适用于本地的 Citrix SD-WAN Orchestrator 14.4

Contents

SD-WAN Orchestrator 本地版 14.4 发行说明

December 10, 2024

本发行说明文档介绍了 Citrix SD-WAN Orchestrator for On-Premium 版本 Build 14.4 的增强功能和更改、已修复和已知问题。

笔记

此发行说明文档不包含与安全相关的修复。有关安全相关修复和公告的列表，请参阅 Citrix 安全公告。

已知问题

14.4 版本中存在的问题。

在 Citrix SD-WAN Orchestrator for On-Premium 中发布 SD-WAN 软件可能会失败，并出现以下错误：

```
Failed to fetch software details from Citrix cloud.
```

解决方法：注销并通过 Citrix SD-WAN Orchestrator for On-premise 重新登录 Citrix Cloud，然后发布 SD-WAN 软件。

[SDW-24980]

本地 SD-WAN Orchestrator 14.3 版本的发行说明

October 21, 2022

本发行说明文档介绍了 Citrix SD-WAN Orchestrator 本地发行版 Build 14.3 中存在的增强功能和更改、已修复问题和已知问题。

备注

本发行说明文档不包括与安全相关的修补程序。有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。

新增功能

版本 14.3 中提供的增强功能和更改。

配置和管理

QoS 策略

对 QoS 策略页面进行了改进，以增强用户体验。自定义应用程序规则、应用程序规则、HDX 规则、应用程序组规则、IP 规则和默认 IP 协议规则等选项已得到增强，外观焕然一新。

[SDW-11029]

平台和系统

管理 **IP/**带内 **IP** 增强功能：

以下用户界面屏幕上的“管理 **IP** ”和“设备访问”列经过增强，可以根据设备与 Citrix SD-WAN Orchestrator for Inclouse 进行通信时使用的 IP 地址类型显示带内 IP 地址或管理 IP 地址：

- 提供商 > 报告 > 库存 > 详情
- 客户 > 配置 > 网络主页 > 操作 > 查看详情
- 客户 > 报告 > 库存 > 详情
- 站点 > 控制面板 > 设备

[SDW-23353]

将报告导出为 CSV

使用 导出为 **CSV** 功能，您可以将任何时间序列（每小时、每周等）的路径图点（虚拟/成员路径）下载为 excel 逗号分隔值 (CSV) 文件，并能够绘制特定站点报告的所有不同数据点。

[SDW-20988]

证书身份验证

适用于本地的 Citrix SD-WAN Orchestrator 支持使用公钥基础架构 (PKI) 作为附加安全功能对静态和动态虚拟路径进行设备身份验证。启用此功能可通过启动交换的设备通过数据路径分发 PKI 证书，从而扩展现有虚拟路径身份验证机制。PKI 增强功能还支持证书吊销列表 (CRL) 管理，以集中撤销受损证书。

[SDW-19295]

SD-WAN Orchestrator

查看配置（预览）

适用于本地的 Citrix SD-WAN Orchestrator 在站点级别引入了“查看配置”页面。本页提供站点在多个子系统上的配置的详细摘要。

[SDW-22284]

网络级实时统计，站点级实时统计

防火墙连接 现已重命名为“防火墙统计”。NAT 和筛选策略是在“统计类型”下拉列表下新添加的。此外，实时统计选项经过重组并分为以下类别：

- 网络统计信息
- 应用程序统计
- 路由统计

[SDW-20966]

移动宽带设置和移动宽带状态

现在，您可以使用宽带互联网连接，将 Citrix SD-WAN 设备从您的站点连接到网络。这种移动宽带状态和配置支持适用于内部调制解调器。您还可以查看设备和活动 SIM 卡的宽带配置状态。

[SDW-10907]

已修复的问题

版本 14.3 中解决的问题。

配置和管理

PKI 证书未显示在适用于本地用户界面的 Citrix SD-WAN Orchestrator 上。之所以出现此问题，是因为 PKI 证书上的“组织单位”字段是必填字段。

[SDW-23726]

其他

有些站点无法连接到适用于本地用户界面的 Citrix SD-WAN Orchestrator。

[SDWANHELP-2601]

已知问题

14.3 版中存在的问题。

Citrix SD-WAN Orchestrator 本地用户界面的“报告”> “使用情况”> “应用程序”页面上的应用程序和应用程序类别图表为空。

[SDW-23817]

当用户返回此页面时，先前在 UI 的“部署”**>** “设置”> “站点部分升级”> “软件版本”页面上选择的软件版本不会被保留。

解决方法：单击导航到“部 署”> “选择站点”，为每个站点手动 选择部分站点升级软件版本。

[SDW-22374]

有时，在执行管理接口设置的配置后，用户界面会显示错误。但是，配置成功，需要刷新才能在用户界面上显示更新的设置。

[SDW-22139]

在提供商管理的设置中，提供商管理员添加的公告不会在客户登录时显示给他们。

[SDW-18491]

本地 **SD-WAN Orchestrator 13.2.1** 版本的发行说明

October 21, 2022

本发行说明文档介绍了 Citrix SD-WAN Orchestrator 本地版本 Build 13.2.1 中存在的增强功能和更改、已修复和已知问题。

备注

本发行说明文档不包括与安全相关的修补程序。有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。

已修复的问题

版本 13.2.1 中解决的问题。

平台和系统

适用于本地的 Citrix SD-WAN Orchestrator 将 TCP 同步数据包发送到 AWS 终端节点。

[SDW-23477]

已知问题

13.2.1 版中存在的问题。

其他

有些站点无法连接到适用于本地用户界面的 Citrix SD-WAN Orchestrator。

解决方法：使用 172.17.x.x 子网以外的其他子网。

[SDWANHELP-2601]

在某些情况下，在为站点部署 Cloud Direct 并推送配置（暂存和激活）后，Cloud Direct 服务无法启动。

解决方法：为每个站点手动启用 Cloud Direct 服务。

[SDW-22493]

当用户返回此页面时，先前在 UI 的“部署”**>**“设置”>“站点部分升级”>“软件版本”页面上选择的软件版本不会被保留。

解决方法：导航到“部 署”>“选择站点”，手动为每个站点 选择部分站点升级软件版本。

[SDW-22374]

有时，在执行管理接口设置的配置后，用户界面会显示错误。但是，配置成功，需要刷新才能在用户界面上显示更新的设置。

[SDW-22139]

在提供商管理的设置中，提供商管理员添加的公告不会在客户登录时显示给他们。

[SDW-18491]

平台和系统

无法访问其中一个 Citrix SD-WAN 设备的用户界面，因为网络统计提供商正在重复使用会话，这导致 HTTPD 进程行为不正常（在极少数情况下）。

[SDW-23392]

在 Citrix SD-WAN 210 设备上，如果您移除 SE 附加许可证，则服务将被禁用。

解决方法：在删除 SE 附加许可证（或）从 AE 移至 SE 许可证之前，请删除具有安全配置文件的防火墙策略，将设备配置为带外管理（如果配置了带内管理），然后继续转储和激活过程以将设备转换为标准版。

[SDW-18031]

本地 **SD-WAN Orchestrator 13.2** 版本的发行说明

October 21, 2022

本发行说明文档介绍了 Citrix SD-WAN Orchestrator 本地版本 Build 13.2 中存在的增强功能和更改、已修复和已知问题。

备注

本发行说明文档不包括与安全相关的修补程序。有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。

新增功能

版本 13.2 中提供的增强功能和更改。

配置和管理

恢复以前的版本

适用于本地的 Citrix SD-WAN Orchestrator 引入了恢复先前版本的功能。选择“恢复以前的版本”选项后，Citrix SD-WAN Orchestrator for Inclouse 将在网络范围内激活以前的配置，并在您的网络上恢复之前激活的配置（/软件）。

[SDW-22042]

许可增强功能

检索许可证并将其升级到生产环境后，“升级到生产”按钮标签将更改为“已 升级到生产”，表示许可证升级已完成。

[SDW-20674]

API-站点地址解析：

使用 API 创建站点时，会使用纬度和经度值自动获取站点地址，这些值是在网站创建过程中使用 Google Maps API 传递的。

[SDW-20654]

网络菜单重组

Citrix SD-WAN Orchestrator 本地全局配置菜单已经过重组，以帮助更好地对 Citrix SD-WAN 的关键功能进行分类和发现。此外，每种交付服务现在都可以在交付渠道和每个关键功能页面中使用，以满足全局或按功能上下文进行管理员配置。例如，管理员可以在第 0 天在交付通道下全局配置 Citrix SIA 服务，也可以在“云安全服务”下执行“安全”下的第 N 天功能以进行任何更改。

网络级别的配置页面增强如下：

- 网络配置主目录 已重命名为 网络主目录。
- 配置 **>** 传送渠道下的交付服务现已重命名为“服务定义”。
- 在“配置” **>** “安全”下，“网络加密”页面重命名为“网络安全”。
- 为便于发现，“配置” **>** “安全”下的页面按逻辑分组如下：

组	菜单选项
SD-WAN 覆盖安全	网络安全
	虚拟路径 IPsec
基础防火墙	防火墙区域
	防火墙默认值
	防火墙策略
IPsec 和 GRE	证书
	IPsec 加密配置文件
	IPsec 服务
	GRE 服务
无线网络安全	半径配置文件
	SSID 配置文件

- 您可以从“配置”> “传送通道”**>** “服务定义”或“配置”“安全”中配置以下服务：
  - IPsec 的
  - GRE
- **ECMP** 组 页面移至“配置”**>** “路由”下。
- 您可以在配置 **>** 路由 下在网络级别配置 **BGP**、**OSPF**、多播组和 **VRRP**。您可以选择一个站点，然后单击“开始”。它将您带到站点级别的特定配置页面。以前，这些配置仅在站点级别可用。
- 您可以通过配置 **>** 交付渠道 **>** 服务定义或配置 **>** 路由 ******SaaS 和 Cloud On Ramp 配置 Cloud**Direct 服务
- 应用程序和 **DNS** 设置 页面已重命名为 应用程序设置和群组。
- 之前位于“配置”**>** “应用程序和 **DNS** 设置”**>** “应用程序设置”下的 **DPI** 相关设置 移至 配置 **>** 应用程序设置和群组 **> DPI** 设置下。
- 位于“配置”**>** “交付 **@@** 服务”下的网络定位服务 页面直接位于“配置”下方。

[SDW-14698]

出错时回滚

在网络部署（激活）期间，未能连接到 Citrix SD-WAN Orchestrator for Inclouse 的站点将回滚到以前的版本以尝试恢复连接。此类网站的回滚是在离线一段指定时间（目前为 30 分钟）后启动的。

如果网络中的任何一个站点正在尝试回滚，则会出现一个弹出框，其中包含两个选项：要么回滚整个网络，要么忽略这些站点并结束部署。

在启动网络部署之前，必须启用“出错时回滚”功能。

[SDW-11153]

其他

IP 规则

在“**IP** 规则”**>** “虚拟路径流量策略”部分下添加了“覆盖服务”选项。当 流量策略 被选为 覆盖服务时，可以选择虚拟路径服务覆盖的服务类型为 Intranet、Internet、直通或丢弃。

[SDW-22213]

配置差异

在网络级别的“配置”下新增了“配置差异”功能。C **onfig Diff** 功能可帮助您查看任意两个版本的配置检查点之间的差异。您还可以在全局和站点级别查看配置。

[SDW-4563]

设备设置

适用于本地的 Citrix SD-WAN Orchestrator 引入了配置管理网络优先级的选项。您可以选择带内或带外作为网络的管理接口。仅当 SD-WAN 设备运行的软件版本为 11.4.2 或更高版本时，此选项才可用。

[NSSDW-35774]

平台和系统

证书身份验证

适用于本地的 Citrix SD-WAN Orchestrator 支持使用公钥基础架构 (PKI) 作为一项额外的安全功能，对静态和动态虚拟路径进行设备身份验证。启用此功能可通过启动交换的设备通过数据路径分发 PKI 证书，从而扩展现有虚拟路径身份验证机制。PKI 增强功能还支持证书吊销列表 (CRL) 管理，以集中撤销受损证书。

[SDW-19295]

提供商审核日志 和 网络审核日志 增强功能

提供商审核日志 和 网络审计日志 页面通过以下选项进行了增强：

- 来源 **IP** -此字段显示配置 SD-WAN 功能的端点的 IP 地址。此字段显示在“审核日志”页面和“审计信息”页面上。
- 导出为 **CSV** -此选项允许您将审计日志导出为 CSV 格式。
- 更改内容 -此部分显示通过用户界面对功能进行的所有更改的日志。启用“日志负载”切换按钮以在“审计信息”页面上查看此部分。目前，此部分可在网络审计信息页面上找到。

[SDW-19219]

自定义端口，基于域名的应用程序的协议配置

基于域名的应用程序现在支持适用于本地的 Citrix SD-WAN Orchestrator 中的可配置端口和协议。选中 配置端口 复选框后，可以根据需要编辑、添加或删除任何端口或端口范围。此外，您还可以将协议更改/选择为 TCP、UDP 或任意。以前（在禁用配置端口复选框的情况下），应用程序下分组的域仅支持端口 80 和 443 以及协议 **Any**。

[NSSDW-29930]

已修复的问题

版本 13.2 中解决的问题。

其他

适用于本地用户界面的 Citrix SD-WAN Orchestrator 无法访问。当 {page.productname}} 中运行的服务无法响应心跳请求并且已超过重启限制时，就会出现此问题。

[SDWANHELP-2544]

在适用于本地的 Citrix SD-WAN Orchestrator 上传软件升级包失败。在软件包上载过程中，当用户离开上传页面时，会出现此问题。

[SDWANHELP-2495]

平台和系统

当 Citrix SD-WAN Orchestrator 为本地部署的 SD-WAN 设备分配许可证后，运行 11.4.1 软件版本的 SD-WAN 设备将进入宽限模式。

[SDW-23171]

已知问题

13.2 版中存在的问题。

配置和管理

在新导入的适用于本地的 Citrix SD-WAN Orchestrator 实例上，暂存停留在“准备软件包”状态。如果在创建新虚拟机后不久启动转储进程，就会出现此问题。

解决方法：重试暂存流程。

[SDW-20863]

其他

运行软件版本为 11.4.2 的 SD-WAN 设备的服务状态在适用于本地用户界面的 Citrix SD-WAN Orchestrator 上显示为 **B** AD。显示的错误消息是 **Orchestrator URL** 没有回应。在 Citrix SD-WAN Orchestrator 中为本地配置自定义域时，会出现此问题。

解决方法：重新启动 SD-WAN 设备。

[SDW-23322]

修改部分站点升级列表并在网络 上执行变更管理（暂存和激活）时，恢复先前版本操作失败，并显示 **PSU** 中站点的激活失败 **(ER101**) 错误消息。

解决方法：在应用“恢复以前的版本”操作之前，再执行一轮变更管理。

[SDW-23227]

在某些情况下，在为站点部署 Cloud Direct 并推送配置（暂存并激活）后，Cloud Direct 服务无法启动。

解决方法：为每个站点手动启用 Cloud Direct 服务。

[SDW-22493]

当用户返回此页面时，先前在 UI 的“部署”**>**“设置”>“站点部分升级”>“软件版本”页面上选择的软件版本不会被保留。

解决方法：单击导航到“部 署”> “选择站点”，为每个站点手动 选择部分站点升级软件版本。

[SDW-22374]

有时，在执行管理接口设置的配置后，用户界面会显示错误。但是，配置成功，需要刷新才能在用户界面上显示更新的设置。

[SDW-22139]

在提供商管理的设置中，提供商管理员添加的公告不会在客户登录时显示给他们。

[SDW-18491]

平台和系统

客户无法向自己的 HTTP 服务器发送推送通知。

[SDW-23134]

本地 **SD-WAN Orchestrator 12.3** 版本的发行说明

July 17, 2023

本发行说明文档介绍了 Citrix SD-WAN Orchestrator 本地版本版本 Build 12.3 中存在的增强功能和更改、已修复问题和已知问题。

注意

本发行说明文档不包括与安全相关的修补程序。有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。

新增功能

版本 12.3 中提供的增强功能和更改。

其他

清除设置

适用于本地的 Citrix SD-WAN Orchestrator 使您能够清除早于清除统计数据间隔天数（默认为 30 天）的历史数据。清除数据后，早于选定天数的历史数据将被删除，不再可用。根据您的 SD-WAN 设备上设置的时区，清除过程在每天凌晨 12:48 左右进行。

[SDW-20402]

零接触部署界面

您可以在适用于本地的 Citrix SD-WAN Orchestrator 上启用零接触部署 (ZTD) 接口。通过双向身份验证保护的 ZTD 接口为 SD-WAN 设备和适用于本地的 Citrix SD-WAN Orchestrator 提供了安全的通信接口。

[SDW-19152]

链接的虚拟路径设置

您可以为虚拟路径和与 WAN 链接关联的动态虚拟路径自定义带宽。当某些站点由于带宽问题显示性能下降迹象时，此功能很有用。

[SDW-9760]

SD-WAN Orchestrator

Syslog 服务器设置

适用于本地的 Citrix SD-WAN Orchestrator 支持配置 SD-WAN 设备的 Syslog 服务器设置。通过启用 Syslog 设置，您可以将 SD-WAN 设备的系统警报和事件详细信息发送到外部 syslog 服务器。

[SDW-13990]

已修复的问题

版本 12.3 中解决的问题。

其他

在某些情况下，启用带内管理并插入带外管理时，SD-WAN 设备无法通过带内管理与 Citrix SD-WAN Orchestrator 进行本地通信。

[SDWANHELP-2368]

尽管允许的最大限制为 32，但当动态虚拟路径值设置为大于 8 时，用户界面错误地显示错误。在 VPXL 和 4100 SE 设备上观察到此问题。

[SDWANHELP-2354]

“部分站点升级”设置下的“软件版本”下拉列表显示所有支持的软件版本，而不是仅显示在“基础架构”> “**Orchestrator** 管理”> “软件映像”下发布的那些版本 家电。

如果部分站点升级中列出的软件版本无法在“基础架构”> “**Orchestrator** 管理”> “软件映像”> “设备”下发布，则无法对该版本执行部分站点升级。

[SDW-20992]

已知问题

12.3 版中存在的问题。

配置和管理

在新导入的适用于本地的 Citrix SD-WAN Orchestrator 实例上，暂存停留在“准备软件包”状态。如果在创建新虚拟机后不久启动转储进程，就会出现此问题。

解决方法：重试暂存流程。

[SDW-20863]

其他

运行 VMware ESXi 13 的本地部署版 Citrix SD-WAN Orchestrator 无法重启并进入错误状态。

解决方法：使用 VMware ESXi 版本 9。

[SDWANHELP-2182]

在某些情况下，在为站点部署 Cloud Direct 并推送配置（暂存并激活）后，Cloud Direct 服务无法启动。

解决方法：为每个站点手动启用 Cloud Direct 服务。

[SDW-22493]

当用户执行部分站点升级时，暂存过程会间歇性失败。用户界面显示错误消息“由于异常而暂存失败”。

解决方法：重试暂存流程。

[SDW-22398]

当用户返回此页面时，先前在 UI 的“部署”**>**“设置”>“站点部分升级”>“软件版本”页面上选择的软件版本不会被保留。

解决方法：单击导航到“部 署”>“选择站点”，为每个站点手动 选择部分站点升级软件版本。

[SDW-22374]

有时，在执行管理接口设置的配置后，用户界面会显示错误。但是，配置成功，需要刷新才能在用户界面上显示更新的设置。

[SDW-22139]

用户无法删除在用户界面 基础架构 > Orchestrator 管理 **>** 软件映像页面上传的 **Citrix SD-WAN Orchestratorfor Inclouse **tar.gz** 映像文件。显示的错误信息是删除软件包时出错 **。

解决方法：上传新的软件包。之前上传的文件会被自动删除。

[SDW-22137]

在用户界面的 配置 > 网络配置主 页上，上传配置文件后，辅助 SD-WAN 设备的 Orchestrator 连接状态立即显示为联机。但是，保存站点的配置后，会显示正确的状态。

[SDW-20913]

在提供商管理的设置中，提供商管理员添加的公告不会在客户登录时显示给他们。

[SDW-18491]

在具有相同版本的 Citrix SD-WAN Orchestrator for Inclouse 的另一台设备上恢复设备的数据库备份时，不会恢复用户详细信息。在恢复的设备上，如果您创建的用户名与备份数据库中的用户名相同，则会显示以下错误：

`User has a role already assigned`。

解决方法：使用备份数据库中不存在的不同用户名创建用户。

[SDW-15984]

平台和系统

在 Citrix SD-WAN 210 设备中，如果您删除附加许可证，服务将被禁用。

解决方法：移除具有安全配置文件的防火墙策略，暂存并激活更改以将设备转换为标准版。

[SDW-18031]

本地 **SD-WAN Orchestrator 11.4.0a** 版本的发行说明

July 17, 2023

本发行说明文档介绍了 Citrix SD-WAN Orchestrator 本地发行版 Build 11.4.0a 中存在的增强功能和更改、已修复和已知问题。

备注

- 适用于本地 11.4.0a 的 Citrix SD-WAN Orchestrator 解决了 SDWANHELP-2317 中描述的问题，取代了 11.4 版。
- 本发行说明文档不包括与安全相关的修补程序。有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。

新增功能

Build 11.4.0a 中提供的增强功能和更改。

配置和管理

HTTP 代理

你可以在 Citrix SD-WAN Orchestrator 上为本地配置 HTTP 代理设置。此功能集中管理向 Citrix Cloud 发出的所有传出请求。管理员可以通过 HTTP 代理服务器将来自本地的 Citrix SD-WAN Orchestrator 的传出请求路由到 Citrix Cloud。

[SDW-20247]

云直接服务

适用于本地的 Citrix SD-WAN Orchestrator 支持云直接服务。

无论主机环境（数据中心、云和互联网）如何，Cloud Direct 服务均通过可靠和安全地交付所有互联网流量，以云服务的形式提供 SD-WAN 功能。

Cloud Direct 服务改善了网络的可见性和管理。通过此软件，合作伙伴可以为业务关键型 SaaS 应用程序为其最终客户提供托管 SD 服务。

[SDW-16396]

存储管理-正式上市

存储管理功能现在支持正式发布。

适用于本地的 Citrix SD-WAN Orchestrator 支持将配置和数据从一个磁盘迁移到另一个磁盘。您可以执行磁盘迁移以增加磁盘空间或用于灾难恢复。

- 添加新磁盘：您可以添加一个新磁盘，其存储大小至少是 Citrix SD-WAN Orchestrator for Inclouse 消耗的当前数据的两倍。
- 灾难恢复：发生灾难时，您可以将包含用于本地配置的 Citrix SD-WAN Orchestrator 和数据的磁盘连接到适用于本地虚拟机的 Citrix SD-WAN Orchestrator 的新实例。

[SDW-21316]

云代理零接触部署-正式上市

云代理零接触部署功能现在支持正式上市。

云代理零接触部署是一个自动化流程，它涉及本地的 Citrix SD-WAN Orchestrator 作为代理，在适用于本地的 Citrix SD-WAN Orchestrator 和 Citrix SD-WAN 设备之间建立连接。

[SDW-21312]

Citrix SD-WAN 11.4.1 版本

适用于本地 11.4 的 Citrix SD-WAN Orchestrator 支持 Citrix SD-WAN 11.4.1 版本。

[SDW-21082]

平台和系统

ICMP 探测

适用于本地的 Citrix SD-WAN Orchestrator 支持 ICMP 探测。它使管理员能够确定进出 SD-WAN 设备和目标主机的互联网可访问性。用户界面中引入了以下 ICMP 服务：

- 使用 ICMP 探测器确定链路上互联网的可访问性
- IPv4 ICMP 端点地址
- 探测间隔（以秒为单位）
- 重试次数

[SDW-19292]

覆盖全球交通节点设置

现在，您可以覆盖全局交通节点设置，并选择仅在选定的控制交通节点上启用或禁用分支到分支转发和路由导出。

[SDW-19276]

成员路径统计 **API**（预览版）：

修改成员路径统计信息 API 以允许 API 客户端指定感兴趣的字段。指定的字段将在响应负载中返回。

[SDW-18903]

网站报告：VRRP

VRRP 报告提供已配置 VRRP 组的实时报告。

[SDW-12082]

站点报告:IGMP

IGMP 报告表提供 IGMP 统计数据和 IGMP 代理组的实时报告。

[SDW-12077]

站点报告：IPsec

IPsec 报告提供网络上 IPsec 隧道配置的实时报告。

[SDW-12076]

站点报告：路由协议

路由协议 报告提供与路由协议相关的参数的详细信息。您可以根据需要从“查看”下拉列表中选择协议，然后从“路由域”下拉列表中选择路由域。要查看当前数据，请单击“检索最新数据”。

[SDW-12075]

提供商审计日志、 网络审核日志

提供商级别和网络级别的审核日志页面已得到增强，具有以下功能：

- 搜索：能够根据关键字搜索审计活动。
- 筛选：根据用户、功能和时间范围进行筛选，运行审核日志搜索。对于网络级别的日志，您也可以按站点进行筛选。
- 审计信息：选择“操作”列上的信息图标以导航到“审计信息”部分。本部分提供以下信息：
- 方法：调用的 API 的 HTTP 请求方法。
- 状态：API 请求的结果。当 API 请求失败时，你会看到一条错误消息。
- 负载消息：通过 API 发送的请求消息的正文。
- 网址：已撤销的 API 的 HTTP 网址。
- 记录有效负载：默认情况下，此选项处于禁用状态。启用后，API 消息的请求正文将显示在“审计信息”部分中。

[SDW-18937]

选址组件

以下配置中站点选择组件的可用性因其可用性而得到改进：

1. 网站部分升级
2. 网络定位服务
3. 路由策略
4. QoS 策略
5. 导入路径过滤器
6. 导出路径过滤器
7. 代理自动配置

8. 入侵防御
9. 防火墙策略
10. 应用程序设置

[SDW-16895]

已修复的问题

版本 11.4 中解决的问题。

其他

云中介 ZTD 功能依赖于 SD-WAN Orchestrator 服务才能正常运行。这个问题将在即将发布的 SD-WAN Orchestrator 版本中得到解决。但是，客户无需升级适用于本地的 Citrix SD-WAN Orchestrator。

[SDW-20307]

如果已经在主站点上配置了云 ZTD，则 SD-WAN 云 ZTD 配置不适用于 HA 站点。

[SDW-20208]

尽管 SD-WAN 设备 已连接到本地的 **Citrix SD-WAN Orchestrator**，但本地版 **Citrix SD-WAN Orchestrator** 的状态显示为“未 连接”。

[SDW-18280]

已知问题

11.4 版中存在的问题。

配置和管理

在新导入的适用于本地的 Citrix SD-WAN Orchestrator 实例上，暂存停留在“准备软件包”状态。如果在创建新虚拟机后不久启动转储进程，就会出现此问题。

解决方法：重试暂存流程。

[SDW-20863]

其他

运行 Citrix SD-WAN Orchestrator for Inclouse 11.4 的用户将 Citrix SD-WAN 设备升级到 11.4.1 版本时，暂存过程失败。用户界面显示状态为“暂存失败（无法下载脚本文件）”。当 Citrix SD-WAN 设备和适用于本地的 Citrix SD-WAN Orchestrator 之间的带宽较少时，就会出现此问题。

[SDWANHELP-2317]

运行 VMware ESXi 13 的本地部署版 Citrix SD-WAN Orchestrator 无法重启并进入错误状态。

解决方法：使用 VMware ESXi 版本 9。

[SDWANHELP-2182]

用户界面在“配置”**>**“网络配置主页”和“配置”**>**“部署”页面上显示错误的 **SD-WAN** 设备软件版本。对于新安装的本地实例，在用户执行变更管理之前，Citrix SD-WAN Orchestrator 上会出现此问题。

[SDW-21018]

当 Cloud Direct 站点操作失败时，用户界面无法显示错误消息。

[SDW-21009]

“部分站点升级”设置下的“软件版本”下拉列表显示所有支持的软件版本，而不是仅显示在“基础架构”> “**Orchestrator** 管理”> “软件映像”下发布的那些版本 家电。

如果部分站点升级中列出的软件版本无法在“基础架构”> “**Orchestrator** 管理”> “软件映像”> “设备”下发布，则无法对该版本执行部分站点升级。

[SDW-20992]

在用户界面的 配置 > 网络配置主 页上，上传配置文件后，辅助 SD-WAN 设备的 Orchestrator 连接状态立即显示为联机。但是，保存站点的配置后，会显示正确的状态。

[SDW-20913]

在提供商管理的设置中，提供商管理员添加的公告不会在客户登录时显示给他们。

[SDW-18491]

在具有相同版本的 Citrix SD-WAN Orchestrator for Inclouse 的另一台设备上恢复设备的数据库备份时，不会恢复用户详细信息。在恢复的设备上，如果您创建的用户名与备份数据库中的用户名相同，则会显示以下错误：

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

解决方法：使用备份数据库中不存在的不同用户名创建用户。

[SDW-15984]

本地 **11.1** 版本的 **Citrix SD-WAN Orchestrator** 发行说明

July 17, 2023

本发行说明文档描述了适用于本地的 Citrix SD-WAN Orchestrator 版本 11.1 中存在的增强功能和更改、已修复和已知问题。

备注

本发行说明文档不包括与安全相关的修补程序。有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。

新增功能

11.1 版中提供的增强和更改。

Citrix SD-WAN 11.4.0a 版本

适用于本地的 Citrix SD-WAN Orchestrator 支持 Citrix SD-WAN 11.4.0a 版本。

[SDW-19785]

Citrix SD-WAN 11.3.2 版本

适用于本地的 Citrix SD-WAN Orchestrator 支持 Citrix SD-WAN 11.3.2 版本。

[SDW-19038]

路由摘要

适用于本地的 Citrix SD-WAN Orchestrator 引入了对路由汇总功能的增强。通过此增强功能，您可以在不指定网关 IP 地址的情况下添加汇总路由。

[SDW-19404]

ECMP 负载平衡

等价多路径 (ECMP) 组允许您对多条路由进行分组，使用相同的成本、目的地和服务类型。ECMP 负载均衡可确保：

- 通过多个等价连接分配流量。
- 最佳利用可用带宽。
- 如果路由无法到达，则动态将流量传输到其他 ECMP 成员路由。
- ECMP 组可以通过虚拟路径和内联网服务组成。

[SDW-17452]

存储管理（预览版）

适用于本地的 Citrix SD-WAN Orchestrator 支持将配置和数据从一个磁盘迁移到另一个磁盘。您可以执行磁盘迁移以增加磁盘空间或用于灾难恢复。

- 添加新磁盘：您可以添加一个新磁盘，其存储大小至少是 Citrix SD-WAN Orchestrator for Inclouse 消耗的当前数据的两倍。
- 灾难恢复：发生灾难时，您可以将包含用于本地配置的 Citrix SD-WAN Orchestrator 和数据的磁盘连接到适用于本地虚拟机的 Citrix SD-WAN Orchestrator 的新实例。

[SDW-16404]

云代理零接触部署（预览版）

云代理零接触部署是一个自动化流程，它涉及本地的 Citrix SD-WAN Orchestrator 作为代理，在适用于本地的 Citrix SD-WAN Orchestrator 和 Citrix SD-WAN 设备之间建立连接。

[SDW-11614]

公交节点增强功能

在全局设置中启用中心辐条通信允许所有站点将控制节点用作中转节点，默认情况下，进行站点到站点通信。虚拟叠加交通节点的站点特定首选项允许您覆盖网络中所有站点的全局虚拟叠加交通节点设置。您还可以选择非控制节点作为站点的主中转节点。

[SDW-12443]

IPv6 数据层面支持

适用于本地的 Citrix SD-WAN Orchestrator 支持使用 Citrix SD-WAN 软件版本 11.3.1 或更高版本的以下 Citrix SD-WAN 设备配置的 IPv6 地址：

- DNS 服务器
- 流
- 防火墙连接
- IP 组
- 区域
- DHCP 客户端
- IP 规则和应用程序规则
- 网络地址转换
- GRE 服务
- 接口
- Internet 服务
- 邻居发现协议
- 前缀委派组
- IPsec 服务
- HA 设置
- IP 路线
- 带内管理
- DNS 设置
- DHCP 服务器、DHCP 中继和 DHCP 选项集

[SDW-19194]

已修复的问题

11.1 版中解决的问题。

对于低于 11.1 的本地版本，低于 11.2.0 的 SD-WAN 设备版本无法连接到 Citrix SD-WAN Orchestrator。如果用户想要连接运行低于 11.2.0 的软件版本的 SD-WAN 设备，则推荐使用适用于本地 11.1 的 Citrix SD-WAN Orchestrator。

[SDW-20220]

在将客户的帐户升级到生产帐户时出现故障时，用户界面不会显示失败消息。

[SDW-19574]

对于只有永久许可证的预付费客户，在适用于本地的 Citrix SD-WAN Orchestrator 中升级到生产失败。

[SDW-19558]

在适用于本地的 Citrix SD-WAN Orchestrator 中为站点分配永久许可证失败。

[SDW-19556]

分配许可证失败时，UI 不会在“管理”> “许可”下显示失败消息。

[SDW-19238]

尽管客户管理员无权删除远程身份验证服务器，但用户界面仍会显示删除图标。但是，当客户管理员尝试执行删除操作时，会显示以下错误：

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

[SDW-18945]

在提供商级别的“管理”> “公告”页面中，如果您从顶部菜单栏中选择客户，则会显示一个以 网络管理 为标题的空白页面。

[SDW-18944]

导入有效的生产授权后，即使在 向设备分配许可证之前，也可以在许可下使用“升级到生产”选项。

[SDW-18721]

已知问题

11.1 版中存在的问题。

云中介 ZTD 功能依赖于 SD-WAN Orchestrator 服务才能正常运行。这个问题将在即将发布的 SD-WAN Orchestrator 服务版本中得到解决。但是，客户无需升级适用于本地的 Citrix SD-WAN Orchestrator。

[SDW-20307]

当 Citrix SD-WAN Orchestrator for Incloudal 升级到 11.1 版本时，在先前版本中收集的审计日志将 **sdwan-onprem-sp** 显示为用户，并且用户界面上启用了日志负载切换按钮。这些日志将在 92 天后清除。

[SDW-20305]

如果已经在主站点上配置了云 ZTD，则 SD-WAN 云 ZTD 配置不适用于 HA 站点。

解决方法：

1. 导航到“管理”> “ZTD 设置”**>** “**Cloud Brokered ZTD**”，删除主站点云 **ZTD** 配置。
2. 同时为主站点和辅助站点重新配置 Cloud ZTD 站点。

[SDW-20208]

本地版 Citrix SD-WAN Orchestrator 的提供商托管设置不支持许可功能。提供商可以继续使用试用许可证。提供 60 天的宽限期。

[SDW-18831]

当设备与 Citrix SD-WAN Orchestrator for Inclouse 的连接中断超过 20 分钟并进入重新注册阶段时，它会在注册请求中发送错误的序列号。

解决方法：重新启动设备。

[SDW-18781]

在提供商管理的设置中，提供商管理员添加的公告不会在客户登录时显示给他们。

[SDW-18491]

尽管 SD-WAN 设备 已连接到本地的 **Citrix SD-WAN Orchestrator**，但本地版 **Citrix SD-WAN Orchestrator** 的状态显示为“未 连接”。

解决方法：导航到 配置 > 网络配置主页，然后在适用于本地用户界面的 Citrix SD-WAN Orchestrator 上验证设备的连接状态。

[SDW-18280]

在具有相同版本的 Citrix SD-WAN Orchestrator for Inclouse 的另一台设备上恢复设备的数据库备份时，不会恢复用户详细信息。在恢复的设备上，如果您创建的用户名与备份数据库中的用户名相同，则会显示以下错误：

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

解决方法：使用备份数据库中不存在的不同用户名创建用户。

[SDW-15984]

运行 VMware ESXi 13 的本地部署版 Citrix SD-WAN Orchestrator 无法重启并进入错误状态。

解决方法：使用 VMware ESXi 版本 9。

[SDWANHELP-2182]

本地 **10.3** 版本的 **Citrix SD-WAN Orchestrator** 发行说明

October 21, 2022

本发行说明文档描述了适用于本地的 Citrix SD-WAN Orchestrator 版本 10.3 中存在的增强功能和更改、已修复和已知问题。

备注

本发行说明文档不包括与安全相关的修补程序。有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。

新增功能

10.3 版中提供的增强和更改。

配置和管理

动态路由

从 Citrix SD-WAN 11.3.1 版本开始，您可以为整个协议配置一个路由器 ID，也可以为每个路由域配置一个路由器 ID。通过此增强功能，您可以在多个实例之间启用稳定的动态路由，使不同的路由器 ID 以稳定的方式聚合。

[SDW-17097]

重试暂存

重试暂存选项现在可用于在暂存过程失败的站点重新启动暂存。

[SDW-16538]

自定义应用程序

为基于 IP 协议的自定义应用程序新增了“启用报告”复选框。现在，您还可以在“报告”“使用情况”页面下查看基于 IP 协议和域名的自定义应用程序定义流量。自定义应用程序选项也作为一种类型添加到“应用程序质量配置”页面下。

[SDW-10862]

其他

回退配置

回退配置可确保在发生链路故障、配置不匹配或软件不匹配时设备保持与零接触部署服务的连接。默认情况下，在具有默认配置文件的设备上启用回退配置。如果在站点禁用了备用配置，则可以通过适用于本地的 Citrix SD-WAN Orchestrator 将其启用。

[SDW-13978]

流

现在，您可以使用设备设置 流量 部分来执行以下操作：

- 启用/禁用 Citrix 虚拟广域网服务
- 重启动态路由
- 启用/禁用虚拟路径
- 启用/禁用 WAN 链接

[SDW-13977]

网络管理员和安全管理员角色（预览版）

适用于本地的 Citrix SD-WAN Orchestrator 支持以下角色：

- **Provide-Network-Admin**：只能查看和编辑网络相关信息的管理员。
- **Provider-Security-Admin**：只能查看和编辑安全相关信息的管理员。
- 客户网络管理员：只能查看和编辑网络相关信息的客户管理员。
- 客户安全管理员：只能查看和编辑安全相关信息的客户管理员。

[SDW-13845]

设备设置

现在，您可以通过 Citrix SD-WAN Orchestrator 在站点级别配置日期和时间。您可以手动配置日期和时间，也可以通过 NTP 服务器配置日期和时间，也可以设置时区。

[SDW-13321]

提供商级别支持

适用于本地的 Citrix SD-WAN Orchestrator 支持多租户。借助多租户功能，可以使用适用于本地实例的单个 Citrix SD-WAN Orchestrator 管理多个客户账户。您可以使用以下设置类型之一。

- 提供商托管设置：客户使用多租户功能使用 Citrix 合作伙伴提供的托管 Citrix SD-WAN Orchestrator for 本地服务。
- 客户托管设置：客户将其适用于本地的 Citrix SD-WAN Orchestrator 作为企业的自我管理服务进行管理。

作为提供商托管安装支持的一部分，引入了以下功能：

- 角色：添加了以下提供商级别的角色：
  - Provider-Master-Admin-All
  - Provider-Master-Admin-Tenant
  - Provider-master-read-all
- 控制面 @@ 板：添加了一个新的用户界面页面，提供提供商管理的所有 SD-WAN 客户的鸟瞰图。

- 与 **SD-WAN** 设备的连接：在提供商托管设置中，只有提供商能够启用身份验证类型并重新生成 Citrix SD-WAN Orchestrator for Incloudal 证书。客户可以上传设备证书。
- 站点配置文件模板和 **WAN** 链接模板：这些模板允许在客户级别创建 站点配置 文件和 **WAN** 链接配置文件。
- 发布软件：适用于本地的 Citrix SD-WAN Orchestrator 允许提供商管理员下载网络中所有设备所需的 Citrix SD-WAN 设备软件版本。提供商可以发布下载的软件版本。已发布的软件已下载并存储在适用于本地的 Citrix SD-WAN Orchestrator 中。客户管理员可以将已发布的软件部署到由 Citrix SD-WAN Orchestrator 管理的所有本地设备上。
- 管理：提供商管理员可以配置管理 IP、DNS、NTP 服务器和远程身份验证服务器。
- 公告：提供商可以使用 公告 选项向其客户发送公告或通知。
- 报告：提供 商报告 提供商管理的所有客户汇总的警报、使用趋势和库存的可见性。

[SDW-12589]

零接触部署-批处理站点

现在，您可以导入 CSV 文件来同时为零接触部署添加多个站点。用户界面中提供了可下载的示例模板，下载该模板并提供所有站点详细信息。

[SDW-12249]

平台和系统

站点报告：WAN 链路计量

WAN 链路计量 报告提供有关计量的 WAN 链路使用情况的详细信息。您可以查看报告，深入了解按流量计费的 WAN 链接的数据消耗情况。

[SDW-8892]

已知问题

10.3 版中存在的问题。

配置和管理

对于带内 HA，GUI 无法选择将服务类型设置为“任意”的目标规则的方向，从而导致出站规则失败。错误消息 [EC818] At Site site-name：当方向为出站时，可能无法使用服务类型“any”。

[SDW-16968]

其他

尽管客户管理员无权删除远程身份验证服务器，GUI 仍会显示删除图标。但是，当尝试执行删除操作时，会显示以下错误：

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

[SDW-18945]

在提供商级别的“管理”**>**“公告”页面中，如果您从顶部菜单栏中选择客户，则会显示一个以 网络管理 为标题的空白页面。

[SDW-18944]

您无法在客户管理的设置上恢复在提供商管理的设置中创建的数据库备份。同样，您无法在提供商管理的设置上恢复在客户管理的设置中创建的数据库备份。

[SDW-18904]

当对站点配置具有只读访问权限的客户安全管理员角色尝试编辑配置时，会显示带有错误消息的红色横幅，而不是显示未经授权的访问。

[SDW-18840]

本地版 Citrix SD-WAN Orchestrator 的提供商托管设置不支持许可功能。提供商可以继续使用试用许可证。将提供 60 天的宽限期。

[SDW-18831]

当设备与 Citrix SD-WAN Orchestrator for Inclouse 的连接中断超过 20 分钟并进入重新注册阶段时，它会在注册请求中发送错误的序列号。

解决方法：重新启动设备。

[SDW-18781]

导入有效的生产授权后，即使在 将许可证分配给设备之前，也可以在“许可”下使用“升级到生产”选项。

解决方法：只有在 为设备分配许可证后，才单击“升级到生产”。

[SDW-18721]

适用于本地的 Citrix SD-WAN Orchestrator 与设备之间不支持网络地址转换 (NAT)。

[SDW-18703]

在提供商管理的设置中，提供商管理员添加的公告不会在客户登录时显示给他们。

[SDW-18491]

CLI 允许用户创建超出允许的 8—128 长度范围的密码，但如果密码长度超出允许范围，GUI 登录将失败。

解决方法：登录 GUI 时，强制用户将密码长度更改为允许的范围。

[SDW-16068]

当用户尝试登录时，红色横幅可能会在页面顶部显示不到一秒钟，然后才显示登录页面。

[SDW-16024]

在具有相同版本的 Citrix SD-WAN Orchestrator for Inclouse 的另一台设备上恢复设备的数据库备份时，不会恢复用户详细信息。在恢复的设备上，如果您创建的用户名与备份数据库中的用户名相同，则会显示以下错误：

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

解决方法：使用备份数据库中不存在的不同用户名创建用户。

[SDW-15984]

本地 **9.6** 版本的 **Citrix SD-WAN Orchestrator** 发行说明

July 17, 2023

本发行说明文档描述了适用于本地的 Citrix SD-WAN Orchestrator 9.6 版的增强功能和更改、已修复和已知问题。

> 注意：
>
> 本发行说明文档不包括与安全相关的修复。有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。

新增功能

9.6 版中提供的增强和更改。

配置和管理

动态路由

从 Citrix SD-WAN 11.3.1 版本开始，您可以为整个协议配置一个路由器 ID，也可以为每个路由域配置一个路由器 ID。通过此增强功能，您可以在多个实例之间启用稳定的动态路由，使不同的路由器 ID 以稳定的方式聚合。

[SDW-17097]

其他

HTTPS 证书

建立与本地版 Citrix SD-WAN Orchestrator 的安全管理 HTTPS 连接需要 HTTPS 证书。您可以使用适用于本地 GUI 的 Citrix SD-WAN Orchestrator 上提供的默认证书，也可以上传从任何其他框架（例如 OpenSSL）生成的自定义 HTTPS 证书。自定义 HTTPS 证书允许您控制安全性以及与证书相关的其他主题参数。

[SDW-16359]

接口

从 Citrix SD-WAN 11.3.1 版本开始，您可以使用“启用”复选框 启用 或禁用虚拟接口。

[SDW-15993]

已修复的问题

9.6 版中解决的问题。

配置和管理

对于 Citrix SD-WAN 6100 SE 设备，用户界面不会在 配置 **>** 高级设置 下显示 **LAG** 页面。

[SDWANHELP-1895]

其他

适用于本地 GUI 的 Citrix SD-WAN Orchestrator 提示用户每隔一小时登录一次，即使 GUI 处于持续使用状态且未处于空闲状态。

[SDWANHELP-1902]

当您通过克隆现有站点创建站点时，部署配置/软件 **>** 验证配置 失败。

[SDW-16103]

已知问题

9.6 版中存在的问题。

其他

如果在身份验证令牌刷新过程中在新选项卡中打开 Citrix SD-WAN Orchestrator for Inclouse GUI，则浏览器中的所有现有会话都将被注销。

[SDW-17719]

如果将磁盘大小调整到超过 1.8 TB，则不会调整磁盘的大小。

[SDW-16404]

CLI 允许用户创建超出允许的 8—128 长度范围的密码。但是，如果密码长度超出允许范围，GUI 登录将失败。

解决方法：登录 GUI 时，强制用户将密码长度更改为允许的范围。

[SDW-16068]

当用户尝试登录时，红色横幅可能会在页面顶部显示不到一秒钟，然后才显示登录页面。

[SDW-16024]

在具有相同版本的 Citrix SD-WAN Orchestrator for Inclouse 的另一台设备上恢复设备的数据库备份时，不会恢复用户详细信息。在恢复的设备上，如果您创建的用户名与备份数据库中的用户名相同，则会显示以下错误：

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

解决方法：使用备份数据库中不存在的不同用户名创建用户。

[SDW-15984]

本地 **1.0** 版本的 **Citrix SD-WAN Orchestrator** 发行说明

October 21, 2022

适用于本地的 Citrix SD-WAN Orchestrator 是一项自托管的管理服务，可作为单独的实例提供给每个客户。它提供了一个单窗格的玻璃管理平台，使您能够配置、监控和分析 SD-WAN 网络上的所有 SD-WAN 设备。

对于在数据主权和数据隐私方面有严格监管要求的客户，建议使用适用于本地的 Citrix SD-WAN Orchestrator。

以下是一些关键功能：

- 身份验证: 支持本地和 RADIUS/TACACS+ 身份验证。
- 集中配置：集中配置 SD-WAN 网络，提供引导式工作流程、视觉辅助工具和配置文件。
- 零接触配置：无缝启动网络和连接。
- 以应用程序为中心的策略：基于应用程序的流量引导、服务质量 (QoS) 和防火墙策略，可全局配置或按站点配置。
- 分层总结运行状况：能够集中监控整个网络的运行状况、使用情况、质量和性能，并能够深入研究各个站点和相关连接。
- 故障排除：设备和审核日志、诊断实用程序，例如 Ping、Traceroute、数据包捕获，用于对网络连接问题进行故障排除。

必备条件

- 电器：至少两台设备。每个 SD-WAN 设备或虚拟实例都必须配置一个 IP 地址。
- **Citrix SD-WAN Orchestrator** 服务帐户：要在本地使用 Citrix SD-WAN Orchestrator，您必须在 Citrix SD-WAN Orchestrator 服务中拥有一个帐户。有关更多信息，请参阅启用 Citrix SD-WAN Orchestrator 服务。

适用于本地 **Citrix SD-WAN Orchestrator 1.0.1**

已修复的问题

- **SDW-16456**：适用于本地的 Citrix SD-WAN Orchestrator 不支持任何路由域。
- **SDW-16063**：在网络级别，Wi-Fi 摘要报告不可用。
- **SDW-16054**：如果在 Citrix SD-WAN Orchestrator 服务上在美国地区之外创建客户账户，则身份和管理 (IDAM) 页面从 Citrix Cloud 获得的 API 令牌不起作用。客户登录本地版 Citrix SD-WAN Orchestrator 失败，并显示以下错误消息：“客户 ID、客户端 ID 或客户端密钥无效”。

  现在，在首次启动 Citrix SD-WAN **O** rchestrator for Incloudator 时，您可以选择登录您的云帐户的 POP。

已知问题

- **SDW-16068**：CLI 允许用户创建超出允许的 8—128 长度范围的密码，但如果密码长度超出允许范围，GUI 登录将失败。
  - 解决方法：登录 GUI 时，强制用户将密码长度更改为允许的范围。
- **SDW-16024**：当用户登录到用户界面时，在显示登录页面之前，页面顶部可能会显示一个红色横幅持续不到一秒钟。
- **SDW-15984**：在具有相同版本的 Citrix SD-WAN Orchestrator for Inclouse 的另一台设备上恢复设备的数据库备份时，不会恢复用户详细信息。在恢复的设备上，如果您创建的用户名与备份数据库中的用户名相同，则会显示以下错误：

  已经为用户分配了角色
  - 解决方法：使用备份数据库中不存在的不同用户名创建用户。
- **SDW-16103**：通过克隆现有站点创建站点时，“部署配置**/**软件”**>** “验证配置”失败。
  - 解决方法：不要通过克隆现有站点来创建站点。
- **SDW-16404**：如果将磁盘大小调整到超过 1.8 TB，则不会调整磁盘的大小。

系统要求和安装

October 21, 2022

在虚拟机 (VM) 上安装 Citrix SD-WAN Orchestrator for Orchestrator 之前，请确保您必须了解硬件和软件要求并满足先决条件。

> 注意
>
> 系统要求对于单区域网络和多区域网络都很常见。

硬件要求

以下是 Citrix SD-WAN Orchestrator for Indealistrator 平均存储 1 个月的数据或每个站点两个 WAN 链接的统计数据的硬件要求：

站点数量	处理器	RAM	存储
2000	256 个 vCPU 3 GHz 或更高	512 GB	2 TB
1000	128 个 vCPU 3 GHz 或更高	256 GB	1 TB
500	64 个 vCPU 3 GHz 或更高	128 GB	500 GB
256	32 vCPU 3 GHz 或更高	64 GB	256 GB
128	8 个 vCPU 3 GHz 或更高	16 GB	256 GB

软件

适用于本地 VPX 的 Citrix SD-WAN Orchestrator 可以在以下平台上配置：

虚拟机管理程序

- VMware ESXi 7.0 更新 1。
- VMware ESXi 服务器，版本 6.5。
- Citrix XenServer 6.5 或更高版本。

浏览器必须启用 cookie，并且已安装并启用了 JavaScript。

以下浏览器支持用于本地 Web 接口的 Citrix SD-WAN Orchestrator：

- Google Chrome 40.0+
- Microsoft Internet Explorer 11+
- 火狐火狐 41.0+

必备条件

以下是安装和部署 Citrix SD-WAN Orchestrator 本地部署的先决条件：

- SD-WAN 主控制节点 (MCN) 和现有客户端节点必须升级到最新的 Citrix SD-WAN 软件版本。

- 建议在 SD-WAN 网络中提供并配置 DHCP 服务器。
- 你必须有适用于本地的 Citrix SD-WAN Orchestrator 安装文件。

> 注意
>
> 您无法在适用于本地的 Citrix SD-WAN Orchestrator 上自定义或安装任何第三方软件。但是，您可以修改 vCPU、内存和存储设置。

下载适用于本地软件的 **Citrix SD-WAN Orchestrator**

从下载页面 下载 适用于本地管理控制台的 Citrix SD-WAN Orchestrator 软件安装文件，适用于所需版本和平台。

适用于本地安装文件的 Citrix SD-WAN Orchestrator 使用以下命名惯例：

- ctx-sdw-onprem-build.ext
- ctx-onprem-build.ext
- ctx-onprem-build.ext

平台	扩展
Citrix XenServer	.xva
VMware ESXi	-vmware.ova

安装和配置清单

本部分提供了完成本地安装和部署的 Citrix SD-WAN Orchestrator 所需信息的清单。

收集或确定以下信息：

- 托管 Citrix SD-WAN Orchestrator 用于本地虚拟机 (VM) 的 ESXi 服务器和 XenServer 的 IP 地址。
- 分配给本地虚拟机的 Citrix SD-WAN Orchestrator 的唯一名称。
- 为本地虚拟机的 Citrix SD-WAN Orchestrator 分配的内存量。
- 要为 VM 的虚拟磁盘分配的磁盘容量。
- 适用于本地的 Citrix SD-WAN Orchestrator 用于与外部网络通信的网关 IP 地址。
- 安装适用于本地虚拟机的 Citrix SD-WAN Orchestrator 的网络的子网掩码。

> 注意
>
> Citrix 建议定期拍摄虚拟机和 SD-WAN 配置的快照。

适用于本地的 **SD-WAN Orchestrator** 和 **Citrix SD-WAN Orchestrator** 服务之间的区别

October 21, 2022

功能

功能	Citrix SD-WAN Orchestrator 服务	适用于本地的 Citrix SD-WAN Orchestrator
高级版平台	是	否
高级版平台	是	否
Zscaler 服务	是	否
Azure 虚拟广域网服务	是	否
Citrix Secure Internet Access 服务	是	否
托管防火墙	是	否
预设 DPI 应用程序和自定义应用程序（基于 FQDN 或 IP）上的应用程序路由	是	是
需要动态签名更新的应用程序（例如 Office 365、Citrix Cloud 和新支持的应用程序）上的应用程序路由。	是	否
Orchestrator-高可用性	是	否

要求

要求	Citrix SD-WAN Orchestrator 服务	本地 SD-WAN Orchestrator
需要 SD-WAN 出厂映像	全部（工厂发货版本）	Citrix SD-WAN 10.2.7、11.1.1、11.2.0、11.2.2、11.3.0 及更高版本。*
部署在网络中的设备	全部	Citrix SD-WAN 11.2.2、11.3.0 及更高版本。*
SD-WAN 设备互联网连接	必需	不是必填项

要求	Citrix SD-WAN Orchestrator 服务	本地 SD-WAN Orchestrator
要打开的防火墙端口	443	443、22、ICMP
Licensing	后付费和预付费模式	仅限预付费模式

- 支持的 Citrix SD-WAN 软件版本取决于适用于本地软件版本的 SD-WAN Orchestrator。

在 **ESXi** 服务器上为本地安装和配置 **SD-WAN Orchestrator**

October 21, 2022

安装 **VMware vSphere** 客户端

以下是下载和安装用于创建和部署适用于本地虚拟机 (VM) 的 Citrix SD-WAN Orchestrator 的 VMware vSphere 客户端的基本说明。

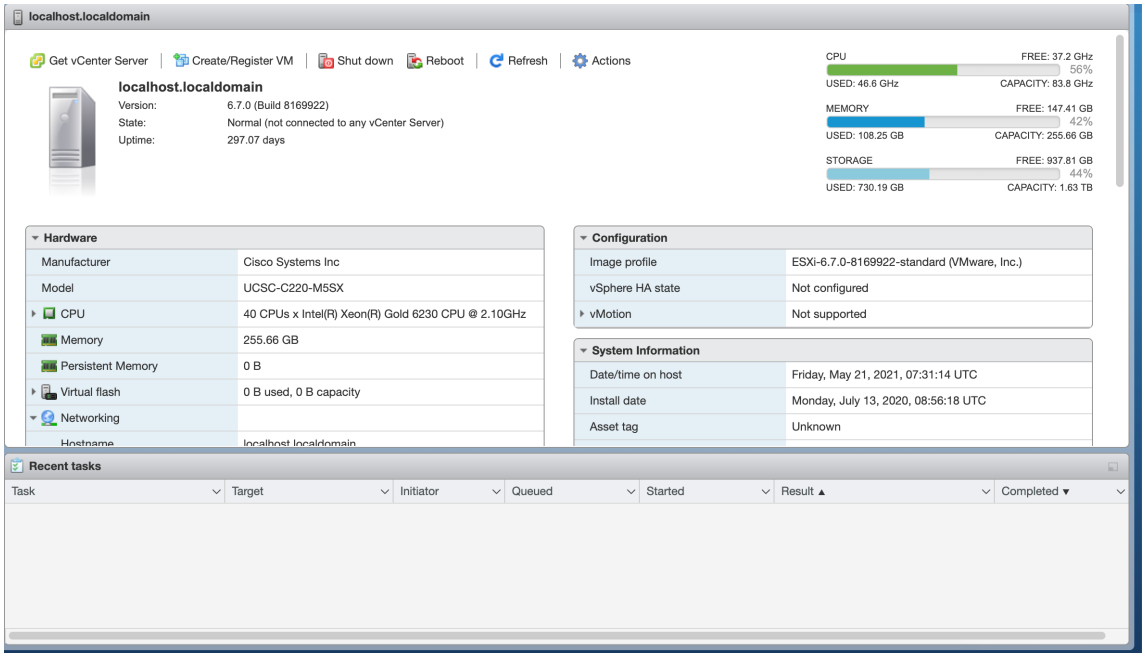
要下载并安装 VMware vSphere 客户端，请执行以下操作：

1. 打开浏览器并导航到托管 vSphere Client 的 ESXi 服务器和适用于本地虚拟机实例的 Citrix SD-WAN Orchestrator。将出现 VMware ESXi 欢迎页面。
2. 单击“下载 **vSphere Client** ”链接以下载 vSphere Client 安装文件。
3. 安装 vSphere 客户端。

   运行您下载的 vSphere Client 安装程序文件，并在出现提示时接受每个默认选项。
4. 安装完成后，启动 vSphere 客户端程序。

   将出现 VMware vSphere Client 登录页面，提示您输入 ESXi 服务器登录凭据。
5. 输入 ESXi 服务器登录凭据：

   - **IP** 地址/名称：输入托管 Citrix SD-WAN Orchestrator for 本地虚拟机实例的 ESXi 服务器的 IP 地址或完全限定域名 (FQDN)。
   - 用户名：输入服务器管理员帐户名。默认值为根。
   - 密码：输入与此管理员帐户关联的密码。
6. 单击“登录”。
   将出现 vSphere 客户端主页面。



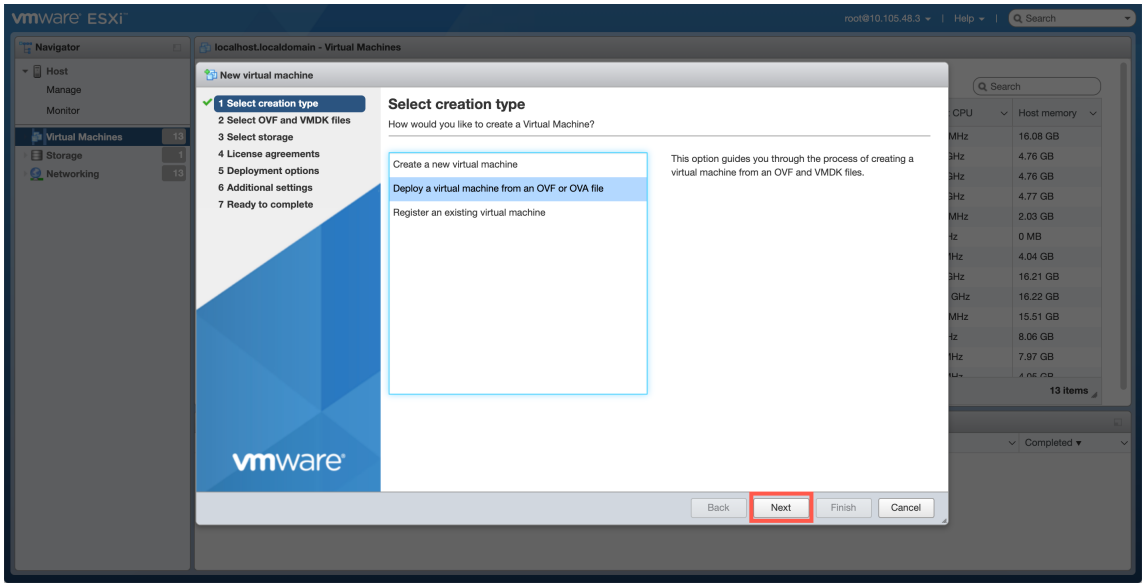
使用 **OVF** 模板为本地虚拟机创建 **Citrix SD-WAN Orchestrator**

安装 VMware vSphere 客户端后，为本地虚拟机创建 Citrix SD-WAN Orchestrator。

1. 如果您尚未这样做，请将 Citrix SD-WAN Orchestrator for 本地 OVF 模板文件（.ova 文件）下载到本地 PC。

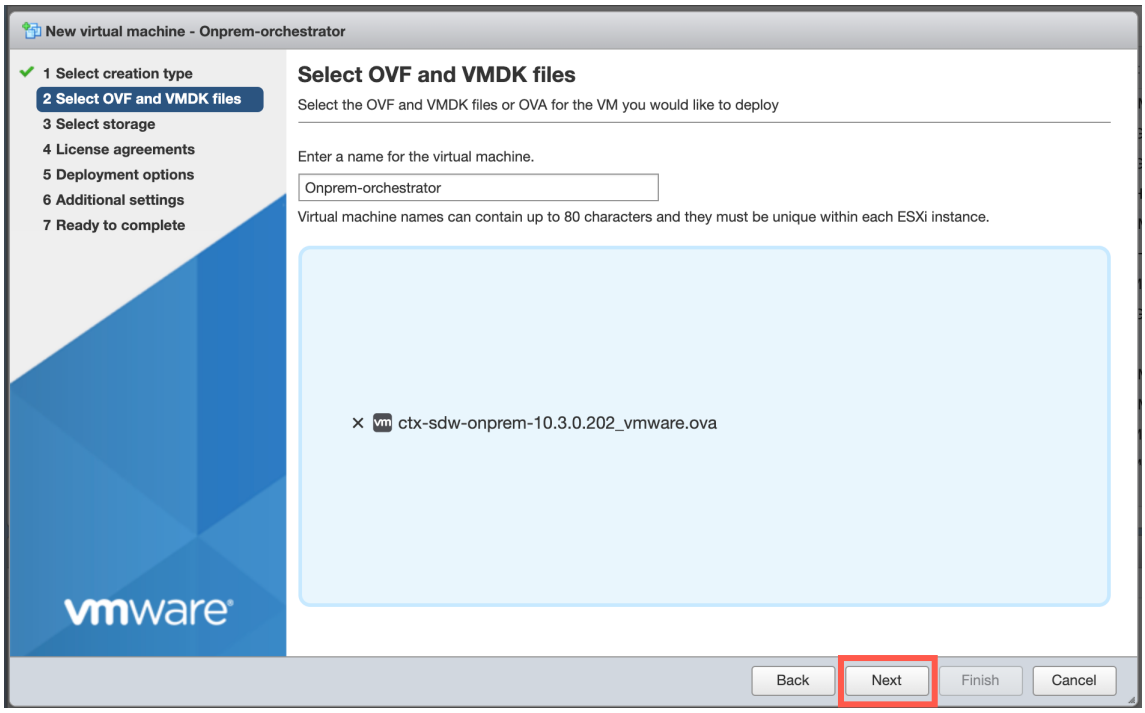
   有关更多信息，请参阅 系统要求和安装。

2. 在 vSphere Client 中，单击“创建/注册虚拟机”，然后从列表中选择“从 **OVF** 或 **OVA** 文件部署虚拟机”。单击下一步。



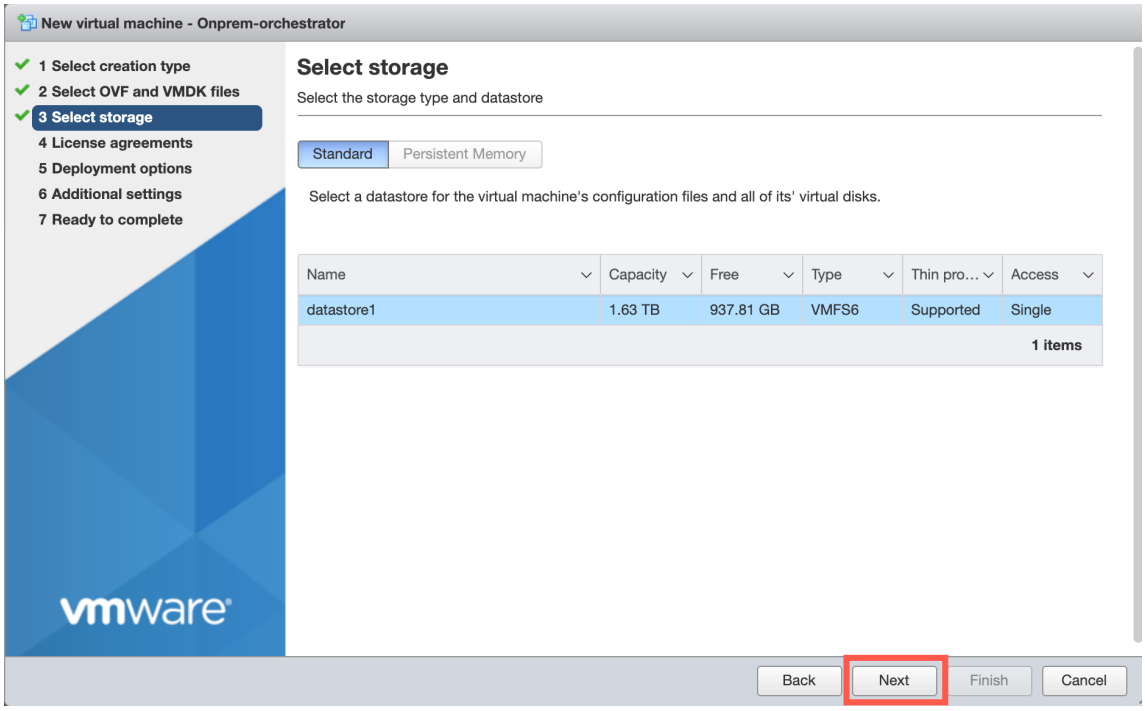
3. 为新虚拟机输入一个唯一名称。

4. 在框内单击，然后选择要安装的 Citrix SD-WAN Orchestrator for Inclouse OVF 模板（.ova 文件），或者您可以将文件拖入框中。
5. 单击下一步。

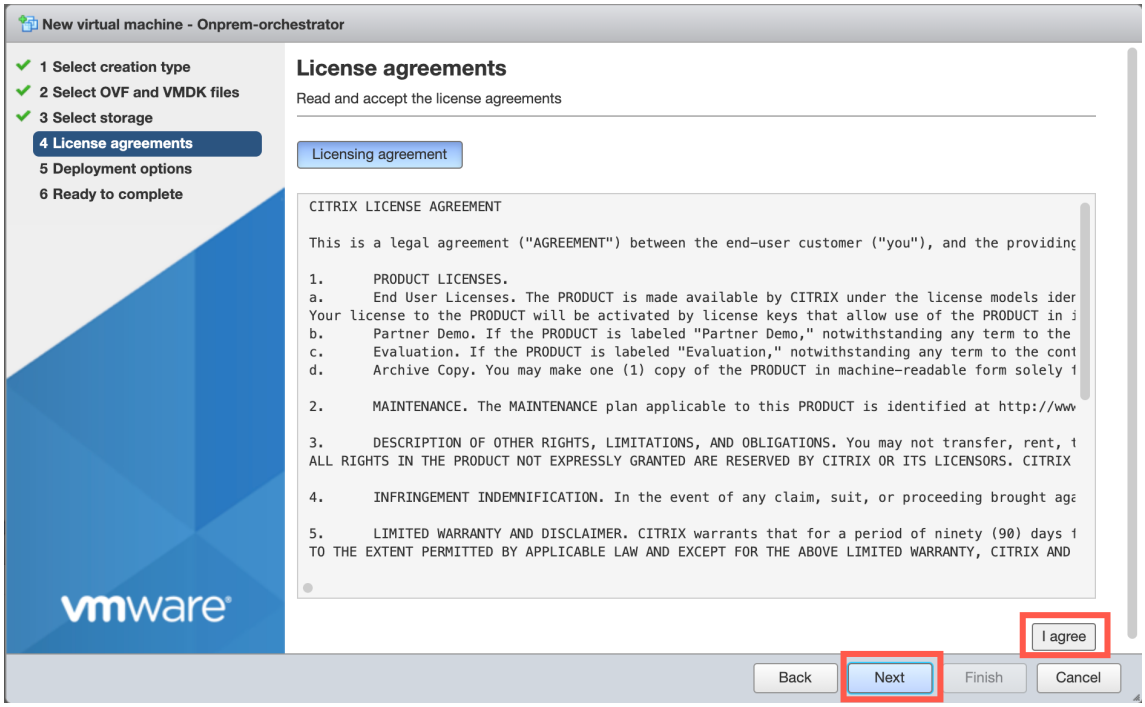


6. 单击下一步。

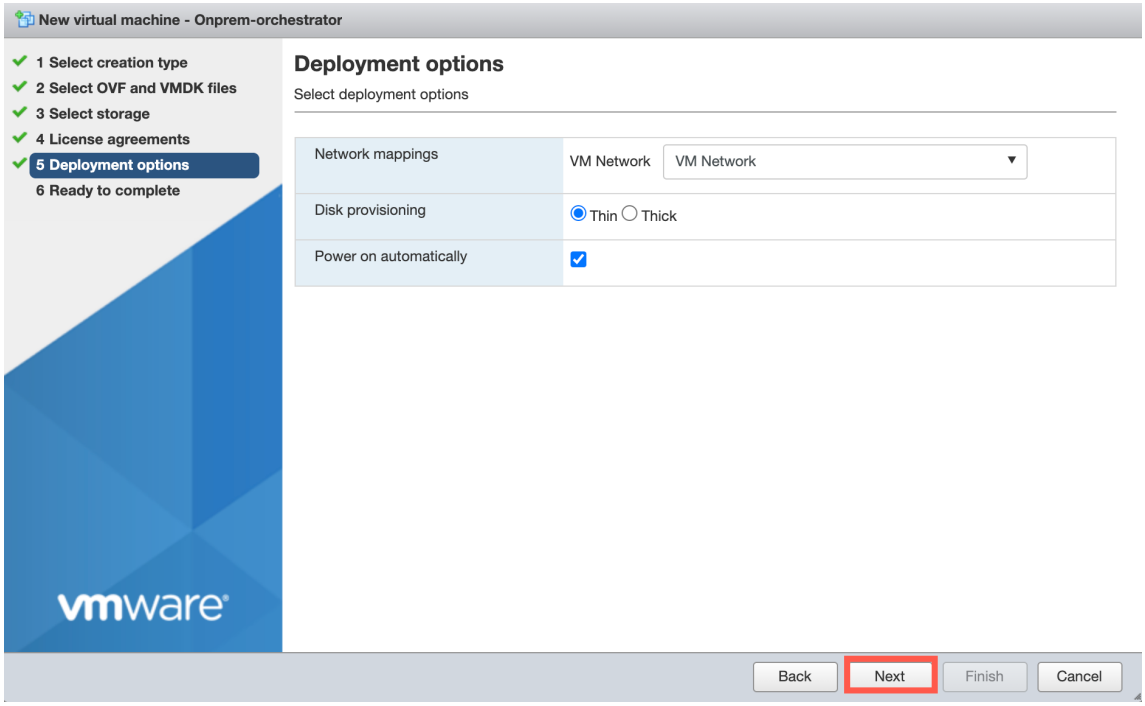
   将显示“存储”页面。
7. 单击“下一步”接受默认存储资源。



8. 在 EULA 页面上，单击“我同意”，然后单击“下一步”。

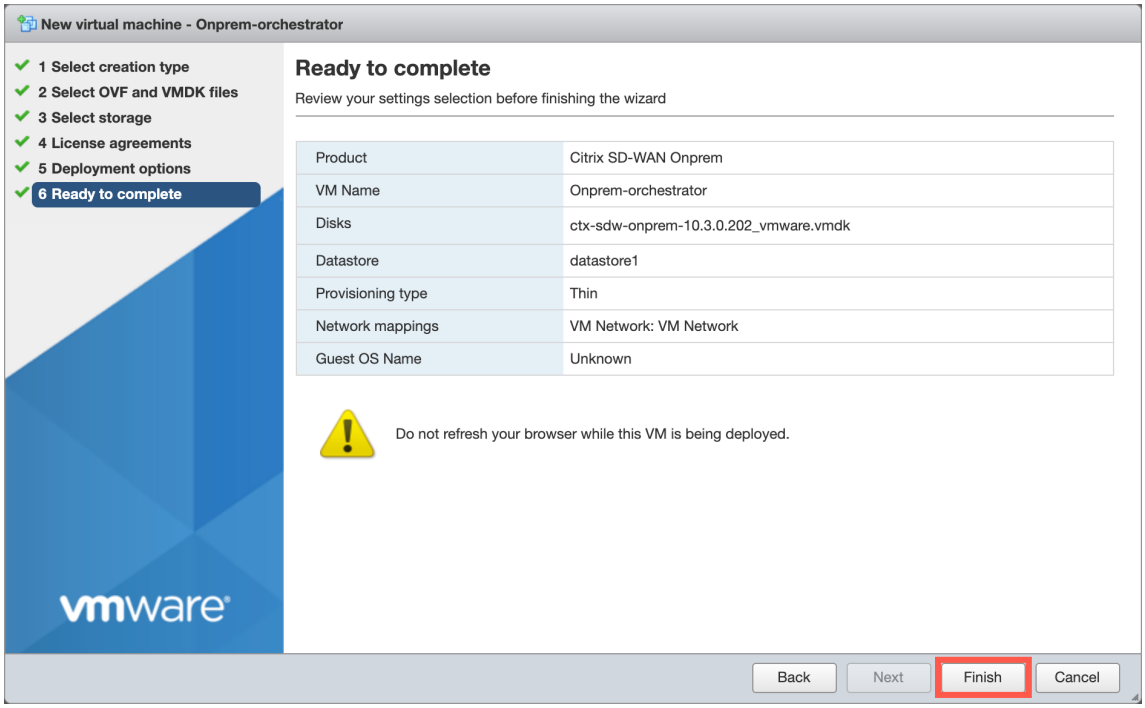


9. 在部署选项页面上，从下拉列表中选择虚拟机网络并接受其他字段的默认设置。单击下一步。



10. 在“即将完成”页面上，单击“完成”以创建虚拟机。

> 注意：
>
> 将磁盘映像解压缩到服务器上可能需要几分钟。

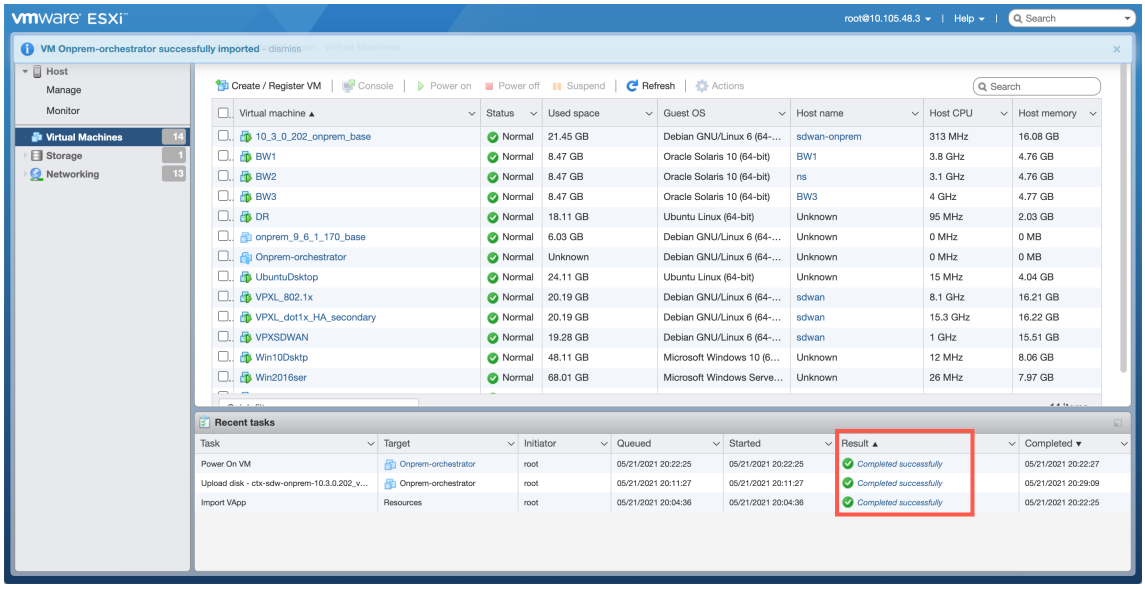


查看和记录 **ESXi** 服务器上的管理 **IP** 地址

管理 IP 地址是适用于本地虚拟机的 Citrix SD-WAN Orchestrator 的 IP 地址，使用此 IP 地址登录本地 Web 用户界面的 Citrix SD-WAN Orchestrator。

要显示管理 IP 地址，请执行以下操作：

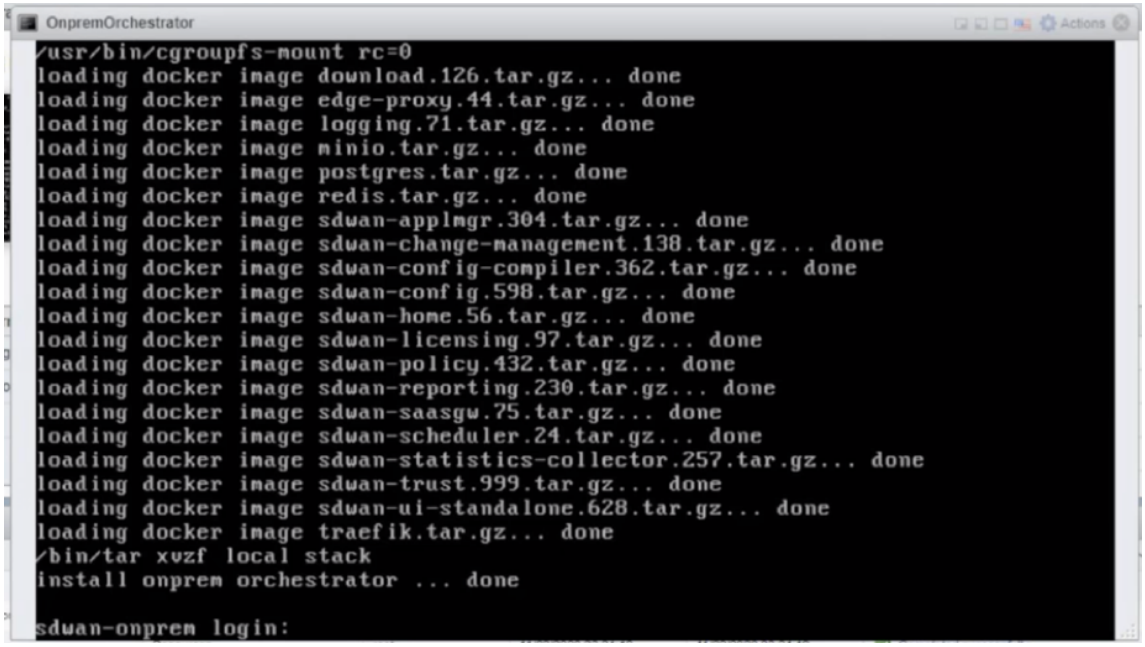
1. 在 vSphere 客户端清单页面上，选择适用于本地虚拟机的新 Citrix SD-WAN Orchestrator。
2. 在 Citrix SD-WAN Orchestrator 本地部署页面上的“近期任务”下，等待结果显示为已完成。



3. 选择 控制台 选项卡，然后单击控制台区域内的任意位置进入控制台模式。

   > 注意
   >
   > 要释放控制台对光标的控制，请同时按下 <Ctrl> 和 <Alt> 键。

4. 按 **Enter** 键显示控制台登录提示。

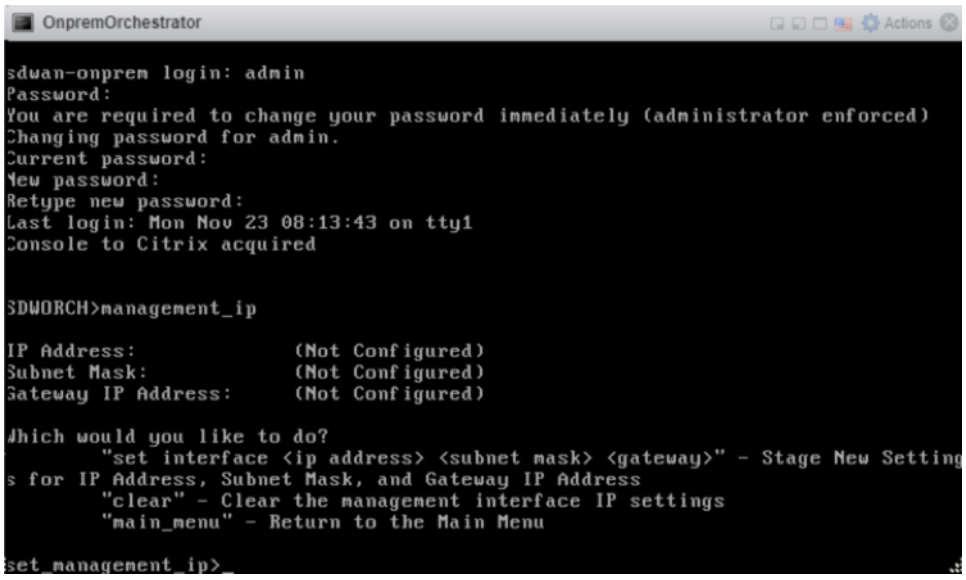


5. 登录到虚拟机控制台。

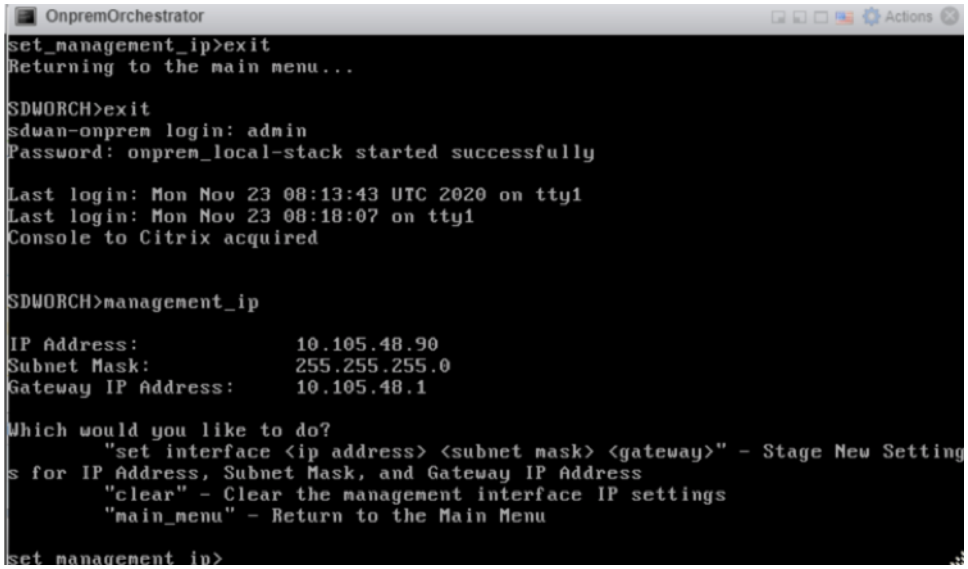
   适用于本地虚拟机的新 Citrix SD-WAN Orchestrator 的默认登录凭据如下所示：

   - 登录：管理员
   - **Password**（密码）：password

   > 注意
   >
   > 首次登录时必须更改默认的管理员用户帐户密码。同时使用 CLI 和 UI 强制执行此更改。



6. 记录 Citrix SD-WAN Orchestrator 用于本地虚拟机的管理 IP 地址，该地址在您登录时显示的欢迎消息中显示为主机 IP 地址。



> 注意
>
> - DHCP 服务器必须存在并且在 SD-WAN 网络中可用，否则此步骤将无法完成。
> - 在控制台中，输入 CLI 命令 `set_dns` 以确认当前的 DNS 服务器设置，如果现有 DNS 服务器无法提供 DNS 服务，则重新配置 DNS 服务器。有关该 `set_dns` 命令用法的更多信息，请参阅用于 本地登录的 Citrix SD-WAN Orchestrator。

如果未在 SD-WAN 网络中配置 DHCP 服务器，则必须手动输入静态 IP 地址。

要将静态 IP 地址配置为管理 IP 地址，请执行以下操作：

1. 虚拟机启动后，单击“控制台”选项卡。
2. 登录到虚拟机。适用于本地虚拟机的新 Citrix SD-WAN Orchestrator 的默认登录凭据如下所示：
   - 登录：管理员
   - **Password**（密码）：password
3. 在控制台中输入 CLI 命令 `management_ip`。
4. 输入命令 `set interface <ipaddress> <subnetmask> <gateway>`以配置管理 IP。
5. 您确定要更改管理接口 IP 设置吗?

   您可能会断开与设备的连接。<y/n>?

   按“y”更改 IP 并在将近 6-7 分钟后访问配置的新管理 IP。

在 XenServer 上安装和配置适用于本地的 SD-WAN Orchestrator

October 21, 2022

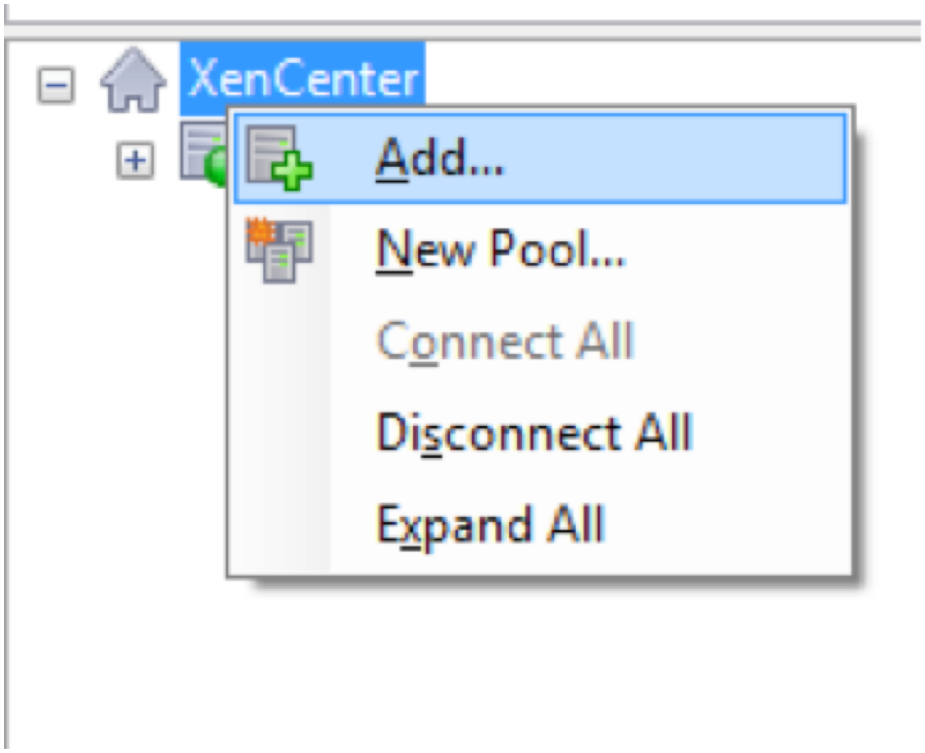
在 XenServer 服务器上安装适用于本地虚拟机的 Citrix SD-WAN Orchestrator 之前，请按照 安装和配置清单中的说明收集必要的信息。

安装 **XenServer** 服务器

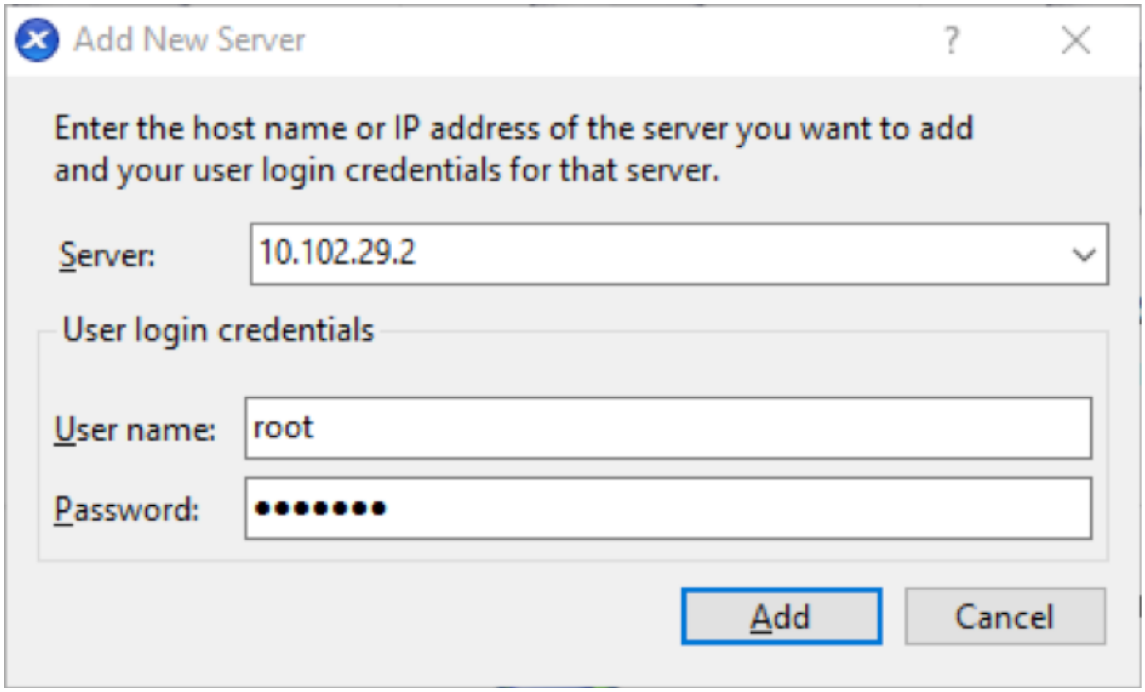
要安装部署 Citrix SD-WAN Orchestrator 适用于本地虚拟机的 Citrix XenServer 服务器，必须在计算机上安装 XenCenter。如果您尚未这样做，请下载并安装 XenCenter。

要安装 XenServer 服务器，请执行以下操作：

1. 在计算机上打开 XenCenter 应用程序。
2. 在左侧树窗格中，右键单击 **XenCenter** 并选择 添加。



3. 在“添加新服务器”窗口中，在以下字段中输入所需信息：
    - 服务器：输入托管本地虚拟机实例的 Citrix SD-WAN Orchestrator 的 XenServer 服务器的 IP 地址或完全限定域名 (FQDN)。
    - 用户名：输入服务器管理员帐户名。默认值为根。
    - 密码：输入与此管理员帐户关联的密码。



4. 单击添加。

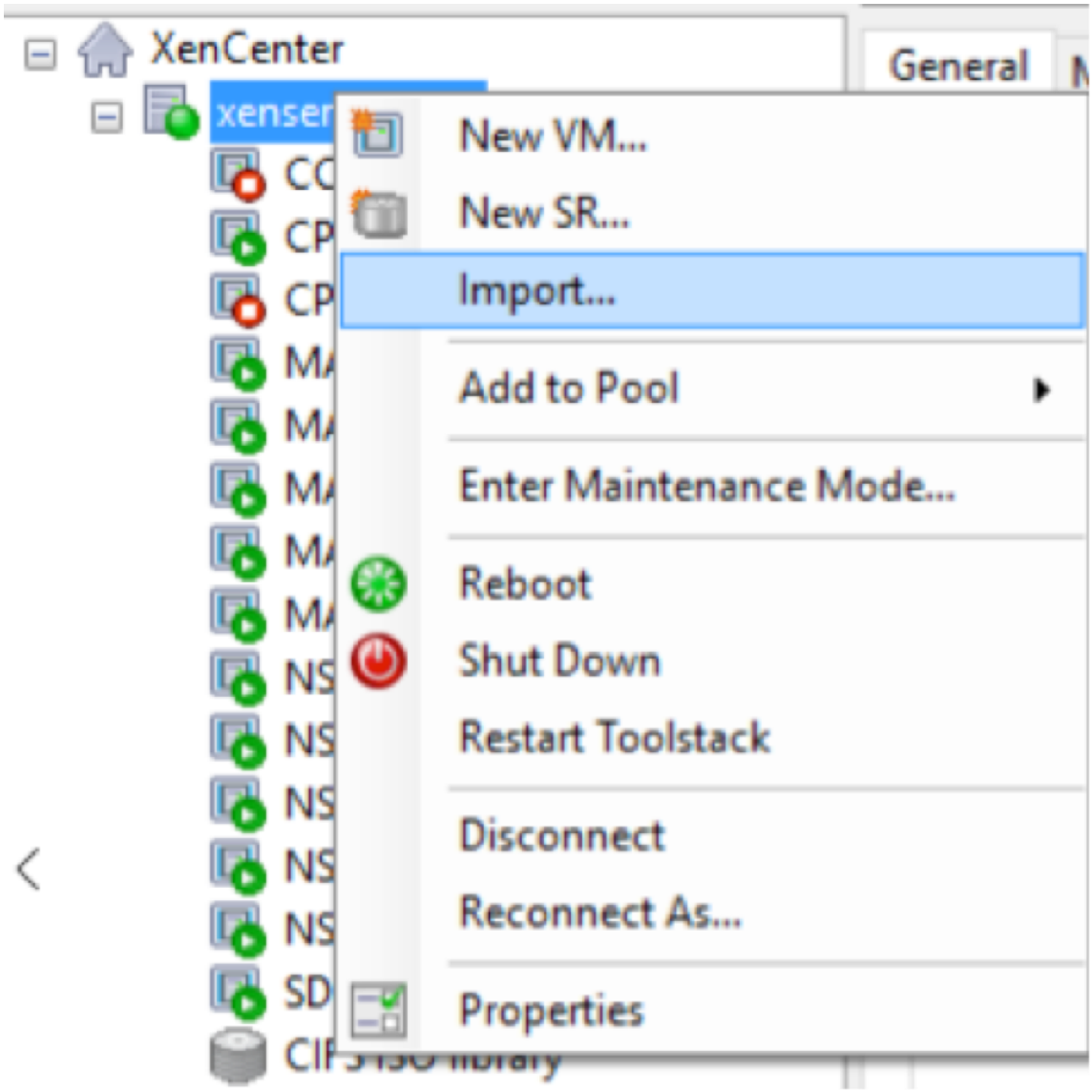
新服务器的 IP 地址显示在左窗格中。

使用 **XVA** 文件为本地虚拟机创建 **Citrix SD-WAN Orchestrator**

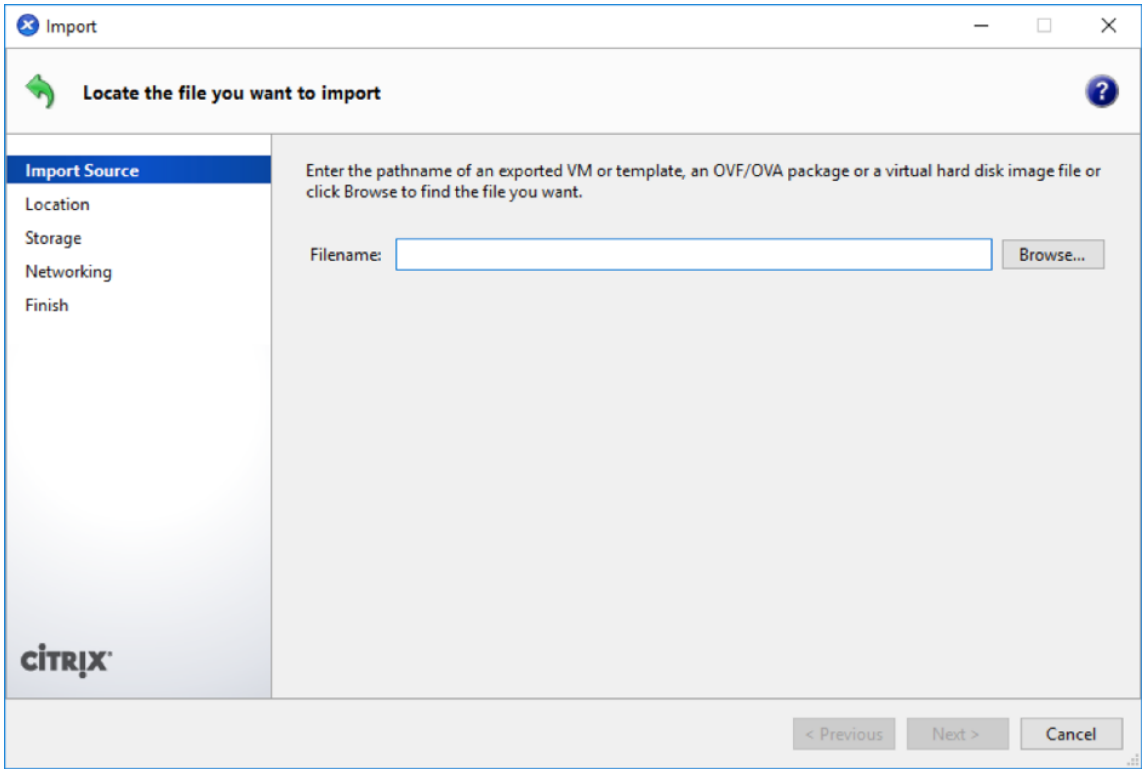
适用于本地虚拟机软件的 Citrix SD-WAN Orchestrator 作为 XVA 文件分发。如果您尚未下载.xva 文件，请下载该文件。有关更多信息，请参阅 系统要求和安装。

要为本地虚拟机创建 Citrix SD-WAN Orchestrator，请执行以下操作：

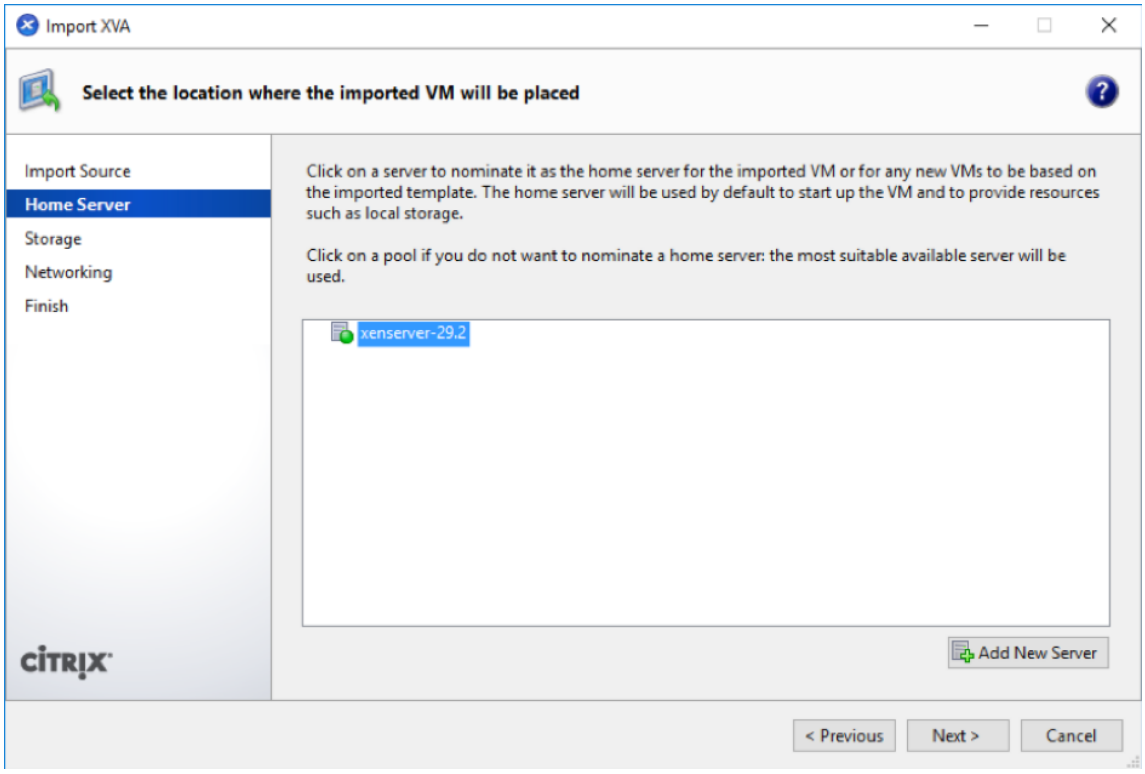
1. 在 XenCenter 中，右键单击 **XenServer** ，然后单击 导入。



2. 浏览到下载的.xva 文件，将其选中，然后单击“下一步”。

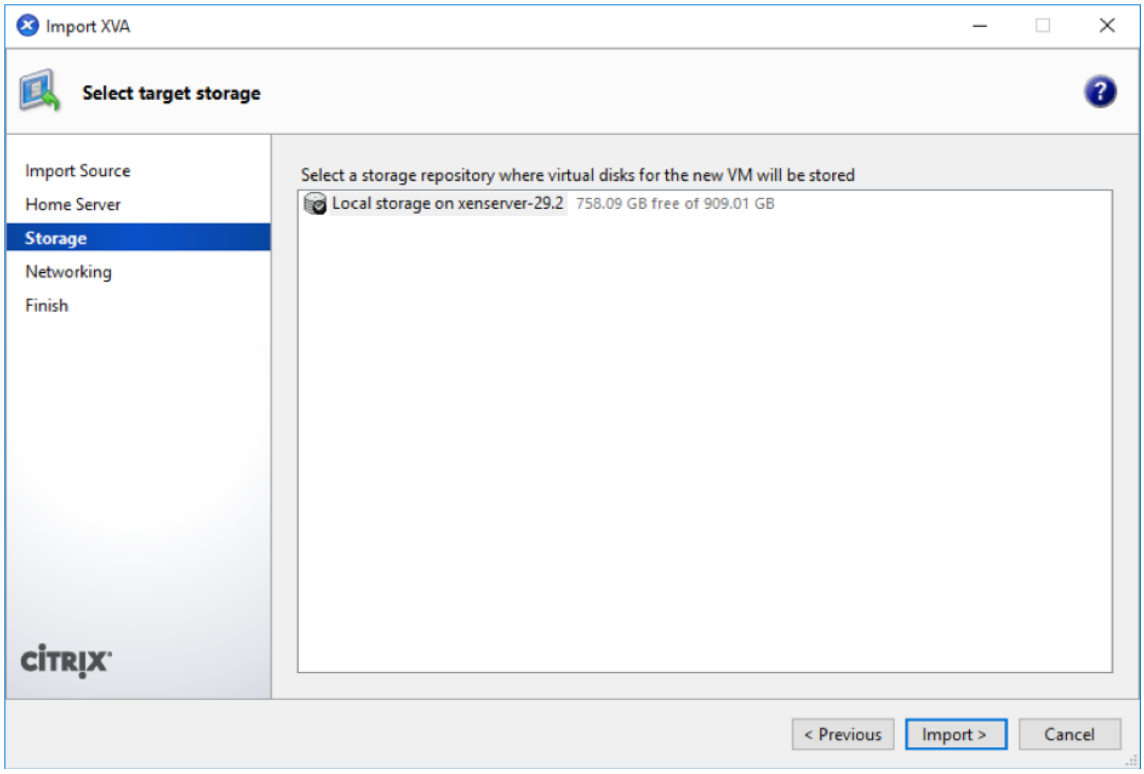


3. 选择先前创建的 XenServer 服务器作为导入虚拟机的位置，然后单击“下一步”。



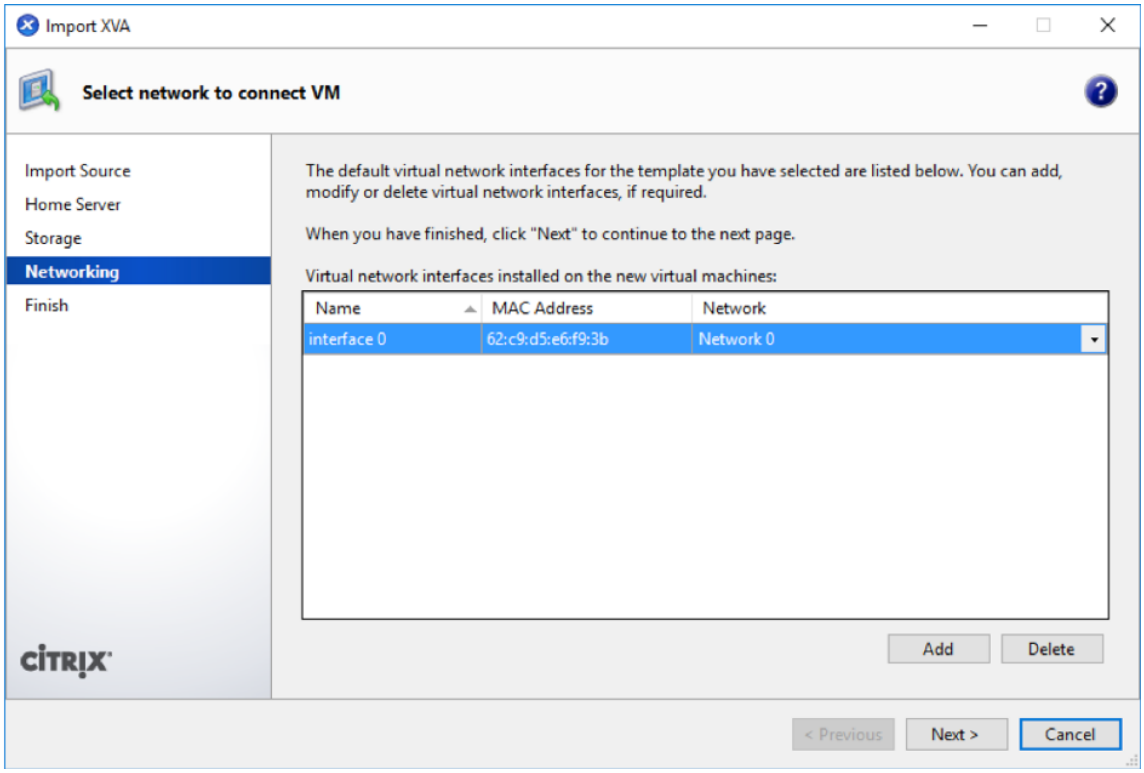
4. 选择存储新虚拟机虚拟磁盘的存储库，然后单击 Import（导入）。

   现在，您可以接受默认存储资源。或者你可以配置数据存储。



导入的适用于本地虚拟机的 Citrix SD-WAN Orchestrator 显示在左窗格中。

5. 选择要连接虚拟机的网络，然后单击“下一步”。



6. 单击完成。

在 **XenServer** 上查看和记录管理 **IP** 地址

管理 IP 地址是适用于本地虚拟机的 Citrix SD-WAN Orchestrator 的 IP 地址，使用此 IP 地址登录本地 Web 用户界面的 Citrix SD-WAN Orchestrator。

> 注意
>
> DHCP 服务器必须存在并且在 SD-WAN 网络中可用。

要显示管理 IP 地址，请执行以下操作：

1. 在 XenCenter 界面的左窗格中，右键单击适用于本地虚拟机的新 Citrix SD-WAN Orchestrator，然后选择启动。
2. 虚拟机启动后，单击“控制台”选项卡。

3. 记下管理 IP 地址。

   > 注意
   >
   > DHCP 服务器必须存在并且在 SD-WAN 网络中可用，否则此步骤将无法完成。

4. 登录到虚拟机。适用于本地虚拟机的新 Citrix SD-WAN Orchestrator 的默认登录凭据如下所示：

   登录：管理员

   Password（密码）：password

   > 注意
   >
   > 首次登录时必须更改默认的管理员用户帐户密码。同时使用 CLI 和 UI 强制执行此更改。

   如果未在 Citrix SD-WAN 网络中配置 DHCP 服务器，则必须手动输入静态 IP 地址。

要将静态 IP 地址配置为管理 IP 地址，请执行以下操作：

1. 虚拟机启动后，单击“控制台”选项卡。
2. 登录到虚拟机。适用于本地虚拟机的新 Citrix SD-WAN Orchestrator 的默认登录凭据如下所示：

   登录：管理员

   Password（密码）：password
3. 在控制台中输入 CLI 命令 `management_ip`。
4. 输入命令 `set interface <ipaddress> <subnetmask> <gateway>`以配置管理 IP。
5. 您确定要更改管理接口 IP 设置吗?

   您可能会断开与设备的连接。<y/n>?

   按“y”更改 IP 并在将近 6-7 分钟后访问配置的管理 IP。

为本地部署 **SD-WAN Orchestrator** 入门

October 21, 2022

以下是适用于本地的 Citrix SD-WAN Orchestrator 入门流程的概述：

- 入职提供商和租户：我们的客户可以使用 Citrix 合作伙伴提供的托管 SD-WAN 服务，该服务由多租户 Citrix SD-WAN Orchestrator 服务启用。
- 入门“自己动手”(DIY) 企业：Citrix SD-WAN Orchestrator 服务也可作为自助管理服务提供给企业。

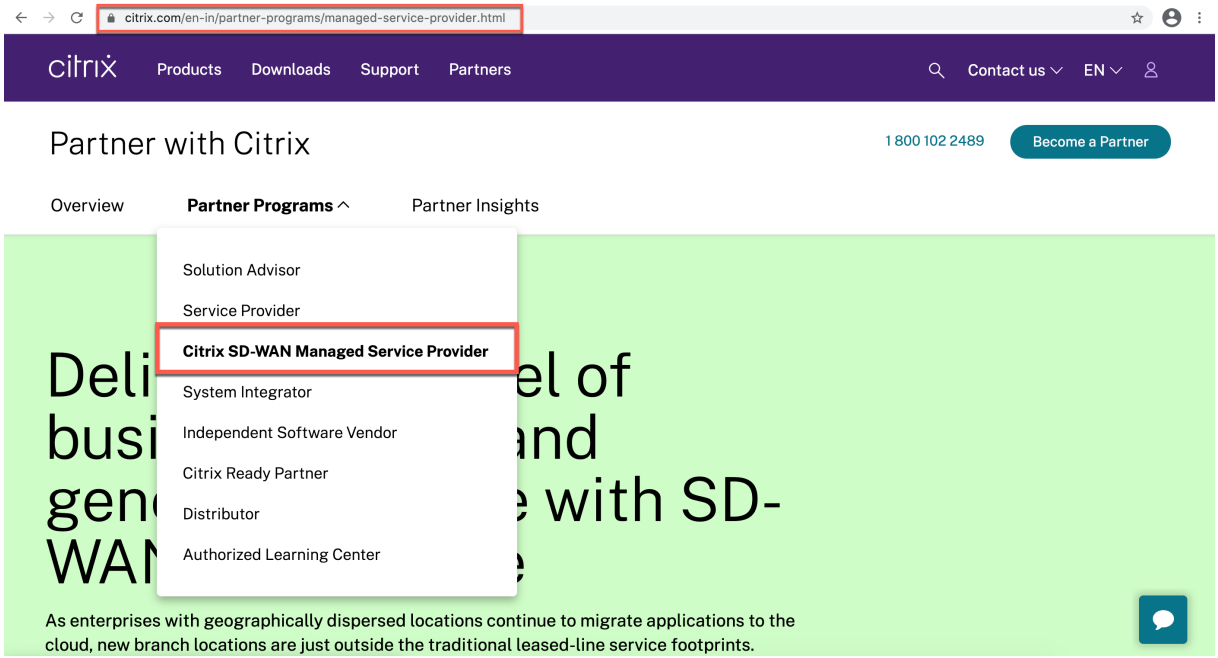
入职提供商和租户

本节介绍了 Citrix 合作伙伴及其租户的入职流程。
以下是入职流程的摘要：

1. 潜在合作伙伴注册成为 Citrix Partner。
2. Citrix Partner 注册为 Citrix SD-WAN 经销商。

合作伙伴注册参加 **Citrix** 合作伙伴计划

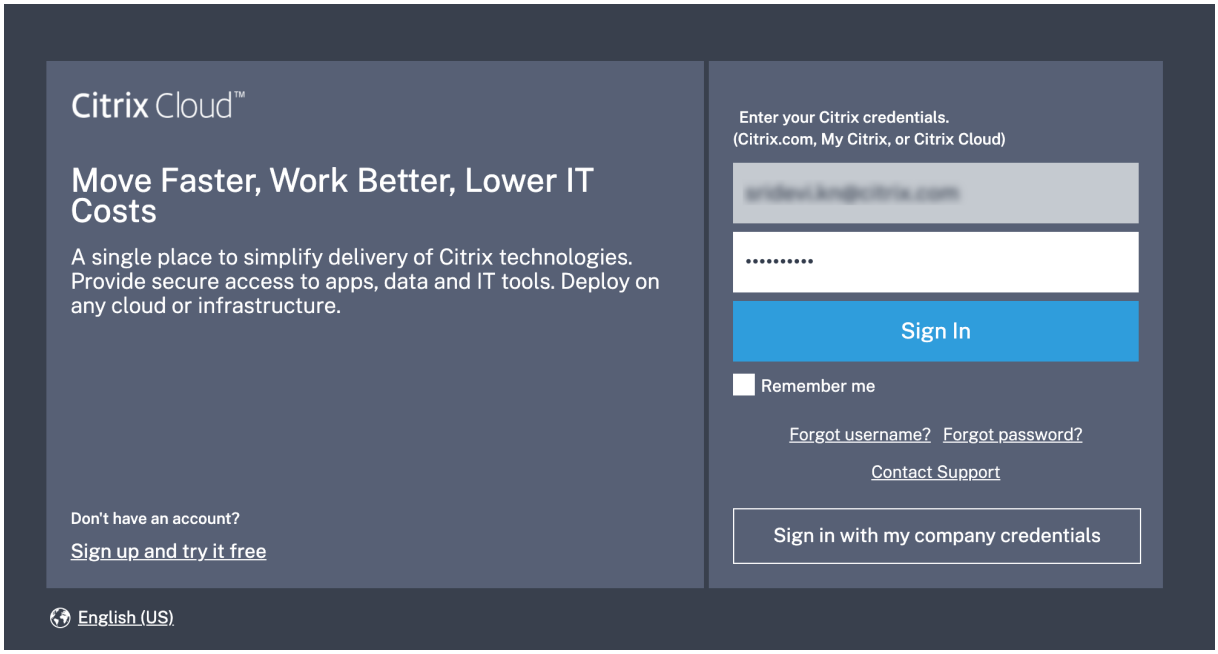
潜在合作伙伴需要注册 Citrix 服务提供商计划 (CSP)- CSP 注册。
合作伙伴还可以注册 Citrix SD-WAN 托管服务提供商计划，该计划是专为 Citrix SD-WAN 合作伙伴精心设计的- SD-WAN MSP 注册。



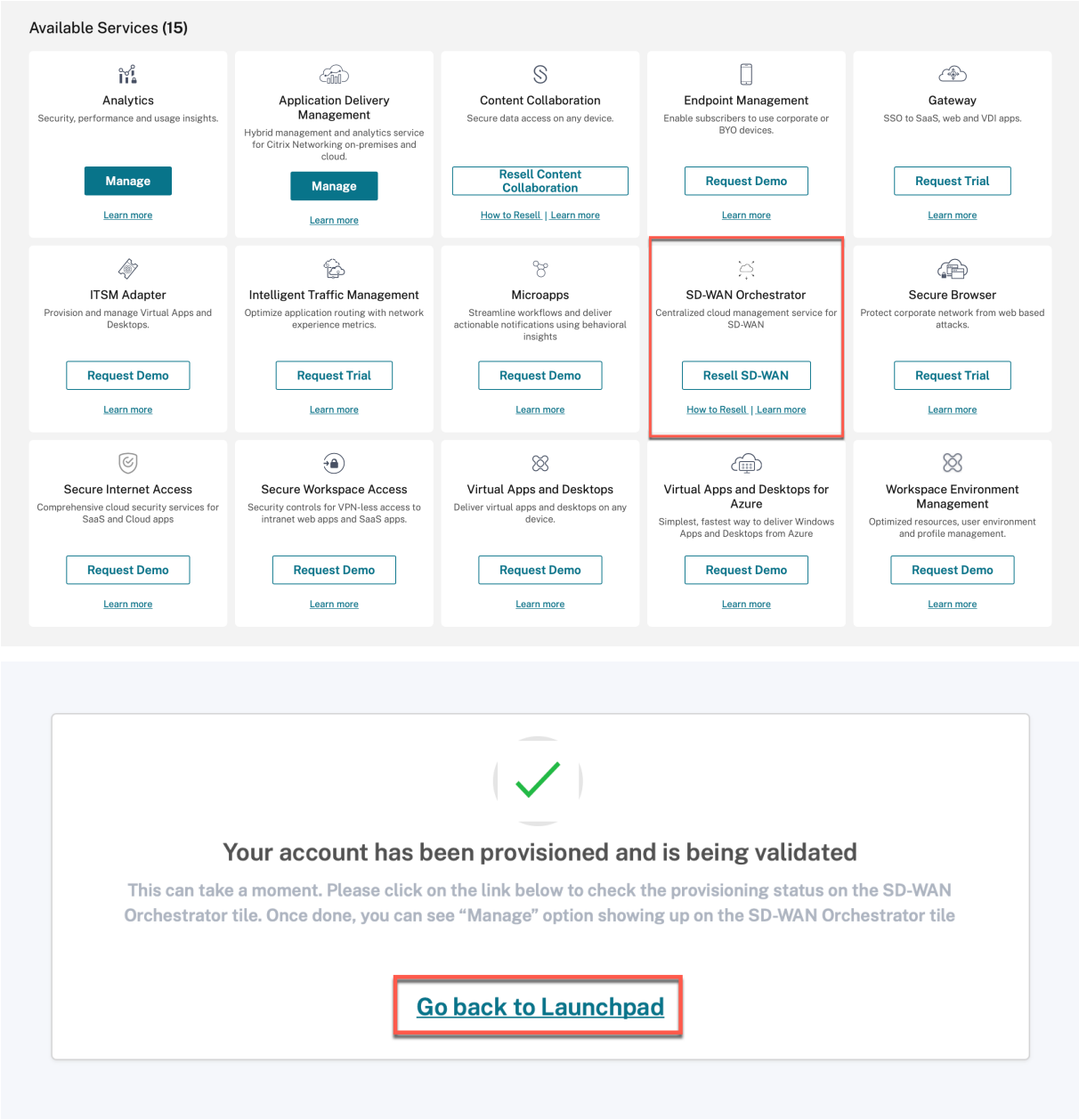
作为注册过程的一部分，将为合作伙伴创建 Citrix Cloud (CC) 帐户。有关更多信息，请参阅 注册 Citrix Cloud。

合作伙伴注册成为 **Citrix SD-WAN** 经销商

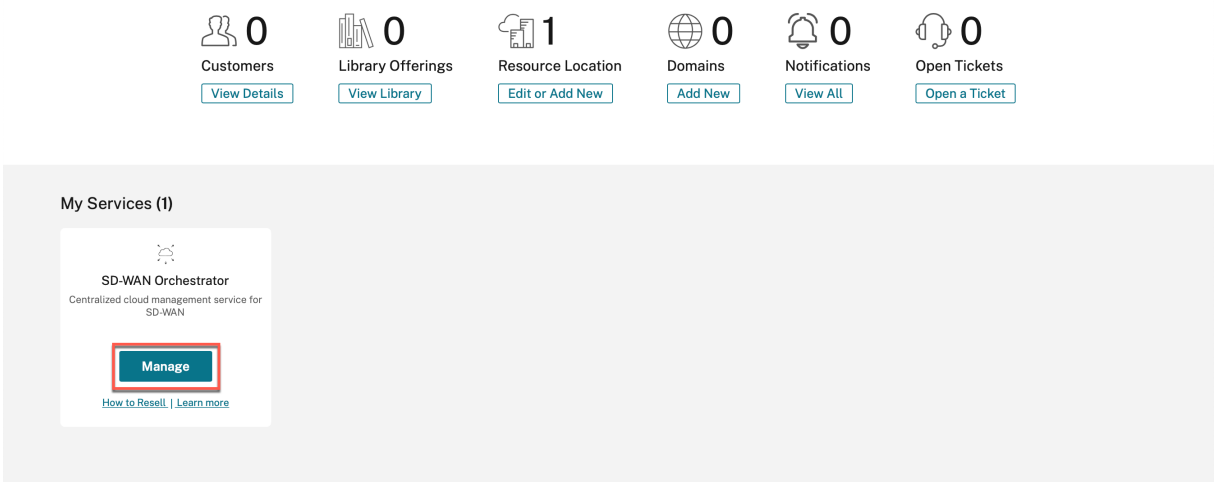
合作伙伴登录 Citrix Cloud 帐户。



Citrix Cloud 上提供的所有可用服务的菜单显示在主页上。**Citrix SD-WAN Orchestrator** 服务 磁贴可以在“可用服务”部分找到。合作伙伴单击图块上的“转售 **SD-WAN** ”，将自己注册为 Citrix SD-WAN 经销商或服务提供商。



Citrix SD-WAN Orchestrator 服务 磁贴现在显示在“我的服务”下方。

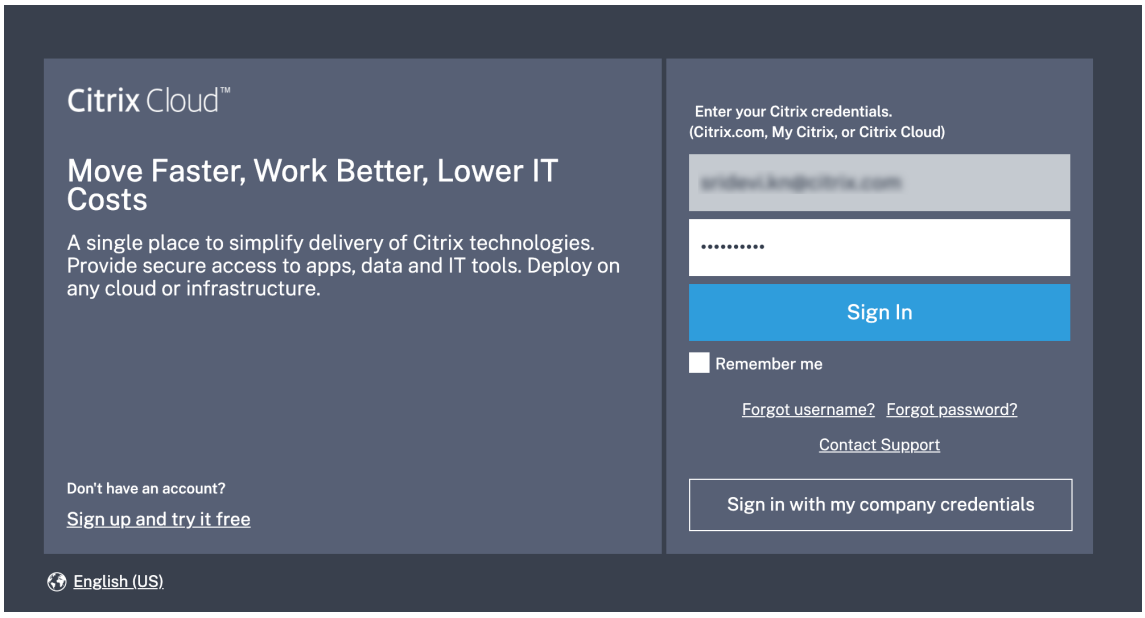


入门 **DIY** 企业客户

本节介绍加入 DIY 企业客户的流程以及邀请管理员管理其 SD-WAN 网络的程序。

入门 **DIY** 客户

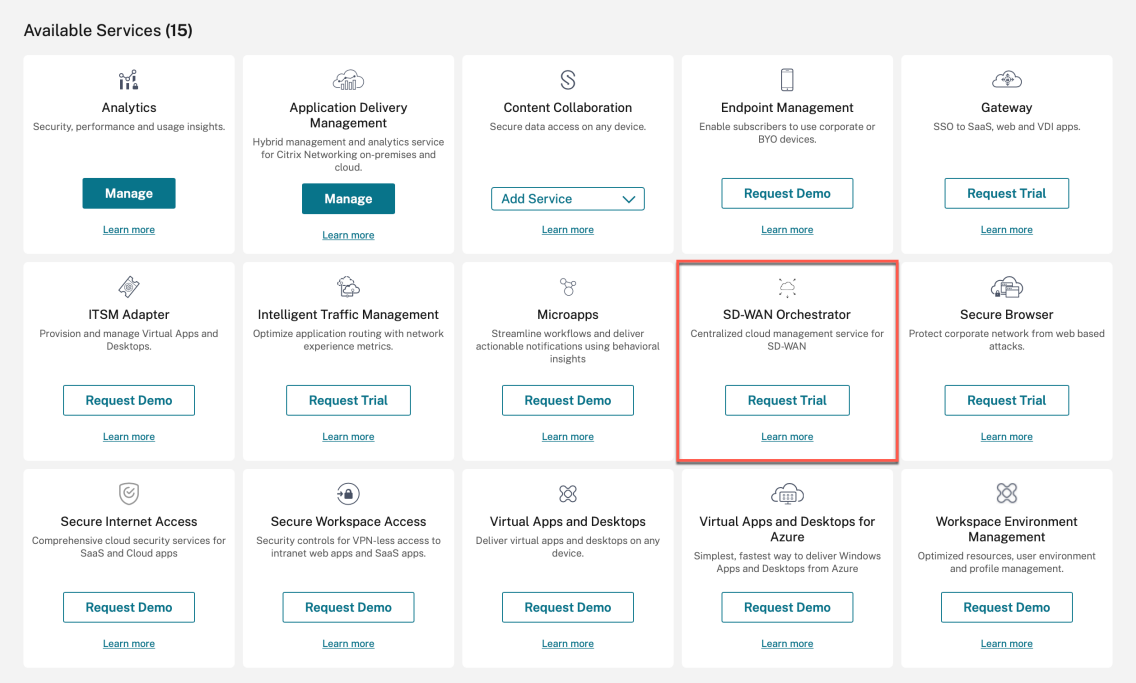
1. 客户登录 Citrix Cloud 帐户。



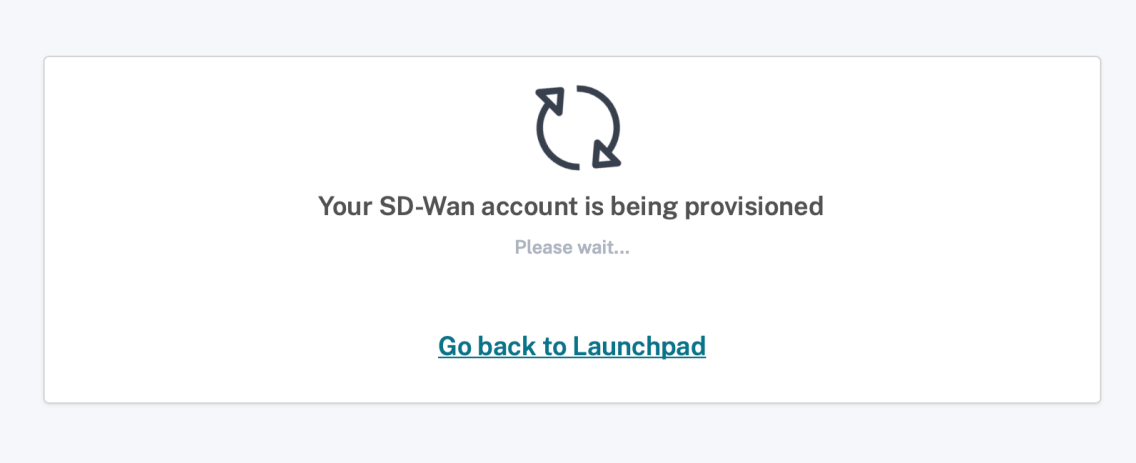
   Citrix Cloud 上提供的所有可用服务的菜单显示在主页上。**Citrix SD-WAN Orchestrator** 服务 磁贴可以在“可用服务”部分找到。

> 注意
>
> 确保您仅使用一个官方帐户注册 Citrix Cloud。使用的公司名称和电子邮件 ID 必须仅与一个 Citrix Cloud 帐户关联。

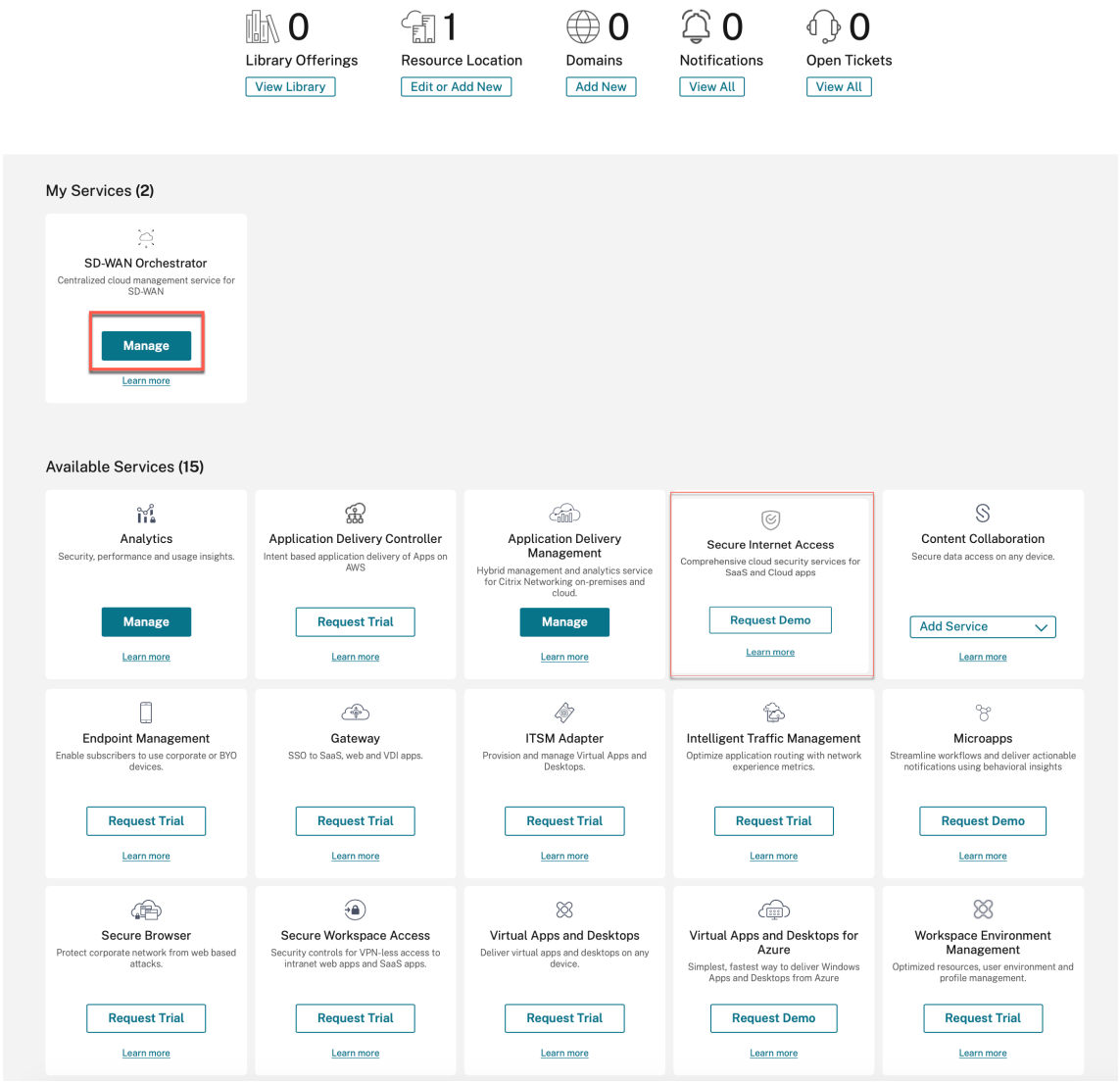
2. 客户单击“申请试用”。



配置了客户的 SD-WAN 账户。



3. **Citrix SD-WAN Orchestrator** 服务 磁贴现在显示在“我的服务”下方。



用于本地登录的 **Citrix SD-WAN Orchestrator**

July 17, 2023

本文介绍客户如何首次登录本地版 Citrix SD-WAN Orchestrator。

以下是登录本地版 Citrix SD-WAN Orchestrator 之前需要具备的先决条件：

- 您必须拥有 CCitrix Cloud 帐户。有关更多信息，请参阅 客户访问 SD-WAN Orchestrator。
- 要在本地使用 Citrix SD-WAN Orchestrator，您必须在 Citrix SD-WAN Orchestrator 服务中拥有一个帐户。有关更多信息，请参阅启用 Citrix SD-WAN Orchestrator 服务。

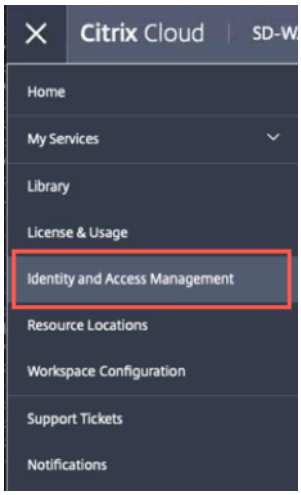
- 创建具有自定义权限的管理员。
- 从 API 访问页面创建客户端，以获取客户 ID、ID 和密钥详细信息。在 Citrix SD-WAN Orchestrator for 本地登录期间需要这些详细信息

> 注意
>
> 如果没有云端登录，则无法继续进行本地登录。

创建管理员

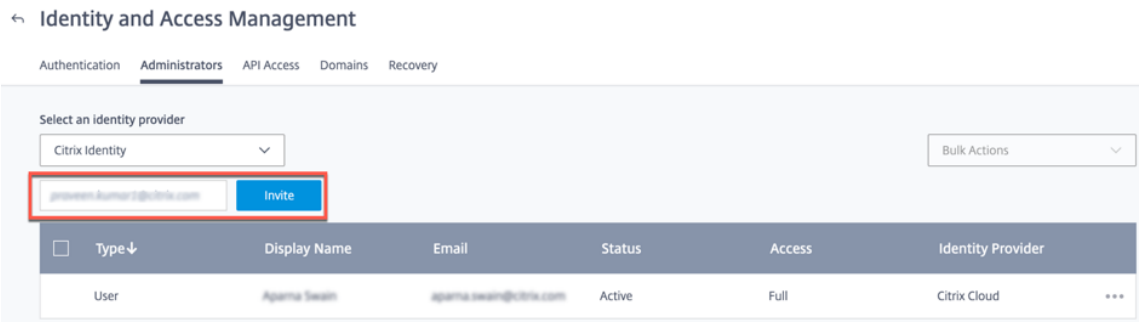
提供商或企业客户可以邀请管理员管理其 SD-WAN 网络。要邀请管理员，请执行以下步骤：

1. 登录 Citrix Cloud 并导航到 身份和访问管理。

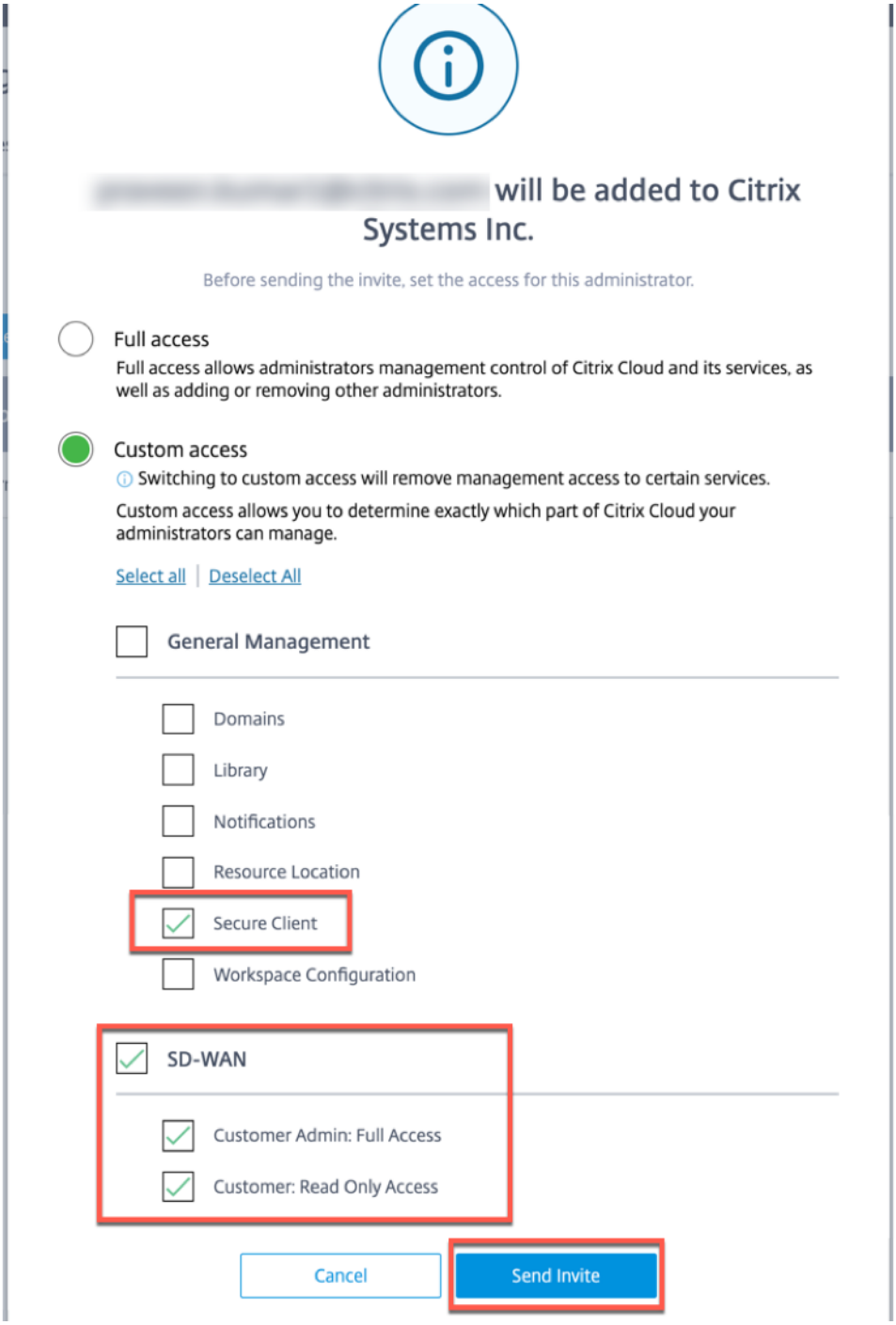


2. 转到 管理员 页面，然后从 身份提供商下拉列表中选择 **Citrix** 身份。

3. 输入新的管理员电子邮件 ID，然后单击“邀请”。



4. 您可以选择“完全访问权限”或“自定义访问权限”。建议为仅管理 SD-WAN 服务的管理员设置自定义访问权限。选择“自定义访问”单选按钮时，还必须从“常规管理”部分和 **SD-WAN** 复选框中选中“安全客户端”复选框。



5. 单击发送邀请。

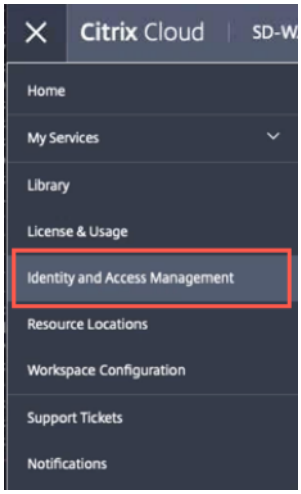
创建管理员帐户后，通过管理员帐户登录以生成 **API** 密钥。

> 注意
>
> 如果您已经拥有自定义管理员角色，则可以使用它来创建 API 令牌。

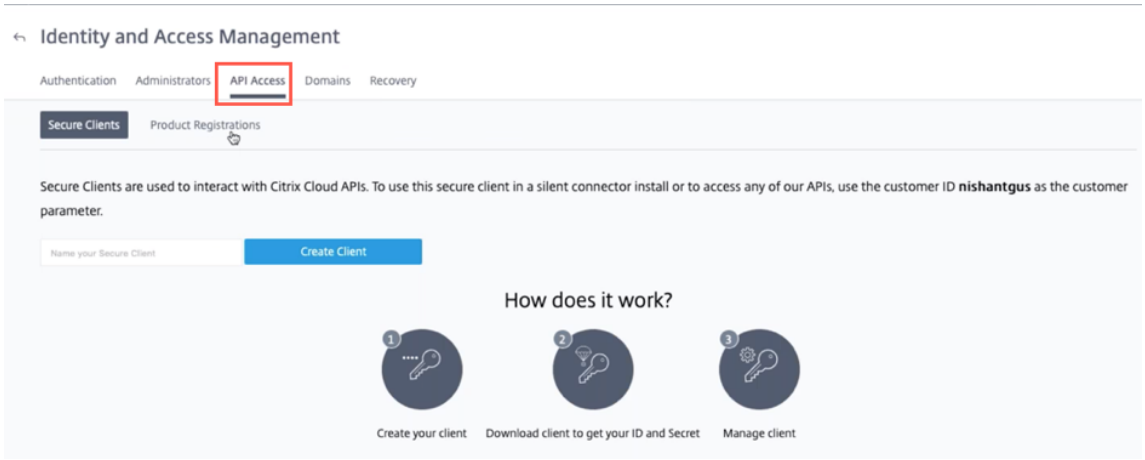
生成 **API** 代币

执行以下步骤登录本地版 Citrix SD-WAN Orchestrator。

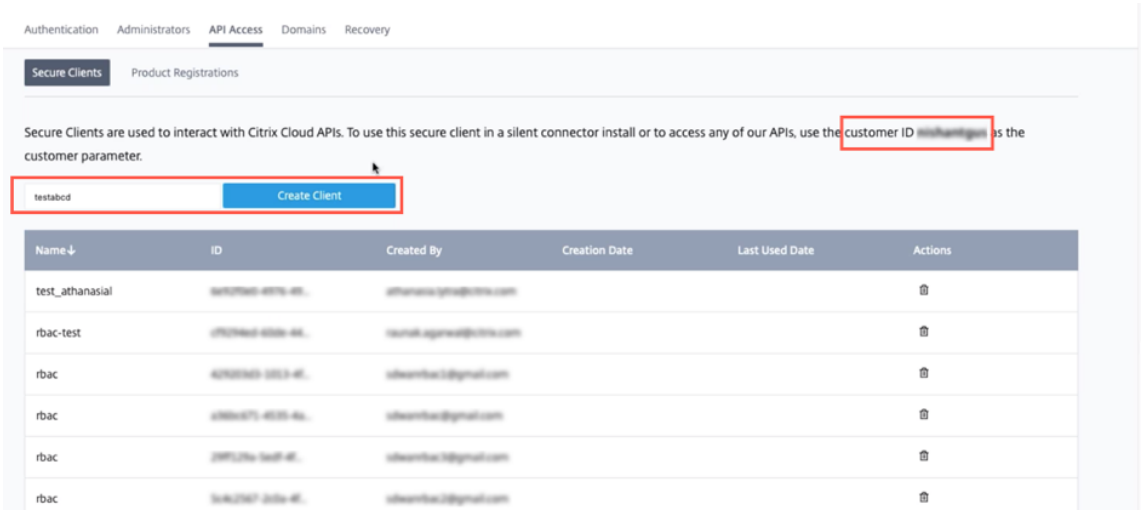
1. 登录 Citrix Cloud 并导航到 身份和访问管理。



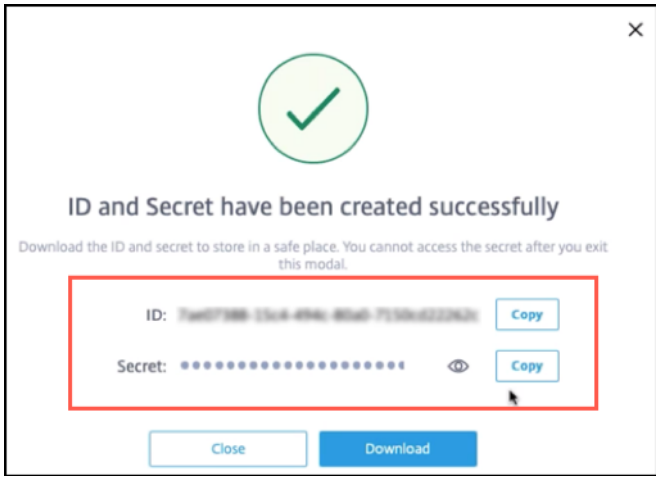
2. 转到 **API** 访问 页面。



3. 创建客户端。记下稍后登录本地版 Citrix SD-WAN Orchestrator 所需的 客户 **ID** 。



4. 单击“创建客户端”后，它会为您提供 **ID** 和 密钥，您可以复制、保存或下载这些密钥。



5. 转到你的 Citrix Hypervisor（XenServer/VMware），然后启动适用于本地的 Citrix SD-WAN Orchestrator
6. 启动本地版 Citrix SD-WAN Orchestrator 后，提供默认用户名（管理员）和密码（密码）。

> 注意
>
> 首次登录时必须更改默认的管理员用户帐户密码。同时使用 CLI 和 UI 强制执行此更改。

7. 如果未在 SD-WAN 网络中配置 DHCP 服务器，则必须手动输入静态 IP 地址。要将静态 IP 地址配置为管理 IP 地址，请执行以下操作：

   - 在控制台中，输入 CLI 命令 `management_ip`。
   - 输入命令 `set interface <ipaddress> <subnetmask> <gateway>`。

> 注意
>
> - 管理 IP 地址是适用于本地虚拟机的 Citrix SD-WAN Orchestrator 的 IP 地址，使用此 IP 地址登录本地 Web 用户界面的 Citrix SD-WAN Orchestrator。

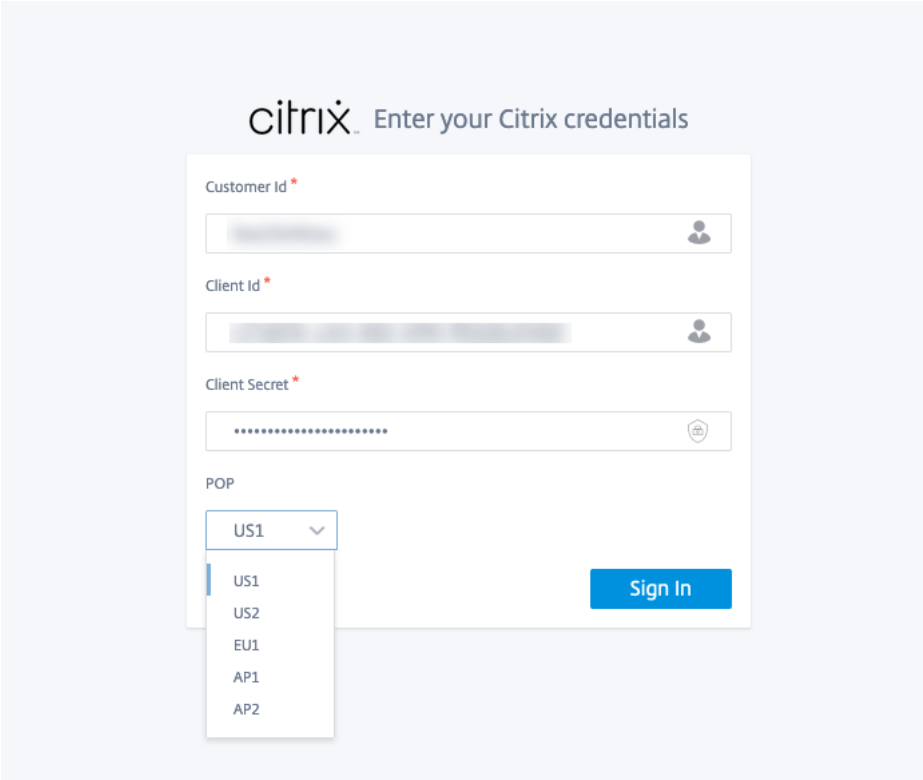
> - 可以通过两种方法（CLI 和 DHCP）配置管理接口。

8. 启动本地版 Citrix SD-WAN Orchestrator 后，默认情况下，它将分别将 DNS 服务器 9.9.9.9 和 149.112.112.112 配置为主服务器和辅助服务器。如有必要，您可以使用以下命令更改 DNS 服务器 IP 地址：

   - 在控制台中，输入 CLI 命令 `set_dns`。
   - 输入命令，`set primary <ipaddress>` 然后输 `y` 入，确认更改。
   - 输入命令 `set secondary <ipaddress>` 并输 `y` 入，确认更改。

```
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
```

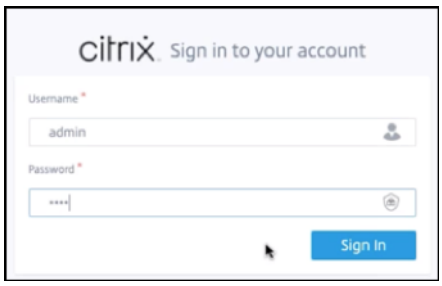
9. 使用管理 IP 打开新浏览器。出现以下屏幕：



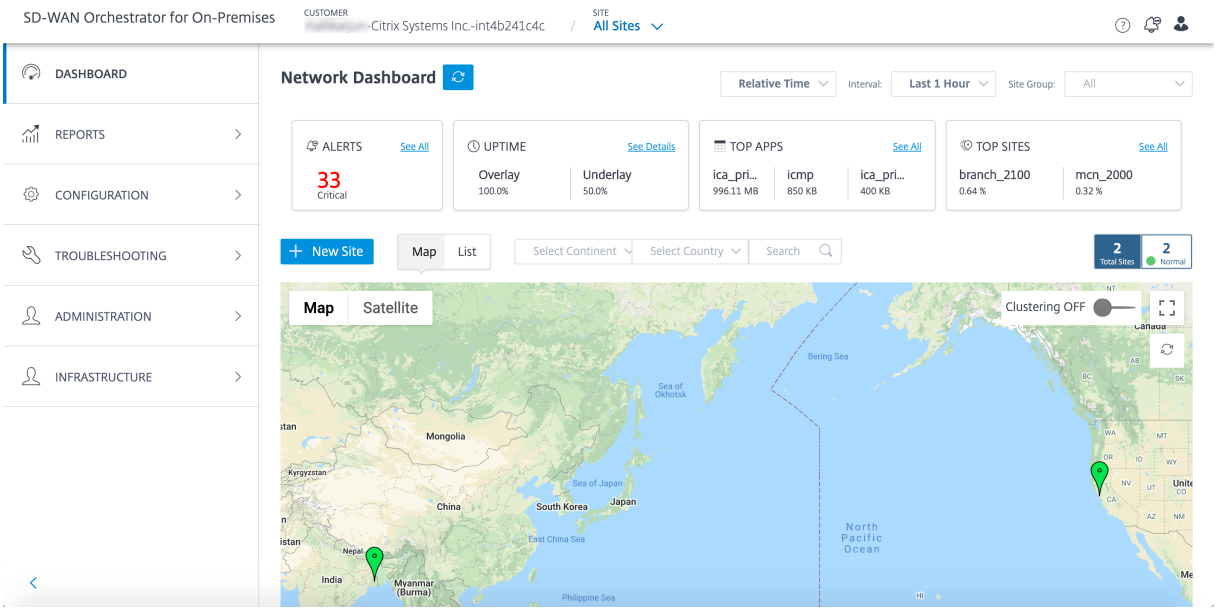
10. 提供您之前在从云 端 **Orchestrator** 创建客户端时保存或下载的客户 **ID**、客户端 **ID** 和客户端密钥。选择您的云账户登录的 POP。成功登录后无法更改 POP。

    > 注意
    >
    > 此屏幕每隔 15 天出现一次。在随后的登录/注销中，您只能看到本地登录页面。

11. 在本地登录页面上提供默认的用户名和密码。



你可以看到 Citrix SD-WAN Orchestrator 本地控制面板页面出现了。



用于本地许可的 **Citrix SD-WAN Orchestrator**

October 21, 2022

适用于本地许可的 Citrix SD-WAN Orchestrator 适用于自己动手 (DIY) 客户—直接企业客户。

作为 Citrix SD-WAN Orchestrator 获得本地许可的先决条件，请确保您已登录 Citrix Cloud。有关更多信息，请参阅用于 本地登录的 Citrix SD-WAN Orchestrator。

