Citrix SD-WAN Orchestrator für Lokal 14.3

Contents

Versionshinweise für SD-WAN Orchestrator for On-premises 14.3

October 21, 2022

In diesem Dokument mit den Versionshinweisen werden die Verbesserungen und Änderungen sowie behobenen und bekannten Probleme beschrieben, die für den Citrix SD-WAN Orchestrator for On-Premises-Version Build 14.3 bestehen.

Hinweise

Dieses Dokument mit Versionshinweisen enthält keine sicherheitsbezogenen Fixes. Eine Liste der sicherheitsbezogenen Fixes und Advisorys finden Sie im Citrix Security Bulletin.

Neuigkeiten

Die Erweiterungen und Änderungen, die in Build 14.3 verfügbar sind.

Konfiguration und Management

QoS-Richtlinien

Die Seite mit den QoS-Richtlinien wurde überarbeitet, um die Benutzererfahrung zu verbessern. Die Optionen wie benutzerdefinierte Anwendungsregeln, Anwendungsregeln, HDX-Regeln, Anwendungsgruppenregeln, IP-Regeln und Standard-IP-Protokollregeln wurden um ein neues Erscheinungsbild erweitert.

[SDW-11029]

Plattform und Systeme

Verbesserungen der IP-/In-Band-IP-Verwaltung:

Die Spalten **Management-IP** und **Gerätezugriff** auf den folgenden Benutzeroberflächenbildschirmen wurden erweitert, sodass entweder die In-Band-IP-Adresse oder die Verwaltungs-IP-Adresse basierend auf dem Typ der IP-Adresse angezeigt wird, die das Gerät für die Kommunikation mit Citrix SD-WAN Orchestrator for On-premises verwendet:

- Anbieter > Berichterstattung > Bestand > Details
- Kunde > Konfiguration > Netzwerkstartseite > Aktionen > Details anzeigen
- Kunde > Berichterstattung > Bestand > Details

- Seite > Dashboard > Geräte

[SDW-23353]

Bericht als CSV exportieren

Mit der Funktion **Als CSV exportieren** können Sie die Pfaddiagrammpunkte (virtueller/Mitgliedspfad) für jede Zeitreihe (stündlich, wöchentlich usw.) als Excel-Datei mit kommagetrennten Werten (CSV) herunterladen und alle eindeutigen Datenpunkte für einen bestimmten Standortbericht darstellen.

[SDW-20988]

Zertifikatauthentifizierung

Citrix SD-WAN Orchestrator for On-premises unterstützt die Appliance-Authentifizierung für statische und dynamische virtuelle Pfade mithilfe der Public Key Infrastructure (PKI) als zusätzliches Sicherheitsfeature. Durch Aktivieren der Funktion wird der vorhandene Authentifizierungsmechanismus für virtuelle Pfade erweitert, indem PKI-Zertifikate über den Datenpfad durch die Appliance verteilt werden, die den Austausch initiiert. Die PKI-Erweiterung unterstützt auch die Verwaltung der Zertifikatsperrliste (Certificate Revocation List, CRL) für die zentrale Sperrung gefährdeter Zertifikate.

[SDW-19295]

SD-WAN Orchestrator

Konfiguration anzeigen (Vorschau)

Citrix SD-WAN Orchestrator for On-premises führt die Seite **„Konfiguration anzeigen** “auf Site-Ebene ein. Diese Seite bietet eine detaillierte Zusammenfassung der Konfiguration einer Site über mehrere Subsysteme hinweg.

[SDW-22284]

Echtzeitstatistiken aufNetzwerkebene, Echtzeitstatistikenauf Standortebene

Die **Firewall-Verbindung** wurde jetzt in **Firewall-Statistik**umbenannt. NAT- und Filterrichtlinien wurden in der Dropdownliste Statistiktyp neu hinzugefügt. Außerdem wurden die Echtzeit-Statistikoptionen neu strukturiert und in die folgenden Kategorien unterteilt:

- Netzwerk-Statistiken
- Anwendungsstatistiken
- Routenstatistik

[SDW-20966]

Einstellungen für mobiles Breitband und Status des mobilen Breitband

Sie können jetzt die Citrix SD-WAN-Appliance von Ihrem Standort aus über eine Breitband-Internetverbindung mit einem Netzwerk verbinden. Diese Unterstützung für Status und Konfiguration von mobilem Breitband ist für interne Modems verfügbar. Sie können auch den Status der Breitbandkonfiguration Ihres Geräts und der aktiven SIM-Karte anzeigen.

[SDW-10907]

Behobene Probleme

Die Probleme, die in Build 14.3 angesprochen werden.

Konfiguration und Management

Das PKI-Zertifikat wurde nicht auf der Benutzeroberfläche von Citrix SD-WAN Orchestrator for On-premises angezeigt. Dieses Problem trat auf, weil das Feld **Organisationseinheit** im PKI-Zertifikat obligatorisch war.

[SDW-23726]

Sonstiges

Einige Sites können keine Verbindung zur Citrix SD-WAN Orchestrator for On-Premises-Benutzeroberfläche herstellen.

[DWANHELP-2601]

Bekannte Probleme

Die Probleme, die in Version 14.3 bestehen.

Die Diagramme Anwendungen und Anwendungskategorien sind auf der Seite **Berichte** > **Verwendung** > **Anwendungen** der Citrix SD-WAN Orchestrator for On-Premises-Benutzeroberfläche leer.

[SDW-23817]

Die zuvor auf der Seite **Bereitstellung** > **Einstellungen** > **Teilweise Site-Aktualisierung** > **Softwareversion** der Benutzeroberfläche ausgewählte Softwareversion wird nicht beibehalten, wenn die Benutzer zu dieser Seite zurückkehren.

Problemumgehung: Wählen Sie die Softwareversion für partielle Site-Upgrades manuell für jede Site aus, indem Sie auf Navigieren zu **Bereitstellung** > **Sites auswählen**klicken.

[SDW-22374]

Manchmal zeigt die Benutzeroberfläche einen Fehler an, nachdem eine Konfiguration der Einstellungen der Verwaltungsschnittstelle durchgeführt wurde. Die Konfiguration ist jedoch erfolgreich und eine Aktualisierung ist erforderlich, damit die aktualisierten Einstellungen auf der Benutzeroberfläche angezeigt werden.

[SDW-22139]

In einem vom Anbieter verwalteten Setup werden die von den Anbieteradministratoren hinzugefügten Ankündigungen den Kunden bei ihrer Anmeldung nicht angezeigt.

[SDW-18491]

Versionshinweise für SD-WAN Orchestrator for On-premises 13.2.1

October 21, 2022

In diesem Dokument mit den Versionshinweisen werden die Verbesserungen und Änderungen sowie behobenen und bekannten Probleme beschrieben, die für den Citrix SD-WAN Orchestrator for On-Premises-Version Build 13.2.1 bestehen.

Hinweise

Dieses Dokument mit Versionshinweisen enthält keine sicherheitsbezogenen Fixes. Eine Liste der sicherheitsbezogenen Fixes und Advisorys finden Sie im Citrix Security Bulletin.

Behobene Probleme

Die Probleme, die in Build 13.2.1 angesprochen werden.

Plattform und Systeme

Citrix SD-WAN Orchestrator for On-premises sendet TCP-Synchronisationspakete an den AWS-Endpunkt.

[SDW-23477]

Bekannte Probleme

Die Probleme, die in Version 13.2.1 bestehen.

Sonstiges

Einige Sites können keine Verbindung zur Citrix SD-WAN Orchestrator for On-Premises-Benutzeroberfläche herstellen.

Problemumgehung: Verwenden Sie ein anderes Subnetz als das 172.17.x.x-Subnetz.

[DWANHELP-2601]

In einigen Szenarien wird der Cloud Direct Service nach der Bereitstellung von Cloud Direct für die Sites und dem Pushen der Konfigurationen (Staging und Aktivierung) nicht angezeigt.

Problemumgehung: Aktivieren Sie den Cloud Direct Service manuell für jede Site.

[SDW-22493]

Die zuvor auf der Seite **Bereitstellung** > **Einstellungen** > **Teilweise Site-Aktualisierung** > **Softwareversion** der Benutzeroberfläche ausgewählte Softwareversion wird nicht beibehalten, wenn die Benutzer zu dieser Seite zurückkehren.

Problemumgehung: Wählen Sie die Softwareversion für das partielle Site-Upgrade manuell für jede Site aus, indem Sie zu **Bereitstellung** > **Sites auswählen**navigieren.

[SDW-22374]

Manchmal zeigt die Benutzeroberfläche einen Fehler an, nachdem eine Konfiguration der Einstellungen der Verwaltungsschnittstelle durchgeführt wurde. Die Konfiguration ist jedoch erfolgreich und eine Aktualisierung ist erforderlich, damit die aktualisierten Einstellungen auf der Benutzeroberfläche angezeigt werden.

[SDW-22139]

In einem vom Anbieter verwalteten Setup werden die von den Anbieteradministratoren hinzugefügten Ankündigungen den Kunden bei ihrer Anmeldung nicht angezeigt.

[SDW-18491]

Plattform und Systeme

Auf die Benutzeroberfläche einer der Citrix SD-WAN-Appliances kann nicht zugegriffen werden, da der Netzwerkstatistikanbieter eine Sitzung wiederverwendet und dies dazu führte, dass sich der HTTPD-Prozess (in seltenen Fällen) nicht ordnungsgemäß verhält.

[SDW-23392]

Wenn Sie auf der Citrix SD-WAN 210-Appliance die SE-Zusatzlizenz entfernen, werden die Dienste deaktiviert.

Problemumgehung: Bevor Sie eine SE-Zusatzlizenz entfernen (oder) von einer AE- zu einer SE-Lizenz wechseln, entfernen Sie die Firewall-Richtlinien mit dem Sicherheitsprofil, konfigurieren Sie die Appliance als Out-of-Band-Verwaltung (wenn die In-Band-Verwaltung konfiguriert ist) und fahren Sie dann mit der Phase und dem Aktivierungsprozess fort konvertieren Sie die Appliance auf die Standardversion.

[SDW-18031]

Versionshinweise für SD-WAN Orchestrator for On-premises Version 13.2

October 21, 2022

In diesem Dokument mit den Versionshinweisen werden die Verbesserungen und Änderungen sowie behobenen und bekannten Probleme beschrieben, die für den Citrix SD-WAN Orchestrator for On-Premises-Version Build 13.2 bestehen.

Hinweise

Dieses Dokument mit Versionshinweisen enthält keine sicherheitsbezogenen Fixes. Eine Liste der sicherheitsbezogenen Fixes und Advisorys finden Sie im Citrix Security Bulletin.

Neuigkeiten

Die Erweiterungen und Änderungen, die in Build 13.2 verfügbar sind.

Konfiguration und Management

Vorgängerversion wiederherstellen

Citrix SD-WAN Orchestrator for On-premises führt die Funktion zum Wiederherstellen früherer Versionen ein. Wenn die Option **Vorherige Version wiederherstellen** ausgewählt ist, initiiert Citrix SD-WAN Orchestrator for On-premises eine netzwerkweite Aktivierung der vorherigen Konfiguration und stellt die zuvor aktivierte Konfiguration (/Software) in Ihrem Netzwerk wieder her.

[SDW-22042]

Verbesserungen bei der Lizenzierung

Nachdem die Lizenzen abgerufen und auf die Produktion aktualisiert wurden, ändert sich die Beschriftung der Schaltfläche Auf **Produktion aktualisieren** in Auf **Produktion aktualisiert**, was darauf hinweist, dass das Lizenzupgrade bereits abgeschlossen ist.

[SDW-20674]

API —Auflösung der Site-Adresse:

Wenn eine Site mithilfe einer API erstellt wird, wird die Site-Adresse automatisch anhand der Breiten- und Längengradwerte abgerufen, die im Rahmen der Site-Erstellung mithilfe der Google Maps-API übergeben werden.

[SDW-20654]

Umstrukturierung des Netzwerkmenüs

Das Menü Citrix SD-WAN Orchestrator for On-premises Global Configuration wurde umstrukturiert, um eine bessere Kategorisierung und Auffindbarkeit der wichtigsten Funktionen von Citrix SD-WAN zu ermöglichen. Außerdem ist jeder Delivery-Service jetzt sowohl in den Bereitstellungskanälen als auch auf jeder wichtigen Funktionsseite verfügbar, um die Admin-Konfiguration aus dem globalen oder pro Funktionskontext zu ermöglichen. Beispielsweise kann ein Administrator den Citrix SIA SIA-Dienst an Tag 0 global unter einem Bereitstellungskanal konfigurieren und unter Cloud Security Services auch Day N-Funktionen unter Sicherheit ausführen, um Änderungen vorzunehmen.

Die Konfigurationsseiten auf Netzwerkebene werden wie folgt erweitert:

- **Network Config Home** wurde in **Network Home**umbenannt.
- **Delivery Services** unter **Konfiguration > Bereitstellungskanäle** wurde jetzt in **Dienstdefinitionen**umbenannt.
- Unter **Konfiguration > Sicherheit**wird die Seite **Netzwerkverschlüsselung** in **Netzwerksicherheit**umbenannt.
- Die Seiten unter **Konfiguration > Sicherheit** sind zur leichteren Auffindbarkeit logisch wie folgt gruppiert:

Gruppe	Menüoptionen
SD-WAN-Overlay-Sicherheit	Netzwerksicherheit
	Virtueller Pfad IPSec
Basis-Firewall	Firewallzone
	Firewall-Standardeinstellungen
	Firewall-Richtlinien
IPSec & GRE	Zertifikate

Gruppe	Menüoptionen
	IPSec-Verschlüsselungsprofile
	IPSec-Dienst
	GRE-Dienst
Wi-Fi-Sicherheit	RADIUS-Profile
	SSID-Profile

- Sie können die folgenden Dienste entweder über **Konfiguration > Bereitstellungskanäle > Dienstdefinition** oder über **Konfiguration > Sicherheit**konfigurieren:
  - IPsec
  - GRE
- Die Seite **ECMP-Gruppen** wird unter **Konfiguration > Routing**verschoben.
- Sie können **BGP, OSPF, Multicast-Gruppen und VRRP** auf Netzwerkebene unter **Konfiguration > Routing**konfigurieren. Sie können eine Site auswählen und auf **Los**klicken. Sie gelangen auf die spezifische Konfigurationsseite auf Site-Ebene. Bisher waren diese Konfigurationen nur auf Standortebene verfügbar.
- Sie können den Cloud Direct Service entweder über **Konfiguration > Bereitstellungskanäle > Dienstdefinition** oder über **Konfiguration > Routing > SaaS & Cloud On Ramp**konfigurieren
- Die Seite **„Anwendungs- und DNS-Einstellungen** “wurde in **App-Einstellungen und Gruppen**umbenannt.
- DPI-bezogene Einstellungen, die zuvor unter **Konfiguration > App- und DNS-Einstellungen > Anwendungseinstellungen** standen, wurden unter **Konfiguration > App-Einstellungen & Gruppen > DPI-Einstellungen**verschoben.
- Die Seite**Network Location Service**, die sich unter **Konfiguration > Bereitstellungsdienste** befand, befindet sich direkt unter **Konfiguration.**

[SDW-14698]

Rollback bei Fehler

Während der Netzwerkbereitstellung (Aktivierung) werden Sites, die keine Verbindung zu Citrix SD-WAN Orchestrator for On-premises herstellen können, auf die vorherige Version zurückgesetzt, um zu versuchen, die Konnektivität wiederherzustellen. Rollback auf solchen Websites wird initiiert, nachdem er für eine bestimmte Zeit offline ist (derzeit 30 Minuten).

Wenn eine der Sites im Netzwerk versucht, ein Rollback durchzuführen, wird ein Popup-Fenster mit zwei Optionen angezeigt, mit denen Sie entweder das gesamte Netzwerk zurücksetzen oder diese Sites ignorieren und die Bereitstellung beenden können.

Die Funktion Rollback bei Fehler muss aktiviert sein, bevor eine Netzwerkbereitstellung initiiert wird.

[SDW-11153]

Sonstiges

IP-Regeln

Die Option Dienst außer Kraft setzen wird im Abschnitt **IP-Regeln > Datenverkehrsrichtlinie für virtuelle Pfade** hinzugefügt. Wenn die **Verkehrsrichtlinie** als **Dienst außer Kraft setzen**ausgewählt ist, können Sie den Diensttyp als Intranet, Internet, Passthrough oder Verwerfen auswählen, für den der virtuelle Pfaddienst außer Kraft gesetzt wird.

[SDW-22213]

Unterschied bei der Konfiguration

Eine **Config Diff-Funktion** wurde auf Netzwerkebene unter **Konfiguration**neu hinzugefügt. Mit der **Config Diff-Funktion** können Sie den Unterschied zwischen zwei beliebigen Versionen von Konfigurationsprüfpunkten überprüfen. Sie können die Konfigurationen auch sowohl auf globaler Ebene als auch auf Site-Ebene anzeigen.

[SDW-4563]

Appliance-Einstellungen

Citrix SD-WAN Orchestrator for On-premises führt eine Option zum Konfigurieren der Priorität des Verwaltungsnetzwerks ein. Sie können In-Band oder Out-of-Band als Verwaltungsschnittstelle für Ihr Netzwerk auswählen. Diese Option ist nur verfügbar, wenn auf der SD-WAN-Appliance eine Softwareversion von 11.4.2 oder höher ausgeführt wird.

[NSSDW-35774]

Plattform und Systeme

Zertifikatauthentifizierung

Citrix SD-WAN Orchestrator for On-premises unterstützt die Appliance-Authentifizierung für statische und dynamische virtuelle Pfade mithilfe der Public Key Infrastructure (PKI) als zusätzliche Sicherheitsfunktion. Durch Aktivieren der Funktion wird der vorhandene Authentifizierungsmechanismus für virtuelle Pfade erweitert, indem PKI-Zertifikate über den Datenpfad durch die Appliance verteilt

werden, die den Austausch initiiert. Die PKI-Erweiterung unterstützt auch die Verwaltung der Zertifikatsperrliste (Certificate Revocation List, CRL) für die zentrale Sperrung gefährdeter Zertifikate.

[SDW-19295]

Verbesserungendes Anbieterüberwachungsprotokollsund des Netzwerk

Die Seiten **Provider Audit-Protokolle** und **Netzwerk-Audit-Protokolle** wurden um die folgenden Optionen erweitert:

- **Quell-IP** - Dieses Feld zeigt die IP-Adresse des Endpunkts an, von dem aus eine SD-WAN-Funktion konfiguriert ist. Dieses Feld wird auf der Seite **Audit-Logs** und der **Audit-Info-Seite** angezeigt.
- **Als CSV exportieren** —Mit dieser Option können Sie die Audit-Logs in ein CSV-Format exportieren.
- **Was hat sich geändert** - In diesem Abschnitt werden die Protokolle aller Änderungen angezeigt, die über die Benutzeroberfläche an den Funktionen vorgenommen wurden. Aktivieren **Sie die Umschaltfläche Payloads protokollieren**, um diesen Abschnitt auf der Seite **Audit-Info** anzuzeigen. Derzeit ist dieser Abschnitt auf der Seite Network Audit Info verfügbar.

[SDW-19219]

Benutzerdefinierte Ports, Protokollkonfiguration für domänennamenbasierte Anwendungen

Die auf Domänennamen basierenden Anwendungen unterstützen jetzt konfigurierbare Ports und Protokolle in Citrix SD-WAN Orchestrator for On-premises. Wenn Sie das Kontrollkästchen **Port konfigurieren** aktivieren, können Sie jeden Port oder Portbereich nach Bedarf bearbeiten, hinzufügen oder löschen. Sie können das Protokoll auch als TCP, UDP oder Beliebig ändern/auswählen. Zuvor (und bei deaktiviertem Kontrollkästchen Port konfigurieren) wurden nur die Ports 80 und 443 sowie das Protokoll **Beliebig** für Domänen unterstützt, die unter einer Anwendung gruppiert wurden.

[NSSDW-29930]

Behobene Probleme

Die Probleme, die in Build 13.2 angesprochen werden.

Sonstiges

Auf die Benutzeroberfläche von Citrix SD-WAN Orchestrator for On-premises kann nicht zugegriffen werden. Dieses Problem tritt auf, wenn Dienste, die in {page.productname} ausgeführt werden, nicht auf Heartbeat-Anforderungen reagieren und das Neustartlimit überschritten wurde.

[DWANHELP-2544]

Das Hochladen des Software-Upgrade-Pakets schlägt auf Citrix SD-WAN Orchestrator for On-premises fehl. Dieses Problem tritt auf, wenn ein Benutzer die Upload-Seite verlässt, während das Hochladen des Softwarepakets ausgeführt wird.

[SDWANHELP-2495]

Plattform und Systeme

Eine SD-WAN-Appliance, auf der eine Softwareversion von 11.4.1 ausgeführt wird, wechselt in den Grace-Modus, wenn der Appliance Lizenzen von Citrix SD-WAN Orchestrator for On-premises zugewiesen werden.

[SDW-23171]

Bekannte Probleme

Die Probleme, die in Version 13.2 bestehen.

Konfiguration und Management

Auf einer neu importierten Citrix SD-WAN Orchestrator for On-Premises-Instanz bleibt das Staging im Status **Preparing Package** hängen. Dieses Problem tritt auf, wenn der Staging-Prozess kurz nach dem Erstellen einer neuen virtuellen Maschine initiiert wird.

Problemumgehung: Wiederholen Sie den Staging-Vorgang.

[SDW-20863]

Sonstiges

Der Dienststatus einer SD-WAN-Appliance, auf der eine Softwareversion von 11.4.2 ausgeführt wird, wird auf der Benutzeroberfläche von Citrix SD-WAN Orchestrator for On-premises als **SCHLECHT** angezeigt. Die angezeigte Fehlermeldung lautet **Keine Antwort von Orchestrator-URL**. Dieses Problem tritt auf, wenn eine benutzerdefinierte Domäne in Citrix SD-WAN Orchestrator for On-premises konfiguriert ist.

Problemumgehung: Starten Sie die SD-WAN-Appliance neu.

[SDW-23322]

Der Vorgang „ **Vorherige Version wiederherstellen** “schlägt mit der Fehlermeldung **Aktivierung fehlgeschlagen (ER101)** für die Standorte in der PSU fehl, wenn die Liste der partiellen Site-Upgrades geändert wird und eine Änderungsverwaltung (Stagierung und Aktivierung) in einem Netzwerk durchgeführt wird.

Problemumgehung: Führen Sie eine weitere Runde des Änderungsmanagements durch, bevor Sie die Aktion **Vorherige Version wiederherstellen** anwenden.

[SDW-23227]

In einigen Szenarien wird der Cloud Direct Service nach der Bereitstellung von Cloud Direct für die Sites und dem Pushen der Konfigurationen (Bereitstellen und Aktivieren) nicht angezeigt.

Problemumgehung: Aktivieren Sie den Cloud Direct Service manuell für jede Site.

[SDW-22493]

Die zuvor auf der Seite **Bereitstellung** > **Einstellungen** > **Teilweise Site-Aktualisierung** > **Softwareversion** der Benutzeroberfläche ausgewählte Softwareversion wird nicht beibehalten, wenn die Benutzer zu dieser Seite zurückkehren.

Problemumgehung: Wählen Sie die Softwareversion für partielle Site-Upgrades manuell für jede Site aus, indem Sie auf Navigieren zu **Bereitstellung** > **Sites auswählen**klicken.

[SDW-22374]

Manchmal zeigt die Benutzeroberfläche einen Fehler an, nachdem eine Konfiguration der Einstellungen der Verwaltungsschnittstelle durchgeführt wurde. Die Konfiguration ist jedoch erfolgreich und eine Aktualisierung ist erforderlich, damit die aktualisierten Einstellungen auf der Benutzeroberfläche angezeigt werden.

[SDW-22139]

In einem vom Anbieter verwalteten Setup werden die von den Anbieteradministratoren hinzugefügten Ankündigungen den Kunden bei ihrer Anmeldung nicht angezeigt.

[SDW-18491]

Plattform und Systeme

Der Kunde kann keine Push-Benachrichtigung an seinen eigenen HTTP-Server senden.

[SDW-23134]

Versionshinweise für SD-WAN Orchestrator for On-premises Version 12.3

July 17, 2023

In diesem Dokument mit den Versionshinweisen werden die Verbesserungen und Änderungen sowie behobenen und bekannten Probleme beschrieben, die für den Citrix SD-WAN Orchestrator for On-Premises-Version Build 12.3 bestehen.

Hinweis

Dieses Dokument mit Versionshinweisen enthält keine sicherheitsbezogenen Fixes. Eine Liste der sicherheitsbezogenen Fixes und Advisorys finden Sie im Citrix Security Bulletin.

Neuigkeiten

Die Erweiterungen und Änderungen, die in Build 12.3 verfügbar sind.

Sonstiges

Einstellungen löschen

Mit Citrix SD-WAN Orchestrator for On-premises können Sie historische Daten löschen, die älter sind als die Intervalltage für die Bereinigungsstatistik (standardmäßig 30 Tage). Wenn die Daten gelöscht werden, werden die historischen Daten, die älter als die ausgewählte Anzahl von Tagen sind, entfernt und sind nicht mehr verfügbar. Der Löschvorgang findet täglich gegen 12:48 Uhr statt, basierend auf der auf Ihrer SD-WAN-Appliance eingestellten Zeitzone.

[SDW-20402]

Zero-Touch-Bereitstellungsschnittstelle

Sie können eine ZTD (Zero Touch Deployment) -Schnittstelle auf Citrix SD-WAN Orchestrator for On-premises aktivieren. Die ZTD-Schnittstelle, die durch bidirektionale Authentifizierung gesichert ist, bietet eine sichere Kommunikationsschnittstelle für SD-WAN-Appliances und Citrix SD-WAN Orchestrator für lokale Geräte.

[SDW-19152]

Virtuelle Pfadeinstellungen für den Link

Sie können Bandbreiten für virtuelle Pfade und dynamische virtuelle Pfade anpassen, die einer WAN-Verbindung zugeordnet sind. Diese Funktion ist nützlich, wenn einige Websites aufgrund von Bandbreitenproblemen Anzeichen für Leistungseinbußen aufweisen.

[SDW-9760]

SD-WAN Orchestrator

Syslog-Servereinstellungen

Citrix SD-WAN Orchestrator for On-premises unterstützt die Konfiguration von Syslog-Servereinstellungen für SD-WAN-Appliances. Durch Aktivieren der Syslog-Einstellungen können Sie Systemwarnungen und Ereignisdetails der SD-WAN-Appliances an einen externen Syslog-Server senden.

[SDW-13990]

Behobene Probleme

Die Probleme, die in Build 12.3 angesprochen werden.

Sonstiges

Unter bestimmten Bedingungen kann die SD-WAN-Appliance nicht mit Citrix SD-WAN Orchestrator for On-premises über In-Band-Verwaltung kommunizieren, wenn die In-Band-Verwaltung aktiviert und die Out-of-Band-Verwaltung angeschlossen ist.

[DWANHELP-2368]

Die Benutzeroberfläche zeigt fälschlicherweise einen Fehler an, wenn der Wert für dynamische virtuelle Pfade auf mehr als 8 festgelegt ist, obwohl die maximal zulässige Grenze 32 beträgt. Dieses Problem tritt bei VPXL- und 4100 SE-Appliances auf.

[DWANHELP-2354]

In der Dropdownliste **Softwareversion** unter Einstellungen für partielles Site-Upgrade werden alle unterstützten Softwareversionen angezeigt, anstatt nur die Versionen anzuzeigen, die unter **Infrastruktur** > **Orchestrator-Verwaltung** > **Software-Images** > veröffentlicht wurden **Gerät.

Wenn eine unter Teilweises Site-Upgrade aufgeführte Softwareversion unter **Infrastruktur** > **Orchestrator-Verwaltung** > **Software-Images** > **Appliance**nicht zur Veröffentlichung verfügbar ist, kann für diese Version kein teilweises Standort-Upgrade durchgeführt werden.

[SDW-20992]

Bekannte Probleme

Die Probleme, die in Version 12.3 bestehen.

Konfiguration und Management

Auf einer neu importierten Citrix SD-WAN Orchestrator for On-Premises-Instanz bleibt das Staging im Status **Preparing Package** hängen. Dieses Problem tritt auf, wenn der Staging-Prozess kurz nach dem Erstellen einer neuen virtuellen Maschine initiiert wird.

Problemumgehung: Wiederholen Sie den Staging-Vorgang.

[SDW-20863]

Sonstiges

Citrix SD-WAN Orchestrator for On-premises, auf dem VMware ESXi 13 ausgeführt wird, kann nicht neu gestartet werden und geht in einen fehlerhaften Zustand über.

Problemumgehung: Verwenden Sie VMware ESXi Version 9.

[SDWANHELP-2182]

In einigen Szenarien wird der Cloud Direct Service nach der Bereitstellung von Cloud Direct für die Sites und dem Pushen der Konfigurationen (Bereitstellen und Aktivieren) nicht angezeigt.

Problemumgehung: Aktivieren Sie den Cloud Direct Service manuell für jede Site.

[SDW-22493]

Der Staging-Prozess schlägt zeitweise fehl, wenn Benutzer ein teilweises Site-Upgrade durchführen. Auf der Benutzeroberfläche wird die Fehlermeldung **Stagingfehler aufgrund einer Ausnahme**angezeigt.

Problemumgehung: Wiederholen Sie den Staging-Vorgang.

[SDW-22398]

Die zuvor auf der Seite **Bereitstellung** > **Einstellungen** > **Teilweise Site-Aktualisierung** > **Softwareversion** der Benutzeroberfläche ausgewählte Softwareversion wird nicht beibehalten, wenn die Benutzer zu dieser Seite zurückkehren.

Problemumgehung: Wählen Sie die Softwareversion für partielle Site-Upgrades manuell für jede Site aus, indem Sie auf Navigieren zu **Bereitstellung** > **Sites auswählen**klicken.

[SDW-22374]

Manchmal zeigt die Benutzeroberfläche einen Fehler an, nachdem eine Konfiguration der Einstellungen der Verwaltungsschnittstelle durchgeführt wurde. Die Konfiguration ist jedoch erfolgreich und eine Aktualisierung ist erforderlich, damit die aktualisierten Einstellungen auf der Benutzeroberfläche angezeigt werden.

[SDW-22139]

Benutzer können die Imagedatei **tar.gz** von Citrix SD-WAN Orchestrator for On-premises, die auf der Seite **Infrastruktur** > **Orchestrator-Administration** > **Software-Images** der Benutzeroberfläche hochgeladen wurde, nicht löschen. Die angezeigte **Fehlermeldung lautet Beim Löschen des Softwarepakets ist ein Fehler aufgetreten**.

Problemumgehung: Laden Sie ein neues Softwarepaket hoch. Die zuvor hochgeladene Datei wird automatisch gelöscht.

[SDW-22137]

Auf der **Startseite**Konfiguration**> Netzwerkkonfiguration** der Benutzeroberfläche wird der Orchestrator-Konnektivitätsstatus für eine sekundäre SD-WAN-Appliance unmittelbar nach dem Hochladen der Konfigurationsdatei online angezeigt. Der richtige Status wird jedoch angezeigt, nachdem die Konfiguration für die Site gespeichert wurde.

[SDW-20913]

In einem vom Anbieter verwalteten Setup werden die von den Anbieteradministratoren hinzugefügten Ankündigungen den Kunden bei ihrer Anmeldung nicht angezeigt.

[SDW-18491]

Wenn die Datenbanksicherung einer Appliance auf einer anderen Appliance mit derselben Version von Citrix SD-WAN Orchestrator for On-premises wiederhergestellt wird, werden die Benutzerdetails nicht wiederhergestellt. Wenn Sie auf der wiederhergestellten Appliance einen Benutzer mit demselben Benutzernamen wie in der gesicherten Datenbank erstellen, wird der folgende Fehler angezeigt:

`User has a role already assigned`.

Problemumgehung: Erstellen Sie einen Benutzer mit einem anderen Benutzernamen, der in der gesicherten Datenbank nicht vorhanden war.

[SDW-15984]

Plattform und Systeme

Wenn Sie in der Citrix SD-WAN 210-Appliance die Zusatzlizenz entfernen, werden die Dienste deaktiviert.

Problemumgehung: Entfernen Sie die Firewallrichtlinie mit Sicherheitsprofil, stellen Sie die Änderungen bereit und aktivieren Sie sie, um die Appliance in die Standard Edition zu konvertieren.

[SDW-18031]

Versionshinweise für SD-WAN Orchestrator für lokale Version 11.4.0a

July 17, 2023

In diesem Dokument mit den Versionshinweisen werden die Verbesserungen und Änderungen sowie behobenen und bekannten Probleme beschrieben, die für den Citrix SD-WAN Orchestrator for On-Premises-Release Build 11.4.0a bestehen.

Hinweise

- Citrix SD-WAN Orchestrator for On-premises 11.4.0a behebt das in SDWANHELP-2317 beschriebene Problem und ersetzt Version 11.4.
- Dieses Dokument mit Versionshinweisen enthält keine sicherheitsbezogenen Fixes. Eine Liste der sicherheitsbezogenen Fixes und Advisorys finden Sie im Citrix Security Bulletin.

Neuigkeiten

Die Erweiterungen und Änderungen, die in Build 11.4.0a verfügbar sind.

Konfiguration und Management

HTTP-Proxy

Sie können HTTP-Proxyeinstellungen auf Citrix SD-WAN Orchestrator for On-premises konfigurieren. Diese Funktion zentralisiert die Verwaltung aller ausgehenden Anfragen an Citrix Cloud. Die Administratoren können die ausgehenden Anforderungen von Citrix SD-WAN Orchestrator for On-premises über einen HTTP-Proxyserver an Citrix Cloud weiterleiten.

[SDW-20247]

Cloud Direct Service

Citrix SD-WAN Orchestrator for On-premises unterstützt den Cloud Direct Service.

Der Cloud Direct Service bietet SD-WAN-Funktionalitäten als Cloud-Dienst durch zuverlässige und sichere Bereitstellung für den gesamten internetgebundenen Datenverkehr unabhängig von der Host-Umgebung (Rechenzentrum, Cloud und Internet).

Der Cloud Direct Service verbessert die Sichtbarkeit und Verwaltung des Netzwerks. Damit können Partner ihren Endkunden verwaltete SD-WAN-Services für geschäftskritische SaaS-Anwendungen anbieten.

[SDW-16396]

Speichermanagement —Allgemeine Verfügbarkeit

Die Speicherverwaltungsfunktion unterstützt jetzt die allgemeine Verfügbarkeit.

Citrix SD-WAN Orchestrator for On-premises unterstützt die Migration der Konfiguration und der Daten von einer Festplatte auf eine andere. Sie können die Festplattenmigration entweder zur Erhöhung des Speicherplatzes oder zur Notfallwiederherstellung durchführen.

- **Hinzufügen einer neuen Festplatte**: Sie können eine neue Festplatte mit einer Speichergröße hinzufügen, die mindestens doppelt so groß ist wie die aktuellen Daten, die von Citrix SD-WAN Orchestrator for On-premises verbraucht werden.
- **Notfallwiederherstellung: Im Katastrophenfall**können Sie die Festplatte, die die Konfiguration und die Daten von Citrix SD-WAN Orchestrator für die lokale Konfiguration enthält, an eine neue Instanz von Citrix SD-WAN Orchestrator für lokale virtuelle Maschine anhängen.

[SDW-21316]

Cloud-vermittelte Zero-Touch-Bereitstellung —Allgemeine Verfügbarkeit

Die von der Cloud vermittelte Zero-Touch-Bereitstellungsfunktion unterstützt jetzt die allgemeine Verfügbarkeit.

Die Cloud-vermittelte Zero-Touch-Bereitstellung ist ein automatisierter Prozess, an dem Citrix SD-WAN Orchestrator for On-premises als Broker beteiligt ist, um die Konnektivität zwischen Citrix SD-WAN Orchestrator for On-premises und den Citrix SD-WAN-Appliances herzustellen.

[SDW-21312]

Citrix SD-WAN 11.4.1 Version

Die Version Citrix SD-WAN 11.4.1 wird auf Citrix SD-WAN Orchestrator for On-premises 11.4 unterstützt.

[SDW-21082]

Plattform und Systeme

ICMP-Sondierung

Citrix SD-WAN Orchestrator for On-premises unterstützt ICMP-Prüfungen. Es ermöglicht Administratoren, die Erreichbarkeit des Internets zu/von der SD-WAN-Appliance und dem Zielhost zu bestimmen. Die folgenden ICMP-Dienste werden in der Benutzeroberfläche eingeführt:

- Ermitteln der Interneterreichbarkeit über eine Verbindung mithilfe von ICMP-Sonden
- IPv4-ICMP-Endpunktadresse
- Sondenintervall (in Sekunden)

- Wiederholte Versuche

[SDW-19292]

Einstellungen für globale Transitknoten außer Kraft

Sie können jetzt die globalen Transitknoteneinstellungen außer Kraft setzen und festlegen, dass die Spoke-to-Spoke-Weiterleitung und der Routenexport nur auf ausgewählten Kontroll-Transitknoten aktiviert oder deaktiviert

[SDW-19276]

API für Mitgliedspfadstatistiken (Vorschau):

Die API für Mitgliedspfadstatistiken wurde geändert, damit der API-Client die Interessenfelder angeben kann. Die angegebenen Felder werden in der Antwortnutzlast zurückgegeben.

[SDW-18903]

Site-Berichte: VRRP

Der VRRP-Bericht liefert einen Echtzeitbericht der konfigurierten VRRP-Gruppen.

[SDW-12082]

Site-Berichte: IGMP

Die Tabelle IGMP-Berichte enthält einen Echtzeitbericht der IGMP-Statistiken und IGMP-Proxygruppen.

[SDW-12077]

Site-Berichte: IPSec

Die IPSec-Berichte stellen den Echtzeitbericht der IPSec-Tunnelkonfigurationen in Ihrem Netzwerk bereit.

[SDW-12076]

Site-Berichte: Routing-Protokolle

Der Bericht **Routing-Protokolle** enthält Einzelheiten zu den Parametern, die den Routingprotokollen zugeordnet sind. Sie können das Protokoll nach Bedarf aus der Dropdownliste **Ansicht** einer Routingdomäne aus der Dropdown-Liste **Routingdomäne** auswählen. Um die aktuellen Daten anzuzeigen, klicken Sie auf **Neueste Daten abrufen**.

[SDW-12075]

Anbieterprüfprotokolle, Netzwerk-

Die Überwachungsprotokollseiten auf Provider- und Netzwerkebene wurden um die folgenden Funktionen erweitert:

- **Suche**: Möglichkeit, anhand eines Schlüsselworts nach einer Auditaktivität zu suchen.

- **Filtern**: Führen Sie eine Auditprotokollsuche durch, indem Sie nach Benutzer, Funktion und Zeitraum filtern. Bei Protokollen auf Netzwerkebene können Sie auch nach Site filtern.
- **Audit-Info**: Wählen Sie das Info-Symbol in der Spalte **Aktion** aus, um zum Abschnitt **Audit-Informationen** zu navigieren. Dieser Abschnitt enthält die folgenden Informationen:
- **Methode**: HTTP-Anforderungsmethode der aufgerufenen API.
- **Status**: Ergebnis der API-Anfrage. Sie sehen eine Fehlermeldung, wenn die API-Anfrage fehlschlägt.
- **Payload-Nachricht**: Text der über die API gesendeten Anforderungsnachricht.
- **URL**: HTTP-URL der widerrufenen API.
- **Payloads protokollieren**: Diese Option ist standardmäßig deaktiviert. Wenn diese Option aktiviert ist, wird der Anforderungstext der API-Nachricht im Abschnitt **Audit-Info** angezeigt.

[SDW-18937]

Komponente Standortwahl

Die Benutzerfreundlichkeit der Komponente für die Standortauswahl in den folgenden Konfigurationen wurde aufgrund ihrer Benutzerfreundlichkeit verbessert:

1. Partielles Site-Upgrade
2. Netzwerkstandort-Service
3. Routing-Richtlinien
4. QoS-Richtlinien
5. Routenfilter importieren
6. Routenfilter exportieren
7. Proxy-Auto-Konfig
8. Intrusion Prevention
9. Firewall-Richtlinien
10. Anwendungseinstellungen

[SDW-16895]

Behobene Probleme

Die Probleme, die in Build 11.4 angesprochen werden.

Sonstiges

Die von der Cloud vermittelte ZTD-Funktion ist vom SD-WAN Orchestrator Service abhängig, damit sie funktioniert. Dies wird in einer kommenden SD-WAN Orchestrator Orchestrator-Version behoben. Kunden müssen jedoch ihren Citrix SD-WAN Orchestrator for On-premises nicht aktualisieren.

[SDW-20307]

Die SD-WAN-Cloud-ZTD-Konfiguration funktioniert nicht für HA-Sites, wenn die Cloud-ZTD bereits auf einem primären Standort konfiguriert ist.

[SDW-20208]

Citrix SD-WAN Orchestrator for On-premises zeigt den Status als **Nicht verbunden** an, obwohl die SD-WAN-Appliance mit Citrix SD-WAN Orchestrator for On-premises verbunden ist.

[SDW-18280]

Bekannte Probleme

Die Probleme, die in Version 11.4 bestehen.

Konfiguration und Management

Auf einer neu importierten Citrix SD-WAN Orchestrator for On-Premises-Instanz bleibt das Staging im Status **Preparing Package** hängen. Dieses Problem tritt auf, wenn der Staging-Prozess kurz nach dem Erstellen einer neuen virtuellen Maschine initiiert wird.

Problemumgehung: Wiederholen Sie den Staging-Vorgang.

[SDW-20863]

Sonstiges

Der Staging-Prozess schlägt fehl, wenn Benutzer, die Citrix SD-WAN Orchestrator for On-premises 11.4 ausführen, ihre Citrix SD-WAN-Appliances auf die Version 11.4.1 aktualisieren. Auf der Benutzeroberfläche wird der Status **Staging Failed (Skriptdateien konnten nicht heruntergeladen werden)**angezeigt. Dieses Problem tritt auf, wenn die Bandbreite zwischen der Citrix SD-WAN-Appliance und dem Citrix SD-WAN Orchestrator for On-premises geringer ist.

[SDWANHELP-2317]

Citrix SD-WAN Orchestrator for On-premises, auf dem VMware ESXi 13 ausgeführt wird, kann nicht neu gestartet werden und geht in einen fehlerhaften Zustand über.

Problemumgehung: Verwenden Sie VMware ESXi Version 9.

[SDWANHELP-2182]

Die Benutzeroberfläche zeigt auf den Seiten **Konfiguration >**Netzwerkkonfiguration Home**und**Konfiguration**** > ****Bereitstellung** eine falsche Software-Version der SD-WAN-Appliance an. Dieses Problem tritt

auf Citrix SD-WAN Orchestrator for On-Premises-Instanzen auf, die neu installiert wurden und bevor Benutzer eine Änderungsverwaltung durchführen.

[SDW-21018]

Die Benutzeroberfläche zeigt keine Fehlermeldung an, wenn der Cloud Direct-Site-Vorgang fehlschlägt.

[SDW-21009]

In der Dropdownliste **Softwareversion** unter Einstellungen für partielles Site-Upgrade werden alle unterstützten Softwareversionen angezeigt, anstatt nur die Versionen anzuzeigen, die unter **Infrastruktur** > **Orchestrator-Verwaltung** > **Software-Images** > veröffentlicht wurden **Gerät.

Wenn eine unter Teilweises Site-Upgrade aufgeführte Softwareversion unter **Infrastruktur** > **Orchestrator-Verwaltung** > **Software-Images** > **Appliance**nicht zur Veröffentlichung verfügbar ist, kann für diese Version kein teilweises Standort-Upgrade durchgeführt werden.

[SDW-20992]

Auf der **Startseite**Konfiguration**> Netzwerkkonfiguration** der Benutzeroberfläche wird der Orchestrator-Konnektivitätsstatus für eine sekundäre SD-WAN-Appliance unmittelbar nach dem Hochladen der Konfigurationsdatei online angezeigt. Der richtige Status wird jedoch angezeigt, nachdem die Konfiguration für die Site gespeichert wurde.

[SDW-20913]

In einem vom Anbieter verwalteten Setup werden die von den Anbieteradministratoren hinzugefügten Ankündigungen den Kunden bei ihrer Anmeldung nicht angezeigt.

[SDW-18491]

Wenn die Datenbanksicherung einer Appliance auf einer anderen Appliance mit derselben Version von Citrix SD-WAN Orchestrator for On-premises wiederhergestellt wird, werden die Benutzerdetails nicht wiederhergestellt. Wenn Sie auf der wiederhergestellten Appliance einen Benutzer mit demselben Benutzernamen wie in der gesicherten Datenbank erstellen, wird der folgende Fehler angezeigt:

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

Problemumgehung: Erstellen Sie einen Benutzer mit einem anderen Benutzernamen, der in der gesicherten Datenbank nicht vorhanden war.

[SDW-15984]

Versionshinweise für Citrix SD-WAN Orchestrator for On-premises Version 11.1

July 17, 2023

In diesem Dokument mit den Versionshinweisen werden die Verbesserungen und Änderungen sowie behobenen und bekannten Probleme beschrieben, die für den Citrix SD-WAN Orchestrator for On-premises Version 11.1 bestehen.

Hinweise

Dieses Dokument mit Versionshinweisen enthält keine sicherheitsbezogenen Fixes. Eine Liste der sicherheitsbezogenen Fixes und Advisorys finden Sie im Citrix Security Bulletin.

Neuigkeiten

Die Verbesserungen und Änderungen, die in Release 11.1 verfügbar sind.

Citrix SD-WAN 11.4.0a Version

Die Version Citrix SD-WAN 11.4.0a wird in Citrix SD-WAN Orchestrator for On-premises unterstützt.

[SDW-19785]

Citrix SD-WAN 11.3.2 Version

Die Version Citrix SD-WAN 11.3.2 wird in Citrix SD-WAN Orchestrator for On-premises unterstützt.

[SDW-19038]

Routenzusammenfassung

Citrix SD-WAN Orchestrator for On-premises führt eine Erweiterung der Routenzusammenfassungsfunktion ein. Mit dieser Erweiterung können Sie Zusammenfassungsrouten hinzufügen, ohne die Gateway-IP-Adresse anzugeben.

[SDW-19404]

ECMP Load Balancing

Equal Cost Multi-Path (ECMP) -Gruppen ermöglichen es Ihnen, mehrere Routen mit denselben Kosten, Zielen und demselben Servicetyp zu gruppieren. Der ECMP-Lastenausgleich gewährleistet:

- Verteilung des Datenverkehrs über mehrere gleichzeitige Verbindungen.
- Optimale Nutzung der verfügbaren Bandbreite.

- Dynamische Übertragung des Traffics auf andere ECMP-Mitgliederroute, wenn eine Route nicht erreichbar wird.
- ECMP-Gruppen können über Virtual Paths und Intranet-Services gebildet werden.

[SDW-17452]

Speicherverwaltung (Vorschau)

Citrix SD-WAN Orchestrator for On-premises unterstützt die Migration der Konfiguration und der Daten von einer Festplatte auf eine andere. Sie können die Festplattenmigration entweder zur Erhöhung des Speicherplatzes oder zur Notfallwiederherstellung durchführen.

- **Hinzufügen einer neuen Festplatte**: Sie können eine neue Festplatte mit einer Speichergröße hinzufügen, die mindestens doppelt so groß ist wie die aktuellen Daten, die von Citrix SD-WAN Orchestrator for On-premises verbraucht werden.
- **Notfallwiederherstellung: Im Katastrophenfall**können Sie die Festplatte, die die Konfiguration und die Daten von Citrix SD-WAN Orchestrator für die lokale Konfiguration enthält, an eine neue Instanz von Citrix SD-WAN Orchestrator für lokale virtuelle Maschine anhängen.

[SDW-16404]

Cloud-vermittelte Zero-Touch-Bereitstellung (Vorschau)

Die Cloud-vermittelte Zero-Touch-Bereitstellung ist ein automatisierter Prozess, an dem Citrix SD-WAN Orchestrator for On-premises als Broker beteiligt ist, um die Konnektivität zwischen Citrix SD-WAN Orchestrator for On-premises und den Citrix SD-WAN-Appliances herzustellen.

[SDW-11614]

Verbesserungen am Transitknoten

Durch das Aktivieren der Hub-and-Spoke-Kommunikation als Teil globaler Einstellungen können alle Standorte die Steuerungsknoten standardmäßig als Transit-Knoten für die Kommunikation von Standort zu Standort verwenden. Site-spezifische Einstellungen für virtuelle Overlay-Transit-Knoten ermöglichen es Ihnen, die globalen Einstellungen für virtuelle Overlay-Transitknoten für alle Standorte in Ihrem Netzwerk zu überschreiben. Sie können auch einen nicht zu steuernden Knoten als primären Transitknoten für einen Standort auswählen.

[SDW-12443]

Unterstützung der IPv6-Datenebene

Citrix SD-WAN Orchestrator for On-premises unterstützt IPv6-Adressen für die folgenden Citrix SD-WAN-Appliance-Konfigurationen mit der Citrix SD-WAN-Softwareversion 11.3.1 oder höher:

- DNS-Server
- Strömungen
- Firewall-Verbindungen

- IP-Gruppen
- Regionen
- DHCP-Client
- IP-Regeln und Anwendungsregeln
- Übersetzung von Netzwerkadressen
- GRE Service
- Schnittstellen
- Internet Service
- Protokoll zur Entdeckung von Nachbarn
- Präfix-Delegierungsgruppe
- IPsec-Dienst
- HA-Einstellungen
- IP-Routen
- In-Band-Verwaltung
- DNS-Einstellungen
- DHCP-Server, DHCP-Relay und DHCP-Optionen festgelegt

[SDW-19194]

Behobene Probleme

Die Probleme, die in Version 11.1 behoben werden.

SD-WAN-Appliance-Versionen unter 11.2.0 können für lokale Versionen unter 11.1 keine Verbindung zu Citrix SD-WAN Orchestrator herstellen. Citrix SD-WAN Orchestrator for On-premises 11.1 ist die empfohlene Version, wenn Benutzer ihre SD-WAN-Appliances mit einer Softwareversion unter 11.2.0 verbinden möchten.

[SDW-20220]

Wenn beim Upgrade eines Kundenkontos auf die Produktion ein Fehler auftritt, zeigt die Benutzeroberfläche die Fehlermeldung nicht an.

[SDW-19574]

Das Upgrade auf die Produktion schlägt in Citrix SD-WAN Orchestrator for On-premises fehl, für Prepaid-Kunden, die nur unbefristete Lizenzen haben.

[SDW-19558]

Das Zuweisen unbefristeter Lizenzen zu Standorten schlägt in Citrix SD-WAN Orchestrator for On-premises fehl.

[SDW-19556]

Wenn beim Zuweisen von Lizenzen ein Fehler auftritt, zeigt die Benutzeroberfläche die Fehlermeldung unter **Administration** > **Lizenzierung**nicht an.

[SDW-19238]

Obwohl der Kundenadministrator keinen Zugriff zum Löschen der Remote-Authentifizierungsserver hat, zeigt die Benutzeroberfläche das Löschsymbol an. Wenn der Kundenadministrator jedoch versucht, den Löschvorgang auszuführen, wird der folgende Fehler angezeigt:

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

[SDW-18945]

Wenn Sie auf der Seite **Administration** > **Ankündigungen** auf Anbieterebene einen Kunden aus der oberen Menüleiste auswählen, wird eine leere Seite mit **Netzwerkadministration** als Überschrift angezeigt.

[SDW-18944]

Nach dem Import gültiger Produktionsberechtigungen wird die Option **Upgrade auf Produktion** unter **Lizenzierung** verfügbar gemacht, noch bevor die Lizenz der Appliance zugewiesen wird.

[SDW-18721]

Bekannte Probleme

Die Probleme, die in Version 11.1 bestehen.

Die von der Cloud vermittelte ZTD-Funktion ist vom SD-WAN Orchestrator Service abhängig, damit sie funktioniert. Dies wird in einer kommenden SD-WAN Orchestrator Service Orchestrator-Dienstversion behoben. Kunden müssen jedoch ihren Citrix SD-WAN Orchestrator for On-premises nicht aktualisieren.

[SDW-20307]

Wenn Citrix SD-WAN Orchestrator for On-premises auf die Version 11.1 aktualisiert wird, zeigen die in den vorherigen Versionen gesammelten Überwachungsprotokolle **sdwan-onprem-sp** als Benutzer an, und die Umschaltfläche für Protokollnutzlasten ist auf der Benutzeroberfläche aktiviert. Diese Protokolle werden nach 92 Tagen gelöscht.

[SDW-20305]

Die SD-WAN-Cloud-ZTD-Konfiguration funktioniert nicht für HA-Sites, wenn die Cloud-ZTD bereits auf einem primären Standort konfiguriert ist.

Workaround:

1. Löschen Sie die ZTD-Konfiguration der primären Site-Cloud, indem Sie zu **Administration** > **ZTD-Einstellungen** > **Cloud Brokered ZTD**navigieren.

2. Konfigurieren Sie den Cloud-ZTD-Site gleichzeitig für primäre und sekundäre Standorte neu.

[SDW-20208]

Die Lizenzierungsfunktion wird im vom Anbieter verwalteten Setup von Citrix SD-WAN Orchestrator for On-premises nicht unterstützt. Anbieter können mit den Testlizenzen fortfahren. Eine Nachfrist von 60 Tagen ist vorgesehen.

[SDW-1831]

Wenn eine Appliance länger als 20 Minuten die Verbindung zu Citrix SD-WAN Orchestrator for On-premises verliert und in die Phase der erneuten Registrierung übergeht, sendet sie eine falsche Seriennummer in der Registrierungsanforderung.

Problemumgehung: Starten Sie die Appliance neu.

[SDW-18781]

In einem vom Anbieter verwalteten Setup werden die von den Anbieteradministratoren hinzugefügten Ankündigungen den Kunden bei ihrer Anmeldung nicht angezeigt.

[SDW-18491]

Citrix SD-WAN Orchestrator for On-premises zeigt den Status als **Nicht verbunden** an, obwohl die SD-WAN-Appliance mit Citrix SD-WAN Orchestrator for On-premises verbunden ist.

Problemumgehung: Navigieren Sie zu **Konfiguration** > **Network Config Home**, und überprüfen Sie den Konnektivitätsstatus der Appliance auf der Benutzeroberfläche von Citrix SD-WAN Orchestrator for On-premises.

[SDW-18280]

Wenn die Datenbanksicherung einer Appliance auf einer anderen Appliance mit derselben Version von Citrix SD-WAN Orchestrator for On-premises wiederhergestellt wird, werden die Benutzerdetails nicht wiederhergestellt. Wenn Sie auf der wiederhergestellten Appliance einen Benutzer mit demselben Benutzernamen wie in der gesicherten Datenbank erstellen, wird der folgende Fehler angezeigt:

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

Problemumgehung: Erstellen Sie einen Benutzer mit einem anderen Benutzernamen, der in der gesicherten Datenbank nicht vorhanden war.

[SDW-15984]

Citrix SD-WAN Orchestrator for On-premises, auf dem VMware ESXi 13 ausgeführt wird, kann nicht neu gestartet werden und geht in einen fehlerhaften Zustand über.

Problemumgehung: Verwenden Sie VMware ESXi Version 9.

[SDWANHELP-2182]

Versionshinweise für Citrix SD-WAN Orchestrator for On-premises 10.3

October 21, 2022

In diesem Dokument mit den Versionshinweisen werden die Verbesserungen und Änderungen sowie behobenen und bekannten Probleme beschrieben, die für den Citrix SD-WAN Orchestrator for On-premises Version 10.3 bestehen.

Hinweise

Dieses Dokument mit Versionshinweisen enthält keine sicherheitsbezogenen Fixes. Eine Liste der sicherheitsbezogenen Fixes und Advisorys finden Sie im Citrix Security Bulletin.

Neuigkeiten

Die Verbesserungen und Änderungen, die in Release 10.3 verfügbar sind.

Konfiguration und Management

Dynamisches Routing

Ab Citrix SD-WAN 11.3.1 können Sie eine Router-ID für das gesamte Protokoll und auch eine Router-ID pro Routingdomäne konfigurieren. Mit dieser Erweiterung können Sie ein stabiles dynamisches Routing über mehrere Instanzen hinweg aktivieren, wobei verschiedene Router-IDs stabil konvergieren.

[SDW-17097]

Staging wiederholen

Die Option Staging wiederholen ist jetzt verfügbar, um das Staging an den Standorten erneut zu initiieren, an denen der Staging-Prozess fehlgeschlagen ist.

[SDW-16538]

Benutzerdefinierte Anwendung

Das Kontrollkästchen **Reporting aktivieren** wurde für die auf dem IP-Protokoll basierenden benutzerdefinierten Anwendungen neu hinzugefügt. Jetzt können Sie auch das IP-Protokoll und den auf Domänennamen basierenden benutzerdefinierten, anwendungsdefinierten Datenverkehr auf der Seite **Berichte Verwendung** anzeigen. Die benutzerdefinierte Anwendungsoption wird auch als Typ auf der **Konfigurationsseite für die Anwendungsqualität** hinzugefügt.

[SDW-10862]

Sonstiges

Fallback-Konfiguration

Die Fallback-Konfiguration stellt sicher, dass die Appliance mit dem Zero-Touch-Bereitstellungsdienst verbunden bleibt, wenn ein Verbindungsfehler, eine Konfigurations- oder Softwarekdiskrepanz vorliegt. Die Fallbackkonfiguration ist standardmäßig auf den Appliances aktiviert, die über ein Standardkonfigurationsprofil verfügen. Wenn die Fallback-Konfiguration an einem Standort deaktiviert ist, können Sie sie über Citrix SD-WAN Orchestrator for On-premises aktivieren.

[SDW-13978]

Strömungen

Sie können jetzt den Abschnitt **Flows** für Appliance-Einstellungen verwenden, um die folgende Aktion auszuführen:

- Aktivieren/deaktivieren des Citrix Virtual WAN-Dienstes
- Dynamisches Routing neu
- Virtuelle Pfade aktivieren/deaktivieren
- WAN-Links aktivieren/deaktivieren

[SDW-13977]

Rollen Netzwerkadministrator und Sicherheitsadministrator (Vorschau)

Citrix SD-WAN Orchestrator for On-premises unterstützt die folgenden Rollen:

- **Provide-Network-Admin**: Ein Administrator, der nur die netzwerkbezogenen Informationen anzeigen und bearbeiten kann.
- **Provider-Security-Admin**: Ein Administrator, der nur die sicherheitsbezogenen Informationen anzeigen und bearbeiten kann.
- **Kunden-Netzwerk-Admin**: Ein Kundenadministrator, der nur netzwerkbezogene Informationen anzeigen und bearbeiten kann.
- **Customer-Security-Admin**: Ein Kundenadministrator, der nur sicherheitsbezogene Informationen anzeigen und bearbeiten kann.

[SDW-13845]

Appliance-Einstellungen

Sie können jetzt Datum und Uhrzeit auf Standortebene über Citrix SD-WAN Orchestrator for On-premises konfigurieren. Sie können Datum und Uhrzeit entweder manuell oder über einen NTP-Server konfigurieren und auch die Zeitzone festlegen.

[SDW-13321]

Support auf Provider-Ebene

Citrix SD-WAN Orchestrator for On-premises unterstützt Mehrmandantenfähigkeit. Mit der Mandantenanzfunktion können mehrere Kundenkonten mit einer einzigen Citrix SD-WAN Orchestrator for On-Premises-Instanz verwaltet werden. Sie können eine der folgenden Arten von Setups haben.

- Vom**Anbieter verwaltetes Setup**: Kunden verwenden einen verwalteten Citrix SD-WAN Orchestrator for On-Premises-Dienst von Citrix-Partnern, die die Mandantenfähigkeit verwenden.
- **Vom Kunden verwaltetes Setup**: Kunden verwalten ihren Citrix SD-WAN Orchestrator for On-premises als selbstverwalteten Service für ihr Unternehmen.

Im Rahmen der Unterstützung von Provider Managed Setup werden die folgenden Funktionen eingeführt:

- **Rollen**: Die folgenden Rollen auf Anbieterebene wurden hinzugefügt:
  - Provider-Master-Admin-All
  - Provider-Master-Admin-Tenant
  - Provider-Master-Readonly-All
- **Dashboard**: Eine neue UI-Seite wurde hinzugefügt, die eine Vogelperspektive aller SD-WAN-Kunden bietet, die von einem Anbieter verwaltet werden.
- **Konnektivität mit SD-WAN-Appliances**: In einem vom Anbieter verwalteten Setup können nur Anbieter den Authentifizierungstyp aktivieren und das Citrix SD-WAN Orchestrator for On-Premises-Zertifikat neu generieren. Kunden haben die Möglichkeit, das Appliance-Zertifikat hochzuladen.
- **Standortprofilvorlagen und WAN-Link-Vorlagen**: Die Vorlagen ermöglichen die Erstellung von **Standortprofilen** und **WAN-Link-Profilen** auf Kundenebene.
- **Software veröffentlichen**: Mit Citrix SD-WAN Orchestrator for On-premises können Anbieteradministratoren die für alle Appliances in Ihrem Netzwerk erforderliche Citrix SD-WAN-Appliance-Softwareversion herunterladen. Anbieter können die heruntergeladene Softwareversion veröffentlichen. Die veröffentlichte Software wird heruntergeladen und in Citrix SD-WAN Orchestrator for On-premises gespeichert. Kundenadministratoren können die veröffentlichte Software auf allen Appliances bereitstellen, die von Citrix SD-WAN Orchestrator for On-premises verwaltet werden.
- **Administration**: Anbieteradministratoren können Management-IP, DNS, NTP-Server und Remoteauthentifizierungsserver konfigurieren.
- **Ankündigungen**: Anbieter können die Option **Ankündigungen** verwenden, um Ankündigungen oder Benachrichtigungen an ihre Kunden zu senden.
- **Berichte**: Die **Anbieterberichte** bieten Einblick in Warnmeldungen, Nutzungstrends und Inventar, das über alle von einem Anbieter verwalteten Kunden hinweg aggregiert wird.

[SDW-12589]

Zero-Touch-Bereitstellung —Batch

Sie können jetzt eine CSV-Datei importieren, um mehrere Standorte gleichzeitig für Zero Touch Deployment hinzuzufügen. Eine herunterladbare Beispielvorlage ist in der Benutzeroberfläche verfügbar. Laden Sie sie herunter und geben Sie alle Site-Details an.

[SDW-12249]

Plattform und Systeme

Standortberichte: WAN-Link-Messung

Die **WAN-Link-Metering-Berichte** enthalten Details zur gemessenen WAN-Link-Nutzung. Sie können die Berichte anzeigen, um Einblicke in den Datenverbrauch der gemessenen WAN-Verbindungen zu erhalten.

[SDW-8892]

Bekannte Probleme

Die Probleme, die in Version 10.3 bestehen.

Konfiguration und Management

Für In-Band-HA hat die GUI keine Option, um die Richtung der Zielregel mit Diensttyp als Beliebig auszuwählen, was zu einem Fehler bei ausgehenden Regeln führt. Die Fehlermeldung [EC818] At Site site-name: Diensttyp ‘any’darf nicht verwendet werden, wenn die Richtung ausgeht.

[SDW-16968]

Sonstiges

Obwohl der Kundenadministrator keinen Zugriff hat, um die Remote-Authentifizierungsserver zu löschen, zeigt die GUI das Löschsymbol an. Beim Versuch, den Löschvorgang auszuführen, wird jedoch der folgende Fehler angezeigt:

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

[SDW-18945]

Wenn Sie auf der Seite **Administration > Ankündigungen** auf Anbieterebene einen Kunden aus der oberen Menüleiste auswählen, wird eine leere Seite mit **Netzwerkadministration** als Überschrift angezeigt.

[SDW-18944]

Sie können die Datenbanksicherung, die in einem vom Anbieter verwalteten Setup in einem vom Kunden verwalteten Setup erstellt wurde, nicht wiederherstellen. Ebenso können Sie die Datenbanksicherung, die in einem vom Kunden verwalteten Setup in einem vom Anbieter verwalteten Setup erstellt wurde, nicht wiederherstellen.

[SDW-18904]

Wenn die Rolle customersecurity-admin mit schreibgeschütztem Zugriff auf die Site-Konfiguration versucht, die Konfiguration zu bearbeiten, anstatt unbefugten Zugriff anzuzeigen, wird ein rotes Banner mit einer Fehlermeldung angezeigt.

[SDW-1840]

Die Lizenzierungsfunktion wird im vom Anbieter verwalteten Setup von Citrix SD-WAN Orchestrator for On-premises nicht unterstützt. Anbieter können mit den Testlizenzen fortfahren. Es wird eine Nachfrist von 60 Tagen gewährt.

[SDW-1831]

Wenn eine Appliance länger als 20 Minuten die Verbindung zu Citrix SD-WAN Orchestrator for On-premises verliert und in die Phase der erneuten Registrierung übergeht, sendet sie eine falsche Seriennummer in der Registrierungsanforderung.

Problemumgehung: Starten Sie die Appliance neu.

[SDW-18781]

Nach dem Import gültiger Produktionsberechtigungen wird **die Option Upgrade auf Produktion** unter Lizenzierung verfügbar gemacht, noch bevor die Lizenz der Appliance zugewiesen wird.

Problemumgehung: Klicken Sie erst **auf Upgrade auf Produktion**, nachdem die Lizenz der Appliance zugewiesen wurde.

[SDW-18721]

Network Address Translation (NAT) wird zwischen Citrix SD-WAN Orchestrator for On-premises und der Appliance nicht unterstützt.

[SDW-18703]

In einem vom Anbieter verwalteten Setup werden die von den Anbieteradministratoren hinzugefügten Ankündigungen den Kunden bei ihrer Anmeldung nicht angezeigt.

[SDW-18491]

Die CLI ermöglicht es Benutzern, ein Kennwort außerhalb des zulässigen Längenbereichs von 8—128 zu erstellen, aber die GUI-Anmeldung schlägt fehl, wenn die Kennwortlänge außerhalb des zulässigen Bereichs liegt.

Problemumgehung: Bei der Anmeldung an der GUI ist der Benutzer gezwungen, die Länge des Kennworts auf den zulässigen Bereich zu ändern.

[SDW-16068]

Wenn ein Benutzer versucht, sich anzumelden, wird möglicherweise für den Bruchteil einer Sekunde oben auf der Seite ein rotes Banner angezeigt, bevor die Anmeldeseite angezeigt wird.

[SDW-16024]

Wenn die Datenbanksicherung einer Appliance auf einer anderen Appliance mit derselben Version von Citrix SD-WAN Orchestrator for On-premises wiederhergestellt wird, werden die Benutzerdetails nicht wiederhergestellt. Wenn Sie auf der wiederhergestellten Appliance einen Benutzer mit demselben Benutzernamen wie in der gesicherten Datenbank erstellen, wird der folgende Fehler angezeigt:

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

Problemumgehung: Erstellen Sie einen Benutzer mit einem anderen Benutzernamen, der in der gesicherten Datenbank nicht vorhanden war.

[SDW-15984]

Versionshinweise für Citrix SD-WAN Orchestrator for On-premises Version 9.6

July 17, 2023

In diesem Dokument mit den Versionshinweisen werden die Verbesserungen und Änderungen sowie behobene und bekannte Probleme beschrieben, die für den Citrix SD-WAN Orchestrator for On-premises Version 9.6 bestehen.

> **Hinweis**
>
> Dieses Dokument mit Versionshinweisen enthält keine sicherheitsbezogenen Fixes. Eine Liste der sicherheitsbezogenen Fixes und Advisorys finden Sie im Citrix Security Bulletin.

Neuigkeiten

Die Verbesserungen und Änderungen, die in Release 9.6 verfügbar sind.

Konfiguration und Management

Dynamisches Routing

Ab Citrix SD-WAN 11.3.1 können Sie eine Router-ID für das gesamte Protokoll und auch eine Router-ID pro Routingdomäne konfigurieren. Mit dieser Erweiterung können Sie ein stabiles dynamisches Routing über mehrere Instanzen hinweg aktivieren, wobei verschiedene Router-IDs stabil konvergieren.

[SDW-17097]

Sonstiges

HTTPS-Zertifikat

Das HTTPS-Zertifikat ist erforderlich, um eine sichere HTTPS-Verwaltungsverbindung mit Citrix SD-WAN Orchestrator for On-premises herzustellen. Sie können das Standardzertifikat verwenden, das auf dem Citrix SD-WAN Orchestrator for On-premises GUI verfügbar ist, oder ein benutzerdefiniertes HTTPS-Zertifikat hochladen, das aus einem anderen Framework wie OpenSSL generiert wurde. Mit dem benutzerdefinierten HTTPS-Zertifikat haben Sie die Kontrolle über die Sicherheit und die anderen Betreffparameter im Zusammenhang mit dem Zertifikat.

[SDW-16359]

Schnittstellen

Ab der Version Citrix SD-WAN 11.3.1 können Sie eine virtuelle Schnittstelle mithilfe des Kontrollkästchens **Aktiviert** aktivieren oder deaktivieren.

[SDW-15993]

Behobene Probleme

Die Probleme, die in Version 9.6 behoben werden.

Konfiguration und Management

Für die Citrix SD-WAN 6100 SE-Appliance zeigt die Benutzeroberfläche die **LAG-Seite** unter **Konfiguration > Erweiterte Einstellungen**nicht an.

[DWAN-HILFE-1895]

Sonstiges

Citrix SD-WAN Orchestrator for On-premises GUI fordert die Benutzer auf, sich alle eine Stunde anzumelden, auch wenn die GUI kontinuierlich verwendet wird und nicht im Leerlauf gelassen wird.

[DWAN-HILFE-1902]

Wenn Sie eine Site durch Klonen einer vorhandenen Site erstellen, schlägt die **Bereitstellung von Konfiguration/Software > Konfiguration überprüfen** fehl.

[SDW-16103]

Bekannte Probleme

Die Probleme, die in Version 9.6 bestehen.

Sonstiges

Wenn Sie Citrix SD-WAN Orchestrator for On-premises GUI auf einer neuen Registerkarte öffnen, während die Aktualisierung des Authentifizierungstokens ausgeführt wird, werden alle vorhandenen Sitzungen im Browser abgemeldet.

[SDW-17719]

Wenn die Größe der Festplatte auf mehr als 1,8 TB geändert wird, erfolgt keine Größenänderung der Festplatte.

[SDW-16404]

Mit der CLI können Benutzer ein Kennwort außerhalb des zulässigen Längenbereichs von 8 bis 128 erstellen. Die GUI-Anmeldung schlägt jedoch fehl, wenn die Kennwortlänge außerhalb des zulässigen Bereichs liegt.

Problemumgehung: Bei der Anmeldung an der GUI ist der Benutzer gezwungen, die Länge des Kennworts auf den zulässigen Bereich zu ändern.

[SDW-16068]

Wenn ein Benutzer versucht, sich anzumelden, wird möglicherweise für den Bruchteil einer Sekunde oben auf der Seite ein rotes Banner angezeigt, bevor die Anmeldeseite angezeigt wird.

[SDW-16024]

Wenn die Datenbanksicherung einer Appliance auf einer anderen Appliance mit derselben Version von Citrix SD-WAN Orchestrator for On-premises wiederhergestellt wird, werden die Benutzerdetails nicht wiederhergestellt. Wenn Sie auf der wiederhergestellten Appliance einen Benutzer mit demselben Benutzernamen wie in der gesicherten Datenbank erstellen, wird der folgende Fehler angezeigt:

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

Problemumgehung: Erstellen Sie einen Benutzer mit einem anderen Benutzernamen, der in der gesicherten Datenbank nicht vorhanden war.

[SDW-15984]

Versionshinweise für Citrix SD-WAN Orchestrator for On-premises 1.0

October 21, 2022

Citrix SD-WAN Orchestrator for On-Premises ist ein selbst gehosteter Verwaltungsdienst, der als separate Instanz für jeden Kunden verfügbar ist. Es bietet eine zentrale Glasmanagementplattform, mit der Sie alle SD-WAN-Appliances in Ihrem SD-WAN-Netzwerk konfigurieren, überwachen und analysieren können.

Citrix SD-WAN Orchestrator für On-Premises wird Kunden mit strengen behördlichen Anforderungen in Bezug auf Datenhoheit und Datenschutz empfohlen.

Im Folgenden sind einige der wichtigsten Funktionen aufgeführt:

- **Authentifizierung**: Unterstützt lokale und RADIUS-/TACACS+-Authentifizierung.
- **Zentralisierte Konfiguration**: Zentralisierte Konfiguration von SD-WAN-Netzwerken mit geführten Workflows, visuellen Hilfen und Profilen.
- **Zero-Touch-Bereitstellung**: Nahtloses Hochfahren des Netzwerks und der Verbindungen.
- **Anwendungsorientierte Richtlinien**: Anwendungsbasierte Verkehrssteuerung, Quality of Service (QoS) und Firewall-Richtlinien, global oder pro Standort konfigurierbar.
- **Hierarchische Zusammenfassung des Zustands**: Fähigkeit, den Zustand, die Nutzung, die Qualität und die Leistung eines Netzwerks als Ganzes zentral zu überwachen, mit der Möglichkeit, einzelne Standorte und zugehörige Verbindungen zu untersuchen.
- **Fehlerbehebung**: Geräte- und Überwachungsprotokolle, Diagnosedienstprogramme wie Ping, Traceroute, Paketerfassung zur Behebung von Netzwerkverbindungsproblemen.

Voraussetzungen

- **Geräte**: Mindestens zwei Geräte. Für jede SD-WAN-Appliance oder virtuelle Instanz muss eine IP-Adresse konfiguriert sein.
- **Citrix SD-WAN Orchestrator Service Orchestrator-Dienstkonto**: Um Citrix SD-WAN Orchestrator for On-premises verwenden zu können, müssen Sie über ein Konto im Citrix SD-WAN Orchestrator Service verfügen. Weitere Informationen finden Sie unter Onboarding des Citrix SD-WAN Orchestrator Service.

Citrix SD-WAN Orchestrator für Lokal 1.0.1

Behobene Probleme

- **SDW-16456**: Jede Routingdomäne wird in Citrix SD-WAN Orchestrator for On-premises nicht unterstützt.
- **SDW-16063**: Auf Netzwerkebene sind die Wi-Fi-Zusammenfassungsberichte nicht verfügbar.

- **SDW-16054**: Wenn ein Kundenkonto außerhalb der US-Region im Citrix SD-WAN Orchestrator Service erstellt wird, funktioniert das API-Token, das von der Seite Identity and Management (IDAM) von Citrix Cloud abgerufen wurde, nicht. Die Anmeldung des Kunden bei Citrix SD-WAN Orchestrator for On-premises schlägt mit der folgenden Fehlermeldung fehl: „Ungültige Kunden-ID, Client-ID oder Client Secret“.

  Sie können jetzt den **POP** auswählen, in dem Ihr Cloud-Konto integriert war, wenn Sie den Citrix SD-WAN Orchestrator for On-premises zum ersten Mal starten.

Bekannte Probleme

- **SDW-16068**: Mit der CLI können Benutzer ein Kennwort außerhalb des zulässigen Längenbereichs von 8—128 erstellen, aber die GUI-Anmeldung schlägt fehl, wenn die Kennwortlänge außerhalb des zulässigen Bereichs liegt.
  - **Problemumgehung**: Bei der Anmeldung an der GUI ist der Benutzer gezwungen, die Länge des Kennworts auf den zulässigen Bereich zu ändern.
- **SDW-16024**: Wenn sich ein Benutzer bei der Benutzeroberfläche anmeldet, wird möglicherweise für den Bruchteil einer Sekunde oben auf der Seite ein rotes Banner angezeigt, bevor die Anmeldeseite angezeigt wird.
- **SDW-15984**: Wenn die Datenbanksicherung einer Appliance auf einer anderen Appliance mit derselben Version von Citrix SD-WAN Orchestrator for On-premises wiederhergestellt wird, werden die Benutzerdetails nicht wiederhergestellt. Wenn Sie auf der wiederhergestellten Appliance einen Benutzer mit demselben Benutzernamen wie in der gesicherten Datenbank erstellen, wird der folgende Fehler angezeigt:

  Dem Benutzer wurde bereits eine Rolle zugewiesen
  - **Problemumgehung**: Erstellen Sie einen Benutzer mit einem anderen Benutzernamen, der in der gesicherten Datenbank nicht vorhanden war.
- **SDW-16103**: Wenn Sie eine Site durch Klonen einer vorhandenen Site erstellen, schlägt das **Bereitstellen von Konfiguration/Software > Konfiguration überprüfen** fehl.
  - **Problemumgehung**: Erstellen Sie keine Site, indem Sie eine vorhandene Site klonen.
- **SDW-16404**: Wenn die Größe der Festplatte auf mehr als 1,8 TB geändert wird, erfolgt keine Größenänderung der Festplatte.

Systemanforderungen und Installation

October 21, 2022

Stellen Sie vor der Installation von Citrix SD-WAN Orchestrator for On-premises auf einer virtuellen Maschine (VM) sicher, dass Sie die Hardware- und Softwareanforderungen verstehen und die Voraussetzungen erfüllt haben.

> **Hinweis:**
>
> Die Systemanforderungen gelten sowohl für Netzwerke mit einer Region als auch für Netzwerke mit mehreren Regionen.

Hardwareanforderungen

Im Folgenden sind die Hardwareanforderungen für Citrix SD-WAN Orchestrator for On-premises aufgeführt, um Daten von einem Monat oder Statistiken für zwei WAN-Verbindungen pro Standort im Durchschnitt zu speichern:

Anzahl der Standorte	Prozessor	RAM	Speicher
2000	256 vCPUs 3 GHz oder höher	512 GB	2 TB
1000	128 vCPUs 3 GHz oder höher	256 GB	1 TB
500	64 vCPUs 3 GHz oder höher	128 GB	500 GB
256	32 vCPU 3 GHz oder höher	64 GB	256 GB
128	8 vCPUs 3 GHz oder höher	16 GB	256 GB

Software

Citrix SD-WAN Orchestrator for On-premises VPX kann auf den folgenden Plattformen konfiguriert werden:

Hypervisor

- VMware ESXi 7.0 Update 1.
- VMware ESXi Server, Version 6.5.

- Citrix XenServer 6.5 oder höher.

Browser müssen Cookies aktiviert und JavaScript installiert und aktiviert haben.

Citrix SD-WAN Orchestrator for On-premises Webinterface wird in den folgenden Browsern unterstützt:

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

Voraussetzungen

Im Folgenden sind die Voraussetzungen für die Installation und Bereitstellung von Citrix SD-WAN Orchestrator for On-premises aufgeführt:

- Der SD-WAN Master Control Node (MCN) und vorhandene Clientknoten müssen auf die neueste Citrix SD-WAN-Softwareversion aktualisiert werden.
- Es wird empfohlen, einen DHCP-Server im SD-WAN-Netzwerk verfügbar und konfiguriert zu haben.
- Sie müssen über die Installationsdateien von Citrix SD-WAN Orchestrator for On-premises verfügen.

> **Hinweis**
>
> Sie können keine Software von Drittanbietern auf Citrix SD-WAN Orchestrator for On-premises anpassen oder installieren. Sie können jedoch die vCPU-, Arbeitsspeicher- und Speichereinstellungen ändern.

Laden Sie die Citrix SD-WAN Orchestrator for On-Premises-Software herunter

Laden Sie die Softwareinstallationsdateien für Citrix SD-WAN Orchestrator for On-premises Management Console für die erforderliche Version und Plattform von der Seite Downloads herunter .

Die Installationsdateien von Citrix SD-WAN Orchestrator for On-premises verwenden die folgende Namenskonvention:

- ctx-sdw-onprem-build.Erweiterung
- ctx-onprem-build.Erweiterung
- ctx-onprem-build.Erweiterung

Plattform	Erweiterung
Citrix XenServer	.xva
VMware ESXi	-vmware.ova

Installations- und Konfigurationsprüfliste

Dieser Abschnitt enthält eine Checkliste mit den Informationen, die Sie zum Ausfüllen Ihres Citrix SD-WAN Orchestrator für die lokale Installation und Bereitstellung benötigen.

Sammeln oder ermitteln Sie die folgenden Informationen:

- Die IP-Adresse des ESXi-Servers und des XenServer, der den Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen (VM) hostet.
- Ein eindeutiger Name, der dem Citrix SD-WAN Orchestrator für lokale VM zugewiesen werden kann.
- Die Speichermenge, die für den Citrix SD-WAN Orchestrator für lokale VM zugewiesen werden soll.
- Die Menge der Datenträgerkapazität, die für das virtuelle Laufwerk für die VM zugewiesen werden soll.
- Die Gateway-IP-Adresse, die der Citrix SD-WAN Orchestrator für lokale Netzwerke verwendet, um mit externen Netzwerken zu kommunizieren.
- Die Subnetzmaske für das Netzwerk, in dem der Citrix SD-WAN Orchestrator für lokale VM installiert ist.

> **Hinweis**
>
> Citrix empfiehlt, regelmäßig Snapshots der VM- und SD-WAN-Konfigurationen zu erstellen.

Unterschied zwischen SD-WAN Orchestrator for On-premises und Citrix SD-WAN Orchestrator Service

October 21, 2022

Features

Features	Citrix SD-WAN Orchestrator-Dienst	Citrix SD-WAN Orchestrator für lokal
Advanced Edition-Plattform	Ja	Nein
Premium Edition-Plattform	Ja	Nein
Zscaler-Service	Ja	Nein
Azure Virtual WAN-Dienst	Ja	Nein
Citrix Secure Internet Access-Dienst	Ja	Nein
Gehostete Firewall	Ja	Nein
Anwendungsrouting auf voreingestellten DPI-Apps und benutzerdefinierten Apps (FQDN- oder IP-basiert)	Ja	Ja
Anwendungsrouting für Apps, die dynamische Signaturaktualisierungen erfordern (wie Office 365, Citrix Cloud und neu unterstützte Apps).	Ja	Nein
Orchestrator — Hochverfügbarkeit	Ja	Nein

Anforderungen

Anforderungen	Citrix SD-WAN Orchestrator-Dienst	SD-WAN Orchestrator für On-Premises
SD-WAN Factory-Image erforderlich	Alle (Werksversandversion)	Citrix SD-WAN 10.2.7, 11.1.1, 11.2.0, 11.2.2, 11.3.0 und höher. *
Im Netzwerk bereitgestellte Appliance	Alle	Citrix SD-WAN 11.2.2, 11.3.0 und höher. *
Internetverbindung der SD-WAN-Appliance	Erforderlich	Nicht erforderlich
Firewall-Ports sollen geöffnet sein	443	443, 22, ICMP
Lizenzierung	Postpaid- und Prepaid-Modelle	Nur Prepaid-Modell

Anforderungen	Citrix SD-WAN Orchestrator-Dienst	SD-WAN Orchestrator für On-Premises

- Die unterstützte Citrix SD-WAN-Softwareversion hängt von der SD-WAN Orchestrator for On-Premises-Softwareversion ab.

Installieren und Konfigurieren von SD-WAN Orchestrator für On-Premises auf ESXi Server

October 21, 2022

Installieren Sie den VMware vSphere Client

Im Folgenden finden Sie die grundlegenden Anweisungen zum Herunterladen und Installieren des VMware vSphere-Clients, den Sie zum Erstellen und Bereitstellen des Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen (VM) verwenden.

Gehen Sie wie folgt vor, um den VMware vSphere Client herunterzuladen und zu installieren:

1. Öffnen Sie einen Browser und navigieren Sie zu dem ESXi-Server, der Ihren vSphere Client und die Citrix SD-WAN Orchestrator for On-Premises-Instanz der virtuellen Maschine hostet. Die Willkommensseite von VMware ESXi wird angezeigt.
2. Klicken Sie auf den Link **vSphere Client** herunterladen, um die vSphere Client-Installationsdatei herunterzuladen.
3. Installieren Sie den vSphere Client.

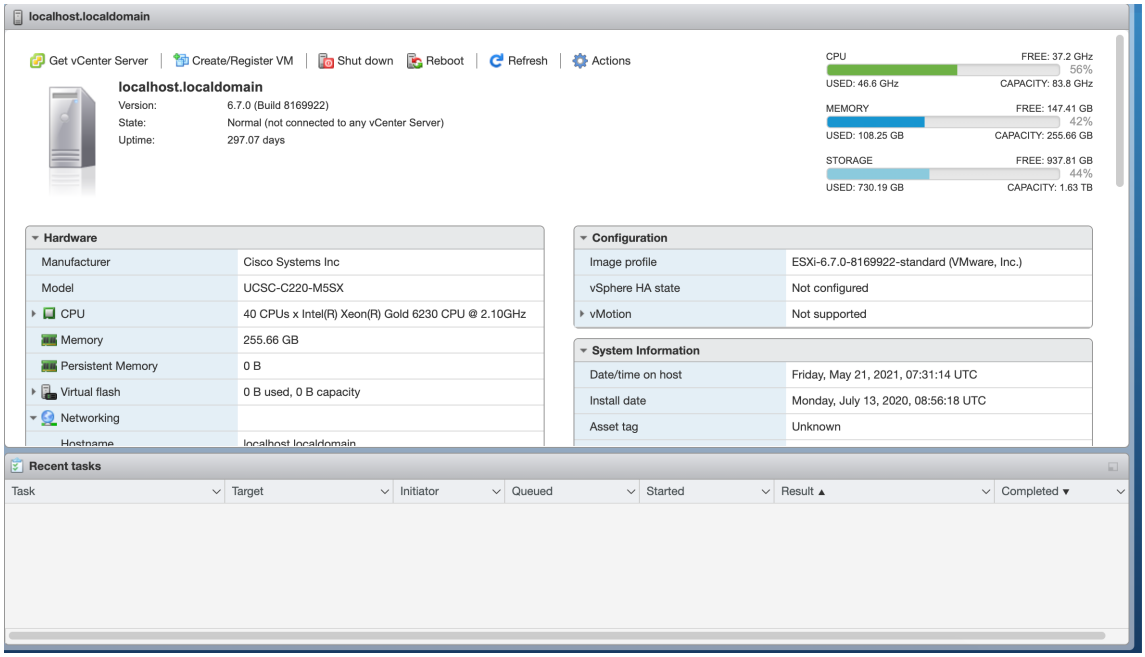
   Führen Sie die heruntergeladene vSphere Client-Installationsdatei aus und akzeptieren Sie jede der Standardoptionen, wenn Sie dazu aufgefordert werden.
4. Starten Sie nach Abschluss der Installation das vSphere Client-Programm.

   Die Anmeldeseite für den VMware vSphere Client wird angezeigt und fordert Sie zur Eingabe der Anmeldeinformationen für den ESXi-Server auf.
5. Geben Sie die Anmeldeinformationen für den ESXi-Server ein:

   - **IP-Adresse/Name**: Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) für den ESXi-Server ein, der Ihre Instanz von Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen hostet.

- **Benutzername**: Geben Sie den Namen des Serveradministratorkontos ein. Der Standardwert ist Stamm.
- **Passwort**: Geben Sie das Passwort ein, das mit diesem Administratorkonto verknüpft ist.

6. Klicken Sie auf **Anmelden**.
   Die vSphere Client-Hauptseite wird angezeigt.



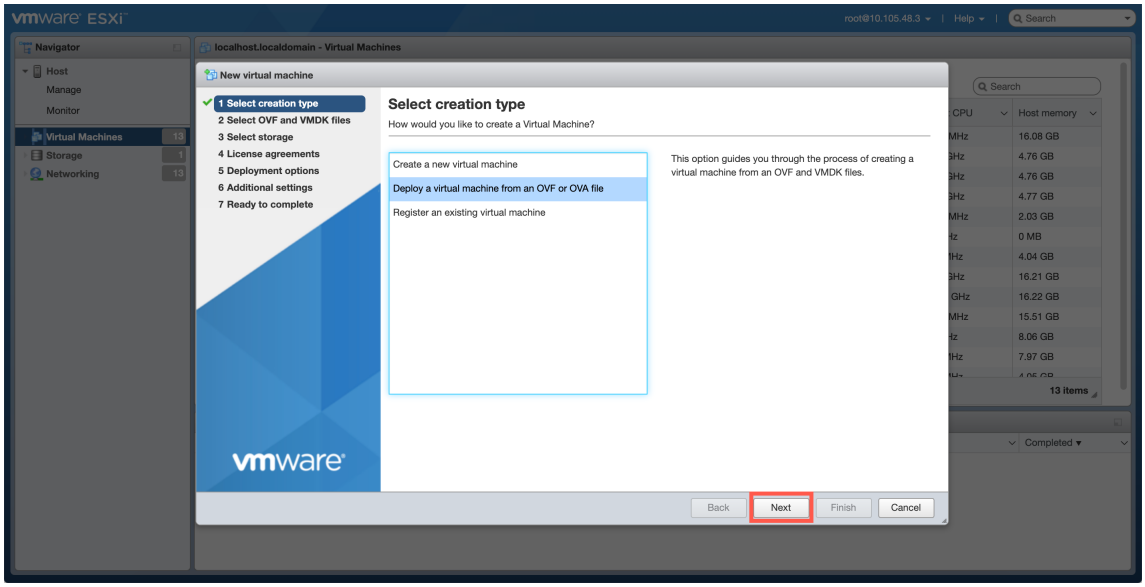
Erstellen des Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen mithilfe der OVF-Vorlage

Erstellen Sie nach der Installation des VMware vSphere-Clients den Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen.

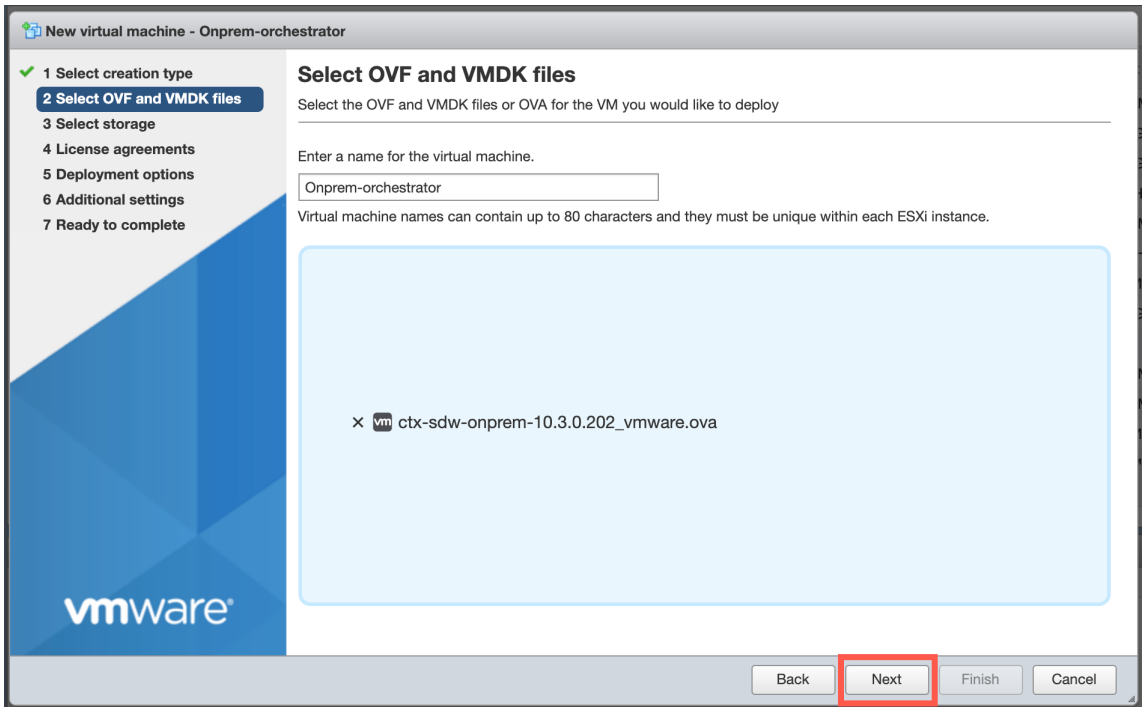
1. Wenn Sie dies noch nicht getan haben, laden Sie die Citrix SD-WAN Orchestrator for On-premises OVF-Vorlagendatei (.ova-Datei) auf den lokalen PC herunter.

   Weitere Informationen finden Sie unter Systemanforderungen und Installation.

2. Klicken Sie im vSphere Client auf **VM erstellen/registrieren**und wählen Sie dann **Bereitstellen einer virtuellen Maschine aus einer OVF- oder OVA-Datei** aus der Liste aus. Klicken Sie auf **Weiter**.

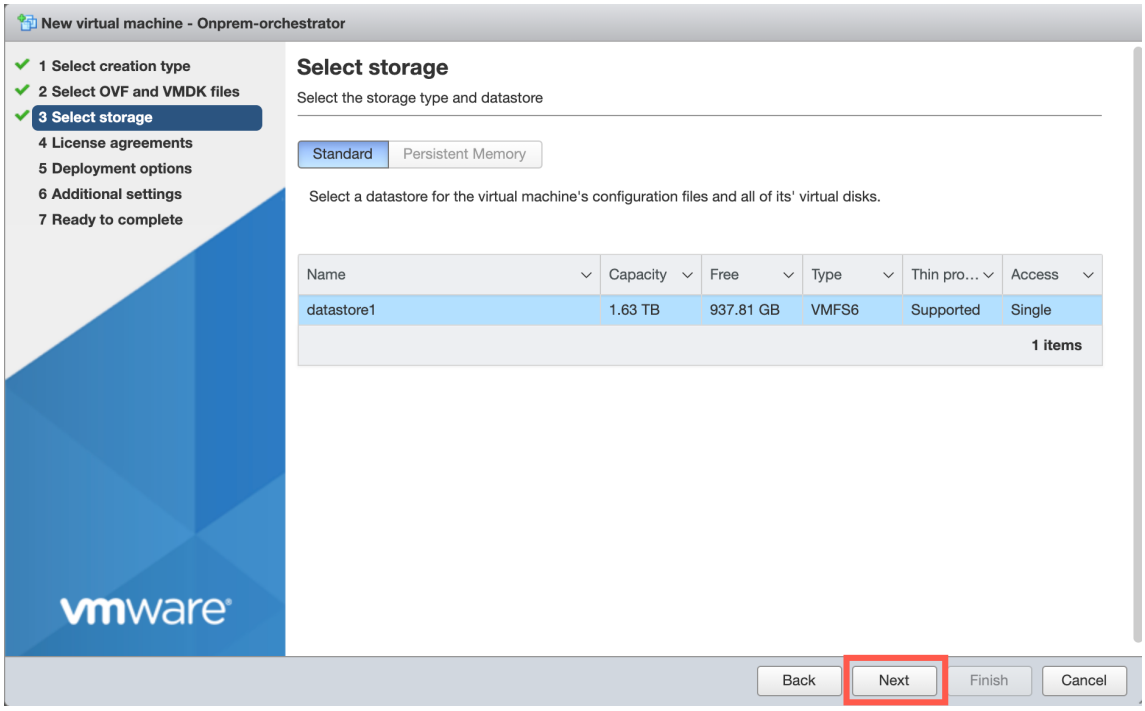


3. Geben Sie einen eindeutigen Namen für die neue virtuelle Maschine ein.
4. Klicken Sie in das Feld und wählen Sie die Citrix SD-WAN Orchestrator for On-premises OVF-Vorlage (.ova-Datei) aus, die Sie installieren möchten, oder ziehen Sie die Datei in das Feld.
5. Klicken Sie auf **Weiter**.

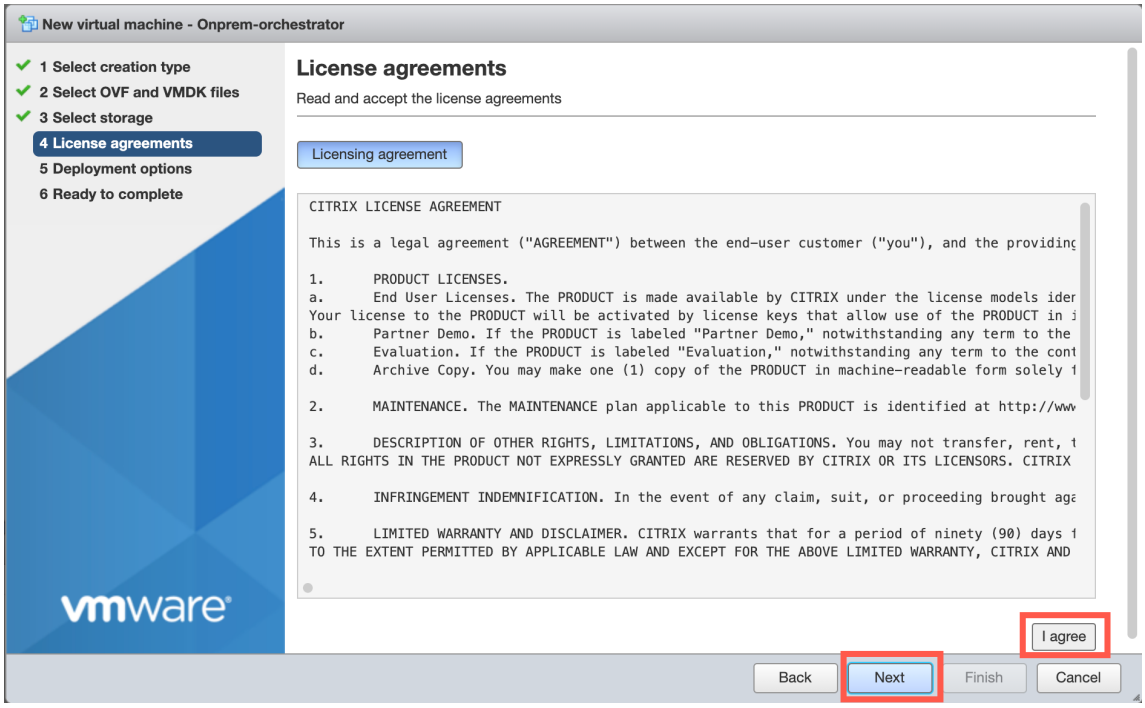


6. Klicken Sie auf **Weiter**.

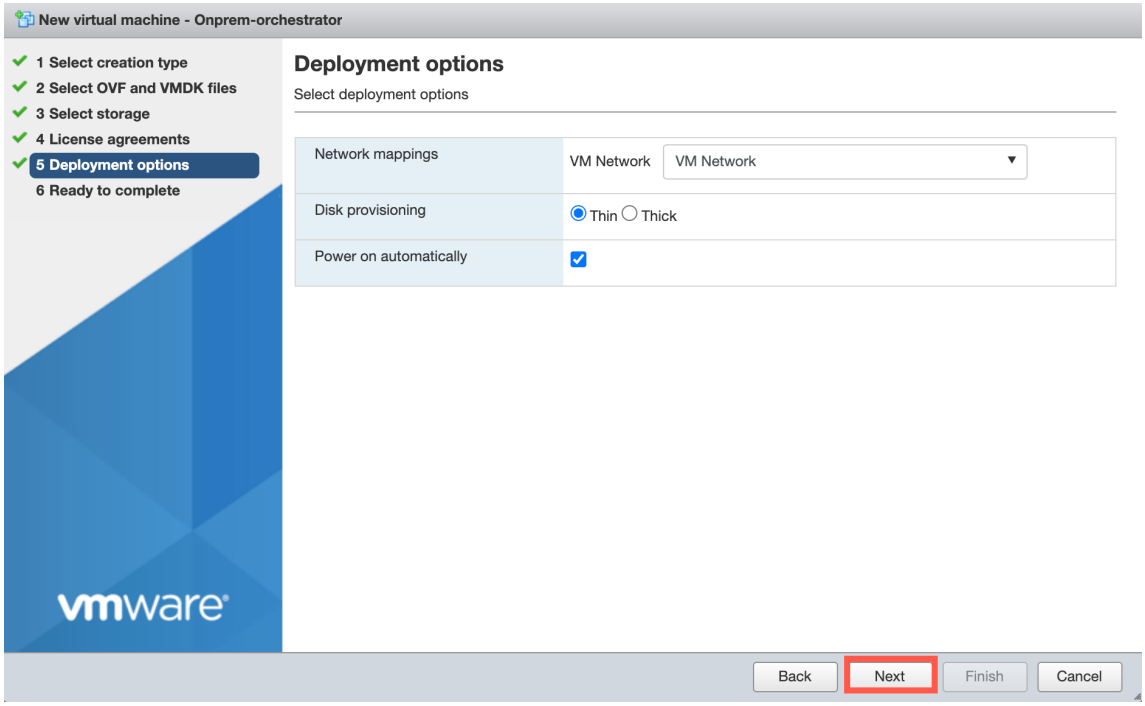
   Die Seite „Speicher“wird angezeigt.
7. Übernehmen Sie die Standardspeicherressource, indem Sie auf **Weiter**



8. Klicken Sie auf der Seite EULA auf **Ich stimme zu**und klicken Sie auf **Weiter**.

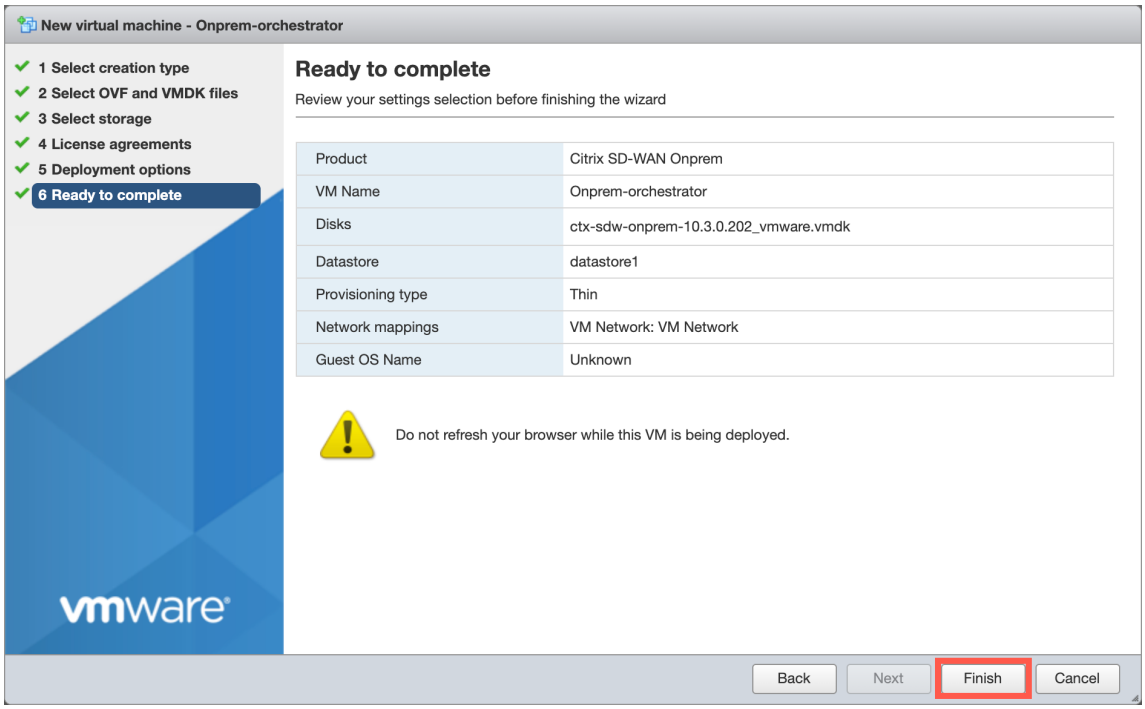


9. Wählen Sie auf der Optionsseite Bereitstellung das VM-Netzwerk aus der Dropdownliste aus und akzeptieren Sie die Standardeinstellungen für andere Felder. Klicken Sie auf **Weiter**.



10. Klicken Sie auf der Seite Bereit zur Fertigstellung auf **Fertig stellen**, um die virtuelle Maschine zu erstellen.

> **Hinweis:**
>
> Das Dekomprimieren des Disk-Images auf dem Server kann mehrere Minuten dauern.

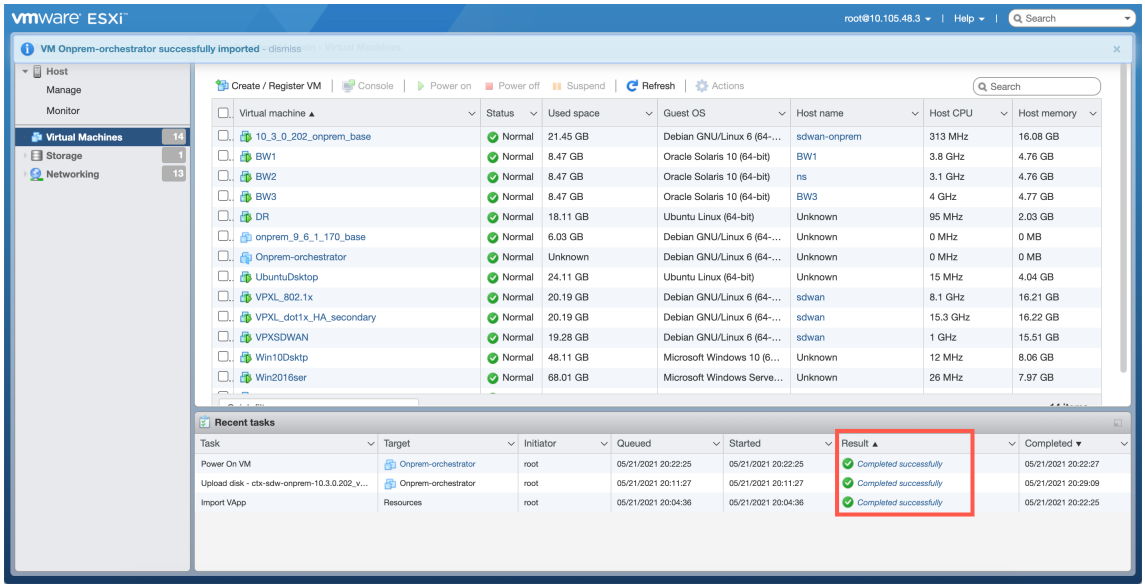


Anzeigen und Aufzeichnen der Verwaltungs-IP-Adresse auf dem ESXi-Server

Die Verwaltungs-IP-Adresse ist die IP-Adresse des Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen. Verwenden Sie diese IP-Adresse, um sich bei der Citrix SD-WAN Orchestrator for On-premises Web-Benutzeroberfläche anzumelden.

Gehen Sie wie folgt vor, um die Verwaltungs-IP-Adresse anzuzeigen:

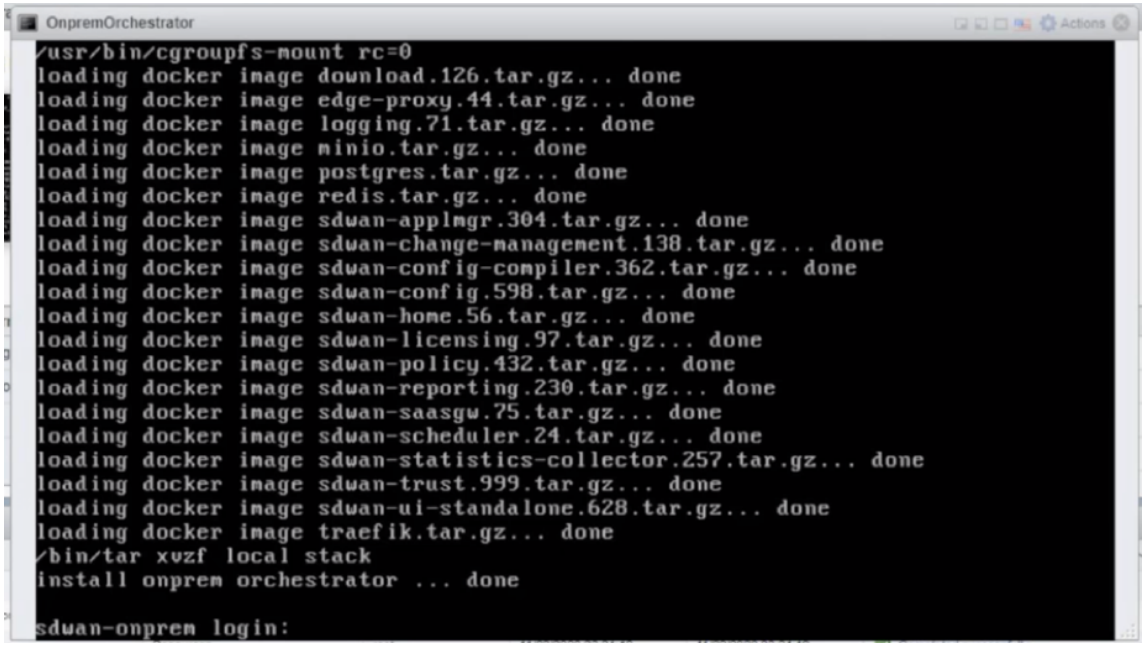
1. Wählen Sie auf der Seite vSphere Client Inventory den neuen Citrix SD-WAN Orchestrator für lokale virtuelle Maschine aus.
2. Warten Sie auf der Seite Citrix SD-WAN Orchestrator for On-premises unter Letzte Aufgaben, bis das Ergebnis als abgeschlossen angezeigt wird.



3. Wählen Sie die Registerkarte **Konsole** und klicken Sie dann auf eine beliebige Stelle im Konsolenbereich, um in den Konsolenmodus zu wechseln

> **Hinweis**
>
> Um die Konsolensteuerung des Cursors freizugeben, drücken Sie gleichzeitig die <Alt> Tasten <Ctrl> und.

4. Drücken Sie die **Eingabetaste**, um die Anmeldeaufforderung für die Konsole anzuzeigen.

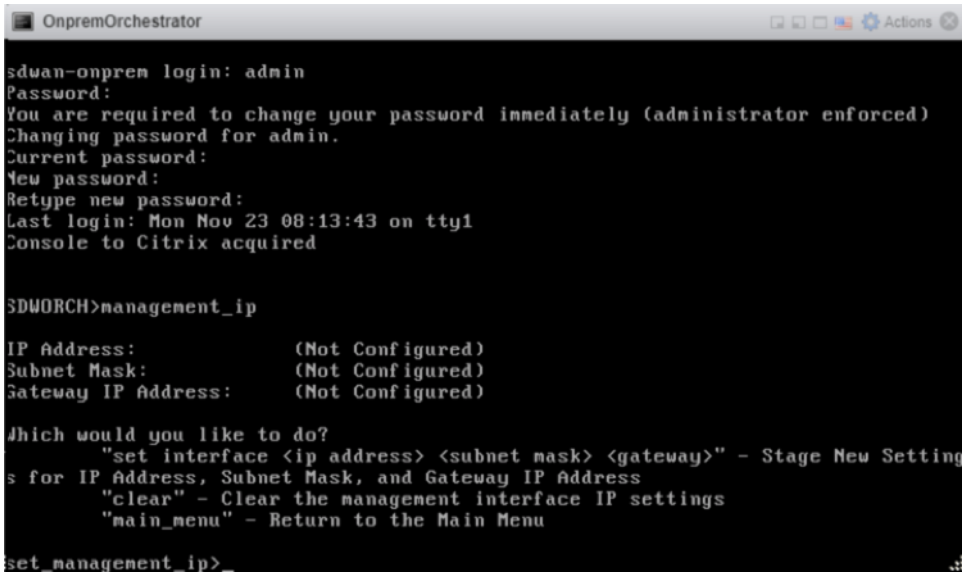


5. Melden Sie sich bei der VM-Konsole an.

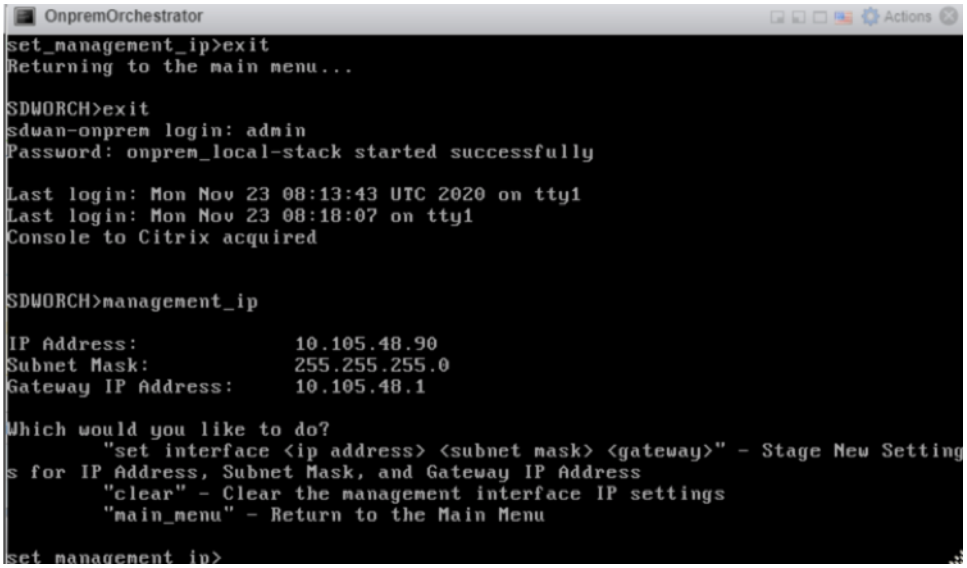
   Die Standardanmeldeinformationen für den neuen Citrix SD-WAN Orchestrator für lokale virtuelle Maschine lauten wie folgt:

   - **Einloggen**: admin
   - **Kennwort**: password

   > **Hinweis**
   >
   > Es ist zwingend erforderlich, das Standardkennwort für das Admin-Benutzerkonto bei der ersten Anmeldung zu ändern. Diese Änderung wird sowohl mit CLI als auch mit der Benutzeroberfläche erzwungen.



6. Notieren Sie die Verwaltungs-IP-Adresse der virtuellen Maschine von Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen, die als Host-IP-Adresse in einer Begrüßungsnachricht angezeigt wird, die bei der Anmeldung angezeigt wird.



> **Hinweis**
>
> - Der DHCP-Server muss im SD-WAN-Netzwerk vorhanden und verfügbar sein, andernfalls kann dieser Schritt nicht abgeschlossen werden.
> - Geben Sie in der Konsole den CLI-Befehl ein, `set_dns` um die aktuelle DNS-Servereinstellung zu bestätigen und den DNS-Server neu zu konfigurieren, wenn der vorhandene DNS-Server den DNS-Dienst nicht bereitstellen kann. Weitere Informationen zur Verwendung des `set_dns` Befehls finden Sie unter Citrix SD-WAN Orchestrator für die lokale Anmeldung.

Wenn der DHCP-Server nicht im SD-WAN-Netzwerk konfiguriert ist, müssen Sie manuell eine statische IP-Adresse eingeben.

So konfigurieren Sie eine statische IP-Adresse als Verwaltungs-IP-Adresse:

1. Wenn die virtuelle Maschine gestartet wird, klicken Sie auf die Registerkarte **Konsole** .
2. Melden Sie sich bei der virtuellen Maschine an. Die Standardanmeldeinformationen für den neuen Citrix SD-WAN Orchestrator für lokale virtuelle Maschine lauten wie folgt:
   - **Einloggen**: admin
   - **Kennwort**: password
3. Geben Sie in der Konsole den CLI-Befehl ein `management_ip`.
4. Geben Sie den Befehl ein `set interface <ipaddress> <subnetmask> <gateway>`, um die Management-IP zu konfigurieren.
5. Sind Sie sicher, dass Sie die IP-Einstellungen der Verwaltungsschnittstelle ändern möchten?

   Sie können die Verbindung zur Appliance verlieren. <y/n>?

   Drücken Sie „y“, um die IP zu ändern und nach fast 6—7 Minuten auf die neue konfigurierte Management-IP zuzugreifen.

Installieren und konfigurieren Sie SD-WAN Orchestrator für On-Premises auf XenServer

October 21, 2022

Bevor Sie den Citrix SD-WAN Orchestrator für eine lokale virtuelle Maschine auf einem XenServer installieren, sammeln Sie die erforderlichen Informationen, wie in Installations- und Konfigurationscheckliste beschrieben.

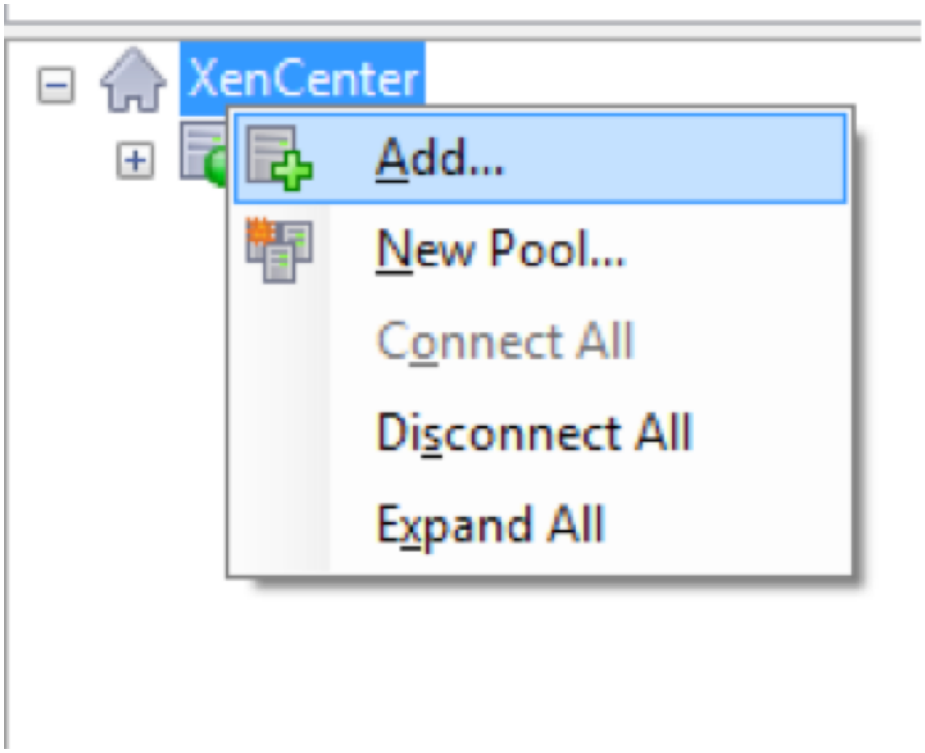
Installieren Sie den XenServer-Server

Um den Citrix XenServer zu installieren, auf dem Sie den Citrix SD-WAN Orchestrator für lokale virtuelle Maschine bereitstellen, muss XenCenter auf Ihrem Computer installiert sein. Wenn Sie dies noch nicht getan haben, laden Sie XenCenter herunter und installieren Sie es.

So installieren Sie einen XenServer-Server:

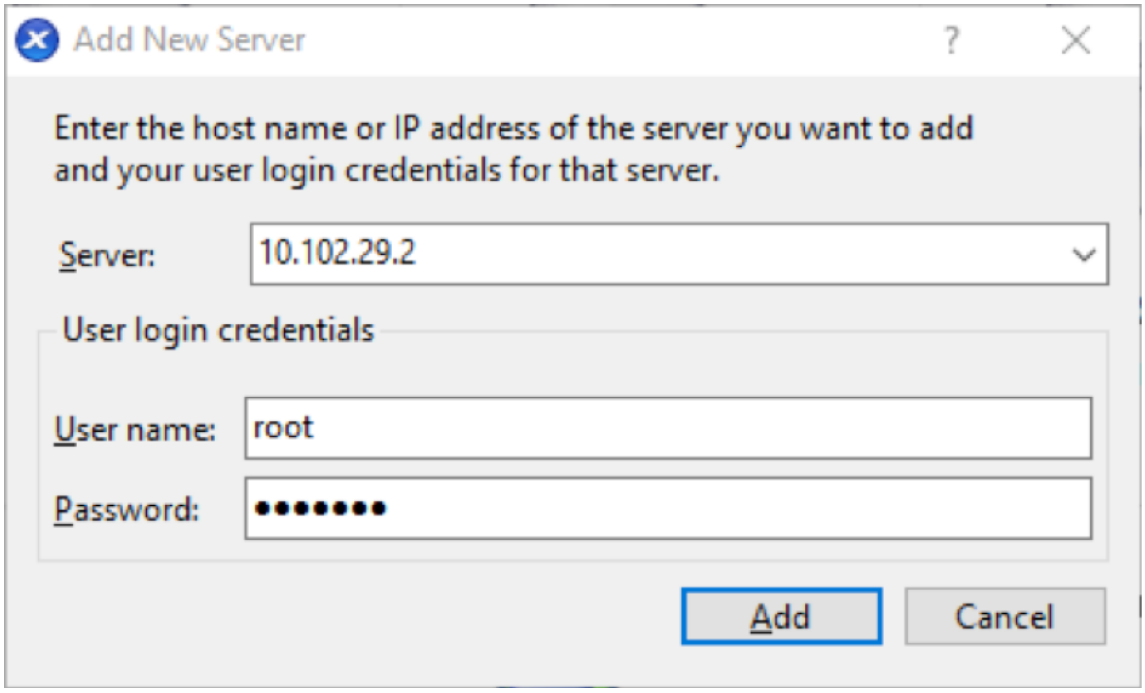
1. Öffnen Sie die XenCenter-Anwendung auf Ihrem Computer.

2. Klicken Sie im linken Strukturbereich mit der rechten Maustaste auf **XenCenter** und wählen Sie **Hinzufügen**aus.



3. Geben **Sie im Fenster Neuen Server hinzufügen** die erforderlichen Informationen in die folgenden Felder ein:

   - **Server**: Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) des XenServer-Servers ein, der die Instanz von Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen hostet.
   - **Benutzername**: Geben Sie den Namen des Serveradministratorkontos ein. Der Standardwert ist Stamm.
   - **Passwort**: Geben Sie das Passwort ein, das mit diesem Administratorkonto verknüpft ist.



4. Klicken Sie auf **Hinzufügen**.

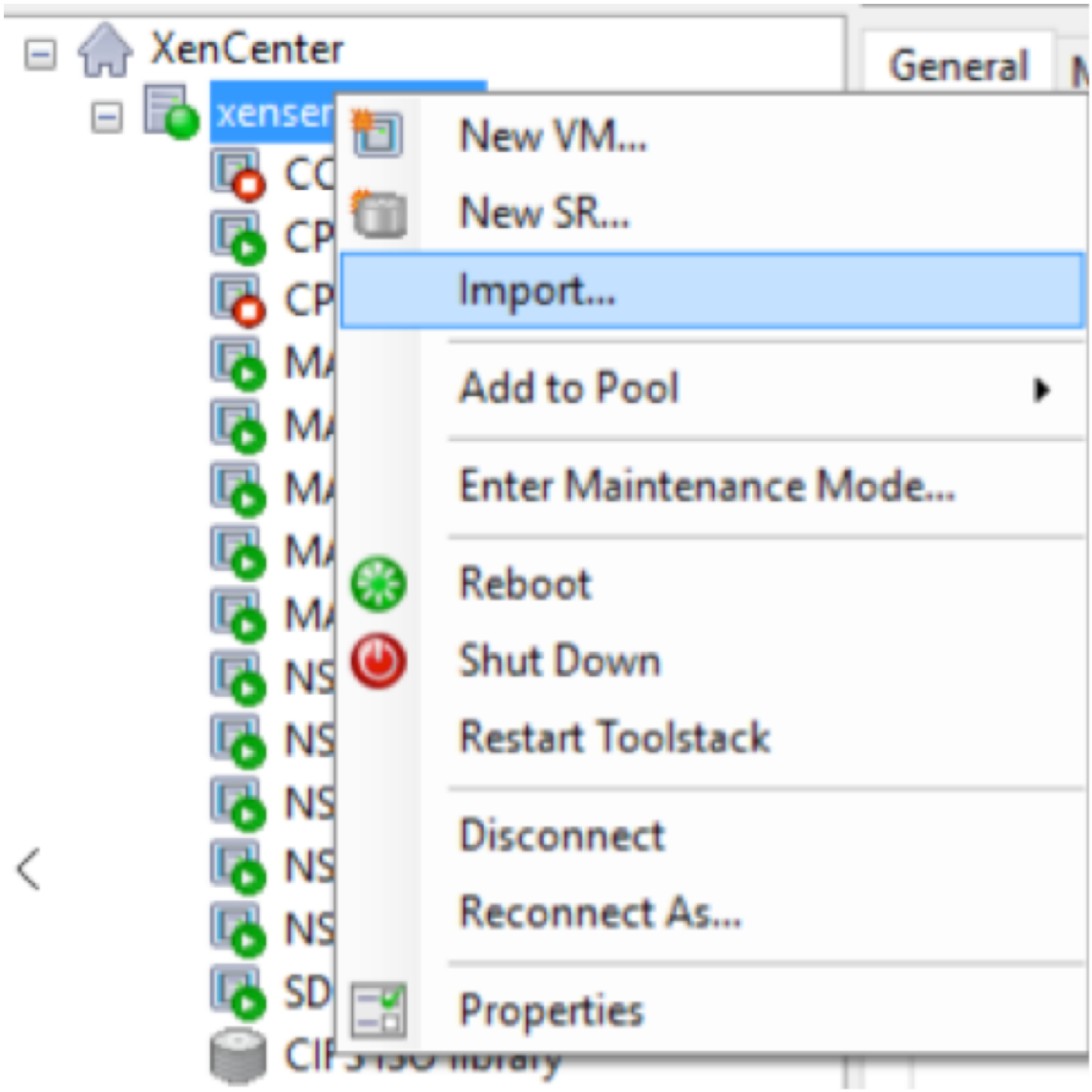
Die IP-Adresse des neuen Servers wird im linken Bereich angezeigt.

Erstellen Sie den Citrix SD-WAN Orchestrator für lokale virtuelle Maschine mithilfe der XVA-Datei

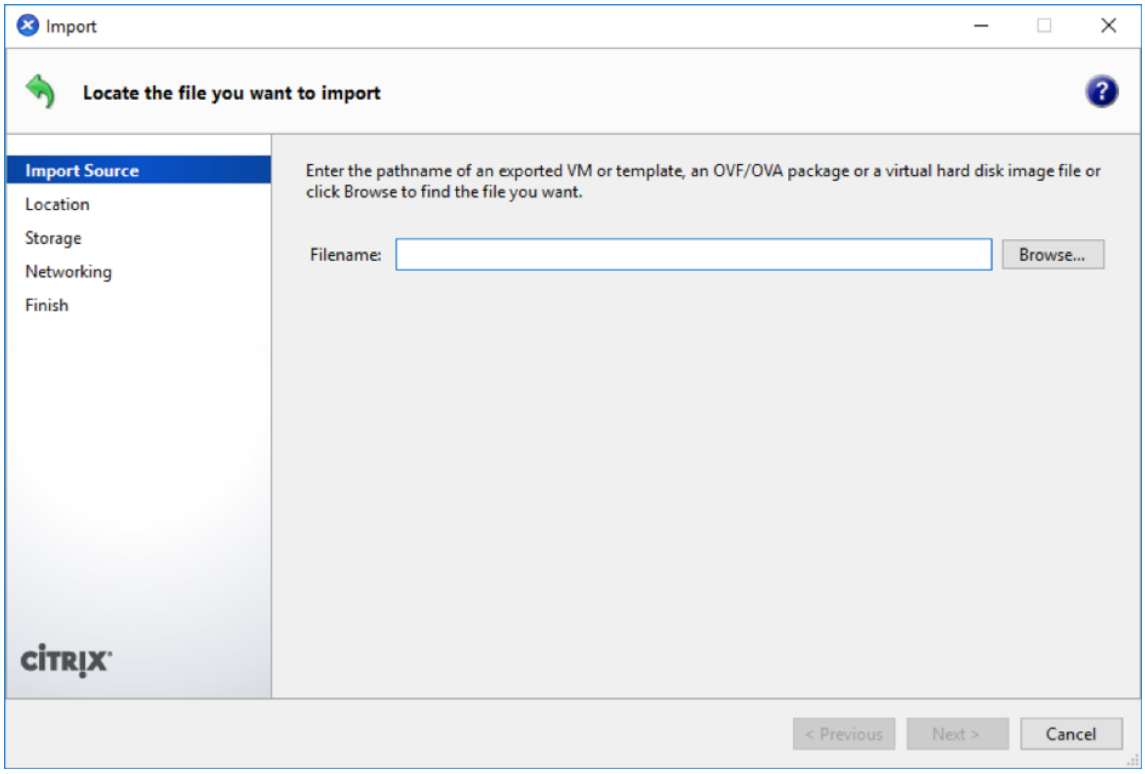
Die Software Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen wird als XVA-Datei bereitgestellt. Wenn Sie dies noch nicht getan haben, laden Sie die XVA-Datei herunter. Weitere Informationen finden Sie unter Systemanforderungen und Installation.

So erstellen Sie den Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen:

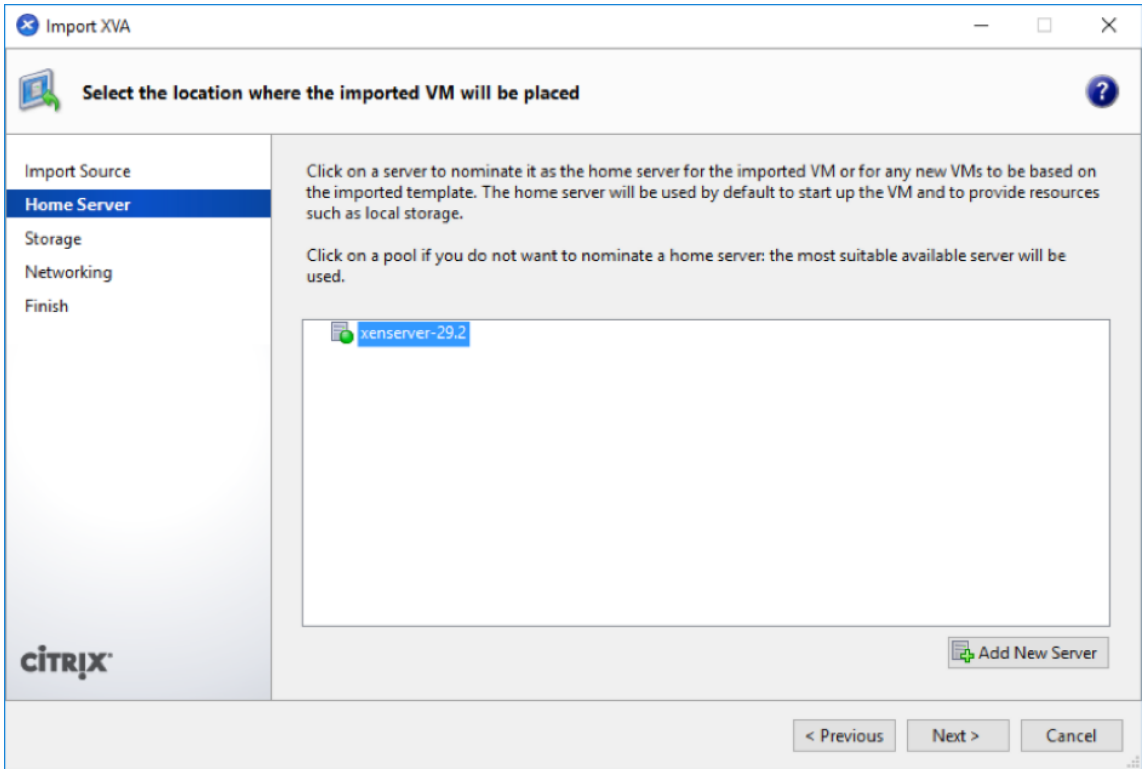
1. Klicken Sie in XenCenter mit der rechten Maustaste auf **XenServer** und klicken **Sie**auf



2. Navigieren Sie zur heruntergeladenen XVA-Datei, wählen Sie sie aus und klicken Sie auf **Weiter**.



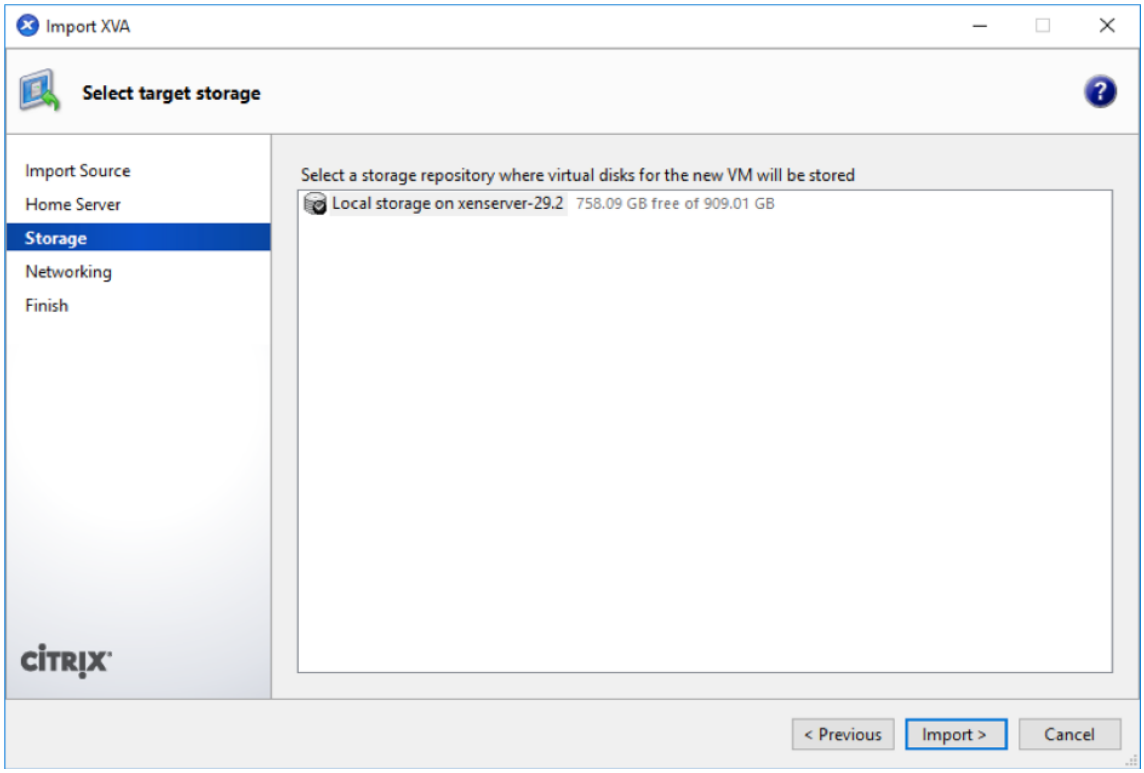
3. Wählen Sie einen zuvor erstellten XenServer-Server als Speicherort aus, in den die virtuelle Maschine importiert werden soll, und klicken Sie auf **Weiter**.



4. Wählen Sie ein Speicher-Repository aus, in dem das virtuelle Laufwerk für die neue virtuelle

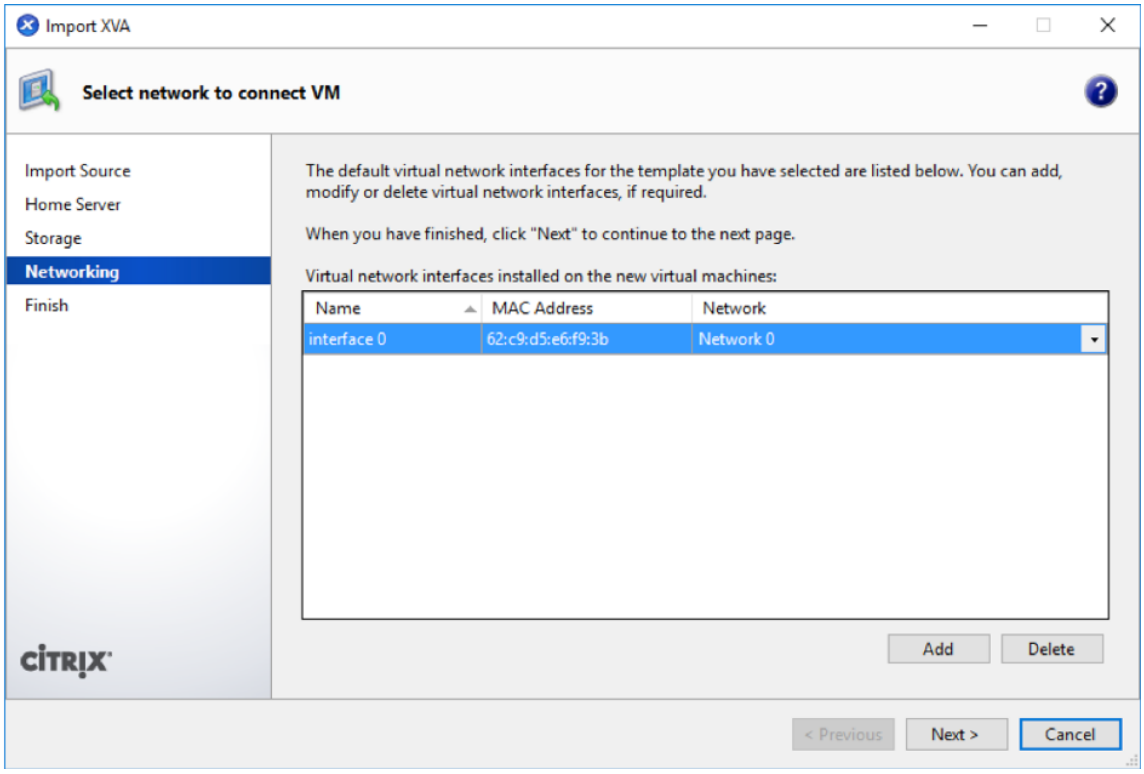
Maschine gespeichert ist, und klicken Sie auf **Importieren**.

Im Moment können Sie die Standardspeicherressource akzeptieren. Oder Sie können den Datenspeicher konfigurieren.



Der importierte Citrix SD-WAN Orchestrator für lokale virtuelle Maschine wird im linken Bereich angezeigt.

5. Wählen Sie ein Netzwerk aus, mit dem die virtuelle Maschine verbunden werden soll, und klicken Sie auf **Weiter**.



6. Klicken Sie auf **Fertig stellen**.

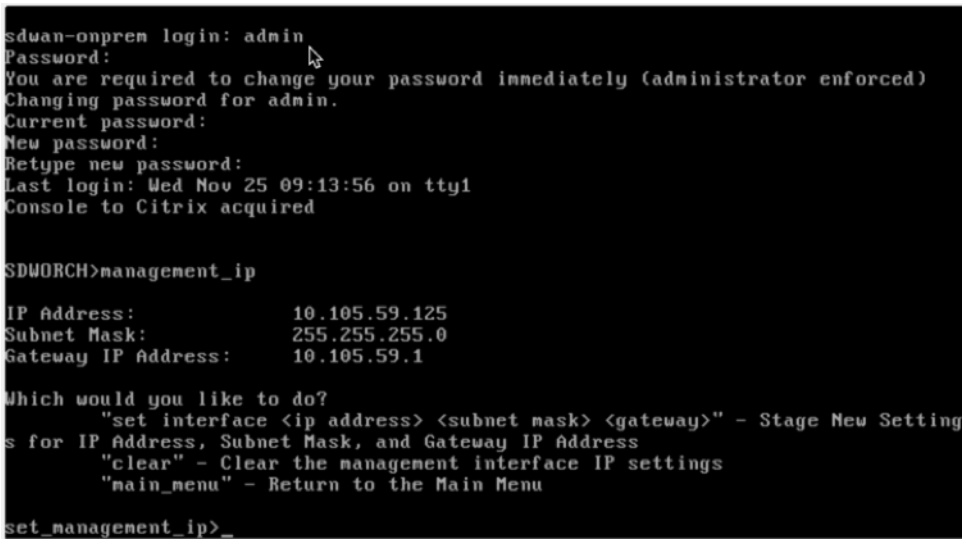
Anzeigen und Aufzeichnen der Management-IP-Adresse auf XenServer

Die Verwaltungs-IP-Adresse ist die IP-Adresse des Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen. Verwenden Sie diese IP-Adresse, um sich bei der Citrix SD-WAN Orchestrator for On-premises Web-Benutzeroberfläche anzumelden.

> **Hinweis**
>
> Der DHCP-Server muss im SD-WAN-Netzwerk vorhanden und verfügbar sein.

So zeigen Sie die Management-IP-Adresse an:

1. Klicken Sie in der XenCenter-Oberfläche im linken Bereich mit der rechten Maustaste auf die neue virtuelle Maschine Citrix SD-WAN Orchestrator for On-premises, und wählen Sie **Start**aus.
2. Wenn die virtuelle Maschine gestartet wird, klicken Sie auf die Registerkarte **Konsole** .



3. Notieren Sie sich die Management-IP-Adresse.

   > **Hinweis**
   >
   > Der DHCP-Server muss im SD-WAN-Netzwerk vorhanden und verfügbar sein, andernfalls kann dieser Schritt nicht abgeschlossen werden.

4. Melden Sie sich bei der virtuellen Maschine an. Die Standardanmeldeinformationen für den neuen Citrix SD-WAN Orchestrator für lokale virtuelle Maschine lauten wie folgt:

   Einloggen: admin

   Kennwort: password

   > **Hinweis:**
   >
   > Es ist zwingend erforderlich, das Standardkennwort für das Admin-Benutzerkonto bei der ersten Anmeldung zu ändern. Diese Änderung wird sowohl mit CLI als auch mit der Benutzeroberfläche erzwungen.

   Wenn der DHCP-Server nicht im Citrix SD-WAN-Netzwerk konfiguriert ist, müssen Sie manuell eine statische IP-Adresse eingeben.

So konfigurieren Sie eine statische IP-Adresse als Verwaltungs-IP-Adresse:

1. Wenn die virtuelle Maschine gestartet wird, klicken Sie auf die Registerkarte Konsole.
2. Melden Sie sich bei der virtuellen Maschine an. Die Standardanmeldeinformationen für den neuen Citrix SD-WAN Orchestrator für lokale virtuelle Maschine lauten wie folgt:

   Einloggen: admin

   Kennwort: password

3. Geben Sie in der Konsole den CLI-Befehl ein `management_ip`.
4. Geben Sie den Befehl ein `set interface <ipaddress> <subnetmask> <gateway>`, um die Management-IP zu konfigurieren.
5. Sind Sie sicher, dass Sie die IP-Einstellungen der Verwaltungsschnittstelle ändern möchten?

   Sie können die Verbindung zur Appliance verlieren. <y/n>?

   Drücken Sie „y“, um die IP zu ändern und nach fast 6—7 Minuten auf die konfigurierte Management-IP zuzugreifen.

Onboarding des SD-WAN Orchestrator für On-Premises

October 21, 2022

Hier finden Sie eine Übersicht über den Onboarding-Prozess von Citrix SD-WAN Orchestrator for On-premises:

- Onboarding-Anbieter und Mandanten: Unsere Kunden können einen verwalteten SD-WAN-Dienst von Citrix-Partnern nutzen, der durch den mandantenfähigen Citrix SD-WAN Orchestrator-Dienst aktiviert wird.
- Onboarding „Do It Yourself“(DIY) -Unternehmen: Der Citrix SD-WAN Orchestrator Service ist auch als selbstverwalteter Dienst für Unternehmen verfügbar.

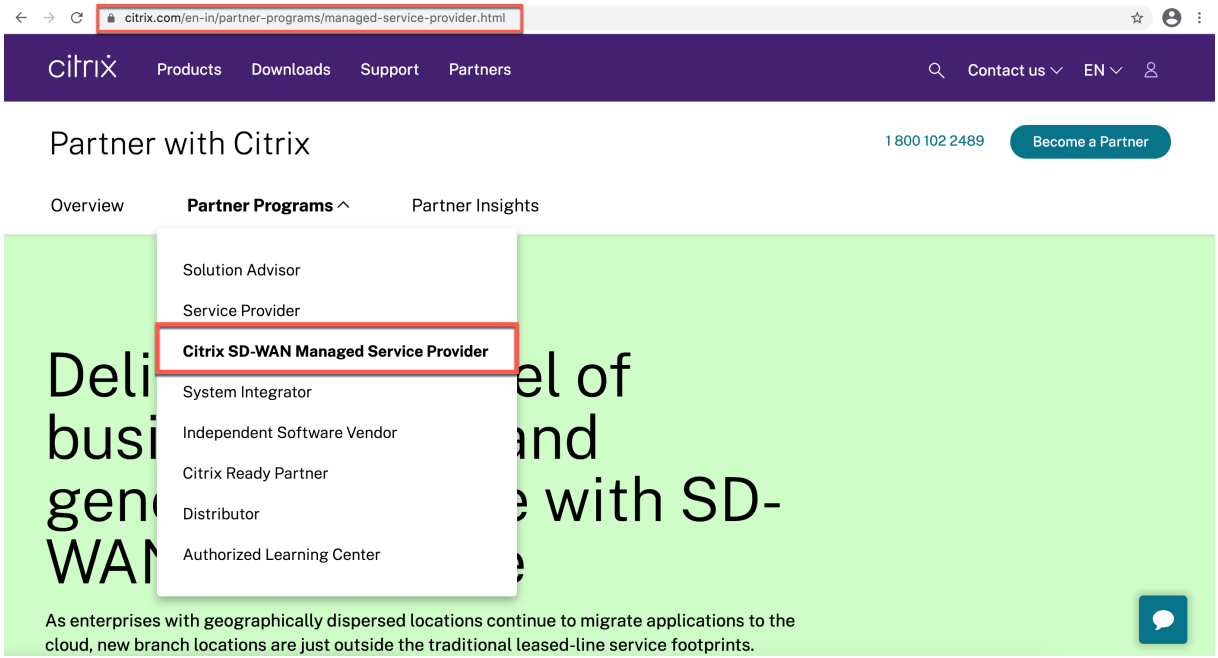
Onboarding-Anbieter und Mieter

In diesem Abschnitt wird der Onboarding-Prozess für Citrix-Partner und ihre Mandanten beschrieben. Hier ist eine Zusammenfassung des Onboarding-Prozesses:

1. Ein potenzieller Partner meldet sich als Citrix Partneran.
2. Citrix Partner registriert sich als Citrix SD-WAN Reseller.

Partner meldet sich für ein Citrix-Partnerprogramm an

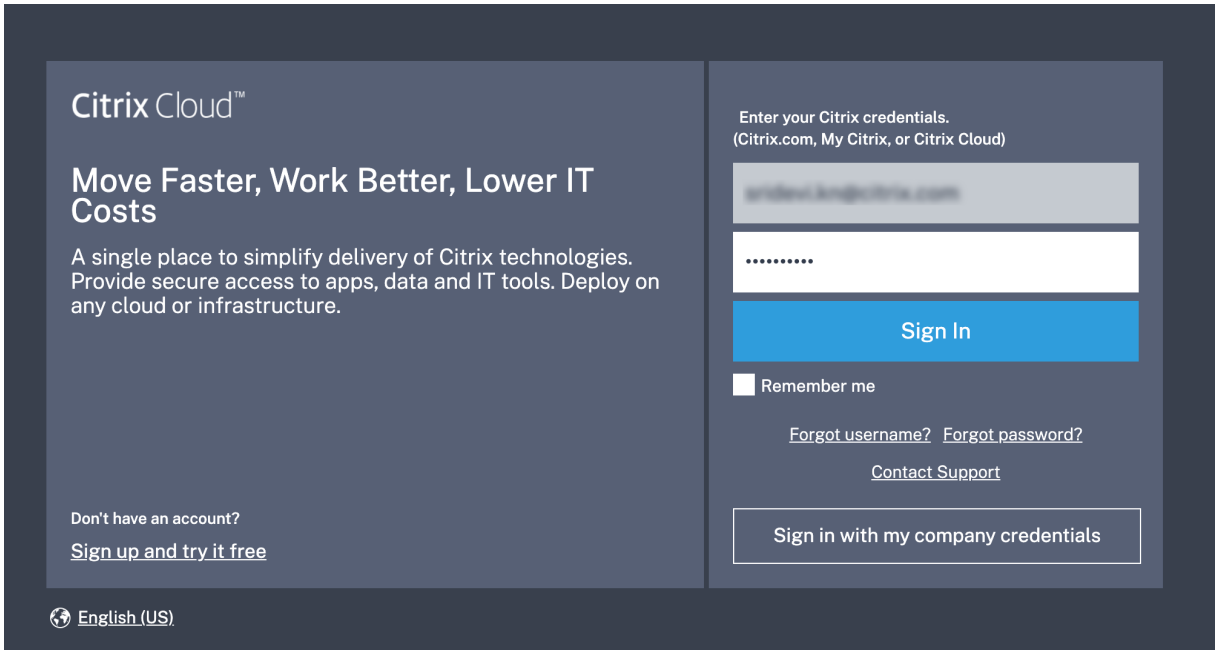
Ein potenzieller Partner muss sich für das Citrix Service Provider Program (CSP) - CSP-Anmeldung anmelden.
Ein Partner kann sich auch für das Citrix SD-WAN Managed Service Provider-Programm anmelden, das speziell für Citrix SD-WAN-Partner entwickelt wurde - SD-WAN MSP-Anmeldung.



Im Rahmen des Registrierungsprozesses wird für den Partner ein Citrix Cloud (CC) -Konto erstellt. Weitere Informationen finden Sie unter Anmelden für Citrix Cloud.

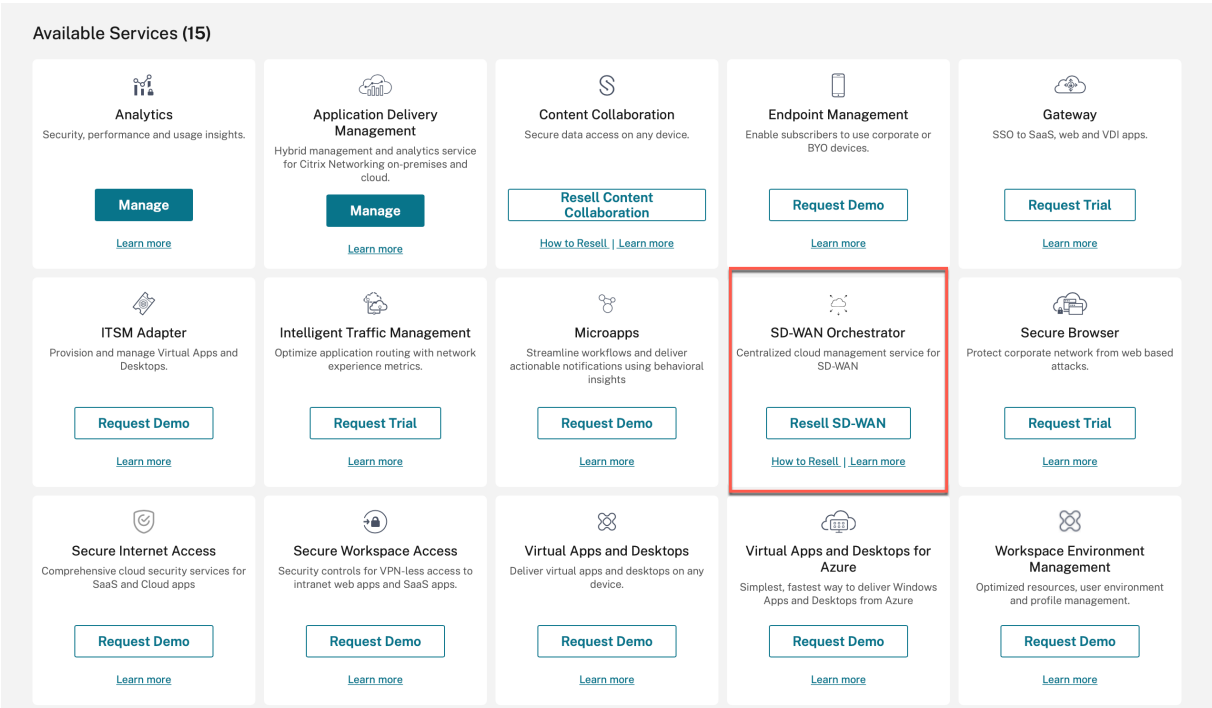
Partner registriert sich als Citrix SD-WAN-Reseller

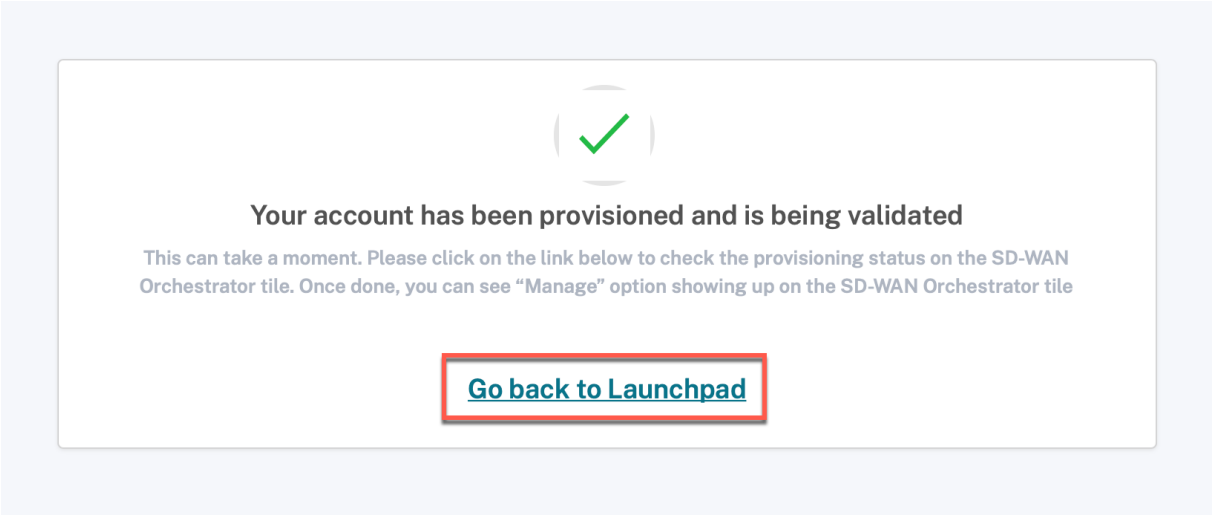
Der Partner meldet sich beim Citrix Cloud-Konto an.



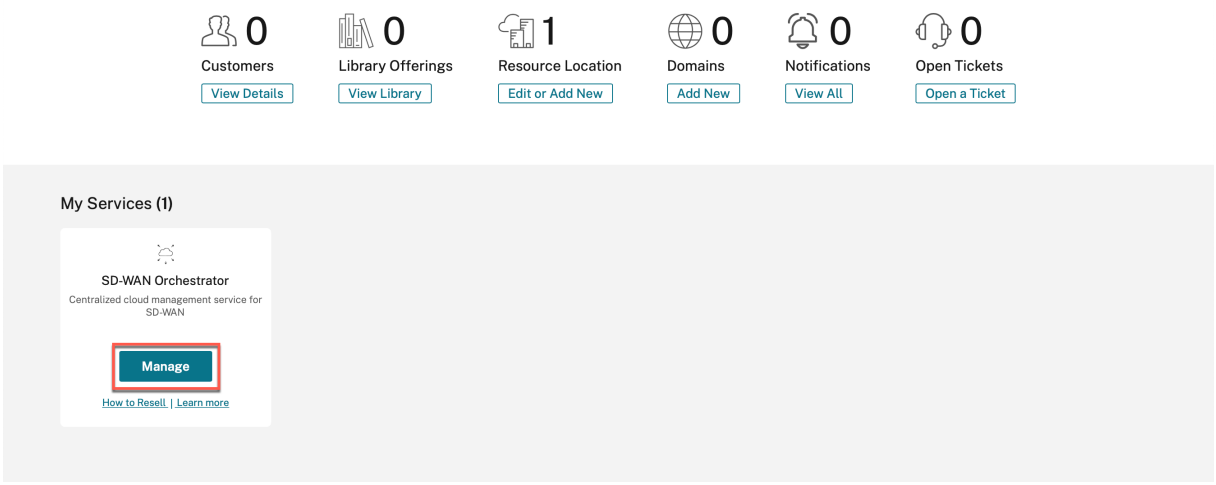
Ein Menü mit allen verfügbaren Diensten, die in Citrix Cloud angeboten werden, wird auf der Startseite angezeigt. Die **Citrix SD-WAN Orchestrator Service Orchestrator-Dienstkachel** finden Sie im

Abschnitt **Verfügbare Dienste** . Der Partner klickt in der Kachel auf **SD-WAN weiterverkaufen**, um sich als Citrix SD-WAN-Reseller oder -Dienstanbieter zu registrieren.





Die **Citrix SD-WAN Orchestrator Service Orchestrator-Dienstkachel** wird jetzt unter **Meine Dienste**angezeigt.

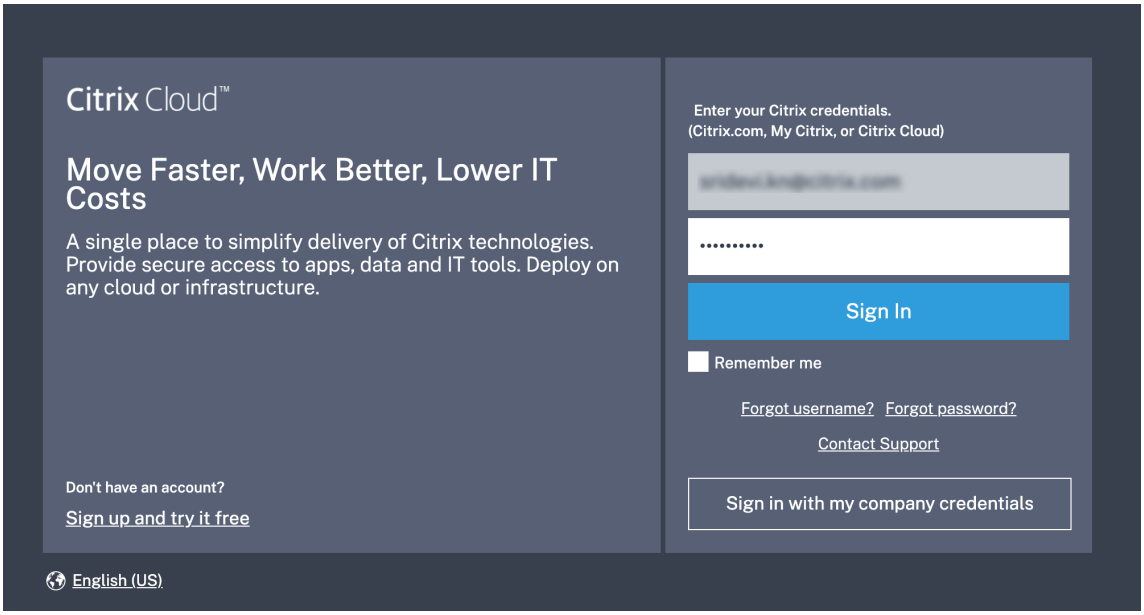


Onboarding von DIY-Unternehmenskunden

In diesem Abschnitt wird der Prozess zur Einbindung von DIY-Unternehmenskunden und das Verfahren zum Einladen von Administratoren zur Verwaltung ihres SD-WAN-Netzwerks beschrieben.

Onboarding von DIY-Kunden

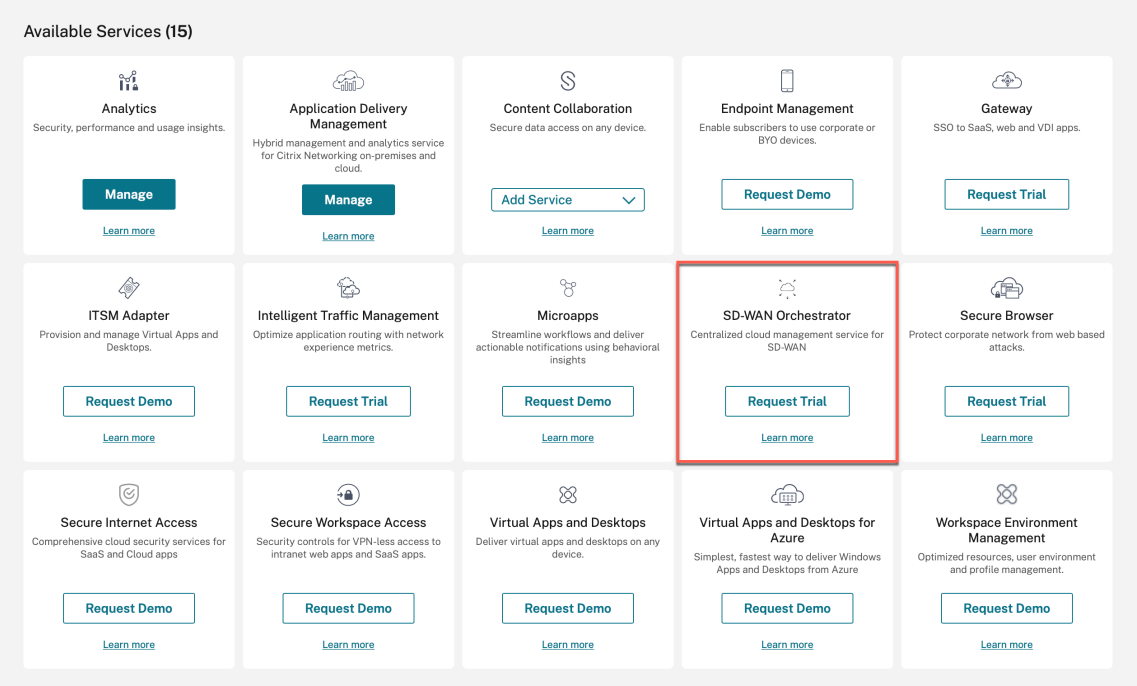
1. Der Kunde meldet sich beim Citrix Cloud Cloud-Konto an.



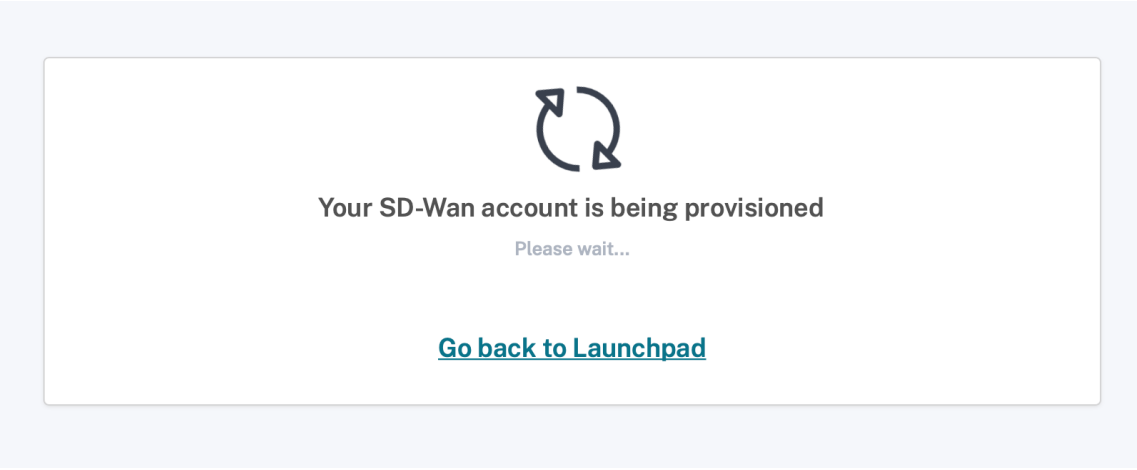
   Ein Menü mit allen verfügbaren Diensten, die in Citrix Cloud angeboten werden, wird auf der Startseite angezeigt. Die **Citrix SD-WAN Orchestrator Service Orchestrator-Dienstkachel** finden Sie im Abschnitt **Verfügbare Dienste** .

> **Hinweis**
>
> Stellen Sie sicher, dass Sie sich mit nur einem offiziellen Konto bei Citrix Cloud anmelden. Der verwendete Firmenname und die E-Mail-ID müssen nur mit einem Citrix Cloud-Konto verknüpft sein.

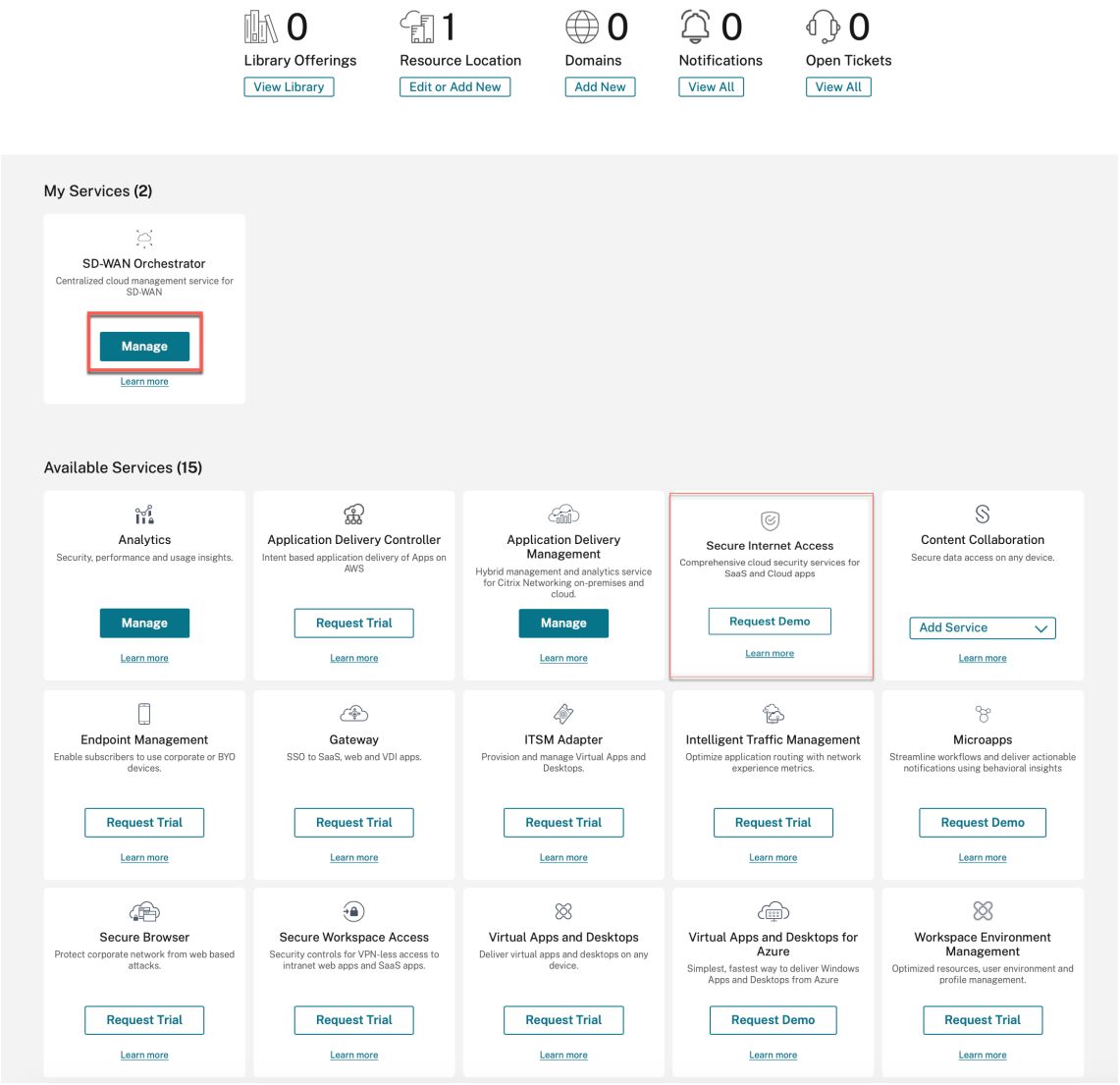
2. Der Kunde klickt auf **Testversion anfordern**.



Das SD-WAN-Konto des Kunden wird bereitgestellt.



3. Die **Citrix SD-WAN Orchestrator Service Orchestrator-Dienstkachel** wird jetzt unter **Meine Dienste**angezeigt.



Citrix SD-WAN Orchestrator für die lokale Anmeldung

July 17, 2023

In diesem Artikel wird beschrieben, wie sich ein Kunde zum ersten Mal beim Citrix SD-WAN Orchestrator for On-premises anmelden kann.

Im Folgenden sind die Voraussetzungen aufgeführt, die Sie benötigen, bevor Sie sich beim Citrix SD-WAN Orchestrator for On-premises anmelden:

- Sie müssen über ein Citrix Cloud Cloud-Konto verfügen. Weitere Informationen finden Sie unter Kunde greift auf SD-WAN Orchestratorzu.

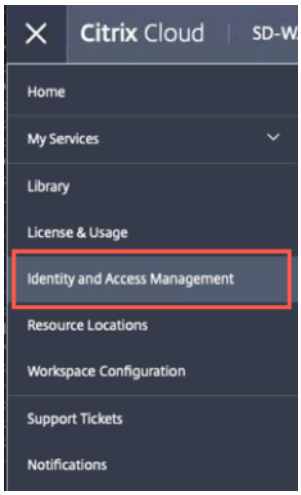
- Um Citrix SD-WAN Orchestrator for On-premises verwenden zu können, müssen Sie über ein Konto im Citrix SD-WAN Orchestrator Service verfügen. Weitere Informationen finden Sie unter Onboarding des Citrix SD-WAN Orchestrator Service.
- Erstellen Sie einen Administrator mit benutzerdefinierten Berechtigungen.
- Erstellen Sie einen Client über die API-Zugriffsseite, um die Kunden-ID, die ID und das geheime Detail abzurufen. Diese Details werden während der Anmeldung von Citrix SD-WAN Orchestrator for On-premises benötigt.

> **Hinweis**
>
> Ohne Cloud-Login können Sie nicht mit der lokalen Anmeldung fortfahren.

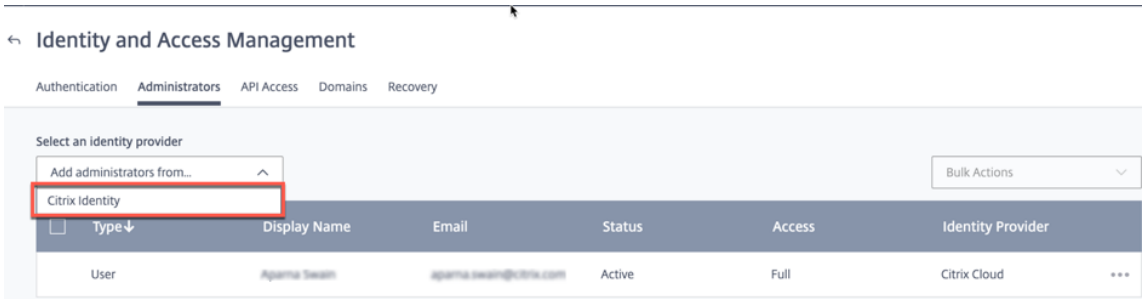
Administrator erstellen

Ein Anbieter oder ein Unternehmenskunde kann einen Administrator einladen, sein SD-WAN-Netzwerk zu verwalten. Führen Sie die folgenden Schritte aus, um einen Administrator einzuladen:

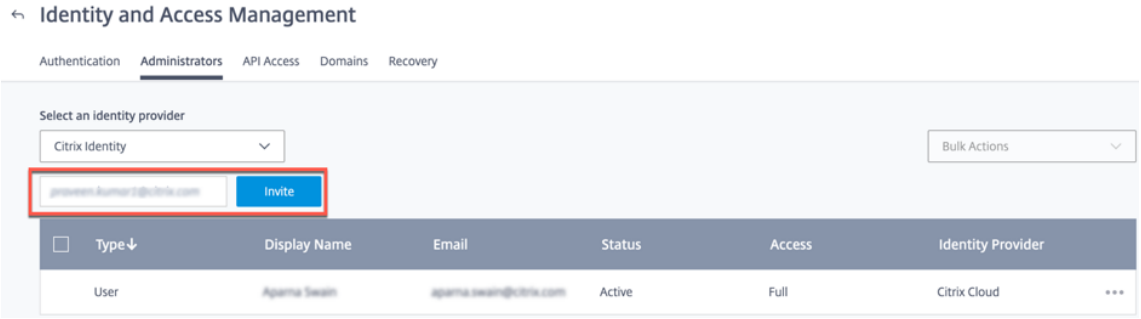
1. Melden Sie sich bei der Citrix Cloud an und navigieren Sie zu **Identity and Access Management**.



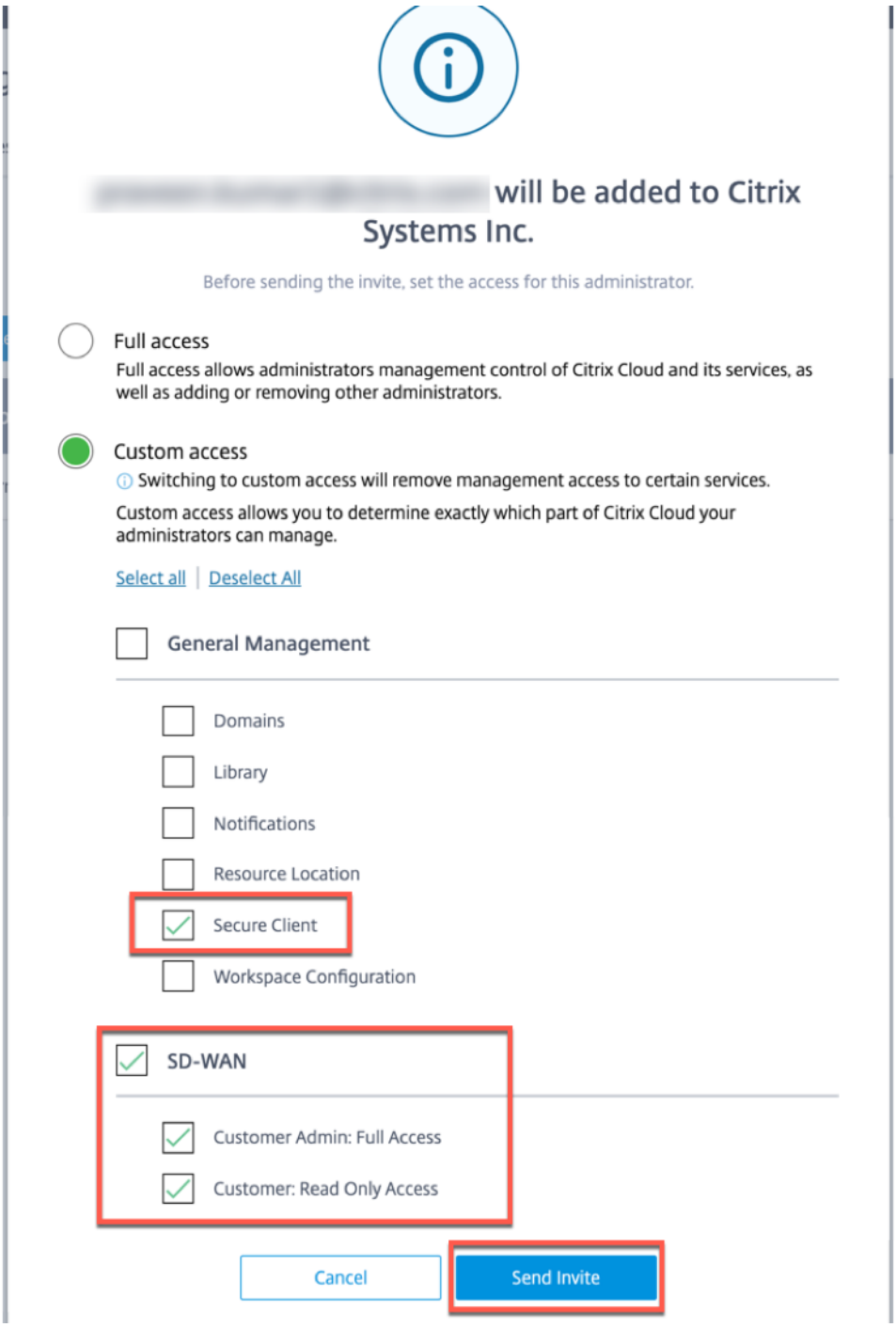
2. Gehen Sie zur Seite **Administratoren** und wählen Sie in der Dropdownliste Identitätsanbieter die Option **Citrix** Identität aus.



3. Geben Sie die neue Administrator-E-Mail-ID ein und klicken Sie auf **Einladen**



4. Sie können entweder **Vollzugriff** oder **Benutzerdefinierter Zugriff** wählen. Es wird empfohlen, den benutzerdefinierten Zugriff für den Administrator festzulegen, der nur SD-WAN-Dienste verwaltet. Wenn das Optionsfeld **Benutzerdefinierter Zugriff** ausgewählt ist, müssen Sie auch das Kontrollkästchen **Secure Client** im Abschnitt **Allgemeine Verwaltung** und das Kontrollkästchen **SD-WAN** aktivieren.



5. Klicken Sie auf **Einladung senden**.

Nachdem Sie das Administratorkonto erstellt haben, melden Sie sich über das Administratorkonto an, um die **API-Schlüssel** zu generieren.

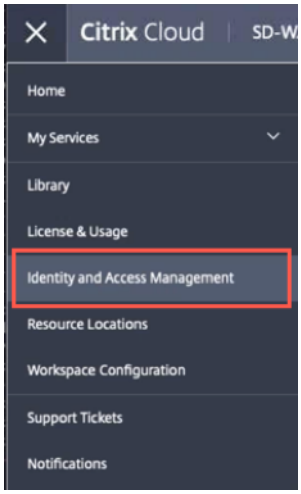
> **Hinweis:**
>
> Wenn Sie bereits eine benutzerdefinierte Administratorrolle haben, können Sie diese verwenden,

> um das API-Token zu erstellen.

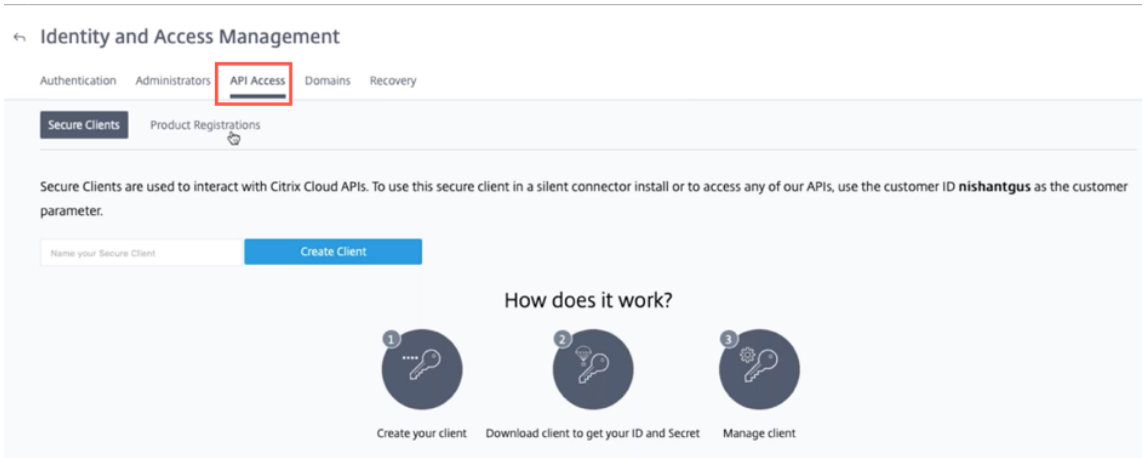
API Token generieren

Führen Sie die folgenden Schritte aus, um sich bei Citrix SD-WAN Orchestrator for On-premises anzumelden.

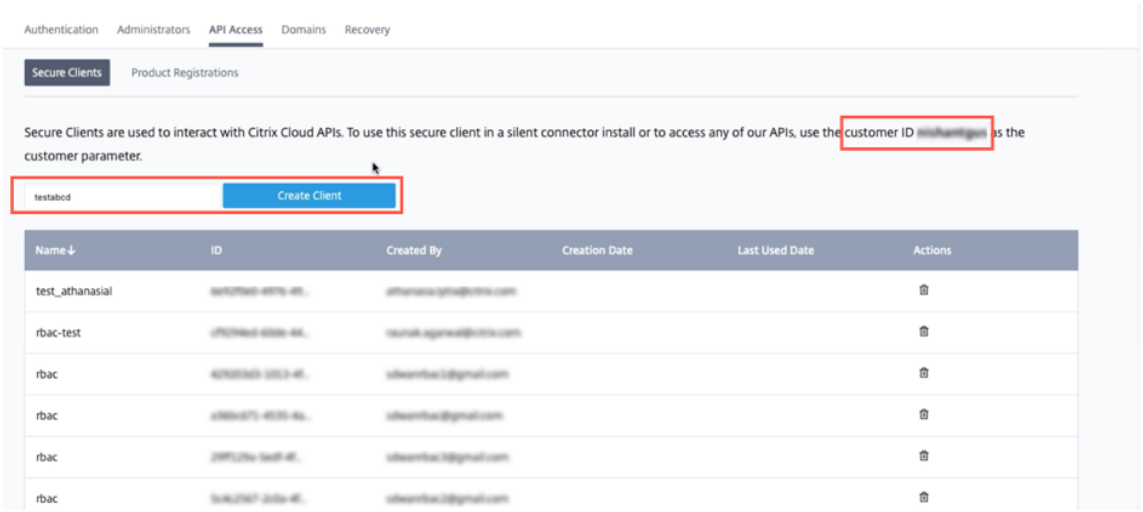
1. Melden Sie sich bei der Citrix Cloud an und navigieren Sie zu **Identity and Access Management**.



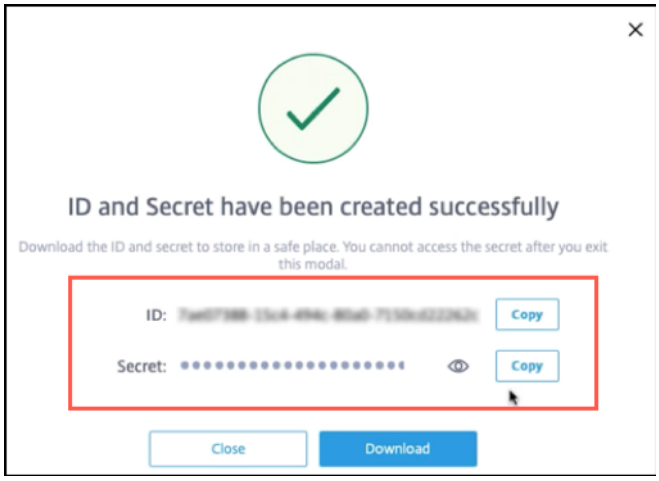
2. Gehen Sie zur **API-Zugriffsseite** .



3. Erstellen Sie einen Kunden. Notieren Sie sich die **Kunden-ID**, die Sie später benötigen, um sich bei Citrix SD-WAN Orchestrator for On-premises anzumelden.



4. Wenn Sie auf **Create Client**klicken, erhalten Sie die **ID** und einen **geheimen Schlüssel**, den Sie kopieren und speichern oder herunterladen können.



5. Gehen Sie zu Ihrem Citrix Hypervisor (XenServer/VMware) und starten Sie Citrix SD-WAN Orchestrator for On-premises.
6. Nachdem der Citrix SD-WAN Orchestrator for On-premises gestartet wurde, geben Sie den Standardbenutzernamen (admin) und das Kennwort (Kennwort) an.

   > **Hinweis:**
   >
   > Es ist zwingend erforderlich, das Standardkennwort für das Admin-Benutzerkonto bei der ersten Anmeldung zu ändern. Diese Änderung wird sowohl mit CLI als auch mit der Benutzeroberfläche erzwungen.

7. Wenn der DHCP-Server nicht im SD-WAN-Netzwerk konfiguriert ist, müssen Sie manuell eine statische IP-Adresse eingeben. So konfigurieren Sie eine statische IP-Adresse als Verwaltungs-IP-Adresse:

- Geben Sie in der Konsole den CLI-Befehl ein `management_ip`.
- Geben Sie den Befehl ein `set interface <ipaddress> <subnetmask> <gateway>`.

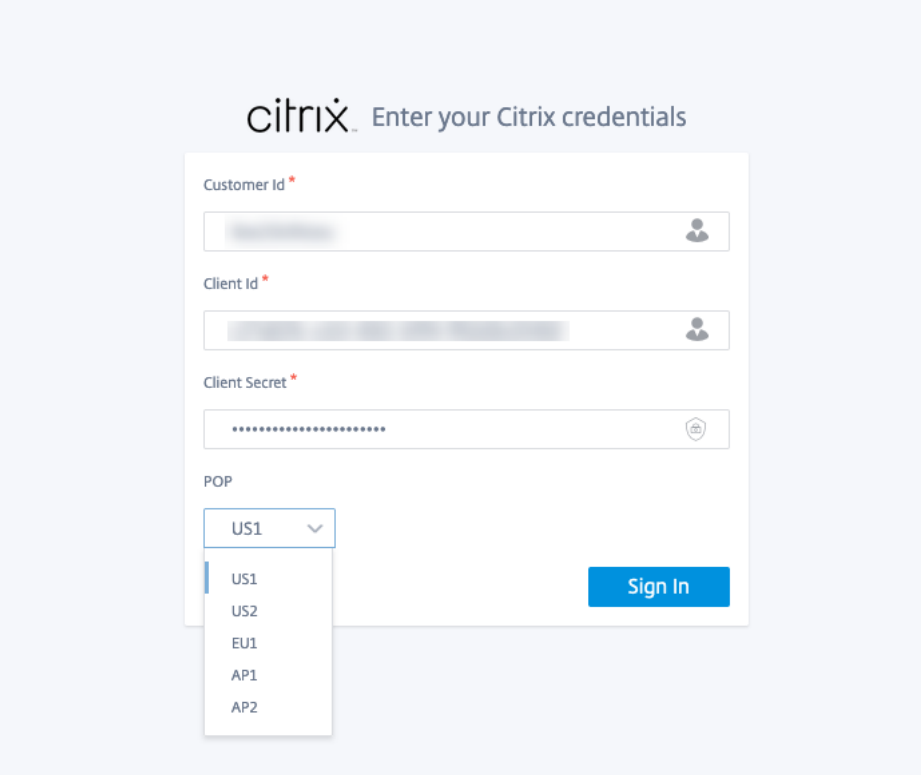
> **Hinweis**
>
> - Die Verwaltungs-IP-Adresse ist die IP-Adresse des Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen. Verwenden Sie diese IP-Adresse, um sich bei der Citrix SD-WAN Orchestrator for On-premises Web-Benutzeroberfläche anzumelden.
> - Die Verwaltungsschnittstelle kann über die beiden Methoden CLI und DHCP konfiguriert werden.

8. Sobald der Citrix SD-WAN Orchestrator for On-premises gestartet wurde, ist er standardmäßig mit den DNS-Servern 9.9.9.9 und 149.112.112.112 als primär bzw. sekundär konfiguriert. Bei Bedarf können Sie die IP-Adresse des DNS-Servers mit den folgenden Befehlen ändern:

   - Geben Sie in der Konsole den CLI-Befehl ein `set_dns`.
   - Geben Sie den Befehl `set primary <ipaddress>` und dann die Eingabetaste ein `y`, um die Änderung zu bestätigen.
   - Geben Sie den Befehl ein `y`, `set secondary <ipaddress>` und bestätigen Sie die Änderung.

```
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
```

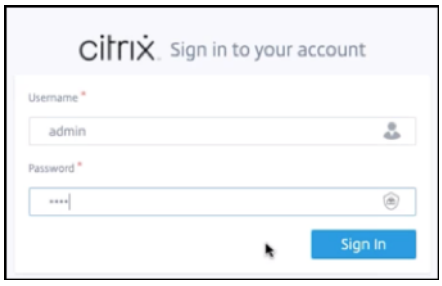
9. Öffnen Sie einen neuen Browser mit der Management-IP. Der folgende Bildschirm wird angezeigt:



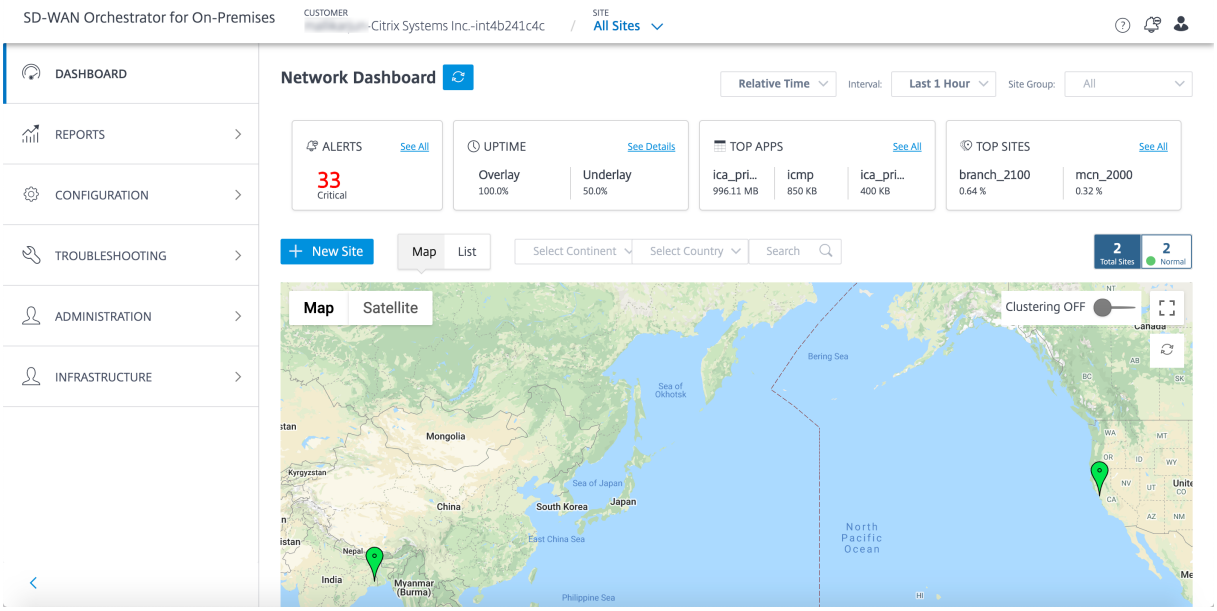
10. Geben Sie die **Kunden-ID, die Client-ID** und das **Client-Geheimnis** an, die Sie zuvor beim Erstellen des Clients über den Cloud-Orchestrator gespeichert oder heruntergeladen haben. Wählen Sie den POP aus, in dem Ihr Cloud-Konto an Bord war. Sie können den POP nach einer erfolgreichen Anmeldung nicht mehr ändern.

> **Hinweis**
>
> Dieser Bildschirm wird einmal in 15 Tagen angezeigt. Für das anschließende An- und Abmelden sehen Sie nur die lokale Anmeldeseite.

11. Geben Sie den Standardbenutzernamen und das Standardkennwort auf der lokalen Anmeldeseite an.



Sie können sehen, dass die Seite Citrix SD-WAN Orchestrator for On-premises Dashboard angezeigt wird.



Citrix SD-WAN Orchestrator für lokale Lizenzierung

October 21, 2022

Die Citrix SD-WAN Orchestrator for On-Premises-Lizenzierung gilt für Do It Yourself (DIY) -Kunden — Direct Enterprise-Kunden.

Stellen Sie als Voraussetzung für die Citrix SD-WAN Orchestrator for On-Premises-Lizenzierung sicher, dass Sie bei der Citrix Cloud angemeldet sind. Weitere Informationen finden Sie unter Citrix SD-WAN Orchestrator für die lokale Anmeldung.

Citrix SD-WAN Orchestrator für die lokale Bereitstellung ist kostenlos erhältlich, der Kunde muss jedoch die Kosten für die Infrastruktur und Wartung des Managementservers tragen.

Test-Modus

Das Citrix SD-WAN Orchestrator for On-Premises-Konto des Kunden wird im Testmodus bereitgestellt. Der Testmodus wird für einen Standardzeitraum von 60 Tagen fortgesetzt.

Nach Ablauf der Testphase werden die Datenpfade des Kunden heruntergefahren. Zusätzliche Änderungen können erst bereitgestellt werden, wenn gültige Lizenzen hochgeladen wurden. Die Citrix Cloud Cloud-Berechtigung des Kunden für Citrix SD-WAN Orchestrator for On-premises ändert sich von Testversion zu Produktion, wenn die erste gültige Lizenz darauf gehostet wird. Basierend auf der Anzahl und Art der hochgeladenen Lizenzen kann eine entsprechende Anzahl von Sites die richtigen Bandbreitenberechtigungen aufweisen. Eine permanente Meldung **Ihre Testversion ist abgelaufen.**

Führen Sie ein Upgrade auf Produktion durch, indem Sie mindestens eine gültige Lizenzberechtigung auf dem Orchestrator abrufen, um die Netzwerkfunktionalität wiederherzustellen und die Nutzung fortzusetzen. wird für Prepaid-Kunden angezeigt. Weitere Informationen finden Sie unter Abrufen und Zuweisen von Berechtigungen für das Prepaid-Abrechnungsmodell.

Prepaid Abrechnungsmodell

Für Citrix SD-WAN Orchestrator für lokale Kunden wird ein Prepaid-Abrechnungsmodell bereitgestellt. Die folgenden drei Arten von Prepaid-Abrechnungsmodellen sind verfügbar:

- **Vorausbezahltes Jahresabonnement**: Das Prepaid-Abonnement hat einen 1-Jahres- und einen 3-Jahres-Plan. Das Abonnement läuft am Verfallsdatum ab. Alle Geräte im Kundennetzwerk haben ein vorausbezahltes Jahresabonnement. Wartungslizenzen sind im Abonnementpaket enthalten und bieten die Möglichkeit, Appliances auf neuere Softwareversionen zu aktualisieren.
- **Perpetual Prepaid**: Bei Prepaid Perpetual haben die Lizenzen keine zeitliche Begrenzung, eingeschränkte Dauer oder Ablauf. Die Hardware-Wartungslizenz ist jedoch als kostenpflichtiges Add-on erhältlich und muss separat erworben werden. Alle Geräte im Kundennetzwerk haben ein unbefristetes Prepaid-Abonnement.

Um das Abrechnungsmodell in Citrix SD-WAN Orchestrator for On-premises anzuzeigen, navigieren Sie auf Netzwerkebene zu **Administration** > **Lizenzierung** > **Abrechnungsmodell auswählen**. Das Abrechnungsmodell wird als **Vorauszahlung jährlich und unbefristet**angezeigt.

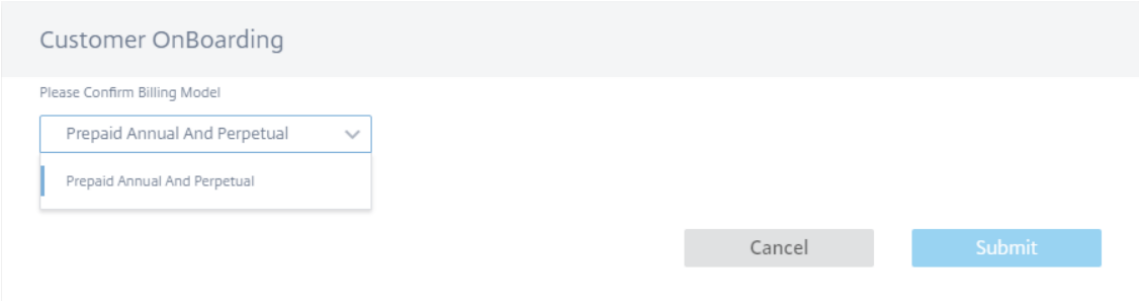
Laden Sie die Lizenzen auf alle Kundenstandorte hoch. Weitere Informationen finden Sie unter Abrufen und Zuweisen von Berechtigungen für das Prepaid-Abrechnungsmodell.

Abrufen und Zuweisen von Berechtigungen für Prepaid-Abrechnungsmodell

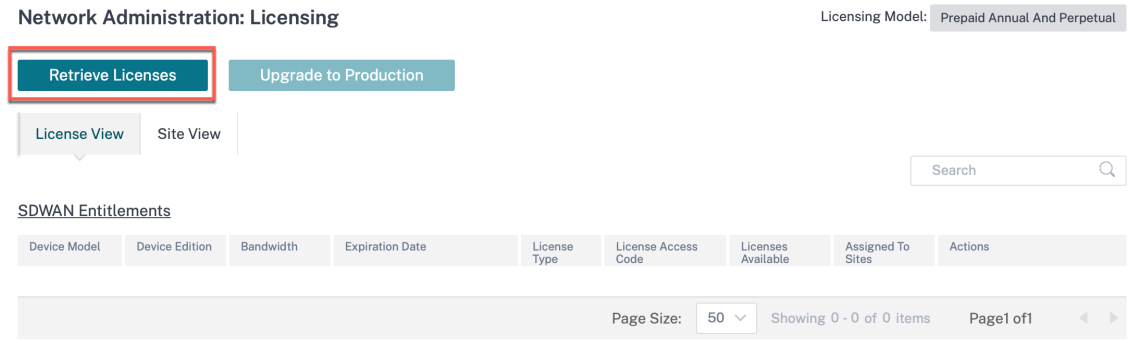
Sie können die Lizenzberechtigungen mit dem von Citrix per E-Mail bereitgestellten Zugangscode abrufen. Alternativ kann der Kunde den Zugangscode auch im Lizenzverwaltungsportal in Citrix Cloud anzeigen. Der Kunde kann entweder ein **unbefristetes Prepaid-Abrechnungsmodell**oder ein **Prepaid-Jahresabonnement** im Netzwerk haben.

Voraussetzung: Stellen Sie sicher, dass die Citrix SD-WAN Orchestrator for On-Premises-Lizenzen nicht zugewiesen sind, indem Sie sich beim Lizenzverwaltungsportalanmelden. Wenn die Lizenzen zugewiesen sind, geben Sie die Lizenzen frei/entfernen Sie die Zuweisung, bevor Sie die Lizenzzugriffscodes im Citrix SD-WAN Orchestrator for On-Premises-Produkt verwenden.

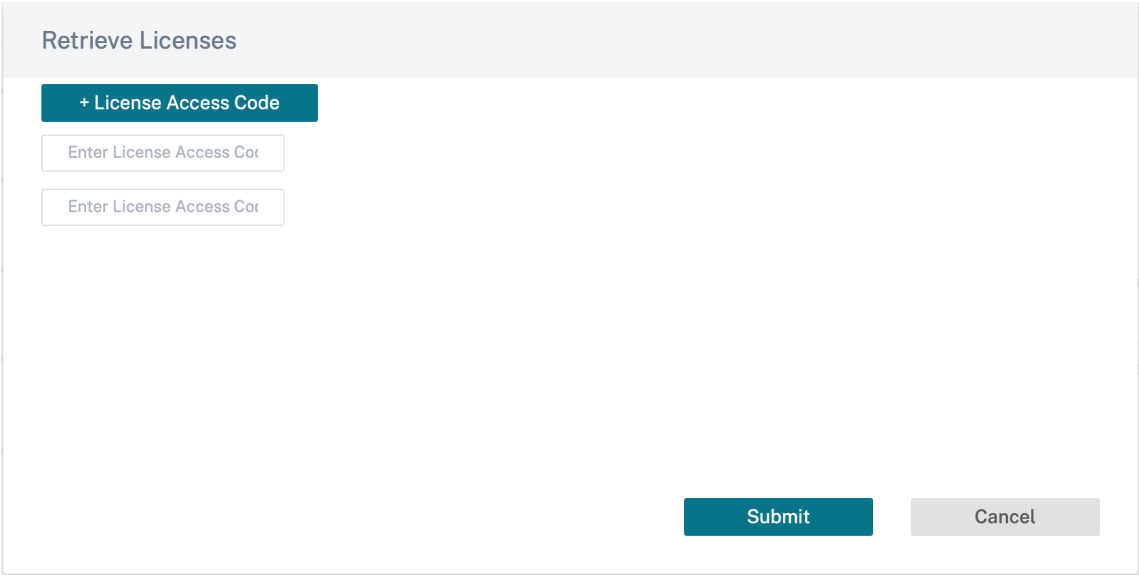
1. Navigieren Sie in der Benutzeroberfläche von Citrix SD-WAN Orchestrator for On-premises zu **Administration** > **Lizenzierung** und klicken Sie auf **Abrechnungsmodell auswählen**. Wählen Sie ein Abrechnungsmodell und klicken Sie auf **Senden**.



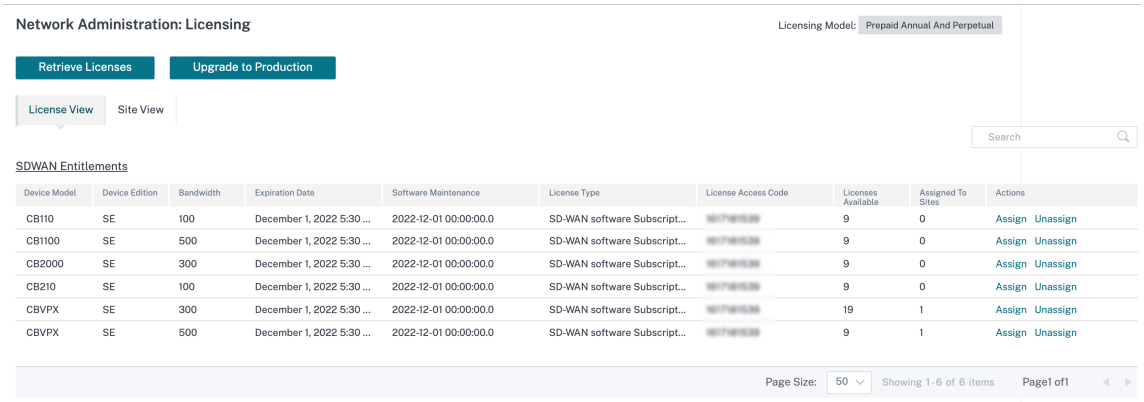
2. Klicken Sie auf **Lizenzen abrufen**.



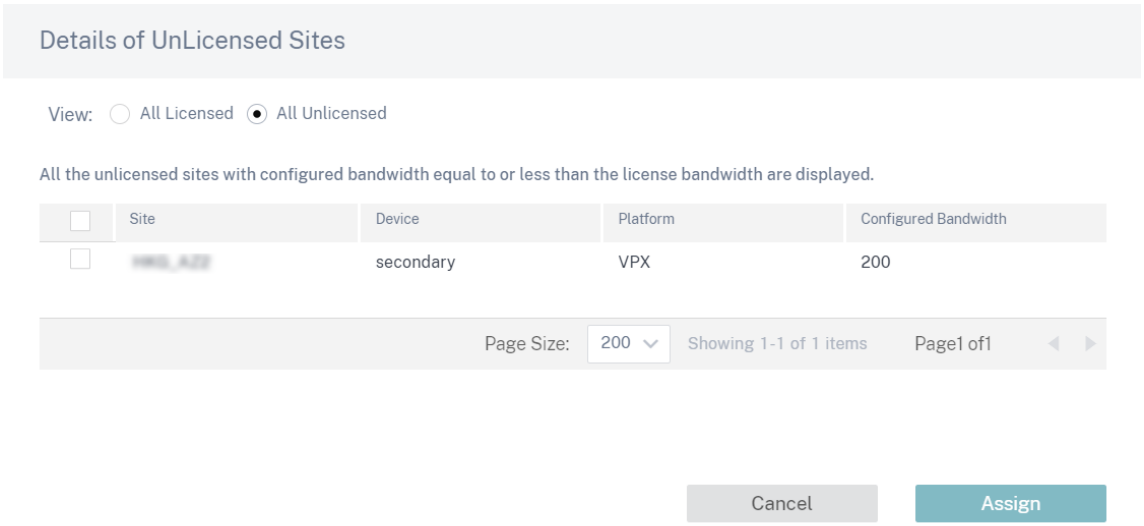
3. Klicken Sie auf **+ Lizenzzugangscode**, geben Sie die erforderliche Anzahl von Zugangscodes ein, um die Berechtigungen abzurufen, und klicken Sie auf **Senden**



Der Citrix SD-WAN Orchestrator for On-premises ruft die Berechtigungen ab und füllt die Lizenztabelle auf.

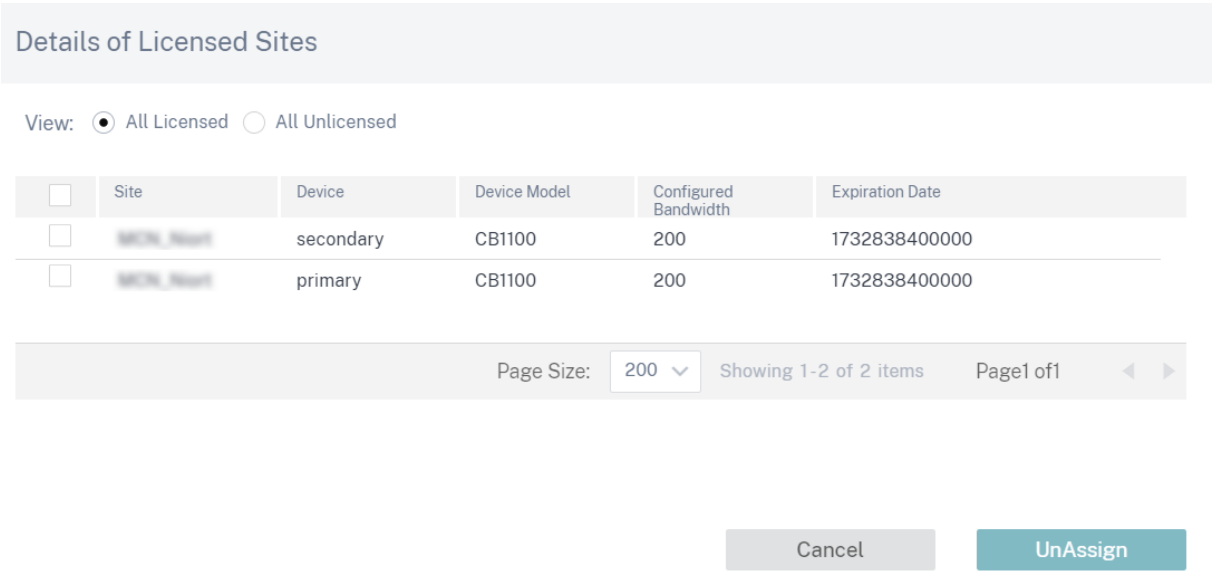


4. Klicken Sie auf **Zuweisen/Aufheben** und wählen Sie **Alle nicht lizenzierten**. Alle nicht lizenzierten Sites mit konfigurierter Bandbreite, die der Lizenzbandbreite entspricht oder der Lizenzbandbreite entspricht, wird angezeigt.



5. Wählen Sie die Standorte aus, klicken Sie auf **Zuweisen** und dann auf **Upgrade auf Produktion**.

In der Ansicht **Alle lizenzierten** Websites wird eine Liste der lizenzierten Websites angezeigt. Sie können die Zuweisung der Lizenzen aufheben und sie wieder an den Pool freigeben.



In der **Site-Ansicht**werden die Sites basierend auf der konfigurierten Bandbreite und Lizenzbandbreite automatisch mit Lizenzen abgeglichen, sodass Sie Lizenzen schnell zuweisen können.

> **Hinweis**
>
> Um der Appliance eine Lizenz zuzuweisen, muss eine Appliance über eine verifizierte Seriennummer verfügen.

Ablauf der Lizenz

Wenn die Lizenz abläuft, wird eine Nachfrist von 30 Tagen gewährt. Der Partner/Kunde wird voraussichtlich während dieser Zeit seine Lizenzen erneuern. Nach Ablauf der Kulanzfrist werden die Netzwerkdatenpfade des Kunden heruntergefahren, und zusätzliche Änderungen können erst bereitgestellt werden, wenn die Lizenzen erneuert wurden.

Konnektivität mit Citrix SD-WAN-Appliances

October 21, 2022

Stellen Sie nach dem Konfigurieren von Sites auf Citrix SD-WAN Orchestrator for On-premises die Konnektivität zwischen Citrix SD-WAN-Appliances an den Standorten mit Citrix SD-WAN Orchestrator for On-premises her. Sie können die Konnektivität auf eine der folgenden Arten herstellen:

- **Einseitige Authentifizierung**: Die SD-WAN-Appliance authentifiziert Citrix SD-WAN Orchestrator für lokal. Wenn Sie die unidirektionale Authentifizierung aktivieren, müssen Sie das Zertifikat Citrix SD-WAN Orchestrator for On-premises herunterladen und auf die SD-WAN-Appliance hochladen.
- **Zwei-Wege-Authentifizierung**: Das SD-WAN authentifiziert sich gegenseitig mithilfe der ausgetauschten Zertifikate. Wenn Sie die bidirektionale Authentifizierung aktivieren, müssen Sie das Zertifikat der SD-WAN-Appliance auf Citrix SD-WAN Orchestrator for On-premises und das Citrix SD-WAN Orchestrator for On-Premises-Zertifikat auf die SD-WAN-Appliance hochladen.
- **Keine Authentifizierung**: Die Konnektivität zwischen dem Citrix SD-WAN Orchestrator für lokale Geräte und SD-WAN-Appliances ohne Authentifizierung wird hergestellt. Sie müssen die SD-WAN-Appliance oder den Citrix SD-WAN Orchestrator für das lokale Zertifikat nicht verwenden. Sie können No Authentication verwenden, wenn Sie über ein sicheres Netzwerk wie MPLS verfügen.

> **Hinweis:**
>
> Es wird empfohlen, nur die **unidirektionale Authentifizierung** oder die bidirektionale Authentifizierung Falls keine Authentifizierung erfolgt, müssen Sie den sicheren DNS-Server auswählen.

Sie können die Konnektivität mit jedem Standort manuell konfigurieren oder die automatisierte Zero-Touch-Bereitstellung verwenden.

> **Hinweis**
>
> Citrix SD-WAN 11.3.0 ist die Mindestsoftwareversion, die für eine Appliance erforderlich ist, um eine Verbindung mit Citrix SD-WAN Orchestrator for On-premises herzustellen.

Zero-Touch-Bereitstellung

Die Zero-Touch-Bereitstellung ist ein automatisierter Prozess zum Konfigurieren der Konnektivität zwischen den Appliances und dem Citrix SD-WAN Orchestrator for On-premises. Sie können die Konnektivität automatisch mithilfe der Zero-Touch-Bereitstellung ohne Cloud oder über die Cloud vermittelten Zero-Touch-Bereitstellungseinstellungen herstellen.

Zero-Touch-Bereitstellung ohne Cloud

Mit den Zero-Touch-Bereitstellungseinstellungen ohne Cloud können Sie Citrix SD-WAN Orchestrator für lokale Informationen auf SD-WAN-Appliances konfigurieren. Die im Backend ausgeführte NITRO-

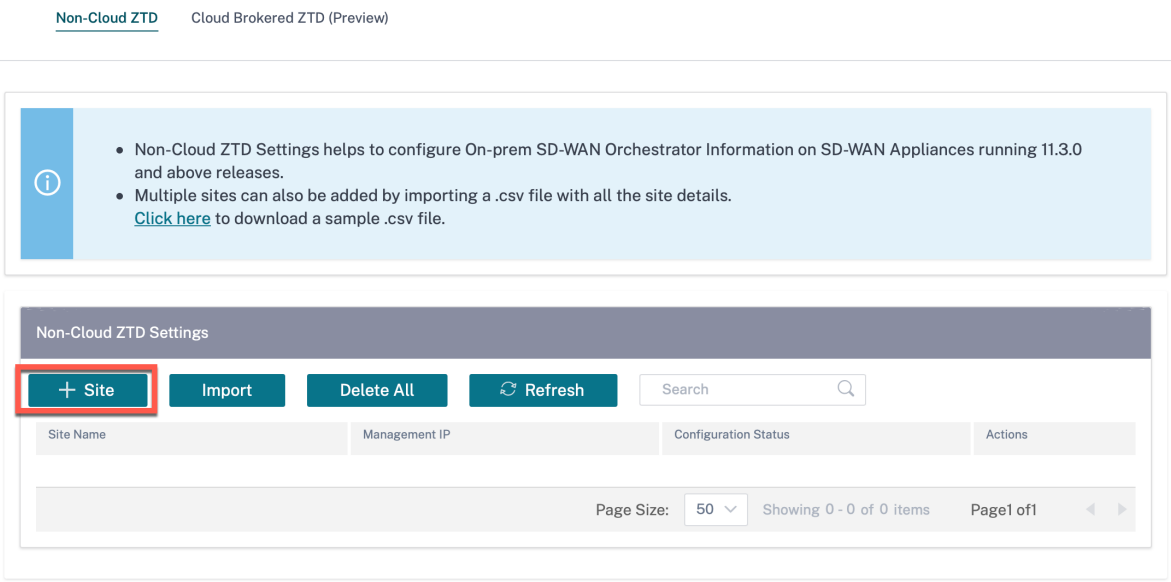
API verarbeitet das Herunterladen und Hochladen von Zertifikaten. Es lädt das Zertifikat von Citrix SD-WAN Orchestrator for On-premises herunter, meldet sich bei der SD-WAN-Appliance an und lädt das Zertifikat hoch. Es lädt auch das SD-WAN-Appliance-Zertifikat herunter und lädt es auf Citrix SD-WAN Orchestrator for On-premises hoch.

> **Hinweis:**
>
> Die Nicht-Cloud-Zero-Touch-Bereitstellung wird auf SD-WAN-Appliances unterstützt, die mit der Version 11.3.0 oder höher ausgeführt werden.

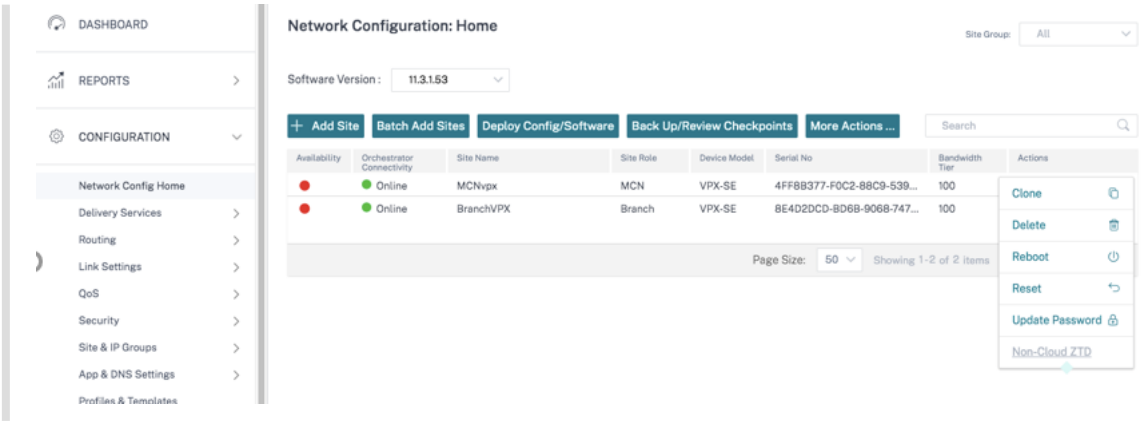
Zero-Touch-Bereitstellung unterstützt nur die **einseitige Authentifizierung** und die **bidirektionale Authentifizierung Keine Authentifizierung** wird nicht unterstützt. Wenn der **Authentifizierungstyp** auf der Seite **Administration > Zertifikatsauthentifizierung** aktiviert ist, wird die bidirektionale Authentifizierung eingerichtet. Wenn **Authentifizierungstyp** deaktiviert ist, wird die unidirektionale Authentifizierung eingerichtet.

Sie können Websites entweder manuell hinzufügen oder eine CSV-Datei importieren, um mehrere Websites gleichzeitig hinzuzufügen.

Um Zero-Touch-Bereitstellungseinstellungen ohne Cloud zu konfigurieren, navigieren Sie zu **Administration** > **ZTD-Einstellungen** > **Non-Cloud-ZTD**und klicken Sie auf **+ Site**.



> **Hinweis**
>
> Sie können auch über die **Startseite der Netzwerkkonfiguration** auf Zero-Touch-Bereitstellungseinstellungen außerhalb der Cloud für jede Site zugreifen. Klicken Sie auf das Aktionssymbol für die Site und wählen Sie **Non-Cloud ZTD**aus.



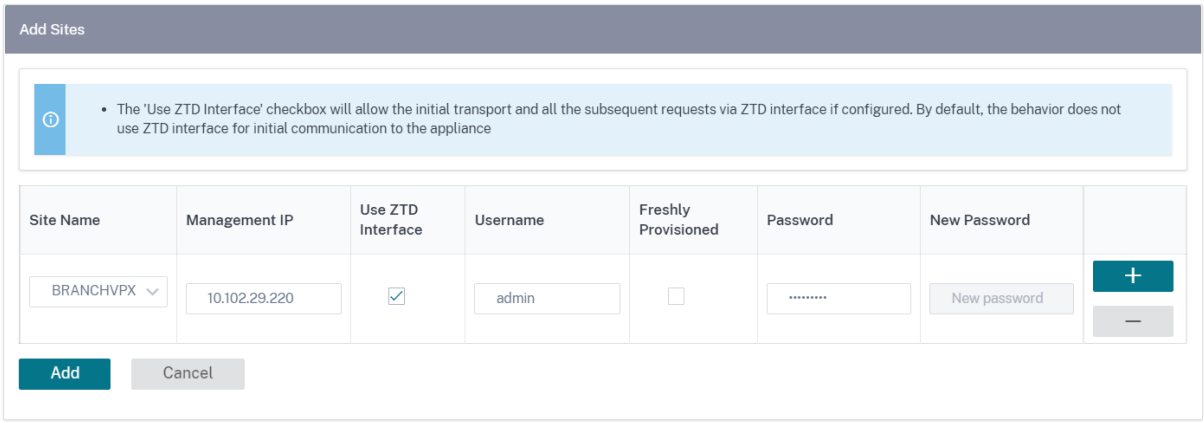
Wählen Sie in der Dropdownliste **Sitename eine Site** aus und geben Sie die **Verwaltungs-IP-Adresse** der Citrix SD-WAN-Appliance ein.

Durch Aktivieren der Option **ZTD-Schnittstelle verwenden** wird sichergestellt, dass die ZTD-Schnittstelle für Nicht-Cloud-ZTD verwendet wird, wenn die ZTD-Schnittstelle auf SD-WAN Orchestrator for On-Premises aktiviert ist.

> **Hinweis**
>
> - Ignorieren **Sie die Option ZTD-Schnittstelle verwenden**, wenn die ZTD-Schnittstelle auf SD-WAN Orchestrator for On-premises nicht aktiviert ist.
> - Aktivieren **Sie die Option ZTD-Schnittstelle verwenden**, wenn die SD-WAN-Appliance auf die IP-Adresse der ZTD-Schnittstelle zugreifen kann, aber nicht auf die Management-IP-Adresse zugreifen kann.
> - Wenn Sie die Option **ZTD-Schnittstelle verwenden** nach dem Aktivieren der ZTD-Schnittstelle nicht auswählen, bedeutet dies nicht, dass die IP-Adresse der Verwaltungsschnittstelle für die Kommunikation zwischen der SD-WAN-Appliance und dem SD-WAN Orchestrator für lokale Geräte verwendet wird. Die Option **ZTD-Schnittstelle verwenden** wird nur für die Erstkonfiguration der Appliance mit ZTD ohne Cloud verwendet.

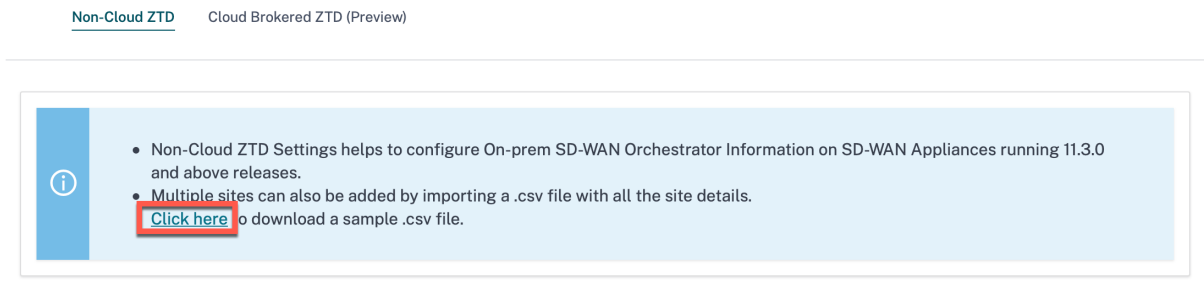
Geben Sie den Benutzernamen und das Kennwort der Appliance an. Aktivieren Sie **das Kontrollkästchen Freshly Provisioned**, wenn Sie eine neu bereitgestellte Site hinzufügen, auf der das Standardkennwort nicht geändert wurde. Geben Sie das **neue Passwort ein**. Das Standardkennwort wird während dieses Zero-Touch-Bereitstellungsprozesses in das neue Passwort geändert.

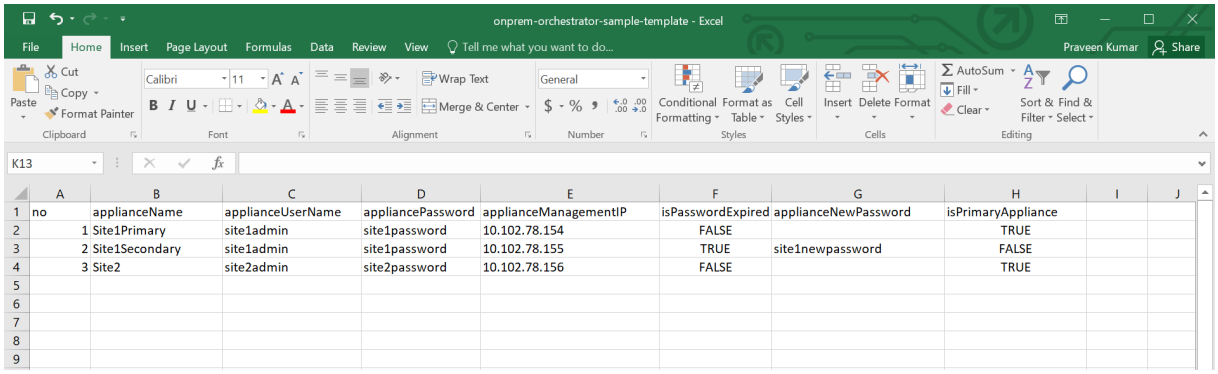
> **Hinweis**
>
> Für eine neu bereitgestellte Site ist es zwingend erforderlich, das Standardkennwort bei der ersten Anmeldung zu ändern.



Klicken Sie auf **+**, um weitere Websites hinzuzufügen.

Sie können auch eine CSV-Datei importieren, um mehrere Websites gleichzeitig hinzuzufügen. Eine herunterladbare Beispielvorlage ist in der Benutzeroberfläche verfügbar. Laden Sie es herunter und geben Sie die Site-Details an



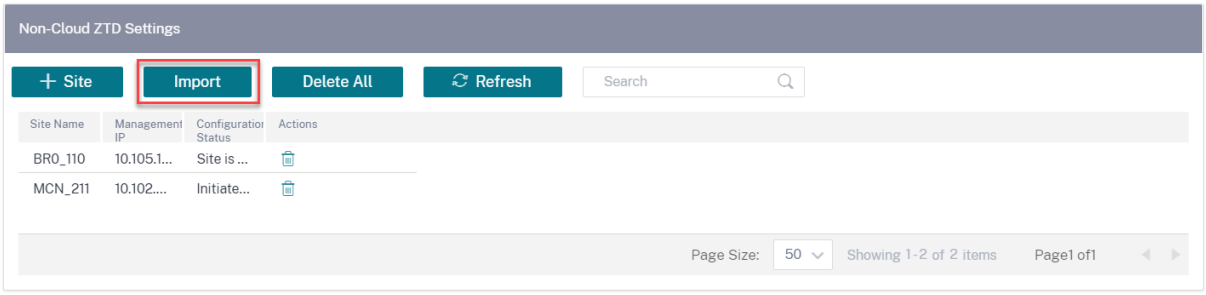


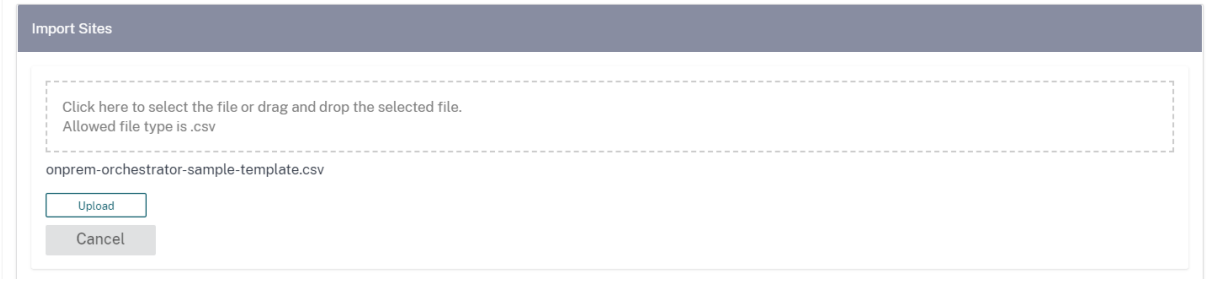
- **Appliance-Name**: Der bei der Sitekonfiguration konfigurierte Site-Name. Weitere Informationen finden Sie unter Site-Konfiguration.
- **Appliance-Benutzername**: Der auf der Site-Appliance konfigurierte Benutzername.
- **Appliance-Passwort**: Das entsprechende Passwort für die Site-Appliance.
- **Ist das Kennwort abgelaufen**: Legt fest, ob die Appliance neu bereitgestellt wurde. Wenn der Wert **True**ist, geben Sie das **neue Kennwort für die Appliance**an.
- **Neues Passwort der Appliance**: Das Passwort für neu bereitgestellte Appliances. Wenn der Wert **Is password expired** auf **True**festgelegt ist, geben Sie für die **Appliance ein neues Ken-**

nwort ein

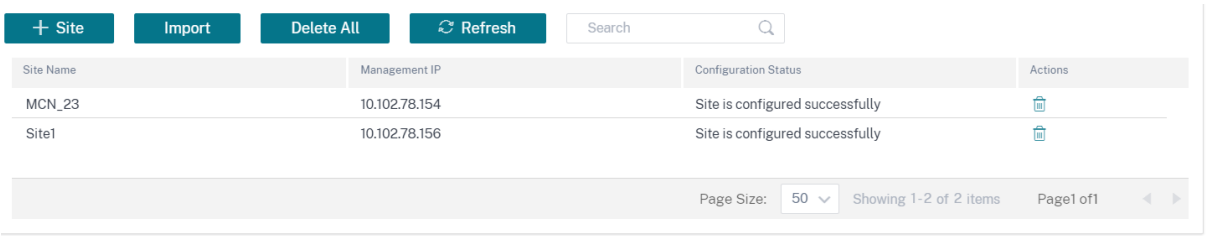
- **Ist primäres Gerät**: Wenn High Availability (HA) konfiguriert ist, muss die aktive Appliance den Wert True und die Standby-Appliance den Wert False haben. Wenn HA nicht konfiguriert ist, muss der Wert True sein.

Klicken Sie auf **Importieren**, wählen Sie die CSV-Datei aus und klicken **Sie**auf





Der Konfigurationsstatus der Standorte wird angezeigt. Sie können Standorte einzeln löschen oder Alle löschen, wenn Standorte für die Zero-Touch-Bereitstellung nicht erforderlich sind.



Über die Cloud vermittelte Zero-Touch-Bereitstellung

Die in der Cloud vermittelte Zero-Touch-Bereitstellung verwendet den Citrix SD-WAN Orchestrator Service als Broker zwischen Citrix SD-WAN Orchestrator for On-premises und den Citrix SD-WAN-Appliances. Citrix SD-WAN Orchestrator for On-premises sendet ein Cloud-Zero-Touch-Bereitstellungskonfigurationspaket an den Citrix SD-WAN Orchestrator Service. Das Cloud-Zero-Touch-Bereitstellungskonfigurationspaket besteht aus den folgenden Informationen:

- Identitätsinformationen vor Ort
- Authentifizierungstyp

- Zertifikat vor Ort
- Gerätedetails (Liste der Seriennummern)

Der Citrix SD-WAN Orchestrator Service speichert die Informationen, die von Citrix SD-WAN Orchestrator for On-premises empfangen wurden. Wenn eine Appliance den Citrix SD-WAN Orchestrator Service mit seiner Seriennummer kontaktiert, bestimmt die erworbene Intelligenz des Citrix SD-WAN Orchestrator Service, dass die Appliance von Citrix SD-WAN Orchestrator for On-premises verwaltet werden muss. Der Citrix SD-WAN Orchestrator Service übergibt den Citrix SD-WAN Orchestrator für lokale Details an die Appliance. Die Citrix SD-WAN-Appliance sendet ihr Zertifikat an den Orchestrator-Dienst. Der Citrix SD-WAN Orchestrator Service empfängt und speichert das Appliance-Zertifikat.

Citrix SD-WAN Orchestrator for On-premises ruft das Appliance-Zertifikat regelmäßig vom Citrix SD-WAN Orchestrator Service ab. Sobald eine sichere Verbindung zwischen Citrix SD-WAN Orchestrator for On-premises und der Appliance hergestellt wurde, überträgt der Citrix SD-WAN Orchestrator for On-premises die Konfiguration und die relevanten Dateien an die Appliances.

Über die Cloud vermittelte Zero-Touch-Bereitstellungseinstellungen sind nur für Kunden in einem vom Kunden verwalteten Setup verfügbar. Das vom Anbieter verwaltete Setup unterstützt keine über die Cloud vermittelten Zero-Touch-Bereitstellungseinstellungen.

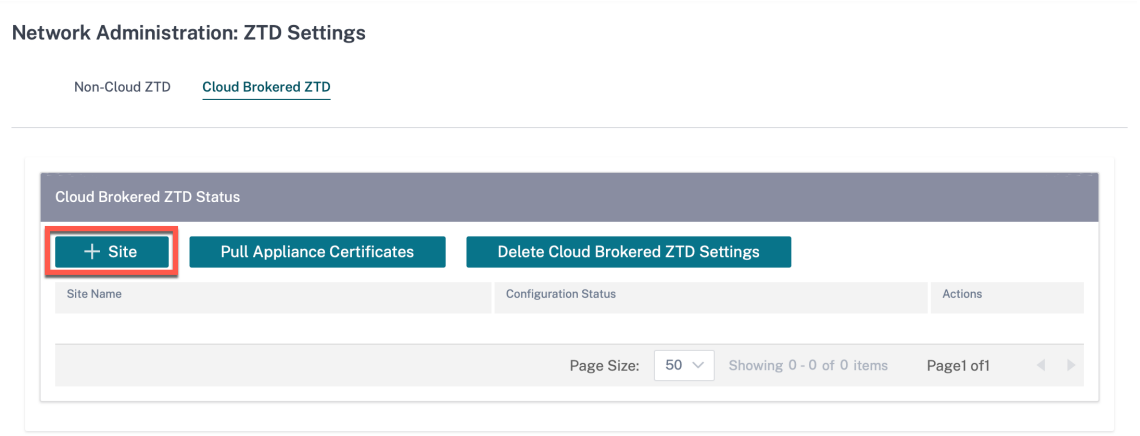
Voraussetzungen

- Appliances benötigen Zugriff auf die folgenden Domänennamen, um eine Verbindung mit dem Citrix SD-WAN Orchestrator Service herzustellen:
  - sdwanzt.citrixnetworkapi.net
  - herunterladen.citrixnetworkapi.net
  - trust.citrixnetworkapi.net
  - sdwan-home.citrixnetworkapi.net
- Stellen Sie sicher, dass Citrix SD-WAN Orchestrator for On-premises immer über Konnektivität zum Citrix SD-WAN Orchestrator Service verfügt, um SD-WAN-Appliances zu integrieren.
- Stellen Sie sicher, dass die Citrix SD-WAN-Appliance während des ersten Onboarding-Prozesses und wenn die SD-WAN-Appliance auf die Werkseinstellungen zurückgesetzt wird, über eine Verbindung zum SD-WAN Orchestrator Service verfügt.

