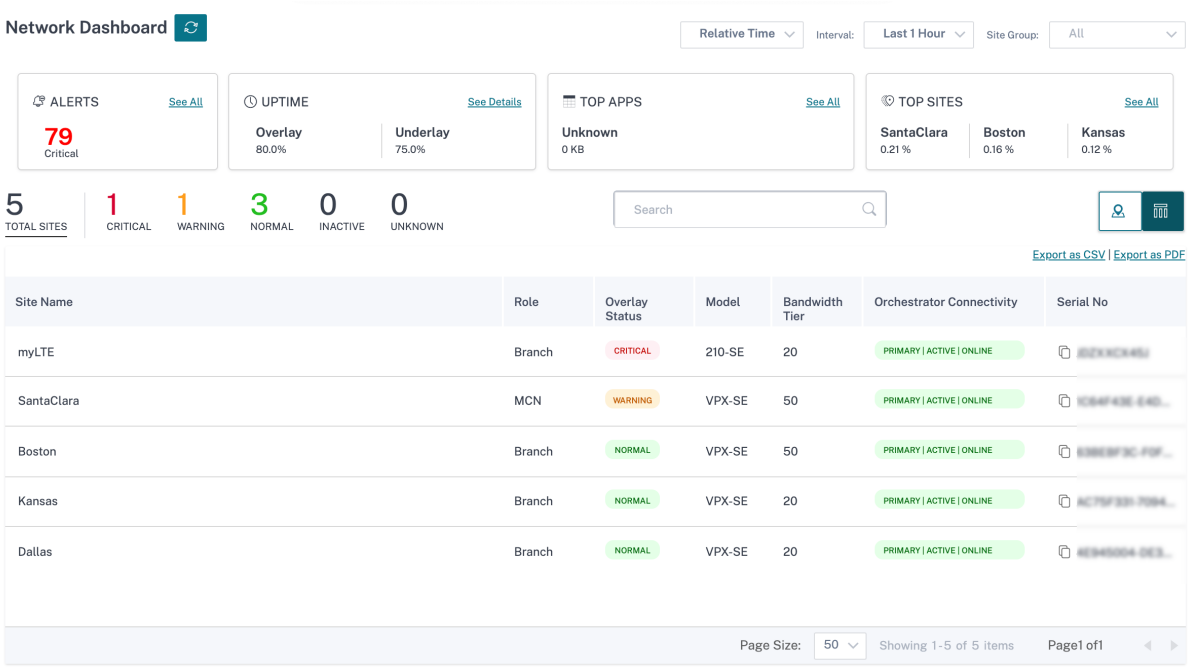
| Leyendas de color | Descripción |
|---|---|
| | Todos los sitios del clúster son verdes. Esto significa que cada sitio tiene todas las rutas virtuales y las rutas de los miembros asociadas (UP). |
| | Todos los sitios del clúster son de color naranja. Esto significa que cada sitio tiene al menos una ruta de miembro ABAJO, pero todas las rutas virtuales ARRIBA |
| | Todos los sitios del clúster son de color rojo. Esto significa que cada sitio tiene al menos una ruta virtual ABAJO |
| | El clúster tiene una combinación de sitios verdes y naranjas |
| | El clúster tiene una combinación de sitios rojos y no rojos |

También puede verificar el aspecto de la red si pasa el mouse sobre cualquier clúster. Las alertas críticas o de advertencia son visibles en la parte superior del clúster como una ventana emergente.

Si hace clic en el clúster, se acerca a ese clúster y muestra otros clústeres. Puede ver una barra de vista con el número de clústeres. La opción de flecha ayuda a traerle de vuelta un paso. Haga clic en el botón **Cerrar (X)** para volver a la página original.

Como alternativa, puede ver el resumen de la red en la **vista de lista**.




- Al hacer clic en cualquier sitio “subconfigurado”inactivo que aún no se haya implementado, accederá al flujo de trabajo de configuración del sitio.
- Al hacer clic en cualquier sitio activo que ya se haya implementado, accederá al **panel de control del sitio**.

> **Nota**
>
> Los túneles superposición de Citrix SD-WAN se denominan rutas virtuales. Normalmente, tendría un túnel de ruta virtual entre cada sitio y el nodo de control maestro (MCN), y rutas virtuales de sitio adicionales, según sea necesario. Las rutas virtuales se forman uniendo los enlaces WAN/rutas WAN del calco subyacente. Por lo tanto, cada ruta virtual comprende varias rutas de miembro.
>
> Esto se puede mostrar cuando un usuario pasa el cursor sobre el término ruta virtual o ruta de miembro.

Puede arrastrar el **Pegman** al mapa para abrir la vista de la calle.

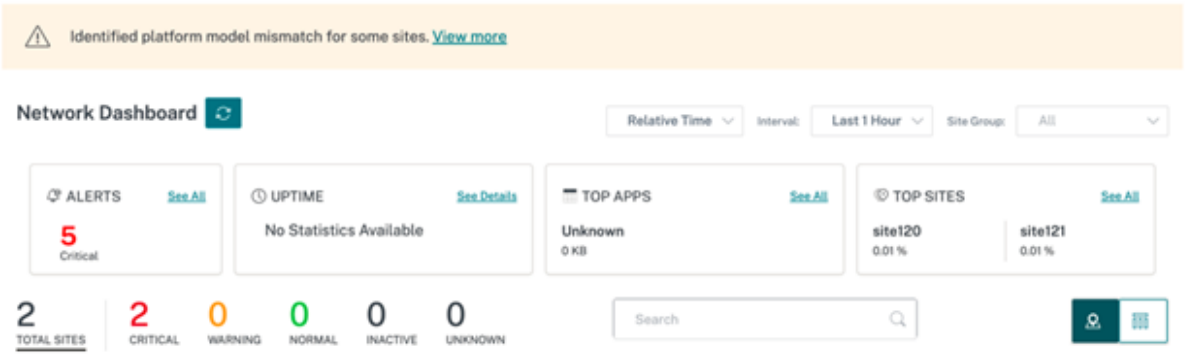
 


## Registrar la discrepancia

El servicio Citrix SD-WAN Orchestrator informa de una discrepancia que se identifica entre el modelo de plataforma notificado por el dispositivo y el modelo de plataforma informado por el usuario.

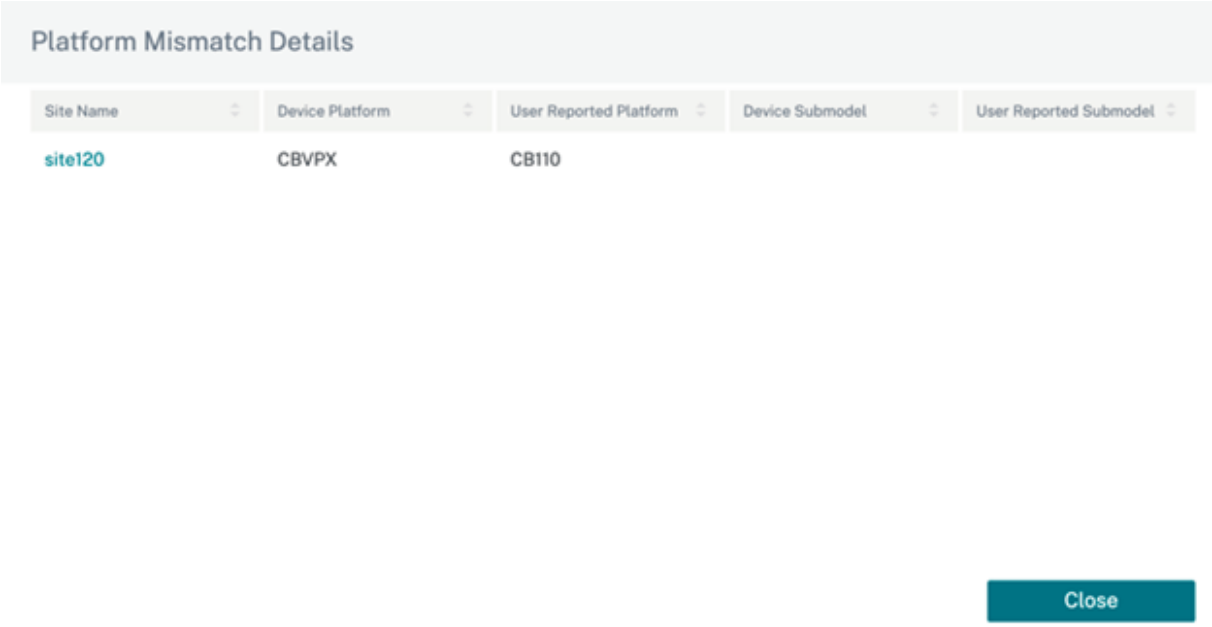
Cuando el modelo de plataforma y el submodelo proporcionados por un usuario durante la configuración del sitio no coinciden con el modelo y el submodelo de plataforma proporcionados por el dispositivo durante el registro inicial en el servicio Citrix SD-WAN Orchestrator, se muestra una notificación sobre la discrepancia en el panel de control de la red. En tal caso, asegúrese de configurar el modelo de plataforma indicado por el dispositivo.

Haga clic en **Ver más para obtener** una representación tabular de la discrepancia del modelo de plataforma para cada sitio.




**Los detalles de discrepancia de plataforma** proporcionan información como el nombre del sitio, el modelo y el submodelo de plataforma informados por el dispositivo y el modelo y submodelo de plataforma informados por el usuario.




## Panel del sitio

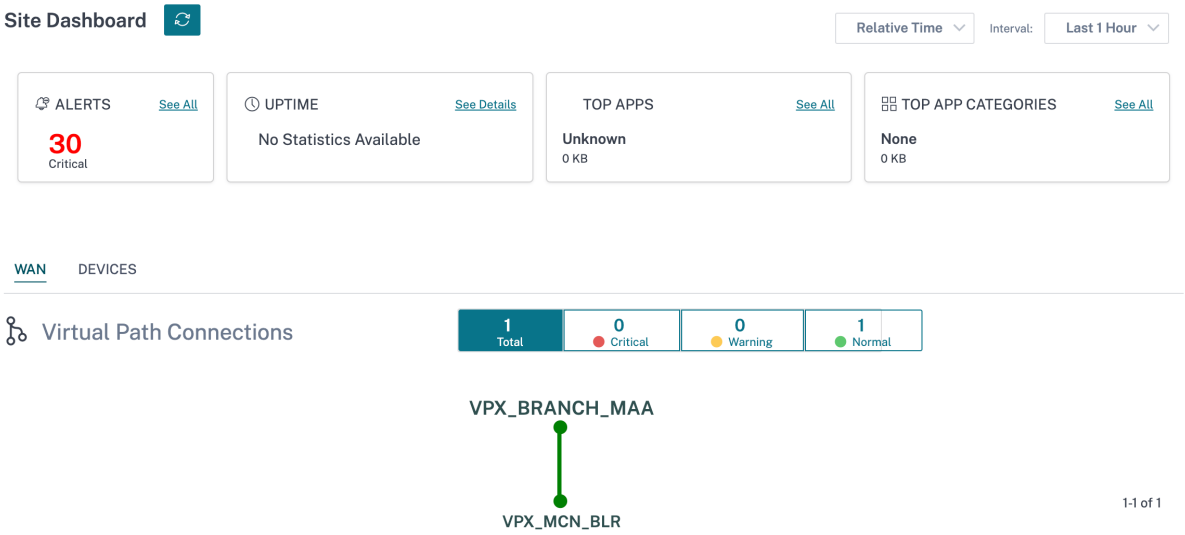
October 31, 2022

El panel del sitio proporciona una descripción general del estado y las tendencias de uso de un sitio.

El panel resume los siguientes aspectos de un sitio, con una provisión para profundizar para obtener más detalles.

- **Alertas críticas**: Recuento continuo de las alertas de salud críticas, si las hay, que aparecen en el sitio.
- **Tiempo de actividad**: Comparación en paralelo del tiempo de actividad promedio que ofrecen las rutas de superposición virtual de SD-WAN con las rutas subyacentes físicas asociadas a un sitio
- **Tendencias de uso**: Principales aplicaciones y categorías de aplicaciones asociadas a un sitio, según el volumen de tráfico
- **Detalles del sitio**: Conexiones WAN y dispositivos asociados a un sitio




> **Sugerencia**
>
> Haga clic en **Ver todoo Ver detalles** para ver estadísticas más detalladas.

Todas las conexiones de ruta virtual superpuestas asociadas a un sitio se muestran con codificación de colores adecuada para reflejar el estado de cada conexión.

Puede seleccionar cualquier conexión de ruta virtual, para revisar las métricas de estado y tendencias correspondientes.

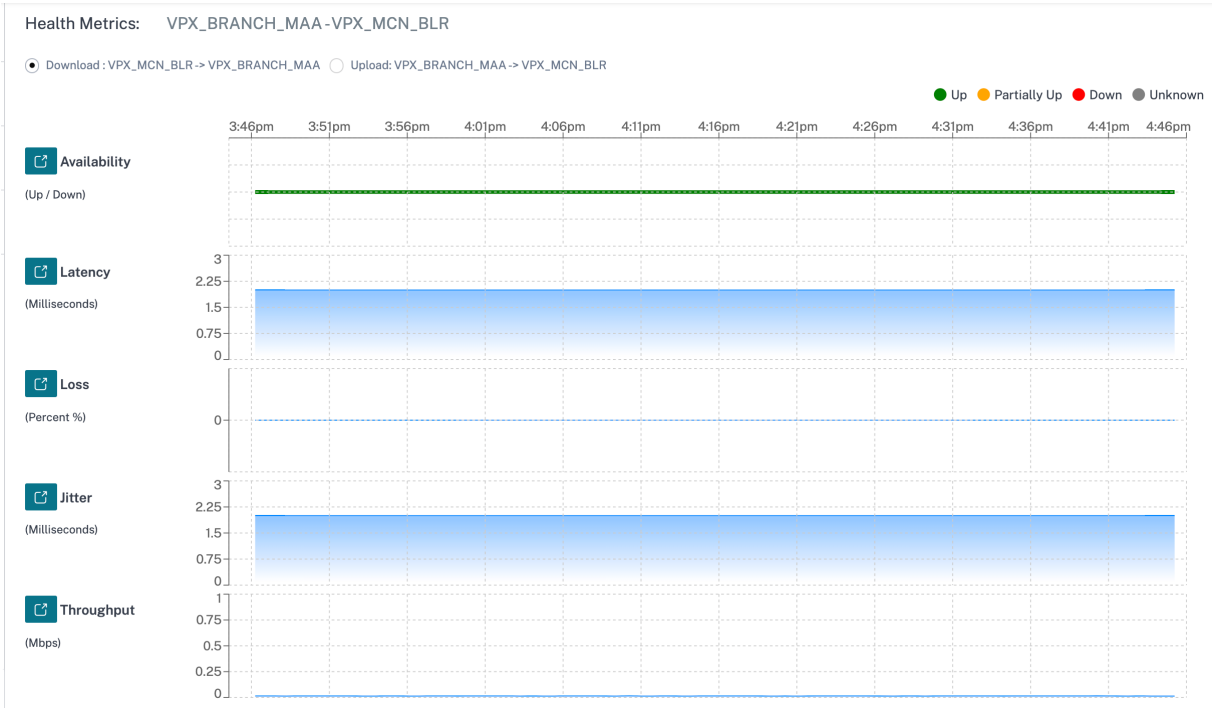
Los criterios de codificación de colores utilizados para las conexiones de rutas virtuales son:

- **Crítico (rojo)**: La ruta virtual está DESACTIVADA.
- **Advertencia (naranja)**: La ruta virtual está ARRIBA, pero al menos una ruta de miembro está ABAJO.
- **Normal (verde)**: La ruta virtual y todas las rutas de los miembros están activas.

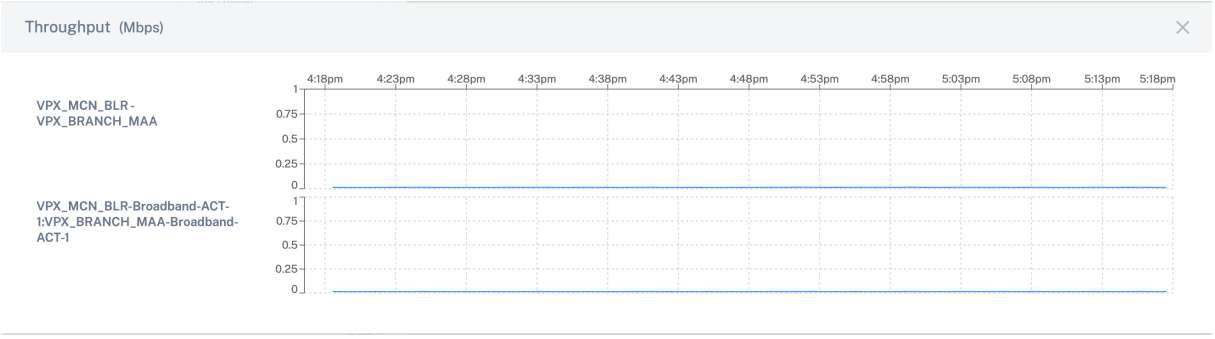
### Métricas de estado

Las métricas de estado y las tendencias gráficas en torno a la disponibilidad, latencia, pérdida, fluctuación y rendimiento se muestran para la conexión de ruta virtual seleccionada. Estas estadísticas están disponibles en ambas direcciones: **WAN a LAN** y **LAN a WAN**. Todas las métricas se pueden revisar en relación con una línea de tiempo común, para ayudar a reducir rápidamente el dominio del problema durante la solución de problemas.




Puede profundizar más en cada métrica de mantenimiento para obtener una vista comparativa de la ruta virtual de superposición y las rutas de miembro del calco subyacente para la misma métrica. Esto ayudaría a solucionar problemas de superposición versus calco subyacente.

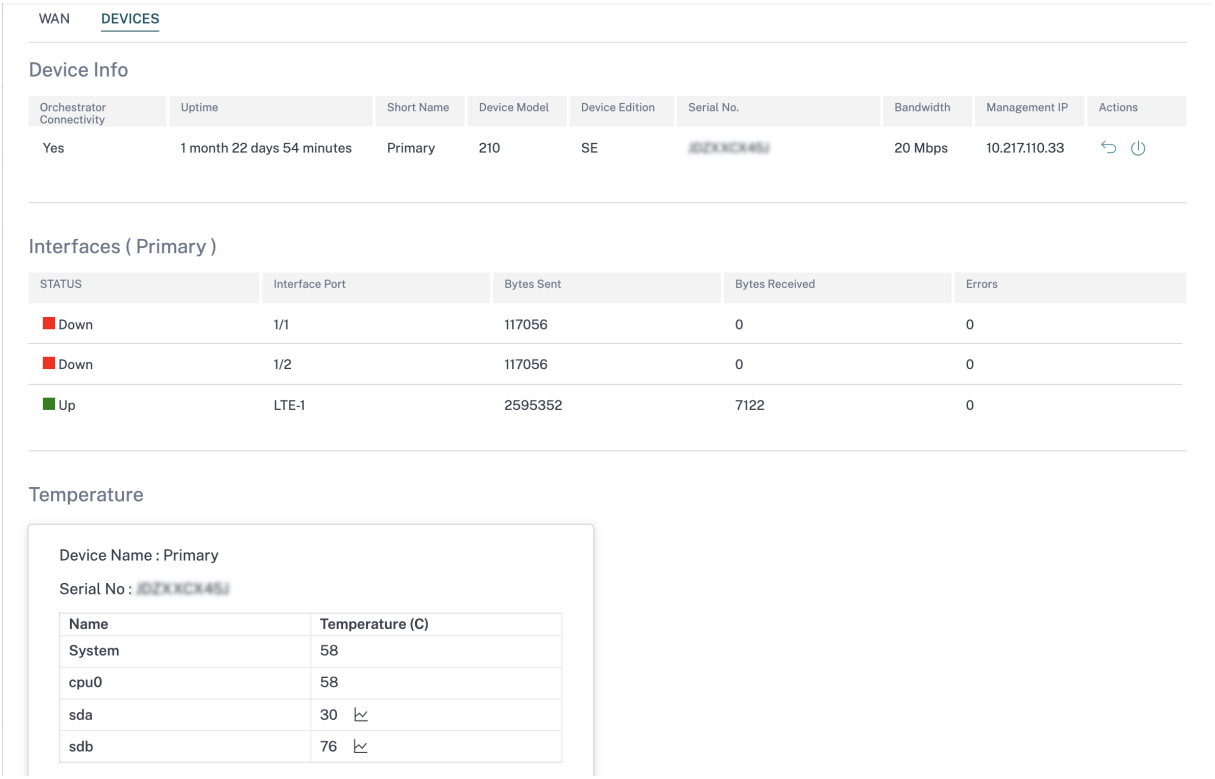



## Dispositivos

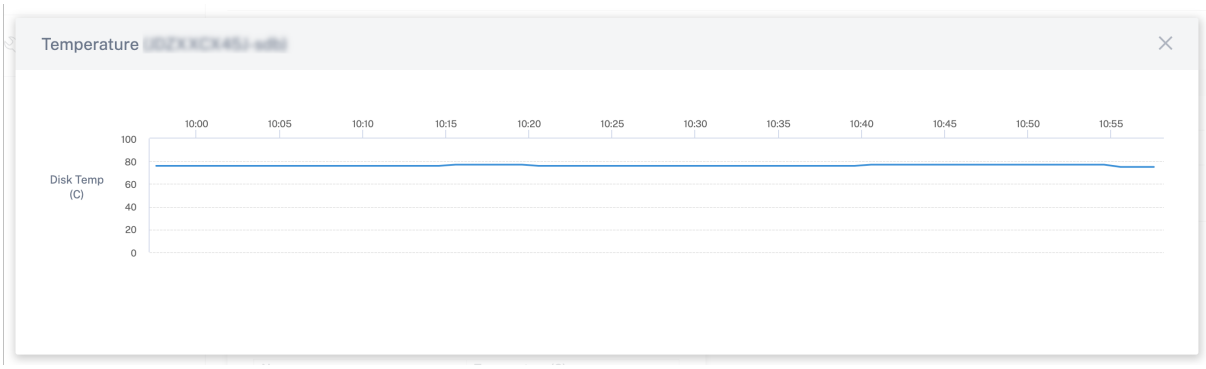
La ficha **Dispositivos** muestra los detalles asociados con los dispositivos, las interfaces y la temperatura del disco del sitio. También puede reiniciar el dispositivo, restablecer la configuración del dispositivo o descargar los registros del dispositivo.

La sección **Temperatura** muestra la temperatura del sistema, la CPU y los discos en grados Celsius.




También puede hacer clic en el icono gráfico de la columna **Temperatura (C)** y ver la información en forma gráfica.




## Solución de problemas del proveedor

October 31, 2022

La página de registros de auditoría de proveedores muestra los registros al nivel de proveedor y los registros de dispositivos, lo que permite solucionar problemas

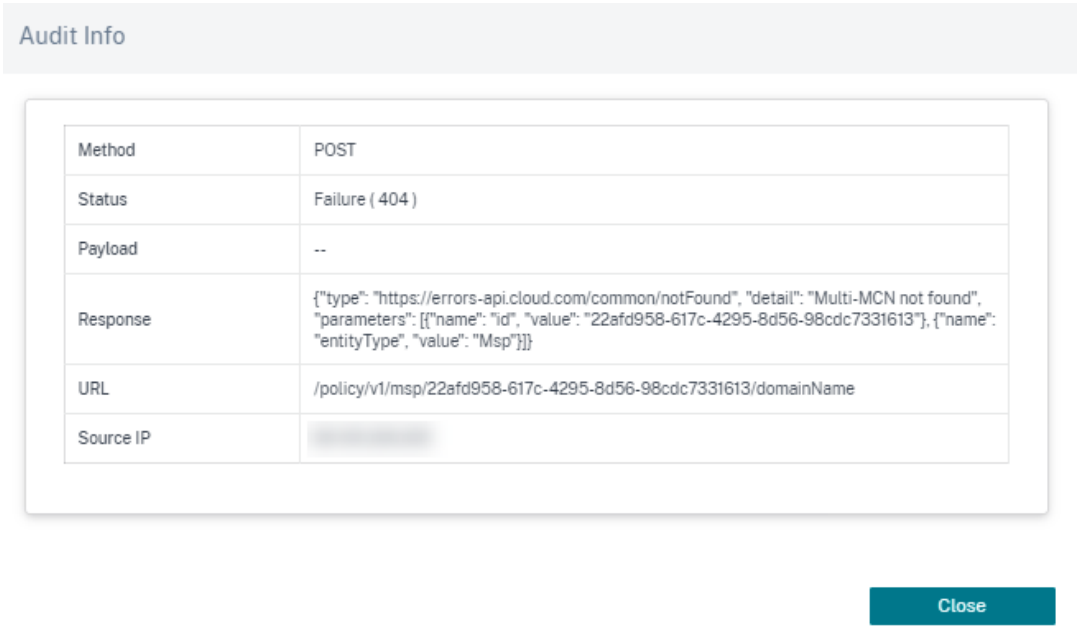
### Registros de auditoría

Los registros de auditoría capturan la acción, la hora y el resultado de la acción realizada por los proveedores. Vaya a **Solución de problemas** > **Registros de auditoría** para ver la página **Solución de problemas del proveedor: Registros de auditoría**.

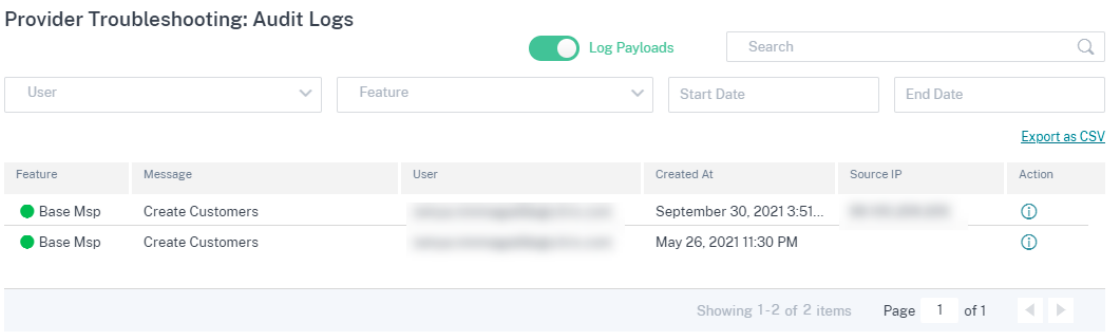
La página de registros de auditoría de proveedores muestra la siguiente información:

- **Barra de**búsqueda: busque una actividad de auditoría basada en una palabra clave.
- **Opciones de filtrado**: Ejecute una búsqueda en el registro de auditoría filtrando según los siguientes criterios:
  - Usuario
  - Función
  - Intervalo de tiempo
- **Exportar como CSV**: Al hacer clic en esta opción, las entradas del registro de auditoría se exportan a un archivo CSV.
- **Información de auditoría**: Seleccione el icono de la columna **Acción** para ir a la sección **Información de auditoría**. En esta sección se proporciona la siguiente información:
  - **Método: método**de solicitud HTTP de la API invocada.
  - **Estado**: Resultado de la solicitud de API.
  - **Carga útil**: Cuerpo de la solicitud enviada a través de la API.
  - **Respuesta: Respuesta**de error cuando la solicitud de la API falla. Este campo solo se muestra cuando se produce un error en la solicitud de API.
  - **URL**: URL HTTP de la API revocada.
  - **IP de origen**: La dirección IP del punto final desde el que se configuró la función. Este campo se muestra en la página Registros de auditoría y en la página Información de auditoría.




- **Registrar cargas útiles**: De forma predeterminada, esta opción está inhabilitada. Cuando se habilita, el cuerpo de la solicitud del mensaje de la API se muestra en la sección **Información de auditoría**. Para obtener más información sobre la API, consulte la guía de API para Citrix SD-WAN Orchestrator.




## Solución de problemas de red

October 31, 2022

Los clientes pueden ver los registros de todos los dispositivos de red, lo que permite solucionar problemas rápidamente.

### Registros de auditoría

Los registros de auditoría capturan la acción, la hora y el resultado de la acción realizada por los usuarios en la red de un cliente. Vaya a **Solución de problemas de SD-WAN** > **Registros de auditoría** para ver la página **Registros de auditoría de solución de problemas de SD-WAN**.

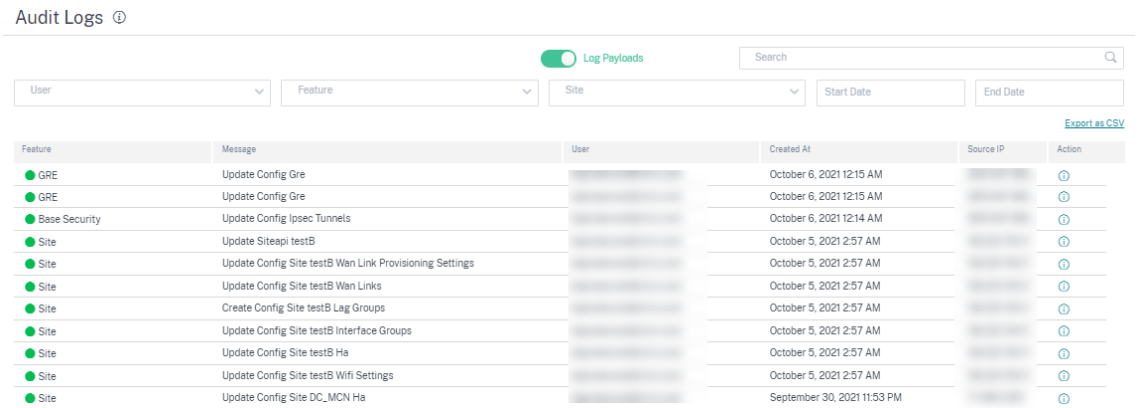
La página Registros de auditoría de solución de problemas de SD-WAN muestra la siguiente información:

- **Barra de**búsqueda: busque una actividad de auditoría basada en una palabra clave.
- **Opciones de filtrado**: Ejecute una búsqueda en el registro de auditoría filtrando según los siguientes criterios:
  - Usuario
  - Función
  - Sitio
  - Intervalo de tiempo
- **Exportar como CSV**: Al hacer clic en esta opción, las entradas del registro de auditoría se exportan a un archivo CSV.
- **Información de auditoría**: Seleccione el icono de la columna **Acción** para ir a la sección **Información de auditoría**. En esta sección se proporciona la siguiente información:
  - **Método: método**de solicitud HTTP de la API invocada.
  - **Estado**: Resultado de la solicitud de API. Aparece la siguiente respuesta de error cuando se produce un error en la solicitud de la API.
  - **Carga útil**: Cuerpo de la solicitud enviada a través de la API.
  - **Respuesta: Respuesta**de error cuando la solicitud de la API falla. Este campo solo se muestra cuando se produce un error en la solicitud de API.
  - **URL**: URL HTTP de la API revocada.

- **IP de origen**: La dirección IP del punto final desde el que se configuró la función. Este campo se muestra en la página Registros de auditoría y en la página Información de auditoría.
- **Qué ha cambiado**: Esta sección muestra los registros de todos los cambios realizados en las funciones a través de la interfaz de usuario. Active el botón Registrar cargas útiles para ver los cambios en la sección Información de auditoría.


- **Registrar cargas útiles**: De forma predeterminada, esta opción está inhabilitada. Cuando se habilita, el cuerpo de la solicitud del mensaje de la API se muestra en la sección **Información de auditoría**. Para obtener más información sobre la API, consulte la guía de API para Citrix SD-WAN Orchestrator.

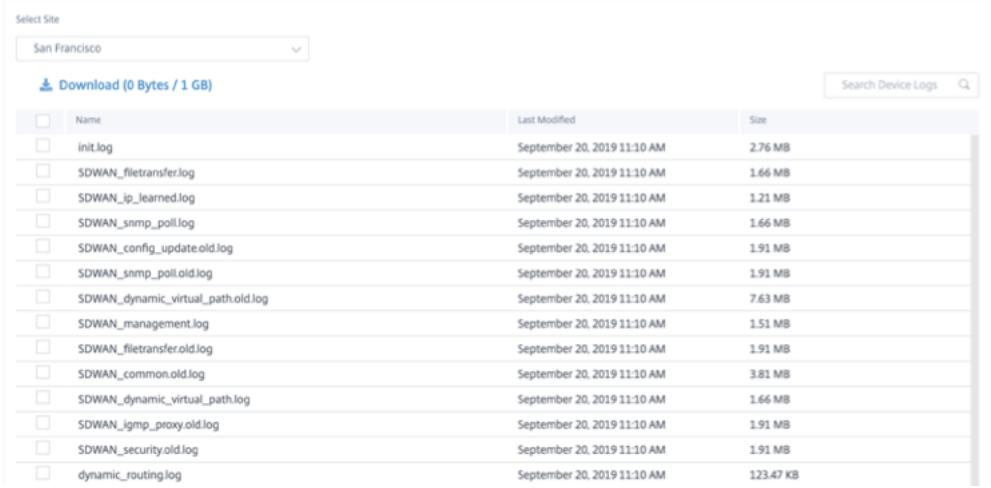


### Registros de dispositivos

Los clientes pueden ver los registros de dispositivos específicos de los sitios.

Puede seleccionar registros de dispositivos específicos, descargarlos y compartirlos con administradores del sitio si es necesario.



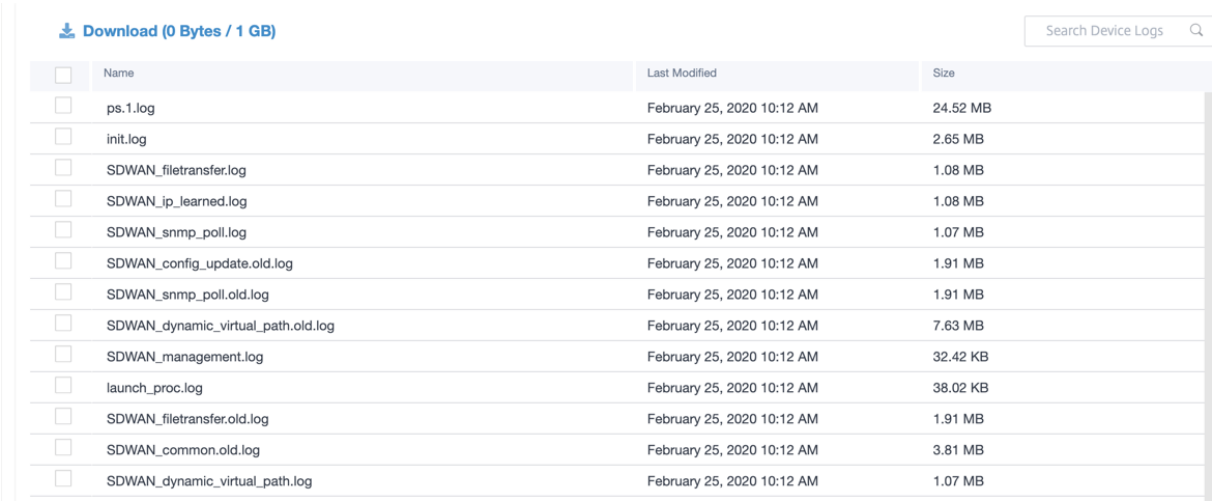

## Solución de problemas del sitio

October 31, 2022

### Registros de dispositivos

Los registros son útiles para solucionar problemas. El administrador del sitio puede ver una lista de todos los registros capturados en todos los dispositivos del sitio. También puede descargar registros para verificarlos.

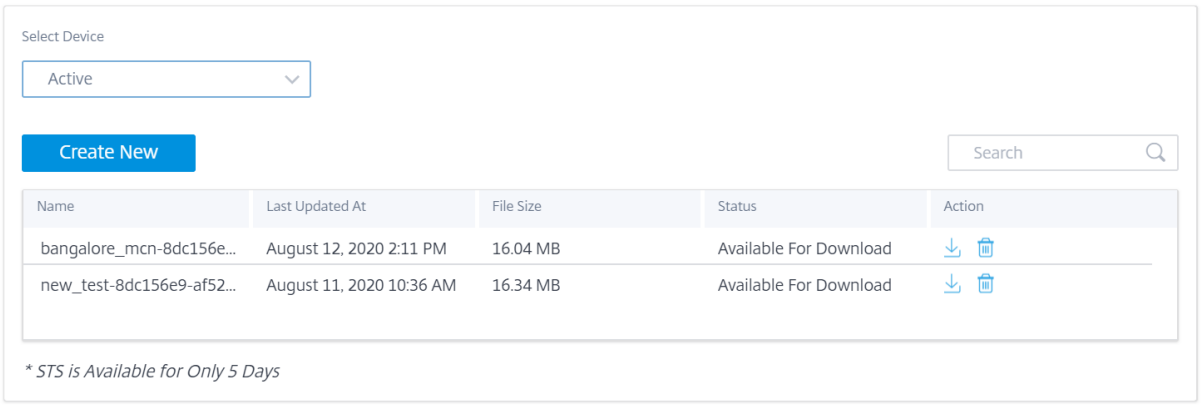



## Mostrar paquete de soporte técnico

El paquete Show Tech Support (STS) contiene información importante del sistema en tiempo real, como registros de acceso, registros de diagnóstico y registros de firewall. El paquete STS se utiliza para solucionar problemas en los dispositivos SD-WAN. Puede crear, descargar el paquete STS y compartirlo con los representantes de soporte de Citrix.

Si un sitio está configurado en el modo de implementación de HA, puede seleccionar el dispositivo activo o en espera para el que quiere crear o descargar el paquete STS.

Para crear un paquete de STS para un dispositivo de sitio, al nivel de sitio, vaya a **Solución de problemas** > **Paquete de STS** y haga clic en **Crear nuevo**.

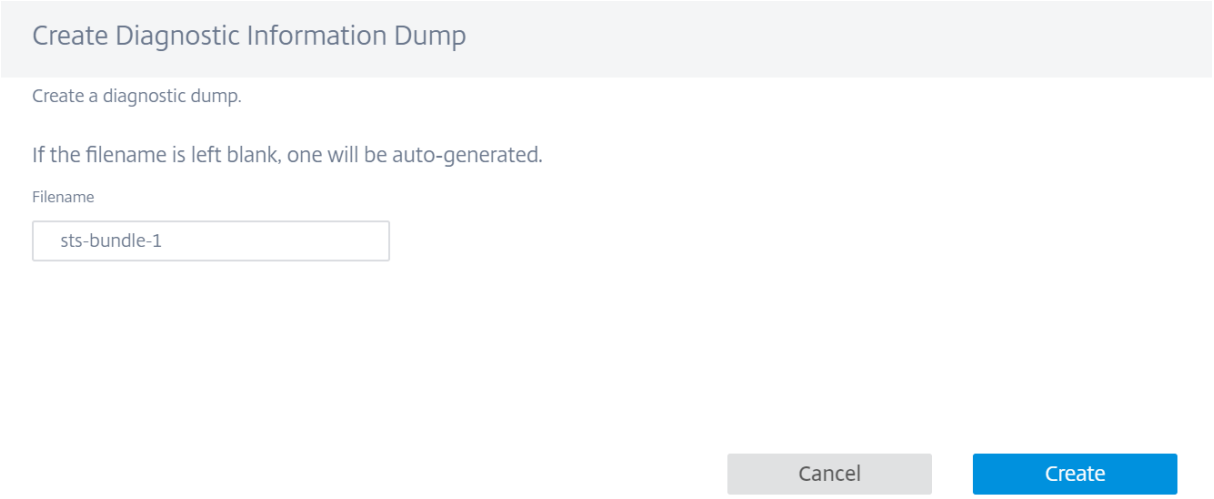



Proporcione un nombre para el paquete STS. El nombre debe comenzar con una letra y puede contener letras, números, guiones y guiones bajos. La longitud máxima permitida del nombre es de 32 caracteres. El nombre proporcionado por el usuario se utiliza como prefijo en el nombre final. Para garantizar que los nombres de los archivos sean únicos (fecha y hora) y para ayudar a reconocer el dispositivo en el paquete STS (número de serie), el servicio genera un nombre completo. Si no se

proporciona ningún nombre, se generará automáticamente un nombre al crear el paquete.

Puede solicitar un nuevo STS solo cuando el dispositivo esté en línea y no se esté ejecutando ningún proceso de STS en ejecución en el dispositivo. Puede descargar un STS ya disponible desde el servicio Citrix SD-WAN Orchestrator incluso si el dispositivo está fuera de línea.




En un momento dado, el proceso STS se encuentra en uno de los siguientes estados:

| Estado STS | Descripción |
|---|---|
| Solicitada | Se solicita un nuevo paquete STS. La solicitud tarda unos minutos en procesarse. Puede optar por cancelar el proceso de creación de STS, si es necesario. |
| Cargando | El paquete STS creado se carga en el servicio en la nube. La duración depende del tamaño del paquete. El estado se actualiza cada 5 segundos. No puede cancelar el proceso de carga STS. |
| Fracaso | El proceso STS ha fallado durante la creación o la carga. Puede eliminar las entradas de operaciones STS fallidas. |
| Disponible para descarga | El proceso de creación y carga de STS se realiza correctamente. Ahora puede descargar o eliminar los paquetes STS. |

Una vez que se inicia el proceso STS en el dispositivo, el progreso se actualiza en la columna de estado a intervalos regulares. Por ejemplo, **Solicitado (Recopilación de archivos de registro)**.

Los paquetes STS y los registros de errores se mantienen durante 7 días, después de los cuales se

eliminan automáticamente.

# Informes de proveedores

October 31, 2022

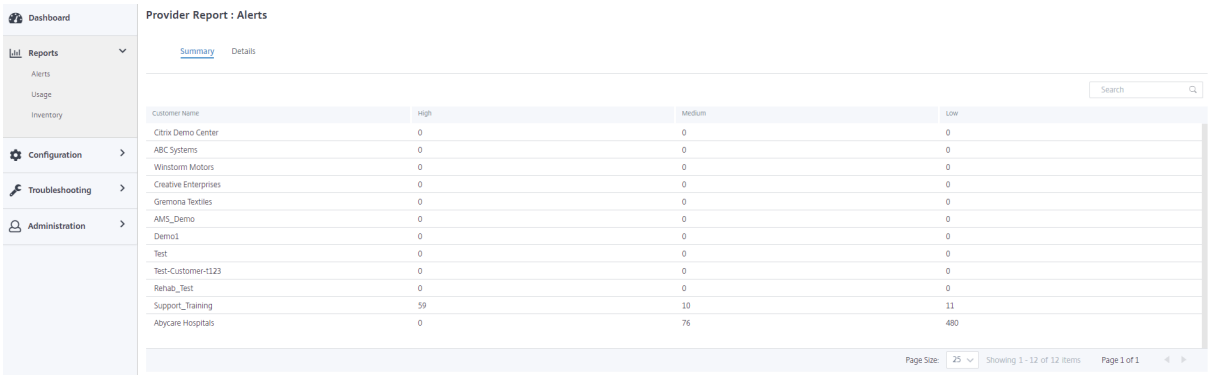
**Los informes de proveedores** proporcionan visibilidad de las alertas, las tendencias de uso y el inventario agregado de todos los clientes gestionados por un proveedor.

En la interfaz de usuario al nivel de proveedor de servicios de Citrix SD-WAN Orchestrator, vaya a **Informes**.

## Alertas

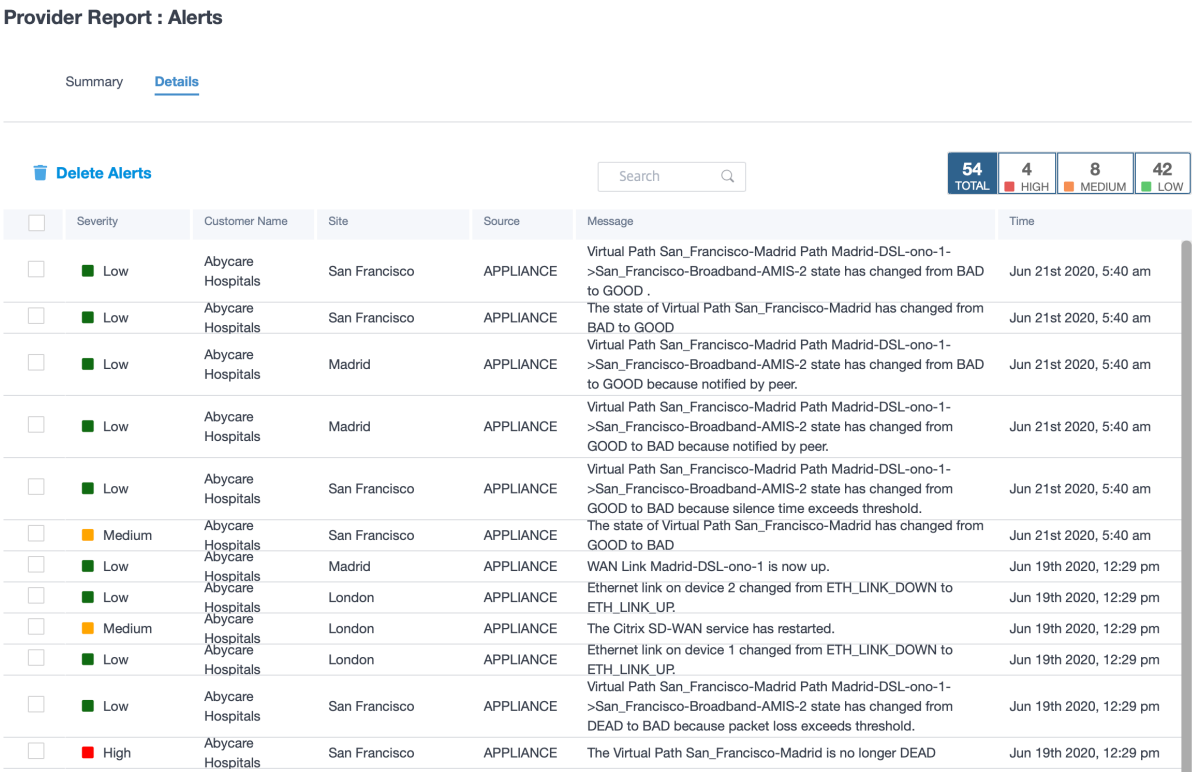
El proveedor puede revisar todos los eventos y alertas generados en todas las redes de clientes.

La vista de **resumen** muestra el número de alertas altas, medias y bajas para cada cliente.




También puede ver la gravedad, el sitio en el que se originó la alerta, el mensaje de alerta, la hora y otra información en **Detalles**.




| Severity | Customer Name | Site | Source | Message | Time |
|---|---|---|---|---|---|
| Low | Abycare Hospitals | San Francisco | APPLIANCE | Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has changed from BAD to GOOD . | Jun 21st 2020, 5:40 am |
| Low | Abycare Hospitals | San Francisco | APPLIANCE | The state of Virtual Path San_Francisco-Madrid has changed from BAD to GOOD | Jun 21st 2020, 5:40 am |
| Low | Abycare Hospitals | Madrid | APPLIANCE | Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has changed from BAD to GOOD because notified by peer. | Jun 21st 2020, 5:40 am |
| Low | Abycare Hospitals | Madrid | APPLIANCE | Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has changed from GOOD to BAD because notified by peer. | Jun 21st 2020, 5:40 am |
| Low | Abycare Hospitals | San Francisco | APPLIANCE | Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has changed from GOOD to BAD because silence time exceeds threshold. | Jun 21st 2020, 5:40 am |
| Medium | Abycare Hospitals | San Francisco | APPLIANCE | The state of Virtual Path San_Francisco-Madrid has changed from GOOD to BAD | Jun 21st 2020, 5:40 am |
| Low | Abycare Hospitals | Madrid | APPLIANCE | WAN Link Madrid-DSL-ono-1 is now up. | Jun 19th 2020, 12:29 pm |
| Low | Abycare Hospitals | London | APPLIANCE | Ethernet link on device 2 changed from ETH_LINK_DOWN to ETH_LINK_UP. | Jun 19th 2020, 12:29 pm |
| Medium | Abycare Hospitals | London | APPLIANCE | The Citrix SD-WAN service has restarted. | Jun 19th 2020, 12:29 pm |
| Low | Abycare Hospitals | London | APPLIANCE | Ethernet link on device 1 changed from ETH_LINK_DOWN to ETH_LINK_UP. | Jun 19th 2020, 12:29 pm |
| Low | Abycare Hospitals | San Francisco | APPLIANCE | Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has changed from DEAD to BAD because packet loss exceeds threshold. | Jun 19th 2020, 12:29 pm |
| High | Abycare Hospitals | San Francisco | APPLIANCE | The Virtual Path San_Francisco-Madrid is no longer DEAD | Jun 19th 2020, 12:29 pm |

Se pueden utilizar las opciones de filtrado adecuadas según sea necesario, por ejemplo: busque las alertas de alta gravedad en todos los clientes o las alertas de un cliente determinado, etc.

También puede seleccionar y eliminar alertas.

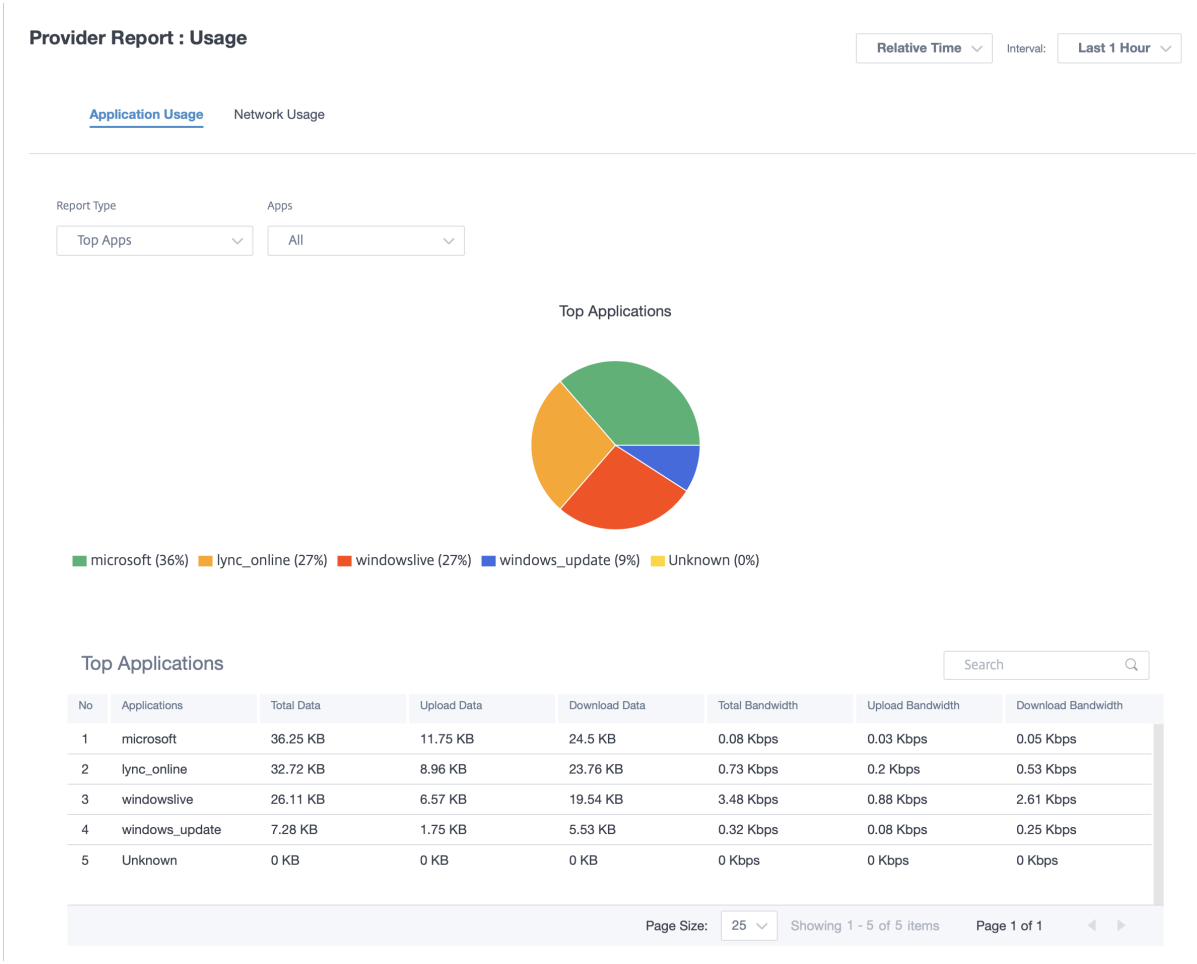
## Uso

El proveedor puede revisar las tendencias de uso entre clientes, como las **principales aplicaciones, lasprincipales categorías de aplicaciones**, el ancho de**banda de las aplicacionesylos sitios principales**.

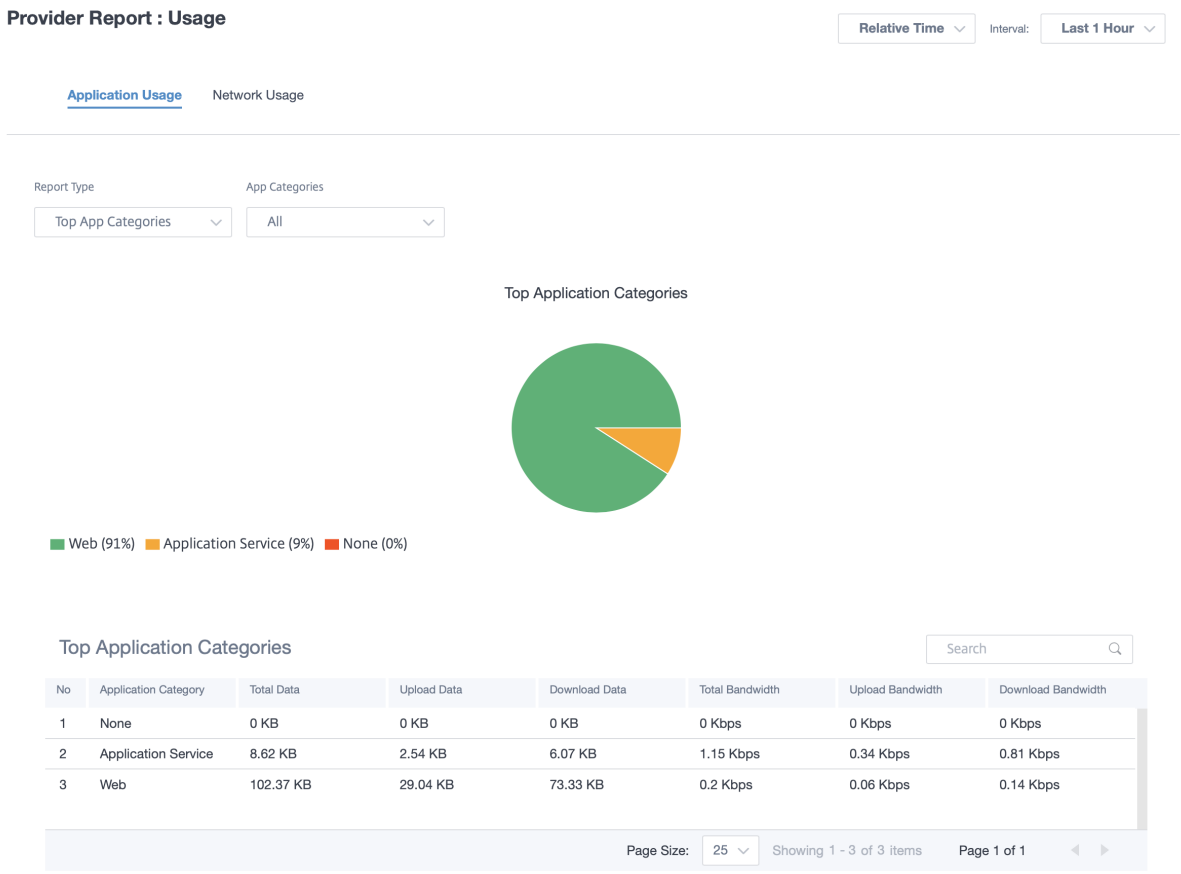
### Principales categorías de aplicaciones y aplicaciones

El cuadro de **aplicaciones principalesy categorías de aplicaciones** principales muestra las aplicaciones y familias de aplicaciones que se utilizan ampliamente en todas las redes de clientes. Esto le permite analizar el patrón de consumo de datos y reasignar el límite de ancho de banda para cada clase de datos, si es necesario.

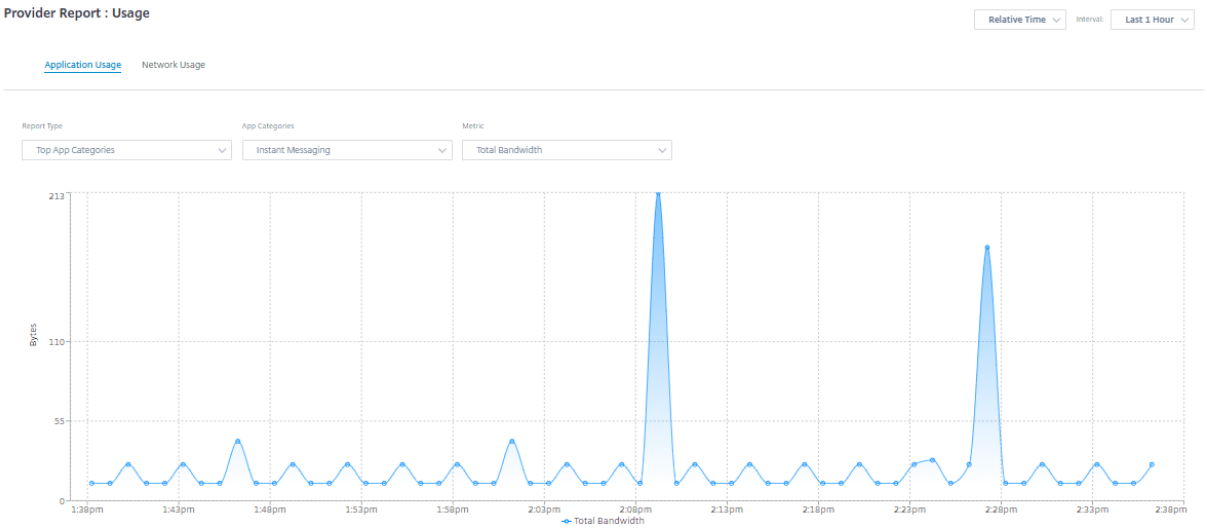
 






Puede ver las estadísticas de uso del ancho de banda. Las estadísticas de ancho de banda se recopilan para el intervalo de tiempo seleccionado. Puede filtrar el informe de estadísticas según el **tipo de informe, las categorías de aplicaciones o aplicaciones** y **las métricas**.




- **Tipo de informe: S**eleccione las **mejores aplicaciones o categorías** de aplicaciones de la lista.
- **Aplicaciones/Categorías de aplicaciones: S**eleccione las principales aplicaciones o categorías

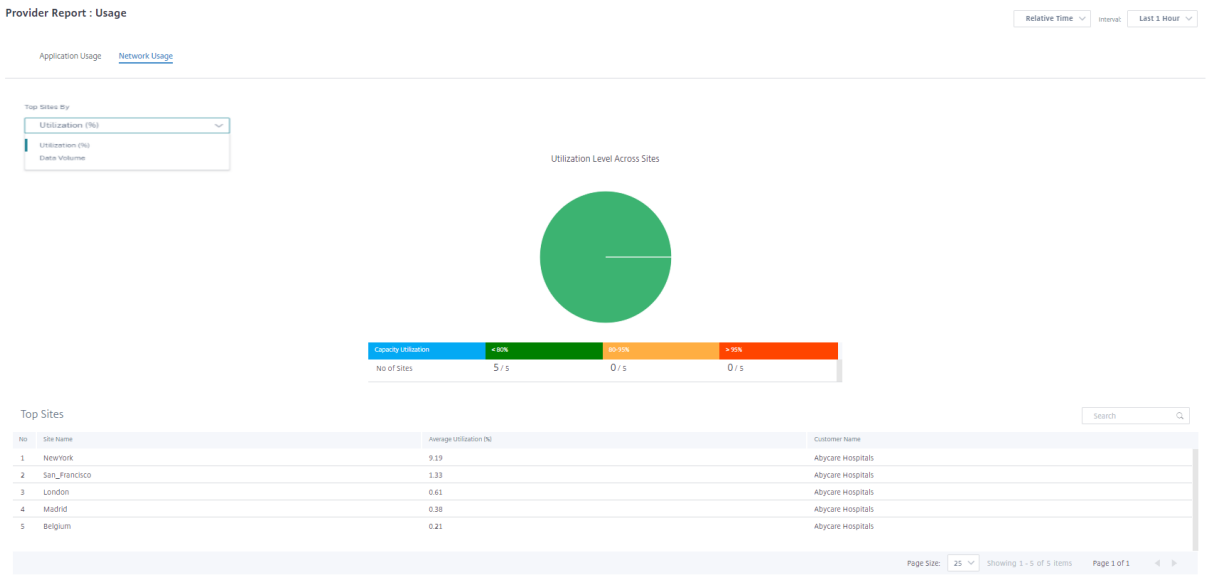
 

de la lista.

- **Métrica: S**eleccione la métrica de ancho de banda (como datos totales, datos entrantes, ancho de banda total) de la lista.

### Uso de la red

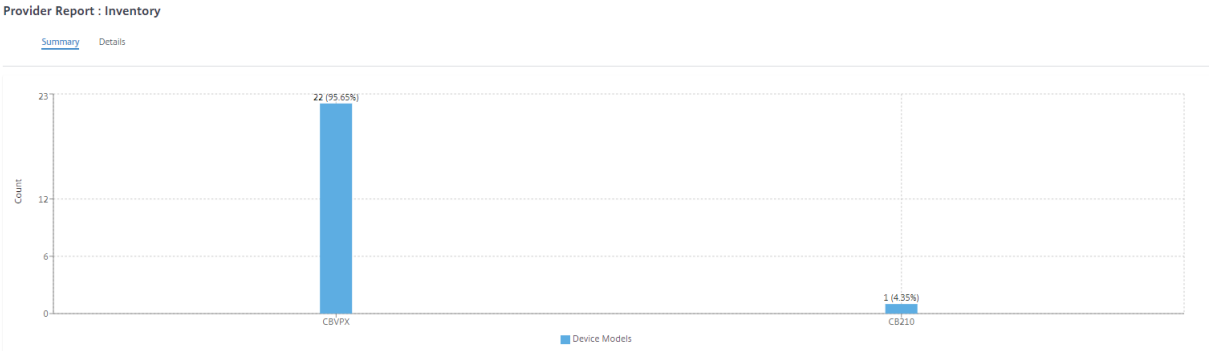
El gráfico de uso de red muestra los 10 sitios principales de todos los clientes que tienen el mayor uso de ancho de banda. Puede ver los sitios por uso (%) o volumen de datos (MB).