用于本地部署的 Citrix SD-WAN Orchestrator 是免费提供的，但客户需要承担管理服务器基础架构和维护的费用。

试用模式

客户的 Citrix SD-WAN Orchestrator 本地账户是在试用模式下配置的。试用模式将继续默认 60 天。

试用期到期后，客户的数据路径将中断。在上传有效许可证之前，无法部署其他更改。当第一个有效许可证托管在客户的 Citrix SD-WAN Orchestrator 上时，该客户的 Citrix Cloud 权限将从试用版更改为生产版。根据上传的许可证的数量和类型，相当数量的站点可以提供正确的带宽权利。一条持续消息：您的试用版已过期。在 **Orchestrator** 上检索至少一项有效的许可证权限，即可升级到生产环境，以恢复网络功能并继续使用。为预付费客户显示。有关更多信息，请参阅 检索和分配预付费计费模式的权限。

预付费账单模式

为本地客户提供了 Citrix SD-WAN Orchestrator 的预付费计费模式。以下三种类型的预付费计费模式可供选择：

- 预付费年度订阅：预付费订阅有 1 年和 3 年的计划。订阅在到期日到期。客户网络中的所有设备都有预付费年度订阅。维护许可证包含在订阅包中，可将设备升级到更新的软件版本。
- 预付费永久版：使用预付费永久许可证，许可证没有时间限制、有效期限或到期。但是，硬件维护许可证作为付费附加组件提供，必须单独购买。客户网络中的所有设备都有预付费永久订阅。

要在 Citrix SD-WAN Orchestrator for Inclouse 中查看计费模型，请在网络级别导航到 管理 > 许可 > 选择计费模式。计费模式显示为“预付年费”和“永久”。

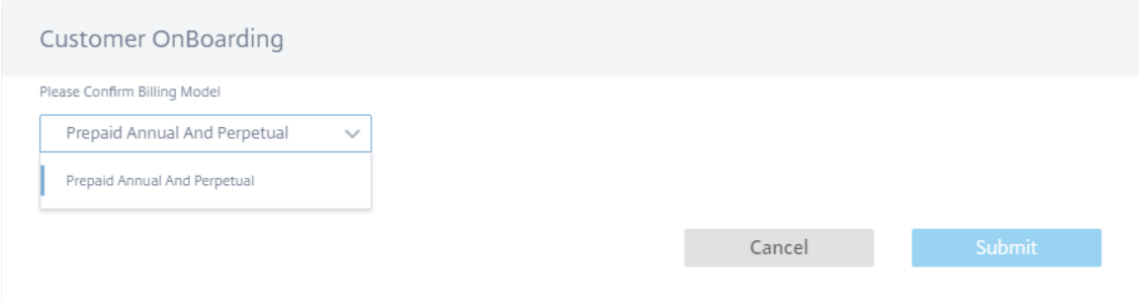
将许可证上传到所有客户站点。有关更多信息，请参阅 检索和分配预付费计费模式的权限。

检索并分配预付费账单模型的权利

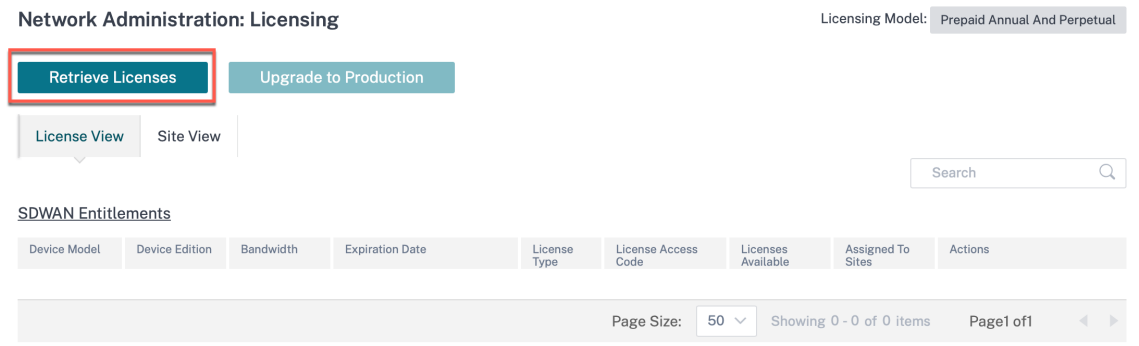
您可以使用 Citrix 通过电子邮件提供的访问代码检索许可证授权。或者，客户还可以在 Citrix Cloud 的 许可证管理 门户中查看访问代码。客户可以在网络中使用 预付永久或 预付年度订阅 计费模式。

先决条件：确保未通过登录许可证 管理门户来分配 Citrix SD-WAN Orchestrator 本地许可证。如果分配了许可证，请先释放/取消分配许可证，然后再使用 Citrix SD-WAN Orchestrator 本地产品中的许可证访问代码。

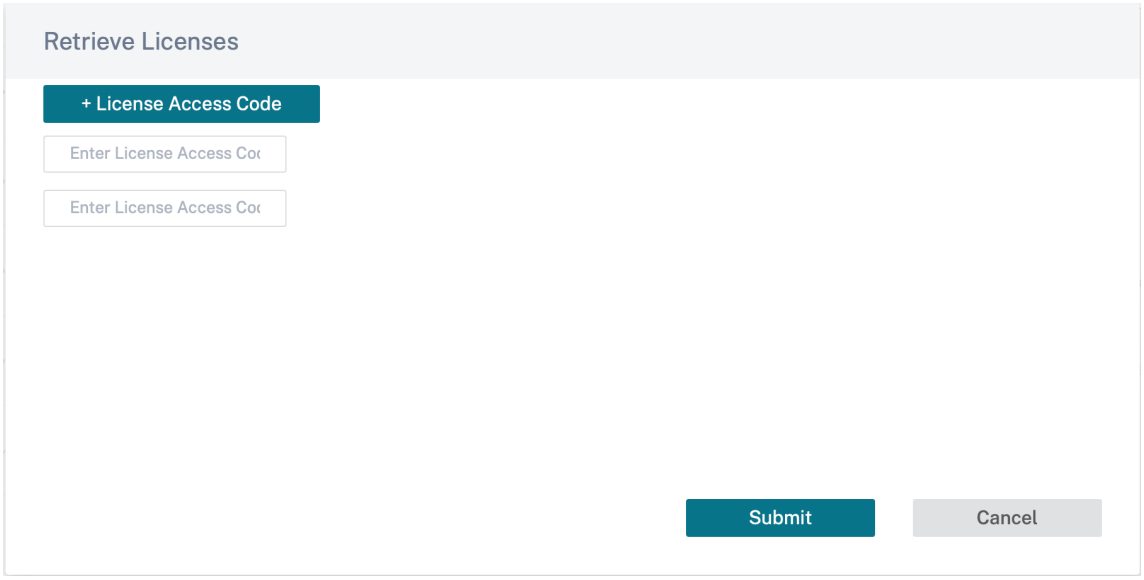
1. 在适用于本地用户界面的 Citrix SD-WAN Orchestrator 中，导航到 管理 > 许可，然后单击 选择计费模式。选择计费模式，然后点击 提交。



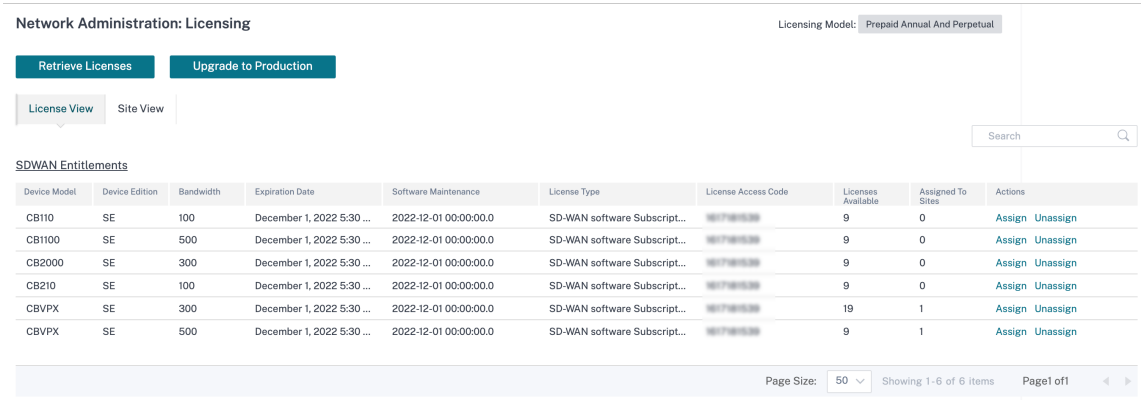
2. 单击“检索许可证”。



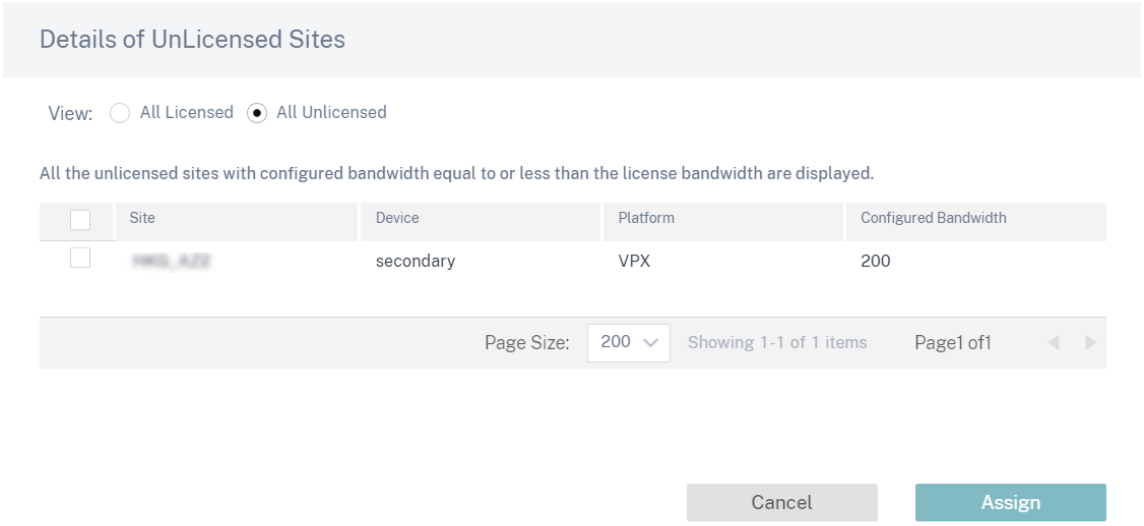
3. 单击 + 许可证访问代码，输入所需数量的访问代码以检索授权，然后单击“提交”。



适用于本地的 Citrix SD-WAN Orchestrator 检索授权并填充许可证表。

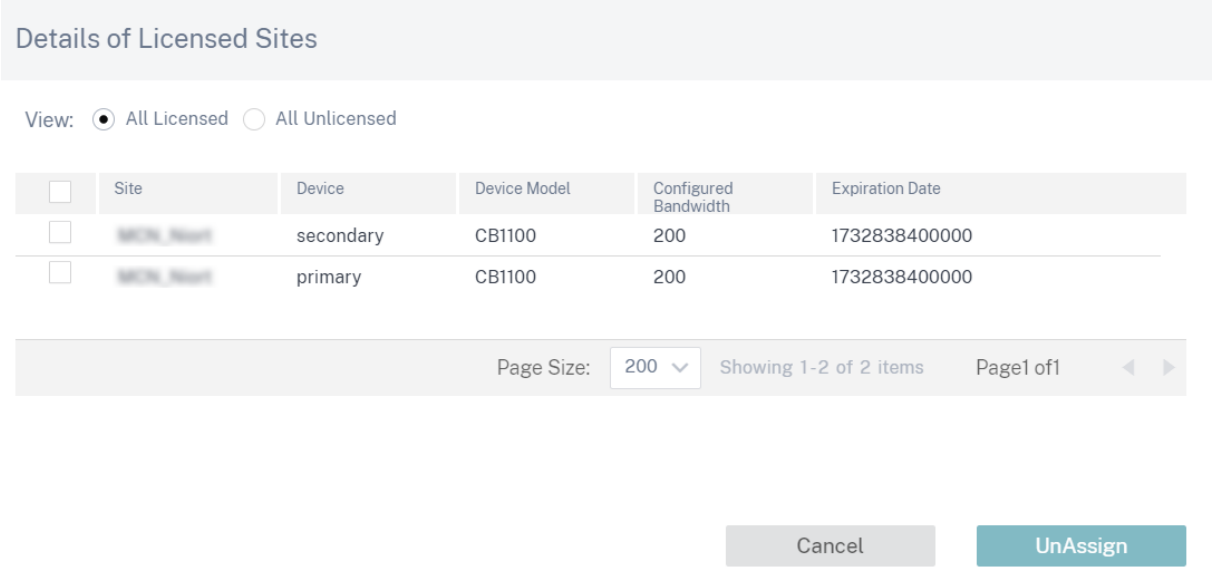


4. 单击“分配/取消分配”，然后选择“全部未许可”。将显示配置带宽等于或小于许可证带宽的所有未许可站点。



5. 选择站点，单击“分配”，然后单击“升级到生产”。

在“所有许可”视图中，将显示已许可站点的列表。您可以选择取消分配许可证并将其释放回池。



在“站点视图”下，会根据配置的带宽和许可证带宽自动将站点与许可证进行匹配，从而使您能够快速分配许可证。

> 注意
>
> 要为设备分配许可证，设备必须具有经过验证的序列号。

许可证过期

许可证到期后，将授予 30 天的宽限期。合作伙伴/客户应在此期间续订其许可证。宽限期到期后，客户的网络数据路径将中断，并且在许可证续订之前无法部署其他更改。

与 **Citrix SD-WAN** 设备的连接

October 21, 2022

在 Citrix SD-WAN Orchestrator 上为本地配置站点后，使用适用于本地的 Citrix SD-WAN Orchestrator 在站点上的 Citrix SD-WAN 设备之间建立连接。您可以通过以下方式之一建立连接：

- 单向身份验证：SD-WAN 设备对本地的 Citrix SD-WAN Orchestrator 进行身份验证。启用单向身份验证后，必须下载 Citrix SD-WAN Orchestrator 本地证书并将其上传到 SD-WAN 设备上。
- 双向身份验证：SD-WAN 使用交换的证书互相进行身份验证。启用双向身份验证后，您必须将 SD-WAN 设备证书上传到本地的 Citrix SD-WAN Orchestrator 上，还必须在 SD-WAN 设备上上传本地的 Citrix SD-WAN Orchestrator 证书。
- 无需身份验证：在本地的 Citrix SD-WAN Orchestrator 和 SD-WAN 设备之间建立连接，无需身份验证。您无需使用 SD-WAN 设备或 Citrix SD-WAN Orchestrator 获取本地证书。如果您拥有安全网络（例如 MPLS），则可以使用无身份验证。

> 注意
>
> 建议仅使用 单向身份验证 或双向身份验证。如果没有身份验证，则必须选择安全的 DNS 服务器。

您可以手动配置与每个站点的连接，也可以使用自动零接触部署。

> 注意
>
> Citrix SD-WAN 11.3.0 是设备连接到本地的 Citrix SD-WAN Orchestrator 所需的最低软件版本。

零接触部署

零接触部署是一个自动流程，用于配置设备与本地的 Citrix SD-WAN Orchestrator 之间的连接。您可以使用非云端零接触部署或云代理零接触部署设置自动建立连接。

非云零接触部署

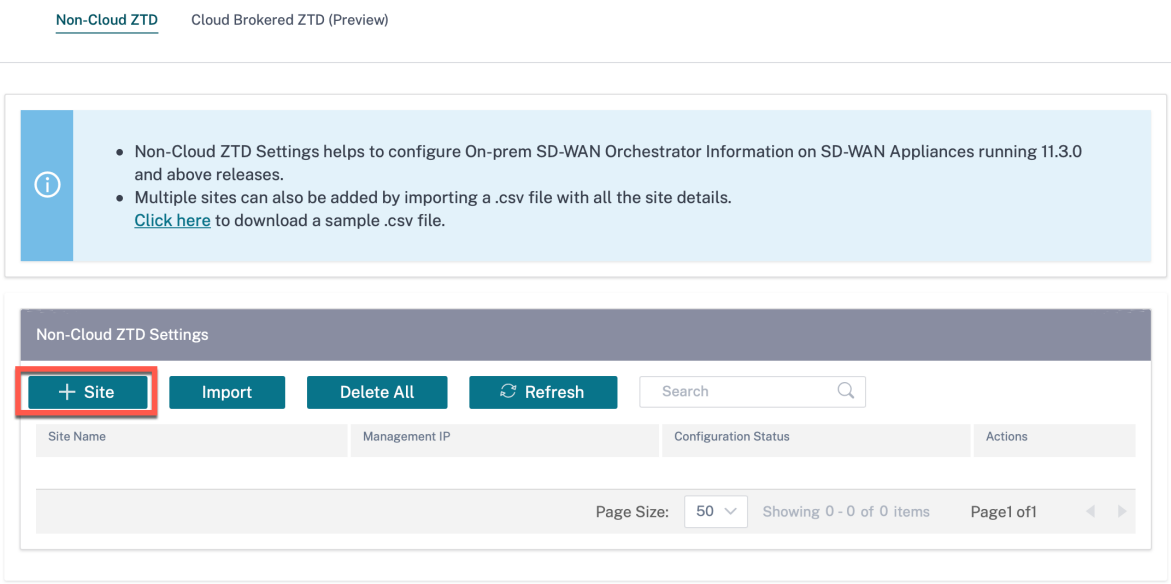
非云零接触部署设置允许您在 SD-WAN 设备上配置 Citrix SD-WAN Orchestrator 以获取本地信息。在后端运行的 NITRO API 处理证书的下载和上传。它从适用于本地的 Citrix SD-WAN Orchestrator 下载证书，登录 SD-WAN 设备，然后上传证书。它还会下载 SD-WAN 设备证书并将其上传到适用于本地的 Citrix SD-WAN Orchestrator 上。

> 注意
>
> 运行 11.3.0 或更高版本的 SD-WAN 设备支持非云零接触部署。

零接触部署仅支持 单向身份验证 和 双向身份验证。不支持任何身份验证。如果在“管理”**>**“证书身份验证”页面上启用了“身份验证类型”，则会建立双向身份验证。如果禁用身份验证类型，则建立单向身份验证。

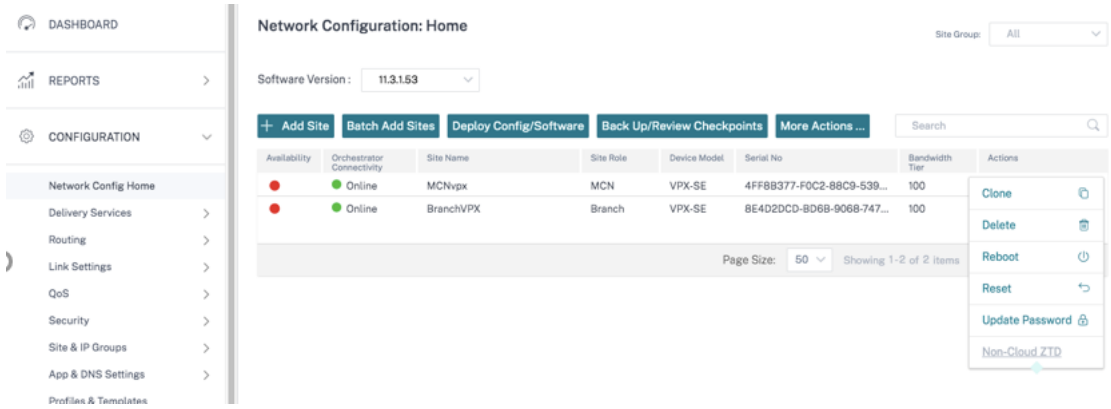
您可以手动添加站点，也可以导入 CSV 文件以同时添加多个站点。

要配置非云零接触部署设置，请导航到 管理 > **ZTD** 设置 > 非云 **ZTD**，然后单击 **+** 站点。



注意

您还可以从 网络配置主 页访问每个站点的非云零接触部署设置。单击该站点的操作图标，然后选择 非云端 **ZTD**。



从“站点名称”下拉列表中选择一个站点，然后输入 Citrix SD-WAN 设备的 管理 **IP** 地址。

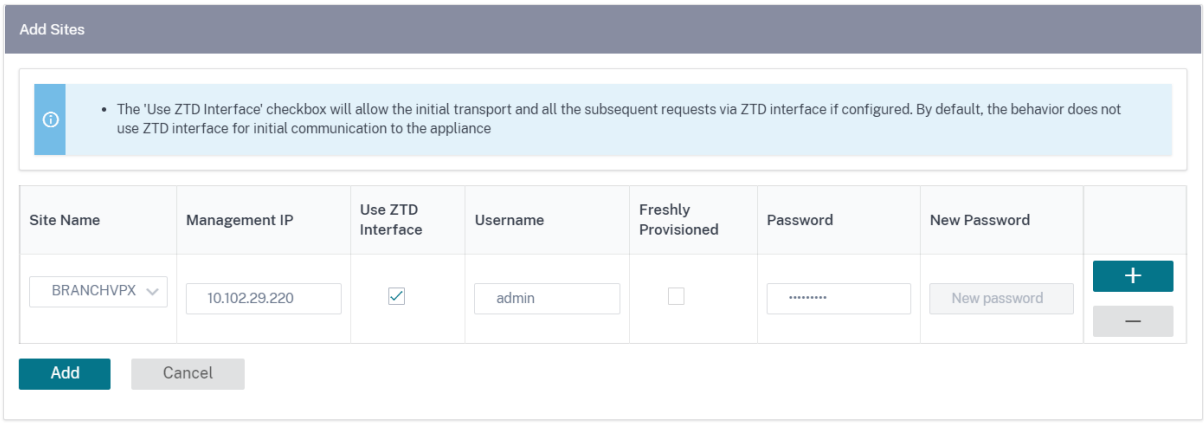
启用“使用 **ZTD** 接口”选项可确保 ZTD 接口用于非云 ZTD，前提是在 SD-WAN Orchestrator 上启用了 ZTD 接口。

注意

- 如果未在内部部署 S **D-WAN Orchestrator** 上启用 **ZTD** 接口，请忽略“使用 ZTD 接口”选项。
- 当 SD-WAN 设备可以访问 **ZTD** 接口 **IP** 地址但无法访问管理 **IP** 地址时，启用“使用 ZTD 接口”选项。
- 启 用 **ZTD** 接口后未选择“使用 ZTD 接口”选项，并不意味着管理接口 IP 地址用于 SD-WAN 设备与 SD-WAN Orchestrator 之间的通信。使用 **ZTD** 接口 选项仅用于使用非云 ZTD 对设备进行初始配置。

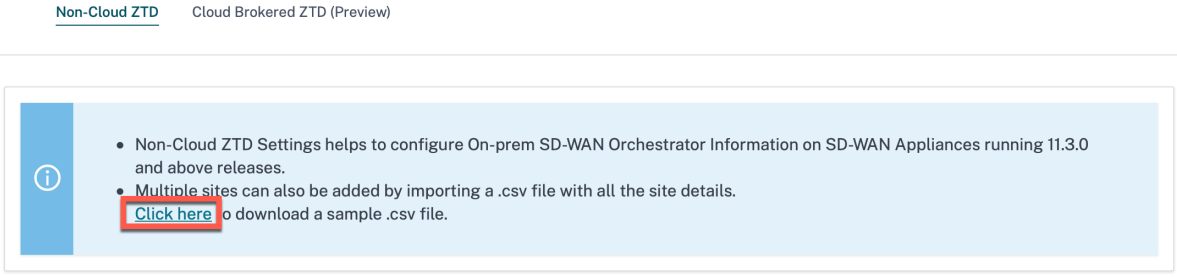
提供设备的用户名和密码。如果您要添加未更改默认密码的新配置站点，请选中“全新配置”复选框。提供 新密码。在此零接触部署过程中，默认密码已更改为新密码。

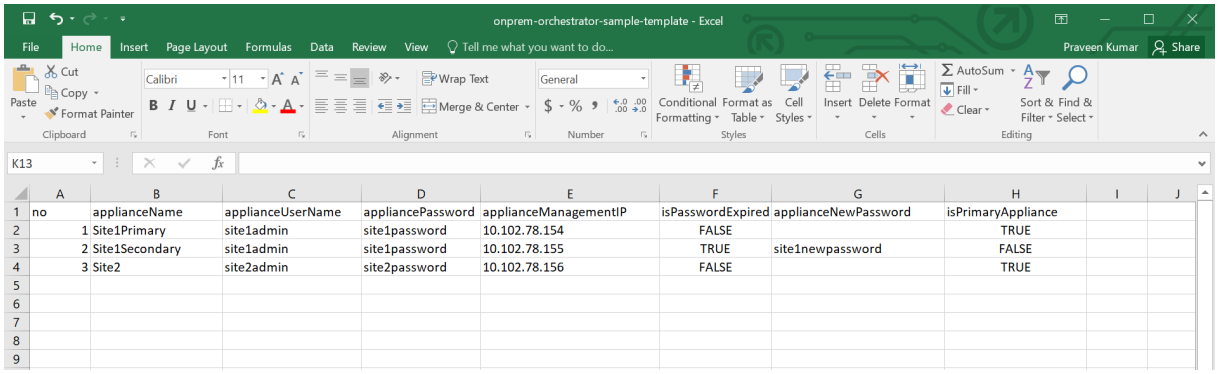
> 注意
>
> 对于新配置的站点，必须在首次登录时更改默认密码。



单击 **+** 继续添加更多站点。

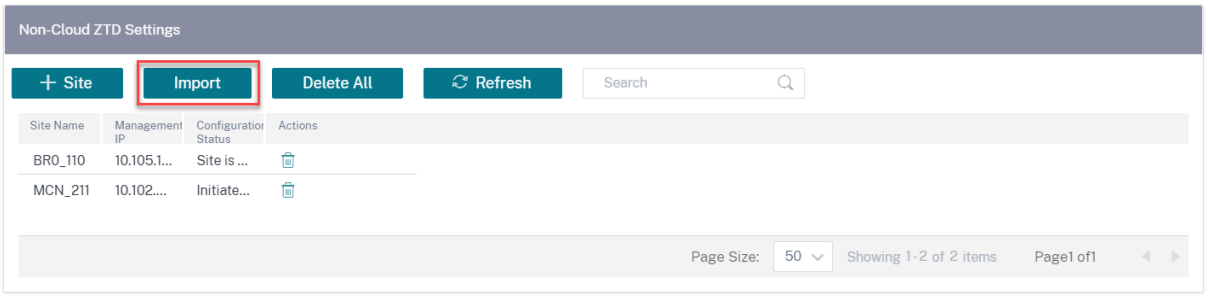
您也可以导入 CSV 文件以同时添加多个站点。用户界面中提供了可下载的示例模板。下载并提供站点详细信息。

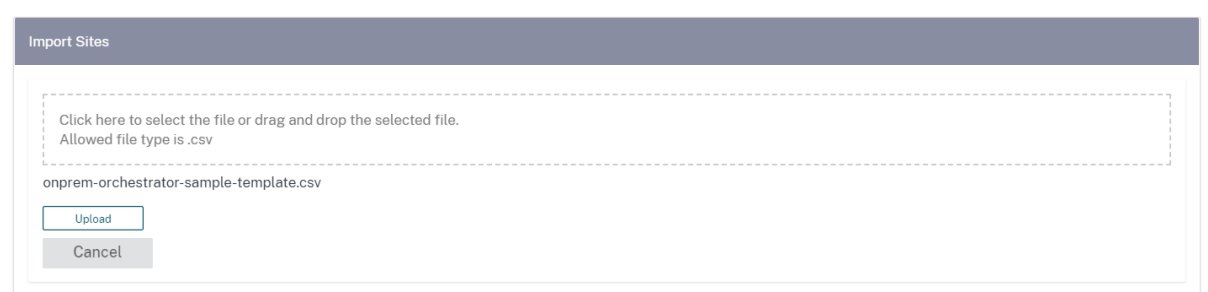




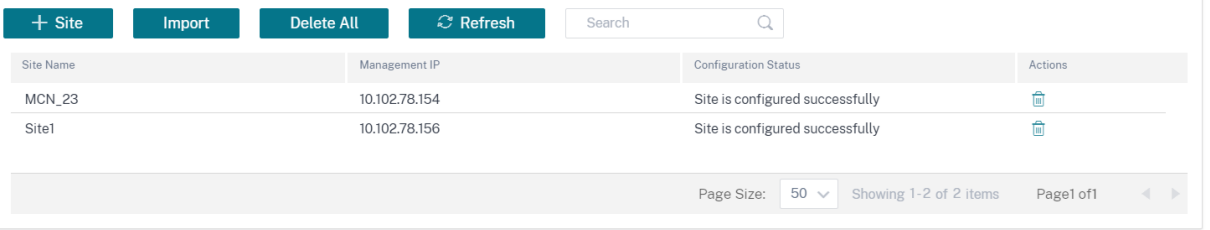
- 设备名称：在站点配置期间配置的站点名称。有关更多信息，请参阅 站点配置。
- 设备用户名：在站点设备上配置的用户名。
- 设备密码：站点设备的相应密码。
- 密码是否已过期：确定设备是否已全新配置。如果值为 **True**，请提供 设备新密码。
- 设备新密码：新配置的设备的密码。如果“密码已过期”值为 **True**，请为 设备提供新密码。
- 是主设备：如果配置了高可用性 (HA)，则活动设备的值必须为 True，备用设备的值必须为 False。如果未配置 HA，则该值必须为 True。

单击“导入”，选择 CSV 文件，然后单击“上传”。





显示站点的配置状态，您可以选择单独删除站点，或者如果不需要站点进行零接触部署，则可以选择全部删除。



云代理零接触部署

云代理零接触部署使用 Citrix SD-WAN Orchestrator 服务作为本地部署的 Citrix SD-WAN Orchestrator 和 Citrix SD-WAN 设备之间的代理。适用于本地的 Citrix SD-WAN Orchestrator 向 Citrix SD-WAN Orchestrator 服务发送云零接触部署配置包。云零接触部署配置包包含以下信息：

- 本地身份信息
- 身份验证类型
- 本地证书
- 设备详情（序列号列表）

Citrix SD-WAN Orchestrator 服务存储从 Citrix SD-WAN Orchestrator 接收的本地信息。当设备使用其序列号联系 Citrix SD-WAN Orchestrator 服务时，Citrix SD-WAN Orchestrator 服务获得的情报决定该设备必须由 Citrix SD-WAN Orchestrator 本地管理。Citrix SD-WAN Orchestrator 服务通过 Citrix SD-WAN Orchestrator 将本地详细信息传递给设备。Citrix SD-WAN 设备将其证书发送到 Orchestrator 服务。Citrix SD-WAN Orchestrator 服务接收并存储设备证书。

适用于本地的 Citrix SD-WAN Orchestrator 定期从 Citrix SD-WAN Orchestrator 服务获取设备证书。在适用于本地的 Citrix SD-WAN Orchestrator 与设备之间建立安全连接后，适用于本地的 Citrix SD-WAN Orchestrator 将配置和相关文件推送到设备。

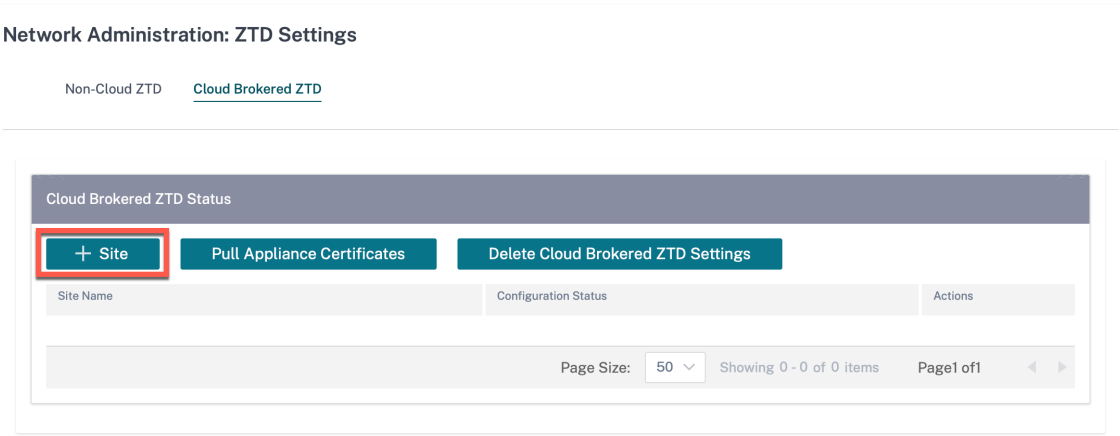
云代理零接触部署设置仅适用于客户托管设置中的客户。提供商托管设置不支持云代理零接触部署设置。

必备条件

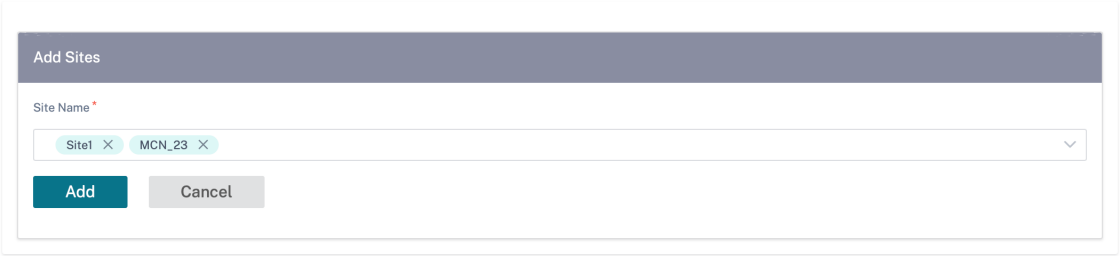
- 设备需要访问以下域名才能与 Citrix SD-WAN Orchestrator 服务建立连接：
  - sdwanzt.citrixnetworkapi.net
  - 下载.citrixnetworkapi.net
  - trust.citrixnetworkapi.net
  - sdwan-home.citrixnetworkapi.net
- 确保适用于本地的 Citrix SD-WAN Orchestrator 始终可以连接到 Citrix SD-WAN Orchestrator 服务以连接到板载 SD-WAN 设备。
- 确保 Citrix SD-WAN 设备在初始启动过程中以及在 SD-WAN 设备上恢复出厂设置时可以连接到 SD-WAN Orchestrator 服务。

要配置云代理零接触部署设置，请执行以下操作：

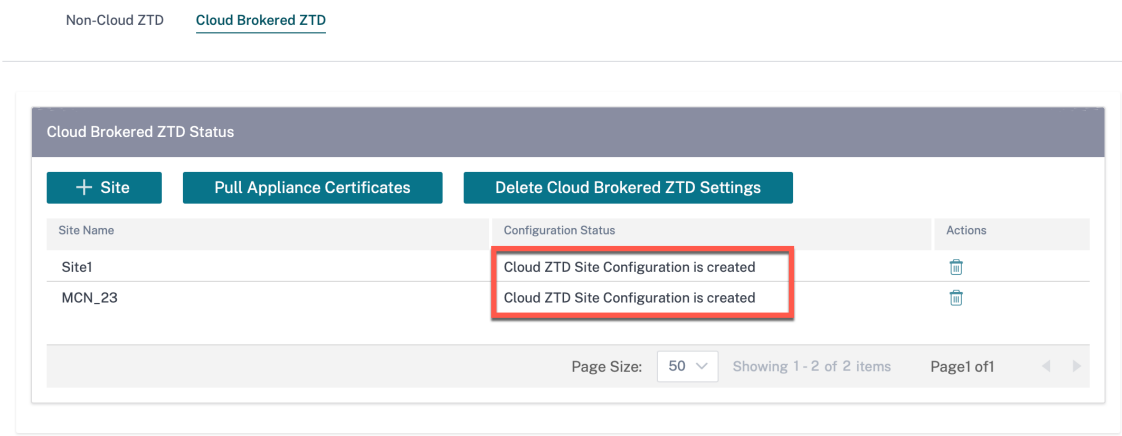
1. 在适用于本地的 Citrix SD-WAN Orchestrator 中，使用引导式工作流程创建和定义站点。有关更多信息，请参阅 站点配置。
2. 使用部署跟踪器验证并编译配置。有关更多信息，请参阅 网络配置 主题中的“部署跟踪器”部分。
3. 导航到 管理 **> ZTD** 设置 **> Cloud Brokered ZTD** ，然后单击 **+** 站点。



4. 从下拉列表中选择一个站点名称，然后单击“添加”。这些站点是根据您的配置列出的。您可以选择单个站点或多个站点。



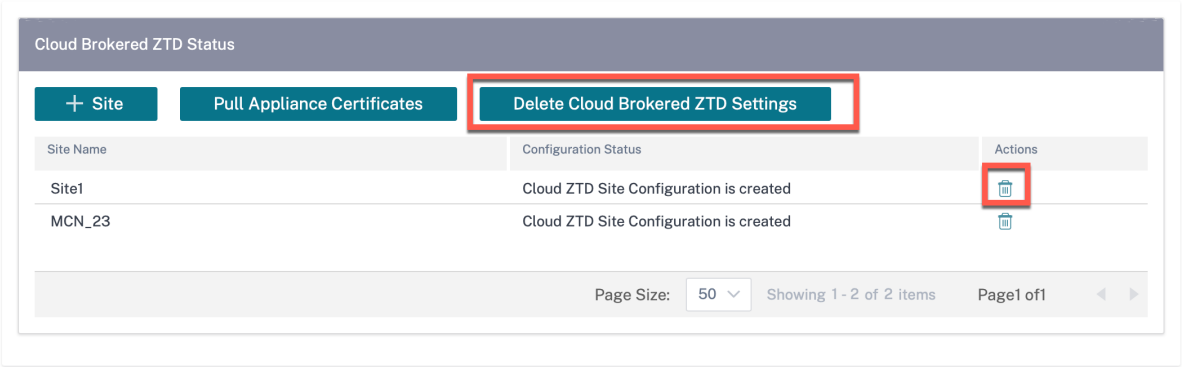
5. 云零接触部署配置已创建并发送到 Citrix SD-WAN Orchestrator 服务。



6. 在数据中心和分支站点接通电缆并打开 SD-WAN 设备的电源。
7. 这些设备使用其序列号联系 Citrix SD-WAN Orchestrator 服务。
8. Citrix SD-WAN Orchestrator 服务充当本地部署的 Citrix SD-WAN Orchestrator 和设备之间的代理。它允许交换证书，Citrix SD-WAN 设备与本地的 Citrix SD-WAN Orchestrator 建立安全连接。零接触部署成功后，配置的站点将联机并显示在 **Orchestrator** 连接 列中的“配置” **>** “网络配置主页”下。
9. 激活 并 暂 存配置，将配置和软件推送到设备。
10. 应用配置/软件后，将建立虚拟路径，并使用相应的虚拟路径状态更新“配置” **>** “网络配置主页”下的“可用性”列。

> 注意：
>
> 适用于本地的 Citrix SD-WAN Orchestrator 大约需要 30 分钟才能获取设备证书并完全加载设备。要立即提取设备证书（无需等待 30 分钟），请单击“提取设备证书”。

如有必要，您可以选择单击“删除 **Cloud Brokered ZTD** 设置”。它会删除与所有站点相关的信息。如果您需要删除特定的站点信息，请单击与该站点对应的删除图标。



限制

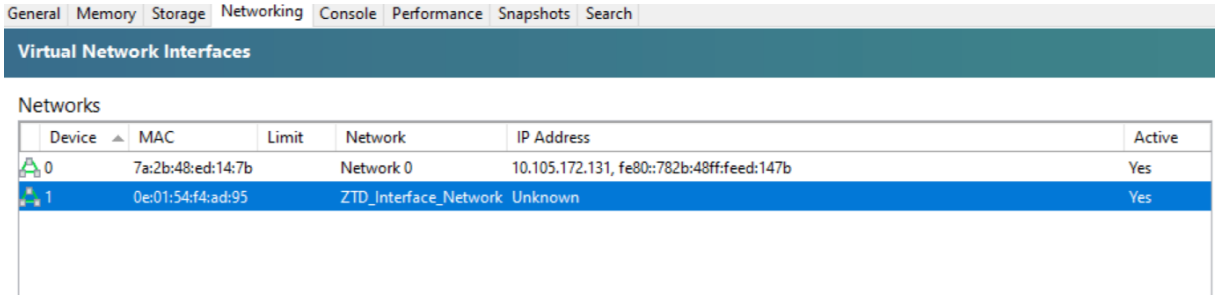
- SD-WAN 设备无法连接到共享云登录凭据的 Citrix SD-WAN Orchestrator for Inclouse 的多个实例。例如，SD-WAN 设备保持与首次配置的本地版 Citrix SD-WAN Orchestrator 的连接。接下来配置的 Citrix SD-WAN Orchestrator 本地详细信息不会推送到 SD-WAN 设备。
- 通过 LTE 连接的 SD-WAN 设备无法与在私有网络上托管的 Citrix SD-WAN Orchestrator 建立连接。

ZTD 接口设置

你可以在本地的 SD-WAN Orchestrator 上启用零接触部署 (ZTD) 接口。通过双向身份验证保护的 ZTD 接口为 SD-WAN 设备 和本地的 SD-WAN Orchestrator 提供了安全的通信接口。

启用 ZTD 接口后，通过非云 ZTD 和 Cloud-Brokered ZTD 部署的新 D-WAN 设备使用 ZTD 接口 IP 地址与本地的 SD-WAN Orchestrator 通信。

作为先决条件，请确保用于本地虚拟机的 SD-WAN Orchestrator 除了管理接口之外还有其他接口。



> 注意
>
> 对于 VMware ESXi 虚拟机，请确保在为 ZTD 添加额外接口后重新启动虚拟机。

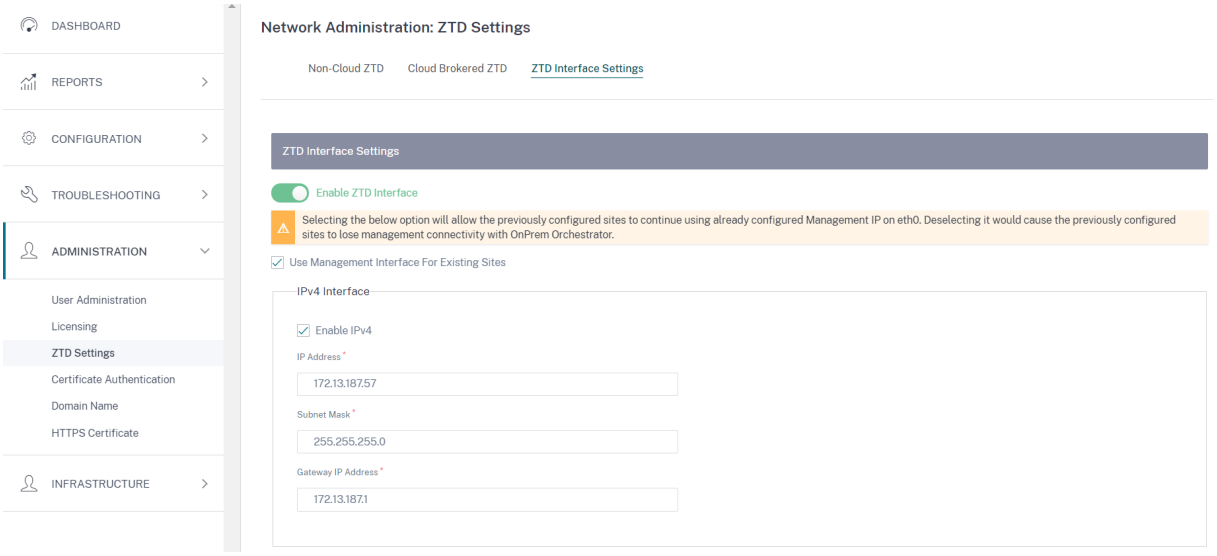
Hardware Configuration	
CPU	8 vCPUs
Memory	16 GB
Hard disk 1	64.97 GB
Network adapter 1	VM Network (Connected)
Network adapter 2	VM Network (Connected)
Video card	4 MB
CD/DVD drive 1	Remote device CD/DVD drive 0
Others	Additional Hardware

启用 **ZTD** 接口

在适用于本地 GUI 的 SD-WAN Orchestrator 中，导航到 管理 > **ZTD** 设置，然后选择 启用 **ZTD** 接口 以启用 ZTD 接口。提供 ZTD 接口 IP 地址、子网掩码和网关 IP 地址。

选择“对现有站点使用管理接口”，以确保已经通过非云 ZTD 或 Cloud Brokered-ZTD 部署的 SD-WAN 设备继续使用管理接口 IP 地址与本地的 SD-WAN Orchestrator 连接。

> 警告
>
> 如果未选择“使用现有站点的管理接口”，则已通过非云 ZTD 或 Cloud Brokered-ZTD 部署的 SD-WAN 设备将断开与本地的 SD-WAN Orchestrator 的连接。



使用 **ZTD** 接口配置非云 **ZTD** 如果选择“使用现有站点的管理接口”选项，则已使用非云 ZTD 部署的设备将继续使用管理接口 IP 地址连接本地的 SD-WAN Orchestrator。在设备上启动非云 ZTD，使用 ZTD 接口 IP 地址与本地的 SD-WAN Orchestrator 建立连接。

> 注意
>
> 在所有 SD-WAN 设备通过 ZTD 接口 IP 地址与本地的 SD-WAN Orchestrator 建立连接后，您可以禁用“使用现有站点的管理接口”选项。

如果未选择“使用现有站点的管理接口”选项，则已使用非云 ZTD 部署的 SD-WAN 设备将丢失与本地的 SD-WAN Orchestrator 的连接。使用 ZTD 接口 IP 地址在 SD-WAN 设备上启动非云 ZTD，以恢复与本地版 SD-WAN Orchestrator 的连接。

使用 **ZTD** 接口配置云代理 **ZTD** 如果选择“使用现有站点的管理接口”选项，则已使用 Cloud Brokered ZTD 部署的设备将继续使用管理接口 IP 地址连接本地的 SD-WAN Orchestrator。要使用 ZTD 接口 IP 地址与本地的 SD-WAN Orchestrator 建立连接，请执行以下操作之一：

- 在 SD-WAN 设备上，更新本地版 SD-WAN Orchestrator 的 IP 地址和证书。

  > 注意
  >
  > 只有在手动重新生成证书时才更新证书，如果设备已经有证书，则无需更新证书。

- 恢复出厂设置并在设备上启动 Cloud Brokered-ZTD，使用 ZTD 接口 IP 地址与本地的 SD-WAN Orchestrator 建立连接。

> 注意
>
> 在所有 SD-WAN 设备通过 ZTD 接口 **IP** 地址与本地的 **SD-WAN Orchestrator** 建立连接后，您可以禁用“使用现有站点的管理 接口”选项。

如果未选择“使用现有站点的管理接口”选项，则已使用 Cloud brokered ZTD 部署的 SD-WAN 设备将丢失与本地的 SD-WAN Orchestrator 的连接。要使用 ZTD 接口 IP 地址恢复与本地版 SD-WAN Orchestrator 的连接，请执行以下操作之一：

- 在 SD-WAN 设备上，更新本地版 SD-WAN Orchestrator 的 IP 地址和证书。
- 恢复出厂设置并在设备上启动 Cloud Brokered-ZTD，使用 ZTD 接口 IP 地址与本地的 SD-WAN Orchestrator 建立连接。

手动连接配置

手动配置连接时，必须下载 Citrix SD-WAN Orchestrator 本地证书，然后将其上传到网络中的每个设备上。它涉及手动登录每个设备以上传证书。

要手动配置连接-

1. 导航到 管理 **>** 证书身份验证 并启用 身份验证类型。

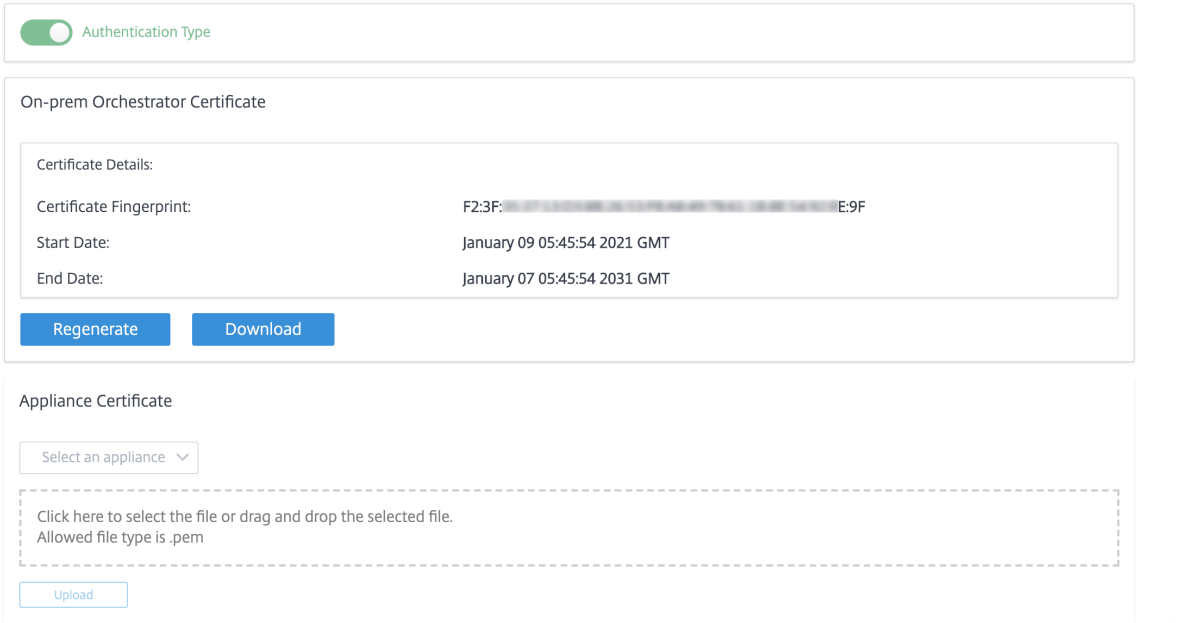
   启用身份验证类型后，SD-WAN 设备只能通过双向身份验证连接到适用于本地的 Citrix SD-WAN Orchestrator。禁用身份验证类型后，SD-WAN 设备可以通过无身份验证、单向身份验证或双向身份验证连接到 Citrix SD-WAN Orchestrator for IndLocial。

   > 注意
   >
   > 在提供商托管设置中，只有提供商才能启用身份验证类型和为本地证书重新生成 Citrix SD-WAN Orchestrator。

2. 单击“重新生成 并 下载 Citrix SD-WAN Orchestrator 本地证书”。
3. 从“设备 证书”部分选择一个设备，然后上传从 SD-WAN 设备下载的相应证书。有关下载设备证书的详细信息，请参阅 SD-WAN 设备上的 Citrix SD-WAN Orchestrator 本地配置。

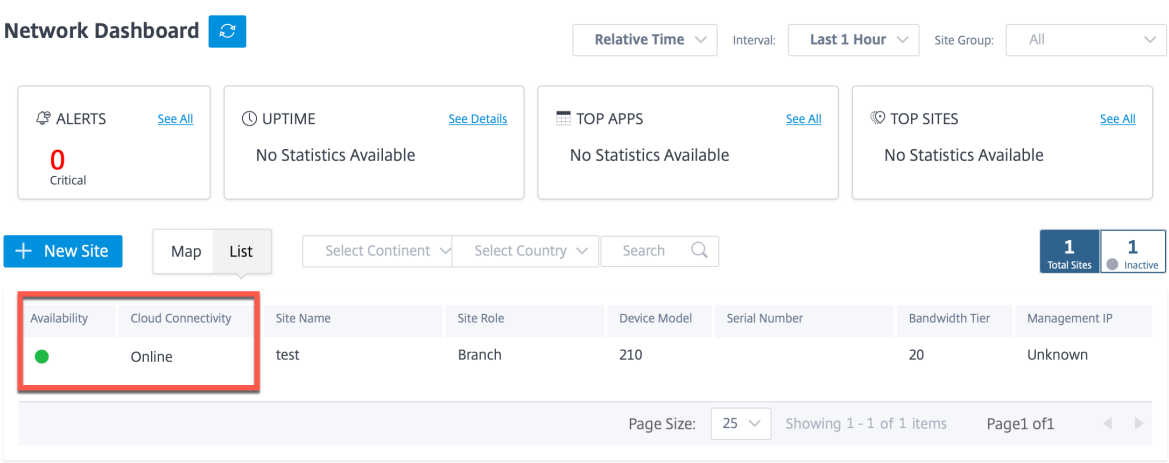
   > 注意
   >
   > - 仅支持.pem 文件类型。
   > - 只有客户管理员才能上传设备证书。

4. 登录 SD-WAN 设备用户界面，导航到 配置 **>** 虚拟广域网 **>** 本地 **SD-WAN Orchestrator**。上传从 Citrix SD-WAN Orchestrator 下载的本地证书。有关详细信息，请参阅 Citrix SD-WAN Orchestrator 在 SD-WAN 设备上进行本地配置。



验证连接

要验证设备的连接状态，请导航到 配置 **>** 网络配置主页，然后检查与您的站点对应的 **Cloud Con** nectivity 列。

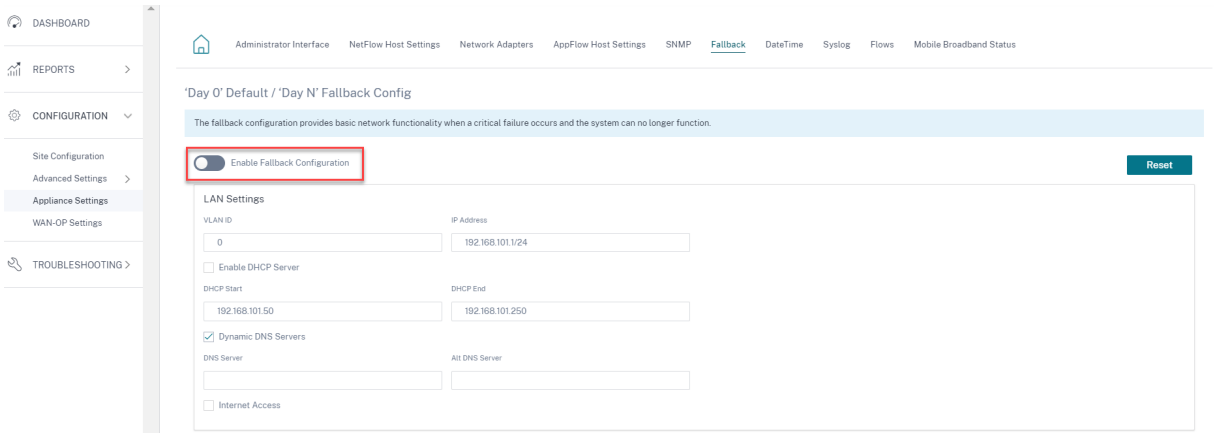


> 注意
>
> 您可以在 基础架构 > **Orchestrator** 管理 > 软件映像 > 设备下发布所需的软件以升级设备。有关更多信息，请参阅 发布软件。

回退配置

备用配置可确保通过设备的带内管理 IP 保留您与 Citrix SD-WAN 设备建立的用于本地连接的 Citrix SD-WAN Orchestrator。

要在站点级别的 Citrix SD-WAN Orchestrator 上启用备用配置，您可以导航到 配置 > 设备设置 > 回退 并单击“启用回退配置”。

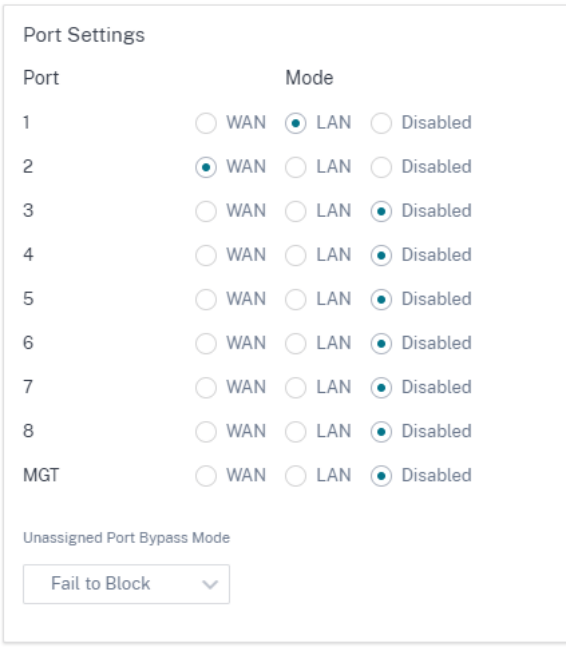


有关备用配置的详细信息，请参阅 带内管理。

> 注意
>
> 如果您使用的是 Citrix SD-WAN 110 SE 以外的设备，请确保运行的是 SD-WAN 11.2 或更高版本以启用默认回退配置。

下表提供了在不同平台上用于备用配置的预先指定 WAN 和 LAN 端口的详细信息：

平台	WAN 端口	LAN 端口
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)



提供程序级别配置

December 7, 2020

配置文件

配置文件是 实时配置模板。常规模板旨在帮助创建新实体。但是，创建模板后，模板中的后续更改不适用于使用基础模板创建的新实体。配置文件用作实时中央主实体，所有子实体都从该实体继承，而不是在配置文件的整个生命周期内。与该配置文件关联的所有子实体会自动继承在配置文件中所做的任何更改。

例如，管理员创建一个名为小型零售商店 的站点配置配置文件，并将其应用于公司拥有的所有小型零售店。现在，在任何给定时间对小型零售店简介所做的任何更改都将自动应用到继承此配置文件的所有商店。配置文件配置中的某些参数可以保留为未设置，具体取决于所有实体的通用情况以及不应使用哪些功能。此类参数可自定义，在继承同一个配置文件的各个实体之间可能会有所差别。

服务提供商的配置文件模板

合作伙伴可以创建个人资料模板，客户可以在创建个人资料时使用

例如，提供程序可以创建四个站点配置文件模板，即小型分支、中型分支、大型分支和数据中心。这些模板将自动提供给与合作伙伴关联的客户帐户。客户在创建配置文件时可以使用这些模板。

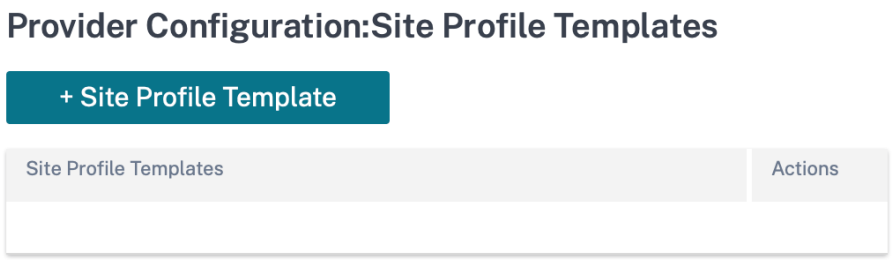
例如，假设一个客户决定为小型分支配置创建一个配置文件。客户可以选择合作伙伴共享的模板之一，该模板可通过下拉列表提供，作为配置文件配置的一部分。客户可以在保存配置文件之前根据其网络需求对其进行定制。配置文件模板不是活动实体。这只是帮助在客户级别创建配置文件。可以在客户级别创建配置文件，并且这些配置文件应用作主配置记录的活动实体。

提供程序可以创建配置文件，可以根据需要与部分或所有客户共享这些配置文件。当前支持站点和 WAN 配置文件。

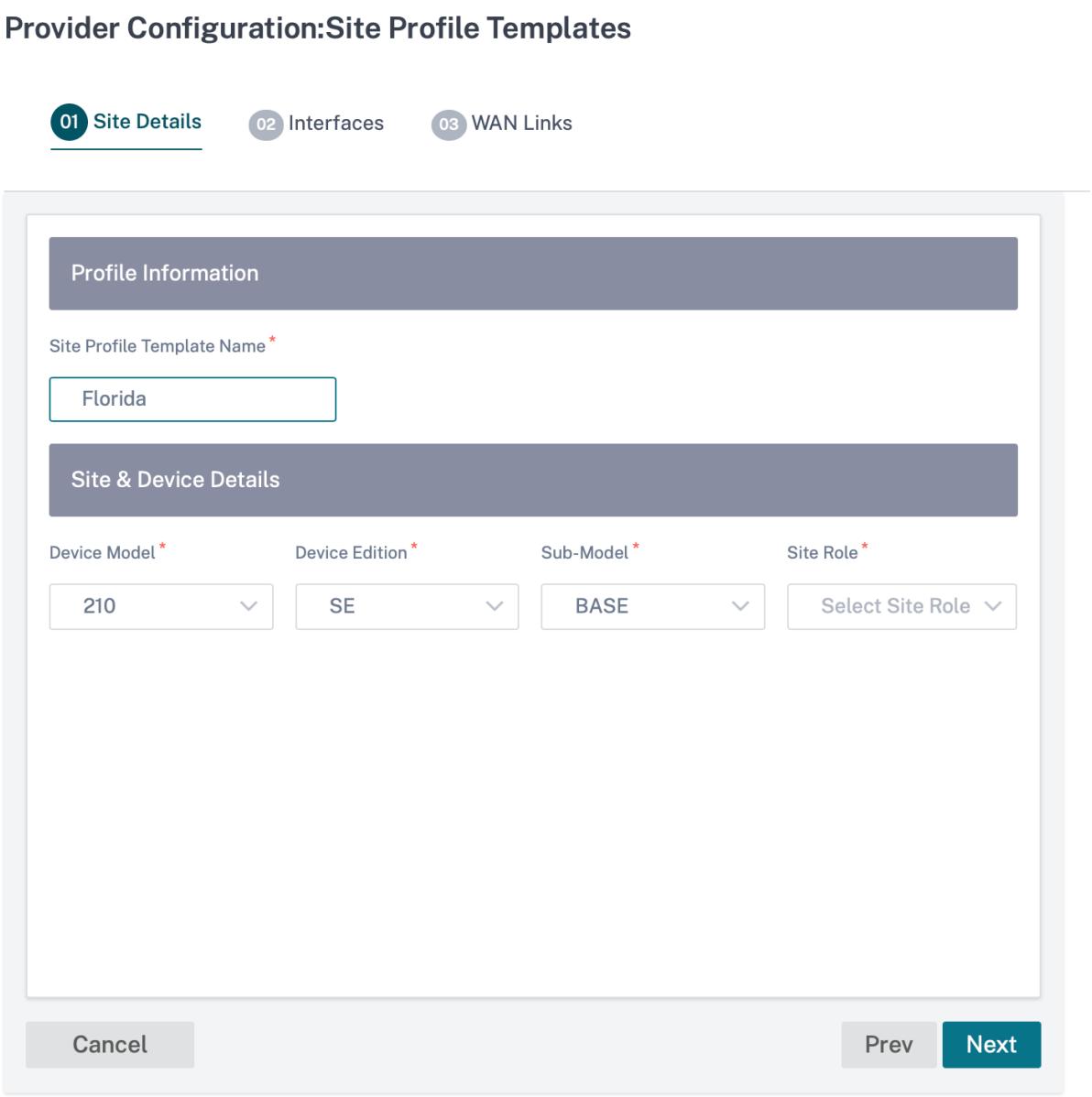
站点配置文件模板

站点配置文件模板是由服务提供商创建的站点配置模板，用于在客户级别创建站点配置文件。

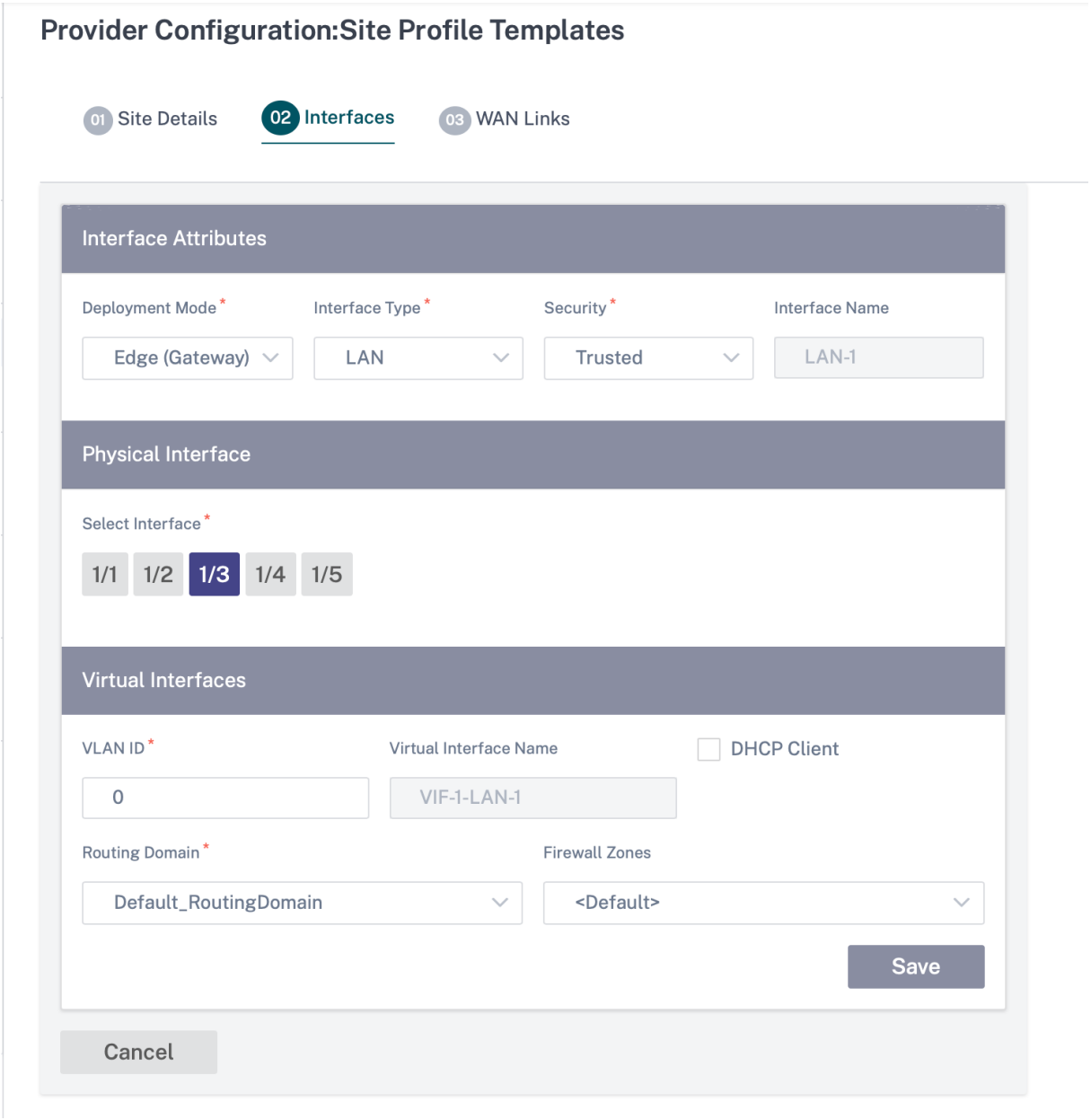
要创建配置文件模板，请导航到 配置 > 站点配置文件模板，然后单击 **+** 站点配置文



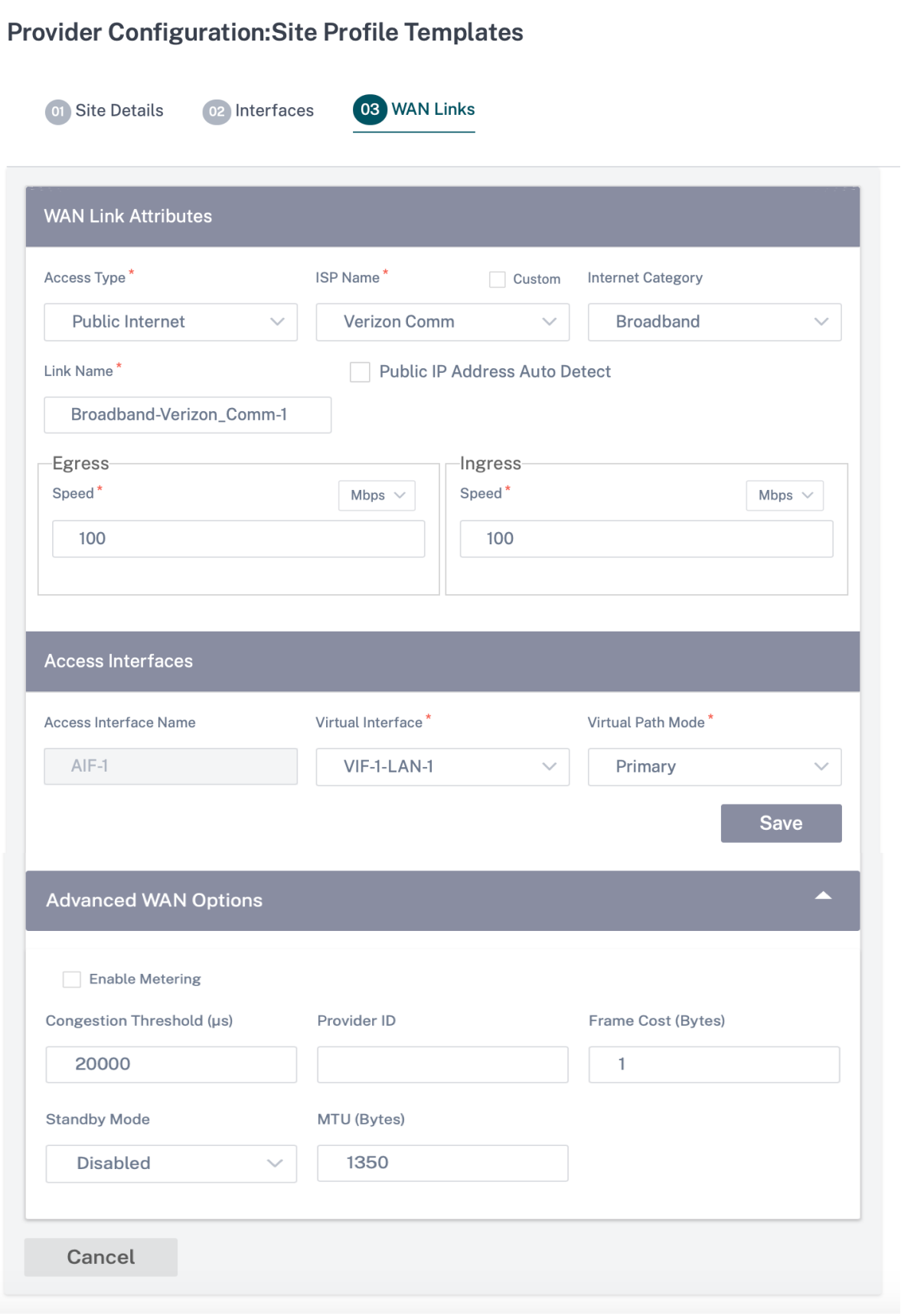
要创建站点配置文件模板，您需要配置 站点详细信息、**** 接口和 WAN 链接 ****。有关配置站点的详细说明，请参阅 站点详细信息。



通过单击 **+** 界面选项为站点分配接口。要添加接口，您需要填写接口属性、物理接口和虚拟接口字段。有关配置接口的详细说明，请参阅接口。

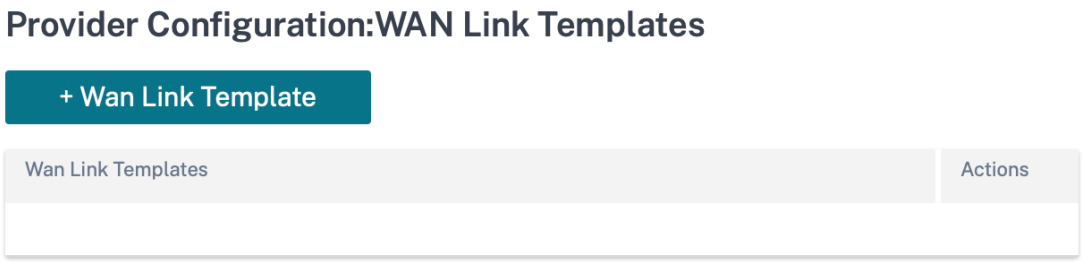


通过 高级选项提供 WAN 链接属性 **、** 访问接口和 ** 服务 **。有关配置 WAN 链接的详细说明，请参阅 WAN 链接。



WAN 链接模板

WAN 配置文件模板是由服务提供商创建的 WAN 链接配置模板，用于在客户级别创建 WAN 链接配置文件。



要创建 WAN 链接模板，请单击 **+ WAN** 链接模板。您需要填写 WAN 链接信息，例如 配置文件名称、访问类型、互联网类别、局域网到 **WAN** 的费率等。有关配置 WAN 链接的详细说明，请参阅 WAN 链接。

网络主页

October 21, 2022

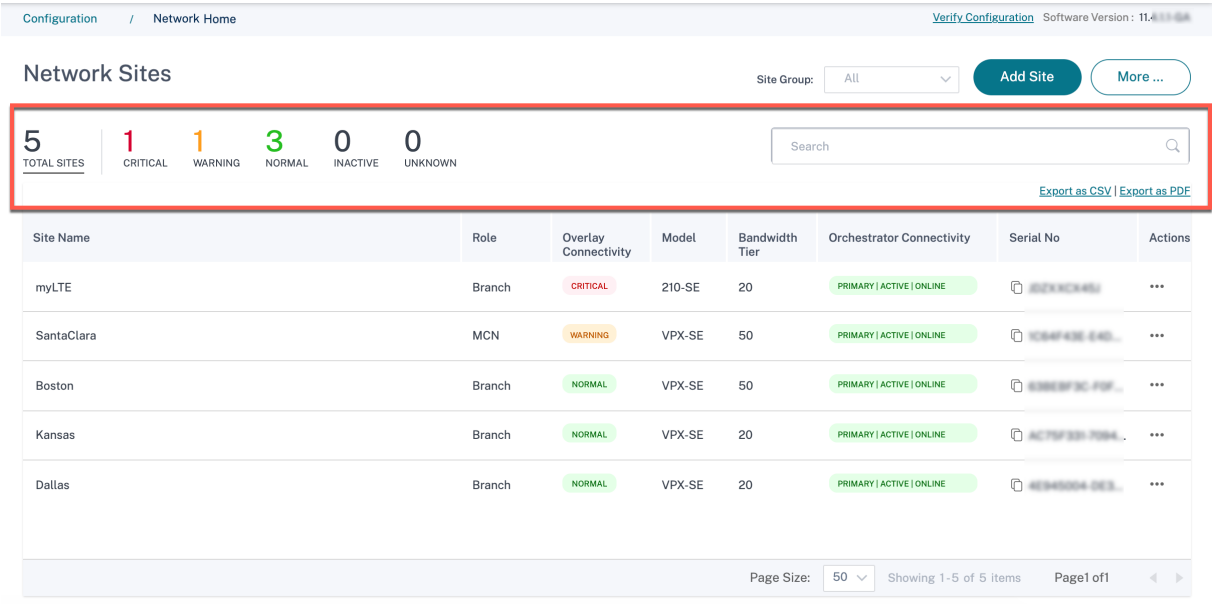
网络主页 充当网络配置的锚点，提供企业网络级配置功能，并作为配置企业 SD-WAN 网络的起点。

网络主 页显示网络中的站点总数，并根据站点的连接状态对站点进行隔离。选择带编号的链接，根据以下状态类别查看站点：

- 关键 -所有关联虚拟路径均处于关闭状态的站点。
- 警告 -至少有一条虚拟路径处于关闭状态的站点。
- 正常 -站点的所有虚拟路径和关联的成员路径均已启动。
- 非活动 -站点处于未部署和非活动状态。
- 未知 -站点状态未知。

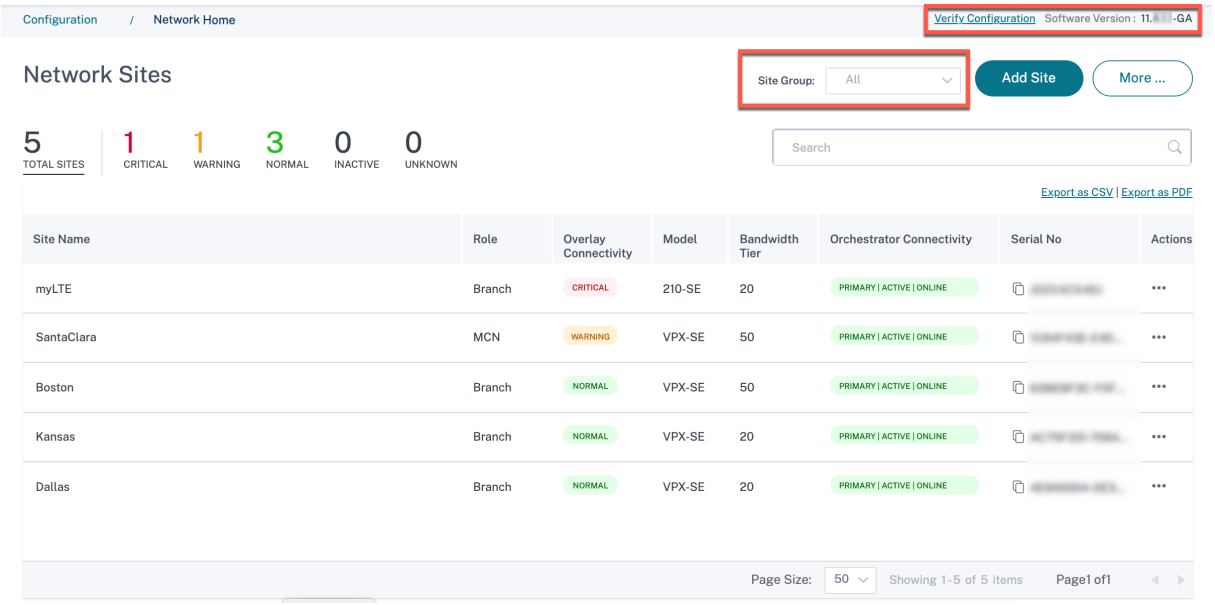
单击状态会根据站点的状态筛选站点并显示详细信息。您还可以使用 搜索 栏根据站点名称、角色、覆盖连接、型号、带宽层和序列号参数查看站点的详细信息。

您可以使用“导出为 CSV”和“导出为 PDF”选项，将筛选后的结果 导出到 **CSV** 或 **PDF** 文件中。CSV 和 PDF 文件名以 **SiteList** 为前缀，后跟导出文件的日期和时间。



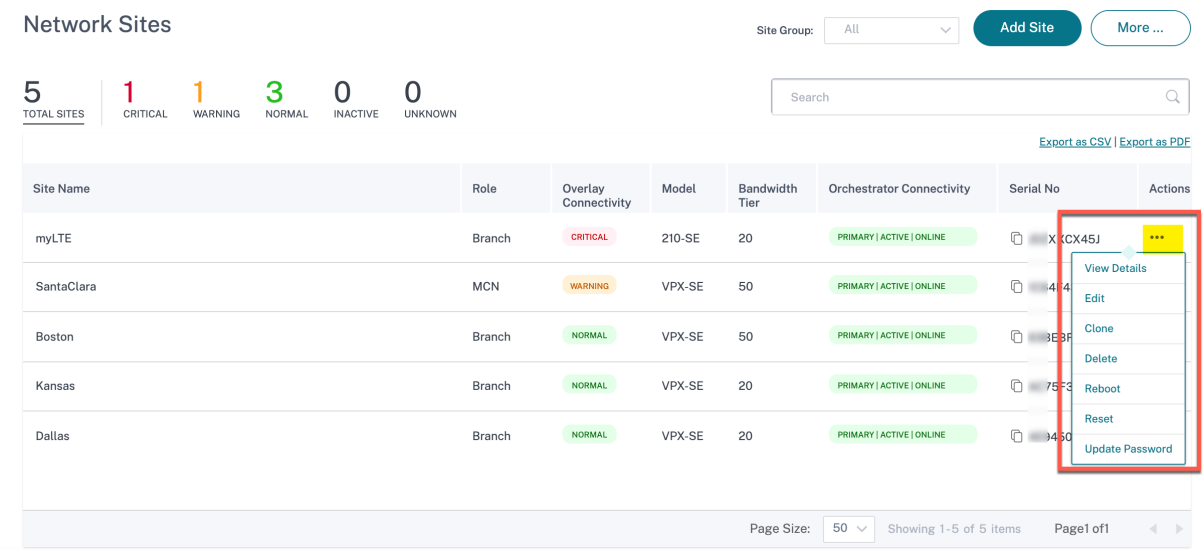
在屏幕的右上角，您可以查看当前的软件版本。单击“验证配置”以验证所有审计错误。有关更多详细信息，请参阅 验证配置。

您可以使用站点组下拉列表根据 站点所属的组 /区域筛选站点。

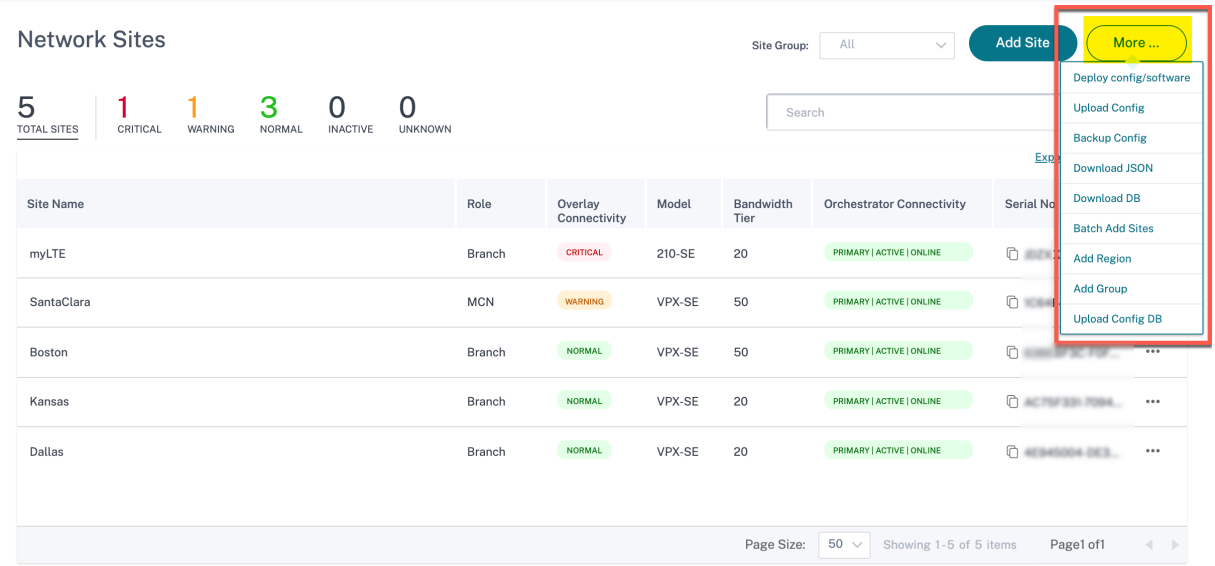


在筛选结果中单击站点名称将进入 站点配置 屏幕。如果站点处于高可用性设置中，则 **Orchestrator** 连接 列会显示主设备和辅助设备的状态。序列号 列显示设备的序列号。在高可用性设置中，会显示主设备和辅助设备的序列号。您可以使用复制图标复制设备的序列号。

使用“操作”列，您可以查看详细信息、编辑、克隆、删除、重置和更新站点的密码。您还可以重新启动与站点关联的设备。



您可以使用 更多…选项执行其他操作，例如上传配置、批量添加站点、下载 **JSON** 等。



添加网站

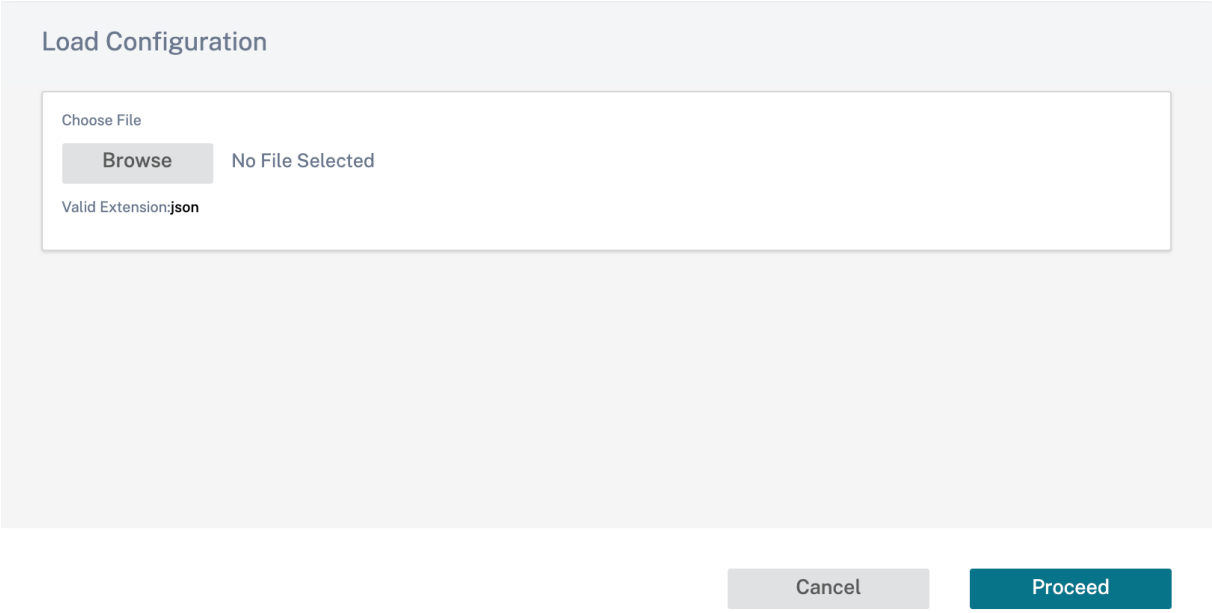
使用 **+** 添加站点 选项添加新站点。有关站点配置工作流程的更多信息，请参阅 站点配置。

部署配置和软件

“更多” **>** “部署配置/软件”选项将带您进入“部署”部分，该部分有助于在网络上验证、暂存和激活配置。有关部署配置和软件的更多信息，请参阅 部署。

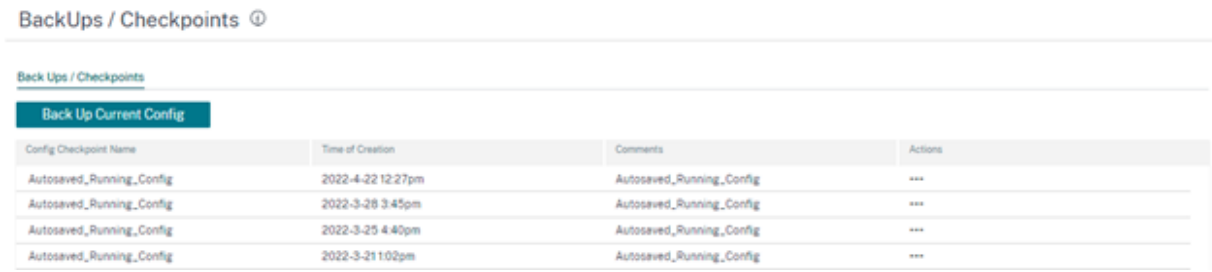
上传配置

更多 **>** 上传配置 选项允许您浏览和上传以前保存的配置之一。新上传的配置用作网络的活动配置。



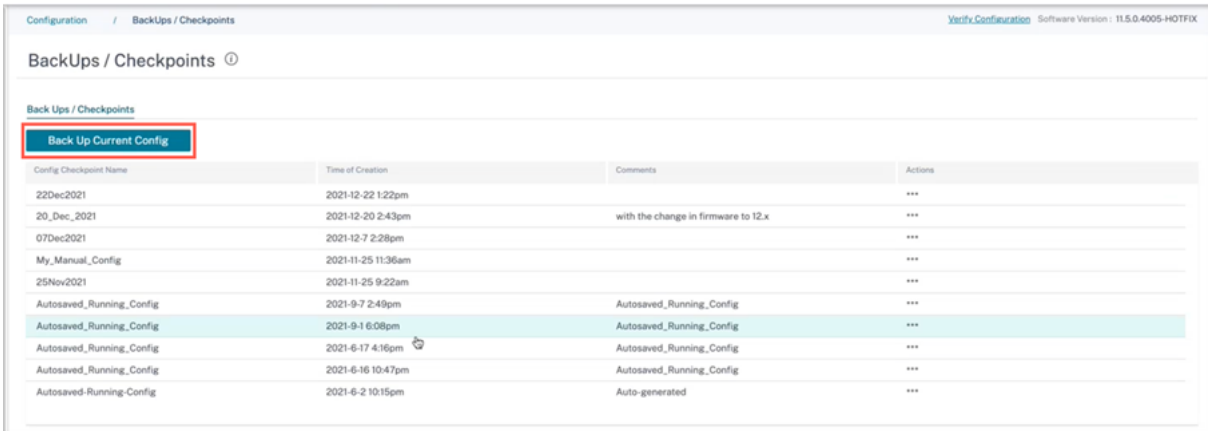
备份/检查点

“更多” **>** “备份配置”选项将带您进入“备份/检查点”页面，让您能够备份和恢复配置，或者查看保存的检查点。

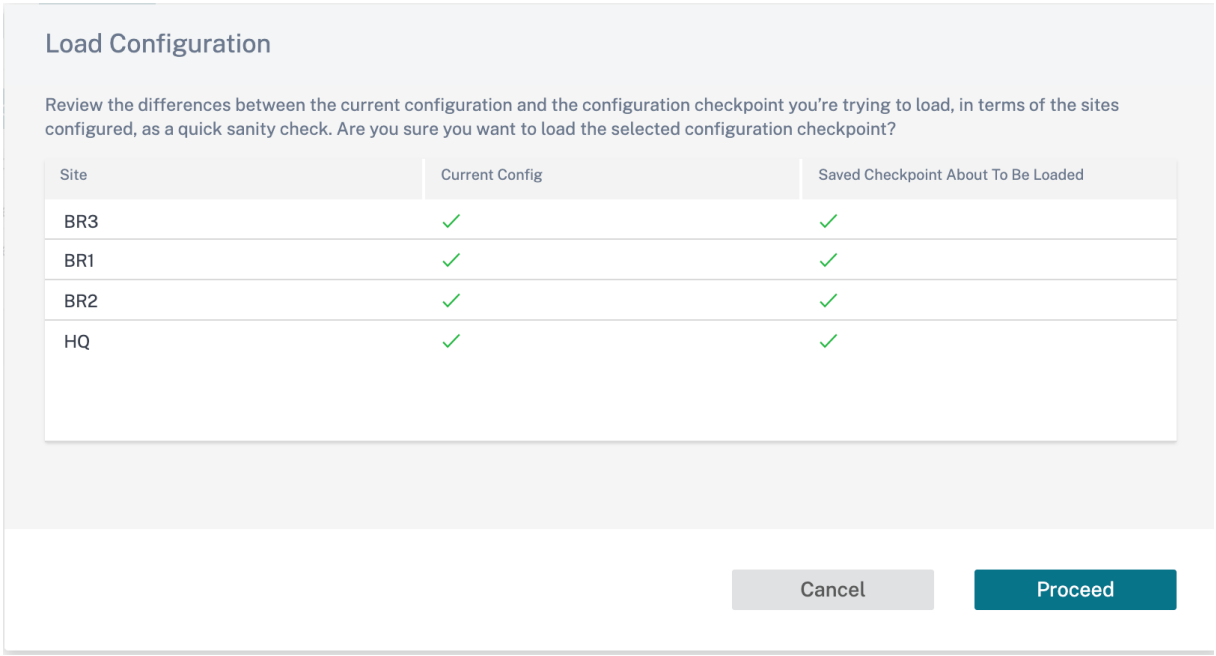


单击“验证配置”以验证任何审计错误。

单击“备份当前配置”，将当前配置作为检查点进行备份，以备将来使用。



单击“加载配置”（在“操作”下）以加载保存的配置。单击继续。



单击“复制”（在“操作”下）以创建现有配置的类似副本。您还可以下载、编辑和删除已保存的配置检查点。这些操作在“操作”下可用。

下载 **JSON**

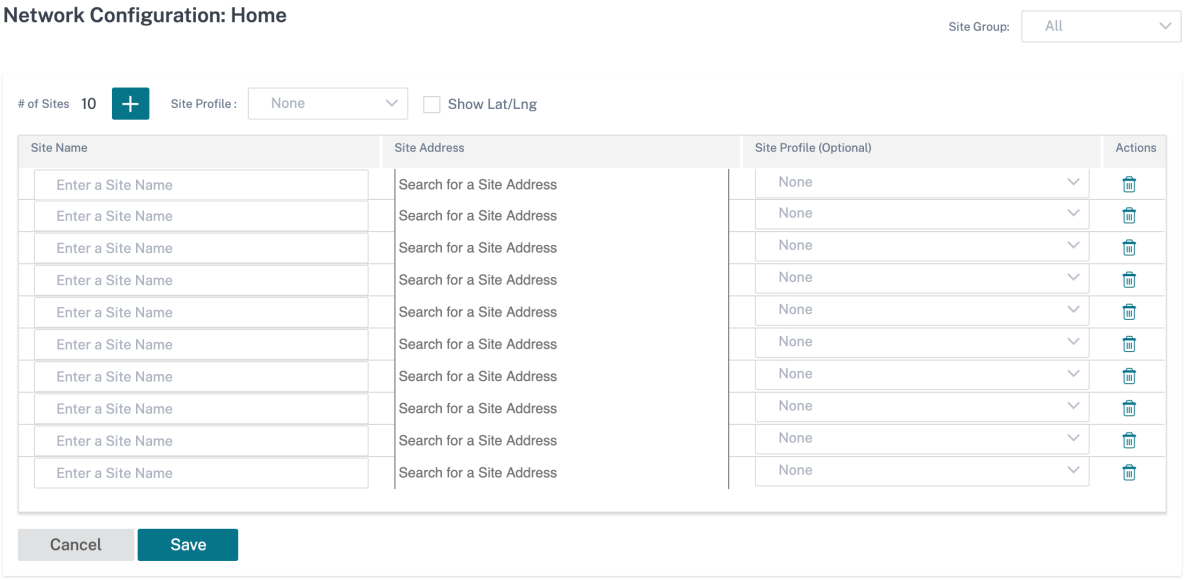
更多 **>** 下载 **JSON** 选项允许您以 JSON 格式下载和导出当前配置，以供离线查看。

下载数据库

更多 **>** 下载数据库 选项允许您以 DB 格式下载和导出当前配置。

批量添加站点

“更多” **>** “批量添加站点”选项允许您快速批量添加多个站点。您也可以选择用于每个站点的站点配置文件，只剩下唯一的参数，例如 IP 地址，这些参数还有待为每个站点配置。



添加地区

更多 **>** 添加区域 选项允许您创建区域并带您进入 站点和 **IP** 组 **>** 区域 页面。有关更多信息，请参阅 区域。

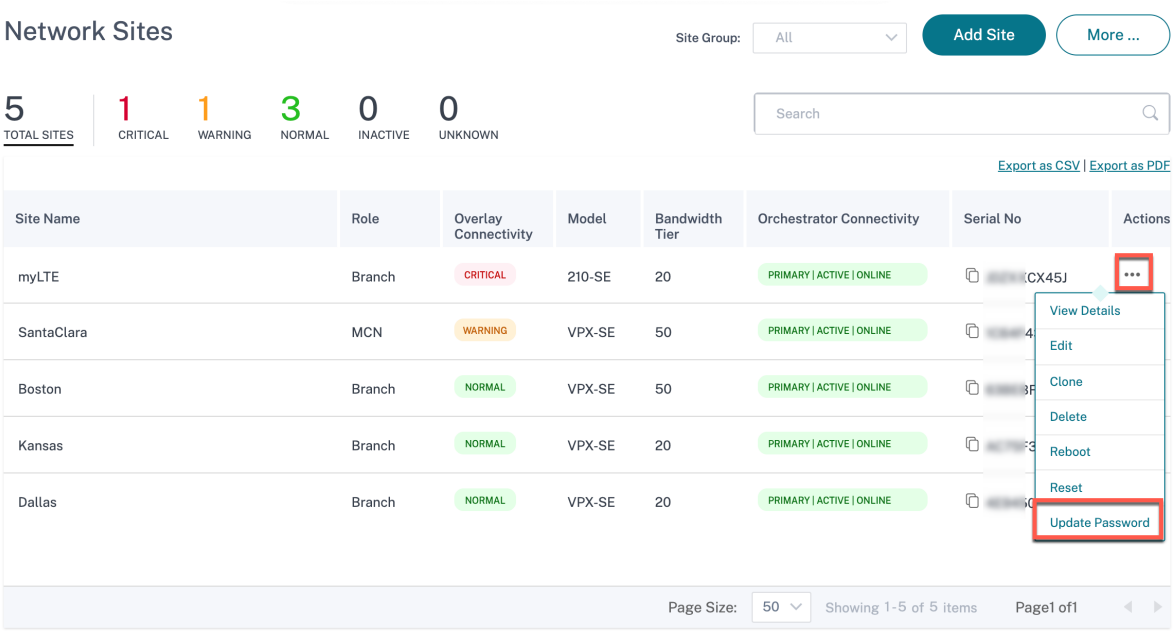
添加群组

“更多” **>** “添加群组”选项将您带到 站点和 **IP** 群组 **>** 自定义群组 页面，您可以在其中创建区域。有关更多信息，请参阅 自定义群组。

更新密码

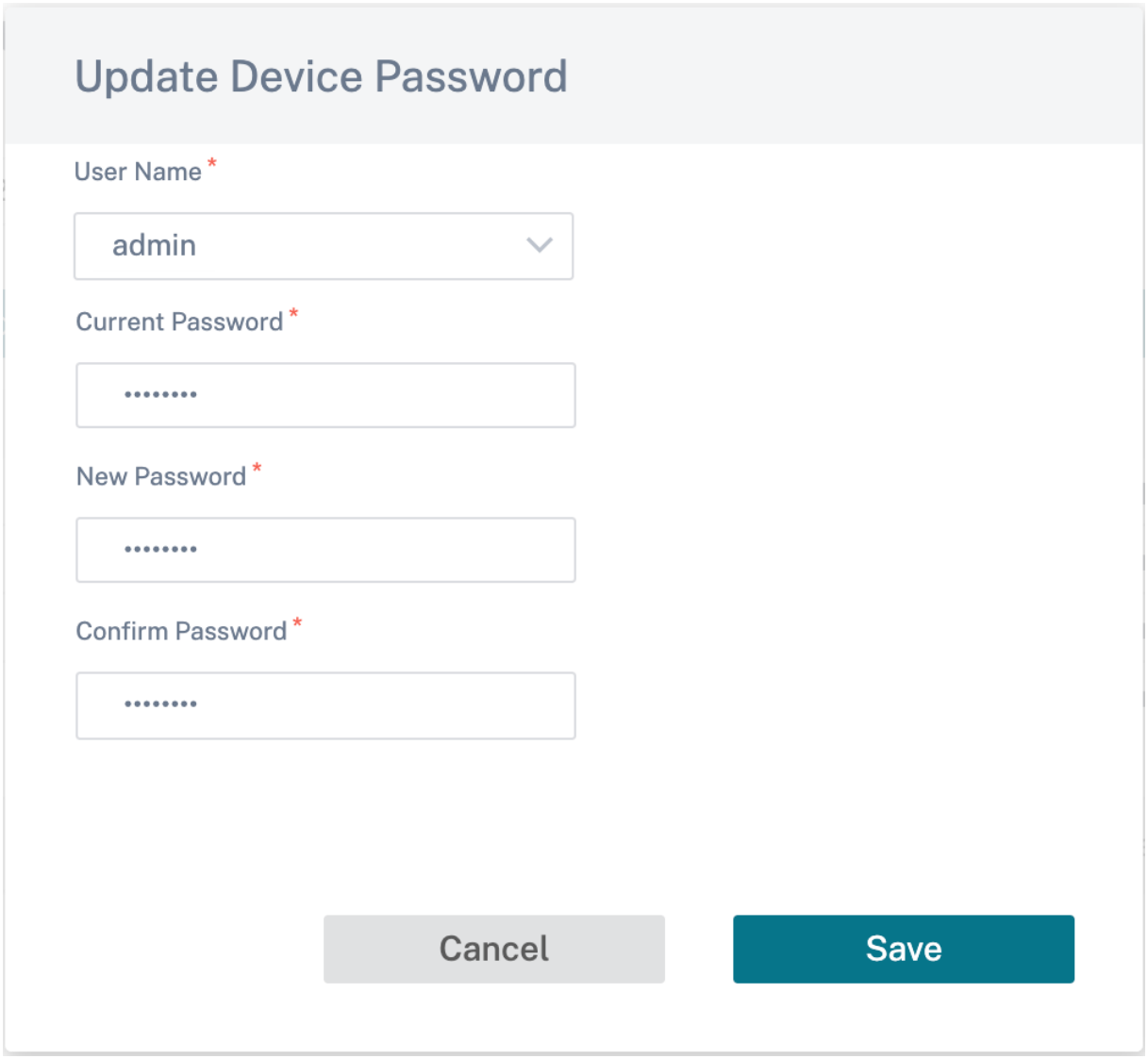
您可以通过本地的 Citrix SD-WAN Orchestrator 在网络上更改不同站点的 SD-WAN 设备的密码。

要更改密码，对于联机设备，请单击“更多”图标并选择“更新密码”。



为以下字段提供值：

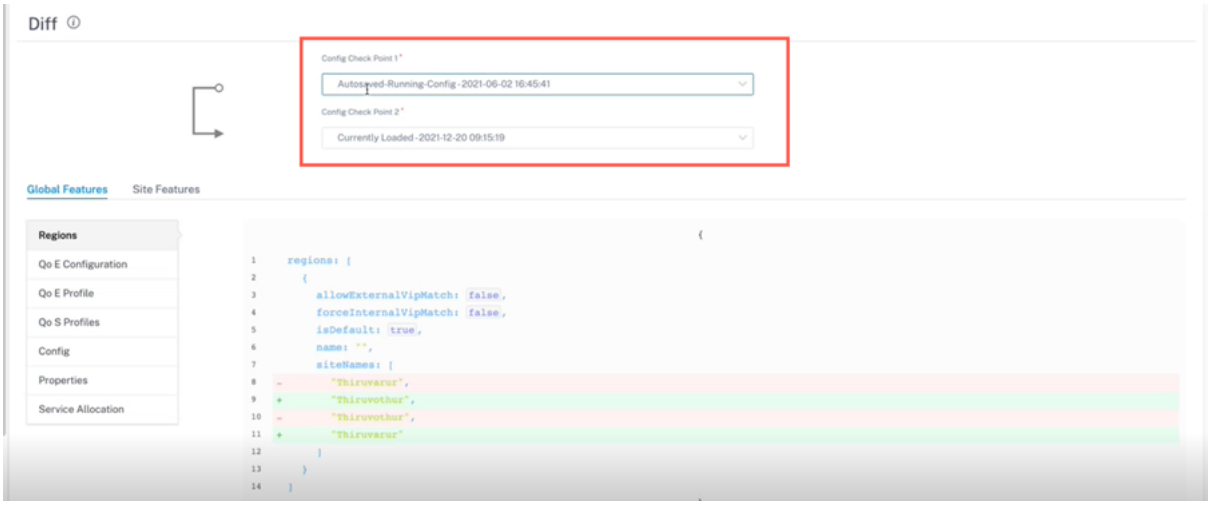
- 用户名：从站点配置的用户列表 中选择要更改密码的用户名。
- 当前密码：输入当前密码。对于管理员用户，此字段是可选的。
- 新密码：输入您选择的新密码。
- 确认密码：重新输入密码进行确认。



配置差异

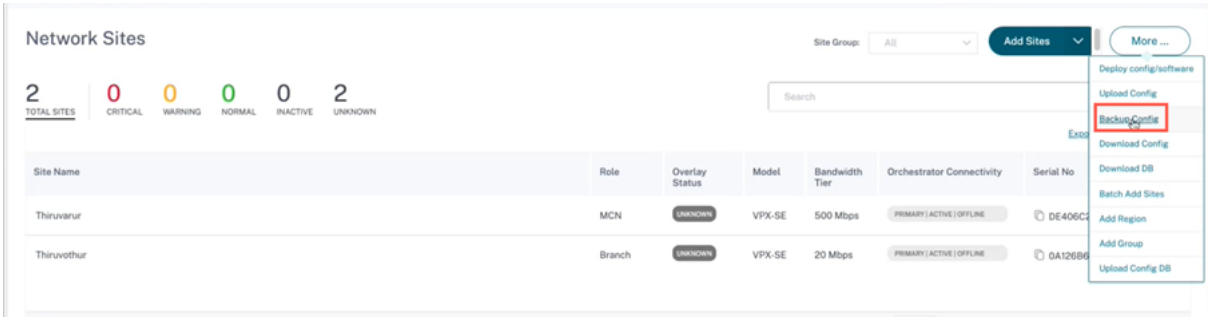
October 21, 2022

C **onfig Diff** 功能可帮助您查看任意两个版本的配置检查点之间的差异。配置差异 选项在网络级别的 配置 **>** 配置差异 下可用。

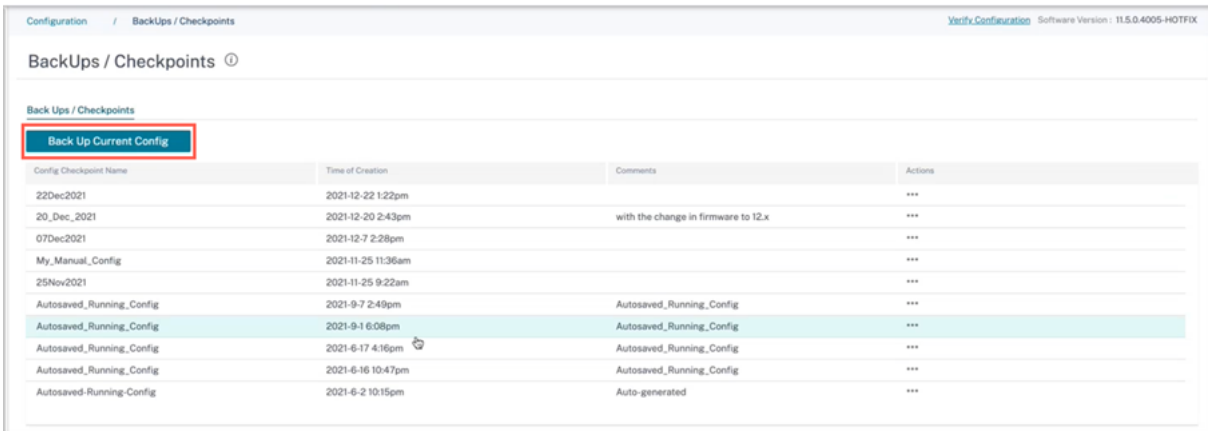


在部署期间，您可以使用合适的名称保存配置。保存的配置称为检查点。在比较两种配置之间的差异时，您需要从 **Config Check Point 1/2** 下拉列表中选择所需的配置。

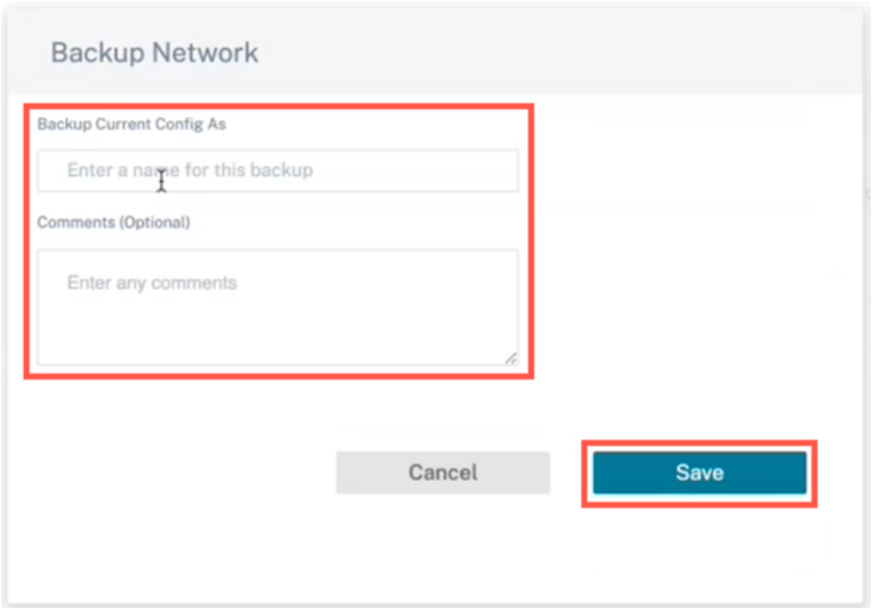
您可以在配置 > N **etwork Hom** e > 从“更多”下拉列表中选择“备份配置”下查看保存的配置备份 /检查点列表。



进行部署时，每次都会自动备份配置。您也可以手动备份当前配置。为此，请单击“备份当前配置”选项。



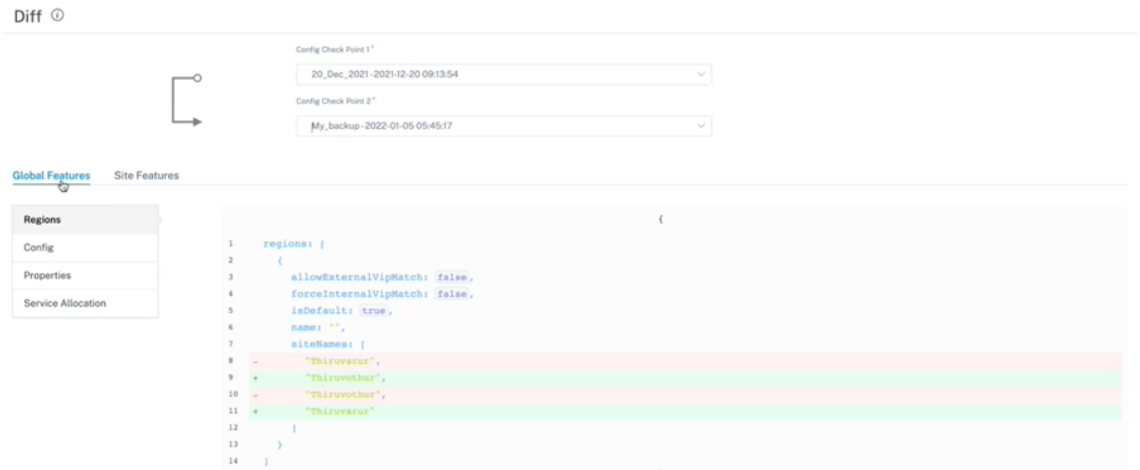
提供名称以保存您的配置和注释（可选）。单击保存。



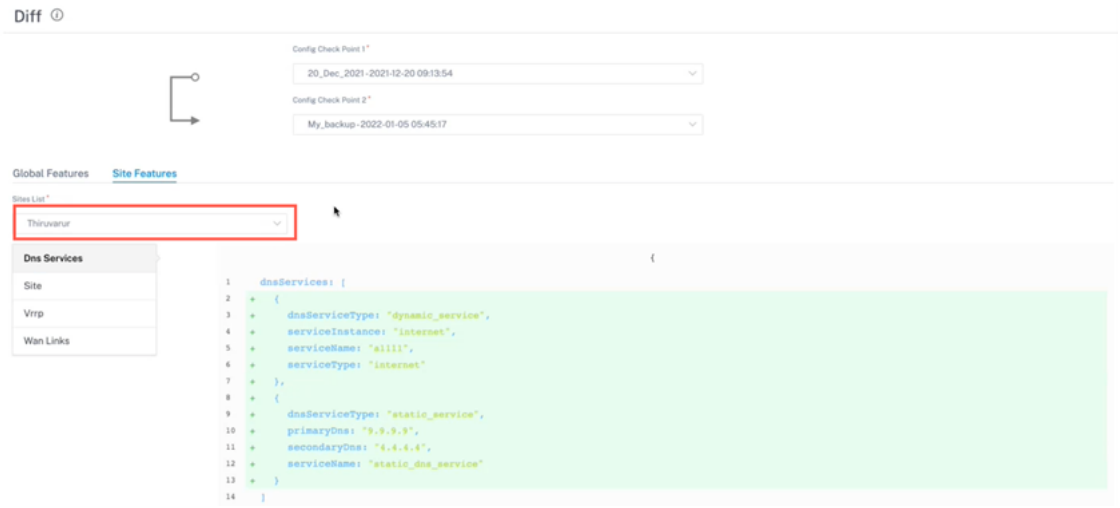
> 注意：
>
> 您最多可以保存/创建五个配置备份。创建新备份会自动删除最旧的备份配置。

有两种类型的配置可供选择：

- 全局级别：在全局类别下，您可以查看更新的全局功能列表，例如区域、属性和配置。



- 站点级别：在站点类别下，您可以从下拉列表中选择站点并查看修改后的详细信息，例如站点、WAN 链接和 DNS 服务。



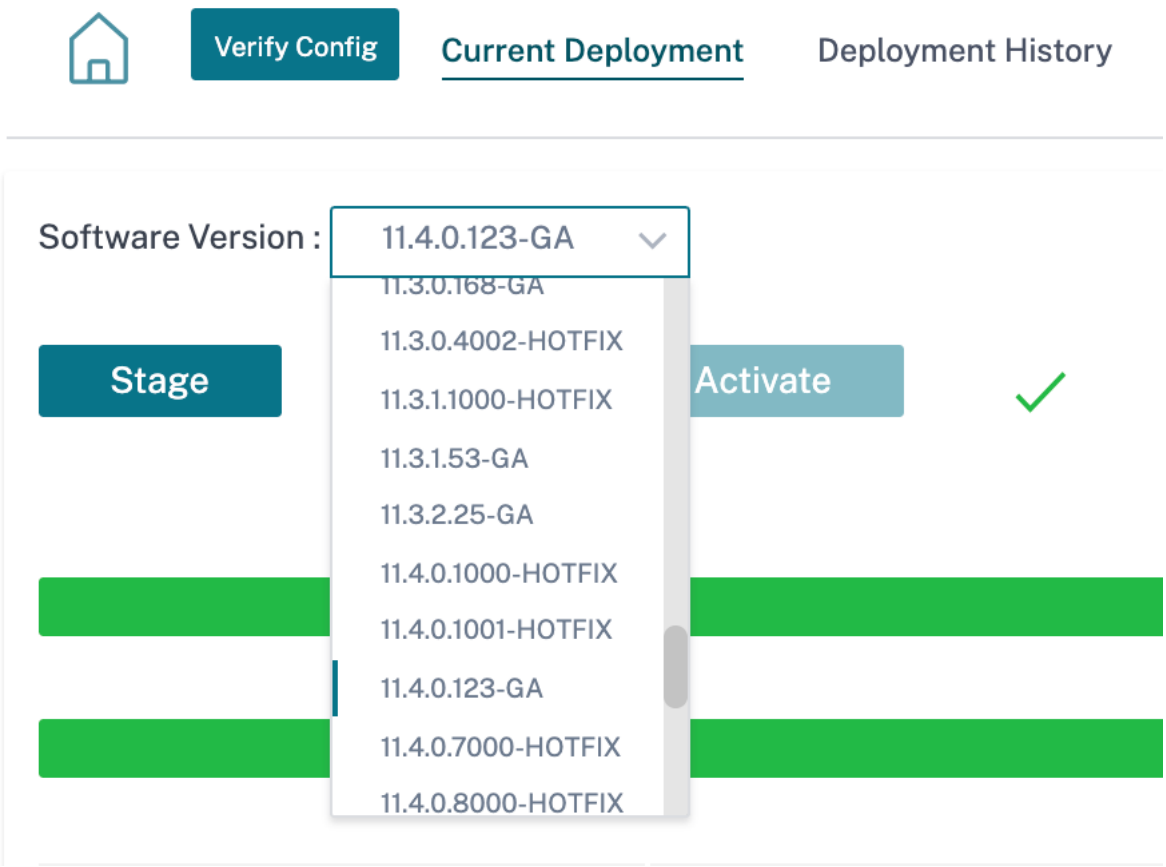
删除的值以红色背景显示，带有减号，更新/添加的值以绿色背景显示，带有加号符号。

部署

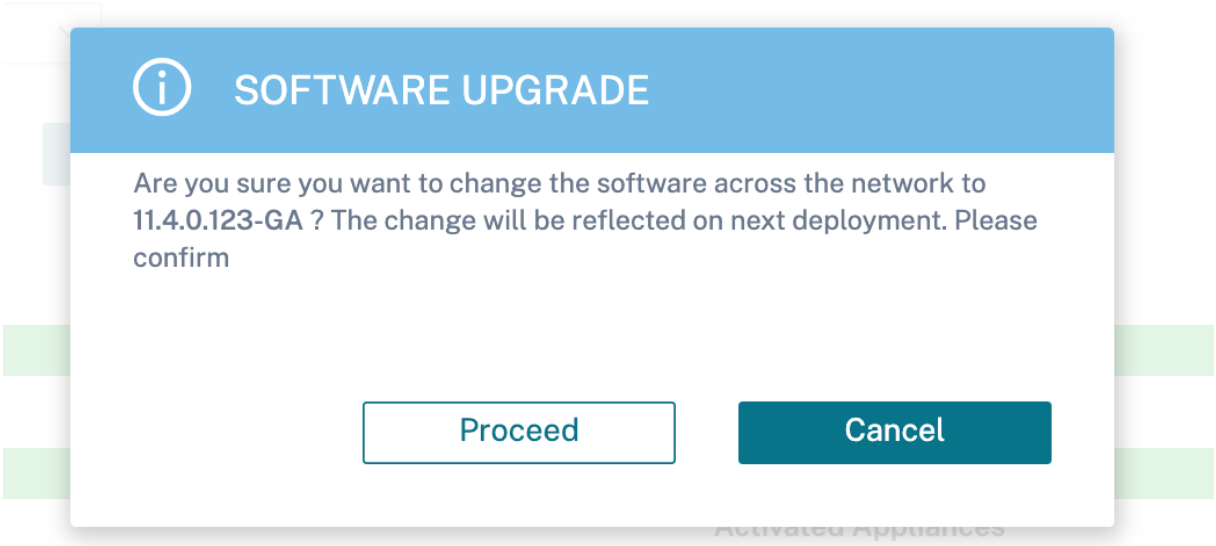
October 21, 2022

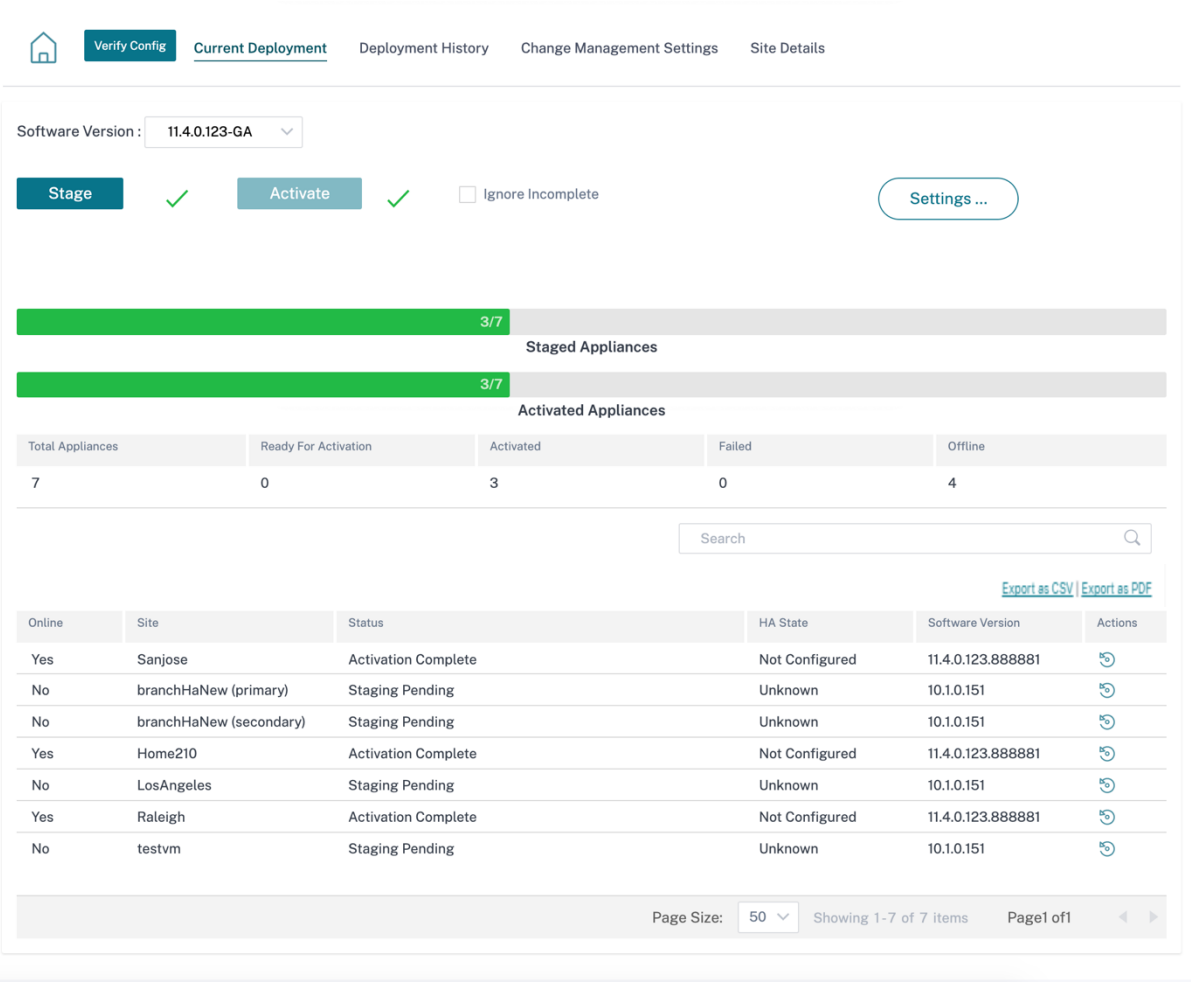
配置完站点后，“部 署”页面允许您通过网络更改软件版本、暂存和部署配置。

通过在“软件版本”字段中选择设备软件版本，您可以升级网络上所有设备上的 SD-WAN 软件。



此时将显示一条确认消息。单击继续。





出错时回滚

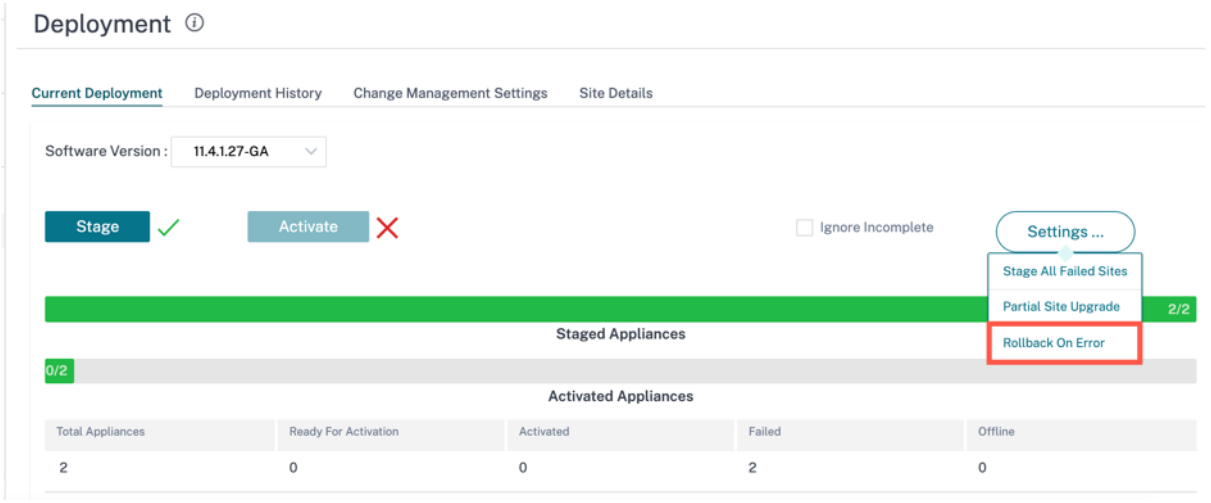
启用“错误时回滚”功能后，在 执行网络激活后（作为部署的一部分）无法连接到 Citrix SD-WAN Orchestrator 服务的站点会触发自动回滚到以前的版本（上次暂存的软件包）以尝试恢复连接。

> 注意
>
> 自动回滚仅适用于未能连接到 Citrix SD-WAN Orchestrator 服务的站点，不适用于整个网络。

只有在设备丢失 Citrix SD-WAN Orchestrator 服务连接时才会触发回滚，在虚拟路径状态关闭等其他情况下不会触发回滚。

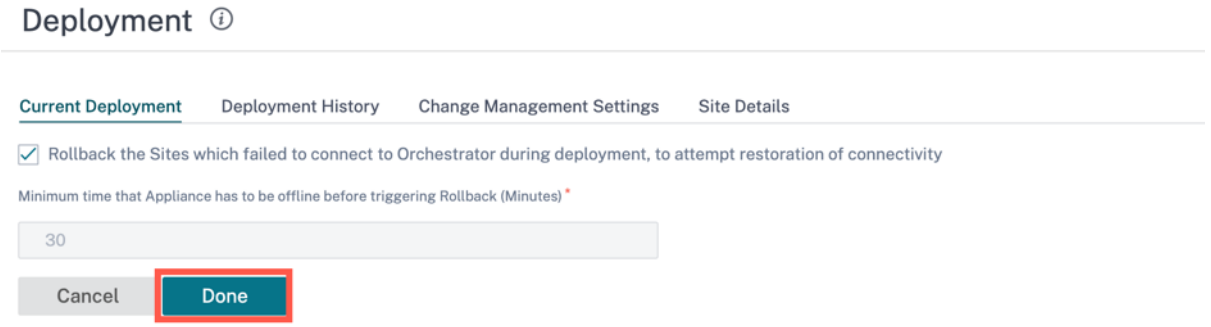
如果网络中至少有一个站点启动回滚，则警告消息会显示正在尝试回滚的站点列表以及启动所有在线站点的全网回滚的选项。您可以检查这些网站的进度并选择相应的操作。

要启用出错时回滚功能，请导航到 配置 **>** 部署 **>** 设置 **>** 出错时回滚。



您可以选中“出错时回滚”复选框以启用激活后未能连接到 Citrix SD-WAN Orchestrator 服务的站点的自动回滚。在开始部署之前，必须启用“出错时回滚”功能才能启用其功能。

要使站点触发自动回滚，它必须在激活后至少保持 30 分钟（目前不可更改）的离线状态。如果站点可以在 30 分钟内连接到 Citrix SD-WAN Orchestrator 服务，则不会触发回滚。

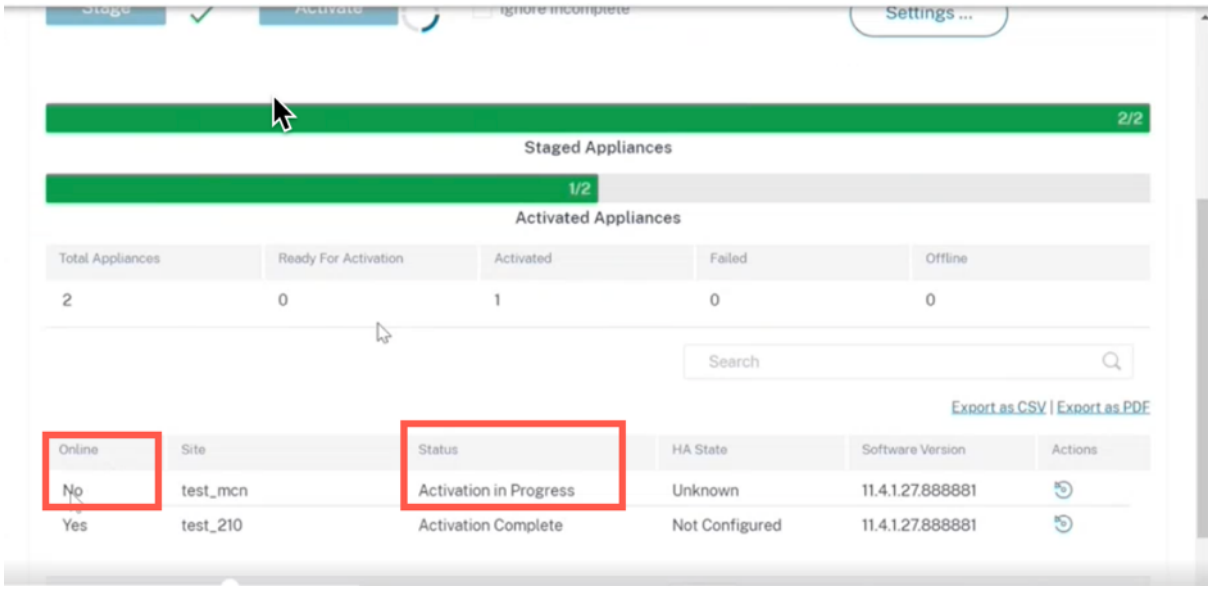


> 注意
>
> 只有在激活后站点失去连接时，才在站点上执行回滚。如果站点处于在线状态且激活失败，则不会触发回滚。

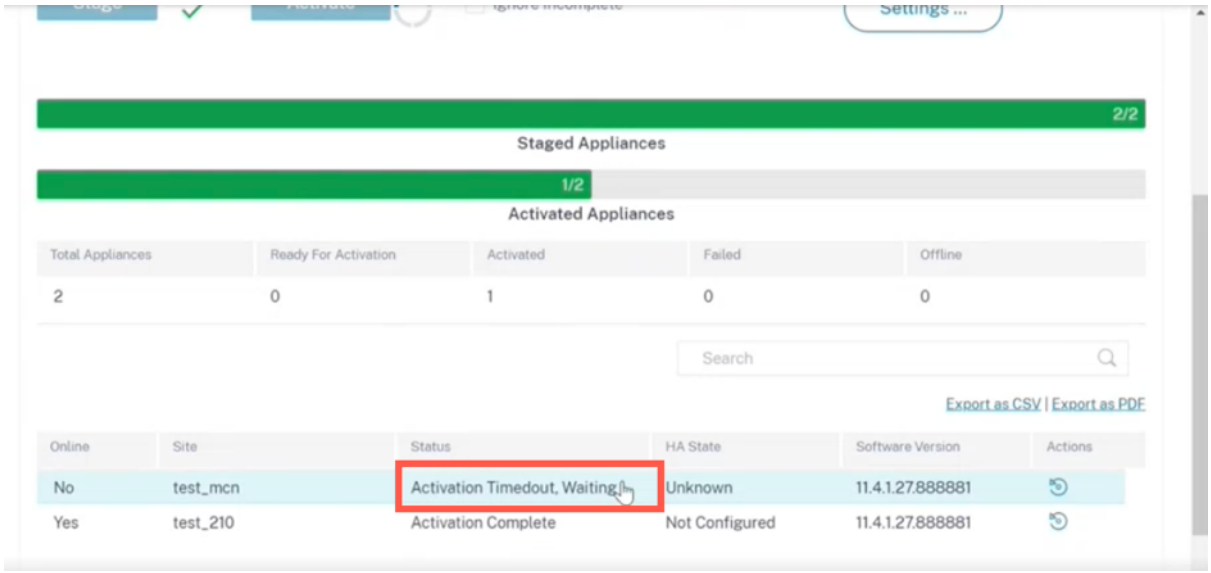
启用“出错时回滚”后，单击“完成”。

用例 **1**：无中断升级

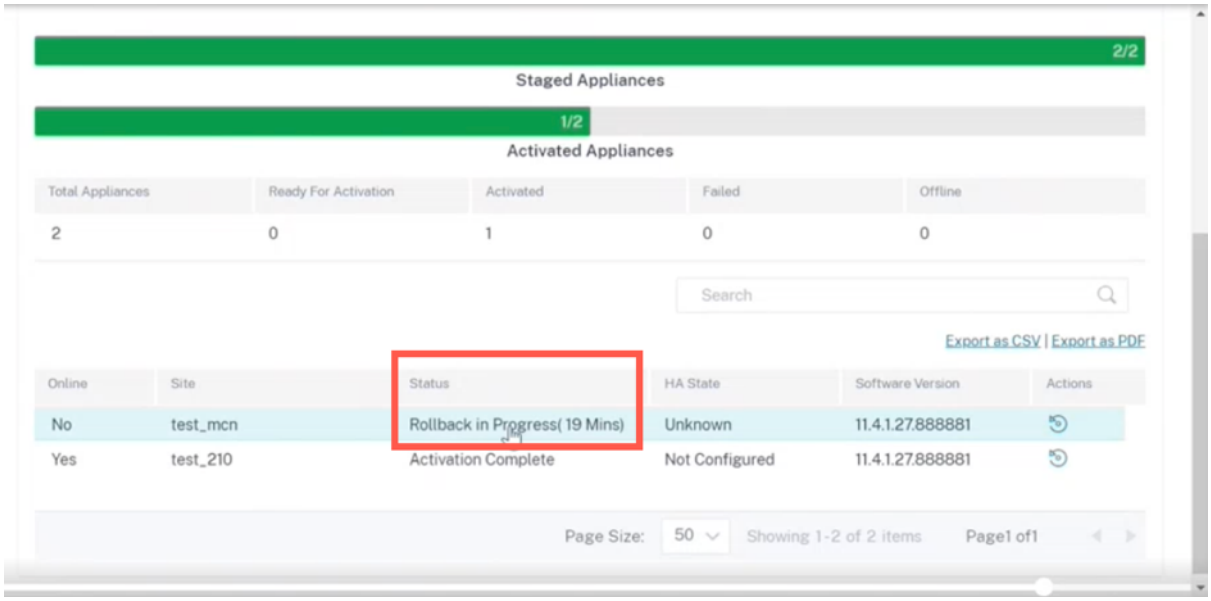
站点在指定时间内等待激活完成，状态为“激活进行中”。



在该超时之后，如果站点仍处于脱机状态，Citrix SD-WAN Orchestrator 服务将再等待 30 分钟（回滚启动超时），以便站点有机会重新连接。在此阶段，状态显示为“激活超时”、“等待启动回滚”（剩余时间以分钟为单位）。

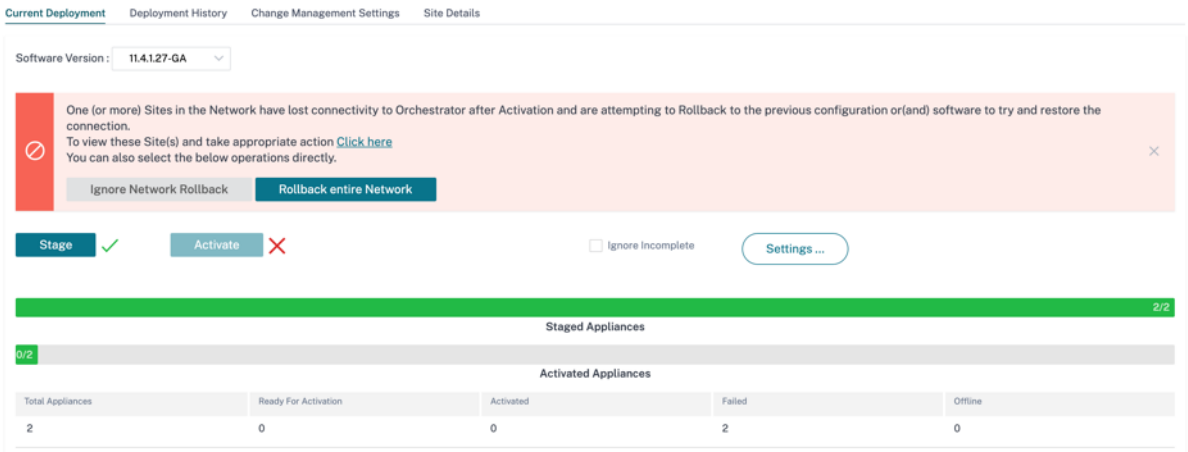


在 30 分钟的等待期之后，设备会触发自动回滚到以前的配置或（和）软件，以尝试恢复 Citrix SD-WAN Orchestrator 服务连接。Citrix SD-WAN Orchestrator 服务等待 20 分钟（不可配置的设置），设备才能连接到 Citrix SD-WAN Orchestrator 服务，在此期间，状态显示为正在 回滚（剩余时间以分钟为单位）。



如果设备无法重新连接，则在这 20 分钟内，Citrix SD-WAN Orchestrator 服务会将回滚操作标记为失败，状态显示为 设备回滚失败。

在网络中，如果至少有一台设备启动了自动回滚，则会向用户显示如下标语：



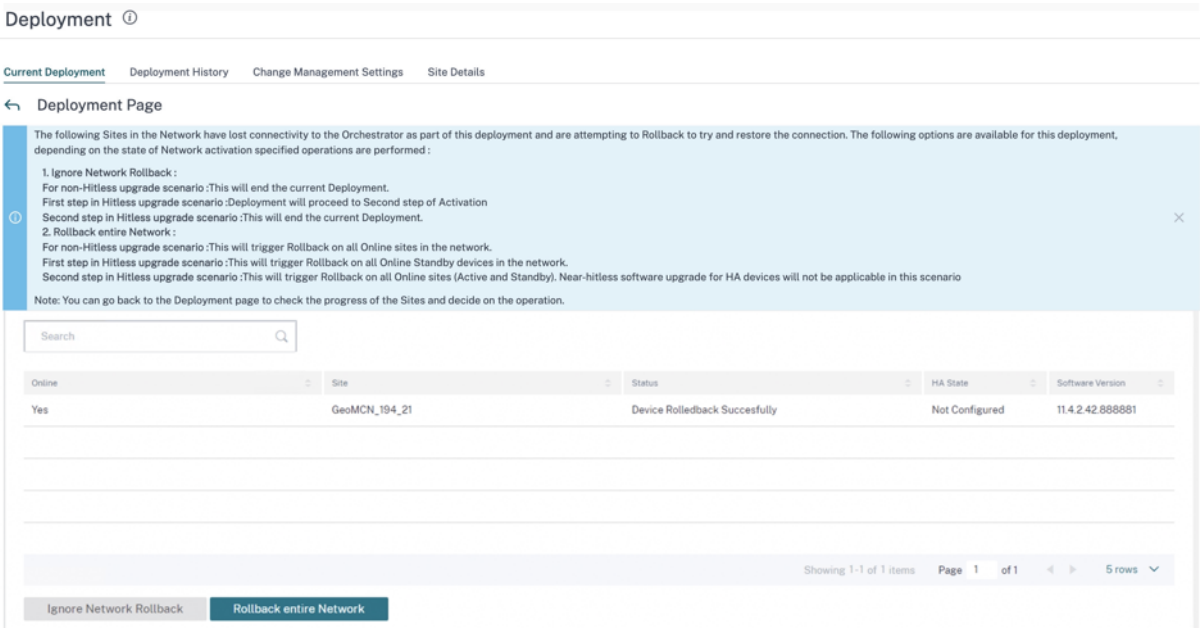
根据网络激活中的阶段，显示的选项执行以下操作：

- 忽略网络回滚：
  - 对于无中断升级方案：结束当前部署。
  - **Hitless** 升级场景中的第一步：部署进入激活的第二步。
  - **Hitless** 升级场景中的第二步：结束当前部署。
- 回滚整个网络：
  - 对于非中断升级场景：在网络中的所有在线站点上触发回滚。
  - **Hitless** 升级场景中的第一步：触发网络中所有在线待机设备的回滚。

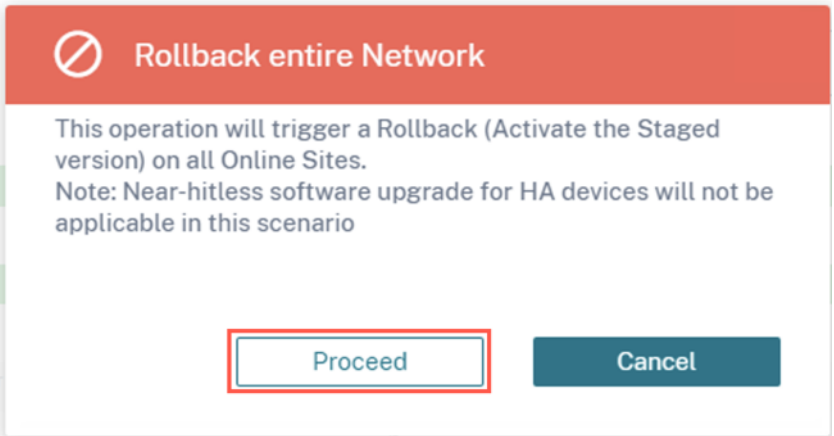
- **Hitless** 升级场景中的第二步：在所有在线站点（活动和待机）上触发回滚。在这种情况下，高可用性设备的近乎无中断的软件升级不适用。

您可以单击更多“单击此处”超链接，查看正在回滚或已完成回滚的站点列表，并对该页面执行上述操作。

您也可以等到触发回滚的站点成功或失败后再决定触发全网回滚。



如果选择“回滚整个网络”选项，则会出现以下弹出框。



> 注意：
> 高可用性设备的 Near-Hitless 软件升级不适用于这种情况，也就是说，如果网络中有任何高可用性站点，则触发全网回滚会同时激活该站点的两个高可用性设备，这可能会导致一些网络停机。

单击“继续”开始在所有在线站点上进行全网回滚。

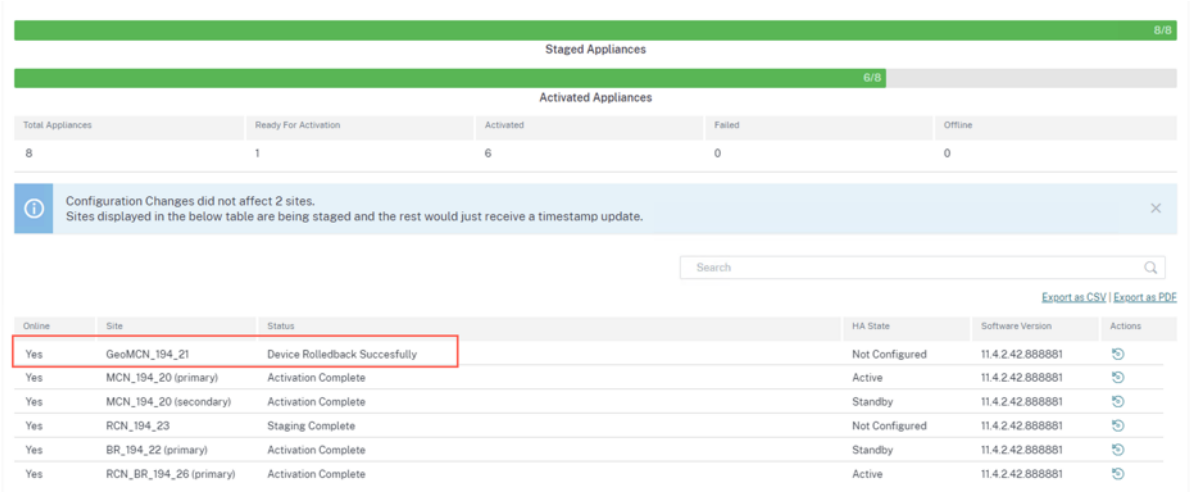
用例 **2**：无中断升级

在 Hitless 升级的情况下，将首先激活备用设备，然后激活活动和非高可用性设备。作为第一步的一部分，如果备用设备在激活后脱机并启动回滚，则可以使用以下选项：

- 忽略网络回滚：忽略处于脱机状态的待机设备，继续激活活动设备。
- 回滚整个网络：回滚所有已完成激活的在线备用设备并结束正在进行的部署。在这种情况下，不激活活动和非高可用性设备。

无中断升级的下一步是激活活动和非高可用性设备，如上面 非中断升级 部分所述，遵循相同的错误回滚工作流程。在这种情况下，如果您选择“回滚整个网络”，则会触发所有（活动和待机）设备的回滚操作。

站点完成回滚并连接回 Citrix SD-WAN Orchestrator 服务后，该站点的状态将显示 设备回滚成功 且站点处于联机状态。



限制

不支持对回滚或回滚设备和网络进行自动更正。

> 注意
> 自动站点回滚只是一种备份机制，用于尝试恢复与 Citrix SD-WAN Orchestrator 服务断开的连接。如果设备仍然无法连接到 Citrix SD-WAN Orchestrator 服务，请检查此设备的网络配置。

您可以使用“导出为 CSV”和“导出为 PDF”选项，将筛选后的结果 导出到 **CSV** 或 **PDF** 文件中。CSV 和 PDF 文件名以 部署站点列表 为前缀，后跟导出文件的日期和时间。

- 阶段：成功验证配置后，单击 **Stag** e 将配置文件分发到网络中的所有设备。默认情况下，Citrix SD-WAN Orchestrator 服务在允许用户激活之前会等待所有控制节点（MCN、RCN、Geo MCN、Geo RCN）和在线分支设备进入暂存状态。

  如果转移过程在任何站点失败，请使用“操作”列下的“重试暂 存”选项来重新启动过渡进程。

- 激活：单击“激活”以激活网络中所有站点上的暂存配置。
- 忽略未完成：选中后，激活 复选框仅在所有在线控制节点（MCN、RCN、Geo MCN、Geo RCN）上线后启用。即使某些在线分支设备未暂存，您也可以选择激活。无法暂存的联机分支设备将被忽略。
- 部分站点升级设置：添加“部分站点升级”选项以使用其他版本对所选站点进行升级或降级。通过 局部站点升级 功能，可以在将新版本部署到整个网络之前测试新版本。

使用 部分站点升级 功能，可以错开升级，从而减少工作时间内软件升级的影响。

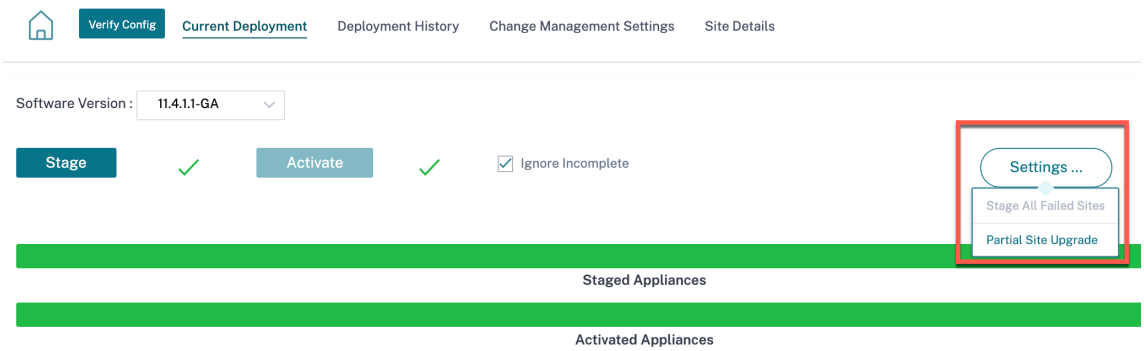
> 注意
>
> 只有当网络中的所有站点都运行 Citrix SD-WAN 软件版本 11.2.2 或更高版本时，才能执行部分站点升级。

部分站点升级 的任何配置更改都需要变更管理才能使更改生效。部分站点升级 会选择较低版本并生成相同版本的配置。当网络处于“部分站点升级”模式时，无法测试任何新功能。

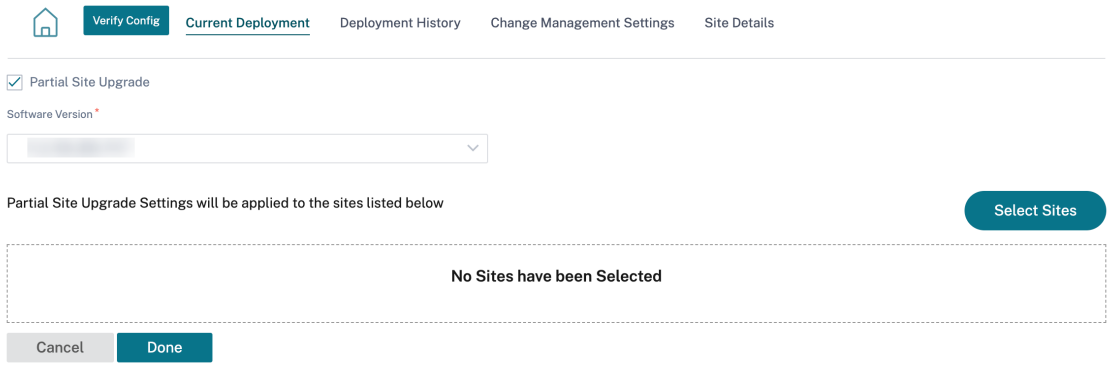
当您使用 部分站点升级从较新版本降级到较旧版本时，如果某项功能仅在较新版本中受支持（新版本和旧版本中均存在相似配置），则会出现审计错误。例如，选择了一个只有较新版本支持的新平台，那么这将引发审计错误。