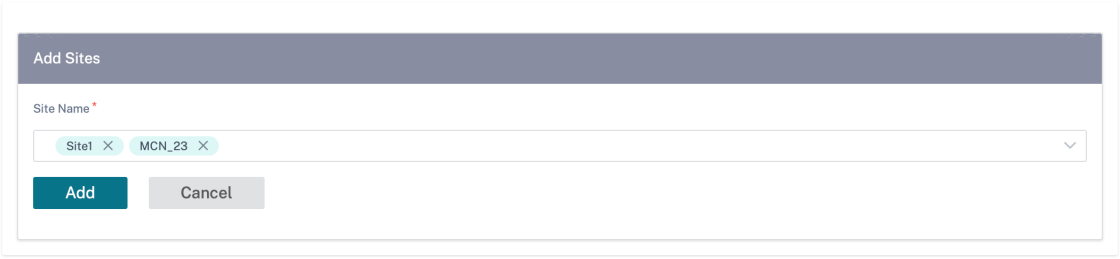
So konfigurieren Sie über Cloud vermittelte Zero-Touch-Bereitstellungseinstellungen:

1. Erstellen und definieren Sie in Citrix SD-WAN Orchestrator for On-premises Sites mithilfe des geführten Workflows. Weitere Informationen finden Sie unter Sitekonfiguration.
2. Überprüfen und kompilieren Sie die Konfiguration mit dem Deployment Tracker. Weitere Informationen finden Sie im Abschnitt Deployment Tracker im Thema Netzwerkkonfiguration .

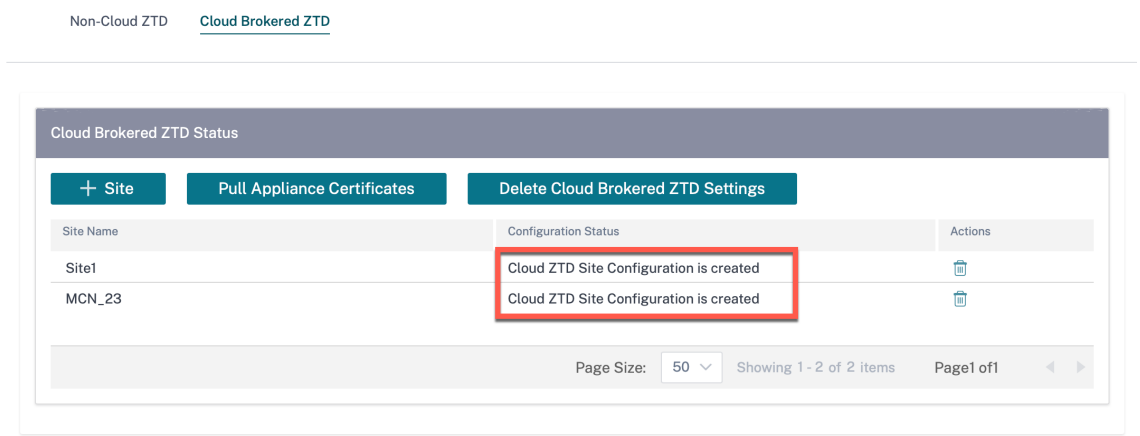
3. Navigieren Sie zu **Administration > ZTD-Einstellungen > Cloud Brokered ZTD** und klicken Sie auf **+ Site**.



4. Wählen Sie in der Dropdownliste einen Site-Namen aus und klicken Sie auf **Hinzufügen** Die Sites werden basierend auf Ihrer Konfiguration aufgelistet. Sie können eine einzelne Site oder mehrere Standorte auswählen.



5. Die Cloud-Zero-Touch-Bereitstellungskonfiguration wird erstellt und an den Citrix SD-WAN Orchestrator Service gesendet.

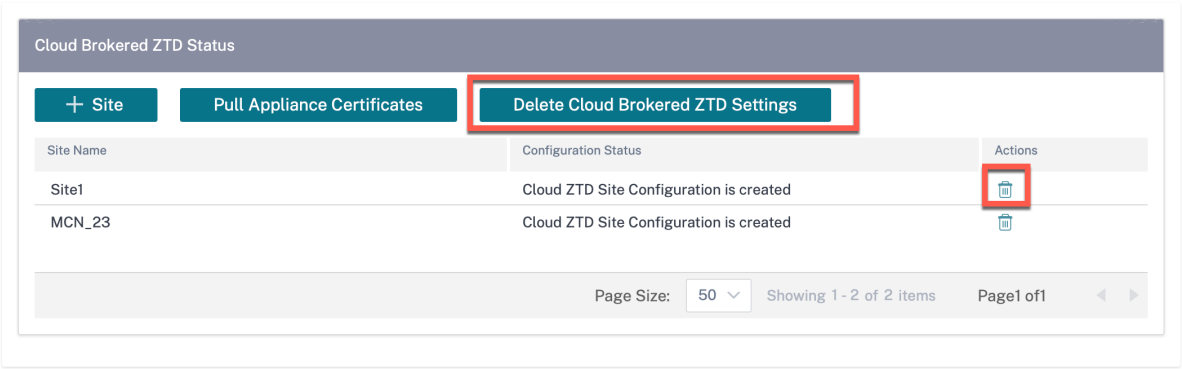


6. Verkabeln und Einschalten der SD-WAN-Appliances im Rechenzentrum und in Zweigstellen.
7. Die Appliances kontaktieren den Citrix SD-WAN Orchestrator Service mit ihrer Seriennummer.

8. Der Citrix SD-WAN Orchestrator Service fungiert als Broker zwischen Citrix SD-WAN Orchestrator for On-premises und den Appliances. Es ermöglicht den Austausch von Zertifikaten und die Citrix SD-WAN-Appliance stellt eine sichere Verbindung mit Citrix SD-WAN Orchestrator for On-premises her. Sobald die Zero-Touch-Bereitstellung erfolgreich war, geht die konfigurierte Site online und wird in der Spalte **Orchestrator-Konnektivität** unter **Konfiguration > Netzwerkkonfiguration Home**angezeigt.
9. **Aktivieren** und **inszenieren** Sie die Konfiguration, um die Konfiguration und Software per Push an die Appliances zu
10. Sobald die Konfiguration/Software angewendet wurde, werden virtuelle Pfade eingerichtet und die Spalte **Verfügbarkeit** unter **Konfiguration > Netzwerkkonfiguration Home** wird mit dem entsprechenden virtuellen Pfadstatus aktualisiert.

> **HINWEIS:**
>
> Citrix SD-WAN Orchestrator for On-premises benötigt etwa 30 Minuten, um das Appliance-Zertifikat abzurufen und die Appliances vollständig zu integrieren. Um die Appliance-Zertifikate sofort abzurufen (ohne 30 Minuten zu warten), klicken Sie auf **Appliance-Zertifikate abrufen**.

Bei Bedarf können Sie auf **Cloud Brokered ZTD-Einstellungen löschen**klicken. Es entfernt Informationen, die sich auf alle Websites beziehen. Wenn Sie eine bestimmte Site-Information löschen müssen, klicken Sie auf das Löschen-Symbol, das dieser Site entspricht.



Einschränkungen

- SD-WAN-Appliances können keine Verbindung zu mehreren Instanzen von Citrix SD-WAN Orchestrator for On-premises herstellen, die Cloud-Anmeldeinformationen gemeinsam nutzen. Beispielsweise bleibt eine SD-WAN-Appliance mit dem Citrix SD-WAN Orchestrator for On-premises verbunden, der zum ersten Mal konfiguriert wurde. Die als nächstes konfigurierten Citrix SD-WAN Orchestrator for On-Premises-Details werden nicht an die SD-WAN-Appliance übertragen.

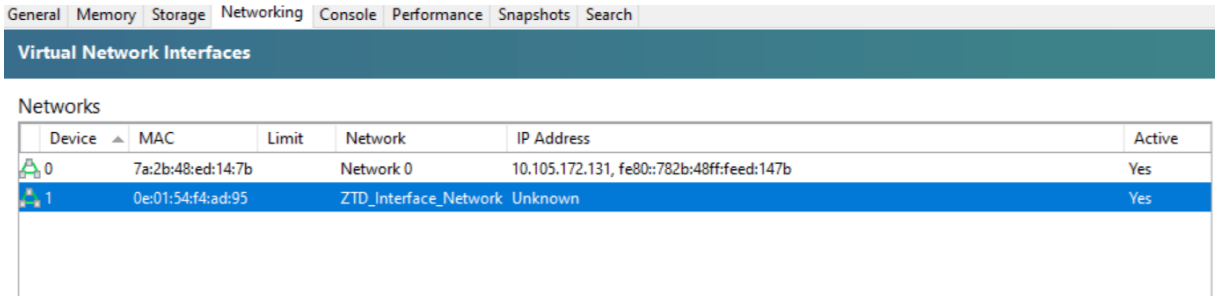
- SD-WAN-Appliances, die über LTE verbunden sind, können keine Verbindung mit Citrix SD-WAN Orchestrator für lokale Geräte herstellen, die in einem privaten Netzwerk gehostet werden.

ZTD-Schnittstelleneinstellungen

Sie können eine ZTD (Zero Touch Deployment) -Schnittstelle auf dem SD-WAN Orchestrator for On-Premises aktivieren. Die ZTD-Schnittstelle, die durch bidirektionale Authentifizierung gesichert ist, bietet eine sichere Kommunikationsschnittstelle für SD-WAN-Appliances und den SD-WAN Orchestrator für lokale Geräte.

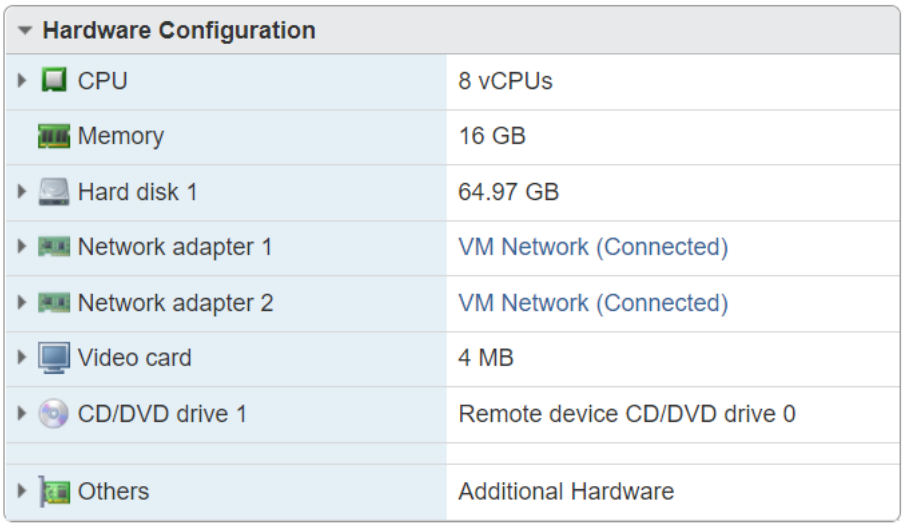
Nach dem Aktivieren der ZTD-Schnittstelle verwenden neue D-WAN-Appliances, die über Non-Cloud ZTD und Cloud-Brokered ZTD bereitgestellt werden, die IP-Adresse der ZTD-Schnittstelle, um mit dem SD-WAN Orchestrator for On-Premises zu kommunizieren.

Stellen Sie als Voraussetzung sicher, dass SD-WAN Orchestrator for On-premises Virtual Machine neben der Verwaltungsschnittstelle über eine zusätzliche Schnittstelle verfügt.



Hinweis

Stellen Sie für die virtuelle VMware ESXi ESXi-Maschine sicher, dass die virtuelle Maschine neu gestartet wird, nachdem Sie eine zusätzliche Schnittstelle für ZTD hinzugefügt haben.

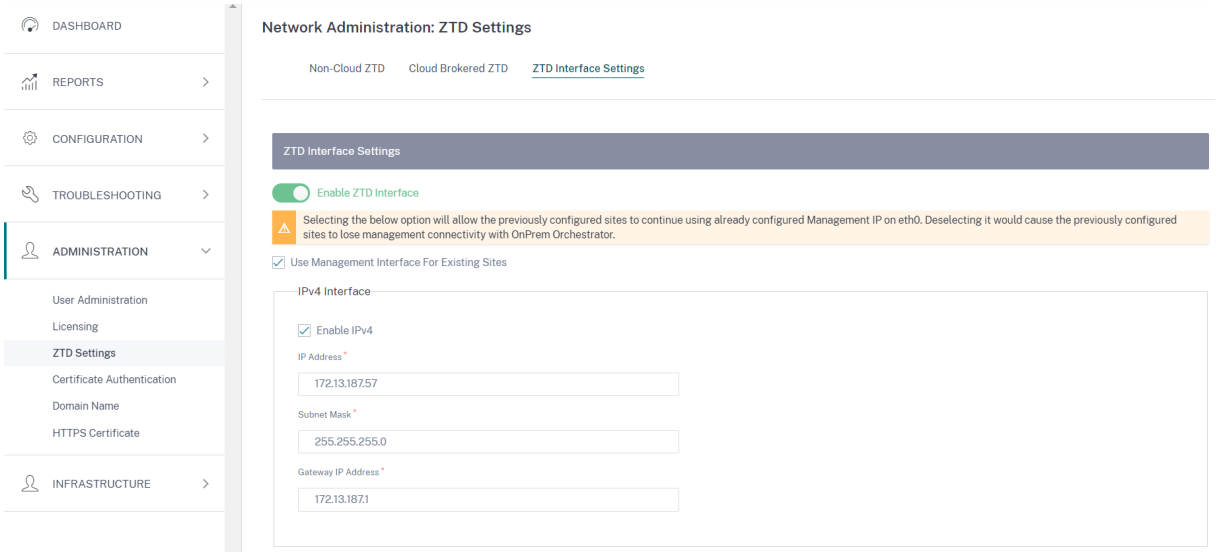


ZTD-Schnittstelle aktivieren

Navigieren Sie in SD-WAN Orchestrator for On-premises GUI zu **Administration** > **ZTD-Einstellungen** und wählen Sie **ZTD-Schnittstelle aktivieren**, um die ZTD-Schnittstelle zu aktivieren. Geben Sie die IP-Adresse der ZTD-Schnittstelle, die Subnetzmaske und die Gateway-IP-Adresse an.

Wählen Sie **Verwaltungsschnittstelle für vorhandene Sites verwenden**, um sicherzustellen, dass SD-WAN-Appliances, die bereits über die Non-Cloud ZTD oder Cloud Brokered-ZTD bereitgestellt wurden, weiterhin über die IP-Adresse der Verwaltungsschnittstelle eine Verbindung mit dem SD-WAN Orchestrator for On-Premises herstellen.

> **Warnung**
>
> Wenn die Option **Verwaltungsschnittstelle für vorhandene Sites verwenden** nicht ausgewählt ist, verlieren SD-WAN-Appliances, die bereits über das Non-Cloud ZTD oder das Cloud Brokered-ZTD bereitgestellt wurden, die Verbindung zum SD-WAN Orchestrator for On-Premises.



Nicht-Cloud-ZTD mithilfe der ZTD-Schnittstelle konfigurieren Wenn die Option **Verwaltungsschnittstelle für vorhandene Sites verwenden** ausgewählt ist, verwenden die Appliances, die bereits mit Non-Cloud ZTD bereitgestellt wurden, weiterhin die IP-Adresse der Verwaltungsschnittstelle, um eine Verbindung mit SD-WAN Orchestrator for On-premises herzustellen. Initiieren Sie Non-Cloud ZTD auf den Appliances, um eine Verbindung mit dem SD-WAN Orchestrator for On-Premises unter Verwendung der ZTD-Schnittstellen-IP-Adresse herzustellen.

> **Hinweis**
>
> Sie können die Option Verwaltungsschnittstelle für vorhandene Sites verwenden deaktivieren,

> nachdem alle SD-WAN-Appliances über die IP-Adresse der ZTD-Schnittstelle eine Verbindung mit dem SD-WAN Orchestrator for On-premises hergestellt haben.

Wenn die Option **Verwaltungsschnittstelle für vorhandene Sites verwenden** nicht ausgewählt ist, verlieren SD-WAN-Appliances, die bereits mit Non-Cloud ZTD bereitgestellt wurden, die Verbindung zu SD-WAN Orchestrator for On-premises. Initiieren Sie Non-Cloud ZTD auf SD-WAN-Appliances, um die Verbindung mit dem SD-WAN Orchestrator for On-Premises mithilfe der ZTD-Schnittstellen-IP-Adresse wiederherzustellen.

Cloud Brokerd ZTD mithilfe der ZTD-Schnittstelle konfigurieren Wenn die Option **Verwaltungsschnittstelle für vorhandene Sites verwenden** ausgewählt ist, verwenden die Appliances, die bereits mit Cloud Brokered ZTD bereitgestellt wurden, weiterhin die IP-Adresse der Verwaltungsschnittstelle, um eine Verbindung mit SD-WAN Orchestrator for On-premises herzustellen. Führen Sie einen der folgenden Schritte aus, um eine Verbindung mit SD-WAN Orchestrator for On-premises mithilfe der IP-Adresse der ZTD-Schnittstelle herzustellen:

- Aktualisieren Sie auf den SD-WAN-Appliances die IP-Adresse und das Zertifikat von SD-WAN Orchestrator for On-premises.

  > **Hinweis**
  >
  > Aktualisieren Sie das Zertifikat nur, wenn die Zertifikate manuell neu generiert werden. Sie müssen das Zertifikat nicht aktualisieren, wenn die Appliances bereits über die Zertifikate verfügen.

- Führen Sie einen Werksreset durch und initiieren Sie Cloud Brokered-ZTD auf den Appliances, um eine Verbindung mit dem SD-WAN Orchestrator for On-premises unter Verwendung der ZTD-Schnittstellen-IP-Adresse herzustellen.

> **Hinweis**
>
> Sie können die Option **Verwaltungsschnittstelle für vorhandene Sites verwenden** deaktivieren, nachdem alle SD-WAN-Appliances über die IP-Adresse der ZTD-Schnittstelle eine Verbindung mit dem SD-WAN Orchestrator for On-premises hergestellt haben.

Wenn die Option **Verwaltungsschnittstelle für vorhandene Sites verwenden** nicht ausgewählt ist, verlieren SD-WAN-Appliances, die bereits mit Cloud-vermitteltem ZTD bereitgestellt wurden, die Verbindung zu SD-WAN Orchestrator for On-premises. Führen Sie einen der folgenden Schritte aus, um die Verbindung mit SD-WAN Orchestrator for On-premises mithilfe der ZTD-Schnittstellen-IP-Adresse wiederherzustellen:

- Aktualisieren Sie auf den SD-WAN-Appliances die IP-Adresse und das Zertifikat von SD-WAN Orchestrator for On-premises.

- Führen Sie einen Werksreset durch und initiieren Sie Cloud Brokered-ZTD auf den Appliances, um eine Verbindung mit dem SD-WAN Orchestrator for On-premises unter Verwendung der ZTD-Schnittstellen-IP-Adresse herzustellen.

Manuelle Konnektivitätskonfiguration

Bei der manuellen Konfiguration der Konnektivität müssen Sie das Zertifikat Citrix SD-WAN Orchestrator for On-premises herunterladen und auf jede Appliance im Netzwerk hochladen. Dazu müssen Sie sich manuell bei jeder Appliance anmelden, um die Zertifikate hochzuladen.

So konfigurieren Sie die Konnektivität manuell-

1. Navigieren Sie zu **Administration > Zertifikatsauthentifizierung**, und aktivieren **Sie Authentifiz**

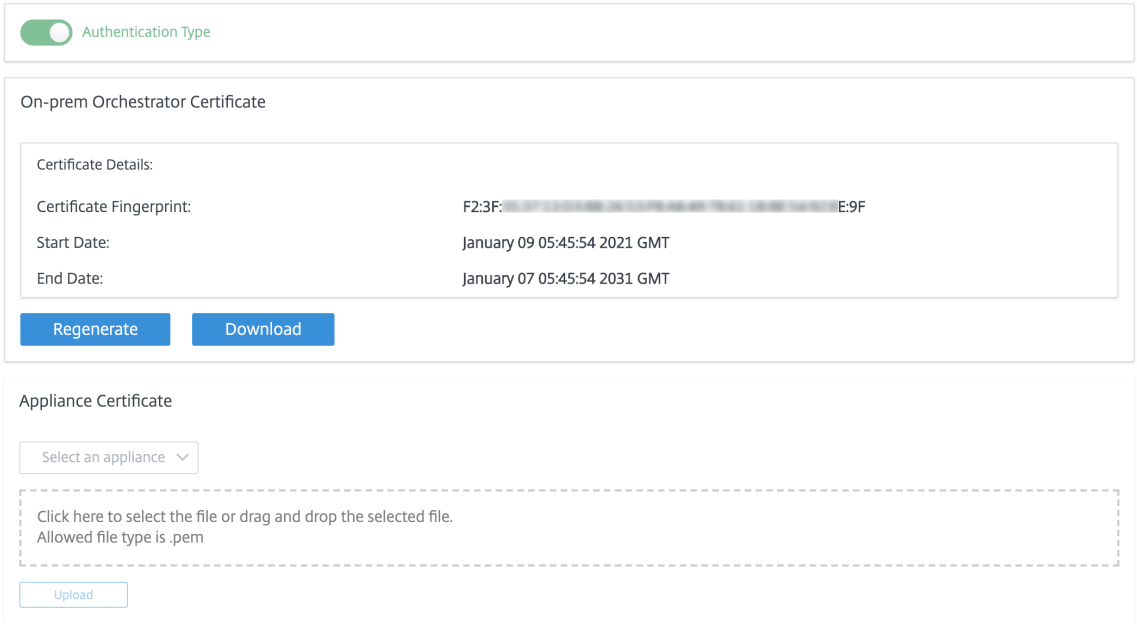
   Wenn der Authentifizierungstyp aktiviert ist, kann die SD-WAN-Appliance nur über die bidirektionale Authentifizierung eine Verbindung mit Citrix SD-WAN Orchestrator für lokale Umgebungen herstellen. Wenn der Authentifizierungstyp deaktiviert ist, kann die SD-WAN-Appliance entweder über Keine Authentifizierung, unidirektionale Authentifizierung oder bidirektionale Authentifizierung eine Verbindung zu Citrix SD-WAN Orchestrator for On-premises herstellen.

   > **Hinweis**
   >
   > In einem vom Anbieter verwalteten Setup können nur Anbieter den Authentifizierungstyp aktivieren und das Citrix SD-WAN Orchestrator for On-Premises-Zertifikat neu generieren.

2. Klicken Sie auf **Regenerieren** und **laden Sie** das Zertifikat Citrix SD-WAN Orchestrator for On-premises herunter.
3. Wählen Sie im Abschnitt **Appliance-Zertifikat eine Appliance** aus und laden Sie das entsprechende Zertifikat hoch, das von der SD-WAN-Appliance heruntergeladen wurde. Detaillierte Informationen zum Herunterladen des Appliance-Zertifikats finden Sie unter on-premises Konfiguration von Citrix SD-WAN Orchestrator auf der SD-WAN-Appliance.

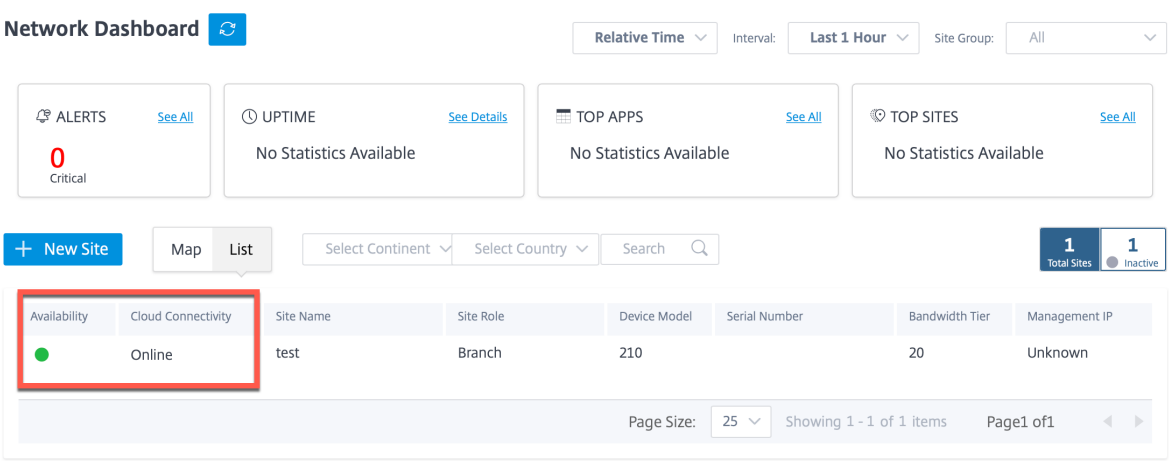
   > **HINWEIS:**
   >
   > - Es wird nur der PEM-Dateityp unterstützt.
   > - Nur Kundenadministratoren können das Appliance-Zertifikat hochladen.

4. Melden Sie sich an der Benutzeroberfläche der SD-WAN-Appliance an und navigieren Sie zu **Konfiguration > Virtuelles WAN > On-Prem SD-WAN Orchestrator**. Laden Sie das Zertifikat hoch, das Sie von Citrix SD-WAN Orchestrator for On-premises heruntergeladen haben. Detaillierte Informationen finden Sie unter Citrix SD-WAN Orchestrator für die lokale Konfiguration auf der SD-WAN-Appliance.



Konnektivität verifizieren

Um den Konnektivitätsstatus der Appliance zu überprüfen, navigieren Sie zu **Konfiguration > Netzwerkkonfiguration Home**und überprüfen Sie die Spalte **Cloud-Konnektivität**, die Ihrer Site entspricht.

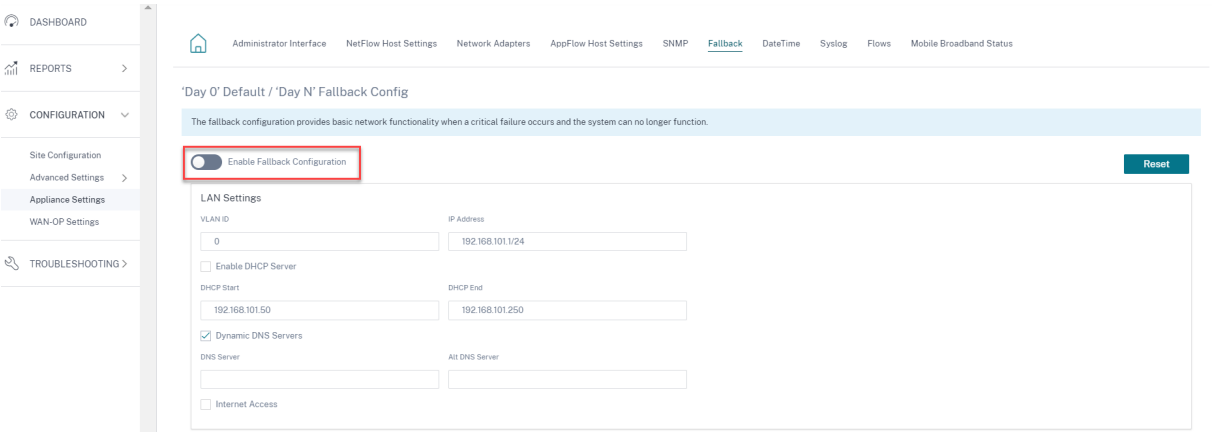


> **Hinweis:**
>
> Sie können die gewünschte Software für das Upgrade der Appliances unter **Infrastruktur > Orchestrator-Administration > Software-Images > Appliance**veröffentlichen. Weitere Informationen finden Sie unter Veröffentlichen von Software.

Fallback-Konfiguration

Die Fallback-Konfiguration stellt sicher, dass der Citrix SD-WAN Orchestrator für lokale Konnektivität, den Sie mit der Citrix SD-WAN-Appliance eingerichtet haben, über die In-Band-Verwaltungs-IP der Appliance beibehalten wird.

Sie können die Fallback-Konfiguration auf Citrix SD-WAN Orchestrator for On-premises auf Standortebene aktivieren, indem Sie zu **Konfiguration** > **Appliance-Einstellungen** > **Fallback** navigieren und auf **Fallback-Konfiguration aktivieren**klicken.

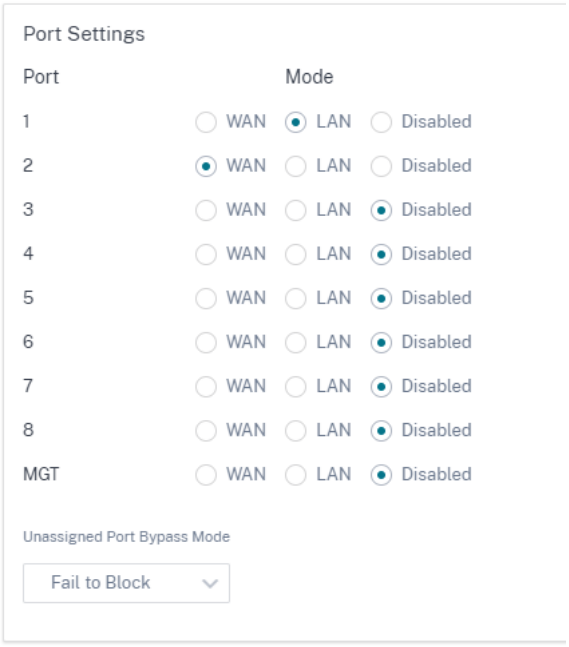


Detaillierte Informationen zur Fallback-Konfiguration finden Sie unter Inband-Verwaltung.

> **Hinweis:**
>
> Wenn Sie eine andere Appliance als Citrix SD-WAN 110 SE verwenden, stellen Sie sicher, dass Sie SD-WAN 11.2 oder eine höhere Version ausführen, um die Standardausfallkonfiguration zu aktivieren.

Die folgende Tabelle enthält die Details der vordefinierten WAN- und LAN-Ports für die Fallbackkonfiguration auf verschiedenen Plattformen:

Plattform	WAN-Ports	LAN-Ports
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)



Konfiguration auf Anbieterebene

October 31, 2022

Profile

Ein Profil ist eine **Live-Konfigurationsvorlage**. Eine reguläre Vorlage soll die Schaffung einer neuen Entität unterstützen. Sobald die Vorlage erstellt wurde, gelten nachfolgende Änderungen in der Vorlage nicht für die neuen Entitäten, die mit der Basisvorlage erstellt wurden. Ein Profil dient als zentrale Haupt-Entität, von der alle untergeordneten Entitäten nicht nur während der Erstellung, sondern auch während der gesamten Lebensdauer eines Profils erben. Alle untergeordneten Entitäten, die dem Profil zugeordnet sind, erben automatisch alle in einem Profil vorgenommenen Änderungen.

Beispielsweise erstellt ein Administrator ein Site-Konfigurationsprofil namens **kleines Einzelhandelsgeschäft** und wendet es auf alle kleinen Einzelhandelsgeschäfte an, die einem Unternehmen gehören. Nun werden alle Änderungen, die zu einem bestimmten Zeitpunkt am Profil des kleinen Einzelhandelsgeschäfts vorgenommen wurden, automatisch auf alle Geschäfte angewendet, die dieses Profil erben. Basierend auf dem, was in allen Entitäten üblich ist und was nicht, können bestimmte Parameter in der Profilkonfiguration nicht festgelegt werden. Solche Parameter wären anpassbar und können zwischen den Entitäten variieren, die das gleiche Profil erben.

Profilvorlagen für Dienstanbieter

Partner können Profilvorlagen erstellen, die ihre Kunden beim Erstellen von Profilen verwenden können.

Ein Anbieter kann beispielsweise vier Siteprofilvorlagen erstellen: Kleiner Zweig, Mittlerer Zweig, Großer Zweig und Rechenzentrum. Diese Vorlagen werden automatisch den Kundenkonten zur Verfügung gestellt, die dem Partner zugeordnet sind. Kunden können diese Vorlagen beim Erstellen von Profilen verwenden.

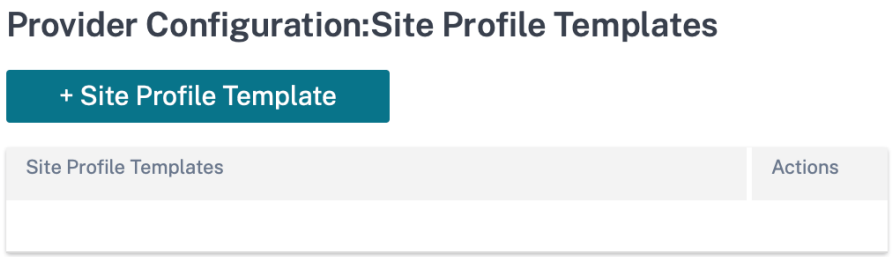
Angenommen, ein Kunde entscheidet sich, ein Profil für die Konfiguration kleiner Zweigstellen zu erstellen. Der Kunde kann eine der vom Partner freigegebenen Vorlagen auswählen, die im Rahmen der Profilkonfiguration über eine Dropdownliste zur Verfügung gestellt werden. Der Kunde kann es vor dem Speichern des Profils an seine Netzwerkanforderungen anpassen. Die Profilvorlage ist keine Live-Entität. Es unterstützt nur die Erstellung von Profilen auf Kundenebene. Profile können nur auf Kundenebene erstellt werden und sind als Live-Entitäten gedacht, die als Stammkonfigurationsdatensätze dienen.

Der Anbieter kann Konfigurationsprofile erstellen, die bei Bedarf mit einigen oder allen Kunden geteilt werden können. Site- und WAN-Profile werden derzeit unterstützt.

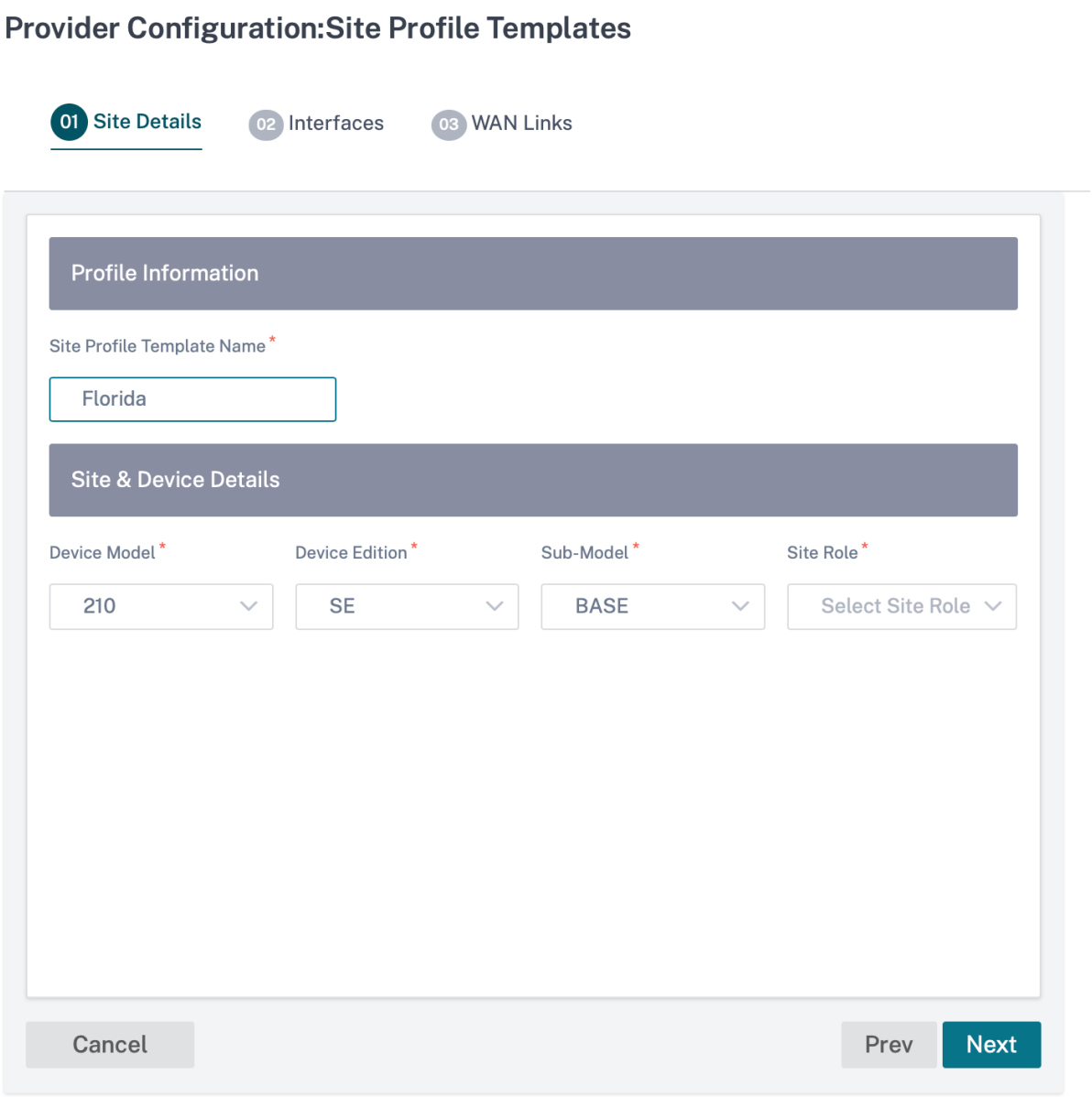
Siteprofilvorlagen

Siteprofilvorlagen sind Sitekonfigurationsvorlagen, die von Dienstanbietern erstellt werden, um die Erstellung von Siteprofilen auf Kundenebene zu ermöglichen.

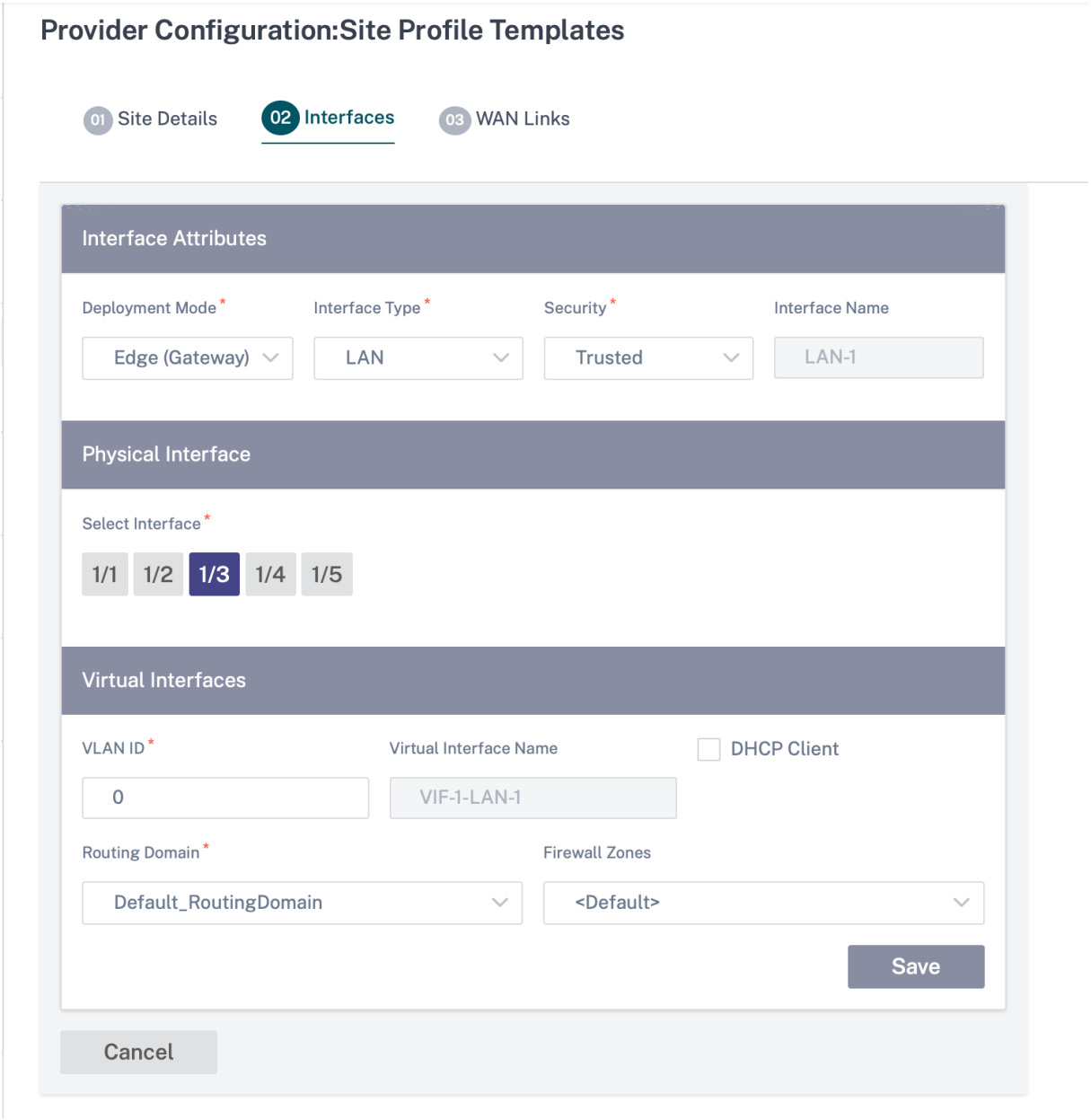
Um Profilvorlagen zu erstellen, navigieren Sie zu **Konfiguration** > **Siteprofilvorlagen** und klicken Sie auf **+ Site-Profilvorlage**.



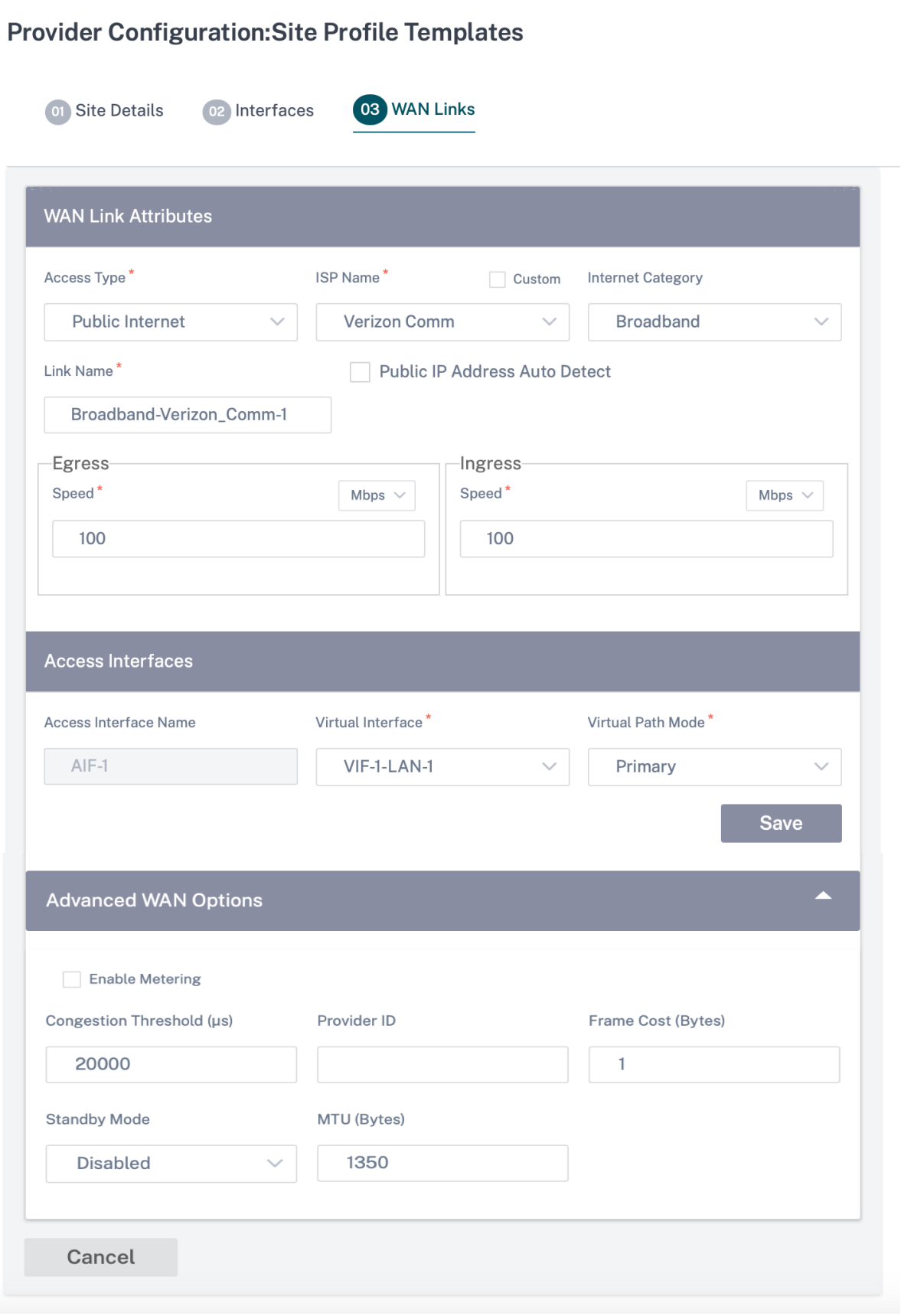
Um eine Siteprofilvorlage zu erstellen, müssen Sie die **Site-Details**, **Schnittstellen** und **WAN-Links konfigurieren**. Eine detaillierte Beschreibung der Konfiguration von Sites finden Sie unter Site-Details.



Weisen Sie der Site eine Schnittstelle zu, indem Sie auf die Option **+ Interface** klicken. Um eine Schnittstelle hinzuzufügen, müssen Sie die Felder **Interface-Attribute**, **Physical Interface** und **Virtual Interfaces** ausfüllen. Eine ausführliche Beschreibung der Konfiguration von Schnittstellen finden Sie unter Interfaces.



Stellen Sie **WAN-Link-Attribute**, **Access Interfaces** und **Services** mit **Advanced Options** bereit. Eine ausführliche Beschreibung der Konfiguration von WAN-Verbindungen finden Sie unter WAN-Links.



WAN-Link-Vorlagen

WAN-Profilvorlagen sind WAN-Link-Konfigurationsvorlagen, die von Dienstanbietern erstellt werden, um die Erstellung von WAN-Link-Profilen auf Kundenebene zu ermöglichen.

Um eine WAN-Link-Vorlage zu erstellen, klicken Sie auf **+ WAN-Link-Vorlage**. Sie müssen die WAN-Link-Informationen wie **Profilname**, **Zugangstyp**, **Internetkategorie**, **LAN-zu-WAN-Rate** usw. ausfüllen. Eine ausführliche Beschreibung der Konfiguration von WAN-Verbindungen finden Sie unter WAN-Links.

Netzwerk-Startseite

October 21, 2022

Die **Netzwerkstartseite** dient als Anker für die Netzwerkkonfiguration, bietet Konfigurationsfunktionen auf Unternehmensnetzwerkebene und dient als Ausgangspunkt für die Konfiguration des SD-WAN-Netzwerks eines Unternehmens.

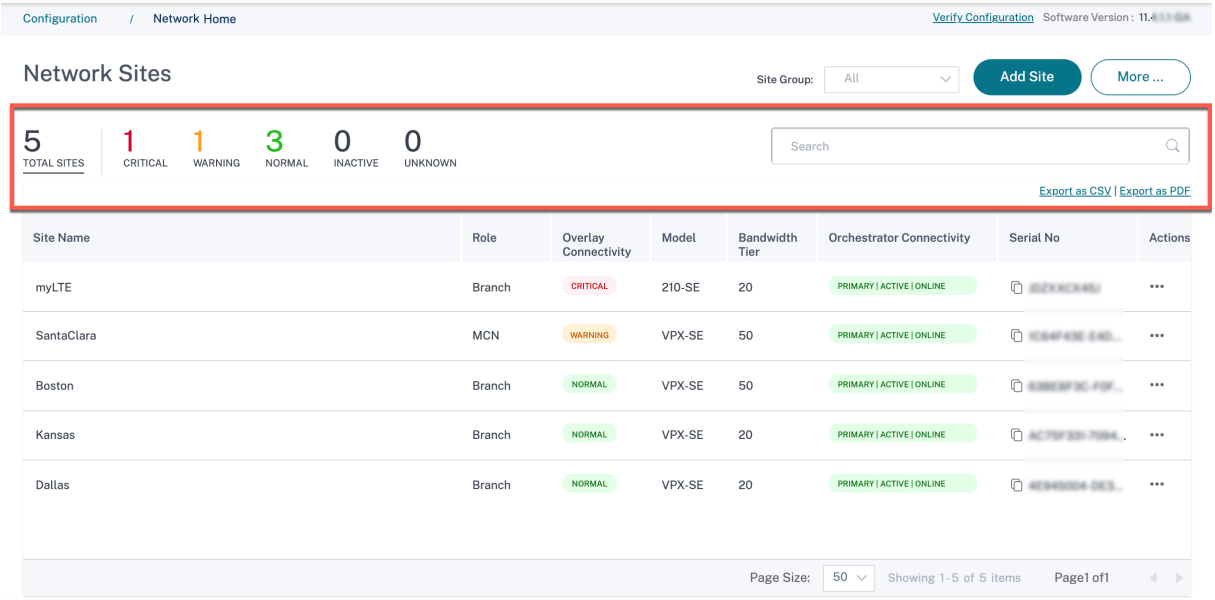
Die **Netzwerkstartseite** zeigt die Gesamtzahl der Standorte innerhalb des Netzwerks an und trennt die Standorte basierend auf ihrem Konnektivitätsstatus. Wählen Sie die nummerierten Links aus, um die Websites basierend auf den folgenden Statuskategorien anzuzeigen:

- **Kritisch** —Standorte, bei denen alle zugehörigen virtuellen Pfade ausgefallen sind.
- **Warnung** —Websites, bei denen mindestens ein virtueller Pfad ausgefallen ist.
- **Normal** - Alle virtuellen Pfade und zugehörigen Mitgliedspfade der Site sind aktiv.
- **Inaktiv** —Standorte befinden sich im Status „Nicht bereitgestellt“und „inaktiv“
- **Unbekannt** —Der Status der Website ist unbekannt.

Durch Klicken auf den Status werden die Websites anhand ihres Status gefiltert und die Details angezeigt. Sie können auch die **Suchleiste** verwenden, um die Details einer Site basierend auf

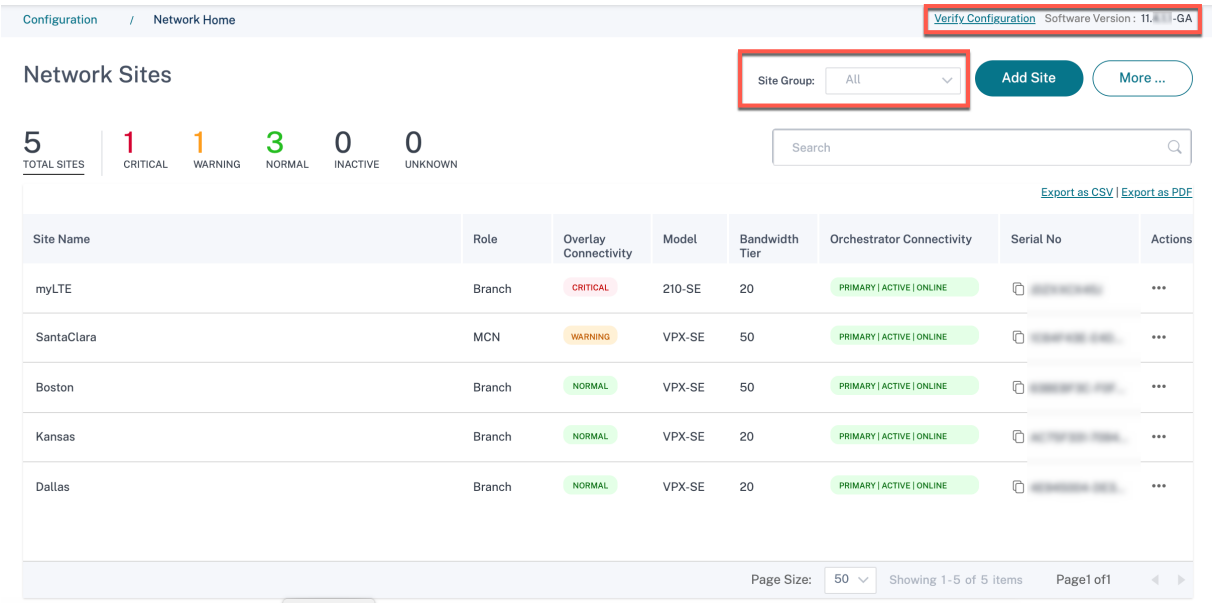
dem Site-Namen, der Rolle, der Overlay-Konnektivität, dem Modell, der Bandbreitenstufe und den Seriennummernparametern anzuzeigen.

Sie können die gefilterten Ergebnisse in eine CSV- oder PDF-Datei **exportieren, indem Sie die Optionen Als CSVexportieren und Als PDF**exportieren verwenden. Dem CSV- und PDF-Dateinamen wird**SiteList** vorangestellt, gefolgt von Datum und Uhrzeit, zu der die Datei exportiert wird.



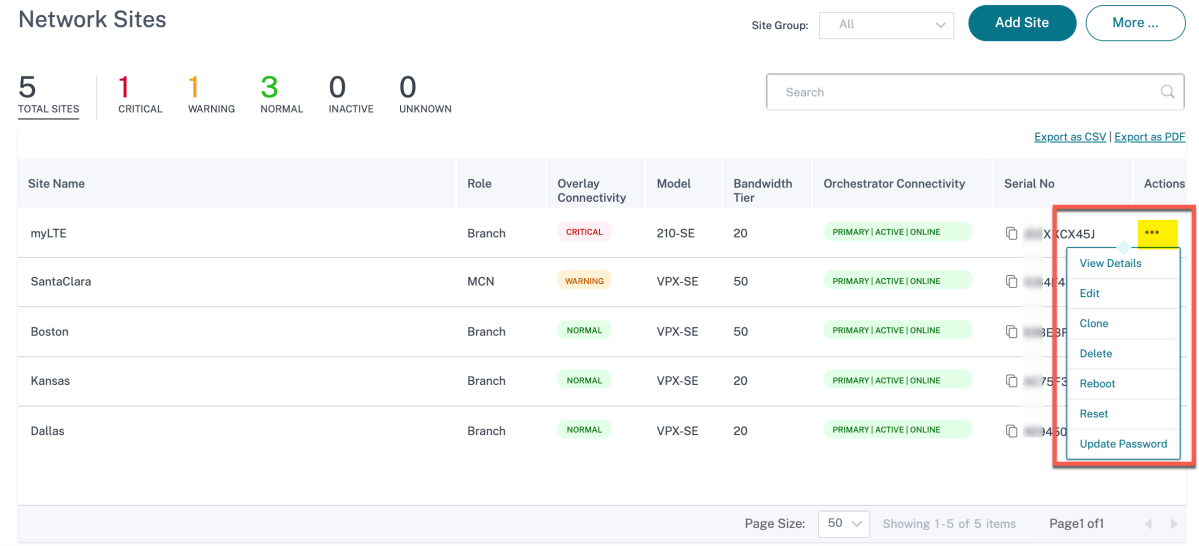
In der oberen rechten Ecke des Bildschirms können Sie die aktuelle Softwareversion anzeigen. Klicken Sie auf **Konfiguration überprüfen**, um alle Überwachungsfehler zu überprüfen. Weitere Informationen finden Sie unter Konfiguration überprüfen.

Sie können die Sites anhand der Gruppe/Region filtern, zu der sie gehören, indem Sie die Dropdown-Liste **Sitegruppe** verwenden.

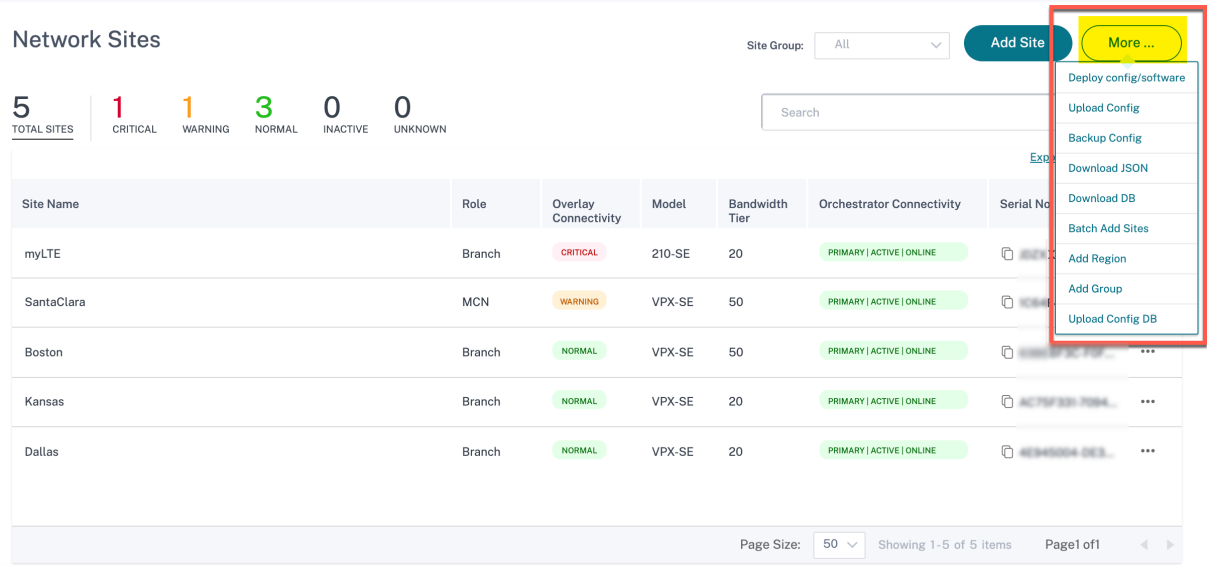


Wenn Sie im gefilterten Ergebnis auf den Site-Namen klicken, gelangen Sie zum Bildschirm **Site-Konfiguration** . Wenn sich der Standort in einem Hochverfügbarkeits-Setup befindet, wird in der Spalte **Orchestrator-Konnektivität** der Status der primären und sekundären Appliances angezeigt. In der Spalte **Seriennummer** wird die Seriennummer der Appliance angezeigt. In einem Hochverfügbarkeits-Setup werden die Seriennummern der primären und sekundären Appliance angezeigt. Sie können die Seriennummer der Appliance mithilfe des Kopiersymbols kopieren.

In der Spalte **Aktionen** können Sie Details anzeigen, das Kennwort der Site bearbeiten, klonen, löschen, zurücksetzen und aktualisieren. Sie können auch die mit einer Site verknüpften Geräte neu starten.



Sie können andere Aktionen wie Upload-Konfiguration, Hinzufügen von Websites in einem Stapel, Herunterladen von JSON usw. mit der Option **Mehr...** ausführen.



Site hinzufügen

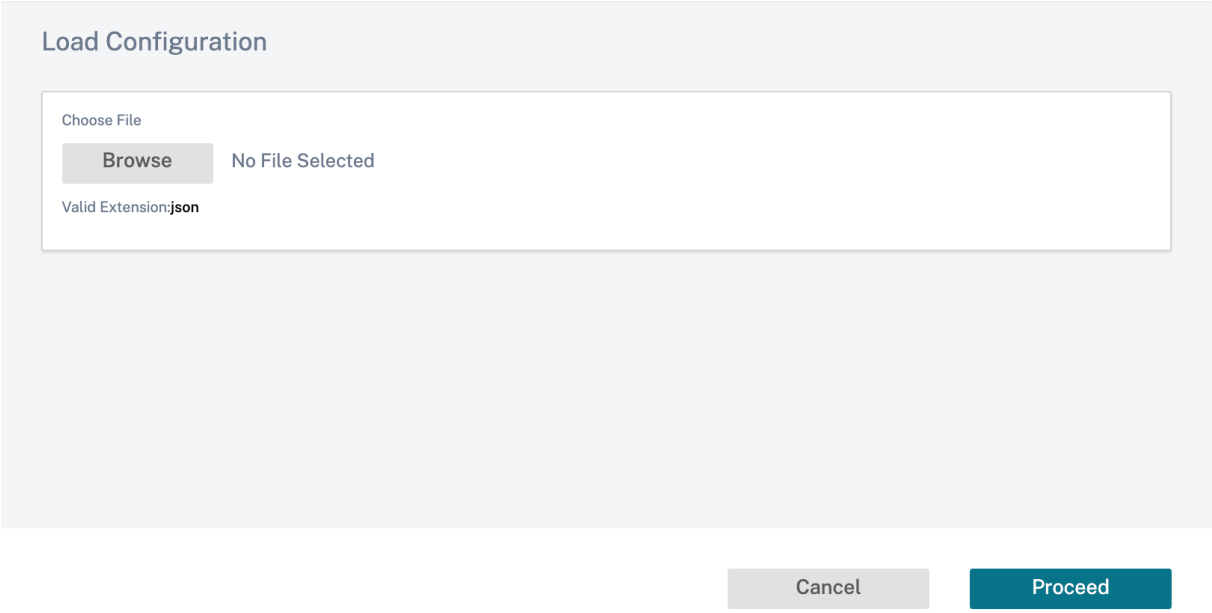
Verwenden Sie die Option **+ Site hinzufügen**, um eine neue Site hinzuzufügen. Weitere Informationen zum Workflow der Standortkonfiguration finden Sie unter Standortkonfiguration.

Konfiguration und Software bereitstellen

Mit der Option **Mehr > Konfiguration/Software bereitstellen** gelangen Sie zum Abschnitt **Bereitstellung**, in dem Sie die Konfiguration im gesamten Netzwerk überprüfen, bereitstellen und aktivieren können. Weitere Informationen zum Bereitstellen von Konfiguration und Software finden Sie unter Bereitstellung.

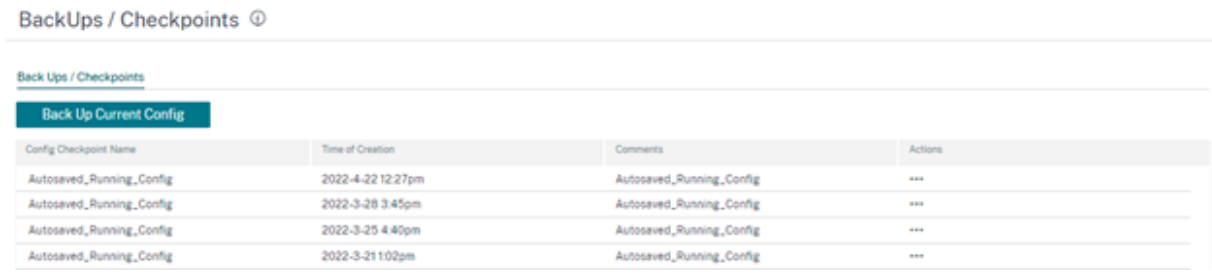
Konfiguration hochladen

Mit der Option **Mehr > Konfiguration hochladen** können Sie eine der zuvor gespeicherten Konfigurationen durchsuchen und hochladen. Die neu hochgeladene Konfiguration dient als aktive Konfiguration für das Netzwerk.



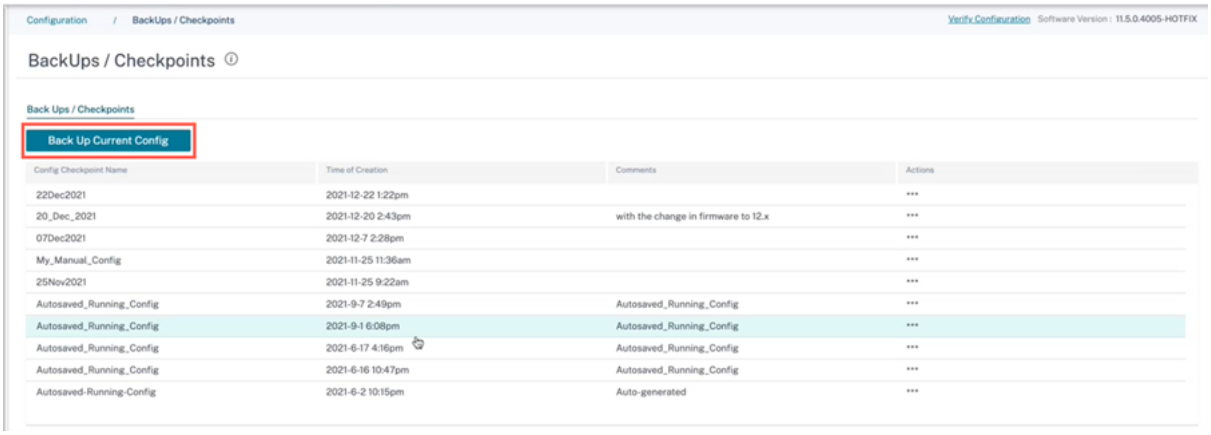
Backups/Checkpoints

Die Option **Mehr > Backup-Konfiguration** führt Sie zur Seite **Backups/Checkpoints** und bietet die Möglichkeit, die Konfiguration zu sichern und wiederherzustellen oder die gespeicherten Checkpoints zu überprüfen.

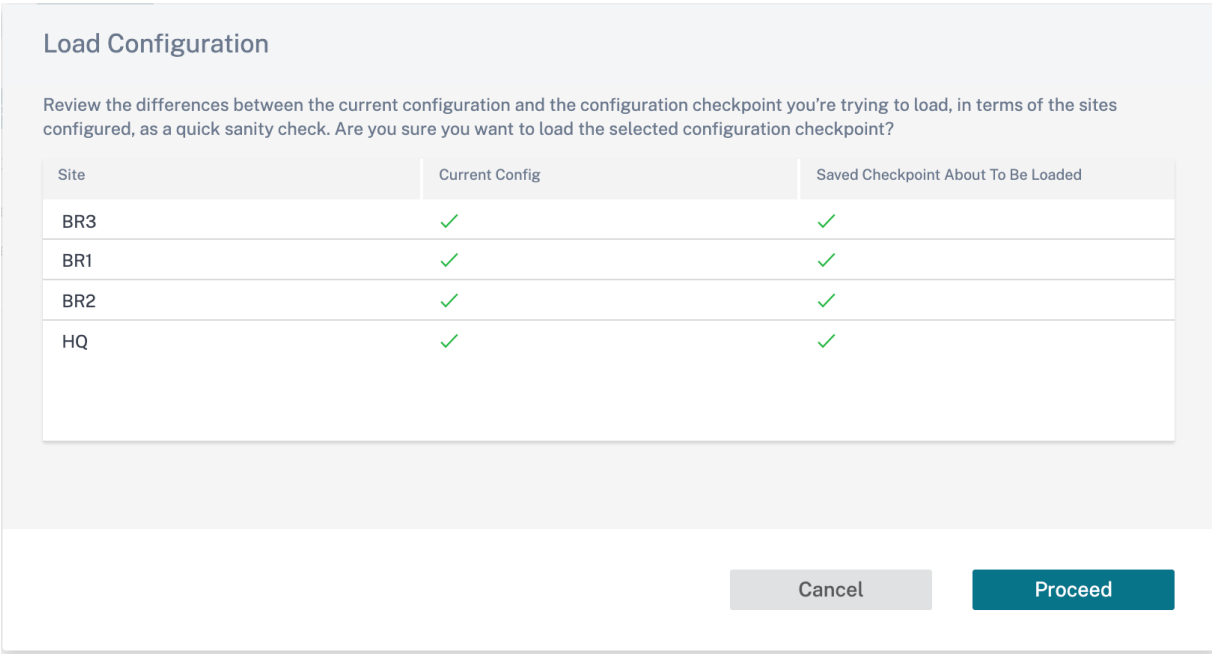


Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen.

Klicken Sie auf **Aktuelle Konfiguration** sichern, um die aktuelle Konfiguration als Checkpoint für die zukünftige Verwendung zu sichern.



Klicken Sie auf **Konfiguration laden** (unter **Aktionen**), um eine gespeicherte Konfiguration zu laden. Klicken Sie auf **Weiter**.



Klicken Sie auf **Kopieren** (unter **Aktionen**), um eine ähnliche Kopie einer vorhandenen Konfiguration

zu erstellen. Sie können die gespeicherten Konfigurationsprüfpunkte auch herunterladen, bearbeiten und löschen. Diese Operationen sind unter **Aktionen**verfügbar.

JSON herunterladen

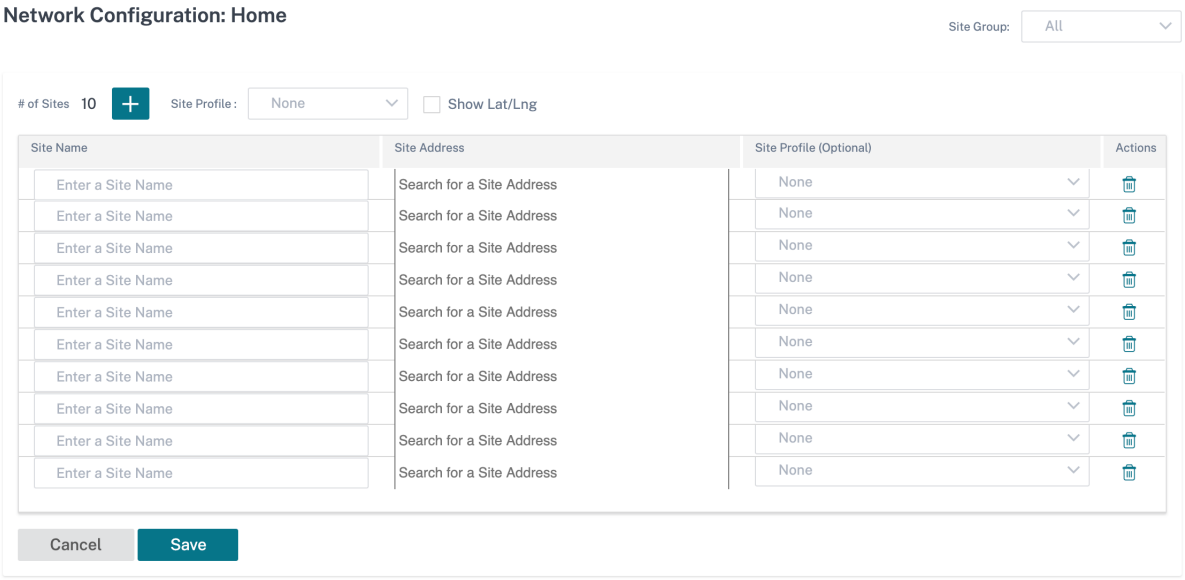
Mit der Option **Mehr > JSON herunterladen** können Sie die aktuelle Konfiguration im JSON-Format herunterladen und exportieren, um sie offline zu überprüfen.

DB herunterladen

Mit der Option **Mehr > DB herunterladen** können Sie die aktuelle Konfiguration im DB-Format herunterladen und exportieren.

Hinzufügen von Websites in einem Stapel

Mit der Option **Mehr > Sites stapelweise hinzufügen** können Sie schnell mehrere Sites in einem Stapel hinzufügen. Sie können auch ein Standortprofil auswählen, das für jede Site verwendet werden soll, sodass Sie nur eindeutige Parameter wie IP-Adressen erhalten, die für jede Site noch konfiguriert werden müssen.



Region hinzufügen

Mit der Option **Mehr > Region hinzufügen** können Sie eine Region erstellen und gelangen zur **Seite Standort- und IP-Gruppen > Regionen** . Weitere Informationen finden Sie unter Regionen.

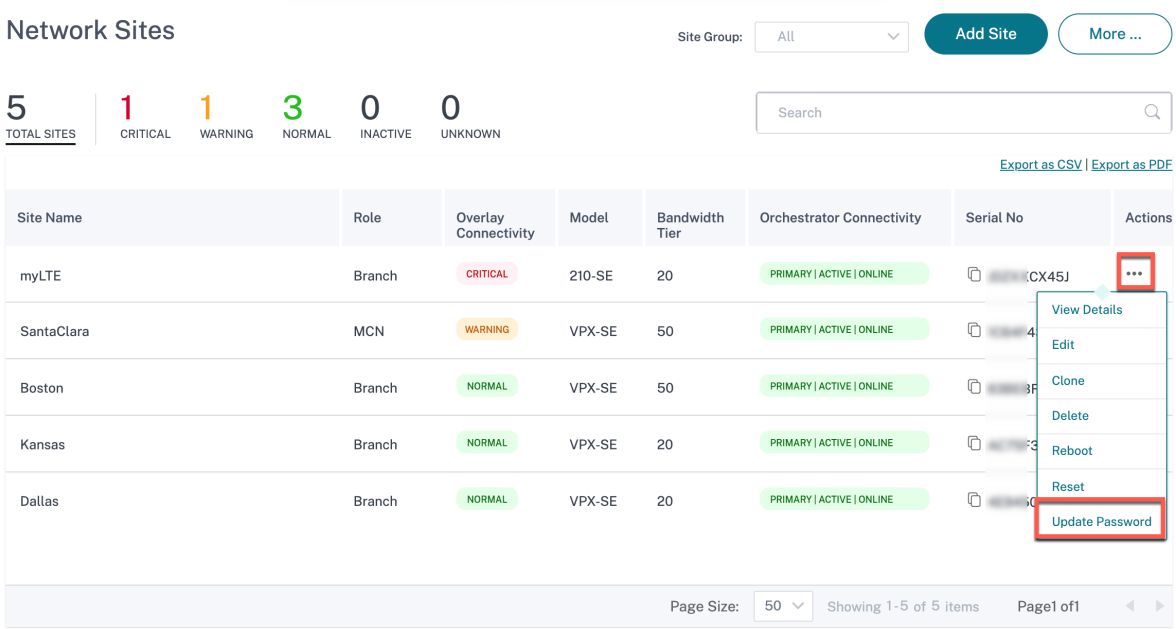
Gruppe hinzufügen

Mit der Option **Mehr > Gruppe hinzufügen** gelangen Sie zur **Seite Standort- und IP-Gruppen > Benutzerdefinierte Gruppen**, auf der Sie eine Region erstellen können. Weitere Informationen finden Sie unter Benutzerdefinierte Gruppen.

Kennwort aktualisieren

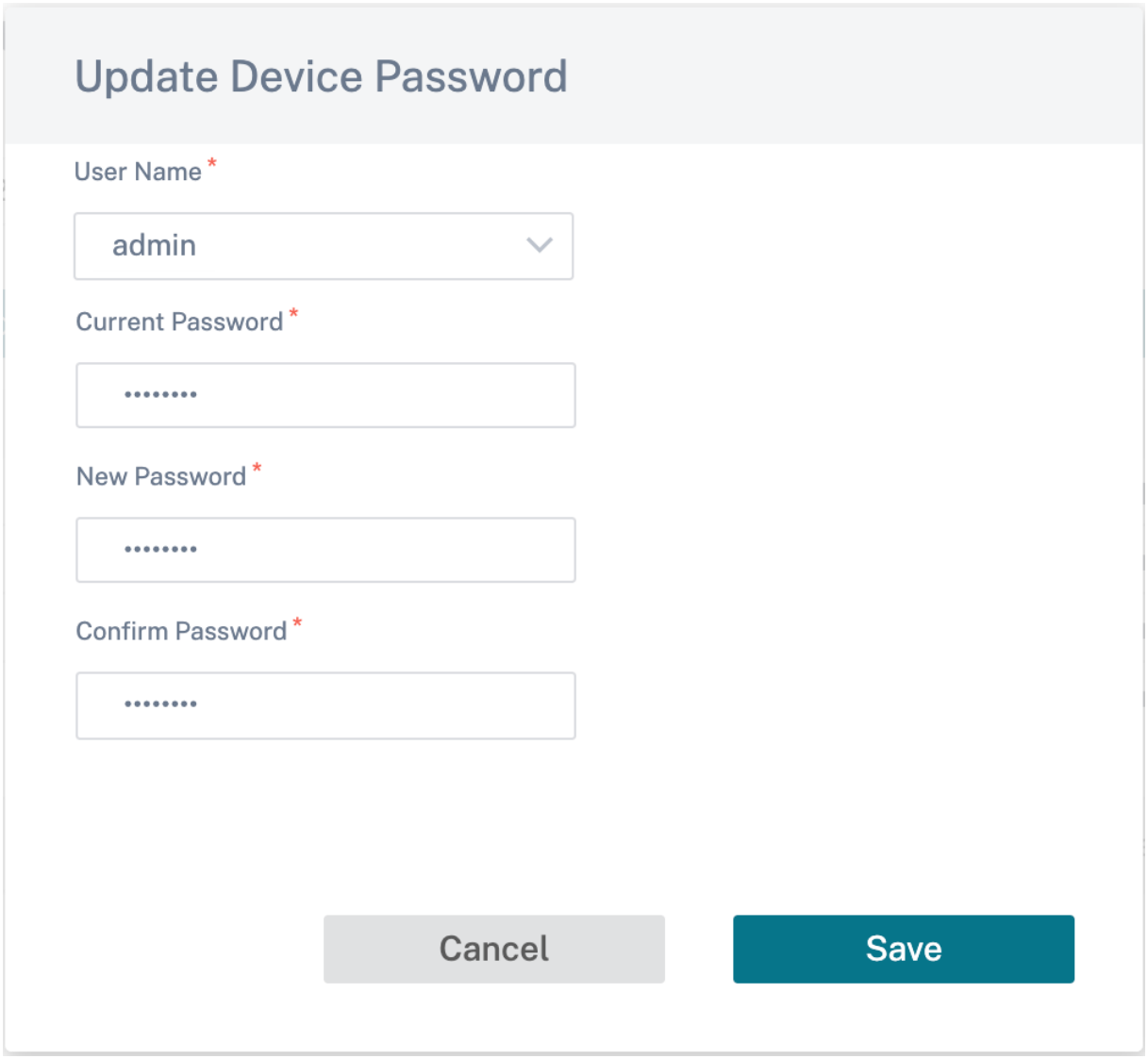
Sie können das Kennwort der SD-WAN-Appliances an verschiedenen Standorten im Netzwerk über den Citrix SD-WAN Orchestrator for On-premises ändern.

Um das Kennwort zu ändern, klicken Sie für eine Appliance, die online ist, auf das Symbol „Mehr“und wählen Sie **Passwort aktualisieren**



Geben Sie die Werte für die folgenden Felder an:

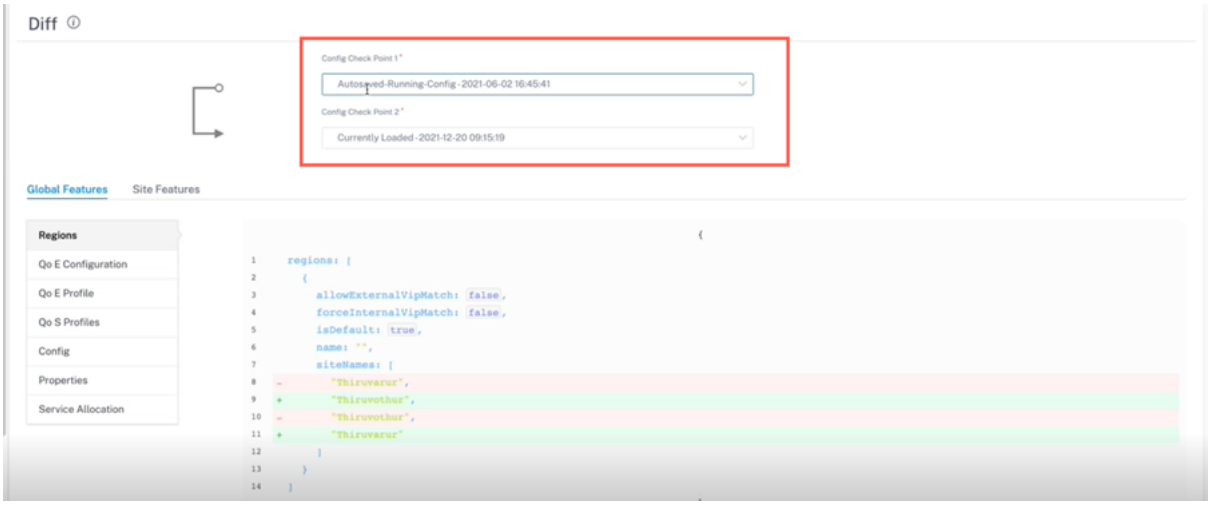
- **Benutzername**: Wählen Sie aus der Liste der auf der Site konfigurierten Benutzer einen Benutzernamen aus, für den Sie das Kennwort ändern möchten.
- **Aktuelles Passwort**: Geben Sie das aktuelle Passwort ein. Dieses Feld ist für Admin-Benutzer optional.
- **Neues Passwort**: Geben Sie ein neues Passwort Ihrer Wahl ein.
- **Passwort bestätigen**: Geben Sie das Passwort zur Bestätigung erneut ein.



Unterschied bei der Konfiguration

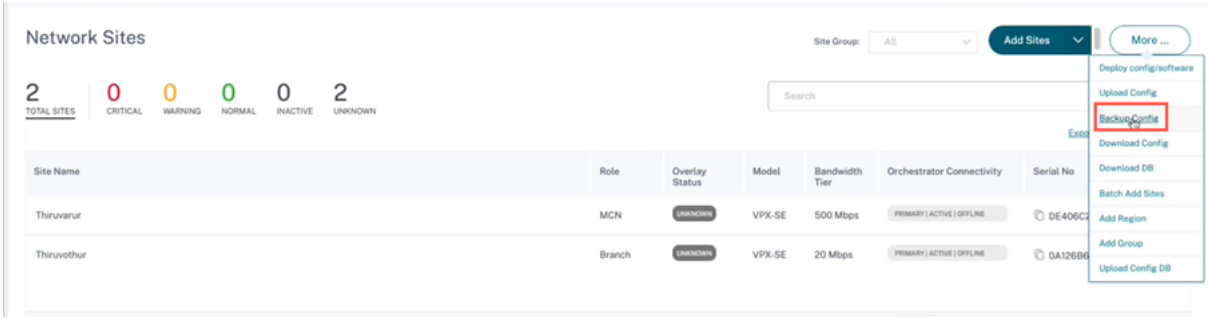
October 21, 2022

Mit der **Config Diff-Funktion** können Sie den Unterschied zwischen zwei beliebigen Versionen von Konfigurationsprüfpunkten überprüfen. Die Option **Config Diff** ist auf Netzwerkebene unter **Konfiguration** > **Config Diff**verfügbar.

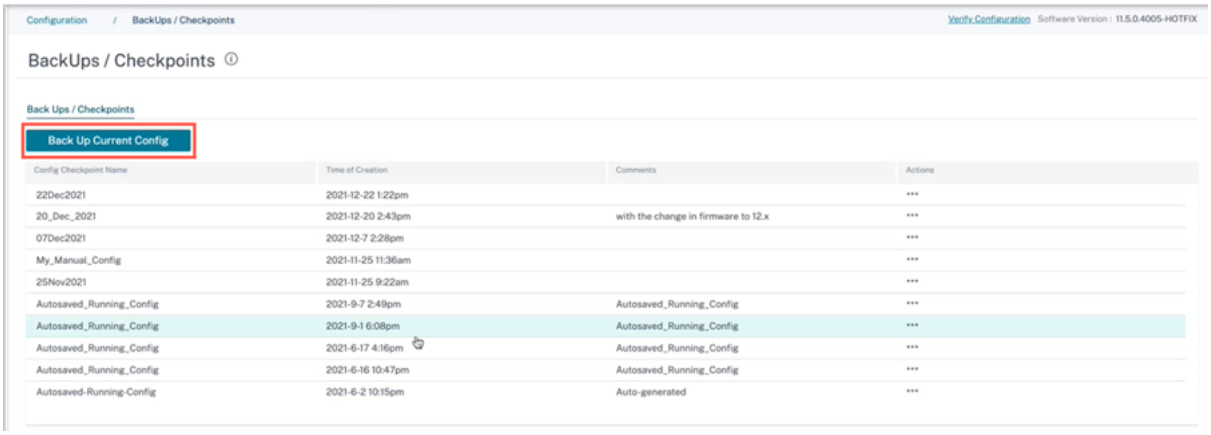


Während der Bereitstellung können Sie eine Konfiguration mit einem passenden Namen speichern. Die gespeicherten Konfigurationen werden als Checkpoints bezeichnet. Beim Vergleich der Unterschiede zwischen den beiden Konfigurationen müssen Sie die erforderlichen Konfigurationen aus den Dropdown-Listen **Config Check Point 1/2** auswählen.

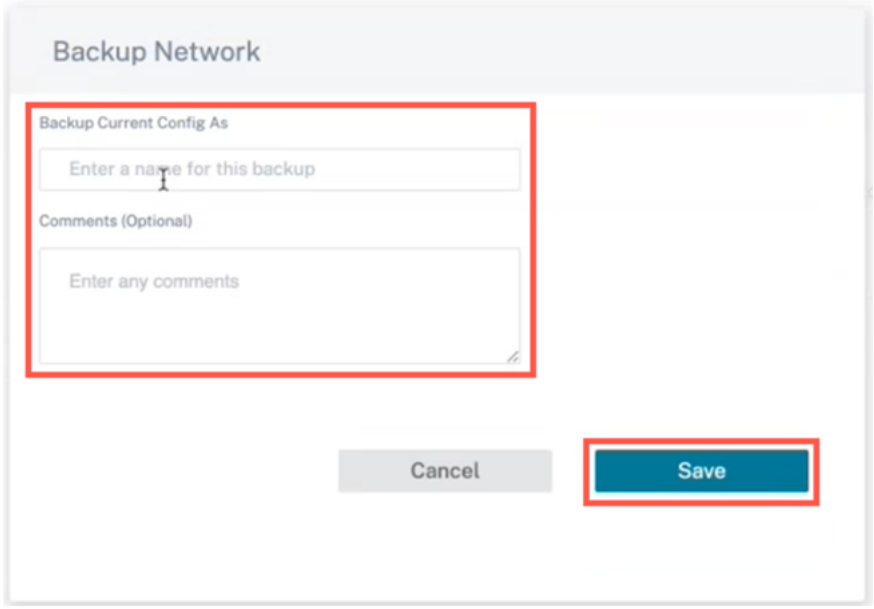
Sie können die Liste der gespeicherten Konfigurationen, Backups/Prüfpunkte unter **Konfiguration > Netzwerkstartseite** wählen SieBackup-Konfigurationaus der Dropdown-ListeMehr** anzeigen.



Wenn eine Bereitstellung stattfindet, wird die Konfiguration jedes Mal automatisch gesichert. Sie können die aktuelle Konfiguration auch manuell Backup. Klicken Sie dazu auf die Option **Aktuelle Konfiguration sichern** .



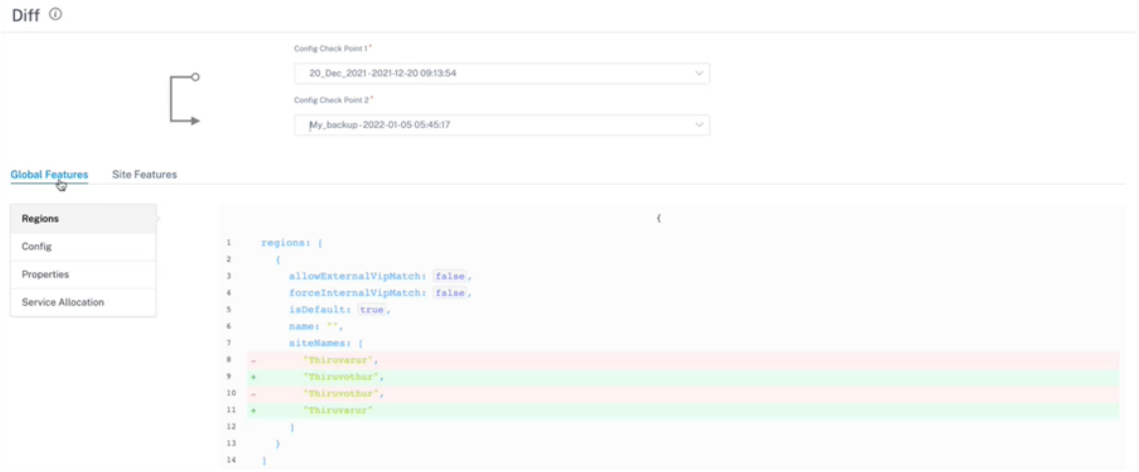
Geben Sie einen Namen an, um Ihre Konfiguration zusammen mit Kommentaren zu speichern (optional). Klicken Sie auf **Speichern**.



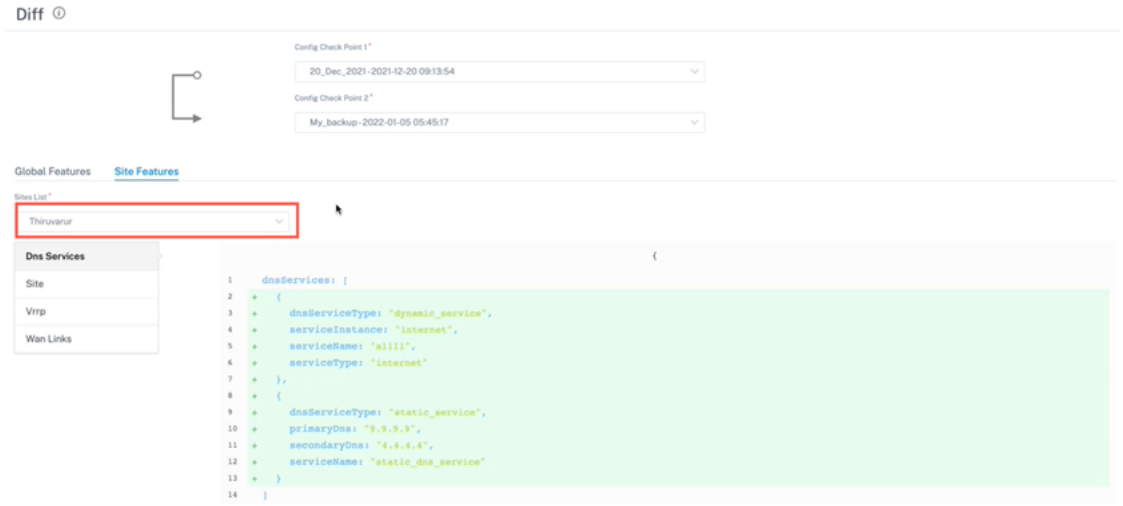
> **Hinweis:**
>
> Sie können maximal fünf Konfigurationssicherungen speichern/erstellen. Beim Erstellen eines neuen Backup wird automatisch die älteste Backup-Konfiguration gelöscht.

Es stehen zwei Arten von Konfigurationen zur Verfügung:

- **Globale Ebene**: Unter globaler Kategorie können Sie eine Liste der aktualisierten globalen Features wie Regionen, Eigenschaften und Konfiguration anzeigen.



- **Standortebene**: Unter Sitekategorie können Sie die Site aus der Dropdownliste auswählen und die geänderten Details wie Standort, WAN-Links und DNS-Dienste anzeigen.



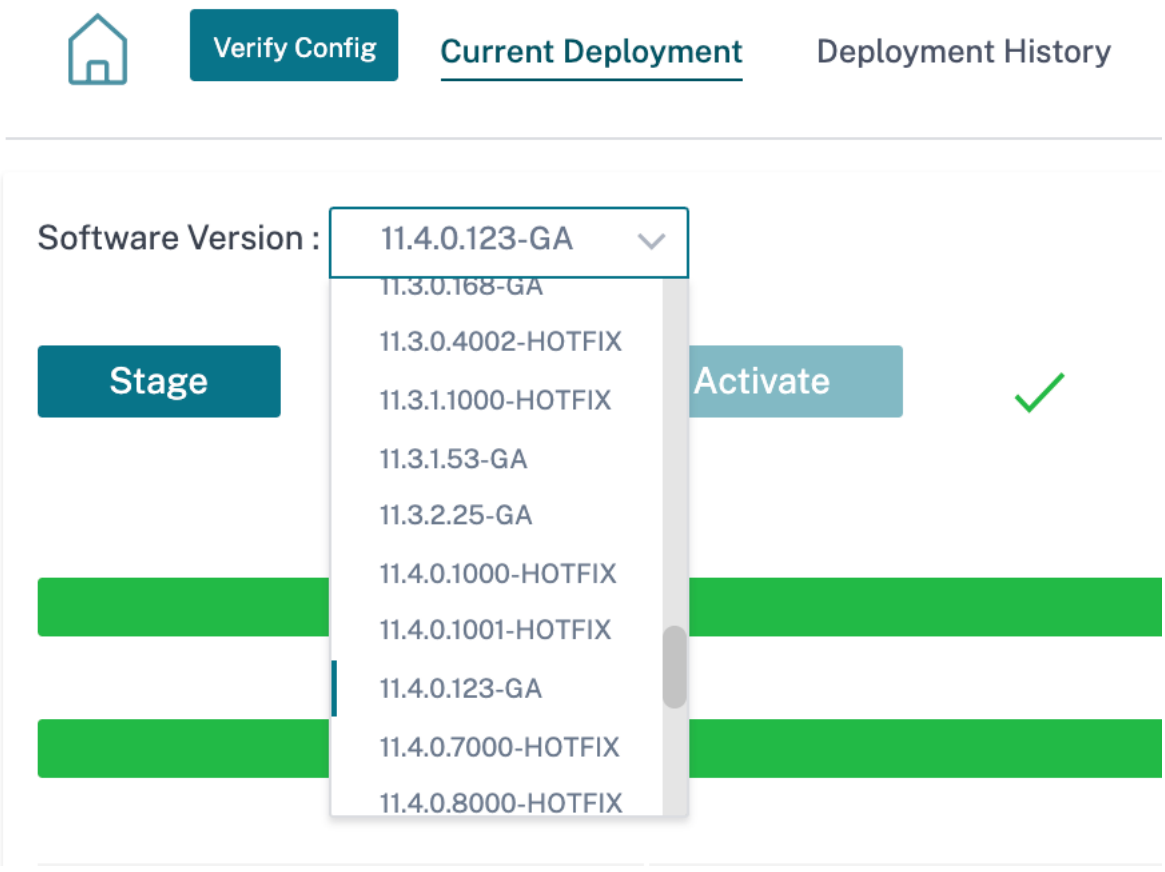
Ein gelöschter Wert erscheint auf rotem Hintergrund mit Minussymbol und der aktualisierte/hinzugefügte Wert erscheint auf grünem Hintergrund mit Pluszeichen.

Bereitstellung

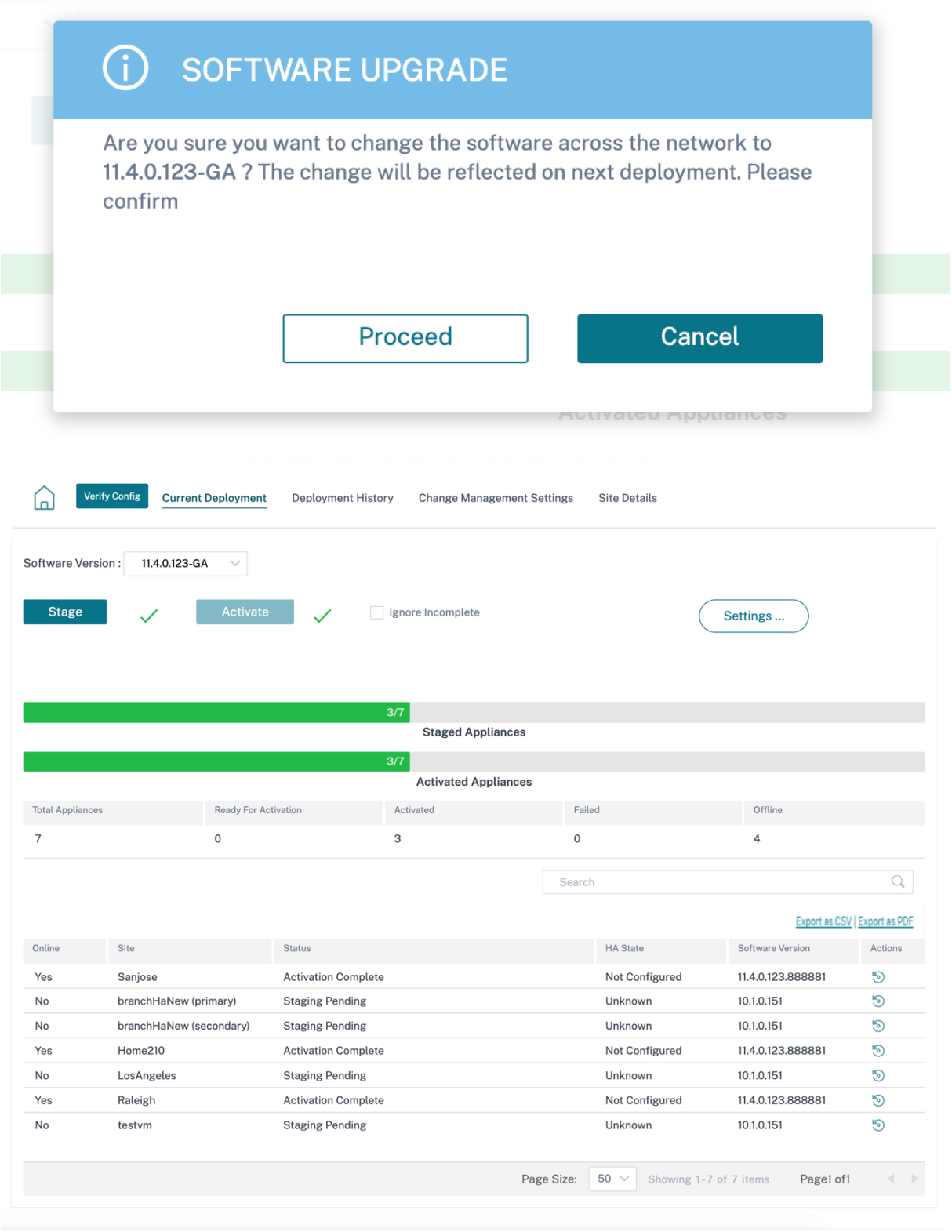
October 21, 2022

Nachdem die Sites konfiguriert wurden, können Sie auf der Seite **Bereitstellung** die Softwareversion ändern, die Konfiguration bereitstellen und im gesamten Netzwerk bereitstellen.

Sie können die SD-WAN-Software auf allen Appliances im Netzwerk aktualisieren, indem Sie im Feld Softwareversion eine **Appliance-Softwareversion** auswählen.



Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **Weiter**.



Rollback bei Fehler

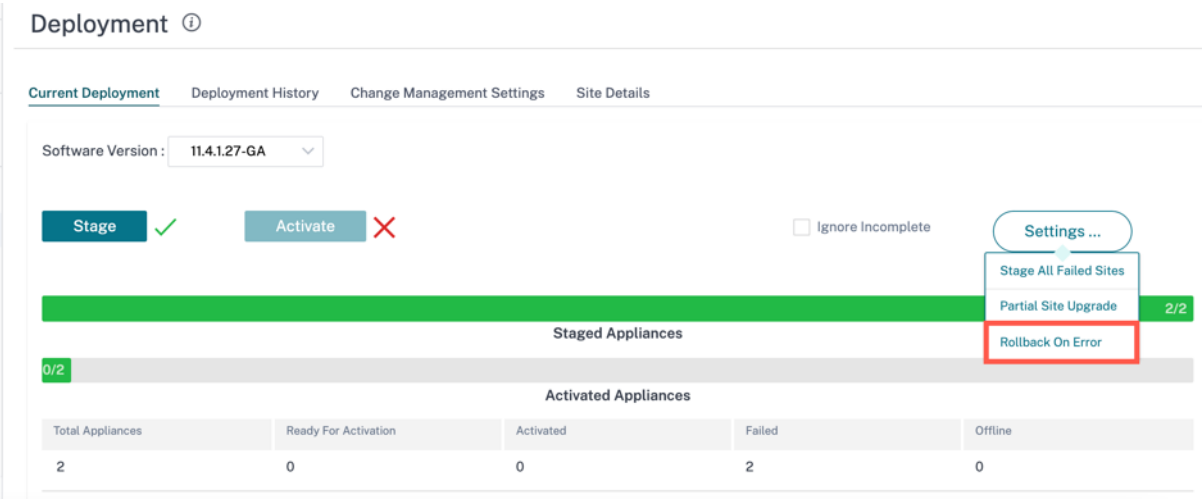
Wenn die Funktion **„Rollback on Error** “aktiviert ist, lösen Sites, die nach der Netzwerkaktivierung (als Teil der Bereitstellung) keine Verbindung zum Citrix SD-WAN Orchestrator Service herstellen können, ein automatisches Rollback auf die vorherige Version (letztes bereitgestelltes Paket) aus, um zu versuchen, die Konnektivität wiederherzustellen.

> **Hinweis**
> Das automatische Rollback gilt nur für die Site, die keine Verbindung zum Citrix SD-WAN Orchestrator Service herstellen konnte, und nicht für das gesamte Netzwerk.

Das Rollback wird nur ausgelöst, wenn die Appliance die Konnektivität des Citrix SD-WAN Orchestrator Service verliert, nicht in anderen Szenarien, z. B. wenn der Status des virtuellen Pfads ausfällt oder so weiter.

Wenn mindestens ein Standort im Netzwerk ein Rollback initiiert, wird eine Warnmeldung mit einer Liste der Sites angezeigt, die versuchen, ein Rollback durchzuführen, sowie eine Option zum Initiieren eines netzwerkweiten Rollbacks aller Online-Sites. Sie können den Fortschritt dieser Websites überprüfen und die entsprechende Aktion auswählen.

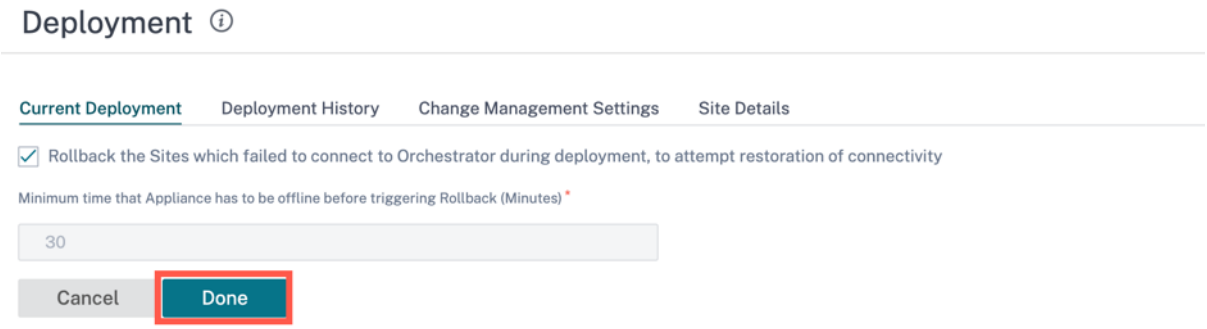
Um die Rollback-Funktion bei einem Fehler zu aktivieren, navigieren Sie zu **Konfiguration > Bereitstellung > Einstellungen > Rollback bei Fehler**.



Sie können das Kontrollkästchen **Rollback bei Fehler** aktivieren, um das automatische Rollback von Sites zu aktivieren, die nach der Aktivierung keine Verbindung zum Citrix SD-WAN Orchestrator Service herstellen konnten. Die Funktion **Rollback bei Fehler** muss aktiviert sein, bevor Sie die Bereitstellung starten, um ihre Funktionalität zu aktivieren.

Damit eine Site ein automatisches Rollback auslösen kann, muss sie nach der Aktivierung mindestens 30 Minuten (derzeit nicht änderbar) offline bleiben. Wenn die Site innerhalb von 30 Minuten eine

Verbindung zum Citrix SD-WAN Orchestrator Service herstellen kann, wird das Rollback nicht ausgelöst.

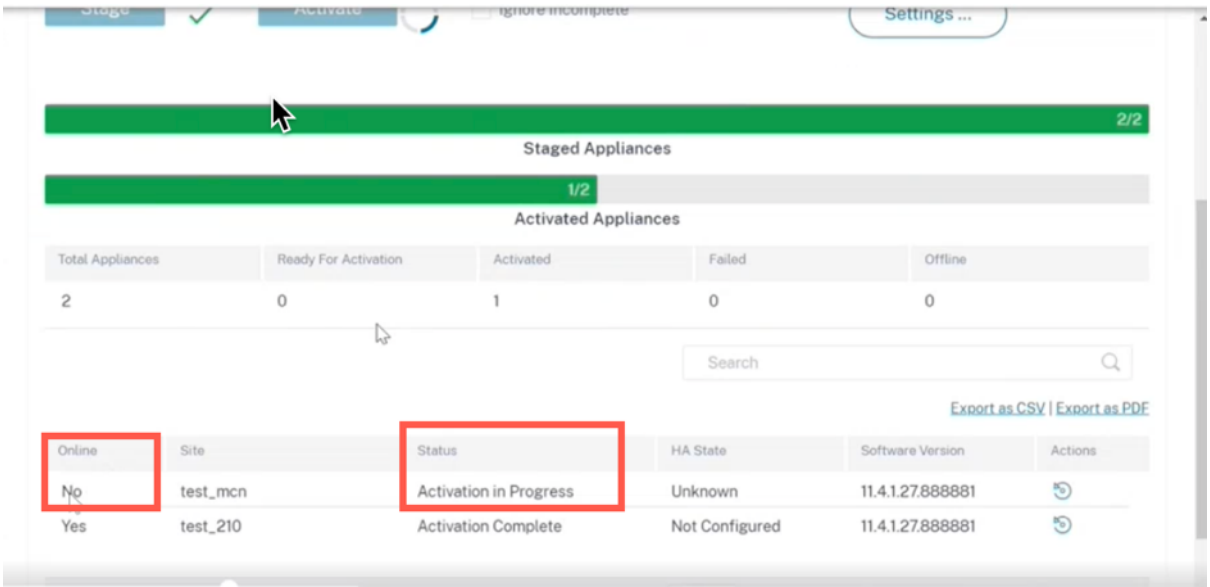


> **Hinweis:**
> Rollback auf Sites wird nur durchgeführt, wenn die Site nach der Aktivierung die Verbindung verliert. Rollback wird nicht ausgelöst, wenn die Website online ist und die Aktivierung fehlgeschlagen ist.

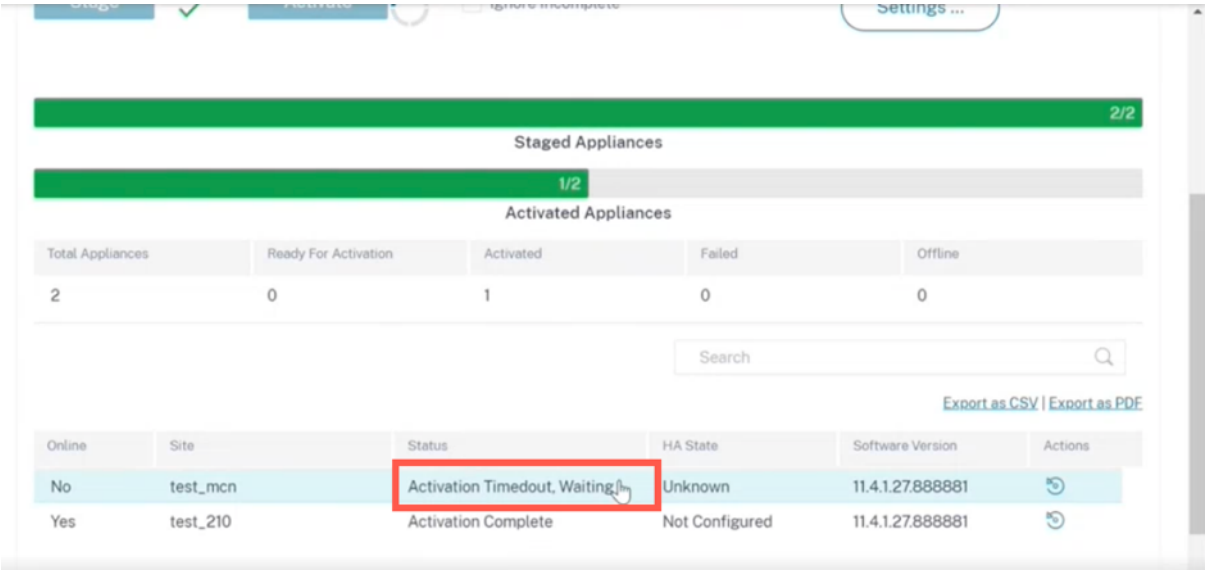
Klicken Sie auf **Fertig**, wenn Sie **Rollback on Error** aktiviert haben.

Anwendungsfall 1: Upgrade ohne Treffer

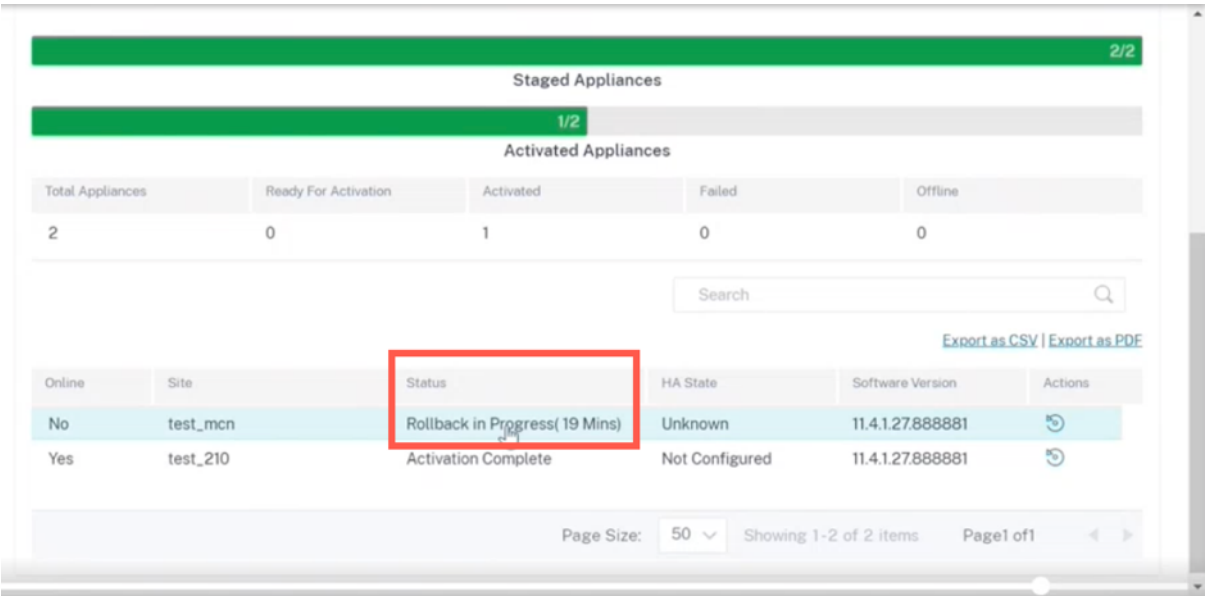
Eine Site wartet für eine bestimmte Zeit auf den Abschluss der Aktivierung mit dem Status „**Aktivierung in Bearbeitung**“.



Wenn die Site nach diesem Timeout noch offline ist, wartet der Citrix SD-WAN Orchestrator Service weitere 30 Minuten (Zeitlimit für die Rollback-Initiierung), um der Site die Möglichkeit zu geben, eine Verbindung herzustellen. In dieser Phase wird der Status als **Aktivierungs-Timeout, Warten auf Initiierung des Rollbacks angezeigt (verbleibende Zeit in Minuten)**.

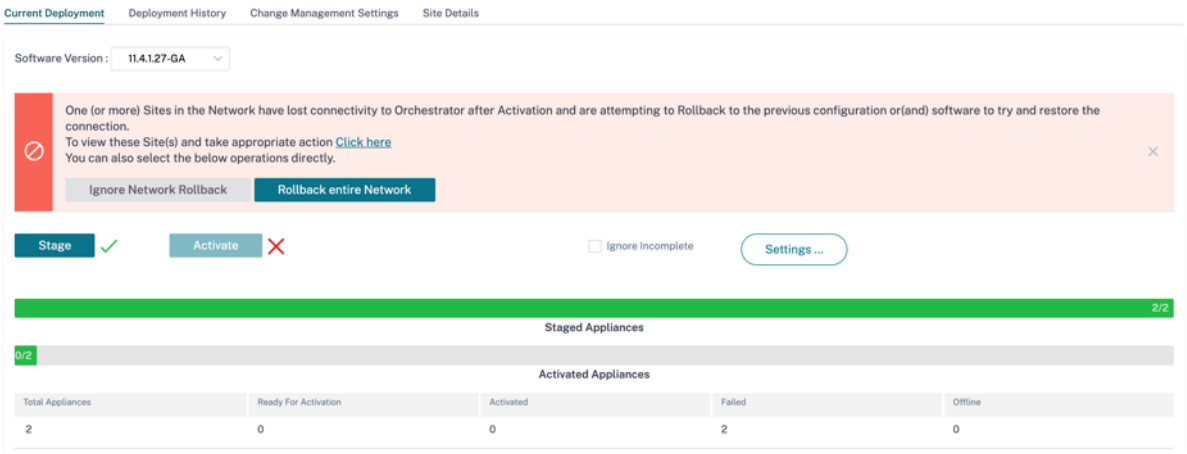


Nach Ablauf der 30-minütigen Wartezeit löst die Appliance ein automatisches Rollback auf die vorherige Konfiguration oder (und) Software aus, um zu versuchen, die Konnektivität des Citrix SD-WAN Orchestrator Service wiederherzustellen. Der Citrix SD-WAN Orchestrator Service wartet 20 Minuten (nicht konfigurierbare Einstellung), bis die Appliance eine Verbindung zum Citrix SD-WAN Orchestrator Service herstellt. Während dieses Zeitraums wird der Status als **Rollback in Bearbeitung angezeigt (verbleibende Zeit in Minuten)**.



Wenn die Appliance keine Verbindung mehr herstellen kann, markiert der Citrix SD-WAN Orchestrator Service den Rollback-Vorgang in diesen 20 Minuten als fehlgeschlagen und der Status wird als **Geräterollback fehlgeschlagen**angezeigt.

Wenn im Netzwerk mindestens ein Gerät den automatischen Rollback initiiert hat, wird dem Benutzer ein Banner wie folgt präsentiert:

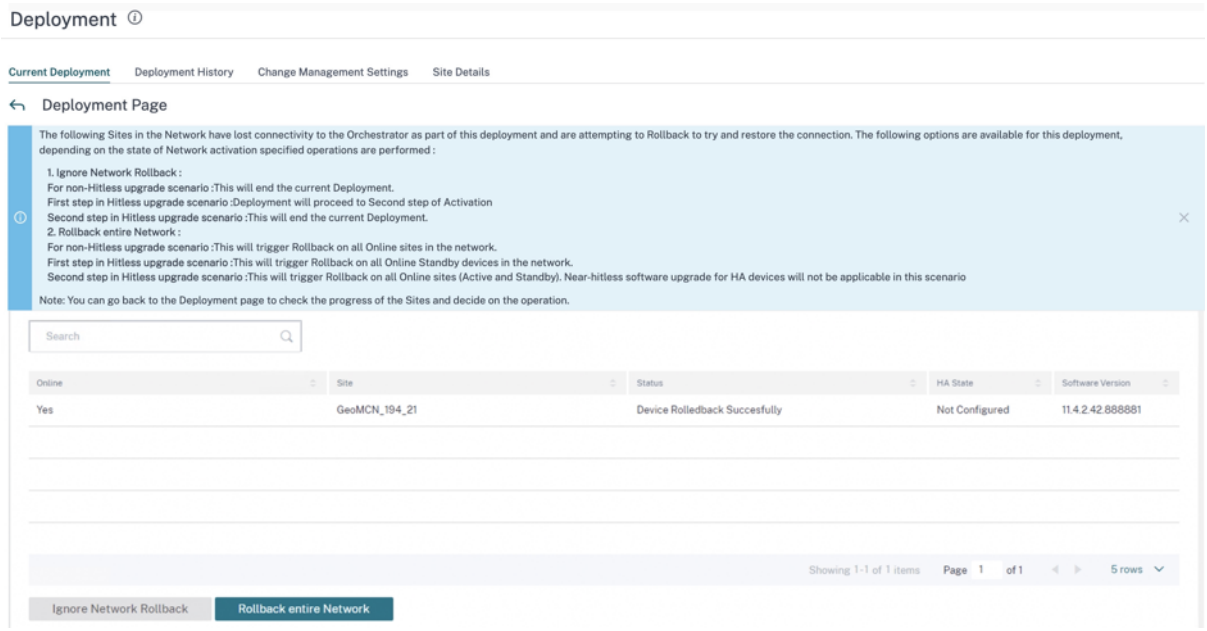


Basierend auf der Phase der Netzwerkaktivierung führen die angezeigten Optionen die folgenden Vorgänge aus:

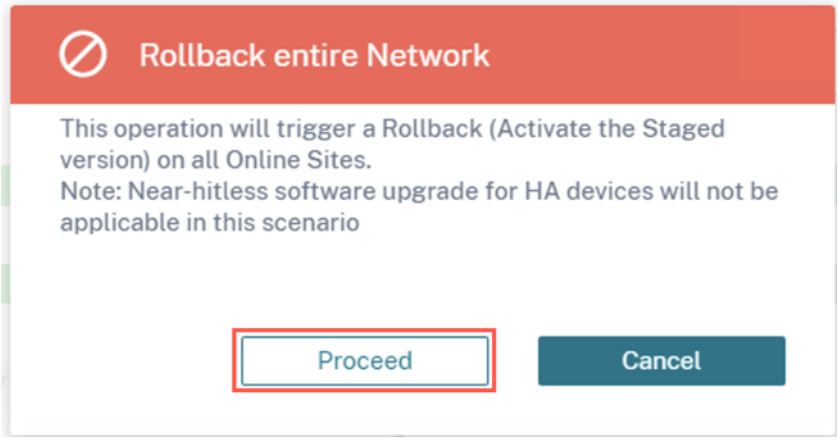
- Netzwerk-Rollback ignorieren:
  - **Für Upgradeszenario ohne Treffer**: Beenden Sie die aktuelle Bereitstellung.
  - **Erster Schritt im Hitless-Upgrade-Szenario**: Die Bereitstellung geht zum zweiten Schritt der Aktivierung über.
  - **Zweiter Schritt im Hitless-Upgrade-Szenario**: Beenden der aktuellen Bereitstellung.
- Rollback des gesamten Netzwerks:
  - **Für ein Upgrade-Szenario ohne Treffer**: Lösen Sie Rollback auf allen Online-Sites im Netzwerk aus.
  - **Erster Schritt im Hitless-Upgrade-Szenario**: Rollback auf allen Online-Standby-Geräten im Netzwerk auslösen.
  - **Zweiter Schritt im Hitless-Upgrade-Szenario**: Rollback auf allen Online-Sites (aktiv und Standby) auslösen. Ein Software-Upgrade ohne Treffer für Geräte mit hoher Verfügbarkeit ist in diesem Szenario nicht anwendbar.

Sie können auf den Hyperlink Mehr **hier klicken klicken**, um die Liste der Websites anzuzeigen, für die ein Rollback ausgeführt oder abgeschlossen wurde, und die oben genannten Aktionen für diese Seite ausführen.

Sie können auch warten, bis die Sites, die das Rollback ausgelöst haben, erfolgreich sind oder fehlschlagen, bevor Sie entscheiden, das netzwerkweite Rollback auszulösen.



Wenn Sie die Option **Gesamtes Netzwerk zurücksetzen** auswählen, wird das folgende Popup-Fenster angezeigt.



> **Hinweis:**
> Das Software-Upgrade ohne Treffer für Hochverfügbarkeits-Appliances ist in diesem Szenario nicht anwendbar. Wenn also Standorte mit hoher Verfügbarkeit im Netzwerk vorhanden sind, werden beim Auslösen eines netzwerkweiten Rollbacks beide Hochverfügbarkeits-Appliances dieses Standorts gleichzeitig aktiviert, was zu Netzwerkausfallzeiten.

Klicken Sie auf **Fortfahren**, um das netzwerkweite Rollback auf allen Online-Sites zu starten.

Anwendungsfall 2: Hitless Upgrade

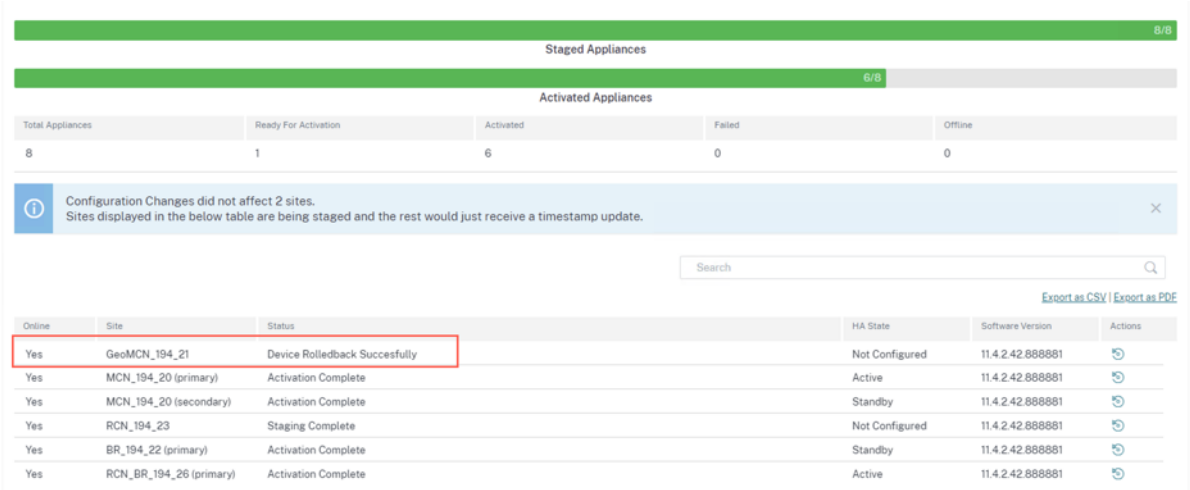
Im Falle eines Hitless-Upgrades würden zuerst die Standby-Appliances aktiviert, gefolgt von den aktiven und nicht hochverfügbaren Appliances. Wenn die Standby-Appliance nach der Aktivierung of-

fline geht und ein Rollback einleitet, stehen im ersten Schritt die folgenden Optionen zur Verfügung:

- **Netzwerk-Rollback**ignorieren: Ignorieren Sie die Standby-Geräte, die offline sind, und fahren Sie mit der Aktivierung der aktiven Appliances fort.
- **Rollback des gesamten Netzwerks**: Rollback aller Online-Standby-Appliances, die die Aktivierung abgeschlossen haben, und beenden Sie die laufende Bereitstellung. In diesem Fall erfolgt keine Aktivierung der aktiven Appliance und Appliance ohne Hochverfügbarkeit.

Im nächsten Schritt des Hitless-Upgrades, bei dem es sich um die Aktivierung einer aktiven Appliance und einer Appliance ohne hohe Verfügbarkeit handelt, wird derselbe Rollback-On-Fehler-Workflow befolgt, wie im obigen Abschnitt für ein Upgrade ohne Treffer beschrieben. Wenn Sie in diesem Szenario **Rollback gesamtes Netzwerk**auswählen, wird das Rollback für alle (sowohl aktiven als auch Standby-Appliances) ausgelöst.

Sobald die Site das Rollback abgeschlossen hat und eine Verbindung zum Citrix SD-WAN Orchestrator Service hergestellt wird, zeigt der Status für diese Site **Geräterollback erfolgreich an** und die Sites sind online.



Einschränkungen

Autokorrektur für Rollback- oder Rollback-Appliances und Netzwerke wird nicht unterstützt.

> **Hinweis**
> Das automatische Site-Rollback ist nur ein Sicherungsmechanismus, um zu versuchen, die verlorene Konnektivität zum Citrix SD-WAN Orchestrator Service wiederherzustellen. Wenn die Appliance immer noch keine Verbindung zum Citrix SD-WAN Orchestrator Service herstellen kann, überprüfen Sie die Netzwerkkonfiguration dieser Appliance.

Sie können die gefilterten Ergebnisse in eine CSV- oder PDF-Datei **exportieren, indem Sie die Optionen Als CSVexportieren und Als PDF**exportieren verwenden. Dem CSV- und PDF-Dateinamen wird

die**Bereitstellungssiteliste** vorangestellt, gefolgt von Datum und Uhrzeit, zu der die Datei exportiert wird.

- **Phase**: Wenn die Überprüfung der Konfiguration erfolgreich war, klicken Sie auf **Stage**, um die Konfigurationsdateien an alle Appliances in Ihrem Netzwerk zu verteilen. Standardmäßig wartet der Citrix SD-WAN Orchestrator Service darauf, dass alle Kontrollknoten (MCN, RCN, Geo MCN, Geo RCN) und die Online-Zweiggeräte bereitgestellt werden, bevor der Benutzer die Aktivierung ermöglicht.

  Wenn der Staging-Prozess an einem beliebigen Standort fehlschlägt, verwenden Sie die Option **Staging wiederholen** in der Spalte **Aktionen**, um den Staging-Prozess erneut zu starten.
- **Aktivieren**: Klicken Sie auf **Aktivieren**, um die bereitgestellte Konfiguration auf allen Sites im Netzwerk zu aktivieren.
- **Unvollständig ignorieren**: Wenn diese Option aktiviert ist, wird das Kontrollkästchen **Aktivieren** erst aktiviert, nachdem alle Online-Kontrollknoten (MCN, RCN, Geo MCN, Geo RCN) bereitgestellt wurden. Sie können die Aktivierung auch dann aktivieren, wenn einige der Online-Branch-Appliances nicht bereitgestellt werden. Die Online-Branch-Appliances, die nicht bereitgestellt werden können, werden ignoriert.
- **Einstellung für partielles Site-Upgrade**: Die Option **Teilweises Site-Upgrade** wird hinzugefügt, um ein Upgrade oder Downgrade der ausgewählten Sites mit einer anderen Version durchzuführen. Die Funktion **Partielles Site-Upgrade** bietet die Möglichkeit, eine neue Version zu testen, bevor sie im gesamten Netzwerk bereitgestellt wird.

Mit der Funktion „ **Partielles Site-Upgrade** “können Upgrades gestaffelt werden, wodurch die Auswirkungen von Software-Upgrades während der Geschäftszeiten verringert werden.

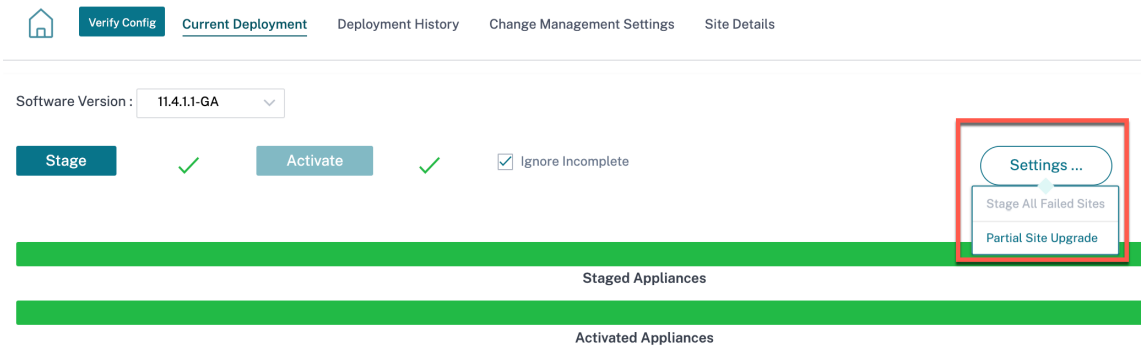
> **Hinweis**
>
> Ein teilweises Site-Upgrade kann nur durchgeführt werden, wenn auf allen Standorten im Netzwerk die Citrix SD-WAN-Softwareversion 11.2.2 oder höher ausgeführt wird.

Alle Konfigurationsänderungen für das **partielle Site-Upgrade** erfordern ein Änderungsmanagement, damit die Änderungen wirksam werden. Das **partielle Site-Upgrade** wählt die niedrigere Version aus und generiert die Konfiguration für dieselbe. Neue Funktionen können nicht getestet werden, während sich das Netzwerk im Modus **Partielles Standort-Upgrade** befindet.

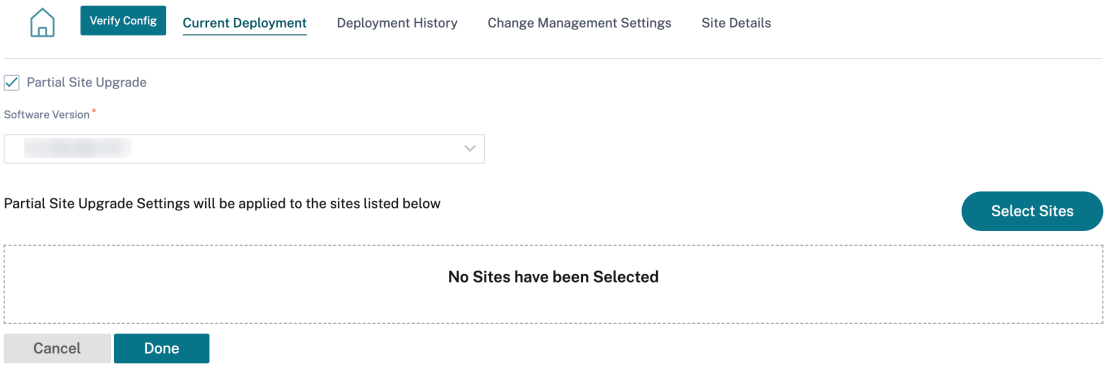
Wenn Sie ein Downgrade von einer neueren auf eine ältere Version mithilfe des **partiellen Standort-Upgrades durchführen**und eine Funktion verwenden, die nur in der neueren Version unterstützt wird (wobei die ähnliche Konfiguration sowohl in der neuen als auch in der älteren Version vorhanden ist), treten Überwachungsfehler auf. Zum Beispiel wird eine neue Plattform ausgewählt, die nur von der neueren Version unterstützt wird. Dies führt zu Auditfehlern.

So führen Sie das teilweise Site-Upgrade durch:

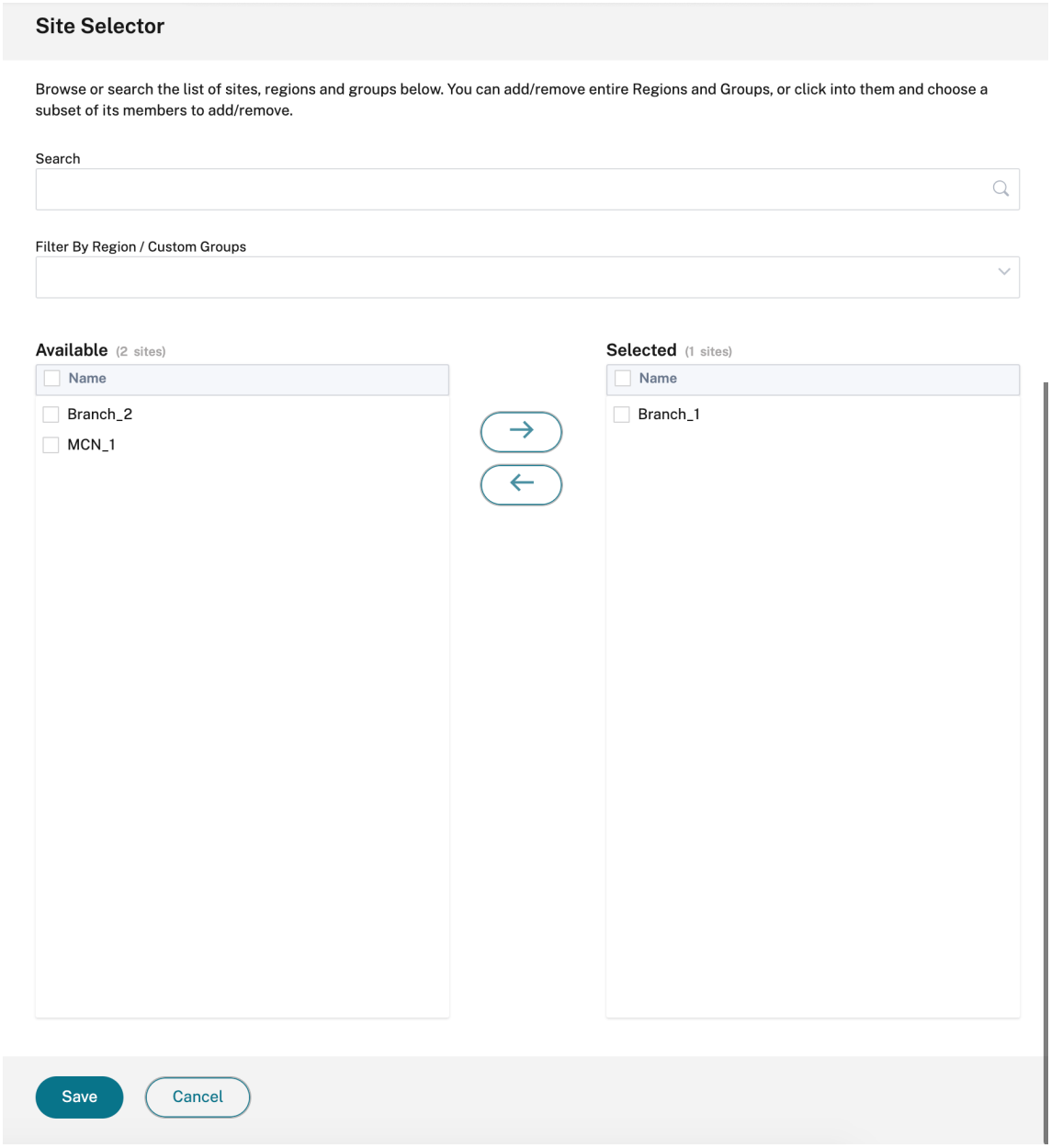
1. Klicken Sie auf die **Einstellung...** und wählen Sie die Option **Teilweises Site-Upgrade** .

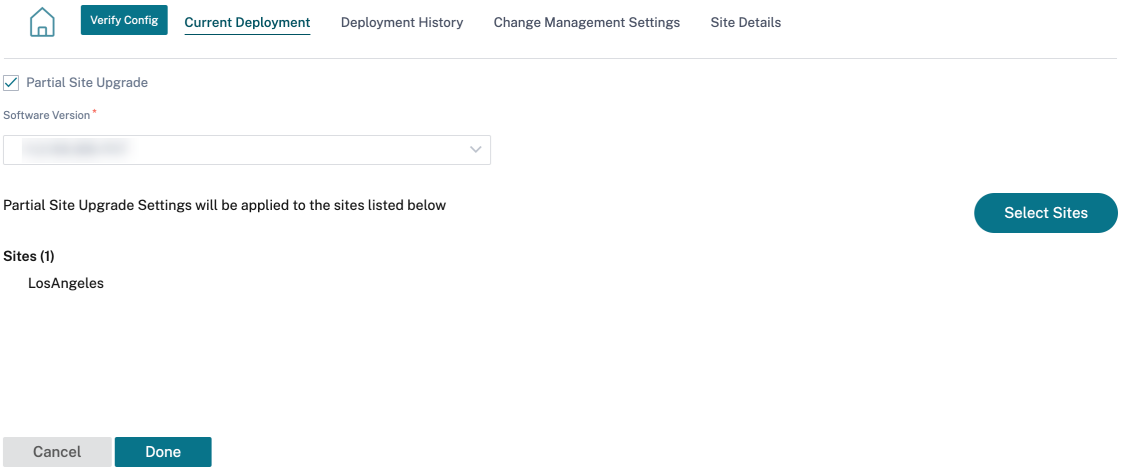


2. Aktivieren Sie das Kontrollkästchen Teilweises Site-Upgrade, wählen Sie die Softwareversion aus und klicken Sie auf **Sites auswählen**, um neue Sites hinzuzufügen.



3. Wählen Sie die Websites und klicken Sie auf **Speichern**.

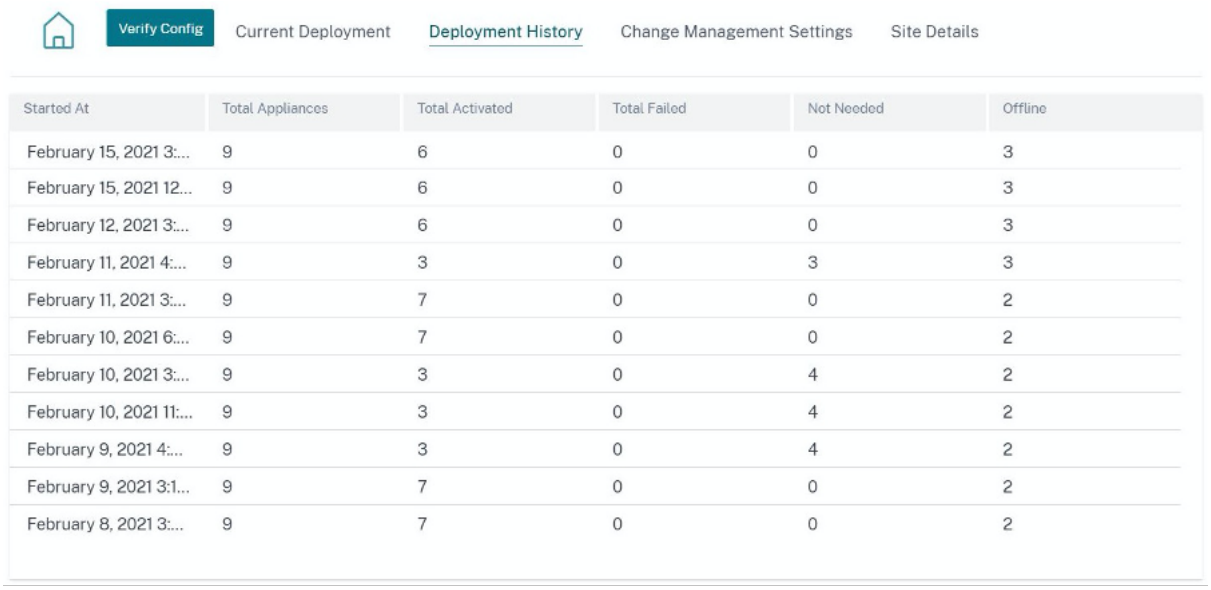




Bei einem reinen Konfigurationsupdate werden nur die Sites bereitgestellt und aktiviert, die Konfigurationsänderungen aufweisen. Für die übrigen Websites wird der Zeitstempel aktualisiert und verarbeitet.

Wenn die Softwareversion geändert wird, werden sowohl die Konfiguration als auch das Softwarepaket an allen Standorten im Netzwerk bereitgestellt und aktiviert.

Im Abschnitt **Bereitstellungsverlauf** können Sie die vorherigen Bereitstellungsvorgänge und Ergebnisse überprüfen.



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

HA nahezu hitless Softwareupgrade

Während des Software-Upgrades (11.0.x und frühere Versionen) werden das Staging und die Aktivierung aller Appliances im Netzwerk gleichzeitig durchgeführt. Dies umfasst das

High Availability (HA) -Paar, das zu Netzwerkausfallzeiten führt. Mit der fast trefferlosen HA-Softwareaktualisierungsfunktion stellt der Citrix SD-WAN Orchestrator Service sicher, dass die Ausfallzeit während des Software-Upgrade-Prozesses (11.1.x und höher) im Laufe der Zeit nicht höher ist als der HA-Switch.

> **Hinweis**
>
> Das HA-Hitless-Softwareupgrade gilt für Folgendes:
>
> - Die Sites, die im Hochverfügbarkeitsmodus (HA) bereitgestellt werden. Sie gilt nicht für Nicht-HA-Sites.
> - Nur dienstbasierte Citrix SD-WAN Orchestrator-Bereitstellungen und nicht für Netzwerke, die über das SD-WAN Center oder MCN verwaltet werden.
> - Nur Softwareupgrade und keine Konfigurationsupdates. Wenn im Rahmen des Upgrades zusammen mit der Software Konfigurationsänderungen vorgenommen werden, führt der Citrix SD-WAN Orchestrator Service kein HA-Near-Hitless-Softwareupgrade durch und setzt das Upgrade auf frühere Weise fort (Upgrade in einem Schritt).

Die Zusammenfassung der Aktualisierungssequenz:

1. Der Citrix SD-WAN Orchestrator Service überprüft den HA-Status aller Appliances im Netzwerk.
2. Rüstet alle sekundären Geräte auf, die sich im **Standby-Zustand** befinden.
3. Die HA-Umschaltung wird ausgelöst und der Status der **Active** - und **Standby-Appliances** wird umgeschaltet.
4. Aktualisert die primären Geräte, die sich jetzt im **Standby-Zustand** befinden.

Das HA-Hitless-Softwareupgrade ist ein zweistufiger Upgrade-Prozess:

Schritt 1: Während des Softwareupgrades führt der Citrix SD-WAN Orchestrator Service nach der Version 11.1 zunächst ein Software-Upgrade für alle Appliances durch, die sich im Netzwerk im **Standby-Zustand** befinden. Das Netzwerk ist immer noch in Betrieb, wenn die **aktiven Appliances** vorhanden sind.

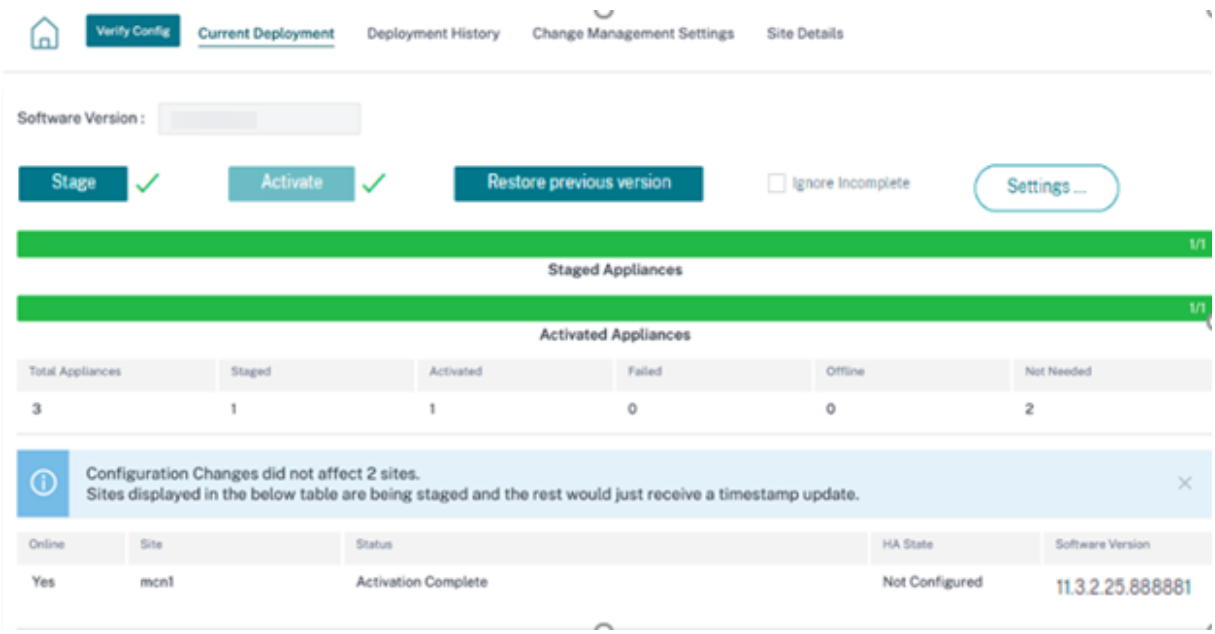
Nachdem alle **Standby-Geräte** auf die neueste Software aktualisiert wurden, wird die HA-Switchover im gesamten Netzwerk ausgelöst. Die **Standby-Geräte** (mit der neuesten Software) werden **aktiv**.

Schritt 2: Die aktuellen **Standby-Geräte** mit einer alten Softwareversion werden auf die neueste Software aktualisiert und laufen weiterhin im **Standby-Modus** .

Während dieses Softwareupgrade-Vorgangs werden auch alle anderen Sites außerhalb von HA mit der neuesten Software aktiviert.

Weitere Informationen finden Sie in den FAQs.

Sie können den Upgrade-Status anzeigen, indem Sie zu **Deployment Tracker** > **Aktuelle Bereitstellung**navigieren.



- **Phase**: Klicken Sie auf **Stage**, um die Konfigurationsdateien an alle Appliances in Ihrem Netzwerk zu verteilen. Standardmäßig wartet der Citrix SD-WAN Orchestrator Service, bis alle Kontrollknoten (MCN, RCN, Geo MCN, Geo RCN) und die Online-Zweiggeräte bereitgestellt werden, bevor der Benutzer die Aktivierung ermöglicht.
- **Aktivieren**: Klicken Sie auf **Aktivieren**, um die bereitgestellte Konfiguration auf allen Sites im Netzwerk zu aktivieren.
- **Vorherige Version wiederherstellen**: Klicken Sie auf **Vorherige Version** wiederherstellen, um zur zuvor aktivierten Konfiguration in Ihrem Netzwerk zurückzukehren. Das fast trefferlose HA-Softwareupgrade ist anwendbar, wenn Sie die vorherige Version wiederherstellen, wenn es sich bei der zuvor aktiven Version nur um eine Änderung der Softwareversion und nicht um eine Konfigurationsänderung handelt. Weitere Informationen zu dieser Funktion finden Sie unter Wiederherstellen der vorherigen Version.
- **Unvollständig ignorieren**: Wenn diese Option aktiviert ist, wird das Kontrollkästchen **Aktivieren** erst aktiviert, nachdem alle Online-Kontrollknoten (MCN, RCN, Geo MCN, Geo RCN) bereitgestellt wurden. Sie können die Aktivierung auch dann aktivieren, wenn einige der Online-Branch-Appliances nicht bereitgestellt werden. Die Online-Branch-Appliances, die nicht bereitgestellt werden können, werden ignoriert.

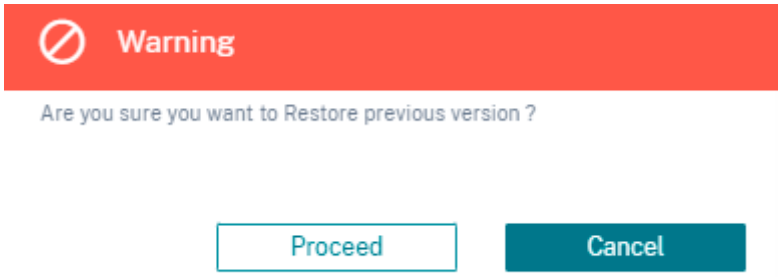
Bei einem reinen Konfigurationsupdate werden nur die Sites bereitgestellt und aktiviert, die Konfigurationsänderungen aufweisen. Für die übrigen Websites wird der Zeitstempel aktualisiert und verarbeitet. In der Spalte **Nicht erforderlich wird** die Anzahl der Sites aufgeführt, für die keine Konfigurationsänderung vorgenommen wurde.

Wenn die Softwareversion geändert wird, werden sowohl die Konfiguration als auch das Softwarepaket an allen Standorten im Netzwerk bereitgestellt und aktiviert.

Vorgängerversion wiederherstellen

In der Funktion zum Wiederherstellen der vorherigen Version initiiert der Citrix SD-WAN Orchestrator Service eine netzwerkweite Aktivierung der vorherigen Konfiguration und stellt die zuvor aktivierte Konfiguration (und/oder Software) in Ihrem Netzwerk wieder her.

Wenn Sie die Option **Vorgängerversion wiederherstellen** auswählen, wird die folgende Bestätigungsmeldung angezeigt:



> **Hinweis:**
>
> Die Aktion „Vorherige Version wiederherstellen“kann ausgeführt werden, wenn sich das Netzwerk nicht im Bereitschaftszustand befindet. Diese Option ist für bereitgestellte Netzwerke deaktiviert.

Autokorrektur für Konfiguration und Softwareupgrade

Im Citrix SD-WAN Orchestrator Service ist die Autokorrekturfunktion im Änderungsmanagement-Workflow implementiert.

Wenn das Staging für eine Site fehlgeschlagen ist und wenn die Site, für die das Staging fehlgeschlagen ist, als Steuerknoten dient, müssen Sie nach der Stagingfehlermeldung neu starten. Die Schaltfläche **Aktivieren** wird nicht aktiviert, wenn das Staging für die Kontrollknoten fehlschlägt. Wenn es sich bei der Site, bei der das Staging fehlgeschlagen ist, um einen Verzweigungsknoten handelt, können Sie die Aktivierung dennoch fortsetzen. Um diese Zweigstelle jedoch mit dem Netzwerk synchron zu machen, führen Sie eine weitere Runde des Änderungsmanagements durch.

> **Hinweis**
>
> - Die Autokorrekturprüfung beginnt erst, nachdem auf die Schaltfläche **Aktivieren** geklickt wurde, und stoppt, sobald die nächste Stufe über die Citrix SD-WAN Orchestrator Service Orchestrator-Dienstbenutzeroberfläche ausgegeben wird.
> - Die Wartungsmodus-Funktion gilt nur für die Autokorrekturfunktion. Wenn Sie ein **Staging**

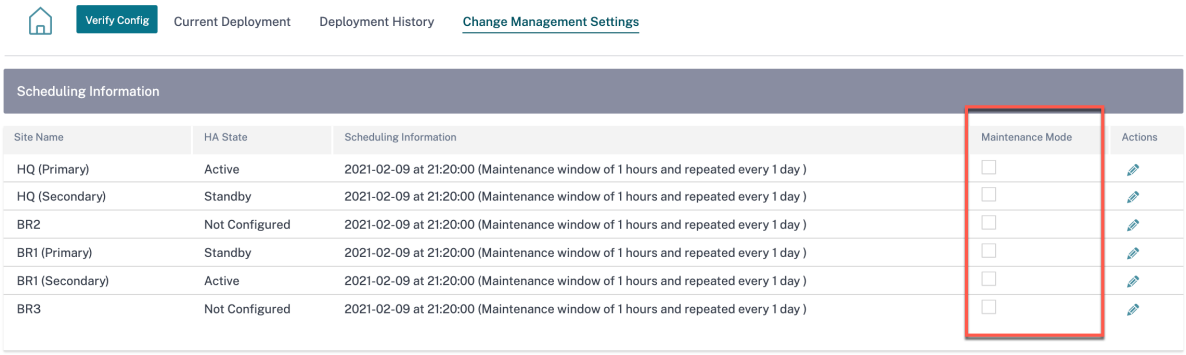
> und eine **Aktivierung**initiieren, wird die Appliance mit aktiviertem Wartungsmodus ebenfalls mit den Software- und Konfigurationsänderungen aktualisiert.

Mit der Verbesserung der automatischen Korrekturfunktion schiebt der automatische Korrekturmechanismus bei einem Staging-Fehler die erwartete Software- und Konfigurationsversion auf den ausgefallenen Zweig und versucht, sie mit dem aktuellen Netzwerk synchron zu gestalten. Die Autokorrekturfunktion ist für Stagingfehler auf dem Zweigknoten und Aktivierungsfehler auf jedem Knoten anwendbar.

Im Folgenden sind die beiden Triggerpunkte aufgeführt, wenn die Autokorrektur beginnt:

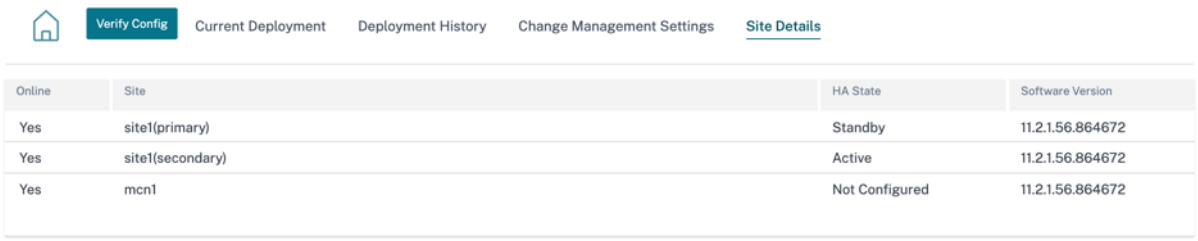
- Sobald Sie in der Benutzeroberfläche des Citrix SD-WAN Orchestrator Service Deployment Tracker die Meldung **Staging Failed** oder **Activation Failed** erhalten, wird die Autokorrektur im Hintergrund ausgeführt. Die Autokorrekturprüfung beginnt, sobald die Aktivierung abgeschlossen ist.
- Im Falle einer Nichtübereinstimmung zwischen Software und Konfiguration, bei der die Appliance nicht die erwartete Software- und Konfigurationsversion bereitgestellt hat, beginnt der Citrix SD-WAN Orchestrator Service, die tatsächlich erforderliche Software und Konfigurationskopie zur Aktivierung auf die Appliance zu übertragen.

Um Fehler bei einer Appliance manuell zu beheben, aktivieren Sie das Kontrollkästchen Wartungsmodus unter den **Änderungsverwaltungseinstellungen**. Dieses Kontrollkästchen wird verwendet, um zu steuern, ob das Gerät auf Autokorrektur überprüft werden muss oder nicht. Sobald das Kontrollkästchen Wartungsmodus deaktiviert ist, synchronisiert die automatische Korrektur die Appliance mit der Netzwerksoftware und der Konfigurationsversion.



Site-Einzelheiten

Die Registerkarte **Site-Details** unter dem Deployment Tracker enthält Informationen zu allen Geräten im Netzwerk. Die Tabelle enthält den Appliance-Namen, die Citrix SD-WAN Orchestrator Service Orchestrator-Dienstkonnektivität, den Hochverfügbarkeitsstatus (HA) und die aktuell ausgeführte Softwareversion.



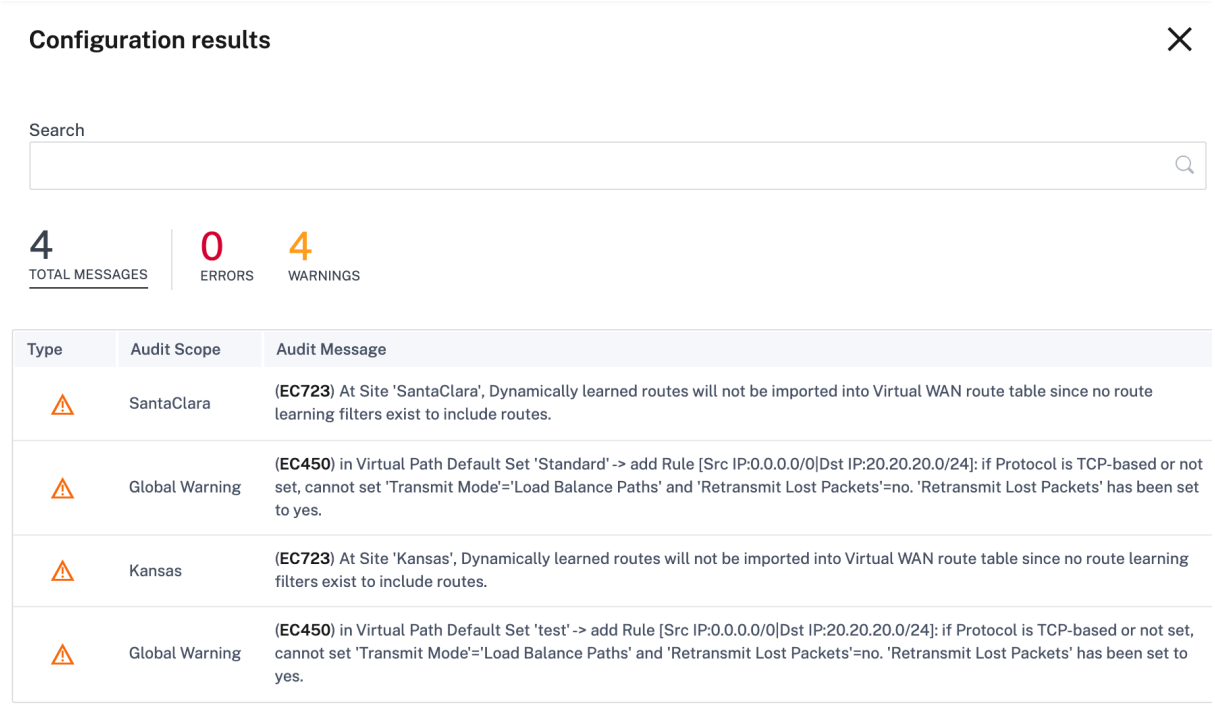
Konfiguration überprüfen

Sie können auf **Konfiguration überprüfen** klicken, um die Netzwerkkonfiguration zu validieren und nach Überwachungsfehlern oder -warnungen zu suchen. Wenn Sie auf **Konfiguration überprüfen**klicken, wird die Seite mit den **Konfigurationsergebnissen** angezeigt. Diese Seite enthält Details zu Auditfehlern und Warnungen.

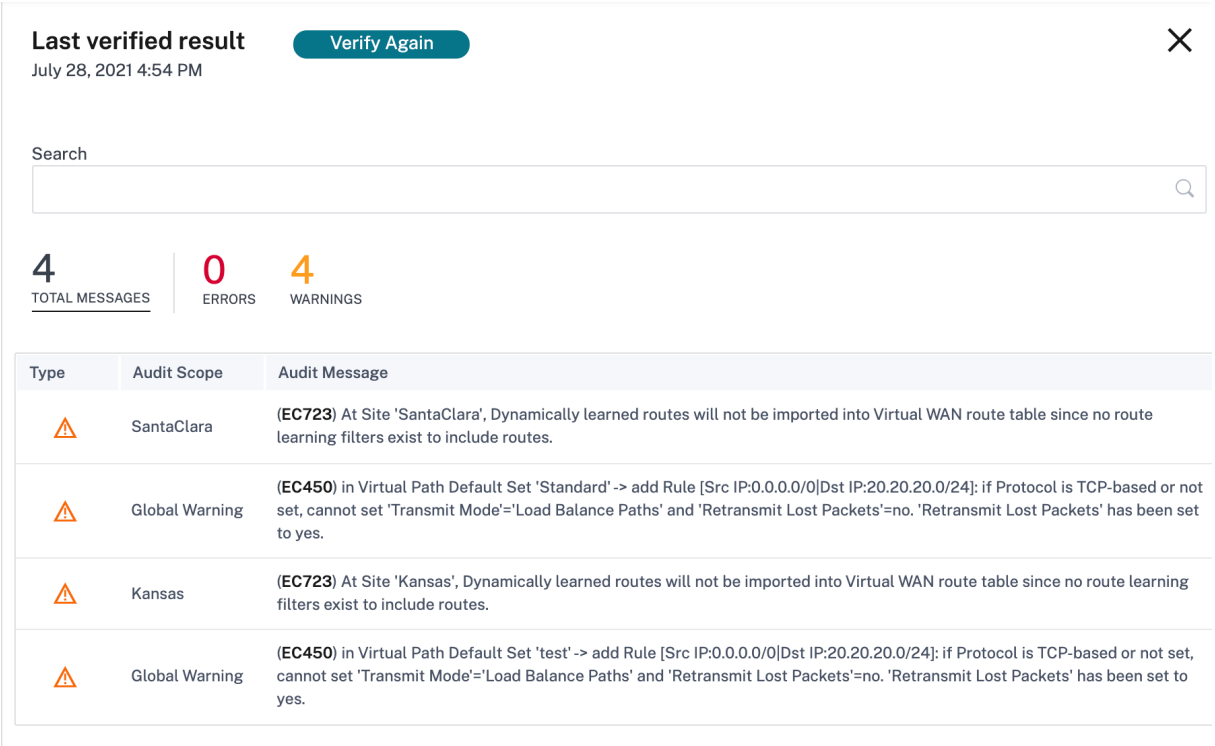
Die Konfigurationsergebnisse zeigen die Gesamtzahl der Auditfehler und Warnungen an. Die Ergebnisse werden auch basierend auf dem Prüftyp (Fehler oder Warnung) gefiltert und mit unterschiedlichen Farbcodes angezeigt. Sie können auf die Zahlen-Links klicken, um die gefilterten Ergebnisse anzuzeigen.

In der Spalte **Typ** wird ein Symbol angezeigt, das angibt, ob es sich um einen Fehler oder eine Warnung handelt. In der Spalte **Prüfungsumfang** wird angegeben, ob der Fehler oder die Warnung für einen Standort oder auf Netzwerkebene gilt. Wenn der Fehler oder die Warnung spezifisch für eine Site ist, wird der Name der Site angezeigt. Wenn sich der Fehler oder die Warnung auf globaler Ebene befindet, wird **Global Error** bzw. **Global Warning** angezeigt. Die Spalte **Prüfmeldung** enthält den Fehlercode und die Fehlermeldung.

Sie können die Suchleiste verwenden, um anhand des Typs, des Fehlercodes, des Site-Namens oder der Fehlermeldung nach bestimmten Fehlern oder Warnungen zu suchen.



Wenn Sie zum zweiten Mal auf **Konfiguration überprüfen** klicken, wird die Seite **Konfigurationsergebnisse** geöffnet, auf der dieselben Ergebnisse angezeigt werden, als die Konfiguration zuletzt überprüft wurde, zusammen mit dem Datums- und Zeitstempel. Falls erforderlich, können Sie auf **Erneut überprüfen** klicken, um die Überprüfung erneut auszuführen.



Service-Definitionen

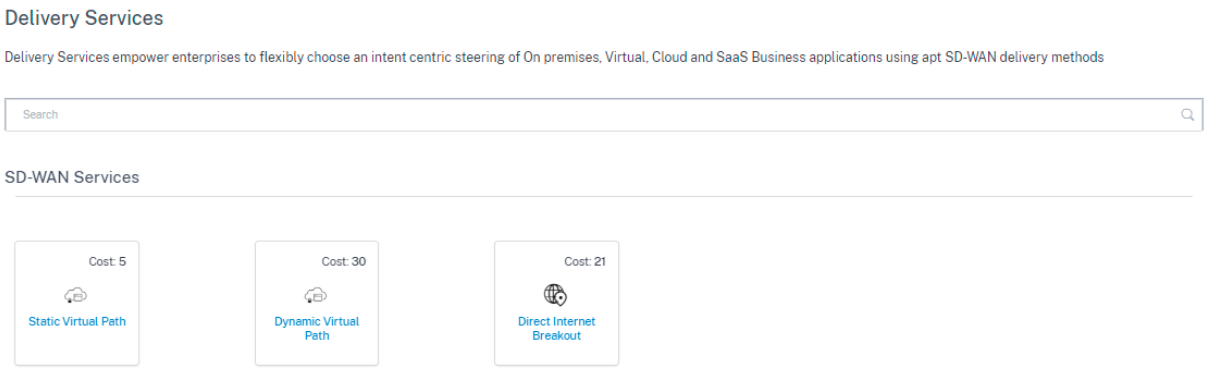
October 21, 2022

Bereitstellungskanäle werden grob in Services-Definitionen und Bandbreitenzuweisung unterteilt.

Delivery Services sind Bereitstellungsmechanismen, die auf Citrix SD-WAN verfügbar sind, um verschiedene Anwendungen oder Verkehrsprofile mithilfe der richtigen Bereitstellungsmethoden basierend auf der Geschäftsabsicht zu steuern. Sie können Bereitstellungsdienste wie Internet, Intranet, virtuelle Pfade, IPSec und LAN GRE konfigurieren. Die Bereitstellungsdienste sind global definiert und werden je nach Bedarf auf WAN-Links an einzelnen Standorten angewendet.

Jede WAN-Verbindung kann alle oder eine Teilmenge der relevanten Dienste anwenden und relative Bandbreitenanteile (%) unter allen Lieferdiensten einrichten.

Der Virtual Path-Dienst ist standardmäßig für alle Links verfügbar. Die anderen Dienste können nach Bedarf hinzugefügt werden.
Um Delivery Services zu konfigurieren, navigieren Sie auf Kundenebene zu **Konfiguration** > **Bereitstellungskanäle** > **Service-Definitionen**.



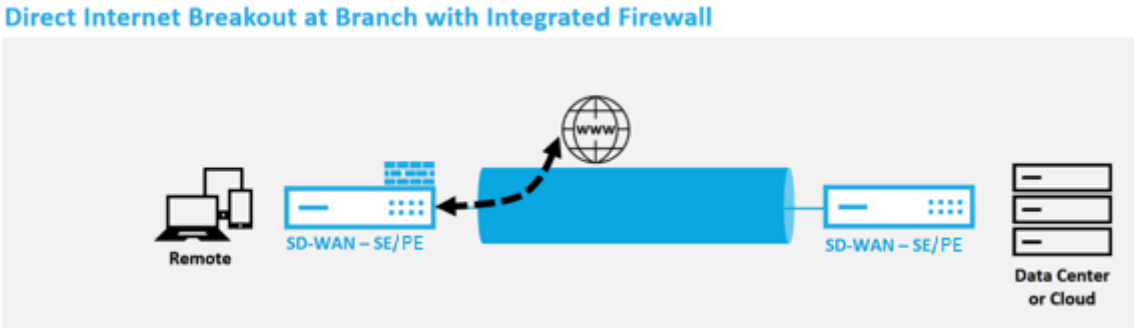
Delivery Services können im Großen und Ganzen wie folgt kategorisiert werden:

- **Virtual Path Service**: Der Dual-Ended-Overlay-SD-WAN-Tunnel, der eine sichere, zuverlässige und qualitativ hochwertige Konnektivität zwischen zwei Standorten bietet, die SD-WAN-Appliances oder virtuelle Instanzen hosten. Legen Sie die mindestens reservierte Bandbreite für jeden virtuellen Pfad in Kbps fest. Diese Einstellung wird auf alle WAN-Verbindungen an allen Standorten im Netzwerk angewendet.
- **Internetdienst**: Direkter Kanal zwischen einer SD-WAN-Site und dem öffentlichen Internet, ohne dass eine SD-WAN-Kapselung erforderlich ist. Citrix SD-WAN unterstützt die Funktion zum Lastenausgleich von Sitzungen für internetgebundenen Datenverkehr über mehrere Internetverbindungen.

- **Intranetdienst**: Unterlegen Sie die link-basierte Konnektivität von einem SD-WAN-Site zu einem beliebigen Nicht-SD-WAN-Site. Der Datenverkehr ist nicht gekapselt oder kann jede nicht-virtuelle Pfadkapselung wie IPSec, GRE verwenden. Sie können mehrere Intranetdienste einrichten.

Internet Service

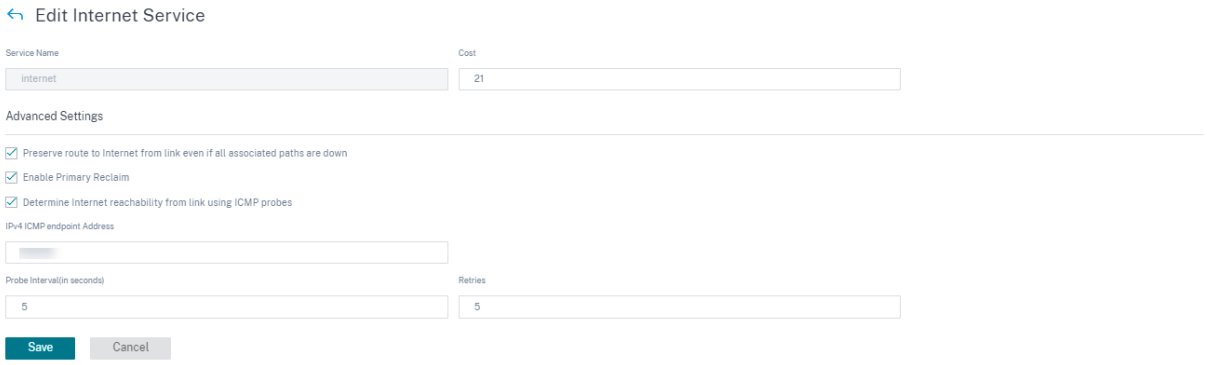
Internet Service ist standardmäßig als Teil der Lieferservices verfügbar. Um einen Internetdienst zu konfigurieren, navigieren Sie auf Kundenebene zu **Konfiguration** > **Bereitstellungskanäle** > **Dienstdefinitionen**. Wählen Sie im Abschnitt **SD-WAN-Dienste** die Kachel **Direct Internet Breakout** aus und klicken Sie dann auf **Hinzufügen**.



Sie können die folgenden Internetdienste konfigurieren:

- **Route zum Internet vom Link beibehalten, auch wenn alle zugehörigen Pfade ausgefallen sind**: Sie können die Routenkosten für Internetdienste im Verhältnis zu anderen Bereitstellungsdiensten konfigurieren. Mit diesem Dienst können Sie die Route über den Link zum Internet beibehalten, auch wenn alle zugehörigen Pfade ausgefallen sind. Wenn alle mit einer WAN-Verbindung verknüpften Pfade tot sind, verwendet die SD-WAN-Appliance diese Route zum Senden/Empfangen von Internetverkehr.
- **Ermitteln der Internet-Erreichbarkeit über eine Verbindung mithilfe von ICMP-Prüfpunkten**: Sie können ICMP-Prüfungen für bestimmte Internet-WAN-Verbindungen zu einem expliziten Server im Internet aktivieren. Mit der ICMP-Testeinstellung behandelt die SD-WAN-Appliance die Internetverbindung als aktiv, wenn entweder die Mitgliedspfade der Verbindung aktiv sind oder wenn die ICMP-Testantwort vom Server empfangen wird.
- **IPv4-ICMP-Endpunktadresse**: Die IPv4-Zieladresse oder die Serveradresse.

- **Prüfintervall (in Sekunden)**: Zeitintervall, in dem die SD-WAN-Appliance Tests über die im Internet konfigurierten WAN-Verbindungen sendet. Standardmäßig sendet die SD-WAN-Appliance alle 5 Sekunden Tests auf den konfigurierten WAN-Verbindungen.
- **Wiederholungsversuche**: Anzahl der Wiederholungsversuche, die Sie versuchen können, bevor Sie feststellen, ob die WAN-Verbindung aktiv ist oder nicht. Nach 3 aufeinanderfolgenden Sondenfehlern wird die WAN-Verbindung als tot betrachtet. Maximal zulässige Wiederholungsversuche sind 10.



Unterstützte Bereitstellungsmodi

Der Internetdienst kann in den folgenden Bereitstellungsmodi verwendet werden:

- Inline-Bereitstellungsmodus (SD-WAN-Overlay)

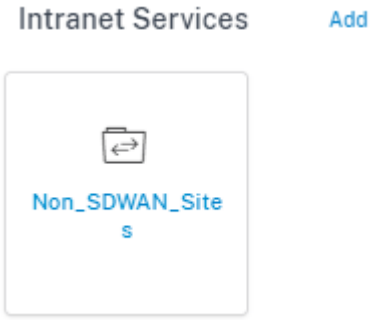
Citrix SD-WAN kann als Overlay-Lösung in jedem Netzwerk bereitgestellt werden. Als Overlay-Lösung wird SD-WAN im Allgemeinen hinter vorhandenen Edge-Routern und/oder Firewalls eingesetzt. Wenn SD-WAN hinter einer Netzwerk-Firewall bereitgestellt wird, kann die Schnittstelle als vertrauenswürdig konfiguriert werden und der Internetverkehr kann als Internet-Gateway an die Firewall übermittelt werden.

- Edge- oder Gateway Modus

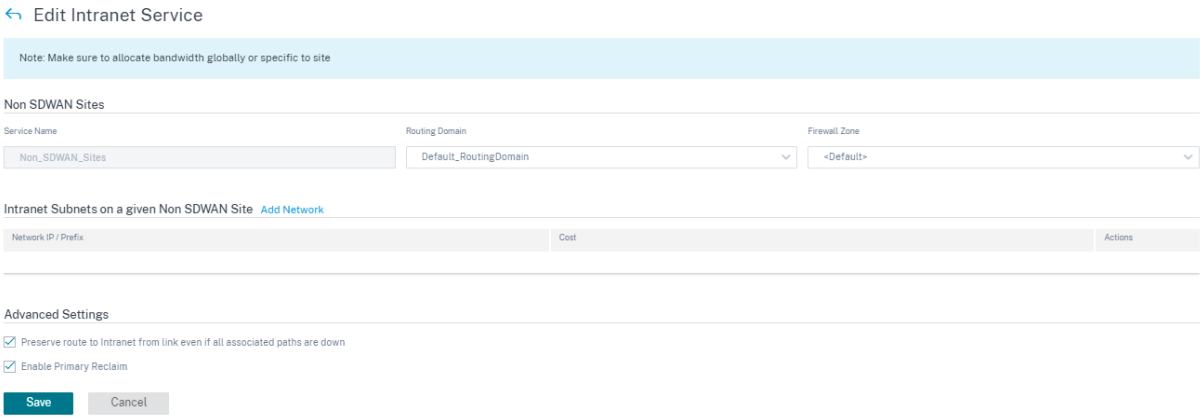
Citrix SD-WAN kann als Edge-Gerät bereitgestellt werden und ersetzt vorhandene Edge-Router- und/oder Firewall-Geräte. Die integrierte Firewall-Funktion ermöglicht es SD-WAN, das Netzwerk vor direkter Internetverbindung zu schützen. In diesem Modus wird die Schnittstelle, die mit der öffentlichen Internetverbindung verbunden ist, als nicht vertrauenswürdig konfiguriert, wodurch die Verschlüsselung aktiviert wird, und Firewall- und Dynamische NAT-Funktionen sind aktiviert, um das Netzwerk zu schützen.

Intranet-Service

Sie können mehrere Intranetdienste erstellen. Um einen Intranet-Service hinzuzufügen, navigieren Sie auf Kundenebene zu **Konfiguration** > **Bereitstellungskanäle** > **Dienstdefinitionen**. Klicken Sie im Abschnitt **Intranetdienste** auf **Hinzufügen**.



Sobald der Intranetdienst auf globaler Ebene erstellt wurde, können Sie ihn auf WAN-Link-Ebene referenzieren. Geben Sie einen **Dienstnamen**an, wählen Sie die gewünschte **Routingdomäne** und **Firewallzone**aus Fügen Sie alle Intranet-IP-Adressen im Netzwerk hinzu, damit andere Standorte im Netzwerk interagieren könnten. Sie können die Route zum Intranet auch von der Verbindung aus beibehalten, selbst wenn alle zugehörigen Pfade ausgefallen sind.

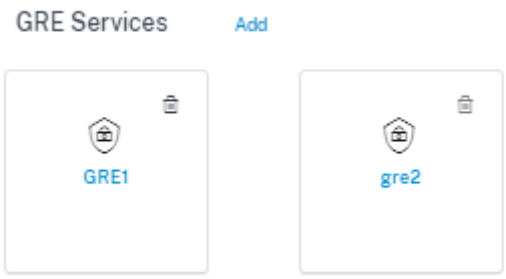


GRE Service

Sie können SD-WAN-Appliances so konfigurieren, dass GRE-Tunnel im LAN beendet werden.

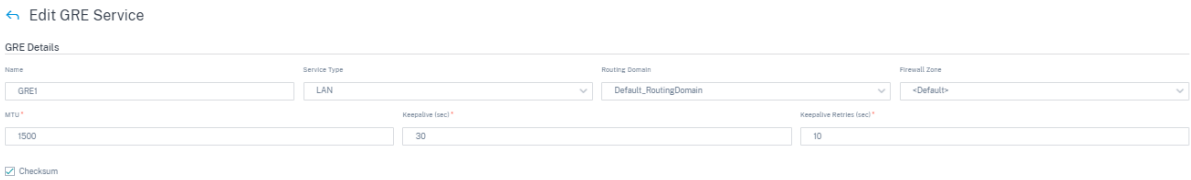
Um einen GRE-Service hinzuzufügen, navigieren Sie auf Kundenebene zu **Konfiguration** > **Bereitstellungskanäle** > **Dienstdefinitionen**. Sie können auch unter Konfiguration **> Sicherheit zur Konfigurationsseite für**GRE-Dienste**navigieren.

Navigieren Sie im Abschnitt **IPSec & GRE** zu **IPSec-Dienste** und klicken Sie auf **Hinzufügen**.



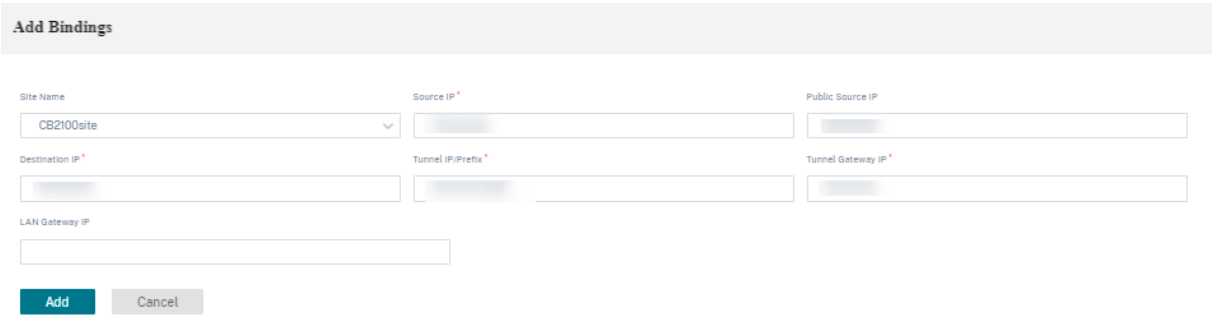
GRE-Details:

- **Diensttyp**: Wählen Sie den Dienst aus, den der GRE-Tunnel verwendet.
- **Name**: Name des LAN GRE-Dienstes.
- **Routingdomäne**: Die Routingdomäne für den GRE-Tunnel.
- **Firewall-Zone**: Die für den Tunnel gewählte Firewall-Zone. Standardmäßig wird der Tunnel in die default_LAN_Zone platziert.
- **MTU**: Maximale Übertragungseinheit —die Größe des größten IP-Datagramms, das über eine bestimmte Verbindung übertragen werden kann. Der Bereich reicht von 576 bis 1500. Der Standardwert ist 1500.
- **Bleib am Leben**: Der Zeitraum zwischen dem Senden von Keep-Alive-Nachrichten. Bei der Konfiguration auf 0 werden keine Keep Alive-Pakete gesendet, der Tunnel bleibt jedoch weiter oben.
- **Keep alive Wiederholungen**: Die Häufigkeit, mit der die Citrix SD-WAN Appliance Keepalive-Pakete ohne Antwort sendet, bevor der Tunnel heruntergefahren wird.
- **Prüfsumme**: Aktiviert oder deaktiviert Checksum für den GRE-Header des Tunnels.



Site-Bindungen:

- **Site Name**: Der Standort, an dem der GRE Tunnel zugeordnet werden soll.
- **Quell-IP**: Die Quell-IP-Adresse des Tunnels. Dies ist eine der virtuellen Schnittstellen, die an dieser Site konfiguriert sind. Die ausgewählte Routingdomäne bestimmt die verfügbaren Quell-IP-Adressen.
- **Public Source IP**: Die Quell-IP, wenn der Tunnelverkehr über NAT verläuft.
- **Ziel-IP**: Die Ziel-IP-Adresse des Tunnels.
- **Tunnel-IP/Präfix**: Die IP-Adresse und das Präfix des GRE-Tunnels.
- **Tunnel-Gateway-IP**: Die IP-Adresse des nächsten Hops, um den Tunnelverkehr weiterzuleiten
- **LAN Gateway-IP**: Die IP-Adresse des nächsten Hops, um den LAN-Verkehr weiterzuleiten.



IPsec-Dienst

Citrix SD-WAN-Appliances können feste IPSec-Tunnel mit Peers von Drittanbietern auf LAN- oder WAN-Seite aushandeln. Sie können die Tunnelendpunkte definieren und die Standorte den Tunnelendpunkten zuordnen.

Sie können auch ein IPsec-Sicherheitsprofil auswählen und anwenden, das das Sicherheitsprotokoll und die IPsec-Einstellungen definiert.

So konfigurieren Sie IPsec-Einstellungen für virtuelle Pfade:

- Aktivieren Sie Virtual Path IPsec-Tunnel für alle virtuellen Pfade, bei denen FIPS-Konformität erforderlich ist.
- Konfigurieren Sie die Nachrichtenauthentifizierung, indem Sie den IPsec-Modus in AH oder ESP+Auth ändern und eine FIPS-zugelassene Hashing-Funktion verwenden. SHA1 wird von FIPS akzeptiert, aber SHA256 wird dringend empfohlen.
- Die IPsec-Lebensdauer sollte nicht länger als 8 Stunden (28.800 Sekunden) konfiguriert werden.

Citrix SD-WAN verwendet IKE Version 2 mit Pre-Shared-Keys, um IPSec-Tunnel über den virtuellen Pfad mit den folgenden Einstellungen auszuhandeln:

- DH Gruppe 19: ECP256 (256-Bit Elliptische Kurve) für Schlüsselaushandlung
- 256-Bit-AES-CBC-Verschlüsselung
- SHA256-Hashing für die Nachrichtenauthentifizierung
- SHA256-Hashing für Nachrichtenintegrität
- DH Gruppe 2: MODP-1024 für perfekte Vorwärtsgeheimnis

So konfigurieren Sie IPSec-Tunnel für einen Drittanbieter:

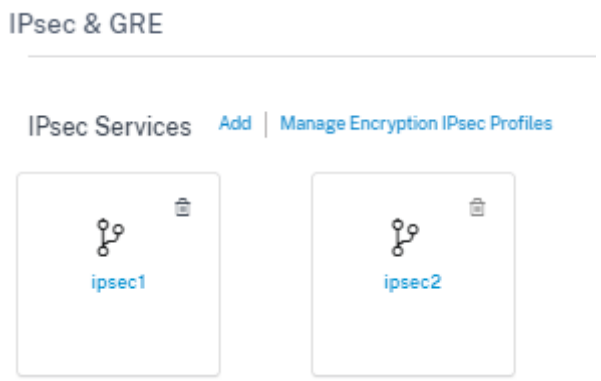
- Konfigurieren Sie die FIPS-genehmigte DH-Gruppe Die Gruppen 2 und 5 sind unter FIPS zulässig, jedoch werden Gruppen 14 und höher dringend empfohlen.
- Konfigurieren Sie die FIPS-genehmigte Hash-Funktion. SHA1 wird von FIPS akzeptiert, jedoch wird SHA256 dringend empfohlen.

- Konfigurieren Sie bei Verwendung von IKEv2 eine FIPS-zugelassene Integritätsfunktion. SHA1 wird von FIPS akzeptiert, jedoch wird SHA256 dringend empfohlen.
- Konfigurieren Sie eine IKE-Lebensdauer und maximale Lebensdauer von nicht mehr als 24 Stunden (86.400 Sekunden).
- Konfigurieren Sie die IPsec-Nachrichtenauthentifizierung, indem Sie den IPsec-Modus in AH oder ESP+Auth ändern und eine FIPS-zugelassene Hashing-Funktion verwenden. SHA1 wird von FIPS akzeptiert, aber SHA256 wird dringend empfohlen.
- Konfigurieren Sie eine IPsec-Lebensdauer und eine maximale Lebensdauer von nicht mehr als acht Stunden (28.800 Sekunden).

Einen IPSec-Tunnel konfigurieren

Navigieren Sie auf Kundenebene zu **Konfiguration** > **Bereitstellungskanäle** > **Servicedefinitionen**. Sie können auch unter **Konfiguration > Sicherheit** zur Seite **IPSec-Dienste**navigieren.

Klicken Sie im Abschnitt **IPSec & GRE** > **IPSec-Dienste** auf **Hinzufügen**. Die Seite **IPSec-Dienst bearbeiten** wird angezeigt.



1. Geben Sie die Dienstdetails an.

   - **Dienstname**: Der Name des IPsec-Diensts.
   - **Diensttyp**: Wählen Sie den Dienst aus, den der IPSec-Tunnel verwendet.
   - **Routingdomäne**: Wählen Sie für IPsec-Tunnel über LAN eine Routingdomäne aus. Wenn der IPSec-Tunnel einen Intranetdienst verwendet, bestimmt der Intranetdienst die Routingdomäne.
   - **Firewall-Zone**: Die Firewall-Zone für den Tunnel. Standardmäßig wird der Tunnel in die default_LAN_Zone platziert.
   - **ECMP aktivieren**: Wenn das Kontrollkästchen **ECMP aktivieren** aktiviert ist, ist der ECMP-Lastenausgleich für den IPSec-Tunnel aktiviert.
   - **ECMP-Typ**: Wählen Sie den Typ des ECMP-Lastausgleichsmechanismus nach Bedarf aus. Weitere Informationen zu ECMP-Typen finden Sie unter ECMP-Lastenausgleich.

2. Fügen Sie den Tunnelendpunkt hinzu.

    - **Name**: Wenn **Diensttyp** Intranet ist, wählen Sie einen Intranetdienst aus, den der Tunnel schützt. Andernfalls geben Sie einen Namen für den Dienst ein.
    - **Peer-IP**: Die IP-Adresse des Remote-Peers.
    - **IPSec-Profil**: IPSec-Sicherheitsprofil, das das Sicherheitsprotokoll und die IPSec-Einstellungen definiert.
    - **Pre Shared Key**: Der für die IKE-Authentifizierung verwendete vorinstallierte Schlüssel.
    - **Peer Pre Shared Key**: Der vorgefertigte Schlüssel, der für die IKEv2-Authentifizierung verwendet wird.
    - **Identitätsdaten**: Die Daten, die bei Verwendung der manuellen Identität oder des Benutzer-FQDN-Typs als lokale Identität verwendet werden sollen.
    - **Peer-Identitätsdaten**: Die Daten, die als Peer-Identität verwendet werden sollen, wenn eine manuelle Identität oder ein Benutzer-FQDN-Typ verwendet wird.
    - **Zertifikat**: Wenn Sie Certificate als IKE-Authentifizierung wählen, wählen Sie aus den konfigurierten Zertifikaten.

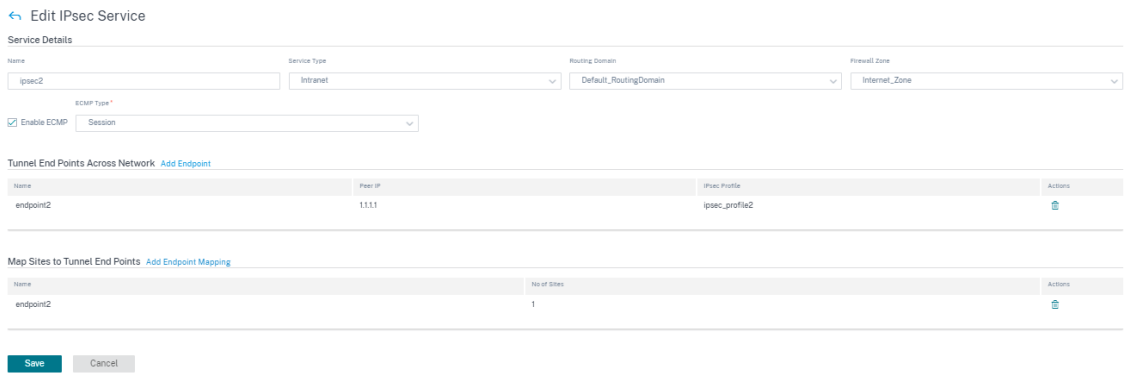
3. Ordnen Sie Standorte den Endpunkten des Tunnels zu.

    - **Endpunkt wählen**: Der Endpunkt, der einer Site zugeordnet werden soll.
    - **Site-Name**: Die Site, die dem Endpunkt zugeordnet werden soll.
    - **Name der virtuellen Schnittstelle**: Die virtuelle Schnittstelle am Standort, die als Endpunkt verwendet werden soll.
    - **Lokale IP**: Die lokale virtuelle IP-Adresse, die als lokaler Tunnelendpunkt verwendet werden soll.
    - **Gateway-IP**: Die IP-Adresse des nächsten Hops.

4. Erstellen Sie das geschützte Netzwerk.

    - **Quellnetzwerk-IP/-Präfix**: Die Quell-IP-Adresse und das Präfix des Netzwerkverkehrs, den der IPsec-Tunnel schützt.
    - **Zielnetzwerk-IP/-Präfix**: Die Ziel-IP-Adresse und das Präfix des Netzwerkverkehrs, den der IPsec-Tunnel schützt.

5. Stellen Sie sicher, dass die IPsec-Konfigurationen auf der Peer-Appliance gespiegelt werden.



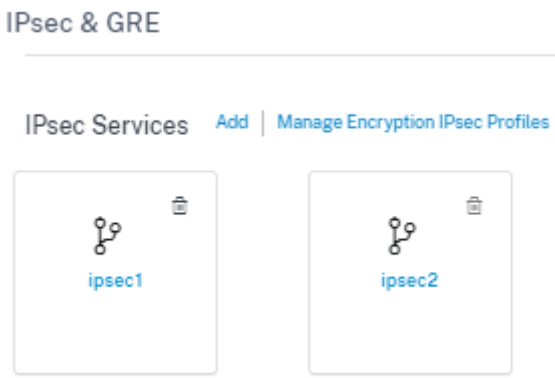
Weitere Informationen zur FIPS-Konformität finden Sie unter Netzwerksicherheit.

> **Hinweis**
>
> Citrix SD-WAN Orchestrator for On-premises unterstützt die Konnektivität zur Oracle Cloud Infrastructure (OCI) über IPSec.

IPSec-Verschlüsselungsprofile

Um ein IPSec-Verschlüsselungsprofil hinzuzufügen, navigieren Sie auf Kundenebene zu **Konfiguration** > **Bereitstellungskanäle** > **Dienstdefinitionen**. Sie können auch unter Konfiguration **> Sicherheit zur Konfigurationsseite für**IPSec-Verschlüsselungsprofile**navigieren.

Wählen Sie im Abschnitt **IPSec & GRE** die Option **Verschlüsselungs-IPSec-Profile verwalten**.



IPsec bietet sichere Tunnel. Citrix SD-WAN unterstützt virtuelle IPsec-Pfade, sodass Geräte von Drittanbietern IPsec-VPN-Tunnel auf LAN- oder WAN-Seite einer Citrix SD-WAN-Appliance beenden können. Sie können Standort-zu-Standort-IPSec-Tunnel sichern, die auf einer SD-WAN-Appliance beendet werden, indem Sie eine 140-2 Level 1 FIPS-zertifizierte kryptografische IPSec-Binärdatei verwenden.

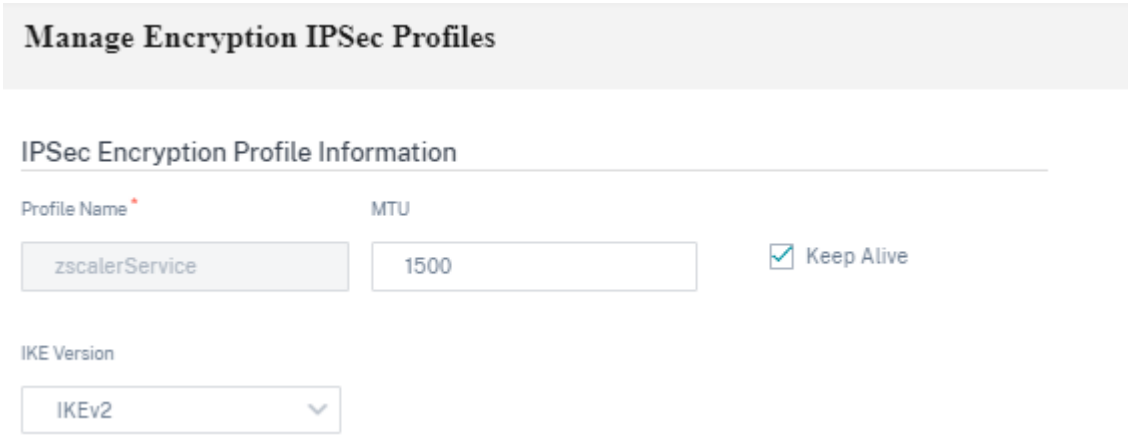
Citrix SD-WAN unterstützt auch das robuste IPsec-Tunneling mithilfe eines differenzierten virtuellen Pfadtunneling-Mechanismus.

IPsec-Profile werden beim Konfigurieren von IPsec-Diensten als Bereitstellungsdienstsätze verwendet. Geben Sie auf der Seite IPSec-Sicherheitsprofil die erforderlichen Werte für die folgenden **IPSec-Verschlüsselungsprofile, IKE-Einstellungen** und **IPSec-Einstellungen**ein.

Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen.

Informationen zum IPSec-Verschlüsselungsprofil:

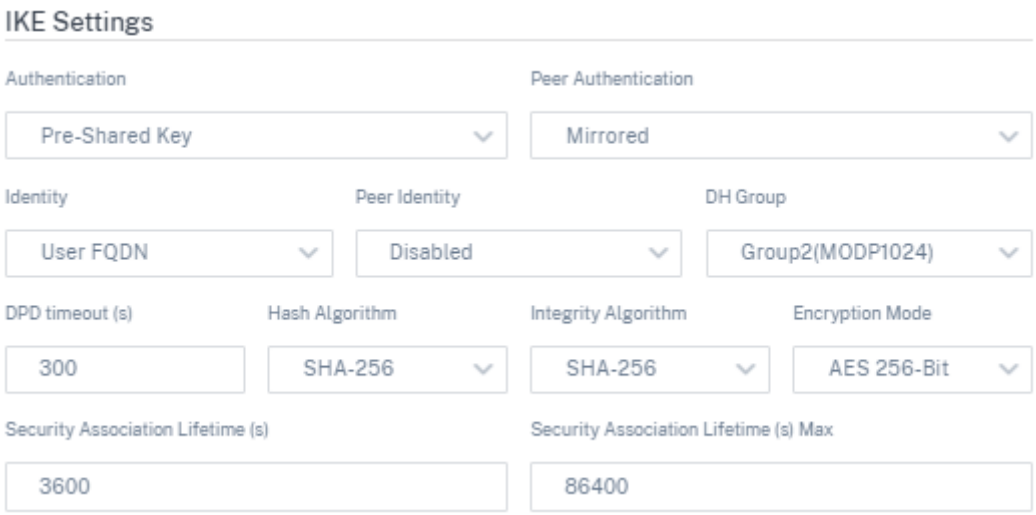
- **Profilname**: Geben Sie einen Profilnamen an.
- **MTU**: Geben Sie die maximale IKE- oder IPSec-Paketgröße in Byte ein.
- **Keep Alive**: Aktivieren Sie das Kontrollkästchen, um den Tunnel aktiv zu halten und die Routenberechtigung zu aktivieren.
- **IKE-Version**: Wählen Sie eine IKE-Protokollversion aus der Dropdownliste.



IKE-Einstellungen

- **Modus**: Wählen Sie entweder Hauptmodus oder Aggressiver Modus aus der Dropdown-Liste für den IKE-Phase-1-Verhandlungsmodus aus.
  - **Main**: Während der Verhandlung werden keine Informationen potenziellen Angreifern ausgesetzt, sind aber langsamer als der aggressive Modus. **Der Hauptmodus** ist FIPS-konform.
  - **Aggressiv**: Einige Informationen (z. B. die Identität der Verhandlungskollegen) werden während der Verhandlung potenziellen Angreifern ausgesetzt, sind aber schneller als der Hauptmodus. Der**aggressive** Modus ist nicht FIPS-konform.
- **Authentifizierung**: Wählen Sie im Dropdownmenü den Authentifizierungstyp Zertifikat oder Pre-Shared Key aus.
- **Peer-Authentifizierung**: Wählen Sie den Peer-Authentifizierungstyp aus der Dropdownliste.
- **Identität**: Wählen Sie die Identitätsmethode aus der Dropdownliste aus.

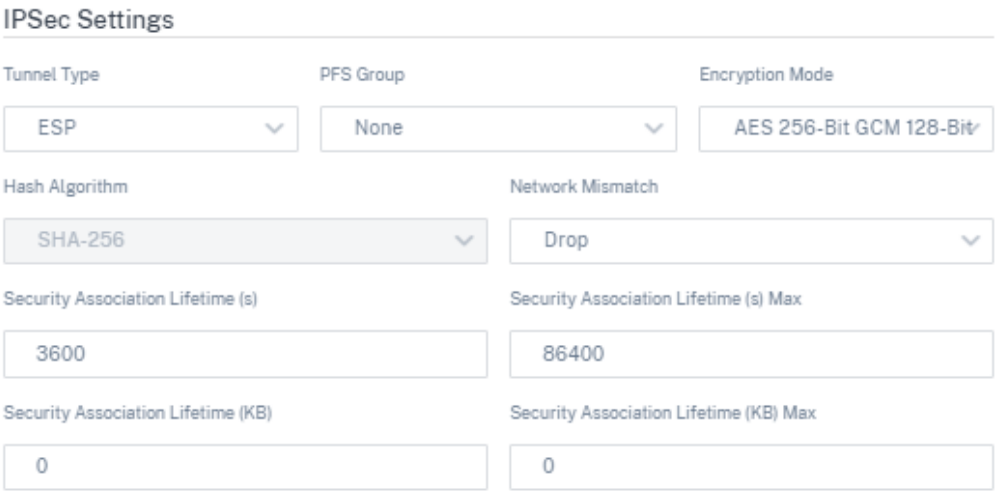
- **Peer-Identität**: Wählen Sie die Peer-Identity-Methode aus der Dropdownliste aus.
- **DH-Gruppe**: Wählen Sie die Diffie-Hellman (DH) -Gruppe aus, die für die IKE-Schlüsselgenerierung verfügbar ist.
- **DPD-Timeout (s)**: Geben Sie den Dead Peer Detection Timeout (in Sekunden) für VPN-Verbindungen ein.
- **Hash-Algorithmus**: Wählen Sie einen Hashing-Algorithmus aus der Dropdown-Liste aus, um IKE-Nachrichten zu authentifizieren.
- **Integritätsalgorithmus**: Wählen Sie den IKEv2-Hashing-Algorithmus, der für die HMAC-Überprüfung verwendet werden soll
- **Verschlüsselungsmodus**: Wählen Sie den Verschlüsselungsmodus für IKE-Nachrichten aus der Dropdownliste.
- **Lebenszeit (en) der Sicherheitszuordnung**: Geben Sie die Zeitspanne in Sekunden ein, die eine IKE-Sicherheitszuordnung bestehen soll.
- **Max. Lebensdauer (en) der Sicherheitszuordnung**: Geben Sie die maximale Zeit in Sekunden ein, die das Bestehen einer IKE-Sicherheitszuordnung zulassen soll.



IPsec-Einstellungen

- **Tunneltyp**: Wählen Sie **ESP**, **ESP+Auth**, **ESP+NULL**oder **AH** als Tunnelkapselungstyp aus der Dropdown-Liste. Diese sind unter FIPS-konformen und nicht FIPS-konformen Kategorien zusammengefasst.
  - **ESP**: Verschlüsselt nur die Benutzerdaten
  - **ESP+Auth**: Verschlüsselt die Benutzerdaten und beinhaltet einen HMAC
  - **ESP+NULL**: Pakete werden authentifiziert, aber nicht verschlüsselt
  - **AH**: Beinhaltet nur einen HMAC

- **PFS-Gruppe**: Wählen Sie im Dropdown-Menü die Diffie-Hellman-Gruppe aus, die für die Generierung von Perfect Forward Secrecy-Schlüsseln verwendet werden soll
- **Verschlüsselungsmodus**: Wählen Sie im Dropdownmenü den Verschlüsselungsmodus für IPSec-Nachrichten aus.
- **Hash-Algorithmus**: Die Hash-Algorithmen MD5, SHA1 und SHA-256 sind für die HMAC-Überprüfung verfügbar.
- **Netzwerkkonflikt**: Wählen Sie aus dem Dropdown-Menü eine Aktion aus, die ausgeführt werden soll, wenn ein Paket nicht mit den geschützten Netzwerken des IPSec-Tunnels übereinstimmt.
- **Lebensdauer (en) der Sicherheitszuordnung**: Geben Sie den Zeitraum (in Sekunden) ein, für den eine IPSec-Sicherheitszuordnung bestehen soll.
- **Max. Lebensdauer (en) der Sicherheitszuordnung**: Geben Sie die maximale Zeitspanne (in Sekunden) ein, die das Bestehen einer IPSec-Sicherheitszuordnung zulassen soll.
- **Lebensdauer der Sicherheitszuordnung (KB)**: Geben Sie die Datenmenge (in Kilobyte) ein, die eine IPSec-Sicherheitszuordnung bestehen soll.
- **Max. Lebensdauer der Sicherheitszuordnung (KB)**: Geben Sie die maximale Datenmenge (in Kilobyte) ein, die das Vorhandensein einer IPSec-Sicherheitszuordnung zulassen soll.

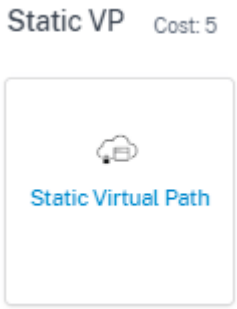


Statischer virtueller Pfad

Die Einstellungen für den virtuellen Pfad werden von den globalen Einstellungen für den automatischen WAN-Linkpfad übernommen. Sie können diese Konfigurationen überschreiben und den Mitgliedspfad hinzufügen oder entfernen. Sie können die virtuellen Pfade auch basierend auf der Site und dem angewendeten QoS-Profil filtern. Geben Sie eine Tracking-IP-Adresse für den WAN-Link

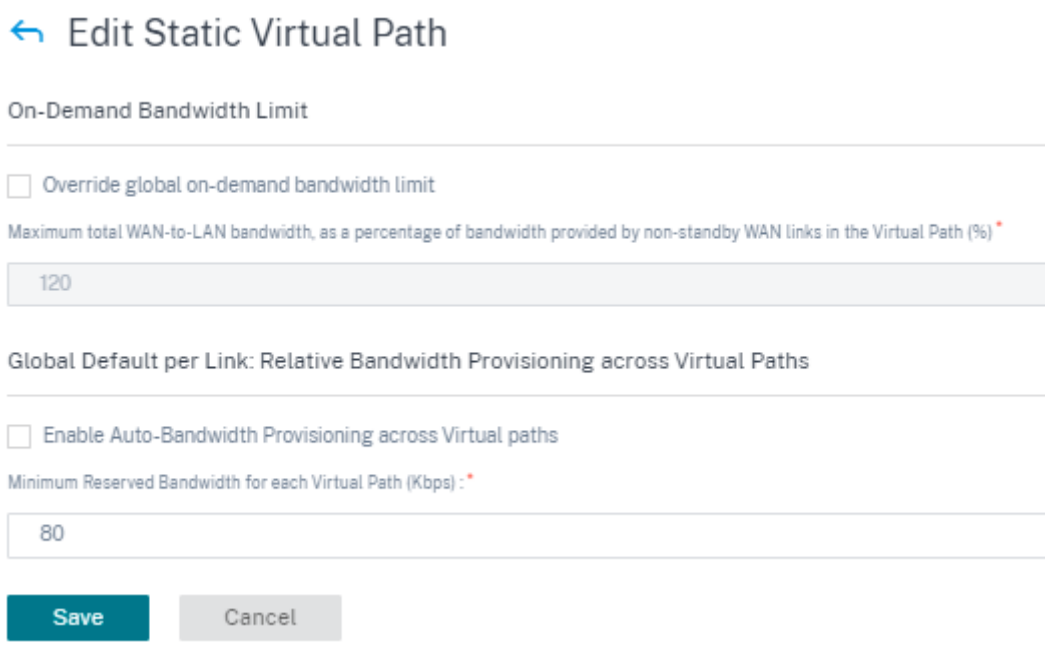
an, die angepingt werden kann, um den Status des WAN-Link zu bestimmen. Sie können auch eine Reverse-Tracking-IP für den umgekehrten Pfad angeben, der angepingt werden kann, um den Status des Rückwärtspfads zu bestimmen.

Um statische virtuelle Pfade zu konfigurieren, navigieren Sie auf Kundenebene zu **Konfiguration** > **Bereitstellungskanäle**und klicken Sie auf die Kachel **Statischer virtueller Pfad** .



Im Folgenden sind einige der unterstützten Einstellungen aufgeführt:

- **Bandbreitenliste nach Bedarf**
  - **Globales On-Demand-Bandbreitenlimit außer Kraft setzen**: Wenn aktiviert, werden die globalen Bandbreitengrenzwerte durch standortspezifische Werte ersetzt
  - **Maximale gesamte WAN-zu-LAN-Bandbreite als Prozentsatz der Bandbreite, die von WAN-Verbindungen ohne Standby-Funktion im virtuellen Pfad bereitgestellt wird (%)**: Aktualisieren Sie die maximale Bandbreitenbeschränkung in%.
- **Globaler Standard pro Link: Provisioning relativer Bandbreite über virtuelle Pfade hinweg**:
  - **Automatische Bandbreitenbereitstellung über virtuelle Pfade hinweg aktivieren**: Wenn diese Option aktiviert ist, wird die Bandbreite für alle Dienste automatisch berechnet und entsprechend der Größe der von den Remotestandorten verbrauchten Bandbreite angewendet.
  - **Mindestreservierte Bandbreite für jeden virtuellen Pfad (Kbit/s)**: Die maximale Bandbreite, die ausschließlich für jeden Dienst auf jeder WAN-Verbindung reserviert werden muss.

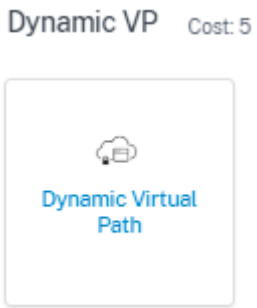


Einstellungen für dynamische virtuelle Pfade

Die globalen Einstellungen für dynamische virtuelle Pfade ermöglichen es Administratoren, Standardwerte für dynamische virtuelle Pfade im gesamten Netzwerk zu konfigurieren.

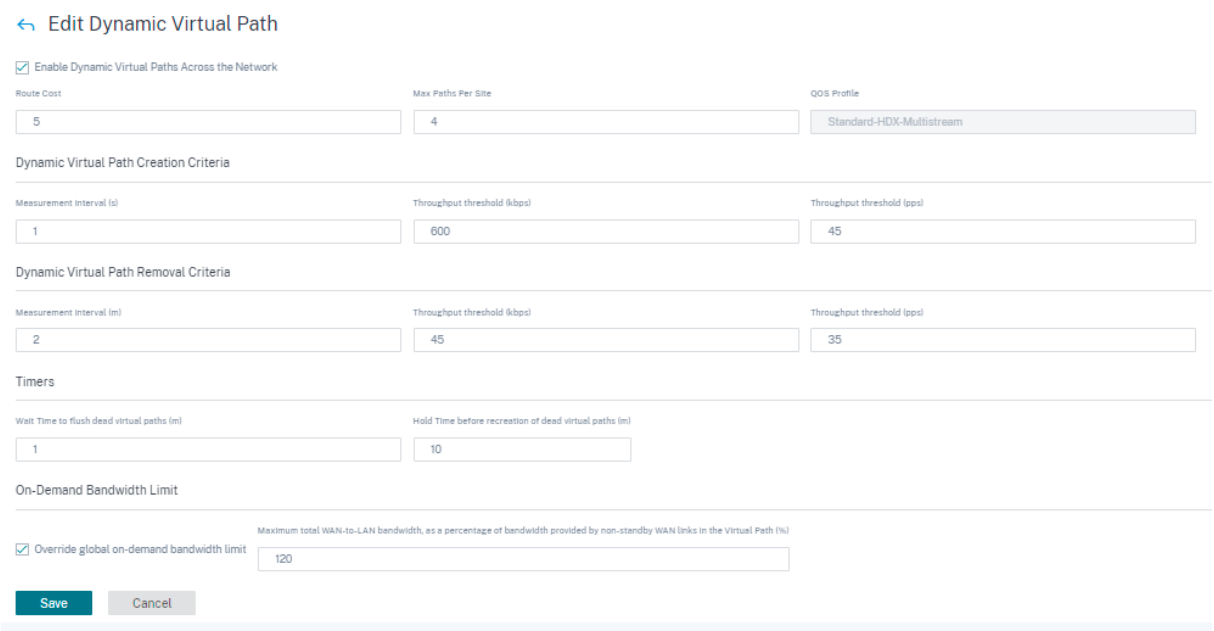
Ein dynamischer virtueller Pfad wird dynamisch zwischen zwei Standorten instanziiert, um eine direkte Kommunikation ohne dazwischenliegende SD-WAN-Knoten-Hops zu ermöglichen. In ähnlicher Weise wird auch die dynamische virtuelle Pfadverbindung dynamisch entfernt. Sowohl das Erstellen als auch das Entfernen dynamischer virtueller Pfade werden basierend auf Bandbreitenschwellen und Zeiteinstellungen ausgelöst.

Um dynamische virtuelle Pfade zu konfigurieren, navigieren Sie auf Kundenebene zu **Konfiguration** > **Bereitstellungskanäle** > **Dienstdefinitionen**, und klicken Sie auf die Kachel **Dynamischer virtueller Pfad** .



Im Folgenden sind einige der unterstützten Einstellungen aufgeführt:

- Bereitstellung zum Aktivieren oder Deaktivieren dynamischer virtueller Pfade im Netzwerk
- Die Routenkosten für dynamische virtuelle Pfade
- Das zu verwendende QoS-Profil —**Standard** standardmäßig.
- Kriterien zur Erstellung dynamischer virtueller Pfade
  - **Messintervall (Sekunden)**: Die Zeitspanne, über die Paketanzahl und Bandbreite gemessen werden, um zu bestimmen, ob der dynamische virtuelle Pfad zwischen zwei Standorten erstellt werden muss —in diesem Fall zwischen einem bestimmten Zweig und dem Control Node.
  - **Durchsatzschwelle (kbps)**: Der Schwellenwert für den Gesamtdurchsatz zwischen zwei Standorten, gemessen über das **Messintervall**, bei dem der dynamische virtuelle Pfad ausgelöst wird. In diesem Fall gilt der Schwellenwert für den Control Node.
  - **Durchsatzschwelle (pps)** - Der Schwellenwert des Gesamtdurchsatzes zwischen zwei Standorten, gemessen über das **Messintervall**, bei dem der dynamische virtuelle Pfad ausgelöst wird.
- Kriterien zum Entfernen dynamischer virtueller Pfade
  - **Messintervall (Minuten)**: Die Zeitspanne, über die Paketanzahl und Bandbreite gemessen werden, um zu bestimmen, ob ein dynamischer virtueller Pfad zwischen zwei Standorten entfernt werden muss —in diesem Fall zwischen einem bestimmten Zweig und dem Control Node.
  - **Durchsatzschwelle (kbps)** - Der Schwellenwert für den Gesamtdurchsatz zwischen zwei Standorten, gemessen über das **Messintervall**, bei dem der dynamische virtuelle Pfad entfernt wird.
  - **Durchsatzschwelle (pps)** - Der Schwellenwert des Gesamtdurchsatzes zwischen zwei Standorten, gemessen über das **Messintervall**, bei dem der dynamische virtuelle Pfad entfernt wird.
- Timer
  - **Wartezeit bis zum Löschen toter virtueller Pfade (m)**: Die Zeit, nach der ein DEAD Dynamic Virtual Path entfernt wird.
  - **Haltezeit vor der Wiederherstellung toter virtueller Pfade (m)**: Die Zeit, nach der ein dynamischer virtueller Pfad, der als DEAD entfernt wurde, neu erstellt werden kann.
- Bandbreitenliste auf
  - **Globales On-Demand-Bandbreitenlimit außer Kraft setzen**: Wenn aktiviert, werden die globalen Bandbreitengrenzwerte durch standortspezifische Werte ersetzt
  - **Maximale gesamte WAN-zu-LAN-Bandbreite als Prozentsatz der Bandbreite, die von WAN-Verbindungen ohne Standby-Funktion im virtuellen Pfad bereitgestellt wird (%)**: Aktualisieren Sie die maximale Bandbreitenbeschränkung in%.



Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen.

Routing

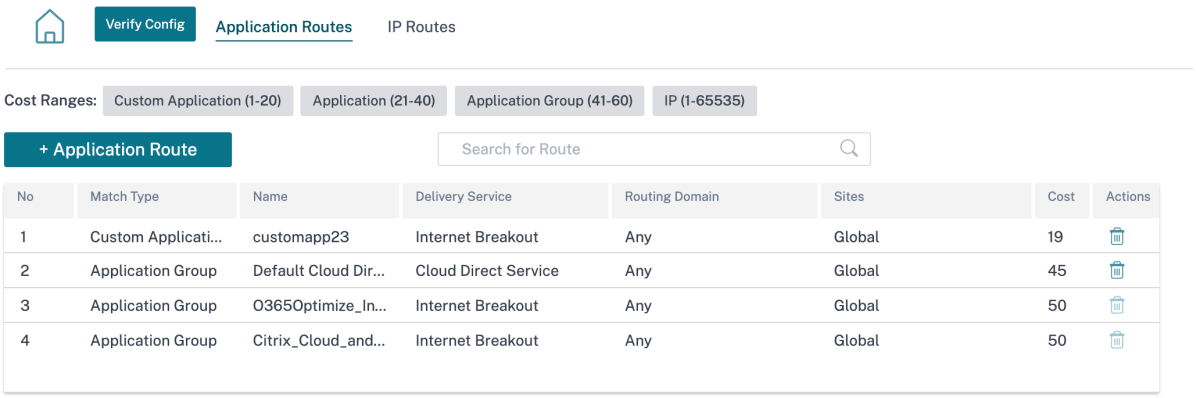
October 21, 2022

Der Abschnitt **Routing** bietet die folgenden Optionen:

- Routing-Richtlinien
- Routenzusammenfassung
- Domains weiterleiten
- Routenprofile importieren
- Routenprofile exportieren
- Transit-Knoten

Routing-Richtlinien

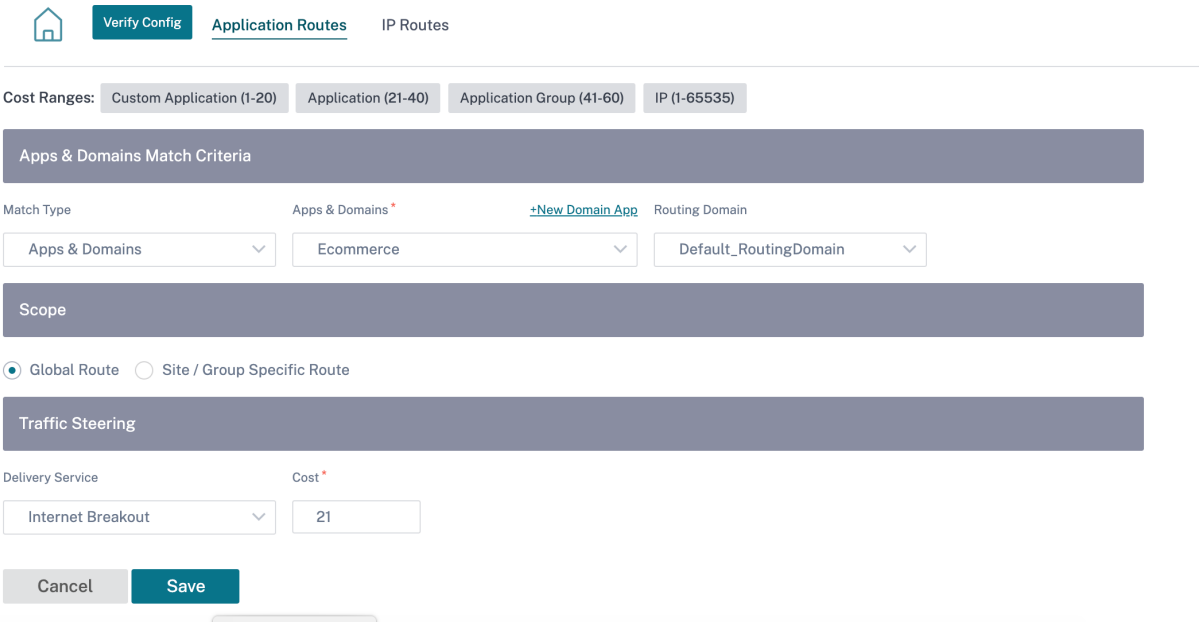
Routing-Richtlinien helfen dabei, die Verkehrssteuerung zu ermöglichen. Basierend auf der Auswahl (Anwendungsrouten und IP-Routen) können Sie verschiedene Möglichkeiten nutzen, um den Datenverkehr zu steuern.



Anwendungsrouten

Klicken Sie auf **+ Anwendungsroute**, um eine Anwendungsroute zu erstellen.

- **Übereinstimmungskriterien für benutzerdefinierte Anwendungen**:
  - **Übereinstimmungstyp**: Wählen Sie den Übereinstimmungstyp als **Anwendung/Benutzerdefinierte Anwendung/Anwendungsgruppe** aus der Dropdown-Liste
  - **Anwendung**: Wählen Sie eine Anwendung aus der Liste aus.
  - **Routingdomäne**: Wählen Sie eine Routingdomäne
- **Geltungsbereich**: Sie können die Anwendungsroute auf globaler Ebene oder auf site- und gruppenspezifischer Ebene festlegen.
- **Verkehrssteuerung**;
  - **Lieferservice**: Wählen Sie einen Lieferdienst aus der Liste.
  - **Kosten**: Spiegelt die relative Priorität jeder Route wider. Senken Sie die Kosten, je höher die Priorität.
- **Berechtigung basierend auf Pfad**:
  - **Pfad hinzufügen**: Wählen Sie eine Site und WAN-Links. Wenn der gewählte Pfad abfällt, erhält die Anwendungsroute keinen Datenverkehr.

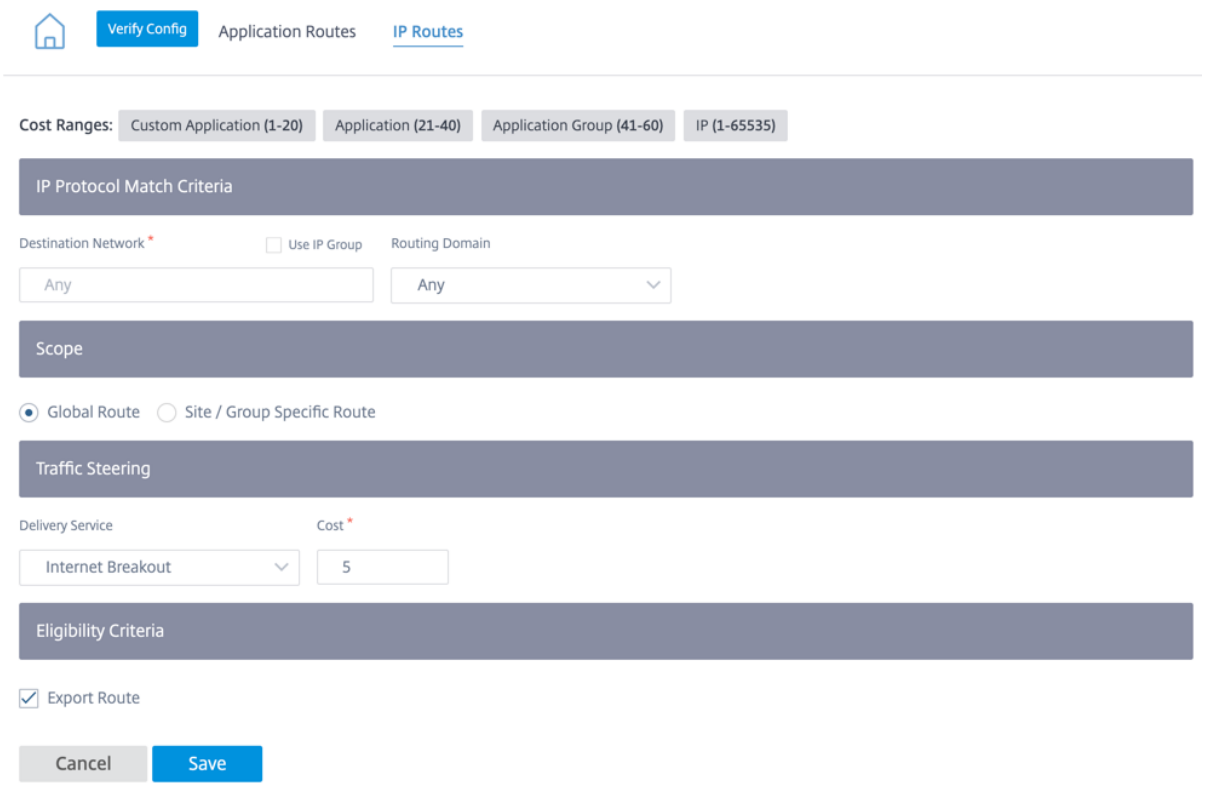


Wenn eine neue Anwendungsroute hinzugefügt wird, müssen die Routenkosten im folgenden Bereich liegen:

- **Benutzerdefinierte Anwendung**: 1—20
- **Anwendung**: 21—40
- **Anwendungsgruppe**: 41—60

IP-Routen

Gehen Sie zur Registerkarte **IP-Routen** und klicken Sie auf **+ IP-Route** to IP-Routenrichtlinie, um den Datenverkehr zu steuern.



- **IP-Protokoll-Übereinstimmungskriterien**:
  - **Zielnetzwerk**: Fügen Sie das Zielnetzwerk hinzu, das beim Weiterleiten der Pakete hilft.
  - **IP-Gruppe verwenden**: Sie können ein Zielnetzwerk hinzufügen oder das Kontrollkästchen **IP-Gruppe verwenden** aktivieren, um eine IP-Gruppe aus der Dropdown-Liste auszuwählen.
  - **Routingdomäne**: Wählen Sie eine Routingdomäne aus der Dropdownliste
- **Geltungsbereich**: Sie können die IP-Route auf globaler Ebene oder auf site- und gruppenspezifischer Ebene festlegen.
- **Verkehrssteuerung**:
  - **Lieferservice**: Wählen Sie einen Zustelldienst aus der Dropdownliste aus.
  - **Kosten**: Spiegelt die relative Priorität jeder Route wider. Senken Sie die Kosten, je höher die Priorität.

  Wenn eine neue IP-Route hinzugefügt wird, müssen die Routenkosten im Bereich von 1—20 liegen.
- **Zulassungskriterien**:
  - **Route exportieren**: Wenn das Kontrollkästchen **Route exportieren** aktiviert ist und es sich bei der Route um eine lokale Route handelt, kann die Route standardmäßig exportiert

werden. Wenn es sich bei der Route um eine INTRANET/INTERNET-basierte Route handelt, muss WAN-zu-WAN-Weiterleitung aktiviert werden, damit der Export funktioniert. Wenn das Kontrollkästchen **Route exportieren** deaktiviert ist, kann die lokale Route nicht in ein anderes SD-WAN exportiert werden und hat lokale Bedeutung.

- **Berechtigung basierend auf Pfad**:
  - **Pfad hinzufügen**: Wählen Sie eine Site und WAN-Links. Wenn der hinzugefügte Pfad ausfällt, erhält die IP-Route keinen Datenverkehr.

Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen.

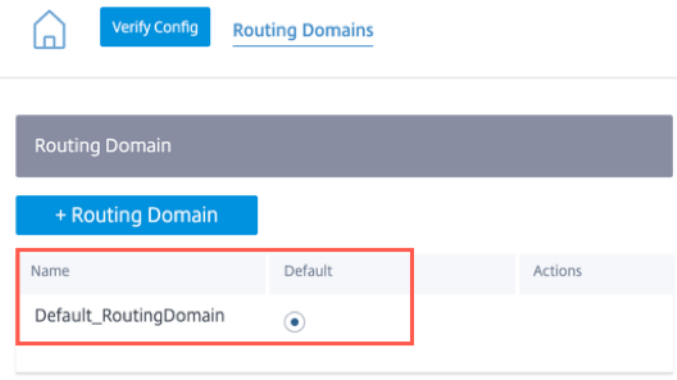
Routenzusammenfassung

Routenzusammenfassung reduziert die Anzahl der Routen, die ein Router verwalten muss. Eine zusammenfassende Route ist eine einzelne Route, die zur Darstellung mehrerer Routen verwendet wird. Es spart Bandbreite, indem eine Anzeige für eine einzelne Route gesendet wird, wodurch die Anzahl der Verbindungen zwischen Routern reduziert wird. Es spart Speicher, da nur eine Routenadresse beibehalten wird. Die CPU-Ressourcen werden effizienter genutzt, indem rekursive Lookups vermieden werden. Sie können Zusammenfassungsrouten hinzufügen, ohne die Gateway-IP-Adresse anzugeben.

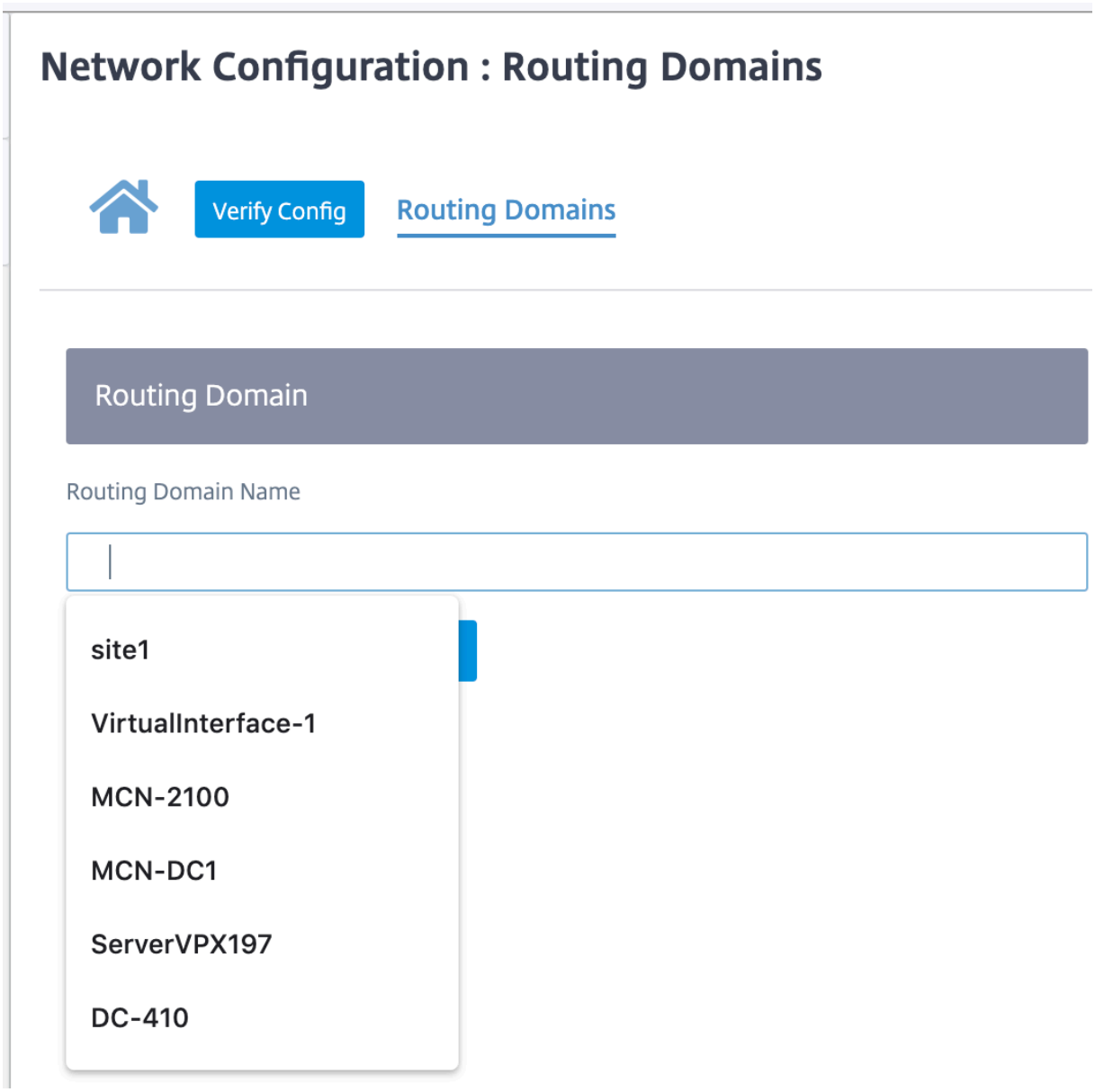
Routing-Domänen

Routingdomänen werden für getrennten Datenverkehr über VLAN verwendet. Sobald die Routingdomänen erstellt wurden, können Sie sie auf globaler Ebene (für Intranetdienste) oder auf Schnittstellenebene referenzieren.

Sie können auch die Standard-Routingdomäne auswählen, die für alle Standorte gilt.



Um Routen aus einer bestimmten Routingdomäne zuzuordnen, klicken Sie auf **+ Routingdomäne** und wählen Sie eine der konfigurierten Routingdomänen aus der Dropdownliste Klicken Sie auf **Speichern**.



Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen.

Weitere Informationen finden Sie unter Routingdomäne.

Domänendienst für den übergreifenden Routing

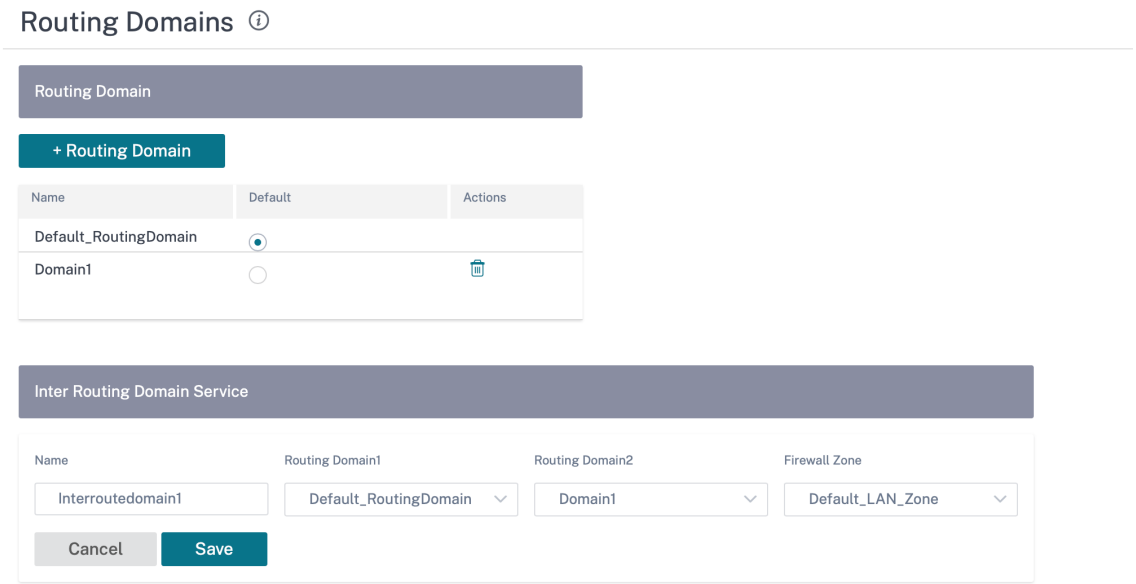
Citrix SD-WAN Orchestrator for On-premises bietet einen statischen Inter-Routing-Domänendienst, der das Leaking von Routen zwischen Routingdomänen innerhalb eines Standorts oder zwischen verschiedenen Standorten ermöglicht. Dadurch entfällt die Notwendigkeit, dass ein Edgerouter Routeleaking verarbeitet. Der Inter-VRF-Routingdienst kann weiterhin verwendet werden, um Routen, Firewall-Richtlinien und NAT-Regeln einzurichten.

Weitere Informationen finden Sie unter Inter-Routing-Domänendienst.