## Inventory

El proveedor puede ver todo el inventario del dispositivo en todos los clientes. Puede elegir ver un resumen del inventario o una vista detallada.

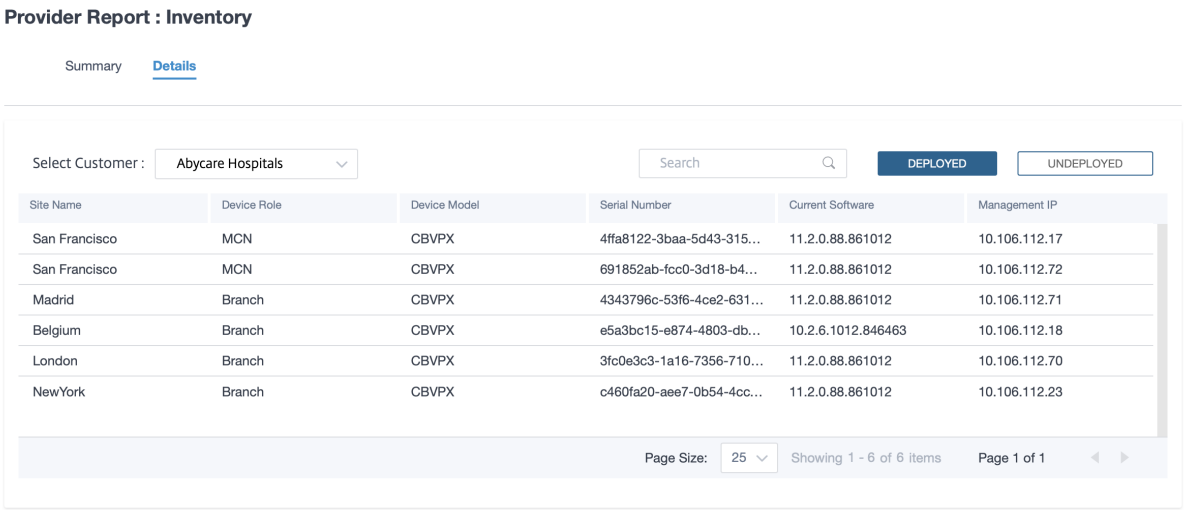
La vista de resumen de inventario proporciona un gráfico de la distribución del inventario, que muestra los distintos modelos de dispositivos y el número de cada tipo de dispositivos utilizados en las redes de clientes.



Se pueden utilizar opciones de filtrado adecuadas según sea necesario, por ejemplo: Busque todos los dispositivos pertenecientes a un cliente específico, o todos los dispositivos con un determinado modelo de dispositivo, etc.

La vista detallada del inventario proporciona una lista de todos los dispositivos que se implementan y aquellos que están configurados pero aún no implementados. Elija un cliente de la lista desplegable **Seleccionar cliente**. Puede ver el nombre del sitio, el rol del dispositivo, el modelo del dispositivo, el número de serie del dispositivo, el software actual y la dirección IP de administración del dispositivo.




## Informes de cliente/red

October 31, 2022

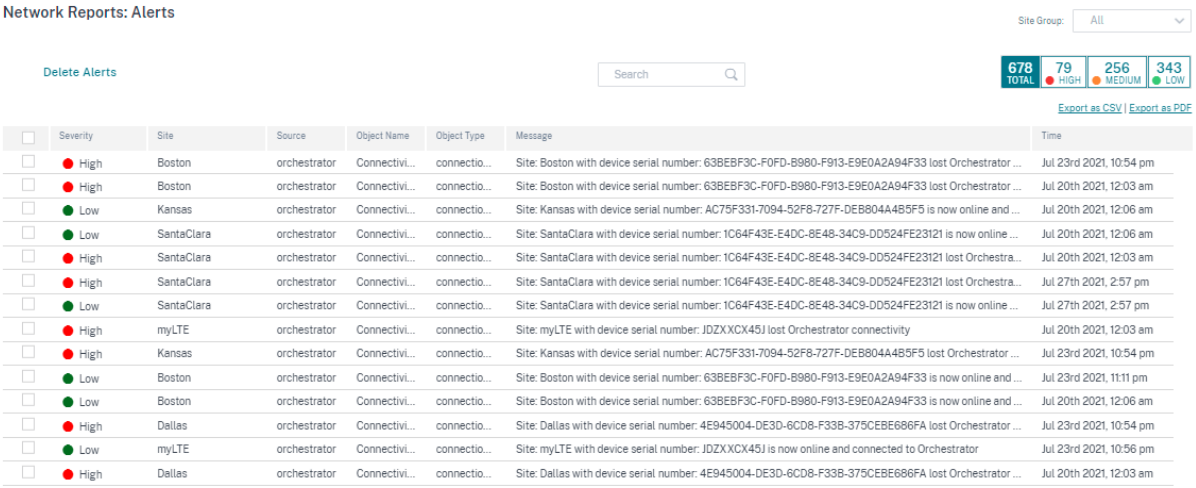
**Los informes de clientes** proporcionan visibilidad de las alertas de toda la red, las tendencias de uso, el inventario, la calidad, los diagnósticos y el estado del firewall agregados en todos los sitios de una red de clientes.

### Alertas

El cliente puede revisar un informe detallado de todos los eventos y alertas generados en todos los sitios de esta red.

Incluye la gravedad, el sitio en el que se originó la alerta, el mensaje de alerta, la hora y otros detalles.




| Severity | Site | Source | Object Name | Object Type | Message | Time |
|---|---|---|---|---|---|---|
| High | Boston | orchestrator | Connectivi... | connectio... | Site: Boston with device serial number: 63BEBF3C-F0FD-B980-F913-E9E0A2A94F33 lost Orchestrator ... | Jul 23rd 2021, 10:54 pm |
| High | Boston | orchestrator | Connectivi... | connectio... | Site: Boston with device serial number: 63BEBF3C-F0FD-B980-F913-E9E0A2A94F33 lost Orchestrator ... | Jul 20th 2021, 12:03 am |
| Low | Kansas | orchestrator | Connectivi... | connectio... | Site: Kansas with device serial number: AC75F331-7094-52F8-727F-DEB804A4B5F5 is now online and ... | Jul 20th 2021, 12:06 am |
| Low | SantaClara | orchestrator | Connectivi... | connectio... | Site: SantaClara with device serial number: 1C64F43E-E4DC-8E48-34C9-DD524FE23121 is now online ... | Jul 20th 2021, 12:06 am |
| High | SantaClara | orchestrator | Connectivi... | connectio... | Site: SantaClara with device serial number: 1C64F43E-E4DC-8E48-34C9-DD524FE23121 lost Orchestra... | Jul 20th 2021, 12:03 am |
| High | SantaClara | orchestrator | Connectivi... | connectio... | Site: SantaClara with device serial number: 1C64F43E-E4DC-8E48-34C9-DD524FE23121 lost Orchestra... | Jul 27th 2021, 2:57 pm |
| Low | SantaClara | orchestrator | Connectivi... | connectio... | Site: SantaClara with device serial number: 1C64F43E-E4DC-8E48-34C9-DD524FE23121 is now online ... | Jul 27th 2021, 2:57 pm |
| High | myLTE | orchestrator | Connectivi... | connectio... | Site: myLTE with device serial number: JDZXXCX45J lost Orchestrator connectivity | Jul 20th 2021, 12:03 am |
| High | Kansas | orchestrator | Connectivi... | connectio... | Site: Kansas with device serial number: AC75F331-7094-52F8-727F-DEB804A4B5F5 lost Orchestrator ... | Jul 23rd 2021, 10:54 pm |
| Low | Boston | orchestrator | Connectivi... | connectio... | Site: Boston with device serial number: 63BEBF3C-F0FD-B980-F913-E9E0A2A94F33 is now online and ... | Jul 23rd 2021, 11:11 pm |
| Low | Boston | orchestrator | Connectivi... | connectio... | Site: Boston with device serial number: 63BEBF3C-F0FD-B980-F913-E9E0A2A94F33 is now online and ... | Jul 20th 2021, 12:06 am |
| High | Dallas | orchestrator | Connectivi... | connectio... | Site: Dallas with device serial number: 4E945004-DE3D-6CD8-F33B-375CEBE686FA lost Orchestrator ... | Jul 23rd 2021, 10:54 pm |
| Low | myLTE | orchestrator | Connectivi... | connectio... | Site: myLTE with device serial number: JDZXXCX45J is now online and connected to Orchestrator | Jul 23rd 2021, 10:56 pm |
| High | Dallas | orchestrator | Connectivi... | connectio... | Site: Dallas with device serial number: 4E945004-DE3D-6CD8-F33B-375CEBE686FA lost Orchestrator ... | Jul 20th 2021, 12:03 am |

Las opciones de filtrado adecuadas se pueden utilizar según sea necesario, por ejemplo: Busque todas las alertas de alta gravedad en todos los sitios, o todas las alertas de un sitio en particular, etc.

También puede seleccionar y borrar alertas.

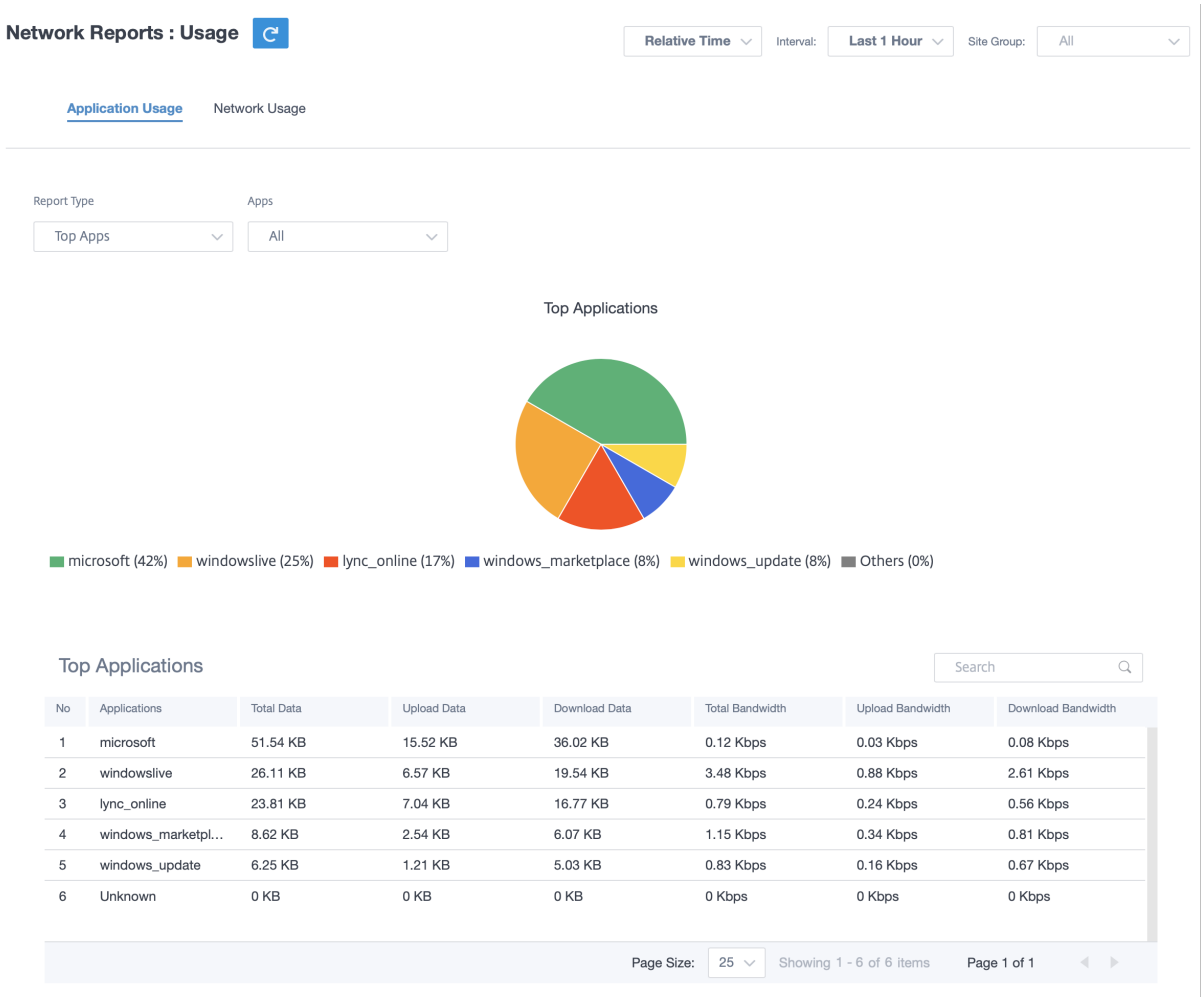
## Uso

Los clientes pueden revisar las tendencias de uso, como las **aplicaciones principales, lascategorías de aplicaciones**principales, el**ancho**de banda de las aplicaciones y los**sitios principales** en todos los sitios de su red.

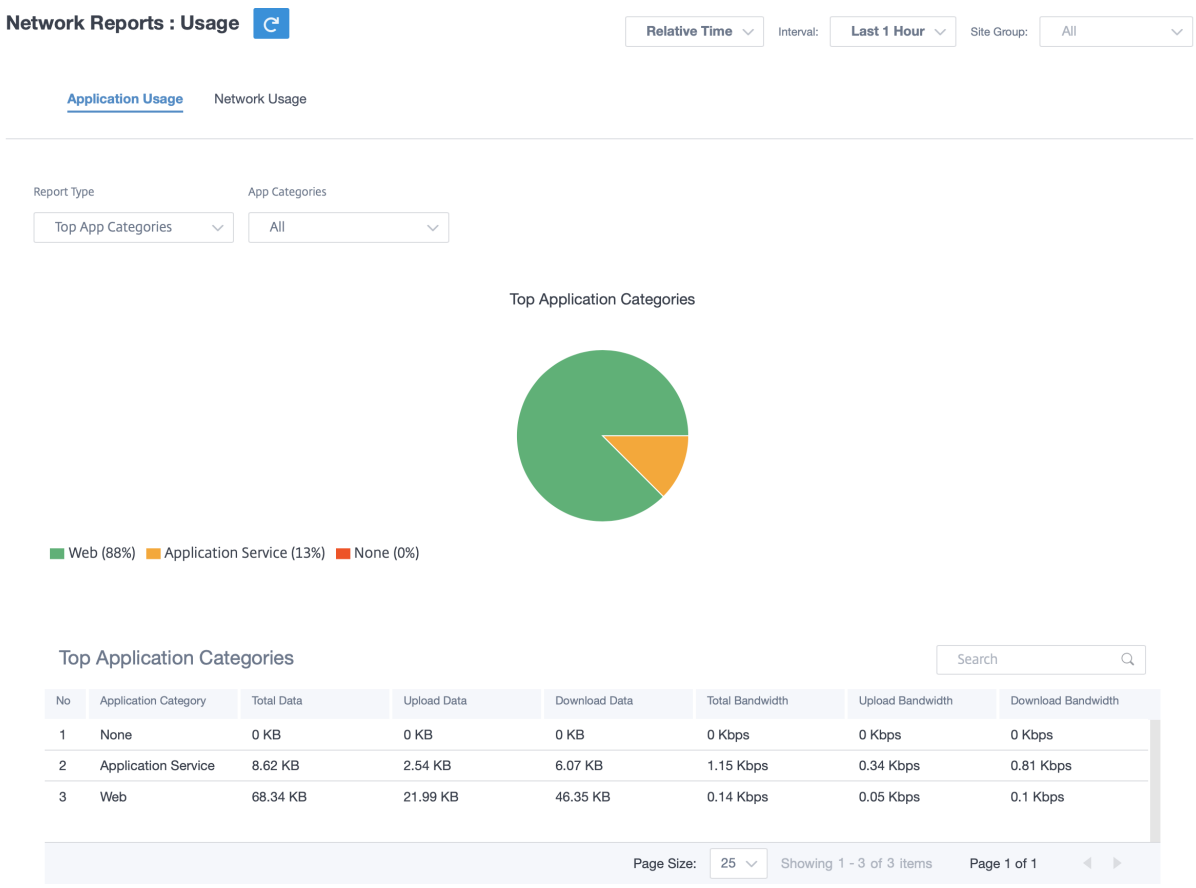
### Principales categorías de aplicaciones y aplicaciones

La tabla de **aplicaciones principalesy categorías de aplicaciones** principales muestra las aplicaciones principales y las principales familias de aplicaciones que se utilizan ampliamente en todos los sitios. Esto le permite analizar el patrón de consumo de datos y reasignar el límite de ancho de banda para cada clase de datos dentro de la red.



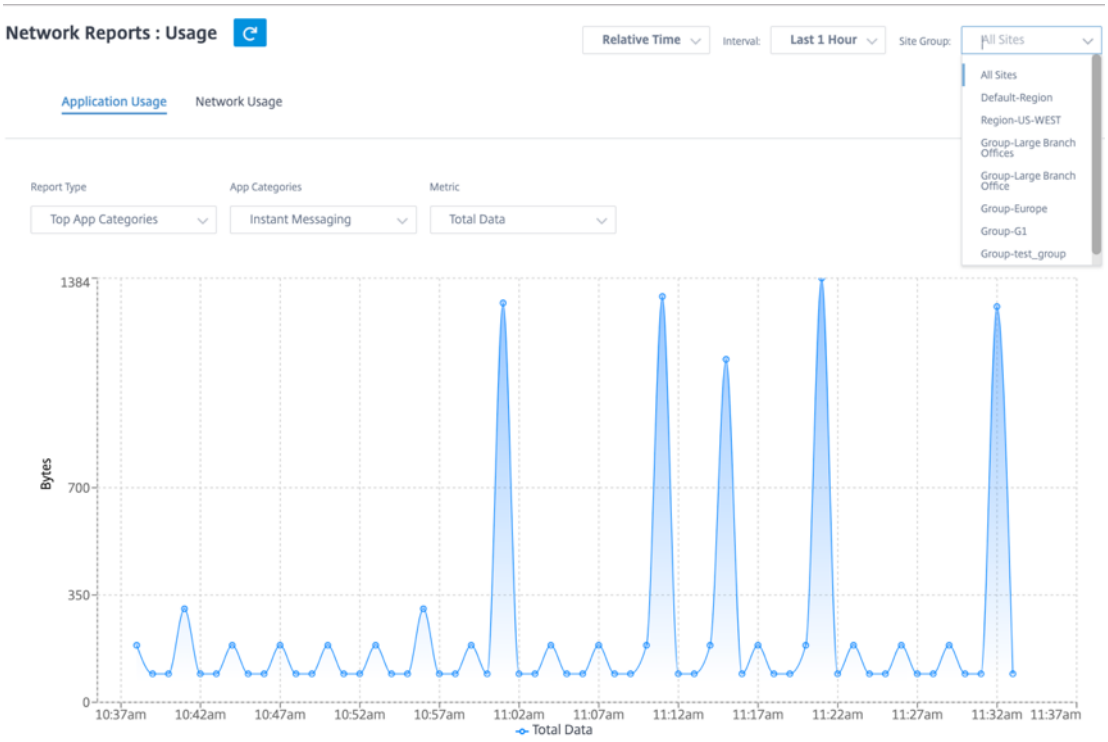

 




### Ancho de banda

Puede ver las estadísticas de uso de ancho de banda para el grupo de sitios seleccionado o para todos los sitios. Las estadísticas de ancho de banda se recopilan para el intervalo de tiempo seleccionado. Puede filtrar el informe de estadísticas según el **tipo de informe, las categorías de aplicaciones o aplicaciones** y **las métricas**.

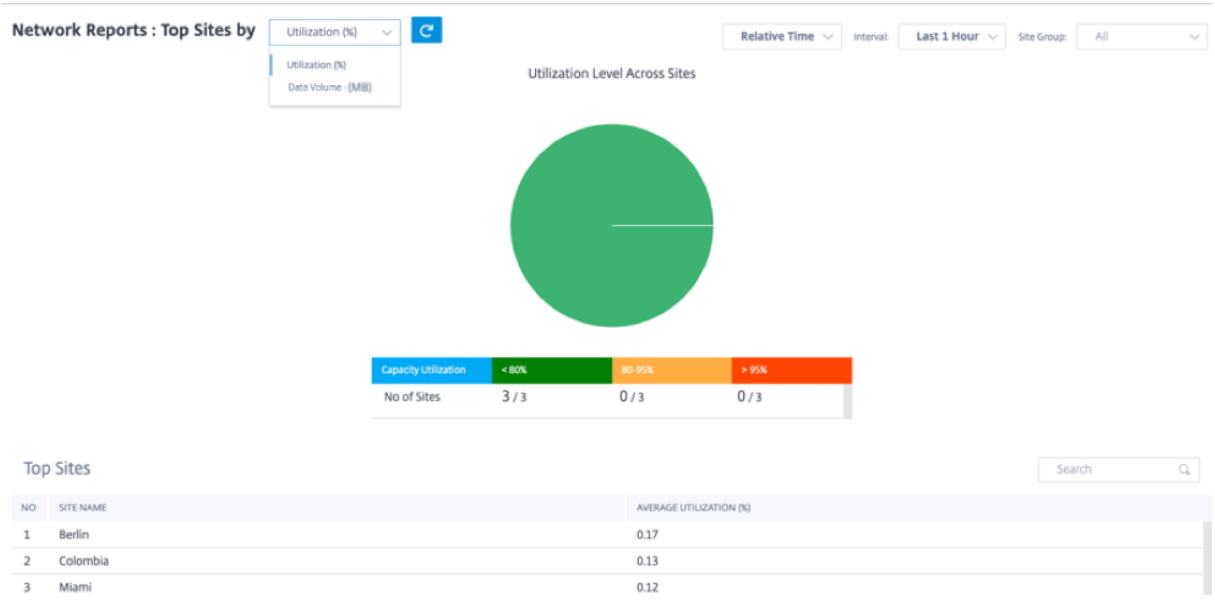



- **Tipo de informe: S**eleccione las **mejores aplicaciones o categorías** de aplicaciones de la lista.
- **Aplicaciones/categorías de aplicaciones: S**eleccione las aplicaciones o categorías principales (como el servicio de red) de la lista.
- **Métrica: S**eleccione la métrica de ancho de banda (como datos totales, datos entrantes, ancho de banda total) de la lista.

### Uso de la red

El gráfico de **sitios principales** muestra los sitios principales de la red de clientes que tienen el mayor uso de ancho de banda. Puede ver los sitios por utilización (%) o volumen de tráfico (MB).

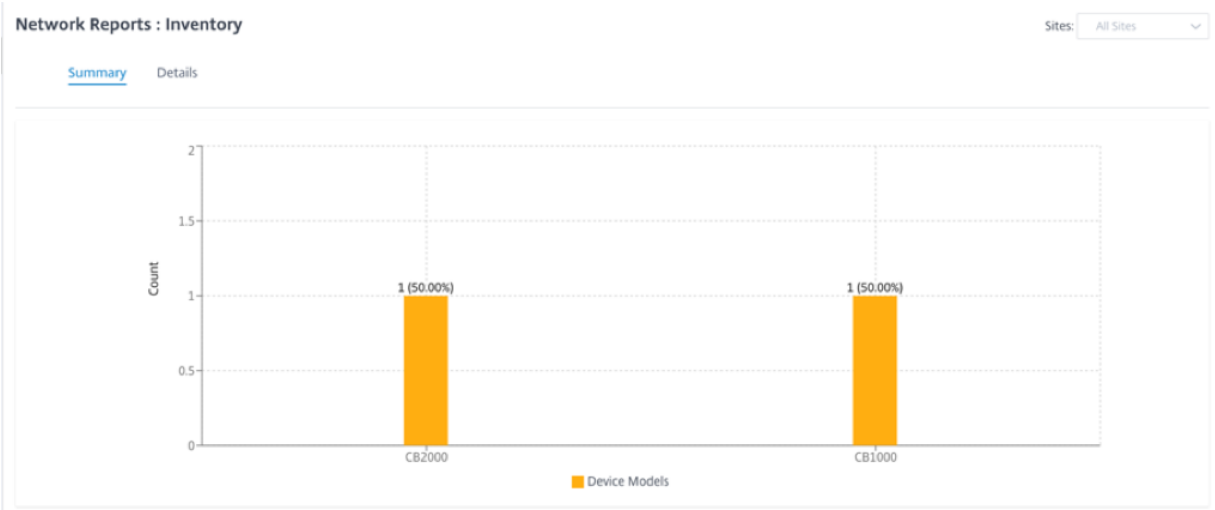
 




## Inventory

El cliente puede ver todo el inventario de dispositivos en todos los sitios de la red. Puede elegir ver un resumen del inventario o una vista detallada.

La vista de resumen de inventario proporciona un gráfico de la distribución del inventario, que muestra los diversos modelos de dispositivos y el número de cada tipo de dispositivos utilizados en todos los sitios de la red de clientes.

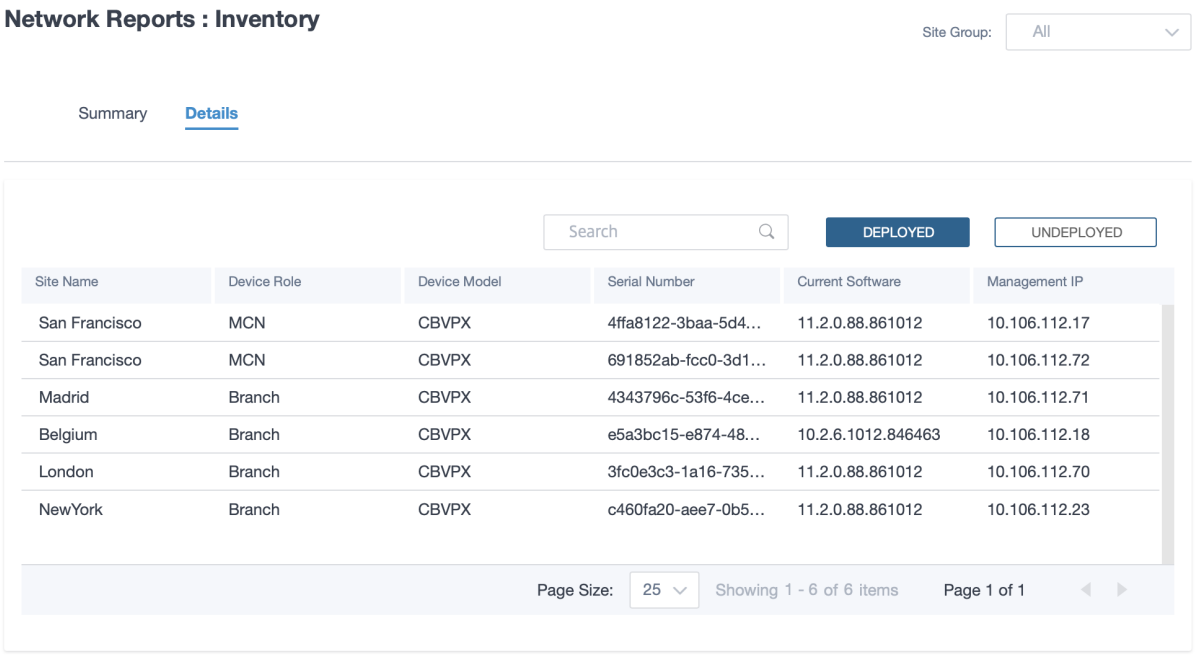



Se pueden utilizar las opciones de filtrado adecuadas según sea necesario, por ejemplo: busque todos los dispositivos que pertenezcan a un sitio específico o todos los dispositivos con un determinado modelo de dispositivo, etc.

La vista detallada del inventario proporciona una lista de todos los dispositivos que se implementan

y aquellos que están configurados pero aún no implementados. Junto con el cliente, el nombre del sitio, la función del dispositivo, el número de serie del dispositivo, el software actual y la dirección IP de administración de dispositivos.



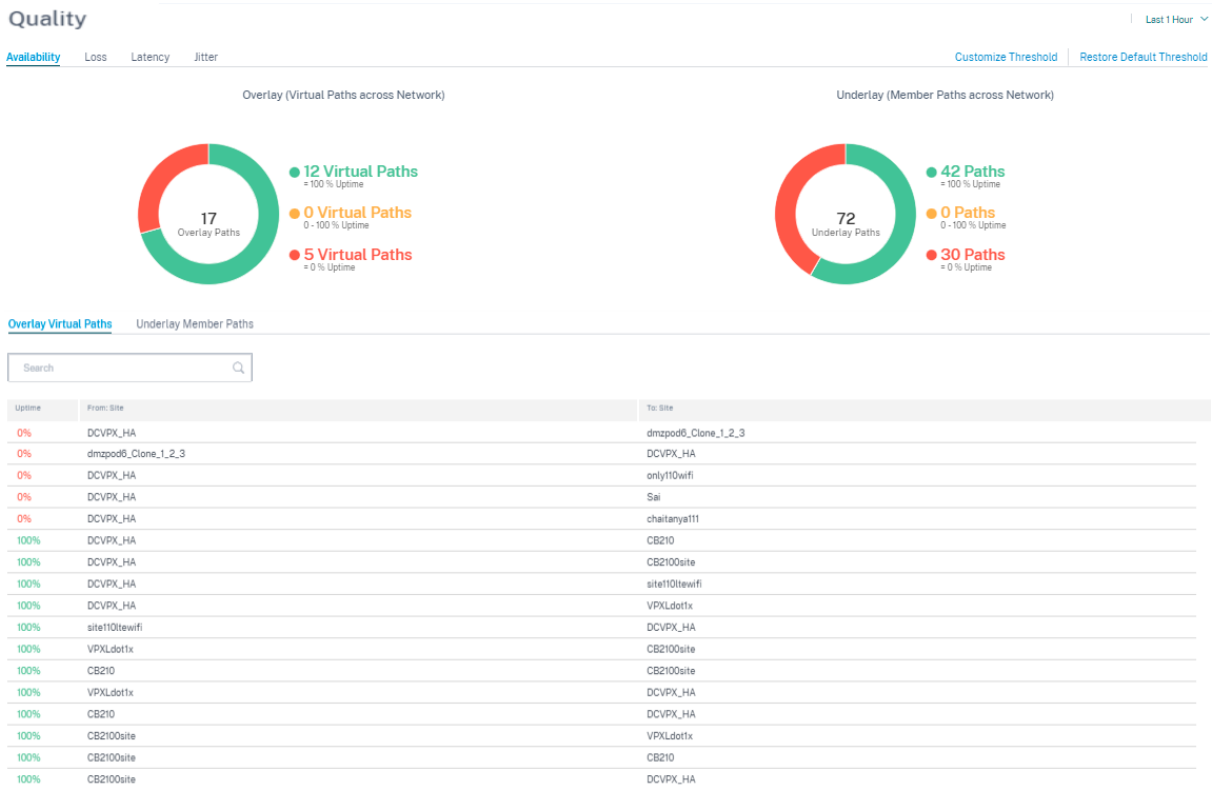

### Panel e informes HDX

Para obtener más información sobre el panel de control y los informes de HDX, consulte Panel e informesde HDX.

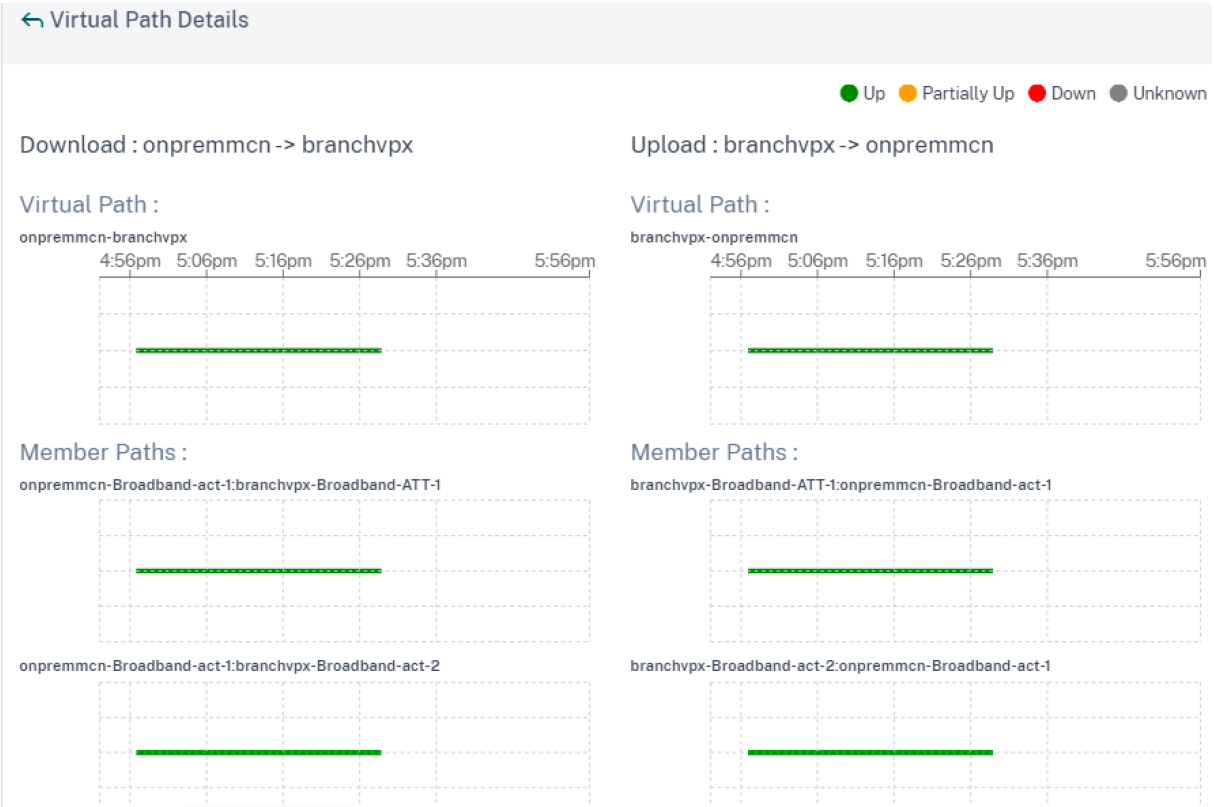
### Calidad

El informe de **calidad** de la red permite una comparación al nivel de red entre la superposición virtual y las rutas subyacentes físicas en términos de disponibilidad y pérdida, latencia y fluctuación. Esto ayuda a monitorear de manera efectiva el desempeño de la superposición en relación con la red subyacente y también ayuda a solucionar problemas. Para Latency and Jitter, solo se muestran los detalles de las rutas de los miembros subyacentes.

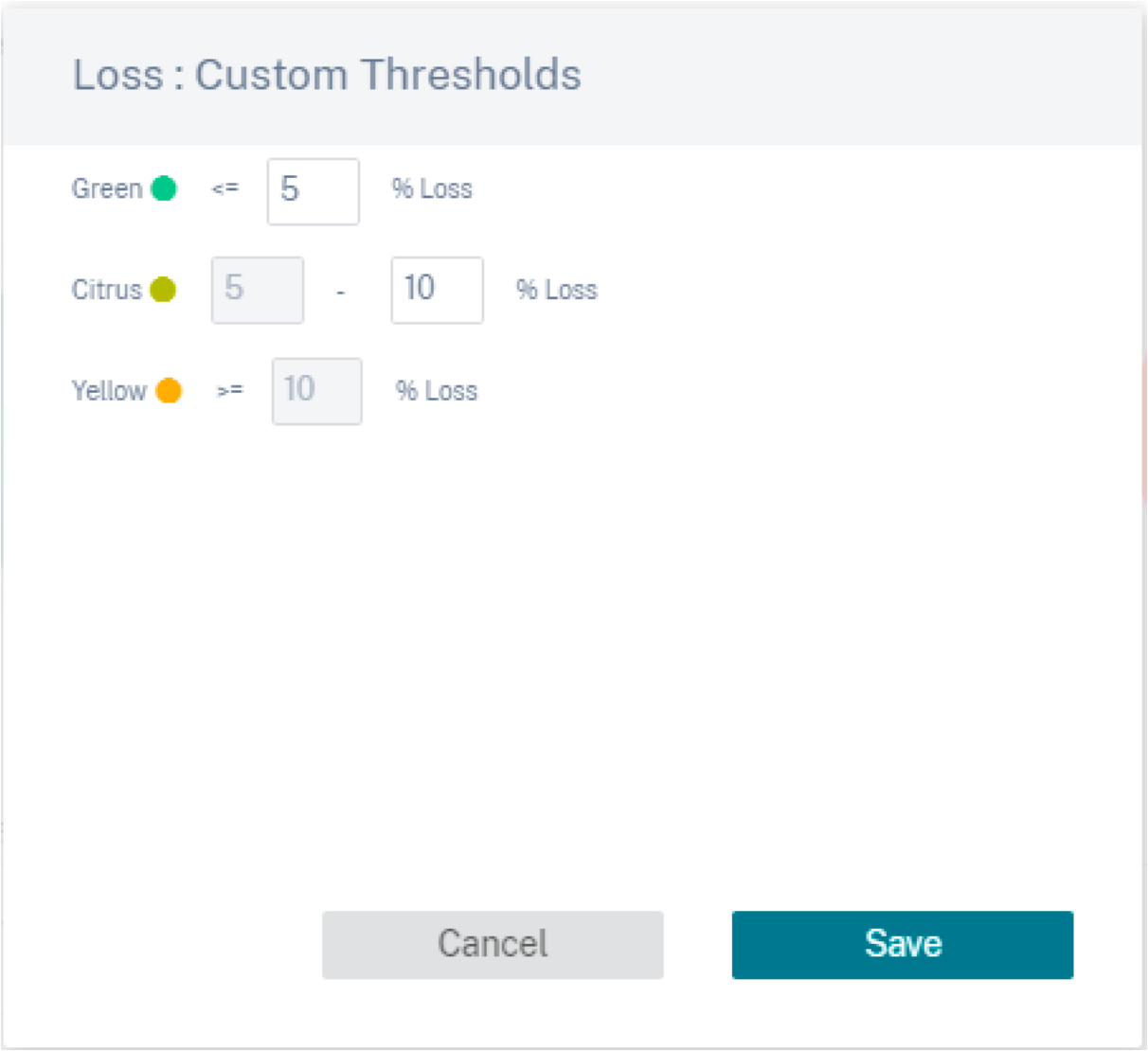



Haga clic en la entrada de la tabla para ver la vista detallada.



Puede personalizar el umbral de cada parámetro de calidad de la red.

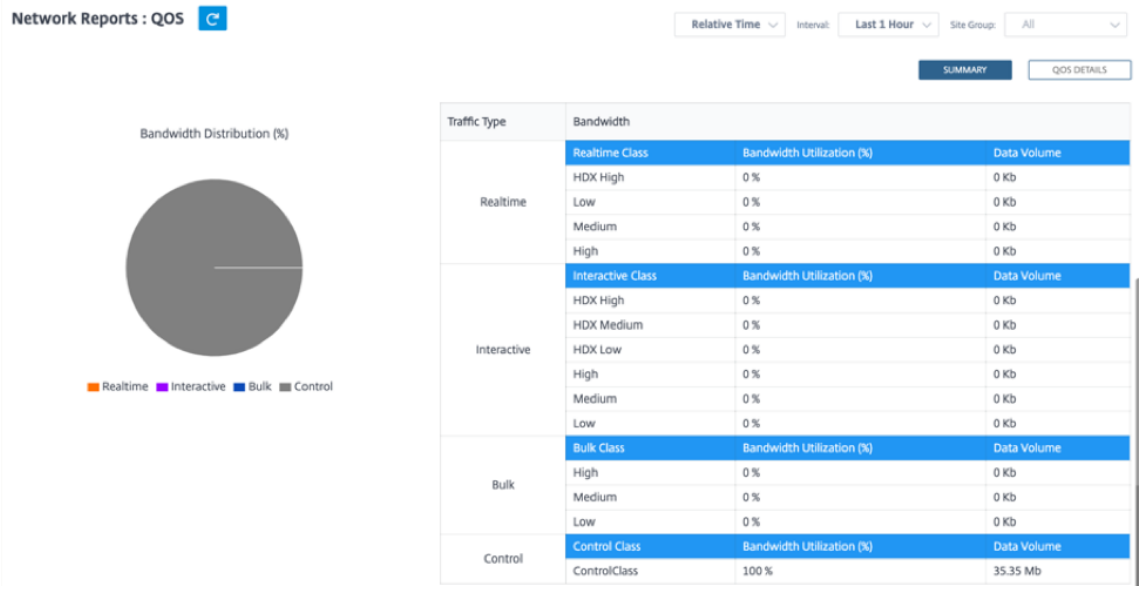



### Calidad del servicio

Quality of Service (QoS) administra el tráfico de datos para reducir la pérdida de paquetes, la latencia y la fluctuación en la red. Para obtener más información, consulte Calidad de servicio. Las siguientes son dos formas de ver el informe de calidad de servicio (QoS):

- **Vista de resumen: L**a vista de resumen proporciona una visión general del consumo de ancho de banda en todos los tipos de tráfico: En tiempo real, interactivo, masivo y de control en la red y por sitio.

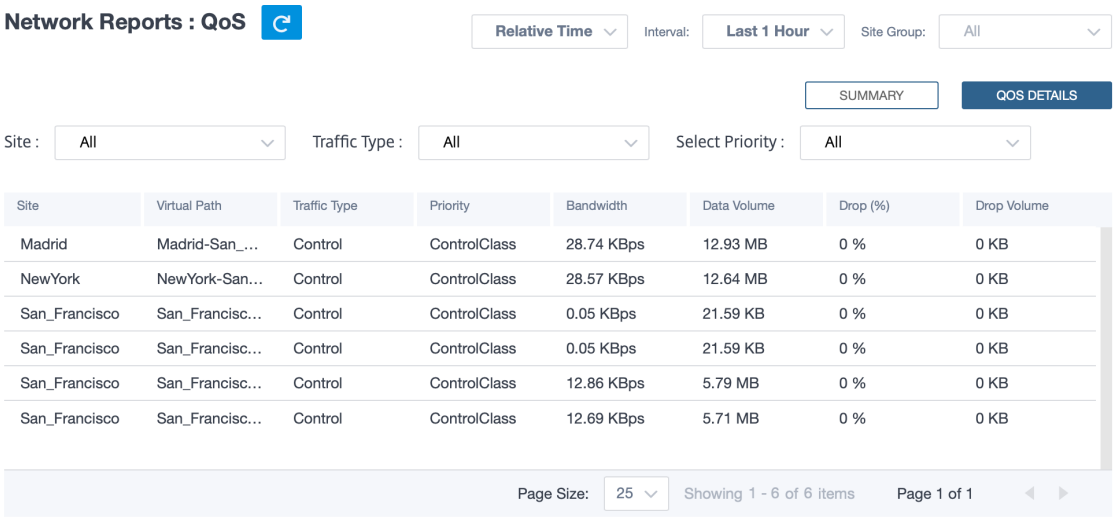
 




  - **Tiempo real: S**e usa para tráfico de baja latencia, bajo ancho de banda y urgente. Las aplicaciones en tiempo real son sensibles al tiempo, pero realmente no necesitan un ancho de banda alto (por ejemplo, voz sobre IP). Las aplicaciones en tiempo real son sensibles a la latencia y la fluctuación, pero pueden tolerar algunas pérdidas.
  - **Interactivo: S**e usa para tráfico interactivo con requisitos de latencia baja a media y requisitos de ancho de banda bajos a medios. Las aplicaciones interactivas implican la intervención humana en forma de clics del ratón o movimientos del cursor. La interacción suele ser entre un cliente y un servidor. Es posible que la comunicación no necesite un ancho de banda alto, pero es sensible a la pérdida y la latencia. Sin embargo, el servidor al cliente necesita un gran ancho de banda para transferir información gráfica, que puede no ser susceptible de pérdida.
  - **Masivo: S**e usa para tráfico de gran ancho de banda que puede tolerar una latencia Las aplicaciones que manejan la transferencia de archivos y necesitan un ancho de banda alto se clasifican como clase masiva. Estas aplicaciones implican poca interferencia humana y son manejadas principalmente por los propios sistemas.
  - **Control: S**e usa para transferir paquetes de control que contienen información de enrutamiento, programación y estadísticas de enlaces.

- **Vista detallada: La vista** detallada captura las tendencias en torno al consumo de ancho de banda, el volumen de tráfico, los paquetes descartados, etc., para cada clase de QoS asociada a una ruta virtual superpuesta.




Este informe está disponible en el nivel de sitio donde el usuario puede ver estadísticas de QoS basadas en la ruta virtual entre los dos sitios. Para obtener más información, consulte Informes del sitio.

## Estadísticas históricas

Para cada sitio, puede ver las estadísticas como gráficos para los siguientes parámetros de red:

- Sitios
- Rutas virtuales
- Rutas
- Enlaces WAN
- Interfaces
- Clases
- Túneles GRE
- Túneles IPsec

Las estadísticas se recogen como gráficos. Estos gráficos se trazan como línea temporal frente al uso, lo que le permite comprender las tendencias de uso de varias propiedades de objetos de red. Puede ver gráficos para estadísticas de aplicaciones de toda la red.

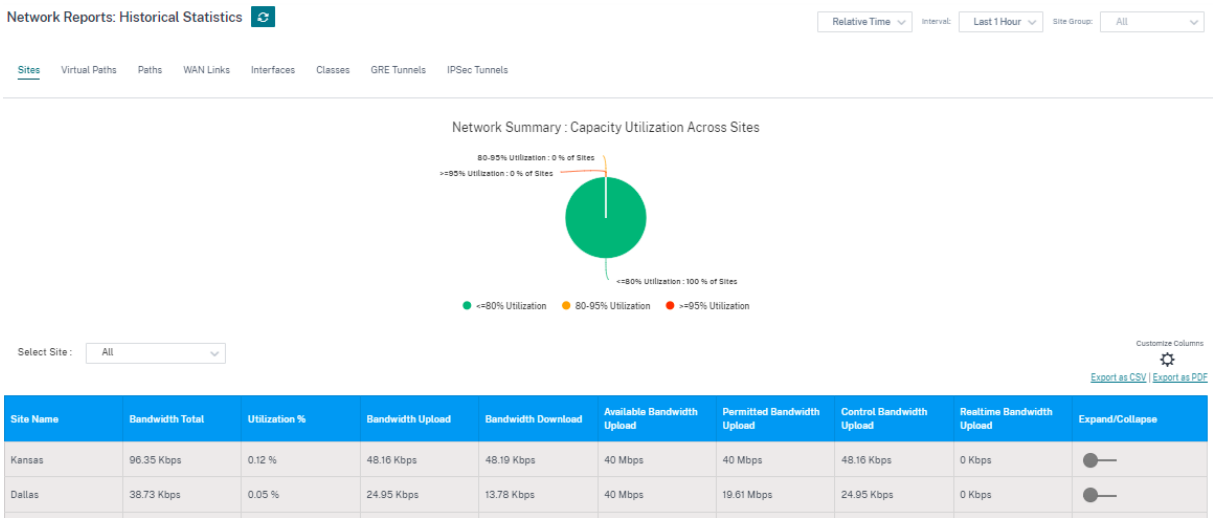
Puede ver u ocultar los gráficos y personalizar las columnas según sea necesario.

### Sitios

Para ver las estadísticas del sitio, vaya a **Informes > Estadísticas históricas > ficha Sitios**.

Seleccione el nombre del sitio en la lista.



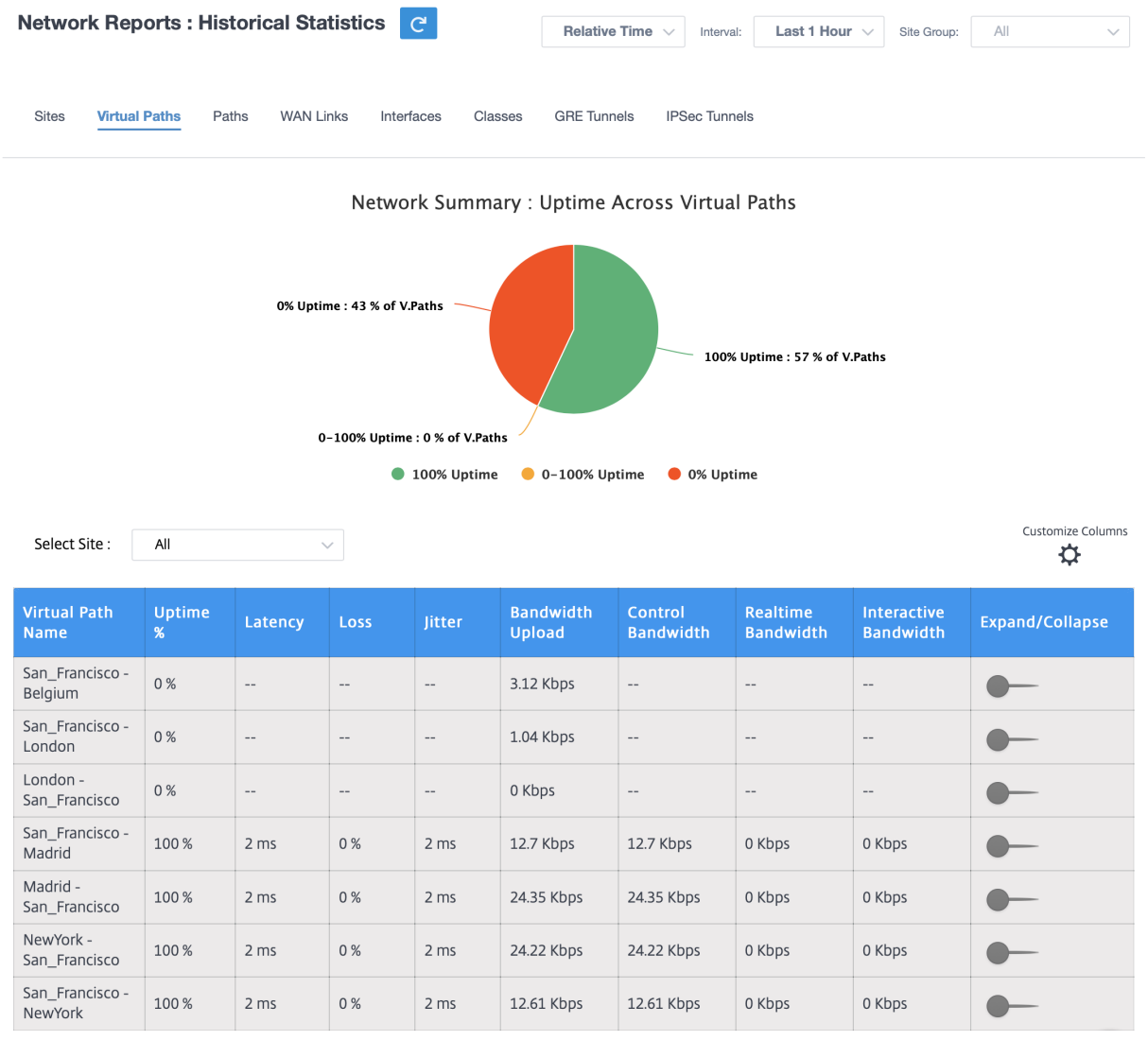

Puede ver las siguientes métricas:

- **Nombre del sitio**: El nombre del sitio.
- **Ancho de banda total**: Ancho de banda total que consumen todos los tipos de paquetes Ancho de banda = Control de ancho de banda + ancho de banda en tiempo real + ancho de banda interactiva + ancho de banda
- **Utilización**: Puede ver las estadísticas del sitio por utilización (%).
- **Entrada de ancho de**banda: La velocidad máxima y mínima de descarga a través del puerto WAN.
- **Salida de ancho de**banda: La velocidad máxima y mínima de carga a través del puerto WAN.
- **Entrada de ancho de banda disponible**: Ancho de banda total asignado a todos los enlaces WAN de un sitio.
- **Entrada de ancho de banda permitida**: Ancho de banda disponible para transmitir información.
- **Control del ingreso de ancho**de banda: Ancho de banda utilizado para transferir paquetes de control que contienen información de enrutamiento, programación y estadísticas de enlaces.
- Entrada de**ancho de banda en tiempo real**: Ancho de banda que consumen las aplicaciones que pertenecen al tipo de clase en tiempo real en la configuración SD-WAN de NetScaler. El rendimiento de tales aplicaciones depende en gran medida de la latencia de la red. Un paquete retrasado es peor que un paquete perdido (por ejemplo, VoIP, Skype for Business).
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

### Rutas virtuales

Para ver las estadísticas de **rutas virtuales**, vaya a **Informes > Estadísticas > Rutas virtuales**.




| Virtual Path Name | Uptime % | Latency | Loss | Jitter | Bandwidth Upload | Control Bandwidth | Realtime Bandwidth | Interactive Bandwidth | Expand/Collapse |
|---|---|---|---|---|---|---|---|---|---|
| San_Francisco - Belgium | 0 % | -- | -- | -- | 3.12 Kbps | -- | -- | -- | |
| San_Francisco - London | 0 % | -- | -- | -- | 1.04 Kbps | -- | -- | -- | |
| London - San_Francisco | 0 % | -- | -- | -- | 0 Kbps | -- | -- | -- | |
| San_Francisco - Madrid | 100 % | 2 ms | 0 % | 2 ms | 12.7 Kbps | 12.7 Kbps | 0 Kbps | 0 Kbps | |
| Madrid - San_Francisco | 100 % | 2 ms | 0 % | 2 ms | 24.35 Kbps | 24.35 Kbps | 0 Kbps | 0 Kbps | |
| NewYork - San_Francisco | 100 % | 2 ms | 0 % | 2 ms | 24.22 Kbps | 24.22 Kbps | 0 Kbps | 0 Kbps | |
| San_Francisco - NewYork | 100 % | 2 ms | 0 % | 2 ms | 12.61 Kbps | 12.61 Kbps | 0 Kbps | 0 Kbps | |

Puede ver las siguientes métricas:

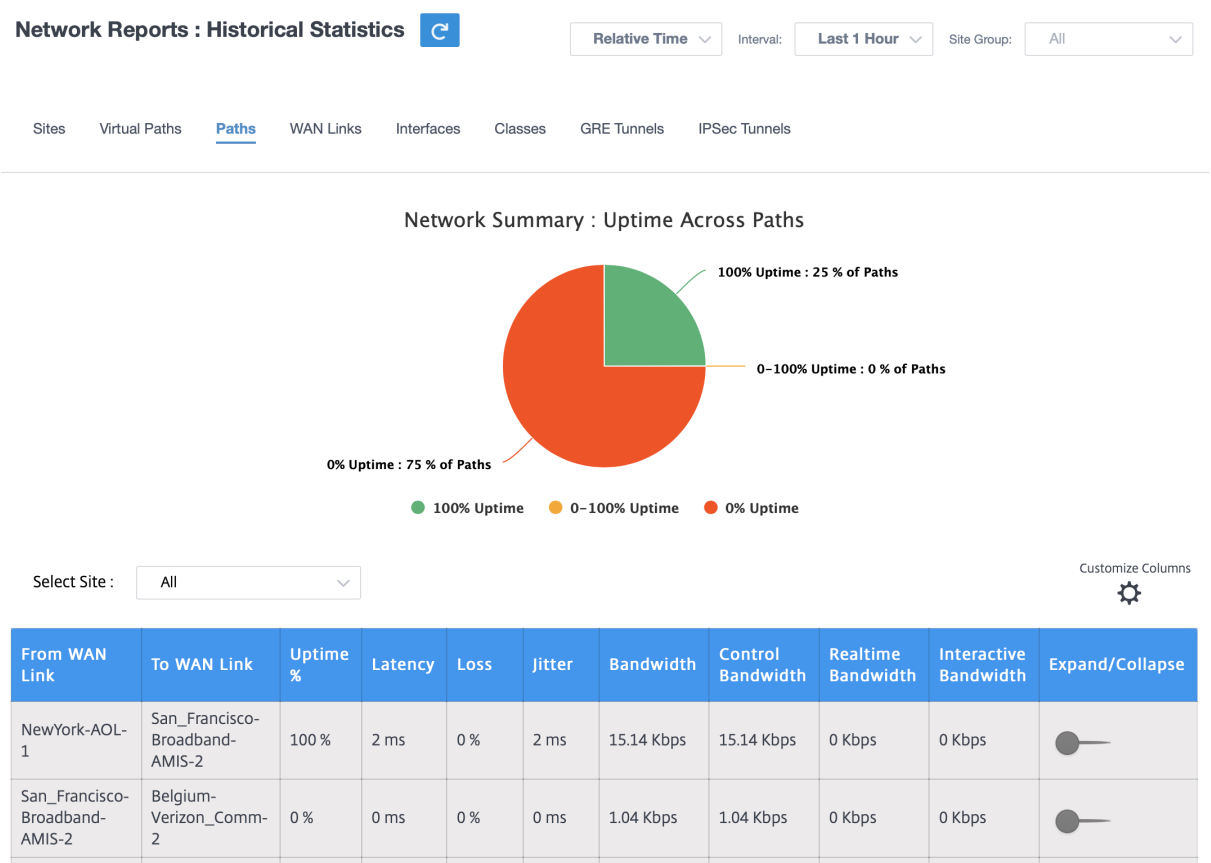
- **Nombre de la ruta virtual**: El nombre de la ruta virtual.
- **Latencia**: L a latencia en milisegundos del tráfico en tiempo real.
- **Pérdida**: Porcentaje de paquetes perdidos.
- **Fluctuación**: variación en el retraso de los paquetes recibidos, en milisegundos.
- **Entrada de ancho**de banda: Uso de ancho de banda de ingreso (LAN a WAN) durante el período de tiempo seleccionado.
- **Ancho de banda de control**: Ancho de banda utilizado para transferir paquetes de control que contienen información de enrutamiento, programación y estadísticas de enlaces.
- Ancho de**banda en tiempo real**: Ancho de banda que consumen las aplicaciones que pertenecen al tipo de clase en tiempo real en la configuración de SD-WAN. El rendimiento de tales aplicaciones depende en gran medida de la latencia de la red. Un paquete retrasado es peor que un paquete perdido (por ejemplo, VoIP, Skype for Business).

- Ancho de**banda interactivo**: Ancho de banda que consumen las aplicaciones que pertenecen al tipo de clase interactiva en la configuración de SD-WAN. El rendimiento de estas aplicaciones depende en gran medida de la latencia de la red y de la pérdida de paquetes (por ejemplo, XenDesktop, XenApp).
- Ancho de**banda masivo**: Ancho de banda que consumen las aplicaciones que pertenecen al tipo de clase masiva en la configuración de SD-WAN. Estas aplicaciones implican poca intervención humana y son manejadas por los propios sistemas (por ejemplo, FTP, operaciones de copia de seguridad).
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

### Rutas

Para ver las estadísticas de **rutas**, vaya a la ficha **Informes > Estadísticas > Rutas**.




Puede ver las siguientes métricas:

- **Desde el enlace WAN**: El enlace WAN de origen.
- **Al enlace WAN**: El enlace WAN de destino.
- **Latencia**: La latencia en milisegundos del tráfico en tiempo real.
- **Pérdida**: Porcentaje de paquetes perdidos.

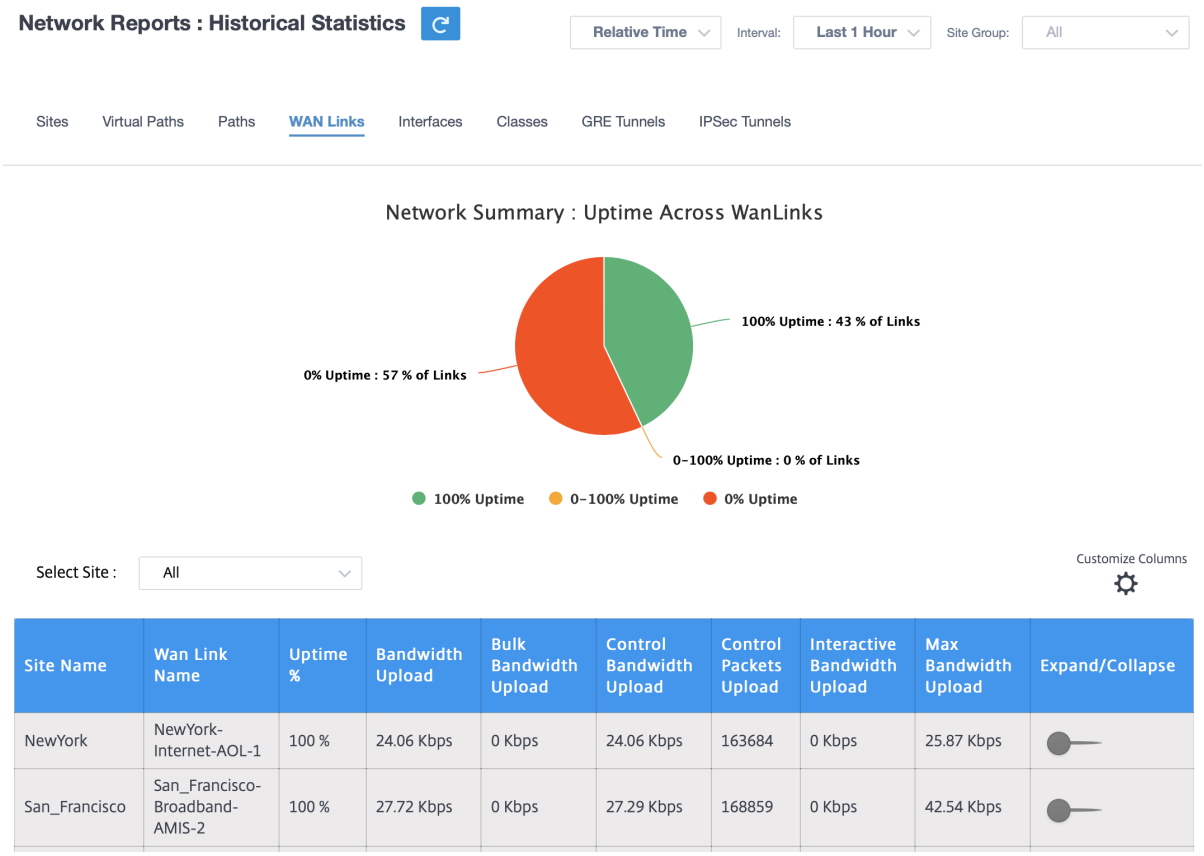
 

- **Fluctuación**: variación en el retraso de los paquetes recibidos, en milisegundos.
- **Ancho de banda**: Ancho de banda total que consumen todos los tipos de paquetes Ancho de banda = Control de ancho de banda + ancho de banda en tiempo real + ancho de banda interactiva + ancho de banda
- **Ancho de banda de control**: Ancho de banda utilizado para transferir paquetes de control que contienen información de enrutamiento, programación y estadísticas de enlaces.
- Ancho de**banda en tiempo real**: Ancho de banda que consumen las aplicaciones que pertenecen al tipo de clase en tiempo real en la configuración de SD-WAN. El rendimiento de tales aplicaciones depende en gran medida de la latencia de la red. Un paquete retrasado es peor que un paquete perdido (por ejemplo, VoIP, Skype for Business).
- Ancho de**banda interactivo**: Ancho de banda que consumen las aplicaciones que pertenecen al tipo de clase interactiva en la configuración de SD-WAN. El rendimiento de estas aplicaciones depende en gran medida de la latencia de la red y de la pérdida de paquetes (por ejemplo, XenDesktop, XenApp).
- Ancho de**banda masivo**: Ancho de banda que consumen las aplicaciones que pertenecen al tipo de clase masiva en la configuración de SD-WAN. Estas aplicaciones implican poca intervención humana y son manejadas por los propios sistemas (por ejemplo, FTP, operaciones de copia de seguridad).
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

**Enlaces WAN**

Para ver las estadísticas al nivel de **enlace WAN**, vaya a **Informes > Estadísticas > ficha Vínculos WAN**.