要执行部分站点升级，请执行以下操作：

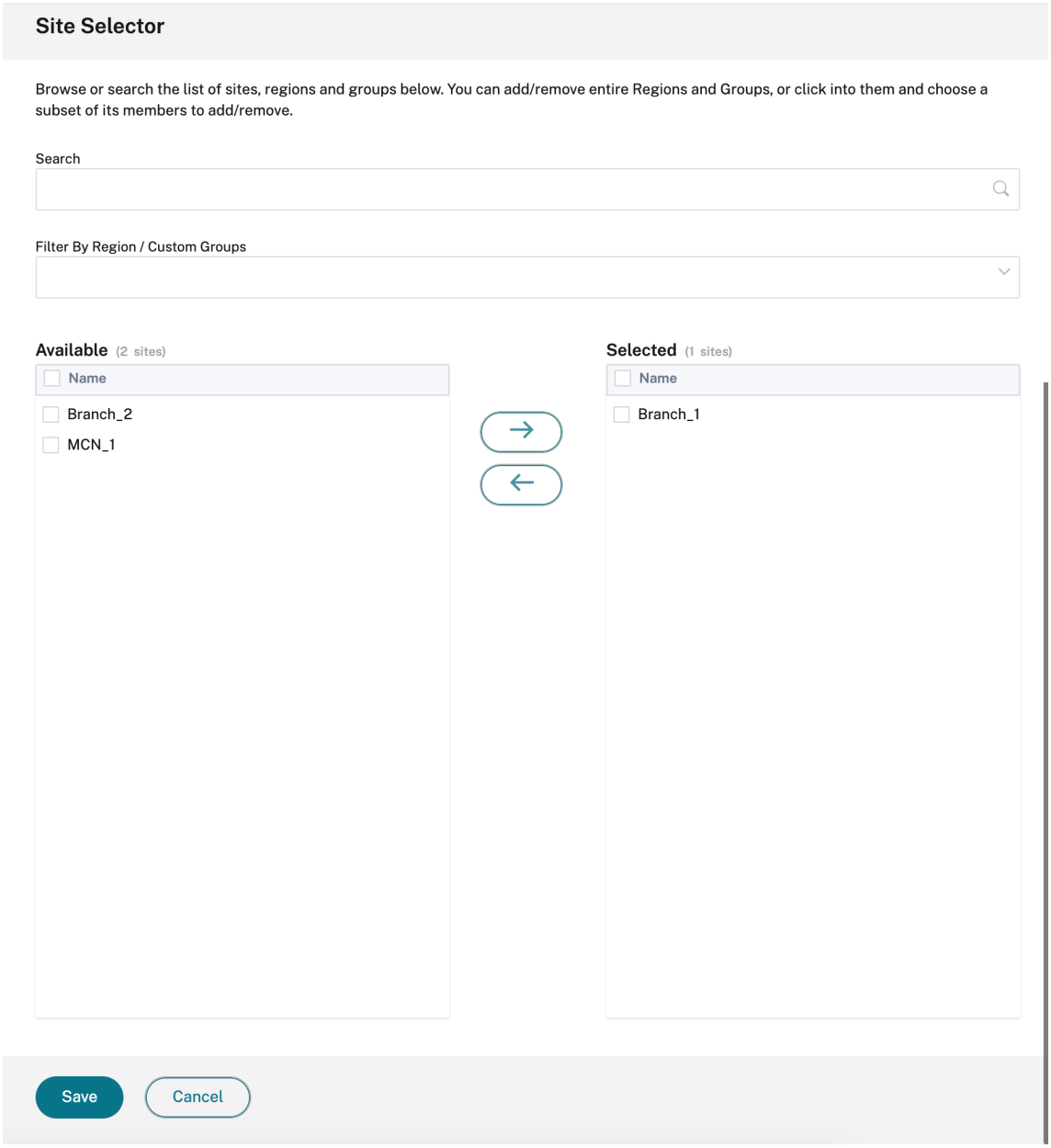
1. 点击 设置…图标并选择“部分站点升级”选项。

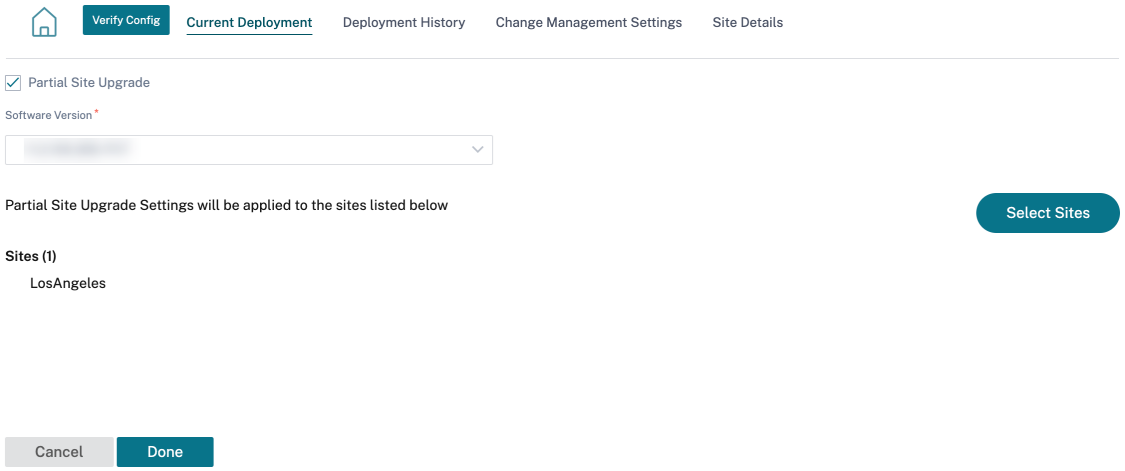


2. 选中“部分站点升级”复选框，选择软件版本，然后单击“选择站点”以添加新站点。



3. 选择站点，然后单击“保存”。

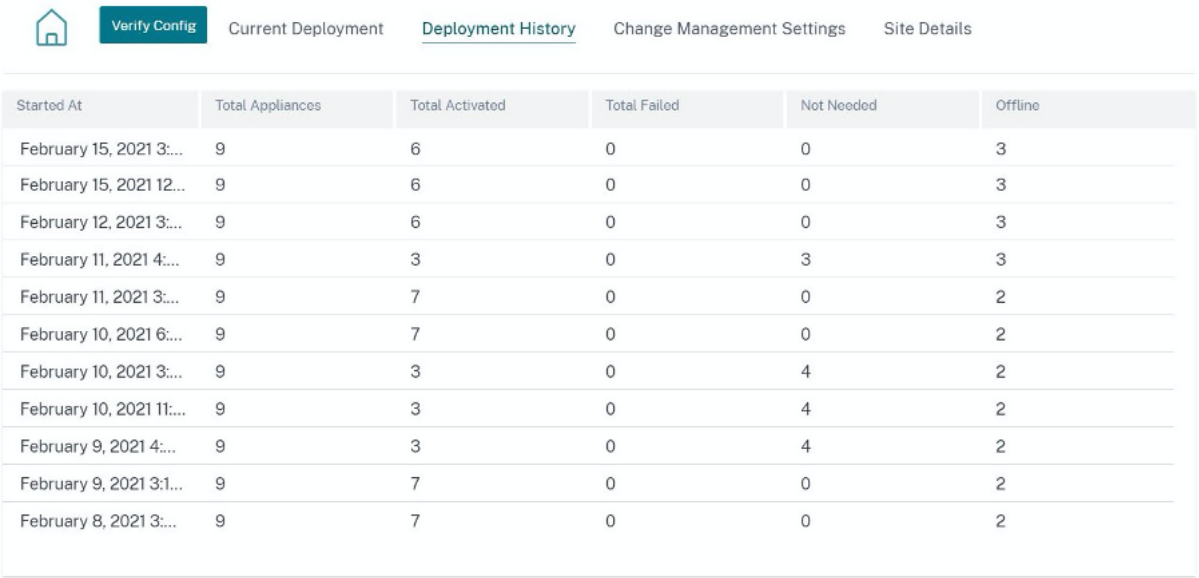




如果是仅限配置的更新，则仅暂存和激活配置更改的站点。对于其余站点，时间戳已更新和处理。

如果要更改软件版本，则配置和软件包都将在网络中的所有站点上暂存和激活。

部署历史记录 部分有助于查看以前的部署操作和结果。



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 几乎无中断的软件升级

在软件升级（11.0.x 及更早版本）期间，网络中所有设备的试运行和激活是同时完成的。这包括高可用性 (HA) 对，导致网络停机。借助 HA 近乎无中断的软件升级功能，Citrix SD-WAN Orchestrator 服务可确保软件升级（11.1.x 及更高版本）过程中的停机时间随着时间的推移不超过 HA 切换。

> 注意
>
> HA 几乎无中断的软件升级适用于以下方面：
>
> - 在高可用性 (HA) 模式下部署的站点。它不适用于非医管局网站。
> - Citrix SD-WAN Orchestrator 仅基于服务的部署，不适用于使用 SD-WAN Center 或 MCN 管理的网络。
> - 仅进行软件升级，而不是配置更新。如果在升级过程中随软件一起更改了配置，则 Citrix SD-WAN Orchestrator 服务不会执行 HA 近乎无中断的软件升级，而是继续以较早的方式（单步升级）升级。

升级顺序摘要：

1. Citrix SD-WAN Orchestrator 服务检查网络中所有设备的 HA 状态。
2. 升级所有处于 待机 状态的辅助设备。
3. 触发 HA 切换并切换 活动 和 待机设备的状态。
4. 升级现在处于 待机 状态的主设备。

HA 几乎无中断的软件升级是一个两个步骤的升级过程：

步骤 **1**：在软件升级期间，在 11.1 版本之后，Citrix SD-WAN Orchestrator 服务首先对网络中处于 待机 状态的所有设备执行软件升级。在 Act **ive** 设备 到位的情况下，网络仍在运行中。

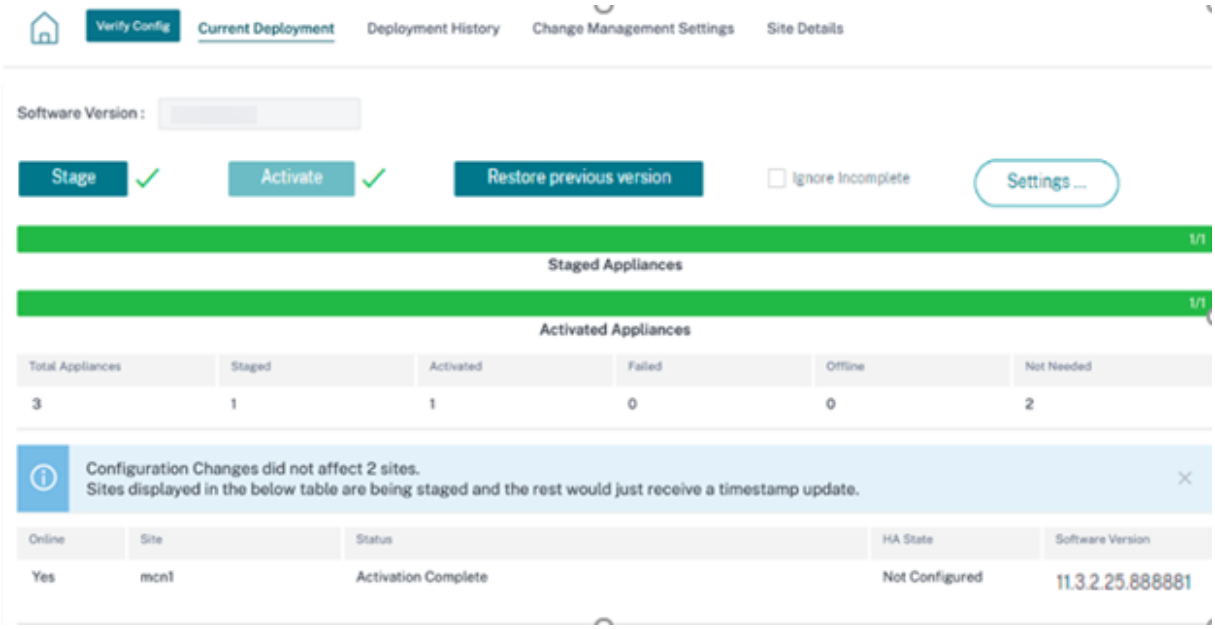
将所有 待机 设备升级到最新软件后，将通过网络触发 HA 切换。备用 设备（装有最新软件）变为 活动状态。

步骤 **2**：使用旧软件版本的当前 待机 设备已升级到最新软件，并将继续在 待机 模式下运行。

在此软件升级过程中，所有其他非 HA 站点也将使用最新软件激活。

有关更多信息，请参阅 常见问题解答。

您可以通过导航到“部署跟踪器” **>** “当前部署”来查看升级状态。



- 阶段：单击 **Stage** 将配置文件分发到网络中的所有设备。默认情况下，Citrix SD-WAN Orchestrator 服务会等待所有控制节点（MCN、RCN、Geo MCN、Geo RCN）和在线分支设备进入暂存状态，然后才允许用户激活。
- 激活：单击“激活”以激活网络中所有站点上的暂存配置。
- 恢复以前的版本：单击“恢复以前的版本”可回滚到网络上之前激活的配置。如果以前的活动版本只是软件版本更改而不是配置更改，则在恢复先前版本时适用 HA 近乎无中断的软件升级。有关此功能的更多信息，请参阅 恢复以前的版本。
- 忽略未完成：选中后，激活 复选框仅在所有在线控制节点（MCN、RCN、Geo MCN、Geo RCN）上线后启用。即使某些在线分支设备未暂存，您也可以选择激活。无法暂存的联机分支设备将被忽略。

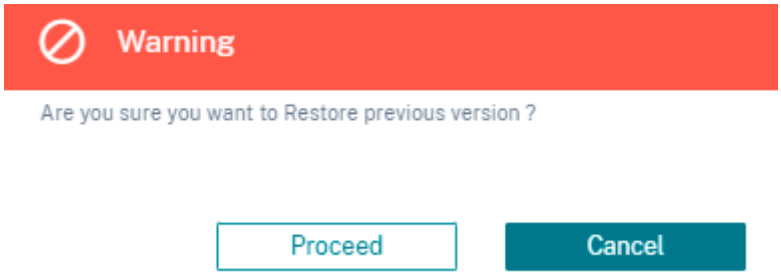
如果是仅限配置的更新，则仅暂存和激活配置更改的站点。对于其余站点，时间戳已更新和处理。“不需要”列出了未进行任何配置更改的站点数量。

如果要更改软件版本，则配置和软件包都将在网络中的所有站点上暂存和激活。

恢复以前的版本

在恢复先前版本的功能中，Citrix SD-WAN Orchestrator 服务在网络范围内启动先前配置的激活，并在您的网络上恢复之前激活的配置（和/或软件）。

选择“恢复以前的版本”选项时，将显示以下确认消息：



> 注意
>
> 当网络未处于暂存状态时，可以执行“恢复以前的版本”操作。对于分段网络，此选项处于禁用状态。

自动更正配置和软件升级

在 Citrix SD-WAN Orchestrator 服务中，自动更正功能是在变更管理工作流中实现的。

当一个站点的暂存失败时，如果暂存失败的站点是控制节点，则需要在收到暂存失败消息后重新暂存。如果控制节点的转移失败，则不会启用“激活”按钮。如果暂存失败的站点是分支节点，则仍允许您继续进行激活。但是，要使该分支机构与网络同步，请执行另一轮变更管理。

> 注意
>
> - 自动更正检查仅在单击“激活”按钮后启动，并在 Citrix SD-WAN Orchestrator 服务用户界面发出下一

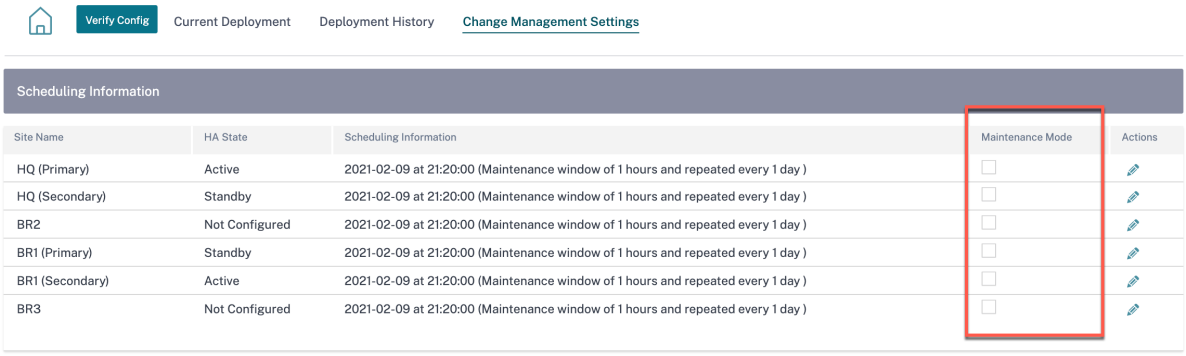
> 阶段后停止。
>
> - 维护模式功能仅适用于自动更正功能。如果您启动“暂存 和 激活”，则启用维护模式的设备也会根据软件和配置更改进行更新。

借助自动校正功能增强功能，当发生暂存失败时，自动校正机制会将预期的软件和配置版本推送到出现故障的分支，并尝试使其与当前网络同步。自动更正功能适用于分支节点上的转移失败和任何节点上的激活失败。

以下是自动校正开始时的两个触发点：

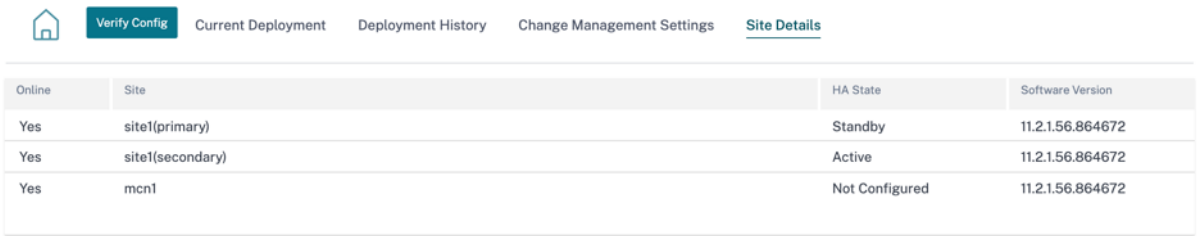
- 在 Citrix SD-WAN Orchestrator 服务部署跟踪器用户界面中，一旦收到“暂存失败”或“激活失败”消息，自动更正就会开始在后台运行。激活完成后，自动更正检查将开始。
- 如果软件和配置不匹配，设备没有提供预期的软件和配置版本，Citrix SD-WAN Orchestrator 服务会开始将实际需要的软件和配置副本推送到设备进行激活。

要手动对设备进行故障排除，请启用“更改管理设置”下方的维护模式复选框。此复选框用于控制是否需要检查设备以进行自动更正。清除维护模式复选框后，自动更正将使设备与网络软件和配置版本同步。



网站详情

部署跟踪器下的“站点详细信息”选项卡提供有关网络中所有设备的信息。该表包含设备名称、Citrix SD-WAN Orchestrator 服务连接、高可用性 (HA) 状态和当前正在运行的软件版本。



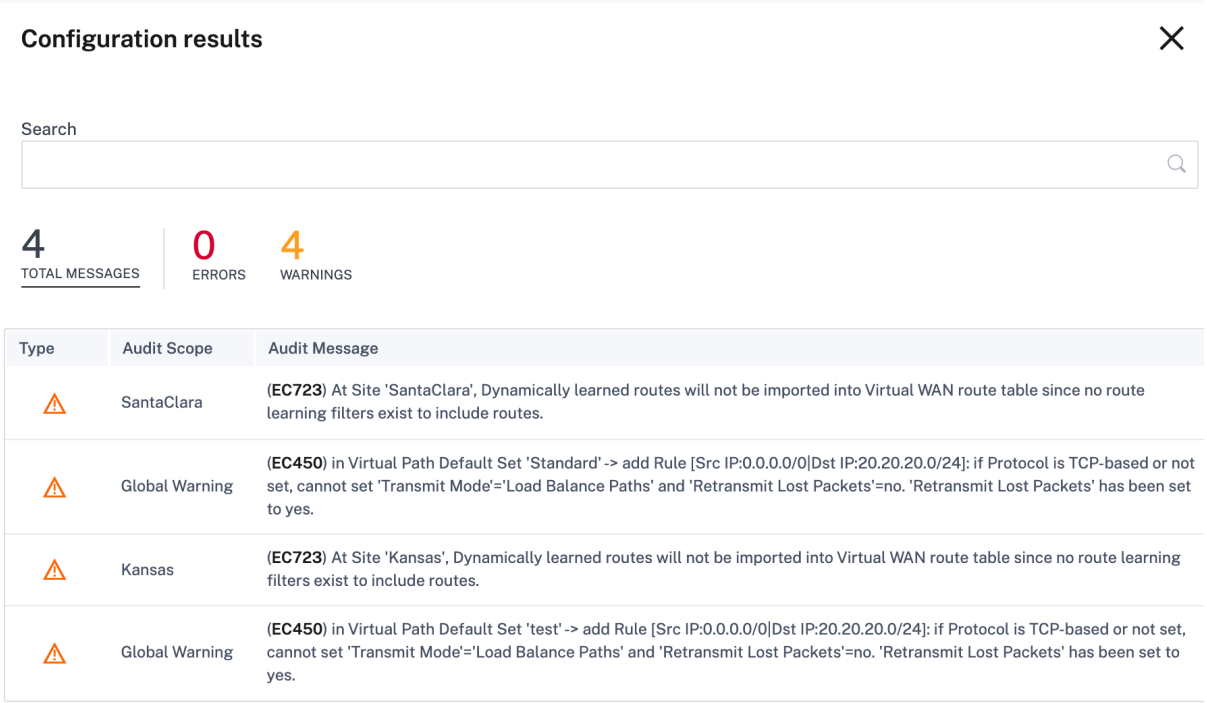
验证配置

您可以单击“验证配置”来验证网络配置并检查是否存在任何审计错误或警告。当您单击“验证配置”时，将显示“配置结果”页面。此页面包含审计错误和警告的详细信息。

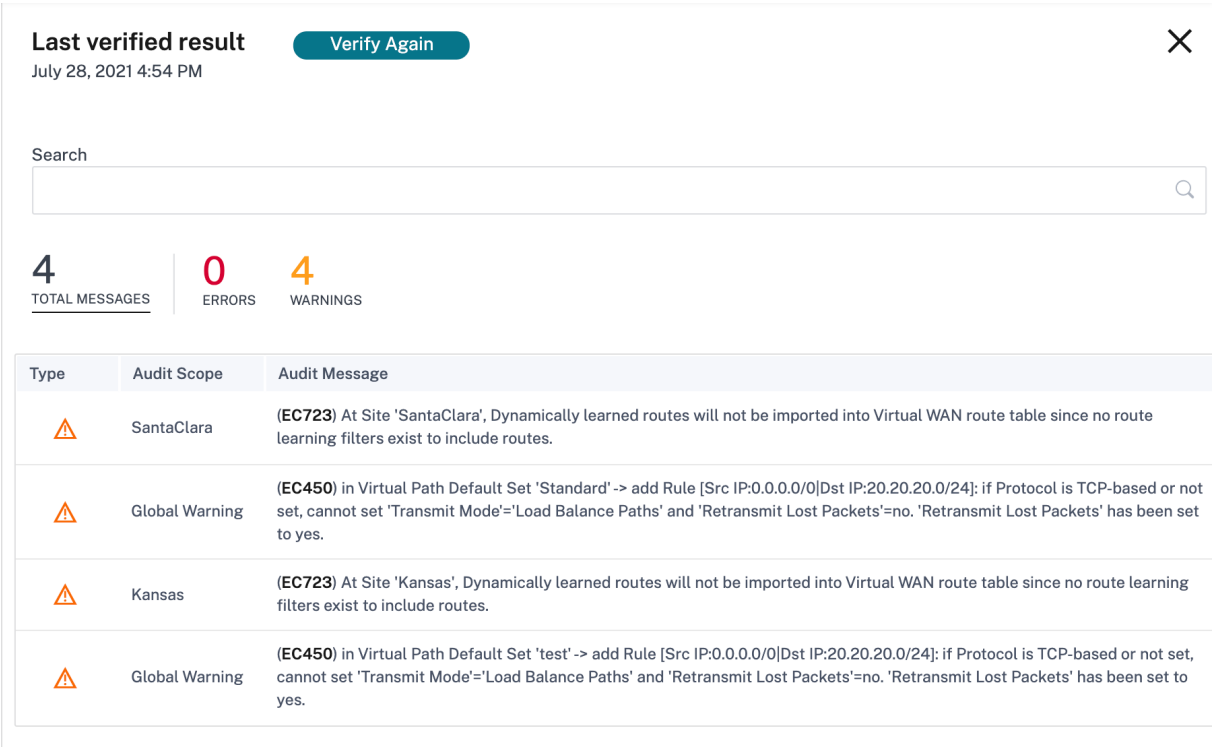
配置结果显示审计错误和警告的总数。还会根据审计类型（错误或警告）对结果进行筛选，并使用不同的颜色代码显示。您可以单击数字链接查看筛选结果。

类型 列显示一个图标以指示它是错误还是警告。审计范围 列指定错误或警告是针对站点还是网络级别。如果错误或警告是特定于某个站点的，则会显示该站点的名称。如果错误或警告位于全局级别，则分别显示 全局错误 或 全局警告。审计消息 列包含错误代码和错误消息。

您可以使用搜索栏根据类型、错误代码、站点名称或错误消息搜索任何特定的错误或警告。



当您第二次单击“验证配置”时，将打开“配置结果”页面，显示上次验证配置时的相同结果以及日期和时间戳。如有必要，可以单击“再次验 证”以重新运行验证。



服务定义

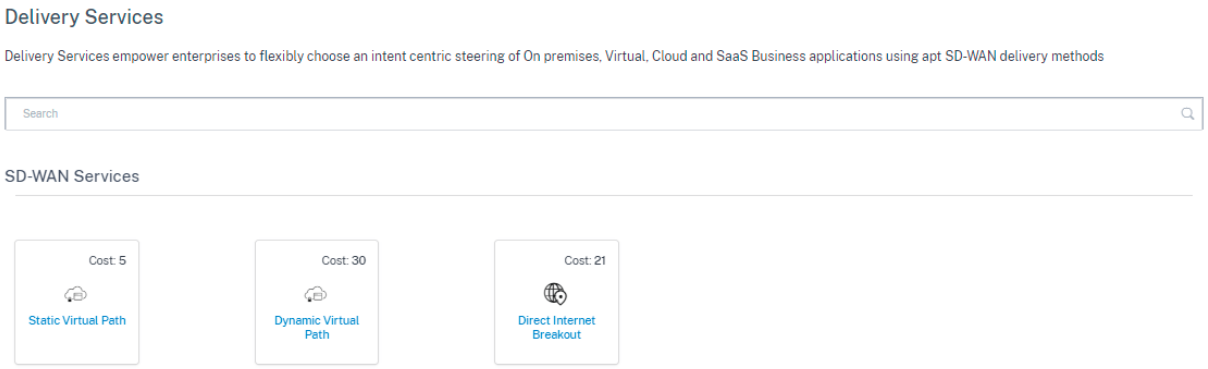
October 21, 2022

交付渠道大致分为服务定义和带宽分配。

交付服务是 Citrix SD-WAN 上可用的交付机制，用于根据业务意图使用正确的交付方法来引导不同的应用程序或流量配置文件。您可以配置传送服务，例如互联网、内联网、虚拟路径、IPsec 和 LAN GRE。交付服务在全球范围内定义，并应用于各个站点的 WAN 链接（视情况而定）。

每个 WAN 链接可以应用全部或部分相关服务，并在所有交付服务中设置带宽的相对份额 (%)。

默认情况下，虚拟路径服务在所有链接上都可用。可以根据需要添加其他服务。
要配置交付服务，请在客户级别导航到 配置 > 交付渠道 > 服务定义。

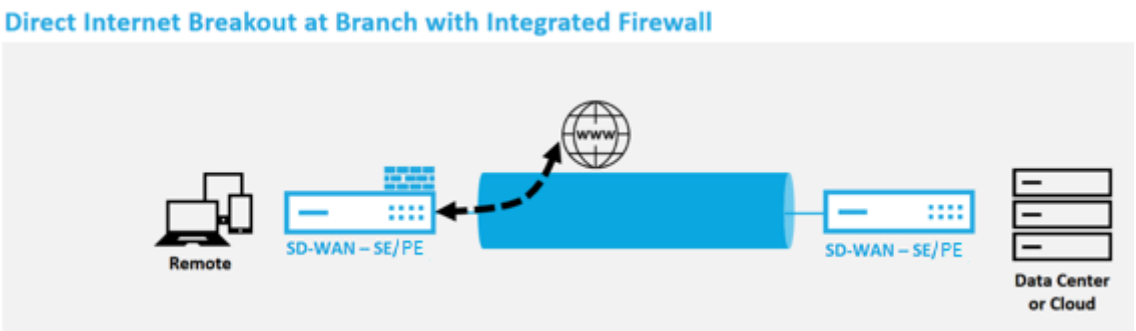


送货服务可大致归类为以下内容：

- 虚拟路径服务：双端叠加 SD-WAN 隧道，在托管 SD-WAN 设备或虚拟实例的两个站点之间提供安全、可靠和高质量的连接。以 Kbps 为单位设置每个虚拟路径的最小预留带宽。此设置应用于网络中所有站点上的所有 WAN 链接。
- 互联网服务：SD-WAN 站点和公共互联网之间的直接通道，不涉及 SD-WAN 封装。Citrix SD-WAN 支持会话负载平衡功能，用于跨多个互联网链接的互联网绑定流量。
- **Intranet** 服务：基于底层链接从 SD-WAN 站点到任何非 SD-WAN 站点的连接。流量未封装或者可以使用任何非虚拟路径封装，例如 IPsec、GRE。您可以设置多个 Intranet 服务。

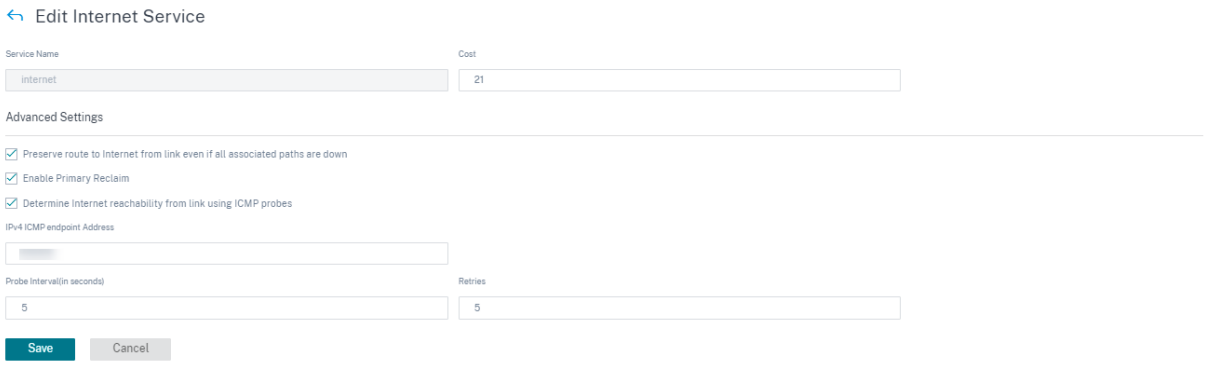
Internet 服务

默认情况下，互联网服务 作为交付服务的一部分可用。要配置 Internet 服务，请从客户级别导航到 配置 > 交付渠道 > 服务定义。在 **SD-WAN** 服务 部分中，选择 Direc **t Internet Breakout** 磁贴，然后单击“添加”。



您可以配置以下互联网服务：

- 即使所有关联路径均处于关闭状态，也可以保留从链接到互联网的路由：您可以配置相对于其他交付服务的互联网服务路径成本。使用此服务，即使所有关联路径均处于关闭状态，您也可以保留从链路到互联网的路由。如果与 WAN 链接关联的所有路径均失效，则 SD-WAN 设备使用此路由发送/接收 Internet 流量。
- 使用 **ICMP** 探测器确定链路的互联网可访问性：您可以为指向互联网上的显式服务器的特定 Internet WAN 链接启用 ICMP 探测器。使用 ICMP 探测设置时，SD-WAN 设备会在链路的成员路径启用或从服务器收到 ICMP 探测响应时将互联网链接视为已启动。
- **IPv4 ICMP** 端点地址：目标 IPv4 地址或服务器地址。
- 探测间隔（以秒为单位）：SD-WAN 设备在 Internet 配置的 WAN 链接上发送探测的时间间隔。默认情况下，SD-WAN 设备每 5 秒钟在配置的 WAN 链路上发送一次探测器。
- 重试次数：在确定 WAN 链路是否开启之前可以尝试的重试次数。在连续 3 次探测失败后，WAN 链路被视为失效。允许的最大重试次数为 10。



支持的部署模式

可以在以下部署模式下使用 Internet 服务：

- 内联部署模式（SD-WAN 覆盖）

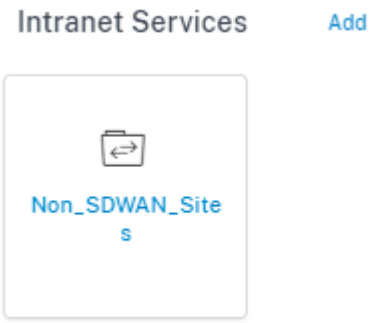
Citrix SD-WAN 可以作为覆盖解决方案部署在任何网络中。作为叠加解决方案，SD-WAN 通常部署在现有边缘路由器和/或防火墙后面。如果 SD-WAN 部署在网络防火墙后面，则可以将该接口配置为可信接口，互联网流量可以作为 Internet 网关传送到防火墙。

- 边缘或网关模式

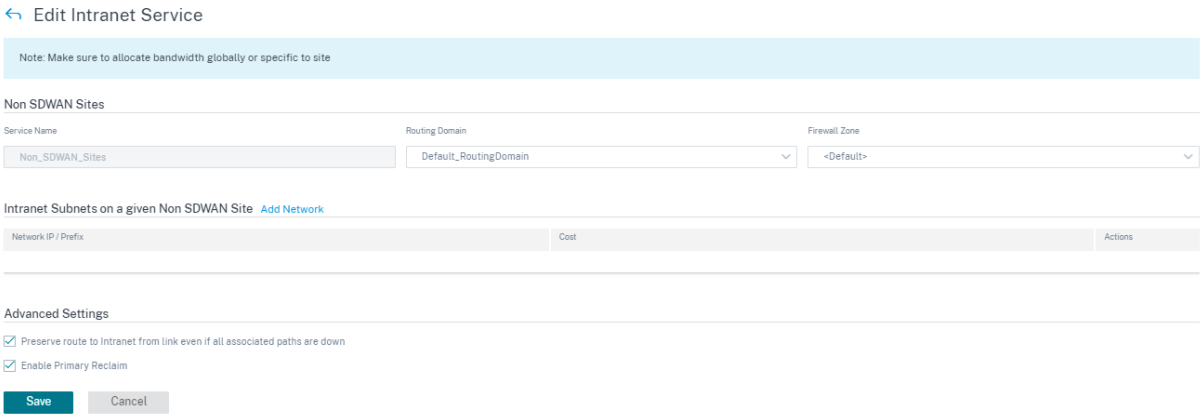
Citrix SD-WAN 可以部署为边缘设备，替换现有的边缘路由器和/或防火墙设备。板载防火墙功能允许 SD-WAN 保护网络免受直接 Internet 连接。在此模式下，连接到公用 Internet 链接的接口配置为不受信任，强制启用加密，并启用防火墙和动态 NAT 功能以保护网络。

内联网服务

您可以创建多个 Intranet 服务。要添加 Intranet 服务，请从客户级别导航到 配置 > 交付渠道 > 服务定义。在“内联网服务”部分中，单击“添加”。



在全局级别创建 Intranet 服务后，您可以在 WAN Link 级别对其进行引用。提供 服务名称，选择所需的 路由域 和 防火墙区域。添加网络中的所有 Intranet IP 地址，网络中的其他站点可能会进行交互。即使所有关联路径都已关闭，也可以保留从链接到 Intranet 的路由。

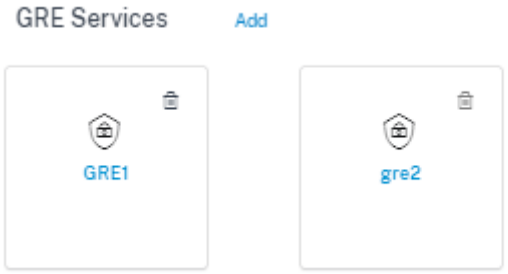


GRE 服务

您可以配置 SD-WAN 设备以终止 LAN 上的 GRE 隧道。

要添加 GRE 服务，请从客户级别导航到 配置 > 交付渠道 > 服务定义。您也可以从“配置” **>** “安全”导航到 GRE 服务配置页面。

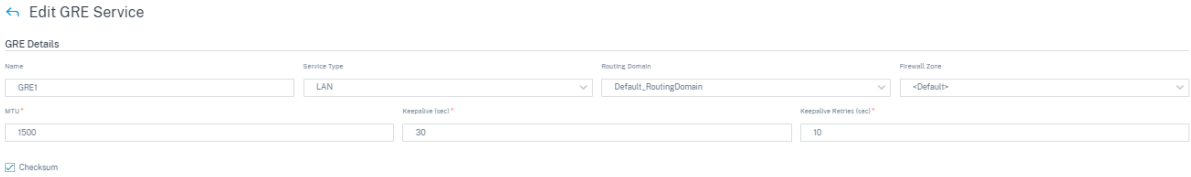
在 **IPsec** 和 **GRE** 部分中，导航到 **IPsec** 服务 并单击“添加”。



GRE 详情：

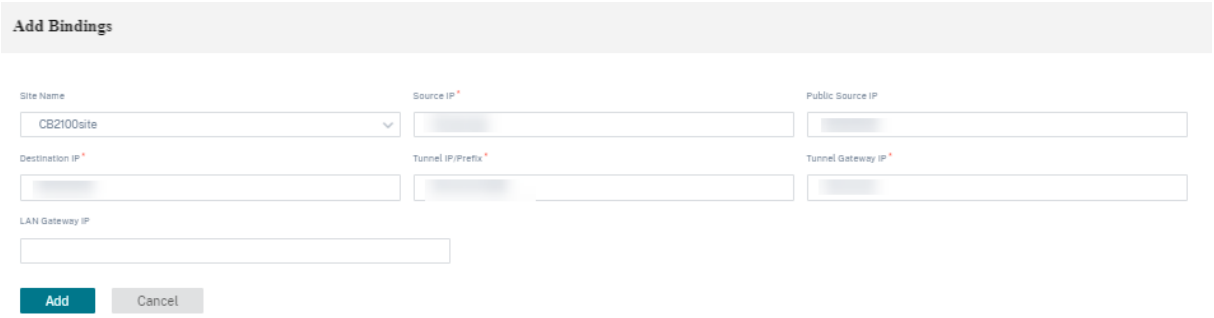
- 服务类型：选择 GRE 隧道使用的服务。

- 名称：局域网 GRE 服务的名称。
- 路由域：GRE 通道的路由域。
- 防火墙区域：为通道选择的防火墙区域。默认情况下，通道放置在 Default_LAN_Zone 中。
- **MTU**：最大传输单位-可以通过特定链路传输的最大 IP 数据报的大小。范围从 576 到 1500。默认值为 1500。
- 保持活动状态：发送保持活动状态消息之间的时间如果配置为 0，则不会发送保持活动状态的数据包，但通道保持正常运行。
- 保持活动状态重试次数：Citrix SD-WAN 设备在关闭隧道之前在没有响应的情况下发送保持活动状态数据包的次数。
- 校验和：启用或禁用隧道的 GRE 标头的校验和。



网站绑定：

- 站点名称：要映射 GRE 通道的站点。
- 源 **IP**：通道的源 IP 地址。这是在此站点配置的虚拟接口之一。选定的路由域决定了可用的源 IP 地址。
- 公用源 **IP**：通道流量通过 NAT 传输时的源 IP。
- 目标 **IP**：通道的目标 IP 地址。
- 隧道 **IP/**前缀：GRE 隧道的 IP 地址和前缀。
- 隧道网关 **IP**：用于路由隧道流量的下一跳 IP 地址。
- 局域网网关 **IP**：路由局域网流量的下一跳 IP 地址。



IPsec 服务

Citrix SD-WAN 设备可以与 LAN 或 WAN 端的第三方对等方协商固定 IPsec 通道。您可以定义隧道端点并将站点映射到隧道端点。

还可以选择并应用用于定义安全协议和 IPsec 设置的 IPsec 安全配置文件。

要配置虚拟路径 IPsec 设置，请执行以下操作：

- 为需要 FIPS 合规性的所有虚拟路径启用虚拟路径 IPsec 通道。
- 通过将 IPsec 模式更改为 AH 或 ESP+ 身份验证来配置消息身份验证，并使用 FIPS 批准的哈希函数。SHA1 被 FIPS 接受，但强烈推荐使用 SHA256。
- IPsec 生命周期应配置不超过 8 小时（28800 秒）。

Citrix SD-WAN 使用带有预共享密钥的 IKE 版本 2 使用以下设置通过虚拟路径协商 IPsec 隧道：

- 卫生署 19 组：ECP256（256 位椭圆曲线）密钥协商
- 256 位 AES-CBC 加密
- 用于消息身份验证的 SHA256 哈希
- 用于消息完整性的 SHA256 哈希
- DH 组 2：完全向前保密的 MODP-1024

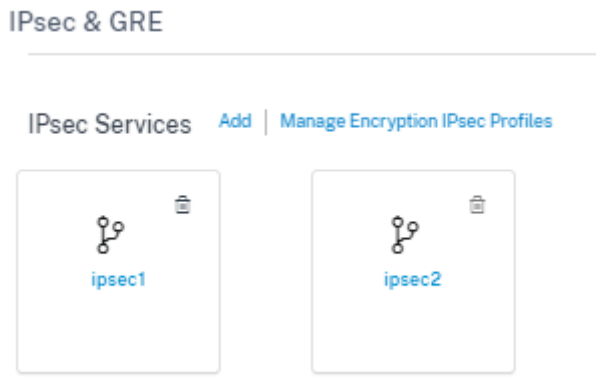
要为第三方配置 IPsec 隧道，请执行以下操作：

- 配置 FIPS 批准的 DH 组。根据 FIPS，第 2 组和第 5 组是允许的，但强烈推荐 14 组及以上组。
- 配置 FIPS 批准的哈希函数。SHA1 被 FIPS 接受，但强烈推荐使用 SHA256。
- 如果使用 IKEv2，请配置 FIPS 批准的完整性功能。SHA1 被 FIPS 接受，但强烈推荐使用 SHA256。
- 将 IKE 生命周期和最大生命周期配置为不超过 24 小时（86,400 秒）。
- 通过将 IPsec 模式更改为 AH 或 ESP+ 身份验证来配置 IPsec 消息身份验证，并使用 FIPS 批准的哈希函数。SHA1 被 FIPS 接受，但强烈推荐使用 SHA256。
- 配置 IPsec 生命周期和最长生命周期不超过 8 小时（28,800 秒）。

配置 **IPsec** 隧道

在客户层面，导航到 配置 > 交付渠道 > 服务定义。您也可以从“配置” **>** “安全”导航到 **IPSec** 服务页面。

在 **IPsec** 和 **GRE** > **IPsec** 服务 部分中，单击“添加”。屏幕上将显示 “编辑 **IPsec** 服务”页面。



1. 指定服务详细信息。

    - 服务名称：IPsec 服务的名称。
    - 服务类型：选择 IPsec 隧道使用的服务。

- 路由域：对于通过 LAN 传输的 IPsec 通道，请选择一个路由域。如果 IPsec 通道使用 intranet 服务，intranet 服务将确定路由域。
- 防火墙区域：通道的防火墙区域。默认情况下，通道放置在 Default_LAN_Zone 中。
- 启用 **ECMP**：选中“启用 **ECMP** ”复选框后，将启用 IPsec 隧道的 ECMP 负载平衡。
- **ECMP** 类型：根据需要选择 ECMP 负载平衡机制的类型。有关 ECMP 类型的更多详细信息，请参阅 ECMP 负载均衡。

2. 添加通道终结点。

   - 名称：当 服务类型 为 Intranet 时，选择隧道保护的 Intranet 服务。否则，请输入服务的名称。
   - 对等 **IP**：远程对等体的 IP 地址。
   - **IPsec** 配置文件：定义安全协议和 IPsec 设置的 IPsec 安全配置文件。
   - 预共享密钥：用于 IKE 身份验证的预共享密钥。
   - 对等体预共享密钥：用于 IKEv2 身份验证的预共享密钥。
   - 身份数据：使用手动身份或用户 FQDN 类型时用作本地身份的数据。
   - 对等体身份数据：使用手动身份或用户 FQDN 类型时用作对等体身份的数据。
   - 证书：如果选择证书作为 IKE 身份验证，请从配置的证书中进行选择。

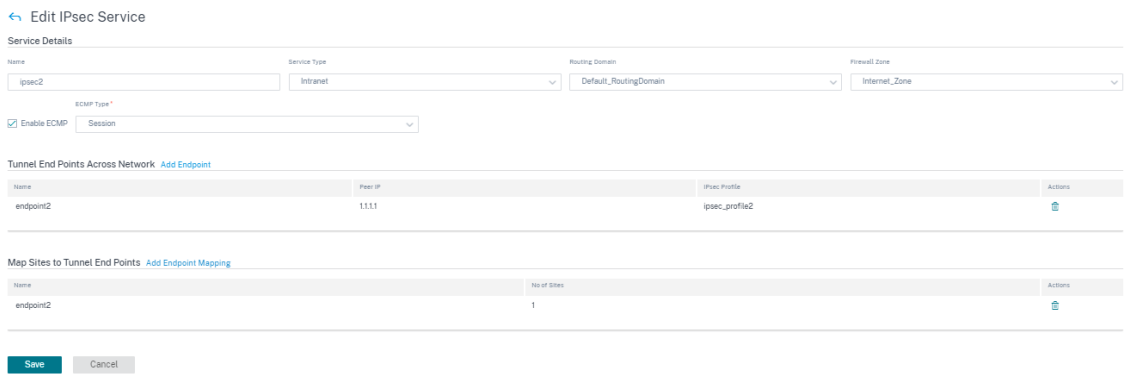
3. 将站点映射到通道端点。

   - 选择 **Endpoint**：要映射到站点的终端节点。
   - 站点名称：要映射到终端节点的站点。
   - 虚拟接口名称：站点上用作终端节点的虚拟接口。
   - 本地 **IP**：用作本地通道端点的本地虚拟 IP 地址。
   - 网关 **IP**：下一跳 IP 地址。

4. 创建受保护的网络。

   - 源网络 **IP/** 前缀：IPsec 通道保护的网络流量的源 IP 地址和前缀。
   - 目标网络 **IP/** 前缀：IPsec 通道保护的网络流量的目标 IP 地址和前缀。

5. 确保对等设备上的 IPsec 配置进行镜像。



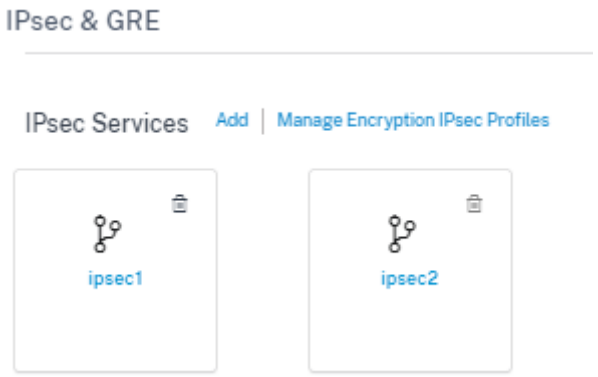
有关 FIPS 合规性的更多信息，请参阅 网络安全。

> 注意
>
> 适用于本地的 Citrix SD-WAN Orchestrator 支持通过 IPsec 连接到 Oracle 云基础设施 (OCI)。

IPsec 加密配置文件

要添加 IPsec 加密配置文件，请在客户级别导航到 配置 > 交付渠道 > 服务定义。您也可以从“配置” **>** “安全”导航到 **IPsec** 加密配置文件配置页面。

在 **IPsec** 和 **GRE** 部分中，选择 管理加密 **IPsec** 配置文件。



IPsec 提供安全通道。Citrix SD-WAN 支持 IPsec 虚拟路径，使第三方设备能够终止 Citrix SD-WAN 设备的局域网或广域网端的 IPsec VPN 通道。可以使用 140-2 Level 1 FIPS 认证的 IPsec 加密二进制文件保护在 SD-WAN 设备上终止的站点到站点 IPsec 通道。

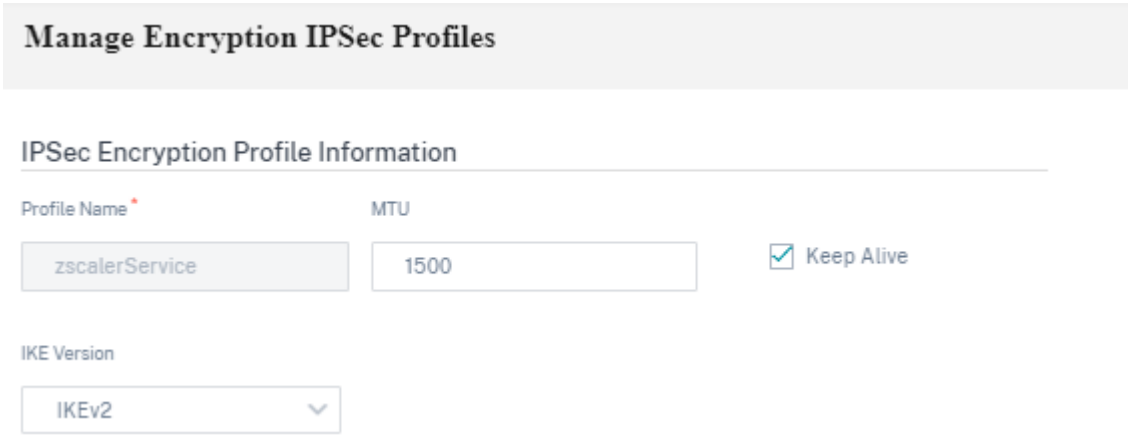
Citrix SD-WAN 还支持使用存在差别的虚拟路径通道机制的弹性 IPsec 通道。

在将 IPsec 服务配置为交付服务集时，将使用 IPsec 配置文件。在 IPsec 安全配置文件页面中，输入以下 **IPsec** 加密配置文件、**IKE** 设置 和 **IPsec** 设置的所需值。

单击“验证配置”以验证任何审计错误。

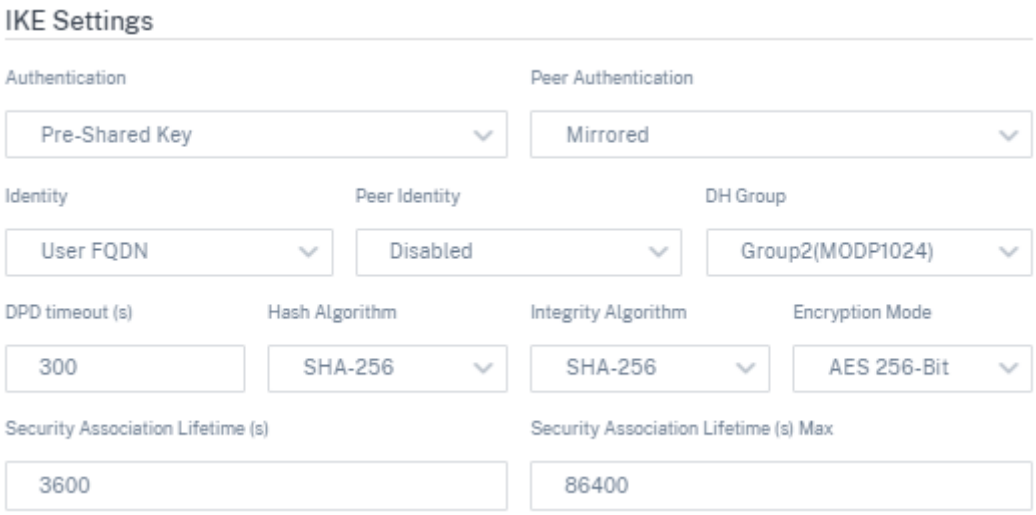
IPsec 加密配置文件信息：

- 配置文件名称：提供配置文件名称。
- **MTU**：输入最大的 IKE 或 IPsec 数据包大小（以字节为单位）。
- 保持活动状态：选中该复选框可使隧道保持活动状态并启用路径资格。
- **IKE** 版本：从下拉列表中选择 IKE 协议版本。



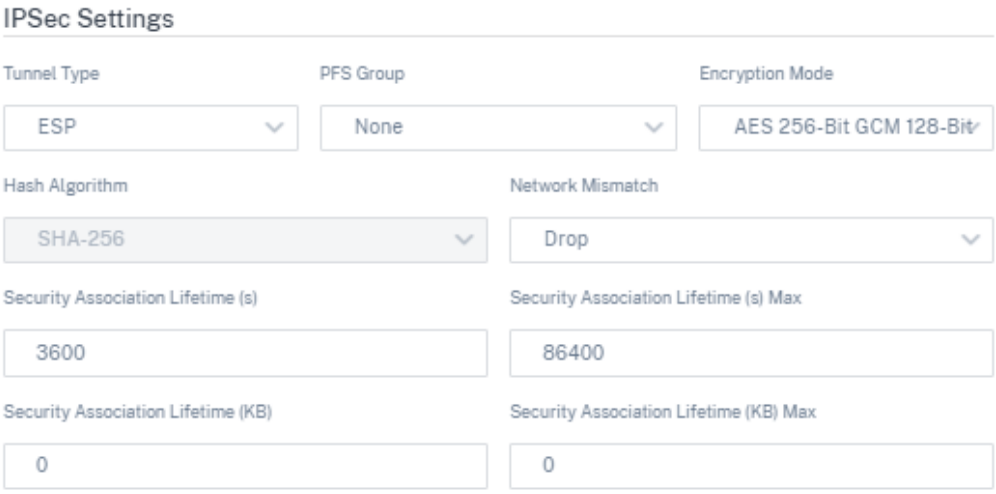
IKE 设置

- 模式：从 IKE 第 1 阶段协商模式的下拉列表中选择“主模式”或“主动模式”。
  - 主模式：协商期间不会向潜在攻击者泄露任何信息，但是速度低于积极模式。主 模式符合 FIPS 标准。
  - 主动: 协商期间向潜在攻击者泄露某些信息 (例如，协商对等体的身份)，但是速度高于主模式。主动 模式不兼容 FIPS。
- 身份验证：从下拉菜单中选择身份验证类型为“证书”或“预共享密钥”。
- 对等身份验证：从下拉列表中选择对等身份验证类型。
- 身份：从下拉列表中选择身份方法。
- 对等身份：从下拉列表中选择对等身份方法。
- **DH** 组：选择可用于 IKE 密钥生成的 Diffie-Hellman (DH) 组。
- **DPD** 超时：输入 VPN 连接的失效对等体检测超时（以秒为单位）。
- 哈希算法：从下拉列表中选择哈希算法以验证 IKE 消息。
- 完整性算法：选择用于 HMAC 验证的 IKEv2 哈希算法。
- 加密模式：从下拉列表中选择 IKE 消息的加密模式。
- 安全关联有效期：输入 **IKE** 安全关联存在的时间量（以秒为单位）。
- 安全关联最大有效期：输入允许 **IKE** 安全关联存在的最大时间（以秒为单位）。



IPsec 设置

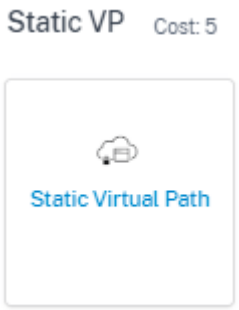
- 隧道类型：从下拉列表中选择 **ESP**、**ESP+AUTH**、**ESP+NULL** 或 **AH** 作为隧道封装类型。这些分类归入符合 FIPS 标准和不符合 FIPS 标准的类别。
  - **ESP**：仅加密用户数据
  - **ESP+Auth**：加密用户数据并包含 HMAC
  - **ESP+NULL**：数据包经过身份验证但未加密
  - 啊：只包含 HMAC
- **PFS** 组：从下拉菜单中选择 Diffie-Hellman 组以用于完美的前向保密密钥生成。
- 加密模式：从下拉菜单中选择 IPsec 消息的加密模式。
- 哈希算法：MD5、SHA1 和 SHA-256 哈希算法可用于 HMAC 验证。
- 网络不匹配：从下拉菜单中选择数据包与 IPsec 隧道的受保护网络不匹配时要采取的操作。
- 安全关联有效期：输入 IPsec 安全关联存在的时间量（以秒为单位）。
- 安全关联最大有效期：输入允许 IPsec 安全关联存在的最大时间（以秒为单位）。
- 安全关联寿命 **(KB)**：输入 IPsec 安全关联存在的数据量（以千字节为单位）。
- 安全关联生命周期 **(KB)** 最大值：输入允许 IPsec 安全关联存在的最大数据量（以千字节为单位）。



静态虚拟路径

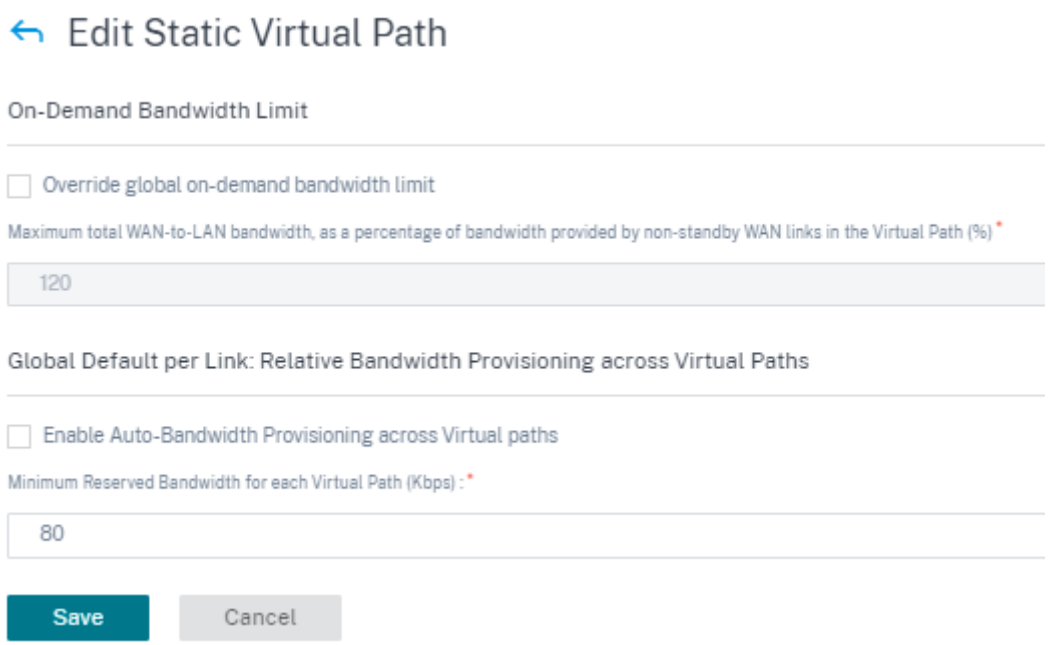
虚拟路径设置继承自全局 WAN 链接自动路径设置。您可以覆盖这些配置，然后添加或删除成员路径。您还可以根据站点和应用的 QoS 配置文件过滤虚拟路径。为 WAN 链接指定一个跟踪 IP 地址，该地址可以通过 Ping 来确定 WAN 链路的状态。您还可以为反向路径指定反向跟踪 IP，该 IP 可以通过 Ping 来确定反向路径的状态。

要配置静态虚拟路径，请从客户级别导航到 配置 > 交付通道，然后单击 静态虚拟路径 磁贴。



以下是一些支持的设置：

- 按需带宽列表：
  - 覆盖全局按需带宽限制：启用后，全局带宽限制值将替换为特定于站点的值。
  - **WAN** 到 **LAN** 的最大总带宽，占虚拟路径中非待机 **WAN** 链路提供的带宽的百分比 **(%)**：更新最大带宽限制，以百分比为单位。
- 每条链路的全局默认值：虚拟路径间的相对带宽 **Provis**ioning：
  - 启用虚拟路径间的自动带宽 **Pro**visioning：启用后，将根据远程站点消耗的带宽量自动计算和应用所有服务的带宽。
  - 每条虚拟路径的最小预留带宽 **(Kbps)**：专为每个 WAN 链路上的每项服务预留的最大带宽。

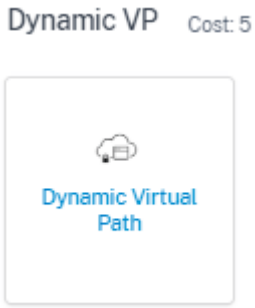


动态虚拟路径设置

全局动态虚拟路径设置允许管理员在网络上配置动态虚拟路径默认值。

动态虚拟路径在两个站点之间动态实例化，以实现直接通信，无需任何中间 SD-WAN 节点跳跃。同样，动态虚拟路径连接也被动态删除。动态虚拟路径的创建和删除都会根据带宽阈值和时间设置触发。

要配置动态虚拟路径，请从客户级别导航到 配置 > 交付渠道 > 服务定义，然后单击 动态虚拟路径 磁贴。



以下是一些支持的设置：

- 配置以启用或禁用网络上的动态虚拟路径
- 动态虚拟路径的路径成本
- 要使用的 QoS 配置文件-默认为 标准。
- 动态虚拟路径创建标准：

  - 测量间隔（秒）：测量数据包数量和带宽以确定是否必须在两个站点之间（在本例中为给定分支和控制节点之间）创建动态虚拟路径的时间长度。
  - 吞吐量阈值 **(kbps)**：两个站点之间的总吞吐量阈值，在 测量间隔内测量，在此时触发动态虚拟路径。在这种情况下，阈值适用于控制节点。
  - 吞吐量阈值 **(pps)** -在触发动态虚拟路径的 测量间隔内测量的两个站点之间的总吞吐量阈值。

- 动态虚拟路径删除标准：

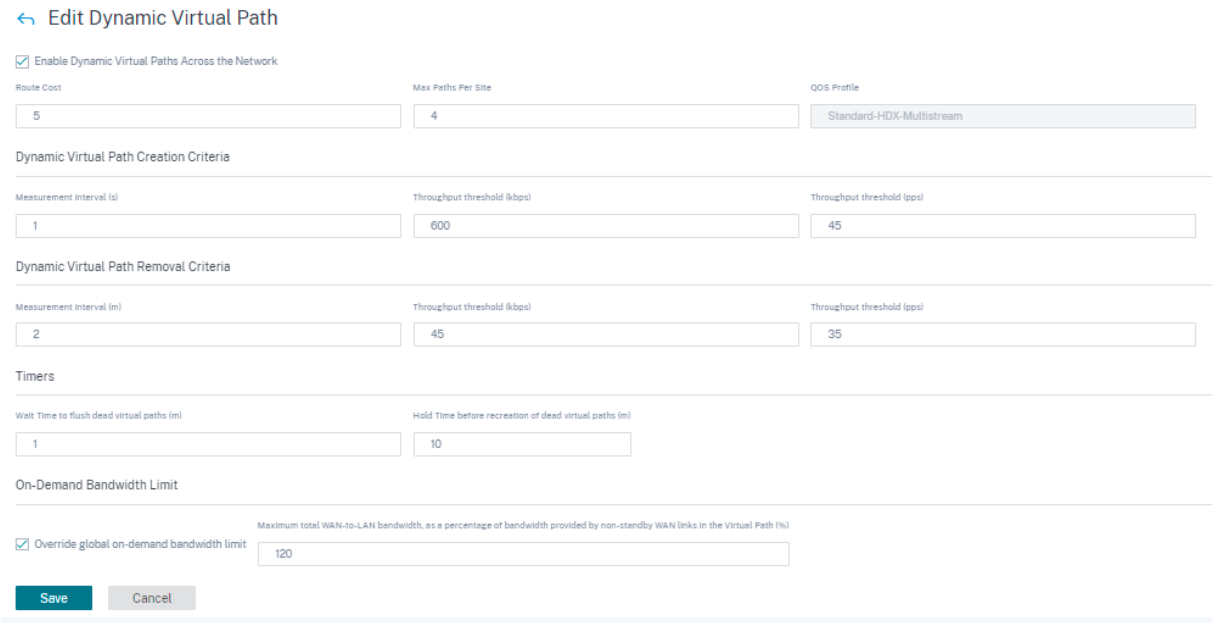
  - 测量间隔（分钟）：测量数据包数量和带宽以确定是否必须删除两个站点之间（在本例中为给定分支和控制节点之间）的动态虚拟路径所花费的时间量。
  - 吞吐量阈值 **(kbps)** -两个站点之间的总吞吐量阈值，在 测量间隔内测量，在此时动态虚拟路径将被删除。
  - 吞吐量阈值 **(pps)** -两个站点之间的总吞吐量阈值，在 测量间隔内测量，在此时动态虚拟路径将被删除。

- 计时器

  - 等待清空失效虚拟路径的时间 **(m)**：移除 DEAD 动态虚拟路径的时间。
  - 在重新创建 @@ 失效虚拟路径之前的等待时间 **(m)**：在此时间之后可以重新创建因失效而移除的动态虚拟路径。

- 按需带宽列表

  - 覆盖全局按需带宽限制：启用后，全局带宽限制值将替换为特定于站点的值。
  - **WAN** 到 **LAN** 的最大总带宽，占虚拟路径中非待机 **WAN** 链路提供的带宽的百分比 **(%)**：更新最大带宽限制，以百分比为单位。



单击“验证配置”以验证任何审计错误。

路由

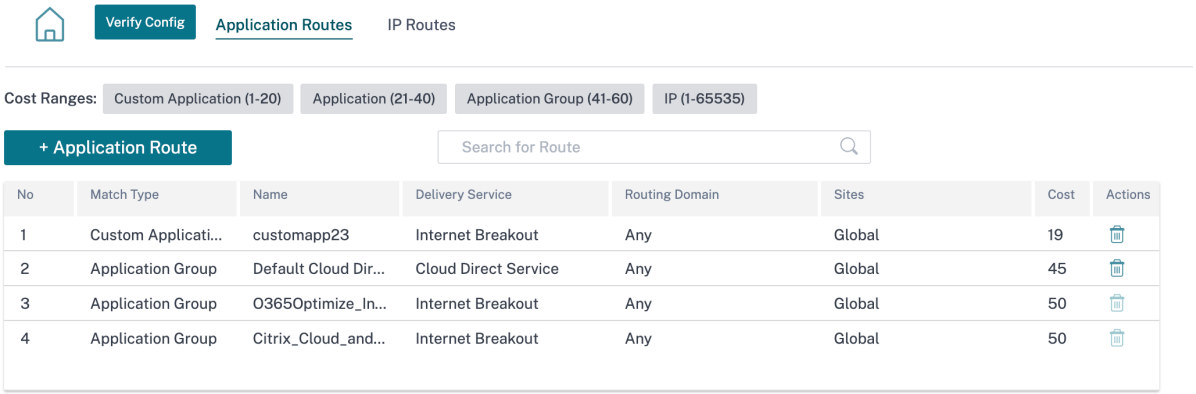
October 21, 2022

路由 部分提供以下选项：

- 路由策略
- 路由汇总
- 路由域
- 导入路由配置文件
- 导出路由配置文件
- 交通节点

路由策略

路由策略有助于启用交通指导。根据选择（应用程序路由和 IP 路由），您可以使用不同的方式来引导流量。



应用程序路由

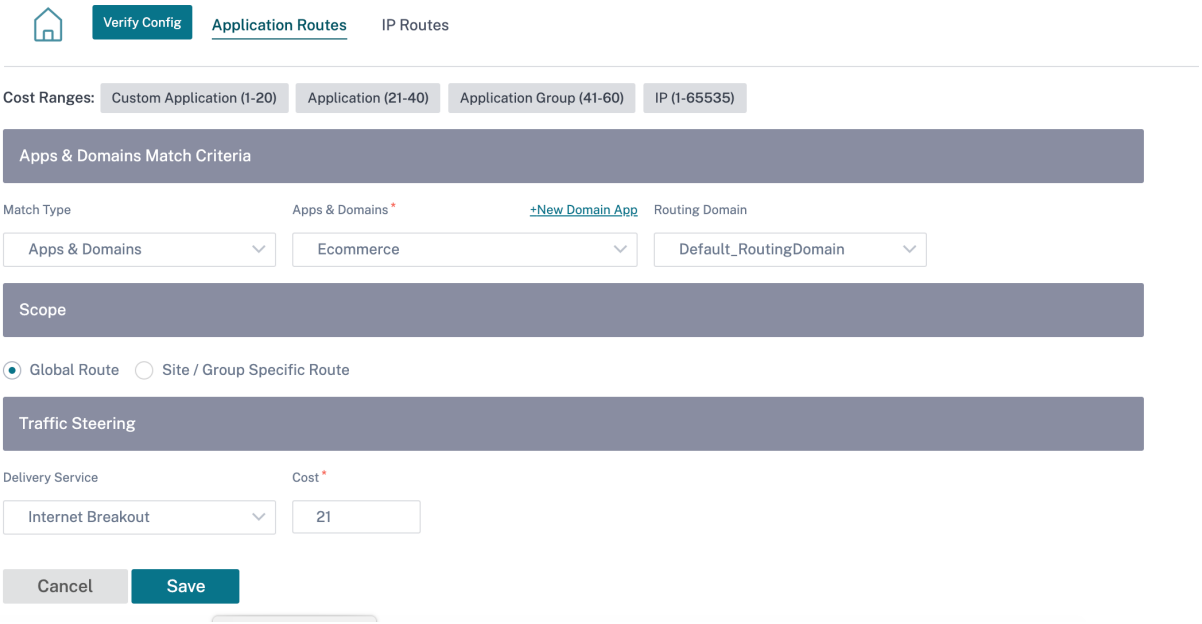
单击 **+** 应用程序路由，创建应用程序路由。

- 自定义应用程序匹配标准：
  - 匹配类型：从下拉列表中选择匹配类型为“应用程序/自定义应用程序/应用程序组”。
  - 应用程序：从列表中选择一个应用程序。
  - 路由域：选择路由域。
- 范围：您可以在全局级别或站点和组特定级别确定应用程序路由的范围。
- 交通引导；

  - 配送服务：从列表中选择一项配送服务。
  - 成本：反映每条路径的相对优先级。成本降低，优先级越高。

- 基于路径的资格：

  - 添加路径：选择站点和 WAN 链接。如果选择的路径出现故障，则应用程序路由不会接收任何流量。

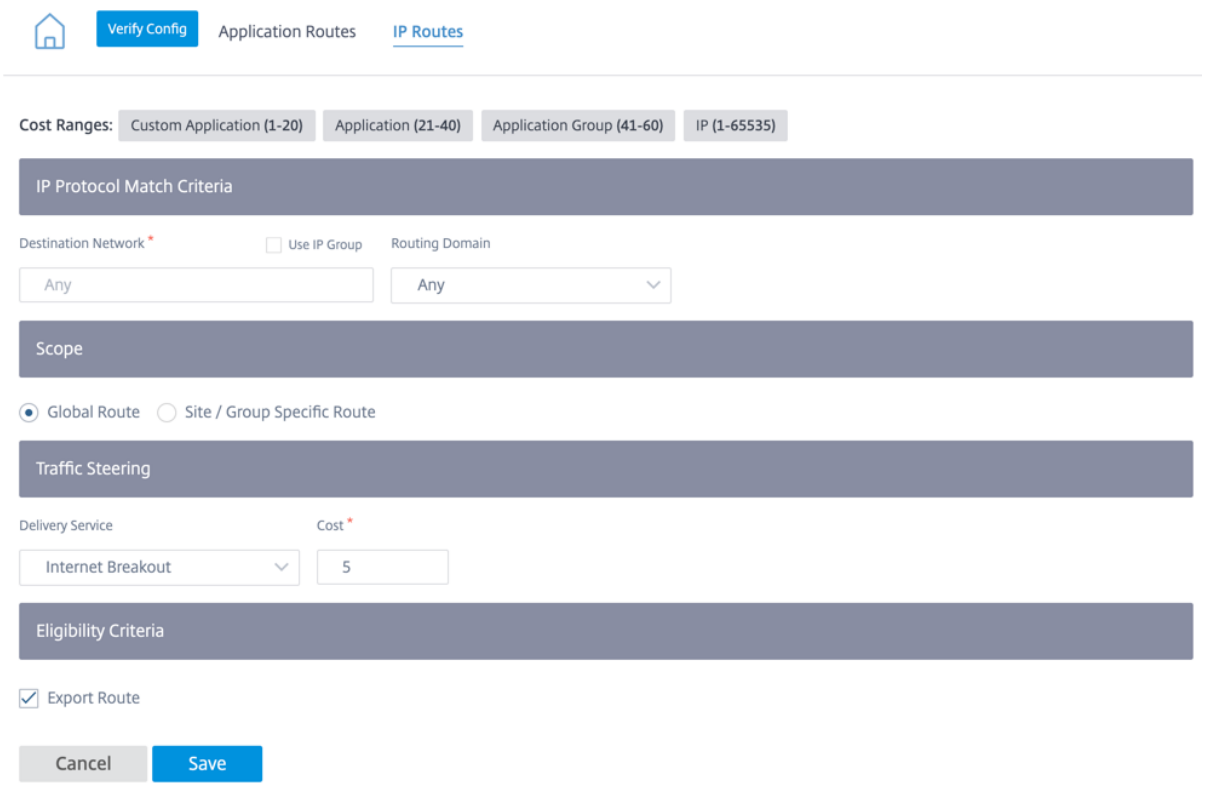


如果添加了新的应用程序路由，则路由成本必须在以下范围内：

- 自定义应用程序：1—20
- 应用程序：21—40
- 应用程序组：41—60

IP 路线

转到 **IP** 路由 选项卡，然后单击 **+ IP** 路由 到 IP 路由策略以引导流量。



- **IP** 协议匹配标准：
  - 目标网络：添加有助于转发数据包的目标网络。
  - 使用 **IP** 组：您可以添加目标网络或启用“使用 **IP** 组”复选框以从下拉列表中选择任何 IP 组。
  - 路由域：从下拉列表中选择一个路由域。
- 范围：您可以在全局级别或站点和组特定级别上确定 IP 路由的范围。
- 交通引导：
  - 配送服务：从下拉列表中选择一项配送服务。
  - 成本：反映每条路径的相对优先级。成本降低，优先级越高。

  如果添加了新的 IP 路由，则路由开销必须在 1—20 范围内。
- 资格标准：
  - 导出路径：如果选中“导出路径”复选框并且该路径是本地路径，则默认情况下该路径符合导出条件。如果路由是基于 INTRANET/INTERNET 的路由，则必须启用 WAN 到 WAN 转发才能导出。如果清除“导出路径”复选框，则本地路径不符合导出到其他 SD-WAN 的条件，并且具有本地意义。
- 基于路径的资格：
  - 添加路径：选择站点和 WAN 链接。如果添加的路径出现故障，则 IP 路由不会接收任何流量。

单击“验证配置”以验证任何审计错误。

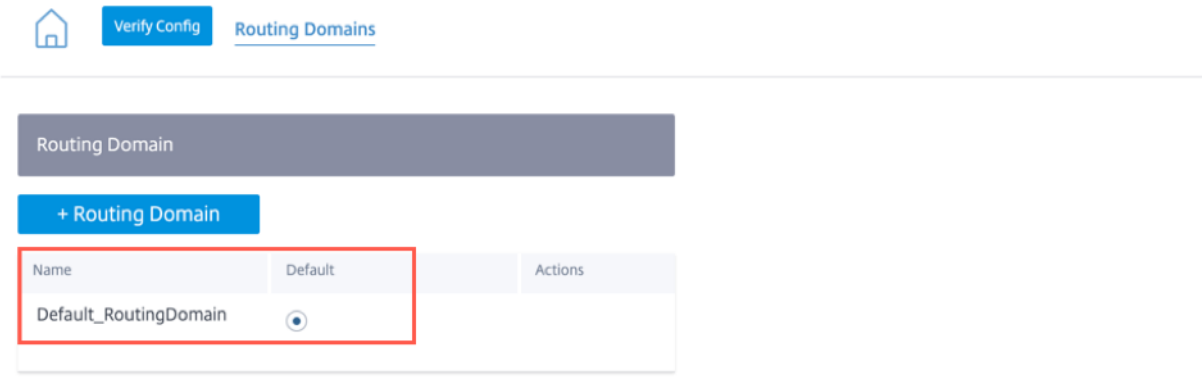
路由汇总

路由汇总减少路由器必须维护的路由数。汇总路径是用于表示多个路径的单个路径。它通过发送单个路由公告来节省带宽，从而减少路由器之间的链接数量。它可以节省内存，因为只保留一个路由地址。通过避免递归查找，CPU 资源可以更有效地使用。无需指定网关 IP 地址即可添加汇总路由。

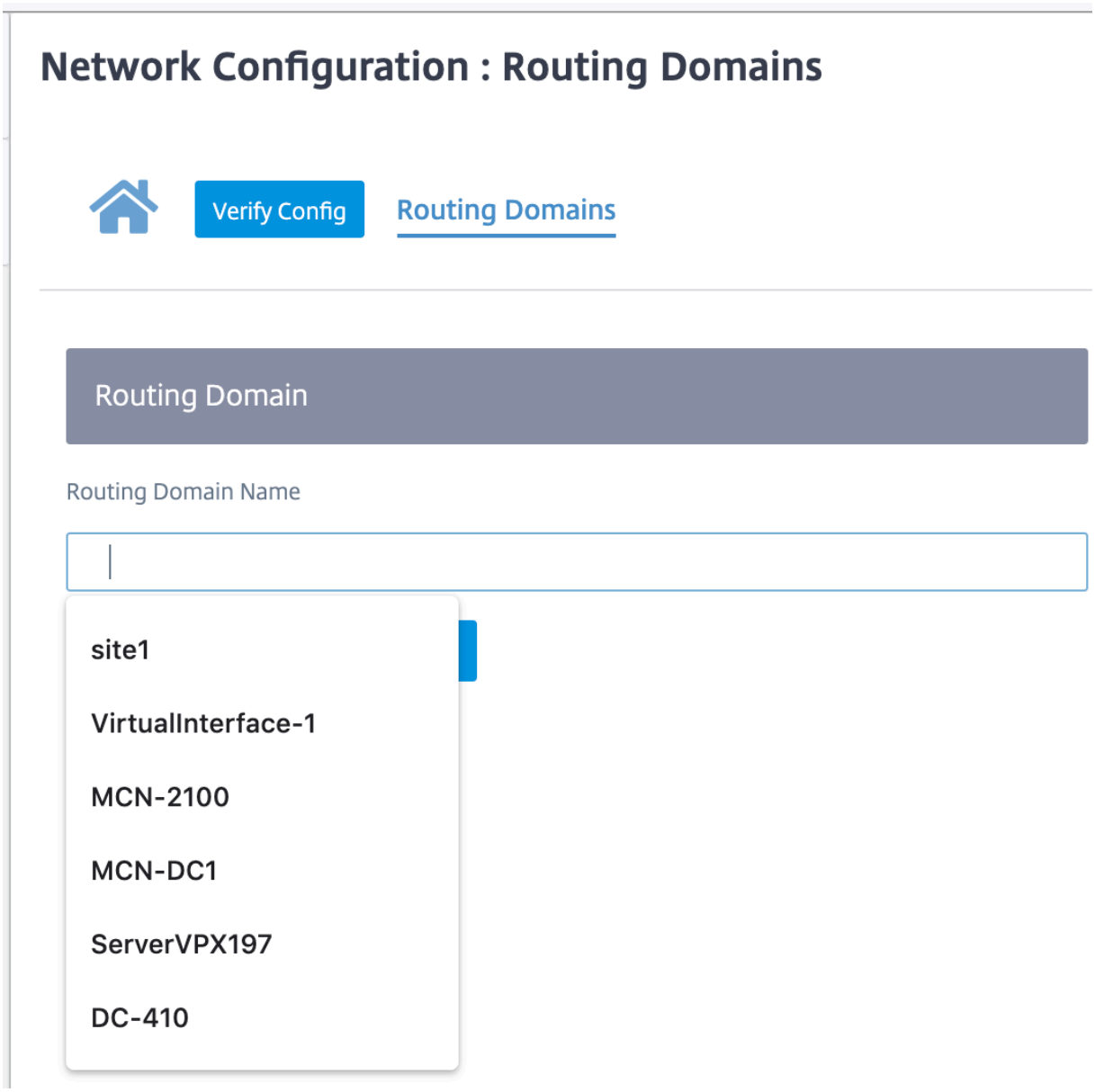
路由域

路由域 用于隔离通过 VLAN 的流量。创建路由域后，您可以在全局级别（针对 Intranet 服务）或接口级别引用它们。

您也可以选择适用于所有站点的默认路由域。



要匹配来自特定路由域的路由，请单击 **+** 路由域，然后从下拉列表中选择一个已配置的路由域。单击保存。



单击“验证配置”以验证任何审计错误。

有关更多信息，请参阅 路由域。

路由间域服务

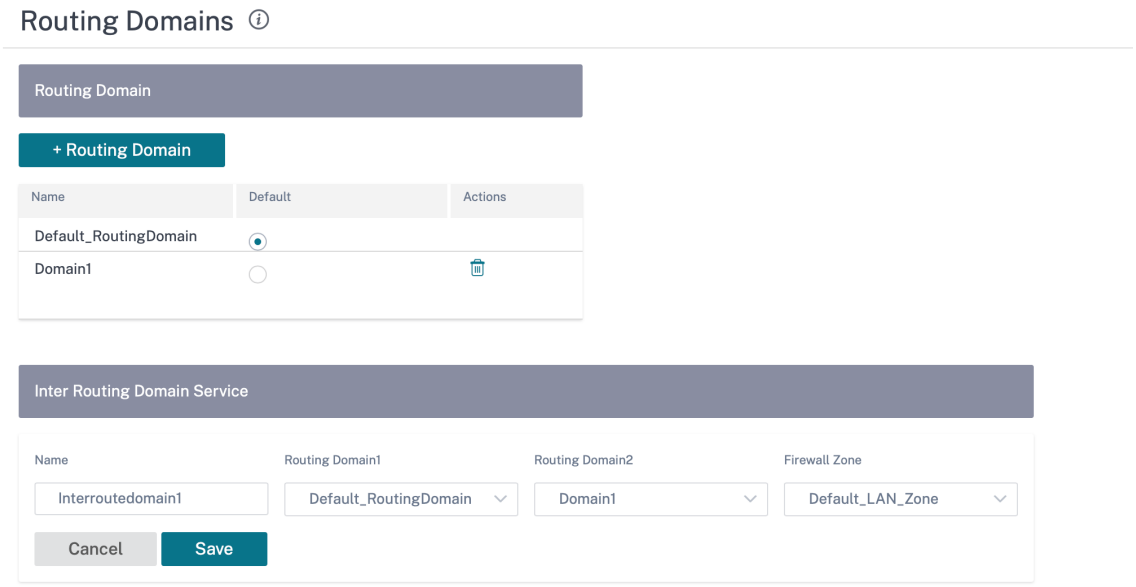
适用于本地的 Citrix SD-WAN Orchestrator 提供静态路由间域服务，允许在站点内的路由域之间或不同站点之间的路由泄露。这样就不需要边缘路由器来处理路由泄漏。Inter-VRF 路由服务可以进一步用于设置路由、防火墙策略和 NAT 规则。

有关更多信息，请参阅 路由间域服务。

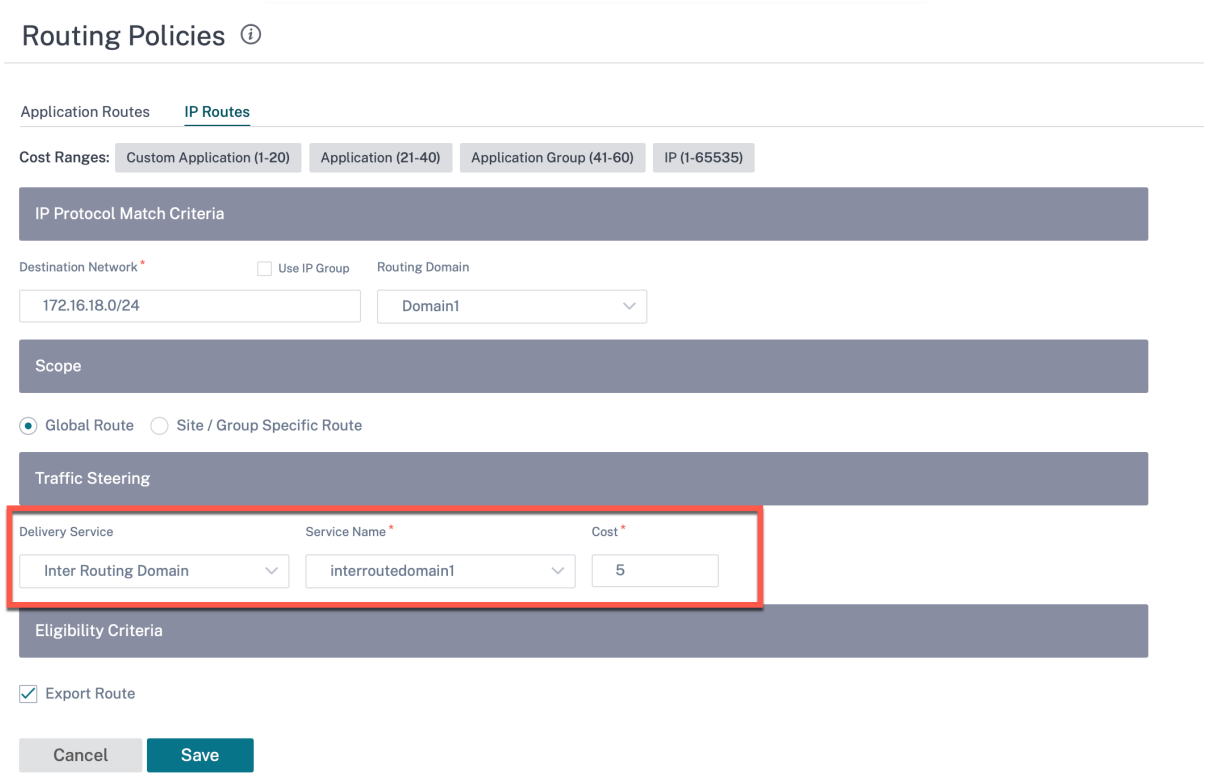
要通过 Citrix SD-WAN Orchestrator 为本地配置路由间域服务，请执行以下操作：

1. 在网络级别，导航到 配置 > 路由 > 路由域 > 路由域间服务。
2. 单击 **+** 路由间域，然后输入以下参数的值：

- 名称：路由间域服务的名称。
- 路由域 **1**：对的第一个路由域。
- 路由域 **2**：对的第二个路由域。
- 防火墙区域：服务的防火墙区域。
  - 默认：已分配 **Inter_Routing_Domain_Z** one 防火墙区域。
  - 无：该服务的行为类似于管道，它没有区域并维护数据包的原始区域。
  - 可能会选择网络中配置的所有区域。

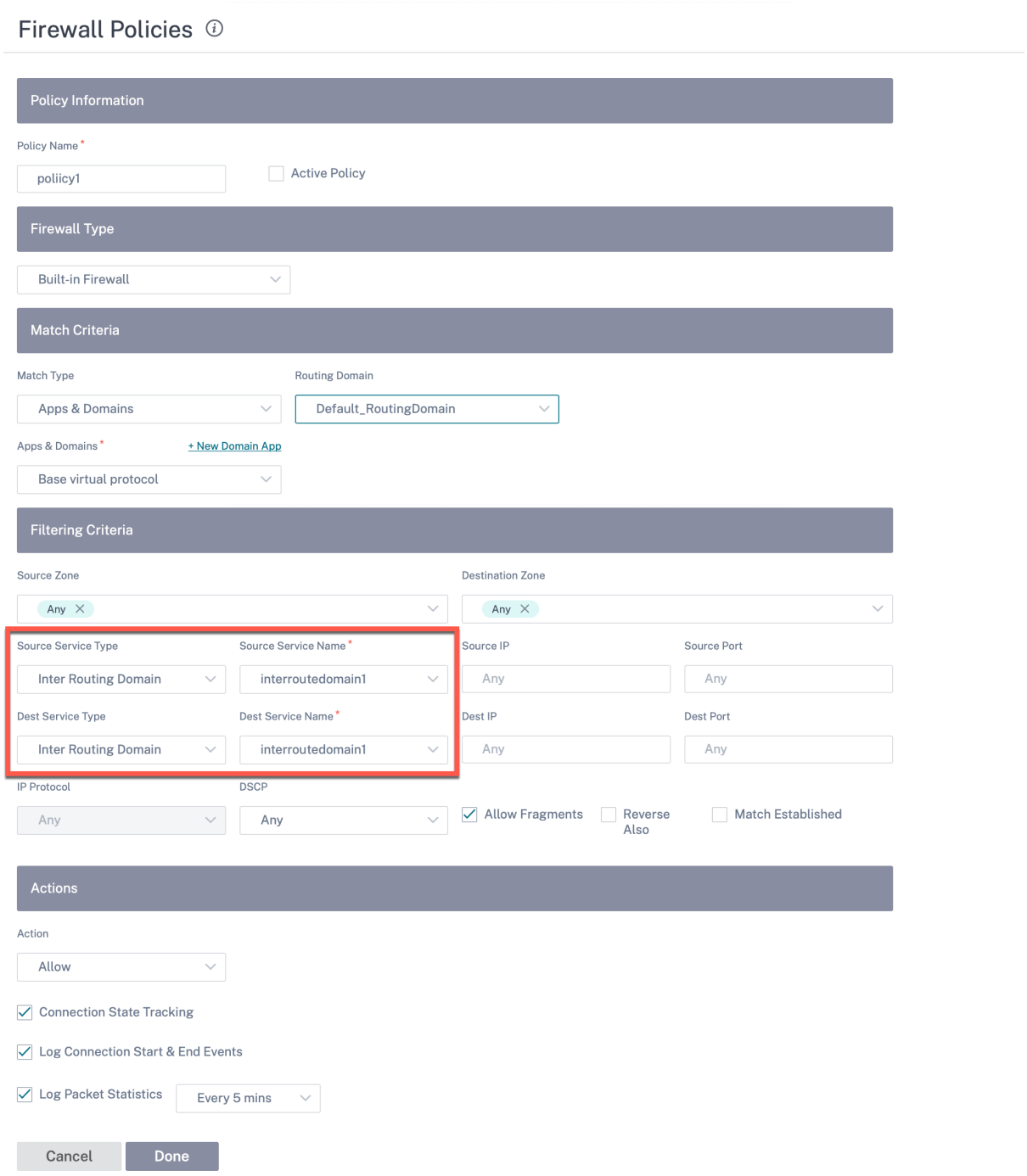


要使用路由间域服务创建路由，请创建一个服务类型为路由间域服务的路由，然后选择路由间域服务。有关配置路由的更多信息，请参阅 路由策略。



同时添加来自其他路由域对的路由，以建立与两个路由域之间的连接。

您还可以配置防火墙策略来控制路由域之间的流量。在防火墙策略中，为源服务和目标服务选择路由间域服务，然后选择所需的防火墙操作。有关配置防火墙策略的信息，请参阅 防火墙策略。

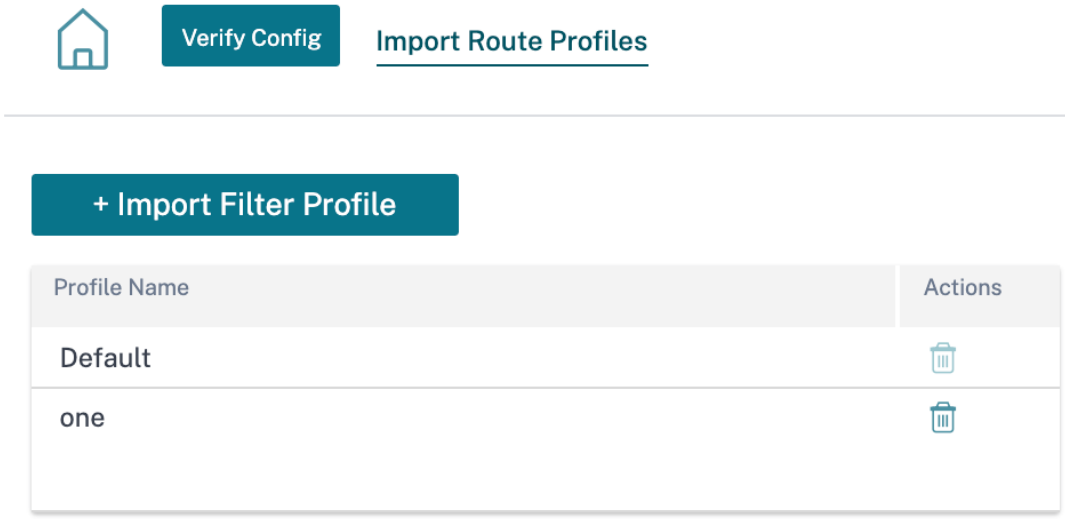


您还可以选择 Intranet 服务类型来配置静态和动态 NAT 策略。有关配置 NAT 策略的更多信息，请参阅 网络地址转换。

导入路径配置文件

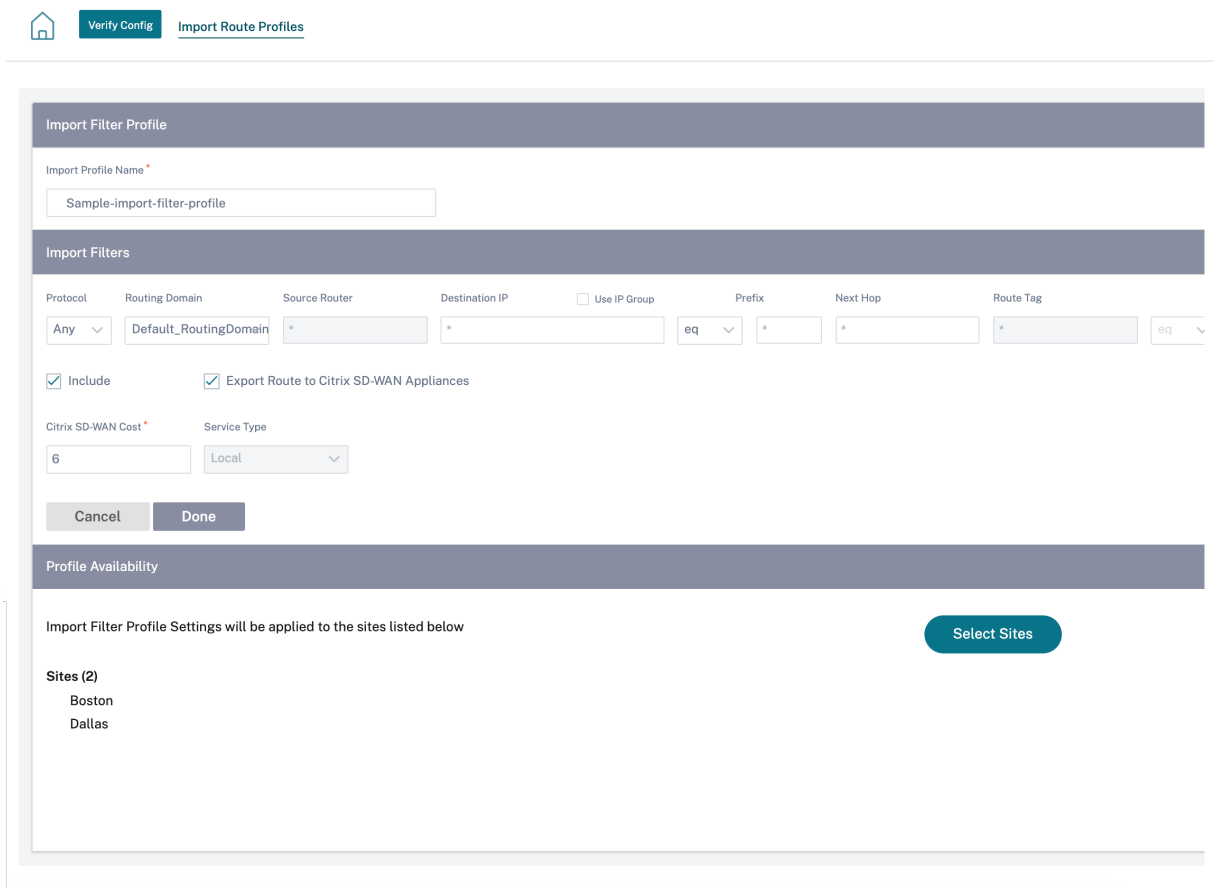
您可以配置过滤器来微调路由学习的进行方式。

导入筛选规则是将动态路由导入 SD-WAN 路由数据库之前必须满足的规则。默认情况下，不导入路由。



添加 导入筛选器配置文件，其中包含“导入配置文件名称”、“配置文件可用性”和“导入筛选器”以及以下字段：

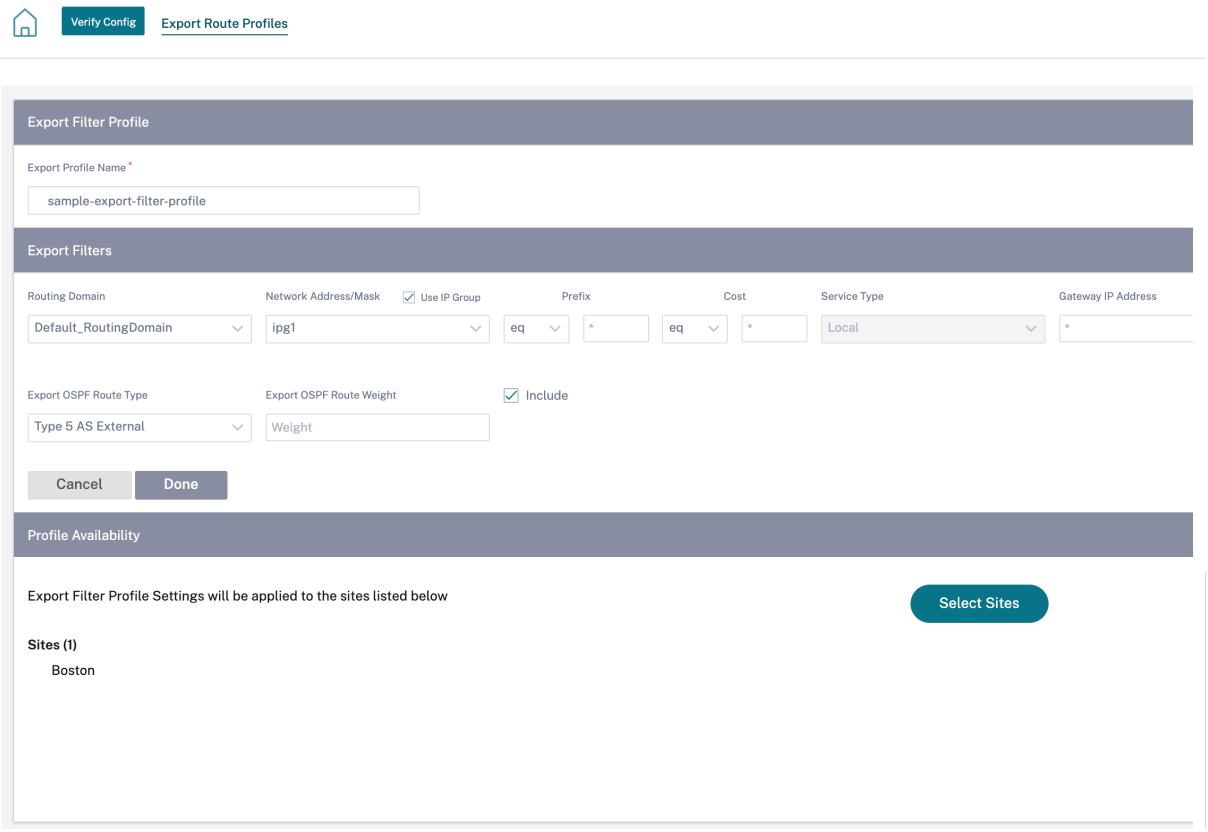
- 协议 -从列表中选择协议。
- 路由域 -要匹配来自特定路由域的路由，请从列表中选择一个已配置的路由域。
- 源路由器 -输入描述路由网络的已配置网络对象的 IP 地址和网络掩码。
- 目标 **IP** -输入目标 IP 地址。
- 前缀 -要按前缀匹配路由，请从列表中选择一个匹配谓词，然后在相邻字段中输入路由前缀。
- 下一跳 -输入下一跳目的地。
- 路线标签 -填写路线标签。
- 成本 -用于缩小导出路由选择范围的方法（谓词）和 SD-WAN 路由成本。



单击“验证配置”以验证任何审计错误。

导出路径配置文件

定义通过动态路由协议通告 SD-WAN 路由时必须满足的规则。默认情况下，所有路由都会通告给对等方。



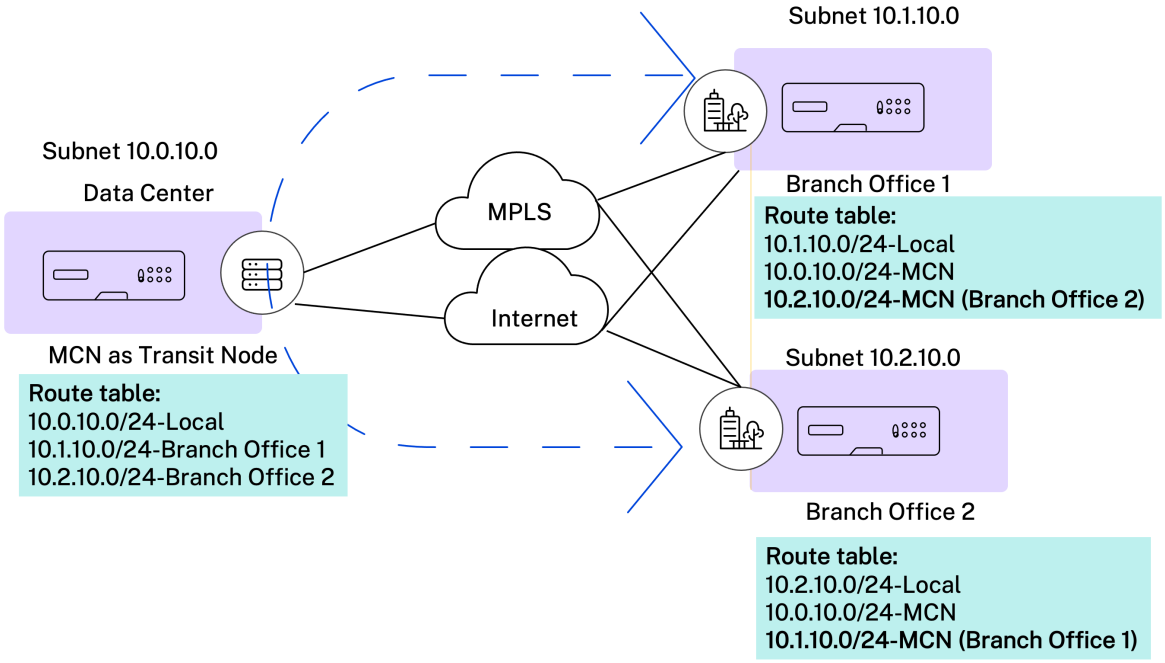
单击“验证配置”以验证任何审计错误。

中转节点

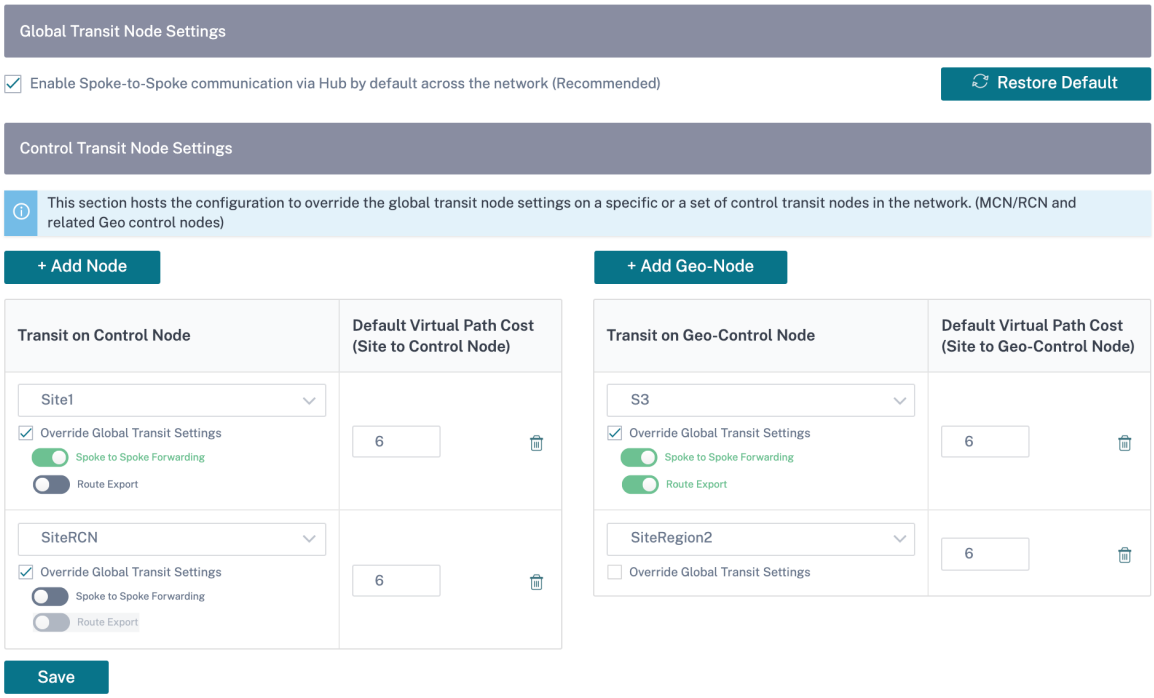
虚拟叠加中转节点

交通节点是能够在区域内一个或多个分支之间转发流量的站点。

通过调整路径成本，可以影响两个节点之间的流量选择中转节点作为中间跳点。中转节点用于将数据路由到不相邻的节点。例如，如果在 A-B-C 系列中连接了三个节点，则从 A 到 C 的数据可以通过 B 路由。您可以在 Citrix SD-WAN Orchestrator 服务中指定传输节点和要通过传输节点路由的站点。虚拟路径按成本的升序选择。降低成本，优先级越高。



默认全局虚拟叠加交通节点　您可以指定控制节点 (MCN/RCN) 和地理控制节点 (Geo-MCN/RCN) 作为网络中默认的全球虚拟叠加交通节点。启用通过集线器进行分支和分支通信作为全局设置的一部分，默认情况下，允许所有站点使用配置的控制节点作为传输节点进行点对点通信。



添加要用作虚拟叠加交通节点的控制节点和地理控制节点，然后指定虚拟路径成本。控制节点和地理控制节点有 6 和 7 作为各自的默认虚拟路径成本。您可以选择根据网络要求更改虚拟路径成本。单击“恢复默认值”以恢复默认交通节点

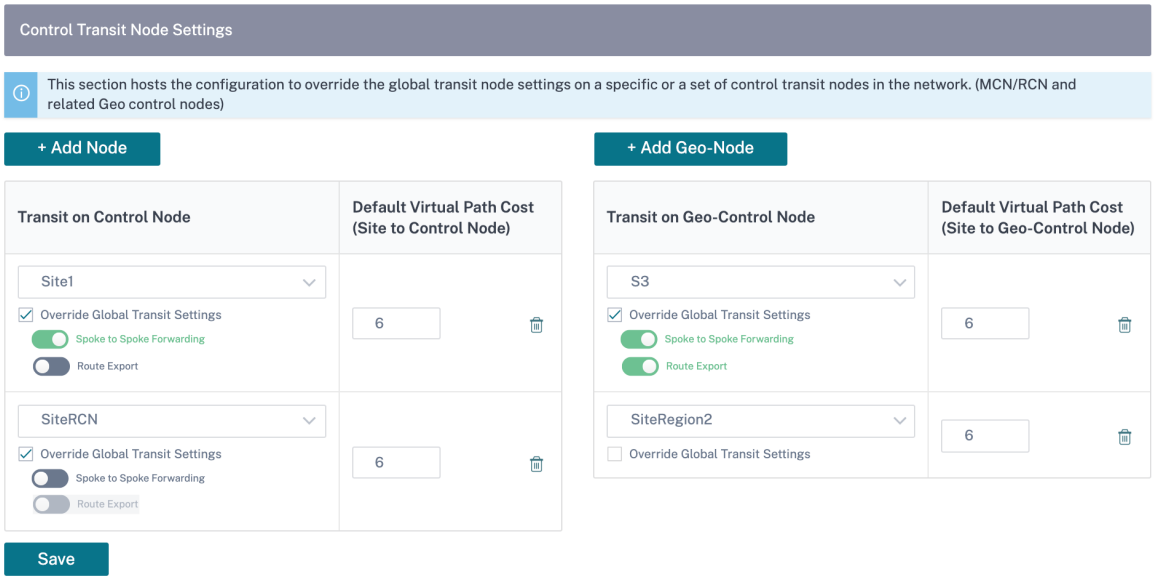
的默认虚拟路径成本。

> 注意
>
> 您最多可以添加 3 个控制节点和 3 个地理控制节点作为交通节点。

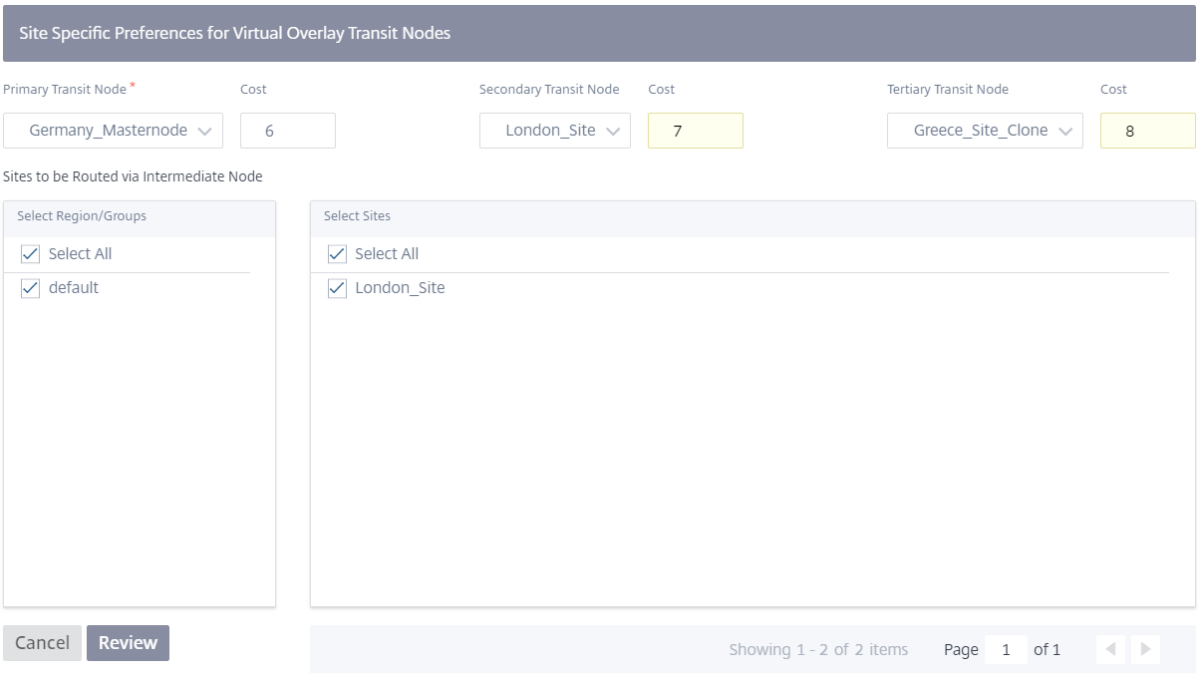
默认情况下，在与所选控制节点和地理控制节点关联的所有路径上启用 WAN 到 WAN 转发。WAN 到 WAN 转发允许站点充当任何站点到站点、互联网或内联网流量的两个相邻站点之间的中间跳跃，并充当动态虚拟路径的调解员。

您可以覆盖全局传输节点设置，选择仅在选定的控制传输节点上启用或禁用分支到分支转发。启用“分 支转发”后，传输控制节点会导出与其连接的站点之间的路由。启用了仅连接到传输节点的站点间的点对点通信和动态虚拟路径。

启用 路由导出 可在所有站点路径上启用虚拟路径到虚拟路径转发和路由导出（WAN 到 WAN 转发）。禁用切换按钮仅启用虚拟路径到虚拟路径转发，并禁用所有站点路径上的路由导出。只有启用分支 到分支转发 时，才能启用路由导出。



虚拟叠加交通节点的站点特定首选项　虚拟叠加交通节点的站点特定首选项允许您覆盖网络中所有站点的全局虚拟叠加交通节点设置。您还可以选择非控制节点作为站点的主中转节点。选择控制节点或地理控制节点作为辅助和第三交通节点。如果主中转节点关闭，站点将使用辅助中转节点。如果主要和辅助交通节点都关闭，则站点将使用第三交通节点。指定交通节点的成本，然后选择应用特定于站点的虚拟叠加交通节点设置的站点。



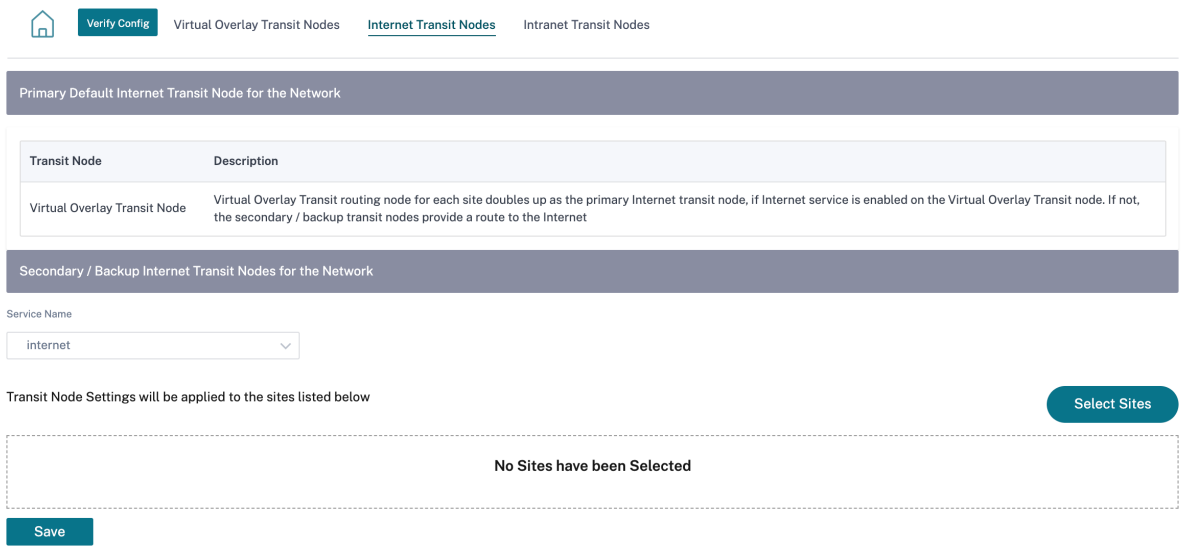
互联网交通节点

您可以将站点添加为互联网交通站点，以启用互联网访问这些站点。需要直接互联网连接的站点必须至少有一个启用 Internet 服务的链接。这意味着，至少有一个链路设置为非零带宽共享%。

可以为每个交通站点分配路线成本。提供互联网服务的站点可以直接访问互联网，因为直接路由将是成本最低的路由路径。没有互联网服务的站点可以通过配置的传输站点路由到互联网。配置互联网交通站点后，通过这些交通站点到互联网的路由将自动推送到所有站点。互联网交通站点是启用互联网服务的站点。

例如，如果将旧金山和纽约配置为互联网交通站点。通过旧金山和纽约的互联网路线会自动推送到所有站点。

启用了 Internet 服务的虚拟叠加传输节点充当主互联网传输节点。如果虚拟叠加传输节点上未启用互联网服务，辅助/备份互联网传输节点将提供通往互联网的路由。

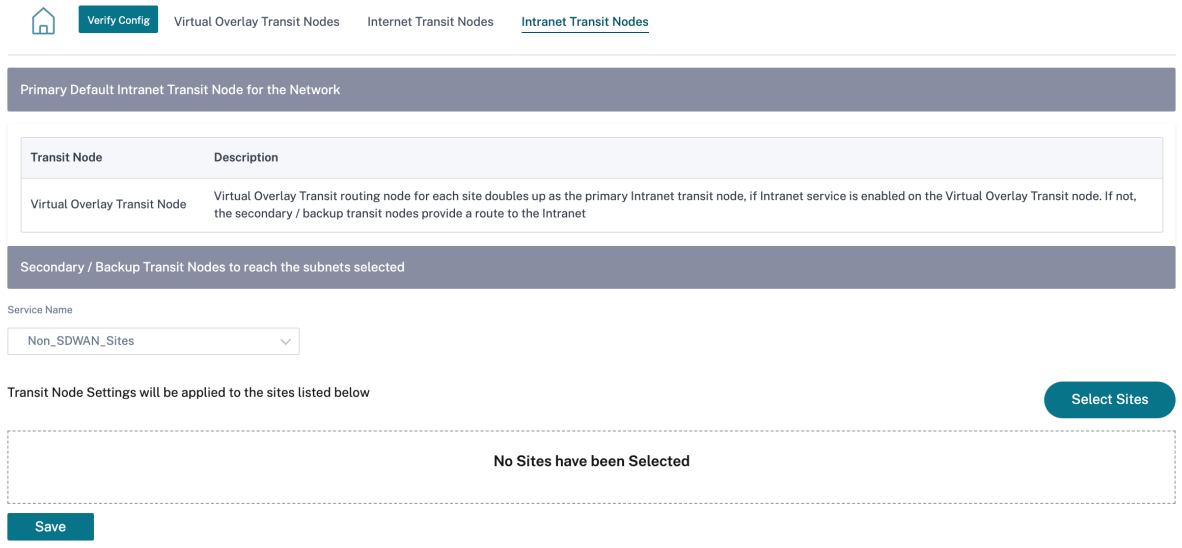


内联网中转节点

Intranet 中转节点使所有非 Intranet 站点都能访问已配置的 Intranet 网络。可以为每个交通站点分配路线成本。具有 Intranet 服务的可用站点直接访问 Intranet 网络，因为直接路由是成本最低的路由路径。没有 Intranet 服务的站点可以通过配置的传输站点路由到内联网网络。配置交通站点后，通过这些交通站点到 Intranet 网络的路由将自动推送到所有站点。

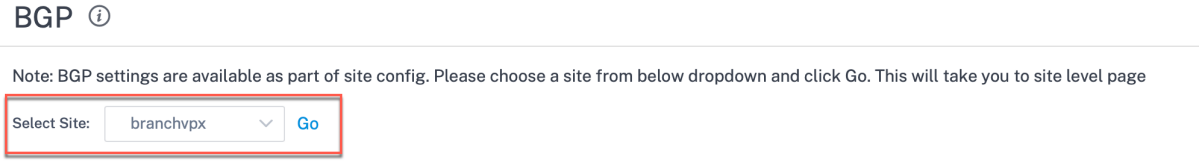
例如，如果 10.2.1.0/24 是内联网网络，而奥斯汀和达拉斯是配置的交通站点。通过奥斯汀和达拉斯到达该网络地址的路由会自动推送到所有站点。

启用 Intranet 服务的虚拟叠加中转节点充当主 Intranet 中转节点。如果未在虚拟叠加中转节点上启用 Intranet 服务，则辅助/备份 Intranet 中转节点将提供到 Intranet 的路由。



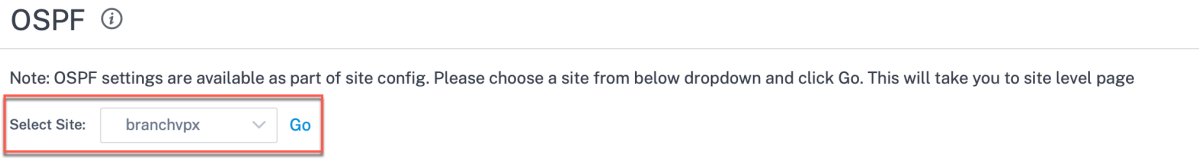
BGP

您可以通过从下拉列表中选择所需的站点并单击 G **O** 来为站点配置 BGP 设置。这将带您进入站点级 BGP 配置页面。有关配置 BGP 的详细信息，请参阅 BGP。



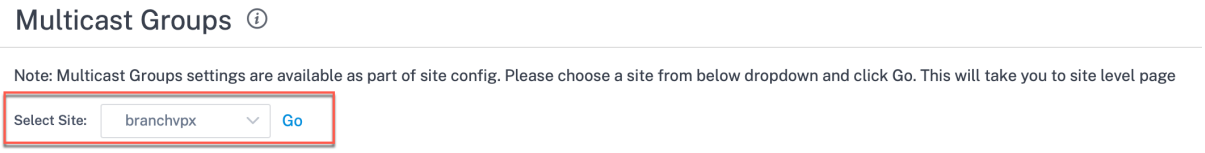
OSPF

通过从下拉列表中选择所需的站点，然后单击“开始”，可以为站点配置 **OSPF** 设置。这将带您进入站点级 OSPF 配置页面。有关配置 OSPF 的详细信息，请参阅 OSPF。



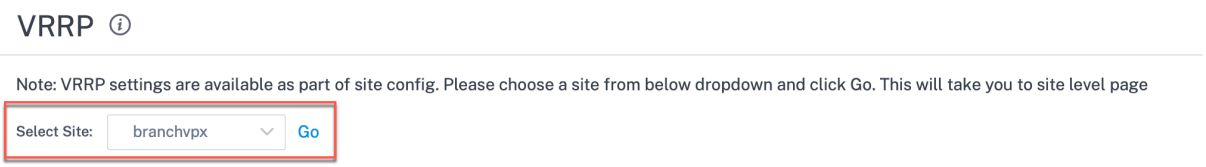
多播组

您可以通过从下拉列表中选择所需的站点并单击“开始”来为站点配置多点传送路由。这将带您进入站点级多播组配置页面。有关配置多播路由的详细信息，请参阅 多播组。



VRRP

您可以通过从下拉列表中选择所需的站点并单击“开始”来为站点配置虚拟路由器冗余协议 **(VRRP)**。这将带您进入站点级 VRRP 配置页面。有关配置多播路由的详细信息，请参阅 VRRP。



链路间通信

October 21, 2022

链路间通信设置用于在兼容的 WAN 链路之间创建自动路径。您可以在“站点配置”和“虚拟路径”下覆盖这些设置，可以在其中为给定虚拟路径选择或取消选择单个成员路径。

目前，有以下两种设置可用：

- 用于在兼容的 WAN 链接之间自动创建路径的规则。
- 动态虚拟路径的全局默认值

这些设置由客户网络中的所有 WAN 链路继承。

单击“验证配置”以验证任何审计错误。

默认的链路间通信组

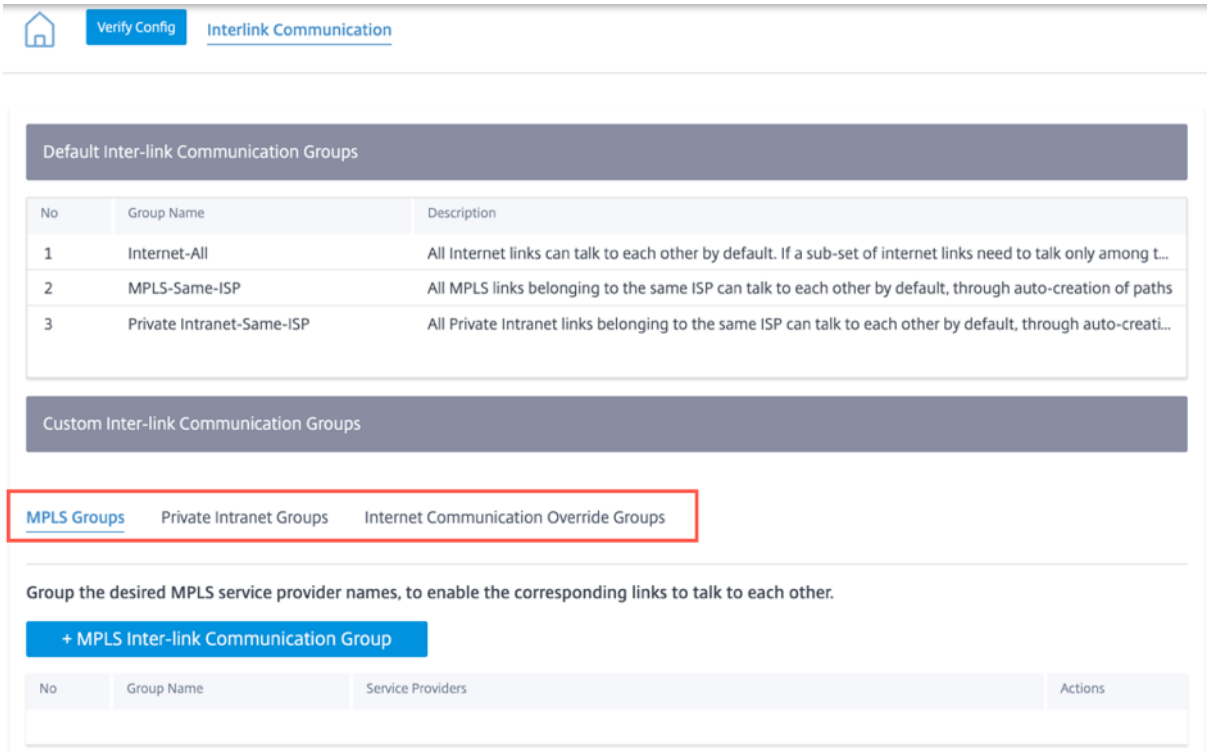
默认的链路间通信组旨在自动创建以下之间的路径：

- 任意两个互联网链接
- 共享服务提供商的任意两个 MPLS 链路，以及
- 共享服务提供商的任意两个私有 Intranet 链接

自定义链路间通信组

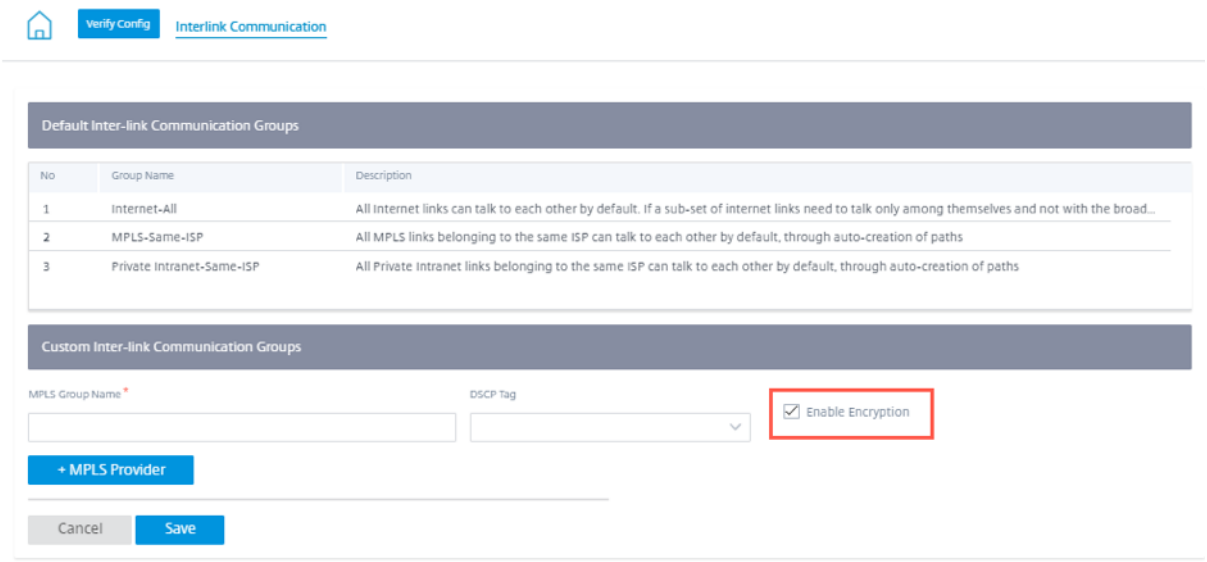
自定义互联网通信组使私有 Intranet、公共 Internet 或 MPLS 链接能够自动创建与不同服务提供商之间的其他私有 Intranet、公共 Internet 或 MPLS 链接的路径。

例如，以这种情况为例-一家公司在美国和印度设有办事处。美国办事处使用 AT & T MPLS 链接，而印度办事处使用 Airtel MPLS 链接。假设 AT & T 和 Airtel MPLS 链路在 DSCP 标签和相关参数方面是兼容的，并且可以相互创建路径。自定义链路间通信规则允许您选择 ISP 对（在本例中为 ATT —Airtel），并启用属于这些 ISP 的链路之间的自动创建路径。



- **MPLS** 组：您可以对所需的 MPLS 服务提供商名称进行分组，以使相应的链接能够相互通信。单击 **+ MPLS** 链路间通信组 并提供 MPLS 组名称。从下拉列表中选择 DSCP 标签。您还可以通过从下拉列表中选择 ISP 名称来添加 MPLS 提供商。启用加密 复选框有助于为每个自定义 MPLS 链路间通信组启用加密。在极少数情况下，为了消除加密开销，可以禁用此选项。
- 私有 **Intranet** 群组：您可以对所需的 Intranet 服务提供商名称进行分组，以使相应的链接能够相互通信。单击 **+** 私有 **Intranet InterLink** 通信组 并提供私有内联网组名称。从下拉列表中选择 DSCP 标签。您还可以通过从下拉列表中选择 ISP 名称来添加私有 Intranet 提供商。启用加密 复选框有助于启用/禁用每个自定义私有 Intranet InterLink 通信组的加密。
- **Internet** 通信覆盖组：如果一部分 Internet 链路只能相互通信，不能与其余 Internet 链路通信，则可以对相应的 ISP 名称进行分组，以便从默认组中排除。

互联网链接的其余部分仍然可以彼此通信。单击 **+** 公共互联网 **InterLink** 通信组 并提供公共互联网组名称。从下拉列表中选择 DSCP 标签。您还可以通过从下拉列表中选择 ISP 名称来添加公共互联网提供商。启用加密 选项可确保在虚拟路径上发送的链路间通信组的数据包经过加密。



安全性

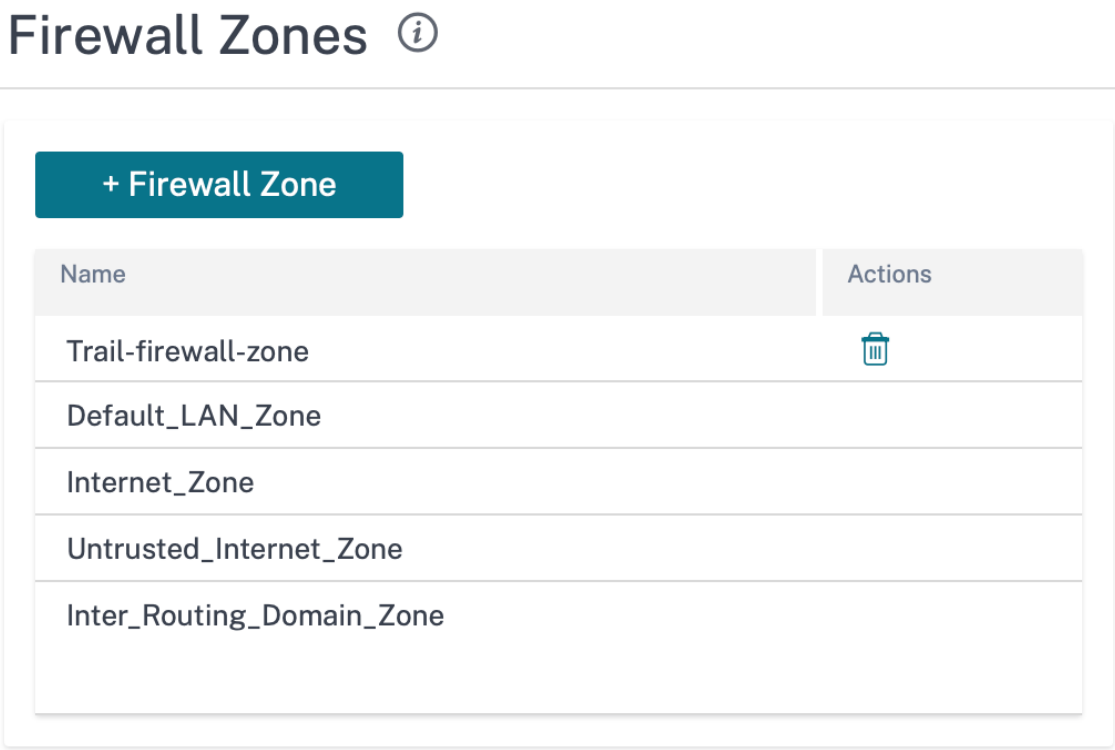
October 21, 2022

您可以配置适用于网络中所有设备的安全设置，例如网络安全、虚拟路径 IPsec、防火墙和证书。

防火墙区域

您可以在网络中配置区域并定义策略来控制流量进出区域的方式。默认情况下，以下区域可用：

- de@@**fault_LAN_Zon**e：适用于进出具有可配置区域的对象的流量，但该区域尚未设置。
- **Internet_Zone**：适用于使用可信接口进出互联网服务的流量。
- **Untrusted_Internet_Zon**e：适用于使用不可信接口进出互联网服务的流量。



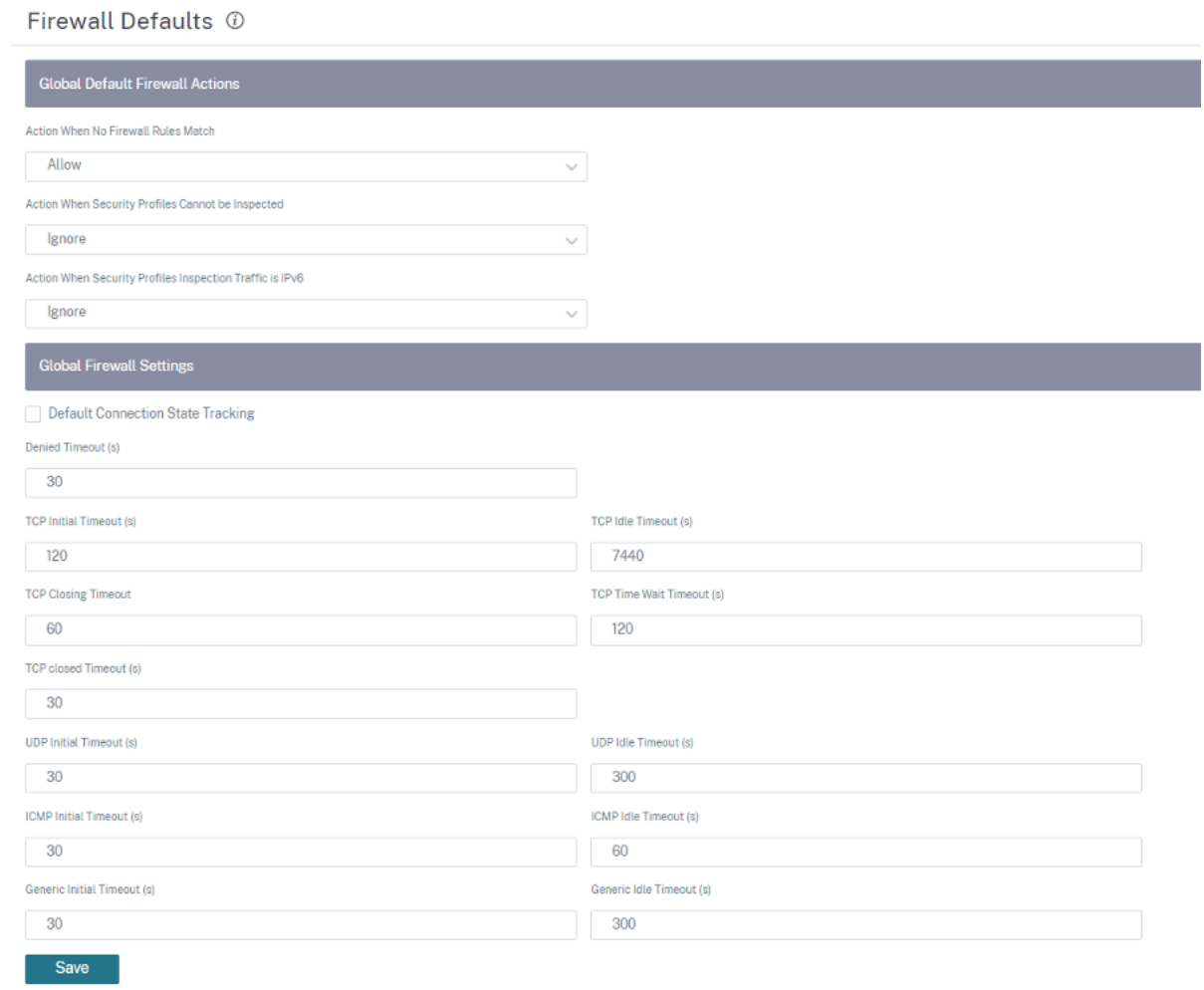
您还可以创建自己的区域并将其分配给以下类型的对象：

- 虚拟网络接口
- 内联网服务
- GRE 通道
- 局域网 IPsec 通道

单击“验证配置”以验证任何审计错误。

防火墙默认

您可以配置可应用于 SD-WAN 网络中所有设备的全局默认防火墙操作和全局防火墙设置。还可以在覆盖全局设置的站点级别定义设置。



- 防火墙规则不匹配时的操作：从列表中选择与防火墙策略不匹配的数据包的操作（允许或丢弃）。
- 无法检查安全配置文件时的操作：为符合防火墙规则并使用安全配置文件但暂时无法被 Edge Security 子系统检查的数据包选择操作（忽略或丢弃）。如果选择“忽略”，则相关防火墙规则将被视为不匹配，并按顺序评估下一个防火墙规则。如果选择 **Drop**，则与相关防火墙规则匹配的数据包将被丢弃。
- 默认防火墙操作：从列表中选择与策略不匹配的数据包的操作（允许/删除）。
- 默认连接状态跟踪：对与筛选策略或 NAT 规则不匹配的 TCP、UDP 和 ICMP 流启用定向连接状态跟踪。

  > 注意
  >
  > 启用 “默认连接状态跟踪” 后，即使没有定义防火墙策略，非对称流量也会被阻止。如果站点有可能出现不对称流量，则建议在站点或策略级别而不是在全球范围内启用它。

- 拒绝超时：在关闭被拒绝的连接之前等待新数据包的时间（以秒为单位）。
- **TCP** 初始超时：在关闭未完成的 TCP 会话之前等待新数据包的时间（以秒为单位）。
- **TCP** 空闲超时：在关闭活动 TCP 会话之前等待新数据包的时间（以秒为单位）。

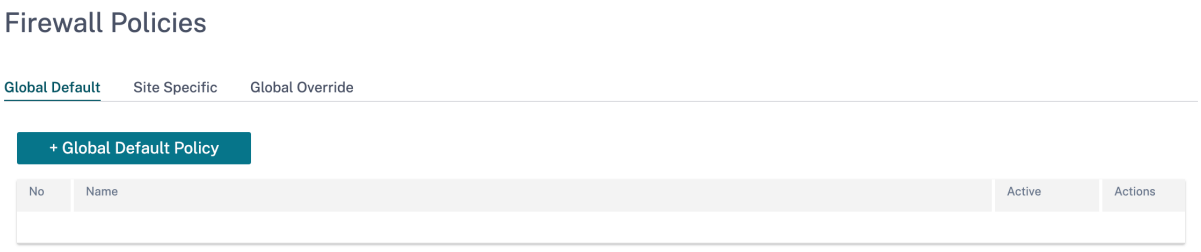
- **TCP** 关闭超时：在终止请求后关闭 TCP 会话之前等待新数据包的时间（以秒为单位）。
- **TCP** 等待时间超时：在关闭已终止的 TCP 会话之前等待新数据包的时间（以秒为单位）。
- **TCP** 关闭超时：在关闭中止的 TCP 会话之前等待新数据包的时间（以秒为单位）。
- **UDP** 初始超时：在关闭未看到双向流量的 UDP 会话之前等待新数据包的时间（以秒为单位）。
- **UDP** 空闲超时：在关闭活动 UDP 会话之前等待新数据包的时间（以秒为单位）。
- **ICMP** 初始超时：在关闭未看到双向流量的 ICMP 会话之前等待新数据包的时间（以秒为单位）
- **ICMP** 空闲超时：在关闭活动 ICMP 会话之前等待新数据包的时间（以秒为单位）。
- 通用初始超时：在关闭没有双向流量的通用会话之前等待新数据包的时间（以秒为单位）。
- 通用空闲超时：在关闭活动通用会话之前等待新数据包的时间（以秒为单位）。

单击“验证配置”以验证任何审计错误。

防火墙策略

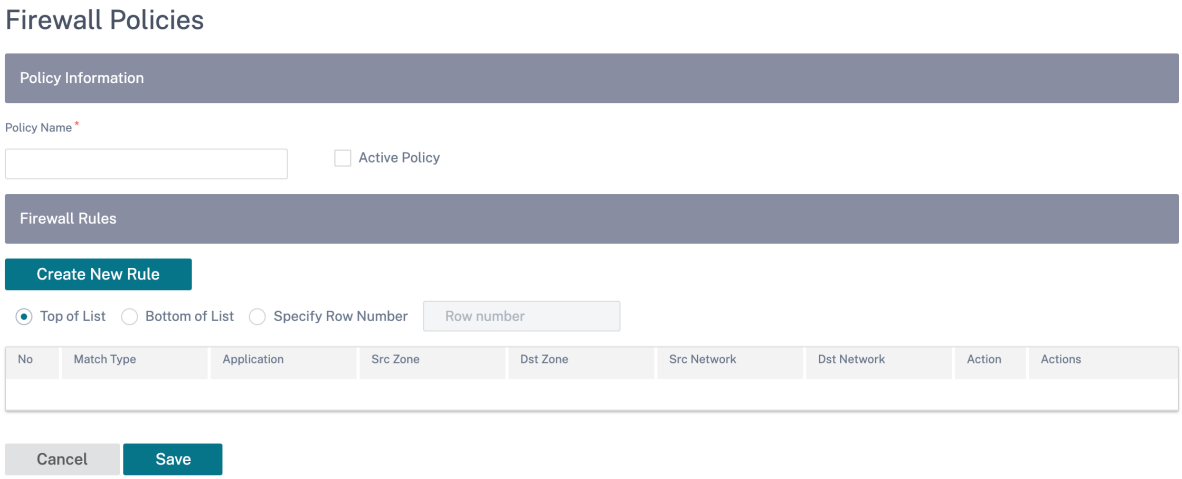
防火墙配置文件通过确保网络流量仅限于特定的防火墙规则，具体取决于匹配条件，并通过应用特定操作来提供安全性。防火墙策略 包含三个部分。

- 全局默认 -全局默认策略是几个防火墙规则的聚合。您在“全局默认”部分下创建的策略将应用于网络中的所有站点。
- 特定站点 -您可以将定义的防火墙规则应用于某些特定站点。
- 全局覆盖 -您可以使用全局覆盖策略来 覆盖全局和特定站点的策略。

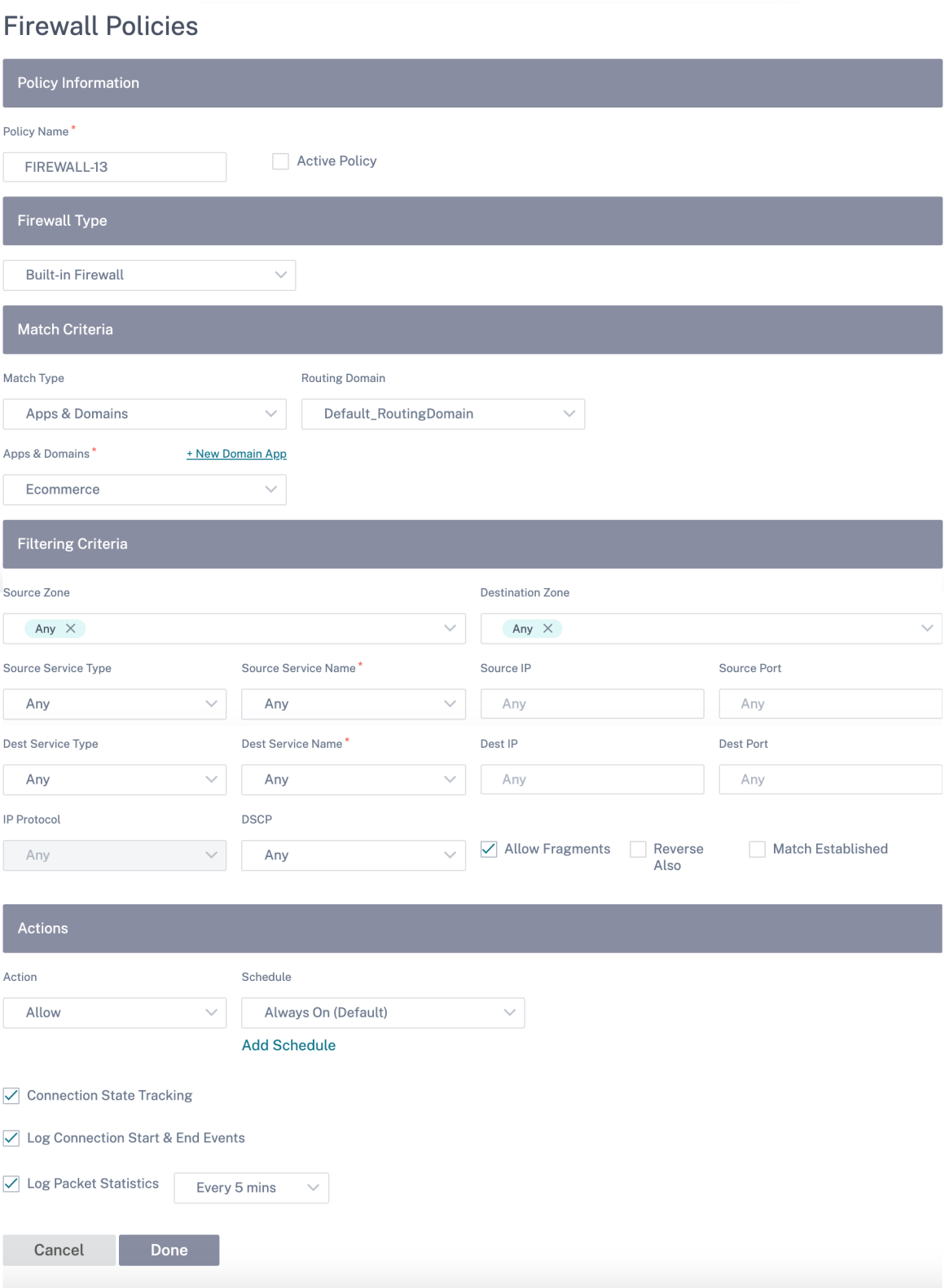


您可以定义防火墙规则并根据优先级进行放置。您可以选择从列表顶部、列表底部或特定行开始的优先顺序。

建议在顶部为应用程序或子应用程序设置更具体的规则，然后对代表更广泛流量的应用程序或子应用程序使用不太具体的规则。



要创建防火墙规则，请单击“创建新规则”。



- 如果要应用所有防火墙规则，请提供 策略名称并选中 **Activ** e Policy 复选框。
- 匹配条件定义规则的流量，例如，应用程序、自定义的应用程序、应用程序组、应用程序系列或基于 IP 协议的流

量。

- 筛选条件：
  - 源区域：源防火墙区域。
  - 目标区域：目标防火墙区域。
  - 源服务类型：源 SD-WAN 服务类型-本地、虚拟路径、Intranet、IP 主机或互联网是服务类型的示例。
  - 源服务名称：与服务类型相关的服务的名称。例如，如果为源服务类型选择了虚拟路径，则该路径将是特定虚拟路径的名称。这并不总是必需的，取决于所选服务类型。
  - 源 **IP**：规则用于匹配的 IP 地址和子网掩码。
  - 源端口：特定应用程序使用的源端口。
  - 目标服务类型：目标 SD-WAN 服务类型-本地、虚拟路径、Intranet、IP 主机或互联网是服务类型的示例。
  - 目标服务名：与服务类型关联的服务的名称。这并不总是必需的，取决于所选服务类型。
  - 目标 **IP**：筛选器用于匹配的 IP 地址和子网掩码。
  - 目标端口：特定应用程序使用的目标端口（即 TCP 协议的 HTTP 目标端口 80）。
  - **IP** 协议：如果选择此匹配类型，请选择与该规则匹配的 IP 协议。选项包括 “任意”、“TCP”、“UDP ICMP” 等。
  - **DSCP**：允许用户在 DSCP 标签设置上进行匹配。
  - 允许分段：允许匹配此规则的 IP 分段。
  - 还反向：自动添加此筛选策略的副本，同时颠倒来源和目标设置。
  - 匹配已建立：匹配允许传出数据包的连接的传入数据包。
- 可以对匹配的流程执行以下操作：
  - 允许：允许流量通过防火墙。
  - 丢弃：通过丢弃数据包来拒绝流经防火墙。
  - 拒绝：拒绝通过防火墙的流量并发送协议特定的响应。TCP 发送重置，ICMP 会发送错误消息。
  - 计数并继续：计算此流的数据包数和字节数，然后继续沿策略列表向下移动。

除了定义要执行的操作外，您还可以选择要捕获的日志。

网络安全

选择要在网络上使用的加密机制。您可以配置保护整个 SD-WAN 网络的全局安全设置。

网络加密模式定义用于 SD-WAN 网络中所有加密路径的算法。它不适用于非加密路径。您可以将加密设置为 AES-128 或 AES-256。

FIPS 合规性

FIPS 模式强制用户为其 IPSec 隧道配置 FIPS 兼容设置，为虚拟路径配置 IPSec 设置。

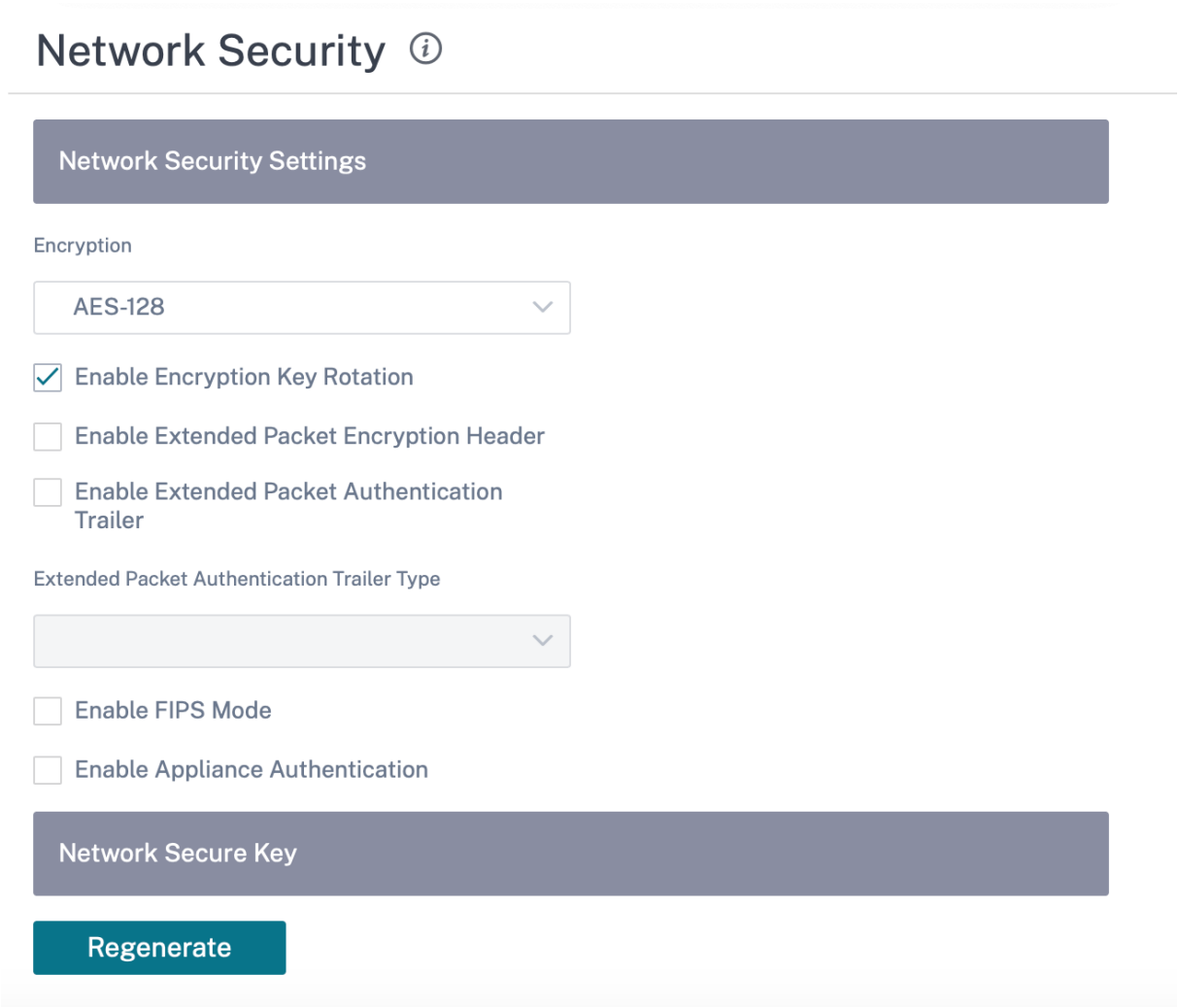
启用 FIPS 模式可提供以下功能：

- 显示符合 FIPS 的 IKE 模式。
- 显示符合 FIPS 标准的 IKE DH 组，用户可以从中选择在 FIPS 兼容模式（2,5,14-21）下配置设备所需的参数。
- 在虚拟路径的 IPsec 设置中显示符合 FIPS 标准的 IPsec 通道类型
- IKE 哈希和（IKEv2）完整性模式，IPsec 身份验证模式。
- 对基于 FIPS 的生命周期设置执行审计错误。

要在 Citrix SD-WAN Orchestrator 服务上启用 FIPS 合规性：

1. 转到 配置 > 安全 > 网络安全。
2. 在“网络安全设置”部分中，单击“启用 **FIPS** 模式”复选框。

启用 FIPS 模式会在配置期间强制执行检查，以确保所有与 IPsec 相关的配置参数都符合 FIPS 标准。系统会通过审计错误和警告提示您 配置 IPsec。



如果启用 IPSec 配置时不符合 FIPS 标准，则可能会触发审计错误。以下是您在适用于本地 UI 的 Citrix SD-WAN Orchestrator 上单击“验证配置”时显示的审计错误类型。

- 启用 FIPS 模式并选择不符合 FIPS 的选项时。
- 启用 FIPS 模式且输入的生命周期值不正确时。
- 启用 FIPS 模式并启用虚拟路径的 IPsec 设置时，默认设置也处于启用状态，并且选择了错误的隧道模式（ESP 与 ESP_AUTH/AH）。
- 启用 FIPS 模式时，还会启用虚拟路径默认设置的 IPsec 设置，并且输入的生命周期值不正确。