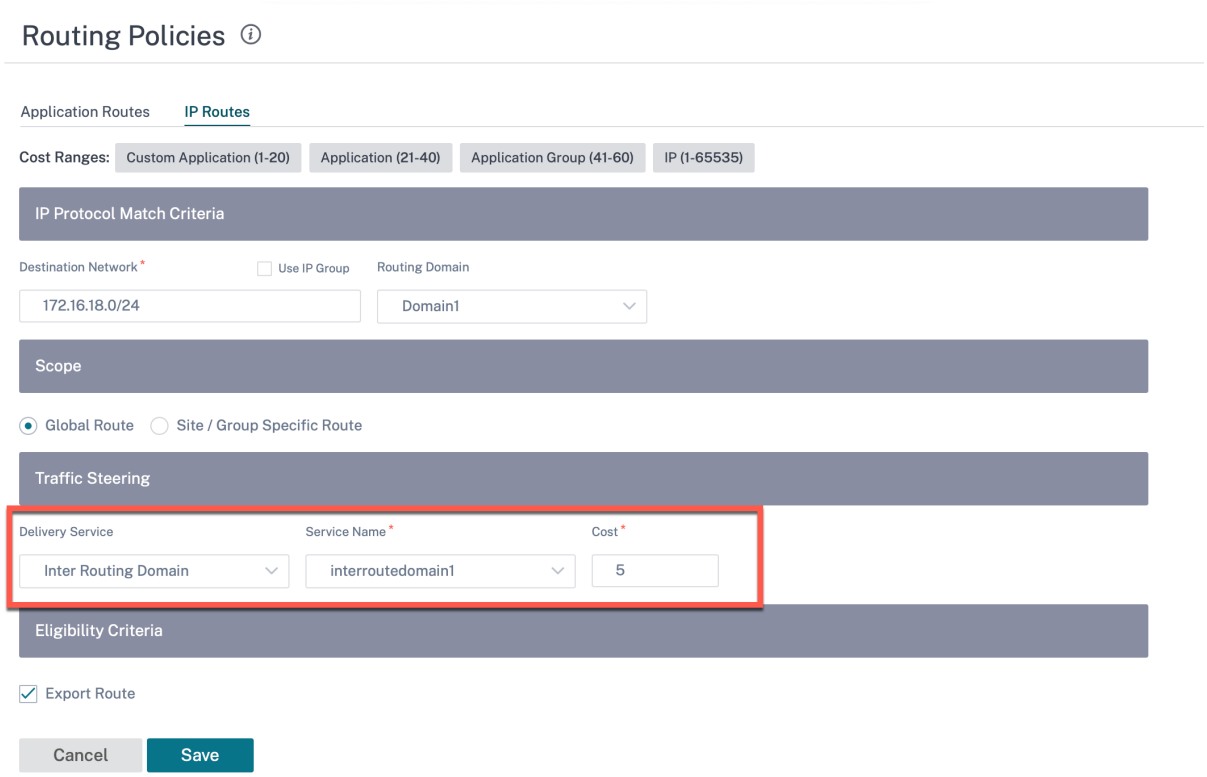
So konfigurieren Sie den Inter-Routing-Domänendienst über den Citrix SD-WAN Orchestrator for On-premises:

1. Navigieren Sie auf Netzwerkebene zu **Konfiguration** > **Routing >**Routingdomänen**** > ****Inter-Routing-Domänendienst**.
2. Klicken Sie auf **+ Inter-Routing Domain** und geben Sie Werte für die folgenden Parameter ein:

- **Name**: Der Name des Inter-Routing Domain-Dienstes.
- **Routingdomäne 1**: Die erste Routingdomäne des Paares.
- **Routingdomäne 2**: Die zweite Routingdomäne des Paares.
- **Firewall-Zone**: Die Firewall-Zone des Dienstes.
  - **Standard**: Die **Firewallzone Inter_Routing_Domain_Zone** ist zugewiesen.
  - **Keine**: Der Dienst verhält sich wie ein Conduit, der keine Zone hat und die ursprüngliche Zone des Pakets beibehält.
  - Möglicherweise sind alle im Netzwerk konfigurierten Zonen ausgewählt.

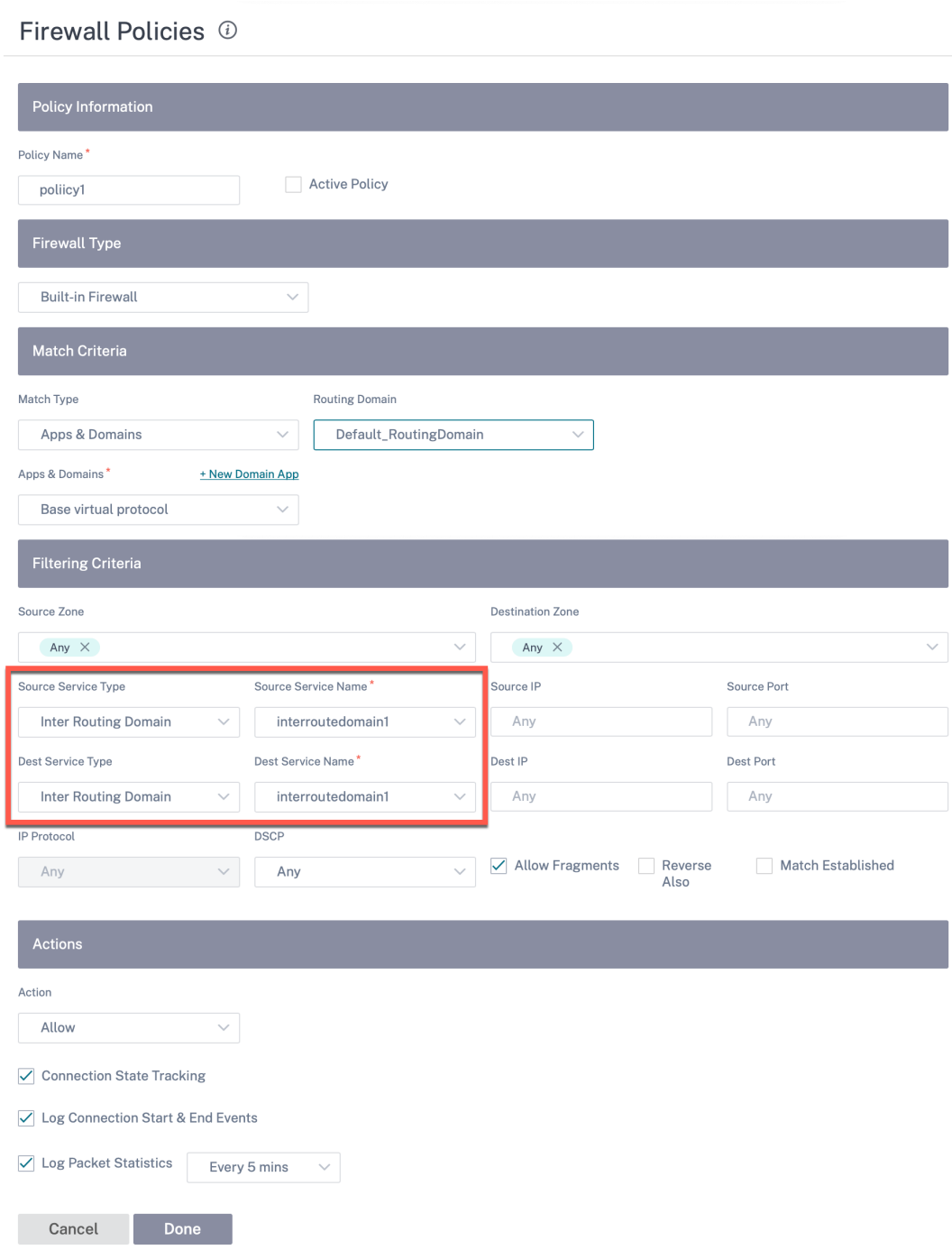


Um Routen mit dem Inter-Routing-Domänendienst zu erstellen, erstellen Sie eine Route mit dem Diensttyp als Inter-Routing Domain Service und wählen Sie den Inter-Routing-Domänendienst aus. Weitere Informationen zum Konfigurieren von Routen finden Sie unter Routing-Richtlinien.



Fügen Sie außerdem eine Route aus dem anderen Routingdomänenpaar hinzu, um eine Verbindung zwischen den beiden Routingdomänen herzustellen.

Sie können Firewall-Richtlinien auch konfigurieren, um den Datenverkehr zwischen Routingdomänen zu steuern. Wählen Sie in den Firewall-Richtlinien die Option Inter-Routing-Domänendienst für die Quell- und Zieldienste aus, und wählen Sie die erforderliche Firewall-Aktion aus. Informationen zum Konfigurieren von Firewall-Richtlinien finden Sie unter Firewall-Richtlinien.

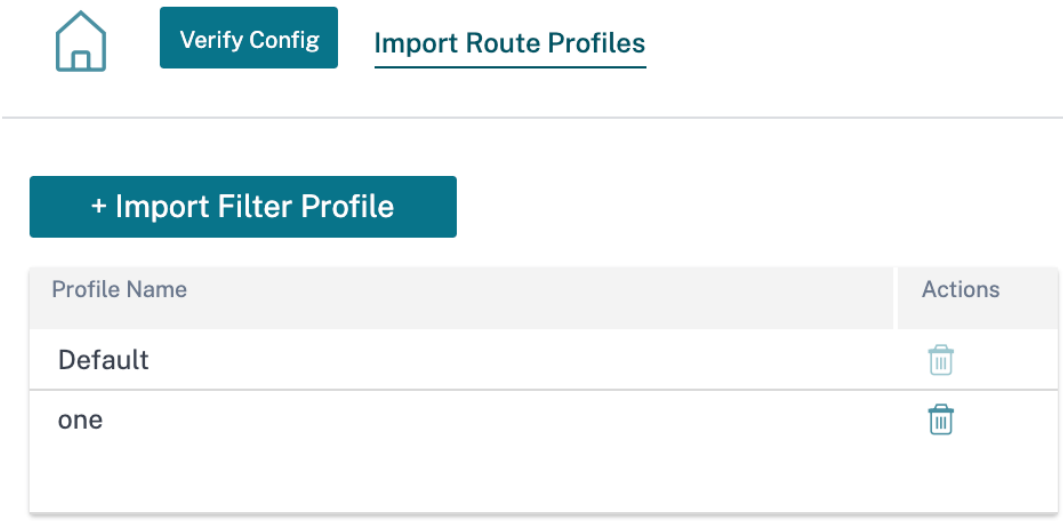


Sie können auch den Intranetdiensttyp auswählen, um statische und dynamische NAT-Richtlinien zu konfigurieren. Weitere Informationen zum Konfigurieren von NAT-Richtlinien finden Sie unter Netzwerkadressübersetzung.

Routenprofile importieren

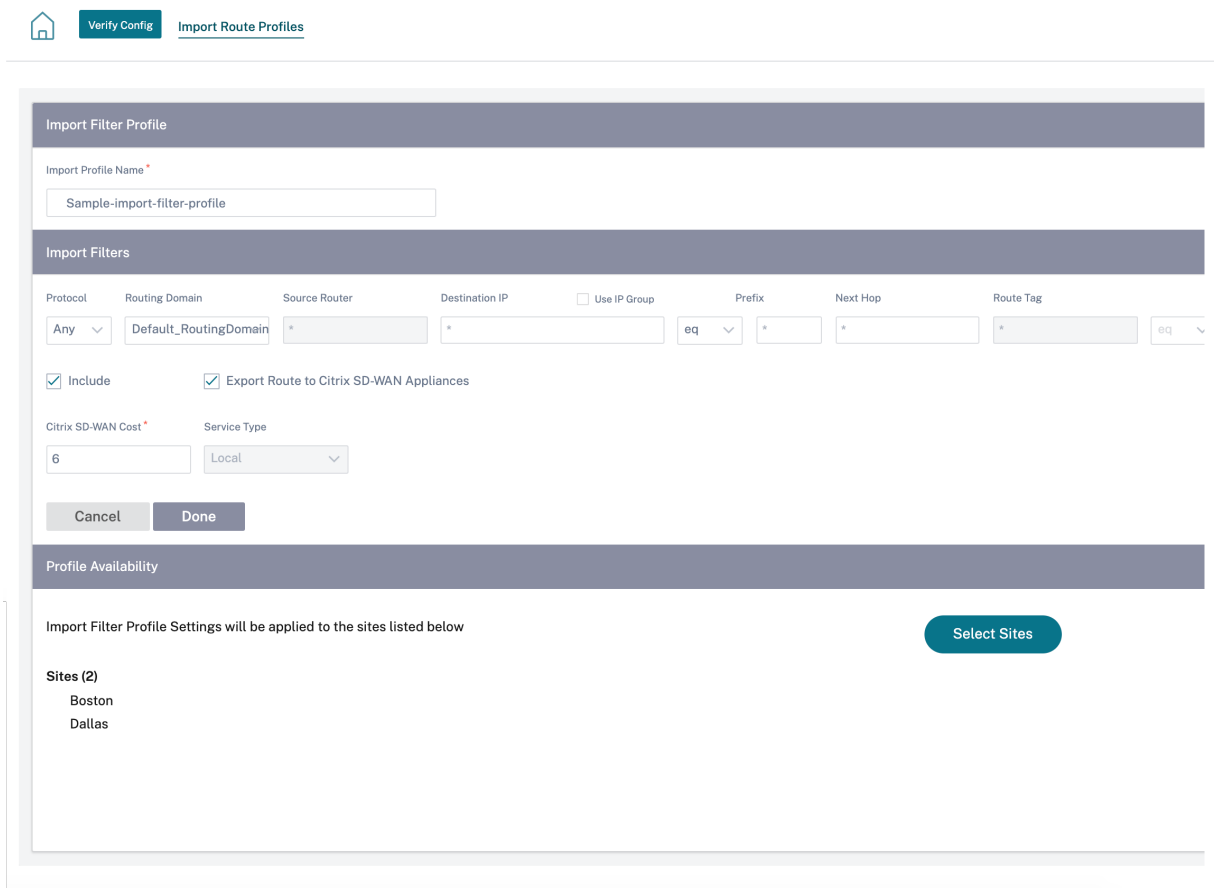
Sie können Filter konfigurieren, um die Art und Weise, wie das Routenlernen stattfindet, zu optimieren.

Importfilterregeln sind Regeln, die erfüllt sein müssen, bevor dynamische Routen in die SD-WAN-Routendatenbank importiert werden. Standardmäßig werden keine Routen importiert.



Fügen Sie ein **Importfilterprofil** mit dem **Namen des Importprofils, der Profilverfügbarkeit** und den **Importfiltern** sowie den folgenden Feldern hinzu:

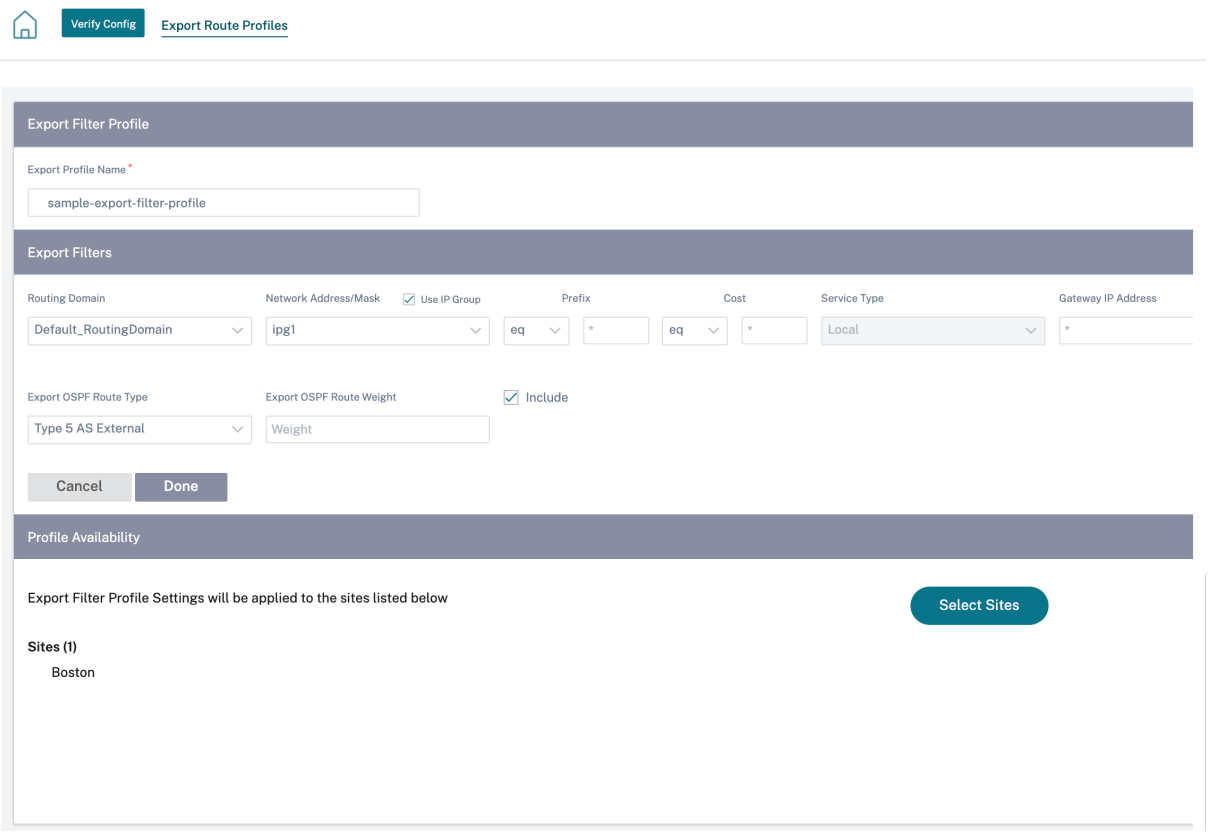
- **Protokoll** —Wählen Sie das Protokoll aus der Liste aus.
- **Routingdomäne** —Um Routen aus einer bestimmten Routingdomäne zuzuordnen, wählen Sie eine der konfigurierten Routingdomänen aus der Liste aus.
- **Quellrouter** —Geben Sie die IP-Adresse und Netzmaske des konfigurierten Netzwerkobjekts ein, das das Netzwerk der Route beschreibt.
- **Ziel-IP** —Geben Sie die Ziel-IP-Adresse ein.
- **Präfix** - Um Routen nach Präfix zuzuordnen, wählen Sie ein Übereinstimmungsprädikat aus der Liste aus und geben Sie ein Routenpräfix in das angrenzende Feld ein.
- **Nächster Hop** - Geben Sie das nächste Hop-Ziel ein.
- **Routen-Tag** —Füllen Sie das Routen-Tag
- **Kosten** - Die Methode (Prädikat) und die SD-WAN-Routenkosten, die verwendet werden, um die Auswahl der exportierten Routen einzuschränken.



Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen.

Routenprofile exportieren

Definieren Sie die Regeln, die bei der Werbung für SD-WAN-Routen über dynamische Routing-Protokolle erfüllt werden müssen. Standardmäßig werden alle Routen für Peers angekündigt.



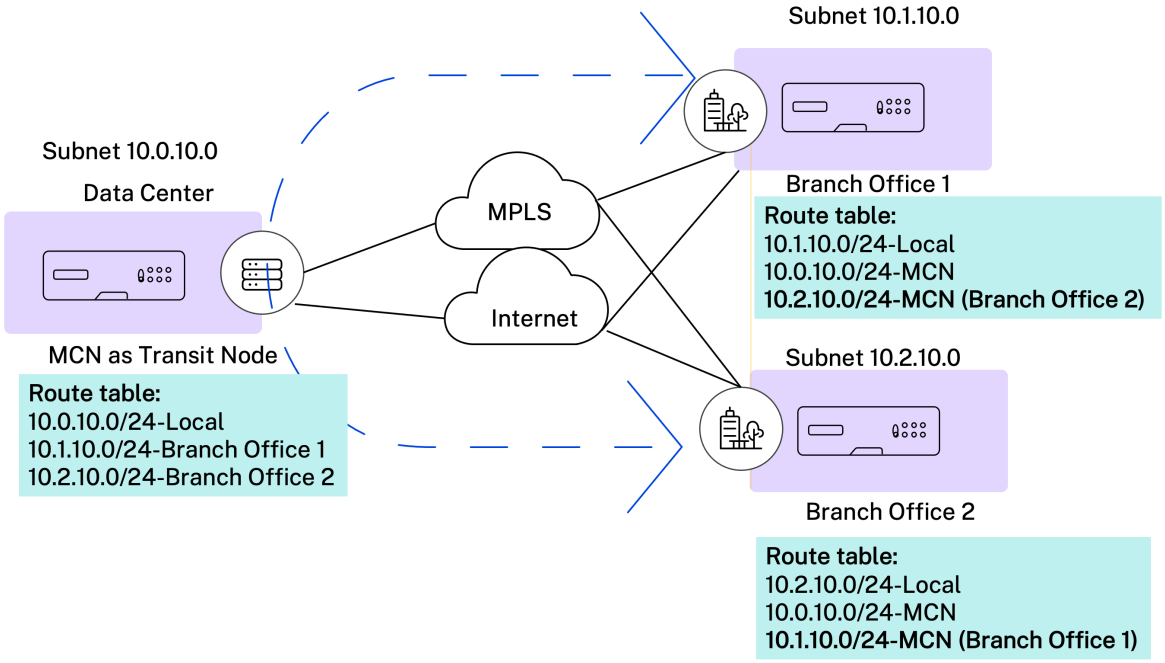
Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen.

Transit-Knoten

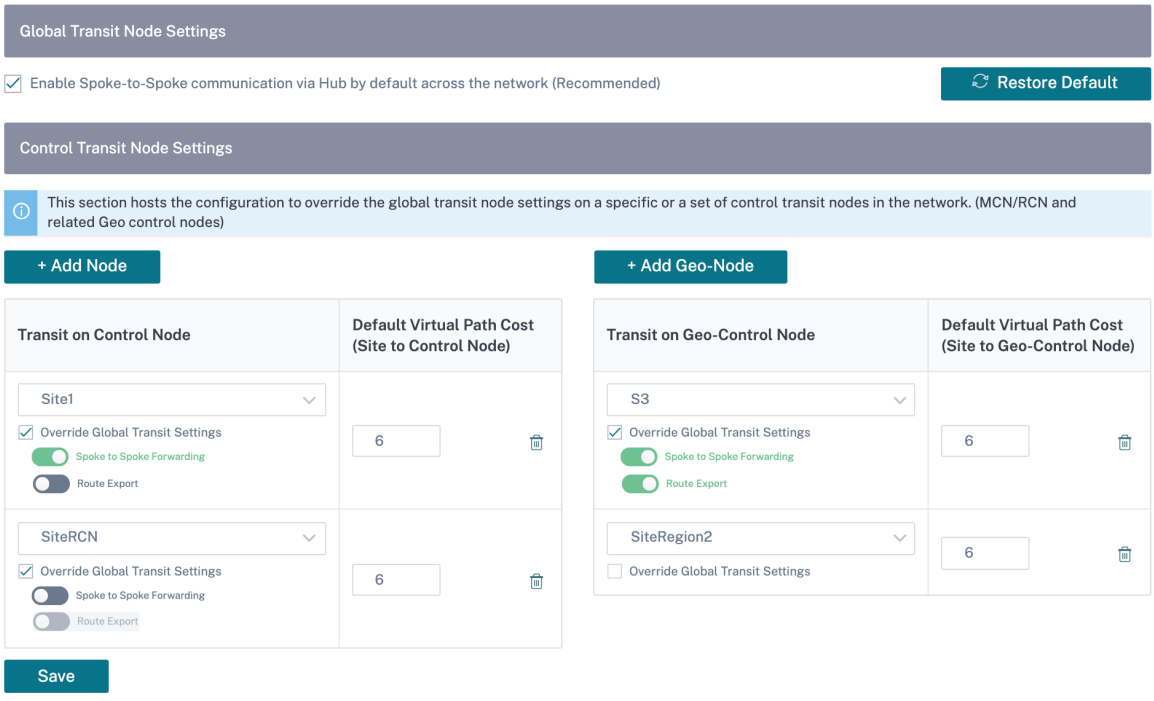
Virtueller Overlay-Transit-Knoten

Transitknoten sind die Standorte, die Datenverkehr zwischen einer oder mehreren Filialen innerhalb einer Region weiterleiten können.

Der Verkehr zwischen zwei Knoten kann beeinflusst werden, um den Transitknoten als Zwischen-Hop auszuwählen, indem die Routenkosten angepasst werden. Transit-Knoten werden verwendet, um Daten an nicht benachbarte Knoten weiterzuleiten. Wenn beispielsweise drei Knoten in der Reihe A-B-C verbunden sind, können Daten von A nach C über B geroutet werden. Sie können den Transitknoten und die Standorte angeben, die durch den Transitknoten geroutet werden sollen, im Citrix SD-WAN Orchestrator Service. Die virtuellen Pfade werden in aufsteigender Reihenfolge der Kosten gewählt. Senken Sie die Kosten, höher die Priorität.



Standardmäßige globale virtuelle Overlay-Transit-Knoten Sie können die Kontrollknoten (MCN/RCN) und die Geo-Control-Knoten (Geo-MCN/RCN) als standardmäßige globale virtuelle Overlay-Transitknoten in einem Netzwerk angeben. Durch die Aktivierung der Spoke-and-Spoke-Kommunikation über Hub als Teil der globalen Einstellungen können alle Standorte die konfigurierten Steuerknoten standardmäßig als Transitknoten für die Site-to-Site-Kommunikation verwenden.



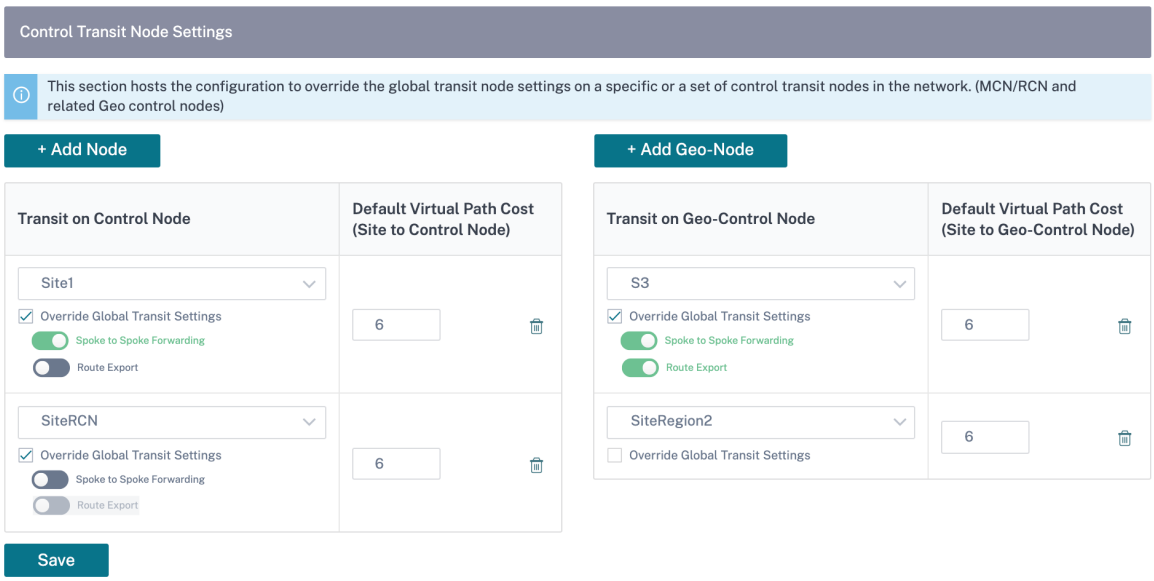
Fügen Sie den Kontrollknoten und die Geo-Control-Knoten hinzu, die Sie als virtuelle Overlay-Transitknoten verwenden möchten, und geben Sie die Kosten für den virtuellen Pfad an. Die Kontrollknoten und Geo-Control-Knoten haben 6 und 7 als die jeweiligen standardmäßigen virtuellen Pfadkosten. Sie können die Kosten für den virtuellen Pfad gemäß Ihren Netzwerkanforderungen ändern. Klicken Sie auf **Standard wiederherstellen**, um die Standardkosten für den virtuellen Pfad für die Standard-Transitknoten wiederherzustellen.

> **Hinweis**
>
> Sie können maximal 3 Kontrollknoten und 3 Geo-Control-Knoten als Transit-Knoten hinzufügen.

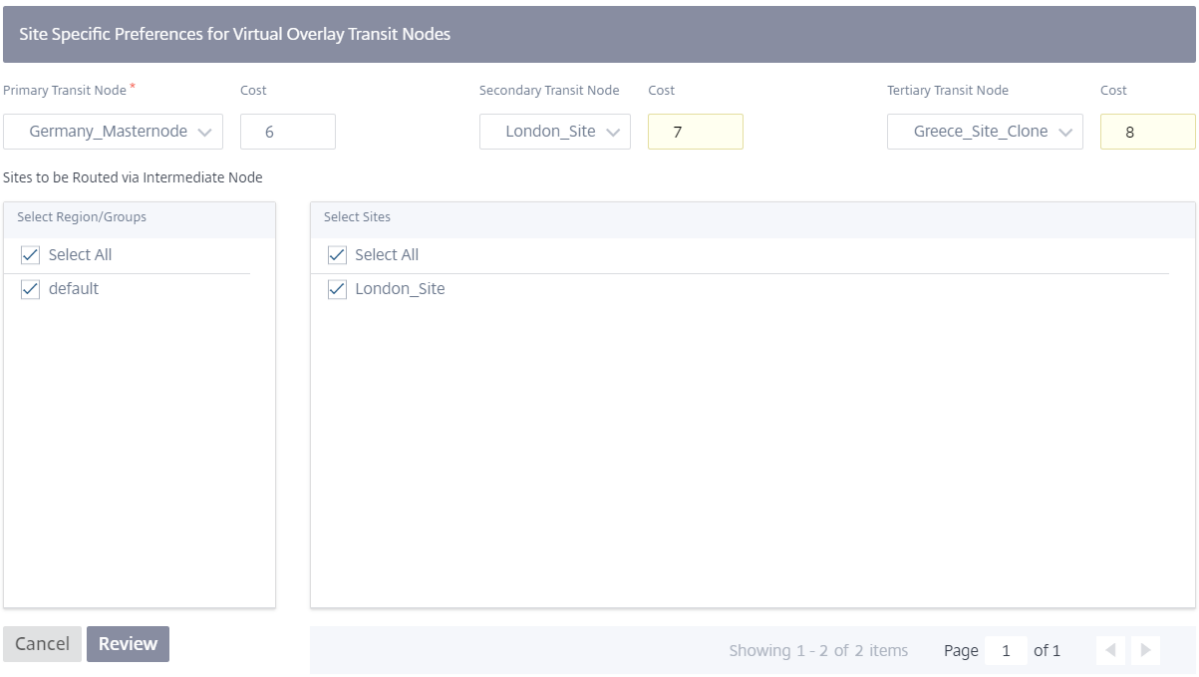
Standardmäßig ist die WAN-zu-WAN-Weiterleitung für alle Pfade aktiviert, die mit den ausgewählten Steuerungs- und Geo-Control-Knoten verknüpft sind. Die WAN-zu-WAN-Weiterleitun ermöglicht es einer Site, als Zwischensprung zwischen zwei benachbarten Standorten für Site-zu-Site-, Internet- oder Intranetdatenverkehr zu fungieren und als Vermittler für dynamische virtuelle Pfade zu fungieren.

Sie können die globalen Transitknoteneinstellungen außer Kraft setzen und die Spoke-to-Spoke-Weiterleitung nur auf ausgewählten Kontroll-Transitknoten aktivieren oder deaktivieren. Wenn **Spoke to Spoke Forwarding** aktiviert ist, exportiert der Transitsteuerungsknoten Routen über die mit ihm verbundenen Standorte. Die Site-to-Site-Kommunikation und der dynamische virtuelle Pfad zwischen Standorten, die allein mit dem Transitknoten verbunden sind, werden aktiviert.

Durch Aktivieren des **Routenexports** werden die Weiterleitung von virtuellem Pfad zu virtuellem Pfad und der Routenexport (WAN-to-WAN-Weiterleitung) auf allen Standortpfaden Durch Deaktivieren der Umschaltfläche wird nur die Weiterleitung von virtuellem Pfad zu virtuellem Pfad aktiviert und der Routenexport auf allen Sitepfaden deaktiviert. Routenexport kann nur aktiviert werden, wenn **Spoke to Spoke Forwarding** aktiviert ist.



Site-spezifische Einstellungen für virtuelle Overlay-Transit-Knoten Site-spezifische Einstellungen für virtuelle Overlay-Transit-Knoten ermöglichen es Ihnen, die globalen Einstellungen für virtuelle Overlay-Transitknoten für alle Standorte in Ihrem Netzwerk zu überschreiben. Sie können auch einen nicht zu steuernden Knoten als primären Transitknoten für einen Standort auswählen. Wählen Sie einen Kontrollknoten oder Geo-Kontrollknoten als sekundären und tertiären Transitknoten. Wenn der primäre Transitknoten ausgefallen ist, verwenden die Standorte den sekundären Transitknoten. Wenn sowohl primäre als auch sekundäre Transitknoten ausgefallen sind, verwenden die Standorte den tertiären Transitknoten. Geben Sie die Kosten für die Transitknoten an, und wählen Sie die Standorte aus, auf die die standortspezifischen Einstellungen für den virtuellen Overlay-Transitknoten angewendet werden.



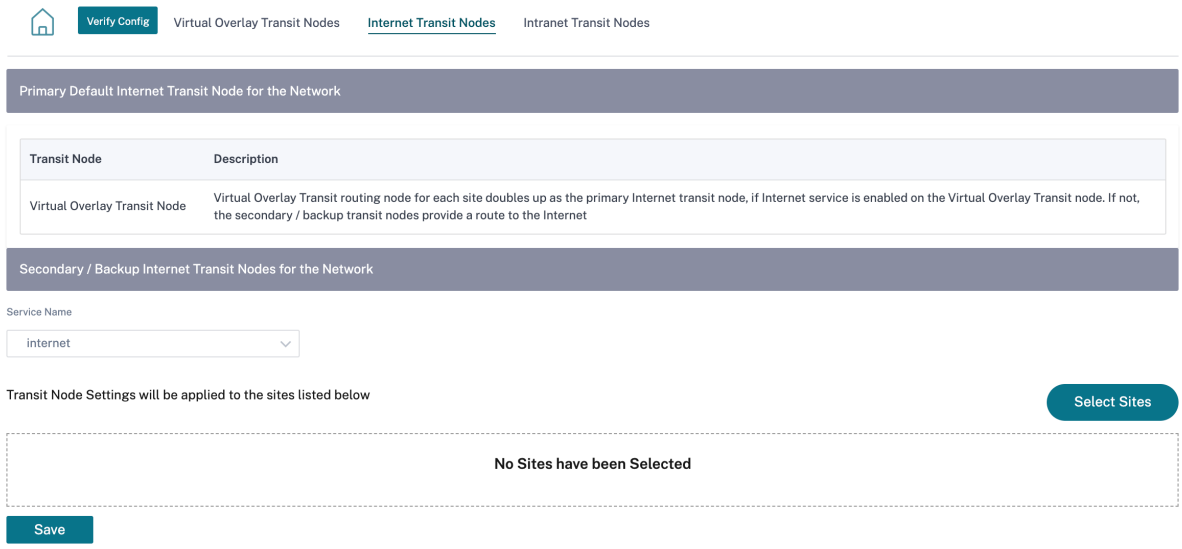
Internet-Transit-Knoten

Sie können Standorte als Internet-Transitstandorte hinzufügen, um den Internetzugriff auf die Standorte zu ermöglichen. Sites, die eine direkte Internetverbindung benötigen, müssen mindestens eine Verbindung mit aktiviertem Internetdienst haben. Das bedeutet, dass mindestens ein Link auf einen Bandbreitenanteil ungleich Null gesetzt ist%.

Jedem Transitstandort können Routenkosten zugewiesen werden. Die Standorte mit verfügbarem Internetdienst greifen direkt auf das Internet zu, da die direkte Route der kostengünstigste Routingpfad wäre. Websites ohne Internetdienst können über die konfigurierten Transitstandorte eine Weiterleitung zum Internet durchführen. Wenn die Internet-Transitorte konfiguriert sind, werden Routen zum Internet über diese Transitsites automatisch an alle Standorte weitergeleitet. Internet-Transit-Websites sind Standorte mit aktiviertem Internetdienst.

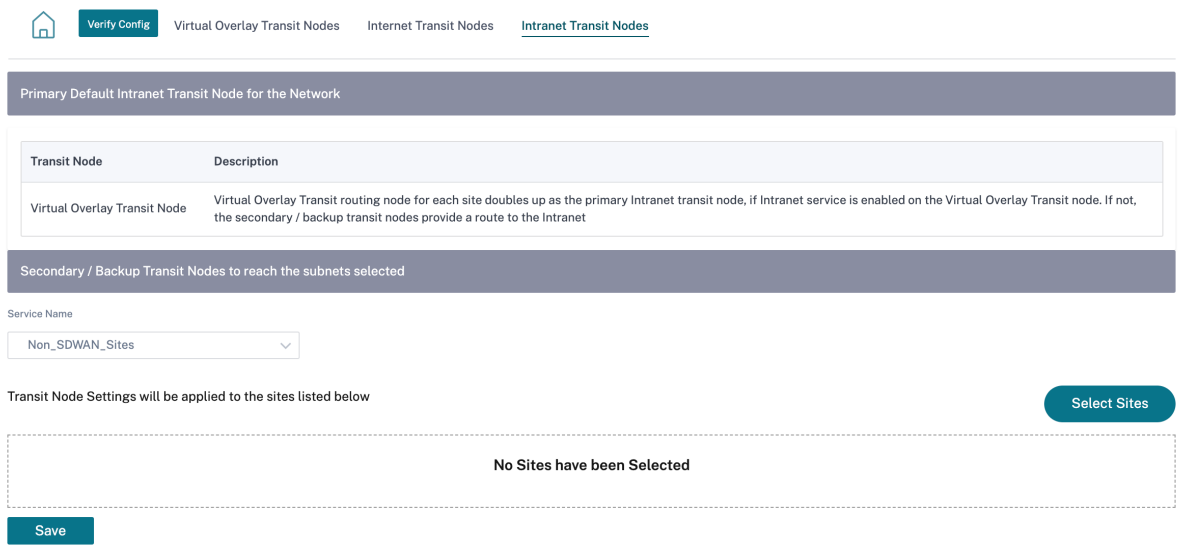
Zum Beispiel, wenn San Francisco und New York als Internet-Transitstandorte konfiguriert sind. Routen zum Internet über San Francisco und New York werden automatisch an alle Standorte übertragen.

Der virtuelle Overlay-Transitknoten mit aktiviertem Internetdienst fungiert als primärer Internet-Transit-Knoten. Wenn der Internetdienst auf dem virtuellen Overlay-Transitknoten nicht aktiviert ist, bietet der sekundäre/backup internet Transit-Knoten eine Route zum Internet.



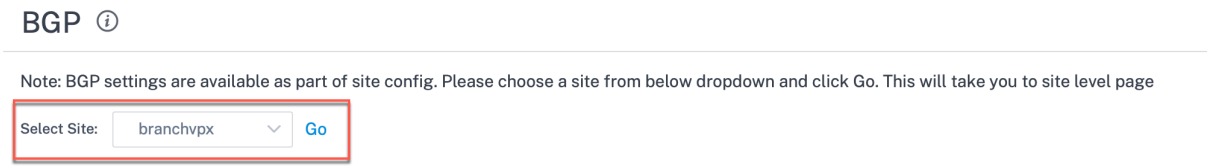
Intranet-Transit-Knoten

Der Intranet-Transitknoten ermöglicht allen Nicht-Intranet-Sites den Zugriff auf die konfigurierten Intranetnetzwerke. Jedem Transitstandort können Routenkosten zugewiesen werden. Die verfügbaren Standorte mit Intranetdienst greifen direkt auf die Intranet-Netzwerke zu, da die direkte Route der kostengünstigste Routingpfad wäre. Sites ohne Intranetdienst können über die konfigurierten Transitsites an die Intranetnetzwerke weiterleiten. Wenn die Transitstandorte konfiguriert sind, werden Routen zu Intranetnetzwerken über diese Transitstandorte automatisch an alle Standorte übertragen.
Zum Beispiel, wenn 10.2.1.0/24 ein Intranetnetzwerk ist und Austin und Dallas die konfigurierten Transitsites sind. Routen zu dieser Netzwerkadresse über Austin und Dallas werden automatisch an alle Standorte übertragen.
Der virtuelle Overlay-Transitknoten mit aktiviertem Intranetdienst fungiert als primärer Intranet-Transitknoten. Wenn der Intranetdienst auf dem virtuellen Overlay-Transitknoten nicht aktiviert ist, bietet der sekundäre/backup Intranet-Transitknoten eine Route zum Intranet.



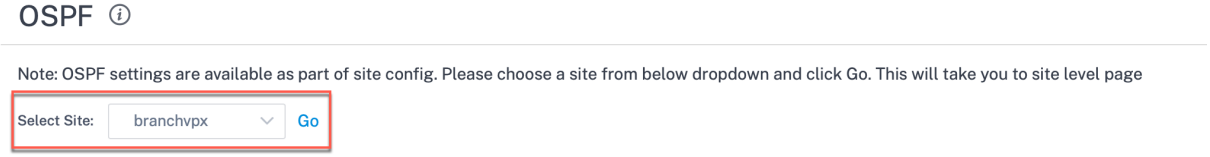
BGP

Sie können BGP-Einstellungen für eine Site konfigurieren, indem Sie die gewünschte Site aus der Dropdown-Liste auswählen und auf **GO**klicken. Dadurch gelangen Sie zur BGP-Konfigurationsseite auf Standortebene. Detaillierte Informationen zur Konfiguration von BGP finden Sie unter BGP.



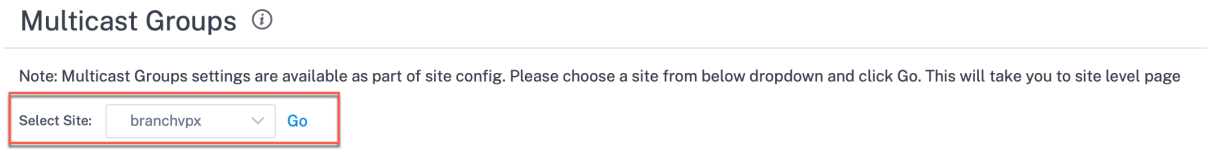
OSPF

Sie können die OSPF-Einstellungen für eine Site konfigurieren, indem Sie die gewünschte Site aus der Dropdown-Liste auswählen und auf **GO**klicken. Dadurch gelangen Sie zur OSPF-Konfigurationsseite auf Standortebene. Detaillierte Informationen zur Konfiguration von OSPF finden Sie unter OSPF.



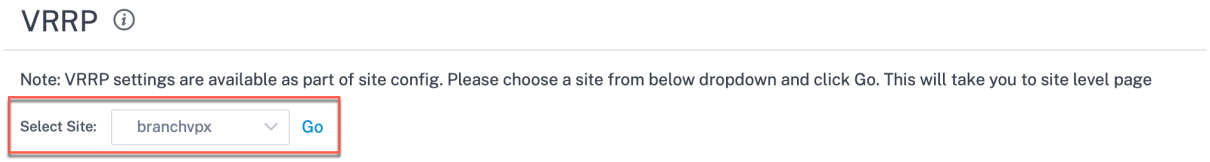
Multicast-Gruppen

Sie können das Multicast-Routing für einen Standort konfigurieren, indem Sie den gewünschten Standort aus der Dropdownliste auswählen und auf **GO**klicken. Dadurch gelangen Sie zur Konfigurationsseite für Multicastgruppen auf Standortebene. Detaillierte Informationen zur Konfiguration des Multicast-Routings finden Sie unter Multicastgruppen.



VRRP

Sie können das Virtual Router Redundancy Protocol (VRRP) für einen Standort konfigurieren, indem Sie den gewünschten Standort aus der Dropdown-Liste auswählen und auf **GO**klicken. Dadurch gelangen Sie zur VRRP-Konfigurationsseite auf Site-Ebene. Detaillierte Informationen zur Konfiguration des Multicast-Routings finden Sie unter VRRP.



Interlink-Kommunikation

October 21, 2022

Interlink-Kommunikationseinstellungen werden für die automatische Pfaderstellung zwischen kompatiblen WAN-Verbindungen verwendet. Sie können diese Einstellungen unter **Sitekonfiguration** und **Virtuelle Pfade**außer Kraft setzen, wobei Sie einzelne Mitgliedspfade für einen bestimmten virtuellen Pfad auswählen oder deren Auswahl aufheben können.

Derzeit sind die folgenden zwei Einstellungen verfügbar:

- Regeln zur Automatisierung der Erstellung von Pfaden zwischen kompatiblen WAN-Links.
- Globale Standardeinstellungen für dynamische virtuelle Pfade

Diese Einstellungen werden von allen WAN-Verbindungen im Kundennetzwerk übernommen.

Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen.

Standardgruppen für Inter-Link-Kommunikation

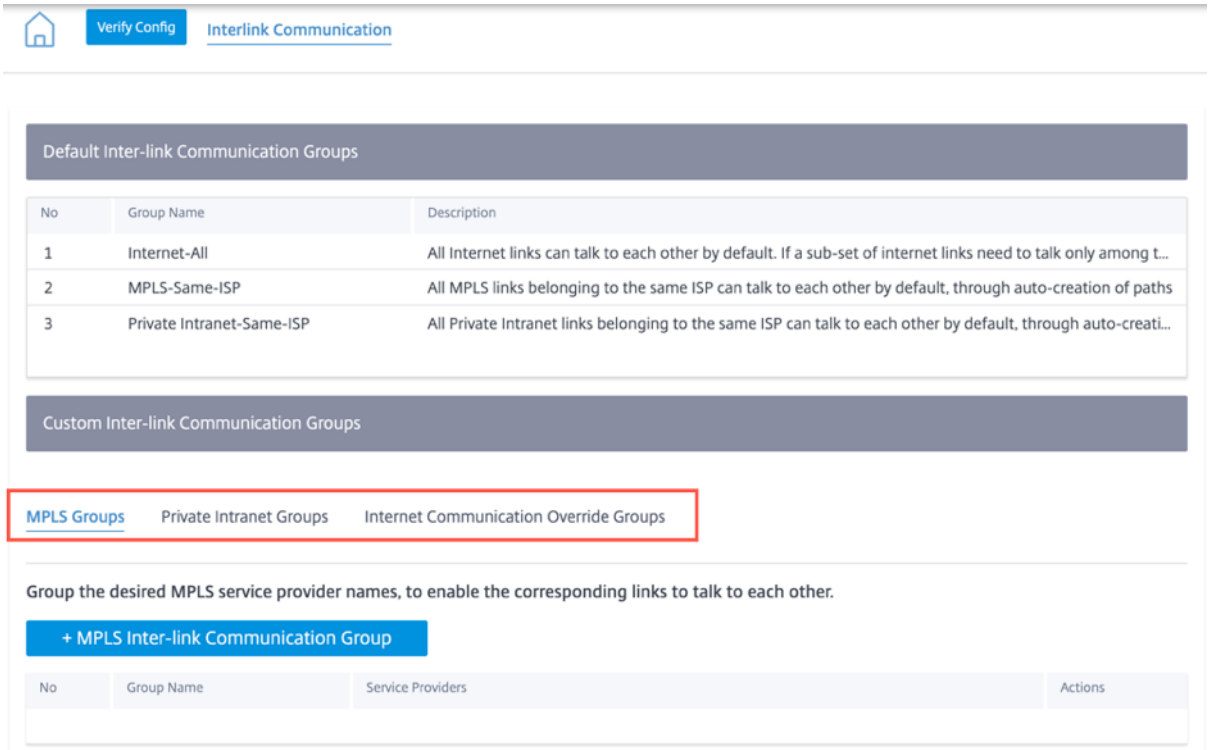
Standard-Inter-Link-Kommunikationsgruppen sollen die Erstellung von Pfaden zwischen folgenden Komponenten automatisieren:

- Zwei beliebige Internetlinks
- Zwei beliebige MPLS-Links, die einen Dienstanbieter gemeinsam nutzen, und
- Zwei beliebige private Intranet-Links, die einen Dienstanbieter gemeinsam nutzen

Benutzerdefinierte Interlink-Kommunikationsgruppen

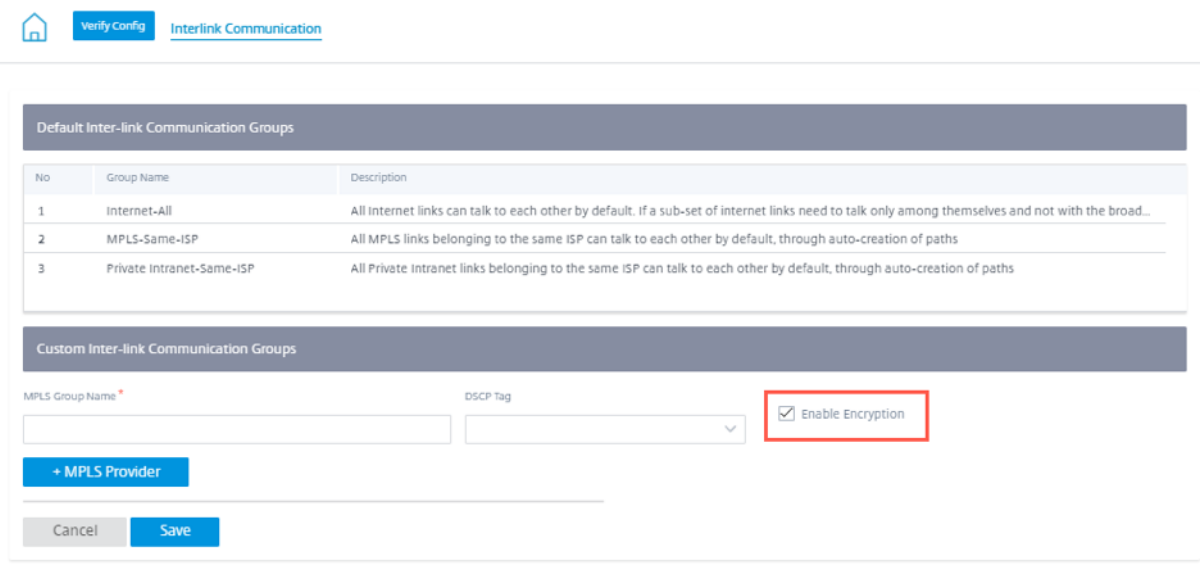
Benutzerdefinierte Inter-Link-Kommunikationsgruppen ermöglichen es privaten Intranet-, öffentlichen Internet- oder MPLS-Links, automatisch Pfade mit anderen privaten Intranet-, öffentlichen Internet- oder MPLS-Links bei verschiedenen Dienstanbietern zu erstellen.

Betrachten Sie zum Beispiel dieses Szenario: Ein Unternehmen hat Niederlassungen in den USA und Indien. Die US-Büros verwenden AT&T MPLS-Verbindungen, während die Büros in Indien Airtel MPLS-Verbindungen verwenden. Nehmen wir an, AT&T- und Airtel MPLS-Links sind in Bezug auf DSCP-Tags und verwandte Parameter kompatibel und für die Erstellung von Pfaden untereinander geeignet. Mit benutzerdefinierten Interlink-Kommunikationsregeln können Sie ein ISP-Paar auswählen (in diesem Fall z. B. ATT —Airtel) und die automatische Erstellung von Pfaden zwischen den Links dieser ISPs aktivieren.



- **MPLS-Gruppen**: Sie können die gewünschten MPLS-Dienstanbieternamen gruppieren, damit die entsprechenden Links miteinander kommunizieren können. Klicken Sie auf **+ MPLS Interlink Communication Group** und geben Sie einen MPLS-Gruppennamen an. Wählen Sie das DSCP-Tag aus der Dropdownliste aus. Sie können den MPLS-Anbieter auch hinzufügen, indem Sie den Namen des Internetdienstanbieters aus der Dropdownliste auswählen. Das Kontrollkästchen **Verschlüsselung aktivieren** hilft dabei, die Verschlüsselung für jede benutzerdefinierte MPLS Inter-Link Communication Group zu aktivieren. In seltenen Fällen können Sie diese Option deaktivieren, um den Verschlüsselungsaufwand zu vermeiden.
- **Private Intranetgruppen**: Sie können die Namen der gewünschten Intranetdienstanbieter gruppieren, damit die entsprechenden Links miteinander kommunizieren können. Klicken Sie auf **+ Privates Intranet Interlink Communication Group** und geben Sie den Namen der privaten Intranetgruppe an. Wählen Sie das DSCP-Tag aus der Dropdownliste aus. Sie können den privaten Intranet-Anbieter auch hinzufügen, indem Sie den Namen des Internetdienstanbieters aus der Dropdownliste auswählen. Das Kontrollkästchen **Verschlüsselung aktivieren** hilft dabei, die Verschlüsselung für jede benutzerdefinierte private Intranet-Inter-Link-Kommunikationsgruppe zu aktivieren/deaktivieren.
- **Gruppen zum Außerkraftsetzen der Internetkommunikation**: Wenn eine Teilmenge der Internetverbindungen nur untereinander und nicht mit den übrigen Internetverbindungen kommunizieren darf, können Sie die entsprechenden ISP-Namen gruppieren, um den Ausschluss aus der Standardgruppe zu aktivieren.

Die restlichen Internet-Links können weiterhin miteinander kommunizieren. Klicken Sie auf **+ Öffentliches Internet Interlink Communication Group** und geben Sie einen öffentlichen Internetgruppennamen an. Wählen Sie das DSCP-Tag aus der Dropdownliste aus. Sie können den öffentlichen Internetanbieter auch hinzufügen, indem Sie den Namen des Internetdienstanbieters aus der Dropdownliste auswählen. Die Option **Enable Encryption** stellt sicher, dass die Pakete der Inter-Link Communication Group, die auf den virtuellen Pfaden gesendet werden, verschlüsselt werden.



Sicherheit

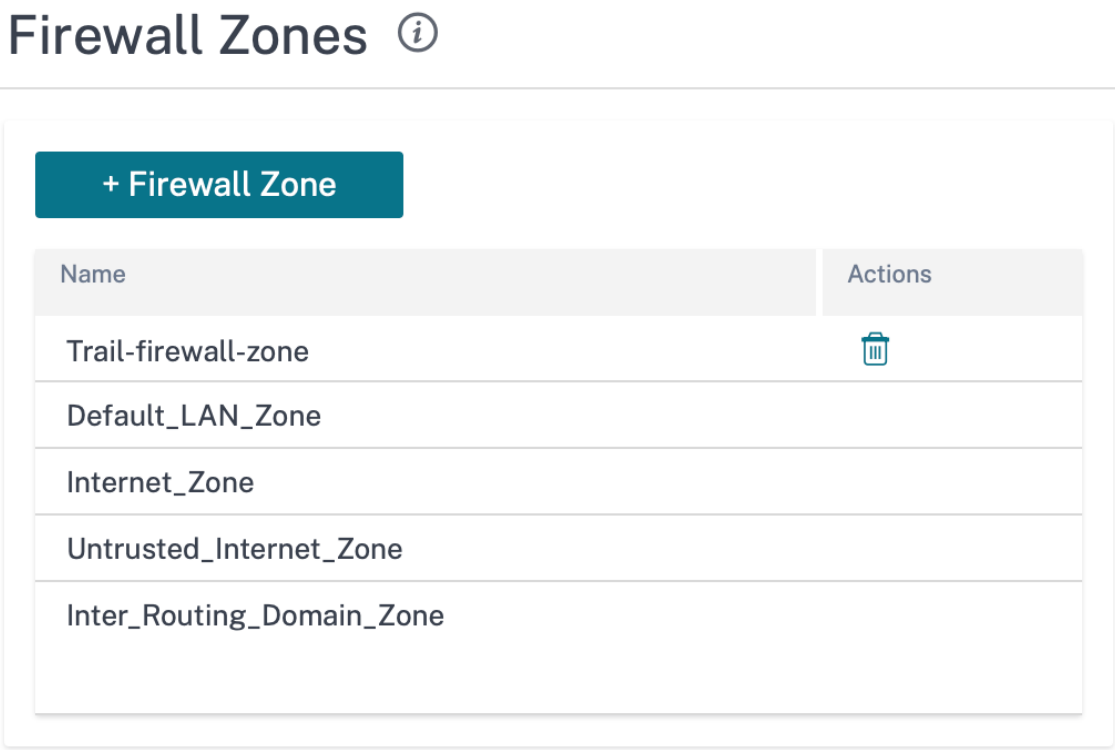
October 21, 2022

Sie können die Sicherheitseinstellungen wie Netzwerksicherheit, IPSec des virtuellen Pfads, Firewall und Zertifikate konfigurieren, die für alle Appliances im Netzwerk gelten.

Firewall-Zonen

Sie können Zonen im Netzwerk konfigurieren und Richtlinien definieren, um zu steuern, wie der Datenverkehr in die Zonen ein- und ausläuft. Die folgenden Zonen sind standardmäßig verfügbar:

- **default_LAN_ZONE**: Gilt für Datenverkehr zu oder von einem Objekt mit einer konfigurierbaren Zone, in der die Zone nicht festgelegt wurde.
- **Internet_Zone**: Gilt für Datenverkehr zu oder von einem Internetdienst über eine vertrauenswürdige Schnittstelle.
- **Untrusted_Internet_Zone**: Gilt für Datenverkehr zu oder von einem Internetdienst, der eine nicht vertrauenswürdige Schnittstelle verwendet.



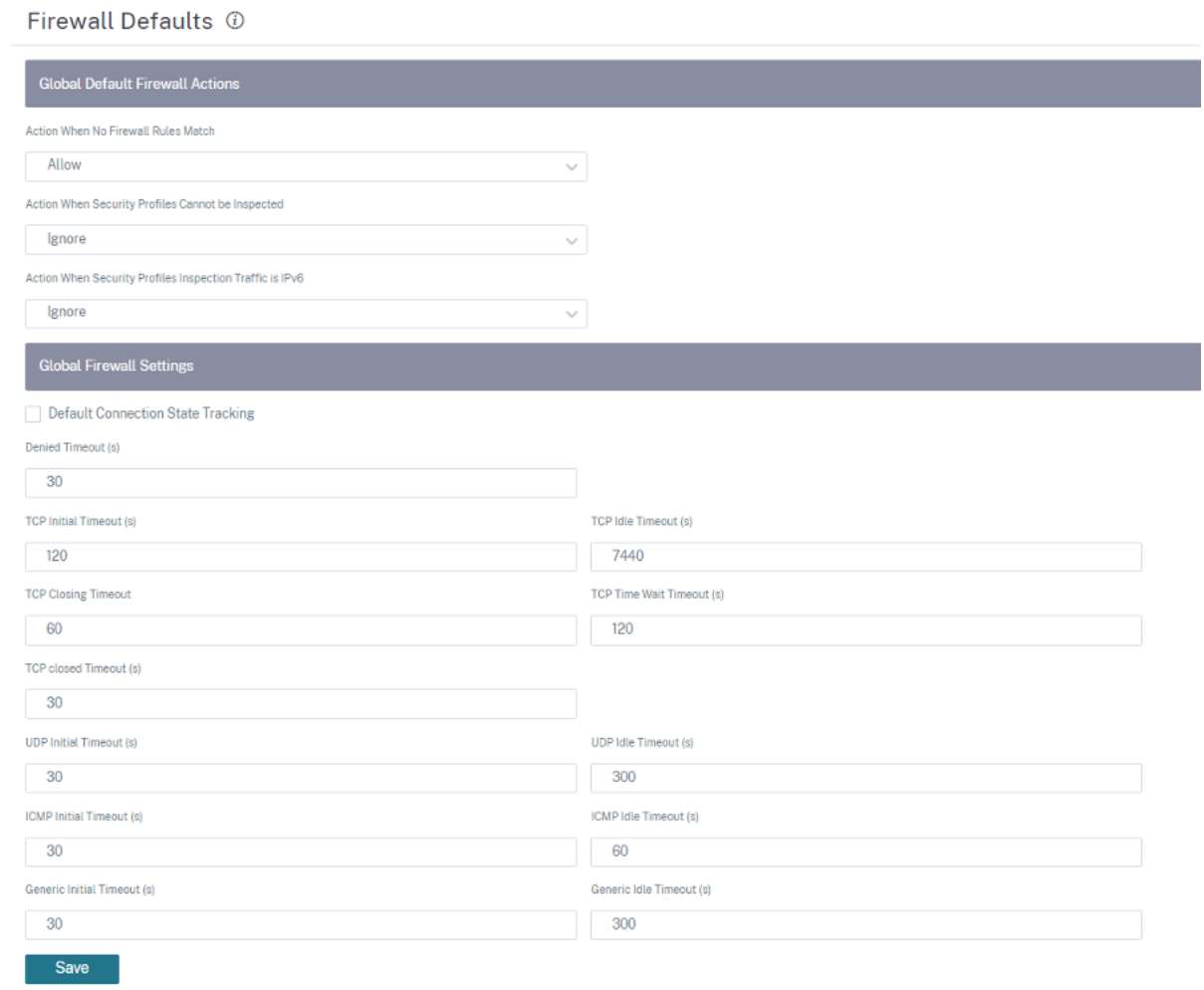
Sie können auch eigene Zonen erstellen und sie den folgenden Objekttypen zuweisen:

- Virtuelle Netzwerkschnittstellen
- Intranetdienste
- GRE Tunnel
- LAN IPsec-Tunnel

Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen.

Firewall-Standardeinstellungen

Sie können die globalen Standard-Firewallaktionen und globalen Firewalleinstellungen konfigurieren, die auf alle Appliances im SD-WAN-Netzwerk angewendet werden können. Die Einstellungen können auch auf Standortebene definiert werden, wodurch die globale Einstellung außer Kraft gesetzt wird.



- **Aktion, wenn keine Firewallregeln übereinstimmen**: Wählen Sie eine Aktion (Zulassen oder Löschen) aus der Liste für die Pakete aus, die nicht mit einer Firewall-Richtlinie übereinstimmen.
- **Aktion, wenn Sicherheitsprofile nicht überprüft werden können**: Wählen Sie eine Aktion (Ignorieren oder Verwerfen) für die Pakete aus, die einer Firewallregel entsprechen und ein Sicherheitsprofil aktivieren, aber vorübergehend nicht vom Edge-Security-Subsystem überprüft werden können. Wenn Sie **Ignorieren**auswählen, wird die entsprechende Firewallregel als nicht übereinstimmend behandelt, und die nächste Firewallregel wird in der Reihenfolge ausgewertet. Wenn Sie **Drop**auswählen, werden die Pakete, die der entsprechenden Firewall-Regel entsprechen, verworfen.
- **Standard-Firewall-Aktion**: Wählen Sie eine Aktion (Zulassen/Verwerfen) aus der Liste für Pakete aus, die nicht mit einer Richtlinie übereinstimmen.
- **Standardmäßige Verbindungsstatusverfolgung**: Aktiviert die direktionale Verbindungsstatusverfolgung für TCP-, UDP- und ICMP-Flows, die keiner Filterrichtlinie oder NAT-Regel entsprechen.

> **Hinweis**
>
> Asymmetrische Datenflüsse werden blockiert, wenn die **Standardverfolgung des Verbindungsstatus** aktiviert ist, auch wenn keine Firewall-Richtlinien definiert sind. Wenn an einem Standort die Möglichkeit asymmetrischer Datenflüsse besteht, wird empfohlen, diese auf Standort- oder Richtlinienebene und nicht global zu aktivieren.

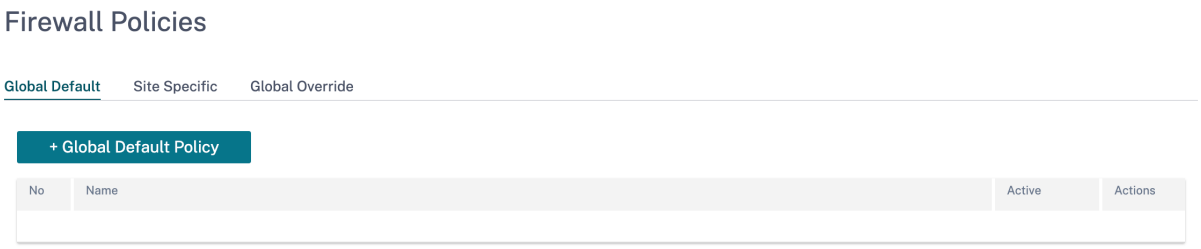
- **Verweigerte Timeout (s)**: Zeit (in Sekunden), um auf neue Pakete zu warten, bevor verweigerte Verbindungen geschlossen werden.
- **TCP-Anfangs-Timeout (s)**: Zeit (in Sekunden), um auf neue Pakete zu warten, bevor eine unvollständige TCP-Sitzung geschlossen wird.
- **TCP-Leerlauf-Timeout (s)**: Zeit (in Sekunden), um auf neue Pakete zu warten, bevor eine aktive TCP-Sitzung geschlossen wird.
- **TCP-Schließzeitlimit**: Zeit (in Sekunden), um auf neue Pakete zu warten, bevor eine TCP-Sitzung nach einer Termin-Anforderung geschlossen wird.
- **TCP-Zeitwarte-Timeouts (s)**: Zeit (in Sekunden), um auf neue Pakete zu warten, bevor eine beendete TCP-Sitzung geschlossen wird.
- **TCP-Zeitlimit für geschlossene**Pakete: Zeit (in Sekunden), um auf neue Pakete zu warten, bevor eine abgebrochene TCP-Sitzung geschlossen wird.
- **Anfängliche UDP-Timeout (s)**: Zeit (in Sekunden), um auf neue Pakete zu warten, bevor die UDP-Sitzung geschlossen wird, die keinen Datenverkehr in beide Richtungen gesehen hat.
- **UDP-Leerlauf-Timeout (s)**: Zeit (in Sekunden), um auf neue Pakete zu warten, bevor eine aktive UDP-Sitzung geschlossen wird.
- **ICMP Initial Timeout (s)**: Zeit (in Sekunden), um auf neue Pakete zu warten, bevor eine ICMP-Sitzung geschlossen wird, bei der kein Datenverkehr in beide Richtungen gesehen wurde
- **ICMP Idle Timeout (s)**: Zeit (in Sekunden), um auf neue Pakete zu warten, bevor eine aktive ICMP-Sitzung geschlossen wird.
- **Generisches anfängliches Timeout (s)**: Zeit (in Sekunden), um auf neue Pakete zu warten, bevor eine generische Sitzung geschlossen wird, in der kein Datenverkehr in beide Richtungen verzeichnet wurde.
- **Generisches Leerlauf-Timeout (s)**: Zeit (in Sekunden), um auf neue Pakete zu warten, bevor eine aktive generische Sitzung geschlossen wird.

Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen.

Firewall-Richtlinien

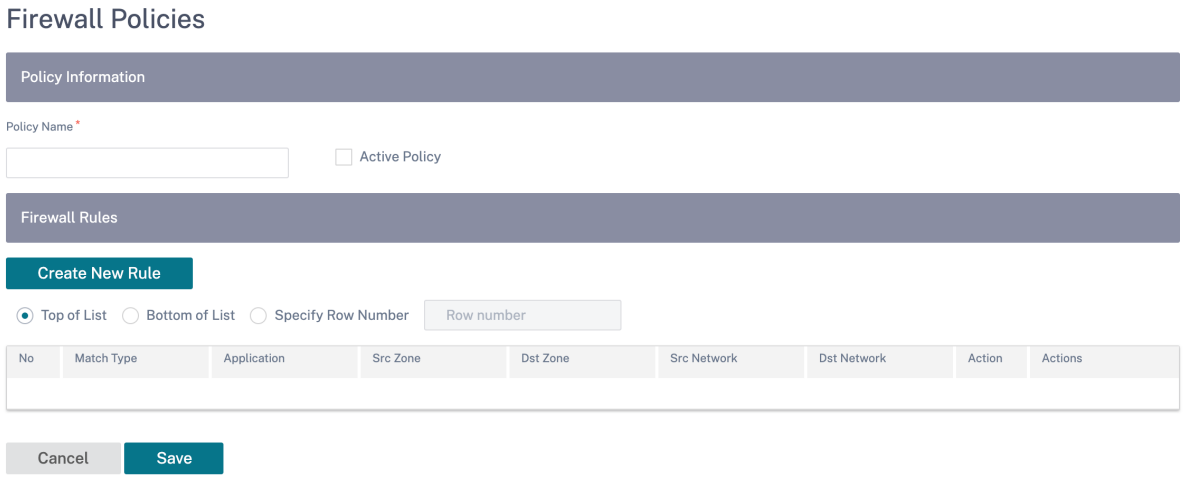
Firewall-Profile bieten Sicherheit, indem sichergestellt wird, dass der Netzwerkverkehr nur auf eine bestimmte Firewall-Regel beschränkt ist, abhängig von den Übereinstimmungskriterien und durch Anwendung spezifischer Aktionen. Die **Firewall-Richtlinien** bestehen aus drei Abschnitten.

- **Globaler Standard** —Die globale Standardrichtlinie ist eine Zusammenfassung einiger Firewall-regeln. Die Richtlinie, die Sie im Abschnitt **Global Default** erstellen, wird auf alle Standorte im Netzwerk angewendet.
- **Site-spezifisch** —Sie können die definierten Firewallregeln auf bestimmte Sites anwenden.
- **Globale Außerkraftsetzung** —Mit der globalen Override-Richtlinie können Sie sowohl **globale als auch standortspezifische Richtlinien außer**

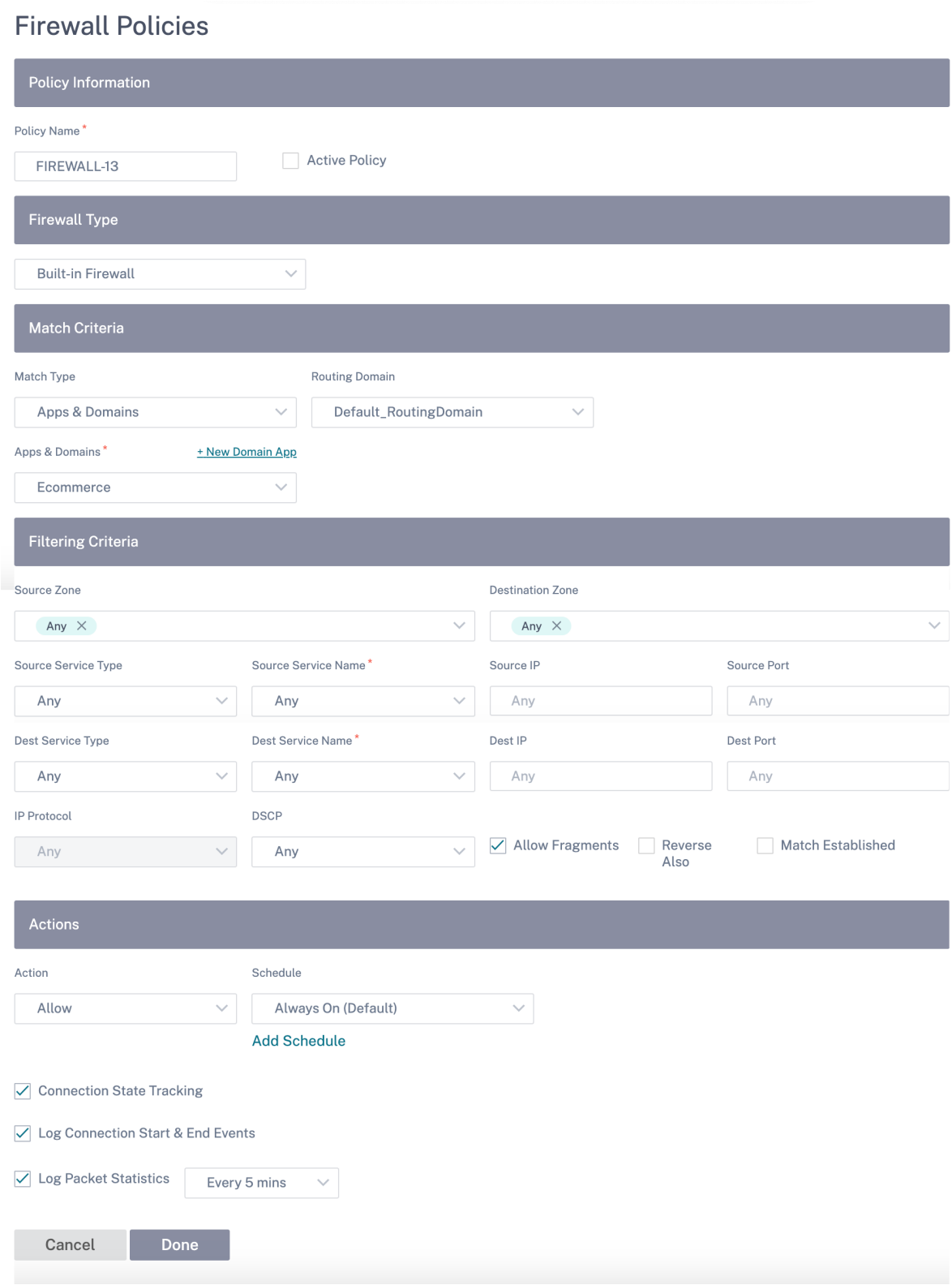


Sie können Firewallregeln definieren und sie basierend auf der Priorität platzieren. Sie können die Prioritätsreihenfolge auswählen, um am Anfang der Liste, am Ende der Liste oder in einer bestimmten Zeile zu beginnen.

Es wird empfohlen, am Anfang spezifischere Regeln für Anwendungen oder Unteranwendungen zu haben, gefolgt von weniger spezifischen Regeln für diejenigen, die einen breiteren Datenverkehr darstellen.



Um eine Firewallregel zu erstellen, klicken Sie auf **Neue Regel erstellen**.



- Geben Sie einen Richtliniennamen an, und aktivieren Sie das Kontrollkästchen **Aktive Richtlinie**, wenn Sie alle Firewallregeln anwenden möchten.

- Die Übereinstimmungskriterien definieren den Datenverkehr für die Regel, z. B. eine Anwendung, eine benutzerdefinierte Anwendung, eine Gruppe von Anwendungen, eine Anwendungsfamilie oder ein IP-Protokoll basierend.
- Filter-Kriterien:
  - **Quellzone**: Die Quell-Firewallzone.
  - **Zielzone**: Die Ziel-Firewallzone.
  - **Quelldiensttyp**: Der Quell-SD-WAN-Diensttyp —Lokal, Virtueller Pfad, Intranet, IP-Host oder Internet sind Beispiele für Diensttypen.
  - **Quelldienstname**: Der Name eines Dienstes, der an den Diensttyp gebunden ist. Wenn beispielsweise der virtuelle Pfad für den Quelldiensttyp ausgewählt ist, wäre dies der Name des spezifischen virtuellen Pfads. Dies ist nicht immer erforderlich und hängt vom ausgewählten Servicetyp ab.
  - **Quell-IP**: Die IP-Adresse und Subnetzmaske, mit der die Regel übereinstimmt.
  - **Quellport**: Der Quellport, den die spezifische Anwendung verwendet.
  - **Testdiensttyp**: Der SD-WAN-Zieldiensttyp —Lokal, Virtueller Pfad, Intranet, IP-Host oder Internet sind Beispiele für Diensttypen.
  - **Dest Service Name**: Name eines Dienstes, der an den Diensttyp gebunden ist. Dies ist nicht immer erforderlich und hängt vom ausgewählten Servicetyp ab.
  - **Ziel-IP**: Die IP-Adresse und Subnetzmaske, die der Filter für die Übereinstimmung verwendet.
  - **Zielport**: Der Zielport, den die spezifische Anwendung verwendet (d. h. HTTP-Zielport 80 für das TCP-Protokoll).
  - **IP-Protokoll**: Wenn dieser Übereinstimmungstyp ausgewählt ist, wählen Sie ein IP-Protokoll aus, mit dem die Regel übereinstimmt. Zu den Optionen gehören ANY, TCP, UDP, ICMP und so weiter.
  - **DSCP**: Ermöglicht dem Benutzer, eine Übereinstimmung mit einer DSCP-Tag-Einstellung vorzunehmen.
  - **Fragmente zulassen**: Erlaubt IP-Fragmente, die dieser Regel entsprechen.
  - **Auch umkehren**: Fügen Sie automatisch eine Kopie dieser Filterrichtlinie hinzu, wobei die Quell- und Zieleinstellungen umgekehrt sind.
  - **Übereinstimmung eingerichtet**: Ordnen Sie eingehende Pakete einer Verbindung zu, für die ausgehende Pakete zulässig waren.
- Die folgenden Aktionen können für einen übereinstimmenden Flow ausgeführt werden:

- **Zulassen**: Erlaubt den Durchfluss durch die Firewall.
- **Drop**: Verweigern Sie den Durchfluss durch die Firewall, indem Sie die Pakete löschen.
- **Ablehnen**: Verweigern Sie den Durchfluss durch die Firewall und senden Sie eine protokollspezifische Antwort. TCP sendet einen Reset, ICMP sendet eine Fehlermeldung.
- **Zählen und fortfahren**: Zählen Sie die Anzahl der Pakete und Bytes für diesen Flow und fahren Sie dann in der Richtlinienliste fort.

Neben der Definition der auszuführenden Aktion können Sie auch die zu erfassenden Protokolle auswählen.

Netzwerksicherheit

Wählen Sie den Verschlüsselungsmechanismus aus, der im Netzwerk verwendet werden soll. Sie können die globalen Sicherheitseinstellungen konfigurieren, die das gesamte SD-WAN-Netzwerk schützen.

Der Netzwerkverschlüsselungsmodus definiert den Algorithmus, der für alle verschlüsselten Pfade im SD-WAN-Netzwerk verwendet wird. Sie gilt nicht für unverschlüsselte Pfade. Sie können die Verschlüsselung auf AES-128 oder AES-256 festlegen.

FIPS-Konformität

Im FIPS-Modus müssen Benutzer FIPS-konforme Einstellungen für ihre IPSec-Tunnel und IPSec-Einstellungen für virtuelle Pfade konfigurieren.

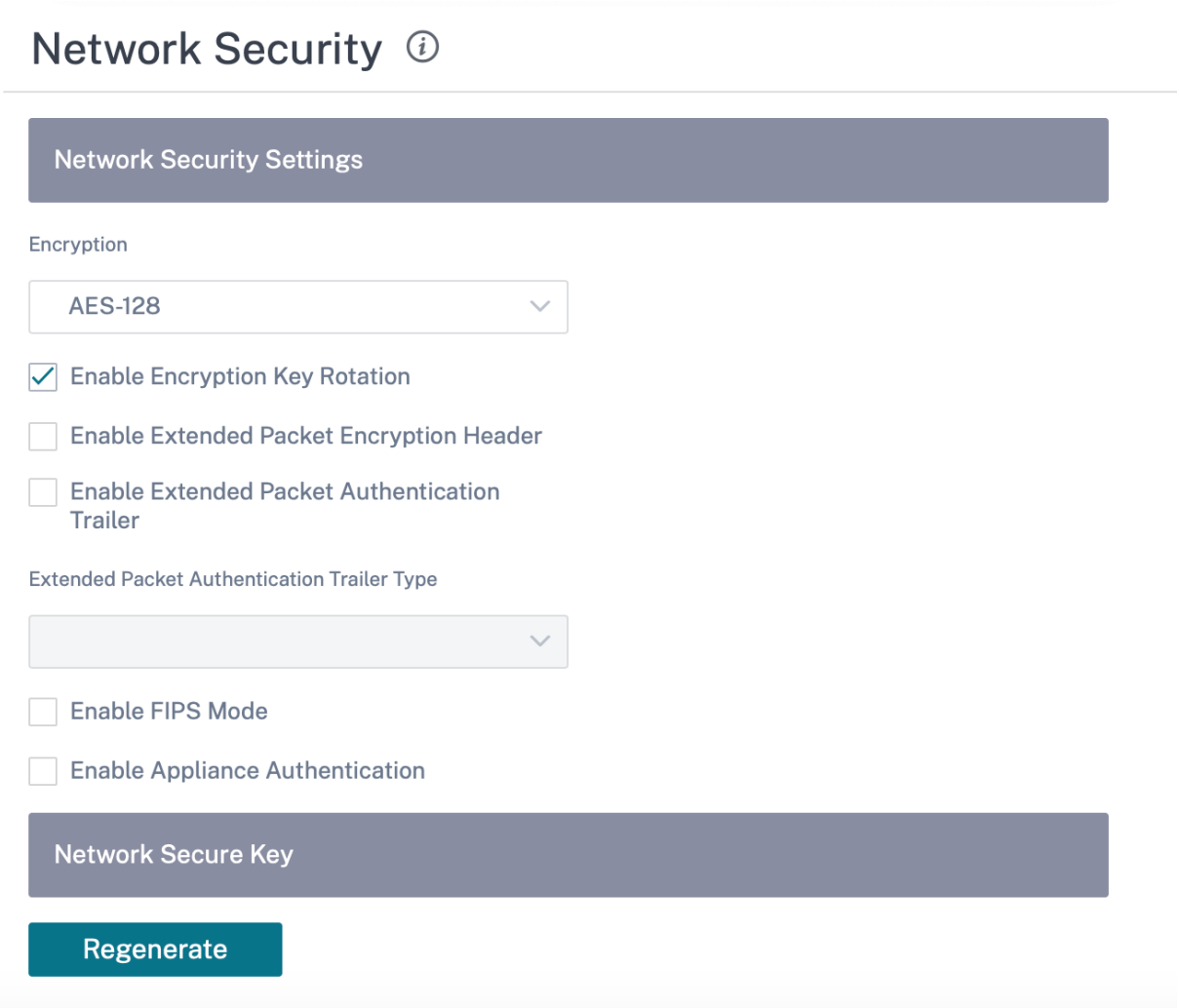
Die Aktivierung des FIPS-Modus bietet die folgenden Funktionen:

- Zeigt den FIPS-konformen IKE-Modus an.
- Zeigt eine FIPS-konforme IKE DH-Gruppe an, aus der Benutzer die erforderlichen Parameter für die Konfiguration der Appliance im FIPS-konformen Modus auswählen können (2,5,14 —21).
- Zeigt den FIPS-kompatiblen IPsec-Tunneltyp in IPsec-Einstellungen für virtuelle Pfade an
- IKE-Hash- und (IKEv2) Integritätsmodus, IPsec-Authentifizierungsmodus.
- Führt Überwachungsfehler für FIPS-basierte Lebensdauereinstellungen durch.

So aktivieren Sie die FIPS-Konformität für den Citrix SD-WAN Orchestrator Service:

1. Gehen Sie zu **Konfiguration** > **Sicherheit** > **Netzwerksicherheit**.
2. Klicken Sie im Abschnitt **Netzwerksicherheitseinstellungen** auf das Kontrollkästchen **FIPS-Modus aktivieren** .

Das Aktivieren des FIPS-Modus erzwingt Überprüfungen während der Konfiguration, um sicherzustellen, dass alle IPSec-bezogenen Konfigurationsparameter den FIPS-Standards entsprechen. Sie werden durch Audit-Fehler und Warnungen zur Konfiguration von IPsec aufgefordert.



Wenn die IPSec-Konfiguration bei Aktivierung nicht den FIPS-Standards entspricht, wird möglicherweise ein Überwachungsfehler ausgelöst. Im Folgenden sind die Arten von Überwachungsfehlern aufgeführt, die angezeigt werden, wenn Sie auf der Benutzeroberfläche von Citrix SD-WAN Orchestrator for On-premises auf **Konfiguration überprüfen** klicken.

- Wenn der FIPS-Modus aktiviert ist und die Option Nicht FIPS-konform ausgewählt ist.
- Wenn der FIPS-Modus aktiviert ist und ein falscher Lebensdauerwert eingegeben wurde.
- Wenn der FIPS-Modus aktiviert ist und die IPSec-Einstellungen für virtuelle Pfade ebenfalls aktiviert sind und ein falscher Tunnelmodus ausgewählt ist (ESP vs. ESP_Auth /AH).
- Wenn der FIPS-Modus aktiviert ist, werden auch die IPSec-Einstellungen für die Standardeinstellung des virtuellen Pfads aktiviert, und es wird ein falscher Lebensdauerwert eingegeben.

Enable Encryption Key Rotation: Wenn diese Option aktiviert ist, werden Verschlüsselungsschlüssel

in Intervallen von 10—15 Minuten gedreht.

Extended Packet Encryption Header aktivieren: Wenn diese Option aktiviert ist, wird ein 16-Byte-verschlüsselter Zähler dem verschlüsselten Datenverkehr vorangestellt, um als Initialisierungsvektor zu dienen und die Paketverschlüsselung zufällig zu machen.

Extended Packet Authentication Trailer aktivieren: Wenn diese Option aktiviert ist, wird ein Authentifizierungscode an den Inhalt des verschlüsselten Datenverkehrs angehängt, um zu überprüfen, ob die Nachricht unverändert zugestellt wird.

Trailertyp für erweiterte Paketauthentifizierung: Dies ist der Anhängertyp, der zur Validierung des Paketinhalts verwendet wird. Wählen Sie eine der folgenden Optionen aus dem Dropdownmenü: **32-Bit-Prüfsumme** oder **SHA-256**.

SSL Inspektion

Die Secure Sockets Layer (SSL) -Inspektion ist ein Prozess zum Abfangen, Entschlüsseln und Scannen des HTTPS- und sicheren SMTP-Datenverkehrs auf schädliche Inhalte. Die SSL-Überprüfung bietet Sicherheit für den Datenverkehr, der zu und von Ihrem Unternehmen fließt. Sie können das Stammzertifizierungsstellenzertifikat Ihrer Organisation generieren und hochladen und die Man-in-the-Middle-Inspektion des Datenverkehrs durchführen.

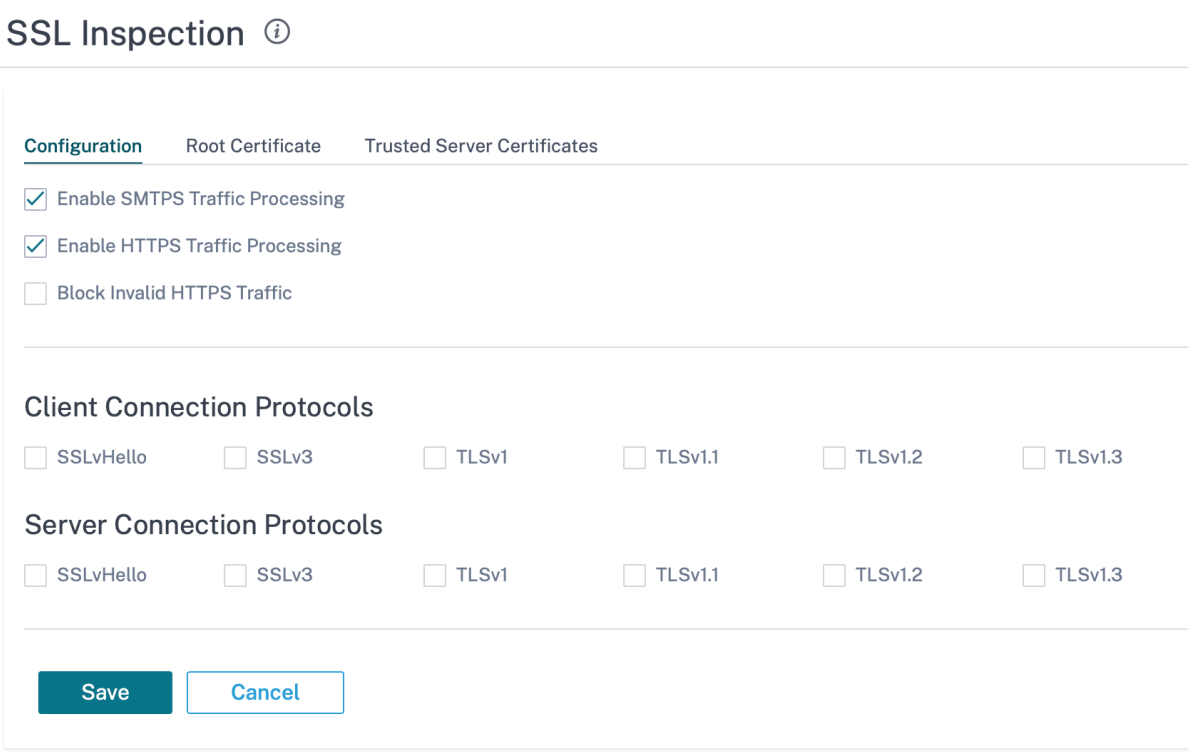
> **HINWEIS:**
>
> Die SSL-Inspektion wird ab der Version Citrix SD-WAN 11.3.0 unterstützt.

Um die SSL-Überprüfung zu aktivieren, navigieren Sie auf Netzwerkebene zu **Konfiguration > Sicherheit > SSL-Inspektion > Konfiguration**, und definieren Sie die folgenden SSL-Konfigurationseinstellungen.

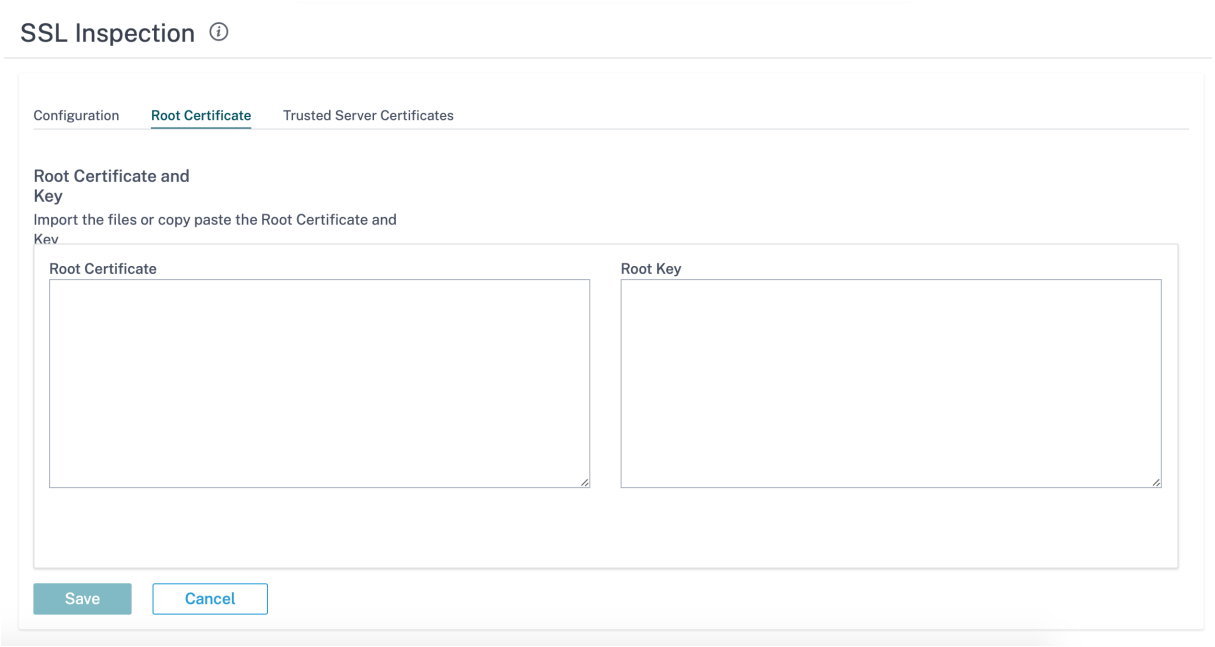
- **SMTPS-Datenverkehrsverarbeitung aktivieren**: Der sichere SMTP-Datenverkehr wird einer SSL-Überprüfung unterzogen.
- **HTTPS-Verkehrsverarbeitung aktivieren**: Der HTTPS-Datenverkehr wird einer SSL-Überprüfung unterzogen.
- **Ungültigen HTTPS-Verkehr blockieren**: Wenn das Kontrollkästchen **Ungültigen HTTPS-Verkehr blockieren** deaktiviert ist, wird Nicht-HTTPS-Datenverkehr auf Port 443 standardmäßig ignoriert und darf ungehindert fließen. Wenn **Ungültigen HTTPS-Verkehr blockieren** ausgewählt ist, wird Nicht-HTTPS-Datenverkehr für die SSL-Überprüfung blockiert. Das Aktivieren dieser Option kann dazu führen, dass ansonsten legitimer Datenverkehr blockiert wird, d. h. HTTP-Verkehr auf Port 443 oder HTTPS-Verkehr von Websites mit abgelaufenem Zertifikat.
- **Client-Verbindungsprotokolle**: Wählen Sie die erforderlichen Client-Protokolle aus. Die verfügbaren Protokolle sind SSLvHello, SSLv3, TLSv1, TSlV1.1, TLSv1.2 und TLSv1.3.

- **Serververbindungsprotokolle**: Wählen Sie die erforderlichen Serverprotokolle aus. Die verfügbaren Protokolle sind SSLvHello, SSLv3, TLSv1, TSlV1.1, TLSv1.2 und TLSv1.3.

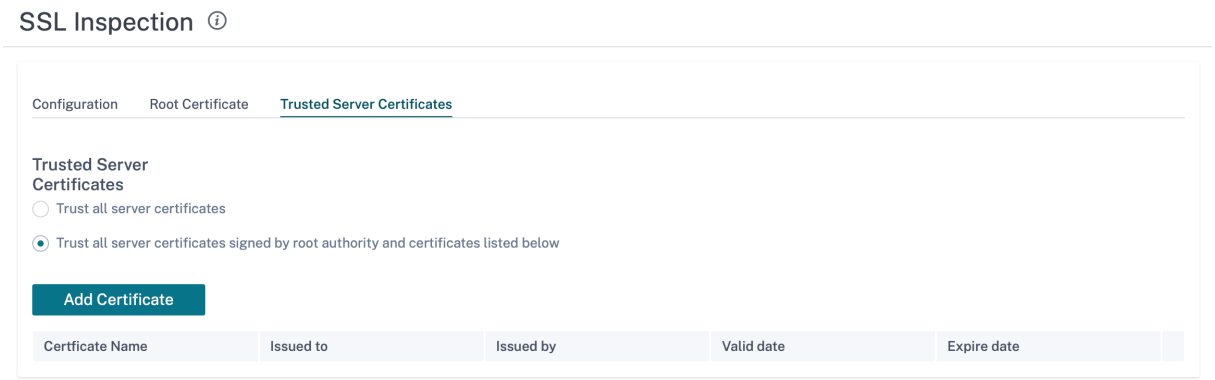
> **HINWEIS**
>
> Die Versionen älter als TLSv1.2 gelten als anfällig und dürfen nicht aktiviert werden, es sei denn, Abwärtskompatibilität ist wichtig.



Kopieren Sie auf der Registerkarte **Stammzertifikat** das Stammzertifikat und den Schlüssel der Root Certificate Authority (CA) Ihrer Organisation, und fügen Sie sie ein. Die Stammzertifizierungsstelle wird verwendet, um eine gefälschte Kopie der Zertifikate der ursprünglichen Sites zu erstellen und zu signieren, sodass eine SSL-Überprüfung durchgeführt werden kann. Es wird implizit angenommen, dass das Root-CA-Zertifikat auf allen Client-Arbeitsstationen und Geräten installiert ist, deren Datenverkehr SSL überprüft werden kann.



Die Standardoption **Allen Serverzertifikaten vertrauen, die von der Stammautorität signiert wurden, und den unten aufgeführten Zertifikaten** führt dazu, dass SD-WAN alle Serverzertifikate anhand der Standardliste der Stammzertifizierungsstellen und der zuvor konfigurierten Stammzertifizierungsstelle validiert. Außerdem werden Server verworfen, die über ein ungültiges Zertifikat verfügen. Um dieses Verhalten außer Kraft zu setzen, laden Sie das selbstsignierte SSL-Zertifikat interner Server auf der Registerkarte **Trusted Server Certificates** hoch. Klicken Sie auf **Zertifikat hinzufügen**, geben Sie einen Namen ein, suchen Sie nach dem Zertifikat und laden Sie es hoch. Wenn Sie **Alle Serverzertifikate vertrauen**auswählen, werden alle Server unabhängig von ihrem Zertifikatvalidierungsstatus von Citrix SD-WAN als vertrauenswürdig angesehen.



Als Teil von Sicherheitsprofilen können Sie SSL-Regeln erstellen und diese für die SSL-Überprüfung aktivieren. Weitere Informationen zum Erstellen von SSL-Regeln für ein Sicherheitsprofil finden Sie unter Edge-Sicherheit.

Intrusion Prevention

Intrusion Prevention System (IPS) erkennt und verhindert, dass bösartige Aktivitäten in Ihr Netzwerk gelangen. IPS überprüft den Netzwerkverkehr und ergreift automatisierte Aktionen für alle eingehenden Verkehrsflüsse. Es enthält eine Datenbank mit über 34.000 Signaturerkennungen und heuristischen Signaturen für Portscans, sodass Sie die meisten verdächtigen Anfragen effektiv überwachen und blockieren können.

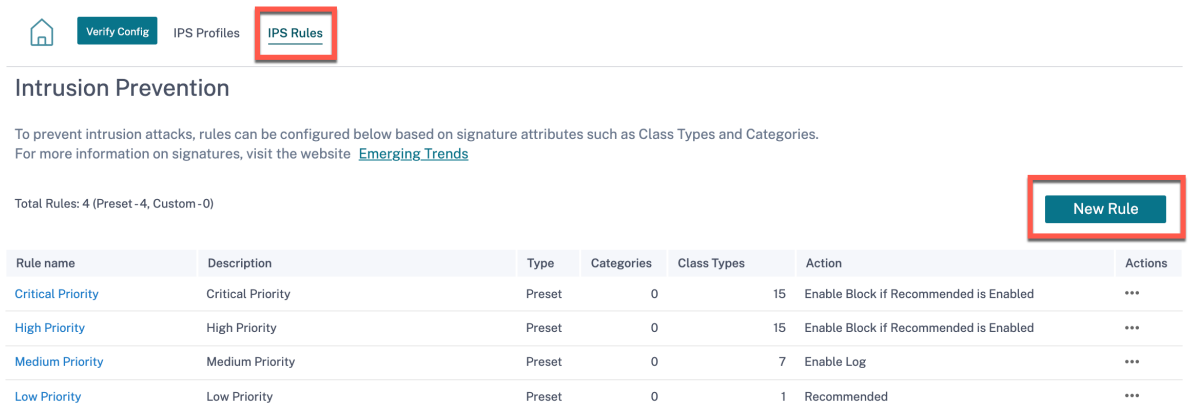
IPS verwendet eine signaturbasierte Erkennung, die die eingehenden Pakete mit einer Datenbank eindeutig identifizierbarer Exploit- und Angriffsmuster abgleicht. Die Signaturdatenbank wird täglich automatisch aktualisiert. Da es Tausende von Signaturen gibt, sind die Signaturen in Kategorie- und Klassentypen gruppiert.

Sie können IPS-Regeln erstellen und nur die Signaturkategorien oder Klassentypen aktivieren, die Ihr Netzwerk benötigt. Da es sich bei der Intrusion Prevention um einen rechnersensiblen Prozess handelt, sollten Sie nur die minimale Anzahl von Signaturkategorien oder Klassentypen verwenden, die für Ihr Netzwerk relevant sind.

Sie können ein IPS-Profil erstellen und eine Kombination von IPS-Regeln aktivieren. Diese IPS-Profile können dann global dem gesamten Netzwerk oder nur bestimmten Standorten zugeordnet werden.

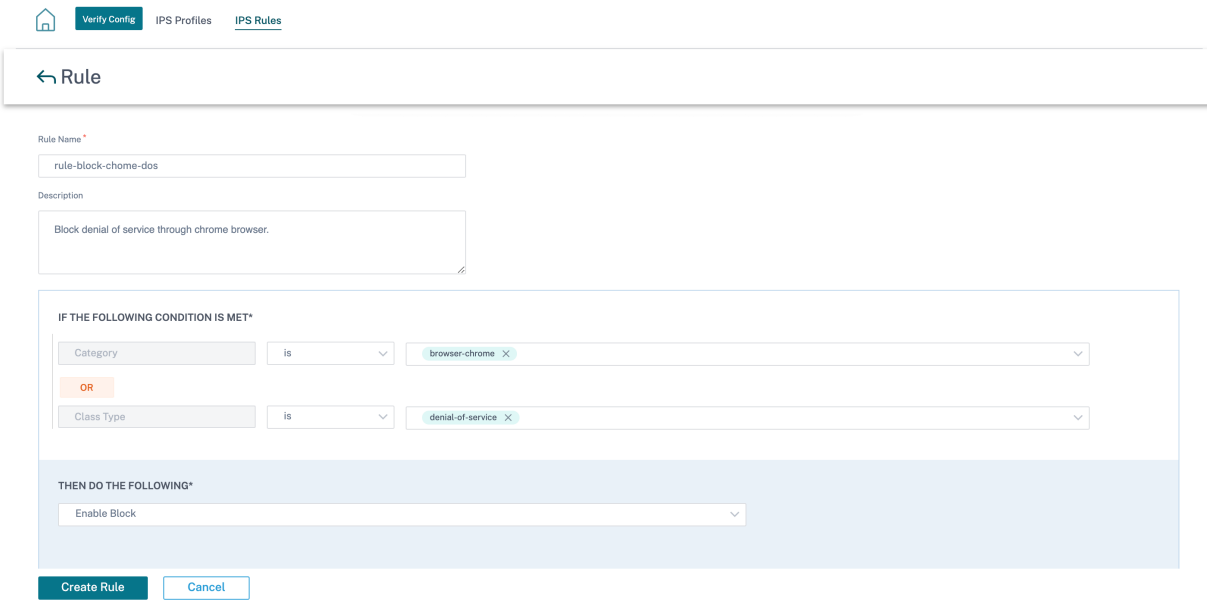
Jede Regel kann mehreren IPS-Profilen zugeordnet werden, und jedes IPS-Profil kann mehreren Standorten zugeordnet werden. Wenn ein IPS-Profil aktiviert ist, überprüft es den Netzwerkverkehr für die Standorte, denen das IPS-Profil zugeordnet ist, und für die IPS-Regeln, die in diesem Profil aktiviert sind.

Um IPS-Regeln zu erstellen, navigieren Sie auf Netzwerkebene zu **Konfiguration > Sicherheit > Intrusion Prevention > IPS-Regeln**, und klicken Sie auf **Neue Regel**.



Geben Sie einen Regelnamen und eine Beschreibung an. Wählen Sie die Signaturattribute für Übereinstimmungskategorie oder Klassentyp aus, wählen Sie eine Aktion für die Regel aus, und aktivieren Sie sie. Sie können aus den folgenden Regelaktionen wählen:

Regel-Aktion	Funktion
Empfohlen	Für jede Signatur sind empfohlene Maßnahmen festgelegt. Führen Sie die empfohlene Aktion für die Signaturen durch.
Log aktivieren	Erlauben und protokollieren Sie den Datenverkehr, der einer der Signaturen in der Regel entspricht.
Aktivieren Sie Blockieren wenn “Empfohlen” aktiviert	Wenn die Regelaktion „ **Empfohlen** “lautet und die empfohlene Aktion der Signatur „ **Protokoll aktivieren**“lautet, löschen Sie den Datenverkehr, der mit einer der Signaturen in der Regel übereinstimmt.
Blockieren aktivieren	Lassen Sie den Datenverkehr fallen, der mit einer der Signaturen in der Regel übereinstimmt.

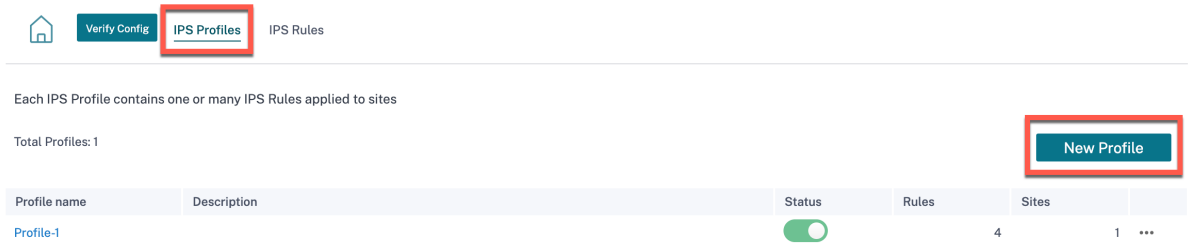


Hinweis

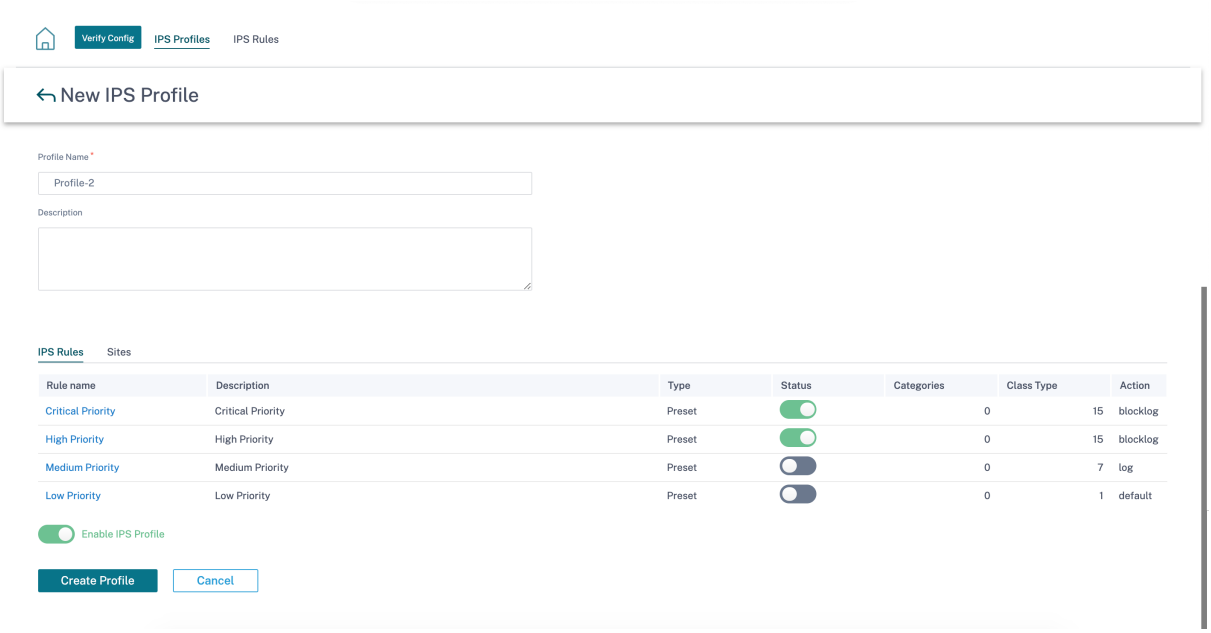
- Da es sich bei Intrusion Prevention um einen rechensensitiven Prozess handelt, verwenden Sie nur den minimalen Satz von Signaturkategorien, die für Ihre Edge-Sicherheitsbereitstellungen relevant sind.
- Die SD-WAN-Firewall senkt den Datenverkehr auf allen WAN L4-Ports, die nicht Port-Weiterleitung sind und in der IPS-Engine nicht sichtbar sind. Dies bietet eine zusätzliche

> Sicherheitsschicht gegen triviale DOS- und Scan-Angriffe.

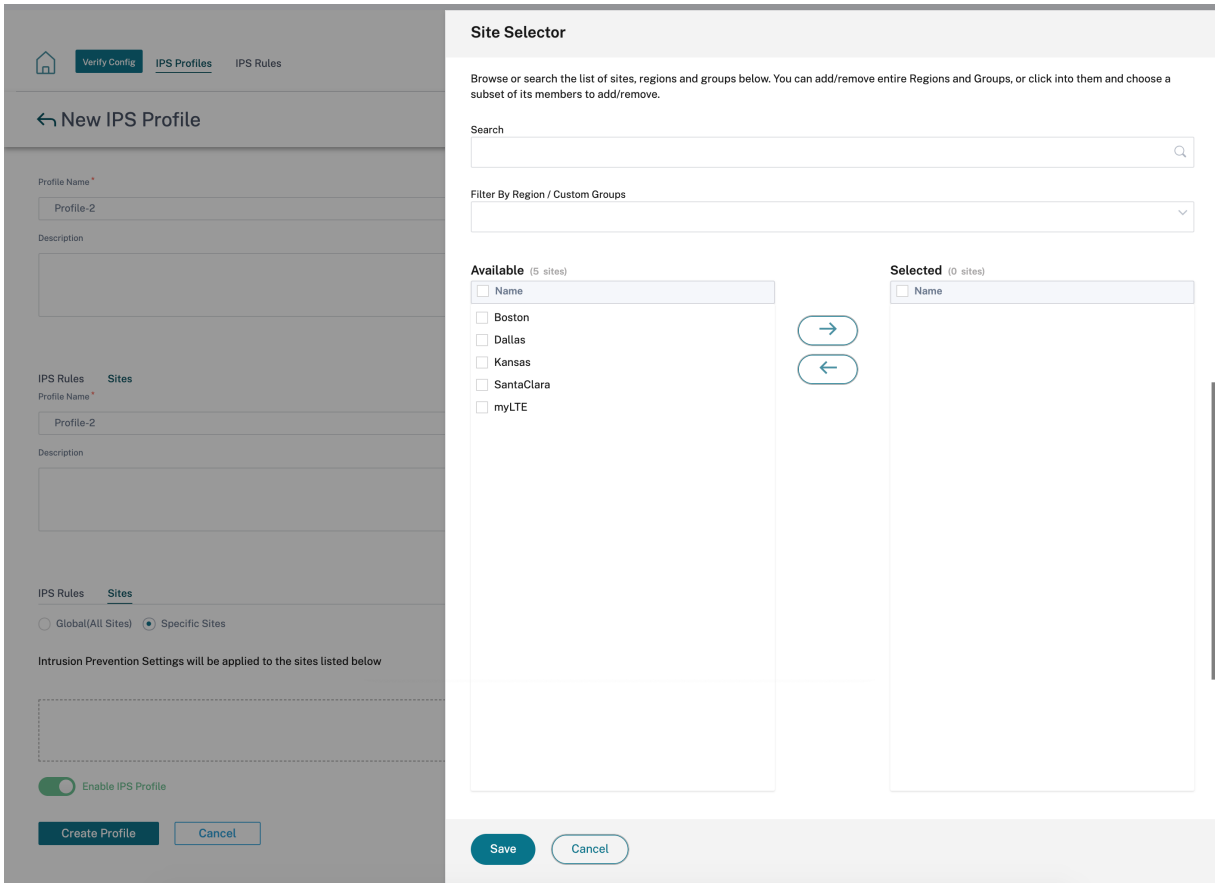
Um IPS-Profile zu erstellen, navigieren Sie auf Netzwerkebene zu **Konfiguration > Sicherheit > Intrusion Prevention > IPS-Profile**, und klicken Sie auf **Neues Profil**.



Geben Sie einen Namen und eine Beschreibung für das IPS-Profil an. Aktivieren Sie auf der Registerkarte **IPS-Regeln** die erforderlichen **IPS-Regeln** und aktivieren Sie **IPS-Profile aktivieren**.



Klicken Sie auf der Registerkarte **Sites** auf **Sites auswählen**. Wählen Sie die Websites und klicken Sie auf **Speichern**. Klicken Sie auf **Profil erstellen**.



Sie können diese IPS-Profile beim Erstellen von Sicherheitsprofilen aktivieren oder deaktivieren. Die Sicherheitsprofile werden verwendet, um Firewall-Regeln zu erstellen. Weitere Informationen finden Sie unter Sicherheitsprofil —Intrusion Prevention.

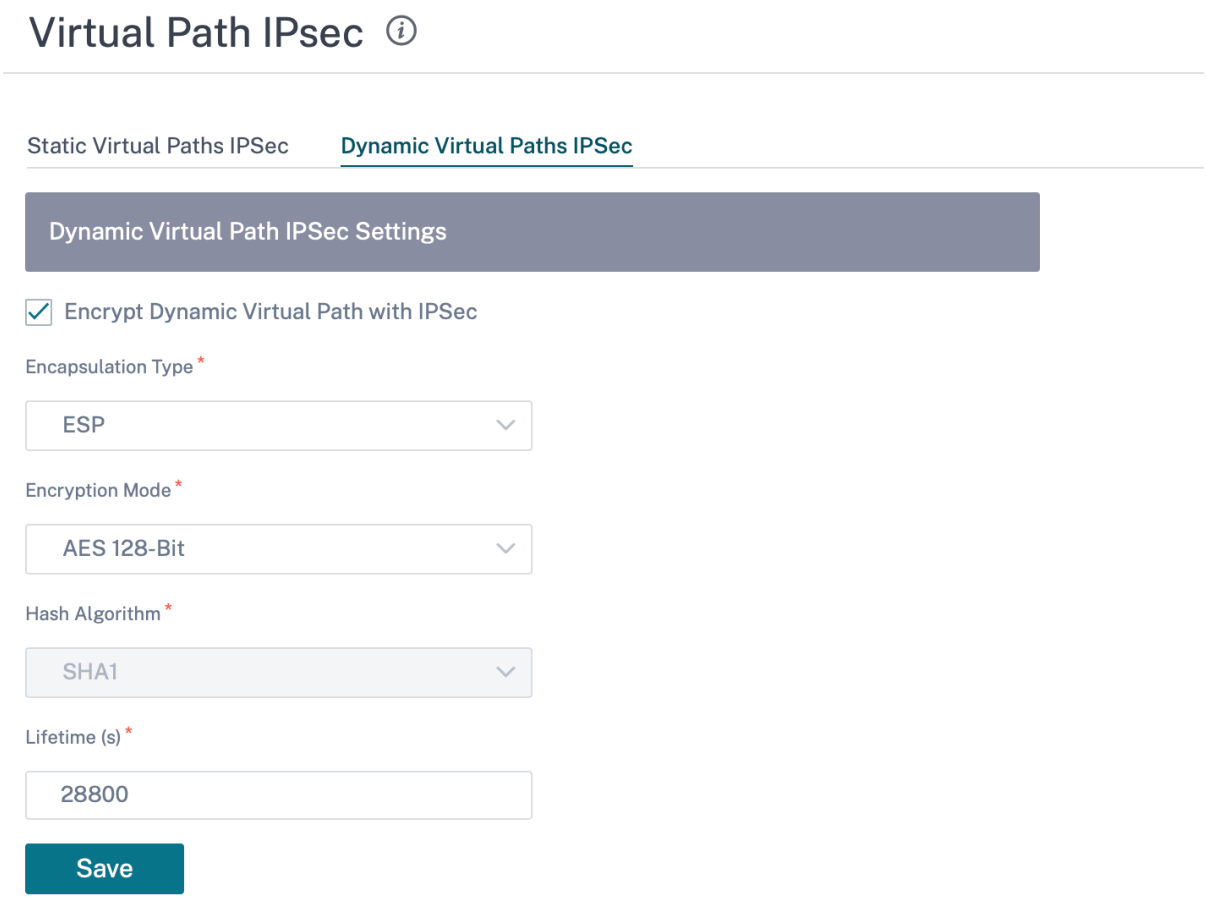
Virtueller Pfad IPSec

Virtual Path IPSec definiert die IPSec-Tunneleinstellungen, um eine sichere Übertragung von Daten über die statischen virtuellen Pfade und dynamischen virtuellen Pfade zu gewährleisten. Wählen Sie die Registerkarte **Statische virtuelle Pfade IPSec** oder **Dynamic Virtual Paths IPsec**, um die IPSec-Tunneleinstellungen zu definieren

- **Kapselungstyp**: Wählen Sie einen der folgenden Sicherheitstypen:
  - **ESP**: Daten sind gekapselt und verschlüsselt.
  - **ESP+Auth**: Daten werden mit einem HMAC gekapselt, verschlüsselt und validiert.
  - **AH**: Daten werden mit einem HMAC validiert.
- **Verschlüsselungsmodus**: Der bei aktiviertem ESP verwendete Verschlüsselungsalgorithmus.
- **Hash-Algorithmus**: Der Hash-Algorithmus, der zum Generieren eines HMAC verwendet wird.

- **Lebensdauer (en)**: Die bevorzugte Dauer in Sekunden, für die eine IPSec-Sicherheitszuordnung besteht. Geben Sie 0 für unbegrenzt ein.

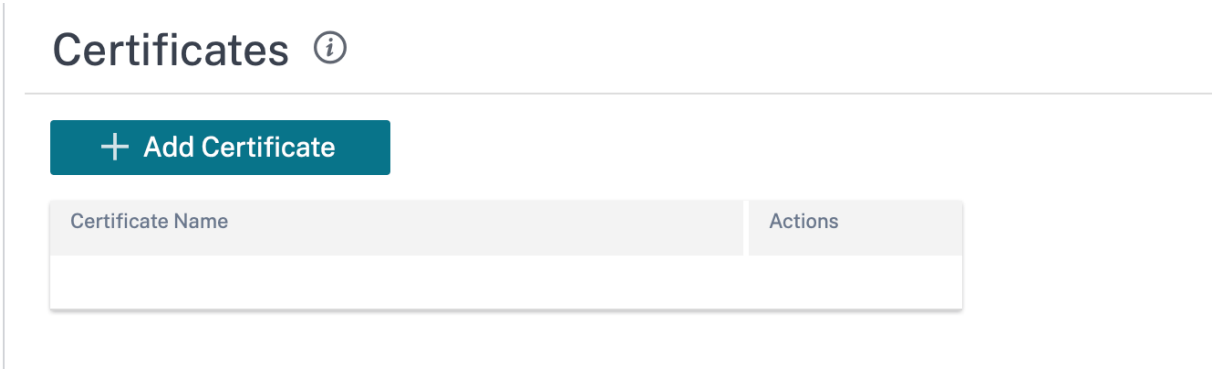
Informationen zum Konfigurieren des IPSec-Dienstes finden Sie unter IPSec-Dienst.



Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen

Zertifikate

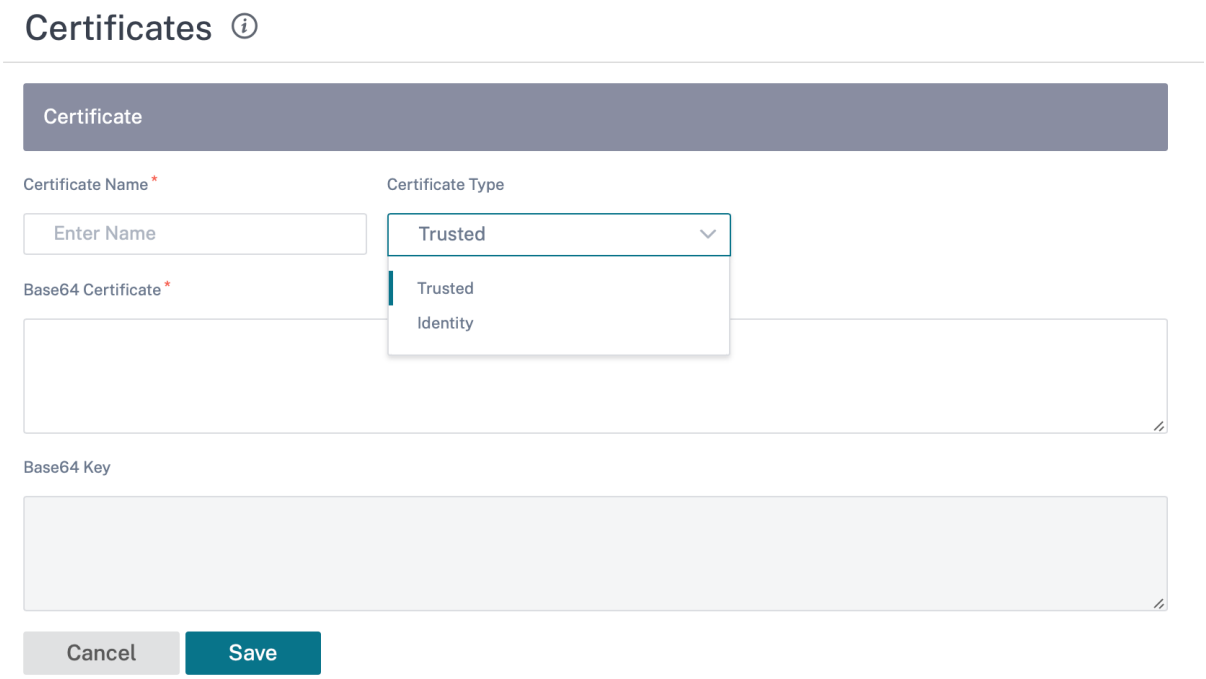
Es gibt zwei Arten von Zertifikaten: Identity und Trusted. Identitätszertifikate werden verwendet, um Daten zu signieren oder zu verschlüsseln, um den Inhalt einer Nachricht und die Identität des Absenders zu überprüfen. Vertrauenswürdige Zertifikate werden zur Überprüfung von Nachrichtensignaturen verwendet. Citrix SD-WAN-Appliances akzeptieren sowohl Identitäts- als auch vertrauenswürdige Zertifikate. Administratoren können Zertifikate im Konfigurationseditor verwalten.



Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen

Um ein Zertifikat hinzuzufügen, klicken Sie auf **Zertifikat hinzufügen**.

- **Zertifikatsname**: Geben Sie den Zertifikatsnamen an.
- **Zertifikatstyp**: Wählen Sie den Zertifikatstyp aus der Dropdownliste aus.
  - **Identitätszertifikate**: Identitätszertifikate erfordern, dass der private Schlüssel des Zertifikats dem Unterzeichner zur Verfügung steht. Identitätszertifikate oder deren Zertifikatsketten, denen ein Peer vertraut, um den Inhalt und die Identität des Absenders zu überprüfen. Die konfigurierten Identitätszertifikate und ihre jeweiligen Fingerabdrücke werden im Konfigurations-Editor angezeigt.
  - **Vertrauenswürdige Zertifikate**: Vertrauenswürdige Zertifikate sind selbstsignierte Zertifikate, Zwischenzertifikate der Zertifizierungsstelle (CA) oder Stammzertifizierungsstellen, die zur Überprüfung der Identität eines Peers verwendet Für ein vertrauenswürdiges Zertifikat ist kein privater Schlüssel erforderlich. Die konfigurierten vertrauenswürdigen Zertifikate und ihre jeweiligen Fingerabdrücke sind hier aufgelistet.

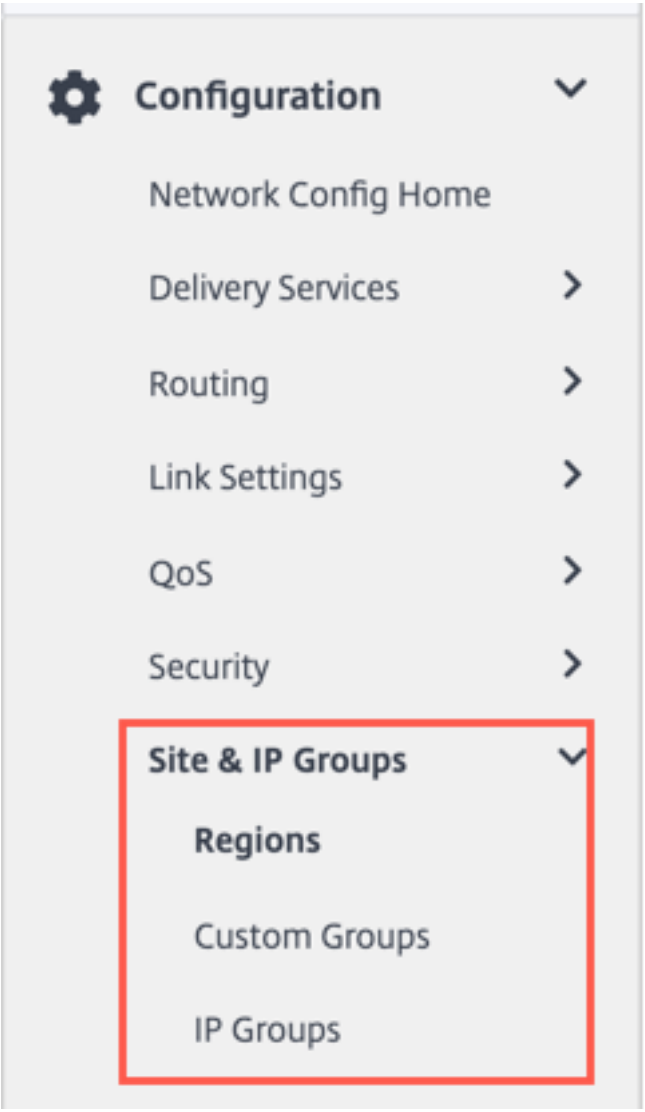


Site- und IP-Gruppen

October 21, 2022

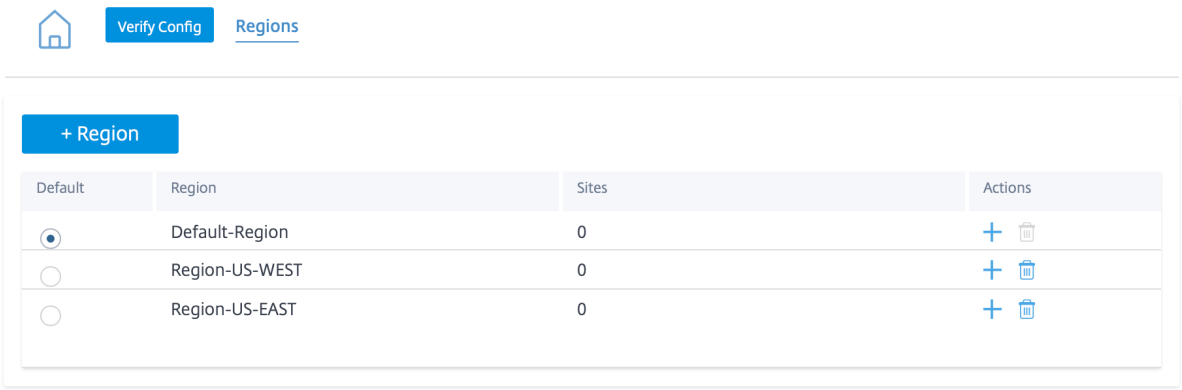
Administratoren können Standorte oder IP-Adressen gruppieren, um allgemeine Anwendungsrichtlinien über mehrere Standorte oder Netzwerkadressen hinweg zu vereinfachen, und auch als Filter für Berichte dienen.

Um Regionen, Standorte und IP-Gruppen anzuzeigen, navigieren Sie zu **Konfiguration** > **Standort- und IP-Gruppen**.



Regionen

Regionen tragen dazu bei, administrative Grenzen innerhalb großer Netzwerke zu schaffen, die Hunderte bis Tausende von Standorten umfassen. Wenn Ihre Organisation über ein großes Netzwerk verfügt, das sich über mehrere administrative (oder geografische) Grenzen erstreckt, können Sie Regionen erstellen, um das Netzwerk zu segmentieren.



Derzeit werden maximal 1000 Standorte pro Region unterstützt. Jede Region wird voraussichtlich über einen Regional Control Node (RCN) verfügen, der als Drehscheibe und Controller für die Region dient. Daher würden Sie in der Regel eine Bereitstellung mit mehreren Regionen in Betracht ziehen, wenn Ihr Netzwerk über mehr als 500 Standorte verfügt. Standardmäßig sind alle Netzwerke Netzwerke mit einer Region, wobei der Master Control Node (MCN) als Hub und Steuerknoten für alle Standorte dient. Beim Hinzufügen einer oder mehrerer Regionen wird das Netzwerk zu einem Netzwerk mit mehreren Regionen. Die mit dem MCN verknüpfte Region wird als **Standardregion**bezeichnet.

Ein Netzwerk mit mehreren Regionen unterstützt eine hierarchische Architektur mit einem MCN, der mehrere RCNs steuert. Jeder RCN wiederum kontrolliert mehrere Zweigstandorte. Selbst in einer Bereitstellung mit mehreren Regionen können Sie den MCN als direkten Hub-Knoten für eine Teilmenge der Sites verdoppeln, während der Rest der Sites ihre jeweiligen RCNs als Hub-Knoten verwenden lässt.

Die Standorte, die direkt vom MCN verwaltet werden, dh die RCNs und möglicherweise einige andere Standorte, die direkt vom MCN verwaltet werden, sollen sich in der **Standardregion** befinden. Die **Standardregion** wäre die einzige Region für ein Netzwerk, bevor andere Regionen hinzugefügt werden. Nachdem Sie weitere Regionen hinzugefügt haben, können Sie die Option **Standard** auswählen, um eine gewünschte Region als Standardregion zu verwenden.

So erstellen Sie eine Region:

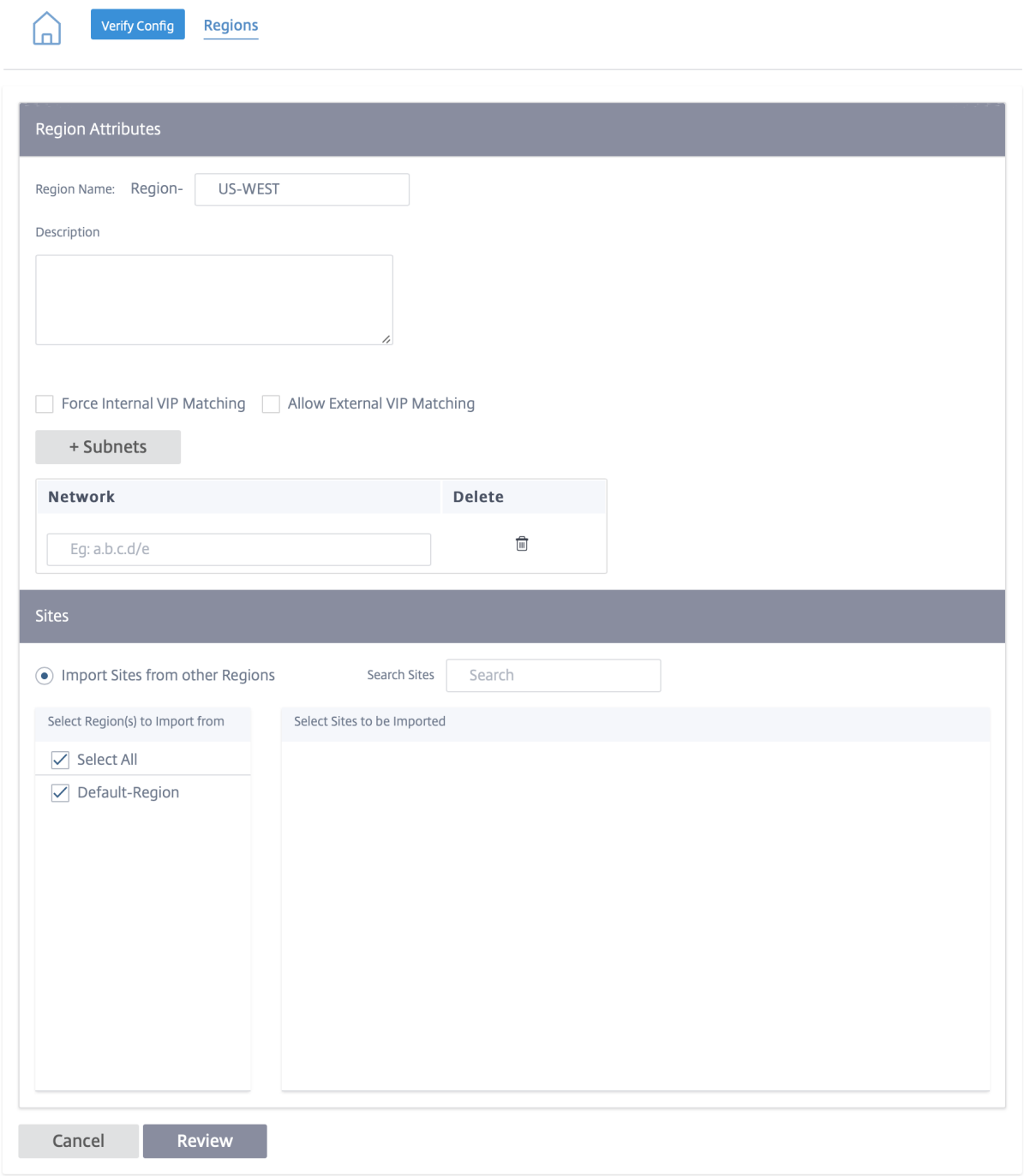
1. Klicken Sie auf **+ Region**. Geben Sie einen Namen und eine Beschreibung der Region an.
2. Aktivieren Sie den Intervall-VIP-Abgleich je nachdem, ob Sie einen **erzwungenen internen VIP-Abgleich** oder **einen externen VIP-Abgleich**

    - Erzwungener interner VIP-Abgleich: Wenn diese Option aktiviert ist, müssen alle nicht privaten virtuellen IP-Adressen in der Region mit den konfigurierten Subnetzen übereinstimmen.
    - Zulässiger externer VIP-Abgleich: Wenn diese Option aktiviert ist, können nicht private virtuelle IP-Adressen aus anderen Regionen mit den konfigurierten Subnetzen überein-

stimmen.

3. Klicken Sie auf **+ Subnetze**, um Subnetze hinzuzufügen. Geben Sie eine **Netzwerkadresse** ein. Die Netzwerkadresse ist die IP-Adresse und die Maske für das Subnetz.
4. Wählen Sie die Sites aus.
5. Klicken Sie auf **Überprüfen** und dann auf **Speichern**. Der neu erstellte Bereich wird der vorhandenen Liste der Regionen hinzugefügt.

> **Hinweis:**
>
> Ein Kunde kann nur statische oder dynamische virtuelle Pfade innerhalb einer Region haben.



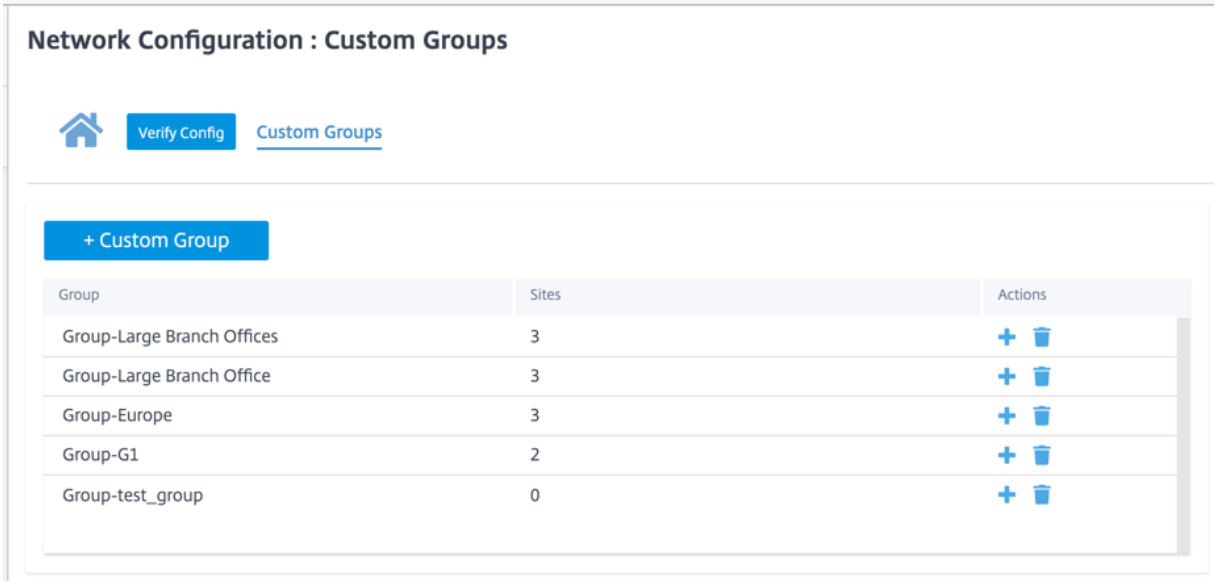
Sie können Standorte unter der Region platzieren, sobald eine Region erfolgreich erstellt wurde.

> **Hinweis:**
>
> Dynamische virtuelle Pfade können nicht zwischen Zweigen in verschiedenen Regionen eingerichtet werden.

Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen.

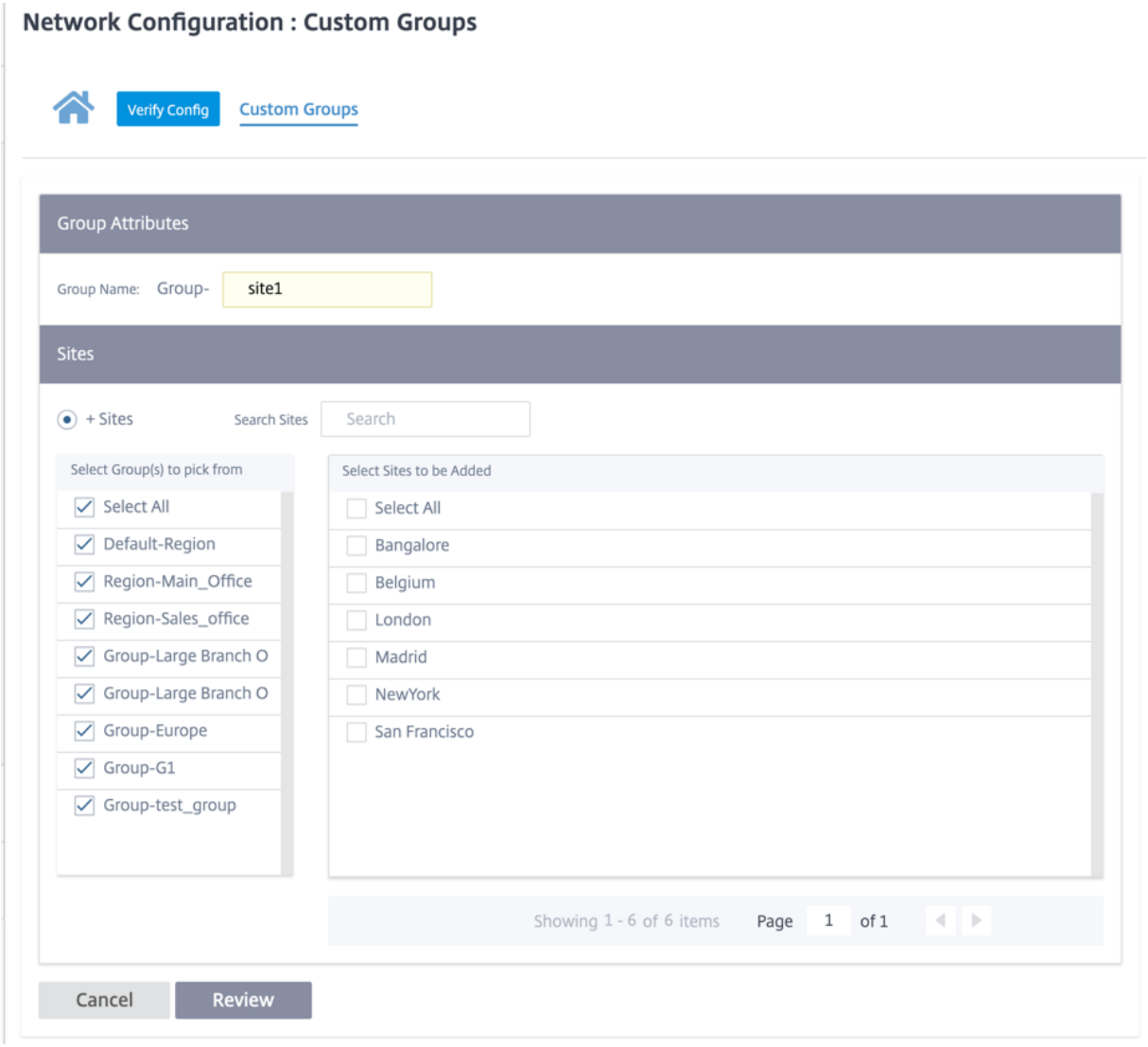
Angepasste Gruppen

Benutzerdefinierte Gruppen bieten Benutzern die Flexibilität, Websites nach Bedarf zu gruppieren. Benutzer können Richtlinien für Gruppen von Websites gleichzeitig anwenden, ohne sich unbedingt mit jeder Site einzeln befassen zu müssen. Gruppen können auch als Filter für Dashboards, Berichte oder Netzwerkkonfigurationen dienen. Im Gegensatz zu Regionen können sich Gruppen in Bezug auf Standorte überschneiden. Mit anderen Worten, dieselben Websites können Teil mehrerer Gruppen sein.



Ein Benutzer kann beispielsweise eine Gruppe mit dem Namen **Business Critical Sites** erstellen, um gemeinsame Richtlinien für alle Ihre geschäftskritischen Websites zu konfigurieren. Der Benutzer kann seinen Zustand und seine Leistung auch separat als Gruppe überwachen. Einige dieser Standorte können beispielsweise auch Teil einer **großen Zweigstellengruppe** sein.

Benutzerdefinierte Sitegruppen bieten eine Möglichkeit, Sites für Berichtszwecke logisch zu gruppieren. Sie können benutzerdefinierte Gruppen erstellen und Websites zu jeder benutzerdefinierten Gruppe hinzufügen. Um eine benutzerdefinierte Gruppe zu erstellen, klicken Sie auf **+ Benutzerdefinierte Gruppe**. Geben Sie einen Gruppennamen an und wählen oder fügen Sie Sites hinzu. Klicken Sie auf **Überprüfen** und dann auf **Speichern**.

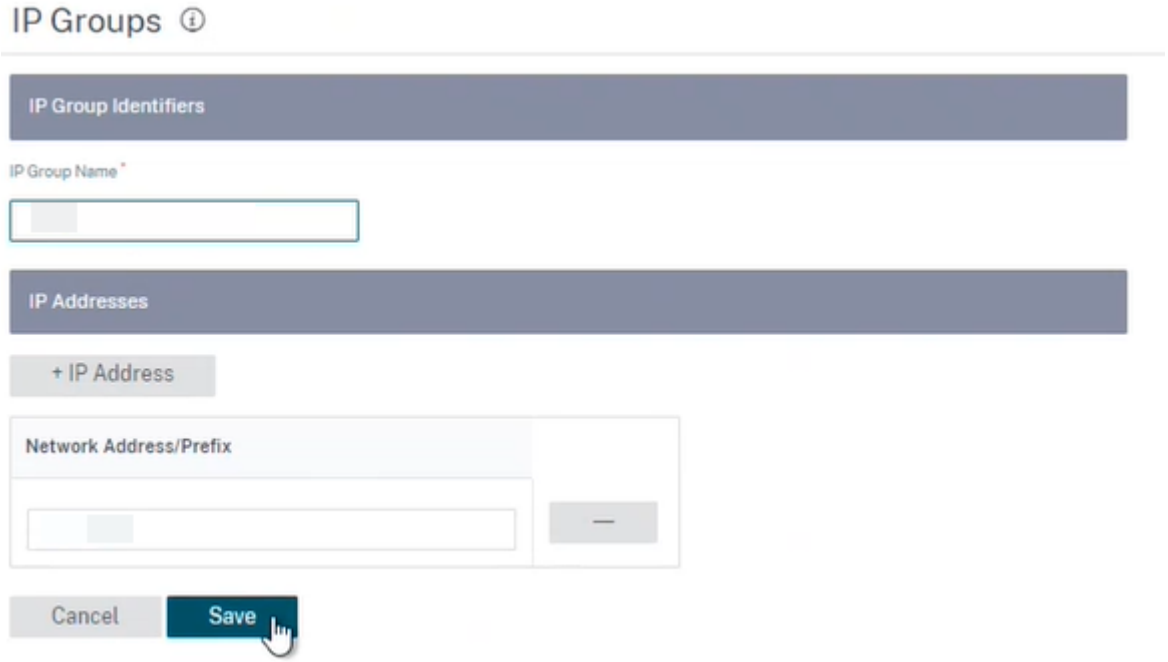


Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen.

IP-Gruppen

Der Citrix SD-WAN Orchestrator Service bietet die Option zum Hinzufügen von IP-Gruppen (Netzwerkobjekten). Mit dieser Option können Sie IP- und Netzwerkadressen gruppieren, indem Sie **IP-Gruppen** verwenden, während Sie einen Routenfilter definieren, anstatt für jedes Subnetz einen Filter zu erstellen. Diese Gruppen können bei Bedarf in Konfigurationen und Richtlinien verwendet werden, ohne dass jedes Mal einzelne IP-Adressen eingegeben werden müssen.

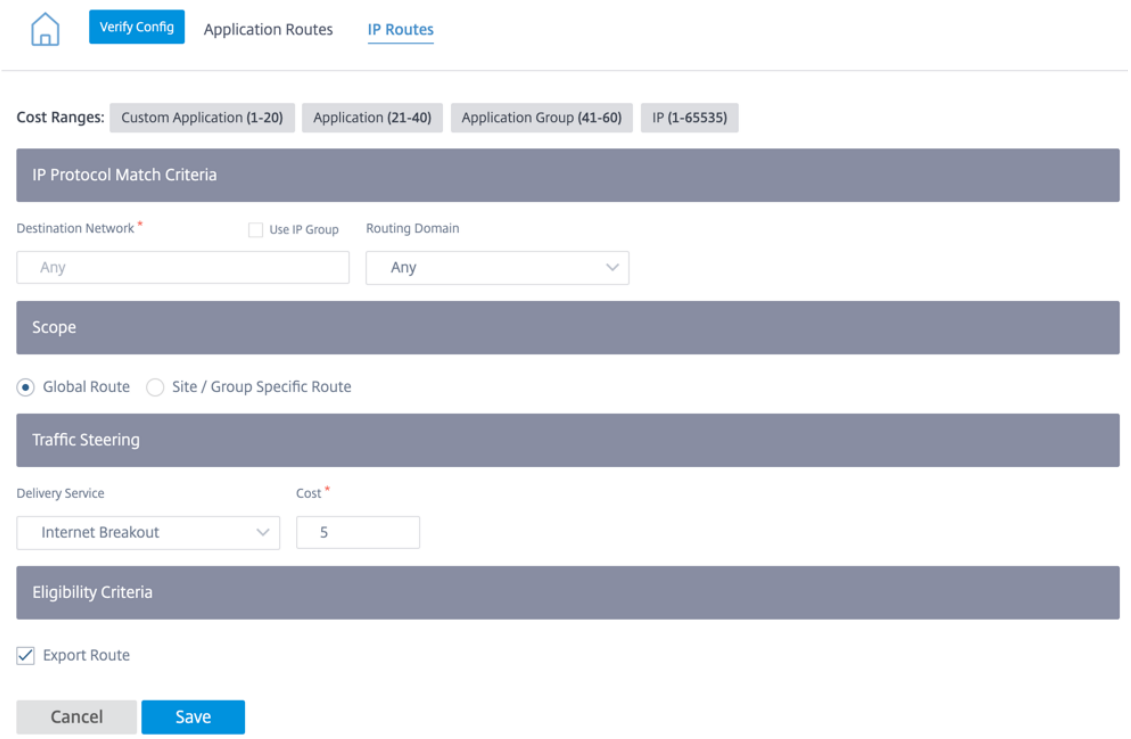
Sie können IP-Gruppen erstellen und Netzwerkadressen und Präfixe hinzufügen. Um eine IP-Gruppe zu erstellen, wählen Sie **IP-Gruppen** aus und klicken Sie auf **+ IP-Gruppe**. Geben Sie einen Gruppennamen an. Klicken Sie auf **+ IP-Adresse** und geben Sie die **IP-Adressen** ein, die der IP-Gruppe hinzugefügt werden sollen.



Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen

Die folgenden Funktionen nutzen die IP-Gruppen:

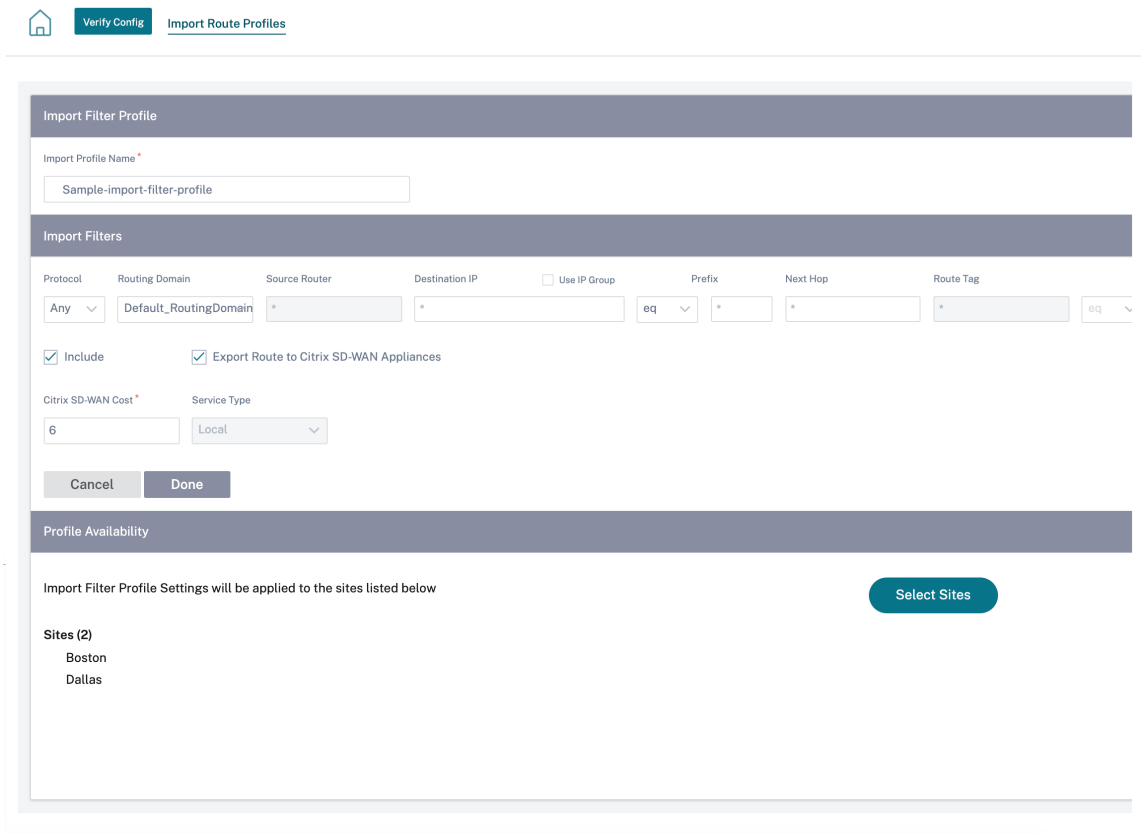
- **Erstellen einer IP-Route**: Sie können ein Zielnetzwerk hinzufügen oder das Kontrollkästchen **IP-Gruppe verwenden** aktivieren, um eine vorhandene IP-Gruppe auszuwählen. Weitere Informationen finden Sie unter IP-Gruppen.



- **Routenprofile importieren**: Beim Erstellen eines Importfilterprofils können Sie aus der Liste der in Ihrem Netzwerk verfügbaren IP-Gruppen auswählen.

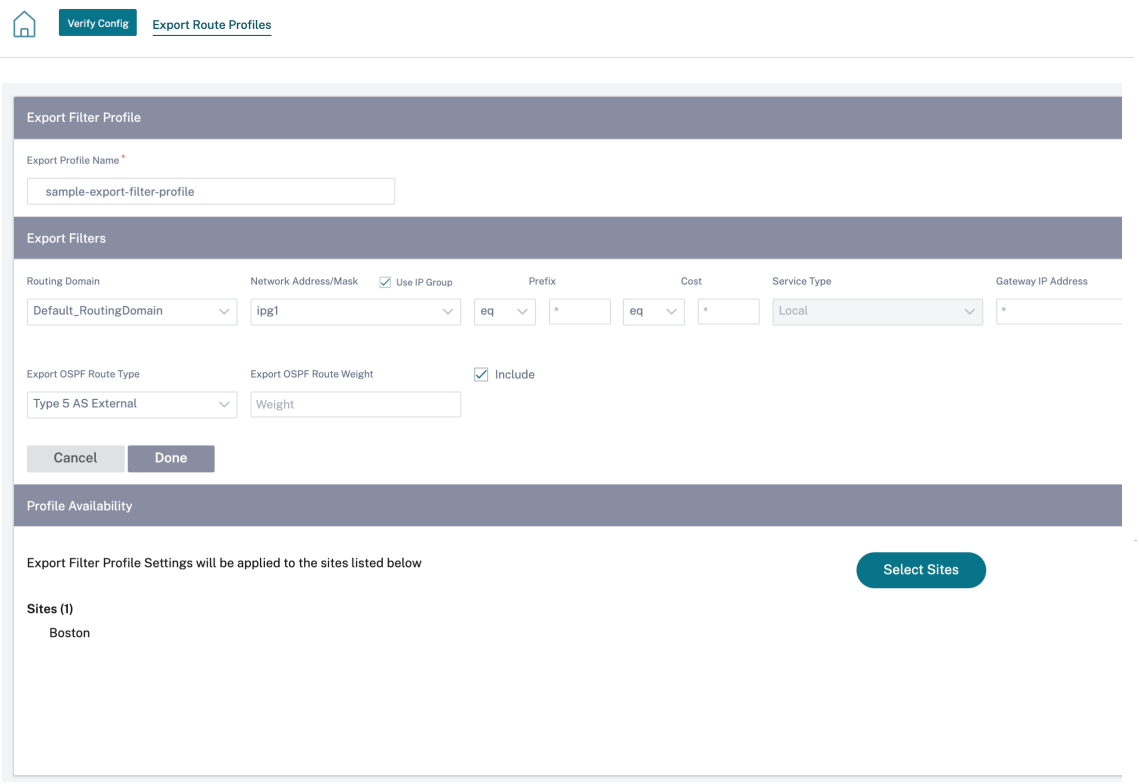
  Sie können ein Zielnetzwerk hinzufügen oder das Kontrollkästchen **IP-Gruppe verwenden** aktivieren, um eine vorhandene IP-Gruppe auszuwählen.

  Weitere Informationen finden Sie unter Importieren von Routenprofilen.



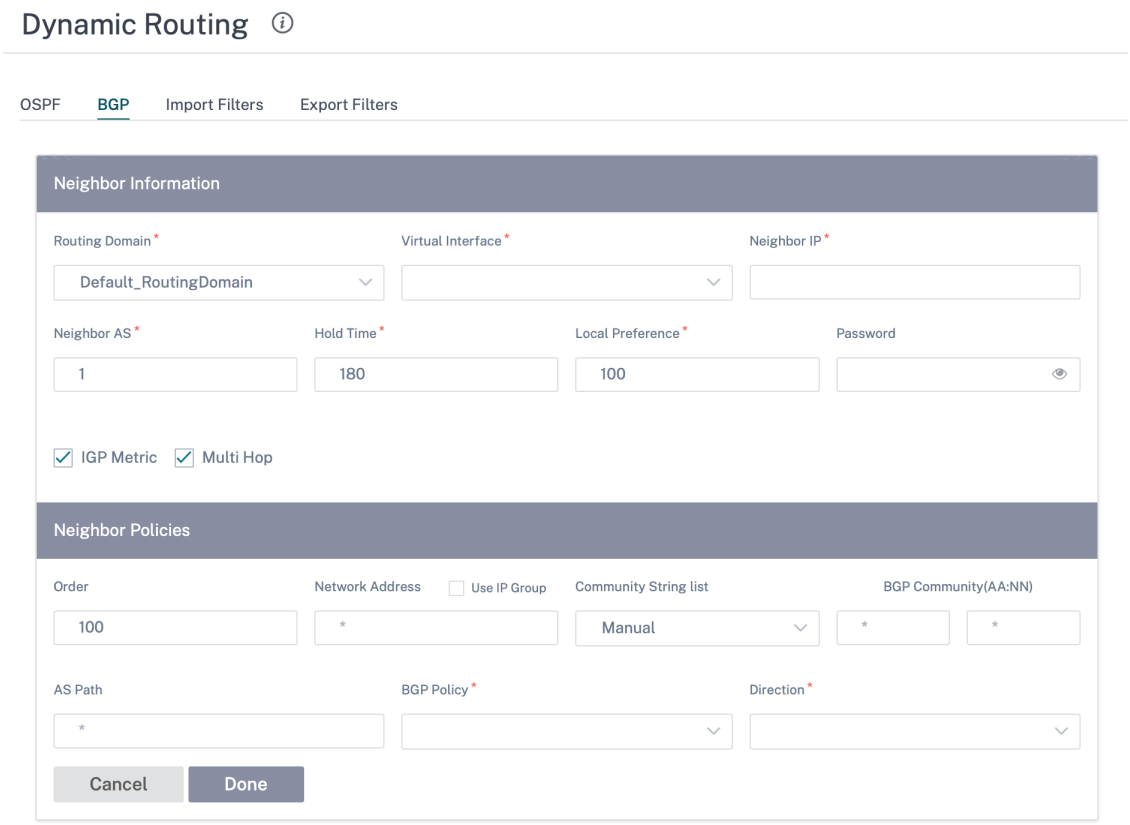
- **Routenprofile exportieren**: Beim Erstellen eines Exportfilterprofils können Sie eine Netzwerkadressmaske hinzufügen oder das Kontrollkästchen **IP-Gruppe verwenden** aktivieren, um eine vorhandene IP-Gruppe auszuwählen.

  Weitere Informationen finden Sie unter Exportieren von Routenprofilen.



- **BGP-Nachbarrichtlinien**: Beim Hinzufügen einer konfigurierten BGP-Richtlinie für benachbarte Router können Sie eine Netzwerkadresse hinzufügen oder das Kontrollkästchen **IP-Gruppe verwenden** aktivieren, um eine vorhandene IP-Gruppe auszuwählen.

  Weitere Informationen finden Sie unter BGP.



Anwendungseinstellungen und Gruppen

October 21, 2022

In diesem Abschnitt können Benutzer Anwendungen individuell definieren, Anwendungen für die Verwendung in Richtlinien, QoS-Profilen und DNS-Einstellungen gruppieren.

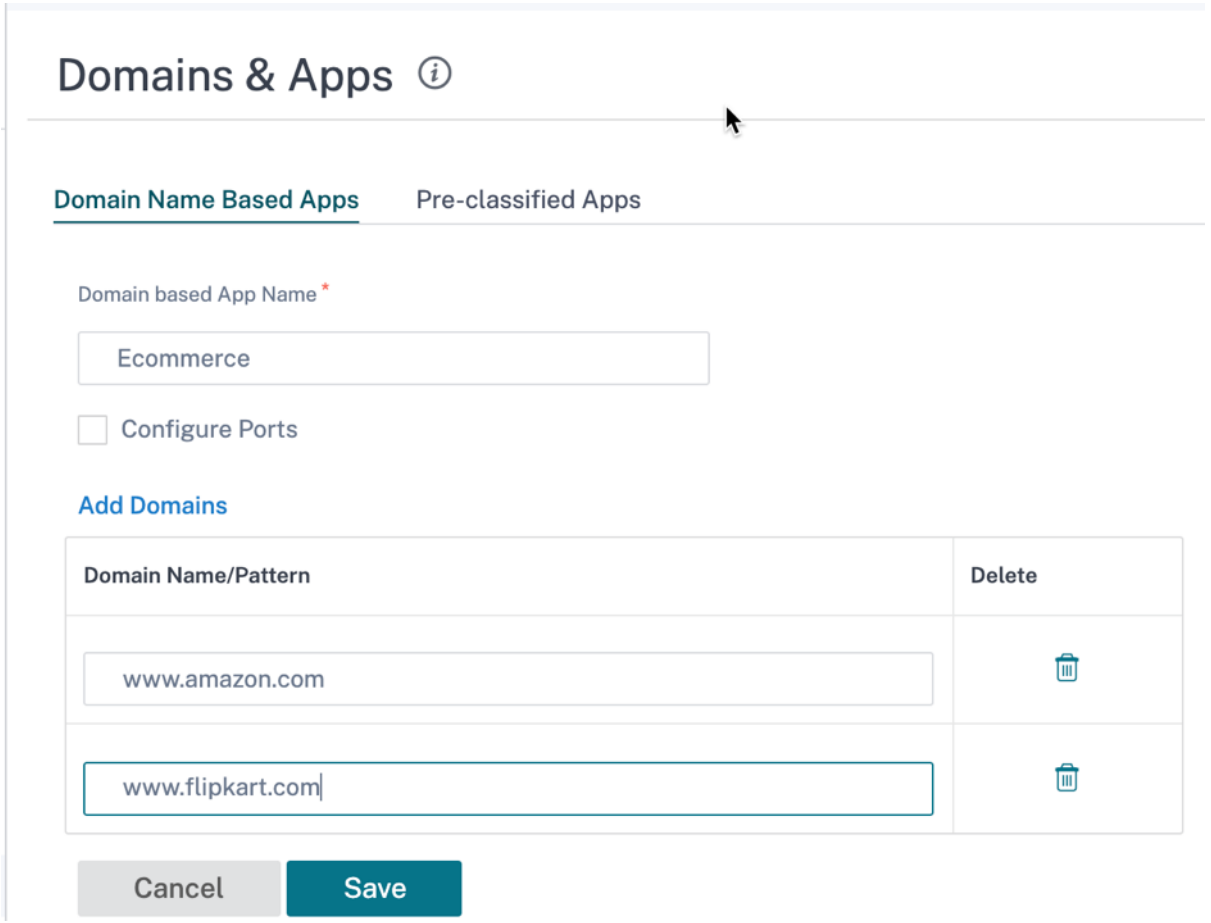
Sie können eine **Anwendungsgruppe** sowohl für vordefinierte als auch für benutzerdefinierte Anwendungen definieren. Eine **Anwendungsgruppe** enthält Anwendungen, die bei der Definition einer Sicherheitsrichtlinie ähnlich behandelt werden müssen.

Sie können die **Anwendungsgruppen** häufig wiederverwenden, wenn Sie Richtlinien wie Anwendungssteuerung oder Firewallregeln definieren. Es entfällt die Notwendigkeit, mehrere Einträge für jede einzelne Anwendung zu erstellen. In ähnlicher Weise unterstützt Application Groups bei der Verwendung von Anwendungsdiensten gängige Anwendungen mit einem eindeutigen Namen für eine vereinfachte und konsistente Wiederverwendung.

Um **Anwendungsgruppen**anzuzeigen, navigieren Sie zu **Konfiguration > App-Einstellungen und Gruppen**.

Domänen und Anwendungen

Sie können interne Anwendungen basierend auf Domänennamen erstellen, die nicht in der Liste der veröffentlichten Anwendungen auf der Seite **Domains & Apps** verfügbar sind. Um Anwendungen basierend auf dem Domänennamen zu erstellen, navigieren Sie auf Netzwerkebene zur Registerkarte **App-Einstellungen und -Gruppen > Domänen und Apps > Domänennamenbasierte Apps**, und klicken Sie auf **Neue domänennamenbasierte Anwendung**. Geben Sie den Anwendungsnamen ein und fügen Sie die Domänennamen oder Muster hinzu. Sie können entweder den vollständigen Domainnamen eingeben oder am Anfang Wildcards verwenden.



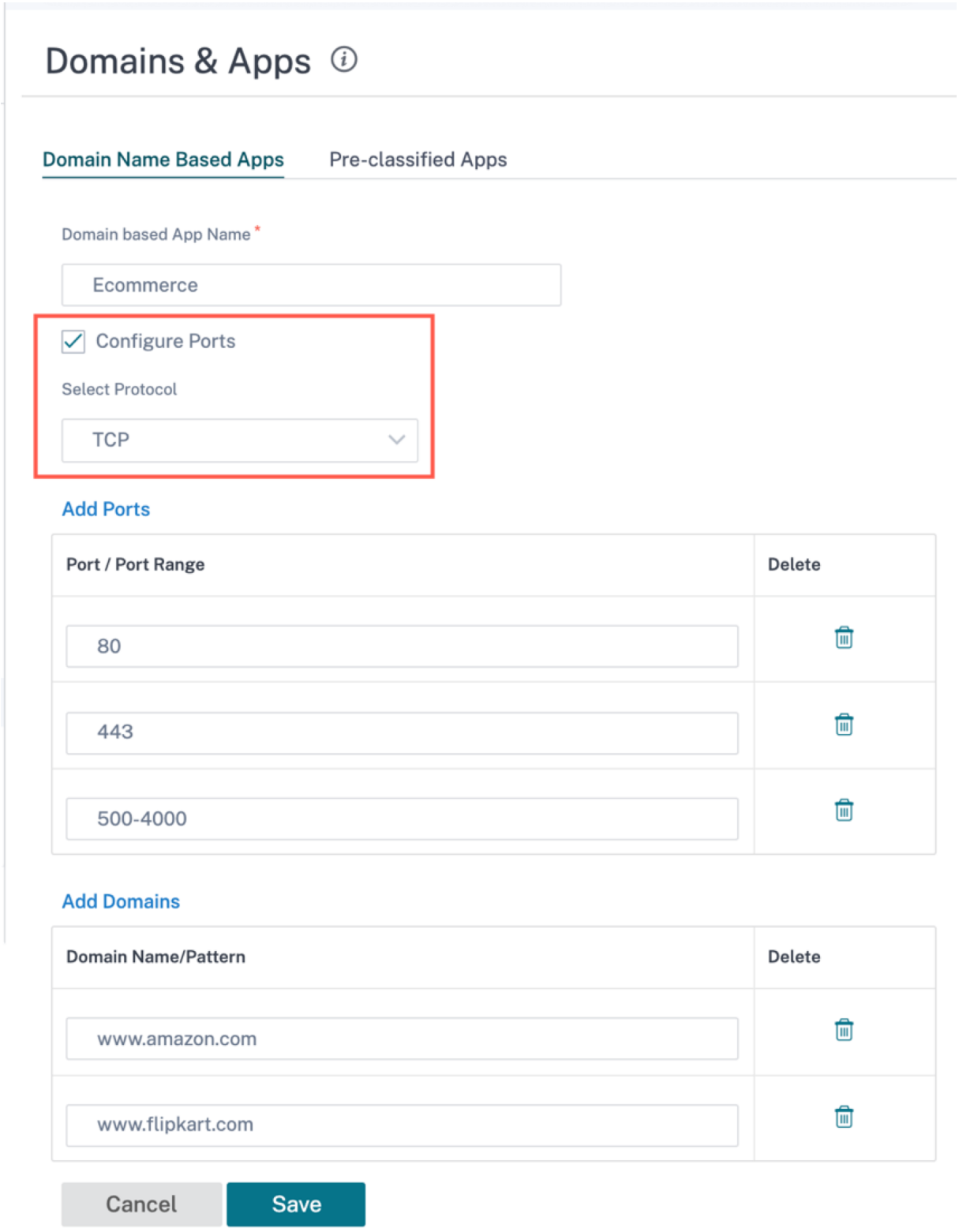
Alle auf Domänennamen basierenden Anwendungen sind in **Anwendungsrouting**, **Anwendungsregeln**und **Firewall-Richtlinien**sichtbar.

Ab Version Citrix SD-WAN 11.4.2 wird die Option **Ports konfigurieren** unter **Domänennamenbasierte Anwendungen**verfügbar gemacht. Wenn das Kontrollkästchen **Ports konfigurieren** aktiviert ist, bietet es die Flexibilität, eine Gruppe von mehreren Ports, Portbereichen und einem Protokoll (TCP/UDP/Any) für die domänenbasierte Anwendung zu konfigurieren.

Zuvor wurden die Ports **80** und **443**sowie das Protokoll **Any** für Domänen unterstützt, die unter einer Anwendung gruppiert waren. Sie können dasselbe Verhalten sehen, wenn das Kontrollkästchen **Ports**

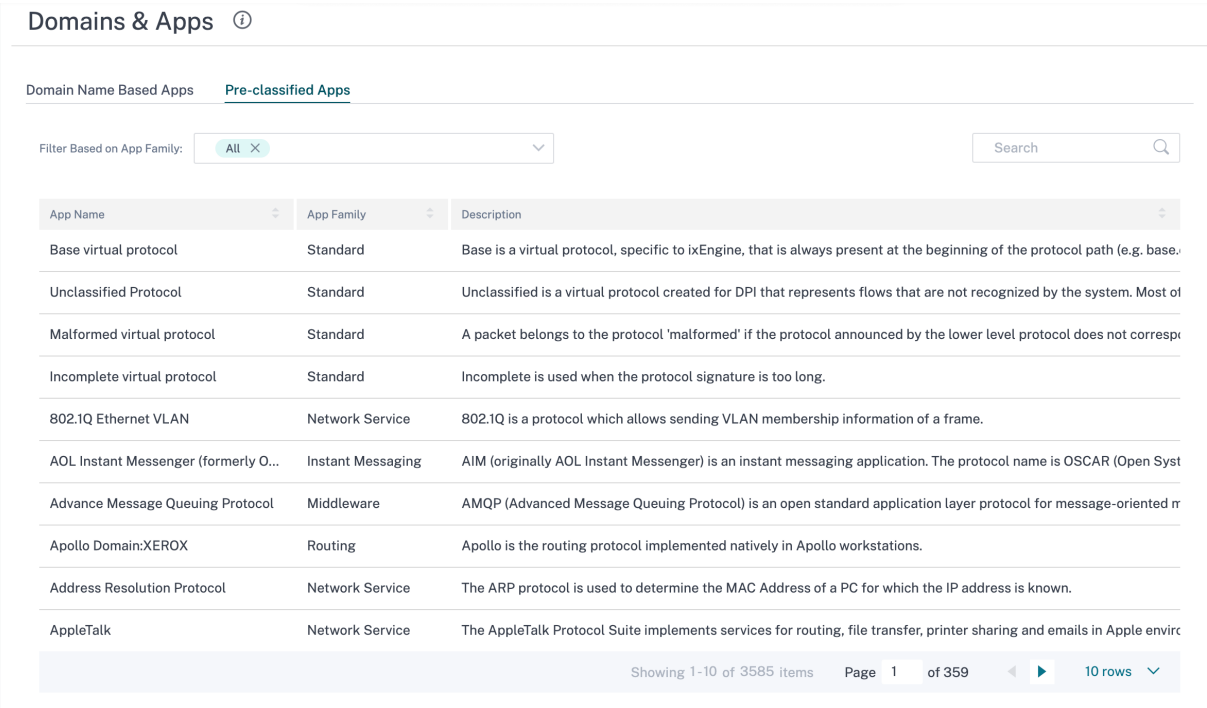
konfigurieren deaktiviert ist. Das Kontrollkästchen **Ports konfigurieren** ist standardmäßig deaktiviert.

Wenn Sie das Kontrollkästchen **Port konfigurieren** aktivieren, können Sie jeden Port oder Portbereich bearbeiten, hinzufügen oder löschen, zusammen mit der Protokollauswahl als TCP, UDP oder Beliebig. Standardmäßig ist der Protokollwert auf Any festgelegt **und** die Ports sind auf **80** und **443**festgelegt.



Sie können die Liste der vordefinierten Anwendungen auch auf der Registerkarte **Vorklassifizierte**

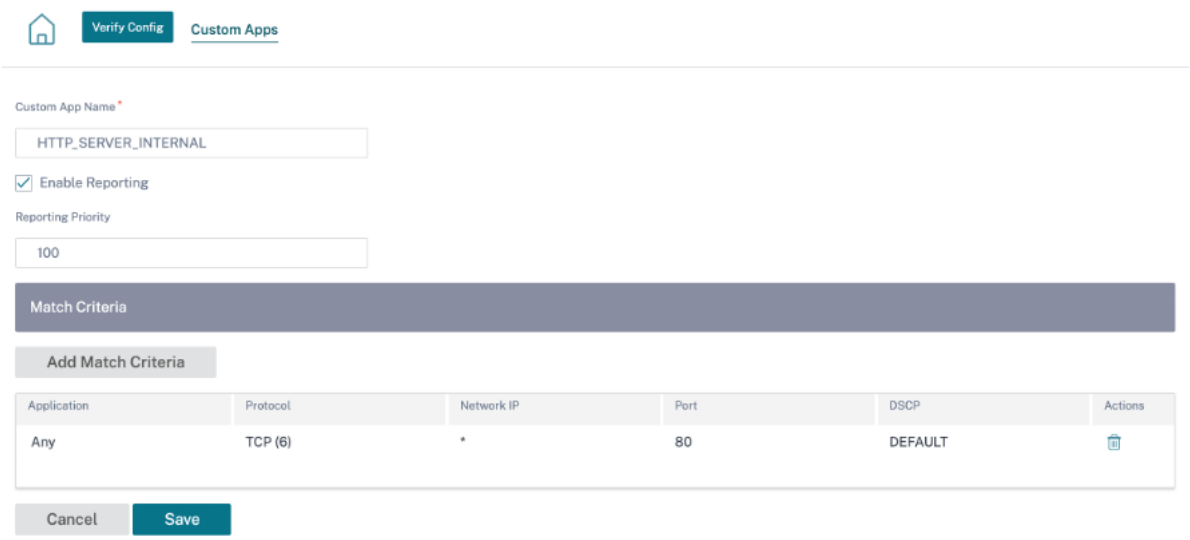
Apps anzeigen. Sie können mit der Suchleiste **nach einer bestimmten Anwendung suchen** oder die Liste anhand der Anwendungsfamilie filtern.



Benutzerdefinierte Anwendung

Die **benutzerdefinierten Anwendungen** werden verwendet, um interne Anwendungen oder IP-Port-Kombinationen zu erstellen, die in der Liste der veröffentlichten Anwendungen nicht verfügbar sind. Der Administrator muss eine benutzerdefinierte Anwendung definieren, die auf dem IP-Protokoll basiert und bei Bedarf in mehreren Richtlinien verwendet werden kann, ohne jedes Mal auf die Informationen zur IP-Adresse und Portnummer zu verweisen.

Um eine benutzerdefinierte Anwendung zu erstellen, navigieren Sie auf Netzwerkebene zu **App-Einstellungen & Gruppen > Benutzerdefinierte Apps**, klicken Sie auf **+ Benutzerdefinierte Anwendung** und geben Sie einen Namen für die benutzerdefinierte Anwendung ein. Geben Sie die Übereinstimmungskriterien wie IP-Protokoll, Netzwerk-IP-Adresse, Portnummer und DSCP-Tag an. Der Datenfluss, der diesen Kriterien entspricht, wird als benutzerdefinierte Anwendung gruppiert.

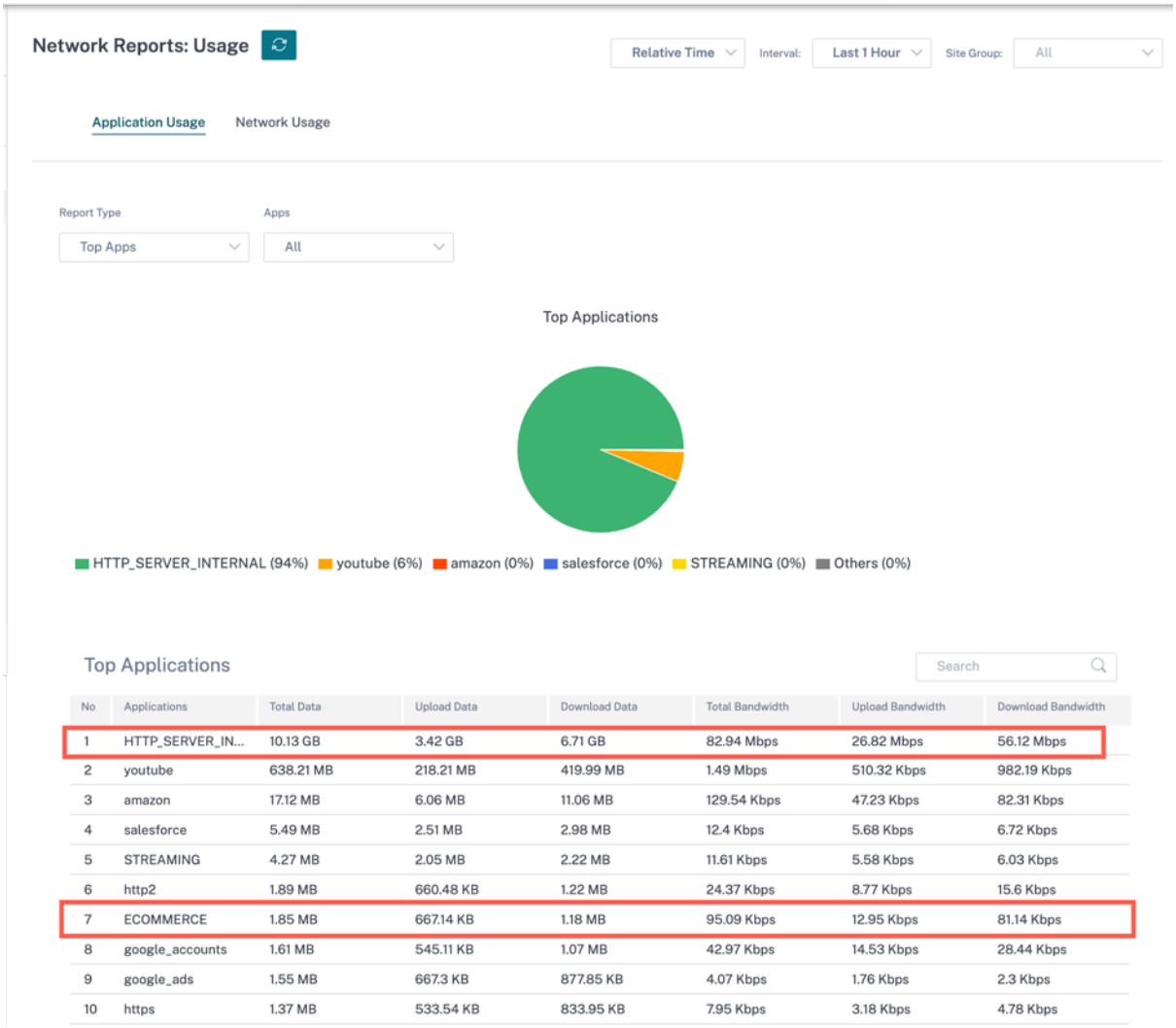


Nach dem Speichern werden die benutzerdefinierten Anwendungen in einer Liste angezeigt und können nach Bedarf bearbeitet oder gelöscht werden.

Das Kontrollkästchen **Reporting aktivieren** wurde für die auf dem IP-Protokoll basierenden benutzerdefinierten Anwendungen und Anwendungsgruppen hinzugefügt. Sie müssen das Kontrollkästchen **Reporting aktivieren aktivieren aktivieren** und die Berichtspriorität angeben.

Wenn das Kontrollkästchen **Reporting aktivieren** aktiviert ist, können Sie den benutzerdefinierten IP-Anwendungsdatenverkehr unter **Berichte** > **Verwendung**anzeigen.

Berichtspriorität ist die Reihenfolge, in der auf IP-Protokollen basierende benutzerdefinierte Anwendungen oder Anwendungsgruppen für das Reporting ausgewählt werden. Es ist hilfreich, die benutzerdefinierte Anwendung oder Anwendungsgruppe mit hoher Priorität für die Berichterstattung auszuwählen, wenn mehrere Übereinstimmungen mit aktivierter Berichterstellung vorliegen. Wenn beispielsweise die Berichtspriorität einer benutzerdefinierten Anwendung auf 1 festgelegt ist, bedeutet dies, dass die benutzerdefinierte Anwendung beim Reporting die höchste Priorität erhält. Wenn die Berichtspriorität auf 100 festgelegt ist, hat die benutzerdefinierte Anwendung bei der Berichterstattung einen viel geringeren Vorrang.

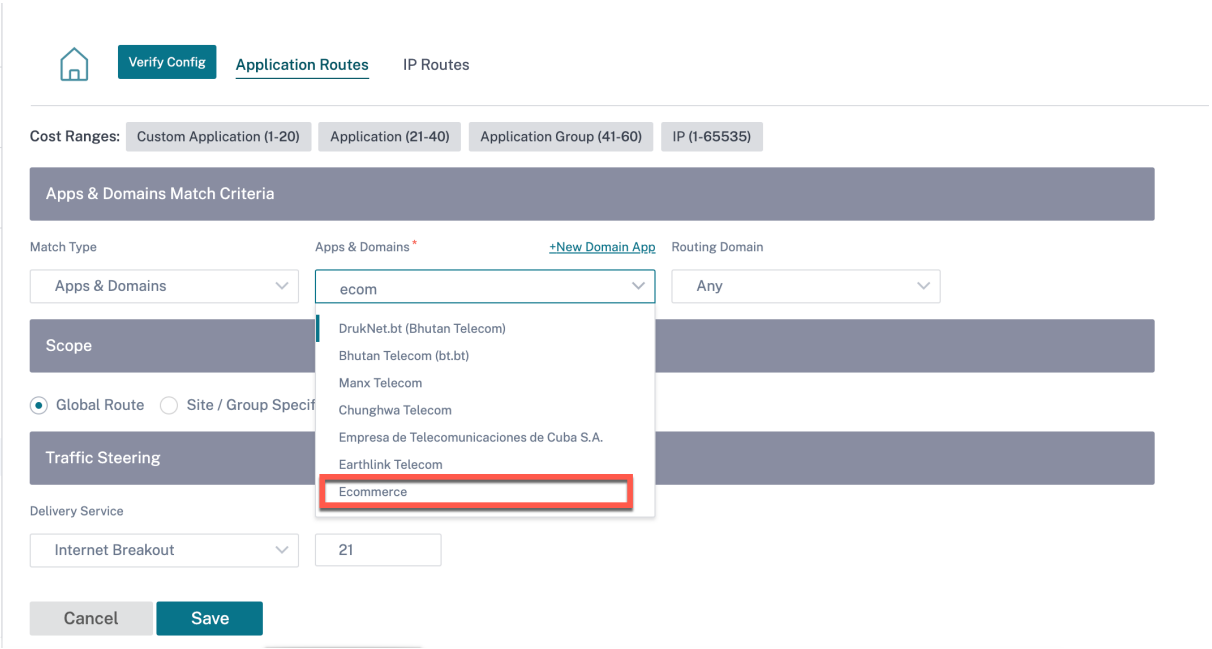


No	Applications	Total Data	Upload Data	Download Data	Total Bandwidth	Upload Bandwidth	Download Bandwidth
1	HTTP_SERVER_IN...	10.13 GB	3.42 GB	6.71 GB	82.94 Mbps	26.82 Mbps	56.12 Mbps
2	youtube	638.21 MB	218.21 MB	419.99 MB	1.49 Mbps	510.32 Kbps	982.19 Kbps
3	amazon	17.12 MB	6.06 MB	11.06 MB	129.54 Kbps	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

Hinweis

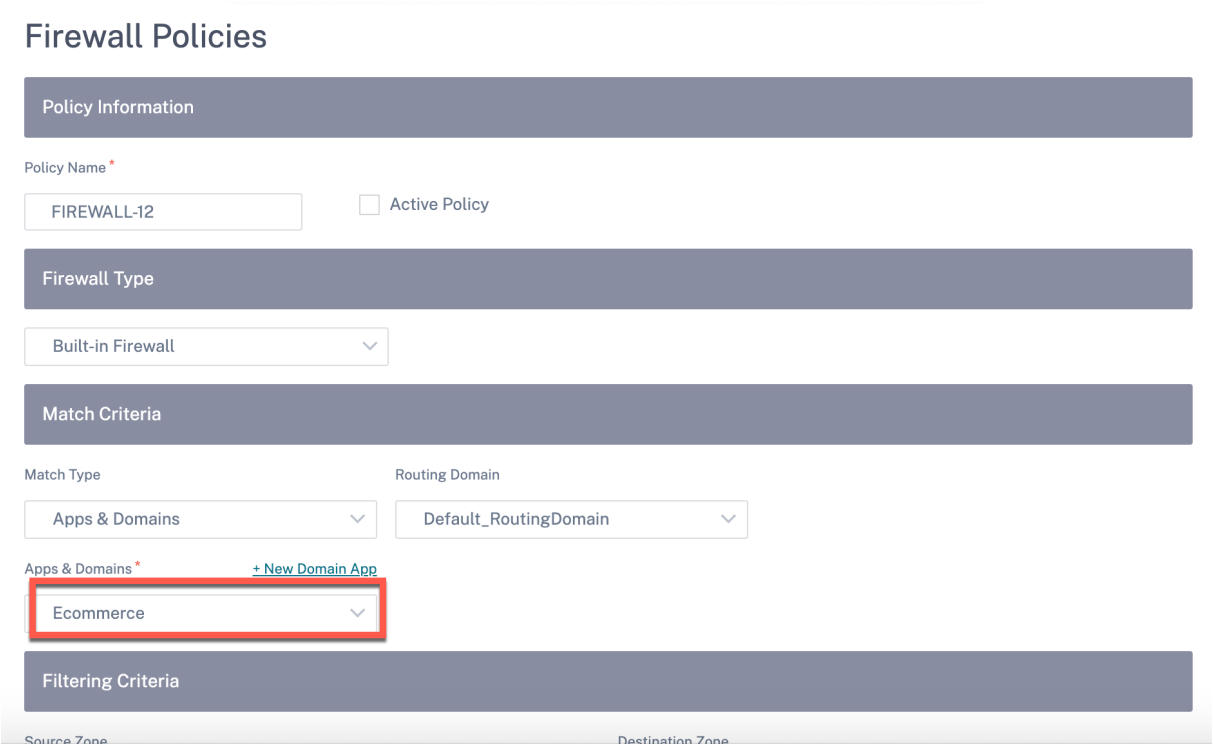
- Damit Sie eine auf Domänennamen basierende Anwendung verwenden können, müssen **Apps & Domänen** beim Erstellen der Anwendungsroute, der QoS-Richtlinie und der Firewall-Richtlinie als Übereinstimmungskriterien aufgeführt werden.
- Damit Sie eine benutzerdefinierte Anwendung verwenden können, muss die **benutzerdefinierte Anwendung** beim Erstellen der Anwendungsroute, der QoS-Richtlinie und der Firewall-Richtlinie als Übereinstimmungskriterien aufgeführt werden.

Nachdem Sie die benutzerdefinierte Anwendung erstellt haben, navigieren Sie zum Ausführen des Anwendungsroutings zu **Routing > Routing-Richtlinien > + Anwendungsroute**und wählen Sie **Benutzerdefinierte Anwendung** aus der Dropdown-Liste **Übereinstimmungstyp** aus. In ähnlicher Weise wählen Sie für die auf Domänennamen basierende Anwendung **Apps & Domains** aus der Dropdown-Liste **Übereinstimmungstyp** aus.

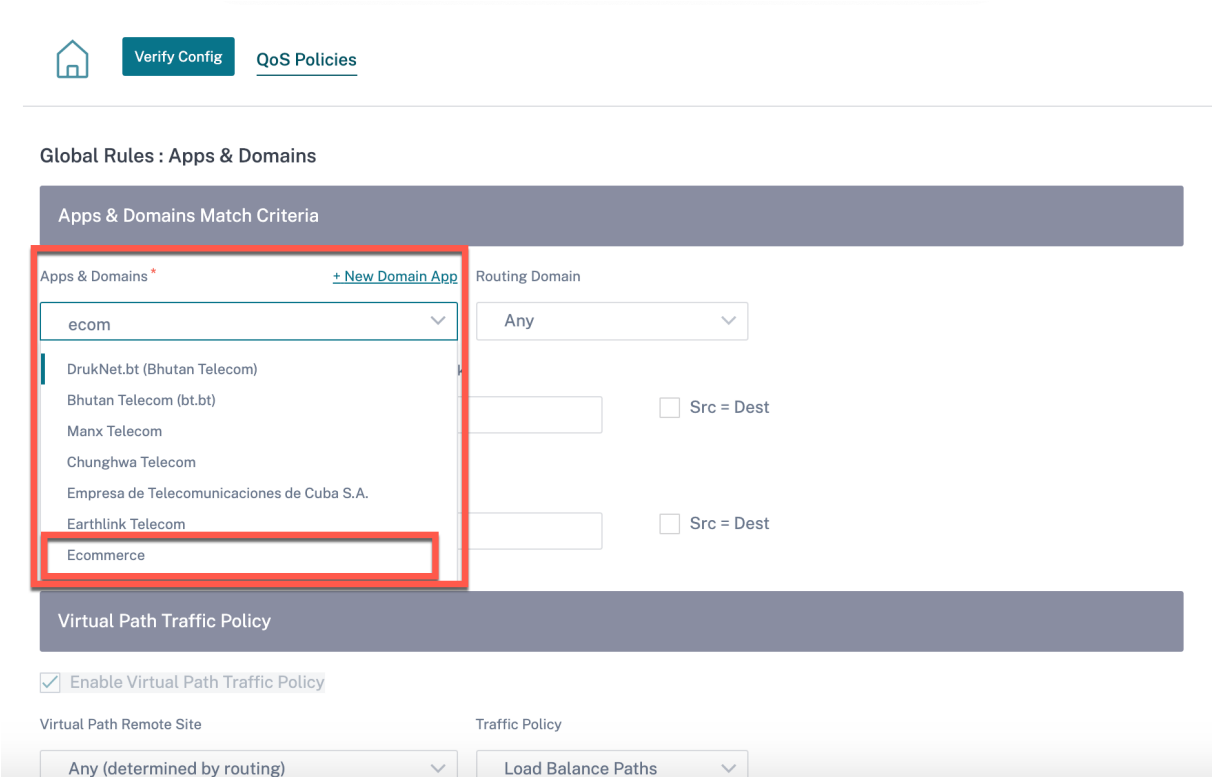


Sie können auch eine auf Domänennamen basierende Anwendung unter den Übereinstimmungskriterien auswählen, während Sie eine benutzerdefinierte **IP-Protokollanwendung** erstellen.

Um die benutzerdefinierte Anwendung unter den **Firewall-Richtlinien**anzuzeigen, navigieren Sie zu **Sicherheit > Firewall-Richtlinien**. Die Anwendung kann für jede Art von Richtlinie verwendet werden (globale Überschreibung/Site-spezifische oder globale Richtlinien). Klicken Sie auf **Neue Regel erstellen** und wählen Sie unter **Übereinstimmungskriterien**in der Dropdown-Liste **Übereinstimmungstyp** die Option **Benutzerdefinierte** Um die auf dem Domänennamen basierende Anwendung anzuzeigen, wählen Sie **Apps & Domains** aus der Dropdown-Liste **Übereinstimmungstyp** aus.



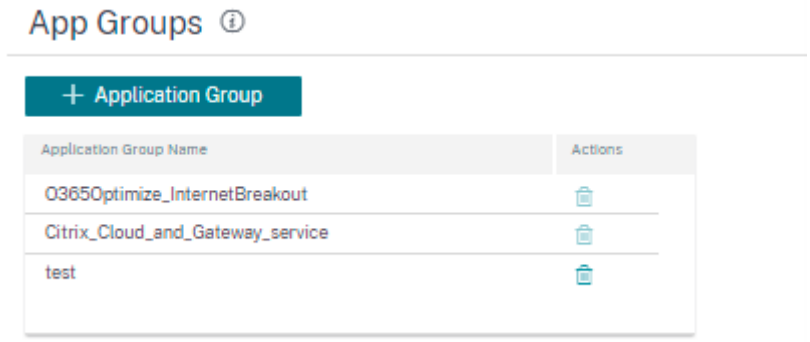
Sie können die auf Domänennamen basierenden benutzerdefinierten Anwendungen sowohl unter **Globale als auch unter Standort-/Gruppenspezifische Regel**anzeigen. Um die auf Domänennamen basierenden Anwendungen anzuzeigen, navigieren Sie zu **QoS > QoS-Richtlinien > Globale Regeln > Anwendungsregel > + Anwendungsregel**, und wählen Sie die gewünschte domänennamenbasierte Anwendung aus der Dropdown-Liste **Apps & Domänen** aus. Um benutzerdefinierte Anwendungen anzuzeigen, navigieren Sie zu **QoS > QoS-Richtlinien > Globale Regeln > Regeln für benutzerdefinierte Anwendungen > + Benutzerdefinierte Anwendungsregel**, und wählen Sie die gewünschte benutzerdefinierte Anwendung aus der Dropdown-Liste **Benutzerdefinierte Anwendung** aus.



Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen.

Anwendungsgruppen

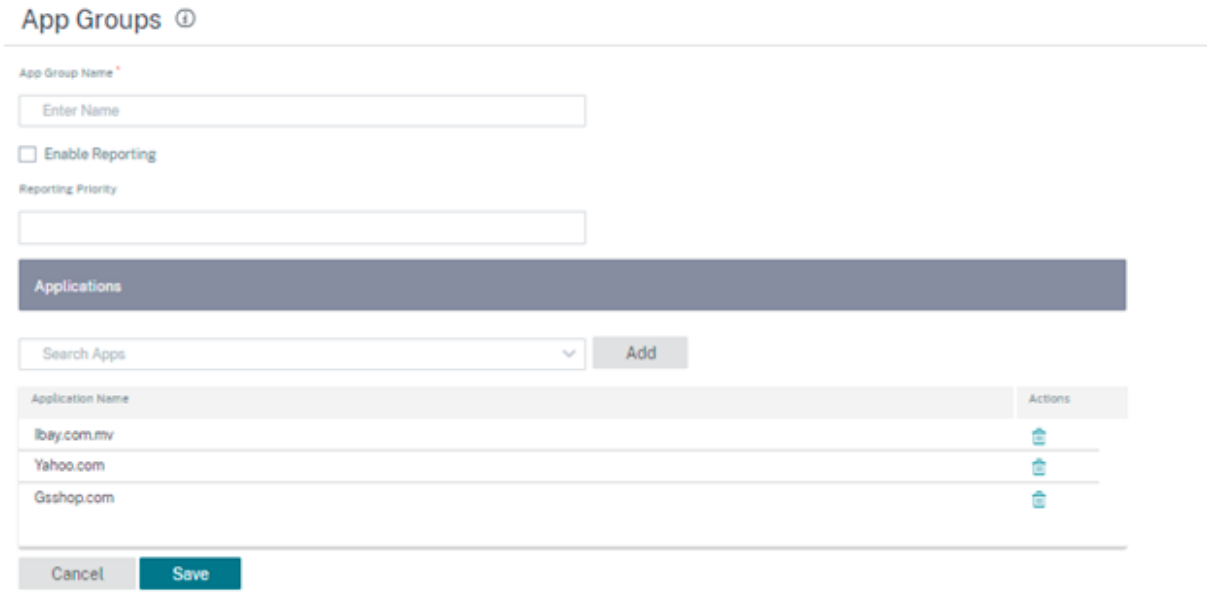
Mit einer **Anwendungsgruppe** können Administratoren ähnliche Anwendungen für die Verwendung in gemeinsamen Richtlinien gruppieren, ohne dass sie für jede einzelne Anwendung eine Richtlinie erstellen müssen.



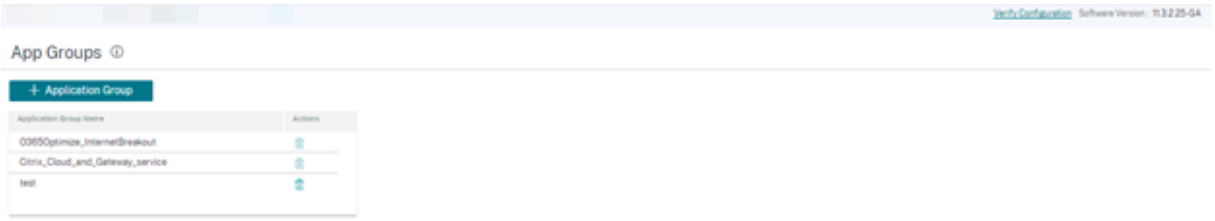
Sie können eine **Anwendungsgruppe** erstellen, indem **Sie die Option Anwendungsgruppen hinzufügen** verwenden. Sie können dieselbe Anwendungsgruppe beim Erstellen einer Richtlinie gemäß der Anwendungsrolle referenzieren. Die Richtlinie, die für die jeweilige Gruppe definiert ist, wird auf jede Anwendung angewendet, die der spezifischen Kategorie entspricht.

Sie können beispielsweise eine **Anwendungsgruppe** als **soziales Netzwerk** erstellen und der Gruppe soziale Netzwerke wie Facebook, LinkedIn und Twitter hinzufügen, um bestimmte Richtlinien für Anwendungen in sozialen Netzwerken zu definieren.

Um eine **Anwendungsgruppe**zu erstellen, geben Sie einen Gruppennamen an, suchen und fügen Sie Apps aus der **Anwendungsliste** hinzu.
Sie können jederzeit zurückgehen und Ihre Einstellungen bearbeiten oder die **Anwendungsgruppe** nach Bedarf löschen.

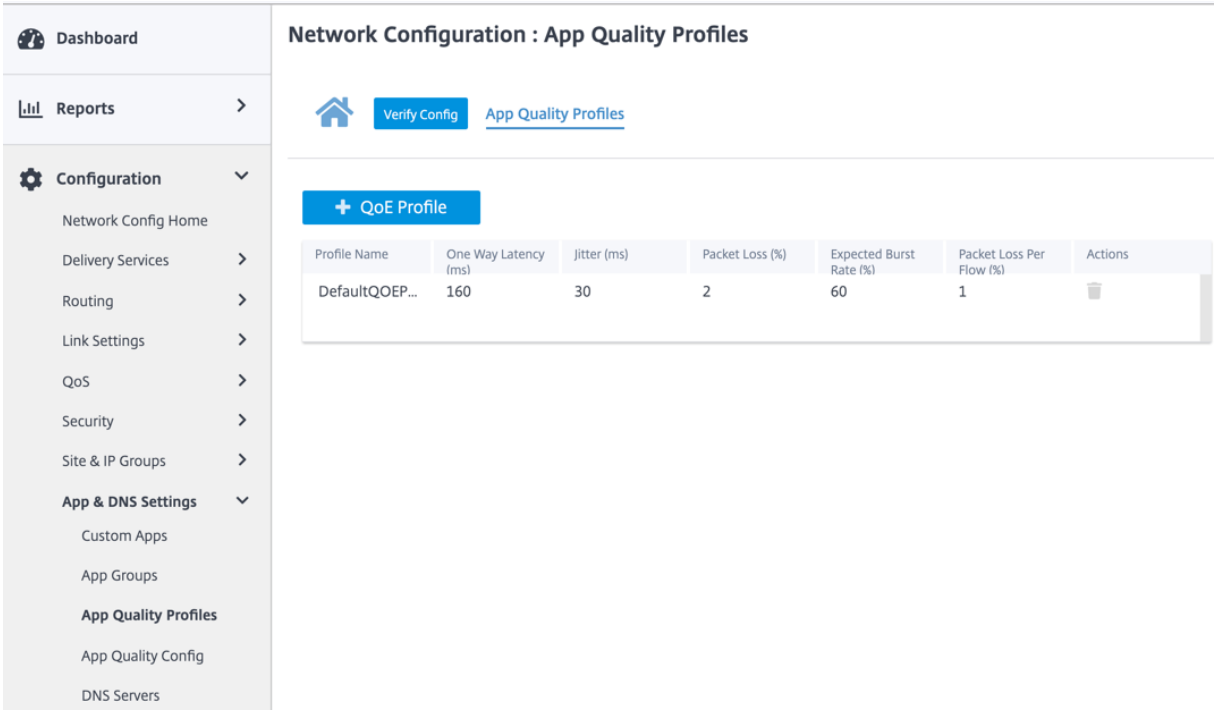


Klicken Sie auf der Seite Konfiguration**>**App-Einstellungen und Gruppen > **App-Gruppen**** auf Konfiguration überprüfen, um alle Überwachungsfehler zu überprüfen.**



Profile für Anwendungsqualität

In diesem Abschnitt können Sie Profile für die Anwendungsqualität anzeigen und erstellen.



Anwendung QoE ist ein Maß für die Qualität der Erfahrung von Anwendungen im SD-WAN-Netzwerk. Es misst die Qualität von Anwendungen, die durch die virtuellen Pfade zwischen zwei SD-WAN-Appliances fließen.

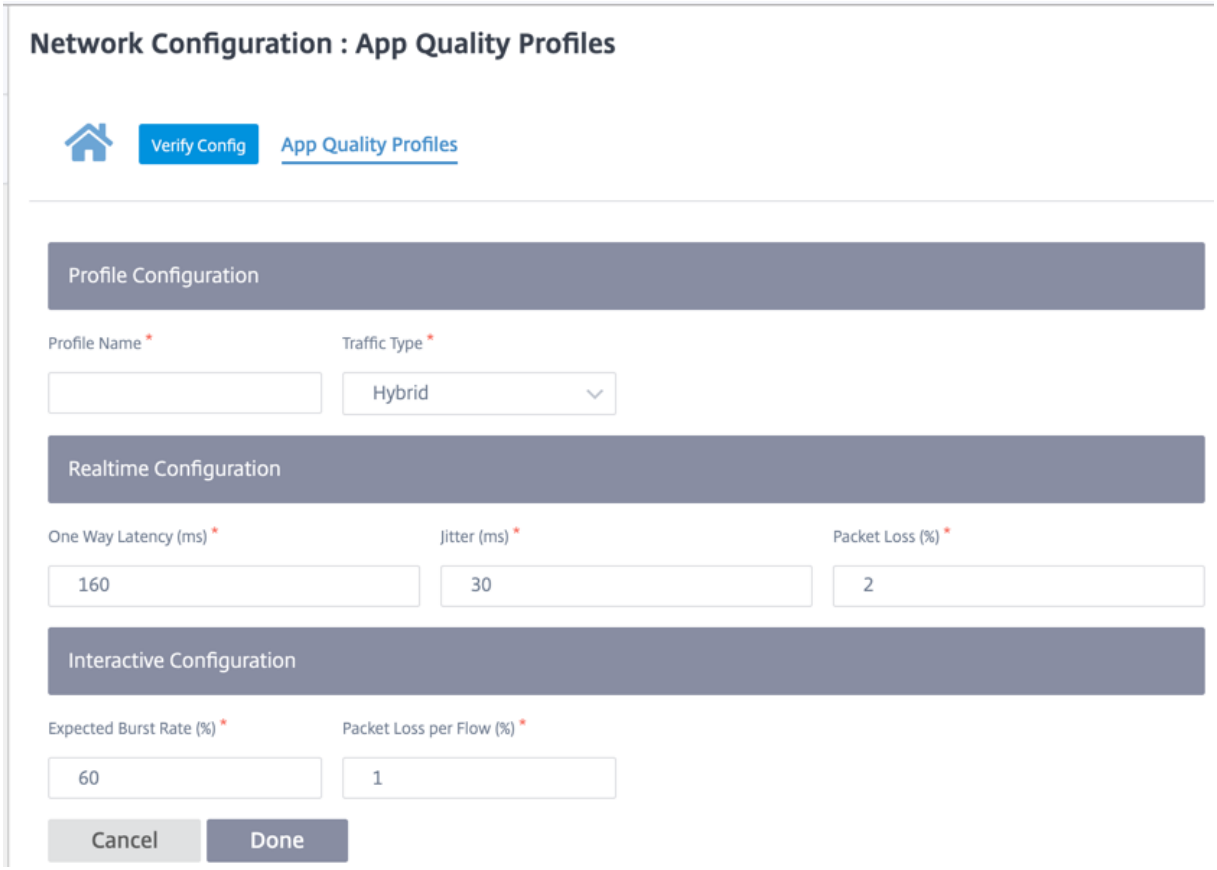
Der QoE-Wert der Anwendung ist ein Wert zwischen 0 und 10. Der Wertungsbereich, in den er fällt, bestimmt die Qualität einer Anwendung.

Qualität	Reichweite
Gut	8–10
Fair	4–8
Schlecht	0–4

Der QoE-Wert für Anwendungen kann verwendet werden, um die Qualität von Anwendungen zu messen und problematische Trends zu erkennen.

Konfiguration des Profils

Klicken Sie auf **+ QoE-Profil**, um ein QoE-Profil zu erstellen, geben Sie einen Profilnamen an und wählen Sie einen Verkehrstyp aus der Dropdown-Liste aus.



Konfiguration in Echtzeit

Sie können die Qualitätsschwellenwerte für Echtzeit- und interaktive Appliances mithilfe von QoE-Profilen definieren und diese Profile Anwendungen oder Anwendungsobjekten zuordnen.

Die Application QoE-Berechnung für Echtzeitanwendungen verwendet eine innovative Citrix Technik, die aus dem MOS-Score abgeleitet wird.

Die Standardschwellenwerte sind:

- Latenzschwelle (ms): 160
- Jitter-Schwellenwert (ms): 30
- Schwellenwert für Paketverlust (%): 2

Ein Fluss einer Echtzeitanwendung, der die Schwellenwerte für Latenz, Verlust und Jitter erfüllt, wird als von guter Qualität angesehen.

QoE für Echtzeitanwendungen wird aus dem Prozentsatz der Flüsse, die den Schwellenwert erreichen, geteilt durch die Gesamtzahl der Flussproben bestimmt.

QoE für Echtzeit = (Anzahl der Flussproben, die den Schwellenwert erreichen/Gesamtzahl der Durchflussproben) * 100

Es wird als QoE-Score von 0 bis 10 dargestellt.

Interaktive Konfiguration

Die Application QoE für interaktive Anwendungen verwendet eine innovative Citrix Technik, die auf Paketverlust und Burst-Rate-Schwellenwerten basiert.

Interaktive Anwendungen reagieren empfindlich auf Paketverlust und -durchsatz. Daher messen wir den Prozentsatz des Paketverlusts und die Burst-Rate des Ein- und Ausstiegsverkehrs in einem Flow.

Die konfigurierbaren Schwellenwerte sind:

- Prozentsatz des Paketverlusts.
- Prozentsatz der erwarteten Austritt Burst Rate im Vergleich zur Ingress Burst Rate.

Die Standardschwellenwerte sind:

- Schwellenwert für Paketverlust: 1%
- Burst-Rate: 60%

Ein Fluss ist von guter Qualität, wenn die folgenden Bedingungen erfüllt sind:

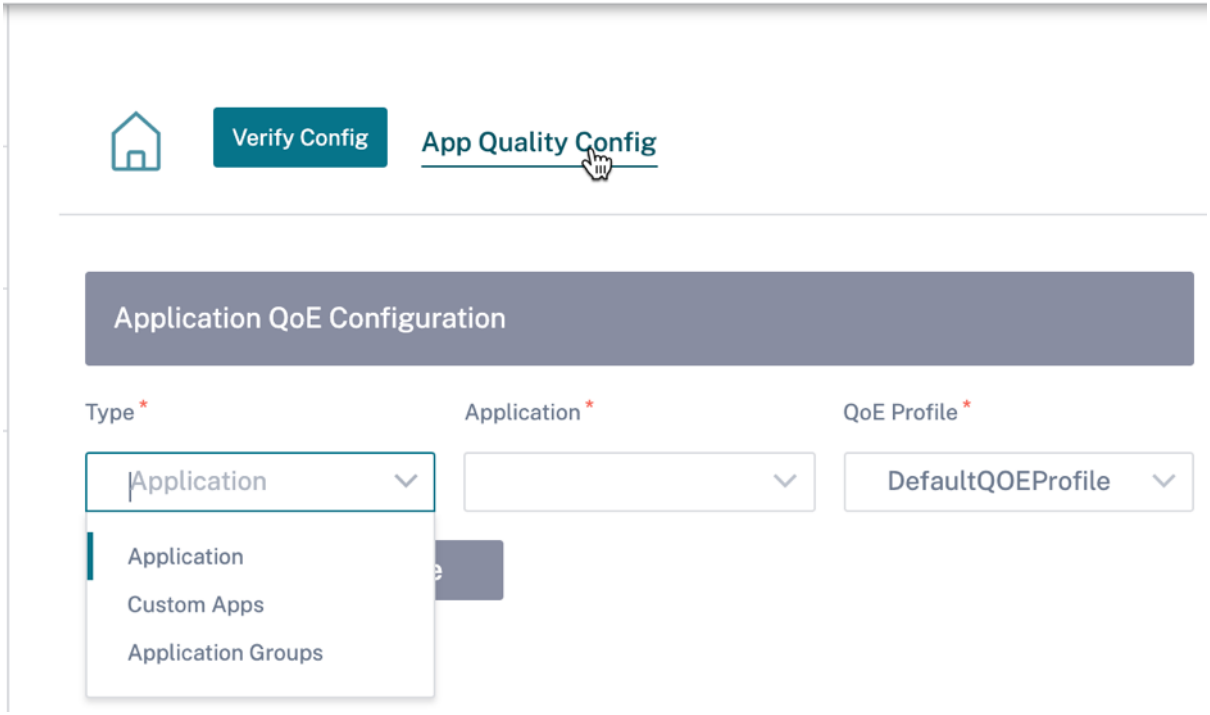
- Der prozentuale Verlust für einen Fluss liegt unter dem konfigurierten Schwellenwert.
- Die ausgehende Burstrate entspricht mindestens dem konfigurierten Prozentsatz der eingehenden Burstrate.

Konfiguration der Anwendungsqualität

Ordnen Sie Anwendungs- oder Anwendungsobjekte Standard-oder benutzerdefinierten QoE-Profilen Sie können benutzerdefinierte QoE-Profile für Echtzeit- und interaktiven Datenverkehr erstellen.

Klicken Sie **+QoE-Konfiguration**, um benutzerdefinierte QoE-Profile zu erstellen:

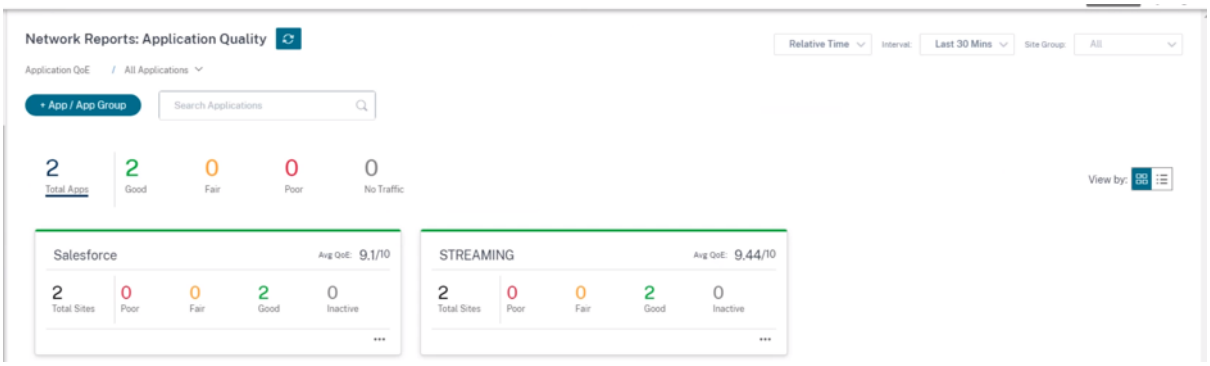
- **Typ**: Wählen Sie die DPI-Anwendung oder ein Anwendungsobjekt aus (Anwendung, Benutzerdefinierte Apps und Anwendungsgruppen).
- **Anwendung**: Suchen und wählen Sie eine Anwendung oder ein Anwendungsobjekt basierend auf dem ausgewählten Typ aus.
- **QoE-Profil**: Wählen Sie ein QoE-Profil aus, das der Anwendung oder dem Anwendungsobjekt zugewiesen werden soll.



Klicken Sie auf **Fertig**.

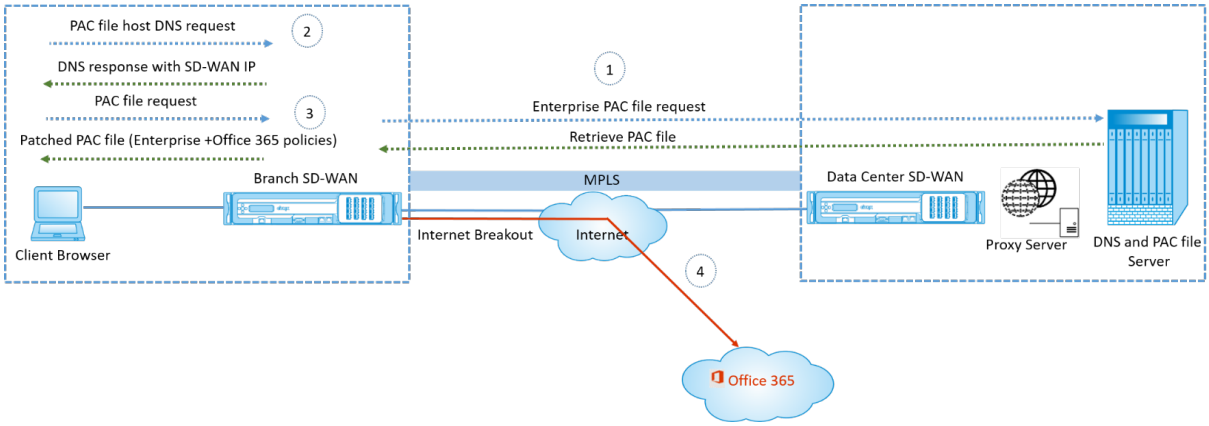
Klicken Sie auf **Konfiguration überprüfen**, um einen Überwachungsfehler zu überprüfen.

Sobald Sie die QoE der Anwendung mit dem benutzerdefinierten Anwendungstyp konfiguriert haben, wird unter **Berichte > Anwendungsqualität automatisch eine entsprechende Anwendungsberichtskachel**generiert. Jeglicher Datenverkehr, der mit der ausgewählten Anwendung übereinstimmt, wird über den virtuellen Pfad für die benutzerdefinierte Anwendung geleitet.



So funktioniert die Anpassung von PAC-Dateien

Idealerweise werden die PAC-Datei des Unternehmensnetzwerks Host auf dem internen Webserver, diese Proxyeinstellungen über Gruppenrichtlinien verteilt. Der Client-Browser fordert vom Unternehmens-Webserver nach PAC-Dateien. Die Citrix SD-WAN Appliance stellt die benutzerdefinierten PAC-Dateien für Sites bereit, auf denen Office 365-Breakout aktiviert ist.



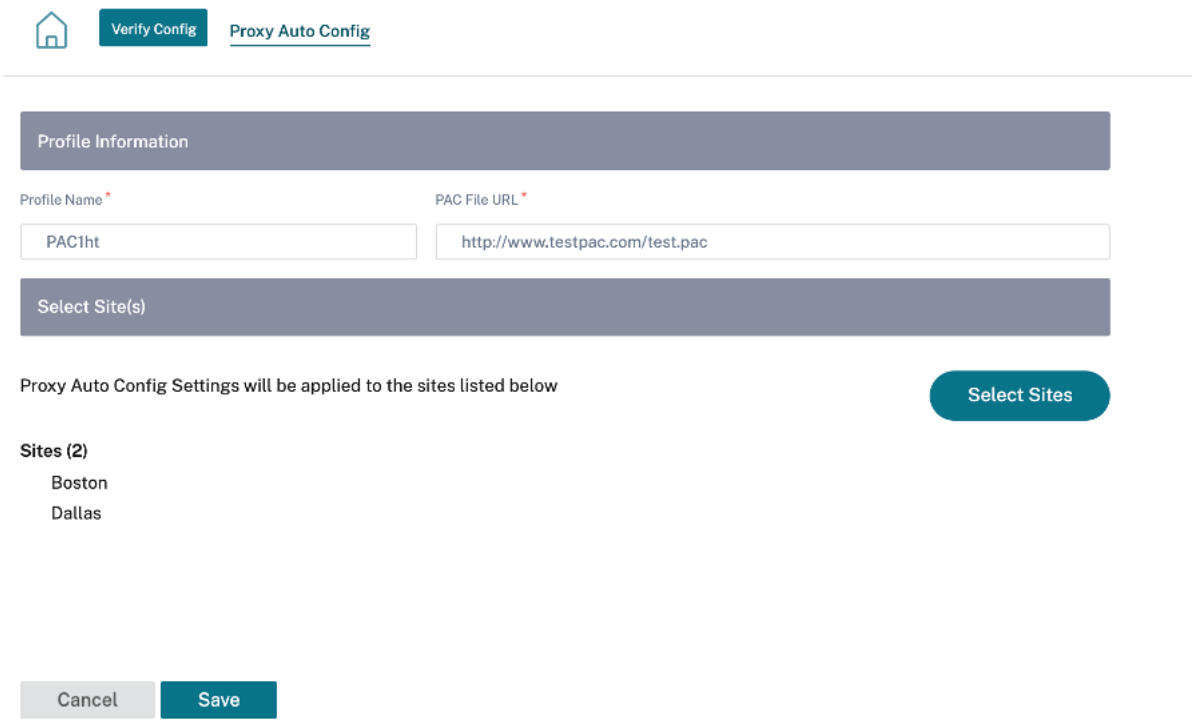
1. Citrix SD-WAN fordert regelmäßig die neueste Kopie der Enterprise-PAC-Datei vom Unternehmens-Webserver an und ruft sie ab. Die Citrix SD-WAN-Appliance patcht Office 365-URLs an die PAC-Datei des Unternehmens. Es wird erwartet, dass die Unternehmens-PAC-Datei einen Platzhalter (SD-WAN-spezifisches Tag) enthält, in dem die Office 365-URLs nahtlos gepatcht werden.
2. Der Client-Browser wirft eine DNS-Anfrage für den Unternehmens-PAC-Dateihost aus. Citrix SD-WAN fängt die Anforderung für die Proxy-Konfigurationsdatei FQDN ab und antwortet mit dem Citrix SD-WAN VIP.
3. Der Client-Browser fordert die PAC-Datei an. Die Citrix SD-WAN Appliance stellt die gepatchte PAC-Datei lokal bereit. Die PAC-Datei enthält die Unternehmensproxy-Konfiguration und Office 365-URL-Ausschlussrichtlinien.
4. Nach Erhalt einer Anfrage für die Office 365-Anwendung führt die Citrix SD-WAN Appliance ein direktes Internetbreakout durch.

Voraussetzungen

1. Die Unternehmen müssen eine PAC-Datei gehostet haben.
2. Die PAC-Datei muss einen Platzhalter *SDWAN_TAG* oder ein Vorkommen der `findproxyforurl` Funktion zum Patchen von Office 365-URLs haben.
3. Die URL der PAC-Datei muss domänenbasiert und nicht IP-basiert sein.
4. Die PAC-Datei wird nur über die vertrauenswürdigen Identitäts-VIPs bereitgestellt.
5. Die Citrix SD-WAN Appliance muss in der Lage sein, die Unternehmens-PAC-Datei über ihre Verwaltungsschnittstelle herunterzuladen.

Konfigurieren der automatischen Proxy-Konfiguration

Navigieren Sie in der SD-WAN Orchestator-Benutzeroberfläche auf Netzwerkebene zu **Konfiguration** > **App-Einstellungen und Gruppen** > **Automatische Proxy-Konfiguration** und klicken Sie auf **+ PAC-Dateiprofil**.



Geben Sie einen Namen für das PAC-Dateiprofil ein und geben Sie die URL des PAC-Dateiservers des Unternehmens an. Die Office 365-Breakoutregeln werden dynamisch in die Enterprise-PAC-Datei gepatcht.

Wählen Sie die Sites aus, auf die das PAC-Dateiprofil angewendet wird. Wenn für jede Site unterschiedliche URLs vorhanden sind, erstellen Sie pro Site ein anderes Profil.

Einschränkungen

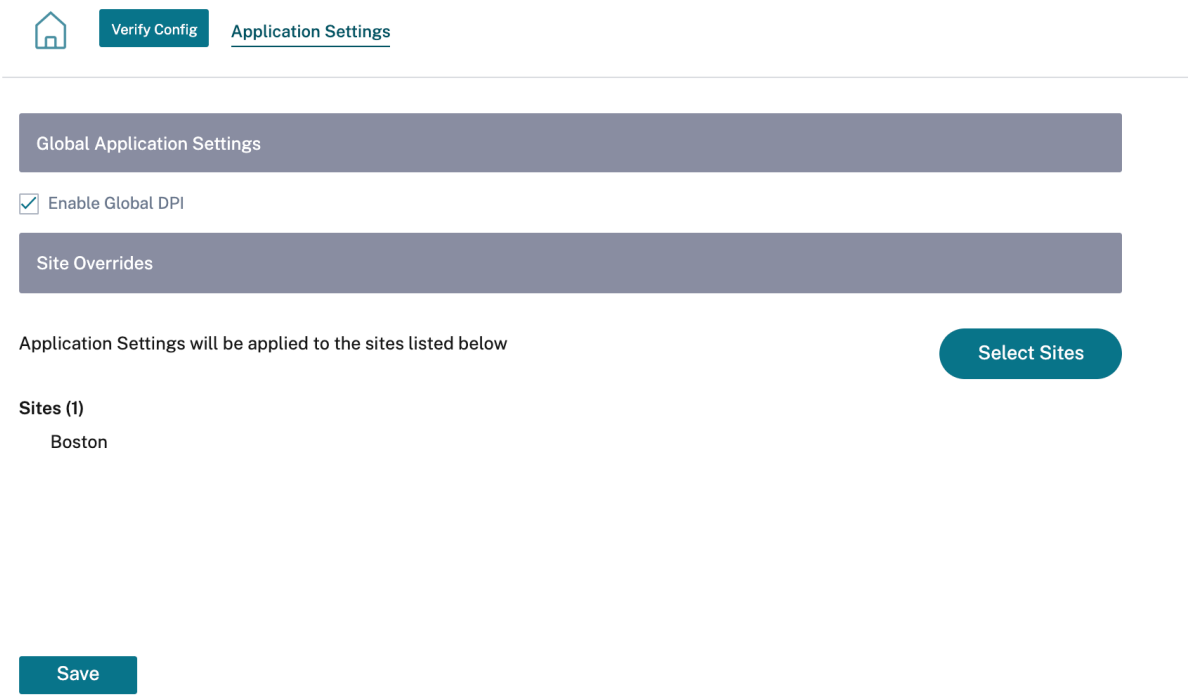
- HTTPS PAC-Dateiserver-Anfragen werden nicht unterstützt.
- Mehrere PAC-Dateien in einem Netzwerk werden nicht unterstützt, einschließlich PAC-Dateien für Routingdomänen oder Sicherheitszonen.
- Das Erzeugen einer PAC-Datei auf Citrix SD-WAN von Grund auf wird nicht unterstützt.
- WPAD über DHCP wird nicht unterstützt.

DPI-Einstellungen

Die Citrix SD-WAN Appliances führen Deep Packet Inspection (DPI) durch, um Anwendungen zu identifizieren und zu klassifizieren. Die DPI-Bibliothek erkennt Tausende von kommerziellen Anwendungen. Es ermöglicht die Erkennung und Klassifizierung von Anwendungen in Echtzeit. Mithilfe der DPI-Technologie analysiert die SD-WAN-Appliance die eingehenden Pakete und klassifiziert den Datenverkehr als zu einer bestimmten Anwendung oder Anwendungsfamilie.

DPI ist standardmäßig global für alle Sites in Ihrem Netzwerk aktiviert. Die Deaktivierung von DPI stoppt die DPI-Klassifizierungsfunktion auf der Appliance. Sie können keine DPI-klassifizierten Anwendungs-/Anwendungskategorien mehr verwenden, um Firewall-, QoS- und Routing-Richtlinien zu konfigurieren. Sie können auch den Bericht über die wichtigsten Anwendungen und Anwendungskategorien nicht anzeigen.

Um globale DPI-Werte zu deaktivieren, navigieren Sie auf Netzwerkebene zu **Konfiguration > App-Einstellungen & Gruppen > DPI-Einstellungen** und deaktivieren Sie das Kontrollkästchen **Globale DPI aktivieren** .



Sie können DPI auch nur für bestimmte Sites deaktivieren, indem Sie die globalen DPI-Einstellungen überschreiben. Um DPI für ausgewählte Sites zu deaktivieren, fügen Sie die Sites zur Liste **Site-Überschreibungen** hinzu.

Profile und Vorlagen

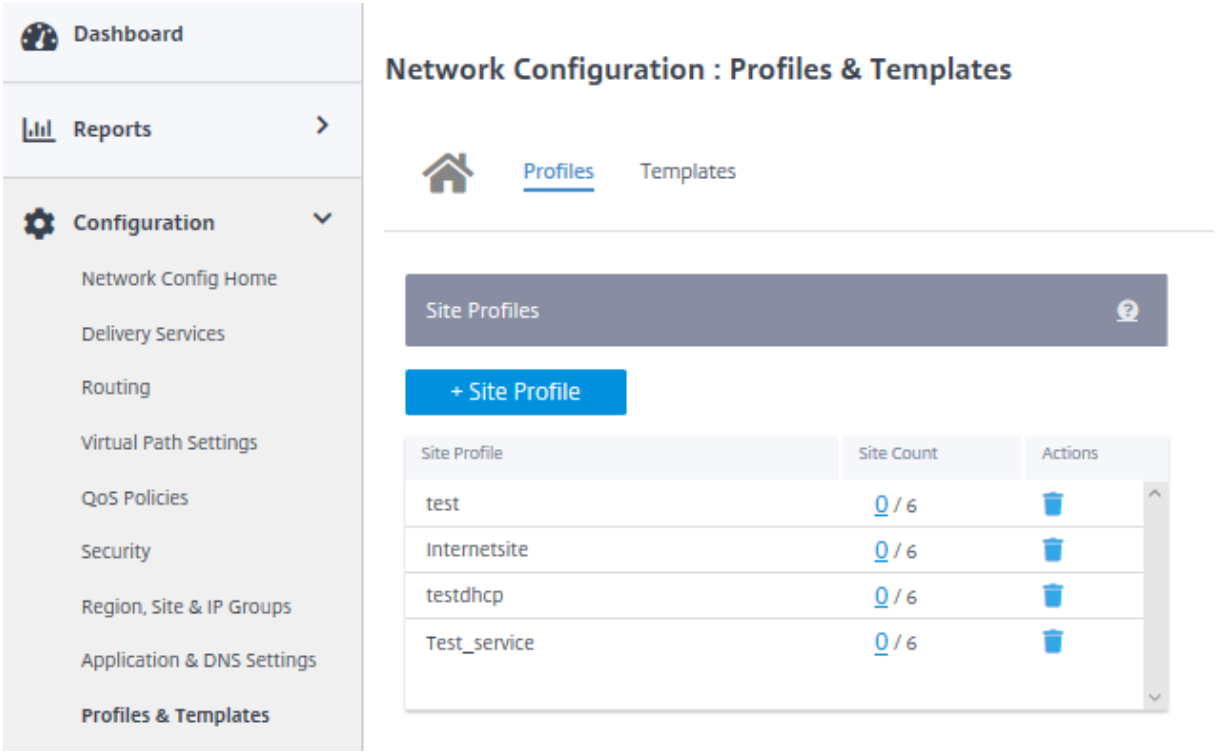
October 21, 2022

Ein Profil ist eine Live-Konfigurationsvorlage. Eine reguläre Vorlage hilft bei der Erstellung einer neuen Entität. Sobald die Vorlage erstellt wurde, gelten nachfolgende Änderungen in der Vorlage nicht für die vorhandenen Entitäten, die mit der Basisvorlage erstellt wurden. Ein Profil dient als zentrale Live-Master-Entität. Alle untergeordneten Entitäten erben vom Profil, nicht nur während der Erstellung, sondern auch während der gesamten Lebensdauer eines Profils. Alle untergeordneten Entitäten, die dem Profil zugeordnet sind, erben automatisch alle in einem Profil vorgenommenen Änderungen.

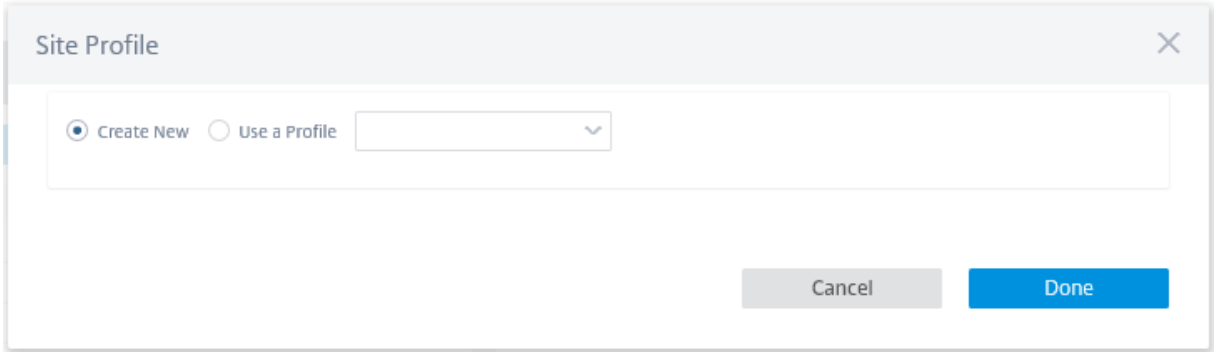
Ein Administrator erstellt beispielsweise ein Site-Konfigurationsprofil, das als kleines Einzelhandelsgeschäft bezeichnet wird, und wendet es auf alle kleinen Einzelhandelsgeschäfte an, die einem Unternehmen gehören. Jetzt werden alle Änderungen, die zu einem bestimmten Zeitpunkt am Profil eines kleinen Einzelhandelsgeschäfts vorgenommen wurden, automatisch auf alle Geschäfte angewendet, die dieses Profil erben. Basierend auf dem, was in allen Entitäten gemeinsam ist und was nicht, können bestimmte Parameter in der Profilkonfiguration nicht festgelegt werden. Solche Parameter wären anpassbar und können zwischen den Entitäten, die dasselbe Profil erben, variieren.

Site-Profile

Mit Site-Profilen können Sie Websites einfach und schnell konfigurieren. Sie können ein Site-Profil einmal erstellen und es beim Erstellen von Websites mehrmals wiederverwenden.

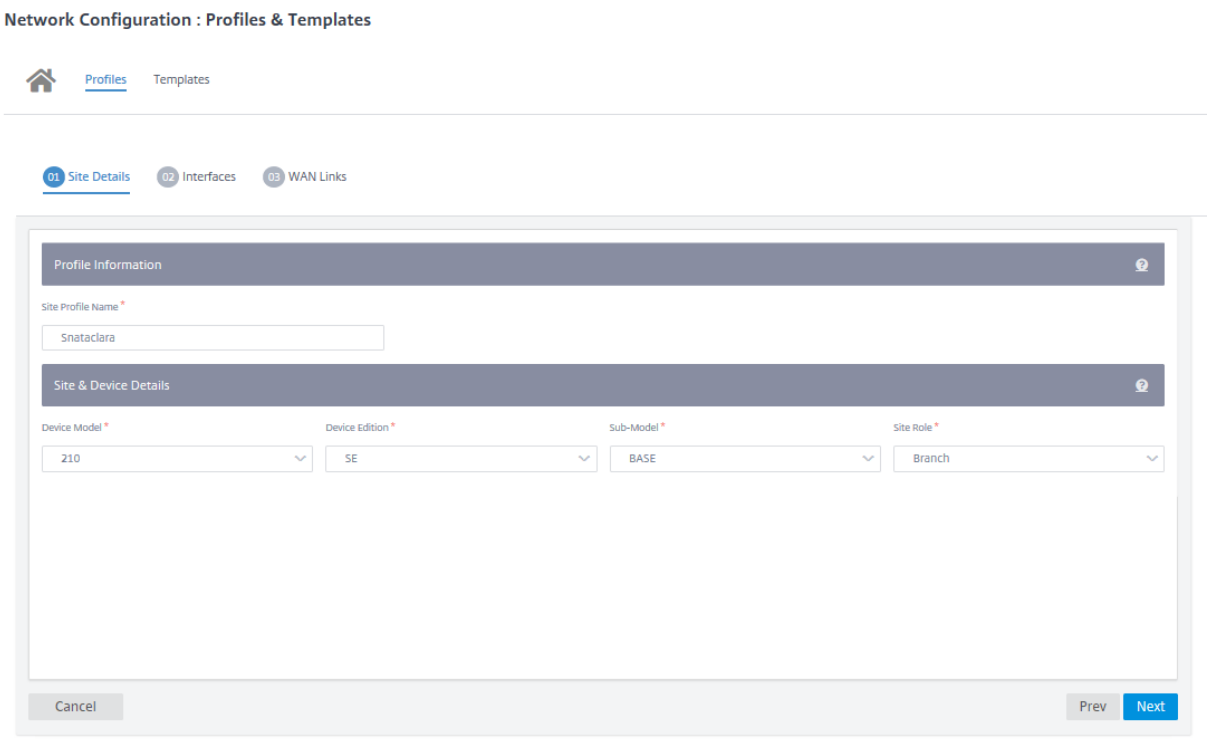


Um ein Site-Profil zu erstellen, klicken Sie auf **+ Site-Profil**. Sie können ein Profil von Grund auf neu erstellen oder ein vorhandenes Site-Profil bearbeiten und es als neues Profil speichern.