Puede ver las siguientes métricas:

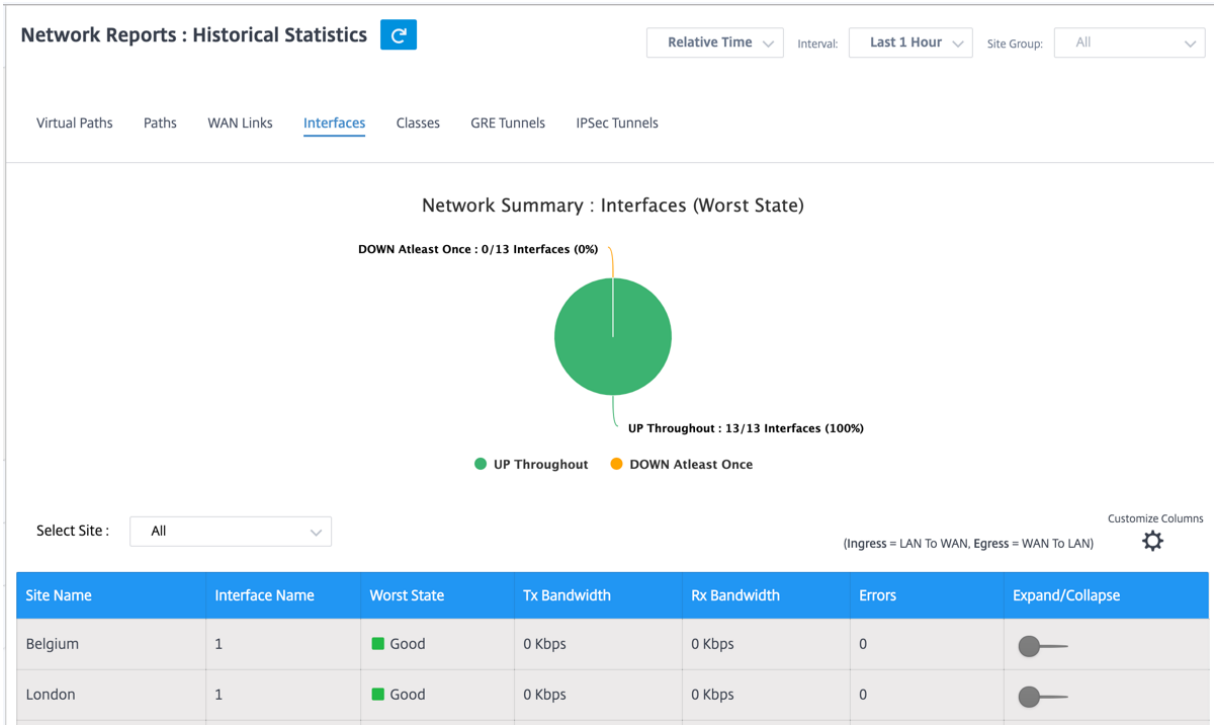
- **Nombre del enlace WAN**: El nombre de la ruta.
- **Entrada de ancho**de banda: Uso de ancho de banda de ingreso (LAN a WAN) durante el período de tiempo seleccionado.
- **Entrada masiva de ancho**de banda: Ancho de banda de entrada (LAN a WAN) de ruta virtual utilizado por el tráfico masivo durante el período de tiempo seleccionado.
- **Entrada de ancho de banda de control**: Ancho de banda de acceso (LAN a WAN) de ruta virtual utilizado por Control Traffic durante el período de tiempo seleccionado.
- **Entrada de paquetes de control**: Paquetes de control de ruta virtual de ingreso (LAN a WAN) para el período de tiempo seleccionado.
- Entrada de**ancho de banda interactiva**: Ancho de banda de entrada (LAN a WAN) de ruta virtual utilizado por el tráfico interactivo durante el período de tiempo seleccionado.
- **Entrada de ancho**de banda máxima: Ancho de banda máximo de entrada (LAN a WAN) utilizado en un minuto durante el período de tiempo seleccionado.
- **Entrada de ancho**de banda mínima: Ancho de banda de entrada mínimo (LAN a WAN) utilizado en un minuto durante el período de tiempo seleccionado.
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

### Interfaces

El informe estadístico de Interfaces le ayuda durante la resolución de problemas para ver rápidamente si alguno de los puertos está inactivos. También puede ver el ancho de banda transmitido y recibido o los detalles del paquete en cada puerto. También puede ver el número de errores que se produjeron en estas interfaces durante un período de tiempo determinado.

Para ver las estadísticas de la **interfaz**, vaya a la ficha **Informes > Estadísticas > Interfaces**.




Puede ver las siguientes métricas:

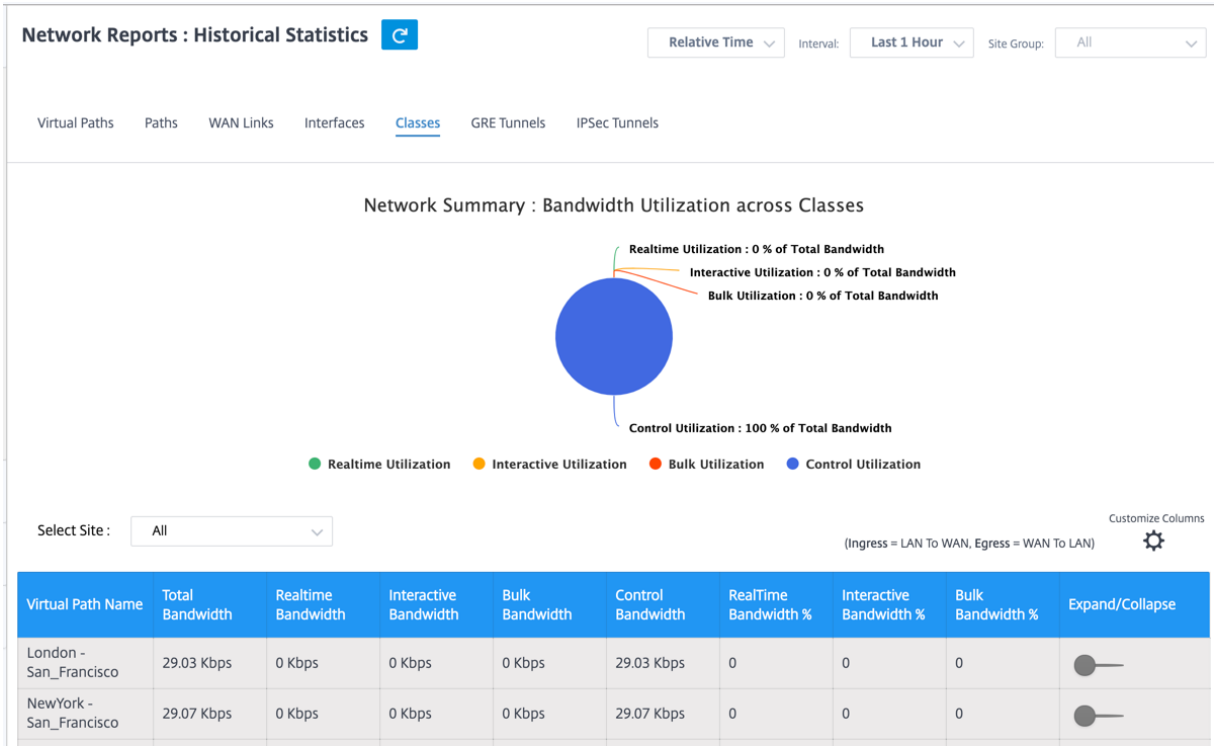
- **Nombre de la interfaz**: El nombre de la interfaz Ethernet.
- **Ancho de banda Tx**: Ancho de banda transmitido.
- **Ancho de banda Rx**: Ancho de banda recibido.
- **Errores**: Número de errores observados durante el período de tiempo seleccionado.
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

### Clases

Los servicios virtuales se pueden asignar a clases de QoS particulares, y se pueden aplicar restricciones de ancho de banda diferentes a diferentes clases.

Para ver las estadísticas de las **clases**, vaya a la ficha **Informes > Estadísticas > Clases**.




Puede ver las siguientes métricas:

- **Clase de QoS**: El nombre de la clase.
- **Ancho de banda**: Ancho de banda transmitido
- **Volumen**de datos: Datos enviados, en Kbps.
- **Volumen de caída**: Porcentaje de datos descartados.
- **Porcentaje de caída**: Porcentaje de datos descartados.
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

### Túneles GRE

Puede utilizar un mecanismo de túnel para transportar paquetes de un protocolo dentro de otro protocolo. El protocolo que lleva el otro protocolo se denomina protocolo de transporte, y el protocolo transportado se denomina protocolo de pasajeros. Generic Routing Encapsulation (GRE) es un mecanismo de tunelización que utiliza IP como protocolo de transporte y puede llevar muchos protocolos de pasajeros diferentes.

La dirección de origen del túnel y la dirección de destino se utilizan para identificar los dos extremos de los vínculos virtuales punto a punto del túnel. Para obtener más información sobre la configuración de túneles GRE en dispositivos Citrix SD-WAN, consulte Túnel GRE.

Para ver las estadísticas **del túnel GRE**, vaya a **Informes > Estadísticas > ficha Túneles GRE**.

Puede ver las siguientes métricas:

- **Nombre del sitio**: El nombre del sitio.
- **Ancho de banda Tx**: Ancho de banda transmitido.
- **Ancho de banda Rx**: Ancho de banda recibido.
- **Paquete eliminado**: Número de paquetes descartados debido a la congestión de la red.
- **Paquetes Fragmentados**: Número de paquetes fragmentados. Los paquetes se fragmentan para crear paquetes más pequeños que pueden pasar a través de un enlace con una MTU más pequeña que el datagrama original. El host receptor vuelve a ensamblar los fragmentos.
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

#### Túneles IPsec

Los protocolos de seguridad IP (IPsec) proporcionan servicios de seguridad como el cifrado de datos confidenciales, la autenticación, la protección contra la reproducción y la confidencialidad de los datos para los paquetes IP. Carga útil de seguridad encapsulada (ESP) y Encabezado de autenticación (AH) son los dos protocolos de seguridad IPsec utilizados para proporcionar estos servicios de seguridad.

En el modo de túnel IPsec, todo el paquete IP original está protegido por IPsec. El paquete IP original está envuelto y cifrado, y se agrega un nuevo encabezado IP antes de transmitir el paquete a través del túnel VPN.
Para obtener más información sobre la configuración de túneles IPSec en dispositivos Citrix SD-WAN, consulte Terminación de túneles IPSec.

Para ver las estadísticas **del túnel IPSec**, vaya a **Informes > estadísticas > ficha Túneles IPSec**.

Puede ver las siguientes métricas:

- **Nombre del túnel**: Nombre del túnel.
- **Estado del túnel: Estado**del túnel IPsec.
- **MTU**: Unidad de transmisión máxima: Tamaño del datagrama IP más grande que se puede transferir a través de un enlace específico.
- **Paquetes recibidos**: Número de paquetes recibidos.
- **Paquetes enviados**: Número de paquetes enviados.
- **Paquete eliminado**: Número de paquetes descartados debido a la congestión de la red.
- **Bytes eliminados**: Número de bytes eliminados.
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

### Estadísticas en tiempo real

La página de estadísticas en tiempo real muestra la siguiente información estadística al nivel de cliente:

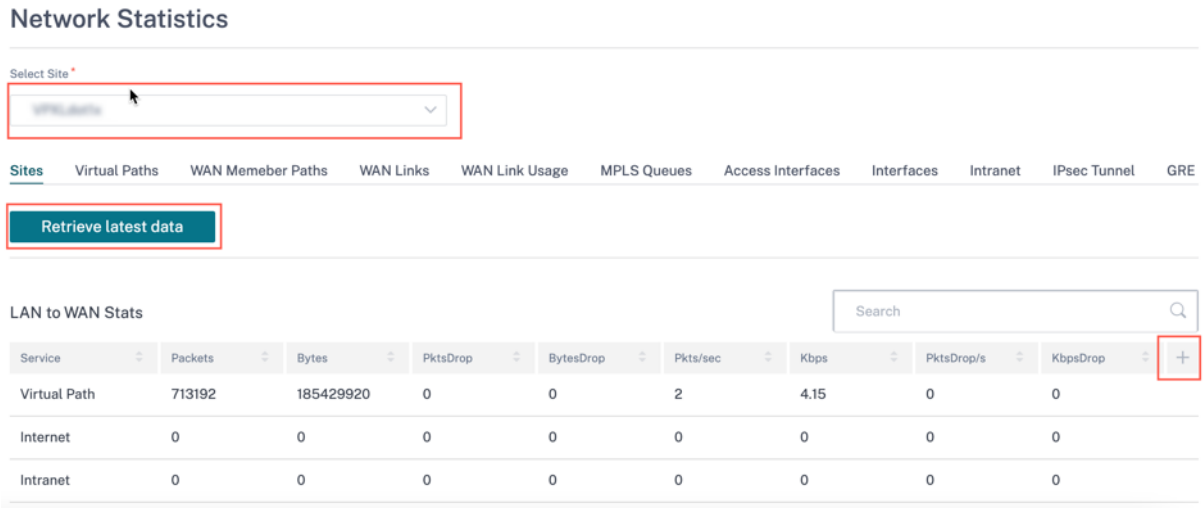
 

### Estadísticas de red

La página **Estadísticas de red** proporciona la siguiente información estadística en tiempo real en **Informes** > **Tiempo real** > **Estadísticas de red**:

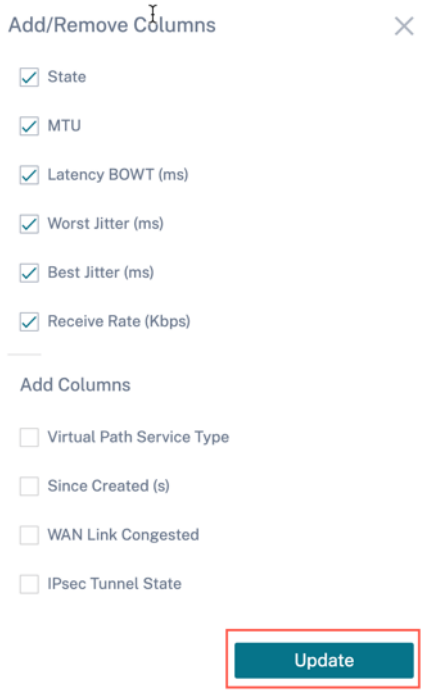
- Sitios
- Rutas virtuales
- Rutas de miembros de WAN
- Enlaces WAN
- Uso de vínculos WAN
- Colas MPLS
- Interfaces de acceso
- Interfaces
- Intranet
- Túnel IPsec
- GRE

Para obtener un informe estadístico en tiempo real, vaya a la ficha correspondiente (como sitios, rutas virtuales, enlaces WAN), seleccione el sitio en la lista desplegable y haga clic en **Recuperar los datos más recientes**.




Haga clic en el símbolo más (+) para agregar o eliminar cualquier columna de la tabla de estadísticas y haga clic en **Actualizar**.



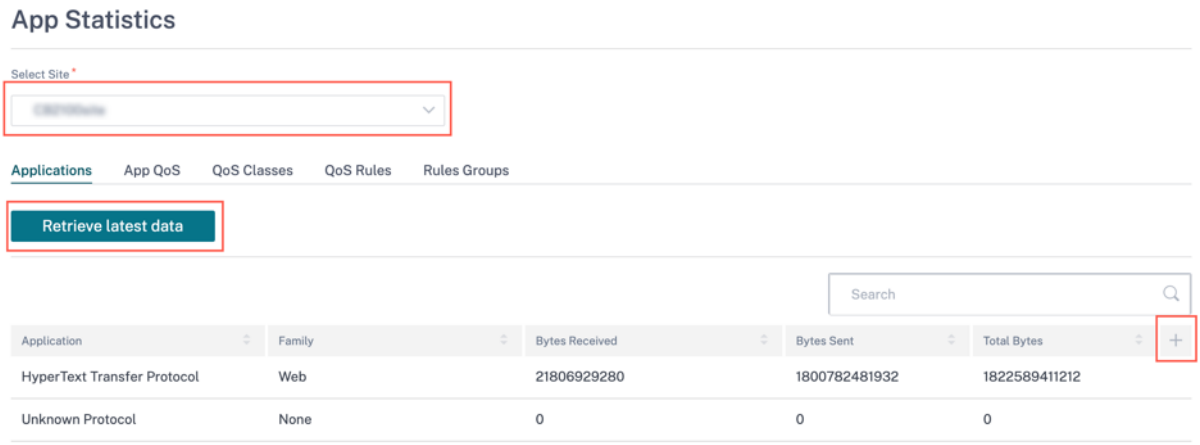

### Estadísticas de la aplicación

La página **Estadísticas de la aplicación** proporciona la siguiente información estadística en tiempo real en **Informes > Tiempo real > Estadísticas de la aplicación**:

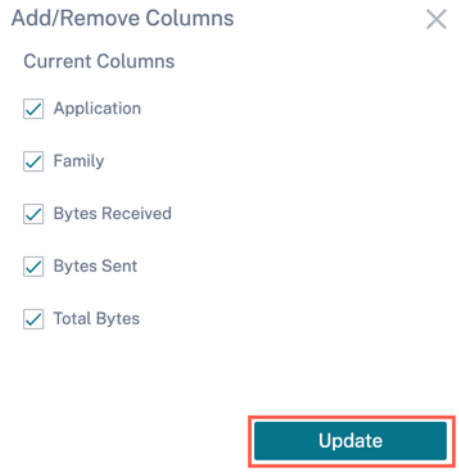
- Aplicaciones
- QoS de aplicaciones
- Clases de QoS
- Reglas de QoS
- Grupos de reglas

Para obtener un informe estadístico en tiempo real, vaya a la ficha requerida (como aplicaciones, reglas de QoS, clases de QoS), seleccione el sitio en la lista desplegable y haga clic en **Recuperar los datos más recientes**.




Haga clic en el símbolo más (+) si quiere agregar o eliminar cualquier columna de la tabla de estadísticas y, a continuación, haga clic en **Actualizar**.



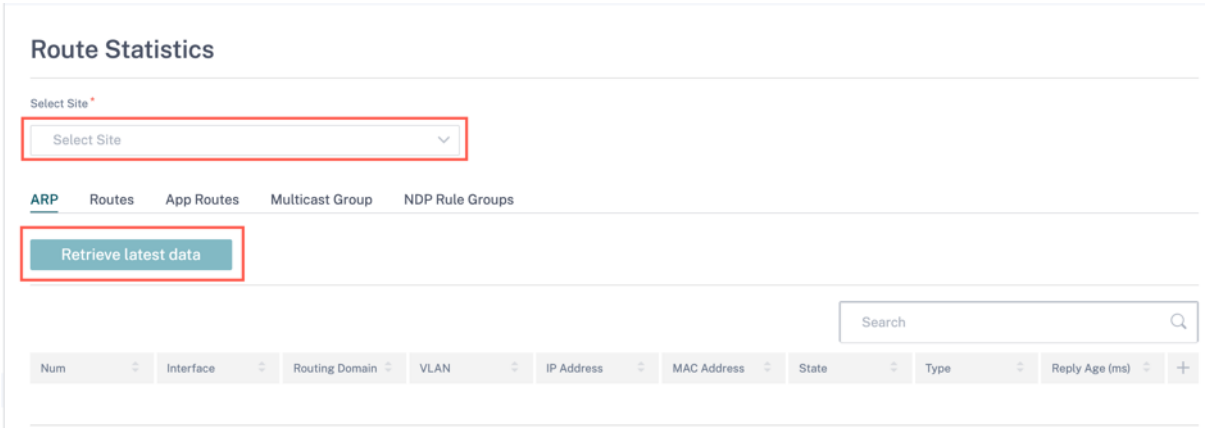

### Estadísticas de rutas

La página **Estadísticas de rutas** proporciona la siguiente información estadística en tiempo real en **Informes > Tiempo real > Estadísticas de rutas**:

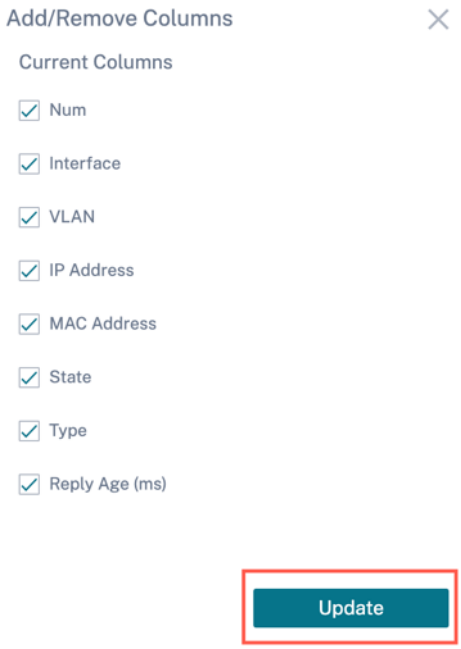
- ARP
- Rutas
- Rutas de aplicación
- Protocolos observados
- Grupo de multidifusión
- Grupos de reglas de NDP

Para obtener un informe estadístico en tiempo real, vaya a la ficha requerida (como ARP, Rutas, Rutas de aplicaciones), seleccione el sitio en la lista desplegable y haga clic en **Recuperar los datos más recientes**.



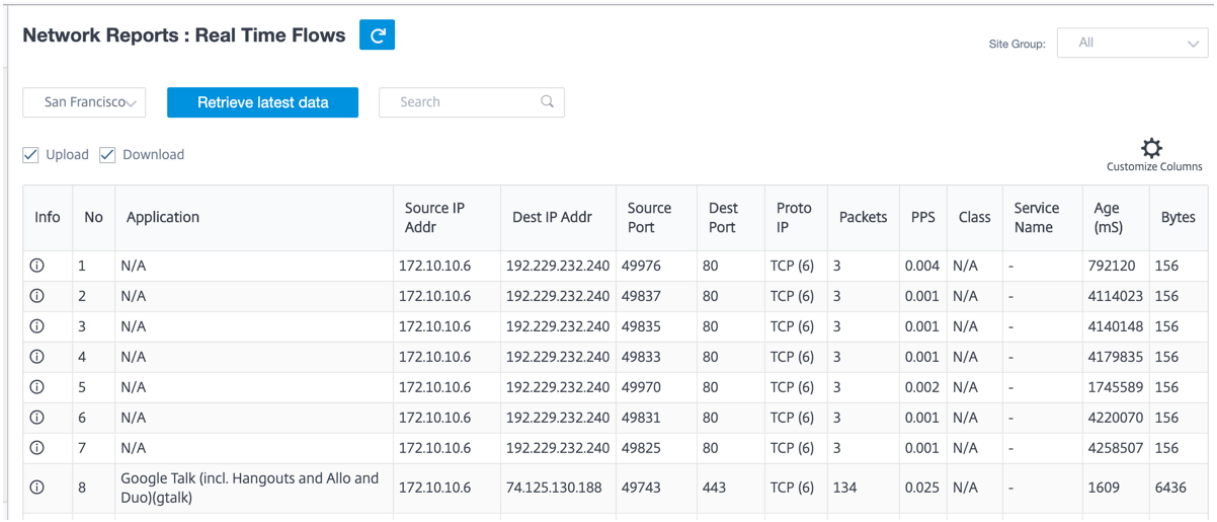

Haga clic en el símbolo más (+) si quiere agregar o eliminar cualquier columna de la tabla de estadísticas y, a continuación, haga clic en **Actualizar**.




### Flujos

En el nivel de red, seleccione el sitio en la lista desplegable antes de obtener las estadísticas. La función **Flujos** proporciona información de flujo unidireccional relacionada con una sesión en particular que pasa por el dispositivo. Esto proporciona información sobre el tipo de servicio de destino en el que cae el flujo y también la información relacionada con la regla y el tipo de clase, así como el modo de transmisión.

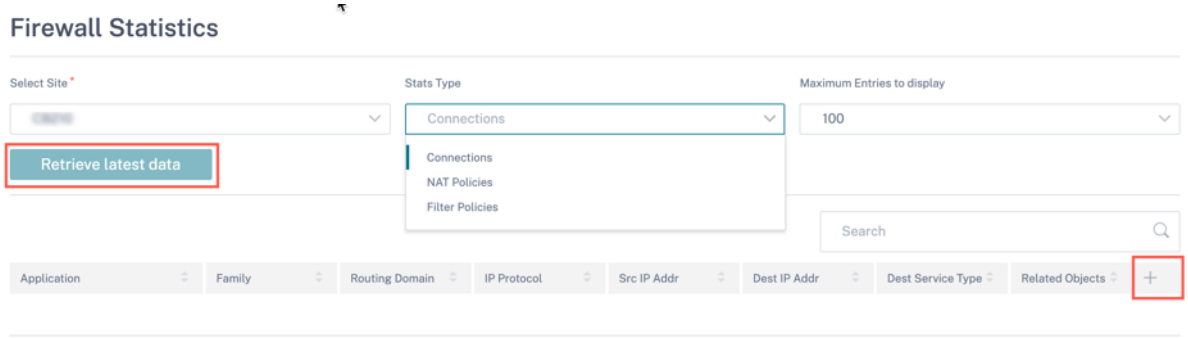
 




| Info | No | Application | Source IP Addr | Dest IP Addr | Source Port | Dest Port | Proto IP | Packets | PPS | Class | Service Name | Age (mS) | Bytes |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ⓘ | 1 | N/A | 172.10.10.6 | 192.229.232.240 | 49976 | 80 | TCP (6) | 3 | 0.004 | N/A | - | 792120 | 156 |
| ⓘ | 2 | N/A | 172.10.10.6 | 192.229.232.240 | 49837 | 80 | TCP (6) | 3 | 0.001 | N/A | - | 4114023 | 156 |
| ⓘ | 3 | N/A | 172.10.10.6 | 192.229.232.240 | 49835 | 80 | TCP (6) | 3 | 0.001 | N/A | - | 4140148 | 156 |
| ⓘ | 4 | N/A | 172.10.10.6 | 192.229.232.240 | 49833 | 80 | TCP (6) | 3 | 0.001 | N/A | - | 4179835 | 156 |
| ⓘ | 5 | N/A | 172.10.10.6 | 192.229.232.240 | 49970 | 80 | TCP (6) | 3 | 0.002 | N/A | - | 1745589 | 156 |
| ⓘ | 6 | N/A | 172.10.10.6 | 192.229.232.240 | 49831 | 80 | TCP (6) | 3 | 0.001 | N/A | - | 4220070 | 156 |
| ⓘ | 7 | N/A | 172.10.10.6 | 192.229.232.240 | 49825 | 80 | TCP (6) | 3 | 0.001 | N/A | - | 4258507 | 156 |
| ⓘ | 8 | Google Talk (incl. Hangouts and Allo and Duo)(gtalk) | 172.10.10.6 | 74.125.130.188 | 49743 | 443 | TCP (6) | 134 | 0.025 | N/A | - | 1609 | 6436 |

### Estadísticas de firewall

En el nivel de red, seleccione el sitio en la lista desplegable antes de obtener las estadísticas. Las **estadísticas del firewall** proporcionan el estado de la conexión relacionada con una sesión en particular en función de la acción de firewall configurada. Las conexiones de firewall también proporcionan detalles completos sobre el origen y el destino de la conexión.

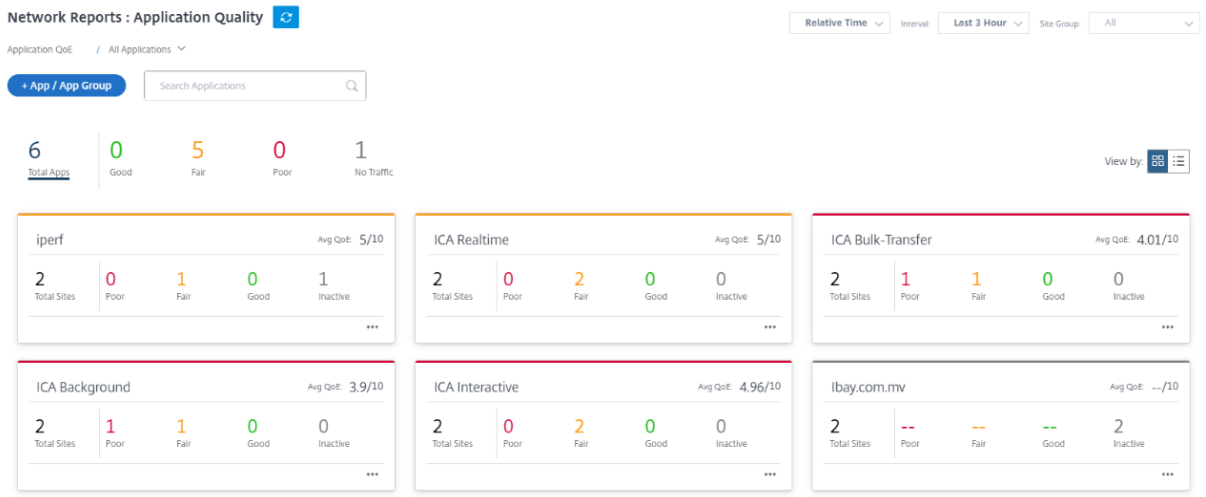



### Calidad de la aplicación

LaQoE de la aplicación es una medida de calidad de experiencia de aplicaciones en la red SD-WAN. Mide la calidad de las aplicaciones que fluyen por las rutas virtuales entre dos dispositivos SD-WAN. La puntuación QoE de la aplicación es un valor entre 0 y 10. El rango de puntuación en el que cae determina la calidad de una aplicación. La QoE de la aplicación permite a los administradores de red revisar la calidad de la experiencia de las aplicaciones y tomar medidas proactivas cuando la calidad está por debajo del umbral aceptable.

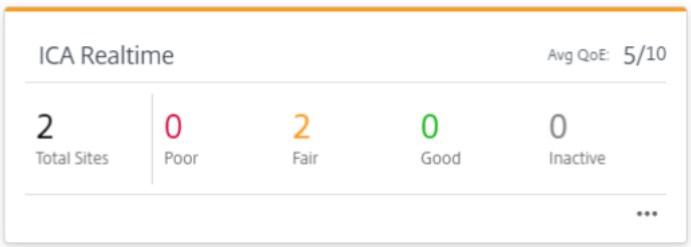
 

| Calidad | Rango | Codificación de colores |
|---|---|---|
| Bueno | 8–10 | Verde |
| Normal | 4–8 | Naranja |
| Mala | 0–4 | Rojo |




La parte superior del panel muestra el número total de aplicaciones y el número de aplicaciones que tienen QoE de aplicaciones buena, justa o deficiente en la red. También muestra el número de aplicaciones que no tienen tráfico.

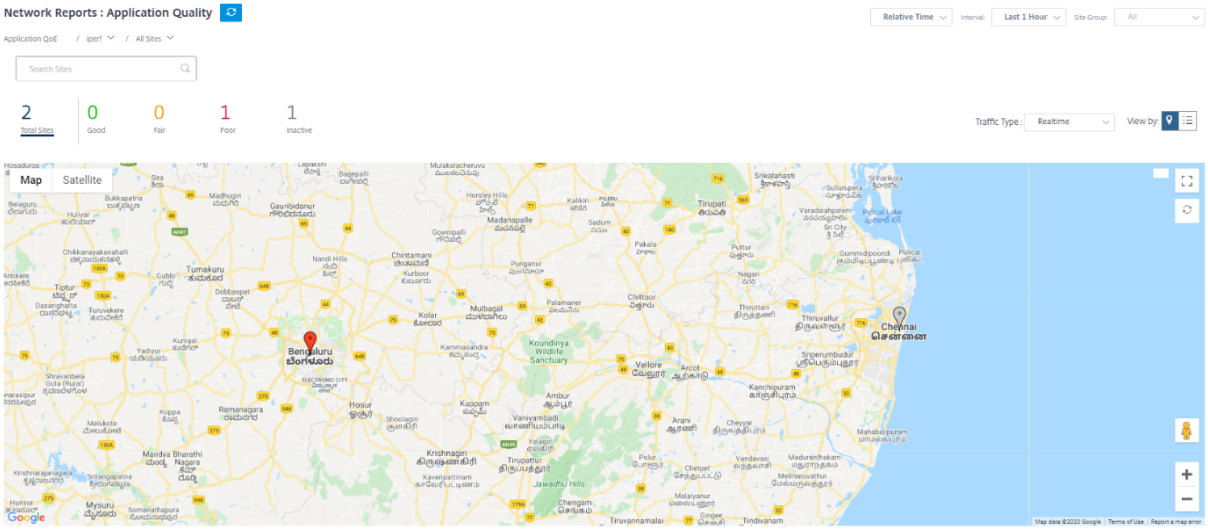

La tarjeta de aplicación individual muestra el número de sitios que tienen QoE de aplicación deficiente, justa o buena para la aplicación específica. También muestra el número de sitios que no están utilizando activamente la aplicación. El QoE promedio es la puntuación media de QoE de la aplicación en todos los sitios de la red.




Haga clic en una tarjeta de solicitud individual para ver los detalles sobre el número de sitios que tienen QoE de aplicación buena, justa o deficiente para la aplicación seleccionada. Se muestra una

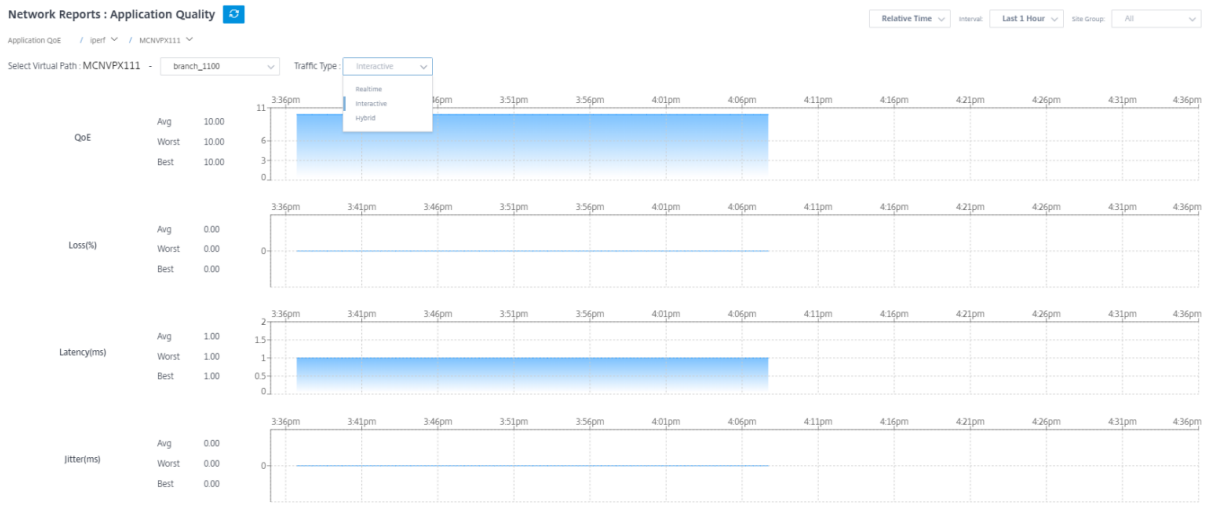
 

vista de mapa de todos los sitios que ejecutan la aplicación seleccionada. Haga clic en un sitio del mapa para profundizar y ver las estadísticas de QoE de la aplicación de las distintas rutas virtuales del sitio.




Puede ver las siguientes métricas para el tráfico en tiempo real, interactivo e híbrido para el período de tiempo seleccionado:

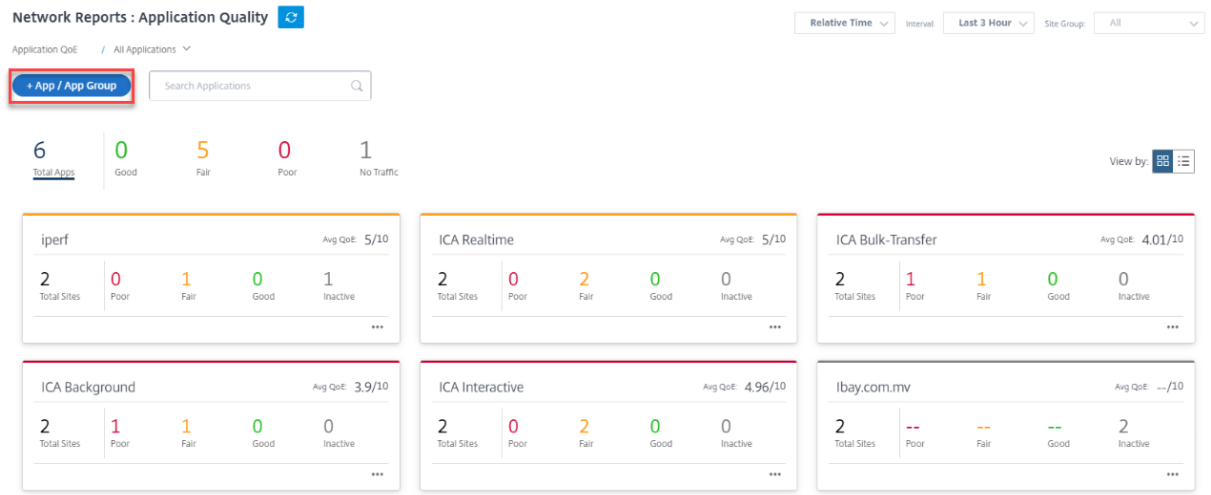
- **QoE**: La puntuación de QoE del tráfico.
- **Pérdida**: El porcentaje de pérdida del tráfico.
- **Latencia**: La latencia en milisegundos del tráfico.
- **Fluctuación**: fluctuación observada en milisegundos para el tráfico.



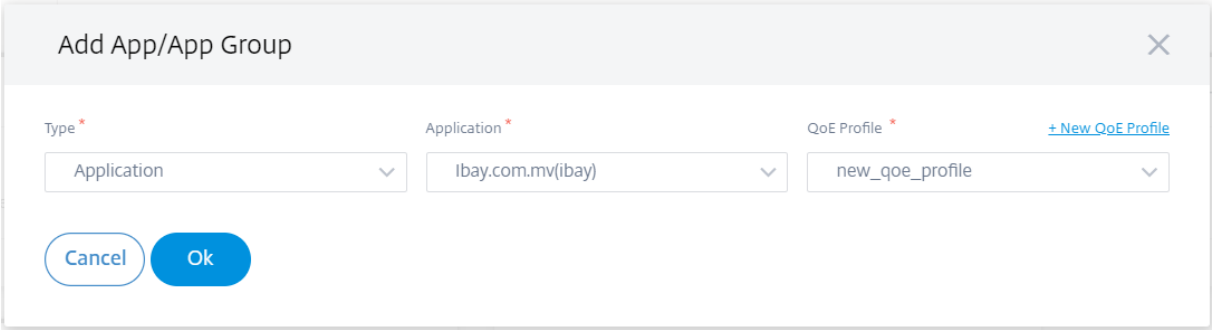

 

### Perfiles QoE de la aplicación

Haga clic en **+ Aplicación/Grupo** de aplicaciones para asignar aplicaciones, aplicaciones personalizadas o grupos de aplicaciones a los perfiles de QoE predeterminados o personalizados.




Los perfiles QoE definen el umbral para el tráfico en tiempo real, interactivo e híbrido. Los umbrales QoE según los perfiles QoE se aplican a la aplicación o grupo de aplicaciones seleccionado.




Haga clic en **+ Nuevo perfil de QoE** para crear un nuevo perfil de QoE de la aplicación e introduzca el valor de los siguientes parámetros:

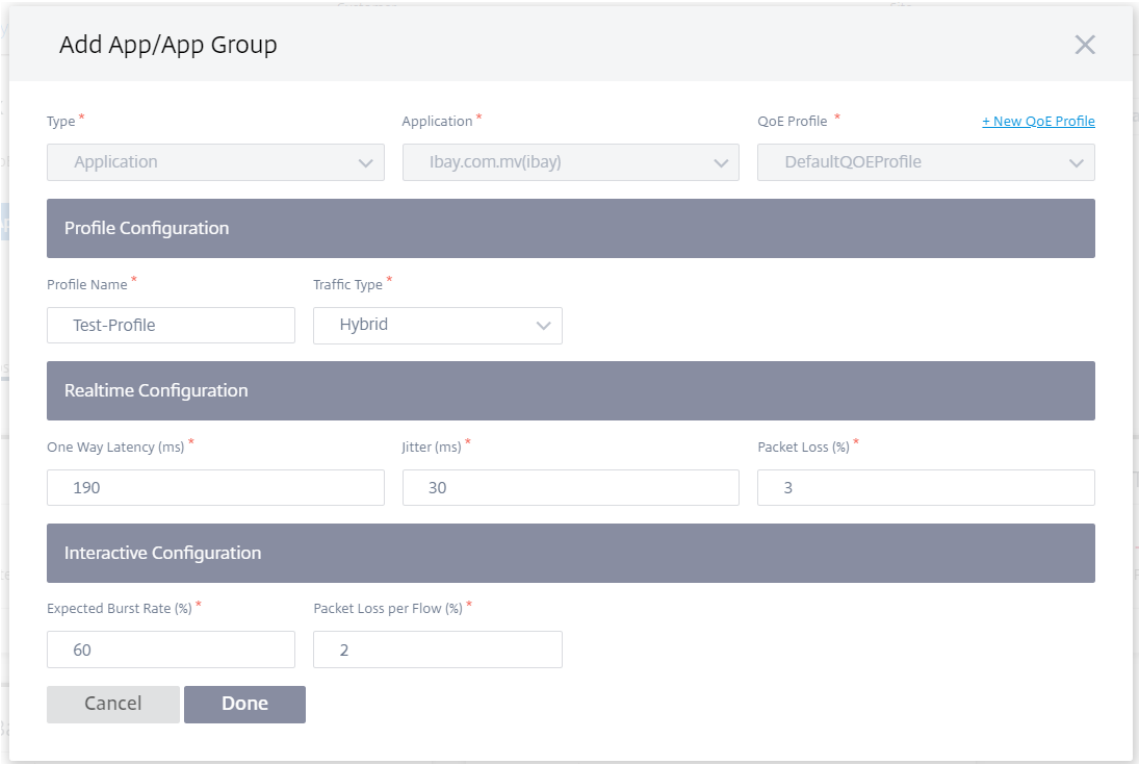
- **Nombre del perfil**: Nombre para identificar el perfil que establece los umbrales para el tráfico interactivo y en tiempo real.
- **Tipo de tráfico**: Elija el tipo de tráfico: En tiempo real, interactivo o híbrido. Si el tipo de tráfico es Híbrido, puede configurar umbrales de perfil QoE en tiempo real e interactivo.
- **Configuración en tiempo real**: C onfigure umbrales para los flujos de tráfico que seleccionan la directiva de QoS en tiempo real. Un flujo de una aplicación en tiempo real que cumple los siguientes umbrales de latencia, pérdida y fluctuación se considera de buena calidad.
  - **Latencia unidireccional**: El umbral de latencia en milisegundos. El valor predeterminado del perfil QoE es 160 ms.

  - **Jitter**: El umbral de jitter en milisegundos. El valor predeterminado del perfil QoE es de 30 ms.
  - **Pérdida de paquetes**: Porcentaje de pérdida de paquetes. El valor predeterminado del perfil QoE es del 2%.

- **Configuración interactiva**: Configure umbrales para los flujos de tráfico que seleccionen la directiva de QoS interactiva. Un flujo de una aplicación interactiva que cumple el siguiente umbral de relación de ráfaga y pérdida de paquetes se considera de buena calidad.

  - **Velocidad de ráfaga esperada**: Porcentaje de la tasa de ráfaga esperada. La velocidad de ráfaga de salida debe ser al menos el porcentaje configurado de velocidad de ráfaga de entrada. El valor predeterminado del perfil QoE es del 60%.
  - **Pérdida de paquetes por flujo**: Porcentaje de pérdida de paquetes. El valor predeterminado del perfil QoE es 1%.




La aplicación recién agregada se muestra en el panel Calidad de la aplicación.

También puede definir y configurar la QoE de la aplicación desde los ajustes de la aplicación y el DNS para obtener más información, consulte Perfiles de calidad de la aplicación y Configuración de la calidadde

# Informes del sitio

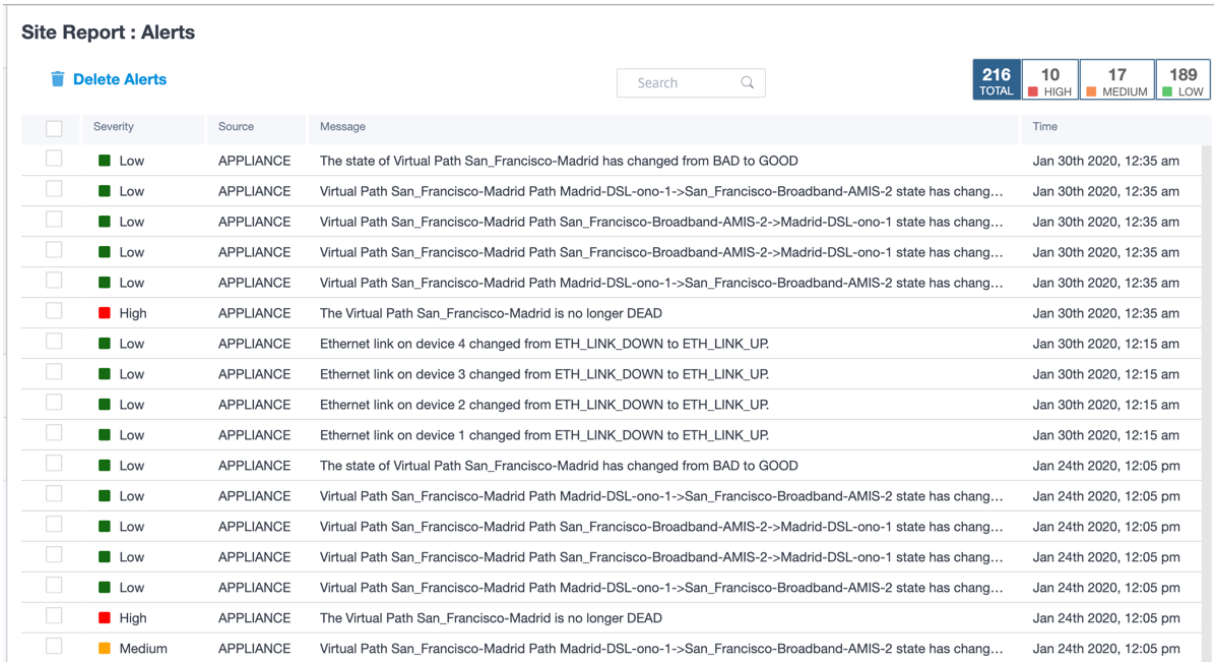
October 31, 2022

**Los informes del sitio** proporcionan visibilidad de las alertas a nivel del sitio, las tendencias de uso, la calidad, la información del dispositivo y las estadísticas del firewall.

## Alertas

El administrador del sitio puede revisar un informe detallado de todos los eventos y alertas generados al nivel de sitio.

Incluye la gravedad, el sitio en el que se originó la alerta, el mensaje de alerta, la hora y otros detalles.




| Severity | Source | Message | Time |
|---|---|---|---|
| Low | APPLIANCE | The state of Virtual Path San_Francisco-Madrid has changed from BAD to GOOD | Jan 30th 2020, 12:35 am |
| Low | APPLIANCE | Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang... | Jan 30th 2020, 12:35 am |
| Low | APPLIANCE | Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang... | Jan 30th 2020, 12:35 am |
| Low | APPLIANCE | Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang... | Jan 30th 2020, 12:35 am |
| Low | APPLIANCE | Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang... | Jan 30th 2020, 12:35 am |
| High | APPLIANCE | The Virtual Path San_Francisco-Madrid is no longer DEAD | Jan 30th 2020, 12:35 am |
| Low | APPLIANCE | Ethernet link on device 4 changed from ETH_LINK_DOWN to ETH_LINK_UP. | Jan 30th 2020, 12:15 am |
| Low | APPLIANCE | Ethernet link on device 3 changed from ETH_LINK_DOWN to ETH_LINK_UP. | Jan 30th 2020, 12:15 am |
| Low | APPLIANCE | Ethernet link on device 2 changed from ETH_LINK_DOWN to ETH_LINK_UP. | Jan 30th 2020, 12:15 am |
| Low | APPLIANCE | Ethernet link on device 1 changed from ETH_LINK_DOWN to ETH_LINK_UP. | Jan 30th 2020, 12:15 am |
| Low | APPLIANCE | The state of Virtual Path San_Francisco-Madrid has changed from BAD to GOOD | Jan 24th 2020, 12:05 pm |
| Low | APPLIANCE | Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang... | Jan 24th 2020, 12:05 pm |
| Low | APPLIANCE | Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang... | Jan 24th 2020, 12:05 pm |
| Low | APPLIANCE | Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang... | Jan 24th 2020, 12:05 pm |
| Low | APPLIANCE | Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang... | Jan 24th 2020, 12:05 pm |
| High | APPLIANCE | The Virtual Path San_Francisco-Madrid is no longer DEAD | Jan 24th 2020, 12:05 pm |
| Medium | APPLIANCE | Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang... | Jan 24th 2020, 12:05 pm |

Se pueden utilizar las opciones de filtrado adecuadas según sea necesario, por ejemplo: busque todas las alertas de alta gravedad en el sitio o las alertas que se produjeron durante un período determinado.

También puede seleccionar y borrar alertas.

## Uso

Los administradores del sitio pueden revisar las tendencias de uso, como **las aplicaciones principales, las categorías de aplicaciones**principales y el ancho de **banda** de las aplicaciones en un sitio

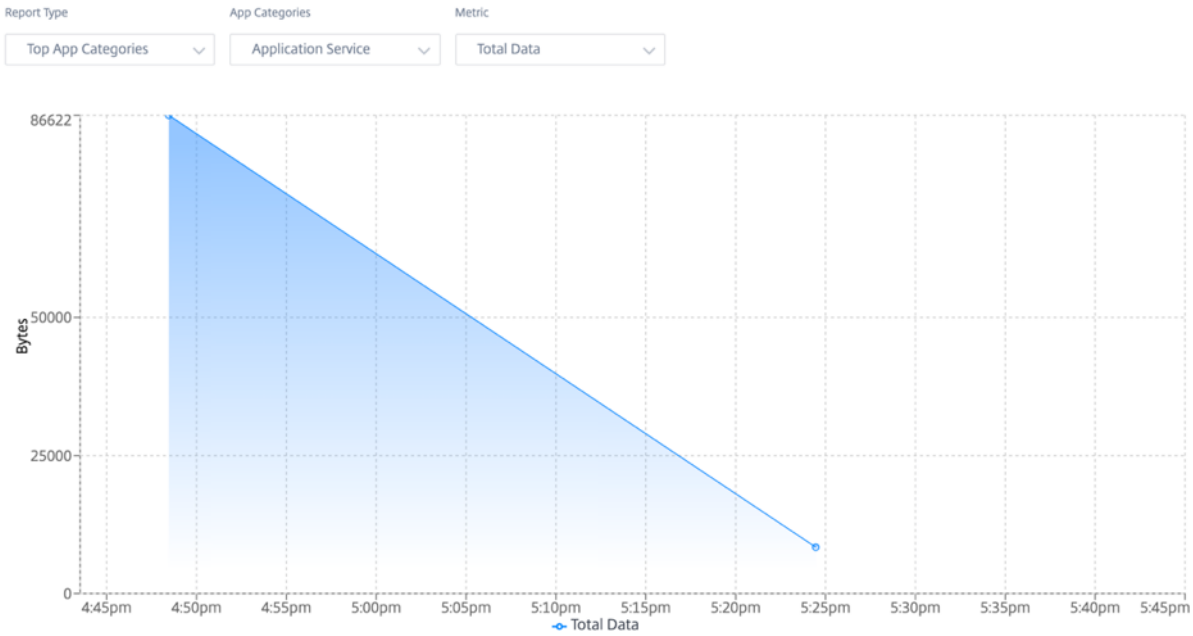
 

en

### Principales aplicaciones y categorías de aplicaciones

La tabla de **aplicaciones principalesy categorías de aplicaciones** principales muestra las aplicaciones principales y las principales familias de aplicaciones que se utilizan ampliamente en el sitio. Esto le permite analizar el patrón de consumo de datos y reasignar el límite de ancho de banda para cada clase de datos dentro del sitio.

También puede ver las estadísticas de uso del ancho de banda. Las estadísticas de ancho de banda se recopilan para el intervalo de tiempo seleccionado. Puede filtrar el informe estadístico según el **tipo de informe, las categorías de aplicaciones o aplicaciones** y **las métricas**.



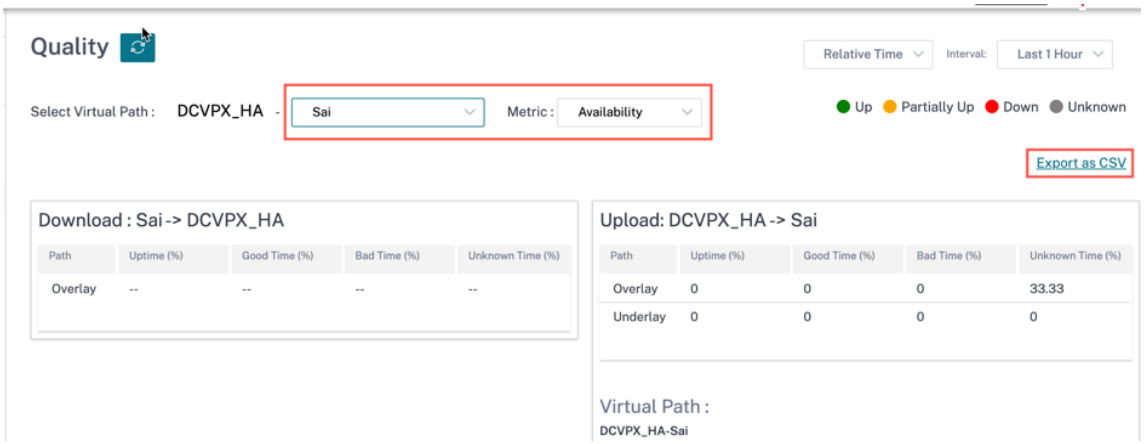

- **Tipo de informe: S**eleccione las **mejores aplicaciones o categorías** de aplicaciones de la lista.
- **Aplicaciones/categorías de aplicaciones: S**eleccione las aplicaciones o categorías principales (como el servicio de red) de la lista.
- **Métrica: S**eleccione la métrica de ancho de banda (como datos totales, datos entrantes, ancho de banda total) de la lista.

## Calidad

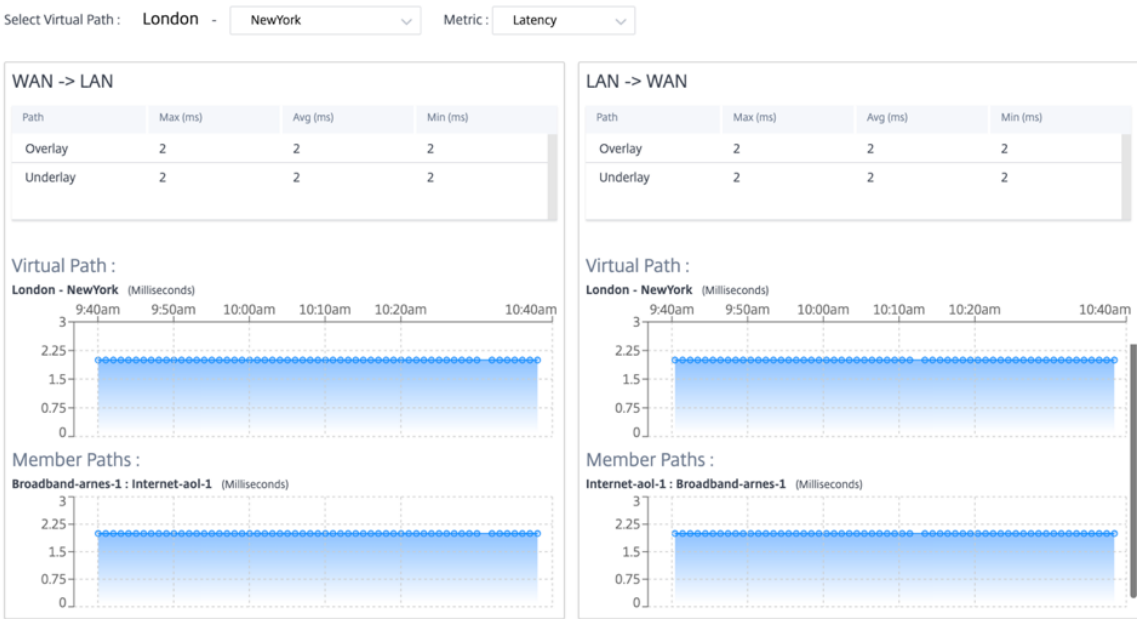
Los administradores del sitio pueden utilizar los informes de calidad para analizar la calidad de la experiencia (QoE) en el sitio para cada métrica de QoS, como disponibilidad, pérdida, latencia y fluctuación. La métrica de calidad se muestra tanto para las rutas virtuales superpuestas como para las rutas de miembro subyacentes.