启用加密密钥轮替：启用后，加密密钥每隔 10 至 15 分钟轮换一次。

启用扩展数据包加密标头：启用后，将在加密流量之前添加一个 16 字节的加密计数器，用作初始化向量，并随机进行数据包加密。

启用扩展数据包身份验证尾部：启用后，身份验证代码会附加到加密流量的内容，以验证邮件是否未经更改地传递。

扩展数据包身份验证拖车类型：这是用于验证数据包内容的拖车类型。从下拉菜单中选择以下选项之一：**32** 位校验和或 **SHA-256**。

SSL 检查

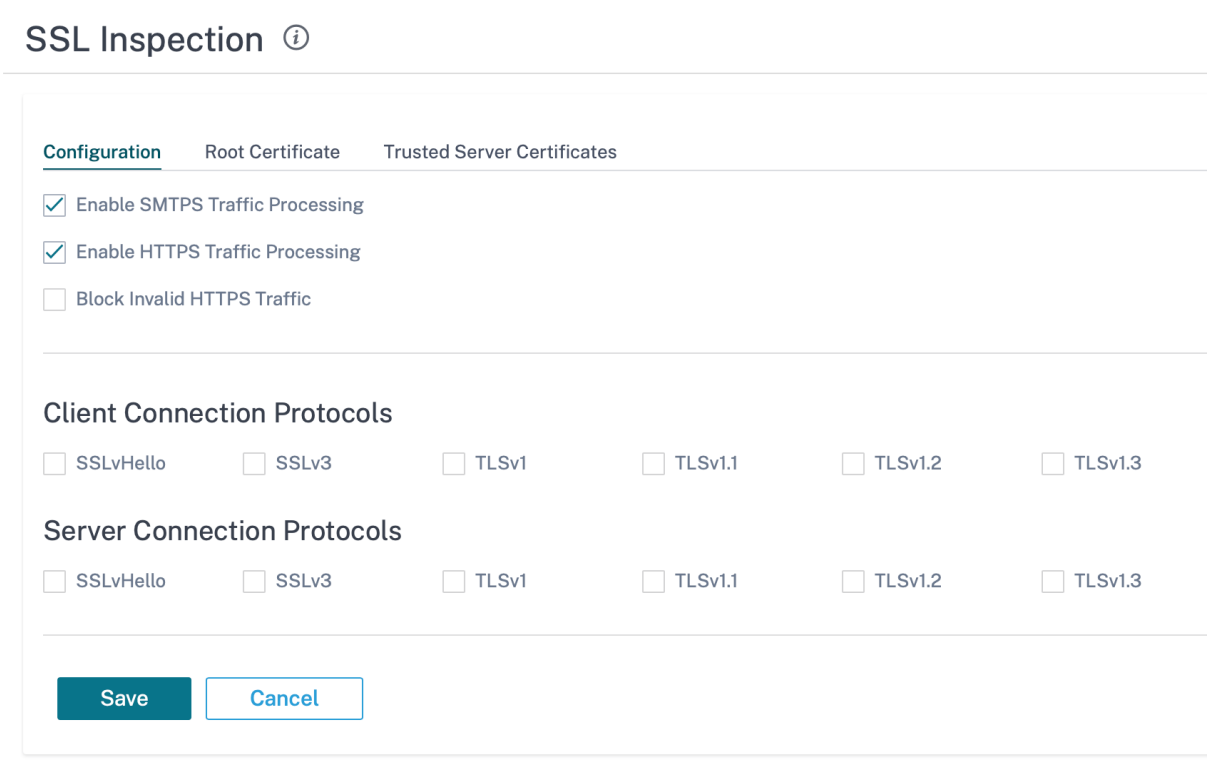
安全套接字层 (SSL) 检查是拦截、解密和扫描 HTTPS 和安全 SMTP 流量中是否存在恶意内容的过程。SSL 检查为流入和流出您的组织的流量提供安全保障。您可以生成和上传贵组织的根 CA 证书，并对流量进行中间人检查。

> 注意
>
> Citrix SD-WAN 11.3.0 版本以后支持 SSL 检查。

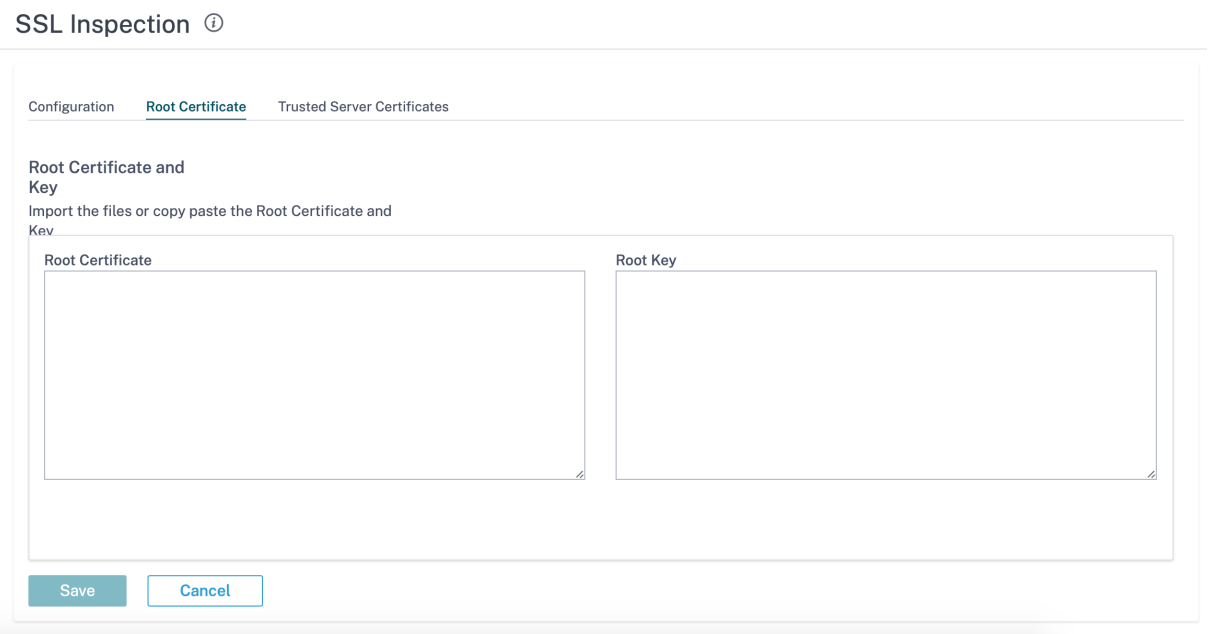
要启用 SSL 检查，请在网络级别导航到 配置 **>** 安全 **> SSL** 检查 **>** 配置，然后定义以下 SSL 配置设置。

- 启用 **SMTPS** 流量处理：安全 SMTP 流量经过 SSL 检查。
- 启用 **HTTPS** 流量处理：HTTPS 流量经过 SSL 检查。
- 阻止无效的 **HTTPS** 流量：默认情况下，当清除“阻止无效 **HTTPS** 流量”复选框时，端口 443 上的非 HTTPS 流量将被忽略并允许畅通无阻地流动。选择 阻止无效的 **HTTPS** 流量 时，将阻止非 HTTPS 流量以进行 SSL 检查。启用此选项可能会导致原本合法的流量被阻止，即端口 443 上的 HTTP 流量或来自证书过期站点的 HTTPS 流量。
- 客户机连接协议：选择所需的客户机协议。可用的协议有 sslvHello、SSLv3、tlsv1、tslv1.1、tlsv1.2 和 tlsv1.3。
- 服务器连接协议：选择所需的服务器协议。可用的协议有 sslvHello、SSLv3、tlsv1、tslv1.1、tlsv1.2 和 tlsv1.3。

> 注意
>
> 早于 TLSv1.2 的版本被视为易受攻击，除非向后兼容很重要，否则不得启用。

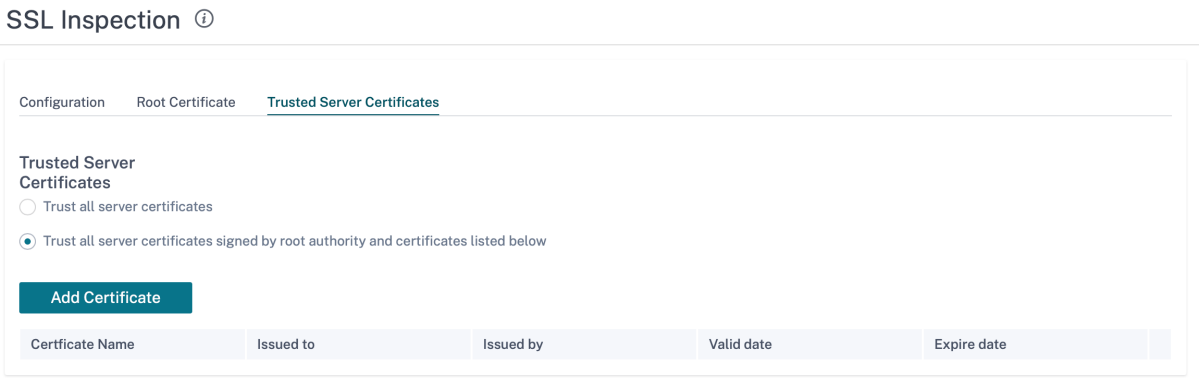


在“根证书”选项卡上，复制并粘贴您的组织根证书颁发机构 (CA) 的根证书和密钥。根 CA 用于创建和签署原始站点证书的伪造副本，以便执行 SSL 检查。隐含地假定根 CA 证书安装在所有可以对其流量 SSL 进行检查的客户端工作站和设备上。



默认的“信任根机构签发的所有服务器证书和下面列出的证书”选项会导致 SD-WAN 根据根证书的标准列表和先前配置的根 CA 对所有服务器证书进行验证。它还会丢弃证书无效的服务器。要覆盖此行为，请在“可信服务器证书”选项卡

上上传内部服务器的 **SSL** 自签名证书。单击“添加证书”并提供名称，浏览并上传证书。或者，如果您选择“信任所有服务器证书”，则无论其证书验证状态如何，Citrix SD-WAN 都将所有服务器视为信任。



作为安全配置文件的一部分，您可以创建 SSL 规则并将其启用以进行 SSL 检查。有关为安全配置文件创建 SSL 规则的更多信息，请参阅 Edge 安全。

入侵防御

入侵防御系统 (IPS) 可检测并防止恶意活动进入您的网络。IPS 检查网络流量并对所有传入流量采取自动操作。它包括一个包含超过 34,000 个签名检测和用于端口扫描的启发式签名的数据库，使您能够有效地监视和阻止大多数可疑请求。

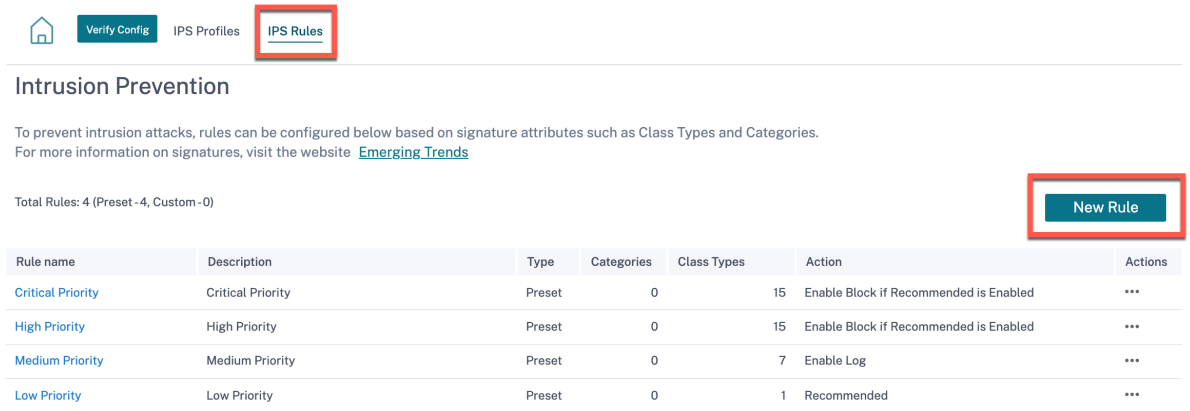
IPS 使用基于特征的检测，它将传入的数据包与具有唯一可识别的漏洞和攻击模式的数据库进行匹配。签名数据库每天自动更新。由于有成千上万个签名，因此签名被分组为类别和类类型。

您可以创建 IPS 规则并仅启用网络所需的签名类别或类类型。由于入侵防护是一个对计算敏感的过程，因此请仅使用与您的网络相关的最少签名类别或类类型集。

您可以创建 IPS 配置文件并启用 IPS 规则组合。然后，这些 IPS 配置文件可以与整个网络全局关联，也可以仅与特定站点关联。

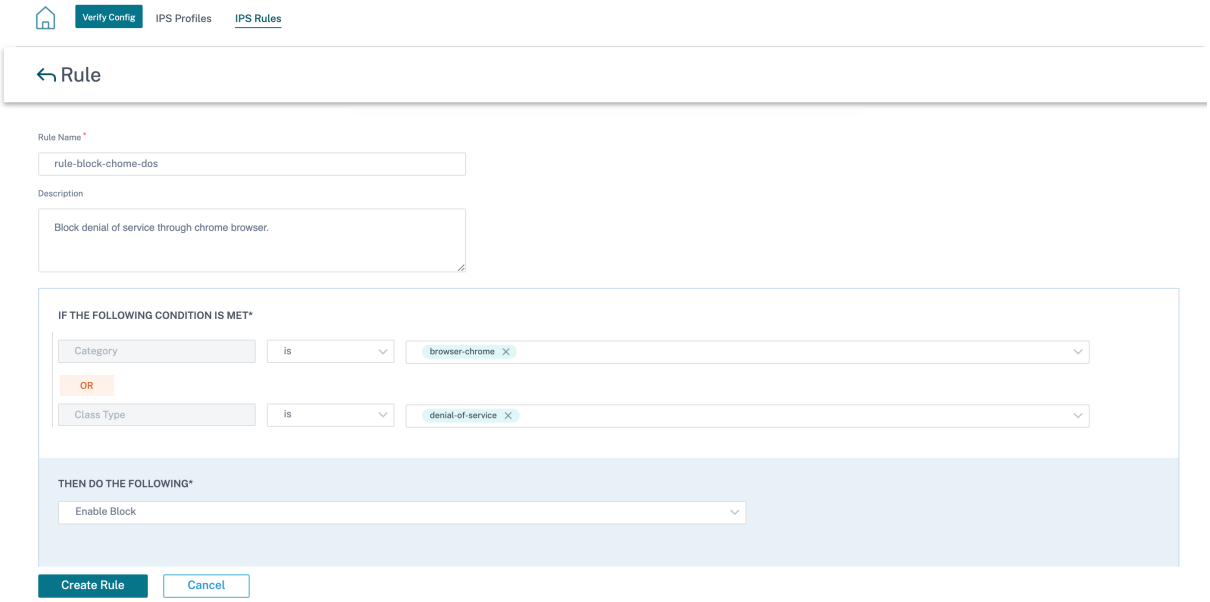
每个规则可以与多个 IPS 配置文件相关联，每个 IPS 配置文件可以与多个站点关联。启用 IPS 配置文件后，它会检查与 IPS 配置文件关联的站点的网络流量以及该配置文件中启用的 IPS 规则。

要创建 IPS 规则，请在网络级别导航到 配置 **>** 安全 **>** 入侵防御 **> IPS** 规则，然后单击“新建规则”。



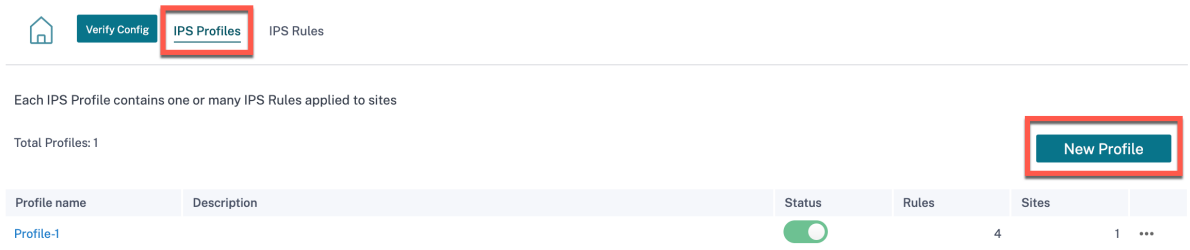
提供规则名称和描述。选择匹配类别或类别类型签名属性，为规则选择一个操作，然后将其启用。您可以从以下规则操作中进行选择：

规则操作	功能
推荐	为每个签名定义了建议的操作。对签名执行建议的操作。
启用日志	允许并记录与规则中任何签名匹配的流量。
启用“如果推荐”启用阻止	如果规则操作为“推荐”，而签名的推荐操作为“启用日志”，则删除与规则中任何签名匹配的流量。
启用阻止	丢弃与规则中任何签名匹配的流量。

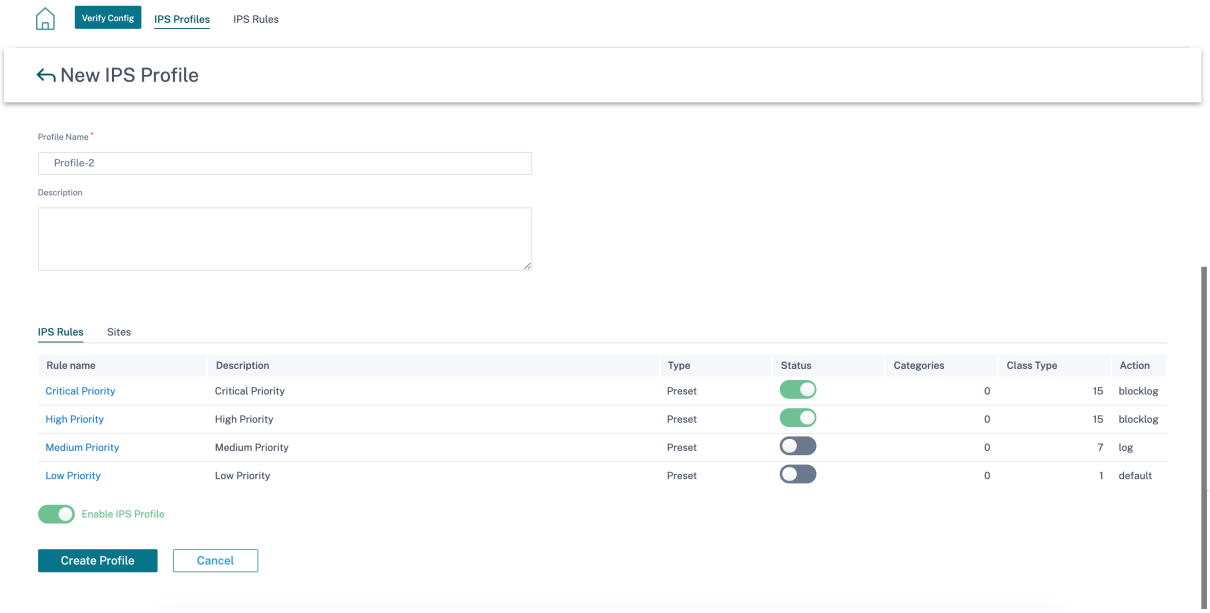


> 注意
>
> - 由于入侵防护是一个计算敏感的进程，因此只使用与边缘安全部署相关的最低限度的签名类别集。
> - SD-WAN 防火墙会丢弃所有未端口转发且在 IPS 引擎中不可见的 WAN L4 端口上的流量。这为防止微不足道的 DOS 和扫描攻击提供了额外的安全层。

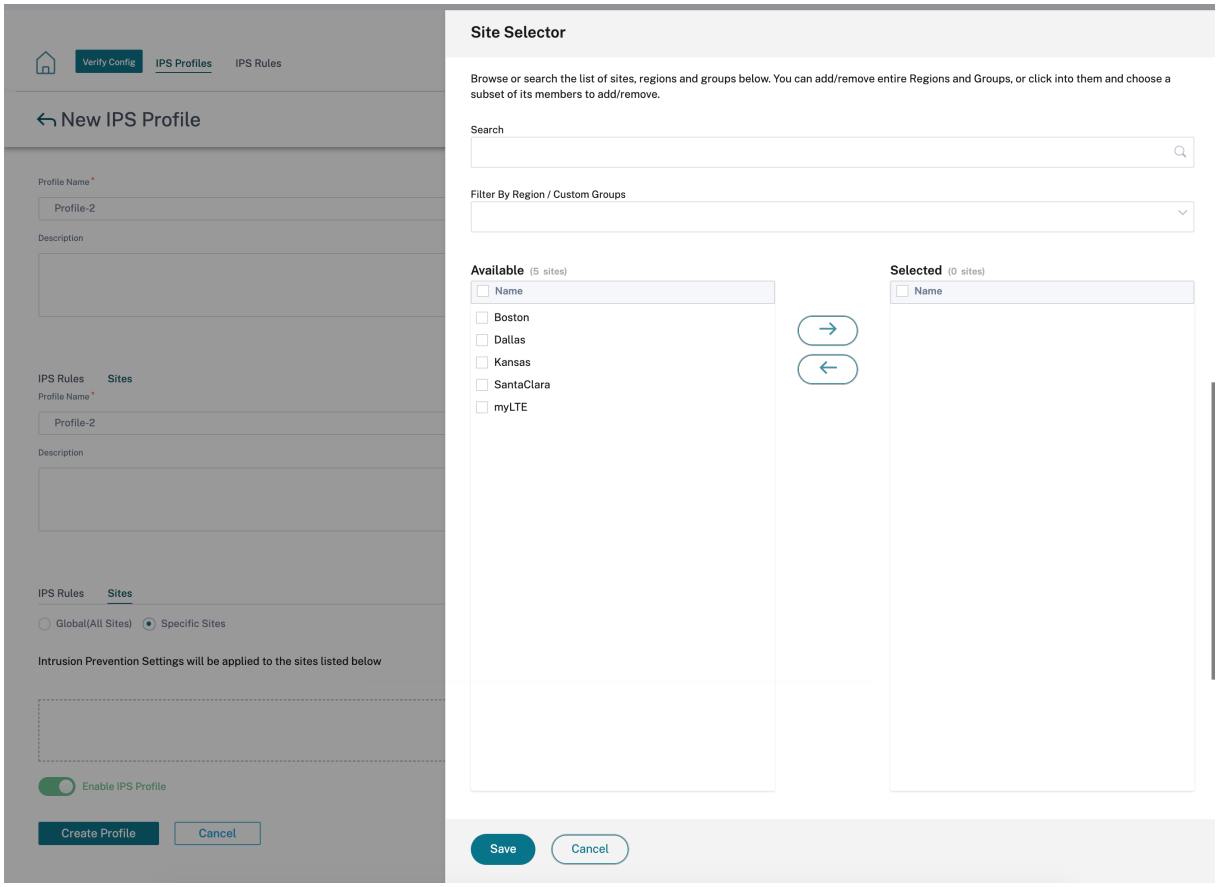
要创建 IPS 配置文件，请在网络级别导航到 配置 **>** 安全 **>** 入侵防护 **> IPS** 配置文件，然后单击“新建配置文件”。



提供 IPS 配置文件的名称和描述。在 **IPS** 规则 选项卡上，启用所需的 **IPS** 规则，然后打开“启用 **IPS** 配置文件”。



在“站点”选项卡上，单击“选择站点”。选择站点，然后单击“保存”。单击“创建个人资料”。



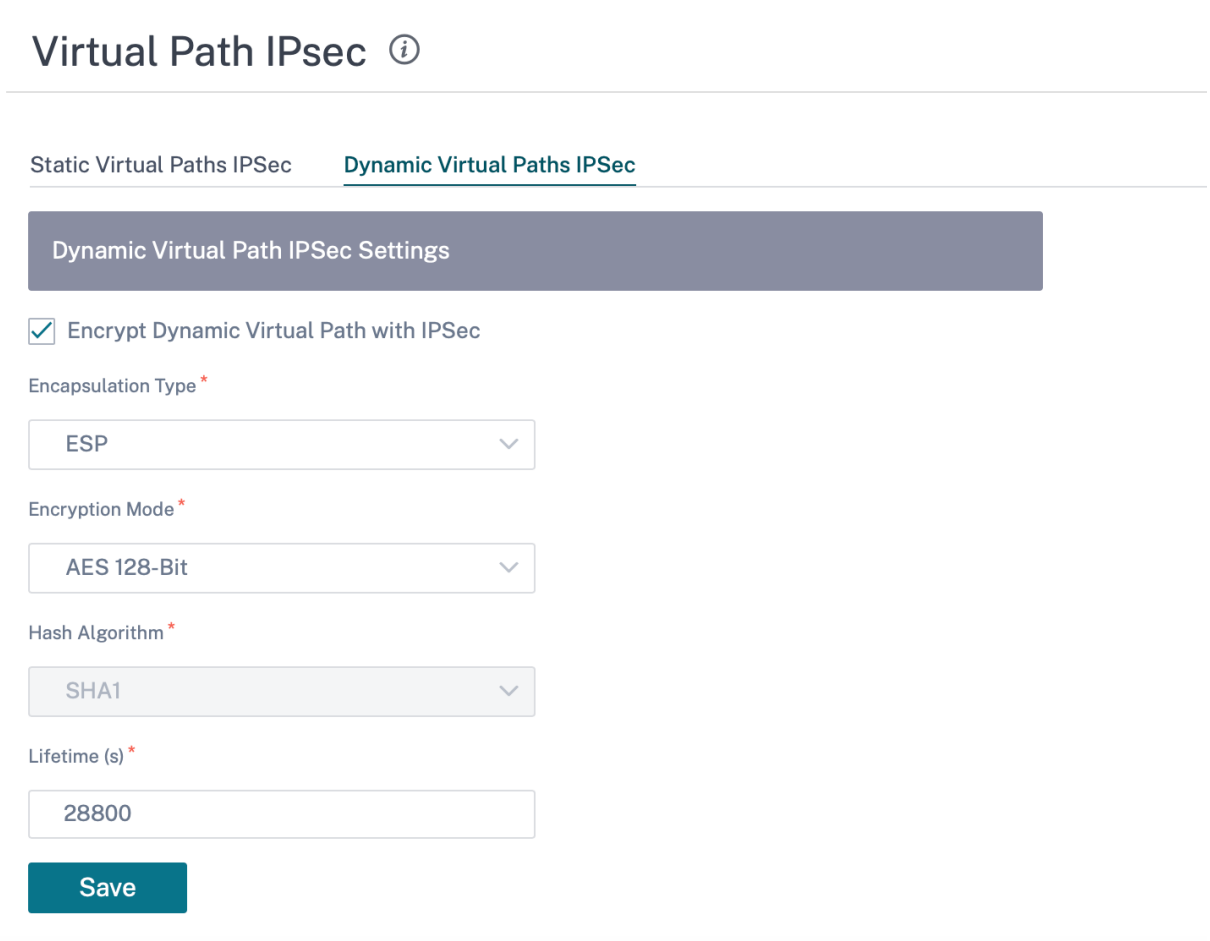
您可以在创建安全配置文件时启用或禁用这些 IPS 配置文件。安全配置文件用于创建防火墙规则。有关更多信息，请参阅 安全配置文件-入侵防御。

虚拟路径 **IPsec**

虚拟路径 **IPsec** 定义 IPsec 隧道设置，以确保通过静态虚拟路径和动态虚拟路径安全传输数据。选择“静态虚拟路径 **IPsec**”或“动态虚拟路径 **IPsec**”选项卡以定义 IPsec 隧道设置。

- 封装类型：选择以下安全类型之一：
  - **ESP**：数据已封装和加密。
  - **ESP+Auth**：使用 HMAC 对数据进行封装、加密和验证。
  - 啊：数据通过 HMAC 进行验证。
- 加密模式：启用 ESP 时使用的加密算法。
- 哈希算法：用于生成 HMAC 的哈希算法。
- 生命周期：**IPs**ec 安全关联存在的首选持续时间，以秒为单位。输入 0 表示无限制。

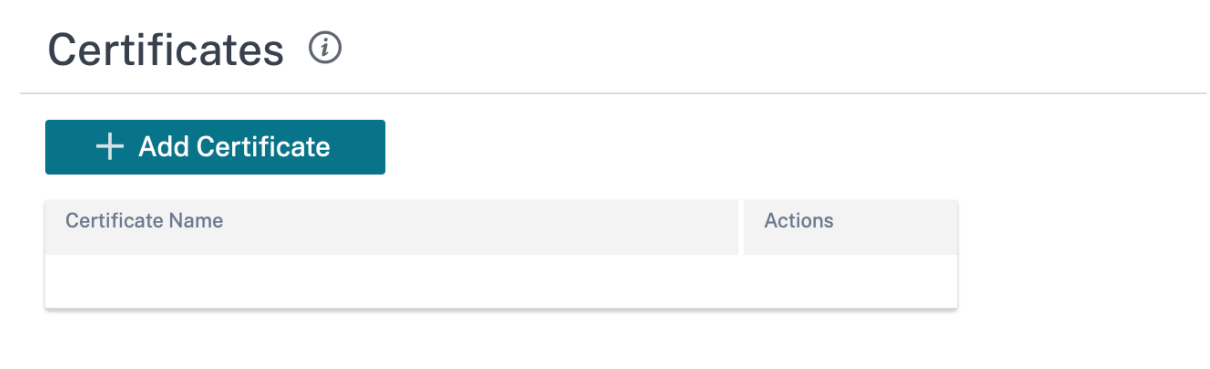
有关配置 IPsec 服务的信息，请参阅 IPsec 服务。



单击“验证配置”以验证任何审计错误

证书

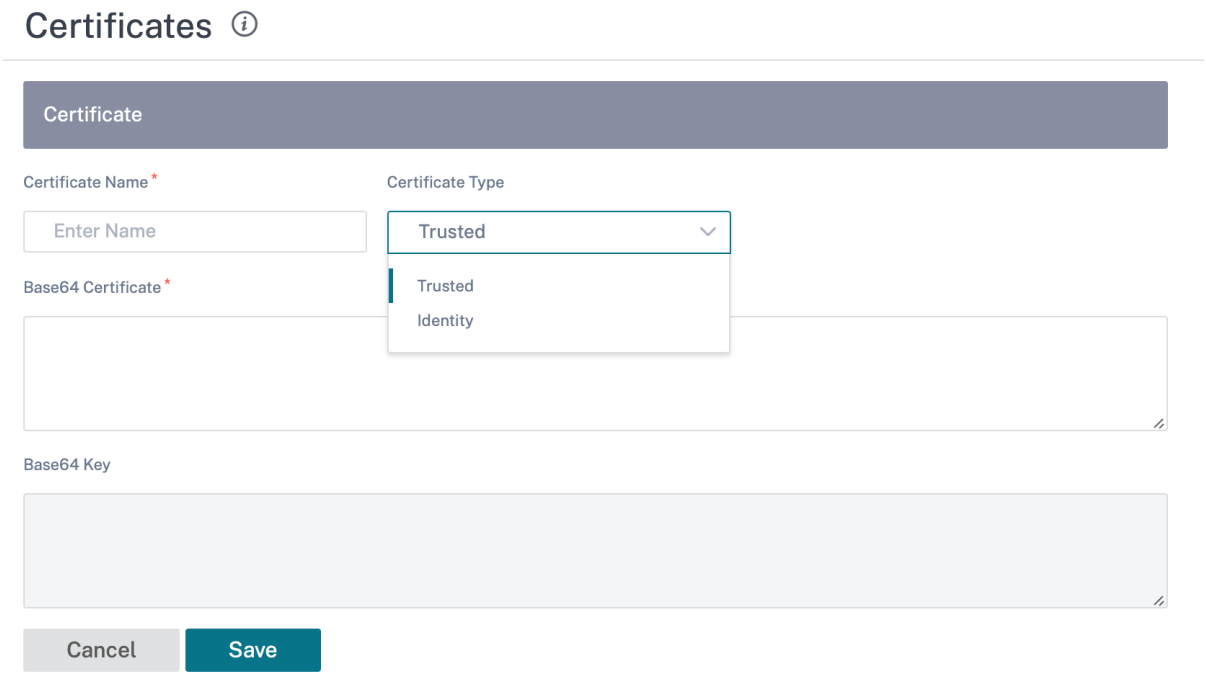
有两种类型的证书：身份证书和可信证书。身份证书用于对数据进行签名或加密，以验证消息的内容和发件人的身份。可信证书用于验证消息签名。Citrix SD-WAN 设备接受身份和可信证书。管理员可以在配置编辑器中管理证书。



单击“验证配置”以验证任何审计错误

要添加证书，请单击“添加证书”。

- 证书名称：提供证书名称。
- 证书类型：从下拉列表中选择证书类型。
  - 身份证书：身份证书要求证书的私钥可供签名者使用。对等体信任的身份证书或其证书链来验证发件人的内容和身份。配置的身份证书及其相应的指纹显示在配置编辑器中。
  - 可信证书：可信证书是自签名的中间证书颁发机构 (CA) 或根 CA 证书，用于验证对等方的身份。可信证书不需要私钥。此处列出了已配置的可信证书及其相应的指纹。

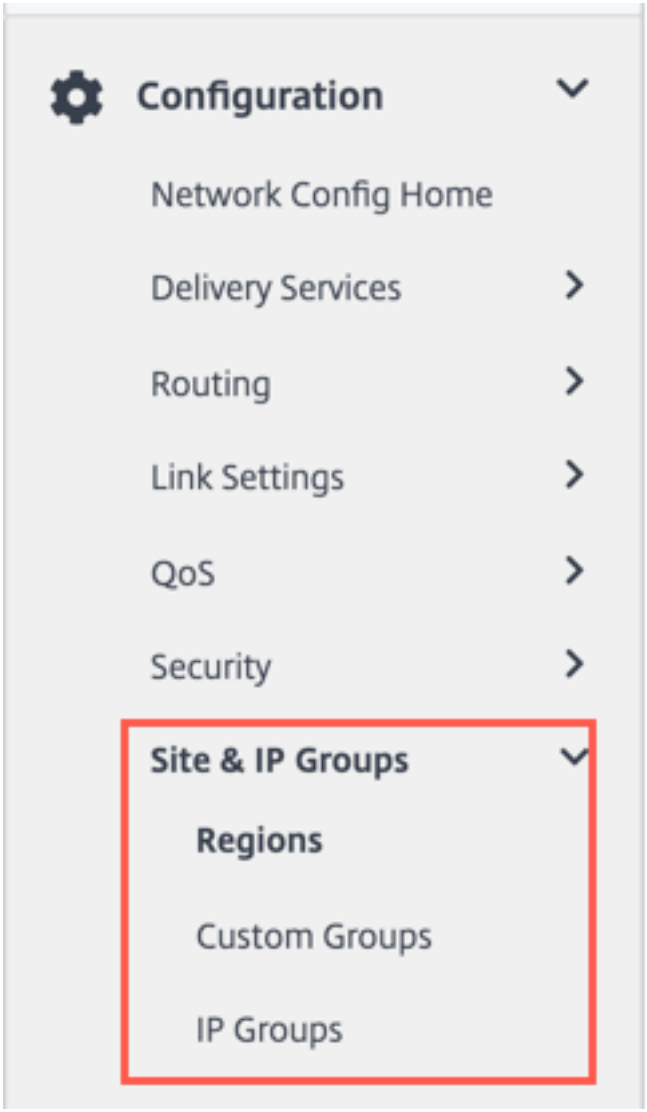


站点和 IP 组

October 21, 2022

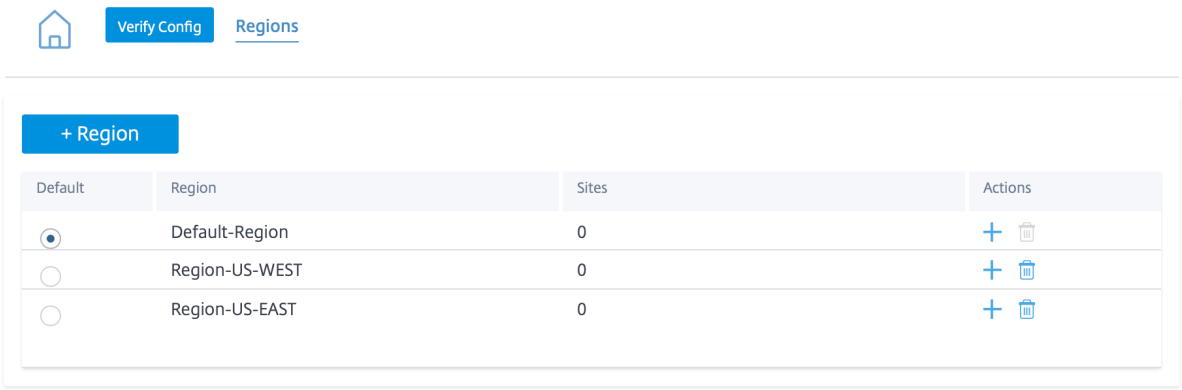
管理员可以对站点或 IP 地址进行分组，以简化跨多个站点或网络地址的常用应用程序策略，还可以用作报告的过滤器。

要查看区域、站点和 IP 组，请导航到 配置 > 站点和 **IP** 组。



区域

区域有助于在跨越数百到数千个站点的大型网络中创建管理边界。如果您的组织拥有跨越多个管理（或地理）边界的大型网络，则可以考虑创建区域来对网络进行分段。



目前，每个区域最多支持 1000 个站点。预计每个区域都有一个区域控制节点 (RCN)，作为该区域的中心和 Controller。因此，如果您的网络拥有超过 500 个站点，则通常会考虑多区域部署。默认情况下，所有网络都是单区域网络，其中主控制节点 (MCN) 充当所有站点的中心和控制节点。添加一个或多个区域后，该网络变为多区域网络。与 MCN 关联的区域称为 默认区域。

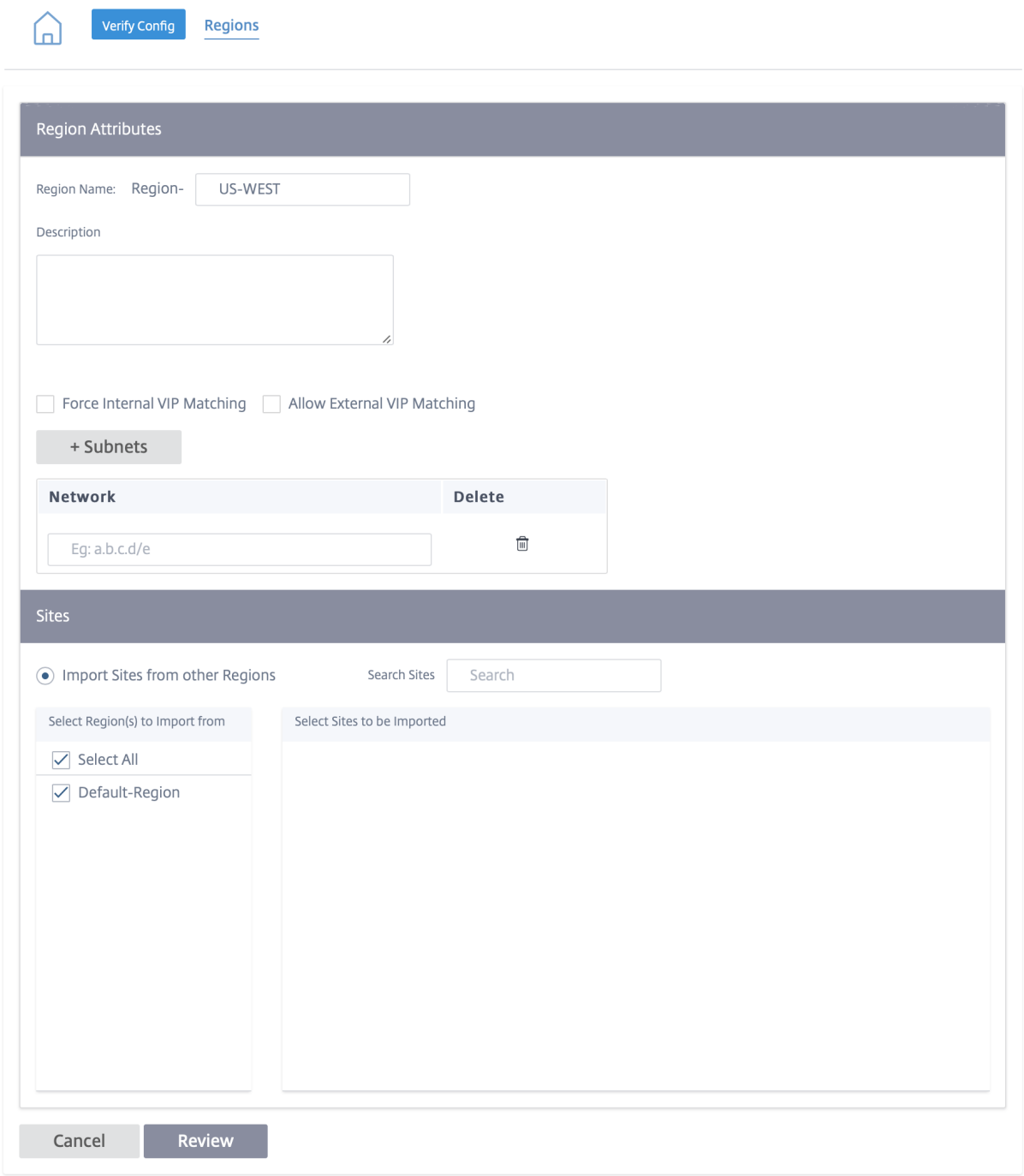
多区域网络支持分层架构，其中 MCN 控制多个 RCN。反过来，每个 RCN 控制多个分支站点。即使在多区域部署中，您也可以将 MCN 加倍作为部分站点的直接中心节点，同时让其余站点使用各自的 RCN 作为中心节点。

由 MCN 直接管理的站点，即 RCN 以及可能由 MCN 直接管理的其他一些站点，据说位于 默认 区域。在添加其他 区域之前，默认 区域将是网络的唯一区域。添加其他区域后，您可以选择“默认”选项以使用所需区域作为默认区域。

要创建区域：

1. 单击 **+** 区域。提供区域名称和描述。
2. 根据您是想要 强制内部 **VIP** 匹配还是允许外部 **VIP** 匹配启用间隔 **VIP** 匹配。
   - 强制内部 VIP 匹配：启用后，区域中的所有非私有虚拟 IP 地址都被强制与配置的子网匹配。
   - 允许的外部 VIP 匹配：启用后，允许来自其他区域的非私有虚拟 IP 地址与配置的子网匹配。
3. 单击 **+** 子网 添加子网。输入网 络 地址。网络地址是子网的 IP 地址和掩码。
4. 选择站点。
5. 单击“查看”，然后单击“保存”。新创建的区域将添加到现有的区域列表中。

> 注意
>
> 客户只能在区域内拥有静态或动态虚拟路径。



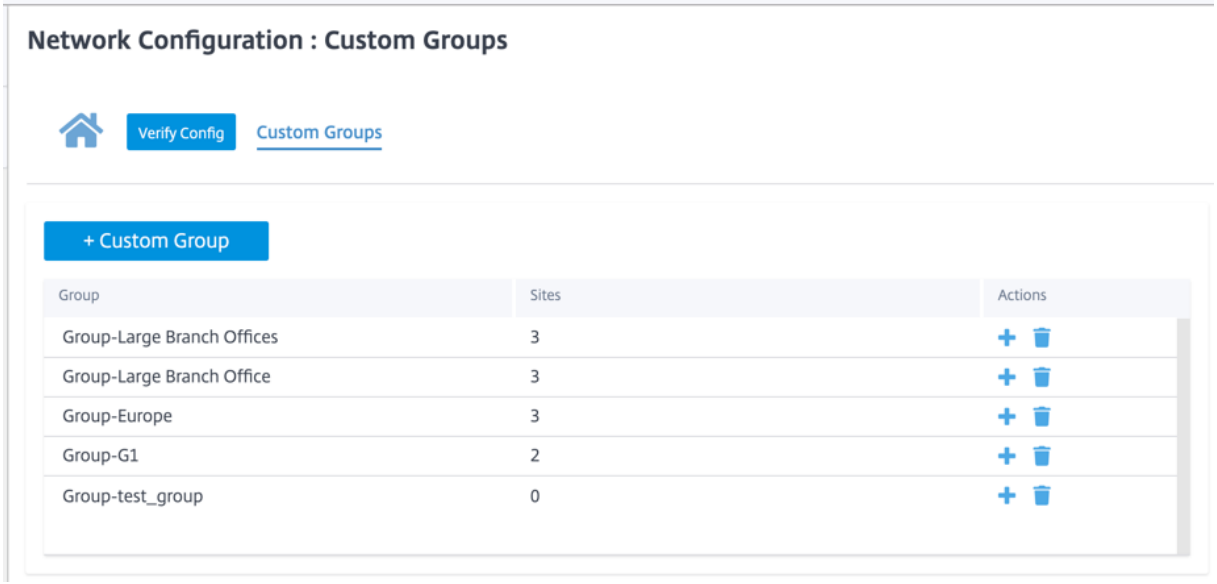
成功创建区域后，您可以在该区域下放置站点。

> 注意
>
> 无法在不同区域的分支之间建立动态虚拟路径。

单击“验证配置”以验证任何审计错误。

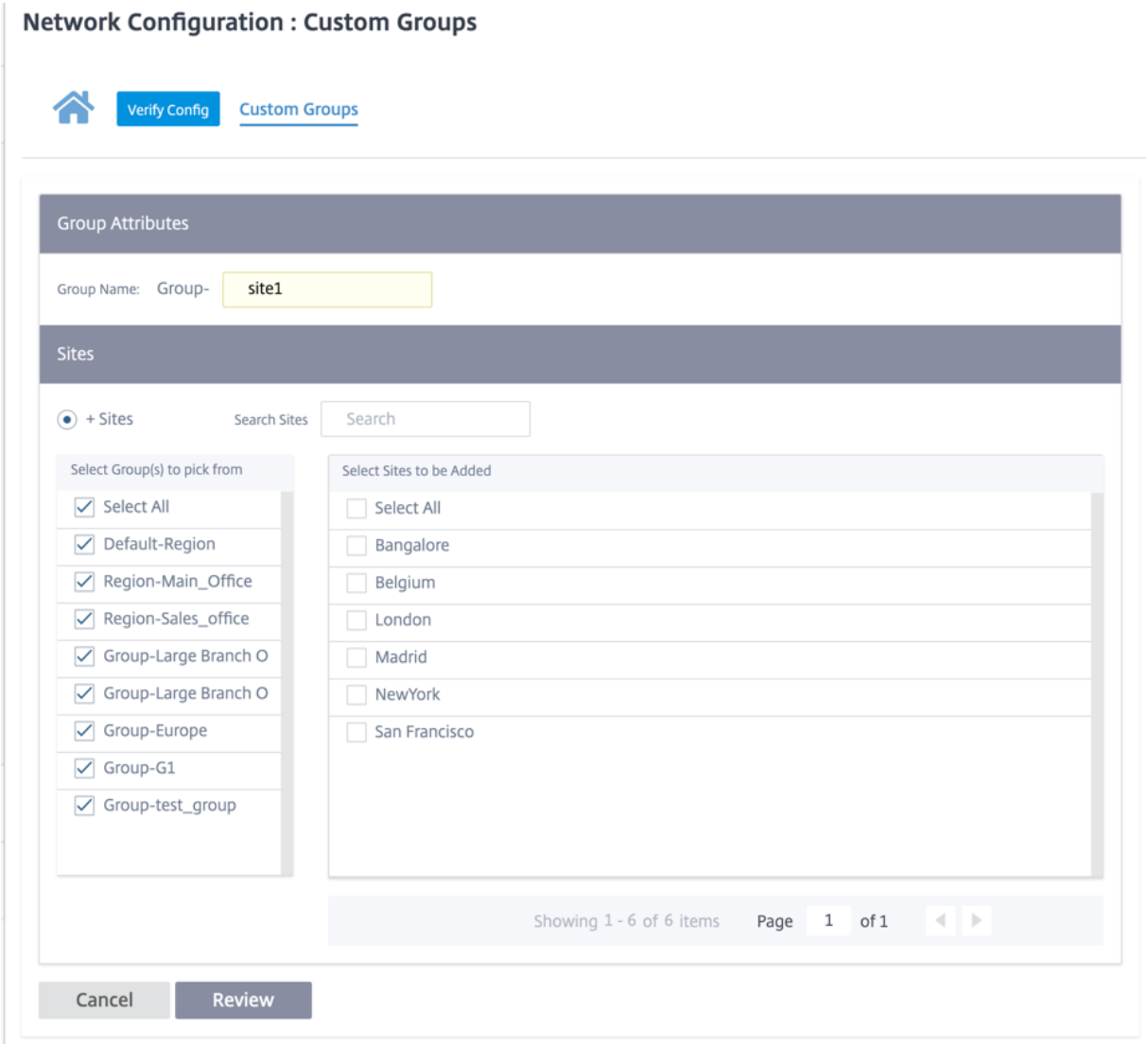
自定义群组

自定义群组 使用户可以根据需要灵活地对站点进行分组。用户可以一次性为一组站点应用策略，而不必单独处理每个站点。群组还可以用作仪表板、报告或网络配置的筛选器。与区域不同，群组在站点方面可以重叠。换句话说，相同的站点可以是多个组的一部分。



例如，用户可以创建一个名为“关键业务站 点”的群组，为所有关键业务站点配置通用策略。用户还可以作为一个组单独监控其运行状况和性能。例如，其中一些站点也可以是 大型分支机构 组的一部分。

自定义站点组 提供了一种以逻辑方式将站点分组在一起以用于报告目的的方法。您可以创建自定义群组并将站点添加到每个自定义群组。要创建自定义群组，请单击 **+** 自定义群组。提供组名称并选择或添加站点。单击“查看”，然后单击“保存”。



单击“验证配置”以验证任何审计错误。

IP 组

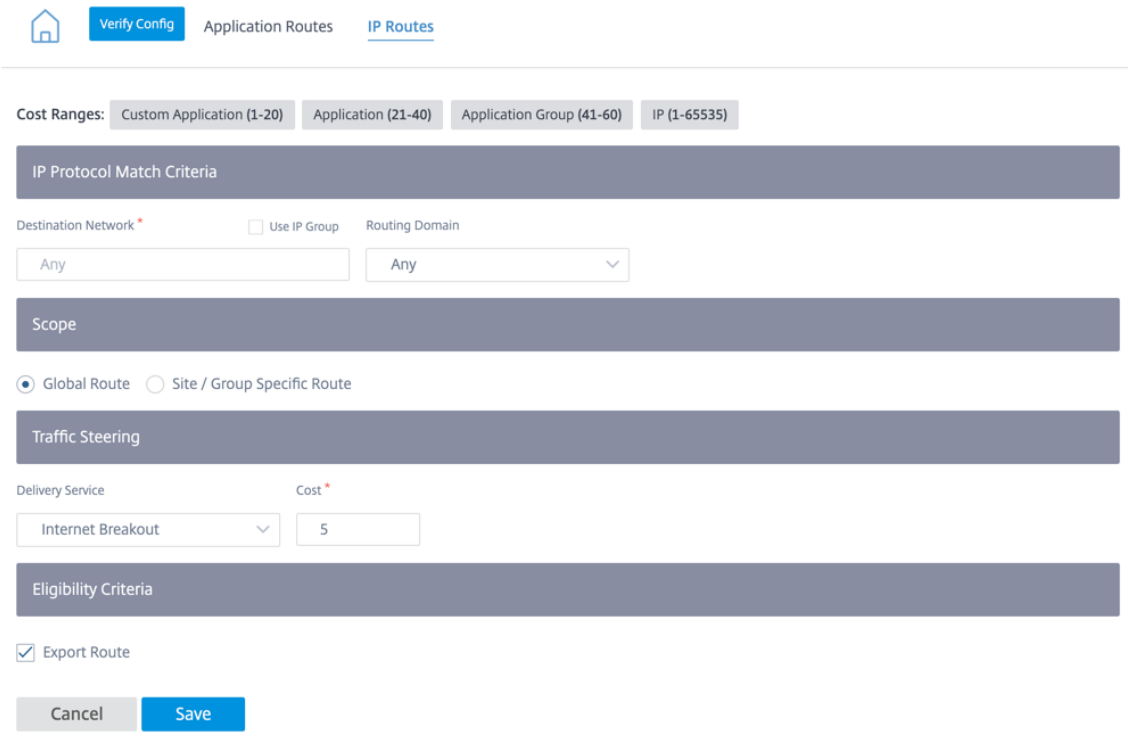
Citrix SD-WAN Orchestrator 服务引入了添加 IP 组（网络对象）的选项。使用此选项，您可以在定义路由筛选器时使用 IP 组对 **IP** 和网络地址进行分组，而不是为每个子网创建筛选器。这些组可以根据需要在配置和策略中使用，而不必每次都键入单独的 IP 地址。

您可以创建 IP 组并添加网络地址和前缀。要创建 IP 组，请选择 **IP** 组 并单击 **+ IP** 组。提供组名称。单击 **+ IP** 地址，然后输入要添加到 IP 组的 IP 地址。

单击“验证配置”以验证任何审计错误

以下功能使用 IP 组：

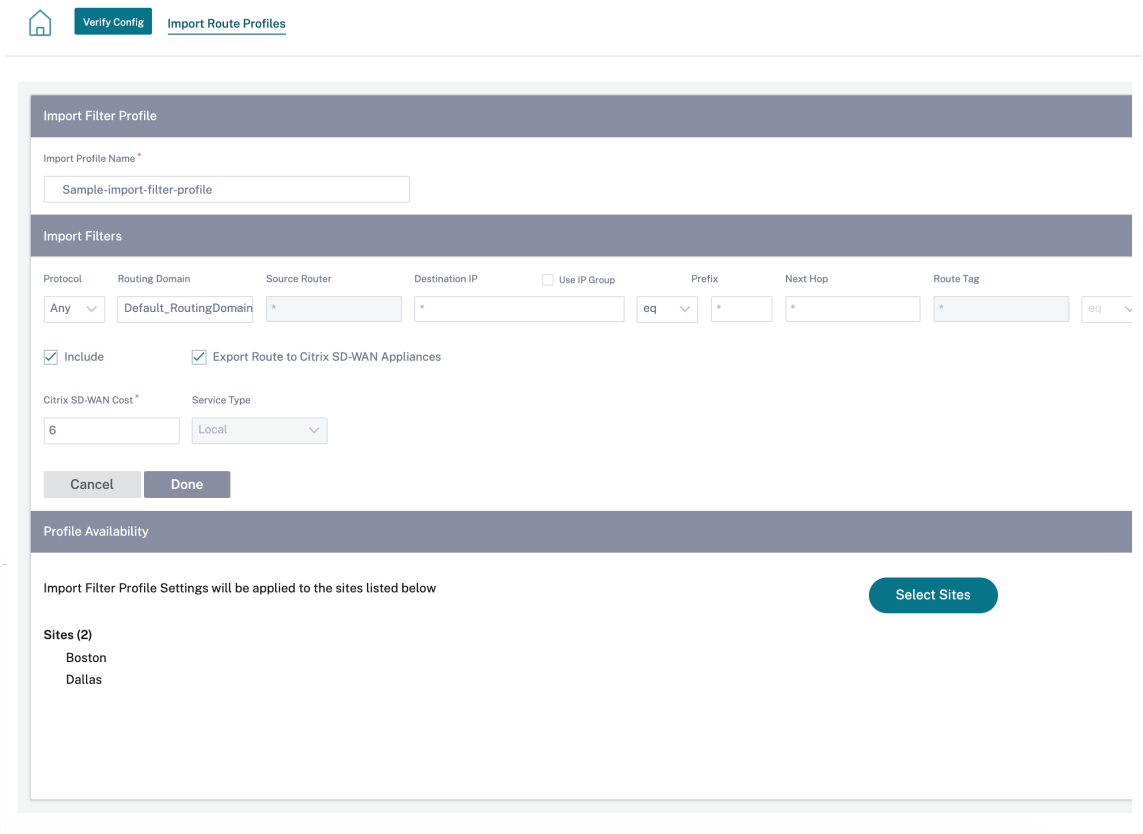
- 创建 **IP** 路由：您可以添加目标网络或启用“使用 **IP** 组”复选框来选择现有 IP 组。有关更多信息，请参阅 IP 组。



- 导入路由配置文件：创建导入筛选配置文件时，您可以从网络上可用的 IP 组列表中进行选择。

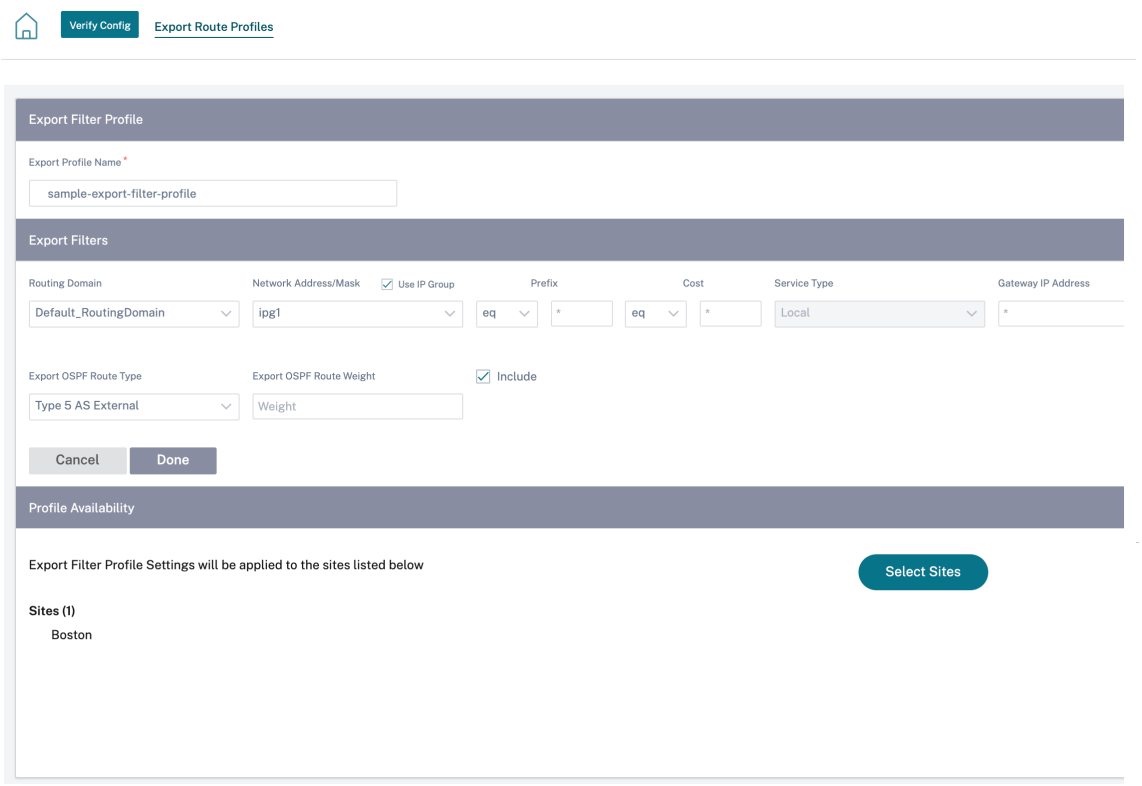
  您可以添加目标网络或启用“使用 **IP** 组”复选框来选择现有 IP 组。

  有关更多信息，请参阅 导入路由配置文件。



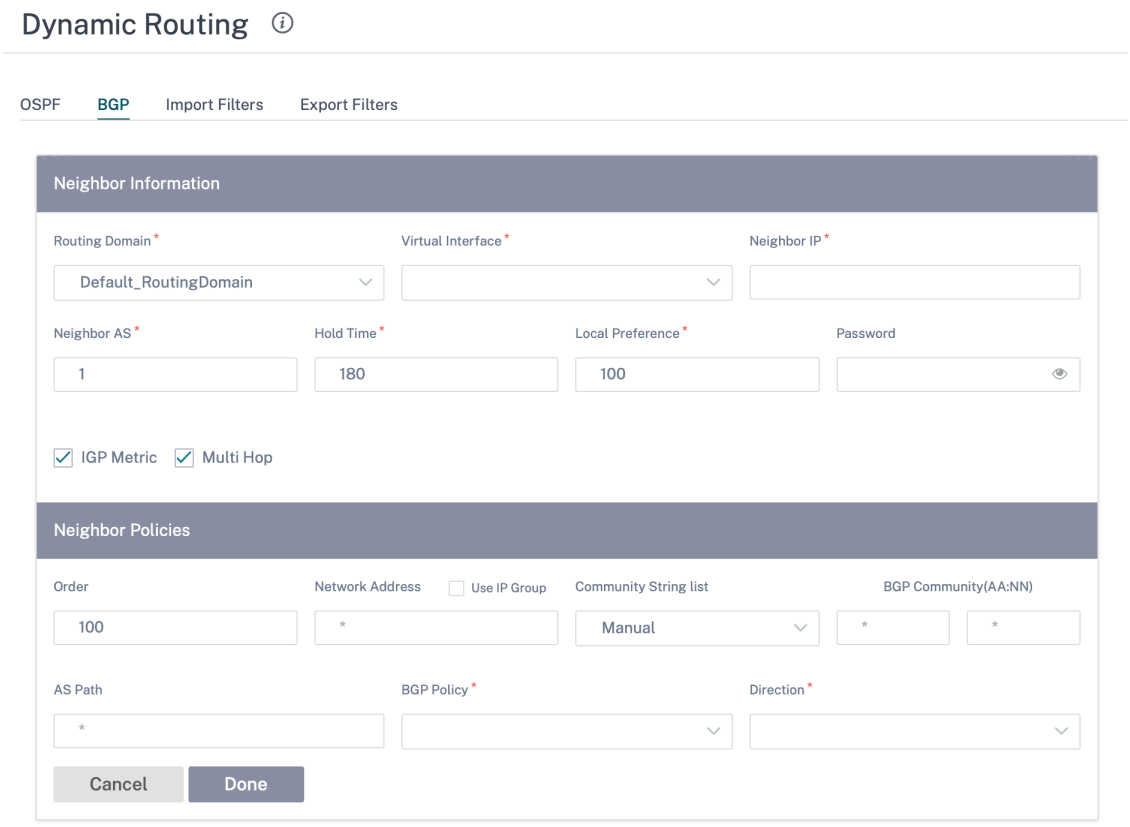
- 导出路由配置文件：创建导出筛选配置文件时，可以添加网络地址掩码或启用“使用 **IP** 组”复选框以选择现有 IP 组。

  有关更多信息，请参阅 导出路由配置文件。



- **BGP** 邻居策略：在为相邻路由器添加已配置的 BGP 策略时，可以添加网络地址或启用“使用 **IP** 组”复选框来选择现有 IP 组。

  有关更多信息，请参阅 BGP。



应用程序设置和群组

October 21, 2022

本部分允许用户自定义应用程序、将应用程序分组以便在策略中使用、QoS 配置文件以及 DNS 设置。

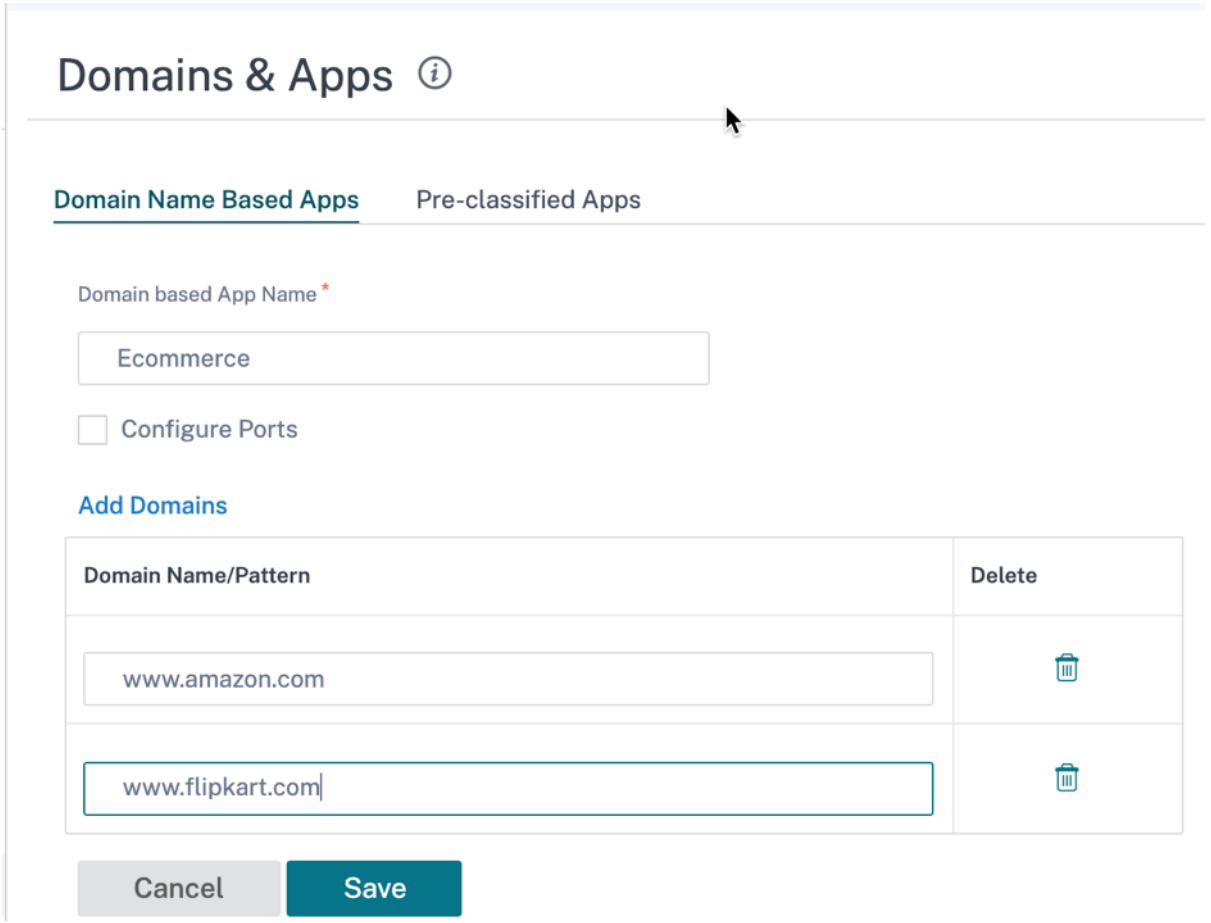
您可以为预定义和自定义 应用程序定义应用程序组。应用程序组 包含在定义安全策略时需要类似处理的应用程序。

在定义诸如 应用程序指导或防火墙规则之类的策略时，可以经常重复使用应用程序组。它无需为每个应用程序创建多个条目。同样，在使用任何应用程序服务时，Application Groups 支持具有唯一名称的常见应用程序，以便简化和一致地重复使用。

要查看 应用程序组，请导航到 配置 **>** 应用程序设置和组。

域和应用程序

您可以根据域名 和应用程序页面的已发布应用程序列表中没有的域名创建内部应用程序。要基于域名创建应用程序，请在网络级别导航到 应用程序设置和群组 **>** 域名和应用程序 **>** 基于域名的应用程序 选项卡，然后单击 新建基于域名的应用程序。输入应用程序名称并添加域名或模式。您可以在开头输入完整域名或使用通配符。

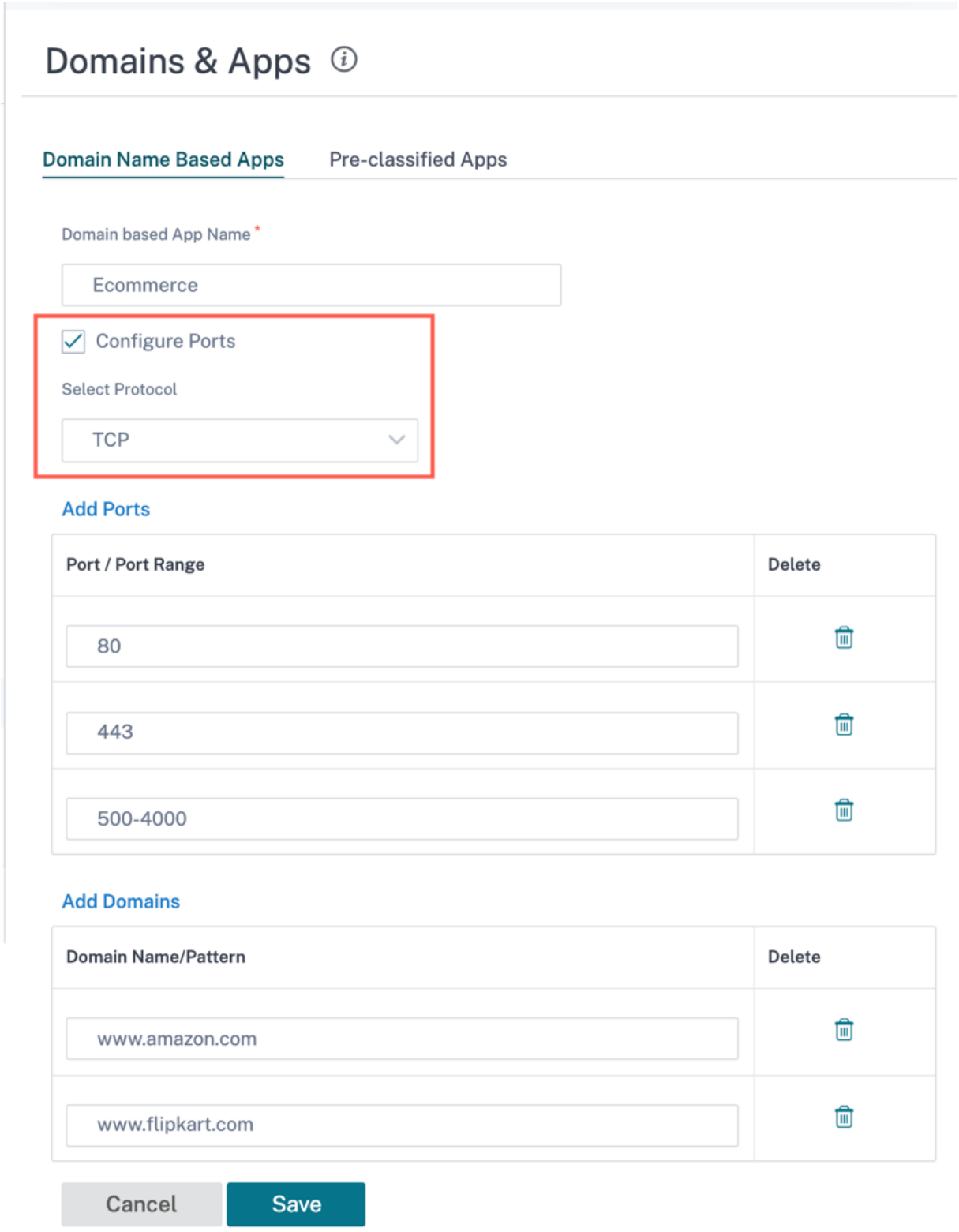


所有基于域名的应用程序都可以在应用程序 路由、应用程序规则和防火墙策略中看到。

从 Citrix SD-WAN 11.4.2 版本开始，“配置端口”复选框选项在“基于域名的应用程序”下可用。启用“配置端口”复选框后，可以灵活地为基于域的应用程序配置一组多个端口、端口范围和协议 (TCP/UDP/Any)。

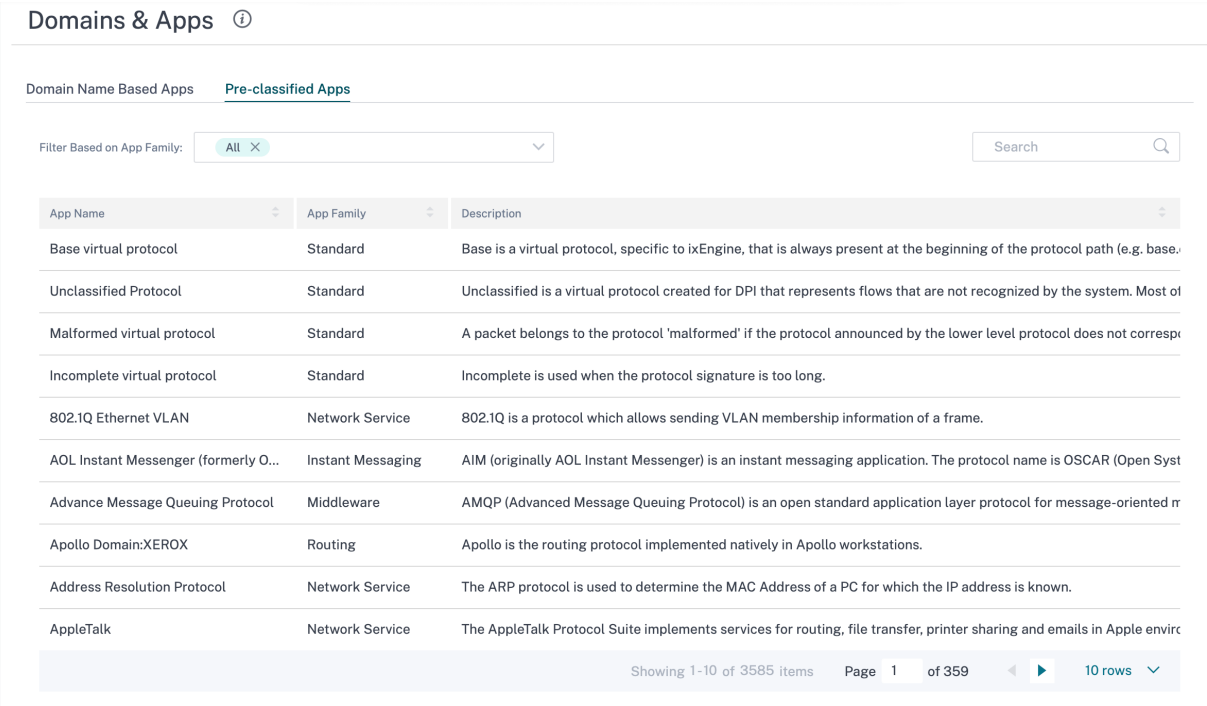
以前，应用程序下分组的域支持端口 80 和 443 以及协议 **Any**。如果清除“配置端口”复选框，则会看到相同的行为。默认情况下，“配置端口”复选框处于禁用状态。

选中“配置端口”复选框时，可以根据需要编辑、添加或删除任何端口或端口范围以及 TCP、UDP 或 Any 等协议选择。默认情况下，协议值设置为 An **y** ，端口设置为 **80** 和 **443**。



您还可以在“预 分类应用程序”选项卡下查看预定义应用程序 列表。您可以使用搜索栏 搜索 特定的应用程序，也可以

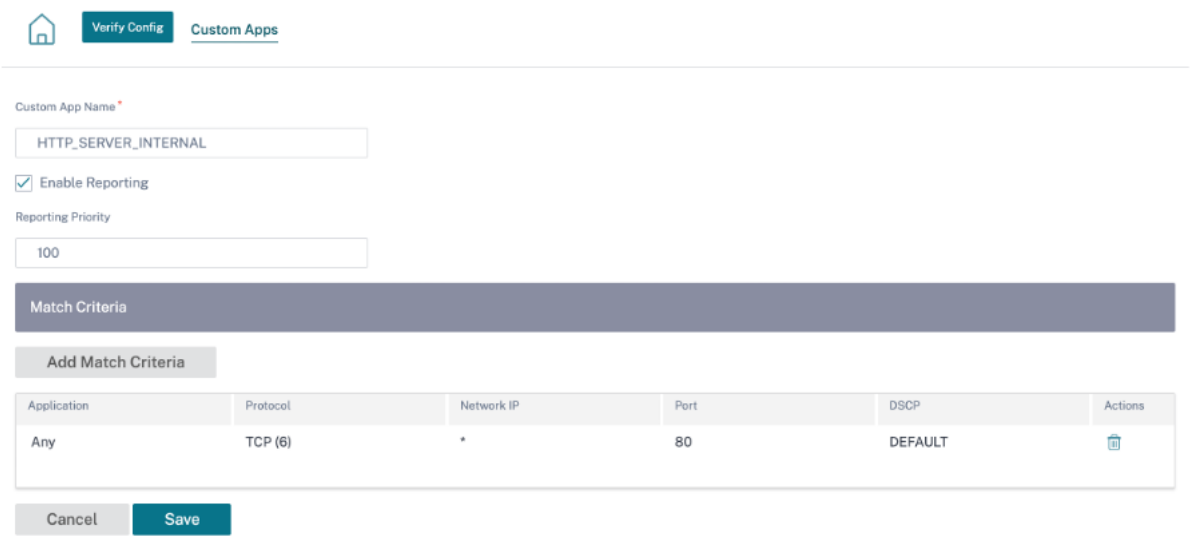
根据应用程序系列筛选列表。



自定义应用程序

自定义应用程序 用于创建内部应用程序或 IP 端口组合，这些组合在已发布应用程序列表中不可用。管理员需要定义一个基于 IP 协议的自定义应用程序，该应用程序可以根据需要在多个策略中使用，而不必每次都提及 IP 地址和端口号的详细信息。

要创建自定义应用程序，请在网络级别导航到“应用程序设置和群组”**>**“自定义应用程序”，单击“**+** 自定义应用程序”并提供自定义应用程序的名称。指定匹配标准，例如 IP 协议、网络 IP 地址、端口号和 DSCP 标记。符合此条件的数据流被分组为自定义应用程序。

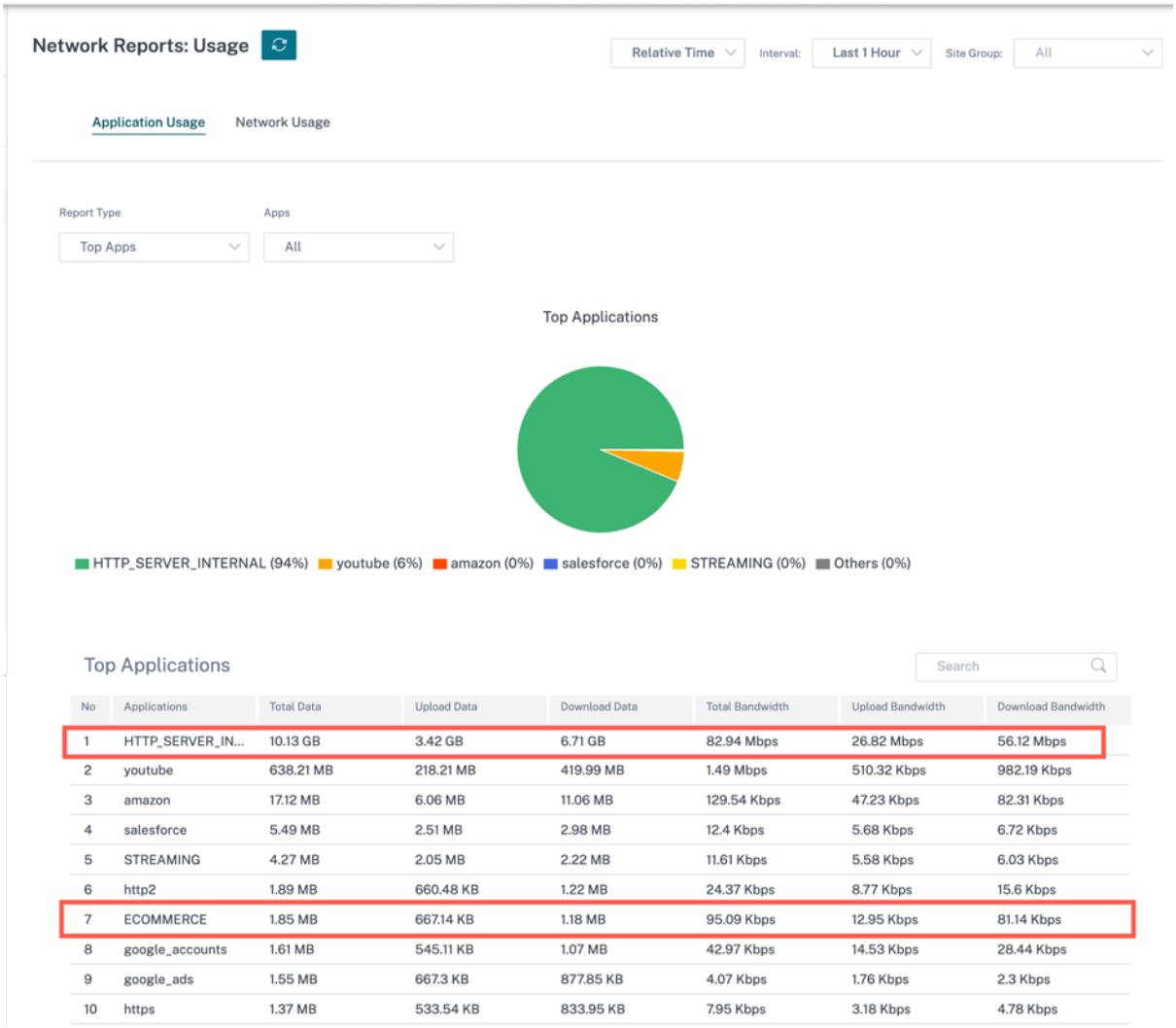


保存后，自定义应用程序将显示在列表中，可以根据需要进行编辑或删除。

为基于 IP 协议的自定义应用程序和应用程序组添加了“启用报告”复选框。必须选中“启用报告”复选框并提供报告优先级。

选中“启用报告”复选框后，您可以在“报告”> “使用情况”下查看 IP 自定义应用程序流 量。

报告优先级是为报告选择基于 IP 协议的自定义应用程序或应用程序组的顺序。当存在多个匹配项且启用报告时，选择用于报告的高优先级自定义应用程序或应用程序组会有所帮助。例如，如果自定义应用程序的报告优先级设置为 1，则表示该自定义应用程序在报告中获得最高优先级。而如果报告优先级设置为 100，则自定义应用程序在报告中的优先级要低得多。

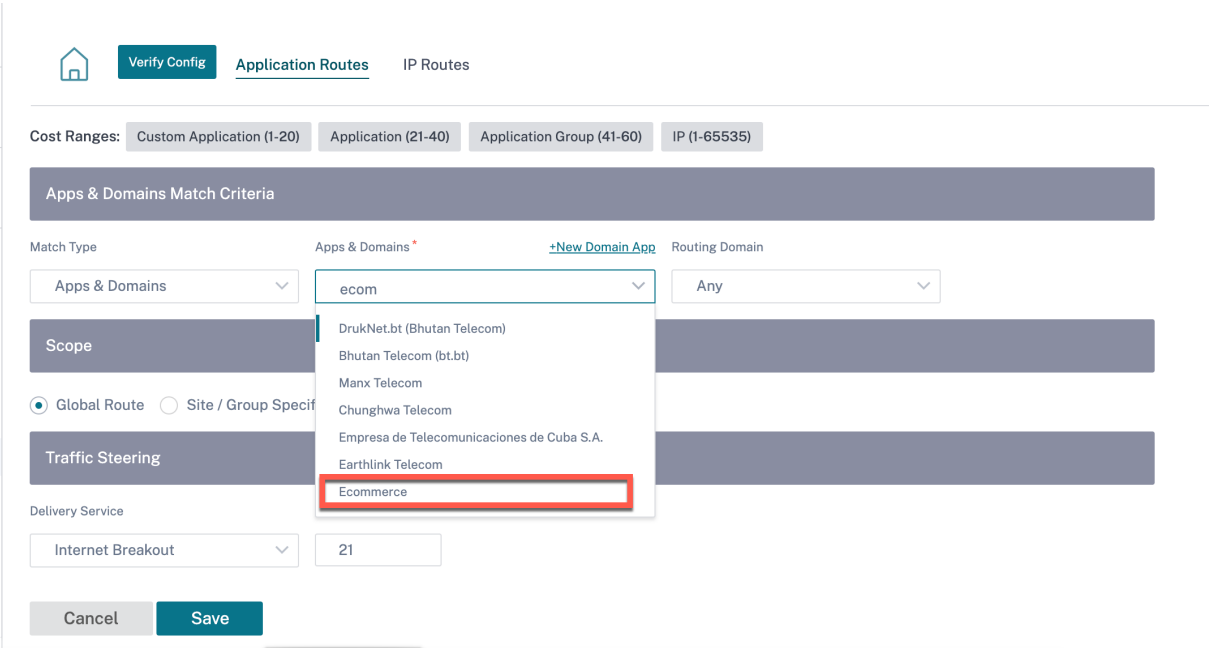


No	Applications	Total Data	Upload Data	Download Data	Total Bandwidth	Upload Bandwidth	Download Bandwidth
1	HTTP_SERVER_IN...	10.13 GB	3.42 GB	6.71 GB	82.94 Mbps	26.82 Mbps	56.12 Mbps
2	youtube	638.21 MB	218.21 MB	419.99 MB	1.49 Mbps	510.32 Kbps	982.19 Kbps
3	amazon	17.12 MB	6.06 MB	11.06 MB	129.54 Kbps	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

注意

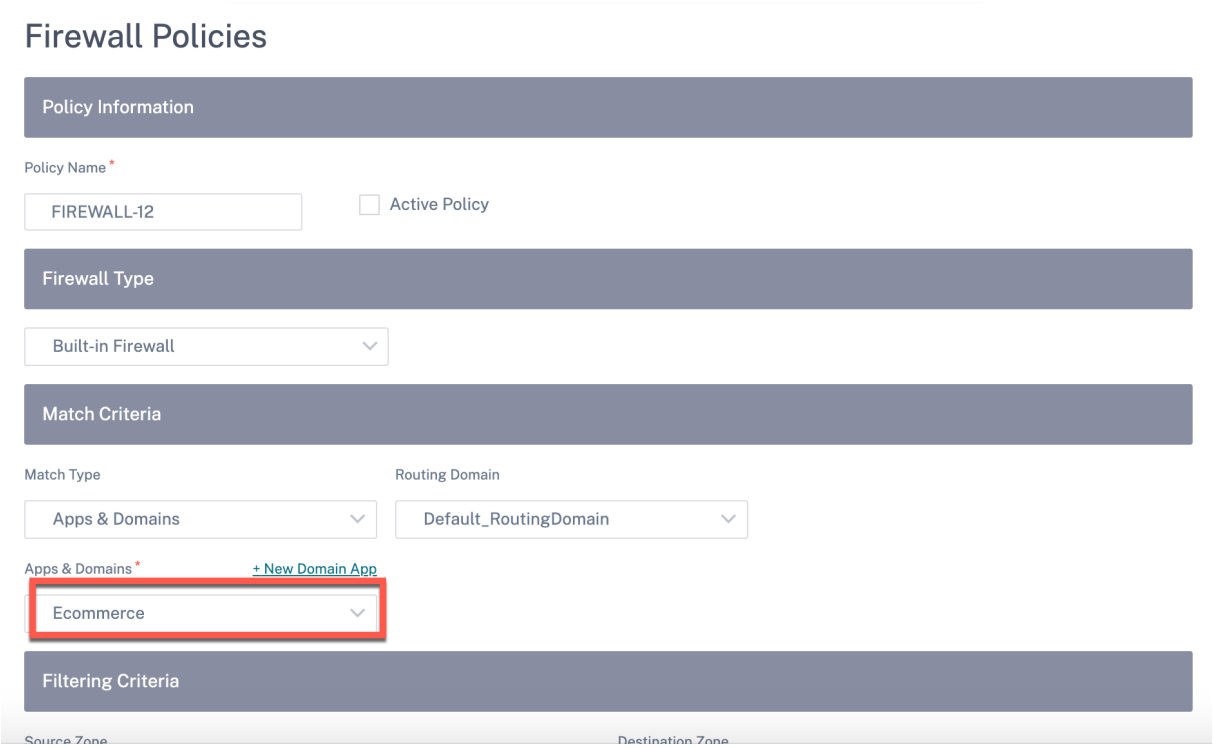
- 要使用基于域名的 应用程序，在创建应用程序路由、**QoS** 策略和防火墙策略时，必须将应用程序和域 列为匹配标准。
- 要使用自定义应用程序，在创建应用程序路由、QoS 策略和防火墙策略时，必须将 自定义 应用程序列为匹配条件。

创建自定义应用程序后，要执行应用程序路由，请导航到路由 **>** 路由策略 **> +** 应用程序路由，从“匹配类型”下拉列表中选择“自定义应用程序”。同样，对于基于域名的 应用程序，从“匹配类型”下拉列表中选择“应用程序和域”。

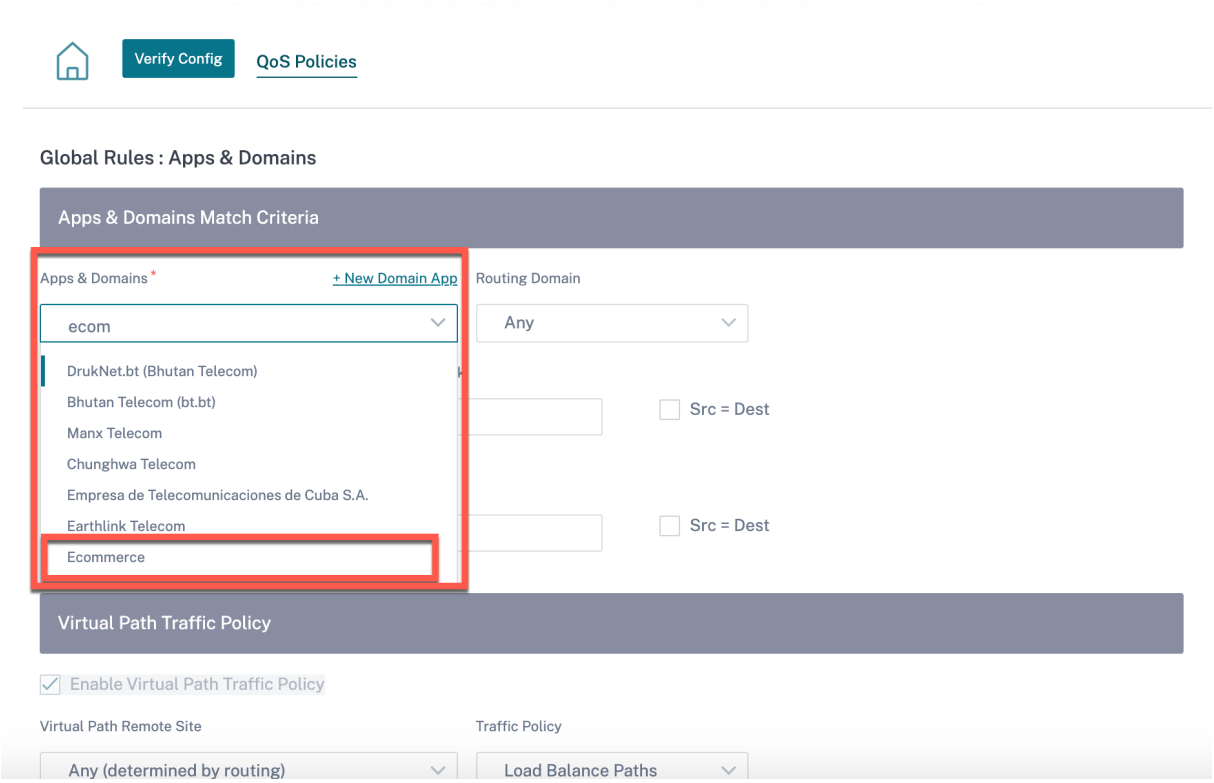


在创建 **IP** 协议 自定义应用程序时，您还可以在匹配条件下选择基于域名的应用程序。

同样，要查看“防火墙策略”下的自定义应用程序，请导航到“安全”**>** “防火墙策略”。该应用程序可用于任何类型的策略（全局覆盖/站点特定/全局策略）。单击“创建新规则”，在“匹配条件”下，从“匹配类型”下拉列表中选择“自定义应用程序”。要查看基于域名的 应用程序，请从“匹配类型”下拉列表中选择“应用程序和域”。



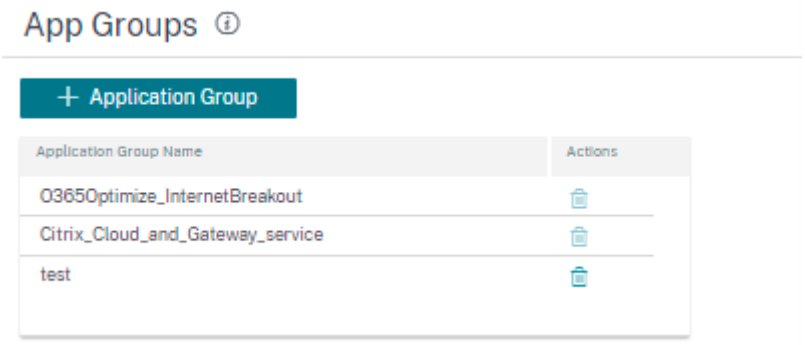
您可以在“全局规则”或“站点/组特定规则”下查看基于域名的自定义应用程序。要查看基于域名的应用程序，请导航到 **QoS > QoS** 策略 **>** 全局规则 **>** 应用程序规则 **> +** 应用程序规则，然后从“应用程序和域”下拉列表中选择所需的基于 域名的应用程序。要查看自定义应用程序，请导航到 **QoS > QoS** 策略 **>** 全局规则 **>** 自定义应用程序规则 **> +** 自定义应用程序规则，然后从“自定义应用程序”下拉列表中选择所需的 自定义应用程序。



单击“验证配置”以验证任何审计错误。

应用程序组

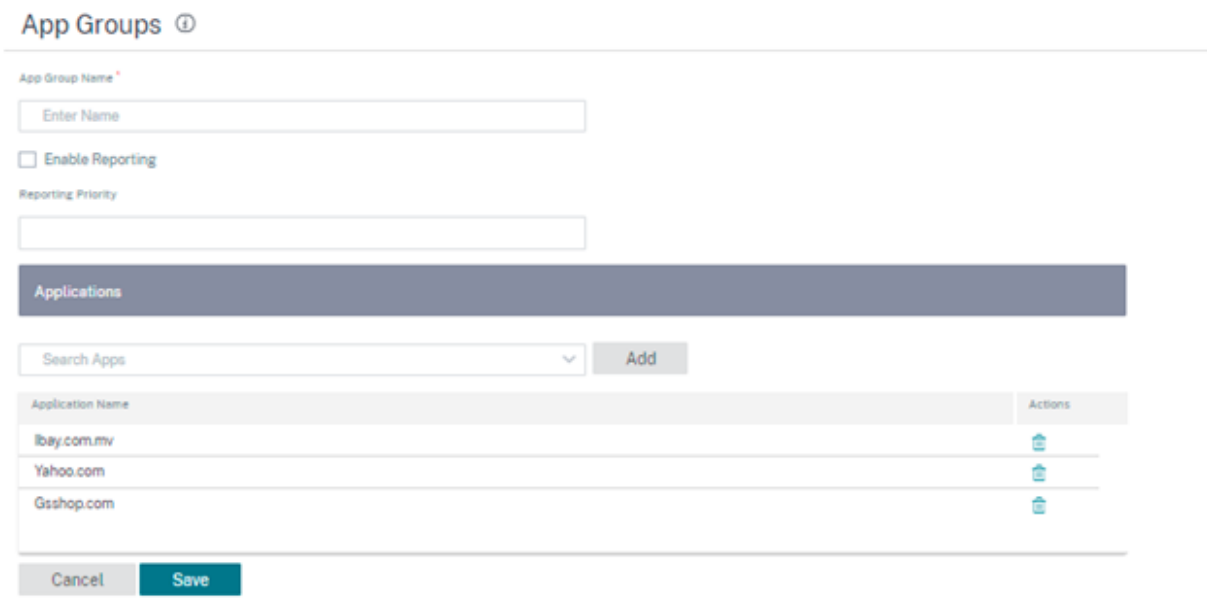
应用程序组 可帮助管理员将相似的应用程序组合在一起以用于通用策略，而不必为每个单独的应用程序创建策略。



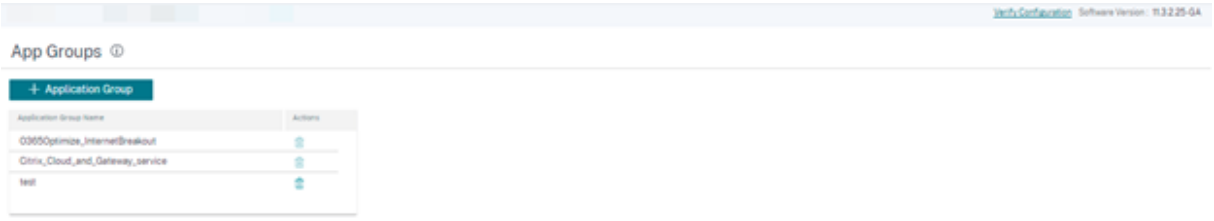
您可以使用“添加应用程序组”选项创建应用程序组。您可以根据应用程序角色在创建策略时引用同一个应用程序组。为特定组定义的策略将应用于与特定类别匹配的每个应用程序。

例如，您可以将 应用程序组 创建为 社交 网络，然后将 Facebook、LinkedIn 和 Twitter 等社交网络添加到该组中，为社交网络应用程序定义某些策略。

要创建 应用程序组，请指定组名称，搜索并从“应用程序”列表中添加 应用程序。
您可以随时返回编辑设置或根据需要删除 应用程序组。

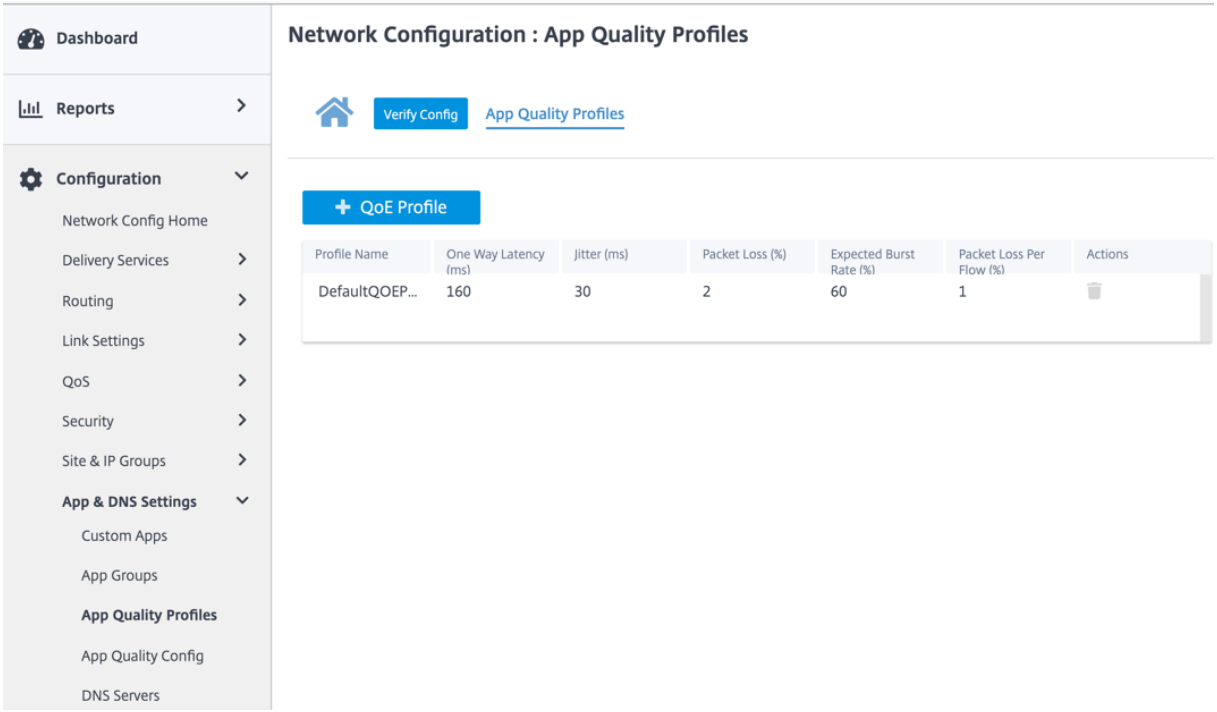


单击“配置”> “应用程序设置和组”**>** “应用程序组”页面上的“验证 ****** 配置”以验证任何审计错误。******



应用程序质量档

此部分使您能够查看和创建应用程序质量配置文件。



应用程序 **QoE** 是 SD-WAN 网络中应用程序体验质量的度量标准。它测量通过两个 SD-WAN 设备之间的虚拟路径的应用程序的质量。

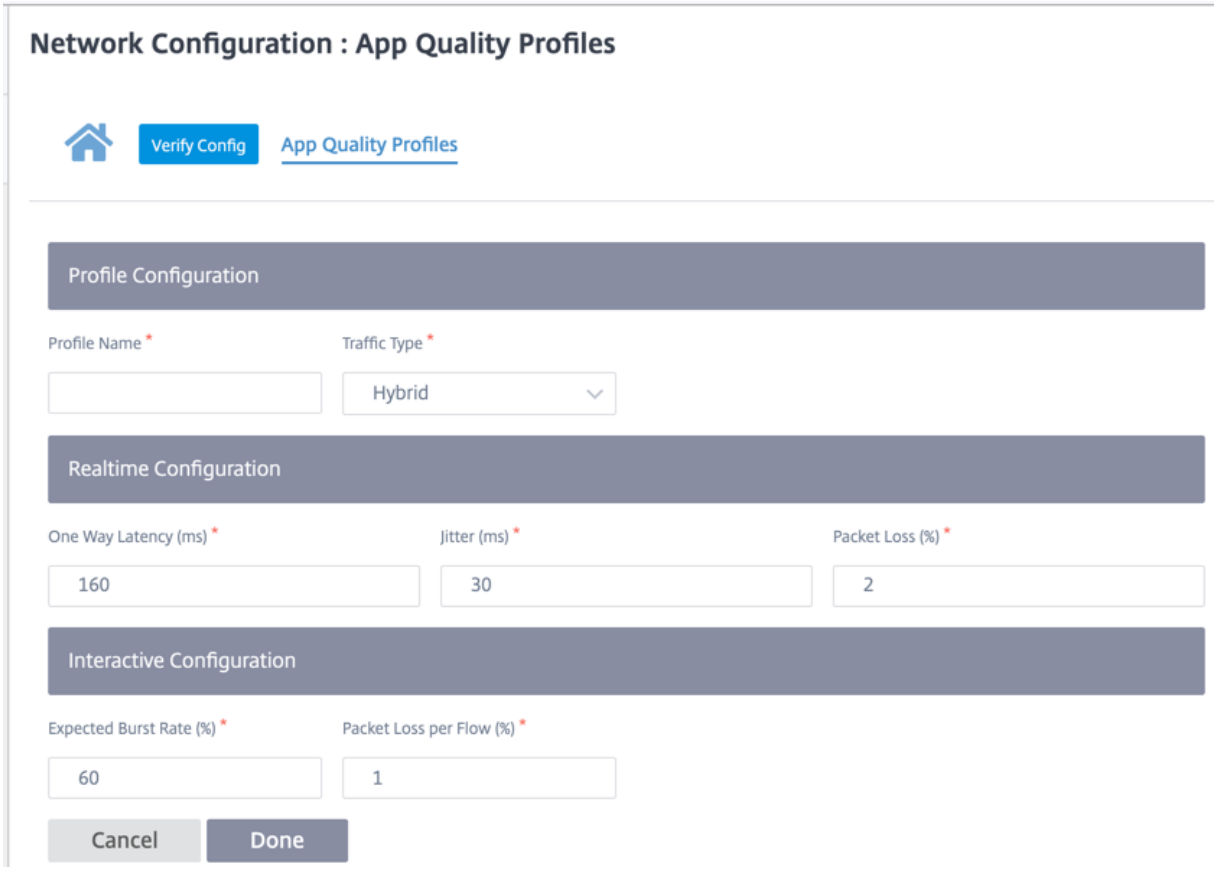
应用程序 QoE 分数是介于 0 到 10 之间的值。它所属的分数范围决定了应用程序的质量。

质量	范围
良好	8–10
一般	4–8
不佳	0–4

应用程序 QoE 分数可用于衡量应用程序的质量并识别有问题的趋势。

配置式配置

单击 **+ QoE** 配置文件 创建 QoE 配置文件，指定配置文件名称，然后从下拉列表中选择流量类型。



实时配置

您可以使用 QoE 配置文件定义实时和交互式设备的质量阈值，并将这些配置文件映射到应用程序或应用程序对象。

实时应用程序的应用程序 QoE 计算使用 Citrix 创新技术，该技术来自 MOS 分数。

默认阈值为：

- 延迟阈值（毫秒）：160
- 抖动阈值（毫秒）：30
- 数据包丢失阈值 (%)：2

满足延迟、损耗和抖动阈值的实时应用程序流被认为具有良好的质量。

实时应用的 QoE 取决于达到阈值的流量百分比除以流量样本总数。

实时 QoE =（达到阈值的流量样本数量/流量样本总数）* 100

它被表示为 QoE 分数范围从 0 到 10。

交互式配置

交互式应用程序的应用程序 QoE 使用基于丢包和突发速率阈值的 Citrix 创新技术。

交互式应用程序对数据包丢失和吞吐量很敏感。因此，我们测量流中的数据包丢失百分比以及入口和出口流量的突发率。

可配置阈值为：

- 数据包丢失百分比。
- 预期出口突发率与入口突发率的比较。

默认阈值为：

- 数据包丢失阈值：1%
- 爆发率：60%

如果满足以下条件，则流程质量良好：

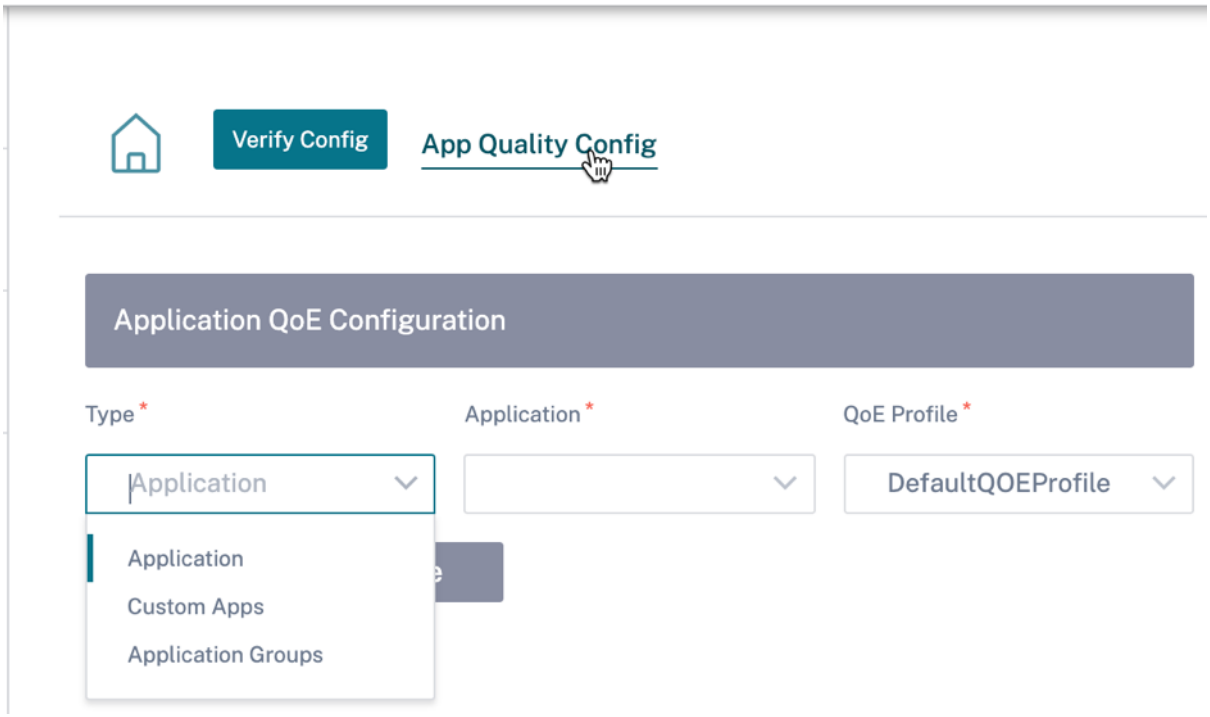
- 流的百分比损失小于配置的阈值。
- 出口突发率至少是已配置的入口突发率百分比。

应用质量配置

将应用程序或应用程序对象映射到默认或自定义 QoE 配置文件。您可以为实时和交互式流量创建自定义 QoE 配置文件。

单击 **+QoE** 配置 以创建自定义 QoE 配置文件：

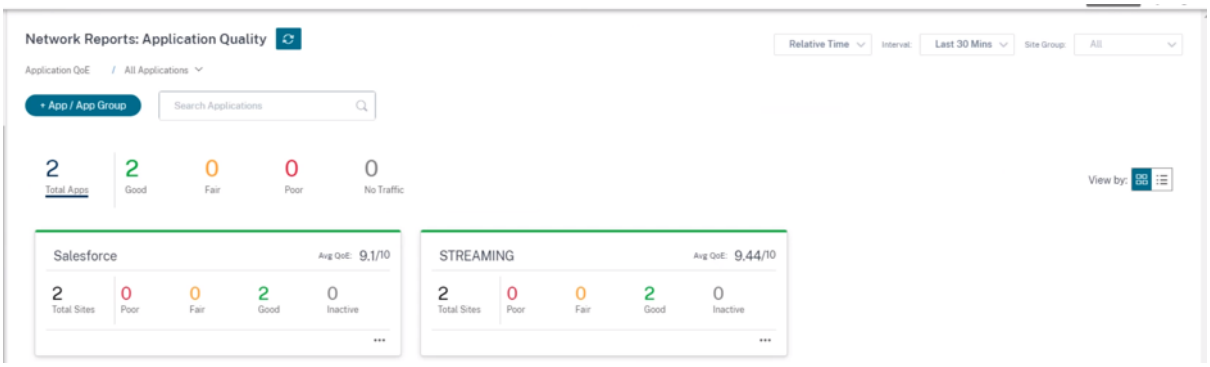
- 类型：选择 DPI 应用程序或应用程序对象（应用程序、自定义应用程序和应用程序组）。
- 应用程序：根据选定的类型搜索并选择应用程序或应用程序对象。
- **QoE** 配置文件：选择要映射到应用程序或应用程序对象的 QoE 配置文件。



单击完成。

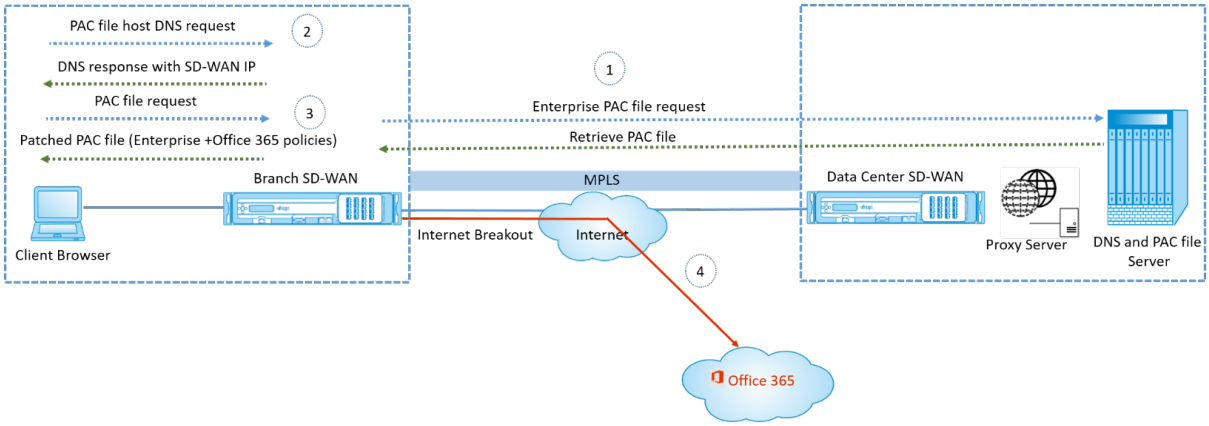
单击“验证配置”以验证任何审计错误。

使用自定义应用程序类型配置应用程序 QoE 后，将在报告 **>** 应用程序质量下自动生成相关的应用程序报告磁贴。与所选应用程序匹配的任何流量都会经过自定义应用程序的虚拟路径。



PAC 文件自定义的工作原理

理想情况下，企业网络主机 PAC 文件在内部 Web 服务器上，这些代理设置通过组策略分发。客户端浏览器从企业 Web 服务器请求 PAC 文件。Citrix SD-WAN 设备为启用 Office 365 分组的站点提供自定义 PAC 文件。



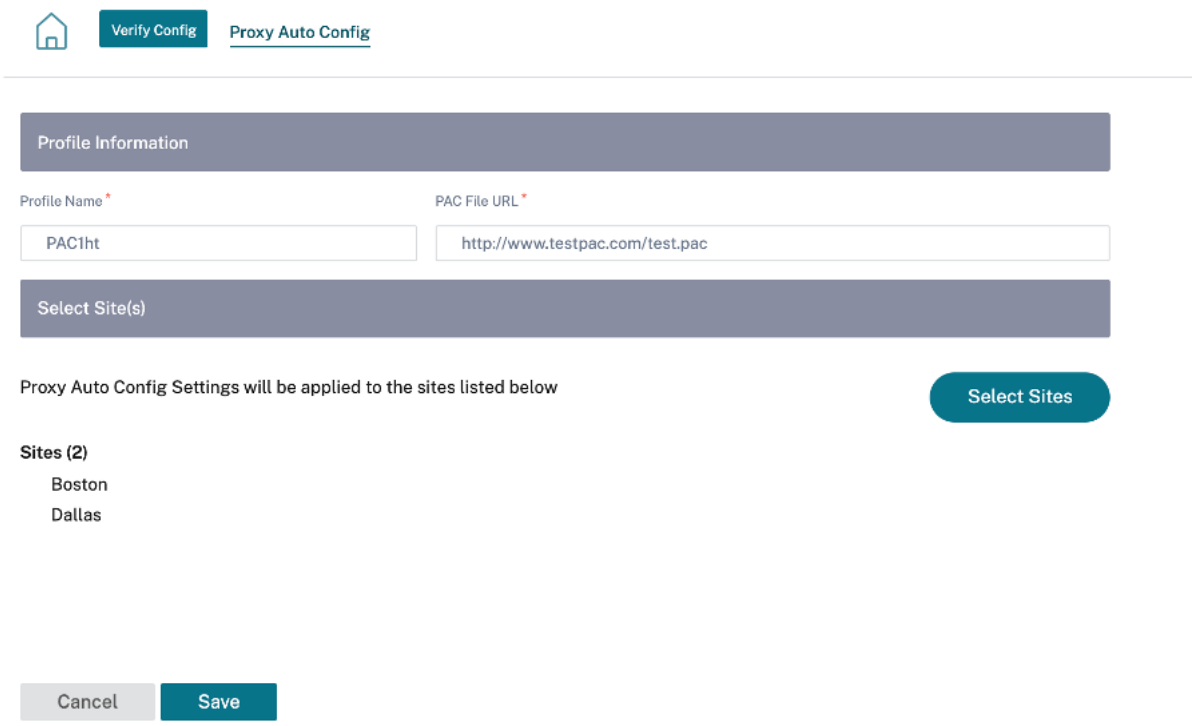
1. Citrix SD-WAN 定期从企业 Web 服务器请求并检索企业 PAC 文件的最新副本。Citrix SD-WAN 设备将 Office 365 URL 修补到企业 PAC 文件。企业 PAC 文件预计将具有占位符（SD-WAN 特定标签），其中 Office 365 URL 无缝修补。
2. 客户端浏览器向企业 PAC 文件主机发出 DNS 请求。Citrix SD-WAN 拦截代理配置文件 FQDN 的请求，并使用 Citrix SD-WAN VIP 进行响应。
3. 客户端浏览器请求 PAC 文件。Citrix SD-WAN 设备在本地提供修补的 PAC 文件。PAC 文件包括企业代理配置和 Office 365 URL 排除策略。
4. 在收到 Office 365 应用程序的请求后，Citrix SD-WAN 设备将直接执行互联网突围。

必备条件

1. 企业必须托管 PAC 文件。
2. PAC 文件必须有占位符 *SDWAN_TAG* 或者一次出现修补 Office 365 URL 的 `findproxyforurl` 函数。
3. PAC 文件 URL 必须基于域，而不是基于 IP。
4. PAC 文件仅通过受信任的身份 VIP 提供。
5. Citrix SD-WAN 设备必须能够通过其管理界面下载企业 PAC 文件。

配置代理自动配置

在 SD-WAN Orchestartor 用户界面中，在网络级别导航到 配置 > 应用程序设置和群组 > 代理自动配置，然后单击 **+ PAC** 文件配置文件。



输入 PAC 文件配置文件的名称，提供企业 PAC 文件服务器的 URL。Office 365 突破规则动态修补到企业 PAC 文件。

选择应用 PAC 文件配置文件的站点。如果每个站点有不同的 URL，请为每个站点创建不同的配置文件。

限制

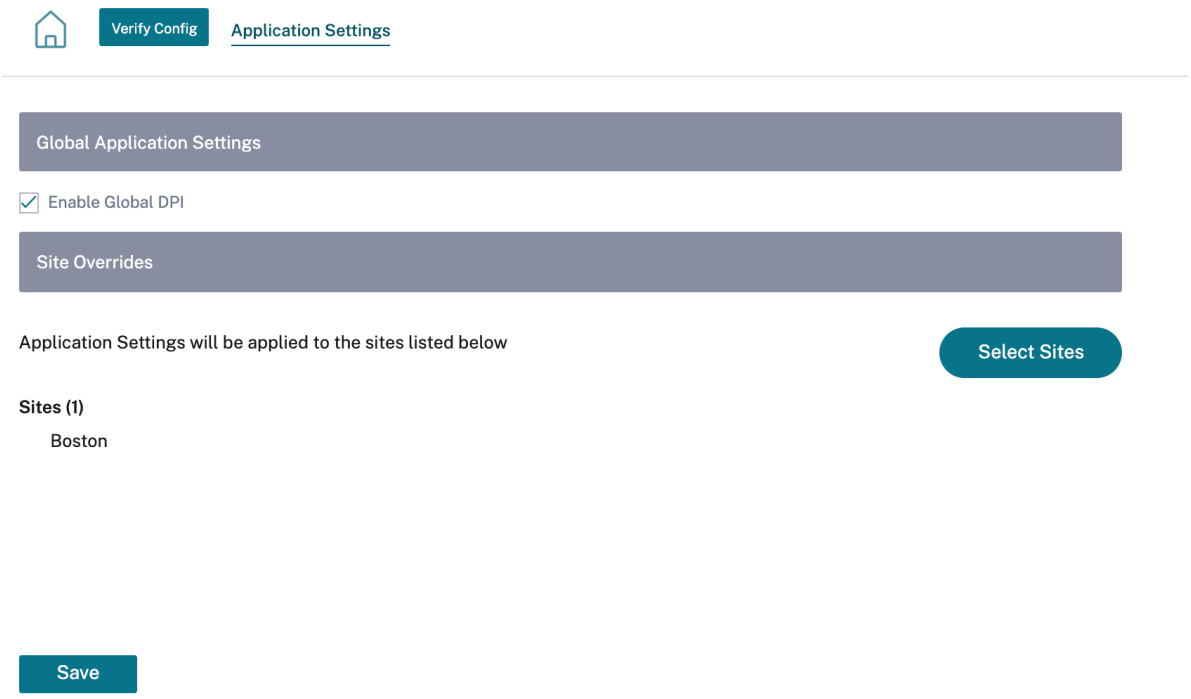
- 不支持 HTTPS PAC 文件服务器请求。
- 不支持网络中的多个 PAC 文件，包括路由域或安全区域的 PAC 文件。
- 不支持从头在 Citrix SD-WAN 上生成 PAC 文件。
- 不支持通过 DHCP 进行 WPAD。

DPI 设置

Citrix SD-WAN 设备执行深度数据包检查 (DPI) 来识别应用程序并对其进行分类。DPI 库可识别成千上万的商业应用程序。它可实现应用程序的实时发现和分类。SD-WAN 设备使用 DPI 技术分析传入的数据包，并将流量分类为属于特定应用程序或应用程序系列。

默认情况下，对网络中的所有站点启用 DPI。禁用 DPI 将停止设备上的 DPI 分类功能。您不能再使用 DPI 分类的应用程序/应用程序类别来配置防火墙、QoS 和路由策略。您也无法查看热门应用程序和应用程序类别报告。

要禁用全局 DPI，请在网络级别导航到 配置 **>** 应用程序设置和群组 **> DPI** 设置，然后清除“启用全局 **DPI** ”复选框选项。



您还可以选择仅通过覆盖全局 DPI 设置来禁用某些站点的 DPI。要禁用选定站点的 DPI，请将这些站点添加到“站点覆盖”列表中。

配置文件和模板

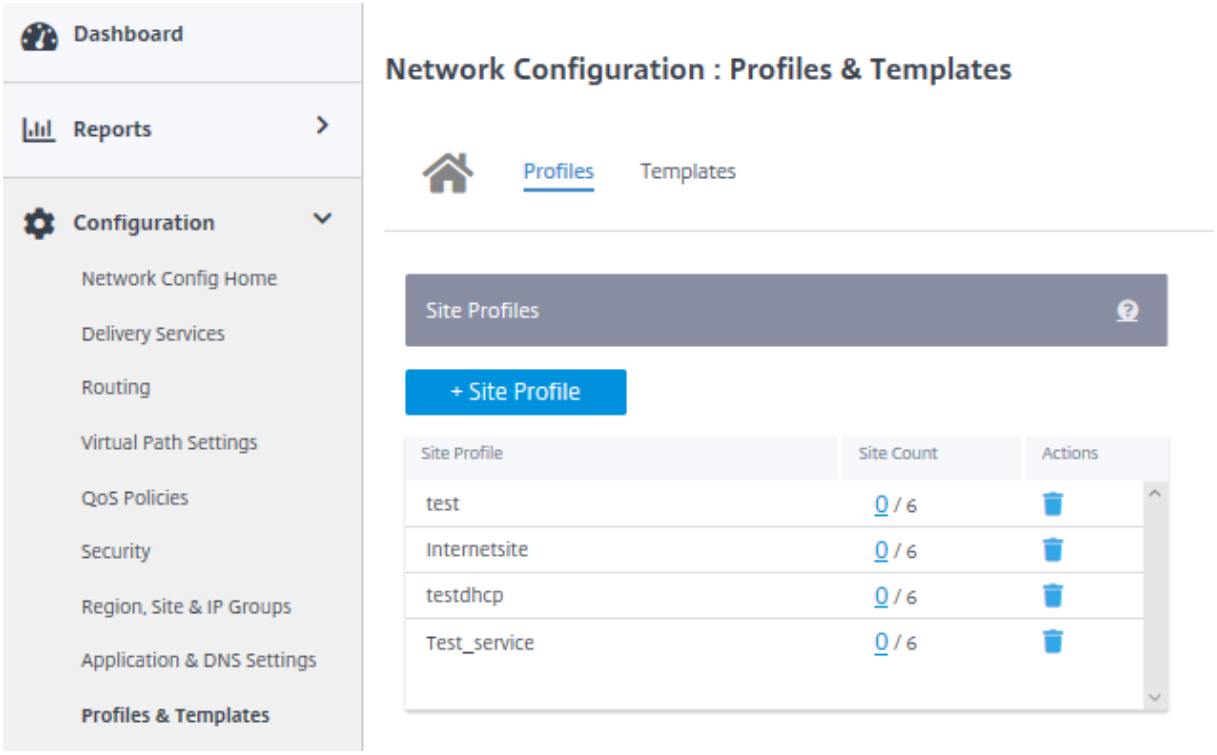
October 21, 2022

配置文件是 实时配置模板。常规模板有助于创建新实体。但是，一旦创建了模板，模板中的后续更改将不适用于使用基本模板创建的现有实体。配置文件作为实时中央主实体。所有子实体不仅在创建期间，而且在配置文件的整个生命周期内都从配置文件继承。与配置文件关联的所有子实体都会自动继承配置文件中所做的任何更改。

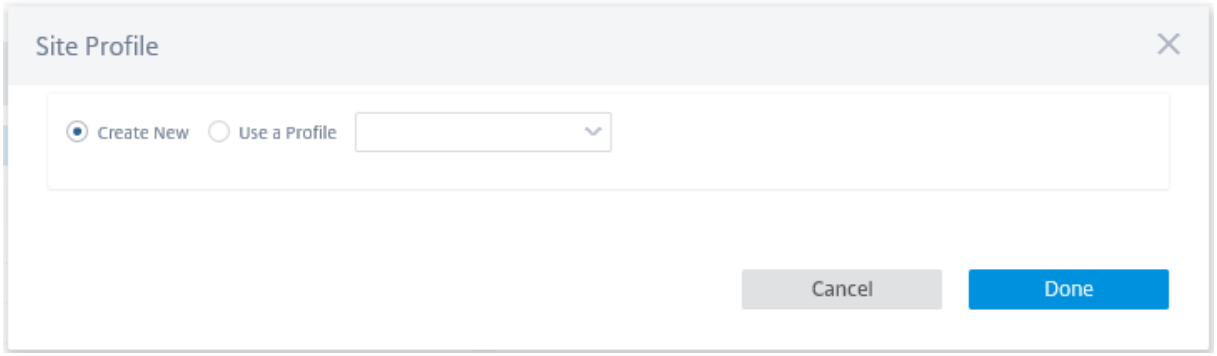
例如，管理员创建一个称为小型零售商店的站点配置配置文件，并将其应用于公司拥有的所有小型零售店。现在，在任何给定时间对小型零售店简介所做的任何更改都将自动应用到继承此配置文件的所有商店。根据所有实体的共同点和非共同点，可以不设置配置文件配置中的某些参数。此类参数可以自定义，并且在继承相同配置文件的实体之间可能会有所不同。

网站简介

站点配置文件可帮助您轻松快速地配置站点。您可以创建一次站点配置文件，然后在创建站点时多次重复使用。

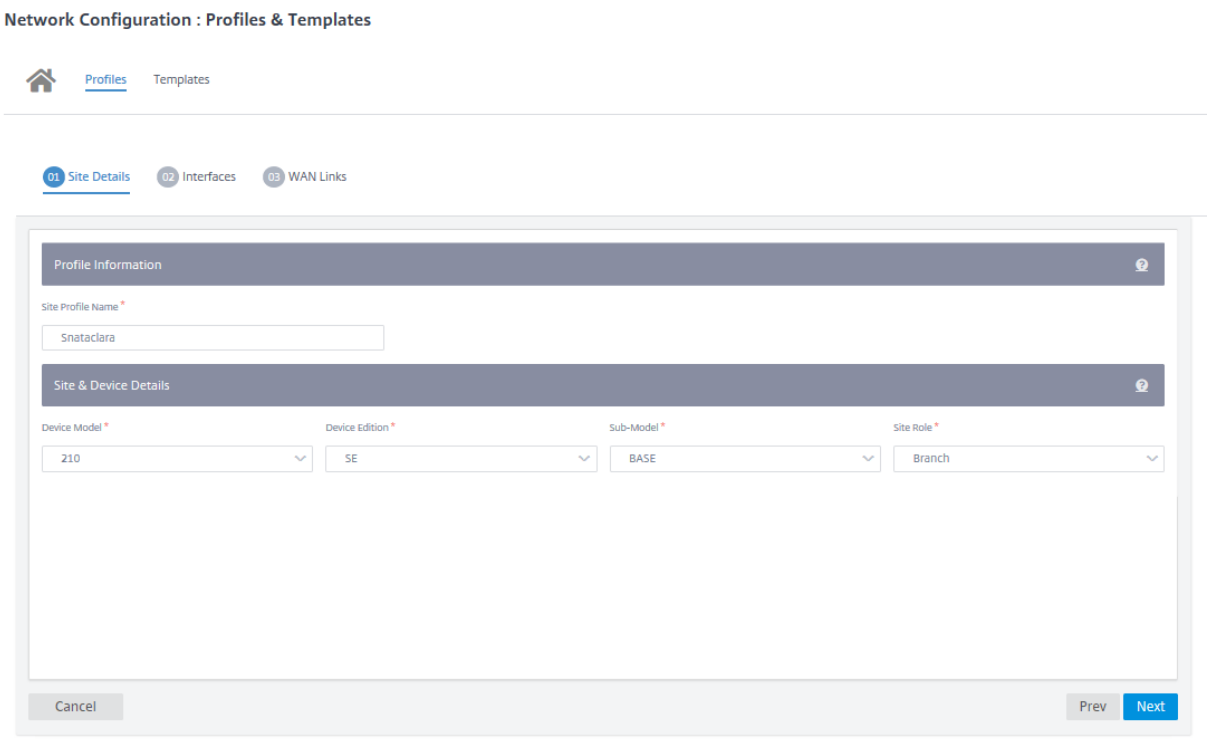


要创建站点配置文件，请单击 **+** 站点配置文件。您可以从头开始创建配置文件或编辑现有站点配置文件并将其另存为新配置文件。

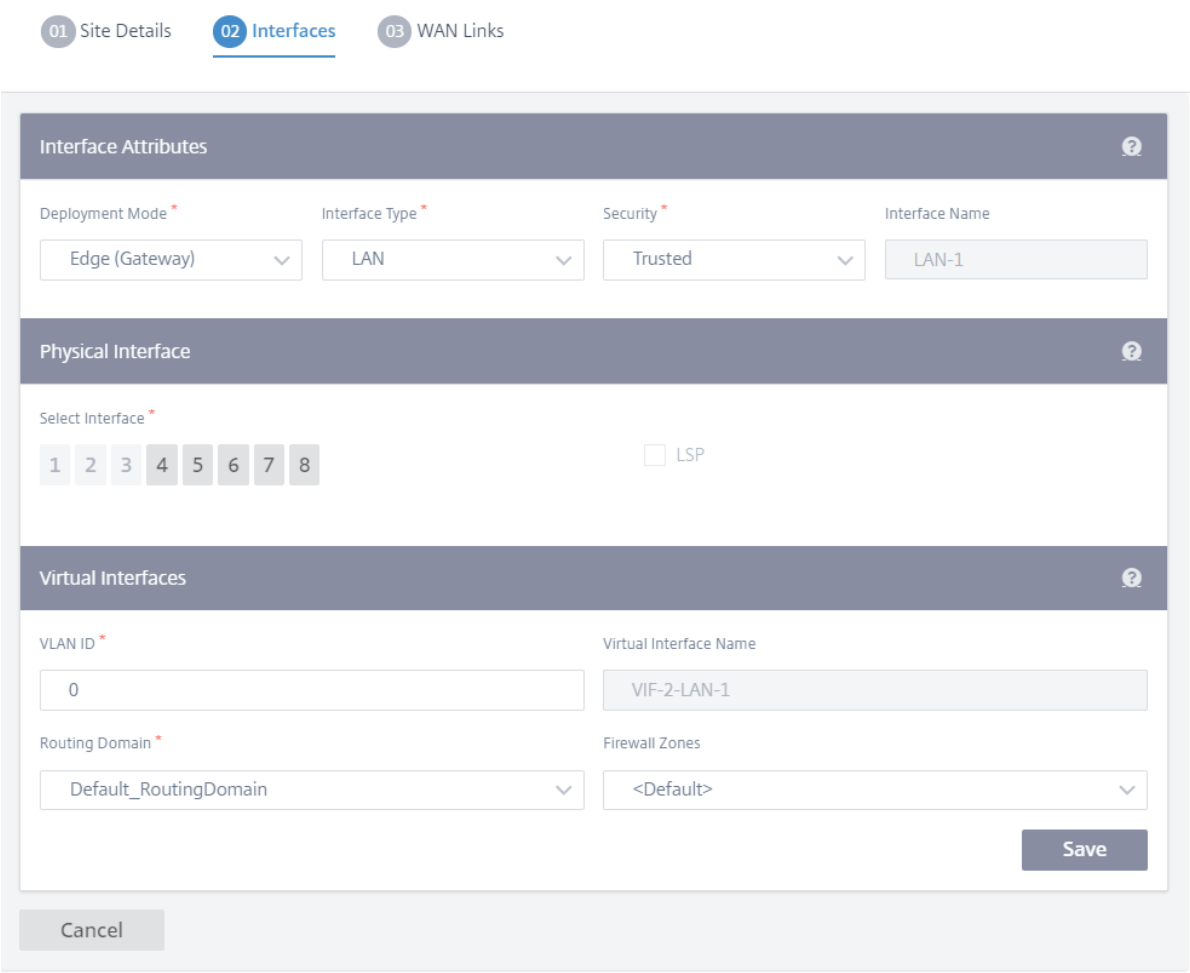


要创建站点配置文件，您需要配置 站点详细信息、接口和 **WAN** 链接。有关配置站点的详细说明，请参阅 站点 详细信息。

提供设备详细信息。

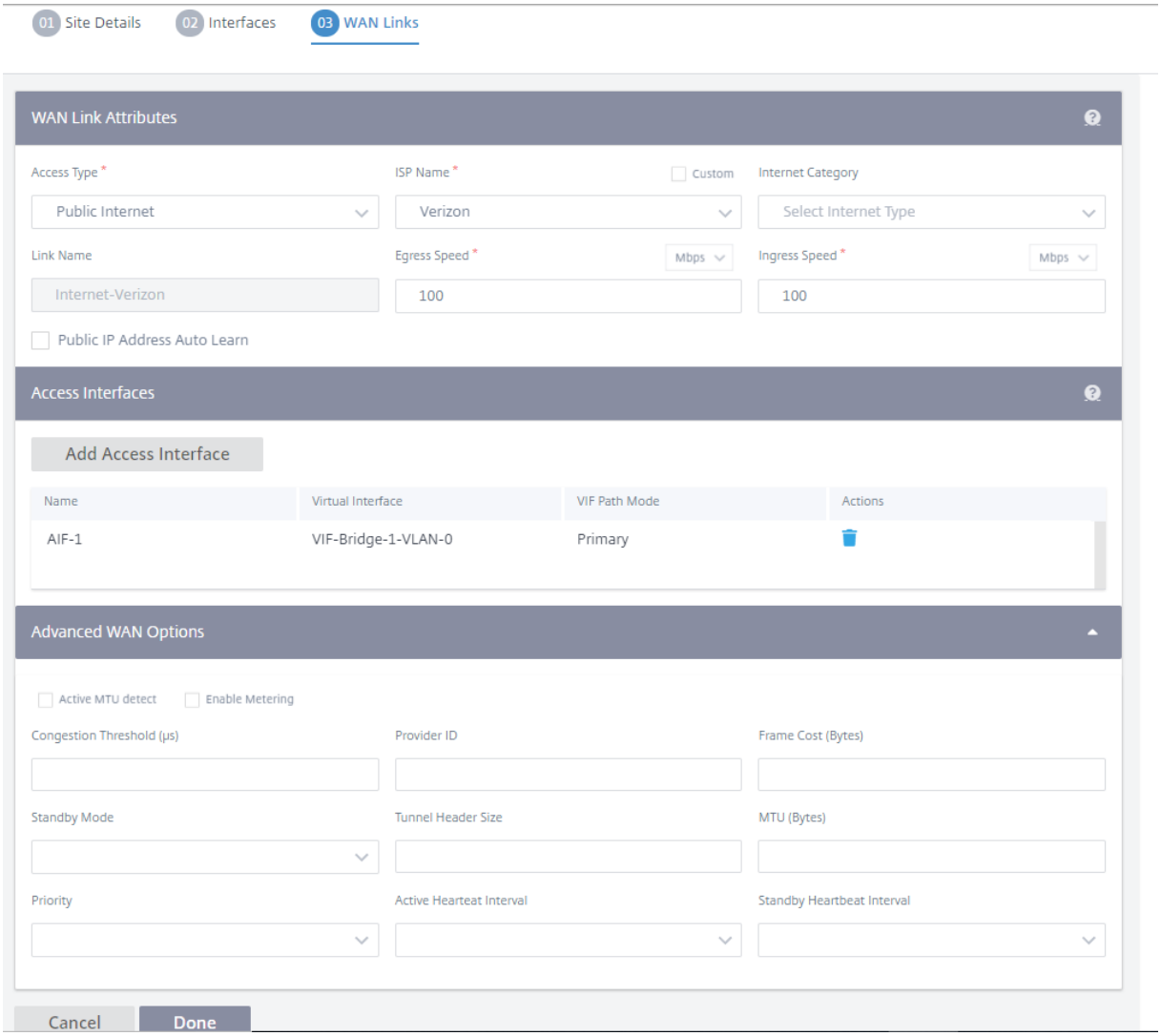


单击 **+** 接口选项为站点分配接口。要添加接口，您需要填写 “接口属性”、“物理接口”和“虚拟接口”字段。有关配置接口的详细说明，请参阅 接口。



使用 高级选项填充 **WAN** 链接属性、访问接口 和 服务。

有关配置 WAN 链接的详细说明，请参阅 WAN 链接。



模板

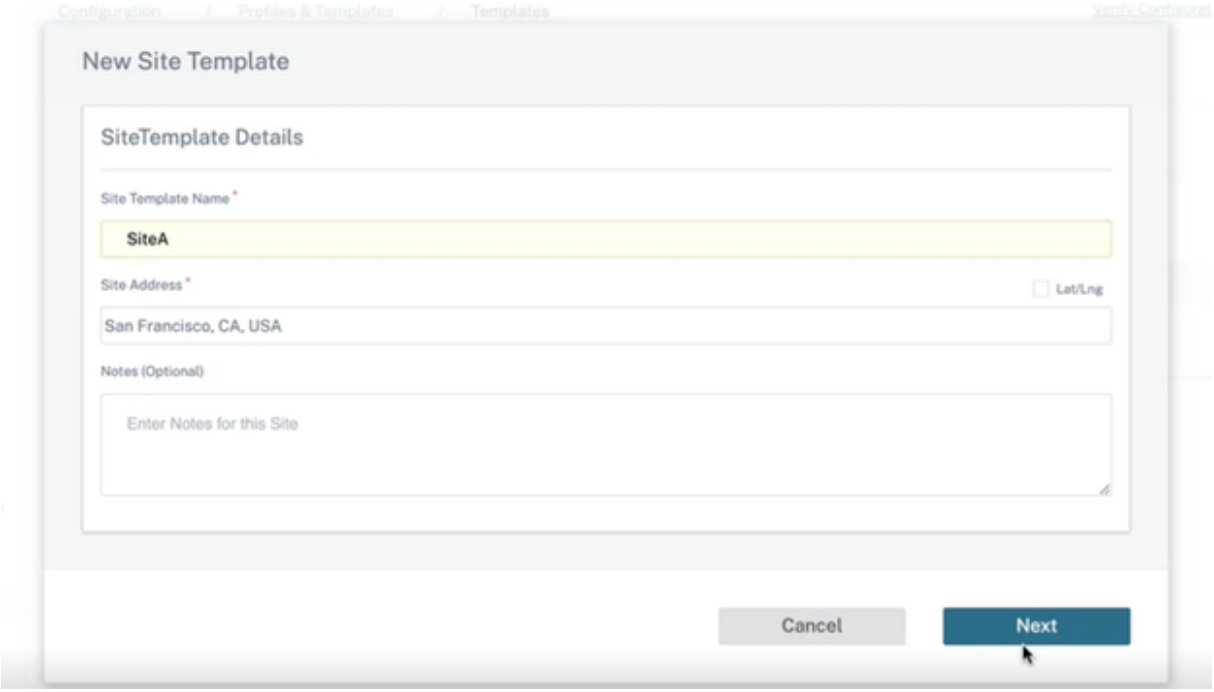
Citrix SD-WAN Orchestrator 服务允许您使用模板作为一组预定义字段来配置新站点或 WAN 链接。

网站模板

站点模板是用于创建网站的预定义模板。要使用预定义的站点模板配置站点，请在客户级别导航到 配置 **>** 配置文件和模板 > 模板。在“网站模板”部分中，单击“添加网站模板”。

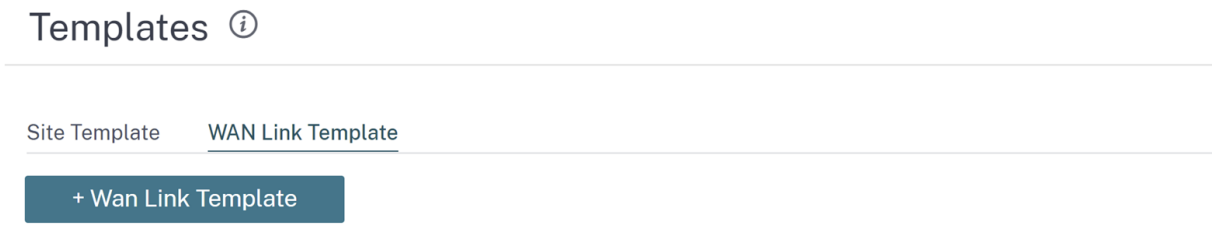
在显示的“新建站点模板”屏幕上，提供所需的详细信息，然后单击“下一步”。

> 注意
>
> 当您使用站点模板克隆站点或创建站点并且源配置了 Wi-Fi 时，Wi-Fi 设置不会复制到新站点。

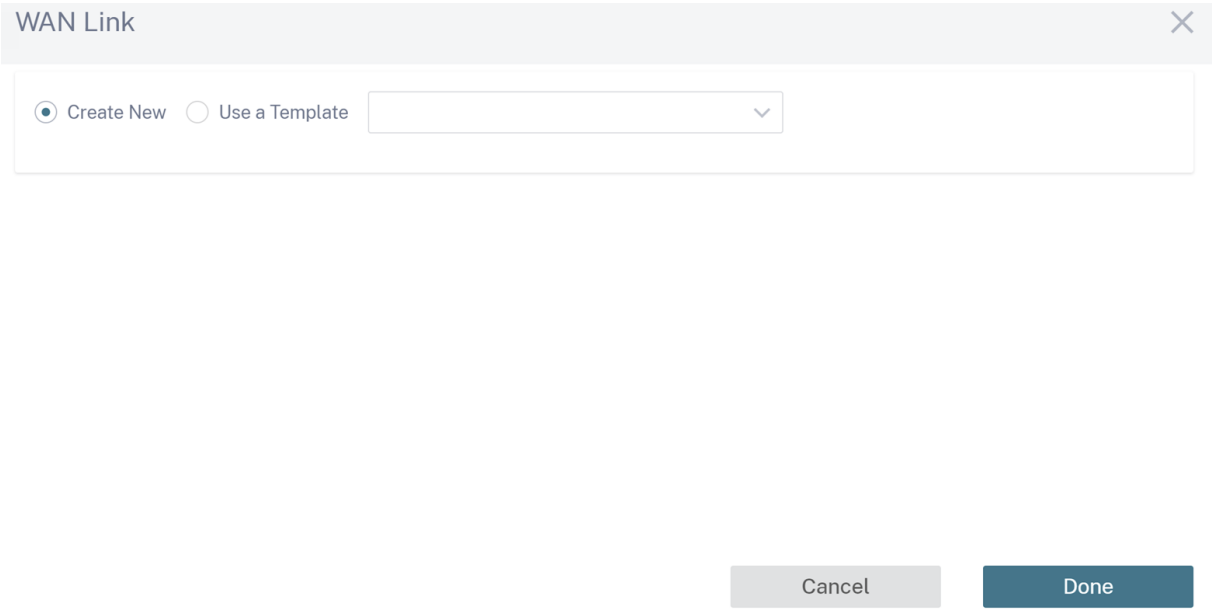


WAN 链接模板

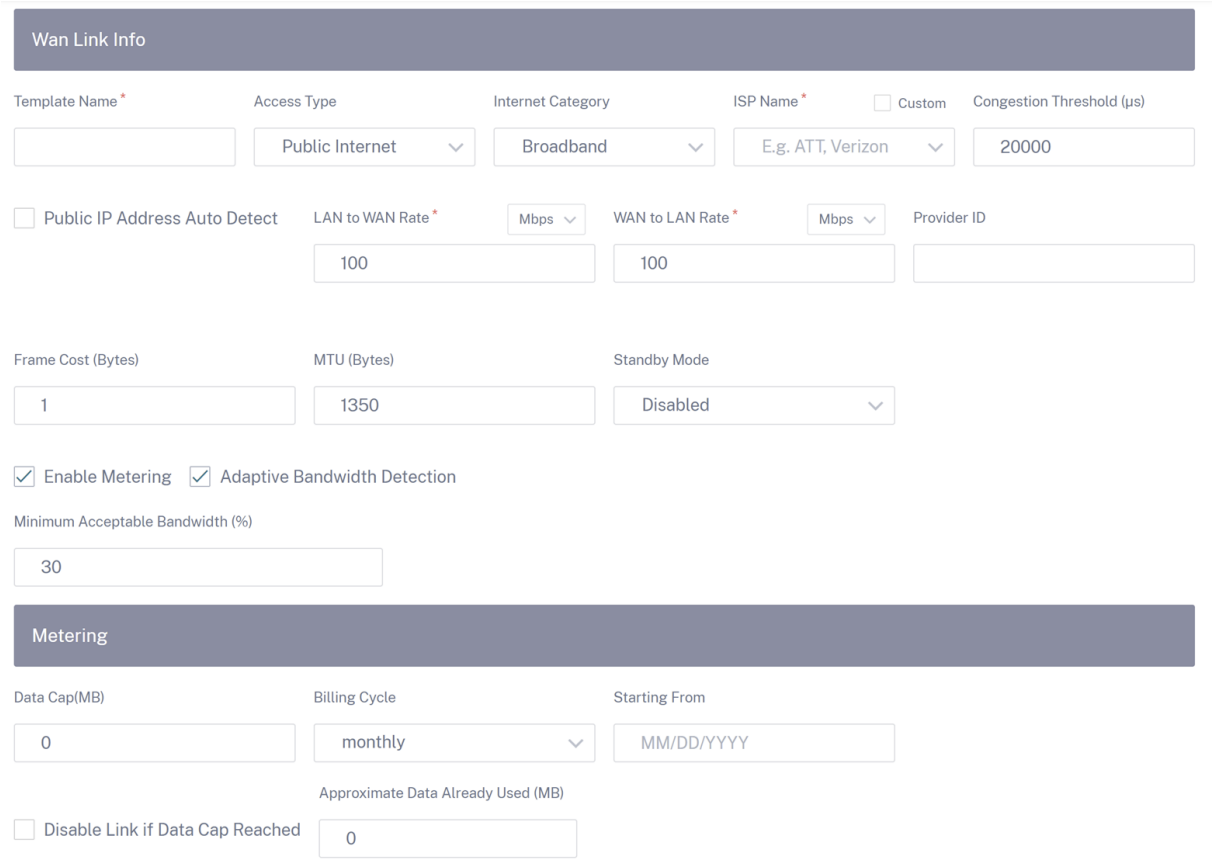
WAN 链接模板可帮助您轻松快速地配置 WAN 链接。您可以创建一次 WAN 链接模板，然后在配置 WAN 链接时多次重复使用。您甚至可以将修改后的 WAN 链接模板配置复制到使用 WAN 链接模板创建的站点 WAN 链接配置中。



要创建 WAN 链接模板，请单击 **+ WAN** 链接模板。您可以从头开始创建模板，也可以编辑现有 WAN 链接模板并将其另存为新模板。



提供 WAN 链接信息，例如 配置文件名称、访问类型、互联网类别、**LAN** 到 **WAN** 速率 (Mbps) 等，以创建 WAN 配置文件。有关配置 WAN 链接的详细说明，请参阅 WAN 链接。

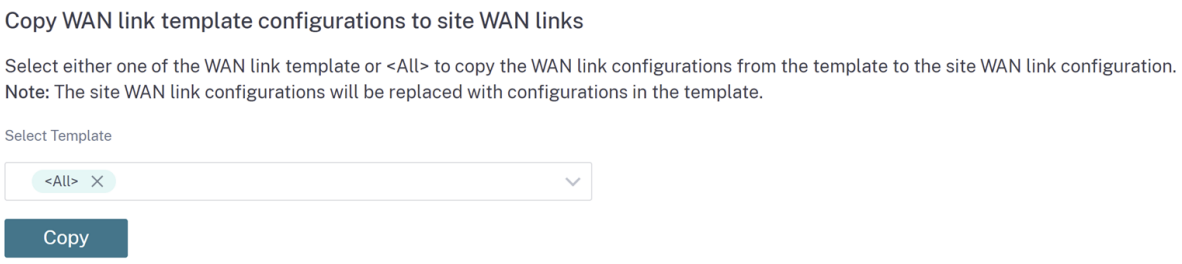


以前，将修改后的 WAN 链接模板配置复制到站点 WAN 链接配置的选项不可用。例如，如果用户已经使用 WAN 链接模板创建了多个站点 WAN 链接，并且必须修改特定的配置（例如，拥塞阈值设置），则该用户必须单独在每个站点

WAN 链接上进行修改。从现在开始，用户可以使用新的拥塞阈值设置更新 WAN 链接模板，并将最新的 WAN 链接模板配置复制到使用 WAN 链接模板创建的所有站点 WAN 链接。

当您选择一个或多个 WAN 链接模板并单击“复制”时，您在 WAN 链接模板上所做的更新将复制到使用所选模板创建的站点 WAN 链接配置中。

> 注意
>
> 使用站点配置文件功能创建的 WAN 链接站点配置不会更新。



网络定位服务

July 10, 2024

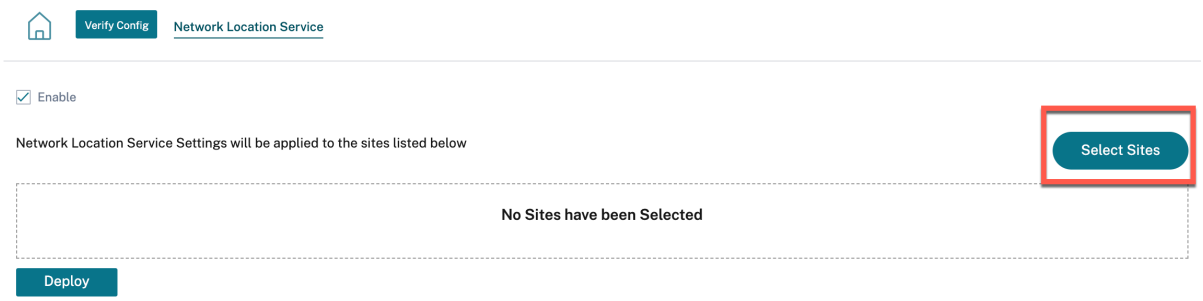
> 重要更新：
>
> 在 Citrix SD-WAN Orchestrator 服务部署中弃用了此功能。但是，您仍然可以使用 Citrix Cloud 启用 NLS。有关详细信息，请参阅使用直接工作负载连接优化与工作区的连接。

网络定位服务 (NLS) 是一项 Citrix Cloud 服务，用于确定连接到 Citrix Virtual Apps and Desktops 用户是否来自内部网络。使用 NLS，您可以避免通过 PowerShell 脚本手动配置 Citrix SD-WAN 部署位置的 IP 地址。有关 NLS 的详细信息，请参阅 Citrix Workspace 网络定位服务。

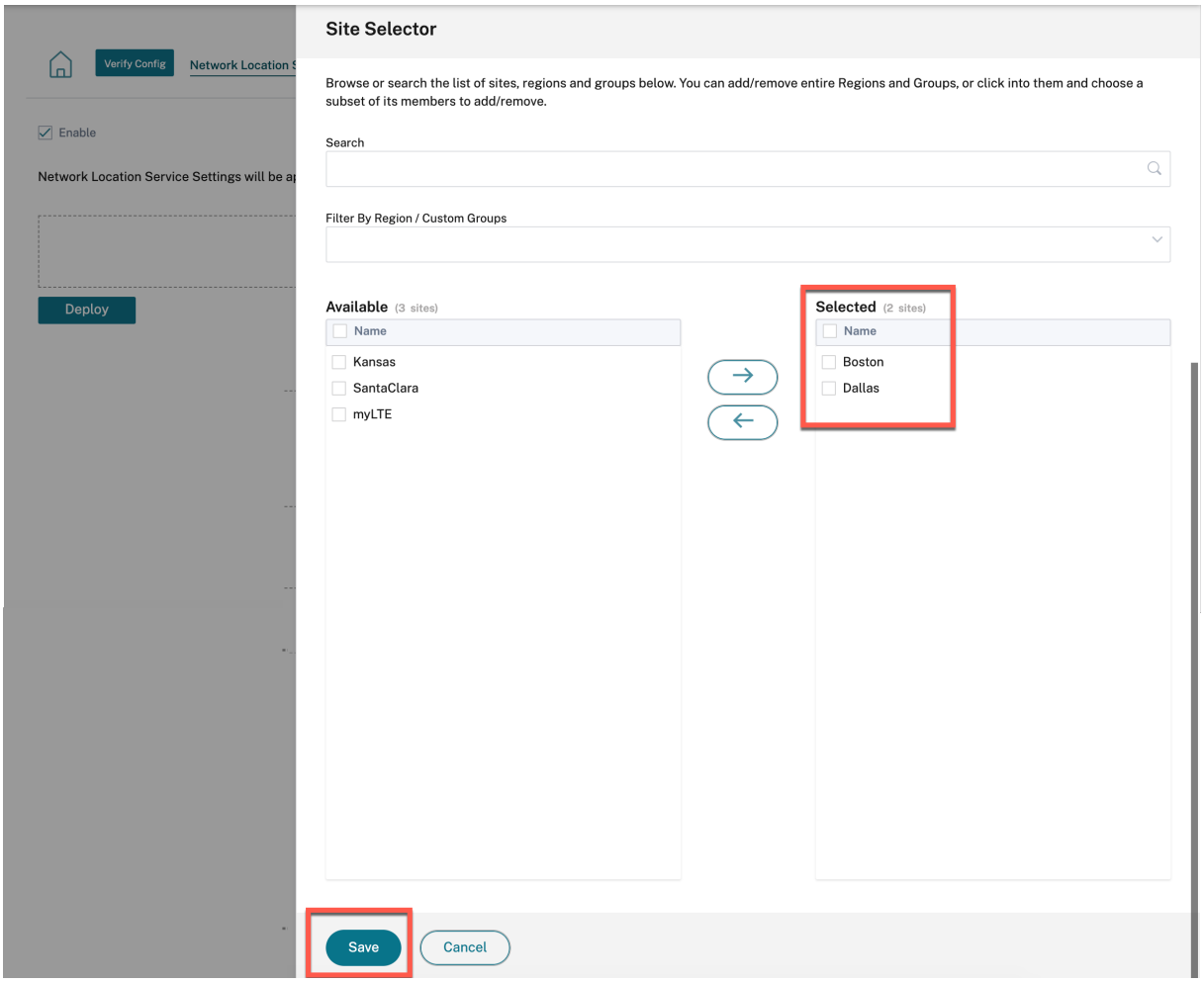
您可以为网络中的所有站点或特定站点启用 NLS。启用 NLS 的站点与 NLS 数据库共享其所有 Internet WAN 链接的公有 IP 地址以及其他站点详细信息，例如地理位置、时区。通过这些详细信息，网络定位服务可以确定连接到 Citrix Virtual Apps and Desktops 用户是否位于 Citrix SD-WAN 的网络前端。

如果用户请求来自 Citrix SD-WAN 的网络前端，则用户将绕过 Citrix Gateway 服务直接连接到 Citrix Virtual Apps and Desktops Virtual Delivery Agent。

要启用 NLS，请在客户级别导航到配置 **>** 网络定位服务。



如果要为网络中的所有站点启用 NLS，请选择启用。要为特定站点启用 NLS，请单击选择站点。选择区域并相应地选择地点。单击保存，然后单击部署。



ECMP 负载平衡

October 21, 2022

等价多路径 (ECMP) 组允许您将多条路径分组成相同的成本、目标和服务。连接或会话数据在 ECMP 组中的所有路径之间进行负载平衡，具体取决于 ECMP 组的类型。例如，假设分支机构和数据中心之间具有两条 WAN 链路的网络，路由成本相同。传统上，其中一个 WAN 链路将处于活动状态，另一条仍处于休眠状态，充当后备链路。使用 ECMP Groups，您可以将这些 WAN 链路组合在一起，并允许通过两个 WAN 链路进行负载平衡流量。ECMP 负载均衡可确保：

- 通过多条等价路径分布流量。
- 最佳利用可用带宽。
- 如果路由不可达，则将流量动态传输到其他 ECMP 成员路径。

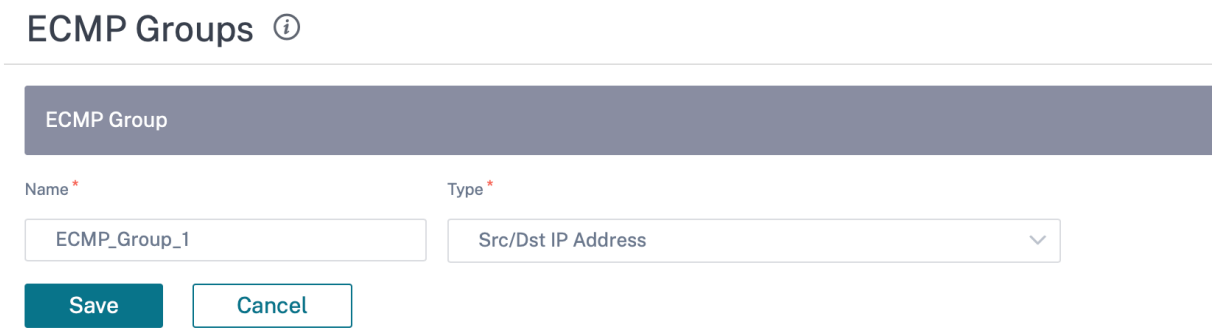
以下服务支持 ECMP 负载均衡：

- 虚拟路径
- Citrix Secure Internet Access
- Zscaler
- IPsec 的
- GRE

您最多可以在网络中定义 254 个 ECMP 组。ECMP 组中符合 ECMP 条件的路由的最大数量取决于您的设备和许可证类型。Citrix SD-WAN 支持以下两种类型的 ECMP 组：

- 源/目标 IP 地址：多个客户端尝试连接到同一目标的 网络，连接在同等成本的 WAN 链路之间进行负载平衡。
- 会话：一个客户端连接到目标并生成多个会话的 网络。会话数据在同等成本的 WAN 链路之间进行负载平衡。

要配置 ECMP 组，请在网络级别导航到 配置 **>** 路由 **> ECMP** 组。提供 ECMP 组的名称，然后根据需要选择类型为 **Src/Dest IP** 地址 或 会话。

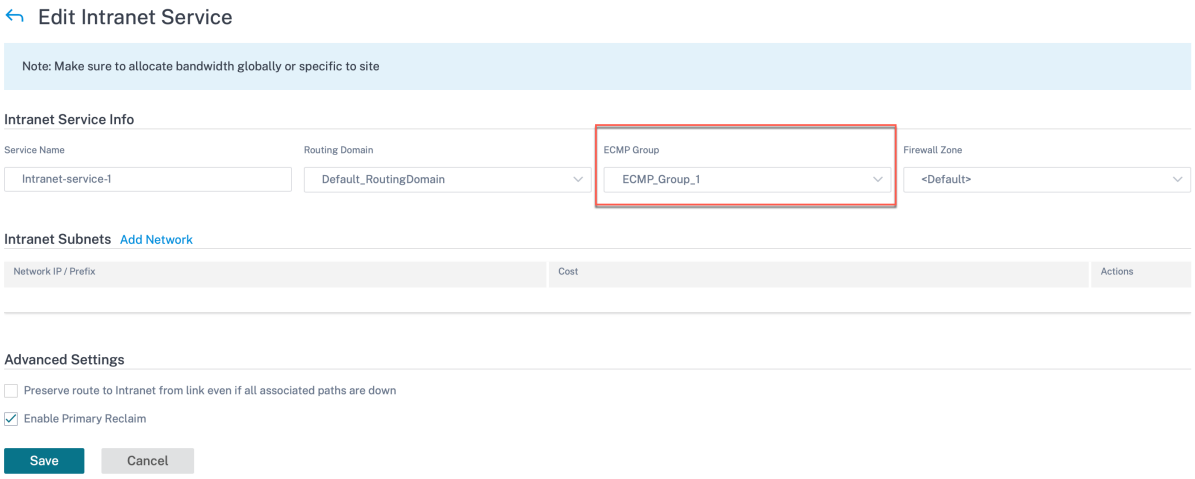


您可以将 ECMP 组关联到以下服务：

- 虚拟路径（站点级别）
- Citrix Secure Internet Access
- Zscaler
- IPsec 的
- GRE

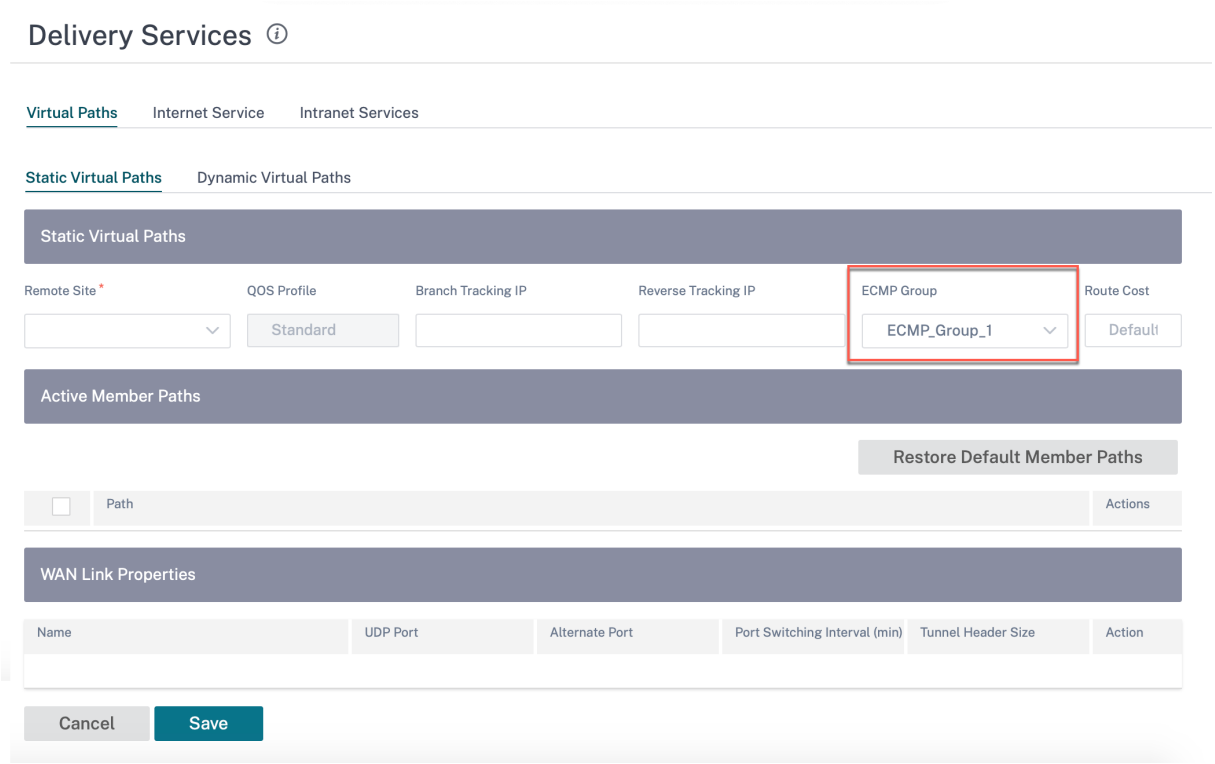
要在 Intranet 服务上启用 ECMP 配置，请在网络 * 级别导航到 配置 **>** 传送通道 **>** 带宽分配 **> Intranet +** 服务，然后将 服务类型 选择为 内联网。在配置内联网服务时选择 ECMP 组。

> 注意
>
> 选择“无”不会在服务上启用 ECMP 配置。



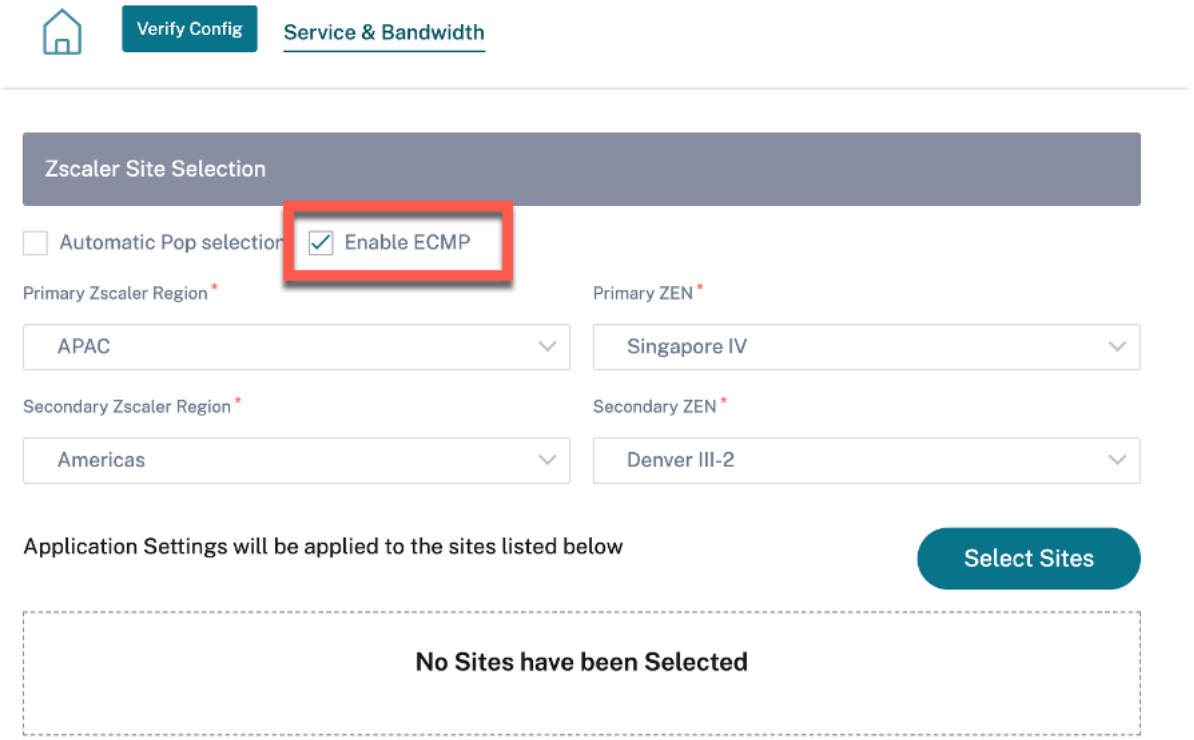
要在虚拟路径上启用 ECMP 配置，请在站点级别导航到 配置 > 高级设置 > 交付服务 > 虚拟路径 > 静态虚拟路径 > **+** 虚拟路径。在配置静态虚拟路径时选择 ECMP 组。

> 注意
>
> 选择“无”不会在服务上启用 ECMP 配置。



要在 Zscaler 服务上启用 ECMP 配置，请在网络级别导航到 配置 **>** 服务和带宽。单击“配送服务”列下方列出的 Zscaler 旁边的 设置 图标。进行身份验证并单击 **+** 站点。添加站点时选中“启用 **ECMP** ”复选框。

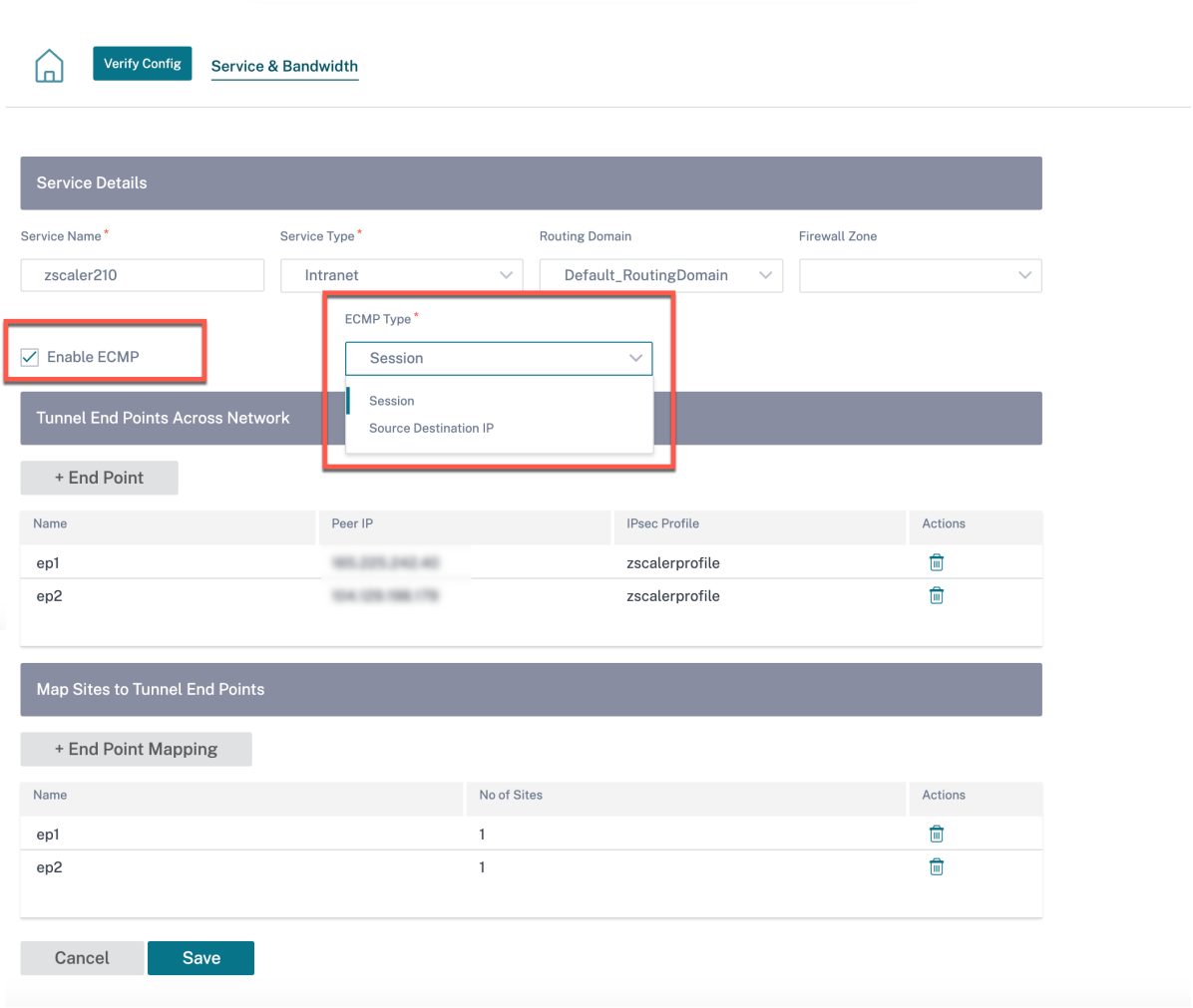
> 注意
>
> Zscaler 服务仅支持基于会话的 ECMP 负载均衡。



要在 Citrix Secure Internet Access 服务上启用 ECMP 配置，请在网络级别导航到 配置 **>** 服务和带宽。单击“安全互联网接入服务”旁边的“设置”图标，然后单击 **+** 站点。选择站点后，选中“启用 **ECMP** ”复选框。

> 注意
>
> Citrix Secure Internet Access 服务仅支持基于会话的 ECMP 负载平衡。

要在固定 IPsec 隧道上启用 ECMP 配置，在 LAN 或 WAN 端与第三方对等方启用 ECMP 配置，请导航到配置 **>** 服务和带宽 **> Intranet +** 服务，然后将 服务类型 选择为 **IPsec**。选中“启用 **ECMP** ”复选框，然后从 **ECMP** 类型下拉列表中选择一种类型。



应用程序规则

October 21, 2022

应用程序规则允许 Citrix SD-WAN 设备解析传入流量并将其归类为属于特定应用程序或应用程序组。这种分类通过创建和应用应用程序规则来提高单个应用程序或应用程序系列的服务质量 (QoS)。

您可以根据应用程序、应用程序组或应用程序对象的匹配类型筛选流量，并将应用程序规则应用于这些流量。应用程序规则类似于互联网协议 (IP) 规则。有关 IP 规则的信息，请参阅 IP 规则。

对于每个应用程序规则，您可以指定流量策略。以下是可用的流量策略：

- 负载平衡路径：流的应用程序流量在多个路径之间进行平衡。通过最佳路径发送流量，直到使用该路径为止。剩余的数据包将通过下一个最佳路径发送。
- 持久路径：应用程序流量将保持在同一路径上，直到路径不再可用为止。

- 重复路径：应用程序流量跨多个路径复制，从而提高可靠性。
  应用程序规则与类相关联。

如何应用申请规则?