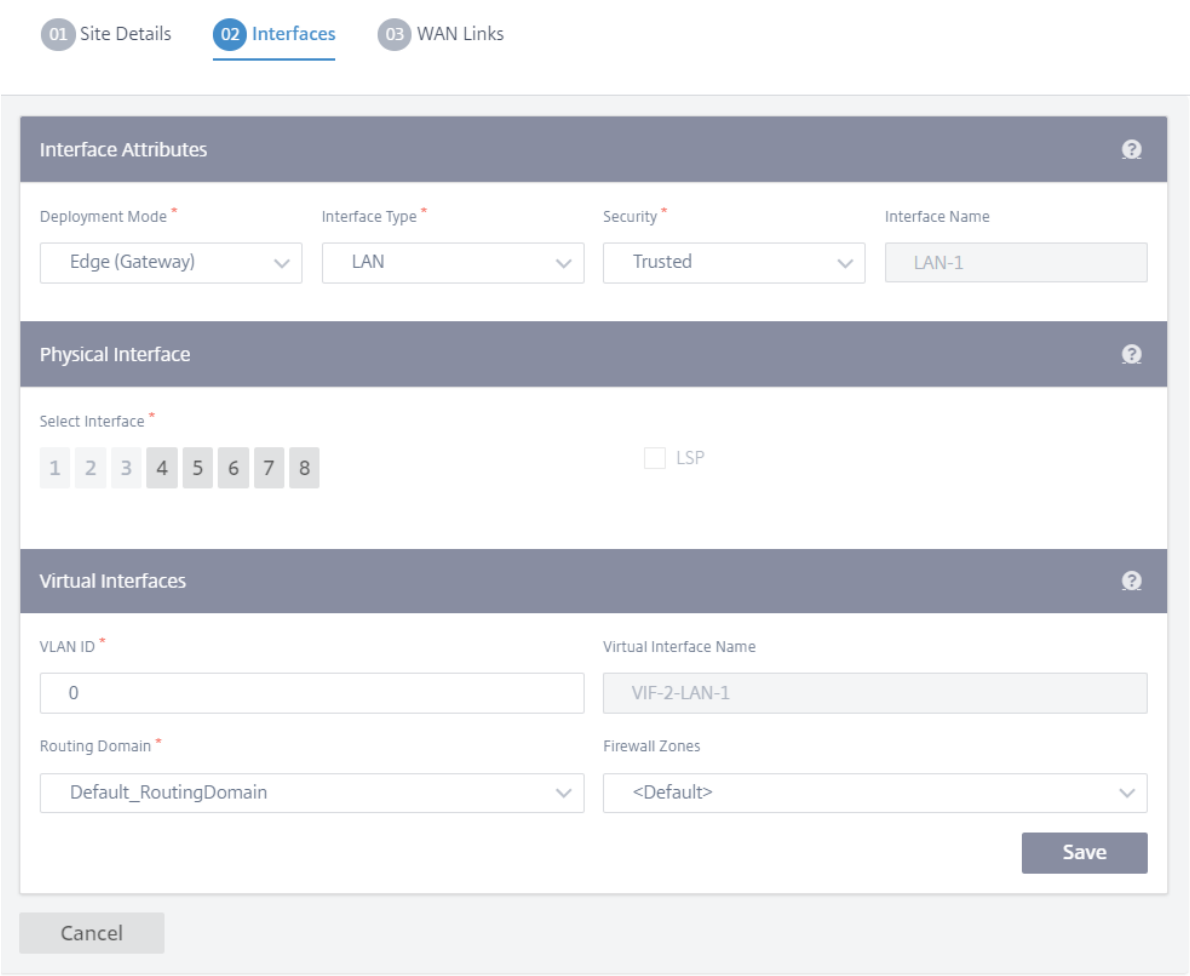


Um ein Standortprofil zu erstellen, müssen Sie die **Standortdetails**, **Schnittstellen**und **WAN-Links**konfigurieren. Eine detaillierte Beschreibung der Konfiguration von Sites finden Sie unter Site-Details .

Geben Sie die Gerätedetails an.

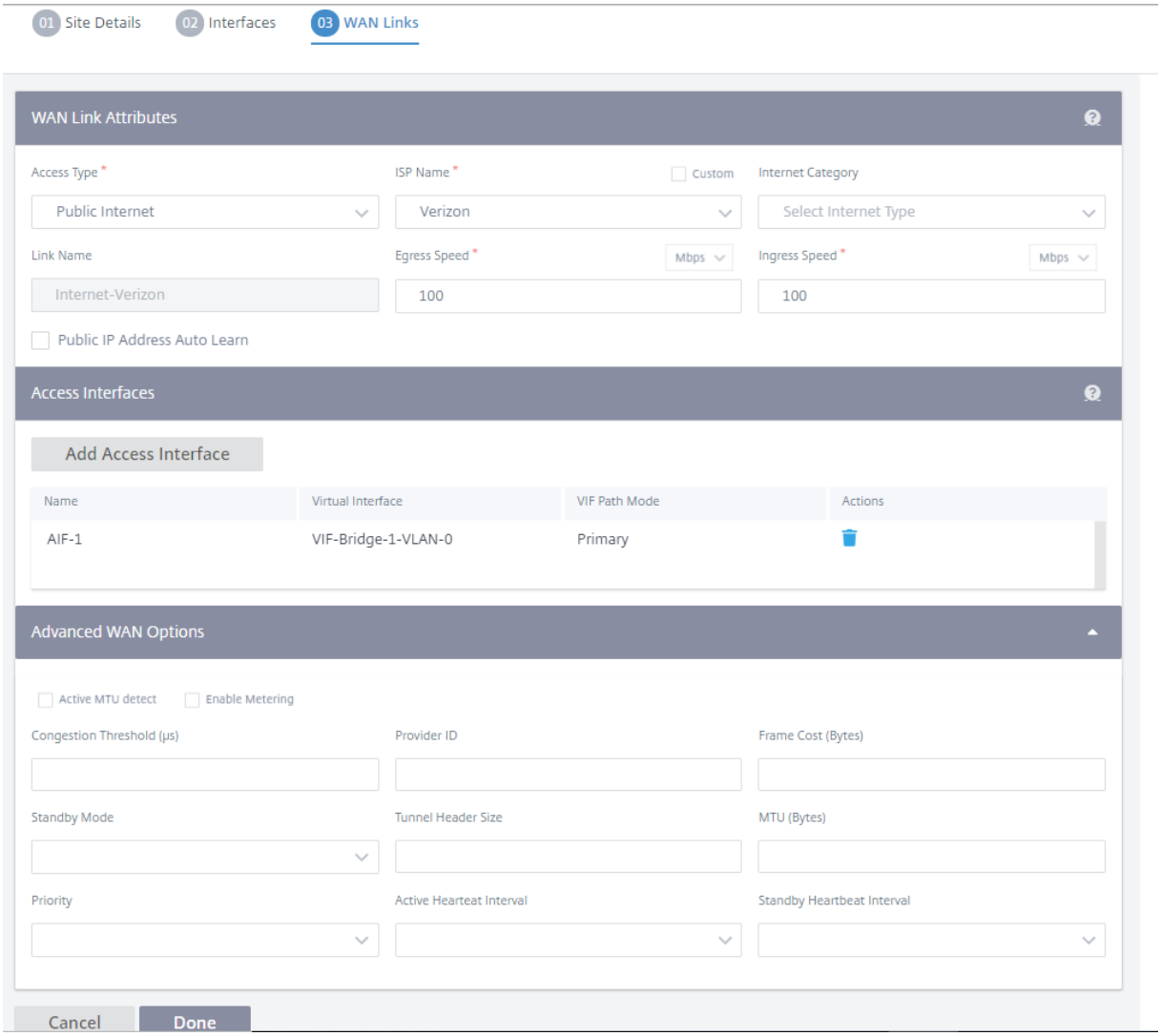


Weisen Sie der Site eine Schnittstelle zu, indem Sie auf die Option **+ Schnittstelle** klicken. Um eine Schnittstelle hinzuzufügen, müssen Sie die Felder **Schnittstellenattribute**, **Physikalische Schnittstelle**und **Virtuelle Schnittstellen** ausfüllen. Eine detaillierte Beschreibung der Konfiguration von Schnittstellen finden Sie unter Interfaces.



Füllen Sie **WAN-Link-Attribute**, **Zugriffsschnittstellen**und **Dienste** mit **erweiterten Optionen**.

Eine ausführliche Beschreibung der Konfiguration von WAN-Verbindungen finden Sie unter WAN-Links.



Vorlagen

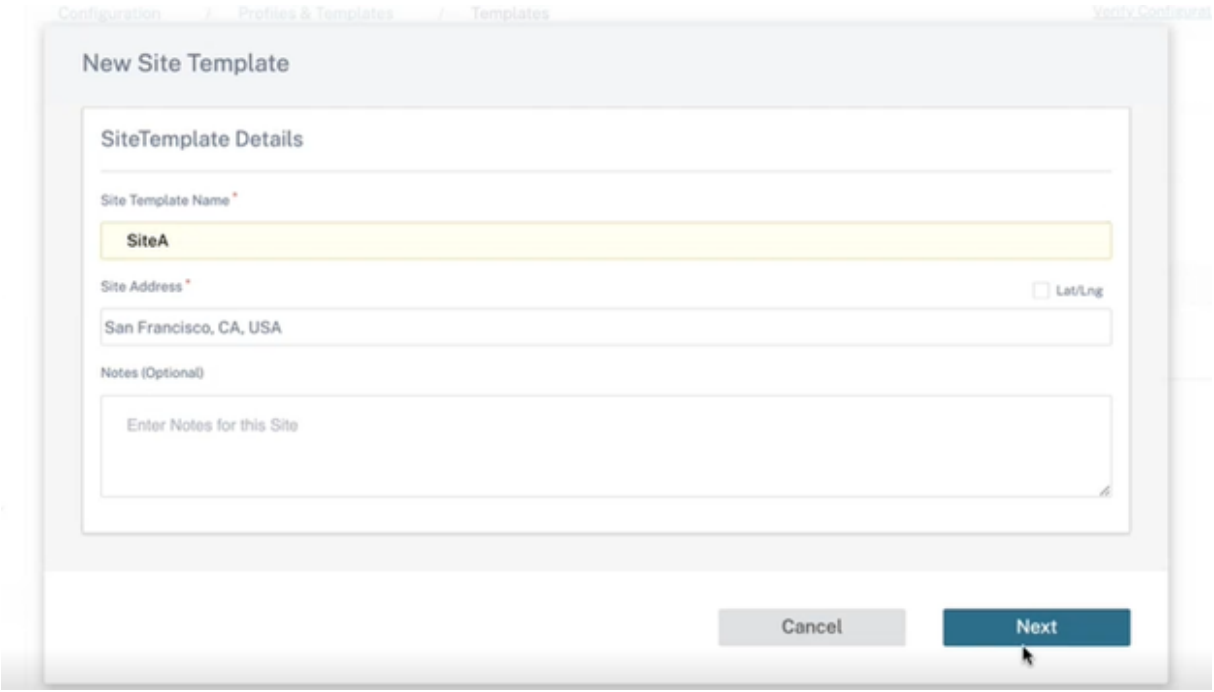
Mit dem Citrix SD-WAN Orchestrator Service können Sie Vorlagen als vordefinierten Satz von Feldern verwenden, um eine neue Site oder eine WAN-Verbindung zu konfigurieren.

Site-Vorlage

Eine Site-Vorlage ist eine vordefinierte Vorlage, die für die Site-Erstellung verwendet Um eine Site mithilfe einer vordefinierten Site-Vorlage zu konfigurieren, navigieren Sie auf Kundenebene zu **Konfiguration** > **Profile und Vorlagen** > **Vorlagen**. Klicken Sie im Abschnitt **Site-Vorlage** auf **Site-Vorlage hinzufügen**.

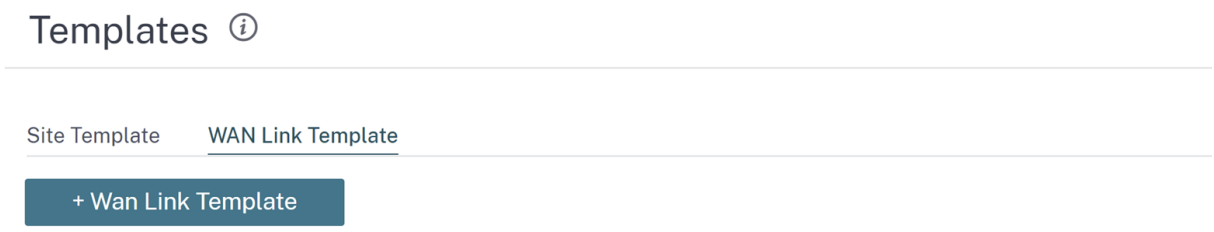
Geben Sie im angezeigten Bildschirm **Neue Site-Vorlage** die erforderlichen Details ein und klicken Sie auf **Weiter**.

> **Hinweis**
>
> Wenn Sie eine Site klonen oder eine Site mithilfe einer Site-Vorlage erstellen und für die Quelle Wi-Fi konfiguriert ist, werden die Wi-Fi-Einstellungen nicht auf die neue Site kopiert.

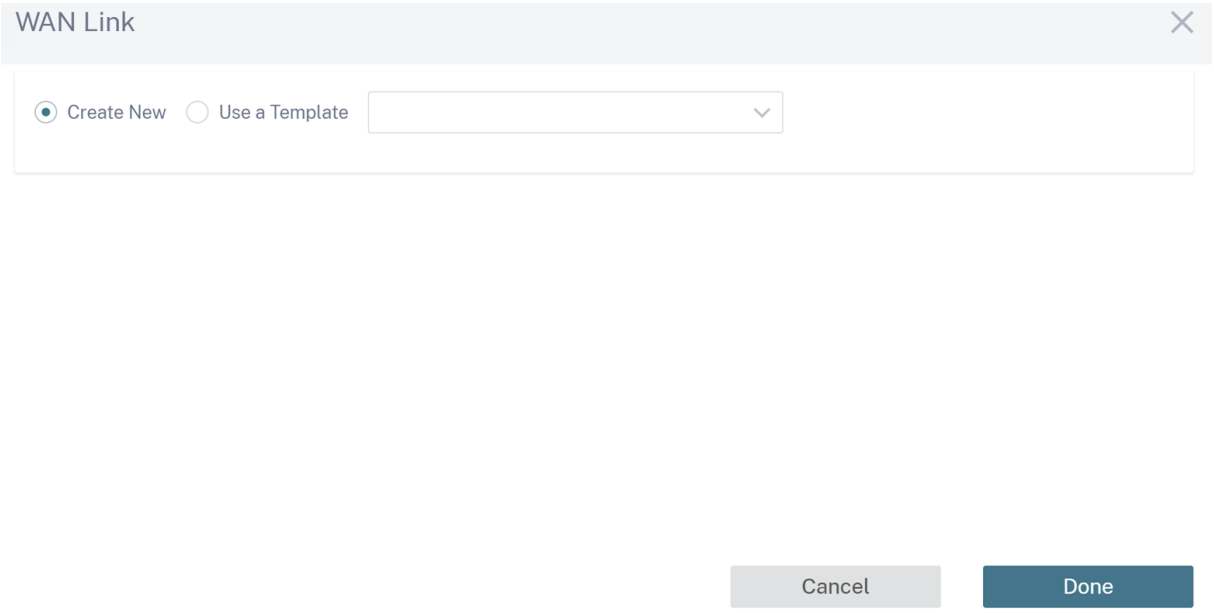


WAN-Link-Vorlage

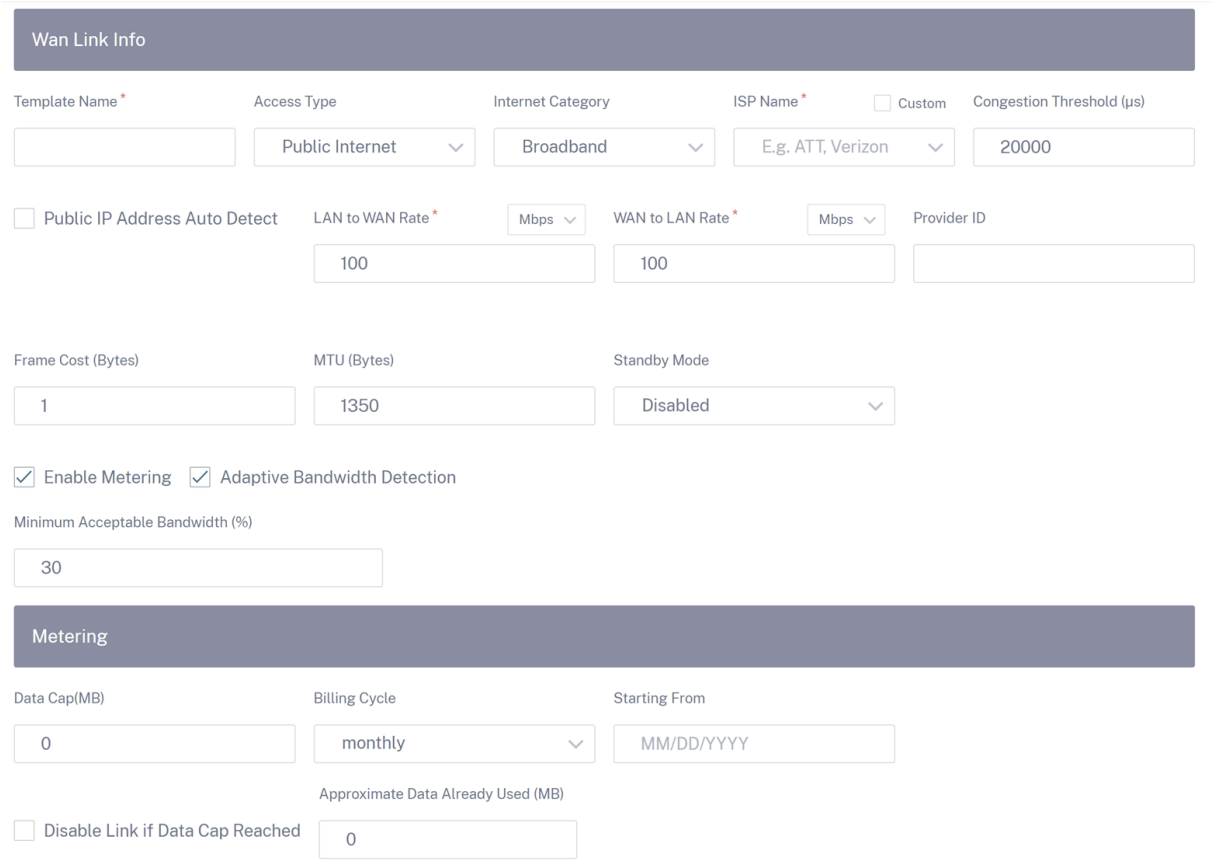
Mithilfe von WAN-Link-Vorlagen können Sie WAN-Links einfach und schnell konfigurieren. Sie können eine WAN-Link-Vorlage einmal erstellen und bei der Konfiguration von WAN-Verbindungen mehrmals wiederverwenden. Sie können sogar die geänderten WAN-Link-Vorlagenkonfigurationen in die WAN-Link-Konfigurationen des Standorts kopieren, die mit der WAN-Link-



Zum Erstellen einer WAN-Link-Vorlage klicken Sie auf **+ WAN-Link-Vorlage**. Sie können eine Vorlage von Grund auf neu erstellen oder eine vorhandene WAN-Link-Vorlage bearbeiten und als neue Vorlage speichern.



Geben Sie die WAN-Link-Informationen wie **Profilname**, **Zugriffstyp**, **Internetkategorie**, **LAN-zu-WAN-Rate** (Mbit/s) usw. an, um ein WAN-Profil zu erstellen. Eine ausführliche Beschreibung der Konfiguration von WAN-Verbindungen finden Sie unter WAN-Links.

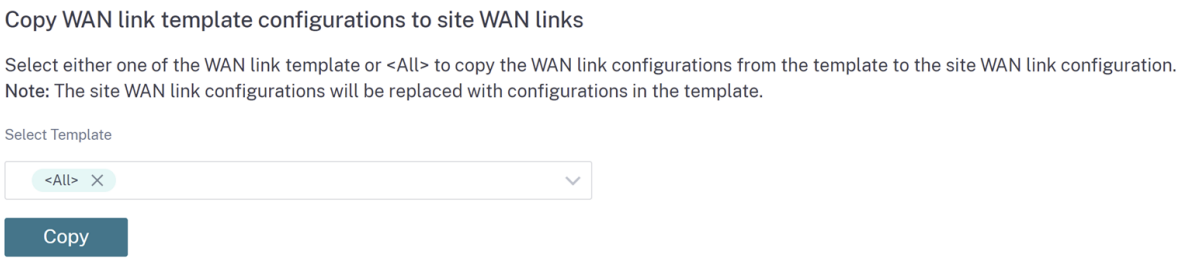


Bisher war die Option zum Kopieren der geänderten WAN-Link-Vorlagenkonfigurationen in Standort-

WAN-Link-Konfigurationen nicht verfügbar. Wenn ein Benutzer beispielsweise bereits mehrere Standort-WAN-Links mithilfe einer WAN-Link-Vorlage erstellt hatte und eine bestimmte Konfiguration ändern musste (z. B. die Einstellung des Überlastungsschwellenwerts), musste der Benutzer dies für jede Standort-WAN-Verbindung einzeln vornehmen. Von nun an kann der Benutzer die WAN-Link-Vorlage mit der neuen Einstellung für den Überlastungsschwellenwert aktualisieren und die neuesten WAN-Link-Vorlagenkonfigurationen auf alle WAN-Links des Standorts kopieren, die mithilfe der WAN-Link-Vorlage

Wenn Sie eine oder mehrere WAN-Link-Vorlagen auswählen und auf Kopieren klicken, werden die an der WAN-Link-Vorlage vorgenommenen Aktualisierungen in die WAN-Link-Konfiguration des Standorts kopiert, die mit den ausgewählten Vorlagen erstellt wurde.

> **Hinweis:**
>
> Die WAN-Link-Site-Konfigurationen, die mithilfe der Standortprofilfunktion erstellt wurden, werden nicht aktualisiert.



Netzwerkstandort-Service

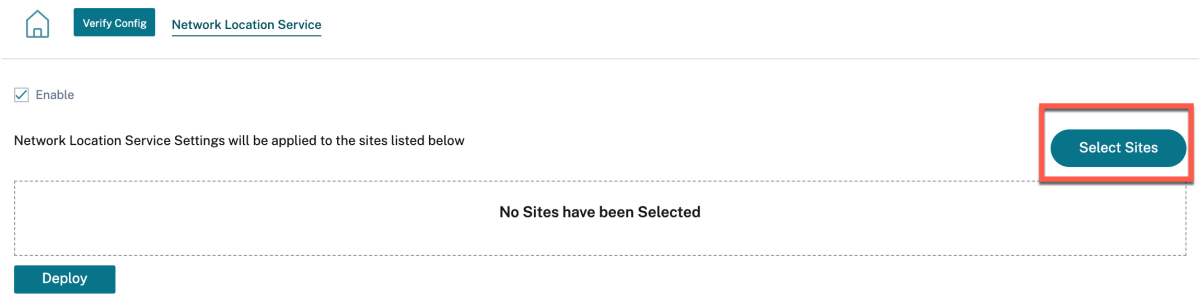
October 21, 2022

Der Netzwerkstandortdienst (NLS) ist ein Citrix Cloud Cloud-Dienst, der bestimmt, ob der Benutzer, der eine Verbindung zu Citrix Virtual Apps and Desktops herstellt, aus dem internen Netzwerk stammt. Mit NLS können Sie vermeiden, dass IP-Adressen von von Citrix SD-WAN bereitgestellten Speicherorten über das PowerShell-Skript manuell konfiguriert werden. Detaillierte Informationen zu NLS finden Sie unter Citrix Workspace Network Location Service.

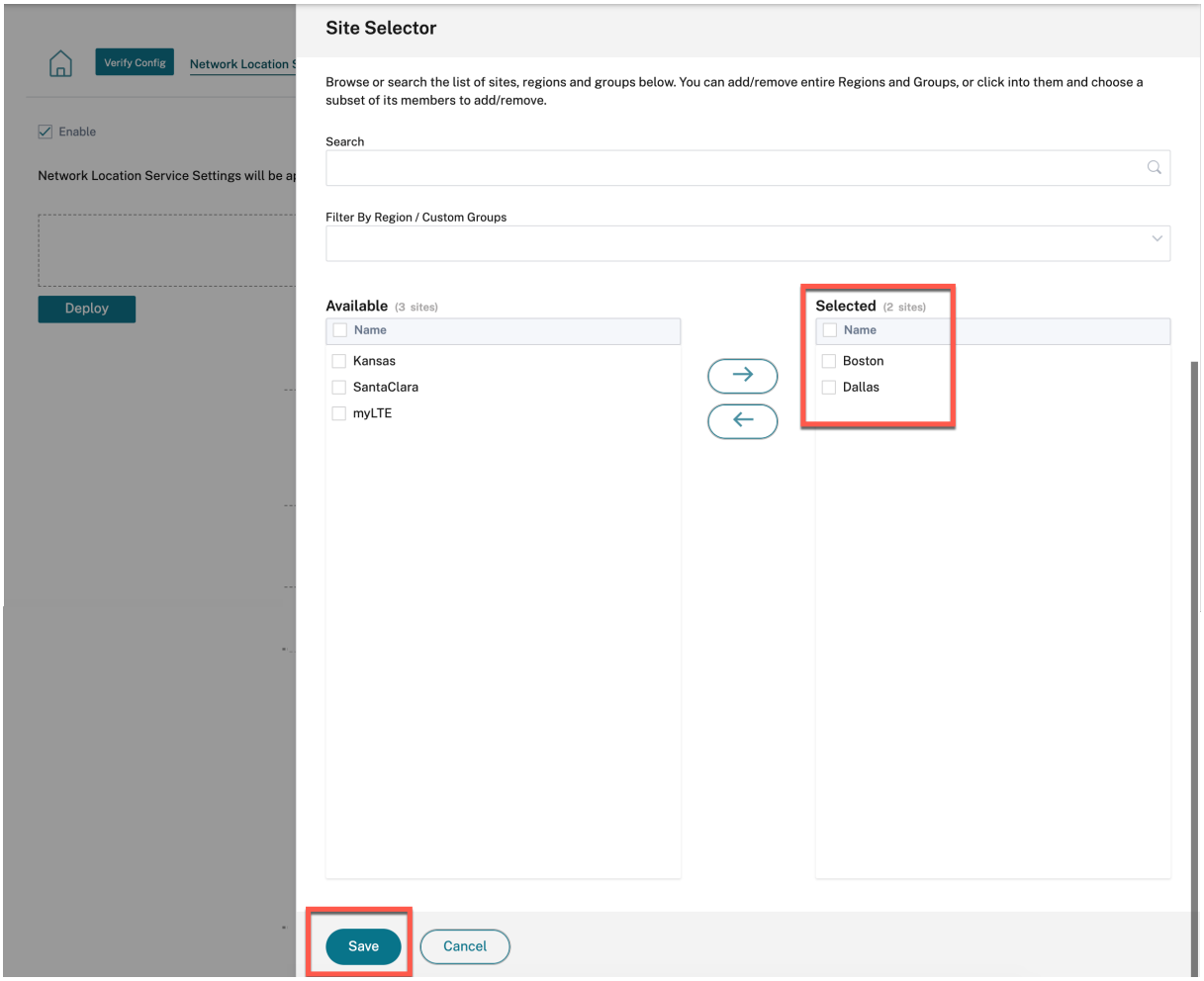
Sie können NLS für alle Standorte innerhalb des Netzwerks oder für bestimmte Sites aktivieren. Die für NLS aktivierte Site teilt die öffentliche IP-Adresse aller Internet-WAN-Links zusammen mit anderen Standortdetails wie geografischem Standort und Zeitzone mit der NLS-Datenbank. Anhand dieser Details bestimmt der Netzwerkstandortdienst, ob sich der Benutzer, der eine Verbindung zu Citrix Virtual Apps and Desktops herstellt, in einem Netzwerk befindet, das von Citrix SD-WAN bereitgestellt wird.

Wenn eine Benutzeranforderung von einem Front-End-Netzwerk von Citrix SD-WAN kommt, wird der Benutzer unter Umgehung des Citrix Gateway-Dienstes direkt mit dem Citrix Virtual Apps and Desktops Virtual Delivery Agent verbunden.

Um NLS zu aktivieren, navigieren Sie auf Kundenebene zu **Konfiguration > Network Location Service**.



Wählen Sie **Aktivieren**, wenn Sie NLS für alle Standorte im Netzwerk aktivieren möchten. Um NLS für bestimmte Sites zu aktivieren, klicken Sie auf **Sites auswählen**. Wählen Sie die **Region** und wählen Sie die Standorte entsprechend aus. Klicke auf **Speichern** und dann auf **Bereitstellen**.



ECMP Load Balancing

October 21, 2022

Equal Cost Multi-Path (ECMP) -Gruppen ermöglichen es Ihnen, mehrere Pfade mit denselben Kosten, Zielen und demselben Service zu gruppieren. Die Verbindungen oder Sitzungsdaten haben je nach Typ der ECMP-Gruppe einen Lastenausgleich über alle Pfade in der ECMP-Gruppe. Stellen Sie sich beispielsweise ein Netzwerk mit zwei WAN-Verbindungen zwischen einer Zweigstelle und einem Rechenzentrum mit den gleichen Routenkosten vor. Traditionell wäre einer der WAN-Verbindungen aktiv und der andere bleibt inaktiv und fungiert als Fallback-Link. Mit ECMP-Gruppen können Sie diese WAN-Verbindungen zusammenfassen und den Lastausgleich des Datenverkehrs über beide WAN-Verbindungen zulassen. Der ECMP-Lastenausgleich gewährleistet:

- Verteilung des Datenverkehrs auf mehrere kostengleiche Wege.
- Optimale Nutzung der verfügbaren Bandbreite.

- Dynamische Übertragung des Datenverkehrs auf einen anderen ECMP-Mitgliedspfad, wenn eine Route nicht mehr erreichbar ist.

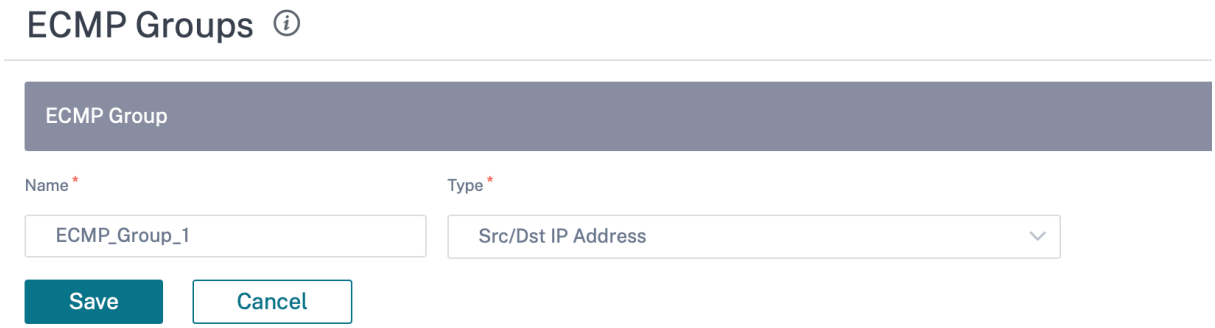
ECMP-Lastenausgleich wird von den folgenden Diensten unterstützt:

- Virtuelle Pfade
- Citrix Secure Internet Access
- Z-Scaler
- IPsec
- GRE

Sie können maximal 254 ECMP-Gruppen in Ihrem Netzwerk definieren. Die maximale Anzahl von ECMP-berechtigten Routen in einer ECMP-Gruppe hängt von Ihrer Appliance und Ihrem Lizenztyp ab. Die folgenden zwei Arten von ECMP-Gruppen werden auf Citrix SD-WAN unterstützt:

- Quell-/Ziel-IP-Adresse: Netzwerke, in denen mehrere Clients versuchen, sich mit demselben Ziel zu verbinden, sind die Verbindungen über kostengünstige WAN-Verbindungen Lastausgleich.
- Sitzung: Netzwerke, in denen ein einzelner Client mit einem Ziel verbunden ist und mehrere Sitzungen erzeugt werden. Die Sitzungsdaten haben einen Lastausgleich bei WAN-Verbindungen mit gleichen Kosten.

Um eine ECMP-Gruppe zu konfigurieren, navigieren Sie auf Netzwerkebene zu **Konfiguration > Routing > ECMP-Gruppen**. Geben Sie einen Namen für die ECMP-Gruppe an und wählen Sie nach Bedarf den Typ als **Src/Dest-IP-Adresse** oder **Session** aus.

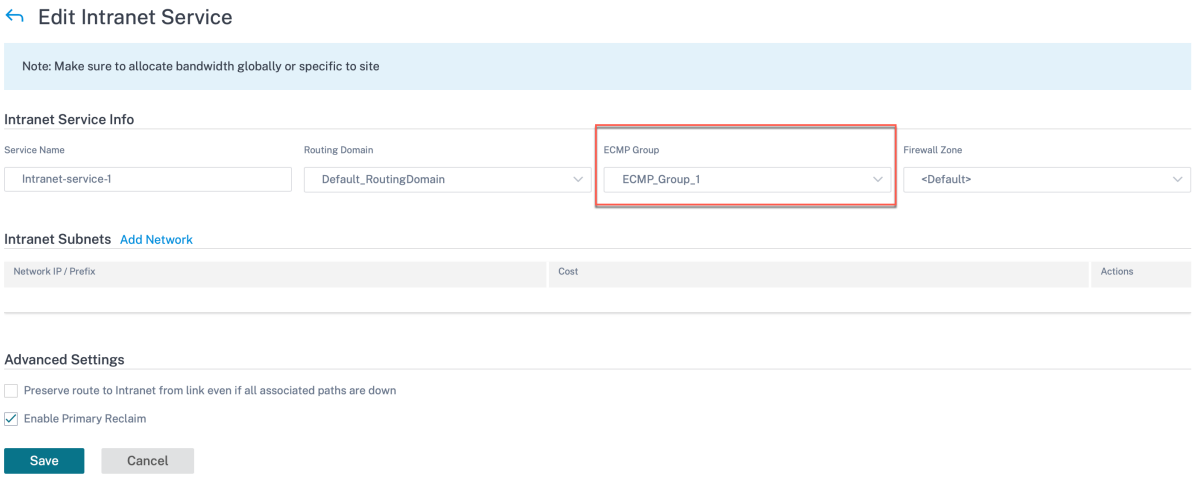


Sie können die ECMP-Gruppen den folgenden Diensten zuordnen:

- Virtuelle Pfade (auf Site-Ebene)
- Citrix Secure Internet Access
- Z-Scaler
- IPsec
- GRE

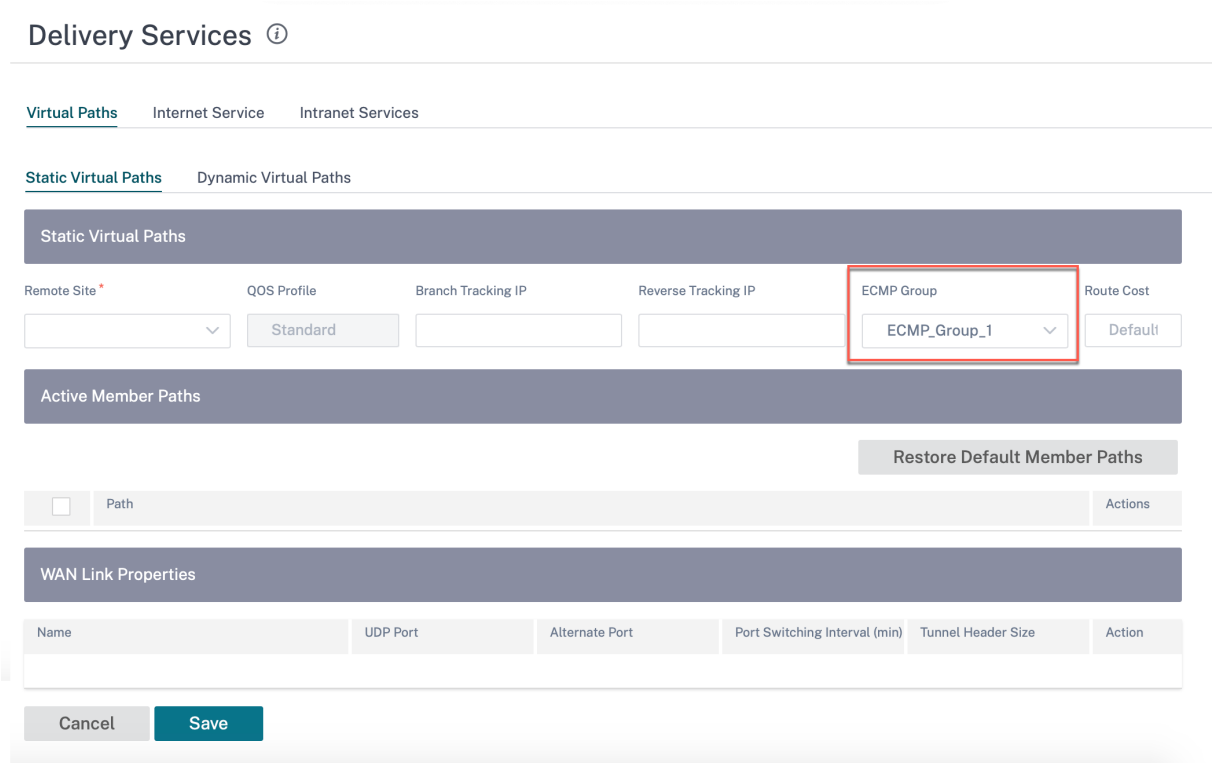
Um die ECMP-Konfiguration für Intranetdienste zu aktivieren, navigieren Sie auf Netzwerkebene zu **Konfiguration > Bereitstellungskanäle > Bandbreitenzuweisung > Intranet+Dienst**, und wählen Sie den **Diensttyp** als **Intranet**aus. Wählen Sie bei der Konfiguration des Intranetdienstes die ECMP-Gruppe aus.

> **Hinweis**
>
> Wenn Sie **Keine** auswählen, wird die ECMP-Konfiguration für den Dienst nicht aktiviert.



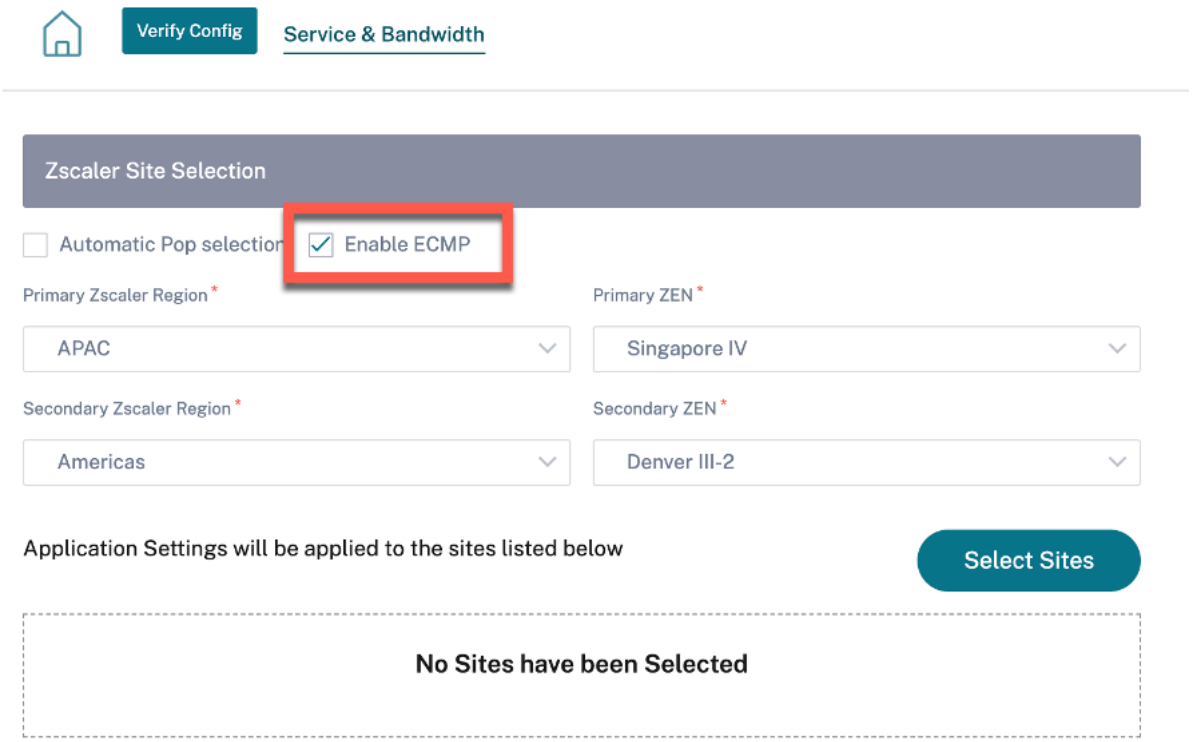
Um die ECMP-Konfiguration für virtuelle Pfade zu aktivieren, navigieren Sie auf Standortebene zu **Konfiguration** > **Erweiterte Einstellungen** > **Bereitstellungsdienste** > **Virtuelle Pfade** > **Statische virtuelle Pfade** > **+ Virtuelle Pfade**. Wählen Sie die ECMP-Gruppe aus, während Sie die statischen virtuellen Pfade konfigurieren.

> **Hinweis**
>
> Wenn Sie **Keine** auswählen, wird die ECMP-Konfiguration für den Dienst nicht aktiviert.



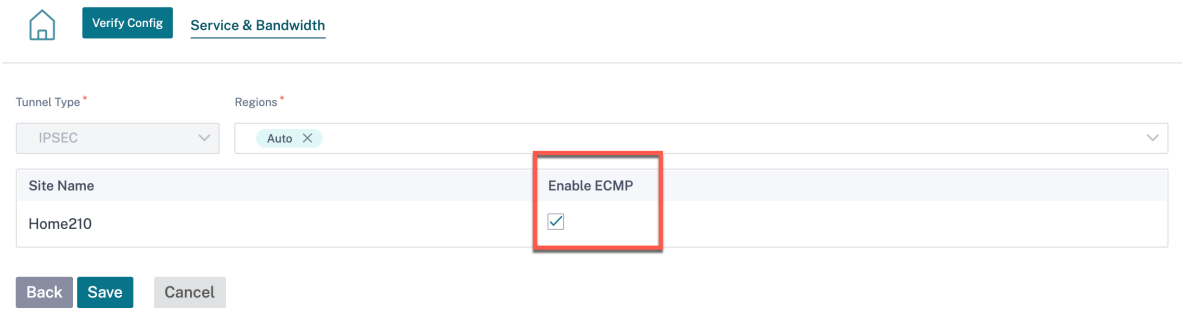
Um die ECMP-Konfiguration für Zscaler-Dienste zu aktivieren, navigieren Sie auf Netzwerkebene zu **Konfiguration > Dienste und Bandbreite**. Klicken Sie auf das Symbol **Einstellungen** neben Zscaler, das in der Spalte **Delivery Services** aufgeführt ist. Authentifizieren Sie sich und klicken Sie auf **+ Site** Aktivieren Sie beim Hinzufügen von Sites das Kontrollkästchen **ECMP** aktivieren.

> **HINWEIS: Der**
>
> Zscaler-Dienst unterstützt nur den sitzungsbasierten ECMP-Lastenausgleich.

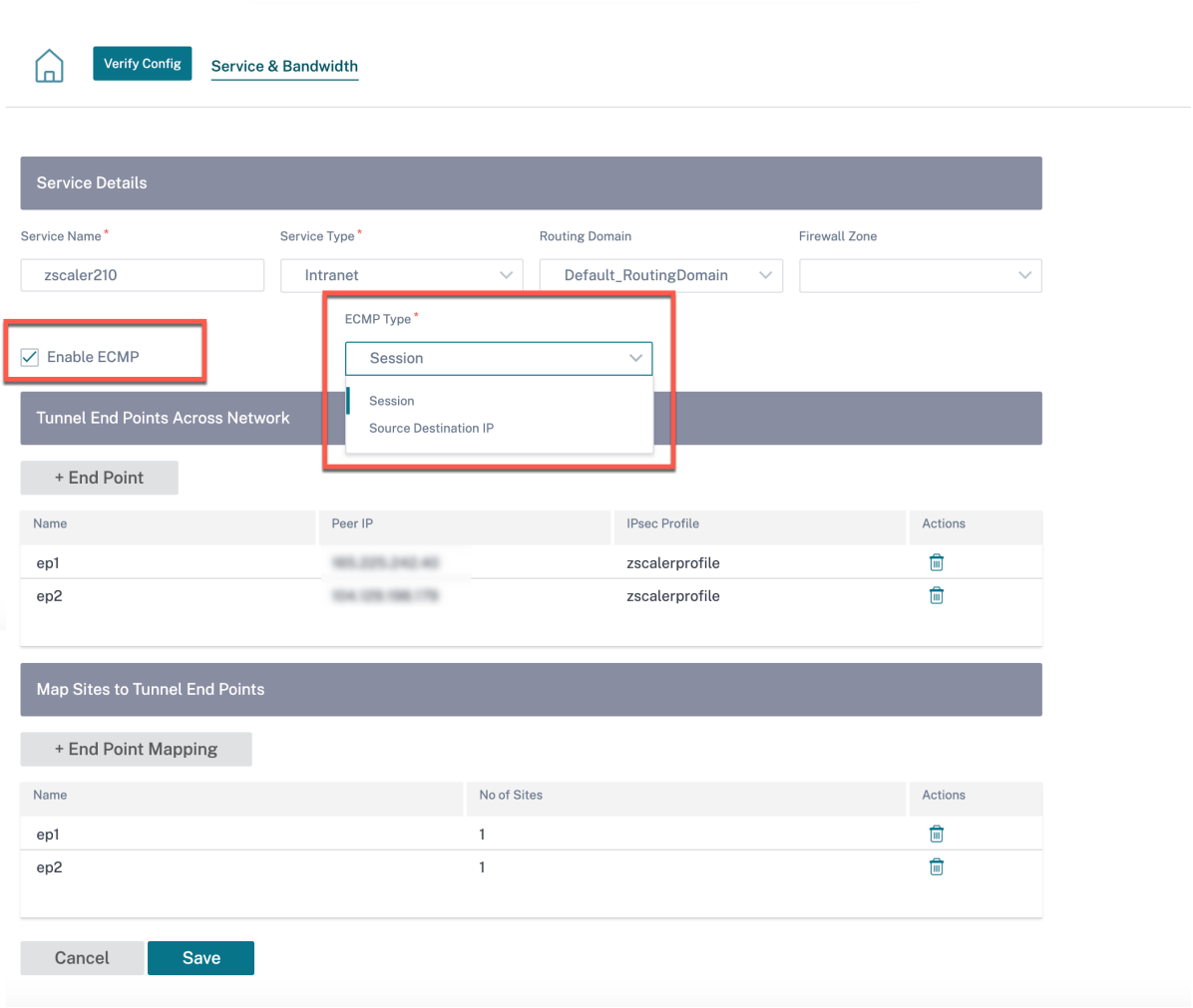


Um die ECMP-Konfiguration für den Citrix Secure Internet Access Service zu aktivieren, navigieren Sie auf Netzwerkebene zu **Konfiguration > Dienste und Bandbreite**. Klicken Sie auf das Symbol **Einstellungen** neben **Secure Internet Access Service** und dann auf **+ Site**. Aktivieren Sie das Kontrollkästchen **ECMP aktivieren**, nachdem Sie die Standorte ausgewählt haben.

> **HINWEIS Der**
>
> Citrix Secure Internet Access Service unterstützt nur den sitzungsbasierten ECMP-Lastenausgleich.



Um die ECMP-Konfiguration in festen IPSec-Tunneln mit Peers von Drittanbietern auf LAN- oder WAN-Seite zu aktivieren, navigieren Sie zu **Konfiguration > Dienste und Bandbreite > Intranet+Dienst** und wählen Sie den **Diensttyp** als **IPSec**aus. Aktivieren Sie das Kontrollkästchen **ECMP aktivieren**, und wählen Sie einen Typ aus der Dropdown-Liste **ECMP-Typ** aus.



Regeln für die Anwendung

October 21, 2022

Anwendungsregeln ermöglichen es der Citrix SD-WAN-Appliance, eingehenden Datenverkehr zu analysieren und ihn als Teil einer bestimmten Anwendung oder Anwendungsgruppe zu klassifizieren. Diese Klassifizierung verbessert die Quality of Service (QoS) einzelner Anwendungen oder Anwendungsfamilien, indem Anwendungsregeln erstellt und angewendet werden.

Sie können Datenverkehrsflüsse basierend auf Übereinstimmungstypen von Anwendungen, Anwendungsgruppen oder Anwendungsobjekten filtern und Anwendungsregeln auf sie anwenden. Die Anwendungsregeln ähneln den IP-Regeln (Internet Protocol). Weitere Informationen zu IP-Regeln finden Sie unter IP-Regeln.

Für jede Anwendungsregel können Sie die Verkehrsrichtlinie angeben. Im Folgenden sind die verfüg-

baren Verkehrsrichtlinien aufgeführt:

- **Load Balance-Pfad**: Der Anwendungsverkehr für den Flow wird über mehrere Pfade verteilt. Der Datenverkehr wird über den besten Pfad gesendet, bis dieser Pfad verwendet wird. Die verbleibenden Pakete werden über den nächstbesten Pfad gesendet.
- **Persistenter Pfad**: Der Anwendungsverkehr bleibt auf demselben Pfad, bis der Pfad nicht mehr verfügbar ist.
- **Doppelter Pfad**: Anwendungsdatenverkehr wird über mehrere Pfade dupliziert, was die Zuverlässigkeit erhöht.
  Die Anwendungsregeln sind Klassen zugeordnet.

Wie werden Anwendungsregeln angewendet?

Wenn im SD-WAN-Netzwerk die eingehenden Pakete die SD-WAN-Appliance erreichen, werden die ersten paar Pakete keiner DPI-Klassifizierung unterzogen. An dieser Stelle werden die IP-Regelattribute wie Klasse, TCP-Terminierung auf die Pakete angewendet. Nach der DPI-Klassifizierung überschreiben die Anwendungsregelattribute wie Klasse und Verkehrsrichtlinie die IP-Regelattribute.

Die IP-Regeln haben im Vergleich zu den Anwendungsregeln eine größere Anzahl von Attributen. Die Anwendungsregel überschreibt nur einige IP-Regelattribute. Die restlichen IP-Regelattribute bleiben in den Paketen verarbeitet.

Angenommen, Sie haben eine Anwendungsregel für eine Webmail-Anwendung wie Google Mail angegeben, die das SMTP-Protokoll verwendet. Der IP-Regelsatz für das SMTP-Protokoll wird zunächst vor der DPI-Klassifizierung angewendet. Nachdem die Pakete analysiert und als zur Google Mail-Anwendung gehörend klassifiziert wurden, wird die für die Google Mail-Anwendung angegebene Anwendungsregel angewendet.

Anwendungsregeln erstellen

Um Anwendungsregeln zu erstellen, navigieren Sie zu **Konfiguration > QoS > QoS-Richtlinien** > **Anwendungsregeln**. Wählen Sie **die Registerkarte Globale Regeln**, um Anwendungsregeln auf globaler Ebene zu erstellen, oder **Standort-/Gruppenspezifische Regeln**, um Regeln auf Standortebene zu erstellen.

Klicken Sie im Abschnitt ****Anwendungsregeln auf Neue Anwendungsregel**** .

- Übereinstimmungskriterien für Apps und Domains
  - **Apps & Domains**: Wählen Sie eine Anwendung oder Domain aus der Dropdownliste aus. Sie können auch eine Domain-App erstellen, indem Sie auf **+ Neue Domain-App**klicken. Geben Sie einen Namen ein und fügen Sie Domains hinzu

- **Routingdomäne**: Wählen Sie eine Routingdomäne Sie können die Standard-Routingdomäne auswählen oder **Beliebig**auswählen.
- **Quellnetzwerk**: Quell-IP-Adresse und Subnetzmaske, die mit dem Datenverkehr abgeglichen werden sollen.
- **Zielnetzwerk**: Ziel-IP-Adresse und Subnetzmaske, die mit dem Datenverkehr abgeglichen werden sollen.
- **Quellport**: Quellportnummer oder Portbereich, um mit dem Verkehr übereinzustimmen.
- **Zielport**: Ziel-Portnummer oder Portbereich, um mit dem Verkehr übereinzustimmen.
- **Src = Dest**: Wenn ausgewählt, wird der Quellport auch für den Zielport verwendet.

• Verkehrsrichtlinie für virtuelle Pfade

Aktivieren Sie das Kontrollkästchen **Verkehrsrichtlinie für virtuelle Pfade** aktivieren.

- **Virtueller Pfad Remote-Site**: Wählen Sie den virtuellen Pfad für die Remote-Site aus.
- **Verkehrsrichtlinie**: Wählen Sie nach Bedarf eine der folgenden Verkehrsrichtlinien.
  - **Lastausgleichspfade**: Der Anwendungsdatenverkehr für den Flow wird über mehrere Pfade verteilt. Der Datenverkehr wird über den besten Pfad gesendet, bis dieser Pfad verwendet wird. Die verbleibenden Pakete werden über den nächstbesten Pfad gesendet.
  - **Persistenter Pfad**: Der Anwendungsverkehr bleibt auf demselben Pfad, bis der Pfad nicht mehr verfügbar ist. Wählen Sie eine der folgenden **Persistenzrichtlinien**aus:
    - **Behalten Sie den ursprünglichen Link an**: Der Anwendungsdatenverkehr verbleibt auf dem ursprünglichen Link, bis der Pfad nicht mehr verfügbar ist.
    - **Bleiben Sie auf dem MPLS-Link, falls verfügbar, andernfalls auf dem ursprünglichen Link**: Der Anwendungsdatenverkehr verbleibt auf dem MPLS-Link. Wenn der MPLS-Link nicht verfügbar ist, verbleibt der Datenverkehr auf dem ursprünglichen Link.
    - **Bleiben Sie auf dem Internetlink, falls verfügbar, andernfalls auf dem ursprünglichen Link**: Der Anwendungsverkehr verbleibt auf dem Internetlink. Wenn die Internetverbindung nicht verfügbar ist, verbleibt der Datenverkehr auf dem ursprünglichen Link.
    - **Bleiben Sie auf dem privaten Intranet-Link, falls verfügbar, andernfalls auf dem ursprünglichen Link**: Der Anwendungsdatenverkehr verbleibt auf dem privaten Intranet-Link. Wenn der private Intranetlink nicht verfügbar ist, verbleibt der Datenverkehr auf dem ursprünglichen Link.

    Persistenzimpedanz ist die Zeit (in ms), bis zu der der Anwendungsdatenverkehr auf der Verbindung verbleibt.
  - **Doppelte Pfade**: Anwendungsdatenverkehr wird über mehrere Pfade dupliziert, was die Zuverlässigkeit erhöht

- QoS-Einstellungen (QoS-Klasse)
  - **Transferart**: Wählen Sie eine der folgenden Übertragungsarten:
    - **Echtzeit**: Wird für zeitkritischen Datenverkehr mit geringer Latenz, geringer Bandbreite verwendet. Echtzeitanwendungen sind zeitkritisch, benötigen aber keine wirklich hohe Bandbreite (z. B. Voice over IP). Echtzeitanwendungen reagieren empfindlich auf Latenz und Jitter, können jedoch einige Verluste tolerieren.
    - **Interaktiv**: Wird für interaktive Datenverkehr mit niedrigen bis mittleren Latenzanforderungen und niedrigen bis mittleren Bandbreitenanforderungen verwendet. Die Interaktion erfolgt in der Regel zwischen einem Client und einem Server. Die Kommunikation benötigt möglicherweise keine hohe Bandbreite, ist aber empfindlich gegenüber Verlust und Latenz.
    - **Bulk**: Wird für Traffic mit hoher Bandbreite und Anwendungen verwendet, die hohe Latenz tolerieren können. Anwendungen, die die Dateiübertragung verarbeiten und eine hohe Bandbreite benötigen, werden als Bulkklasse eingestuft. Diese Anwendungen beinhalten wenig menschliche Eingriffe und werden meist von den Systemen selbst behandelt.
  - **Priorität**: Wählen Sie eine Priorität für den ausgewählten Übertragungstyp.

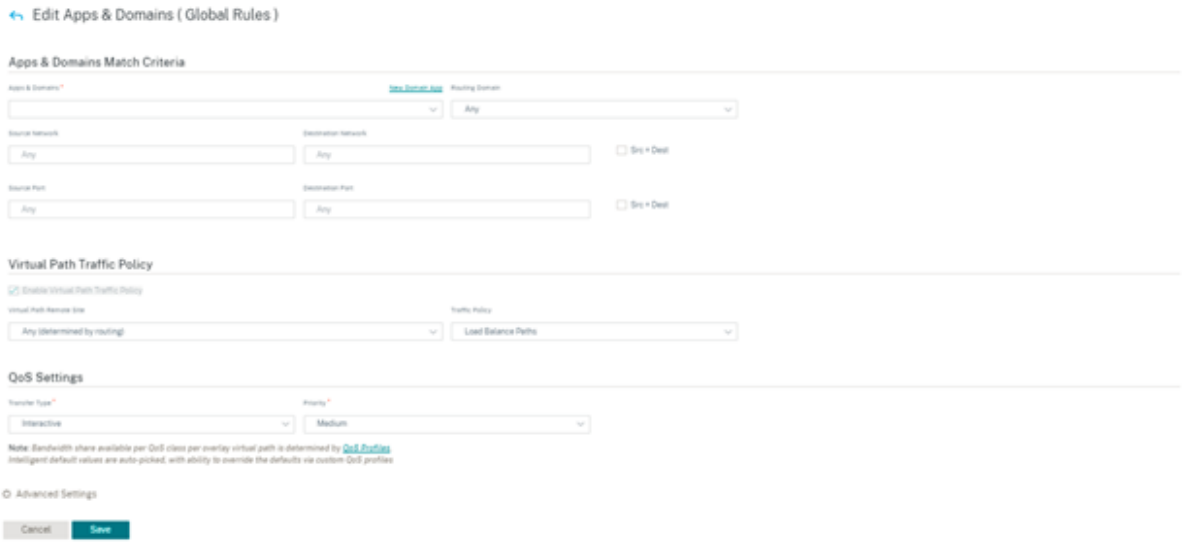
Erweiterte Einstellungen

- WAN Allgemeines
  - **Verlorene Pakete erneut übertragen**: Sendet Datenverkehr, der dieser Regel entspricht, über einen zuverlässigen Dienst an die Remote-Appliance und überträgt verlorene Pakete erneut.
  - **Paketaggregation aktivieren**: Aggregiert kleine Pakete zu größeren Paketen.
- LAN zu WAN
  - **Drop-Tiefe (Byte)**: Schwellenwert für die Warteschlangentiefe, nach dem Pakete verworfen
  - **Drop-Limit**: Zeit, nach der Pakete, die im Klassenplaner warten, verworfen werden. Gilt nicht für eine Massenklasse.
  - **RED aktivieren**: Random Early Detection (RED) gewährleistet eine faire gemeinsame Nutzung von Klassenressourcen, indem Pakete verworfen werden, wenn eine Überlastung auftritt.
  - **Duplicate Packet Disable Depth (Byte)**: Die Warteschlangentiefe des Klassenplaners, an der die doppelten Pakete nicht generiert werden.
  - **Deaktivierungslimit für doppelte Pakete**: Zeit, für die die Duplizierung deaktiviert werden kann, um zu verhindern, dass doppelte Pakete Bandbreite verbrauchen
- WAN zu LAN

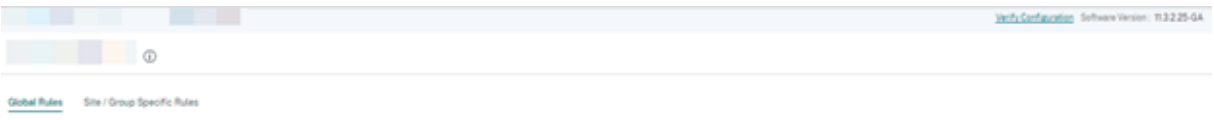
- **DSCP-Tag**: DSCP-Tag, das auf die Pakete angewendet wird, die dieser Regel auf WAN to LAN entsprechen, bevor sie an das LAN gesendet werden.
- **Paketresequenzierung aktivieren**: Die Datenverkehrsflüsse, die der Regel entsprechen, werden für die Sequenzreihenfolge markiert, und die Pakete werden (falls erforderlich) auf der WAN-zu-LAN-Appliance neu angeordnet.
- **Haltezeit**: Zeitintervall, für das die Pakete zur erneuten Sequenzierung gehalten werden, nach dem die Pakete an das LAN gesendet werden. Wenn der Timer abläuft, werden die Pakete an das LAN gesendet, ohne weiter auf die erforderlichen Sequenznummern zu warten.

  Wenn die Regel eine Verkehrsrichtlinie als doppelter Pfad hat, beträgt die Standardhaltezeit 80 ms. Andernfalls ist der Standardwert 900 ms für TCP-Regeln und 250 ms für Nicht-TCP-Regeln.
- **Pakete mit verspäteter Resequenzierung**verwerfen: Verwirft Pakete außerhalb der Reihenfolge, die eingetroffen sind, nachdem die für die Resequenzierung benötigten Pakete an das LAN gesendet wurden.

Klicken Sie auf **Speichern**, um die Konfigurationseinstellungen zu speichern.



Klicken Sie auf der Seite Konfiguration**>**QoS > **QoS-Richtlinien**** auf Konfiguration überprüfen, um alle Überwachungsfehler zu validieren und alle Überwachungsfehler zu validieren.**

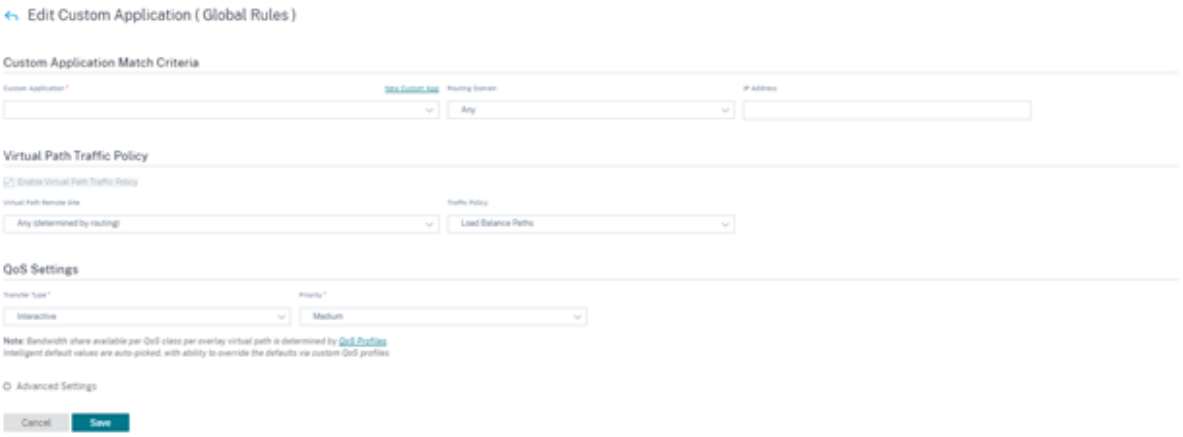


Erstellen Sie benutzerdefinierte Anwendungsregeln

Sie können auch benutzerdefinierte Anwendungsregeln erstellen. Um eine benutzerdefinierte Anwendungsregel zu erstellen, navigieren Sie zu **Konfiguration > QoS > QoS-Richtlinien** > **Benutzerdefinierte Anwendungsregeln**. Wählen Sie **die Registerkarte Globale Regeln**, um benutzerdefinierte Anwendungsregeln auf globaler Ebene zu erstellen, oder **Standort-/Gruppenspezifische Regeln**, um Regeln auf Standortebene zu erstellen.

Klicken Sie im Abschnitt **Regeln für**benutzerdefinierte Anwendungen auf Neue benutzerdefinierte Anwendungsregel**** . Klicken Sie neben dem Feldnamen **Benutzerdefinierte Anwendung auf Neue benutzerdefinierteApp** . Geben Sie einen Namen für die benutzerdefinierte Anwendung ein. Wählen Sie im Abschnitt **Übereinstimmungskriterien** die Anwendung, das Protokoll und das DSCP-Tag aus und geben Sie die Netzwerk-IP und die Portnummer ein. Klicken Sie auf **Speichern**.

Geben Sie bei Bedarf Details in die anderen Felder ein. Informationen zu Feldbeschreibungen finden Sie unter Erstellen von Anwendungsregeln.

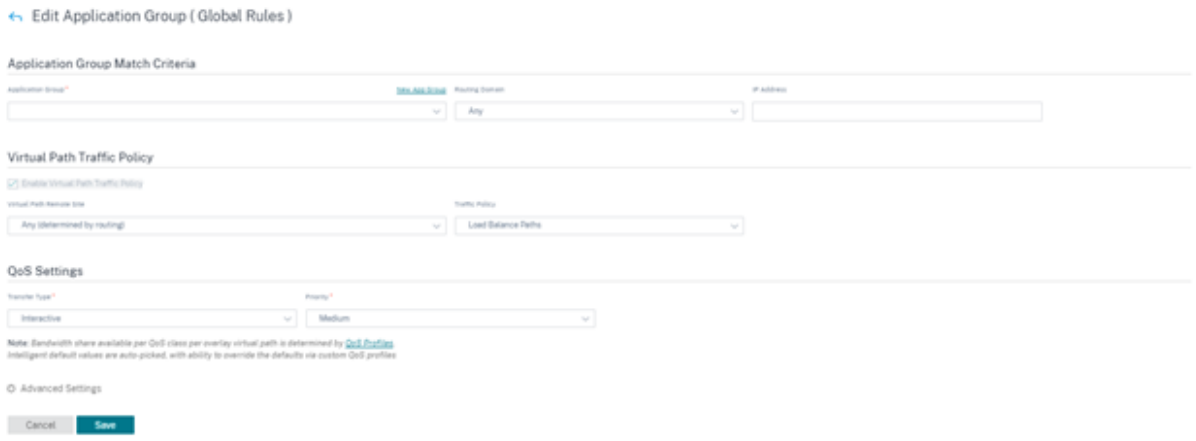


Regeln für Anwendungsgruppen erstellen

Sie können Regeln für eine Gruppe von Anwendungen erstellen. Um Anwendungsgruppenregeln zu erstellen, navigieren Sie zu **Konfiguration > QoS > QoS-Richtlinien** > **Anwendungsgruppenregeln**. Wählen Sie **die Registerkarte Globale Regeln**, um Anwendungsgruppenregeln auf globaler Ebene zu erstellen, oder **Standort-/Gruppenspezifische Regeln**, um Regeln auf Standortebene zu erstellen.

Klicken Sie im Abschnitt ****Anwendungsgruppenregeln auf Neue Anwendungsgruppenregel**** . Klicken Sie neben dem Feldnamen der **Anwendungsgruppe** auf **Neue App-Gruppe** . Geben Sie einen Namen für die Anwendungsgruppe ein. Suchen und fügen Sie Anwendungen nach Bedarf hinzu. Klicken Sie auf **Speichern**.

Geben Sie bei Bedarf Details in die anderen Felder ein. Informationen zu Feldbeschreibungen finden Sie unter Erstellen von Anwendungsregeln.



Überprüfen Sie die Anwendungsregeln

Um die Anwendungsregeln zu überprüfen, navigieren Sie zu **Berichte > Echtzeit > Flows**. Wählen Sie die Site aus, für die Sie die Flow-Informationen anzeigen möchten, und die Anzahl der anzuzeigenden Flows. Klicken Sie auf **Spalten anpassen**, und aktivieren Sie die Kontrollkästchen für die Flow-Informationen, die Sie anzeigen möchten. Überprüfen Sie, ob die Flussinformationen den konfigurierten Regeln entsprechen.

Navigieren Sie zu **Berichte > Echtzeit > Statistiken**, und wählen Sie **Regeln**aus. Wählen Sie die Site aus und klicken Sie auf **Neueste Daten abrufen**. Überprüfen Sie die konfigurierten Regeln.

Weitere Informationen zum Reporting finden Sie unter Flows.

HDX QoE

October 21, 2022

Netzwerkparameter wie Latenz, Jitter und Paketabfall wirken sich auf die Benutzererfahrung von HDX-Benutzern aus. Quality of Experience (QoE) hilft den Benutzern, ihre ICA-Erlebnisqualität zu verstehen und zu überprüfen. QoE ist ein berechneter Index, der die ICA-Verkehrsleistung angibt. Die Benutzer können die Regeln und Richtlinien zur Verbesserung der QoE einstellen.

Die QoE ist ein numerischer Wert zwischen 0—100, je höher der Wert desto besser die Benutzererfahrung.

Die zur Berechnung der QoE verwendeten Parameter werden zwischen den beiden Citrix SD-WAN-Appliances auf Client- und Serverseite gemessen und nicht zwischen dem Client oder den Servergeräten selbst gemessen. Latenz, Jitter und Paketabfall werden auf der Flussstufe gemessen

und kann sich von den Statistiken auf der Linkebene unterscheiden. Die Endhostanwendung (Client oder Server) weiß möglicherweise nie, dass ein Paketverlust im WAN vorliegt. Wenn die erneute Übertragung erfolgreich ist, ist die Paketverlustrate des Flusspegels niedriger als der Verlust der Verbindungsebene. Infolgedessen kann es die Latenz und den Jitter etwas erhöhen.

Sie können eine grafische Darstellung der Gesamtqualität von HDX-Anwendungen im HDX-Dashboard auf Citrix SD-WAN Orchestrator for On-premises anzeigen. Die HDX-Anwendungen werden in die folgenden drei Qualitätskategorien eingeteilt:

Qualität	QoE-Bereich
Gut	71-100
Fair	51-70
Schlecht	0-50

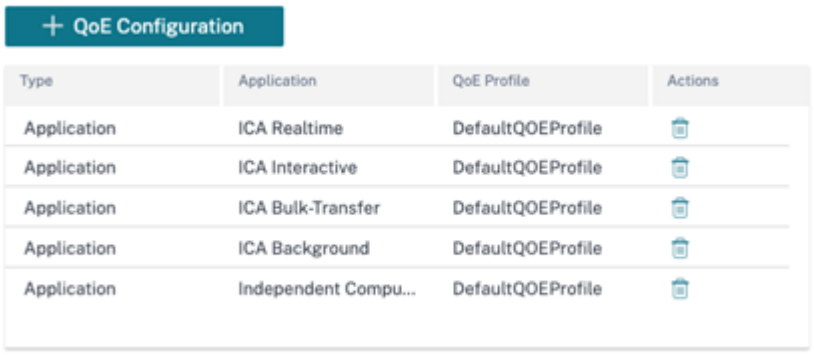
Abhängig von der ausgewählten UI-Seite wird im HDX-Dashboard eine Liste der untersten (mindestens QoE) fünf Sites, fünf Benutzer, fünf Sitzungen oder alle von ihnen angezeigt.

Eine grafische Darstellung des QoE für unterschiedliche Zeitintervalle ermöglicht es Ihnen, die Leistung von HDX-Anwendungen an jedem Standort zu überwachen.

HDX QoE konfigurieren

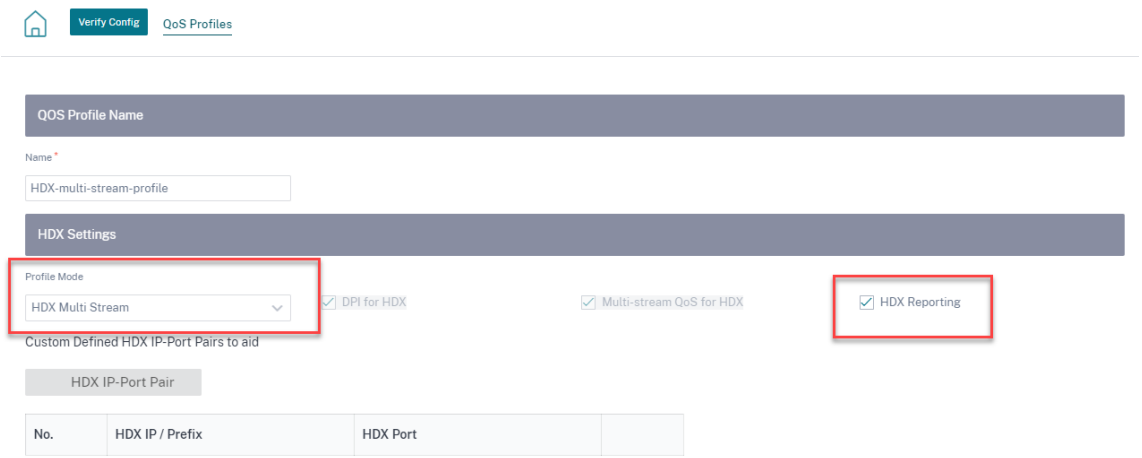
1. Navigieren Sie auf Netzwerkebene zu **Konfiguration > App-Einstellungen & Gruppen > App Quality Config** und klicken Sie auf **+ QoE-Konfiguration**. Fügen Sie die folgenden Anwendungen mithilfe des QoE-Profils hinzu, das Sie für die Berechnung des HDX-Verhaltens verwenden möchten:

    - ICA Echtzeit (ica_priority_0)
    - ICA Interaktiv (ica_priority_1)
    - ICA-Massenübertragung (ica_priority_2)
    - ICA-Hintergrund (ica_priority_3)
    - Unabhängige Datenverarbeitungsarchitektur (Citrix) (ICA)

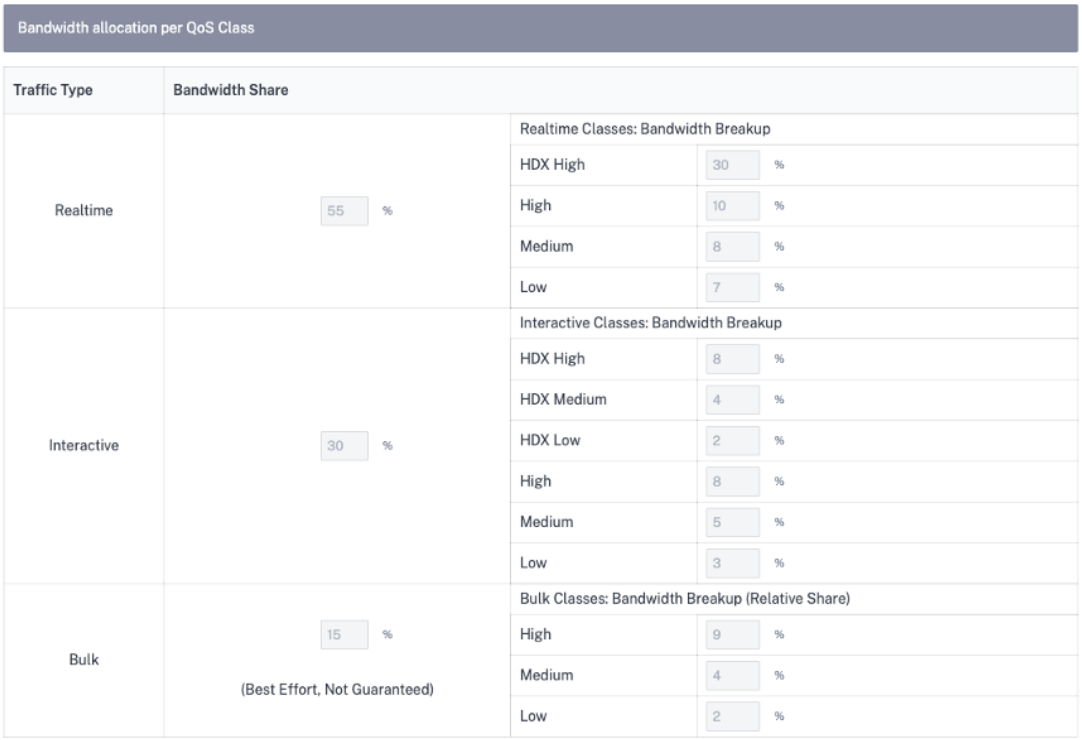


Diese Konfigurationen stellen die Parameter bereit, um die im HDX-Bericht verwendete HDX-Leistung über das Profil zu messen. Konfiguration von ICA-Echtzeit, ICA Interactive, ICA-Bulk-Transfer und ICA-Hintergrund sind für HDX Multistream (MSI) -Verbindungen erforderlich, Independent Computing Architecture (Citrix) ist für Single Stream (SSI) -Verbindungen erforderlich.

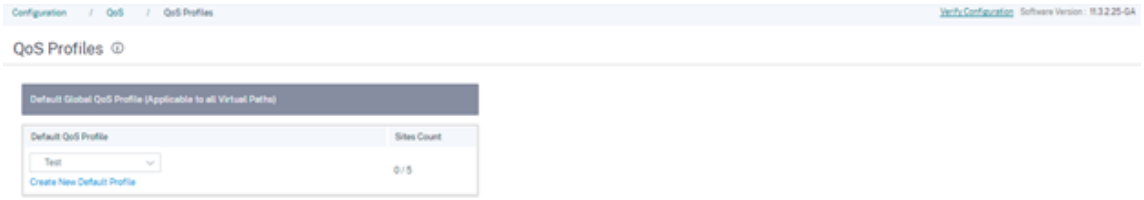
2. Navigieren Sie zu **Konfiguration > QoS > QoS-Profile**. Wählen Sie **Standard-HDX-Multistream** als Standard-QoS-Profil und aktivieren Sie das Kontrollkästchen **HDX Reporting** . Löschen Sie **HDX Reporting**, wenn kein HDX-Reporting erforderlich ist.



In jedem QoS-Profil gibt es einen vordefinierten Bandbreitenprozentsatz für jede Klasse. Sie sind konfigurierbar, um die Bandbreite anzupassen, die den Klassen zugewiesen ist, die der HDX-Datenverkehr verwendet.

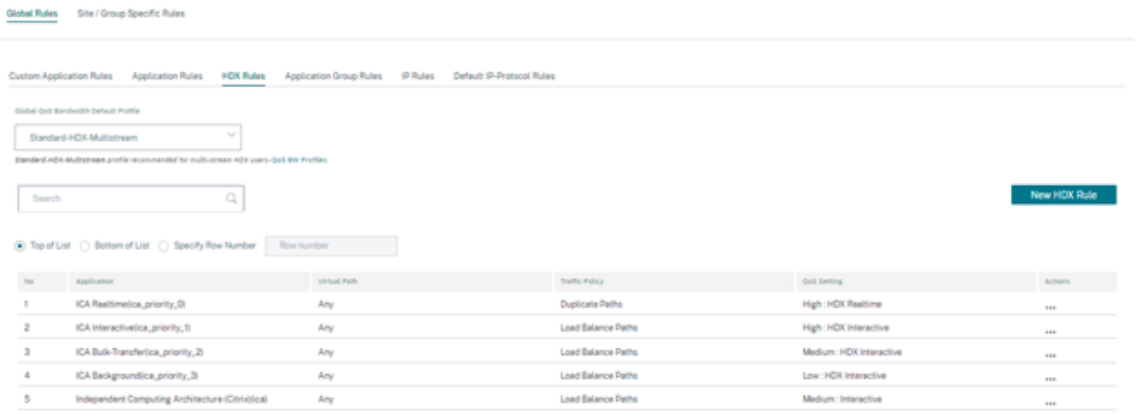


3. Stellen Sie sicher, dass das neue QoS-Profil aktiv verwendet wird, indem Sie den Indikator **Site-Anzahl** aktivieren.



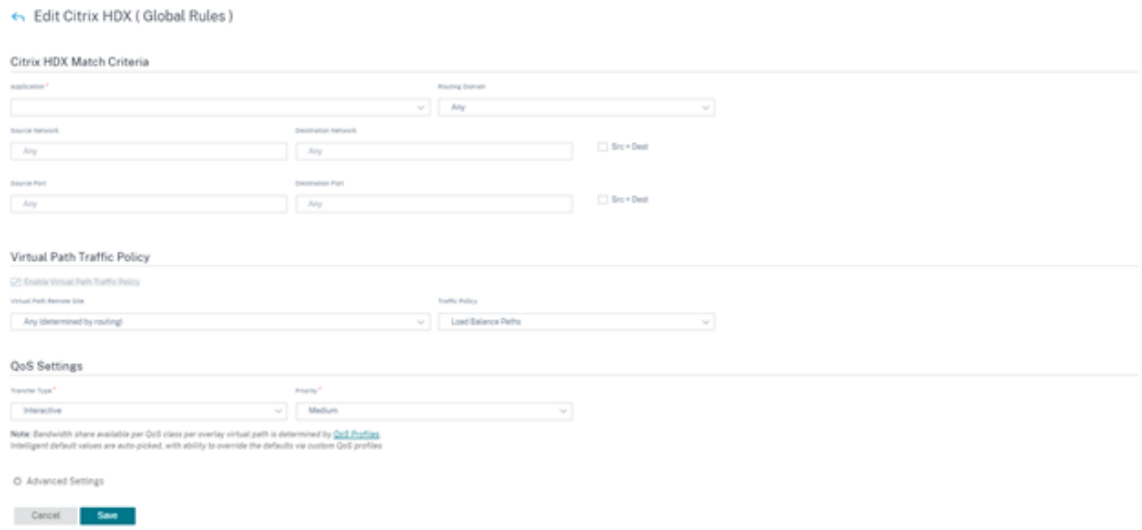
4. Navigieren Sie zu **Konfiguration > QoS > QoS-Richtlinien** > **HDX-Regeln**, und legen Sie das neue QoS-Profil mit der aktivierten HDX-Berichterstattung als **Standardprofil für globale QoS-Bandbreite**fest.

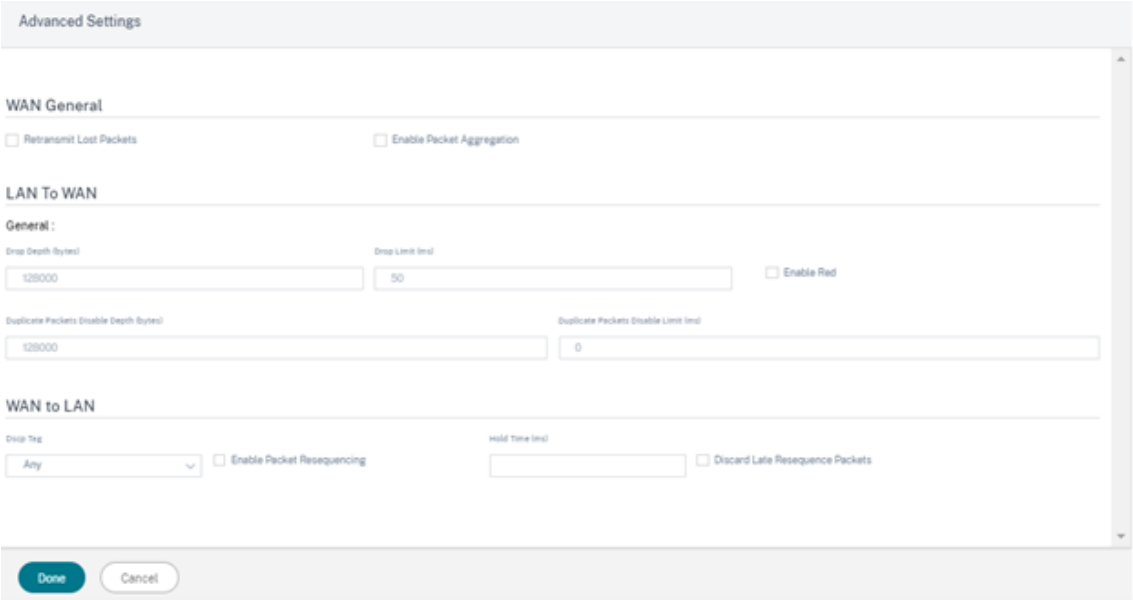
5. Fügen Sie HDX-Regeln hinzu. Diese Konfigurationen weisen HDX-Verbindungen die richtigen QoS-Einstellungen zu. Um die Regeldetails zu überprüfen oder die Regeln zu bearbeiten, navigieren Sie zum unteren Bereich der Seite **HDX-Regeln** . Wechseln Sie in der Tabelle Regeln zur Spalte **Aktionen** und wählen Sie **Bearbeiten**aus. Um die Einstellung einer Standardregel zu ändern, klicken Sie auf **Klonen** und nehmen Sie die erforderlichen Änderungen vor.



Diese Konfigurationen können geändert werden:

- QoS-Klasse: Echtzeit, interaktiv, Bulk
- Richtlinien für den Verkehr:
  - **Doppelte Pfade**: Der Datenverkehr wird über mehrere Pfade dupliziert, um die Zuverlässigkeit zu erhöhen.
  - **Persistenter Pfad**: Der Datenverkehr eines Flows bleibt auf demselben Pfad, sofern der Pfad nicht mehr verfügbar ist.
  - **Load Balancing-Pfade**: Der Datenverkehr eines Flows wird über mehrere Pfade verteilt.
  - **Erweiterte Einstellungen**: Legen Sie Richtlinien für erneute Übertragung, RED und späte Pakete fest.





HDX Dashboard und Berichte

Citrix SD-WAN Orchestrator for On-premises bietet das HDX-Dashboard für aktuelle, detaillierte Messungen der Benutzererfahrung von Citrix Virtual Applications and Desktops im gesamten Netzwerk für jeden Standort, Benutzer und jede Sitzung.

Es gibt zwei Arten von HDX-Sitzungen —Single-Stream und Multistream. Eine Single-Stream-Sitzung hat nur eine Verbindung in der Sitzung, während eine Multi-Stream-Sitzung vier hat. Multi-Stream-Sitzungen ermöglichen fortgeschrittenere QoS. Die Verbindung in einer Single-Stream-HDX-Sitzung ist standardmäßig die interaktive Klasse, während die Verbindung einer Multi-Stream-HDX-Sitzung standardmäßig auf eine Echtzeitklasse und die anderen drei auf die interaktive Klasse vorgegeben wird. Dies ist konfigurierbar.

Der Quality of Experience (QoE) -Wert ist ein numerischer Wert zwischen 0 und 100. Je höher der Wert desto besser ist die Benutzererfahrung. Echtzeit-Klassenverkehr QoE wird basierend auf Jitter, Latenz und Verlustrate berechnet. Die interaktive Klasse QoE wird basierend auf Burstrate und Verlustrate berechnet. Die QoE einer Sitzung ist der Durchschnitt aller Verbindungen in der Sitzung. Die QoE eines Benutzers ist der Durchschnitt aller von diesem Benutzer gestarteten Sitzungen. Die QoE einer Site ist der Durchschnitt aller Sitzungen auf dieser Site.

Alle Statistiken sind Metriken:

- Für HDX-Verkehr auf dieser Site
- Von diesem Benutzer erfahren
- Von allen Verbindungen in dieser Sitzung

Sie enthalten nicht die Metriken anderer Arten von Verkehr. Die Metriken sind entweder der Durchschnitt des ausgewählten Zeitraums oder die Gesamtsumme des ausgewählten Zeitraums.

> **Hinweis:**
>
> Für HDX-Berichte sind mindestens Softwareversionen erforderlich:
>
> - Citrix Virtual Apps and Desktops 7—1912 LTSR (oder aktuelle Version)
> - Citrix Workspace Workspace-App für Windows 19.12 LTSR (oder aktuelle Version)
> - SD-WAN 11.2.0 (oder aktuelle Version)

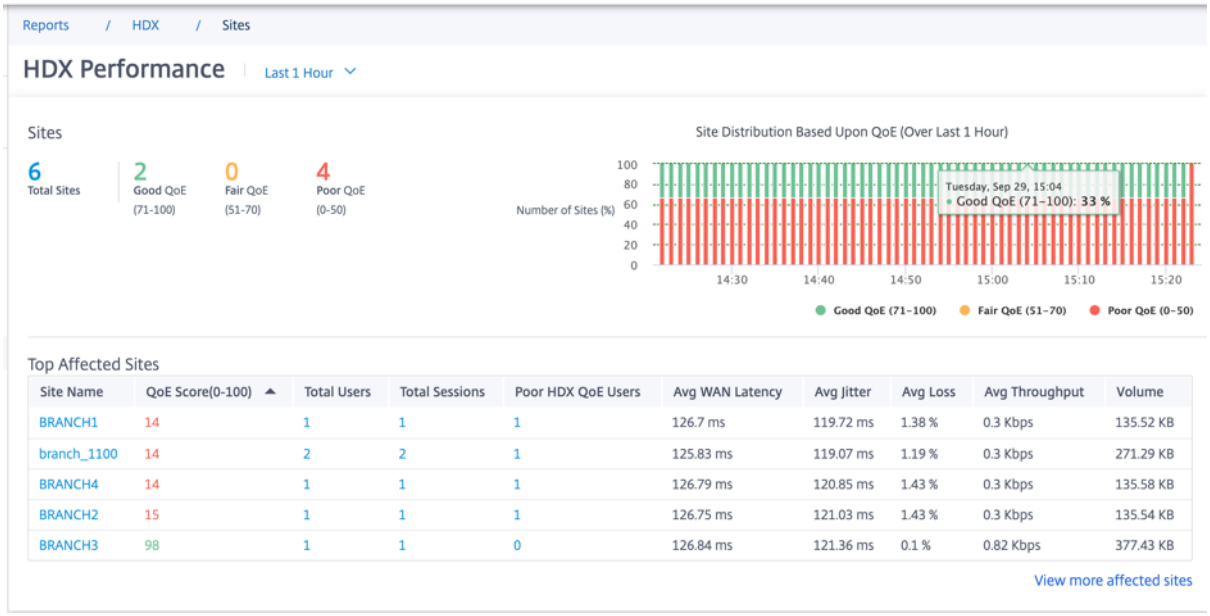
Citrix empfiehlt immer, die neueste Softwareversion zu verwenden, um die neuesten Fehlerbehebungen und Verbesserungen zu erhalten. SD-WAN erfordert beispielsweise die Version 11.2.3 oder 11.3.1, um Unterstützung für neue EDT-Befehle zu haben, die in späteren Versionen von Citrix Virtual Apps and Desktops LTSR eingeführt wurden.

Mac-Clients und Linux-Clients bieten keine vollständige Unterstützung für Multistream-ICA- und HDX-Berichte über Citrix SD-WAN. Zum Beispiel unterstützen Linux-Clients Multistream, es fehlen jedoch Details wie Roundtrip-Zeit und Verzögerung. Die CWA-Featurematrix gibt Aufschluss darüber, welche Betriebssysteme die **Multiport-ICA** - und **HDX Insight mit NSAP VC-Funktionen** unterstützen.

Benutzer müssen außerhalb der Citrix Gateway Gateway-Verschlüsselung auf HDX zugreifen, entweder über direkten Zugriff auf StoreFront oder über Beacon Points oder den Network Location Service.

Sites

Dieser HDX-Bericht liefert detaillierte HDX-Daten pro Standort. Um die Sitestatistiken anzuzeigen, navigieren Sie zu **Berichte** > **HDX** > **Sites**.



Das Dashboard berichtet vor Ort mit HDX-Verkehr, der während des ausgewählten Zeitintervalls ausgeführt wird (z. B. letzte 5 Minuten, letzte 30 Minuten, letzte 1 Tag, letzte Monat usw.). Die Standortleistung wird basierend auf der QoE des HDX-Verkehrs der Site als gut (71-100), fair (51-70) oder schlecht (0-50) eingestuft. Der QoE-Wert im Zusammenfassungsbereich und in der Tabelle „Am **häufigsten betroffene Standorte** "ist der Durchschnittswert für den ausgewählten Zeitraum. Der Grafikbericht der Zeitreihen zeigt eine detaillierte Historie mit Zeitraffer. Jeder Balken zeigt den Prozentsatz der guten, fairen und schlechten QoE-Standorte zu dieser Zeit an.

Sie können auch die prozentuale Anzahl der Standorte mit guter, fairer und schlechter QoE unter dem Diagramm **Standortverteilung basierend auf QoE** anzeigen. Bewegen Sie die Maus auf die Farbleiste, um die prozentuale Anzahl von Sites in einem guten/mittleren/schlechten Zustand zu sehen.

HINWEIS:

- Die Statistiken werden in eine Richtung von der Gegenseite auf die aktuelle Site erhoben. Zum Beispiel wird für eine Sitzung zwischen Site-A und Standort-B der Bericht von Site-A über den Datenverkehr gesammelt, der von Site-B zu Standort-A kommt, während der Bericht von Site-B über den Datenverkehr von Standort-A in Site-B gesammelt wird. Daher können die Statistiken derselben Sitzung auf Standort-A und Site-B unterschiedlich sein.
- In der Tabelle „Am **häufigsten betroffene Standorte** "werden nur die 5 am stärksten betroffenen Standorte angezeigt. Standardmäßig werden die 5 Sites mit den niedrigsten QoE-Ergebnissen angezeigt. Jede Spalte ist jedoch sortierbar, aufsteigend oder absteigend und wird als Abfragekriterium verwendet. Wenn Sie beispielsweise auf den Spaltentitel **Avg Jitter** klicken, werden entweder die 5 Websites mit dem niedrigsten durchschnittlichen Jitter oder dem höchsten durchschnittlichen Jitter angezeigt. Das Gleiche gilt für andere Spal-

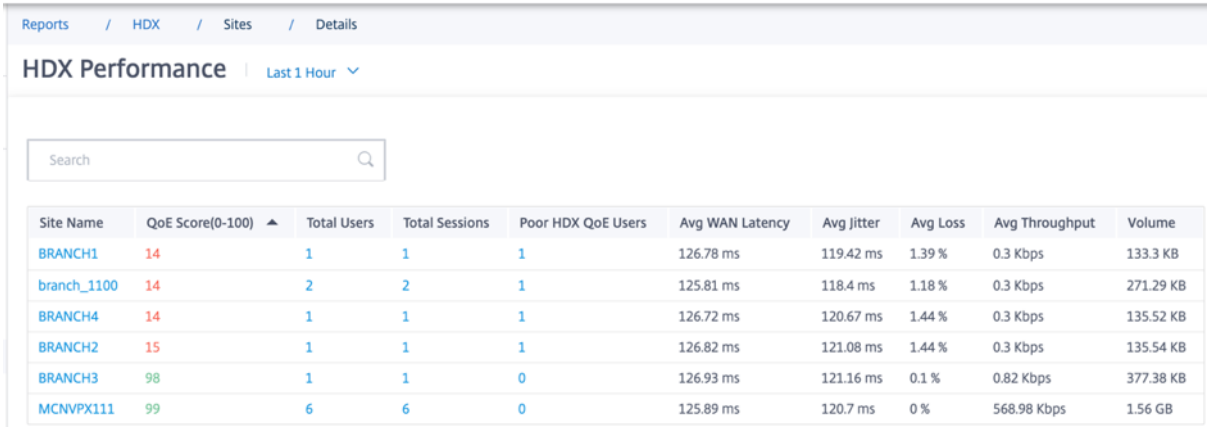
> ten. Um die Details aller Sites mit HDX-Datenverkehr während des ausgewählten Zeitraums **anzuzeigen, klicken Sie auf Weitere betroffene Sites**anzeigen.

Im Folgenden sind die Details jeder Site aufgeführt:

- **Site-Name**: Der Site-Name.
- **QoE Score (0-100)**: Der durchschnittliche QoE-Wert dieser Website.
- **Benutzer insgesamt**: Die Gesamtzahl der aktiven HDX-Benutzer, die während des ausgewählten Zeitraums auf der Website gesehen wurden.
- **Sitzungen insgesamt**: Die Gesamtzahl der HDX-Sitzungen, die während des ausgewählten Zeitraums auf der Site angezeigt wurden, einschließlich Einzelstream- und Multistream-Sitzungen.
- **Schlechte HDX QoE-Benutzer**: Die Anzahl der HDX-Benutzer, die unter schlechter QoE leiden (unter 50).
- **Durchschn. WAN-Latenz**: Durchschnittliche Latenz über das WAN vom Remote-Standort bis zu diesem Standort.
- **Durchschn. Jitter**: Der durchschnittliche Jitterwert für die gewählte Dauer.
- **Durchschn. Verlust**: Der durchschnittliche prozentuale Paketverlust für die ausgewählte Dauer.
- **Durchschn. Durchsatz**: Der durchschnittliche Datendurchsatzwert für die ausgewählte Dauer.
- **Volumen**: Das gesamte Verkehrsaufkommen auf dieser Website. Die Citrix SD-WAN Orchestrator for On-premises GUI passt die Einheit möglicherweise basierend auf dem Zahlenwert an und ändert sie.

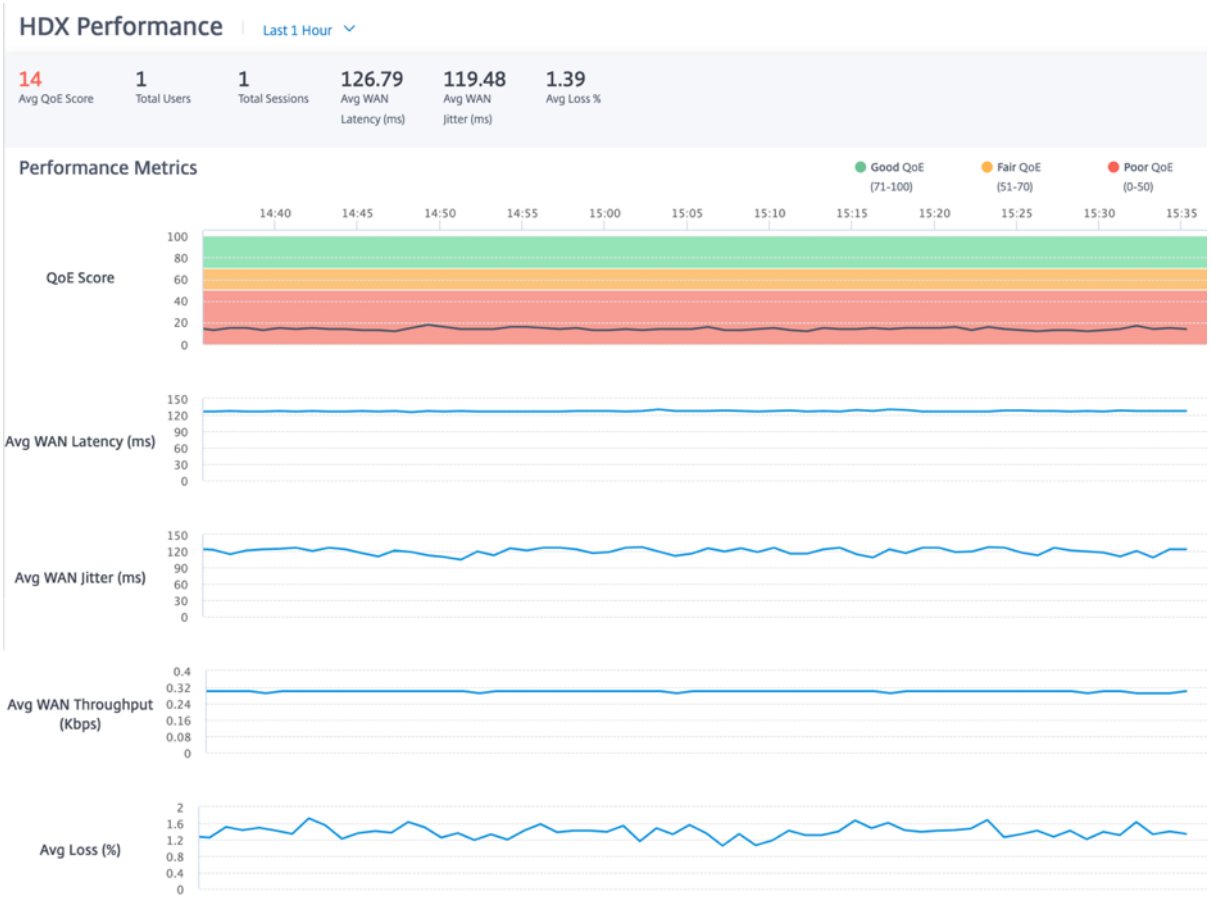
Wenn Sie auf einen Spaltentitel klicken, wird der Bericht nach dieser Spalte sortiert angezeigt. Klicken Sie auf **Weitere betroffene Websites anzeigen**, um die Berichte aller Websites anzuzeigen. Wenn Sie auf eine einzelne Zeile klicken, wird der detaillierte Bericht für diese Site angezeigt.

Die Tabelle im folgenden Screenshot ist ein Beispiel für die Berichtstabelle, in der alle Websites angezeigt werden. Sie hat dieselben Spalten wie die Tabelle **Top Affected Sites** .



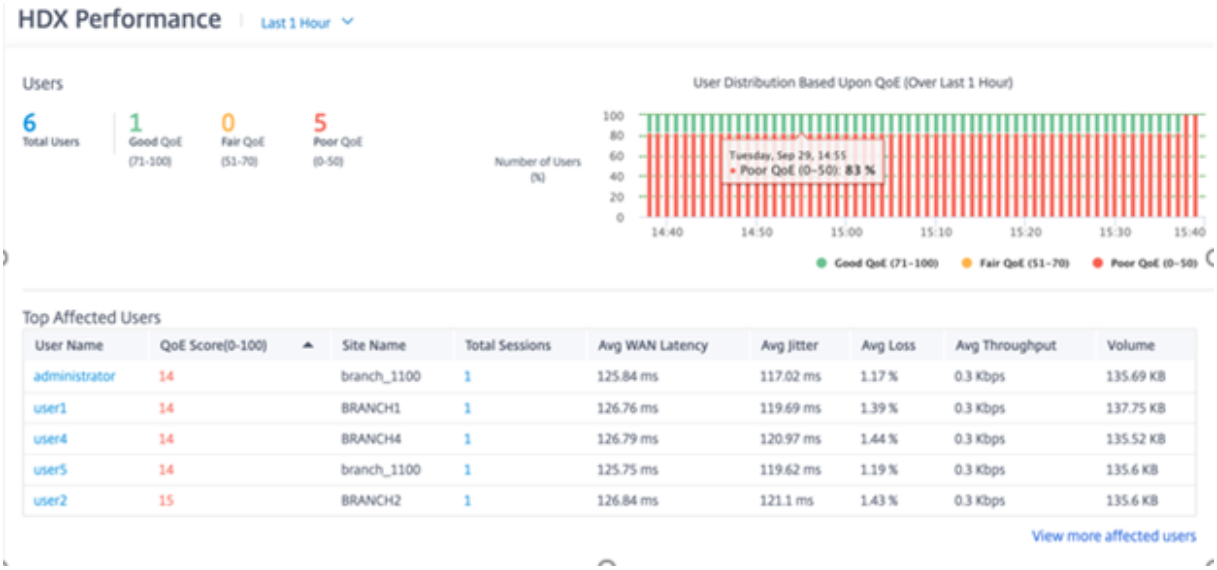
Site Name	QoE Score(0-100)	Total Users	Total Sessions	Poor HDX QoE Users	Avg WAN Latency	Avg Jitter	Avg Loss	Avg Throughput	Volume
BRANCH1	14	1	1	1	126.78 ms	119.42 ms	1.39 %	0.3 Kbps	133.3 KB
branch_1100	14	2	2	1	125.81 ms	118.4 ms	1.18 %	0.3 Kbps	271.29 KB
BRANCH4	14	1	1	1	126.72 ms	120.67 ms	1.44 %	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

Klicken Sie auf die Zeile der einzelnen Site, um eine grafische Darstellung der Performance-Metriken anzuzeigen. Wenn Sie mit der Maus über die Grafik fahren, erhalten Sie weitere Details.



Benutzer

Um den HDX-Benutzerbericht anzuzeigen, navigieren Sie zu **Berichte > HDX > Benutzer**.



Der Benutzerbericht zeigt die Leistung der einzelnen Benutzer während des ausgewählten Zeitraums an (z. B. letzte 5 Minuten, letzte 30 Minuten, letzter Tag, letzter 1 Monat usw.). Wenn der Benutzer während des ausgewählten Zeitraums auf mehreren Sites war, wird die letzte Site, von der sich der Benutzer angemeldet hat, im Bericht angezeigt. Die Benutzererfahrung wird basierend auf dem QoE-Wert ihres HDX-Datenverkehrs als gut (71-100), fair (51-70) oder schlecht (0-50) eingestuft. Die QoE-Werte im Zusammenfassungsbereich und in der Tabelle „ **Am häufigsten betroffene Benutzer** “sind die Durchschnittswerte für den ausgewählten Zeitraum. Der Grafikbericht der Zeitreihen zeigt eine detaillierte Historie mit Zeitraffer. Jeder Balken zeigt den Prozentsatz der Nutzer mit guter, fairer und schlechter QoE zu dieser Zeit an.

Sie können auch die prozentuale Anzahl der Benutzer mit guter, fairer und schlechter QoE unter dem Diagramm **Benutzerverteilung basierend auf QoE** anzeigen. Bewegen Sie die Maus auf die Farbleiste, um die prozentuale Anzahl der Benutzer im guten/heftenden/schlechteren Zustand zu sehen.

Personenbezogene Daten Derzeit enthalten die HDX-QoE-Berichte die folgenden zwei Felder für persönlich identifizierbare Informationen (PII):

- **Benutzername**: Zeigt den Benutzernamen an.
- **IP-Adresse**: Zeigt die Client-IP-Adresse an.

> **HINWEIS:**
>
> - Wenn der Benutzername nicht verfügbar ist, wird die IP-Adresse im Feld **Benutzername** angezeigt.
> - Die HDX-Benutzerberichte basieren auf Statistiken des clientseitigen SD-WAN, nicht dem VDA-seitigen SD-WAN (Virtual Delivery Agent). Dies spiegelt die HDX-Erfahrung des Endbe-

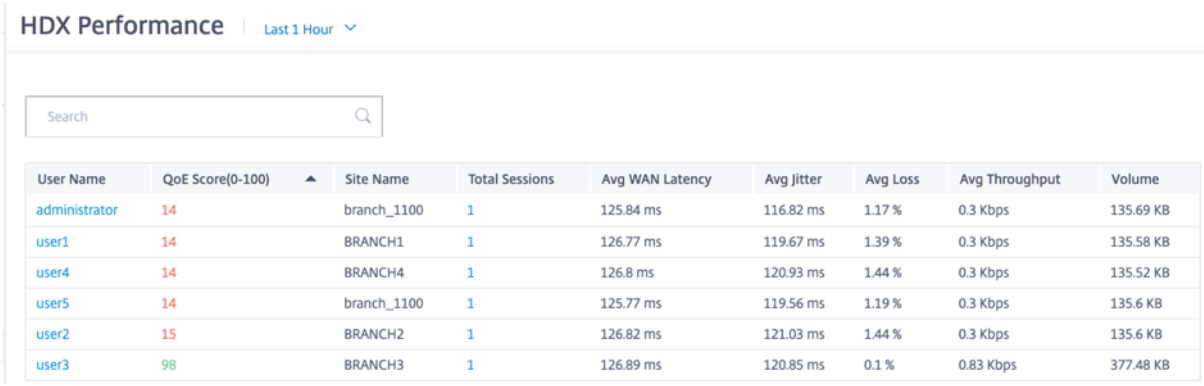
> nutzers wider.
>
> - In der Tabelle „Am **häufigsten betroffene Benutzer** "werden nur die fünf am stärksten betroffenen Benutzer angezeigt. Standardmäßig werden die Top-5-Benutzer mit der niedrigsten QoE angezeigt. Jede Spalte ist jedoch sortierbar, aufsteigend oder absteigend und wird als Abfragekriterium verwendet. Wenn Sie beispielsweise auf den Spaltentitel **Avg Jitter** klicken, werden entweder die 5 Benutzer mit dem niedrigsten durchschnittlichen Jitter oder dem höchsten durchschnittlichen Jitter angezeigt. Um die Details aller Benutzer anzuzeigen, die während des ausgewählten Zeitraums HDX-Datenverkehr hatten, klicken Sie auf **Weitere betroffene Benutzer anzeigen**.

Im Folgenden sind die Details jedes Benutzers aufgeführt:

- **Benutzername**: Der Benutzername.
- **QoE Score (0-100)**: Der durchschnittliche QoE-Wert dieses Benutzers.
- **Site-Name**: Der Site-Name, von dem aus sich der Benutzer angemeldet hat.
- **Sitzungen insgesamt**: Die Gesamtzahl der aktiven HDX-Sitzungen dieses Benutzers, einschließlich Einzelstream- und Multistream-Sitzungen.
- **Durchschnittliche WAN-Latenz**: Durchschnittliche Latenz über das WAN, die auf der Clientseite auftritt.
- **Durchschn. Jitter**: Der durchschnittliche Jitterwert für die gewählte Dauer.
- **Durchschn. Verlust**: Der durchschnittliche prozentuale Paketverlust für die ausgewählte Dauer.
- **Durchschn. Durchsatz**: Der durchschnittliche Datendurchsatzwert für die ausgewählte Dauer.
- **Volumen**: Das gesamte Verkehrsaufkommen, das von diesem Benutzer verwendet wird. Die Citrix SD-WAN Orchestrator for On-premises GUI passt die Einheit möglicherweise basierend auf dem Zahlenwert an und ändert sie.

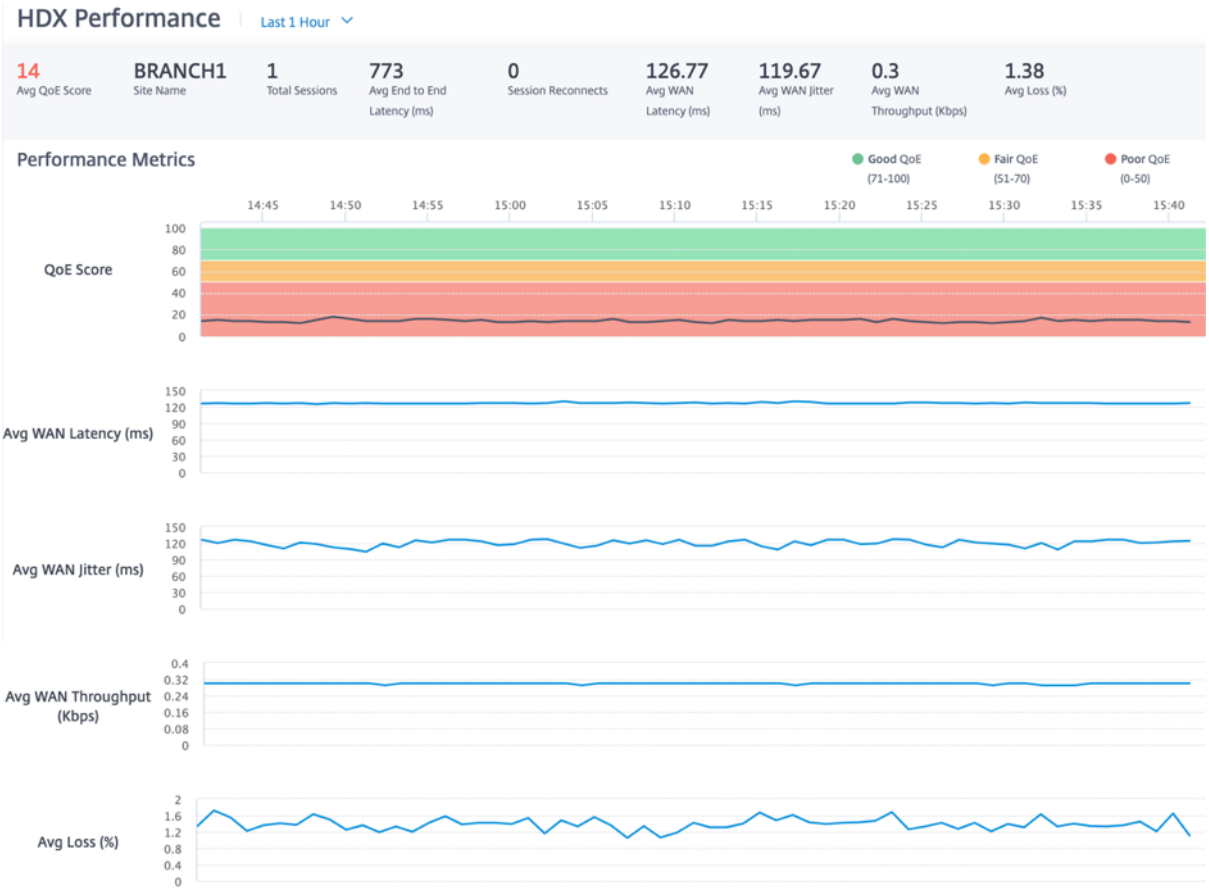
Wenn Sie auf einen Spaltentitel klicken, wird der Bericht nach dieser Spalte sortiert angezeigt. Klicken Sie auf **Weitere betroffene Benutzer anzeigen**, um die Berichte aller Benutzer anzuzeigen. Wenn Sie auf eine einzelne Zeile klicken, wird der detaillierte Bericht für diesen Benutzer angezeigt.

Der folgende Screenshot ist ein Beispiel für den Bericht, in dem alle Benutzer angezeigt werden. Sie hat dieselben Spalten wie die Tabelle „ **Am häufigsten betroffene Benutzer**".



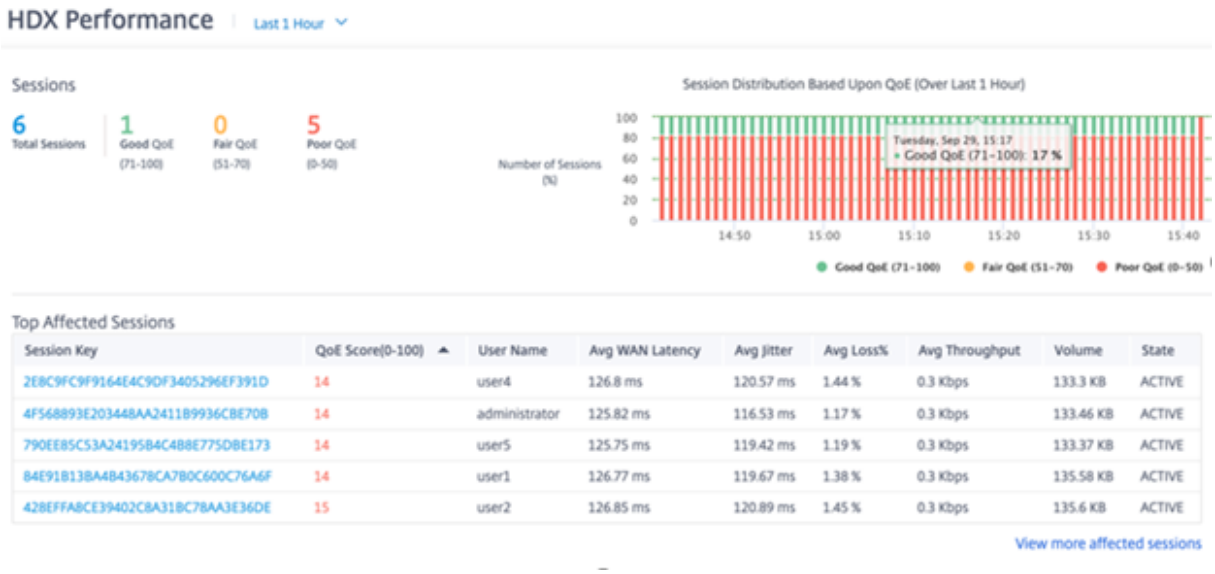
User Name	QoE Score(0-100)	Site Name	Total Sessions	Avg WAN Latency	Avg Jitter	Avg Loss	Avg Throughput	Volume
administrator	14	branch_1100	1	125.84 ms	116.82 ms	1.17 %	0.3 Kbps	135.69 KB
user1	14	BRANCH1	1	126.77 ms	119.67 ms	1.39 %	0.3 Kbps	135.58 KB
user4	14	BRANCH4	1	126.8 ms	120.93 ms	1.44 %	0.3 Kbps	135.52 KB
user5	14	branch_1100	1	125.77 ms	119.56 ms	1.19 %	0.3 Kbps	135.6 KB
user2	15	BRANCH2	1	126.82 ms	121.03 ms	1.44 %	0.3 Kbps	135.6 KB
user3	98	BRANCH3	1	126.89 ms	120.85 ms	0.1 %	0.83 Kbps	377.48 KB

Klicken Sie auf eine einzelne Benutzerzeile, um eine grafische Darstellung der Performance-Metriken dieses Benutzers anzuzeigen.



Sitzungen

Der Sitzungsbericht enthält Details auf Sitzungsebene. Um den Sitzungsbericht anzuzeigen, navigieren Sie zu **Berichte > HDX > Sitzungen**.



Das Dashboard zeigt die Berichte der HDX-Sitzungen an, die während des ausgewählten Zeitraums ausgeführt wurden (z. B. letzte 5 Minuten, letzte 30 Minuten, letzter Tag, letzter Monat usw.). Die Sitzungen werden basierend auf der QoE dieser Sitzung als gut (71-100), fair (51-70) oder schlecht (0-50) eingestuft. Der QoE-Wert im Zusammenfassungsabschnitt und in der Tabelle Top Affected ist der Durchschnittswert für den ausgewählten Zeitraum. Der Grafikbericht der Zeitreihen zeigt eine detaillierte Historie mit Zeitraffer. Jeder Balken zeigt den Prozentsatz guter, fairer und schlechter QoE-Sitzungen zu dieser Zeit an.

Sie können auch die prozentuale Anzahl der Sitzungen mit guter, fairer und schlechter QoE im Diagramm **Sitzungsverteilung basierend auf QoE** anzeigen. Bewegen Sie den Mauszeiger auf die Farbleiste, um die prozentuale Anzahl der Sitzungen im guten/mittleren/schlechten Zustand zu sehen.

> **Hinweis**
>
> - Die HDX-Sitzungsberichte basieren auf Statistiken des Client-Seite-SD-WAN, nicht des VDA-Seite-SD-WAN. Dies spiegelt die HDX-Erfahrung des Endbenutzers wider.
> - In der Tabelle „Am **häufigsten betroffene Sitzungen** "werden nur die 5 am stärksten betroffenen Sitzungen angezeigt. Standardmäßig werden die Top 5 Sessions mit der niedrigsten QoE angezeigt. Jede Spalte ist jedoch sortierbar, aufsteigend oder absteigend und wird als Abfragekriterium verwendet. Wenn Sie beispielsweise auf den Spaltentitel **Avg Jitter** klicken, werden entweder die 5 Sitzungen mit dem niedrigsten durchschnittlichen Jitter oder dem höchsten durchschnittlichen Jitter angezeigt. Um die Details aller HDX-Sitzungen während des ausgewählten Zeitraums **anzuzeigen, klicken Sie auf Weitere betroffene Sitzungen**anzeigen.

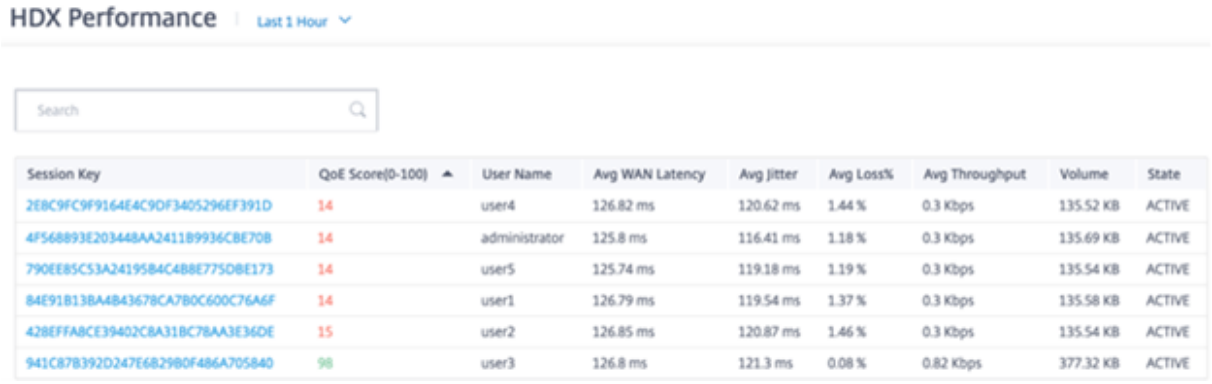
Im Folgenden sind die Details der obersten jeder Sitzung aufgeführt:

- **Sitzungsschlüssel**: Die eindeutige Identität für eine HDX-Sitzung.

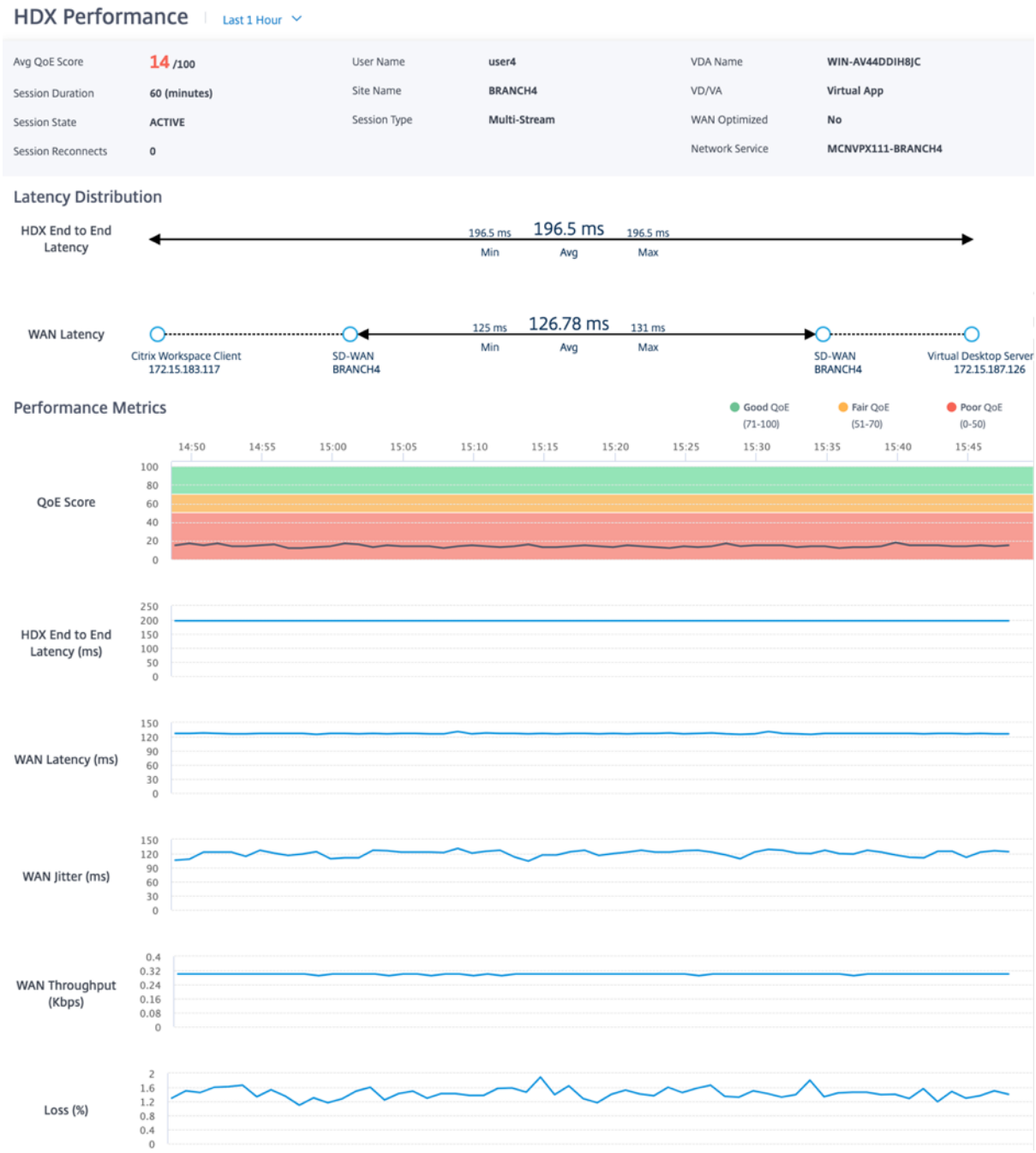
- **QoE Score (0-100)**: Die durchschnittliche QoE dieser Sitzung.
- **Benutzername**: Der Benutzername.
- **Durchschnittliche WAN-Latenz**: Die durchschnittliche WAN-Latenz der Sitzung für die ausgewählte Dauer, gemessen auf der Clientseite.
- **Durchschn. Jitter**: Der durchschnittliche Jitterwert der Sitzung für die gewählte Dauer.
- **Durchschn. Verlust%**: Der durchschnittliche prozentuale Verlustwert der Sitzung für die ausgewählte Dauer.
- **Durchschn**. Durchsatz: Der durchschnittliche Durchsatzwert der Sitzung für die ausgewählte Dauer.
- **Volumen**: Das gesamte Verkehrsaufkommen, das von dieser Sitzung verwendet wird. Die Citrix SD-WAN Orchestrator for On-premises GUI passt die Einheit möglicherweise basierend auf dem Zahlenwert an und ändert sie.
- **Status**: Status der Sitzung.

Wenn Sie auf einen Spaltentitel klicken, wird der Bericht nach dieser Spalte sortiert angezeigt. Klicken Sie auf **Weitere betroffene Sitzungen anzeigen**, um die Berichte aller Sitzungen anzuzeigen. Wenn Sie auf eine einzelne Zeile klicken, wird der detaillierte Bericht zu dieser Sitzung angezeigt.

Der folgende Screenshot ist ein Beispiel für die Berichtstabelle, in der alle Sitzungen angezeigt werden. Sie hat dieselben Spalten wie die Tabelle „ **Am häufigsten betroffene Sitzungen**“.



Klicken Sie auf den einzelnen Sitzungsschlüssel, um eine grafische Darstellung der Performance-Metriken zusammen mit den Details zu allen Variablen anzuzeigen, die QoE beeinflussen.



- **Durchschn. QoE Score**: Die durchschnittliche QoE über den ausgewählten Zeitraum.
- **Benutzername**: Der Benutzer, der diese Sitzung gestartet hat.
- **VDA-Name**: Name des VDA, von dem der veröffentlichte Desktop/die veröffentlichte Anwendung bereitgestellt wird.
- **Sitzungsdauer**: Die aktive Zeit dieser Sitzung im ausgewählten Zeitraum.
- **Site-Name**: Die Client-Site des Benutzers, als die Sitzung gestartet wurde.
- **VD/VA**: Ob es sich bei dieser Sitzung um eine **virtuelle Desktop** - oder eine **virtuelle Anwendungssitzung** handelt.

- **Sitzungsstatus**: Der Status der Sitzung am Ende des ausgewählten Zeitraums.
- **Sitzungstyp**: Gibt an, ob es sich beim letzten Start der Sitzung um eine Multistream-Sitzung oder eine Single-Stream-Sitzung handelt.
- **WAN-optimiert**: Gibt an, ob diese Sitzung WAN-optimiert war. Wenn das SD-WAN eine PE-Plattform ist, ist die WAN-Optimierung für HDX aktiviert und diese Sitzung optimiert ist, zeigt dieses Feld "true"an.
- **Wiederverbinden der Sitzung**: Wenn die Sitzung aufgrund eines Netzwerkproblems automatisch getrennt und erneut verbunden wurde, gibt dieses Feld die Anzahl solcher Ereignisse an.
- **Netzwerkdienst**: Dies ist der Dienstname, über den diese Sitzung bereitgestellt wird.
- **End-to-End-Latenz von HDX**: Die Hälfte des Werts der Roundtrip-Zeit zwischen dem VDA und dem Client.
- **WAN-Latenz**: Die Latenz vom VDA-SD-WAN zum clientseitigen SD-WAN.

IP-Regeln

October 21, 2022

IP-Regeln helfen Ihnen dabei, Regeln für Ihr Netzwerk zu erstellen und bestimmte Quality of Service (QoS) -Entscheidungen auf der Grundlage der Regeln zu treffen. Sie können benutzerdefinierte Regeln für Ihr Netzwerk erstellen. Sie können beispielsweise eine Regel wie folgt erstellen: Wenn die Quell-IP-Adresse 172.186.30.74 und die Ziel-IP-Adresse 172.186.10.89 ist, legen Sie die **Verkehrsrichtlinie** als **Persistenter Pfad und denDatenverkehrstyp**als**Echtzeit**fest.

Sie können Regeln für den Verkehrsfluss erstellen und die Regeln Anwendungen und Klassen zuordnen. Sie können Kriterien zum Filtern des Datenverkehrs für einen Flow angeben und allgemeine Verhaltensweisen, LAN-zu-WAN-Verhalten, WAN-zu-LAN-Verhalten und Paketprüfungsregeln anwenden.

Sie können globale und standortspezifische IP-Regeln auf Netzwerkebene erstellen. Wenn eine Site mit der global erstellten Regel verknüpft ist, können Sie Site-spezifische Regeln erstellen. In solchen Fällen haben standortspezifische Regeln Vorrang und setzen die global erstellte Regel außer Kraft.

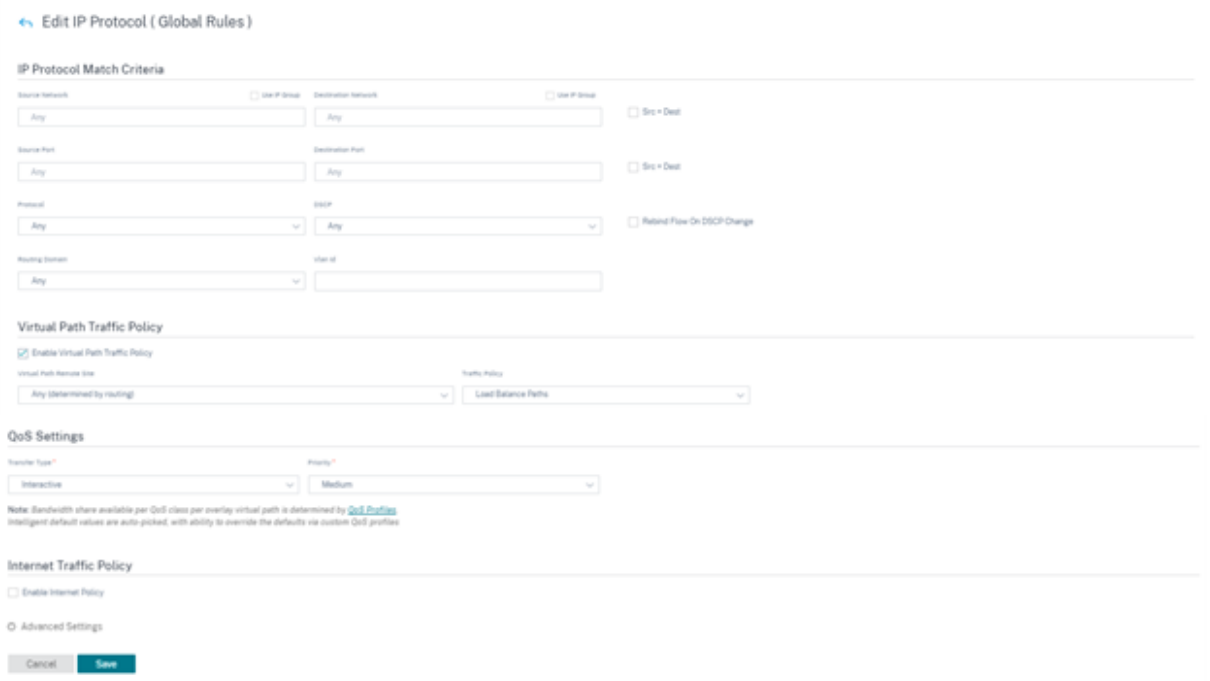
Die Standard-IP-Protokollregeln HTTP, HTTPS und ALTHTTPS werden in der Tabelle Regeln immer oben in der Liste angezeigt. Site-spezifische IP-Regeln (einmal erstellt) werden jedoch über HTTP-, HTTPS-, ALTHTTPS- und globalen IP-Regeln in der Tabelle Regeln angezeigt.

IP-Regeln erstellen

Um IP-Regeln zu erstellen, navigieren Sie zu **Konfiguration > QoS > QoS-Richtlinien** > **IP-Regeln**. Wählen Sie die Registerkarte **Globale Regeln** zum Erstellen von IP-Regeln auf globaler Ebene oder

Site-/Gruppenspezifische Regeln zum Erstellen von Regeln auf Standortebene.

Klicken Sie im Abschnitt **IP-Regeln auf NeueIP-Regel** .



- Übereinstimmungskriterien für das
  - **Sites hinzufügen/entfernen**: (nur beim Erstellen einer Site-spezifischen IP-Regel verfügbar) Wählen Sie die Sites aus, klicken Sie auf **Überprüfen**und dann auf **Fertig**.
  - **Quellnetzwerk**: Die Quell-IP-Adresse und Subnetzmaske, mit der die Regel übereinstimmt.
  - **Zielnetzwerk**: Die Ziel-IP-Adresse und Subnetzmaske, mit der die Regel übereinstimmt.
  - **IP-Gruppe verwenden**: Aktivieren Sie das Kontrollkästchen **IP-Gruppe verwenden**, um eine vorhandene IP-Gruppe aus der Dropdown-Liste auszuwählen.
  - **Src = Dst**: Wenn ausgewählt, wird die Quell-IP-Adresse auch für die Ziel-IP-Adresse verwendet.
  - **Quellport**: Der Quellport (oder Quellportbereich), dem die Regel entspricht.
  - **Zielport**: Der Zielport (oder Zielportbereich), dem die Regel entspricht.
  - **Src = Dst**: Wenn ausgewählt, wird der Quellport auch für den Zielport verwendet.
  - **Protokoll**: Das Protokoll, mit dem die Regel übereinstimmt. Sie können eines der vordefinierten Protokolle auswählen oder Beliebig **oderNumber**auswählen.
  - **Protokollnummer**: Dieses Feld wird nur angezeigt, wenn Sie in der Dropdownliste **Protokoll** die Option **Nummer** auswählen. Wenn Sie eine Protokollnummer auswählen, wird die dem Protokoll zugeordnete Ganzzahl für die Back-End-Konfigurationen verwendet.
  - **DSCP**: Das DSCP-Tag im IP-Header, dem die Regel entspricht.
  - **Routingdomäne**: Die Routingdomäne, der die Regel entspricht.

- **VLAN-ID**: Geben Sie die VLAN-ID für die Regel ein. Die VLAN-ID identifiziert den Datenverkehr zur und von der virtuellen Schnittstelle. Verwenden Sie die VLAN-ID als 0, um nativen oder nicht markierten Datenverkehr festzulegen.
- **Flow bei DSCP-Änderung neu binden**: Wenn diese Option ausgewählt ist, werden Flows, die ansonsten hinsichtlich der Übereinstimmungskriterien identisch sind, als separate Flows behandelt, wenn sich ihre DSCP-Felder unterscheiden.

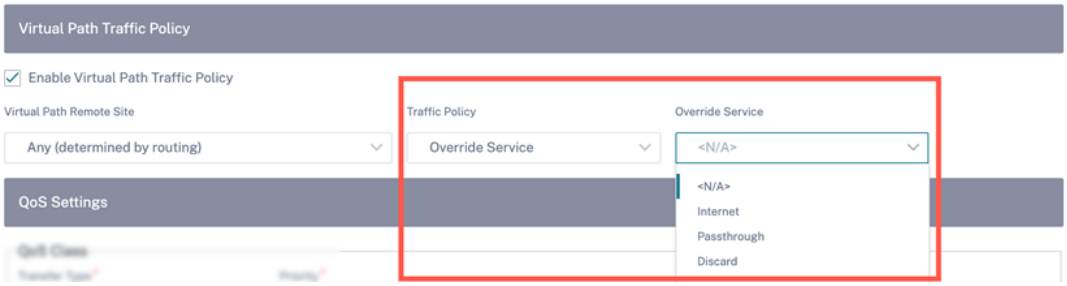
• Verkehrsrichtlinie für virtuelle Pfade

Aktivieren Sie das Kontrollkästchen **Verkehrsrichtlinie für virtuelle Pfade** aktivieren.

- **Virtueller Pfad Remote-Site**: Wählen Sie den virtuellen Pfad für die Remote-Site aus.
- **Verkehrsrichtlinie**: Wählen Sie nach Bedarf eine der folgenden Verkehrsrichtlinien.
  - **Lastausgleichspfade**: Der Anwendungsdatenverkehr für den Flow wird über mehrere Pfade verteilt. Der Datenverkehr wird über den besten Pfad gesendet, bis dieser Pfad verwendet wird. Die verbleibenden Pakete werden über den nächstbesten Pfad gesendet.
  - **Persistenter Pfad**: Der Anwendungsverkehr bleibt auf demselben Pfad, bis der Pfad nicht mehr verfügbar ist. Wählen Sie eine der folgenden **Persistenzrichtlinien**aus:
    - **Behalten Sie den ursprünglichen Link an**: Der Anwendungsdatenverkehr verbleibt auf dem ursprünglichen Link, bis der Pfad nicht mehr verfügbar ist.
    - **Bleiben Sie auf dem MPLS-Link, falls verfügbar, andernfalls auf dem ursprünglichen Link**: Der Anwendungsdatenverkehr verbleibt auf dem MPLS-Link. Wenn der MPLS-Link nicht verfügbar ist, verbleibt der Datenverkehr auf dem ursprünglichen Link.
    - **Bleiben Sie auf dem Internetlink, falls verfügbar, andernfalls auf dem ursprünglichen Link**: Der Anwendungsverkehr verbleibt auf dem Internetlink. Wenn die Internetverbindung nicht verfügbar ist, verbleibt der Datenverkehr auf dem ursprünglichen Link.
    - **Bleiben Sie auf dem privaten Intranet-Link, falls verfügbar, andernfalls auf dem ursprünglichen Link**: Der Anwendungsdatenverkehr verbleibt auf dem privaten Intranet-Link. Wenn der private Intranetlink nicht verfügbar ist, verbleibt der Datenverkehr auf dem ursprünglichen Link.

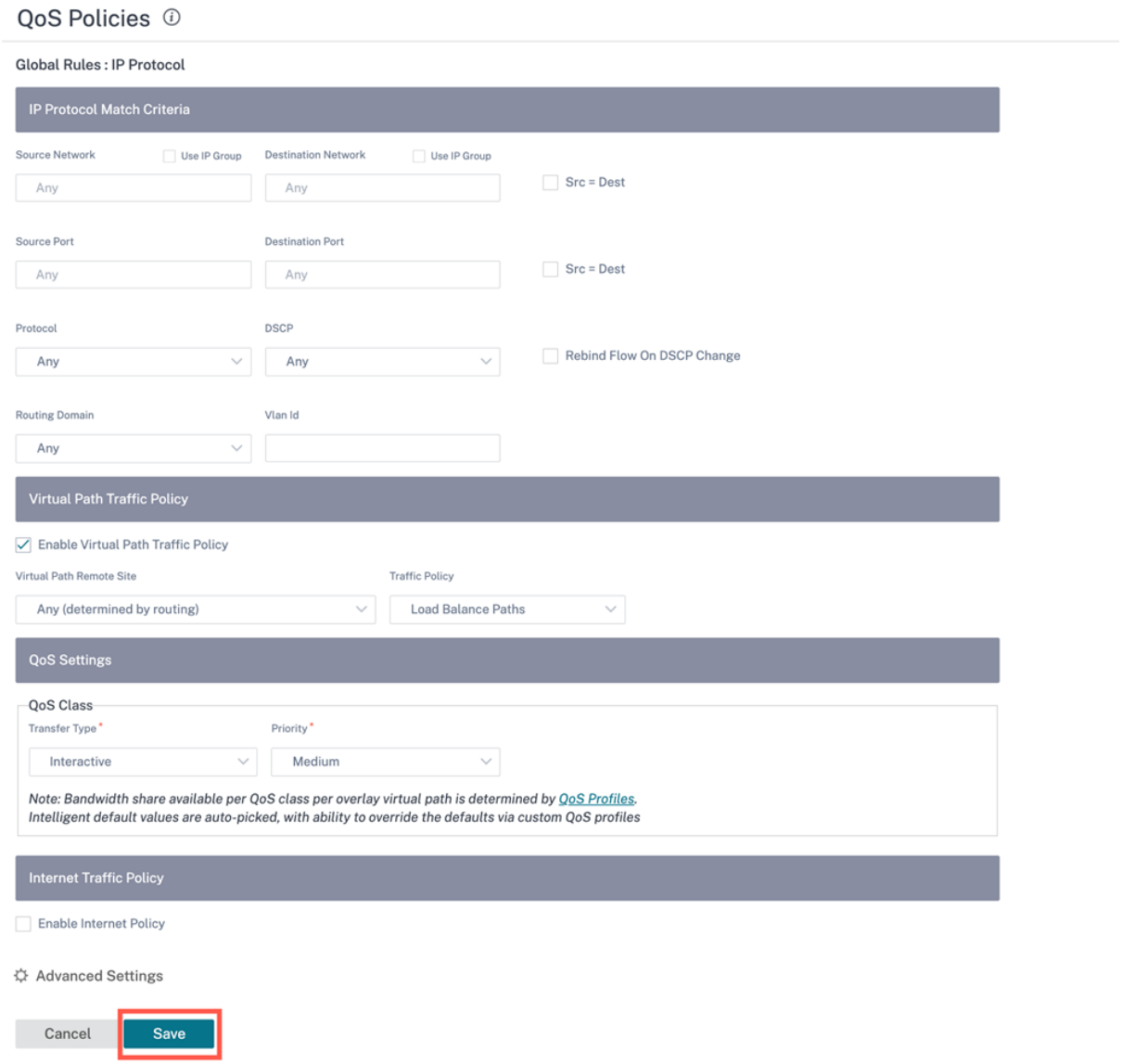
    Persistenzimpedanz ist die Zeit (in ms), bis zu der der Anwendungsdatenverkehr auf der Verbindung verbleibt.
  - **Doppelte Pfade**: Anwendungsdatenverkehr wird über mehrere Pfade dupliziert, was die Zuverlässigkeit erhöht
  - **Dienst außer Kraft setzen**: Der Verkehr für den Fluss wird zu einem anderen Dienst

überschrieben. Wählen Sie den Diensttyp Intranet, Internet, Passthrough oder Verwerfen aus, für den der virtuelle Pfaddienst außer Kraft gesetzt wird.

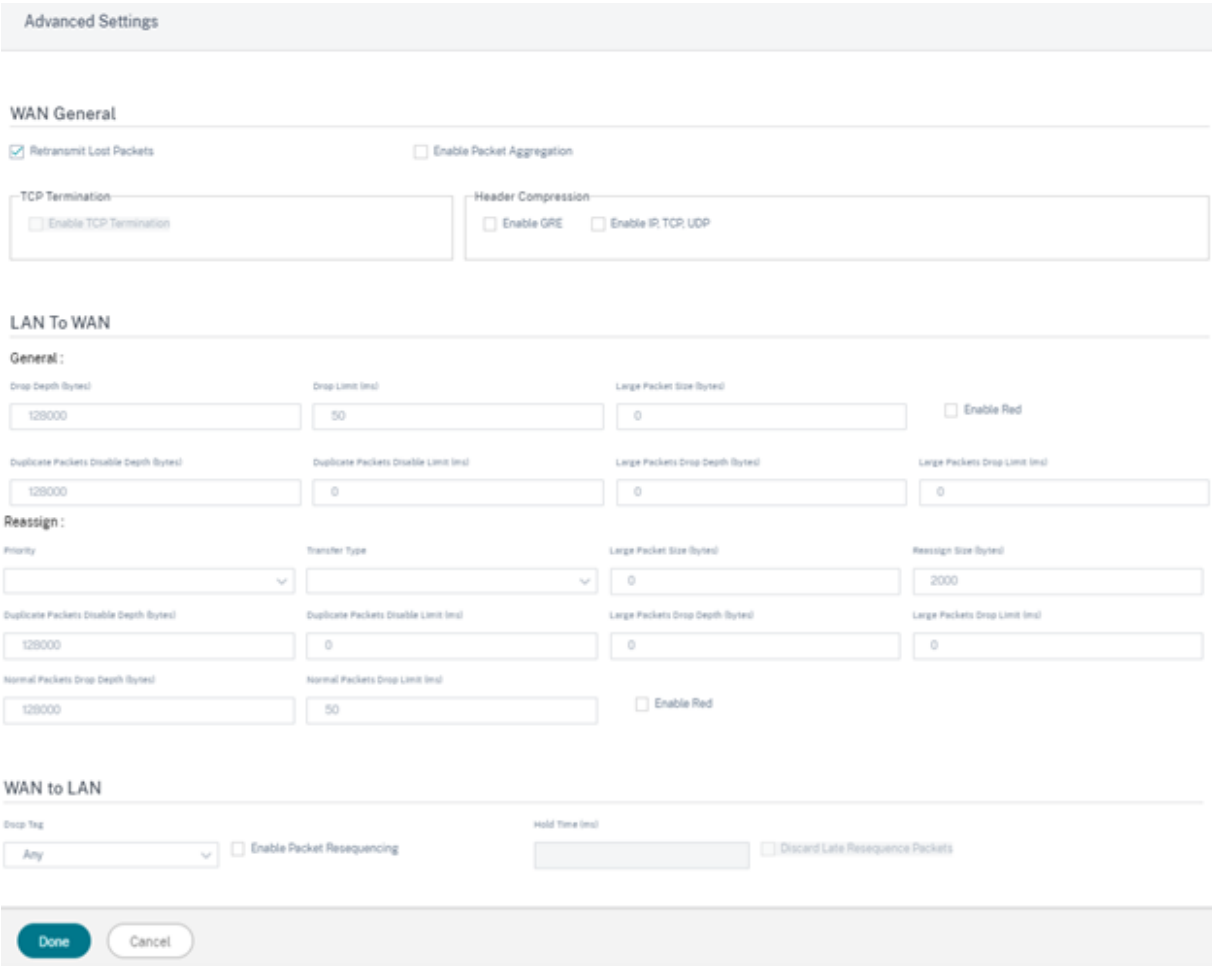


- QoS-Einstellungen (QoS-Klasse)
  - **Transferart**: Wählen Sie eine der folgenden Übertragungsarten:
    - **Echtzeit**: Wird für zeitkritischen Datenverkehr mit geringer Latenz, geringer Bandbreite verwendet. Echtzeitanwendungen sind zeitkritisch, benötigen aber keine wirklich hohe Bandbreite (z. B. Voice over IP). Echtzeitanwendungen reagieren empfindlich auf Latenz und Jitter, können jedoch einige Verluste tolerieren.
    - **Interaktiv**: Wird für interaktive Datenverkehr mit niedrigen bis mittleren Latenzanforderungen und niedrigen bis mittleren Bandbreitenanforderungen verwendet. Die Interaktion erfolgt in der Regel zwischen einem Client und einem Server. Die Kommunikation benötigt möglicherweise keine hohe Bandbreite, ist aber empfindlich gegenüber Verlust und Latenz.
    - **Bulk**: Wird für Traffic mit hoher Bandbreite und Anwendungen verwendet, die hohe Latenz tolerieren können. Anwendungen, die die Dateiübertragung verarbeiten und eine hohe Bandbreite benötigen, werden als Bulkklasse eingestuft. Diese Anwendungen beinhalten wenig menschliche Eingriffe und werden meist von den Systemen selbst behandelt.
  - **Priorität**: Wählen Sie eine Priorität für den ausgewählten Übertragungstyp.
- Richtlinien für den Internetverkehr
  - Aktivieren Sie das Kontrollkästchen **Internetrichtlinie aktivieren**, um die Richtlinie für den Internetverkehr zu konfigurieren.
  - **Modus**: Die Methode zum Senden und Empfangen von Paketen für Flows, die der Regel entsprechen. Sie können nach Bedarf **Override Service** oder **WAN-Link** wählen.
  - **WAN-Verbindung**: Die WAN-Verbindung, die von Flows verwendet werden soll, die der Regel entsprechen, wenn Internet Load Balancing aktiviert ist.
  - **Dienst überschreiben**: Der Zieldienst für Flows, die der Regel entsprechen.

> **Hinweis:**
>
> Ein virtueller Pfaddienst kann keinen anderen virtuellen Pfaddienst überschreiben



Erweiterte Einstellungen



- WAN Allgemeines
  - **Verlorene Pakete erneut übertragen**: Sendet Datenverkehr, der dieser Regel entspricht, über einen zuverlässigen Dienst an die Remote-Appliance und überträgt verlorene Pakete erneut.
  - **Paketaggregation aktivieren**: Aggregiert kleine Pakete zu größeren Paketen.
  - **TCP-Terminierung aktivieren**: Aktiviert die TCP-Terminierung des Datenverkehrs für Die Roundtrip-Zeit für die Bestätigung von Paketen wird reduziert und verbessert somit den Durchsatz.
  - **GRE aktivieren**: Komprimiert Header in GRE-Paketen.
  - **IP, TCP und UDP aktivieren**: Komprimiert Header in IP-, TCP- und UDP-Paketen.

    > **Hinweis:**
    >
    > IPv6-Pakete unterstützen keine Header-Komprimierung.

- LAN zu WAN

Allgemein

- **Drop-Tiefe (Byte)**: Schwellenwert für die Warteschlangentiefe, nach dem Pakete verworfen
- **Drop-Limit**: Zeit, nach der Pakete, die im Klassenplaner warten, verworfen werden. Gilt nicht für eine Massenklasse.
- **Große Paketgröße**: Paketen, die kleiner oder gleich dieser Größe sind, werden die Werte für Drop-Limit und Drop-Tiefe zugewiesen, die in den Feldern **Abwurftiefe großer Pakete (Byte)** und **Abwurflimit für große Pakete (ms)** angegeben sind. Paketen, die größer als diese Größe sind, werden die in den Standardfeldern Drop-Limit und Drop-Tiefe angegebenen Werte zugewiesen
- **RED aktivieren**: Random Early Detection (RED) gewährleistet eine faire gemeinsame Nutzung von Klassenressourcen, indem Pakete verworfen werden, wenn eine Überlastung auftritt.
- **Duplicate Packet Disable Depth (Byte)**: Die Warteschlangentiefe des Klassenplaners, an der die doppelten Pakete nicht generiert werden.
- **Deaktivierungslimit für doppelte Pakete**: Zeit, für die die Duplizierung deaktiviert werden kann, um zu verhindern, dass doppelte Pakete Bandbreite verbrauchen
- **Abwurftiefe großer Pakete (Byte)**: Wenn die Warteschlangentiefe diesen Schwellenwert überschreitet, werden die Pakete verworfen und Statistiken gezählt.
- **Abwurflimit für große Pakete (ms)**: Die maximale geschätzte Zeit, die Pakete, die größer oder gleich der Größe großer Pakete sind, im Klassenplaner warten müssen. Wenn die geschätzte Zeit diesen Schwellenwert überschreitet, werden die Pakete verworfen und Statistiken werden gezählt. Nicht gültig für Bulk-Klassen.

Erneut zuweisen

- **Priorität**: Sie können die Priorität der Standby-WAN-Verbindung nach Bedarf festlegen. Die Priorität der Standby-WAN-Verbindung gibt die Reihenfolge an, in der eine Standby-WAN-Verbindung aktiv wird. Eine Standby-WAN-Verbindung mit hoher Priorität wird zuerst aktiv. Eine WAN-Verbindung mit niedriger Priorität wird zuletzt aktiv.
- **Übertragungstyp**: Wählen Sie eine Übertragungsart aus, mit der diese Regel verknüpft werden soll.
- **Duplicate Packet Disable Depth (Byte)**: Die Warteschlangentiefe des Klassenplaners, an der keine doppelten Pakete generiert werden.
- **Deaktivierungslimit für doppelte Pakete**: Gibt die Zeit an, die ein Paket in der Warteschlange wartet, bevor keine Duplizierung durchgeführt wird. Dadurch wird verhindert, dass doppelte Pakete Bandbreite verbrauchen, wenn die Bandbreite begrenzt ist.
- **Abwurftiefe großer Pakete (Byte)**: Wenn die Warteschlangentiefe diesen Schwellenwert überschreitet, werden die Pakete verworfen und Statistiken gezählt.

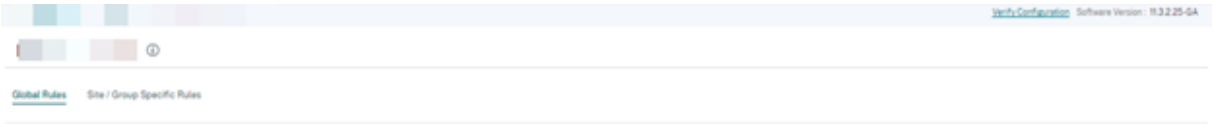
  - **Abwurflimit für große Pakete (ms)**: Wenn die geschätzte Zeit diesen Schwellenwert überschreitet, werden die Pakete verworfen und Statistiken werden gezählt. Nicht gültig für Bulk-Klassen.
  - **Normale Paket-Drop-Tiefe (Byte)**: Wenn die Warteschlangentiefe diesen Schwellenwert überschreitet, werden die Pakete verworfen und Statistiken werden gezählt.
  - **Normal Packets Drop Limit (ms)**: Wenn die geschätzte Zeit diesen Schwellenwert überschreitet, werden die Pakete verworfen und Statistiken werden gezählt. Nicht gültig für Bulk-Klassen.

- WAN zu LAN

  - **DSCP-Tag**: DSCP-Tag, das auf die Pakete angewendet wird, die dieser Regel auf WAN to LAN entsprechen, bevor sie an das LAN gesendet werden.
  - **Paketresequenzierung aktivieren**: Die Datenverkehrsflüsse, die der Regel entsprechen, werden für die Sequenzreihenfolge markiert, und die Pakete werden (falls erforderlich) auf der WAN-zu-LAN-Appliance neu angeordnet.
  - **Haltezeit**: Zeitintervall, für das die Pakete zur erneuten Sequenzierung gehalten werden, nach dem die Pakete an das LAN gesendet werden. Wenn der Timer abläuft, werden die Pakete an das LAN gesendet, ohne weiter auf die erforderlichen Sequenznummern zu warten.

    Wenn die Regel eine Verkehrsrichtlinie als doppelter Pfad hat, beträgt die Standardhaltezeit 80 ms. Andernfalls ist der Standardwert 900 ms für TCP-Regeln und 250 ms für Nicht-TCP-Regeln.
  - **Pakete mit verspäteter Resequenzierung**verwerfen: Verwirft Pakete außerhalb der Reihenfolge, die eingetroffen sind, nachdem die für die Resequenzierung benötigten Pakete an das LAN gesendet wurden.

Klicken Sie auf **Speichern**, um die Konfigurationseinstellungen zu speichern. **Klicken Sie auf der Seite**Konfiguration**>**QoS-Richtlinien**auf Konfiguration überprüfen, um alle Überwachungsfehler zu überprüfen.**



IP-Regeln überprüfen

Um IP-Regeln zu überprüfen, navigieren Sie zu **Berichte > Echtzeit > Flows**. Wählen Sie die Site aus, für die Sie die Flow-Informationen anzeigen möchten, und die Anzahl der anzuzeigenden Flows. Klicken Sie auf **Spalten anpassen**, und aktivieren Sie die Kontrollkästchen für die

Flow-Informationen, die Sie anzeigen möchten. Überprüfen Sie, ob die Flussinformationen den konfigurierten Regeln entsprechen.

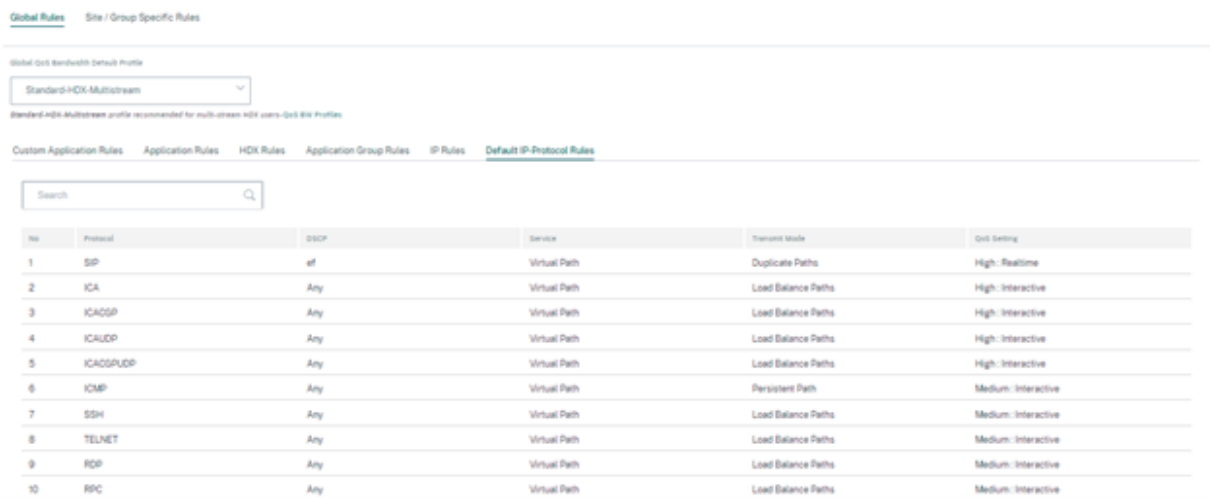
Navigieren Sie zu **Berichte > Echtzeit > Statistiken**, und wählen Sie **Regeln**aus. Wählen Sie die Site aus und klicken Sie auf **Neueste Daten abrufen**. Überprüfen Sie die konfigurierten Regeln. Weitere Informationen finden Sie unter Site-Berichte.

QoS-Richtlinien

October 21, 2022

Ein Administrator kann Anwendungs- und Verkehrsrichtlinien definieren. Diese Richtlinien helfen dabei, Verkehrssteuerung, Quality of Service (QoS) und Filterfunktionen für Anwendungen zu aktivieren. Geben Sie an, ob eine definierte Regel global auf alle Standorte im Netzwerk oder auf bestimmte Standorte angewendet werden kann.

Richtlinien werden in Form mehrerer Regeln definiert, die in der benutzerdefinierten Reihenfolge angewendet werden.



Neue Regel erstellen

Ein Administrator muss die definierte Regel basierend auf der Priorität platzieren. Die Prioritäten werden anhand von Parametern wie dem Anfang der Liste, dem Ende der Liste oder einer bestimmten Zeile kategorisiert.

Es wird empfohlen, am Anfang **spezifischere** Regeln für Anwendungen oder Unteranwendungen zu haben, gefolgt von **weniger spezifischen** Regeln für diejenigen, die einen breiteren Datenverkehr darstellen.

Sie können beispielsweise spezifische Regeln sowohl für Facebook Messenger (Unteranwendung) als auch für Facebook (Anwendung) erstellen. Setzen Sie eine Facebook Messenger-Regel auf die Facebook-Regel, damit die Facebook Messenger-Regel ausgewählt wird. Wenn die Bestellung rückgängig gemacht wird und Facebook Messenger eine Unteranwendung der Facebook-Anwendung ist, wird die Facebook Messenger-Regel nicht ausgewählt. Es ist wichtig, die richtige Reihenfolge zu finden.

Übereinstimmungskriterien

Wählen Sie Traffic für eine definierte Regel aus, z. B.:

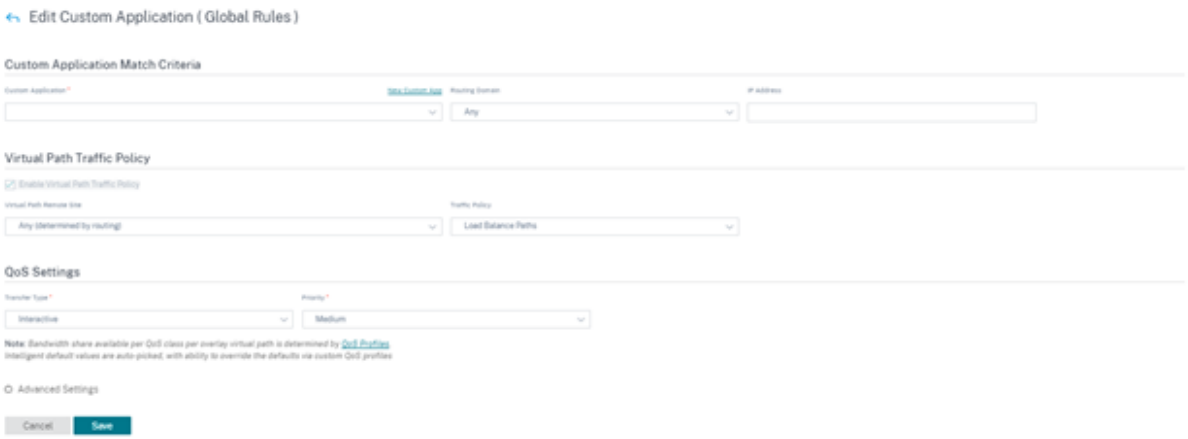
- Eine Bewerbung
- Benutzerdefinierte Anwendung
- Anwendungsgruppe oder IP-Protokoll-basierte Regel

Umfang der Regel

Geben Sie an, ob eine definierte Regel global auf alle Standorte im Netzwerk oder auf bestimmte Standorte angewendet werden kann.

Anwendungssteuerung

Navigieren Sie zu **Konfiguration** > **QoS** > **Benutzerdefinierte Anwendungsregeln**. Geben Sie an, wie der Verkehr gesteuert werden soll.

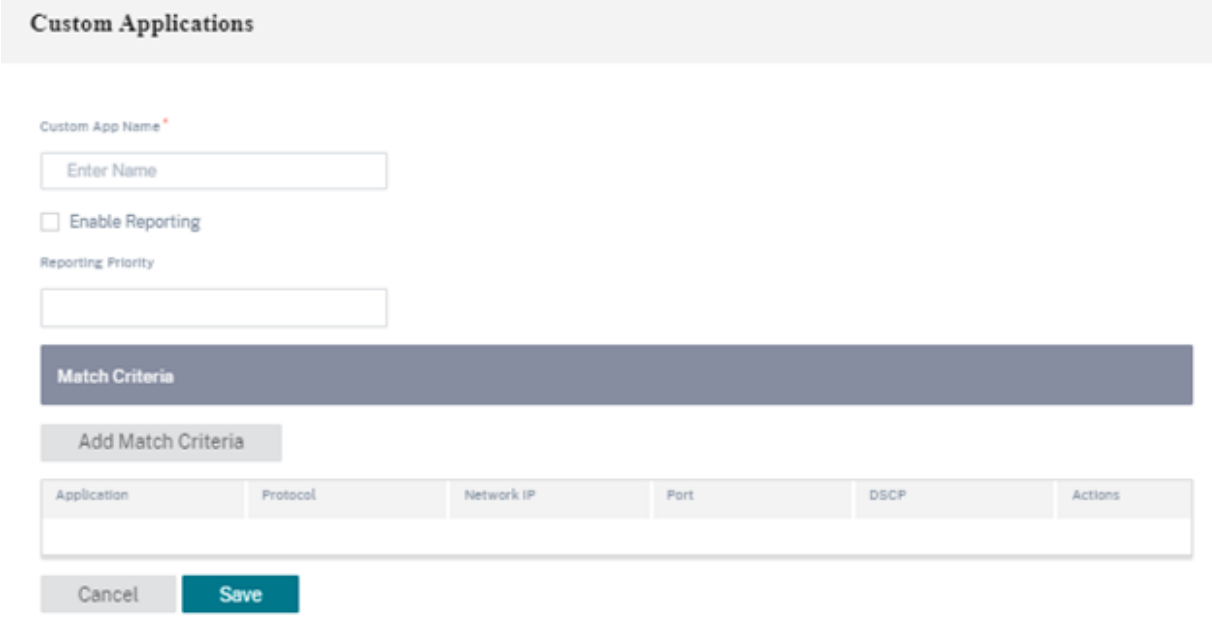


Neue benutzerdefinierte App: Wählen Sie ein Übereinstimmungskriterium aus der Liste aus. Der Administrator kann eine neue benutzerdefinierte Anwendung hinzufügen, indem er folgenden Namen gibt:

- Benutzerdefinierte Anwendung

- Protokoll (TCP, UDP, ICMP)
- Netzwerk-IP/Präfix
- Port
- DSCP Tag

Sie können auch eine auf Domainnamen basierende benutzerdefinierte Anwendung erstellen.

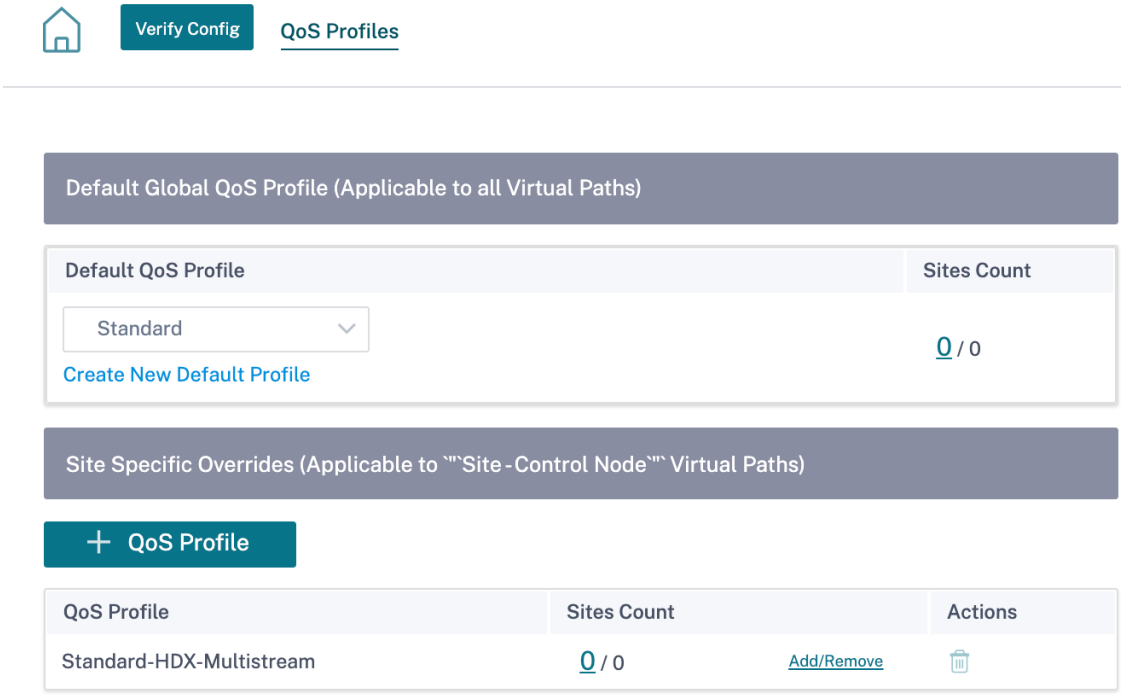


Klicken Sie auf der Seite Konfiguration**>**QoS-Richtlinien**auf Konfiguration überprüfen, um alle Überwachungsfehler zu überprüfen.**

IP-Regeln **IP-Regeln** helfen Ihnen dabei, Regeln für Ihr Netzwerk zu erstellen und bestimmte Quality of Service (QoS) -Entscheidungen auf der Grundlage der Regeln zu treffen. Weitere Informationen zu IP-Regeln finden Sie unter IP-Regeln.

QoS-Profile

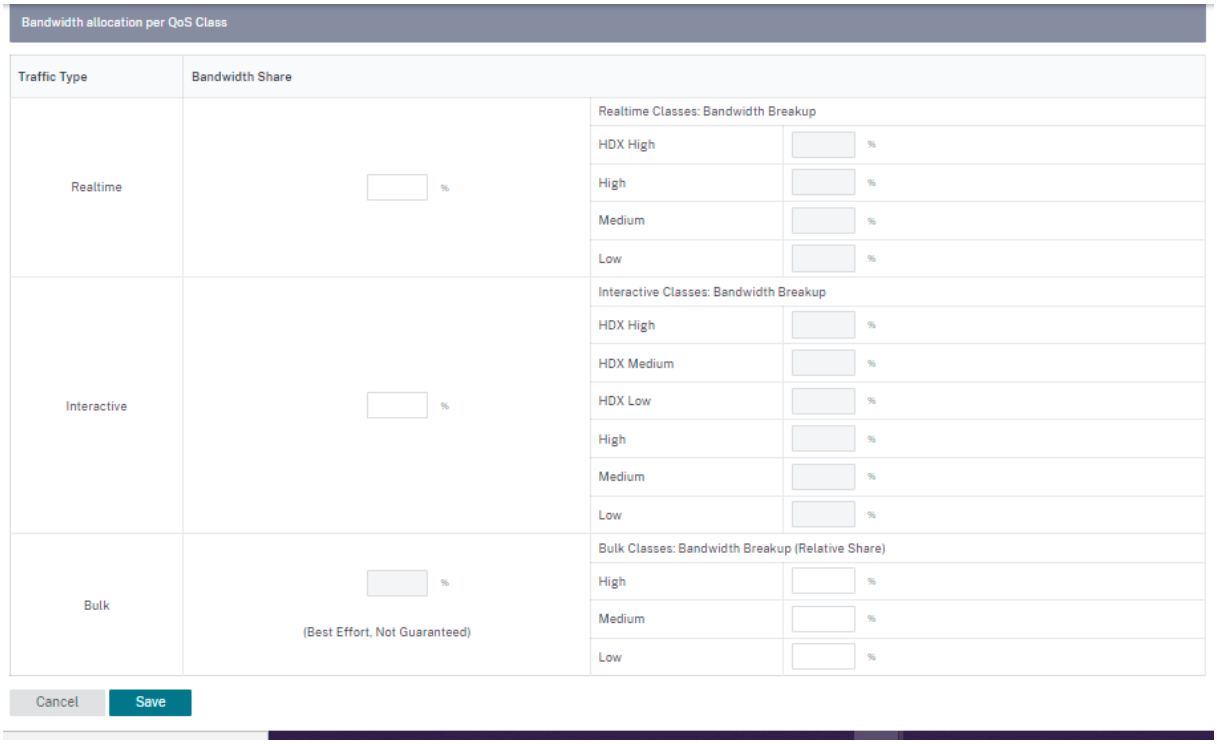
Der Abschnitt Quality of Service (QoS) hilft beim Erstellen des QoS-Profils mithilfe der Option **+ QoS-Profil** . Das QoS-Profil bietet verbesserten Service für bestimmten Datenverkehr. Das Ziel von QoS ist es, Priorität einschließlich der Art des Datenverkehrs (Echtzeit-, Interaktiv- und Massenklassen) und dedizierter Bandbreite bereitzustellen. Die Bandbreitenunterbrechungen sind in %-Werten verfügbar. Dies verbesserte auch die Verlusteigenschaften.



Klicken Sie auf der Seite Konfiguration**>**QoS-Richtlinien**auf Konfiguration überprüfen, um alle Überwachungsfehler zu überprüfen.**

Anpassen von QoS-Profilen

Wenn die Standardsätze für virtuelle Pfade verwendet werden, können Klassen unter **Konfiguration** > **QoS >**QoS-Profile****geändert werden. Klicken Sie auf **Neues Standardprofil erstellen**, geben Sie einen Namen für das Standardset ein, wählen Sie die Standorte aus und aktualisieren Sie die Bandbreitenzuweisung für die QoS-Klasse. Klicken Sie auf **Speichern**. Weitere Informationen zu Klassen finden Sie unter Klassen.

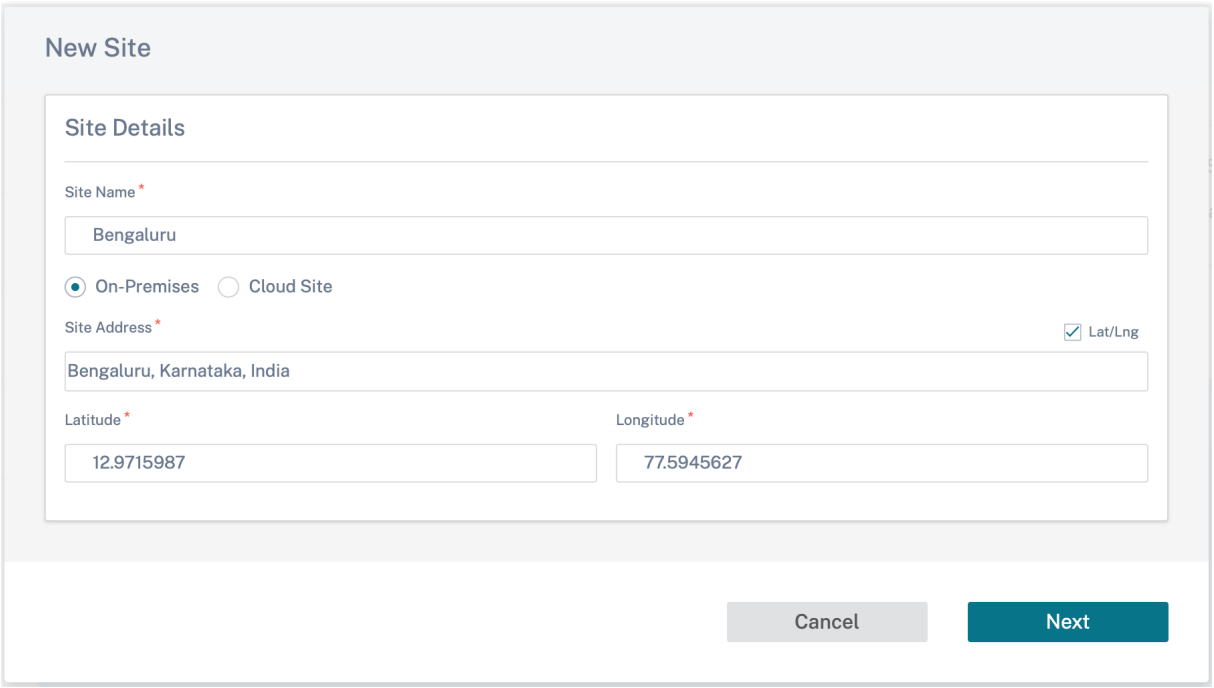


Site-Konfiguration

October 21, 2022

Sie können neue Sites über die **Netzwerkstartseite** oder über den Abschnitt **Profile & Vorlagen** hinzufügen, um Ihr SD-WAN-Netzwerk zu konfigurieren.

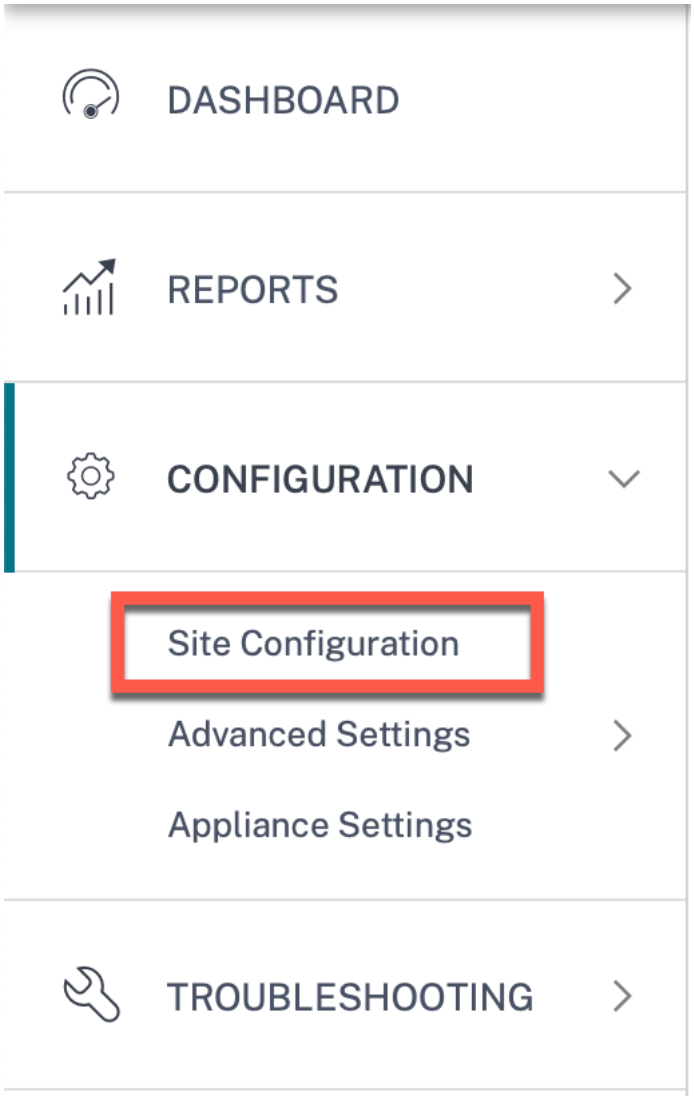
Um eine Site zu erstellen, klicken Sie im Netzwerk-Dashboard auf **+ Neue Site** . Geben Sie einen Namen und einen Speicherort für die Site an.



Sie können eine Site von Grund auf neu erstellen oder ein Site-Profil verwenden, um eine Site schnell zu konfigurieren.

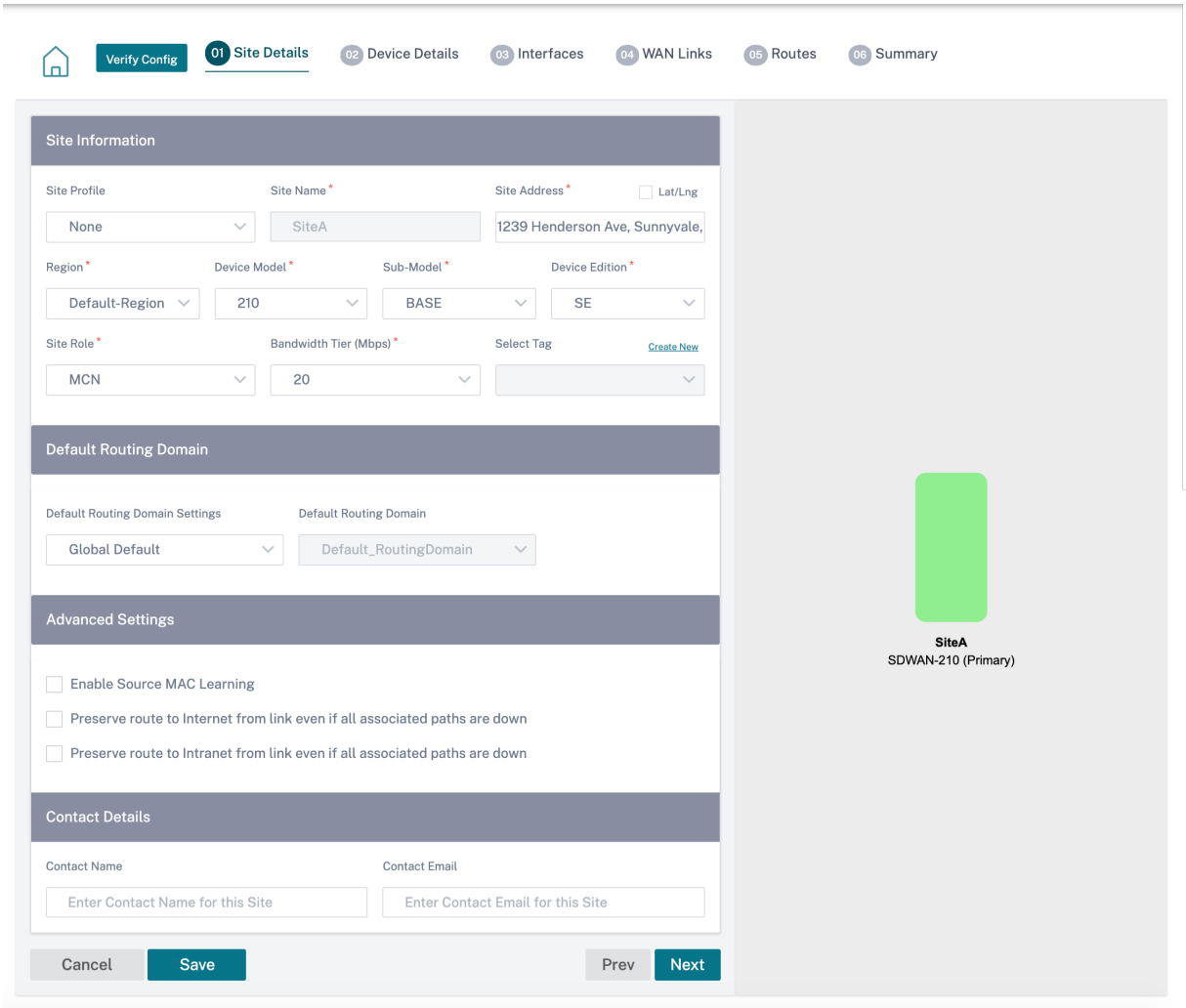
Eine grafische Anzeige auf der rechten Seite des Bildschirms zeigt ein dynamisches Topologiediagramm an, während Sie mit der Konfiguration fortfahren.

Um die Standortkonfiguration anzuzeigen, wählen Sie Site aus und navigieren Sie zu **Konfiguration > Standortkonfiguration**.

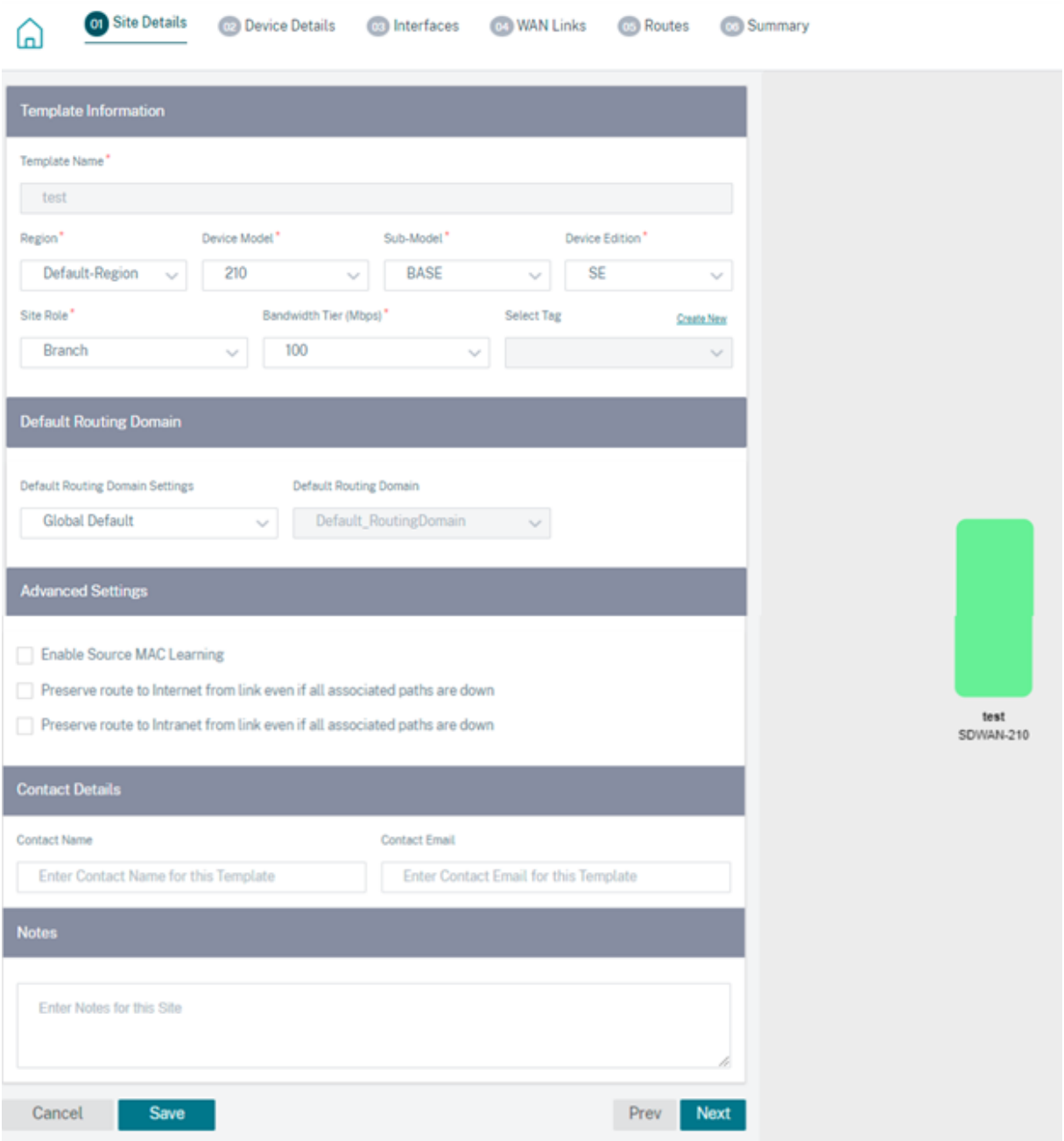


Site-Einzelheiten

Der erste Schritt umfasst die Eingabe der Site, des Geräts, der erweiterten Einstellungen und der Site-Kontaktdaten.



Wenn Sie Sites mithilfe einer Site-Vorlage konfigurieren, wird der folgende Bildschirm angezeigt.



Site-/Vorlageninformationen

- Wenn Sie ein **Standortprofil** auswählen, werden die Site-, Schnittstellen- und WAN-Linksparameter basierend auf der Standortprofilkonfiguration automatisch ausgefüllt.
- **Site-Adresse** und **Site-Name** werden basierend auf den im vorherigen Schritt angegebenen Details automatisch ausgefüllt.
- Aktivieren Sie das Kontrollkästchen **Lat/Lng**, um den Breiten- und Längengrad eines Standorts

abzurufen.

- Wählen Sie die **Region** aus der Dropdownliste aus.
- **Gerätemodell** und **Submodell** können basierend auf dem Hardwaremodell oder der virtuellen Appliance ausgewählt werden, die an einem bestimmten Standort verwendet werden.
- Die**Device Edition** wird automatisch basierend auf dem ausgewählten Gerätemodell wiedergegeben. Derzeit werden Premium Edition (PE), Advanced Edition (AE) und Standard Edition (SE) unterstützt. Das PE-Modell wird nur auf 1100-, 2100-, 5100- und 6100-Plattformen unterstützt. Das AE-Modell wird auf 210- und 1100-Plattformen unterstützt.

  > **Hinweis**
  >
  > Der Citrix SD-WAN Orchestrator Service unterstützt keine Advanced Edition- und Premium Edition-Plattformen.

- **Site-Rolle** definiert die Rolle des Geräts. Sie können einer Site eine der folgenden Rollen zuweisen:
  - **MCN**: Master Control Node (MCN) dient als Controller des Netzwerks, und nur ein aktives Gerät in einem Netzwerk kann als MCN bezeichnet werden.
  - **Niederlassung**: Appliances an den Zweigstellen, die vom MCN konfiguriert werden und an der Einrichtung virtueller WAN-Funktionalitäten für die Zweigstellen beteiligt sind. Es kann mehrere Filialen geben.
  - **RCN**: Regional Control Node (RCN) unterstützt eine hierarchische Netzwerkarchitektur und ermöglicht die Bereitstellung von Netzwerken in mehreren Regionen. MCN steuert mehrere RCNs und jeder RCN wiederum steuert mehrere Zweigstandorte.
  - **Georedundanter MCN**: Ein Standort an einem anderen Standort, der die Verwaltungsfunktionen des MCN übernimmt, falls er nicht verfügbar ist, wodurch eine Notfallwiederherstellung sichergestellt wird. Der georedundante MCN bietet keine Hochverfügbarkeits- oder Failover-Funktionen für den MCN.
  - **Georedundanter RCN**: Ein Standort an einem anderen Standort, der die Verwaltungsfunktionen des RCN übernimmt, falls er nicht verfügbar ist, wodurch eine Notfallwiederherstellung sichergestellt wird. Die georedundante RCN bietet keine Hochverfügbarkeits- oder Failover-Funktionen für den RCN.
- **Bandbreiten-Tier** ist die abrechenbare Bandbreitenkapazität, die Sie je nach Gerätemodell auf jedem Gerät konfigurieren können. Zum Beispiel unterstützt die SD-WAN 410 Standard Edition (SE) -Appliance Bandbreitensteinen von 20, 50, 100, 150 und 200 Mbit/s. Abhängig von Ihren Bandbreitenanforderungen für eine bestimmte Site können Sie die gewünschte Stufe auswählen. Jeder Standort wird für die konfigurierte Bandbreitenstufe in Rechnung gestellt.

Routing-Domäne

Im Abschnitt **Routingdomäne** können Sie die Standard-Routingdomäne für den Standort auswählen. **Routingdomäneneinstellungen** können entweder global oder standortspezifisch sein. Wenn Sie **Globale Standardwerte**auswählen, wird die global gültige Standard-Routingdomäne automatisch ausgewählt. Wenn Sie **Standortspezifisch**auswählen, können Sie die Standard-Routingdomäne aus der Dropdown-Liste **Routingdomäne** auswählen.

Routing Unterstützung für LAN-Segmentierung

Die SD-WAN Standard und Enterprise Edition (SE/PE) -Appliances implementieren die LAN-Segmentierung über verschiedene Standorte hinweg, an denen eine der beiden Appliances bereitgestellt wird. Die Appliances erkennen und verwalten eine Aufzeichnung der verfügbaren LAN-seitigen VLANs und konfigurieren Regeln dafür, zu welchen anderen LAN-Segmenten (VLANs) an einem Remotestandort mit einer anderen SD-WAN SE/PE-Appliance eine Verbindung herstellen können.

Die obige Funktion wird mithilfe einer VRF-Tabelle (Virtual Routing and Forwarding) implementiert, die in der SD-WAN SE/PE-Appliance verwaltet wird und die Remote-IP-Adressbereiche verfolgt, auf die ein lokales LAN-Segment zugreifen kann. Dieser VLAN-zu-VLAN-Datenverkehr würde das WAN immer noch über denselben vorab festgelegten virtuellen Pfad zwischen den beiden Appliances durchqueren (es müssen keine neuen Pfade erstellt werden).

Ein Beispiel für diese Funktionalität ist, dass ein WAN-Administrator in der Lage sein könnte, die Netzwerkumgebung einer lokalen Zweigstelle über ein VLAN zu segmentieren und einigen dieser Segmente (VLANs) Zugriff auf DC-seitige LAN-Segmente zu gewähren, die Zugriff auf das Internet haben, während andere möglicherweise keinen solchen Zugriff erhalten. Die Konfiguration der VLAN-zu-VLAN-Verknüpfungen erfolgt über die Webschnittstelle des Citrix SD-WAN Orchestrator Service.

Erweiterte Einstellungen

- **Quell-MAC-Lernen aktivieren**: Speichert die Quell-MAC-Adresse der empfangenen Pakete, sodass ausgehende Pakete an dasselbe Ziel an denselben Port gesendet werden können.
- **Route zum Internet vom Link beibehalten, auch wenn alle zugehörigen Pfade ausgefallen sind**: Wenn diese Option aktiviert ist, wählen die für den Internetdienst bestimmten Pakete weiterhin den Internetdienst aus, auch wenn nicht alle WAN-Links für den Internetdienst verfügbar sind.
- **Route zum Intranet vom Link beibehalten, auch wenn alle zugehörigen Pfade ausgefallen sind**: Wenn diese Option aktiviert ist, wählen die für den Intranetdienst bestimmten Pakete

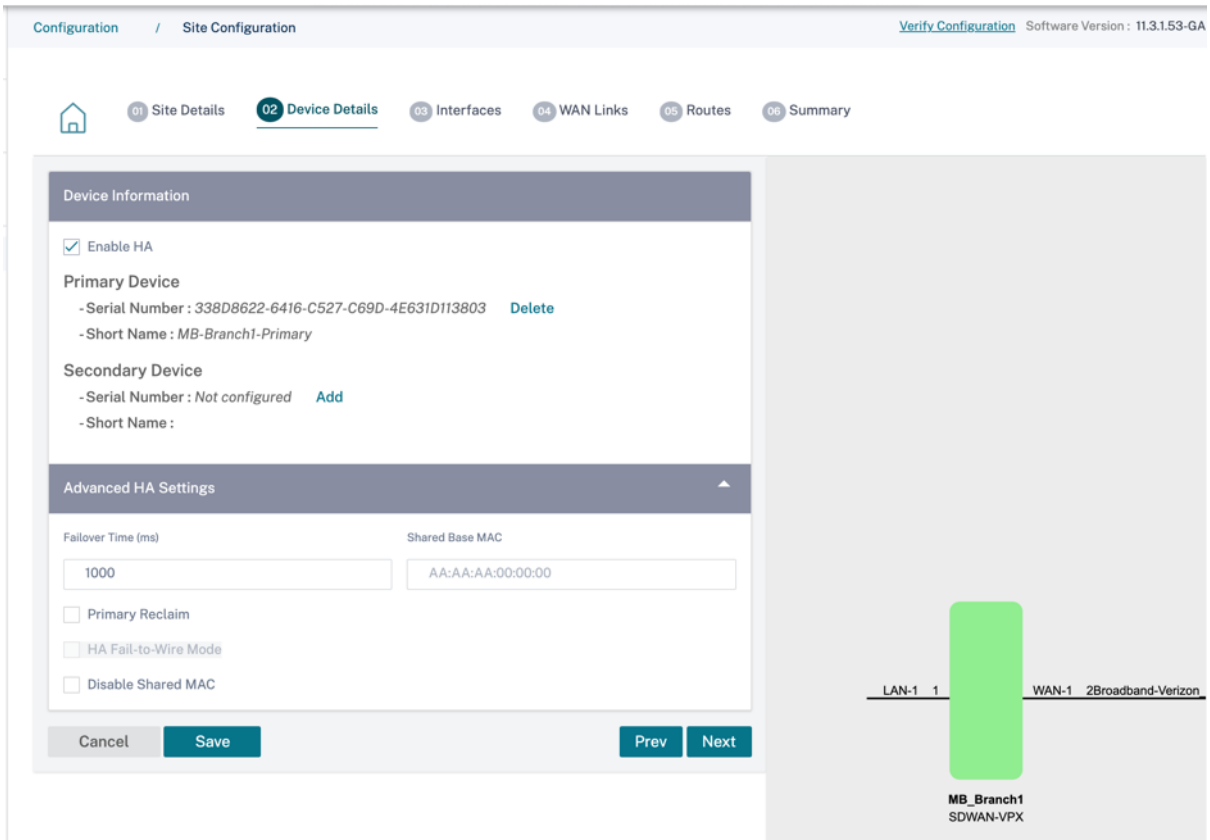
weiterhin den Intranetdienst aus, auch wenn nicht alle WAN-Links für den Intranetdienst verfügbar sind.

- Die Kontaktdaten des Administrators sind auf der Website verfügbar.

Ein dynamisches Netzwerkschema rechts neben dem Konfigurationspanel bietet fortlaufend visuelles Feedback, während Sie den Konfigurationsprozess durchlaufen.

Gerätedetails

Im Abschnitt "Gerätedetails"können Sie High Availability (HA) an einem Standort konfigurieren und aktivieren. Mit HA können zwei Appliances an einem Standort als aktive primäre und passive Sekundärstufe eingesetzt werden. Die sekundäre Appliance übernimmt, wenn die primäre Ausfall erfolgt. Weitere Informationen finden Sie unter Hochverfügbarkeit.

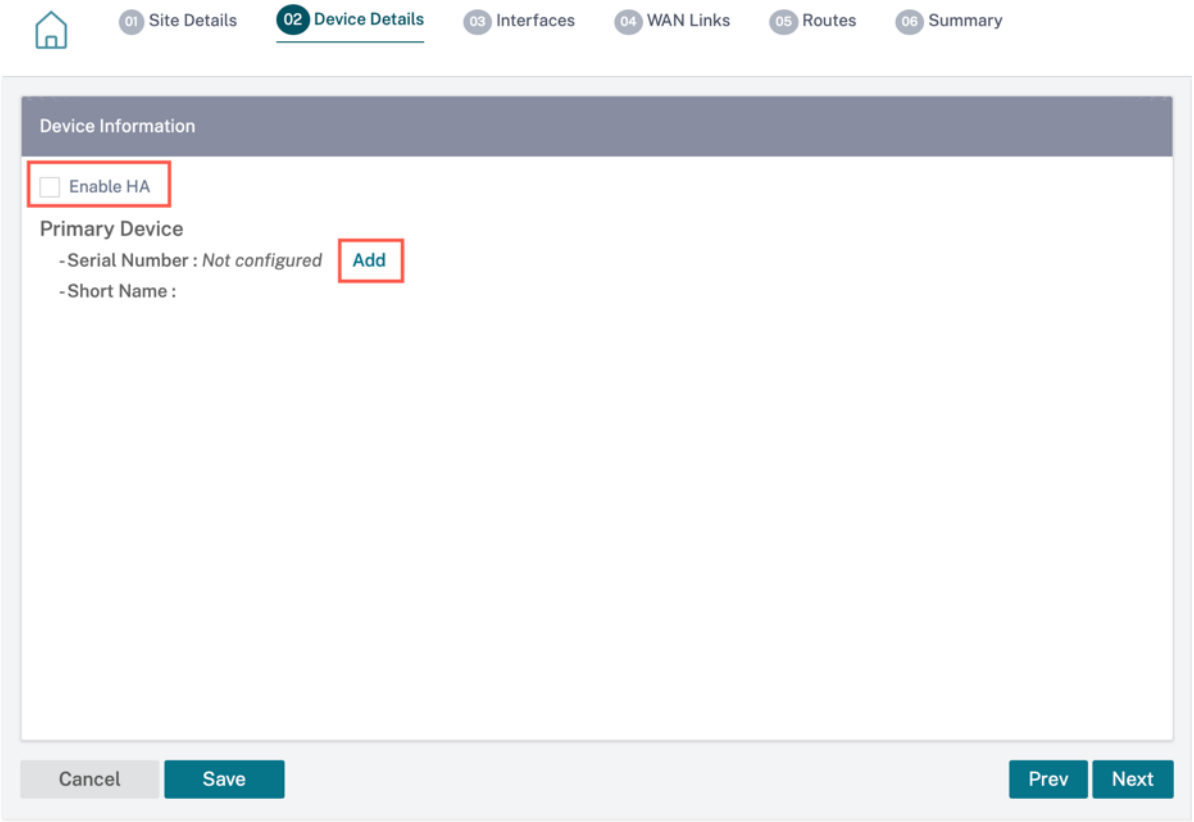


Hinweis

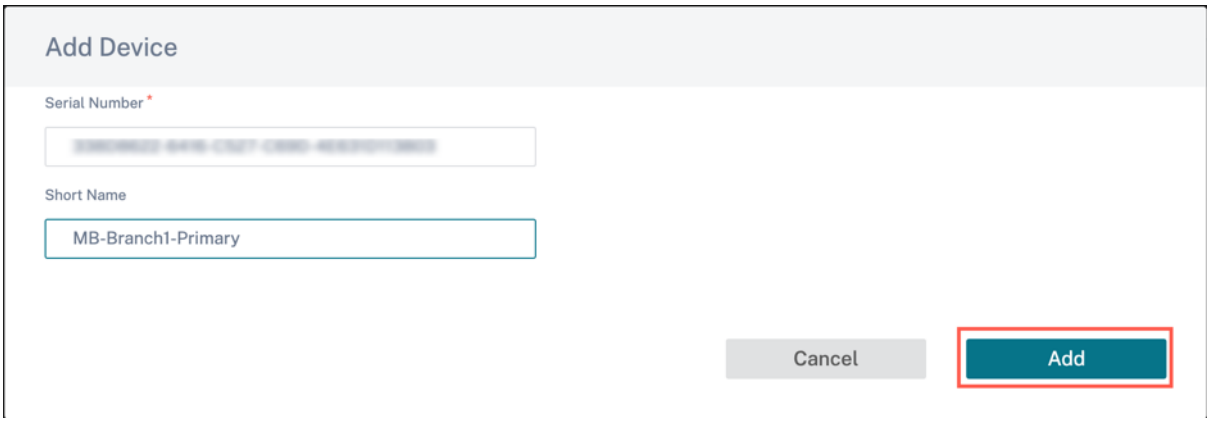
Seriennummern können nicht mithilfe der Site-Vorlagen konfiguriert werden.

Geräteinformationen

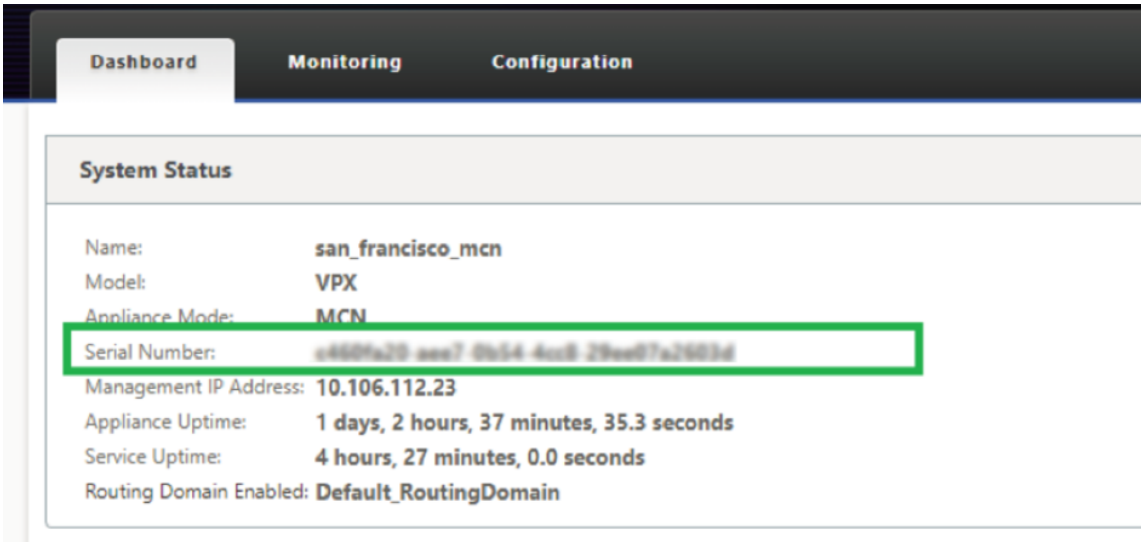
Aktivieren Sie HA und geben Sie die Seriennummer und einen Kurznamen für die primären und sekundären Appliances ein. Klicken Sie auf **Hinzufügen** und geben Sie die Seriennummer zusammen mit dem Kurznamen der Site an.



Klicken Sie auf **Hinzufügen**.



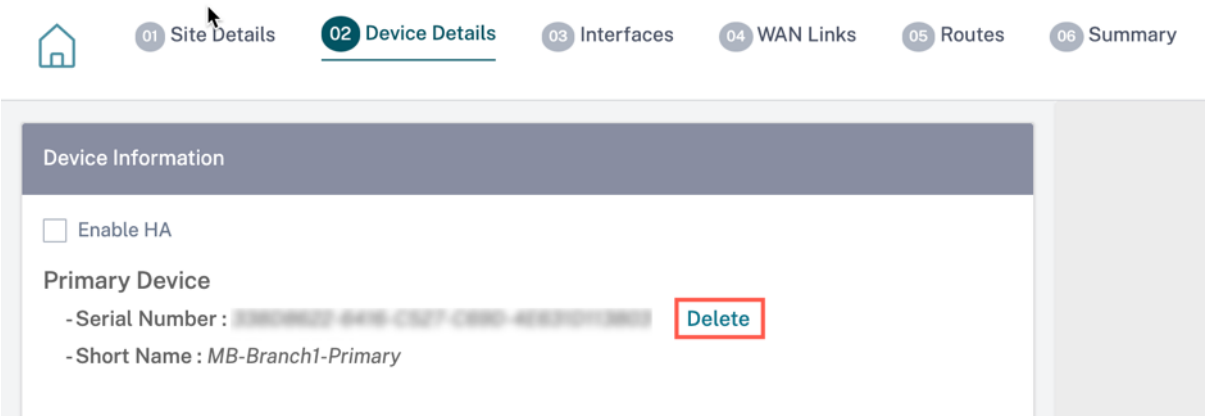
- **Seriennummer**: Auf die **Seriennummer** einer virtuellen SD-WAN-Instanz (VPX) kann über die VPX-Webkonsole zugegriffen werden, wie im folgenden Screenshot hervorgehoben. Eine Seriennummer einer Hardware-Appliance finden Sie auch auf dem Geräteetikett.



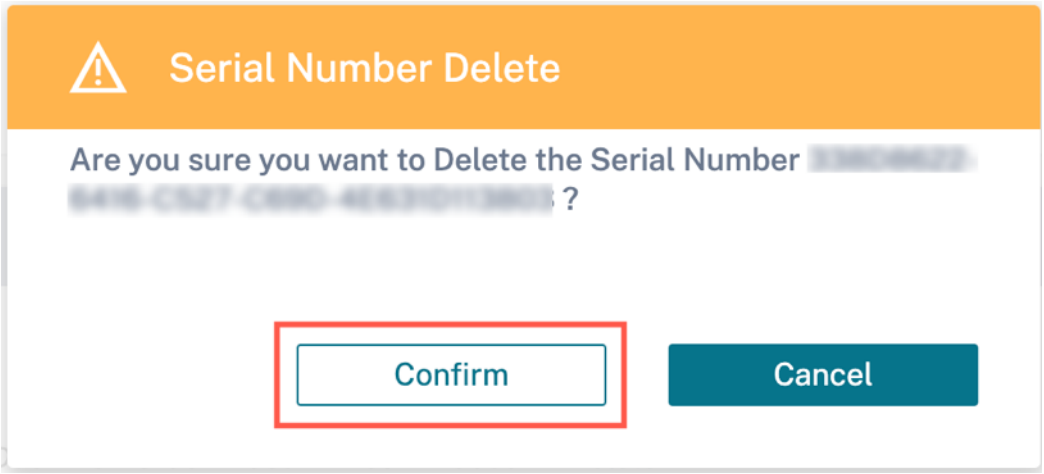
- **Kurzname**: Das Feld **Kurzname** wird verwendet, um einen leicht identifizierbaren Kurznamen für eine Site anzugeben oder eine Site bei Bedarf zu kennzeichnen.

Klicken Sie auf die Option **Löschen**, wenn Sie die Seriennummer löschen möchten.

> **Hinweis:**
> Um die Seriennummer zu aktualisieren, müssen Sie die vorhandene Seriennummer löschen und eine neue einlesen.



Wenn Sie auf die Option **Löschen** klicken, wird ein Popup-Fenster angezeigt, um zu bestätigen, ob Sie die Seriennummer löschen möchten oder nicht.



Erweiterte HA-Einstellungen

- **Failover-Zeit (ms)**: Die Wartezeit nach dem Verlust des Kontakts mit der primären Appliance, bevor die Standby-Appliance aktiv wird.
- **Gemeinsamer Basis-MAC**: Die gemeinsam genutzte MAC-Adresse für die Geräte mit hoher Verfügbarkeit. Wenn ein Failover auftritt, verfügt die sekundäre Appliance über dieselben virtuellen MAC-Adressen wie die fehlgeschlagene primäre Appliance.
- **Shared Base MAC deaktivieren**: Diese Option ist nur auf Hypervisor- und Cloud-basierten Plattformen verfügbar. Wählen Sie diese Option, um die gemeinsam genutzte virtuelle MAC-Adresse zu deaktivieren.
- **Primäre Rückforderung**: Die designierte primäre Appliance übernimmt beim Neustart nach einem Failover-Ereignis die Kontrolle zurück.
- **HA-Fail-to-Wire-Modus**: Der HA-Fail-to-Wire-Modus ist aktiviert. Weitere Einzelheiten finden Sie unter HA-Bereitstellungsmodi.
- **Y-Kabel-Unterstützung aktivieren**: Die Small Form-Factor Pluggable (SFP) -Ports können mit einem Glasfaser-Y-Kabel verwendet werden, um die Hochverfügbarkeitsfunktion für die Edge-Modus-Bereitstellung zu aktivieren. Diese Option ist nur für Citrix SD-WAN 1100 SE/PE Appliances verfügbar. Weitere Informationen finden Sie unter Hochverfügbarkeit im Edge-Modus mithilfe von Glasfaser-Y-Kabeln aktivieren.

Wi-Fi-Einzelheiten

Sie können eine Citrix SD-WAN-Appliance, die Wi-Fi unterstützt, als Wi-Fi-Zugangspunkt konfigurieren.

Die folgenden zwei Varianten der Citrix SD-WAN 110-Plattform unterstützen Wi-Fi und können als Wi-Fi-Zugangspunkt konfiguriert werden:

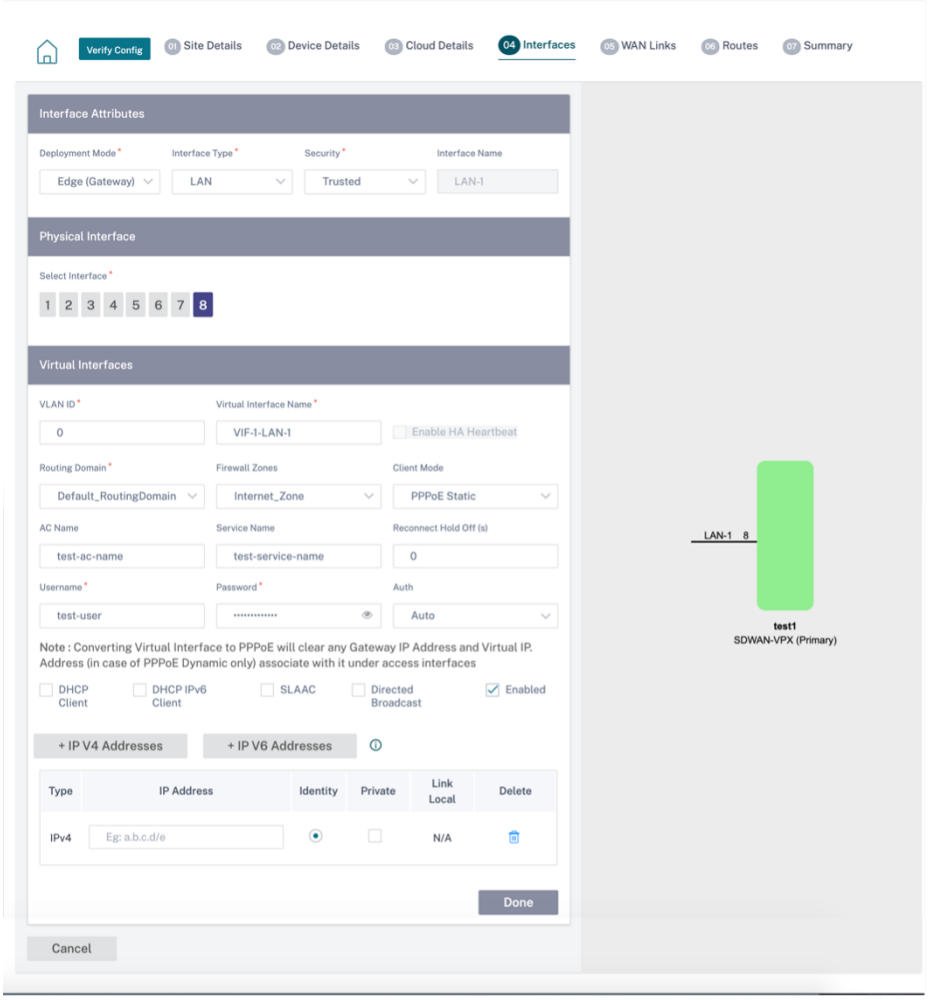
- Citrix SD-WAN 110-WiFi-SE
- Citrix SD-WAN 110-LTE-WLAN

Weitere Informationen zur Wi-Fi-Konfiguration finden Sie unter Wi-Fi Access Point

Schnittstellen

Der nächste Schritt besteht darin, die Schnittstellen hinzuzufügen und zu konfigurieren. Klicken Sie auf **+ Schnittstelle**, um die Konfiguration der Schnittstelle zu starten Klicken Sie auf **+ HA-Schnittstelle**, um die HA-Schnittstelle zu konfigurieren Die Option **+ HA-Schnittstelle** ist nur verfügbar, wenn Sie eine sekundäre Appliance für hohe Verfügbarkeit konfiguriert haben.

Bei der Schnittstellenkonfiguration wird der Bereitstellungsmodus ausgewählt und die Attribute auf Schnittstellenebene festgelegt. Diese Konfiguration gilt sowohl für LAN- als auch für WAN-Verbindungen.



In-Band-Verwaltung

Mit der In-Band-Verwaltung können Sie die SD-WAN-Datenports für die Verwaltung verwenden. Es trägt sowohl Daten- als auch Verwaltungsverkehr, ohne dass ein zusätzlicher Verwaltungspfad konfiguriert werden muss. Durch die In-Band-Verwaltung können virtuelle IP-Adressen mit Verwaltungsdiensten wie Web-UI und SSH verbunden werden. Sie können auf die Web-UI und SSH über die Management-IP und virtuelle In-Band-IPs zugreifen.

Um die In-Band-Verwaltung zu aktivieren, wählen Sie eine IPv4-Adresse aus der Dropdown-Liste **InBand-Verwaltungs-IP** oder eine IPv6-Adresse aus der Dropdown-Liste **InBand-Verwaltung IPv6** aus. Wählen Sie aus der Dropdown-Liste InBand Management DNS oder InBand Management DNS **V6 den**DNS-Proxy**aus, an den alle**DNS-Anforderungen**über die Inband- und Backup-Verwaltungsebene** weitergeleitet werden.

Weitere Informationen zur In-Band-Verwaltung finden Sie unter In-Band-Verwaltung.

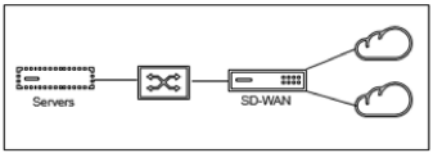
Die für Schnittstellen konfigurierten IP-Adressen werden in der Dropdownliste **InBand Management IP** aufgeführt. Die unter **Erweiterte Einstellungen > DNS konfigurierten DNS-Proxydienste** werden in der Dropdownliste **InBand Management DNS** aufgelistet.

Interface-Attribute

Die folgenden Bereitstellungsmodi werden unterstützt:

1. Edge (Gateway)
2. Inline —Fail-to-Wire, Fail-to-Block und virtuell inline.

- **Bereitstellungsmodus**: Wählen Sie einen der folgenden Bereitstellungsmodi aus.
  - **Edge (Gateway)**:

    Der Gateway-Modus impliziert, dass SD-WAN als „Gateway“zum WAN für den gesamten LAN-Verkehr dient. Der **Gateway-Modus** ist der Standardmodus. Sie können die Appliance als Gateway auf der LAN- oder WAN-Seite bereitstellen.
  - **Inline**:

    Wenn SD-WAN inline zwischen einem LAN-Switch und einem WAN-Router bereitgestellt wird, wird erwartet, dass SD-WAN LAN und WAN „überbrückt“.

    Alle Citrix SD-WAN-Appliances verfügen über vordefinierte Bridge-gekoppelte Schnittstellen. Wenn die Option Bridge aktiviert ist, hebt die Auswahl einer beliebigen Schnittstelle auf

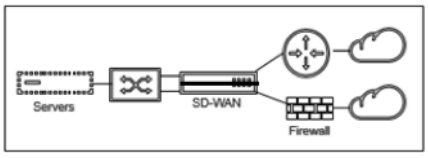
der LAN-Seite automatisch die gekoppelte Schnittstelle hervor, die für das WAN-Ende der Bridge reserviert ist. Beispielsweise sind die physikalischen Schnittstellen 1 und 2 ein überbrücktes Paar.

* **Fail-To-Wire**: Ermöglicht eine physische Verbindung zwischen dem überbrückten Schnittstellenpaar, sodass der Datenverkehr SD-WAN Bypass und im Falle eines Neustarts oder Ausfalls der Appliance direkt über die Bridge fließen kann.

Früher wurde der DHCP-Client nur auf Fail-to-block-Port unterstützt. Mit der Version Citrix SD-WAN 11.2.0 wird die DHCP-Clientfunktion auf dem Fail-to-Wire-Port für den Zweigstandort mit seriellen Hochverfügbarkeitsbereitstellungen (HA) erweitert. Diese Erweiterung:

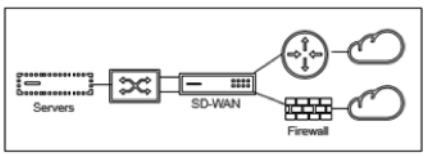
* Ermöglicht die DHCP-Clientkonfiguration für nicht vertrauenswürdige Schnittstellengruppe, die über Fail-to-Wire-Bridge-Paare und serielle HA-Bereitstellungen verfügt
* Ermöglicht die Auswahl von DHCP-Schnittstellen als Teil von privaten Intranet-WAN-Verbindungen.

> **Hinweise**
>
> * Die Inline-Option (Fail-to-Wire) ist nur auf Hardware-Appliances und nicht auf virtuellen Appliances (VPX/VPXL) verfügbar.
> * Der DHCP-Client wird nun auf dem privaten Intranetlink unterstützt.
> * Eine LAN-Schnittstelle darf nicht mit dem Fail-to-Wire-Paar verbunden werden, da Pakete zwischen den Schnittstellen überbrückt werden können.

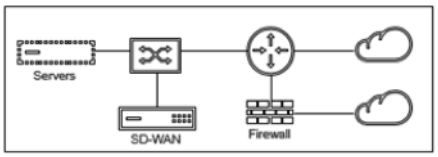


* **Fail-to-Block**: Diese Option deaktiviert die physische Verbindung zwischen den überbrückten Schnittstellenpaaren auf Hardware-Appliances und verhindert so, dass bei einem Neustart oder Ausfall der Appliance Datenverkehr über die Bridge fließt.

> **Hinweis**
>
> Inline (Fail-to-Block) ist die einzige Bridge-Modus-Option, die auf virtuellen Appliances (VPX/VPXL) verfügbar ist.



* **Virtuelles Inline (einarmig)**:



Wenn SD-WAN in diesem Modus bereitgestellt wird, verfügt es über einen **einzigen Arm**, der es mit dem WAN-Router, dem LAN und dem WAN verbindet, die dieselbe Schnittstelle auf SD-WAN teilen. Daher werden die Schnittstelleneinstellungen zwischen den LAN- und WAN-Verbindungen gemeinsam genutzt.

- **Schnittstellentyp:** Wählen Sie den Schnittstellentyp aus der Dropdownliste aus.
- **Sicherheit (vertrauenswürdig/nicht vertrauenswürdig)**: Gibt die Sicherheitsstufe der Schnittstelle an. Vertrauenswürdige Segmente werden durch eine Firewall geschützt.
- **Schnittstellenname:** Basierend auf dem ausgewählten Bereitstellungsmodus wird das Feld **Schnittstellenname** automatisch ausgefüllt.

Physische Schnittstelle

- **Schnittstelle wählen:** Wählen Sie den konfigurierbaren Ethernet-Port aus, der auf der Appliance verfügbar ist.

Virtuelles Interface

- **VLAN-ID**: Die ID zum Identifizieren und Markieren des Datenverkehrs zur und von der Schnittstelle.
- **Name der virtuellen Schnittstelle:** Basierend auf dem ausgewählten Bereitstellungsmodus wird das Feld **Name der virtuellen Schnittstelle** automatisch ausgefüllt.
- **HA Heartbeat**aktivieren: Aktivieren Sie die Synchronisierung von HA-Heartbeats über diese Schnittstelle. Diese Option ist aktiviert, wenn Sie eine sekundäre Appliance für HA konfiguriert haben. Wählen Sie diese Option, damit primäre und sekundäre Appliances die HA-Heartbeats über diese Schnittstelle synchronisieren können. Geben Sie die IP-Adresse der primären und sekundären Appliance an.
- **Routingdomäne**: Die Routingdomäne, die einen zentralen Verwaltungspunkt des Zweigstellennetzwerks oder eines Rechenzentrumsnetzwerks bereitstellt.
- **Firewallzonen**: Die Firewallzone, zu der die Schnittstelle gehört. Firewallzonen sichern und steuern die Schnittstellen in der logischen Zone.
- **Client-Modus:** Wählen Sie in der Dropdownliste **Client-Modus** aus. Bei Auswahl von PPPoE zeigt Static weitere Einstellungen an.

> **Hinweis**
>
> Wenn der Standortmodus (auf der Registerkarte Standortdetails) als **Verzweigung** und das **Feld Sicherheit** (auf der Registerkarte **Schnittstelle**) als **Nicht vertrauenswürdig**ausgewählt ist, ist die Option **PPPoE Dynamic** unter **Client-Modus**verfügbar.

Citrix SD-WAN fungiert als PPPoE-Client. Für IPv4 erhält SD-WAN die dynamische IPv4-Adresse oder verwendet die statische IPv4-Adresse. Für IPv6 bezieht es die lokale Linkadresse vom PPPoE-Server. Für die IPv6-Unicastadresse kann Static IP, DHCP oder SLAAC verwendet werden.

- **DHCP-Client**: Wenn diese Option auf den virtuellen Schnittstellen aktiviert ist, weist der DHCP-Server dem verbundenen Client dynamisch IPv4-Adressen zu.
- **DHCP-IPv6-Client**: Wenn diese Option auf den virtuellen Schnittstellen aktiviert ist, weist der DHCP-Server dem verbundenen Client dynamisch IPv6-Adressen zu.
- **SLAAC**: Diese Option ist nur für IPv6-Adressen verfügbar. Wenn diese Option ausgewählt ist, erhält die Schnittstelle IPv6-Adressen über Stateless Address Autokonfiguration (SLAAC).
- **Directed Broadcast**: Wenn das Kontrollkästchen **Directed Broadcast** aktiviert ist, werden die gerichteten Broadcasts an die virtuellen IP-Subnetze auf der virtuellen Schnittstelle gesendet.
- **Aktiviert**: Standardmäßig ist das Kontrollkästchen **Aktiviert** für alle virtuellen Schnittstellen aktiviert. Wenn Sie die virtuelle Schnittstelle deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Aktiviert** .

  > **Hinweis**
  >
  > - Das Kontrollkästchen **Aktiviert** ist nur ab Citrix SD-WAN Version 11.3.1 verfügbar.
  > - Die Option zum Deaktivieren einer virtuellen Schnittstelle ist nur verfügbar, wenn sie nicht von einem WAN Link Access Interface verwendet wird. Wenn die virtuelle Schnittstelle von einem WAN Link Access Interface verwendet wird, ist das Kontrollkästchen schreibgeschützt und standardmäßig aktiviert.
  > - Bei der Konfiguration anderer Funktionen zusammen mit aktivierten virtuellen Schnittstellen werden auch die deaktivierten virtuellen Schnittstellen aufgelistet, mit Ausnahme von **Access Interfaces** for a **WAN-Link**. Selbst wenn Sie eine deaktivierte virtuelle Schnittstelle auswählen, wird die virtuelle Schnittstelle nicht berücksichtigt und hat keine Auswirkungen auf die Netzwerkkonfiguration.

- **+ IPv4-Adresse**: Die virtuelle IPv4-Adresse und Netzmaske der Schnittstelle.
- **+ IPv6-Adresse**: Die virtuelle IPv6-Adresse und das Präfix der Schnittstelle.

- **Identität**: Wählen Sie eine Identität aus, die für IP-Dienste verwendet werden soll. Beispielsweise wird **Identität** als Quell-IP-Adresse für die Kommunikation mit BGP-Nachbarn verwendet.
- **Privat**: Wenn diese Option aktiviert ist, kann die virtuelle IP-Adresse nur auf der lokalen Appliance routingfähig sein.

> **Hinweis**
>
> - LTE-Ports unterstützen keine statischen IP-Adressen (IPv4 und IPv6).
> - LTE-Ports unterstützen sowohl DHCP als auch SLAAC. Die Konfiguration von DHCPv4 oder DHCPv6 ist obligatorisch. SLAAC ist optional.
> - In LTE-Ports können Link-Local-Adressen für IPv6 oder SLAAC konfiguriert werden.

PPPoE-Anmeldeinformationen

PPPoE (Point to Point Protocol over Ethernet) verbindet mehrere Computerbenutzer in einem Ethernet-LAN mit einem Remotestandort über gängige Appliances, z. B. Citrix SD-WAN. PPPoE ermöglicht Benutzern, eine gemeinsame DSL (Digital Subscriber Line), ein Kabelmodem oder eine drahtlose Verbindung zum Internet freizugeben. PPPoE kombiniert das Point-to-Point-Protokoll (PPP), das üblicherweise in DFÜ-Verbindungen verwendet wird, mit dem Ethernet-Protokoll, das mehrere Benutzer in einem LAN unterstützt. Die PPP-Protokollinformationen sind in einem Ethernet-Frame gekapselt.

Citrix SD-WAN-Appliances verwenden PPPoE, um ISP dabei zu unterstützen, im Gegensatz zu Wählverbindungen über laufende und kontinuierliche DSL- und Kabelmodemverbindungen zu verfügen. PPPoE bietet jeder Benutzer-Remotestandortsitzung die Möglichkeit, die Netzwerkadressen des anderen durch einen ersten Austausch namens “Discovery”zu erfahren. Nachdem eine Sitzung zwischen einem einzelnen Benutzer und dem Remotestandort, beispielsweise einem ISP-Anbieter, eingerichtet wurde, kann die Sitzung überwacht werden. Unternehmen nutzen gemeinsam genutzten Internetzugang über DSL-Leitungen mit Ethernet und PPPoE.

Citrix SD-WAN fungiert als PPPoE-Client. Für IPv4 erhält SD-WAN die dynamische IPv4-Adresse oder verwendet die statische IPv4-Adresse. Für IPv6 bezieht es die lokale Linkadresse vom PPPoE-Server. Für die IPv6-Unicastadresse kann Static IP, DHCP oder SLAAC verwendet werden.

Folgendes ist erforderlich, um erfolgreiche PPPoE-Sitzungen einzurichten:

- Konfigurieren Sie die virtuelle Netzwerkschnittstelle (VNI).
- Eindeutige Anmeldeinformationen für die Erstellung einer PPPoE-Sitzung.
- Konfigurieren Sie WAN-Verbindung. Für jedes VNI kann nur eine WAN-Verbindung konfiguriert sein.

- Konfigurieren Sie die virtuelle IP-Adresse. Jede Sitzung erhält eine eindeutige IP-Adresse, dynamisch oder statisch, basierend auf der bereitgestellten Konfiguration.
- Stellen Sie die Appliance im Bridge-Modus bereit, um PPPoE mit statischer IP-Adresse zu verwenden, und konfigurieren Sie die Schnittstelle als „vertrauenswürdig „
- Statische IP wird bevorzugt, um eine Konfiguration zu haben, um die vom Server vorgeschlagene IP zu erzwingen. Wenn sie sich von der konfigurierten statischen IP unterscheidet, kann ein Fehler auftreten.
- Stellen Sie die Appliance als Edge-Gerät bereit, um PPPoE mit dynamischer IP zu verwenden, und konfigurieren Sie die Schnittstelle als „nicht vertrauenswürdig „
- Unterstützte Authentifizierungsprotokolle sind PAP, CHAP, EAP-MD5, EAP-SRP.
- Die maximale Anzahl mehrerer Sitzungen hängt von der Anzahl der konfigurierten VNIs ab.
- Erstellen Sie mehrere VNIs zur Unterstützung mehrerer PPPoE-Sitzungen pro Schnittstellengruppe.

> **Hinweis:**
>
> Es dürfen mehrere VNIs mit demselben 802.1Q-VLAN-Tag erstellt werden.

Einschränkungen für die PPPoE-Konfiguration:

- 802.1q VLAN-Tagging wird nicht unterstützt.
- Die EAP-TLS-Authentifizierung wird nicht unterstützt.
- Adress-/Steuerungskomprimierung.
- Entleeren Sie die Kompression.
- Verhandlung über Protokoll-Feld-Komprimierung
- Protokoll zur Kompressionssteuerung.
- BSD Kompression komprimieren.
- IPX-Protokolle.
- PPP Multilink.
- TCP/IP-Header-Kompression im Van Jacobson-Stil.
- Verbindungs-ID-Komprimierungsoption bei der TCP/IP-Header-Komprimierung im Van Jacobson-Stil.
- PPPoE wird auf LTE-Schnittstellen nicht unterstützt.

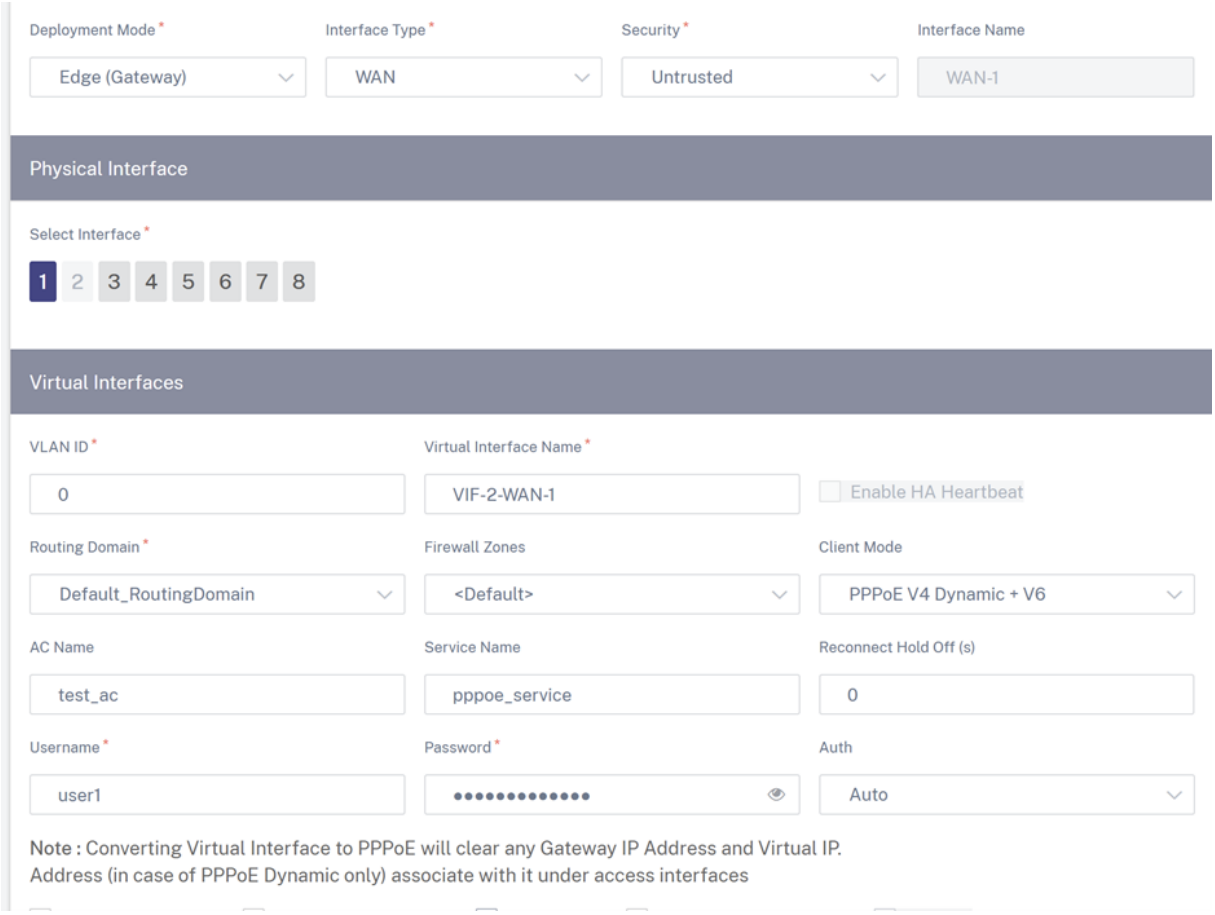
Ab der Citrix SD-WAN 11.3.1-Version wird ein zusätzlicher 8-Byte-PPPoE-Header für die Anpassung der TCP-Maximal-Segmentgröße (MSS) berücksichtigt. Der zusätzliche 8-Byte-PPPoE-Header passt den MSS in den Synchronisierungspaketen basierend auf der MTU an. Die unterstützte MTU reicht von 1280 Byte bis 1492 Byte.