- **Disponibilidad**

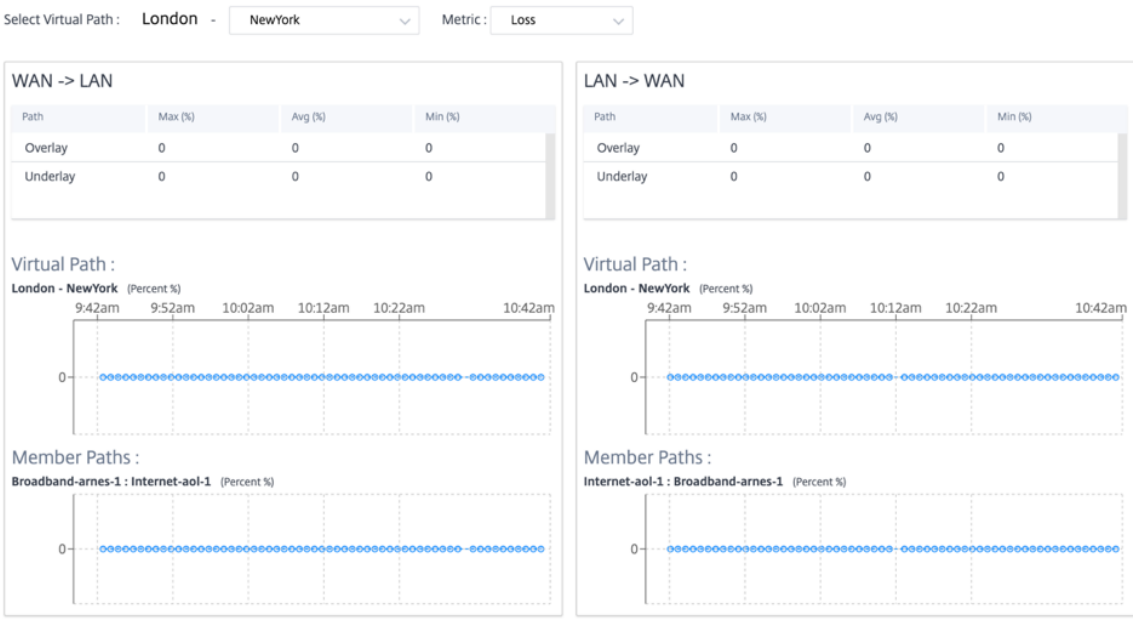



- **Latencia**

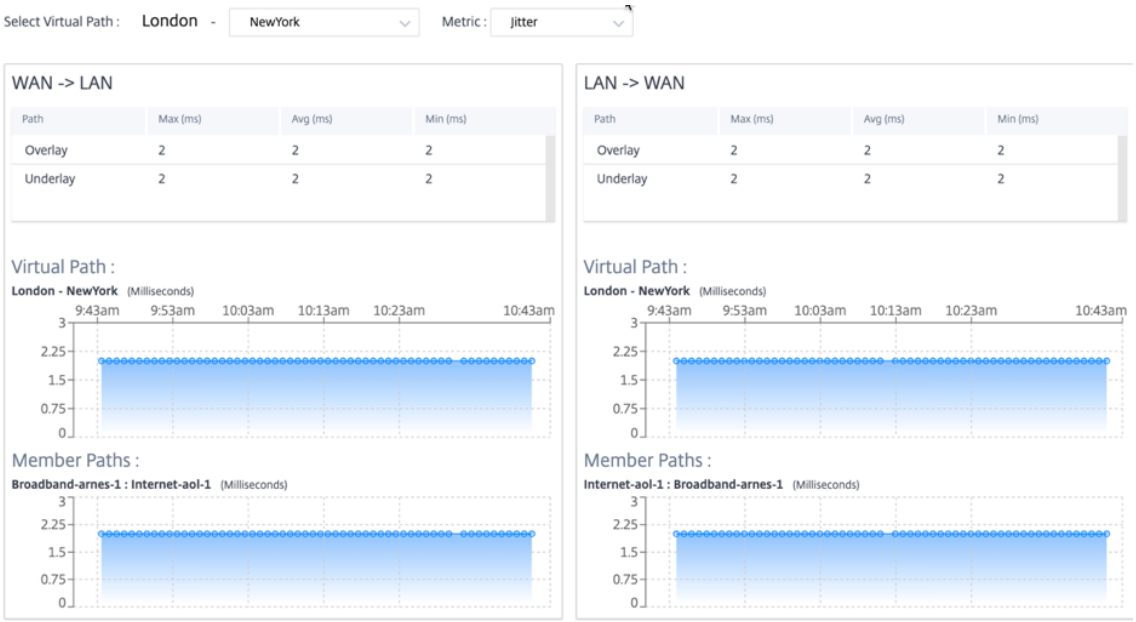



- **Pérdida**

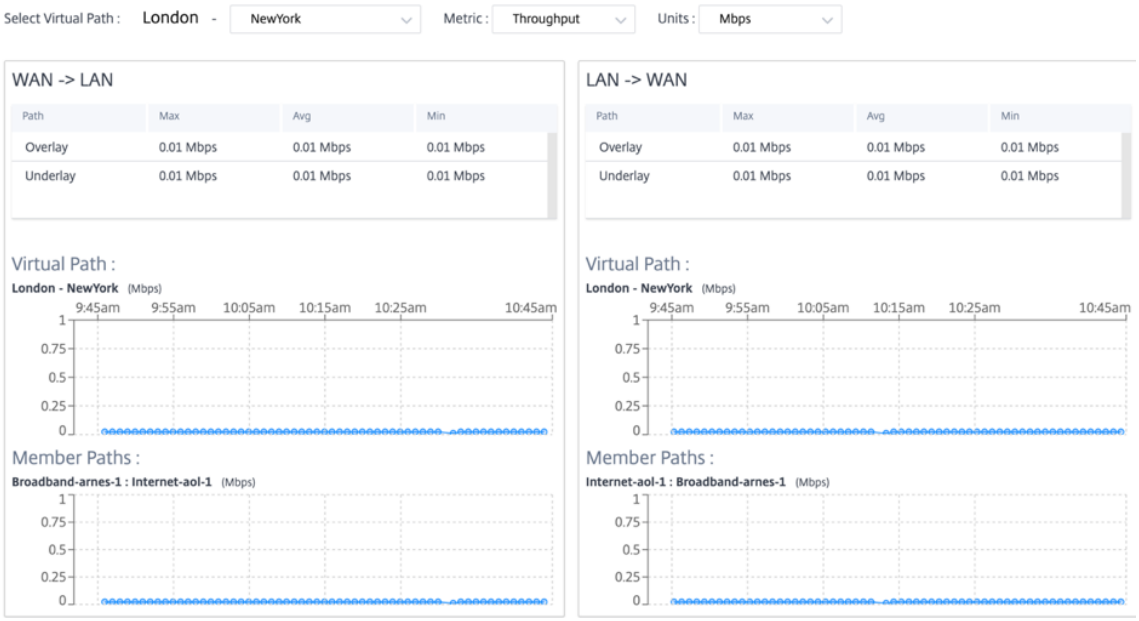



- **Vibración**




- **Rendimiento**

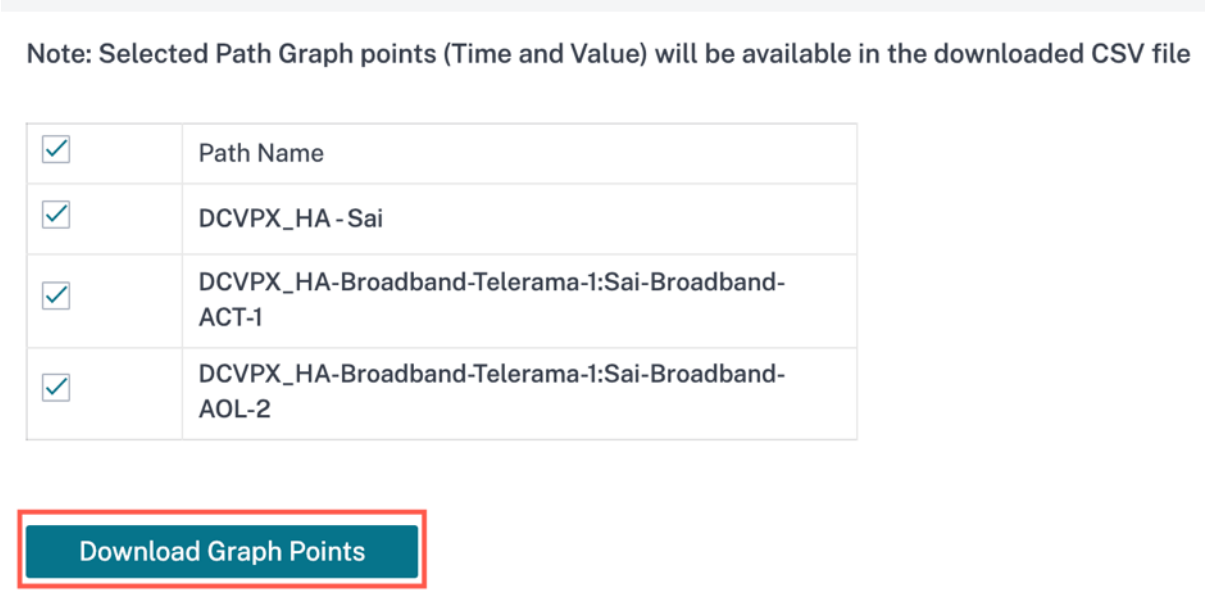



### Exportar como CSV

Con la función **Exportar como CSV**, puede descargar los puntos del gráfico de rutas (ruta virtual/de miembros) para cualquier serie temporal (horaria, semanal, etc.) como un archivo de valores separados por comas (CSV) de Excel y poder trazar todos los puntos de datos distintos para un informe de sitio en particular.

Para descargar/exportar el gráfico de rutas como CSV, vaya a **Informes** > **Calidad** al nivel de sitio. Seleccione el sitio y la métrica en la lista desplegable y haga clic en el enlace **Exportar como CSV**.

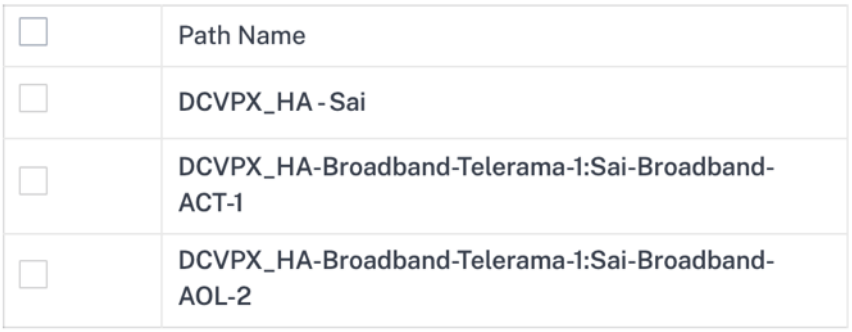
Seleccione la ruta para la que quiere obtener los datos y haga clic en **Descargar puntos del gráfico**.



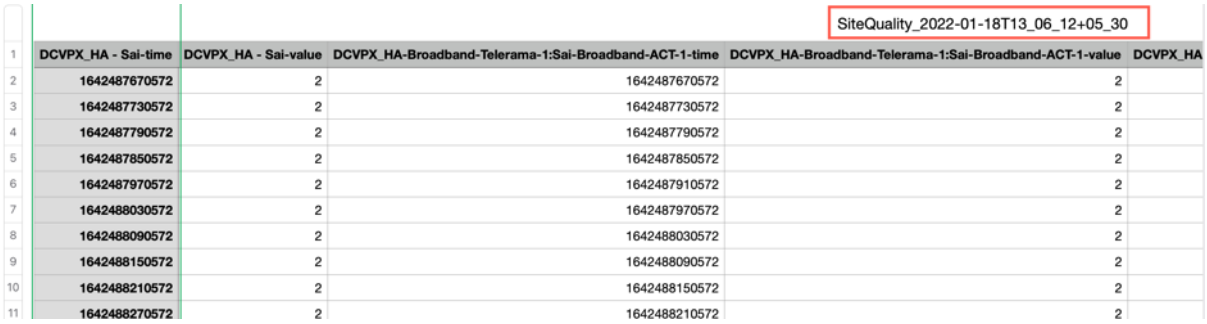
De forma predeterminada, todas las casillas de verificación de la ruta se seleccionan automáticamente. Puede modificarlo según sea necesario.

> **Nota**
>
> Si no se selecciona ninguna de las rutas, el botón **Descargar puntos del gráfico** permanece desactivado.





La convención de nomenclatura del archivo CSV descargado es **SiteQuality**, seguida de una marca de tiempo de la descarga. Puede ver cada ruta con un par de tiempo y valor junto con un identificador único. Puede ver el tiempo en milisegundos y el valor en unidades.



| | SiteQuality_2022-01-18T13_06_12+05_30 | | | | |
|---|---|---|---|---|---|
| 1 | DCVPX_HA - Sai-time | DCVPX_HA - Sai-value | DCVPX_HA-Broadband-Telerama-1:Sai-Broadband-ACT-1-time | DCVPX_HA-Broadband-Telerama-1:Sai-Broadband-ACT-1-value | DCVPX_HA |
| 2 | 1642487670572 | 2 | 1642487670572 | 2 | |
| 3 | 1642487730572 | 2 | 1642487730572 | 2 | |
| 4 | 1642487790572 | 2 | 1642487790572 | 2 | |
| 5 | 1642487850572 | 2 | 1642487850572 | 2 | |
| 6 | 1642487970572 | 2 | 1642487910572 | 2 | |
| 7 | 1642488030572 | 2 | 1642487970572 | 2 | |
| 8 | 1642488090572 | 2 | 1642488030572 | 2 | |
| 9 | 1642488150572 | 2 | 1642488090572 | 2 | |
| 10 | 1642488210572 | 2 | 1642488150572 | 2 | |
| 11 | 1642488270572 | 2 | 1642488210572 | 2 | |

Según la siguiente selección de métricas, puede ver que se están generando diferentes valores en el archivo CSV:

- **Pérdida: E**l valor se muestra en%.
- **Latencia y fluctuación: E**l valor se muestra en milisegundos.
- **Rendimiento: E**l valor se muestra en Kbps.
- **Disponibilidad:** muestra la ruta hacia arriba, parcialmente hacia arriba, hacia abajo y la hora desconocida.
  - Si el valor es 4, la ruta está en estado activo.

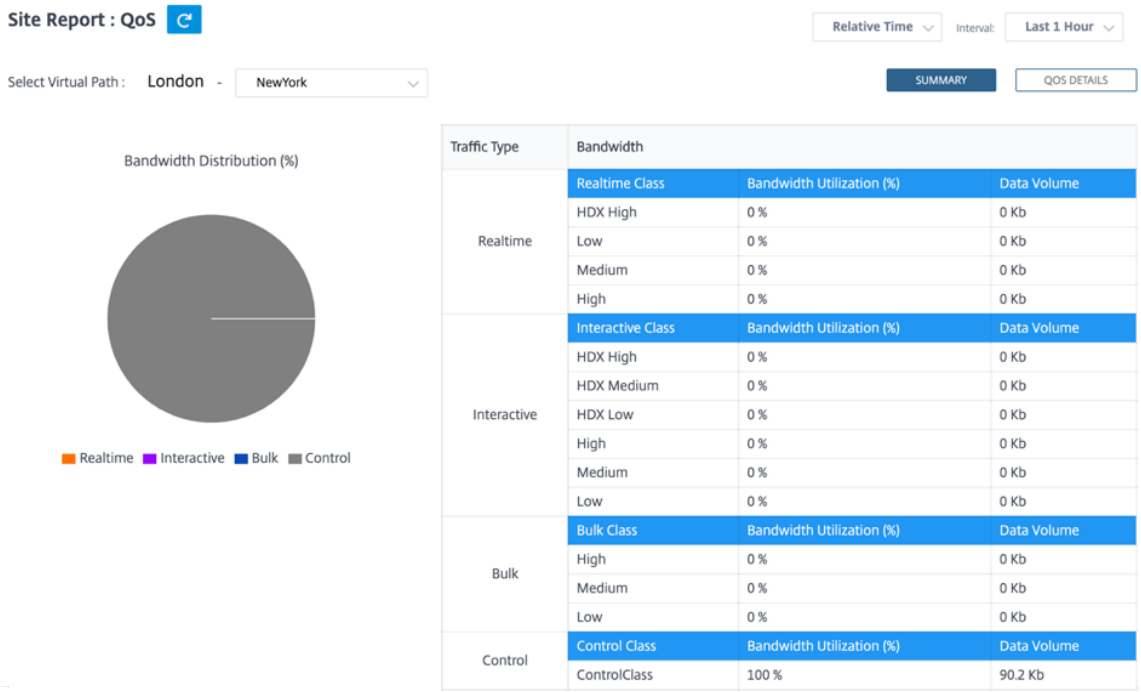
 

- Si el valor es 3, la ruta está parcialmente en estado activo.
- Si el valor es inferior a 3, la ruta está en estado defectuoso/inactivo.

### Calidad del servicio

Quality of Service (QoS) administra el tráfico de datos para reducir la pérdida de paquetes, la latencia y la fluctuación en la red. Para obtener más información, consulte Calidad de servicio. Las siguientes son dos formas de ver el informe de calidad de servicio (QoS):

- **Vista de resumen: L**a vista de resumen proporciona una visión general del consumo de ancho de banda en todos los tipos de tráfico: En tiempo real, interactivo, masivo y de control en la red y por sitio.



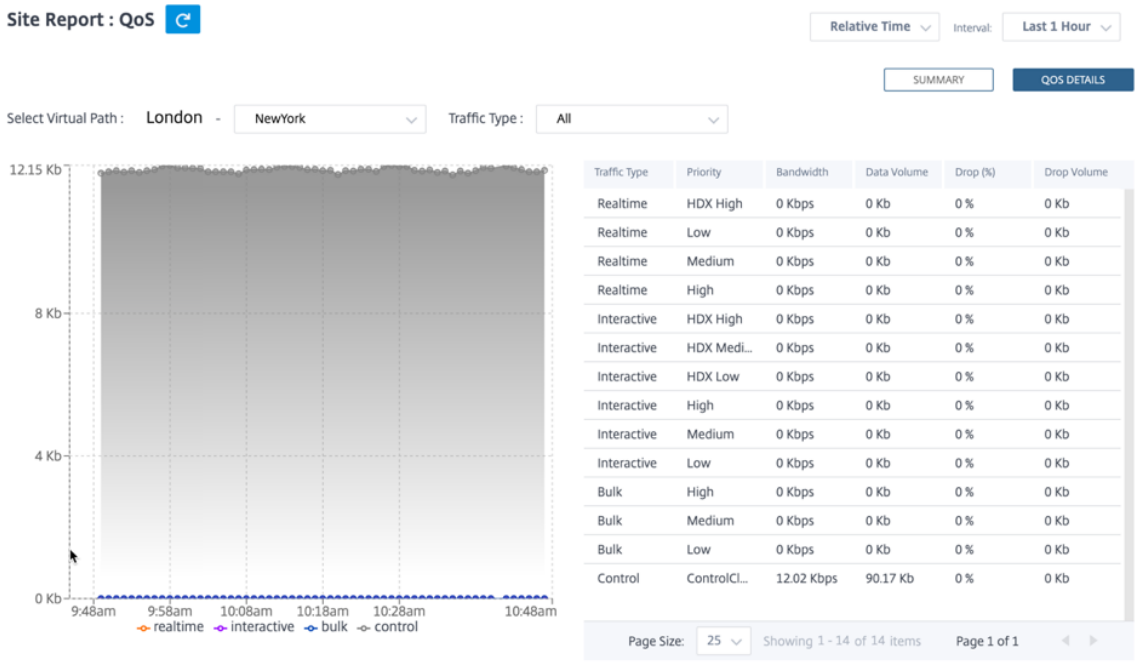

| Traffic Type | Bandwidth | | |
|---|---|---|---|
| Realtime | Realtime Class | Bandwidth Utilization (%) | Data Volume |
| | HDX High | 0 % | 0 Kb |
| | Low | 0 % | 0 Kb |
| | Medium | 0 % | 0 Kb |
| | High | 0 % | 0 Kb |
| Interactive | Interactive Class | Bandwidth Utilization (%) | Data Volume |
| | HDX High | 0 % | 0 Kb |
| | HDX Medium | 0 % | 0 Kb |
| | HDX Low | 0 % | 0 Kb |
| | High | 0 % | 0 Kb |
| | Medium | 0 % | 0 Kb |
| | Low | 0 % | 0 Kb |
| Bulk | Bulk Class | Bandwidth Utilization (%) | Data Volume |
| | High | 0 % | 0 Kb |
| | Medium | 0 % | 0 Kb |
| | Low | 0 % | 0 Kb |
| Control | Control Class | Bandwidth Utilization (%) | Data Volume |
| | ControlClass | 100 % | 90.2 Kb |

  - **Tiempo real: S**e usa para tráfico de baja latencia, bajo ancho de banda y urgente. Las aplicaciones en tiempo real son urgentes, pero en realidad no necesitan un gran ancho de banda (por ejemplo, voz sobre IP). Las aplicaciones en tiempo real son sensibles a la latencia y la fluctuación, pero pueden tolerar algunas pérdidas.
  - **Interactivo: S**e usa para tráfico interactivo con requisitos de latencia baja a media y requisitos de ancho de banda bajos a medios. Las aplicaciones interactivas implican la intervención humana en forma de clics del ratón o movimientos del cursor. La interacción suele ser entre un cliente y un servidor. Es posible que la comunicación no necesite un ancho de banda alto, pero es sensible a la pérdida y la latencia. Sin embargo, el servidor al cliente necesita un gran ancho de banda para transferir información gráfica, que puede no ser susceptible de pérdida.

  - **Masivo: S**e usa para tráfico de gran ancho de banda que puede tolerar una latencia Las aplicaciones que manejan la transferencia de archivos y necesitan un ancho de banda alto se clasifican como clase masiva. Estas aplicaciones implican poca interferencia humana y son manejadas principalmente por los propios sistemas.
  - **Control: S**e usa para transferir paquetes de control que contienen información de enrutamiento, programación y estadísticas de enlaces.

- **Vista detallada: La vista** detallada captura las tendencias en torno al consumo de ancho de banda, el volumen de tráfico, los paquetes descartados, etc. Para cada clase de QoS asociada a una ruta virtual superpuesta. Puede ver las estadísticas de QoS basadas en la ruta virtual entre dos sitios.




## Estadísticas históricas

Para cada sitio, puede ver las estadísticas como gráficos para los siguientes parámetros de red:

- Rutas virtuales
- Rutas
- Enlaces WAN
- Interfaces
- Clases
- Servicios
- Túneles GRE
- Túneles IPsec

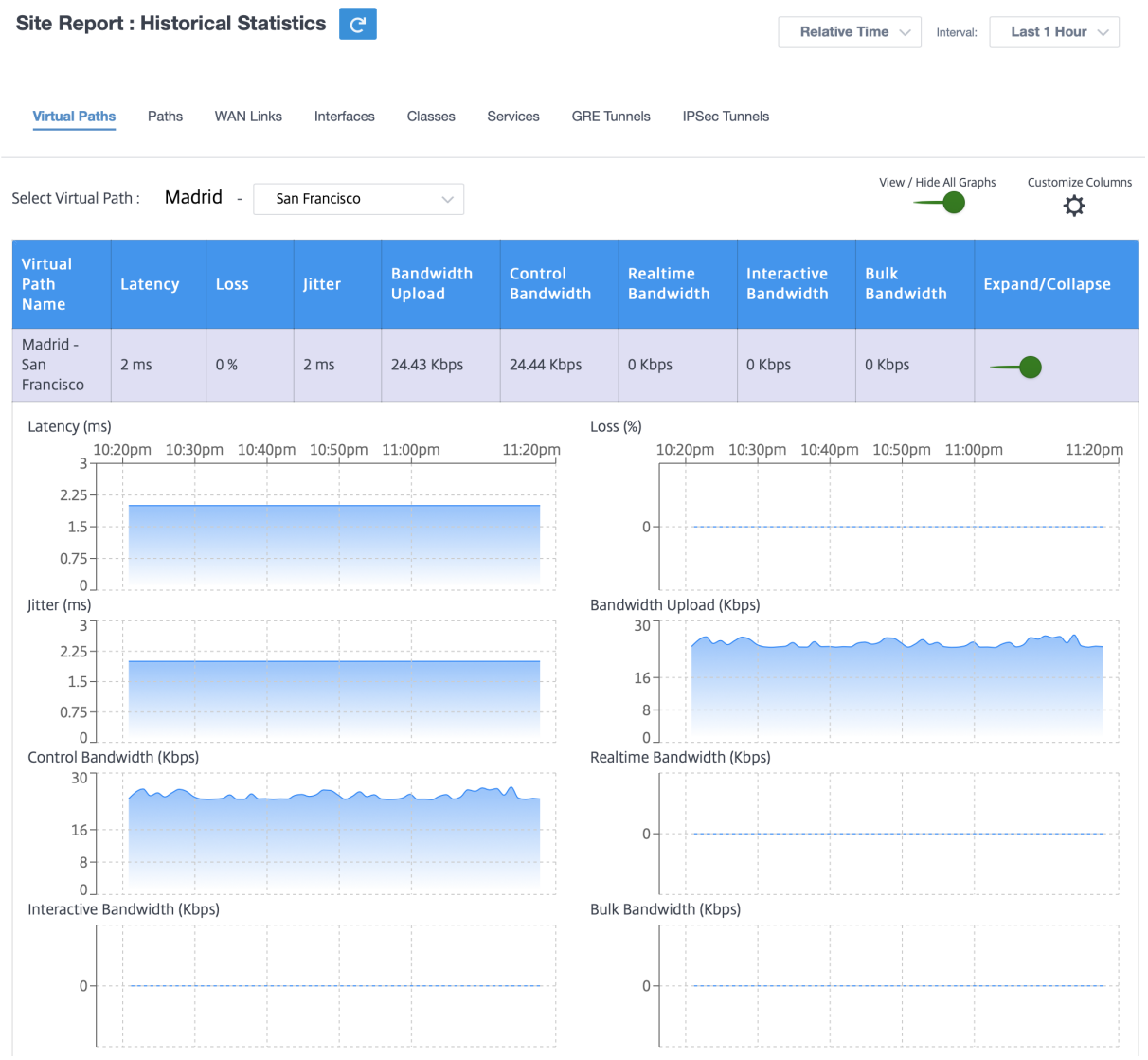
 

Las estadísticas se recogen como gráficos. Estos gráficos se trazan como línea temporal frente al uso, lo que le permite comprender las tendencias de uso de varias propiedades de objetos de red. Puede ver gráficos para estadísticas de aplicaciones de toda la red.

Puede ver u ocultar los gráficos y personalizar las columnas según sea necesario.

### Rutas virtuales

Para ver las estadísticas de **rutas virtuales**, vaya a **Informes > Estadísticas > Rutas virtuales**.




Puede ver las siguientes métricas:

- **Nombre de la ruta virtual**: El nombre de la ruta virtual.
- **Latencia**: L a latencia en milisegundos del tráfico en tiempo real.
- **Pérdida**: Porcentaje de paquetes perdidos.

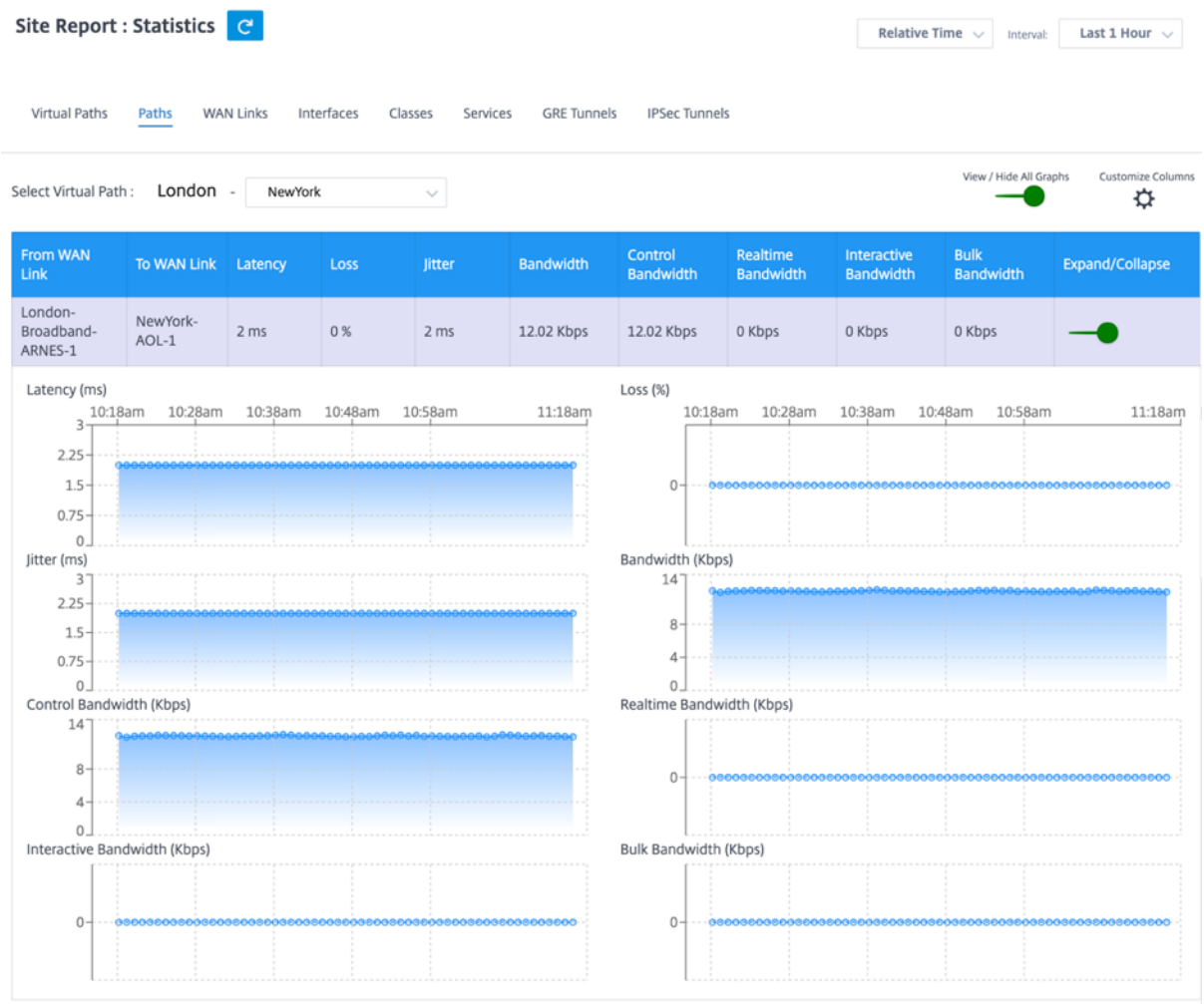
 

- **Fluctuación**: variación en el retraso de los paquetes recibidos, en milisegundos.
- **Entrada de ancho**de banda: Uso de ancho de **banda de ingreso (LAN > WAN)** durante el período de tiempo seleccionado.
- **Ancho de banda de control**: Ancho de banda utilizado para transferir paquetes de control que contienen información de enrutamiento, programación y estadísticas de enlaces.
- Ancho de**banda en tiempo real**: Ancho de banda que consumen las aplicaciones que pertenecen al tipo de clase en tiempo real en la configuración de SD-WAN. El rendimiento de tales aplicaciones depende en gran medida de la latencia de la red. Un paquete retrasado es peor que un paquete perdido (por ejemplo, VoIP, Skype for Business).
- Ancho de**banda interactivo**: Ancho de banda que consumen las aplicaciones que pertenecen al tipo de clase interactiva en la configuración de SD-WAN. El rendimiento de estas aplicaciones depende en gran medida de la latencia de la red y de la pérdida de paquetes (por ejemplo, XenDesktop, XenApp).
- Ancho de**banda masivo**: Ancho de banda que consumen las aplicaciones que pertenecen al tipo de clase masiva en la configuración de SD-WAN. Estas aplicaciones implican poca intervención humana y son manejadas principalmente por los propios sistemas (por ejemplo, FTP, operaciones de copia de seguridad).
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

#### Rutas

Para ver las estadísticas de **rutas**, vaya a la ficha **Informes > Estadísticas > Rutas**.




Puede ver las siguientes métricas:

- **Desde el enlace WAN**: El enlace WAN de origen.
- **Al enlace WAN**: El enlace WAN de destino.
- **Latencia**: La latencia en milisegundos del tráfico en tiempo real.
- **Pérdida**: Porcentaje de paquetes perdidos.
- **Fluctuación**: variación en el retraso de los paquetes recibidos, en milisegundos.
- **Ancho de banda**: Ancho de banda total que consumen todos los tipos de paquetes Ancho de banda = Control de ancho de banda + ancho de banda en tiempo real + ancho de banda interactiva + ancho de banda
- **Ancho de banda de control**: Ancho de banda utilizado para transferir paquetes de control que contienen información de enrutamiento, programación y estadísticas de enlaces.
- Ancho de**banda en tiempo real**: Ancho de banda que consumen las aplicaciones que pertenecen al tipo de clase en tiempo real en la configuración de SD-WAN. El rendimiento de tales aplicaciones depende en gran medida de la latencia de la red. Un paquete retrasado es peor que un paquete perdido (por ejemplo, VoIP, Skype for Business).

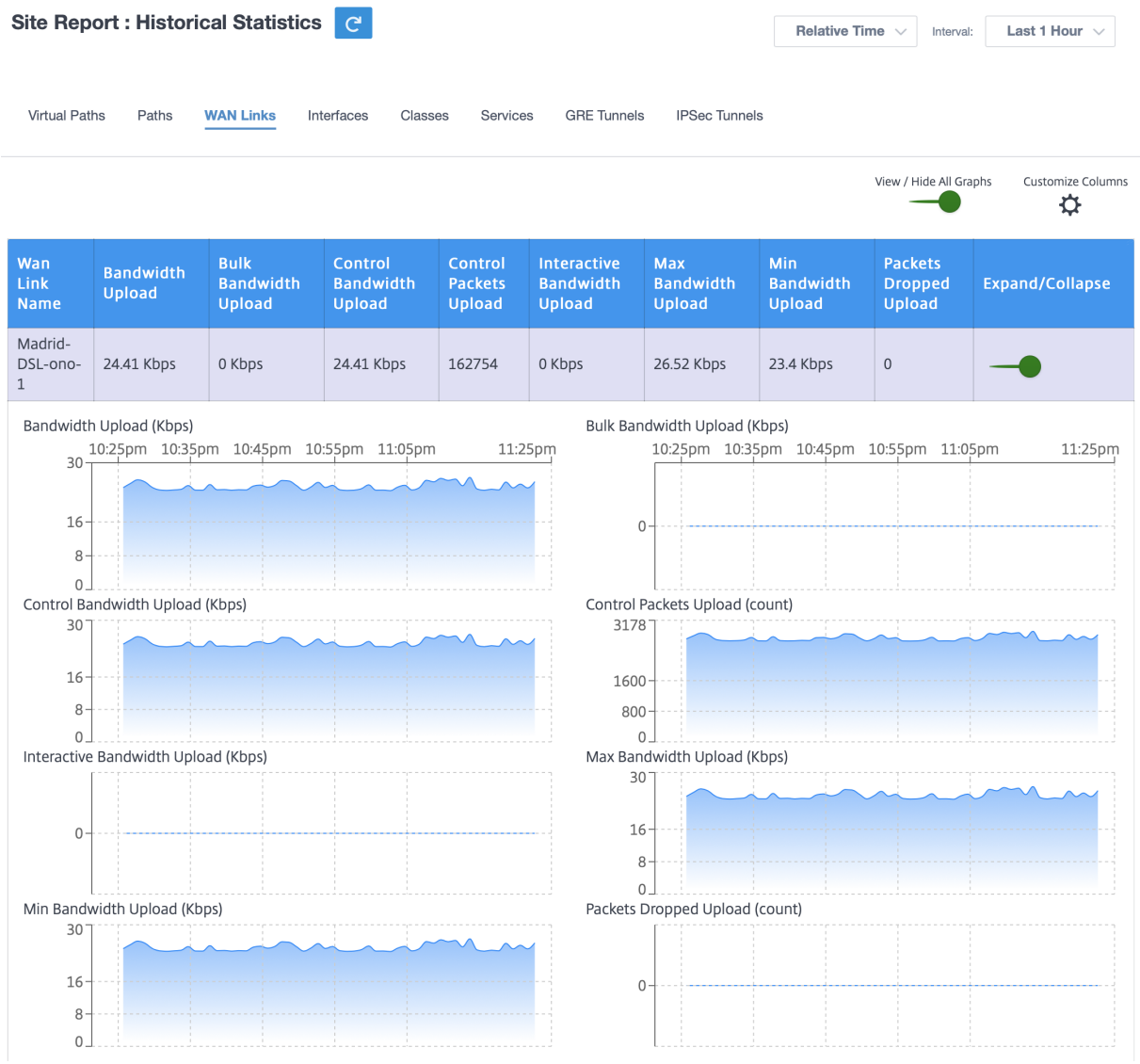
 

- Ancho de**banda interactivo**: Ancho de banda que consumen las aplicaciones que pertenecen al tipo de clase interactiva en la configuración de SD-WAN. El rendimiento de estas aplicaciones depende en gran medida de la latencia de la red y de la pérdida de paquetes (por ejemplo, XenDesktop, XenApp).
- Ancho de**banda masivo**: Ancho de banda que consumen las aplicaciones que pertenecen al tipo de clase masiva en la configuración de SD-WAN. Estas aplicaciones implican poca intervención humana y son manejadas principalmente por los propios sistemas (por ejemplo, FTP, operaciones de copia de seguridad).
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

#### Enlaces WAN

Para ver las estadísticas al nivel de **enlace WAN**, vaya a **Informes > Estadísticas > ficha Vínculos WAN**.




Puede ver las siguientes métricas:

- **Nombre del enlace WAN**: El nombre de la ruta.
- **Entrada de ancho**de banda: Uso de ancho de **banda de ingreso (LAN > WAN)** durante el período de tiempo seleccionado.
- **Entrada masiva de ancho**de banda: Ancho de banda de **entrada (LAN > WAN) de ruta virtual utilizado** por el tráfico masivo durante el período de tiempo seleccionado.
- **Control del ingreso de ancho**de banda: Ancho de banda de acceso **(LAN > WAN) de la ruta virtual utilizado** por Control Traffic durante el período de tiempo seleccionado.
- **Entrada de paquetes de control**: P**aquetes de control de ruta virtual de ingreso (LAN > WAN)** para el período de tiempo seleccionado.
- Entrada de**ancho de banda interactiva**: Ancho **de banda de acceso (LAN > WAN) de ruta virtual utilizado** por el tráfico interactivo durante el período de tiempo seleccionado.

- **Entrada de ancho**de banda **máxima: Ancho de banda máximo de entrada (LAN > WAN) utilizado** en un minuto durante el período de tiempo seleccionado.
- **Entrada de ancho**de banda **mínima: Ancho de banda mínimo de entrada (LAN > WAN) utilizado** en un minuto durante el período de tiempo seleccionado.
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

#### Interfaces

El informe estadístico de las interfaces le ayuda durante la resolución de problemas a ver rápidamente si alguno de los puertos está inactivo. También puede ver el ancho de banda transmitido y recibido o los detalles del paquete en cada puerto. También puede ver el número de errores que se produjeron en estas interfaces durante un período de tiempo determinado.

Para ver las estadísticas de la **interfaz**, vaya a la ficha **Informes > Estadísticas > Interfaces**.

Puede ver las siguientes métricas:

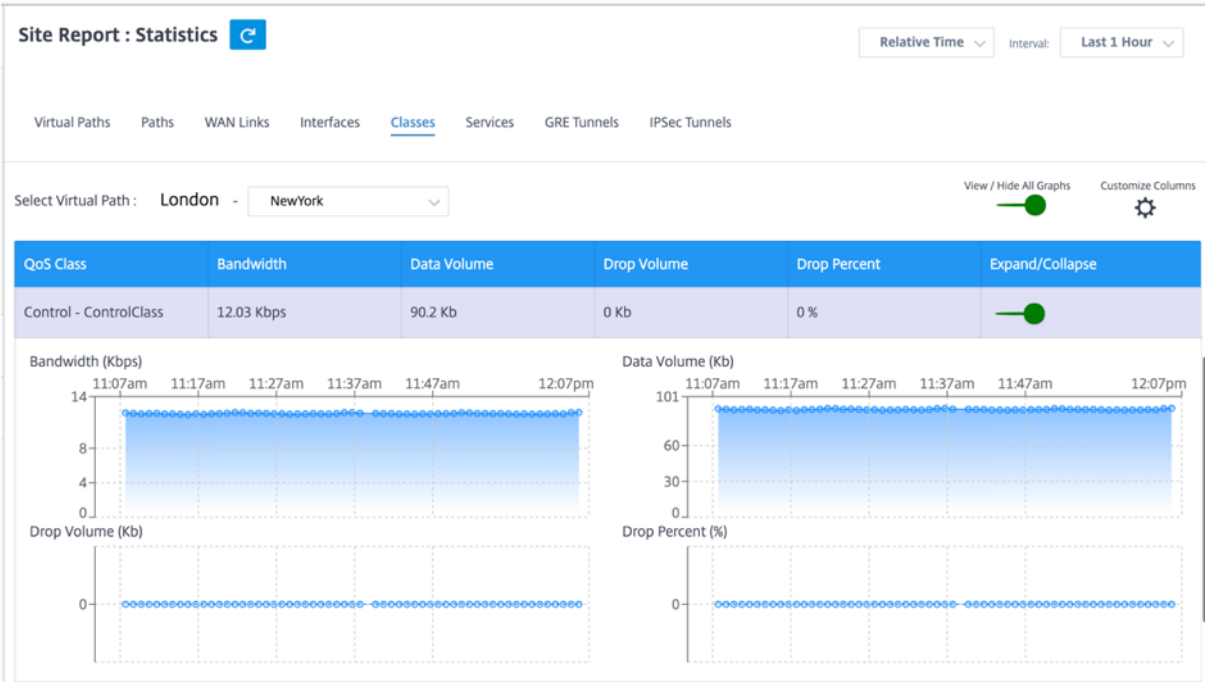
- **Nombre de la interfaz**: El nombre de la interfaz Ethernet.
- **Ancho de banda Tx**: Ancho de banda transmitido.
- **Ancho de banda Rx**: Ancho de banda recibido.
- **Errores**: Número de errores observados durante el período de tiempo seleccionado.
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

#### Clases

Los servicios virtuales se pueden asignar a clases de QoS particulares, y se pueden aplicar restricciones de ancho de banda diferentes a diferentes clases.

Para ver las estadísticas de las **clases**, vaya a la ficha **Informes > Estadísticas > Clases**.




Puede ver las siguientes métricas:

- **Clase de QoS**: El nombre de la clase.
- **Ancho de banda**: Ancho de banda transmitido
- **Volumen**de datos: Datos enviados, en Kbps.
- **Volumen de caída**: Porcentaje de datos descartados.
- **Porcentaje de caída**: Porcentaje de datos descartados.
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

## Servicios

Para ver las estadísticas de **los servicios**, vaya a la ficha **Informes > Estadísticas > Servicios**.

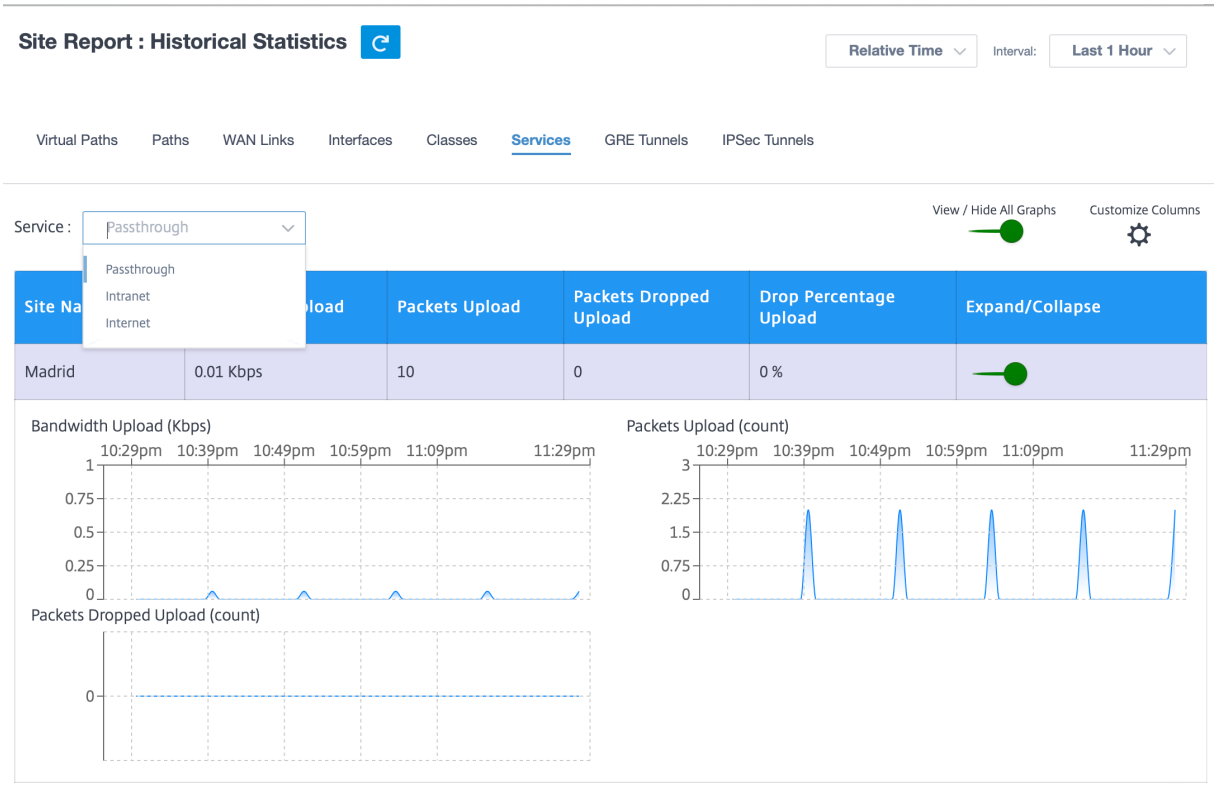
Seleccione el tipo de servicio en la lista. Opciones disponibles:

- **Acceso directo**: Este servicio administra el tráfico que la SD-WAN no intercepta, retrasa, moldea ni cambia. El tráfico dirigido al servicio de acceso directo incluye difusiones, ARP y otro tráfico que no sea IPv4, así como el tráfico en la subred local del dispositivo WAN virtual, subredes configuradas o reglas aplicadas por el administrador de red. La SD-WAN no retrasa, configura ni modifica este tráfico. Por lo tanto, debe asegurarse de que el tráfico PassThrough no consume recursos sustanciales en los enlaces WAN que el dispositivo SD-WAN está configurado para utilizar para otros servicios.
- **Intranet**: Este servicio administra el tráfico de la intranet empresarial que no se ha definido para la transmisión a través de una ruta virtual. Al igual que con el tráfico de Internet, permanece sin

encapsular y la SD-WAN administra el ancho de banda limitando la velocidad de este tráfico en relación con otros tipos de servicios durante los tiempos de congestión. En determinadas condiciones, y si se configura para la reserva de intranet en la ruta virtual, el tráfico que normalmente viaja con una ruta virtual se puede tratar como tráfico de intranet para mantener la fiabilidad de la red.

- **Internet**: Este servicio administra el tráfico entre un sitio de Enterprise y los sitios de la Internet pública. El tráfico de este tipo no está encapsulado. En momentos de congestión, la SD-WAN administra activamente el ancho de banda limitando la velocidad del tráfico de Internet en relación con la ruta virtual y el tráfico de la intranet según la configuración de SD-WAN establecida por el administrador.




Puede ver las siguientes métricas:

- **Nombre del sitio**: El nombre del sitio.
- **Entrada de ancho**de banda: Uso de ancho de **banda de ingreso (LAN > WAN)** durante el período de tiempo seleccionado.
- **Entrada de paquetes**: **(LAN > WAN) Paquetes** enviados durante el intervalo de tiempo seleccionado.
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

### Túneles GRE

Puede utilizar un mecanismo de túnel para transportar paquetes de un protocolo dentro de otro protocolo. El protocolo que lleva el otro protocolo se denomina protocolo de transporte, y el protocolo transportado se denomina protocolo de pasajeros. Generic Routing Encapsulation (GRE) es un mecanismo de tunelización que utiliza IP como protocolo de transporte y puede llevar muchos protocolos de pasajeros diferentes.

La dirección de origen del túnel y la dirección de destino se utilizan para identificar los dos extremos de los vínculos virtuales punto a punto del túnel. Para obtener más información sobre la configuración de túneles GRE en dispositivos Citrix SD-WAN, consulte Túnel GRE.

Para ver las estadísticas **del túnel GRE**, vaya a **Informes > Estadísticas > ficha Túneles GRE**.

Puede ver las siguientes métricas:

- **Nombre del sitio**: El nombre del sitio.
- **Ancho de banda Tx**: Ancho de banda transmitido.
- **Ancho de banda Rx**: Ancho de banda recibido.
- **Paquete eliminado**: Número de paquetes descartados debido a la congestión de la red.
- **Paquetes Fragmentados**: Número de paquetes fragmentados. Los paquetes se fragmentan para crear paquetes más pequeños que pueden pasar a través de un enlace con una MTU más pequeña que el datagrama original. El host receptor vuelve a ensamblar los fragmentos.
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

### Túneles IPsec

Los protocolos de seguridad IP (IPsec) proporcionan servicios de seguridad como el cifrado de datos confidenciales, la autenticación, la protección contra la reproducción y la confidencialidad de los datos para los paquetes IP. Carga útil de seguridad encapsulada (ESP) y Encabezado de autenticación (AH) son los dos protocolos de seguridad IPsec utilizados para proporcionar estos servicios de seguridad.

En el modo de túnel IPsec, todo el paquete IP original está protegido por IPsec. El paquete IP original está envuelto y cifrado, y se agrega un nuevo encabezado IP antes de transmitir el paquete a través del túnel VPN.
Para obtener más información sobre la configuración de túneles IPSec en dispositivos Citrix SD-WAN, consulte Terminación de túneles IPSec.

Para ver las estadísticas **del túnel IPSec**, vaya a **Informes > estadísticas > ficha Túneles IPSec**.

Puede ver las siguientes métricas:

- **Nombre del túnel**: Nombre del túnel.

- **Estado del túnel: Estado**del túnel IPsec.
- **MTU**: Unidad de transmisión máxima: Tamaño del datagrama IP más grande que se puede transferir a través de un enlace específico.
- **Paquetes recibidos**: Número de paquetes recibidos.
- **Paquetes enviados**: Número de paquetes enviados.
- **Paquete eliminado**: Número de paquetes descartados debido a la congestión de la red.
- **Bytes eliminados**: Número de bytes eliminados.
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.

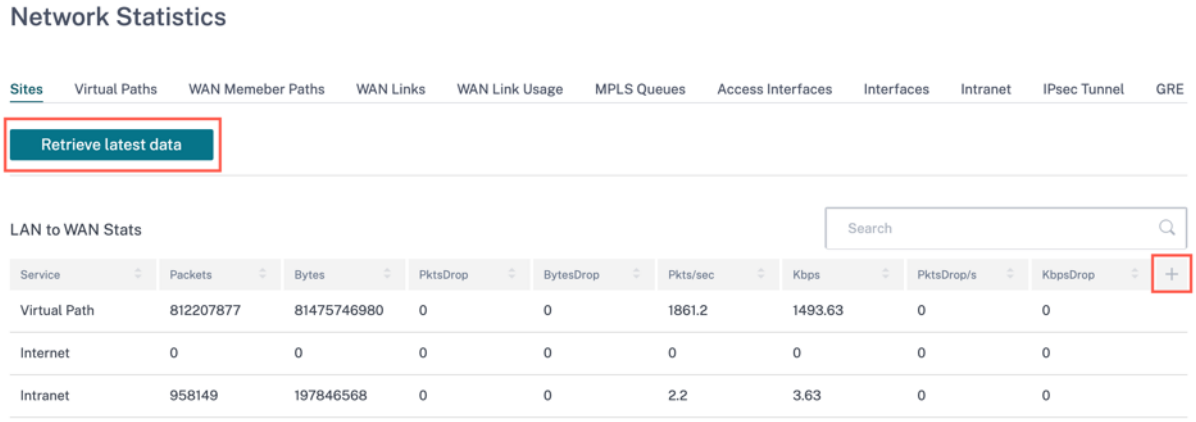
## Estadísticas en tiempo real

### Estadísticas de red

Puede obtener la siguiente información estadística en tiempo real en **Informes > Tiempo real > Estadísticas de red**:

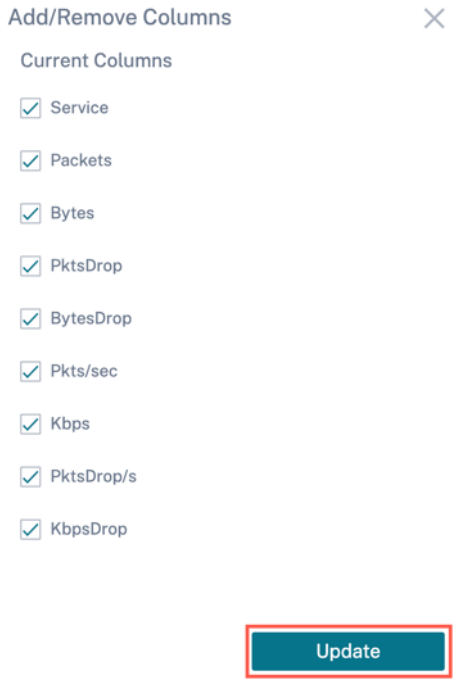
- Sitio
- Rutas virtuales
- Rutas de miembros de WAN
- Enlaces WAN
- Uso de vínculos WAN
- Colas MPLS
- Interfaces de acceso
- Interfaces
- Intranet
- Túnel IPsec
- GRE

Para obtener el informe estadístico en tiempo real, vaya a la ficha correspondiente (como sitio, rutas virtuales, enlaces WAN) y haga clic en **Recuperar los datos más recientes**.



Haga clic en el símbolo más (+) si quiere agregar o eliminar cualquier columna de la tabla de estadísticas y, a continuación, haga clic en **Actualizar**.

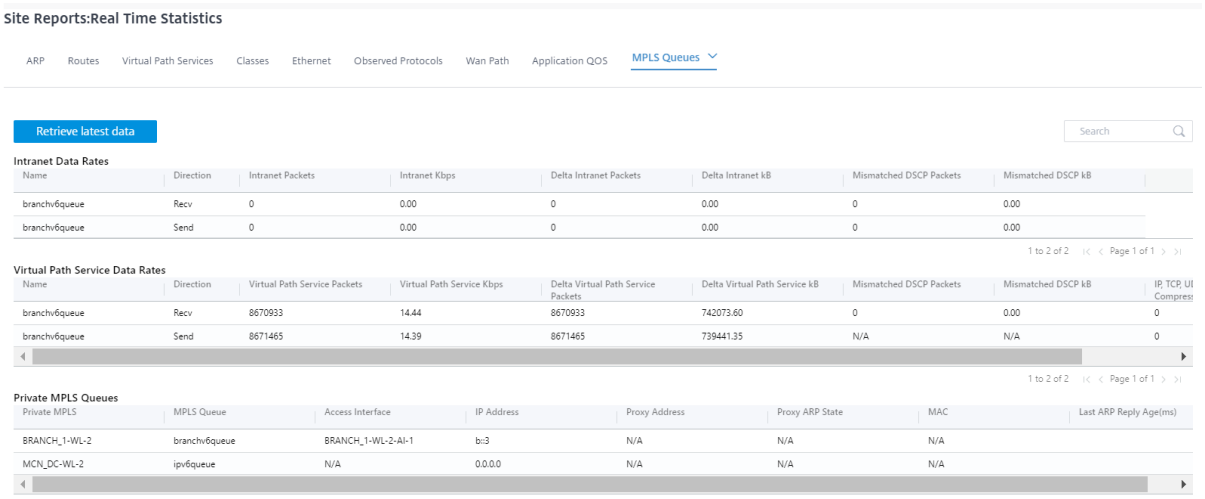



**Colas MPLS** Las colas MPLS permiten definir las colas correspondientes a las colas MPLS de Service Provider, en los Vínculos WAN de MPLS. Para obtener información sobre la configuración de colas MPLS, consulte Colas MPLS.

Para ver las estadísticas de las colas de MPLS, al nivel de sitio, vaya a **Informes** > **Tiempo real** > **Estadísticas de red**. Haga clic en **Colas MPLS**y luego en **Recuperar los datos más recientes**. Los datos más recientes de las colas MPLS se recuperan del dispositivo y se muestran en el Citrix SD-WAN Orchestrator for On-premises.

Puede ver la dirección, el número de paquetes, los paquetes delta y los paquetes DSCP no coincidentes para los servicios de ruta virtual y de intranet.




Para las colas MPLS privadas, puede ver los siguientes detalles:

- **MPLS privado**: El enlace WAN MPLS privado.
- **Cola MPLS**: La cola MPLS asociada al enlace WAN de MPLS.
- **Interfaz de acceso**: La interfaz de acceso asociada a la cola MPLS.
- **Dirección IP**: La dirección IP asociada a la cola MPLS.
- **Dirección de proxy**: La dirección IP del proxy asociada a la cola MPLS.
- **Estado del ARP del proxy**: El estado del protocolo de resolución de direcciones proxy. Habilitado, inhabilitado o N/A
- **MAC**: La dirección MAC de la interfaz asociada a la cola MPLS.
- **Antigüedad de la última respuesta de ARP**: Tiempo en milisegundos en que se recibió la última respuesta de ARP.

Para obtener más información sobre la solución de problemas, consulte Solución de problemas de colas MPLS

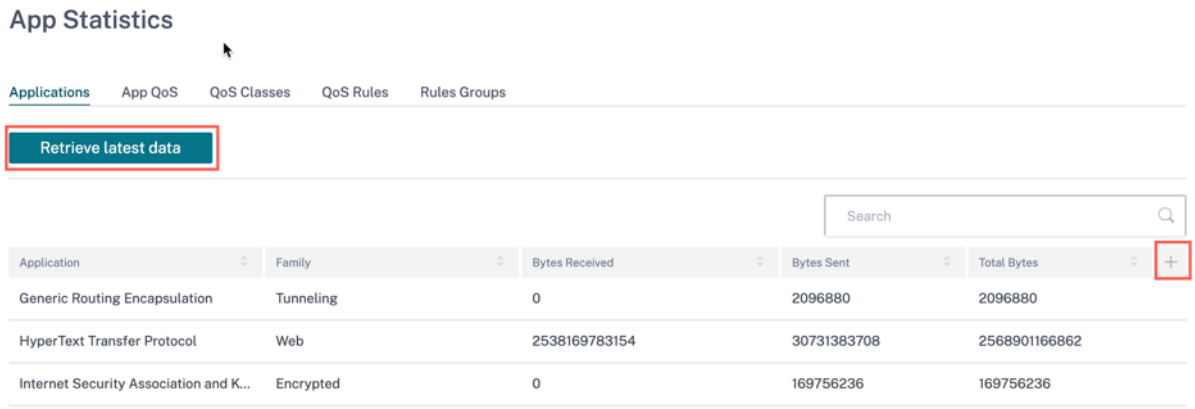
### Estadísticas de la aplicación

Puede obtener la siguiente información estadística en tiempo real en **Informes > Tiempo real > Estadísticas de aplicaciones**:

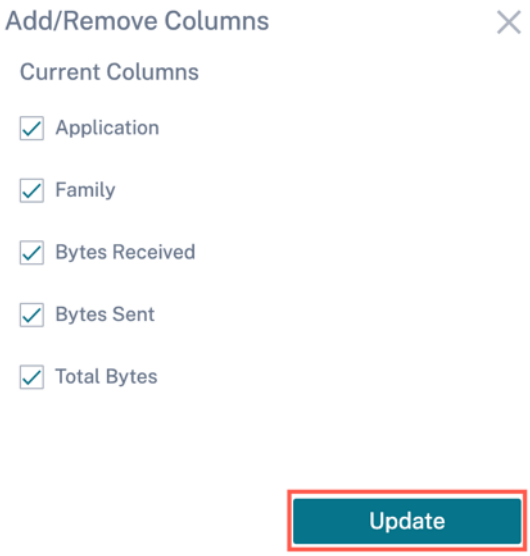
- Aplicaciones
- Protocolos observados
- QoS de aplicaciones
- Clases de QoS
- Reglas de QoS
- Grupos de reglas

Para obtener el informe estadístico en tiempo real, vaya a la ficha correspondiente (como aplicaciones, QoS de la aplicación, regla de QoS) y haga clic en **Recuperar los datos más recientes**.




Haga clic en el símbolo más (+) si quiere agregar o eliminar cualquier columna de la tabla de estadísticas y, a continuación, haga clic en **Actualizar**.



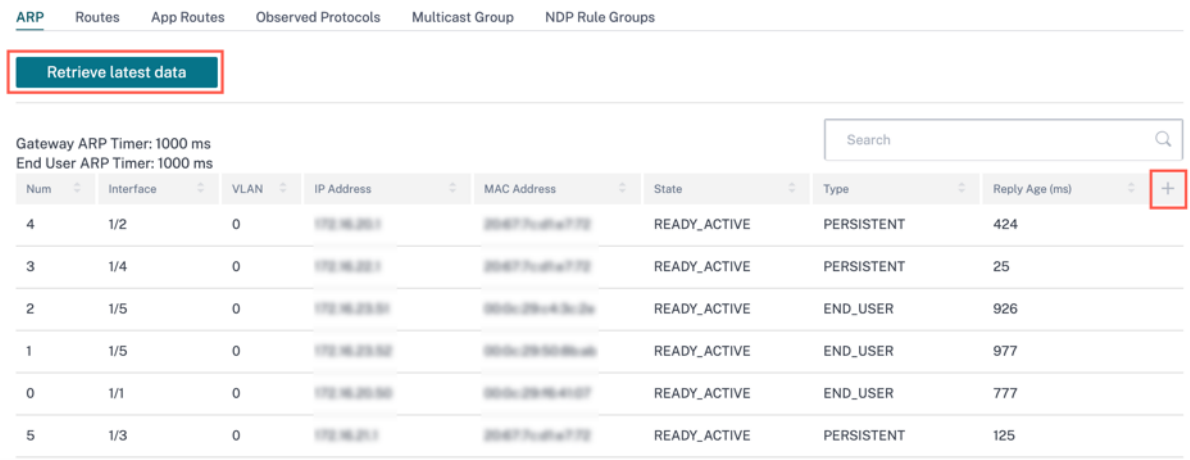

### Estadísticas de rutas

Puede obtener la siguiente información estadística de rutas en tiempo real en **Informes > Tiempo real > Estadísticas de rutas**:

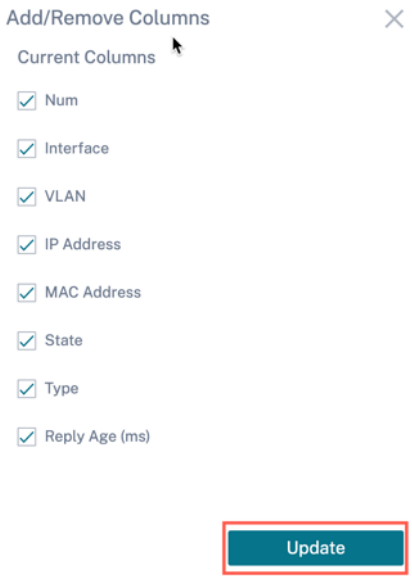
- ARP (Protocolo de resolución de direcciones)
- Rutas
- Rutas de aplicaciones
- Protocolos observados
- Grupo de multidifusión
- Grupos de reglas de NDP

Para obtener el informe estadístico en tiempo real, vaya a la ficha correspondiente (como ARP, Rutas, Rutas de aplicaciones) y haga clic en **Recuperar los datos más recientes**.




Haga clic en el símbolo más (+) si quiere agregar o eliminar cualquier columna de la tabla de estadísticas y, a continuación, haga clic en **Actualizar**.

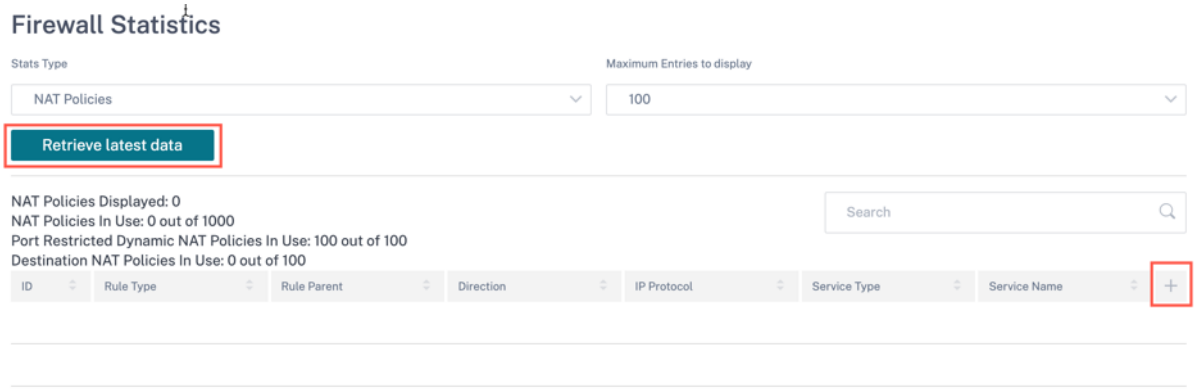



### Estadísticas de firewall

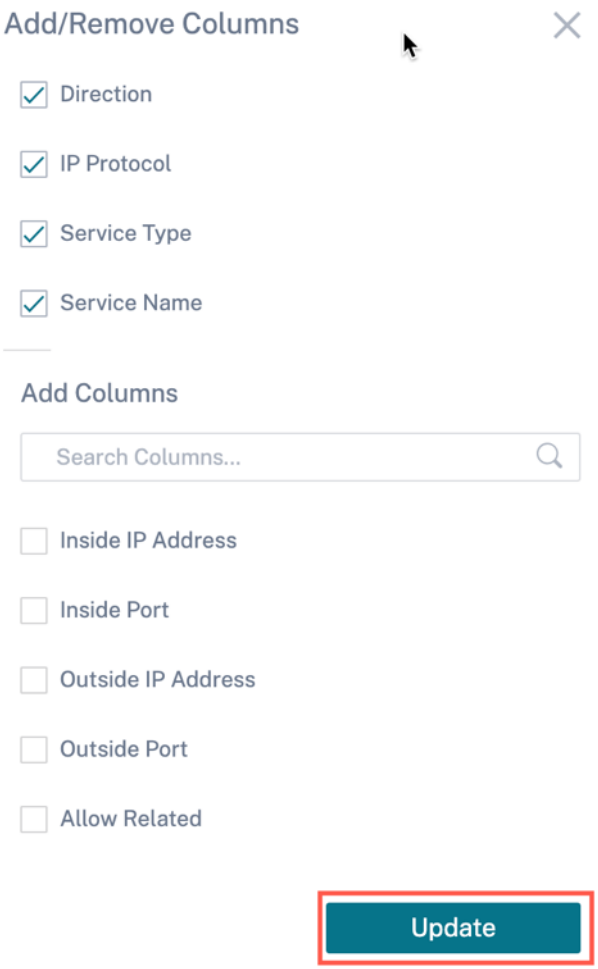
La página de **estadísticas del firewall** proporciona el estado de la conexión, las directivas del Protocolo de direcciones de red (NAT) y las directivas de filtrado relacionadas con una sesión en particular según la acción del firewall configurada. Las conexiones de firewall también proporcionan detalles completos sobre el origen y el destino de la conexión.