在 SD-WAN 网络中，当传入的数据包到达 SD-WAN 设备时，初始数据包不会进行 DPI 分类。此时，IP 规则属性（如类、TCP 终止）将应用于数据包。在 DPI 分类之后，应用程序规则属性（例如类别、流量策略）会覆盖 IP 规则属性。

与应用程序规则相比，IP 规则具有更多的属性。应用程序规则仅覆盖少数 IP 规则属性。其余 IP 规则属性仍在数据包上处理。

例如，假设您已为使用 SMTP 协议的 Web 邮件应用程序（例如 Google Mail）指定了应用程序规则。为 SMTP 协议设置的 IP 规则最初是在 DPI 分类之前应用的。解析数据包并将其归类为属于 Google Mail 应用程序后，将应用为 Google Mail 应用程序指定的应用程序规则。

创建应用程序规则

要创建应用程序规则，请导航到 配置 **> QoS > QoS** 策略 > 应用程序规则。选择“全局规则”选项卡在全局级别创建应用程序规则，或选择“站点/组特定规则”以在站点级别创建规则。

单击“应用程序规则”部分下的“新建应用程序规则”。

- 应用程序和域名匹配标准
  - 应用程序和域名：从下拉列表中选择一个应用程序或域。您也可以通过单击 **+** 新建域名应用程序来创建域名应用程序。输入名称并添加域名。
  - 路由域：选择路由域。您可以选择默认路由域或选择 任意。
  - 源网络：与流量匹配的源 IP 地址和子网掩码。
  - 目标网络：与流量匹配的目标 IP 地址和子网掩码。
  - 源端口：与流量匹配的源端口号或端口范围。
  - 目标端口：要与流量匹配的目标端口号或端口范围。
  - **Src = Des**t：如果选中，则源端口也用于目标端口。
- 虚拟路径流量策略

  选中“启用虚拟路径流量策略”复选框。
  - 虚拟路径远程站点：选择远程站点的虚拟路径。
  - 流量策略：根据需要选择以下流量策略之一。
    - 负载平衡路径：流量的应用程序流量在多条路径上均衡。通过最佳路径发送流量，直到使用该路径为止。剩余的数据包将通过下一个最佳路径发送。
    - 持久路径：应用程序流量将保持在同一路径上，直到路径不再可用为止。选择以下 持久性策略之一：
      - 在 @@ 源链路上保留：应用程序流量将保留在源链路上，直到该路径不再可用。

- 如果可用，请在 **MPLS** 链接上保留，否则保留在原始链路上：应用程序流量保留在 MPLS 链路上。如果 MPLS 链路不可用，则流量将保留在始发链路上。
- 如果可用，则保留在互联网链接上，否则保留在原始链接上：应用程序流量保留在互联网链接上。如果 Internet 链接不可用，则流量将保留在原始链路上。
- 如果可用，则保留在私有 **Intranet** 链接上，否则保留在原始链接上：应用程序流量保留在私有 Intranet 链接上。如果私有 Intranet 链接不可用，则流量将保留在原始链路上。

持续阻抗 是指应用程序流量在链路上停留的时间（以毫秒为单位）。

* 重复路径：应用程序流量在多条路径上复制，从而提高了可靠性。

- QoS 设置（QoS 类别）
  - 转账类型：选择以下转账类型之一：
    * 实时：用于低延迟、低带宽、对时间敏感的流量。实时应用程序具有时间敏感性，但实际上并不需要高带宽（例如 IP 语音）。实时应用程序对延迟和抖动很敏感，但可以承受一些损失。
    * 交互式：用于具有中低延迟要求和中低带宽要求的交互式流量。通常情况下，在客户端与服务器之间进行交互。通信可能不需要高带宽，但对丢失和延迟非常敏感。
    * 批量：用于高带宽流量和可容忍高延迟的应用程序。处理文件传输并需要高带宽的应用程序被归类为批量类。这些应用很少涉及人为干扰，主要由系统自己处理。
  - 优先级：为所选传输类型选择优先级。

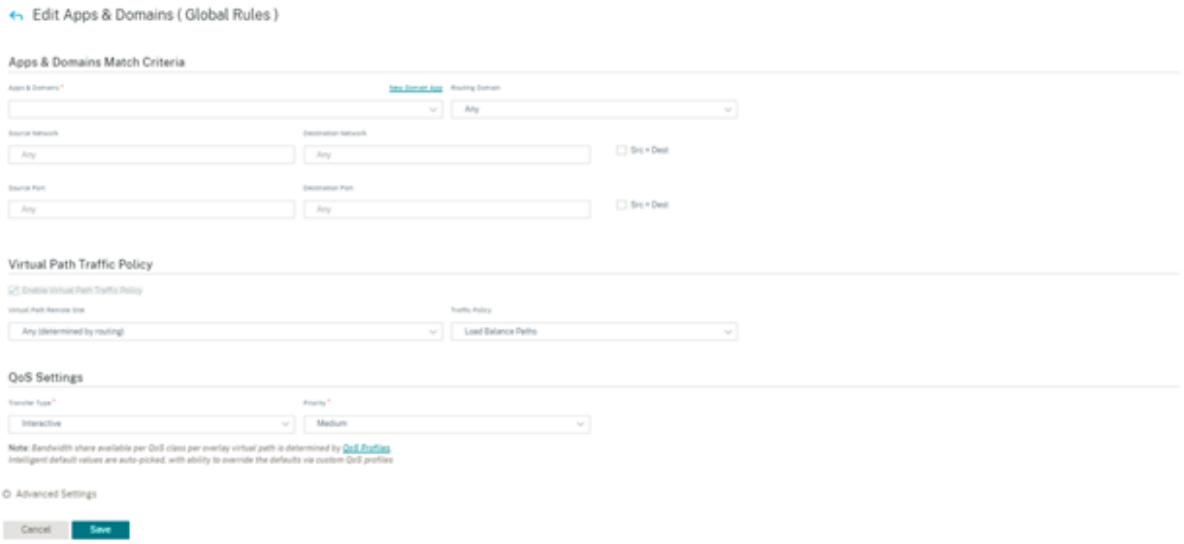
高级设置

- 广域网通用
  - 重新传输丢失的数据包：通过可靠的服务将符合此规则的流量发送到远程设备，并重新传输丢失的数据包。
  - 启用数据包聚合：将小数据包聚合成较大的数据包。
- 局域网到 WAN
  - 丢弃深度（字节）：队列深度阈值，超过该阈值后，数据包将被丢弃。
  - 丢弃限制：在类调度程序中等待的数据包被丢弃的时间。不适用于批量类。
  - 启用 **RED**：随机早期检测 (RED) 通过在拥塞发生时丢弃数据包来确保公平共享类资源。
  - 重复数据包禁用深度（字节）：类调度器的队列深度，此时未生成重复数据包。
  - 重复数据包禁用限制：可以禁用复制以防止重复数据包消耗带宽的时间。
- WAN 到局域网
  - **DSCP** 标签：在将数据包发送到局域网之前，DSCP 标记应用于在广域网到局域网上匹配此规则的数据包。
  - 启用数据包重新排序：与规则匹配的流量被标记为顺序顺序，数据包在 WAN to LAN 设备上被重新排序（如有必要）。
  - 保持时间：保留数据包以进行重新排序的时间间隔，在此之后数据包将被发送到局域网。计时器到期时，数据包将发送到 LAN，无需再等待必备序列号。

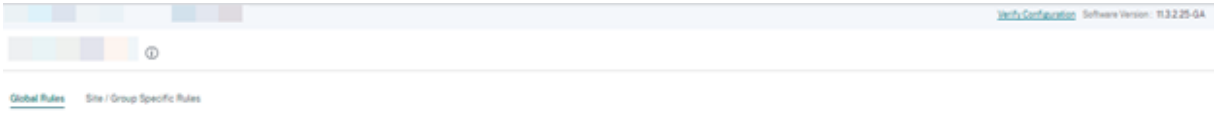
如果规则将流量策略作为重复路径，则默认保持时间为 80 ms。否则，TCP 规则的默认值为 900 毫秒，非 TCP 规则的默认值为 250 毫秒。

- 丢弃延迟重排序数据包：丢弃在重新排序所需的数据包发送到局域网后到达的无序数据包。

单击“保存”保存配置设置。



在“配置”**>** “QoS”**>** “QoS 策略”页面上单击“验证配置”以验证任何审计错误。

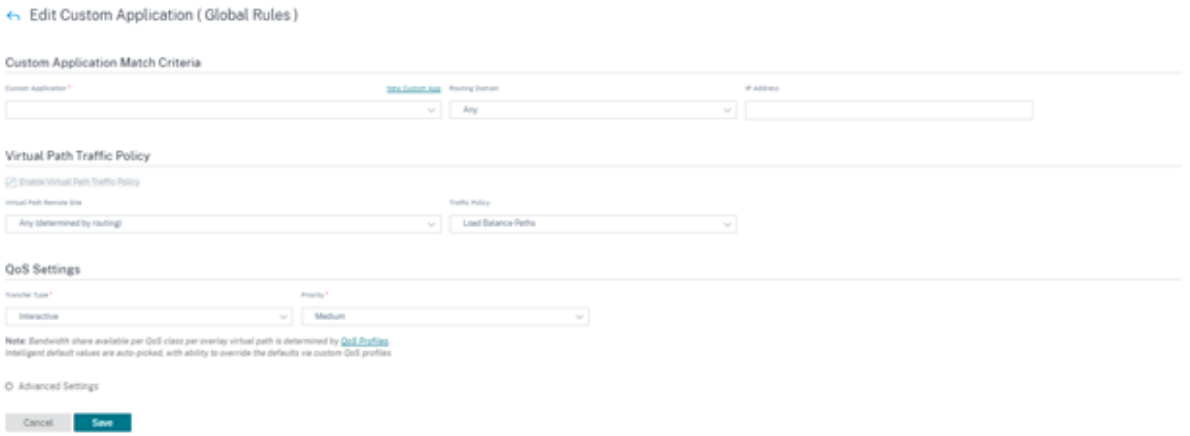


创建自定义应用程序规则

您也可以创建自定义应用程序规则。要创建自定义应用程序规则，请导航到 配置 **> QoS > QoS** 策略 > 自定义应用程序规则。选择“全局规则”选项卡在全局级别创建自定义应用程序规则，或选择“站点/组特定规则”以在站点级别创建规则。

单击“自定义应用程序规则”部分下的“新建自定义应用程序规则”。单击“自定义应用程序”字段名称旁边的“新建自定义应用程序”。输入自定义应用程序的名称。在“匹配标准”部分中，选择应用程序、协议、DSCP 标记，然后输入网络 IP 和端口号。单击保存。

根据需要在其他字段中输入详细信息。有关字段描述的信息，请参阅 创建应用程序规则。

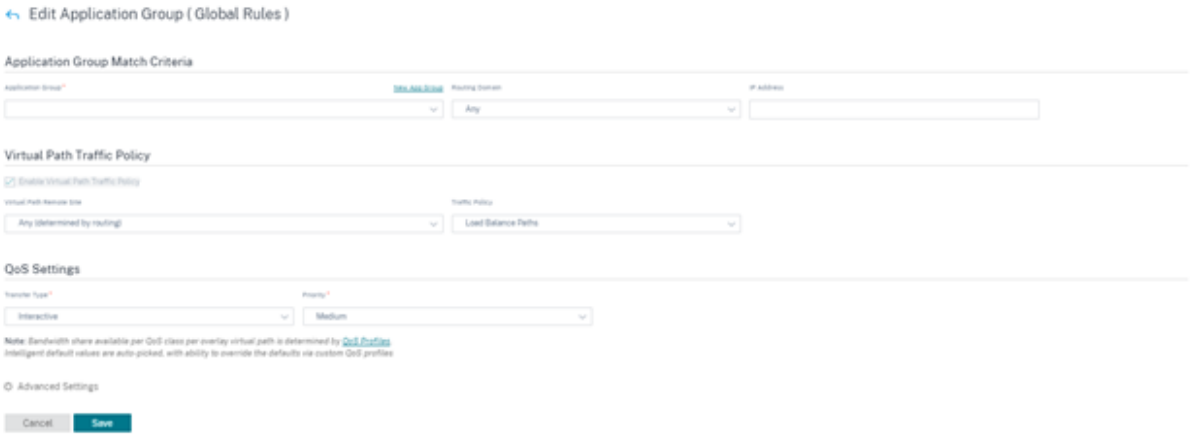


创建应用程序组规则

您可以为一组应用程序创建规则。要创建应用程序组规则，请导航到 配置 **> QoS > QoS** 策略 > 应用程序组规则。选择“全局规则”选项卡在全局级别创建应用程序组规则，或选择“站点/组特定规则”以在站点级别创建规则。

单击“应用程序组规则”部分下的“新建应用程序组规则”。单击“应用程序组”字段名称旁边的“新建应用程序组”。输入应用程序组的名称。根据需要搜索和添加应用程序。单击保存。

根据需要在其他字段中输入详细信息。有关字段描述的信息，请参阅 创建应用程序规则。



验证应用程序规则

要验证应用程序规则，请导航到 报告 **>** 实时 **>** 流量。选择要查看流量信息和要显示的流量数量的站点。单击“自定义列”，然后选中与要查看的流量信息对应的复选框。验证流信息是否符合配置的规则。

导航到 报告 **>** 实时 **>** 统计信息，然后选择 规则。选择站点，然后单击“检索最新数据”。验证配置的规则。

有关报告的更多信息，请参阅 流量。

HDX QoE

July 10, 2024

网络参数（如延迟、抖动和数据包丢弃）会影响 HDX 用户的用户体验。体验质量 (QoE) 可帮助用户了解和检查他们的 ICA 体验质量。QoE 是一个计算指数，指示 ICA 流量性能。用户可以调整规则和策略来改善 QoE。

QoE 是介于 0—100 之间的数值，值越高，用户体验越好。

用于计算 QoE 的参数是在位于客户端和服务器端的两个 Citrix SD-WAN 设备之间测量的，而不是在客户端或服务器设备本身之间测量的。延迟、抖动和数据包丢弃是在流级别测量的，它可能与链路级别的统计信息不同。最终主机（客户端或服务器）应用程序可能永远不会知道 WAN 上存在数据包丢失。如果重新传输成功，则流量级数据包丢失率低于链路级丢失。但是，因此，它可能会稍微增加延迟和抖动。

您可以在 Citrix SD-WAN Orchestrator 的 HDX 仪表板中查看 HDX 应用程序整体质量的图形表示。HDX 应用分为以下三个质量类别：

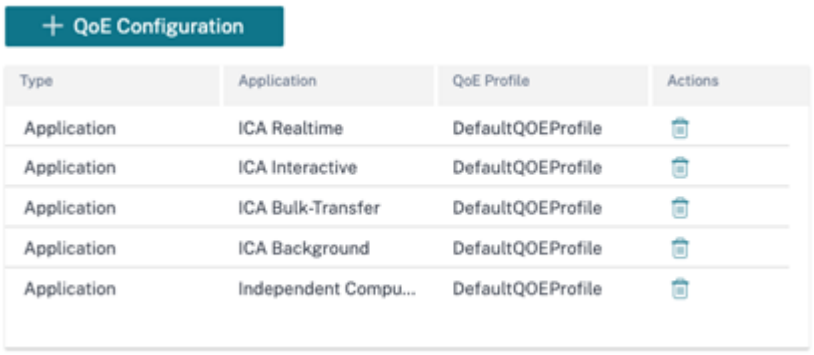
质量	QoE 范围
良好	71-100
一般	51-70
不佳	0-50

根据选定的 UI 页面，HDX 控制面板中将显示底部（最少 QoE）的五个站点、五个用户、五个会话或所有站点的列表。

不同时间间隔的 QoE 图形表示允许您监视每个站点 HDX 应用程序的性能。

配置 **HDX QoE**

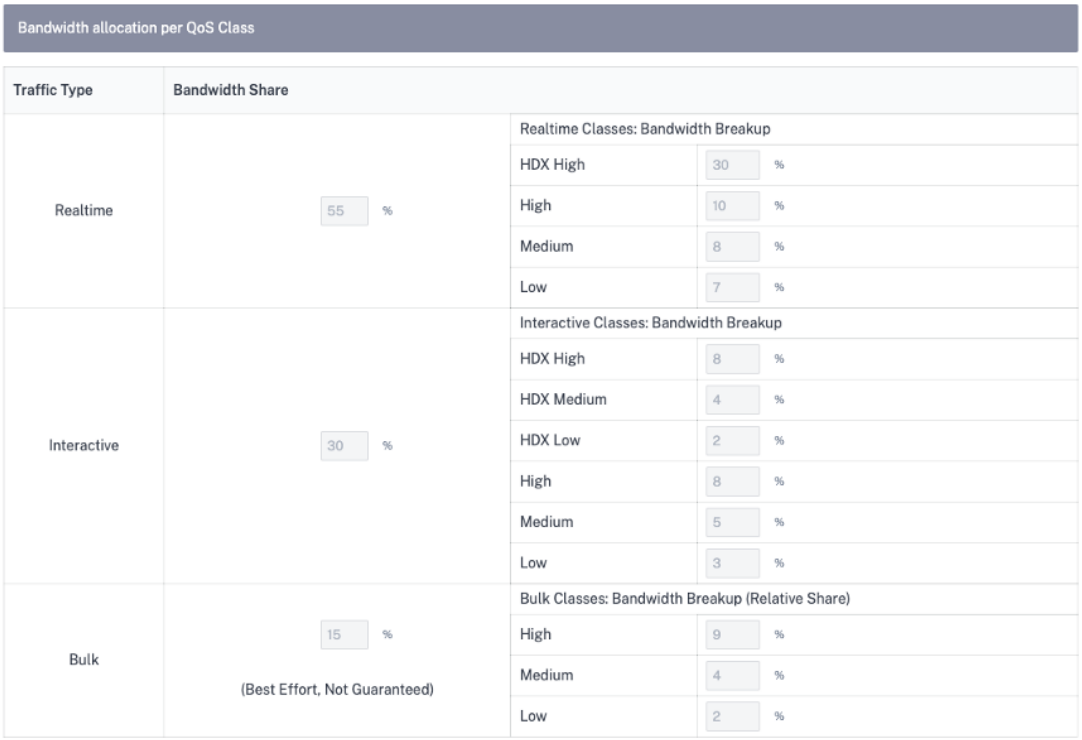
1. 在网络级别，导航到 配置 **>** 应用程序设置和群组 **>** 应用程序质量配置，然后单击 **+ QoE** 配置。使用要用于计算 HDX 行为的 QoE 配置文件添加以下应用程序：
    - ICA 实时（ICA 优先级 _0）
    - ICA 交互式 (ICA 优先级 _1)
    - ICA 批量传输 (ica_priority_2)
    - ICA 背景（优先级 _3）
    - 独立计算架构 (Citrix) (ICA)



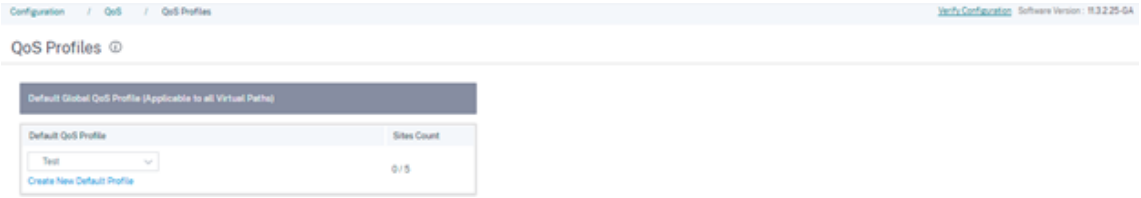
这些配置提供了通过配置文件测量 HDX 报告中使用的 HDX 性能的参数。HDX 多流 (MSI) 连接需要配置 ICA 实时、ICA Interactive、ICA 批量传输、ICA 背景，单流 (SSI) 连接需要独立计算架构 (Citrix)。

2. 导航到 配置 **> QoS > QoS** 配置文件。选择 St **andard-HDX-Multistream** 作为默认 QoS 配置文件，然后选中 **HDX** 报告 复选框。如果不需要 **HDX** 报告，请清除 HDX 报告。

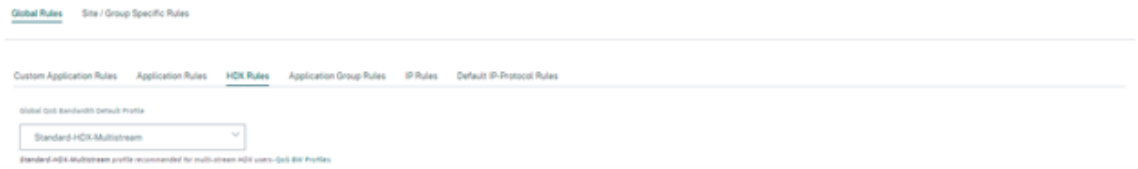
在每个 QoS 配置文件中，每个类别都有预定义的带宽百分比。它们可配置为调整分配给 HDX 流量所用类别的带宽。



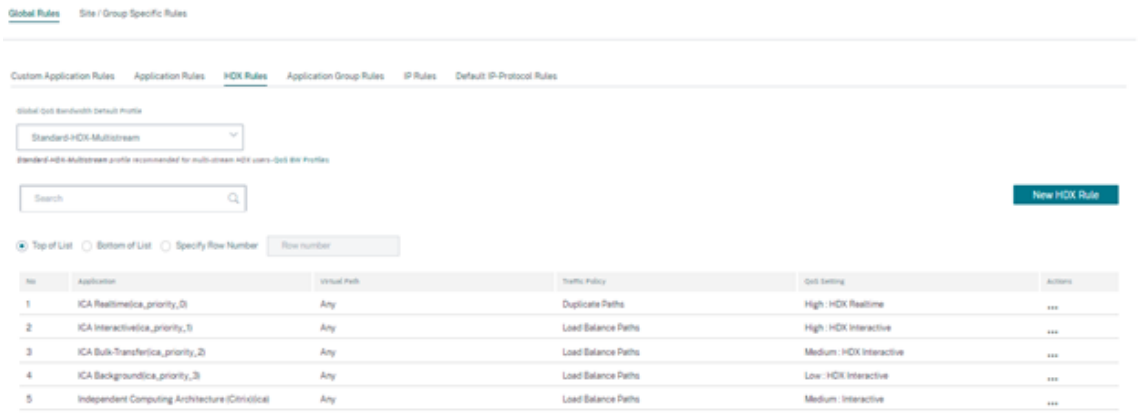
3. 选中“站点数”指示器，确保积极使用新的 QoS 配置文件。



4. 导航到 配置 **> QoS > QoS** 策略 > **HDX** 规则，将启用了 HDX 报告的新 QoS 配置文件设置为 全局 **QoS** 带宽默认配置文件。

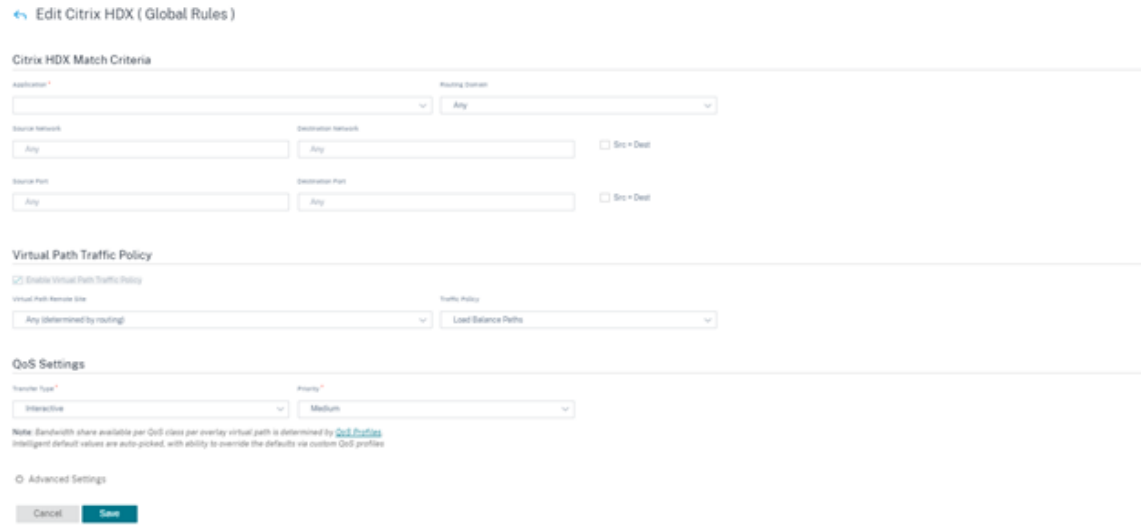


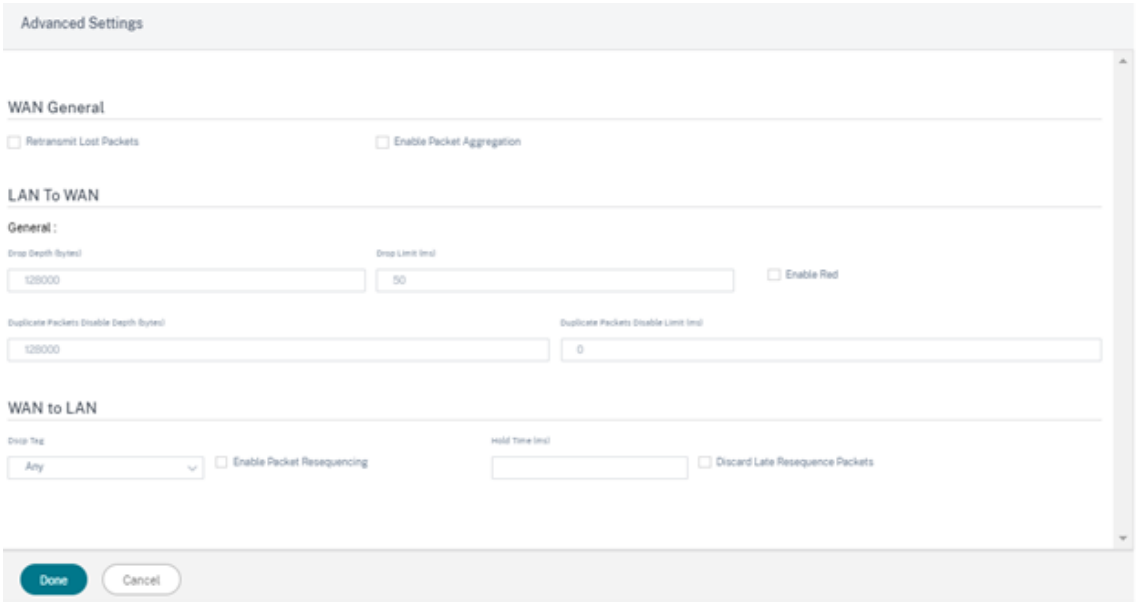
5. 添加 HDX 规则。这些配置为 HDX 连接分配正确的 QoS 设置。要查看规则详细信息或编辑规则，请导航到 **HDX Ru** les 页面的底部。在规则表上，转到 操作 列并选择 编辑。要更改任何默认规则的设置，请单击“克隆”并进行所需的修改。



可以修改以下配置：

- QoS 等级：实时、交互式、批量
- 交通政策：
  - 重复路径：流量将在多条路径上复制以提高可靠性。
  - 永久路径：除非路径不可用，否则流的流量将保持在同一路径上。
  - 负载平衡路径：流的流量在多条路径上均衡。
  - 高级设置：设置策略重传、RED 和延迟数据包。





HDX 仪表板和报告

适用于本地的 Citrix SD-WAN Orchestrator 提供 HDX 仪表板，用于详细衡量网络上每个站点、用户和会话的 Citrix 虚拟应用程序和桌面用户体验。

HDX 会话有两种类型：单流和多流。单流会话在会话中只有一个连接，而一个多流会话有四个连接。多流会话允许更高级的 QoS。单流 HDX 会话中的连接默认为交互式类，而多流 HDX 会话的最高优先级连接默认为实时类，其他三个连接到交互式类。这是可配置的。

体验质量 (QoE) 分数是介于 0—100 之间的数值。价值越高，用户体验越好。实时类流量 QoE 是根据抖动、延迟和丢失率计算的。交互式类 QoE 是根据突发率和损失率计算的。会话的 QoE 是会话中所有连接的平均值。用户的 QoE 是该用户启动的所有会话的平均值。网站的 QoE 是该网站上所有会话的平均值。

所有的统计数据都是指标：

- 对于该网站上的 HDX 流量
- 有该用户的经验
- 在该会话中的所有连接

它们不包括其他类型流量的指标。指标要么是所选期间的平均值，或者是所选期间的总数。

> 注意
>
> HDX 报告要求最低软件版本：
>
> - Citrix Virtual Apps and Desktops 7—1912 LTSR（或当前版本）
> - 适用于 Windows 19.12 LTSR（或当前版本）的 Citrix Workspace
> - SD-WAN 11.2.0（或当前版本）

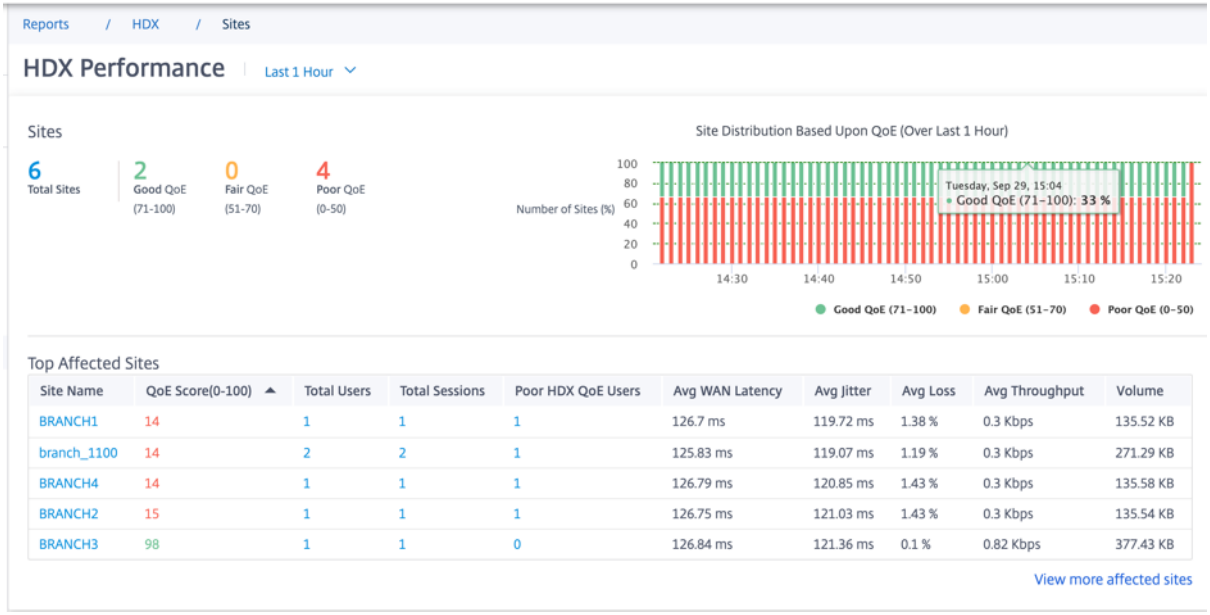
Citrix 始终建议使用最新的软件版本来获得最新的错误修复和增强功能。例如，SD-WAN 需要 11.2.3 或 11.3.1 版本才能支持更高版本的 Citrix Virtual Apps and Desktops LTSR 中引入的新 EDT 命令。

Mac 客户端和 Linux 客户端不完全支持通过 Citrix SD-WAN 进行多流 ICA 和 HDX 报告。例如，Linux 客户端支持多流，但缺少往返时间和延迟等细节。CWA 功能矩阵 可让您深入了解哪些操作系统支持具 有 **NSAP VC** 功能的多端口 ICA 和 **HDX Insight** 。

用户需要在 Citrix Gateway 加密之外访问 HDX，要么直接访问 StoreFront，要么使用 信标点 或 网络定位服务。

站点

此 HDX 报告提供了每个站点的详细 HDX 数据。要查看站点统计信息，请导航到 报告 > **HDX** > 站点。



仪表板在现场报告 HDX 流量在选定的时间间隔内（例如，过去 5 分钟、过去 30 分钟、过去 1 天、过去 1 个月等）运行。根据站点 HDX 流量的 QoE，站点性能被归类为良好 (71-100)、公平 (51-70) 或差 (0-50)。摘要部分和“受影响最多的站点”表中的 QoE 值是选定时间段内的平均值。时间序列图形报告显示具有延时的详细历史记录。每个栏显示当时优秀、公平和差的 QoE 网站的百分比。

您还可以在基于 QoE 的站点 分布图表下查看当时有“良好”、“一般”和“差”的网站数量（以 百分比表示）。将鼠标悬停在颜色栏上可查看处于良好/公平/不佳状态的网站的百分比数量。

> 注意
>
> - 统计数据是在一个方向收集的，从远程一侧收集到当前站点。例如，对于站点 A 和站点 B 之间的会话，收集站点 A 的报告是关于从站点 B 进入站点 A 的流量的，而站点 B 的报告则收集来自站点 A 进入站点 B 的流量。因此，Site-A 和 Site-B 上同一会话的统计数据可能会有所不同。
> - “受影响最大的站点”表仅显示前 5 个受影响最严重的站点。默认情况下，它显示了 QoE 分数最低的 5 个站点。但是，每列都是可排序、升序或降序的，并用作查询条件。例如，单击“平均抖动”列标题可切换显示

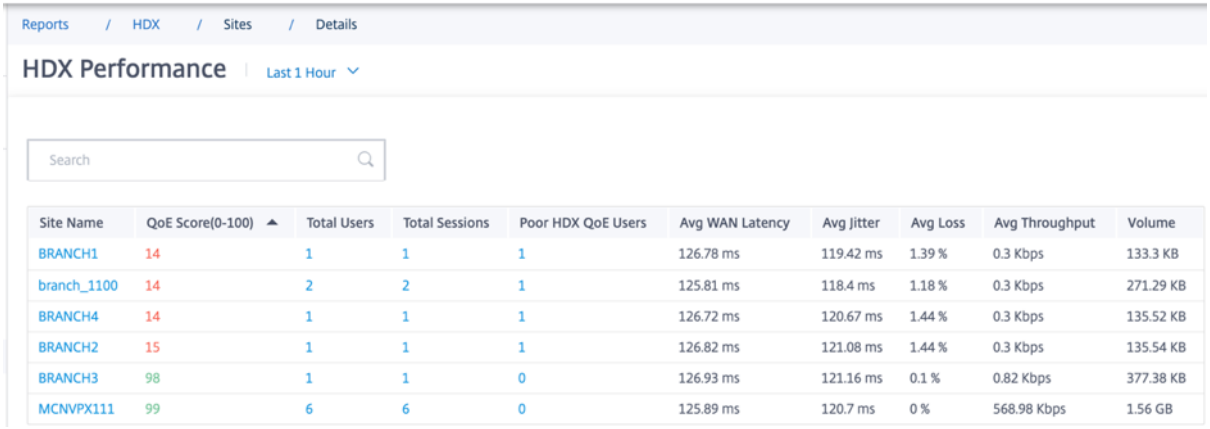
> 平均抖动最低的 5 个站点或平均抖动最高的 5 个站点。其他专栏也是如此。要查看选定时间段内有 HDX 流量的所有站点的详细信息，请单击“查看更多受影响的站点”。

以下是每个网站的详细信息：

- 站点名称：站点名称。
- **QoE** 分数 **(0-100)**：该网站的平均 QoE 分数。
- 用户总数：选定时段内在网站上看到的活跃 HDX 用户总数。
- 会话总数：选定时段内在网站上看到的 HDX 会话总数，包括单流和多流会话。
- 糟糕的 **HDX QoE** 用户：QoE 不佳（低于 50）的 HDX 用户数量。
- 平均 **WAN** 延迟：广域网从远程站点到此站点的平均延迟。
- 平均抖动：所选持续时间内的平均抖动值。
- 平均丢失率：所选持续时间内的平均丢包百分比值。
- 平均吞吐量：所选持续时间内的平均数据吞吐量值。
- 流 @@ 量：在此网站上看到的总流量。适用于本地 GUI 的 Citrix SD-WAN Orchestrator 可能会根据数字值调整和更改单位。

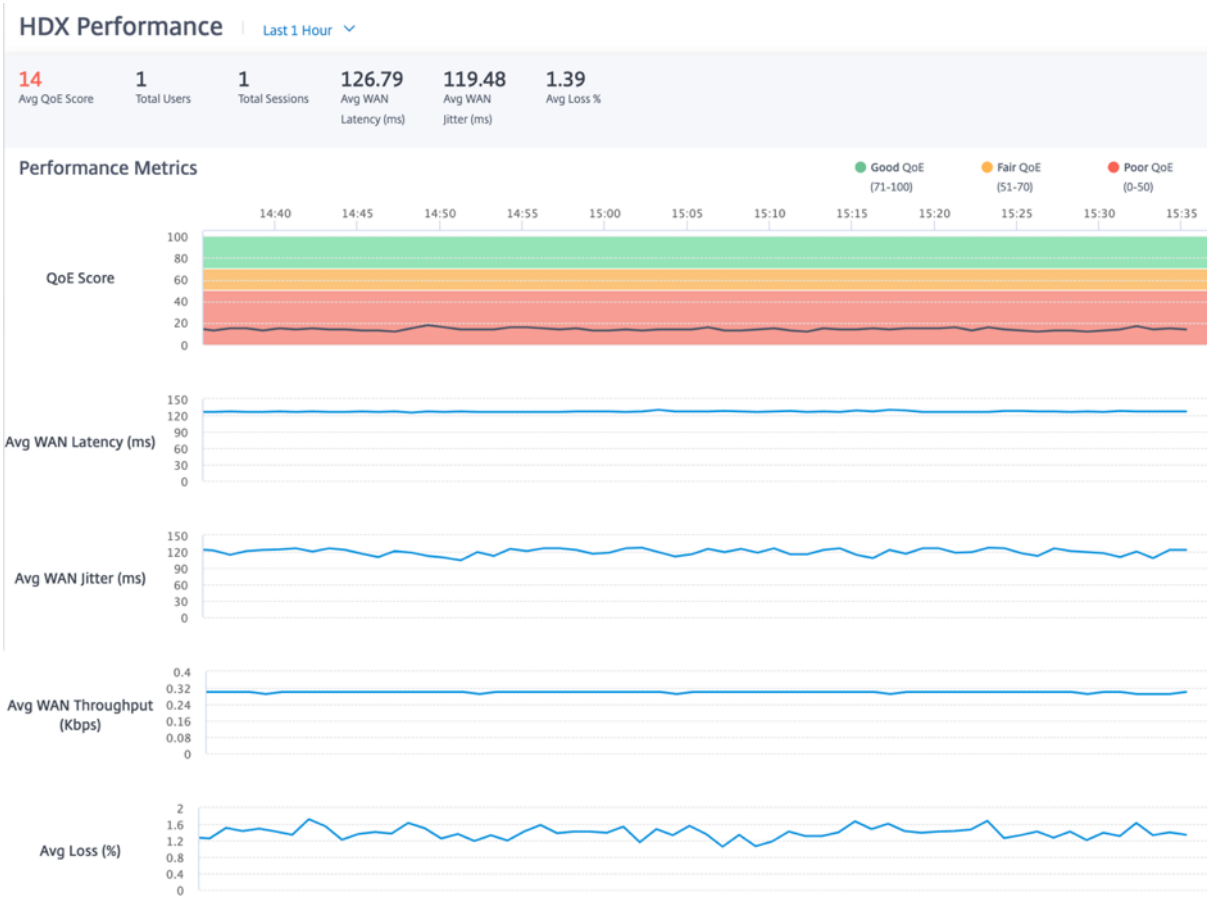
单击任何列标题都会显示在该列上排序的报告。单击“查看更多受影响的站点”以查看所有站点的报告。单击任何一行都会显示该站点的详细报告。

以下屏幕截图中的表格是显示所有站点的报告表的示例。它与“受影响最多的站点”表具有相同的列。



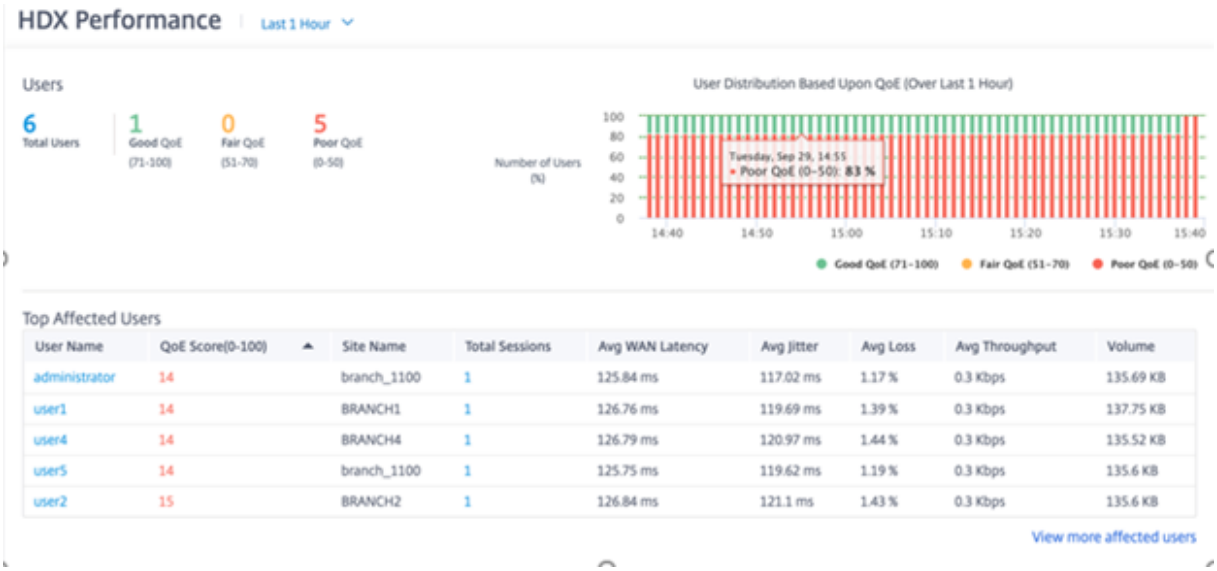
Site Name	QoE Score(0-100)	Total Users	Total Sessions	Poor HDX QoE Users	Avg WAN Latency	Avg Jitter	Avg Loss	Avg Throughput	Volume
BRANCH1	14	1	1	1	126.78 ms	119.42 ms	1.39 %	0.3 Kbps	133.3 KB
branch_1100	14	2	2	1	125.81 ms	118.4 ms	1.18 %	0.3 Kbps	271.29 KB
BRANCH4	14	1	1	1	126.72 ms	120.67 ms	1.44 %	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

单击单个站点行可以查看性能指标的图形表示。将鼠标悬停在图形上可提供更多细节。



用户

要查看 HDX 用户报告，请导航到 报告 **> HDX >** 用户。



用户报告显示了每个用户在选定时间段（例如，最近 5 分钟、最近 30 分钟、最近 1 天、最近 1 个月等）内所经历的表

现。如果用户在选定时间段内在多个站点上，则该用户登录的最后一个站点将显示在报告中。根据 HDX 流量的 QoE 评分，用户体验被分为良好 (71-100)、公平 (51-70) 或差 (0-50)。摘要部分和“受影响最大的用户”表中的 QoE 值是选定时段内的平均值。时间序列图形报告显示具有延时的详细历史记录。每个栏显示当时 QoE 良好、公平和差的用户的百分比。

您还可以在“基于 QoE 的用户 分布”图表下查看当时有“良好”、“一般”和“差”的 **QoE** 的用户数量（以 百分比表示）。将鼠标悬停在颜色条上可查看处于良好/公平/不佳状态的用户百分比。

个人身份信息　目前，HDX QoE 报告有以下两个个人身份信息 (PII) 字段：

- 用户名：显示用户名。
- **IP** 地址：显示客户端 IP 地址。

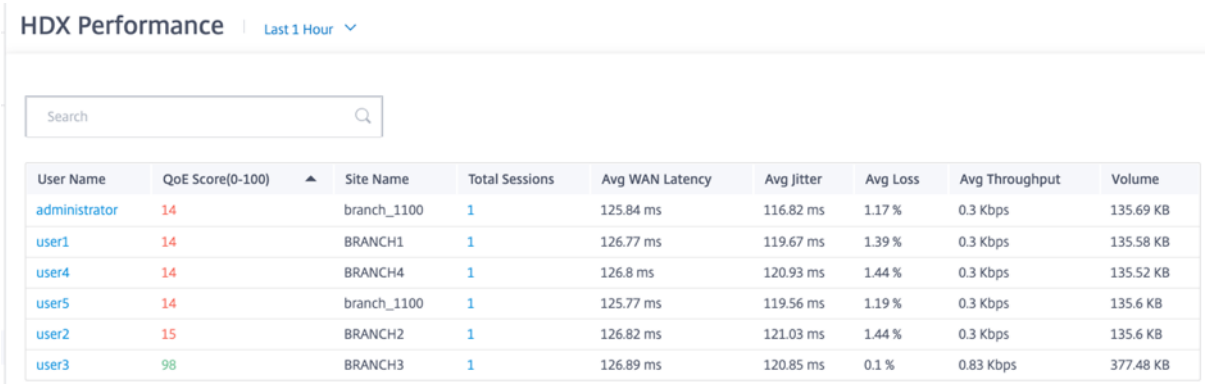
> 注意
>
> - 当用户名不可用时，IP 地址将显示在“用户名”字段中。
> - HDX 用户报告基于客户端 SD-WAN 的统计信息，而不是虚拟交付代理 (VDA) 端 SD-WAN 的统计信息。这反映了最终用户的 HDX 体验。
> - “受影响最大的用户”表仅显示前 5 个受影响最大的用户。默认情况下，它显示 QoE 最低的前 5 位用户。但是，每列都是可排序、升序或降序的，并用作查询条件。例如，单击“平均抖动”列标题可切换显示平均抖动最低的 5 个用户或平均抖动最高的 5 个用户。要查看在选定时间段内拥有 HDX 流量的所有用户的详细信息，请单击“查看更多受影响的用户”。

以下是每个用户的详细信息：

- 用户名：用户名。
- **QoE** 分数 **(0-100)**：该用户的平均 QoE 分数。
- 站点名称：用户登录的站点名称。
- 会话总数：来自该用户的活跃 HDX 会话总数，包括单流和多流会话。
- 平均 **WAN** 延迟：在客户端体验到的 WAN 上的平均延迟。
- 平均抖动：所选持续时间内的平均抖动值。
- 平均丢失率：所选持续时间内的平均丢包百分比值。
- 平均吞吐量：所选持续时间内的平均数据吞吐量值。
- 流 @@ 量：该用户使用的总流量。适用于本地 GUI 的 Citrix SD-WAN Orchestrator 可能会根据数字值调整和更改单位。

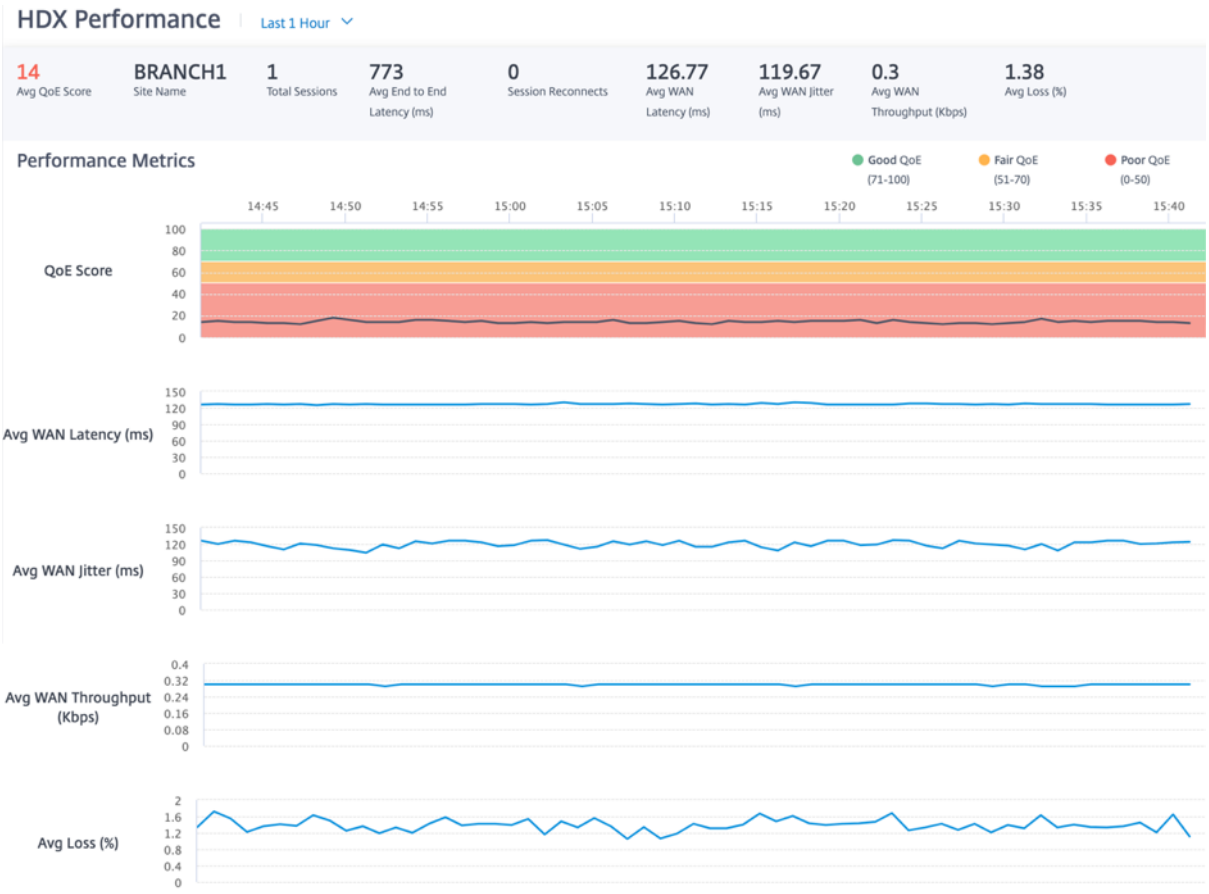
单击任何列标题都会显示在该列上排序的报告。单击“查看更多受影响的用户”以查看所有用户的报告。单击任何一行都会显示该用户的详细报告。

以下屏幕截图是显示所有用户的报告示例。它与“受影响最大的用户”表具有相同的列。



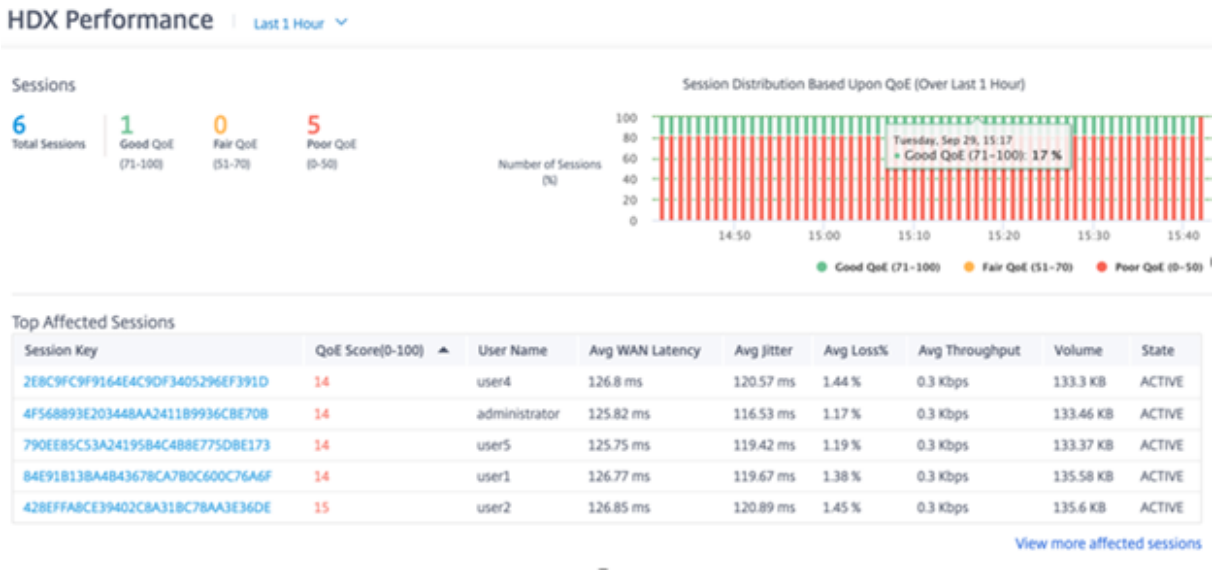
User Name	QoE Score(0-100)	Site Name	Total Sessions	Avg WAN Latency	Avg Jitter	Avg Loss	Avg Throughput	Volume
administrator	14	branch_1100	1	125.84 ms	116.82 ms	1.17 %	0.3 Kbps	135.69 KB
user1	14	BRANCH1	1	126.77 ms	119.67 ms	1.39 %	0.3 Kbps	135.58 KB
user4	14	BRANCH4	1	126.8 ms	120.93 ms	1.44 %	0.3 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

单击单个用户行可以查看该用户性能指标的图形表示。



会话

会话报告提供了会话级别的详细信息。要查看会话报告，请导航到 报告 **> HDX >** 会话。



控制面板显示在选定时间段（例如，最近 5 分钟、最近 30 分钟、最近 1 天、最近 1 个月等）内运行的 HDX 会话的报告。根据该时段的 QoE，会话分为好（71-100）、公平（51-70）或差（0-50）。摘要部分和受影响最大表中的 QoE 值是所选期间的平均值。时间序列图形报告显示具有延时的详细历史记录。每个栏显示当时良好、公平和差的 QoE 会话的百分比。

您还可以在“基于 QoE 的会话 分布”图表下查看当时有“良好”、“一般”和“差”的会话数量（以 百分比表示）。将鼠标悬停在颜色栏上可查看处于良好/公平/不佳状态的会话百分比。

> 注意
>
> - HDX 会话报告基于来自客户端 SD-WAN 的统计数据，而不是 VDA 端 SD-WAN。这反映了最终用户的 HDX 体验。
> - “受影响最多的会话”表仅显示前 5 个受影响最大的会话。默认情况下，它显示 QoE 最低的前 5 个会话。但是，每列都是可排序、升序或降序的，并用作查询条件。例如，单击“平均抖动”列标题可切换显示平均抖动最低的 5 个会话或平均抖动最高的 5 个会话。要查看选定时间段内所有 HDX 会话的详细信息，请单击“查看更多受影响的会话”。

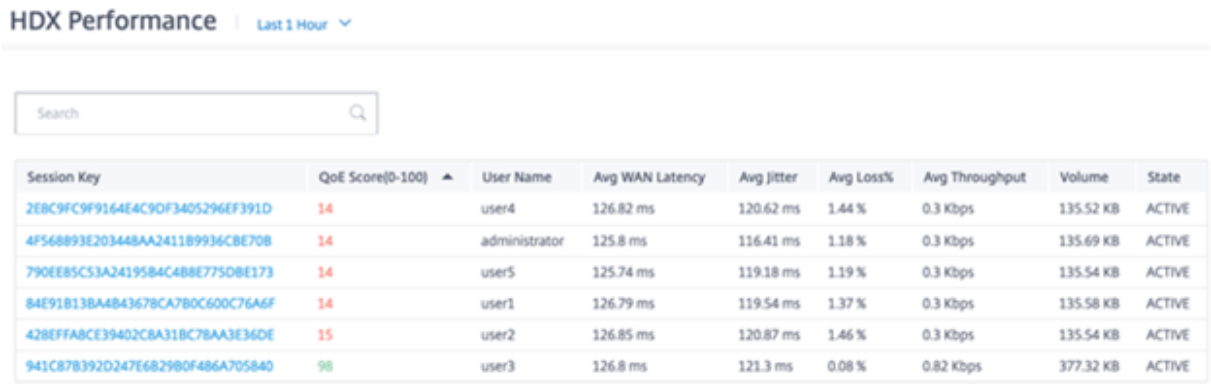
以下是每个会话顶部会议的详细信息：

- 会话密钥：HDX 会话的唯一标识。
- **QoE** 分数 **(0-100)**：本次会话的平均 QoE。
- 用户名：用户名。
- 平均 **WAN** 延迟：选定时长内会话的平均 WAN 延迟，在客户端测量。
- 平均抖动：所选时长内会话的平均抖动值。
- 平均损失百分比：选定持续时间内会话的平均损失百分比值。
- 平均吞吐量：选定持续时间内会话的平均吞吐量值。
- 流 @@ 量：此会话使用的总流量。适用于本地 GUI 的 Citrix SD-WAN Orchestrator 可能会根据数字值调整和更改单位。

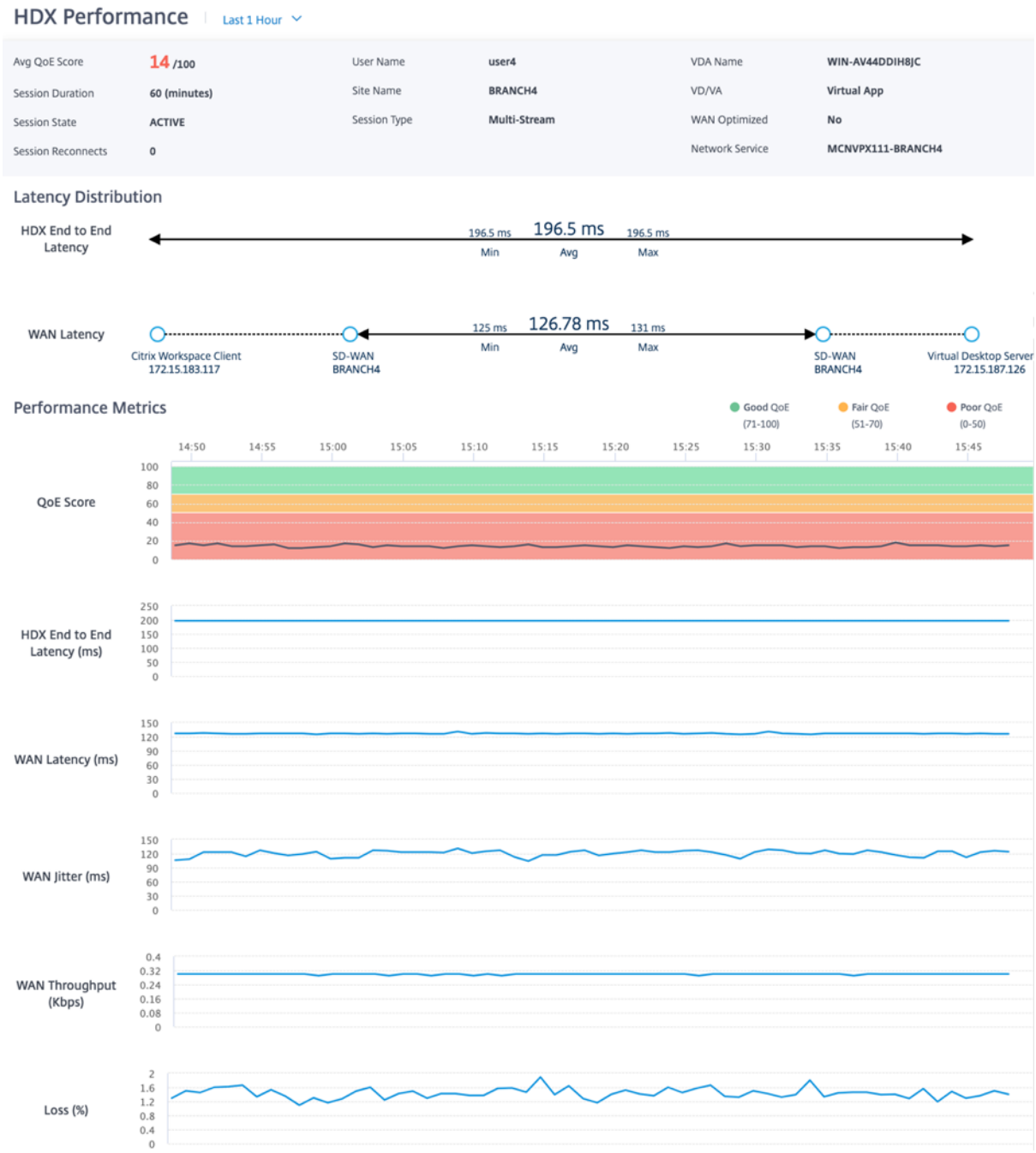
- 状态：会话的状态。

单击任何列标题，将显示在该列上排序的报告。单击“查看更多受影响的会话”以查看所有会话的报告。单击任何一行都会显示该会话的详细报告。

以下屏幕截图是显示所有会话的报告表的示例。它与“受影响最多的会话”表具有相同的列。



单击单个会话键可以查看性能指标的图形表示以及影响 QoE 的所有变量的详细信息。



- 平均 **QoE** 分数：选定时段内的平均 QoE。
- 用户名：启动此会话的用户。
- **VDA** 名称：用于交付已发布桌面/应用程序的 VDA 的名称。
- 会话持续时间：该会话在所选时段内的活动时间。
- 站点名称：启动会话时用户的客户端站点。
- **VD/VA**：此会话是 虚拟桌面 还是 虚拟应用程序 会话。
- 会话状态：选定时段结束时会话的状态。
- 会话类型：上次启动会话时会话是多流会话还是单流会话。

- 广域网优化：此会话是否经过广域网优化。如果 SD-WAN 是 PE 平台，则为 HDX 启用 WAN 优化，并且此会话已优化，则此字段显示为真。
- 会话重新连接：如果会话由于网络问题自动断开连接并重新连接，则此字段是此类事件的发生次数。
- 网络服务：这是传送此会话的服务名称。
- **HDX** 端到端延迟：VDA 与客户端之间往返时间值的一半。
- 广域网延迟：从 VDA 端 SD-WAN 到客户端 SD-WAN 的延迟。

知识产权规则

October 21, 2022

IP 规则 可帮助您为网络创建规则，并根据规则做出某些服务质量 (QoS) 决策。您可以为网络创建自定义规则。例如，您可以将规则创建为：如果源 IP 地址为 172.186.30.74，目标 IP 地址为 172.186.10.89，则将 流量策略 设置为 持久路径，将 流量类型 设置为 实时。

您可以为流量创建规则，并将这些规则与应用程序和类关联起来。您可以指定筛选流量的条件，并可以应用常规行为、LAN 到 WAN 行为、WAN 到 LAN 行为和数据包检查规则。

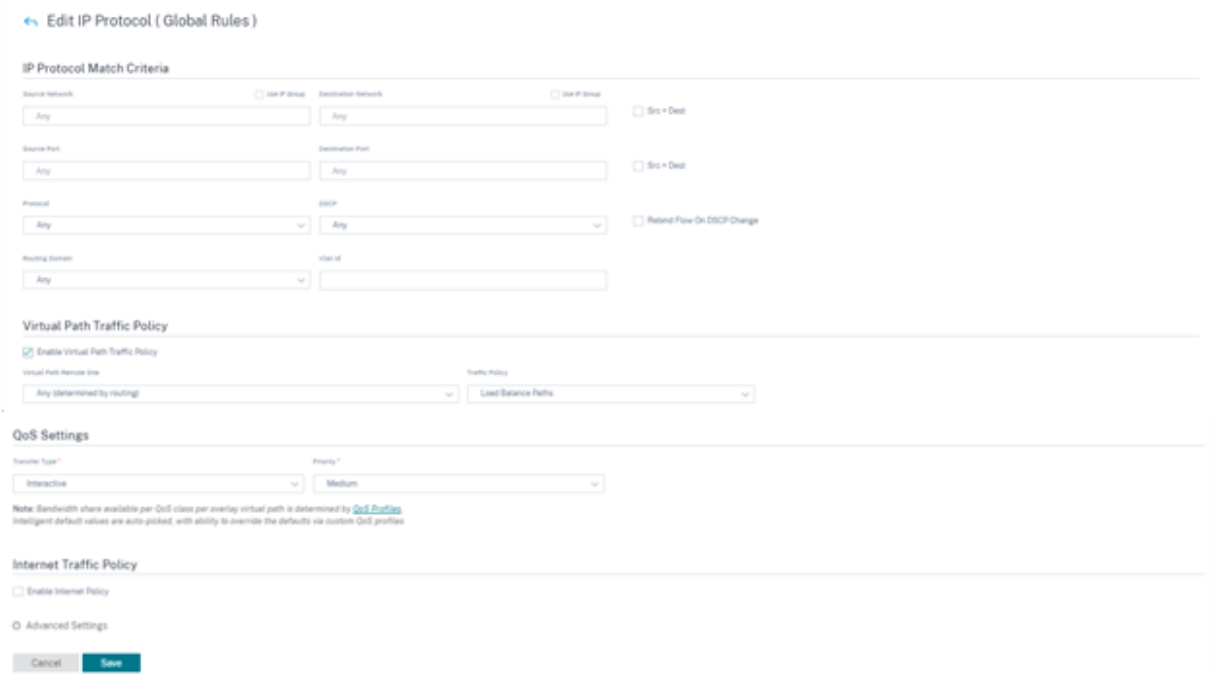
您可以在网络级别创建全局和特定站点的 IP 规则。如果站点与全局创建的规则相关联，则可以创建特定于站点的规则。在这种情况下，特定于站点的规则优先，并优先于全局创建的规则。

默认 IP 协议规则 HTTP、HTTPS 和 ALTHTTPS 始终出现在规则表列表的顶部。但是，站点特定的 IP 规则（一旦创建）会出现在规则表中的 HTTP、HTTPS、ALTHTTPS 和全局 IP 规则上方。

创建 **IP** 规则

要创建 IP 规则，请导航到 配置 **> QoS > QoS** 策略 > **IP** 规则。选择“全局规则”选项卡用于在全局级别创建 IP 规则，或选择“站点**/**组特定规则”以在站点级别创建规则。

单击 **IP** 规则部分下的新建 **IP** 规则。

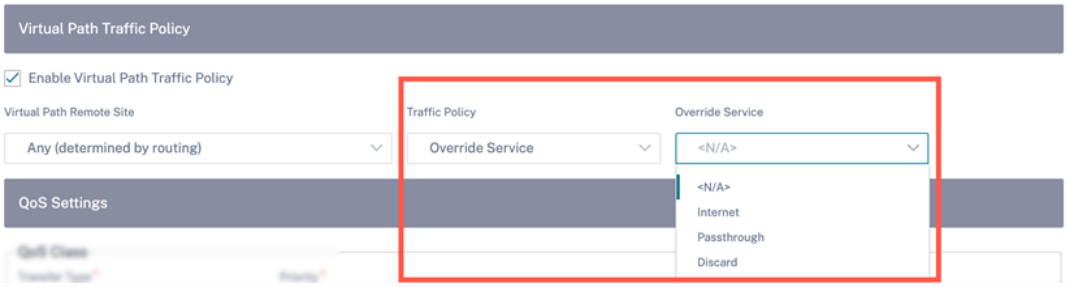


- IP 协议匹配标准
  - 添加/删除站点：（仅在创建特定站点的 IP 规则时可用）选择站点，单击“查看”，然后单击“完成”。
  - 源网络：规则匹配的源 IP 地址和子网掩码。
  - 目标网络：规则匹配的目标 IP 地址和子网掩码。
  - 使用 **IP** 组：选中“使用 **IP** 组”复选框以从下拉列表中选择任何现有 IP 组。
  - **Src = Dst**：如果选中，则源 IP 地址也用作目标 IP 地址。
  - 源端口：规则匹配的源端口（或源端口范围）。
  - 目标端口：规则匹配的目标端口（或目标端口范围）。
  - **Src = Dst**：如果选中，则源端口也用于目标端口。
  - 协议：与规则匹配的协议。您可以选择其中一个预定义协议，也可以选择“任意”或“数字”。
  - 协议编号：仅当您从“协议”下拉列表中选择“编号”时，才会显示此字段。当您选择协议号时，与该协议关联的整数将用于后端配置。
  - **DSCP**：与规则匹配的 IP 标头中的 DSCP 标记。
  - 路由域：规则匹配的路由域。
  - **VLAN ID**：输入规则的 VLAN ID。VLAN ID 标识进出虚拟接口的流量。使用 VLAN ID 作为 0 来指定本地流量或无标记流量。
  - 在 **DSCP** 更改时重新绑定流程：如果选择此选项，则在匹配标准方面原本相同的流量如果 DSCP 字段不同，则被视为单独流。
- 虚拟路径流量策略

  选中“启用虚拟路径流量策略”复选框。
  - 虚拟路径远程站点：选择远程站点的虚拟路径。

- 流量策略：根据需要选择以下流量策略之一。
  - 负载平衡路径：流量的应用程序流量在多条路径上均衡。通过最佳路径发送流量，直到使用该路径为止。剩余的数据包将通过下一个最佳路径发送。
  - 持久路径：应用程序流量将保持在同一路径上，直到路径不再可用为止。选择以下 持久性策略之一：
    - 在 @@ 源链路上保留：应用程序流量将保留在源链路上，直到该路径不再可用。
    - 如果可用，请在 **MPLS** 链接上保留，否则保留在原始链路上：应用程序流量保留在 MPLS 链路上。如果 MPLS 链路不可用，则流量将保留在始发链路上。
    - 如果可用，则保留在互联网链接上，否则保留在原始链接上：应用程序流量保留在互联网链接上。如果 Internet 链接不可用，则流量将保留在原始链路上。
    - 如果可用，则保留在私有 **Intranet** 链接上，否则保留在原始链接上：应用程序流量保留在私有 Intranet 链接上。如果私有 Intranet 链接不可用，则流量将保留在原始链路上。

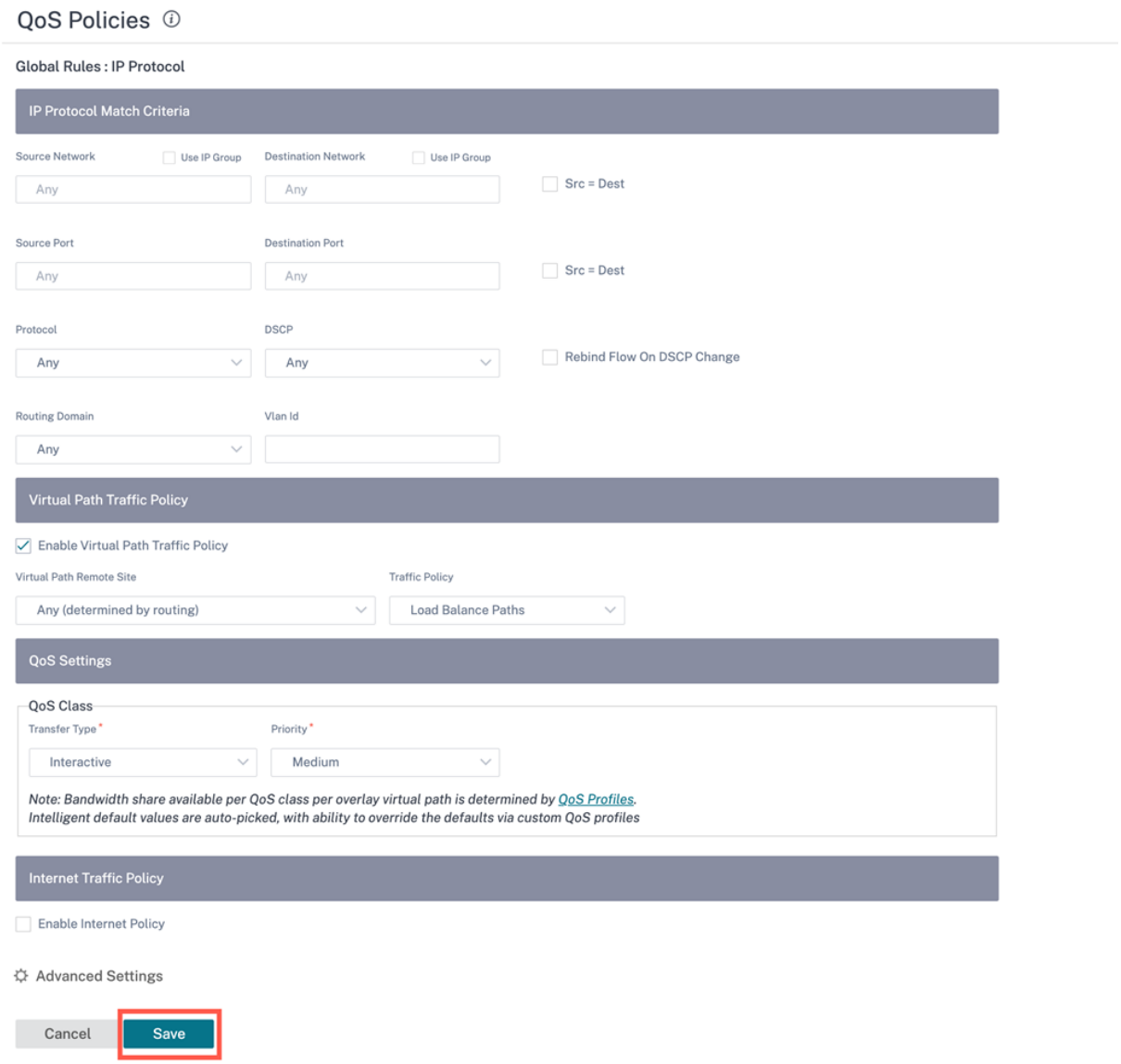
    持续阻抗 是指应用程序流量在链路上停留的时间（以毫秒为单位）。
  - 重复路径：应用程序流量在多条路径上复制，从而提高了可靠性。
  - 覆盖服务：流量的流量将覆盖到其他服务。选择虚拟路径服务覆盖的服务类型为 Intranet、Internet、直通或 Discard。



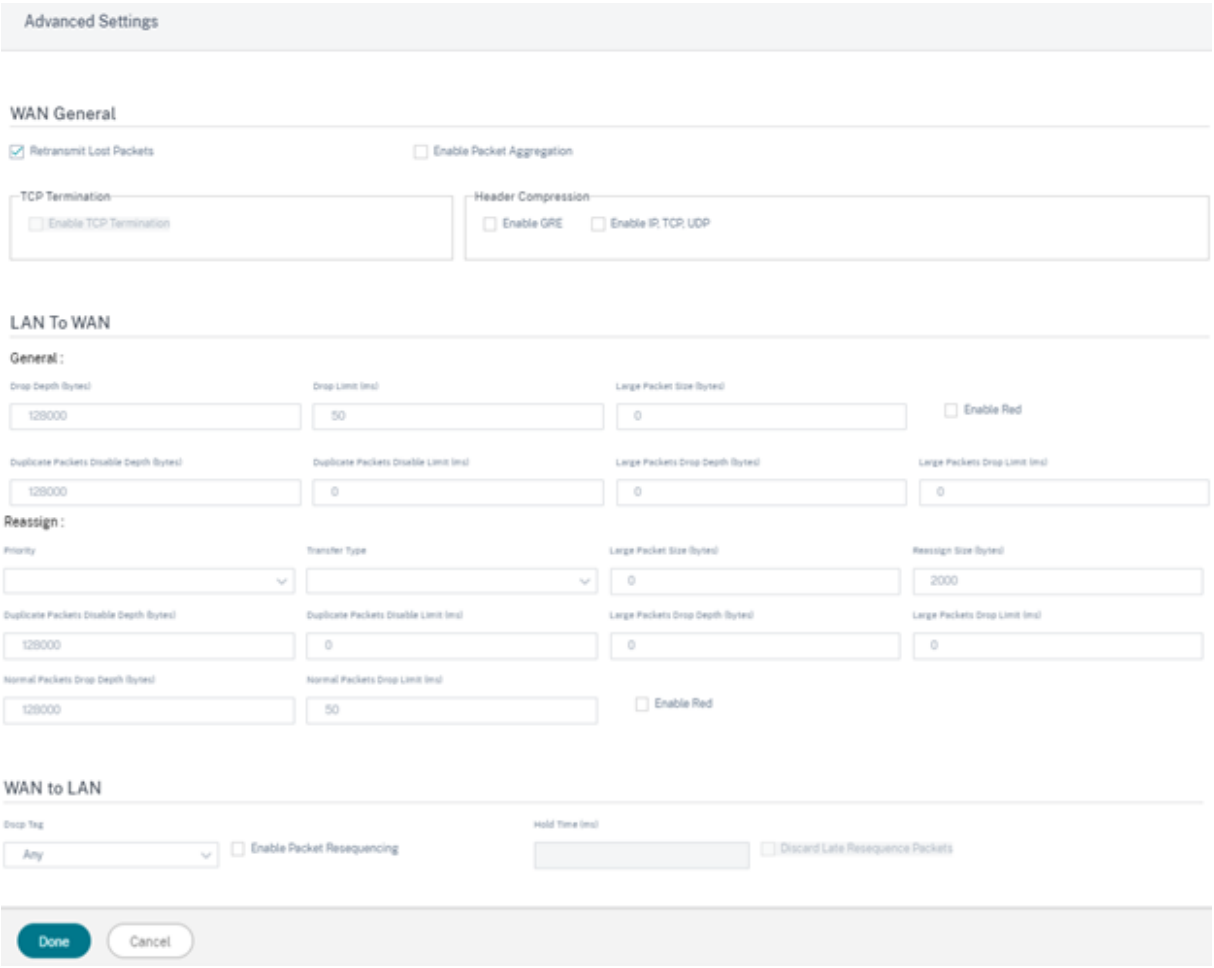
- QoS 设置（QoS 类别）
  - 转账类型：选择以下转账类型之一：
    - 实时：用于低延迟、低带宽、对时间敏感的流量。实时应用程序具有时间敏感性，但实际上并不需要高带宽（例如 IP 语音）。实时应用程序对延迟和抖动很敏感，但可以承受一些损失。
    - 交互式：用于具有中低延迟要求和中低带宽要求的交互式流量。通常情况下，在客户端与服务器之间进行交互。通信可能不需要高带宽，但对丢失和延迟非常敏感。
    - 批量：用于高带宽流量和可容忍高延迟的应用程序。处理文件传输并需要高带宽的应用程序被归类为批量类。这些应用很少涉及人为干扰，主要由系统自己处理。
  - 优先级：为所选传输类型选择优先级。
- 互联网流量政策
  - 选中“启用互联网策略”复选框以配置互联网流量策略。
  - 模式：为符合规则的流量发送和接收数据包的方法。您可以根据需要选择 覆盖服务 或 **WAN** 链接。
  - **WAN** 链接：启用 Internet 负载平衡时，与规则匹配的流量将使用的 WAN 链接。

- 覆盖服务：与规则匹配的流的目标服务。

> 注意
>
> 虚拟路径服务不能覆盖其他虚拟路径服务。



高级设置



- 广域网通用
  - 重新传输丢失的数据包：通过可靠的服务将符合此规则的流量发送到远程设备，并重新传输丢失的数据包。
  - 启用数据包聚合：将小数据包聚合成较大的数据包。
  - 启用 **TCP** 终止：启用此流的 TCP 终止流量。缩短了数据包确认的往返时间，从而提高了吞吐量。
  - 启用 **GRE**：压缩 GRE 数据包中的标头。
  - 启用 **IP**、**TCP** 和 **UDP**：压缩 IP、TCP 和 UDP 数据包中的标头。

    > 注意
    >
    > IPv6 数据包不支持标头压缩。

- 局域网到 WAN

  常规

  - 丢弃深度（字节）：队列深度阈值，超过该阈值后，数据包将被丢弃。
  - 丢弃限制：在类调度程序中等待的数据包被丢弃的时间。不适用于批量类。

- 大型数据包大小：小于或等于此大小的包将被分配在“大型数据包丢弃深度 （字节）”和“大型数据包丢弃限制 (ms)”字段中指定的丢弃限制和丢弃深 度值。大于此大小的数据包将分配默认丢弃限制和丢弃深度字段中指定的值。
- 启用 **RED**：随机早期检测 (RED) 通过在拥塞发生时丢弃数据包来确保公平共享类资源。
- 重复数据包禁用深度（字节）：类调度器的队列深度，此时未生成重复数据包。
- 重复数据包禁用限制：可以禁用复制以防止重复数据包消耗带宽的时间。
- 大型数据包丢弃深度（字节）：如果队列深度超过此阈值，则丢弃数据包并计算统计数据。
- 大型数据包丢弃限制 **(ms)**：大于或等于大型数据包大小的数据包在类调度器中必须等待的最大估计时间。如果估计时间超过此阈值，则丢弃数据包并计算统计数据。对批量课程无效。

重新分配

- 优先级：您可以根据需要设置备用 WAN 链接的优先级。备用 WAN 链路优先级表示备用 WAN 链接变为活动状态的顺序。高优先级备用 WAN 链路首先变为活动状态。低优先级 WAN 链路最后变为活动状态。
- 转移类型：选择要与此规则关联的转移类型。
- 重复数据包禁用深度（字节）：类调度器的队列深度，此时不会生成重复数据包。
- 重复数据包禁用限制：指定数据包在不执行复制之前在队列中等待的时间，这可以防止重复数据包在带宽受限时消耗带宽。
- 大型数据包丢弃深度（字节）：如果队列深度超过此阈值，则丢弃数据包并计算统计数据。
- 大型数据包丢弃限制 **(ms)**：如果估计时间超过此阈值，则丢弃数据包并计算统计数据。对批量课程无效。
- 普通数据包丢弃深度（字节）：如果队列深度超过此阈值，则丢弃数据包并计算统计数据。
- 正常数据包丢弃限制 **(ms)**：如果估计时间超过此阈值，则丢弃数据包并计算统计数据。对批量课程无效。

- WAN 到局域网

  - **DSCP** 标签：在将数据包发送到局域网之前，DSCP 标记应用于在广域网到局域网上匹配此规则的数据包。
  - 启用数据包重新排序：与规则匹配的流量被标记为顺序顺序，数据包在 WAN to LAN 设备上被重新排序（如有必要）。
  - 保持时间：保留数据包以进行重新排序的时间间隔，在此之后数据包将被发送到局域网。计时器到期时，数据包将发送到 LAN，无需再等待必备序列号。

    如果规则将流量策略作为重复路径，则默认保持时间为 80 ms。否则，TCP 规则的默认值为 900 毫秒，非 TCP 规则的默认值为 250 毫秒。
  - 丢弃延迟重排序数据包：丢弃在重新排序所需的数据包发送到局域网后到达的无序数据包。

单击“保存”保存配置设置。在“配置”> “**QoS** 策略”页面上单击“验证 配置”以验证任何审计错误。

验证 **IP** 规则

要验证 IP 规则，请导航到 报告 **>** 实时 **>** 流量。选择要查看流量信息和要显示的流量数量的站点。单击“自定义列”，然后选中与要查看的流量信息对应的复选框。验证流信息是否符合配置的规则。

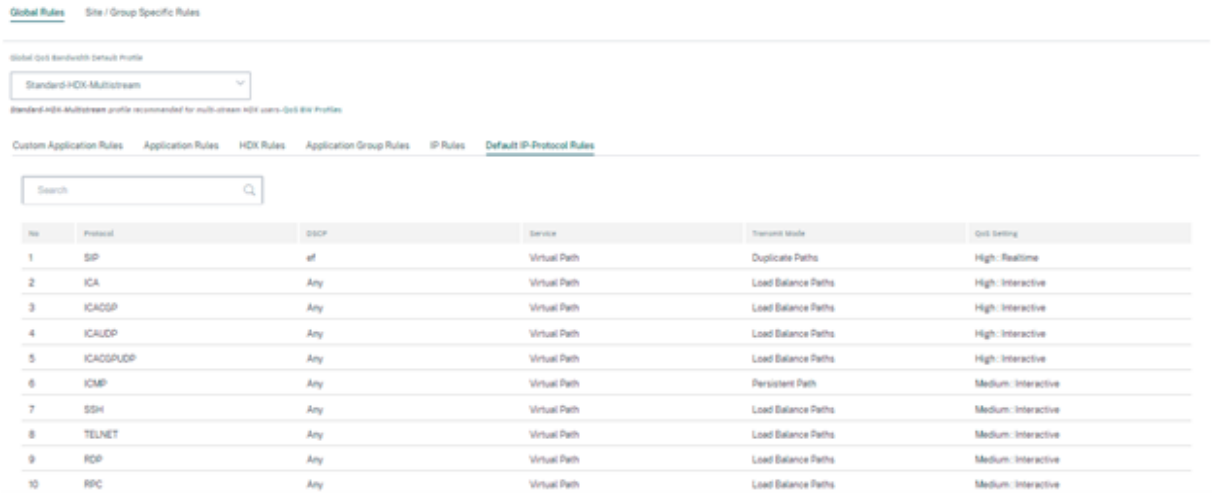
导航到 报告 **>** 实时 **>** 统计信息，然后选择 规则。选择站点，然后单击“检索最新数据”。验证配置的规则。有关更多信息，请参阅 站点报告。

QoS 策略

October 21, 2022

管理员可以定义应用程序和流量策略。这些策略有助于为应用程序启用流量引导、服务质量 (QoS) 和过滤功能。指定定义的规则是可以在网络中的所有站点上全局应用还是适用于某些特定站点。

策略以多个规则的形式定义，这些规则将按用户定义的顺序应用。



创建新规则

管理员必须根据优先级放置定义的规则。优先级根据列表顶部、列表底部或特定行等参数进行分类。

建议在顶部为应用程序或子应用程序设置 更具体 的规则，然后对代表更广泛流量的应用程序使用 不太具体 的规则。

例如，你可以为 Facebook Messenger（子应用程序）和 Facebook（应用程序）创建特定的规则。将 Facebook 信使规则放在 Facebook 规则之上，以便选择 Facebook 信使规则。如果顺序被撤销，Facebook Messenger 是 Facebook 应用程序的子应用程序，Facebook Messenger 规则将不会被选中。正确下达订单很重要。

比赛标准

为已定义的规则选择流量，例如：

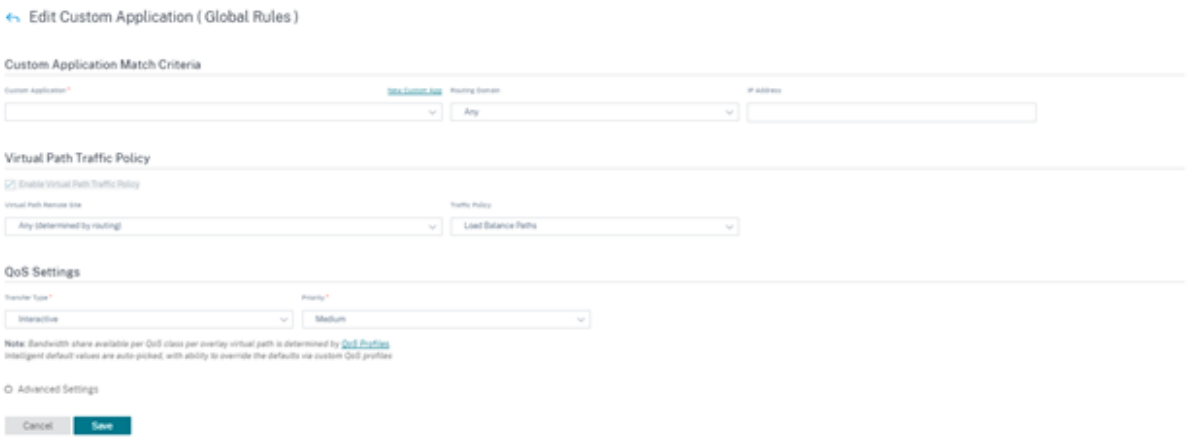
- 一个应用程序
- 自定义应用程序
- 一组应用程序或基于 IP 协议的规则

规则范围

指定定义的规则是可以在网络中的所有站点上全局应用还是适用于某些特定站点。

应用程序控制

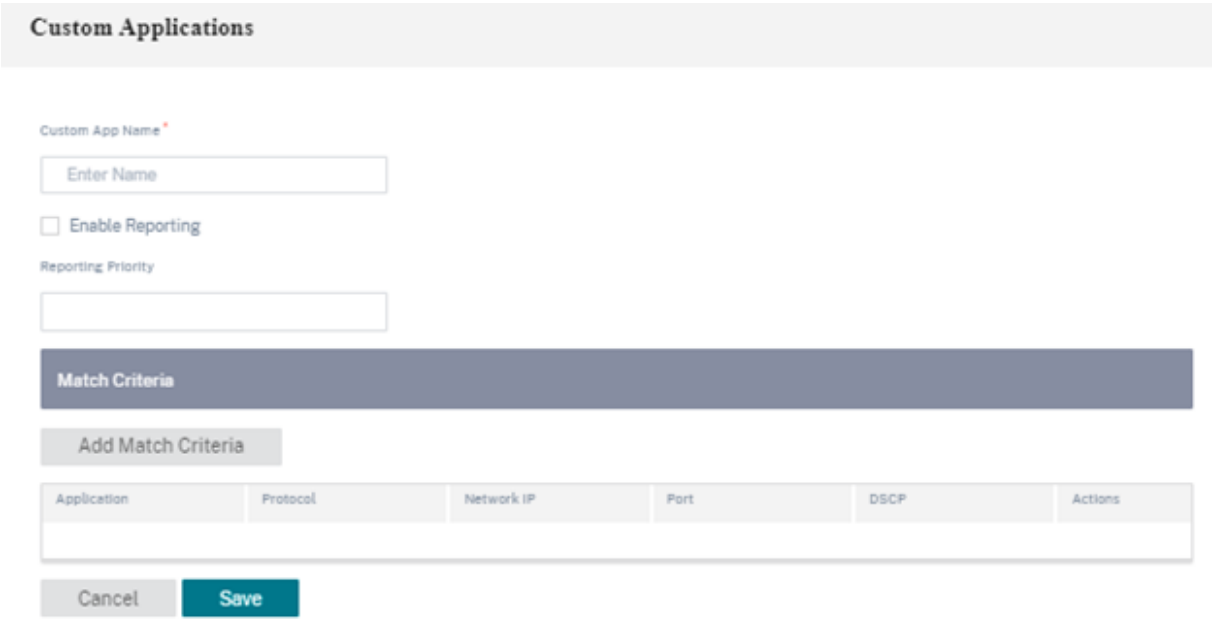
导航到 配置 > **QoS** > 自定义应用程序规则。指定需要如何引导流量。



新建自定义应用程序：从列表中选择匹配标准。管理员可以通过为以下名称命名来添加新的自定义应用程序：

- 自定义应用程序
- 协议（TCP、UDP、ICMP）
- 网络 IP/前缀
- 端口
- DSCP 标记

您还可以创建基于域名的自定义应用程序。

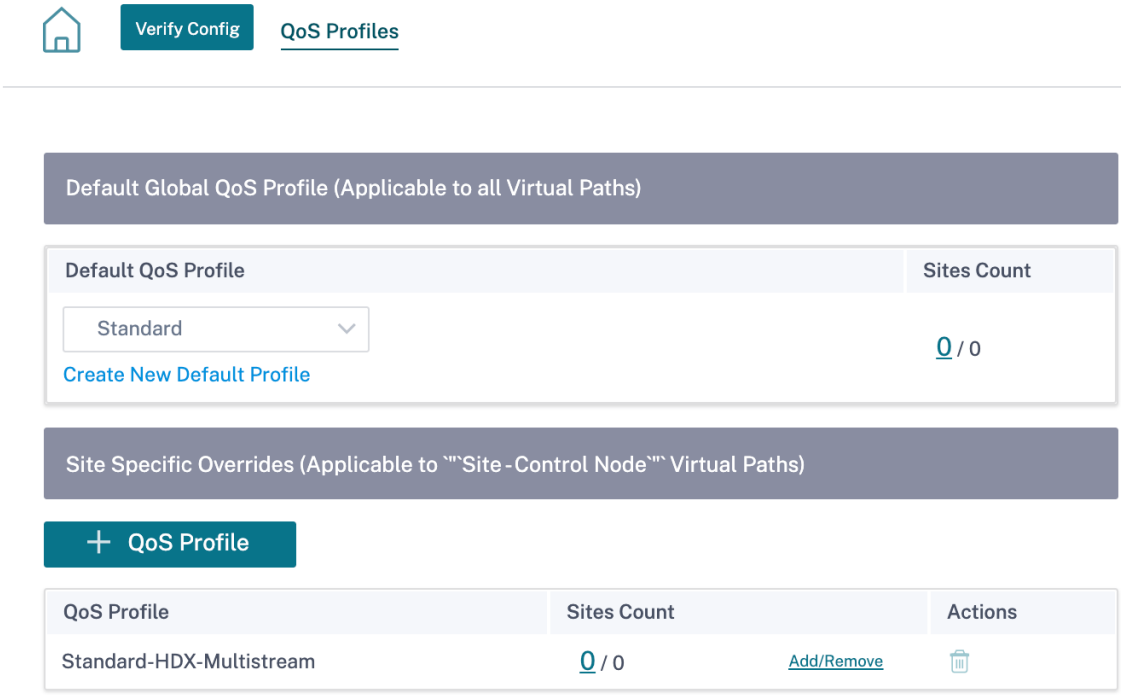


在“配置”> “**QoS** 策略”页面上单击“验证 配置”以验证任何审计错误。

IP 规则　**IP** 规则 可帮助您为网络创建规则，并根据规则做出某些服务质量 (QoS) 决策。有关 IP 规则的更多信息，请参阅 IP 规则。

QoS 配置文件

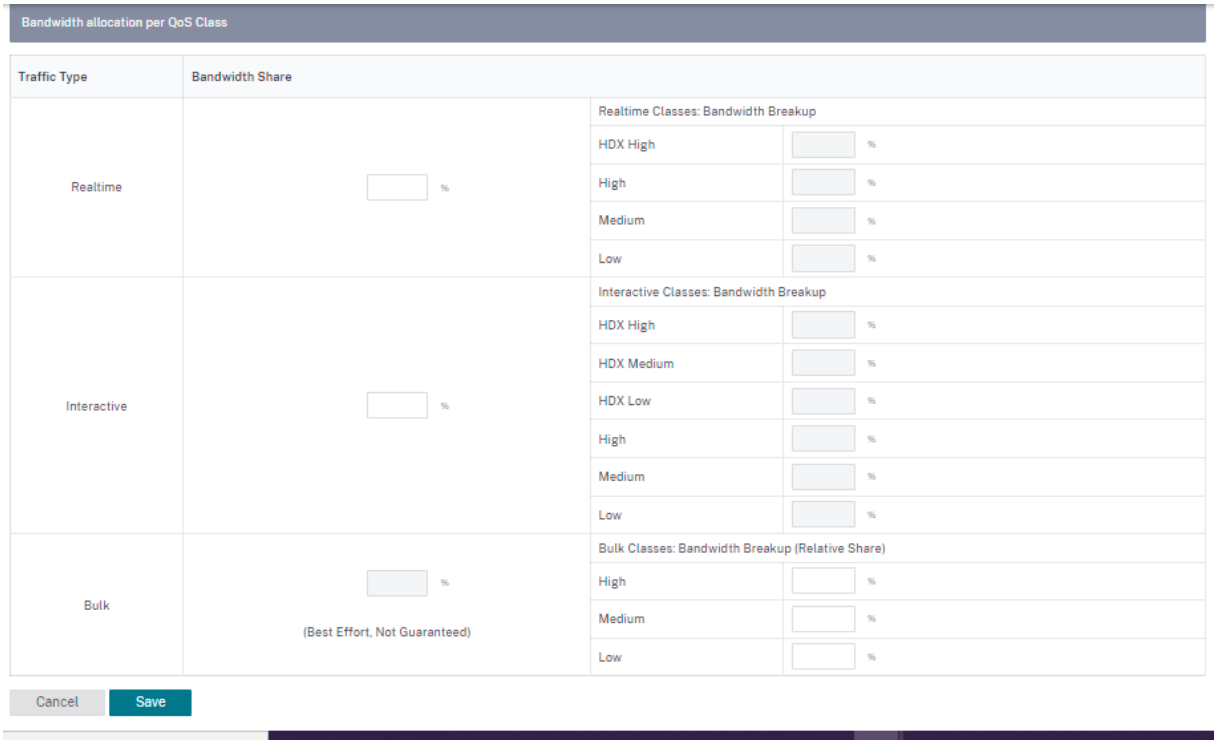
服务质量 (QoS) 部分有助于使用 **+ QoS** 配置文件选项创建 **QoS** 配置文件。QoS 配置文件为某些流量提供更好的服务。QoS 的目标是提供优先级，包括流量类型（实时、交互和批量类别）和专用带宽。带宽分解以百分比值表示。这也改善了损耗特性。



在“配置”> “**QoS** 策略”页面上单击“验证 配置”以验证任何审计错误。

自定义 **QoS** 配置文件

如果正在使用虚拟路径默认集，则可以在 配置 **>**QoS > QoS 配置文件下修改类别。单击“创建新的默认配置文件”，输入默认集的名称，选择站点，然后更新 QoS 类别的带宽分配。单击保存。有关类的更多信息，请参阅 课程。

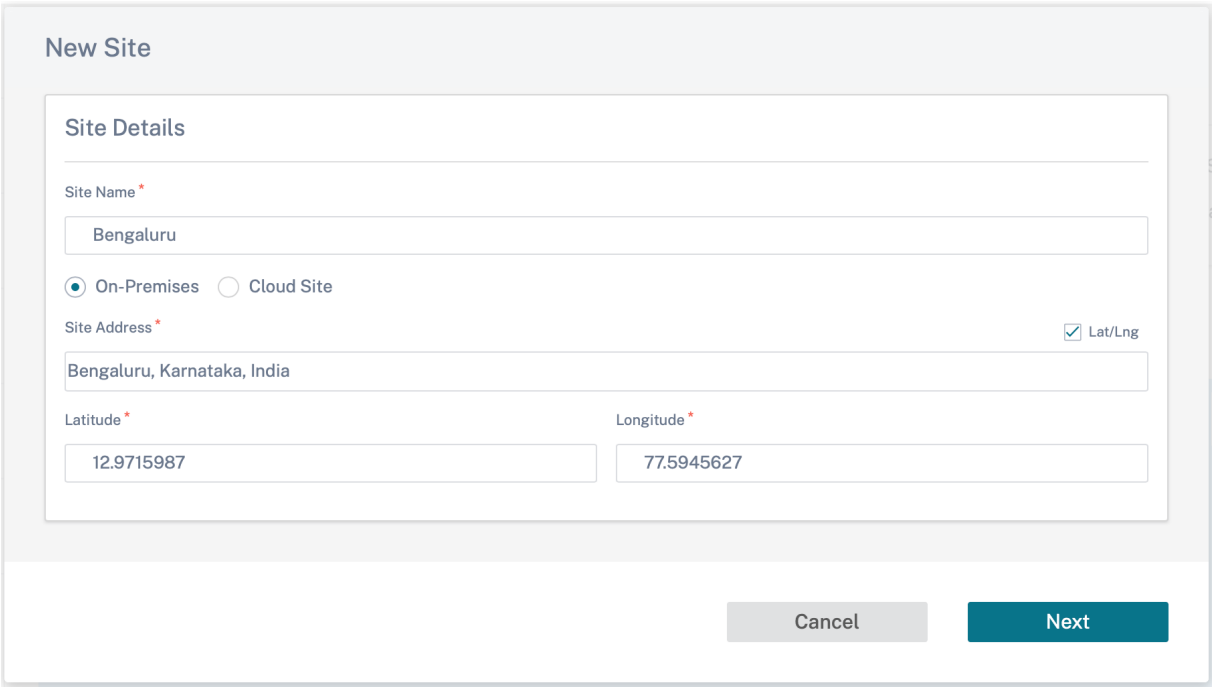


站点配置

October 21, 2022

您可以从 网络主 页或“配置 文件和模板”部分添加新站点来配置您的 SD-WAN 网络。

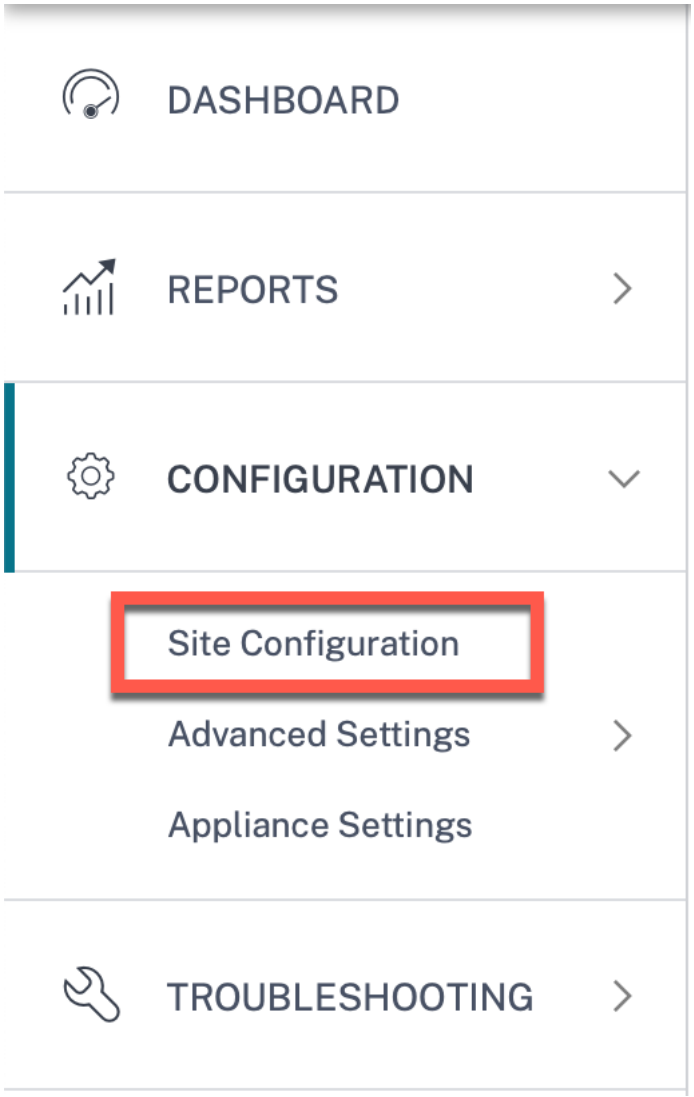
要创建站点，请单击“网络控制面板”上的“**+** 新建站点”。提供站点的名称和位置。



您可以从头开始创建站点，也可以使用 站点配置文件 快速配置站点。

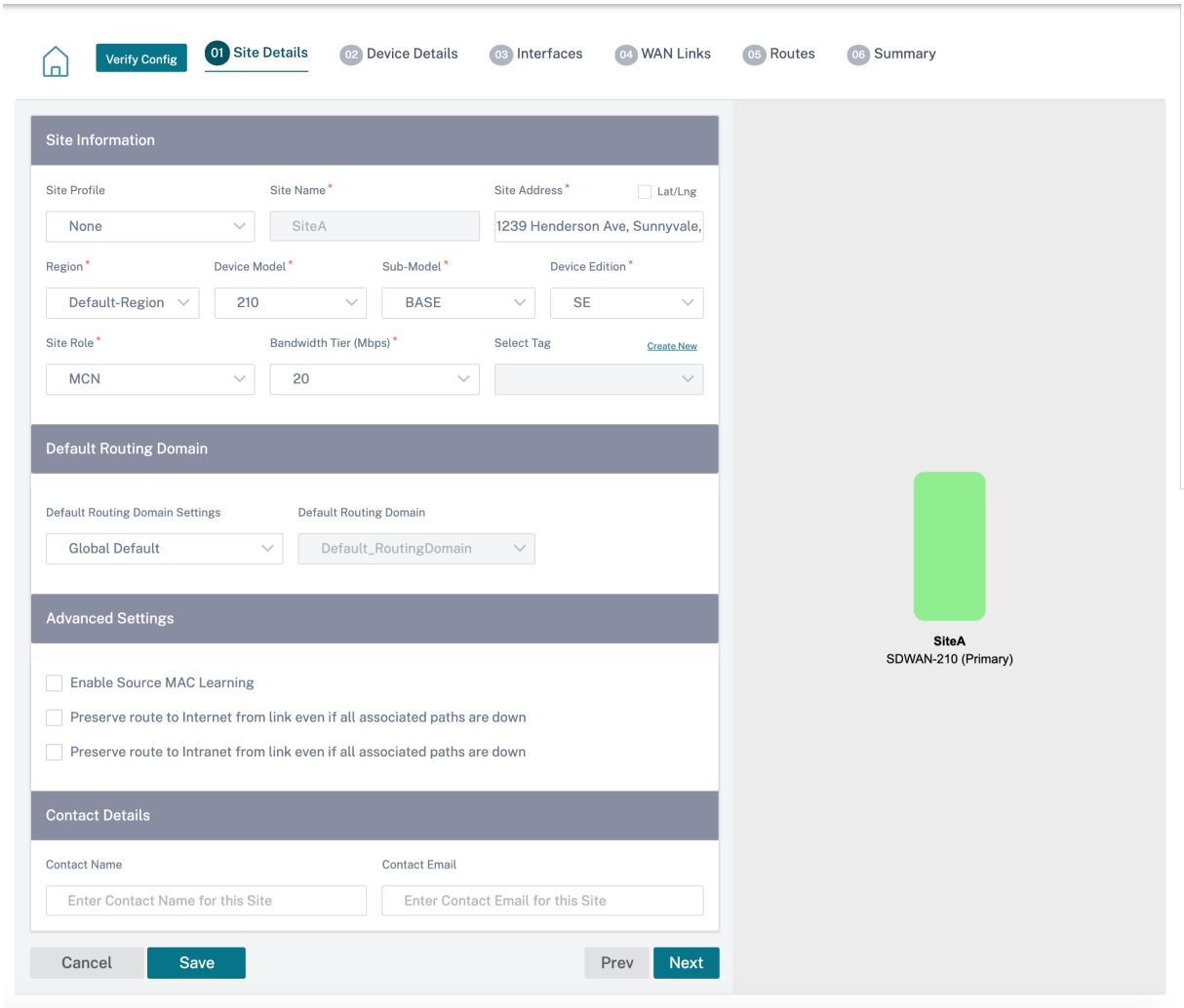
屏幕右侧的图形显示屏在您继续配置时提供动态拓扑图。

要查看站点配置，请选择站点并导航到 配置 **>** 站点配置。

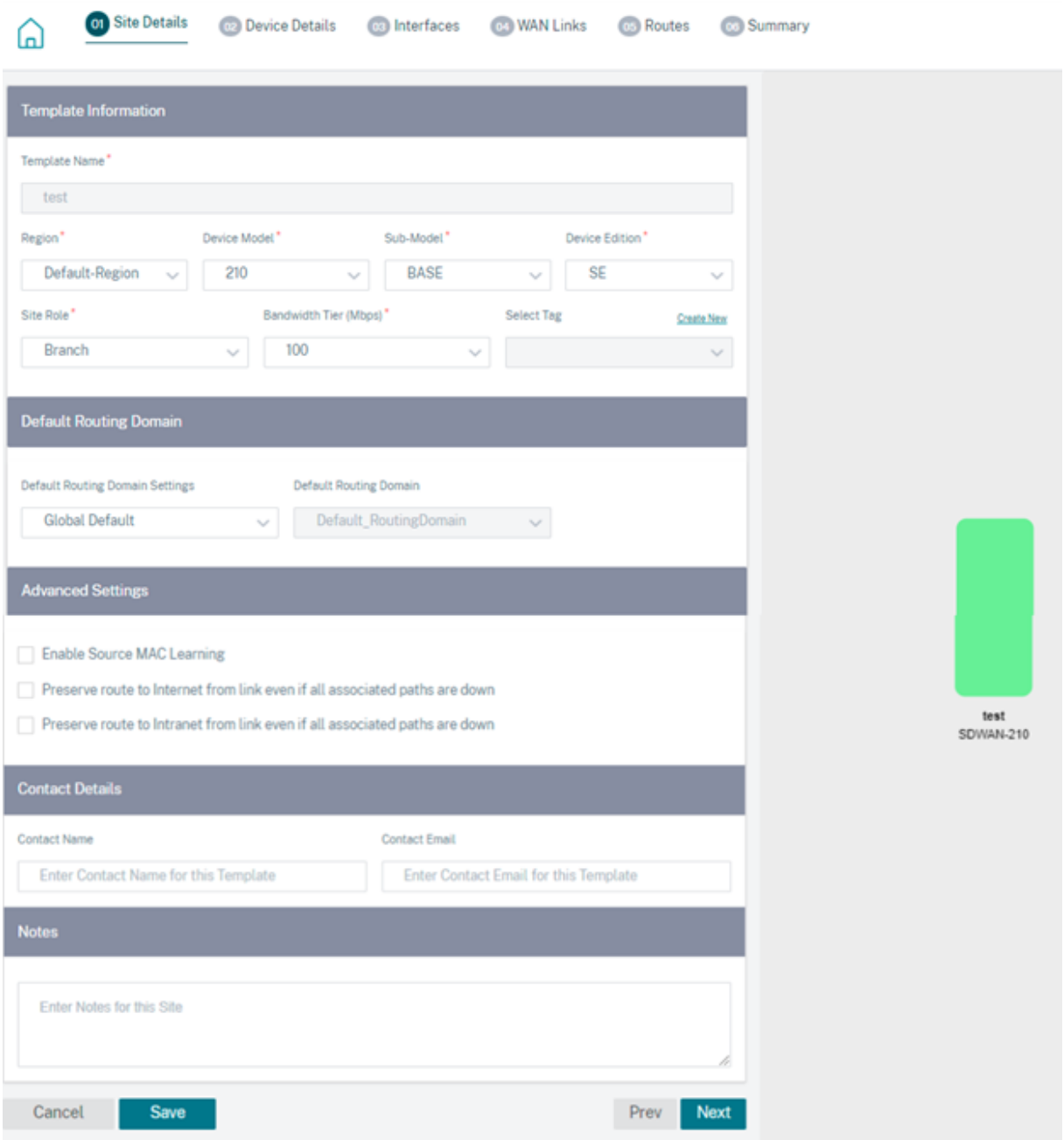


网站详情

第一步是输入站点、设备、高级设置和站点联系人详细信息。



使用站点模板配置站点时，将显示以下屏幕。



站点/模板信息

- 选择 站点配置文件 将根据站点配置文件配置自动填充站点、接口和 WAN 链接参数。
- 站点地址 和 站点名称 是根据上一步中提供的详细信息自动填充的。
- 启用 L **at/L** ng 复选框以获取站点的纬度和经度。
- 从下拉列表中选择 区域。
- 可以根据给定站点使用的硬件型号或虚拟设备来选择设备型号和子型号。

- 设备版本 会根据所选设备型号自动反映。目前支持高级版 (PE)、高级版 (AE) 和标准版 (SE)。PE 型号仅在 1100、2100、5100 和 6100 平台上受支持。AE 模型在 210 和 1100 平台上受支持。

  > 注意
  >
  > Citrix SD-WAN Orchestrator 服务不支持高级版和高级版平台。

- 站点角色 定义了设备的角色。您可以为站点分配以下角色之一：
  - **MCN**：主控制节点 (MCN) 充当网络的控制器，网络中只能将一台活动设备指定为 MCN。
  - 分支机构：分支站点上接收来自 MCN 的配置并参与为分支机构建立虚拟 WAN 功能的设备。可以有多个分支站点。
  - **RCN**：区域控制节点 (RCN) 支持分层网络架构，支持多区域网络部署。MCN 控制多个 RCN，而每个 RCN 依次控制多个分支站点。
  - 地理冗余 **MCN**：位于不同位置的站点，在 MCN 不可用时接管 MCN 的管理功能，确保灾难恢复。地理冗余 MCN 不为 MCN 提供高可用性或故障转移功能。
  - 地理冗余 **RCN**：位于不同位置的站点，在 RCN 不可用时接管 RCN 的管理功能，确保灾难恢复。地理冗余 RCN 不为 RCN 提供高可用性或故障转移功能。

- 带宽层 是您可以在任何设备上配置的计费带宽容量，具体取决于设备型号。例如，SD-WAN 410 标准版 (SE) 设备支持 20、50、100、150 和 200 Mbps 的带宽层。根据给定站点的带宽需求，您可以选择所需的等级。每个站点都按配置的带宽层计费。

路由域

路由域 部分允许您为站点选择默认路由域。路由域 设置可以是全局的，也可以是特定于站点的。如果选择“全局默认值”，则会自动选择全局适用的默认路由域。如果选择“特定站点”，则可以从“路由域”下拉列表中选择默认 路由域。

局域网分段路由支持

SD-WAN 标准版和企业版 (SE/PE) 设备在部署任一设备的不同站点上实现局域网分段。这些设备识别并保留可用局域网端 VLAN 的记录，并围绕其他局域网分段 (VLAN) 可以在远程位置与另一台 SD-WAN SE/PE 设备连接的规则进行配置。

上述功能是通过使用 SD-WAN SE/PE 设备中维护的虚拟路由和转发 (VRF) 表实现的，该表跟踪本地局域网段可访问的远程 IP 地址范围。此 VLAN 到 VLAN 的流量仍然会通过两个设备之间的相同预先建立的虚拟路径遍历 WAN（无需创建新路径）。

此功能的一个用例示例是，WAN 管理员可能能够通过 VLAN 对本地分支网络环境进行分段，并将其中一些分段 (VLAN) 提供给可以访问互联网的 DC 端 LAN 分段，而其他分段 (VLAN) 则可能无法获得此类访问权限。VLAN 到 VLAN 关联的配置是通过 Citrix SD-WAN Orchestrator 服务 Web 界面实现的。

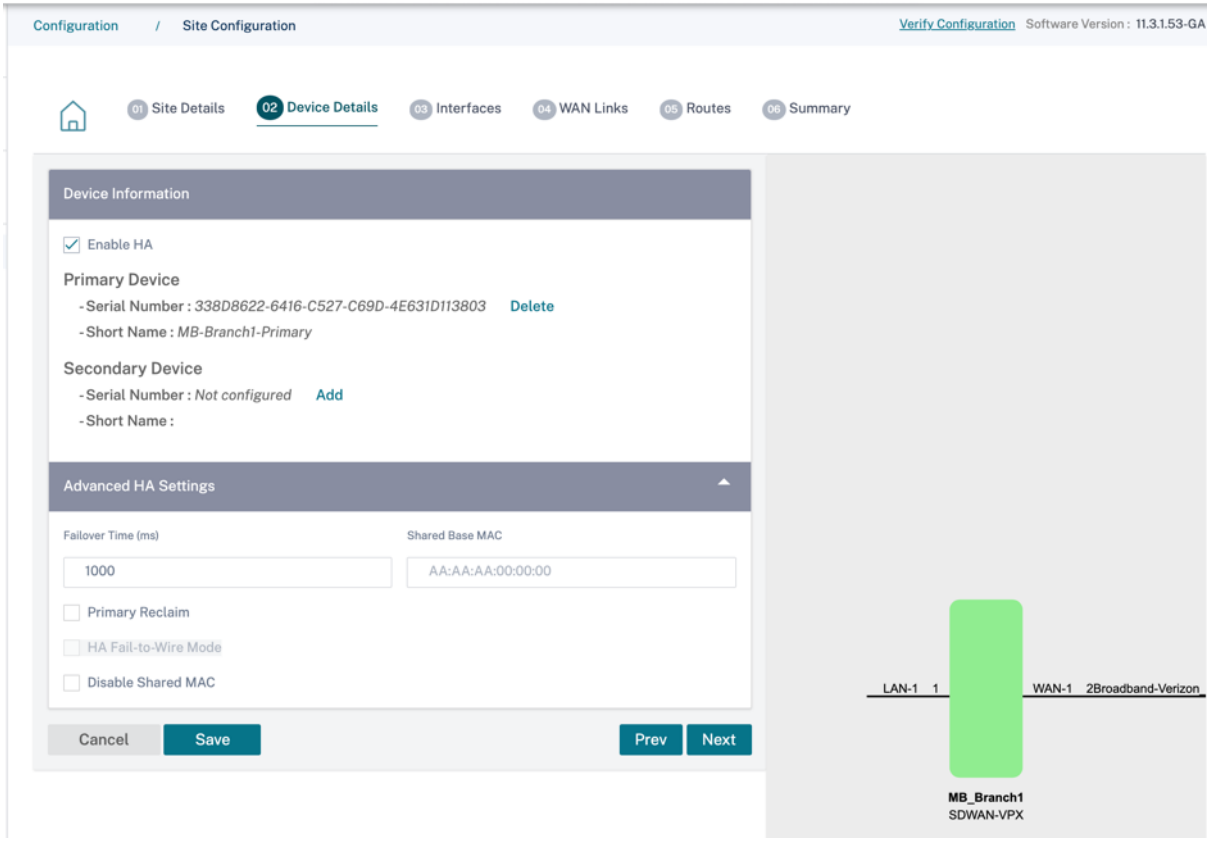
高级设置

- 启用源 **MAC** 学习：存储收到的数据包的源 MAC 地址，以便发往相同目的地的传出数据包可以发送到同一个端口。
- 即使所有关联路径均处于关闭状态，仍保留从链接到互联网的路由：启用后，即使互联网服务的所有 WAN 链接都不可用，发往互联网服务的数据包仍会继续选择互联网服务。
- 即使所有关联路径均处于关闭状态，仍保留从链接到内联网的路由：启用后，即使内联网服务的所有 WAN 链接都不可用，发往 Intranet 服务的数据包仍会继续选择内网服务。
- 管理员的联系方式可在网站上找到。

配置面板右侧的动态网络图可在您完成配置过程中持续提供可视化反馈。

设备详细信息

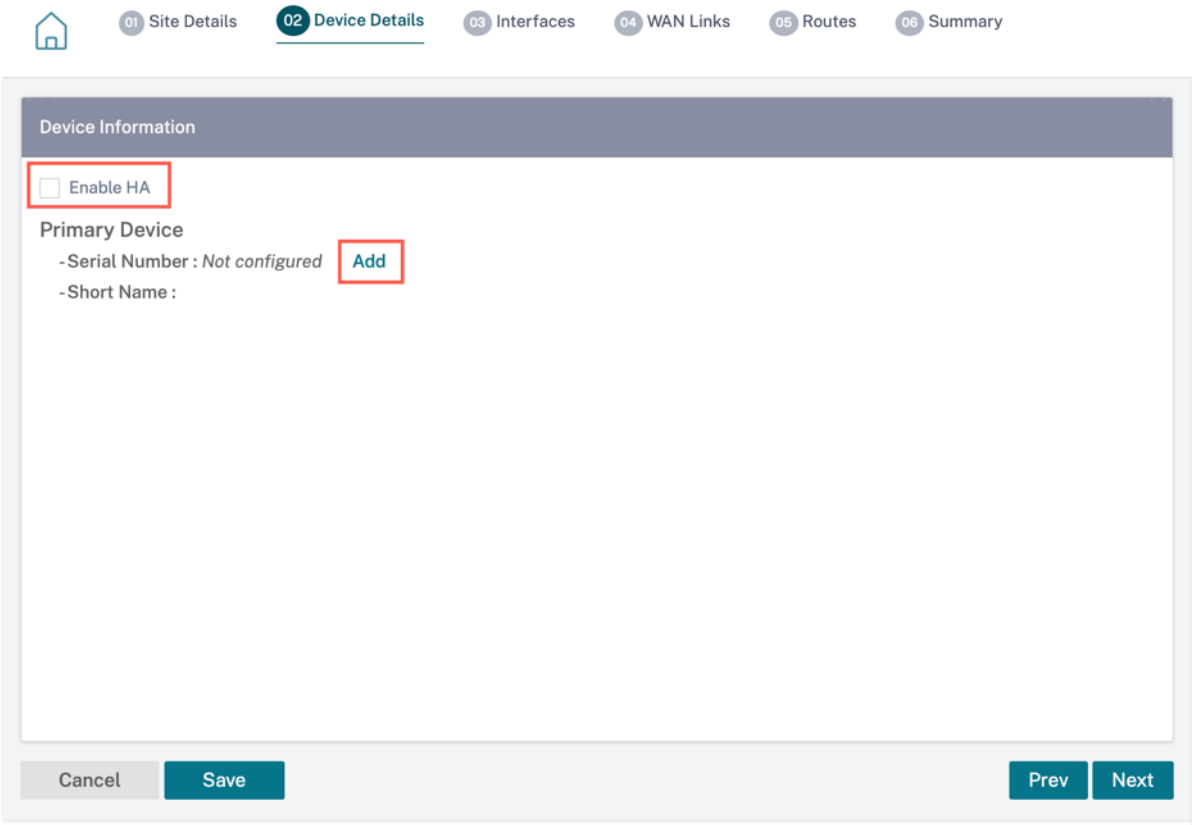
设备详细信息部分允许您在站点配置和启用高可用性 (HA)。使用 HA，可以将两个设备作为主动主设备和被动辅助设备部署在站点上。主设备出现故障时，辅助设备将接管。有关更多信息，请参阅 高可用性。



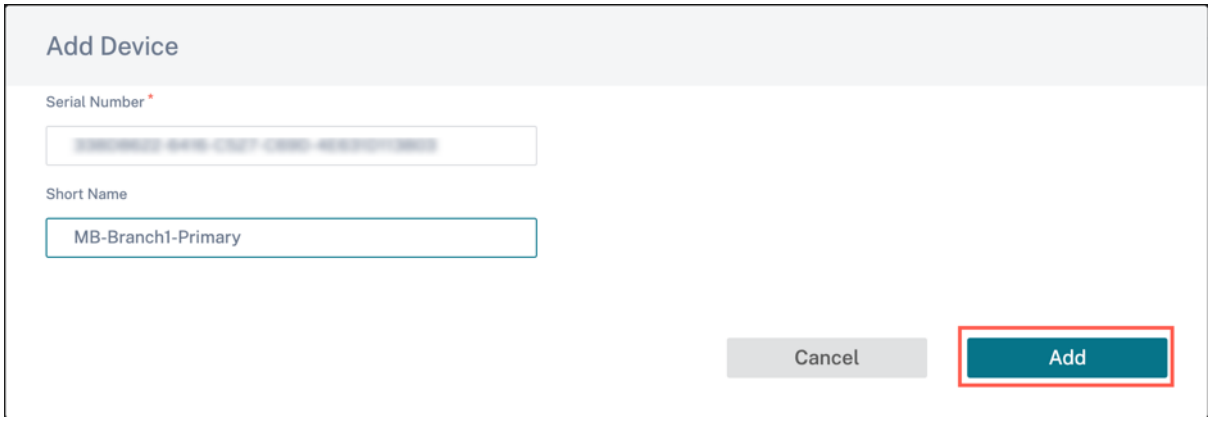
> 注意
>
> 无法使用站点模板配置序列号。

设备信息

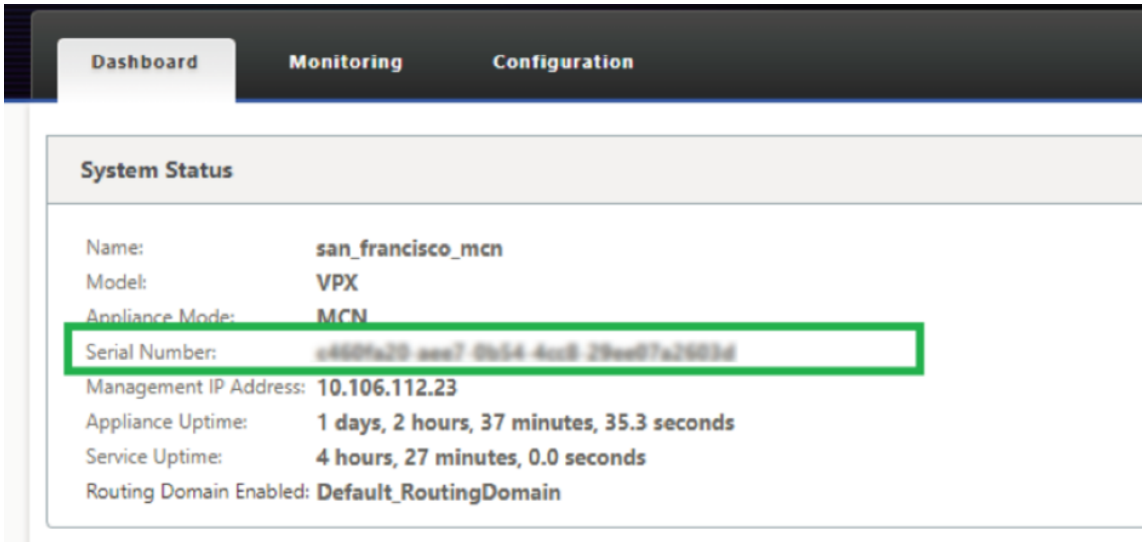
启用 HA，然后输入主设备和辅助设备的序列号和短名称。单击“添加”并提供序列号和站点简称。



单击添加。



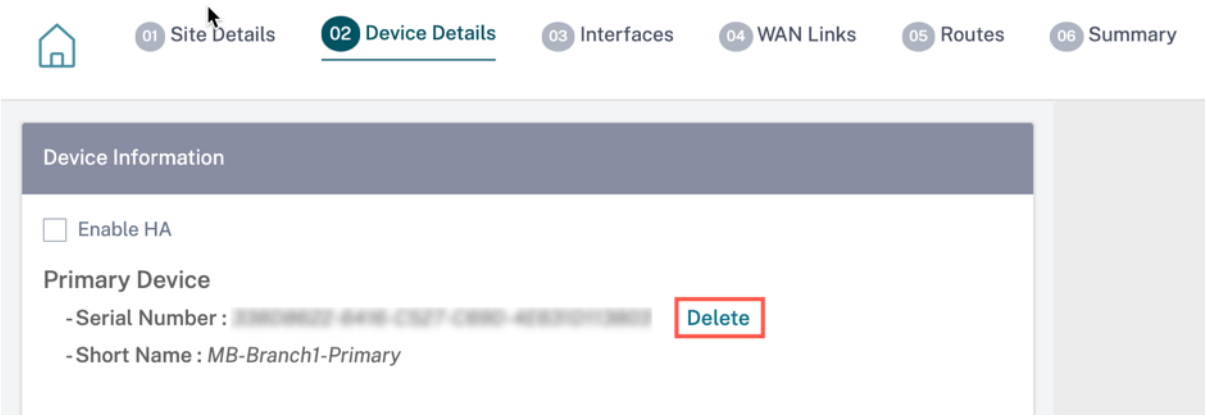
- 序列号：可以从 VPX Web 控制台访问虚拟 SD-WAN 实例 (VPX) 的 序列号，如以下屏幕截图所示。硬件设备的序列号也可以在设备标签上找到。



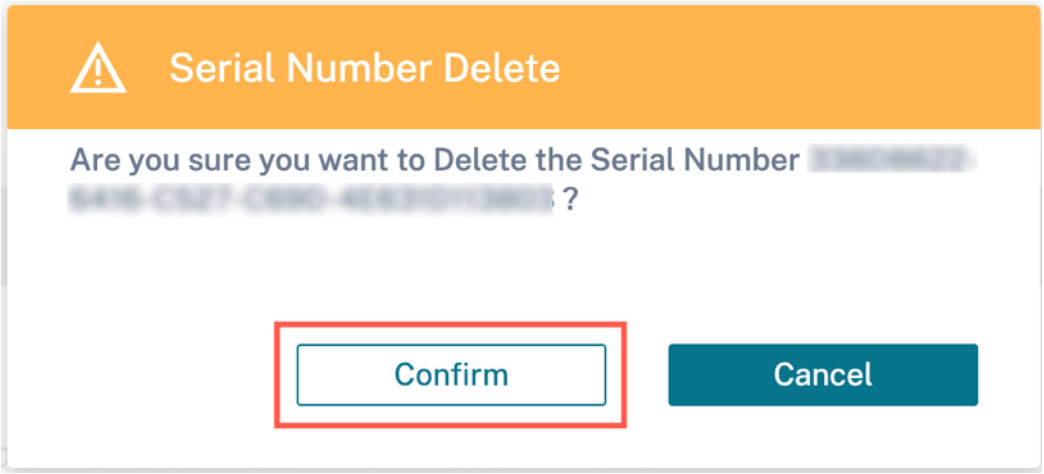
- 短名称：短名称 字段用于为站点指定易于识别的短名称或根据需要标记站点。

如果要 删除 序列号，请单击“删除”选项。

> 注意
>
> 更新序列号需要删除现有序列号并读取新的序列号。



单击“删除”选项后，会出现一个弹出窗口，确认您是否要删除序列号。



高级 **HA** 设置

- 故障转移时间 **(ms)**：丢失与主设备联系后、备用设备处于活动状态之前的等待时间。
- 共享基本 **MAC**：高可用性对设备的共享 MAC 地址。发生故障转移时，辅助设备具有与发生故障的主设备相同的虚拟 MAC 地址。
- 禁用 **Shared Base MAC**：此选项仅在虚拟机管理程序和基于云的平台上可用。选择此选项可禁用共享虚拟 MAC 地址。
- 主回收：指定的主设备在故障转移事件发生后重新启动时恢复控制权。
- **HA** 故障到线模式：HA 故障到线模式已启用。有关更多详细信息，请参阅 HA 部署模式。
- 启用 **Y** 型电缆支持：小型封装可插拔 (SFP) 端口可与光纤 Y 型电缆一起使用，以实现边缘模式部署的高可用性功能。此选项仅适用于 Citrix SD-WAN 1100 SE/PE 设备。有关详细信息，请参阅 使用光纤 Y 型电缆启用边缘模式高可用性。

无线网络详情

您可以配置支持 Wi-Fi 作为 Wi-Fi 接入点的 Citrix SD-WAN 设备。

Citrix SD-WAN 110 平台的以下两个变体支持 Wi-Fi，可以配置为 Wi-Fi 接入点：

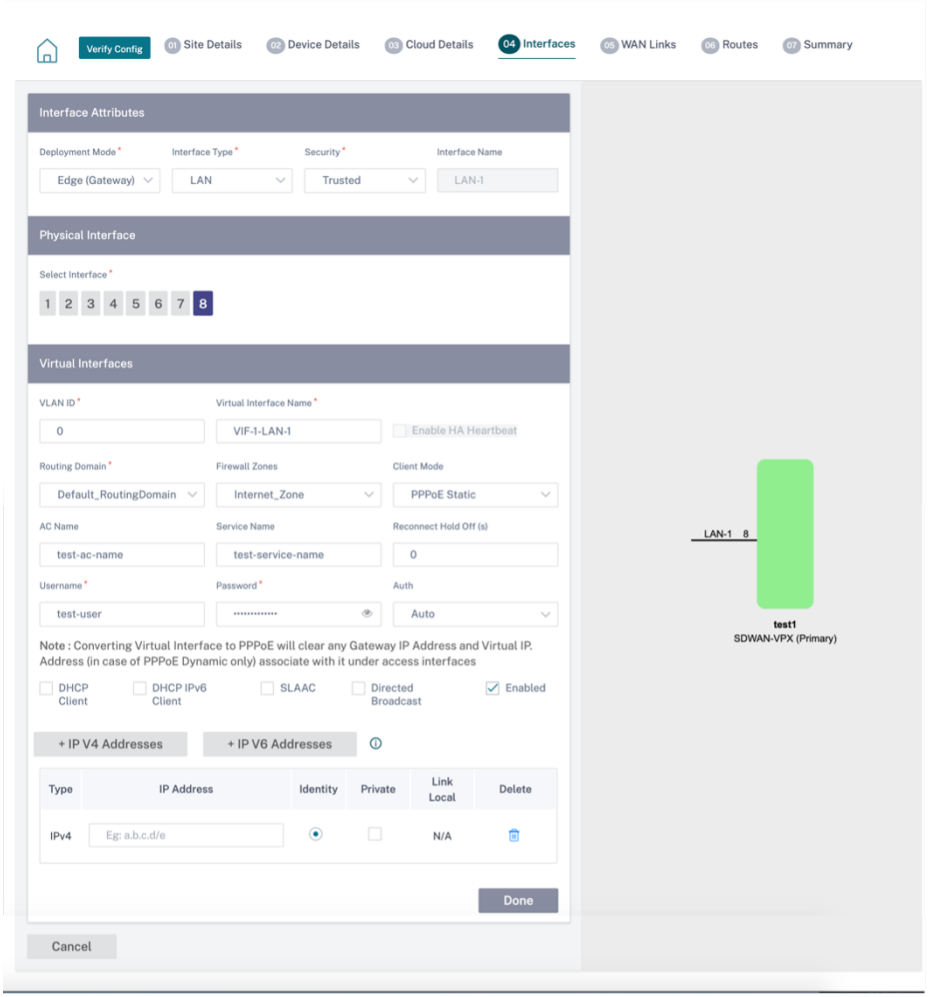
- Citrix SD-WAN 110-wifi-SE
- Citrix SD-WAN 110-lte-WiFi

有关 Wi-Fi 配置的更多详细信息，请参阅 Wi-Fi 接入点

接口

下一步是添加和配置接口。单击 **+** 接口 开始配置接口。单击 **+ HA** 接口 开始配置 HA 接口。只有在配置了辅助设备以实现高可用性时，**+ HA** 接口 选项才可用。