PPPoE-Konfiguration Auf einem MCN können Sie nur statische PPPoE konfigurieren. In einer Zweigstelle können Sie entweder PPPoE statisch oder PPPoE dynamisch konfigurieren.

Um PPPoE zu konfigurieren, navigieren Sie auf Standortebene zur Registerkarte **Konfiguration > Standortkonfiguration > Schnittstellen** . Wählen Sie im Abschnitt **Virtuelle Schnittstellen** die entsprechende PPPoE-Option aus der Dropdown-Liste **Client-Modus** aus.

Hinweis

- Ein mit mehreren Schnittstellen konfiguriertes VNI kann nur eine Schnittstelle für PPPoE-Konnektivität verwenden.
- Wenn ein VNI, das mit mehreren Schnittstellen und einer PPPoE-Konnektivität konfiguriert ist, in eine andere Schnittstelle geändert wird, kann die Seite **Berichte > Echtzeit > PP-PoE** verwendet werden, um die bestehende Sitzung zu beenden und eine neue Sitzung zu starten. Die neue Sitzung kann dann über die neue Schnittstelle eingerichtet werden.
- Wenn PPPoE Dynamic ausgewählt ist, muss der VNI “Nicht vertrauenswürdig”sein.



- **AC-Name:** Geben Sie den Access Concentrator (AC) -Namen für die PPPoE-Konfiguration an.
- **Dienstname:** Geben Sie einen Dienstnamen ein.
- **Haltezeit erneut verbinden:** Geben Sie die Haltezeit für den Wiederverbindungsversuch ein.
- **Benutzername:** Geben Sie den Benutzernamen für die PPPoE-Konfiguration ein.
- **Passwort:** Geben Sie das Passwort für die PPPoE-Konfiguration ein.

- **Auth:** Wählen Sie das Autorisierungsprotokoll aus der Dropdownliste aus.
  - Wenn die Option **Auth** auf Auto gesetzt ist, berücksichtigt die SD-WAN-Appliance die vom Server empfangene unterstützte Authentifizierungsprotokollanforderung.
  - Wenn die Option **Auth** auf PAP/CHAP/EAP gesetzt ist, werden nur bestimmte Authentifizierungsprotokolle berücksichtigt. Wenn PAP in der Konfiguration ist und der Server eine Authentifizierungsanfrage mit CHAP sendet, wird die Verbindungsanforderung zurückgewiesen. Wenn der Server nicht mit PAP aushandelt, tritt ein Authentifizierungsfehler auf.

Pro statischem oder dynamischem PPPoE-VNI ist nur eine WAN-Link-Erstellung zulässig. Die WAN-Verbindungskonfiguration hängt von der VNI-Auswahl des Clientmodus ab.

Wenn der VNI mit dem dynamischen PPPoE-Clientmodus konfiguriert ist:

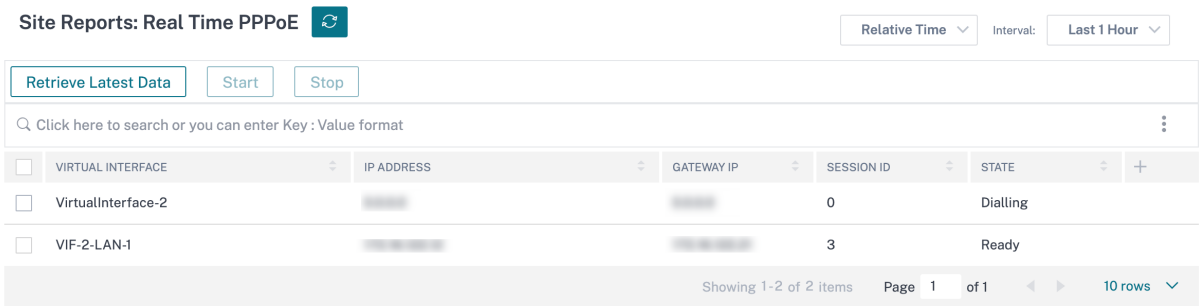
- IP-Adress- und Gateway-IP-Adressfelder werden inaktiv.
- Der virtuelle Pfadmodus ist auf “Primär”eingestellt.
- Proxy ARP kann nicht konfiguriert werden.

Standardmäßig ist Gateway MAC-Adressbindung ausgewählt.

Wenn das VNI mit dem statischen PPPoE-Client-Modus konfiguriert ist, konfigurieren Sie die IP-Adresse.

> **Hinweis:**
>
> Wenn der Server die konfigurierte statische IP-Adresse nicht berücksichtigt und eine andere IP-Adresse anbietet, tritt ein Fehler auf. Die PPPoE-Sitzung versucht, die Verbindung in regelmäßigen Abständen wiederherzustellen, bis der Server die konfigurierte IP-Adresse akzeptiert.

PPPoE-Überwachung und Fehlerbehebung Navigieren Sie auf Standortebene zum Abschnitt **Berichte > Echtzeit > PPPoE**, um Informationen zu den konfigurierten VNIs im statischen oder dynamischen PPPoE-Client-Modus anzuzeigen. Es ermöglicht Ihnen, die Sitzungen zur Fehlerbehebung manuell zu starten oder zu beenden.



Wenn es ein Problem beim Einrichten einer PPPoE-Sitzung gibt:

- Wenn Sie mit der Maus über den Status „Fehlgeschlagen“fahren, wird der Grund für den letzten Fehler angezeigt.
- Starten Sie die Sitzung neu, um eine neue Sitzung einzurichten oder um Probleme bei einer aktiven PPPoE-Sitzung zu beheben.
- Wenn eine PPPoE-Sitzung manuell beendet wird, kann sie erst gestartet werden, wenn sie manuell gestartet und eine Konfigurationsänderung aktiviert wurde oder der Dienst neu gestartet wurde.

Eine PPPoE-Sitzung kann aus folgenden Gründen fehlschlagen:

- Wenn SD-WAN sich aufgrund eines falschen Benutzernamen/Passworts in der Konfiguration nicht beim Peer authentifizieren kann.
- Die PPP-Verhandlung schlägt fehl - die Verhandlung erreicht nicht den Punkt, an dem mindestens ein Netzwerkprotokoll ausgeführt wird.
- Problem mit Systemspeicher oder Systemressourcen.
- Ungültig/schlechte Konfiguration (falscher AC-Name oder Dienstname).
- Die serielle Port konnte aufgrund eines Betriebssystemfehlers nicht geöffnet werden.
- Keine Antwort für die Echo-Pakete empfangen (Link ist fehlerhaft oder der Server reagiert nicht).
- Es gab mehrere ununterbrochene erfolglose Wählsitzungen in einer Minute.

Nach 10 aufeinanderfolgenden Ausfällen wird der Grund für das Scheitern beobachtet.

- Wenn der Fehler normal ist, wird er sofort neu gestartet.
- Wenn der Fehler ein Fehler ist, wird der Neustart für 10 Sekunden zurückgesetzt.
- Wenn der Fehler schwerwiegend ist, wird der Neustart vor dem Neustart für 30 Sekunden zurückgesetzt.

LCP-Echo-Anforderungspakete werden alle 60 Sekunden von SD-WAN generiert, und das Nichtempfangen von 5 Echoantworten wird als Verbindungsfehler angesehen und stellt die Sitzung wieder her.

- Wenn der VNI betriebsbereit ist, zeigen die IP- und Gateway-IP-Spalten die aktuellen Werte in der Sitzung an. Es zeigt an, dass es sich um kürzlich empfangene Werte handelt.
- Wenn der VNI angehalten ist oder sich im Status „Fehlgeschlagen“befindet, sind die Werte die zuletzt empfangenen Werte.
- Wenn Sie den Mauszeiger über die Spalte Gateway-IP bewegen, wird die MAC-Adresse des PPPoE Access Concentrators angezeigt, von dem die Sitzung und die IP empfangen werden.
- Wenn Sie mit der Maus über den Wert „state“fahren, wird eine Meldung angezeigt, die für einen Status „Failed“nützlicher ist.

PPPoE-Sitzungstyp	Status-Farbe	Beschreibung
Konfiguriert	Gelb	Ein VNI ist mit PPPoE konfiguriert. Dies ist ein Ausgangszustand.
Dialing	Gelb	Nachdem ein VNI konfiguriert wurde, wechselt der PPPoE-Sitzungsstatus in den Wählzustand, indem die PPPoE-Erkennung gestartet wird. Paketinformationen werden erfasst.
Sitzungsfortbestehen	Gelb	VNI wird vom Discovery-Status in den Sitzungsstatus verschoben und wartet auf den Empfang der IP, wenn es dynamisch ist, oder wartet auf Bestätigung vom Server für die angekündigte IP, falls statisch.
Bereit	Grün	IP-Pakete werden empfangen und die VNI und die zugehörige WAN-Verbindung sind einsatzbereit.
Fehlgeschlagen	Rot	PPP/PPPoE-Sitzung wird beendet. Der Grund für den Fehler kann eine ungültige Konfiguration oder ein schwerwiegender Fehler sein. Die Sitzung versucht nach 30 Sekunden wieder eine Verbindung herzustellen.
Beendet	Gelb	PPP/PPPoE-Sitzung wird manuell gestoppt.

PPPoE-Sitzungstyp	Status-Farbe	Beschreibung
Kündigung	Gelb	Ein Zwischenzustand, der aus einem bestimmten Grund endet. Dieser Zustand beginnt automatisch nach einer bestimmten Dauer (5 Sekunden für normalen Fehler oder 30 Sekunden für einen schwerwiegenden Fehler).
Deaktiviert	Gelb	Der SD-WAN-Dienst ist deaktiviert.

Die Datei *SDWAN_ip_learned.log* enthält Protokolle, die sich auf PPPoE beziehen. Navigieren Sie zu **Fehlerbehebung > Geräteprotokolle**, um die Datei *SDWAN_ip_learned.log* anzuzeigen oder herunterzuladen.

Kabelgebundene 802.11x-Konfiguration

Wired 802.1X ist ein Authentifizierungsmechanismus, bei dem sich Clients authentifizieren müssen, bevor sie auf die LAN-Ressourcen zugreifen können. Der Citrix SD-WAN Orchestrator-Service unterstützt die Konfiguration der kabelgebundenen 802.1X-Authentifizierung auf LAN-Schnittstellen.

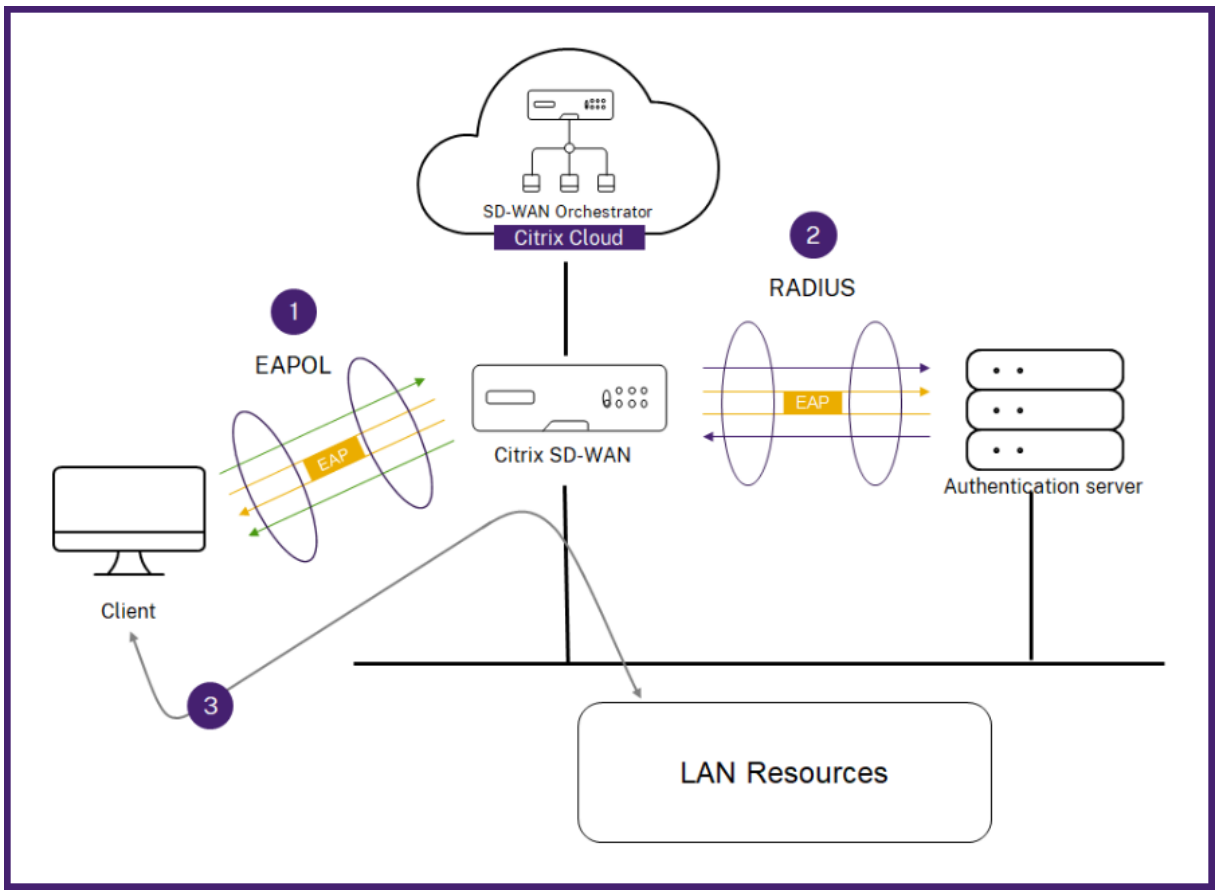
Im Citrix SD-WAN-Netzwerk senden die Clients Authentifizierungsanfragen an die Citrix SD-WAN Appliance, um auf die LAN-Ressourcen zuzugreifen. Die Citrix SD-WAN Appliance fungiert als Authentifikator und sendet die Authentifizierungsanfragen an den Authentifizierungsserver. Der Citrix SD-WAN Orchestrator-Service unterstützt nur RADIUS-Server, die als Authentifizierungsserver konfiguriert werden.

Bei der ersten Authentifizierung können nur EAPOL-Pakete oder DHCP-Pakete verarbeitet werden, die die 802.1X-Authentifizierung über das standardmäßige virtuelle LAN initialisieren können. Ein neu verbundener Client muss innerhalb von 90 Sekunden authentifiziert werden. Wenn die Authentifizierung erfolgreich ist, erhält sie Zugriff auf die LAN-Ressourcen.

Wenn die Authentifizierung fehlschlägt, erhält der Client keinen Netzwerkzugriff und alle Pakete werden verworfen. Die Clients, die direkt mit der Citrix SD-WAN-Appliance verbunden sind, können die Authentifizierung erneut versuchen, indem sie das Ethernet-Kabel abziehen und erneut einsetzen. Optional können Sie ein bestimmtes virtuelles LAN definieren, um Zugriff auf eingeschränkte LAN-Ressourcen für die fehlgeschlagenen Authentifizierungsanforderungen zu gewähren. In solchen Fällen erhalten die fehlgeschlagenen Authentifizierungsanforderungen Zugriff auf das angegebene

virtuelle LAN. Sie können den Zugriff auf den authentifizierten Datenverkehr mithilfe verschiedener Routingdomänen oder Firewallzonen einschränken, während Sie das virtuelle LAN erstellen.

> **Hinweis**
>
> - Im standardmäßigen virtuellen LAN muss immer 802.1X aktiviert sein.
> - Dynamische virtuelle LANs werden nicht unterstützt.



Die Citrix SD-WAN-Appliance erwartet den Empfang von Paketen ohne 802.1Q-Tag (Pakete ohne Tags). Wenn die Citrix SD-WAN-Appliance ein Paket mit einem 802.1Q-Tag empfängt, das auf das zugewiesene virtuelle LAN festgelegt ist, müssen alle vom MAC stammenden Pakete markiert werden. Wenn ein Paket ohne 802.1Q-Tag im Header oder mit einem anderen Tag als dem virtuellen LAN empfangen wird, zu dem die MAC-Adresse gehört, wird das Paket verworfen.

Wenn mehrere Clients, die mit einem Switch verbunden sind, versuchen, sich gleichzeitig über einen einzigen Port zu authentifizieren, wird jeder Client einzeln authentifiziert, bevor er Zugriff auf die LAN-Ressourcen erhalten kann. Die Clients, die sich nicht authentifizieren können, können die Authentifizierung erneut versuchen, indem sie das Ethernet-Kabel abziehen, 3 Minuten warten und das Ethernet-Kabel erneut einstecken. Die Plattformen Citrix SD-WAN 110, 210 und 410 unterstützen maximal 32 Clients (sowohl authentifizierte als auch nicht authentifizierte). Alle anderen Plattformen un-

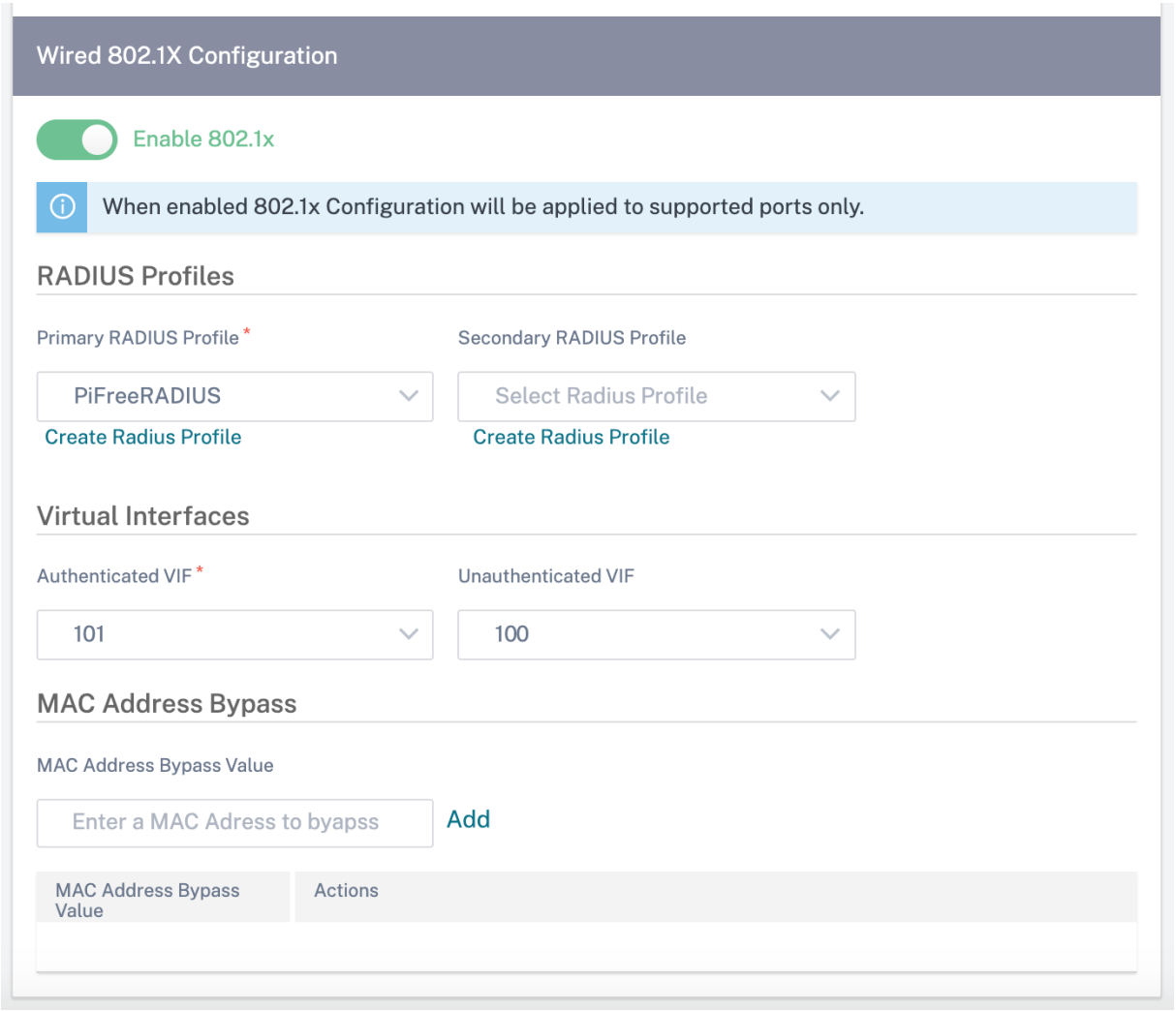
terstützen maximal 64 Clients (sowohl authentifizierte als auch nicht authentifizierte).

Um die 802.1X-Authentifizierung zu konfigurieren, navigieren Sie zu **Standortkonfiguration > Schnittstellen**, und **aktivieren Sie die Umschaltfläche 802.1x-Aktivierung** . Wählen Sie ein vorhandenes RADIUS-Profil aus oder klicken Sie auf **RADIUS-Profil** erstellen, um ein RADIUS-Profil Einzelheiten zum Erstellen eines RADIUS-Profils finden Sie unter RADIUS-Serverprofile. Sie können dieselben RADIUS-Profile für die kabelgebundene 802.1x- und die drahtlose WPA2-Enterprise-Authentifizierung verwenden, vorausgesetzt, Ihre Appliance unterstützt Wireless WPA2-Enterprise.

Wählen Sie in der Dropdownliste **Authentifizierte VIF** eine virtuelle Schnittstelle aus. Die ausgewählte virtuelle Schnittstelle gewährt Zugriff auf die LAN-Ressourcen für erfolgreiche Authentifizierungsanforderungen.

Optional können Sie eine Schnittstelle aus der Dropdown-Liste **Nicht authentifizierte VIF** auswählen. Die ausgewählte virtuelle Schnittstelle gewährt Zugriff auf eine bestimmte LAN-Ressource für die fehlgeschlagenen authentifizierten Anforderungen.

Sie können eine Liste von MAC-Adressen hinzufügen, die den Authentifizierungsprozess umgeht. Datenverkehr von diesen MAC-Adressen wird implizit als authentifiziert behandelt. Diese MAC-Adressen sind anfällig für böswillige Angriffe. Verwenden Sie diese Funktion daher nur in physisch sicheren Umgebungen und für Legacy-Hardware, die keine kabelgebundene 802.1x-Authentifizierung unterstützt.



Sie können die Warnungen im Zusammenhang mit kabelgebundenen 802.1x-Authentifizierungsanforderungen unter **Berichte > Warnungen anzeigen**. Weitere Informationen finden Sie unter Warnmeldungen.

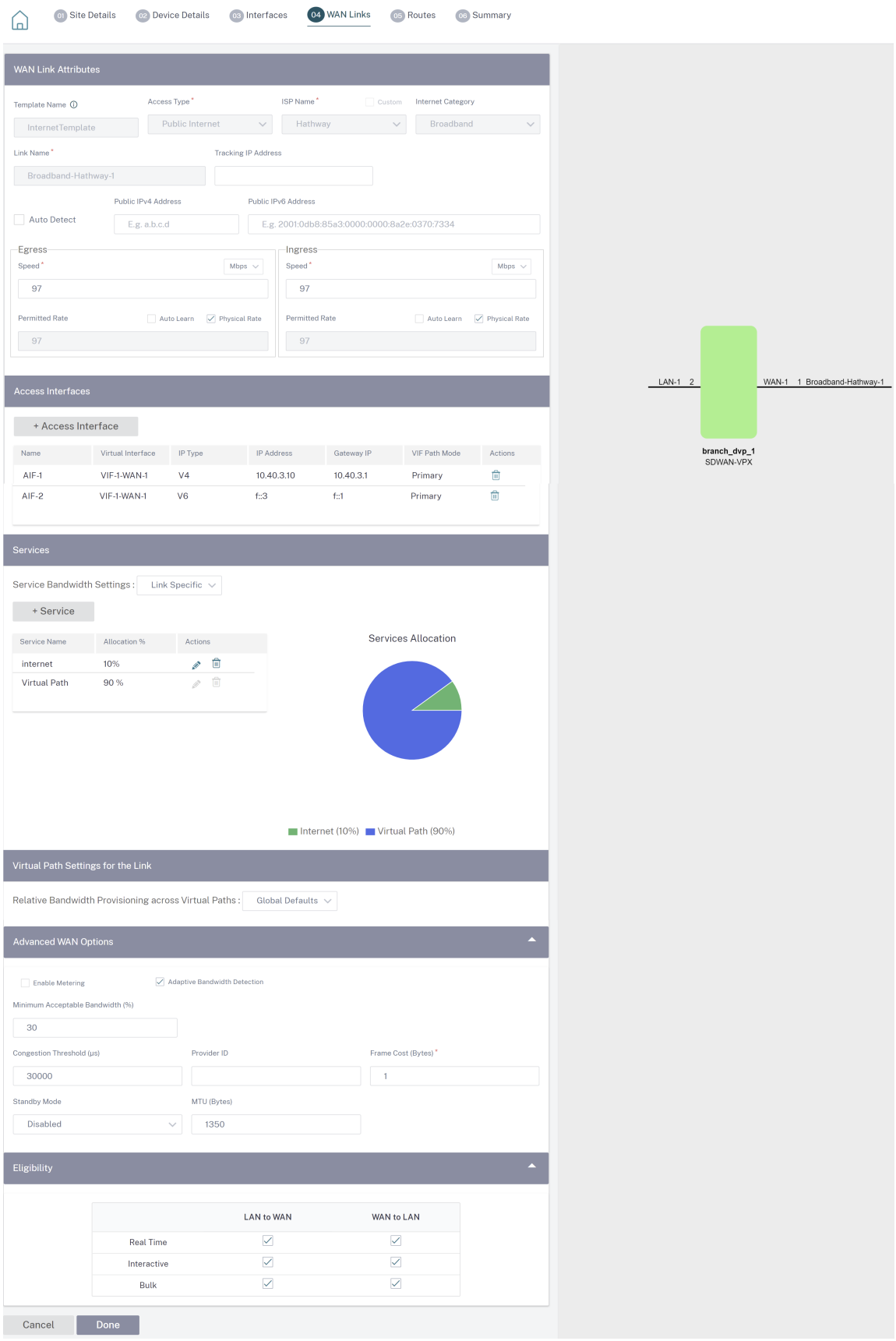
WAN-Links

Der nächste Schritt ist die Konfiguration von WAN-Verbindungen. Klicken Sie auf **+ WAN Link**, um die Konfiguration einer WAN-Verbindung zu starten.

Die WAN-Link-Konfiguration umfasst das Einrichten des WAN-Link-Zugriffstyps und der Attribute der

Sie können das **WAN-Link-Attribut** von Grund auf neu konfigurieren oder eine WAN-Link-Vorlage verwenden, um WAN-Link-Attribute schnell zu konfigurieren. Wenn Sie bereits ein Standortprofil verwendet haben, werden die **WAN-Link-Attribute** automatisch ausgefüllt.

WAN-Link-Attribute



- **Vorlagenname**: Der Name der WAN-Link-Vorlage, die zum Erstellen der WAN-Verbindung verwendet wird. Der Name der WAN-Link-Vorlage kann nach dem Erstellen von WAN-Links nicht geändert werden. Sobald WAN-Verbindungen mithilfe einer WAN-Link-Vorlage erstellt wurden, können Sie den Zugriffstyp, den ISP-Namen oder die Internetkategorie nicht mehr bearbeiten.
- **Zugriffstyp**: Gibt den WAN-Verbindungstyp der Verbindung an.
  - **Öffentliches Internet**: Zeigt an, dass der Link über einen ISP mit dem Internet verbunden ist.
  - **Privates Intranet**: Gibt an, dass der Link mit einem oder mehreren Standorten innerhalb des SD-WAN-Netzwerks verbunden ist und keine Verbindung zu Standorten außerhalb des SD-WAN-Netzwerks herstellen kann.
  - **MPLS**: Spezialisierte Variante von Private Intranet. Gibt an, dass die Verbindung ein oder mehrere DSCP-Tags verwendet, um die Quality of Service zwischen zwei oder mehr Punkten in einem Intranet zu steuern, und dass keine Verbindung zu Standorten außerhalb des SD-WAN-Netzwerks hergestellt werden kann.
- **ISP-Name**: Der Name des Dienstanbieters.
- **Internetkategorie**: Die Art des WAN-Link-Internetzugangstechnologiedienstes (Breitband, Satellit, Glasfaser, LTE usw.), der auf der WAN-Verbindung aktiviert ist.
- **Linkname**: Automatisch ausgefüllt basierend auf den vorherigen Eingaben.
- **Tracking-IP-Adresse: Die**virtuelle IP-Adresse auf dem virtuellen Pfad, an die ein Ping gesendet werden kann, um den Status des Pfads zu ermitteln.
- **Öffentliche IPv4-Adresse** und **öffentliche IPv6-Adresse: Die**IP-Adresse des NAT- oder DNS-Servers. Diese Adresse ist nur anwendbar und offengelegt, wenn der Zugriffstyp für WAN-Verbindungen Public Internet oder Privates Intranet in der Serial HA-Bereitstellung ist. Öffentliche IP-Adressen können entweder manuell konfiguriert oder mithilfe der Option Auto Learn automatisch erlernt werden.
- **Automatische Erkennung**: Wenn diese Option aktiviert ist, erkennt die SD-WAN-Appliance automatisch die öffentliche IP-Adresse. Diese Option ist nur verfügbar, wenn es sich bei der Geräterolle um einen **Zweig** und nicht um den **Master Control Node (MCN)**handelt.
- **Ausgangsgeschwindigkeit**: Die Geschwindigkeit von WAN zu LAN.
  - **Geschwindigkeit**: Die verfügbare oder zulässige Geschwindigkeit des WAN-zu-LAN-Datenverkehrs in Kbit/s oder Mbit/s.
  - **Zulässige Rate**: In Fällen, in denen die gesamte WAN-Link-Kapazität nicht von der SD-WAN-Appliance genutzt werden soll, ändern Sie die zulässige Rate entsprechend.
  - **Automatisches Lernen**: Wenn Sie sich über die Bandbreite nicht sicher sind und die Links nicht zuverlässig sind, können Sie die Funktion Auto Learn aktivieren. Die Auto-Learn-Funktion lernt nur die zugrunde liegende Linkkapazität und verwendet in Zukunft denselben Wert.
  - **Physische Rate**: Die tatsächliche Bandbreitenkapazität der WAN-Verbindung.

- **Eingangsgeschwindigkeit**: Die LAN-zu-WAN-Geschwindigkeit.
  - **Geschwindigkeit**: Die verfügbare oder zulässige Geschwindigkeit des LAN-zu-WAN-Datenverkehrs in Kbit/s oder Mbit/s.
  - **Zulässige Rate**: In Fällen, in denen die gesamte LAN-Verbindungskapazität nicht von der SD-WAN-Appliance genutzt werden soll, ändern Sie die zulässige Rate entsprechend.
  - **Automatisches Lernen**: Wenn Sie sich über die Bandbreite nicht sicher sind und die Links nicht zuverlässig sind, können Sie die Funktion Auto Learn aktivieren. Die Auto-Learn-Funktion lernt nur die zugrunde liegende Linkkapazität und verwendet in Zukunft denselben Wert.
  - **Physikalische Rate**: Die tatsächliche Bandbreitenkapazität der LAN-Verbindung.

MPLS-Warteschlangen

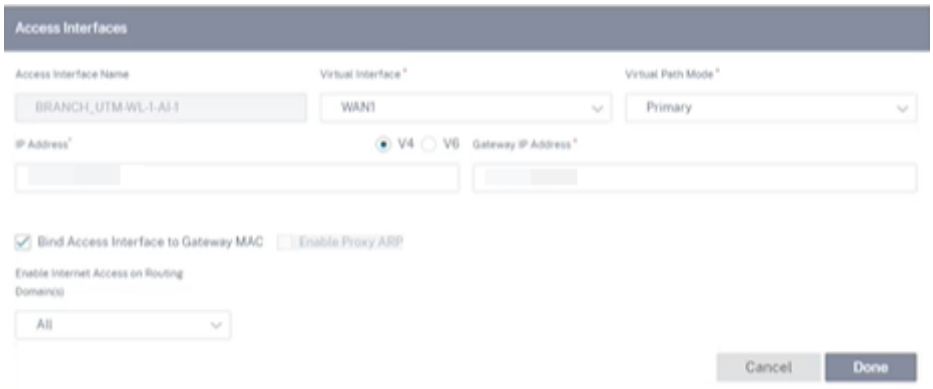
Die **MPLS-Warteschlangeneinstellungen** sind nur für den WAN-Link-Zugriffstyp MPLS verfügbar. Diese Option soll die Definition von Warteschlangen aktivieren, die den MPLS-Warteschlangen des Service Providers auf dem MPLS-WAN-Link entsprechen. Informationen zum Hinzufügen von MPLS-Warteschlangen finden Sie unter MPLS-Warteschlangen.

Access Interface

Ein Access Interface definiert die IP-Adresse und die Gateway-IP-Adresse für einen WAN-Link. Für jeden WAN-Link ist mindestens ein Access Interface erforderlich. Im Folgenden sind die Parameter für das Access Interface aufgeführt:

- **Name der Zugriffsschnittstelle**: Der Name, mit dem auf die Access-Schnittstelle verwiesen wird. Die Standardeinstellung verwendet die folgende Benennungskonvention: WAN_link_name-AI-number: Wobei WAN_link_name der Name der WAN-Verbindung ist, die Sie dieser Schnittstelle zuordnen, und “number”ist die Anzahl der derzeit für diese Verbindung konfigurierten Access Interfaces, erhöht um 1.
- **Virtuelle Schnittstelle**: Die virtuelle Schnittstelle, die das Access Interface verwendet. Wählen Sie einen Eintrag aus dem Dropdown-Menü von Virtuelle Interfaces aus, das für die aktuelle Zweigstelle konfiguriert ist.
- **Virtueller Pfadmodus**: Gibt die Priorität für den Virtual Path-Datenverkehr auf der aktuellen WAN-Verbindung an. Die Optionen sind: Primär, Sekundäroder Ausschließen. Wenn auf Exclude festgelegt ist, wird das Access Interface nur für Internet- und Intranetdatenverkehr verwendet.
- **IP-Adresse: Die**IP-Adresse für den Access Interface-Endpunkt von der Appliance zum WAN. Wählen Sie nach Bedarf V4 (IPv4) oder V6 (IPv6) aus.
- **Gateway-IP-Adresse**: Die IP-Adresse für den Gateway-Router.

- **Zugangsschnittstelle an Gateway-MAC binden**: Wenn aktiviert, muss die Quell-MAC-Adresse von Paketen, die über Internet- oder Intranetdienste empfangen werden, mit den Gateway-MAC-AddressWank-Links > Erweiterte WAN-Optionen
- **Proxy-ARP aktivieren**: Wenn diese Option aktiviert ist, antwortet die virtuelle WAN-Appliance auf ARP-Anforderungen für die Gateway-IP-Adresse, wenn das Gateway nicht erreichbar ist.
- **Internetzugriff auf Routingdomänen aktivieren**: Erstellt automatisch eine DEFAULT-Route (0.0.0.0/0) in allen Routingtabellen der jeweiligen Routingdomänen. Sie können für alle Routingdomänen oder keine aktivieren. Es vermeidet die Notwendigkeit, eine exklusive statische Route für alle Routingdomänen zu erstellen, wenn sie einen Internetzugang benötigen.



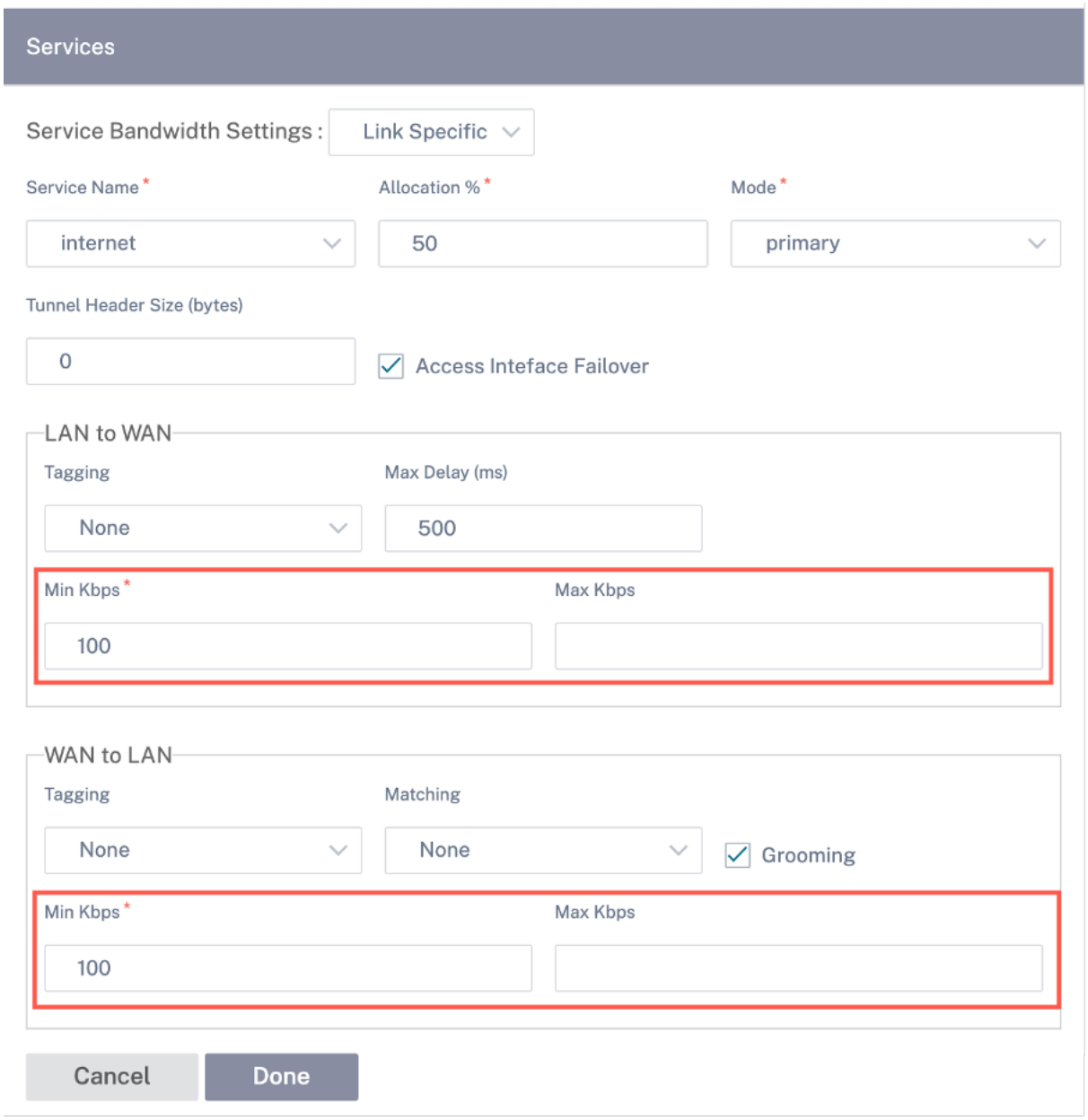
Services

Im Abschnitt **Dienste** können Sie Diensttypen hinzufügen und den Prozentsatz der Bandbreite zuweisen, der für jeden Diensttyp verwendet werden soll. Sie können die Diensttypen definieren und Attribute dafür im Abschnitt Delivery Services konfigurieren. Sie können diese globalen Standardeinstellungen verwenden oder in der Dropdown-Liste Dienstbandbreiteneinstellungen verbindungsspezifische **Einstellungen für die Dienstbandbreite** konfigurieren. Wenn Sie Linkspezifisch wählen, geben Sie die folgenden Details ein:

- **Dienstname**: Der Name des WAN-Link-Dienstes.
- **Zuweisung%**: Der garantierte faire Anteil der Bandbreite, der dem Dienst aus der Gesamtkapazität der Verbindung zugewiesen wurde.
- **Modus**: Der Betriebsmodus des WAN-Links, basierend auf dem ausgewählten Dienst. Für das Internet gibt es eine von Primary, Secondary und Balance und für Intranet gibt es Primär und Sekundär.
- **Tunnel-Header-Größe**: Die Größe des Tunnel-Headers in Byte.
- **LAN-zu-WAN-Tag**: Das DHCP-Tag, das auf LAN-zu-WAN-Pakete im Dienst angewendet werden soll.
- **LAN-zu-WAN-Verzögerung**: Die maximale Zeit zum Puffern von Paketen, wenn die Bandbreite der WAN-Links überschritten wird.

- **Min. Kbit/s von LAN zu WAN**: Der minimale Wert für die Upload-Bandbreite, der für den Dienst reserviert ist. Das **Min-Kbps** ist ein Pflichtfeld.
- **Max. Kbit/s von LAN zu WAN**: Der maximale Wert für die Upload-Bandbreite, der für den Dienst reserviert ist. Das Feld **Max. Kbps** ist optional und der Wert darf nicht kleiner als der konfigurierte Mindestwert für die Upload-Bandbreite sein. Der Wert muss größer oder gleich dem Mindestwert für die Upload-Bandbreite sein.
- **WAN-zu-LAN-Tag**: Das DHCP-Tag, das auf WAN-zu-LAN-Pakete im Dienst angewendet werden soll.
- **WAN-zu-LAN-Übereinstimmung**: Die Übereinstimmungskriterien für Internet-WAN-LAN-Pakete, die dem Dienst zugewiesen werden sollen.
- **Min. Kbps von WAN zu LAN**: Der Mindestwert für die Download-Bandbreite, der für den Dienst reserviert ist. Das **Min-Kbps** ist ein Pflichtfeld.
- **Max. Kbps von WAN zu LAN**: Der maximale Wert für die Download-Bandbreite, der für den Dienst reserviert ist. Das Feld **Max. Kbps** ist optional und der Wert darf nicht kleiner als der konfigurierte Mindestwert für die Downloadbandbreite sein. Der Wert muss größer oder gleich dem Mindestwert für die Download-Bandbreite sein.
- **WAN-zu-LAN-Optimierung: Wenn**diese Option aktiviert ist, werden Pakete nach dem Zufallsprinzip verworfen, um zu verhindern, dass der WAN-zu-LAN-Datenverkehr die vom Dienst bereitgestellte Bandbreite überschreitet.

> **Hinweis**
>
> Die minimalen und maximalen Kbit/s-Felder sind für den virtuellen Pfad nicht verfügbar.



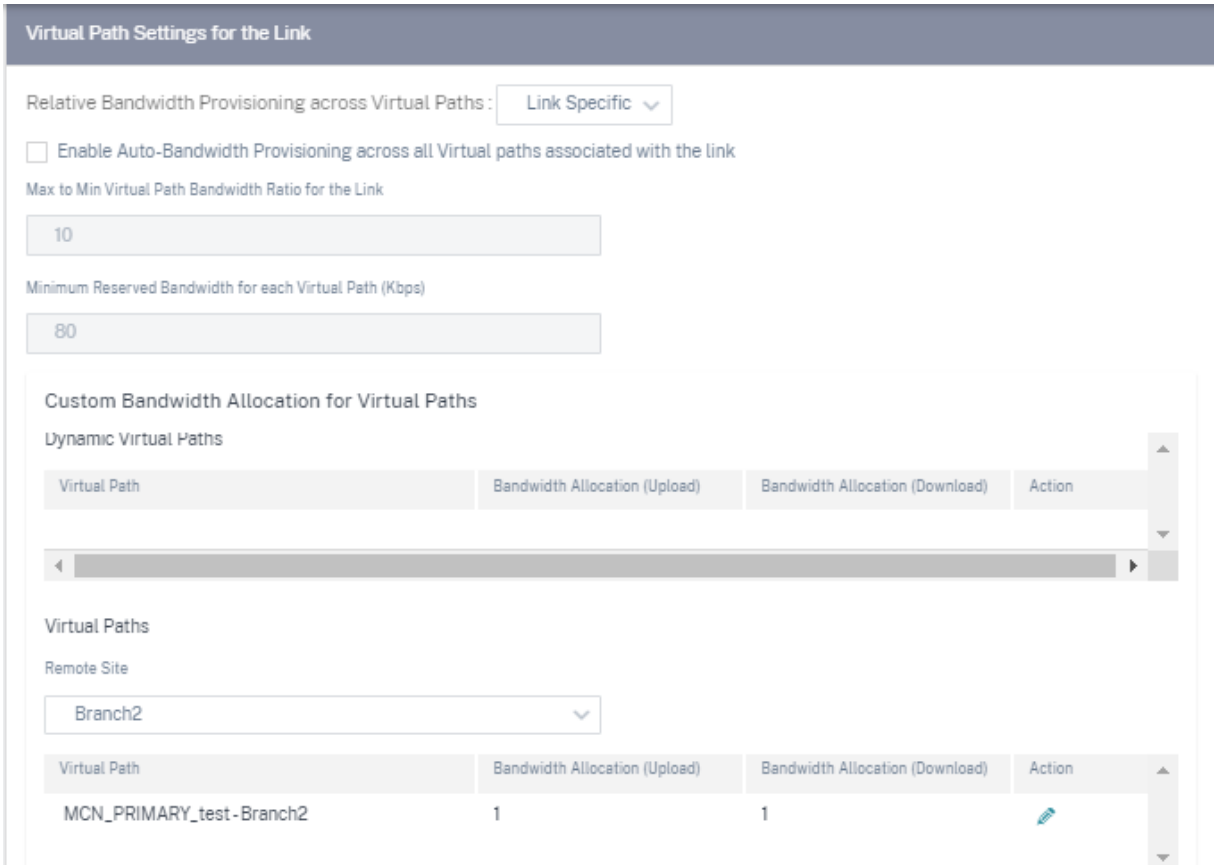
Virtuelle Pfadeinstellungen für den Link

Wählen Sie die relative Bandbreitenbereitstellung über virtuelle Pfade hinweg je nach Bedarf als **Global Default** oder **Linkspezifisch** aus. Wenn Sie **Verbindungsspezifisch**auswählen und die automatische Bandbreitenbereitstellung aktivieren, wird der Anteil der Bandbreite für den virtuellen Pfaddienst automatisch berechnet und entsprechend der Bandbreite angewendet, die möglicherweise von Remotestandorten verbraucht wird.

- **Max zu Min. Bandbreitenverhältnis des virtuellen Pfades für den Link**: Sie können das maximale zu minimale virtuelle Pfadverhältnis festlegen, das auf die ausgewählte WAN-Verbindung

angewendet werden kann.

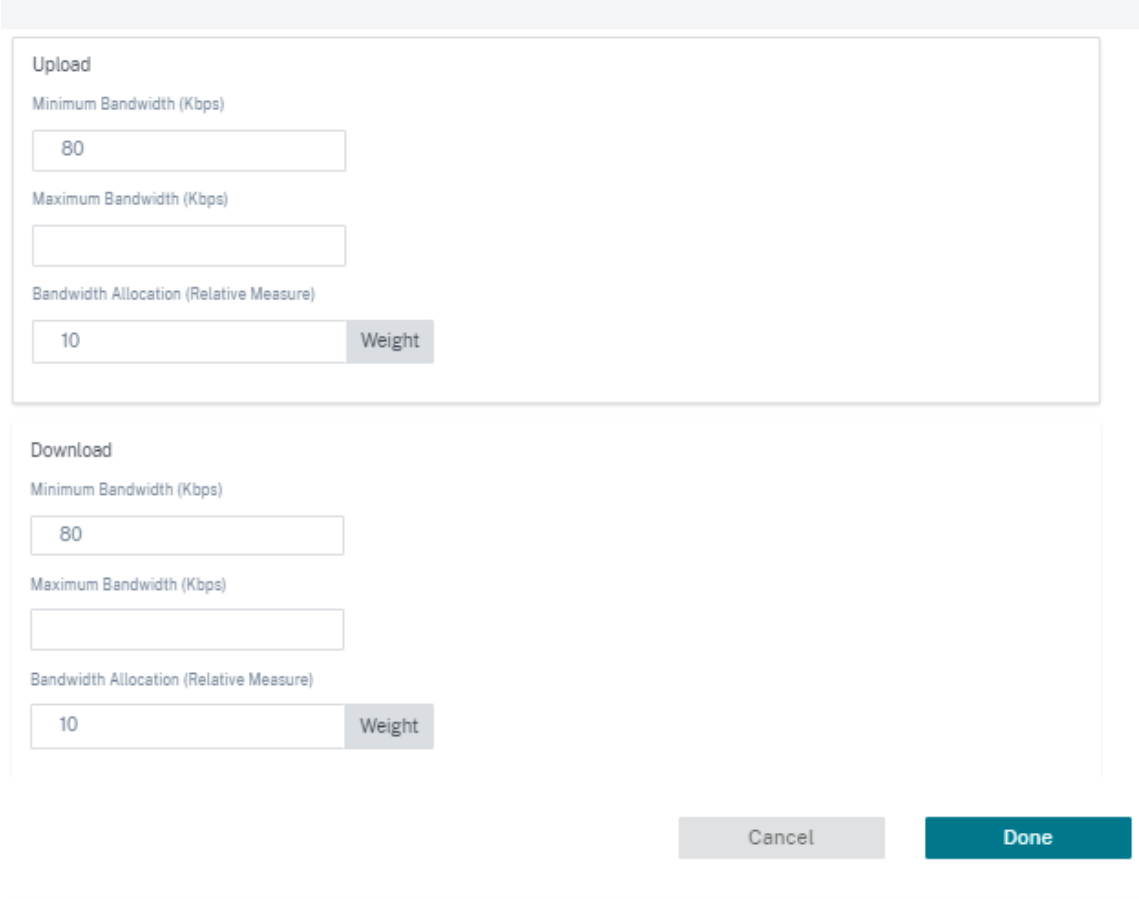
- **Mindestreservierte Bandbreite für jeden virtuellen Pfad (Kbit/s)**: Sie können den Mindestwert für die reservierte Bandbreite in Kbit/s für jeden virtuellen Pfad festlegen.



So passen Sie die Bandbreiten für die virtuellen Pfade an, die einer WAN-Verbindung zugeordnet sind:

1. **Deaktivieren Sie das Kontrollkästchen Automatische Bandbreitenbereitstellung über alle virtuellen Pfade hinweg aktivieren, die mit dem Link verknüpft sind** .
2. Wählen Sie im Abschnitt **Benutzerdefinierte Bandbreitenzuweisung für virtuelle Pfade** eine Remote-Site aus. Sie können Bandbreiten für die virtuellen Pfade zur Remote-Site bereitstellen.
    - **Minimale Bandbreite (Kbit/s)**: Die Mindestbandbreite, die für den virtuellen Pfad reserviert ist. Die Mindestbandbreite, die Sie für einen virtuellen Pfad festlegen können, beträgt 80 Kbps.
    - **Maximale Bandbreite (Kbit/s)**: Die maximale Bandbreite, die der virtuelle Pfad über die WAN-Verbindung nutzen kann. Wenn die maximale Bandbreite nicht festgelegt ist, nutzt die Site die gesamte verfügbare Bandbreite.
    - **Bandbreitenzuweisung (relative Kennzahl)**: Die Bandbreitenfreigabe, die einem virtuellen Pfad aus der berechtigten Bandbreite seiner Gruppe zugewiesen wurde. Wenn

beispielsweise eine WAN-Verbindungsgruppe aus 3 virtuellen Pfaden für eine Bandbreite von 30 Mbit/s geeignet ist und Sie jedem virtuellen Pfad die gleiche Bandbreite zuweisen möchten, aktualisieren Sie 10 als Bandbreitenzuweisung am Remotestandort.



3. Klicken Sie auf **Fertig**.

> **Hinweis**
>
> Der Citrix SD-WAN Orchestrator Service behält die zuvor konfigurierten benutzerdefinierten Bandbreiteneinstellungen bei, auch nachdem die zuvor konfigurierten dynamischen virtuellen Pfade zwischen zwei Standorten deaktiviert wurden. Achten Sie darauf, die benutzerdefinierten Bandbreiteneinstellungen manuell zu aktualisieren, wenn Sie die dynamischen virtuellen Pfade neu konfigurieren.

Zu berücksichtigende Punkte für die Bereitstellung von Bandbreite

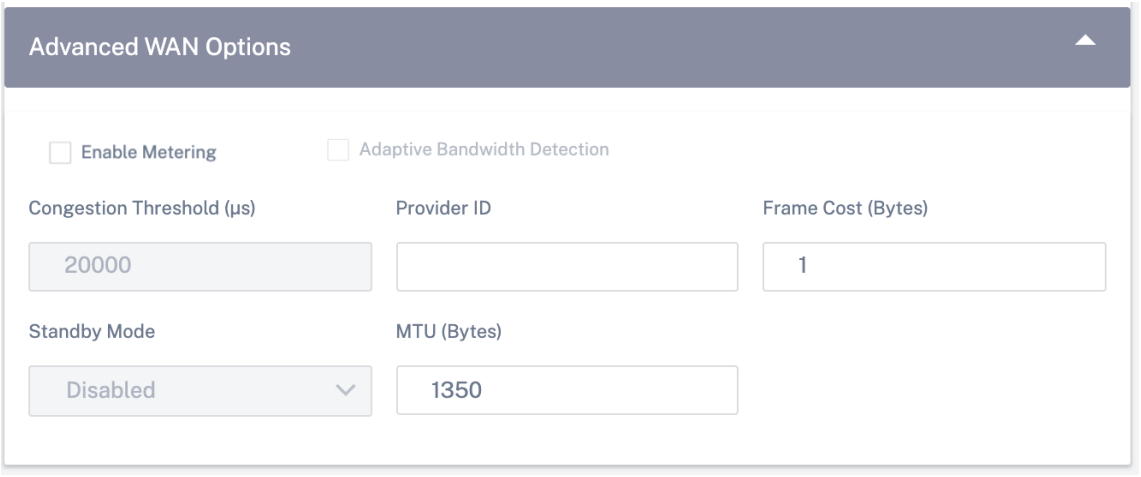
- Standardmäßig erhalten alle Filialen und WAN-Dienste (Virtual Path/Internet/Intranet) eine Gewichtung von jeweils 1.
- Eine Anpassung der Bandbreite ist erforderlich, wenn es große Unterschiede in Bezug auf den Bandbreitenbedarf gibt.

- Wenn dynamische virtuelle Pfade zwischen den verfügbaren Standorten aktiviert sind, wird die WAN-Link-Kapazität zwischen dem statischen virtuellen Pfad zum Datencenter und den dynamischen virtuellen Pfaden gemeinsam genutzt.

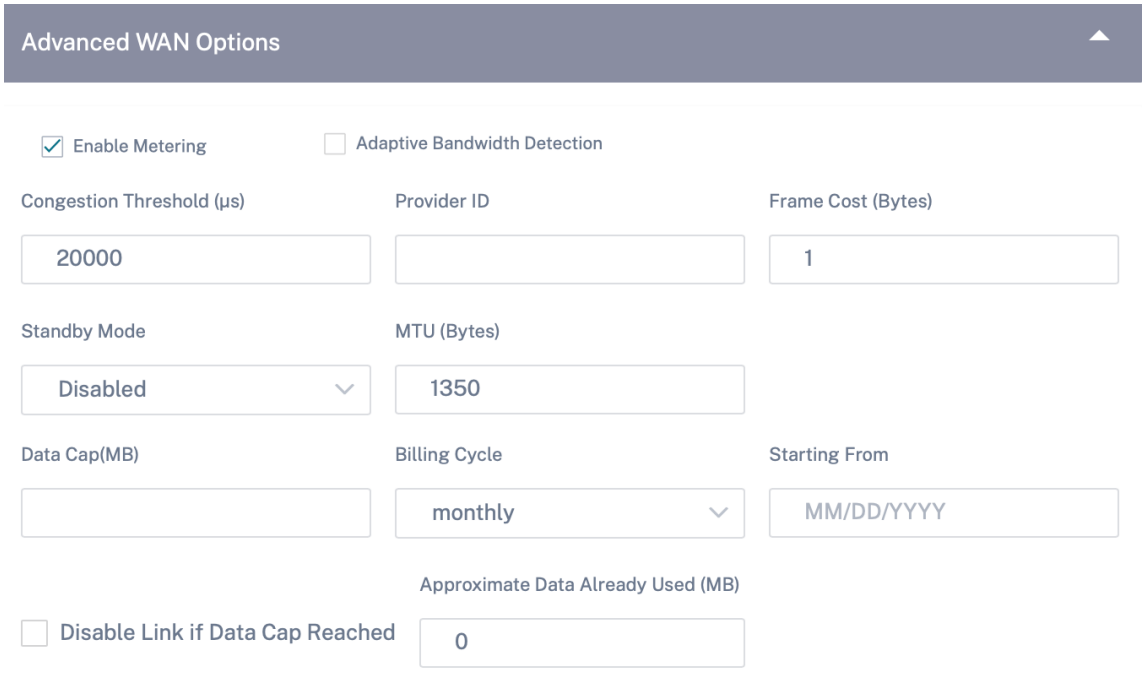
Erweiterte WAN-Optionen

Die erweiterten WAN-Link-Einstellungen ermöglichen die Konfiguration der **ISP-spezifischen** Attribute.

- **Überlastungsschwelle**: Die Menge der Überlastung, nach der die WAN-Verbindung die Paketübertragung drosselt, um weitere Staus zu vermeiden.
- **Provider-ID**: Eindeutige Kennung für den Anbieter zur Unterscheidung von Pfaden beim Senden doppelter Pakete.
- **Rahmenkosten (Byte)**: Zusätzliche Header/Trailer-Bytes werden zu jedem Paket hinzugefügt, z. B. für Ethernet-IPG- oder AAL5-Trailer.
- **MTU (Byte)**: Die größte Rohpaketgröße in Byte, ohne die Rahmenkosten.
- **Standby-Modus**: Eine Standby-Verbindung wird nicht verwendet, um Benutzerverkehr zu übertragen, es sei denn, sie wird aktiv. Der Standby-Modus einer WAN-Verbindung ist standardmäßig deaktiviert. Weitere Informationen zum Standby-Modus finden Sie unter Standby-Modus.



- **Metering aktivieren**: Verfolgt die Nutzung einer WAN-Verbindung und warnt den Benutzer, wenn die Verbindungsnutzung die konfigurierte Datenobergrenze überschreitet. Detaillierte Informationen zur Messung finden Sie unter Metering und Standby-WAN-Verbindungen.



- **Adaptive Bandbreitenerkennung**: Verwendet die WAN-Verbindung mit einer reduzierten Bandbreitenrate, wenn ein Verlust festgestellt wird. Wenn die verfügbare Bandbreite unter der konfigurierten **minimal akzeptablen Bandbreite liegt**, wird der Pfad als SCHLECHT markiert. Verwenden Sie die benutzerdefinierte Empfindlichkeit für schlechten Verlust unter der Pfad- oder Autopath-Gruppe mit der Adaptiven Bandbreitenerkennung.

  > **Hinweis**
  >
  > Die adaptive Bandbreitenerkennung ist nur für den Client und nicht für MCN verfügbar.

  - **Zulässige Mindestbandbreite**: Bei variierender Bandbreitenrate ist dies der Prozentsatz der zulässigen Rate von WAN zu LAN, unterhalb dessen der Pfad als SCHLECHT markiert ist. Die minimalen KBit/s sind auf jeder Seite eines virtuellen Pfades unterschiedlich. Der Wert kann im Bereich von 10% bis 50% und der Standardwert 30% liegen.

Weitere Informationen finden Sie unter Adaptive Bandbreitenerkennung

Routen

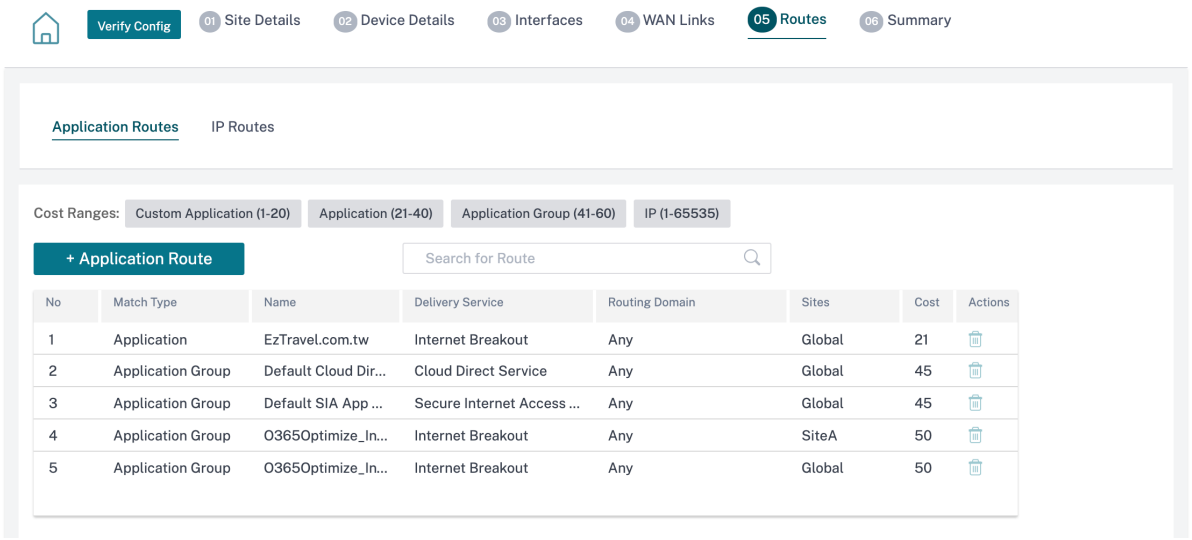
Der nächste Schritt im Workflow für die Sitekonfiguration besteht darin, Routen zu erstellen. Sie können Anwendungs- und IP-Routen basierend auf Ihren Site-Anforderungen erstellen.

> **HINWEIS:**
>
> Die Routen, die vor der Einführung der Registerkarten **Anwendungsroute** und **IP-Route** hinzuge-

> fügt wurden, werden unter der Registerkarte **IP-Routen** mit **Delivery Service** als Internet aufgeführt.

Die globalen Routen und standortspezifischen Routen, die auf Netzwerkebene erstellt werden, werden automatisch unter **Routen > Anwendungsrouten** und **-routen > IP-Routen** aufgelistet. Sie können die globalen Routen nur auf Siteebene anzeigen. Um eine globale Route zu bearbeiten oder zu löschen, navigieren Sie zu Konfigurationen auf Netzwerkebene.

Sie können Routen auch auf Siteebene erstellen, bearbeiten oder löschen.



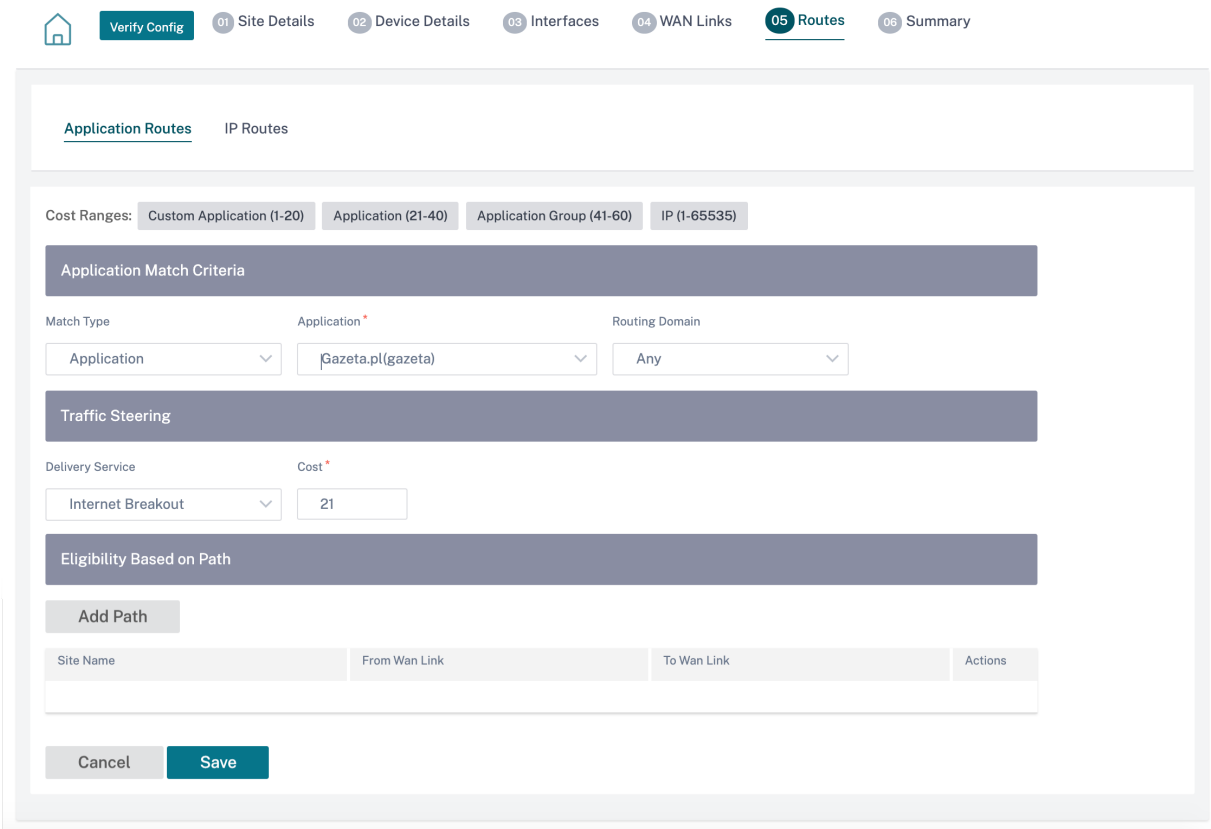
Anwendungs-Routen

Klicken Sie auf **+ Anwendungsroute**, um eine Anwendungsroute zu erstellen.

- **Übereinstimmungskriterien für benutzerdefinierte Anwendungen**:
  - **Übereinstimmungstyp**: Wählen Sie den Übereinstimmungstyp als ****Anwendung/Benutzerdefinierte**Anwendung/Anwendungsgruppe** aus der Dropdown-Liste
  - **Anwendung**: Wählen Sie eine Anwendung aus der Dropdownliste aus.
  - **Routingdomäne**: Wählen Sie eine Routingdomäne
- **Traffic Steering**
  - **Lieferservice**: Wählen Sie einen Lieferdienst aus der Liste.
  - **Kosten**: Spiegelt die relative Priorität jeder Route wider. Senken Sie die Kosten, je höher die Priorität.
- **Berechtigung basierend auf Pfad**:
  - **Pfad hinzufügen**: Wählen Sie eine Site und WAN-Links, sowohl zu als auch von. Wenn der hinzugefügte Pfad ausfällt, erhält die Anwendungsroute keinen Datenverkehr.

Wenn eine neue Anwendungsroute hinzugefügt wird, müssen die Routenkosten im folgenden Bereich liegen:

- Kundenspezifische Anwendung: 1-20
- Anwendung: 21-40
- Anwendungsgruppe: 41-60



IP-Routen

Gehen Sie zur Registerkarte **IP-Routen** und klicken Sie auf **+ IP-Route**, um die IP-Routenrichtlinie zur Steuerung des Datenverkehrs zu erstellen.

- **IP-Protokoll-Übereinstimmungskriterien**:
  - **Zielnetzwerk**: Fügen Sie das Zielnetzwerk hinzu, das beim Weiterleiten der Pakete hilft.
  - **IP-Gruppe verwenden**: Sie können ein Zielnetzwerk hinzufügen oder das Kontrollkästchen IP-Gruppe verwenden aktivieren, um eine IP-Gruppe aus der Dropdown-Liste auszuwählen.
  - **Routingdomäne**: Wählen Sie eine Routingdomäne aus der Dropdownliste
- **Traffic Steering**

  - **Lieferservice**: Wählen Sie einen Zustelldienst aus der Dropdownliste aus.
  - **Kosten**: Spiegelt die relative Priorität jeder Route wider. Senken Sie die Kosten, je höher die Priorität.

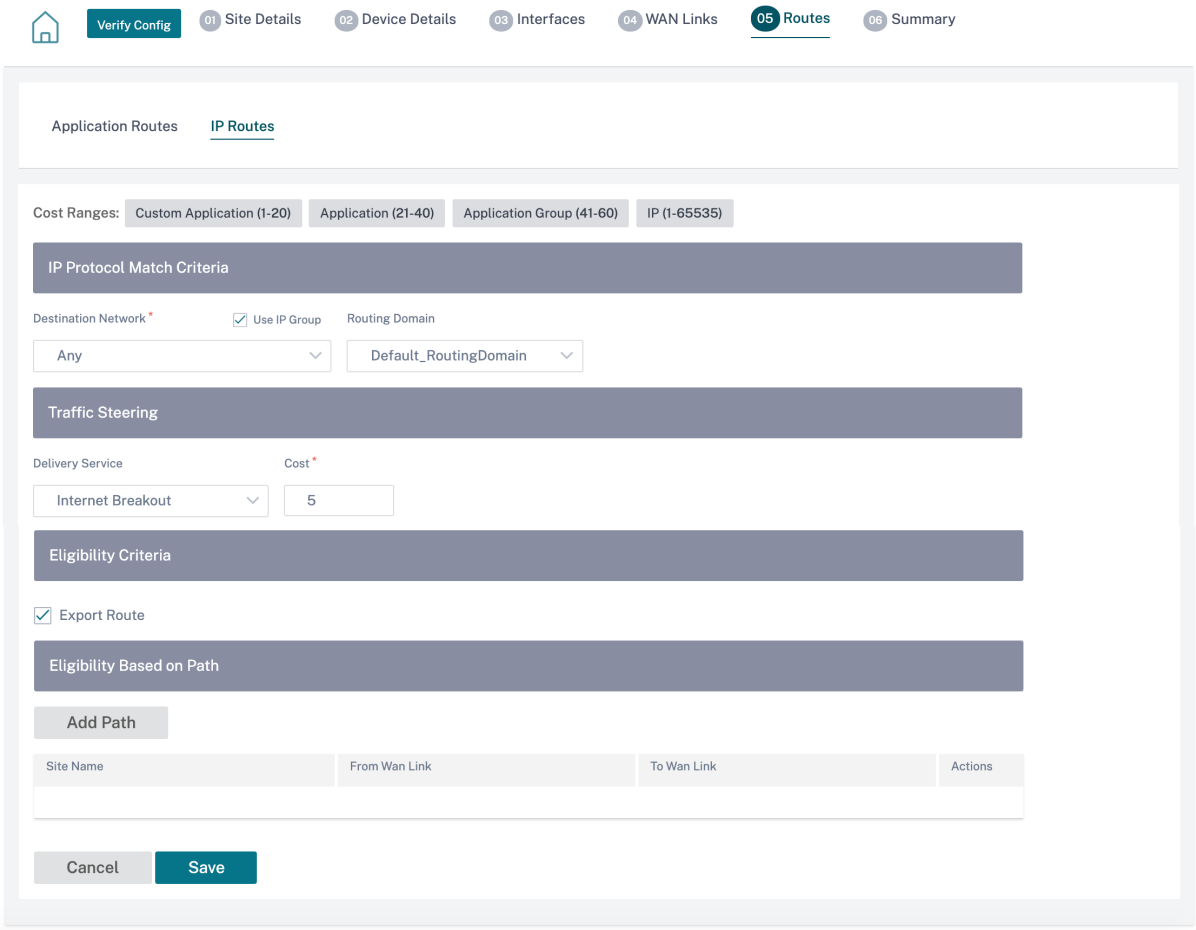
- **Zulassungskriterien**:

  - **Route exportieren**: Wenn das Kontrollkästchen Route exportieren aktiviert ist und es sich bei der Route um eine lokale Route handelt, kann die Route standardmäßig exportiert werden. Wenn es sich bei der Route um eine INTRANET/INTERNET-basierte Route handelt, muss WAN-zu-WAN-Weiterleitung aktiviert werden, damit der Export funktioniert. Wenn das Kontrollkästchen Exportroute deaktiviert ist, kann die lokale Route nicht in ein anderes SD-WAN exportiert werden und hat lokale Bedeutung.

- **Berechtigung basierend auf Pfad**:

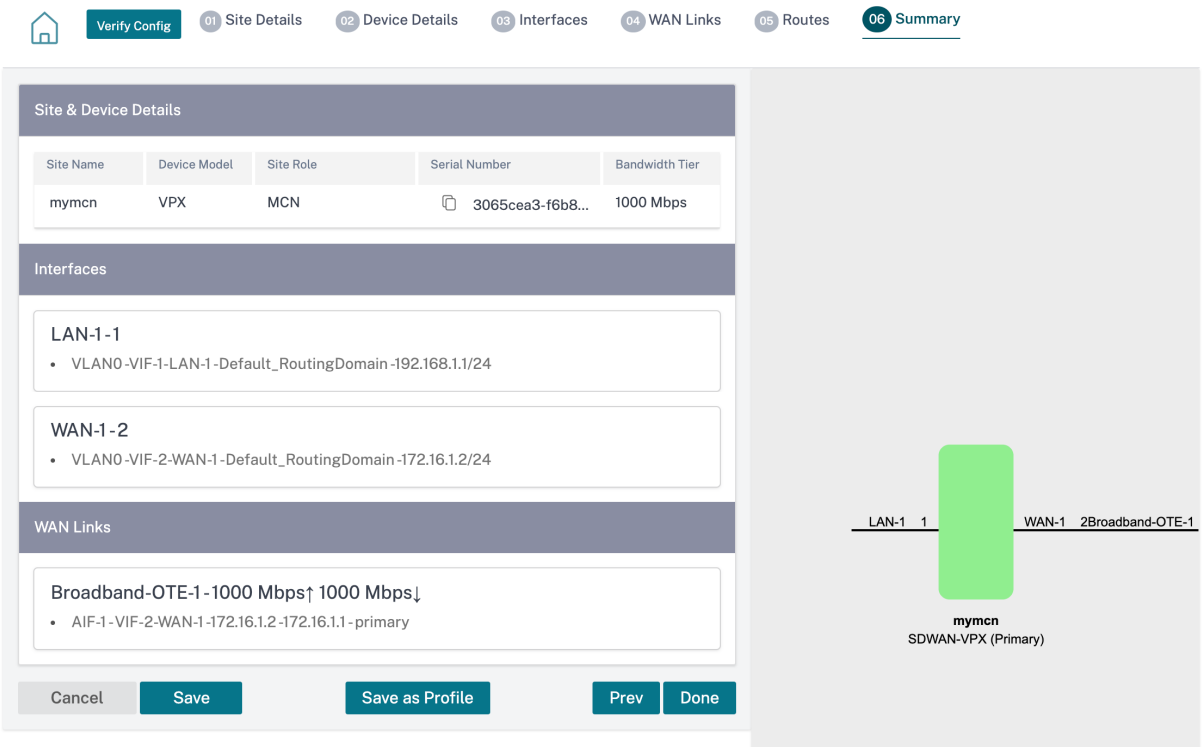
  - **Pfad hinzufügen**: Wählen Sie eine Site und WAN-Links, sowohl zu als auch von. Wenn der hinzugefügte Pfad ausfällt, erhält die IP-Route keinen Datenverkehr.

Wenn eine neue IP-Route hinzugefügt wird, müssen die Routenkosten im Bereich von 1—20 liegen.



Zusammenfassung

Dieser Abschnitt enthält eine Zusammenfassung der Site-Konfiguration, um eine schnelle Überprüfung zu ermöglichen, bevor Sie diese einreichen.



Verwenden **Sie die Option Als Vorlage speichern**, um die Sitekonfiguration als Vorlage für die Wiederverwendung in anderen Sites zu speichern. Wenn Sie auf **Fertig** klicken, wird die Standortkonfiguration abgeschlossen und Sie gelangen zur Seite **Netzwerkkonfiguration** —**Startseite**, auf der Sie alle konfigurierten Sites überprüfen können. Weitere Informationen finden Sie unter Netzwerkkonfiguration.

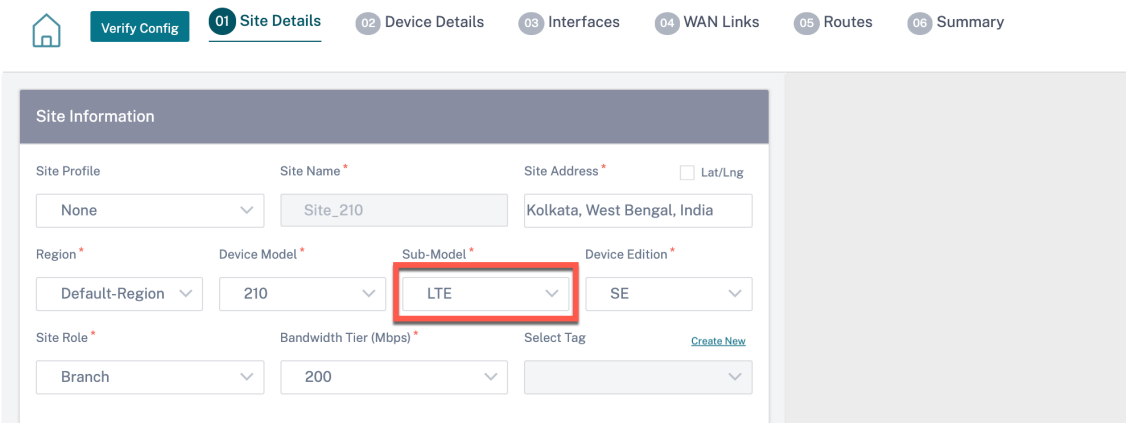
LTE-Firmware-Upgrade

October 21, 2022

Mit dem Citrix SD-WAN Orchestrator Service können Sie alle LTE-Sites in Ihrem Netzwerk konfigurieren und verwalten. Es umfasst Geräte, die über ein internes LTE-Modem oder ein externes USB-LTE-Modem verbunden sind.

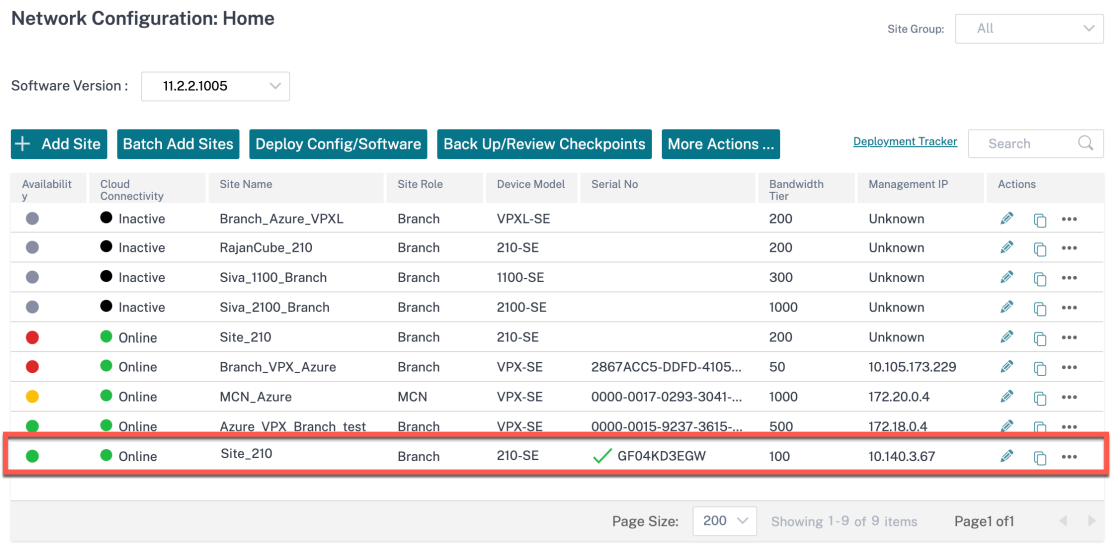
So konfigurieren Sie die LTE-Sites in Ihrem Netzwerk:

1. Navigieren Sie auf Standortebene zu **Konfiguration > Standortkonfiguration**.



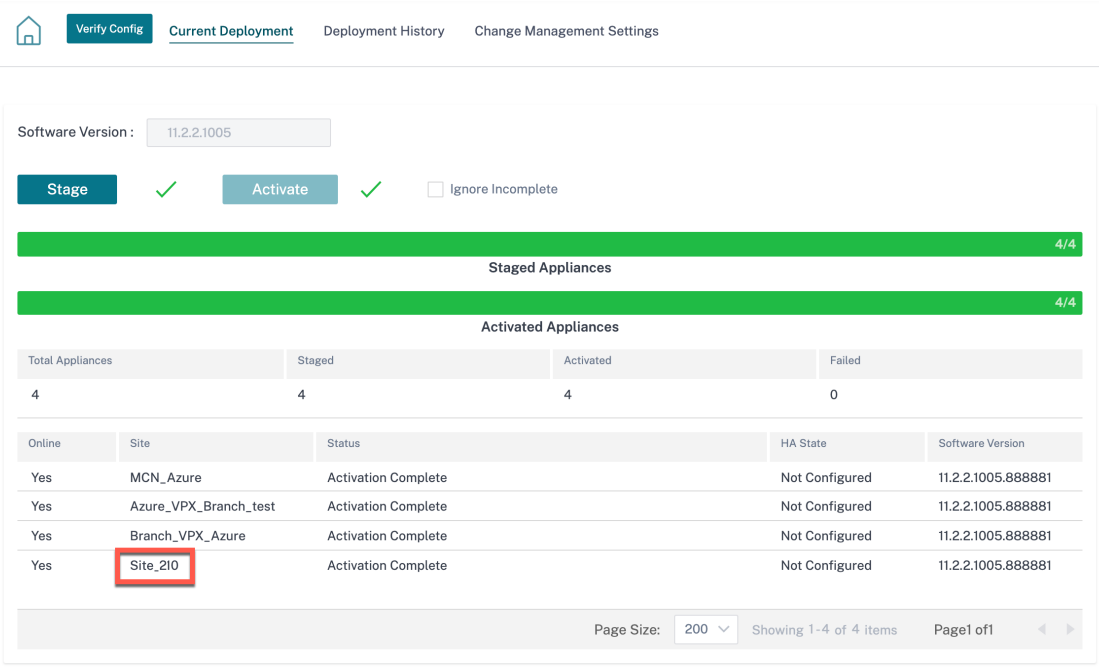
2. Wählen Sie das Submodell als **LTE** zusammen mit anderen erforderlichen Details aus und klicken Sie auf Speichern. Weitere Informationen zur Sitekonfiguration finden Sie unter Sitekonfiguration.

3. Nachdem die Site erstellt wurde, navigieren Sie zur **Startseite der Netzwerkkonfiguration** und klicken Sie auf die Schaltfläche **Konfiguration/Software bereitstellen** .



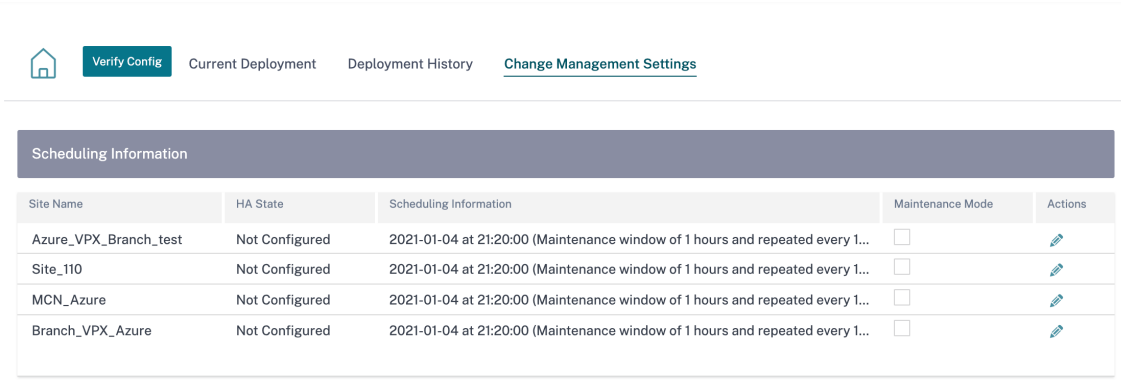
> C
>
> **Hinweis**
>
> Derzeit ist die LTE-Unterstützung auf Citrix SD-WAN 210-Appliances verfügbar.

4. Das Feld **Softwareversion** wird automatisch mit dem neuesten Softwareversionspaket gefüllt und das Feld kann nicht bearbeitet werden. Sobald Sie auf **Stage**klicken, wird die gesamte entsprechende LTE-Firmware für die ausgewählte Softwareversion heruntergeladen.



Es dauert einige Minuten, um das Staging abzuschließen. Sie können den Status anzeigen, um den Fortschritt des Stagings zu verfolgen. Zunächst zeigt der Status **Staging Pending**, **Downloaden der Appliance-Software**und schließlich **Staging Complete**an. Sie können das Staging jederzeit abbrechen, indem Sie auf die Schaltfläche **Phase abbrechen** klicken.

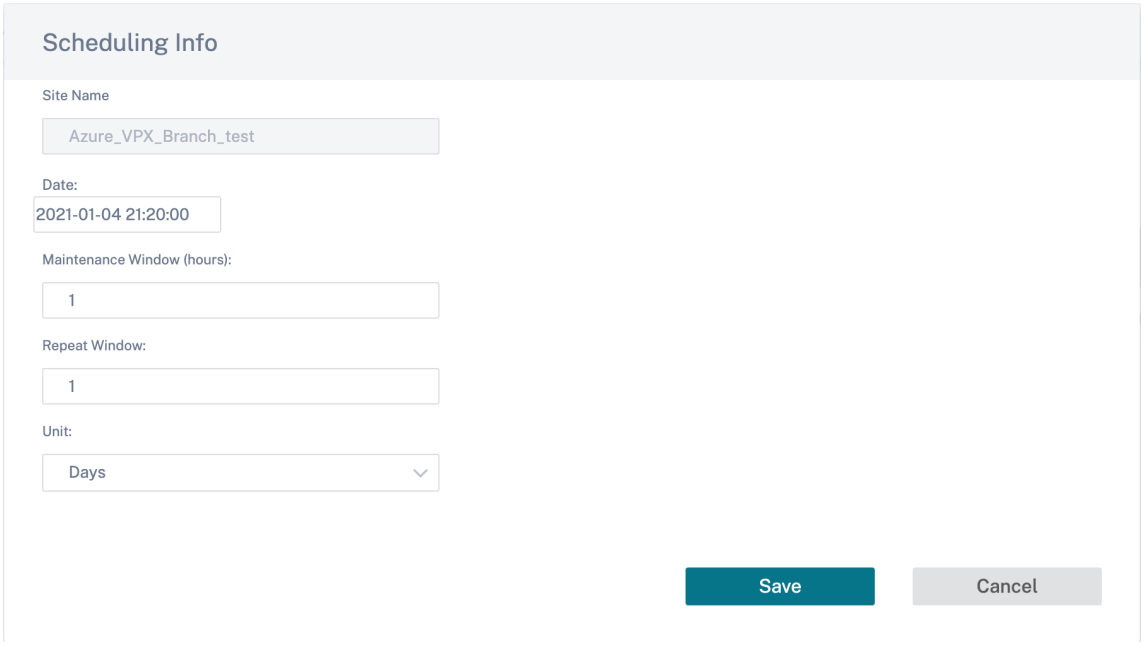
5. Sobald die Bereitstellung abgeschlossen ist, klicken Sie auf die Schaltfläche **Aktivieren**, um die Software zu aktivieren.
6. Die Aktivierung der LTE-Software ist Teil des Zeitplanungsfensters. Um die LTE-Software zu aktualisieren, navigieren Sie zur Registerkarte **Verwaltungseinstellungen ändern** . Sie können eine Liste von Sitenamen mit Planungsinformationen und einer Aktionsoption anzeigen.



Im Planungsfenster wird ein bestimmter Zeitrahmen für den Abschluss des LTE-Softwareupgrades festgelegt.

7. Klicken Sie auf das Aktionssymbol und geben Sie die Planungsinformationen an - Datum mit Uhrzeit, Dauer des Wartungsfensters in Stunden, Wiederholungsfenster mit Einheit als Tage/-

Wochen/Monate. Klicken Sie auf **Speichern**.



Sobald das Timing festgelegt ist, werden die Informationen an die Appliance weitergegeben. Die LTE-Firmware wird aktualisiert, wenn die Zeit in der Appliance mit der im Zeitplanfenster eingestellten Zeit übereinstimmt. Im Zeitplanfenster können Sie eine bestimmte Zeit für das Upgrade der LTE-Firmware konfigurieren. Das LTE-Firmware-Upgrade wird nicht sofort gestartet, wenn Sie das Zeitplanfenster festlegen.

> **Hinweis**
>
> Für alle Appliances sind die folgenden Standardplanungsinformationen, die bereits festgelegt sind:
>
> - **Zeitplanfenster** - 21:20:00
> - **Wartungsfenster** —1 Stunde
> - **Wiederholtes Fenster** - 1 Tag Wenn Sie
>
> also die Einstellungen für das Änderungsmanagement nicht konfigurieren, verarbeitet das Planungsfenster das Update automatisch. Wenn Sie den Wert von **Wartungsfenster (Stunden)** auf **0**setzen, erfolgt das LTE-Firmware-Upgrade sofort.

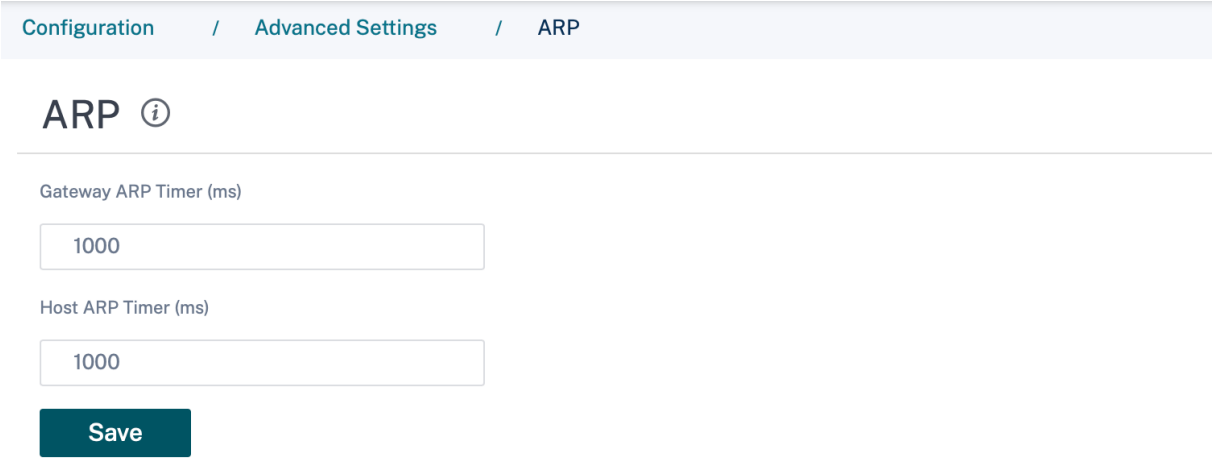
Ab 11.1.0 wird auf der Seite der Site-Interface-Gruppe ein neuer Konfigurations-Regler für die In-Band-Verwaltungskonfiguration hinzugefügt. Dies ist eine obligatorische Konfiguration für jede Appliance, die über eine Inband-IP verwaltet werden muss. Das Fehlen dieser Konfiguration im Citrix SD-WAN Orchestrator Service kann dazu führen, dass die Appliance offline geht (besonders wichtig, wenn die 210 s und 110 s, die über LTE verwaltet wurden, auf 11.1.0 aktualisiert wurden).

Protokoll zur Adressauflösung

October 21, 2022

In Citrix SD-WAN-Bereitstellungen wie Gateway und One-ARM werden die Access Points überlastet, wenn die ARP-Anforderungen (Address Resolution Protocol) häufig empfangen werden, was den Verkehrsfluss beeinträchtigt. Um die Verkehrsüberlastung zu überwinden, können Sie die folgenden ARP-Timer so konfigurieren, dass die ARP-Anforderungen mit bestimmten Intervallzeiten gesendet werden.

- **Gateway-ARP-Timer (ms)**: Die Zeit (Bereich: 100—20000 Millisekunden) zwischen ARP-Anforderungen für konfigurierte Gateway-IP-Adressen.
- **Host-ARP-Timer (ms)**: Die Zeit (Bereich: 1000—180000 Millisekunden) zwischen ARP-Anforderungen für konfigurierte Host-IP-Adressen.



Protokoll zur Entdeckung von Nachbarn

October 21, 2022

In einem IPv6-Netzwerk übertragen Citrix SD-WAN-Appliances regelmäßig Routerankündigungsmeldungen, um ihre Verfügbarkeit anzukündigen und Informationen an die benachbarten Appliances im SD-WAN-Netzwerk zu übermitteln. Die Router-Anzeigen enthalten die IPv6-Präfix-Informationen. Das auf Citrix SD-WAN-Appliances ausgeführte Neighbor Discovery-Protokoll (NDP) verwendet diese Routerankündigungen, um die benachbarten Geräte auf derselben Verbindung zu ermitteln. NDP ermittelt auch die Link-Layer-Adressen des jeweils anderen, findet Nachbarn und verwaltet Informationen zur Erreichbarkeit aktiver Nachbarn.

Um die NDP-Routerankündigung zu konfigurieren, navigieren Sie zu **Konfiguration > Erweiterte Einstellungen > NDP**, und klicken Sie auf **+ NDP**.

Wählen Sie eine der konfigurierten virtuellen Schnittstellen aus der Dropdown-Liste **Virtuelle Schnittstelle** aus. Wählen Sie **Ankündigung aktivieren**, um das Senden von regelmäßigen Router-Ankündigungen und das Beantworten von Router-Anfragen für die ausgewählte virtuelle Schnittstelle zu ermöglichen

Geben Sie die maximalen, minimalen und Router-Lebenszeitintervalle an.

- **Maximales Intervall**: Die maximal zulässige Zeit (in Sekunden) zwischen dem Senden periodischer unerwünschter Multicast-Router-Werbung.
- **Mindestintervall**: Die Mindestdauer (in Sekunden), die zwischen dem Senden periodischer unerwünschter Multicast-Router-Werbung zulässig ist.
- **Router-Lebensdauer**: Die Zeit (in Sekunden), in der der Router von den Hosts als gültig angesehen wird. 0 gibt an, dass der Router nicht als Standardrouter verwendet werden kann

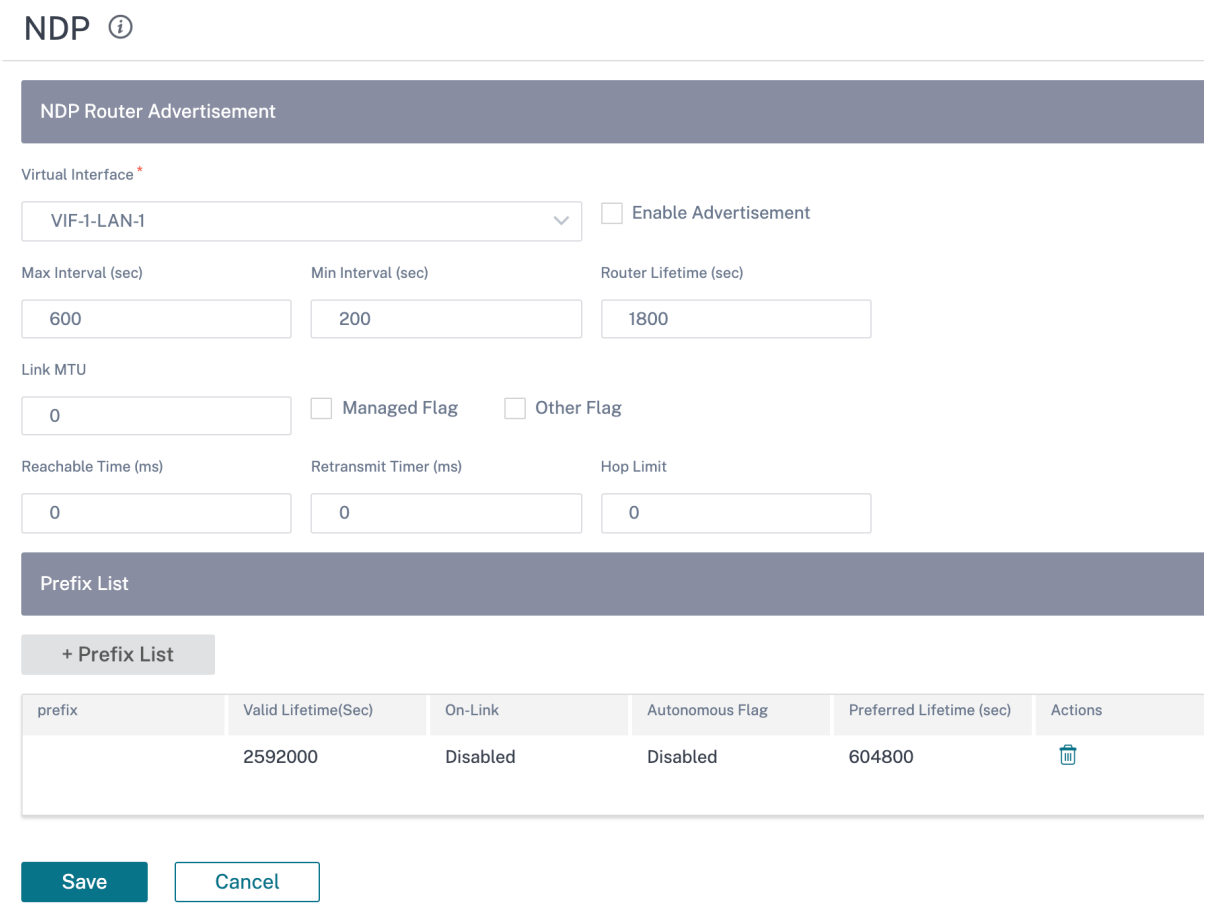
Wählen Sie **Managed Flag** aus, wenn IP-Adressen über das DHCPv6-Protokoll verfügbar sind. Wählen Sie **Anderes Flag**, wenn die Konfigurationsinformationen (außer den IP-Adressen) über das DHCPv6-Protokoll verfügbar sind.

Geben Sie die folgenden Werte für die ausgewählte Schnittstelle an.

- **Link MTU**: Die empfohlene Maximum Transmission Unit (MTU) für die Schnittstelle.
- **Erreichbare Zeit**: Die Zeit (in Millisekunden), die das NDP-Protokoll im Status "**Reachable** "verbleibt.
- **Retransmit-Timer**: Die Zeit (in Millisekunden) zwischen der erneuten Übertragung von Neighbor Solicitation Nachrichten beim Auflösen einer IP-Adresse oder der Untersuchung eines Nachbarn.
- **Hop-Limit**: Die maximale Anzahl von Hops, die in die Router-Werbung aufgenommen werden sollen.

Klicken Sie auf +Präfixliste und geben Sie die folgenden Werte ein:

- **Präfix**: Die Präfix- und Präfixlänge in der Cassless Inter-Domain Routing (CIDR) -Notation.
- **Gültige Lebensdauer**: Die Zeit in Sekunden, bis zu der das Präfix gültig ist. -1 steht für unendlich, was bedeutet, dass das Präfix für immer erhalten bleibt.
- **On-Link**: Wenn diese Option ausgewählt ist, wird das Präfix als lokal für das Netzwerk betrachtet.
- **Autonomes Flag**: Wenn diese Option aktiviert ist, wird das Präfix von der Stateless Address Autoconfiguration (SLAAC) des Hosts verwendet, um die IP-Adresse zu generieren.
- **Präfix-Lebensdauer**: Die Zeit (in Sekunden), bis zu der das Präfix als bevorzugt gilt.



Virtuelle Pfade

October 21, 2022

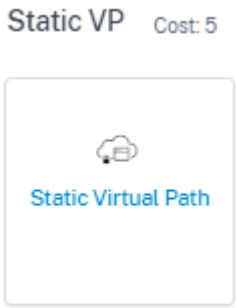
Ein virtueller Pfad ist eine logische Verbindung zwischen zwei WAN-Verbindungen. Es besteht aus einer Sammlung von WAN-Pfaden, die kombiniert werden, um eine hohe Service-Level-Kommunikation zwischen zwei SD-WAN-Knoten zu ermöglichen. Dies geschieht durch ständiges Messen und Anpassen an sich ändernde Anwendungsanforderungen und WAN-Bedingungen. Die SD-WAN-Appliances messen das Netzwerk auf einer Pro-Path-Basis. Ein virtueller Pfad kann statisch (immer existiert) oder dynamisch sein (existiert nur, wenn der Datenverkehr zwischen zwei SD-WAN-Appliances einen konfigurierten Schwellenwert erreicht).

Statische virtuelle Pfade

Die Einstellungen für den virtuellen Pfad werden von den globalen Einstellungen für den automatischen WAN-Linkpfad übernommen. Sie können diese Konfigurationen überschreiben und den

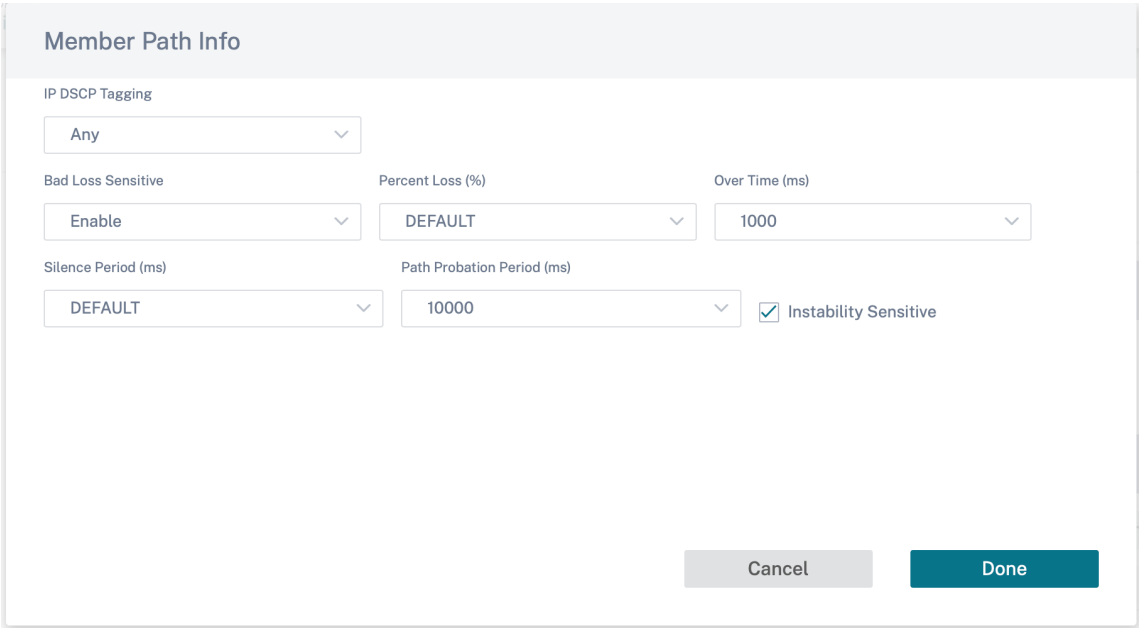
Mitgliedspfad hinzufügen oder entfernen. Sie können die virtuellen Pfade auch basierend auf der Site und dem angewendeten QoS-Profil filtern. Geben Sie eine Tracking-IP-Adresse für den WAN-Link an, die angepingt werden kann, um den Status des WAN-Link zu bestimmen. Sie können auch eine Reverse-Tracking-IP für den umgekehrten Pfad angeben, der angepingt werden kann, um den Status des Rückwärtspfads zu bestimmen.

Um statische virtuelle Pfade zu konfigurieren, navigieren Sie auf Standortebene zu **Konfiguration** > **Erweiterte Einstellungen** > **Virtuelle Pfade** > **Statische virtuelle Pfade**.



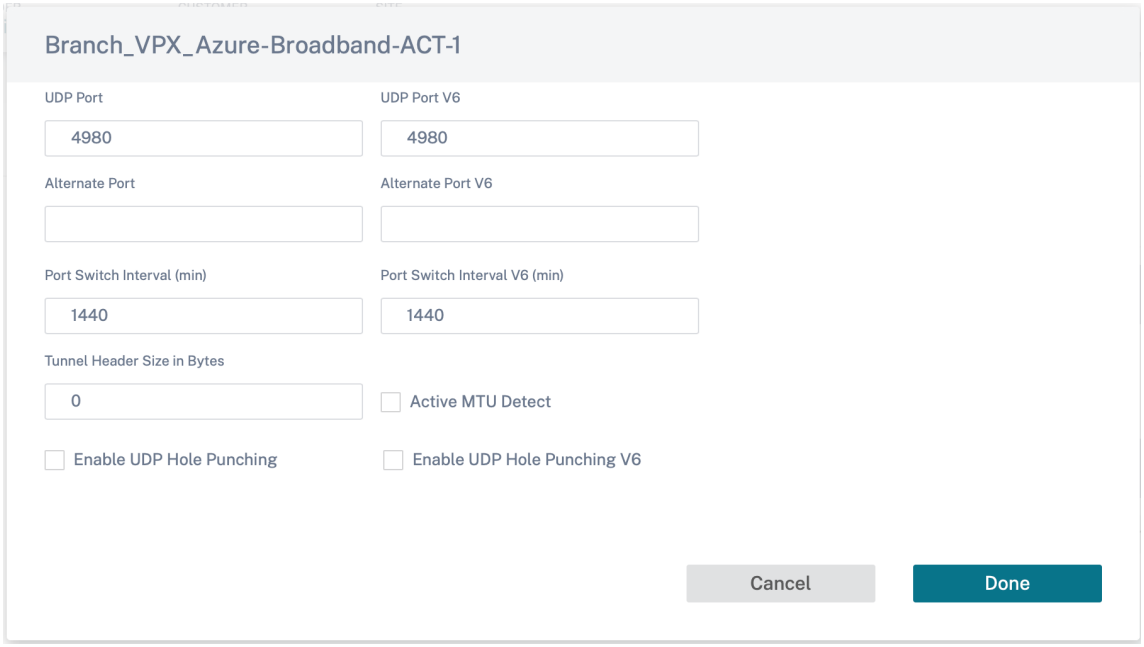
Die aktiven Mitgliedspfade werden im Abschnitt **Aktive Mitgliedspfade** aufgeführt. Sie können die Mitgliedspfadeinstellungen anzeigen oder bearbeiten.

- **IP-DSCP-Tagging**: Ein Tag für den externen IP-Header des Virtual Path Control Protocol (VPCP) -Frames.
- **Verlustsensitiv**: Wenn diese Option aktiviert ist, kann ein Pfad aufgrund eines Verlusts als BAD markiert werden und führt zu einer Latenzstrafe in einem Pfad-Score. Legen Sie den Prozentsatz des Verlusts über die Zeit fest, die erforderlich ist, um den Pfad als BAD zu markieren Deaktivieren Sie diese Option, wenn ein Verlust der Bandbreite nicht tolerierbar ist.
- **Prozentualer Verlust**: Wenn der Paketverlust den festgelegten Prozentsatz über die konfigurierte Zeit überschreitet, ändert sich der GOOD Path-Status in BAD.
- **Im Laufe der Zeit**: Wenn der Paketverlust in dieser konfigurierten Zeit den festgelegten Prozentsatz überschreitet, wird der Pfadstatus als SCHLECHT markiert.
- **Ruhezeit**: Der Pfadstatus wechselt von GUT zu SCHLECHT, wenn innerhalb der angegebenen Zeitspanne keine Pakete empfangen werden.
- **Pfad-Probezeit: Der Zeitraum**, der gewartet werden muss, bevor der Pfadstatus von BAD in GOOD geändert wird.
- **Instabilitätssensitiv**: Latenzstrafen aufgrund des Status BAD und anderer Latenzspitzen werden berücksichtigt.



Die WAN-Link-Details für die ausgewählten aktiven Mitgliedspfade werden aufgelistet. Sie können die Einstellungen nach Bedarf ändern. Die **UDP-Porteinstellungen** können sowohl für IPv4 als auch für IPv6 konfiguriert werden.

- **UDP-Port**: Der für die LAN-zu-WAN- und WAN-zu-LAN-Paketübertragung verwendete Port. Sie können auch angeben.
- **Alternativer Port**: Der alternative UDP-Port, der verwendet werden soll, wenn UDP-Portwechsel aktiviert ist
- **Port-Switch-Intervall**: Das Intervall in Minuten, in dem der WAN-Link seinen UDP-Port wechselt.
- **Tunnel-Header-Größe in Byte**: Die Größe des Tunnel-Headers in Byte, falls zutreffend.
- **Aktive MTU-Erkennung**: Die LAN-zu-WAN-Pfade für dynamische virtuelle Pfade werden aktiv auf MTU untersucht.
- **UDP Hole Punching aktivieren**: Der MCN unterstützt die UDP-Konnektivität zwischen kompatiblen NAT-geschützten Client-Sites.

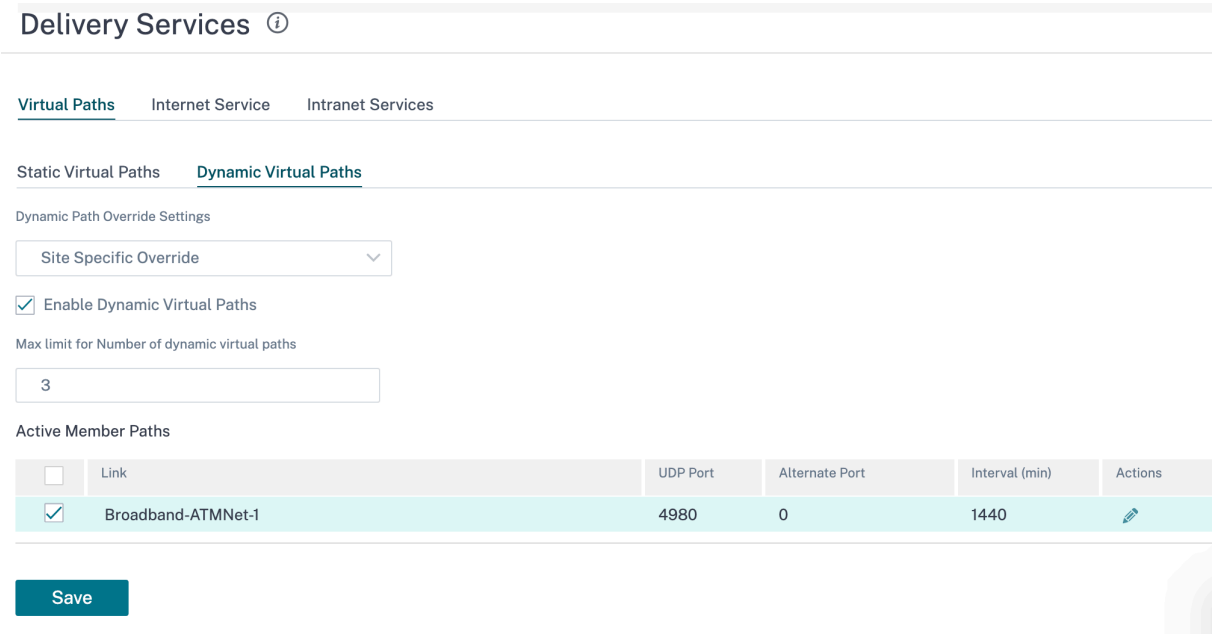


Dynamische virtuelle Pfade

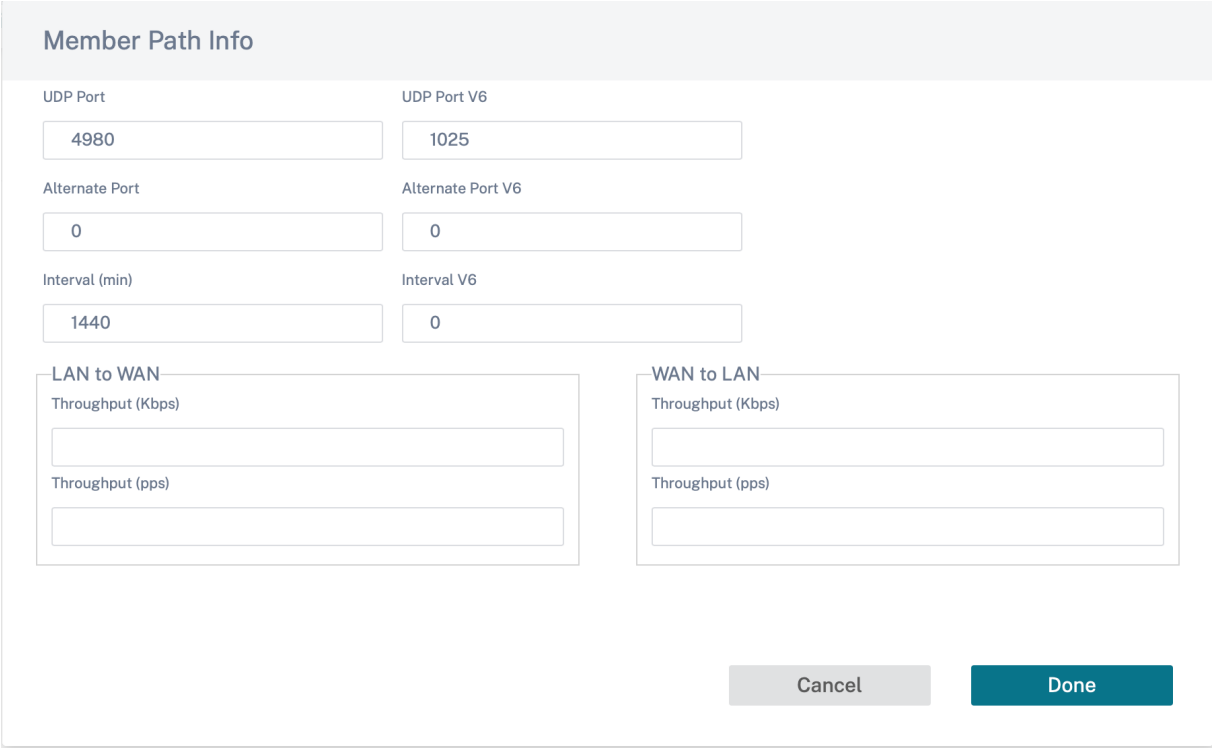
Angesichts der Nachfrage nach VoIP und Videokonferenzen hat der Verkehr zwischen den Büros zugenommen. Das Einrichten vollständiger Mesh-Verbindungen über Rechenzentren ist zeitaufwändig und ineffizient. Mit Citrix SD-WAN können Sie mit der Funktion Dynamic Virtual Path automatisch Pfade zwischen Büros bei Bedarf erstellen. Die Sitzung verwendet anfänglich einen vorhandenen festen Pfad. Wenn der Bandbreiten- und Zeitschwellenwert erreicht ist, wird ein neuer Pfad dynamisch erstellt, wenn dieser neue Pfad bessere Leistungsmerkmale aufweist als der feste Pfad. Der Sitzungsverkehr wird über den neuen Weg übertragen, was zu einer effizienten Nutzung der Ressourcen führt. Die dynamischen virtuellen Pfade existieren nur, wenn sie benötigt werden, und reduzieren den Datenverkehr, der zum und vom Rechenzentrum übertragen wird.

Um dynamische virtuelle Pfade zu konfigurieren, navigieren Sie auf Standortebene zu **Konfiguration** > **Erweiterte Einstellungen** > **Virtuelle Pfade** > **Dynamische virtuelle Pfade**.

Wählen Sie „ **Globale Standardwerte** außer Kraft setzen“, um die von den globalen Einstellungen für den automatischen Pfad der WAN-Links übernommenen Wählen Sie **Dynamische virtuelle Pfade aktivieren**, um dynamische virtuelle Pfade zwischen dieser Site und anderen über einen Zwischenknoten verbundenen Sites zuzulassen. Legen Sie die maximal zulässigen dynamischen virtuellen Pfade für die Site fest.



Legen Sie den Schwellenwert für den UDP-Port und den dynamischen Geben Sie den Durchsatzschwellenwert in Kbit/s oder Paketen pro Sekunde an, an dem die dynamischen virtuellen Pfade von LAN zu WAN oder WAN to LAN ausgelöst werden.



Dynamisches Routing

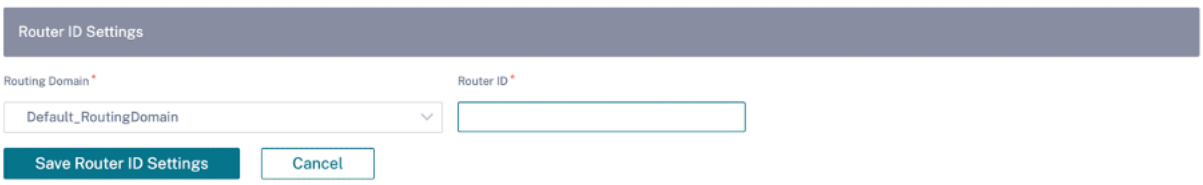
October 21, 2022

Nach der Konfiguration und Bereitstellung von SD-WAN-Appliances im Netzwerk und nach dem Aufbau der Verbindungen ist es wichtig sicherzustellen, dass der Datenverkehr ordnungsgemäß über das Overlay-SD-WAN-Netzwerk umgeleitet wird. Sie können die Verkehrsumleitung mithilfe von Ping- und Traceroute-Diagnosetools überprüfen. Wenn die Ping- und Traceroute-Tests ergeben, dass die Konnektivität über die zugrunde liegenden Pfade hergestellt wird, kann die Verkehrsumleitung mithilfe der folgenden dynamischen Routing-Protokolle erreicht werden.

- **Open Shortest Path First (OSPF)**: Es handelt sich um ein internes Gateway-Protokoll, mit dem der Datenverkehr innerhalb eines autonomen Systems wie dem Unternehmensnetzwerk umgeleitet wird OSPF verwendet einen Link-State-Routing-Algorithmus, um Änderungen in der Netzwerktopologie zu erkennen und Pakete umzuleiten, indem zuerst der kürzeste Pfad für jede Route berechnet wird. Verwenden Sie dieses Protokoll, um MPLS-Verkehr umzuleiten. Weitere Informationen finden Sie im Abschnitt **OSPF** .
- **Border Gateway Protocol (BGP)**: Es ist ein externes Gateway-Protokoll, das entwickelt wurde, um Verkehrsroutings- und Erreichbarkeitsinformationen zwischen verschiedenen autonomen Systemen im Internet umzuleiten Es ist in der Lage, Routing-Entscheidungen auf der Grundlage von von ISPs festgelegten Pfaden zu treffen Verwenden Sie dieses Protokoll, um den Internetverkehr umzuleiten. Weitere Informationen finden Sie im Abschnitt **Konfiguration von BGP** .

Zuvor war die dynamische Routing-Funktion nur für eine einzelne Router-ID verfügbar. Sie konnten eine eindeutige Router-ID entweder global für alle konfigurierten Routingdomänen (eine für OSPF und BGP) konfigurieren oder keine Router-ID angeben. Ab Citrix SD-WAN 11.3.1 können Sie nicht nur eine Router-ID für das gesamte Protokoll konfigurieren, sondern auch eine Router-ID für jede Routingdomäne konfigurieren. Mit dieser Verbesserung können Sie stabiles dynamisches Routing über mehrere Instanzen hinweg ermöglichen, wobei verschiedene Router-IDs auf stabile Weise konvergieren.

Wenn Sie eine Router-ID für eine bestimmte Routingdomäne konfigurieren, überschreibt die spezifische Router-ID die Routingdomäne auf Protokollebene.



OSPF

Um OSFF zu konfigurieren, navigieren Sie zu **Konfiguration > Erweiterte Einstellungen > Dynamisches Routing > OSPF**.

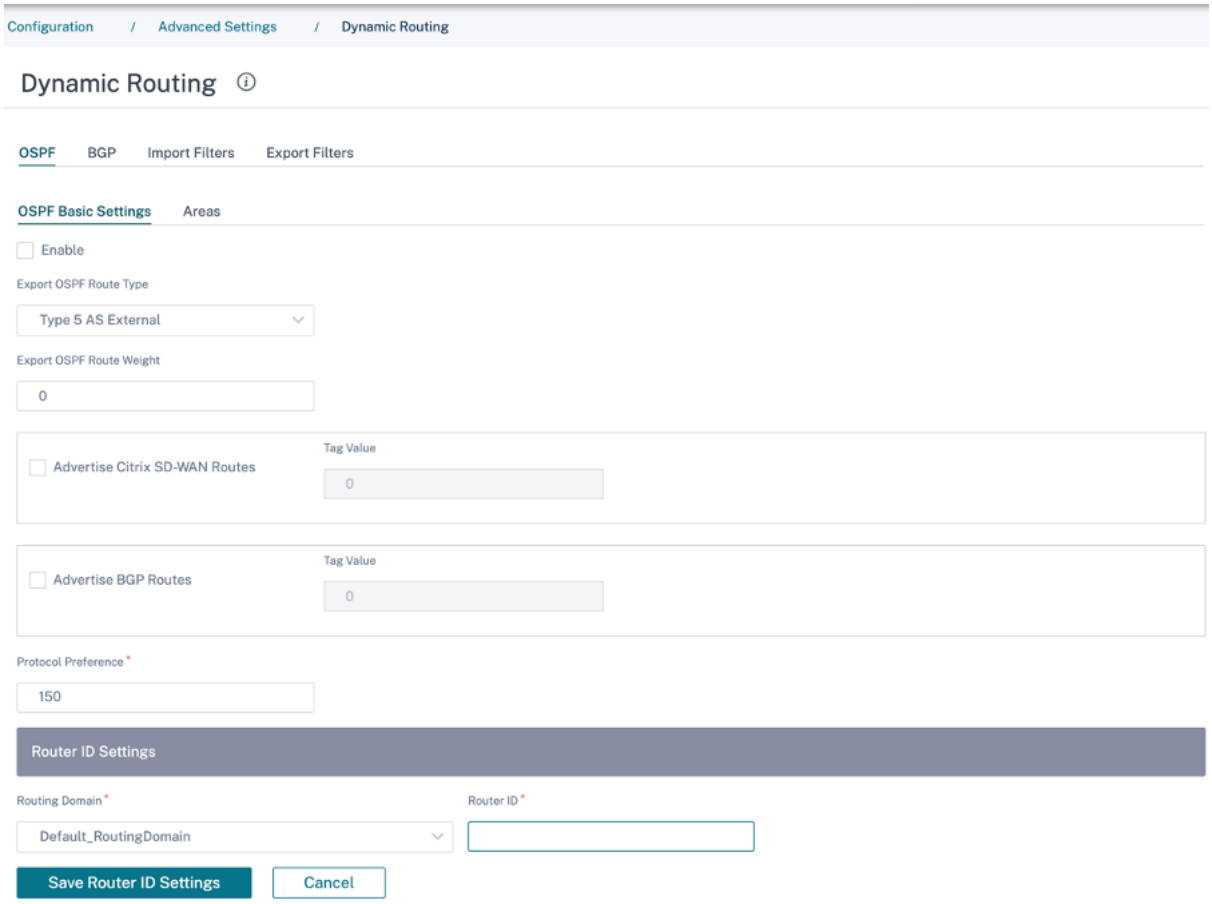
OSPF-Grundeinstellungen

Hier sind die Parameter, die konfiguriert werden müssen:

- **Aktivieren**: Erlauben Sie dem OSPF-Routingprotokoll auf der SD-WAN-Appliance, Hello-Pakete zwischen benachbarten Routern auszutauschen.
- **Router-ID**: Die IPv4-Adresse, die für OSPF-Werbung verwendet wird. Das Feld ist optional. Wenn es nicht angegeben ist, wird die niedrigste virtuelle IPv4-Adresse der virtuellen Schnittstellen ausgewählt, die am Routing teilnehmen. Für die IPv6-Schnittstelle ist es zwingend erforderlich, die Router-ID im IPv4-Format anzugeben. Zum Beispiel 1.1.1.1.

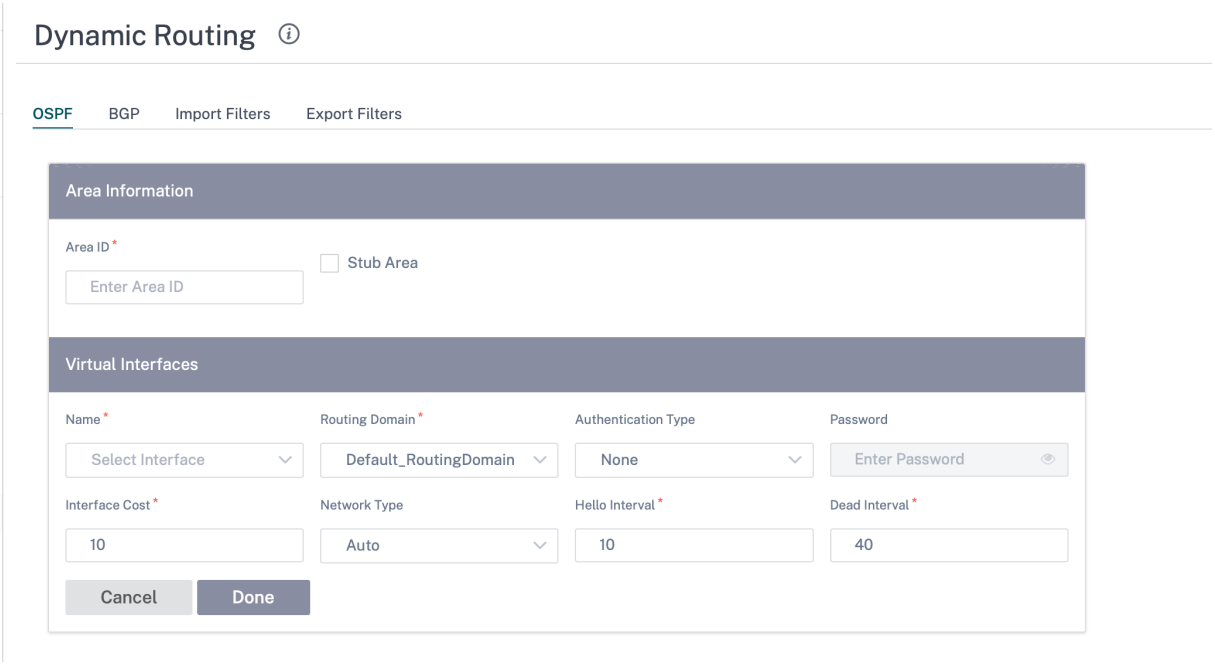
  > **Hinweis**
  >
  > - Die Router-ID-Konfiguration ist optional für ein IPv4-Netzwerk. Für ein IPv6-Netzwerk ist die Router-ID-Konfiguration jedoch obligatorisch. Die Router-ID für ein IPv6-Netzwerk muss im gleichen IPv4-Format (32-Bit-Notation) konfiguriert sein.
  >
  >   * Sie müssen separate IPv4- und IPv6-Peering an denselben Router (falls zutreffend) für Lern- und Werbezwecke erstellen.

- **OSPF-Routentyp exportieren: Geben**Sie die SD-WAN-Route an OSPF-Nachbarn als Typ 1 Intra-Area-Route oder als externe Route vom Typ 5 an.
- **OSPF-Routengewicht exportieren**: Die den OSPF-Nachbarn angekündigten Kosten sind die ursprünglichen Routenkosten und das hier konfigurierte Gewicht.
- **SD-WAN-Routen bewerben**: Um SD-WAN-Routen zu den Peer-Netzwerkelementen anzukündigen.
- **BGP-Routen bewerben**: Um die Umverteilung von BGP-Routen in die OSPF-Domain zu ermöglichen.



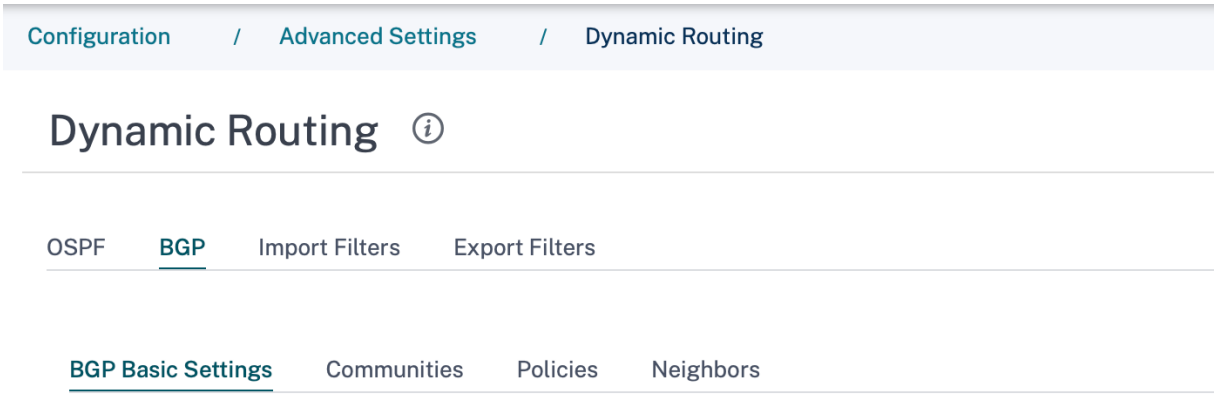
Bereiche

Klicken Sie auf **+ Gebiet** und geben Sie die Gebiets-ID des Netzwerks an, aus dem OSPF Routen lernt und Routen ankündigt. Der Stub-Bereich stellt sicher, dass dieser Bereich keine Routenwerbung von außerhalb des ausgewiesenen Autonomen Systems erhält. Konfigurieren Sie die Einstellungen der virtuellen Schnittstelle.



BGP

Um BGP zu konfigurieren, navigieren Sie zu **Konfiguration > Erweiterte Einstellungen > Dynamisches Routing > BGP**.



BGP Grundeinstellungen

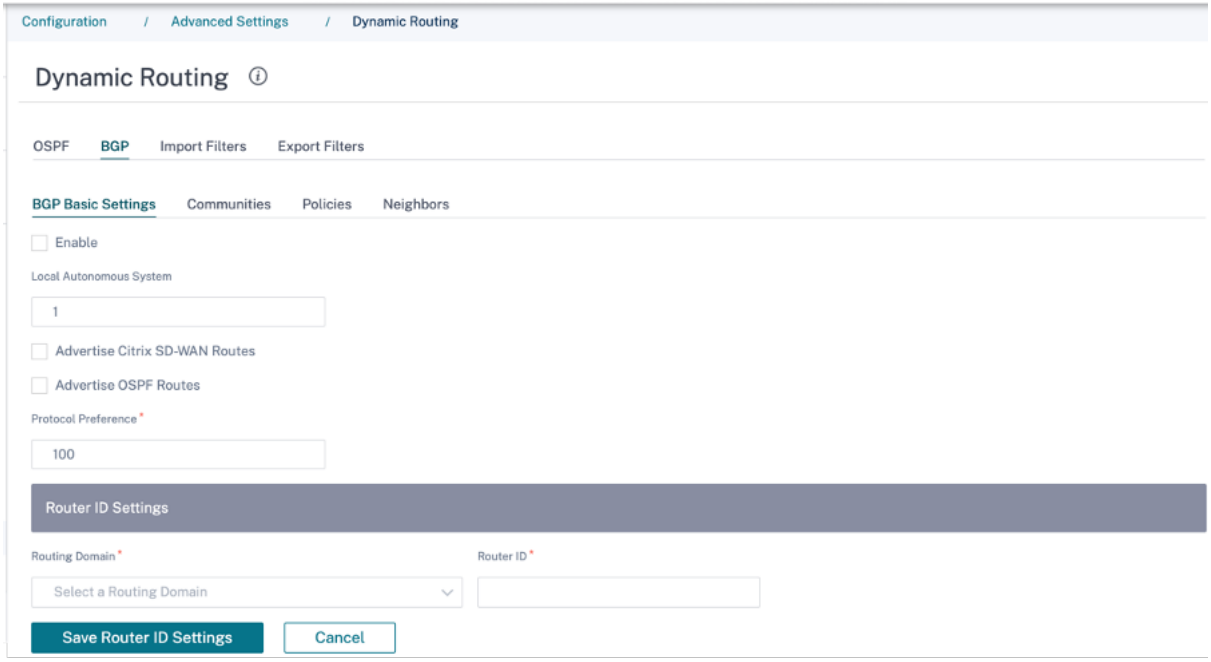
Im Folgenden sind die zu konfigurierenden Parameter aufgeführt:

- **Aktivieren**: Erlauben Sie dem BGP-Routingprotokoll auf der SD-WAN-Appliance, im Rahmen des BGP-Peerings mit dem Senden einer offenen Nachricht zu beginnen.
- **Router-ID**: Die IPv4-Adresse, die für BGP-Werbung verwendet wird. Wenn die Router-ID nicht angegeben ist, wird die niedrigste virtuelle IPv4-Adresse der am Routing beteiligten virtuellen

Schnittstellen ausgewählt.

> **Hinweis**
>
> – Die Router-ID-Konfiguration ist optional für ein IPv4-Netzwerk. Für ein IPv6-Netzwerk ist die Router-ID-Konfiguration jedoch obligatorisch. Die Router-ID für ein IPv6-Netzwerk muss im gleichen IPv4-Format (32-Bit-Notation) konfiguriert sein.
>
> * Sie müssen separate IPv4- und IPv6-Peering an denselben Router (falls zutreffend) für Lern- und Werbezwecke erstellen.

- **Lokales autonomes System**: Autonome Systemnummer, unter der das BGP-Protokoll ausgeführt wird.
- **SD-WAN-Routen bewerben**: Um SD-WAN-Routen zu den Peer-Netzwerkelementen anzukündigen.
- **Werbung für OSPF-Routen**: Ermöglicht die Umverteilung von OSPF-Routen in die BGP-Domain.

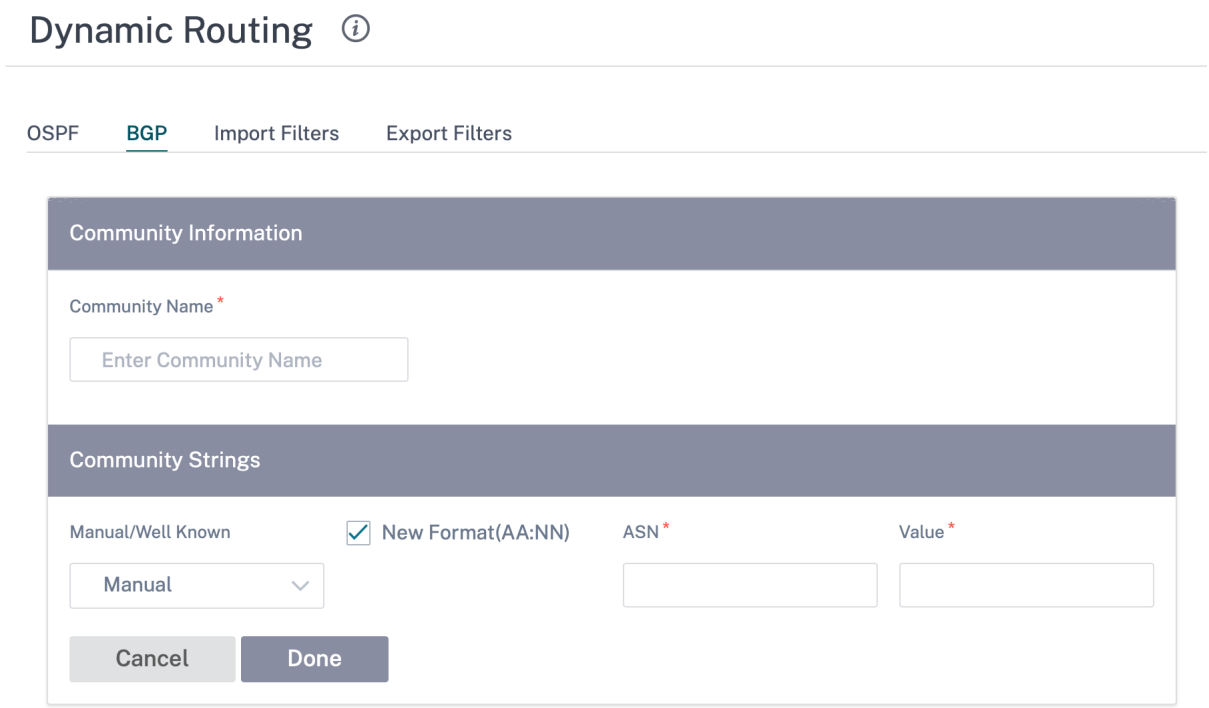


Communities

Klicken Sie auf **+ Community**, um eine Community hinzuzufügen. Eine Sammlung von BGP-Communities, die für die Routenfilterung verwendet werden können. Die Community-Liste kann auch verwendet werden, um die Communities einer übereinstimmenden Route festzulegen oder zu ändern.

Für jede Richtlinie können Benutzer mehrere Community-Zeichenfolgen, AS-PATH-PREPEND, **MED-Attribut** konfigurieren. Benutzer können bis zu 10 Attribute für jede Richtlinie konfigurieren.

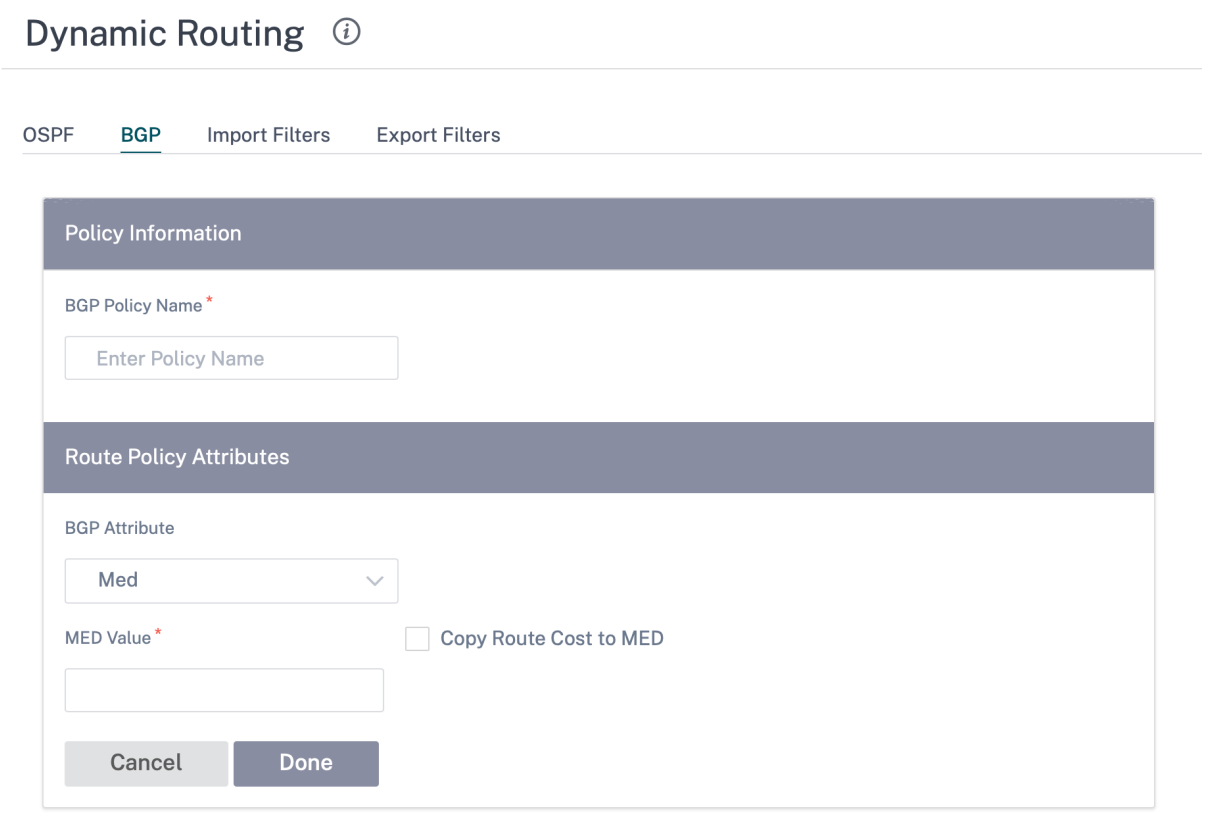
Geben Sie den Namen für die Community an und geben Sie eine Community-Zeichenfolge ein, die angekündigt werden soll.



- **Community-Name**: Geben Sie einen Communitynamen ein.
- **Manuell/Bekannt**: Konfigurieren Sie die BGP-Community manuell oder wählen Sie eine bekannte Standard-BGP-Community aus der Liste aus.
- **Neues Format (AA:NN)**: Aktivieren Sie das Kontrollkästchen, um das neue Format für die Konfiguration der BGP-Community zu verwenden.
- **ASN**: Die ersten 16 Ziffern der BGP-Community bei Verwendung des neuen Formats für die Konfiguration.
- **Wert**: Geben Sie den BGP-Community-Wert ein.

Richtlinien

Eine Sammlung von BGP-Attributen, die zum Festlegen oder Ändern von Routenattributen für jeden BGP-Peer verwendet werden können. Erstellen Sie BGP-Richtlinien, die selektiv auf eine Gruppe von Netzwerken pro Nachbarn angewendet werden, in beide Richtungen (Import oder Export). Eine SD-WAN-Appliance unterstützt acht Richtlinien pro Site, wobei bis zu acht Netzwerkobjekte (oder acht Netzwerke) mit einer Richtlinie verknüpft sind.

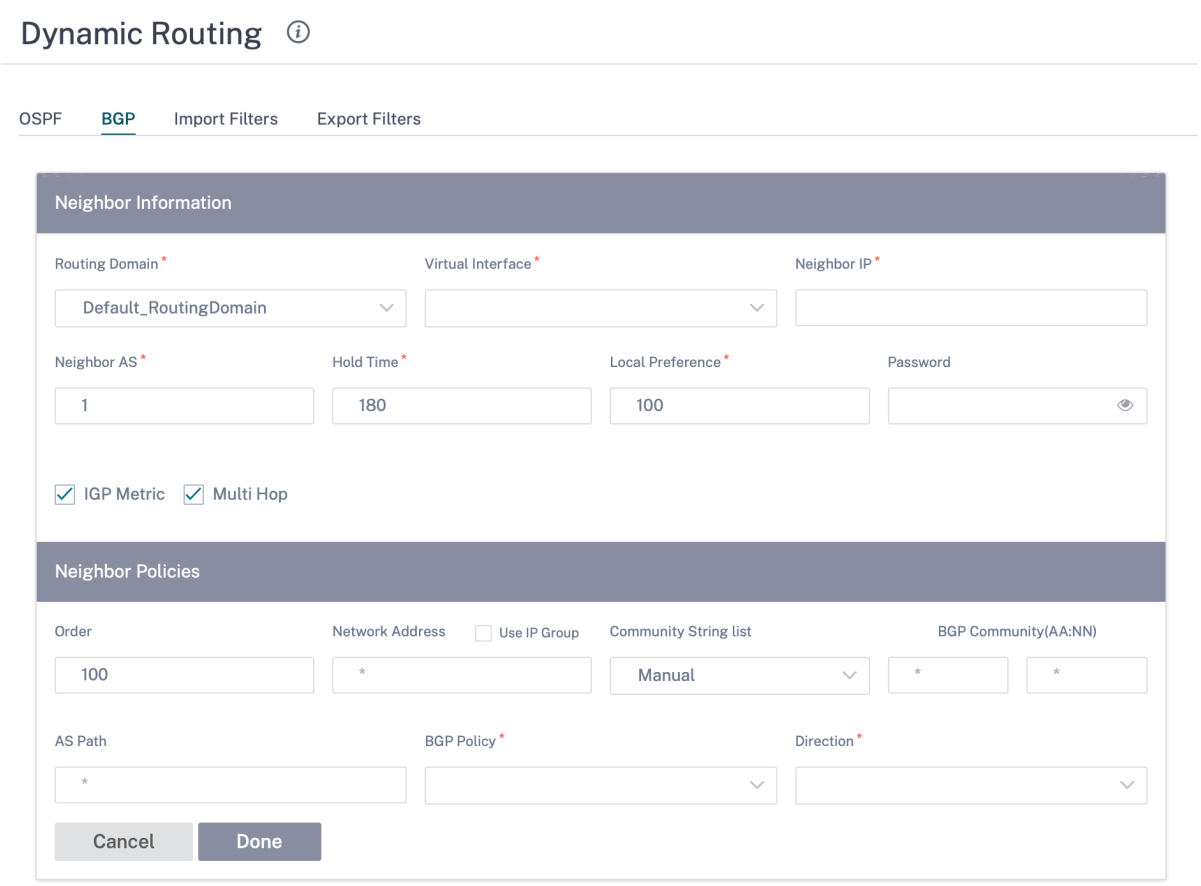


- **Name der BGP-Richtlinie**: Geben Sie den BGP-Richtliniennamen ein.
- **BGP-Attribute**: Wählen Sie die BGP-Attribute aus der Liste aus und geben Sie die erforderlichen Informationen an.

Nachbarn

Nachbarn sind alle konfigurierten BGP-Peer-Router, die überprüft werden, um die kürzesten Pfade für das Routing zu finden. Alle Nachbarn müssen Teil desselben Autonomen Systems sein.

Klicken Sie auf **+ Nachbar**, um eine konfigurierte BGP-Richtlinie für benachbarte Router hinzuzufügen. Sie können die Richtung angeben, um anzugeben, ob diese Richtlinie für eingehende oder ausgehende Routen angewendet wird.



Routenfilterung

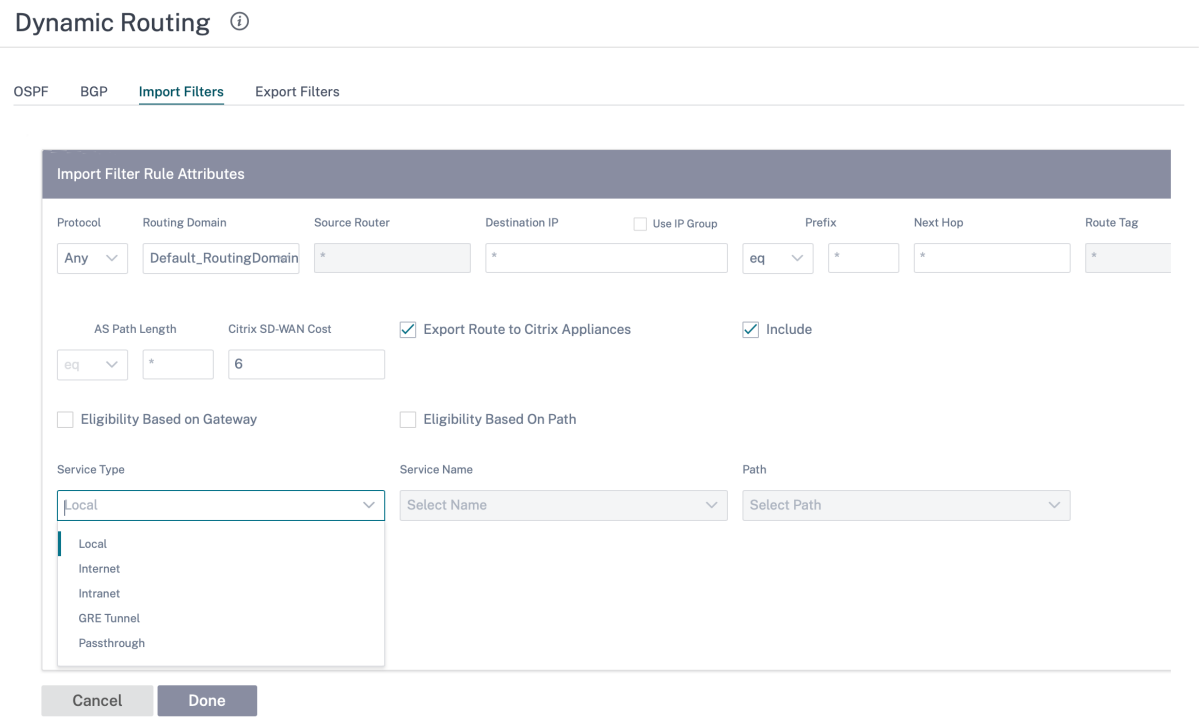
Für Netzwerke mit aktiviertem Route Learning bietet Citrix SD-WAN Orchestrator mehr Kontrolle darüber, welche SD-WAN-Routen den Routing-Nachbarn angekündigt werden und welche Routen von Routing-Nachbarn empfangen werden, anstatt alle oder keine Routen anzukündigen und zu akzeptieren.

Importieren von Filtern

Importfilter werden verwendet, um Routen zu akzeptieren oder nicht zu akzeptieren, die mithilfe von OSPF- und BGP-Nachbarn empfangen werden, basierend auf bestimmten Übereinstimmungskriterien. Importfilterregeln sind die Regeln, die erfüllt sein müssen, bevor dynamische Routen in die SD-WAN-Routendatenbank importiert werden. Standardmäßig werden keine Routen importiert.

Sie können Filter konfigurieren, um die Art und Weise, wie das Routenlernen stattfindet, zu optimieren.

Klicken Sie auf **+ Regel importieren**.



Verwenden Sie die folgenden Kriterien, um jeden Exportfilter zu erstellen, den Sie erstellen möchten.

Feld-Kriterien	Beschreibung	Wert
Protokoll	Das Routing-Protokoll, mit dem eine Route erlernt wird. Wählen Sie das Protokoll aus der Dropdownliste aus.	Beliebig, OSPF, BGP
Routingdomäne	Geben Sie die Routingdomäne aus der Dropdownliste ein	• Routing-Domainname
Quell-Router	Die IP-Adresse des Quellrouters gilt nur für iBGP	• IP-Adresse
Ziel-IP	Die IP-Adresse und Subnetzmaske des Ziels einer Route	• IP-Adresse
IP-Gruppe verwenden	Aktivieren Sie bei Bedarf das Kontrollkästchen **IP-Gruppe verwenden** .	• IP-Gruppe

Feld-Kriterien	Beschreibung	Wert
Präfix	Um Routen nach Präfix abzugleichen, wählen Sie ein Übereinstimmungs-Prädikat aus dem Menü und geben Sie ein Routen-Präfix in das angrenzende Feld ein	• eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to
Weiter Hop	Die IP-Adresse des nächsten Hop	• IP-Adresse
Routen-Tag	Das OSPF-Route-Tag, mit dem der Filter übereinstimmt. OSPF-Route-Tags verhindern Routingschleifen bei gegenseitiger Umverteilung zwischen OSPF und anderen Protokollen	Numerischer Wert
Kosten	Die Routenkosten, mit denen OSPF-Routen für den Import übereinstimmen	Numerischer Wert
AS-Pfadlänge	Die AS-Pfadlänge, mit der BGP-Routen für den Import übereinstimmt	Numerischer Wert
Route zu Citrix Appliances exportieren	Aktivieren Sie das Kontrollkästchen, um diesen Filter zu aktivieren. Andernfalls wird der Filter ignoriert	Ohne
Einschließen	Aktivieren Sie das Kontrollkästchen, um Routen einzuschließen, die diesem Filter entsprechen. Ansonsten werden passende Routen ignoriert	Ohne
Berechtigung basierend auf Gateway	Aktivieren Sie dieses Kontrollkästchen, und geben Sie den **Diensttyp**, den **Dienstnamen** und den **Pfad** aus der Dropdown-Liste an.	Diensttyp (Lokal, Internet, Intranet, GRE-Tunnel, Passthrough), Dienstname und Pfad

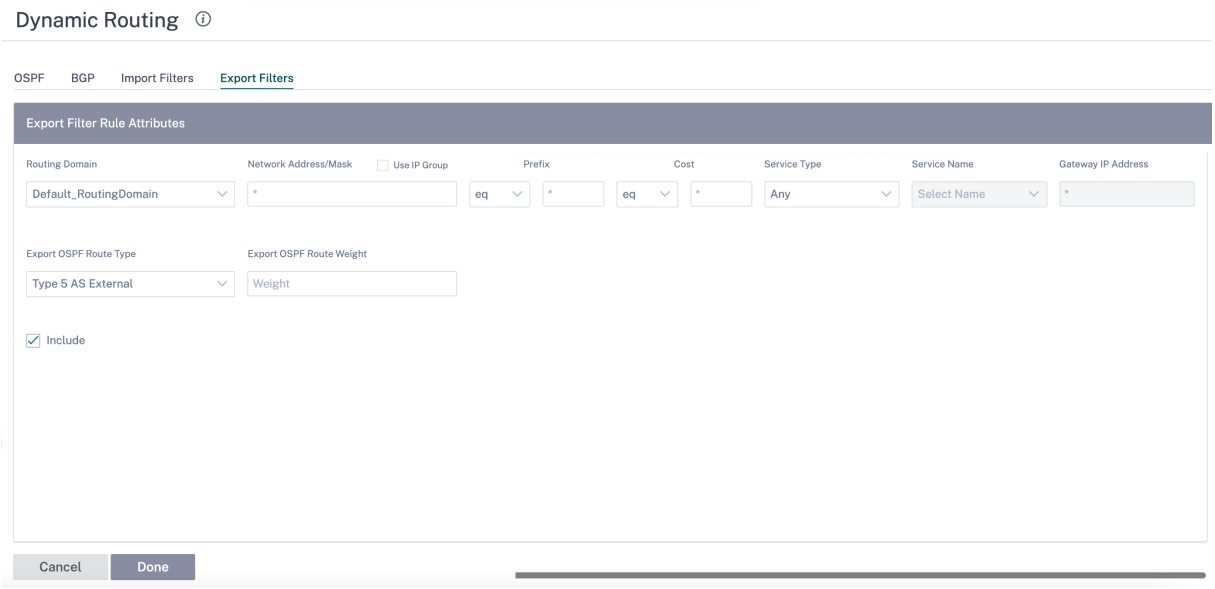
Feld-Kriterien	Beschreibung	Wert
Berechtigung basierend auf Pfad	Aktivieren Sie dieses Kontrollkästchen, und geben Sie den **Diensttyp**, den **Dienstnamen** und den **Pfad** aus der Dropdown-Liste an.	Diensttyp (Lokal, Internet, Intranet, GRE-Tunnel, Passthrough), Dienstname und Pfad

Klicken Sie auf **Fertig** um die Einstellungen zu speichern

Filter exportieren

Exportfilter werden verwendet, um Routen für Werbung mit OSPF- und BGP-Protokollen basierend auf bestimmten Übereinstimmungen ein- oder auszuschließen Kriterien. Exportfilterregeln sind die Regeln, die erfüllt werden müssen, wenn SD-WAN-Routen über dynamische Routingprotokolle geworben werden. Alle Routen werden standardmäßig an Peers angekündigt.

Klicken Sie auf **+ Regel exportieren**.



Verwenden Sie die folgenden Kriterien, um jeden Exportfilter zu erstellen, den Sie erstellen möchten.

Feld-Kriterien	Beschreibung	Wert
Routingdomäne	Wählen Sie die Routingdomäne aus der Dropdownliste aus	Routing-Domäne

Feld-Kriterien	Beschreibung	Wert
Netzwerkadresse/Maske	Geben Sie die **IP-Adresse** und Subnetzmaske des konfigurierten Netzwerkobjekts ein, das das Netzwerk der Route beschreibt	• IP-Adresse
IP-Gruppe verwenden	Aktivieren Sie bei Bedarf das Kontrollkästchen und geben Sie die IP-Gruppe aus der Dropdown-Liste ein.	• IP-Gruppe
Präfix	Um Routen nach Präfix abzugleichen, wählen Sie ein Übereinstimmungs-Prädikat aus dem Menü und geben Sie ein Routen-Präfix in das angrenzende Feld ein	• eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to
Kosten	Die Methode (Prädikat) und die SD-WAN-Routenkosten, die verwendet werden, um die Auswahl der exportierten Routen einzugrenzen	Numerischer Wert
Servicetyp	Wählen Sie die Diensttypen aus, die übereinstimmenden Routen aus einer Liste von Citrix SD-WAN-Diensten zugewiesen sind	Beliebig, Lokal, Virtueller Pfad, Internet, Intranet, LAN GRE Tunnel, LAN IPsec Tunnel
Standort-/Dienstname	Geben Sie für Intranet, LAN GRE Tunnel und LAN IPsec-Tunnel den Namen des konfigurierten Diensttyps an, der verwendet werden soll.	Textzeichenfolge
Gateway-IP-Adresse	Wenn Sie den LAN GRE-Tunnel als Servicetyp wählen, geben Sie die Gateway-IP für den Tunnel ein.	IP-Adresse

Feld-Kriterien	Beschreibung	Wert
OSPF-Routentyp exportieren	Kündigen Sie die Citrix SD-WAN-Route zu OSPF-Nachbarn als Typ 1 Intra-Area-Route oder als externe Typ-5-Route an. Die Standardroute wird immer als externe Route Typ 5 zu normalen Gebieten und Typ-3-Zusammenfassungsroute zu Stub-Bereichen angekündigt.	Routen-Typ
Exportieren Sie OSPF Routengewicht	Beim Exportieren von Citrix SD-WAN-Routen nach OSPF und das Gewicht für die Citrix SD-WAN-Kosten jeder Route als Gesamtkosten.	Gewicht
Einschließen	Aktivieren Sie das Kontrollkästchen, um Routen einzuschließen, die diesem Filter entsprechen. Ansonsten werden passende Routen ignoriert	Ohne

Die Routenfilterung wird auf LAN-Routen und virtuellen Pfadrouten in einem SD-WAN-Netzwerk (Data Center/Branch) implementiert und über BGP und OSPF an ein Nicht-SD-WAN-Netzwerk angekündigt.

Sie können bis zu 512 Exportfilter und 512 Importfilter konfigurieren. Dies ist das Gesamtlimit, nicht pro Routingdomänenlimit.

Übersetzung von Netzwerkadressen

October 21, 2022

Network Address Translation (NAT) auf der SD-WAN-Appliance führt eine IP-Adresserhaltung durch, um die begrenzte Anzahl registrierter IP-Adressen beizubehalten. Es übersetzt die privaten Adressen im internen Netzwerk in eine legale öffentliche Adresse und verbindet Ihr privates SD-WAN-Netzwerk

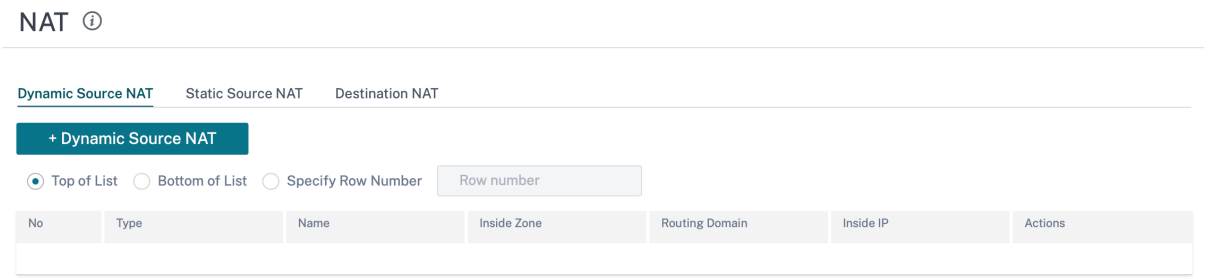
mit dem öffentlichen Internet. Die öffentliche IP-Adresse wird für die Kommunikation über das Internet verwendet. NAT sorgt auch für zusätzliche Sicherheit, indem nur eine Adresse für das gesamte Netzwerk im Internet Werbung gemacht wird und das gesamte interne Netzwerk versteckt.

Sie können die folgenden NAT-Typen konfigurieren:

- Dynamisches Quell-NA
- Statische NAT
- Ziel-NAT

> **Hinweis:**
>
> Die NAT-Funktion kann nur auf Standortebene konfiguriert werden. Es gibt keine globale Konfiguration (Vorlagen) für NAT.

Um NAT für einen Standort mithilfe des Citrix SD-WAN Orchestrator Service zu konfigurieren, navigieren Sie auf Standortebene zu **Konfiguration > Erweiterte Einstellungen > NAT**.



Eingehende und ausgehende NAT

Die Richtung für eine Verbindung kann entweder von innen nach außen oder von außen nach innen sein. Wenn eine NAT-Regel erstellt wird, können Sie die Richtung mithilfe des Kontrollkästchens **Bei Empfang** definieren. Wenn das Kontrollkästchen aktiviert ist, wird die Richtung als **Eingehend** konfiguriert, und wenn das Kontrollkästchen deaktiviert ist, wird die Richtung als **Ausgehend**konfiguriert.

- **Inbound**: Die Quelladresse wird für Pakete übersetzt, die für den Dienst empfangen wurden. Die Zieladresse wird für Pakete übersetzt, die über den Dienst übertragen werden. Beispiel: Internetdienst-zu-LAN-Dienst —Für empfangene Pakete (Internet zu LAN) wird die Quell-IP-Adresse übersetzt. Bei übertragenen Paketen (LAN to Internet) wird die Ziel-IP-Adresse übersetzt.
- **Ausgehend**: Die Zieladresse wird für Pakete übersetzt, die für den Dienst empfangen wurden. Die Quelladresse wird für Pakete übersetzt, die über den Dienst übertragen werden. Beispielsweise LAN-Dienst zum Internetdienst —für übertragene Pakete (LAN zu Internet) wird die Quell-

IP-Adresse übersetzt. Bei empfangenen Paketen (Internet to LAN) wird die Ziel-IP-Adresse übersetzt.

Zonenableitung

Die Quell- und Ziel-Firewallzonen für den eingehenden oder ausgehenden Datenverkehr dürfen nicht identisch sein. Wenn sowohl die Quell- als auch die Ziel-Firewallzonen identisch sind, wird NAT nicht für den Datenverkehr ausgeführt.

Für ausgehende NAT wird die externe Zone automatisch vom Dienst abgeleitet. Jeder Dienst auf SD-WAN ist standardmäßig einer Zone zugeordnet. Beispielsweise ist der Internetdienst auf einer vertrauenswürdigen Internetverbindung mit der vertrauenswürdigen Internetzone verknüpft. Ebenso wird für einen eingehenden NAT die innere Zone vom Dienst abgeleitet.

Für einen Virtual Path Service NAT Zonenableitung nicht automatisch erfolgt, müssen Sie manuell die innere und äußere Zone eingeben. NAT wird nur für den Verkehr durchgeführt, der zu diesen Zonen gehört. Zonen können nicht für virtuelle Pfade abgeleitet werden, da sich innerhalb der virtuellen Pfadsubnetze möglicherweise mehrere Zonen befinden.

Dynamisches Quell-NA

Dynamic Source NAT ist eine Viele-zu-Eins-Zuordnung einer privaten IP-Adresse oder Subnetze innerhalb des SD-WAN-Netzwerks zu einer öffentlichen IP-Adresse oder einem Subnetz außerhalb des SD-WAN-Netzwerks. Es ermöglicht mehreren Hosts, ihre Quell-IP-Adressen in dieselbe öffentliche IP-Adresse mit unterschiedlichen Portnummern übersetzen zu lassen. Port Restricted NAT verwendet denselben externen Port für alle Übersetzungen, die sich auf eine interne IP-Adresse und ein Portpaar beziehen. Der Datenverkehr aus verschiedenen Zonen und Subnetzen über vertrauenswürdige (innerhalb) IP-Adressen im LAN-Segment wird über eine einzelne öffentliche (externe) IP-Adresse gesendet.

> **Hinweis:**
>
> Dynamische NAT-Übersetzungen erlauben den gesamten wechselseitigen Datenverkehr für eine vom internen Netzwerk initiierte Sitzung. Um diese Verbindungen zu filtern, fügen Sie Filterrichtlinien für den ausgehenden Datenverkehr hinzu.

Übersetzung der Port-Adresse

Dynamic NAT führt Port Address Translation (PAT) zusammen mit der IP-Adressenübersetzung durch. Portnummern werden verwendet, um zu unterscheiden, welcher Datenverkehr zu welcher IP-Adresse gehört. Eine einzelne öffentliche IP-Adresse wird für alle internen privaten IP-Adressen verwendet,

jeder privaten IP-Adresse wird jedoch eine andere Portnummer zugewiesen. PAT ist eine kostengünstige Möglichkeit, mehrere Hosts die Verbindung mit dem Internet über eine einzelne öffentliche IP-Adresse zu ermöglichen.

Das Kontrollkästchen **Symmetrisch** definiert die PAT-Konfiguration. Wenn beim Konfigurieren von NAT-Regeln das Kontrollkästchen aktiviert ist, wird symmetrische NAT konfiguriert, und wenn diese Option deaktiviert ist, wird Port Restricted NAT im Back-End konfiguriert.

- **Port restricted**: Port Restricted NAT verwendet denselben externen Port für alle Übersetzungen, die sich auf eine Inside IP Address und Port-Paar beziehen. Dieser Modus wird normalerweise verwendet, um Internet-P2P-Anwendungen zuzulassen.
- **Symmetrisch**: Symmetric NAT verwendet denselben externen Port für alle Übersetzungen, die sich auf eine Innen-IP-Adresse, einen Innenanschluss, eine externe IP-Adresse und ein Outside Port Tupel beziehen. Dieser Modus wird normalerweise verwendet, um die Sicherheit zu erhöhen oder die maximale Anzahl von NAT-Sitzungen zu erweitern.

Port-Weiterleitung

Dynamische NAT mit Portweiterleitung ermöglicht dem Datenverkehr von einem externen Netzwerk den Zugriff auf bestimmte Hosts und Ports im internen Netzwerk, ohne dass die Sitzung von innen initiiert wird. Dies wird normalerweise für Hosts wie Webserver verwendet.

Sobald der dynamische NAT konfiguriert ist, können Sie die Portweiterleitungsrichtlinien definieren. Konfigurieren Sie dynamische NAT für die IP-Adressenübersetzung und definieren Sie die Portweiterleitungsrichtlinie, um einen externen Port einem internen Port zuzuordnen. Dynamische NAT-Portweiterleitung wird normalerweise verwendet, um Remotehosts die Verbindung zu einem Host oder Server in Ihrem privaten Netzwerk zu ermöglichen.

Dynamic Source NAT konfigurieren

Um dynamische NAT für einen Standort mithilfe des Citrix SD-WAN Orchestrator Service zu konfigurieren, navigieren Sie auf Standortebene zur Registerkarte **Konfiguration > Erweiterte Einstellungen > NAT > Dynamische Quell-NAT** . Klicken Sie **+ Dynamic Source NAT**.

- **Typ**: Die SD-WAN-Diensttypen, auf die die NAT-Richtlinie angewendet wird. Für statische NAT werden lokale, virtuelle Pfade, Internet, Intranet und Routingübergreifende Domänendienste unterstützt.
- **Routingdomäne**: Wählen Sie die Routingdomäne aus, für die die ausgewählte Übersetzung gilt.
- **IP-Adresstyp**: Wählen Sie den IPv4- oder IPv6-Adresstyp basierend auf Ihren Präferenzen aus.
- **Zieldienst**: Geben Sie einen Namen für den Dienst an, der dem Diensttyp entspricht.
- **Inside Zone**: Der Match-Typ der Inside Firewall Zone, aus dem das Paket stammen muss, um die Übersetzung zu ermöglichen.

- **Innere IP/Präfix**: Die interne IP-Adresse und das Präfix, in die übersetzt werden muss, wenn die Übereinstimmungskriterien erfüllt sind.
- **Externe IP**: Die externe IP-Adresse und das Präfix, in das die interne IP-Adresse übersetzt wird, wenn die Übereinstimmungskriterien erfüllt sind. Für ausgehenden Datenverkehr mit Internet- und Intranetdiensten wird die konfigurierte WAN-Link-IP-Adresse dynamisch als externe IP-Adresse gewählt.
- **Portparität**: Wenn diese Option aktiviert ist, behalten externe Ports für NAT-Verbindungen die Parität bei (auch wenn der innere Port gerade ist, ungerade, wenn der externe Port ungerade ist).
- **Responder-Route binden**: Stellt sicher, dass der Antwortdatenverkehr über denselben Dienst gesendet wird, auf dem er empfangen wurde, um ein asymmetrisches Routing zu vermeiden.
- **Related zulassen**: Datenverkehr im Zusammenhang mit dem Flow zulassen, der der Regel entspricht. Beispielsweise bezieht sich die ICMP-Umleitung auf den spezifischen Fluss, der mit der Richtlinie übereinstimmte, wenn ein Fehler im Zusammenhang mit dem Flow aufgetreten ist.
- **IPSec-Passthrough**: Ermöglicht die Übersetzung einer IPSec-Sitzung (AH/ESP).
- **GRE/PPTP-Passthrough**: Stellt sicher, dass der Antwortdatenverkehr über denselben Dienst gesendet wird, auf dem er empfangen wird, um asymmetrisches Routing zu vermeiden.
- **Bei Empfang**: Wenn dieses Kontrollkästchen aktiviert ist, wird eingehender NAT konfiguriert. Wenn diese Option deaktiviert ist, ist Outbound NAT konfiguriert.
- **Symmetrisch**: Wenn dieses Kontrollkästchen aktiviert ist, wird die symmetrische NAT konfiguriert. Wenn diese Option deaktiviert ist, ist NAT mit Portbeschränkung

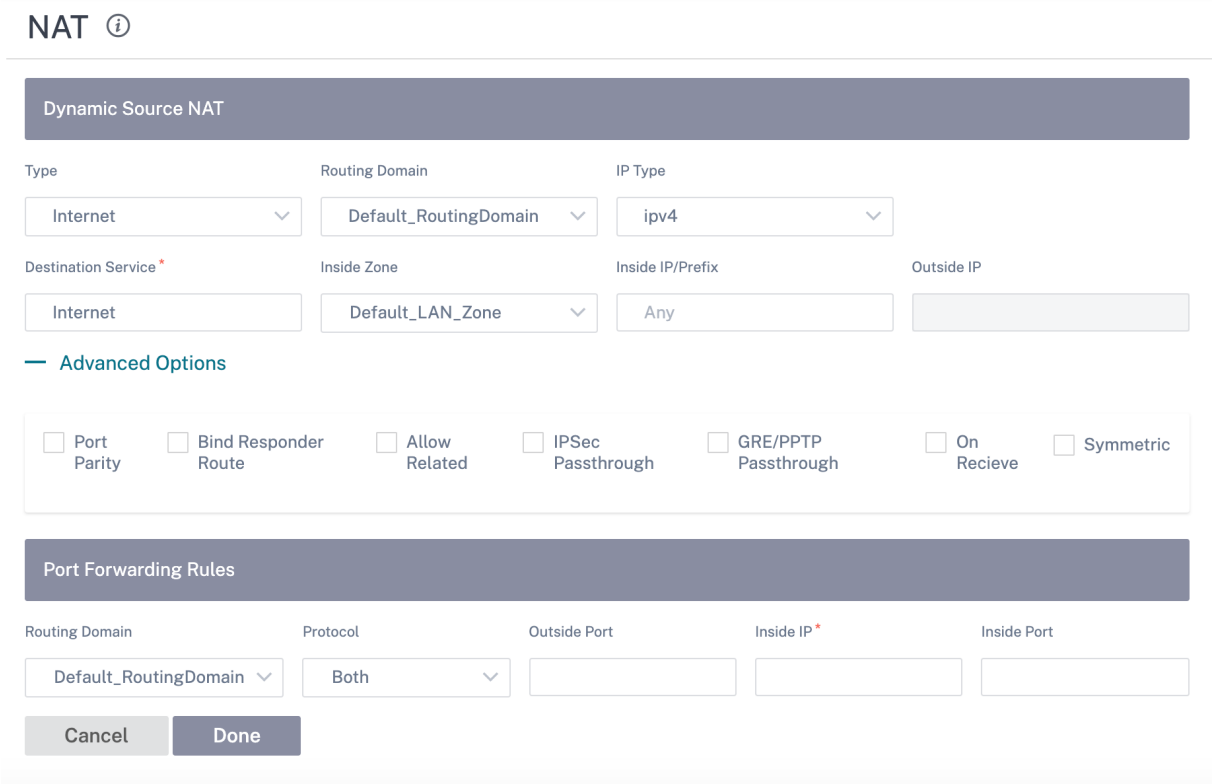
Regeln für Portweiterleitung:

- **Routingdomäne**: Wählen Sie die Routingdomäne aus, für die die ausgewählte Übersetzung gilt.
- **Protokoll**: TCP, UDP oder beides.
- **Externer Port**: Der externe Port, der an den internen Port weitergeleitet wird.
- **Interne IP**: Die interne Adresse zum Weiterleiten übereinstimmender Pakete.
- **Interner Port**: Der interne Port, an den der externe Port weitergeleitet wird.

Jede Portweiterleitungsregel hat eine übergeordnete NAT-Regel. Die externe IP-Adresse wird der übergeordneten NAT-Regel entnommen.

> **Hinweis**
>
> Die Benutzeroberfläche des Citrix SD-WAN Orchestrator Service zeigt automatisch erstellte NAT-Regeln an, wenn die folgenden Bedingungen erfüllt sind:
>
> - Der Internetdienst ist auf der Site aktiviert.
> - Die dynamische IPv4-Quell-NAT-Regel für ausgehenden Internet ist am Standort nicht konfiguriert.

- Mindestens eine WAN-Verbindung befindet sich auf einer nicht vertrauenswürdigen Schnittstelle, oder das Internet ist auf allen Routingdomänen aktiviert.



Statische Quelle NAT

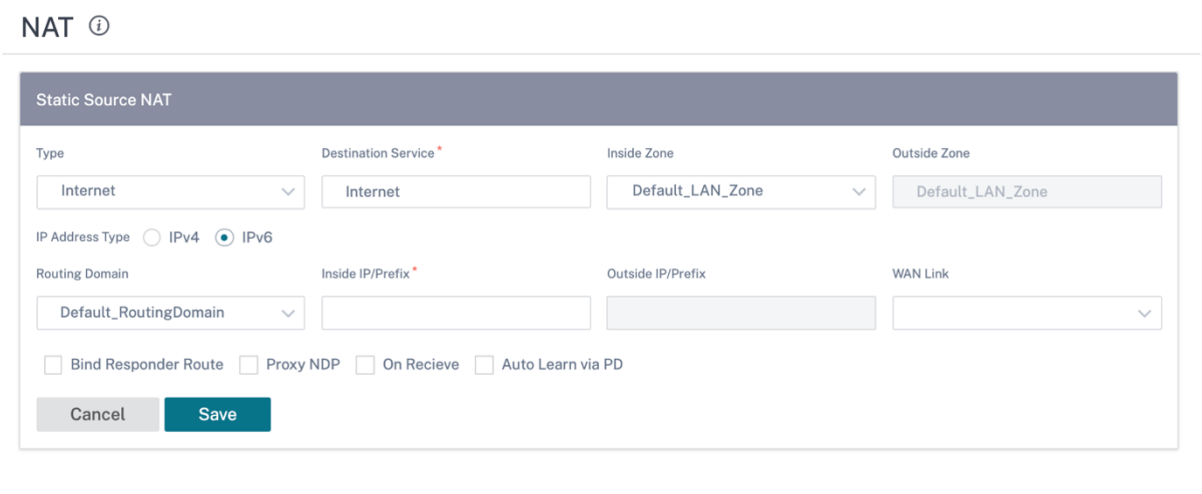
Statische NAT ist eine 1:1 -Zuordnung einer privaten IP-Adresse oder eines Subnetzes innerhalb des SD-WAN-Netzwerks zu einer öffentlichen IP-Adresse oder Subnetz außerhalb des SD-WAN-Netzwerks. Konfigurieren Sie Static NAT, indem Sie manuell die innere IP-Adresse und die externe IP-Adresse eingeben, in die sie übersetzt werden muss. Sie können statische NAT für die lokalen, virtuellen Pfade, Internet, Intranet und Inter-Routing-Domänendienste konfigurieren.

Statische Quell-NAT

Um statische NAT für einen Standort mithilfe des Citrix SD-WAN Orchestrator Service zu konfigurieren, navigieren Sie auf Standortebene zur Registerkarte **Konfiguration > Erweiterte Einstellungen > NAT > Statische Quell-NAT** . Klicken Sie auf **+ Static Source NAT**

- **Typ**: Die SD-WAN-Diensttypen, auf die die NAT-Richtlinie angewendet wird. Für statische NAT werden lokale, virtuelle Pfade, Internet-, Intranet- und Routingdomänendienste unterstützt.
- **Zieldienst**: Geben Sie einen Namen für den Dienst an, der dem Diensttyp entspricht.

- **Inside Zone**: Der Match-Typ der Inside Firewall Zone, aus dem das Paket stammen muss, um die Übersetzung zu ermöglichen.
- **Outside Zone**: Der Match-Typ der externen Firewall-Zone, aus dem das Paket stammen muss, um die Übersetzung zu ermöglichen.
- **IP-Adresstyp**: Wählen Sie den IPv4- oder IPv6-Adresstyp basierend auf Ihren Präferenzen aus.
- **Routingdomäne**: Wählen Sie die Routingdomäne aus, für die die ausgewählte Übersetzung gilt.
- **Innere IP/Präfix**: Die interne IP-Adresse und das Präfix, in die übersetzt werden muss, wenn die Übereinstimmungskriterien erfüllt sind.
- **Externe IP/Präfix**: Die externe IP-Adresse und das Präfix, in das die interne IP-Adresse übersetzt wird, wenn die Übereinstimmungskriterien erfüllt sind.
- **Responder-Route binden**: Stellt sicher, dass der Antwortdatenverkehr über denselben Dienst gesendet wird, auf dem er empfangen wurde, um ein asymmetrisches Routing zu vermeiden.
- **Proxy-ARP**: Stellt sicher, dass die Appliance auf lokale ARP-Anfragen nach der externen IP-Adresse reagiert.
- **Proxy-NDP**: Stellt sicher, dass die Appliance auf lokale NDP-Anforderungen für die externe IP-Adresse reagiert.
- **Bei Empfang**: Wenn dieses Kontrollkästchen aktiviert ist, wird eingehender NAT konfiguriert. Wenn diese Option deaktiviert ist, ist Outbound NAT konfiguriert.
- **Automatisches Lernen über PD**: Dieses Kontrollkästchen wird nur aktiviert, wenn Sie IPv6 als **IP-Adresstyp**auswählen. Wenn diese Option ausgewählt ist, fordert Citrix SD-WAN ein Präfix vom vorgeschalteten delegierenden Router an, und der delegierende Router antwortet mit einem Präfix an Citrix SD-WAN.



Statische NAT-Richtlinien für den IPv6-Internetdienst

Citrix SD-WAN unterstützt statische NAT-Richtlinien für den IPv6-Internetdienst ab Version 11.4.0. Eine statische NAT-Richtlinie für den IPv6-Internetdienst legt die Zuordnung eines internen Net-

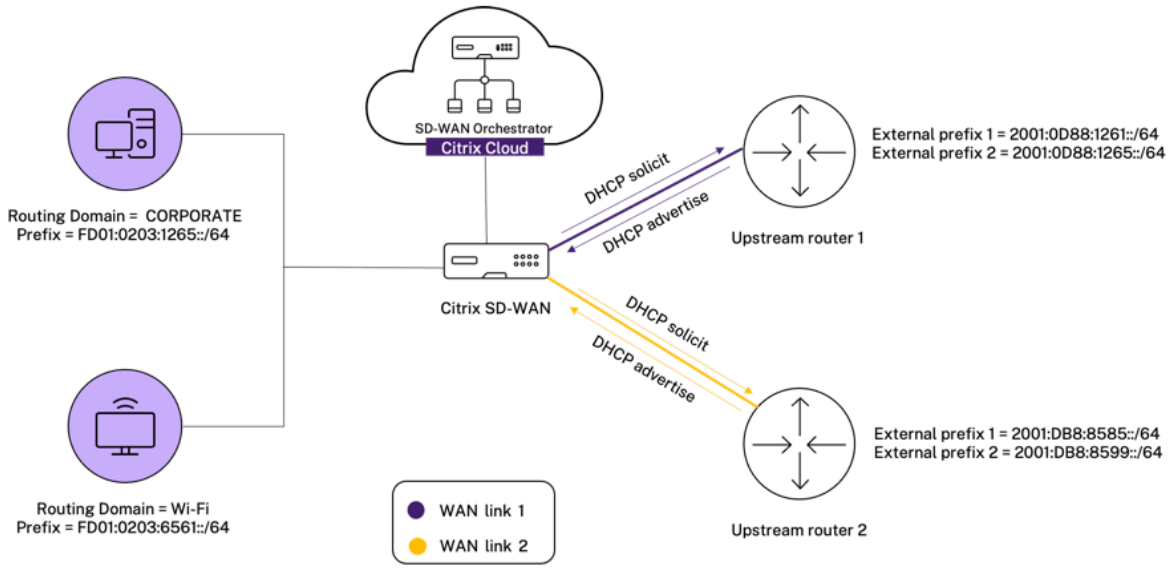
zwerkpräfixes zu einem externen Netzwerkpräfix fest. Die Anzahl der erforderlichen statischen NAT-Richtlinien hängt von der Anzahl der internen Netzwerke und der Anzahl der externen Netzwerke (WAN-Verbindungen) ab. Wenn es eine **M-Anzahl** von internen Netzwerken und eine Anzahl von **N** WAN-Verbindungen gibt, beträgt die Anzahl der erforderlichen statischen NAT-Richtlinien **M x N.**

Ab Citrix SD-WAN Version 11.4.0 können Sie beim Erstellen einer statischen NAT-Richtlinie entweder die externe IP-Adresse manuell eingeben oder **Auto Learn via PD**aktivieren. Wenn **Auto Learn via PD** aktiviert ist, empfängt die SD-WAN-Appliance delegierte Präfixe vom vorgeschalteten delegierenden Router über die DHCPv6-Präfixdelegierung. Vor Citrix SD-WAN Version 11.4.0 wurde die externe IP-Adresse automatisch vom Dienst abgeleitet und es gab keine Möglichkeit, die externe IP-Adresse manuell einzugeben. Wenn Sie eine Appliance auf 11.4.0 oder eine höhere Version aktualisieren und statische NAT-Richtlinien für den IPv6-Internetdienst konfiguriert haben, müssen Sie die Richtlinien manuell aktualisieren.

Beispiel für eine Konfiguration

In der folgenden Topologie ist die Citrix SD-WAN-Appliance mit 2 internen Netzwerken und 2 WAN-Verbindungen konfiguriert:

- Innerhalb von Netzwerk 1 befindet sich in der Routing-Domäne CORPORATE mit dem Netzwerkpräfix FD01:0203:6561::/64
- Innerhalb von Netzwerk 2 befindet sich in der Wi-Fi-Routing-Domäne mit dem Netzwerkpräfix FD01:0203:1265::/64
- Über WAN Link 1 empfängt die SD-WAN-Appliance vom Upstream-Delegierungsrouter über DHCPv6-Präfix-Delegation 2 delegierte Präfixe 2001:0D88:1261::/64 und 2001:0D88:1265::/64. Diese 2 delegierten Präfixe werden als externe Netzwerkpräfixe verwendet, wenn der Verkehr von den inneren Netzwerken die WAN-Verbindung 1 überträgt.
- Über WAN Link 2 empfängt die SD-WAN-Appliance vom Upstream-Delegierungsrouter über die DHCPv6-Präfix-Delegation 2 delegierte Präfixe 2001:DB8:8585::/64 und 2001:DB8:8599::/64. Diese 2 delegierten Präfixe werden als externe Netzwerkpräfixe verwendet, wenn der Verkehr von den inneren Netzwerken die WAN-Verbindung 2 überträgt.



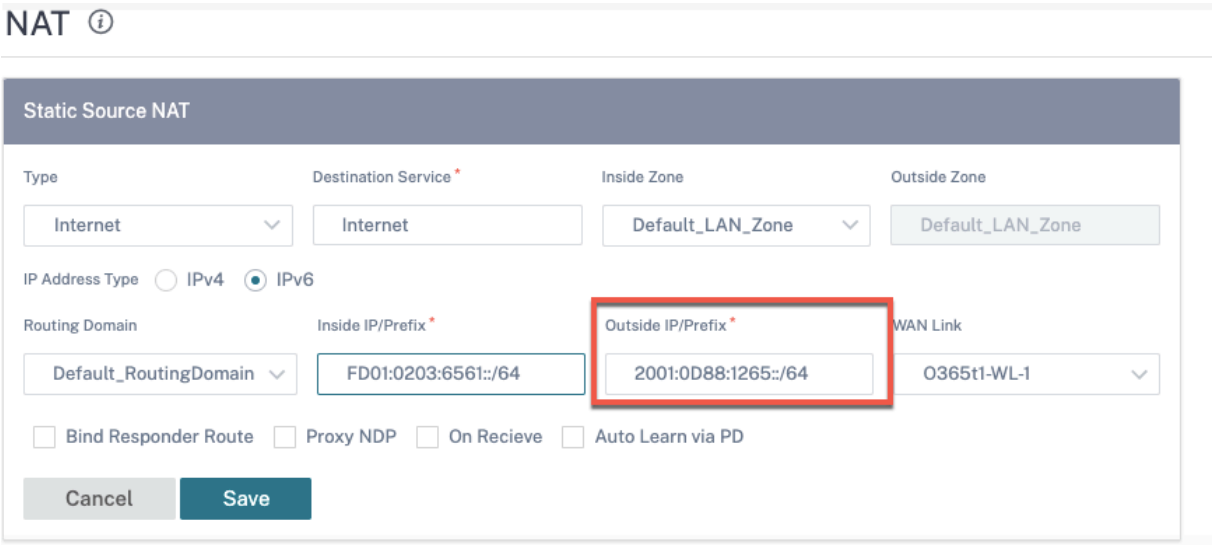
In diesem Szenario gibt es M=2 innerhalb von Netzwerken und N=2 WAN-Verbindungen. Daher beträgt die Anzahl der statischen NAT-Richtlinien, die für eine ordnungsgemäße Bereitstellung des IPv6-Internetdienstes erforderlich sind, 2 x 2 = 4. Diese 4 statischen NAT-Richtlinien spezifizieren die Adressübersetzung für:

- Innerhalb von Netzwerk 1 über WAN-Verbindung 1
- Innerhalb von Netzwerk 1 über WAN-Verbindung 2
- Innerhalb von Netzwerk 2 über WAN-Verbindung 1
- Innerhalb von Netzwerk 2 über WAN-Link 2

Um diese statischen NAT-Richtlinien zu konfigurieren, navigieren Sie auf Standortebene zu **Konfiguration > Erweiterte Einstellungen > NAT > Statische Quell-NAT**. Klicken Sie auf **+ Static Source NAT**

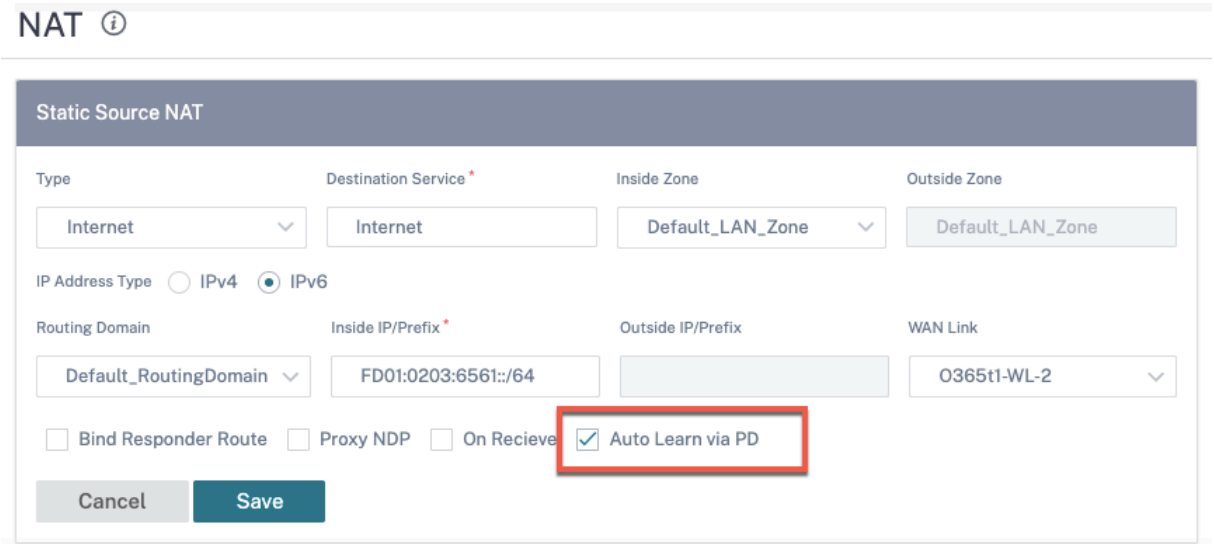
Stellen Sie beim Erstellen von NAT-Richtlinien sicher, dass Sie den **Typ** als **Internet** und den **IP-Adresstyp** als **IPv6**auswählen. Wählen Sie die WAN-Verbindung aus und geben Sie **im Feld Interne IP/Präfix** das interne Netzwerkpräfix ein (nur /64-Präfixe sind zulässig). Im Feld **Externe IP/Präfix** können Sie entweder das externe Netzwerkpräfix manuell eingeben oder das Kontrollkästchen **Auto Learn via PD** aktivieren.

Das Folgende ist ein Beispiel, bei dem die externe IP-Adresse manuell in die statische NAT-Richtlinie eingegeben wird.



Wenn Sie das Kontrollkästchen **Automatisches Lernen über PD** aktivieren, stellen Sie sicher, dass der Upstream-Router die DHCPv6-Präfixdelegierung unterstützt. Citrix SD-WAN fordert ein Präfix vom Delegierungsrouter der Originalautoren an, und der delegierende Router antwortet mit einem Präfix an Citrix SD-WAN. Citrix SD-WAN verwendet dieses delegierte Präfix, um die innere IP-Adresse in die externe IP-Adresse zu übersetzen.

Das Folgende ist ein Beispiel, bei dem **Auto Learn via PD** aktiviert ist, sodass das externe Netzwerkpräfix durch DHCPv6-Präfix-Delegation abgerufen wird.



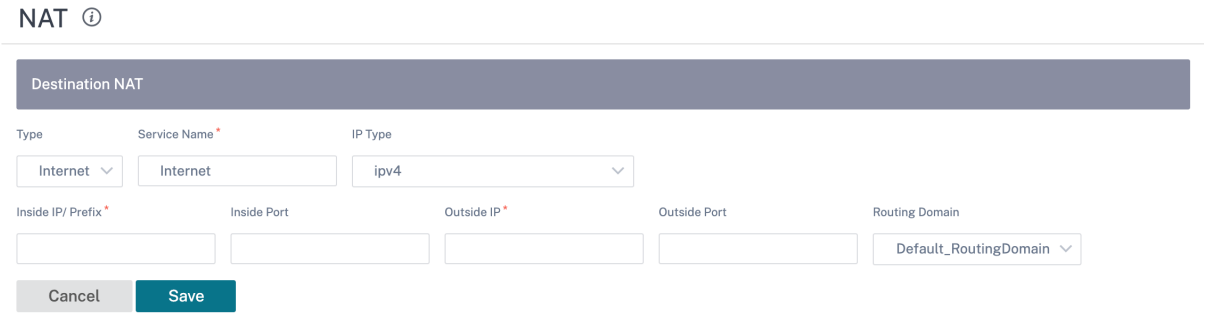
Ziel-NAT

Ziel-NAT-Richtlinien ermöglichen die Konfiguration von Richtlinien für die Netzwerkadressübersetzung zwischen einzelnen Hosts oder Subnetzen.

> **Hinweis**
>
> - Während sowohl eingehende als auch ausgehende Übersetzungen gleichzeitig für einen Dienst konfiguriert werden können, wird nur die erste, die übereinstimmt, verwendet. Mehrere Übersetzungen können auftreten, wenn eine Regel für den Dienst existiert, auf der ein Paket empfangen wird und der Dienst, an den ein Paket gesendet wird.
> - Ziel-NAT-Übersetzungen gelten nur für Datenverkehr, der vom lokalen Dienst stammt.

Um diese Ziel-NAT-Richtlinien zu konfigurieren, navigieren Sie auf Standortebene zu **Konfiguration > Erweiterte Einstellungen > NAT > Ziel-NAT**. Klicken Sie auf **+ Ziel NAT**.

- **Typ**: Die SD-WAN-Diensttypen, auf die die NAT-Richtlinie angewendet wird. Für statische NAT werden lokale, virtuelle Pfade, Internet-, Intranet- und Routingdomänendienste unterstützt.
- **Dienstname**: Geben Sie einen Namen für den Dienst an, der dem Diensttyp entspricht.
- **IP-Typ**: Wählen Sie den IPv4- oder IPv6-Adresstyp basierend auf Ihren Präferenzen aus.
- **Interner Port**: Der interne Port, an den der externe Port weitergeleitet wird.
- **Externe IP**: Die externe IP-Adresse und das Präfix, in das die interne IP-Adresse übersetzt wird, wenn die Übereinstimmungskriterien erfüllt sind. Für ausgehenden Datenverkehr mit Internet- und Intranetdiensten wird die konfigurierte WAN-Link-IP-Adresse dynamisch als externe IP-Adresse gewählt.
- **Externer Port**: Der externe Port, der an den internen Port weitergeleitet wird.
- **Routingdomäne**: Wählen Sie die Routingdomäne aus, für die die ausgewählte Übersetzung gilt.
- **Bei Empfang**: Wenn dieses Kontrollkästchen aktiviert ist, wird eingehender NAT konfiguriert. Wenn diese Option deaktiviert ist, ist Outbound NAT konfiguriert.

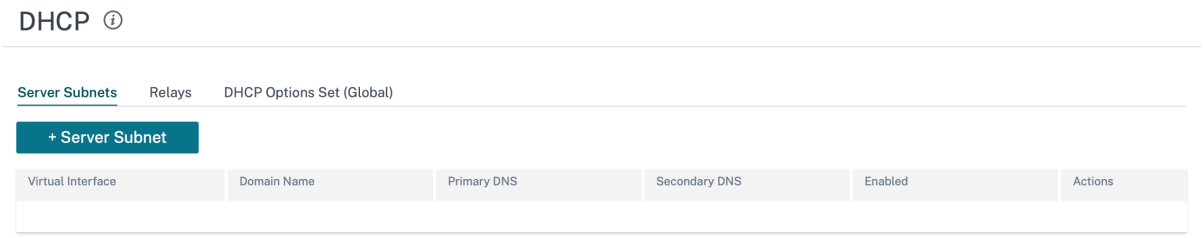


Dynamisches Host-Konfigurationsprotokoll

October 21, 2022

Sie können Ihre SD-WAN-Appliances entweder als **DHCP-Server** oder als **DHCP-Relay-Agent**konfigurieren. Mit der DHCP-Serverfunktion können Geräte im selben Netzwerk wie die LAN/WAN-Schnittstelle

der SD-WAN-Appliance ihre IP-Konfiguration von der SD-WAN-Appliance abrufen. Mit der DHCP-Relayfunktion können Ihre SD-WAN-Appliances DHCP-Pakete zwischen DHCP-Client und Server weiterleiten.



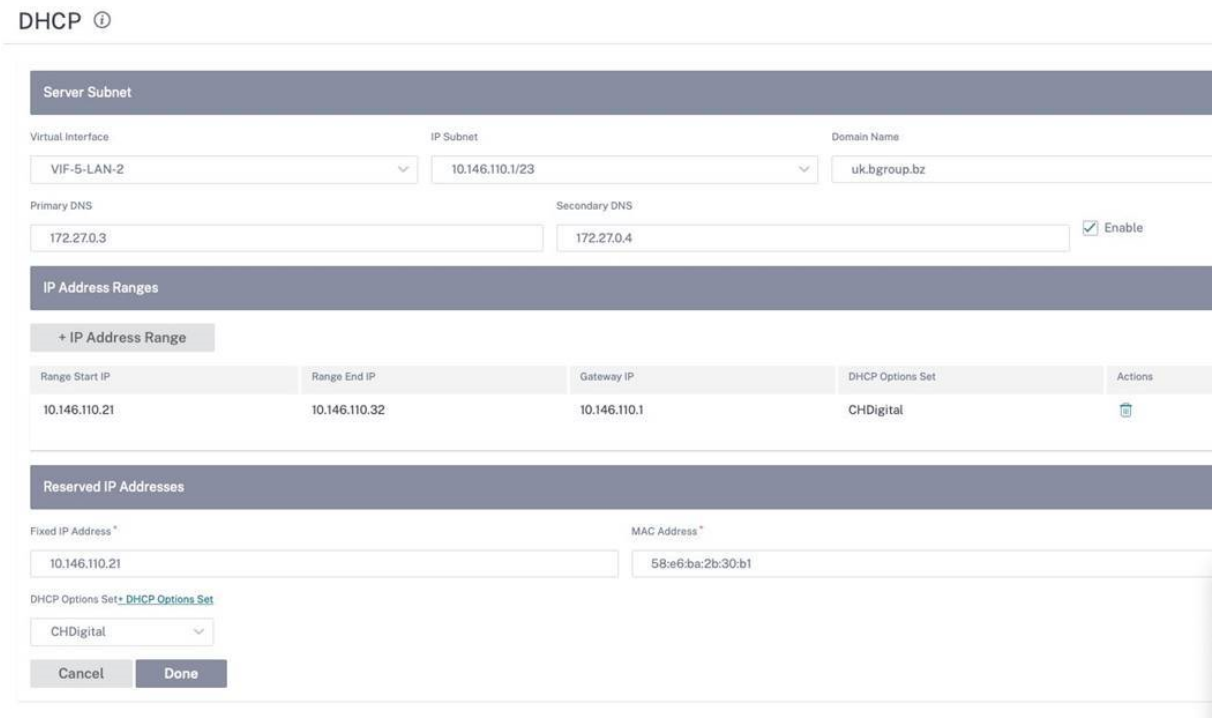
DHCP-Server

Citrix SD-WAN Appliances können als DHCP-Server konfiguriert werden. Es kann DHCP-Clients IP-Adressen aus bestimmten Adresspools innerhalb des Netzwerks zuweisen und verwalten.

Der DHCP-Server kann so konfiguriert werden, dass er andere Parameter wie die DNS-IP-Adresse und das Standardgateway zuweist. Der DHCP-Server akzeptiert Adressenzuweisungsanforderungen und Verlängerungen. Der DHCP-Server akzeptiert auch Übertragungen von lokal angeschlossenen LAN-Segmenten oder von DHCP-Anforderungen, die von anderen DHCP-Relay-Agents im Netzwerk weitergeleitet werden.

Um den DHCP-Server zu konfigurieren, navigieren Sie auf der Seite Site-Konfiguration auf Standortebene zu **Konfiguration > Erweiterte Einstellungen > DHCP > Serversubnetze** > klicken Sie auf **+ Serversubnetz**.

Wählen Sie die **virtuelle Schnittstelle** aus, die für den Empfang der DHCP-Anfragen verwendet werden soll. Das IP-Subnetz, für das der DHCP-Server die IP-Adressen bereitstellt, wird automatisch aufgefüllt.



Geben Sie den **Domainnamen**, das **primäre DNS**und das **sekundäre DNS**ein. Der DHCP-Server leitet diese Informationen an die DHCP-Clients weiter.

Konfigurieren Sie dynamische IP-Adresspools, die zur Zuweisung von IP-Adressen zu Clients verwendet werden. Geben Sie den Start-und Endbereich der IP-Adresse an und wählen Sie den **DHCP-Optionssatz**aus.

> **Hinweis**
>
> Der DHCP-Optionssatz besteht aus Gruppen von DHCP-Einstellungen, die auf einzelne IP-Adressbereiche angewendet werden können. Weitere Informationen finden Sie unter DHCP-Optionssatz.

Legen Sie die reservierte IP-Adresse fest, indem Sie einzelne Hosts, die eine feste IP-Adresse benötigen, ihrer MAC-Adresse zuordnen. Geben Sie die **feste IP-Adresse**und die **MAC-Adresse**ein und wählen Sie einen **DHCP-Optionssatz**aus.

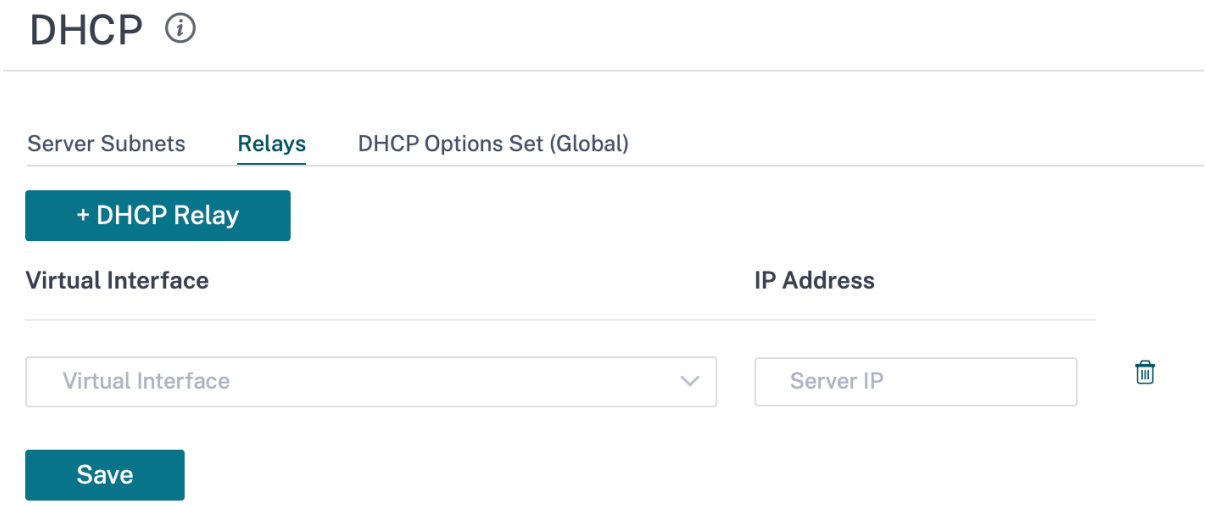
> **Hinweis**
>
> Für reservierte IP-Adressen wird die **Gateway-IP** festgelegt, indem die **Router-Option** im **DHCP-Optionssatz konfiguriert wird**.

DHCP-Relais

Die Citrix SD-WAN-Appliance kann als DHCP-Relay konfiguriert werden. Es leitet DHCP-Anfragen und -Antworten zwischen den lokalen DHCP-Clients und einem Remote-DHCP-Server weiter.

Es ermöglicht lokalen Hosts, dynamische IP-Adressen vom Remote-DHCP-Server zu erfassen. Der Relay-Agent empfängt DHCP-Nachrichten und generiert eine neue DHCP-Nachricht, die auf einer anderen Schnittstelle gesendet wird.

Um den DHCP-Server zu konfigurieren, navigieren Sie auf der Seite Site-Konfiguration zu **Konfiguration > Erweiterte Einstellungen > DHCP > Relays** klicken Sie auf **+ DHCP-Relay**.



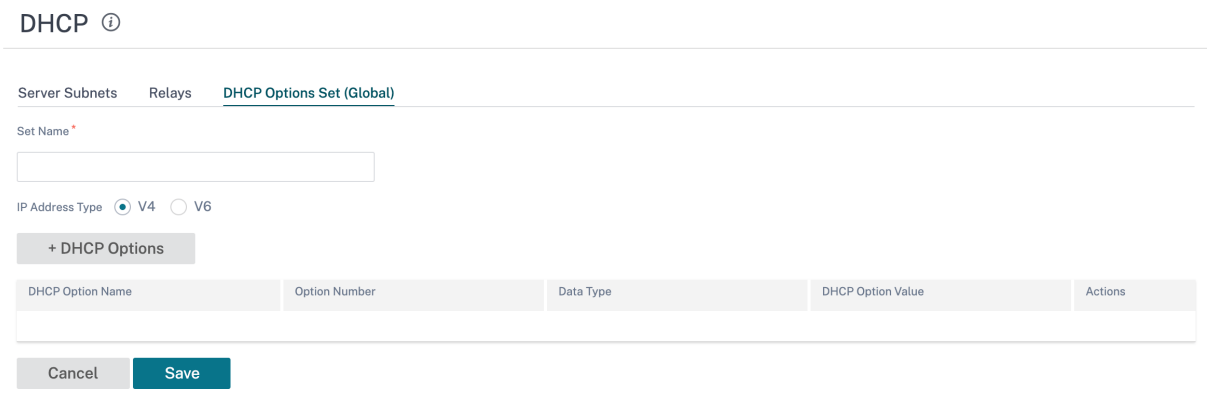
Wählen Sie eine **virtuelle Schnittstelle** aus, die mit einem Remote-DHCP-Server kommuniziert. Geben Sie die **DHCP-Server-IP** ein, die das Relay verwendet, um die Anfrage und Antwort von den Clients weiterzuleiten.

Sie können ein einzelnes **DHCP-Relay** mithilfe einer gemeinsamen virtuellen Netzwerkschnittstelle konfigurieren und es auf mehrere DHCP-Server verweisen.

Festgelegte DHCP-Optionen

DHCP-Optionen sind eine Gruppe von DHCP-Konfigurationen, die auf einzelne IP-Adressbereiche oder einen einzelnen Host angewendet werden können.

Legen Sie einen Namen für das DHCP-Optionsprofil fest und wählen Sie den **IP-Adresstyp**aus. Klicken Sie auf **+ DHCP-Optionssatz** und wählen Sie einen DHCP-Optionsnamen aus der Liste aus. Die Optionsnummer ist vorkonfiguriert. Für benutzerdefinierte Optionen liegt der Bereich zwischen 224 und 254. Wählen Sie einen **Datentyp** aus, und geben Sie einen **Wert** für die Option ein.



WAN-Link-IP-Adressen-Lernen über DHCP-Client

Citrix SD-WAN-Appliances unterstützen das Erlernen von WAN-Link-IP-Adressen durch DHCP-Clients. Diese Funktionalität reduziert den Umfang der manuellen Konfiguration, die für die Bereitstellung von SD-WAN-Appliances erforderlich ist, und senkt die ISP-Kosten, da keine statischen IP-Adressen gekauft werden müssen. SD-WAN-Appliances können dynamische IP-Adressen für WAN-Links auf nicht vertrauenswürdigen Schnittstellen abrufen. Dadurch entfällt die Notwendigkeit, dass ein zwischengeschalteter WAN-Router diese Funktion ausführen kann.

> **Hinweise**
>
> - DHCP-Client kann nur für nicht vertrauenswürdige, nicht überbrückte Schnittstellen konfiguriert werden, die als Clientknoten konfiguriert sind.
> - Der DHCP-Client und der Datenport können nur auf MCN/RCN aktiviert werden, wenn die öffentliche IP-Adresse konfiguriert ist.
> - Die Bereitstellung von Einarm- oder Richtlinienbasiertem Routing (PBR) wird auf dem Standort mit der DHCP-Clientkonfiguration nicht unterstützt.
> - DHCP-Ereignisse werden nur aus Sicht des Clients protokolliert und es werden keine DHCP-Serverprotokolle generiert.

Informationen zum Konfigurieren von DHCP für eine nicht vertrauenswürdige virtuelle Schnittstelle im Fail-to-Block-Modus und Fail-to-Wire-Modus finden Sie unter Konfiguration auf Site-Ebene.

Multicast-Routing

October 21, 2022

Multicast-Routing ermöglicht eine effiziente Verteilung des 1:n-Datenverkehrs. Eine Multicastquelle sendet Multicast-Datenverkehr in einem einzelnen Stream an eine Multicast-Gruppe. Die Multicastgruppe enthält Empfänger wie Hosts und angrenzende Router, die das IGMP-Protokoll für die Multicastkommunikation verwenden. Voice over IP, Video on Demand, IP-TV und Videokonferenzen sind einige der gängigen Technologien, die Multicast-Routing verwenden. Wenn Sie Multicastrouting auf der Citrix SD-WAN Appliance aktivieren, fungiert die Appliance als Multicastrouter.

Quellspezifischer Multicast

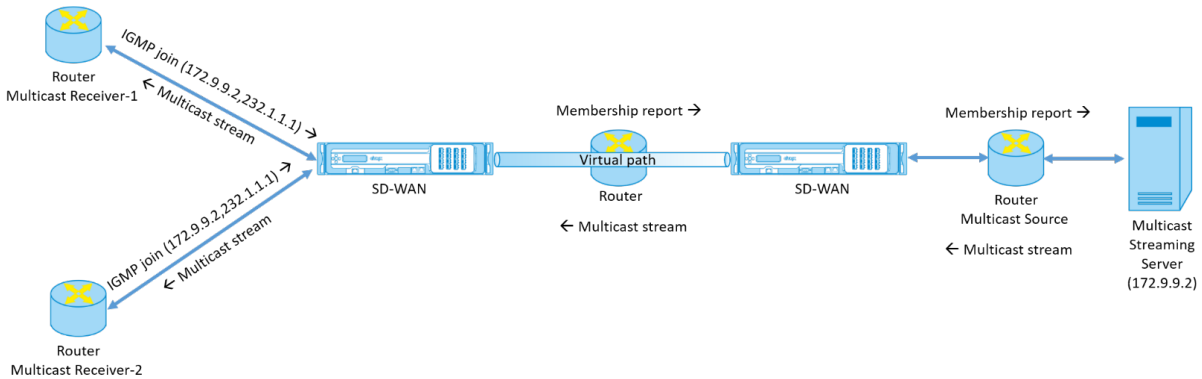
Multicast-Protokolle ermöglichen Multicastempfänger in der Regel den Empfang von Multicast-Datenverkehr von jeder Quelle.

Mit dem quellspezifischen Multicast (SSM) können Sie die Quelle angeben, von der die Empfänger den Multicast-Verkehr erhalten. Es stellt sicher, dass die Empfänger nicht offene Listener für jede Quelle sind, die Multicast-Streams sendet, sondern vielmehr eine bestimmte Multicastquelle hören.

Der SSM senkt die Kosten für Ressourcen, die für den Verbrauch von Datenverkehr aus allen möglichen Quellen verwendet werden. Der SSM bietet auch eine Sicherheitsebene, indem sichergestellt wird, dass die Empfänger Datenverkehr von einem bekannten Absender erhalten.

Die folgende Topologie zeigt zwei Multicastempfänger an einem Zweigstandort und einen Multicastserver (172.9.9.2) im Rechenzentrum. Der Multicast-Server streamt Datenverkehr über eine bestimmte Gruppe (232.1.1.1), wobei die Empfänger der Gruppe beitreten. Jeder Datenverkehr, der in der Multicastgruppe gestreamt wird, wird an alle Empfänger weitergeleitet, die der Gruppe beigetreten sind.

> **Hinweis**
>
> Damit SSM funktioniert, muss die IP der Multicastgruppe im Bereich 232.0.0.0/8 liegen.



1. Die Multicastempfänger senden eine IP-IGMP-Join-Anforderung, die angibt, dass die Empfänger der Multicastgruppe beitreten und den Multicast-Stream von der Quelle empfangen möchten.

Der IGMP-Join enthält 2 Attribute die Multicastquelle und -gruppe (S, G). IGMP Version 3 wird für SSM auf der Multicastquelle und der Empfänger verwendet, um einige INCLUDE-spezifische Quelladressen weiterzuleiten.

Der SSM ermöglicht es den Empfängern, Streams explizit von bestimmten Multicast-Servern zu empfangen, deren Quelladresse explizit von den Empfängern im Rahmen der JOIN-Anfrage bereitgestellt wird. In diesem Beispiel wird eine IGMP v3-Join-Anforderung mit einer expliziten Include-Quellliste ausgelöst, die die Quelle 172.9.9.2 enthält, um die Adresse zu sein, die den Multicast-Stream über die Gruppe 232.1.1.1 sendet.

2. Das Citrix SD-WAN in der Zweigstelle hört alle IGMP-Anforderungen von diesen Empfängern ab und konvertiert sie in einen Mitgliedschaftsbericht und sendet ihn über den virtuellen Pfad an die SD-WAN-Appliance im Rechenzentrum.
3. Die Citrix SD-WAN Appliance im Rechenzentrum empfängt den Mitgliedschaftsbericht über den virtuellen Pfad und leitet ihn an die Multicastquelle weiter, um einen Kontrollkanal zu erstellen.
4. Die Multicastquelle überträgt den Multicast-Stream über den virtuellen Pfad an die Multicastempfänger.

Der Datenverkehr des Kontrollkanals und der Multicast-Stream fließen durch den etablierten virtuellen Pfad zwischen der Zweigstelle und dem Rechenzentrum. Der Citrix SD-WAN Overlay-Pfad sichert und isoliert Multicast-Datenverkehr vor WAN-Verschlechterung oder Link-Brownouts.

Multicast-Konfiguration

Um Multicast zu konfigurieren, führen Sie die folgenden Schritte für den SD-WAN Orchestrator Service sowohl an der Quelle als auch am Ziel aus.

1. Multicastgruppe erstellen - Geben Sie einen Namen und eine IP-Adresse für die Multicastgruppe an. Die IP der Multicastgruppe muss im Bereich 232.0.0.0/8 für quellspezifisches Multicast liegen.
2. IGMP-Proxy aktivieren —Sie können die Citrix SD-WAN-Appliance als IGMP/MLD-Proxy konfigurieren, um die IGMP-Steuerkanalinformationen für das Multicast-Routing zu übertragen.
3. Definieren der Upstream- und Downstream-Dienste - Eine Upstream-Schnittstelle ermöglicht es dem IGMP PROXY, eine Verbindung mit der SD-WAN-Appliance herzustellen, die näher an der eigentlichen Multicastquelle liegt, die den Datenverkehr streamt. Eine Downstream-Schnittstelle ermöglicht es dem IGMP-Proxy, eine Verbindung zu den Hosts herzustellen, die weiter von der eigentlichen Multicastquelle entfernt sind, die den Datenverkehr streamt.
   Die Upstream- und Downstream-Dienste unterscheiden sich für die Appliance an der Quelle und die Appliance am Ziel.

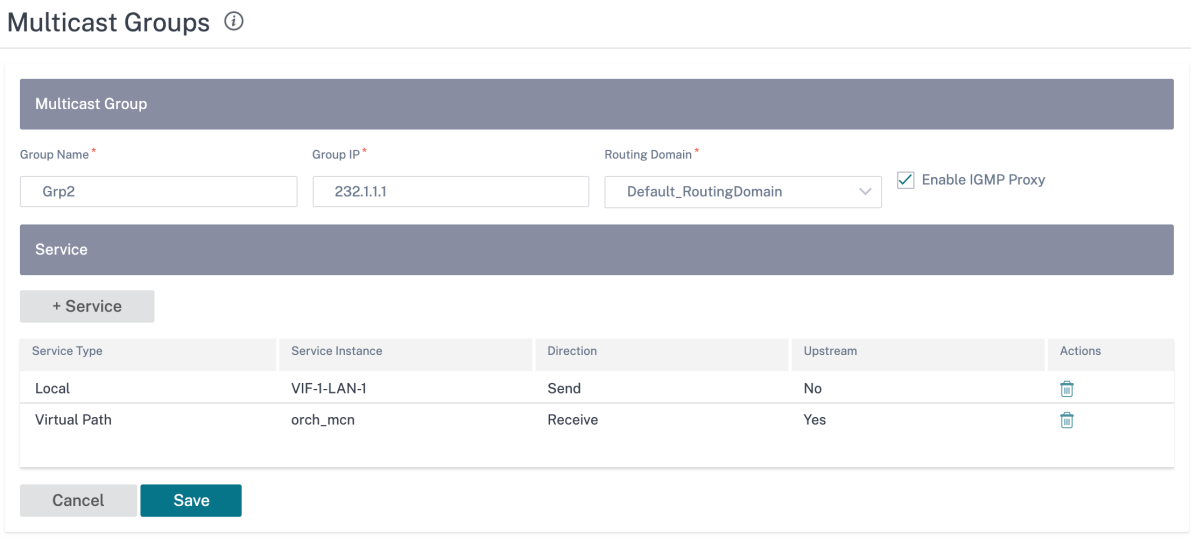
> **Hinweis:**
>
> Sobald der Branch oder MCN als Upstream konfiguriert ist, muss er auch für die anderen Gruppen als Upstream konfiguriert werden.

Um Multicast zu konfigurieren, navigieren Sie auf Standortebene zu **Konfiguration** > **Erweiterte Einstellungen** > **Multicastgruppen**. Erstellen Sie eine Multicastgruppe, indem Sie einen Namen und eine IP-Adresse (IPv4 oder IPv6) für die Multicastgruppe angeben. Klicken Sie auf **IGMP-Proxy aktivieren**.

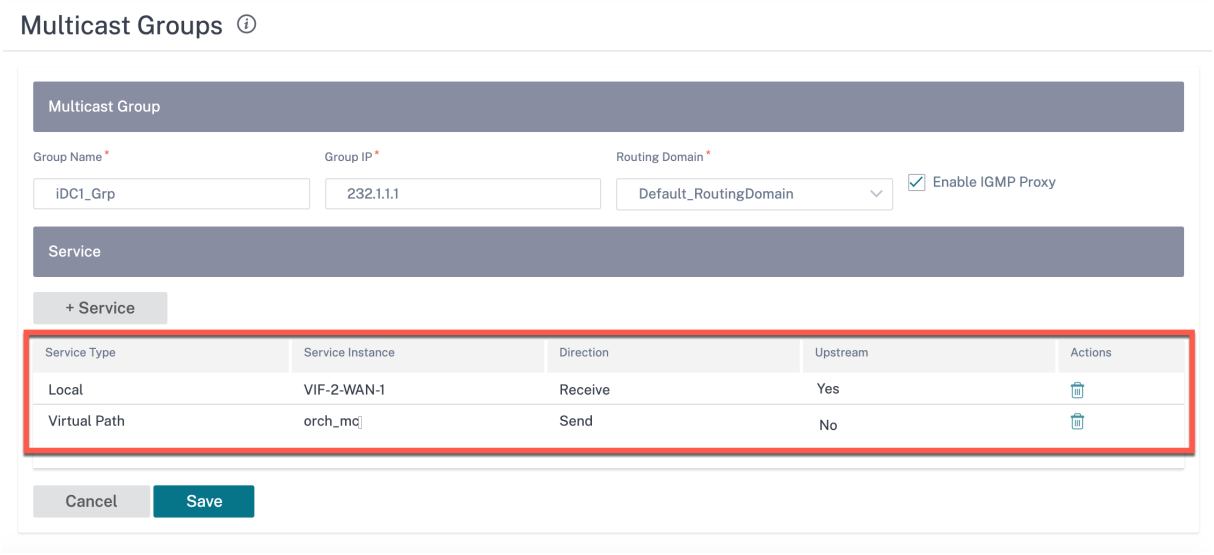
Konfigurieren Sie die Upstream- und Downstream-Pfade für die Zweigstellen- und Rechenzentrumsgeräte.

Für die Appliance, die näher am Multicast-Empfänger (Branch) ist, empfängt die Appliance den Multicast-Verkehr auf dem Virtual Path Interface und sendet den Datenverkehr auf der lokalen Schnittstelle an den Empfänger.

> **Hinweis:**
>
> - Wenn eine Multicastquelle als Intranetdienst konfiguriert ist, muss die Quell-IP des Multicast-Streams eine Route aufweisen, die dem Intranetdienst zugeordnet ist.
> - Stellen Sie sicher, dass Sie geeignete Firewallrichtlinien erstellen, um Multicast-Datenverkehr auf der SD-WAN-Appliance



Für die Appliance, die näher an der Multicast-Quelle (Rechenzentrum) liegt, empfängt die Appliance den Multicast-Verkehr auf der lokalen Schnittstelle und sendet den Datenverkehr auf der virtuellen Pfadschnittstelle.

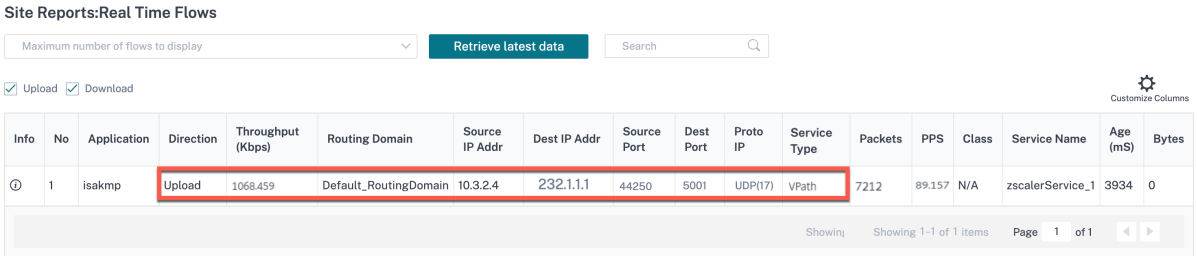


Überwachen

Flows Statistiken

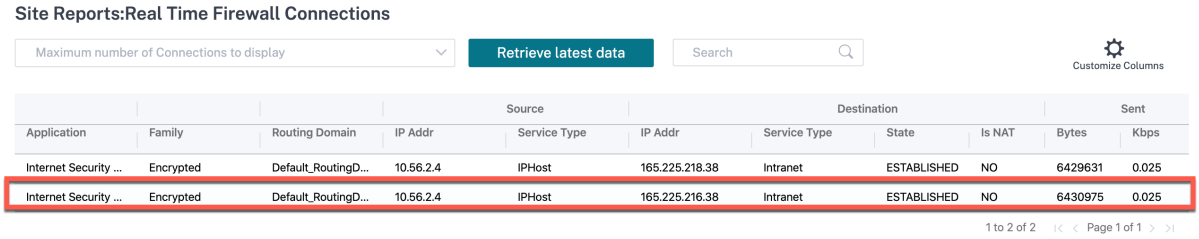
Nachdem der Multicast-Steuerkanal eingerichtet wurde und die Multicast-Quelle mit dem Streaming beginnt, können Sie die Multicast-Flussstatistiken anzeigen. Sie können sehen, dass Multicast-UDP-Datenverkehr über den virtuellen Pfaddienst von einem Receiver an die Multicast-Gruppe 232.1.1.1 gesendet wurde.

> **Hinweis:**
>
> Wenn SSM aktiviert ist und der Datenverkehr von einem anderen Server empfangen wird, der nicht Teil der erwarteten Liste von Quellabsendern ist, hat die SD-WAN-Appliance keine Berichtsdaten.



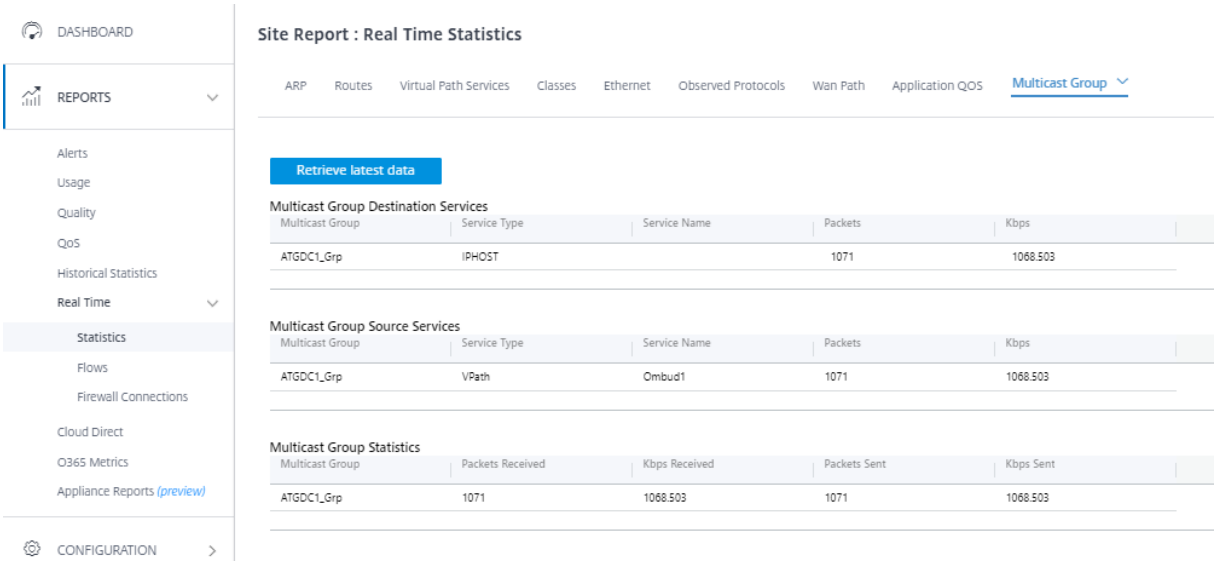
Firewall-Statistiken

Die Firewall-Tabelle zeigt den Multicast-Verkehr, der über die LAN-Schnittstelle über die IP-Adresse der Multicastgruppe kommt, und wird über den virtuellen Pfad gesendet.



Multicast-Gruppenstatistik

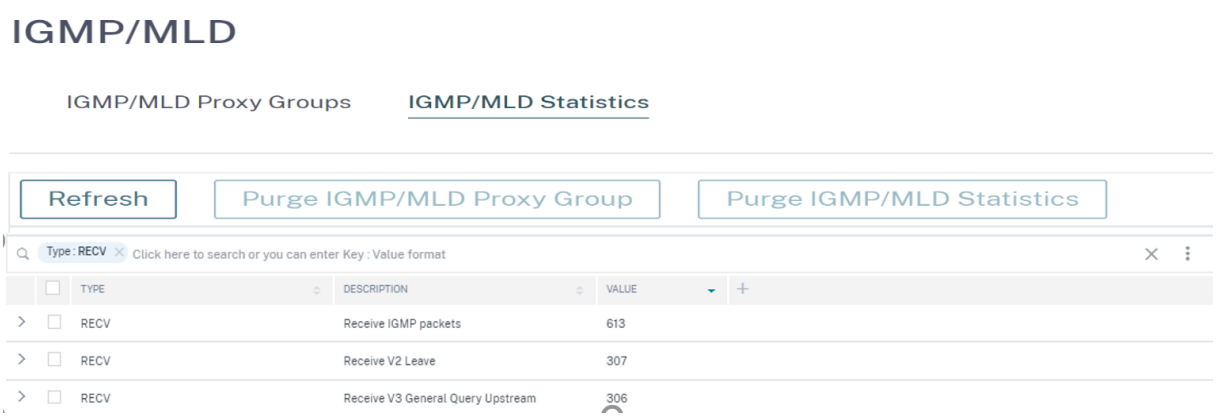
Die Multicastgruppentabelle enthält Details zum Multicastverkehr wie Pakete, die über Quelle, Ziel und die Aggregation von beiden gesendeten und empfangenen Pakete enthalten.



IGMP/MLD

Wenn die Multicast-Empfänger eine Join-Group-Anfrage initiieren, können Sie die Empfängerdetails unter **Berichte** > **Echtzeit** > **IGMP/MLD** > **IGMP/MLD Stats**sehen. Sie können diese Informationen sowohl an der Quelle als auch am Ziel sehen. Klicken Sie auf **Aktualisieren**, um die aktuellen Daten zu erhalten.

Die folgende Abbildung zeigt, dass die empfangenen IGMP/MLD-Pakete und der Filtertyp RECV verwendet werden, um IGMP/MLD-Empfangspakete einzubeziehen.



Um die Details der IGMP-Proxygruppen anzuzeigen, navigieren Sie zu **Berichte** > **Echtzeit** > **IGMP/MLD** > **IGMP/MLD Proxygruppen**. Klicken Sie auf **Aktualisieren**, um die aktuellen Daten zu erhalten.

Wählen Sie **IGMP/MLD-Statistiken** löschen, um IGMP-Statistikdaten aus der IGMP-Statistiktabelle zu löschen.

Wählen Sie **IGMP/MLD-Gruppe** löschen, um IGMP-Gruppendaten aus der IGMP-Gruppentabelle zu löschen.

Redundanzprotokoll für virtuelle Router

October 21, 2022

Virtual Router Redundancy Protocol (VRRP) ist ein weit verbreitetes Protokoll, das Geräteredundanz bietet, um den Single Point of Failure zu eliminieren, der einer statischen Standardumgebung mit Routing innewohnt.

Mit VRRP können Sie zwei oder mehr Router konfigurieren, um eine Gruppe zu bilden. Diese Gruppe wird als einzelnes Standard-Gateway mit einer virtuellen IP-Adresse und einer virtuellen MAC-Adresse angezeigt.

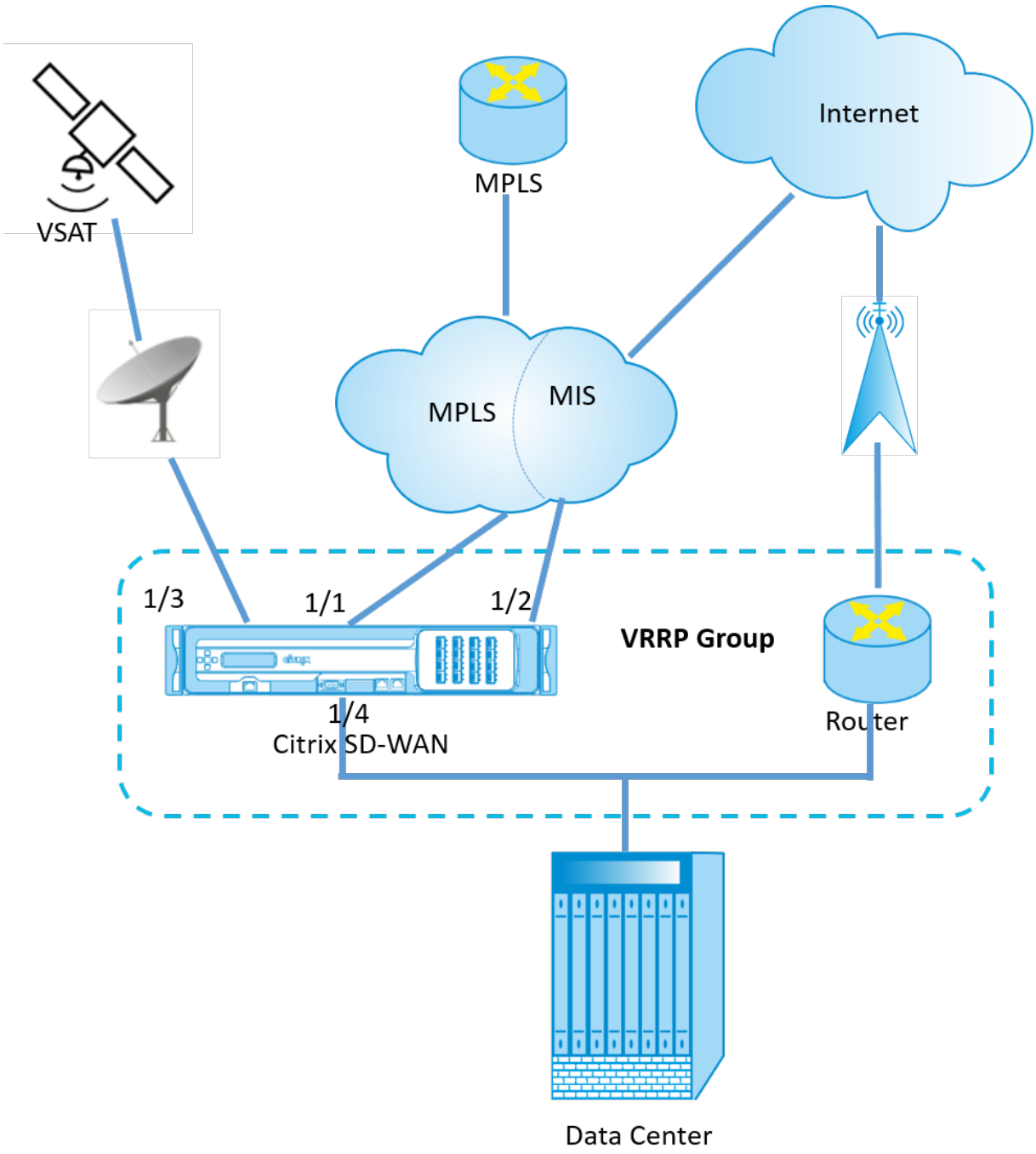
Ein Backup-Router übernimmt automatisch die Kontrolle, wenn der primäre/Hauptrouter ausfällt. In einer VRRP-Setup sendet der Hauptrouter ein VRRP-Paket, das als Ankündigung bezeichnet wird, an die Backup-Router. Wenn der Hauptrouter das Senden der Ankündigung beendet, stellt der Backup-Router den Intervall-Timer ein. Wenn innerhalb dieser Haltefrist keine Ankündigung eingeht, startet der Backup-Router die Failover-Routine.