Puede obtener la información estadística del firewall en tiempo real en **Informes > Tiempo real > Estadísticas del firewall**. Seleccione el tipo de estadísticas de la lista desplegable (conexión, directivas de NAT, directivas de filtro). Seleccione el número máximo de entradas que quiere mostrar y haga clic en **Recuperar los datos más recientes**.



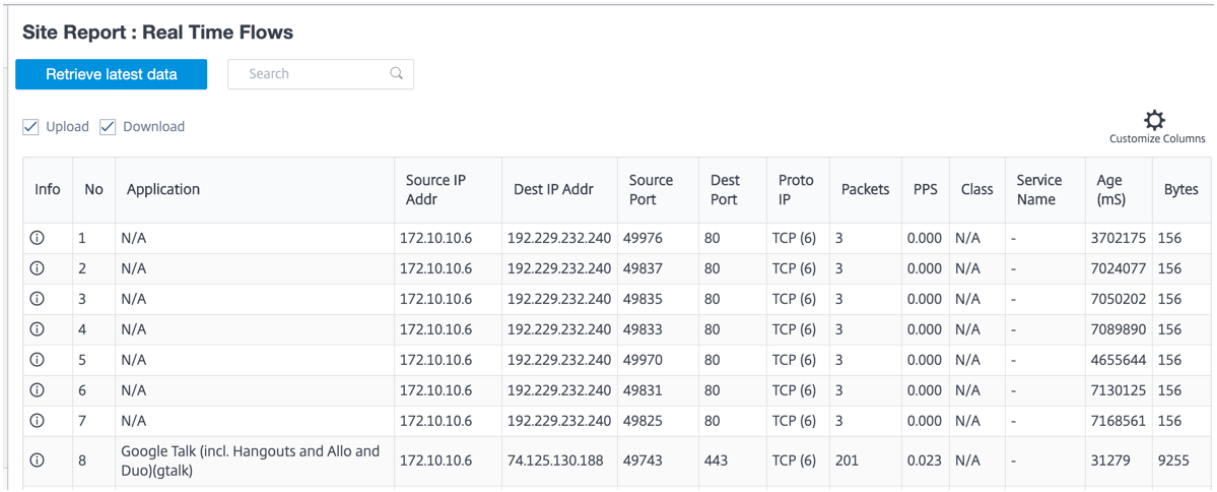

Haga clic en el símbolo más (+) si quiere agregar o eliminar cualquier columna de la tabla de estadísticas y, a continuación, haga clic en **Actualizar**.



### Flujos

La función **Flujos** proporciona información de flujo unidireccional relacionada con una sesión concreta que pasa por el dispositivo. Esto proporciona información sobre el tipo de servicio de destino en el que cae el flujo y también la información relacionada con la regla y el tipo de clase, así como el modo de transmisión.




| Info | No | Application | Source IP Addr | Dest IP Addr | Source Port | Dest Port | Proto IP | Packets | PPS | Class | Service Name | Age (mS) | Bytes |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ⓘ | 1 | N/A | 172.10.10.6 | 192.229.232.240 | 49976 | 80 | TCP (6) | 3 | 0.000 | N/A | - | 3702175 | 156 |
| ⓘ | 2 | N/A | 172.10.10.6 | 192.229.232.240 | 49837 | 80 | TCP (6) | 3 | 0.000 | N/A | - | 7024077 | 156 |
| ⓘ | 3 | N/A | 172.10.10.6 | 192.229.232.240 | 49835 | 80 | TCP (6) | 3 | 0.000 | N/A | - | 7050202 | 156 |
| ⓘ | 4 | N/A | 172.10.10.6 | 192.229.232.240 | 49833 | 80 | TCP (6) | 3 | 0.000 | N/A | - | 7089890 | 156 |
| ⓘ | 5 | N/A | 172.10.10.6 | 192.229.232.240 | 49970 | 80 | TCP (6) | 3 | 0.000 | N/A | - | 4655644 | 156 |
| ⓘ | 6 | N/A | 172.10.10.6 | 192.229.232.240 | 49831 | 80 | TCP (6) | 3 | 0.000 | N/A | - | 7130125 | 156 |
| ⓘ | 7 | N/A | 172.10.10.6 | 192.229.232.240 | 49825 | 80 | TCP (6) | 3 | 0.000 | N/A | - | 7168561 | 156 |
| ⓘ | 8 | Google Talk (incl. Hangouts and Allo and Duo)(gtalk) | 172.10.10.6 | 74.125.130.188 | 49743 | 443 | TCP (6) | 201 | 0.023 | N/A | - | 31279 | 9255 |

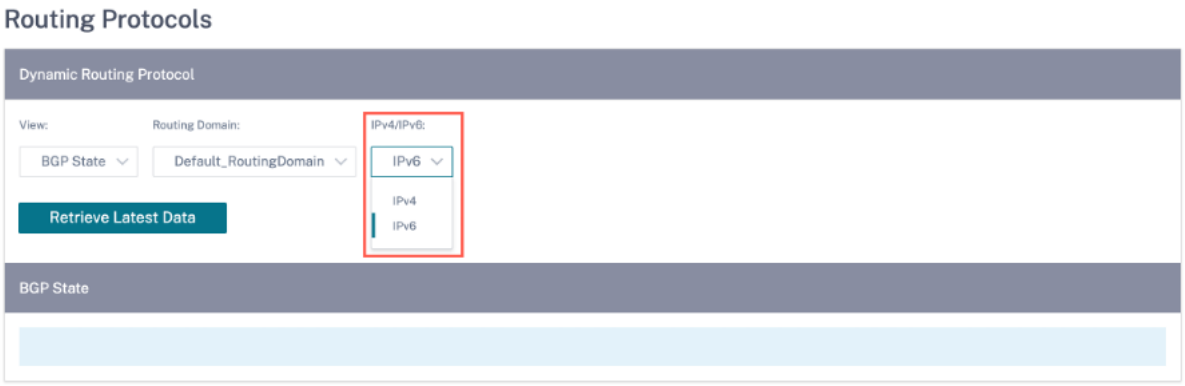
### Protocolos de enrutamiento

El informe de protocolos de enrutamiento proporciona los detalles de los parámetros asociados a los protocolos de enrutamiento. Elija un protocolo de la lista desplegable **Ver** y un dominio de enrutamiento de la lista desplegable **Dominio de enrutamiento**. Haga clic en **Recuperar datos más recientes** para ver los datos actuales.

Puede ver los detalles de los parámetros asociados a lo siguiente:

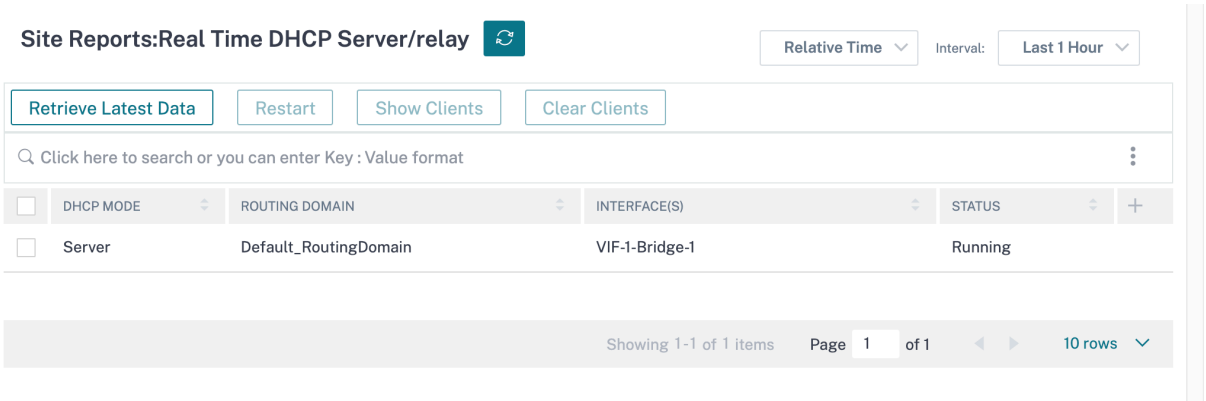
- Estado de BGP
- Estado de OSPF
- Topología OSPF
- Interfaz OSPF
- OSPF LSADB
- Vecinos de OSPF
- Tabla de rutas



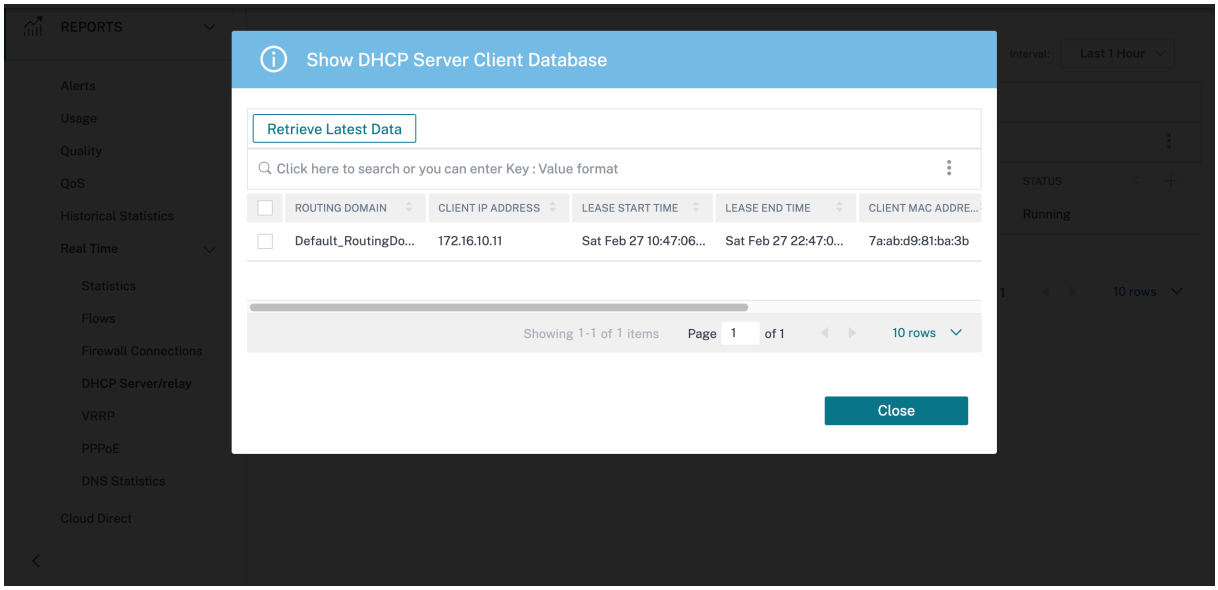

### Servidor DHCP y retransmisión

El informe **Servidor/Relay DHCP** proporciona la información sobre las interfaces configuradas como servidor o retransmisión DHCP y su dominio y estado de enrutamiento asociados. Puede buscar la información de retransmisión o servidor DHCP requerida mediante el formato **Clave: Valor**.

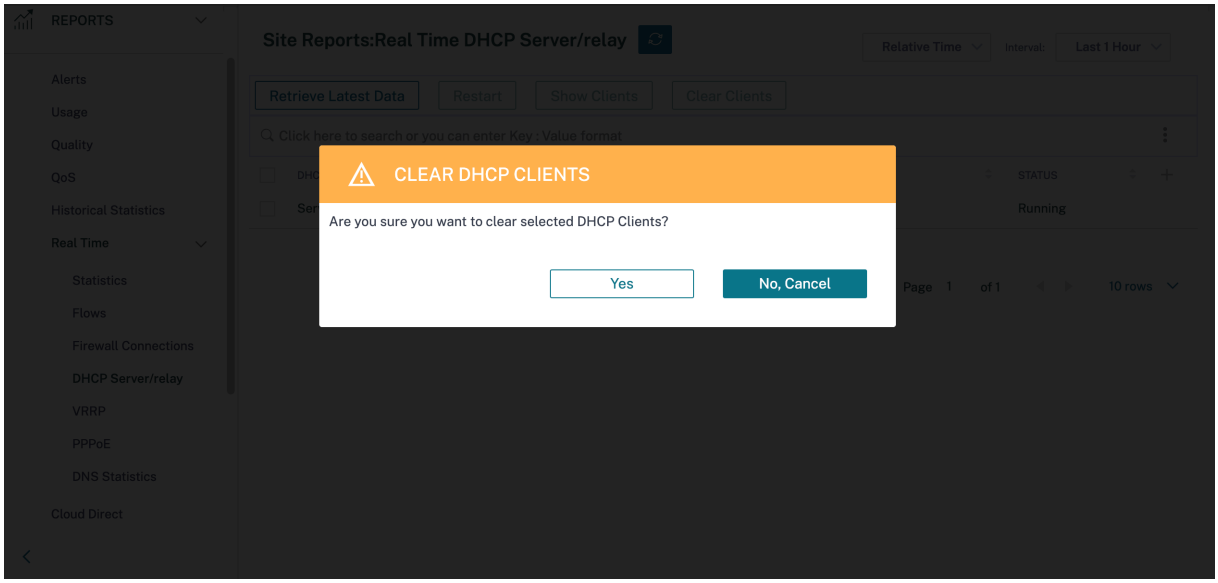



Si el modo es **Servidor**, puede hacer clic en **Mostrar clientes** y ver la lista de clientes DHCP asociados al servidor DHCP.

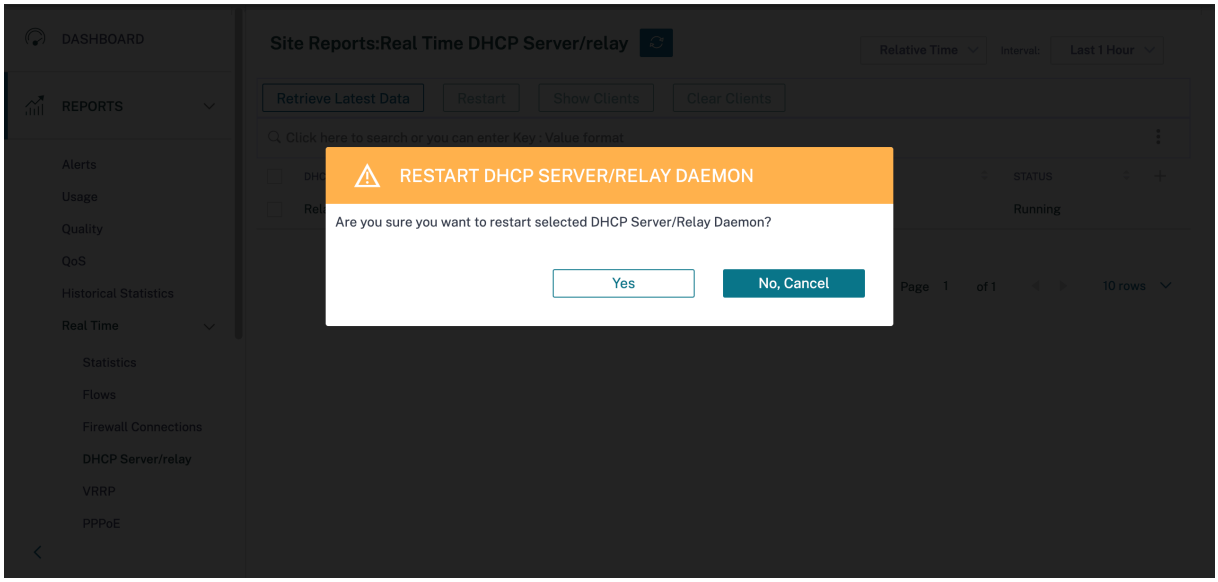



Haga clic en **Borrar clientes** para eliminar los clientes DHCP que están asociados actualmente al servidor DHCP.




Haga clic en **Reiniciar** para reiniciar el servidor DHCP o el relé.

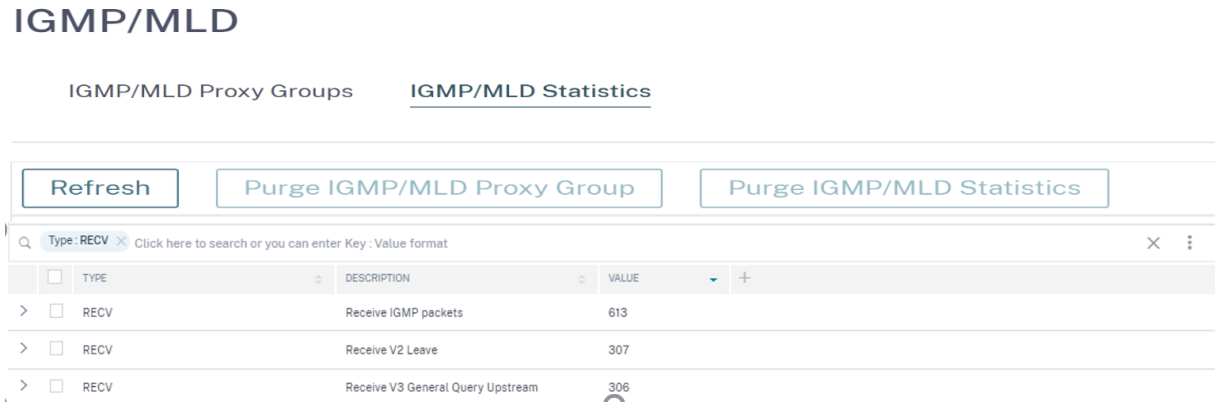
 




### IGMP/MLD

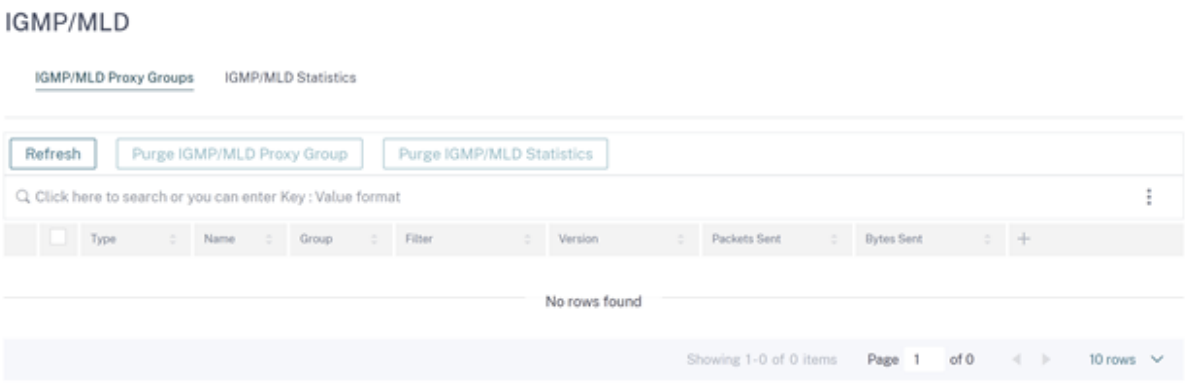
Cuando los receptores de multidifusión inician una solicitud de unión a un grupo, puede ver los detalles del receptor en **Informes** > **Tiempo real** > **IGMP/MLD** > **Estadísticas de IGMP/MLD**. Puede ver esta información tanto en el origen como en el destino. Haga clic en **Actualizar** para obtener los datos actuales.

La siguiente imagen muestra que los paquetes IGMP recibidos y el tipo de filtro RECV se utilizan para incluir los paquetes de recepción IGMP.




Para ver los detalles de los grupos de proxy IGMP, vaya a **Informes** > **Tiempo real** > **IGMP/MLD** > **Grupos de proxy IGMP/MLD**. Haga clic en **Actualizar** para obtener los datos actuales.

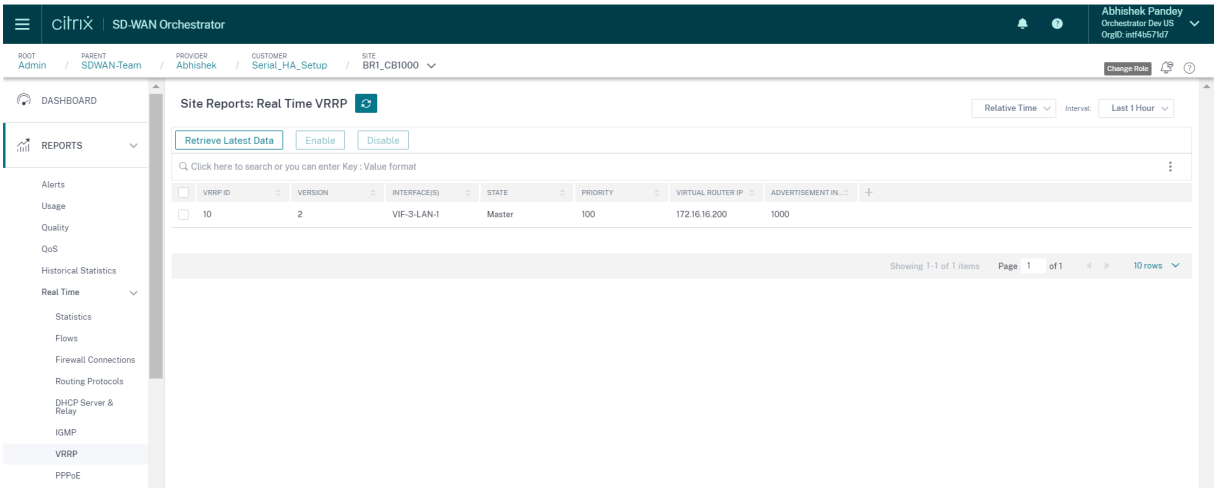



Seleccione **Purgar estadísticas de IGMP/MLD** para eliminar los datos estadísticos de IGMP de la tabla de estadísticas de IGMP.

Seleccione **Purgar grupos IGMP/MLD** para eliminar los datos del grupo IGMP de la tabla de grupos IGMP.

### VRRP

El informe de VRRP en tiempo real proporciona detalles sobre los grupos de VRRP configurados. Para ver el informe del Protocolo de redundancia de enrutador virtual (VRRP), vaya a **Informes** > **Tiempo real** > **VRRP**. Haga clic en **Recuperar datos más recientes** para obtener los datos actuales.




### PPPoE

El informe PPPoE proporciona información de estado de la interfaz virtual configurada con el modo de cliente dinámico o estático de PPPoE. Le permite iniciar o detener manualmente las sesiones para solucionar problemas.

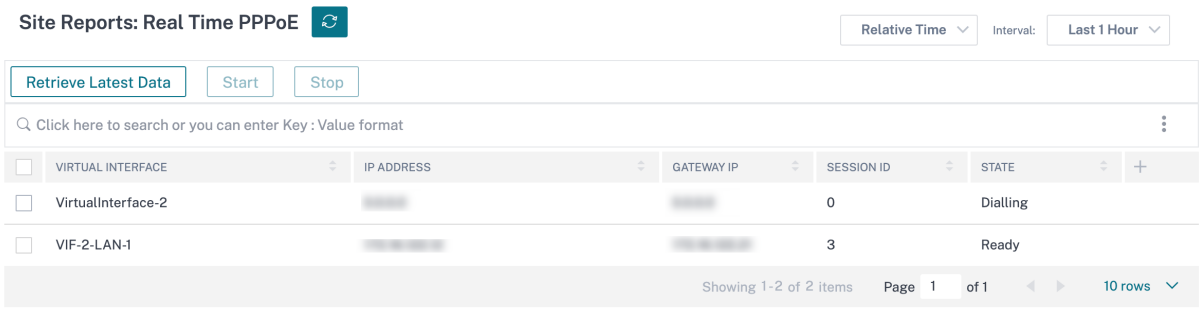
- **Interfaz virtual**: La interfaz virtual asociada a PPPoE.

- **Dirección IP**: La dirección IP asociada a la interfaz virtual. Si la interfaz virtual está activa y lista, muestra los valores recibidos recientemente. Si la interfaz virtual se detiene o se encuentra en estado de error, muestra los últimos valores recibidos.
- **IP de puerta**de enlace: La dirección IP asociada a la puerta de enlace. Si la interfaz virtual está activa y lista, muestra los valores recibidos recientemente. Si la interfaz virtual se detiene o se encuentra en estado de error, muestra los últimos valores recibidos.
- **ID de sesión**: El identificador único asociado a la sesión PPPoE.
- **Estado**: La columna **Estado** muestra el estado de la sesión PPPoE. En la tabla siguiente se describen los estados y las descripciones.

| Tipo de sesión PPPoE | Descripción |
|---|---|
| Configurado | Un VNI está configurado con PPPoE. Este es un estado inicial. |
| Marcación | Después de configurar un VNI, el estado de la sesión PPPoE pasa al estado de marcado iniciando el descubrimiento de PPPoE. Se captura la información del paquete. |
| La función de persistencia | El VNI pasa del estado de detección al estado de sesión, en espera de recibir la IP, si es dinámico o en espera del acuse de recibo del servidor para la IP anunciada, si es estática. |
| Listo | Se reciben paquetes IP y el VNI y el enlace WAN asociado están listos para su uso. |
| Error | La sesión PPP/PPPoE ha finalizado. El motivo del error puede deberse a una configuración no válida o a un error fatal. La sesión intenta volver a conectarse después de 30 segundos. |
| Detenido | La sesión PPP/PPPoE se detiene manualmente. |
| Terminación | Un estado intermedio que termina por un motivo. Este estado se inicia automáticamente después de cierto tiempo (5 segundos para un error normal o 30 segundos para un error grave). |
| Inhabilitado | El servicio SD-WAN está inhabilitado. |

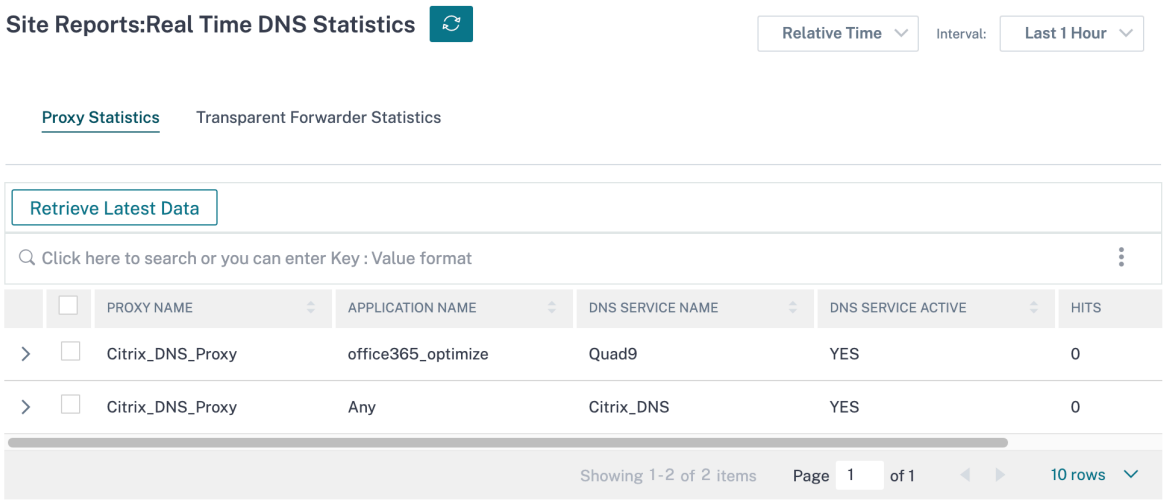
 




### Estadísticas de DNS

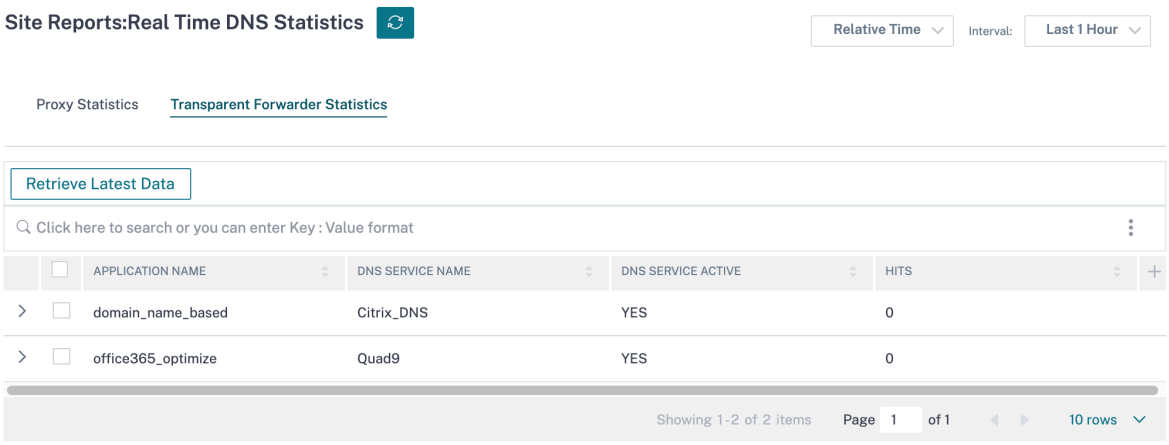
Las **estadísticas de DNS** proporcionan la información sobre el nombre de la aplicación, el nombre del servicio DNS, el estado del servicio DNS y la cantidad de `hits` del servicio DNS. La información del proxy DNS y del reenviador transparente de DNS se muestra en dos fichas diferentes.

Estadísticas de proxy




Estadísticas transparentes del transitario



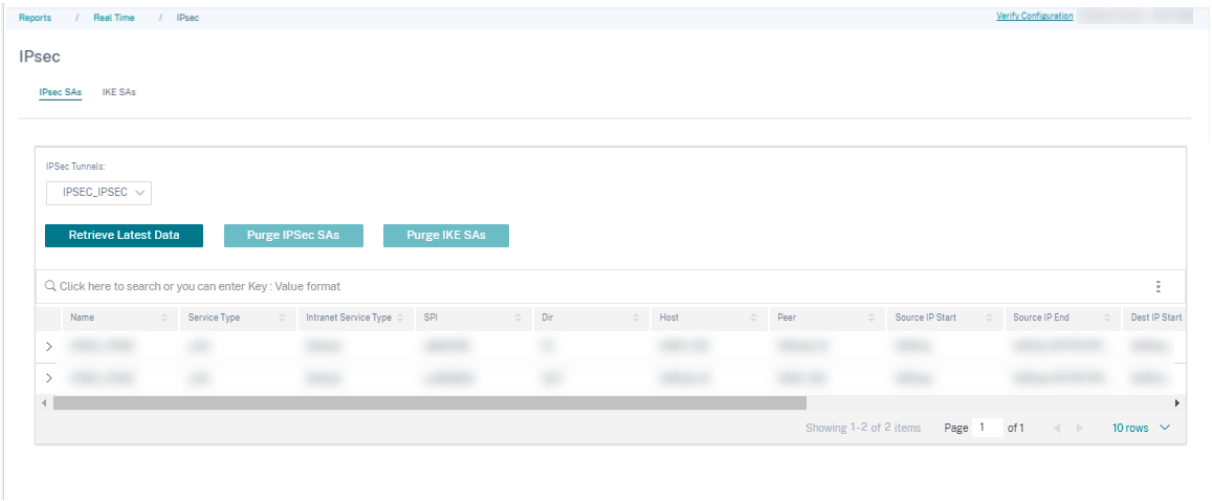

### IPsec

El informe de IPSec en tiempo real proporciona detalles sobre la configuración del túnel IPSec en la red.

Para ver los detalles de las asociaciones de seguridad de IPSec (SA de IPSec), vaya a **Informes** > **Tiempo real** > **IPSec** > **SA de IPSec**. Haga clic en **Recuperar los datos más recientes** para obtener los datos actuales.

Para ver los detalles de las asociaciones de seguridad de intercambio de claves de Internet (SA IKE), vaya a **Informes** > **Tiempo real** > **IPSec** > **SA IKE**. Haga clic en **Recuperar los datos más recientes** para obtener los datos actuales.

También puede purgar los datos del grupo IPSec y los datos estadísticos seleccionando **Purgar grupo IPsec** y **Purgar estadísticas de IKE**, respectivamente.



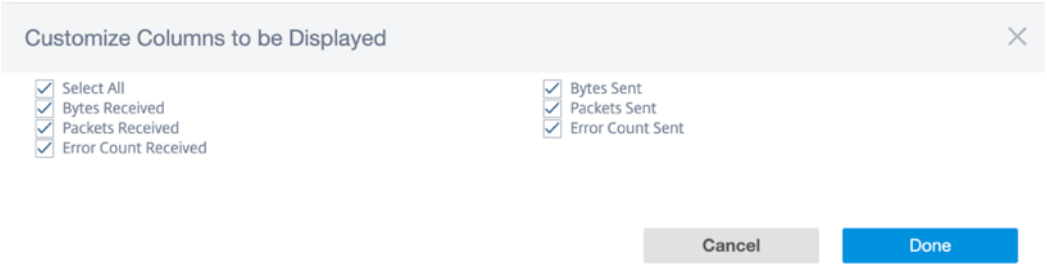

 

## Informes del dispositivo (Vista previa)

Los informes del dispositivo proporcionan el tráfico de red y los informes de uso del sistema. Con estos datos, puede solucionar problemas de red o analizar el comportamiento de sus dispositivos Citrix SD-WAN. Puede ver las siguientes fichas en la página Informes del equipo:

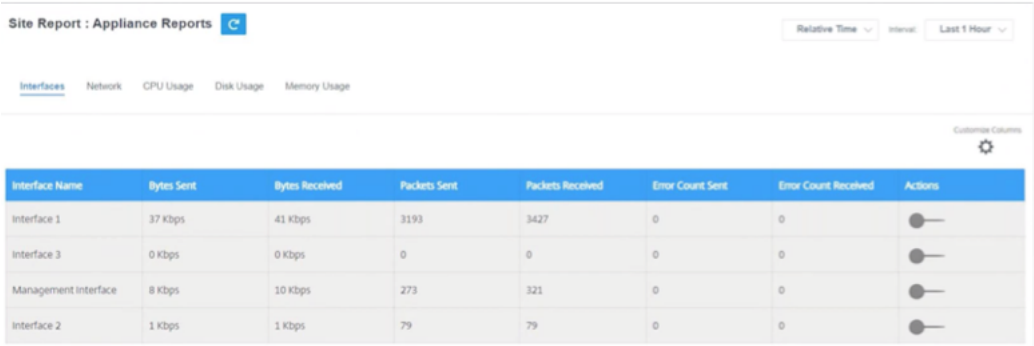
- Interfaz
- Red
- Uso de CPU
- Uso del disco
- Uso de memoria

Haga clic en cada ficha para ver o supervisar el gráfico del dispositivo por hora, día, semanal y mensual. Puede alternar entre Tiempo Absoluto y Relativo según sea necesario. Las columnas de la tabla son personalizables. Haga clic en **Personalizar** la columna en la esquina superior derecha de la tabla y seleccione o deseleccione las opciones que quiere mostrar u ocultar en la tabla.




### Interfaz

La página **de la interfaz** muestra los errores y el tráfico de la interfaz de administración. Toda la red se divide en diferentes interfaces, como Interfaz de Gestión, Interfaz 1/2/3.



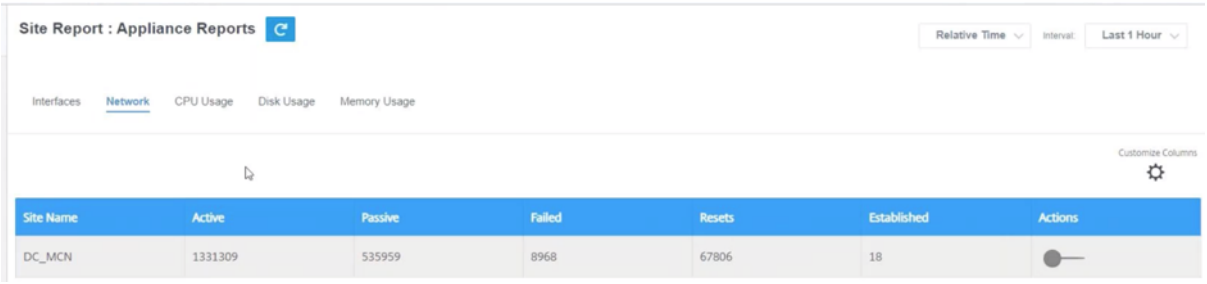

- **Nombre de la interfaz**: Muestra el nombre de la interfaz.
- **Bytes enviados**: Número promedio de bytes enviados durante la duración seleccionada en Kbps.

- **Bytes recibidos**: Número promedio de bytes recibidos durante la duración seleccionada en Kbps.
- **Paquetes enviados**: Número promedio de paquetes enviados durante la duración seleccionada.
- **Paquetes recibidos**: Número promedio de paquetes recibidos durante la duración seleccionada.
- **Recuento de errores enviados**: Número de errores enviados durante la duración seleccionada.
- **Recuento de errores recibido**: Número de errores recibido durante la duración seleccionada.
- **Acciones**: Puede activar el botón de acción para ver el gráfico de la red.

### Red

La página **Red** muestra el número de conexiones TCP para cada sitio configurado.




- **Nombre del sitio**: Muestra el nombre del sitio.
- **Activo**: Número promedio de recuentos de conexiones TCP activas durante la duración seleccionada.
- **Pasivo**: Número promedio de recuentos de conexiones TCP pasivas durante la duración seleccionada.
- **Error**: Número promedio de recuentos de conexiones TCP fallidas durante la duración seleccionada.
- **Restablecer**: Número promedio de recuentos de conexiones TCP restablecidas durante la duración seleccionada.
- **Establecido**: Número promedio de recuentos de conexiones TCP establecidas durante la duración seleccionada.
- **Acciones**: Puede activar el botón de acción para ver el gráfico de la red.

### Uso de CPU

La página **Uso** de la CPU muestra la utilización de la CPU del dispositivo SD-WAN como un porcentaje. El gráfico de CPU muestra el consumo medio de CPU para los intervalos regulares durante el tiempo seleccionado.


- **Nombre del sitio**: Muestra el nombre del sitio.
- **Sistema**: Porcentaje del tiempo total que la CPU dedica a procesar programas del espacio del sistema.
- **Usuarios**: Porcentaje del tiempo total que la CPU dedicó a procesar programas de espacio de usuario.
- **Agradable**: Bueno es cuando la CPU ejecuta una tarea de usuario que tiene una prioridad inferior a la normal.
- **Inactiva**: Porcentaje del tiempo total que la CPU estuvo en modo inactivo.
- **Io Wait**: Porcentaje del tiempo total que la CPU pasó esperando las operaciones de E/S.
- **Irq**: El valor de las solicitudes de interrupción (IRQ) que sirve el núcleo.
- **Robar**: Cuando se ejecuta en un entorno virtualizado, el hipervisor puede robar ciclos destinados a las CPU y dárselos a otra, por diversas razones. Esta vez se conoce como robar.
- **Acciones**: Puede activar el botón de acción para ver el gráfico de la red.

### Uso del disco

La página **Uso del disco** muestra la cantidad de espacio en el disco duro que utilizan el sistema operativo y la partición de datos en un valor de E/S por segundo (IOPS).

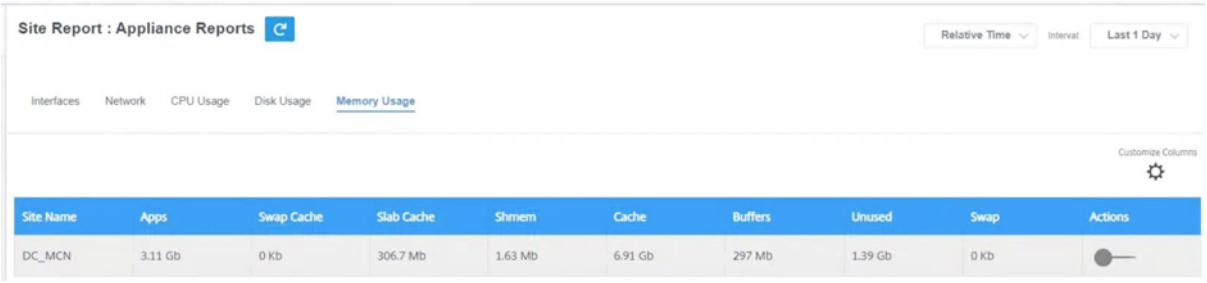

- **Nombre del sitio**: Muestra el nombre del sitio.
- **Nombre del disco**: Muestra el nombre del disco duro.
- **IOPS de lectura**: Muestra el número promedio de IOPS de lectura por segundo durante el período de tiempo seleccionado.
- **IOPS de escritura**: Muestra el número promedio de IOPS de escritura por segundo durante el período de tiempo seleccionado.

- **Latencia**: Muestra el valor de latencia de las solicitudes de lectura y escritura correctas de la carga de trabajo del volumen seleccionado durante el período de tiempo seleccionado. Se recomienda que el valor de latencia inferior a 10 ms sea el mejor para el rendimiento de E/S.
- **Rendimiento de lectura**: Muestra el valor de rendimiento de disco promedio de la operación de lectura del disco durante el tiempo seleccionado en Kbps.
- **Rendimiento de escritura**: Muestra el valor de rendimiento de disco promedio de la operación de escritura en disco durante el tiempo seleccionado en Kbps.
- **Utilización del disco**: Muestra el valor medio de utilización del disco en porcentaje durante el período de tiempo seleccionado.
- **Acciones**: Puede activar el botón de acción para ver el gráfico de la red.

### Uso de memoria

La página **Uso de memoria** muestra el informe de la cantidad de memoria utilizada.



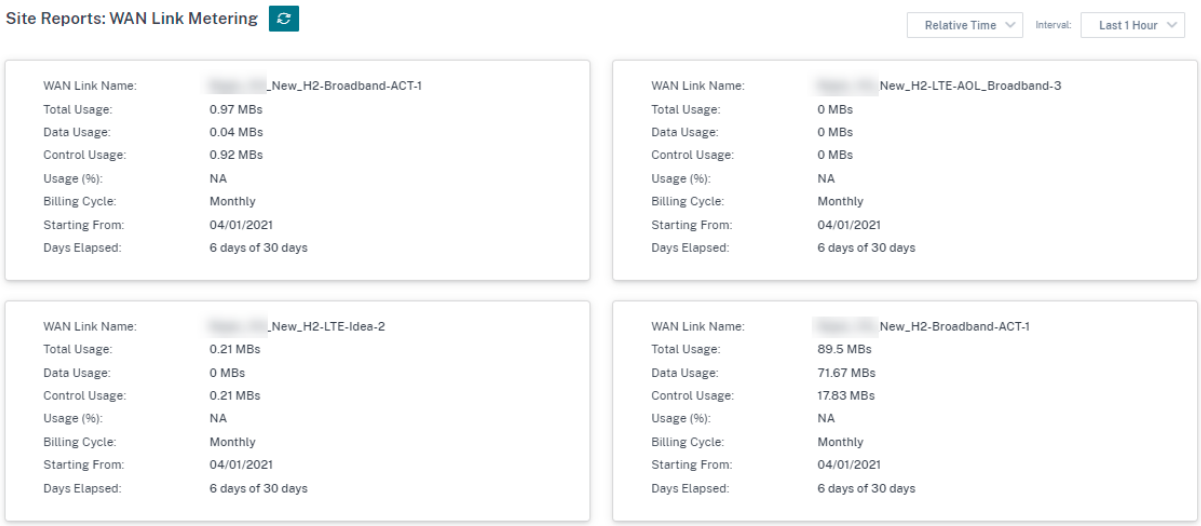

- **Nombre del sitio**: Muestra el nombre del sitio.
- **Aplicaciones**: Muestra el valor de la aplicación utilizada en Gb.
- **Caché de intercambio**: Muestra el número de caché de intercambio en Mb. La caché de intercambio es una lista de entradas de tabla de página con una entrada por página física.
- **Slab Cache**: Muestra el número de bloques de memoria preasignados. En Mb
- **Shmem**: Muestra el valor total de la memoria compartida utilizada en Mb.
- **Caché**: Muestra el número de memorias caché utilizadas en Gb.
- **Búferes**: Muestra el número de memoria física que utiliza la caché de búferes.
- **Sin usar**: Muestra el número de memorias no utilizadas para la memoria caché.
- **Intercambiar**: Muestra el número de espacios de intercambio. El espacio de intercambio se utiliza si necesita alguna extensión de espacio para su memoria física.
- **Acciones**: Puede activar el botón de acción para ver el gráfico de la red.

## Medición de enlaces WAN

Los informes de medición de enlaces WAN proporcionan detalles sobre el uso del enlace WAN medido. Puede ver los informes para obtener información sobre el consumo de datos de los enlaces WAN me-

didos. Para ver los informes de medición de enlaces WAN, vaya a **Informes > Medición de enlaces WAN**.

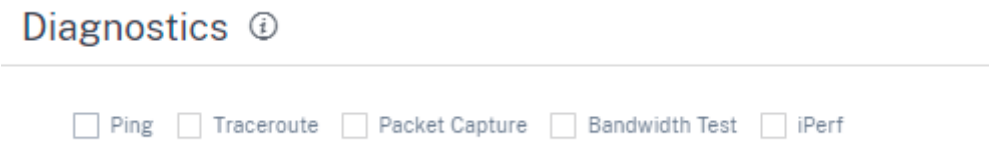



## Diagnóstico

October 31, 2022

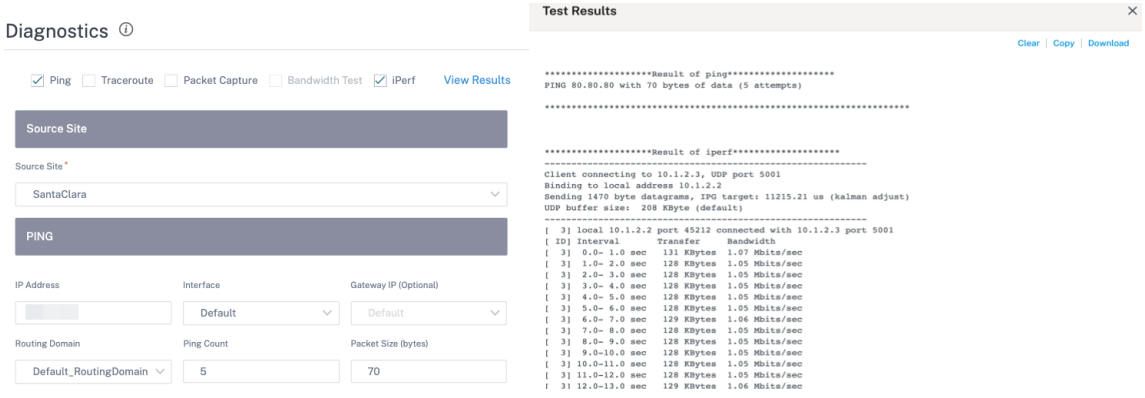
Puede utilizar las utilidades Ping, Traceroute, Packet Capture, Bandwidth test y iPerf para probar e investigar problemas de conectividad de red en su red SD-WAN. Para ver la página de diagnósticos, vaya a **Solución de problemas** > **Diagnóstico**.

Para ver los resultados del diagnóstico, haga clic en **Ver resultados** en la esquina superior derecha de la página de diagnósticos. Puede **descargar**, **copiar**y **borrar** los resultados del informe según sea necesario.

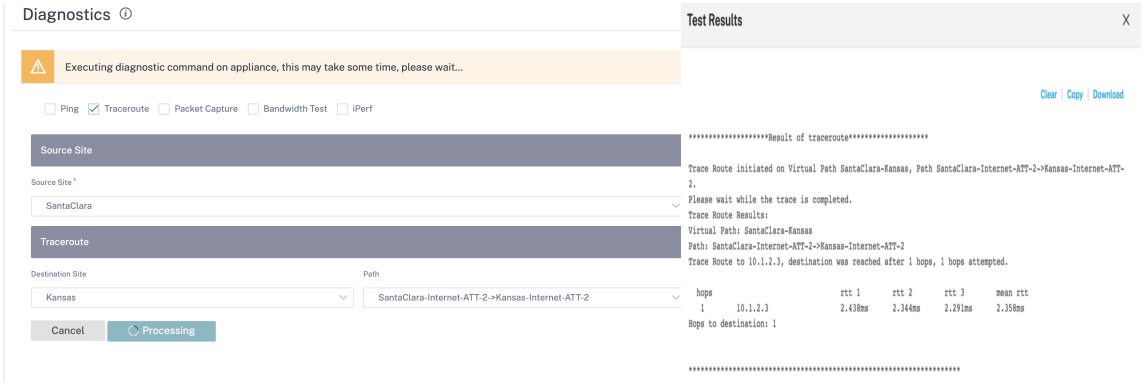



- **Ping**: Puede comprobar la conectividad de la red haciendo ping a un host remoto o a un sitio. Introduzca los detalles de destino, especifique el número de veces que se enviará la solicitud de ping y el número de bytes de datos. Proporcione la **dirección IP** de destino y haga clic en **Ejecutar**.

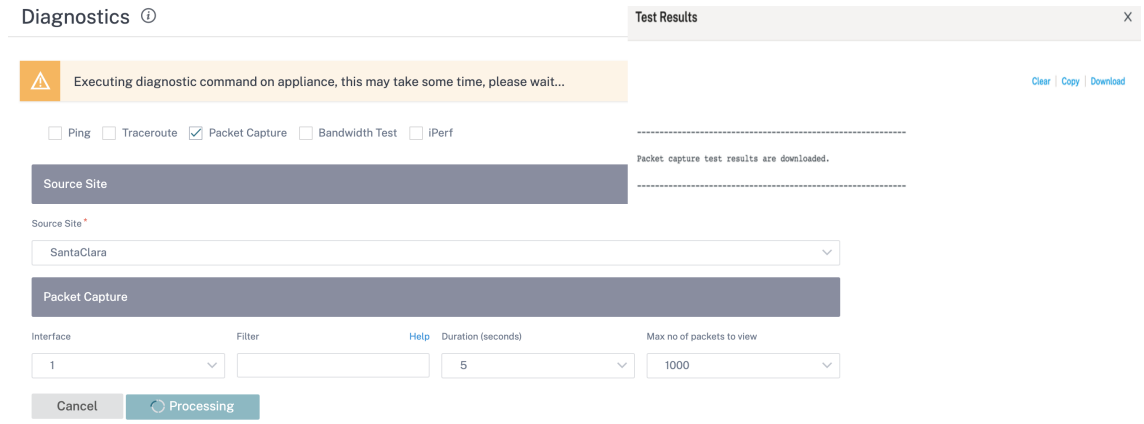
 




- **Traceroute**: Puede trazar la ruta y el número de saltos entre los sitios. Seleccione el sitio de origen y destino junto con la ruta que quiere rastrear y haga clic en **Ejecutar**.



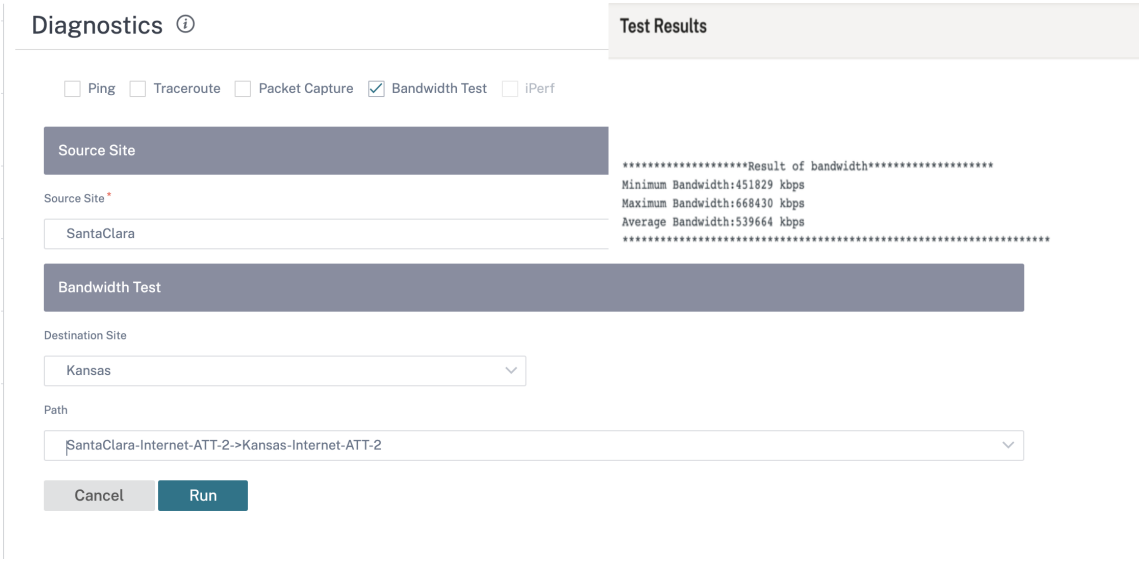

- **Captura de paquetes**: Puede interceptar el paquete de datos que atraviesa la interfaz activa seleccionada presente en el sitio seleccionado. Puede ver los detalles de origen y destino.




La opción **Ayuda** proporciona más detalles sobre las **opciones de filtro**.

- **Prueba de ancho** de banda: Puede ejecutar una prueba de ancho de banda en una ruta específica de un sitio para ver el uso máximo, mínimo y promedio del ancho de banda. Introduzca el sitio de origen, el sitio de destino y seleccione la ruta. Haga clic en **Ejecutar**.

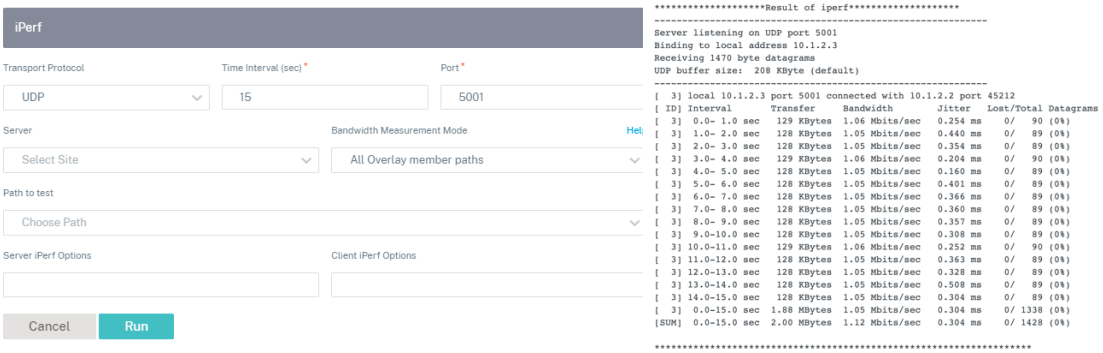
 




- **iPerf**: Puede ejecutar una prueba de iPerf en una ruta específica de un sitio. La herramienta de diagnóstico iPerf se utiliza para generar tráfico de prueba que le permite solucionar problemas de red que podrían provocar:

  - Cambio frecuente en el estado de la ruta de bueno a malo
  - Rendimiento deficiente de la aplicación
  - Mayor pérdida de paquetes

  Para ejecutar una prueba de diagnóstico de iPerf, desde el nivel de cliente, vaya a **Solución de problemas** > **Diagnóstico** y seleccione la casilla de verificación de **iPerf**. Introduzca el protocolo de transporte, el intervalo de tiempo, el número de puerto, el servidor, el modo de medición del ancho de banda, la ruta a probar y las opciones de iPerf del servidor y haga **clic**en



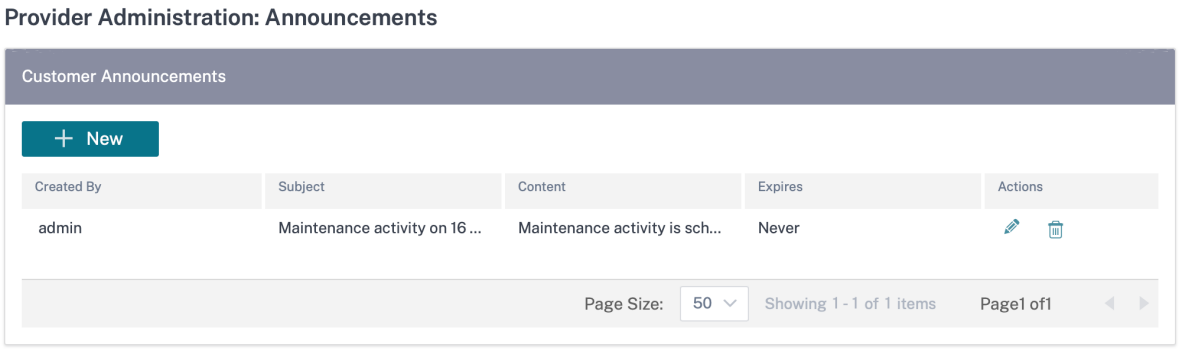

## Anuncios

October 31, 2022

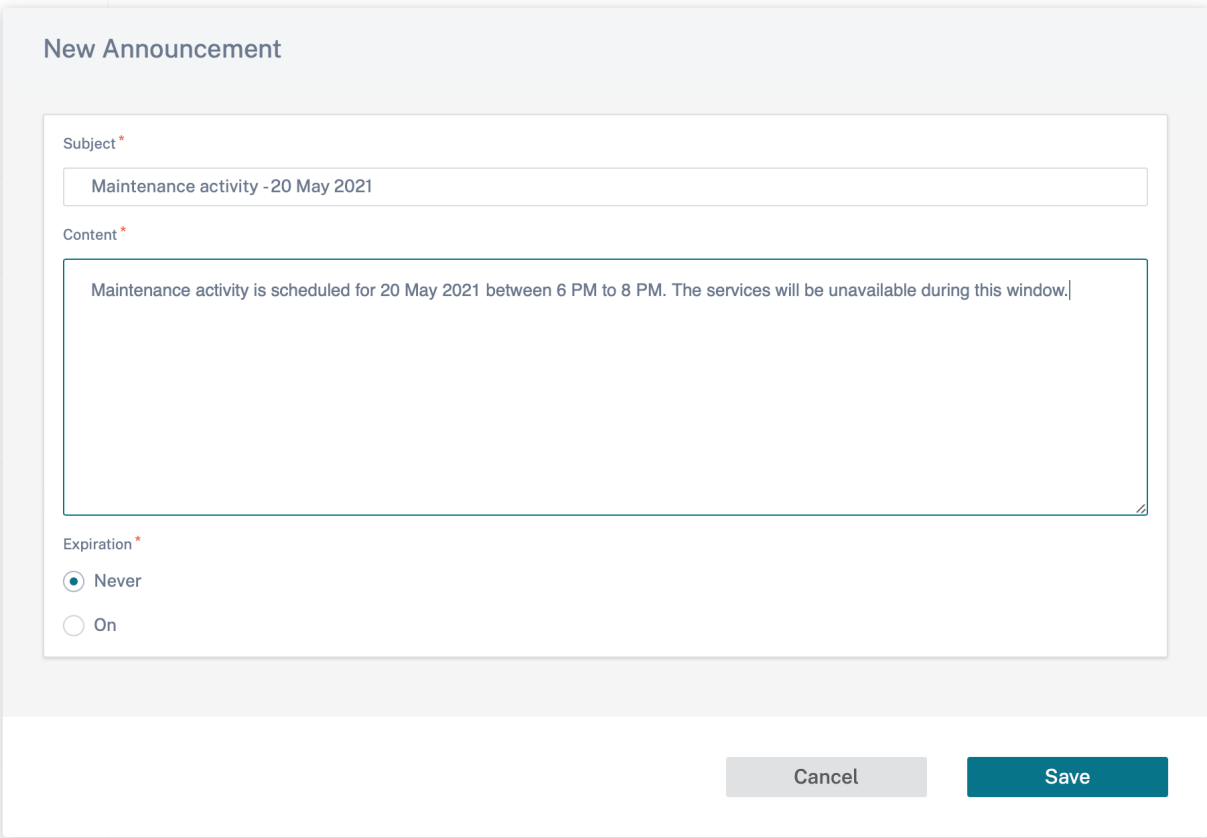
 

Los proveedores pueden usar la opción **Anuncios** para enviar anuncios o notificaciones a sus clientes.

Para crear un anuncio de proveedor, vaya a **Administración > Anuncios** y haga clic en la opción **+ Nuevo**.

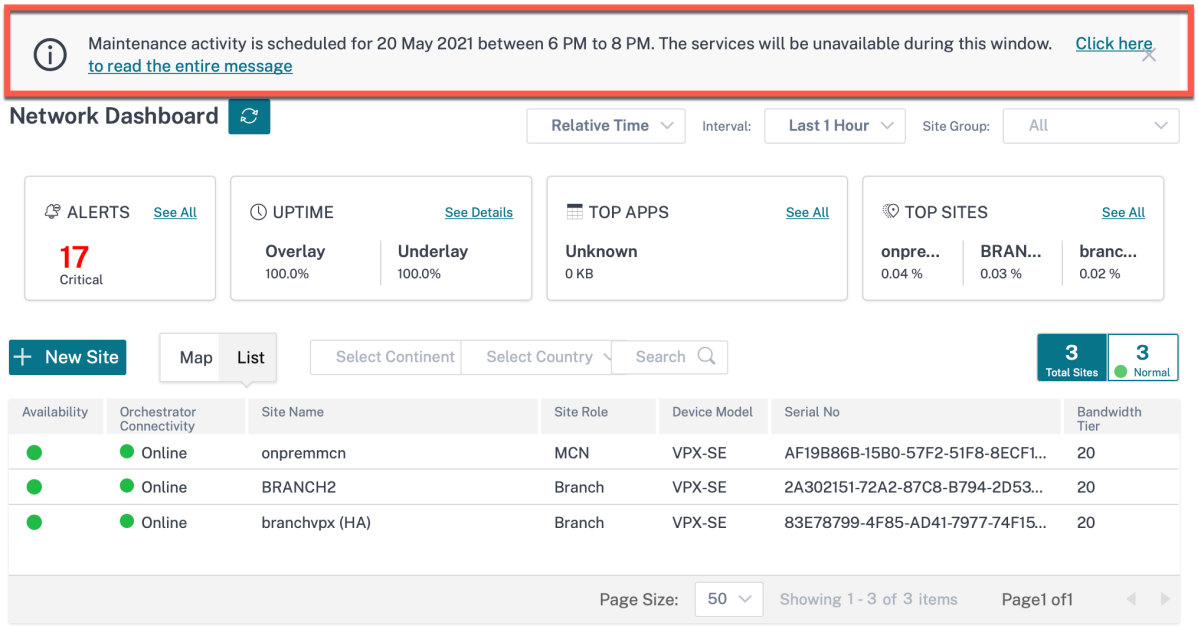



Proporcione una línea de asunto e introduzca contenido en formato HTML o texto sin formato. También puede establecer la caducidad del anuncio.