接口配置包括选择部署模式和设置接口级别的属性。此配置适用于 LAN 和 WAN 链路。



带内管理

带内管理允许您使用 SD-WAN 数据端口进行管理。它同时承载数据流量和管理流量，而无需配置额外的管理路径。带内管理允许虚拟 IP 地址连接到管理服务，如 Web UI 和 SSH。您可以使用管理 IP 和带内虚拟 IP 访问 Web UI 和 SSH。

要启用带内管理，请从“带 内管理 **IP**”下拉列表中选择 **IPv4** 地址，或从“带内管理 **IPv6**”下拉列表中选择 **IPv6** 地址。从“带内管理 **DNS**”或“带内管理 **DNS V6**”下拉列表中选择 **DNS** 代理，通过带内和备用管理平面将所有 **DNS** 请求转发到该代理。

有关带内管理的更多信息，请参阅 带内管理。

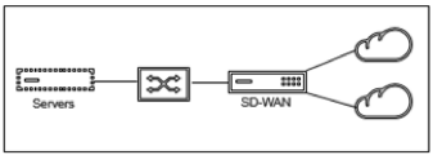
为接口配置的 IP 地址列在 带内管理 **IP** 下拉列表下。在 “高级设置” **>** “**DNS**”下配置的 **DNS** 代理服务将列在“带内管理 **DNS** ”下拉列表中。

接口属性

支持以下部署模式：

1. 边缘（网关）
2. 内联—故障到线、故障到块和虚拟内联。

- 部署模式：选择以下部署模式之一。
  - 边缘（网关）：



网关模式意味着 SD-WAN 充当所有 LAN 流量的 WAN 的“网关”。网关模式 是默认模式。您可以将设备部署为局域网端或广域网端的网关。

  - 内联：

当 SD-WAN 在 LAN 交换机和广域网路由器之间串联部署时，SD-WAN 应该“桥接”局域网和广域网。

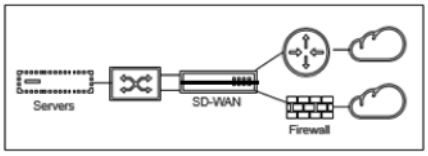
所有 Citrix SD-WAN 设备都有预定义的桥接配对接口。启用 Bridge 选项后，选择 LAN 端的任何接口都会自动突出显示为网桥 WAN 端保留的配对接口。例如，物理接口 1 和 2 是桥接对。

    * **Fail-to-Wire**：启用桥接对接口之间的物理连接，允许流量绕过 SD-WAN，在设备重启或出现故障时直接流经网桥。

此前，DHCP 客户端仅在故障到块端口上受支持。在 Citrix SD-WAN 11.2.0 版本中，通过串行高可用性 (HA) 部署扩展了分支站点的故障连线端口上的 DHCP 客户端功能。此增强功能：

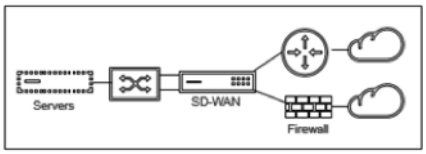
    * 允许在具有故障到线网桥对和串行 HA 部署的不受信任接口组上进行 DHCP 客户端配置。
    * 允许选择 DHCP 接口作为 专用内联网 WAN 链接的一部分。

> 备注
>
> * 内联（故障到线）选项仅在硬件设备上可用，在虚拟设备 (VPX/VPXL) 上不可用。
> * 专用内部网链接现在支持 DHCP 客户端。
> * LAN 接口不得连接到故障到线路对，因为数据包可能在接口之间桥接。

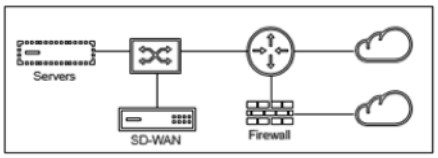


    * **Fail-to-Block**：此选项禁用硬件设备上桥接对接口之间的物理连接，从而在设备重启或出现故障时防止流量流过网桥。

> 注意
>
> 内联（故障阻止）是虚拟设备（VPX/VPXL）上唯一可用的桥接模式选项。



* 虚拟内联（单臂）：



在此模式下部署 SD-WAN 时，它会使用 单臂 将其连接到 WAN 路由器、LAN 和 WAN，在 SD-WAN 上共享相同接口。因此，接口设置在 LAN 和 WAN 链路之间共享。

- 接口类型：从下拉列表中选择接口类型。
- 安全（可信/不可信）：指定接口的安全级别。受信任的区段受防火墙的保护。
- 接口名称：根据所选的部署模式，自动填充“接口名称”字段。

物理接口

- 选择接口：选择设备上可用的可配置以太网端口。

虚拟接口

- **VLAN ID**：用于识别和标记进出接口的流量的 ID。
- 虚拟接口名称：根据所选的部署模式，自动填充“虚拟接口名称”字段。
- 启用 **HA** 心跳信号：启用通过此接口同步 HA 心跳信号。如果您已为 HA 配置了辅助设备，则启用此选项。选择此选项可允许主设备和辅助设备通过此接口同步 HA 检测信号。指定主要和辅助设备的 IP 地址。
- 路由域：为分支机构网络或数据中心网络提供单点管理的路由域。
- 防火墙区域：接口所属的防火墙区域。防火墙区域保护和控制逻辑区域中的接口。
- 客户端模式：从下拉列表中选择 客户端模式。选择 PPPoE 静态时会显示更多设置。

> 注意
>
> 当“站点”模式（在“站点详细信息”选项卡下）被选为“分支”且“安全”字段（在“接口”选项卡下）被

> 选为“不可信”时，**PPPoE** 动态 选项在“客户端模式”下可用。

Citrix SD-WAN 充当 PPPoE 客户端。对于 IPv4，SD-WAN 获取动态 IPv4 地址或使用静态 IPv4 地址。对于 IPv6，它从 PPPoE 服务器获取链路本地地址。对于 IPv6 单播地址，可以使用静态 IP、DHCP 或 SLAAC。

- **DHCP** 客户端：在虚拟接口上启用后，DHCP 服务器将动态分配 IPv4 地址给连接的客户端。
- **DHCP IPv6** 客户端：在虚拟接口上启用后，DHCP 服务器将动态分配 IPv6 地址给连接的客户端。
- **SLAAC**：此选项仅适用于 IPv6 地址。选中后，接口将通过无状态地址自动配置 (SLAAC) 获取 IPv6 地址。
- 定向广播：选中“定 向广播”复选框后，定向广播将发送到虚拟接口上的虚拟 IP 子网。
- 启用：默认情况下，所有虚拟接口的“启用”复选框均处于选中状态。如果要禁用虚拟接口，请清除“启用”复选框。

  > 注意
  >
  > - “启用”复选框仅在 Citrix SD-WAN 版本 11.3.1 之后可用。
  > - 仅当 WAN 链接访问接口未使用虚拟接口时，禁用虚拟接口的选项才可用。如果 WAN 链接访问接口使用虚拟接口，则该复选框为只读且默认处于选中状态。
  > - 在配置其他功能以及已启用的虚拟接口时，禁用的虚拟接口也会列出，但 **WAN** 链接的访问接口下除外。即使选择禁用的虚拟接口，也不考虑虚拟接口，也不会影响网络配置。

- **+ IPv4** 地址：接口的虚拟 IPv4 地址和网络掩码。
- **+ IPv6** 地址：接口的虚拟 IPv6 地址和前缀。
- 身份：选择用于 IP 服务的身份。例如，身份 被用作与 BGP 邻居通信的源 IP 地址。
- 私有：启用后，虚拟 IP 地址只能在本地设备上路由。

> 注意
>
> - LTE 端口不支持静态 IP 地址（IPv4 和 IPv6）。
> - LTE 端口支持 DHCP 和 SLAAC。配置 DHCPv4 或 DHCPv6 是强制性的。SLAAC 是可选的。
> - 在 LTE 端口中，可以为 IPv6 或 SLAAC 配置链路本地地址。

PPPoE 凭证

以太网点对点协议 (PPPoE) 通过常用客户场所设备（例如 Citrix SD-WAN）将以太网 LAN 上的多个计算机用户连接到远程站点。PPPoE 允许用户共享通用的数字用户线 (DSL)、电缆调制解调器或无线连接到 Internet 。PPPoE 将通常用于拨号连接的点对点协议 (PPP) 与支持局域网中多个用户的以太网协议相结合。PPP 协议信息封装在以太网框架内。

与拨号连接不同，Citrix SD-WAN 设备使用 PPPoE 支持 ISP 实现持续持续的 DSL 和有线调制解调器连接。PPPoE 提供每个用户远程站点会话，通过称为 发现 的初始交换来学习彼此的网络地址。在单个用户和远程站点（例如 ISP 提供程序）之间建立会话后，可以监视该会话。公司使用以太网和 PPPoE 通过 DSL 线路使用共享 Internet 接入。

Citrix SD-WAN 充当 PPPoE 客户端。对于 IPv4，SD-WAN 获取动态 IPv4 地址或使用静态 IPv4 地址。对于 IPv6，它从 PPPoE 服务器获取链路本地地址。对于 IPv6 单播地址，可以使用静态 IP、DHCP 或 SLAAC。

要建立成功的 PPPoE 会话，需要以下内容：

- 配置虚拟网络接口 (VNI)。
- 用于创建 PPPoE 会话的唯一凭据。
- 配置 WAN 链接。每个 VNI 只能配置一个 WAN 链接。
- 配置虚拟 IP 地址。每个会话都会根据提供的配置获得一个唯一的 IP 地址（动态或静态）。
- 在桥接模式下部署设备以使用具有静态 IP 地址的 PPPoE，并将接口配置为“可信”。“
- 静态 IP 最好使用配置来强制使用服务器建议的 IP；如果与配置的静态 IP 不同，则可能会出现错误。
- 将设备部署为 Edge 设备以使用具有动态 IP 的 PPPoE 并将接口配置为“不可信”。“
- 支持的身份验证协议有：PAP、CHAP、EA-MD5、EAP-SRP。
- 多个会话的最大数量取决于配置的 VNI 数量。
- 创建多个 VNI 以支持每个接口组的多个 PPPoE 会话。

> 注意
>
> 允许使用相同的 802.1Q VLAN 标记创建多个 VNI。

PPPoE 配置的限制：

- 不支持 802.1q VLAN 标记。
- 不支持 EAP-TLS 身份验证。
- 地址/控制压缩。
- 放气压缩。
- 协议字段压缩协商。
- 压缩控制协议。
- BSD 压缩压缩。
- IPX 协议。
- 购买力平价多链接。
- 范雅各布森风格 TCP/IP 头压缩.
- Van Jacobson 风格的 Connection-ID 压缩选项 TCP/IP 标头压缩。
- LTE 接口不支持 PPPoE。

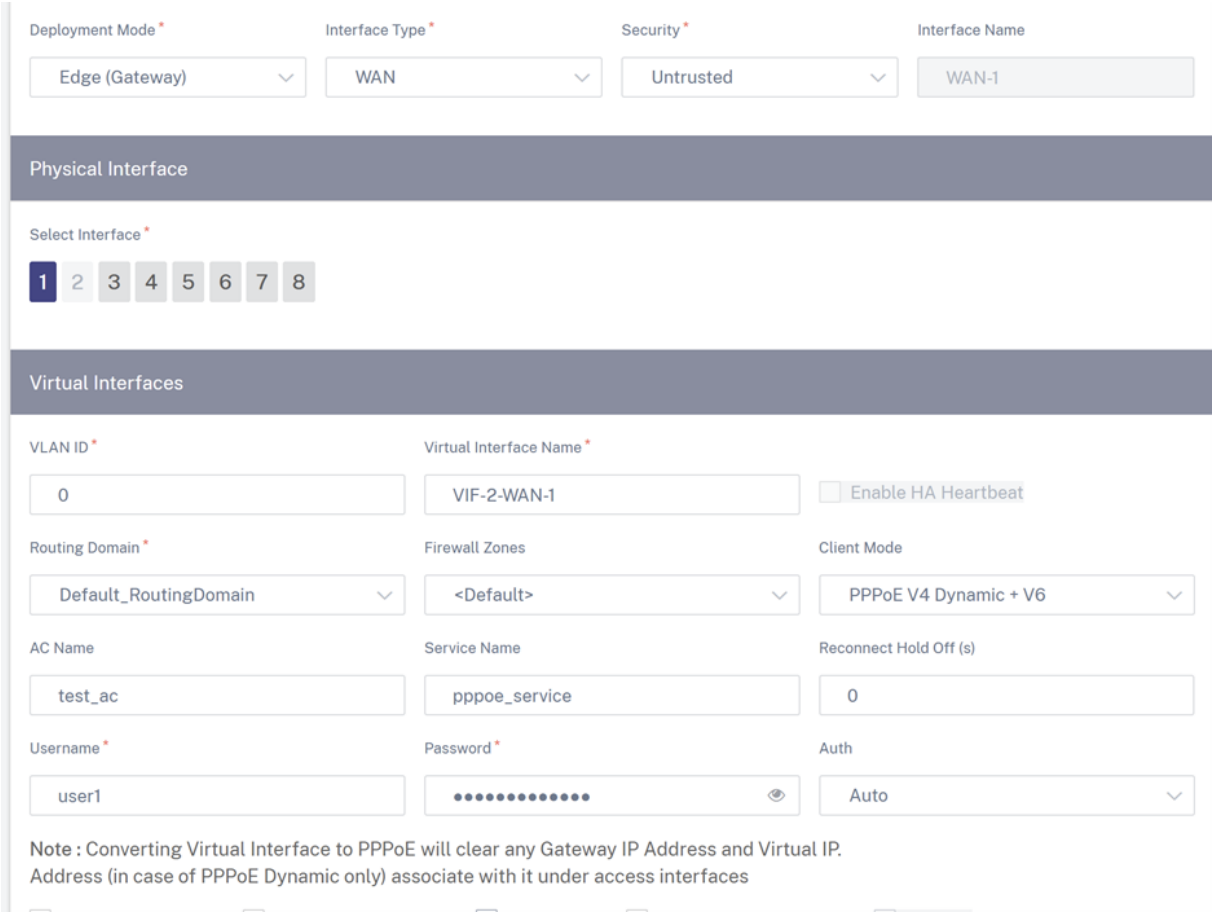
从 Citrix SD-WAN 11.3.1 版本中，需要考虑额外的 8 字节 PPPoE 标头来调整 TCP 最大分段大小 (MSS)。额外的 8 个字节 PPPoE 报头根据 MTU 调整同步数据包中的 MSS。支持的 MTU 范围从 1280 字节到 1492 字节不等。

PPPoE 配置　在 MCN 上，您只能配置 PPPoE 静态。在分支机构上，您可以配置 PPPoE 静态或 PPPoE 动态。

要配置 PPPoE，请在站点级别配置中导航到 配置 **>** 站点配置 **>** 接口 选项卡。在“虚拟接口”部分中，从“客户端模式”下拉列表中选择相应的 PPPoE 选项。

注意

- 配置了多个接口的 VNI 只能有一个接口用于 PPPoE 连接。
- 如果配置了多个接口和 PPPoE 连接的 VNI 更改为其他接口，则可以使用 报告 **>** 实时 **> PPPoE** 页面来停止现有会话并启动新会话。然后可以在新接口上建立新会话。
- 如果选择 PPPoE 动态，则 VNI 必须为“不受信任”。



- **AC** 名称：提供 PPPoE 配置的接入集中器 (AC) 名称。
- 服务名称：输入服务名称。
- 重新连接暂停：输入重新连接尝试暂停时间。
- 用户名：输入 PPPoE 配置的用户名。
- 密码：输入 PPPoE 配置的密码。
- 身份验证：从下拉列表中选择授权协议。
  - 当 **Auth** 选项设置为“自动”时，SD-WAN 设备将接受从服务器收到的支持的身份验证协议请求。
  - 当“身份 验证”选项设置为 PAP/CHAP/EAP 时，则仅支持特定的身份验证协议。如果 PAP 在配置中，并且服务器使用 CHAP 发送身份验证请求，则连接请求将被拒绝。如果服务器不与 PAP 协商，则会发生身份验证失败。

每个 PPPoE 静态或动态 VNI 只允许创建一个 WAN 链接。WAN 链接配置因客户端模式的 VNI 选择而异。

如果 VNI 配置为 PPPoE 动态客户端模式：

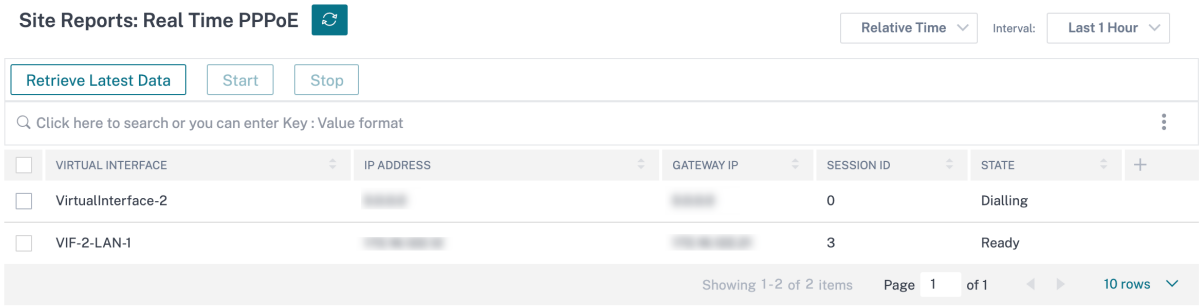
- IP 地址和网关 IP 地址字段变为非活动状态。
- 虚拟路径模式设置为“主”。
- 无法配置代理 ARP。

默认情况下，选择网关 MAC 地址绑定。

如果 VNI 配置为 PPPoE 静态客户端模式，则配置 IP 地址。

> 注意
>
> 如果服务器不支持配置的静态 IP 地址并提供不同的 IP 地址，则会出现错误。PPPoE 会话尝试定期重新建立连接，直到服务器接受配置的 IP 地址。

PPPoE 监控和故障排除　在站点级别，导航“报告”**>**“实时”**>**“**PPPoE**”部分，查看有关使用 PPPoE 静态或动态客户端模式配置的 VNI 的信息。它允许您手动启动或停止会话以进行故障排除。



在建立 PPPoE 会话时出现问题时：

- 将鼠标悬停在失败状态上可显示最近失败的原因。
- 要建立新的会话或对活动的 PPPoE 会话进行故障排除，请重新启动该会话。
- 如果手动停止 PPPoE 会话，则在手动启动并激活配置更改或重新启动服务之前，该会话无法启动。

PPPoE 会话可能会因以下原因而失败：

- 当 SD-WAN 由于配置中的用户名/密码不正确而无法向对等体进行身份验证时。
- PPP 协商失败-协商没有达到至少一个网络协议正在运行的地步。
- 系统内存或系统资源问题。
- 配置无效/错误（错误的 AC 名称或服务名称）。
- 由于操作系统错误，无法打开串行端口。
- echo 数据包没有收到任何响应（链路不好或服务器没有响应）。
- 有几个连续不成功的拨号会话在一分钟内。

在连续 10 次失败后，观察到失败的原因。

- 如果故障正常，它将立即重新启动。
- 如果失败是错误，则重新启动将恢复 10 秒。
- 如果失败是致命的，则重新启动将恢复 30 秒，然后重新启动。

LCP Echo 请求数据包每 60 秒从 SD-WAN 生成一次，未能接收 5 个回显响应被视为链路失败，并重新建立会话。

- 如果 VNI 已启动并准备就绪，IP 和网关 IP 列将显示会话中的当前值。它表示这些是最近接收的值。
- 如果 VNI 已停止或处于故障状态，则这些值是最后收到的值。
- 将鼠标悬停在 Gateway IP 列上会显示 PPPoE 接入集中器的 MAC 地址，从中接收会话和 IP。
- 将鼠标悬停在“状态”值上方会显示一条消息，这对“失败”状态更有用。

PPPoE 会话类型	状态颜色	说明
已配置	黄色	VNI 配置了 PPPoE。这是一个初始状态。
正在拨号	黄色	配置 VNI 后，PPPoE 会话状态通过启动 PPPoE 发现移动到拨号状态。数据包信息被捕获。
会话	黄色	VNI 从发现状态移至会话状态，等待接收 IP（如果是动态的），或者等待服务器确认通告的 IP（静态）。
已就绪	绿色	接收 IP 数据包后，VNI 和关联的 WAN 链路已准备就绪，可供使用。
失败	红色	PPP/PPPoE 会话终止。失败的原因可能是配置无效或致命错误。会话将在 30 秒后尝试重新连接。
已停止	黄色	PPP/PPPoE 会话手动停止。
终止	黄色	由于某种原因而终止的中间状态。此状态在一定持续时间后自动启动（正常错误为 5 秒，致命错误为 30 秒）。
已禁用	黄色	SD-WAN 服务处于禁用状态。

SDWAN_ip_learned.log 文件包含与 PPPoE 相关的日志。导航到故障排除 **>** 设备日志以查看或下载 *SDWAN_ip_learned.log* 文件。

有线 **802.1X** 配置

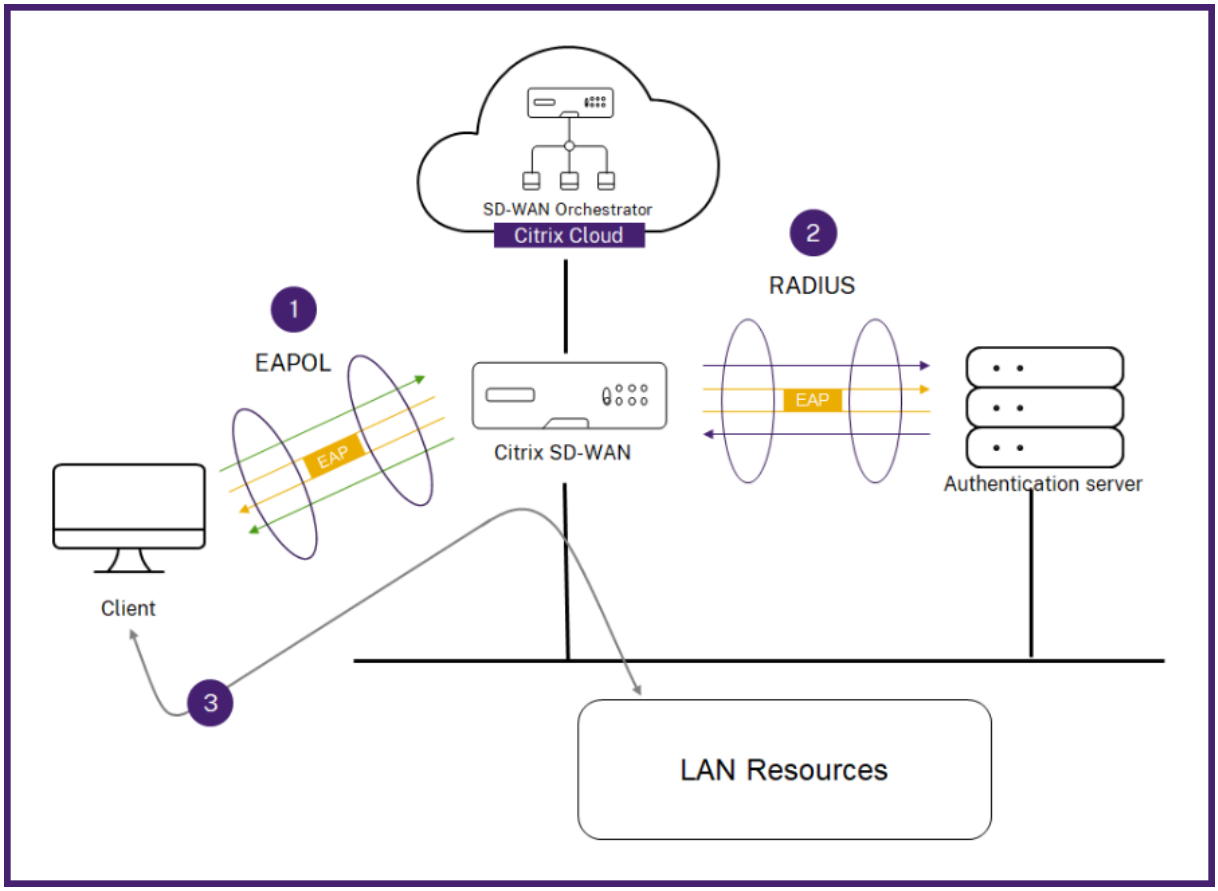
Wired 802.1X 是一种身份验证机制，它要求客户端先进行身份验证，然后才能访问 LAN 资源。Citrix SD-WAN Orchestrator 服务支持在局域网接口上配置有线 802.1X 身份验证。

在 Citrix SD-WAN 网络中，客户端向 Citrix SD-WAN 设备发送身份验证请求以访问 LAN 资源。Citrix SD-WAN 设备充当身份验证器并将身份验证请求发送到身份验证服务器。Citrix SD-WAN Orchestrator 服务仅支持将 RADIUS 服务器配置为身份验证服务器。

首次进行身份验证时，只能处理 EAPOL 数据包或可以从默认虚拟 LAN 初始化 802.1X 身份验证的 DHCP 数据包。新连接的客户端必须在 90 秒内进行身份验证。如果身份验证成功，它就可以访问局域网资源。

如果身份验证失败，则不向客户端授予网络访问权限，所有数据包都将被丢弃。直接连接到 Citrix SD-WAN 设备的客户端可以通过拔下以太网电缆并将其重新插入来重试身份验证。或者，您可以定义特定的虚拟 LAN，为失败的身份验证请求授予对有限局域网资源的访问权限。在这种情况下，失败的身份验证请求可以访问指定的虚拟 LAN。在创建虚拟局域网时，您可以使用不同的路由域或防火墙区域限制对经过身份验证的流量的访问。

> 注意
>
> - 默认虚拟 LAN 必须始终启用 802.1X。
> - 不支持动态虚拟 LAN。



Citrix SD-WAN 设备期望接收没有 802.1Q 标签的数据包（未标记的数据包）。如果 Citrix SD-WAN 设备收到的数据包，其中 802.1Q 标签设置为分配的虚拟局域网，则必须标记所有来自 MAC 的数据包。如果收到的数据包报头中没有 802.1Q 标记，或者其标签不是 MAC 地址所属的虚拟 LAN，则该数据包将被丢弃。

当连接到交换机的多台客户机尝试通过单个端口同时进行身份验证时，每台客户端都要经过单独身份验证，然后才能访

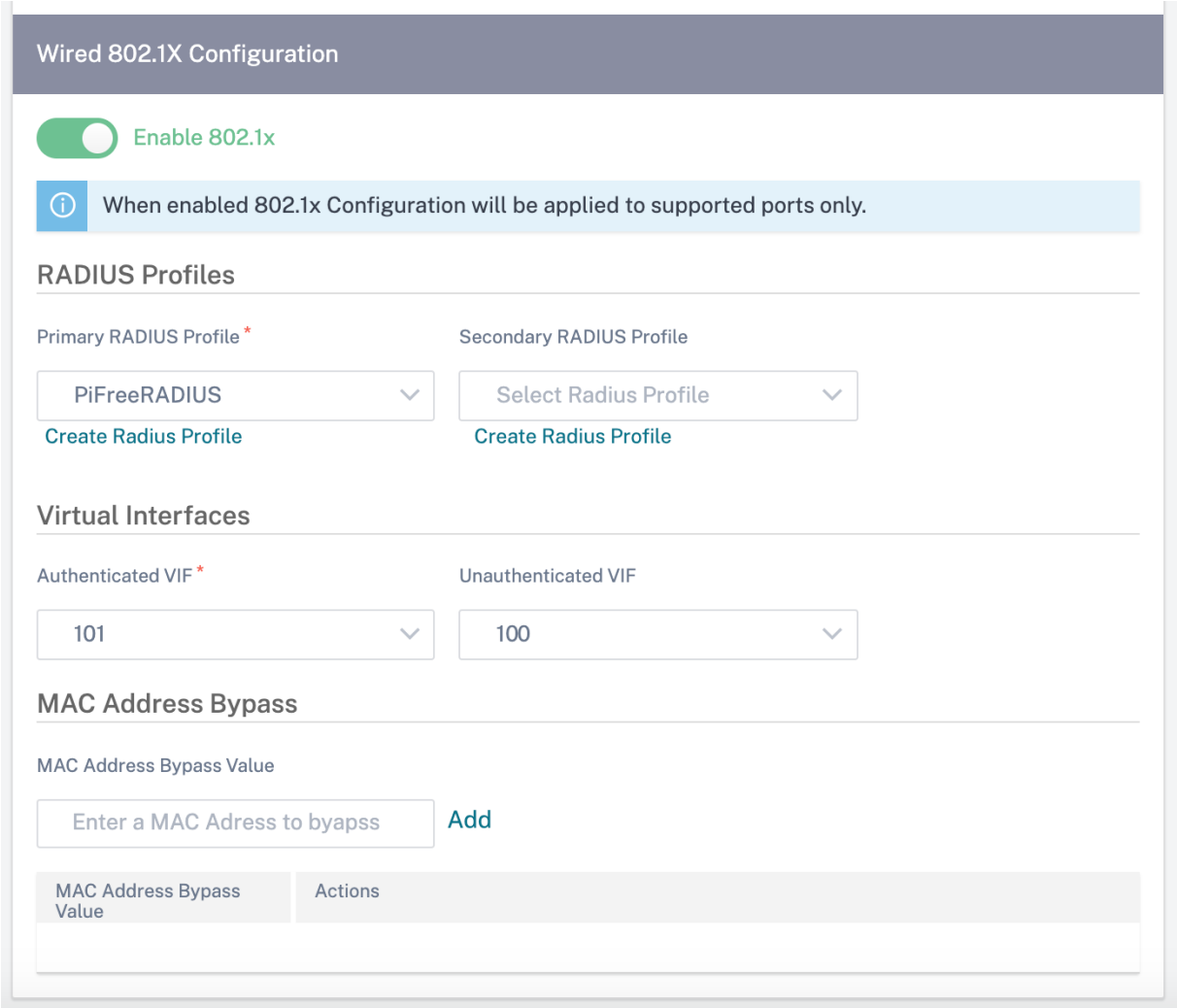
问局域网资源。未能通过身份验证的客户端可以通过拔掉以太网电缆，等待 3 分钟，然后重新插入以太网电缆来重试身份验证。Citrix SD-WAN 110、210 和 410 平台最多支持 32 个客户端（包括经过身份验证和未经身份验证）。所有其他平台最多支持 64 个客户端（包括经过身份验证和未经身份验证）。

要配置 802.1X 身份验证，请导航到“站点配置”**>** “接口”，然后打开“启用 **802.1x**”切换按钮。选择现有 RADIUS 配置文件或单击“创建 **RADIUS** 配置文件”创建 RADIUS 配置文件有关创建 RADIUS 配置文件的详细信息，请参阅 RADIUS 服务器配置文件。只要您的设备支持无线 WPA2-Enterprise，则可以使用相同的 RADIUS 配置文件进行有线 802.1x 和无线 WPA2-Enterprise 身份验证。

从 经过身份验证的 **VIF** 下拉列表中选择一个虚拟接口。选定的虚拟接口授予对 LAN 资源的访问权限，以成功进行身份验证请求。

或者，您可以从 未经身份验证的 **VIF** 下拉列表中选择一个接口。选定的虚拟接口为失败的经过身份验证的请求授予对特定 LAN 资源的访问权限。

您可以添加绕过身份验证过程的 MAC 地址列表。来自这些 MAC 地址的流量将被隐式视为经过身份验证。这些 MAC 地址容易受到恶意攻击。因此，只能在物理安全的环境中以及不支持有线 802.1x 身份验证的传统硬件中使用此功能。



您可以在 报告 **>** 警报下查看与有线 **802.1x** 身份验证请求相关的警报。有关更多信息，请参阅 警报。

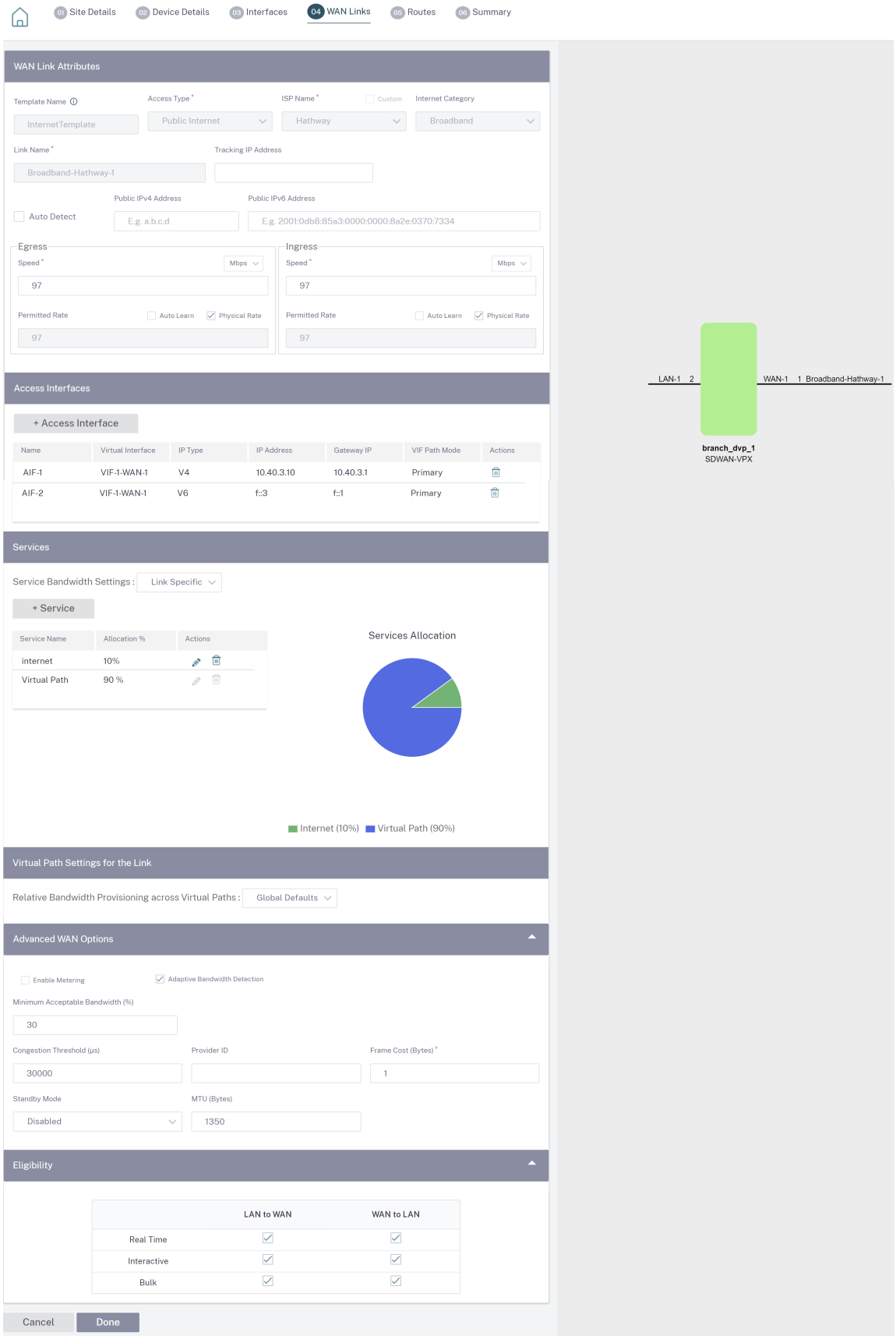
WAN 链接

下一步是配置 WAN 链接。单击 **+ WAN** 链接 开始配置 WAN 链接。

WAN 链接配置包括设置 WAN 链接访问类型和访问接口属性。

您可以从头开始配置 **WAN** 链接 属性，也可以使用 WAN 链接模板 快速配置 WAN 链接属性。如果您已经使用了站点配置文件，则会自动填充 **WAN** 链接 属性。

WAN 链接属性



- 模板名称：用于创建 WAN 链接的 WAN 链接模板的名称。创建 WAN 链接后，无法修改 WAN 链接模板名称。使用 WAN 链接模板创建 WAN 链接后，您就无法编辑访问类型、ISP 名称或互联网类别。
- 访问类型：指定链接的 WAN 连接类型。
  - 公共互联网：表示该链路通过 ISP 连接到互联网。
  - 私有内联网：表示该链接已连接到 SD-WAN 网络中的一个或多个站点，无法连接到 SD-WAN 网络之外的位置。
  - **MPLS**：专用内联网的专用变体。表示该链接使用一个或多个 DSCP 标签来控制 Intranet 上两个或多个点之间的服务质量，并且无法连接到 SD-WAN 网络以外的位置。
- **ISP** 名称：服务提供商的名称。
- 互联网类别：在 WAN 链路上启用的 WAN 链路互联网接入技术服务（宽带、卫星、光纤、LTE 等）的类型。
- 链接名称：根据之前的输入自动填充。
- 跟踪 **IP** 地址：虚拟路径上的虚拟 IP 地址，可通过 ping 来确定路径的状态。
- 公有 **IPv4** 地址 和 公有 **IPv6** 地址：NAT 或 DNS 服务器的 IP 地址。仅当串行 HA 部署中的 WAN 链接访问类型为公共互联网或专用 Intranet 时，此地址才适用并公开。公有 IP 可以手动配置，也可以使用“自动学习”选项自动学习。
- 自动检测：启用后，SD-WAN 设备会自动检测公有 IP 地址。仅当设备角色是 分支 而不是 主控制节点 **(MCN)** 时，此选项才可用。
- 出口速度：广域网到局域网的速度。
  - 速度：广域网到局域网流量的可用或允许速度，以 Kbps 或 Mbps 为单位。
  - 允许速率：如果 SD-WAN 设备不应使用整个 WAN 链接容量，请相应地更改允许的速率。
  - 自动学习：当您不确定带宽并且链路不可靠时，可以启用自动学习功能。自动学习 功能仅学习底层链路容量，并在将来使用相同的值。
  - 物理速率：WAN 链路的实际带宽容量。
- 入口速度：局域网到广域网的速度。
  - 速度：局域网到广域网流量的可用或允许速度，以 Kbps 或 Mbps 为单位。
  - 允许速率：如果 SD-WAN 设备不应使用整个 LAN 链路容量，请相应地更改允许的速率。
  - 自动学习：当您不确定带宽并且链路不可靠时，可以启用自动学习功能。自动学习 功能仅学习底层链路容量，并在将来使用相同的值。
  - 物理速率：局域网链路的实际带宽容量。

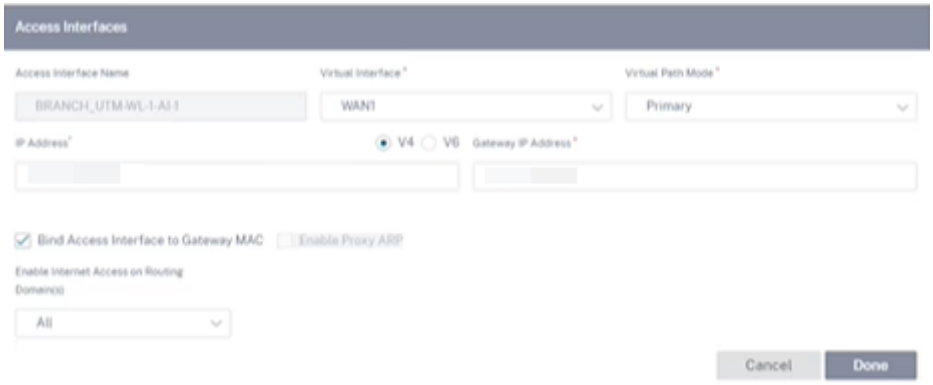
MPLS 队列

MPLS 队列 设置仅适用于 WAN 链路访问类型 MPLS。此选项旨在在 MPLS WAN Link 上启用与服务提供商 MPLS 队列对应的队列的定义。有关添加 MPLS 队列的信息，请参阅 MPLS 队列。

访问界面

访问接口定义 WAN 链路的 IP 地址和网关 IP 地址。每个 WAN 链路至少需要一个接入接口。以下是访问接口参数：

- 访问接口名称：引用访问接口的名称。默认使用以下命名约定：WAN_link_Name-编号：其中 WAN_link_Name 是要与此接口关联的 WAN 链路的名称，编号是当前为此链接配置的接入接口数，递增 1。
- 虚拟接口：访问接口使用的虚拟接口。从为当前分支站点配置的虚拟接口的下拉菜单中选择一个条目。
- 虚拟路径模式：指定当前 WAN 链接上虚拟路径流量的优先级。选项包括：主要、次要或排除。如果设置为“排除”，则访问接口仅用于互联网和内联网流量。
- **IP** 地址：从设备到广域网的访问接口端点的 IP 地址。根据需要选择 V4 (IPv4) 或 V6 (IPv6)。
- 网关 **IP** 地址：网关路由器的 IP 地址。
- 将访问接口绑定到网关 **MAC**：如果启用，则在互联网或内联网服务上接收的数据包的源 MAC 地址必须与网关 MAC AddressWank 链接 > 高级广域网选项相匹配。
- 启用代理 **ARP**：如果启用，则在无法访问网关时，虚拟 WAN 设备会回复网关 IP 地址的 ARP 请求。
- 在路由域上启用 **Internet** 访问：在相应路由域的所有路由表中自动创建默认路由 (0.0.0.0/0)。您可以为所有路由域启用，也可以启用 NONE。如果需要互联网访问，它避免了在所有路由域中创建独占静态路由的需要。



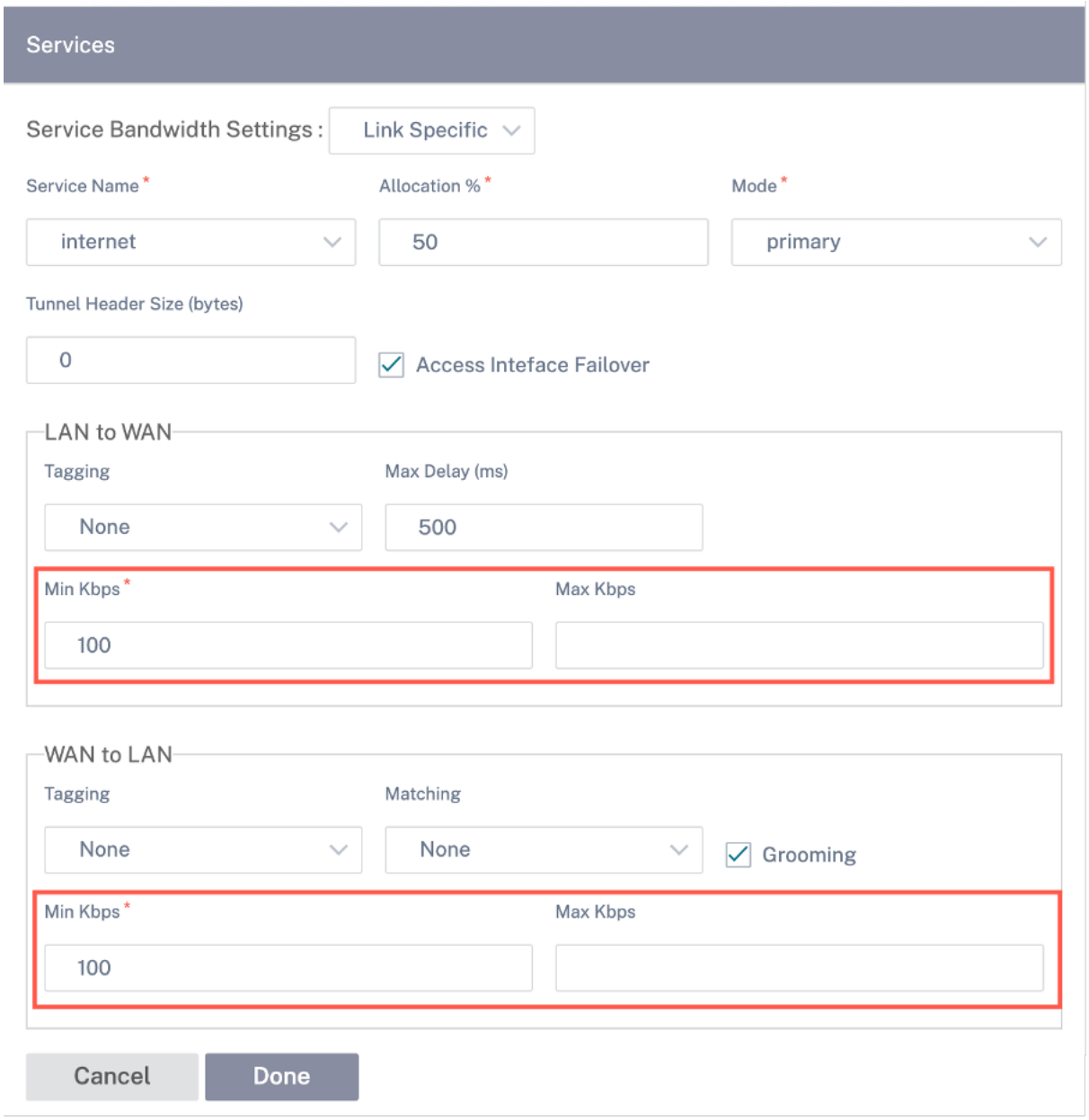
服务

“服务”部分允许您添加服务类型并分配用于每种服务类型的带宽百分比。您可以从“交付 服务”部分定义服务类型并为其配置属性。您可以选择使用这些全局默认设置，也可以从“服务带宽设置”下拉列表中配置链路特定的 服务带宽设置。如果选择链接特定，请输入以下详细信息：

- 服务名称：WAN 链接服务的名称。
- 分配百分比：从链路总容量中分配给服务的带宽的保证公平份额。
- 模式：基于所选服务的 WAN Link 的运行模式。对于 Internet，有“主”、“辅助”和“余额”三种；对于内联网，有“小学”和“辅助”。
- 隧道标头大小：隧道标头的大小，以字节为单位。
- 局域网到广域网标签：应用于服务上局域网到广域网数据包的 DHCP 标签。
- **LAN** 到 **WAN** 延迟：超过 WAN 链路带宽时缓冲数据包的最大时间。
- **LAN** 到 **WAN Min Kbps**：为服务保留的最小上载带宽值。“最低 **Kbps** ”是必填字段。
- **LAN** 到 **WAN** 最大千位数：为服务保留的最大上传带宽值。**Max Kbps** 字段是可选的，该值不能小于配置的最小上传带宽值。该值必须大于或等于最小上传带宽值。
- **WAN to LAN** 标签：应用于服务上的 WAN to LAN 数据包的 DHCP 标签。

- **WAN to LAN** 匹配：分配给服务的互联网广域网与局域网数据包的匹配标准。
- **WAN to LAN** 最小 **Kbps**：为服务保留的最小下载带宽值。“最低 **Kbps** ”是必填字段。
- **WAN to LAN Max Kbps**：为服务保留的最大下载带宽值。**Max Kbps** 字段是可选的，该值不能小于配置的最小下载带宽值。该值必须大于或等于最小下载带宽值。
- **WAN** 到 **LAN** 整理：如果启用，则会随机丢弃数据包，以防止 WAN 到 LAN 的流量超出服务配置的带宽。

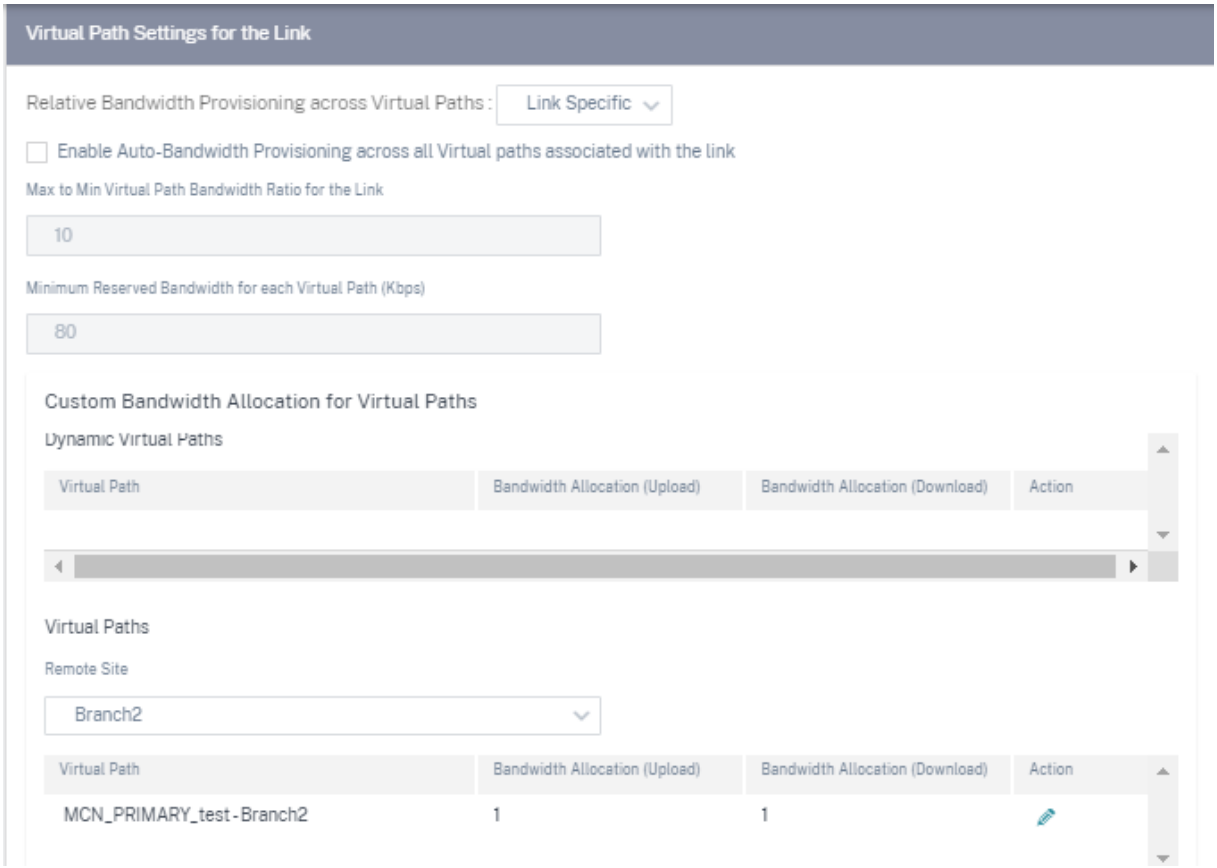
> 注意
>
> 最小和最大 Kbps 字段不适用于虚拟路径。



链接的虚拟路径设置

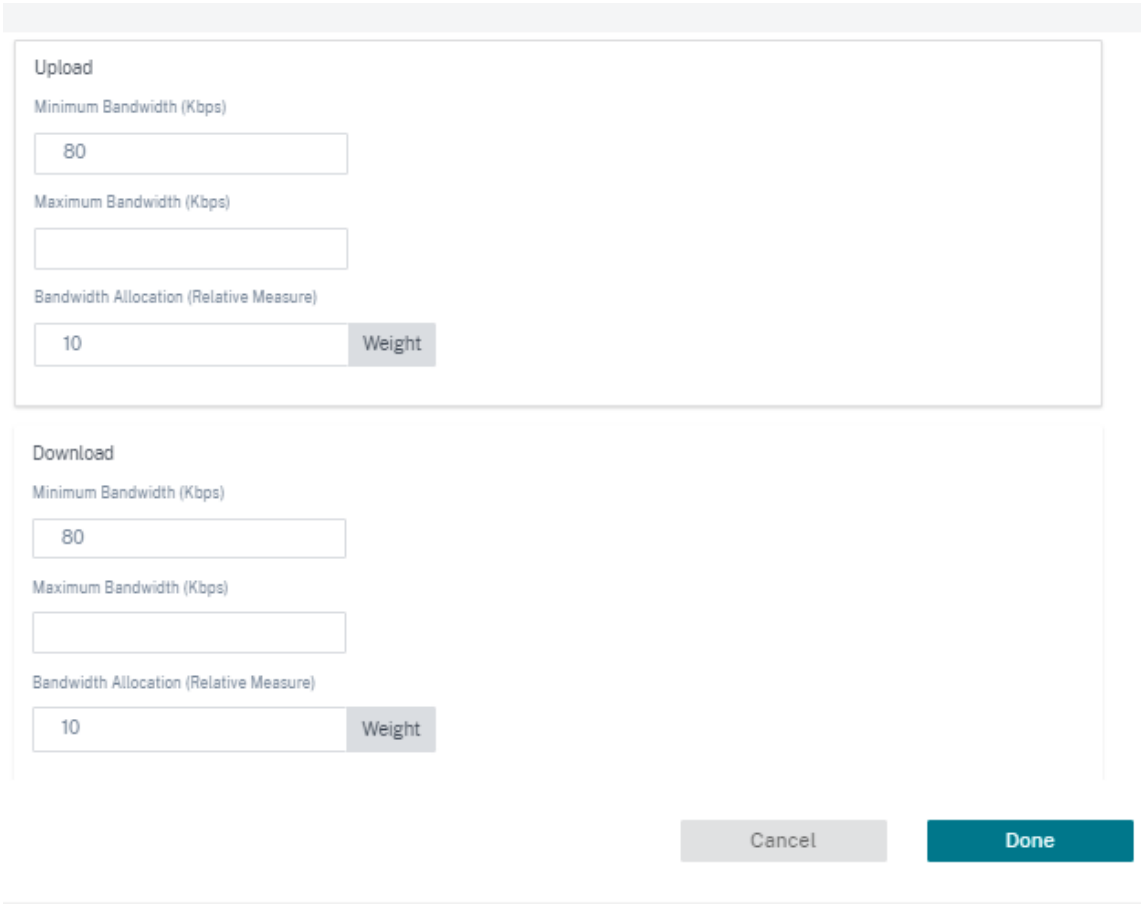
根据需要将虚拟路径上的相对带宽配置选择为“全局默认”或“特定链接”。选择 **Link**Specific 后，当您启用自动带宽配置时，将自动计算虚拟路径服务的带宽份额，并根据远程站点可能消耗的带宽量进行相应应用。

- 链路的最大和最小 虚拟路径带宽比：您可以设置可应用于所选 WAN 链接的最大和最小虚拟路径比率。
- 每条虚拟路径的最小预留带宽 **(Kbps)**：您可以设置每个虚拟路径的最小预留带宽值（以 Kbps 为单位）。



要自定义与 WAN 链接关联的虚拟路径的带宽，请执行以下操作：

1. 清除“在与 链接关联的所有虚拟路径上启用自动带宽 **Pro** visioning”复选框。
2. 在“虚拟路径的自定义带宽分配”部分中，选择一个远程站点。您可以为通往远程站点的虚拟路径配置带宽。
    - 最小带宽 **(Kbps)**：为虚拟路径保留的最小带宽。可以为虚拟路径设置的最小带宽为 80 Kbps。
    - 最大带宽 **(Kbps)**：虚拟路径可以从 WAN 链路使用的最大带宽。如果未设置最大带宽，则站点将使用所有可用带宽。
    - 带宽分配（相对测量）：从虚拟路径组的合格带宽中分配给虚拟路径的带宽份额。例如，如果一个包含 3 个虚拟路径的 WAN 链接组有资格获得 30 Mbps 的带宽，并且您想为每个虚拟路径分配相等的带宽，则将 10 更新为远程站点上的带宽分配。



3. 单击完成。

> 注意
>
> 即使在两个站点之间禁用了先前配置的动态虚拟路径之后，Citrix SD-WAN Orchestrator 服务仍会保留先前配置的自定义带宽设置。重新配置动态虚拟路径时，请务必手动更新自定义带宽设置。

带宽配置需要考虑的几点

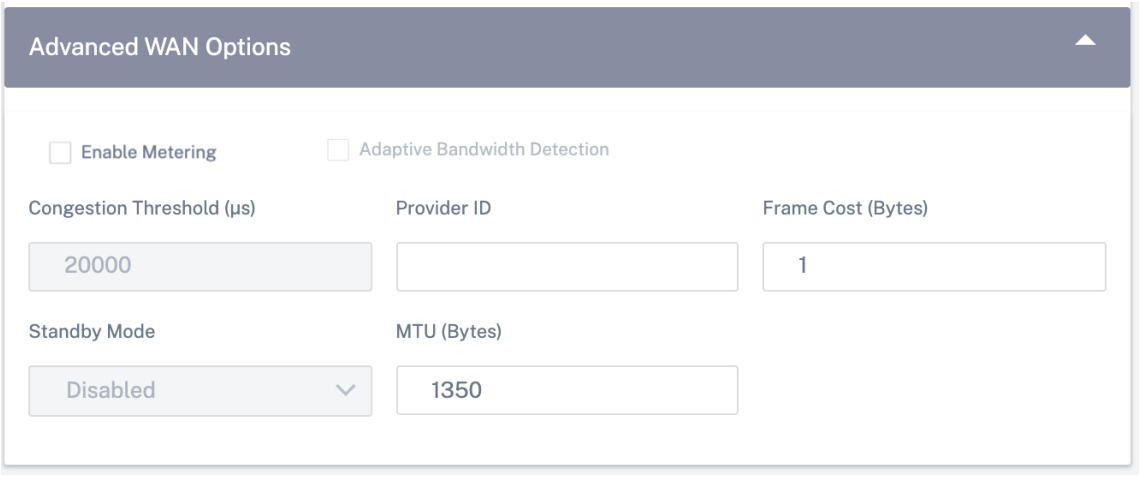
- 默认情况下，所有分支机构和广域网服务（虚拟路径/互联网/内联网）的权重各为 1。
- 当带宽要求存在很大差异时，需要自定义带宽。
- 在可用站点之间启用动态虚拟路径时，WAN 链路容量将在数据中心的静态虚拟路径和动态虚拟路径之间共享。

高级 **WAN** 选项

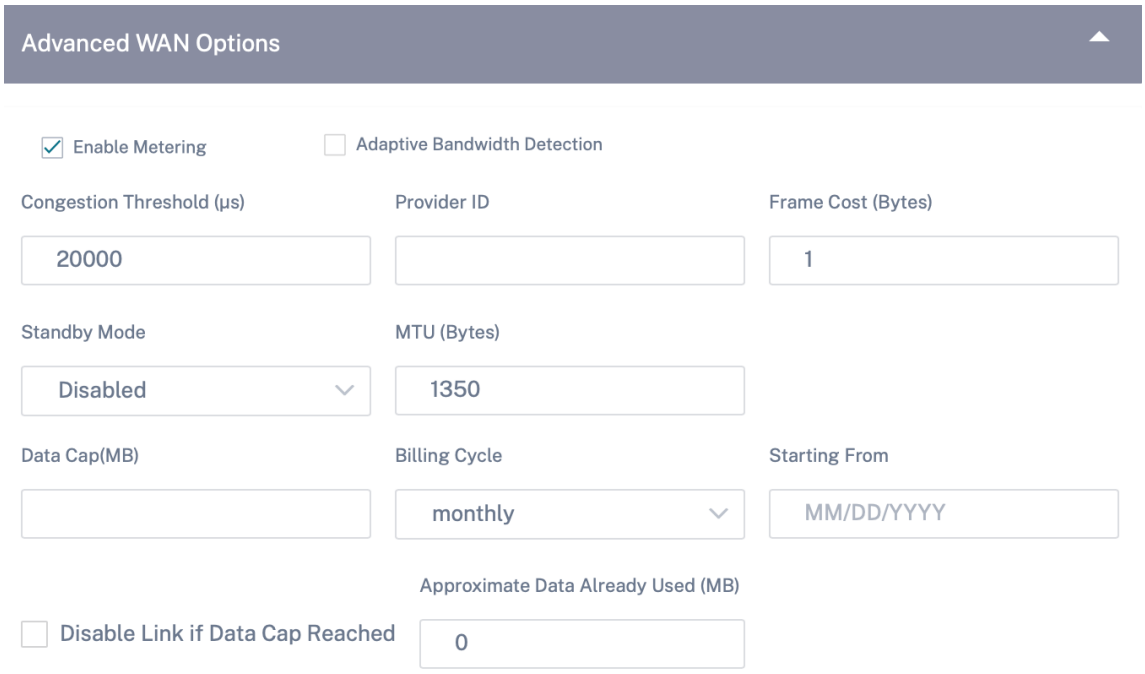
WAN 链路高级设置允许配置 **ISP** 的特定 属性。

- 拥塞阈值：拥塞量过后 WAN 链路会限制数据包传输以避免进一步拥塞。
- 提供商 **ID**：提供商在发送重复数据包时区分路径的唯一标识符。

- 帧成本（字节）：向每个数据包添加额外的报头/尾部字节，例如以太网 IPG 或 AAL5 预告片。
- **MTU**（字节）：以字节为单位的最大原始数据包大小，不包括帧成本。
- 待机模式：待机链路不用于传输用户流量，除非它变为活动状态。默认情况下，WAN 链接的待机模式处于禁用状态。有关待机模式的更多信息，请参阅 待机模式。



- 启用计量：跟踪 WAN 链接的使用情况，并在链接使用量超过配置的数据上限时提醒用户。有关计量的详细信息，请参阅 计量和备用 WAN 链接。



- 自适应带宽检测：检测到丢失时，以较低的带宽速率使用 WAN 链路。当可用带宽低于配置 的最低可接受带宽时，将路径标记为 BAD。使用路径或自适应带宽检测组下的自定义坏损失敏感度。

> 注意
>
> 自适应带宽检测仅适用于客户端，而不适用于 MCN。

- 可接受的最小带宽：当带宽速率不同时，WAN 到 LAN 允许速率的百分比，低于该百分比的路径将被标记为 BAD。虚拟路径两侧的最小 kbps 不同。该值可以在 10%-50%之间，默认值为 30%。

有关更多信息，请参阅 自适应带宽检测

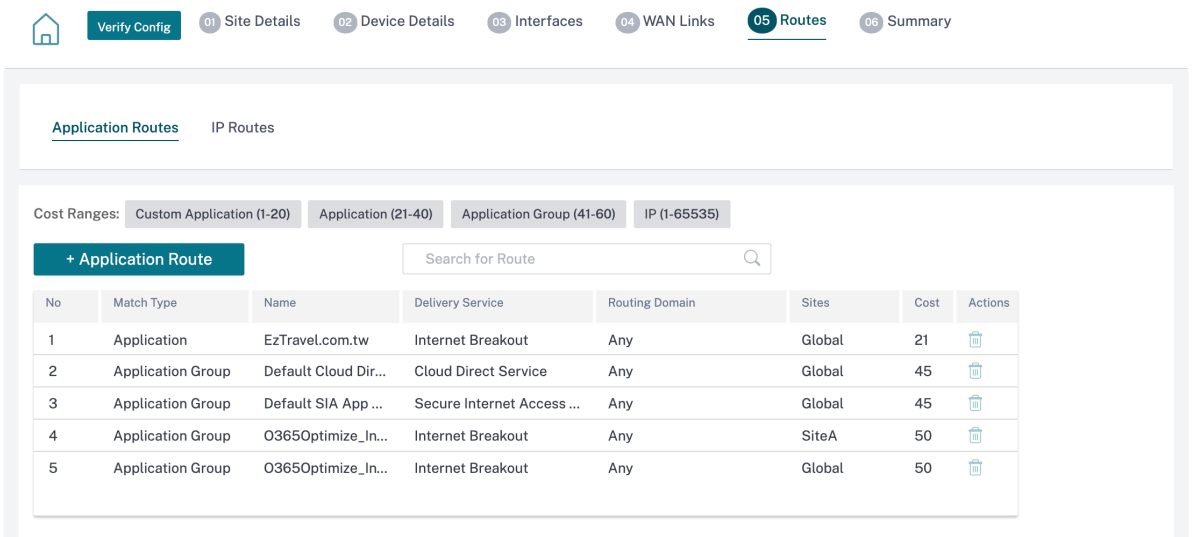
路由

站点配置工作流中的下一步是创建路由。您可以根据自己的站点要求创建应用程序和 IP 路由。

> 注意
>
> 在引入“应用程序路由”和“**IP** 路由”选项卡之前添加的 路由列在“**IP** 路由”选项卡下，“传送服务”为 Internet。

在网络级别创建的全局路由和特定站点的路由会自动列在“路由”> “应用程序路由和路由”“**IP** 路由”选项卡下。您只能在站点级别查看全球路线。要编辑或删除全局路由，请导航到网络级别的配置。

您还可以在站点级别创建、编辑或删除路线。



申请路线

单击 **+** 应用程序路由，创建应用程序路由。

- 自定义应用程序匹配标准：
  - 匹配类型：从下拉列表中选择匹配类型为 应用程序/自定义应用程序/应用程序组。
  - 应用程序：从下拉列表中选择一个应用程序。

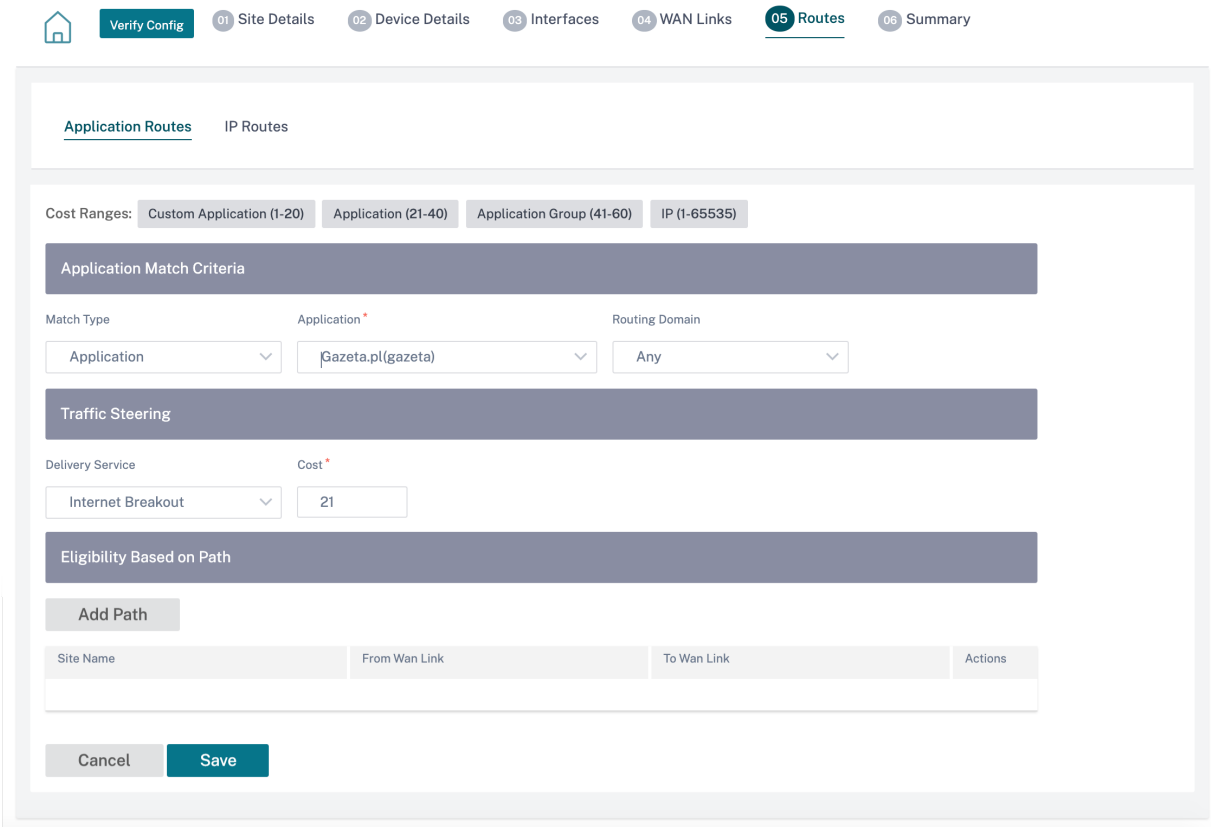
  - 路由域：选择路由域。

- 交通指导
  - 配送服务：从列表中选择一项配送服务。
  - 成本：反映每条路径的相对优先级。成本降低，优先级越高。

- 基于路径的资格：
  - 添加路径：选择站点和 WAN 链接，包括目标和来源。如果添加的路径出现故障，则应用程序路由不会接收任何流量。

如果添加了新的应用程序路由，则路由成本必须在以下范围内：

- 自定义应用程序：1—20
- 应用程序：21—40
- 应用程序组：41—60



IP 路线

转到 **IP** 路由 选项卡，然后单击 **+ IP** 路由 以创建 IP 路由策略来引导流量。

- **IP** 协议匹配标准：

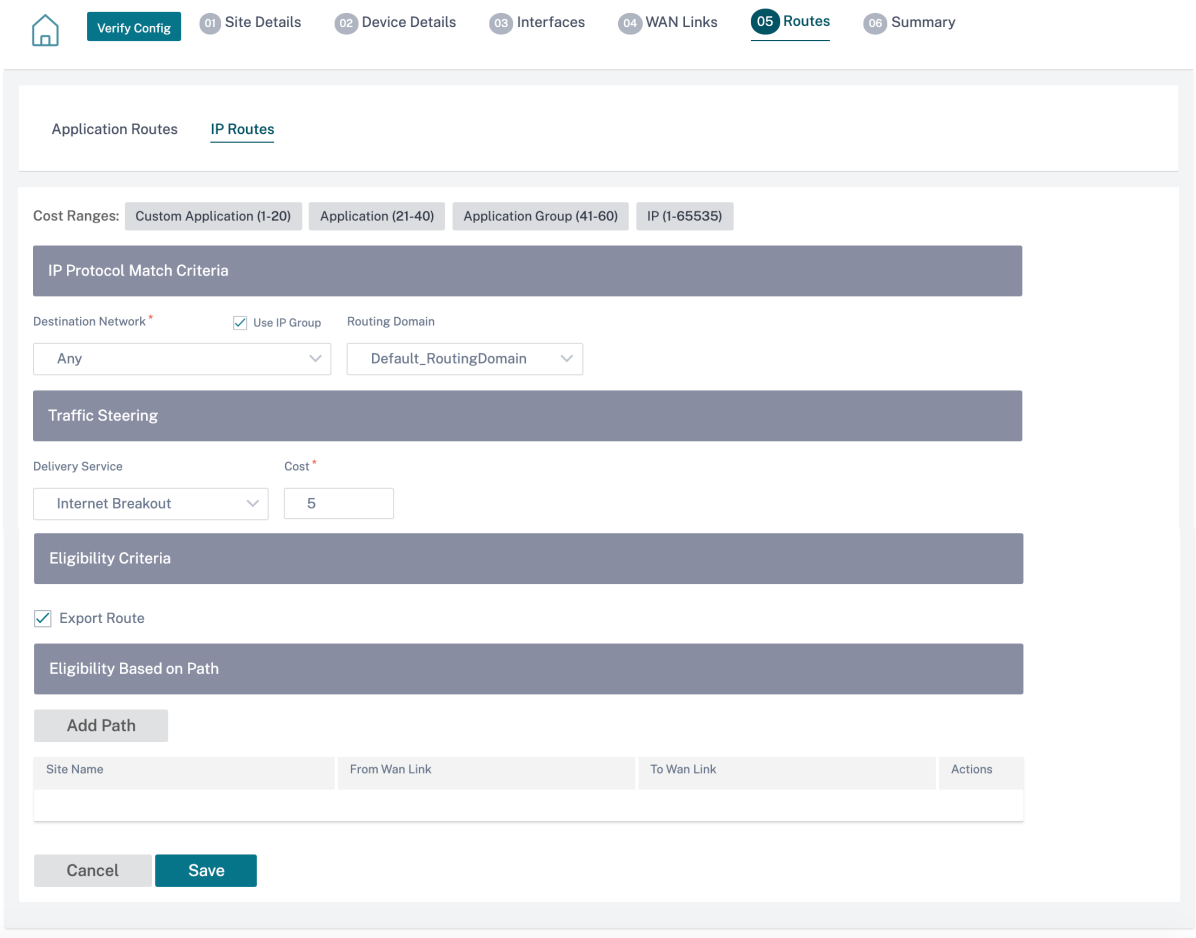
  - 目标网络：添加有助于转发数据包的目标网络。
  - 使用 **IP** 组：您可以添加目标网络或启用“使用 IP 组”复选框以从下拉列表中选择任何 IP 组。
  - 路由域：从下拉列表中选择一个路由域。

- 交通指导
  - 配送服务：从下拉列表中选择一项配送服务。
  - 成本：反映每条路径的相对优先级。成本降低，优先级越高。

- 资格标准：
  - 导出路径：如果选中“导出路径”复选框并且该路径是本地路径，则默认情况下该路径符合导出条件。如果路由是基于 INTRANET/INTERNET 的路由，则必须启用 WAN 到 WAN 转发才能导出。如果清除了 导出路由 复选框，则本地路由不符合导出到其他 SD-WAN 的条件，并且具有本地意义。

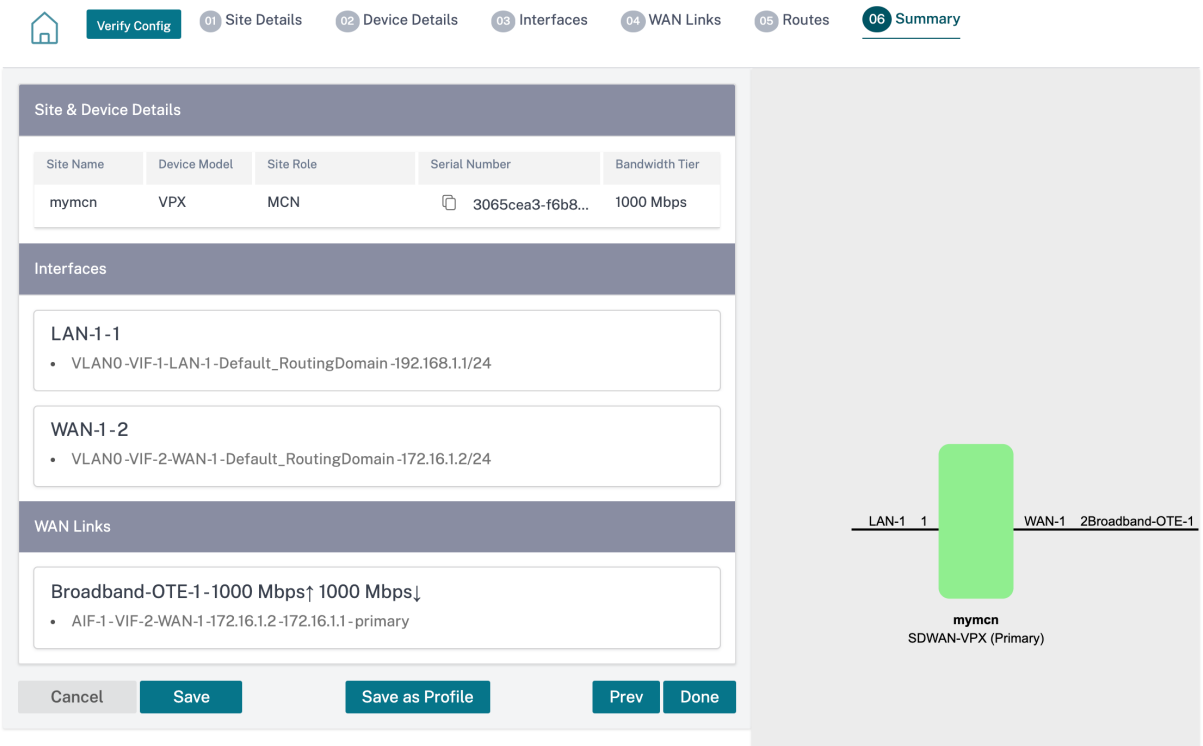
- 基于路径的资格：
  - 添加路径：选择站点和 WAN 链接，包括目标和来源。如果添加的路径出现故障，则 IP 路由不会接收任何流量。

如果添加了新的 IP 路由，则路由开销必须在 1—20 范围内。



摘要

本部分提供站点配置摘要，以便在提交相同配置之前进行快速审阅。



使用“另存为模板”选项将站点配置另存为模板，以便在其他站点中重复使用。单击“完成”标志着站点配置完成，并带您进入 网络配置**-**主 页以查看所有已配置的站点。有关更多信息，请参阅 网络配置。

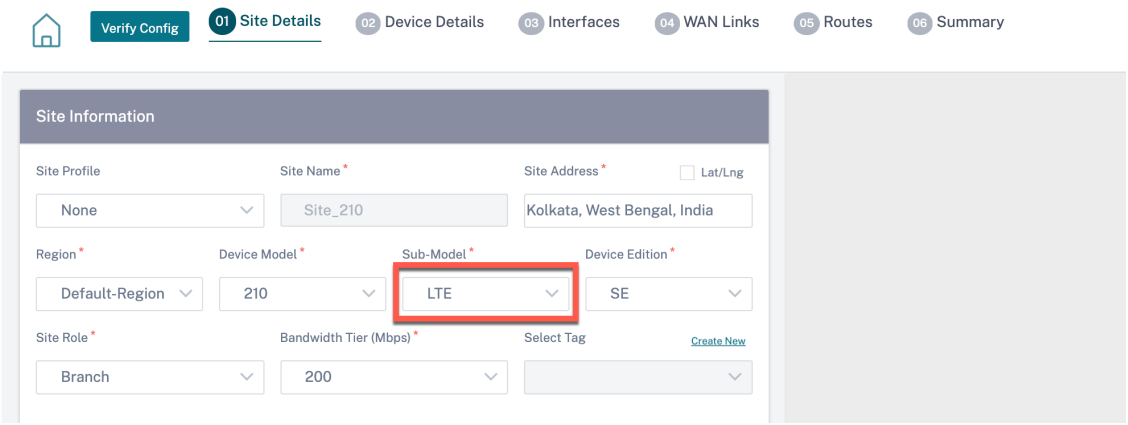
LTE 固件升级

October 21, 2022

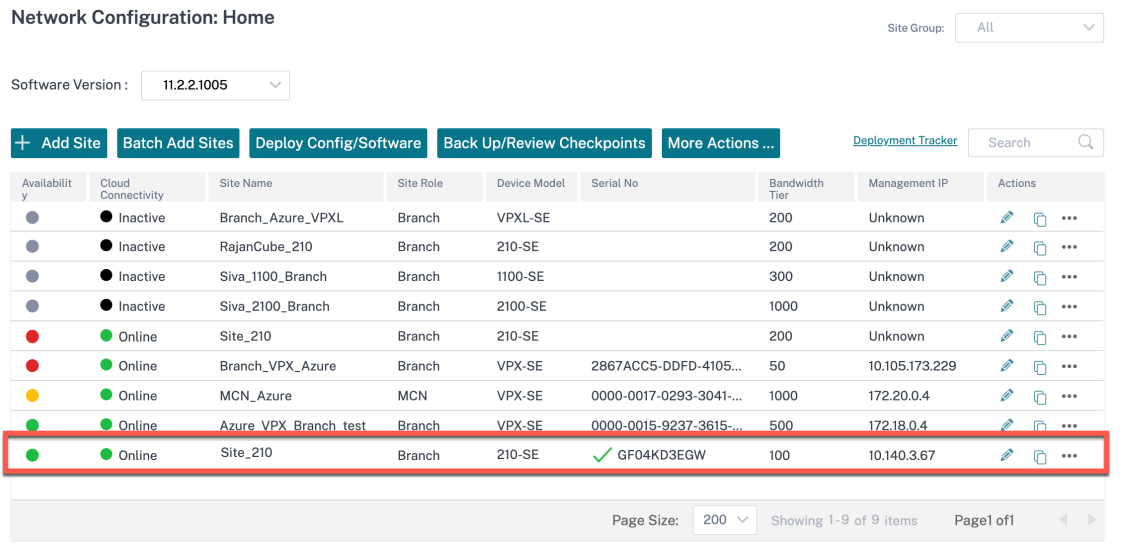
Citrix SD-WAN Orchestrator 服务允许您配置和管理网络中的所有 LTE 站点。它包括通过内部 LTE 调制解调器或外部 USB LTE 调制解调器连接的设备。

要在网络中配置 LTE 站点：

1. 在站点级别，导航到 配置 **>** 站点配置。

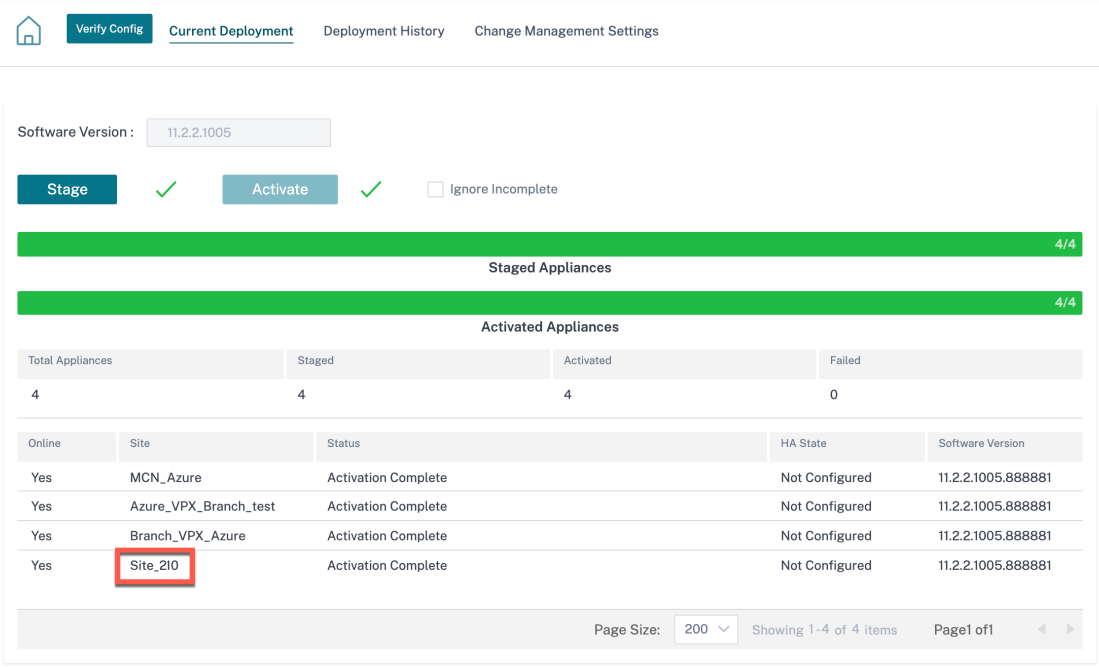


2. 选择子型号为 **LTE** 以及其他必要的详细信息，然后单击“保存”。有关站点配置的更多信息，请参阅 站点配置。
3. 创建站点后，导航到 网络配置主页，然后单击“部署配置/软件”按钮。



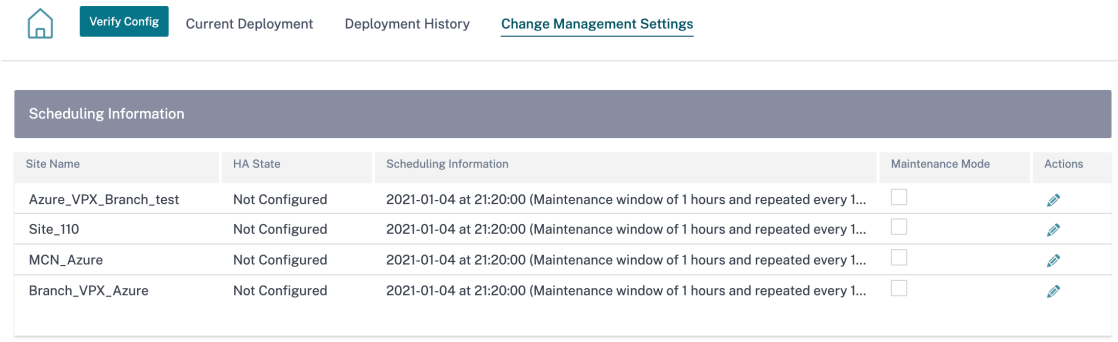
> C
>
> 注意
>
> 目前，Citrix SD-WAN 210 设备支持 LTE。

4. “软件版本”字段自动填充最新的软件版本包，该文件不可编辑。单击 **Stage** 后，它会下载所选软件版本的所有相应 LTE 固件。



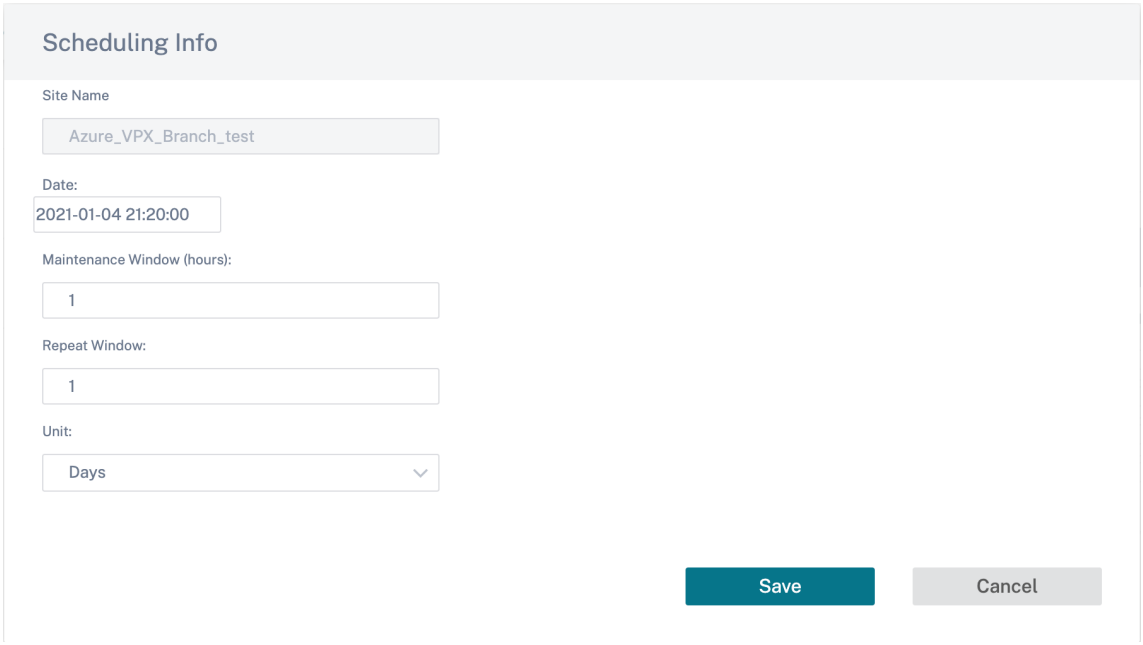
完成暂存需要几分钟的时间。您可以查看状态以跟踪暂存进度。最初，状态显示 暂停运行，然后显示 正在下载设备软件，最后显示 暂存完成。您可以随时通过单击“取消舞台”按钮来 取消登台。

5. 部署完成后，单击“激活”按钮激活软件。
6. LTE 软件激活是计划窗口的一部分。要升级 LTE 软件，请导航到“更改管理设置”选项卡。您可以看到包含计划信息和操作选项的站点名称列表。



在计划窗口中，指定了完成 LTE 软件升级的特定时间范围。

7. 单击操作符号并提供计划信息-日期与时间、维护时段持续时间（以小时为单位）、以天/周/月为单位的重复窗口。单击保存。



一旦设置了时间，它就会将信息传播到设备。当设备中的时间与计划窗口中设置的时间匹配时，LTE 固件将升级。通过计划窗口，您可以配置升级 LTE 固件的特定时间。设置计划窗口后，LTE 固件升级不会立即开始。

> 注意
>
> 对于所有设备，以下是已经设置的默认计划信息：
>
> - 时间表窗口 -21:20:00
> - 维护窗口 -1 小时
> - 重复窗口 - 1 天
>
> 因此，如果您不配置变更管理设置，则计划窗口会自动处理更新。此外，当您将 维护时段（小时）的值设置 为 **0** 时，LTE 固件升级会立即进行。

从 11.1.0 开始，在站点界面组页面上添加了一个新的配置旋钮，用于带内管理配置。对于需要通过带内 IP 管理的任何设备，这是强制性配置。在 Citrix SD-WAN Orchestrator 服务中缺少此配置可能会导致设备脱机（当通过 LTE 管理的 210 和 110 升级到 11.1.0 时，尤其重要）。

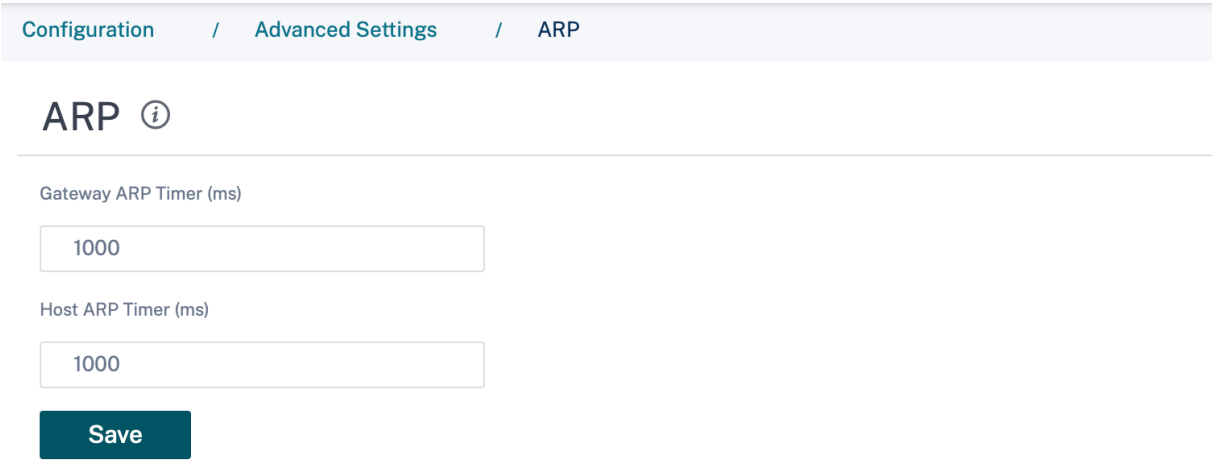
地址解析协议

October 21, 2022

在 Citrix SD-WAN 部署（例如 Gateway 和 One-Arm）中，当频繁收到地址解析协议 (ARP) 请求时，接入点会过载，影响流量。要克服流量过载问题，您可以配置以下 ARP 计时器以特定的间隔时间发送 ARP 请求。

- 网关 **ARP** 计时器 **(ms)**：对已配置的网关 IP 地址进行 ARP 请求之间的时间（范围：100—20000 毫秒）。

- 主机 **ARP** 计时器 **(ms)**：对已配置的主机 IP 地址进行 ARP 请求之间的时间（范围：1000—180000 毫秒）。



邻居发现协议

October 21, 2022

在 IPv6 网络中，Citrix SD-WAN 设备会定期多播路由器广告消息以宣布其可用性并将信息传递给 SD-WAN 网络中的相邻设备。路由器通告包括 IPv6 前缀信息。在 Citrix SD-WAN 设备上运行的邻居发现协议 (NDP) 使用这些路由器通告来确定同一链路上的相邻设备。NDP 还确定彼此的链路层地址、查找邻居并维护活动邻居的可访问性信息。

要配置 NDP 路由器通告，请导航到 配置 **>** 高级设置 **> NDP** ，然后单击 **+ NDP**。

从“虚拟接口”下拉列表中选择一个已配置的 虚拟接口。选择 启用通告 可启用定期发送路由器通告和响应所选虚拟接口的路由器请求。

指定最大、最小和路由器的生命周期间隔。

- 最大间隔：发送定期未经请求的多播路由器通告之间允许的最长时间（以秒为单位）。
- 最小间隔：发送定期未经请求的多播路由器通告之间允许的最短时间（以秒为单位）。
- 路由器寿命：主机认为路由器有效的时间（以秒为单位）。0 表示路由器不能用作默认路由器

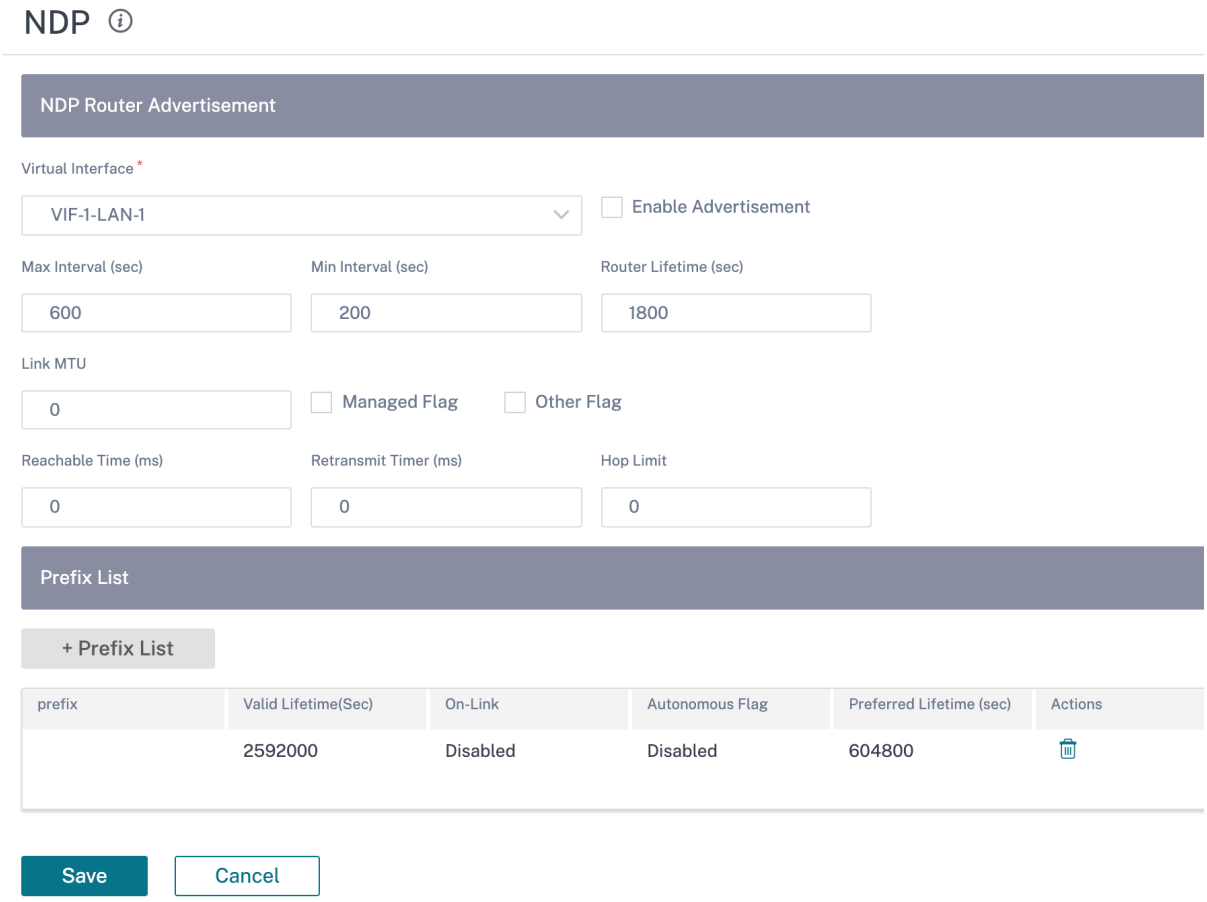
如果 IP 地址可通过 DHCPv6 协议获得，请选择 托管标志。如果配置信息（IP 地址除外）可通过 DHCPv6 协议获得，请选择 其他标志。

为所选接口指定以下值。

- 链路 **MTU**：接口推荐的最大传输单元 (MTU)。
- 可达时间：**NDP** 协议保持在可达状态的时间（以毫秒为单位）。
- 重传计时器：解析 IP 地址或探测邻居时，重新传输邻居请求消息的间隔时间（以毫秒为单位）。
- 跳数限制：路由器通告中包含的最大跳数。

单击 + 前缀列表并输入以下值：

- 前缀：无类域间路由 (CIDR) 表示法中的前缀和前缀长度。
- 有效生命周期：前缀有效的时间（以秒为单位）。-1 表示无穷大，这意味着前缀永久保留。
- **ON-Link**：选中此前缀将被视为网络的本地前缀。
- 自治标志：启用后，主机的无状态地址自动配置 (SLAAC) 将使用该前缀生成 IP 地址。
- 前缀生命周期：前缀被视为首选的时间（以秒为单位）。



虚拟路径

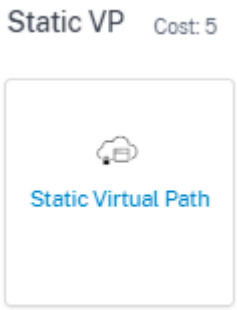
October 21, 2022

虚拟路径是两条 WAN 链路之间的逻辑链路。它包括一组 WAN 路径，组合在一起，在两个 SD-WAN 节点之间提供高服务级别的通信。这是通过不断测量和适应不断变化的应用需求和广域网条件来实现的。SD-WAN 设备根据每个路径测量网络。虚拟路径可以是静态的（始终存在）或动态路径（仅当两个 SD-WAN 设备之间的流量达到配置的阈值时才存在）。

静态虚拟路径

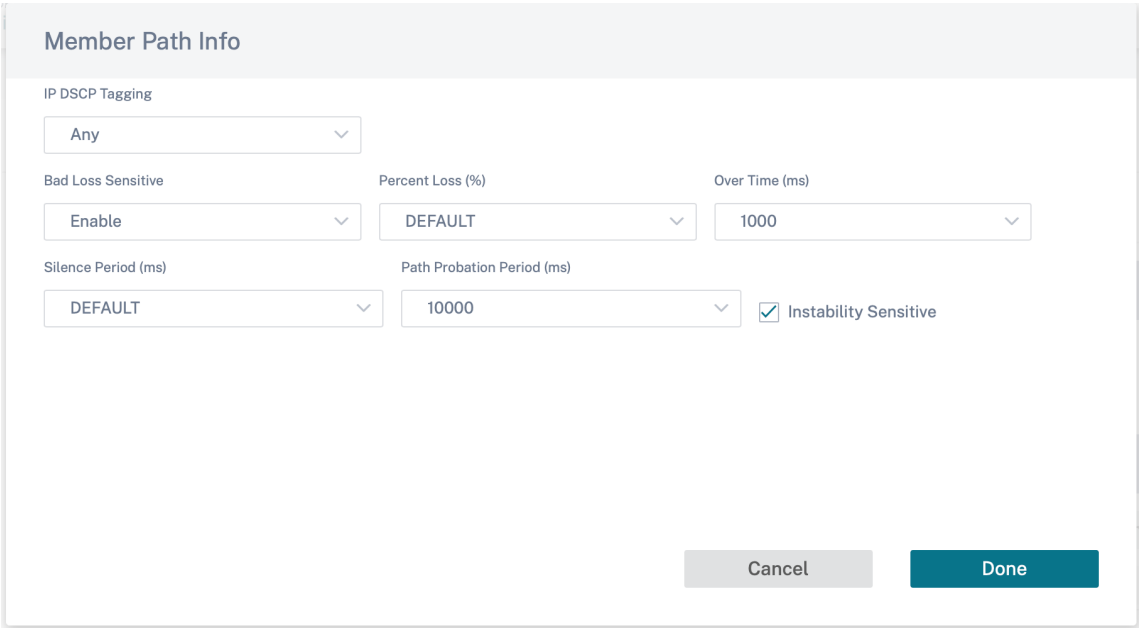
虚拟路径设置继承自全局 WAN 链接自动路径设置。您可以覆盖这些配置，然后添加或删除成员路径。您还可以根据站点和应用的 QoS 配置文件过滤虚拟路径。为 WAN 链接指定一个跟踪 IP 地址，该地址可以通过 Ping 来确定 WAN 链路的状态。您还可以为反向路径指定反向跟踪 IP，该 IP 可以通过 Ping 来确定反向路径的状态。

要配置静态虚拟路径，请从站点级别导航到 配置 > 高级设置 > 虚拟路径 > 静态虚拟路径。



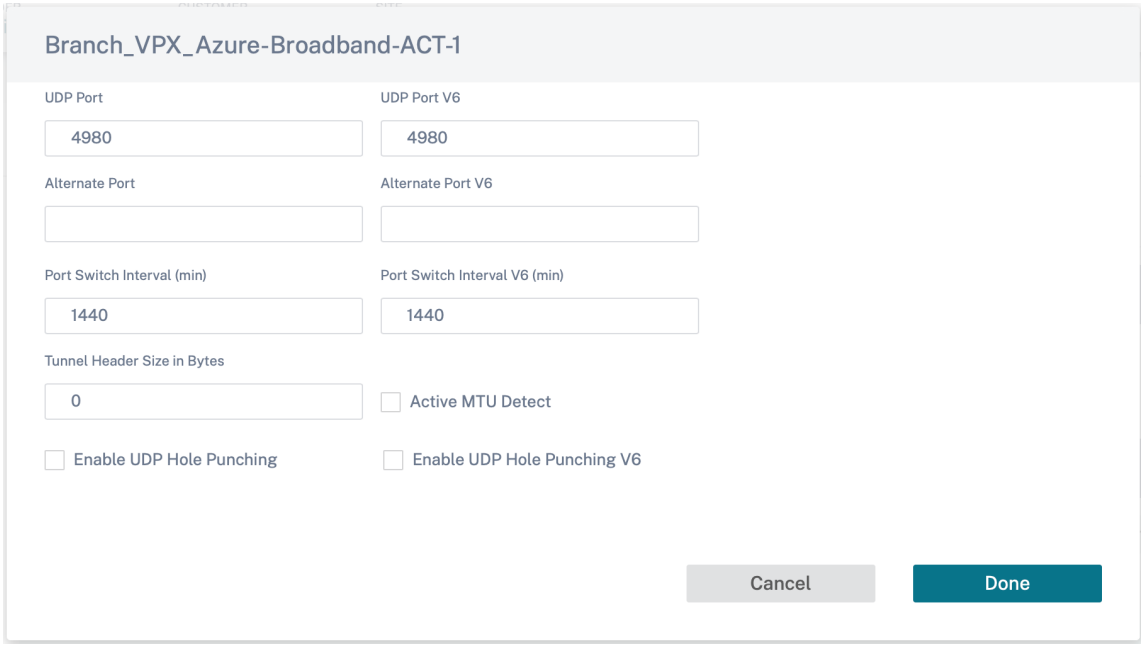
活动成员路径列在“活动成员路径”部分中，您可以查看或编辑成员路径设置。

- **IP DSCP** 标记：虚拟路径控制协议 (VPCP) 帧的外部 IP 标头的标记。
- 丢失敏感：如果启用，路径可能会因为丢失而被标记为 BAD，并在路径分数中造成延迟损失。设置将路径标记为坏所需时间内的损失百分比。如果带宽损失是不可容忍的，请禁用此选项。
- 丢失百分比：如果数据包丢失量在配置的时间内超过设定的百分比，则 GOOD Path 状态将更改为 BAD。
- 随着时间的推移：如果在这段配置的时间内丢包超过设定的百分比，则路径状态将被标记为 BAD。
- 静默期：当在指定时间内未收到任何数据包时，路径状态从 GOOD 转换为 BAD。
- 路径试用期：将路径状态从 BAD 更改为 GOOD 之前需要等待的时间。
- 不稳定性敏感：考虑因状态不良和其他延迟峰值而造成的延迟惩罚。



列出了所选活动成员路径的 WAN 链接详细信息，您可以根据需要更改设置。可以为 IPv4 和 IPv6 配置 **UDP** 端口 设置。

- **UDP** 端口：用于局域网到广域网和广域网到局域网数据包传输的端口。你也可以指定。
- 备用端口：启用 UDP 端口切换时使用的备用 UDP 端口。
- 端口切换间隔：WAN Link 交替其 UDP 端口的时间间隔，以分钟为单位。
- 以字节为单位的隧道标头大小：隧道标头的大小，以字节为单位（如果适用）。
- 主动 **MTU** 检测：动态虚拟路径的 LAN 到 WAN 路径正在主动探测 MTU。
- 启用 **UDP** 打孔：MCN 协助兼容的受 NAT 保护的客户端站点之间进行 UDP 连接。

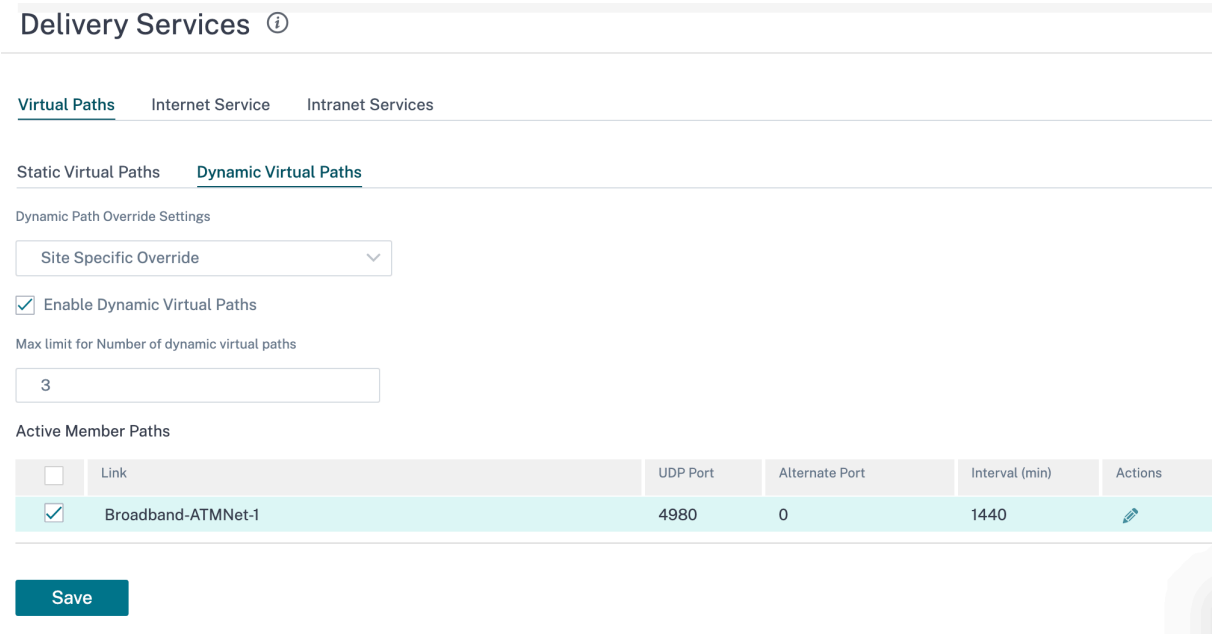


动态虚拟路径

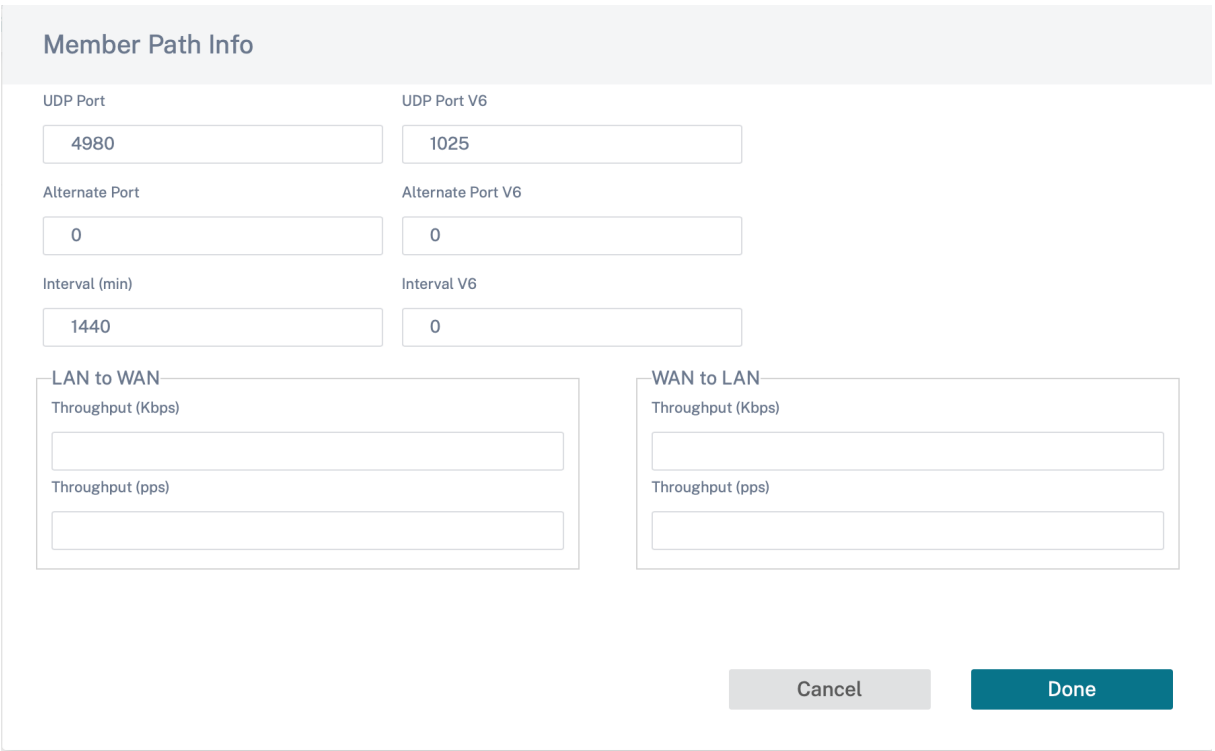
随着对 VoIP 和视频会议的需求，办公室之间的流量增加了。通过数据中心设置全网状连接非常耗时且效率低下。借助 Citrix SD-WAN，您可以使用动态虚拟路径功能按需自动创建办公室之间的路径。会话最初使用现有的固定路径。由于满足带宽和时间阈值，如果新路径比固定路径具有更好的性能特征，则会动态创建新路径。会话流量通过新路径传输，从而有效地使用资源。动态虚拟路径仅在需要时才存在，并减少传入和传出数据中心的流量。

要配置动态虚拟路径，请从站点级别导航到 配置 > 高级设置 > 虚拟路径 > 动态虚拟路径。

选择“覆盖全局默认值”以覆盖继承自全局 WAN 链接自动路径设置的虚拟路径设置。选择“启用动态虚拟路径”以允许此站点与通过中间节点连接的其他站点之间的动态虚拟路径。为站点设置允许的最大动态虚拟路径。



设置 UDP 端口和动态虚拟路径阈值。在 LAN 到 WAN 或 WAN 到 LAN 上触发动态虚拟路径的中间站点上指定吞吐量阈值（以 kbps 或每秒数据包数为单位）。



动态路由

October 21, 2022

在网络中配置和部署 SD-WAN 设备后，连接建立后，务必确保通过覆盖 SD-WAN 网络正确重定向流量。您可以使用 ping 和 traceroute 诊断工具检查流量重定向。如果 ping 和 traceroute 测试表明通过底层路径建立了连接，则可以使用以下动态路由协议实现流量重定向。

- 开放最短路径优先 **(OSPF)**：它是一种内部网关协议，用于在自治系统（如企业网络）内重定向流量。OSPF 使用链路状态路由算法来检测网络拓扑的变化，并通过首先计算每条路由的最短路径来重新路由数据包。使用此协议重定向 MPLS 流量。有关详细信息，请参阅 **OSPF** 部分。
- 边界网关协议 **(BGP)**：它是一种外部网关协议，旨在在互联网上的不同自治系统之间重定向流量路由和可达性信息。它能够根据 ISP 确定的路径做出路由决策。使用此协议重定向互联网流量。有关更多信息，请参阅 “配置 **BGP** ”部分。

以前，动态路由功能仅适用于单个路由器 ID。您可以为所有配置的路由域（一个用于 OSPF 和 BGP）全局配置唯一的路由器 ID，也可以不提供路由器 ID。从 Citrix SD-WAN 11.3.1 以后的版本中，您不仅可以为整个协议配置路由器 ID，还可以为每个路由域配置路由器 ID。借助此增强功能，您可以以稳定的方式在具有不同路由器 ID 的多个实例之间启用稳定的动态路由。

如果为特定路由域配置路由器 ID，则特定路由器 ID 将覆盖协议级路由域。

OSPF

要配置 OSFF，请导航到 配置 **>** 高级设置 **>** 动态路由 **> OSPF**。

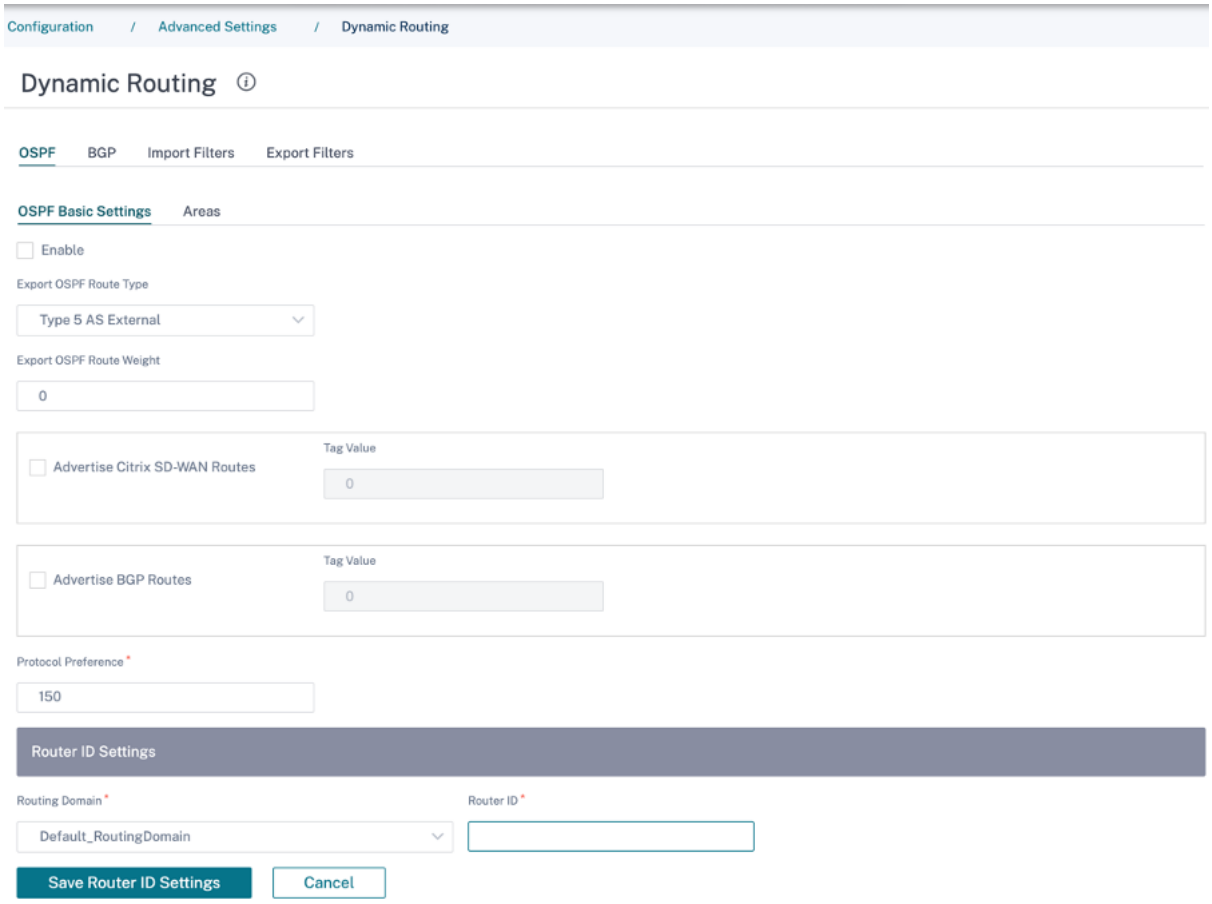
OSPF 基本设置

以下是要配置的参数：

- 启用：允许 SD-WAN 设备上的 OSPF 路由协议开始在相邻路由器之间交换 Hello 数据包。
- 路由器 **ID**：用于 OSPF 通告的 IPv4 地址。此字段为可选字段。如果未指定，则选择参与路由的虚拟接口的最低虚拟 IPv4 地址。对于 IPv6 接口，必须以 IPv4 格式指定路由器 ID。例如，1.1.1.1。

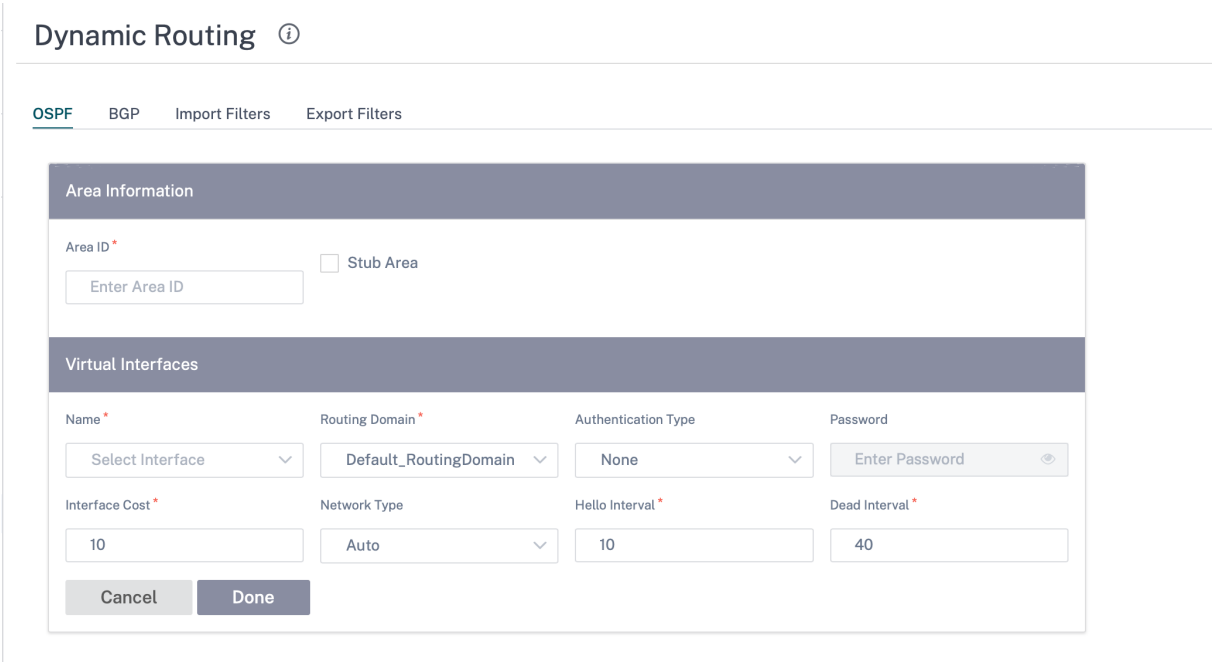
> 注意
>
> - 对于 IPv4 网络，路由器 ID 配置是可选的。但是对于 IPv6 网络，路由器 ID 配置是强制性的。IPv6 网络的路由器 ID 必须配置为相同的 IPv4 格式（32 位表示法）。
>
> * 您必须为同一路由器（如果适用）创建单独的 IPv4 和 IPv6 对等关系，以进行学习和发布。

- 导出 **OSPF** 路由类型：将 SD-WAN 路由作为类型 1 区域内路由或类型 5 外部路由通告给 OSPF 邻居。
- 导出 **OSPF** 路由权重：通告给 OSPF 邻居的成本是原始路由成本和此处配置的权重。
- 通告 **SD-WAN** 路由：向对等网络元素通告 SD-WAN 路由。
- 通告 **BGP** 路由：允许将 BGP 路由重分配到 OSPF 域中。



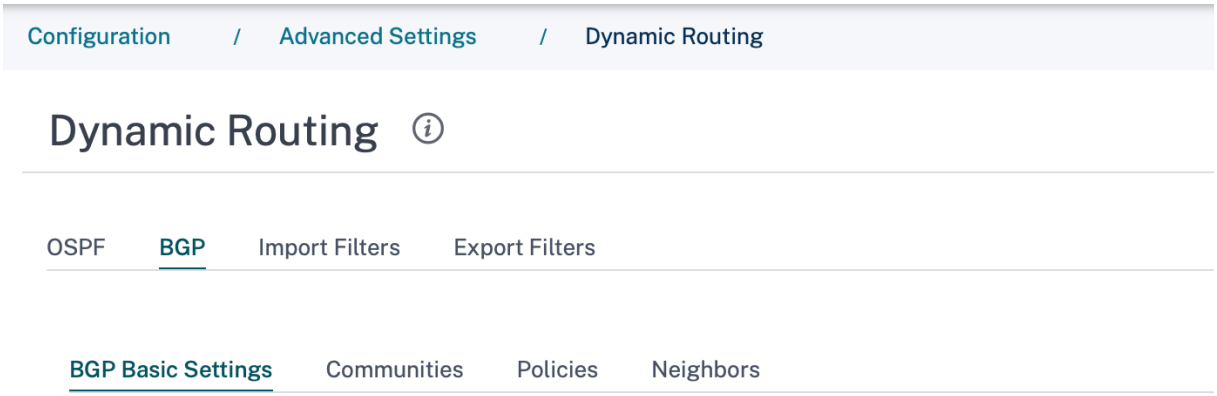
区域

单击 **+ Are** a 并提供网络的区域 ID，OSPF 将从中学习路由并通告路由。末节区域确保该区域不会收到来自指定自治系统之外的路由通告。配置虚拟接口设置。



BGP

要配置 BGP，请导航到 配置 **>** 高级设置 **>** 动态路由 **> BGP**。



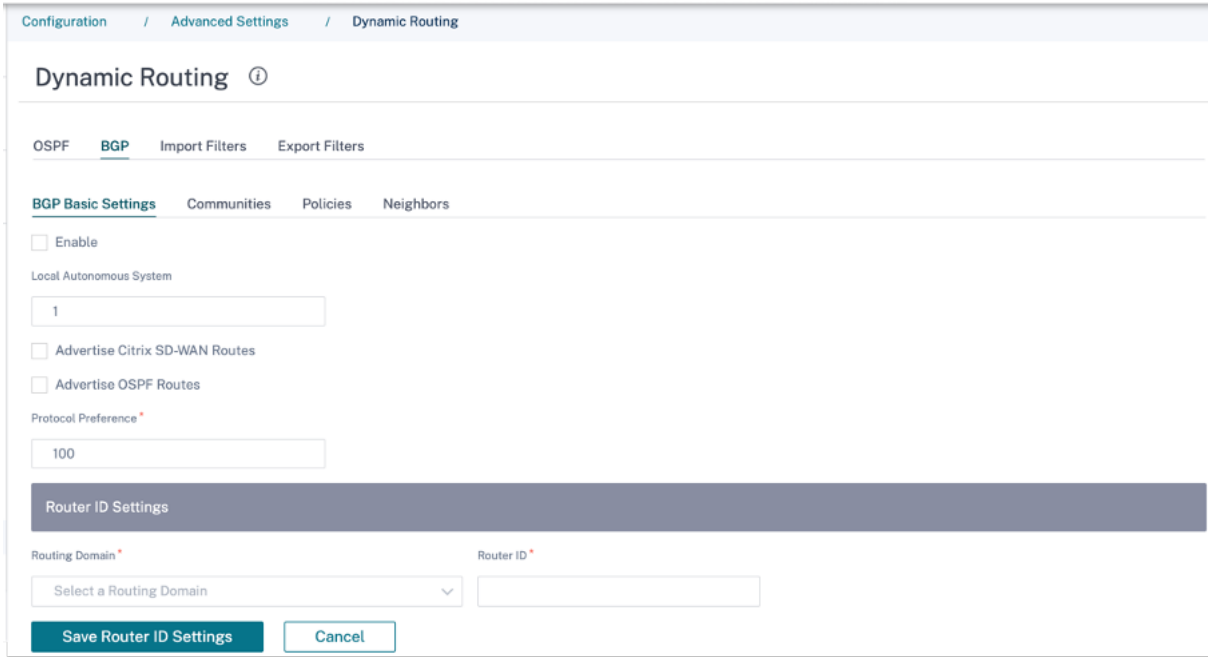
BGP 基本设置

以下是要配置的参数：

- 启用：允许 SD-WAN 设备上的 BGP 路由协议作为 BGP 对等的一部分开始发送打开的消息。
- 路由器 **ID**：用于 BGP 通告的 IPv4 地址。如果未指定路由器 ID，则选择参与路由的虚拟接口的最小虚拟 IPv4 地址。

> 注意
>
> - 对于 IPv4 网络，路由器 ID 配置是可选的。但是对于 IPv6 网络，路由器 ID 配置是强制性的。IPv6 网络的路由器 ID 必须配置为相同的 IPv4 格式（32 位表示法）。
>
> * 您必须为同一路由器（如果适用）创建单独的 IPv4 和 IPv6 对等关系，以进行学习和发布。

- 本地自治系统：运行 BGP 协议的自治系统编号。
- 通告 **SD-WAN** 路由：向对等网络元素通告 SD-WAN 路由。
- 通告 **OSPF** 路由：允许将 OSPF 路由重分配到 BGP 域中。

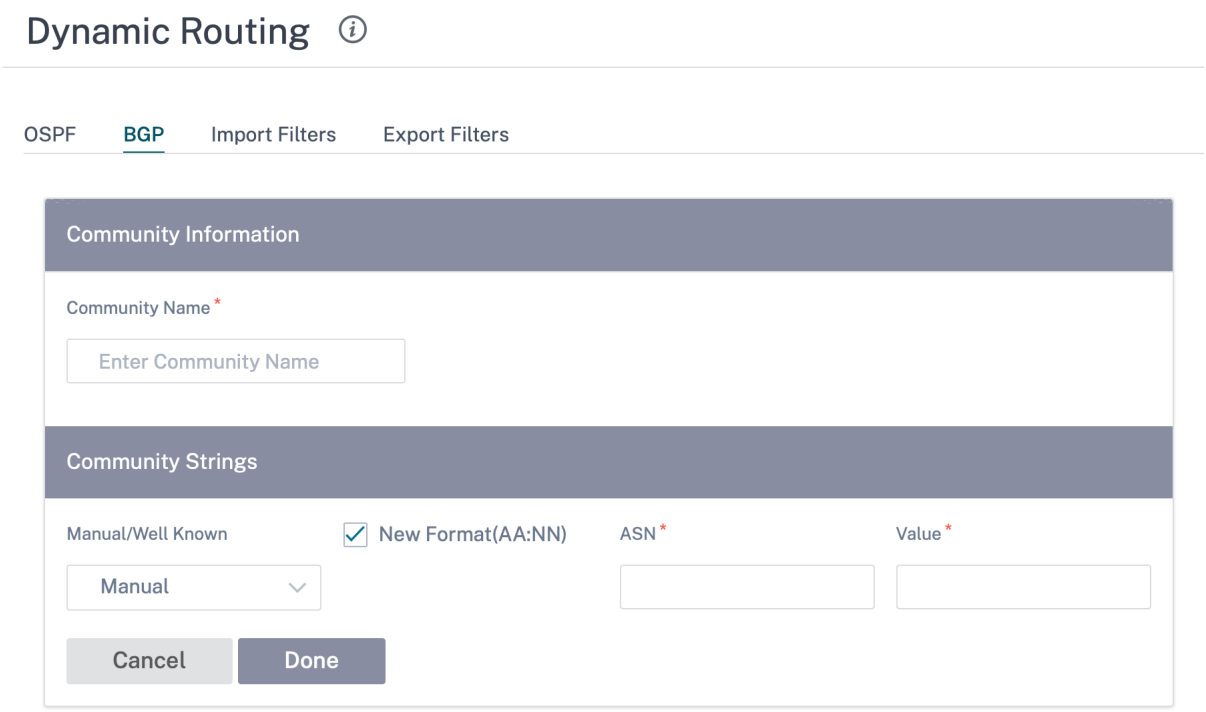


社区

单击 **+** 社区 添加社区。可用于路由过滤的 BGP 社区的集合。社区列表还可用于设置或修改匹配路径的社区。

对于每个策略，用户可以配置多个社区字符串、AS-PATH-PREPEND、**MED** 属性。用户最多可以为每个策略配置 10 个属性。

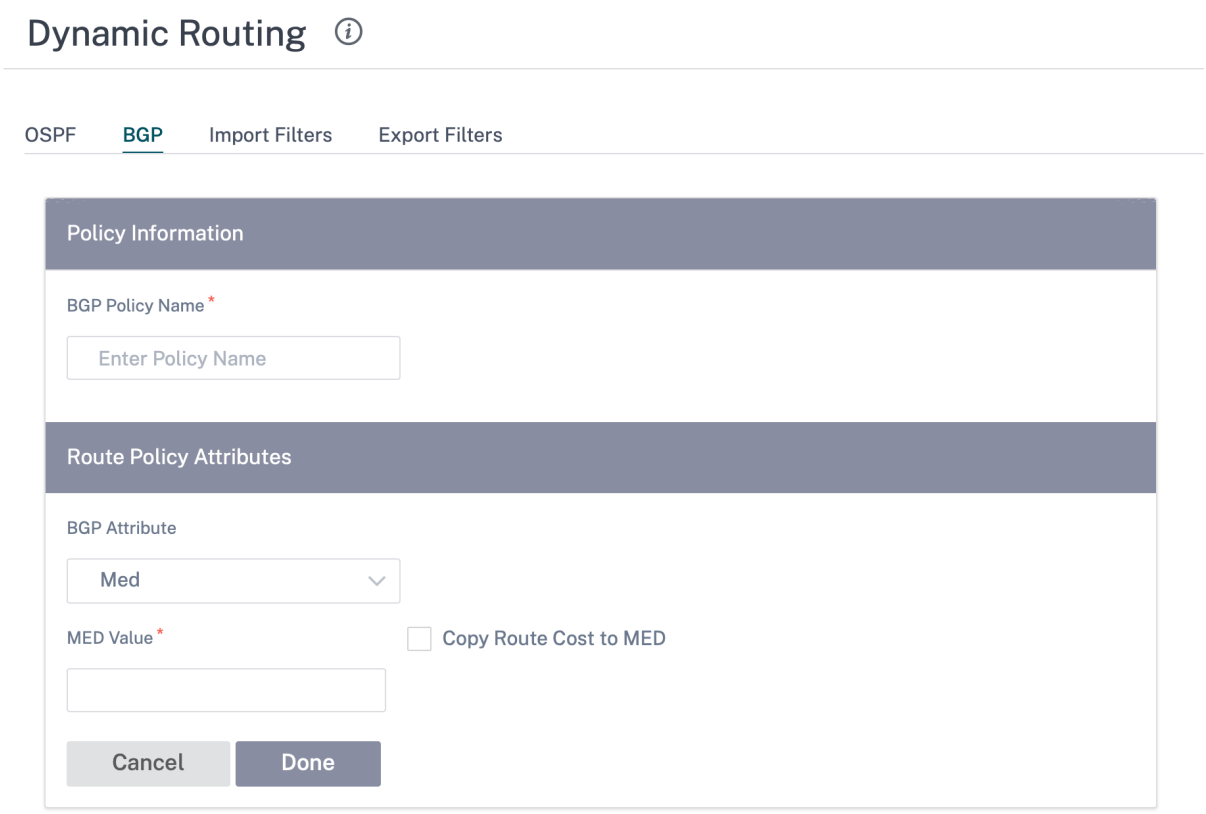
指定社区的名称并输入要发布的社区字符串。



- 社区名称：输入社区名称。
- 手动/众所周知：手动配置 BGP 社区或从列表中选择一个标准的众所周知的 BGP 社区。
- 新格式 **(AA: NN)**：选中该复选框以使用新格式配置 BGP 社区。
- **ASN**：使用新格式进行配置时 BGP 社区的前 16 位数字。
- 值：输入 BGP 社区值。

策略

BGP 属性的集合，可用于设置或修改每个 BGP 对等体的路由属性。在任一方向（导入或导出）创建要选择性应用于每个邻居的一组网络的 BGP 策略。SD-WAN 设备支持每个站点八个策略，最多有八个与策略相关联的网络对象（或八个网络）。

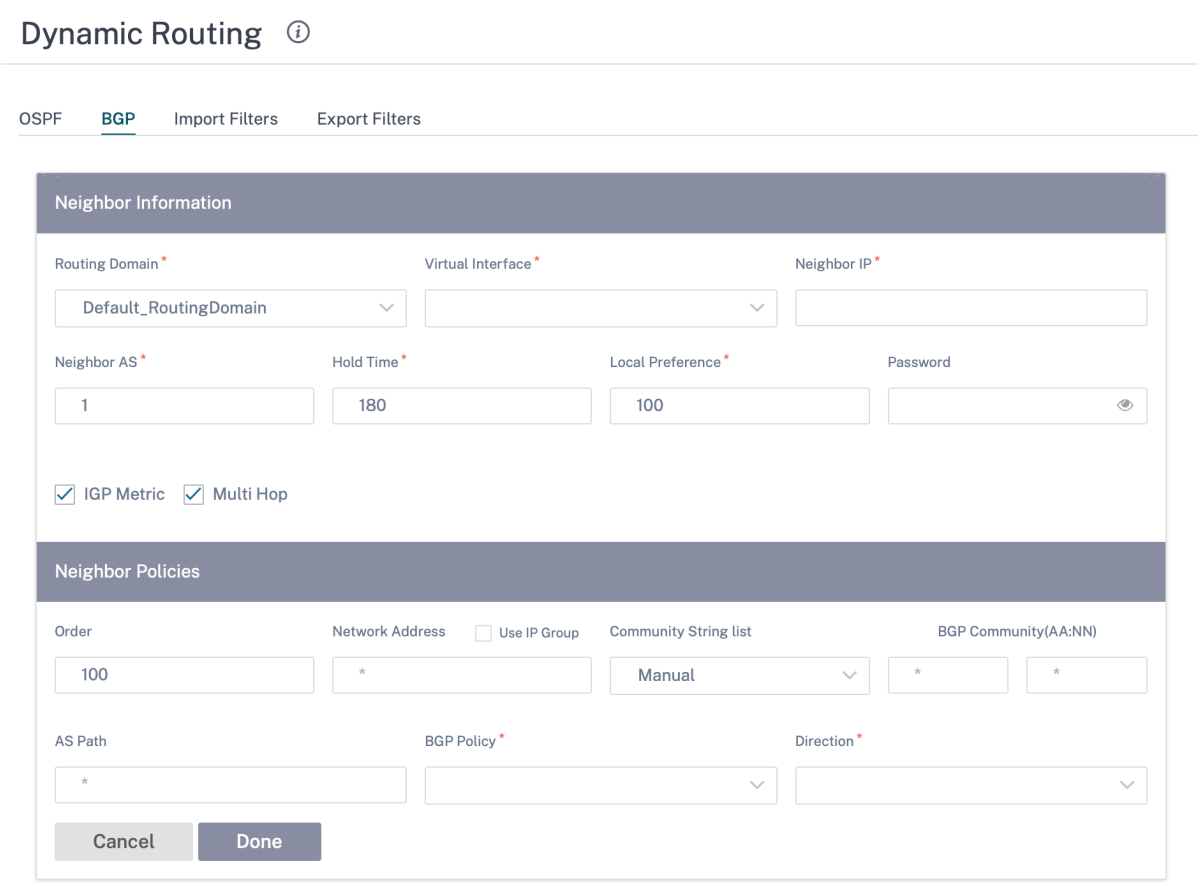


- **BGP** 策略名称：输入 BGP 策略名称。
- **BGP** 属性：从列表中选择 BGP 属性并提供必要的信息。

邻居

邻居是所有已配置的 BGP 对等路由器，这些路由器经过检查以找到最短的路由路径。所有邻居必须属于同一个自治系统。

单击 **+** 邻居为相 邻路由器添加已配置的 BGP 策略。您可以指定方向以指示此策略是否适用于传入或传出的路由。



路由过滤

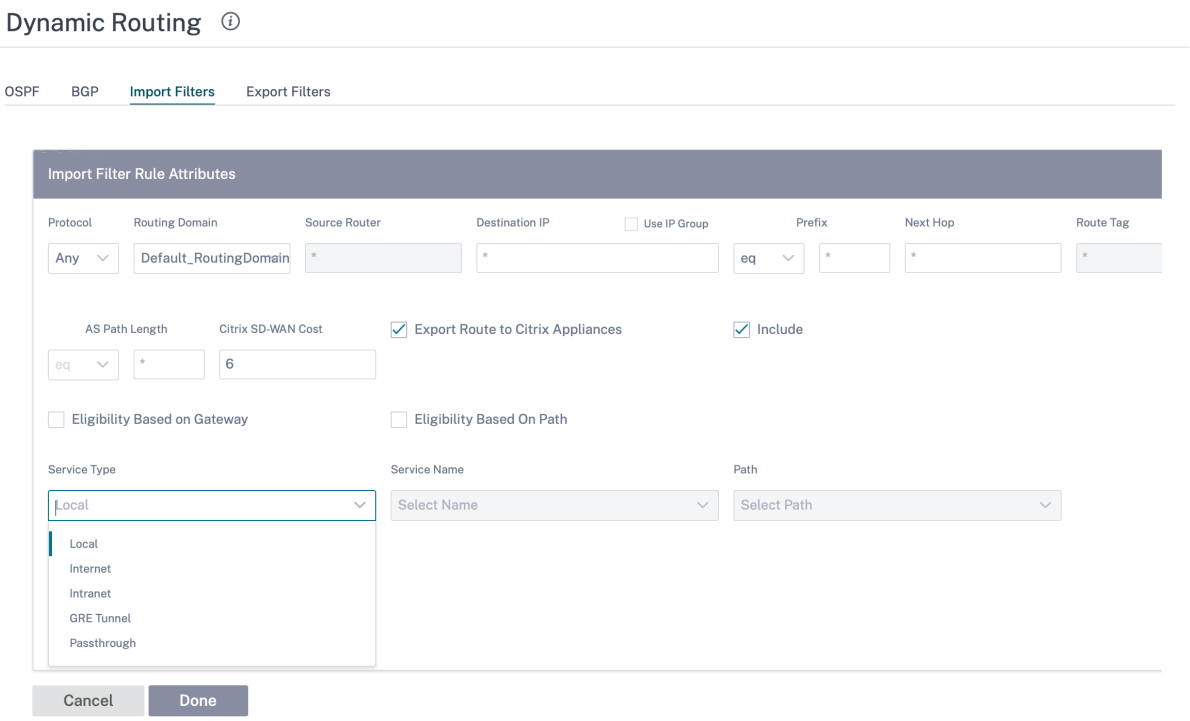
对于启用了路由学习的网络，Citrix SD-WAN Orchestrator 可以更好地控制向路由邻居通告哪些 SD-WAN 路由，以及从路由邻居接收哪些路由，而不是通告和接受全部或不接受路由。

导入过滤器

导入过滤器用于接受或不接受基于特定匹配条件使用 OSPF 和 BGP 邻居接收的路由。导入筛选规则是将动态路由导入 SD-WAN 路由数据库之前必须满足的规则。默认情况下不导入任何路由。

您可以配置过滤器来微调路由学习的进行方式。

单击 **+** 导入规则。



使用以下条件构建要创建的每个导出筛选器。

字段标准	说明	值
协议	用于获知路由的路由协议。从下拉列表中选择协议。	任意、OSPF、BGP
路由域	从下拉列表中输入路由域。	• 路由域名
源路由器	源路由器的 IP 地址，只适用于 iBGP	• IP 地址
目标 IP	路由目的地的 IP 地址和子网掩码	• IP 地址
使用 IP 组	根据需要选中“使用 **IP** 组”复选框。	-知识产权集团
前缀	要按前缀匹配路由，请从菜单中选择匹配谓词，然后在相邻字段中输入路由前缀	• eq: 等于,- LT: 小于,- LE: 小于或等于,- GT: 大于,- ge: 大于或等于
下一个跳	下一个跃点的 IP 地址	• IP 地址
路由标签	筛选器匹配的 OSPF 路由标记。OSPF 路由标签在 OSPF 和其他协议之间相互重新分配过程中防止路由循环	数值
成本	用于匹配导入 OSPF 路由的路由成本	数值
作为路径长度	用于匹配导入 BGP 路由的 AS 路径长度	数值

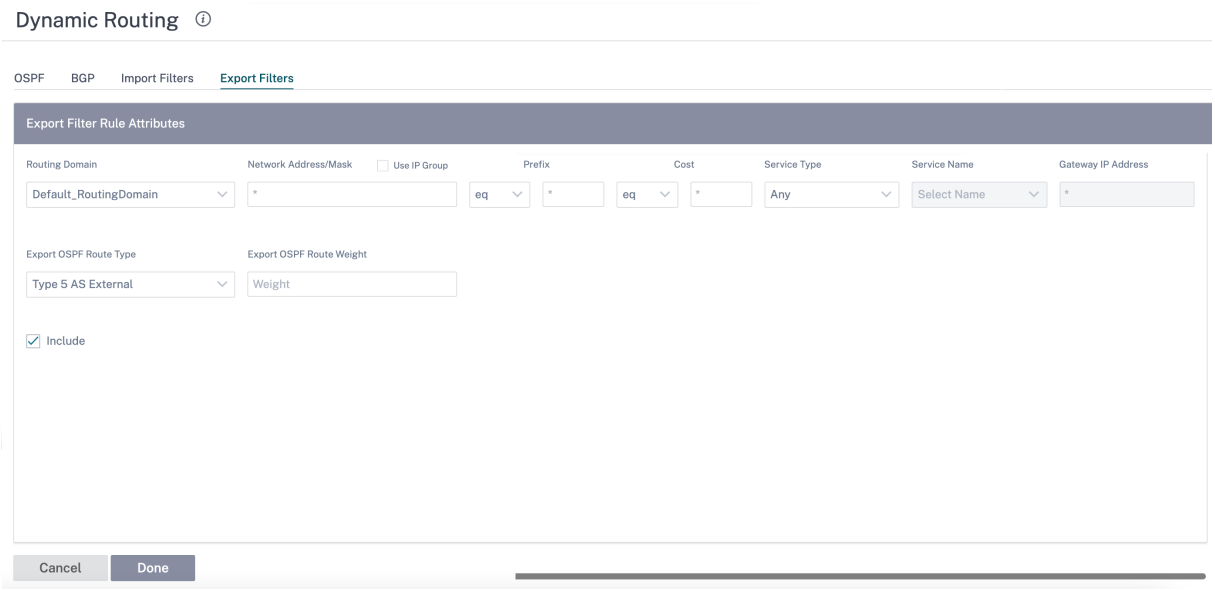
字段标准	说明	值
将路由导出到 Citrix 设备	选中复选框以启用此筛选器。否则，过滤器将被忽略	无
包括	选中 包括与此筛选器匹配的路径 复选框。否则匹配的路由将被忽略	无
基于网关的资格	选中此复选框并从下拉列表中提供 服务类型、服务名称和路径。	服务类型（本地、互联网、内联网、GRE 隧道、直通）、服务名称和路径
基于路径的资格	选中此复选框并从下拉列表中提供 服务类型、服务名称和路径。	服务类型（本地、互联网、内联网、GRE 隧道、直通）、服务名称和路径

单击“完成”保存设置。

导出过滤器

导出 筛选器 用于包含 或 排除 使用 OSPF 和 BGP 协议基于 特定 匹配的 播 发路由 标准。导出筛选规则是通过动态路由协议公布 SD-WAN 路由时必须遵守的规则。默认情况下，所有路由都会公布给同级。

单击 **+** 导出规则。



使用以下条件构建要创建的每个导出筛选器。

字段标准	说明	值
路由域	从下拉列表中选择路由域。	路由域

字段标准	说明	值
网络地址/掩码	输入描述路由网络的已配置网络对象的 **IP** 地址 和子网掩码	• IP 地址
使用 IP 组	如果需要，请选中该复选框并从下拉列表中输入 IP 组。	• IP 组
前缀	要按前缀匹配路由，请从菜单中选择匹配谓词，然后在相邻字段中输入路由前缀	• eq: 等于,- LT: 小于,- LE: 小于或等于,- GT: 大于,- ge: 大于或等于
成本	用于缩小导出路由选择范围的方法（谓词）和 SD-WAN 路由成本	数值
服务类型	从 Citrix SD-WAN 服务列表中选择分配给匹配路由的服务类型	任何、本地、虚拟路径、互联网、内联网、局域网 GRE 隧道、局域网 IPsec 隧道
站点/服务名称	对于 Intranet、LAN GRE 隧道和 LAN IPsec 隧道，请指定要使用的已配置的服务类型的名称	文本字符串
网关 IP 地址	如果您选择 LAN GRE 隧道作为服务类型，请输入隧道的 Gateway IP	IP 地址
导出 OSPF 路由类型	将 Citrix SD-WAN 路由作为类型 1 区域内路由或类型 5 外部路由通告给 OSPF 邻居。默认路由始终被通告为通向普通区域的类型 5 外部路由和通往末节区域的类型 3 汇总路由。	路径类型
导出 OSPF 路由权重	将 Citrix SD-WAN 路由导出到 OSPF 时，将每条路由的 Citrix SD-WAN 成本的权重作为总成本。	权重
包括	选中 包括与此筛选器匹配的路径 复选框。否则匹配的路由将被忽略	无

路由筛选在 SD-WAN 网络（数据中心/分支机构）中的 LAN 路由和虚拟路径路由上实现，并通过 BGP 和 OSPF 将路由通告到非 SD-WAN 网络。

您最多可以配置 512 个导出筛选器和 512 个导入筛选器。这是总体限制，而不是每个路由域限制。

网络地址转换

October 21, 2022

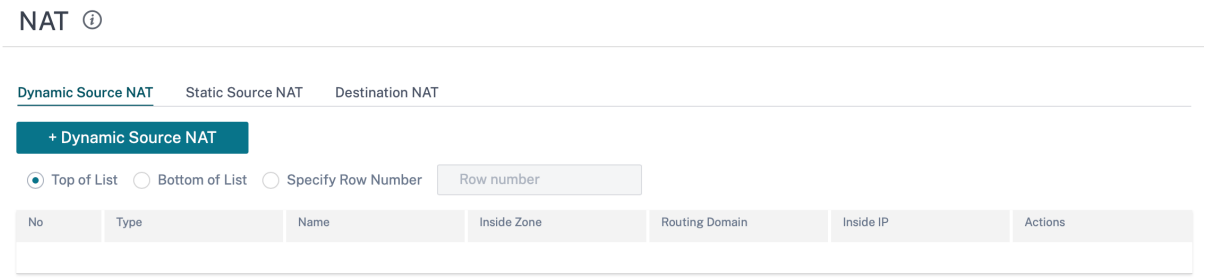
SD-WAN 设备上的网络地址转换 (NAT) 执行 IP 地址保存，以保留有限数量的注册 IP 地址。它将内部网络中的私有地址转换为合法的公共地址，并将您的私有 SD-WAN 网络与公共互联网连接起来。公有 IP 地址用于通过互联网进行通信。NAT 还通过将整个网络的一个地址广告到 Internet ，隐藏整个内部网络，从而确保额外的安全性。

您可以配置以下类型的 NAT：

- 动态源 NAT
- 静态 NAT
- 目标 NAT

> 注意：
>
> 只能在站点级别配置 NAT 功能。NAT 没有全局配置（模板）。

要使用 Citrix SD-WAN Orchestrator 服务为站点配置 NAT，请从站点级别导航到 配置 **>** 高级设置 **> NAT**。



入站和出站 **NAT**

连接的方向可以是内部到外部，也可以是外部到内部。创建 NAT 规则后，可以使用“接收 时”复选框定义方向。选中该复选框后，方向配置为 入站，清除该复选框后，方向配置为 出站。

- 入站：对于在服务上接收的数据包，将转换源地址。转换服务上传输的数据包的目的地址。例如，Internet 服务到局域网服务—对于接收的数据包（Internet 到局域网），将转换源 IP 地址。对于传输的数据包（LAN 到 Internet ），将转换目的 IP 地址。
- 出站：对于在服务上接收的数据包，将转换目标地址。对于在服务上传输的数据包，将转换源地址。例如，局域网服务到 Internet 服务—对于传输的数据包（局域网到 Internet ），将转换源 IP 地址。对于接收的数据包（Internet 到局域网），将转换目的 IP 地址。

区域派生

入站或出站流量的源防火墙区域和目标防火墙区域不得相同。如果源防火墙区域和目标防火墙区域相同，则不会对流量执行 NAT。

对于出站 NAT，外部区域将自动从服务派生。默认情况下，SD-WAN 上的每个服务都与一个区域相关联。例如，受信任的 Internet 链接上的 Internet 服务与受信任的 Internet 区域相关联。同样，对于入站 NAT，内部区域是从服务派生的。

对于虚拟路径服务 NAT 区域派生不会自动发生，您必须手动输入内部和外部区域。NAT 仅对属于这些区域的流量执行。无法为虚拟路径派生区域，因为虚拟路径子网中可能有多个区域。

动态源 **NAT**

动态源 **NAT** 是 SD-WAN 网络内部的私有 IP 地址或子网与 SD-WAN 网络之外的公有 IP 地址或子网的多对一映射。它允许多台主机的源 IP 地址转换为具有不同端口号的同一个公用 IP 地址。受端口限制的 NAT 使用相同的外部端口进行与内部 IP 地址和端口对相关的所有转换。来自不同区域和子网通过 LAN 段中受信任（内部）IP 地址的流量通过单个公有（外部）IP 地址发送。

> 注意：
>
> 动态 NAT 转换允许从内部网络发起的会话的所有互惠流量。要筛选这些连接，请为出站流量添加筛选策略。

端口地址转换

动态 NAT 执行端口地址转换 (PAT) 以及 IP 地址转换。端口号用于区分哪些流量属于哪个 IP 地址。所有内部私有 IP 地址均使用单个公有 IP 地址，但是为每个私有 IP 地址分配了不同的端口号。PAT 是一种经济高效的方式，允许多台主机使用单个公有 IP 地址连接到 Internet 。

对 称 复选框定义了 PAT 配置。配置 NAT 规则时，如果选中该复选框，则配置 Symmetric NAT，清除后，将在后端配置端口限制 NAT。

- 端口限制：端口受限 NAT 对与内部 IP 地址和端口对相关的所有转换使用同一个外部端口。此模式通常用于允许 Internet P2P 应用程序。
- 对称：对称 NAT 将同一个外部端口用于与内部 IP 地址、内部端口、外部 IP 地址和外部端口元组相关的所有转换。此模式通常用于增强安全性或扩展 NAT 会话的最大数量。

端口转发

带有端口转发功能的动态 NAT 允许来自外部网络的流量访问内部网络上的特定主机和端口，而无需从内部启动会话。这通常用于诸如 Web 服务器之类的主机内部。

配置动态 NAT 后，您可以定义端口转发策略。配置用于 IP 地址转换的动态 NAT，并定义端口转发策略以将外部端口映射到内部端口。动态 NAT 端口转发通常用于允许远程主机连接到专用网络上的主机或服务器。

配置动态源 **NAT**

要使用 Citrix SD-WAN Orchestrator 服务为站点配置动态 NAT，请从站点级别导航到 配置 **>** 高级设置 **> NAT >** 动态源 **NAT** 选项卡。单击 **+** 动态源 **NAT**。