VRRP spezifiziert einen Wahlprozess, bei dem der Router mit der höchsten Priorität zum Hauptrouter wird. Wenn die Priorität unter den Routern gleich ist, wird der Router mit der höchsten IP-Adresse zum Hauptrouter. Die anderen Router befinden sich im Backup-Zustand. Der Wahlvorgang wird erneut eingeleitet, wenn der Hauptrouter ausfällt, ein neuer Router der Gruppe beitritt oder ein vorhandener Router die Gruppe verlässt.

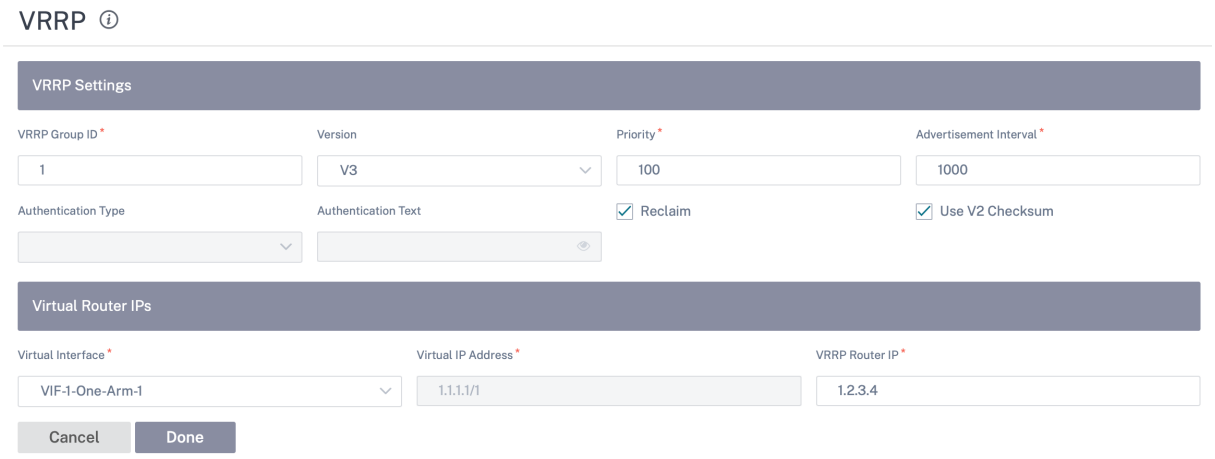
VRRP stellt einen Standardpfad für hohe Verfügbarkeit sicher, ohne dynamische Routing- oder Routererkennungsprotokolle auf jedem Endhost zu konfigurieren.

Citrix SD-WAN Version 10.1 unterstützt VRRP Version 2 und Version 3, um mit Routern von Drittanbietern zu arbeiten. Citrix SD-WAN Version 11.5 unterstützt Version 6. Die SD-WAN-Appliance fungiert als Hauptrouter und leitet den Datenverkehr an, um den Virtual Path Service zwischen Standorten zu verwenden. Sie können die SD-WAN-Appliance als VRRP-Hauptrouter konfigurieren, indem Sie die virtuelle Schnittstellen-IP als VRRP-IP konfigurieren und die Priorität manuell auf einen höheren Wert als die Peer-Router festlegen. Sie können das Ankündigungsintervall und die Präempt-Option konfigurieren.

Das folgende Netzwerkdiagramm zeigt eine Citrix SD-WAN-Appliance und einen als VRRP-Gruppe konfigurierten Router. Die SD-WAN-Appliance ist als Hauptrouter konfiguriert. Wenn die SD-WAN-Appliance ausfällt, übernimmt der Backup-Router innerhalb von Millisekunden und stellt sicher, dass keine Ausfallzeiten vorliegen.



Um VRRP zu konfigurieren, navigieren Sie auf der Seite Site-Konfiguration zu **Konfiguration** > **Erweiterte Einstellungen** > **VRRP** > klicken Sie auf **+ VRRP hinzufügen**.



Sie können die folgenden Mitgliedspfadparameter bearbeiten:

- **VRRP-Gruppen-ID**: Die VRRP-Gruppen-ID. Die Gruppen-ID muss ein Wertebereich von 1—255 sein. Die gleiche Gruppen-ID muss auch auf den Backup-Routern konfiguriert werden.
- **Ausführung**: Die VRRP-Protokollversion. Sie können zwischen VRRP-Protokoll V2 und V3 wählen.
- **Priorität**: Die Priorität der Citrix SD-WAN-Appliance für die VRRP-Gruppe. Der Prioritätsbereich liegt zwischen 1—254. Setzen Sie diesen Wert auf Maximum (254), um die SD-WAN-Appliance zum Hauptrouter zu machen.

  > **Hinweis**
  >
  > Wenn der Router der Besitzer der VRRP-IP-Adresse ist, ist die Priorität standardmäßig auf 255 festgelegt.

- **Ankündigungsintervall**: Die Häufigkeit in Millisekunden, mit der die VRRP-Ankündigungen gesendet werden, wenn die SD-WAN-Appliance der Hauptrouter ist. Das standardmäßige Ankündigungsintervall beträgt eine Sekunde.
- **Authentifizierungstyp**: Sie können **Nur-Text** wählen, um eine Authentifizierungszeichenfolge einzugeben. Die Authentifizierungszeichenfolge wird in den VRRP-Ankündigungen als Klartext ohne Verschlüsselung gesendet. Wählen Sie **Keine**, wenn Sie keine Authentifizierung einrichten möchten.
- **Authentifizierungstext**: Der Authentifizierungsstring, der in der VRRP-Ankündigung gesendet werden soll. Diese Option ist aktiviert, wenn der **Authentifizierungstyp Nur-Text** ist.

  > **Hinweis**
  >
  > Die Parameter **Authentifizierungstyp** und **Authentifizierungstext** sind nur für VRRP-Protokoll Version 2 aktiviert.

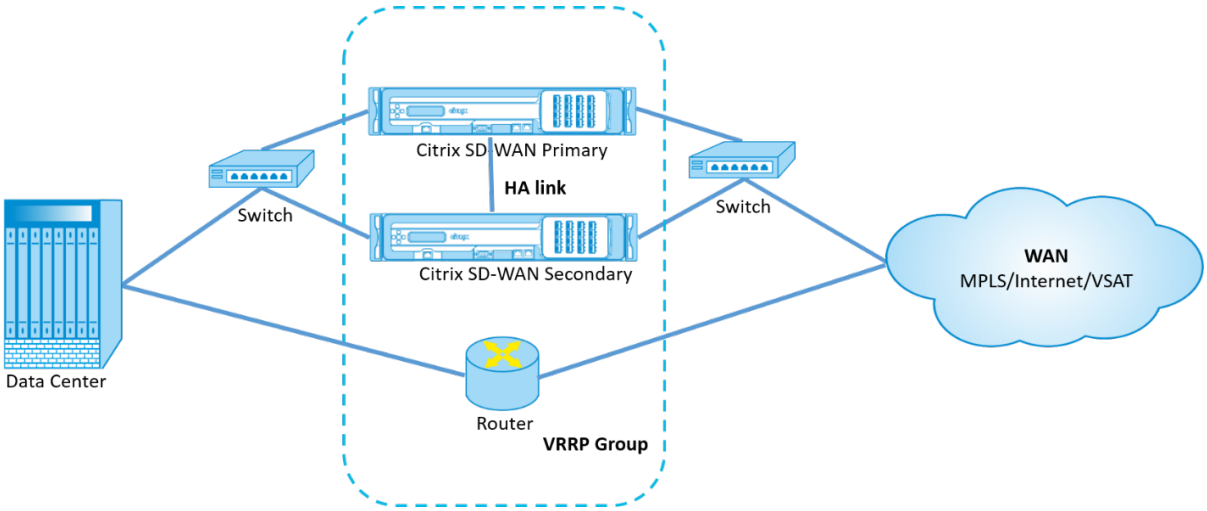
- **V2-Prüfsumme verwenden**: Ermöglicht Kompatibilität mit Netzwerkgeräten von Drittanbietern für VRRPv3. Standardmäßig verwendet VRRPv3 die Prüfsummenberechnungsmethode v3. Bestimmte Geräte von Drittanbietern unterstützen möglicherweise nur die VRRPv2-Prüfsummenberechnung. Aktivieren Sie in solchen Fällen diese Option.
- **Virtuelle Schnittstelle**: Die virtuelle Schnittstelle, die für VRRP verwendet werden soll. Wenn IPv6 verwendet wird, ist für die virtuelle Schnittstelle standardmäßig NDP RA aktiviert. Wählen Sie eine der konfigurierten virtuellen Schnittstellen.
- **Virtuelle IP-Adresse**: Die virtuelle IP-Adresse, die der virtuellen Schnittstelle zugewiesen ist. Wählen Sie eine der konfigurierten virtuellen IP-Adressen für die virtuelle Schnittstelle. Sie können entweder die IPv4- oder IPv6-Adresse angeben.
- **VRRP-Router-IP**: Die IP-Adresse des virtuellen Routers für die VRRP-Gruppe. Standardmäßig wird die virtuelle IP-Adresse der SD-WAN-Appliance als virtuelle Router-IP-Adresse zugewiesen. Die IP des virtuellen VRRP-Routers sollte eine link-lokale IPv6-Adresse sein.

Einschränkungen

- VRRP wird nur in der Gateway-Modus-Bereitstellung unterstützt.
- Sie können bis zu vier VRRP-IDs (VRID) konfigurieren.
- Bis zu 16 virtuelle Netzwerkschnittstellen können an VRID teilnehmen.

Hochverfügbarkeit und VRRP

Sie können Netzwerkausfallzeiten und Verkehrsstörungen erheblich reduzieren, indem Sie sowohl die Hochverfügbarkeits- als auch die VRRP-Funktionen auf Ihr SD-WAN-Netzwerk anwenden. Stellen Sie ein Paar Citrix SD-WAN-Appliance in Aktiv-/Standby-Rollen zusammen mit einem Standby-Router bereit, um die VRRP-Gruppe zu bilden. Diese Gruppe wird als einzelnes Standard-Gateway mit einer virtuellen IP-Adresse und einer virtuellen MAC-Adresse angezeigt.



Im Folgenden sind 2 Fälle mit der Hochverfügbarkeits- und VRRP-Bereitstellung aufgeführt:

1. Fall: Hochverfügbarkeits-Failover-Timer auf SD-WAN entspricht dem VRRP-Failover-Timer.

Das erwartete Verhalten ist ein Switchover mit hoher Verfügbarkeit, der vor dem VRRP-Switchover stattfindet, d. h. der Datenverkehr fließt weiter durch die neue Active SD-WAN-Appliance. In diesem Fall setzt SD-WAN mit der VRRP-Master-Rolle fort.

2. Fall: Hochverfügbarkeits-Failover-Timer auf SD-WAN größer als der VRRP-Failover-Timer.

Das erwartete Verhalten ist die VRRP-Umstellung auf den Router geschieht, das heißt, der Router wird VRRP-Master und Datenverkehr möglicherweise vorübergehend durch den Router fließen, unter Umgehung der SD-WAN-Appliance.

Aber sobald der Hochverfügbarkeits-Switchover passiert, wird SD-WAN wieder zu VRRP Master, d. h. der Datenverkehr fließt jetzt durch die neue aktive SD-WAN-Appliance.

Weitere Informationen zu Bereitstellungsmodi für Hochverfügbarkeit finden Sie unter Hochverfügbarkeit.

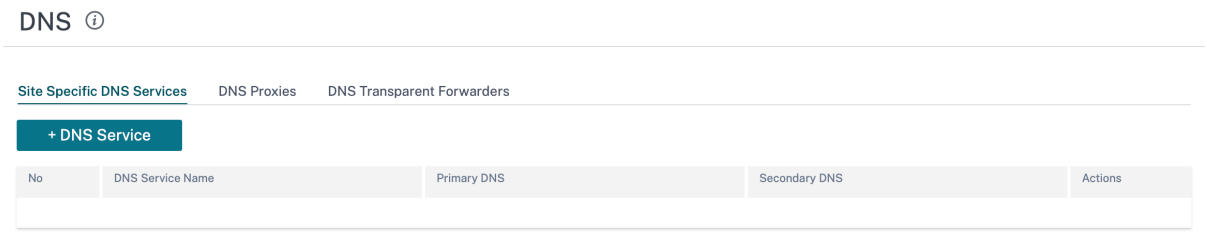
Einstellungen des Domänennamensystems

October 21, 2022

Domain Name System (DNS) übersetzt menschenlesbare Domainnamen in maschinenlesbare IP-Adressen und umgekehrt. Citrix SD-WAN bietet die folgenden DNS-Funktionen:

- DNS-Proxy
- Transparente DNS-Weiterleitung

Um DNS-Einstellungen zu konfigurieren, navigieren Sie auf der Seite Site-Konfiguration zu **Konfiguration > Erweiterte Einstellungen** > **DNS-Einstellungen**.



Sitespezifische DNS-Server

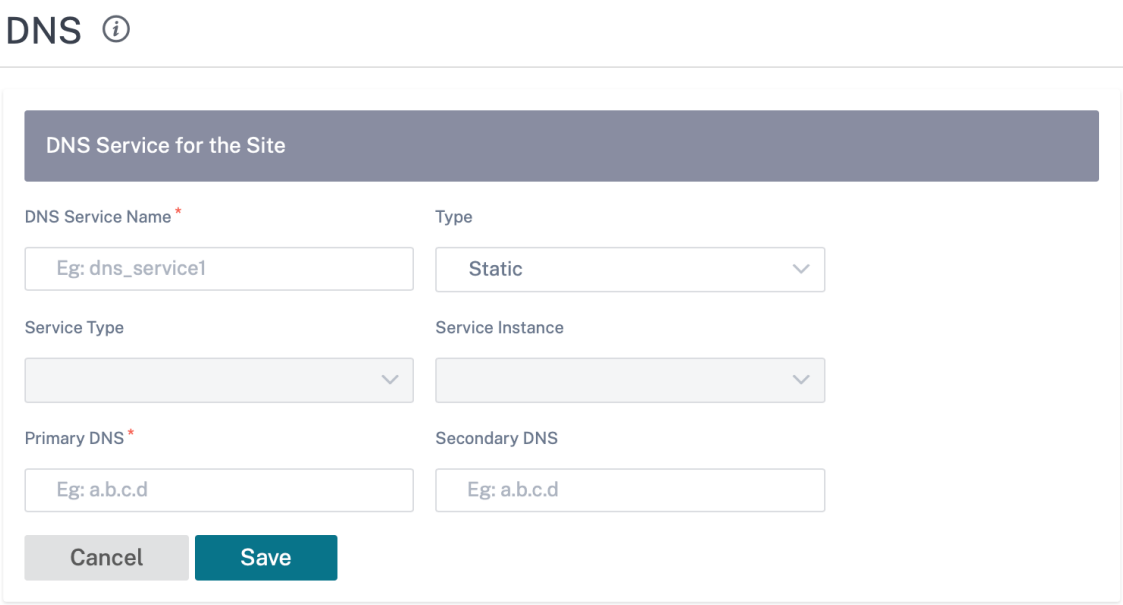
Klicken Sie auf der Registerkarte **Standortspezifische DNS-Server** auf **+ DNS-Server**, um standortspezifische DNS-Server zu konfigurieren, an die die DNS-Anforderungen weitergeleitet werden. Geben Sie einen Namen für den DNS-Server an. Wählen Sie einen der folgenden Diensttypen:

- **Statisch**: Fängt die DNS-Anforderungen ab, die an die Citrix SD-WAN-IP-Adresse bestimmt sind, und leitet sie an die angegebenen IPv4-DNS-Server weiter. Sie können interne, ISP, Google oder einen anderen Open-Source-DNS-Dienst erstellen.
- **Dynamisch**: Fängt die DNS-Anforderungen ab, die an die Citrix SD-WAN-IP-Adresse bestimmt sind, und leitet sie an einen der IPv4-DNS-Server um, die aus den DHCP-basierten WAN-Links gelernt wurden. Wenn die WAN-Verbindung ausfällt, wird ein anderer DHCP-basierter WAN-Verbindungs-DNS-Server ausgewählt. Diese Funktion ist in der Bereitstellung nützlich, bei der ISPs DNS-Anforderungen nur an DNS-Server zulassen, die von ihnen gehostet werden. Dynamischer DNS-Dienst kann nur auf Standortebene konfiguriert werden. Pro Standort ist nur ein dynamischer DNS-Dienst zulässig.
- **StaticV6**: Fängt die DNS-Anforderungen ab, die an die Citrix SD-WAN-IP-Adresse bestimmt sind, und leitet sie an die angegebenen IPv6-DNS-Server weiter. Sie können interne, ISP, Google oder einen anderen Open-Source-DNS-Dienst erstellen.
- **DynamicV6**: Fängt die DNS-Anforderungen ab, die an die Citrix SD-WAN-IP-Adresse bestimmt sind, und leitet sie an einen der IPv6-DNS-Server um, die aus den DHCP-basierten WAN-Links gelernt wurden. Wenn die WAN-Verbindung ausfällt, wird ein anderer DHCP-basierter WAN-Verbindungs-DNS-Server ausgewählt. Diese Funktion ist in der Bereitstellung nützlich, bei der ISPs DNS-Anforderungen nur an DNS-Server zulassen, die von ihnen gehostet werden. Dynamischer DNS-Dienst kann nur auf Standortebene konfiguriert werden. Pro Standort ist nur ein dynamischer DNS-Dienst zulässig.

Um den statischen DNS-Dienst zu konfigurieren, wählen Sie den **Typ** als **statisch** (für IPv4-Adresse) oder **StaticV6** (für IPv6-Adresse) aus und geben Sie ein Paar **primärer DNS** - und **sekundärer DNS-Server-IP-Adressen** ein.

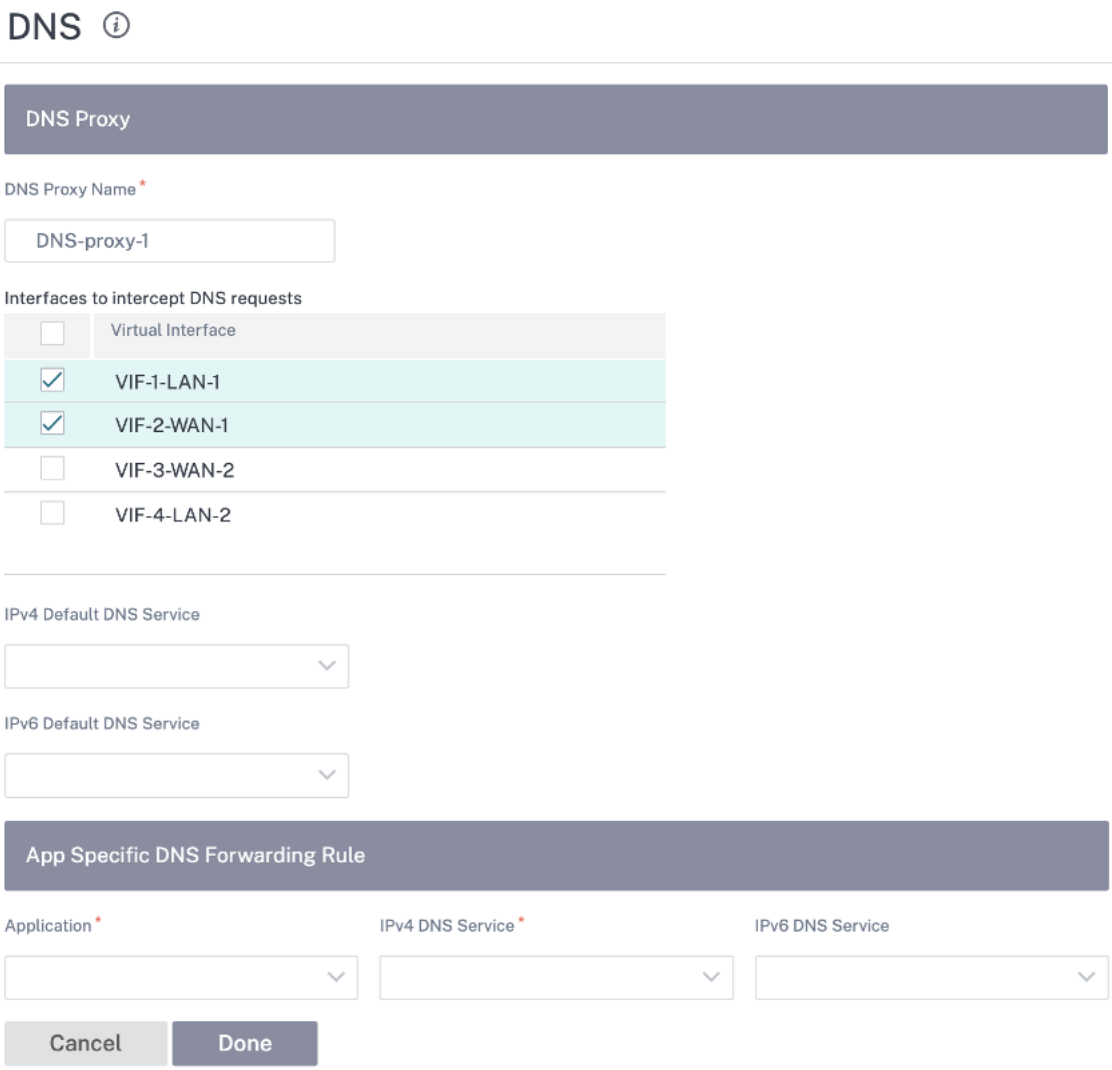
Um den dynamischen DNS-Dienst zu konfigurieren, wählen Sie den **Typ** als **Dynamisch** (für IPv4-Adresse) oder **DynamicV6** (für IPv6-Adresse) und wählen Sie **Internet** für **Diensttyp** und **Dienstinstanz**aus.

Die entsprechenden DNS-Proxydienste werden in der Dropdown-Liste **InBand Management DNS** unter **Standortkonfiguration > Schnittstellen**aufgelistet.



DNS-Proxy

Der DNS-Proxy fängt die DNS-Anforderungen ab, die an die SD-WAN-IP-Adresse bestimmt sind, und leitet sie an die ausgewählten DNS-Server weiter. Sie können einen Proxy mit mehreren Weiterleitungen konfigurieren, mit denen DNS-Anfragen basierend auf Anwendungsdomänennamen gesteuert werden können.

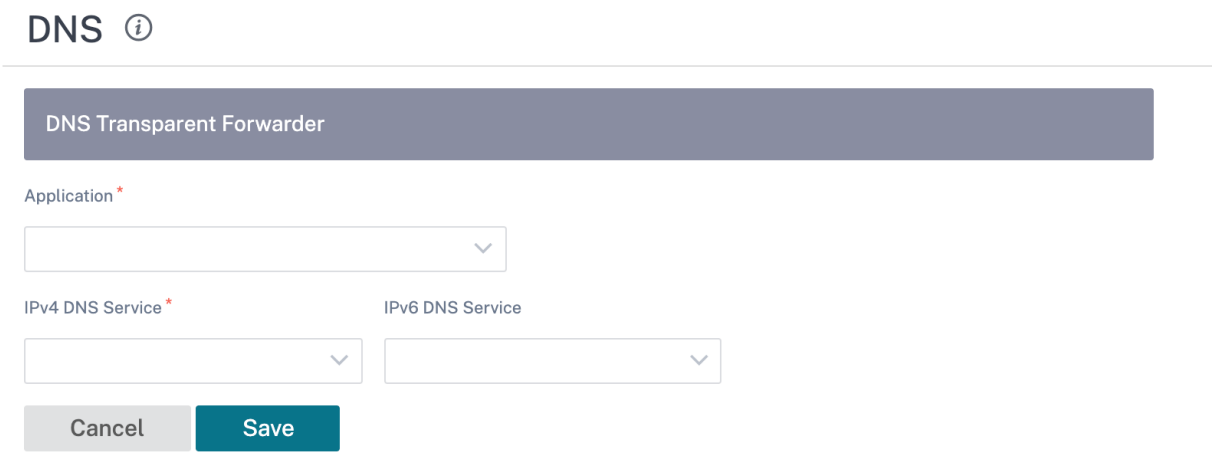


- DNS-Proxyeinstellungen:
  - **DNS-Proxy-Name**: Name des DNS-Proxys.
  - **Schnittstellen zum Abfangen von DNS-Anfragen**: Die Schnittstellen, auf denen die DNS-Anfragen abgefangen werden. Nur vertrauenswürdige Schnittstellen sind zulässig.
  - **Standard-DNS-Server für den gesamten Datenverkehr**: Der Standard-DNS-Server, an den die DNS-Anforderungen weitergeleitet werden, wenn keine der Anwendungen in der DNS-Weiterleitungssuche übereinstimmt.
  - **IPv4-Standard-DNS-Dienst**: Der IPv4-Standard-DNS-Dienst, an den die DNS-Anforderungen weitergeleitet werden, wenn keine der Anwendungen in der DNS-Weiterleitungssuche übereinstimmt.
  - **IPv6-Standard-DNS-Dienst**: Der IPv6-Standard-DNS-Dienst, an den die DNS-Anforderungen weitergeleitet werden, wenn keine der Anwendungen in der DNS-Weiterleitungssuche übereinstimmt.

- Anwendungsspezifische DNS-Weiterleitungsregeln:
  - **Anwendung**: Anwendungen, für die DNS-Anfragen an den ausgewählten DNS-Server weitergeleitet werden müssen.
  - **IPv4-DNS-Dienst**: Der IPv4-DNS-Dienst, an den die DNS-Anforderung für die angegebene Anwendung weitergeleitet wird.
  - **IPv6-DNS-Dienst**: Der IPv6-DNS-Dienst, an den die DNS-Anfrage für die angegebene Anwendung weitergeleitet wird.

Transparente DNS-Weiterleitungen

Citrix SD-WAN kann als transparente DNS-Weiterleitung konfiguriert werden. In diesem Modus kann SD-WAN DNS-Anfragen abfangen, die nicht an seine IP-Adresse bestimmt sind, und sie an die angegebenen DNS-Server weiterleiten. Nur die DNS-Anfragen, die vom lokalen Dienst auf vertrauenswürdigen Schnittstellen stammen, werden abgefangen. Wenn die DNS-Anforderungen mit Anwendungen in der DNS-Weiterleitungsliste übereinstimmen, wird sie an den konfigurierten DNS-Dienst weitergeleitet.



- **Anwendung**: Anwendungen, für die DNS-Anfragen an den ausgewählten DNS-Server weitergeleitet werden müssen.
- **IPv4-DNS-Dienst**: Der IPv4-DNS-Dienst, an den die DNS-Anforderung für die angegebene Anwendung weitergeleitet wird.
- **IPv6-DNS-Dienst**: Der IPv6-DNS-Dienst, an den die DNS-Anfrage für die angegebene Anwendung weitergeleitet wird.

Präfix-Delegierungsgruppen

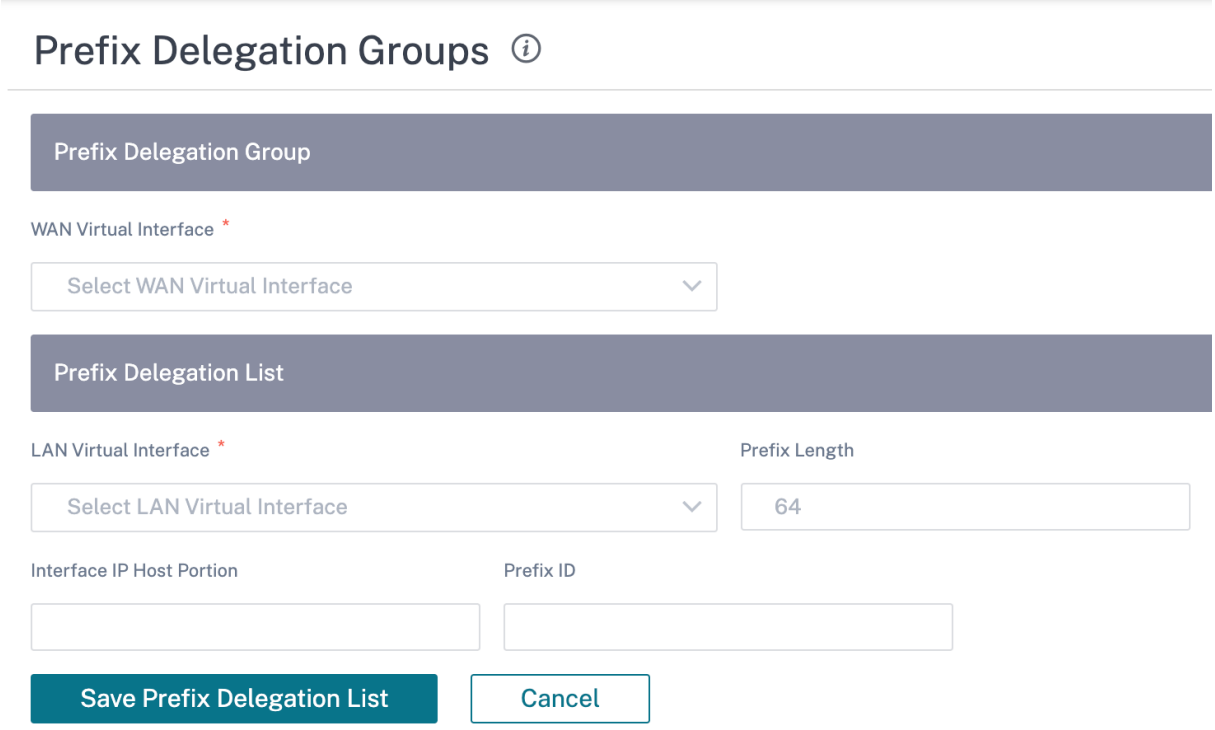
October 21, 2022

Citrix SD-WAN Appliances können als DHCPv6-Client konfiguriert werden, um ein Präfix vom ISP über den konfigurierten WAN-Port anzufordern. Sobald die Citrix SD-WAN-Appliance das Präfix erhält, verwendet sie das Präfix, um einen Pool von IP-Adressen für die LAN-Clients zu erstellen. Die Citrix SD-WAN-Appliance verhält sich dann wie ein DHCP-Server und gibt den LAN-seitigen Clients das Präfix an den LAN-Ports bekannt.

Um die Präfixdelegierung zu konfigurieren, navigieren Sie zu **Konfiguration > Erweiterte Einstellungen > Präfixdelegierungsgruppen**, und klicken Sie auf **+ Präfixdelegierungsgruppen**.

Wählen Sie eine konfigurierte virtuelle WAN-Schnittstelle, auf der das Präfix vom ISP angefordert wird, und geben Sie die folgenden Details an:

- **LAN Virtual Interface**: Wählen Sie eine der konfigurierten virtuellen LAN-Schnittstellen aus, für die das Präfix angefordert wird.
- **Präfixlänge**: Die Anzahl der Bits einer Global Unicast IPv6-Adresse, die Teil des Präfixes sind.
- **Interface-IP-Hostteil**: Der Host-Teil, der für die IP-Adresse der Schnittstelle verwendet werden soll.
- **Präfix-ID**: Eine eindeutige Kennung zur Identifizierung der Präfix-Delegierungsanforderungen für die LAN-Schnittstelle.



Verbindungsaggregationsgruppen

October 21, 2022

Mit der LAG-Funktion (Link Aggregation Groups) können Sie zwei oder mehr Ports auf Ihrer SD-WAN-Appliance gruppieren, um als einen einzigen Port zusammenzuarbeiten. Dies gewährleistet eine erhöhte Verfügbarkeit, Link-Redundanz und verbesserte Leistung.

Citrix SD-WAN Orchestrator for On-premises unterstützt die einfache Link Aggregation Group (ACTIVE-BACKUP). Die 802.3ad LACP-Protokoll-basierten Verhandlungen werden in der aktuellen Version nicht unterstützt. Zu jeder Zeit ist nur ein Port aktiv und die anderen Ports sind im Backupmodus. Die aktiven und Backupunterstützungen basieren auf dem Data Plane Development Kit (DPDK) -Paket für die LAG-Funktionalität.

Die LAG-Funktionalität ist nur auf den folgenden Plattformen verfügbar:

- 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

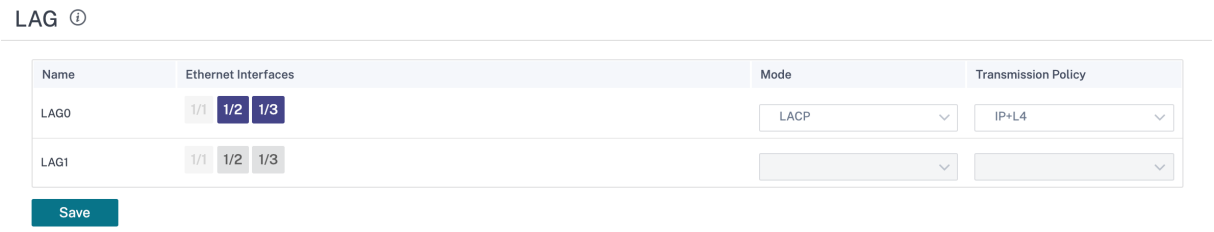
> Hinweis
>
> - Die LAG-Funktionalität wird auf VPX/VPXL-Plattformen nicht unterstützt.
> - Pro LAG werden mindestens zwei Ports und maximal vier Ports unterstützt.
> - Alle Mitglieder von LAG müssen vom gleichen Typ sein, zum Beispiel 1/1 oder 1/2. 1/1 und 10/1 werden nicht unterstützt LAG-Konfiguration.
> - Die Funktion Link State Propagation (LSP) wird nicht unterstützt, wenn LAGs als Ethernet-Schnittstellen in Schnittstellengruppen verwendet werden.

Plattform	Maximale Anzahl unterstützter LAGs	Von LACP unterstützte Ports
110	1	1/1

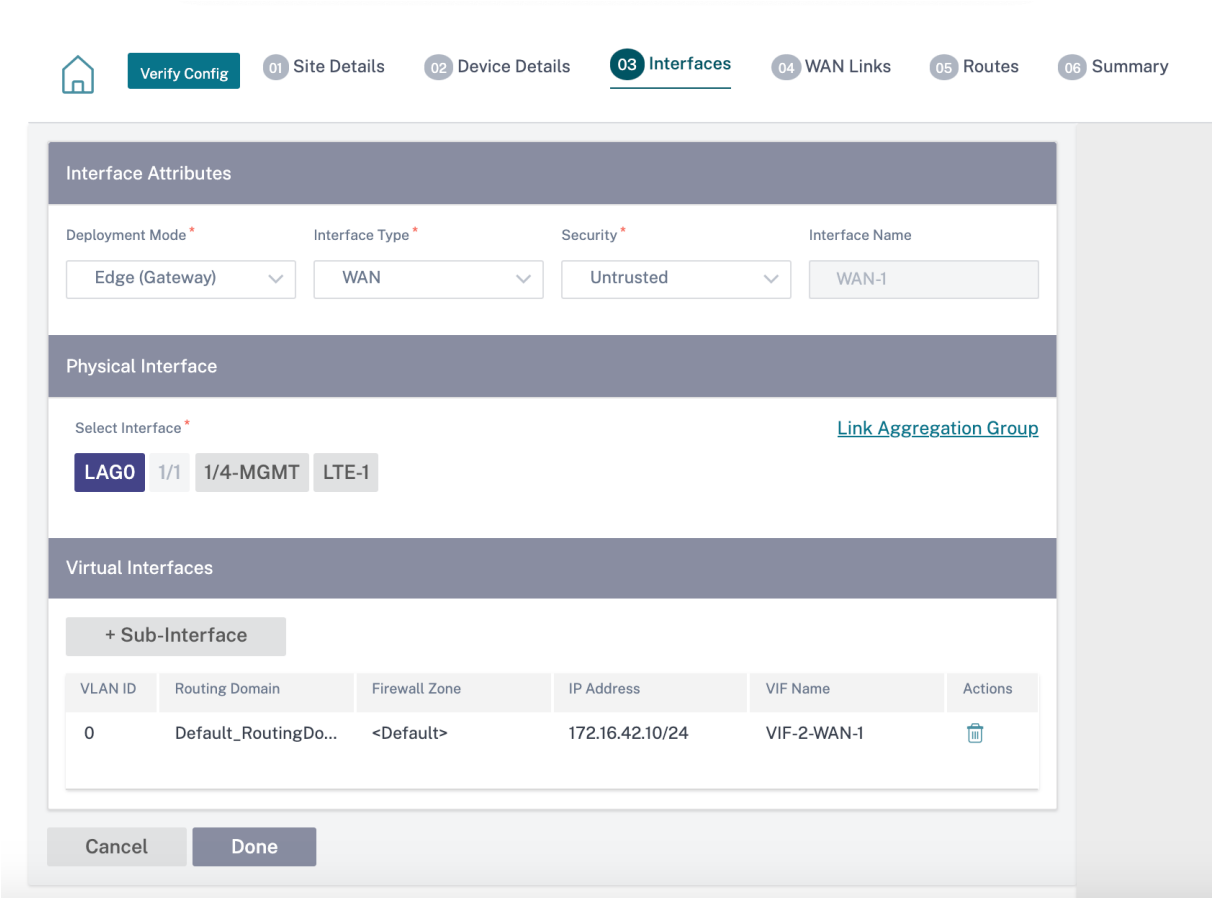
Plattform	Maximale Anzahl unterstützter LAGs	Von LACP unterstützte Ports
210	2	1/1 oder 1/2
410	1	1/1 oder 1/2
1100	3	1/1 oder 1/2
2100	3	1/1 oder 1/2
4100	4	1/1 oder 1/2
5100	3	10/1 oder 10/2

Plattform	Maximale Anzahl unterstützter LAGs	Von LACP unterstützte Ports
6100	4	1/1 oder 1/2

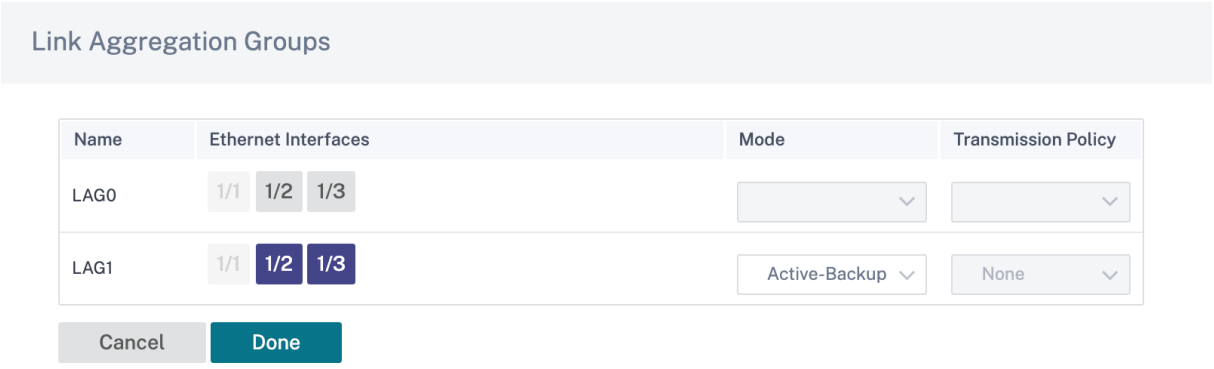
Um Link-Aggregationsgruppen zu konfigurieren, navigieren Sie auf Standortebene zu **Konfiguration > Erweiterte Einstellungen > LAG**, und wählen Sie die Mitglieds-Ethernet-Schnittstellen aus, um eine Linkaggregationsgruppe zu bilden.



Sobald die Ports zur LAG hinzugefügt wurden, können Sie unter **Standortkonfiguration die LAGs zur Konfiguration**der Schnittstellen auswählen. Diese Schnittstellen werden weiter verwendet, um LAN/WAN-Verbindungen und HA zu konfigurieren. Sie können die Einstellungen für einzelne Mitglieds-Ports nicht ändern. Konfigurationsänderungen, die an der LAG vorgenommen wurden, werden automatisch an die Mitglieds-Ports übertragen.



Klicken Sie im Abschnitt **Schnittstellen** auf **Link Aggregation Group**, um die LAG-Konfiguration bei Bedarf schnell zu ändern.



Sie können die Details der Schnittstellen, die mit LAG und LACP konfiguriert sind, unter **Berichte > Appliance-Berichte > LACP-LAG-Gruppe**anzeigen. Weitere Informationen finden Sie unter Appliance-Berichte.

Appliance-Einstellungen

October 21, 2022

Mit dem Citrix SD-WAN Orchestrator Service können Sie die Appliance-Einstellungen auf Standortebene konfigurieren und an die Remotegeräte übertragen.

Sie können die Einstellungen für Benutzer, Netzwerkadapter, NetFlow, AppFlow, SNMP, Fallback-Konfiguration und Bereinigungsfluss konfigurieren.

> **Hinweis**
>
> Die Option zum Konfigurieren der Appliance-Einstellungen ist beim Erstellen oder Bearbeiten einer Site-Vorlage nicht verfügbar.

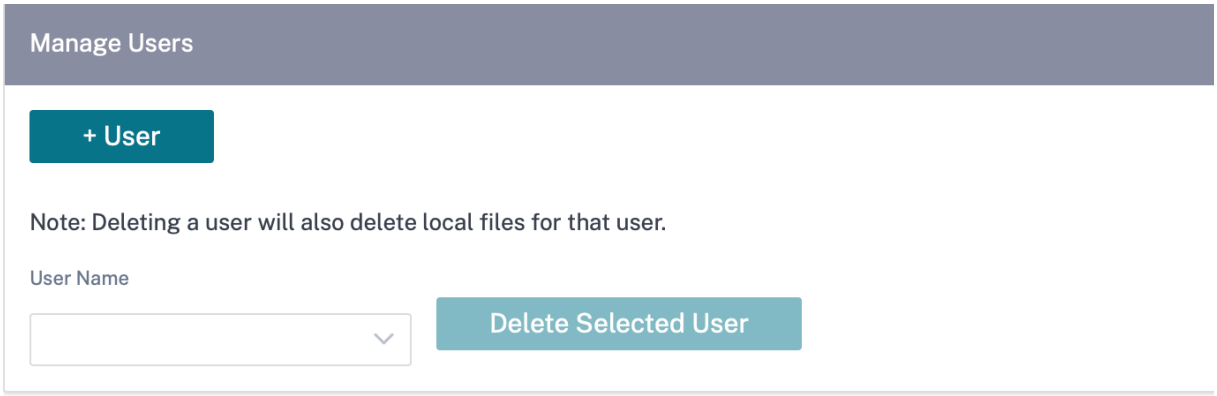
Wenn HA konfiguriert ist, wählen Sie das primäre oder sekundäre Gerät aus, für das Sie die Appliance-Einstellungen ändern möchten.

Administrative Schnittstelle

Über die Verwaltungsoberfläche können Sie lokale und Remote-Benutzerkonten hinzufügen und verwalten. Die Remote-Benutzerkonten werden über die RADIUS- oder TACACS+-Authentifizierungsserver authentifiziert.

Nutzer verwalten

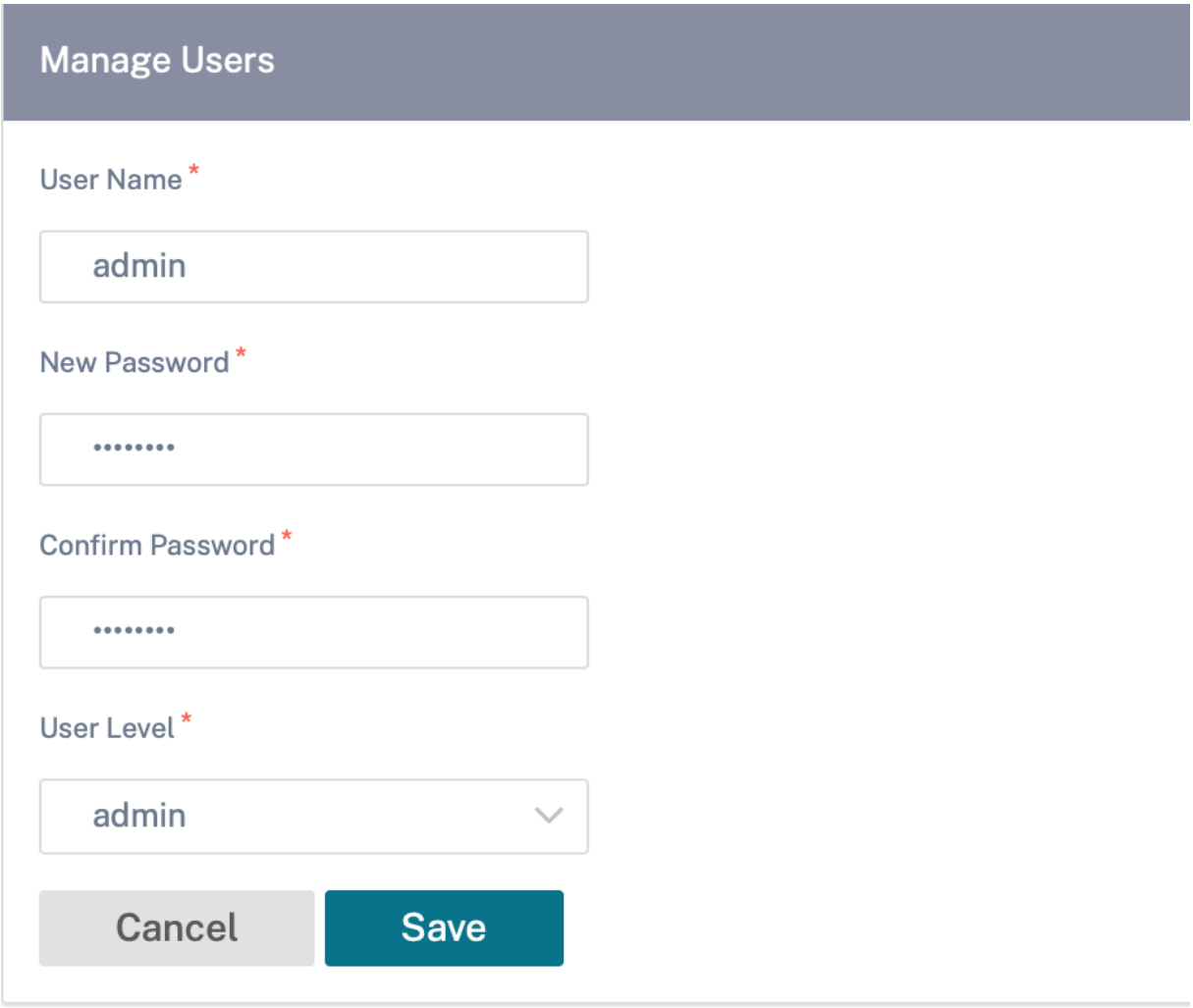
Sie können neue Benutzerkonten für die Site hinzufügen. Um einen neuen Benutzer hinzuzufügen, navigieren Sie zu **Konfiguration** > **Appliance-Einstellungen** > **Administratorschnittstelle** > **Benutzer verwalten**, und klicken Sie auf **+Benutzer**.



Geben Sie die folgenden Details an:

- **Benutzername**: Der Benutzername für das Benutzerkonto.
- **Neues Passwort**: Das Passwort für das Benutzerkonto.
- **Passwort bestätigen**: Geben Sie das Passwort erneut ein, um es zu bestätigen.
- **Benutzerstufe**: Wählen Sie eine der folgenden Kontoberechtigungen aus:
  - **Admin**: Ein Admin-Konto hat Lese- und Schreibzugriff auf alle Einstellungen. Ein Administrator kann eine Konfiguration und ein Softwareupdate für das Netzwerk durchführen.
  - **Betrachter**: Ein Viewer-Konto ist ein schreibgeschütztes Konto mit Zugriff auf die Bereiche Dashboard, Reporting und Monitoring.
  - **Netzwerkadministrator**: Ein Netzwerkadministrator hat Lese- und Schreibzugriff auf die Netzwerkeinstellung und schreibgeschützten Zugriff für andere Einstellungen.
  - **Sicherheitsadministrator**: Ein Sicherheitsadministrator hat Lese- und Schreibzugriff für die Firewall/Sicherheitsbezogene Einstellungen und schreibgeschützten Zugriff für andere Einstellungen.

    > **Hinweis**
    >
    > Der Sicherheitsadministrator hat die Berechtigung, den Schreibzugriff auf die Firewall für andere Benutzer (Admin/Viewer) zu deaktivieren.

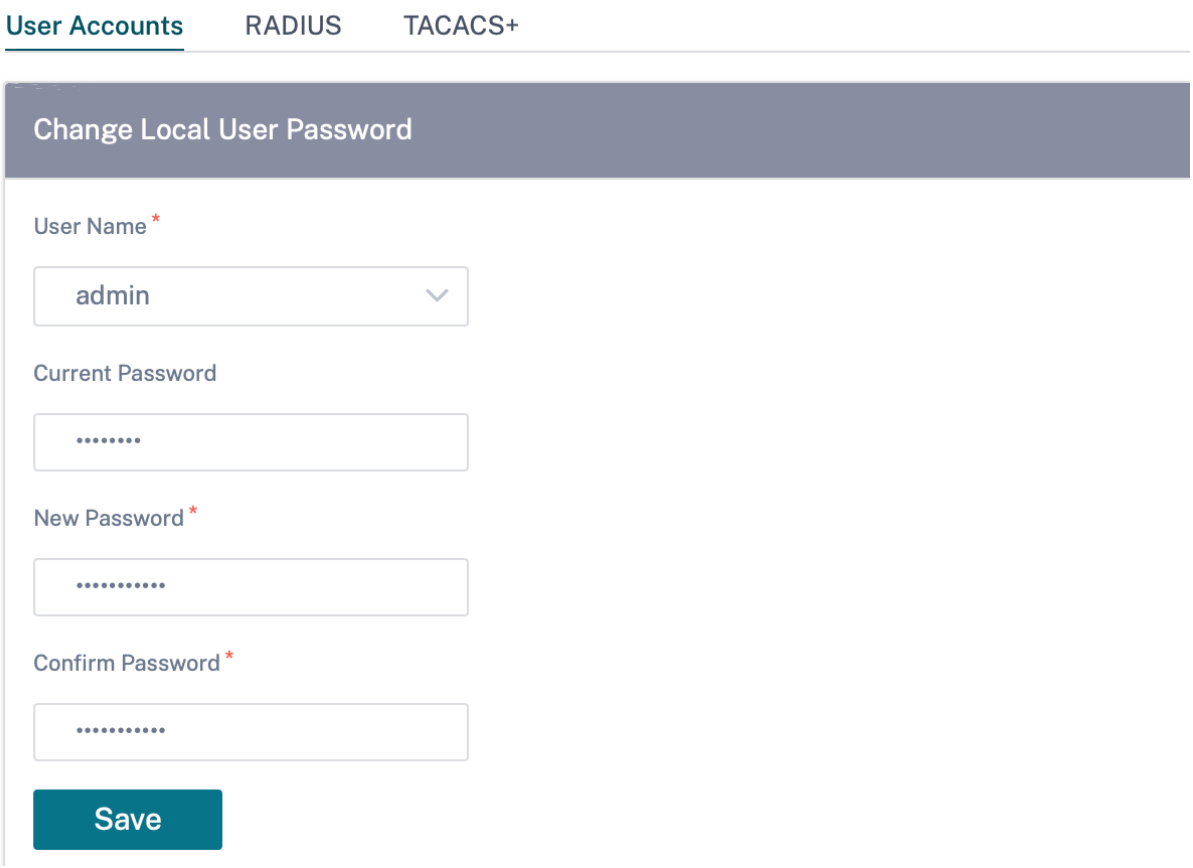


Um einen Benutzer zu löschen, wählen Sie einen Benutzernamen aus und klicken Sie auf **Ausgewählten Benutzer löschen**. Das Benutzerkonto und die lokalen Dateien werden gelöscht.

Ändern Sie das lokale Benutzerkennwort

Um das lokale Benutzerkennwort zu ändern, navigieren Sie zu **Konfiguration** > **Appliance-Einstellungen** > **Administrative Oberfläche** > **Benutzerkonten** > **Lokales Benutzerkennwort ändern** und geben Sie die folgenden Werte an:

- **Benutzername**: Wählen Sie aus der Liste der auf der Site konfigurierten Benutzer einen Benutzernamen aus, für den Sie das Kennwort ändern möchten.
- **Aktuelles Passwort**: Geben Sie das aktuelle Passwort ein. Dieses Feld ist für Admin-Benutzer optional.
- **Neues Passwort**: Geben Sie ein neues Passwort Ihrer Wahl ein.
- **Passwort bestätigen**: Geben Sie das Passwort erneut ein, um es zu bestätigen.



RADIUS-Authentifizierungsserver

RADIUS ermöglicht die Remote-Benutzerauthentifizierung auf der Appliance. Um die RADIUS-Authentifizierung verwenden zu können, müssen Sie mindestens einen RADIUS-Server angeben und konfigurieren. Optional können Sie redundante Backup-RADIUS-Server bis zu maximal drei konfigurieren. Die Server werden nacheinander überprüft. Stellen Sie sicher, dass die erforderlichen Benutzerkonten auf dem RADIUS-Authentifizierungsserver erstellt wurden.

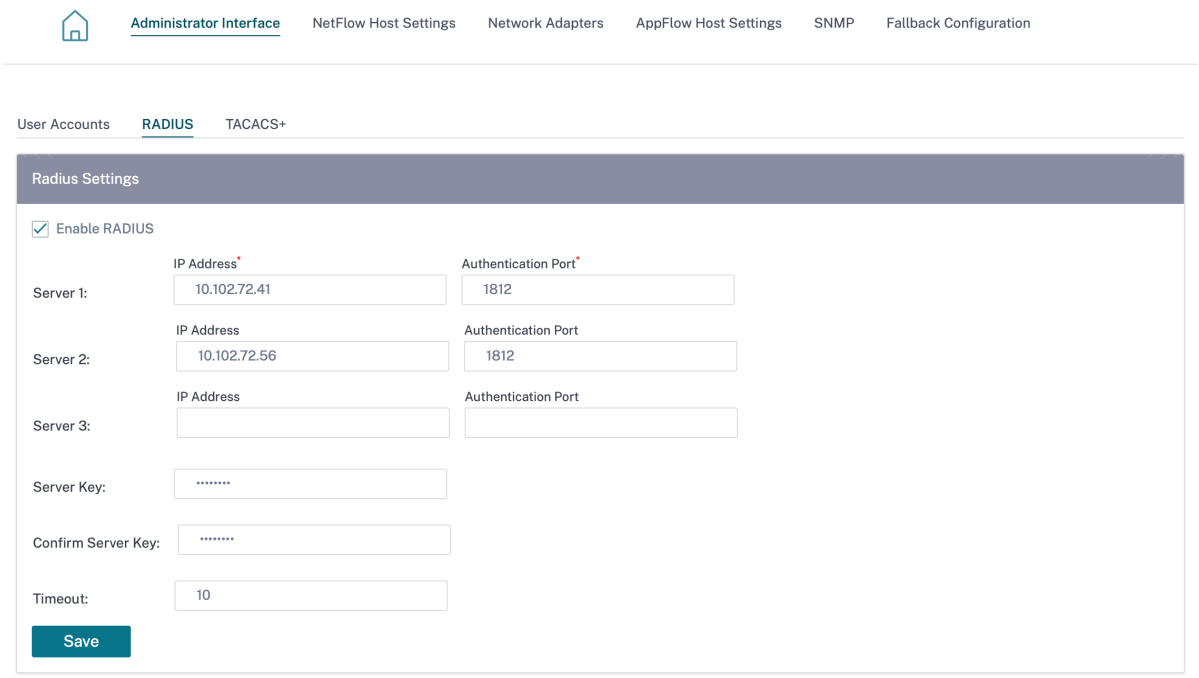
Um die RADIUS-Authentifizierung zu konfigurieren, navigieren Sie zu **Konfiguration** > **Appliance-Einstellungen** > **Administrative Schnittstelle** > **RADIUS**und klicken Sie auf **RADIUS aktivieren**.

> **Hinweis**
>
> Sie können entweder die RADIUS- oder TACACS+-Authentifizierung auf einer Site aktivieren. Sie können nicht beide gleichzeitig aktivieren.

Geben Sie die Host-IP-Adresse des RADIUS-Servers und die Authentifizierungs-Portnummer an. Die Standardportnummer ist 1812. Geben Sie einen Serverschlüssel ein und bestätigen Sie ihn, dass es

sich um einen geheimen Schlüssel handelt, mit dem eine Verbindung zum RADIUS-Server hergestellt wird. Geben Sie das Zeitintervall an, das auf eine Authentifizierungsantwort vom RADIUS-Server gewartet wird. Der Timeout-Wert muss kleiner oder gleich 60 Sekunden sein.

> **Hinweis**
>
> Die Einstellungen **für Serverschlüssel** und **Timeout** werden auf alle konfigurierten Server angewendet.



TACACS+-Authentifizierungsserver

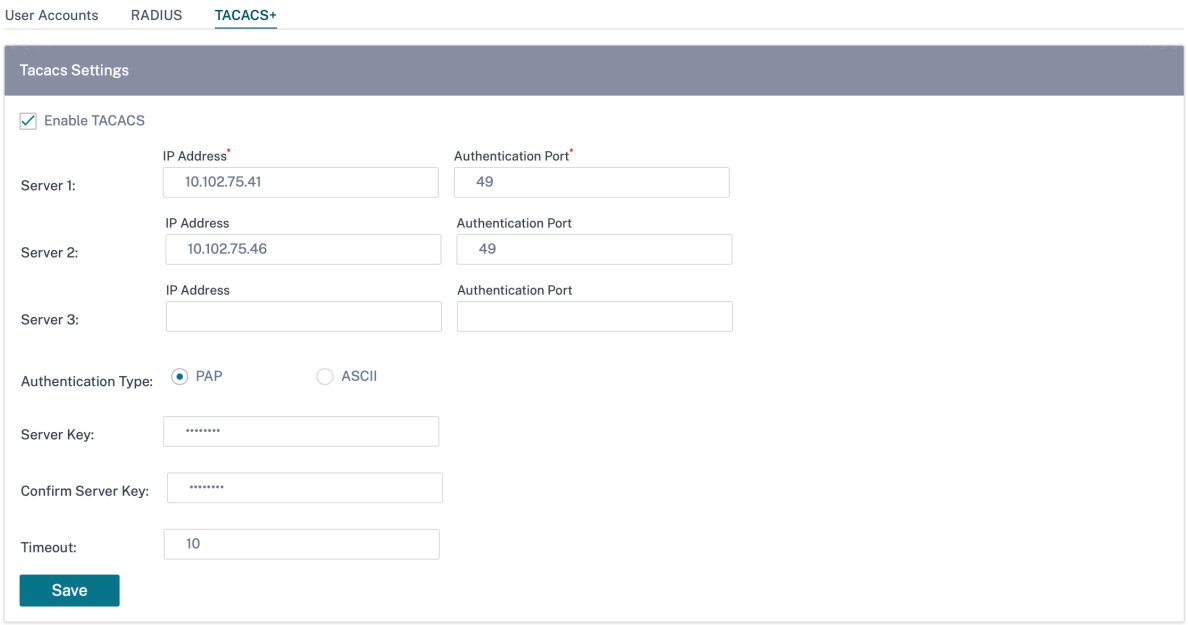
TACACS+ ermöglicht die Remote-Benutzerauthentifizierung auf der Appliance. Um die TACACS+-Authentifizierung verwenden zu können, müssen Sie mindestens einen TACACS+-Server angeben und konfigurieren. Optional können Sie redundante Backup-TACACS+-Server bis zu maximal drei konfigurieren. Die Server werden nacheinander überprüft. Stellen Sie sicher, dass die erforderlichen Benutzerkonten auf dem TACACS+-Authentifizierungsserver erstellt wurden.

Um die TACACS+-Authentifizierung zu konfigurieren, navigieren Sie zu **Konfiguration** > **Appliance-Einstellungen** > **Administrative Schnittstelle** > **TACACS+** und klicken Sie auf **TACACS+ aktivieren**.

> **Hinweis**
>
> Sie können entweder die RADIUS- oder TACACS+-Authentifizierung auf einer Site aktivieren. Sie können nicht beide gleichzeitig aktivieren.

1. Wählen Sie die Verschlüsselungsmethode aus, um den Benutzernamen und das Kennwort an den TACACS+-Server zu senden.
2. Geben Sie die Host-IP-Adresse des TACACS+-Servers und die Authentifizierungs-Portnummer an. Die Standardportnummer ist 49.
3. Geben Sie einen Serverschlüssel ein und bestätigen Sie ihn. Es ist ein geheimer Schlüssel, der für die Verbindung mit dem TACACS+-Server verwendet wird.
4. Geben Sie das Zeitintervall an, in dem auf eine Authentifizierungsantwort vom TACACS+-Server gewartet wird. Der Timeout-Wert muss kleiner oder gleich 60 Sekunden sein.

> **Hinweis**
>
> Die **Einstellungen für**Authentifizierungstyp**,**Serverschlüssel**und Timeout** werden auf alle konfigurierten Server angewendet.



NetFlow Host-Einstellungen

NetFlow Collectors sammeln IP-Netzwerkverkehr, wenn es in eine SD-WAN-Schnittstelle eintritt oder diese verlässt. Mithilfe von NetFlow-Daten können Sie die Quelle und das Ziel des Traffics, die Serviceklasse und die Ursachen für Verkehrsüberlastung ermitteln. Weitere Informationen finden Sie unter Multiple NetFlow Collector.

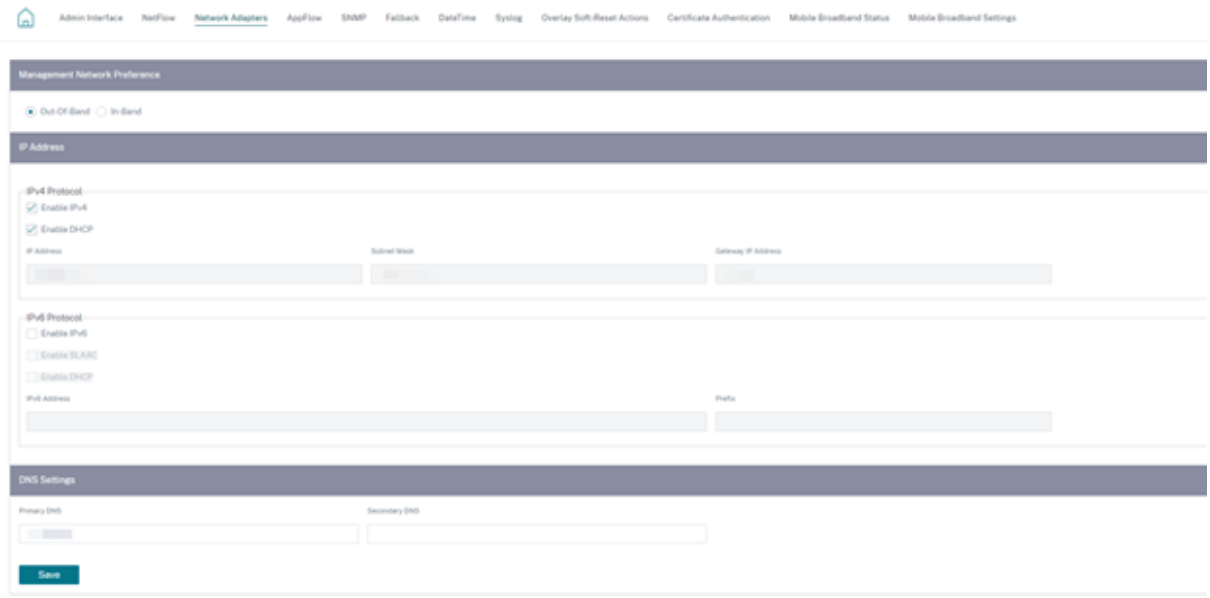
Sie können bis zu drei NetFlow-Hosts konfigurieren. Um NetFlow-Hosteinstellungen zu konfigurieren, navigieren Sie zu **Konfiguration** > **Appliance-Einstellungen** > **NetFlow-Host-Einstellungen**. Wählen Sie **NetFlow aktivieren** aus und geben Sie die IP-Adresse und Portnummer des NetFlow-Hosts an.

Netzwerkadapter

Für Citrix SD-WAN-Appliances können Sie die Verwaltungsnetzwerkpräferenz, die Verwaltungs-IP-Adresse und andere Netzwerkparameter manuell ändern. Sie können die IPv4-Adresse, die Subnetzmaske, die Gateway-IP-Adresse, die IPv6-Adresse und das Präfix der Appliance ändern oder die IP-Adresse automatisch abrufen, indem Sie DHCP oder SLAAC aktivieren (nur für IPv6-Adressen). Weitere Informationen finden Sie unter Dynamisches Host-Konfigurationsprotokoll.

> **Hinweis**
>
> - Sie können die IP-Adresse nicht ändern, wenn die Schnittstelle für die In-Band-Verwaltung verwendet wird. Weitere Informationen zur In-Band-Verwaltung finden Sie unter In-Band-Verwaltung.
> - Die In-Band-Option funktioniert nur, wenn Sie einen Datenport als In-Band-Management-Port konfiguriert haben und der Internetdienst konfiguriert ist. Stellen Sie sicher, dass Sie über die Konfiguration zur Unterstützung der In-Band-Verwaltung für die SD-WAN-Appliance verfügen, bevor Sie die Verwaltungseinstellung festlegen.
> - Der Abschnitt Verwaltungsnetzwerkeinstellungen (Inband und Out-of-Band) ist sichtbar, wenn auf der Appliance eine Softwareversion von 11.4.2 oder höher ausgeführt wird.

Um die Netzwerkadaptereinstellungen zu konfigurieren, navigieren Sie zu **Konfiguration** > **Geräteeinstellungen** > **Netzwerkadapter**.



AppFlow Host-Einstellungen

AppFlow und IPFIX sind Flow-Exportstandards, mit denen Anwendungs- und Transaktionsdaten in der Netzwerkinfrastruktur identifiziert und gesammelt werden. Diese Daten geben eine bessere Einsicht in die Auslastung und Leistung des Anwendungsdatenverkehrs.

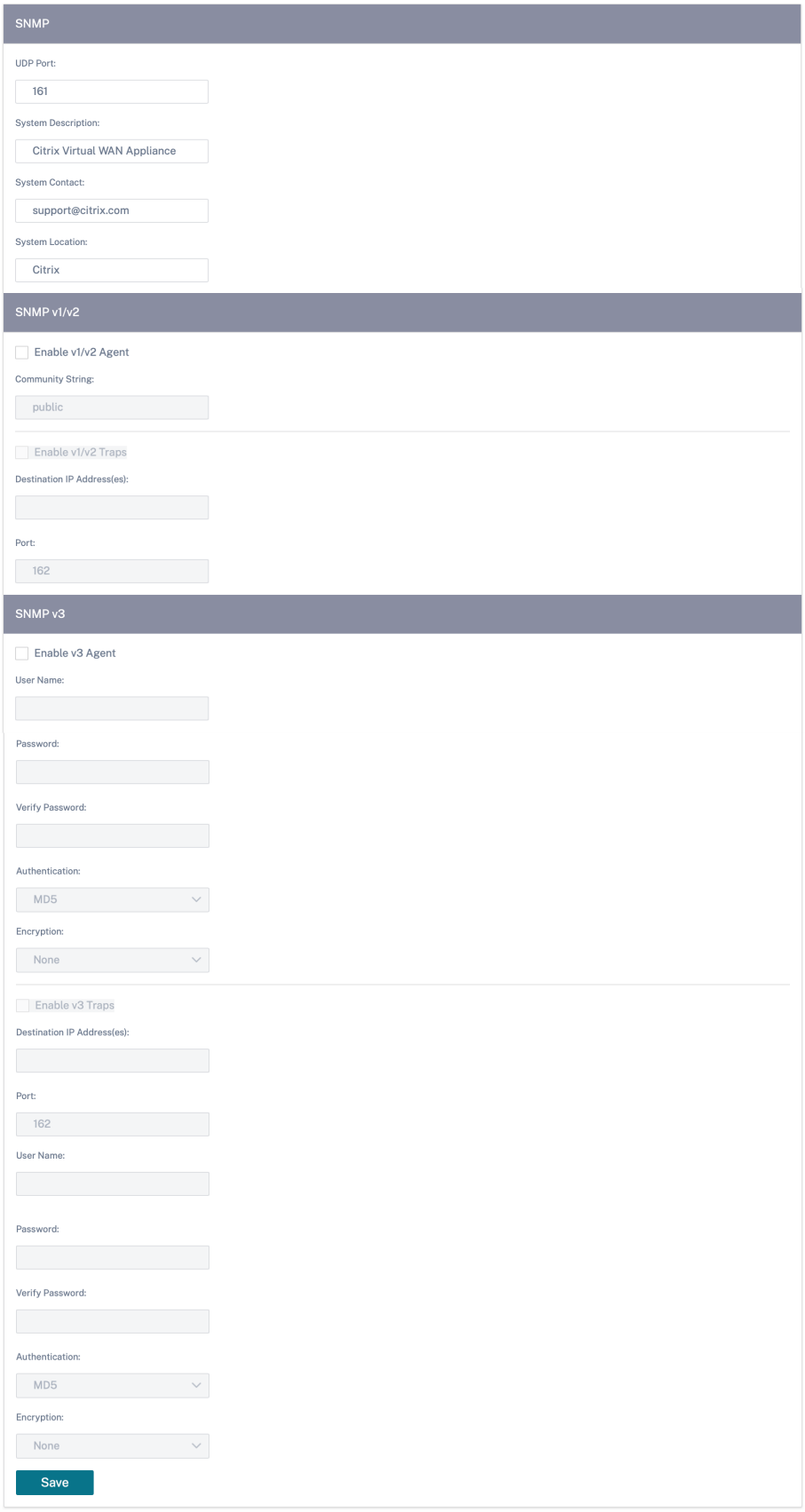
Die gesammelten Daten, Flussaufzeichnungen genannt, werden an einen oder mehrere IPv4-Sammler übertragen. Die Kollektoren aggregieren die Flow-Datensätze und generieren Echtzeit- oder historische Berichte. Weitere Informationen finden Sie unter AppFlow und IPFIX.

SNMP

SNMP wird zum Austausch von Verwaltungsinformationen zwischen Netzwerkgeräten verwendet. SNMPv1 ist die erste Version des SNMP-Protokolls. SNMPv2 ist das überarbeitete Protokoll, das Verbesserungen bei Protokollpakettypen, Transport-Mappings und MIB-Strukturelementen enthält. SNMPv3 definiert die sichere Version des SNMP. Das SNMPv3-Protokoll erleichtert auch die Remote-Konfiguration der SNMP-Entitäten.

Der SNMP-Agent sammelt die Verwaltungsinformationen lokal von der Appliance und sendet sie bei jeder Abfrage an den SNMP-Manager. Wenn der Agent ein Notfallereignis auf der Appliance erkennt, sendet er eine Warnmeldung an den Manager, ohne darauf zu warten, dass Daten abgefragt werden. Diese Notfallnachricht wird als Falle bezeichnet. Aktivieren Sie die erforderlichen Agenten der SNMP-Version, die entsprechenden Traps und geben Sie die erforderlichen Informationen an. Für weitere Details siehe SNMP.

Um SNMP-Einstellungen zu konfigurieren, navigieren Sie zu **Konfiguration** > **Appliance-Einstellungen** > **SNMP**

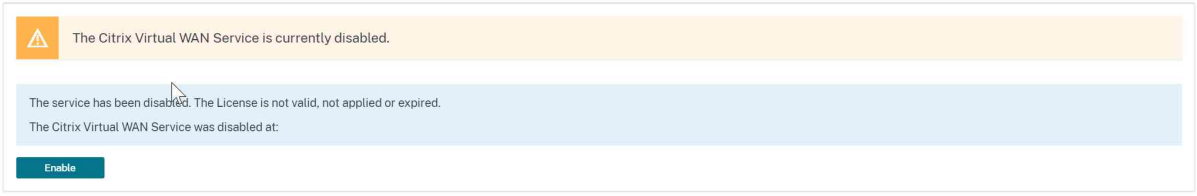


Fallback-Konfiguration

Die Fallback-Konfiguration stellt sicher, dass die Appliance mit dem Zero-Touch-Bereitstellungsdienst verbunden bleibt, wenn ein Verbindungsfehler, eine Konfigurations- oder Softwarekdiskrepanz vorliegt. Die Fallbackkonfiguration ist standardmäßig auf den Appliances aktiviert, die über ein Standardkonfigurationsprofil verfügen. Sie können die Fallback-Konfiguration auch gemäß Ihren vorhandenen LAN-Netzwerkeinstellungen bearbeiten. Weitere Informationen finden Sie unter Fallback-Konfiguration.

Strömungen

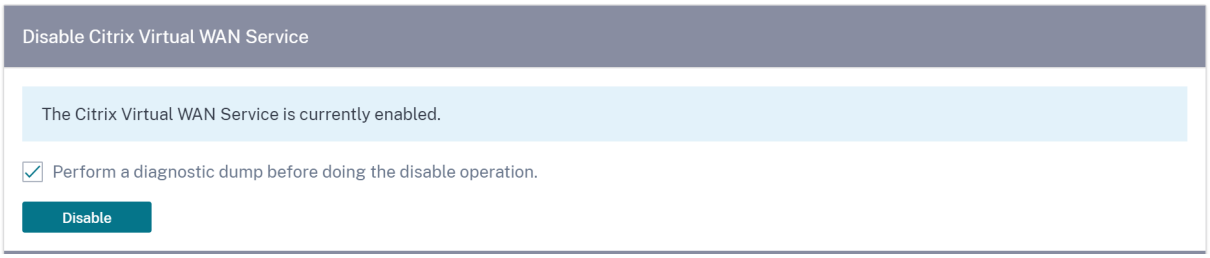
Im Abschnitt Flows können Sie den Citrix Virtual WAN-Dienst auf der Appliance aktivieren oder deaktivieren. Durch die Aktivierung des Dienstes wird der Virtual WAN-Daemon aktiviert und gestartet. Eine Option zum Aktivieren des Citrix Virtual Wan Service ist verfügbar, wenn der Dienst deaktiviert ist.



Deaktivieren des Citrix Virtual WAN-Dienstes

Die Option **Citrix Virtual WAN-Dienst deaktivieren** ist verfügbar, wenn der Dienst aktiviert ist. Durch Deaktivieren des Dienstes wird der Virtual WAN-Daemon auf der Appliance gestoppt.

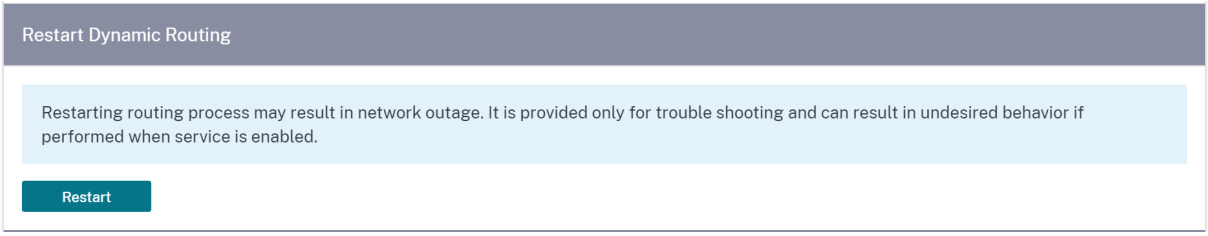
Sie können einen Diagnoseabzug des virtuellen WAN-Netzwerks sammeln, bevor Sie den Citrix Virtual WAN-Dienst deaktivieren.



Dynamisches Routing neu

Sie können den dynamischen Routenlernprozess über die Routingprotokolle OSPF und BGP neu starten. Die Option Dynamisches Routing neu starten wird nur zur Fehlerbehebung bereitgestellt.

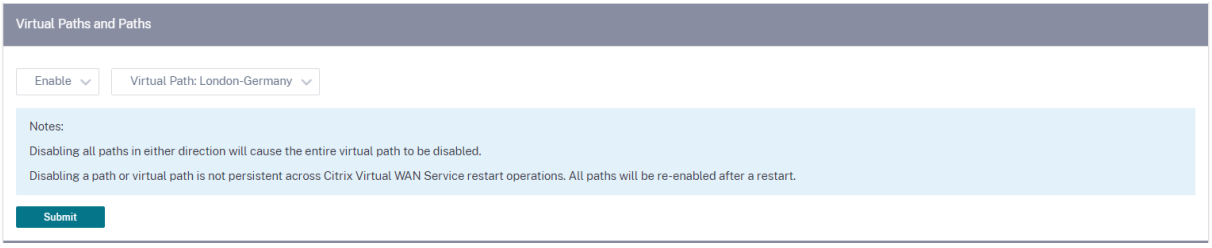
> **Warnung**
>
> Ein Neustart des dynamischen Routings kann zu einem Netzwerkausfall führen.



Virtuelle Pfade

Sie können den virtuellen Pfad zwischen zwei Standorten aktivieren oder deaktivieren. Sie können entweder die zugrunde liegenden einzelnen Pfade in beide Richtungen oder den virtuellen Overlay-Pfad auswählen. Durch das Deaktivieren einzelner Pfade wird der gesamte virtuelle Pfad deaktiviert.

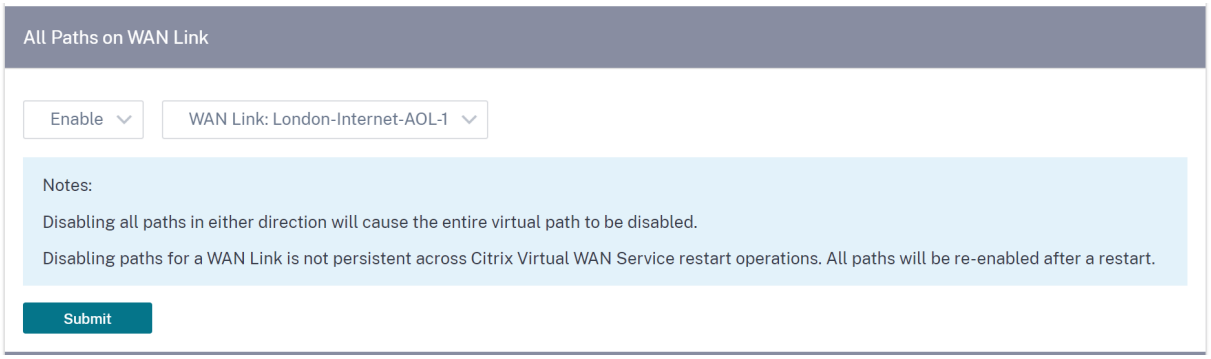
> **Hinweis**
>
> Alle Pfade werden nach dem Neustart des Citrix Virtual WAN-Dienstes wieder aktiviert.



Alle Pfade auf WAN-Link

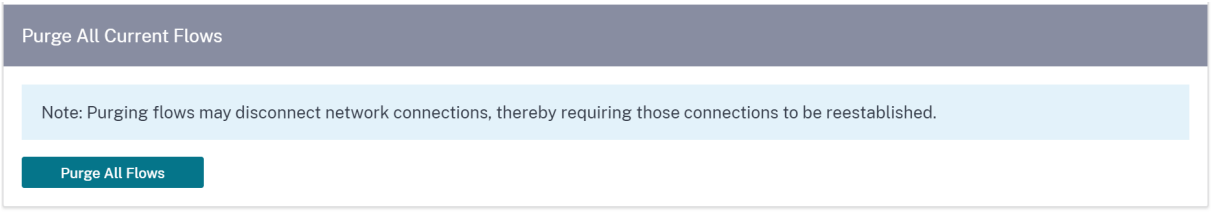
Sie können wählen, ob WAN-Verbindungen zwischen zwei Standorten aktiviert oder deaktiviert werden sollen. Durch Deaktivieren aller WAN-Verbindungen wird der virtuelle Pfad deaktiviert.

> **Hinweis**
>
> Alle WAN-Verbindungen werden nach dem Neustart des Citrix Virtual WAN-Dienstes wieder aktiviert.



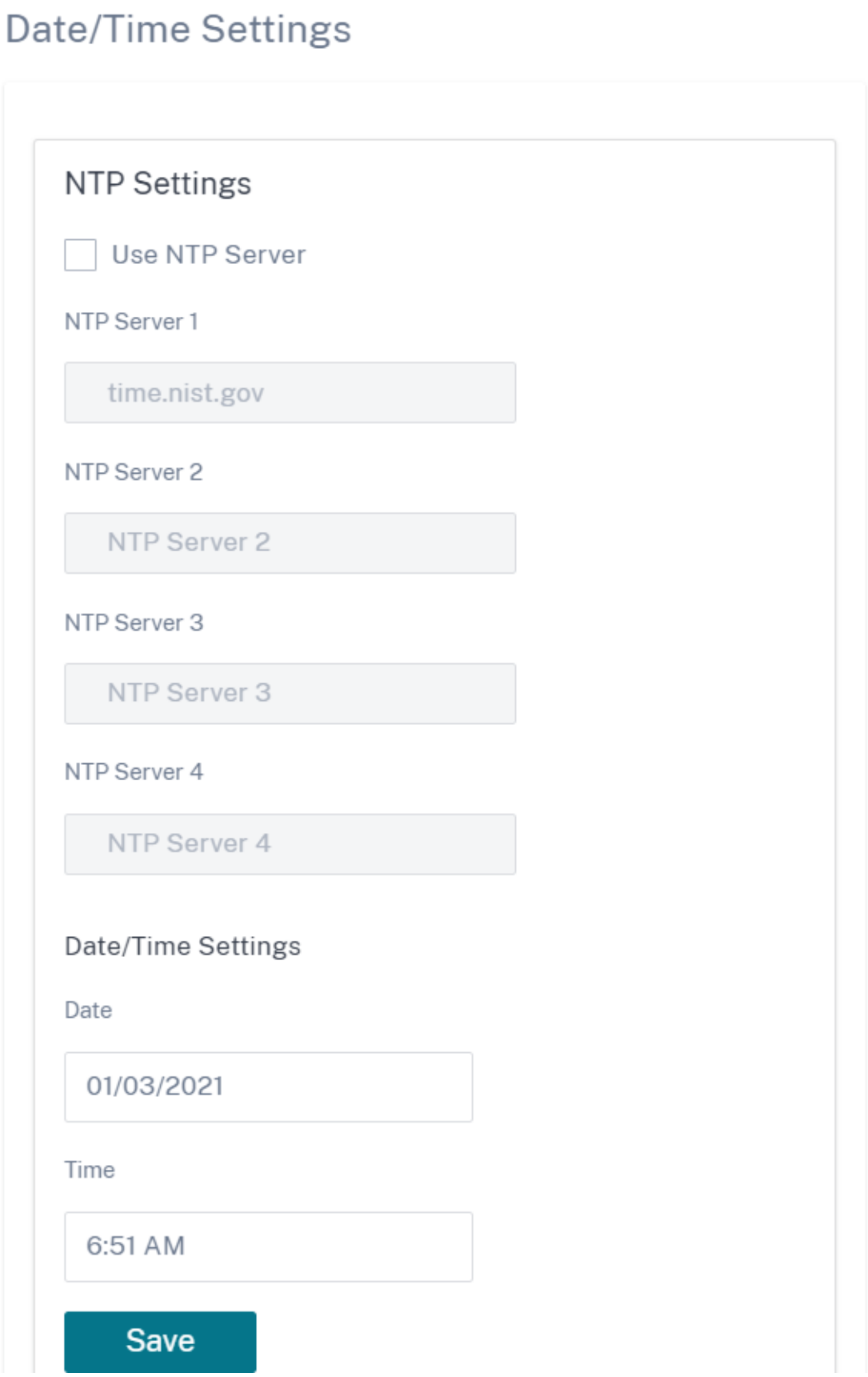
Alle Stromflüsse löschen

Durch das Löschen von Flows werden alle Stromflüsse beendet, die Flusstabellen werden gelöscht, die Flussverbindungen werden wiederhergestellt und die Flow-Tabelle wird erneut aufgefüllt.

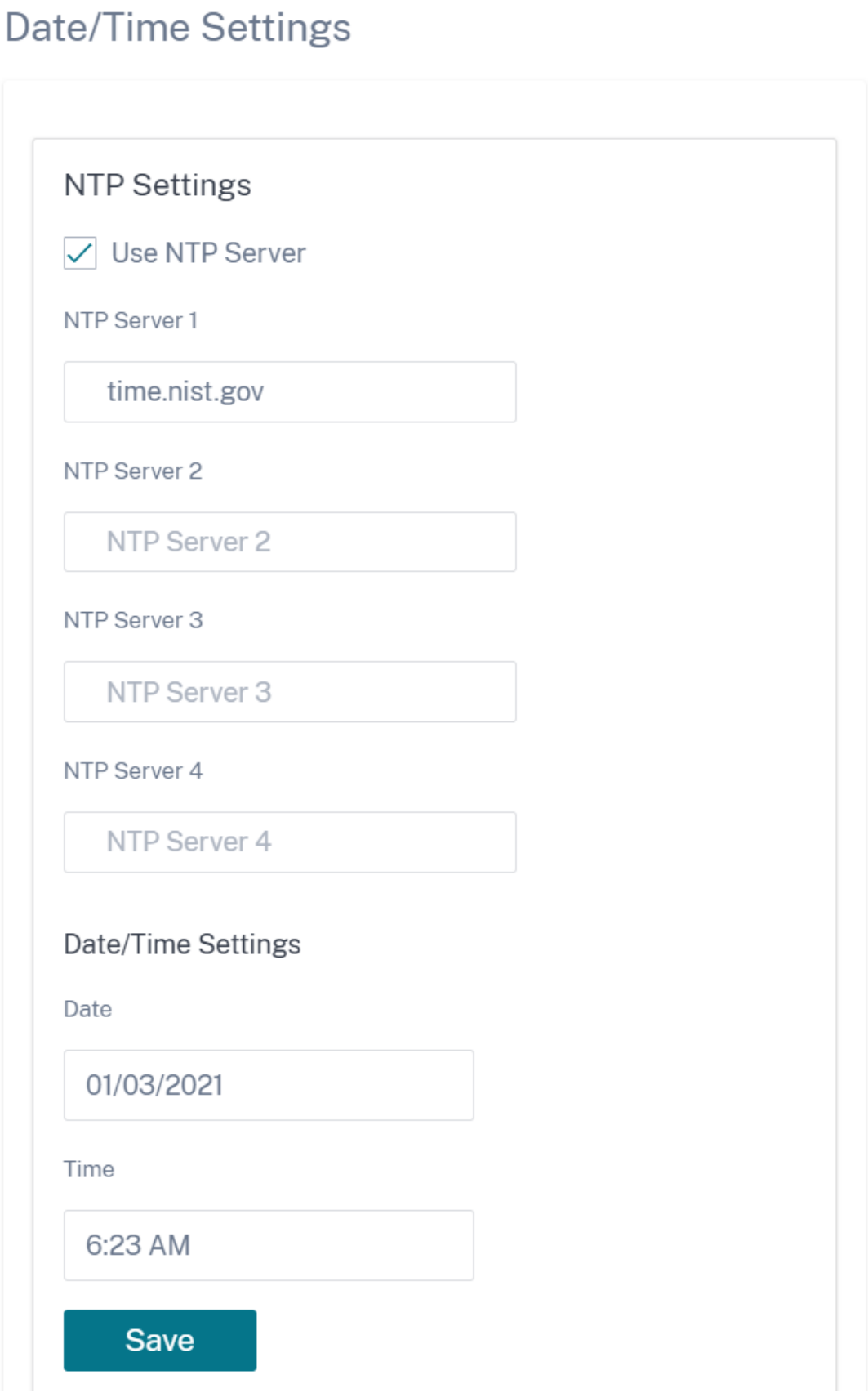


Datum und Uhrzeit

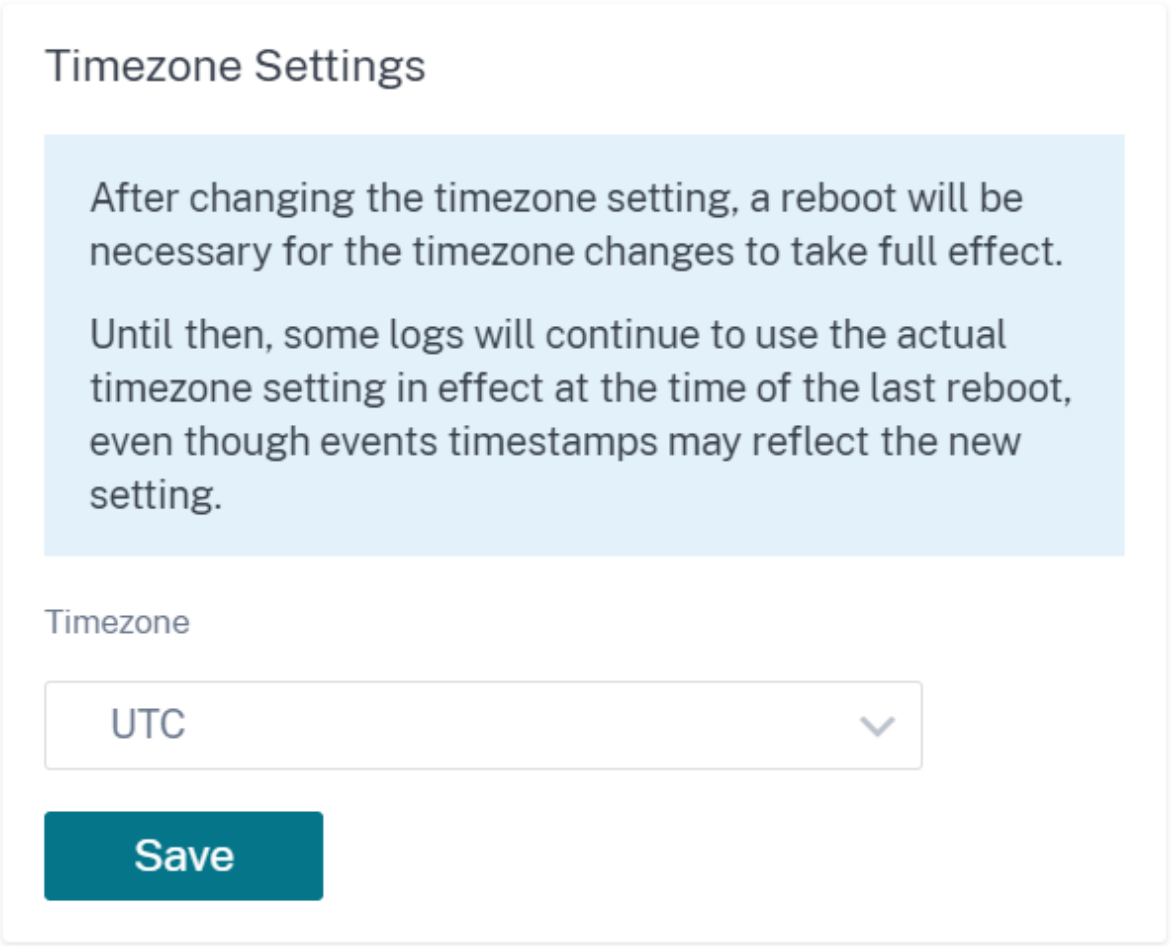
Sie können das Datum und die Uhrzeit der Appliance entweder manuell oder mithilfe eines NTP-Servers ändern. Um Datum und Uhrzeit manuell zu konfigurieren, stellen Sie sicher, dass die Option **NTP-Server verwenden** nicht ausgewählt ist, und geben Sie Datum und Uhrzeit an.



Wenn Sie die Option **NTP-Server verwenden** auswählen, können Sie das aktuelle Datum und die aktuelle Uhrzeit nicht manuell eingeben. Sie können bis zu 4 NTP-Server angeben, aber Sie müssen mindestens einen angeben. Diese fungieren als Backup-NTP-Server. Wenn ein Server ausgefallen ist, synchronisiert sich die Appliance automatisch mit dem anderen NTP-Server. Wenn Sie einen Domänennamen für einen NTP-Server angeben, müssen Sie auch einen DNS-Server konfigurieren, sofern Sie dies nicht bereits getan haben.

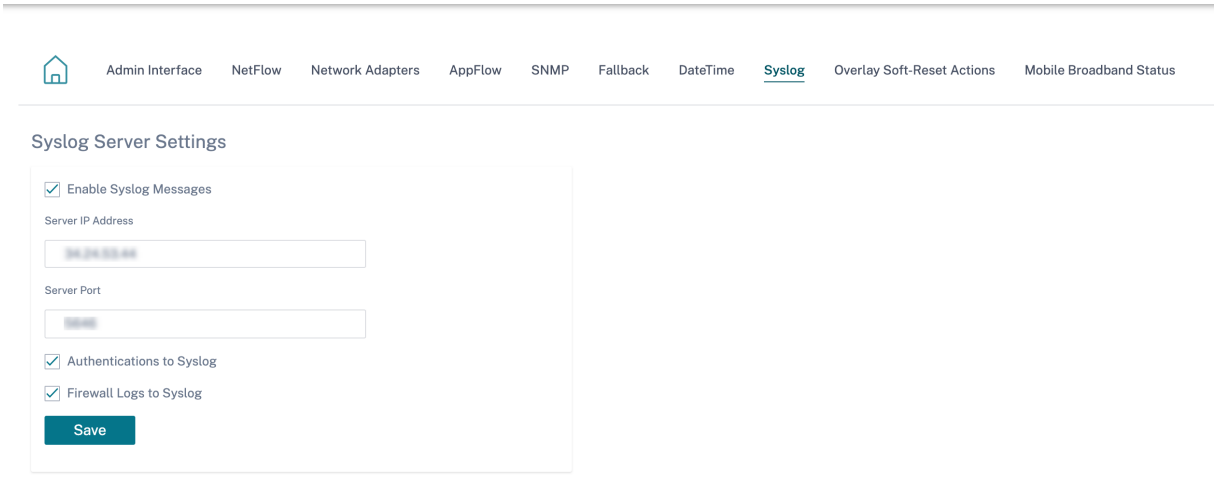


Wenn die Zeitzone geändert werden muss, ändern Sie sie, bevor Sie Datum und Uhrzeit festlegen. Andernfalls bleiben Ihre Einstellungen nicht erhalten. Starten Sie die Appliance nach dem Ändern der Zeitzone neu.



Syslog-Servereinstellungen

Sie können die Syslog-Servereinstellungen von SD-WAN-Appliances mithilfe des Citrix SD-WAN Orchestrator Service konfigurieren. Durch Aktivieren der Syslog-Einstellungen können Sie Systemwarnungen und Ereignisdetails von SD-WAN-Appliances an einen externen Syslog-Server senden. Sie müssen jedoch den Ereignistyp auf der Benutzeroberfläche der SD-WAN-Appliance auswählen, indem Sie zu **Konfiguration** > **Appliance-Einstellungen** > **Protokollierung/Überwachung** > **Alarmoptionen**navigieren. Weitere Informationen finden Sie unter Konfigurieren von Alarmen.



Die folgenden Syslog-Servereinstellungen können über den Citrix SD-WAN Orchestrator Service konfiguriert werden:

- **Syslog-Meldungen**aktivieren: Aktivieren oder deaktivieren Sie das Senden von Protokollen oder Ereignismeldungen an den Syslog-Server.
- **Server-IP-Adresse**: IP-Adresse des Syslog-Servers.
- **Server-Port**: Portnummer des Syslog-Servers.
- **Authentifizierung bei Syslog**: Aktivieren oder deaktivieren Sie das Senden von Authentifizierungsprotokollen oder Ereignismeldungen an den Syslog-Server.
- **Firewall-Protokolle an Syslog**: Aktivieren oder deaktivieren Sie das Senden von Firewallprotokollen an den Syslog-Server.

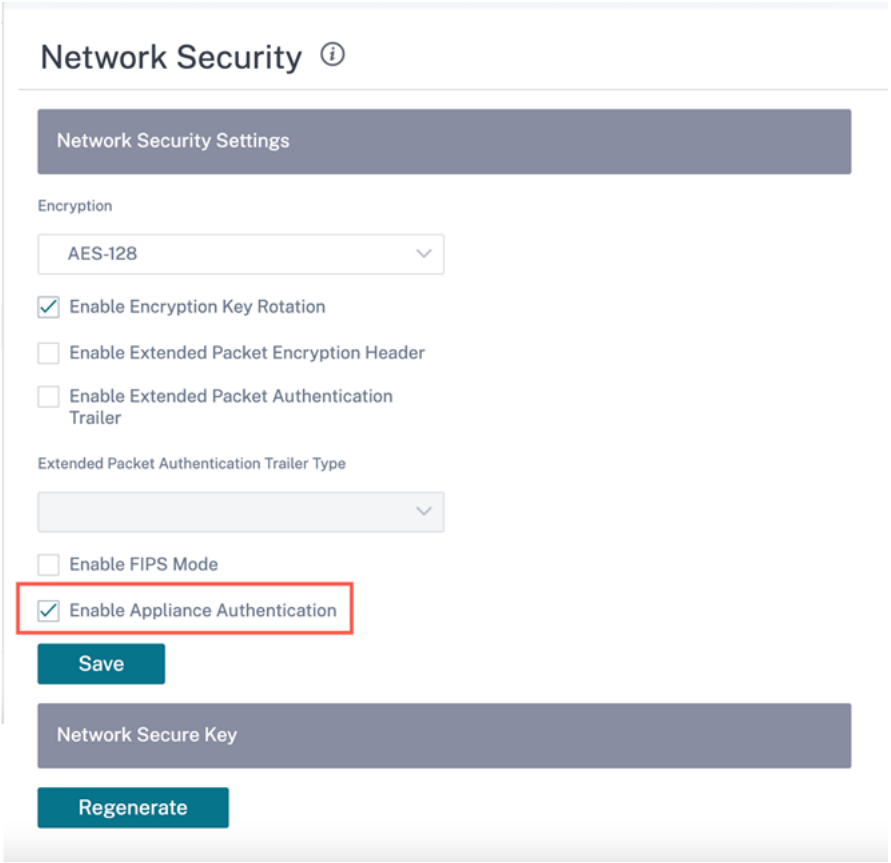
Zertifikatauthentifizierung

Der Citrix SD-WAN Orchestrator Service stellt sicher, dass sichere Pfade zwischen Appliances im SD-WAN-Netzwerk mithilfe von Sicherheitstechniken wie Netzwerkverschlüsselung und IPSec-Tunneln für virtuelle Pfade eingerichtet werden. Zusätzlich zu den vorhandenen Sicherheitsmaßnahmen wird die zertifikatbasierte Authentifizierung im Citrix SD-WAN Orchestrator Service eingeführt.

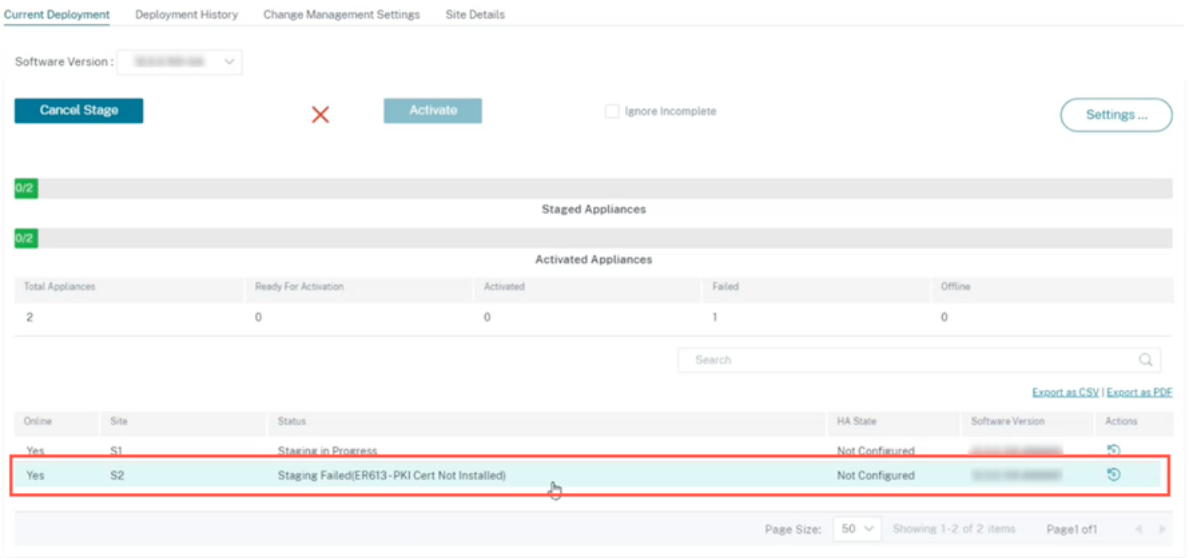
Die Zertifikatauthentifizierung ermöglicht es Unternehmen, von ihrer privaten Zertifizierungsstelle (CA) ausgestellte Zertifikate zur Authentifizierung von Appliances zu verwenden. Die Appliances werden authentifiziert, bevor die virtuellen Pfade eingerichtet werden. Wenn beispielsweise eine Zweigeinheit versucht, eine Verbindung zum Rechenzentrum herzustellen, und das Zertifikat von der Zweigstelle nicht mit dem vom Rechenzentrum erwarteten Zertifikat übereinstimmt, wird der virtuelle Pfad nicht eingerichtet.

Das von der CA ausgestellte Zertifikat bindet einen öffentlichen Schlüssel an den Namen der Appliance. Der öffentliche Schlüssel arbeitet mit dem entsprechenden privaten Schlüssel, der im Besitz der durch das Zertifikat identifizierten Appliance ist.

Um die Appliance-Authentifizierung zu aktivieren, navigieren Sie auf Netzwerkebene zu **Konfiguration** > **Sicherheit** > **Netzwerksicherheit** und wählen Sie **Appliance-Authentifizierung aktivieren**aus. Klicken Sie auf **Speichern**.

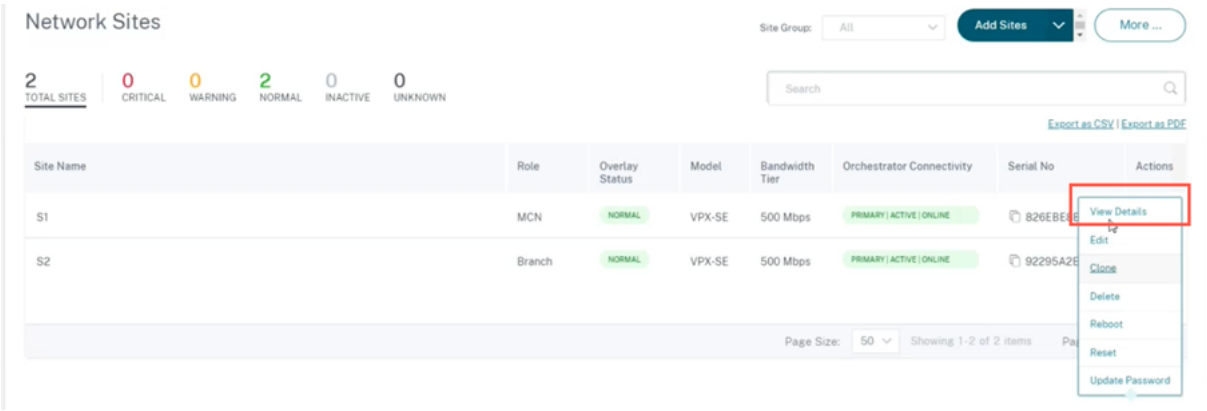


Wenn während der Bereitstellung die Appliance-Authentifizierung aktiviert ist, aber kein PKI-Zertifikat in der Appliance installiert ist, zeigt das Staging den Status „Fehlgeschlagen“an.

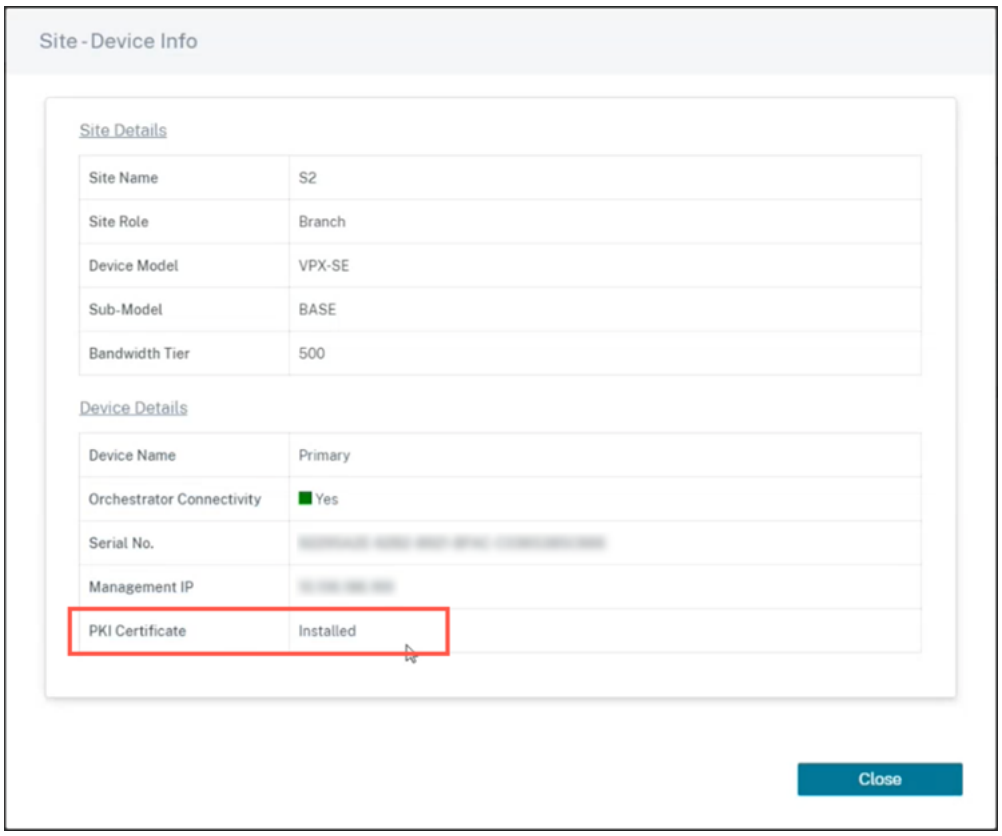


Zertifikat ansehen

Sie können auf der Gerätedetailseite überprüfen, ob das PKI-Zertifikat installiert ist oder nicht. Navigieren Sie dazu zu **Konfiguration >**Netzwerkstartseite**** klicken Sie auf das **Aktionssymbol** für die Site, für die Sie das Zertifikat verifizieren möchten, und klicken Sie auf **Details anzeigen**.



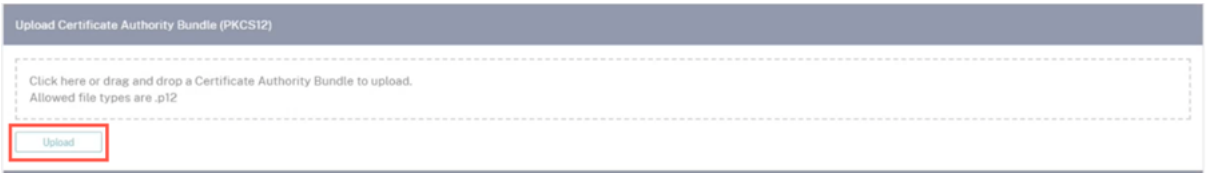
Der folgende Bildschirm wird mit den Site- und Gerätedetails gefüllt:



Im Abschnitt **Gerätedetails** können Sie den Installationsstatus des PKI-Zertifikats anzeigen.

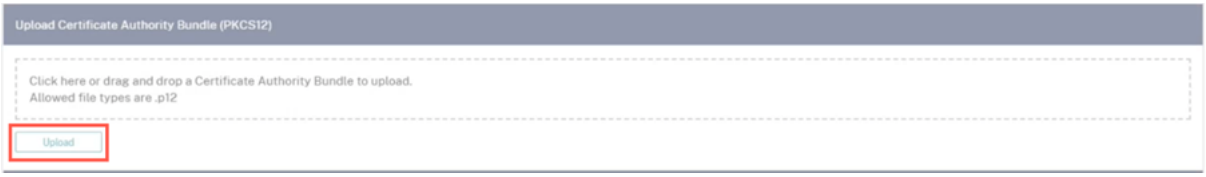
Identitätsbündel hochladen

Das Identity-Paket enthält einen privaten Schlüssel und das dem privaten Schlüssel zugeordnete Zertifikat. Sie können das von der CA ausgestellte Appliance-Zertifikat in die Appliance hochladen. Das Zertifikatspaket ist eine PKCS12-Datei mit der Erweiterung.p12. Sie können es mit einem Kennwort schützen. Ziehen Sie die PKCS12-Datei per Drag & Drop, geben Sie ein Passwort ein und klicken **Sie**auf Wenn Sie das Passwortfeld leer lassen, wird es als kein Passwortschutz behandelt.



Laden Sie das Paket der Zertifizierungsstelle hoch

Laden Sie das PKCS12-Bundle hoch, das der Zertifikatssignierstelle entspricht. Das Zertifizierungsstellenpaket umfasst die komplette Signaturkette, den Stamm und alle zwischengeschalteten Unterzeichnerautoritäten. Ziehen Sie das PKCS12-Paket und klicken Sie auf **Hochladen**.



Erstellen einer Signaturanfrage für

Die Appliance kann ein unsigniertes Zertifikat generieren und eine Certificate Signing Request (CSR) erstellen. Um eine CSR für eine Appliance zu erstellen, geben Sie den Organisationsnamen, die Einheit, die Stadt, die Provinz/Region/den Landkreis/die Stadt, das Land und die E-Mail-Adresse an. Der allgemeine Name der Appliance ist der Site-Name, der automatisch ausgefüllt wird und nicht bearbeitet werden kann. Klicken Sie auf **Create CSR**.

Anfrage zur Zertifikatssignierung

Sobald die CSR erfolgreich vom Backend generiert wurde, müssen Sie die CSR von der Appliance herunterladen und von ihrer Zertifizierungsstelle signieren lassen und sie im PEM- oder DER-Format wieder auf die Appliance hochladen. Dies wird als Identitätszertifikat für die Appliance verwendet. Laden Sie zuerst die CA hoch, um das Zertifikat zu signieren

Laden Sie die signierte CSR hoch, sobald die Zertifizierungsstelle hochgeladen wurde.

Listenmanager für Zertifikatsperrung

Eine Certificate Revocation List (CRL) ist eine veröffentlichte Liste von Zertifikatseriennummern, die im Netzwerk nicht mehr gültig sind. Die CRL-Datei wird regelmäßig heruntergeladen und lokal auf der gesamten Appliance gespeichert. Wenn ein Zertifikat authentifiziert wird, überprüft der Responder die Zertifikatsperrliste, um zu sehen, ob das Initiatorenzertifikat bereits gesperrt wurde. Citrix SD-WAN unterstützt derzeit CRLs der Version 1 im PEM- und DER-Format.

Um CRL zu aktivieren, aktivieren Sie das Kontrollkästchen CRL enabled. Geben Sie den Speicherort an, an dem die CRL-Datei verwaltet wird. HTTP-, HTTPS- und FTP-Speicherorte werden unterstützt. Geben Sie das Zeitintervall zum Überprüfen und Herunterladen der CRL-Datei an. Der Bereich beträgt 1—1440 Minuten. Klicken Sie auf **Einstellungen hochladen**.

> **Hinweis:**
>
> Der Zeitraum für die erneute Authentifizierung für einen virtua1-Pfad kann zwischen 10 und 15 Minuten liegen. Wenn das CRL-Aktualisierungsintervall auf eine kürzere Dauer festgelegt ist, kann die aktualisierte CRL-Liste eine aktuell aktive Seriennummer enthalten. Stellen Sie ein aktiv gesperrtes Zertifikat für kurze Zeit in Ihrem Netzwerk zur Verfügung.

Einstellungen für mobiles Breitband

Mit dem Citrix SD-WAN Orchestrator Service können Sie eine Citrix SD-WAN-Appliance von Ihrem Zweigstellenstandort aus über eine mobile Breitbandverbindung mit einem Netzwerk verbinden.

Um die Einstellungen für mobiles Breitband zu konfigurieren, navigieren Sie auf Standortebene zu **Konfiguration** > **Appliance-Einstellungen > Einstellungenfür mobiles Breitband**.

Derzeit können die Einstellungen für mobiles Breitband auf Citrix SD-WAN 110- und Citrix SD-WAN-210-Appliances konfiguriert werden.

Sie können die folgenden Einstellungen für mobiles Breitband im Citrix SD-WAN Orchestrator Service konfigurieren.

SIM-PIN-Status

Wenn Sie eine SIM-Karte eingelegt haben, die mit einer PIN gesperrt ist, lautet der SIM-Status **Aktiviert**. Sie können die SIM-Karte erst verwenden, wenn sie mit der SIM-PIN verifiziert wurde. Sie können die SIM-PIN vom Anbieter erhalten. Klicken Sie auf **Verify**.

Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **Verifizieren**.

SIM-PIN deaktivieren Sie können die SIM-PIN-Funktion für eine SIM deaktivieren, für die SIM-PIN aktiviert und verifiziert ist. Klicken Sie auf **Deaktivieren**. Gib die SIM-PIN ein und klicke auf **Deaktivieren**

SIM-PIN aktivieren Um die SIM PIN zu aktivieren, klicken Sie auf **Aktivieren**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **Aktivieren**.

Wenn sich der Status der SIM-PIN in **Aktiviert und Nicht verifiziert**ändert, bedeutet dies, dass die PIN nicht verifiziert wurde und Sie keine Vorgänge ausführen können, bis die PIN überprüft wurde.

Klicken Sie auf **PIN überprüfen**. Geben Sie die vom Anbieter bereitgestellte SIM-PIN ein und klicken Sie auf **PIN überprüfen**.

SIM-PIN ändern Sobald die PIN im Status **Aktiviert und Verifiziert** ist, können Sie die PIN ändern.

Klicken Sie auf **Ändern**. Geben Sie die vom Netzanbieter bereitgestellte SIM-PIN ein. Geben Sie die neue SIM-PIN ein und bestätigen Sie sie. Klicken Sie auf **Ändern**.

SIM aufheben Wenn Sie die SIM-PIN vergessen haben, können Sie die SIM-PIN mithilfe der vom Träger erhaltenen SIM-PUK zurücksetzen.

Um die Blockierung einer SIM aufzuheben, klicken Sie auf **Sperre aufheben**. Geben Sie die vom Netzbetreiber erhaltene SIM-PIN und SIM-PUK ein und klicken Sie auf **Entsperren**.

> **Hinweis**
>
> Die SIM-Karte wird mit 10 erfolglosen Versuche von PUK dauerhaft blockiert, während die SIM-Karte entsperrt wird. Wenden Sie sich an den Mobilfunkanbieter, um eine neue SIM-Karte zu erhalten.

APN-Einstellungen

Um die APN-Einstellungen zu konfigurieren, geben Sie den APN, den Benutzernamen, das Passwort und die Authentifizierung ein, die vom Netzbetreiber bereitgestellt wurden. Sie können zwischen **PAP-,**CHAP****- oder **PAPCHAP-Authentifizierungsprotokollen** wählen. Wenn der Anbieter keinen Authentifizierungstyp angegeben hat, setzen Sie ihn auf **Keine**.

Netzwerkeinstellungen

Sie können das Mobilfunknetz auf Citrix SD-WAN-Appliances auswählen, die interne Modems unterstützen.

Roaming

Die Roaming-Option ist standardmäßig auf Ihren Geräten aktiviert. Sie können es deaktivieren.

Firmware verwalten

Jedes Gerät, das LTE aktiviert hat, verfügt über eine Reihe verfügbarer Firmware. Sie können aus der vorhandenen Firmware-Liste auswählen oder eine Firmware hochladen und anwenden. Wenn Sie sich nicht sicher sind, welche Firmware Sie verwenden sollen, wählen Sie die Option AUTO-SIM, damit das LTE-Modem die passendste Firmware basierend auf der im Gerät eingelegten SIM-Karte auswählen kann.

> **Hinweis**
>
> Derzeit kann die Firmware nur auf SD-WAN SE 210 LTE-Geräten angewendet werden.

Modem aktivieren/deaktivieren

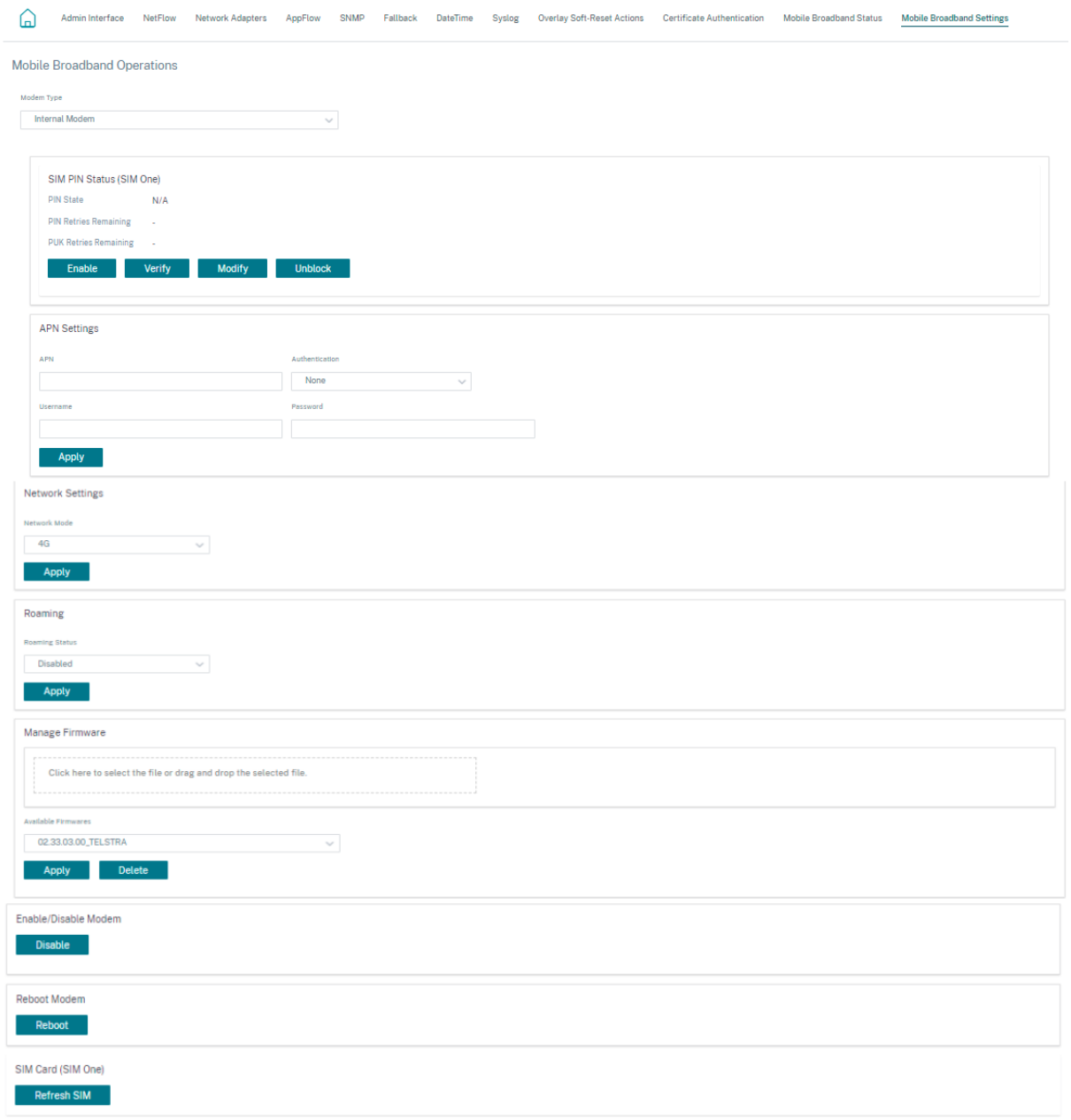
Aktivieren oder deaktivieren Sie das Modem, je nachdem, ob Sie die Breitbandfunktion verwenden möchten. Standardmäßig ist das Modem aktiviert.

Modem neu starten

Startet das Modem neu. Dieser Vorgang kann bis zu 3-5 Minuten dauern, bis der Neustartvorgang abgeschlossen ist.

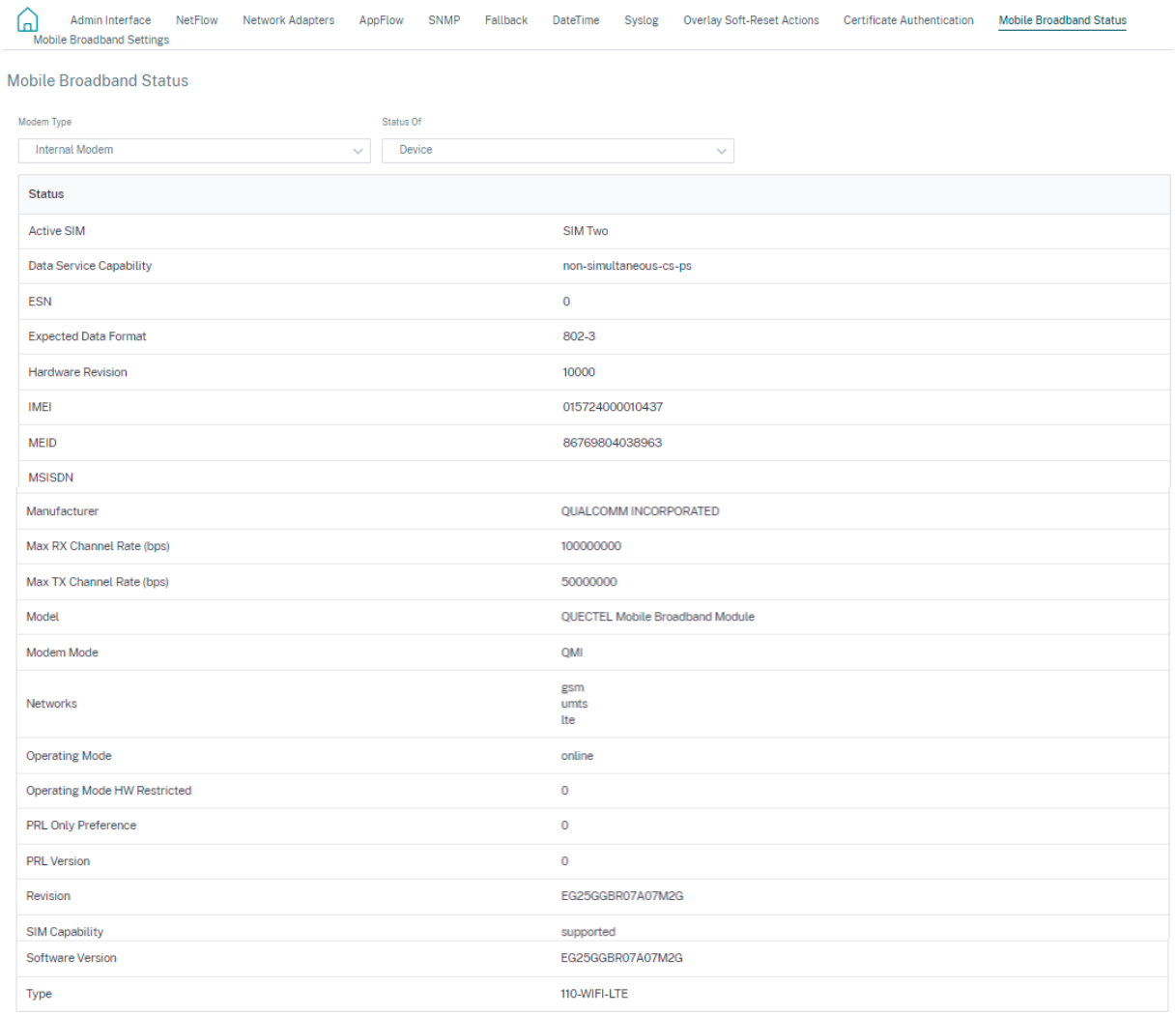
SIM aktualisieren

Verwenden Sie diese Option, wenn Sie die SIM-Karte im laufenden Betrieb austauschen, um eine neue SIM-Karte zu erkennen.



Status des mobilen Breitbands

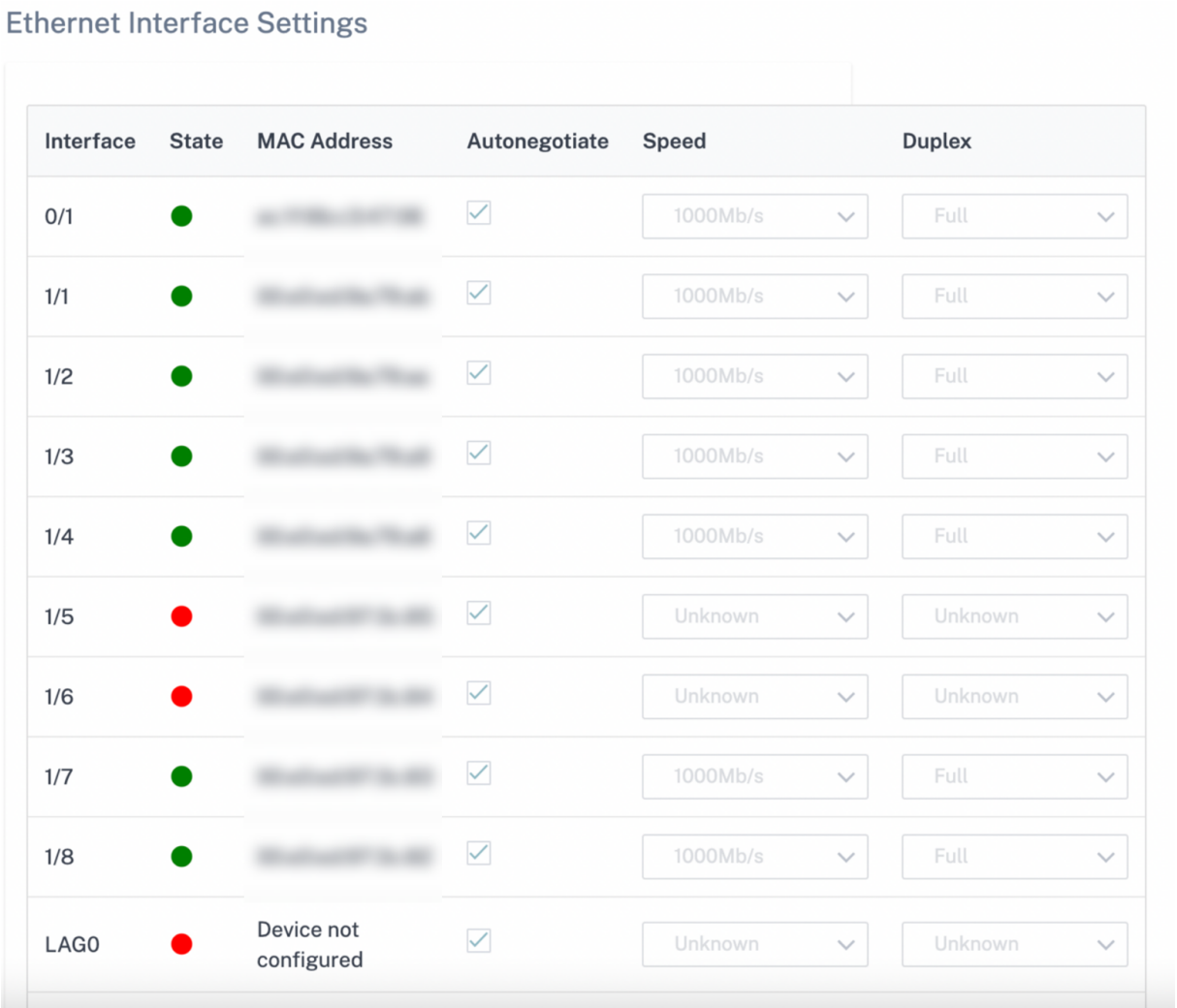
Im Abschnitt Status des mobilen Breitbandnetzes wird der Status Ihrer Breitbandkonfigurationseinstellungen angezeigt. Um den Status des mobilen Breitbandnetzes anzuzeigen, navigieren Sie auf Standortebene zu **Konfiguration** > **Appliance-Einstellungen** > **Status des mobilen Breitbandnetzes**. Sie können den Status Ihres Geräts und der aktiven SIM-Karte anzeigen.



Einstellungen der Ethernet-Schnittstelle

Im Abschnitt Status der Ethernet-Schnittstelle werden der Konnektivitätsstatus der Ethernet-Ports, der Schnittstellentyp, die MAC-Adresse, die automatische Absprache und die Duplexeinstellungen angezeigt. Um die Ethernet-Schnittstelleneinstellungen anzuzeigen, navigieren Sie auf Standortebene zu **Konfiguration** > **Appliance-Einstellungen** > **Ethernet-Schnittstelleneinstellungen**. Die administrativ ausgelaufenen Ports werden rot angezeigt.

> **Hinweis:**
>
> Diese Einstellung ist derzeit im schreibgeschützten Modus auf der Benutzeroberfläche des Citrix SD-WAN Orchestrator Service verfügbar. Wenn Sie die Ethernet-Schnittstelleneinstellungen ändern möchten, können Sie dies mithilfe der neuen Benutzeroberfläche für SD-WAN-Appliances tun.



In-Band-Verwaltung

October 21, 2022

Mit dem Citrix SD-WAN Orchestrator Service können Sie die SD-WAN-Appliance auf zwei Arten verwalten: Out-of-Band-Verwaltung und In-Band-Verwaltung. Mit der Out-of-Band-Verwaltung können Sie eine Verwaltungs-IP mit einem für die Verwaltung reservierten Port erstellen, der nur den Verwaltungsdatenverkehr trägt. Mit der In-Band-Verwaltung können Sie die SD-WAN-Datenports für die Verwaltung verwenden. Es überträgt sowohl Daten- als auch Verwaltungsdatenverkehr, ohne einen zusätzlichen Verwaltungspfad konfigurieren zu müssen.

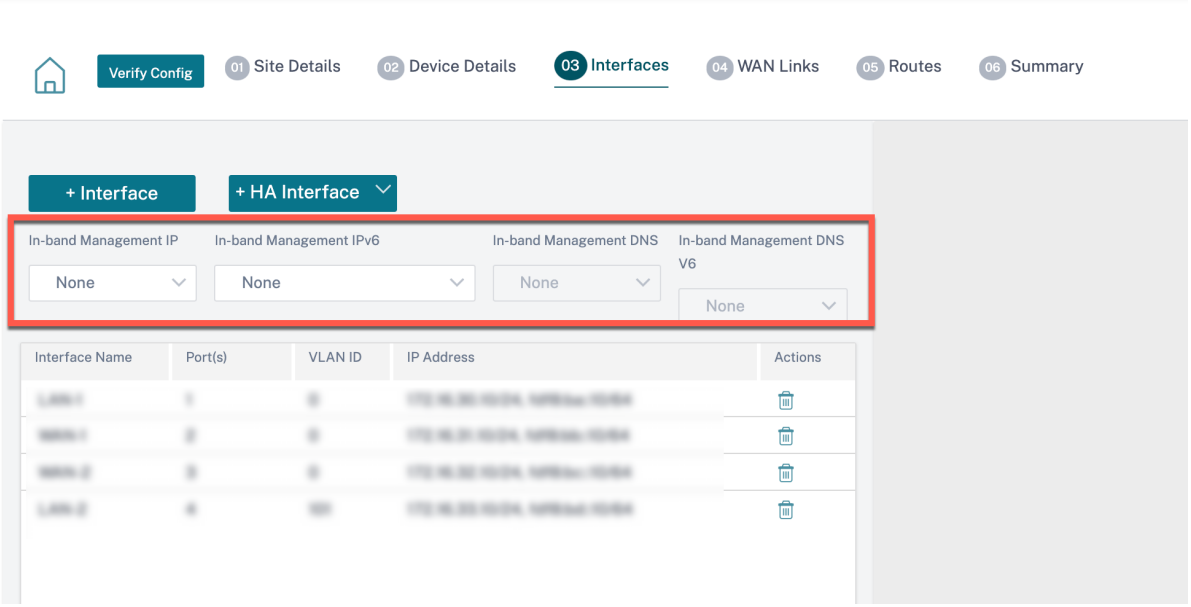
Durch die In-Band-Verwaltung können virtuelle IP-Adressen mit Verwaltungsdiensten wie Web-UI und SSH verbunden werden. Sie können die In-Band-Verwaltung auf einer vertrauenswürdigen

Schnittstelle aktivieren, die für IP-Dienste verwendet werden kann. Sie können auf die Web-UI und SSH über die Management-IP und virtuelle In-Band-IPs zugreifen.

> **Hinweis**
>
> Die In-Band-Verwaltung im Citrix SD-WAN Orchestrator Service wird für Citrix SD-WAN 11.1.1 und höher unterstützt.

Um die In-Band-Verwaltung auf einer virtuellen IP zu aktivieren, navigieren Sie auf Standortebene zu **Konfiguration** > **Standortkonfiguration** > **Schnittstellen**. Wählen Sie die virtuelle IP aus, die als In-Band-Verwaltungsport verwendet werden soll. Sie können die **InBand Management IP** oder **InBand Management IPv6** verwenden, um auf die Web-Benutzeroberfläche und SSH zuzugreifen.

> **Hinweis**
>
> Die In-Band-Verwaltung wird nur auf LAN-Ports unterstützt.



Eine detaillierte Vorgehensweise zur Konfiguration einer virtuellen IP-Adresse finden Sie unter Schnittstellen.

Das In-Band-Management-IP fungiert auch als IP zur Backup-Verwaltung. Sie wird als Verwaltungs-IP-Adresse verwendet, wenn der Verwaltungsport nicht mit einem Standard-Gateway konfiguriert ist. Wählen Sie den **DNS-Proxy** aus, an den alle DNS-Anforderungen über die In-Band-Verwaltungsebene weitergeleitet werden. Informationen zur Konfiguration des DNS-Proxy finden Sie unter DNS-Proxy.

In Anwendungsfällen, in denen die Appliance-Konnektivität zum Citrix SD-WAN Orchestrator Service zwischen Verwaltungs- und Inband-Ports umschaltet, konfigurieren Sie **InBand Management DNS** oder **InBand Management DNS V6**, um eine unterbrechungsfreie Konnektivität des Citrix SD-WAN Orchestrator Service sicherzustellen.

In-Band-Provisioning

Die Notwendigkeit, SD-WAN-Appliances in einfacheren Umgebungen wie zu Hause oder in kleinen Zweigstellen bereitzustellen, ist deutlich gestiegen. Das Konfigurieren separater Verwaltungszugriff für einfachere Bereitstellungen stellt einen zusätzlichen Overhead dar. Die Zero-Touch-Bereitstellung zusammen mit der In-Band-Verwaltungsfunktion ermöglicht die Provisioning und Konfigurationsverwaltung über bestimmte Datenports. Die Zero-Touch-Bereitstellung wird auf den ausgewiesenen Datenports unterstützt und es ist nicht erforderlich, einen separaten Verwaltungsport für die Zero-Touch-Bereitstellung zu verwenden.

Sie können eine Appliance im werksseitigen Auslieferungszustand bereitstellen, die die In-Band-Provisioning unterstützt, indem Sie die Daten oder den Verwaltungsport mit dem Internet verbinden. Die Appliances, die die In-Band-Provisioning unterstützen, verfügen über spezifische Ports für LAN und WAN. Die Appliance im Factory-Reset-Zustand verfügt über eine Standardkonfiguration, die es ermöglicht, eine Verbindung mit dem Zero-Touch-Bereitstellungsdienst herzustellen. Der LAN-Port fungiert als DHCP-Server und weist dem WAN-Port, der als DHCP-Client fungiert, eine dynamische IP zu. Die WAN-Verbindungen überwachen den Quad 9-DNS-Dienst, um WAN-Konnektivität zu ermitteln.

Sobald die IP-Adresse abgerufen und eine Verbindung mit dem Zero-Touch-Bereitstellungsdienst hergestellt wurde, werden die Konfigurationspakete heruntergeladen und auf der Appliance installiert. Informationen zur Zero-Touch-Bereitstellung über den Citrix SD-WAN Orchestrator Service finden Sie unter Zero Touch Deployment.

> **Hinweis**
>
> - Die In-Band-Provisioning gilt für alle Plattformen. Die Standardkonfiguration ist jedoch nur auf Citrix SD-WAN 110- und VPX-Plattformen aktiviert, da die anderen Plattformen mit einer älteren Softwareversion ausgeliefert werden.
> - Für die 0-tägliche Provisioning von SD-WAN-Appliances über die Daten-Ports muss die Softwareversion der Appliance Citrix SD-WAN 11.1.1 oder höher sein.

Die Standardkonfiguration einer Appliance im Zurücksetzungsstatus auf Werkseinstellungen umfasst die folgenden Konfigurationen:

- DHCP-Server auf LAN-Anschluss
- DHCP-Client auf WAN-Port
- QUAD9-Konfiguration für DNS
- Die Standard-LAN-IP ist 192.168.101.1/24 für Citrix SD-WAN Appliances mit Factory-Image 11.1.1.39.
- Die Standard-LAN-IP ist 192.168.0.1/24 für Citrix SD-WAN 110 Appliance mit Factory-Image 11.0.4.
- Grace Lizenz von 35 Tagen.

Nach der Bereitstellung der Appliance wird die Standardkonfiguration deaktiviert und durch die vom Zero-Touch-Bereitstellungsdienst empfangene Konfiguration überschrieben. Wenn eine Appliance-Lizenz oder Grace-Lizenz abläuft, wird die Standardkonfiguration aktiviert, wodurch sichergestellt wird, dass die Appliance mit dem Zero-Touch-Bereitstellungsdienst verbunden bleibt und den lizenzverwalteten Dienst erhält.

Fallback-Konfiguration

Die Fallback-Konfiguration stellt sicher, dass die Appliance mit dem Zero-Touch-Bereitstellungsdienst verbunden bleibt, wenn ein Verbindungsfehler, eine Konfigurations- oder Softwarekdiskrepanz vorliegt. Die Fallbackkonfiguration ist standardmäßig auf den Appliances aktiviert, die über ein Standardkonfigurationsprofil verfügen. Sie können die Fallback-Konfiguration auch gemäß Ihren vorhandenen LAN-Netzwerkeinstellungen bearbeiten.

Die Fallback-Konfiguration behält die Konnektivität zur Appliance über die In-Band-Verwaltungs-IP der Appliance und den Citrix SD-WAN Orchestrator Service in den folgenden Szenarien bei:

- Wo die t2_App abstürzt
- Sie versuchen, die Konfiguration zurückzusetzen

In einem Szenario, in dem für eine Appliance die In-Band-Verwaltung konfiguriert ist und Sie die Konfiguration manuell zurücksetzen oder die t2_app aufgrund der Benutzerkonfiguration innerhalb von 120 Sekunden mehr als viermal abstürzt. In einem solchen Framework wird der Dienst deaktiviert und daher verlieren Sie die Konnektivität zum Citrix SD-WAN Orchestrator Service und der Appliance.

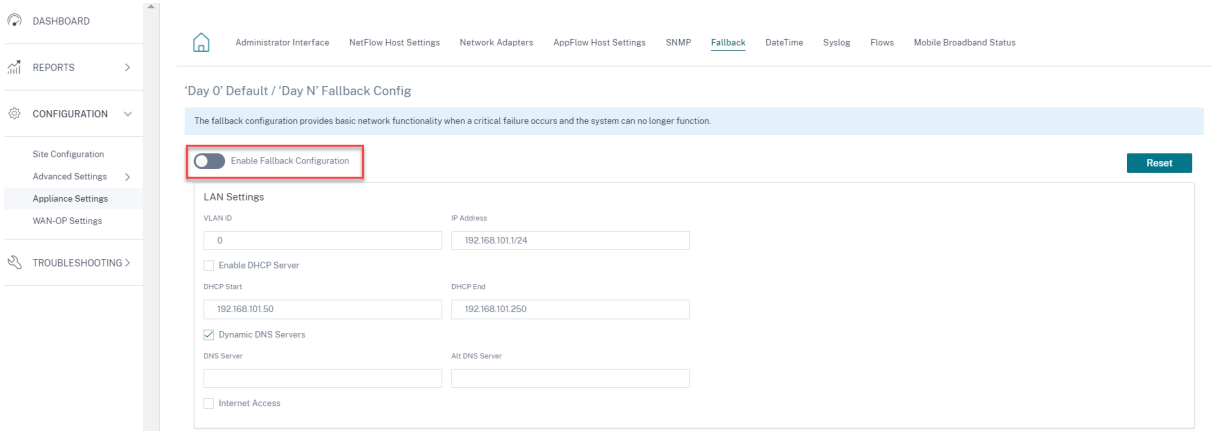
Wenn Sie jedoch die Fallback-Konfiguration aktiviert hatten, erhalten Sie die folgenden Funktionen:

- Grundlegender In-Band-Zugriff auf Verwaltungsfunktionen (Web-UI/SSH/SNMP)
- Fähigkeit der Appliance, über einen In-Band-Port eine Verbindung zu externen Diensten herzustellen (Citrix SD-WAN Orchestrator Service/ZTD)

In solchen Szenarien wird die Dienst-Appliance mit einer Fallback-Konfiguration mit aktiviertem Dienst zurückgesetzt, anstatt sie zu deaktivieren. Die Konnektivität zum Citrix SD-WAN Orchestrator Service und der Appliance über die In-Band-Verwaltungs-IP bleibt erhalten, solange die Verbindung über eine Internetverbindung verfügt.

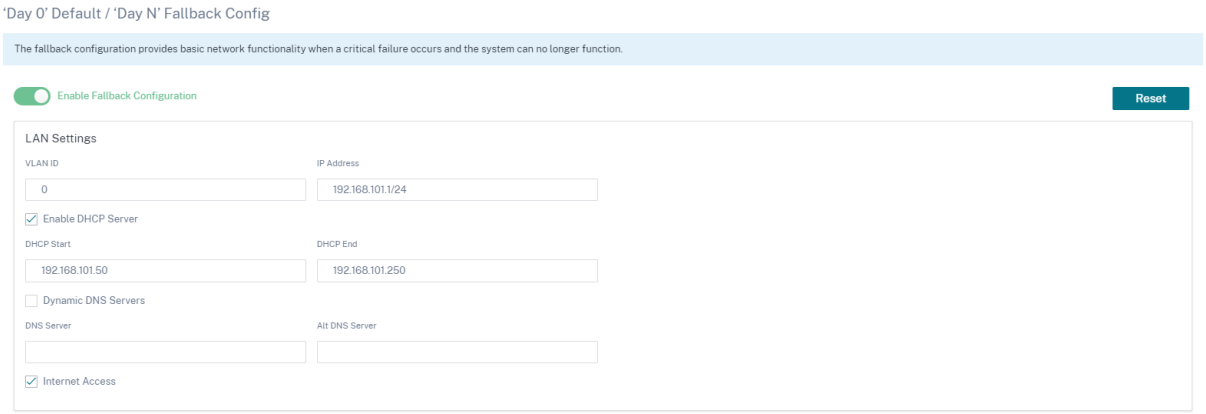
> **Hinweis**
>
> Stellen Sie nach der ersten Appliance-Bereitstellung sicher, dass die Fallback-Konfiguration für die Zero-Touch-Bereitstellungsdienstkonnektivität aktiviert ist.

Wenn die Fallback-Konfiguration deaktiviert ist, können Sie sie über den Citrix SD-WAN Orchestrator Service auf Standortebene aktivieren, indem Sie zu **Konfiguration** > **Appliance-Einstellungen** > **Fallback** navigieren und auf **Fallback-Konfiguration aktivieren** klicken.



Um die Fallback-Konfiguration an Ihr LAN-Netzwerk anzupassen, bearbeiten Sie die Werte für die folgenden LAN-Einstellungen entsprechend Ihren Netzwerkanforderungen. Dies ist die Mindestkonfiguration, die erforderlich ist, um eine Verbindung mit dem Zero-Touch-Bereitstellungsdienst herzustellen.

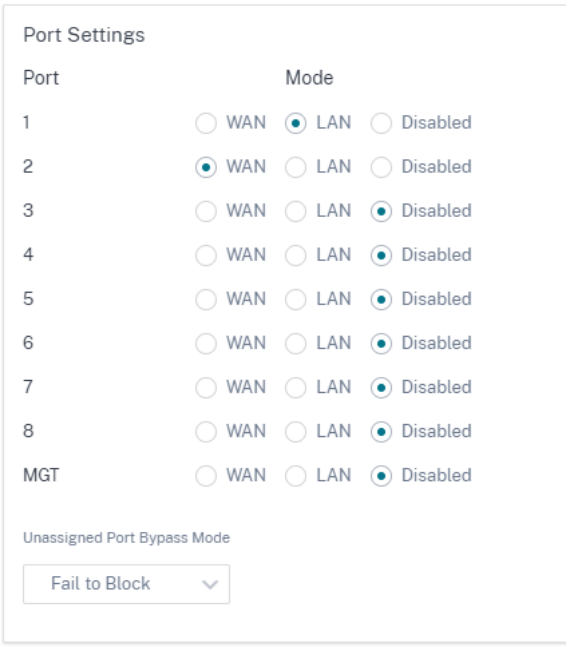
- **VLAN-ID**: Die VLAN-ID, zu der der LAN-Port gruppiert werden muss.
- **IP-Adresse**: Die dem LAN-Port zugewiesene virtuelle IP-Adresse.
- **DHCP-Server aktivieren**: Aktiviert den LAN-Port als DHCP-Server. Der DHCP-Server weist dem WAN-Port dynamische IP-Adressen zu.
- **DHCP-Start und DHCP-Ende**: Der IP-Adressbereich, den DHCP verwendet, um dem WAN-Port dynamisch eine IP zuzuweisen.
- **Dynamischer DNS-Server**: Aktiviert den LAN-Port als Domänennamenserver.
- **DNS-Server**: Die IP-Adresse des primären DNS-Servers.
- **Alt DNS Server**: Die IP-Adresse des sekundären DNS-Servers.
- **Internetzugang**: Erlaubt allen LAN-Clients den Internetzugang ohne weitere Filterung.



Konfigurieren Sie den Modus für jeden Port. Der Port kann ein LAN-Port oder ein WAN-Port sein oder deaktiviert werden. Die angezeigten Ports hängen vom Appliance-Modell ab. Stellen Sie außerdem den Port-Bypass-Modus auf **Fail-to-Blockierung** oder **Fail-to-Wire**ein.

Die folgende Tabelle enthält die Details der vordefinierten WAN- und LAN-Ports für die Fallbackkonfiguration auf verschiedenen Plattformen:

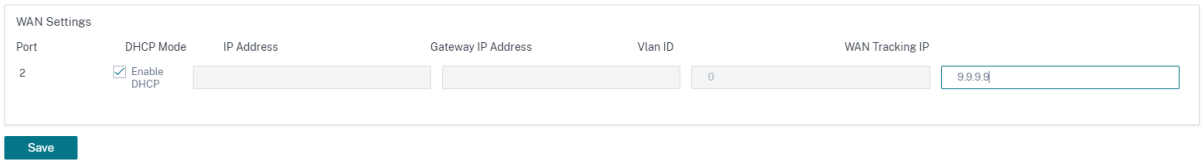
Plattform	WAN-Ports	LAN-Ports
110	1/2	1/1
110-LTE	1/2, LTE-1	1/1
210	1/4, 1/5	1/3
210-LTE	1/4, 1/5, LTE-1	1/3
VPX	2	1
410	1/4, 1/5, 1/6	1/3 (FTB)
1100	1/4, 1/5, 1/6	1/3 (FTB)



Die WAN-Ports können mithilfe des DHCP-Clients als unabhängige WAN-Links konfiguriert werden und den Quad9-DNS-Dienst überwachen, um die WAN-Konnektivität zu ermitteln. Sie können WAN-IPs/Statische IPs für die WAN-Ports ohne DHCP konfigurieren, um das In-Band-Management für die anfängliche Provisioning zu verwenden.

> **Hinweis**
>
> Sie können die Ethernet-Ports nur mit den statischen IPs konfigurieren. Die statischen IPs sind nicht mit LTE-1- und LTE-E1-Ports konfigurierbar. Obwohl Sie den LTE-1 und LTE-E1-Port als WAN hinzufügen können, bleiben die Konfigurationsfelder nicht editierbar.

Wenn Sie einen WAN-Port hinzufügen, wird dieser im Abschnitt **WAN-Einstellungen (Port: 2)** hinzugefügt, wobei das Kontrollkästchen **DHCP aktivieren** standardmäßig aktiviert ist. Wenn das Kontrollkästchen **DHCP-Modus** aktiviert ist, sind die Textfelder **IP-Adresse, Gateway-IP-Adresse**und**VLAN-ID**ausgegraut.**Deaktivieren Sie das Kontrollkästchen DHCP** aktivieren, wenn Sie statische IP konfigurieren möchten.



Standardmäßig wird das Feld **WAN-Tracking-IP-Adresse** automatisch mit 9.9.9.9 gefüllt. Sie können die Adresse nach Bedarf ändern.

> **Hinweis**
>
> Wenn Sie das Kontrollkästchen **Dynamische DNS-Server** aktivieren, stellen Sie sicher, dass mindestens ein WAN-Port mit ausgewähltem **DHCP-Modus** hinzugefügt/konfiguriert wird.

Um die Fallback-Konfiguration jederzeit auf die Standardkonfiguration zurückzusetzen, klicken Sie auf **Zurücksetzen**.

> **Hinweis**
>
> Es wird empfohlen, die Fallback-Konfiguration auf allen Appliances zu aktivieren, die über den mit dem LAN-Subnetz verbundenen In-Band-/Management-Port mit Orchestrator verbunden sind. Stellen Sie sicher, dass die Standardausfallkonfiguration gemäß den Anforderungen Ihres Netzwerksubnetzes eingerichtet ist.

Port-Failover

Der Citrix SD-WAN Orchestrator Service ermöglicht auch ein nahtloses Failover des Verwaltungsverkehrs an den Management-Port, wenn der Datenport ausfällt und umgekehrt. Wenn eine Appliance sowohl über die Verwaltungs- als auch über die In-Band-Ports eine Verbindung zum Internet herstellen kann, wird der Verwaltungsport für die Zero-Touch-Bereitstellung ausgewählt.

Wenn beim Neustart der Appliance das Internet über den In-Band-Port und nicht über den Management-Port verfügbar ist, wird die Appliance sofort mit dem Citrix SD-WAN Orchestrator Service verbunden.

Sobald die Verbindung hergestellt ist, sendet ein auf der Appliance ausgeführter Dienstagent die Heartbeat-Informationen alle 10 Sekunden an den Citrix SD-WAN Orchestrator Service. Wenn der Citrix SD-WAN Orchestrator Service den Heartbeat 5 Minuten lang nicht empfängt, wird das In-Band-Port-Failover aktiviert. Der Citrix SD-WAN Orchestrator Service meldet die Appliance während dieses Zeitraums als offline.

Wenn beim Neustart der Appliance das Internet sowohl über den Verwaltungs- als auch über den In-Band-Port nicht verfügbar ist und die Internetverbindung wiederhergestellt ist, benötigt der Service-Agent etwa 5 Minuten, um neu zu starten und eine Verbindung herzustellen.

Stellen Sie sicher, dass die Option **Route zum Internet von Link beibehalten, auch wenn alle verknüpften Pfade ausgefallen sind**, auf Netzwerkebene aktiviert ist: **Konfiguration** > **Bereitstellungsdienste** > **Internet**. Sicherstellen, dass die Konnektivität zum Citrix SD-WAN Orchestrator Service auch dann aufrechterhalten wird, wenn der virtuelle Pfad ausgefallen ist.

Konfigurierbares Management oder Data-Port

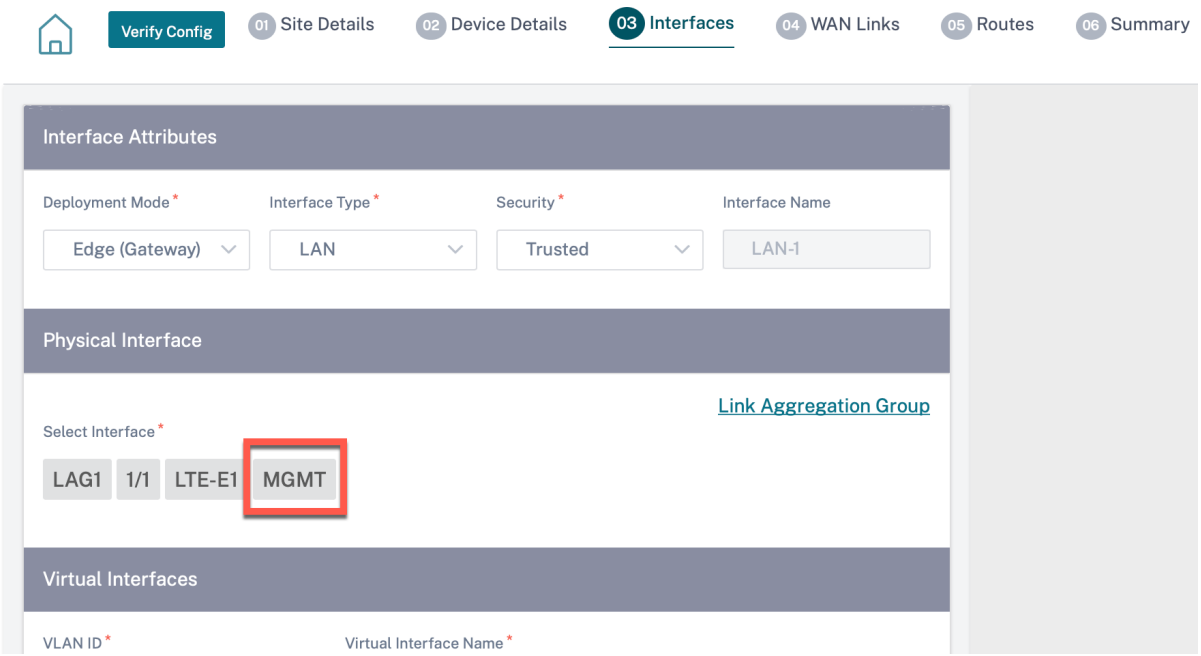
Durch die In-Band-Verwaltung können die Datenports sowohl Daten- als auch Verwaltungsdatenverkehr übertragen, wodurch ein dedizierter Management-Port überflüssig wird. Es lässt den Management-Port ungenutzt auf den Low-End-Appliances, die bereits eine geringe Portdichte aufweisen. Mit Citrix SD-WAN können Sie den Verwaltungsport so konfigurieren, dass er entweder als Datenport oder als Verwaltungsport verwendet wird.

> **Hinweis**
>
> Sie können den Verwaltungsport nur auf den folgenden Plattformen in Datenport konvertieren.
>
> - Citrix SD-WAN 110 SE/LTE
> - Citrix SD-WAN 210 SE/LTE

Verwenden Sie beim Konfigurieren einer Site den Management-Port in Ihrer Konfiguration. Nachdem die Konfiguration aktiviert wurde, wird der Management-Port in einen Datenport konvertiert.

> **Hinweis**
>
> Sie können einen Verwaltungsport nur konfigurieren, wenn die In-Band-Verwaltung auf anderen vertrauenswürdigen Schnittstellen der Appliance aktiviert ist.

Um eine Verwaltungsschnittstelle zu konfigurieren, navigieren Sie auf Standortebene zu **Konfiguration** > **Standortkonfiguration** > **Schnittstellen**, und wählen Sie die MGMT-Schnittstelle aus. Weitere Informationen zum Konfigurieren von Schnittstellengruppen finden Sie unter Schnittstellen.



Um den Verwaltungsport neu zu konfigurieren, um Verwaltungsfunktionen auszuführen, entfernen Sie die Konfiguration. Erstellen Sie eine Konfiguration, ohne den Management-Port zu verwenden, und aktivieren Sie sie.

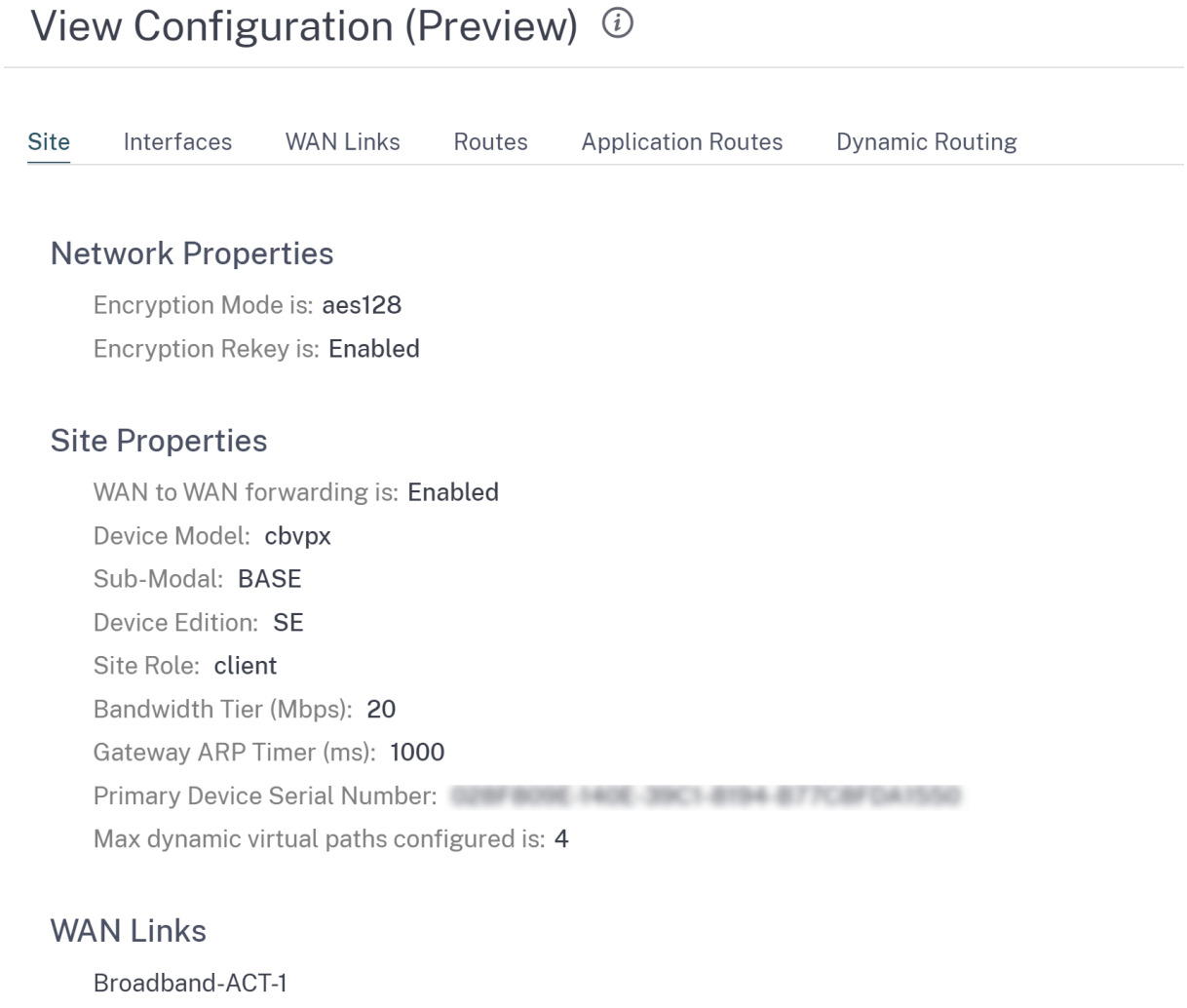
Konfiguration anzeigen (Vorschau)

October 21, 2022

Die Seite **Konfiguration anzeigen** enthält eine konsolidierte Zusammenfassung der Konfigurationseinstellungen einer Site. Um die Konfigurationen anzuzeigen, navigieren Sie auf Standortebene zu **Konfiguration** > **Konfiguration anzeigen**. Weitere Informationen zur Sitekonfiguration finden Sie unter Sitekonfiguration.

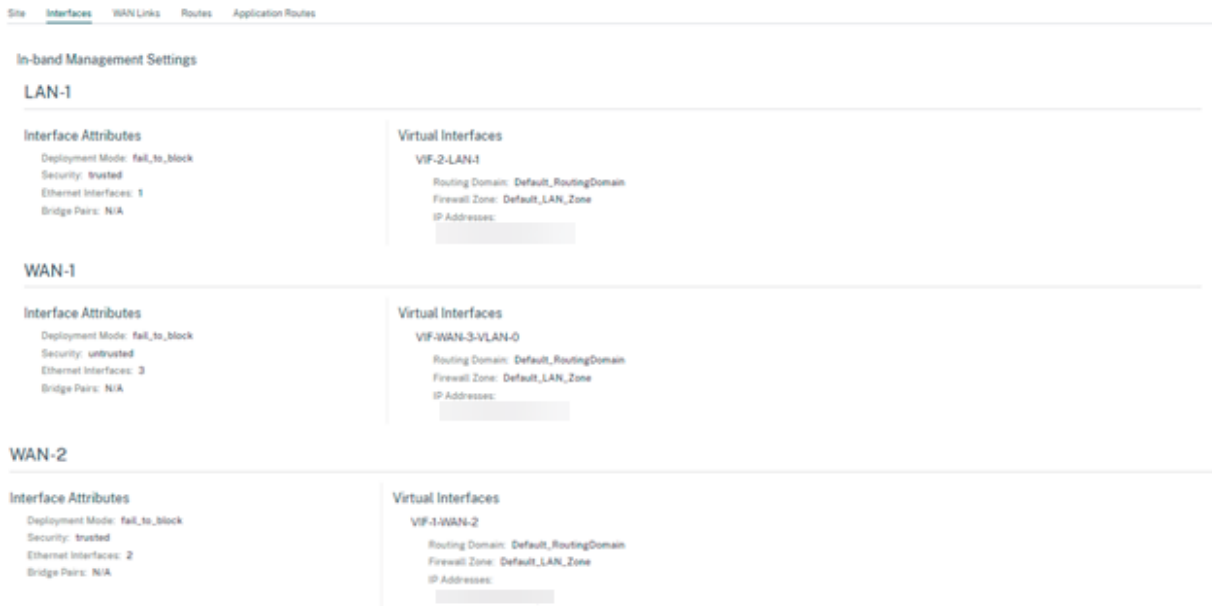
Sites

Auf der Seite **Sites** wird eine Zusammenfassung der Site-Details angezeigt. Die Site-Zusammenfassung enthält Netzwerkeigenschaften, Standorteigenschaften und WAN-Link-Status. Um die Details der Site-Konfiguration anzuzeigen, navigieren Sie zu **Konfiguration** > **Konfiguration anzeigen** > **Site**.



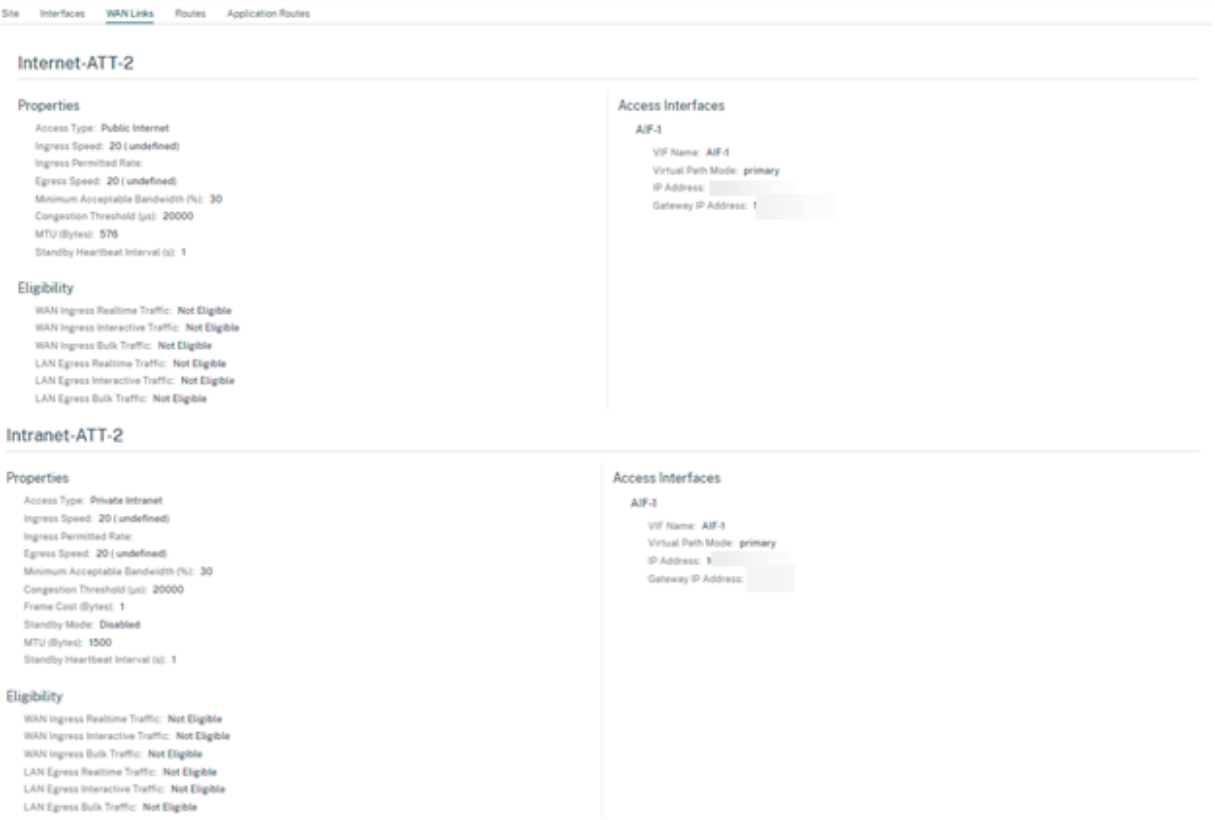
Schnittstellen

Auf der Seite **Schnittstellen** wird eine Zusammenfassung der konfigurierten Schnittstellen angezeigt. Um die Konfigurationsdetails der virtuellen Schnittstellen anzuzeigen, navigieren Sie zu **Konfiguration** > **Konfiguration anzeigen** > **Schnittstellen**.



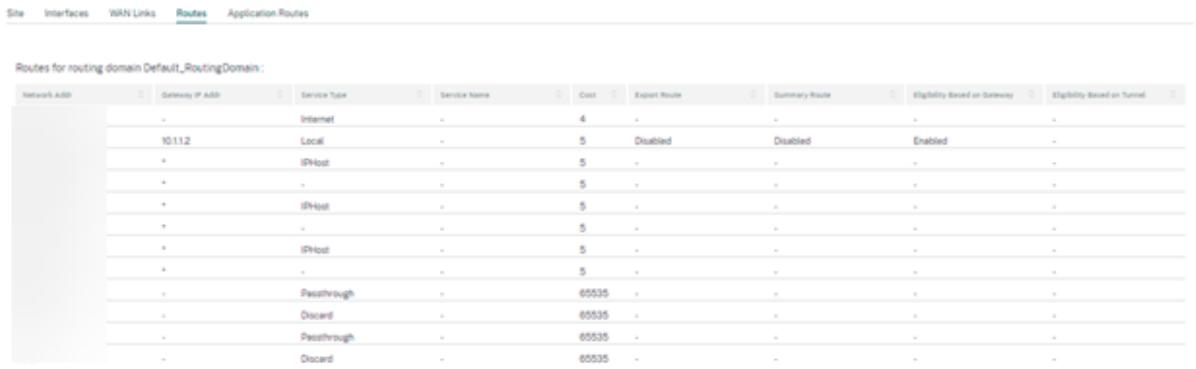
WAN-Links

Um die Konfigurationsdetails der konfigurierten WAN-Links anzuzeigen, navigieren Sie zu **Konfiguration** > **Konfiguration anzeigen** > **WAN-Links**.



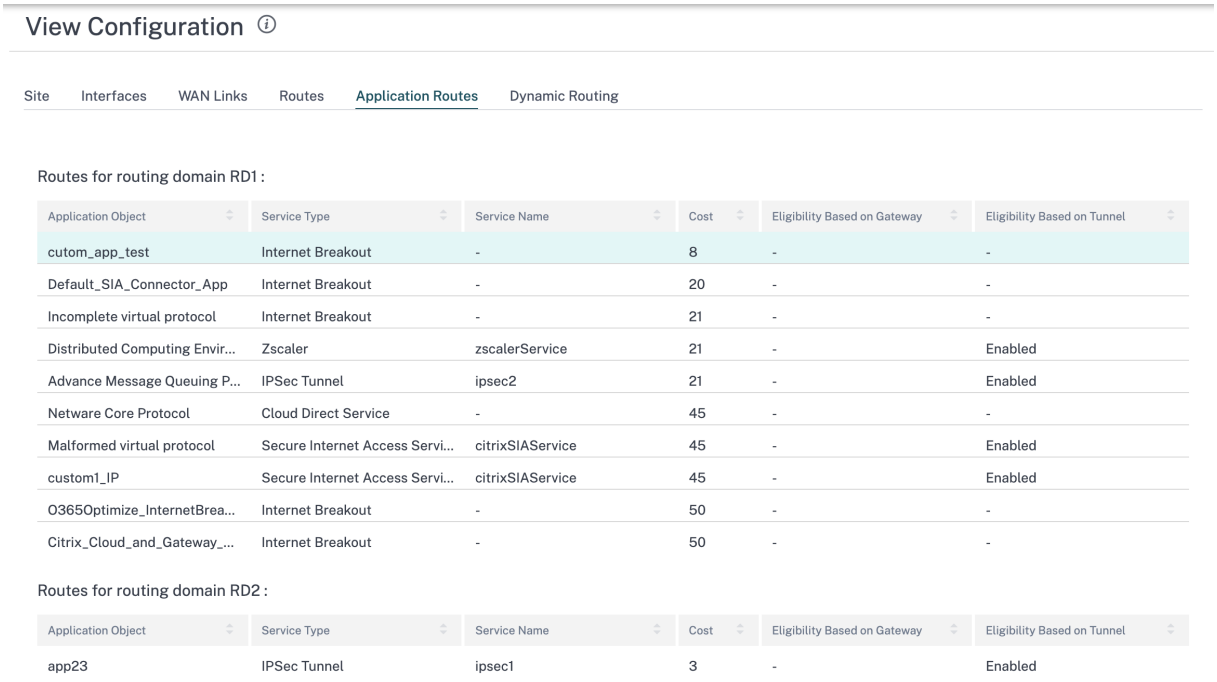
Routen

Um die Routeninformationen der erstellten IP-Routen anzuzeigen, navigieren Sie zu **Konfiguration** > **Konfiguration anzeigen** > **Routen**.



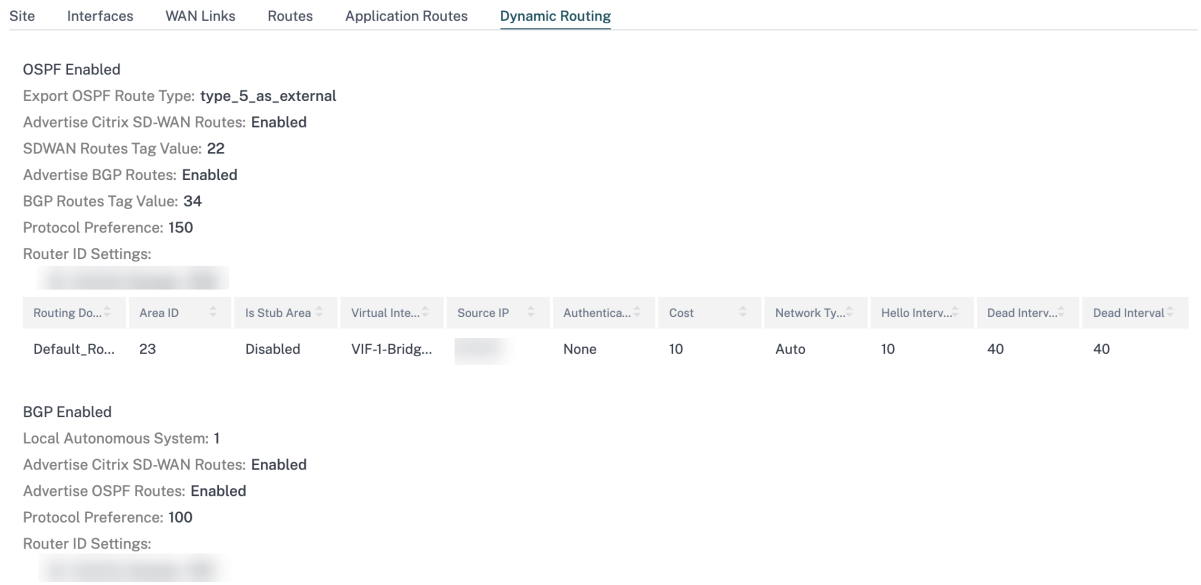
Anwendungs-Routen

Um eine Zusammenfassung der spezifischen Anwendungsrouten anzuzeigen, navigieren Sie zu **Konfiguration** > **Konfiguration anzeigen** > **Anwendungsrouten**.



Dynamisches Routing

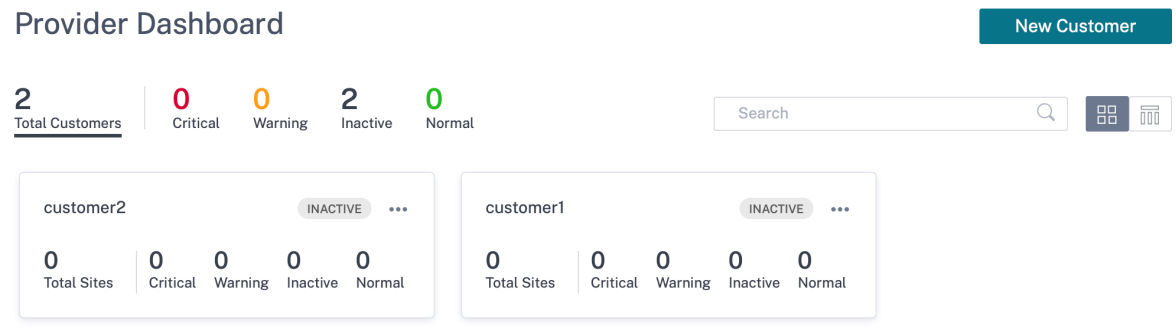
Um eine Zusammenfassung der OSPF-, BGP-, Importfilter- und Exportfilterkonfigurationen anzuzeigen, navigieren Sie zu **Konfiguration > Konfigurationanzeigen**>**Dynamisches Routing**.



Anbieterdashboard

November 16, 2020

Wenn Sie sich als Citrix Partner anmelden, wird das **Provider Dashboard** angezeigt. Es bietet eine Vogelperspektive aller SD-WAN-Kunden, die von einem Dienstleister verwaltet werden.



Ein farbcodierter Integritäts-Snapshot des SD-WAN-Netzwerks jedes Kunden wird bereitgestellt, mit einer Bereitstellung, mit der Sie einen Drilldown für kundenspezifische Details anzeigen können. Das Dashboard ist sowohl in der **Kachelansicht** als auch in der **Listenansicht**.

Die für das Kundennetzwerk verwendeten Farbcodierungskriterien sind:

- Kritisch (Rot): Eine oder mehrere Standorte sind ausgefallen
- Warnung (Orange): Es sind keine Sites ausgefallen, aber es gibt eine oder mehrere kritische Warnungen.
- Normal (Grün): Keine Sites sind ausgefallen und es gibt keine kritischen Warnungen.
- Inaktiv (Grau): Das Netzwerk wird konfiguriert, wurde aber noch nicht bereitgestellt.

Die Kriterien für die Farbcodierung ermöglichen es Administratoren, sich auf die Kunden zu konzentrieren, die ihre Aufmerksamkeit benötigen.

Kunden-/Netzwerk-Dashboard

July 17, 2023

Das Netzwerk-Dashboard bietet eine Vogelperspektive auf das SD-WAN-Netzwerk eines Unternehmens in Bezug auf Zustand und Nutzung an allen Standorten. Das Dashboard erfasst eine Zusammenfassung der netzwerkweiten Warnungen, die Verfügbarkeit der Overlay- und Underlay-Pfade, hebt Nutzungstrends hervor und bietet eine globale Ansicht des Netzwerks.

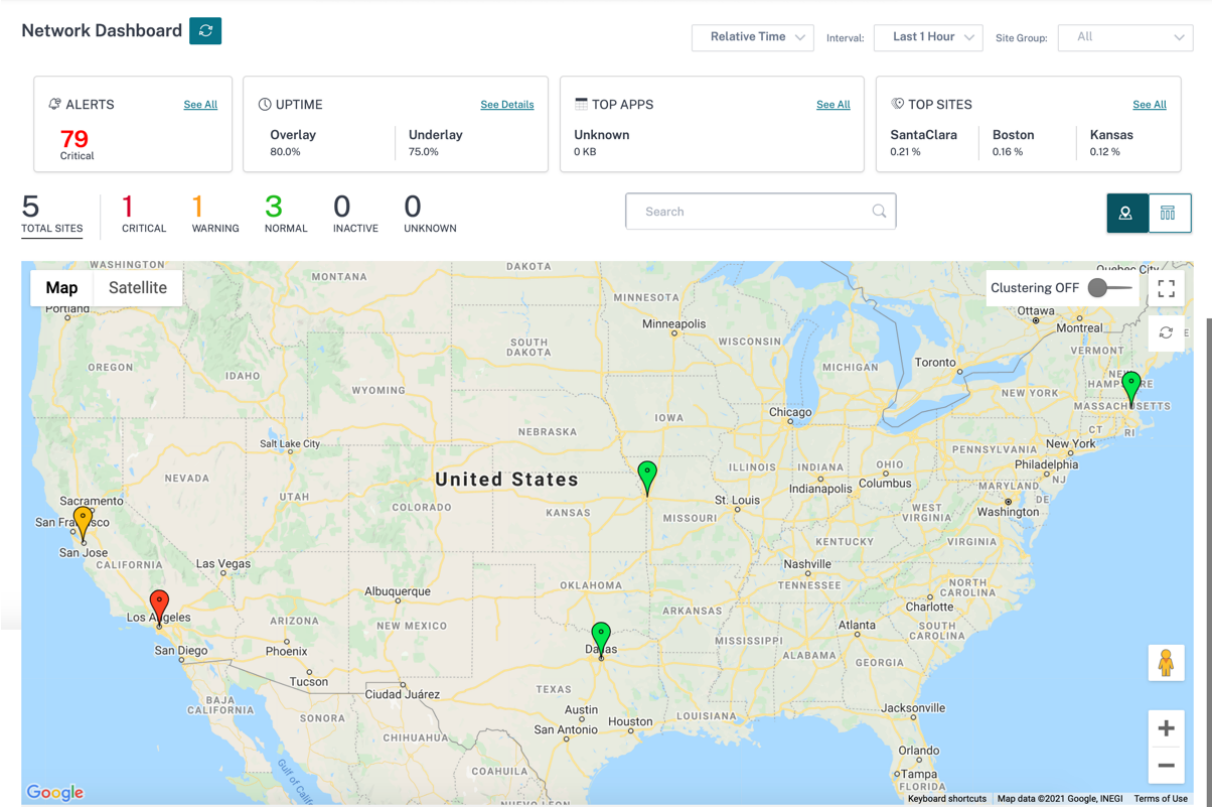
Das Dashboard fasst die folgenden Aspekte eines Netzwerks zusammen, mit einer Bereitstellung für weitere Details.

- **Kritische Warnungen**: Laufende Zählung der kritischen Zustandswarnungen, falls vorhanden, die im Netzwerk angezeigt werden.
- **Betriebszeit**: Side-by-Side-Vergleich der durchschnittlichen Betriebszeit des virtuellen SD-WAN-Overlay-Netzwerks mit dem physischen Underlay-Netzwerk
- **Nutzungstrends**: Top-Apps - basierend auf dem Verkehrsaufkommen und Top-Sites - basierend auf der Kapazitätsauslastung.
- **Netzwerkansicht**: Eine visuelle Darstellung aller Standorte in einem Netzwerk, die sowohl in der Kartenansicht als auch in der Listenansicht verfügbar ist.

Das Dashboard listet die Gesamtzahl der Standorte im Netzwerk auf und trennt die Standorte anhand ihres Konnektivitätsstatus. Wählen Sie die nummerierten Links aus, um die Websites basierend auf den folgenden Statuskategorien anzuzeigen:

- **Kritisch** —Standorte, bei denen alle zugehörigen virtuellen Pfade ausgefallen sind.
- **Warnung** —Websites, bei denen mindestens ein virtueller Pfad ausgefallen ist.
- **Normal** - Alle virtuellen Pfade und zugehörigen Mitgliedspfade der Site sind aktiv.
- **Inaktiv** —Standorte, die sich im Status „Nicht bereitgestellt“und „inaktiv“befinden
- **Unbekannt** —Der Status der Website ist unbekannt.

Durch Klicken auf den Status werden die Websites anhand ihres Status gefiltert und die Details angezeigt. Sie können auch die **Suchleiste** verwenden, um die Details einer Site basierend auf dem Site-Namen, der Rolle, der Overlay-Konnektivität, dem Modell, der Bandbreitenstufe und den Seriennummernparametern anzuzeigen.



Die Karte bietet eine Echtzeitansicht des globalen Netzwerks mit allen Standorten der Organisation, die auf einer Weltkarte dargestellt sind, basierend auf ihren Standorten. Die Farbe jedes Standorts spiegelt seinen aktuellen Zustand wider.

Im Folgenden sind die für jede Site verwendeten Farbcodierungskriterien aufgeführt:

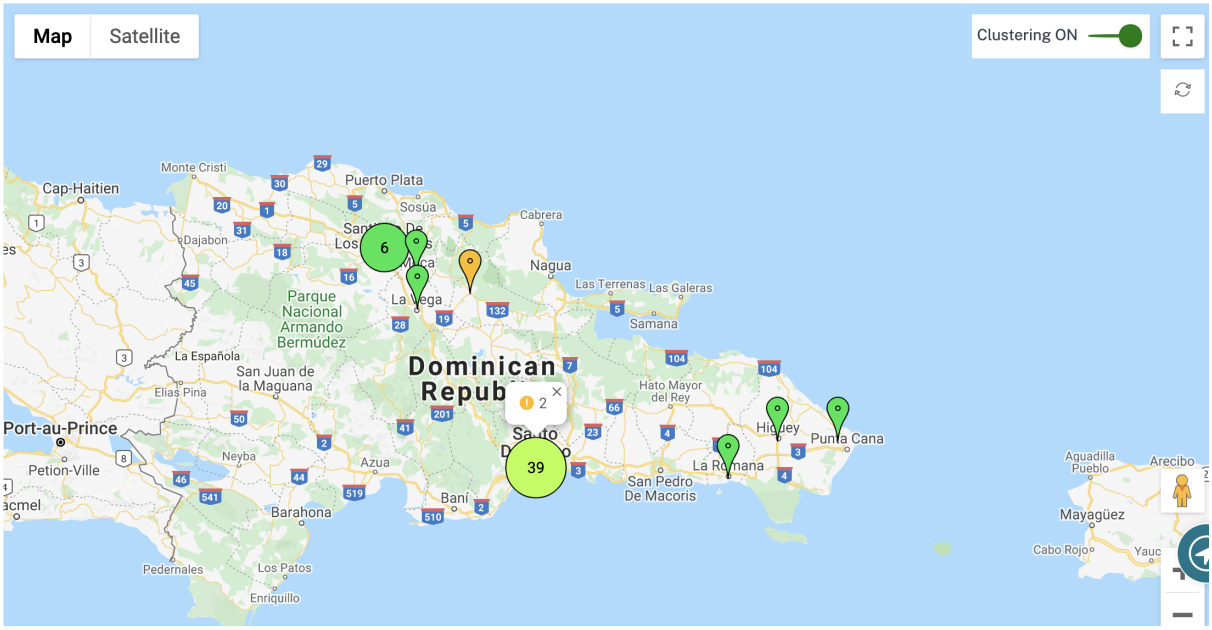
- **Kritisch (rot)**: Mindestens ein virtueller Overlay-Pfad, der einer Site zugeordnet ist, ist DOWN.
- **Warnung (Orange)**: Mindestens ein Unterlagermitgliedspfad ist DOWN, aber alle virtuellen Overlay-Pfade sind UP.
- **Normal (grün)**: Alle virtuellen Overlay-Pfade und die zugehörigen Unterlagenmitgliedspfade sind UP.
- **Inaktiv (grau)**: Die Site befindet sich in der Konfiguration und wurde noch nicht bereitgestellt.

Wenn Sie den Mauszeiger über eine Site bewegen, werden einige der wichtigsten standortspezifischen Details wie die Standortrolle, das Gerätemodell und die Bandbreitenstufe angezeigt. Die mit einer Site verbundenen virtuellen Pfade werden mit geeigneten Farbcodes angezeigt, die ihre Gesundheit widerspiegeln. Die **Listenansicht** bietet dieselben Details für jede Site, zusammengefasst als Einträge in einer Tabelle.

Clustering

Die **Clustering ON-Funktion** überwacht die Konsistenz, den Status und die Integrität verschiedener Standorte eines Clusters oder einer Kombination von Clustern. Der Clustering ON-Dienst bietet eine Echtzeitansicht von Sites, mit deren Hilfe das Failover und der aktuelle Status der Site überwacht werden können.

Diese **Clustering ON-Funktion** wurde eingeführt, um die hohe Dichte von Standorten zu verwalten. Es wird nicht empfohlen, die Option Clustering off zu verwenden, wenn Tausende von Websites vorhanden sind, und dies verringert auch die Leistung.



In der folgenden Tabelle wird der Farbton mit fünf Farben beschrieben, der für Cluster verwendet wird, um den Zustand von Sites darzustellen:

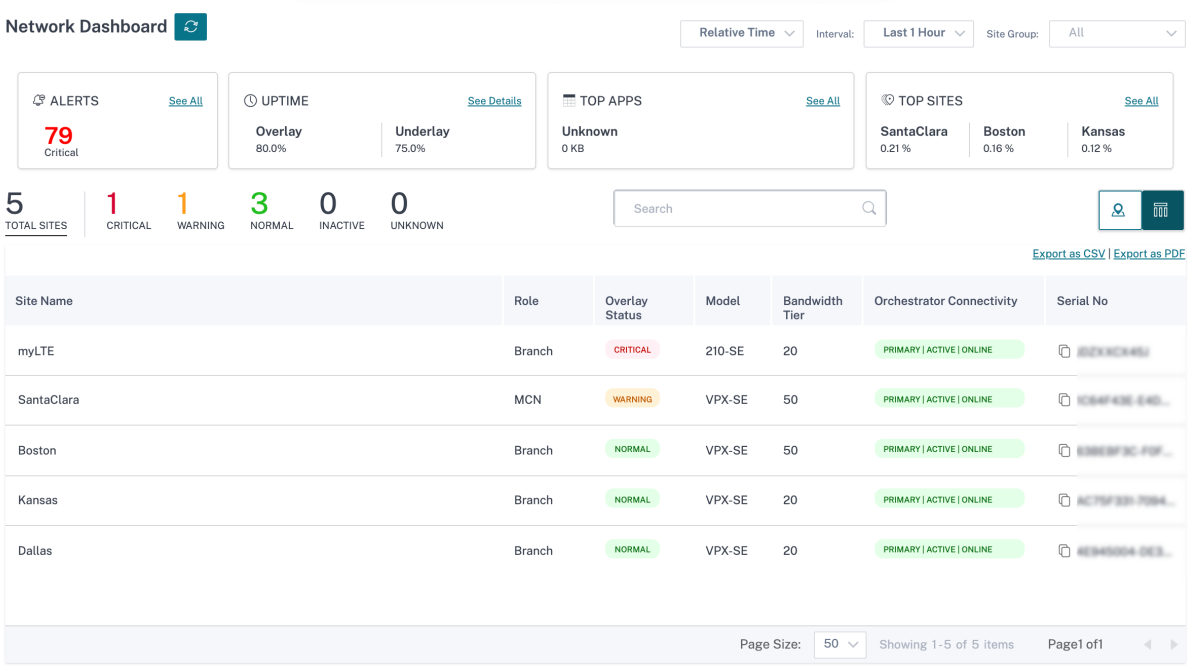
Farb-Legenden	Beschreibung
	Alle Standorte im Cluster sind grün. Das bedeutet, dass jede Site alle virtuellen Pfade und die zugehörigen Mitgliedspfade UP hat.
	Alle Standorte im Cluster sind orange. Das bedeutet, dass jede Site mindestens einen Mitgliedspfad DOWN hat, aber alle virtuellen Pfade UP
	Alle Standorte im Cluster sind rot. Das bedeutet, dass jede Site mindestens einen virtuellen Pfad (DOWN) hat.

Farb-Legenden	Beschreibung
	Der Cluster hat eine Kombination aus grünen und orangefarbenen Standorten
	Der Cluster verfügt über eine Kombination aus roten und nicht-roten Standorten

Sie können das Netzwerkaspekt auch überprüfen, indem Sie den Mauszeiger auf ein beliebiges Cluster bewegen. Die kritischen Warnungen oder Warnmeldungen sind oben im Cluster als Pop-up sichtbar.

Wenn Sie auf den Cluster klicken, zoomt er in diesen Cluster und zeigt andere Cluster an. Sie sehen eine Ansichtsleiste mit der Anzahl der Cluster. Die Pfeiloption hilft Ihnen dabei, einen Schritt zurück zu bringen. Klicken Sie auf die Schaltfläche **Schließen (X)**, um zur ursprünglichen Seite zurückzukehren.

Alternativ können Sie die Netzwerkzusammenfassung in der **Listenansicht anzeigen**.



- Wenn Sie auf eine inaktive Site mit „Unterkonfiguration“klicken, die noch bereitgestellt werden muss, gelangen Sie zum Workflow für die Sitekonfiguration.
- Wenn Sie auf eine aktive Site klicken, die bereits bereitgestellt wurde, gelangen Sie zum **Site-Dashboard**.

> **Hinweis**
>
> Citrix SD-WAN-Overlay-Tunnel werden virtuelle Pfade genannt. Sie hätten in der Regel einen virtuellen Pfadtunnel zwischen jedem Standort und dem Master Control Node (MCN) und bei Bedarf zusätzliche virtuelle Site-Site-Pfade. Virtuelle Pfade werden gebildet, indem die zugrunde liegenden WAN-Links/Pfade miteinander verbunden werden. Jeder virtuelle Pfad umfasst also mehrere Mitgliedspfade.
>
> Dies kann angezeigt werden, wenn ein Benutzer den Mauszeiger über den Begriff virtueller Pfad oder Mitgliedspfad bewegt.

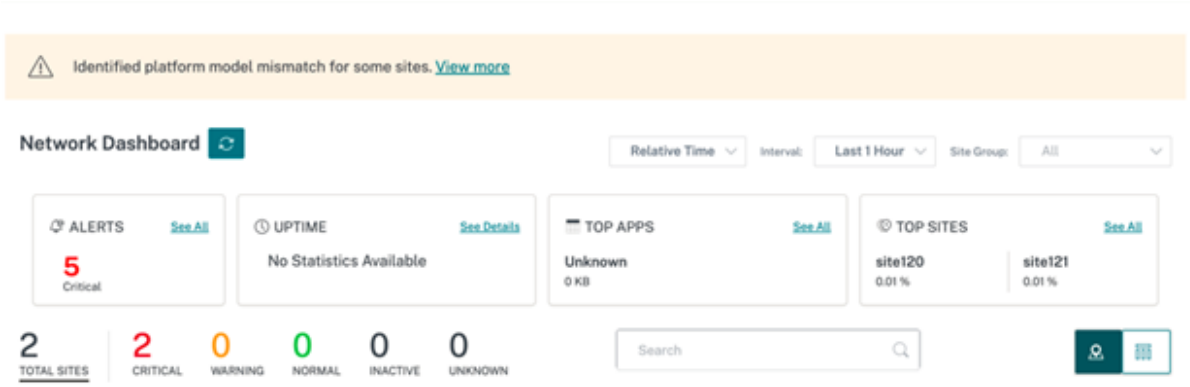
Sie können den **Pegman** auf die Karte ziehen, um die Straßenansicht zu öffnen.

Nichtübereinstimmung des Aufnahmegeräts

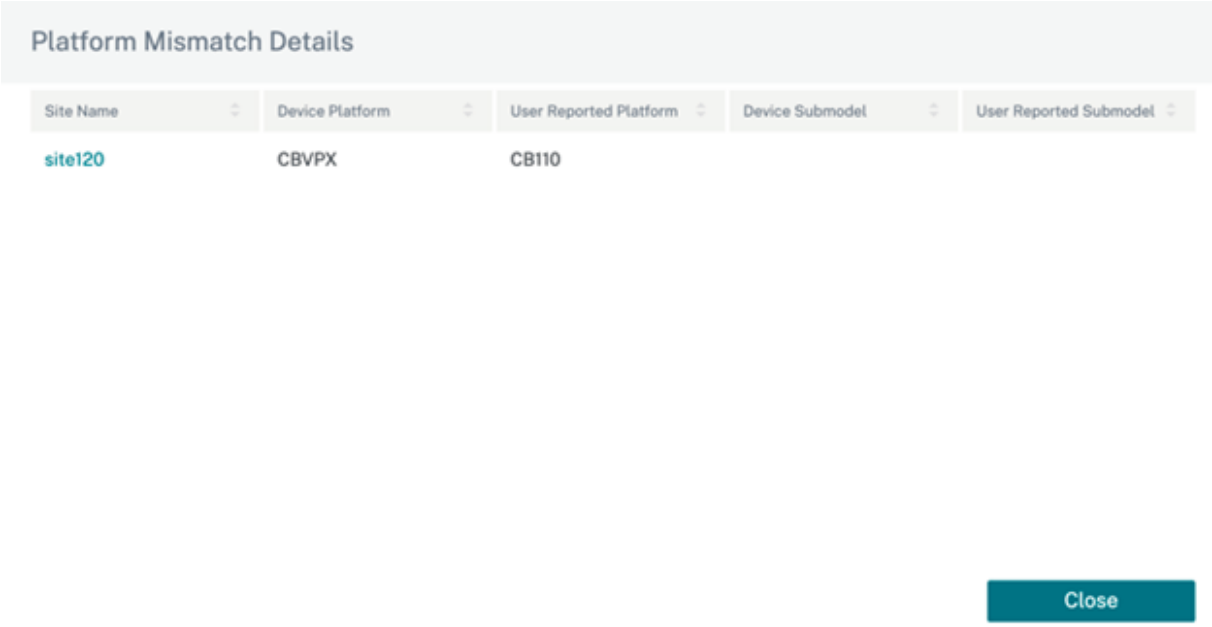
Der Citrix SD-WAN Orchestrator Service meldet eine Nichtübereinstimmung zwischen dem von der Appliance gemeldeten Plattformmodell und dem vom Benutzer gemeldeten Plattformmodell.

Wenn das Plattformmodell und das Submodell, das von einem Benutzer während der Standortkonfiguration bereitgestellt wird, nicht mit dem Plattformmodell und dem Submodell übereinstimmen, das von der Appliance bei der Erstregistrierung beim Citrix SD-WAN Orchestrator Service bereitgestellt wurde, wird im Netzwerk-Dashboard eine Benachrichtigung über die Nichtübereinstimmung angezeigt. Stellen Sie in einem solchen Szenario sicher, dass Sie das von der Appliance gemeldete Plattformmodell konfigurieren.

Klicken Sie auf **Mehr anzeigen**, um eine tabellarische Darstellung der Nichtübereinstimmung des Plattformmodells für jede Site anzuzeigen.



Die **Plattformfehlanpassungsdetails** enthalten Informationen wie den Site-Namen, das von der Appliance gemeldete Plattformmodell und das Submodell sowie das vom Benutzer gemeldete Plattformmodell und Submodell.



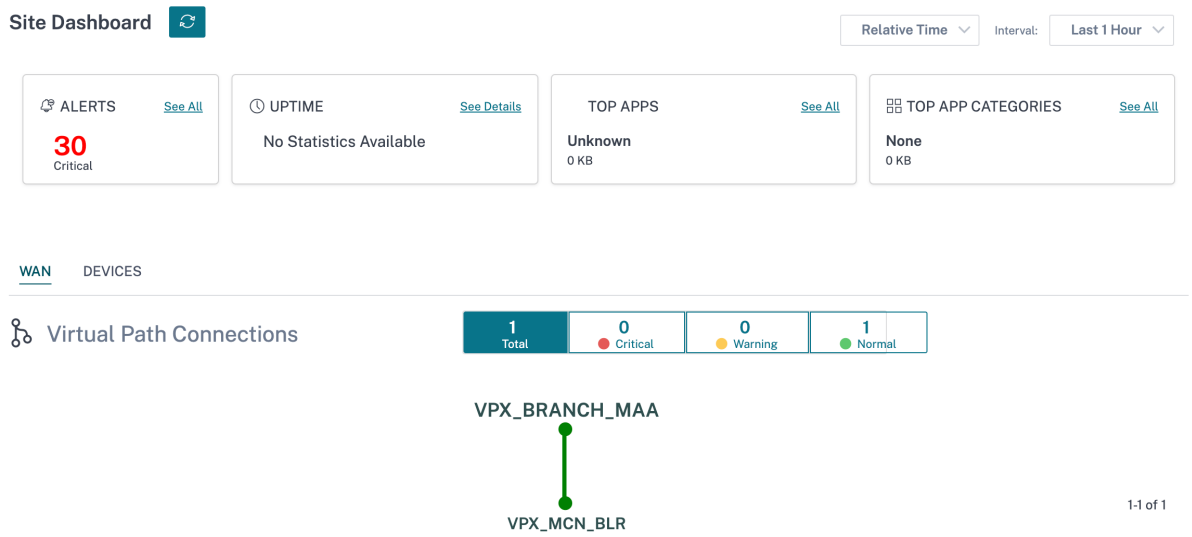
Sitedashboard

October 21, 2022

Das Site-Dashboard bietet einen Überblick über den Zustand und die Nutzungstrends einer Website.

Das Dashboard fasst die folgenden Aspekte einer Site zusammen, mit einer Bestimmung zum Drilldown für weitere Details.

- **Kritische Warnungen**: Laufende Zählung der kritischen Zustandswarnungen, falls vorhanden, die auf der Website angezeigt werden.
- **Betriebszeit**: Side-by-Side-Vergleich der durchschnittlichen Betriebszeit, die von den virtuellen SD-WAN-Overlay-Pfaden angeboten wird, mit den physischen Underlay-Pfaden, die einer Site zugeordnet sind
- **Nutzungstrends**: Mit einer Website verknüpfte Top-Apps und App-Kategorien, basierend auf dem Verkehrsaufkommen
- **Standortdetails**: WAN-Verbindungen und Geräte, die einem Standort zugeordnet sind



> **Tipp**
>
> Klicken Sie auf **Alle** anzeigen oder **Details** anzeigen, um detailliertere Statistiken anzuzeigen.

Alle Overlay-Verbindungen mit virtuellen Pfaden, die einer Site zugeordnet sind, werden mit einer geeigneten Farbcodierung angezeigt, um den Zustand jeder Verbindung widerzuspiegeln.

Sie können eine beliebige virtuelle Pfadverbindung auswählen, um die entsprechenden Integritätsmetriken und Trends zu überprüfen.

Die Farbcodierungskriterien, die für virtuelle Pfadverbindungen verwendet werden, sind:

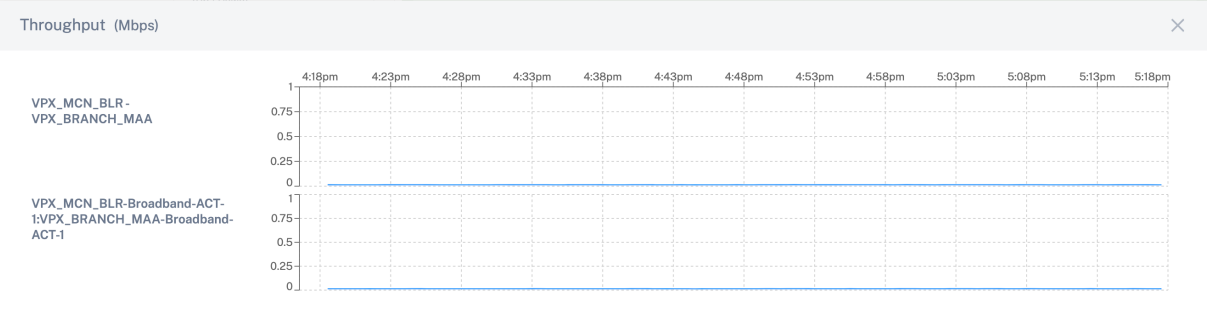
- **Kritisch (rot)**: Virtueller Pfad ist DOWN.
- **Warnung (orange)**: Virtueller Pfad ist UP, aber mindestens ein Mitgliedspfad ist DOWN.
- **Normal (grün)**: Virtueller Pfad und alle Mitgliedspfade sind UP.

Kennzahlen für Gesundheit

Integritätsmetriken und grafische Trends in Bezug auf Verfügbarkeit, Latenz, Verlust, Jitter und Durchsatz werden für die ausgewählte virtuelle Pfadverbindung angezeigt. Diese Statistiken sind in beiden

Richtungen verfügbar: **WAN zu LAN** und **LAN zu WAN**. Alle Metriken können anhand eines gemeinsamen Zeitplans überprüft werden, um den Problembereich bei der Fehlerbehebung schnell einzugrenzen.

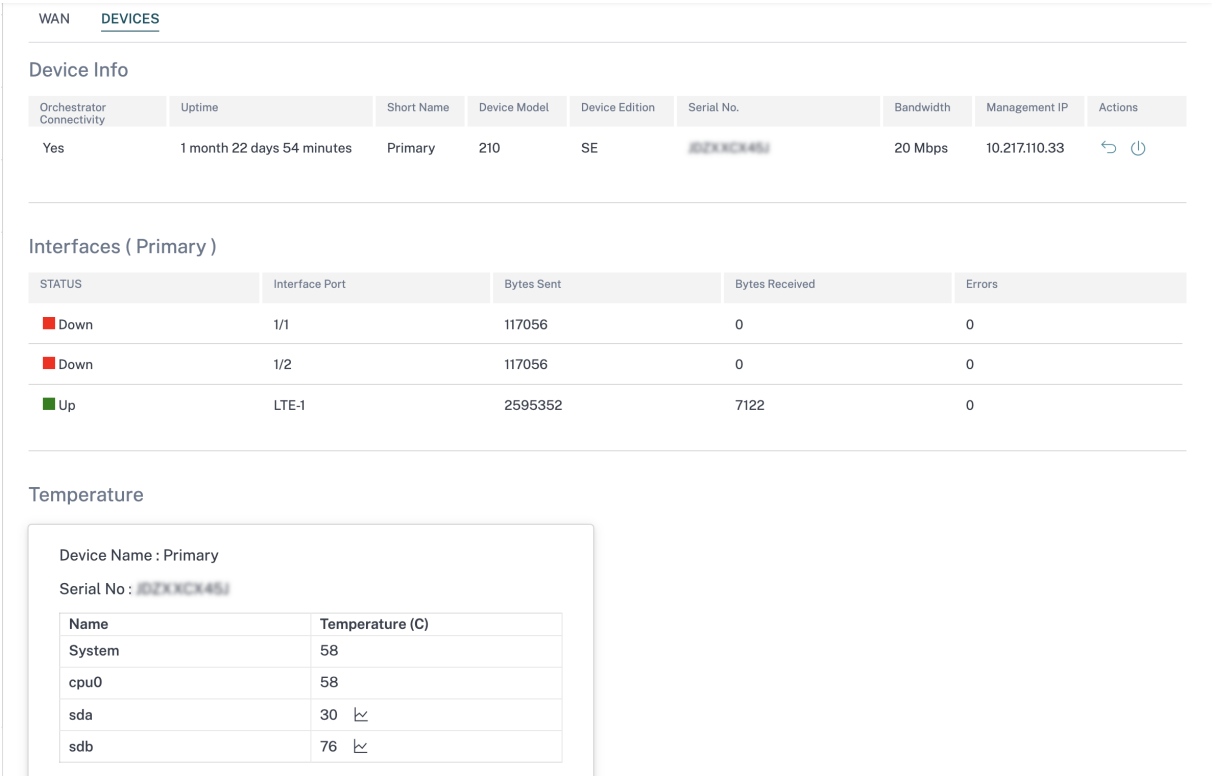
Sie können die einzelnen Integritätsmetriken weiter untersuchen, um eine vergleichende Ansicht des virtuellen Overlay-Pfads und der zugrunde liegenden Mitgliedspfade für dieselbe Metrik zu erhalten. Dies würde bei der Behebung von Overlay-gegen-Underlay-Problemen helfen.



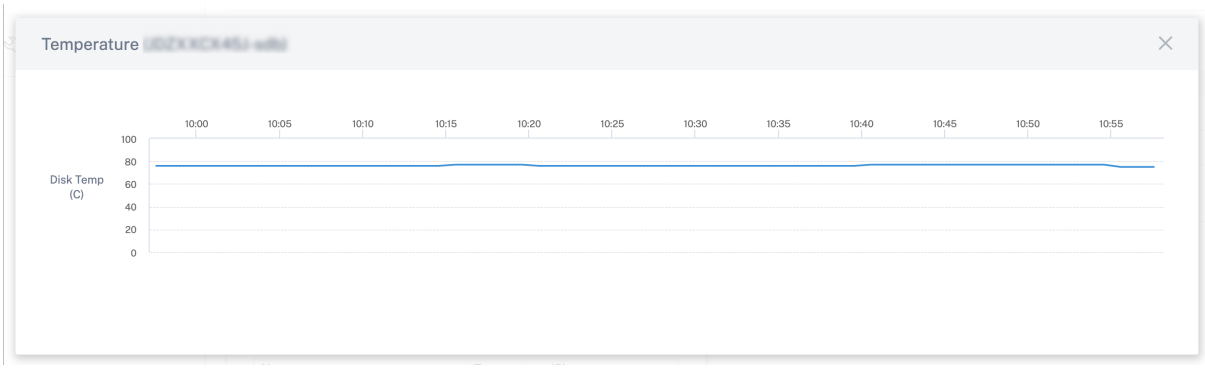
Geräte

Auf der Registerkarte **Geräte** werden Details zu den Geräten, Schnittstellen und der Festplattentemperatur des Standorts angezeigt. Sie können die Appliance auch neu starten, die Appliance-Konfiguration zurücksetzen oder Geräteprotokolle herunterladen.

Im Abschnitt **Temperatur** wird die Temperatur des Systems, der CPU und der Festplatten in Grad Celsius angezeigt.



Sie können auch auf das Diagrammsymbol in der Spalte **Temperatur (C)** klicken und die Informationen in grafischer Form anzeigen.



Problembehandlung - Anbieter

October 21, 2022

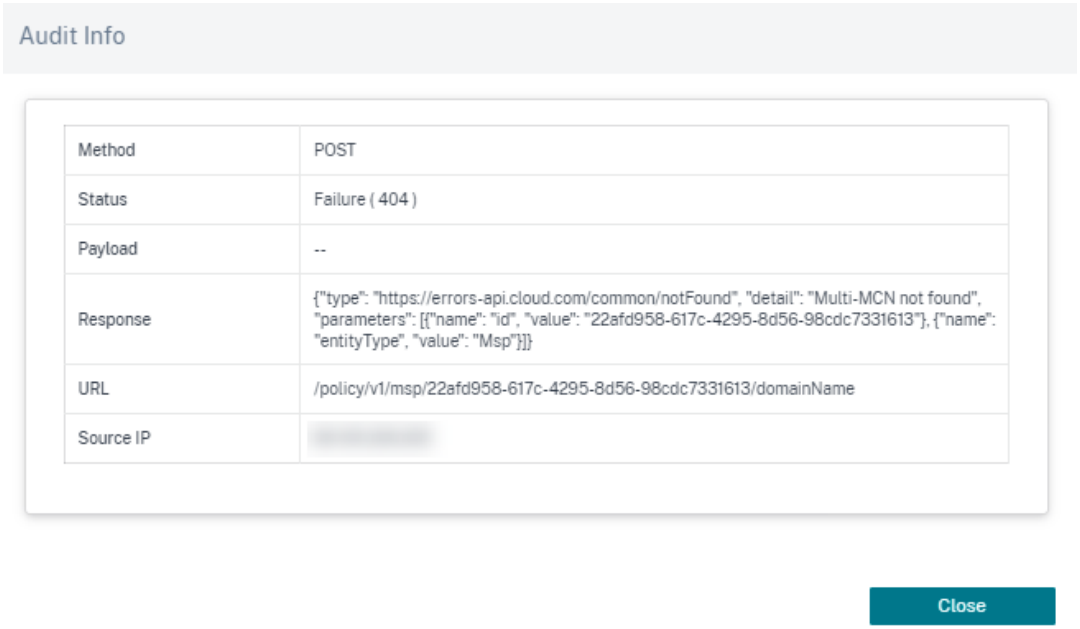
Auf der Seite Anbieterüberwachungsprotokolle werden Protokolle auf Anbieterebene und Geräteprotokolle angezeigt, sodass eine schnelle

Überwachungsprotokolle

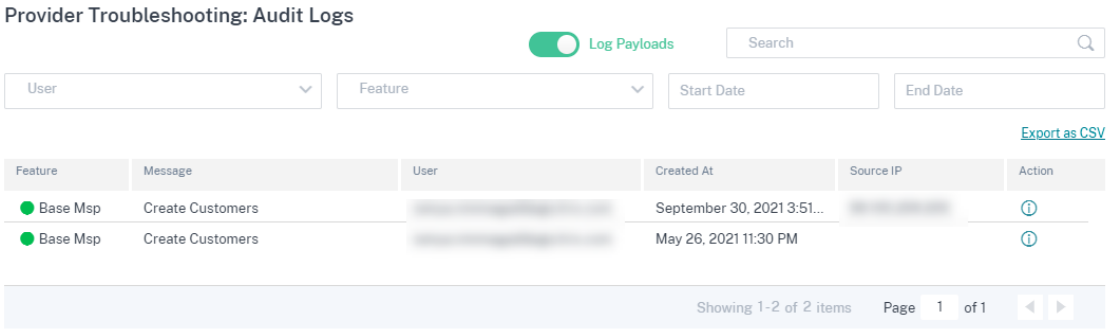
Überwachungsprotokolle erfassen die Aktion, die Zeit und das Ergebnis der von den Anbietern ausgeführten Aktion. Navigieren Sie zu **Fehlerbehebung** > **Überwachungsprotokolle**, um die Seite **Provider-Fehlerbehebung: Audit-**

Auf der Seite Provider Audit-Protokolle werden die folgenden Informationen angezeigt:

- **Suchleiste**: Suchen Sie anhand eines Schlüsselworts nach einer Auditaktivität.
- **Filteroptionen**: Führen Sie eine Auditprotokollsuche durch, indem Sie anhand der folgenden Kriterien filtern:
  - Benutzer
  - Feature
  - Zeitbereich
- **Als CSV exportieren**: Wenn Sie auf diese Option klicken, werden die Einträge des Überwachungsprotokolls in eine CSV-Datei exportiert.
- **Audit-Info**: Wählen Sie das Symbol in der Spalte **Aktion** aus, um zum Abschnitt **Audit-Info** zu navigieren. Dieser Abschnitt enthält die folgenden Informationen:
  - **Methode**: HTTP-Anforderungsmethode der aufgerufenen API.
  - **Status**: Ergebnis der API-Anfrage.
  - **Payload**: Hauptteil der Anfrage, die über die API gesendet wurde.
  - **Antwort**: Fehlerantwort, wenn die API-Anfrage fehlschlägt. Dieses Feld wird nur angezeigt, wenn die API-Anfrage fehlschlägt.
  - **URL**: HTTP-URL der widerrufenen API.
  - **Quell-IP**: Die IP-Adresse des Endpunkts, von dem aus die Funktion konfiguriert wurde. Dieses Feld wird auf der Seite Audit-Logs und der Audit-Info-Seite angezeigt.



- **Payloads protokollieren**: Diese Option ist standardmäßig deaktiviert. Wenn diese Option aktiviert ist, wird der Anforderungstext der API-Nachricht im Abschnitt **Audit-Info** angezeigt. Weitere Informationen zur API finden Sie im API-Handbuch für Citrix SD-WAN Orchestrator.



Problembehandlung - Netzwerk

October 21, 2022

Kunden können Protokolle aller Netzwerk-Appliances anzeigen, was eine schnelle Fehlerbehebung ermöglicht.

Überwachungsprotokolle

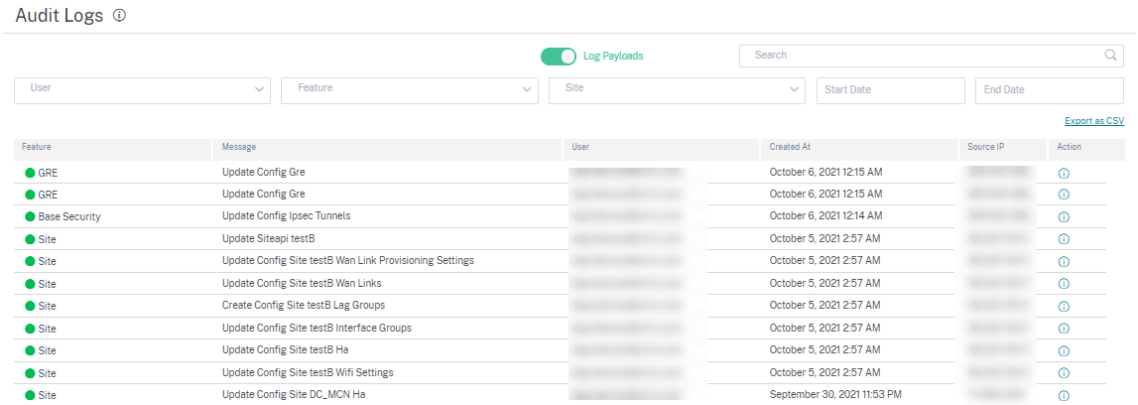
Überwachungsprotokolle erfassen die Aktion, die Zeit und das Ergebnis der von Benutzern in einem Kundennetzwerk ausgeführten Aktion. Navigieren Sie zu **SD-WAN-Fehlerbehebung** > **Überwachungsprotokolle**, um die Seite **Überwachungsprotokolle zur SD-WAN-Fehlerbehebung** anzuzeigen

Auf der Seite Überwachungsprotokolle zur SD-WAN-Fehlerbehebung werden die folgenden Informationen angezeigt:

- **Suchleiste**: Suchen Sie anhand eines Schlüsselworts nach einer Auditaktivität.
- **Filteroptionen**: Führen Sie eine Auditprotokollsuche durch, indem Sie anhand der folgenden Kriterien filtern:
  - Benutzer
  - Feature
  - Site
  - Zeitbereich
- **Als CSV exportieren**: Wenn Sie auf diese Option klicken, werden die Einträge des Überwachungsprotokolls in eine CSV-Datei exportiert.
- **Audit-Info**: Wählen Sie das Symbol in der Spalte **Aktion** aus, um zum Abschnitt **Audit-Info** zu navigieren. Dieser Abschnitt enthält die folgenden Informationen:
  - **Methode**: HTTP-Anforderungsmethode der aufgerufenen API.
  - **Status**: Ergebnis der API-Anfrage. Die folgende Fehlerantwort wird angezeigt, wenn die API-Anfrage fehlschlägt.
  - **Payload**: Hauptteil der Anfrage, die über die API gesendet wurde.
  - **Antwort**: Fehlerantwort, wenn die API-Anfrage fehlschlägt. Dieses Feld wird nur angezeigt, wenn die API-Anfrage fehlschlägt.
  - **URL**: HTTP-URL der widerrufenen API.

- **Quell-IP**: Die IP-Adresse des Endpunkts, von dem aus die Funktion konfiguriert wurde. Dieses Feld wird auf der Seite Audit-Logs und der Audit-Info-Seite angezeigt.
- **Was geändert wurde**: In diesem Abschnitt werden die Protokolle aller Änderungen angezeigt, die über die Benutzeroberfläche an den Funktionen vorgenommen wurden. Aktivieren Sie die Umschaltfläche Payloads protokollieren, um die Änderungen im Abschnitt Audit-Info anzuzeigen.

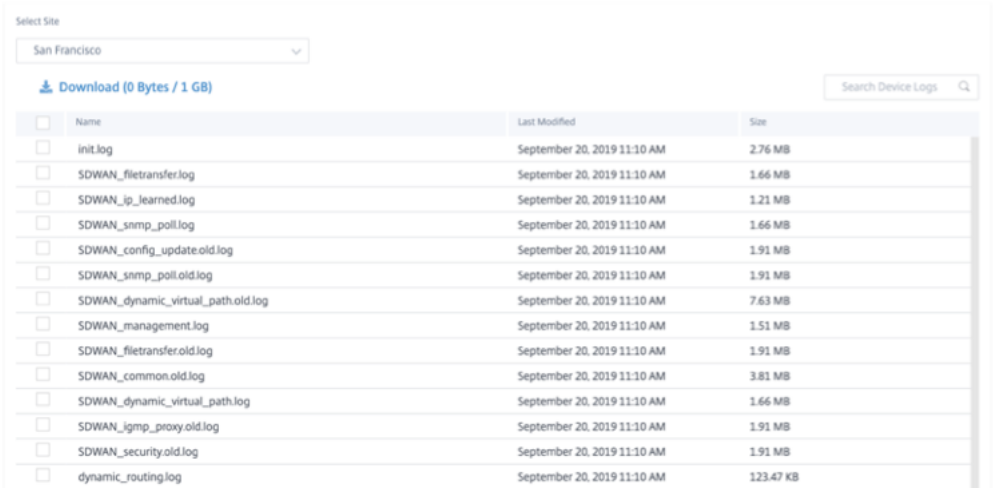
- **Payloads protokollieren**: Diese Option ist standardmäßig deaktiviert. Wenn diese Option aktiviert ist, wird der Anforderungstext der API-Nachricht im Abschnitt **Audit-Info** angezeigt. Weitere Informationen zur API finden Sie im API-Handbuch für Citrix SD-WAN Orchestrator.



Geräte-Logs

Kunden können die für Websites spezifischen Geräteprotokolle anzeigen.

Sie können bestimmte Geräteprotokolle auswählen, herunterladen und bei Bedarf für Site-Administratoren freigeben.

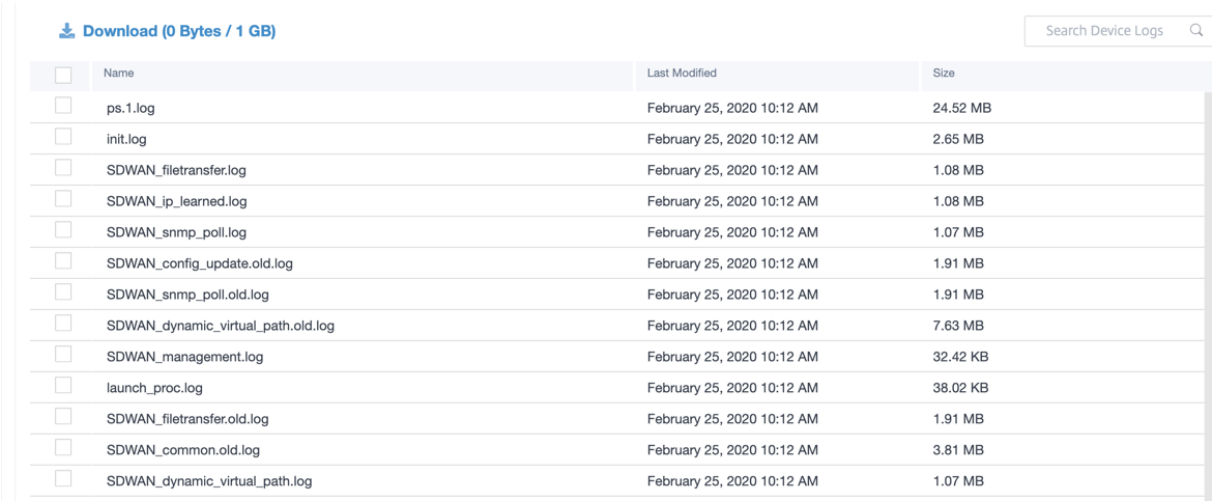


Fehlerbehebung

October 21, 2022

Geräte-Logs

Protokolle sind nützlich, um Probleme zu beheben. Der Site-Administrator kann eine Liste aller Protokolle anzeigen, die auf allen Geräten der Site erfasst werden. Sie können auch Protokolle zur weiteren Überprüfung herunterladen.

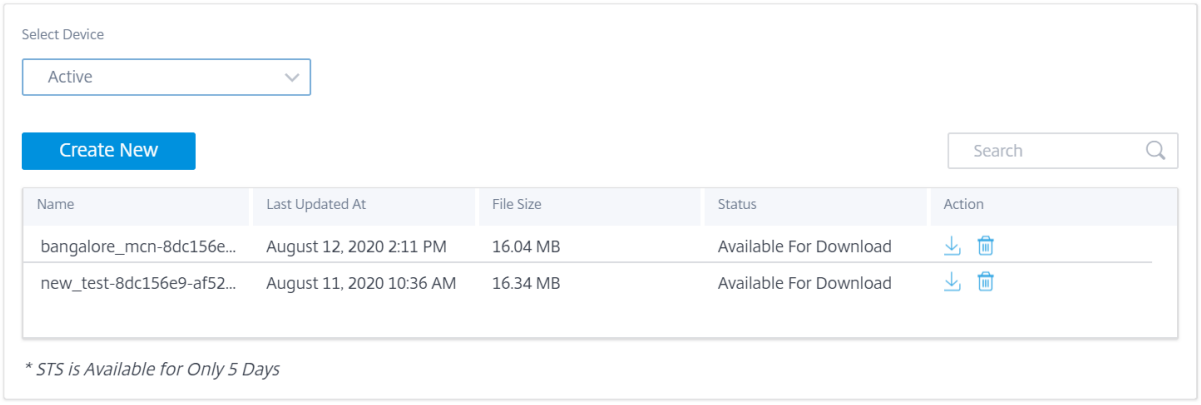


Tech Support Bundle anzeigen

Das Show Tech Support (STS) Bundle enthält wichtige Echtzeit-Systeminformationen wie Zugriffsprotokolle, Diagnoseprotokolle, Firewall-Protokolle. Das STS-Bundle wird verwendet, um Probleme in den SD-WAN-Appliances zu beheben. Sie können das STS-Paket erstellen, herunterladen und es mit Citrix Support Representatives teilen.

Wenn ein Standort im HA-Bereitstellungsmodus konfiguriert ist, können Sie die aktive Appliance oder Standby-Appliance auswählen, für die das STS-Paket erstellt oder heruntergeladen werden soll.

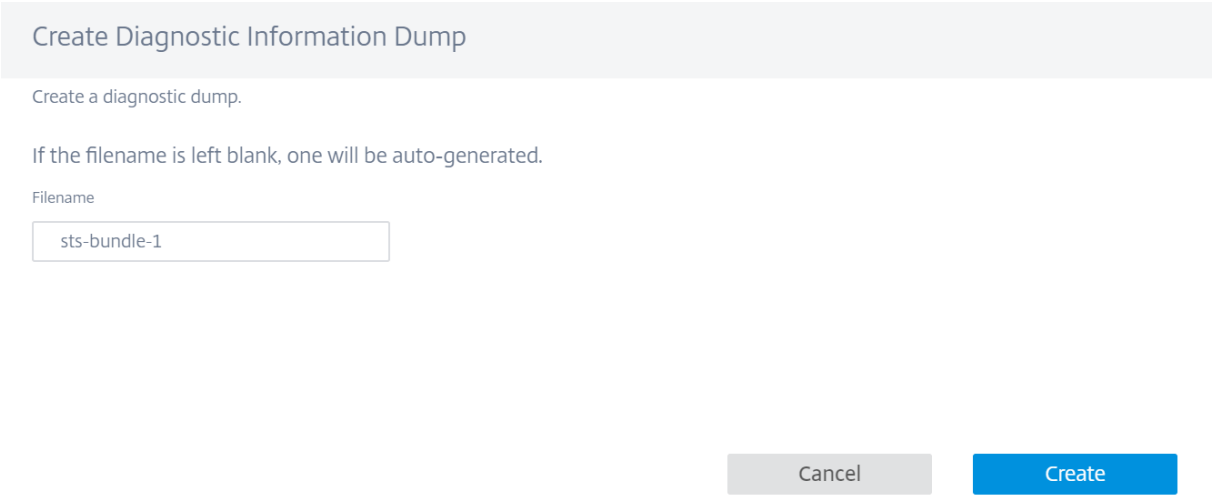
Um ein STS-Bundle für eine Standort-Appliance zu erstellen, navigieren Sie auf Standortebene zu Fehlerbehebung**>**STS-Bundle**, und klicken**



Geben Sie einen Namen für das STS-Paket an. Der Name muss mit einem Buchstaben beginnen und kann Buchstaben, Zahlen, Bindestriche und Unterstriche enthalten. Die maximal zulässige Länge des Namens beträgt 32 Zeichen. Der vom Benutzer angegebene Name wird als Präfix im endgültigen Namen verwendet. Um sicherzustellen, dass die Dateinamen eindeutig sind (Zeitstempel) und um das Gerät anhand des STS-Pakets (Seriennummer) zu erkennen, generiert der Dienst einen vollständigen

Namen. Wenn kein Name angegeben wird, wird beim Erstellen des Bundles automatisch ein Name generiert.

Sie können nur dann eine neue STS anfordern, wenn das Gerät online ist und derzeit kein STS-Prozess auf der Appliance ausgeführt wird. Sie können ein bereits verfügbares STS vom Citrix SD-WAN Orchestrator Service herunterladen, auch wenn das Gerät offline ist.



Der STS-Prozess befindet sich zu einem bestimmten Zeitpunkt in einem der folgenden Zustände:

STS-Status	Beschreibung
Angefragt	Es wird ein neues STS-Paket angefordert. Die Bearbeitung der Anfrage dauert einige Minuten. Sie können den STS-Erstellungsprozess bei Bedarf abbrechen.
Hochladen	Das erstellte STS-Paket wird in den Cloud-Dienst hochgeladen. Die Dauer hängt von der Größe des Pakets ab. Der Status wird alle 5 Sekunden aktualisiert. Sie können den STS-Upload-Prozess nicht abbrechen.
Misserfolg	Der STS-Prozess ist während der Erstellung oder beim Hochladen fehlgeschlagen. Sie können die Einträge von fehlgeschlagenen STS-Vorgängen löschen.
Zum Download verfügbar	Der STS-Erstellungs- und Upload-Prozess ist erfolgreich. Sie können jetzt die STS-Pakete herunterladen oder löschen.

Sobald der STS-Prozess auf der Appliance gestartet wird, wird der Fortschritt in regelmäßigen Abstän-

den in der Statusspalte aktualisiert. Zum Beispiel **Angefordert (Sammeln von Protokolldateien)**.

Die STS-Bundles und Fehlerdatensätze werden 7 Tage lang aufbewahrt, danach werden sie automatisch gelöscht.

Berichte des Anbieters

October 21, 2022

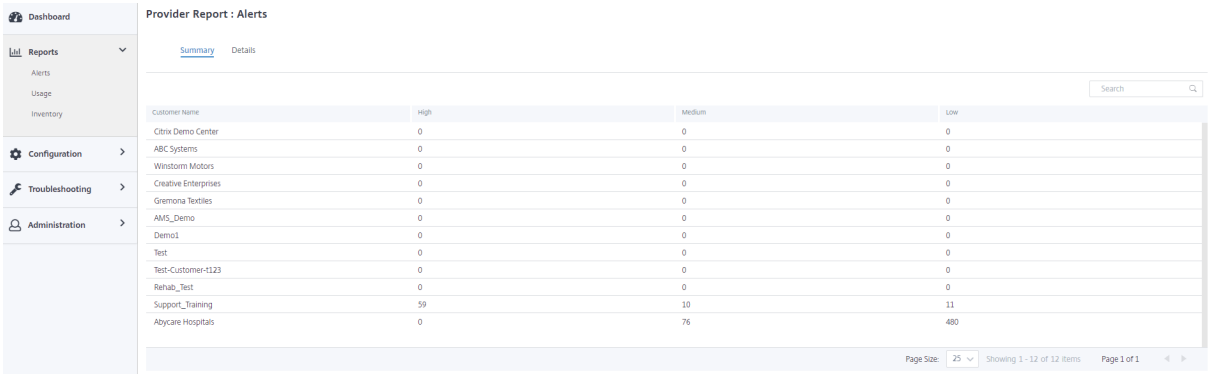
Die **Anbieterberichte** bieten Einblick in Warnmeldungen, Nutzungstrends und Inventar, das über alle von einem Anbieter verwalteten Kunden hinweg aggregiert wird.

Navigieren Sie in der Benutzeroberfläche des Citrix SD-WAN Orchestrator Service Orchestrator-Dienstanbieters zu **Berichte**.