Los anuncios guardados se muestran a todos los clientes.




# Administración de usuarios

October 2, 2024

Citrix SD-WAN Orchestrator for On-premises admite el control de acceso basado en roles (RBAC). El RBAC regula el acceso a los recursos de SD-WAN Orchestrator según las funciones asignadas a los usuarios individuales. RBAC permite a los usuarios acceder únicamente a los datos que su rol exige y restringe cualquier otro dato.

Un rol define los permisos para ver y realizar diversas actividades en Citrix SD-WAN Orchestrator for On-premises. Puede asignar un rol a un usuario de la lista de funciones predefinidas.

De forma predeterminada, se crea una cuenta de usuario en Citrix SD-WAN Orchestrator for On-premises con el nombre de usuario **admin** y la contraseña configurados como **contraseña**. Se pide al usuario que cambie la contraseña predeterminada durante el inicio de sesión inicial.

Puede agregar usuarios que se puedan autenticar de forma local y remota. Los usuarios que se autentican de forma remota se autentican a través de los servidores de autenticación RADIUS o TACACS+.

## Funciones del proveedor

En la tabla siguiente se enumeran las funciones de proveedor predefinidas.

| Rol del proveedor | Descripción |
|---|---|
| Provider-Master-Admin-All | Un administrador que puede administrar el proveedor y toda la información de sus clientes |
| Provider-Master-Admin-Tenant | Un administrador que puede administrar el proveedor y un subconjunto de la información de sus clientes |
| Provider-Master - Solo lectura - Todo | Un administrador que solo puede ver la información del proveedor y del cliente |
| Provider-Network-Admin (versión preliminar) | Un administrador que solo puede ver y modificar la información relacionada con la red |
| Provider-Security-Admin (versión preliminar) | Un administrador que solo puede ver y modificar la información relacionada con la seguridad |

La función **Provider-Master-Admin-All** puede realizar lo siguiente:

- Asignar roles a usuarios en la red de proveedores y clientes
- Administrar el acceso a los clientes para todos los demás roles de administrador
- Modificar o eliminar roles asignados

### Funciones del cliente

En la siguiente tabla se enumeran las funciones de cliente predefinidas:

| Rol | Descripción |
|---|---|
| Customer-Master-Admin | Un administrador de clientes que puede ver y modificar la información del cliente |
| Customer-Master-ReadOnly-Admin | Un administrador de clientes que solo puede ver la información del cliente |
| Customer-Network-Admin (versión preliminar) | Un administrador de clientes que solo puede ver y modificar información relacionada con la red |
| Customer-Security-Admin (versión preliminar) | Un administrador de clientes que solo puede ver y modificar la información relacionada con la seguridad |

Un usuario con la función **Customer-Master-Admin** puede realizar lo siguiente:

- Agregar usuarios y asignar funciones de clientes
- Modificar o eliminar roles asignados

> **Nota:**
>
> Es importante asignar roles críticos (administrador principal, administrador de seguridad y administrador de red) exclusivamente a usuarios confiables.

### Funciones de soporte

Para solucionar problemas, los clientes pueden asignar funciones de soporte y ofrecer a los miembros del equipo de soporte la posibilidad de ver y modificar su información. Los roles de soporte tienen un período de validez que se define al asignar el rol. Una vez que finaliza el período de validez, el usuario de soporte pierde el acceso a la información del cliente. Sin embargo, los detalles del usuario de soporte siguen apareciendo en **Administración > Administración de usuarios**. Según la necesidad, el administrador del cliente puede eliminar o ampliar la validez de la función de soporte.

| Rol | Descripción |
|---|---|
| Soporte del cliente y lectura de escritura | Un miembro del equipo de soporte que puede ver y modificar la información del cliente |
| Soporte del cliente: Solo lectura | Un miembro del equipo de soporte que solo puede ver la información del cliente |

### Tipos de autenticación

Citrix SD-WAN Orchestrator for On-premises admite los siguientes tipos de autenticación:

- Para cambiar a la autenticación de un solo factor, haga clic en **Autenticación**de La lista desplegable del **tipo de autenticación secundaria** se inhabilita y solo se habilita la lista desplegable del **tipo de autenticación principal**.
- **Autenticación de dos factores (TFA)**: La autenticación de dos factores presenta dos métodos de autenticación para que los usuarios puedan acceder a Citrix SD-WAN Orchestrator for On-premises. Introduce una capa adicional de seguridad en la secuencia de inicio de sesión.

Se admiten los siguientes métodos de autenticación para la autenticación de un solo factor y de dos factores:

- **Local**: Cuando se selecciona, el usuario debe usar la contraseña configurada en Citrix SD-WAN Orchestrator for On-premises para obtener acceso.
- **RADIUS**: Cuando se selecciona, el usuario debe usar la contraseña del servidor RADIUS para obtener acceso.
- **TACACS+**: Cuando se selecciona, los usuarios deben usar la contraseña del servidor TACACS+ para obtener acceso.

En la siguiente tabla se enumeran los métodos de autenticación principales y secundarios compatibles con los usuarios que se autentican localmente:

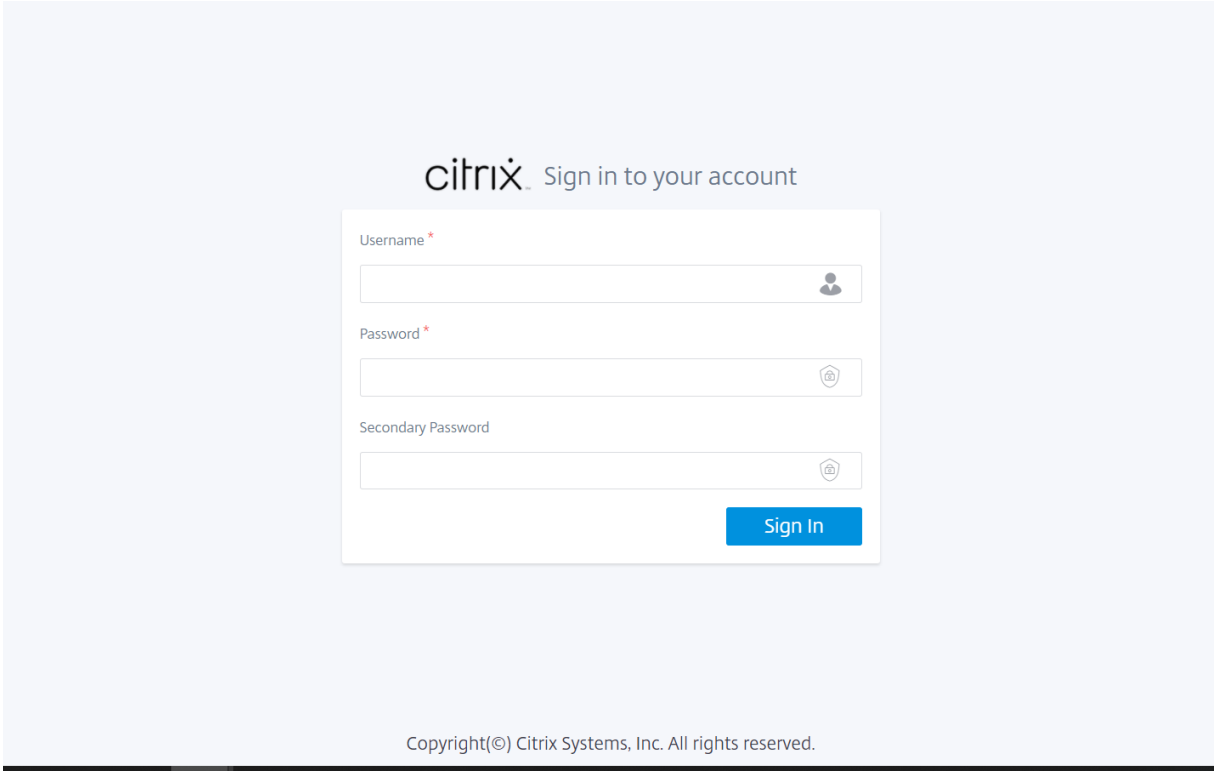
| | Tipo de autenticación principal | Tipo de autenticación secundaria |
|---|---|---|
| **autenticación de un solo factor** | Locales | - |
| **Autenticación de dos factores** | Locales | RADIUS o TACACS+ |

En la siguiente tabla se enumeran los métodos de autenticación principales y secundarios compatibles con los usuarios que se autentican de forma remota:

| | Tipo de autenticación principal | Tipo de autenticación secundaria |
|---|---|---|
| **autenticación de un solo factor** | Local, RADIUS o TACACS+ | - |
| **Autenticación de dos factores** | Local, RADIUS o TACACS+ | RADIUS o TACACS+ |

Si la **autenticación** de dos factores está habilitada y los servidores RADIUS/TACACS+ están configurados como un tipo de autenticación secundario, el campo **Contraseña secundaria** estará visible en la página de inicio de sesión.




### Agregar un usuario

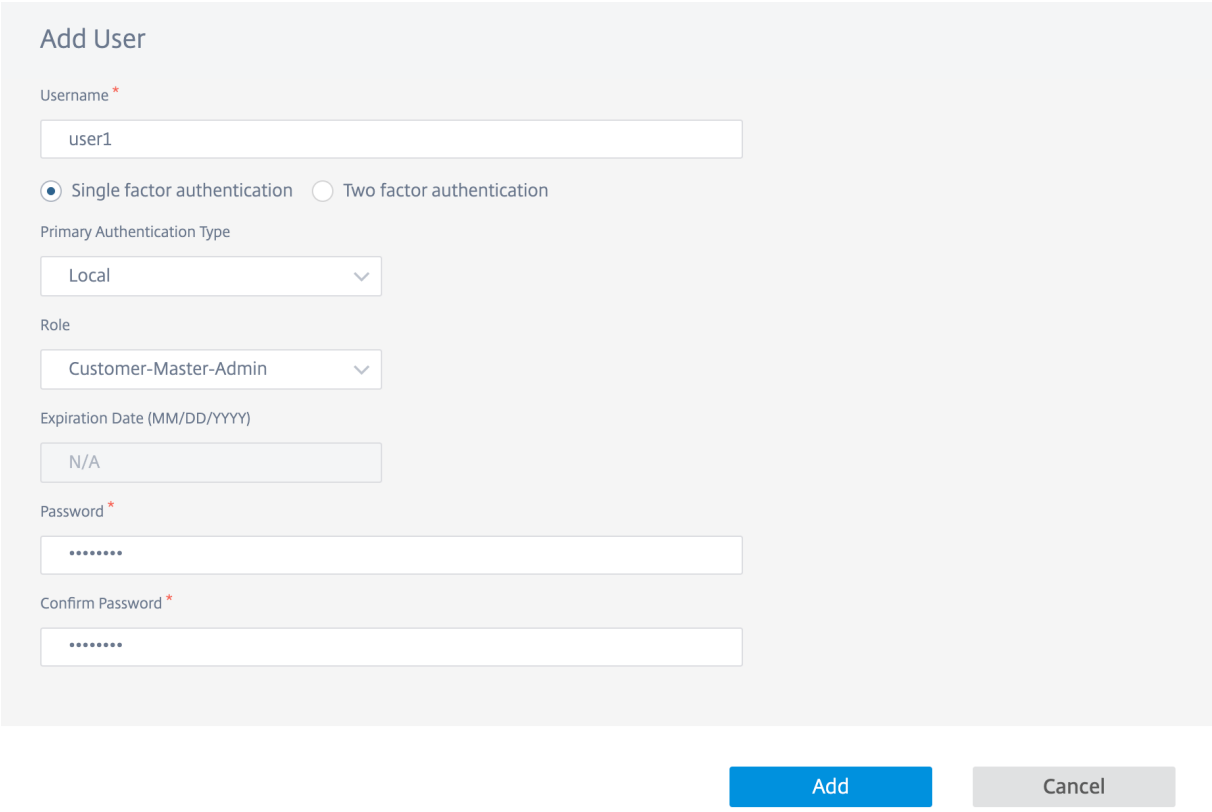
Vaya a **Administración > Administración** de **usuarios** > haga clic en **+ Nuevo** > Introduzca los siguientes detalles > haga clic en **Agregar**.

- Introduzca el nombre de usuario.
- **Autenticación de factor único**: Solo habilita la autenticación principal para iniciar sesión de los usuarios.
- **Autenticación de dos factores**: Permite la autenticación principal y secundaria para iniciar sesión a los usuarios. Para obtener más información, consulte Servidores de autenticación remota.
- **Tipo de autenticación principal**: Seleccione Local o la dirección IP del servidor de autenticación remota.
- **Tipo de autenticación secundaria**: Seleccione la dirección IP del servidor de autenticación remota.

  > **NOTA**
  >
  > El campo **Tipo de autenticación secundaria** aparece atenuado si se selecciona la autenticación de un solo factor.

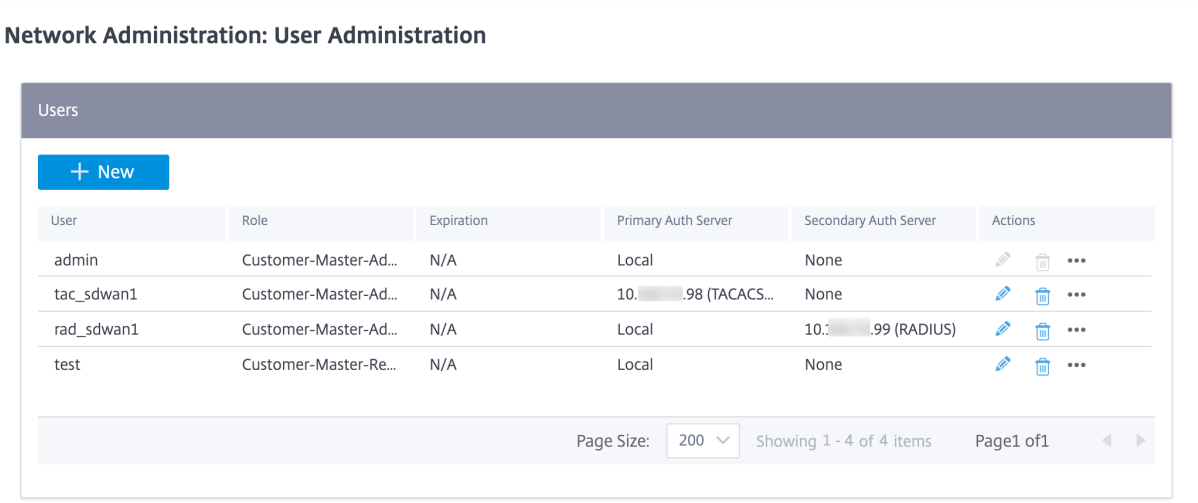
 

- **Función**: Seleccione una función de la lista de funciones disponibles.
- **Denegar el acceso a los clientes**: (Disponible solo al nivel de proveedor). Al agregar usuarios, los proveedores pueden denegar el acceso a clientes específicos.
- **Fecha de caducidad (MM/DD/YYYY)**: fecha hasta la cual el usuario de soporte tiene acceso a la información del cliente. El período de validez predeterminado es de dos semanas a partir de la fecha en que se asigna el rol.
- Introduzca la contraseña. La longitud de la contraseña debe estar entre 8 y 128 caracteres.




Mediante la columna **Acciones**, puede cambiar el rol de usuario, actualizar la contraseña y modificar el tipo de autenticación. También puede eliminar el usuario si es necesario.



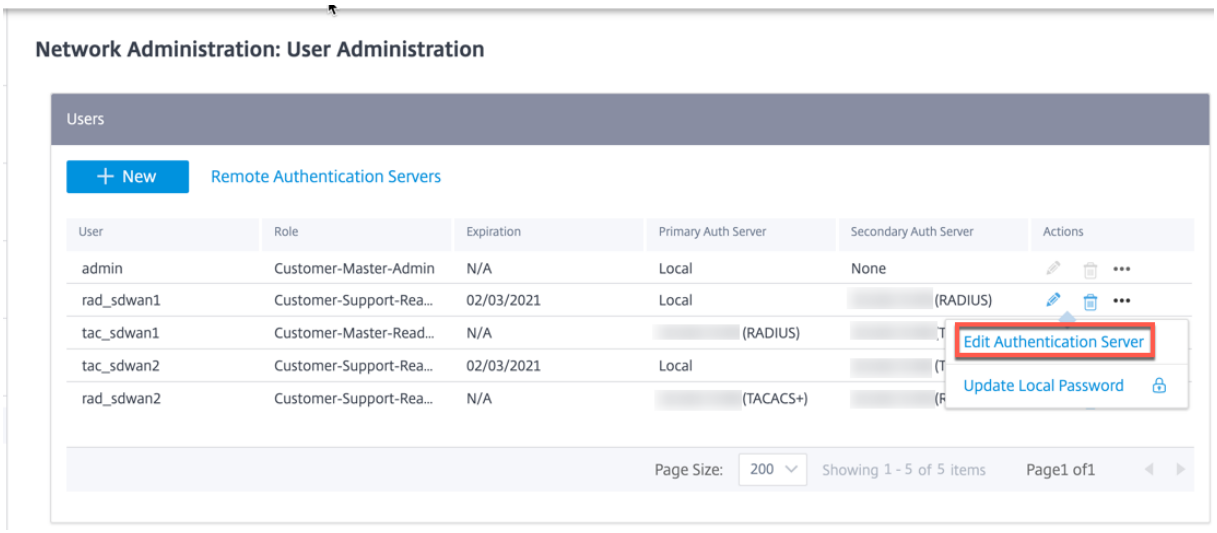

### Limitación

Citrix SD-WAN Orchestrator for On-premises no admite la duplicación de nombres de usuario de un cliente diferente en el mismo proveedor. Cuando se realiza esta acción, aparece el mensaje de error **Error al crear la cuenta**.

## Cambiar el tipo de autenticación

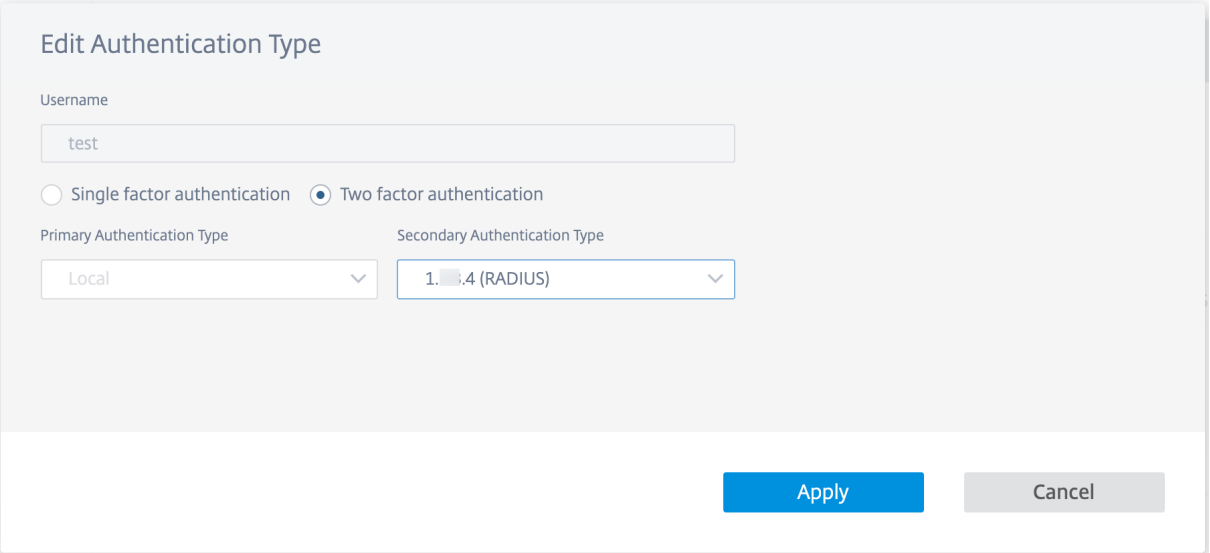
Puede cambiar el tipo de autenticación de un usuario de una autenticación de un solo factor a una autenticación de dos factores y viceversa.

Para cambiar el tipo de autenticación de un usuario, en la columna **Acciones**, haga clic en **...** y, a continuación, en **Modificar servidor de autenticación**.



Si actualmente ha seleccionado **Autenticación de factor único**, puede cambiar a la autenticación de dos factores. Haga clic en **Autenticación de dos factores** y seleccione el servidor remoto en la lista desplegable **Tipo de autenticación secundaria**. Haga clic en **Aplicar**.




Si actualmente ha seleccionado la autenticación de dos factores, puede elegir cambiar solo el tipo de autenticación secundaria o cambiar a la autenticación de factor único.

**Autenticación**de factor único: La autenticación de factor único presenta un método de autenticación para obtener acceso a Citrix SD-WAN Orchestrator for On-premises para los usuarios.

El**tipo de autenticación principal** solo se puede configurar en el momento de la creación del usuario y no se puede modificar más adelante.

### Cambiar contraseña

Puede cambiar la contraseña de los usuarios locales. Para cambiar la contraseña de un usuario, en la columna **Acciones**, haga clic en **...** y **actualice la contraseña local**.

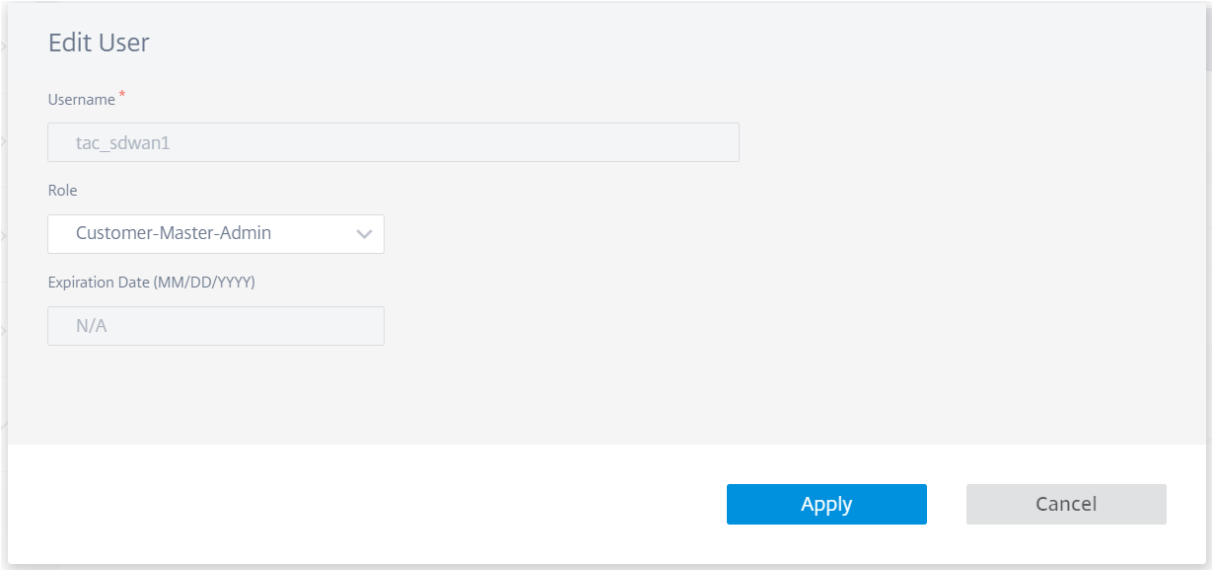
> **NOTA**
>
> Solo puede modificar la contraseña para los usuarios locales. Para los usuarios autenticados de forma remota, debe actualizar la contraseña en el servidor externo.

### Cambiar rol de usuario

Para cambiar el rol del usuario, haga clic en el icono **Modificar** de la columna **Acciones**. Seleccione un **rol** y haga clic en **Aplicar**.

> **NOTA**
>
> No puede modificar el rol del usuario administrador predeterminado.




## Nombre del dominio

October 31, 2022

El nombre de dominio es una URL personalizada que se utiliza en la barra de direcciones para acceder a Citrix SD-WAN Orchestrator for On-premises. El uso del nombre de dominio hace que sea más fácil de recordar y también te permite usar la marca de tu empresa.

Para usar un nombre de dominio, asegúrese de tener un servidor DNS local configurado con un registro DNS que vincule el nombre de dominio a la dirección IP de Citrix SD-WAN Orchestrator para la administración local. Asegúrese de que el nombre de dominio esté configurado durante la configuración inicial. Al configurar un nombre de dominio, los reinicios y certificados de Citrix SD-WAN Orchestrator for On-premises se regeneran automáticamente. Se debe configurar el mismo nombre de dominio en los dispositivos individuales. Para obtener más información, consulte Configuración local de SD-WAN Orchestrator en un dispositivo SD-WAN.

No es obligatorio configurar un nombre de dominio. Si no tiene un nombre de dominio y aún quiere utilizar el servidor DNS para la resolución de direcciones IP, configure registros DNS que apunten a Citrix SD-WAN Orchestrator para IP local para los tres FQDN siguientes:

- sdwanzt.citrixnetworkapi.net
- descargar.citrixnetworkapi.net

- sdwan-home.citrixnetworkapi.net

Por ejemplo, si un dominio de Citrix SD-WAN Orchestrator para locales está configurado como **citrix.com**, debe crear el registro DNS en el servidor DNS para el siguiente FQDN y la dirección IP de Citrix SD-WAN Orchestrator para locales:

- download.citrix.com
- sdwanzt.citrix.com
- sdwan-home.citrix.com

En configuración avanzada:

Por ejemplo: Si un dominio de Citrix SD-WAN Orchestrator for On-premises está configurado como **citrix.com**, el **dominio del servicio de administración de descargas** se configura como **download.citrix.com**y el **dominio del servicio de administración de estadísticas** se configura como **estadísticas. citrix.com**, luego debe crear el registro DNS en el servidor DNS para el siguiente FQDN y la dirección IP correspondiente:

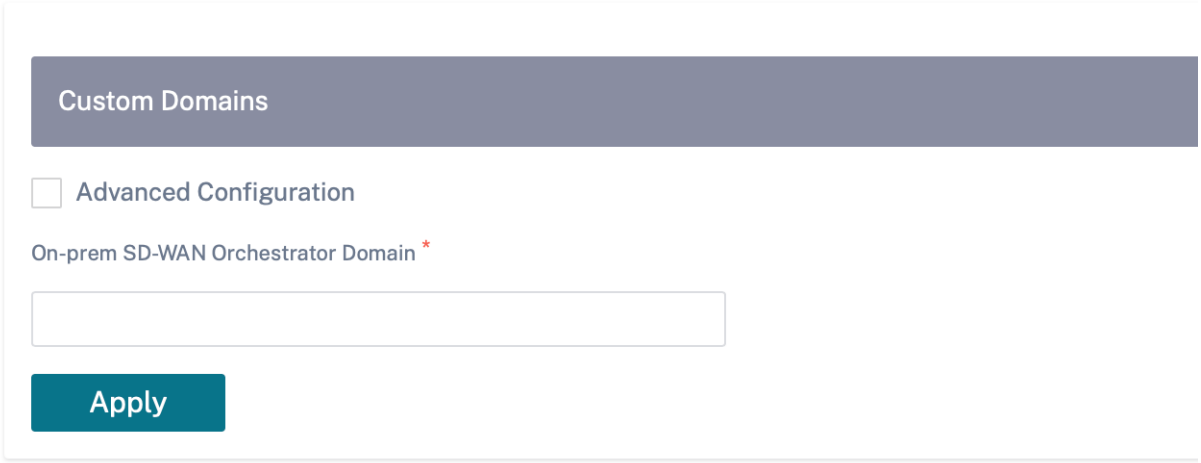
- download.citrix.com
- sdwanzt.citrix.com
- statistics.citrix.com

La configuración o el cambio de un nombre de dominio para una configuración existente afecta a Citrix SD-WAN Orchestrator para la conectividad local y de dispositivos. Debe realizar manualmente el proceso de autenticación por certificado o utilizar la opción de configuración de implementación sin intervención del sitio.

> **Nota**
>
> En una configuración administrada por un proveedor, solo los administradores del proveedor tienen acceso para modificar la información relacionada con el nombre de dominio.

Para configurar un nombre de dominio, al nivel de red, vaya a **Administración > Nombre de dominio y proporcione un nombre** de dominio de Citrix SD-WAN Orchestrator for On-premises.




## Certificado HTTPS

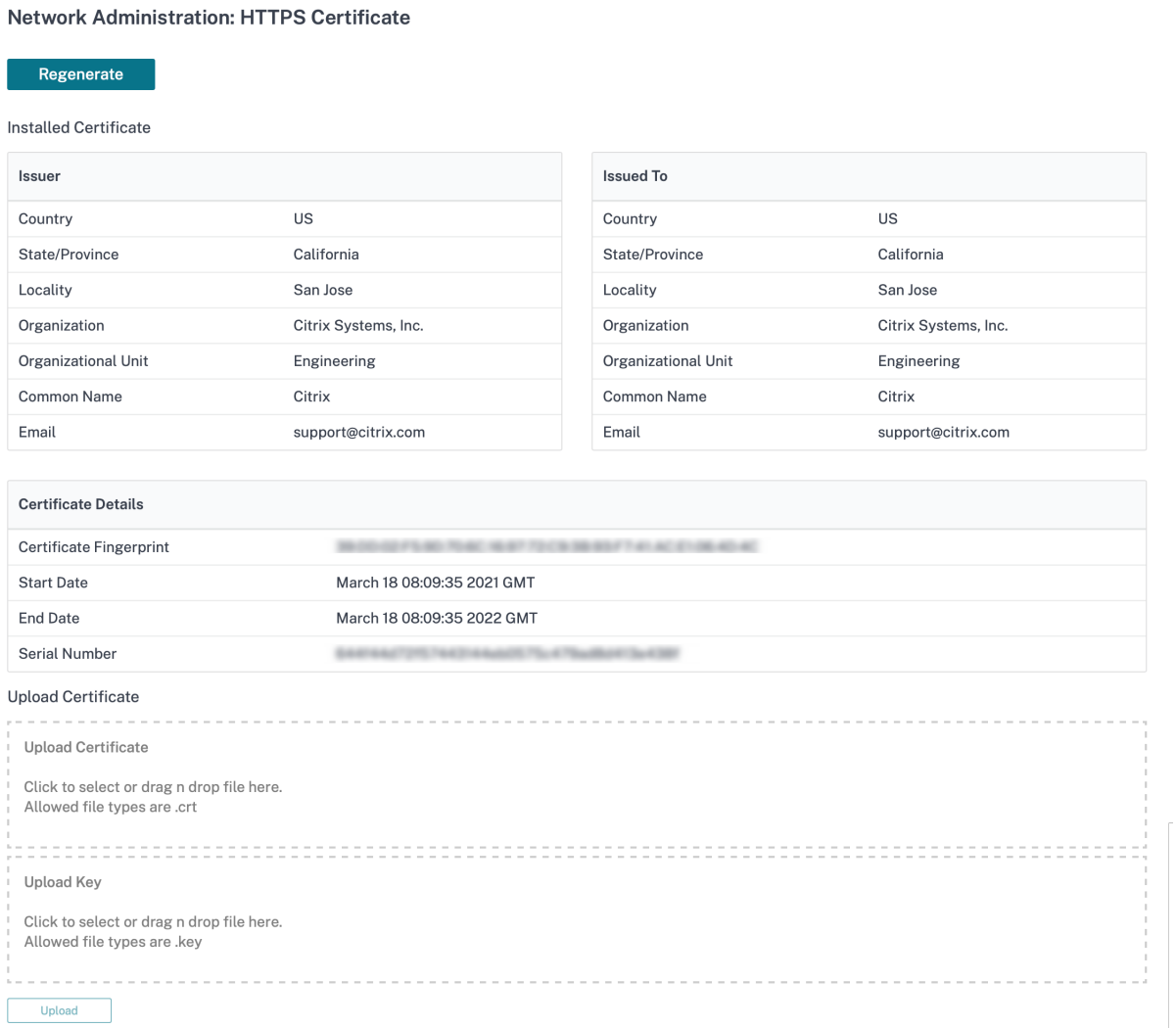
October 31, 2022

Se requiere un certificado HTTPS para establecer una conexión HTTPS de administración segura con Citrix SD-WAN Orchestrator for On-premises. Puede usar el certificado HTTPS predeterminado disponible en la GUI de Citrix SD-WAN Orchestrator for On-premises o cargar un certificado HTTPS personalizado generado a partir de cualquier otro marco, como OpenSSL, o de una autoridad de confianza. El certificado HTTPS personalizado le permite tener control sobre la seguridad y los demás parámetros del tema relacionados con el certificado.

Para ver el certificado predeterminado, vaya a **Administración > Certificado HTTPS**.

> **Nota**
>
> En una configuración administrada por un proveedor, solo los administradores del proveedor tienen acceso para regenerar y cargar el certificado HTTPS.




La sección **Certificado instalado** proporciona un resumen del certificado instalado en el dispositivo. El dispositivo utiliza este certificado para identificarse en la red.

La sección **Emitido a** proporciona detalles sobre a quién se ha emitido el certificado. El **nombre común del** certificado coincide con el nombre del dispositivo, ya que el certificado está vinculado al nombre del dispositivo. En la sección **Emisor se proporcionan los detalles de la entidad emisora** de certificados que firmó el certificado. Los detalles del certificado incluyen la huella digital del certificado, el número de serie y el período de validez del certificado.

Para regenerar el certificado, vaya a **Administración > Certificado HTTPS** y haga clic en **Regenerar**.

> **Nota**
>
> La regeneración del certificado desconecta todas las sesiones HTTPS conectadas existentes y reinicia el servidor HTTPS. Una vez que el certificado se haya regenerado correctamente, la GUI se actualiza automáticamente.

Puede generar certificados HTTPS desde cualquier otro marco, como OpenSSL, o desde una autoridad de confianza y cargarlos en Citrix SD-WAN Orchestrator for On-premises. El formato de certificado admitido es .crt y el formato de clave admitido es .key.

Para cargar un certificado HTTPS personalizado, haga clic en **Cargar** o arrastre el certificado y los archivos clave en los cuadros **Cargar certificado** y **Cargar clave**, respectivamente. Tras la carga correcta, la GUI se actualiza automáticamente.

## Administración del espacio en disco

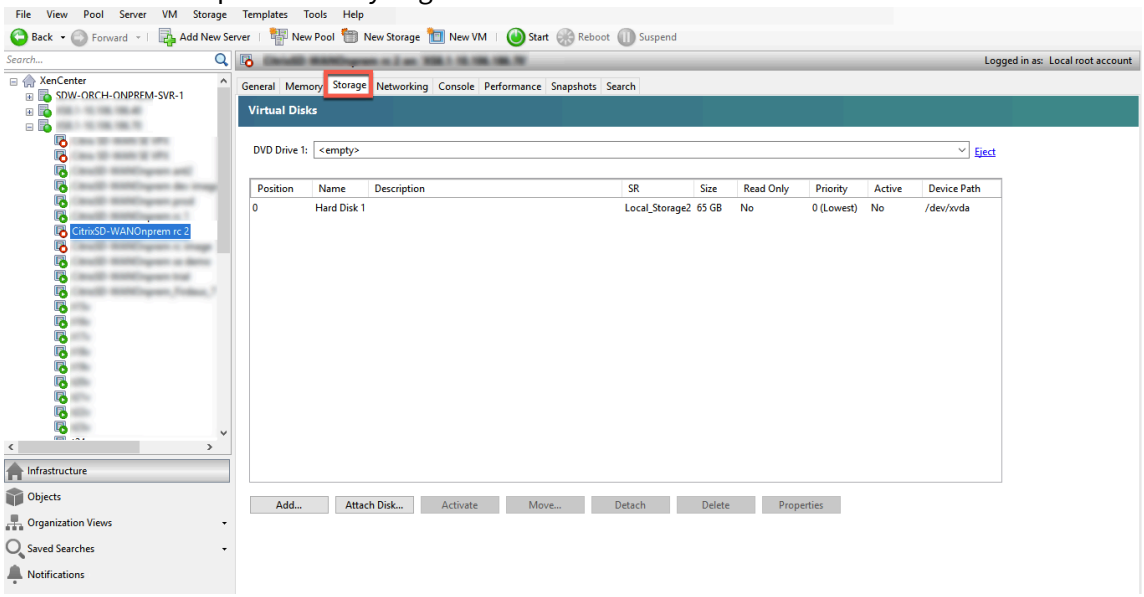
October 31, 2022

Puede aumentar el espacio en disco asignado a Citrix SD-WAN Orchestrator for On-premises.

### Aumente el espacio en disco en Citrix Hypervisor

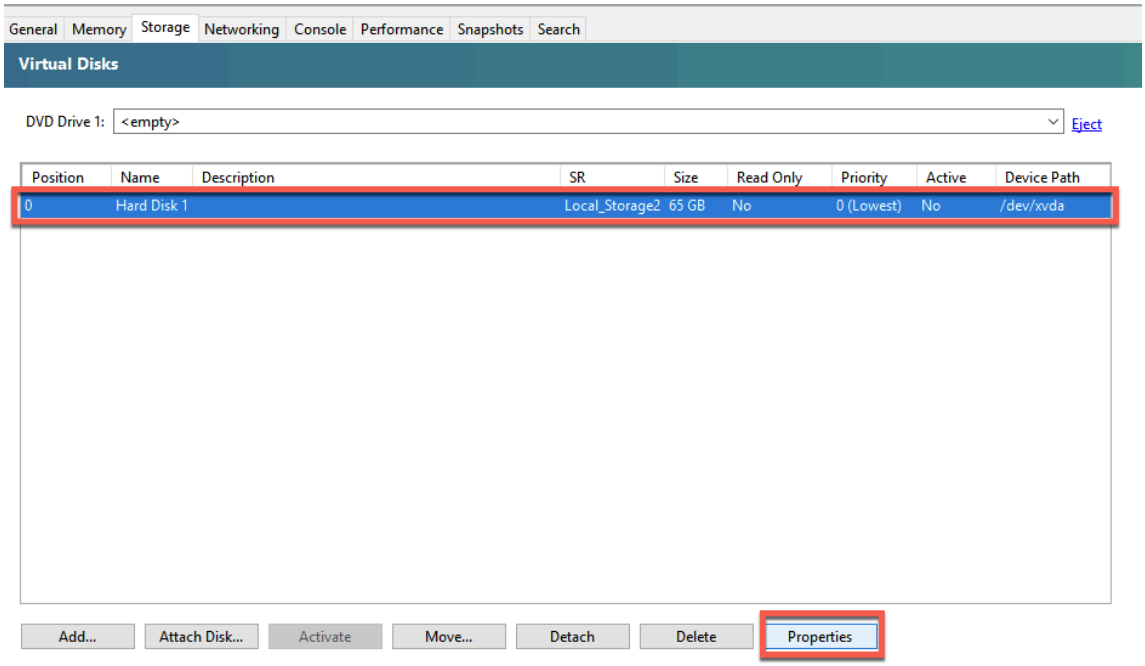
Para aumentar el espacio en disco en Citrix Hypervisor.

1. Apague la máquina virtual (VM) desde el hipervisor.
2. Seleccione la máquina virtual y haga clic en la ficha **Almacenamiento**.

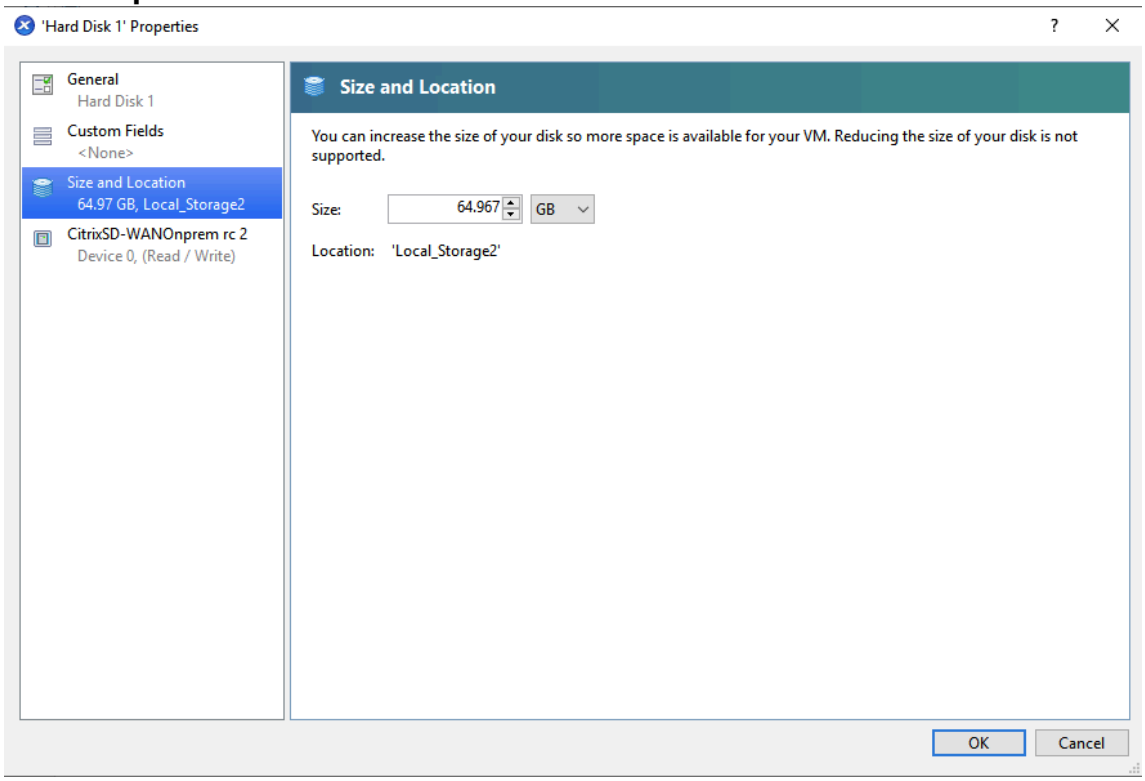



3. Seleccione el disco duro y haga clic en **Propiedades**.

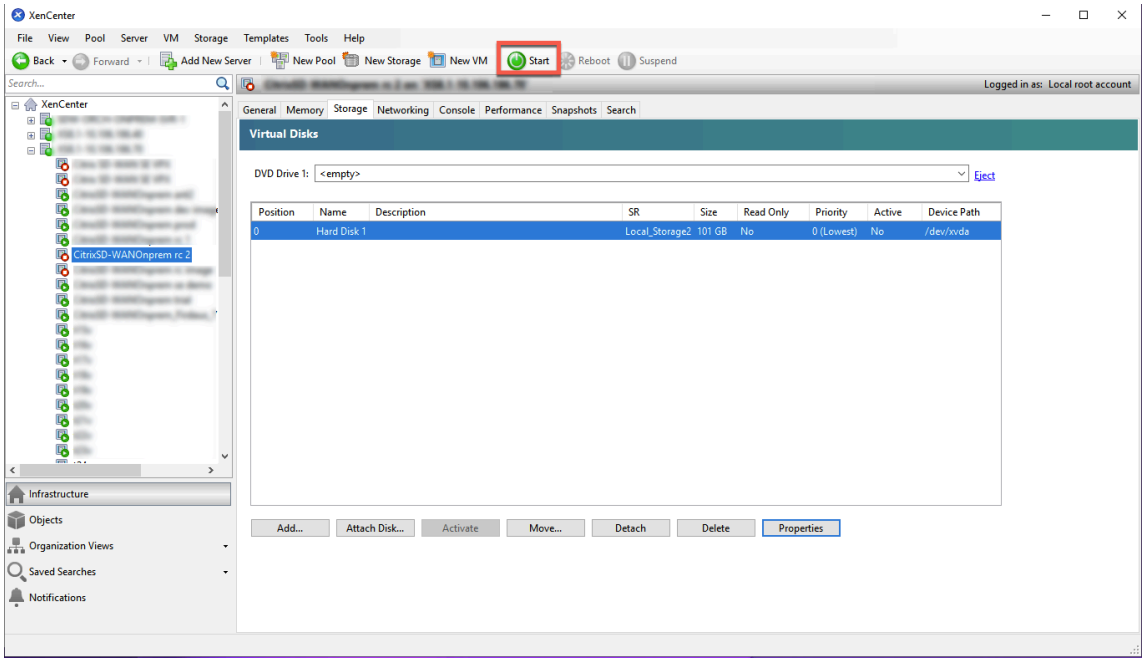



4. Haga clic en la opción **Tamaño y ubicación** y actualice el **tamaño** del espacio en disco. Haga clic en **Aceptar**.




5. Haga clic en **Inicio**.

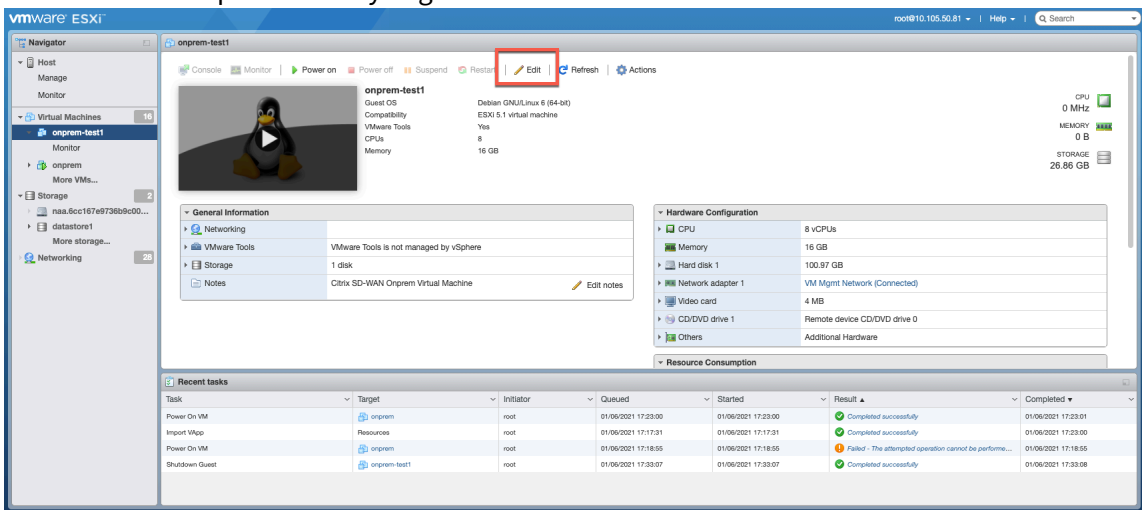
 




## Aumente el espacio en disco en el servidor ESXi

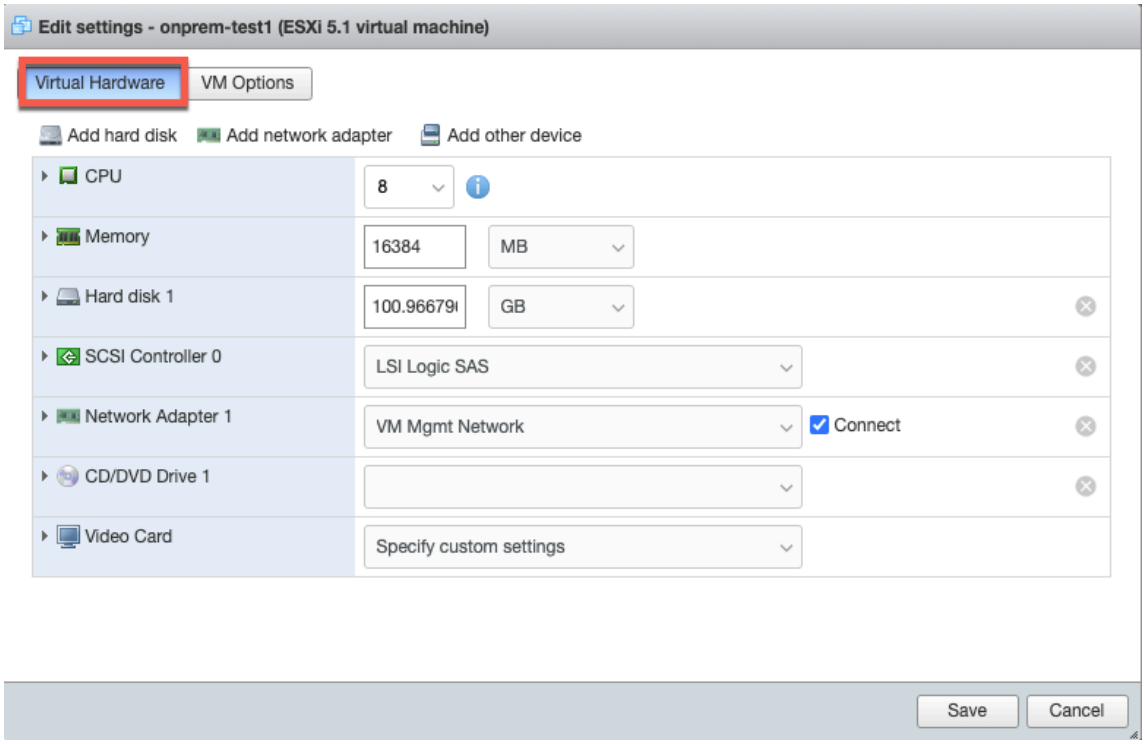
Para aumentar el espacio en disco del servidor ESXi.

1. Apague la máquina virtual (VM) desde el hipervisor.
2. Seleccione la máquina virtual y haga clic en **Modificar**.

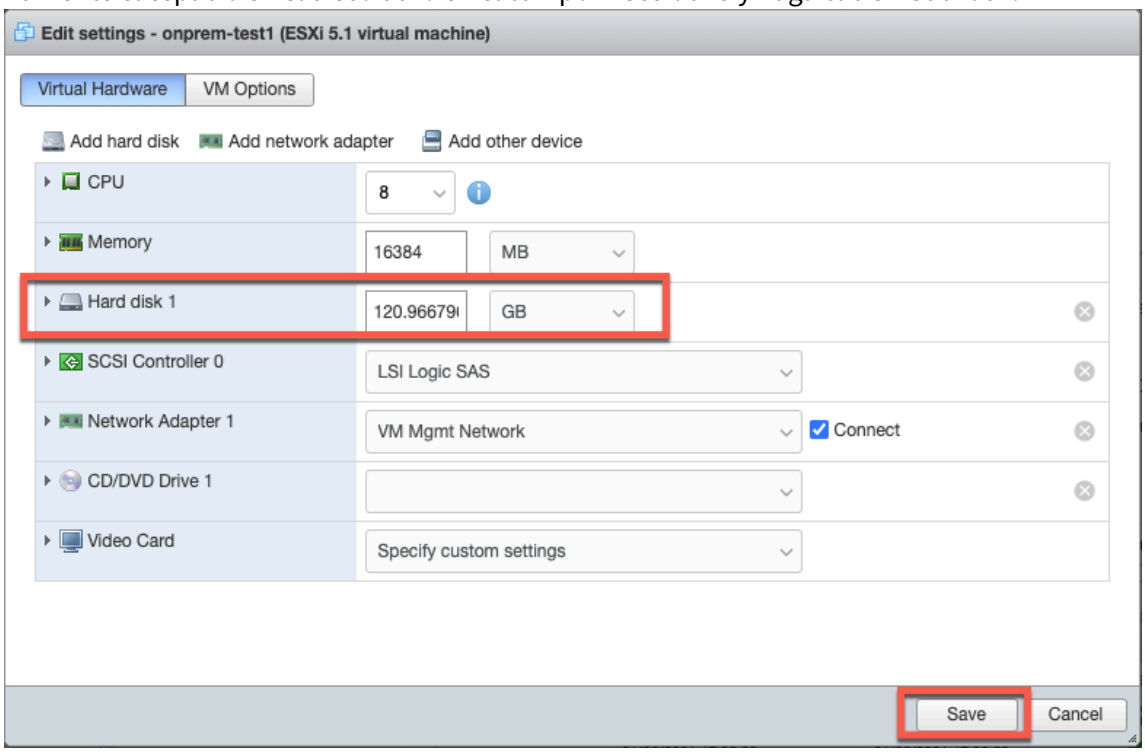



3. Seleccione la ficha **Hardware virtual**.

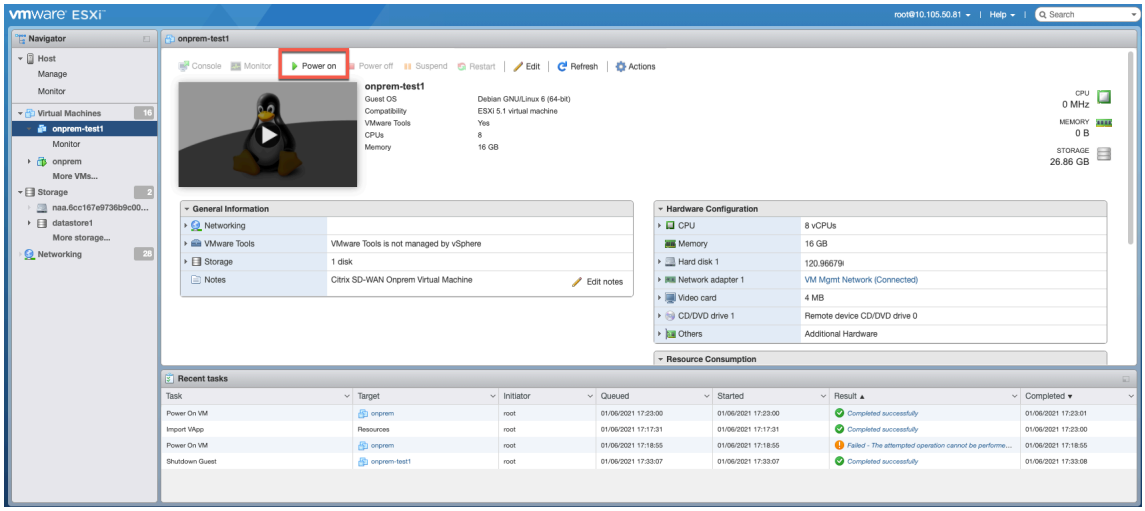



4. Aumente el espacio en el disco duro en el campo **Disco duro** y haga clic en **Guardar**.




5. Haga clic **en Encender**.




## Reemplazar un dispositivo Citrix SD-WAN afectado

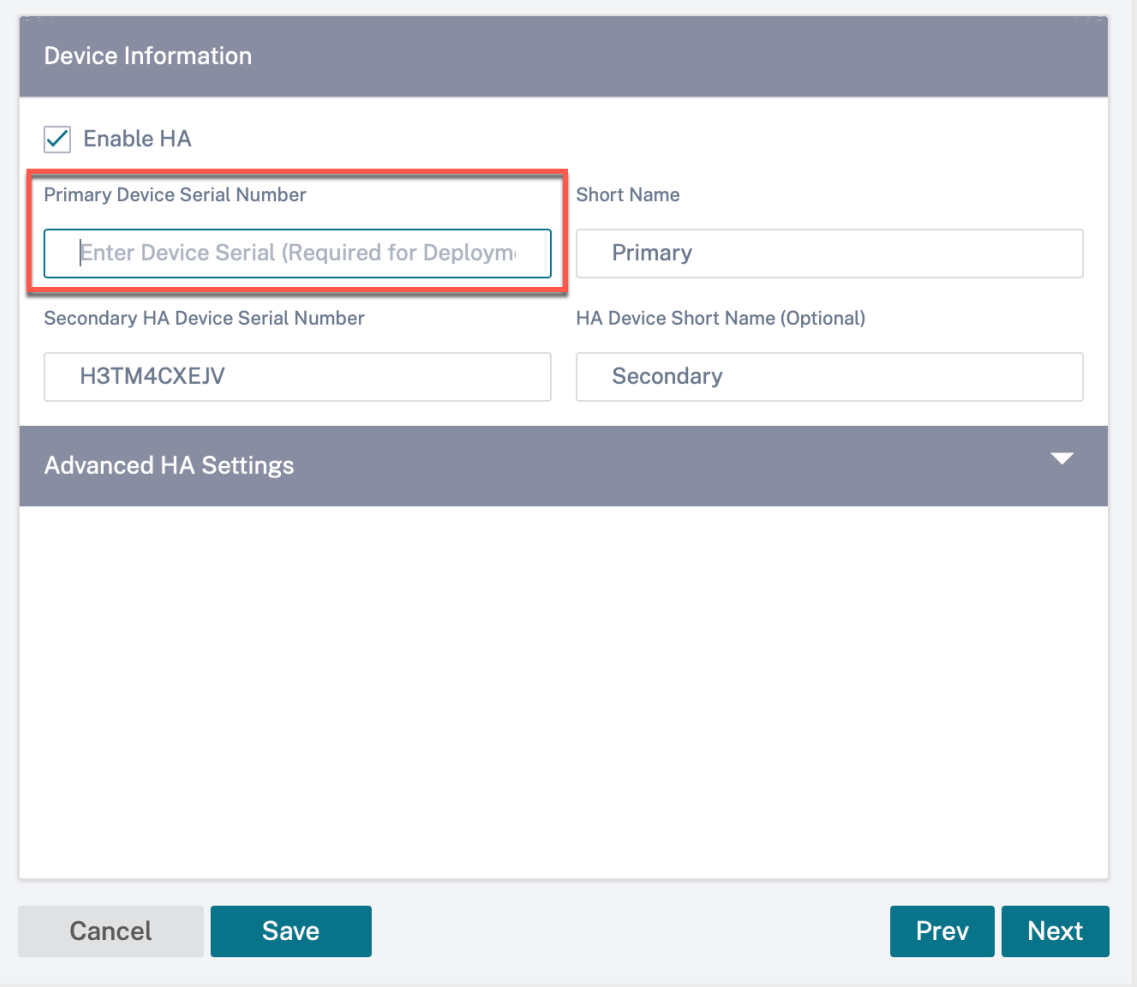
October 31, 2022

Para reemplazar un dispositivo afectado en Citrix SD-WAN Orchestrator for On-premises:

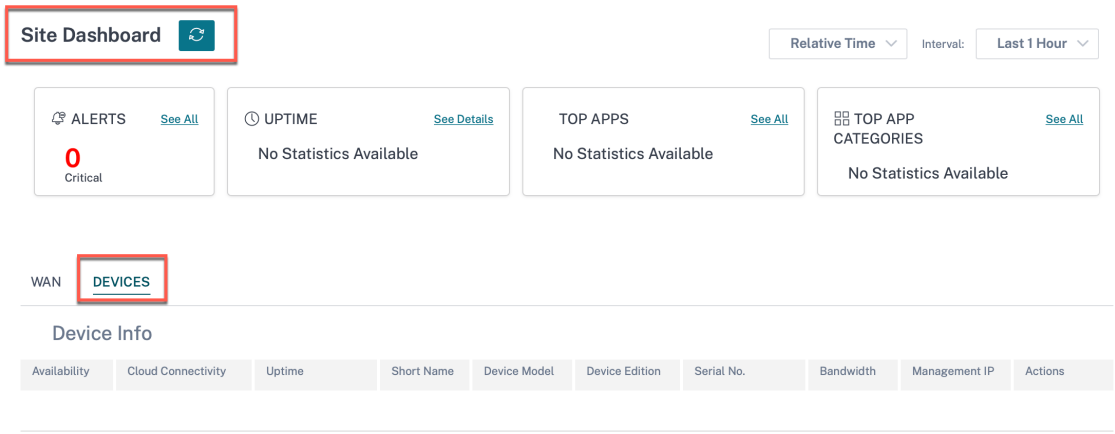
1. Inicie sesión en Citrix SD-WAN Orchestrator for On-premises y seleccione el sitio afectado. A nivel de sitio, vaya a **Configuración > Configuración del sitio > Información del dispositivo** y elimine el número de serie del campo **Número de serie del dispositivo principal**. Haga clic en **Guardar**.

   > **Nota**
   >
   > Si se sigue accediendo al dispositivo a través de Citrix SD-WAN Orchestrator for On-premises, el dispositivo se encuentra en estado de "restablecimiento de fábrica".