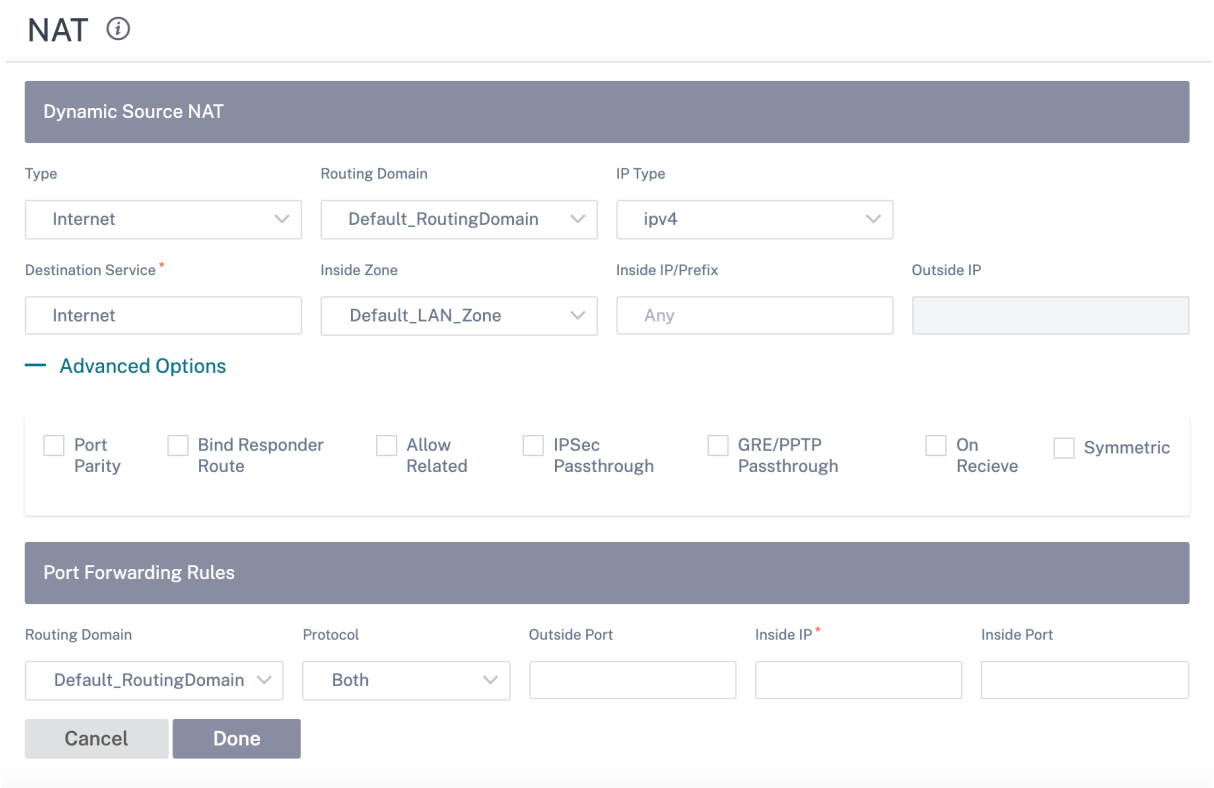
- 类型：应用 NAT 策略的 SD-WAN 服务类型。对于静态 NAT，支持的服务类型为本地、虚拟路径、Internet、Intranet 和路由间域服务。
- 路由域：选择所选转换适用的路由域。
- **IP** 地址类型：根据您的喜好选择 IPv4 或 IPv6 地址类型。
- 目标服务：提供与服务类型对应的服务名称。
- 内部区域：数据包必须来自的内防火墙区域匹配类型才能进行转换。
- 内部 **IP/**前缀：满足匹配标准时必须转换为的内部 IP 地址和前缀。
- 外部 **IP**：满足匹配标准时内部 IP 地址转换为的外部 IP 地址和前缀。对于使用 Internet 和内部网服务的出站流量，已配置的 WAN 链路 IP 地址将动态选择为外部 IP 地址。
- 端口奇偶校验：如果启用，NAT 连接的外部端口将保持奇偶校验（即使内部端口是偶数，如果外部端口为奇数，则为奇数）。
- 绑定响应器路由：确保通过与接收响应流量相同的服务发送响应流量，以避免非对称路由。
- 允许相关：允许与匹配规则的流量相关的流量。例如，如果存在与该策略相关的某种类型的错误，则 ICMP 重定向与该策略匹配的特定流相关。
- **IPsec** 直通：允许转换 IPsec (AH/ESP) 会话。
- **GRE/PPTP** 直通：确保响应流量通过与接收流量相同的服务发送，以避免非对称路由。
- 接收时：选中此复选框后，将配置入站 NAT。清除后，将配置出站 NAT。
- 对称：选中此复选框后，将配置对称 NAT。清除后，配置受端口限制的 NAT。

端口转发规则：

- 路由域：选择所选转换适用的路由域。
- 协议：TCP、UDP 或两者兼而有。
- 外部端口：转发到内部端口的外部端口。
- 内部 **IP**：用于转发匹配数据包的内部地址。
- 内端口：外部端口将被转发到的内部端口。

每个端口转发规则都有一个父 NAT 规则。外部 IP 地址取自父 NAT 规则。

> 注意
>
> 满足以下条件时，Citrix SD-WAN Orchestrator 服务用户界面会显示自动创建的 NAT 规则：
>
> - 该站点已启用互联网服务。
> - 站点上未配置 IPv4 出站互联网动态源 NAT 规则。
> - 至少 1 个 WAN 链路位于不可信接口上，或者在所有路由域上启用了 Internet。



静态源 **NAT**

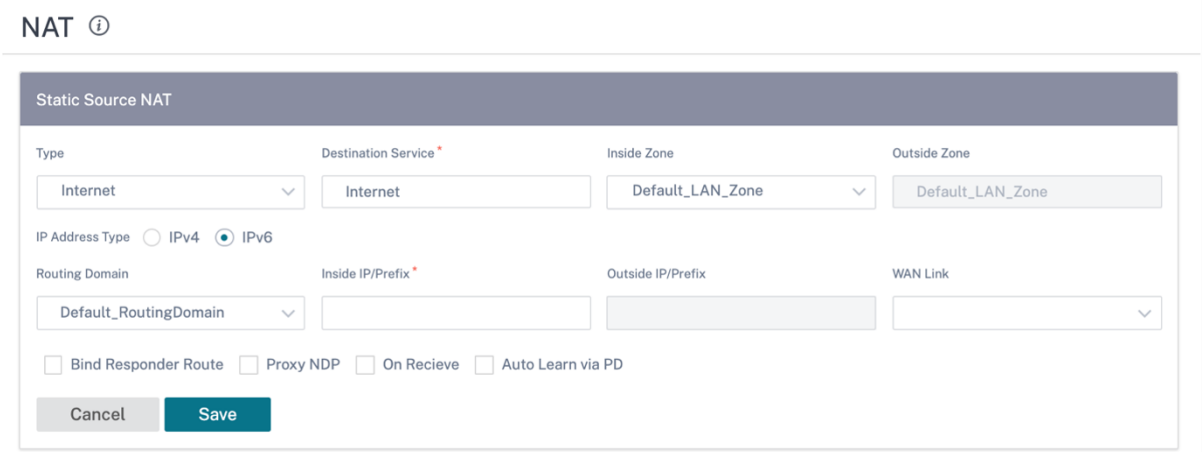
静态 NAT 是 SD-WAN 网络内部的私有 IP 地址或子网到 SD-WAN 网络外部的公有 IP 地址或子网的一对一映射。通过手动输入内部 IP 地址和必须转换到的外部 IP 地址来配置静态 NAT。您可以为本地、虚拟路径、Internet、内部网和路由间域服务配置静态 NAT。

配置静态源 **NAT**

要使用 Citrix SD-WAN Orchestrator 服务为站点配置静态 NAT，请从站点级别导航到 配置 **>** 高级设置 **> NAT >** 静态源 **NAT** 选项卡。单击 **+** 静态源 **NAT**。

- 类型：应用 NAT 策略的 SD-WAN 服务类型。对于静态 NAT，支持的服务类型包括本地、虚拟路径、Internet、Intranet 和路由间域服务
- 目标服务：提供与服务类型对应的服务名称。
- 内部区域：数据包必须来自的内防火墙区域匹配类型才能进行转换。
- 外部区域：数据包必须来自的外部防火墙区域匹配类型才能进行转换。
- **IP** 地址类型：根据您的喜好选择 IPv4 或 IPv6 地址类型。
- 路由域：选择所选转换适用的路由域。
- 内部 **IP/**前缀：满足匹配标准时必须转换为的内部 IP 地址和前缀。
- 外部 **IP/**前缀：满足匹配条件时内部 IP 地址转换为的外部 IP 地址和前缀。

- 绑定响应器路由：确保通过与接收响应流量相同的服务发送响应流量，以避免非对称路由。
- 代理 **ARP**：确保设备响应外部 IP 地址的本地 ARP 请求。
- 代理 **NDP**：确保设备响应本地 NDP 对外部 IP 地址的请求。
- 接收时：选中此复选框后，将配置入站 NAT。清除后，将配置出站 NAT。
- 通过 **PD** 自动学习：只有在选择 IPv6 作为 **IP** 地址类型时，此复选框才会启用。选中后，Citrix SD-WAN 会从上游委托路由器请求前缀，委托路由器会向 Citrix SD-WAN 发送前缀进行响应。



IPv6 Internet 服务的静态 **NAT** 策略

从版本 11.4.0 起，Citrix SD-WAN 支持 IPv6 互联网服务的静态 NAT 策略。IPv6 Internet 服务的静态 NAT 策略指定将内部网络前缀映射到外部网络前缀。所需的静态 NAT 策略的数量取决于内部网络的数量和外部网络（WAN 链路）的数量。如果有 **M** 个内部网络和 **N** 个 WAN 链路，则所需的静态 NAT 策略数为 **M x N**。

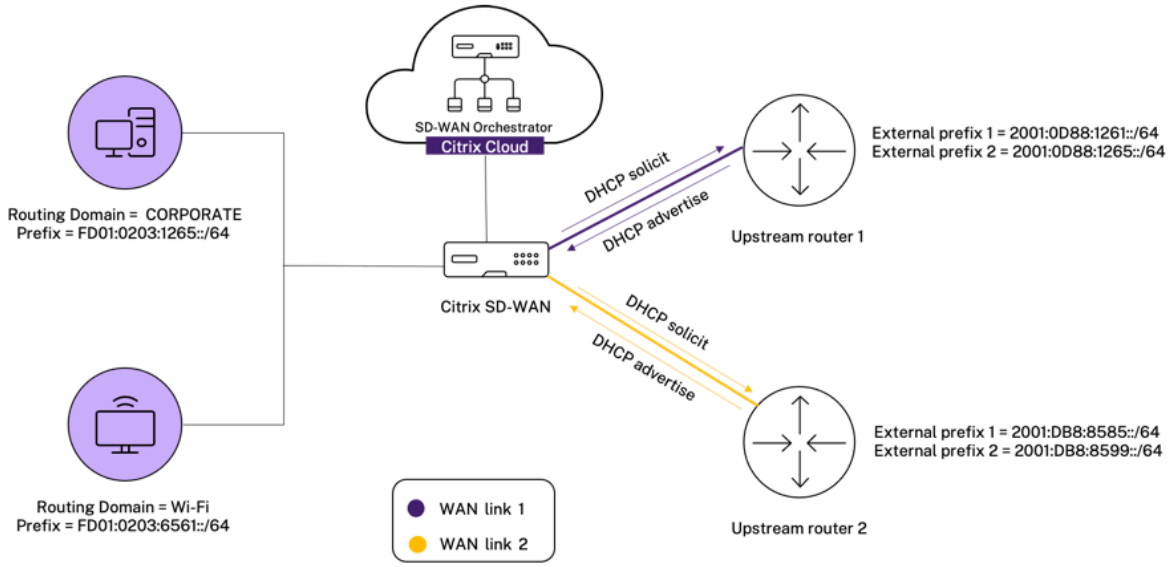
从 Citrix SD-WAN 版本 11.4.0 起，在创建静态 NAT 策略时，您可以手动输入外部 IP 地址，也可以 通过 **PD** 启用 **Auto Le**arn。启用 **Auto Learn via PD** 后，SD-WAN 设备通过 DHCPv6 前缀委派接收来自上游委派路由器的委托前缀。在 Citrix SD-WAN 11.4.0 版之前，外部 IP 地址是自动从服务派生的，因此无法选择手动输入外部 IP 地址。如果要将设备升级到 11.4.0 或更高版本，并且为 IPv6 Internet 服务配置了静态 NAT 策略，则必须手动更新这些策略。

配置示例

在以下拓扑中，Citrix SD-WAN 设备配置有 2 个内部网络和 2 个 WAN 链接：

- 内部网络 1 驻留在具有网络前缀 FD01:0203:6561::/64 的企业路由域中
- 内部网络 2 驻留在 Wi-Fi 路由域中，网络前缀为 FD01:0203:1265::/64
- 通过 WAN Link 1，SD-WAN 设备通过 DHCPv6 前缀委派、2 个委派前缀 2001:0D88:1261::/64 和 2001:0D88:1265::/64 从上游委派路由器接收。当来自内部网络的流量通过 WAN link 1 时，这两个委派的前缀将用作外部网络前缀。

- 通过 WAN Link 2，SD-WAN 设备通过 DHCPv6 前缀委派、2 个委派前缀 2001:DB8:8585::/64 和 2001:DB8:8599::/64 从上游委派路由器接收。当来自内部网络的流量通过 WAN link 2 时，这两个委派的前缀用作外部网络前缀。



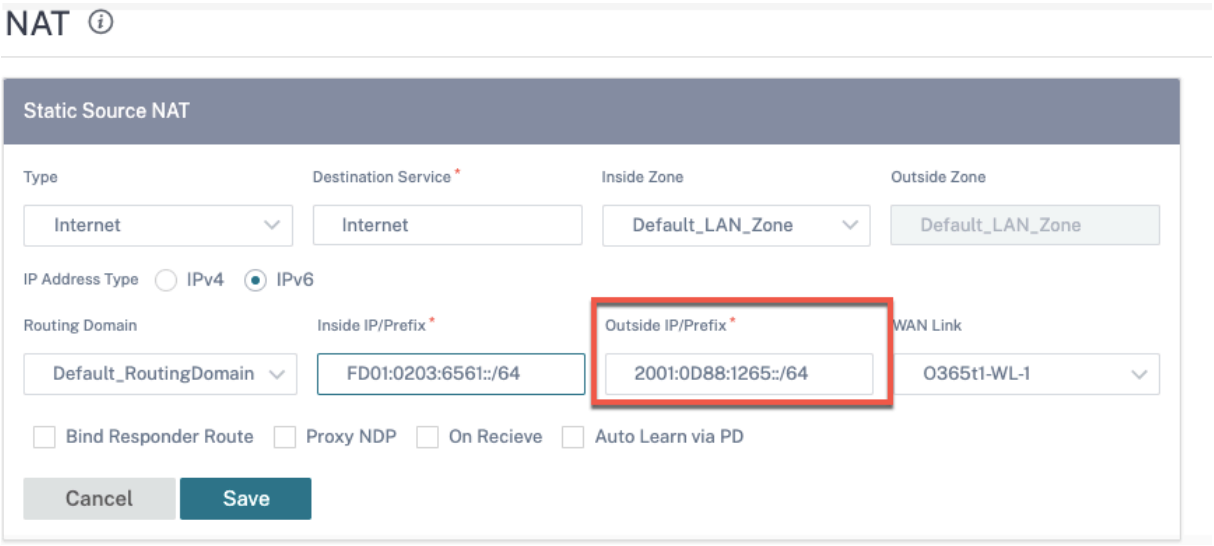
在这种情况下，网络内有 M=2 和 N = 2 WAN 链路。因此，正确部署 IPv6 互联网服务所需的静态 NAT 策略的数量为 2 x 2 = 4。这 4 个静态 NAT 策略为以下各项指定了地址转换：

- 通过 WAN 链路 1 在网络 1 内部
- 在网络 1 内部通过 WAN 链路 2
- 通过 WAN 链路 1 在网络 2 内部
- 通过 WAN 链路 2 在网络 2 内部

要配置这些静态 NAT 策略，请从站点级别导航到 配置 **>** 高级设置 **> NAT >** 静态源 **NAT**。单击 **+** 静态源 **NAT**。

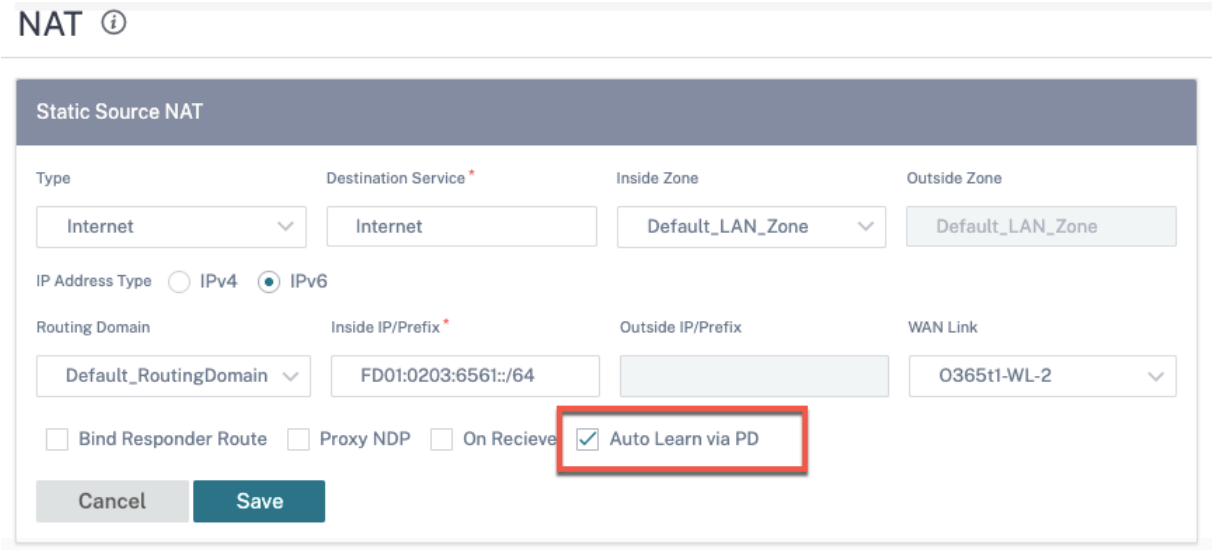
创建 NAT 策略时，请确保将“类型”选为 **Internet** ，将 **IP** 地址类型 选为 **IPv6**。选择 WAN 链接，然后在 **Inside IP/Prefix** 字段中输入内部网络前缀（仅允许使用 /64 前缀）。在 Outside **IP/Prefix** 字段中，您可以手动输入外部网络前缀或选中“通过 **PD** 自动学习”复选框。

以下是在静态 NAT 策略中手动输入外部 IP 地址的示例。



如果选中“通过 **PD** 自动学习”复选框，请确保上游路由器支持 DHCPv6 前缀委派。Citrix SD-WAN 向上游委派路由器请求前缀，委派路由器会向 Citrix SD-WAN 使用前缀进行响应。Citrix SD-WAN 使用此委派前缀将内部 IP 地址转换为外部 IP 地址。

以下是启用 了通过 **PD** 自动学习 的示例，以便通过 DHCPv6 前缀委派获取外部网络前缀。



目标 **NAT**

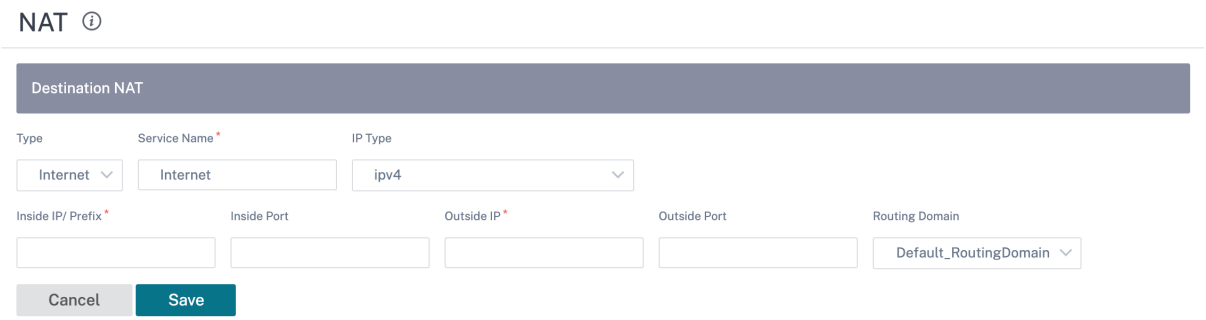
目标 NAT 策略允许在单个主机或子网之间配置网络地址转换策略。

> 注意
>
> - 虽然可以同时为服务配置入站和出站转换，但只会使用第一个匹配的翻译。如果在接收数据包的服务上存在规则，而发送数据包的服务上存在规则，则可能会发生多次转换。

- 目标 NAT 转换仅适用于源自本地服务的流量。

要配置这些目标 NAT 策略，请从站点级别导航到 配置 **>** 高级设置 **> NAT >** 目标 **NAT**。单击 **+** 目标 **NAT**。

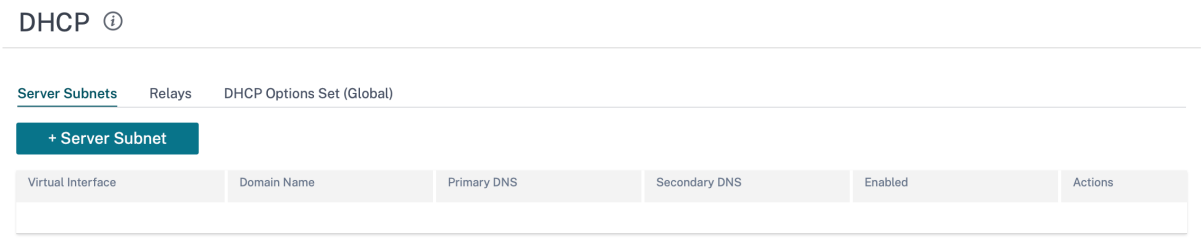
- 类型：应用 NAT 策略的 SD-WAN 服务类型。对于静态 NAT，支持的服务类型包括本地、虚拟路径、Internet、Intranet 和路由间域服务
- 服务名称：提供与服务类型对应的服务名称。
- **IP** 类型：根据您的喜好选择 IPv4 或 IPv6 地址类型。
- 内端口：外部端口将被转发到的内部端口。
- 外部 **IP**：满足匹配标准时内部 IP 地址转换为的外部 IP 地址和前缀。对于使用 Internet 和内部网服务的出站流量，已配置的 WAN 链路 IP 地址将动态选择为外部 IP 地址。
- 外部端口：转发到内部端口的外部端口。
- 路由域：选择所选转换适用的路由域。
- 接收时：选中此复选框后，将配置入站 NAT。清除后，将配置出站 NAT。



动态主机配置协议

October 21, 2022

您可以将 SD-WAN 设备配置为 D **HCP** 服务器 或 DH **CP** 中继代理。DHCP 服务器功能允许与 SD-WAN 设备的 LAN/WAN 接口位于同一网络中的设备从 SD-WAN 设备获取其 IP 配置。通过 DHCP 中继功能，您的 SD-WAN 设备可以在 DHCP 客户端与服务器之间转发 DHCP 数据包。



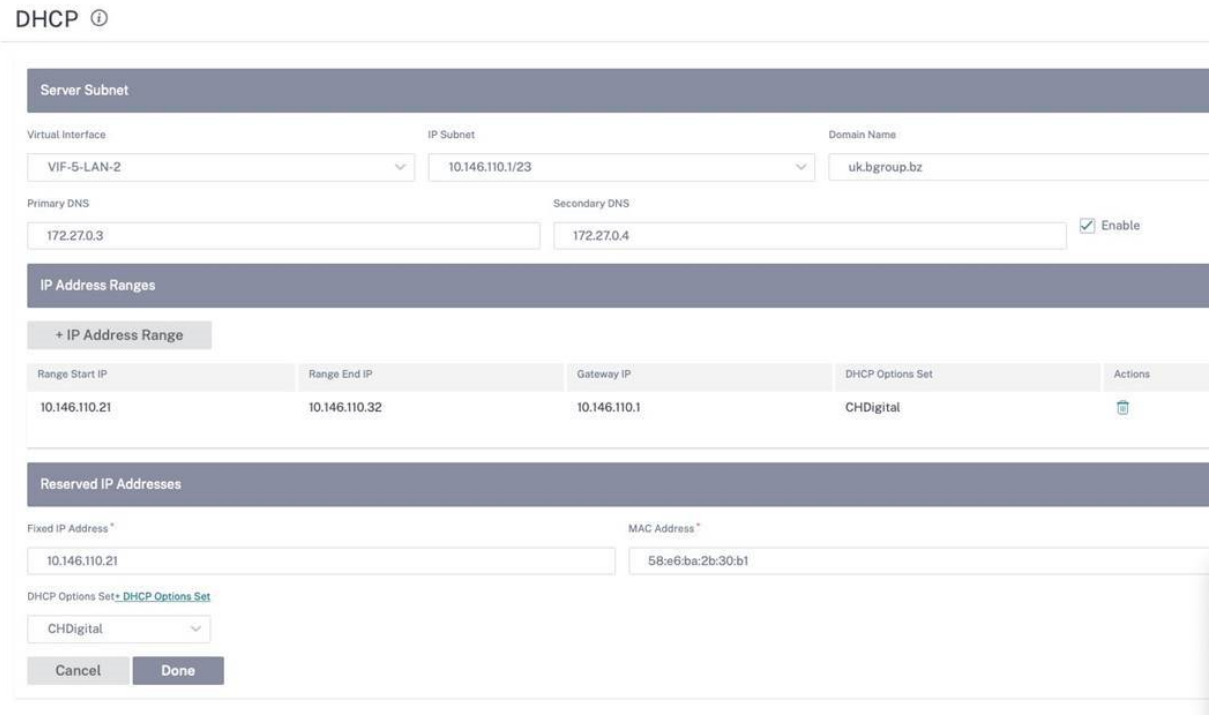
DHCP 服务器

Citrix SD-WAN 设备可以配置为 DHCP 服务器。它可以将网络内指定地址池中的 IP 地址分配和管理给 DHCP 客户端。

可以将 DHCP 服务器配置为分配其他参数，例如 DNS IP 地址和默认网关。DHCP 服务器接受地址分配请求和续订。DHCP 服务器还接受来自本地连接的 LAN 段或网络中其他 DHCP 中继代理所转发的 DHCP 请求的广播。

要配置 DHCP 服务器，请在“站点配置”页面中，从站点级别导航到 配置 **>** 高级设置 **> DHCP >** 服务器子网 > 单击 **+** 服务器子网。

选择用于 接收 **DHCP** 请求的虚拟接口。DHCP 服务器向其提供 IP 地址的 IP 子网是自动填充的。



输入 域名、主 **DNS** 和 辅助 **DNS**。DHCP 服务器将此信息转发给 DHCP 客户机。

配置用于向客户端分配 IP 地址的动态 IP 地址池。指定起始和结束 IP 地址范围，然后选择 **DHCP** 选项集。

> 注意
>
> DHCP 选项集是一组 DHCP 设置，可以应用于单个 IP 地址范围。有关更多信息，请参阅 DHCP 选项集。

通过将需要固定 IP 地址的各个主机映射到其 MAC 地址来设置保留的 IP 地址。输入 固定 **IP** 地址、**MAC** 地址，然后选择 **DHCP** 选项集。

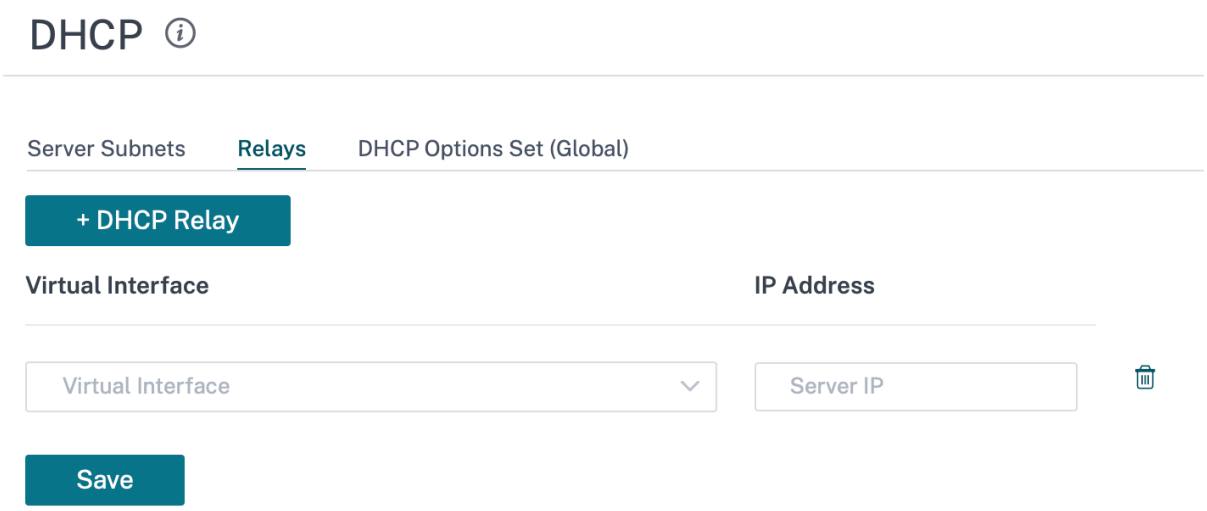
> 注意
>
> 对于保留的 IP 地址，网关 **IP** 是通过在 **DHCP** 选项集中配置路由器选项来设置的。

DHCP 中继

Citrix SD-WAN 设备可以配置为 DHCP 中继。它在本地 DHCP 客户端和远程 DHCP 服务器之间中继 DHCP 请求和回复。

它允许本地主机从远程 DHCP 服务器获取动态 IP 地址。中继代理接收 DHCP 消息并生成要在另一个接口上发出的新 DHCP 消息。

要配置 DHCP 服务器，请在“站点配置”页面中导航到 配置 **>** 高级设置 **> DHCP >** 中继 单击 **+ DHCP** 中继。



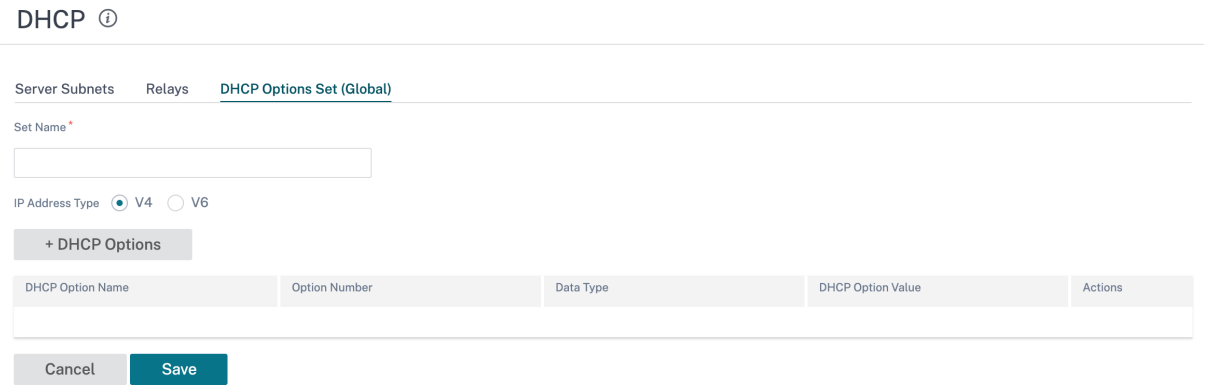
选择与远程 DHCP 服务器通信的 虚拟接口。输入中继用于转发来自客户端的请求和响应的 **DHCP** 服务器 **IP** 。

您可以使用通用虚拟网络接口配置单个 **DHCP** 中继 并将其指向多个 DHCP 服务器。

DHCP 选项集

DHCP 选项是一组 DHCP 配置，可应用于单个 IP 地址范围或单个主机。

为 DHCP 选项配置文件设置名称并选择 **IP** 地址类型。单击 **+ DHCP** 选项集，然后从列表中选择一个 DHCP 选项名称。选项号是预先配置的。对于自定义选项，范围为 224—254。选择 数据类型 并为该选项输入 值。



通过 **DHCP** 客户端进行 **WAN** 链接 **IP** 地址学习

Citrix SD-WAN 设备支持通过 DHCP 客户端进行 WAN 链接 IP 地址学习。此功能减少了部署 SD-WAN 设备所需的手动配置量，并通过无需购买静态 IP 地址来降低 ISP 成本。SD-WAN 装置可以获取不受信任接口上 WAN 链路的动态 IP 地址。这样就不需要中间 WAN 路由器来执行此功能。

> 备注
>
> - DHCP 客户端只能配置为客户端节点的不受信任的非桥接接口。
> - 只有配置了公共 IP 地址，才能在 MCN/RCN 上启用 DHCP 客户端和数据端口。
> - 具有 DHCP 客户端配置的站点上不支持单臂或基于策略的路由 (PBR) 部署。
> - DHCP 事件仅从客户端的角度记录，不会生成 DHCP 服务器日志。

有关在“故障到块”模式和“故障到线”模式下为不可信虚拟接口配置 DHCP 的信息，请参阅 站点级配置。

多播路由

October 21, 2022

组播路由实现了一对多流量的高效分配。多播源，将单个流中的多播流量发送到多播组。多播组包含使用 IGMP 协议进行多播通信的主机和相邻路由器等接收器。IP 语音、视频点播、IP 电视和视频会议是使用多播路由的一些常见技术。在 Citrix SD-WAN 设备上启用多播路由时，该设备将充当多播路由器。

源特定组播

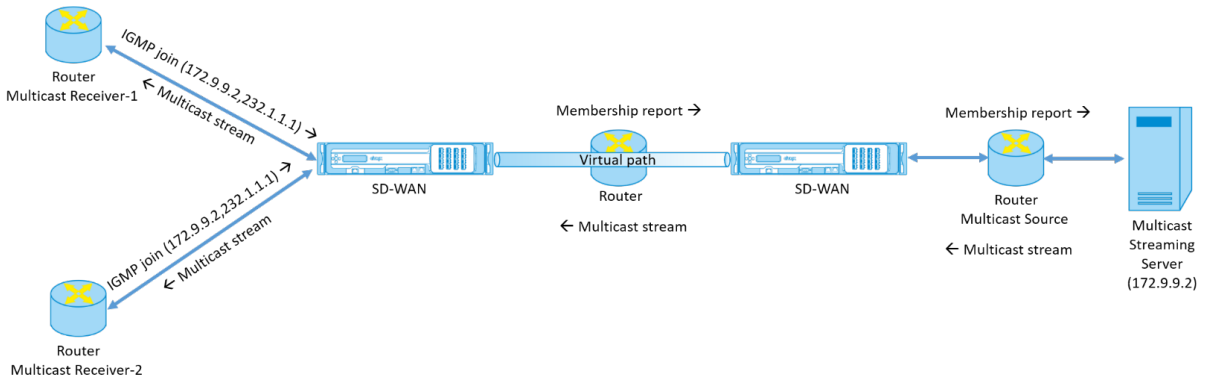
多播协议通常允许多播接收机接收来自任何源的多播通信。

使用源特定组播 (SSM)，您可以指定接收方接收组播流量的源。它确保接收机不是每个发送多播流的源的侦听器，而是侦听特定多播源。

SSM 降低了消耗来自各种可能来源的流量所使用的资源成本。SSM 还通过确保接收方接收来自已知发送者的流量来提供一层安全保护。

以下拓扑显示了一个分支站点上的两个多播接收器和数据中心的一个组播服务器 (172.9.9.2)。多播服务器通过特定组 (232.1.1.1) 流式传输流量，接收机加入组。多播组上传送的任何流量都将中继到加入该组的所有接收机。

> 注意
>
> 要使 SSM 工作，组播组 IP 必须在 232.0.0.0/8 范围内。



1. 多播接收机发送 IP IGMP 加入请求，指示接收机希望加入多播组并希望从源接收多播流。

   IGMP 连接包括 2 个属性，即组播源和组（S, G）。IGMP 版本 3 用于组播源上的 SSM 和接收器中继一些包含特定源地址。

   SSM 允许接收方显式接收来自特定组播服务器的流，接收方在 JOIN 请求中明确提供了其源地址。在此示例中，通过显式包含源 172.9.9.2 来触发 IGMP v3 联接请求，该列表包含源 172.9.9.2，该列表是通过组 232.1.1.1 发送多播流的地址。

2. 分支机构的 Citrix SD-WAN 侦听来自这些接收机的所有 IGMP 请求，并将其转换为成员资格报告，然后通过虚拟路径将其发送到数据中心的 SD-WAN 设备。
3. 数据中心的 Citrix SD-WAN 设备通过虚拟路径接收成员资格报告并将其转发到多播源，从而建立控制通道。
4. 多播源通过虚拟路径将多播流传输到多播接收机。

控制通道流量和多播流经过分支机构和数据中心之间已建立的虚拟路径。Citrix SD-WAN 叠加路径可确保和隔离多播流量免受 WAN 降级或链路变化的影响。

多播配置

要配置多播，请在 SD-WAN Orchestrator 服务上同时在源和目标处执行以下操作。

1. 创建多播组-为多播组提供名称和 IP 地址。对于源特定的多播，组播组 IP 必须在 232.0.0.0/8 范围内。
2. 启用 IGMP 代理—您可以将 Citrix SD-WAN 设备配置为 IGMP/MLD 代理，以携带 IGMP 控制通道信息进行多播路由。
3. 定义上游和下游服务-上游接口使 IGMP 代理能够连接到更接近实际多播源的 SD-WAN 设备，以流式传输流量。下游接口使 IGMP 代理能够连接到远离流通信量的实际多播源的主机。
   源设备和目标设备的上游和下游服务不同。

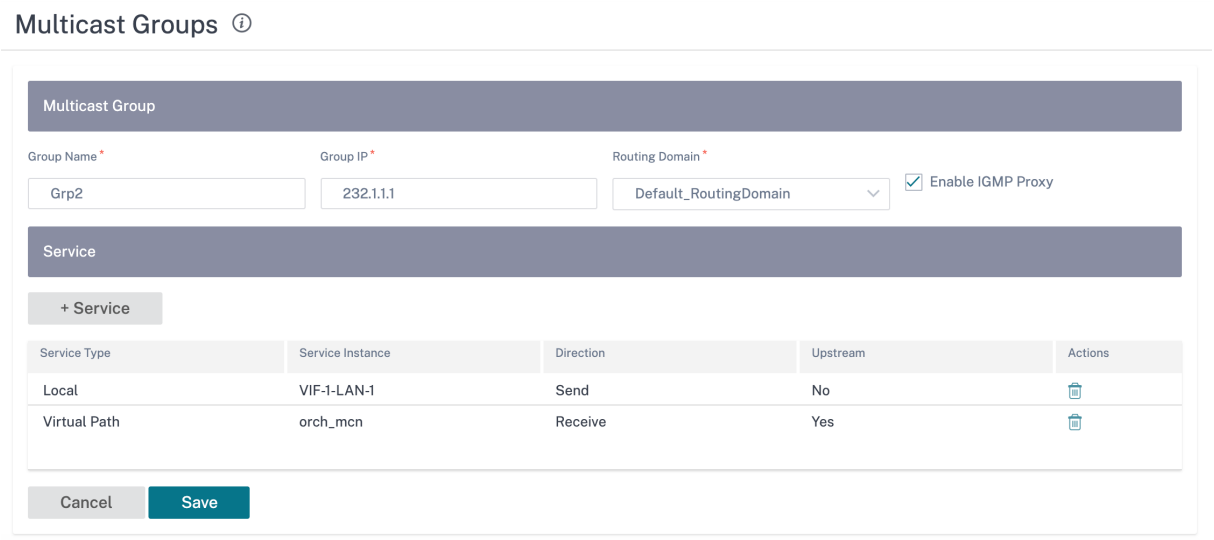
> 注意：
>
> 将 Branch 或 MCN 配置为上游后，也需要将其配置为其他组的上游。

要配置多播，请在站点级别导航到 配置 > 高级设置 > 多播组。通过为多点传送组提供名称和 IP 地址（IPv4 或 IPv6）来创建多点传送组。单击 启用 **IGMP** 代理。

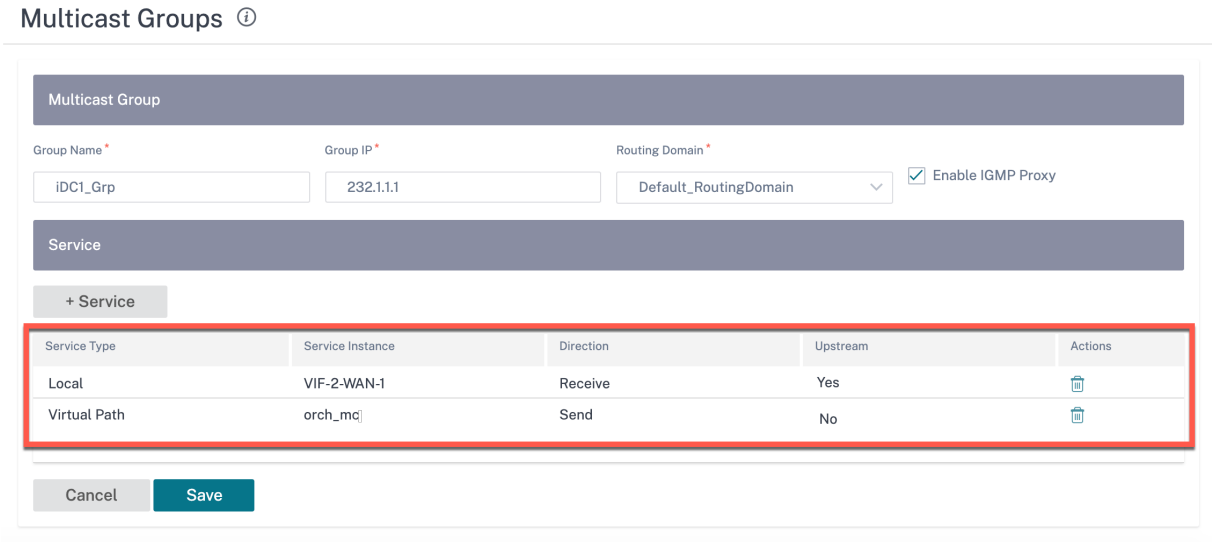
配置分支机构和数据中心设备的上游和下游路径。

对于靠近多播接收器（分支）的设备，设备会在虚拟路径接口上接收组播流量，并将本地接口上的流量发送到接收方。

> 注意：
>
> - 将多播源配置为 Intranet 服务时，多播流的源 IP 必须具有映射到 Intranet 服务的路由。
> - 确保创建相应的防火墙策略以允许 SD-WAN 设备上的多播流量。



对于靠近多播源（数据中心）的设备，设备将在本地接口上接收组播流量，然后在虚拟路径接口上发送流量。

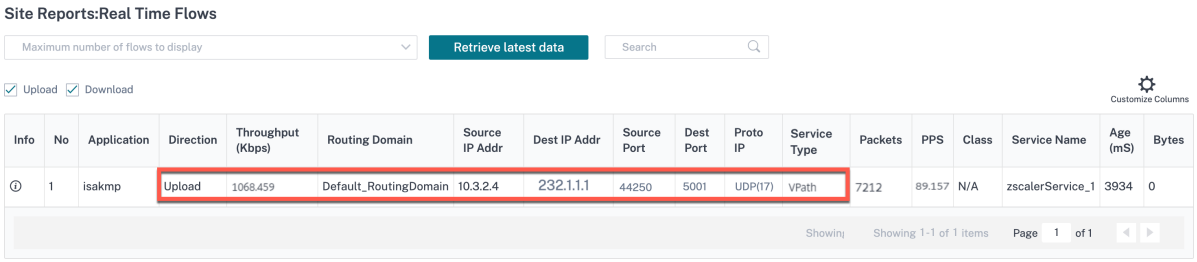


监视

流量统计

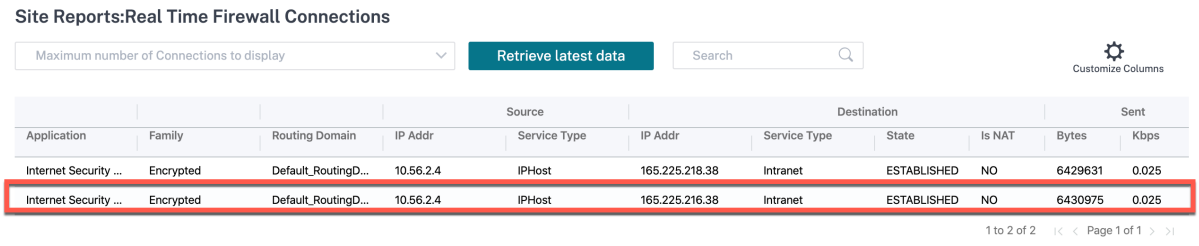
组播控制通道建立并且组播源开始流式传输后，您可以查看组播流统计信息。您可以看到多播 UDP 流量是在虚拟路径服务上从接收方发送到组播组 232.1.1.1。

> 注意：
>
> 如果 SSM 已启用，并且如果从不属于预期的源发送方列表的其他服务器接收流量，SD-WAN 设备将不会有任何报告数据。



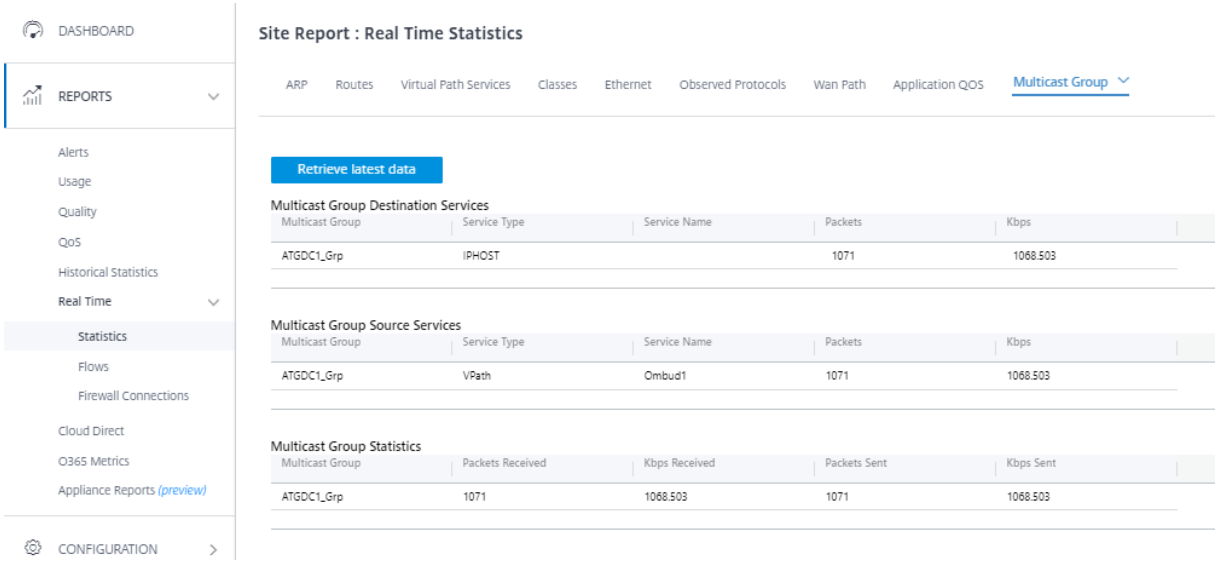
防火墙统计信息

防火墙表显示通过多播组 IP 地址经 LAN 接口并通过虚拟路径发送的多播流量。



多播组统计

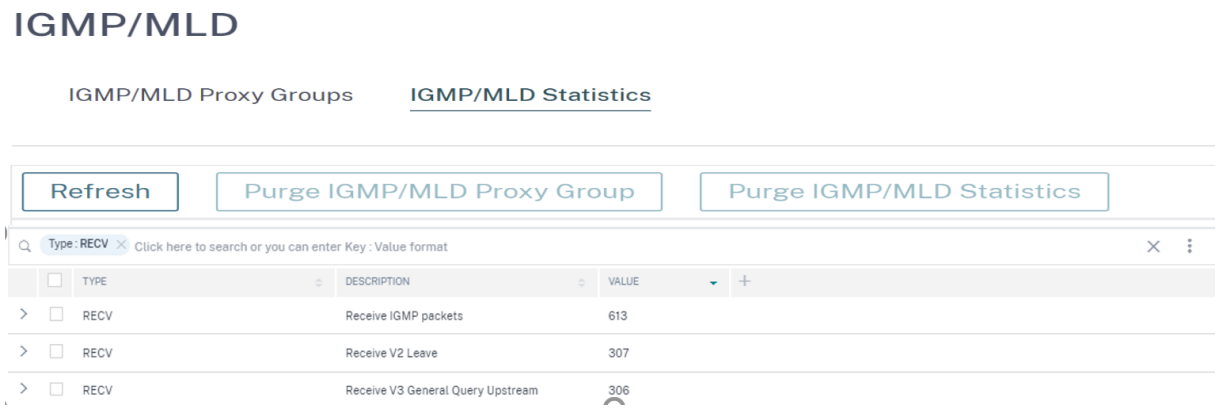
组播组表提供了有关多播流量的详细信息，例如通过源、目标发送和接收的数据包以及两者的聚合。



IGMP/MLD

当多播接收方发起加入组请求时，您可以在 报告 > 实时 > IGMP/MLD > **IGMP/MLD** 统计下查看接收方详细信息。您可以在源和目标处看到此信息。单击刷新 以获取当前数据。

下图显示接收的 IGMP/MLD 数据包和过滤器类型 RECV 用于包括 IGMP/MLD 接收数据包。



要查看 IGMP 代理组的详细信息，请导航到 报告 > 实时 > **IGMP/MLD** > **IGMP/MLD** 代理组。单击 刷新 以获取当前数据。

选择“清除 **IGMP/MLD** 统计信息”以清除 IGMP 统计数据表中的 IGMP 统计数据。

选择“清除 **IGMP/MLD** 组”以清除 IGMP 组表中的 IGMP 组数据。

虚拟路由器冗余协议

October 21, 2022

虚拟路由器冗余协议 (VRRP) 是一种广泛使用的协议，它提供设备冗余以消除静态默认路由环境中固有的单点故障。

通过 VRRP，您可以配置两个或更多个路由器以形成一个组。此组显示为具有一个虚拟 IP 地址和一个虚拟 MAC 地址的单个默认网关。

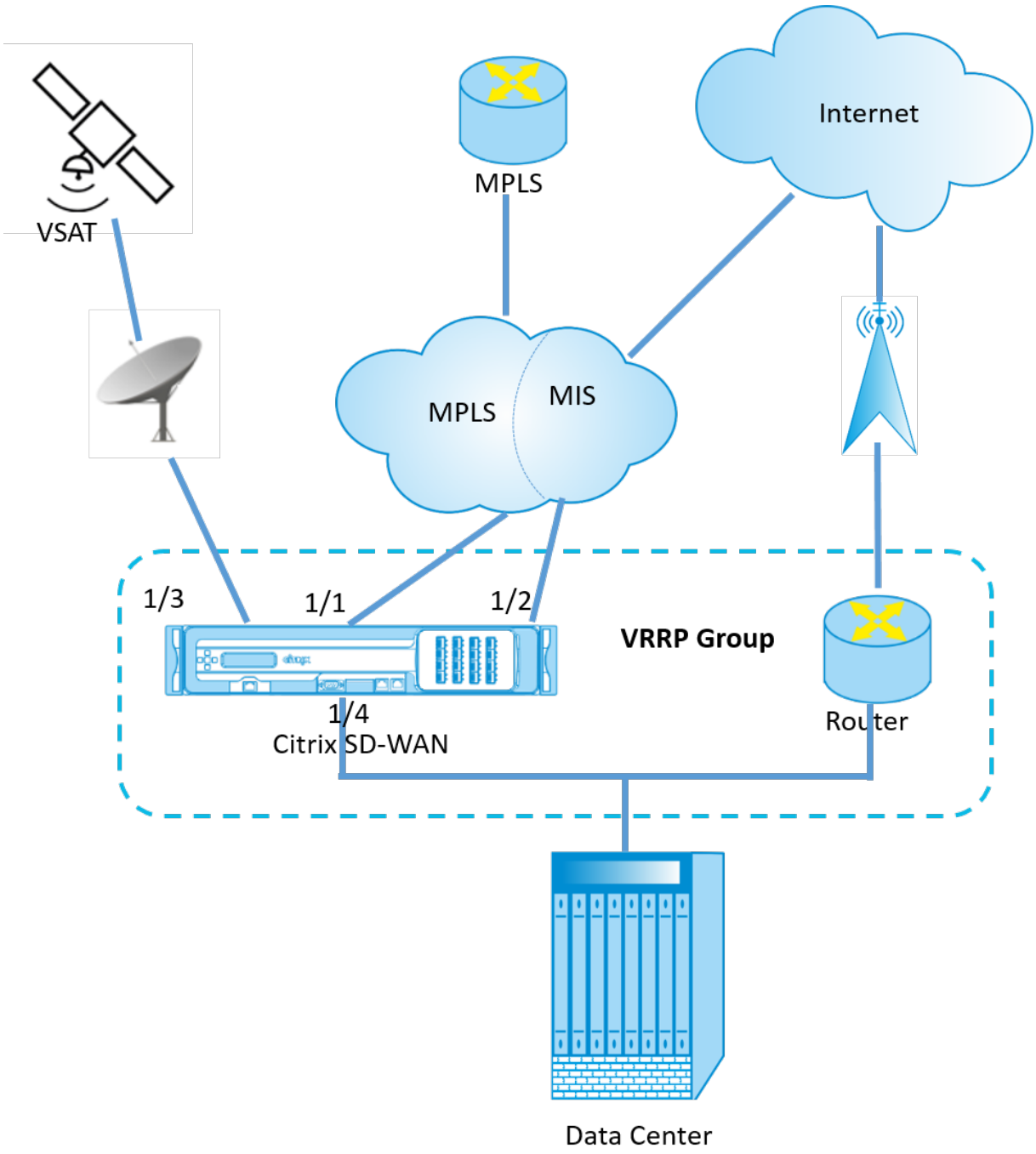
如果主/主路由器出现故障，备用路由器会自动接管。在 VRRP 设置中，主路由器向备用路由器发送一个称为通告的 VRRP 数据包。当主路由器停止发送通告时，备用路由器会设置间隔计时器。如果在此保留期内没有收到任何通告，则备用路由器启动故障切换例程。

VRRP 指定了一个选举过程，在该过程中，优先级最高的路由器成为主路由器。如果路由器之间的优先级相同，则具有最高 IP 地址的路由器将成为主路由器。其他路由器处于备份状态。如果主路由器出现故障、新路由器加入群组或现有路由器退出群组，则选举过程将再次启动。

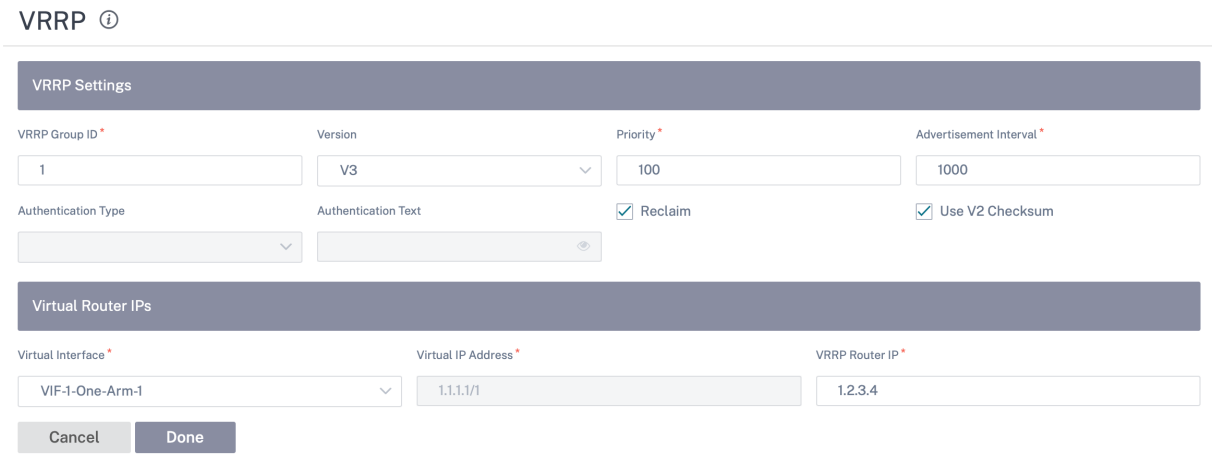
VRRP 可确保高可用性默认路径，而无需在每个终端主机上配置动态路由或路由器发现协议。

Citrix SD-WAN 版本 10.1 支持 VRP 版本 2 和版本 3 与任何第三方路由器互操作。Citrix SD-WAN 发行版 11.5 支持版本 6。SD-WAN 设备充当主路由器，引导流量在站点之间使用虚拟路径服务。您可以将 SD-WAN 设备配置为 VRRP 主路由器，方法是将虚拟接口 IP 配置为 VRRP IP，然后手动将优先级设置为高于对等路由器的值。您可以配置播发间隔和抢占选项。

下面的网络图显示了 Citrix SD-WAN 设备和配置为 VRRP 组的路由器。SD-WAN 设备配置为主路由器。如果 SD-WAN 设备出现故障，备份路由器将在毫秒内接管，以确保没有停机时间。



要配置 VRRP，请在“站点配置”页面中导航到 配置 > 高级设置 > **VRRP** > 单击 **+** 添加 **VRRP**。



您可以编辑以下成员路径参数：

- **VRRP** 组 **ID**：VRRP 组 ID。组 ID 的值范围必须为 1—255。备份路由器上也必须配置相同的组 ID。
- 版本：VRRP 协议版本。可以在 VRRP 协议 V2 和 V3 之间进行选择。
- 优先级：VRRP 组的 Citrix SD-WAN 设备的优先级。优先级范围为 1–254。将此值设置为最大值 (254)，使 SD-WAN 设备成为主路由器。

  > 注意
  >
  > 如果路由器是 VRRP IP 地址的所有者，则默认情况下，优先级设置为 255。

- 通告间隔：当 SD-WAN 设备是主路由器时发送 VRRP 通告的频率（以毫秒为单位）。默认公告时间间隔为 1 秒。
- 身份验证类型：您可以选择 纯文本 来输入身份验证字符串。身份验证字符串以纯文本格式发送，在 VRRP 公告中不进行任何加密。如果不想设置身份验证，请选择“无”。
- 身份验证文本：要在 VRRP 通告中发送的身份验证字符串。如果 身份验证类型 为 纯文本，则启用此选项。

  > 注意
  >
  > 仅为 VRRP 协议版本 2 启用 身份验证类型和身份验证文本 参数。

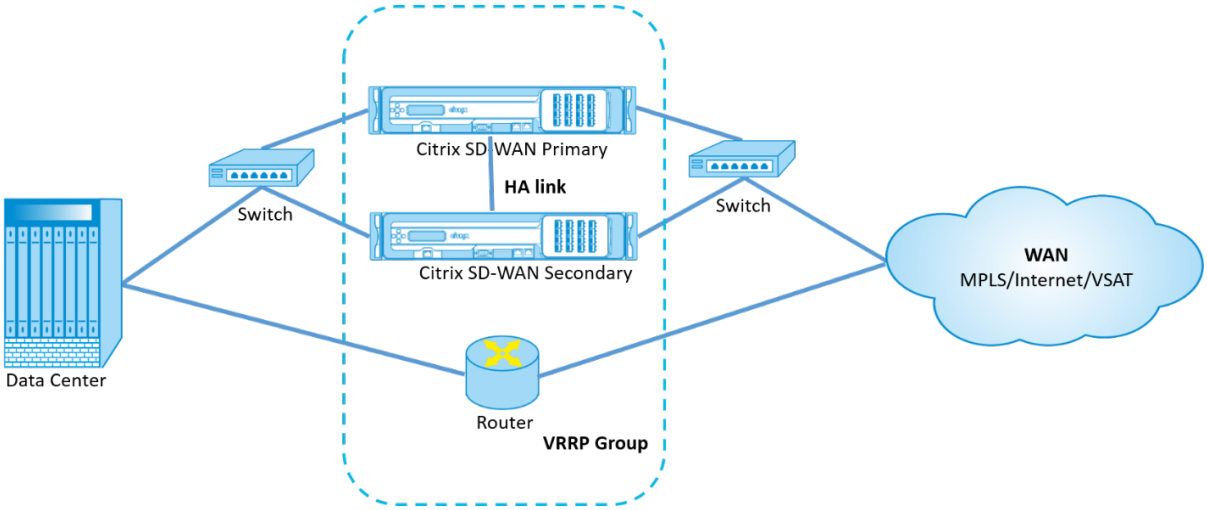
- 使用 **V2** 校验和：为 VRRPv3 启用与第三方网络设备的兼容性。默认情况下，VRRPv3 使用 v3 校验和计算方法。某些第三方设备可能只支持 VRRPv2 校验和计算。在这种情况下，请启用此选项。
- 虚拟接口：用于 VRRP 的虚拟接口。如果使用 IPv6，则虚拟接口将默认启用 NDP RA。选择一个已配置的虚拟接口。
- 虚拟 **IP** 地址：分配给虚拟接口的虚拟 IP 地址。为虚拟接口选择一个已配置的虚拟 IP 地址。您可以指定 IPv4 或 IPv6 地址。
- **VRRP** 路由器 **IP**：VRRP 组的虚拟路由器 IP 地址。默认情况下，将 SD-WAN 设备的虚拟 IP 地址指定为虚拟路由器 IP 地址。VRRP 虚拟路由器 IP 应为链路本地 IPv6 地址。

限制

- 仅在网关模式部署中支持 VRP。
- 您最多可以配置四个 VRRP ID (VRID)。
- 多达 16 个虚拟网络接口可以参与 VRID。

高可用性和 **VRRP**

通过在 SD-WAN 网络上同时应用高可用性和 VRRP 功能，您可以显著减少网络停机时间和流量中断。在主动/备用角色中部署一对 Citrix SD-WAN 设备以及备用路由器，以形成 VRRP 组。此组显示为具有一个虚拟 IP 地址和一个虚拟 MAC 地址的单个默认网关。



以下是高可用性和 VRRP 部署的两个案例：

第一种情况：**SD-WAN** 上的高可用性故障转移计时器等于 **VRRP** 故障切换计时器。

预期的行为是在 VRRP 切换之前发生高可用性切换，即流量继续流经新的活动 SD-WAN 设备。在这种情况下，SD-WAN 将继续使用 VRRP 主角色。

第二种情况：**SD-WAN** 上的高可用性故障转移计时器大于 **VRRP** 故障切换计时器。

预期的行为是发生 VRRP 切换到路由器的情况，即路由器变成 VRRP Master，流量可能会暂时流经路由器，绕过 SD-WAN 设备。

但是，一旦高可用性切换发生，SD-WAN 将再次成为 VRRP 主机，也就是说，流量现在流经新的活动 SD-WAN 设备。

有关高可用性部署模式的详细信息，请参阅 高可用性。

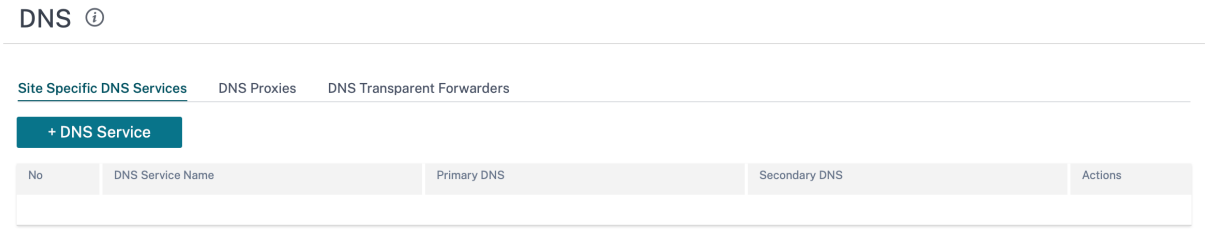
域名系统设置

October 21, 2022

域名系统 (DNS) 将人类可读的域名转换为机器可读的 IP 地址，与此相反。Citrix SD-WAN 提供以下 DNS 功能：

- DNS 代理
- DNS 透明转发

要配置 DNS 设置，请在“站点配置”页面中导航到 配置 **>** 高级设置 > **DNS** 设置。



站点特定的 **DNS** 服务器

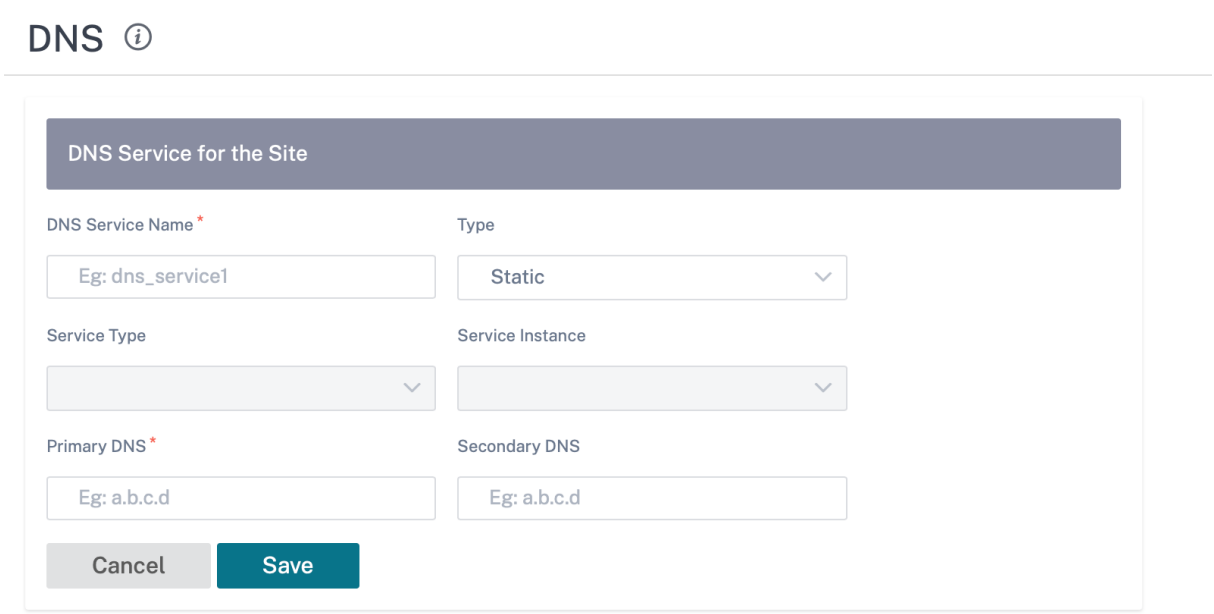
在“站点特定的 **DNS** 服务器”选项卡上，单击 **+ DNS** 服务器 以配置 DNS 请求路由到的特定站点 DNS 服务器。提供 DNS 服务器的名称。选择以下服务类型之一：

- 静态：拦截发往 Citrix SD-WAN IP 地址的 DNS 请求并将其转发到指定的 IPv4 DNS 服务器。可以创建内部、ISP、Google 或任何其他开源 DNS 服务。
- 动态：拦截发往 Citrix SD-WAN IP 地址的 DNS 请求，并将其重定向到从基于 DHCP 的 WAN 链接中获知的 IPv4 DNS 服务器之一。如果 WAN 链路断开，则选择另一个基于 DHCP 的 WAN 链接 DNS 服务器。在 ISP 仅允许向其托管的 DNS 服务器发送 DNS 请求的部署中，此功能非常有用。动态 DNS 服务只能在站点级别配置。每个站点只允许一个动态 DNS 服务。
- **StaticV6**：拦截发往 Citrix SD-WAN IP 地址的 DNS 请求，并将其转发到指定的 IPv6 DNS 服务器。可以创建内部、ISP、Google 或任何其他开源 DNS 服务。
- D@@**ynamicV6**：拦截发往 Citrix SD-WAN IP 地址的 DNS 请求，并将其重定向到从基于 DHCP 的 WAN 链接中获知的 IPv6 DNS 服务器之一。如果 WAN 链路断开，则选择另一个基于 DHCP 的 WAN 链接 DNS 服务器。在 ISP 仅允许向其托管的 DNS 服务器发送 DNS 请求的部署中，此功能非常有用。动态 DNS 服务只能在站点级别配置。每个站点只允许一个动态 DNS 服务。

要配置静态 DNS 服务，请选择 类型 为 静态（对于 IPv4 地址）或 **StaticV6**（对于 IPv6 地址），然后输入一对 主 **DNS** 和 辅助 **DNS** 服务器 IP 地址。

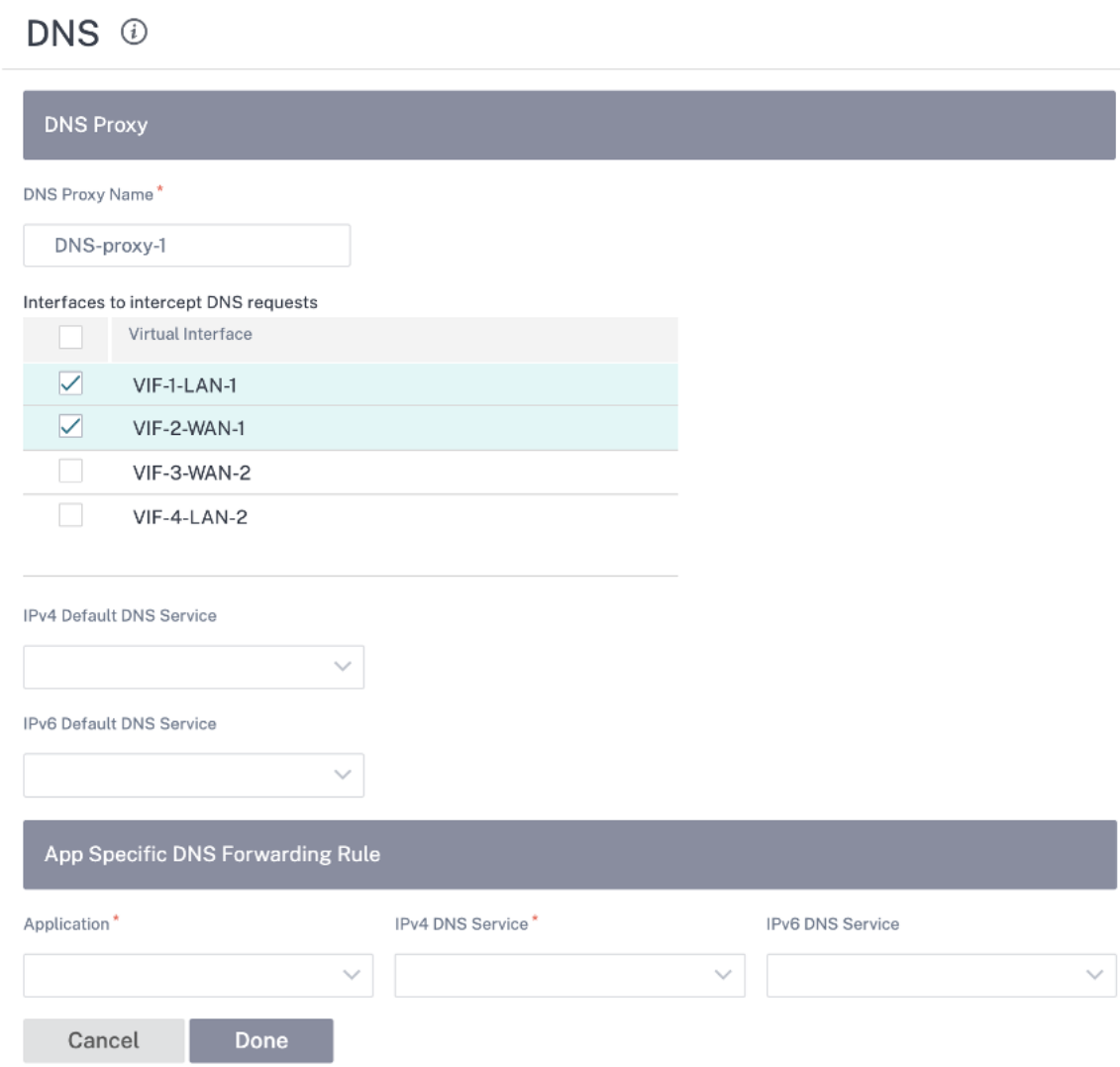
要配置动态 DNS 服务，请将 类型 选择为 动态（对于 IPv4 地址）或 D **ynamicV6** （对于 IPv6 地址），然后选择 **Internet** 作为 服务类型 和 服务实例。

相应的 DNS 代理服务将列在“站点配置” **>** “接口”下的“带内管理 **DNS**”下拉列表中。



DNS 代理

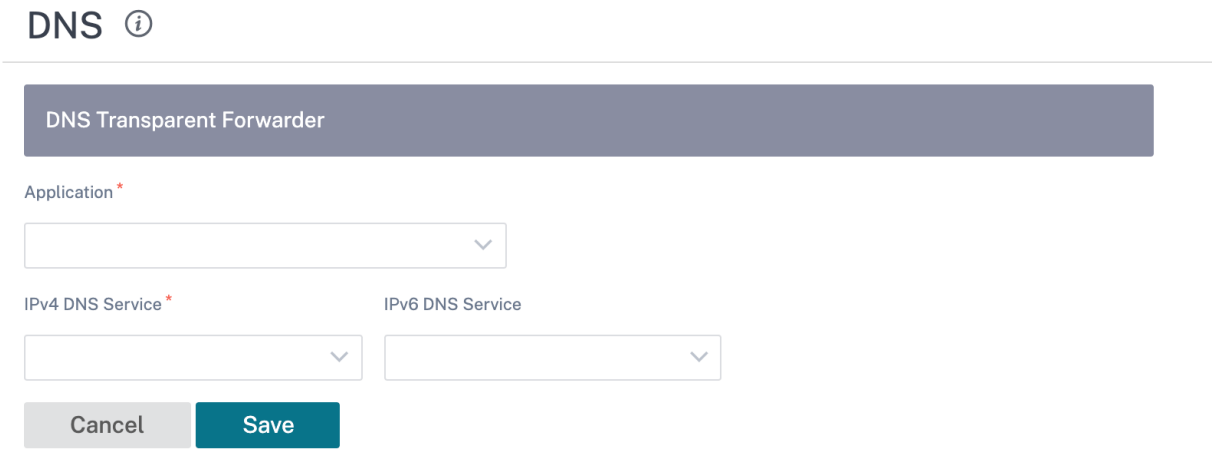
DNS 代理会截获发往 SD-WAN IP 地址的 DNS 请求，然后将其转发到选定的 DNS 服务器。您可以配置包含多个转发器的代理，以帮助根据应用程序域名控制 DNS 请求。



- DNS 代理服务器设置：
  - **DNS** 代理名称：DNS 代理的名称。
  - 拦截 **DNS** 请求的接口：拦截 DNS 请求的接口。仅允许受信任的接口。
  - 所有流量的默认 **DNS** 服务器：如果 DNS 转发器查找中没有任何应用程序匹配，则将 DNS 请求转发到的默认 DNS 服务器。
  - **IPv4** 默认 **DNS** 服务：如果 DNS 转发器查找中没有任何应用程序匹配，则将 DNS 请求转发到的 IPv4 默认 DNS 服务。
  - **IPv6** 默认 **DNS** 服务：如果 DNS 转发器查找中没有任何应用程序匹配，则将 DNS 请求转发到的 IPv6 默认 DNS 服务。
- 应用程序特定的 DNS 转发规则：
  - 应用程序：必须将 DNS 请求转发到选定的 DNS 服务器的应用程序。
  - **IPv4 DNS** 服务：为指定应用程序将 DNS 请求转发到的 IPv4 DNS 服务。
  - **IPv6 DNS** 服务：为指定应用程序将 DNS 请求转发到的 IPv6 DNS 服务。

DNS 透明转发器

Citrix SD-WAN 可以配置为透明 DNS 转发器。在此模式下，SD-WAN 可以拦截未发往其 IP 地址的 DNS 请求并将其转发到指定的 DNS 服务器。只有来自受信任接口上本地服务的 DNS 请求才会被截获。如果 DNS 请求与 DNS 转发器列表中的任何应用程序相匹配，则会将其转发到已配置的 DNS 服务。



- 应用程序：必须将 DNS 请求转发到选定的 DNS 服务器的应用程序。
- **IPv4 DNS** 服务：为指定应用程序将 DNS 请求转发到的 IPv4 DNS 服务。
- **IPv6 DNS** 服务：为指定应用程序将 DNS 请求转发到的 IPv6 DNS 服务。

为委托组加前缀

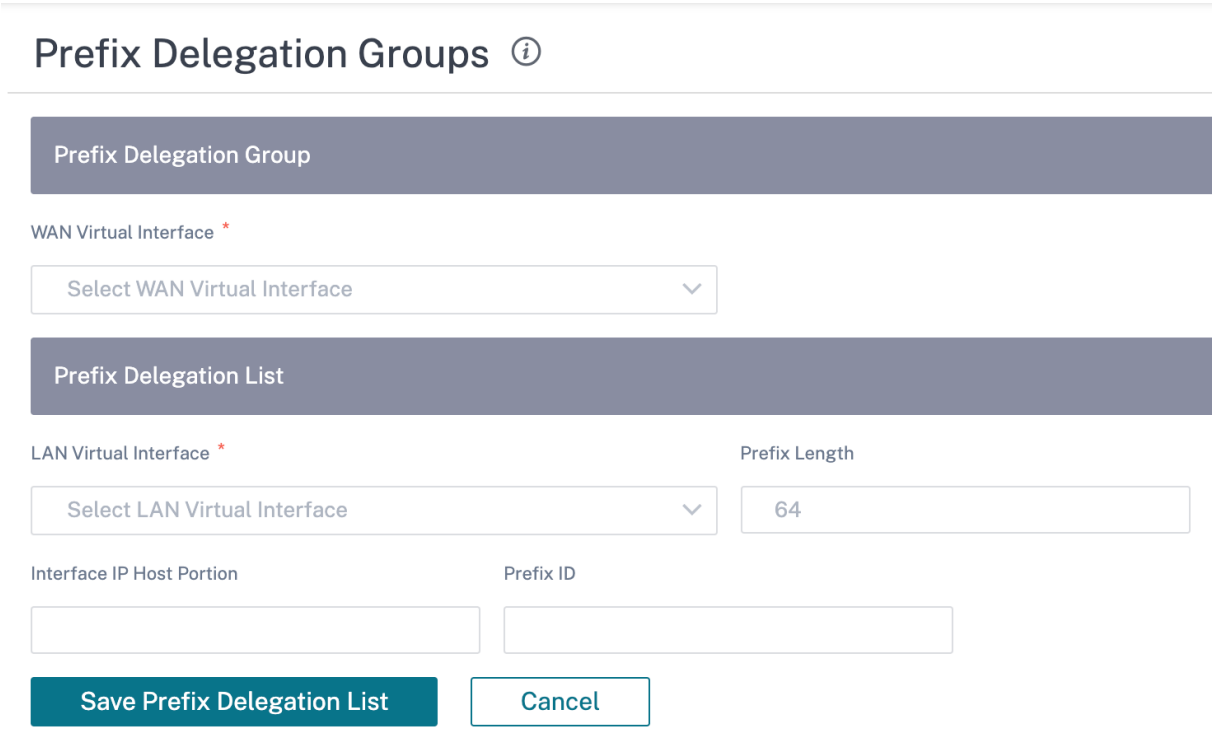
October 21, 2022

Citrix SD-WAN 设备可配置为 DHCPv6 客户端，以使用配置的 WAN 端口向 ISP 请求前缀。Citrix SD-WAN 设备收到前缀后，它将使用该前缀创建 IP 地址池以满足局域网客户端的需求。然后，Citrix SD-WAN 设备充当 DHCP 服务器，并将局域网端口上的前缀通告给局域网端客户端。

要配置前缀委派，请导航到 配置 **>** 高级设置 **>** 前缀委托组，然后单击 **+** 前缀委托组。

选择一个已配置 WAN 虚拟接口，在该接口上请求 ISP 提供前缀，并提供以下详细信息：

- 局域网虚拟接口：选择要求前缀的已配置 LAN 虚拟接口之一。
- 前缀长度：作为前缀一部分的全局单播 IPv6 地址的位数。
- 接口 **IP** 主机部分：用于接口 IP 地址的主机部分。
- 前缀 **ID**：用于标识局域网接口的前缀委派请求的唯一标识符。



链路聚合组

October 21, 2022

链路聚合组 (LAG) 功能允许您对 SD-WAN 设备上的两个或多个端口进行分组，以便作为单个端口一起工作。这可确保提高可用性、链路冗余性和增强性能。

适用于本地的 Citrix SD-WAN Orchestrator 支持简单的链接聚合组（ACTIVE-BACKUP）。当前版本不支持基于 802.3ad LACP 协议的协商。任何时候，只有一个端口处于活动状态，其他端口处于备份模式。活动和备份支持依赖于数据平面开发工具包 (DPDK) 软件包来实现 LAG 功能。

LAG 功能仅在以下平台上可用：

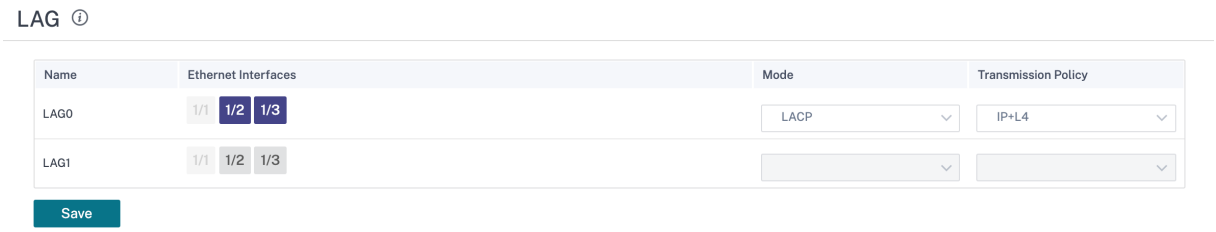
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 410 SE
- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 2100 SE/PE
- Citrix SD-WAN 4100 SE
- Citrix SD-WAN 5100 SE/PE
- Citrix SD-WAN 6100 SE/PE

> 注意
>
> - VPX/VPXL 平台上不支持 LAG 功能。
> - 每个 LAG 至少支持两个端口和最多四个端口。
> - LAG 的所有成员必须是相同的类型，例如 1/1 或 1/2。不支持 LAG 配置 1/1 和 10/1。
> - 如果在 接口组中将 LAG 用作以太网接口，则不支持链路状态传播 (LSP) 功能。

平台	支持的最大 LAG 数量	支持 LACP 的端口
110	1	1/1
210	2	1/1 或 1/2
410	1	1/1 或 1/2
1100	3	1/1 或 1/2
2100	3	1/1 或 1/2
4100	4	1/1 或 1/2

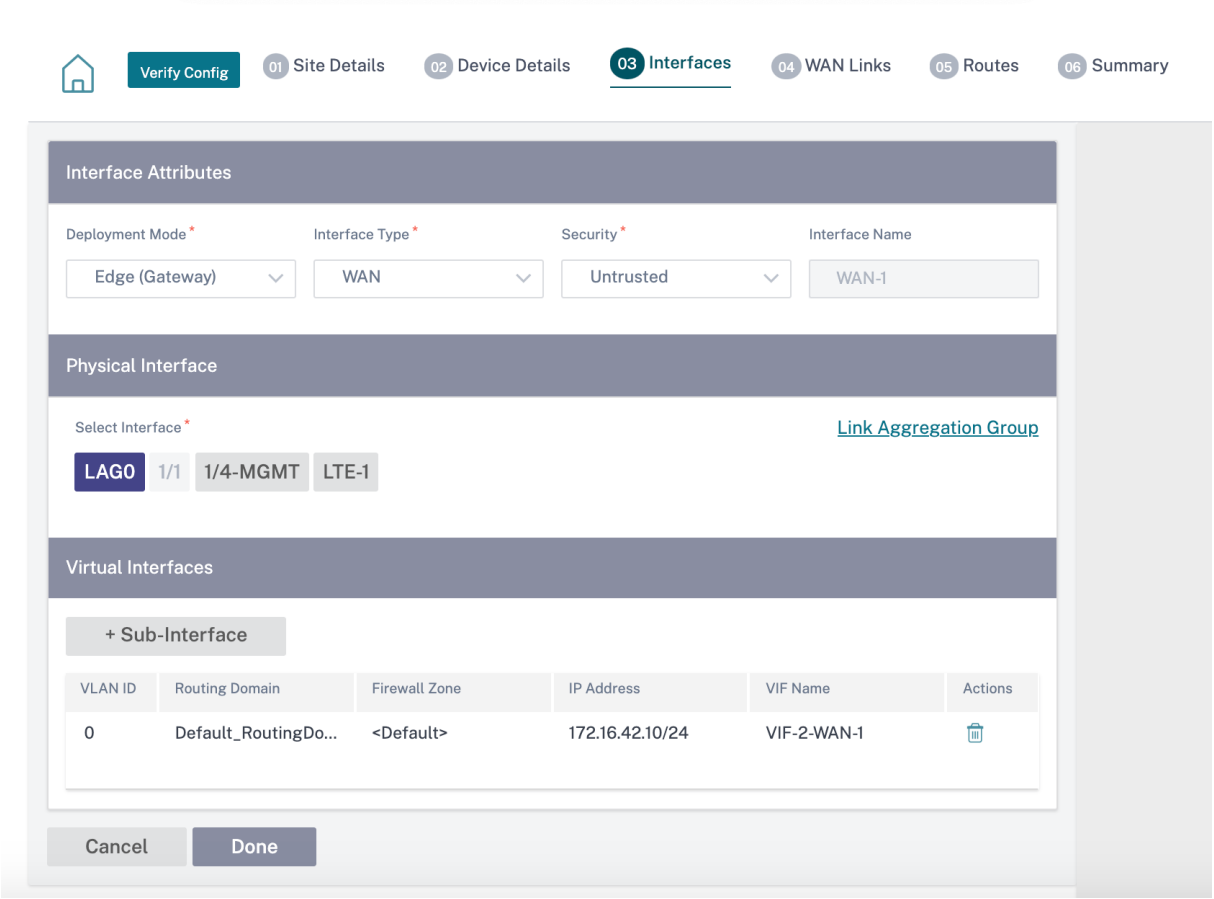
平台	支持的最大 LAG 数量	支持 LACP 的端口
5100	3	10/1 或 10/2
6100	4	1/1 或 1/2

要配置链路聚合组，请在站点级别导航到 配置 **>** 高级设置 **> LAG** ，然后选择成员以太网接口以形成链路聚合组。

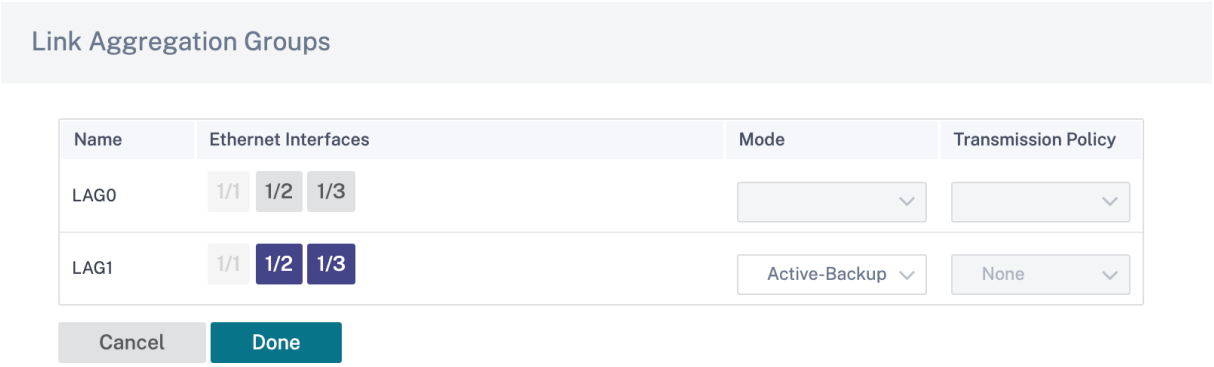


将端口添加到 LAG 后，您可以在“站点配置”下选择 **LAG** 来配置接口。这些接口进一步用于配置 LAN/WAN 链路和

HA。您无法更改单个成员端口的设置，对 LAG 所做的任何配置更改都会自动推送到成员端口。



在“接口”部分中，单击“链路聚合组”，必要时快速更改 LAG 配置。



您可以在 报告 **>** 设备报告 **> LACP LAG** 组下查看配置了 **LAG** 和 **LACP** 的接口的详细信息。有关更多信息，请参阅 设备报告。

设备设置

October 21, 2022

Citrix SD-WAN Orchestrator 服务允许您在站点级别配置设备设置并将其推送到远程设备。

您可以配置用户、网络适配器、NetFlow、AppFlow、SNMP、后备配置和清除流量设置。

> 注意
>
> 创建或编辑站点模板时，配置设备设置的选项不可用。

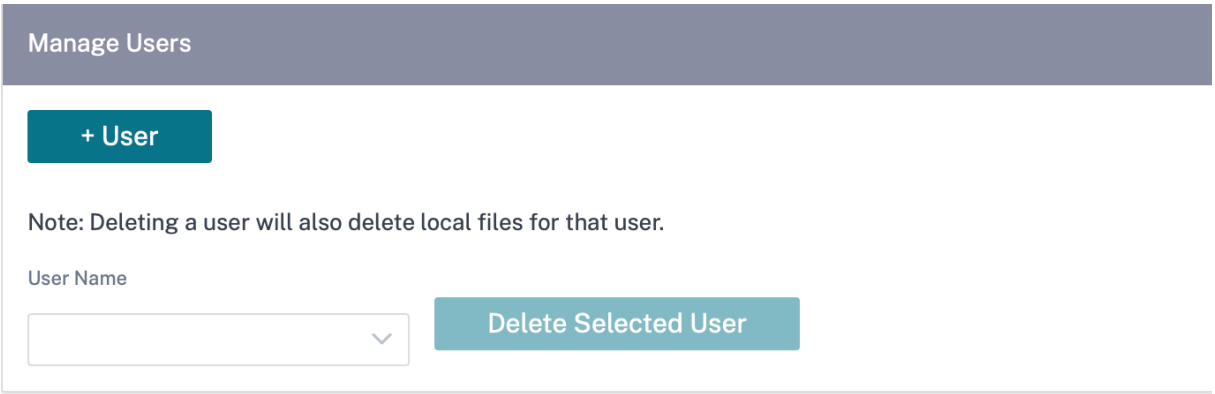
如果配置了 HA，请选择要更改其设备设置的主设备或辅助设备。

管理界面

管理界面允许您添加和管理本地和远程用户帐户。远程用户帐户通过 RADIUS 或 TACACS+ 身份验证服务器进行身份验证。

管理用户

您可以为站点添加新的用户帐户。要添加新用户，请导航到“配置”>“设备设置”**>**“管理员界面”>“管理用户”，然后单击“**+** 用户”。

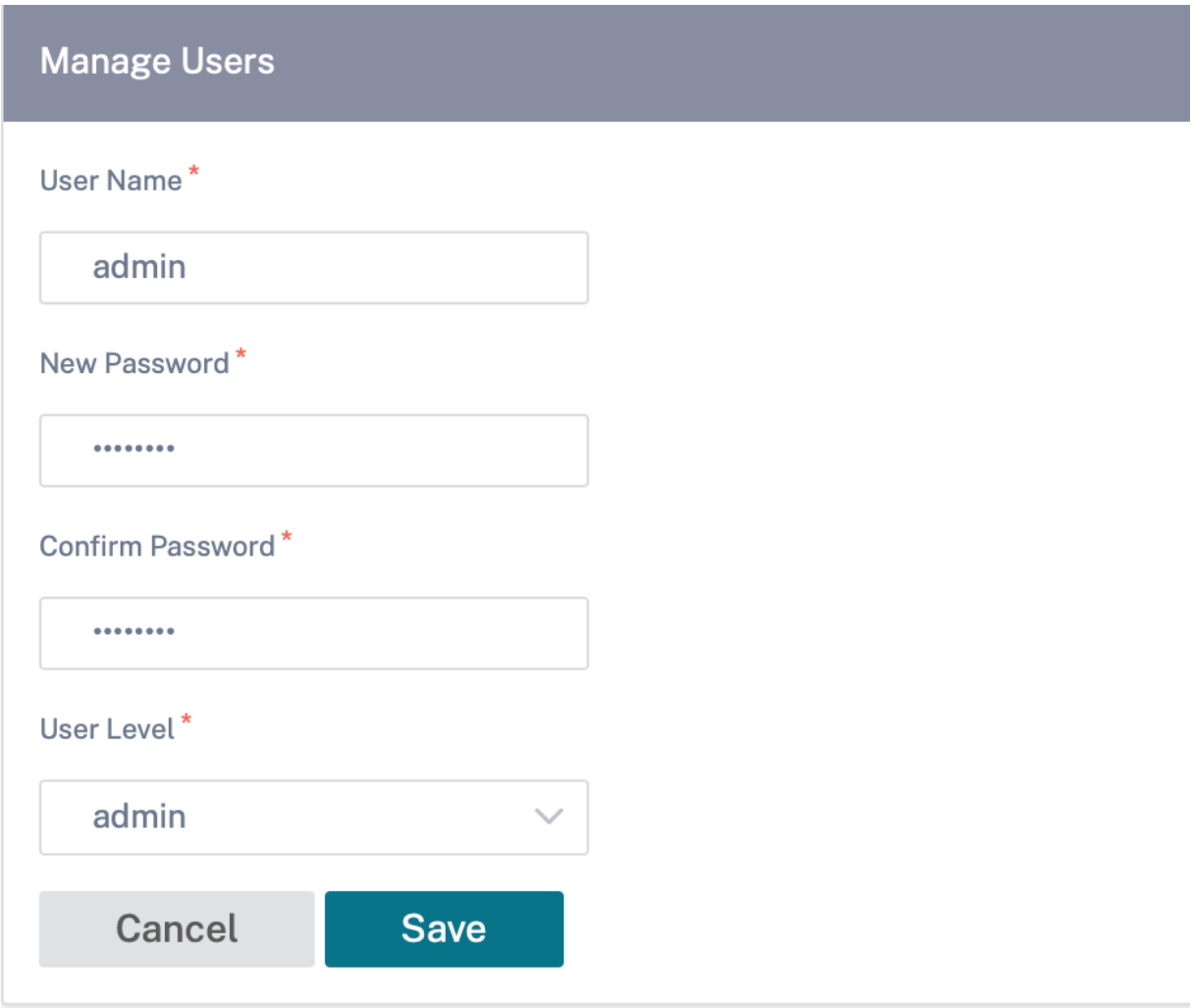


提供以下详细信息：

- 用户名：用户帐户的用户名。

- 新密码：用户帐户的密码。
- 确认密码：重新输入密码进行确认。
- 用户级别：选择以下帐户权限之一：
  - 管理员：管理员帐户对所有设置具有读写权限。管理员可以对网络执行配置和软件更新。
  - 查看者：查看者帐户是一个只读帐户，可以访问控制面板、报告和监控部分。
  - 网络管理员：网络管理员对网络设置具有读写访问权限，对其他设置具有只读访问权限。
  - 安全管理员：安全管理员对防火墙/安全相关设置具有读写权限，对其他设置具有只读访问权限。

    > 注意
    >
    > 安全管理员有权禁用其他用户对防火墙的写入访问权限（管理员/查看器）。

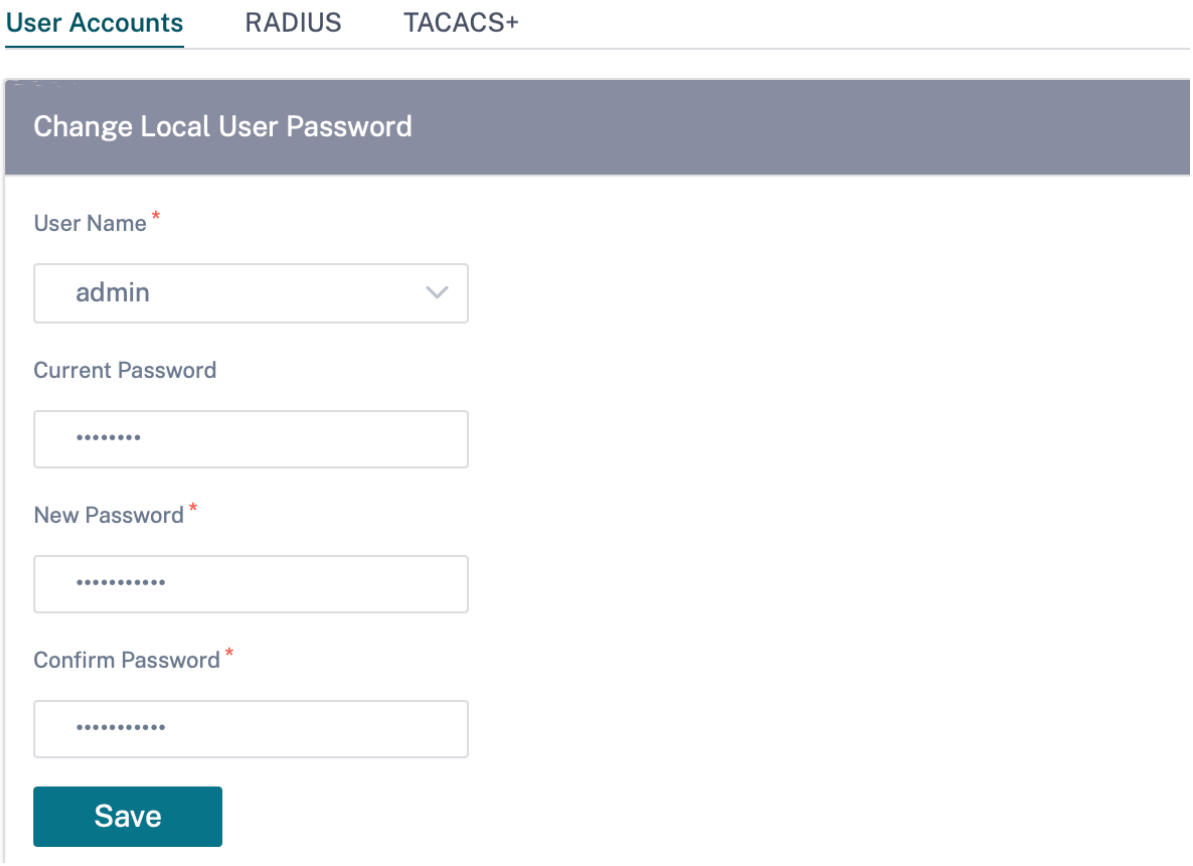


要删除用户，请选择一个用户名并单击“删除选定用户”。用户帐户和本地文件将被删除。

更改本地用户密码

要更改本地用户密码，请导航到 配置 > 设备设置 > 管理界面 > 用户帐户 > 更改本地用户密码 并提供以下值：

- 用户名：从站点配置的用户列表 中选择要更改密码的用户名。
- 当前密码：输入当前密码。对于管理员用户，此字段是可选的。
- 新密码：输入您选择的新密码。
- 确认密码：重新输入密码进行确认。



RADIUS 身份验证服务器

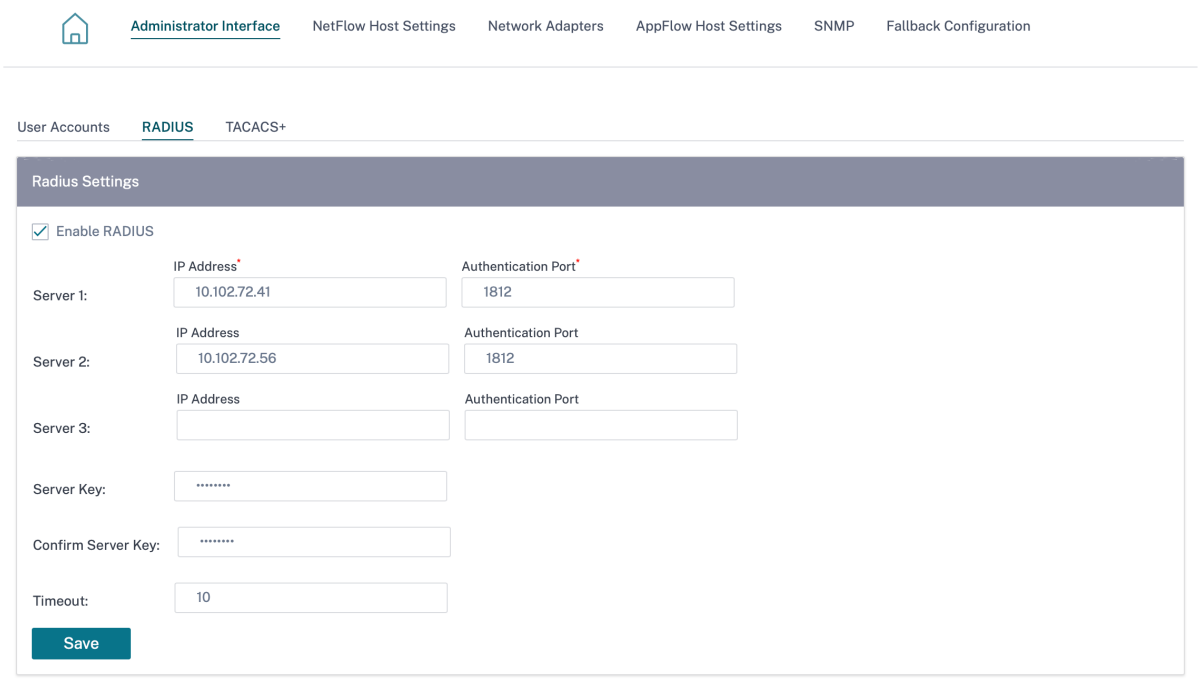
RADIUS 在设备上启用远程用户身份验证。要使用 RADIUS 身份验证，必须指定并配置至少一个 RADIUS 服务器。或者，您可以配置冗余的 RADIUS 服务器，最多可配置三台。服务器将按顺序进行检查。确保在 RADIUS 身份验证服务器上创建了所需的用户帐户。

要配置 RADIUS 身份验证，请导航到 配置 > 设备设置 > 管理界面 > **RADIUS**，然后单击 启用 **RADIUS**。

> 注意
>
> 您可以在站点上启用 RADIUS 或 TACACS+ 身份验证。您不能同时启用两者。

提供 RADIUS 服务器的主机 IP 地址和身份验证端口号。默认端口号为 1812。输入服务器密钥并确认它是用于连接到 RADIUS 服务器的密钥。指定等待来自 RADIUS 服务器的身份验证响应的时间间隔。超时值必须小于或等于 60 秒。

> 注意
>
> 服务器密钥 和 超时 设置应用于所有已配置的服务器。



TACACS+ 身份验证服务器

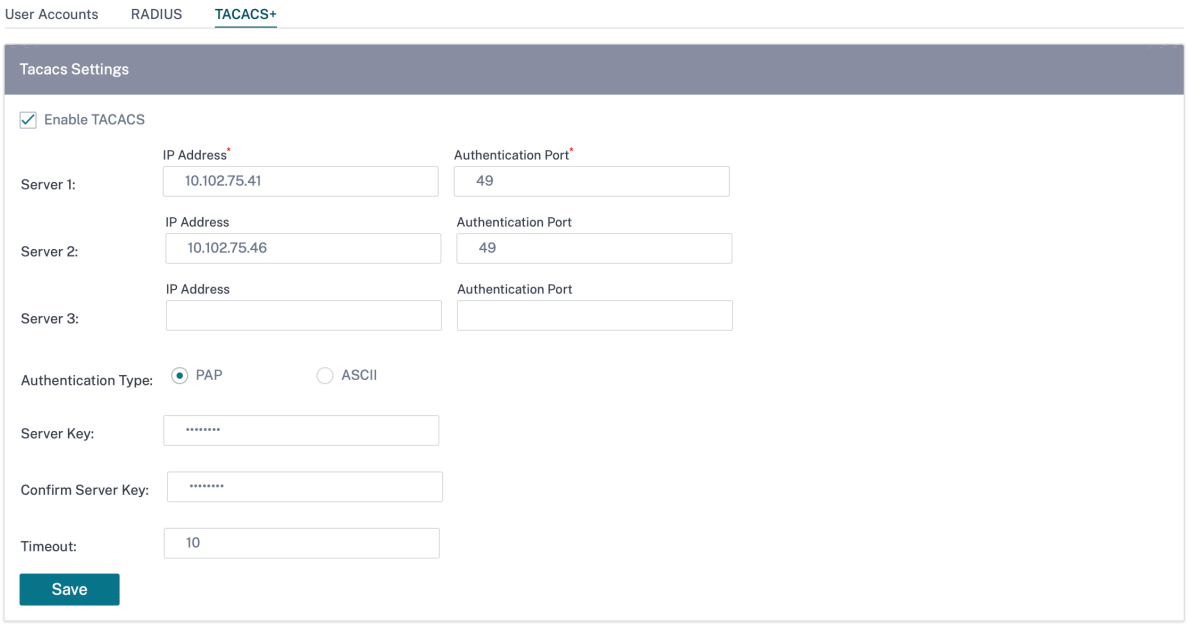
TACACS+ 在设备上启用远程用户身份验证。要使用 TACACS+ 身份验证，必须指定并配置至少一个 TACACS+ 服务器。或者，您可以配置冗余备份 TACACS+ 服务器，最多可配置三台服务器。服务器将按顺序进行检查。确保在 TACACS+ 身份验证服务器上创建所需的用户帐户。

要配置 TACACS+ 身份验证，请导航到 配置 > 设备设置 > 管理界面 > **TACACS+** ，然后单击“启用 **TACACS+**”。

> 注意
>
> 您可以在站点上启用 RADIUS 或 TACACS+ 身份验证。您不能同时启用两者。

1. 选择加密方法以将用户名和密码发送到 TACACS+ 服务器。
2. 提供 TACACS+ 服务器的主机 IP 地址和身份验证端口号。默认端口号为 49。
3. 输入服务器密钥并进行确认。它是用于连接到 TACACS+ 服务器的私有密钥。
4. 指定等待 TACACS+ 服务器发出身份验证响应的时间间隔。超时值必须小于或等于 60 秒。

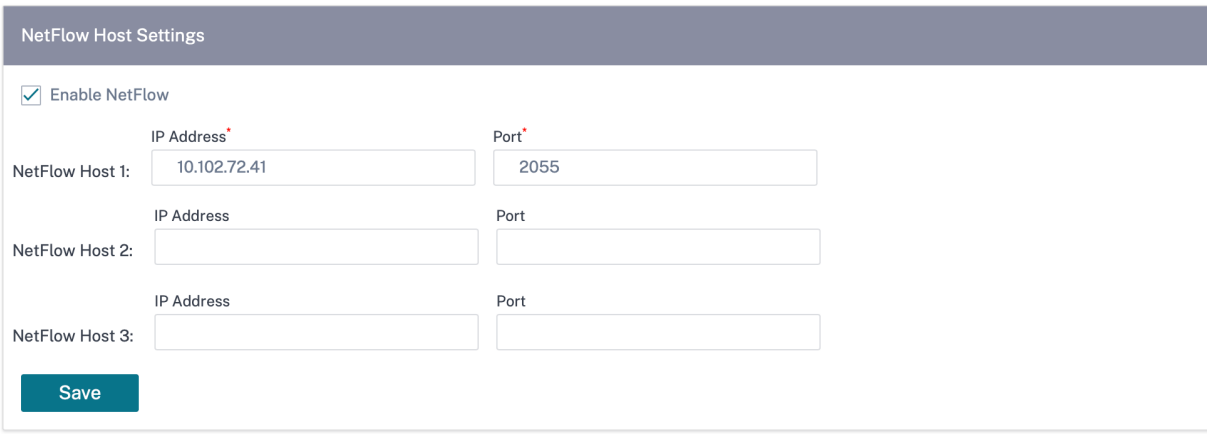
> 注意
>
> 身份验证类型、服务器密钥和 超时设置 应用于所有已配置的服务器。



NetFlow 主机设置

NetFlow 收集器会在 IP 网络流量进入或退出 SD-WAN 接口时收集 IP 网络流量。您可以使用 NetFlow 数据确定流量的来源和目的地、服务类别以及流量拥塞的原因。有关更多信息，请参阅 多个 NetFlow 收集器。

您最多可以配置三台 NetFlow 主机。要配置 NetFlow 主机设置，请导航到 配置 > 设备设置 > **NetFlow** 主机设置。选择 启用 **NetFlow** 并提供 NetFlow 主机的 IP 地址和端口号。

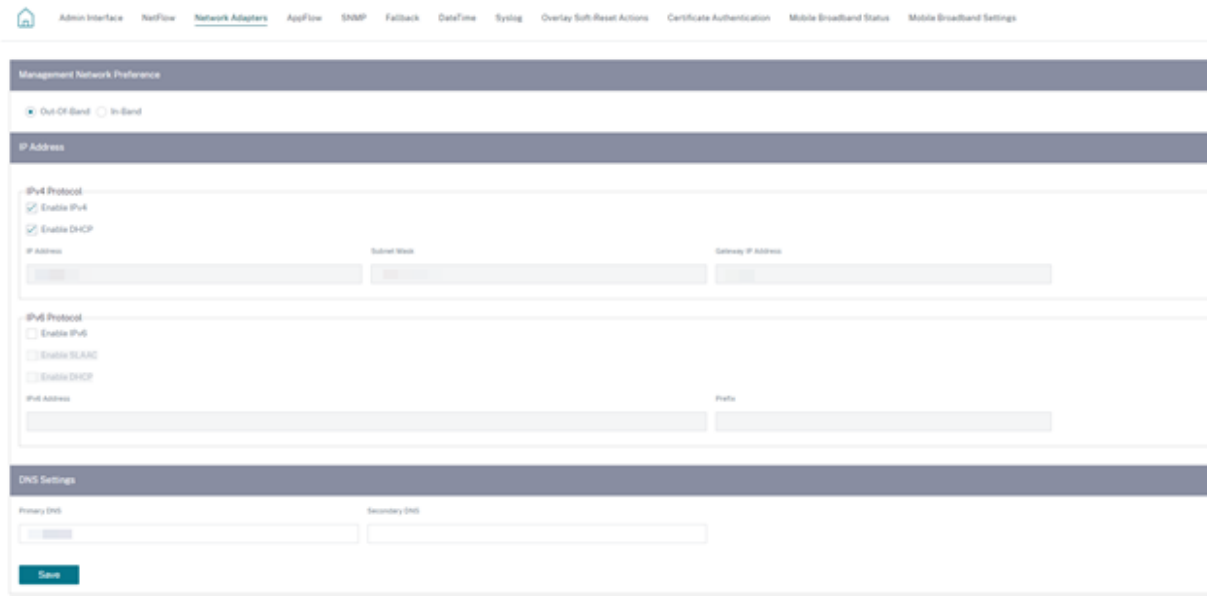


网络适配器

对于 Citrix SD-WAN 设备，您可以手动更改管理网络首选项、管理 IP 地址和其他网络参数。您可以更改设备的 IPv4 地址、子网掩码、网关 IP 地址、IPv6 地址和前缀，或者启用 DHCP 或 SLAAC（仅适用于 IPv6 地址）来自动获取 IP 地址。有关更多信息，请参阅 动态主机配置协议。

> 注意
>
> - 如果接口用于带内管理，则无法更改 IP 地址。有关带内管理的更多信息，请参阅 带内管理。
> - 仅当您将数据端口配置为带内管理端口并且配置了 Internet 服务时，带内选项才有效。在设置管理首选项之前，请确保您的配置支持对 SD-WAN 设备进行带内管理。
> - 如果设备运行的是 11.4.2 或更高版本的软件版本，则可以看到“管理网络首选项（带内和带外）”部分。

要配置网络适配器设置，请导航到 配置 > 设备设置 > 网络适配器。



AppFlow 主机设置

AppFlow 和 IPFIX 是流导出标准，用于识别和收集网络基础架构中的应用程序和事务数据。此数据可更好地了解应用程序流量利用率和性能。

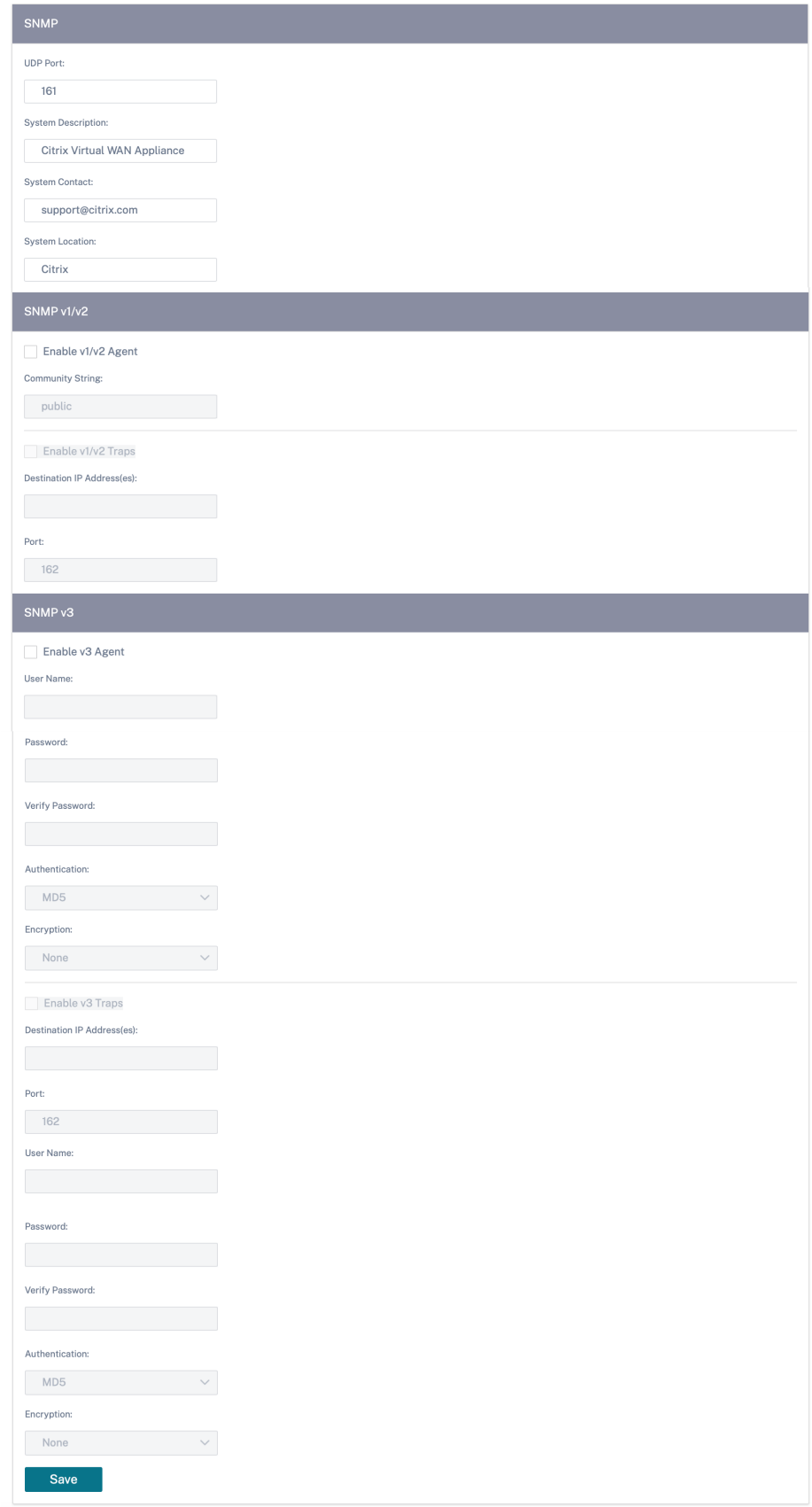
收集到的数据（称为流记录）被传输到一个或多个 IPv4 收集器。收集器可聚合流记录，并生成实时或历史报告。有关更多信息，请参阅 AppFlow 和 IPFIX。

SNMP

SNMP 用于在网络设备之间交换管理信息。SNMPv1 是 SNMP 协议的第一个版本。SNMPv2 是修订后的协议，其中包括协议数据包类型、传输映射和 MIB 结构元素的增强功能。SNMPv3 定义了 SNMP 的安全版本。SNMPv3 协议还有助于 SNMP 实体的远程配置。

SNMP 代理会在本地从设备收集管理信息，并在查询时将其发送给 SNMP 管理器。如果座席检测到设备上的紧急事件，它会向经理发出警告消息，而无需等待查询数据。这个紧急信息被称为陷阱。启用所需的 SNMP 版本代理、相应的陷阱，并提供所需的信息。有关更多详细信息，请参阅 SNMP。

要配置 SNMP 设置，请导航到 配置 > 设备设置 > **SNMP**

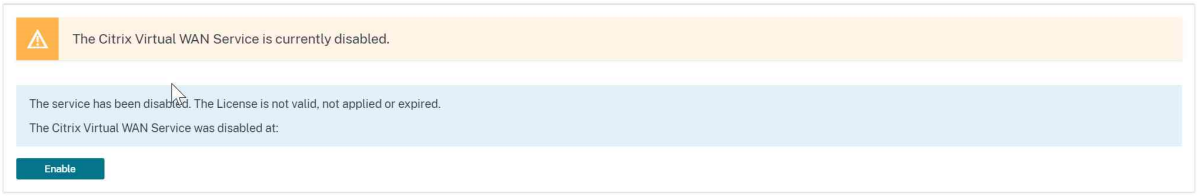


回退配置

回退配置可确保在发生链路故障、配置不匹配或软件不匹配时设备保持与零接触部署服务的连接。默认情况下，在具有默认配置文件的设备上启用回退配置。您还可以根据现有 LAN 网络设置编辑备用配置。有关更多信息，请参阅 备用配置。

流

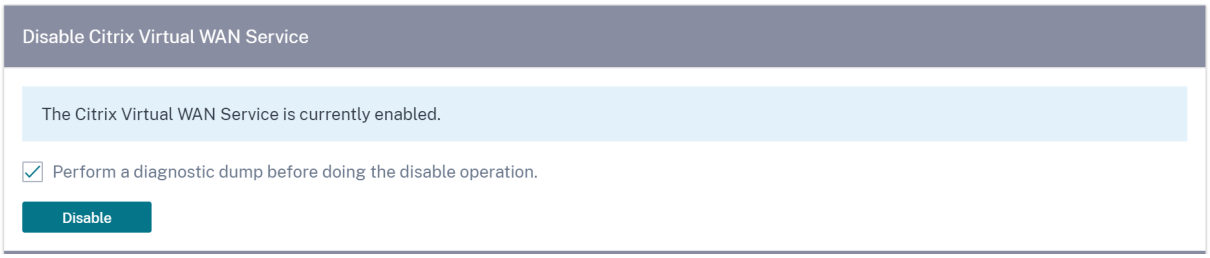
流量部分允许您在设备上启用或禁用 Citrix Virtual WAN 服务。启用该服务可启用并启动虚拟 WAN 守护进程。如果禁用了 Citrix 虚拟广域网服务，则可以选择启用该服务。



禁用 **Citrix** 虚拟广域网服务

如果启用了 **Citrix** 虚拟 **WAN** 服务，则禁 用 Citrix 虚拟广域网服务选项可用。禁用该服务会停止设备上的 Virtual WAN 守护程序。

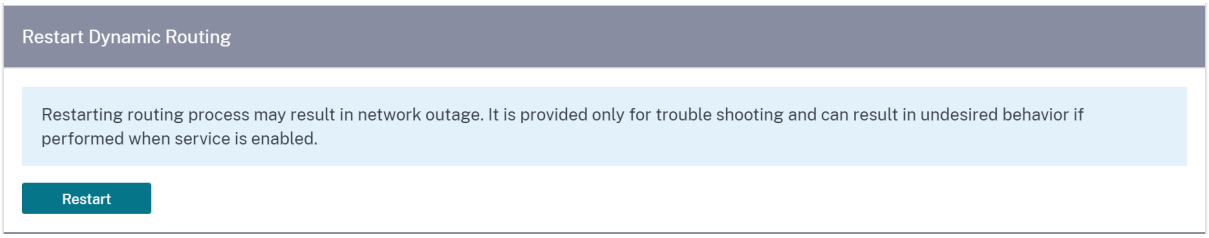
在禁用 Citrix Virtual WAN 服务之前，您可以选择收集虚拟 WAN 网络的诊断转储。



重启动态路由

您可以通过 OSPF 和 BGP 路由协议重新启动动态路由学习进程。重启动态路由选项仅用于故障排除。

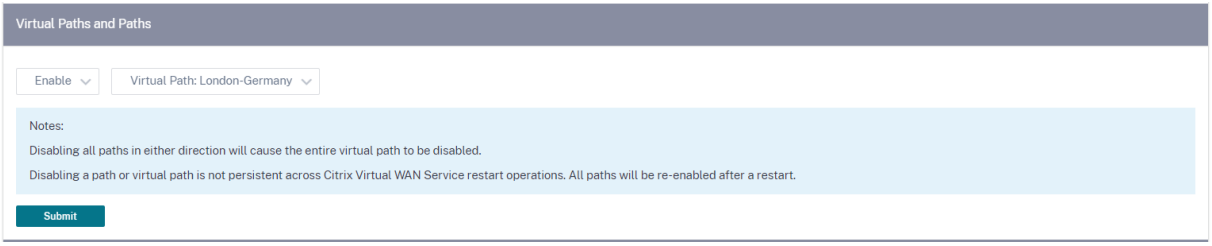
> 警告
>
> 重新启动动态路由可能会导致网络中断。



虚拟路径

您可以选择启用或禁用 2 个站点之间的虚拟路径。您可以选择底层的各个路径（任一方向），也可以选择叠加虚拟路径。禁用单个路径会禁用整个虚拟路径。

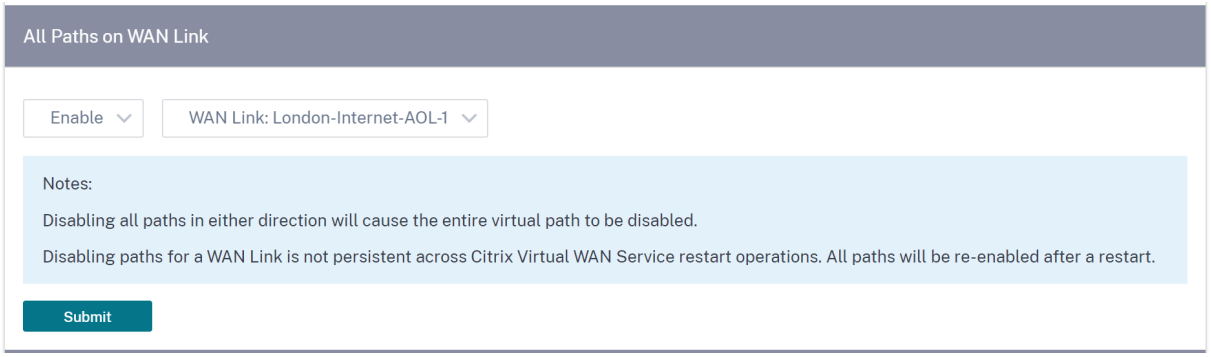
> 注意
>
> 重新启动 Citrix 虚拟广域网服务后，所有路径都将重新启用。



WAN 链路上的所有路径

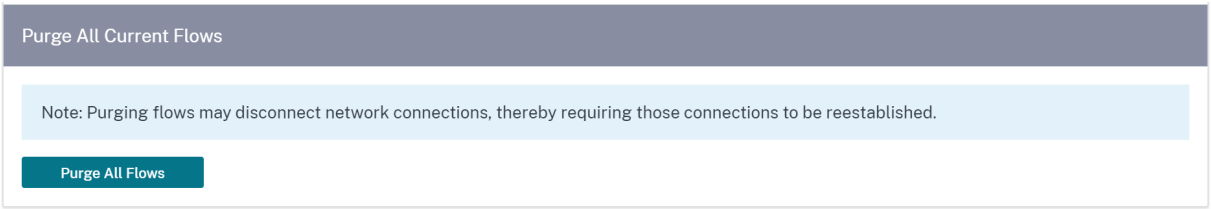
您可以选择启用或禁用 2 个站点之间的 WAN 链接禁用所有 WAN 链接，禁用虚拟路径。

> 注意
>
> 重新启动 Citrix 虚拟广域网服务后，所有广域网链接都将重新启用。



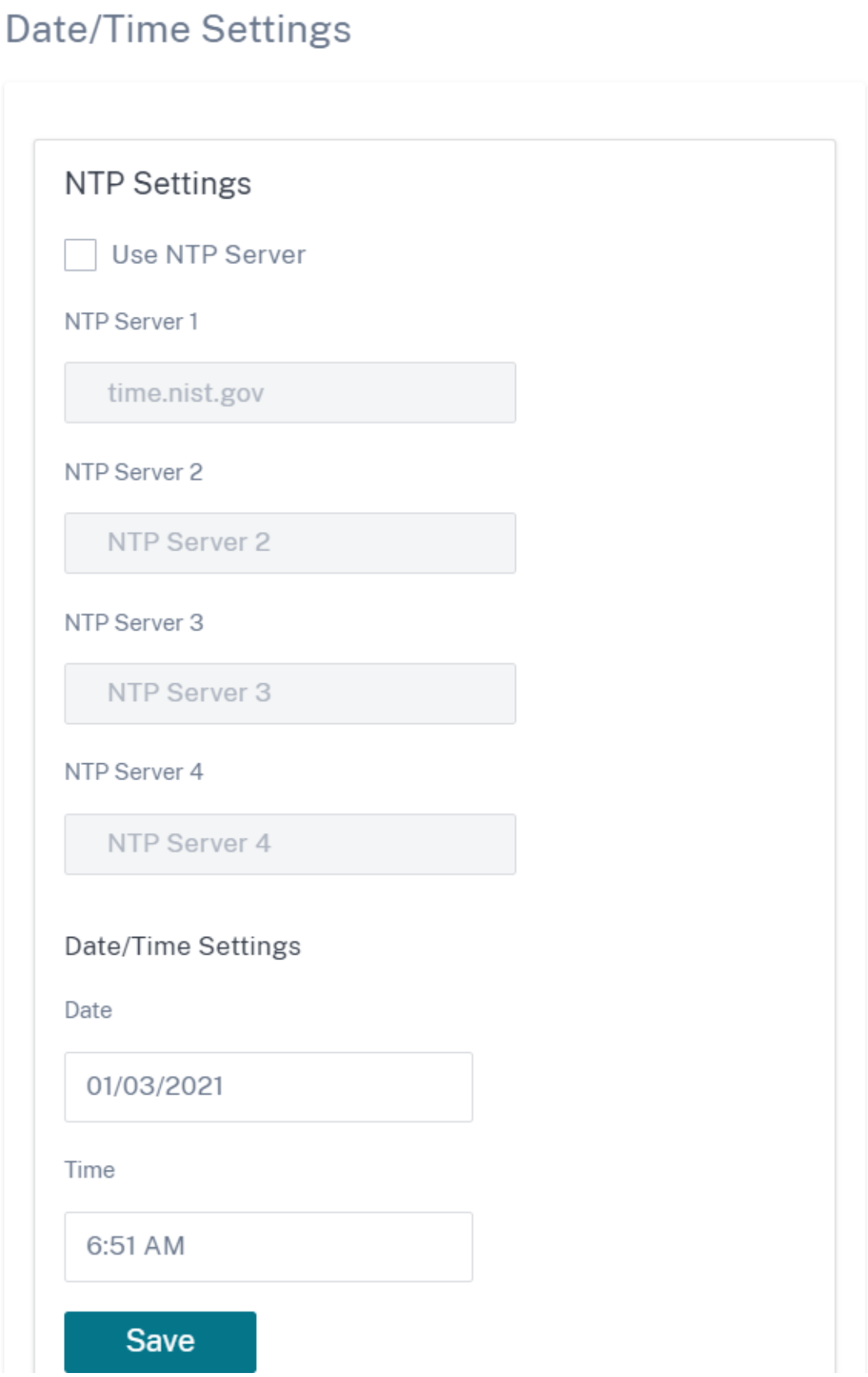
清除所有当前流量

清除流量会结束所有电流流，清除流表，重新建立流量连接，然后重新填充流表。

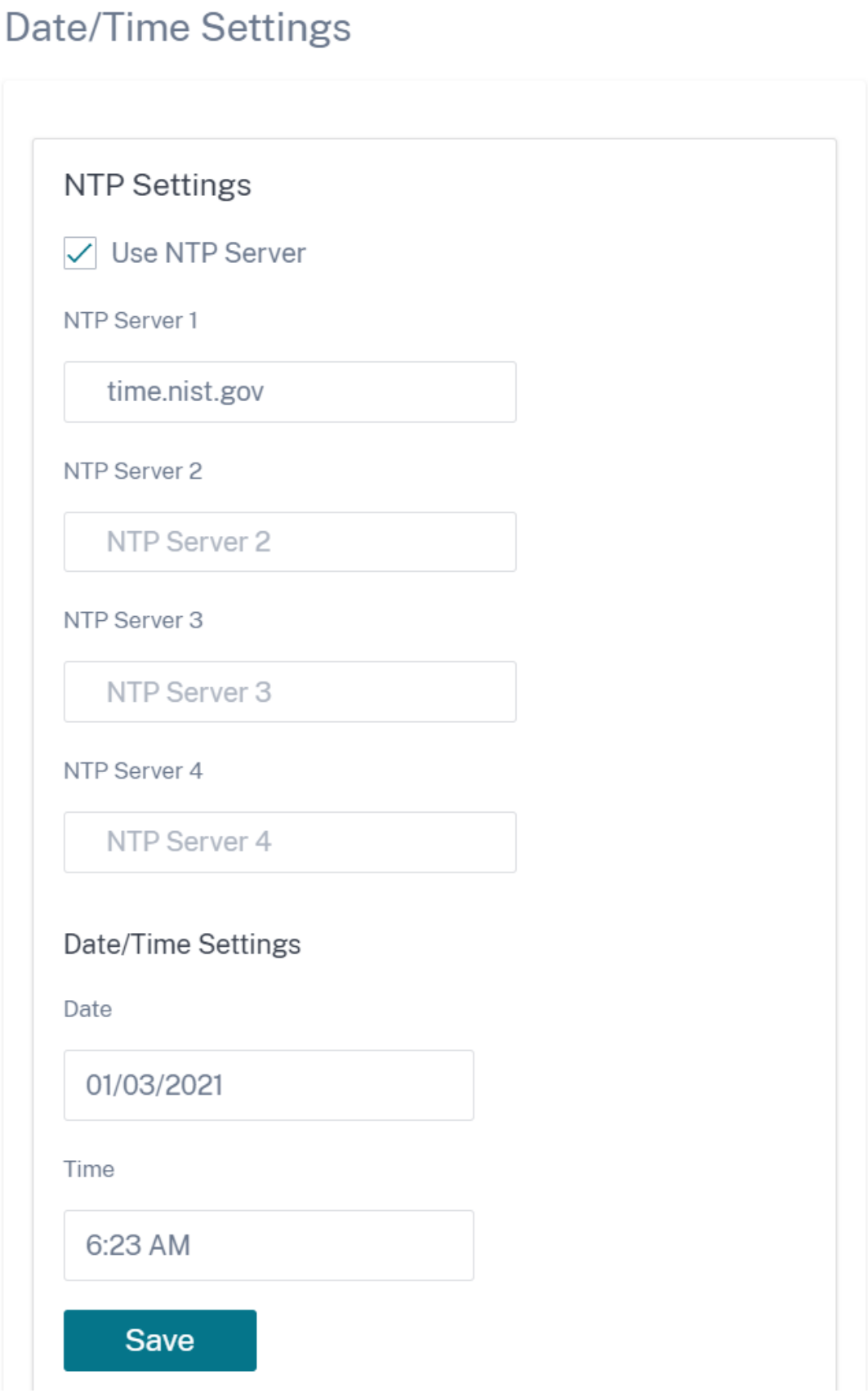


日期和时间

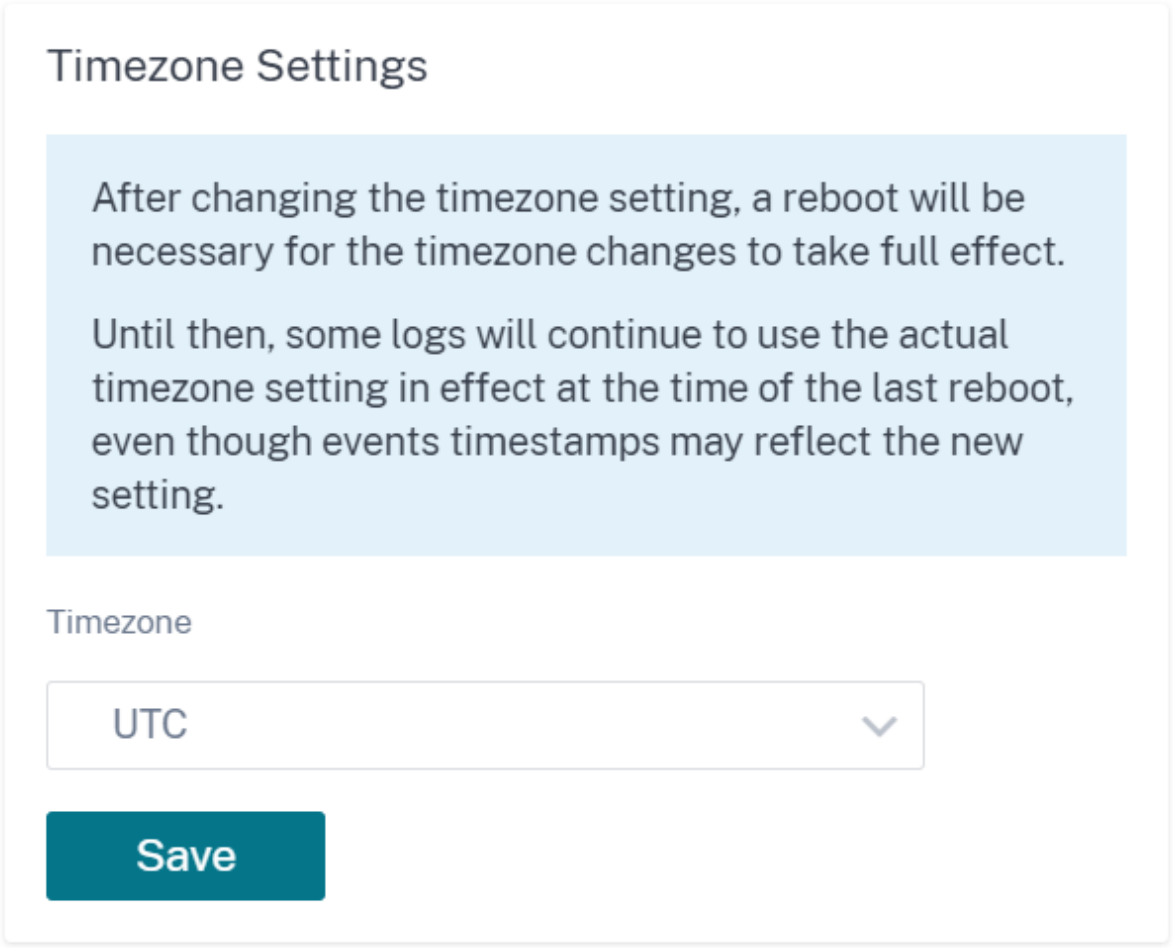
您可以手动或使用 NTP 服务器更改设备的日期和时间。要手动配置日期和时间，请确保未选择“使用 **NTP** 服务器”选项，并提供日期和时间。



如果选择“使用 **NTP** 服务器”选项，则无法手动输入当前日期和时间。您最多可以指定 4 个 NTP 服务器，但必须至少指定一个。它们充当备用 NTP 服务器，如果一台服务器出现故障，则设备会自动与另一台 NTP 服务器同步。如果您为 NTP 服务器指定域名，则还必须配置 DNS 服务器，除非您已经这样做了。

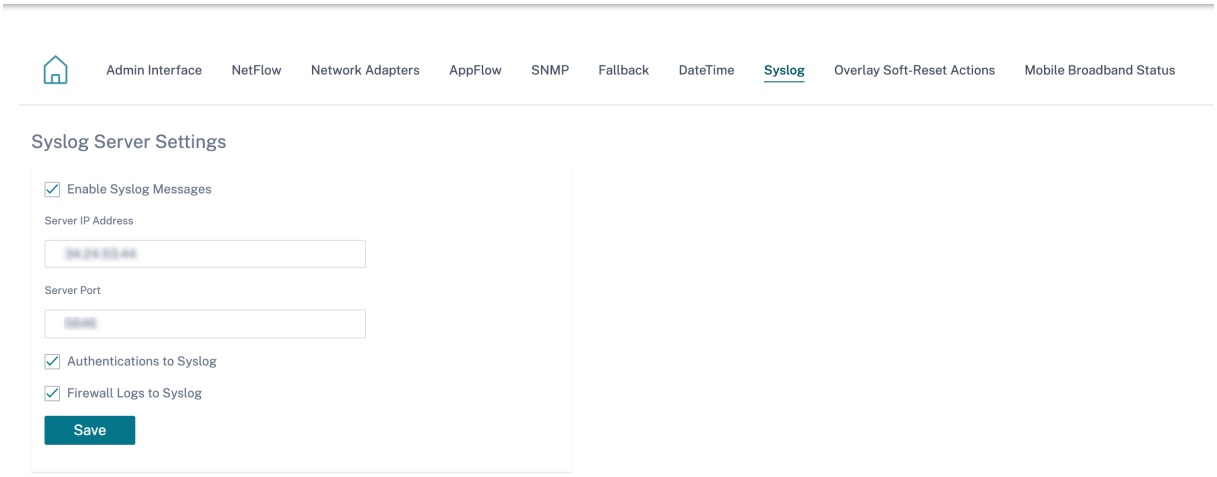


如果必须更改时区，请在设置日期和时间之前进行更改，否则您的设置将无法保留。更改时区后重新启动设备。



Syslog 服务器设置

您可以使用 Citrix SD-WAN Orchestrator 服务配置 SD-WAN 设备的 Syslog 服务器设置。通过启用 Syslog 设置，您可以将 SD-WAN 设备的系统警报和事件详细信息发送到外部 Syslog 服务器。但是，您必须导航到 配置 > 设备 设置 **>** 记录/监控 **>** 警报选项，在 **SD-WAN** 设备用户界面上选择事件类型。有关更多信息，请参阅 配置警报。



以下 Syslog 服务器设置可通过 Citrix SD-WAN Orchestrator 服务进行配置：

- 启用 **Syslog** 消息：启用或禁用向 Syslog 服务器发送日志或事件消息。
- 服务器 **IP** 地址：系统日志服务器的 IP 地址。
- 服务器端口：Syslog 服务器的端口号。
- 向 **Syslog** 进行身份验证：启用或禁用向 Syslog 服务器发送身份验证日志或事件消息。
- 向 **Syslog** 发送防火墙日志：启用或禁用向 Syslog 服务器发送防火墙日志。

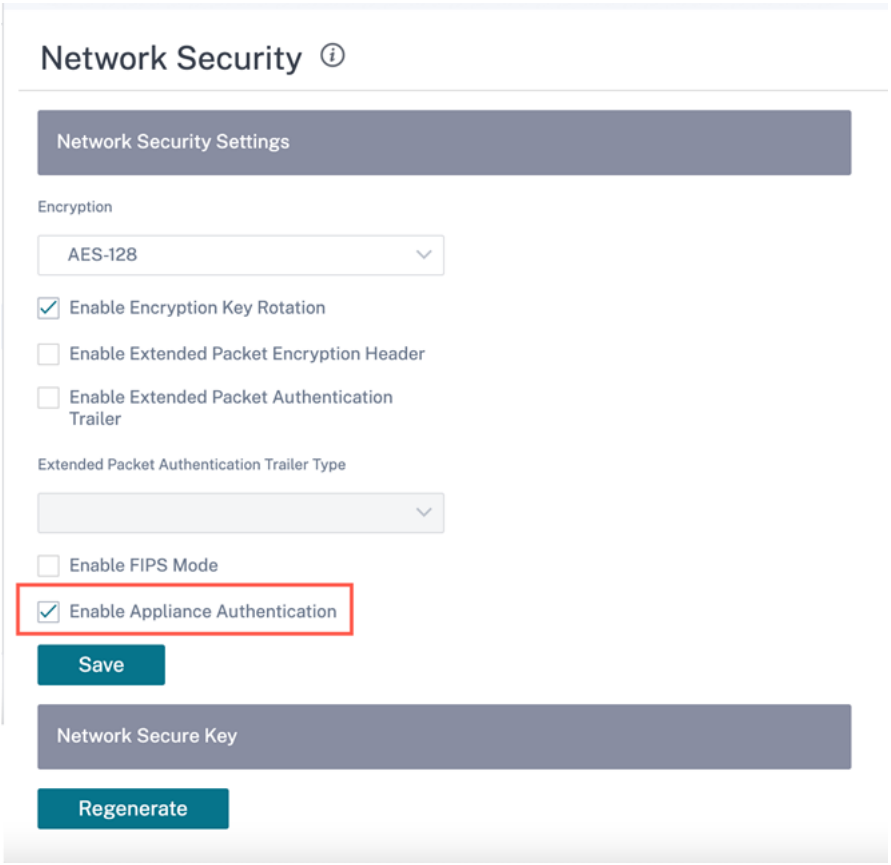
证书身份验证

Citrix SD-WAN Orchestrator 服务使用网络加密和虚拟路径 IPsec 隧道等安全技术，确保在 SD-WAN 网络中的设备之间建立安全路径。除了现有的安全措施外，Citrix SD-WAN Orchestrator 服务中还引入了基于证书的身份验证。

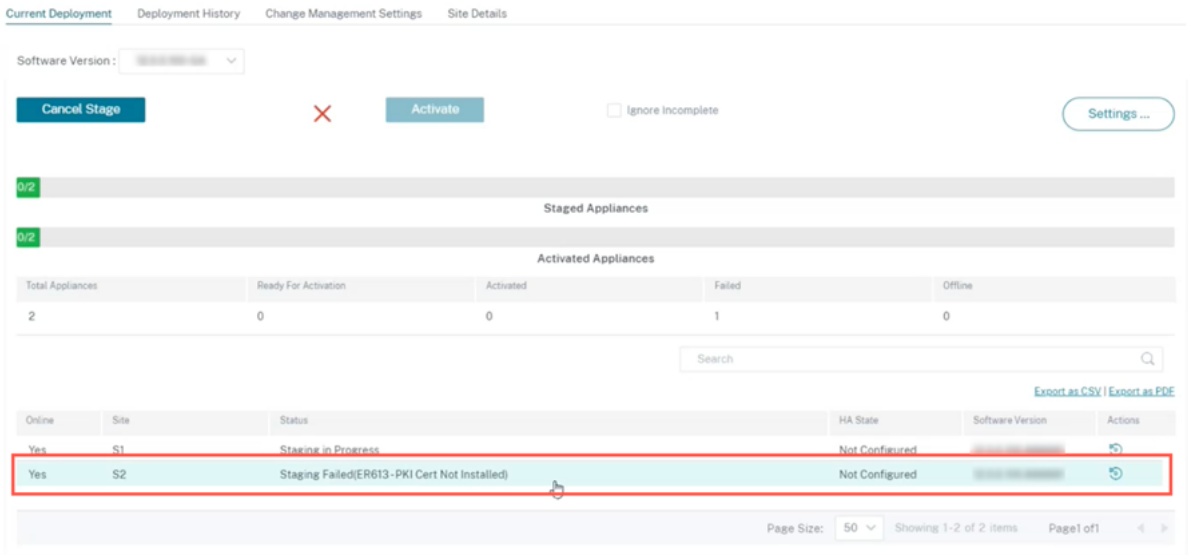
证书身份验证允许组织使用其私有证书颁发机构 (CA) 颁发的证书对设备进行身份验证。设备在建立虚拟路径之前进行身份验证。例如，如果分支设备尝试连接到数据中心，并且分支中心的证书与数据中心期望的证书不匹配，则不会建立虚拟路径。

CA 颁发的证书将公钥绑定到设备名称。公钥与证书标识的设备所拥有的相应私钥一起工作。

要启用设备身份验证，请在网络级别导航到 配置 > 安全 > 网络安全，然后选择 启用设备身份验证。单击保存。

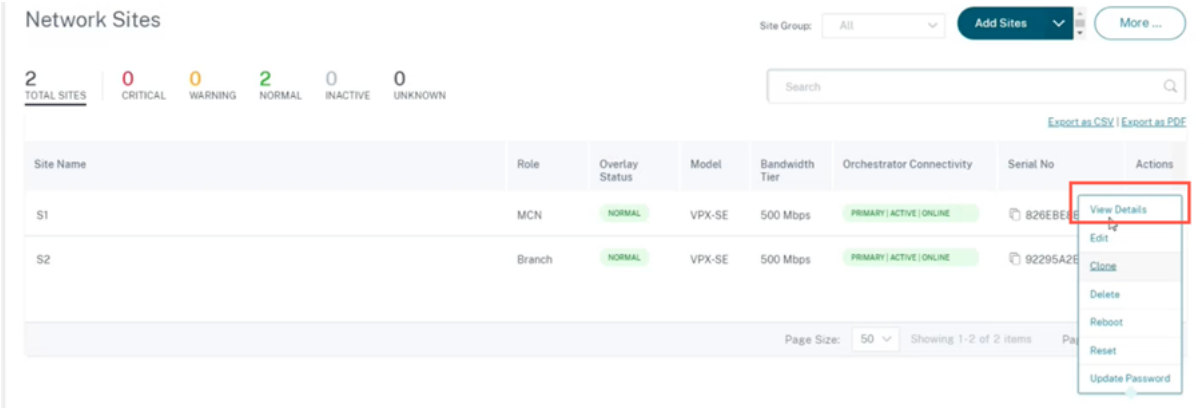


在部署期间，如果启用了设备身份验证，但设备中未安装 PKI 证书，则暂存会显示失败状态。

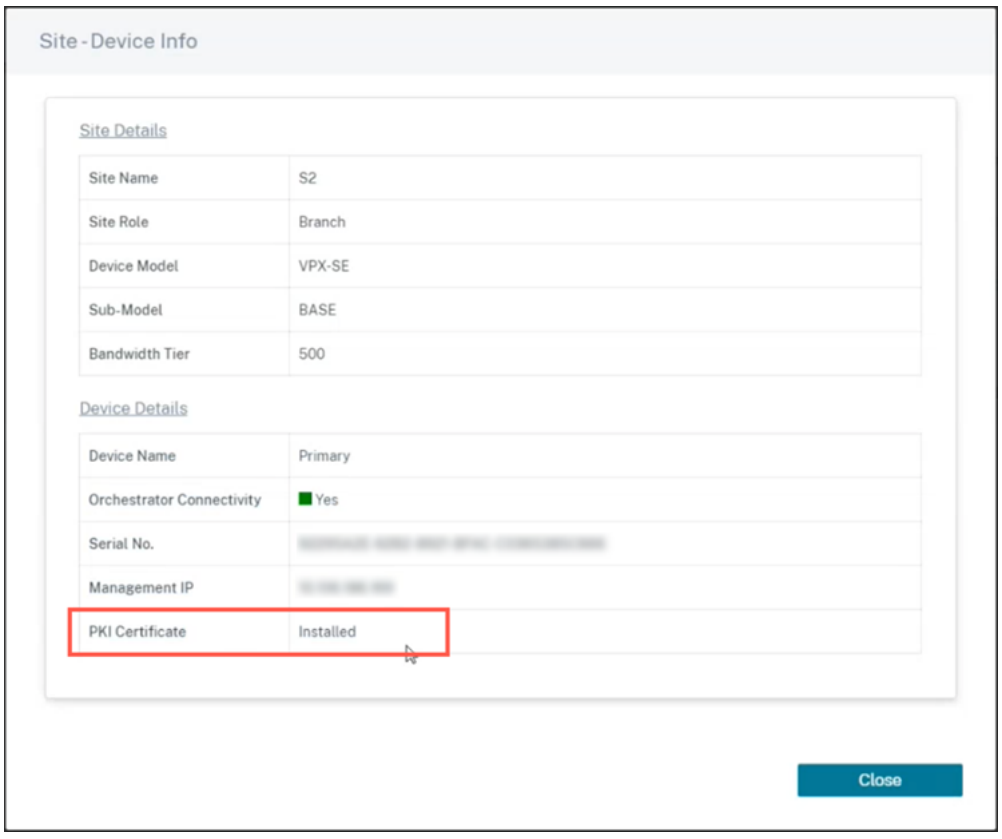


查看证书

您可以前往设备详细信息页面验证 PKI 证书是否已安装。为此，请导航到 配置 > 网络主页 > 单击要验证证书的站点的操作 符号，然后单击 查看详细信息。



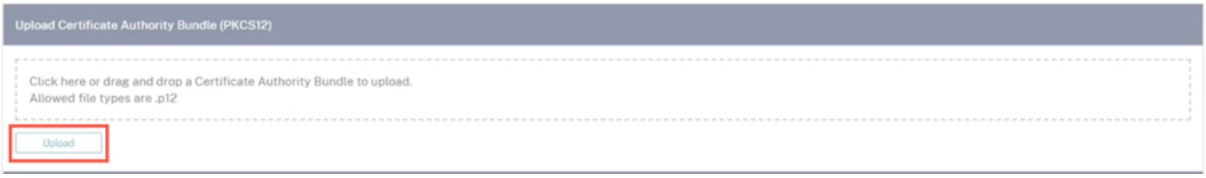
以下屏幕填充了站点和设备详细信息：



在“设备详细信息”部分下，您可以查看 PKI 证书安装状态。

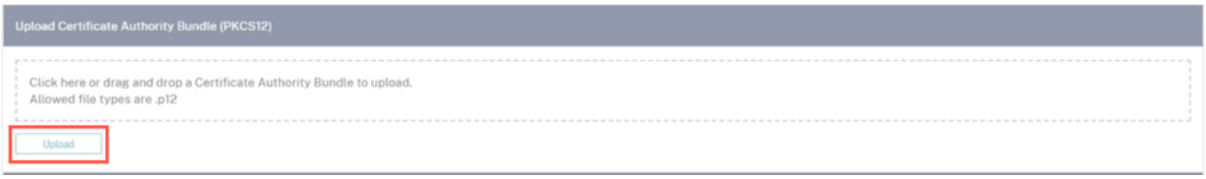
上载身份包

身份包包括私钥和与私钥关联的证书。您可以将 CA 颁发的设备证书上载到设备中。证书包是一个 PKCS12 文件，扩展名为.p12。您可以选择使用密码保护它。拖放 PKCS12 文件，输入密码并单击“上传”。如果将密码字段留空，则视为无密码保护。



上载证书颁发机构包

上传与证书签名机构对应的 PKCS12 包。证书颁发机构捆绑包包括完整的签名链、根签名和所有中间签名机构。拖动 PKCS12 捆绑包并点击 上传。



创建认证签名请求

设备可以生成未签名的证书并创建证书签名请求 (CSR)。要为设备创建 CSR，请提供组织名称、单位、城镇/市、省/地区/县/市、国家和电子邮件地址。设备常用名称是自动填充且不可编辑的站点名称。单击 **Create CSR**（创建 CSR）。

管理证书签名请求

成功从后端生成 CSR 后，您需要从设备下载 CSR 并由其 CA 签名，然后以 PEM 或 DER 格式将其上传回设备。这用作设备的身份证书。首先上传 CA 以签署证书。

上传 CA 后，上传已签名的 CSR。

证书吊销列表管理器

证书吊销列表 (CRL) 是在网络中不再有效的证书序列号的已发布列表。CRL 文件定期下载并在本地所有设备上存储。当验证证书时，响应程序会检查 CRL 以查看启动程序证书是否已被吊销。Citrix SD-WAN 目前支持 PEM 和 DER 格式的版本 1 CRL。

要启用 CRL，请选中“启用 CRL”复选框。提供 CRL 文件的维护位置。支持 HTTP、HTTPS 和 FTP 位置。指定检查和下载 CRL 文件的时间间隔，范围为 1—1440 分钟。单击“上传设置”。

> 注意
>
> virtua1 路径的重新身份验证周期可能在 10 到 15 分钟之间，如果 CRL 更新间隔设置为较短的持续时间，则更新的 CRL 列表可能包含当前有效的序列号。让被主动吊销的证书在短时间内在您的网络中可用。

移动宽带设置

Citrix SD-WAN Orchestrator 服务允许您使用移动宽带连接将 Citrix SD-WAN 设备从分支站点连接到网络。

要配置移动宽带设置，请在站点级别导航到 配置 > 设备设置 > 移动宽带设置。

目前，可以在 Citrix SD-WAN 110 和 Citrix SD-WAN-210 设备上配置移动宽带设置。

您可以在 Citrix SD-WAN Orchestrator 服务上配置以下移动宽带设置。

SIM PIN 状态

如果您插入了使用 PIN 锁定的 SIM 卡，则 SIM 卡的状态为“启用”。在使用 SIM 卡进行验证之前，您无法使用 SIM PIN。您可以从运营商处获取 SIM PIN。单击 **Verify**（验证）。

输入运营商提供的 SIM PIN，然后单击验证。

禁用 **SIM PIN**　对于已启用并验证 SIM PIN 的 SIM 卡，您可以禁用 SIM PIN 功能。单击禁用。输入 SIM PIN，然后单击禁用。

启用 **SIM PIN**　要启用 SIM PIN，请单击“启用”。输入运营商提供的 SIM PIN，然后单击启用。

如果 SIM PIN 状态更改为“已 启用”和“未验证”，则表示 PIN 未经过验证，并且在 PIN 通过验证之前您无法执行任何操作。

单击 验证 **PIN**。输入运营商提供的 SIM PIN，然后单击 验证 **PIN** 码。

修改 **SIM PIN**　PIN 处于“已 启用”和“已验证”状态后，您可以选择更改 PIN。

单击 **Modify**（修改）。输入运营商提供的 SIM PIN。输入新的 SIM PIN 并进行确认。单击 **Modify**（修改）。

取消阻止 **SIM** 卡　如果您忘记了 SIM PIN，可以使用从运营商获得的 SIM PUK 重置 SIM PIN。

要取消阻止 SIM 卡，请单击 取消阻止。输入从运营商处获取的 SIM PIN 和 SIM 卡 PUK，然后单击解除封锁。

> 注意
>
> SIM 卡被永久封锁，因为 10 次尝试 PUK 失败，同时取消阻止 SIM 卡。请联系运营商以获取新的 SIM 卡。

APN 设置

要配置 APN 设置，请输入运营商提供的 APN、用户名、密码和身份验证。您可以从 **PAP**、CHA**P** 或 P **APCHAP** 身份验证协议中进行选择。如果运营商未提供任何身份验证类型，请将其设置为无。