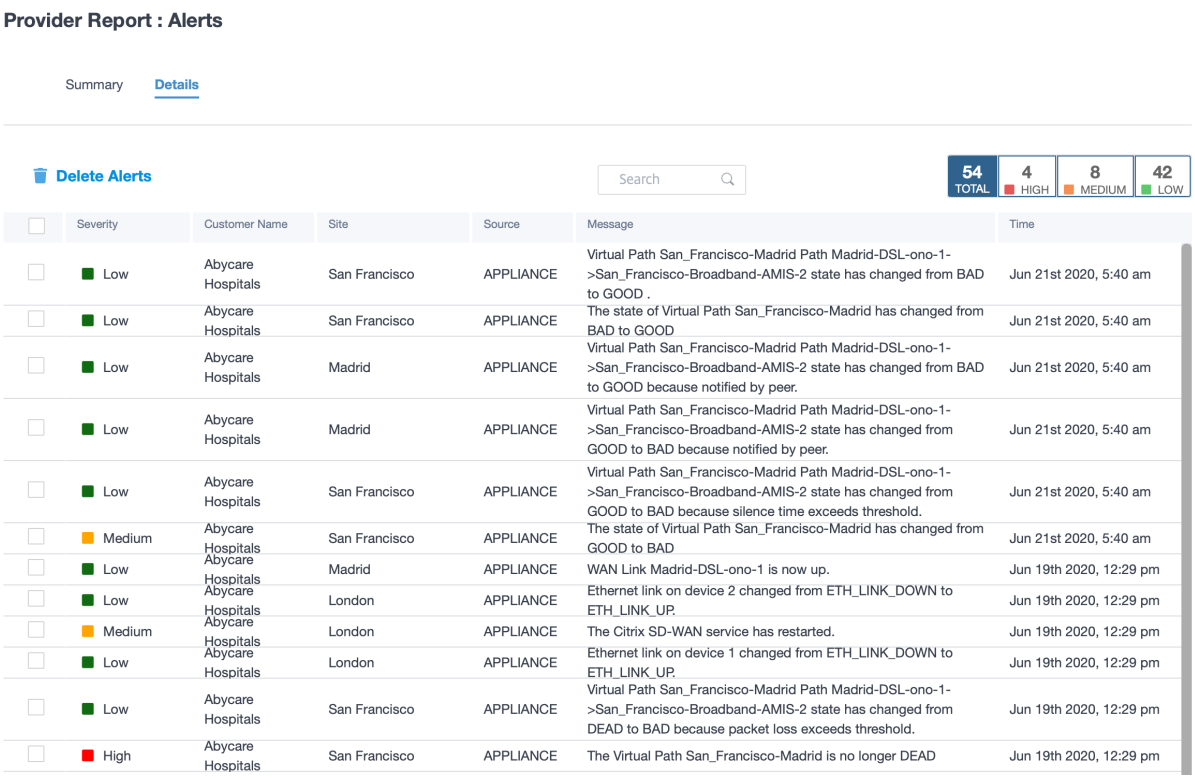
Warnungen

Der Anbieter kann alle Ereignisse und Warnungen überprüfen, die in allen Kundennetzwerken generiert wurden.

In der **Zusammenfassungsansicht** wird die Anzahl der hohen, mittleren und niedrigen Alarme für jeden Kunden angezeigt.



Sie können auch den Schweregrad, den Standort, an dem die Warnung ausgelöst wurde, die Warnmeldung, die Uhrzeit und andere Informationen unter **Details anzeigen**.



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

Geeignete Filteroptionen können nach Bedarf verwendet werden, zum Beispiel: Suchen Sie nach Alerts mit hohem Schweregrad für alle Kunden oder nach Alerts für einen bestimmten Kunden und so weiter.

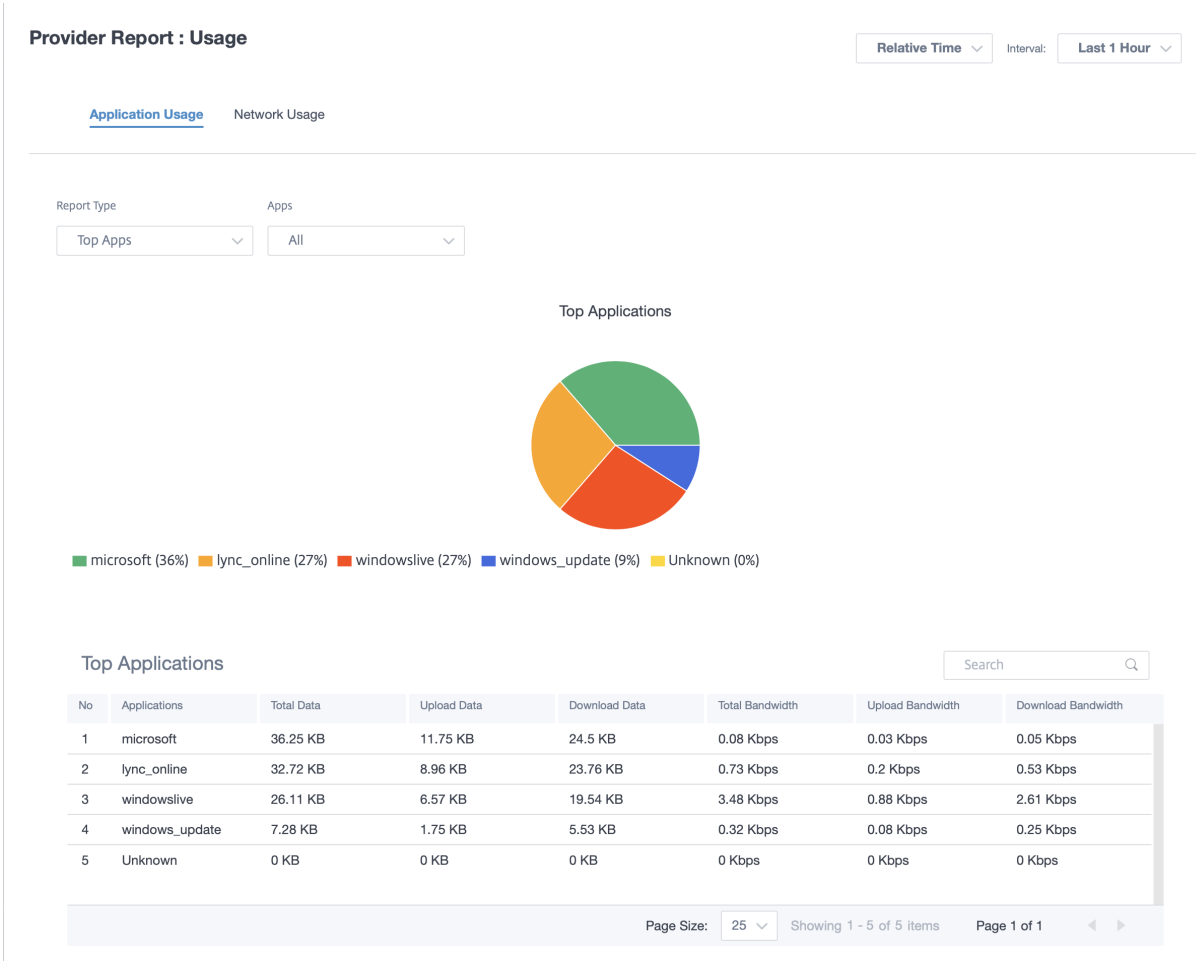
Sie können Warnmeldungen auch auswählen und löschen.

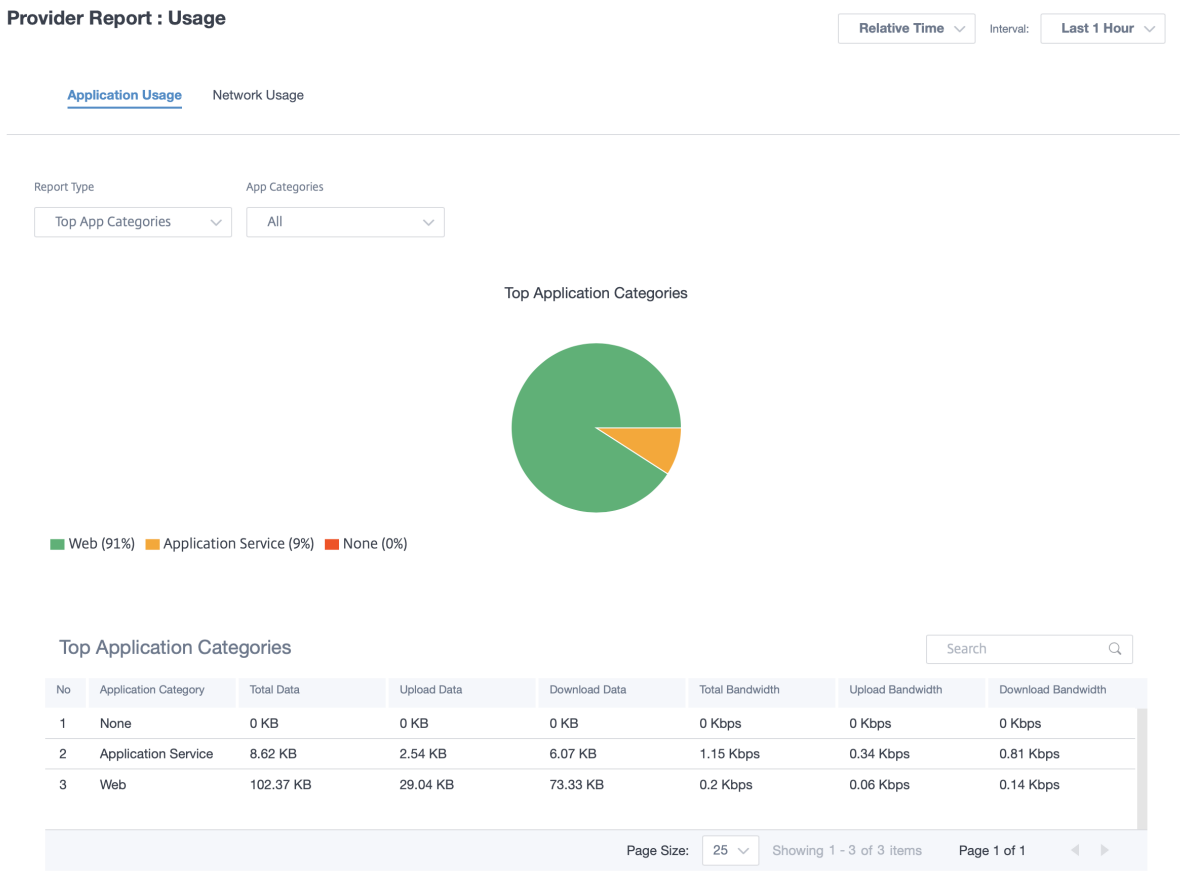
Verwendung

Der Anbieter kann kundenübergreifende Nutzungstrends wie **Top-Anwendungen**, **Top-Anwendungskategorien**, **Anwendungsbandbreite**und **Top-Sites**überprüfen.

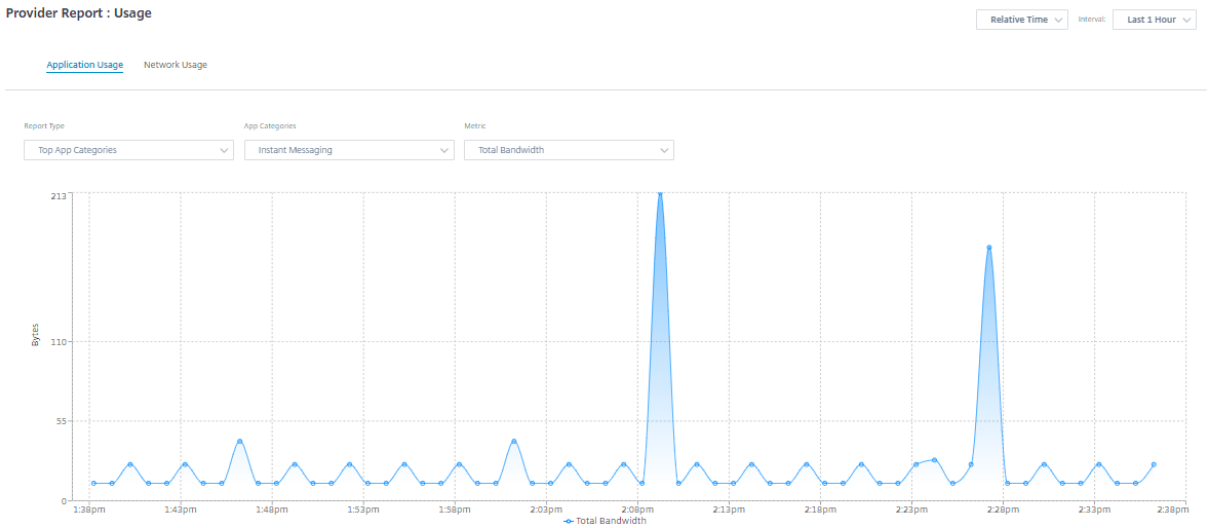
Top Bewerbungs- und Anwendungskategorien

Das Diagramm „ **Top-Anwendungen“und „Top-Anwendungskategorien** “zeigt die Anwendungen und Anwendungsfamilien, die in allen Kundennetzwerken weit verbreitet sind. Auf diese Weise können Sie das Datenverbrauchsmuster analysieren und bei Bedarf das Bandbreitenlimit für jede Datenklasse neu zuweisen.





Sie können die Statistiken zur Bandbreitennutzung anzeigen. Die Bandbreitenstatistiken werden für das ausgewählte Zeitintervall gesammelt. Sie können den Statistikbericht basierend auf **Berichtstyp, Apps- oder Apps-Kategorien** und **Metriken**filtern.

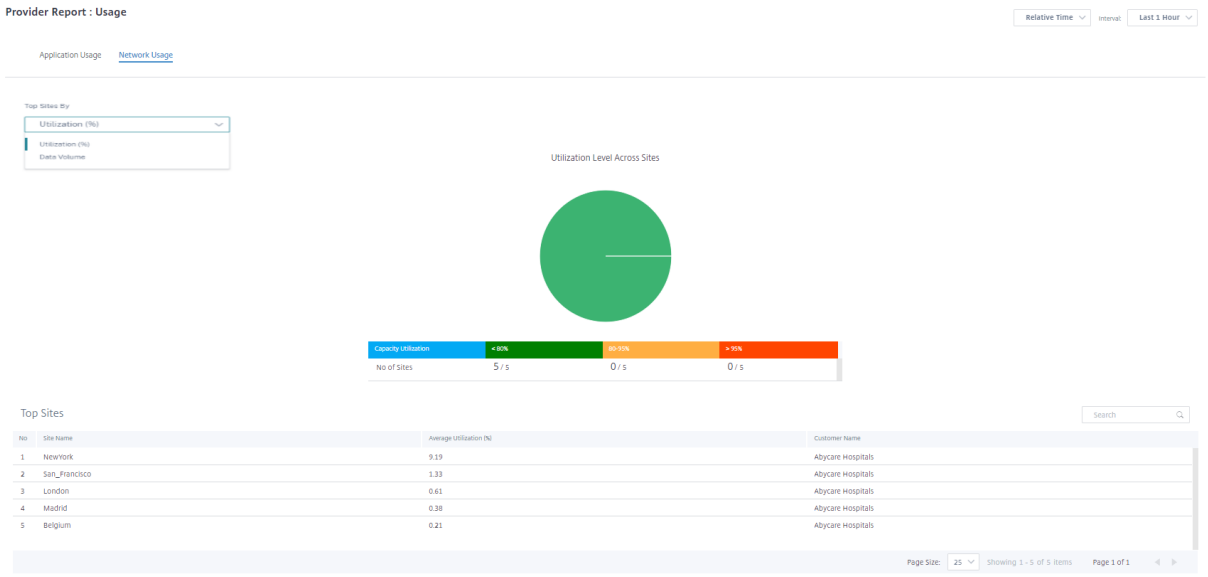


- **Berichtstyp:** Wählen Sie **Top-App- oder App-Kategorien** aus der Liste aus.
- **Apps/App-Kategorien:** Wählen Sie die Top-Anwendung oder Kategorien aus der Liste aus.

- **Metrik:** Wählen Sie die Bandbreitenmetrik (z. B. Gesamtdaten, Eingehende Daten, Gesamtbandbreite) aus der Liste aus.

Netzwerknutzung

Das Diagramm zur Netzwerknutzung zeigt die 10 wichtigsten Standorte aller Kunden mit der höchsten Bandbreitennutzung. Sie können die Sites nach Auslastung (%) oder Datenvolumen (MB) anzeigen.



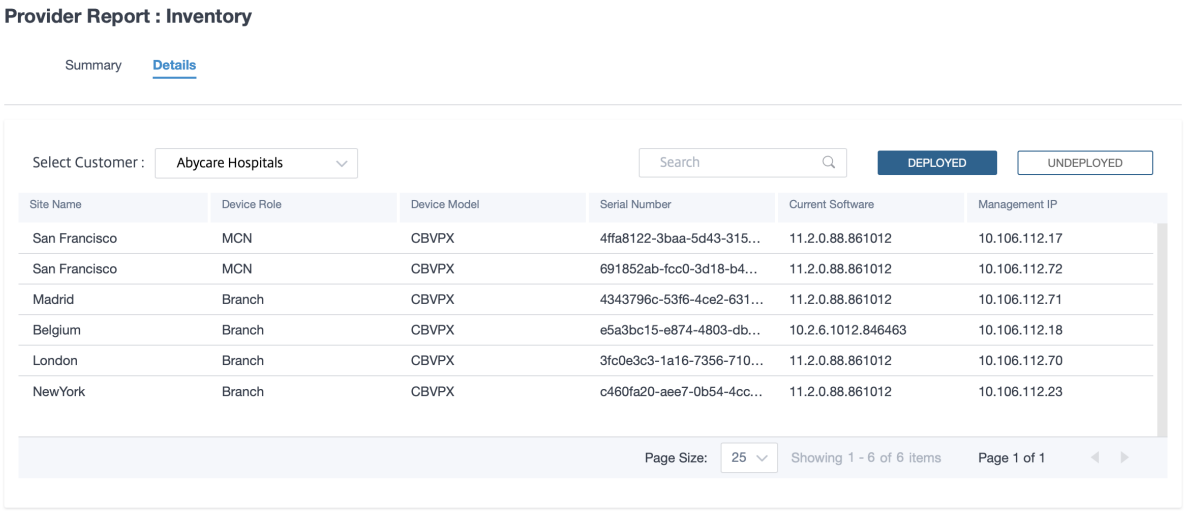
Inventar

Der Anbieter kann den gesamten Gerätebestand aller Kunden einsehen. Sie können wählen, ob Sie eine Inventarzusammenfassung oder eine Detailansicht anzeigen möchten.

Die Inventarzusammenfassungsansicht bietet ein Diagramm der Bestandsverteilung, in dem die verschiedenen Appliance-Modelle und die Anzahl der einzelnen Appliance-Typen dargestellt werden, die in Kundennetzwerken verwendet werden.

Geeignete Filteroptionen können nach Bedarf verwendet werden, zum Beispiel: Suchen Sie nach allen Geräten, die einem bestimmten Kunden gehören, oder nach allen Geräten mit einem bestimmten Gerätemodell und so weiter.

Die Detailansicht des Inventars enthält eine Liste aller bereitgestellten Appliances und der Appliances, die konfiguriert, aber noch nicht bereitgestellt wurden. Wählen Sie in der Dropdownliste **Kunde auswählen** einen Kunden aus. Sie können den Site-Namen, die Geräterolle, das Gerätemodell, die Seriennummer des Geräts, die aktuelle Software und die IP-Adresse der Geräteverwaltung anzeigen.



Kunden-/Netzwerkberichte

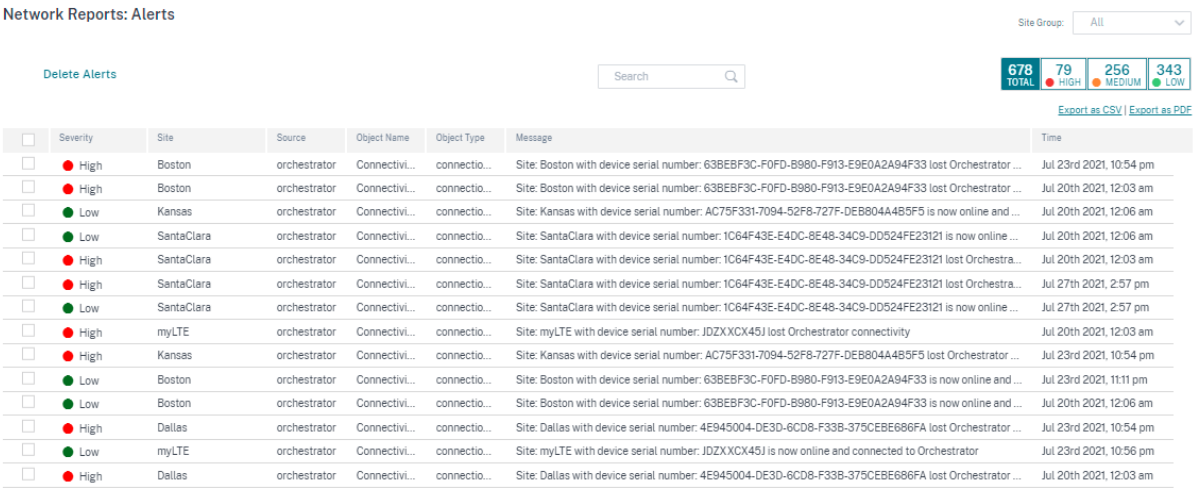
October 21, 2022

Die **Kundenberichte** bieten Einblick in netzwerkweite Warnmeldungen, Nutzungstrends, Inventar, Qualität, Diagnose und Firewallstatus, die über alle Standorte eines Kundennetzwerks hinweg aggregiert werden.

Warnungen

Der Kunde kann einen detaillierten Bericht über alle Ereignisse und Warnungen anzeigen, die an allen Standorten in diesem Netzwerk generiert wurden.

Sie umfasst den Schweregrad, den Ort, an dem die Warnung ausgelöst wurde, die Warnmeldung, die Uhrzeit und andere Details.



Geeignete Filteroptionen können nach Bedarf verwendet werden, zum Beispiel: Suchen Sie nach allen Warnungen mit hohem Schweregrad auf allen Sites oder nach allen Warnungen für eine bestimmte Site und so weiter.

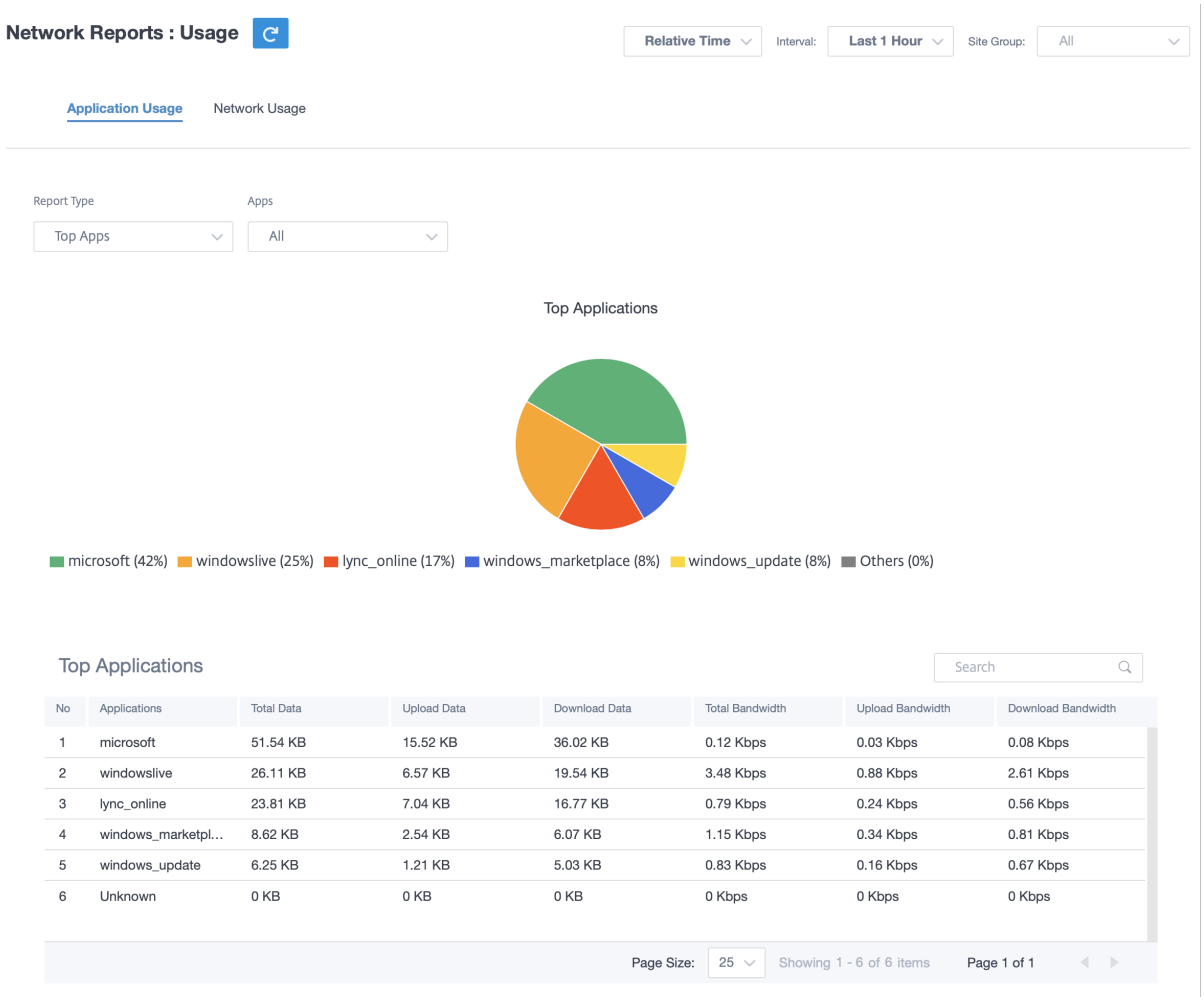
Sie können auch Alarme auswählen und löschen.

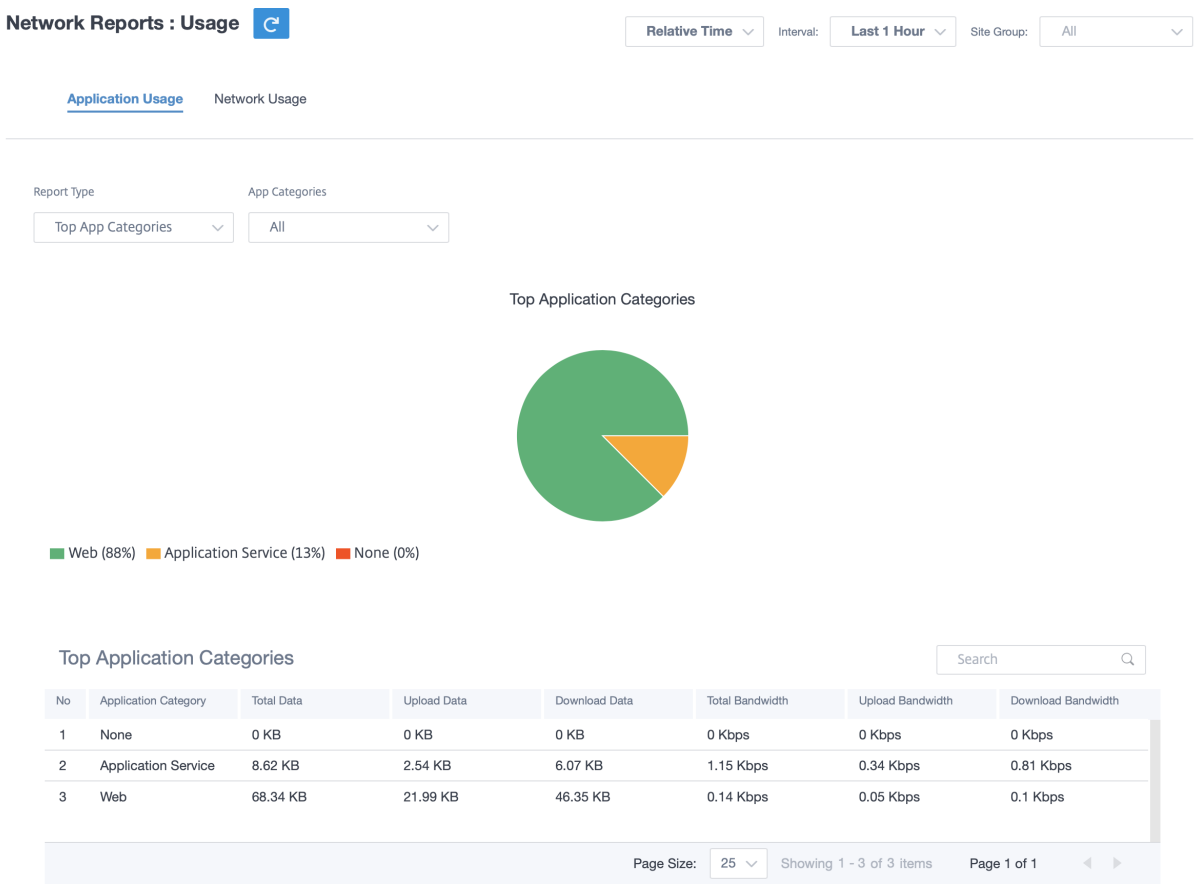
Verwendung

Kunden können Nutzungstrends wie **Top-Anwendungen**, **Top-Anwendungskategorien**, **App-Bandbreite**und **Top-Sites** an allen Standorten in ihrem Netzwerk überprüfen.

Top Bewerbungs- und Anwendungskategorien

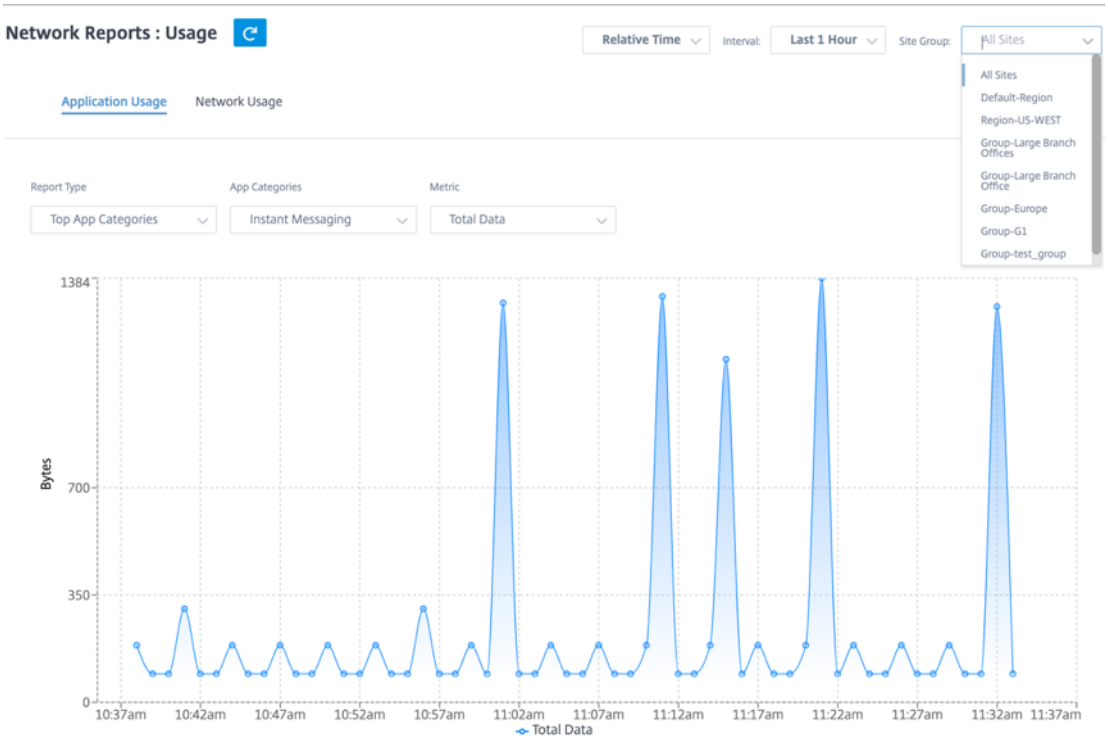
Das Diagramm „ **Top-Anwendungen“und „Top-Anwendungskategorien** “zeigt die wichtigsten Anwendungen und Top-Anwendungsfamilien, die an allen Standorten weit verbreitet sind. Auf diese Weise können Sie das Datenverbrauchsmuster analysieren und das Bandbreitenlimit für jede Datenklasse innerhalb des Netzwerks neu zuweisen.





Bandbreite der Anwendung

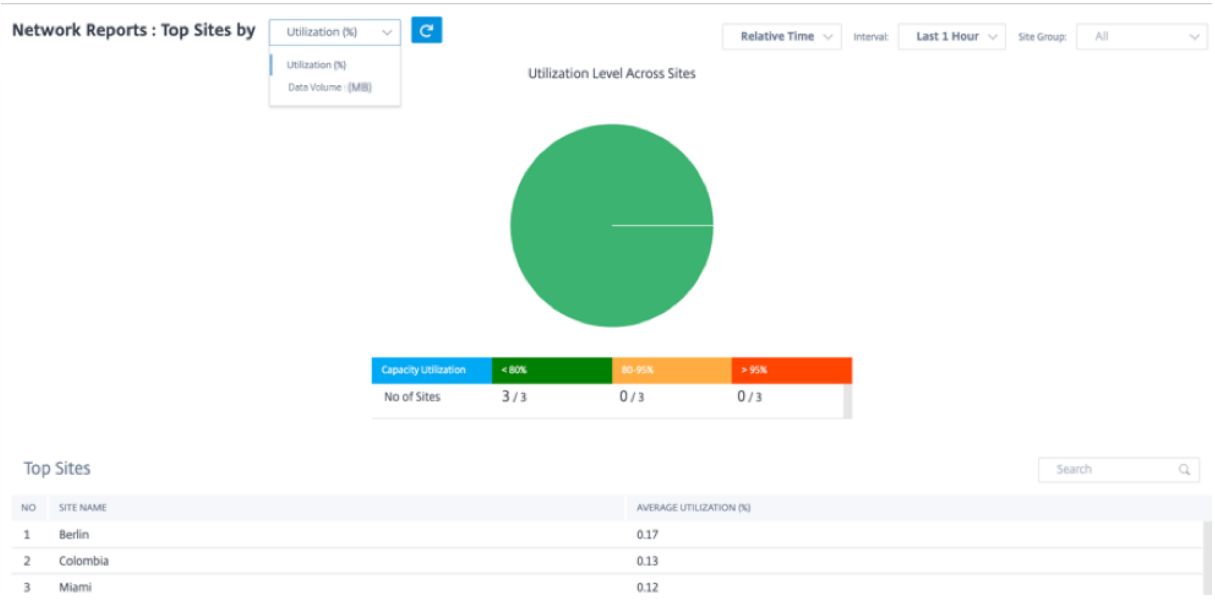
Sie können die Bandbreitennutzungsstatistiken für die ausgewählte Standortgruppe oder für alle Standorte anzeigen. Die Bandbreitenstatistiken werden für das ausgewählte Zeitintervall gesammelt. Sie können den Statistikbericht basierend auf **Berichtstyp, Apps- oder Apps-Kategorien** und **Metriken**filtern.



- **Berichtstyp:** Wählen Sie **Top-App- oder App-Kategorien** aus der Liste aus.
- **Apps/App-Kategorien:** Wählen Sie die wichtigsten Anwendungen oder Kategorien (z. B. Netzwerkdienst) aus der Liste aus.
- **Metrik:** Wählen Sie die Bandbreitenmetrik (z. B. Gesamtdaten, Eingehende Daten, Gesamtbandbreite) aus der Liste aus.

Netzwerknutzung

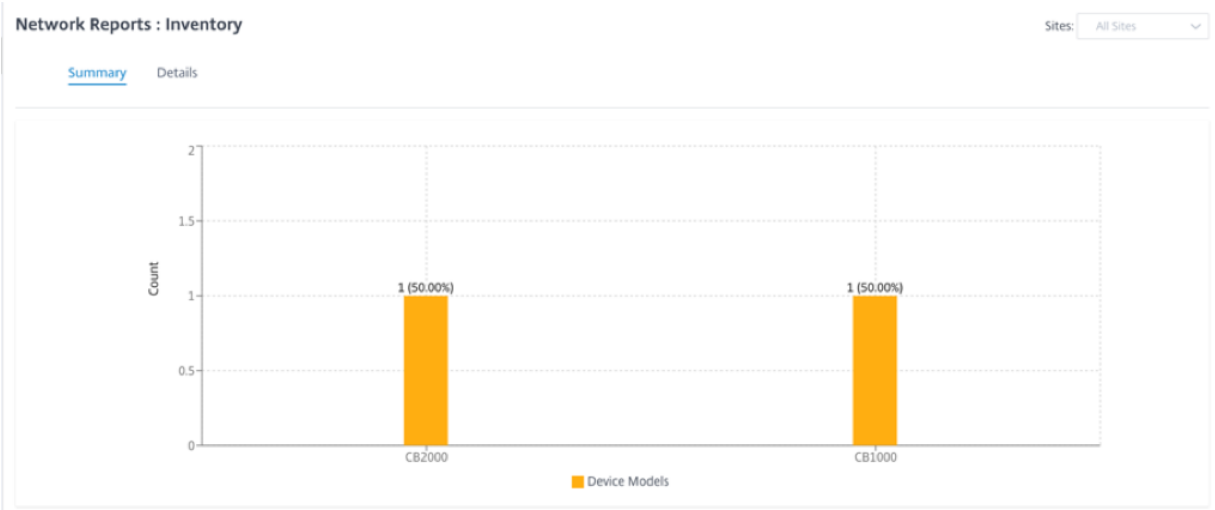
Das Diagramm **Top Sites** zeigt die Top-Sites im Kundennetzwerk, die die höchste Bandbreitennutzung aufweisen. Sie können die Sites nach Auslastung (%) oder Traffic-Volumen (MB) anzeigen.



Inventar

Der Kunde kann den gesamten Gerätebestand an allen Standorten im Netzwerk anzeigen. Sie können wählen, ob Sie eine Inventarzusammenfassung oder eine Detailansicht anzeigen möchten.

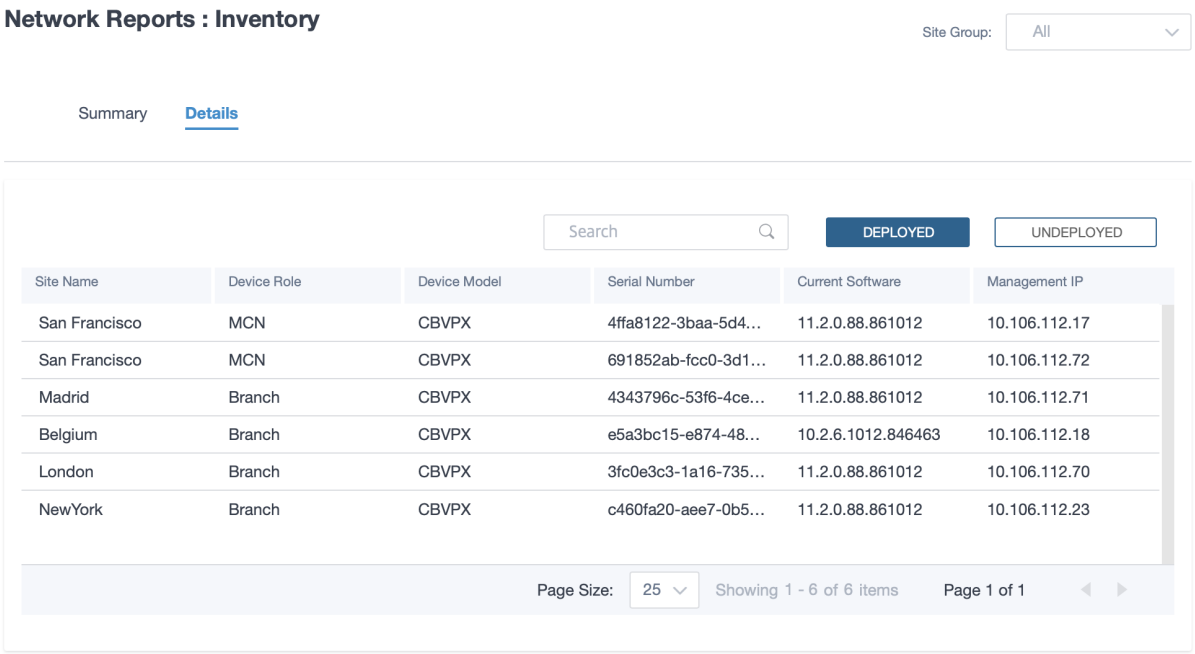
Die Inventarzusammenfassungsansicht bietet ein Diagramm der Bestandsverteilung, in dem die verschiedenen Appliance-Modelle und die Anzahl der einzelnen Appliance-Typen dargestellt werden, die an allen Standorten im Kundennetzwerk verwendet werden.



Geeignete Filteroptionen können nach Bedarf verwendet werden, zum Beispiel: Suchen Sie nach allen Appliances, die zu einer bestimmten Site gehören, oder nach allen Appliances mit einem bestimmten Gerätemodell und so weiter.

Die Detailansicht des Inventars enthält eine Liste aller bereitgestellten Appliances und der Appliances,

die konfiguriert, aber noch nicht bereitgestellt wurden. Zusammen mit dem Kunden, dem Standortnamen, der Geräterolle, der Seriennummer des Geräts, der aktuellen Software und der IP-Adresse der Geräteverwaltung.

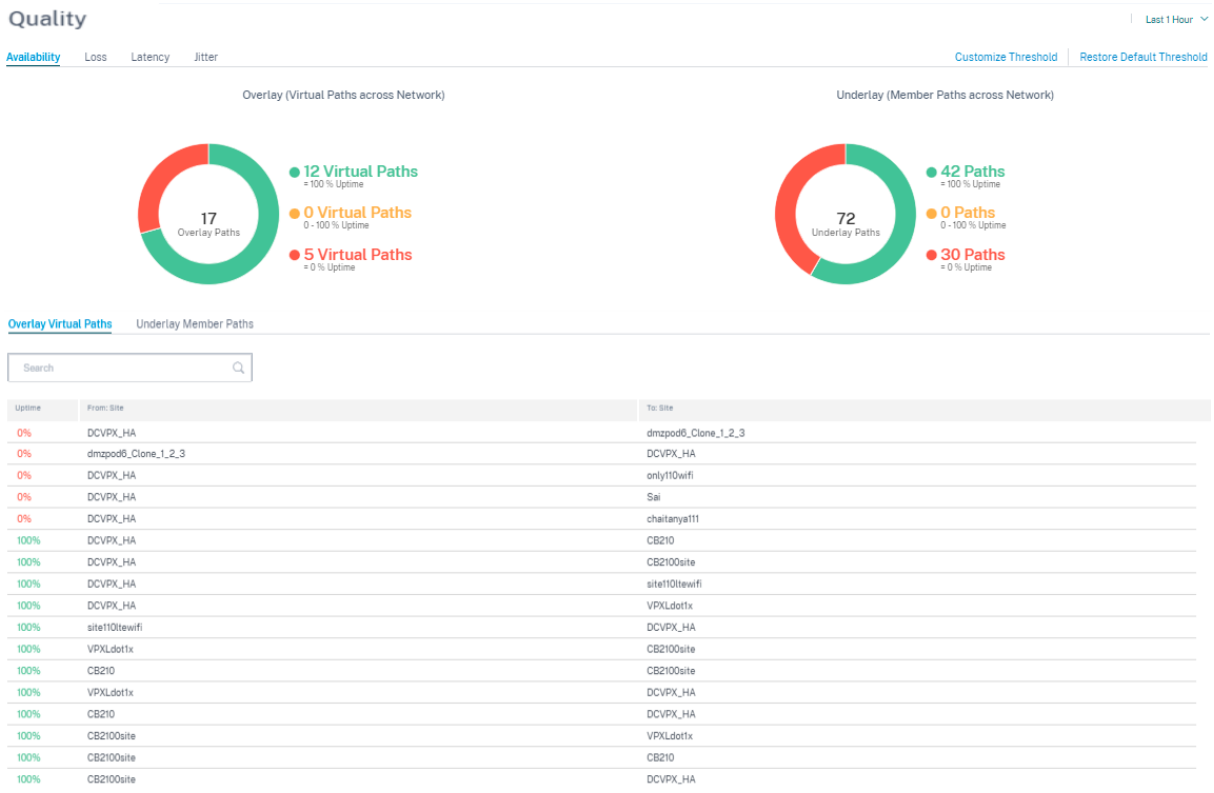


HDX Dashboard und Berichte

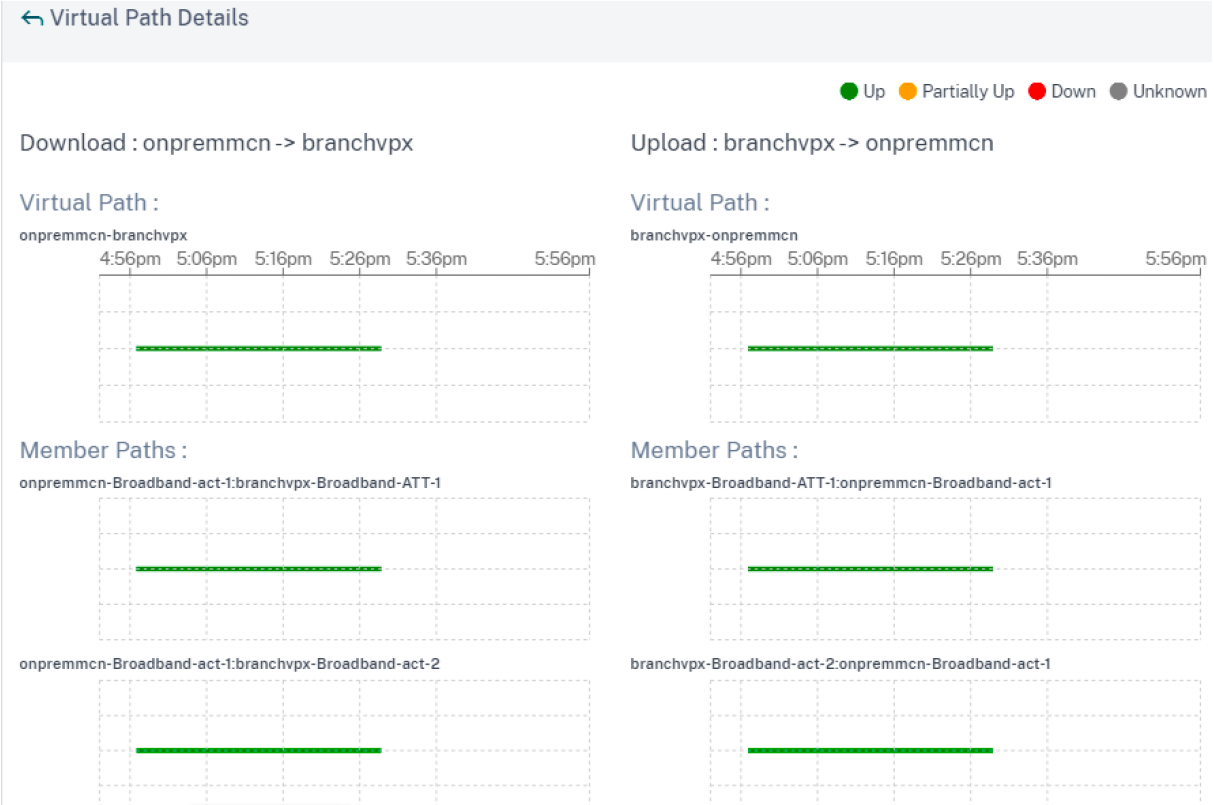
Weitere Informationen zum HDX-Dashboard und zu Berichten finden Sie unter HDX-Dashboard und Berichte.

Qualität

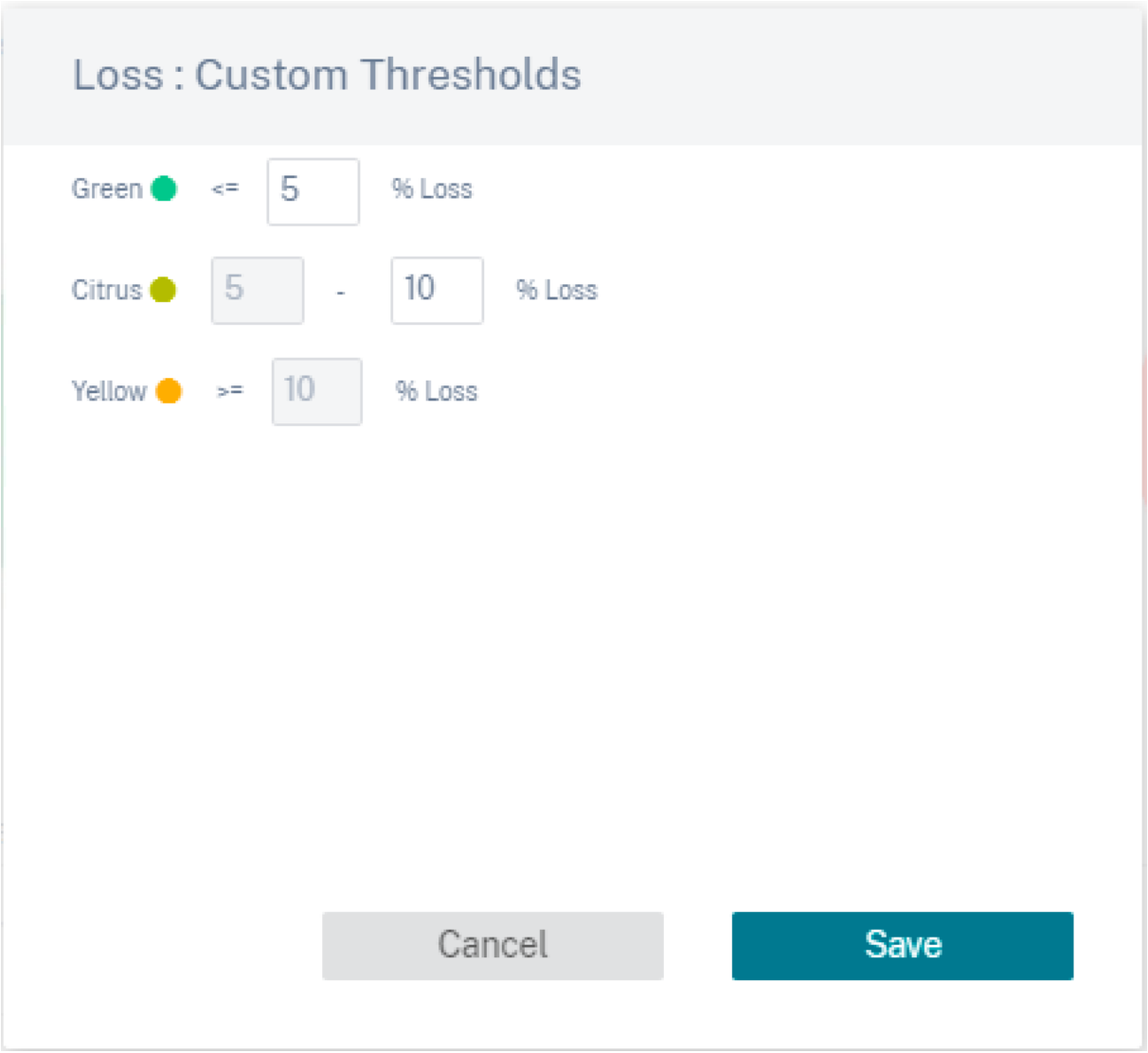
Der Bericht zur **Netzwerkqualität** ermöglicht einen Vergleich zwischen dem virtuellen Overlay und den physischen Underlay-Pfaden auf Netzwerkebene in Bezug auf Verfügbarkeit und Verlust, Latenz und Jitter. Dies hilft dabei, effektiv zu überwachen, wie sich das Overlay im Verhältnis zum Underlay-Netzwerk entwickelt, und hilft auch bei der Fehlerbehebung. Für Latenz und Jitter werden nur die Details der Pfade der Unterlagsmitglieder angezeigt.



Klicken Sie auf den Tabelleneintrag, um die Detailansicht zu sehen.



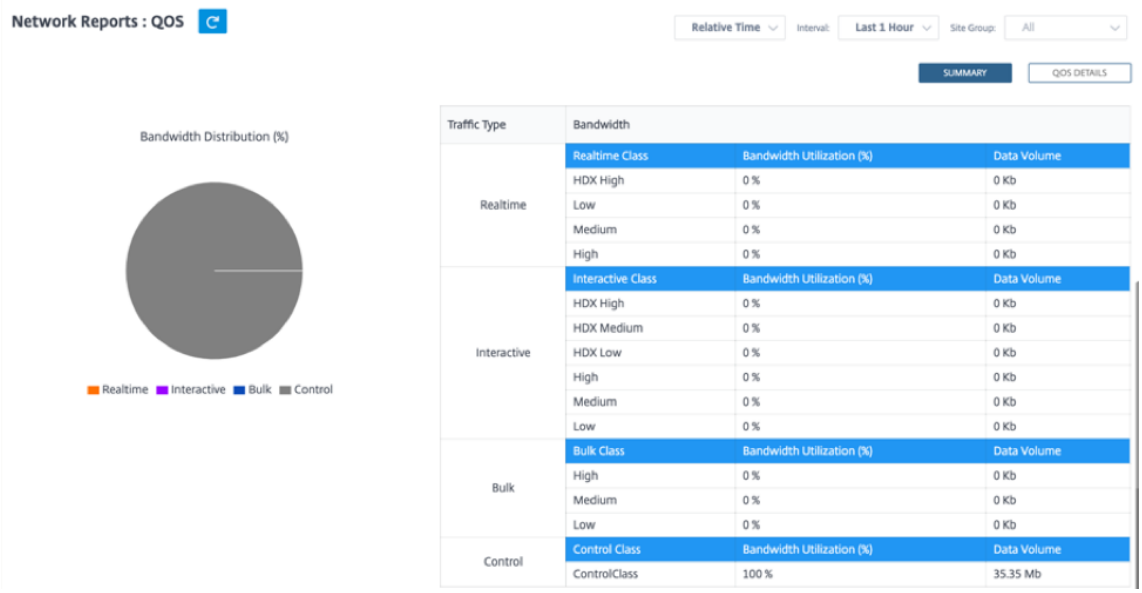
Sie können den Schwellenwert für jeden Netzwerkqualitätsparameter anpassen.



Servicequalität

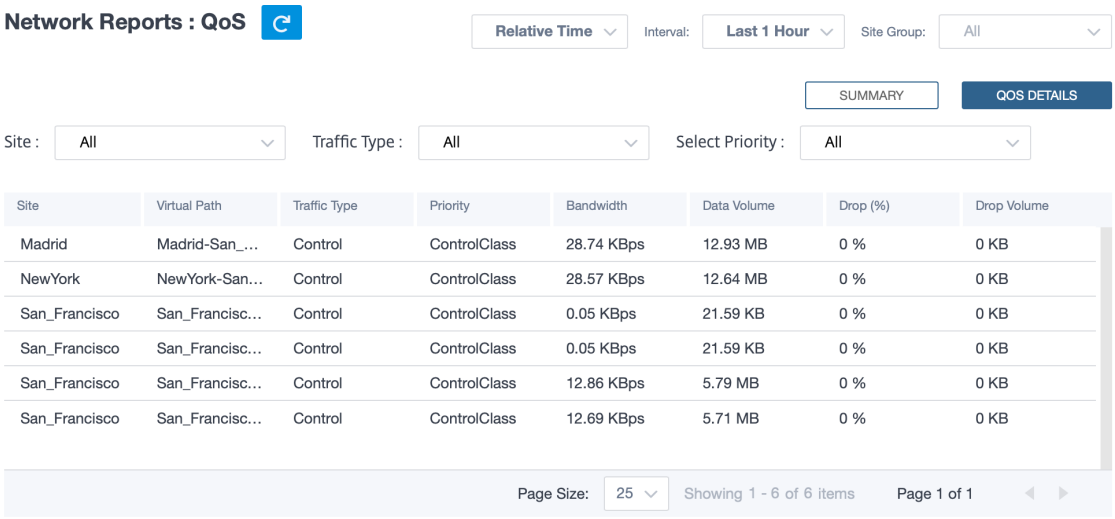
Quality of Service (QoS) verwaltet den Datenverkehr, um Paketverlust, Latenz und Jitter im Netzwerk zu reduzieren. Weitere Informationen finden Sie unter Servicequalität. Es gibt zwei Möglichkeiten, den Quality of Service (QoS) -Bericht anzuzeigen:

- **Zusammenfassungsansicht:** Die Zusammenfassungsansicht bietet einen Überblick über den Bandbreitenverbrauch über alle Arten von Datenverkehr hinweg - Echtzeit, interaktiv, Massenzugriff und Steuerung im gesamten Netzwerk und pro Standort.



  - **Echtzeit:** Wird für zeitkritischen Datenverkehr mit geringer Latenz, geringer Bandbreite verwendet. Echtzeitanwendungen sind zeitempfindlich, benötigen aber keine wirklich hohe Bandbreite (zum Beispiel Voice over IP). Echtzeitanwendungen reagieren empfindlich auf Latenz und Jitter, können aber einige Verluste tolerieren.
  - **Interaktiv:** Wird für interaktiven Datenverkehr mit niedrigen bis mittleren Latenzanforderungen und niedrigen bis mittleren Bandbreitenanforderungen verwendet. Interaktive Anwendungen beinhalten menschliche Eingaben in Form von Mausklicks oder Cursorbewegungen. Die Interaktion erfolgt in der Regel zwischen einem Client und einem Server. Die Kommunikation benötigt möglicherweise keine hohe Bandbreite, ist aber empfindlich gegenüber Verlust und Latenz. Server zu Client benötigt jedoch eine hohe Bandbreite, um grafische Informationen zu übertragen, die möglicherweise nicht verlustempfindlich sind.
  - **Bulk:** Wird für Datenverkehr mit hoher Bandbreite verwendet, der hohe Latenz tolerieren kann. Anwendungen, die Dateiübertragung verarbeiten und eine hohe Bandbreite benötigen, werden als Massenklasse kategorisiert. Diese Anwendungen beinhalten wenig menschliche Eingriffe und werden meist von den Systemen selbst behandelt.
  - **Steuerung:** Wird verwendet, um Steuerpakete zu übertragen, die Informationen zu Routing, Scheduling und Verbindungsstatistiken enthalten.

- **Detailansicht:** Die Detailansicht erfasst Trends in Bezug auf Bandbreitenverbrauch, Verkehrsaufkommen, verworfene Pakete usw. für jede QoS-Klasse, die einem virtuellen Overlay-Pfad zugeordnet ist.



Dieser Bericht ist auf Standortebene verfügbar, auf der der Benutzer QoS-Statistiken basierend auf dem virtuellen Pfad zwischen den beiden Sites anzeigen kann. Weitere Informationen finden Sie unter Site-Berichte.

Historische Statistik

Für jede Site können Sie die Statistiken als Diagramme für die folgenden Netzwerkparameter anzeigen:

- Sites
- Virtuelle Pfade
- Pfade
- WAN-Links
- Schnittstellen
- Klassen
- GRE Tunnel
- IPsec-Tunnel

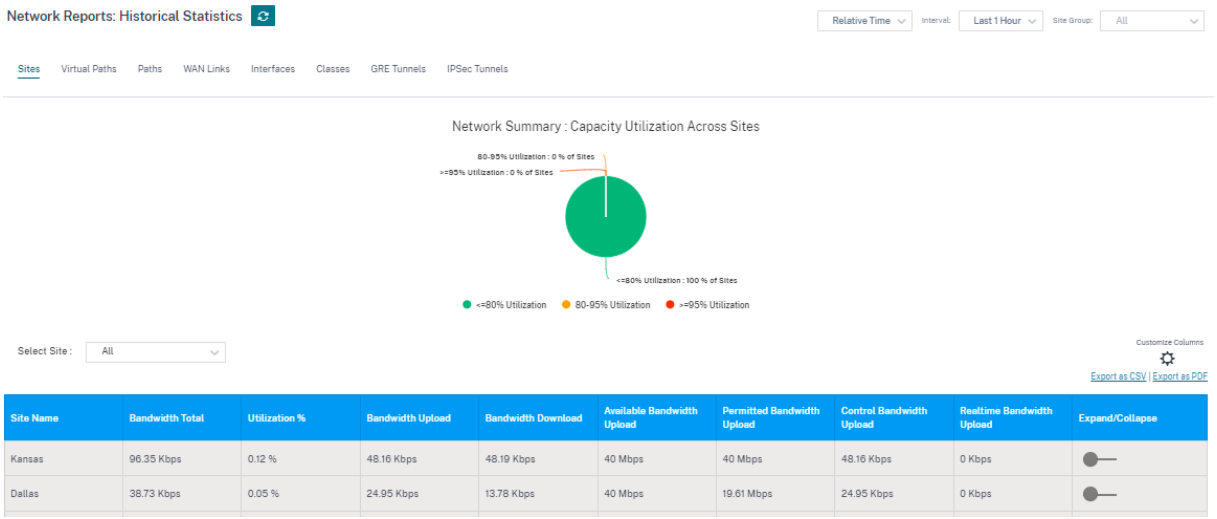
Die Statistiken werden als Grafiken gesammelt. Diese Diagramme werden als Zeitleiste im Vergleich zur Nutzung dargestellt, sodass Sie die Nutzungstrends verschiedener Netzwerkobjekteigenschaften verstehen können. Sie können Diagramme für netzwerkweite Anwendungsstatistiken anzeigen.

Sie können die Grafiken anzeigen oder ausblenden und die Spalten nach Bedarf anpassen.

Sites

Um die Site-Statistiken anzuzeigen, navigieren Sie zu **Berichte > Historische Statistiken > Sites** .

Wählen Sie den Site-Namen aus der Liste aus.

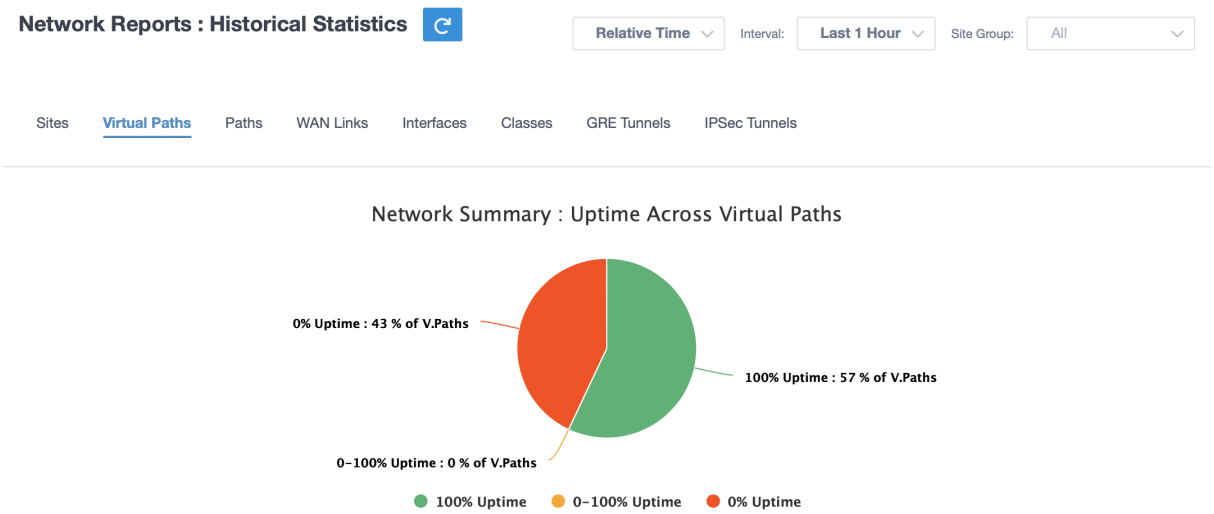


Sie können die folgenden Metriken anzeigen:

- **Site-Name**: Der Site-Name.
- **Bandbreite gesamt: Gesamtbandbreite**, die von allen Pakettypen verbraucht wird. Bandbreite = Kontrollbandbreite + Echtzeit-Bandbreite + Interaktive Bandbreite + Massenbandbreite.
- **Auslastung**: Sie können die Site-Statistiken nach Auslastung (%) anzeigen.
- **Bandbreiteneingang**: Die maximale und minimale Download-Geschwindigkeit über den WAN-Port.
- **Bandbreitenausgang**: Die maximale und minimale Upload-Geschwindigkeit über den WAN-Port.
- **Verfügbarer Bandbreiteneintrag**: Gesamtbandbreite, die allen WAN-Verbindungen eines Standorts zugewiesen ist.
- **Zulässiger Bandbreiteneintrag**: Für die Übertragung von Informationen verfügbare Bandbreite.
- **Bandbreiteneintritt steuern**: Bandbreite, die zur Übertragung von Steuerpaketen verwendet wird, die Informationen zu Routing, Scheduling und Verbindungsstatistiken
- **Realtime Bandwidth Ingress**: Bandbreite, die von Anwendungen verbraucht wird, die zum Echtzeit-Klasstyp in der NetScaler SD-WAN-Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz ab. Ein verzögertes Paket ist schlechter als ein verlorenes Paket (z. B. VoIP, Skype for Business).
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

Virtuelle Pfade

Um die Statistiken zu **virtuellen Pfaden** anzuzeigen, navigieren Sie zur Registerkarte **Berichte > Statistiken > Virtuelle Pfade** .



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	

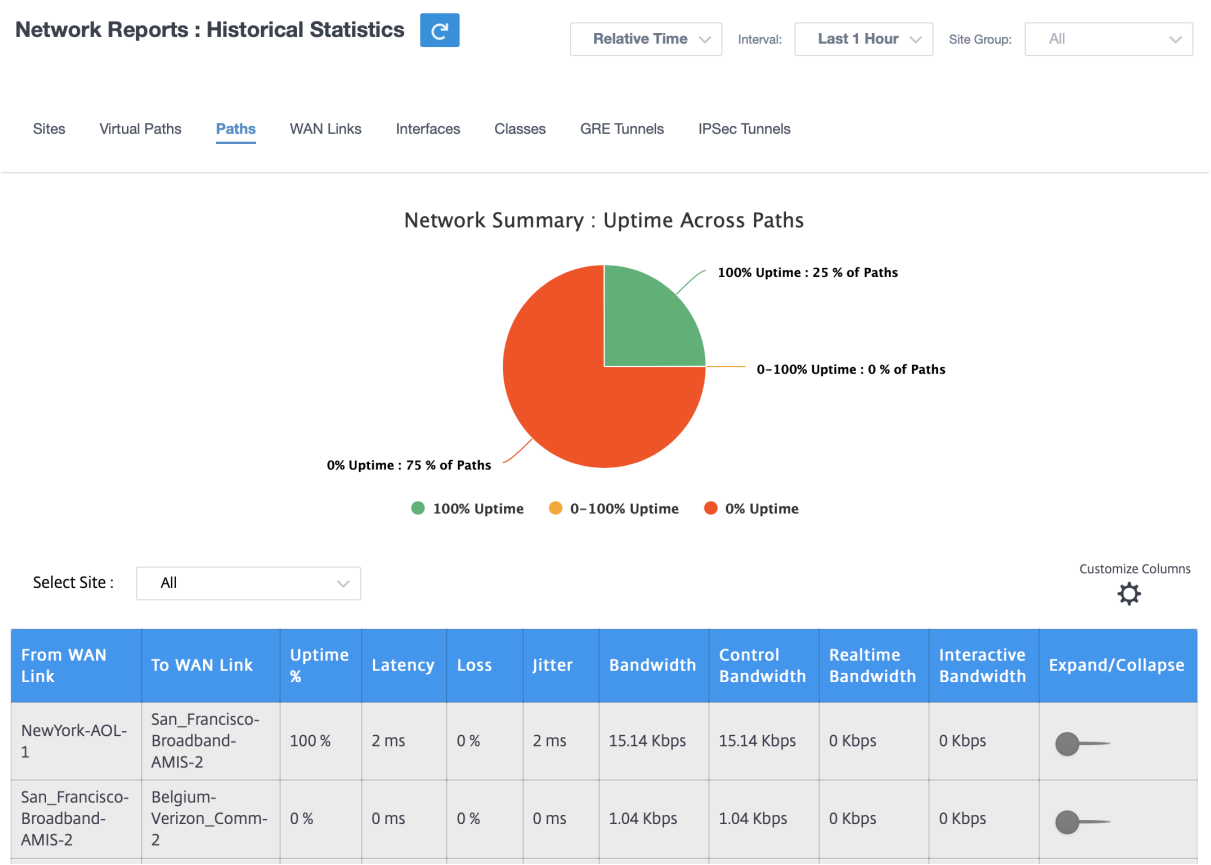
Sie können die folgenden Metriken anzeigen:

- **Name des virtuellen Pfads**: Der Name des virtuellen Pfads.
- **Latenz**: Die Latenz in Millisekunden für Echtzeitverkehr.
- **Verlust**: Prozentsatz der verlorenen Pakete.
- **Jitter**: Variation der Verzögerung empfangener Pakete in Millisekunden.
- **Bandbreiteneingang**: Ingress-Bandbreitennutzung (LAN zu WAN) für den ausgewählten Zeitraum.
- **Bandbreite steuern: Bandbreite**, die für die Übertragung von Steuerpaketen verwendet wird, die Informationen zu Routing, Planung und Verbindungsstatistiken enthalten.
- **Echtzeitbandbreite**: Bandbreite, die von Anwendungen verbraucht wird, die zum Echtzeit-Klasstyp in der SD-WAN-Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz ab. Ein verzögertes Paket ist schlechter als ein verlorenes Paket (z. B. VoIP, Skype for Business).

- **Interaktive Bandbreite**: Bandbreite, die von Anwendungen verbraucht wird, die zum interaktiven Klassentyp in der SD-WAN-Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz und dem Paketverlust ab (z. B. XenDesktop, XenApp).
- **Massenbandbreite**: Bandbreite, die von Anwendungen verbraucht wird, die zum Bulk-Klasstyp in der SD-WAN-Konfiguration gehören. Diese Anwendungen erfordern wenig menschliches Eingreifen und werden von den Systemen selbst behandelt (zum Beispiel FTP, Backup-Operationen).
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

Pfade

Um die **Pfadstatistik** anzuzeigen, navigieren Sie zur Registerkarte **Berichte > Statistiken > Pfade** .



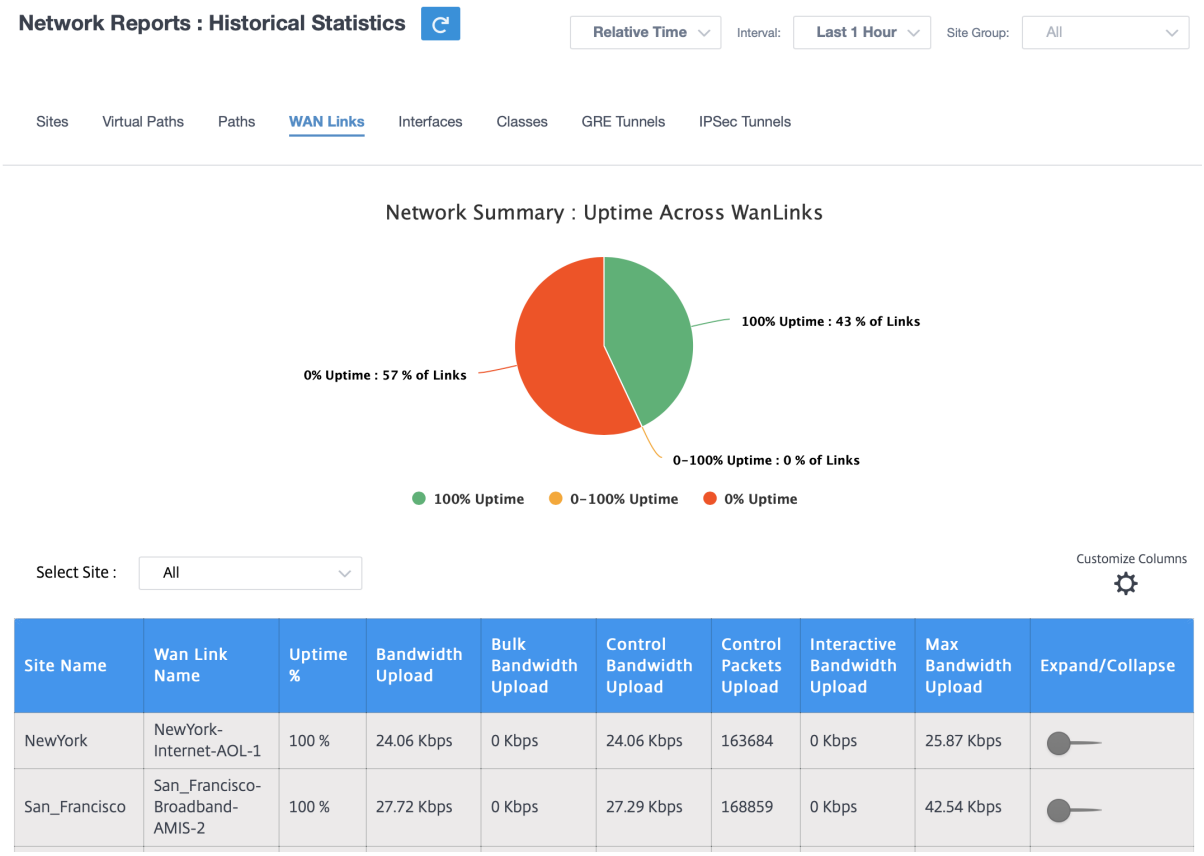
Sie können die folgenden Metriken anzeigen:

- **Von WAN Link**: Der Quell-WAN-Link.
- **Zum WAN-Link**: Die WAN-Zielverbindung.
- **Latenz**: Die Latenz in Millisekunden für Echtzeitverkehr.
- **Verlust**: Prozentsatz der verlorenen Pakete.

- **Jitter**: Variation der Verzögerung empfangener Pakete in Millisekunden.
- **Bandbreite**: Gesamtbandbreite, die von allen Pakettypen verbraucht wird. Bandbreite= Bandbreite steuern + Echtzeitbandbreite + Interaktive Bandbreite + Bulk-Bandbreite.
- **Bandbreite steuern: Bandbreite**, die für die Übertragung von Steuerpaketen verwendet wird, die Informationen zu Routing, Planung und Verbindungsstatistiken enthalten.
- **Echtzeitbandbreite**: Bandbreite, die von Anwendungen verbraucht wird, die zum Echtzeit-Klasstyp in der SD-WAN-Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz ab. Ein verzögertes Paket ist schlechter als ein verlorenes Paket (z. B. VoIP, Skype for Business).
- **Interaktive Bandbreite**: Bandbreite, die von Anwendungen verbraucht wird, die zum interaktiven Klassentyp in der SD-WAN-Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz und dem Paketverlust ab (z. B. XenDesktop, XenApp).
- **Massenbandbreite**: Bandbreite, die von Anwendungen verbraucht wird, die zum Bulk-Klasstyp in der SD-WAN-Konfiguration gehören. Diese Anwendungen erfordern wenig menschliches Eingreifen und werden von den Systemen selbst behandelt (zum Beispiel FTP, Backup-Operationen).
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

WAN-Links

Um die Statistiken auf **WAN-Link-Ebene** anzuzeigen, navigieren Sie zur Registerkarte **Berichte > Statistiken > WAN-Links** .



Site Name	Wan Link Name	Uptime %	Bandwidth Upload	Bulk Bandwidth Upload	Control Bandwidth Upload	Control Packets Upload	Interactive Bandwidth Upload	Max Bandwidth Upload	Expand/Collapse
NewYork	NewYork-Internet-AOL-1	100 %	24.06 Kbps	0 Kbps	24.06 Kbps	163684	0 Kbps	25.87 Kbps	
San_Francisco	San_Francisco-Broadband-AMIS-2	100 %	27.72 Kbps	0 Kbps	27.29 Kbps	168859	0 Kbps	42.54 Kbps	

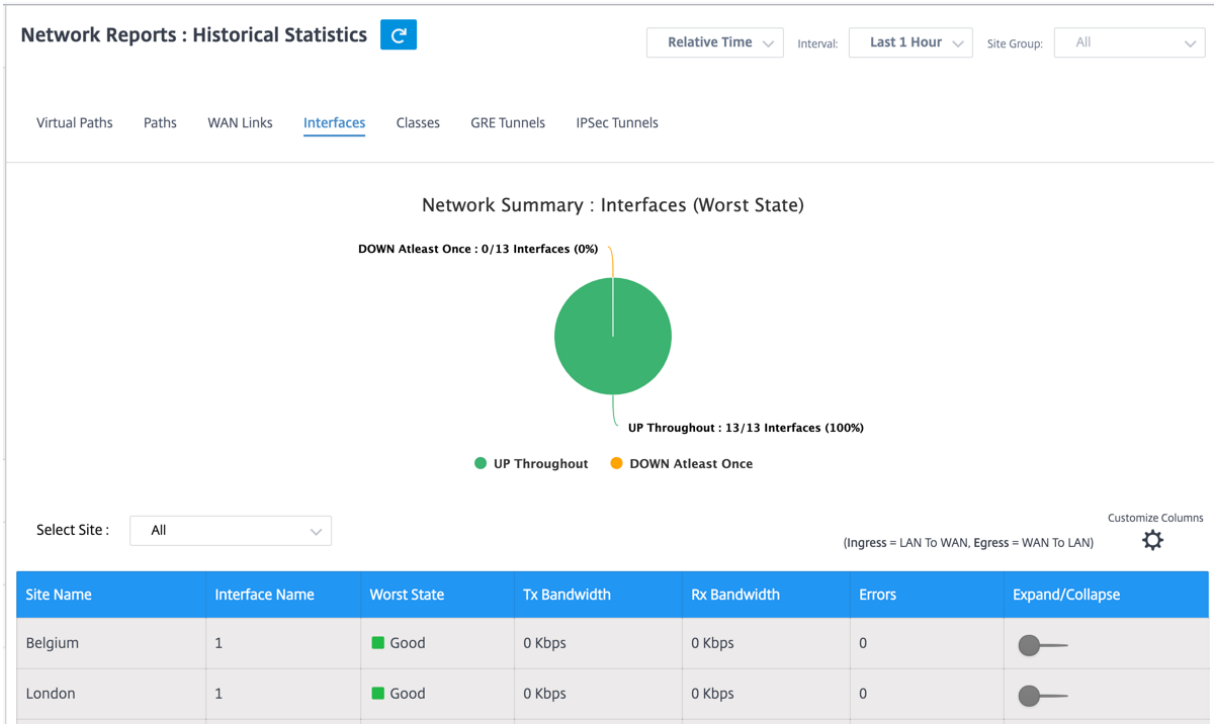
Sie können die folgenden Metriken anzeigen:

- **WAN-Link-Name**: Der Pfadname.
- **Bandbreiteneingang**: Ingress-Bandbreitennutzung (LAN zu WAN) für den ausgewählten Zeitraum.
- **Massenbandbreiteneingang**: Eingangsbandbreite (LAN zu WAN) des virtuellen Pfads, die vom Massenverkehr für den ausgewählten Zeitraum verwendet wird.
- **Bandbreiteneintritt steuern**: Eingangsbandbreite (LAN zu WAN), die vom Kontrolldatenverkehr für den ausgewählten Zeitraum verwendet wird.
- **Control Packet Ingress**: Eingehende (LAN zu WAN) Virtual Path Control-Pakete für den ausgewählten Zeitraum.
- **Interaktiver Bandbreiteneintrag**: Eingangsbandbreite (LAN zu WAN) des virtuellen Pfades, die vom interaktiven Datenverkehr für den ausgewählten Zeitraum verwendet wird.
- **Max. Bandbreiteneintritt**: Max. Eingangsbandbreite (LAN zu WAN), die in einer Minute für den ausgewählten Zeitraum verwendet wird.
- **Min. Bandbreiteneintritt**: Min. Eingangsbandbreite (LAN zu WAN), die in einer Minute für den ausgewählten Zeitraum verwendet wird.
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

Schnittstellen

Der Schnittstellen-Statistikbericht hilft Ihnen bei der Fehlersuche, schnell festzustellen, ob einer der Ports ausgefallen ist. Sie können auch die übertragene und empfangene Bandbreite oder Paketdetails an jedem Port anzeigen. Sie können auch die Anzahl der Fehler anzeigen, die während eines bestimmten Zeitraums auf diesen Schnittstellen aufgetreten sind.

Um **Schnittstellenstatistiken** anzuzeigen, navigieren Sie zur Registerkarte **Berichte > Statistiken > Schnittstellen** .



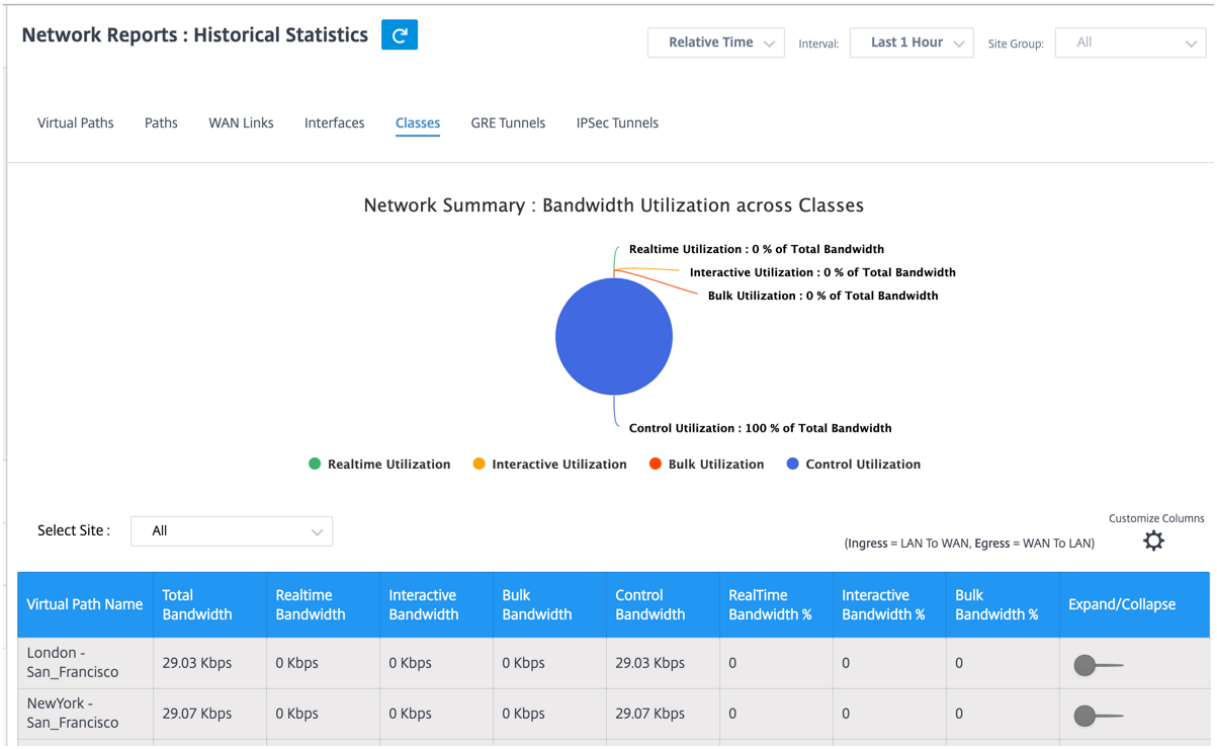
Sie können die folgenden Metriken anzeigen:

- **Schnittstellenname**: Der Name der Ethernet-Schnittstelle.
- **Tx Bandbreite**: Übertragene Bandbreite.
- **Rx-Bandbreite**: Bandbreite erhalten.
- **Fehler**: Anzahl der während des ausgewählten Zeitraums beobachteten Fehler.
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

Klassen

Die virtuellen Dienste können bestimmten QoS-Klassen zugewiesen werden, und unterschiedliche Bandbreitenbeschränkungen können auf verschiedene Klassen angewendet werden.

Um **Klassenstatistiken** anzuzeigen, navigieren Sie zur Registerkarte **Berichte > Statistiken > Klassen** .



Sie können die folgenden Metriken anzeigen:

- **QoS-Klasse**: Der Klassenname.
- **Bandbreite**: Übertragene Bandbreite.
- **Datenvolumen**: Gesendete Daten in Kbps.
- **Drop-Volume**: Prozentsatz der verworfenen Daten.
- **Prozentualer Rückgang**: Prozentsatz der verlorenen Daten.
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

GRE Tunnel

Sie können einen Tunnelmechanismus verwenden, um Pakete eines Protokolls innerhalb eines anderen Protokolls zu transportieren. Das Protokoll, das das andere Protokoll trägt, wird als Transportprotokoll bezeichnet, und das übertragene Protokoll wird als Passagierprotokoll bezeichnet. Generic Routing Encapsulation (GRE) ist ein Tunnelmechanismus, der IP als Transportprotokoll verwendet und viele verschiedene Passagierprotokolle tragen kann.

Die Tunnelquelladresse und die Zieladresse werden verwendet, um die beiden Endpunkte der virtuellen Punkt-zu-Punkt-Verbindungen im Tunnel zu identifizieren. Weitere Informationen zum Konfigurieren von GRE-Tunneln auf Citrix SD-WAN-Appliances finden Sie unter GRE-Tunnel.

Um **GRE-Tunnelstatistiken** anzuzeigen, navigieren Sie zur Registerkarte **Berichte > Statistiken > GRE-Tunnel** .

Sie können die folgenden Metriken anzeigen:

- **Site-Name**: Der Site-Name.
- **Tx Bandbreite**: Übertragene Bandbreite.
- **Rx-Bandbreite**: Bandbreite erhalten.
- **Paket verworfen**: Anzahl der verworfenen Pakete aufgrund von Netzwerküberlastung.
- **Fragmentierte Pakete**: Anzahl fragmentierter Pakete. Pakete werden fragmentiert, um kleinere Pakete zu erstellen, die eine Verbindung mit einer MTU passieren können, die kleiner als das ursprüngliche Datagramm ist. Die Fragmente werden vom empfangenden Host wieder zusammengesetzt.
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

IPsec-Tunnel

IP-Sicherheitsprotokolle (IPsec) bieten Sicherheitsdienste wie Verschlüsselung sensibler Daten, Authentifizierung, Schutz vor Wiederholung und Datenvertraulichkeit für IP-Pakete. Encapsulating Security Payload (ESP) und Authentication Header (AH) sind die beiden IPsec-Sicherheitsprotokolle, die zur Bereitstellung dieser Sicherheitsdienste verwendet werden.

Im IPsec-Tunnelmodus ist das gesamte ursprüngliche IP-Paket durch IPsec geschützt. Das ursprüngliche IP-Paket wird umhüllt und verschlüsselt, und ein neuer IP-Header wird hinzugefügt, bevor das Paket über den VPN-Tunnel übertragen wird.
Weitere Informationen zum Konfigurieren von IPSec-Tunneln auf Citrix SD-WAN-Appliances finden Sie unter IPSec-Tunnelterminierung.

Um **IPSec-Tunnelstatistiken** anzuzeigen, navigieren Sie zur Registerkarte **Reporting > Statistik > IPSec-Tunnel** .

Sie können die folgenden Metriken anzeigen:

- **Tunnelname**: Der Name des Tunnels.
- **Tunnelzustand**: IPsec-Tunnelzustand.
- **MTU**: Maximale Übertragungseinheit —Größe des größten IP-Datagramms, das über eine bestimmte Verbindung übertragen werden kann.
- **Empfangenes Paket**: Anzahl der empfangenen Pakete.
- **Gesendete Pakete**: Anzahl der gesendeten Pakete.
- **Paket verworfen**: Anzahl der verworfenen Pakete aufgrund von Netzwerküberlastung.
- **Byte fallen gelassen**: Anzahl der verworfenen Byte.
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

Statistiken in Echtzeit

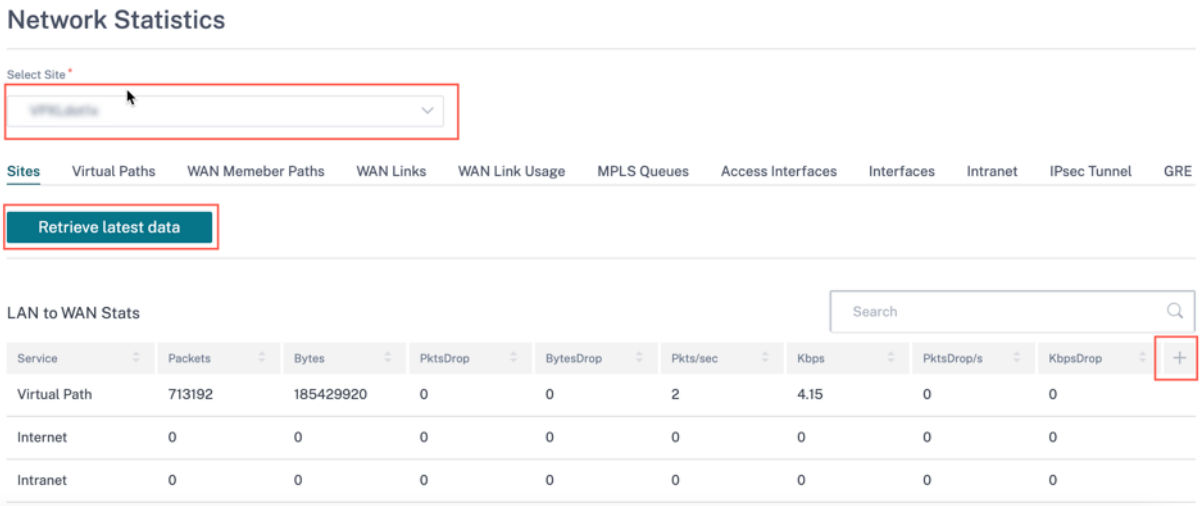
Auf der Seite Echtzeitstatistik werden die folgenden statistischen Informationen auf Kundenebene angezeigt:

Netzwerk-Statistiken

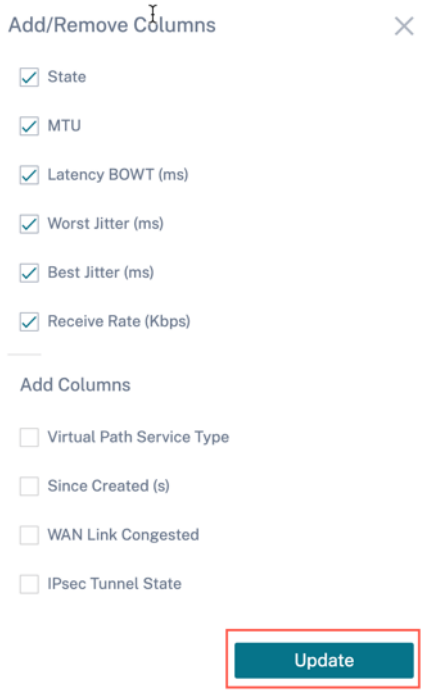
Auf der Seite „ **Netzwerkstatistiken** “finden Sie unter **Berichte** > **Echtzeit** > **Netzwerkstatistiken**die folgenden statistischen Echtzeitinformationen:

- Sites
- Virtuelle Pfade
- Wege für WAN-Mitglieder
- WAN-Links
- WAN-Link-Nutzung
- MPLS-Warteschlangen
- Access Interfaces
- Schnittstellen
- Intranet
- IPsec-Tunnel
- GRE

Um einen statistischen Echtzeitbericht zu erhalten, wechseln Sie zur gewünschten Registerkarte (z. B. Standorte, virtuelle Pfade, WAN-Links), wählen Sie die Site aus der Dropdown-Liste aus und klicken Sie auf **Neueste Daten abrufen**.



Klicken Sie auf das Pluszeichen (+), um der Statistiktabelle eine Spalte hinzuzufügen oder daraus zu entfernen, und klicken Sie auf **Aktualisieren**.

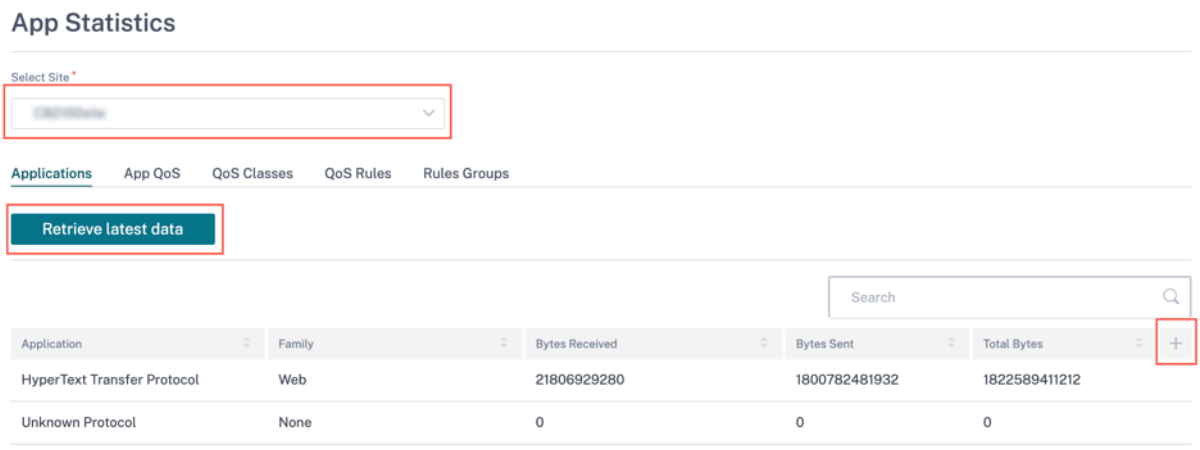


App-Statistik

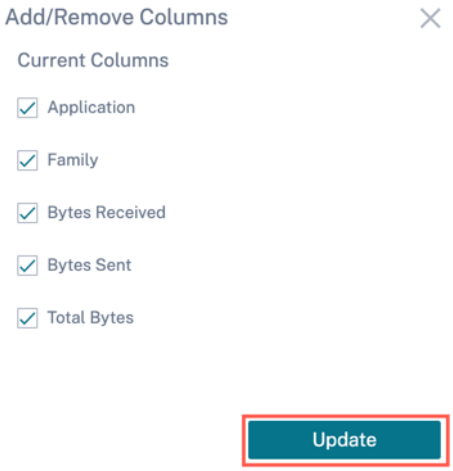
Die Seite „ **App-Statistiken** “bietet unter **Berichte > Echtzeit > App-Statistiken die folgenden statistischen Informationen in Echtzeit**:

- Anwendungen
- App QoS
- QoS-Klassen
- QoS-Regeln
- Regelgruppen

Um einen statistischen Bericht in Echtzeit zu erhalten, wechseln Sie zur erforderlichen Registerkarte (z. B. Anwendungen, QoS-Regel, QoS-Klassen), wählen Sie die Site aus der Dropdown-Liste aus und klicken Sie auf **Neueste Daten abrufen**.



Klicken Sie auf das Pluszeichen (+), wenn Sie der Statistiktabelle eine Spalte hinzufügen oder daraus entfernen möchten, und klicken Sie auf **Aktualisieren**.

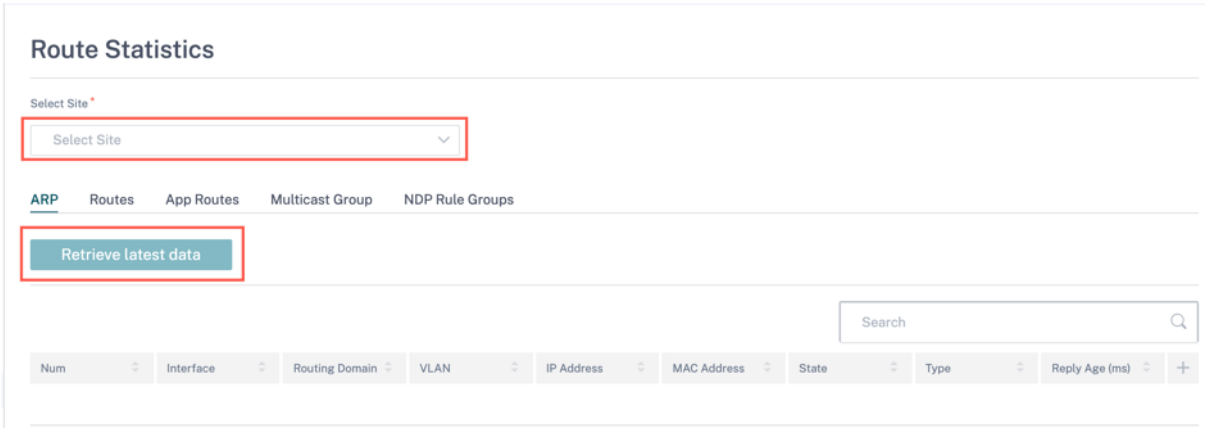


Routenstatistik

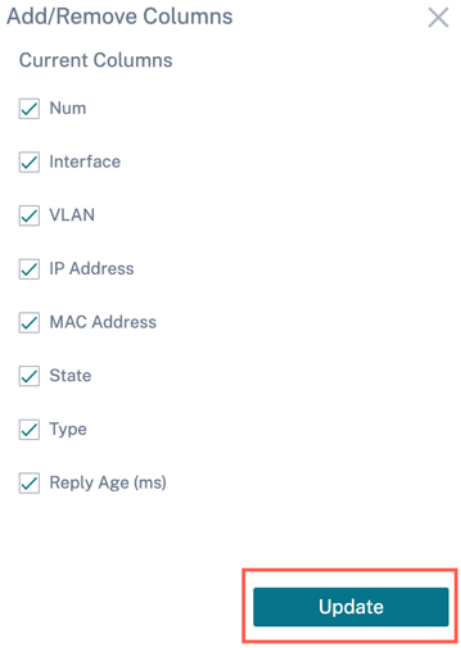
Die Seite „ **Routenstatistik** “bietet unter **Berichte > Echtzeit > Streckenstatistiken die folgenden statistischen Echtzeitinformationen**:

- ARP
- Routen
- Anwendungsrouten
- Beobachtete Protokolle
- Multicastgruppe
- NDP-Regelgruppen

Um einen statistischen Bericht in Echtzeit zu erhalten, wechseln Sie zur gewünschten Registerkarte (z. B. ARP, Routen, Anwendungsrouten), wählen Sie die Site aus der Dropdown-Liste aus und klicken Sie auf **Neueste Daten abrufen**.

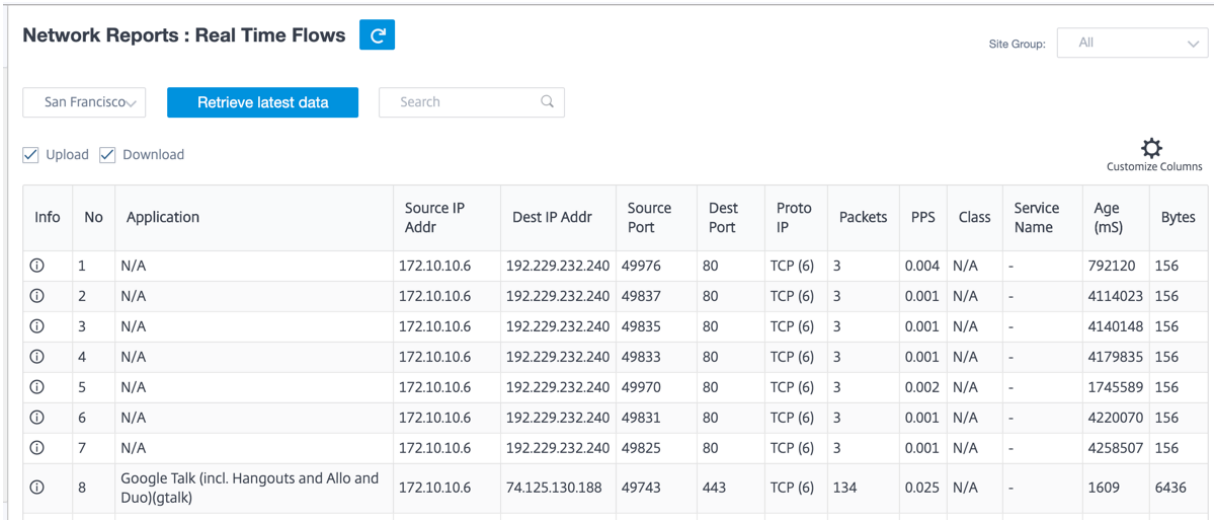


Klicken Sie auf das Pluszeichen (+), wenn Sie der Statistiktabelle eine Spalte hinzufügen oder daraus entfernen möchten, und klicken Sie auf **Aktualisieren**.



Strömungen

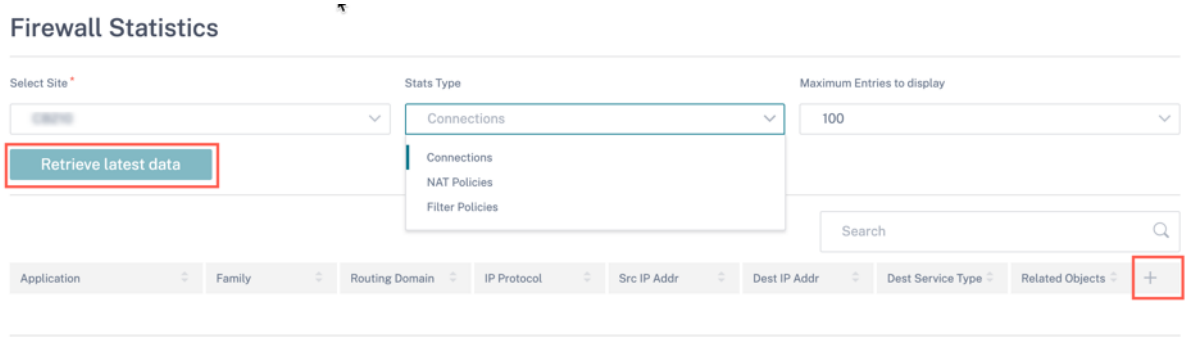
Wählen Sie auf Netzwerkebene die Site aus der Dropdownliste aus, bevor Sie die Statistiken abrufen können. Die **Flows-Funktion** bietet unidirektionale Flussinformationen zu einer bestimmten Sitzung, die durch die Appliance läuft. Dies liefert Informationen über den Zieldiensttyp, in den der Flow fällt, sowie die Informationen, die sich auf den Regel- und Klassentyp sowie den Übertragungsmodus beziehen.



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

Firewall-Statistiken

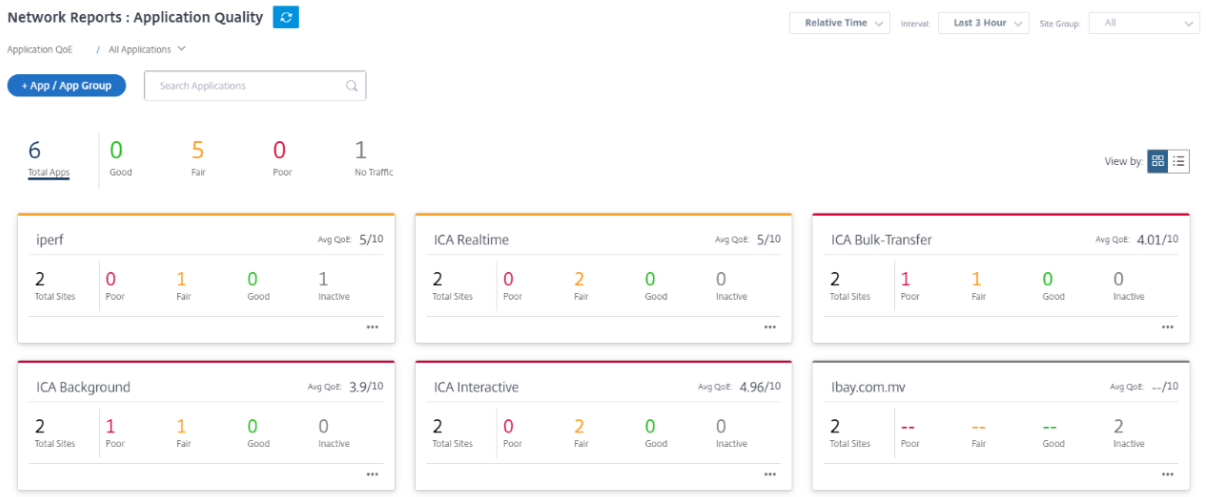
Wählen Sie auf Netzwerkebene die Site aus der Dropdownliste aus, bevor Sie die Statistiken abrufen können. Die **Firewall-Statistik gibt** den Status der Verbindung in Bezug auf eine bestimmte Sitzung basierend auf der konfigurierten Firewallaktion an. Firewall-Verbindungen bieten auch vollständige Details über die Quelle und das Ziel der Verbindung.



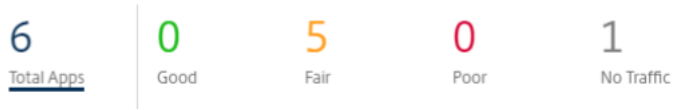
Qualität der Anwendung

Anwendung QoE ist ein Maß für die Qualität der Erfahrung von Anwendungen im SD-WAN-Netzwerk. Es misst die Qualität von Anwendungen, die durch die virtuellen Pfade zwischen zwei SD-WAN-Appliances fließen. Der QoE-Wert der Anwendung ist ein Wert zwischen 0 und 10. Der Wertungsbereich, in den er fällt, bestimmt die Qualität einer Anwendung. Application QoE ermöglicht es Netzwerkadministratoren, die Qualität der Erfahrung von Anwendungen zu überprüfen und proaktive Maßnahmen zu ergreifen, wenn die Qualität unter den akzeptablen Schwellenwert fällt.

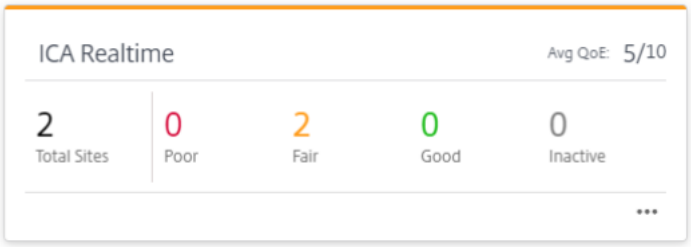
Qualität	Reichweite	Farb-Codierung
Gut	8–10	Grün
Fair	4–8	Orangen
Schlecht	0–4	Rot



Oben im Dashboard zeigt die Gesamtzahl der Anwendungen und die Anzahl der Anwendungen an, die eine gute, faire oder schlechte Anwendungs-QoE im Netzwerk haben. Es zeigt auch die Anzahl der Anwendungen an, die keinen Datenverkehr haben.

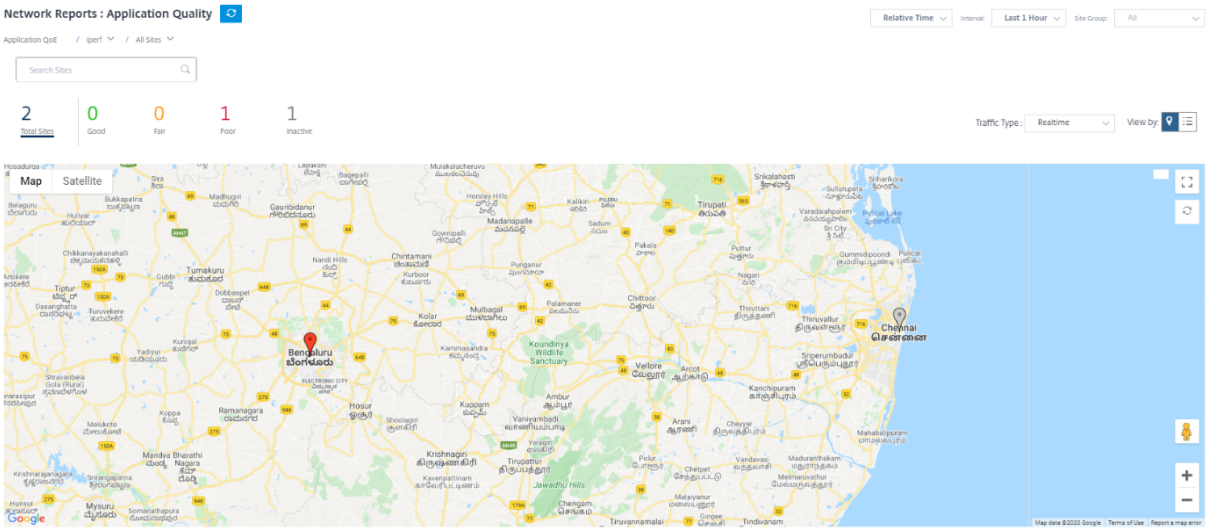


Auf der einzelnen Anwendungskarte wird die Anzahl der Sites angezeigt, die eine schlechte, faire oder gute Anwendungs-QoE für die jeweilige Anwendung aufweisen. Außerdem wird die Anzahl der Sites angezeigt, die die Anwendung nicht aktiv nutzen. Der Avg QoE ist der durchschnittliche QoE-Wert der Anwendung an allen Standorten im Netzwerk.



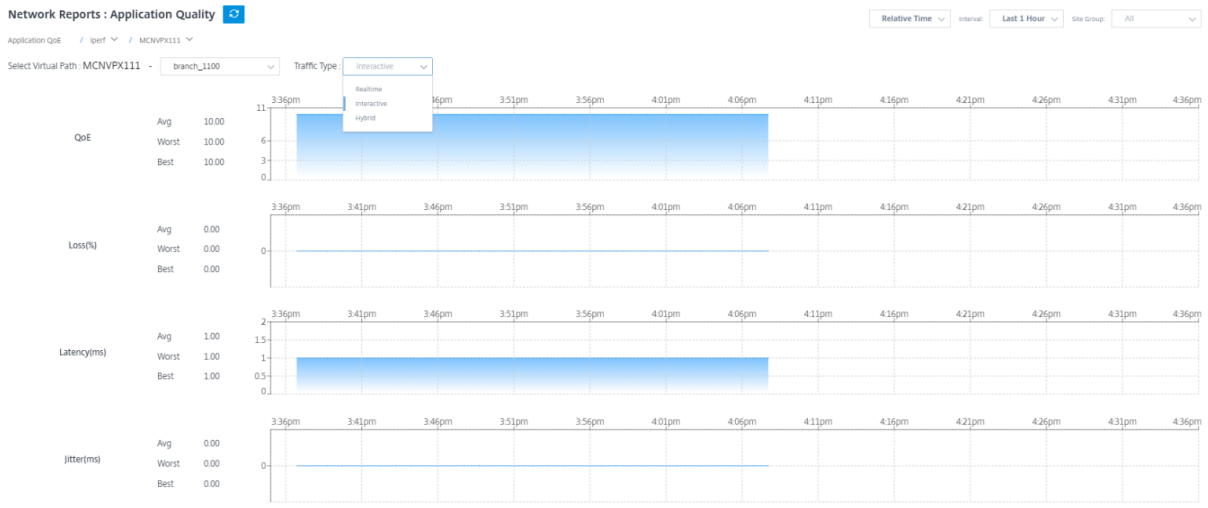
Klicken Sie auf eine einzelne Anwendungskarte, um die Details zur Anzahl der Sites anzuzeigen, die eine gute, faire oder schlechte Anwendungs-QoE für die ausgewählte Anwendung aufweisen. Eine

Kartenansicht aller Sites, auf denen die ausgewählte Anwendung ausgeführt wird, wird angezeigt. Klicken Sie auf eine Site in der Karte, um die Application QoE-Statistiken der verschiedenen virtuellen Pfade auf der Site weiter aufzurufen und anzuzeigen.



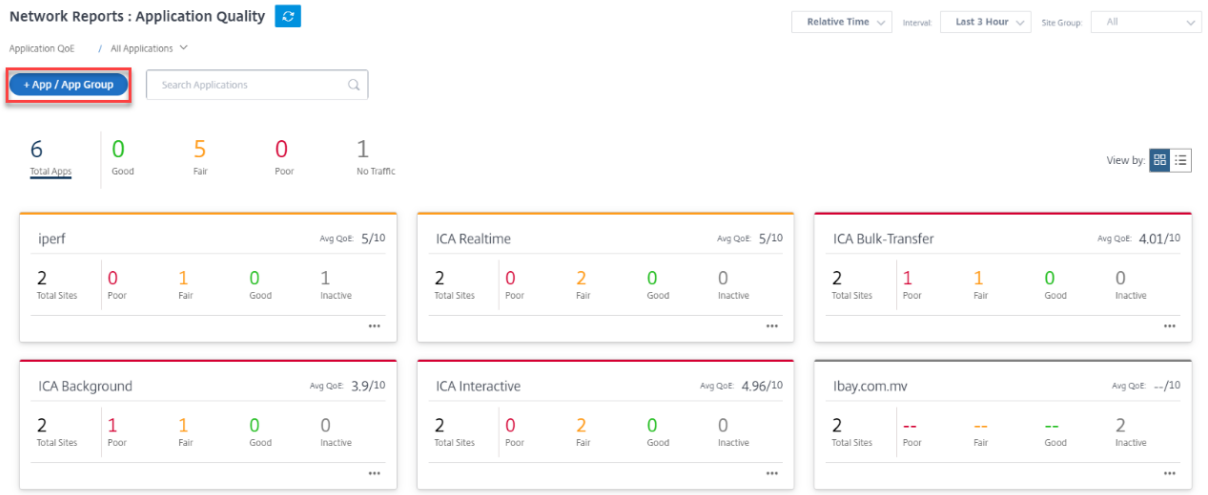
Sie können die folgenden Metriken für Echtzeit-, interaktiven und hybriden Traffic für den ausgewählten Zeitraum anzeigen:

- **QoE**: Der QoE-Score für den Traffic.
- **Verlust**: Der Verlustprozentsatz für den Verkehr.
- **Latenz**: Die Latenz in Millisekunden für den Datenverkehr.
- **Jitter**: Der in Millisekunden beobachtete Jitter für den Verkehr.

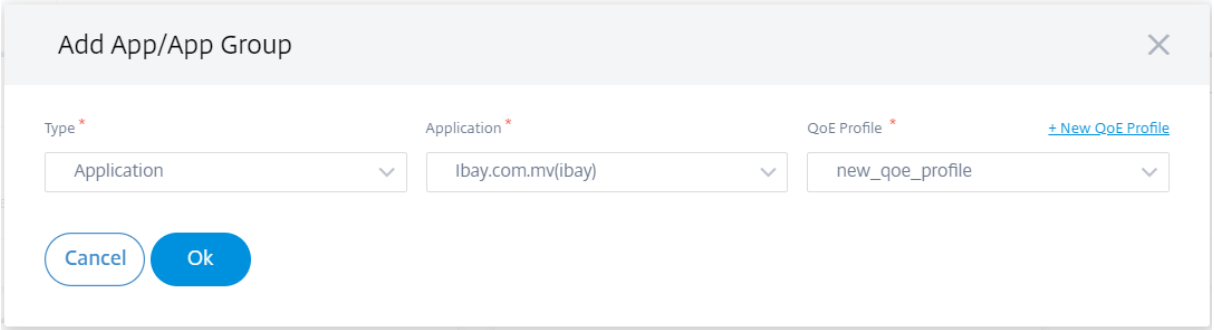


Anwendung QoE-Profile

Klicken Sie auf **+ App/App-Gruppe**, um Anwendungen, benutzerdefinierte Anwendungen oder Anwendungsgruppen den Standard- oder benutzerdefinierten QoE-Profilen zuzuordnen.



Die QoE-Profile definieren den Schwellenwert für Echtzeit-, interaktiven und hybriden Datenverkehr. Die QoE-Schwellenwerte gemäß den QoE-Profilen werden auf die ausgewählte Anwendung oder Anwendungsgruppe angewendet.



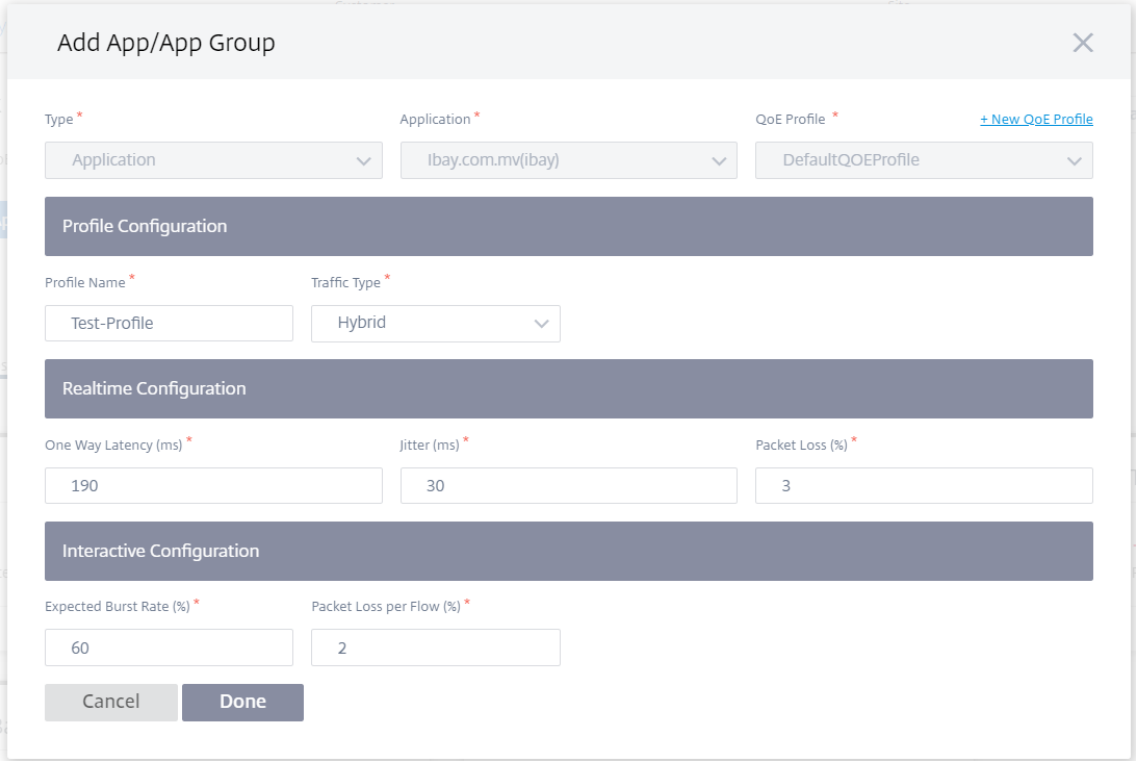
Klicken Sie auf **+ Neues QoE-Profil**, um ein neues QoE-Anwendungsprofil zu erstellen, und geben Sie den Wert für die folgenden Parameter ein:

- **Profilname**: Ein Name zur Identifizierung des Profils, das Schwellenwerte für Echtzeit- und interaktiven Verkehr festlegt.
- **Traffic-Typ**: Wählen Sie die Art des Datenverkehrs —Echtzeit, Interaktiv oder Hybrid. Wenn der Traffic-Typ Hybrid ist, können Sie sowohl Echtzeit- als auch interaktive QoE-Profilschwellenwerte konfigurieren.
- **Echtzeitkonfiguration**: Konfigurieren Sie Schwellenwerte für Datenverkehrsflüsse, die die Echtzeit-QoS-Richtlinie auswählen. Ein Fluss einer Echtzeitanwendung, die die folgenden Schwellenwerte für Latenz, Verlust und Jitter erfüllt, wird als von guter Qualität angesehen.

  - **Einweg-Latenz**: Der Latenzschwellenwert in Millisekunden. Der standardmäßige QoE-Profilwert beträgt 160 ms.
  - **Jitter**: Der Jitter-Schwellenwert in Millisekunden. Der standardmäßige QoE-Profilwert beträgt 30 ms.
  - **Paketverlust**: Der Prozentsatz des Paketverlusts. Der standardmäßige QoE-Profilwert beträgt 2%.

- **Interaktive Konfiguration**: Konfigurieren Sie Schwellenwerte für Datenverkehrsflüsse, die die interaktive QoS-Richtlinie auswählen. Ein Fluss einer interaktiven Anwendung, die den folgenden Schwellenwert für die Burst-Quote und den Paketverlust erfüllt, wird als von guter Qualität angesehen.

  - **Erwartete Burst-Rate**: Der Prozentsatz der erwarteten Burst-Rate. Die Burstrate des Egress muss mindestens dem konfigurierten Prozentsatz der Ingress-Burstrate entsprechen. Der standardmäßige QoE-Profilwert beträgt 60%.
  - **Paketverlust pro Fluss**: Der Prozentsatz des Paketverlusts. Der standardmäßige QoE-Profilwert beträgt 1%.



Die neu hinzugefügte Anwendung wird im Dashboard für Anwendungsqualität angezeigt.

Sie können die Anwendungs-QoE auch in den App- und DNS-Einstellungen definieren und konfigurieren. Weitere Informationen finden Sie unter Anwendungsqualitätsprofile und Konfiguration der Anwendungsqualität.

Site-Berichte

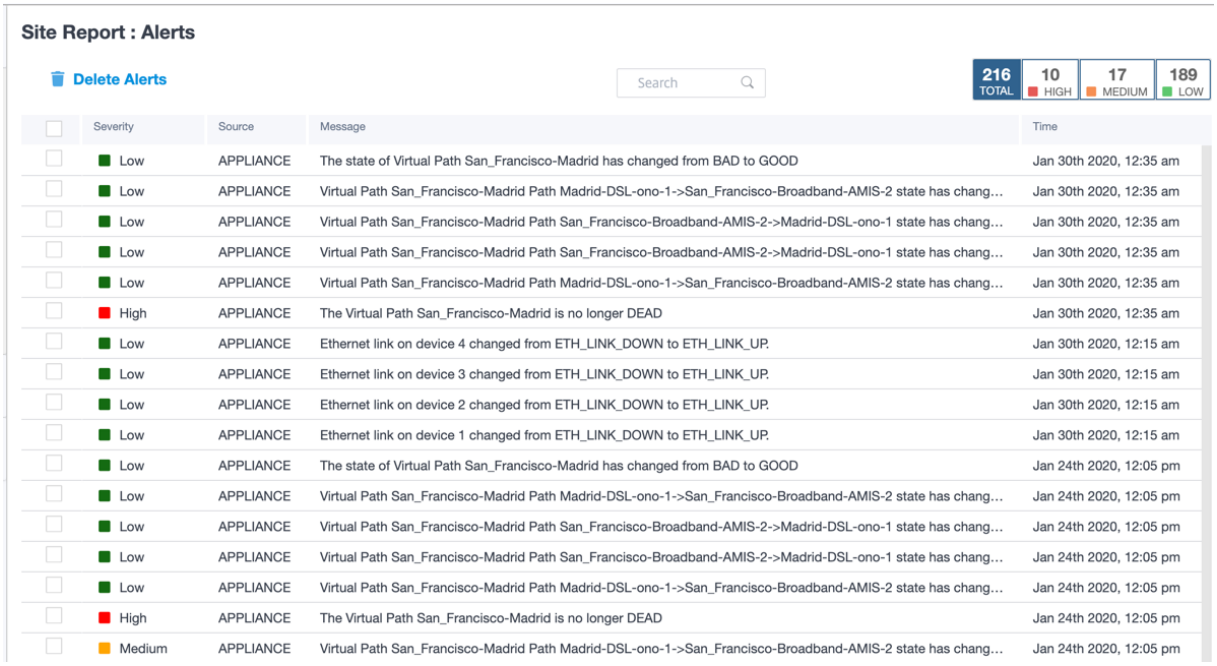
October 21, 2022

Die **Site-Berichte** bieten Einblick in Warnungen auf Standortebene, Nutzungstrends, Qualität, Geräteinformationen und Firewall-Statistiken.

Warnungen

Der Site-Administrator kann einen detaillierten Bericht über alle Ereignisse und Warnungen überprüfen, die auf Standortebene generiert wurden.

Sie umfasst den Schweregrad, den Ort, an dem die Warnung ausgelöst wurde, die Warnmeldung, die Uhrzeit und andere Details.



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

Geeignete Filteroptionen können nach Bedarf verwendet werden, zum Beispiel: Suchen Sie nach allen Warnungen mit hohem Schweregrad am Standort oder nach den Warnungen, die während eines bestimmten Zeitraums aufgetreten sind.

Sie können auch Alarme auswählen und löschen.

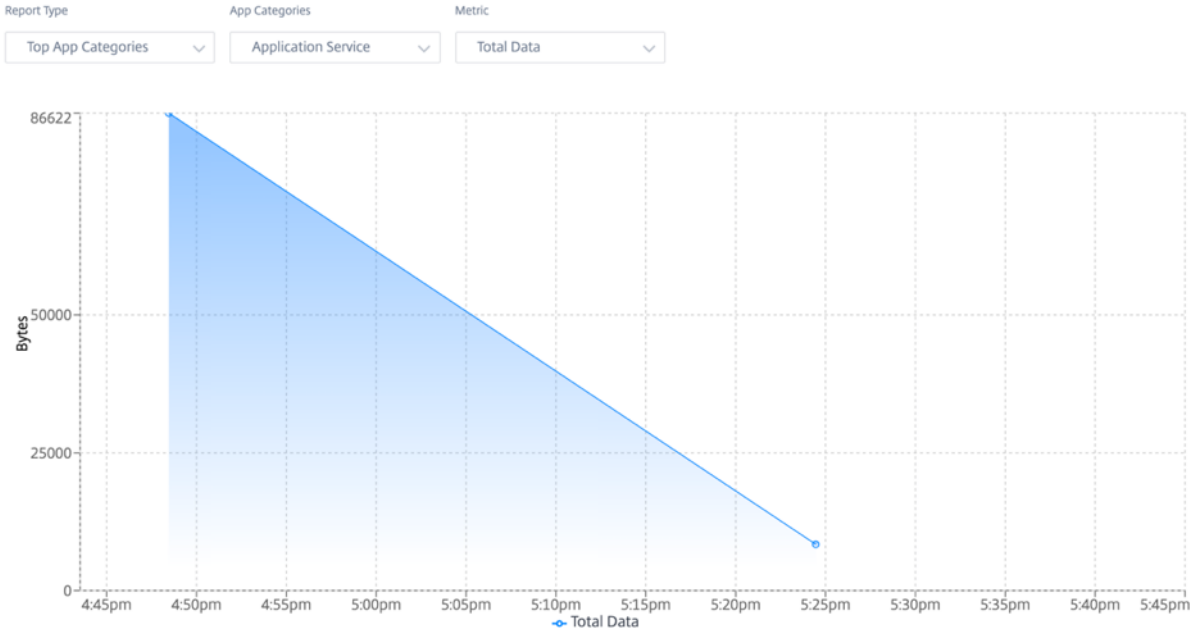
Verwendung

Site-Administratoren können Nutzungstrends wie **Top-Anwendungen, Top-Anwendungskategorien**und **App-Bandbreite** an einer bestimmten Site überprüfen.

Top-Anwendungen und Anwendungskategorien

Das Diagramm „ **Top-Anwendungen“und „Top-Anwendungskategorien** “zeigt die wichtigsten Anwendungen und Top-Anwendungsfamilien, die in der Site häufig verwendet werden. Auf diese Weise können Sie das Datenverbrauchsmuster analysieren und das Bandbreitenlimit für jede Datenklasse innerhalb der Site neu zuweisen.

Sie können auch die Statistiken zur Bandbreitennutzung anzeigen. Die Bandbreitenstatistiken werden für das ausgewählte Zeitintervall gesammelt. Sie können den statistischen Bericht basierend auf **Berichtstyp, Apps- oder App-Kategorien** und **Metriken**filtern.

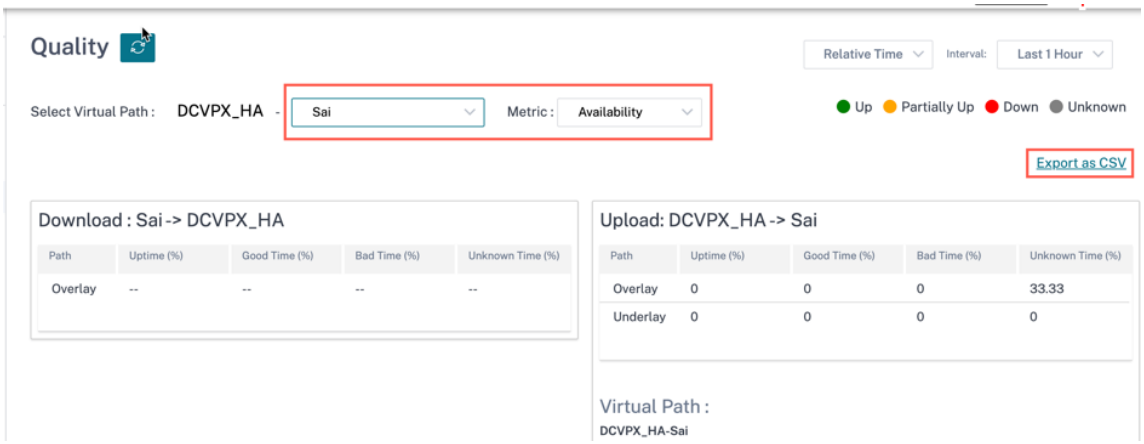


- **Berichtstyp:** Wählen Sie **Top-App- oder App-Kategorien** aus der Liste aus.
- **Apps/App-Kategorien:** Wählen Sie die wichtigsten Anwendungen oder Kategorien (z. B. Netzwerkdienst) aus der Liste aus.
- **Metrik:** Wählen Sie die Bandbreitenmetrik (z. B. Gesamtdaten, Eingehende Daten, Gesamtbandbreite) aus der Liste aus.

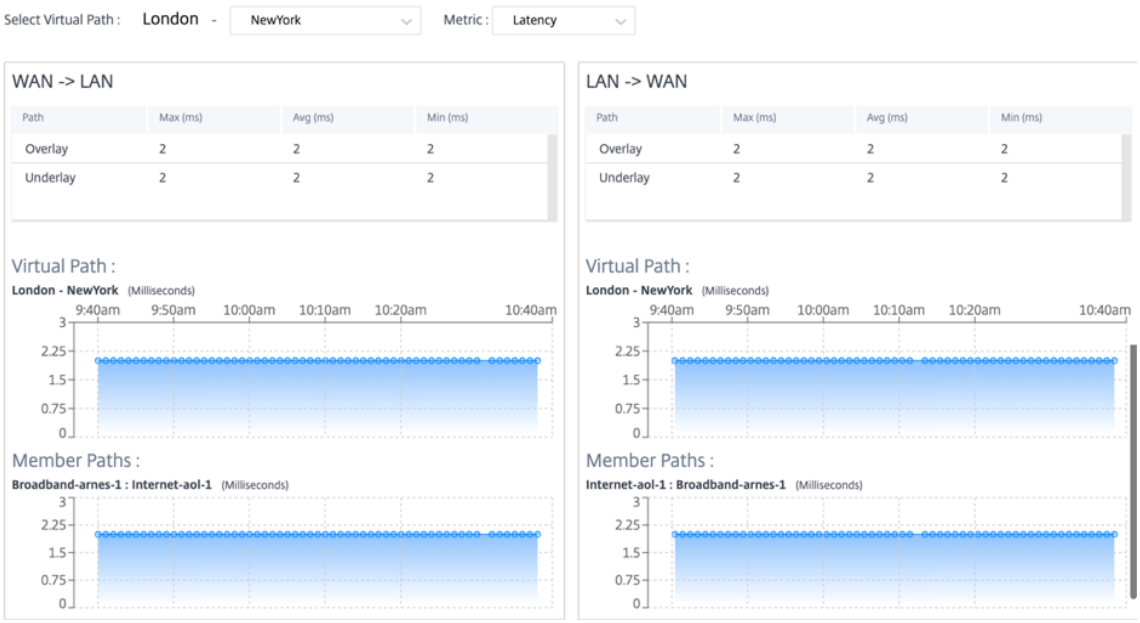
Qualität

Site-Administratoren können die Qualitätsberichte verwenden, um die Quality of Experience (QoE) am Standort für jede QoS-Metrik wie Verfügbarkeit, Verlust, Latenz und Jitter zu analysieren. Die Qualitätsmetrik wird sowohl für die virtuellen Overlay-Pfade als auch für die zugrunde liegenden Mitgliedspfade angezeigt.

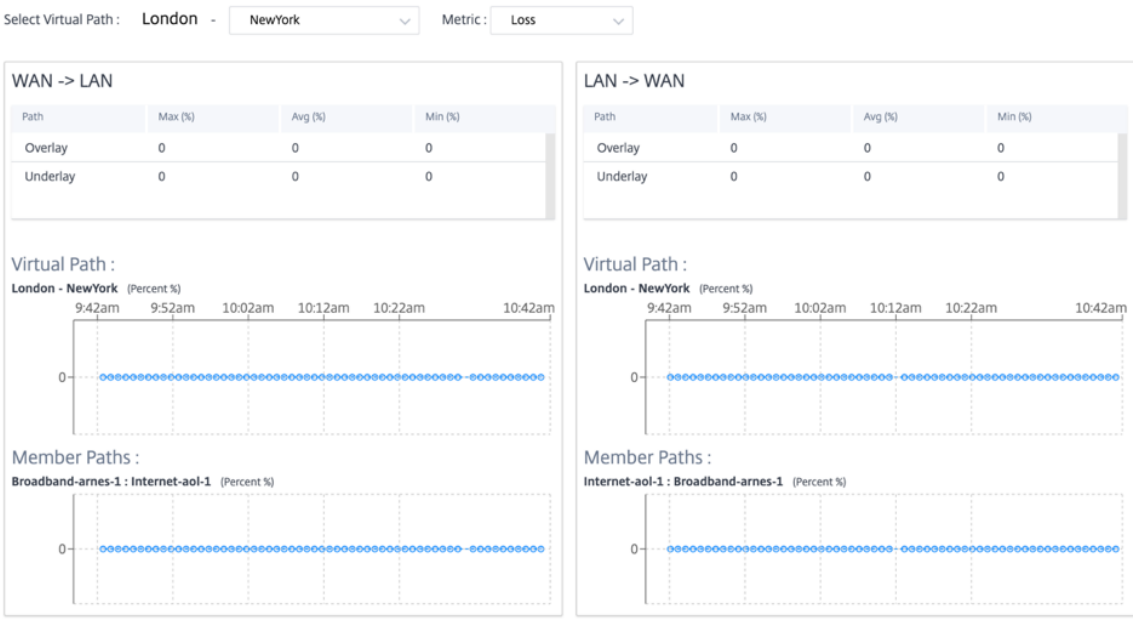
- **Verfügbarkeit**



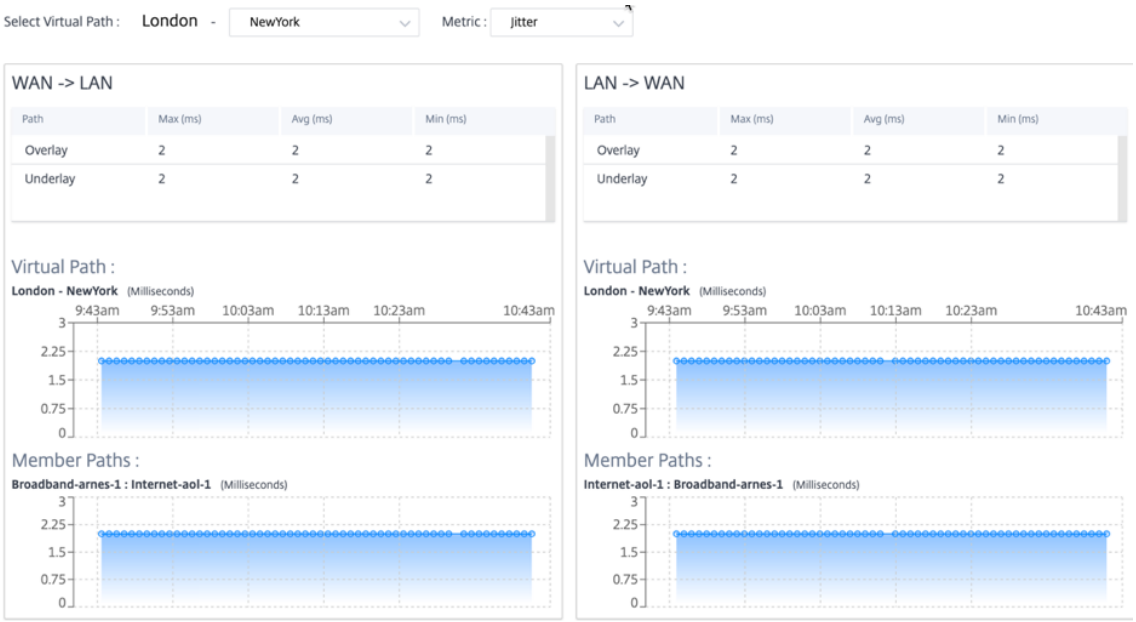
- **Latenz**



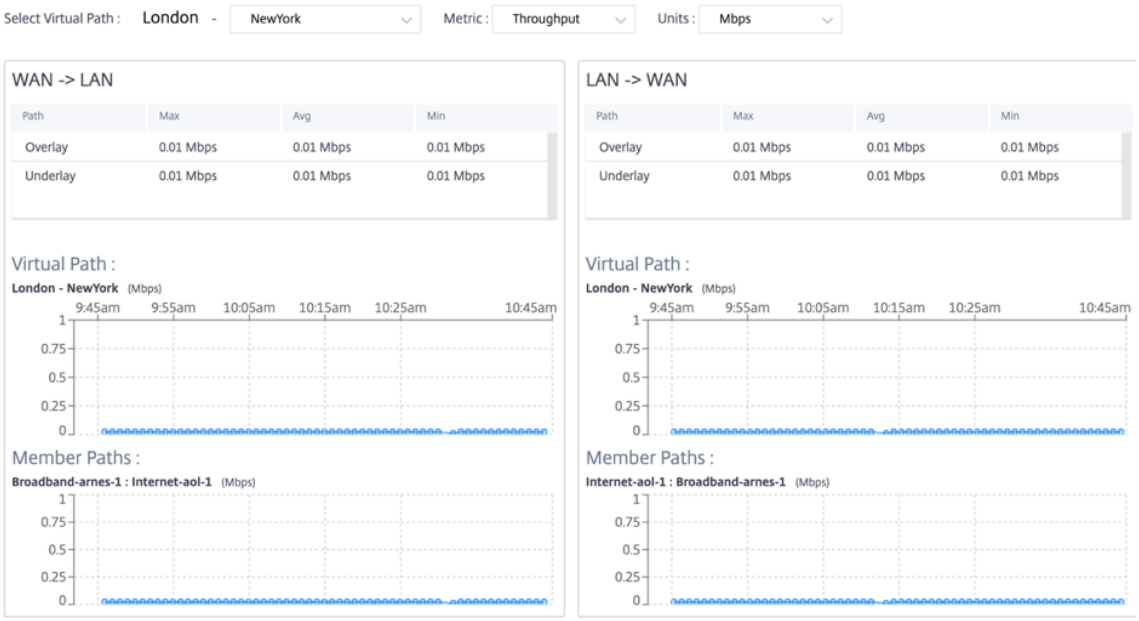
- **Verlust**



- **Jitter**



- **Durchsatz**

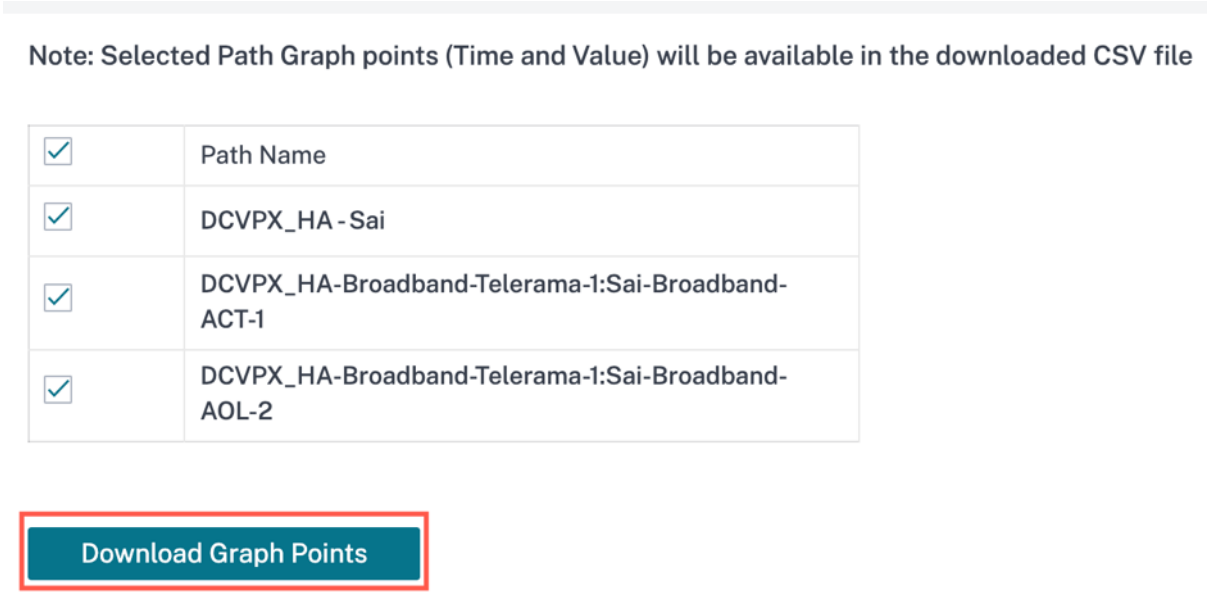


Als CSV exportieren

Mit der Funktion **Als CSV exportieren** können Sie die Pfaddiagrammpunkte (virtueller/Mitgliedspfad) für jede Zeitreihe (stündlich, wöchentlich usw.) als Excel-Datei mit kommagetrennten Werten (CSV) herunterladen und alle eindeutigen Datenpunkte für einen bestimmten Standortbericht darstellen.

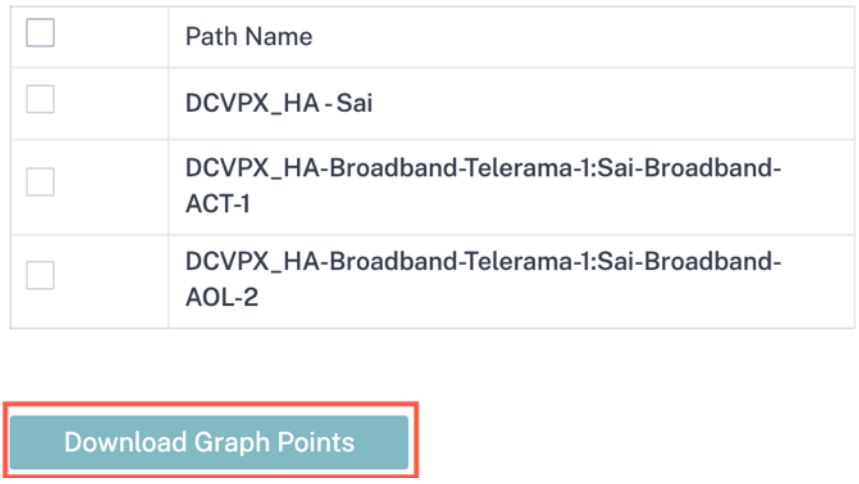
Um das Pfaddiagramm als CSV herunterzuladen/zu exportieren, navigieren Sie zu **Berichte** > **Qualität** auf Standortebene. Wählen Sie die Site und Metrik aus der Dropdownliste aus und klicken Sie auf den Link **Als CSV exportieren** .

Wählen Sie den Pfad aus, für den Sie die Daten abrufen möchten, und klicken Sie auf **Diagrammpunkte herunterladen**.

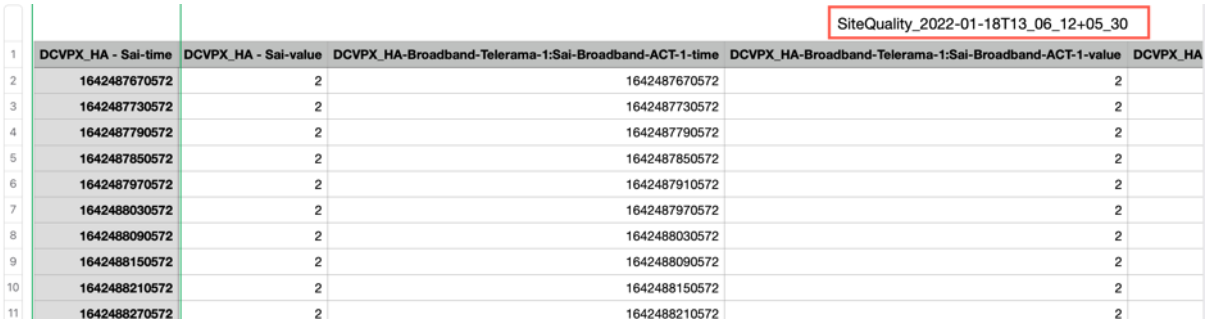


Standardmäßig sind alle Pfadkontrollfelder automatisch aktiviert. Sie können es nach Bedarf ändern.

> **Hinweis:**
>
> Wenn keiner der Pfade ausgewählt ist, bleibt die Schaltfläche **Diagrammpunkte herunterladen** deaktiviert.



Die Namenskonvention der heruntergeladenen CSV-Datei lautet **SiteQuality**, gefolgt von einem Zeitstempel des Downloads. Sie können jeden Pfad mit einem Paar von Zeit und Wert zusammen mit einer eindeutigen Kennung anzeigen. Sie können die Zeit in Millisekunden und den Wert als Einheit sehen.



			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	

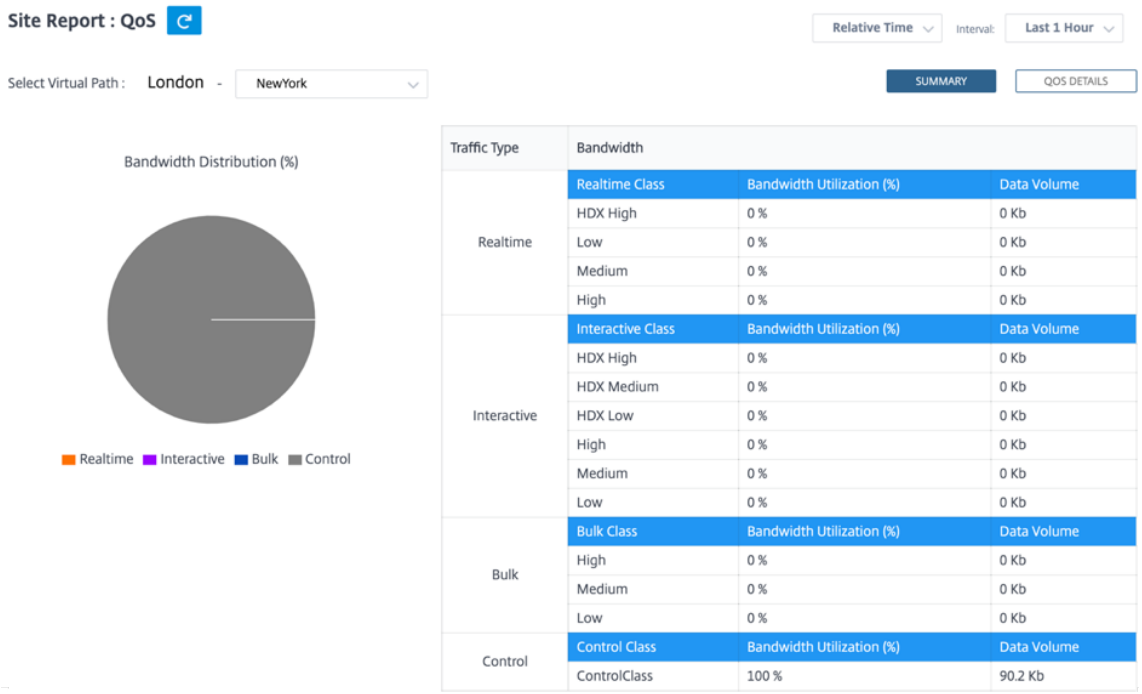
Basierend auf der folgenden Metrikauswahl können Sie sehen, dass in der CSV-Datei verschiedene Werte generiert werden:

- **Verlust:** Wert wird in% angezeigt.
- **Latenz und Jitter:** Wert wird in Millisekunden angezeigt.
- **Durchsatz:** Der Wert wird in Kbit/s angezeigt.
- **Verfügbarkeit:** Zeigt den Pfad nach oben, teilweise nach oben, unten und unbekannte Zeit an.
  - Wenn der Wert 4 ist, befindet sich der Pfad im Status Up.
  - Wenn der Wert 3 ist, befindet sich der Pfad teilweise im Status Up.
  - Wenn der Wert kleiner als 3 ist, befindet sich der Pfad im Status Bad/down.

Servicequalität

Quality of Service (QoS) verwaltet den Datenverkehr, um Paketverlust, Latenz und Jitter im Netzwerk zu reduzieren. Weitere Informationen finden Sie unter Servicequalität. Es gibt zwei Möglichkeiten, den Quality of Service (QoS) -Bericht anzuzeigen:

- **Zusammenfassungsansicht:** Die Zusammenfassungsansicht bietet einen Überblick über den Bandbreitenverbrauch über alle Arten von Datenverkehr hinweg - Echtzeit, interaktiv, Massen-zugriff und Steuerung im gesamten Netzwerk und pro Standort.

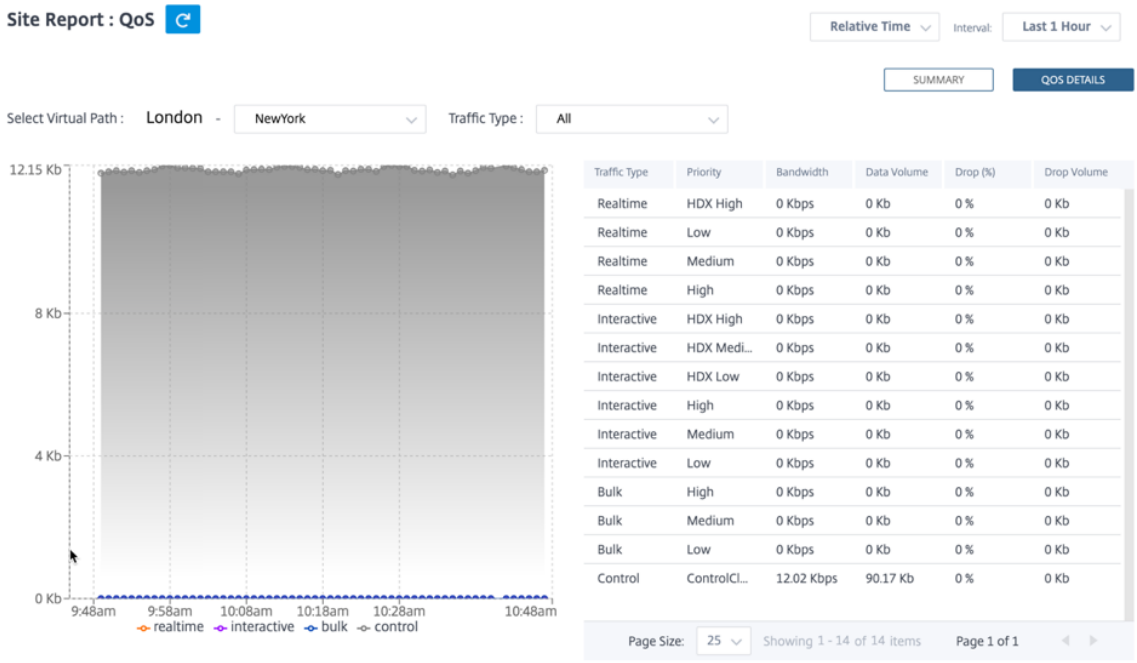


Traffic Type	Bandwidth		
Realtime	Realtime Class	Bandwidth Utilization (%)	Data Volume
	HDX High	0 %	0 Kb
	Low	0 %	0 Kb
	Medium	0 %	0 Kb
	High	0 %	0 Kb
Interactive	Interactive Class	Bandwidth Utilization (%)	Data Volume
	HDX High	0 %	0 Kb
	HDX Medium	0 %	0 Kb
	HDX Low	0 %	0 Kb
	High	0 %	0 Kb
	Medium	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

  - **Echtzeit:** Wird für zeitkritischen Datenverkehr mit geringer Latenz, geringer Bandbreite verwendet. Echtzeitanwendungen sind zeitkritisch, benötigen aber keine wirklich hohe Bandbreite (z. B. Voice over IP). Echtzeitanwendungen reagieren empfindlich auf Latenz und Jitter, können aber einige Verluste tolerieren.
  - **Interaktiv:** Wird für interaktiven Datenverkehr mit niedrigen bis mittleren Latenzanforderungen und niedrigen bis mittleren Bandbreitenanforderungen verwendet. Interaktive Anwendungen beinhalten menschliche Eingaben in Form von Mausklicks oder Cursorbewegungen. Die Interaktion erfolgt in der Regel zwischen einem Client und einem Server. Die Kommunikation benötigt möglicherweise keine hohe Bandbreite, ist aber empfindlich gegenüber Verlust und Latenz. Server zu Client benötigt jedoch eine hohe Bandbreite, um grafische Informationen zu übertragen, die möglicherweise nicht verlustempfindlich sind.
  - **Bulk:** Wird für Datenverkehr mit hoher Bandbreite verwendet, der hohe Latenz tolerieren kann. Anwendungen, die Dateiübertragung verarbeiten und eine hohe Bandbreite benötigen, werden als Massenklasse kategorisiert. Diese Anwendungen beinhalten wenig menschliche Eingriffe und werden meist von den Systemen selbst behandelt.
  - **Steuerung:** Wird verwendet, um Steuerpakete zu übertragen, die Informationen zu Routing, Scheduling und Verbindungsstatistiken enthalten.

- **Detailansicht:** Die Detailansicht erfasst Trends in Bezug auf Bandbreitenverbrauch, Verkehrsaufkommen, verworfene Pakete usw. Für jede QoS-Klasse, die einem virtuellen Overlay-Pfad zugeordnet ist. Sie können QoS-Statistiken basierend auf dem virtuellen Pfad

zwischen zwei Sites anzeigen.



Historische Statistik

Für jede Site können Sie die Statistiken als Diagramme für die folgenden Netzwerkparameter anzeigen:

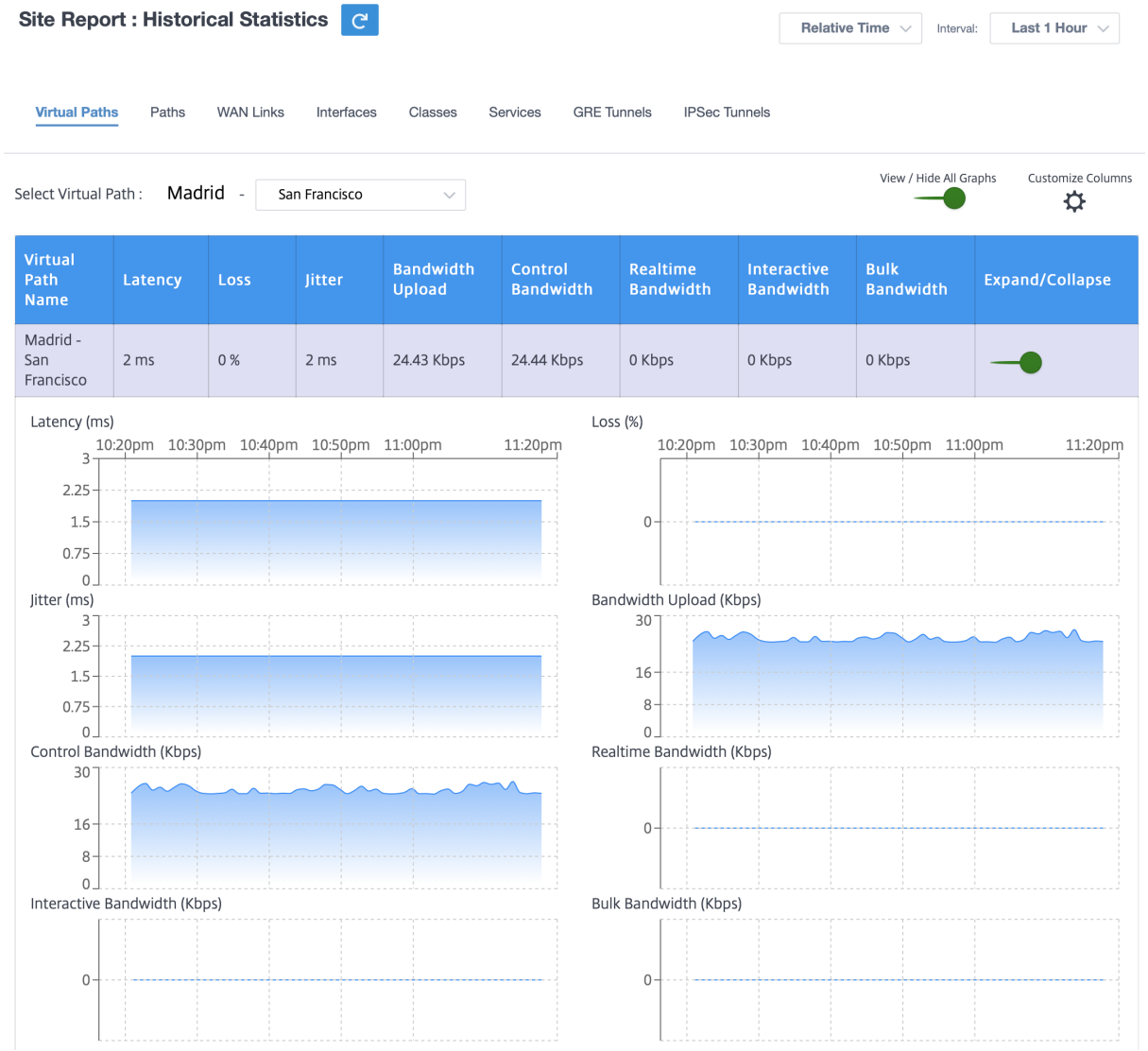
- Virtuelle Pfade
- Pfade
- WAN-Links
- Schnittstellen
- Klassen
- Services
- GRE Tunnel
- IPsec-Tunnel

Die Statistiken werden als Grafiken gesammelt. Diese Diagramme werden als Zeitleiste im Vergleich zur Nutzung dargestellt, sodass Sie die Nutzungstrends verschiedener Netzwerkobjekteigenschaften verstehen können. Sie können Diagramme für netzwerkweite Anwendungsstatistiken anzeigen.

Sie können die Grafiken anzeigen oder ausblenden und die Spalten nach Bedarf anpassen.

Virtuelle Pfade

Um die Statistiken zu **virtuellen Pfaden** anzuzeigen, navigieren Sie zur Registerkarte **Berichte > Statistiken > Virtuelle Pfade** .



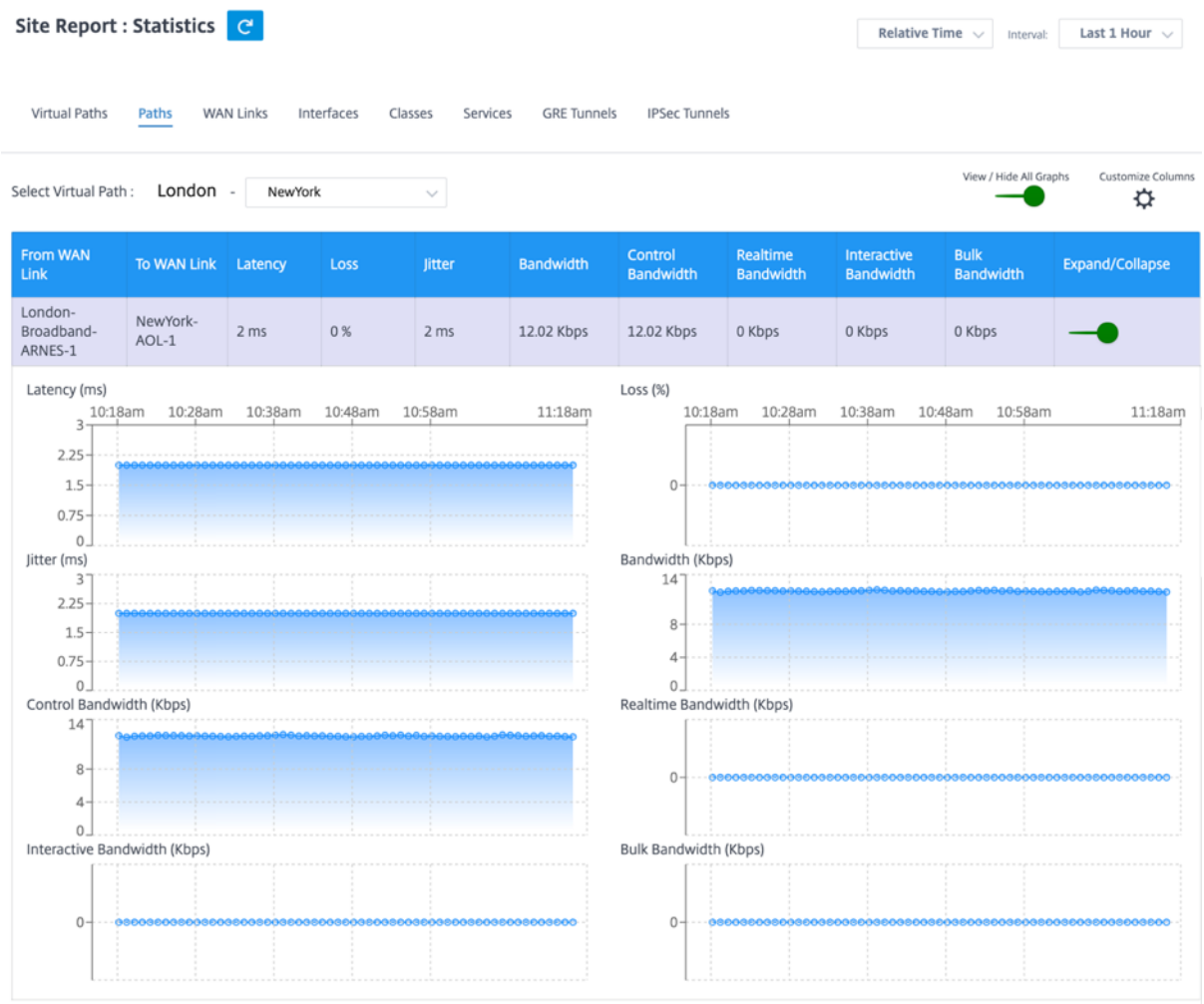
Sie können die folgenden Metriken anzeigen:

- **Name des virtuellen Pfads**: Der Name des virtuellen Pfads.
- **Latenz**: Die Latenz in Millisekunden für Echtzeitverkehr.
- **Verlust**: Prozentsatz der verlorenen Pakete.
- **Jitter**: Variation der Verzögerung empfangener Pakete in Millisekunden.
- **Bandbreiteneingang**: **Ingress-Bandbreitennutzung (LAN > WAN)** für den ausgewählten Zeitraum.
- **Bandbreite steuern: Bandbreite**, die für die Übertragung von Steuerpaketen verwendet wird, die Informationen zu Routing, Planung und Verbindungsstatistiken enthalten.

- **Echtzeitbandbreite**: Bandbreite, die von Anwendungen verbraucht wird, die zum Echtzeit-Klasstyp in der SD-WAN-Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz ab. Ein verzögertes Paket ist schlechter als ein verlorenes Paket (z. B. VoIP, Skype for Business).
- **Interaktive Bandbreite**: Bandbreite, die von Anwendungen verbraucht wird, die zum interaktiven Klassentyp in der SD-WAN-Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz und dem Paketverlust ab (z. B. XenDesktop, XenApp).
- **Massenbandbreite**: Bandbreite, die von Anwendungen verbraucht wird, die zum Bulk-Klasstyp in der SD-WAN-Konfiguration gehören. Diese Anwendungen beinhalten wenig menschliches Eingreifen und werden meist von den Systemen selbst gehandhabt (zum Beispiel FTP, Backup-Operationen).
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

Pfade

Um die **Pfadstatistik** anzuzeigen, navigieren Sie zur Registerkarte **Berichte > Statistiken > Pfade** .



Sie können die folgenden Metriken anzeigen:

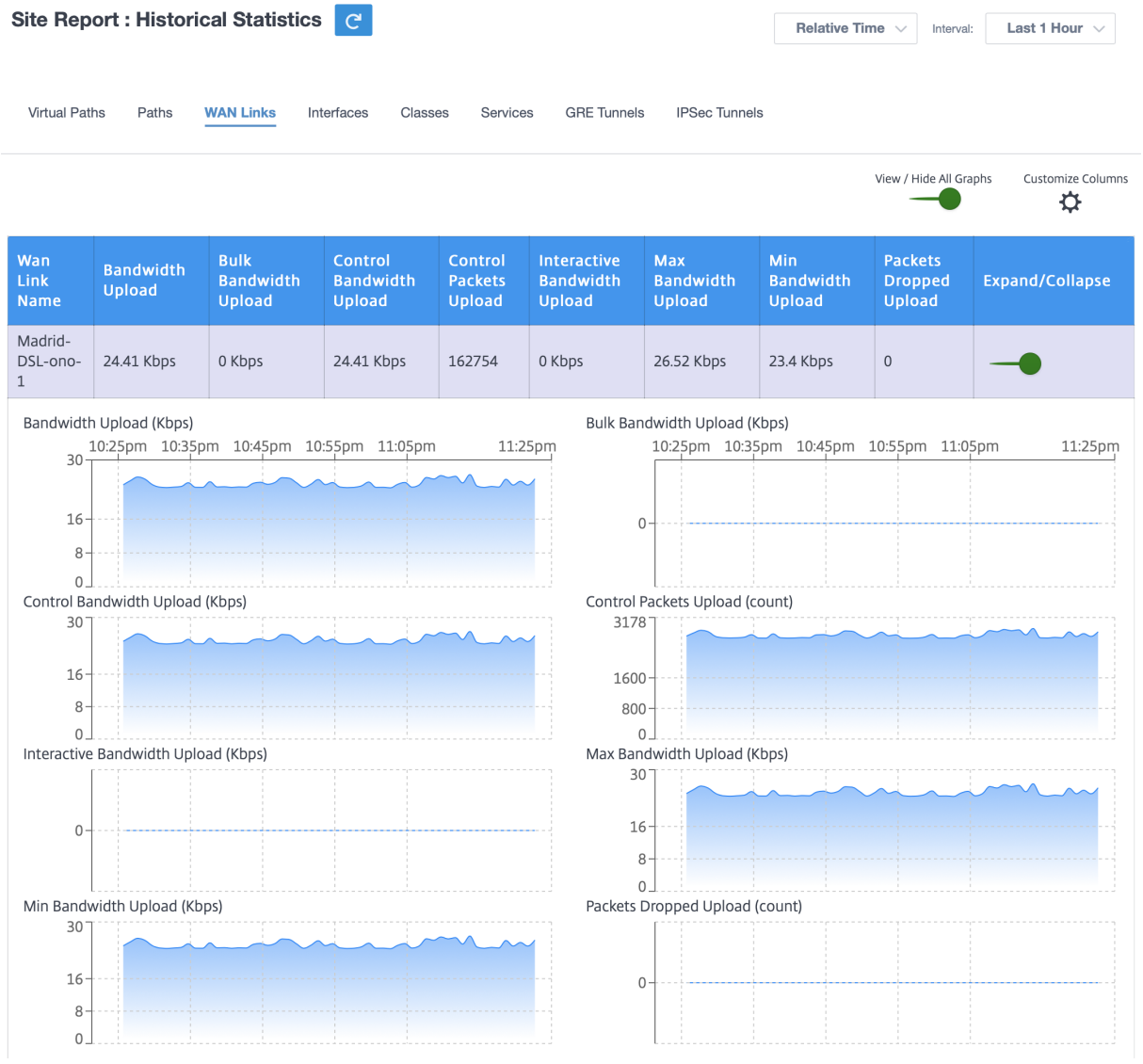
- **Von WAN Link**: Der Quell-WAN-Link.
- **Zum WAN-Link**: Die WAN-Zielverbindung.
- **Latenz**: Die Latenz in Millisekunden für Echtzeitverkehr.
- **Verlust**: Prozentsatz der verlorenen Pakete.
- **Jitter**: Variation der Verzögerung empfangener Pakete in Millisekunden.
- **Bandbreite**: Gesamtbandbreite, die von allen Pakettypen verbraucht wird. Bandbreite= Bandbreite steuern + Echtzeitbandbreite + Interaktive Bandbreite + Bulk-Bandbreite.
- **Bandbreite steuern: Bandbreite**, die für die Übertragung von Steuerpaketen verwendet wird, die Informationen zu Routing, Planung und Verbindungsstatistiken enthalten.
- **Echtzeitbandbreite**: Bandbreite, die von Anwendungen verbraucht wird, die zum Echtzeit-Klasstyp in der SD-WAN-Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz ab. Ein verzögertes Paket ist schlechter als ein verlorenes Paket (z. B. VoIP, Skype for Business).
- **Interaktive Bandbreite**: Bandbreite, die von Anwendungen verbraucht wird, die zum interak-

tiven Klassentyp in der SD-WAN-Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz und dem Paketverlust ab (z. B. XenDesktop, XenApp).

- **Massenbandbreite**: Bandbreite, die von Anwendungen verbraucht wird, die zum Bulk-Klasstyp in der SD-WAN-Konfiguration gehören. Diese Anwendungen beinhalten wenig menschliches Eingreifen und werden meist von den Systemen selbst gehandhabt (zum Beispiel FTP, Backup-Operationen).
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

WAN-Links

Um die Statistiken auf **WAN-Link-Ebene** anzuzeigen, navigieren Sie zur Registerkarte **Berichte > Statistiken > WAN-Links** .



Sie können die folgenden Metriken anzeigen:

- **WAN-Link-Name**: Der Pfadname.
- **Bandbreiteneingang**: **Ingress-Bandbreitennutzung (LAN > WAN)** für den ausgewählten Zeitraum.
- **Massenbandbreiteneingang**: **Eingangsbandbreite (LAN > WAN) des virtuellen Pfads**, die vom Massenverkehr für den ausgewählten Zeitraum verwendet wird.
- **Bandbreiteneingang steuern**: **Eingangsbandbreite (LAN > WAN) des virtuellen Pfads**, die vom Kontrolldatenverkehr für den ausgewählten Zeitraum verwendet wird.
- **Control Packet Ingress**: **Eingehende (LAN > WAN) Virtual Path Control-Pakete** für den ausgewählten Zeitraum.
- **Interaktiver Bandbreiteneintrag**: **Eingangsbandbreite (LAN > WAN) des virtuellen Pfads**, die vom interaktiven Datenverkehr für den ausgewählten Zeitraum verwendet wird.
- **Max. Bandbreiteneintritt**: **Maximale Eingangsbandbreite (LAN > WAN)**, die in einer Minute für den ausgewählten Zeitraum verwendet wird.
- **Min. Bandbreiteneintritt**: **Minimale Eingangsbandbreite (LAN > WAN)**, die in einer Minute für den ausgewählten Zeitraum verwendet wird.
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

Schnittstellen

Der Statistikbericht der Schnittstellen hilft Ihnen bei der Fehlersuche, um schnell festzustellen, ob einer der Ports ausgefallen ist. Sie können auch die übertragene und empfangene Bandbreite oder Paketdetails an jedem Port anzeigen. Sie können auch die Anzahl der Fehler anzeigen, die während eines bestimmten Zeitraums auf diesen Schnittstellen aufgetreten sind.

Um **Schnittstellenstatistiken** anzuzeigen, navigieren Sie zur Registerkarte **Berichte > Statistiken > Schnittstellen** .

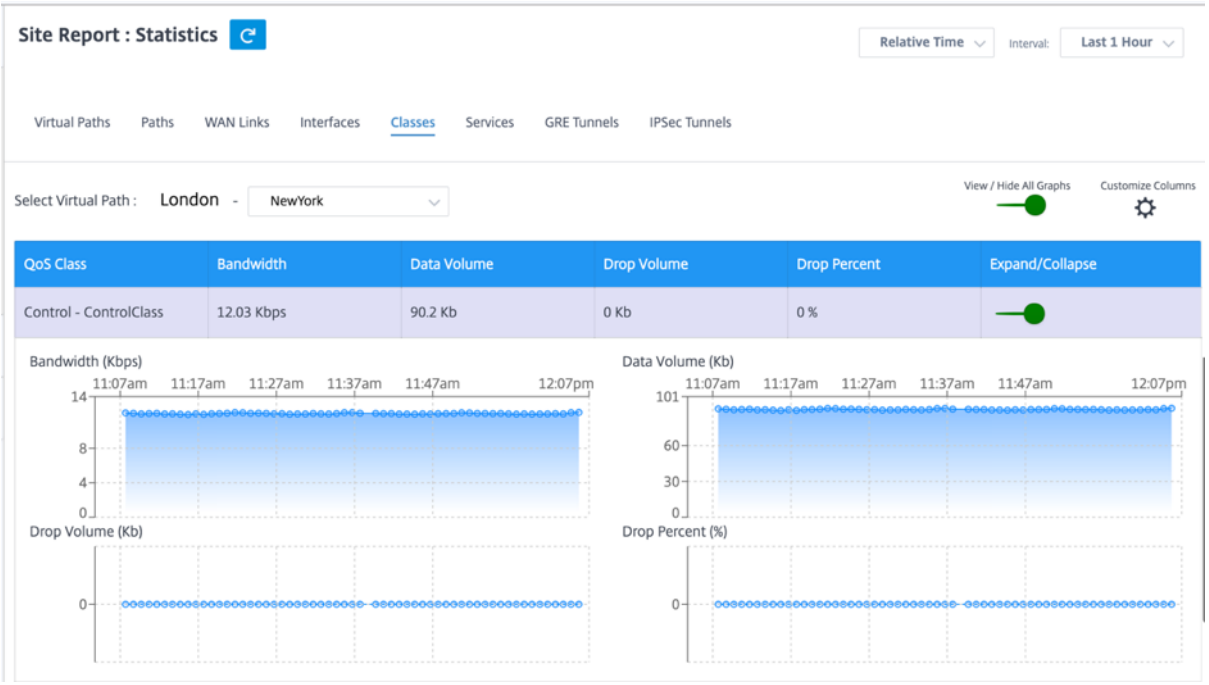
Sie können die folgenden Metriken anzeigen:

- **Schnittstellenname**: Der Name der Ethernet-Schnittstelle.
- **Tx Bandbreite**: Übertragene Bandbreite.
- **Rx-Bandbreite**: Bandbreite erhalten.
- **Fehler**: Anzahl der während des ausgewählten Zeitraums beobachteten Fehler.
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

Klassen

Die virtuellen Dienste können bestimmten QoS-Klassen zugewiesen werden, und unterschiedliche Bandbreitenbeschränkungen können auf verschiedene Klassen angewendet werden.

Um **Klassenstatistiken** anzuzeigen, navigieren Sie zur Registerkarte **Berichte > Statistiken > Klassen** .



Sie können die folgenden Metriken anzeigen:

- **QoS-Klasse**: Der Klassenname.
- **Bandbreite**: Übertragene Bandbreite.
- **Datenvolumen**: Gesendete Daten in Kbps.
- **Drop-Volume**: Prozentsatz der verworfenen Daten.
- **Prozentualer Rückgang**: Prozentsatz der verlorenen Daten.
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

Services

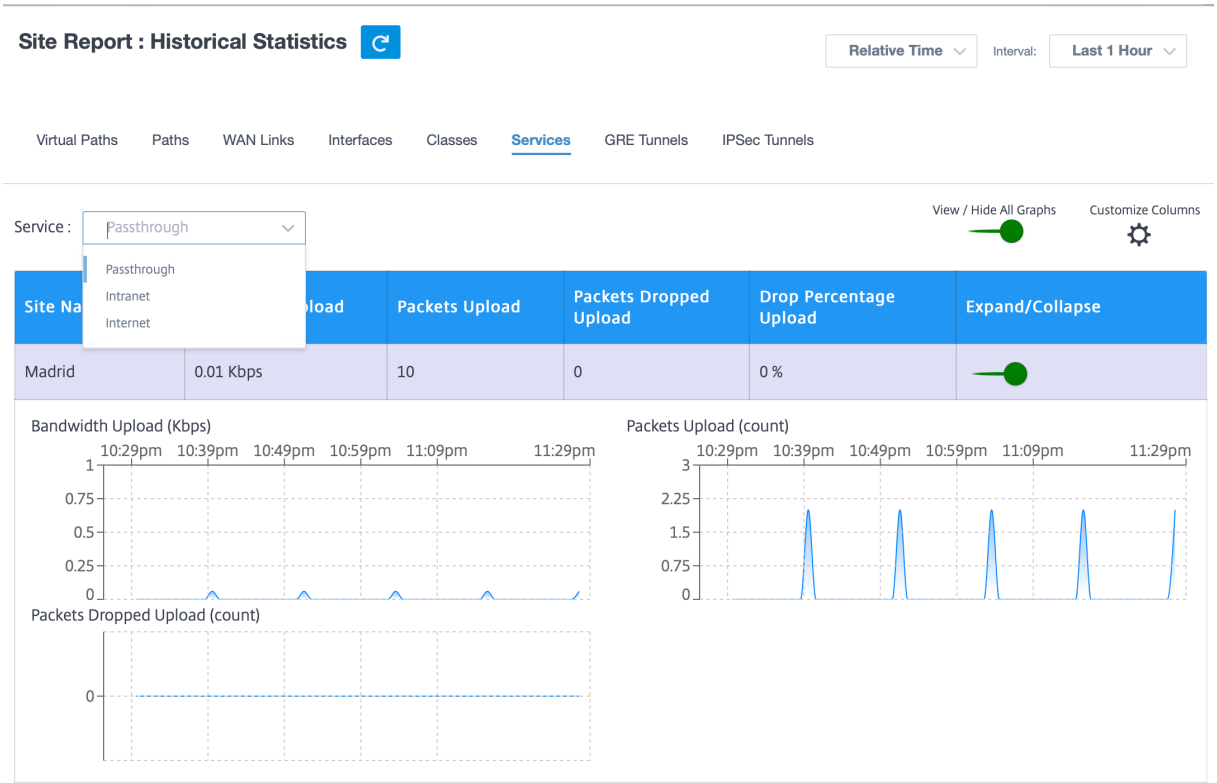
Um die **Servicestatistiken** anzuzeigen, navigieren Sie zur Registerkarte **Berichte > Statistiken > Dienste** .

Wählen Sie den Diensttyp aus der Liste aus. Die folgenden Optionen stehen zur Auswahl:

- **Passthrough** —Dieser Dienst verwaltet Datenverkehr, der vom SD-WAN nicht abgefangen, verzögert, geformt oder geändert wird. Der an den Passthrough-Dienst gerichtete Datenverkehr umfasst Broadcasts, ARPs und anderen Nicht-IPv4-Verkehr sowie Datenverkehr im lokalen Subnetz der Virtual WAN Appliance, konfigurierten Subnetzen oder Regeln, die vom Netzwerkadministrator angewendet werden. Dieser Verkehr wird vom SD-WAN nicht verzögert, geformt oder verändert. Daher müssen Sie sicherstellen, dass Passthrough-Datenverkehr keine

erheblichen Ressourcen auf den WAN-Verbindungen verbraucht, die die SD-WAN-Appliance für andere Dienste konfiguriert ist.

- **Intranet** —Dieser Dienst verwaltet Enterprise Intranet-Verkehr, der nicht für die Übertragung über einen virtuellen Pfad definiert wurde. Wie beim Internetverkehr bleibt er ungekapselt, und das SD-WAN verwaltet die Bandbreite, indem dieser Datenverkehr im Verhältnis zu anderen Diensttypen während der Staus begrenzt wird. Unter bestimmten Bedingungen und wenn für Intranet-Fallback auf dem virtuellen Pfad konfiguriert, kann Datenverkehr, der normalerweise mit einem virtuellen Pfad übertragen wird, stattdessen als Intranet-Verkehr behandelt werden, um die Netzwerkzuverlässigkeit aufrechtzuerhalten.
- **Internet** —Dieser Dienst verwaltet den Verkehr zwischen einer Enterprise-Site und Websites im öffentlichen Internet. Verkehr dieser Art ist nicht gekapselt. In Zeiten der Überlastung verwaltet das SD-WAN aktiv die Bandbreite, indem es den Internetverkehr relativ zum virtuellen Pfad und den Intranet-Verkehr gemäß der vom Administrator festgelegten SD-WAN-Konfiguration begrenzt.



Sie können die folgenden Metriken anzeigen:

- **Site-Name**: Der Site-Name.
- **Bandbreiteneingang**: **Ingress-Bandbreitennutzung (LAN > WAN)** für den ausgewählten Zeitraum.
- **Paketeingang: (LAN > WAN) Pakete**, die für das ausgewählte Zeitintervall gesendet wurden.

- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

GRE Tunnel

Sie können einen Tunnelmechanismus verwenden, um Pakete eines Protokolls innerhalb eines anderen Protokolls zu transportieren. Das Protokoll, das das andere Protokoll trägt, wird als Transportprotokoll bezeichnet, und das übertragene Protokoll wird als Passagierprotokoll bezeichnet. Generic Routing Encapsulation (GRE) ist ein Tunnelmechanismus, der IP als Transportprotokoll verwendet und viele verschiedene Passagierprotokolle tragen kann.

Die Tunnelquelladresse und die Zieladresse werden verwendet, um die beiden Endpunkte der virtuellen Punkt-zu-Punkt-Verbindungen im Tunnel zu identifizieren. Weitere Informationen zum Konfigurieren von GRE-Tunneln auf Citrix SD-WAN-Appliances finden Sie unter GRE-Tunnel.

Um **GRE-Tunnelstatistiken** anzuzeigen, navigieren Sie zur Registerkarte **Berichte > Statistiken > GRE-Tunnel** .

Sie können die folgenden Metriken anzeigen:

- **Site-Name**: Der Site-Name.
- **Tx Bandbreite**: Übertragene Bandbreite.
- **Rx-Bandbreite**: Bandbreite erhalten.
- **Paket verworfen**: Anzahl der verworfenen Pakete aufgrund von Netzwerküberlastung.
- **Fragmentierte Pakete**: Anzahl fragmentierter Pakete. Pakete werden fragmentiert, um kleinere Pakete zu erstellen, die eine Verbindung mit einer MTU passieren können, die kleiner als das ursprüngliche Datagramm ist. Die Fragmente werden vom empfangenden Host wieder zusammengesetzt.
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

IPsec-Tunnel

IP-Sicherheitsprotokolle (IPsec) bieten Sicherheitsdienste wie Verschlüsselung sensibler Daten, Authentifizierung, Schutz vor Wiederholung und Datenvertraulichkeit für IP-Pakete. Encapsulating Security Payload (ESP) und Authentication Header (AH) sind die beiden IPsec-Sicherheitsprotokolle, die zur Bereitstellung dieser Sicherheitsdienste verwendet werden.

Im IPsec-Tunnelmodus ist das gesamte ursprüngliche IP-Paket durch IPsec geschützt. Das ursprüngliche IP-Paket wird umhüllt und verschlüsselt, und ein neuer IP-Header wird hinzugefügt, bevor das Paket über den VPN-Tunnel übertragen wird.
Weitere Informationen zum Konfigurieren von IPSec-Tunneln auf Citrix SD-WAN-Appliances finden Sie unter IPSec-Tunnelterminierung.

Um **IPSec-Tunnelstatistiken** anzuzeigen, navigieren Sie zur Registerkarte **Reporting > Statistik > IPSec-Tunnel** .

Sie können die folgenden Metriken anzeigen:

- **Tunnelname**: Der Name des Tunnels.
- **Tunnelzustand**: IPsec-Tunnelzustand.
- **MTU**: Maximale Übertragungseinheit —Größe des größten IP-Datagramms, das über eine bestimmte Verbindung übertragen werden kann.
- **Empfangenes Paket**: Anzahl der empfangenen Pakete.
- **Gesendete Pakete**: Anzahl der gesendeten Pakete.
- **Paket verworfen**: Anzahl der verworfenen Pakete aufgrund von Netzwerküberlastung.
- **Byte fallen gelassen**: Anzahl der verworfenen Byte.
- **Erweitern/Reduzieren**: Sie können die Daten nach Bedarf erweitern oder reduzieren.

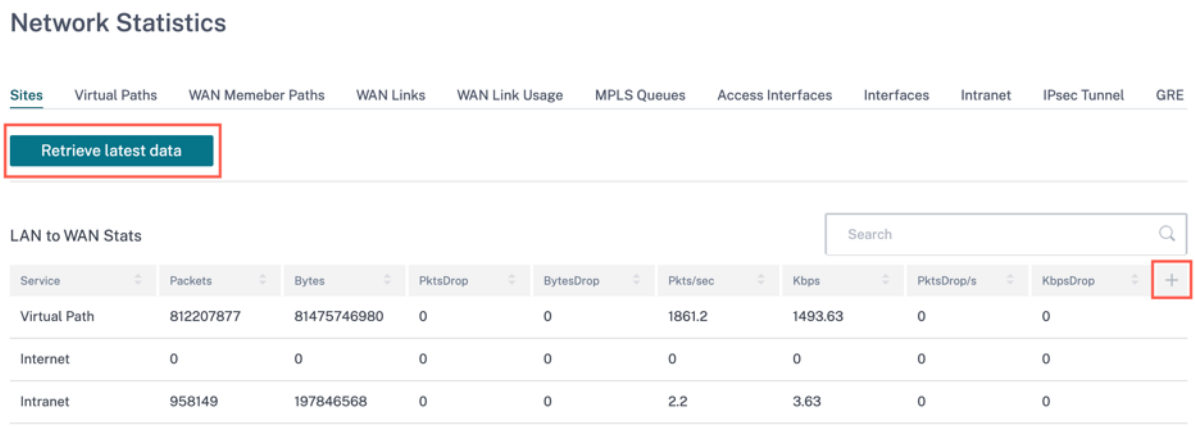
Statistiken in Echtzeit

Netzwerk-Statistik

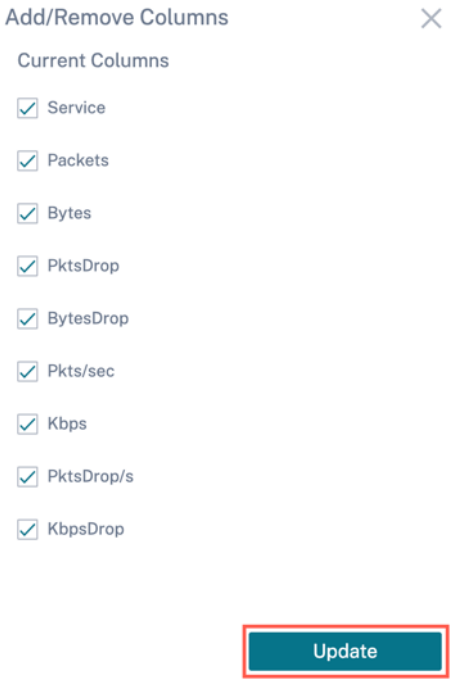
Unter **Berichte > Echtzeit > Netzwerkstatistiken erhalten Sie folgende statistische Informationen in Echtzeit**:

- Site
- Virtuelle Pfade
- Wege für WAN-Mitglieder
- WAN-Links
- WAN-Link-Nutzung
- MPLS-Warteschlangen
- Access Interfaces
- Schnittstellen
- Intranet
- IPsec-Tunnel
- GRE

Um den statistischen Bericht in Echtzeit abzurufen, wechseln Sie zur erforderlichen Registerkarte (z. B. Standort, virtuelle Pfade, WAN-Links) und klicken Sie auf **Neueste Daten abrufen**.



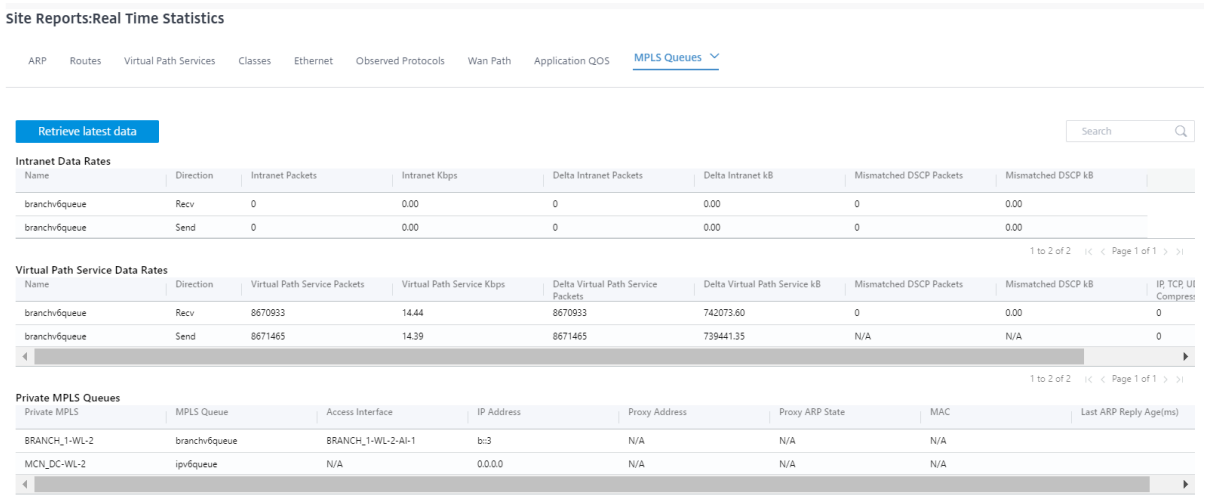
Klicken Sie auf das Pluszeichen (+), wenn Sie der Statistiktabelle eine Spalte hinzufügen oder daraus entfernen möchten, und klicken Sie auf **Aktualisieren**.



MPLS-Warteschlangen Mit MPLS-Warteschlangen können Sie die Warteschlangen definieren, die den MPLS-Warteschlangen des Dienstanbieters für die MPLS-WAN-Verbindungen entsprechen. Informationen zum Konfigurieren von MPLS-Warteschlangen finden Sie unter MPLS-Warteschlangen.

Um MPLS-Warteschlangenstatistiken anzuzeigen, navigieren Sie auf Standortebene zu **Berichte** > **Echtzeit** > **Netzwerkstatistiken**. Klicken Sie auf **MPLS-Warteschlangen**und dann auf **Neueste Daten abrufen**. Die neuesten MPLS-Warteschlangendaten werden von der Appliance abgerufen und im Citrix SD-WAN Orchestrator for On-premises angezeigt.

Sie können die Richtung, das Nein der Pakete, Delta-Pakete und nicht übereinstimmende DSCP-Pakete für Intranet- und virtuelle Pfaddienste anzeigen.



Für private MPLS-Warteschlangen können Sie die folgenden Details einsehen:

- **Private MPLS**: Die private MPLS-WAN-Verbindung.
- **MPLS-Warteschlange**: Die MPLS-Warteschlange, die der MPLS-WAN-Verbindung zugeordnet ist.
- **Zugriffsschnittstelle**: Die mit der MPLS-Warteschlange verknüpfte Zugriffsschnittstelle.
- **IP-Adresse: Die**mit der MPLS-Warteschlange verknüpfte IP-Adresse.
- **Proxyadresse: Die**Proxy-IP-Adresse, die der MPLS-Warteschlange zugeordnet ist.
- **Proxy-ARP-Status**: Der Status des Protokolls zur Auflösung von Proxy-Adressen. Aktiviert, deaktiviert oder N/A
- **MAC**: Die MAC-Adresse der Schnittstelle, die der MPLS-Warteschlange zugeordnet ist.
- **Alter der letzten ARP-Antwort**: Zeit in Millisekunden, zu der die letzte ARP-Antwort empfangen wurde.

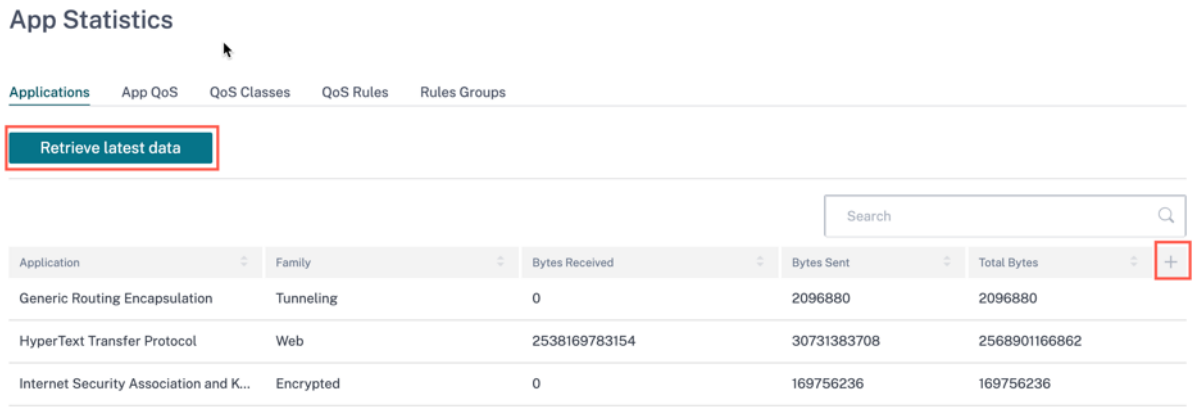
Weitere Informationen zur Problembehandlung finden Sie unter Problembehandlung bei MPLS-Warteschlangen.

App-Statistik

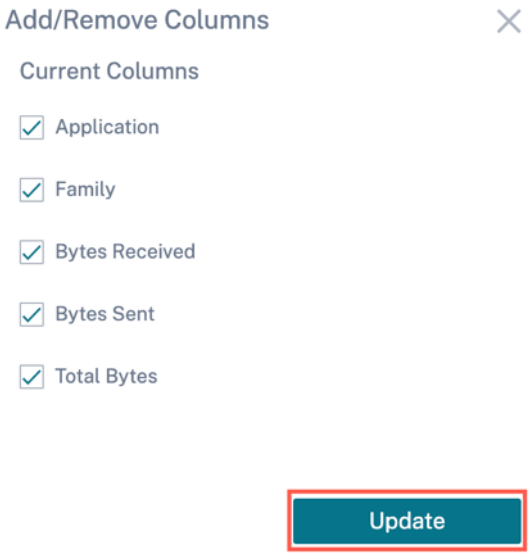
Unter **Berichte > Echtzeit > App-Statistik erhalten Sie folgende statistische Informationen in Echtzeit**:

- Anwendungen
- Beobachtete Protokolle
- App QoS
- QoS-Klassen
- QoS-Regeln
- Regelgruppen

Um den statistischen Bericht in Echtzeit abzurufen, wechseln Sie zur erforderlichen Registerkarte (z. B. Anwendungen, App-QoS, QoS-Regel) und klicken Sie auf **Neueste Daten abrufen**.



Klicken Sie auf das Pluszeichen (+), wenn Sie der Statistiktabelle eine Spalte hinzufügen oder daraus entfernen möchten, und klicken Sie auf **Aktualisieren**.

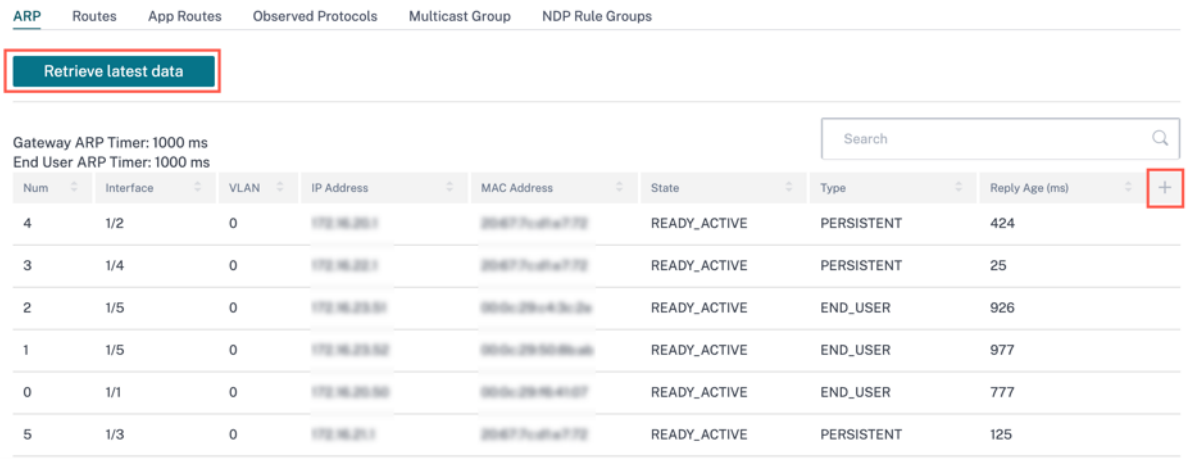


Routenstatistik

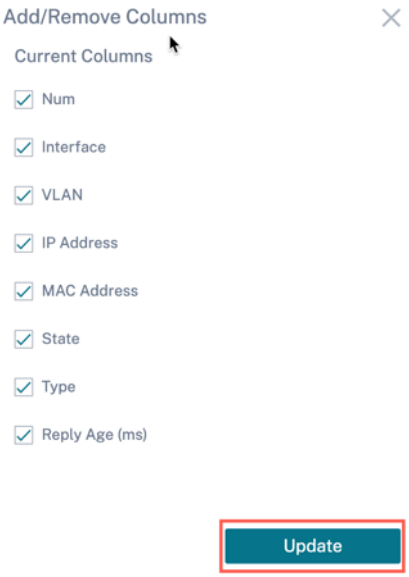
Unter **Berichte > Echtzeit > Streckenstatistik erhalten Sie folgende Echtzeit-Routenstatistik**:

- ARP (Address Resolution Protocol)
- Routen
- App-Routen
- Beobachtete Protokolle
- Multicastgruppe
- NDP-Regelgruppen

Um den statistischen Bericht in Echtzeit zu erhalten, wechseln Sie zur gewünschten Registerkarte (z. B. ARP, Routen, App-Routen) und klicken Sie auf **Neueste Daten abrufen**.



Klicken Sie auf das Pluszeichen (+), wenn Sie der Statistiktabelle eine Spalte hinzufügen oder daraus entfernen möchten, und klicken Sie auf **Aktualisieren**.

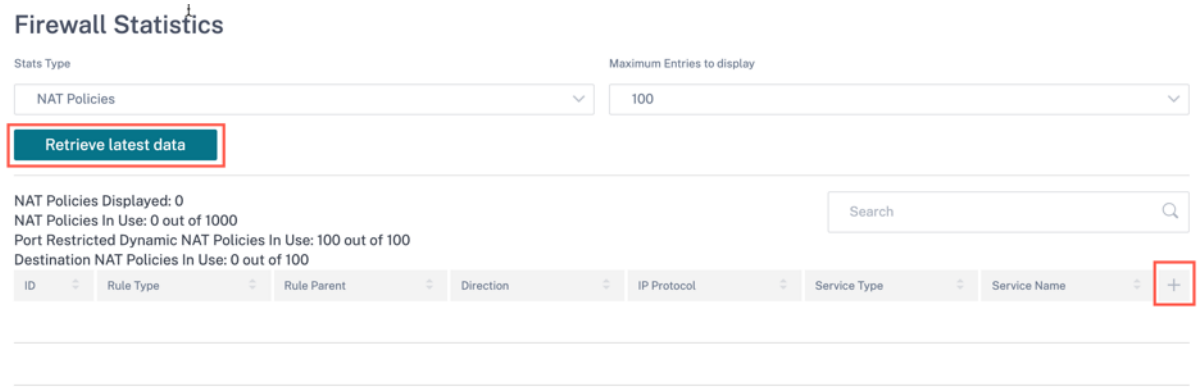


Firewall-Statistiken

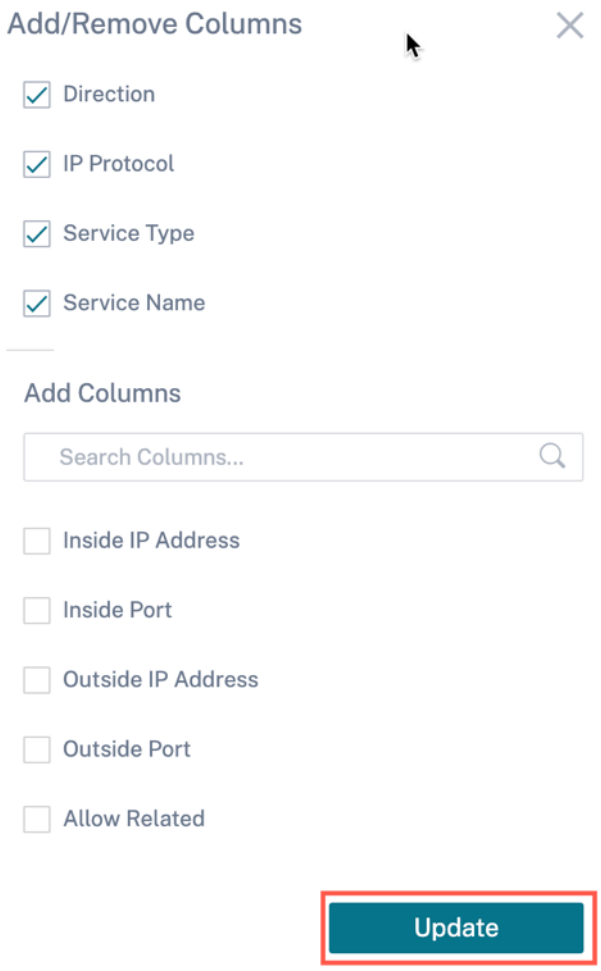
Die Seite **Firewall-Statistik** enthält den Status der Verbindung, NAT-Richtlinien (Network Address Protocol) und Filterrichtlinien für eine bestimmte Sitzung basierend auf der konfigurierten Firewall-laktion. Firewall-Verbindungen bieten auch vollständige Details über die Quelle und das Ziel der Verbindung.

Sie können die statistischen Informationen der Firewall in Echtzeit unter **Berichte > Echtzeit > Firewall-Statistiken**abrufen. Wählen Sie den Statistiktyp aus der Dropdownliste aus (Verbindung,

NAT-Richtlinien, Filterrichtlinien). Wählen Sie die Anzahl aus, die maximal angezeigt werden soll, und klicken Sie auf **Aktuelle Daten abrufen**.

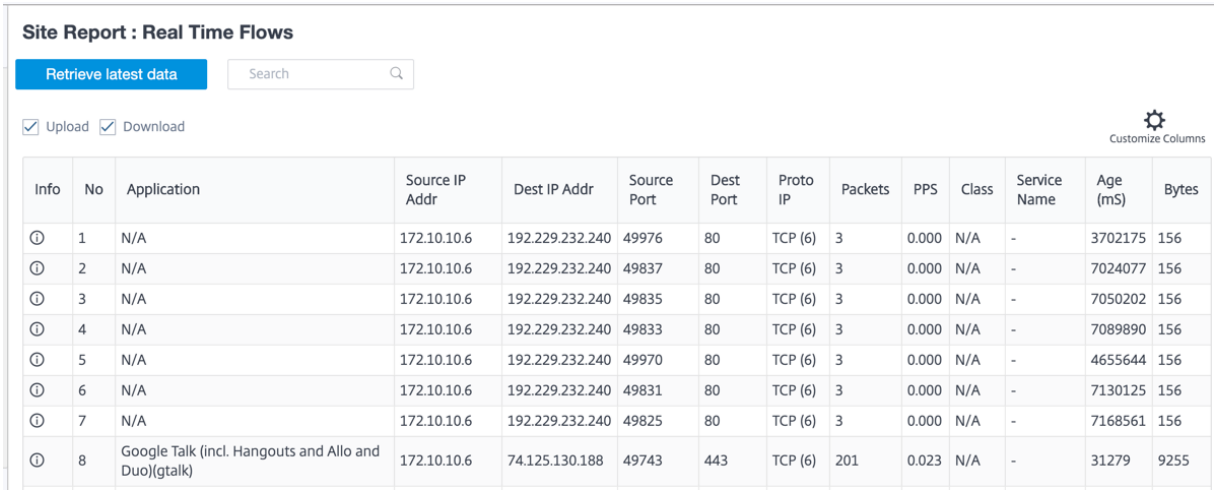


Klicken Sie auf das Pluszeichen (+), wenn Sie der Statistiktabelle eine Spalte hinzufügen oder daraus entfernen möchten, und klicken Sie auf **Aktualisieren**.



Strömungen

Die **Flows-Funktion** bietet unidirektionale Flussinformationen zu einer bestimmten Sitzung, die die Appliance durchläuft. Dies liefert Informationen über den Zieldiensttyp, in den der Flow fällt, sowie die Informationen, die sich auf den Regel- und Klassentyp sowie den Übertragungsmodus beziehen.



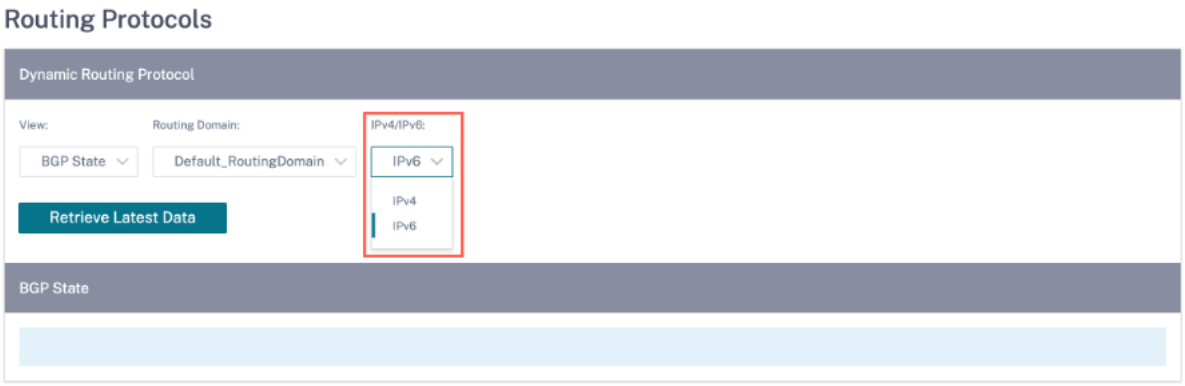
Info	No	Application	Source IP Addr	Dest IP Addr	Source Port	Dest Port	Proto IP	Packets	PPS	Class	Service Name	Age (mS)	Bytes
ⓘ	1	N/A	172.10.10.6	192.229.232.240	49976	80	TCP (6)	3	0.000	N/A	-	3702175	156
ⓘ	2	N/A	172.10.10.6	192.229.232.240	49837	80	TCP (6)	3	0.000	N/A	-	7024077	156
ⓘ	3	N/A	172.10.10.6	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

Routing-Protokolle

Der Bericht Routing-Protokolle enthält Einzelheiten zu den Parametern, die den Routingprotokollen zugeordnet sind. Wählen Sie ein Protokoll aus der Dropdown-Liste **Ansicht** und eine Routingdomäne aus der Dropdown-Liste **Routingdomäne** aus. Klicken Sie auf **Neueste Daten abrufen**, um die aktuellen Daten anzuzeigen.

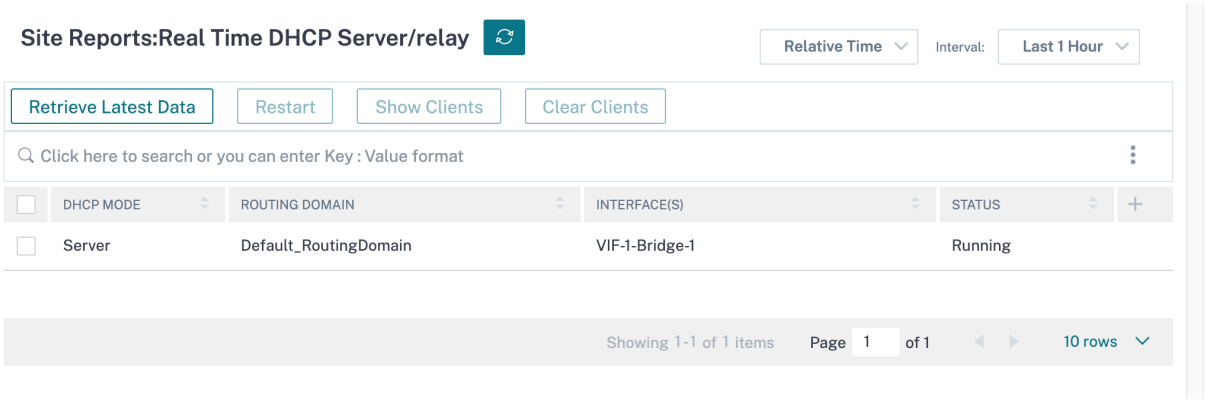
Sie können die Parameterdetails anzeigen, die mit den folgenden verknüpft sind:

- BGP-Staat
- OSPF-Staat
- OSPF-Topologie
- OSPF-Schnittstelle
- OSPF LADB
- OSPF-Nachbarn
- Routen-Tabelle

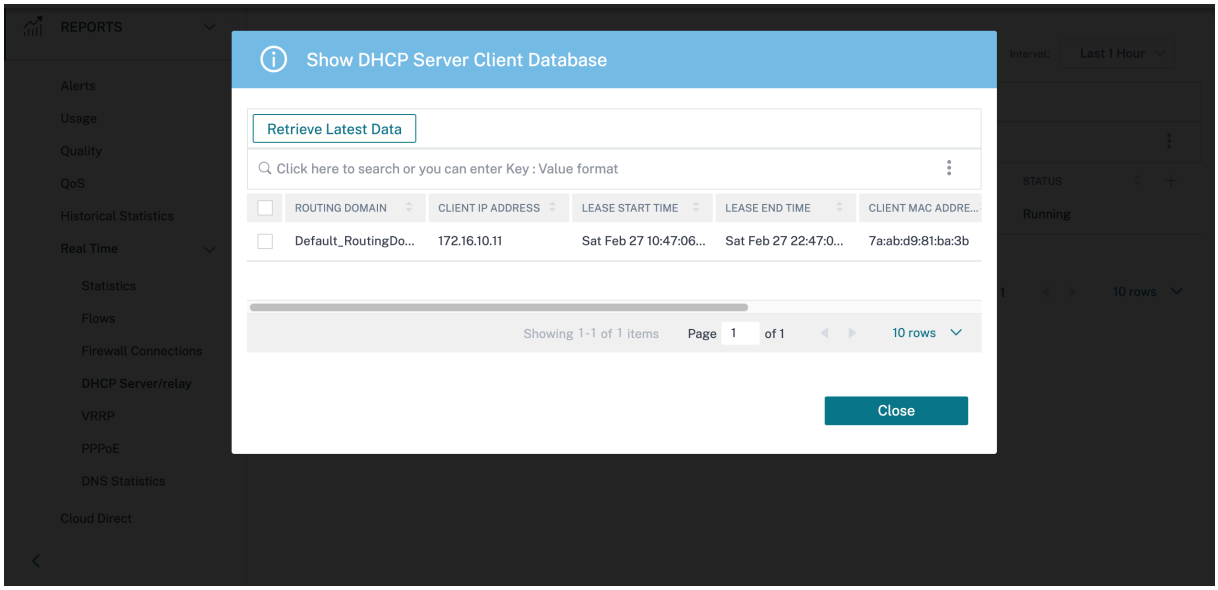


DHCP-Server und -Relay

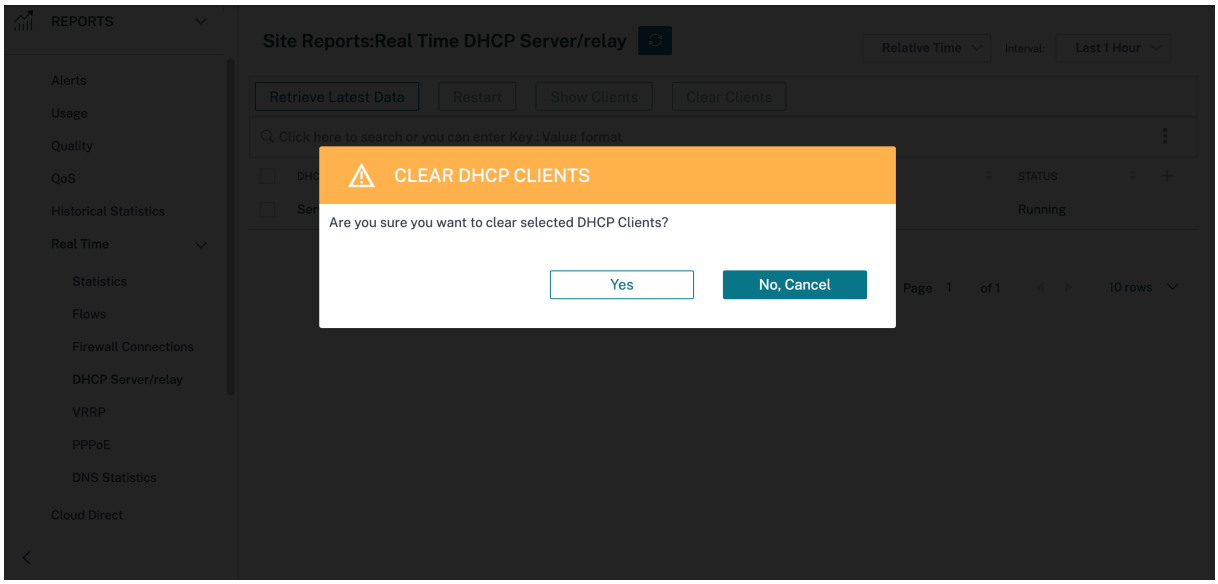
Der **DHCP-Server/Relay-Bericht** enthält die Informationen zu den als DHCP-Server oder -Relay konfigurierten Schnittstellen sowie die zugehörige Routingdomäne und den zugehörigen Status. Sie können im Format **Schlüssel: Wert** nach den erforderlichen DHCP-Server- oder Relay-Informationen suchen.



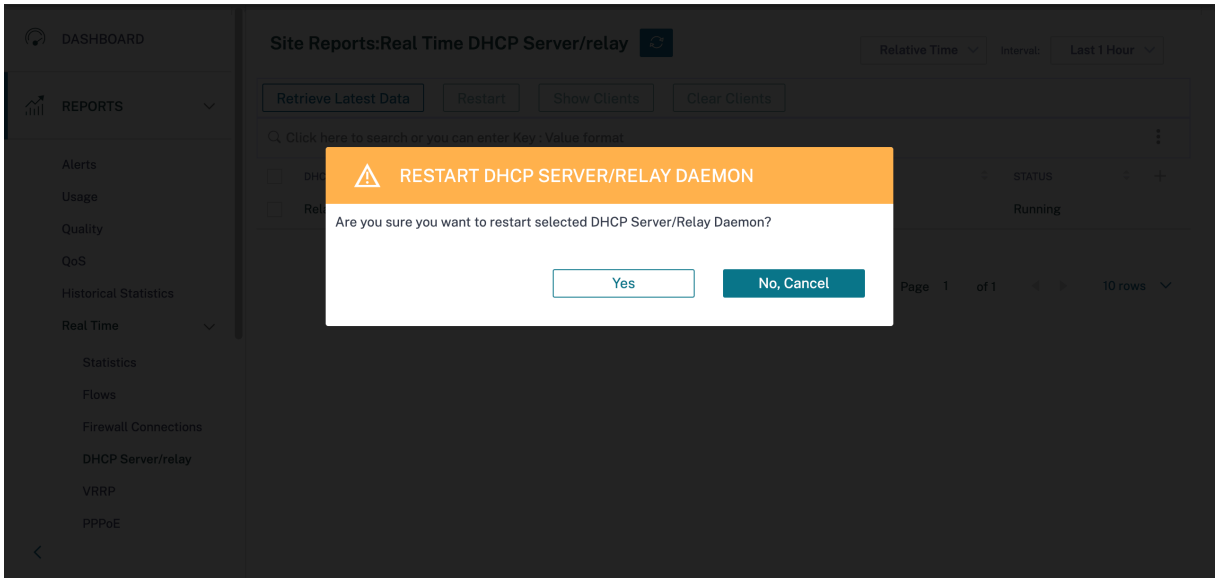
Wenn der Modus **Server**ist, können Sie auf **Clients anzeigen** klicken und die Liste der DHCP-Clients anzeigen, die dem DHCP-Server zugeordnet sind.



Klicken Sie auf **Clients löschen**, um die DHCP-Clients zu entfernen, die derzeit dem DHCP-Server zugeordnet sind.



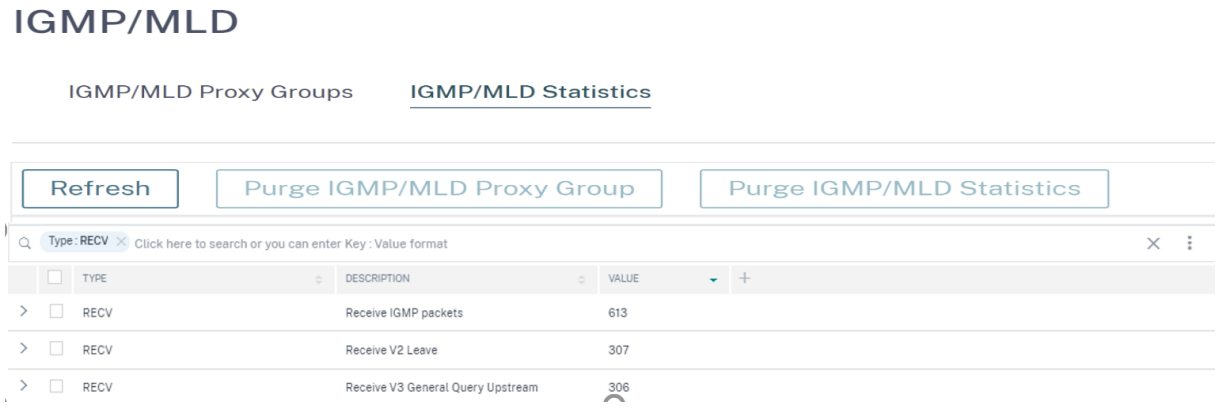
Klicken Sie auf **Neu** starten, um den DHCP-Server oder das Relay neu



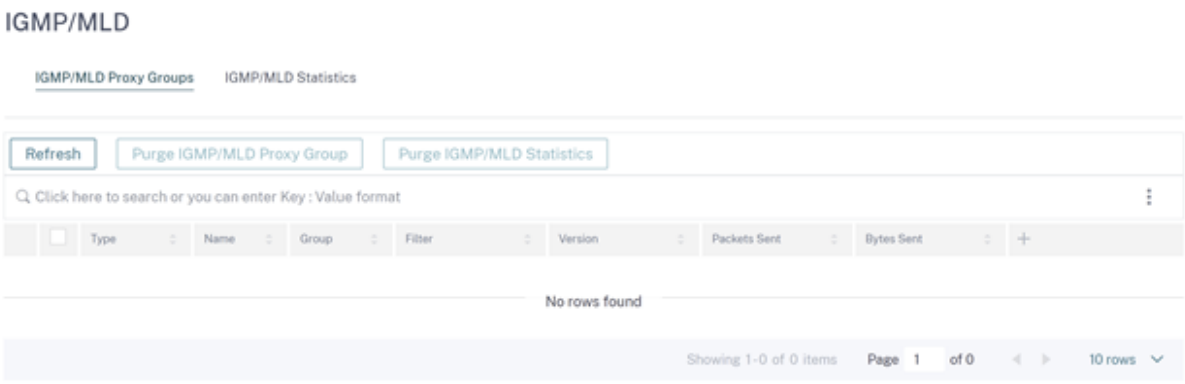
IGMP/MLD

Wenn die Multicast-Empfänger eine Join-Group-Anfrage initiieren, können Sie die Empfängerdetails unter **Berichte** > **Echtzeit** > **IGMP/MLD** > **IGMP/MLD-Statistik**sehen. Sie können diese Informationen sowohl an der Quelle als auch am Ziel sehen. Klicken Sie auf **Aktualisieren**, um die aktuellen Daten zu erhalten.

Die folgende Abbildung zeigt, dass die empfangenen IGMP-Pakete und der Filtertyp RECV verwendet werden, um IGMP-Empfangspakete einzubeziehen.



Um die Details der IGMP-Proxygruppen anzuzeigen, navigieren Sie zu **Berichte** > **Echtzeit** > **IGMP/MLD** > **IGMP/MLD Proxygruppen**. Klicken Sie auf **Aktualisieren**, um die aktuellen Daten zu erhalten.

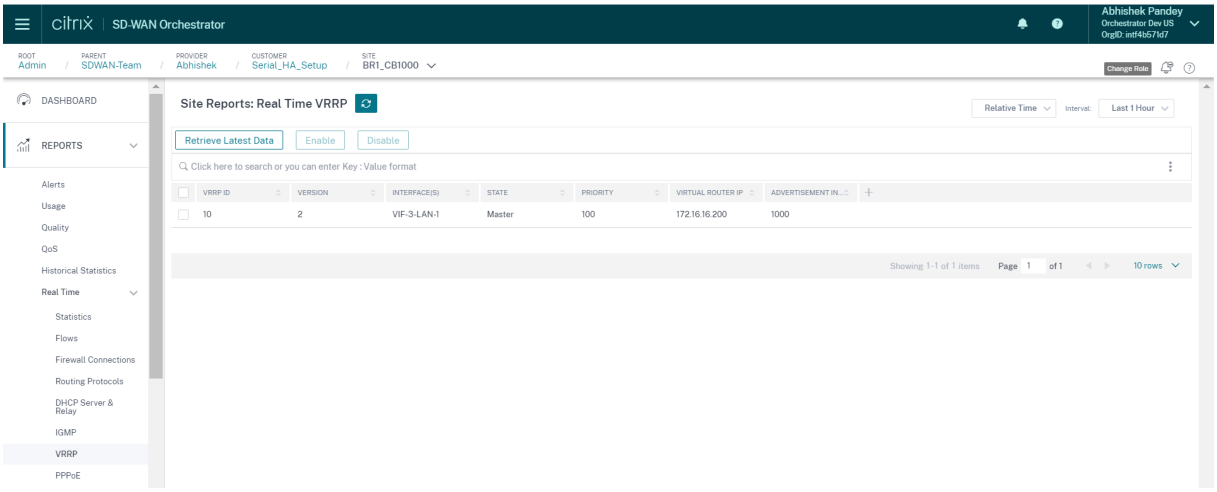


Wählen Sie **IGMP/MLD-Statistiken bereinigen**, um IGMP-Statistikdaten aus der IGMP-Statistiktabelle zu entfernen.

Wählen Sie **IGMP/MLD-Gruppen bereinigen**, um IGMP-Gruppendaten aus der IGMP-Gruppentabelle zu entfernen.

VRRP

Der VRRP-Echtzeitbericht enthält Details zu den konfigurierten VRRP-Gruppen.
Um den Bericht des Virtual Router Redundancy Protocol (VRRP) anzuzeigen, navigieren Sie zu **Berichte** > **Echtzeit** > **VRRP**. Klicken Sie auf **Neueste Daten abrufen**, um die aktuellen Daten abzurufen.



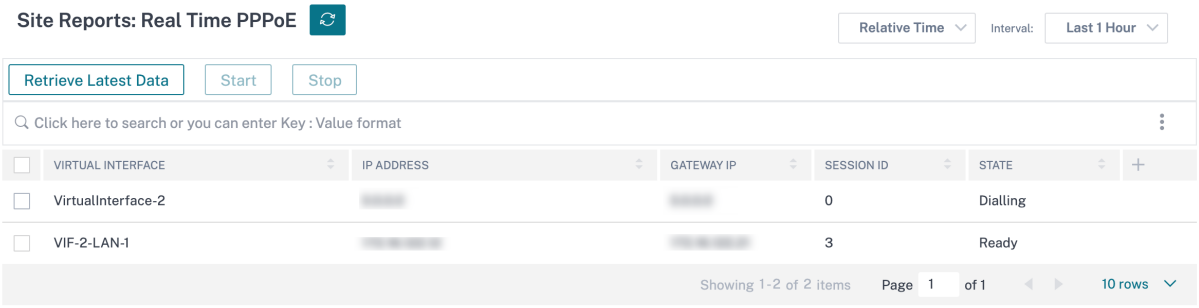
PPPoE

Der PPPoE-Bericht stellt Statusinformationen der konfigurierten virtuellen Schnittstelle mit dem statischen oder dynamischen PPPoE-Client-Modus bereit. Es ermöglicht Ihnen, die Sitzungen zur Fehlerbehebung manuell zu starten oder zu beenden.

- **Virtuelle Schnittstelle**: Die virtuelle Schnittstelle, die mit PPPoE verknüpft ist.
- **IP-Adresse: Die**mit der virtuellen Schnittstelle verknüpfte IP-Adresse. Wenn die virtuelle Schnittstelle aktiv und bereit ist, werden die kürzlich empfangenen Werte angezeigt. Wenn die virtuelle Schnittstelle angehalten ist oder sich im Status „Fehlgeschlagen“befindet, werden die zuletzt empfangenen Werte angezeigt.
- **Gateway-IP**: Die mit dem Gateway verknüpfte IP-Adresse. Wenn die virtuelle Schnittstelle aktiv und bereit ist, werden die kürzlich empfangenen Werte angezeigt. Wenn die virtuelle Schnittstelle angehalten ist oder sich im Status „Fehlgeschlagen“befindet, werden die zuletzt empfangenen Werte angezeigt.
- **Sitzungs-ID**: Die eindeutige Kennung, die der PPPoE-Sitzung zugeordnet ist
- **Status**: In der Spalte **Status** wird der Status der PPPoE-Sitzung angezeigt. In der folgenden Tabelle werden Status und Beschreibungen erklärt.

PPPoE-Sitzungstyp	Beschreibung
Konfiguriert	Ein VNI ist mit PPPoE konfiguriert. Dies ist ein Ausgangszustand.
Dialing	Nachdem ein VNI konfiguriert wurde, wechselt der PPPoE-Sitzungsstatus in den Wählzustand, indem die PPPoE-Erkennung gestartet wird. Paketinformationen werden erfasst.
Sitzungsfortbestehen	VNI wird vom Discovery-Status in den Sitzungsstatus verschoben und wartet auf den Empfang der IP, wenn es dynamisch ist, oder wartet auf Bestätigung vom Server für die angekündigte IP, falls statisch.
Bereit	IP-Pakete werden empfangen und VNI und die zugehörige WAN-Verbindung sind einsatzbereit.
Fehlgeschlagen	PPP/PPPoE-Sitzung wird beendet. Der Grund für den Fehler kann eine ungültige Konfiguration oder ein schwerwiegender Fehler sein. Die Sitzung versucht nach 30 Sekunden wieder eine Verbindung herzustellen.
Beendet	PPP/PPPoE-Sitzung wird manuell gestoppt.
Kündigung	Ein Zwischenzustand, der aus einem bestimmten Grund endet. Dieser Zustand beginnt automatisch nach einer bestimmten Dauer (5 Sekunden für normalen Fehler oder 30 Sekunden für einen schwerwiegenden Fehler).

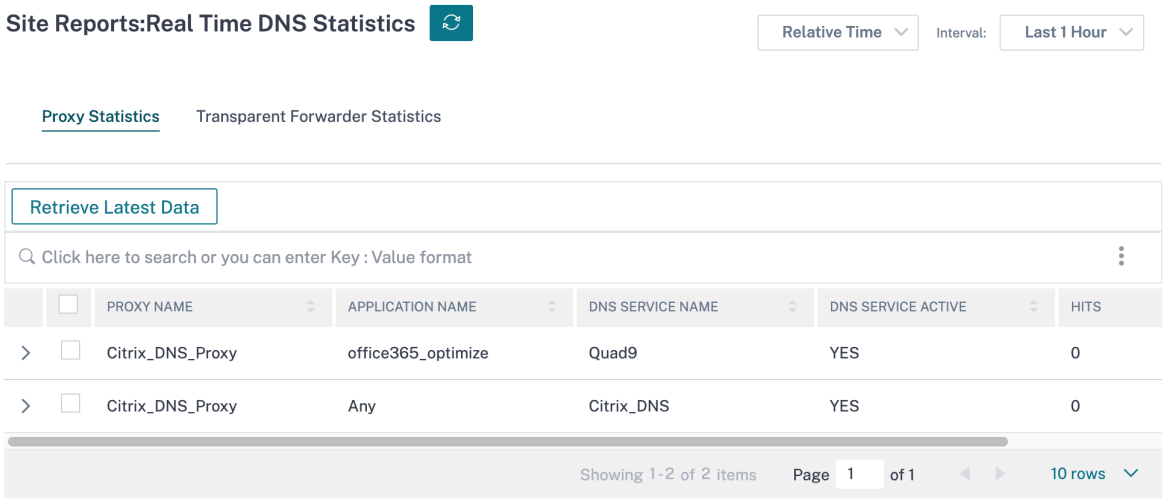
PPPoE-Sitzungstyp	Beschreibung
Deaktiviert	Der SD-WAN-Dienst ist deaktiviert.



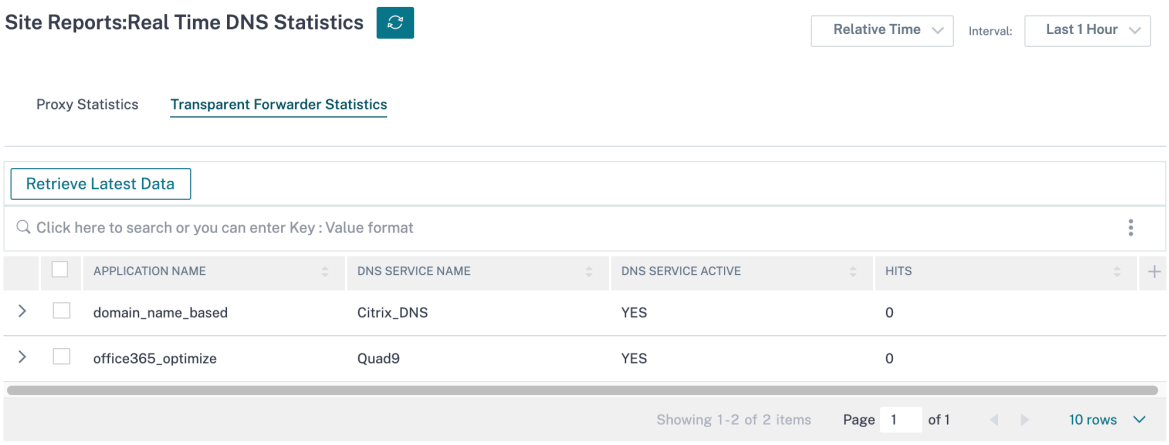
DNS-Statistiken

Die **DNS-Statistik** enthält die Informationen über den Anwendungsnamen, den DNS-Dienstnamen, den DNS-Dienststatus und den Umfang des `hits` DNS-Dienstes. Die Informationen für DNS-Proxy und DNS-transparente Weiterleitung werden auf zwei verschiedenen Registerkarten angezeigt.

Proxy-Statistiken



Transparente Forwarder-Statistiken



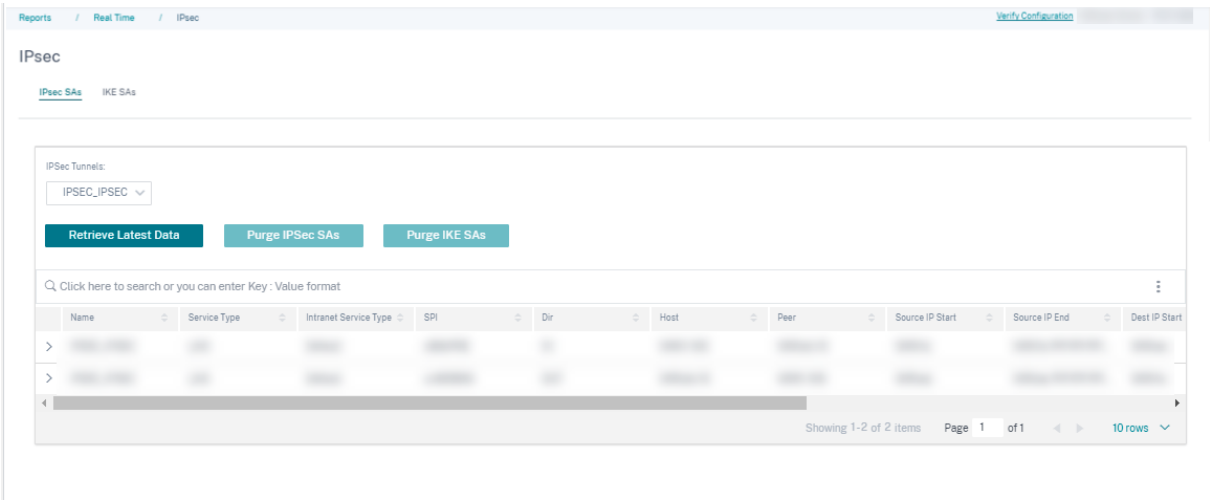
IPsec

Der IPSec-Echtzeitbericht enthält Details zu den IPSec-Tunneleinstellungen in Ihrem Netzwerk.