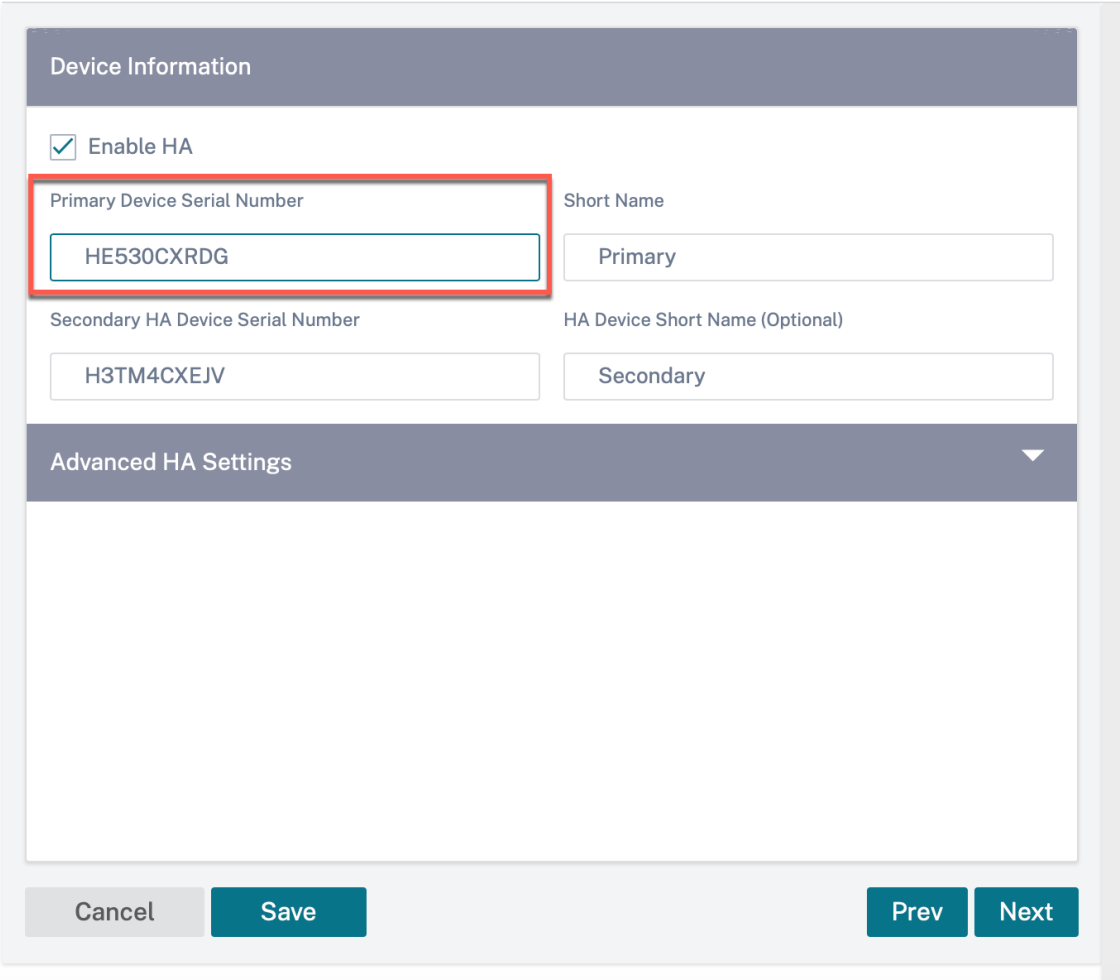

2. Vaya al **Panel de control > Dispositivos** y asegúrese de que el dispositivo afectado se haya eliminado de la lista.




3. Tome nota de la configuración de alimentación y cableado del dispositivo afectado y, a continuación, extraiga el dispositivo del bastidor.

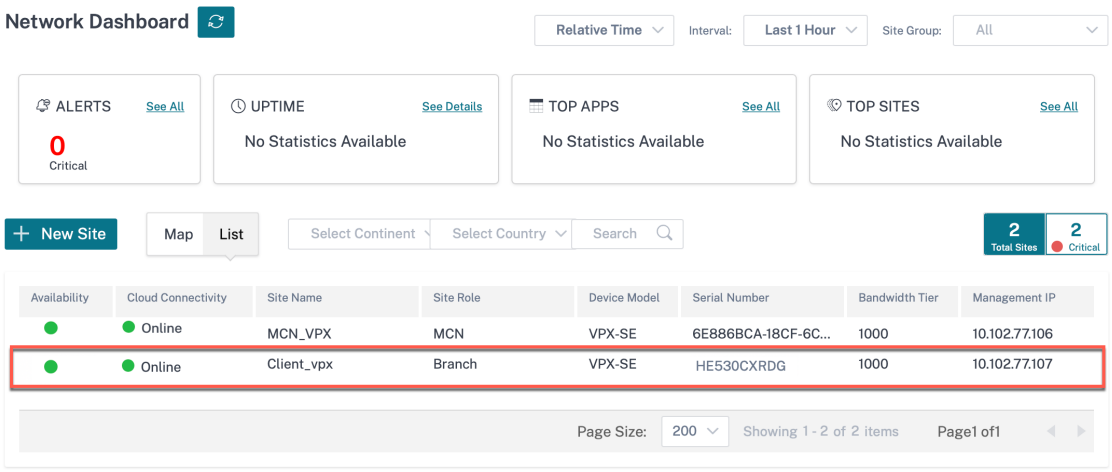
 

4. Monte el nuevo dispositivo en el bastidor y reinicie la alimentación y el cableado tal como estaban para el dispositivo afectado.
5. En la interfaz de usuario de Citrix SD-WAN Orchestrator for On-premises, al nivel de sitio, vaya a **Configuración > Configuración del sitio > Detalles del dispositivo**. Agregue el número de serie del nuevo dispositivo en el campo **Número de serie del dispositivo principal**. Haga clic en **Guardar**.

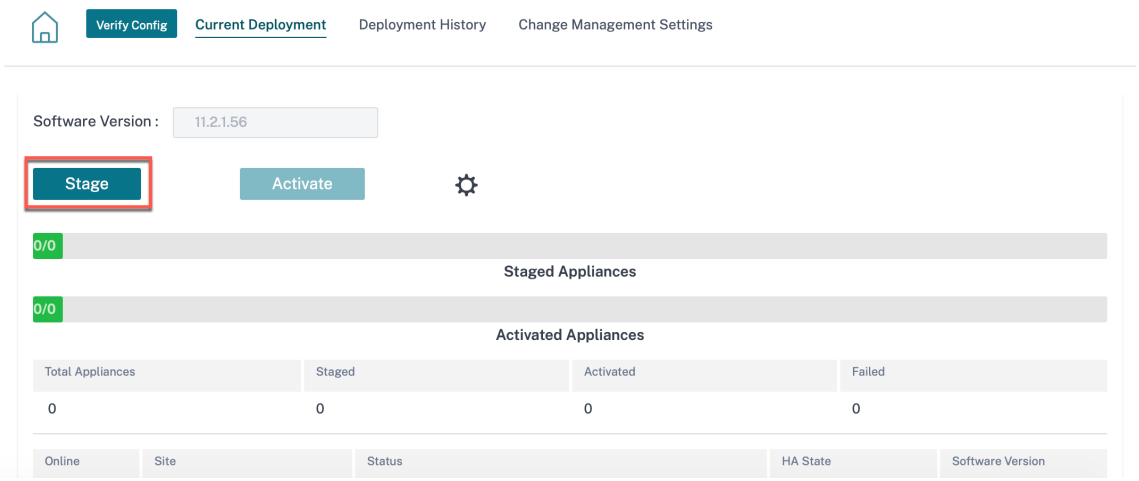



6. Configure la implementación sin intervención. Para obtener más información, consulte Implementación sin intervención.
7. Espere unos minutos para que el dispositivo actualice la conectividad a la nube en el panel del sitio.




8. A nivel de red, vaya a **Configuración > Inicio de configuración de red** y haga clic en **Deploy Config/Software**.
9. Haga clic en **Etapa**.




10. Haga clic en **Activar** una vez finalizada la preparación.
11. Navegue hasta el panel de control del sitio y compruebe que la activación del dispositivo se haya realizado correctamente.

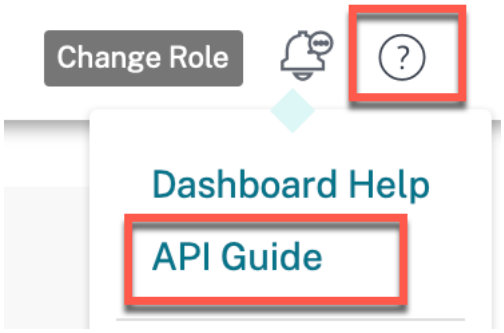
## Guía de API para Citrix SD-WAN Orchestrator for On-premises

October 31, 2022

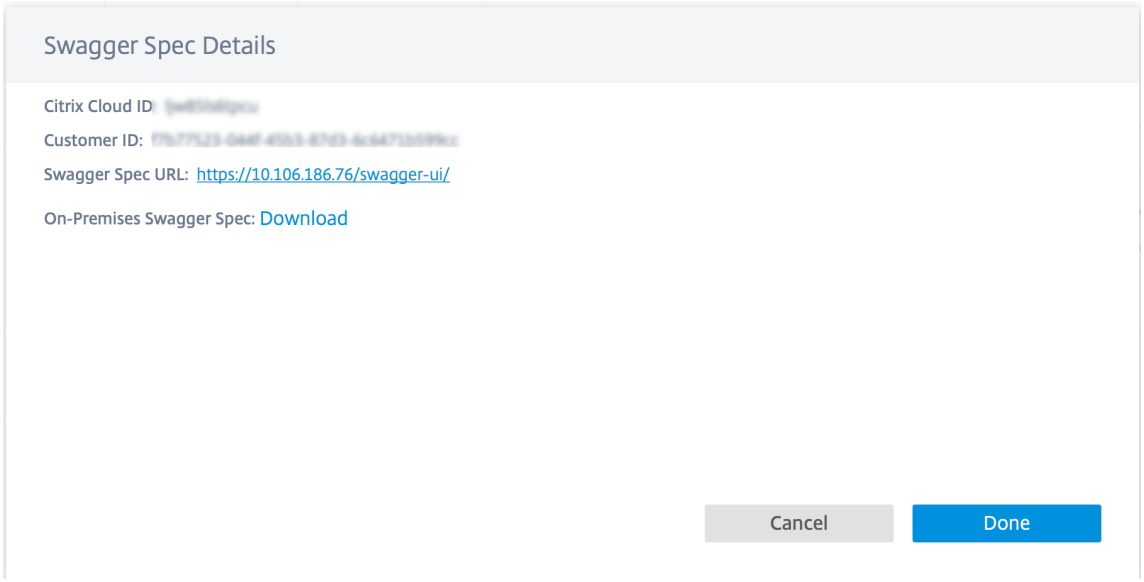
Para acceder a la guía de API de Citrix SD-WAN Orchestrator for On-premises en la interfaz de usuario de Swagger:

1. Inicie sesión en Citrix SD-WAN Orchestrator for On-premises y haga clic en **?** en la esquina superior derecha de la interfaz de usuario y, a continuación, en **Guía de API**.




Se muestran los detalles de la especificación Swagger.




2. Haga clic en la URL de especificación de Swagger para acceder a la guía de API.

## Citrix SD-WAN Orchestrator para API locales a través de curl

### Requisitos previos

- Acceso a la nube
- Inicio de sesión local

Realice los siguientes pasos para usar las API de Citrix On-premises Orchestrator a través de curl:

1. Inicio de**sesión en la nube**: En el caso de un XVA nuevo, primero debe iniciar sesión en la nube.

```
curl -k -X POST -H "Content-Type: application/json "https://<
    onprem-orchestrator-ip>/policy/v1/onprem/cloudLogon  –data '{
```

```
2  "clientId":"<clientId>","clientSecret":"<clientSecret> ","ccId":"
      <ccid>", "pop": "<popName>" }
3  '
```

`clientId`, `clientSecret` y `ccId` se pueden obtener en la página de IAM.

> **Nota**
>
> Asegúrese de que la cuenta del cliente ya esté creada en la nube antes de intentar iniciar sesión en la nube.

2. Inicio de**sesión local**: A continuación, inicie sesión local para obtener el token de autenticación.

```
1  curl -k -X POST -H "Content-Type: application/json" https://<
      onprem-orchestrator-ip>/onpm/v1/logon --data '{
2   "username":"admin","password":"<passwordField>" }
3   '
```

Esto devuelve el **token** y el **ID de cliente** en respuesta. El CustomerID permanece fijo y es necesario en otras llamadas a la API. Guarde el **CustomerID** para usarlo más adelante. El token sigue siendo válido durante una hora. Más adelante, debe realizar un nuevo inicio de sesión.

Ejemplo: Utilice el token de **autenticación** y el **ID de cliente** para activar otras API locales de Citrix.

```
1  curl -k -X GET -H "authorization:CWSAuth bearer= <token> " -H "
      Content-Type: application/json"https://<onprem-orchestrator-ip
      >/onpm/v1/scope/<customerId>/globalSettings/ntpSettings
```

## Administración del orquestador

October 31, 2022

Esta sección proporciona información sobre las actividades administrativas que se pueden realizar en la plataforma Citrix SD-WAN Orchestrator for On-premises.

### Software

Puede descargar la versión del software del dispositivo Citrix SD-WAN necesaria para todos los dispositivos de la red y guardarla en Citrix SD-WAN Orchestrator for On-premises. Utilice el software almacenado para actualizar el software Citrix SD-WAN Orchestrator for On-premises a la versión más reciente.

> **Nota**
>
> La configuración administrada por el proveedor se presenta en la versión 10.3 de Citrix SD-WAN Orchestrator for On-premises. No se admite la degradación a versiones de software anteriores a la versión 10.3 de Citrix SD-WAN Orchestrator for On-premises.

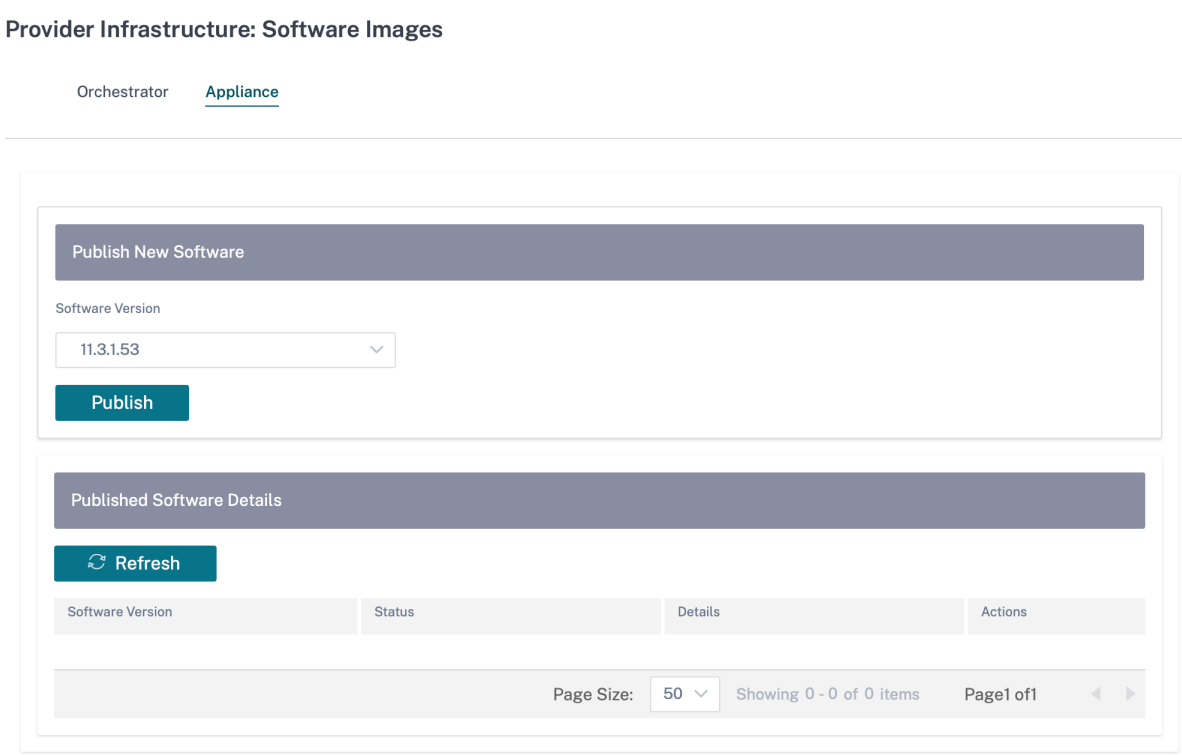
**Publicar software**

En una configuración administrada por un proveedor, Citrix SD-WAN Orchestrator for On-premises permite a los administradores de proveedores descargar la versión de software del dispositivo Citrix SD-WAN requerida para todos los dispositivos de la red. Los administradores de los proveedores pueden publicar la versión de software descargada. El software publicado se descarga y almacena en Citrix SD-WAN Orchestrator for On-premises. Los administradores de clientes pueden implementar el software publicado en todos los dispositivos administrados por Citrix SD-WAN Orchestrator for On-premises.

En una configuración administrada por el cliente, los administradores de clientes pueden descargar la versión de software del dispositivo Citrix SD-WAN requerida para todos los dispositivos de la red. Pueden publicar el software en Citrix SD-WAN Orchestrator for On-premises e implementarlo en todos los dispositivos.

Para publicar software, vaya a **Infraestructura > Administración de Orchestrator > Imágenes de software > Dispositivo**.

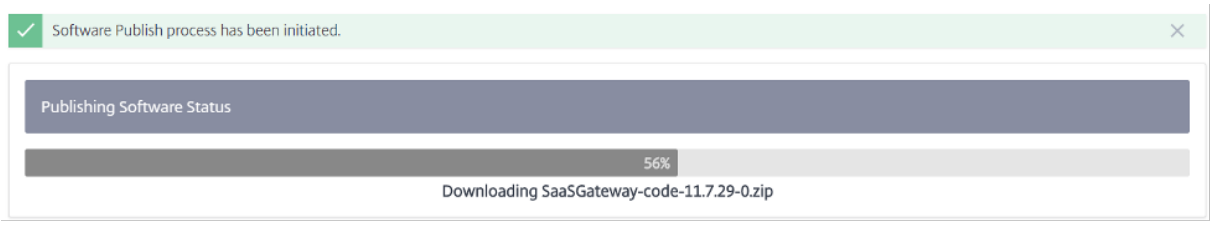
 



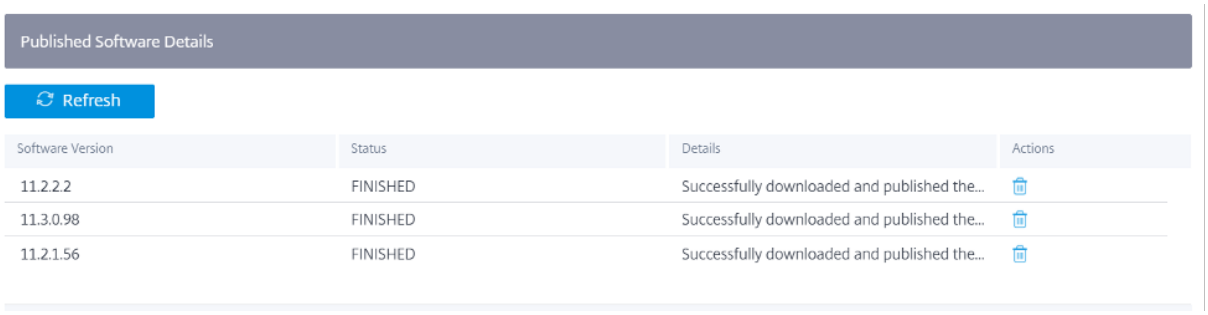

Puede elegir la versión de software que se publicará de una lista prediseñada de versiones de software compatibles con el actual Citrix SD-WAN Orchestrator for On-premises. Para las versiones de software más recientes que no estén disponibles en la lista, actualice a la versión más reciente de Citrix SD-WAN Orchestrator for On-premises, que admite la nueva versión del software. Para obtener información sobre la actualización de Citrix SD-WAN Orchestrator for On-premises, consulte Actualización de software.


Citrix SD-WAN Orchestrator for On-premises descarga el software Citrix SD-WAN de la versión seleccionada para todas las plataformas. Una barra de progreso indica el progreso del proceso de publicación.




Las versiones de software publicadas se muestran en **Detalles del software publicado**. En cualquier momento, Citrix SD-WAN Orchestrator for On-premises puede almacenar hasta tres versiones de software publicadas. Si tiene intención de publicar otra versión de software, elimine una de las tres versiones disponibles antes de iniciar el proceso de publicación.




Una vez que la publicación se haya realizado correctamente, puede implementar, organizar y activar el software en todos los dispositivos de la red desde la página de **configuración de red**. Para obtener más información, consulte Configuración de red. Para una implementación correcta, asegúrese de que todos los dispositivos estén conectados a Citrix SD-WAN Orchestrator for On-premises. Para obtener más información, consulte Conectividad con dispositivos Citrix SD-WAN.

### Actualización de software

En una configuración administrada por un proveedor, solo los administradores de proveedores pueden actualizar el software Citrix SD-WAN Orchestrator for On-premises a la versión más reciente.

En una configuración administrada por el cliente, los administradores de clientes pueden actualizar el software Citrix SD-WAN Orchestrator for On-premises a la versión más reciente.

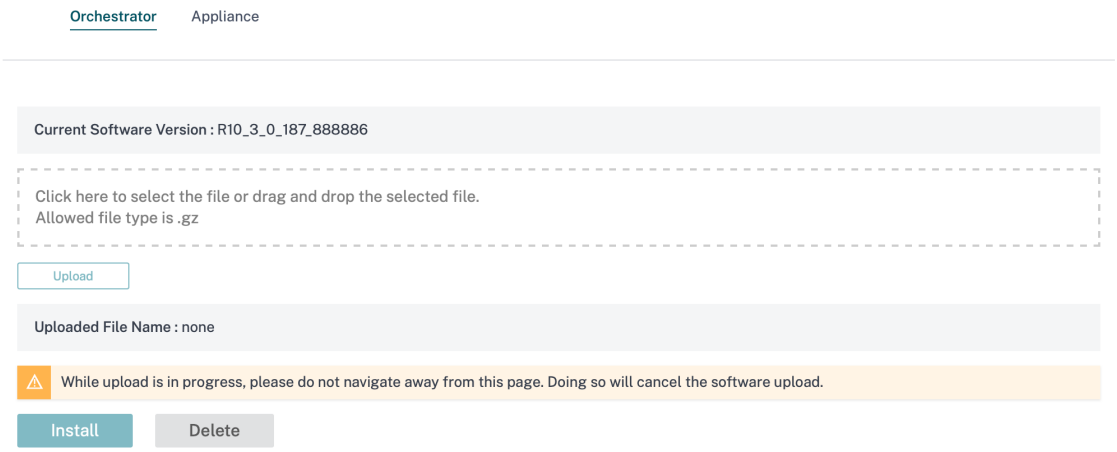
> **NOTA**
>
> - Descargue el paquete de software Citrix SD-WAN Orchestrator for On-premises correspondiente en su equipo local. Puede descargar este paquete desde la página de descargas.
> - Citrix recomienda tomar instantáneas de la máquina virtual en el hipervisor. Además, la configuración de SD-WAN se descarga antes de la actualización.
> - Citrix también recomienda tomar instantáneas de las configuraciones de VM y SD-WAN per-

> iódicamente.

Realice los siguientes pasos para cargar e instalar una nueva versión del software Citrix SD-WAN Orchestrator for On-premises:

1. En la interfaz de usuario de Citrix SD-WAN Orchestrator for On-premises, vaya a **Infraestructura > Administración de Orchestrator > Imágenes de software > Orchestrator**.
2. Haga clic dentro del cuadro y seleccione el archivo binario ctx-onprem-1 (fecha más reciente) .tar.gz que ha descargado y guardado en su sistema local.




3. Haga clic en Cargar para **cargar** el paquete de software seleccionado a la máquina virtual Citrix SD-WAN Orchestrator for On-premises actual.
4. Una vez finalizada la carga, haga clic en **Instalar**.
5. Cuando se le solicite confirmar, haga clic en **Instalar**.

## Configuración de administración

> **Nota**
>
> En una configuración administrada por un proveedor, solo los administradores del proveedor tienen acceso a modificar la configuración en **Infraestructura > Administración de Orchestrator > Configuración de administración**.

### Administración de IP y DNS

Después de implementar Citrix SD-WAN Orchestrator para máquinas virtuales (VM) locales y configurar una IP de administración de forma manual o mediante DHCP, puede cambiar la configuración de **DNS y IP de administración** a través de la GUI de Citrix SD-WAN Orchestrator for Onpremises. La

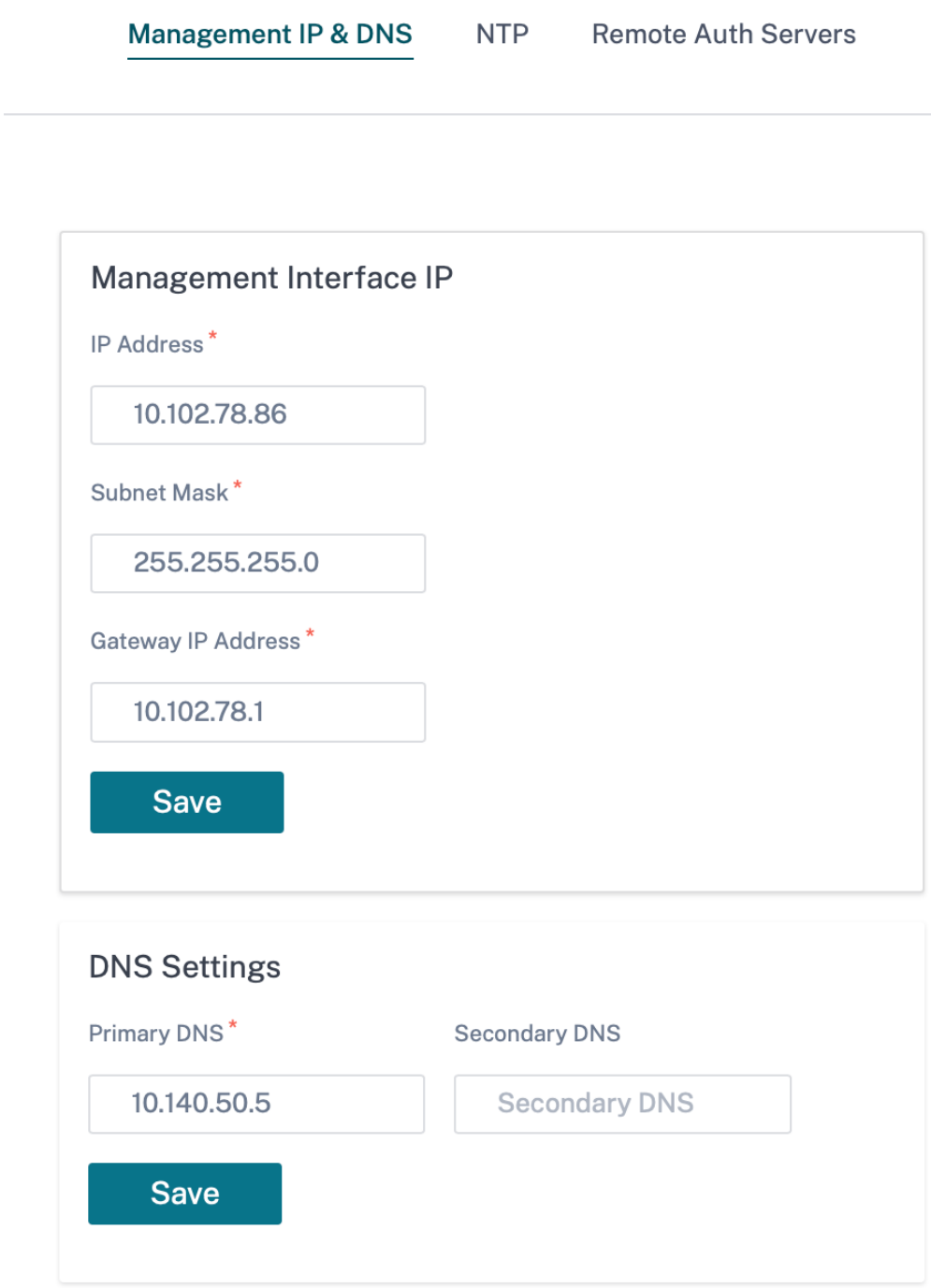
pila Citrix SD-WAN Orchestrator for On-premises tarda unos 3 minutos en reiniciarse. Una vez que se cambia la dirección IP de administración, se restablecen las conexiones SSH.

Para configurar o cambiar la configuración de IP y DNS de administración, al nivel de red, vaya a **Infraestructura > Administración de Orchestrator > Configuración de administración > IP y DNS**de administración.

Proporcione los siguientes detalles:

- **Dirección IP**: La dirección IP de Citrix SD-WAN Orchestrator para máquinas virtuales locales.
- **Dirección IP de puerta**de enlace: La dirección IP de puerta de enlace que Citrix SD-WAN Orchestrator para entornos locales utiliza para comunicarse con redes externas.
- **Máscara de subred**: La máscara de subred que define la red en la que está disponible Citrix SD-WAN Orchestrator for On-premises.
- **DNS principal**: La dirección IP del servidor DNS principal al que se reenvían todas las solicitudes de DNS de Citrix SD-WAN Orchestrator for On-premises.
- **DNS secundario**: La dirección IP del servidor DNS secundario para resolver las solicitudes de DNS si el servidor DNS principal no está disponible.



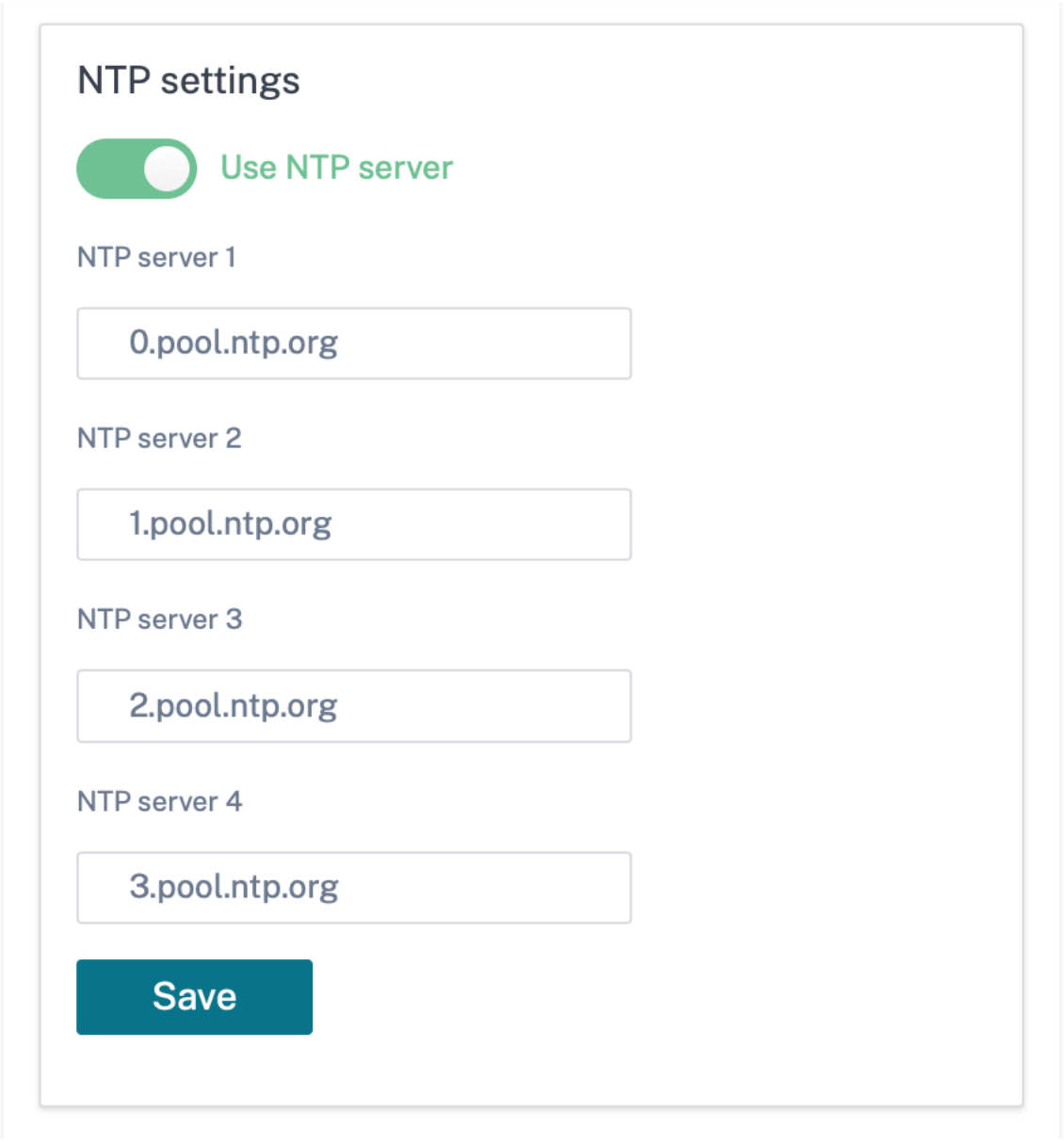
### Configuración de NTP

Puede configurar la fecha y la hora manualmente o utilizar un servidor de protocolo de hora de red (NTP) para sincronizar la hora del reloj de Citrix SD-WAN Orchestrator para entornos locales con la hora universal coordinada (UTC).

Para configurar el servidor NTP, al nivel de red, vaya a **Infraestructura > Administración de Orchestrator > Configuración de administración > NTP** y active **Usar servidor NTP**.

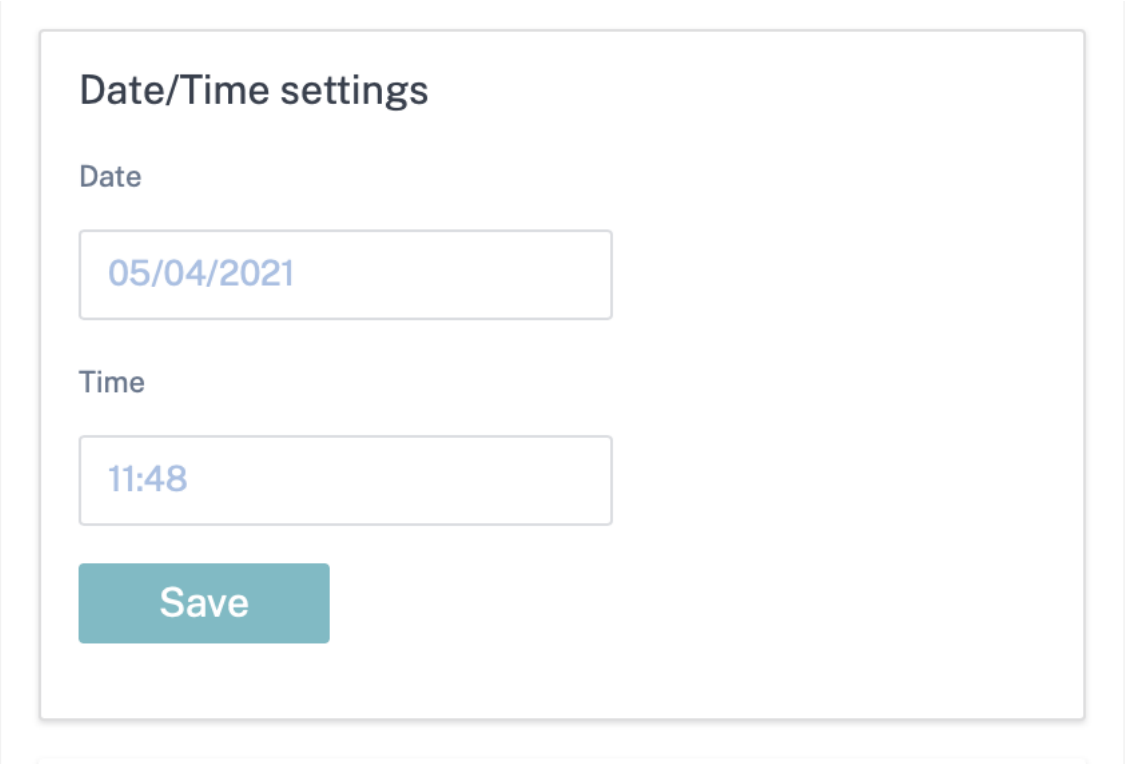
Proporcione la dirección IP o el nombre de dominio del servidor NTP. Puede proporcionar hasta cuatro servidores NTP, pero asegúrese de que al menos uno esté configurado. Si un servidor NTP está inactivo, Citrix SD-WAN Orchestrator for On-premises se sincroniza automáticamente con el otro servidor NTP. Si especifica un nombre de dominio para un servidor NTP, asegúrese de que el servidor DNS externo esté configurado para apuntar el nombre de dominio a la dirección IP.




Para configurar la fecha y la hora manualmente, desactive la opción **Usar servidor NTP** y seleccione manualmente la fecha y la hora.

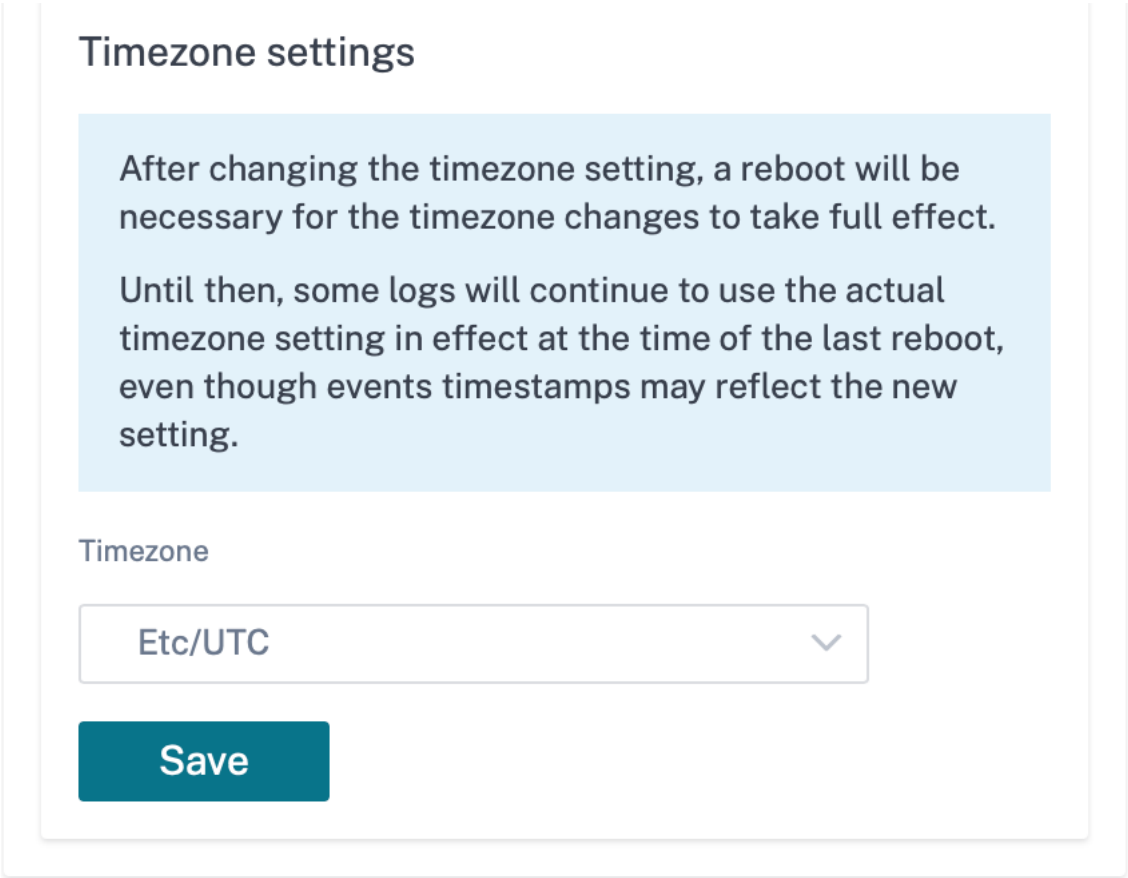
 




Selecciona la zona horaria según tu país o ciudad.

> **NOTA**
>
> Reinicie la máquina virtual de Orchestrator después de cambiar la zona horaria. Algunos registros seguirán utilizando la zona horaria anterior hasta que finalice el reinicio. Para obtener instrucciones, consulte Reboot Orchestrator VM.

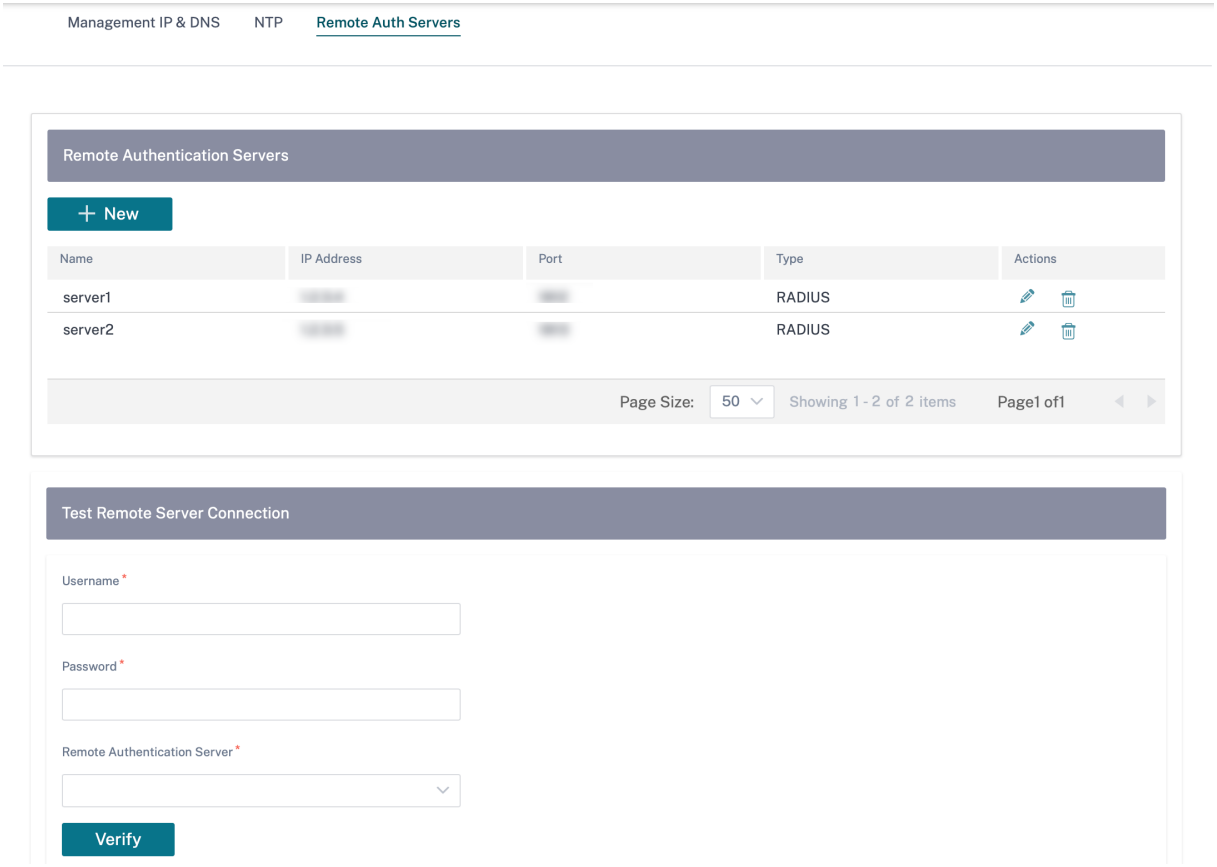



**Servidores de autenticación remota**

En una configuración administrada por un proveedor, solo los administradores de proveedores pueden configurar los servidores RADIUS o TACACS+ para los usuarios que se autentican de forma remota. Los administradores de clientes pueden usar los servidores de autenticación remota configurados por los administradores del proveedor. En una configuración administrada por el cliente, los administradores del cliente pueden configurar los servidores RADIUS o TACACS+.

> **NOTA**
>
> Asegúrese de crear las cuentas de usuario necesarias en el servidor de autenticación RADIUS o TACACS+.

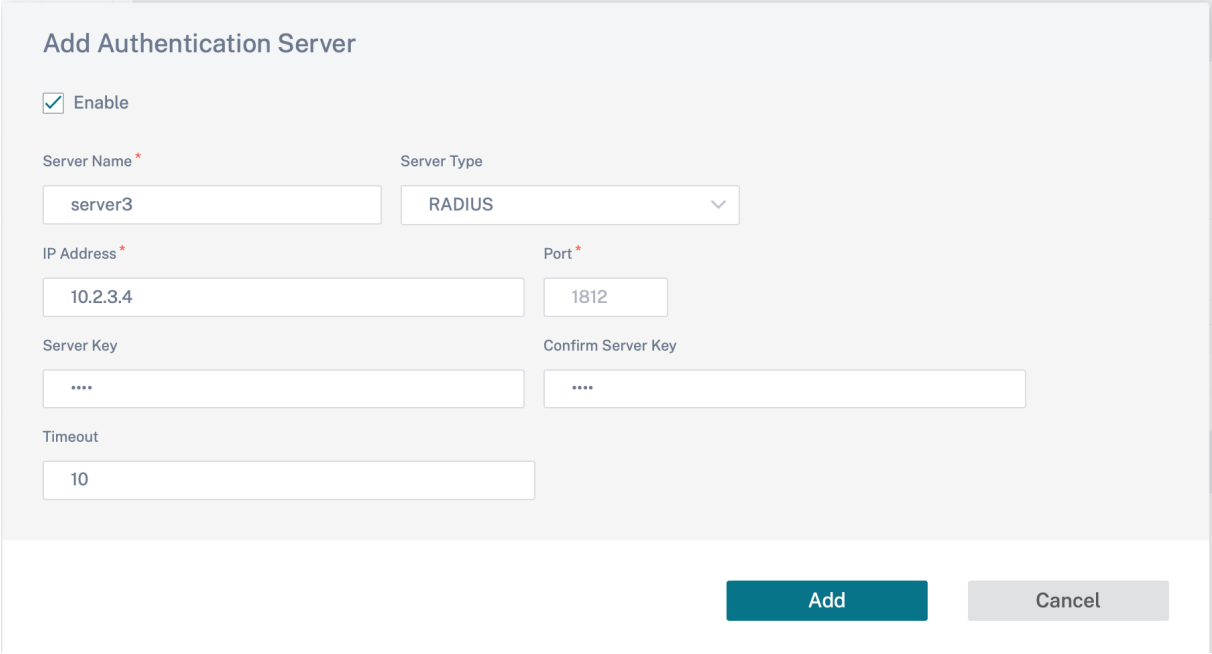



Para configurar la autenticación remota, vaya a **Infraestructura > Administración de Orchestrator > Configuración de administración > Servidores de autenticación remota**. Haga clic en **+ Nuevo**. Introduzca los siguientes detalles:

- **Habilitar: habilita**la configuración del servidor de autenticación remota.
- **Nombre del servidor**: El nombre del servidor de autenticación remota.
- **Tipo de servidor**: El tipo de servidor de autenticación remota: RADIUS o TACACS+.
- **Dirección IP**: La dirección IP del host del servidor de autenticación remota.
- **Puerto**: El número de puerto del servidor de autenticación remota. El puerto predeterminado para el servidor RADIUS es 1812 y el servidor TACACS+ es 49.
- **Clave de servidor** y **clave de servidor de confirmación**: Clave secreta que se usa al conectarse al servidor de autenticación remota.
- **Tipo de autenticación**: (disponible solo para el servidor TACACS+) Seleccione el método de cifrado que se utilizará para enviar el nombre de usuario y la contraseña al servidor TACACS+.
  - **PAP**: Utiliza el Protocolo de autenticación de contraseña (PAP) para reforzar la autenticación de los usuarios mediante la asignación de un secreto compartido seguro al servidor TACACS+.
  - **ASCII**: Utiliza el conjunto de caracteres ASCII para reforzar la autenticación del usuario mediante la asignación de un secreto compartido seguro al servidor TACACS+.

- **Tiempo de espera**: intervalo de tiempo (en segundos) para esperar una respuesta de autenticación del servidor de autenticación remota.




También puede probar la conexión al servidor remoto. En **Probar conexión al servidor remoto**, introduzca su **nombre de usuario** y **contraseña**. Seleccione el servidor de autenticación remota y haga clic en **Verificar**.

### Gestión de bases de

Puede crear una copia de seguridad de la base de datos actual que se ejecuta en Citrix SD-WAN Orchestrator for On-premises y luego usar el archivo de copia de seguridad para restaurar el mismo estado de la base de datos.

> **Nota**
>
> - En una configuración administrada por un proveedor, solo los administradores del proveedor tienen acceso para crear copias de seguridad de la base de datos y restaurarlas.
> - No puede restaurar la copia de seguridad de la base de datos realizada en una configuración administrada por el proveedor en una configuración administrada por el Del mismo modo, no puede restaurar la copia de seguridad de la base de datos realizada en una configuración administrada por el cliente en una configuración administrada por

Para crear una copia de seguridad de la base de datos, vaya a **Infraestructura** > **Administración de Orchestrator** > **Administración** Haga clic en **Copia de seguridad**.

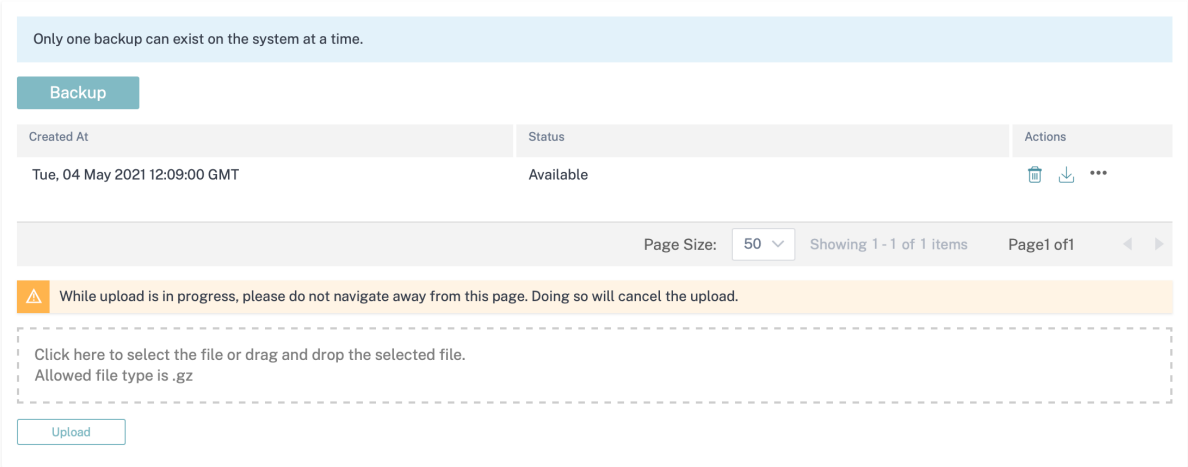
Haga clic en Descargar en la columna **Acciones** para descargar la base de datos respaldada.

Haga clic en **Cargar** para buscar y cargar el archivo descargado. También puede arrastrar el archivo descargado y soltarlo en la pantalla.

Para restaurar, haga clic en **Restaurar** en la columna **Acciones**.

> **NOTA**
>
> - Solo puede guardar una copia de seguridad de la base de datos a la vez. Para reemplazar una copia de seguridad existente por la más reciente, elimínala y haga clic en **Copia de seguridad**.
> - La restauración de la base de datos debe realizarse en la misma versión de Citrix SD-WAN Orchestrator for On-premises desde la que se realizó la copia de seguridad de los datos.
> - La copia de seguridad de la base de datos solo toma la copia de seguridad de la configuración No hace copias de seguridad de los datos relacionados con la plataforma.




## Administración de almacenamiento

Citrix SD-WAN Orchestrator for On-premises admite la migración de las configuraciones de los clientes, las estadísticas, la base de datos local y la versión publicada de Citrix SD-WAN de un disco existente a un disco nuevo.

En una configuración administrada por un proveedor, solo los administradores del proveedor pueden realizar la migración del disco. Los administradores de clientes de la configuración administrada por el proveedor no tienen privilegios para realizar la migración de discos. En una configuración administrada por el cliente, los administradores del cliente pueden realizar la migración del disco.

Puede realizar la migración del disco para aumentar el espacio en disco o para la recuperación ante desastres.

- **Agregar un disco nuevo**: Puede agregar un disco nuevo con un tamaño de almacenamiento de al menos el doble del de los datos actuales consumidos por Citrix SD-WAN Orchestrator for On-premises. A través de la interfaz de usuario de Citrix SD-WAN Orchestrator for On-premises, puede activar el nuevo disco y migrar las configuraciones de los clientes existentes, las estadísticas, la base de datos local y la versión publicada de Citrix SD-WAN. Una vez que se activa el disco recién agregado, se reinicia Citrix SD-WAN Orchestrator for On-premises.
- **Recuperación ante desastres**: En caso de desastre, puede conectar el disco que contiene los datos a una nueva instancia de Citrix SD-WAN Orchestrator para máquinas virtuales locales que se encuentre en la misma versión de Citrix SD-WAN Orchestrator for On-premises. Active el disco sin elegir la opción **Migrar datos** en la interfaz de usuario de Citrix SD-WAN Orchestrator for On-premises. Una vez que se activa el disco, se reinicia Citrix SD-WAN Orchestrator for On-premises.

> **NOTA**
>
> - Cuando la migración del disco esté en curso, no apague ni reinicie manualmente Citrix SD-WAN Orchestrator for On-premises. El apagado o el reinicio manual pueden provocar la pérdida de datos.
> - Cuando se migra un disco desde una partición de disco que se agregó anteriormente a una partición de disco recién creada, después de la migración, los datos del disco antiguo no se eliminan. Para eliminar los datos del disco antiguo, conéctelo a otro sistema operativo y elimine los datos de forma segura.

### Limitaciones

Las siguientes son las limitaciones del proceso de migración de discos:

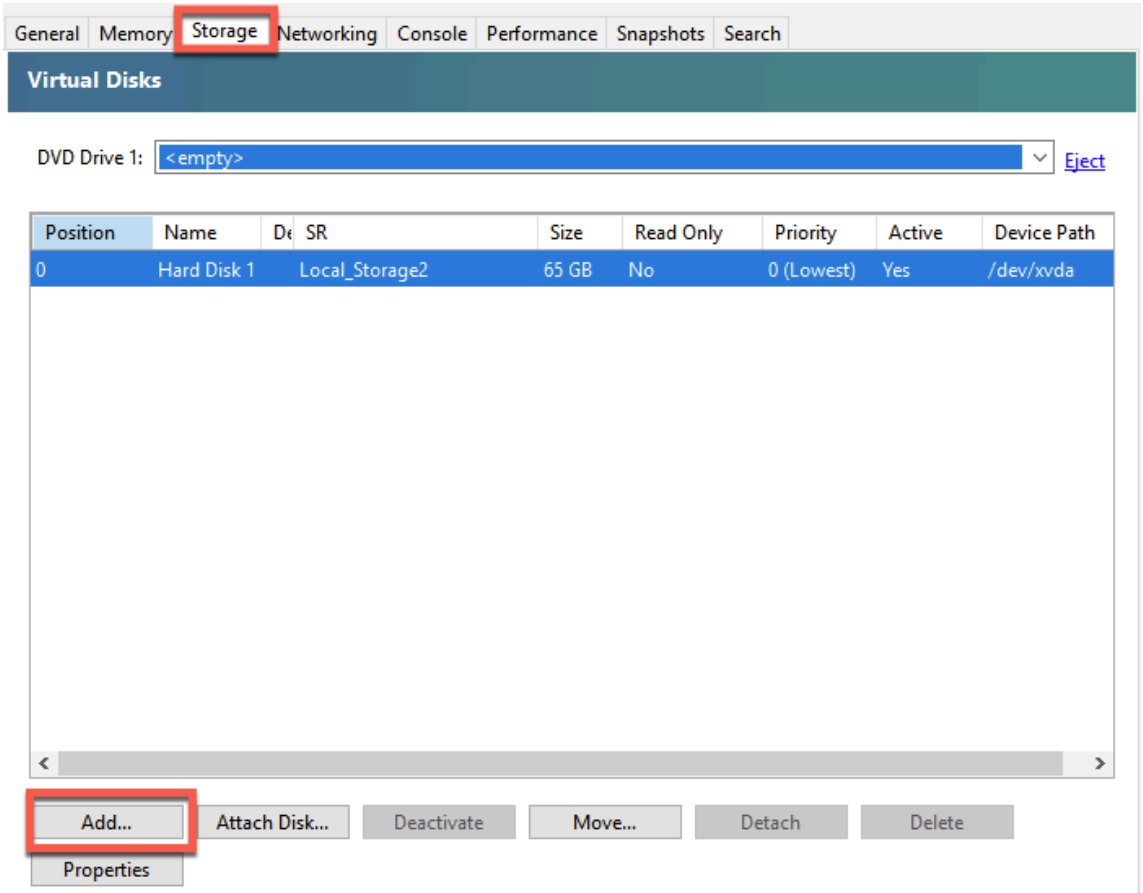
- Los usuarios de la versión anterior no se migran a la nueva versión. Publica la migración, elimina los usuarios y vuelve a crearlos.
- El STS creado en la antigua máquina virtual Citrix SD-WAN Orchestrator for On-premises no se migra. Sin embargo, después de la migración, la interfaz de usuario muestra el STS generado en la antigua máquina virtual Citrix SD-WAN Orchestrator for On-premises. Elimine el STS manualmente.
- La copia de seguridad de la base de datos creada en el antiguo Citrix SD-WAN Orchestrator para locales no se migra. Publica la migración si aparece en la lista, elimínala manualmente.
- De forma predeterminada, se supone que el nuevo Citrix SD-WAN Orchestrator for On-premises al que se migra el disco tiene conectividad con los servidores de autenticación de dos factores. Si la cuenta de administrador utiliza servidores de autenticación de dos factores y las conexiones a los servidores de autenticación de dos factores no están disponibles, ni siquiera el administrador podrá iniciar sesión. En estos casos, póngase en contacto con el soporte de Citrix
- Tras la migración al nuevo disco, no puede aumentar el espacio en disco asignado a Citrix SD-WAN Orchestrator for On-premises.

- En el caso de recuperación ante desastres, debe volver a configurar el dominio personalizado después de activar el disco.
- En el caso de recuperación ante desastres, después de activar el disco, debe realizar una implementación sin intervención fuera de la nube o una implementación sin intervención negociada en la nube para establecer la conectividad entre los dispositivos Citrix SD-WAN en los sitios con Citrix SD-WAN Orchestrator for On-premises.

### Agregar un disco nuevo en Citrix Hypervisor

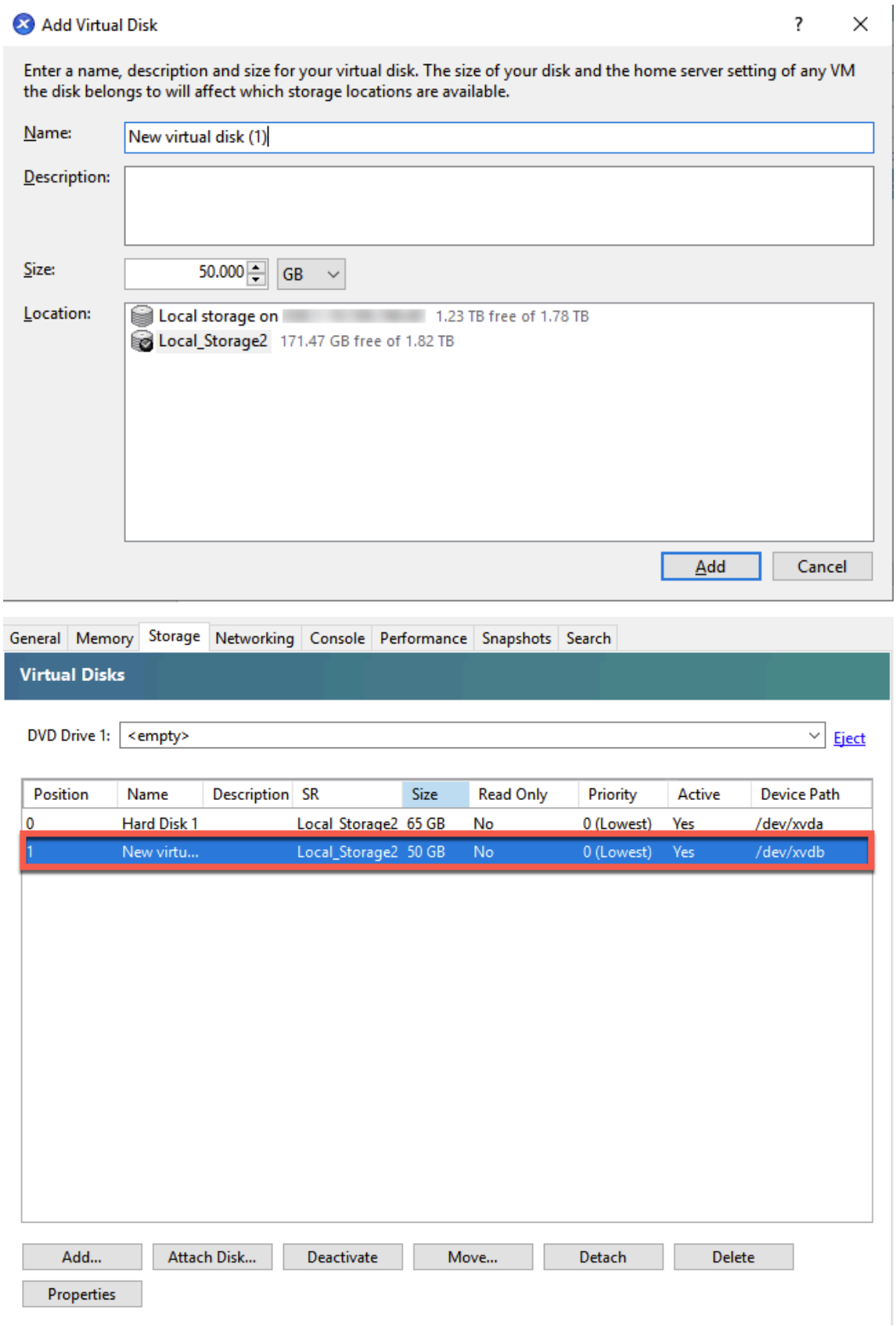
1. Seleccione la máquina virtual (VM) en el hipervisor. Seleccione la ficha **Almacenamiento** y haga clic en **Agregar**.




2. Proporcione detalles como el nombre, la descripción, el tamaño y la ubicación del nuevo disco. Haga clic en **Agregar**. El disco recién agregado aparece en la ficha **Almacenamiento**.

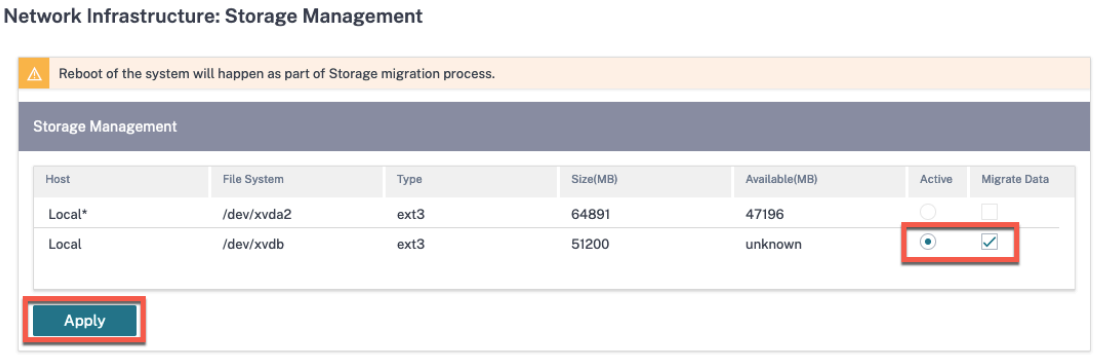
> **NOTA**
>
> El tamaño del disco debe ser al menos el doble del de los datos actuales que consume el Citrix SD-WAN Orchestrator for On-premises.

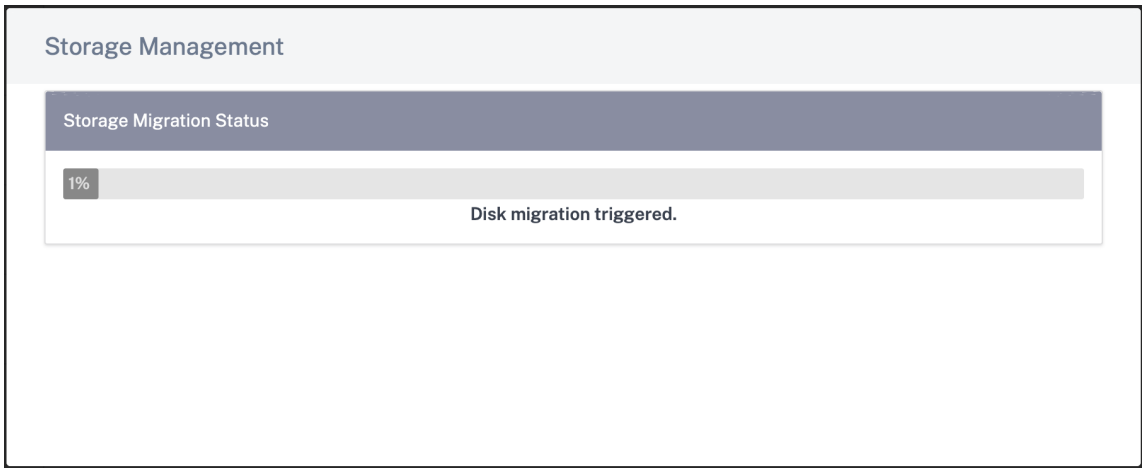


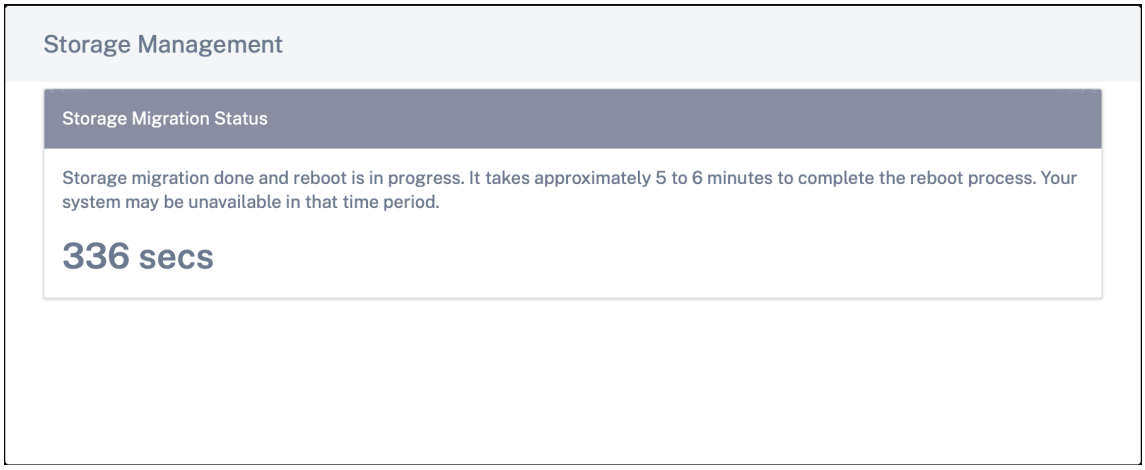

 

3. Inicie sesión en la interfaz de usuario local de Citrix SD-WAN Orchestrator y vaya a **INFRA-STRUCTURE > Orchestrator Administration > Storage Management**. El disco recién conectado aparece automáticamente en **Administración del almacenamiento**.
4. Seleccione el botón de opción **Activo** y seleccione la casilla **Migrar datos**. Haga clic en **Aplicar**.




5. Se activa el proceso de migración del disco. Las configuraciones del cliente, las estadísticas, la base de datos local y la versión de lanzamiento de Citrix SD-WAN en el disco existente se migran al nuevo disco. Una vez completada la migración, se reinicia Citrix SD-WAN Orchestrator for On-premises.

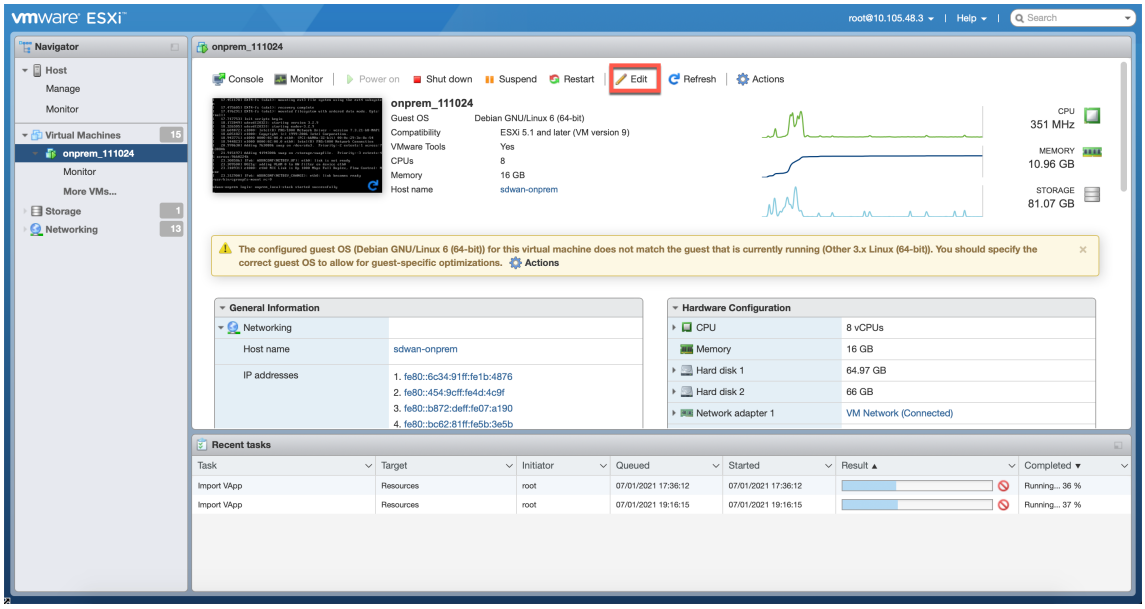


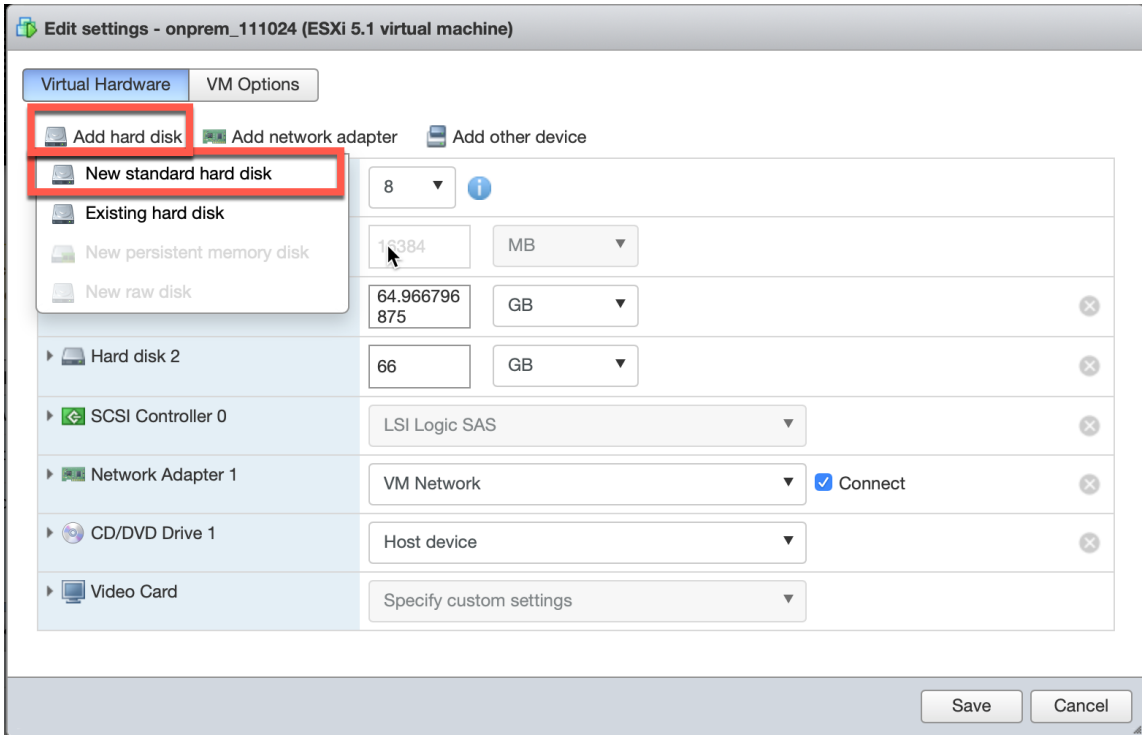

 

### Agregar un disco nuevo en el servidor ESXi

1. Inicie sesión en su servidor ESXi y seleccione la máquina virtual. Haga clic en **Edit**.



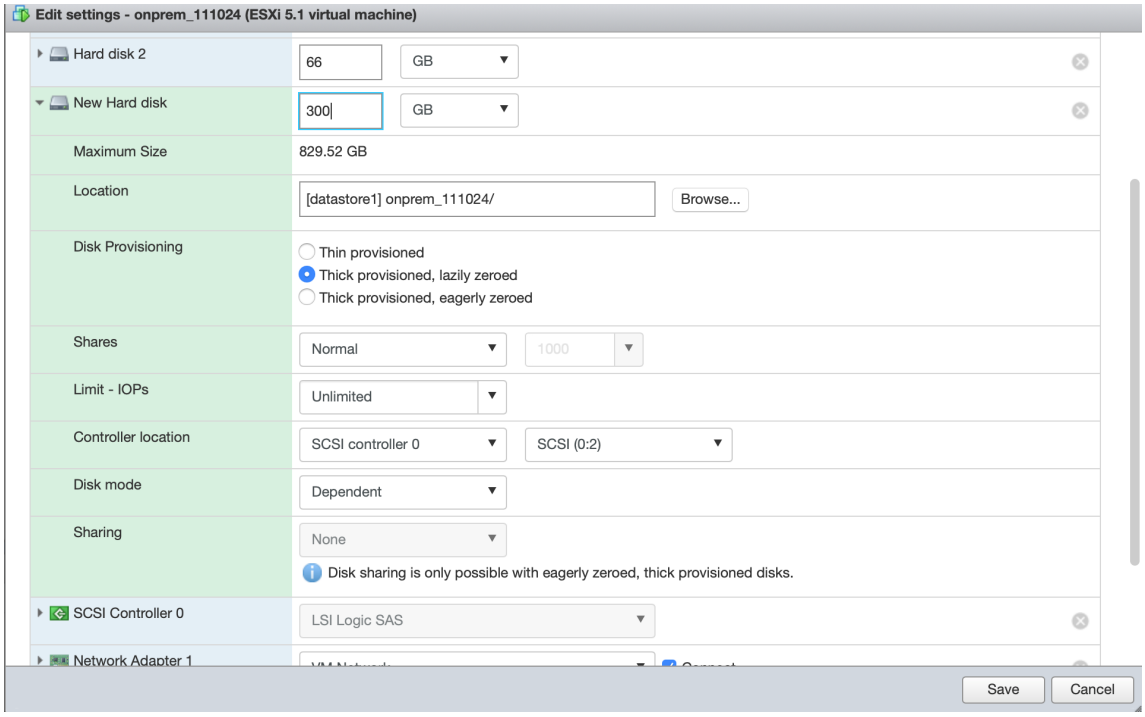

2. Haga clic en **Agregar disco duro > Nuevo disco duro estándar**.



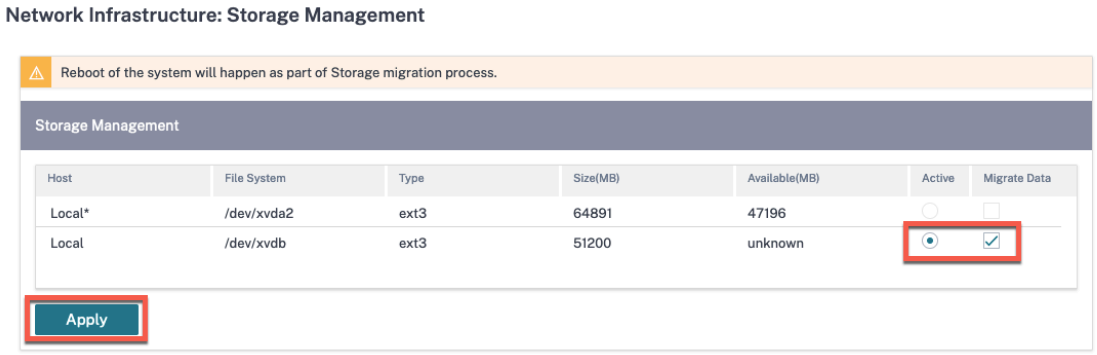

3. Introduzca el espacio de almacenamiento en disco y otros ajustes según sus preferencias. Haga clic en **Guardar**.

> **NOTA**
>
> El tamaño del disco debe ser al menos el doble del de los datos actuales que consume el Citrix SD-WAN Orchestrator for On-premises.

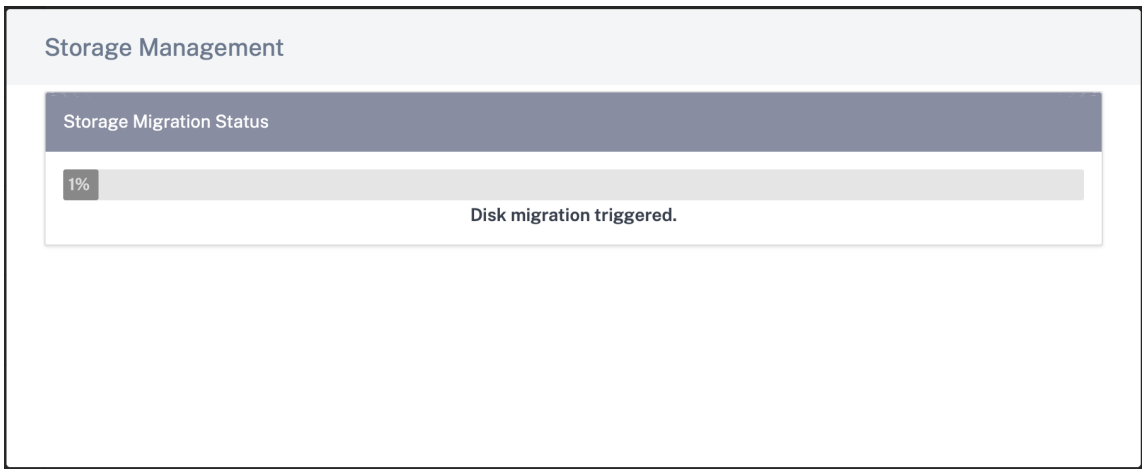


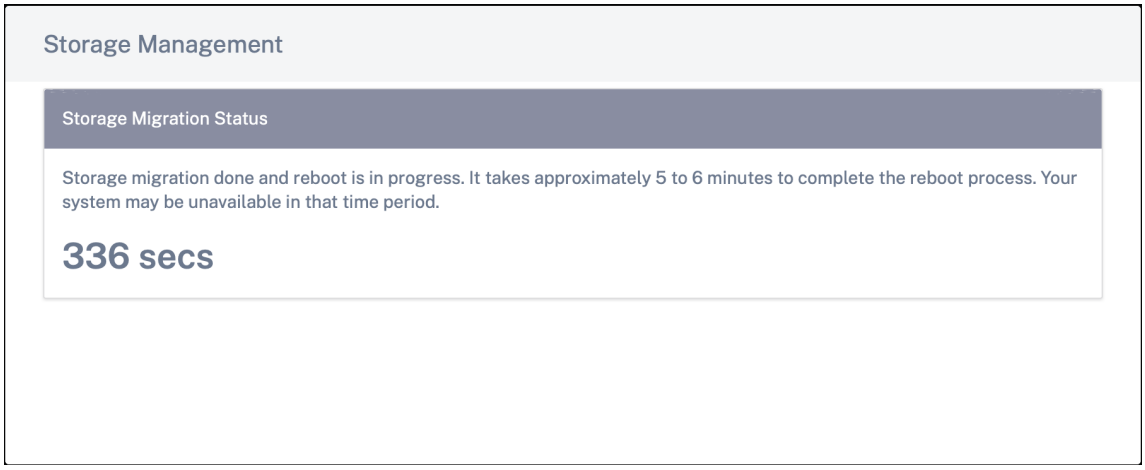

4. Inicie sesión en Citrix SD-WAN Orchestrator for On-premises y vaya a **INFRASTRUCTURE > Orchestrator Administration > Storage Management**. El disco recién conectado aparece aquí.
5. Seleccione el botón de opción **Activo** y seleccione la casilla **Migrar datos**. Haga clic en **Aplicar**.




6. Se activa el proceso de migración del disco. Las configuraciones del cliente, la base de datos local, la versión de lanzamiento de Citrix SD-WAN y las estadísticas de la base de datos del disco existente se migran al nuevo disco. Una vez completada la migración, se reinicia Citrix SD-WAN Orchestrator for On-premises.

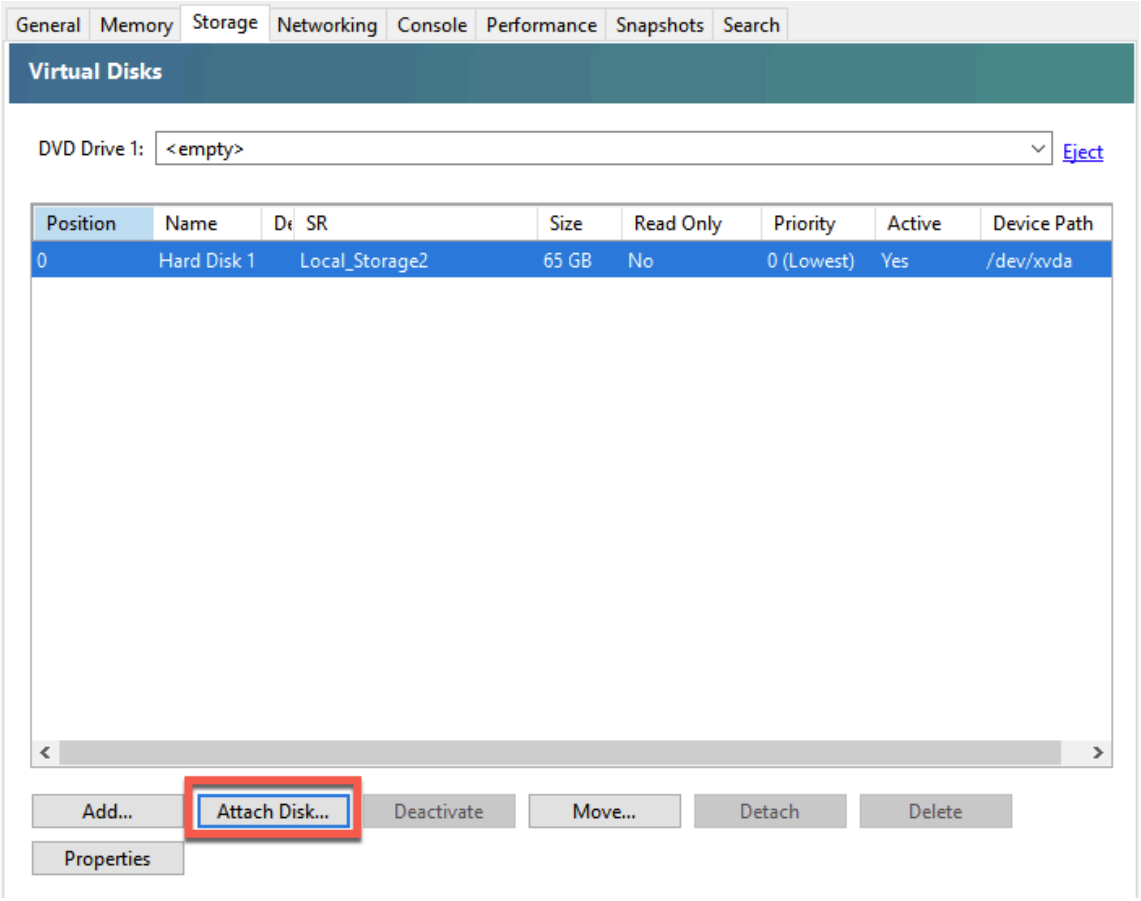



**Recuperación ante desastres en Citrix Hypervisor**

1. Seleccione la máquina virtual (VM) en el hipervisor. Seleccione la ficha **Almacenamiento** y haga clic en **Adjuntar disco**.

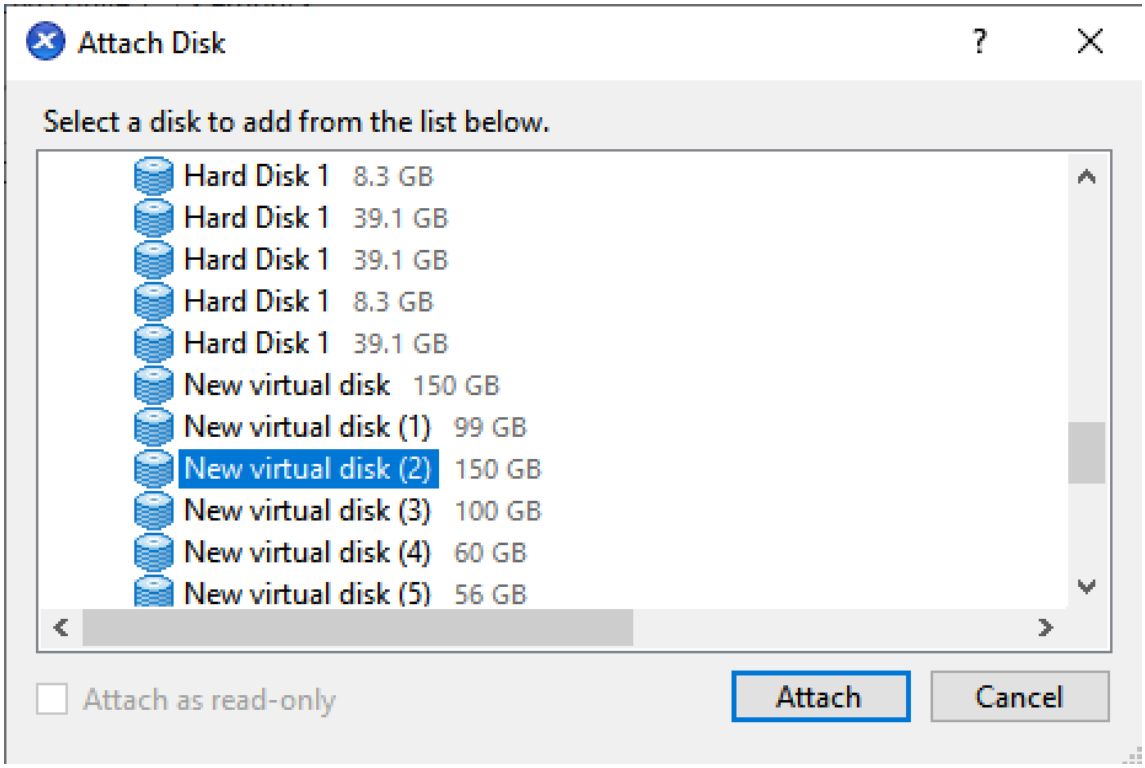
 




2. Seleccione el disco conectado al Citrix SD-WAN Orchestrator for On-premises que se produjo un desastre y haga clic en **Adjuntar**.

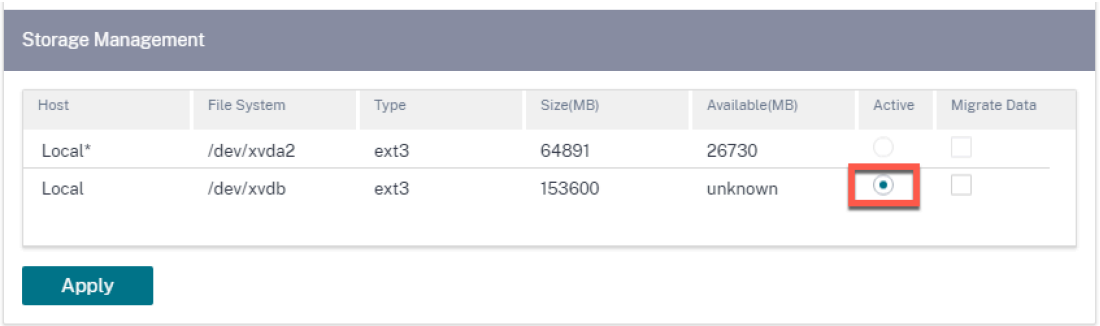
   Si el disco no aparece en la lista, asegúrese de que el disco conectado a Citrix SD-WAN Orchestrator for On-premises en caso de desastre esté desconectado y de que Citrix SD-WAN Orchestrator para locales esté en estado apagado.



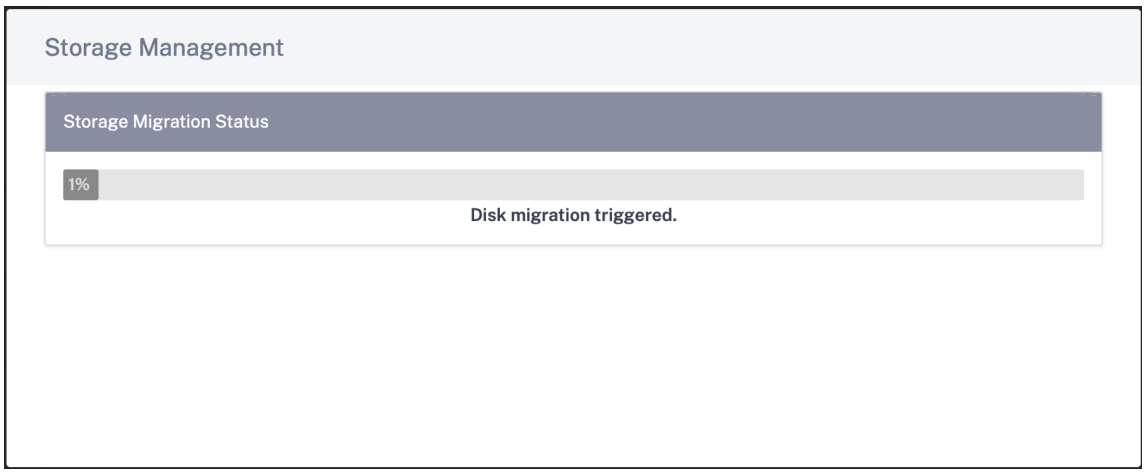

3. Inicie sesión en la interfaz de usuario local de Citrix SD-WAN Orchestrator y vaya a **INFRAESTRUCTURE > Orchestrator Administration > Storage Management**. El disco recién conectado aparece aquí.
4. Seleccione únicamente el botón de opción **Activo** (desactive la casilla **Migrar datos** si está seleccionada) y haga clic en **Aplicar**.

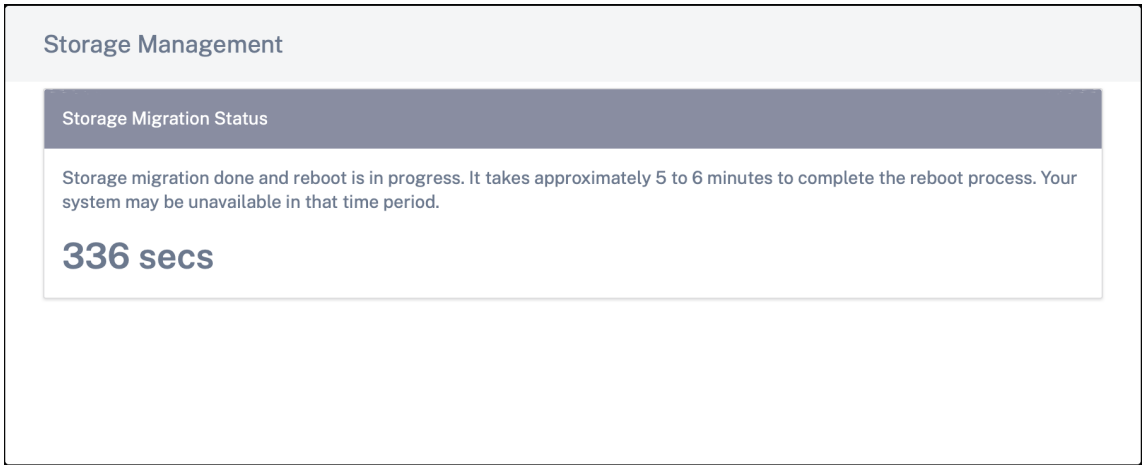
> **Nota**
>
> No active la casilla **Migrar datos**. Citrix SD-WAN Orchestrator for On-premises activa la migración en el back-end y se reinicia automáticamente una vez que se completa la migración.




5. Una vez completada la migración, se reinicia Citrix SD-WAN Orchestrator for On-premises.

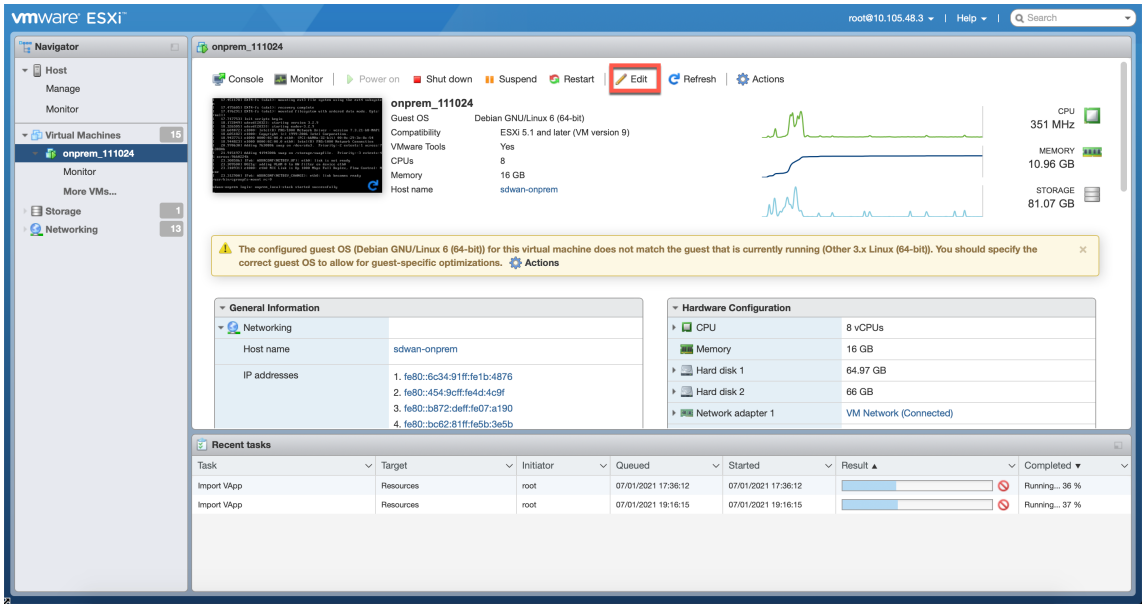


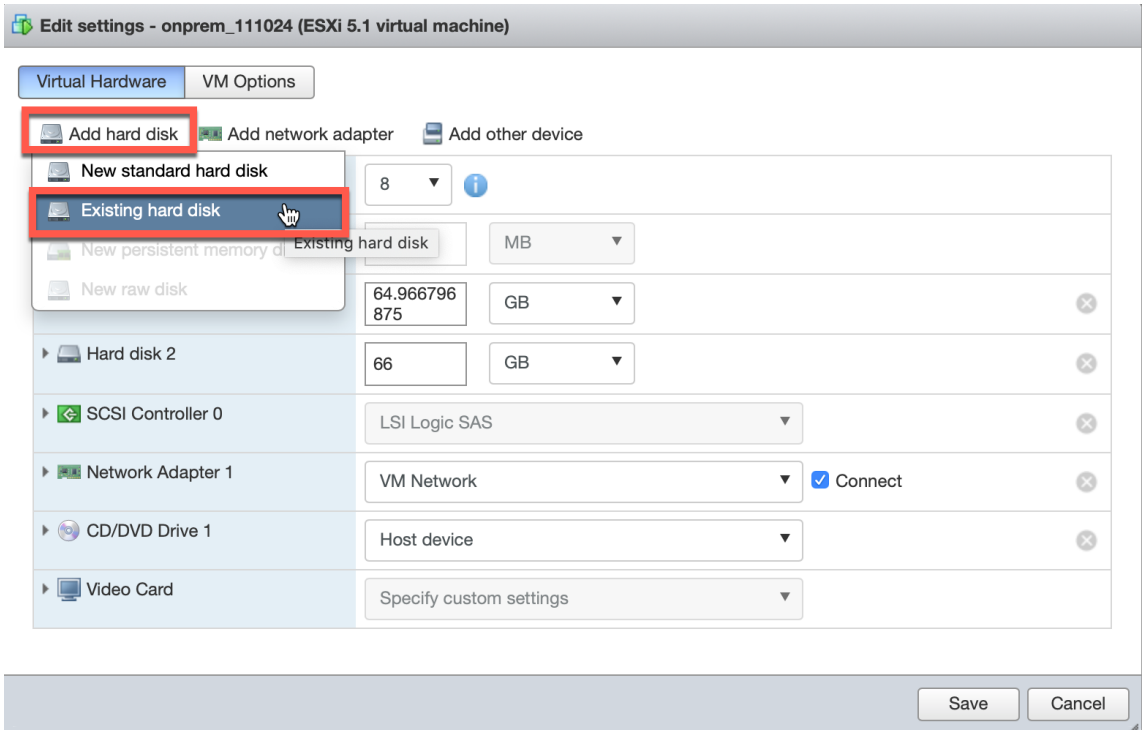

**Recuperación ante desastres en el servidor ESXi**

1. Inicie sesión en el servidor ESXi y seleccione la máquina virtual. Haga clic en **Edit**.

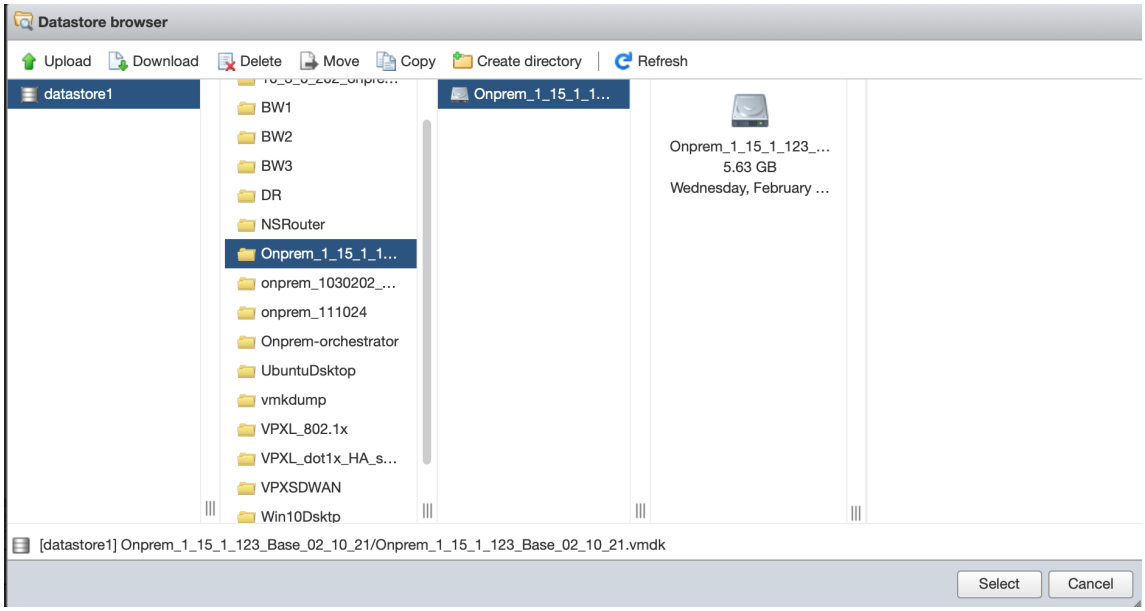



2. Haga clic en **Agregar disco duro > Disco duro existente**.



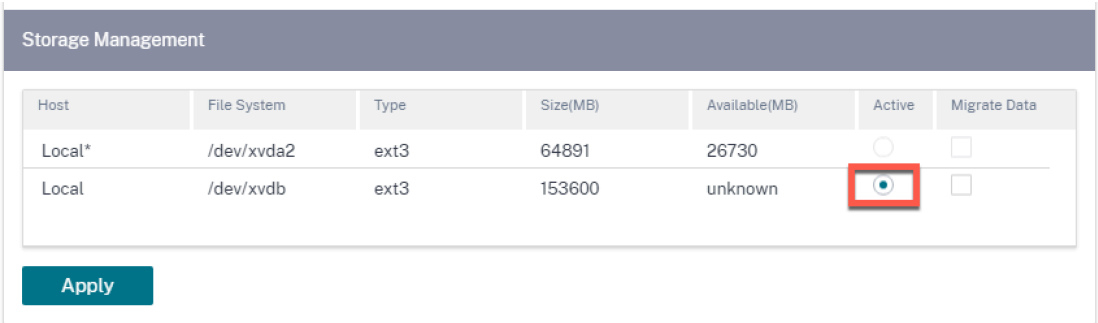

3. Busque el disco conectado al Citrix SD-WAN Orchestrator for On-premises que se produjo un desastre y haga clic en **Seleccionar**.



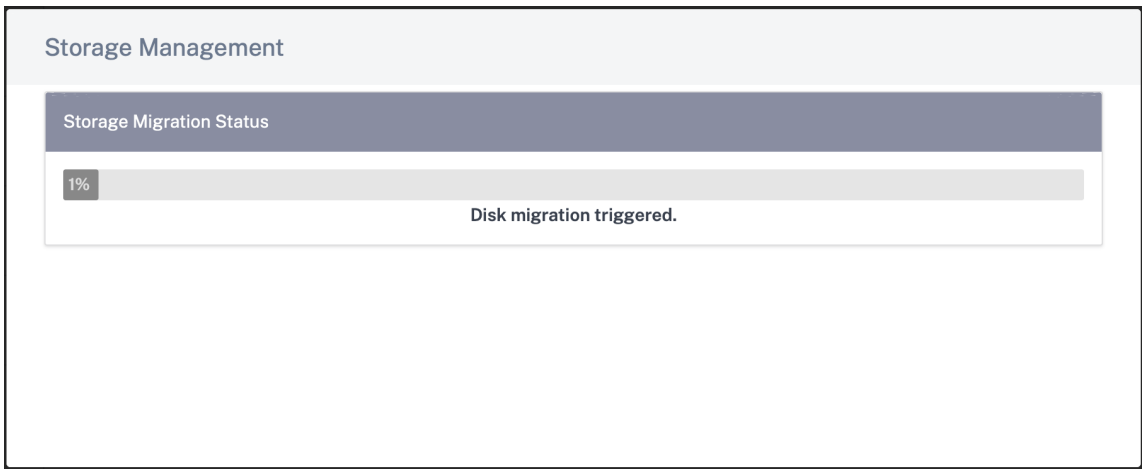

4. Inicie sesión en la interfaz de usuario local de Citrix SD-WAN Orchestrator y vaya a **INFRAESTRUCTURE > Orchestrator Administration > Storage Management**. El disco recién conectado aparece aquí.
5. Seleccione únicamente el botón de opción **Activo** (desactive la casilla **Migrar datos** si está seleccionada) y haga clic en **Aplicar**.

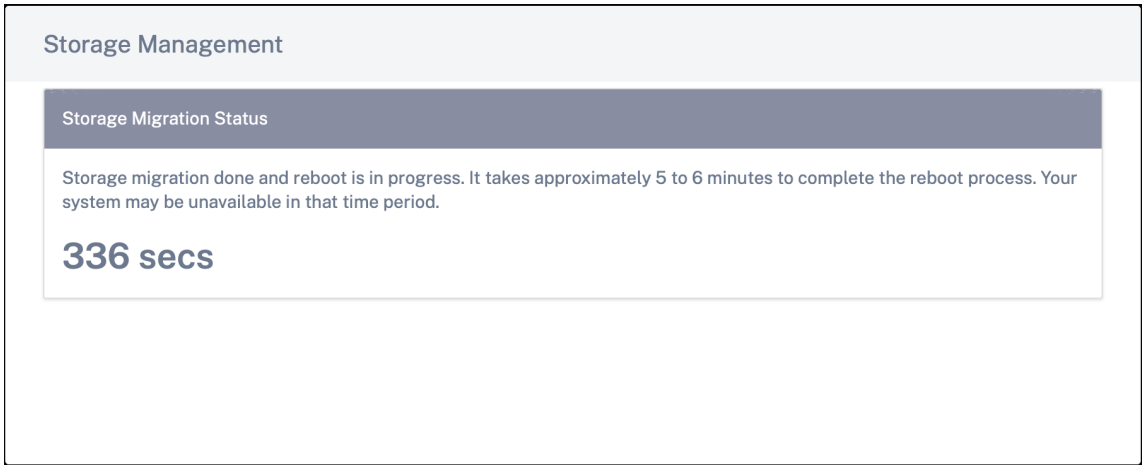
> **Nota**
>
> No active la casilla **Migrar datos**. Citrix SD-WAN Orchestrator for On-premises activa la migración en el back-end y se reinicia automáticamente una vez que se completa la migración.




6. Una vez completada la migración, se reinicia Citrix SD-WAN Orchestrator for On-premises.




## Proxy HTTP

Citrix SD-WAN Orchestrator for On-premises requiere una conexión a Internet para obtener licencias, iniciar sesión en la nube, ZTD negociado en la nube, Cloud direct y publicar software. Si Citrix SD-WAN Orchestrator for On-premises está conectado a Internet a través de un servidor proxy HTTP, puede configurar los ajustes del servidor proxy HTTP en su máquina virtual Citrix SD-WAN Orchestrator for On-premises.

La configuración del proxy HTTP centraliza la administración de todas las solicitudes salientes realizadas a Citrix Cloud. Los administradores pueden dirigir las solicitudes salientes desde Citrix SD-WAN Orchestrator for On-premises a Citrix Cloud a través de un servidor proxy HTTP.

### Antes de comenzar

Para usar el proxy HTTP para iniciar sesión en la nube por primera vez, debe configurar la configuración del proxy HTTP a través de la consola CLI de Citrix SD-WAN Orchestrator for On-premises.

En la página de inicio de sesión en la nube de una nueva máquina virtual Citrix SD-WAN Orchestrator para locales, si quiere que se utilice un proxy HTTP para todas las conexiones salientes desde Citrix SD-WAN Orchestrator for On-premises al servicio Citrix SD-WAN Orchestrator, debe configurar los detalles del proxy HTTP mediante la CLI. Una vez que haya completado el inicio de sesión en la nube y acceda a la página de configuración, podrá configurar los detalles del servidor proxy HTTP en la interfaz de usuario.

#### Configuración de la configuración del proxy HTTP en la CLI

Configure los ajustes del proxy HTTP ejecutando el comando `set_http_proxy`. Puede configurar el proxy HTTP mediante cualquiera de las opciones que se proporcionan a continuación:

- Cuando la autenticación está habilitada en el servidor proxy:

  ```
  set <ip address> <port> <user name> <password>
  ```

- Si la autenticación no está habilitada en el servidor proxy:

  ```
  set <ip address> <port>
  ```

#### Mostrar la configuración del proxy HTTP

- `show`: Este comando muestra la configuración del proxy en la CLI. El resultado no muestra la contraseña.

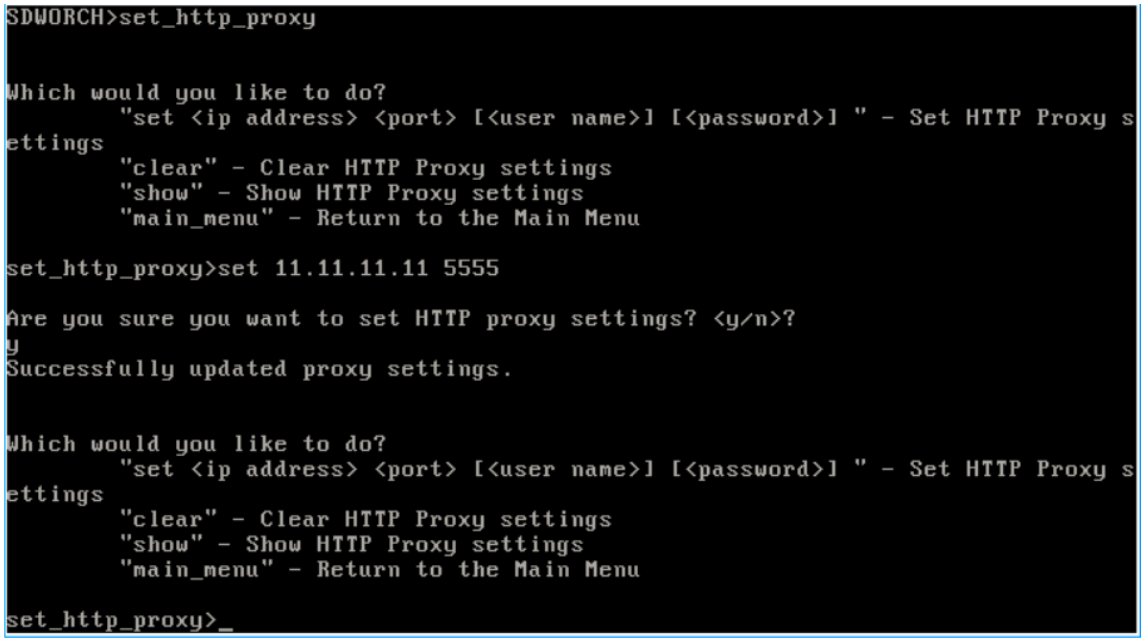
#### Borrar la configuración del proxy HTTP

- `clear`: Este comando elimina la configuración del proxy HTTP.

#### Volver al menú principal

- `main_menu`: Este comando lo redirige a la consola de CLI de Citrix SD-WAN Orchestrator for On-premises.




**Configurar los ajustes del servidor proxy HTTP en la interfaz de usuario**

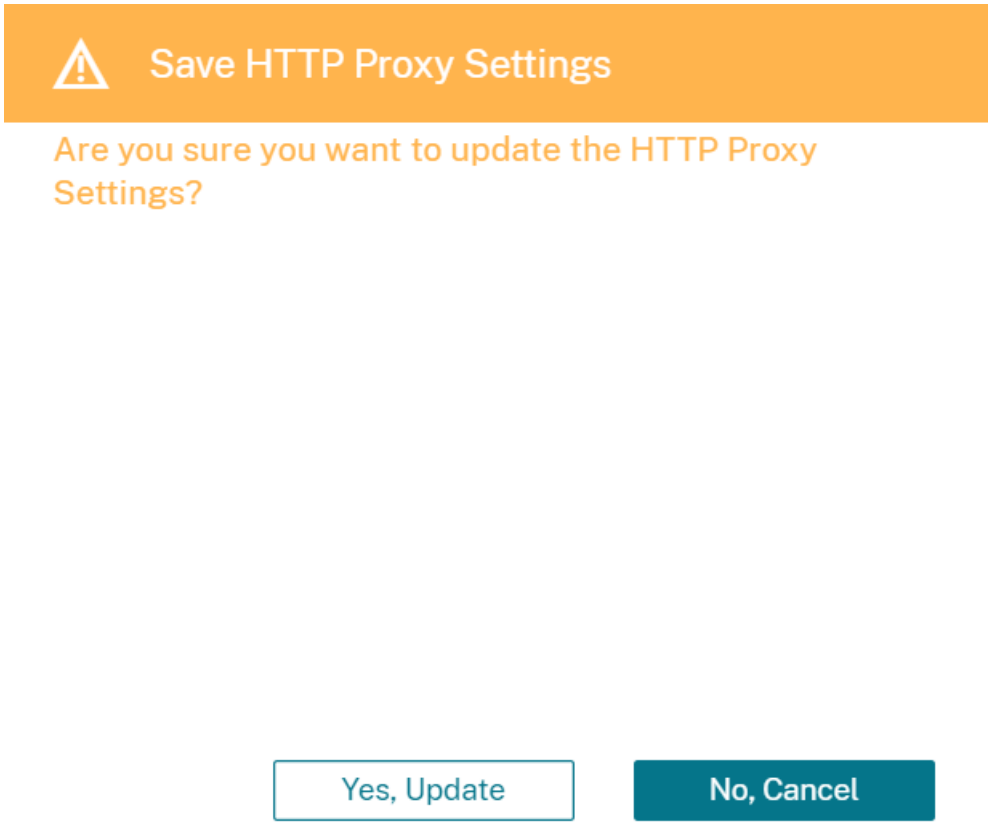
1. Inicie sesión en la interfaz de usuario de Citrix SD-WAN Orchestrator for On-premises y vaya a **Infraestructura** > **Administración de Orchestrator** > **Proxy HTTP**.
2. En la sección **Infraestructura de red: Proxy HTTP**, introduzca valores para los siguientes campos:

   - **Dirección IP**: La dirección IP del servidor proxy.
   - **Puerto**: El número de puerto de red en el que el servidor proxy acepta las conexiones.
   - **Nombre**de usuario: Nombre de usuario del servidor proxy.
   - **Contraseña**: La contraseña del servidor proxy.

   > **Nota:**
   >
   > Puede dejar los campos Nombre de usuario y Contraseña en blanco si no hay ninguna autenticación configurada en el servidor proxy.


3. Haga clic en Aplicar. Aparecerá un cuadro de diálogo de confirmación.
4. Haga clic en Sí, actualizar.




**Notas**

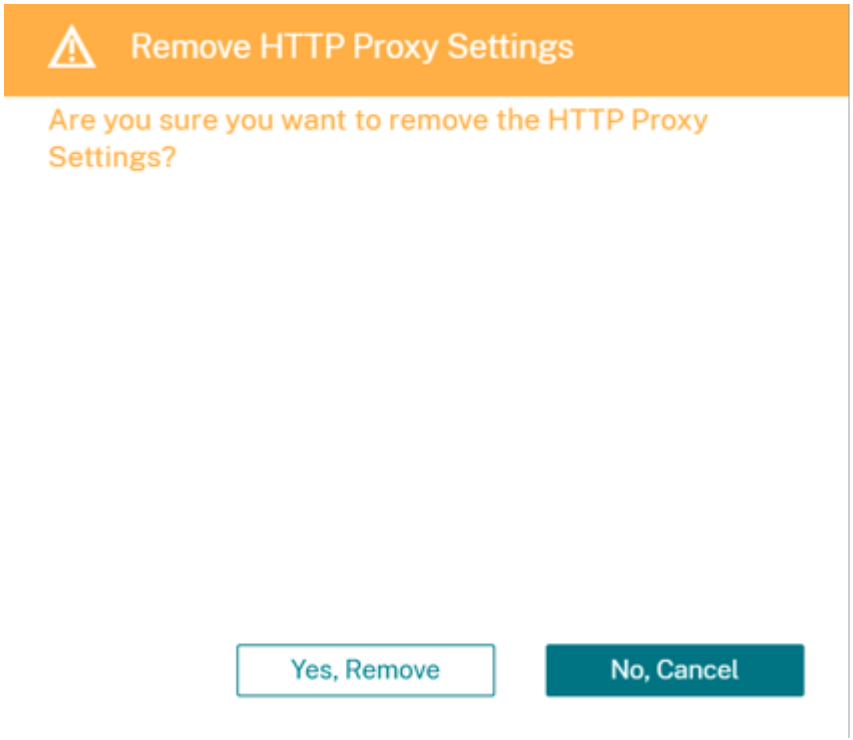
- Para usar el servidor proxy HTTP para el tráfico saliente de Citrix SD-WAN Orchestrator for On-premises a Citrix Cloud, el servidor proxy debe configurarse como un proxy

> HTTP SSL transparente o un servidor proxy HTTP de omisión SSL. El servidor no debe falsificar el certificado SSL del servicio Citrix SD-WAN Orchestrator.
> - Puede eliminar la configuración del servidor proxy por completo si Citrix SD-WAN Orchestrator for On-premises está conectado directamente a Internet. También puede eliminar la configuración del servidor proxy y configurar otro servidor proxy, si es necesario.

**Eliminar la configuración del servidor proxy en la interfaz de usuario**

1. En la interfaz de usuario de Citrix SD-WAN Orchestrator for On-premises, vaya a **Infraestructura** > **Administración de Orchestrator** > **Proxy HTTP**.
2. En la sección **Infraestructura de red: Proxy HTTP**, haga clic en **Eliminar**. Aparecerá un cuadro de diálogo de confirmación.
3. Haga clic en **Sí, quitar**.




## Configuración de purga

Puede borrar las estadísticas o los datos históricos de un intervalo de tiempo seleccionado. Se borran las estadísticas o los datos más antiguos que los días establecidos. Una vez que se borran los datos, dejan de estar disponibles. De forma predeterminada, Citrix SD-WAN Orchestrator for On-premises borra las estadísticas o los datos históricos de más de 30 días.

A nivel de red, vaya a **Infraestructura** > **Administración de Orchestrator** > **Configuración de purga**, seleccione el intervalo de tiempo y haga clic en **Aplicar**. Por ejemplo, si quiere purgar estadísticas o datos históricos de más de 180 días, seleccione 180 en la lista desplegable **Intervalo de estadísticas de purga (días)** y haga clic en **Aplicar**. El proceso de purga se realiza alrededor de las 12:48 a. m., todos los días, en la zona horaria establecida en el dispositivo SD-WAN.


## Diagnóstico del orquestador

October 31, 2022

Esta sección proporciona información sobre las actividades de diagnóstico que se pueden realizar en Citrix SD-WAN Orchestrator para la infraestructura local.

> **Nota**
>
> En una configuración administrada por un proveedor, los administradores de los proveedores tienen acceso a todas las páginas de la GUI **Infraestructura > Diagnóstico de orquestador**. Los administradores de clientes solo tienen acceso para ver **los eventos y registros** de la **plataforma y las páginas de la GUI de estado**

### Eventos y registros de la plataforma

Cualquier cambio en los atributos al nivel de plataforma, como la CPU, la memoria o el almacenamiento en el sistema, se registra como un evento y se muestra en Citrix SD-WAN Orchestrator for On-premises.

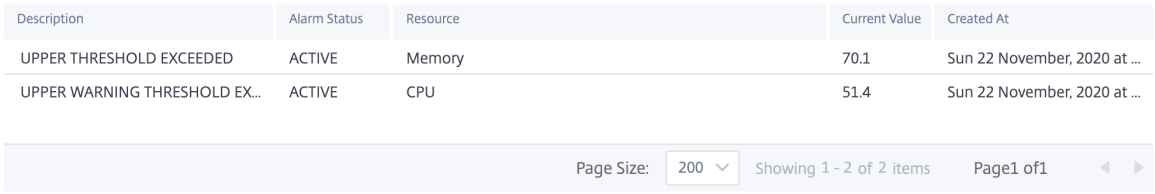
Por ejemplo, si el uso de la CPU supera el límite establecido, se registra un evento de plataforma y se activa una alarma. La alarma aparece en la barra de notificaciones. La notificación se borra si se reduce el uso de la CPU. La página **Eventos y registros de la plataforma** mantiene el historial de todas las alarmas relacionadas con la plataforma que se activaron. Si el uso de la CPU disminuye, el estado de alarma pasa a ser INACTIVO. Si aún está por encima de los límites, el estado de la alarma permanece ACTIVO.

Para ver los eventos de la plataforma, vaya a **Infraestructura** > **Diagnósticos de Orchestrator** > **Eventos y registros de la plataforma**.

Se muestran los siguientes detalles de los eventos de plataforma registrados:

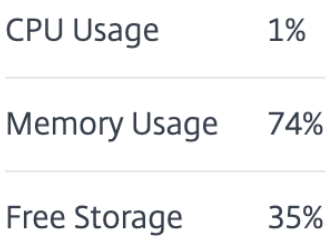
- **Descripción**: La descripción del evento de la plataforma.
- **Estado de alarma**: Estado de la alarma. Si el atributo de plataforma supera el límite establecido, el estado es ACTIVO. Si el atributo de nivel de plataforma disminuye a un valor dentro del límite establecido, el estado de la alarma es INACTIVA.
- **Recurso**: El atributo de nivel de plataforma: CPU, memoria o almacenamiento.
- **Valor actual**: El valor más reciente del atributo de plataforma registrado.
- **Creado en**: El momento en que se produjo el evento de la plataforma.




## Estado de la plataforma

Puede ver el estado de la plataforma Citrix SD-WAN Orchestrator for On-premises. La información de estado incluye valores en tiempo real (en porcentaje) del uso de la CPU, el uso de la memoria y el almacenamiento gratuito disponible.

Para ver el estado de la plataforma, vaya a **Infraestructura > Diagnóstico de Orchestrator > Estado de la plataforma**.



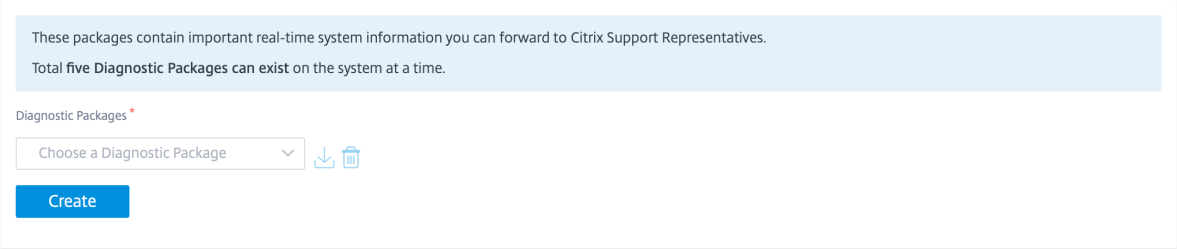

 

### Información de diagnóstico

Un paquete de diagnóstico consta de archivos de registro del sistema, información del sistema y otros detalles necesarios que ayudan al equipo de soporte a diagnosticar y resolver problemas con el sistema.

Para crear un paquete de diagnóstico, vaya a **Infraestructura** > **Diagnóstico de Orchestrator** > **Información de diagnóstico**. Haga clic en **Crear**. Una vez creado el paquete, puede descargarlo a su equipo y compartirlo con el equipo de asistencia.

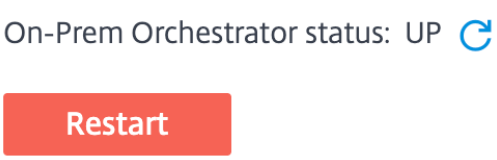
> **NOTA**
>
> Citrix SD-WAN Orchestrator for On-premises puede almacenar un máximo de cinco paquetes de diagnóstico a la vez.




### Reinicie la aplicación Citrix SD-WAN Orchestrator for On-premises

Solo puede reiniciar la aplicación Citrix SD-WAN Orchestrator for On-premises sin reiniciar el sistema operativo (SO). Durante el reinicio, la aplicación Citrix SD-WAN Orchestrator for On-premises se desconecta y todos los servicios dejan de estar disponibles. El reinicio tarda aproximadamente 6 minutos en completarse. Tras el reinicio, aparece la página de inicio de sesión de Citrix SD-WAN Orchestrator for On-premises.

Para reiniciar la aplicación Citrix SD-WAN Orchestrator for On-premises, vaya a **Infraestructura > Diagnóstico de Orchestrator > Reiniciar la aplicación Orchestrator**. Haga clic en **Reiniciar** y **Sí, reiniciar** para confirmar.



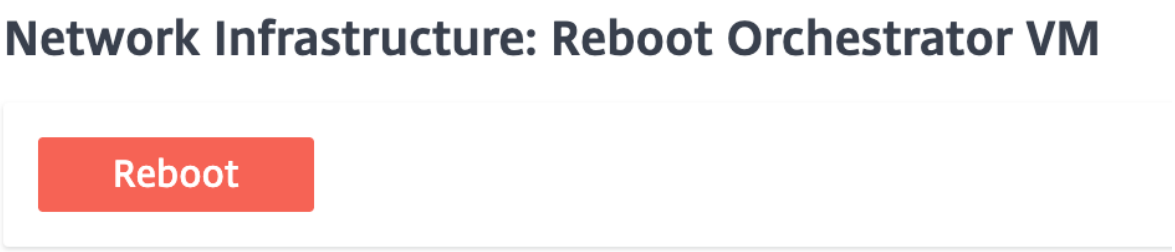

 

### Reinicie Citrix SD-WAN Orchestrator para una máquina virtual local

El proceso de reinicio reinicia el sistema operativo (SO) de Citrix SD-WAN Orchestrator for On-premises. Durante el reinicio, Citrix SD-WAN Orchestrator for On-premises se desconecta y todos los servicios dejan de estar disponibles. El reinicio tarda aproximadamente de 6 a 8 minutos en completarse. Tras el reinicio, aparece la página de inicio de sesión de Citrix SD-WAN Orchestrator for On-premises.

Puede reiniciar Citrix SD-WAN Orchestrator for On-premises como parte de una actividad de solución de problemas o durante una actividad de mantenimiento.

Para reiniciar, vaya a **Infraestructura > Diagnóstico de Orchestrator > Reiniciar máquina virtual de Orchestrator**. Haga clic en **Reiniciar** y **Sí, reiniciar** para confirmar.




## Alarmas

October 31, 2022

Puede ver las alarmas específicas de la plataforma y del servicio asociadas a Citrix SD-WAN Orchestrator for On-premises. Las alarmas específicas de la plataforma muestran alertas relacionadas con la plataforma, como problemas de almacenamiento, RAM o CPU. Las alarmas de servicio muestran el estado de los microservicios que se ejecutan en Citrix SD-WAN Orchestrator for On-premises.

Para ver las alarmas, haga clic en el icono de campana en la esquina superior derecha de la interfaz de usuario de Citrix SD-WAN Orchestrator for On-premises y seleccione Alarmas de **plataforma o Alarmas** de **servicio**, según sea necesario.