Um Details zu IPSec-Sicherheitszuordnungen (IPSec-SAs) anzuzeigen, navigieren Sie zu **Berichte** > **Echtzeit** > **IPSec** > **IPSec-SAs**. Klicken Sie auf **Aktuelle Daten abrufen**, um die aktuellen Daten abzurufen.

Um Details der Internet Key Exchange Security Associations (IKE SAs) anzuzeigen, navigieren Sie zu **Berichte** > **Echtzeit** > **IPSec** > **IKE SAs**. Klicken Sie auf **Aktuelle Daten abrufen**, um die aktuellen Daten abzurufen.

Sie können die IPSec-Gruppendaten und statistischen Daten auch löschen, indem Sie **IPSec-Gruppe löschen** bzw. **IKE-Statistiken bereinigen** auswählen.

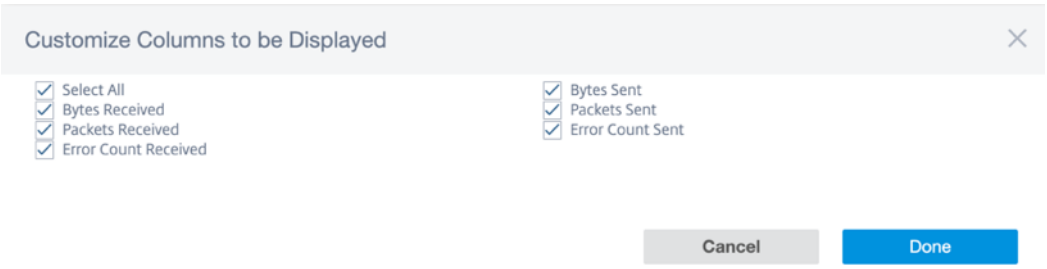


Appliance-Berichte (Vorschau)

Appliance-Berichte liefern die Berichte zum Netzwerkverkehr und zur Systemnutzung. Mit diesen Daten können Sie Netzwerkprobleme beheben oder das Verhalten Ihrer Citrix SD-WAN Geräte analysieren. Sie können die folgenden Registerkarten auf der Seite Appliance-Berichte sehen:

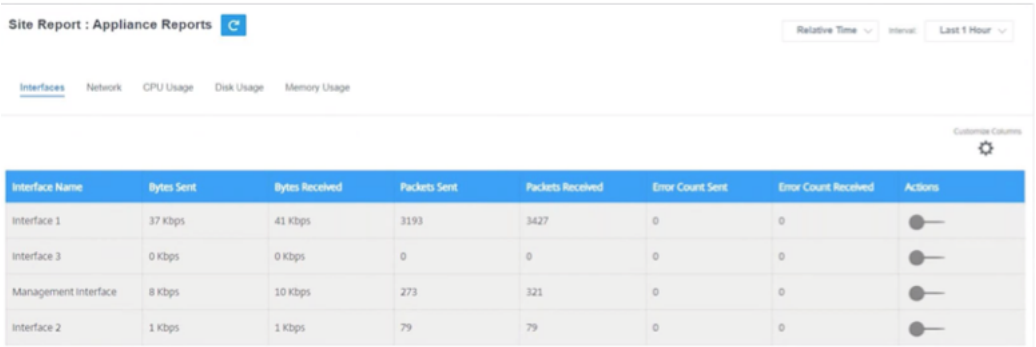
- Schnittstelle
- Netzwerk
- CPU-Nutzung
- Datenträgernutzung
- Speicherauslastung

Klicken Sie auf jede Registerkarte, um das Appliance-Diagramm nach Stunde, Tag, Woche und Monat anzuzeigen oder zu überwachen. Sie können nach Bedarf zwischen absoluter und relativer Zeit wechseln. Die Tabellenspalten sind anpassbar. Klicken Sie auf Spalte **anpassen** rechts oben in der Tabelle und aktivieren/deaktivieren Sie die Optionen, die Sie in der Tabelle ein- oder ausblenden möchten.



Schnittstelle

Auf der Seite **Schnittstelle** werden die Fehler/der Datenverkehr der Verwaltungsschnittstelle angezeigt. Das gesamte Netzwerk ist in verschiedene Schnittstellen unterteilt, z. B. Management Interface, Interface 1/2/3.

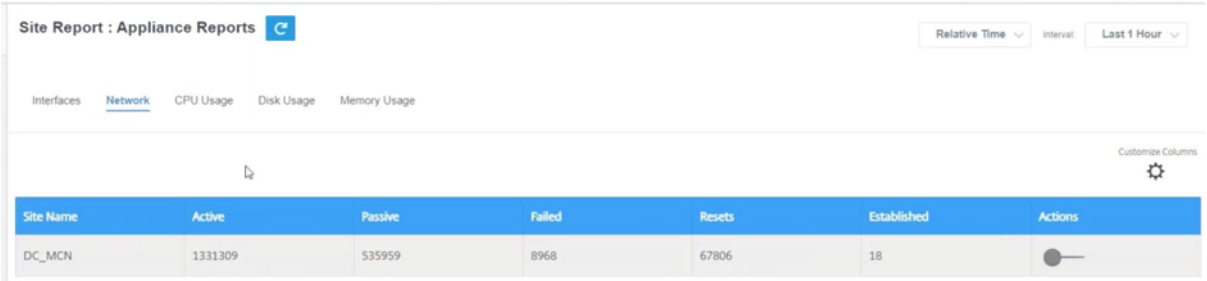


- **Schnittstellenname** —Zeigt den Schnittstellennamen an.
- **Gesendete Byte** —Durchschnittliche Anzahl der für die ausgewählte Dauer gesendeten Byte in Kbit/s.

- **Empfangene Bytes** —Durchschnittliche Anzahl der für die ausgewählte Dauer empfangenen Byte in Kbit/s.
- **Gesendete Pakete** —Die durchschnittliche Anzahl der Pakete, die für die ausgewählte Dauer gesendet wurden.
- **Empfangene Pakete** —Die durchschnittliche Anzahl der Pakete, die für die ausgewählte Dauer empfangen wurden.
- **Anzahl gesendeter** Fehler —Anzahl der für die ausgewählte Dauer gesendeten Fehler.
- **Empfangene Fehleranzahl** —Anzahl der für die ausgewählte Dauer empfangenen Fehler.
- **Aktionen** —Sie können die Aktionstaste einschalten, um das Netzwerkdiagramm anzuzeigen.

Netzwerk

Auf der Seite **Netzwerk** wird die Anzahl der TCP-Verbindungen für jeden konfigurierten Standort angezeigt.



- **Site-Name** —Zeigt den Site-Namen an.
- **Aktiv** —Durchschnittliche Anzahl aktiver TCP-Verbindungen für die ausgewählte Dauer.
- **Passiv** —Durchschnittliche Anzahl passiver TCP-Verbindungen für die ausgewählte Dauer.
- **Fehlgeschlagen** —Die durchschnittliche Anzahl der fehlgeschlagenen TCP-Verbindungen für die ausgewählte Dauer.
- **Resets** —Durchschnittliche Anzahl der zurückgesetzten TCP-Verbindungen für die ausgewählte Dauer.
- **Etabliert** —Durchschnittliche Anzahl etablierter TCP-Verbindungen für die ausgewählte Dauer.
- **Aktionen** —Sie können die Aktionstaste einschalten, um das Netzwerkdiagramm anzuzeigen.

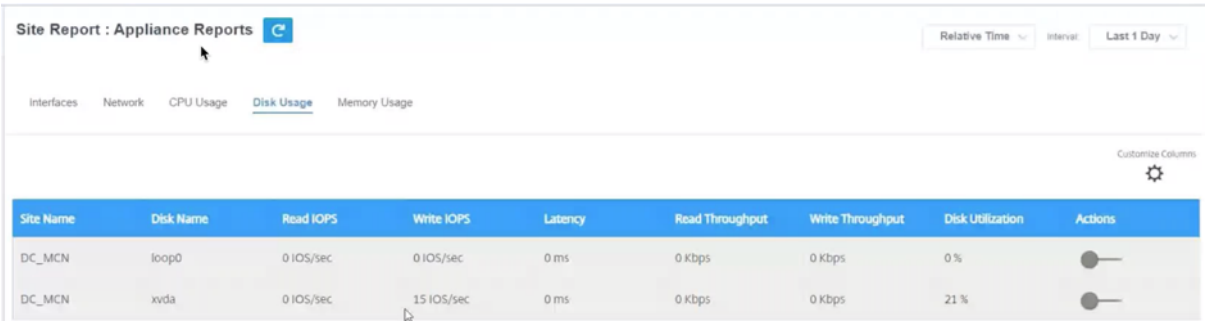
CPU-Nutzung

Auf der Seite „ **CPU-Auslastung** “wird die CPU-Auslastung des SD-WAN-Geräts als Prozentsatz angezeigt. Das CPU-Diagramm zeigt den durchschnittlichen CPU-Verbrauch für die regulären Intervalle während der ausgewählten Zeit.

- **Site-Name** —Zeigt den Site-Namen an.
- **System** —Prozentsatz der Gesamtzeit, die die CPU mit der Verarbeitung von Programmen im Systembereich verbracht hat.
- **Benutzer** —Prozentsatz der Gesamtzeit, die die CPU mit der Verarbeitung von Userspace-Programmen verbrachte.
- **Nice** —Nice ist, wenn die CPU eine Benutzeraufgabe mit unterdurchschnittlicher Priorität ausführt.
- **Leerlauf** —Prozentsatz der Gesamtzeit, in der sich die CPU im Leerlaufmodus befand.
- **Io Wait** —Prozentsatz der Gesamtzeit, die die CPU mit Warten auf I/O-Vorgänge verbracht hat.
- **Irq** —Der Interrupt Requests (IRQs) -Wert, den der Kernel bedient.
- **Stehlen** - Wenn der Hypervisor in einer virtualisierten Umgebung ausgeführt wird, stiehlt er möglicherweise Zyklen, die für Ihre CPUs bestimmt sind, und gibt sie aus verschiedenen Gründen an eine andere weiter. Dieses Mal ist bekannt als Steal.
- **Aktionen** —Sie können die Aktionstaste einschalten, um das Netzwerkdiagramm anzuzeigen.

Datenträgernutzung

Auf der Seite **Datenträgernutzung** wird die Menge des vom Betriebssystem und der Datenpartition verwendeten Festplattenspeichers in einem I/O-pro-Sekunden-Wert (IOPS) angezeigt.

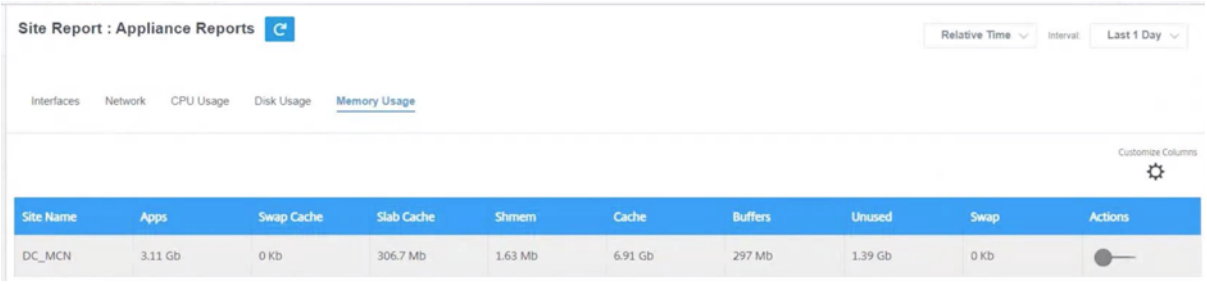


- **Site-Name** —Zeigt den Site-Namen an.
- **Festplattenname** —Zeigt den Namen der Festplatte an.
- **IOPS lesen** —Zeigt die durchschnittliche Anzahl von Lese-IOPS pro Sekunde über den ausgewählten Zeitraum an.

- **Schreib-IOPS** —Zeigt die durchschnittliche Anzahl von Schreib-IOPS pro Sekunde über den ausgewählten Zeitraum an.
- **Latenz** —Zeigt den Latenzwert der erfolgreichen Lese- und Schreibanforderungen des ausgewählten Volume-Workloads über den ausgewählten Zeitraum an. Es wird empfohlen, dass der Latenzwert unter 10 ms am besten für die E/A-Leistung geeignet ist.
- **Lesedurchsatz** —Zeigt den durchschnittlichen Festplattendurchsatzwert des Festplattenlesevorgangs über den ausgewählten Zeitraum in Kbit/s an.
- **Schreibdurchsatz** —Zeigt den durchschnittlichen Festplattendurchsatzwert des Festplattenschreibvorgangs über den ausgewählten Zeitraum in Kbit/s an.
- **Festplattenauslastung** —Zeigt den durchschnittlichen Wert der Festplattenauslastung in Prozent über den ausgewählten Zeitraum an.
- **Aktionen** —Sie können die Aktionstaste einschalten, um das Netzwerkdiagramm anzuzeigen.

Speichernutzung

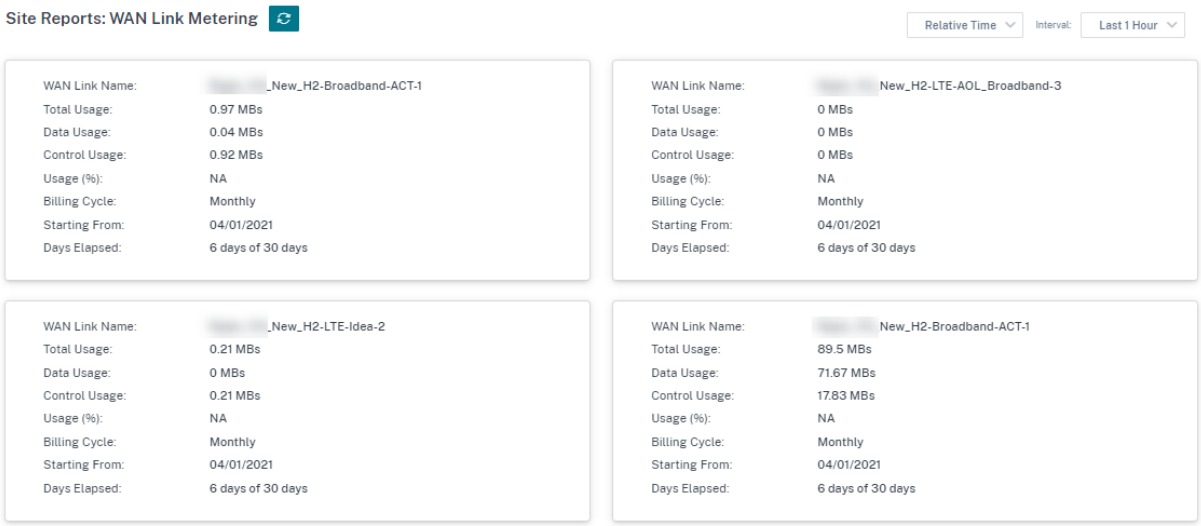
Auf der Seite **Speichernutzung** wird der Bericht über die Menge des verwendeten Speichers angezeigt.



- **Site-Name** —Zeigt den Site-Namen an.
- **Apps** —Zeigt den Wert der verwendeten Anwendung in GB an.
- **Swap Cache** —Zeigt die Swap-Cache-Nummer in MB an. Der Swap-Cache ist eine Liste von Seitentabelleneinträgen mit einem Eintrag pro physischer Seite.
- **Plattencache** —Zeigt die Anzahl der vorab zugewiesenen Speicherplatten an. Auf Mb
- **Shmem** —Zeigt den gesamten verwendeten Shared Memory-Wert in MB an.
- **Cache** —Zeigt die Anzahl der in GB verwendeten Cache-Speicher an.
- **Puffer** —Zeigt die Nummer des physischen Speichers an, der vom Puffer-Cache verwendet wird.
- **Unbenutzt** —Zeigt die Anzahl der nicht verwendeten Speicher für den Cache an.
- **Swap** —Zeigt die Anzahl der Auslagerungsräume an. Der Swap Space wird verwendet, wenn Sie eine gewisse Speicherplatzerweiterung für Ihren physischen Speicher benötigen.
- **Aktionen** —Sie können die Aktionstaste einschalten, um das Netzwerkdiagramm anzuzeigen.

WAN-Link-Messung

Berichte zur WAN-Link-Metering enthalten Details zur gemessenen WAN-Link-Nutzung. Sie können die Berichte anzeigen, um Einblicke in den Datenverbrauch der gemessenen WAN-Verbindungen zu erhalten. Um Berichte zur WAN-Link-Messung anzuzeigen, navigieren Sie zu **Berichte > WAN Link Metering**.

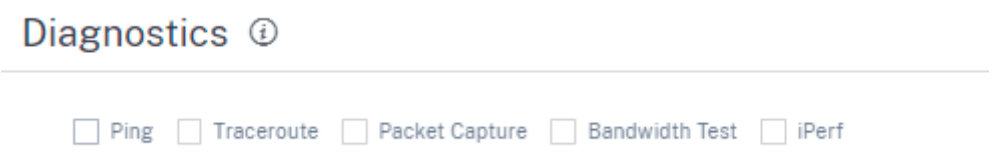


Diagnose

October 21, 2022

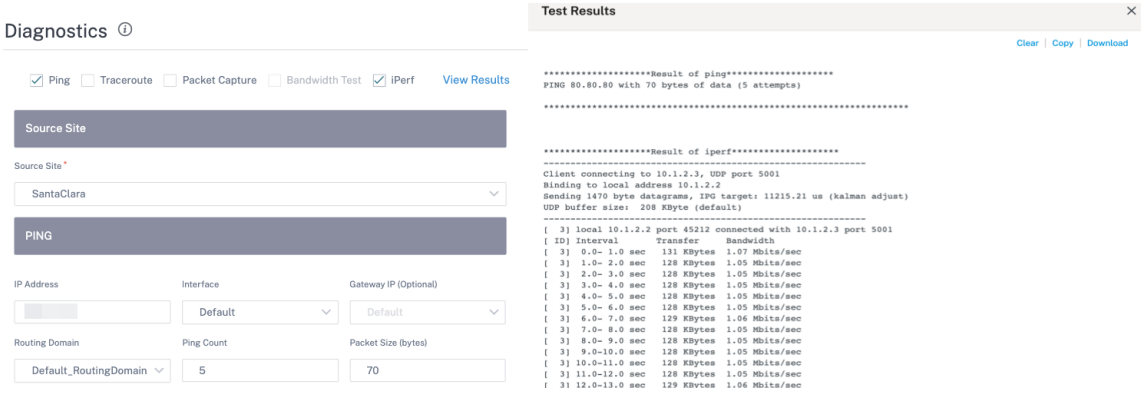
Sie können Ping-, Traceroute-, Packet Capture-, Bandbreitentest- und iPerf-Diagnosedienstprogramme verwenden, um Netzwerkverbindungsprobleme in Ihrem SD-WAN-Netzwerk zu testen und zu untersuchen. Um die Seite „Diagnose“anzuzeigen, navigieren Sie zu **Fehlerbehebung** > **Diagnose**.

Um die **Diagnoseergebnisse anzuzeigen**, klicken Sie oben rechts auf der Diagnoseseite auf Ergebnisse anzeigen. Sie können die Berichtsergebnisse nach Bedarf **herunterladen**, **kopieren**und **löschen** .

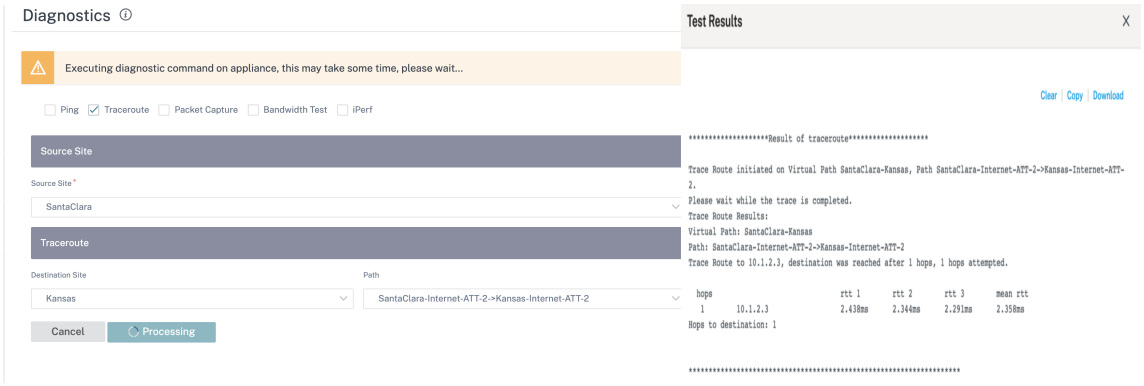


- **Ping** —Sie können die Netzwerkkonnektivität überprüfen, indem Sie einen Remote-Host oder eine Site pingen. Geben Sie die Zieldetails ein, geben Sie an, wie oft die Ping-Anfrage gesendet

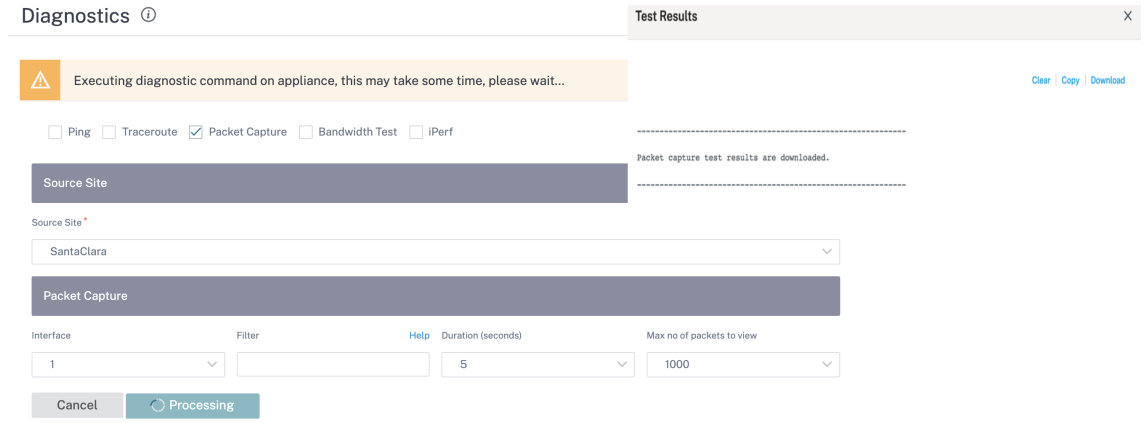
werden soll, und die Anzahl der Datenbytes. Geben Sie die **Ziel-IP-Adresse** an und klicken Sie auf **Ausführen**.



- **Traceroute** - Sie können die Route und die Anzahl der Hops zwischen Standorten verfolgen. Wählen Sie die Quell- und Ziel-Site sowie den Pfad für die Ablaufverfolgung aus und klicken Sie auf **Ausführen**

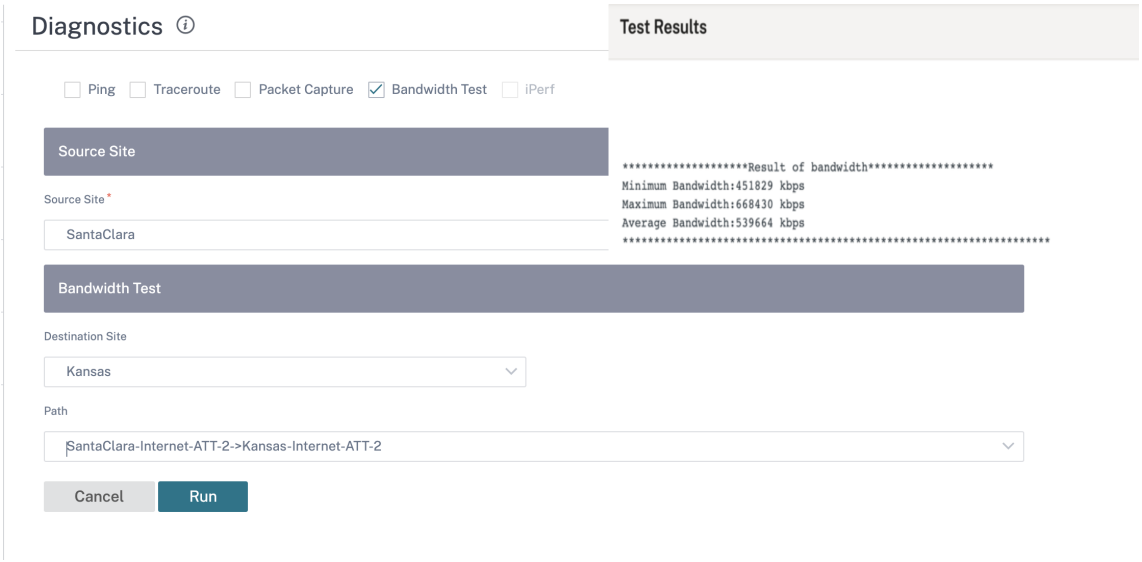


- **Paketerfassung** —Sie können das Datenpaket abfangen, das über die ausgewählte aktive Schnittstelle in der ausgewählten Site übertragen wird. Sie können die Quell- und Zieldetails anzeigen.



Die Option **Hilfe** bietet mehr Details zu den **Filteroptionen**.

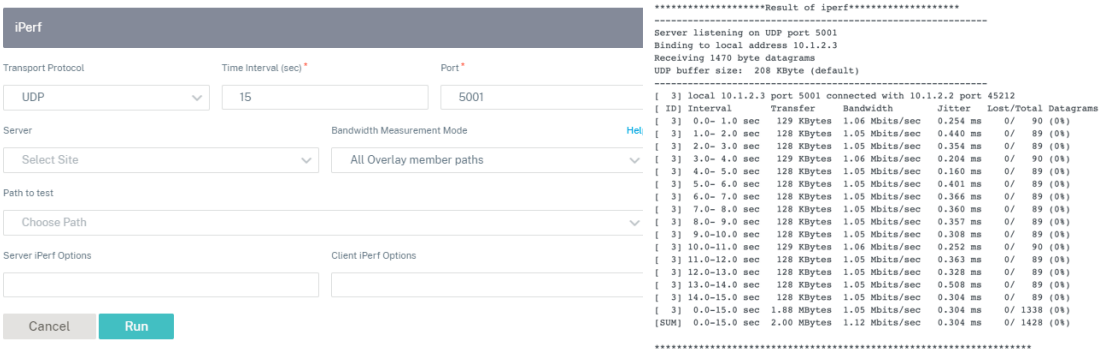
- **Bandbreitentest** —Sie können einen Bandbreitentest für einen bestimmten Pfad einer Site ausführen, um die maximale, minimale und durchschnittliche Bandbreitennutzung anzuzeigen. Geben Sie die Quell-Site und Ziel-Site ein und wählen Sie den Pfad aus. Klicken Sie auf **Ausführen**.



- **iPerf** —Sie können einen iPerf-Test für einen bestimmten Pfad einer Site ausführen. Das iPerf-Diagnosetool wird verwendet, um Testdatenverkehr zu generieren, mit dem Sie Netzwerkprobleme beheben können, die zu folgenden Folgen führen können:

  - Häufiger Wechsel des Pfadzustands von Gut nach Schlecht
  - Schlechte Anwendungsleistung
  - Höherer Paketverlust

  Um einen iPerf-Diagnosetest auszuführen, navigieren Sie auf Kundenebene zu **Fehlerbehebung** > **Diagnose**, und aktivieren Sie das Kontrollkästchen **iPerf** . Geben Sie das Transportprotokoll, das Zeitintervall, die Portnummer, den Server, den Bandbreitenmessmodus, den zu testenden Pfad und die iPerf-Optionen des Servers ein, und **klicken**Sie

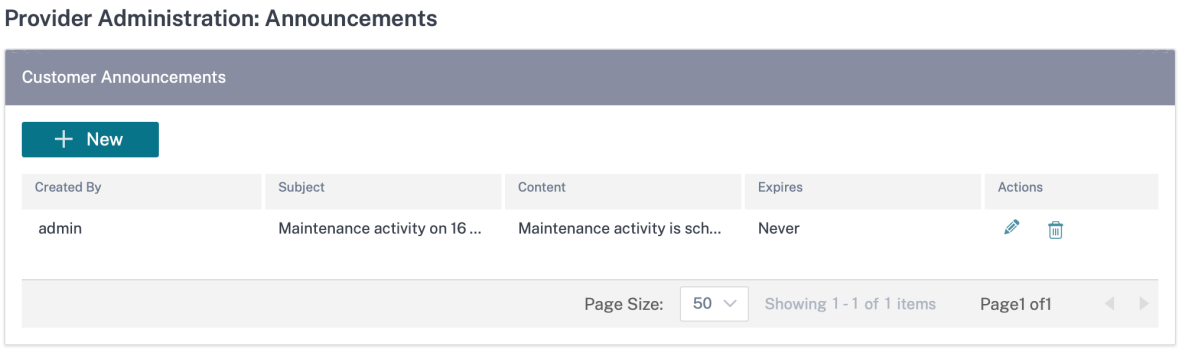


Ankündigungen

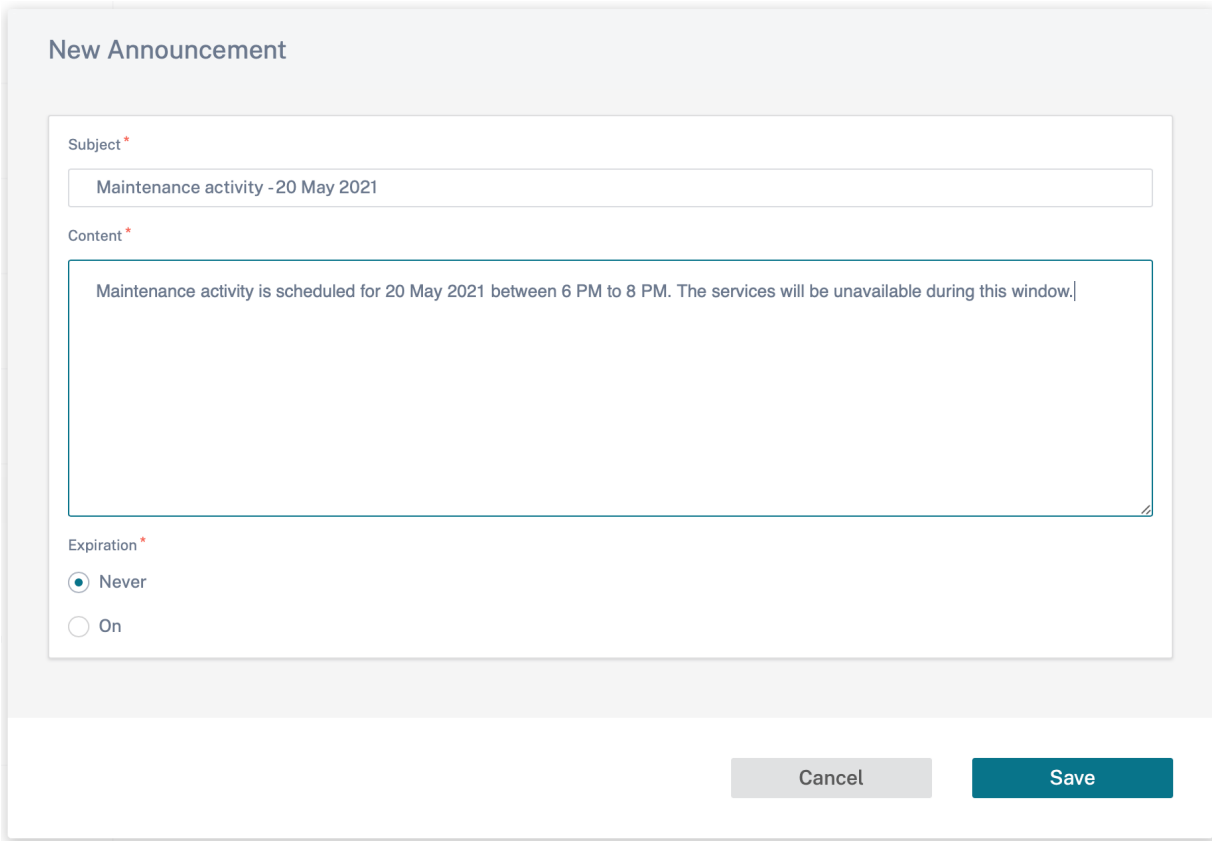
October 21, 2022

Anbieter können die Option **Ankündigungen** verwenden, um Ankündigungen oder Benachrichtigungen an ihre Kunden zu senden.

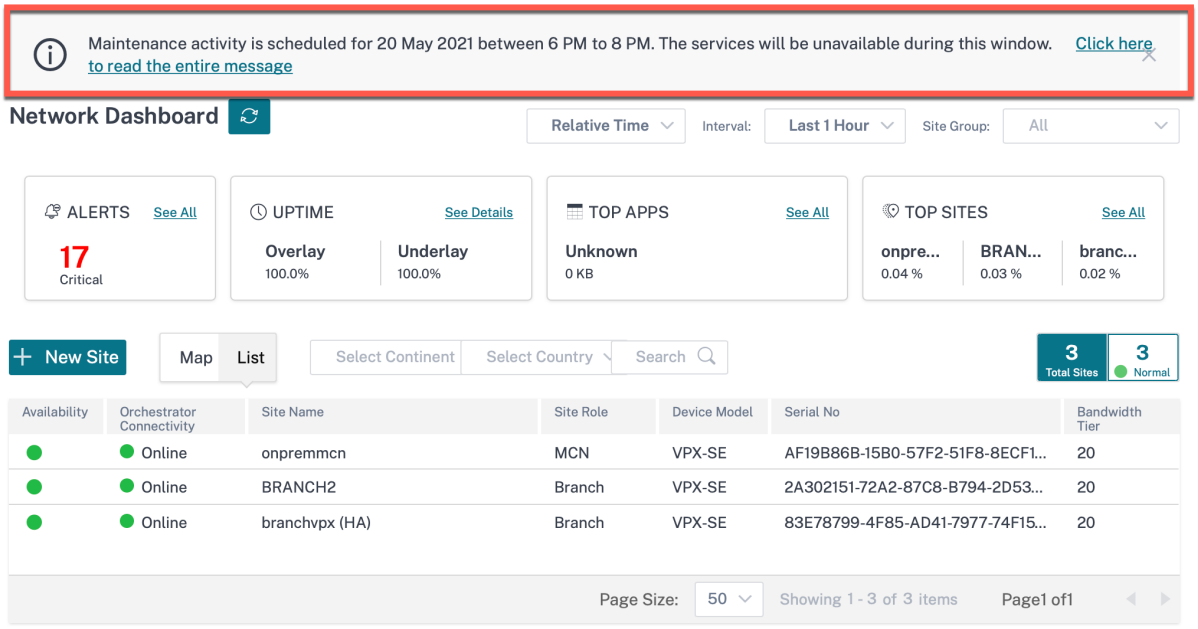
Sie können eine Anbieterankündigung erstellen, indem Sie zu **Administration > Ankündigungen** navigieren und auf die Option **+ Neu** klicken.



Geben Sie eine Betreffzeile an und geben Sie Inhalt im HTML- oder Nur-Text-Format Sie können auch den Ablauf der Ankündigung festlegen.



Die gespeicherten Ankündigungen werden allen Kunden angezeigt.



Verwaltung der Benutzer

October 21, 2022

Citrix SD-WAN Orchestrator for On-premises unterstützt die rollenbasierte Zugriffssteuerung (RBAC). RBAC reguliert den Zugriff auf SD-WAN Orchestrator Orchestrator-Ressourcen basierend auf den Rollen, die einzelnen Benutzern zugewiesen sind. RBAC ermöglicht es Benutzern, nur auf die Daten zuzugreifen, die ihre Rolle erfordert, und schränkt alle anderen Daten ein.

Eine Rolle definiert die Berechtigungen zum Anzeigen und Ausführen verschiedener Aktivitäten in Citrix SD-WAN Orchestrator for On-premises. Sie können einem Benutzer eine Rolle aus der Liste der vordefinierten Rollen zuweisen.

Standardmäßig wird auf Citrix SD-WAN Orchestrator for On-premises ein Benutzerkonto erstellt, wobei der Benutzername **admin** und das Kennwort als **Kennwort**festgelegt sind. Der Benutzer wird bei der ersten Anmeldung aufgefordert, das Standardkennwort zu ändern.

Sie können Benutzer hinzufügen, die lokal und remote authentifiziert werden können. Benutzer, die remote authentifiziert werden, werden über RADIUS- oder TACACS+-Authentifizierungsserver authentifiziert.

Anbeiterrollen

In der folgenden Tabelle sind die vordefinierten Anbieterrollen aufgeführt.

Rolle des Anbieters	Beschreibung
Provider-Master-Admin-All	Ein Administrator, der den Anbieter und alle seine Kundeninformationen verwalten kann
Provider-Master-Admin-Tenant	Ein Administrator, der den Anbieter und einen Teil seiner Kundeninformationen verwalten kann
Provider-Master-Readonly-All	Ein Administrator, der nur Anbieter- und Kundeninformationen einsehen kann
Provider-Netzwerk-Admin (Vorschau)	Ein Administrator, der nur die netzwerkbezogenen Informationen anzeigen und bearbeiten kann
Provider-Security-Admin (Vorschau)	Ein Administrator, der nur die sicherheitsbezogenen Informationen anzeigen und bearbeiten kann

Die **Provider-Master-Admin-All-Rolle** kann Folgendes ausführen:

- Weisen Sie Benutzern im Anbieter- und Kundennetzwerk Rollen zu
- Verwalten des Zugriffs auf Kunden für alle anderen Admin-Rollen
- Bearbeiten oder Löschen von zugewiesenen Rollen

Rollen von Kunden

In der folgenden Tabelle sind die vordefinierten Kundenrollen aufgeführt:

Rolle	Beschreibung
Customer-Master-Admin	Ein Kundenadministrator, der Kundeninformationen anzeigen und bearbeiten kann
Customer-Master-ReadOnly-Admin	Ein Kundenadministrator, der nur Kundeninformationen anzeigen kann
Kunden-Netzwerk-Admin (Vorschau)	Ein Kundenadministrator, der nur netzwerkbezogene Informationen anzeigen und bearbeiten kann
Kundensicherheit-Admin (Vorschau)	Ein Kundenadministrator, der nur sicherheitsbezogene Informationen anzeigen und bearbeiten kann

Ein Benutzer mit der Rolle **Customer-Master-Admin** kann Folgendes ausführen:

- Benutzer hinzufügen und Kundenrollen zuweisen
- Bearbeiten oder Löschen von zugewiesenen Rollen

Support-Rollen

Zur Fehlerbehebung können Kunden Supportrollen zuweisen und Mitgliedern des Support-Teams die Möglichkeit geben, ihre Informationen anzuzeigen und zu bearbeiten. Supportrollen haben einen Gültigkeitszeitraum, der bei der Zuweisung der Rolle definiert wird. Nach Ablauf der Gültigkeitsdauer verliert der Support-Benutzer den Zugriff auf Kundeninformationen. Die Support-Benutzerdetails werden jedoch weiterhin unter **Administration > Benutzerverwaltung**angezeigt. Je nach Bedarf kann der Kundenadministrator die Support-Rolle entweder löschen oder ihre Gültigkeit verlängern.

Rolle	Beschreibung
Customer-Support-ReadWrite	Ein Mitglied des Support-Teams, das die Kundeninformationen anzeigen und bearbeiten kann
Customer-Support-ReadOnly	Ein Mitglied des Support-Teams, das nur die Kundeninformationen anzeigen kann

Arten der Authentifizierung

Citrix SD-WAN Orchestrator for On-premises unterstützt die folgenden Authentifizierungstypen:

- **Einzelfaktor-Authentifizierung**: Die Einzelfaktor-Authentifizierung stellt eine Authentifizierungsmethode dar, um Benutzern Zugriff auf Citrix SD-WAN Orchestrator for On-premises zu erhalten.
- **Zwei-Faktor-Authentifizierung (TFA)**: Die Zwei-Faktor-Authentifizierung bietet zwei Authentifizierungsmethoden, um Benutzern Zugriff auf Citrix SD-WAN Orchestrator for On-premises zu erhalten. Es führt eine zusätzliche Sicherheitsebene in der Anmeldesequenz ein.

Die folgenden Authentifizierungsmethoden werden für die Ein-Faktor- und Zwei-Faktor-Authentifizierung unterstützt:

- **Lokal**: Wenn diese Option ausgewählt ist, muss der Benutzer das auf Citrix SD-WAN Orchestrator for On-premises konfigurierte Kennwort verwenden, um Zugriff zu erhalten.
- **RADIUS**: Wenn ausgewählt, muss der Benutzer das RADIUS-Serverkennwort verwenden, um Zugriff zu erhalten.
- **TACACS+**: Wenn diese Option ausgewählt ist, müssen die Benutzer das TACACS+-Serverkennwort verwenden, um Zugriff zu erhalten.

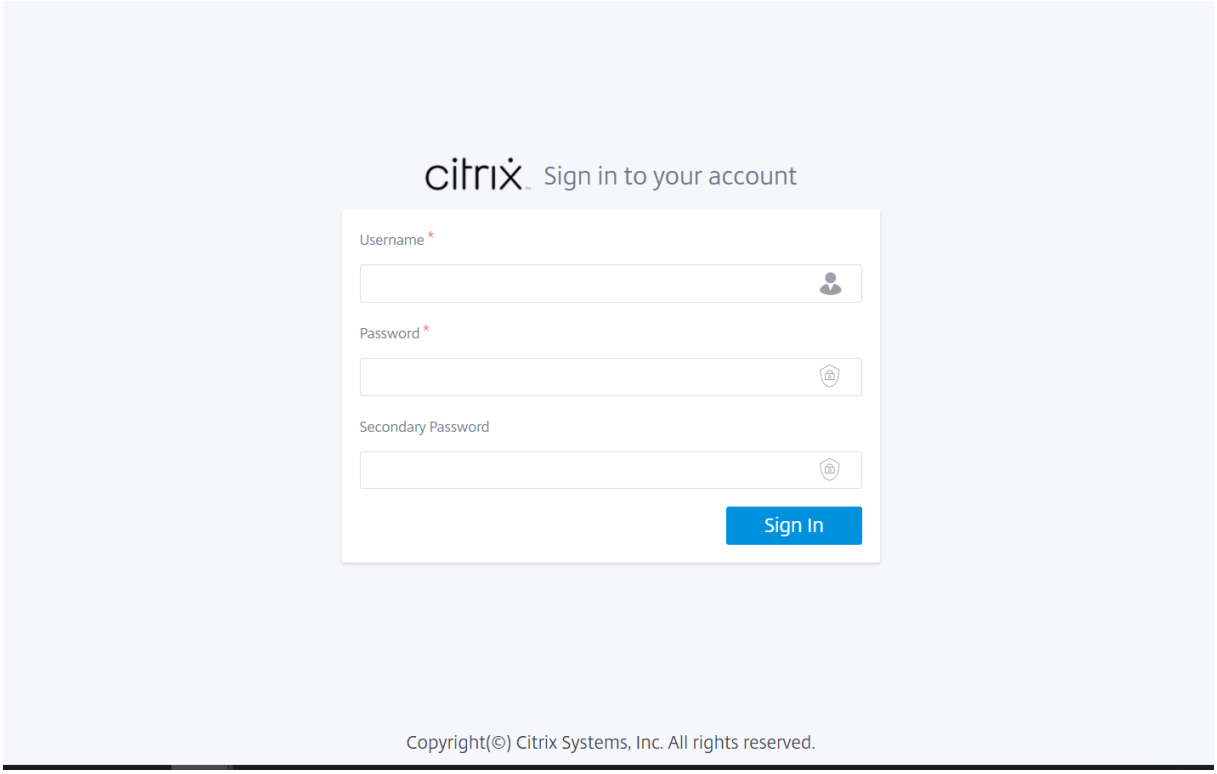
In der folgenden Tabelle sind die primären und sekundären Authentifizierungsmethoden aufgeführt, die für lokal authentifizierte Benutzer unterstützt werden:

	Typ der primären Authentifizierung	Sekundäre Authentifizierungsart
Ein-Faktor-Authentifizierung	Lokal	-
Zweistufige Authentifizierung	Lokal	RADIUS oder TACACS+

In der folgenden Tabelle sind die primären und sekundären Authentifizierungsmethoden aufgeführt, die für remote authentifizierte Benutzer unterstützt werden:

		Typ der primären Authentifizierung	Sekundäre Authentifizierungsart
	Ein-Faktor-Authentifizierung	Lokal, RADIUS oder TACACS+	-
	Zweistufige Authentifizierung	Lokal, RADIUS oder TACACS+	RADIUS oder TACACS+

Wenn die **Zwei-Faktor-Authentifizierung** aktiviert ist und die RADIUS/TACACS+-Server als sekundärer Authentifizierungstyp konfiguriert sind, ist das Feld **Sekundäres Passwort** auf der Anmeldeseite sichtbar.



Benutzer hinzufügen

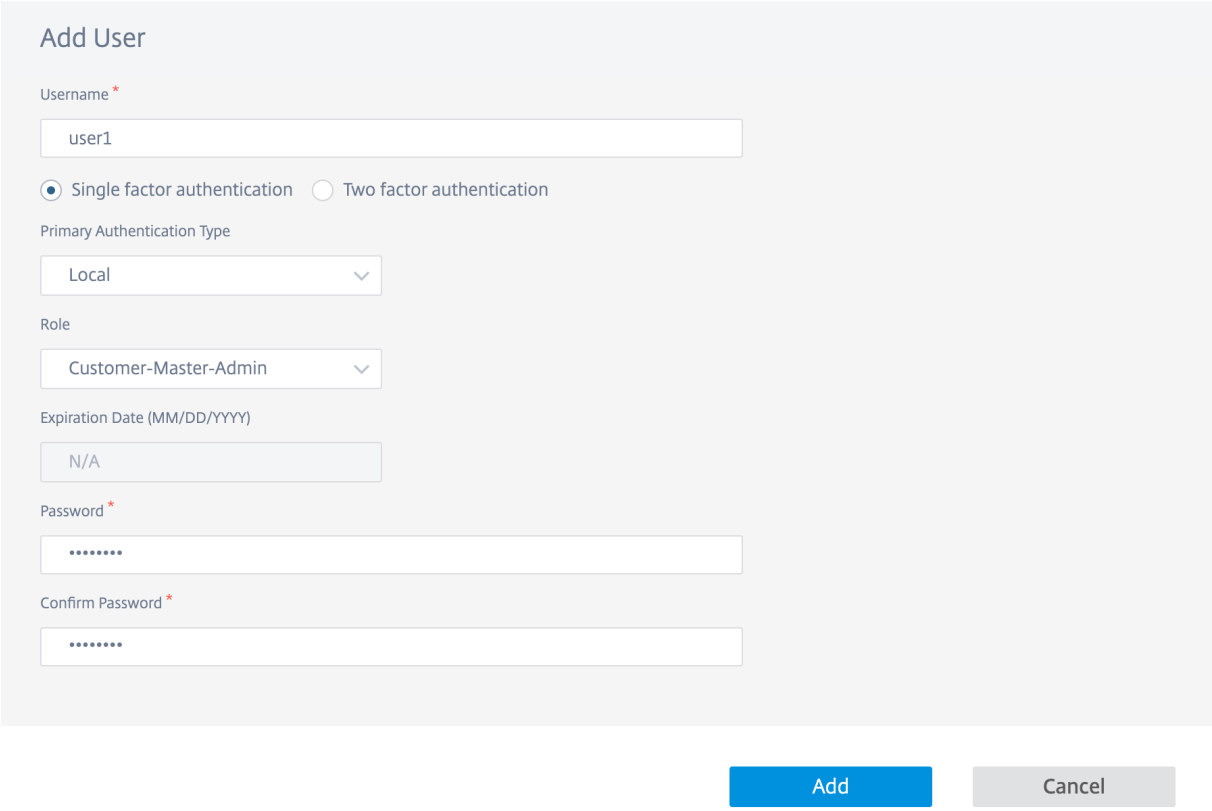
Navigieren Sie zu **Administration** > **Benutzerverwaltung** > klicken Sie auf **+ Neu** > Geben Sie die folgenden Details ein > klicken Sie auf **Hinzufügen**.

- Geben Sie den Benutzernamen ein.
- **Ein-Faktor-Authentifizierung**: Aktiviert nur die primäre Authentifizierung für die Anmeldung der Benutzer.

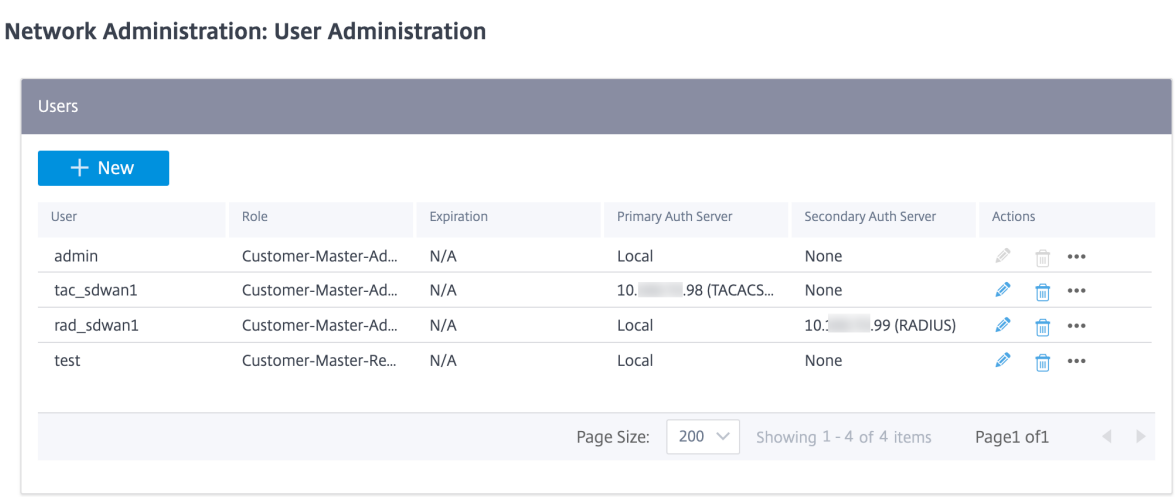
- **Zwei-Faktor-Authentifizierung**: Aktiviert sowohl die primäre als auch die sekundäre Authentifizierung für die Anmeldung der Benutzer. Weitere Informationen finden Sie unter Remoteauthentifizierungsserver.
- **Primärer Authentifizierungstyp**: Wählen Sie Lokal oder die IP-Adresse des Remoteauthentifizierungsservers aus.
- **Sekundärer Authentifizierungstyp**: Wählen Sie die IP-Adresse des Remote-Authentifizierungsservers aus.

  > **HINWEIS**
  >
  > Das Feld **Sekundärer Authentifizierungstyp** ist ausgegraut, wenn die Ein-Faktor-Authentifizierung ausgewählt ist.

- **Rolle**: Wählen Sie eine Rolle aus der Liste der verfügbaren Rollen aus.
- **Zugriff für Kunden verweigern**: (Nur auf Anbieterebene verfügbar). Beim Hinzufügen von Benutzern können Anbieter bestimmten Kunden den Zugriff verweigern.
- **Ablaufdatum (MM/TT/JJJJ)**: Das Datum, bis zu dem der Support-Benutzer Zugriff auf Kundeninformationen hat. Der Standardgültigkeitszeitraum gilt für zwei Wochen ab dem Datum, an dem die Rolle zugewiesen wird.
- Geben Sie Ihr Kennwort ein. Die Länge des Passworts muss zwischen 8 und 128 Zeichen betragen.



In der Spalte **Aktionen** können Sie die Benutzerrolle ändern, das Kennwort aktualisieren und den Authentifizierungstyp bearbeiten. Sie können den Benutzer bei Bedarf auch löschen.



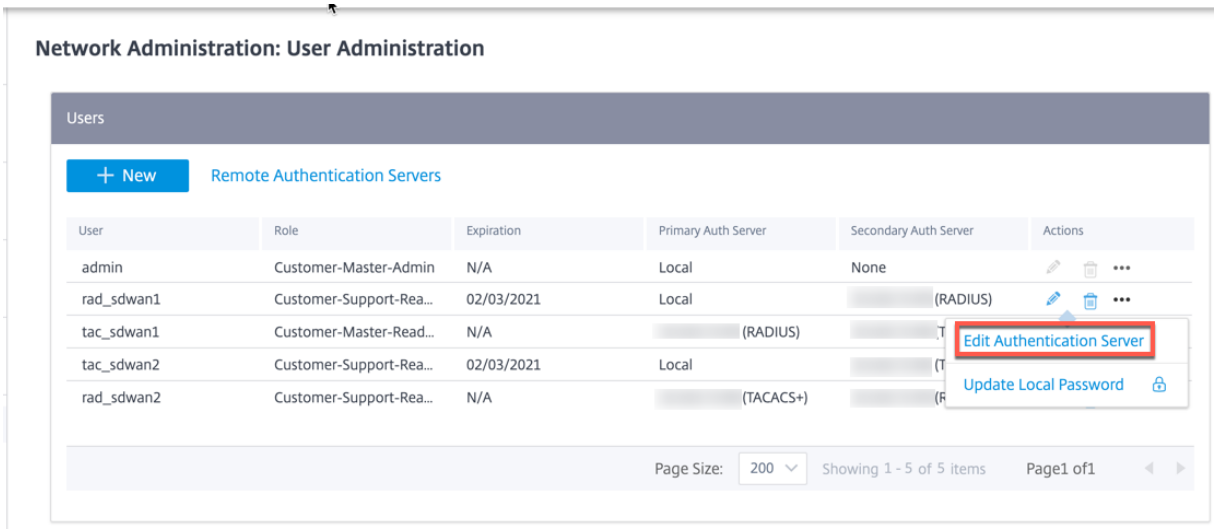
Einschränkung

Citrix SD-WAN Orchestrator for On-premises unterstützt keine Duplizierung von Benutzernamen für einen anderen Kunden unter demselben Anbieter. Wenn diese Aktion ausgeführt wird, wird **bei der Kontoerstellung die Fehlermeldung Fehler**angezeigt.

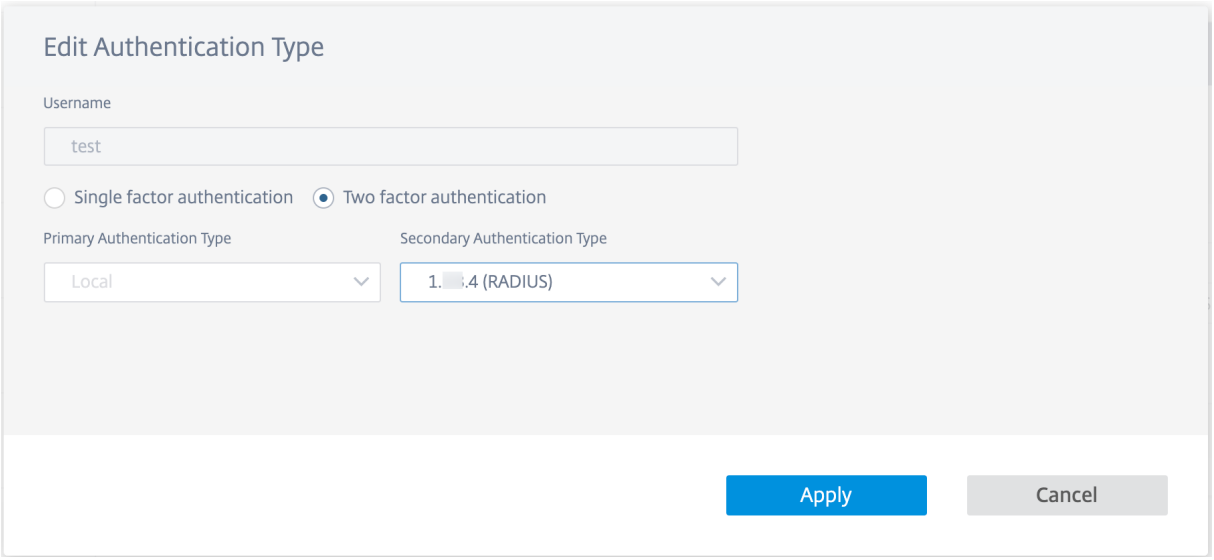
Authentifizierungstyp ändern

Sie können den Authentifizierungstyp eines Benutzers von der Einzelfaktor-Authentifizierung zur Zwei-Faktor-Authentifizierung und umgekehrt ändern.

Um den Authentifizierungstyp eines Benutzers zu ändern, klicken Sie in der Spalte **Aktionen** auf **...** und dann auf **Authentifizierungsserver bearbeiten**.



Wenn Sie derzeit die **Ein-Faktor-Authentifizierung**ausgewählt haben, können Sie zur Zwei-Faktor-Authentifizierung wechseln. Klicken Sie auf **Zwei-Faktor-Authentifizierung**, und wählen Sie den Remoteserver aus der **Dropdown-Liste Sekundärer** Klicken Sie auf **Anwenden**.



Wenn Sie derzeit die Zwei-Faktor-Authentifizierung ausgewählt haben, können Sie nur den sekundären Authentifizierungstyp ändern oder zur Ein-Faktor-Authentifizierung wechseln.

Um zur Ein-Faktor-Authentifizierung zu wechseln, klicken Sie auf **Ein-Faktor-Authentifizierung**. Die Dropdownliste **Sekundärer Authentifizierungstyp** wird deaktiviert und nur die Dropdownliste **Primärauthentifizierungstyp** ist aktiviert.

Der**primäre Authentifizierungstyp** kann nur zum Zeitpunkt der Benutzererstellung festgelegt und später nicht mehr bearbeitet werden.

Kennwort ändern

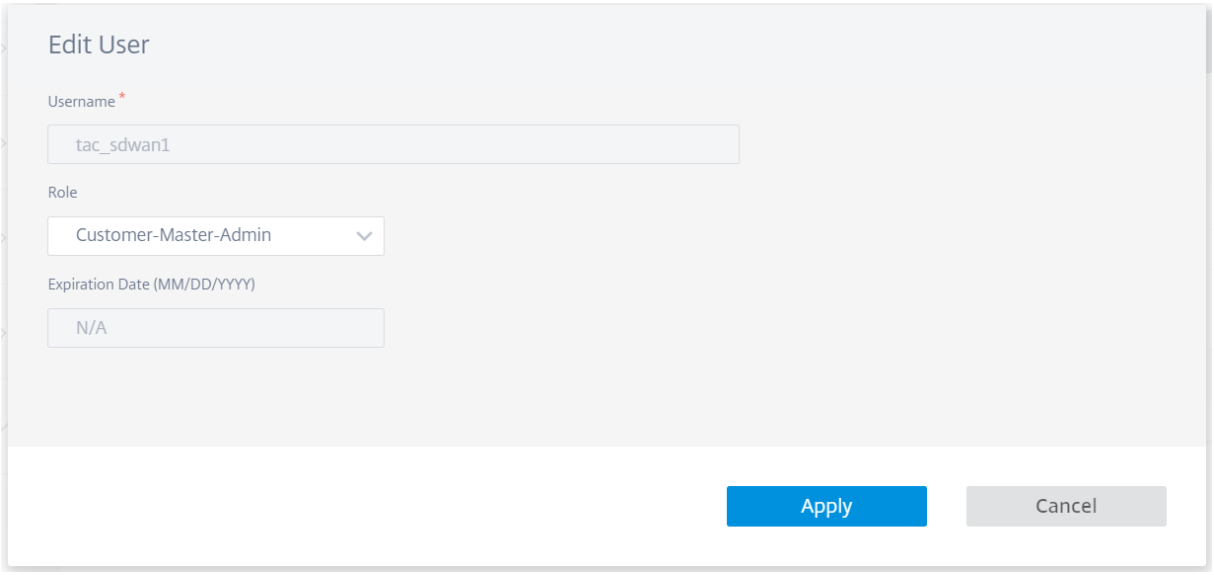
Sie können das Passwort lokaler Benutzer ändern. Um das Kennwort eines Benutzers zu ändern, klicken Sie in der Spalte **Aktionen** auf **...** und dann auf **Lokales Passwort aktualisieren**.

> **HINWEIS**
>
> Sie können das Passwort nur für lokale Benutzer ändern. Für remote authentifizierte Benutzer müssen Sie das Kennwort auf dem externen Server aktualisieren.

Benutzerrolle ändern

Um die Benutzerrolle zu ändern, klicken Sie in der Spalte **Aktionen** auf das Symbol **Bearbeiten** . Wählen Sie eine **Rolle** und klicken Sie auf **Übernehmen**

> **HINWEIS:**
>
> Sie können die Rolle des Standard-Admin-Benutzers nicht bearbeiten.



Domänenname

October 21, 2022

Der Domänenname ist eine Vanity-URL, die in der Adressleiste für den Zugriff auf Citrix SD-WAN Orchestrator for On-premises verwendet wird. Die Verwendung des Domainnamens erleichtert das Erinnern und ermöglicht es Ihnen auch, den Markennamen Ihres Unternehmens zu verwenden.

Um einen Domänennamen zu verwenden, stellen Sie sicher, dass ein lokaler DNS-Server mit einem DNS-Eintrag konfiguriert ist, der den Domänennamen mit der Citrix SD-WAN Orchestrator für die lokale Verwaltungs-IP-Adresse verknüpft. Stellen Sie sicher, dass der Domänenname während der frühen Konfiguration konfiguriert wurde Beim Einrichten eines Domänennamens werden Citrix SD-WAN Orchestrator für lokale Neustarts und Zertifikate automatisch neu generiert. Derselbe Domänenname muss auf den einzelnen Appliances konfiguriert werden. Weitere Informationen finden Sie unter On-Prem SD-WAN Orchestrator Orchestrator-Konfiguration auf der SD-WAN-Appliance.

Es ist nicht zwingend erforderlich, einen Domainnamen zu konfigurieren. Wenn Sie keinen Domänennamen haben und dennoch DNS-Server für die IP-Adressauflösung verwenden möchten, konfigurieren Sie DNS-Einträge, die auf Citrix SD-WAN Orchestrator für lokale IP verweisen, für die folgenden drei FQDNs:

- sdwanzt.citrixnetworkapi.net
- herunterladen.citrixnetworkapi.net
- sdwan-home.citrixnetworkapi.net

Wenn beispielsweise eine Citrix SD-WAN Orchestrator for On-Premises-Domäne als **citrix.com**konfiguriert

ist, müssen Sie den DNS-Eintrag auf dem DNS-Server für den folgenden FQDN und Citrix SD-WAN Orchestrator für die lokale IP-Adresse erstellen:

- download.citrix.com
- sdwanzt.citrix.com
- sdwan-home.citrix.com

In erweiterter Konfiguration:

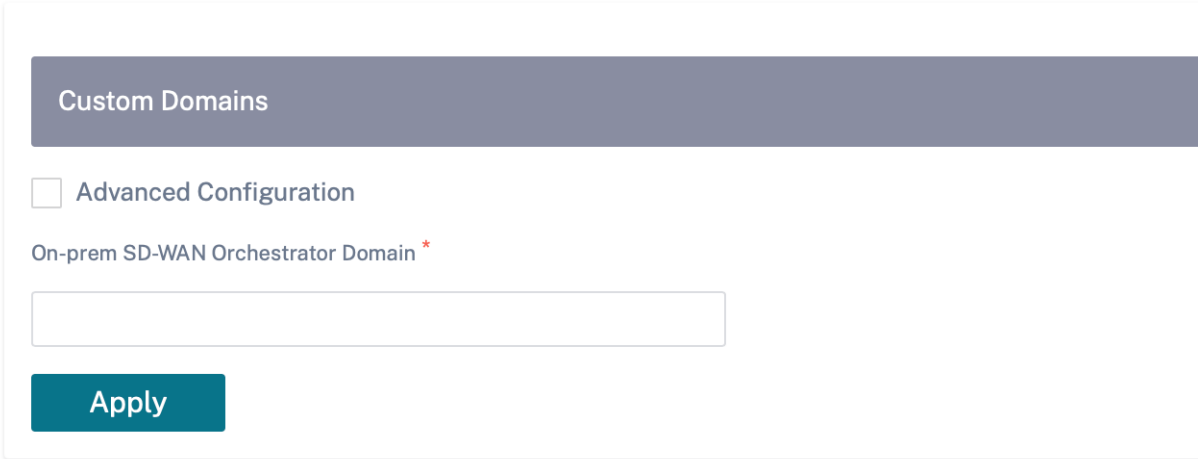
Beispiel: Wenn eine Citrix SD-WAN Orchestrator for On-Premises-Domäne als **citrix.com**konfiguriert ist, wird die **Domain des Download-Verwaltungsdienstes** als **download.citrix.com**und die **Statistikverwaltungsdienstdomäne** als **Statistik konfiguriert. citrix.com**, dann müssen Sie den DNS-Eintrag im DNS-Server für den folgenden FQDN und die entsprechende IP-Adresse erstellen:

- download.citrix.com
- sdwanzt.citrix.com
- statistics.citrix.com

Das Konfigurieren oder Ändern eines Domänennamens für eine vorhandene Konfiguration wirkt sich auf Citrix SD-WAN Orchestrator für lokale Konnektivität und Appliance-Konnektivität aus. Sie müssen den Zertifikatsauthentifizierungsprozess manuell durchführen oder die Option Zero-Touch-Bereitstellungseinstellungen der Site verwenden.

> **Hinweis:**
>
> In einem vom Anbieter verwalteten Setup haben nur Anbieteradministratoren Zugriff, um Informationen zu Domainnamen zu bearbeiten.

Um einen Domänennamen zu konfigurieren, navigieren Sie auf Netzwerkebene zu **Administration > Domänenname**, und geben Sie einen Citrix SD-WAN Orchestrator für den lokalen Domänennamen an.



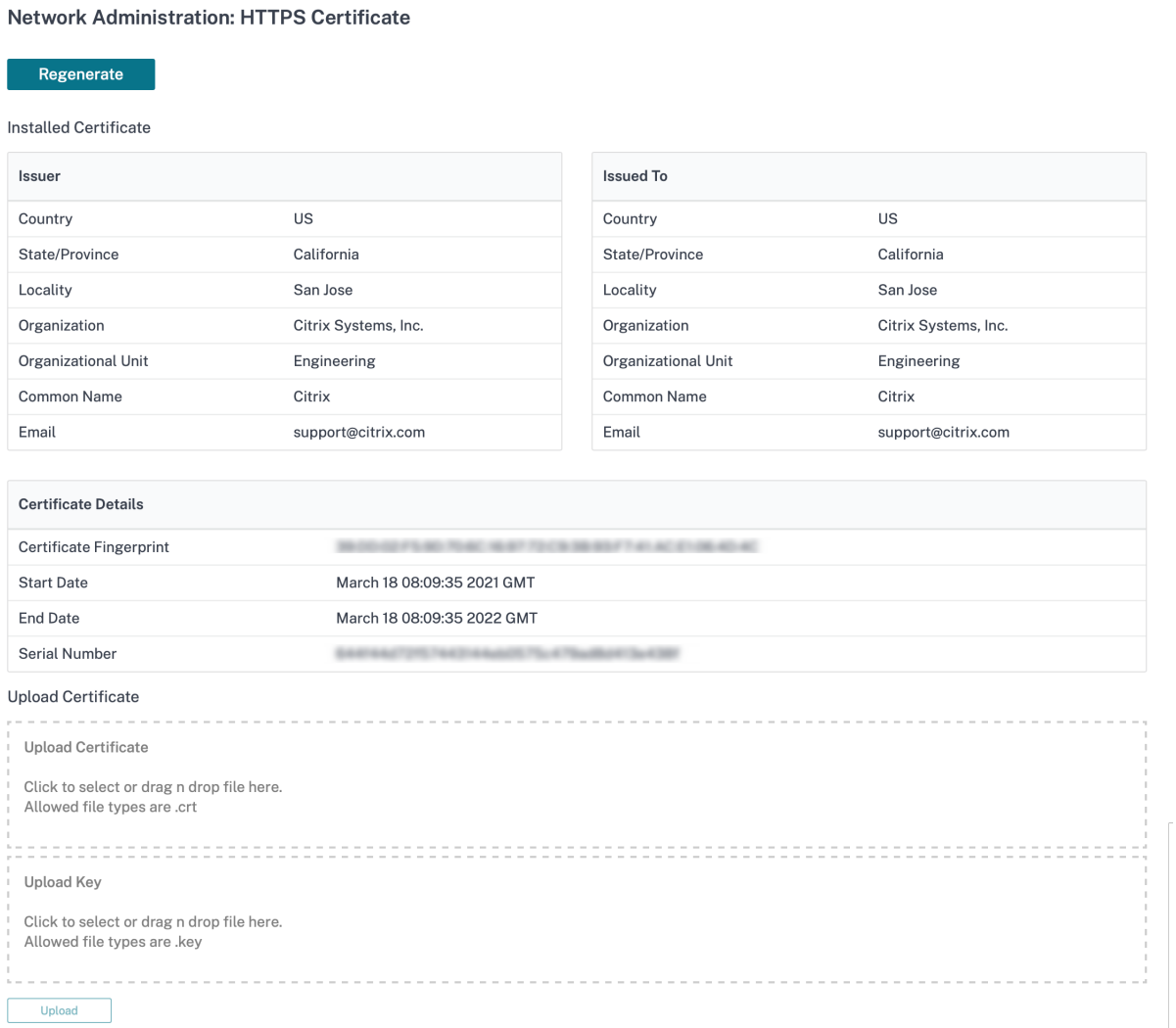
HTTPS-Zertifikat

October 21, 2022

Ein HTTPS-Zertifikat ist erforderlich, um eine sichere HTTPS-Verwaltungsverbindung mit Citrix SD-WAN Orchestrator for On-premises herzustellen. Sie können das Standard-HTTPS-Zertifikat verwenden, das auf dem Citrix SD-WAN Orchestrator for On-premises GUI verfügbar ist, oder ein benutzerdefiniertes HTTPS-Zertifikat hochladen, das aus einem anderen Framework wie OpenSSL oder von einer vertrauenswürdigen Stelle generiert wurde. Mit dem benutzerdefinierten HTTPS-Zertifikat haben Sie die Kontrolle über die Sicherheit und die anderen Betreffparameter im Zusammenhang mit dem Zertifikat.

Um das Standardzertifikat anzuzeigen, navigieren Sie zu **Administration > HTTPS-Zertifikat**.

> **Hinweis**
>
> In einem vom Anbieter verwalteten Setup haben nur Anbieteradministratoren Zugriff, um das HTTPS-Zertifikat neu zu generieren und hochzuladen.



Der Abschnitt **Installiertes Zertifikat** enthält eine Zusammenfassung des auf der Appliance installierten Zertifikats. Die Appliance verwendet dieses Zertifikat, um sich im Netzwerk zu identifizieren.

Der Abschnitt **Ausgestellt** für enthält Einzelheiten darüber, an wen das Zertifikat ausgestellt wurde. Der **allgemeine Name** im Zertifikat stimmt mit dem Namen der Appliance überein, da das Zertifikat an den Appliance-Namen gebunden ist. Der Abschnitt **Aussteller** enthält die Details der Zertifizierungsstelle, die das Zertifikat unterzeichnet hat. Zu den Zertifikatsdetails gehören der Fingerabdruck des Zertifikats, die Seriennummer und die Gültigkeitsdauer des Zertifikats.

Um das Zertifikat neu zu generieren, navigieren Sie zu **Administration > HTTPS-Zertifikat** und klicken Sie auf **Neu generieren**.

> **Hinweis:**
>
> Durch das erneute Generieren des Zertifikats werden alle vorhandenen verbundenen HTTPS-Sitzungen getrennt und der HTTPS-Server neu gestartet. Nachdem das Zertifikat erfolgreich neu

> generiert wurde, wird die GUI automatisch aktualisiert.

Sie können HTTPS-Zertifikate aus jedem anderen Framework wie OpenSSL oder von einer vertrauenswürdigen Behörde generieren und auf den Citrix SD-WAN Orchestrator for On-premises hochladen. Das unterstützte Zertifikatsformat ist .crt und das unterstützte Schlüsselformat ist .key.

Um ein benutzerdefiniertes HTTPS-Zertifikat **hochzuladen, klicken Sie auf Hochladen** oder ziehen Sie das Zertifikat und die Schlüsseldateien in die Felder **Zertifikat hochladenbzw. Schlüssel hochladen** . Nach erfolgreichem Upload wird die GUI automatisch aktualisiert.

Verwaltung des Festplattenspeichers

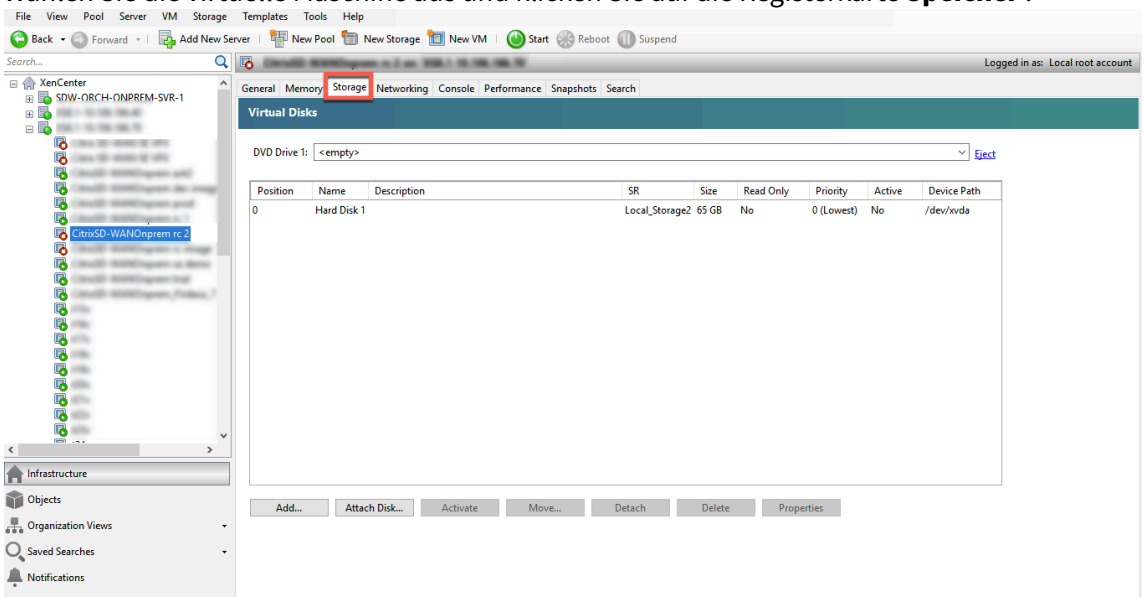
October 21, 2022

Sie können den für Citrix SD-WAN Orchestrator for On-premises zugewiesenen Speicherplatz erhöhen.

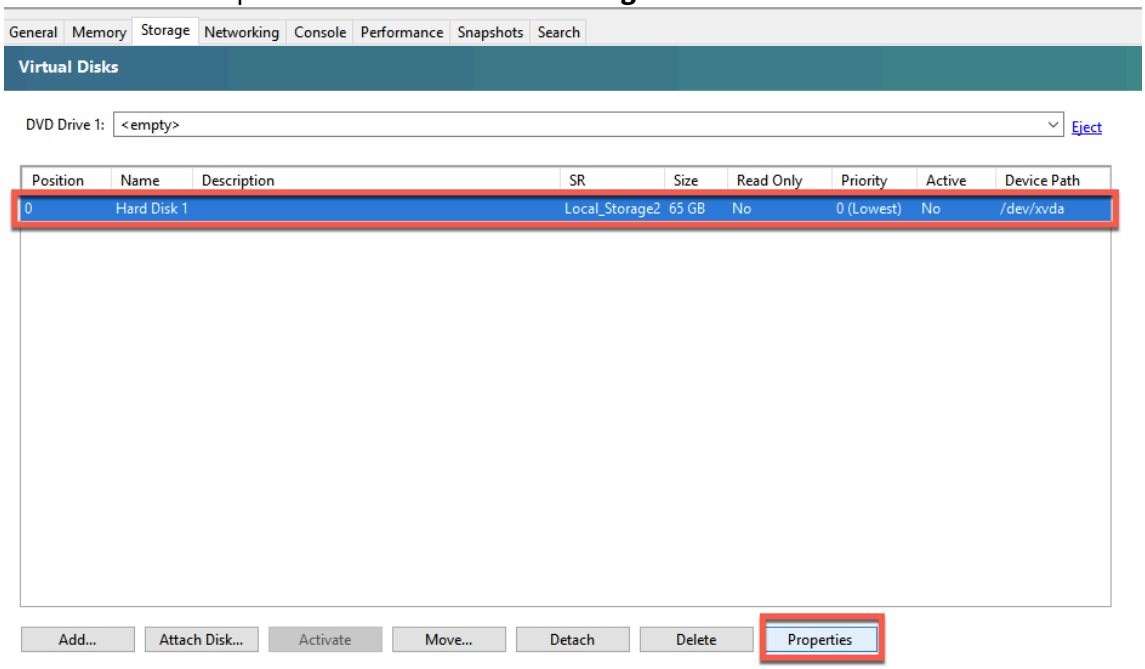
Erhöhen Sie den Speicherplatz auf Citrix Hypervisor

Um den Speicherplatz auf Citrix Hypervisor zu erhöhen.

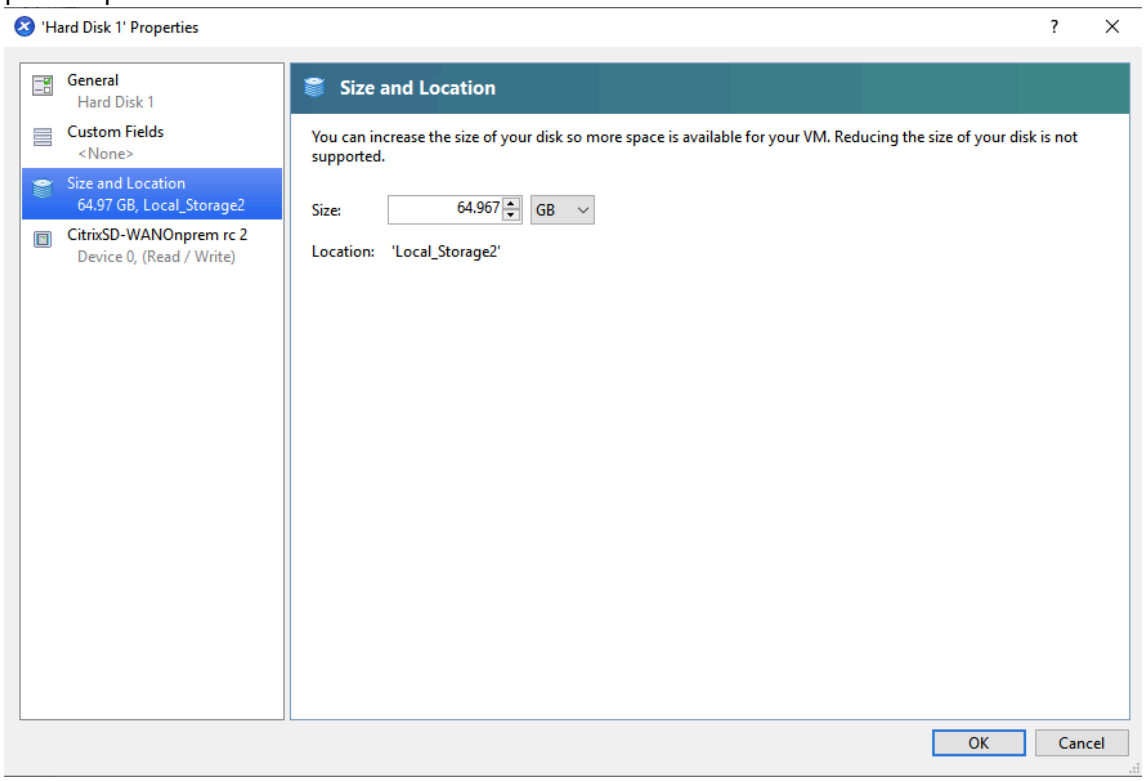
1. Fahren Sie die virtuelle Maschine (VM) vom Hypervisor herunter.
2. Wählen Sie die virtuelle Maschine aus und klicken Sie auf die Registerkarte **Speicher** .



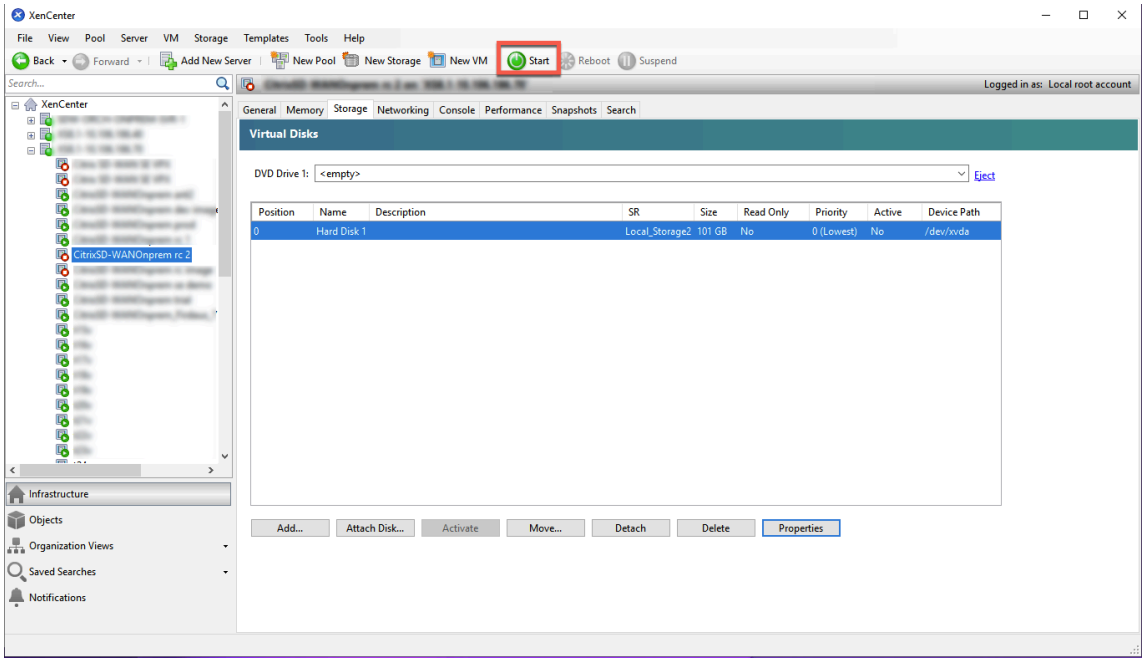
3. Wählen Sie die Festplatte aus und klicken Sie auf **Eigenschaften**.



4. Klicken Sie auf die Option **Größe und Speicherort** und aktualisieren Sie die **Größe** Ihres Festplattenspeichers. Klicken Sie auf **OK**.



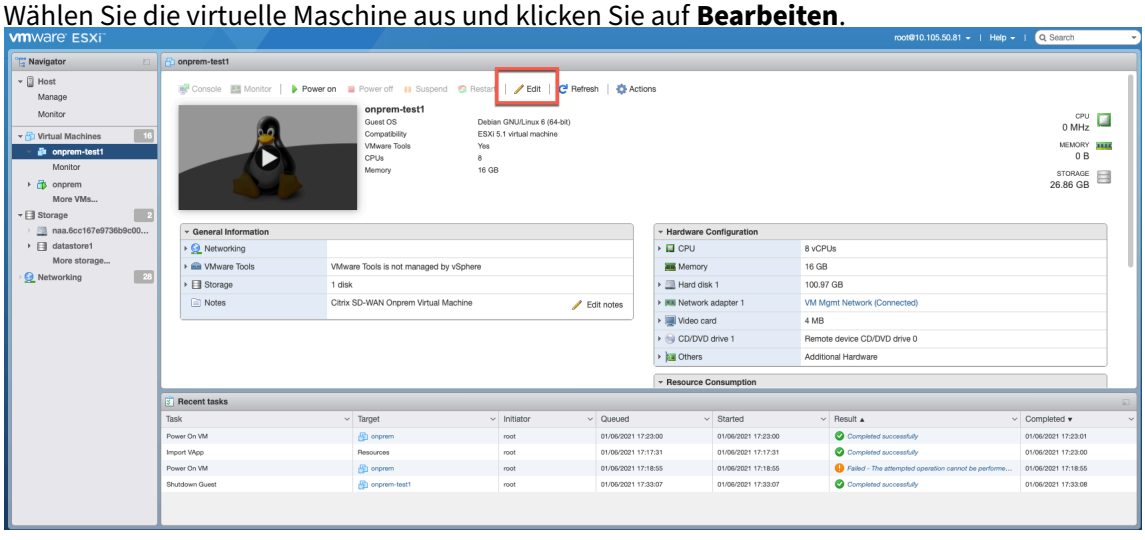
5. Klicken Sie auf **Starten**.



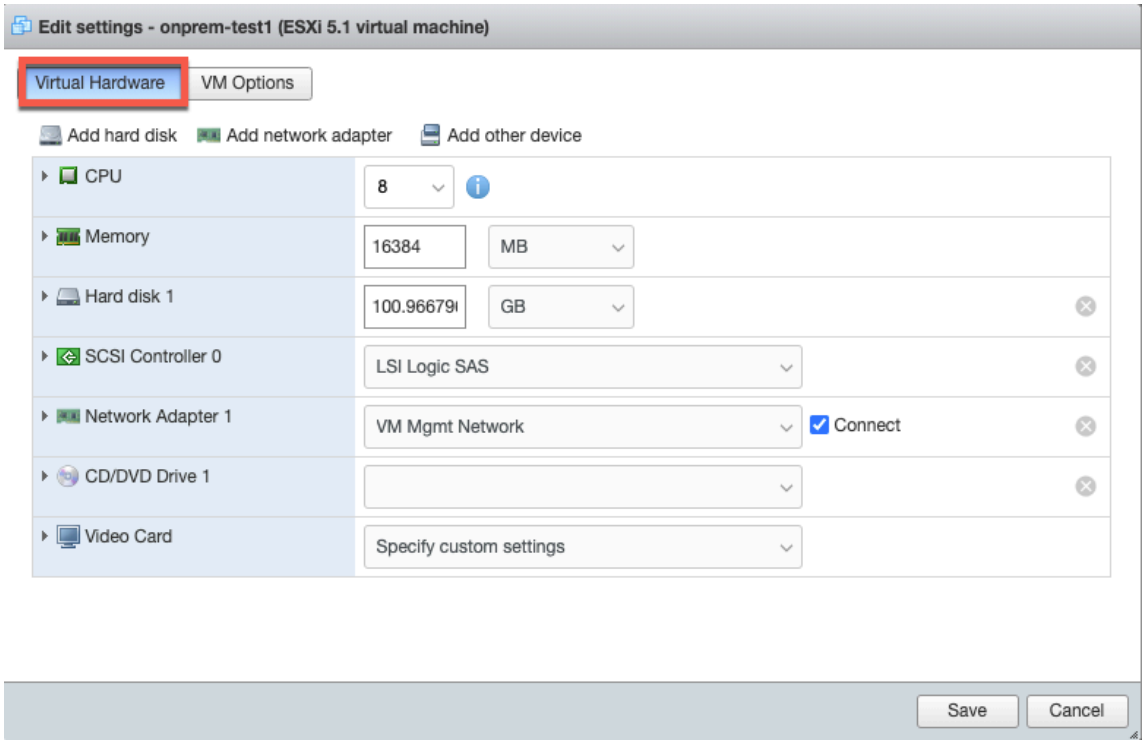
Erhöhen Sie den Speicherplatz auf dem ESXi Server

Um den Festplattenspeicher auf dem ESXi-Server zu erhöhen.

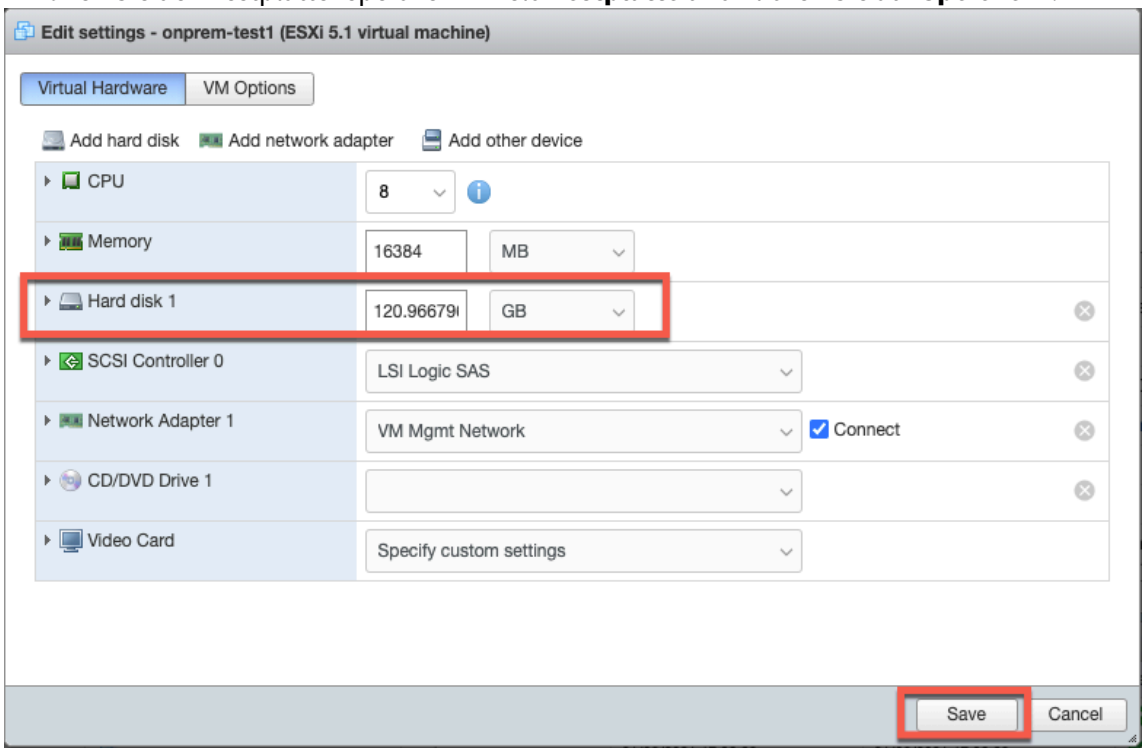
1. Fahren Sie die virtuelle Maschine (VM) vom Hypervisor herunter.
2. Wählen Sie die virtuelle Maschine aus und klicken Sie auf **Bearbeiten**.



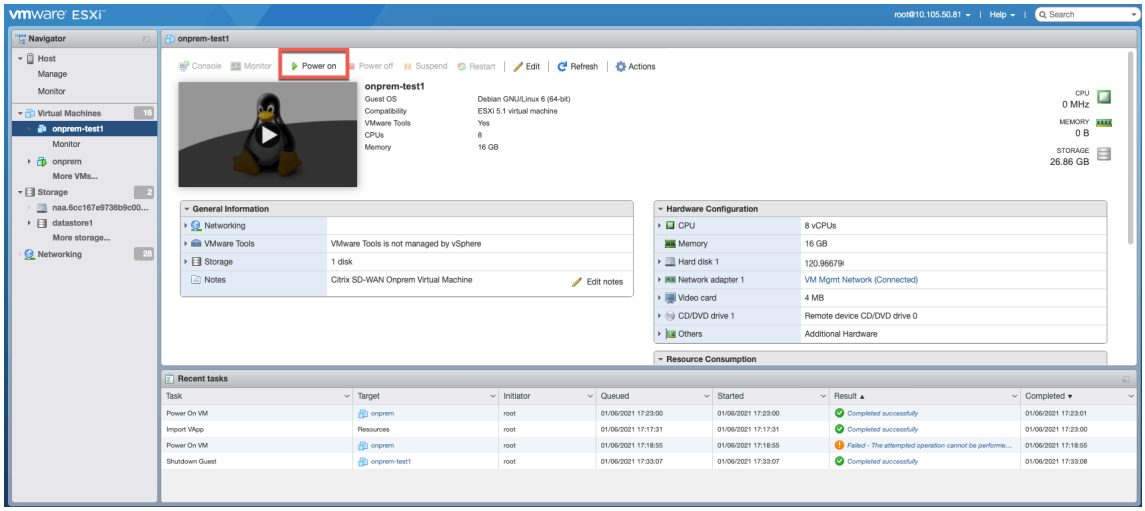
3. Wählen Sie die Registerkarte **Virtuelle Hardware** .



4. Erhöhen Sie den Festplattenspeicher im Feld **Festplatte** und klicken Sie auf **Speichern**.



5. Klicken Sie **auf Einschalten**.



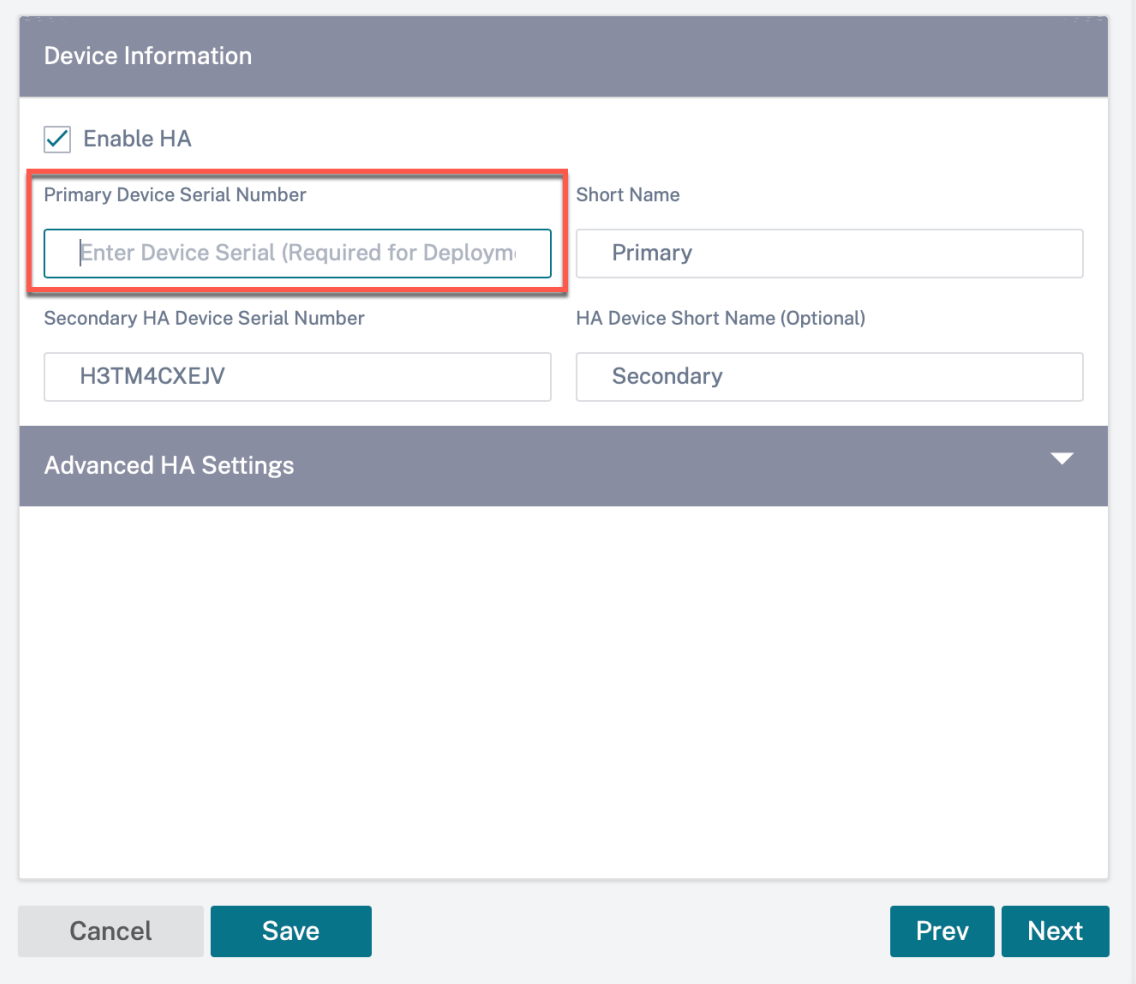
Ersetzen Sie eine betroffene Citrix SD-WAN-Appliance

October 21, 2022

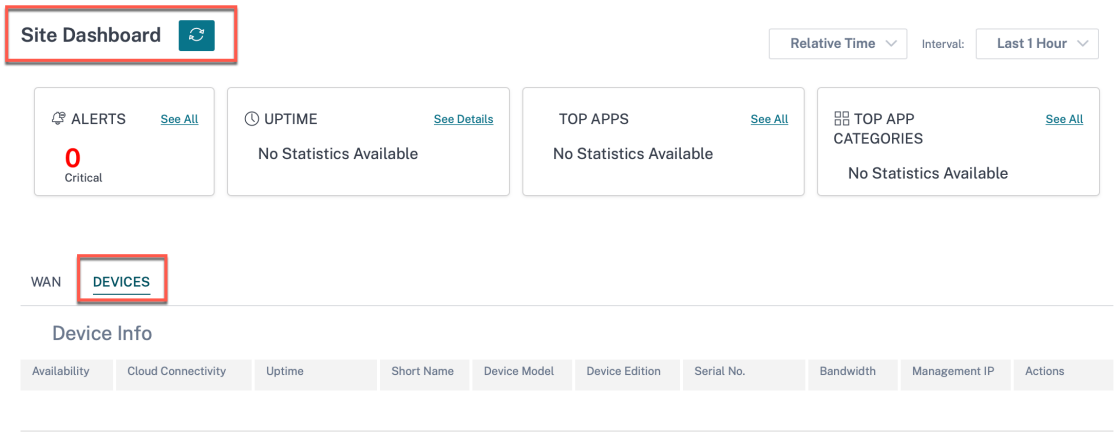
So ersetzen Sie eine betroffene Appliance in Citrix SD-WAN Orchestrator for On-premises:

1. Melden Sie sich bei Citrix SD-WAN Orchestrator for On-premises an und wählen Sie die betroffene Site aus. Navigieren Sie auf Standortebene zu **Konfiguration > Standortkonfiguration > Geräteinformationen**, und entfernen Sie die Seriennummer aus dem Feld **Seriennummer des primären Geräts** . Klicken Sie auf **Speichern**.

   > **Hinweis:**
   >
   > Wenn die Appliance weiterhin über Citrix SD-WAN Orchestrator for On-premises erreichbar ist, befindet sich die Appliance im Status „Auf Werkseinstellungen zurückgesetzt“.

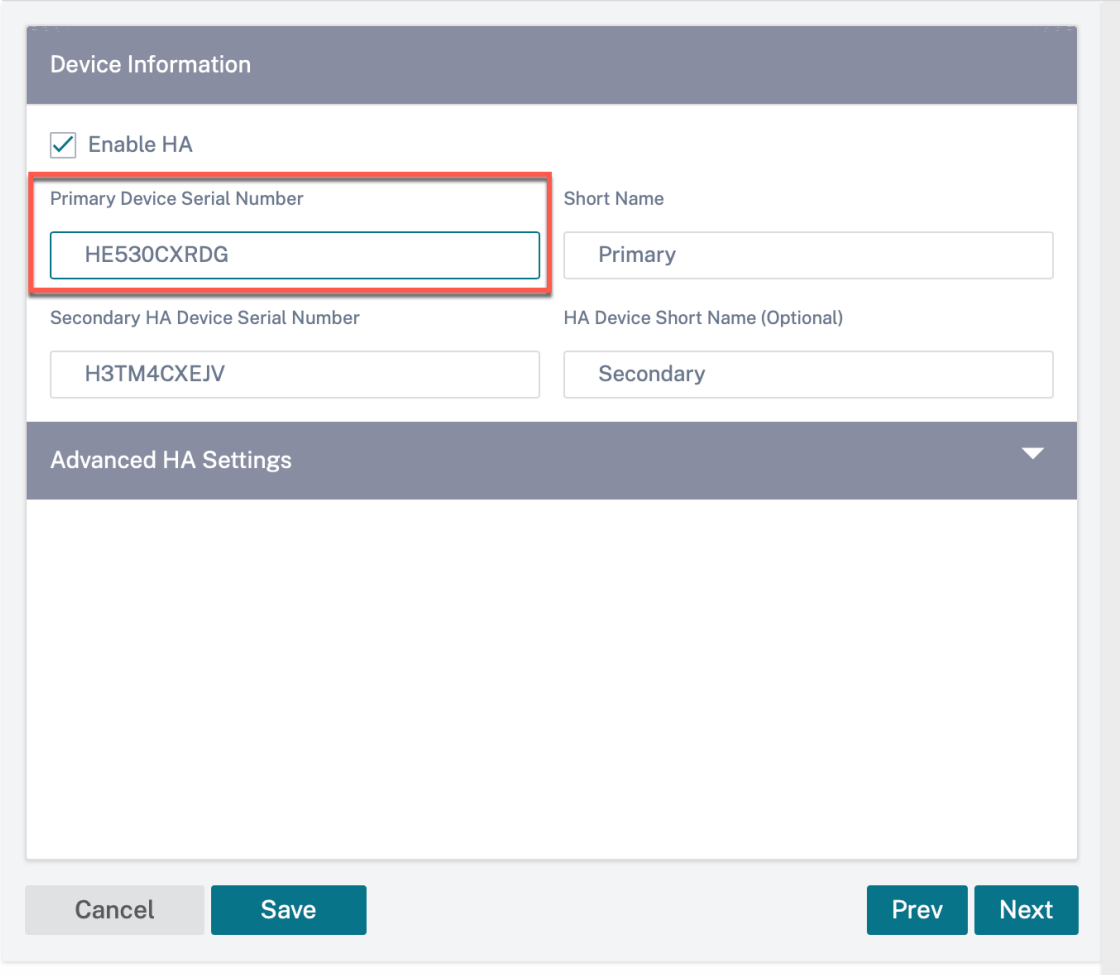


2. Navigieren Sie zu **Dashboard > Geräte** und stellen Sie sicher, dass die betroffene Appliance aus der Liste entfernt wurde.

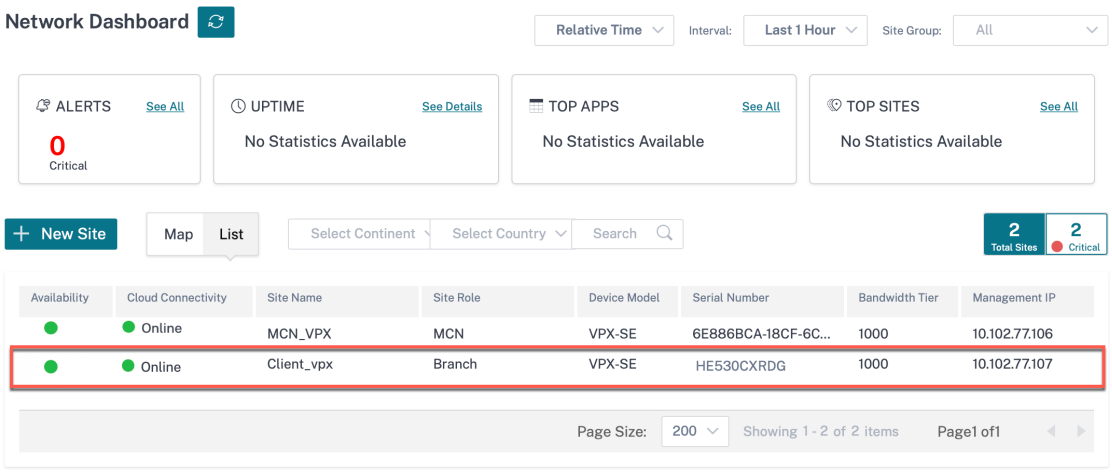


3. Notieren Sie sich die Stromversorgung und Verkabelung des betroffenen Geräts und nehmen Sie das Gerät dann aus dem Rack.

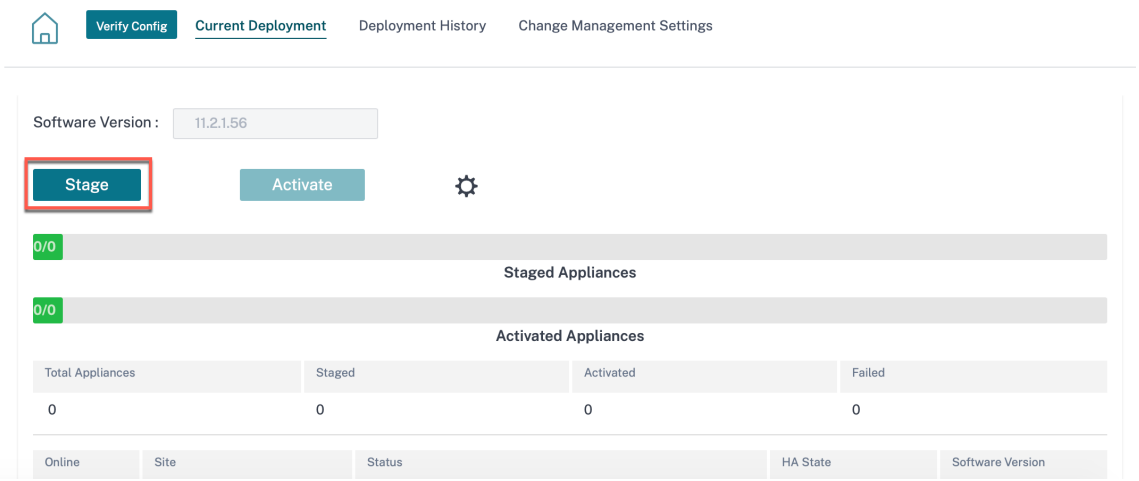
4. Montieren Sie das neue Gerät auf dem Rack und wiederholen Sie die Stromversorgung und Verkabelung wie für das betroffene Gerät.
5. Navigieren Sie in der Benutzeroberfläche von Citrix SD-WAN Orchestrator for On-premises auf Standortebene zu **Konfiguration > Standortkonfiguration > Gerätedetails**. Fügen Sie die Seriennummer der neuen Appliance in das Feld **Seriennummer des primären Geräts** ein. Klicken Sie auf **Speichern**.



6. Zero-Touch-Bereitstellung konfigurieren. Weitere Informationen finden Sie unter Zero-Touch-Bereitstellung.
7. Warten Sie der Appliance einige Minuten, um die Cloud-Konnektivität im Site-Dashboard zu aktualisieren.



8. Navigieren Sie auf Netzwerkebene zu **Konfiguration > Network Config Home** und klicken Sie auf **Konfiguration/Software bereitstellen**.
9. Klicken Sie auf **Bühne**.



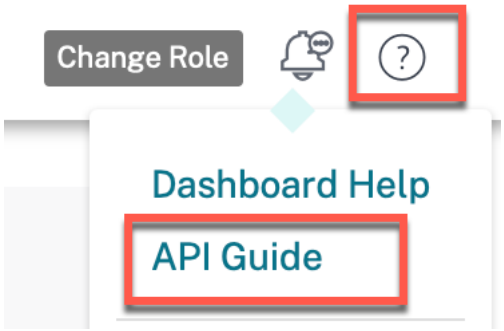
10. Klicken Sie nach Abschluss der Bereitstellung auf **Aktivieren** .
11. Navigieren Sie zum Site-Dashboard und überprüfen Sie die erfolgreiche Aktivierung der Appliance.

API-Leitfaden für Citrix SD-WAN Orchestrator for On-premises

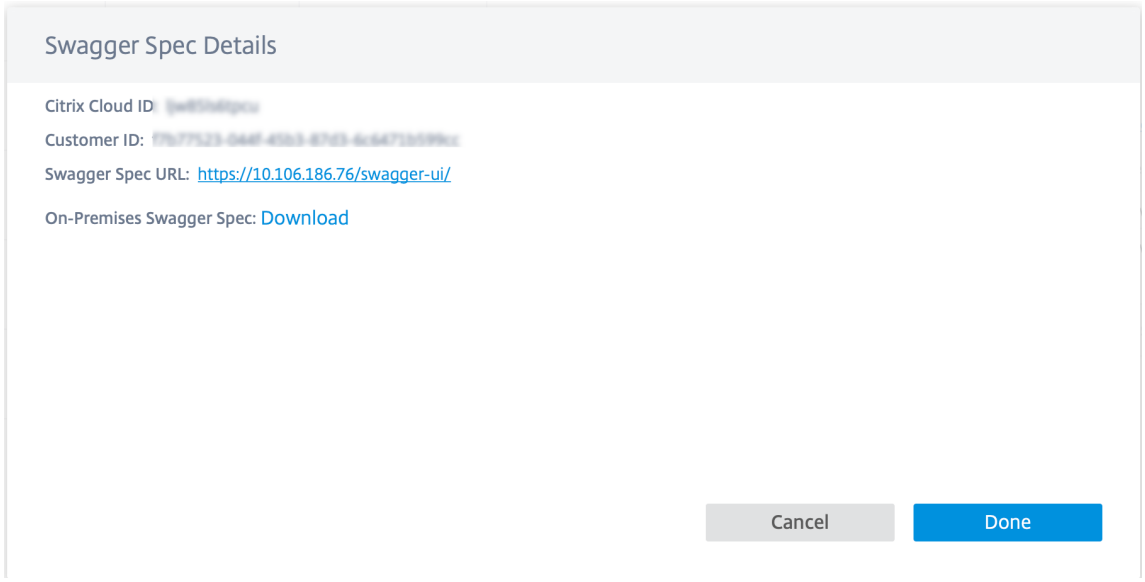
October 21, 2022

So greifen Sie auf das Citrix SD-WAN Orchestrator for On-premises API-Handbuch auf der Swagger-Benutzeroberfläche zu:

1. Melden Sie sich beim Citrix SD-WAN Orchestrator for On-premises an und klicken Sie auf **?** in der oberen rechten Ecke der Benutzeroberfläche und klicken Sie dann auf **API Guide**.



Die Details der Swagger-Spezifikation werden angezeigt.



2. Klicken Sie auf die Swagger-Spezifikations-URL, um auf den API-Leitfaden zuzugreifen.

Citrix SD-WAN Orchestrator für lokale APIs durch curl

Voraussetzungen

- Cloud-Anmeldung
- Lokaler Login

Führen Sie die folgenden Schritte aus, um Citrix On-premises Orchestrator-APIs über curl zu verwenden:

1. **Cloud-Login**: Im Falle einer neuen XVA müssen Sie sich zuerst in der Cloud anmelden.

```
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  '
```

Die `clientIdclientSecret`, und `ccId` können auf der IAM-Seite abgerufen werden.

> **Hinweis Stellen Sie**
>
> sicher, dass das Kundenkonto bereits in der Cloud erstellt wurde, bevor Sie die Cloud-Anmeldung versuchen.

2. **Lokale Anmeldung**: Führen Sie dann eine lokale Anmeldung durch, um das Auth-Token zu erhalten.

```
1  curl -k -X POST -H "Content-Type: application/json" https://<
       onprem-orchestrator-ip>/onpm/v1/logon --data '{
2   "username":"admin","password":"<passwordField>" }
3   '
```

Dies gibt **Token** und **CustomerID** als Antwort zurück. Die CustomerID bleibt fest und wird in anderen API-Aufrufen benötigt. Speichern Sie die **CustomerID** für die spätere Verwendung. Das Token bleibt eine Stunde lang gültig. Später müssen Sie eine neue Anmeldung durchführen.

Beispiel: Verwenden Sie das **Auth-Token** und die **CustomerID**, um andere lokale Citrix APIs auszulösen.

```
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
```

Orchestrator-Verwaltung

October 21, 2022

In diesem Abschnitt finden Sie Informationen zu administrativen Aktivitäten, die auf der Citrix SD-WAN Orchestrator for On-Premises-Plattform ausgeführt werden können.

Software

Sie können die Softwareversion der Citrix SD-WAN-Appliance herunterladen, die für alle Appliances in Ihrem Netzwerk erforderlich ist und in Citrix SD-WAN Orchestrator for On-premises gespeichert ist. Verwenden Sie die gespeicherte Software, um Ihre Citrix SD-WAN Orchestrator for On-Premises-Software auf die neueste Version zu aktualisieren.

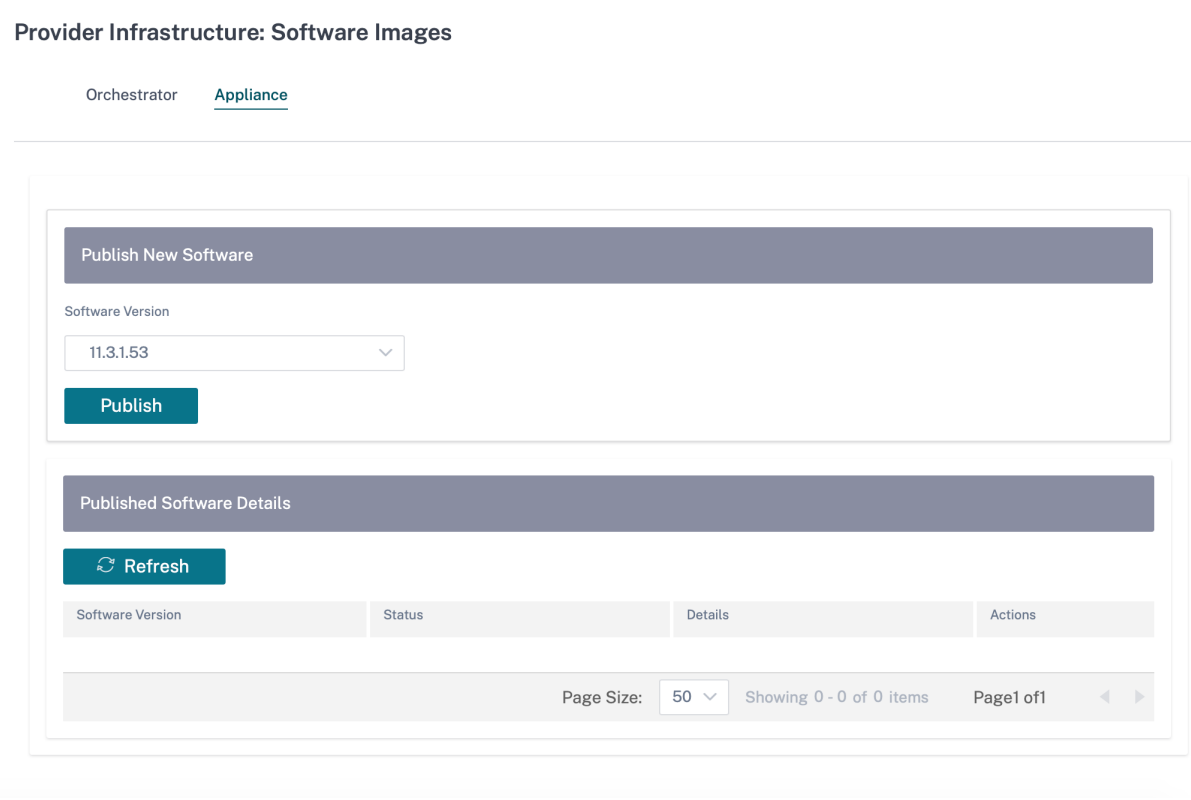
> **Hinweis:**
>
> Das vom Anbieter verwaltete Setup wird von Citrix SD-WAN Orchestrator for On-premises 10.3 eingeführt. Ein Downgrade auf Softwareversionen, die niedriger als die Version Citrix SD-WAN Orchestrator for On-premises 10.3 sind, wird nicht unterstützt.

Software veröffentlichen

In einem vom Anbieter verwalteten Setup ermöglicht Citrix SD-WAN Orchestrator for On-premises Anbieteradministratoren das Herunterladen der Citrix SD-WAN-Appliance-Softwareversion, die für alle Appliances in Ihrem Netzwerk erforderlich ist. Anbieteradministratoren können die heruntergeladene Softwareversion veröffentlichen. Die veröffentlichte Software wird heruntergeladen und in Citrix SD-WAN Orchestrator for On-premises gespeichert. Kundenadministratoren können die veröffentlichte Software auf allen Appliances bereitstellen, die von Citrix SD-WAN Orchestrator for On-premises verwaltet werden.

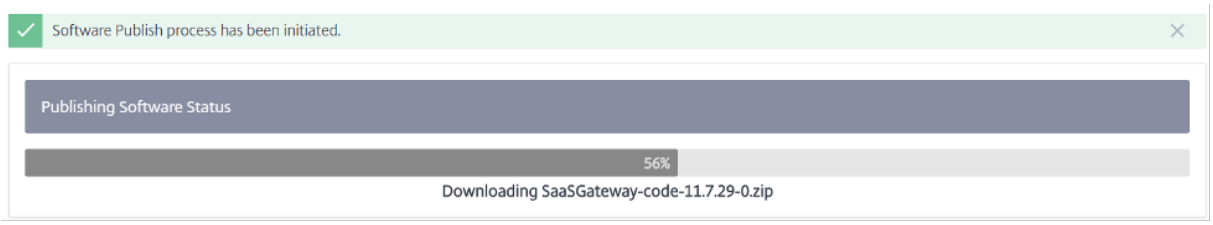
In einem vom Kunden verwalteten Setup können Kundenadministratoren die Citrix SD-WAN-Appliance-Softwareversion herunterladen, die für alle Appliances im Netzwerk erforderlich ist. Sie können die Software in Citrix SD-WAN Orchestrator for On-premises veröffentlichen und die Software auf allen Appliances bereitstellen.

Um Software zu veröffentlichen, navigieren Sie zu **Infrastruktur > Orchestrator-Administration > Software-Images > Appliance**.

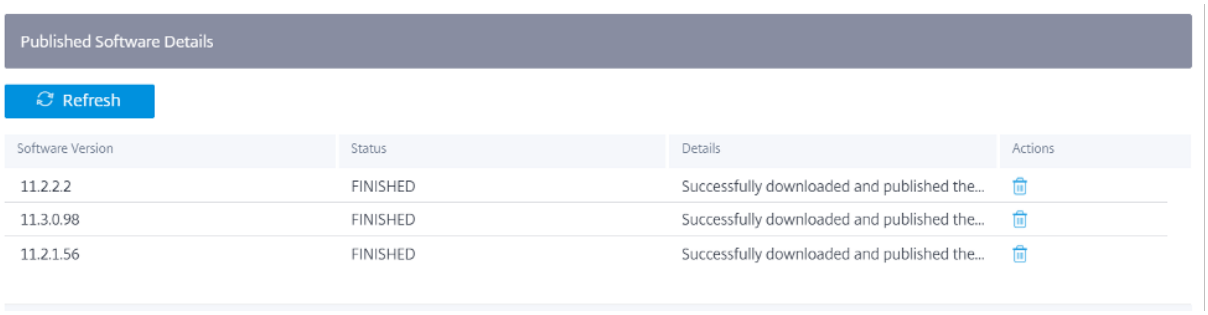


Sie können eine zu veröffentlichende Softwareversion aus einer vorgefertigten Liste von Softwareversionen auswählen, die vom aktuellen Citrix SD-WAN Orchestrator for On-premises unterstützt werden. Für neuere Softwareversionen, die nicht in der Liste verfügbar sind, führen Sie ein Upgrade auf die neueste Version von Citrix SD-WAN Orchestrator for On-premises durch, die die neue Softwareversion unterstützt. Informationen zum Upgrade von Citrix SD-WAN Orchestrator for On-premises finden Sie unter Softwareupgrade.

Citrix SD-WAN Orchestrator for On-premises lädt die Citrix SD-WAN-Software der ausgewählten Version für alle Plattformen herunter. Ein Fortschrittsbalken zeigt den Fortschritt des Veröffentlichungsprozesses an.



Die veröffentlichten Softwareversionen werden unter **Details zur veröffentlichten Software**angezeigt. Zu jedem Zeitpunkt kann Citrix SD-WAN Orchestrator for On-premises bis zu drei veröffentlichte Softwareversionen speichern. Wenn Sie beabsichtigen, eine weitere Softwareversion zu veröffentlichen, löschen Sie eine der drei verfügbaren Versionen, bevor Sie mit der Veröffentlichung beginnen.



Nach erfolgreicher Veröffentlichung können Sie die Software auf der Seite **Netzwerkkonfiguration** für alle Appliances im Netzwerk bereitstellen, bereitstellen und aktivieren. Weitere Informationen finden Sie unter Netzwerkkonfiguration. Stellen Sie für eine erfolgreiche Bereitstellung sicher, dass alle Appliances mit Citrix SD-WAN Orchestrator for On-premises verbunden sind. Weitere Informationen finden Sie unter Konnektivität mit Citrix SD-WAN-Appliances.

Software-Upgrade

In einem vom Anbieter verwalteten Setup können nur Anbieteradministratoren die Citrix SD-WAN Orchestrator for On-Premises-Software auf die neueste Version aktualisieren.

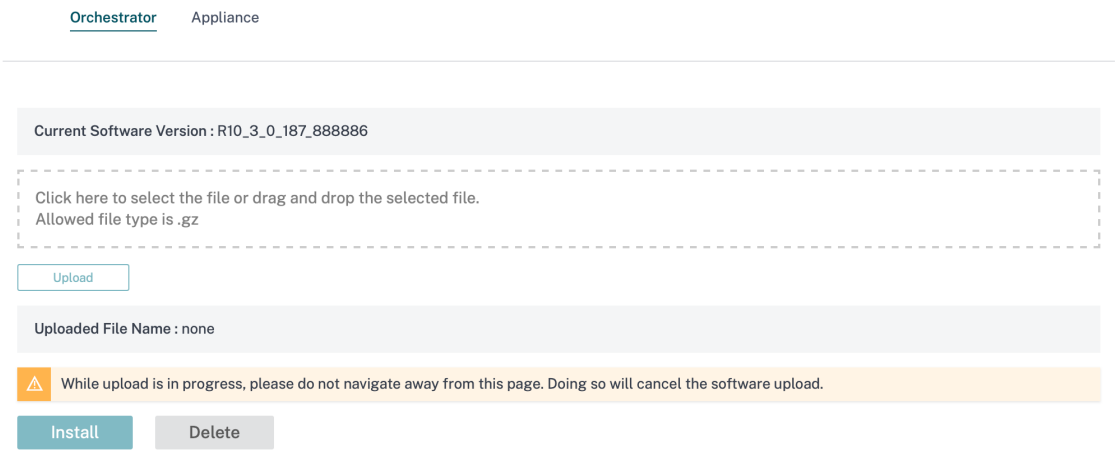
In einem vom Kunden verwalteten Setup können Kundenadministratoren Citrix SD-WAN Orchestrator for On-Premises-Software auf die neueste Version aktualisieren.

> **HINWEIS:**
>
> - Laden Sie das entsprechende Citrix SD-WAN Orchestrator for On-Premises-Softwarepaket auf Ihren lokalen Computer herunter. Sie können dieses Paket von der Downloads-Seite herunterladen.
> - Citrix empfiehlt, Snapshots der virtuellen Maschine im Hypervisor zu erstellen. Außerdem wird die SD-WAN-Konfiguration vor dem Upgrade heruntergeladen.
> - Citrix empfiehlt außerdem, regelmäßig Snapshots der VM- und SD-WAN-Konfigurationen

> zu erstellen.

Führen Sie die folgenden Schritte aus, um eine neue Version der Citrix SD-WAN Orchestrator for On-Premises-Software hochzuladen und zu installieren:

1. Navigieren Sie in der Benutzeroberfläche von Citrix SD-WAN Orchestrator for On-Premises zu **Infrastruktur > Orchestrator-Administration > Software-Images > Orchestrator**.
2. Klicken Sie in das Feld und wählen Sie die ctx-onprem-1 (spätestes Datum) .tar.gz-Binärdatei aus, die Sie heruntergeladen und auf Ihrem lokalen System gespeichert haben.



3. **Klicken Sie auf Hochladen, um das ausgewählte Softwarepaket auf die aktuelle virtuelle Maschine Citrix SD-WAN Orchestrator for On-premises hochzuladen.**
4. Nachdem der Upload abgeschlossen ist, klicken Sie auf **Installieren**.
5. Wenn Sie zur Bestätigung aufgefordert werden, klicken Sie auf **Installieren**.

Verwaltungs-Einstellungen

> **Hinweis:**
>
> In einem vom Anbieter verwalteten Setup haben nur Anbieteradministratoren Zugriff zum Bearbeiten der Konfiguration unter **Infrastruktur > Orchestrator-Administration > Verwaltungseinstellungen**.

IP-Verwaltung und DNS

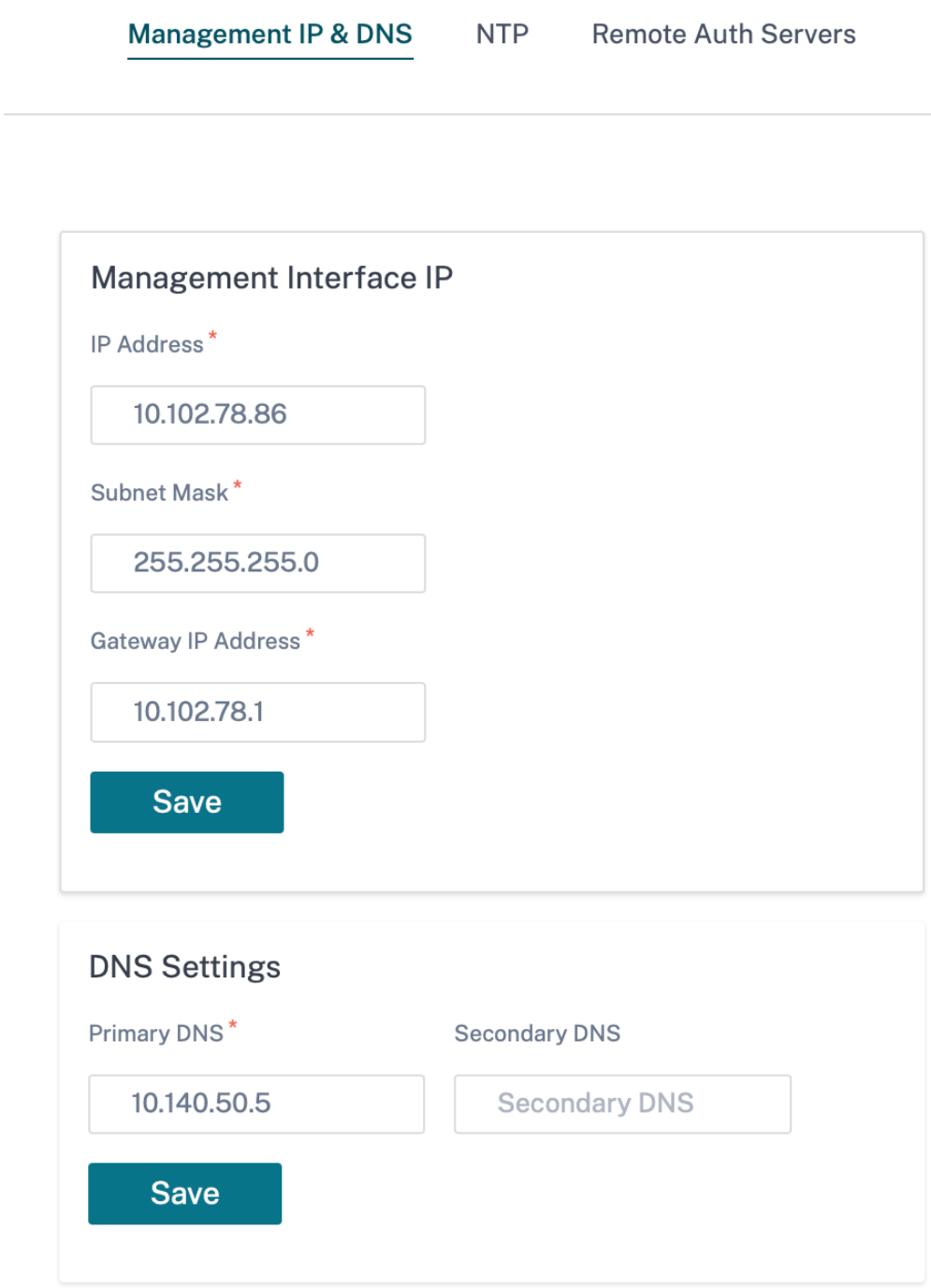
Nachdem Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen (VM) bereitgestellt und eine Verwaltungs-IP entweder manuell oder über DHCP konfiguriert wurde, können Sie die **Verwaltungs-IP- und DNS-Einstellungen** über die Citrix SD-WAN Orchestrator for On-premises GUI ändern. Der

Neustart des Citrix SD-WAN Orchestrator for On-Premises-Stacks dauert etwa 3 Minuten. Sobald die Verwaltungs-IP-Adresse geändert wurde, werden die SSH-Verbindungen wieder hergestellt.

Um die Verwaltungs-IP- und DNS-Einstellungen zu konfigurieren/zu ändern, navigieren Sie auf Netzwerkebene zu **Infrastruktur > Orchestrator-Administration > Verwaltungseinstellungen > Management-IP & DNS**.

Geben Sie die folgenden Details an:

- **IP-Adresse: Die**IP-Adresse für Citrix SD-WAN Orchestrator für lokale VM.
- **Gateway-IP-Adresse: Die**Gateway-IP-Adresse, die Citrix SD-WAN Orchestrator for On-premises für die Kommunikation mit externen Netzwerken verwendet.
- **Subnetzmaske**: Die Subnetzmaske zum Definieren des Netzwerks, in dem Citrix SD-WAN Orchestrator for On-premises verfügbar ist.
- **Primärer DNS**: Die IP-Adresse des primären DNS-Servers, an den alle DNS-Anforderungen von Citrix SD-WAN Orchestrator for On-premises weitergeleitet werden.
- **Sekundärer DNS**: Die IP-Adresse des sekundären DNS-Servers zum Auflösen von DNS-Anforderungen, wenn der primäre DNS-Server nicht verfügbar ist.

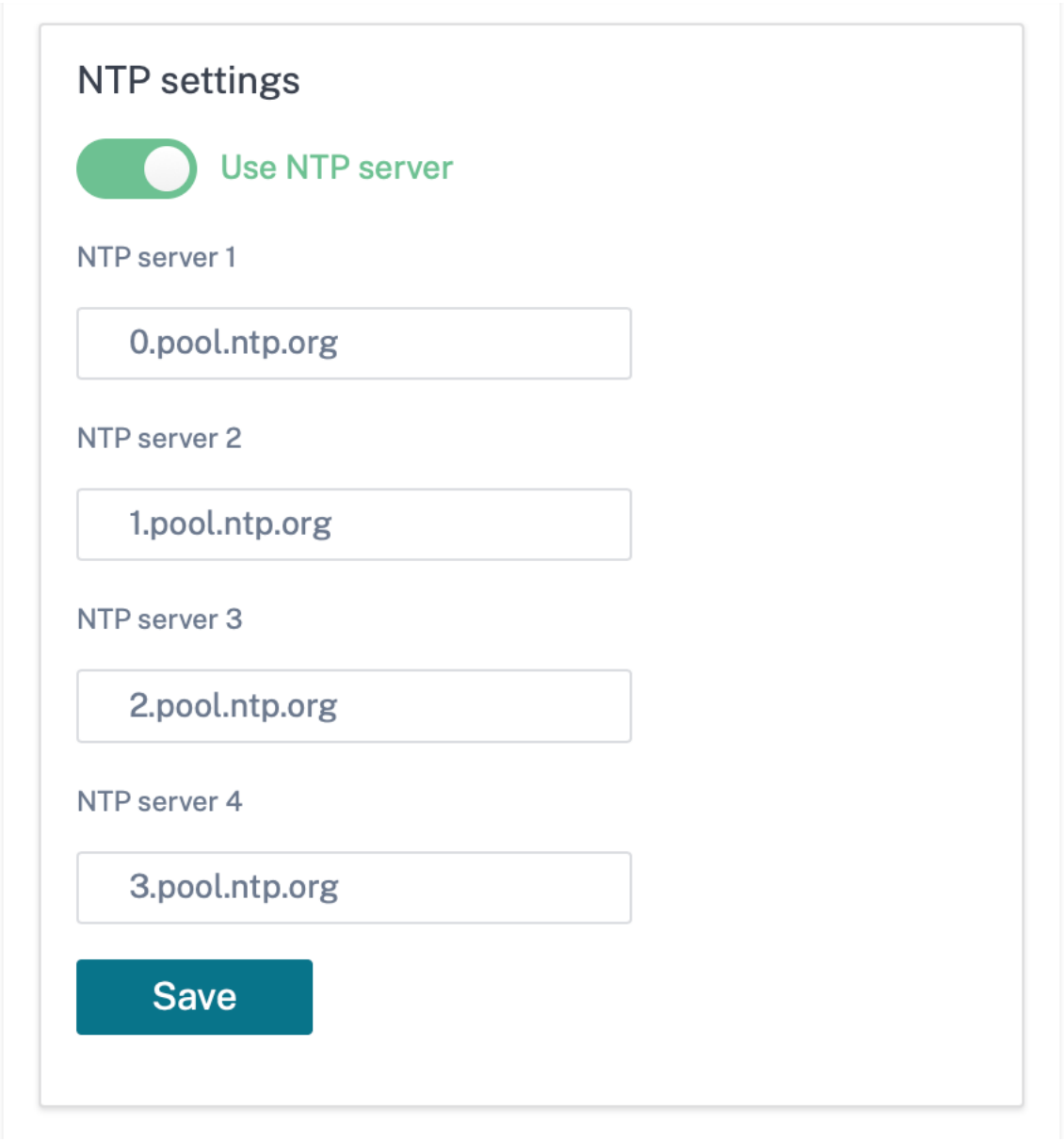


NTP-Einstellungen

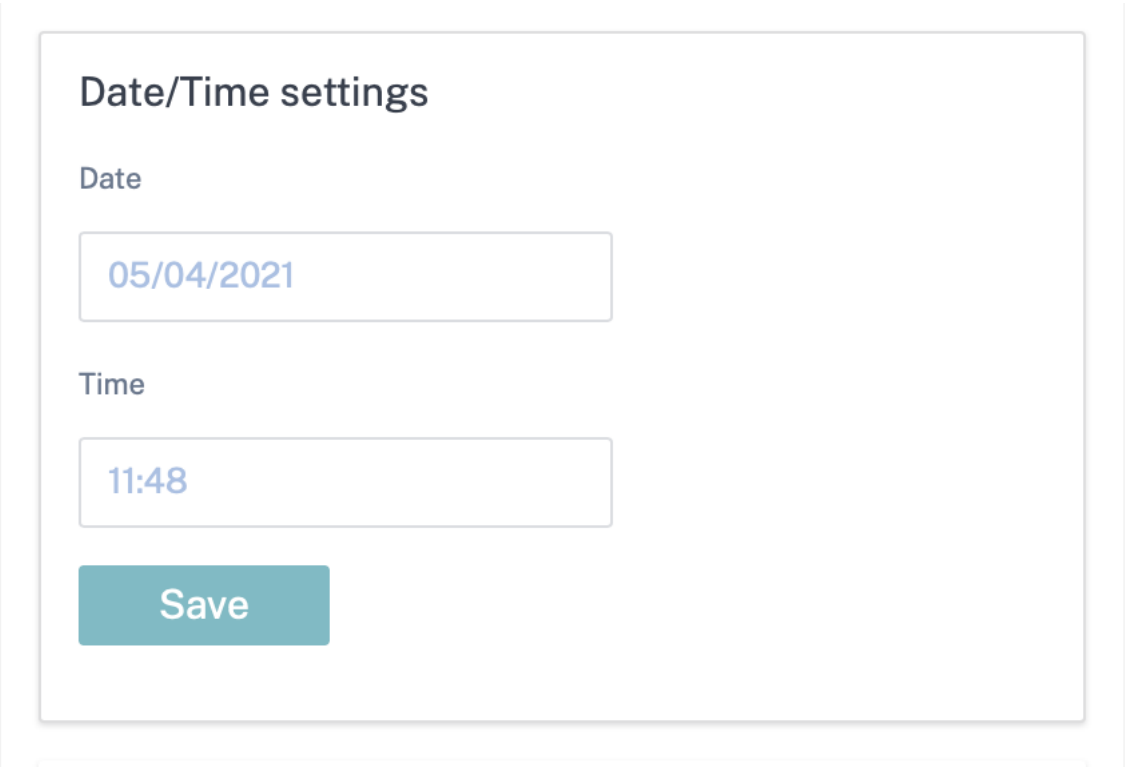
Sie können entweder Datum und Uhrzeit manuell festlegen oder einen NTP-Server (Network Time Protocol) verwenden, um die Uhrzeit von Citrix SD-WAN Orchestrator für lokale Umgebungen mit der koordinierten Weltzeit (UTC) zu synchronisieren.

Um den NTP-Server zu konfigurieren, navigieren Sie auf Netzwerkebene zu **Infrastruktur > Orchestrator-Administration > Verwaltungseinstellungen > NTP** und aktivieren **Sie NTP-Server verwenden**.

Geben Sie die IP-Adresse oder den Domänennamen des NTP-Servers an. Sie können bis zu vier NTP-Server bereitstellen, stellen Sie jedoch sicher, dass mindestens einer konfiguriert ist. Wenn ein NTP-Server ausgefallen ist, synchronisiert Citrix SD-WAN Orchestrator for On-premises automatisch mit dem anderen NTP-Server. Wenn Sie einen Domänennamen für einen NTP-Server angeben, stellen Sie sicher, dass der externe DNS-Server so konfiguriert ist, dass der Domänenname auf die IP-Adresse verweist.

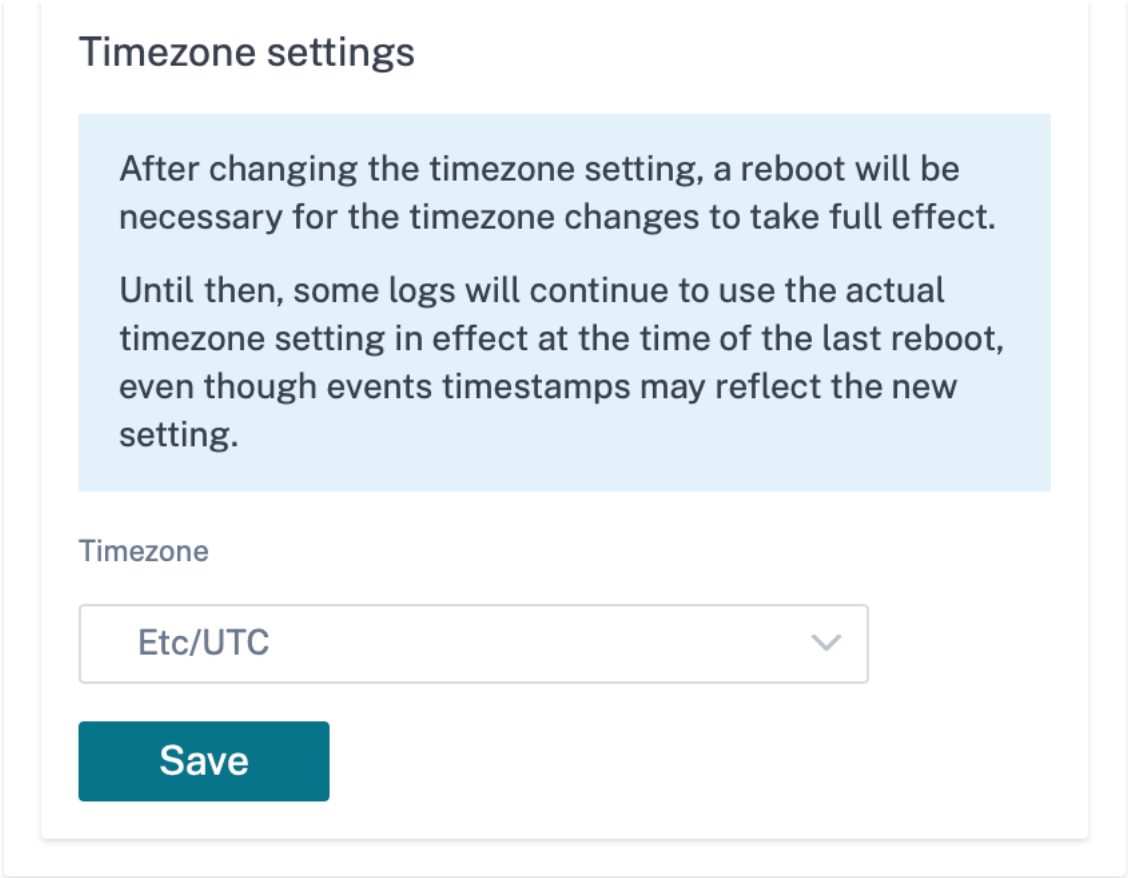


Um Datum und Uhrzeit manuell zu konfigurieren, deaktivieren Sie die Option **NTP-Server verwenden** und wählen Sie Datum und Uhrzeit manuell aus.



Wählen Sie die Zeitzone basierend auf Ihrem Land/Ihrer Stadt aus.

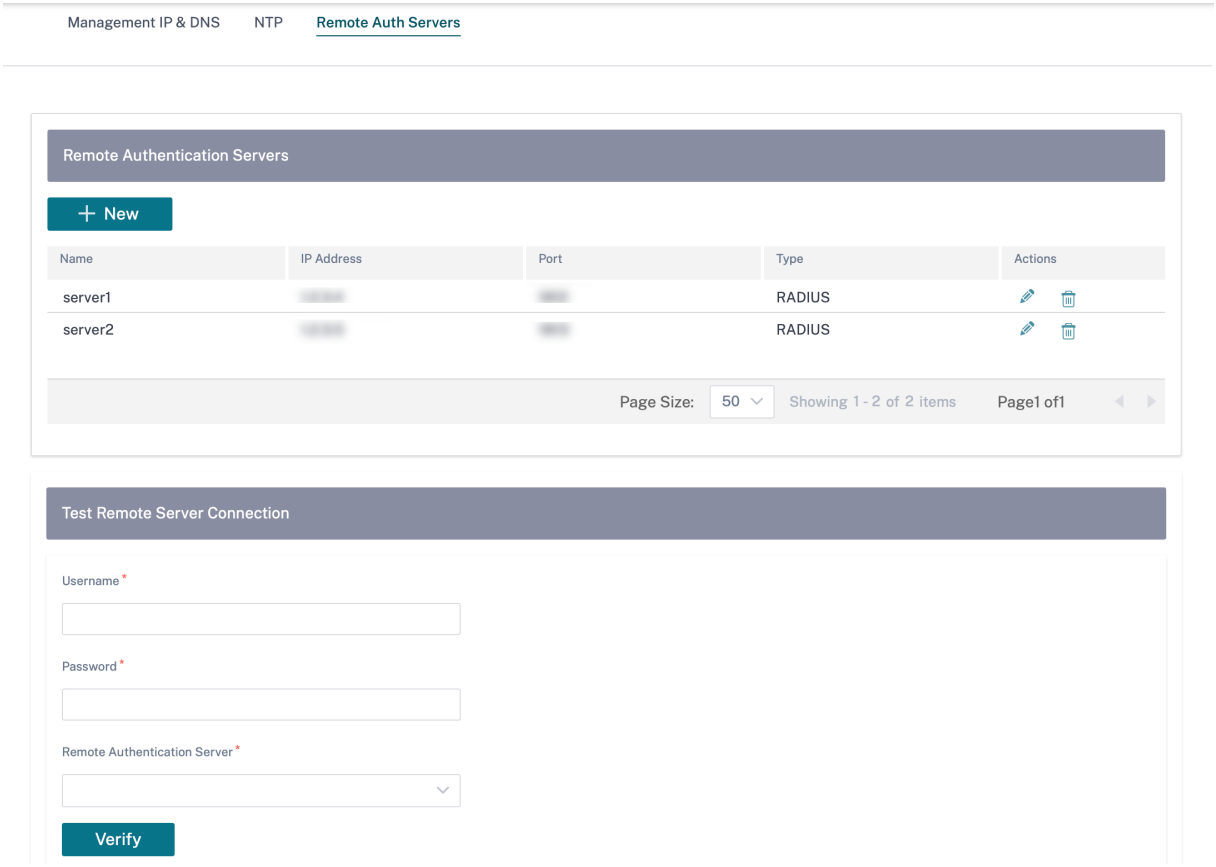
> **HINWEIS Starten Sie**
>
> die Orchestrator-VM neu, nachdem Sie die Zeitzone geändert haben. Einige Protokolle verwenden weiterhin die vorherige Zeitzone, bis der Neustart abgeschlossen ist. Anweisungen finden Sie unter Neustart der Orchestrator-VM.



Server für Remote-Authentifizierung

In einem vom Anbieter verwalteten Setup können nur Anbieteradministratoren RADIUS- oder TACACS+-Server für die remote authentifizierten Benutzer konfigurieren. Kundenadministratoren können die von den Anbieteradministratoren konfigurierten Remote-Authentifizierungsserver verwenden. In einem vom Kunden verwalteten Setup können Kundenadministratoren RADIUS- oder TACACS+-Server konfigurieren.

> **HINWEIS Stellen Sie**
>
> sicher, dass die erforderlichen Benutzerkonten auf dem RADIUS- oder TACACS+-Authentifizierungsserver erstellt wurden.

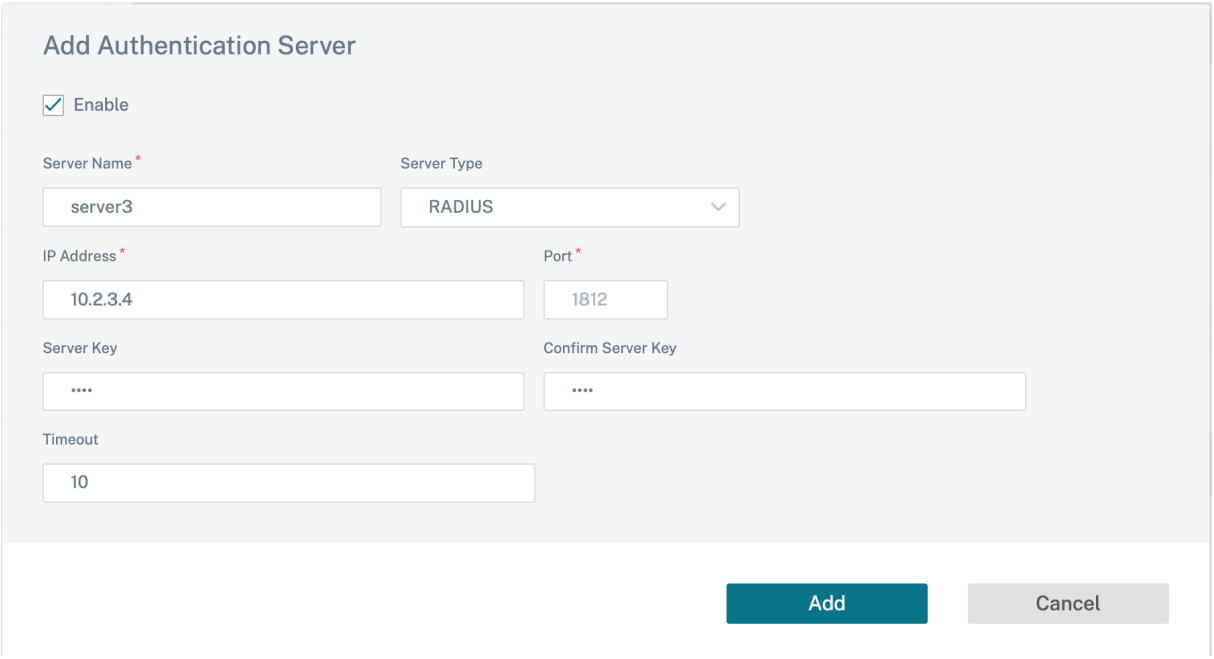


Um die Remote-Authentifizierung zu konfigurieren, navigieren Sie zu **Infrastruktur > Orchestrator-Administration > Verwaltungseinstellungen > Remote-Authentifizierungsserver**. Klicken Sie auf **+ Neu**. Geben Sie folgende Details ein:

- **Aktivieren**: Aktiviert die Konfiguration des Remoteauthentifizierungsservers.
- **Servername**: Der Name des Remote-Authentifizierungsservers.
- **Servertyp**: Der Typ des Remote-Authentifizierungsservers —RADIUS oder TACACS+.
- **IP-Adresse: Die**Host-IP-Adresse für den Remote-Authentifizierungsserver.
- **Port**: Die Portnummer für den Remote-Authentifizierungsserver. Der Standardport für den RADIUS-Server ist 1812 und der TACACS+-Server ist 49.
- **Serverschlüssel** und **Serverschlüssel bestätigen**: Ein geheimer Schlüssel, der beim Herstellen einer Verbindung mit dem Remote-Authentifizierungsserver verwendet wird.
- **Authentifizierungstyp**: (nur für TACACS+-Server verfügbar) Wählen Sie die Verschlüsselungsmethode aus, mit der der Benutzername und das Kennwort an den TACACS+-Server gesendet werden sollen.
  - **PAP**: Verwendet das Password Authentication Protocol (PAP), um die Benutzerauthentifizierung zu stärken, indem dem TACACS+-Server ein starkes gemeinsames Geheimnis zugewiesen wird.
  - **ASCII**: Verwendet den ASCII-Zeichensatz, um die Benutzerauthentifizierung zu stärken, in-

dem dem TACACS+-Server ein starkes gemeinsames Geheimnis zugewiesen wird.

- **Timeout**: Das Zeitintervall (in Sekunden), in dem auf eine Authentifizierungsantwort vom Remote-Authentifizierungsserver gewartet wird.



Sie können auch die Remote-Serververbindung testen. Geben **Sie unter Test Remote Server Connection**Ihren **Benutzernamen** und Ihr **Passwort ein**. Wählen Sie den Remote-Authentifizierungsserver aus und klicken Sie auf **Überprüfen**.

Datenbank-Verwaltung

Sie können eine Backup der aktuellen Datenbank erstellen, die auf Citrix SD-WAN Orchestrator for On-premises ausgeführt wird, und später die gesicherte Datei verwenden, um denselben Datenbankstatus wiederherzustellen.

> **Hinweis**
>
> - In einem vom Anbieter verwalteten Setup haben nur Anbieteradministratoren Zugriff, um Datenbanksicherungen zu erstellen und diese wiederherzustellen.
> - Sie können die Datenbanksicherung, die in einem vom Anbieter verwalteten Setup in einem vom Kunden verwalteten Setup erstellt wurde, nicht wiederherstellen. Ebenso können Sie die Datenbanksicherung, die in einem vom Kunden verwalteten Setup in einem vom Anbieter verwalteten Setup erstellt wurde, nicht wiederherstellen.

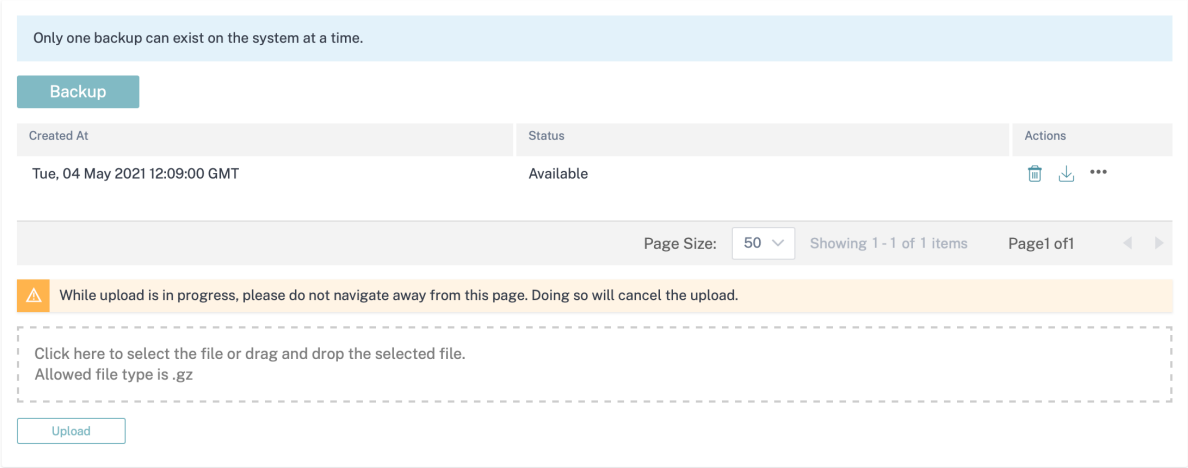
Um eine Datenbanksicherung zu erstellen, navigieren Sie zu **Infrastruktur** > **Orchestrator-Administration** > **Datenbankverwaltung**. Klicken Sie auf **Backup**.

Klicken Sie in der Spalte **Aktionen** auf Herunterladen, um die gesicherte Datenbank herunterzuladen.

Klicken Sie auf „ **Hochladen**“, um die heruntergeladene Datei zu durchsuchen Sie können die heruntergeladene Datei auch per Drag & Drop auf dem Bildschirm ablegen.

Klicken Sie zum **Wiederherstellen** in der Spalte **Aktionen** auf Wiederherstellen.

> **HINWEIS:**
>
> - Sie können jeweils nur eine Datenbanksicherung speichern. Um ein vorhandenes Backup durch das neueste zu ersetzen, löschen Sie das vorhandene Backup und klicken Sie auf **Sichern**.
> - Die Wiederherstellung der Datenbank muss auf derselben Version von Citrix SD-WAN Orchestrator for On-premises erfolgen, von der aus die Datensicherung Backup wurde.
> - Die Datenbanksicherung übernimmt nur die Backup der Konfiguration und Statistik. Es werden keine plattformbezogenen Daten gesichert.



Speicher-Verwaltung

Citrix SD-WAN Orchestrator for On-premises unterstützt die Migration von Kundenkonfigurationen, Statistiken, lokalen Datenbanken und veröffentlichten Citrix SD-WAN-Release-Versionen von einer vorhandenen Festplatte auf eine neue Festplatte.

In einem vom Anbieter verwalteten Setup können nur Anbieteradministratoren die Festplattenmigration durchführen. Kundenadministratoren im vom Anbieter verwalteten Setup haben keine Berechtigungen zum Durchführen der Festplattenmigration. In einem vom Kunden verwalteten Setup können Kundenadministratoren eine Festplattenmigration durchführen.

Sie können die Festplattenmigration entweder zur Erhöhung des Speicherplatzes oder zur Notfallwiederherstellung durchführen.

- **Hinzufügen einer neuen Festplatte**: Sie können eine neue Festplatte hinzufügen, deren Speichergröße mindestens doppelt so groß ist wie die aktuellen Daten, die vom Citrix SD-WAN Orchestrator for On-premises verbraucht werden. Über die Benutzeroberfläche von Citrix SD-WAN Orchestrator for On-premises können Sie die neue Festplatte aktivieren und die vorhandenen Kundenkonfigurationen, Statistiken, die lokale Datenbank und die veröffentlichte Citrix SD-WAN-Versionsversion migrieren. Sobald die neu hinzugefügte Festplatte aktiviert ist, wird Citrix SD-WAN Orchestrator for On-premises neu gestartet.
- **Notfallwiederherstellung**: Im Katastrophenfall können Sie die Festplatte mit den Daten an eine neue Instanz von Citrix SD-WAN Orchestrator for On-premises Virtual Machine anhängen, die sich auf derselben Version von Citrix SD-WAN Orchestrator for On-premises befindet. Aktivieren Sie die Festplatte, ohne die Option **Daten migrieren** in der Benutzeroberfläche von Citrix SD-WAN Orchestrator for On-premises auszuwählen. Sobald die Festplatte aktiviert ist, wird Citrix SD-WAN Orchestrator for On-premises neu gestartet.

> **HINWEIS:**
>
> - Wenn die Festplattenmigration ausgeführt wird, schalten Sie Citrix SD-WAN Orchestrator for On-premises nicht aus oder starten Sie ihn nicht manuell neu. Das Ausschalten oder ein manueller Neustart kann zu Datenverlust führen.
> - Wenn eine Festplatte von einer Festplattenpartition migriert wird, die zuvor zu einer neu erstellten Festplattenpartition hinzugefügt wurde, werden die Daten auf der alten Festplatte nach der Migration nicht entfernt. Um die Daten auf der alten Festplatte zu entfernen, schließen Sie sie an ein anderes Betriebssystem an und löschen Sie die Daten sicher.

Einschränkungen

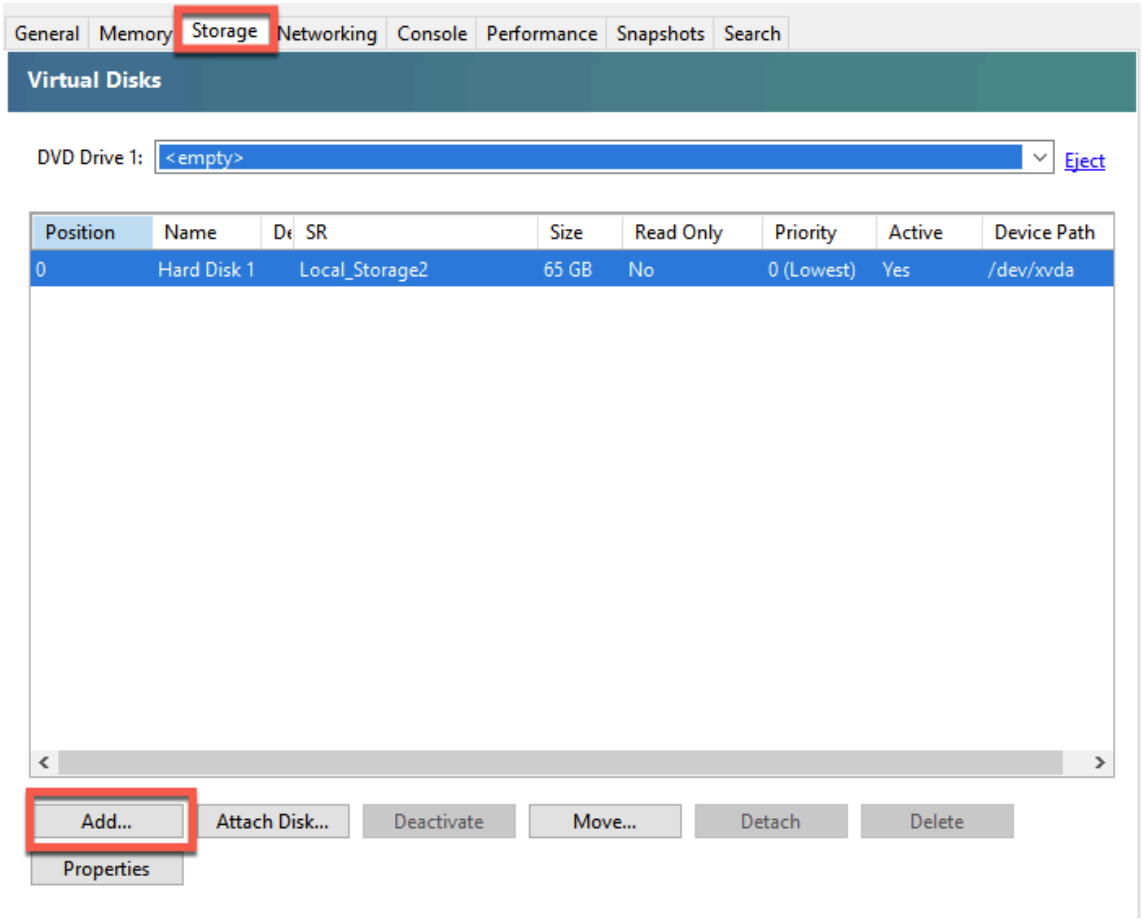
Im Folgenden sind die Einschränkungen beim Festplattenmigrationsprozess aufgeführt:

- Die Benutzer in der alten Version werden nicht auf die neue Version migriert. Löschen Sie nach der Migration die Benutzer und erstellen Sie sie erneut.
- STS, die auf dem alten virtuellen Citrix SD-WAN Orchestrator for On-Premises-Computer erstellt wurden, werden nicht migriert. Nach der Migration listet die Benutzeroberfläche jedoch die STS auf, die auf dem alten Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen generiert wurden. Löschen Sie die STS manuell.
- Datenbanksicherungen, die im alten Citrix SD-WAN Orchestrator for On-premises erstellt wurden, werden nicht migriert. Wenn es nach der Migration aufgelistet wird, löschen Sie es manuell.

- Standardmäßig wird davon ausgegangen, dass der neue Citrix SD-WAN Orchestrator for On-premises, auf den die Festplatte migriert wird, über Konnektivität zu allen Zwei-Faktor-Authentifizierungsservern verfügt. Wenn das Administratorkonto Zwei-Faktor-Authentifizierungsserver verwendet und die Verbindungen zu den Zwei-Faktor-Authentifizierungsservern nicht verfügbar sind, kann sich auch der Administrator nicht anmelden. Wenden Sie sich in solchen Szenarien an den Citrix Support.
- Nach der Migration auf die neue Festplatte können Sie den für Citrix SD-WAN Orchestrator for On-premises zugewiesenen Speicherplatz nicht erhöhen.
- Im Disaster Recovery-Szenario müssen Sie die benutzerdefinierte Domäne neu konfigurieren, nachdem Sie die Festplatte aktiviert haben.
- Im Disaster Recovery-Szenario müssen Sie nach dem Aktivieren der Festplatte entweder eine Zero-Touch-Bereitstellung ohne Cloud oder eine über die Cloud vermittelte Zero-Touch-Bereitstellung durchführen, um die Konnektivität zwischen Citrix SD-WAN-Appliances an den Standorten mit Citrix SD-WAN Orchestrator for On-premises herzustellen.

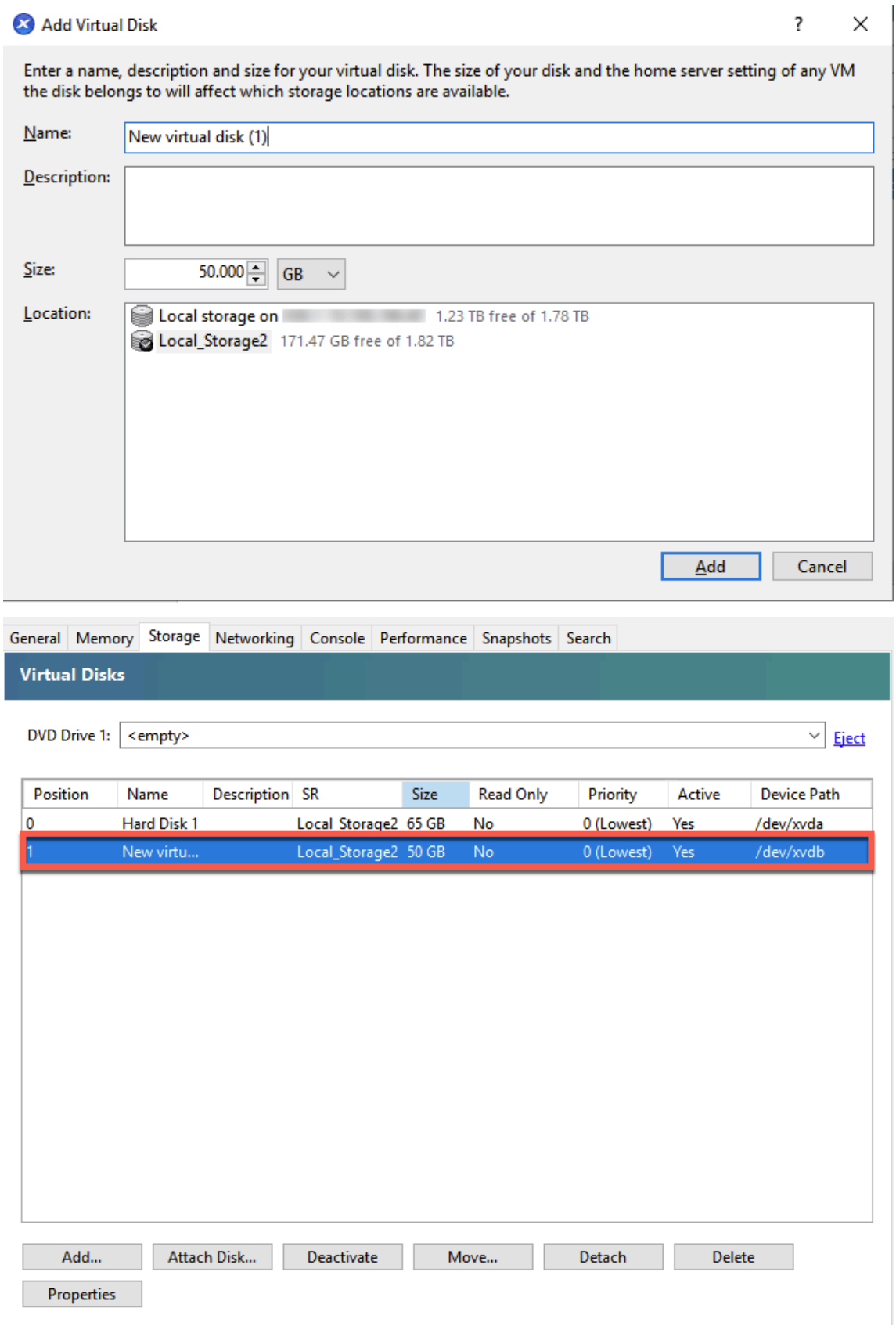
Fügen Sie eine neue Festplatte auf Citrix Hypervisor hinzu

1. Wählen Sie die virtuelle Maschine (VM) vom Hypervisor aus. Wählen Sie die Registerkarte **Speicher** und klicken Sie auf **Hinzufügen**.

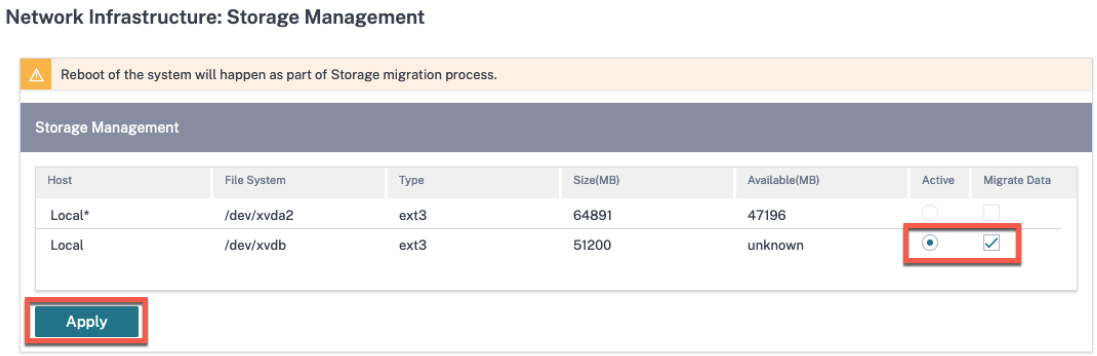


2. Geben Sie Details wie Name, Beschreibung, Größe und Speicherort der neuen Festplatte an. Klicken Sie auf **Hinzufügen**. Die neu hinzugefügte Festplatte wird auf der Registerkarte **Speicher** aufgeführt.

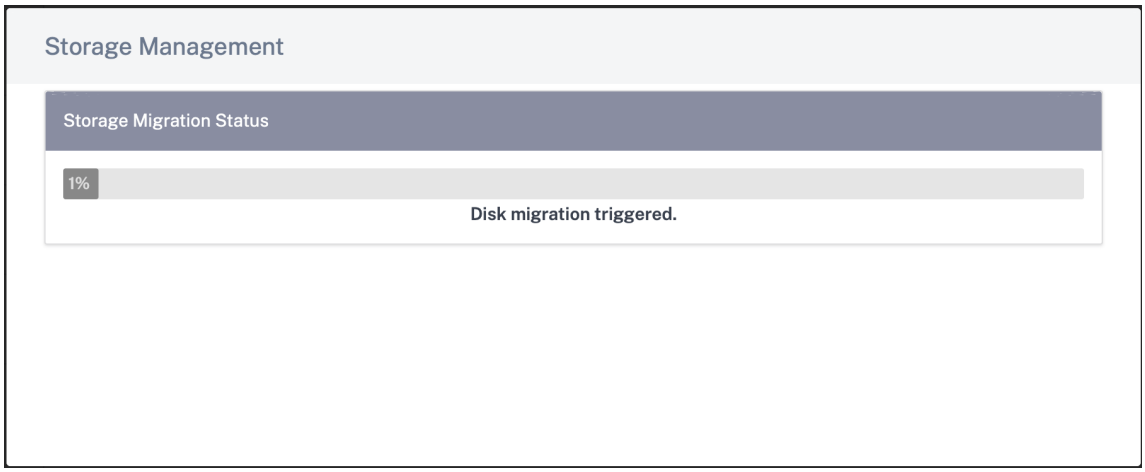
> **HINWEIS**
>
> Die Festplattengröße muss mindestens doppelt so groß sein wie die aktuellen Daten, die vom Citrix SD-WAN Orchestrator for On-premises verbraucht werden.

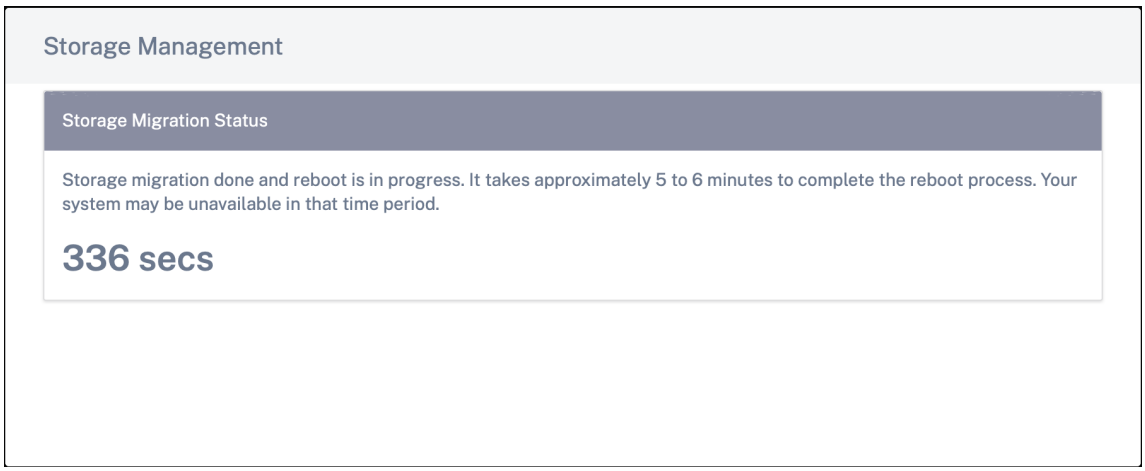


3. Melden Sie sich bei der Citrix SD-WAN Orchestrator for On-Premises-Benutzeroberfläche an und navigieren Sie zu **INFRASTRUKTUR > Orchestrator-Administration > Speicherverwaltung**. Die neu angehängte Festplatte wird automatisch unter **Speicherverwaltung**aufgeführt.
4. Wählen Sie das Optionsfeld **Aktiv** und aktivieren Sie das Kontrollkästchen **Daten migrieren** . Klicken Sie auf **Anwenden**.



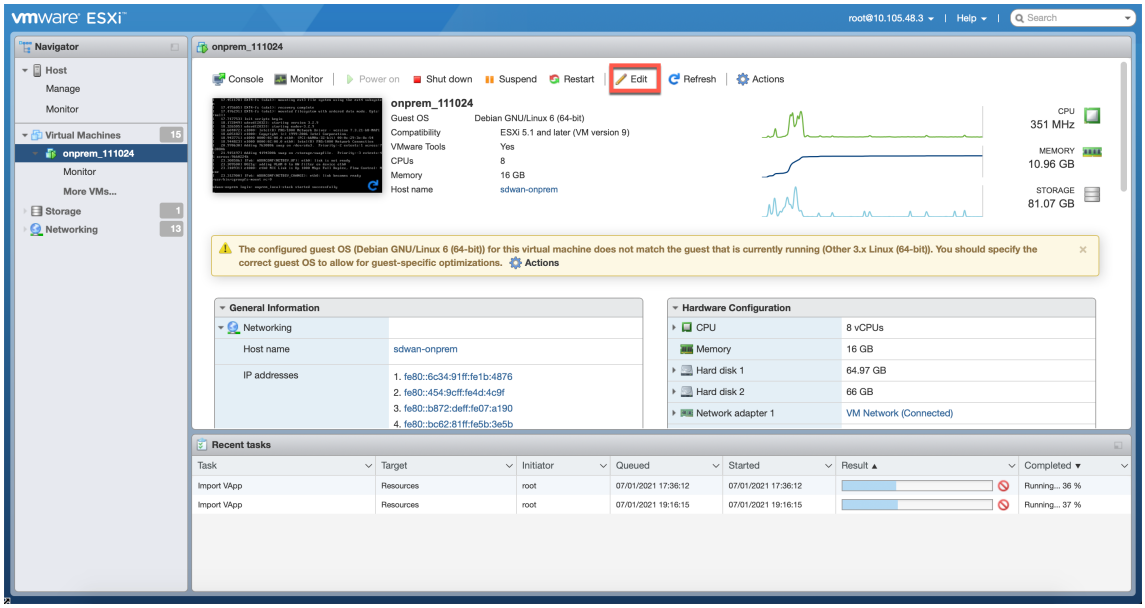
5. Der Festplattenmigrationsprozess wird ausgelöst. Kundenkonfigurationen, Statistiken, lokale Datenbank und Citrix SD-WAN-Release-Version auf der vorhandenen Festplatte werden auf die neue Festplatte migriert. Nach Abschluss der Migration wird Citrix SD-WAN Orchestrator for On-premises neu gestartet.



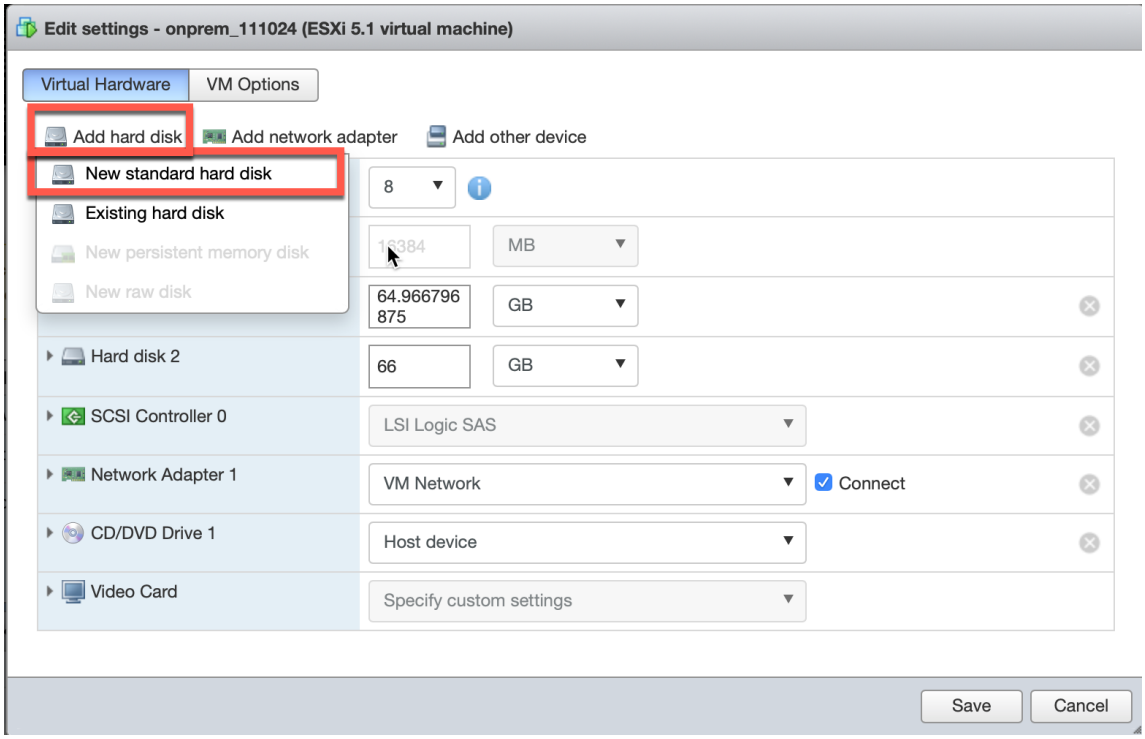


Hinzufügen einer neuen Festplatte auf dem ESXi Server

1. Melden Sie sich bei Ihrem ESXi-Server an und wählen Sie die virtuelle Maschine aus. Klicken Sie auf **Edit**.

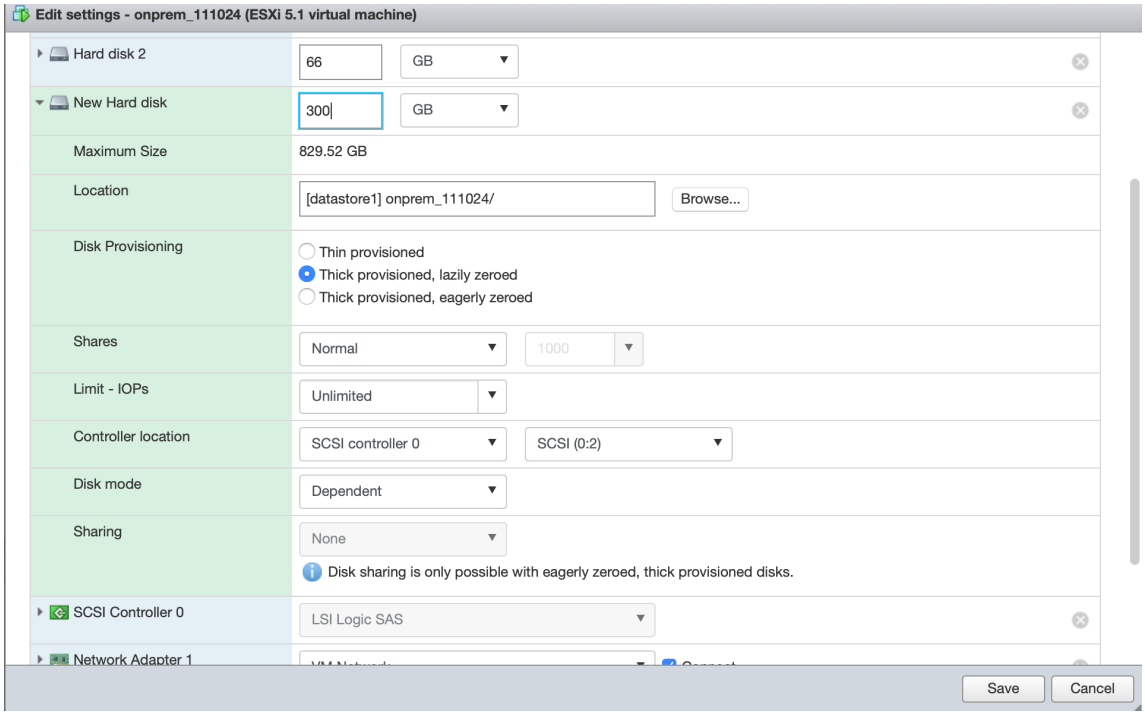


2. Klicken Sie auf **Festplatte hinzufügen > Neue Standardfestplatte**.

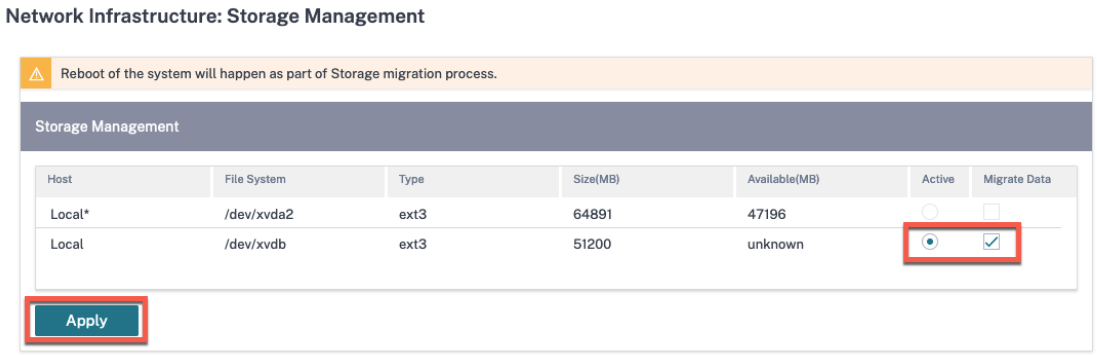


3. Geben Sie den Speicherplatz und andere Einstellungen nach Ihren Wünschen ein. Klicken Sie auf **Speichern**.

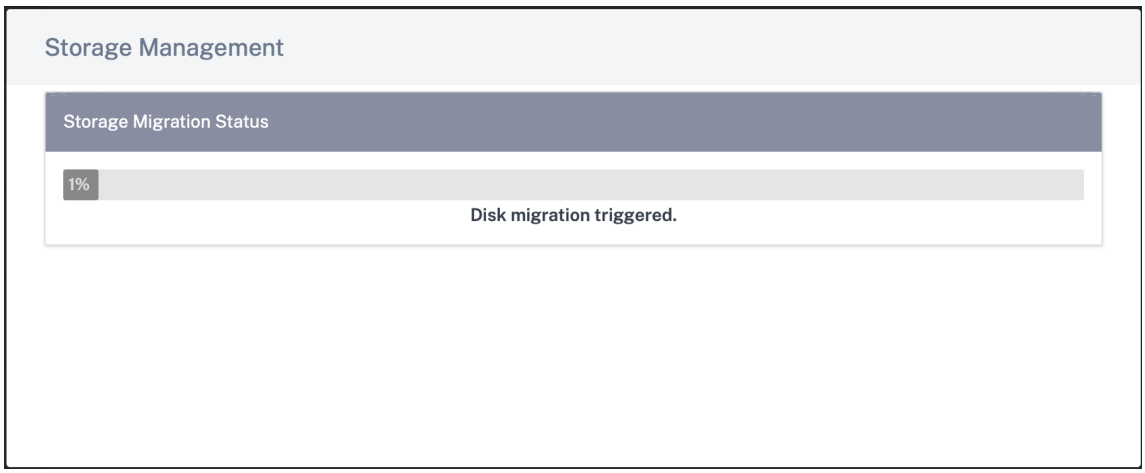
> **HINWEIS**
>
> Die Festplattengröße muss mindestens doppelt so groß sein wie die aktuellen Daten, die vom Citrix SD-WAN Orchestrator for On-premises verbraucht werden.

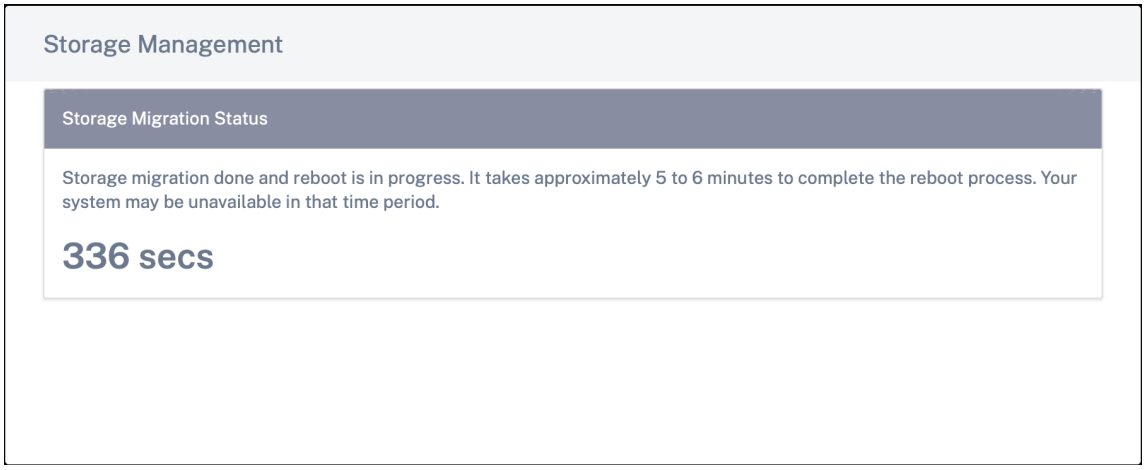


4. Melden Sie sich beim Citrix SD-WAN Orchestrator for On-premises an und navigieren Sie zu **INFRASTRUKTUR > Orchestrator-Administration > Speicherverwaltung**. Die neu angehängte Festplatte wird hier aufgelistet.
5. Wählen Sie das Optionsfeld **Aktiv** und aktivieren Sie das Kontrollkästchen **Daten migrieren** . Klicken Sie auf **Anwenden**.



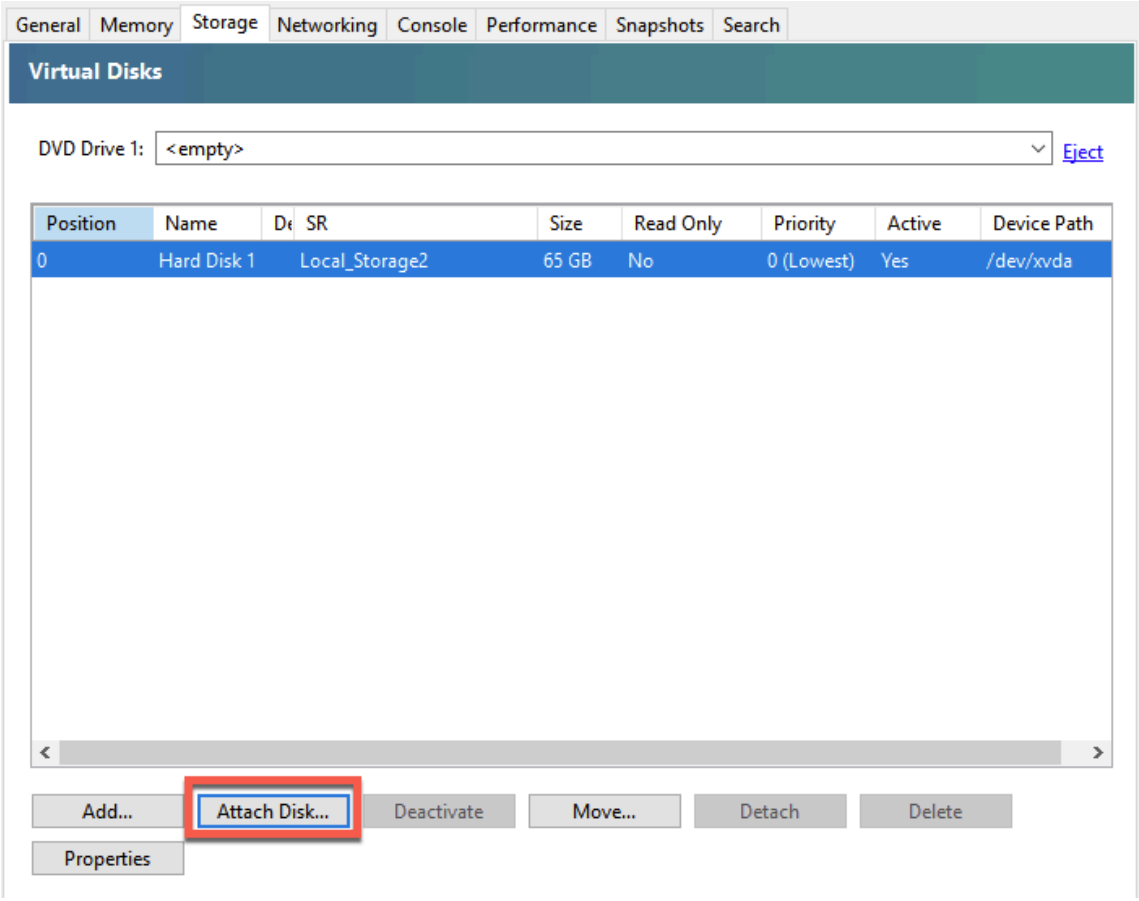
6. Der Festplattenmigrationsprozess wird ausgelöst. Kundenkonfigurationen, lokale Datenbank, Citrix SD-WAN-Release-Version und Datenbankstatistiken auf der vorhandenen Festplatte werden auf die neue Festplatte migriert. Nach Abschluss der Migration wird Citrix SD-WAN Orchestrator for On-premises neu gestartet.





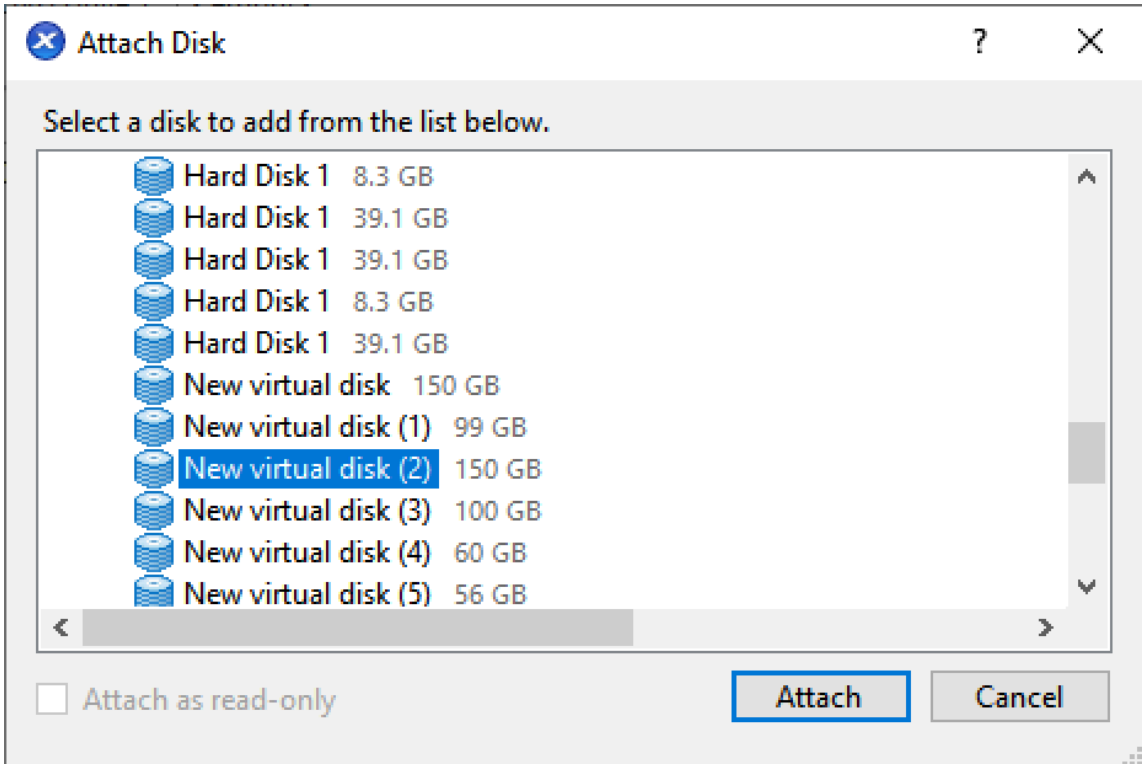
Disaster Recovery auf Citrix Hypervisor

1. Wählen Sie die virtuelle Maschine (VM) vom Hypervisor aus. Wählen Sie die Registerkarte **Speicher** und klicken Sie auf **Festplatte anhängen**.



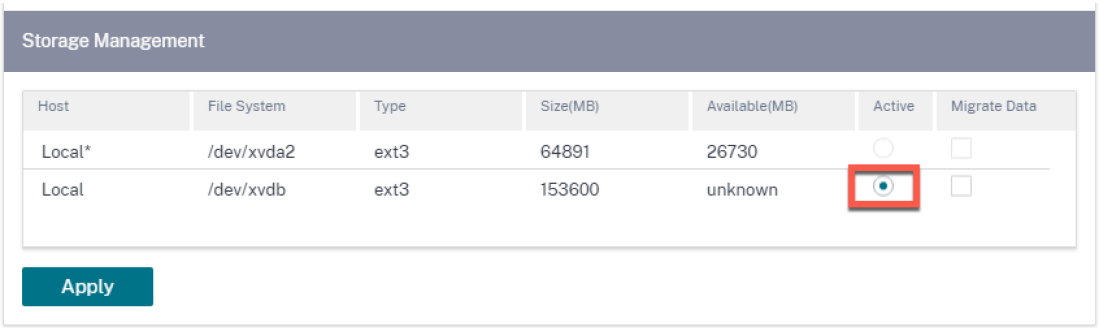
2. Wählen Sie die Festplatte aus, die an den Citrix SD-WAN Orchestrator for On-premises angeschlossen ist und auf „ **Anhängen**“klicken.

   Wenn der Datenträger nicht aufgeführt ist, stellen Sie sicher, dass der Datenträger, der an Citrix SD-WAN Orchestrator for On-premises angeschlossen ist und sich Citrix SD-WAN Orchestrator for On-premises im Status Herunterfahren befindet.

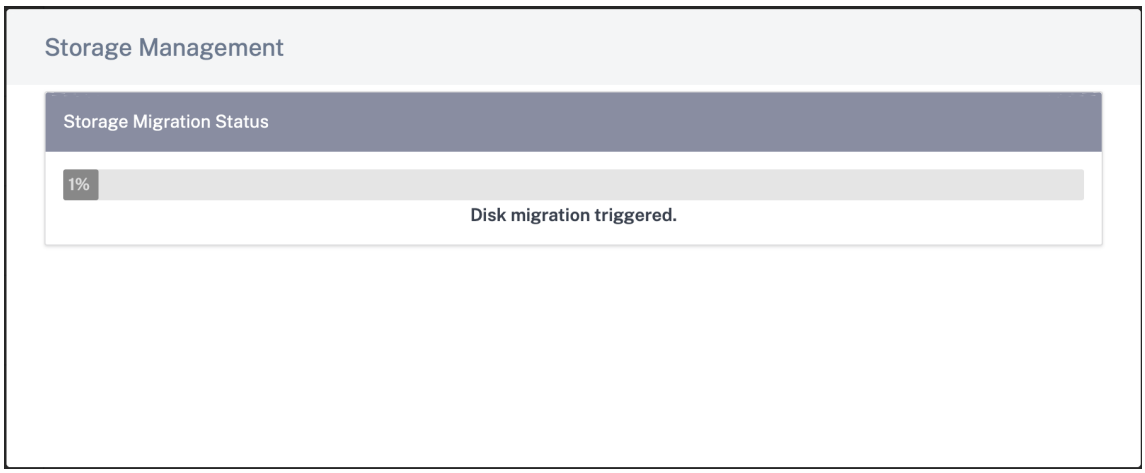


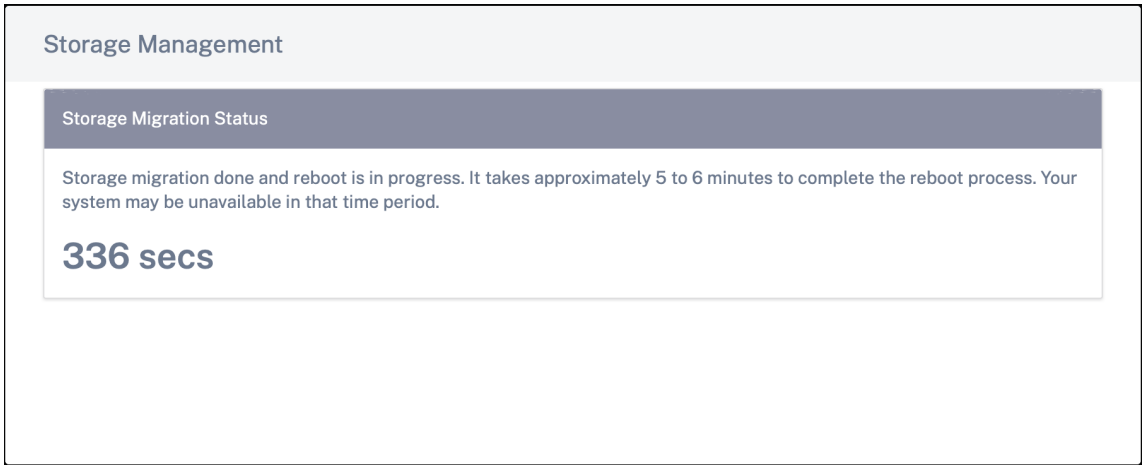
3. Melden Sie sich bei der Citrix SD-WAN Orchestrator for On-Premises-Benutzeroberfläche an und navigieren Sie zu **INFRASTRUKTUR > Orchestrator-Administration > Speicherverwaltung**. Die neu angehängte Festplatte wird hier aufgelistet.
4. Wählen Sie nur das Optionsfeld **Aktiv** aus (deaktivieren Sie das Kontrollkästchen **Daten migrieren**, falls aktiviert) und klicken Sie auf **Übernehmen**.

> **Hinweis**
>
> Aktivieren Sie nicht das Kontrollkästchen **Daten migrieren** . Citrix SD-WAN Orchestrator for On-premises löst die Migration im Backend aus und startet sich selbst neu, sobald die Migration abgeschlossen ist.



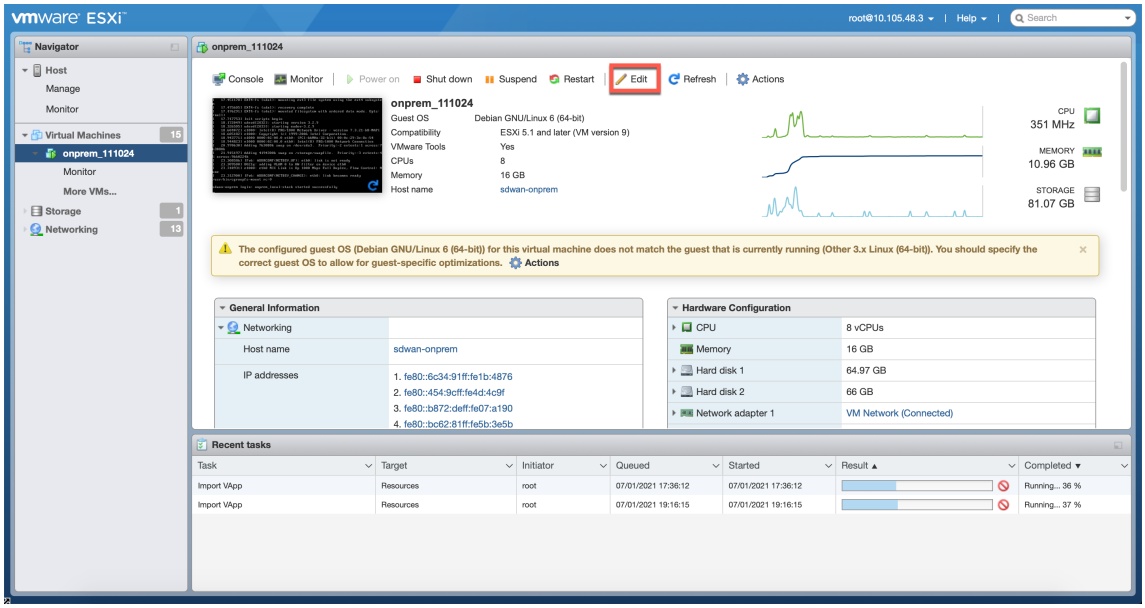
5. Nach Abschluss der Migration wird Citrix SD-WAN Orchestrator for On-premises neu gestartet.



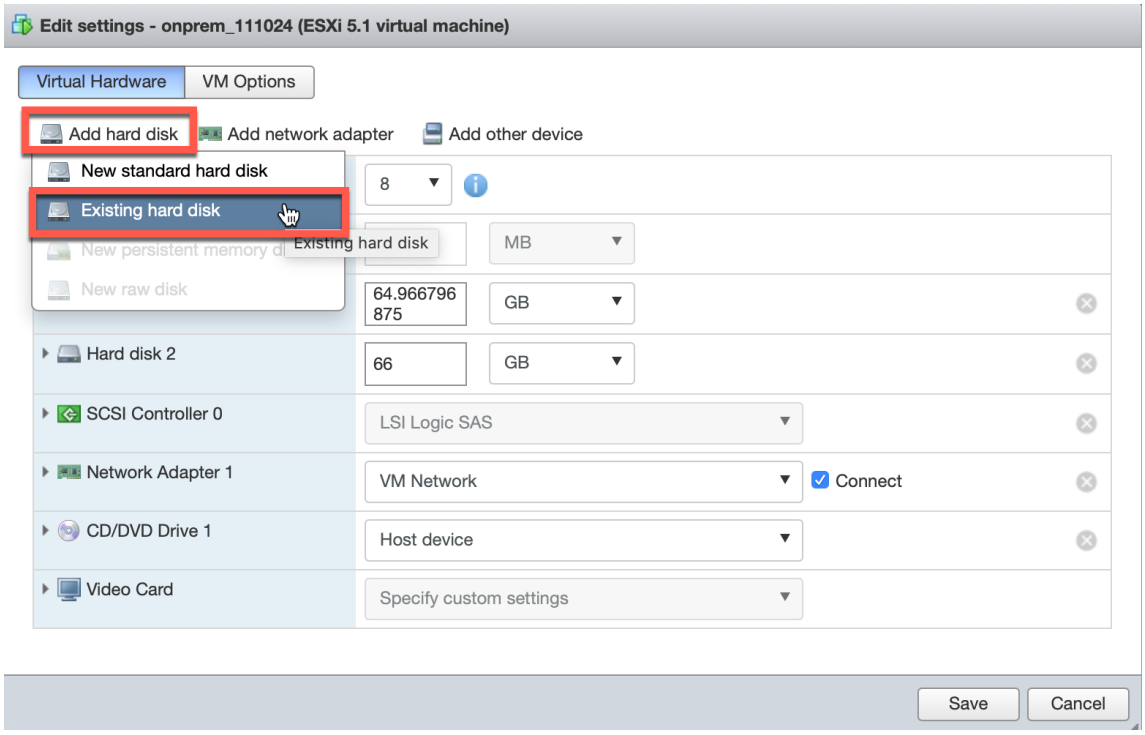


Notfall-Wiederherstellung auf dem ESXi-Server

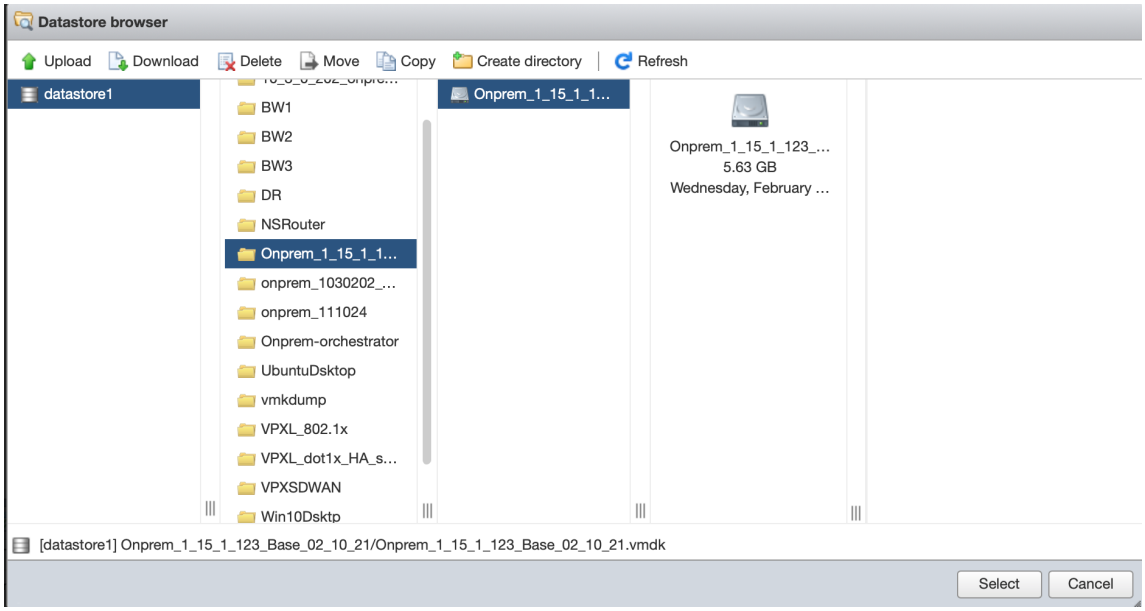
1. Melden Sie sich beim ESXi-Server an und wählen Sie die virtuelle Maschine aus. Klicken Sie auf **Edit**.



2. Klicken Sie auf **Festplatte hinzufügen > Vorhandene Festplatte**.

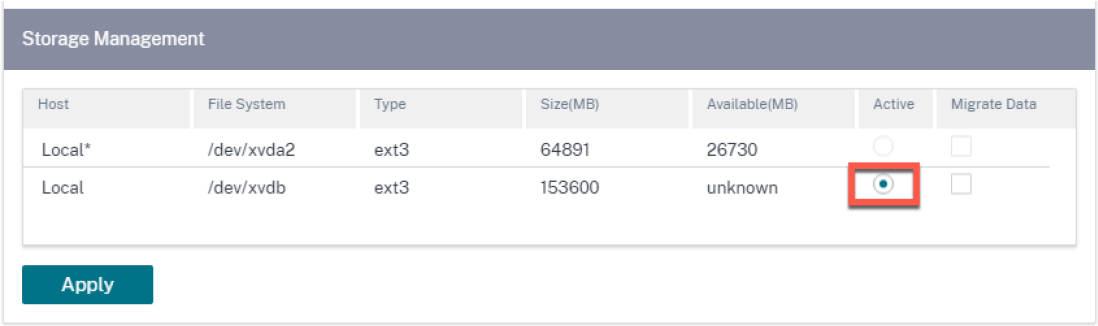


3. Suchen Sie nach der Festplatte, die an den Citrix SD-WAN Orchestrator for On-premises angeschlossen ist und auf **Auswählen**klicken.

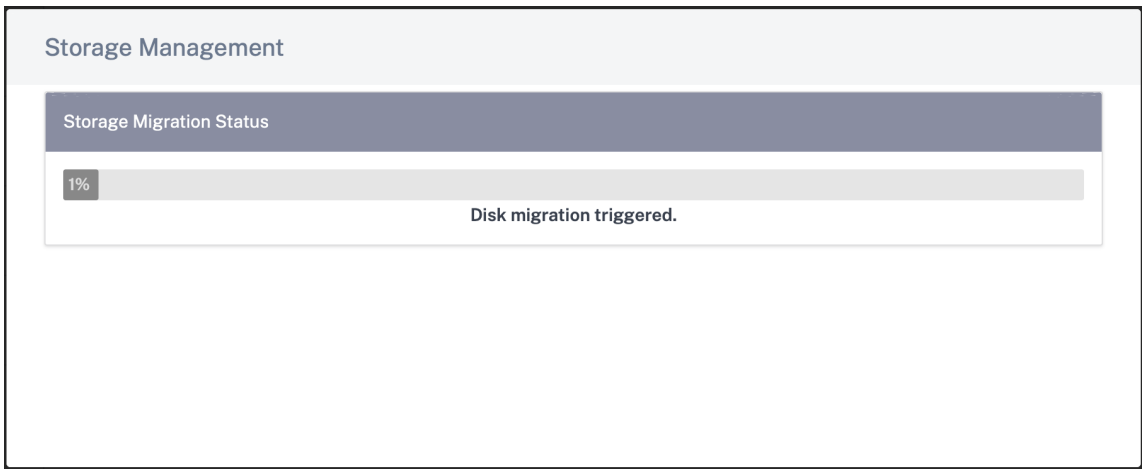


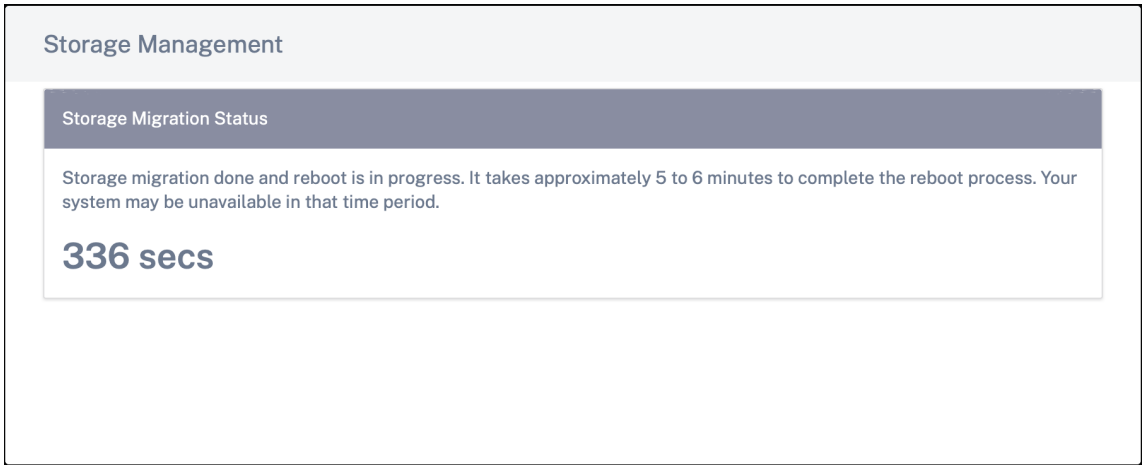
4. Melden Sie sich bei der Citrix SD-WAN Orchestrator for On-Premises-Benutzeroberfläche an und navigieren Sie zu **INFRASTRUKTUR > Orchestrator-Administration > Speicherverwaltung**. Die neu angehängte Festplatte wird hier aufgelistet.
5. Wählen Sie nur das Optionsfeld **Aktiv** aus (deaktivieren Sie das Kontrollkästchen **Daten migrieren**, falls aktiviert) und klicken Sie auf **Übernehmen**.

> **Hinweis**
>
> Aktivieren Sie nicht das Kontrollkästchen **Daten migrieren** . Citrix SD-WAN Orchestrator for On-premises löst die Migration im Backend aus und startet sich selbst neu, sobald die Migration abgeschlossen ist.



6. Nach Abschluss der Migration wird Citrix SD-WAN Orchestrator for On-premises neu gestartet.





HTTP-Proxy

Citrix SD-WAN Orchestrator for On-premises erfordert eine Internetverbindung für Lizenzierung, Cloud-Anmeldung, Cloud-vermittelte ZTD, Cloud Direct und Veröffentlichungssoftware. Wenn Citrix SD-WAN Orchestrator for On-premises über einen HTTP-Proxyserver mit dem Internet verbunden ist, können Sie die Einstellungen des HTTP-Proxyservers auf Ihrem Citrix SD-WAN Orchestrator für lokale virtuelle Maschine konfigurieren.

Die HTTP-Proxyeinstellung zentralisiert die Verwaltung aller ausgehenden Anforderungen an Citrix Cloud. Administratoren können die ausgehenden Anforderungen von Citrix SD-WAN Orchestrator for On-premises über einen HTTP-Proxyserver an Citrix Cloud weiterleiten.

Voraussetzungen

Um den HTTP-Proxy für die Cloud-Anmeldung zum ersten Mal zu verwenden, müssen Sie die HTTP-Proxyeinstellungen über die CLI-Konsole von Citrix SD-WAN Orchestrator for On-premises konfigurieren.

Wenn Sie auf der Cloud-Anmeldeseite einer neuen virtuellen Maschine mit Citrix SD-WAN Orchestrator für lokale virtuelle Maschinen den HTTP-Proxy für alle ausgehenden Verbindungen von Citrix SD-WAN Orchestrator for On-premises zum Citrix SD-WAN Orchestrator Service verwenden möchten, müssen Sie die HTTP-Proxydetails mithilfe der CLI konfigurieren. Sobald die Cloud-Anmeldung abgeschlossen ist und Sie auf die Konfigurationsseite zugreifen, können Sie die Details des HTTP-Proxy-Servers auf der Benutzeroberfläche konfigurieren.

Konfigurieren der HTTP-Proxyeinstellungen in der CLI

Konfigurieren Sie HTTP-Proxyeinstellungen, indem `set_http_proxy` Sie den Befehl ausführen Sie können den HTTP-Proxy mit einer der folgenden Optionen konfigurieren:

- Wenn die Authentifizierung auf dem Proxyserver aktiviert ist:

  `set <ip address> <port> <user name> <password>`

- Wenn die Authentifizierung auf dem Proxyserver nicht aktiviert ist:

  `set <ip address> <port>`

HTTP-Proxyeinstellungen anzeigen

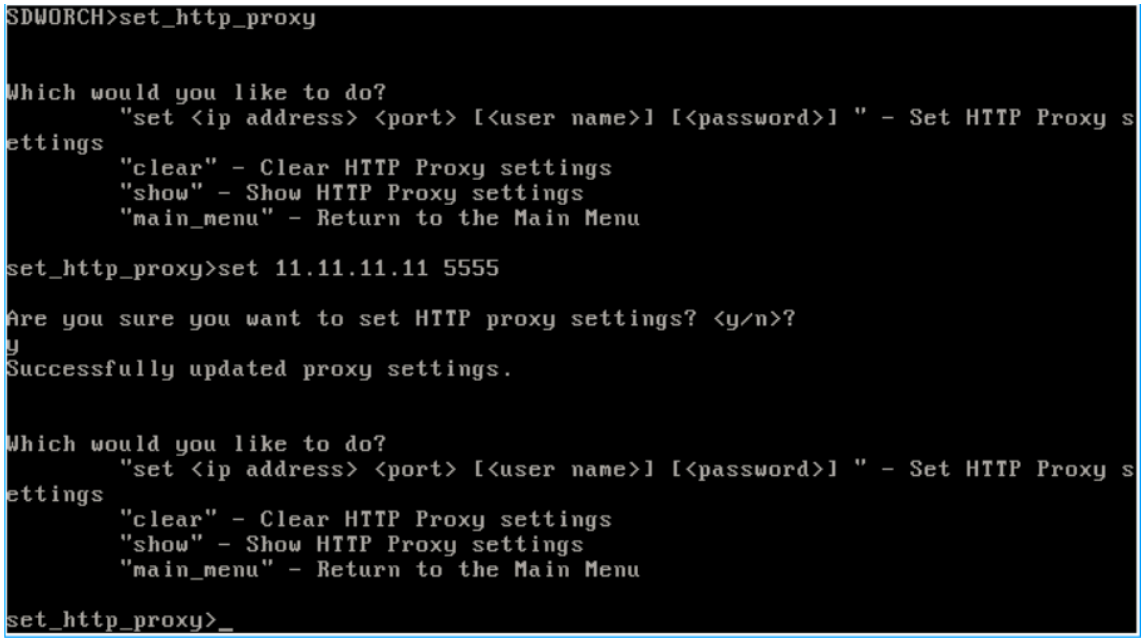
- `show`: Dieser Befehl zeigt die Proxy-Einstellungen in der CLI an. Die Ausgabe zeigt das Passwort nicht an.

HTTP-Proxyeinstellungen löschen

- `clear`: Dieser Befehl löscht die HTTP-Proxyeinstellungen.

Zurück zu main_menu

- `main_menu`: Dieser Befehl leitet Sie zur CLI-Konsole von Citrix SD-WAN Orchestrator for On-premises weiter.



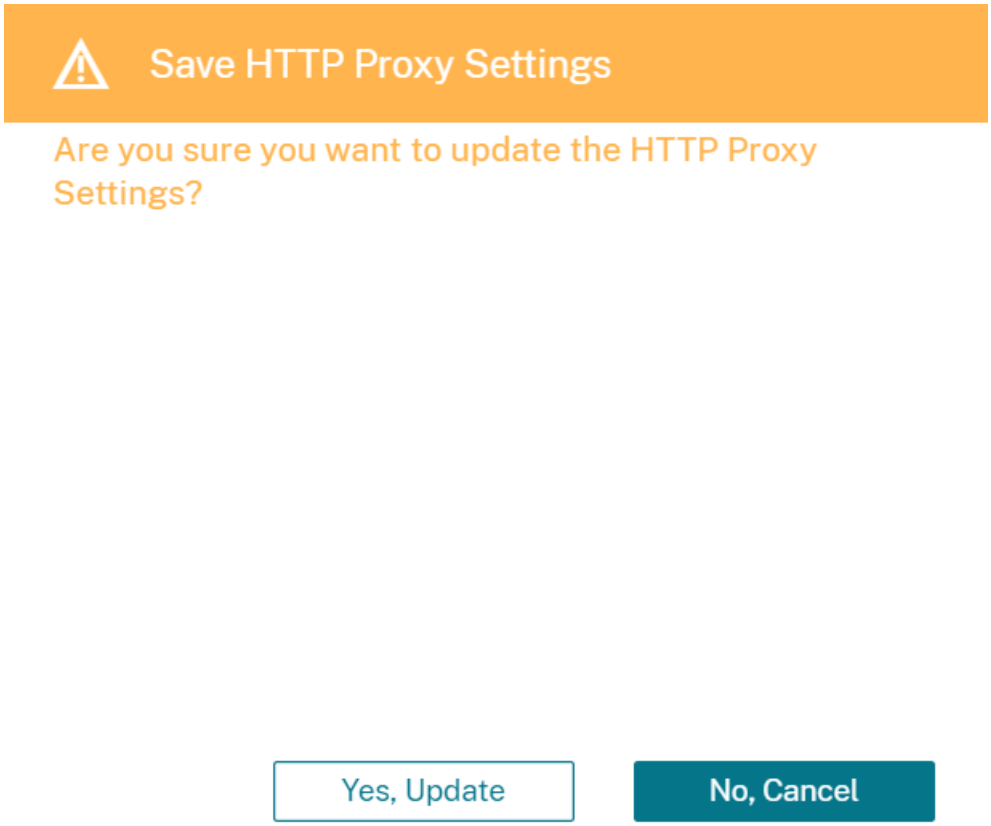
Konfigurieren der HTTP-Proxy-Servereinstellungen auf der Benutzeroberfläche

1. Melden Sie sich bei der Citrix SD-WAN Orchestrator for On-Premises-Benutzeroberfläche an und navigieren Sie zu **Infrastruktur** > **Orchestrator-Administration** > **HTTP-Proxy**.
2. Geben Sie im Abschnitt **Netzwerkinfrastruktur: HTTP-Proxy** Werte für die folgenden Felder ein:

   - **IP-Adresse**: Die IP-Adresse des Proxyservers.
   - **Port**: Die Netzwerkportnummer, auf der der Proxyserver Verbindungen akzeptiert.
   - **Benutzername**: Benutzername des Proxyservers.
   - **Passwort**: Das Passwort für den Proxyserver.

   > **Hinweis:**
   >
   > Sie können die Felder Benutzername und Kennwort leer lassen, wenn auf dem Proxyserver keine Authentifizierung konfiguriert ist.

3. Klicken Sie auf Anwenden. Ein Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf Ja, Aktualisieren.



Hinweise

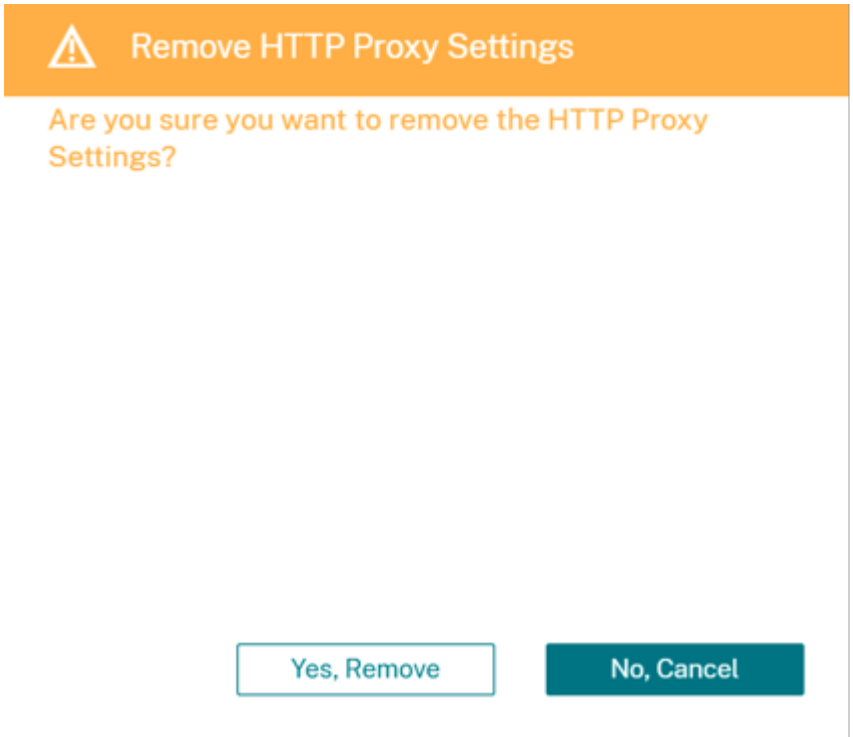
- Um den HTTP-Proxyserver für ausgehenden Datenverkehr von Citrix SD-WAN Orchestrator for On-premises zur Citrix Cloud zu verwenden, muss der Proxyserver als trans-

parenter SSL-HTTP-Proxy oder SSL-Bypass-HTTP-Proxyserver konfiguriert sein. Der Server darf das SSL-Zertifikat des Citrix SD-WAN Orchestrator Orchestrator-Dienstes nicht fälschen.

- Sie können die Proxyservereinstellungen vollständig entfernen, wenn Citrix SD-WAN Orchestrator for On-premises direkt mit dem Internet verbunden ist. Sie können auch die Proxyservereinstellungen entfernen und bei Bedarf einen anderen Proxyserver konfigurieren.

Proxyservereinstellungen auf der Benutzeroberfläche entfernen

1. Navigieren Sie in der Benutzeroberfläche von Citrix SD-WAN Orchestrator for On-Premises zu **Infrastruktur** > **Orchestrator-Administration** > **HTTP-Proxy**.
2. Klicken Sie im Abschnitt **Netzwerkinfrastruktur: HTTP-Proxy** auf **Entfernen**. Ein Bestätigungsdialogfeld wird angezeigt.
3. Klicken Sie auf **Ja, entfernen**.



Bereinigungseinstellungen

Sie können historische Statistiken/Daten für ein ausgewähltes Zeitintervall löschen. Die Statistik/-Daten, die älter als die eingestellten Tage sind, werden gelöscht. Sobald die Daten gelöscht wurden,

sind sie nicht mehr verfügbar. Standardmäßig löscht Citrix SD-WAN Orchestrator for On-premises historische Statistiken/Daten, die älter als 30 Tage sind.

Navigieren Sie auf Netzwerkebene zu **Infrastruktur** > **Orchestrator-Administration** > **Bereinigungseinstellungen,**wählen Sie das Zeitintervall aus und klicken Sie auf **Übernehmen**. Wenn Sie beispielsweise historische Statistiken/Daten, die älter als 180 Tage sind, löschen möchten, wählen Sie 180 aus der Dropdown-Liste **Bereinigungsstatistikintervall (Tage)** aus und klicken Sie auf **Anwenden**. Der Löschvorgang findet täglich gegen 12:48 Uhr in der auf Ihrer SD-WAN-Appliance festgelegten Zeitzone statt.

Orchestrator-Diagnose

October 21, 2022

Dieser Abschnitt enthält Informationen zu den Diagnoseaktivitäten, die in der Citrix SD-WAN Orchestrator for On-Premises-Infrastruktur ausgeführt werden können.

> **Hinweis:**
>
> In einem vom Anbieter verwalteten Setup haben Anbieteradministratoren Zugriff auf alle GUI-Seiten **Infrastruktur > Orchestrator-Diagnose**. Kundenadministratoren haben nur Zugriff auf **Plattformereignisse und -protokolle** sowie GUI-Seiten zum **Plattformzustand**

Plattformereignisse und Protokolle

Jede Änderung der Attribute auf Plattformebene wie CPU, Arbeitsspeicher oder Speicher im System wird als Ereignis protokolliert und auf dem Citrix SD-WAN Orchestrator for On-premises angezeigt.

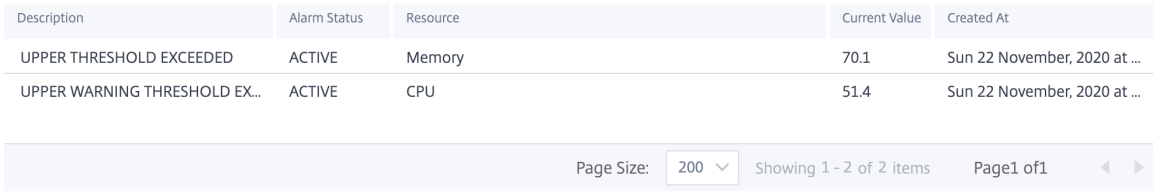
Wenn beispielsweise die CPU-Auslastung den festgelegten Grenzwert überschreitet, wird ein Plattformereignis protokolliert und ein Alarm ausgelöst. Der Alarm wird in der Benachrichtigungsleiste angezeigt. Die Benachrichtigung wird gelöscht, wenn die CPU-Auslastung verringert wird. Auf der Seite **Plattformereignisse und -protokolle** wird der Verlauf aller ausgelösten plattformbezogenen

Alarme verwaltet. Wenn die CPU-Auslastung sinkt, wird der Alarmstatus INAKTIV. Liegt er immer noch über den Grenzwerten, bleibt der Alarmstatus AKTIV.

Um die Plattformereignisse anzuzeigen, navigieren Sie zu **Infrastruktur** > **Orchestrator-Diagnose** > **Plattformereignisse und -protokolle**.

Die folgenden Details werden für protokollierte Plattformereignisse angezeigt:

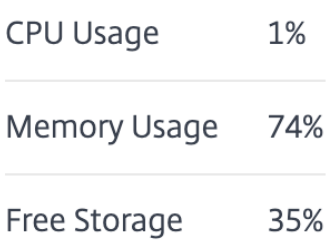
- **Beschreibung**: Die Beschreibung des Plattformereignisses.
- **Alarmstatus**: Der Status des Alarms. Wenn das Plattformattribut den festgelegten Grenzwert überschreitet, ist der Status ACTIVE. Wenn das Attribut auf Plattformebene auf einen Wert innerhalb des festgelegten Grenzwerts absinkt, lautet der Alarmstatus INAKTIV.
- **Ressource**: Das Attribut auf Plattformebene —CPU, Arbeitsspeicher oder Speicher.
- **Aktueller Wert**: Der letzte Wert des protokollierten Plattformattributs.
- **Erstellt um**: Der Zeitpunkt, zu dem das Plattformereignis aufgetreten ist.



Plattform-Gesundheit

Sie können den Zustand der Citrix SD-WAN Orchestrator for On-Premises-Plattform anzeigen. Die Integritätsinformationen umfassen Echtzeitwerte (in Prozent) für die CPU-Auslastung, die Speichernutzung und den verfügbaren freien Speicherplatz.

Um den Plattformzustand anzuzeigen, navigieren Sie zu **Infrastruktur > Orchestrator-Diagnose > Plattformintegrität**.

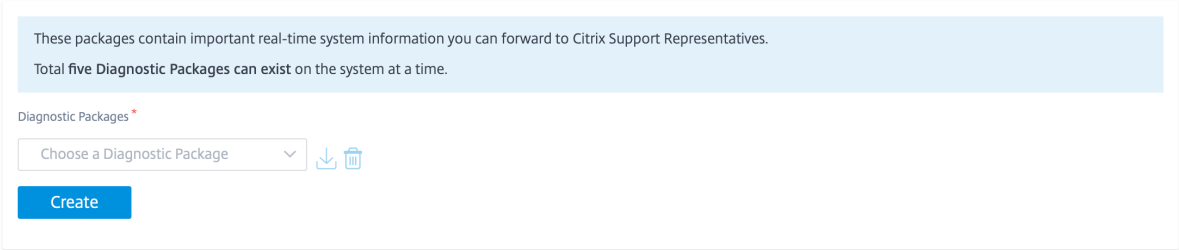


Diagnose-Info

Ein Diagnosepaket besteht aus Systemprotokolldateien, Systeminformationen und anderen notwendigen Details, die das Support-Team bei der Diagnose und Behebung von Problemen mit Ihrem System unterstützen.

Um ein Diagnosepaket zu erstellen, navigieren Sie zu **Infrastruktur** > **Orchestrator-Diagnose** > **Diagnoseinformationen**. Klicken Sie auf **Erstellen**. Nachdem das Paket erstellt wurde, können Sie es auf Ihren Computer herunterladen und dann für das Support-Team freigeben.

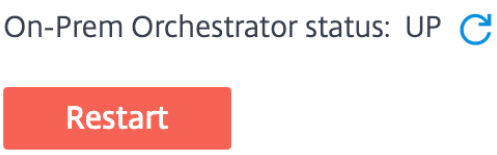
> **HINWEIS:**
>
> Citrix SD-WAN Orchestrator for On-premises kann maximal fünf Diagnosepakete gleichzeitig speichern.



Starten Sie Citrix SD-WAN Orchestrator für die lokale App neu

Sie können nur die Citrix SD-WAN Orchestrator for On-Premises-App neu starten, ohne das Betriebssystem (OS) neu zu starten. Während des Neustarts geht die Citrix SD-WAN Orchestrator for On-Premises-App offline und alle Dienste sind nicht mehr verfügbar. Es dauert ungefähr 6 Minuten, bis der Neustart abgeschlossen ist. Nach dem Neustart wird die Anmeldeseite von Citrix SD-WAN Orchestrator for On-premises angezeigt.

Um die Citrix SD-WAN Orchestrator for On-Premises-App neu zu starten, navigieren Sie zu **Infrastruktur > Orchestrator-Diagnose > Orchestrator-App neu starten**. Klicken Sie zur Bestätigung auf **Neu**starten**und Ja, Neustart** .

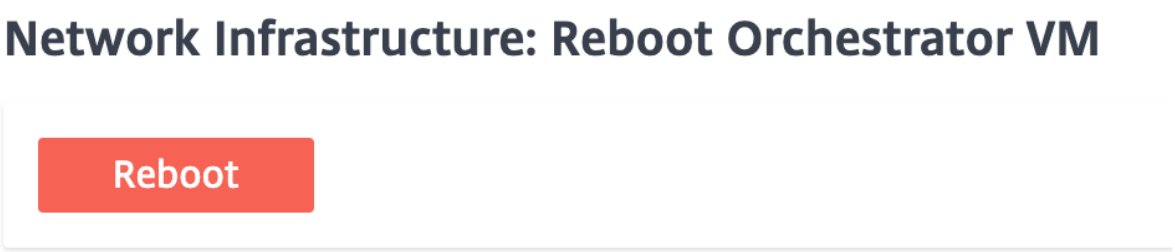


Starten Sie Citrix SD-WAN Orchestrator für lokale VM neu

Der Neustartvorgang startet das Betriebssystem (OS) von Citrix SD-WAN Orchestrator for On-premises neu. Während des Neustarts geht Citrix SD-WAN Orchestrator for On-premises offline und alle Dienste sind nicht mehr verfügbar. Es dauert ungefähr 6 bis 8 Minuten, bis der Neustart abgeschlossen ist. Nach dem Neustart wird die Anmeldeseite von Citrix SD-WAN Orchestrator for On-premises angezeigt.

Sie können Citrix SD-WAN Orchestrator for On-premises im Rahmen einer Problembehandlungsaktivität oder während einer Wartungsaktivität neu starten.

Um neu zu starten, navigieren Sie zu **Infrastruktur > Orchestrator-Diagnose > Orchestrator-VM neu starten**. Klicken Sie zur Bestätigung auf **Rebootund Ja, Reboot** .



Alarme

October 21, 2022

Sie können die plattformspezifischen und dienstspezifischen Alarme anzeigen, die mit Citrix SD-WAN Orchestrator for On-premises verknüpft sind. Plattformspezifische Alarme zeigen plattformbezogene Warnungen wie Speicherproblem, RAM und CPU an. Dienstalarme zeigen den Status der Microservices an, die in Citrix SD-WAN Orchestrator for On-premises ausgeführt werden.

Um die Alarme anzuzeigen, klicken Sie auf das Glockensymbol in der oberen rechten Ecke der Citrix SD-WAN Orchestrator for On-Premises-Benutzeroberfläche und wählen Sie je nach Bedarf **Plattformalarme** oder **Dienstalarme** aus.