网络设置

您可以在支持内部调制解调器的 Citrix SD-WAN 设备上选择移动网络。

漫游

默认情况下，漫游选项在您的设备上处于启用状态。你可以选择禁用它。

管理固件

每个启用了 LTE 的设备都将拥有一组可用固件。您可以从现有的固件列表中选择或上载固件并应用它。如果您不确定要使用哪个固件，请选择 AUTO-SIM 选项，允许 LTE 调制解调器根据设备中插入的 SIM 卡选择最匹配的固件。

> 注意
>
> 目前，该固件只能应用于 SD-WAN SE 210 LTE 设备。

启用/禁用调制解调器

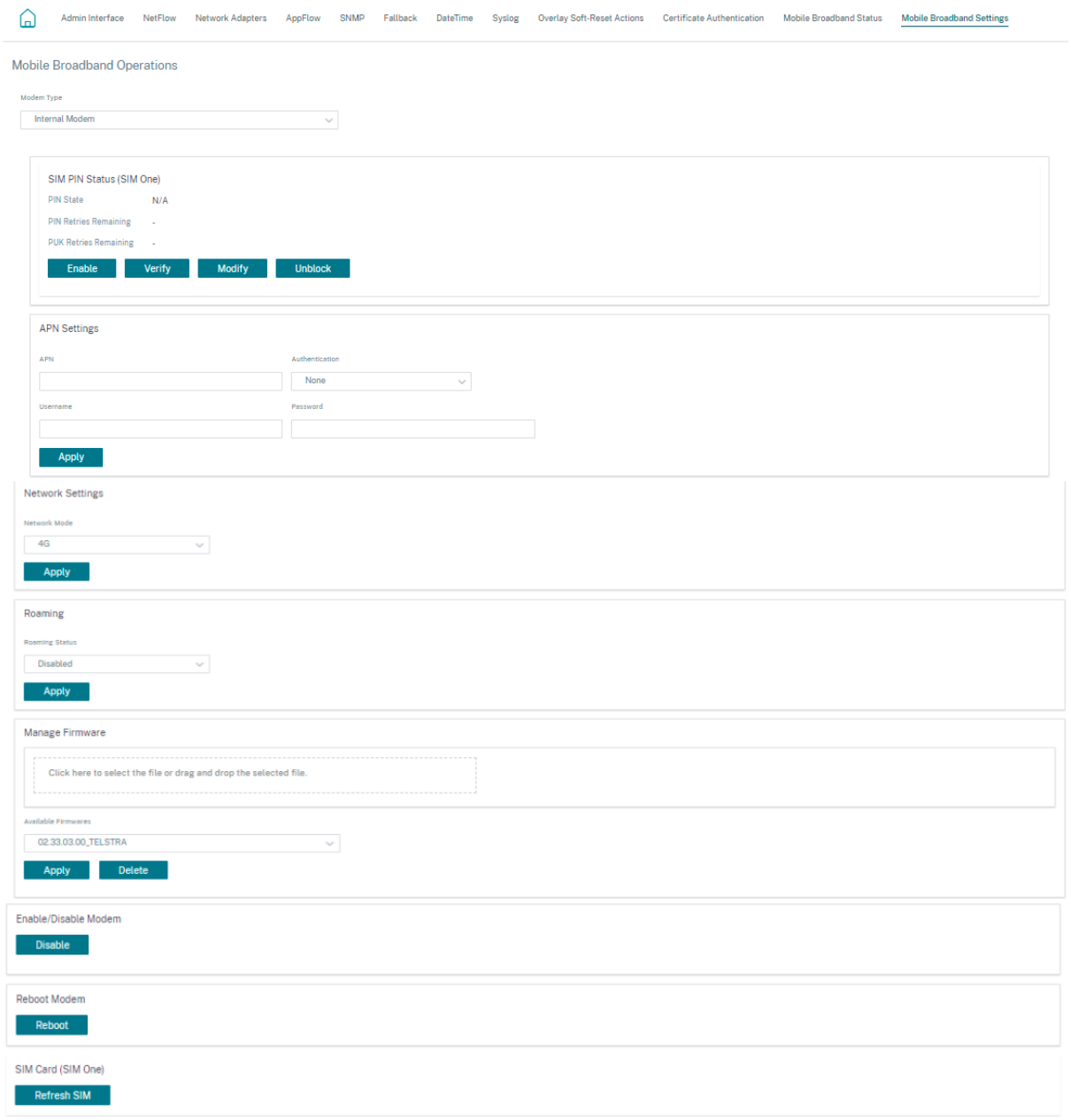
根据您使用宽带功能的意图启用或禁用调制解调器。默认情况下，调制解调器处于启用状态。

重启调制解调器

重新启动调制解调器。此过程最多可能需要 3-5 分钟才能完成重启操作。

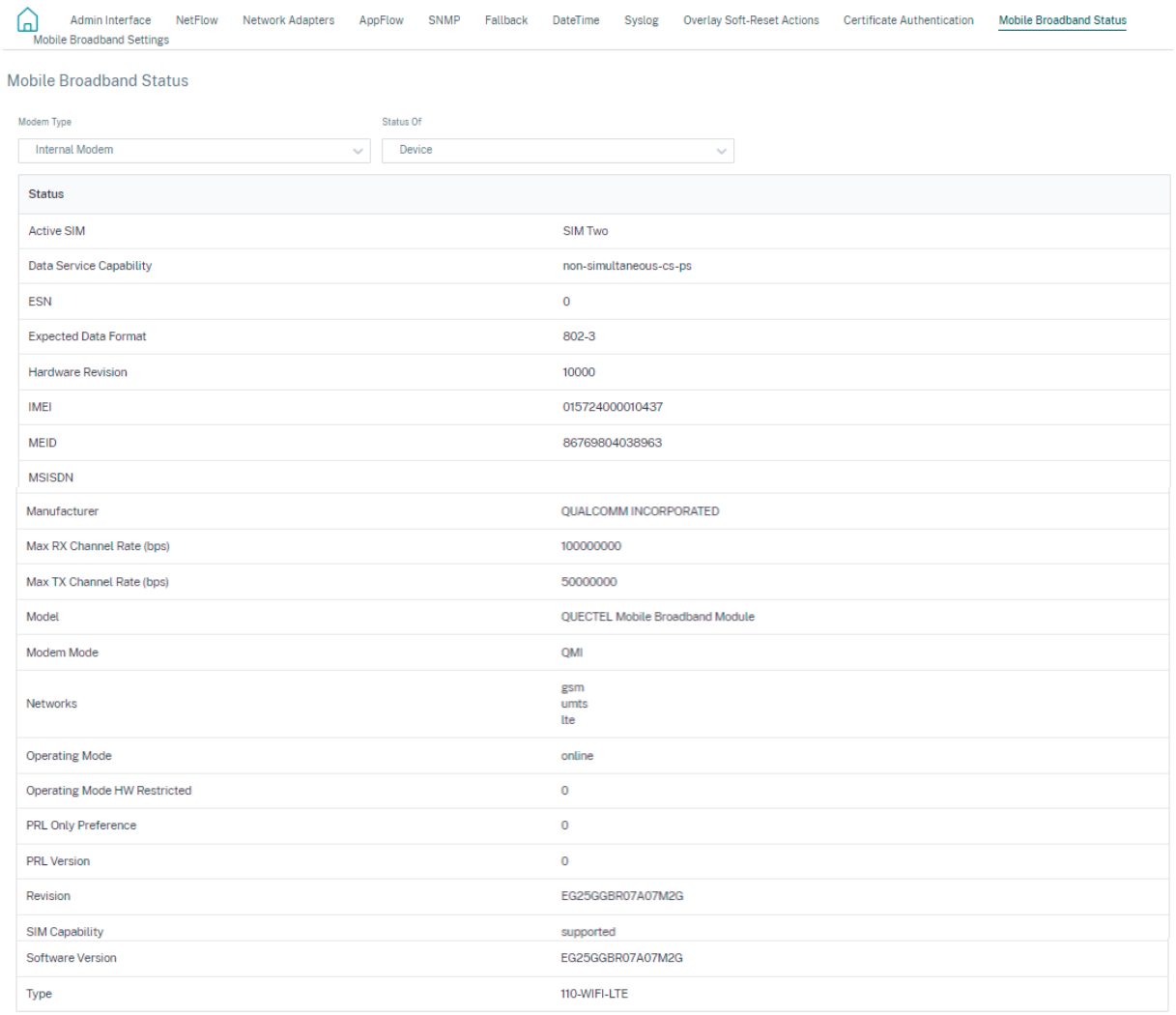
刷新 **SIM** 卡

当您热插拔 SIM 卡以检测新的 SIM 卡时，请使用此选项。



移动宽带状态

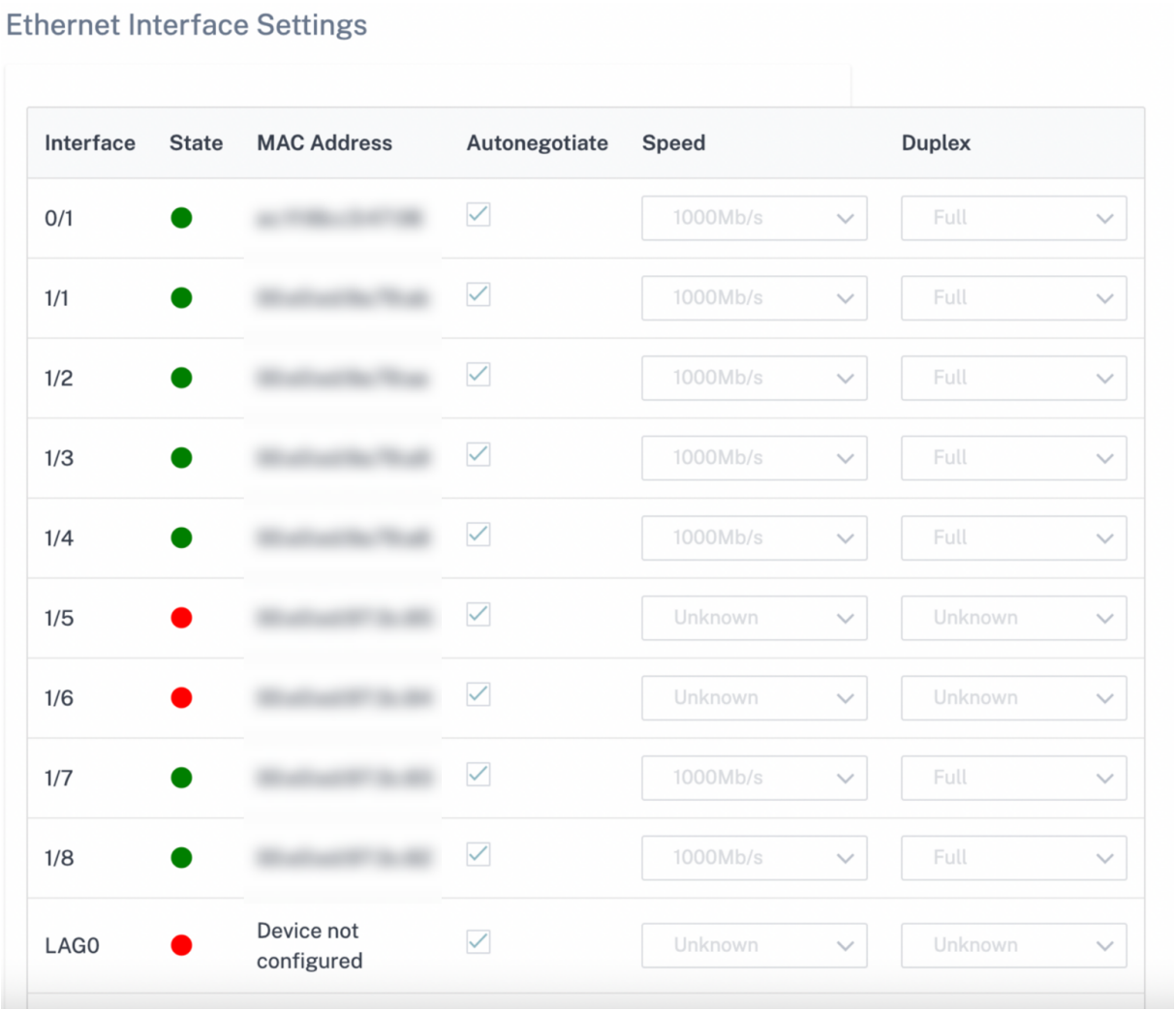
移动宽带状态部分显示您的宽带配置设置的状态。要查看移动宽带状态，请在站点级别导航到 配置 > 设备设置 > 移动宽带状态。您可以查看设备和活动的 SIM 卡的状态。



以太网接口设置

以太网接口状态部分显示以太网端口的连接状态、接口类型、MAC 地址、自动协商和双工设置信息。要查看以太网接口设置，请在站点级别导航到 配置 > 设备设置 > 以太网接口设置。管理性关闭的端口以红色表示。

> 注意
>
> 此设置目前在 Citrix SD-WAN Orchestrator 服务用户界面上以只读模式可用。如果要修改以太网接口设置，可以使用 SD-WAN 设备的新用户界面进行修改。



带内管理

October 21, 2022

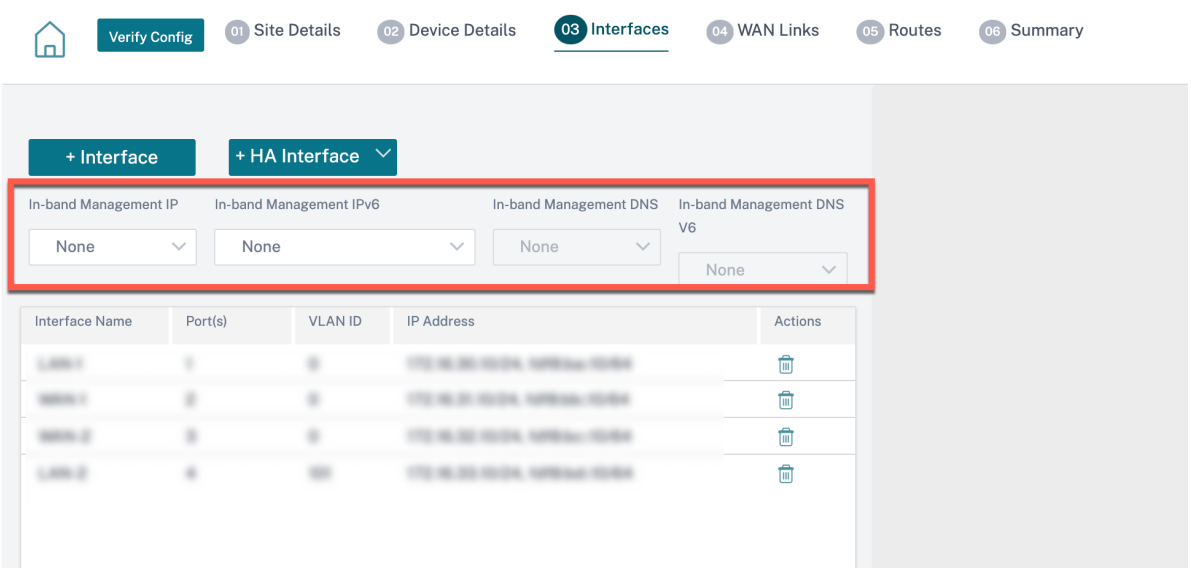
Citrix SD-WAN Orchestrator 服务允许您通过两种方式管理 SD-WAN 设备：带外管理和带内管理。带外管理允许您使用为管理保留的端口创建管理 IP，该端口仅承载管理流量。带内管理允许您使用 SD-WAN 数据端口进行管理。它同时承载数据和管理流量，而无需配置添加管理路径。

带内管理允许虚拟 IP 地址连接到管理服务，如 Web UI 和 SSH。您可以在已启用用于 IP 服务的可信接口上启用带内管理。您可以使用管理 IP 和带内虚拟 IP 访问 Web UI 和 SSH。

> 注意
>
> Citrix SD-WAN 11.1.1 及更高版本支持 Citrix SD-WAN Orchestrator 服务中的带内管理。

要在虚拟 IP 上启用带内管理，请在站点级别导航到 配置 > 站点配置 > 接口。选择要用作带内管理端口的虚拟 IP。您可以使用 带内管理 **IP** 或带内管理 **IPv6** 来访问 Web 用户界面和 SSH。

> 注意
>
> 仅局域网端口支持带内管理。



有关配置虚拟 IP 地址的详细步骤，请参阅 接口。

带内管理 IP 也充当备份管理 IP。如果管理端口未使用默认 Gateway 配置，则将用作管理 IP 地址。选择通过带内管理平面将所有 DNS 请求转发到的 DNS 代理。有关配置 DNS 代理的信息，请参阅 DNS 代理。

对于设备与 Citrix SD-WAN Orchestrator 服务的连接在管理端口和带内端口之间切换的用例，请配置带内 管理 **DNS** 或带内管理 **DNS V6** 以确保 Citrix SD-WAN Orchestrator 服务连接不间断。

带内 **Provisioning**

在家庭或小型分支机构等较简单的环境中部署 SD-WAN 设备的需求显著增加。为更简单的部署配置单独的管理访问权限是额外的开销。零接触部署以及带内管理功能可以通过指定的数据端口进行 Provisioning 和配置管理。指定的数据端口支持零接触部署，无需使用单独的管理端口进行零接触部署。

您可以将设备处于出厂发货状态，通过将数据或管理端口连接到互联网来支持带内 Provisioning 备。支持带内 Provisioning 的设备具有用于 LAN 和 WAN 的特定端口。处于恢复出厂设置状态的设备具有允许与零接触部署服务建立连接的默认配置。LAN 端口充当 DHCP 服务器，并将动态 IP 分配给充当 DHCP 客户端的 WAN 端口。WAN 链路监视四 9 DNS 服务以确定 WAN 连接性。

获取 IP 地址并与零接触部署服务建立连接后，将下载配置包并安装在设备上。有关通过 Citrix SD-WAN Orchestrator 服务进行零接触部署的信息，请参阅 零接触部署。

> 注意
>
> - 带内 Provisioning 适用于所有平台。但是，默认配置仅在 Citrix SD-WAN 110 和 VPX 平台上启用，因为其他平台随附较旧的软件版本。
> - 对于通过数据端口在 0 天 Provisioning SD-WAN 设备，设备软件版本必须为 Citrix SD-WAN 11.1.1 或更高版本。

处于出厂重置状态的设备的默认配置包括以下配置：

- LAN 端口上的 DHCP 服务器
- WAN 端口上的 DHCP 客户端
- 适用于 DNS 的 QUAD9 配置
- 对于具有出厂映像 11.1.1.39 的 Citrix SD-WAN 设备，默认局域网 IP 为 192.168.101.1/24。
- 对于具有出厂映像 11.0.4 的 Citrix SD-WAN 110 设备，默认局域网 IP 为 192.168.0.1/24。
- 35 天的宽限许可证。

置备设备后，默认配置将被禁用并被从零接触部署服务接收的配置覆盖。如果设备许可证或宽限许可证过期，则会激活默认配置，以确保设备保持与零接触部署服务的连接并接收许可证托管服务。

回退配置

回退配置可确保在发生链路故障、配置不匹配或软件不匹配时设备保持与零接触部署服务的连接。默认情况下，在具有默认配置文件的设备上启用回退配置。您还可以根据现有 LAN 网络设置编辑备用配置。

在以下情况下，备用配置通过设备带内管理 IP 和 Citrix SD-WAN Orchestrator 服务保留与设备的连接：

- t2_app 在哪里崩溃
- 你尝试执行配置重置

在这种情况下，设备配置了带内管理，您执行了手动配置重置，或者由于用户配置，t2_app 在 120 秒内崩溃了四次以上。在这样的框架中，该服务被禁用，因此您失去了与 Citrix SD-WAN Orchestrator 服务和设备的连接。

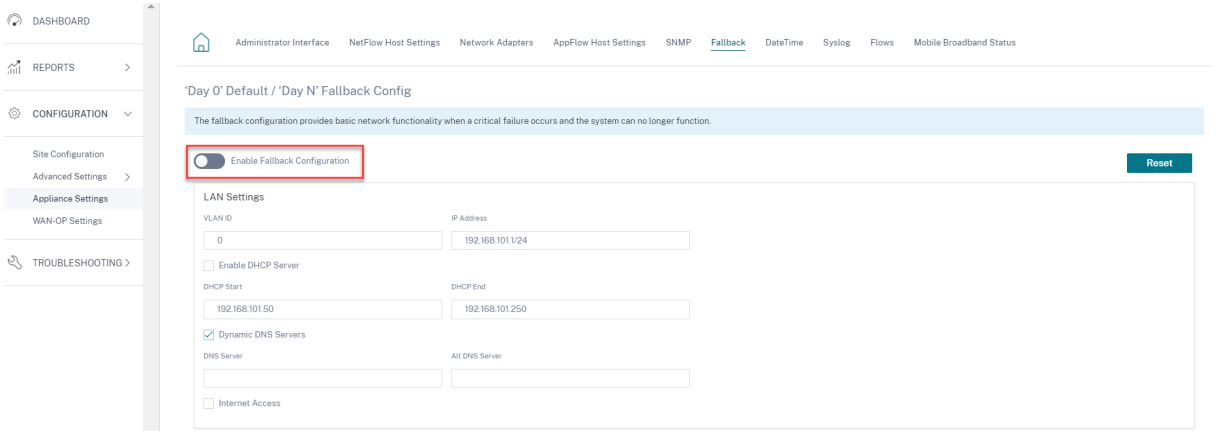
但是，如果您启用了备用配置，则可以获得以下功能：

- 对管理功能（Web UI/SSH/SNMP）的基本带内访问
- 设备能够通过带内端口（Citrix SD-WAN Orchestrator 服务/ZTD）连接到外部服务

对于此类情况，不是禁用服务设备，而是使用启用服务的回退配置。只要链接具有互联网连接，通过带内管理 IP 与 Citrix SD-WAN Orchestrator 服务和设备的连接就会保持不变。

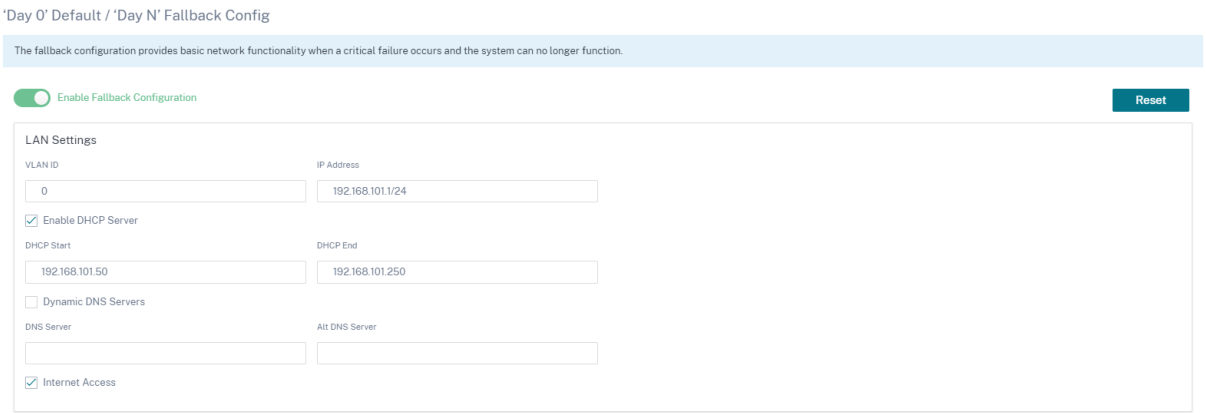
> 注意
>
> 初始设备配置完成后，确保启用备用配置以实现零接触部署服务连接。

如果禁用了备用配置，则可以通过站点级别的 Citrix SD-WAN Orchestrator 服务将其启用，方法是导航到 配置 > 设备设置 > 回退 并单击“启用回退 配置”。



要根据您的局域网自定义备用配置，请根据您的网络要求编辑以下 LAN 设置的值。这是与零接触部署服务建立连接所需的最低配置。

- **VLAN ID**：局域网端口必须分组到的 VLAN ID。
- **IP** 地址：分配给 LAN 端口的虚拟 IP 地址。
- 启用 **DHCP** 服务器：启用局域网端口作为 DHCP 服务器。DHCP 服务器将动态 IP 地址分配给 WAN 端口。
- **DHCP** 起始点和 **DHCP** 结束：DHCP 用来为广域网端口动态分配 IP 的 IP 地址范围。
- 动态 **DNS** 服务器：启用 LAN 端口作为域名服务器。
- **DNS** 服务器：主 DNS 服务器的 IP 地址。
- **Alt DNS** 服务器：辅助 DNS 服务器的 IP 地址。
- 互联网访问：允许所有 LAN 客户端访问互联网，无需其他过滤。

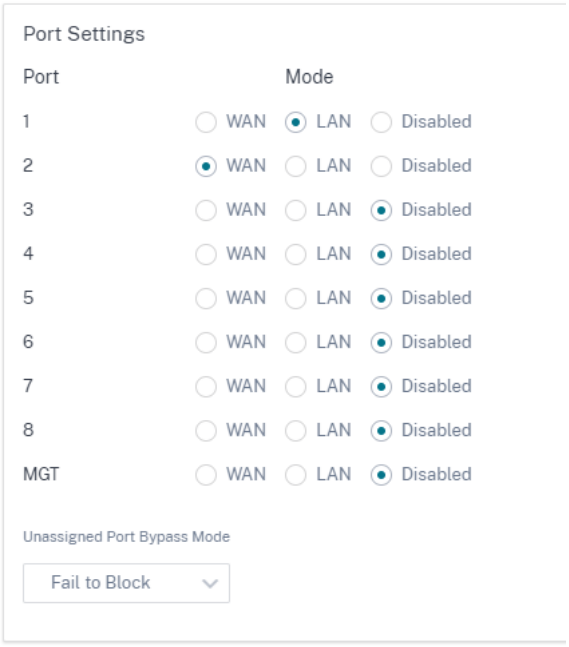


为每个端口配置模式。该端口可以是 LAN 端口或 WAN 端口，也可以禁用。显示的端口取决于设备型号。此外，将端口旁路模式设置为“故障到阻止”或“故障到线”。

下表提供了在不同平台上用于备用配置的预先指定 WAN 和 LAN 端口的详细信息：

平台	WAN 端口	LAN 端口
110	1/2	1/1

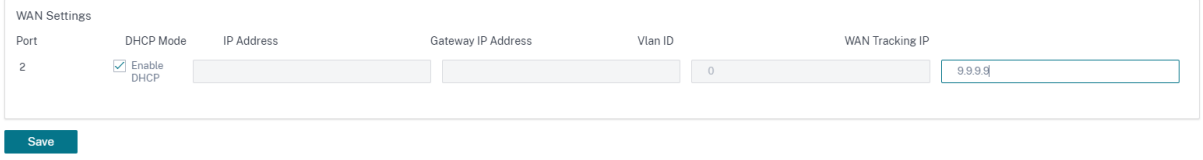
平台	WAN 端口	LAN 端口
110-LTE	1/2，LTE-1	1/1
210	1/4, 1/5	1/3
210-LTE	1/4、1/5、LTE-1	1/3
VPX	2	1
410	1/4, 1/5, 1/6	1/3 (FTB)
1100	1/4, 1/5, 1/6	1/3 (FTB)



可以使用 DHCP 客户端将 WAN 端口配置为独立的 WAN 链路，并监控 Quad9 DNS 服务以确定 WAN 连接。在没有 DHCP 的情况下，您可以为 WAN 端口配置 WAN IPS/静态 IP，以便使用带内管理进行初始配置。

> 注意
>
> 您只能使用静态 IP 配置以太网端口。静态 IP 无法使用 LTE-1 和 LTE-E1 端口进行配置。尽管您可以将 LTE-1 和 LTE-E1 端口添加为 WAN，但配置字段仍然是不可编辑的。

当您添加 WAN 端口时，它会被添加到 **WAN** 设置（端口：**2**）部分下，默认情况下，启用 **DHCP** 复选框处于选中状态。如果选中 **DHCP** 模式 复选框，则 **IP** 地址、网关 **IP** 地址和 **VLAN ID** 文本字段将显示为灰色。如果要配置静态 IP，请清除“启用 **DHCP**”复选框。



默认情况下，**WAN** 跟踪 **IP** 地址 字段自动填充 9.9.9.9。您可以根据需要更改地址。

> 注意
>
> 如果选中“动态 **DNS** 服务器”复选框，请确保在选中 D **HCP** 模式 的情况下添加/配置至少一个 WAN 端口。

要随时将回退配置重置为默认配置，请单击 重置。

> 注意
>
> 建议在通过连接到 LAN 子网的带内/管理端口连接到 Orchestrator 的所有设备上启用备用配置。确保根据您的网络子网要求设置默认备用配置。

端口切换

Citrix SD-WAN Orchestrator 服务还允许在数据端口关闭时将管理流量无缝故障转移到管理端口，反之亦然。如果设备可以通过管理端口和带内端口连接到互联网，则选择管理端口进行零接触部署。

重新启动设备时，如果可以通过带内端口而不是管理端口访问互联网，则设备将立即连接到 Citrix SD-WAN Orchestrator 服务。

建立连接后，在设备上运行的服务代理每 10 秒钟将心跳信息发送到 Citrix SD-WAN Orchestrator 服务。如果 Citrix SD-WAN Orchestrator 服务在 5 分钟内没有收到心跳信号，则会激活带内端口故障转移。Citrix SD-WAN Orchestrator 服务在此期间将设备报告为脱机。

重新启动设备时，如果管理端口和带内端口都无法使用 Internet，并且重新建立 Internet 连接后，服务代理大约需要 5 分钟的时间重新启动并建立连接。

确保在网络级别“配置”> “交付服务”> “互联网”启用“即使所有关联路径均处于关闭状态，也保留从链接到互联网的路由”选项。确保即使虚拟路径出现故障，也能保持与 Citrix SD-WAN Orchestrator 服务的连接。

可配置的管理或数据端口

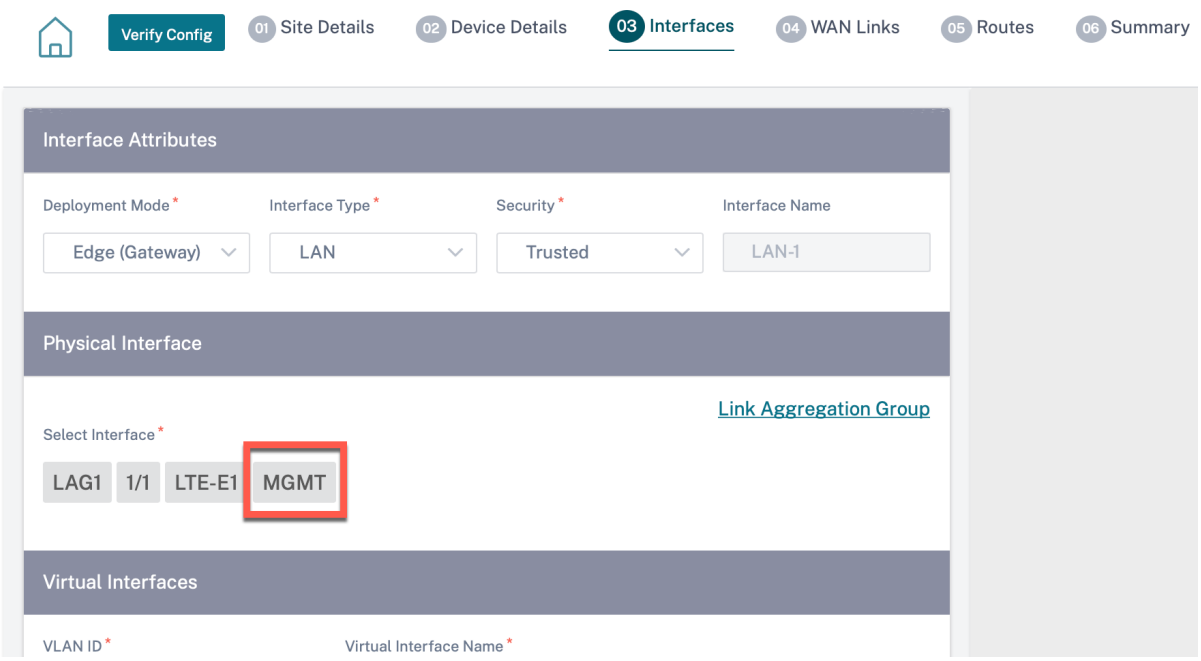
带内管理允许数据端口同时传输数据和管理流量，无需使用专用管理端口。它使管理端口在已经具有较低端端口密度的低端设备上未使用。Citrix SD-WAN 允许您将管理端口配置为作为数据端口或管理端口运行。

> 注意
>
> 您只能在以下平台上将管理端口转换为数据端口。
>
> - Citrix SD-WAN 110 SE/LTE
> - Citrix SD-WAN 210 SE/LTE

配置站点时，请在配置中使用管理端口。激活配置后，管理端口将转换为数据端口。

> 注意
>
> 只有在设备上其他受信任接口上启用带内管理时，才能配置管理端口。

要配置管理接口，请在站点级别导航到 配置 **>** 站点配置 ** **>** ** 接口，然后选择 MGMT 接口。有关配置接口组的更多信息，请参阅 接口。



要重新配置管理端口以执行管理功能，请删除配置。在不使用管理端口的情况下创建配置并将其激活。

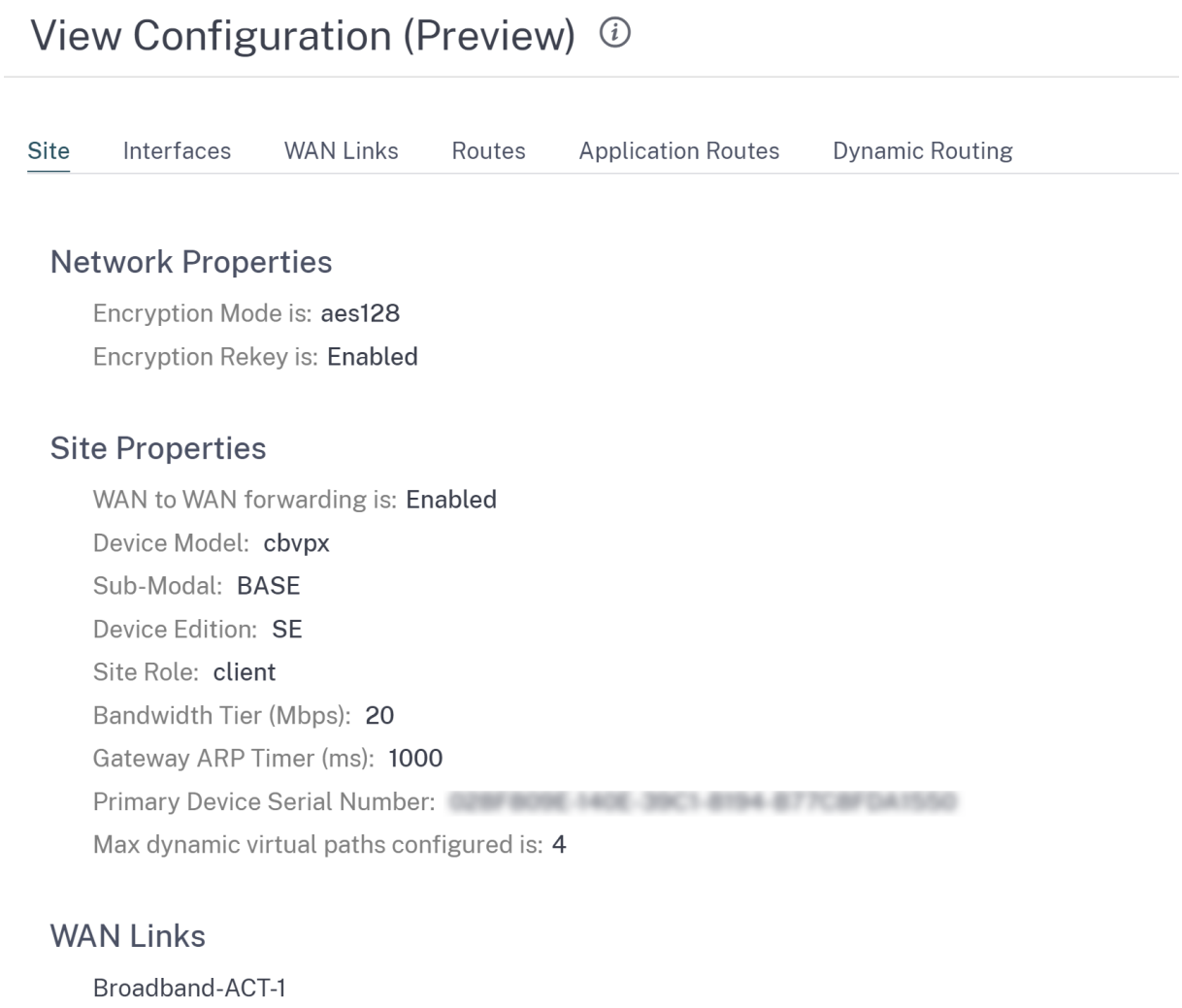
查看配置（预览）

October 21, 2022

查看配置 页面提供站点配置设置的合并摘要。要查看配置，请在站点级别导航到 配置 > 查看配置。有关站点配置的更多信息，请参阅 站点配置。

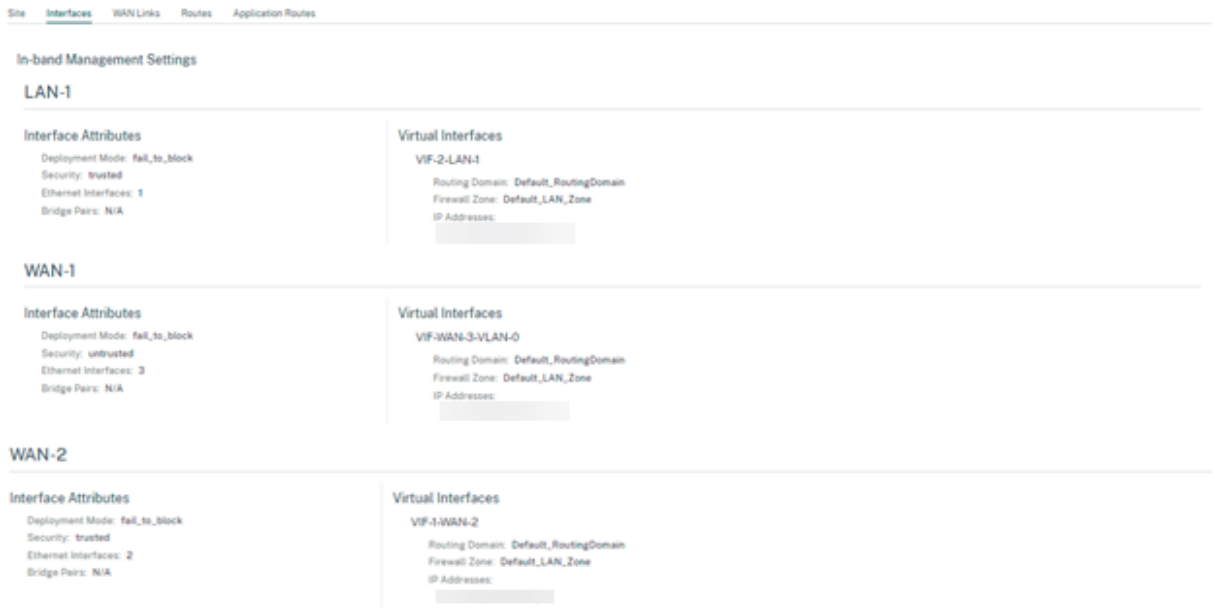
站点

站点 页面显示站点详细信息的摘要。站点摘要包括网络属性、站点属性和广域网链接状态。要查看站点配置的详细信息，请导航到 配置 > 查看配置 > 站点。



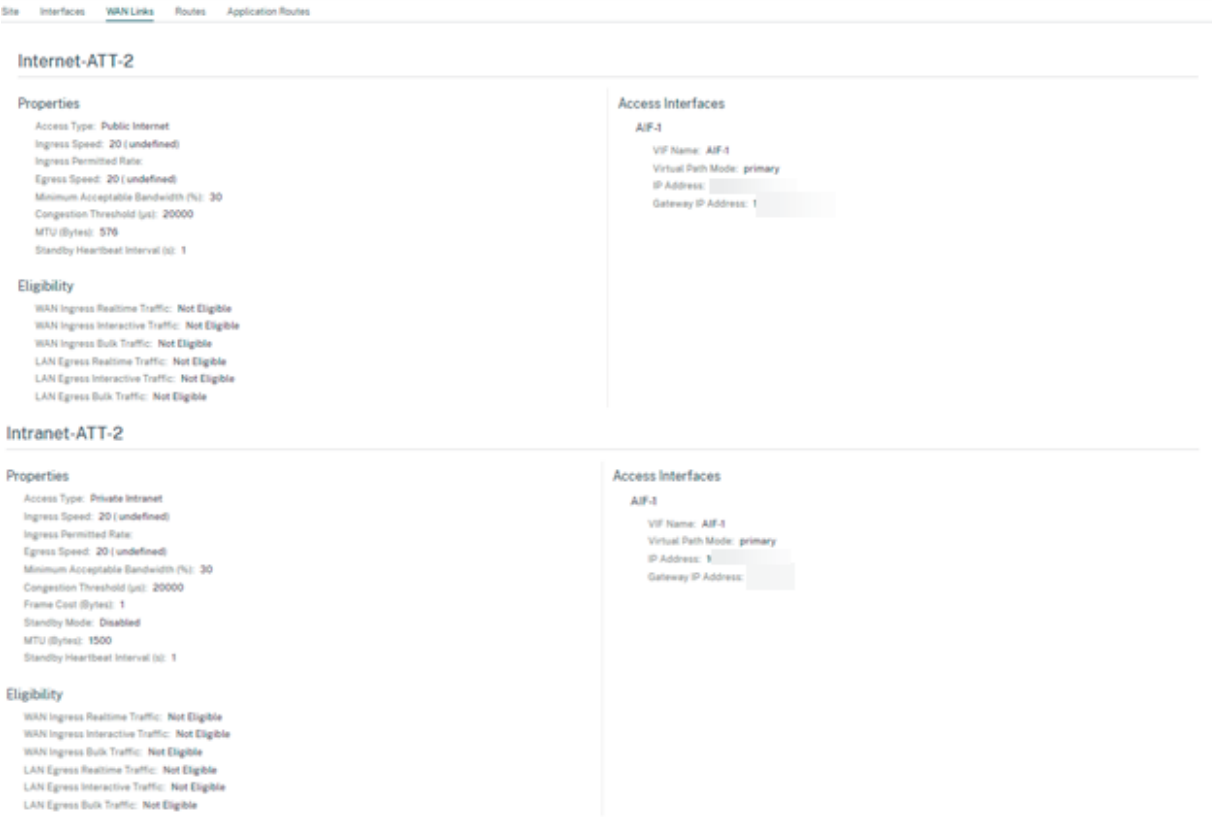
接口

接口 页面显示已配置接口的摘要。要查看虚拟接口的配置详细信息，请导航到 配置 > 查看配置 > 接口。



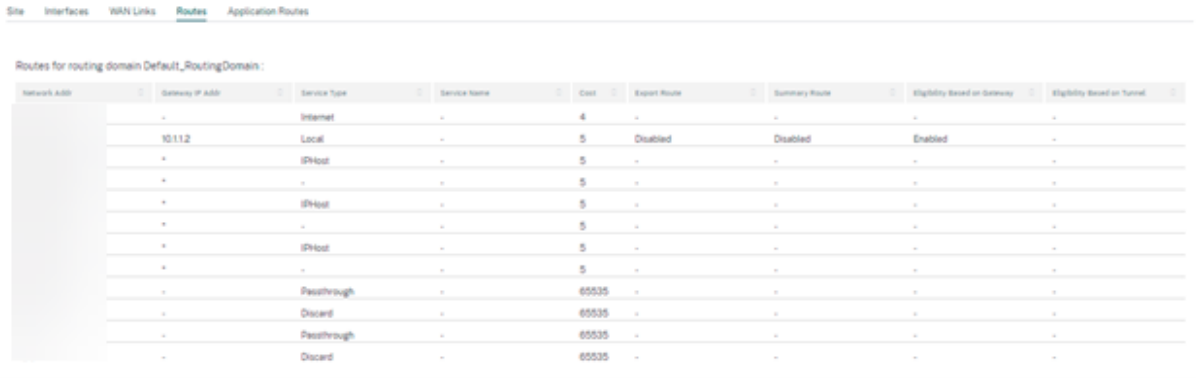
WAN 链接

要查看已配置 WAN 链接的配置详细信息，请导航到 配置 > 查看配置 > **WAN** 链接。



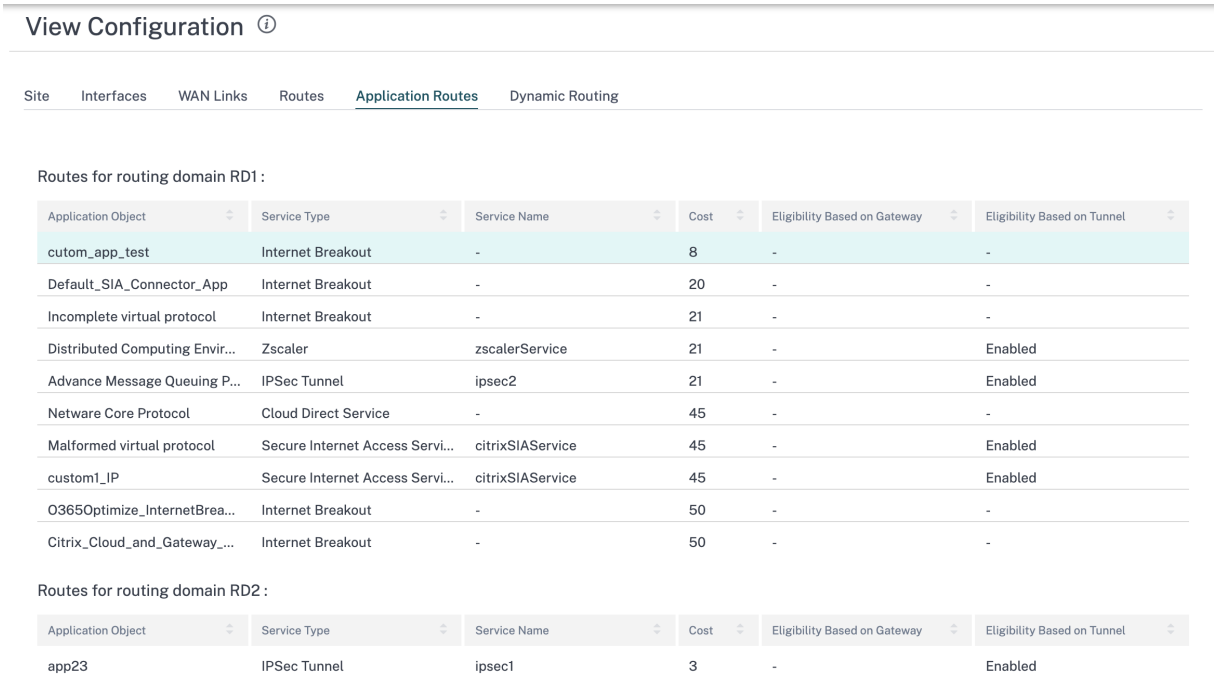
路由

要查看创建的 IP 路由的路由信息，请导航到 配置 > 查看配置 > 路由。



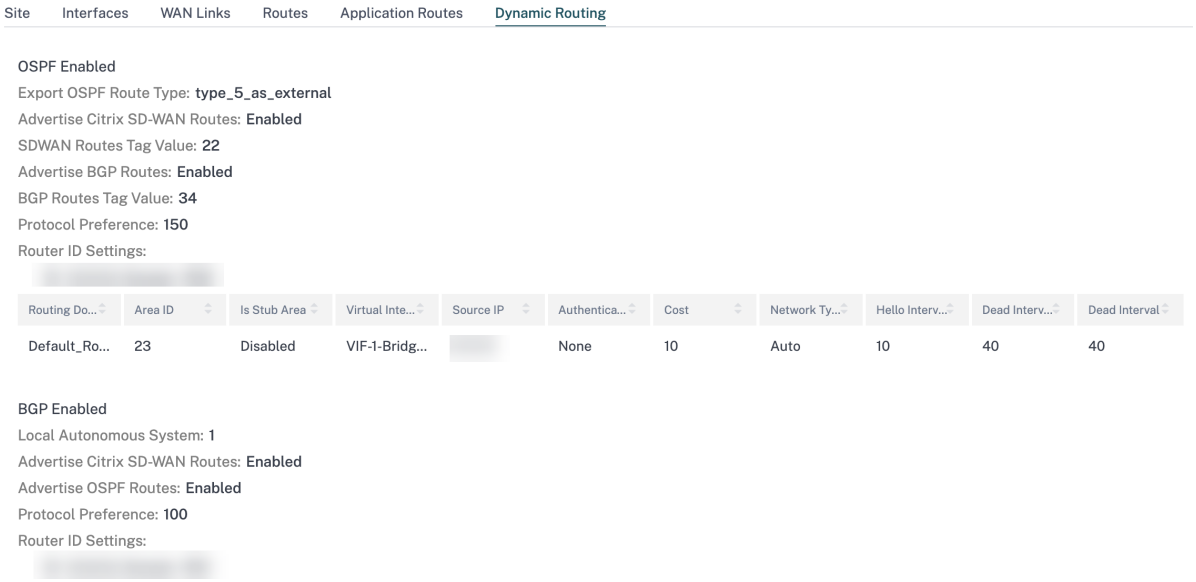
申请路线

要查看有关特定应用程序路由的摘要，请导航到 配置 > 查看配置 > 应用程序路由。



动态路由

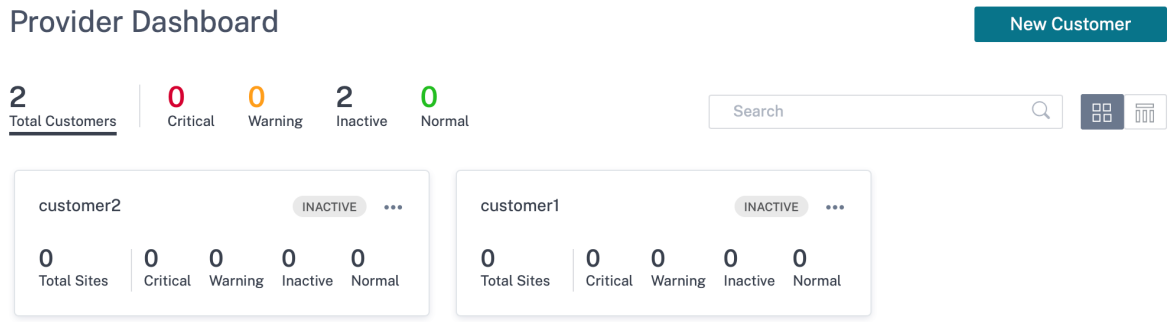
要查看 OSPF、BGP、导入筛选器和导出筛选器配置的摘要，请导航到 配置 > 查看配置 > 动态路由。



提供程序控制板

November 16, 2020

当您以 Citrix 合作伙伴身份登录时，将显示提供程序仪表板。它为服务提供商管理的所有 SD-WAN 客户提供鸟瞰图。



提供了每个客户的 SD-WAN 网络的具有颜色编码的运行状况快照，并提供了一种置备以深入了解特定于客户的详细信息。仪表板在磁贴视图和列表视图中均可用。

用于客户网络的颜色编码标准是：

- 严重（红色）：一个或多个站点已关闭
- 警告（橙色）：所有站点都未关闭，但有一个或多个严重警报。
- 正常（绿色）：所有站点都未关闭，并且没有严重警报。
- 非活动（灰色）：正在配置网络，但尚未部署。

颜色编码标准允许管理员专注于需要他们关注的客户。

客户/网络控制面板

July 10, 2024

网络控制面板提供组织的 SD-WAN 网络的运行状况和所有站点使用情况的鸟瞰图。仪表板可捕获整个网络的警报摘要、覆盖层和底层路径的正常运行时间，突出显示使用趋势，并提供网络的全局视图。

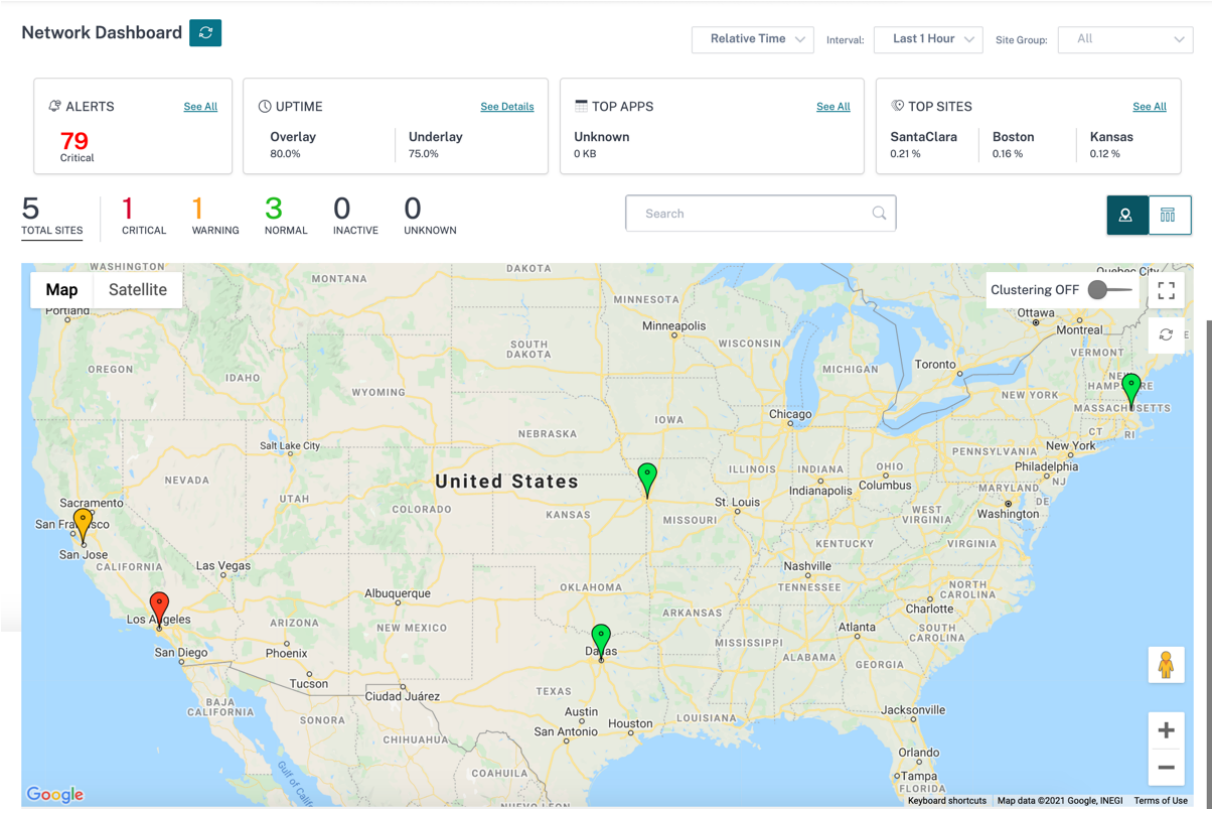
仪表板汇总了网络的以下方面，并附有一条规定可以深入了解更多详细信息。

- 严重警报：网络上弹出的严重运行状况警报（如果有）的运行次数。
- 正常运行时间：将 SD-WAN 虚拟覆盖网络提供的平均正常运行时间与物理底层网络提供的平均正常运行时间进行并行比较
- 使用趋势：热门应用程序（基于流量）和热门站点（基于容量利用率）。
- 网络视图：网络中所有站点的可视化表示，在地图视图和列表视图中均可用。

控制面板列出了网络中的站点总数，还根据站点的连接状态对站点进行了隔离。选择带编号的链接，根据以下状态类别查看站点：

- 关键 -所有关联虚拟路径均处于关闭状态的站点。
- 警告 -至少有一条虚拟路径处于关闭状态的站点。
- 正常 -站点的所有虚拟路径和关联的成员路径均已启动。
- 非活动-处于 未部署和非活动状态的站点。
- 未知 -站点状态未知。

单击状态会根据站点的状态筛选站点并显示详细信息。您还可以使用 搜索 栏根据站点名称、角色、覆盖连接、型号、带宽层和序列号参数查看站点的详细信息。



该地图提供了全球网络的实时视图，该组织的所有地点根据其位置在世界地图上描绘出来。每个站点的颜色反映了其当前的健康状况。

以下是每个站点使用的颜色编码标准：

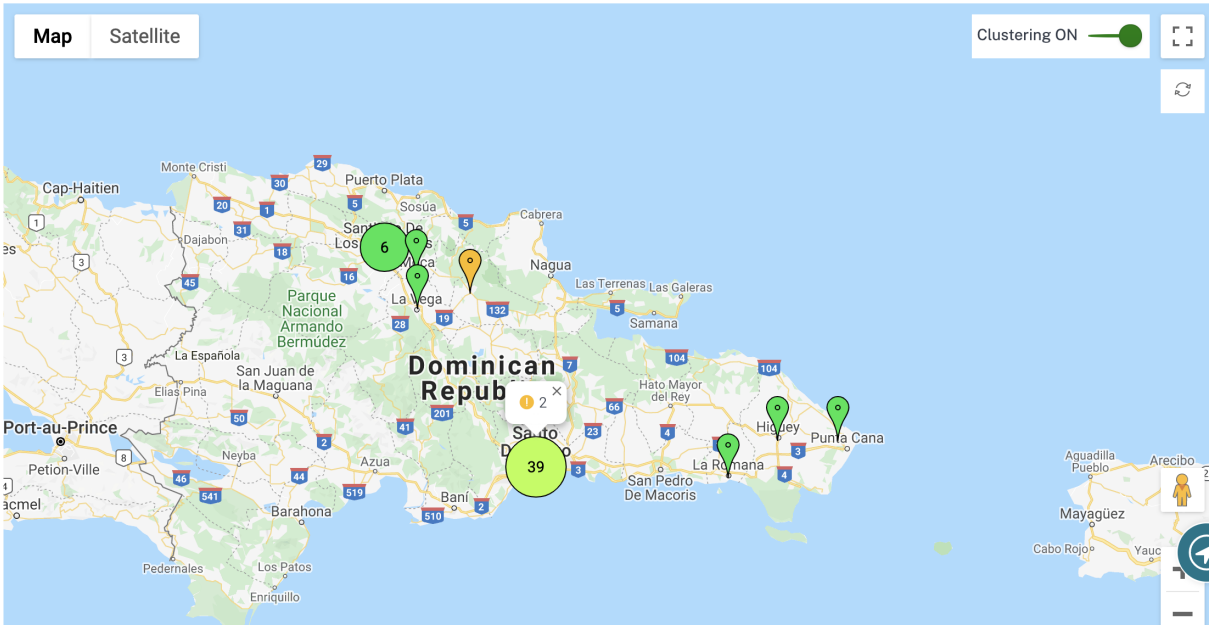
- 严重（红色）：至少有一条与站点关联的叠加 虚拟路径 处于关闭状态。
- 警告（橙色）：至少有一条底层成员路径处于 DOWN 状态，但所有叠加虚拟路径均为 UP。
- 正常（绿色）：所有叠加虚拟路径和关联的底层成员路径均为 UP。
- 非活动（灰色）：站点配置不足，尚未部署。

将鼠标悬停在任何站点上时，将显示一些特定于站点的关键详细信息，例如站点角色、设备型号、带宽层。与网站相关的虚拟路径显示了反映其健康状况的适当颜色代码。列表视图 为每个站点提供相同的详细信息，汇总为表格中的条目。

群集

Clustering **ON** 功能可监控集群或集群组合的各个站点的一致性、状态和运行状况。Clustering ON 服务提供站点的实时视图，有助于监控站点的故障转移和当前状态。

引入了 “开启集群”功能来管理高密度的站点。当有数千个站点时，不建议使用关闭群集选项，这也会降低性能。



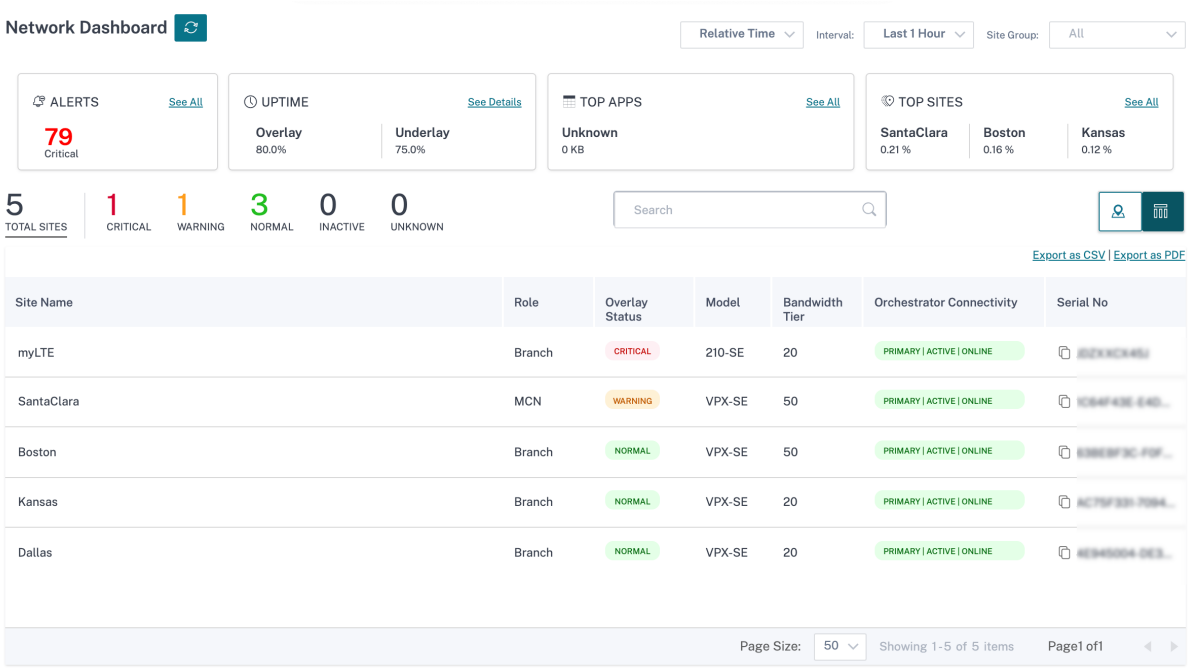
下表介绍了用于群集的五种颜色阴影来表示站点的运行状况：

色彩传奇	说明
	集群中的所有站点均为绿色。这意味着每个站点都有所有虚拟路径，关联的成员路径为 UP
	集群中的所有站点均为橙色。这意味着每个站点至少有一条成员路径处于关闭状态，但所有虚拟路径都处于打开状态
	集群中的所有站点均为红色。这意味着每个站点至少有一条虚拟路径 DOWN
	该集群包含绿色和橙色站点
	集群有红色和非红色站点的组合

您还可以通过将鼠标悬停在任何集群上来验证网络方面。严重警报或警告警报以弹出窗口的形式出现在集群顶部。

如果单击该集群，它将放大到该集群并显示其他群集。你可以看到一个显示群集数量的视图栏。箭头选项可帮助您退后一步。单击“关闭 **(X)** ”按钮恢复到原始页面。

或者，您可以在“列表视图”中查看网络摘要。



- 单击任何尚未部署的非活动“配置不足”站点，将带您进入站点配置工作流程。
- 单击任何已部署的活动站点，将带您进入 站点控制面板。

> 注意
>
> Citrix SD-WAN 叠加隧道被称为虚拟路径。您通常在每个站点和主控制节点 (MCN) 之间有一条虚拟路径隧道，并根据需要使用额外的站点站点虚拟路径。虚拟路径是通过将底层 WAN 链路/路径绑定在一起而形成的。因此，每个虚拟路径都包含多个成员路径。
>
> 当用户将鼠标悬停在“虚拟路径”或“成员路径”这个术语上时，可以显示这一点。

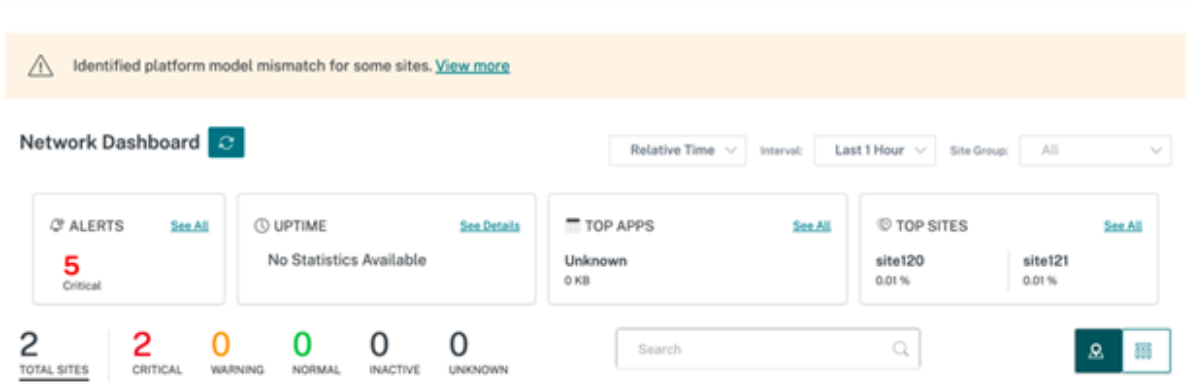
你可以将 **Pegman** 拖到地图上打开街景。

记录设备不匹配

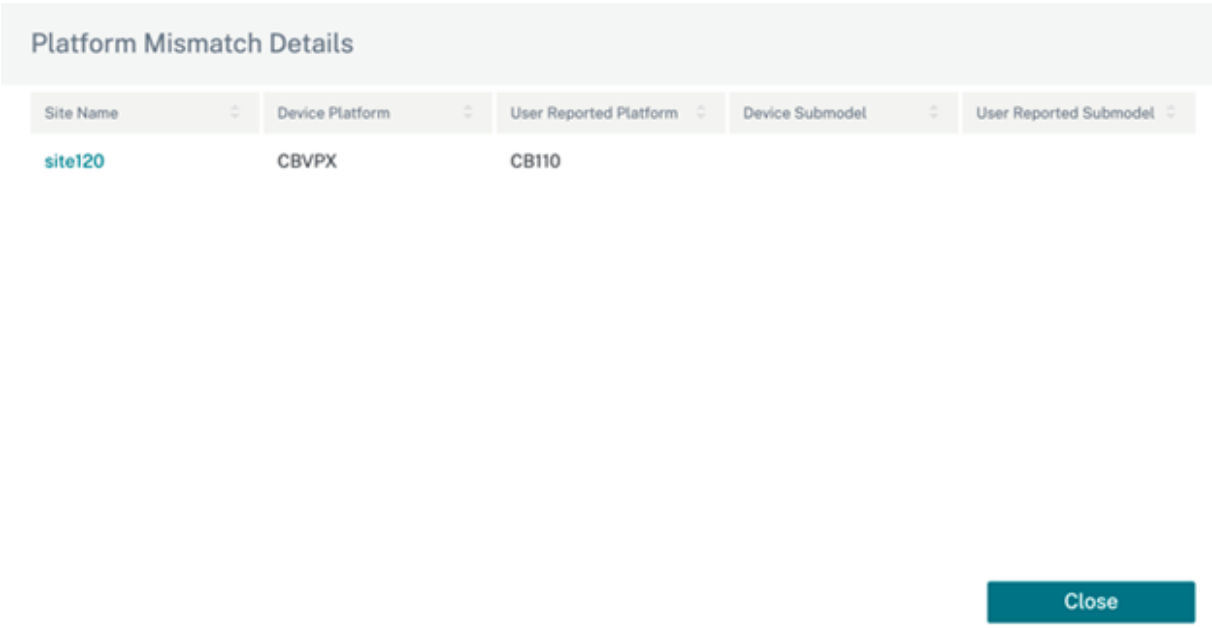
Citrix SD-WAN Orchestrator 服务报告了在设备报告的平台模型和用户报告的平台模型之间发现的不匹配情况。

如果在站点配置期间用户提供的平台模型和子模型与设备在 Citrix SD-WAN Orchestrator 服务初始注册期间提供的平台模型和子模型不匹配，则网络仪表板上会显示有关不匹配的通知。在这种情况下，请确保配置设备报告的平台模型。

单击“查看更多”以表格形式显示每个站点的平台模型不匹配情况。



平台不匹配详细 信息提供站点名称、设备报告的平台型号和子型号以及用户报告的平台型号和子型号等信息。



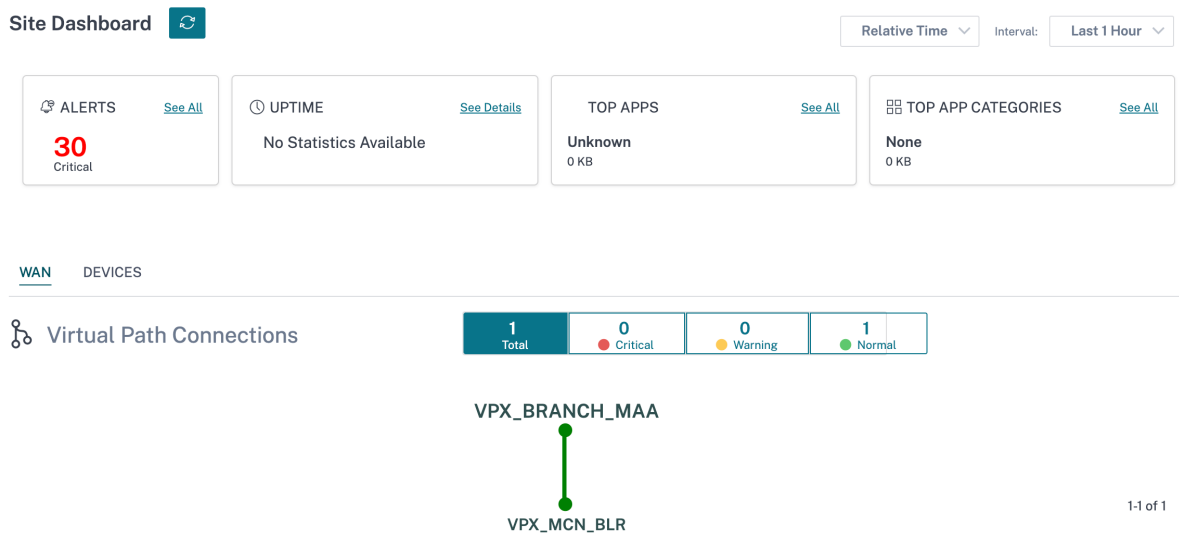
站点控制板

October 21, 2022

站点控制面板概述了网站的运行状况和使用趋势。

仪表板汇总了网站的以下方面，并规定了深入了解更多细节的条款。

- 严重警报：网站上弹出的严重运行状况警报（如果有）的运行次数。
- 正常运行时间：并行比较 SD-WAN 虚拟叠加路径提供的平均正常运行时间与与站点相关的物理底层路径
- 使用趋势：基于流量与网站关联的热门应用程序和应用程序类别
- 站点详细信息：WAN 连接和与站点关联的设备



> 提示
>
> 单击“查看全部”或“查看详细信息”可查看更详细的统计信息。

与站点关联的所有叠加虚拟路径连接均使用适当的颜色编码显示，以反映每个连接的运行状况。

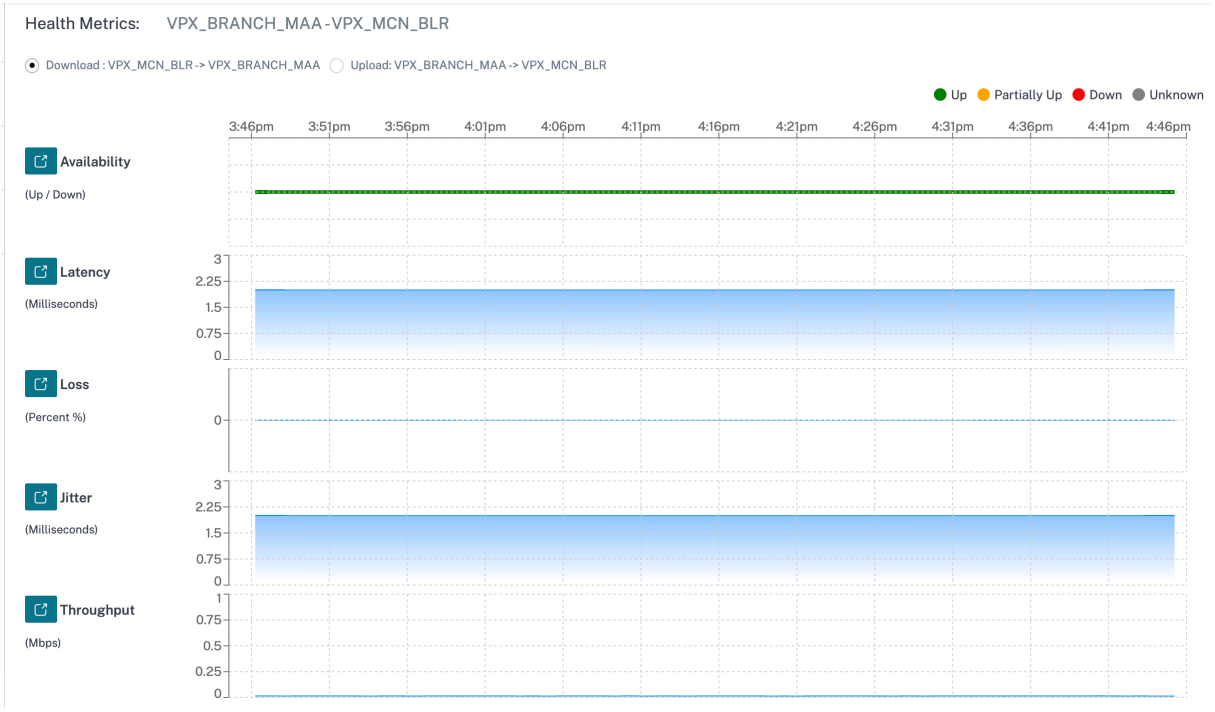
您可以选择任何虚拟路径连接，以查看相应的运行状况指标和趋势。

用于虚拟路径连接的颜色编码标准是：

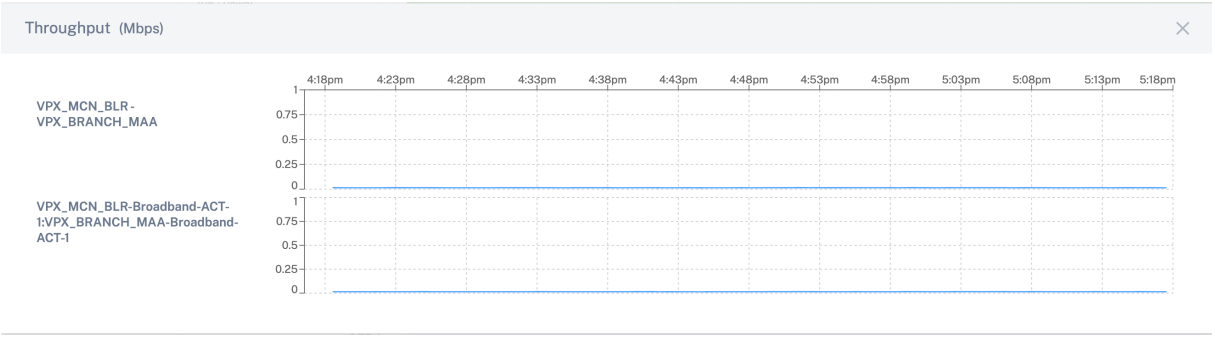
- 严重（红色）：虚拟路径已关闭。
- 警告（橙色）：虚拟路径已启动，但至少有一个成员路径处于关闭状态。
- 正常（绿色）：虚拟路径和所有成员路径均已启动。

健康指标

显示所选虚拟路径连接的运行状况指标和有关可用性、延迟、丢失、抖动和吞吐量的图形趋势。这些统计数据有两个方向：广域网到局域网和局域网到广域网。所有指标均可根据通用时间表进行审查，以帮助在进行故障排除时快速缩小问题范围。



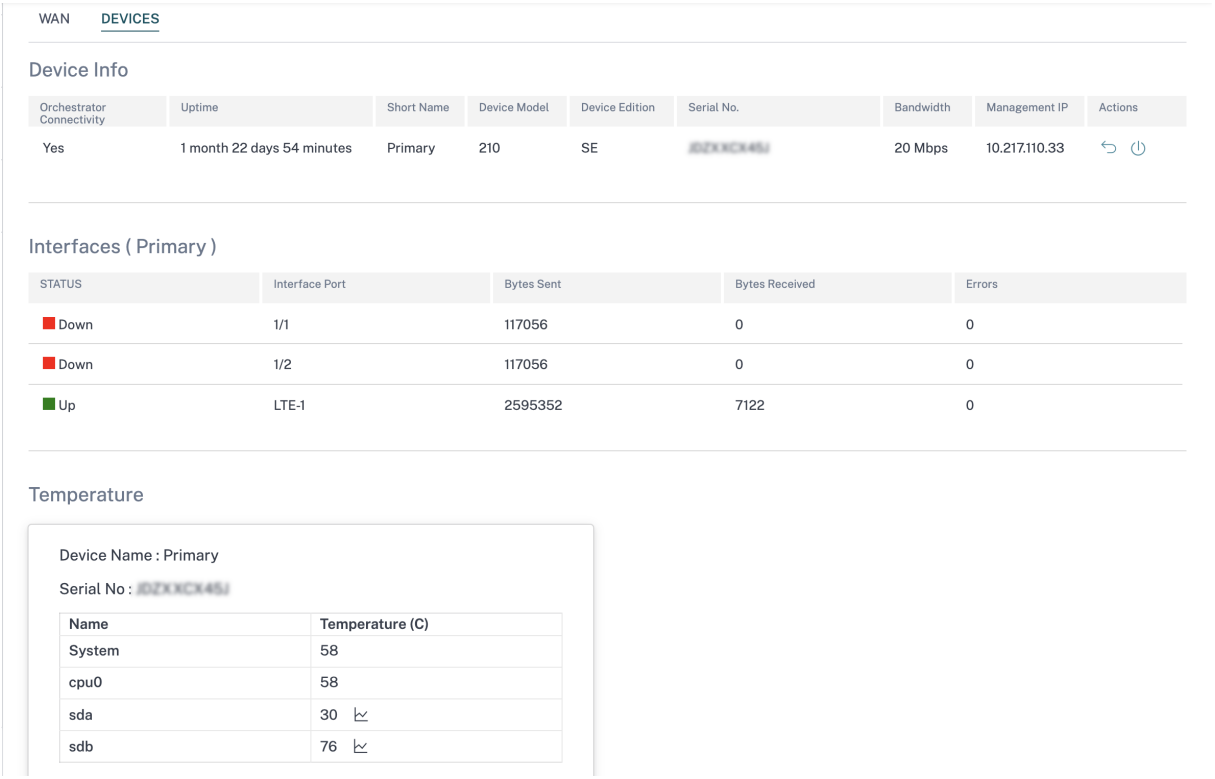
您可以进一步深入研究每个运行状况指标，以获得相同指标的叠加虚拟路径和底层成员路径的比较视图。这将有助于解决叠加层和底层问题。



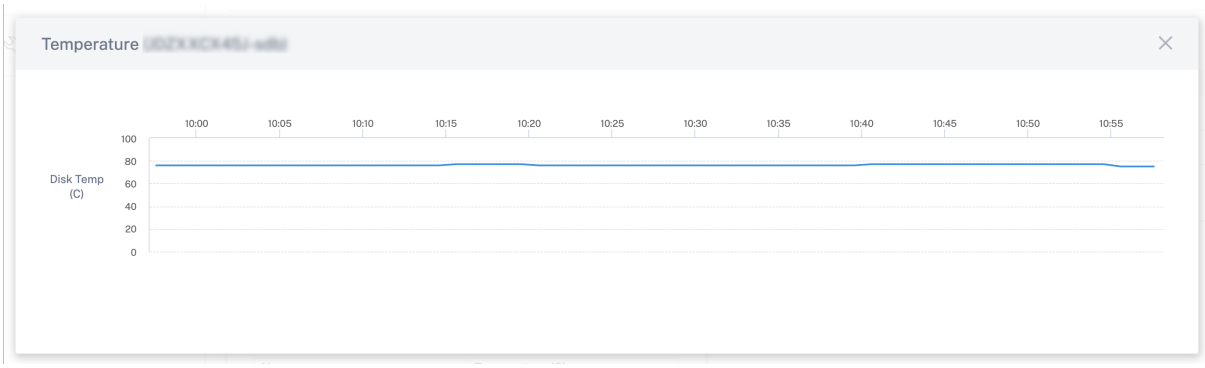
设备

“设备”选项卡显示与站点的设备、接口和磁盘温度相关的详细信息。您也可以重新启动设备、重置设备配置或下载设备日志。

温度 部分以摄氏度为单位显示系统、CPU 和磁盘的温度。



您也可以单击“温度 **(C)** ”列中的图表图标并以图形形式查看信息。



提供商疑难

October 21, 2022

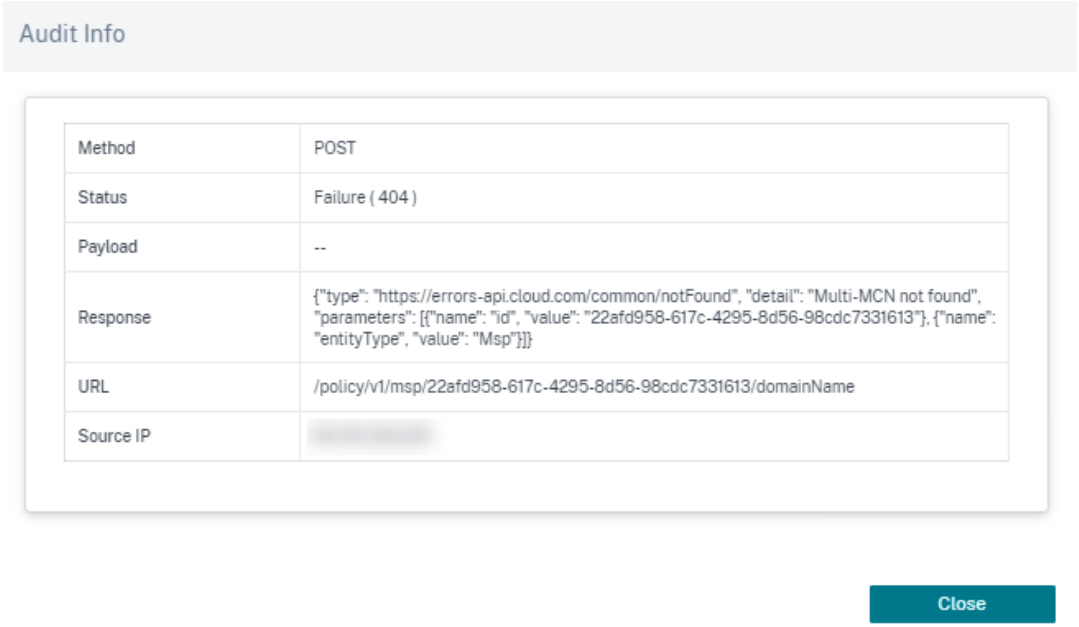
提供商审核日志页面显示提供商级别的日志和设备日志，从而可以快速进行故障排除。

审核日志

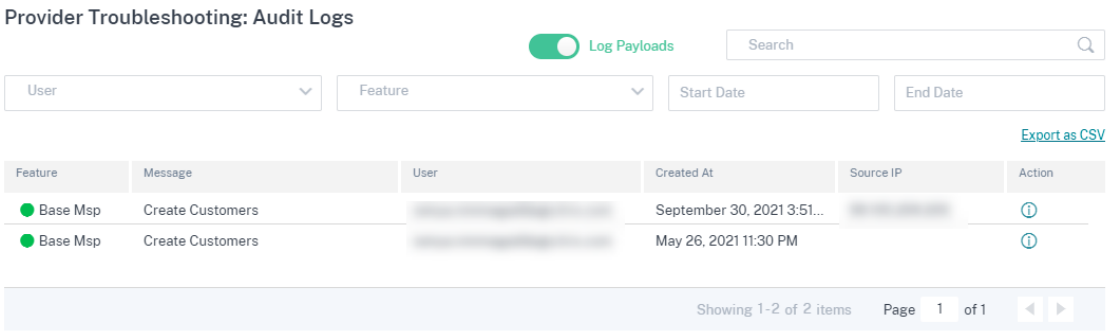
审计日志捕获提供商执行的操作的操作、时间和结果。导航到 故障排除 > 审核日志，查看“提供商疑难解答：审核日志”页面。

提供者审计日志页面显示以下信息：

- 搜索栏：根据关键字搜索审计活动。
- 筛选选项：通过基于以下条件进行筛选来运行审计日志搜索：
  - 用户
  - 功能
  - 时间范围
- 导出为 **CSV**：单击此选项时，审计日志条目将导出到 CSV 文件中。
- 审计信息：选择“操作”列上的图标以导航至“审计信息”部分。本部分提供以下信息：
  - 方法：调用的 API 的 HTTP 请求方法。
  - 状态：API 请求的结果。
  - 负载：通过 API 发送的请求正文。
  - 响应：API 请求失败时的错误响应。此字段仅在 API 请求失败时显示。
  - 网址：已撤销的 API 的 HTTP 网址。
  - 源 **IP**：配置该功能的端点的 IP 地址。此字段显示在“审核日志”页面和“审计信息”页面上。



- 记录有效负载：默认情况下，此选项处于禁用状态。启用后，API 消息的请求正文将显示在“审计信息”部分中。有关 API 的更多信息，请参阅 Citrix SD-WAN Orchestrator 的 API 指南。



网络疑难解

October 21, 2022

客户可以查看所有网络设备的日志，从而实现快速故障排除。

审核日志

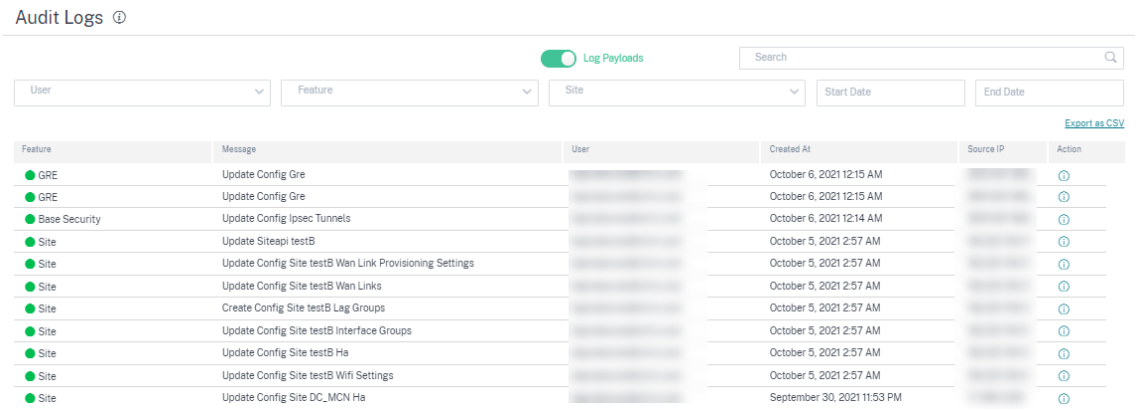
审计日志捕获用户在客户网络上执行的操作的操作、时间和结果。导航到 **SD-WAN** 故障排除 > 审核日志，查看 **SD-WAN** 故障排除审核日志 页面。

SD-WAN 故障排除审核日志页面显示以下信息：

- 搜索栏：根据关键字搜索审计活动。
- 筛选选项：通过基于以下条件进行筛选来运行审计日志搜索：
  - 用户
  - 功能
  - 站点
  - 时间范围
- 导出为 **CSV**：单击此选项时，审计日志条目将导出到 CSV 文件中。
- 审计信息：选择“操作”列上的图标以导航至“审计信息”部分。本部分提供以下信息：
  - 方法：调用的 API 的 HTTP 请求方法。
  - 状态：API 请求的结果。当 API 请求失败时，您会看到以下错误响应。
  - 负载：通过 API 发送的请求正文。
  - 响应：API 请求失败时的错误响应。此字段仅在 API 请求失败时显示。
  - 网址：已撤销的 API 的 HTTP 网址。

- 源 **IP**：配置该功能的端点的 IP 地址。此字段显示在“审核日志”页面和“审计信息”页面上。
- 更改内容：此部分显示通过用户界面对功能进行的所有更改的日志。启用“记录负载”切换按钮以查看“审计信息”部分中的更改。

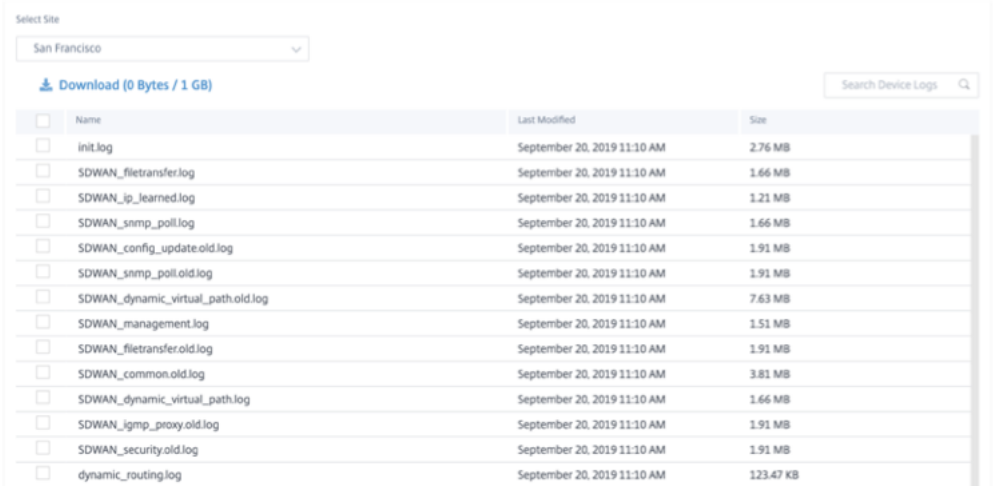
- 记录有效负载：默认情况下，此选项处于禁用状态。启用后，API 消息的请求正文将显示在“审计信息”部分中。有关 API 的更多信息，请参阅 Citrix SD-WAN Orchestrator 的 API 指南。



设备日志

客户可以查看特定于站点的设备日志。

您可以选择特定的设备日志、下载并在必要时与站点管理员共享。

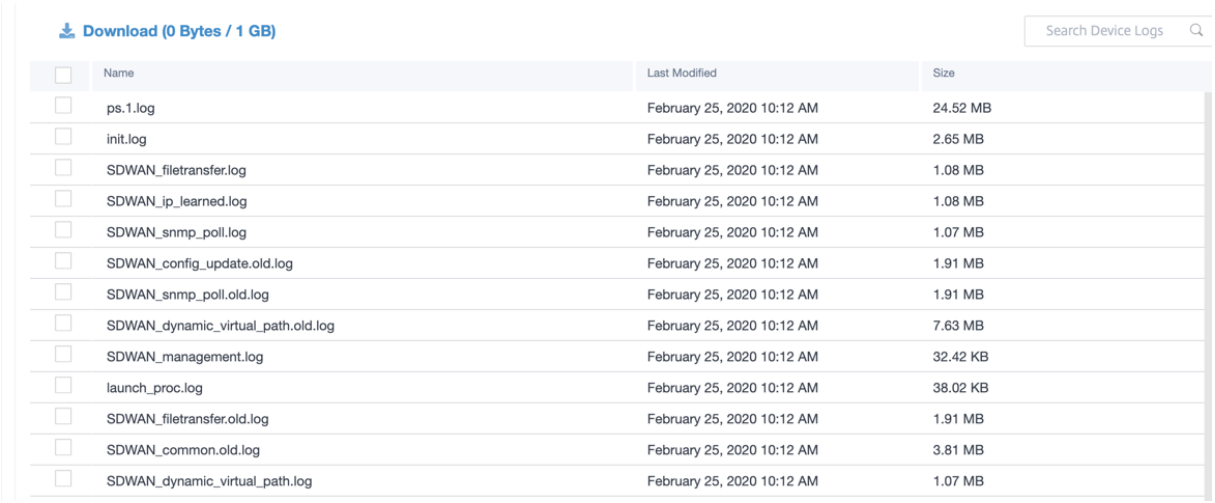


现场疑难解

October 21, 2022

设备日志

日志对于解决问题很有用。站点管理员可以查看在站点的所有设备上捕获的所有日志的列表。您也可以下载日志以进行进一步验证。

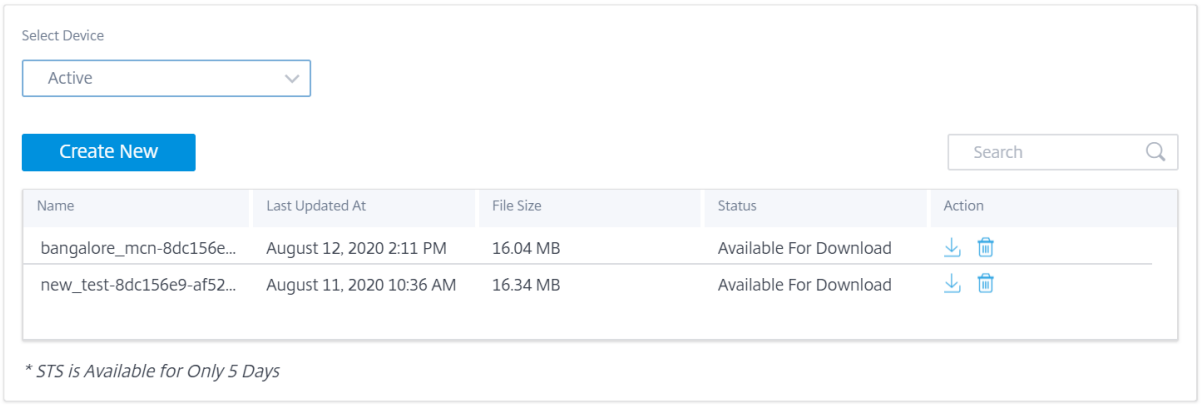


显示技术支持包

Show Tech Support (STS) 捆绑包包含重要的实时系统信息，例如访问日志、诊断日志、防火墙日志。STS 捆绑包用于对 SD-WAN 设备中的问题进行故障排除。您可以创建、下载 STS 捆绑包，然后与 Citrix 支持代表共享。

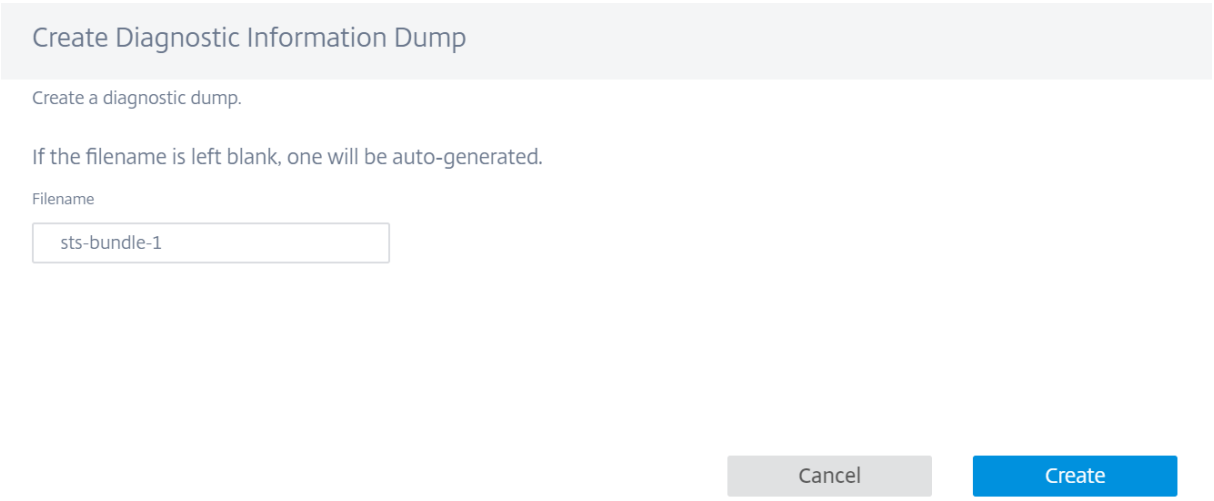
如果在 HA 部署模式下配置站点，则可以选择要为其创建或下载 STS 包的活动或备用设备。

要为站点设备创建 STS 包，请在站点级别导航到 故障排除 > **STS** 捆绑包，然后单击 新建。



提供 STS 捆绑包的名称。名称必须以字母开头，并且可以包含字母、数字、破折号和分数不足。名称的最大允许长度为 32 个字符。用户提供的名称用作最终名称的前缀。为了确保文件名的唯一性（时间戳）并帮助从 STS 包（序列号）中识别设备，该服务会生成一个全名。如果未提供名称，则在创建包时自动生成名称。

只有当设备处于联机状态且设备上当前没有 STS 进程运行时，您才能请求新的 STS。即使设备处于脱机状态，您也可以从 Citrix SD-WAN Orchestrator 服务下载已经可用的 STS。



在任何给定时间，STS 过程处于以下状态之一：

STS 状态	说明
已请求	请求新的 STS 捆绑包。该请求需要几分钟才能得到处理。如有必要，您可以选择取消 STS 创建过程。
正在上传	创建的 STS 软件包将上传到云服务。持续时间取决于包裹的大小。状态每 5 秒更新一次。您无法取消 STS 上传过程。
失败	STS 过程在创建或上传过程中失败。您可以删除失败的 STS 操作的条目。
可供下载	STS 的创建和上传过程已成功。您现在可以下载或删除 STS 软件包。

在设备上启动 STS 进程后，状态列下的进度将定期更新。例如，已请求（收集日志文件）。

STS 捆绑包和故障记录保留 7 天，之后会自动删除。

提供商报告

October 21, 2022

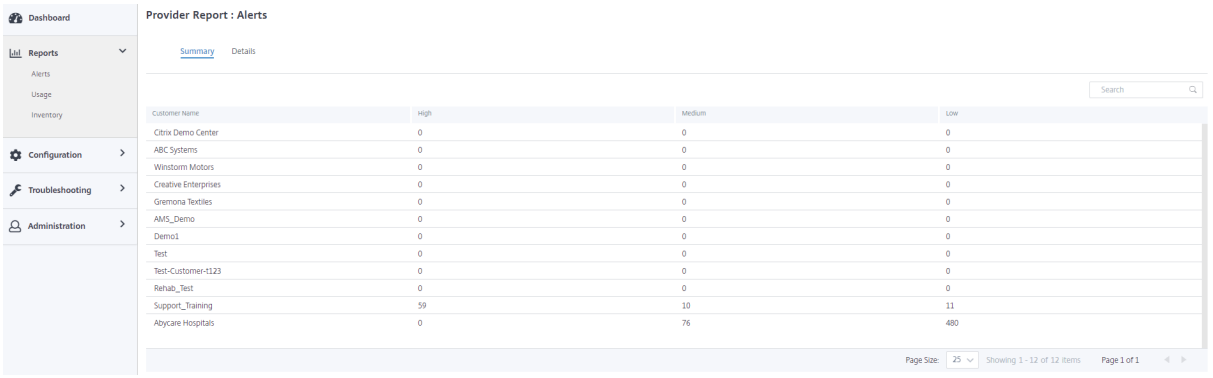
提供 商报告 提供商管理的所有客户汇总的警报、使用趋势和库存的可见性。

在 Citrix SD-WAN Orchestrator 服务提供商级别的用户界面中，导航到 报告。

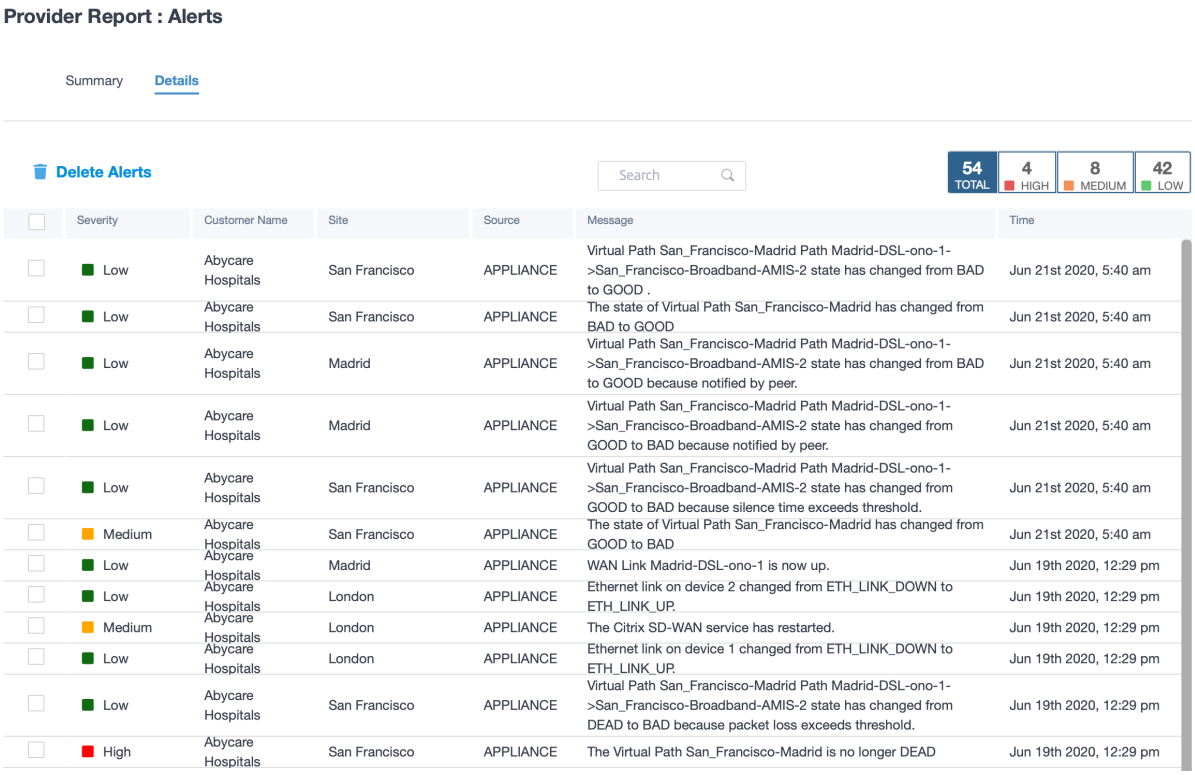
警报

提供商可以查看所有客户网络中生成的所有事件和警报。

摘要 视图显示每个客户的高、中、低警报数量。



您还可以在“详细信息”下查看严重性、警报产生地点、警报消息、时间和其他 信息。



可根据需要使用合适的筛选选项，例如：查找所有客户的高严重性警报，或给定客户的警报等。

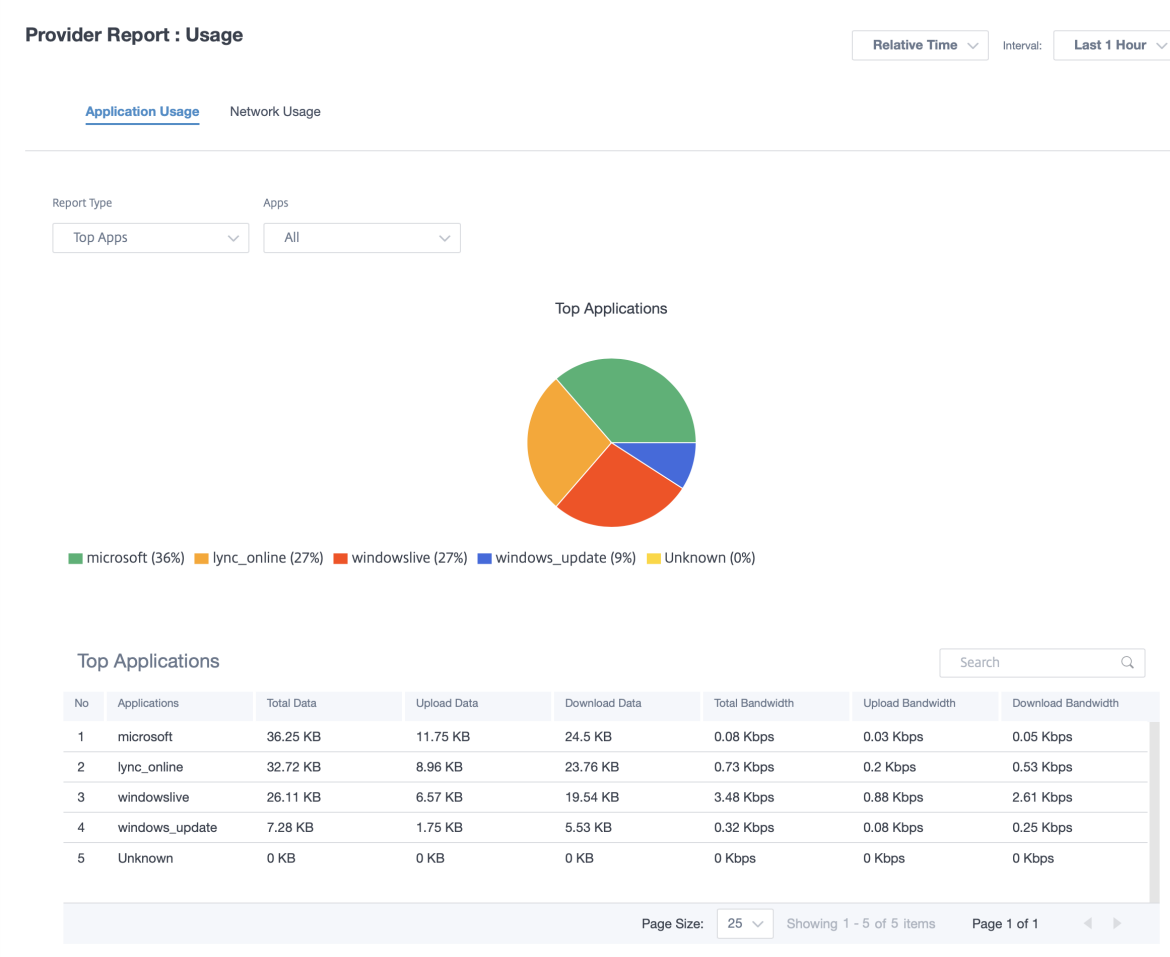
您还可以选择和删除警报。

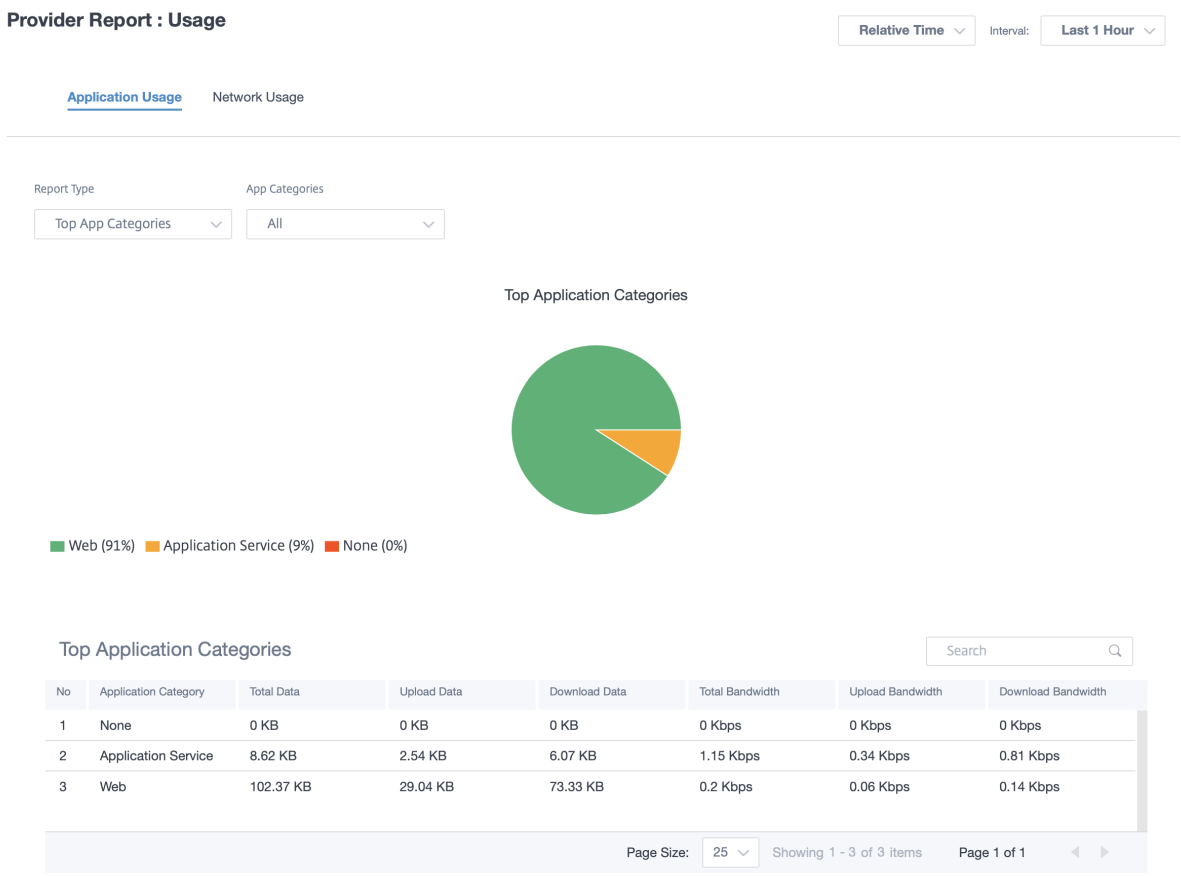
使用情况

提供商可以查看跨客户的使用趋势，例如 热门应用程序、热门应用程序类别、应用程序带宽和 热门站点。

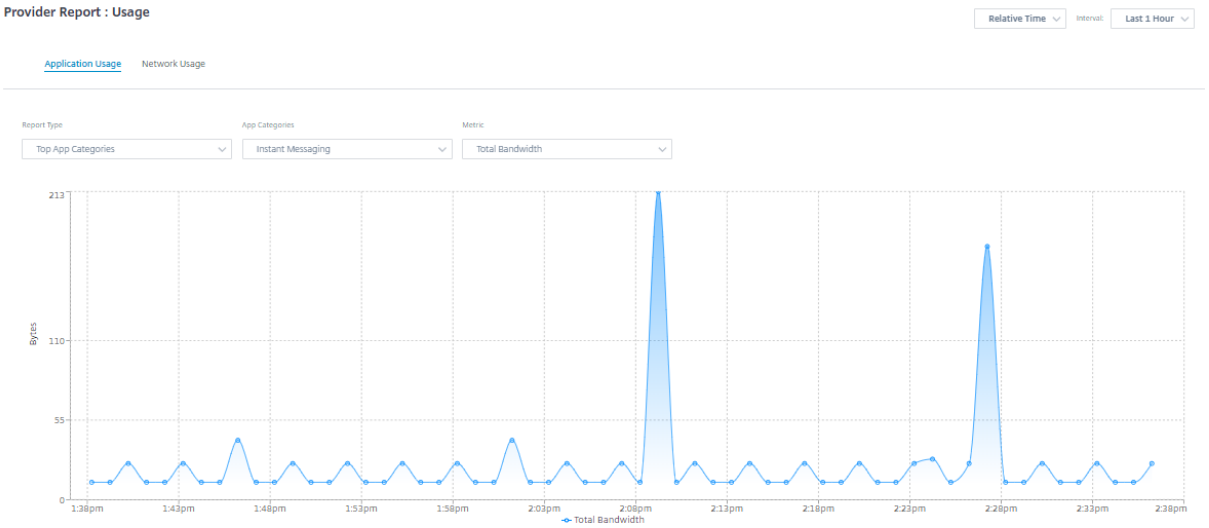
热门应用程序和应用程序类别

热门应用程序 和 热门应用程序类别 图表显示了在所有客户网络中广泛使用的应用程序和应用程序系列。这允许您分析数据消耗模式，并在必要时为每类数据重新分配带宽限制。





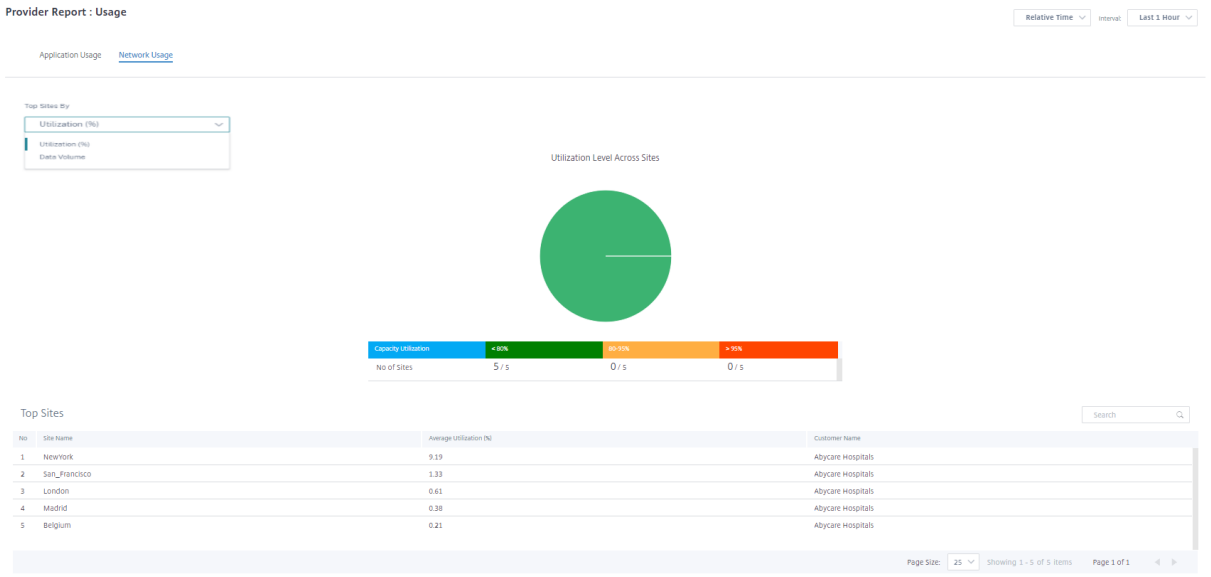
您可以查看带宽使用情况统计信息。在所选时间间隔内收集带宽统计信息。您可以根据 报告类型、应用程序或应用程序类别 以及 指标筛选统计报告。



- 报告类型：从列表中选择 热门应用程序或应用程序类别。
- 应用程序/应用程序类别：从列表中选择热门应用程序或类别。
- 指标：从列表中选择带宽指标（例如总数据、传入数据、总带宽）。

网络使用情况

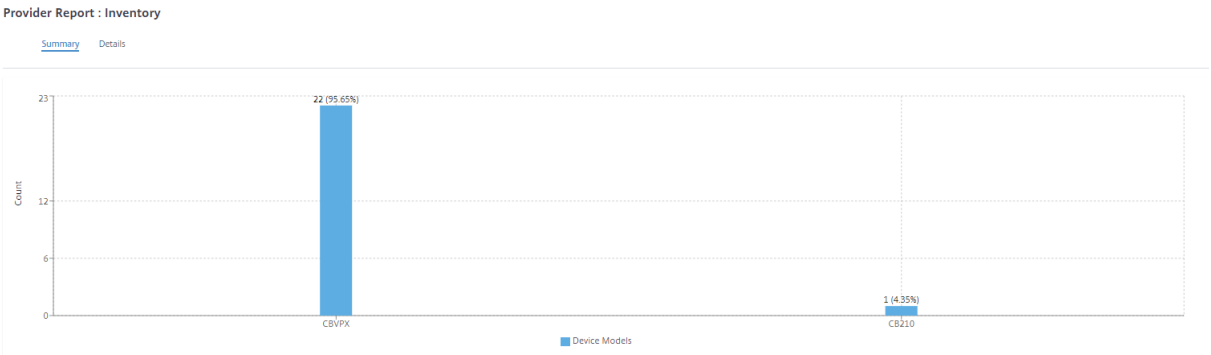
网络使用情况图表描述了带宽使用率最高的所有客户的前 10 个站点。您可以按利用率 (%) 或数据量 (MB) 查看站点。



清单

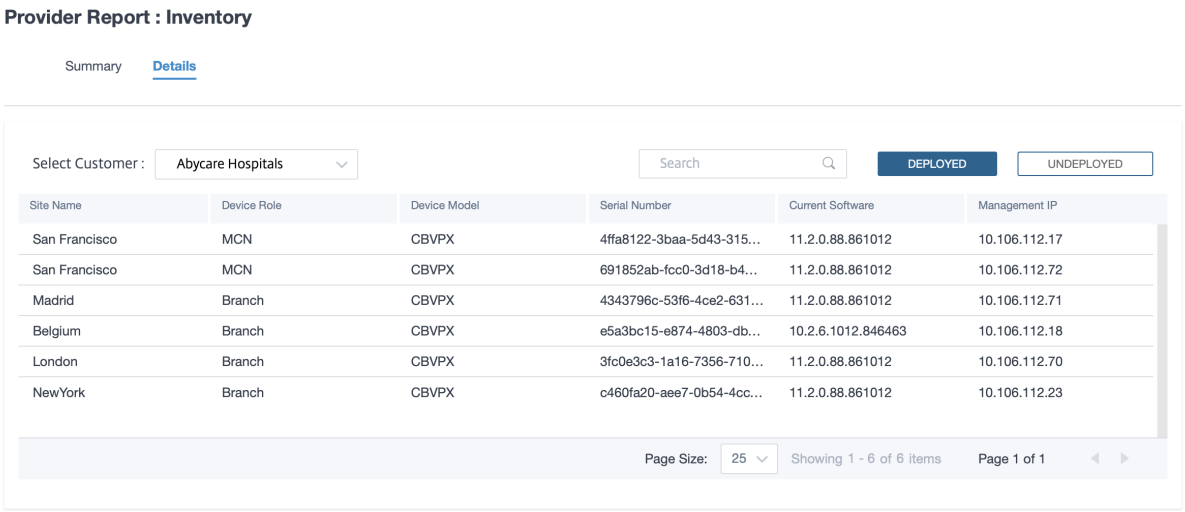
提供商可以查看所有客户的全部设备清单。您可以选择查看库存摘要或详细视图。

库存摘要视图提供了库存分布图表，描述了客户网络中使用的各种设备型号和每种类型的设备的数量。



可以根据需要使用合适的筛选选项，例如：查找属于特定客户的所有设备，或具有特定设备型号的所有设备等

库存详细视图提供了所有已部署的设备以及已配置但尚未部署的设备的列表。从“选择客户”下拉列表 中选择客户。您可以查看站点名称、设备角色、设备型号、设备序列号、当前软件和设备管理 IP 地址。



客户/网络报告

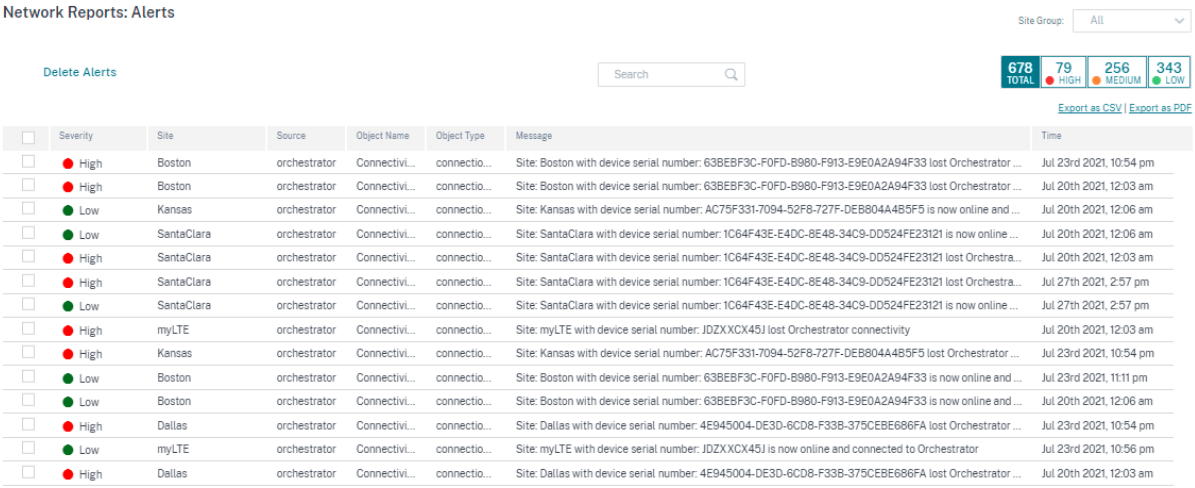
October 21, 2022

客户报告提供了对客户 网络中所有站点汇总的网络警报、使用趋势、库存、质量、诊断和防火墙状态的可见性。

警报

客户可以查看该网络中所有站点生成的所有事件和警报的详细报告。

它包括严重性、警报产生地点、警报消息、时间和其他详细信息。



可以根据需要使用合适的筛选选项，例如：查找所有站点的所有高严重性警报，或特定站点的所有警报等等。

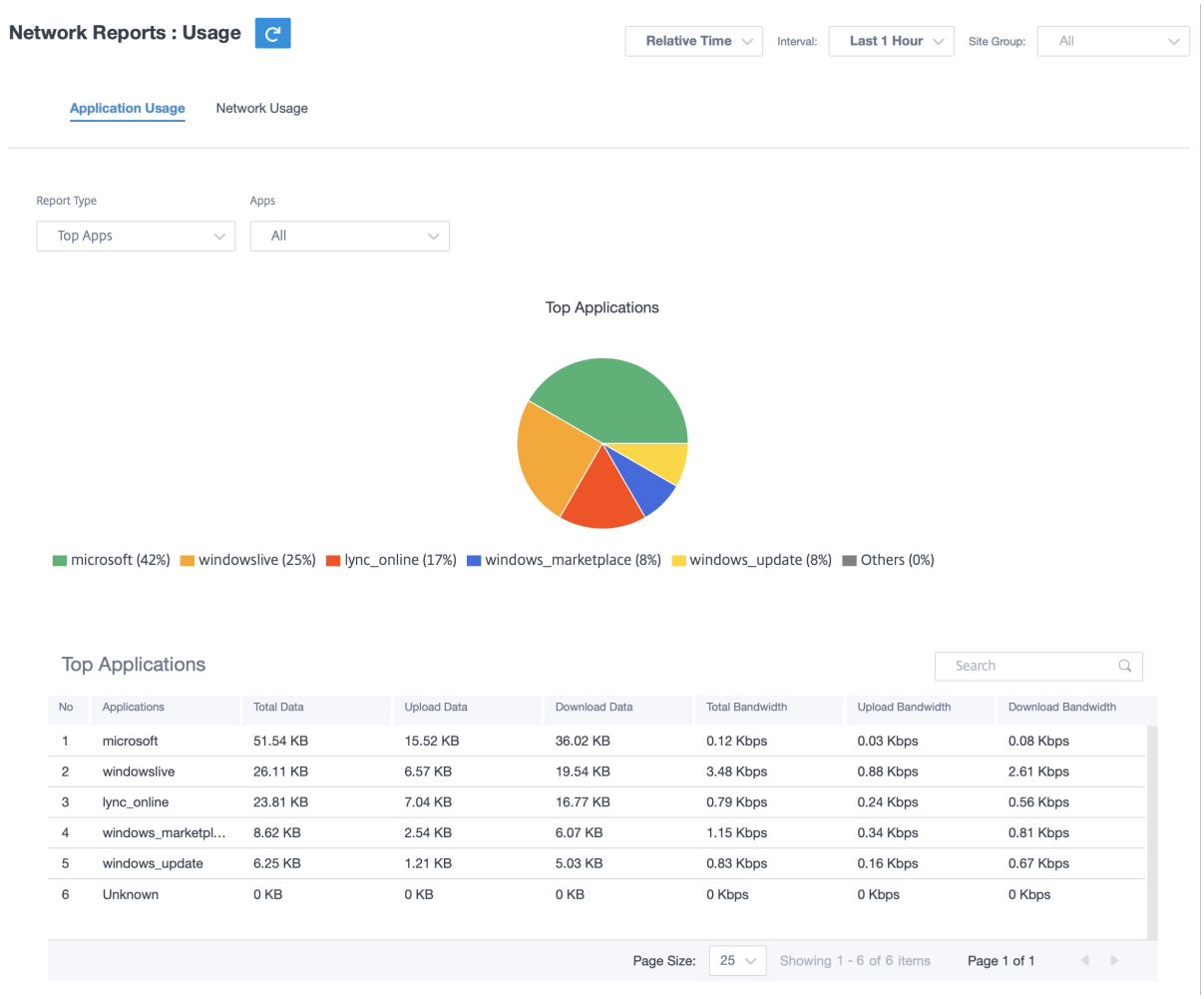
您也可以选择和清除警报。

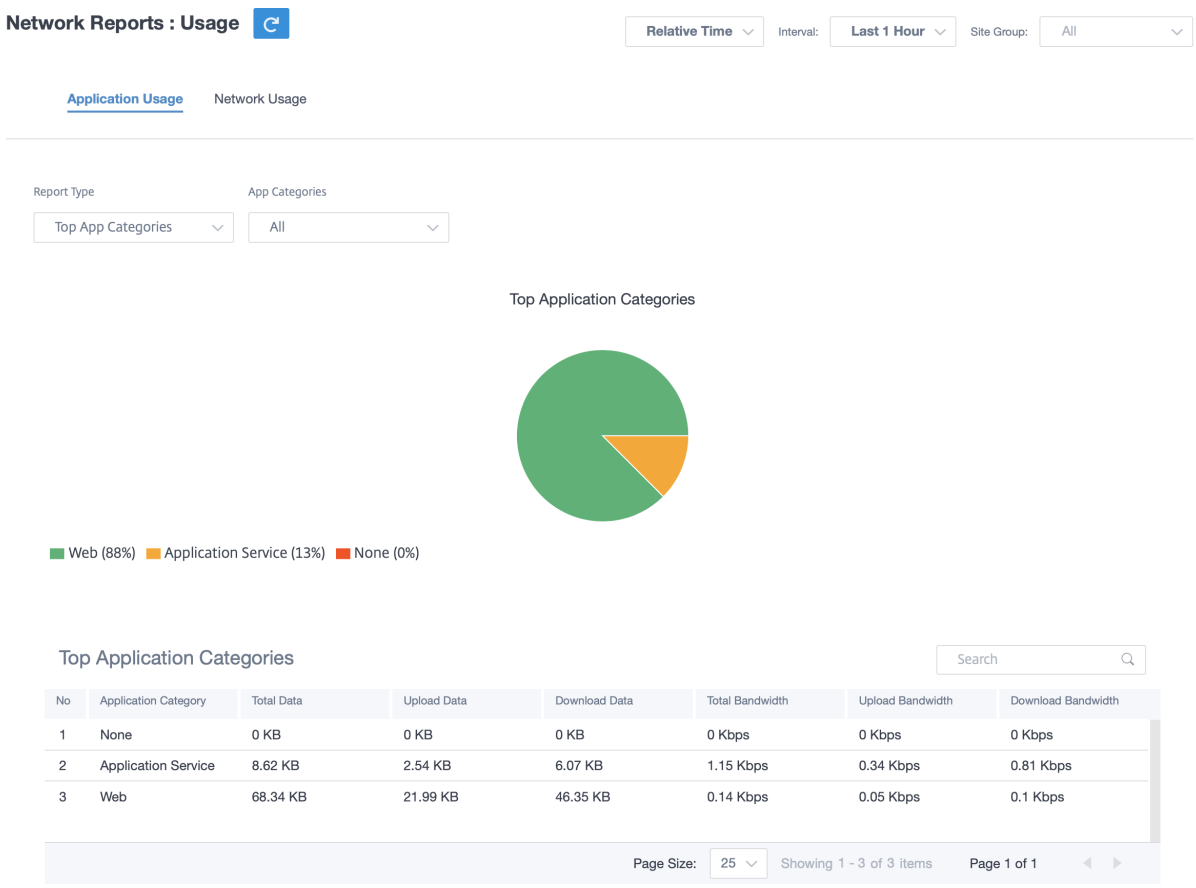
使用情况

客户可以查看其网络中所有 站点的使用趋势，例如热门应用程序 **、热门应用程序类别、应用程序带宽和热门 ** 站点。

热门应用程序和应用程序类别

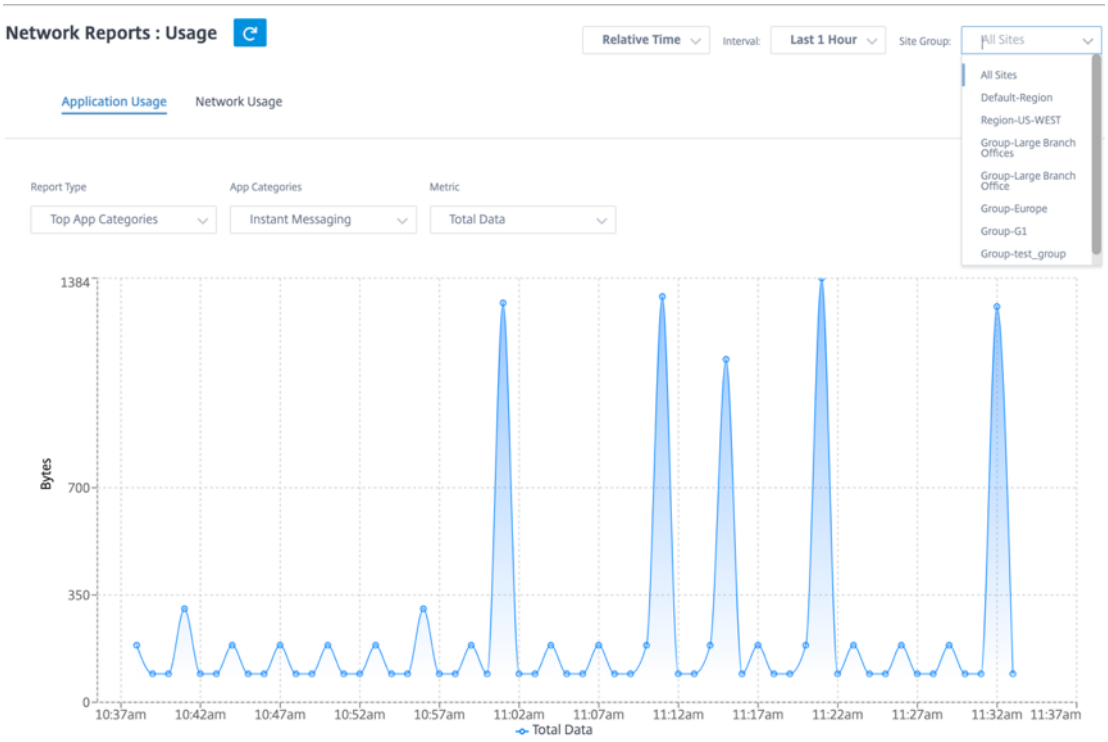
热门应用程序 和 热门应用程序类别 图表显示了在所有站点中广泛使用的顶级应用程序和热门应用程序系列。这使您可以分析数据消耗模式，并为网络中的每一类数据重新分配带宽限制。





应用程序带宽

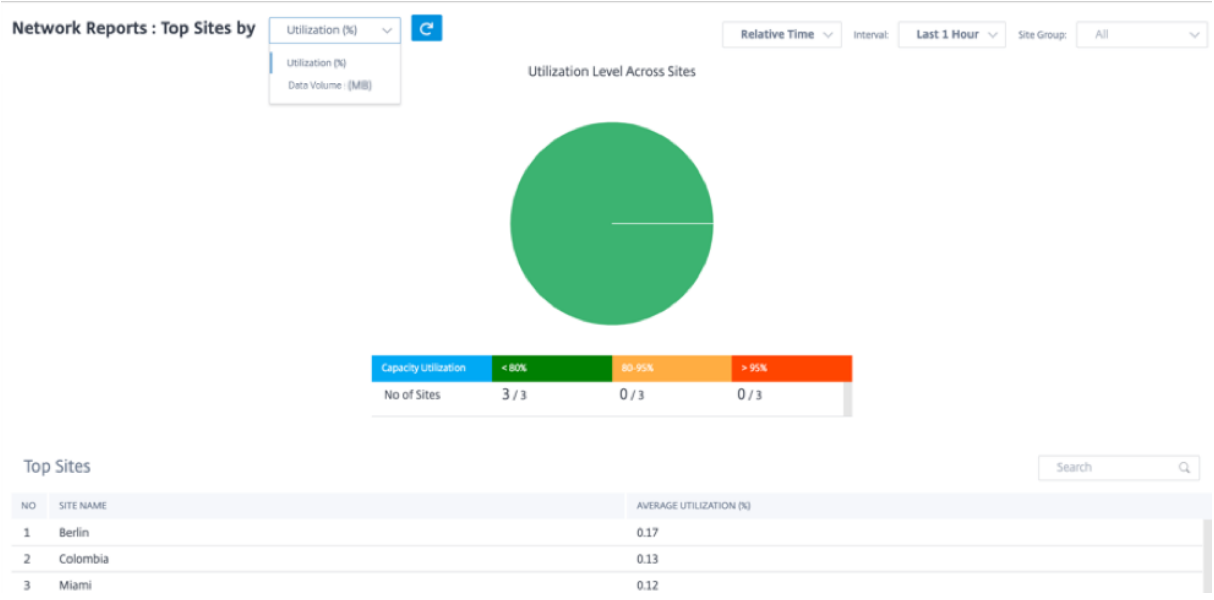
您可以查看所选站点组或所有站点的带宽使用统计信息。在所选时间间隔内收集带宽统计信息。您可以根据 报告类型、应用程序或应用程序类别 以及 指标筛选统计报告。



- 报告类型：从列表中选择 热门应用程序或应用程序类别。
- 应用程序/应用程序类别：从列表中选择热门应用程序或类别（例如网络服务）。
- 指标：从列表中选择带宽指标（例如总数据、传入数据、总带宽）。

网络使用情况

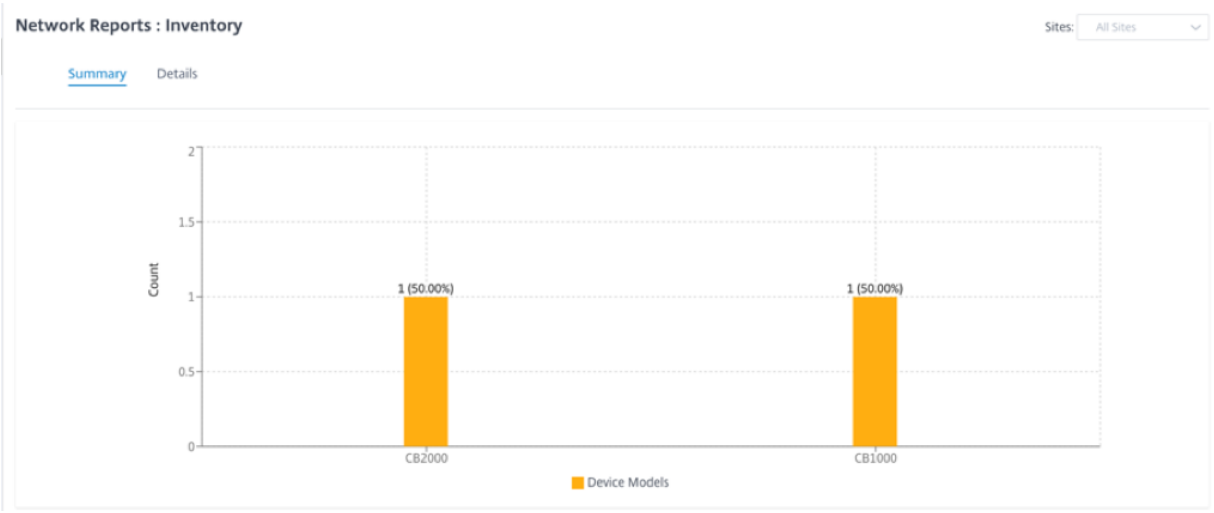
热门站点 图表描述了客户网络中带宽使用率最高的热门站点。您可以按使用率 (%) 或流量 (MB) 查看站点。



清单

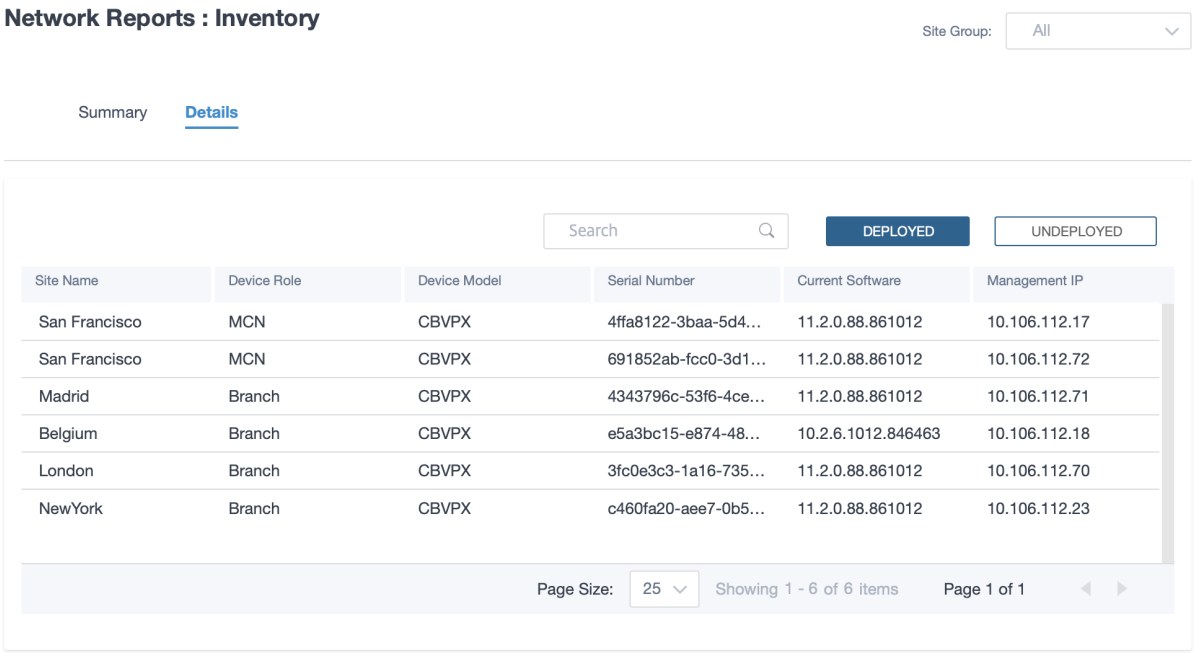
客户可以查看网络中所有站点的全部设备清单。您可以选择查看库存摘要或详细视图。

库存摘要视图提供了库存分布图表，描述了客户网络中所有站点使用的各种设备型号和每种类型的设备的数量。



可以根据需要使用合适的筛选选项，例如：查找属于特定站点的所有设备，或具有特定设备型号的所有设备等。

库存详细视图提供了所有已部署的设备以及已配置但尚未部署的设备的列表。以及客户、站点名称、设备角色、设备序列号、当前软件和设备管理 IP 地址。

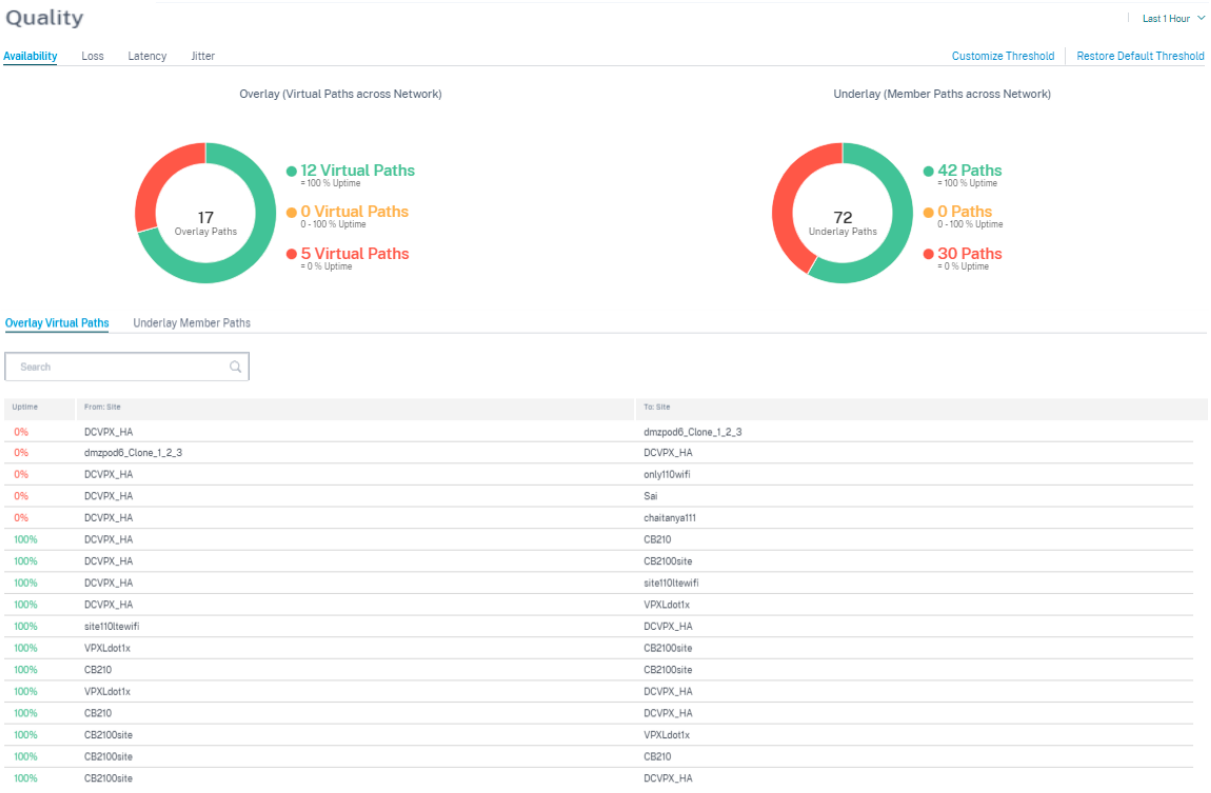


HDX 仪表板和报告

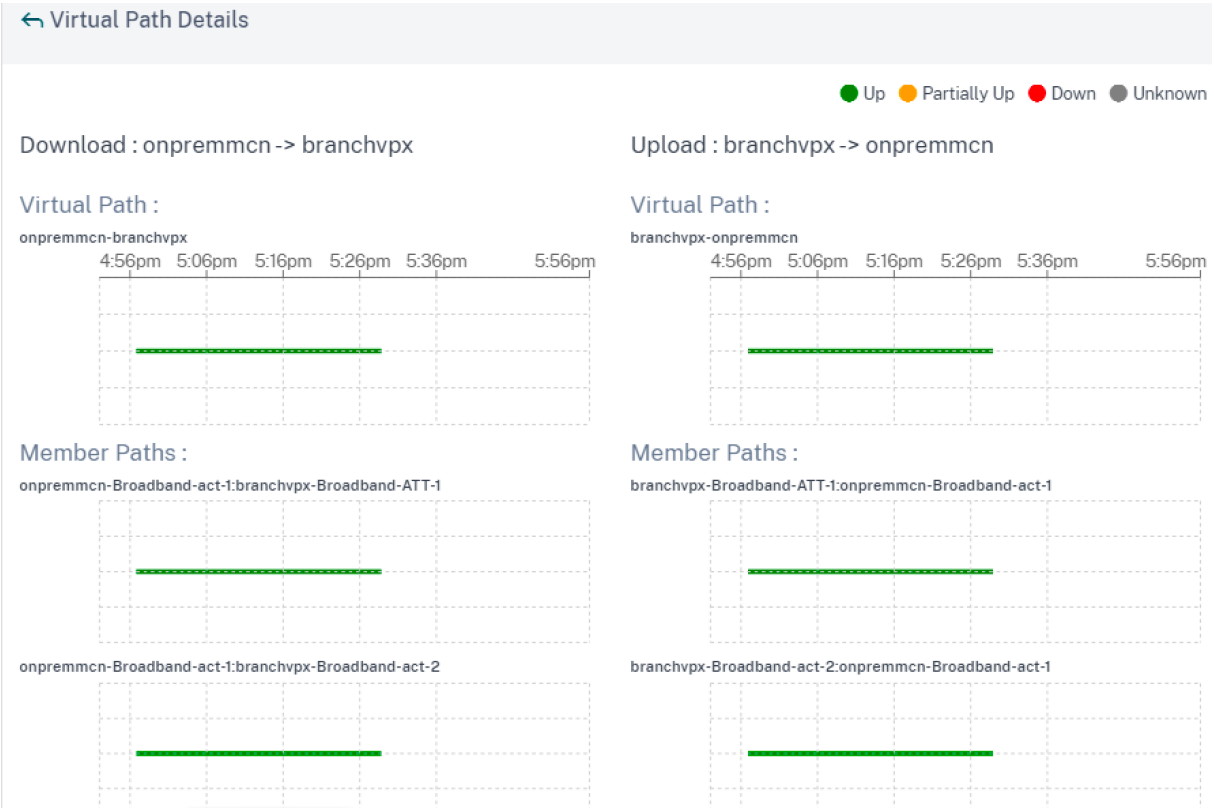
有关 HDX 仪表板和报告的详细信息，请参阅 HDX 仪表板和报告。

质量

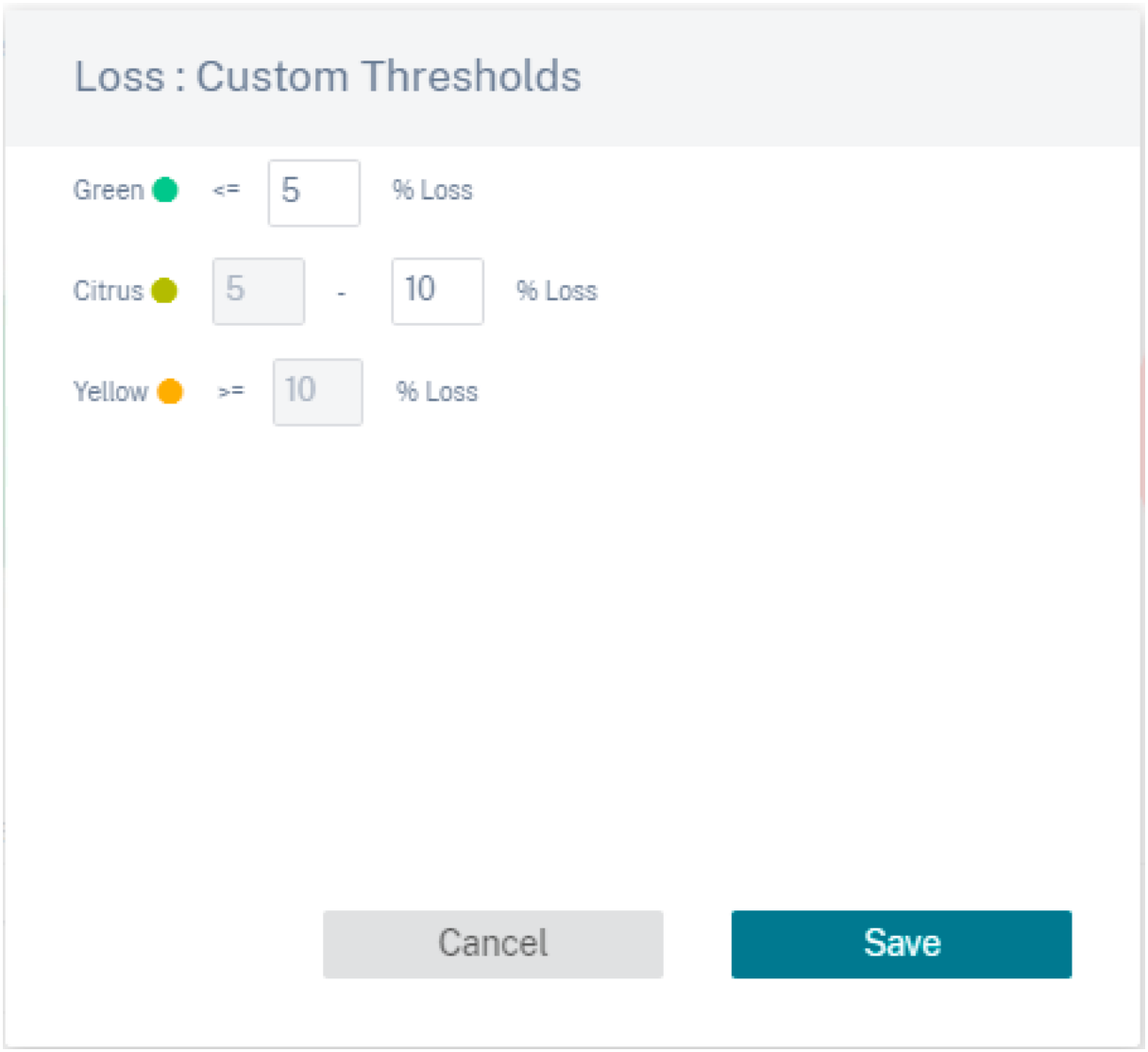
网络质量 报告允许在可用性和丢失、延迟和抖动方面对虚拟覆盖层和物理底层路径进行网络级比较。这有助于有效监控覆盖层相对于底层网络的运行情况，还有助于故障排除。对于延迟和抖动，仅显示底层成员路径的详细信息。



单击表格条目查看详细视图。



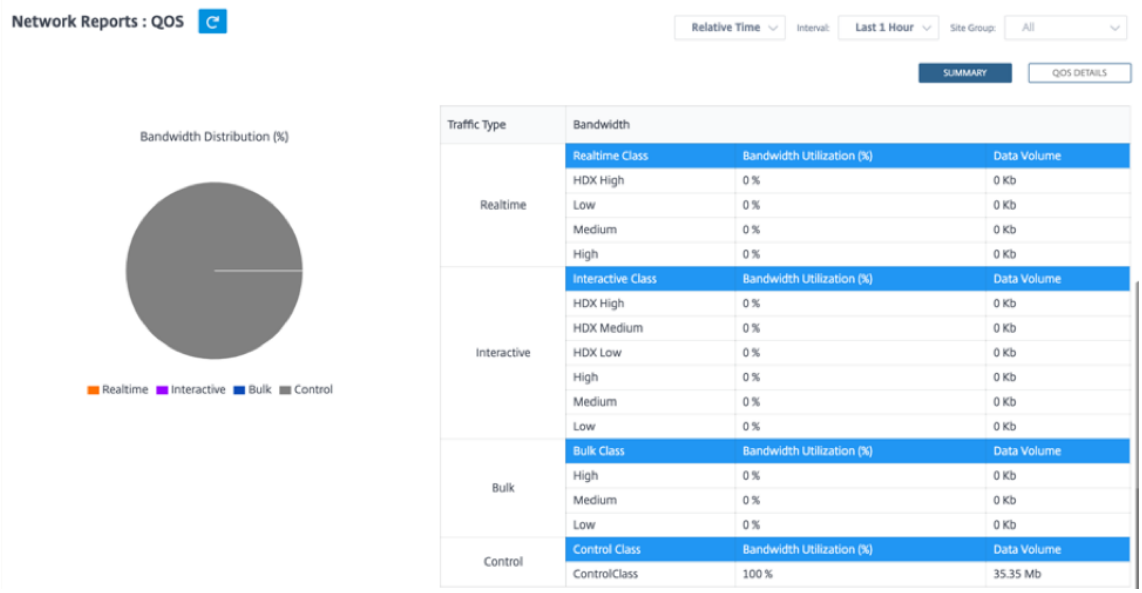
您可以为每个网络质量参数自定义阈值。



服务质量

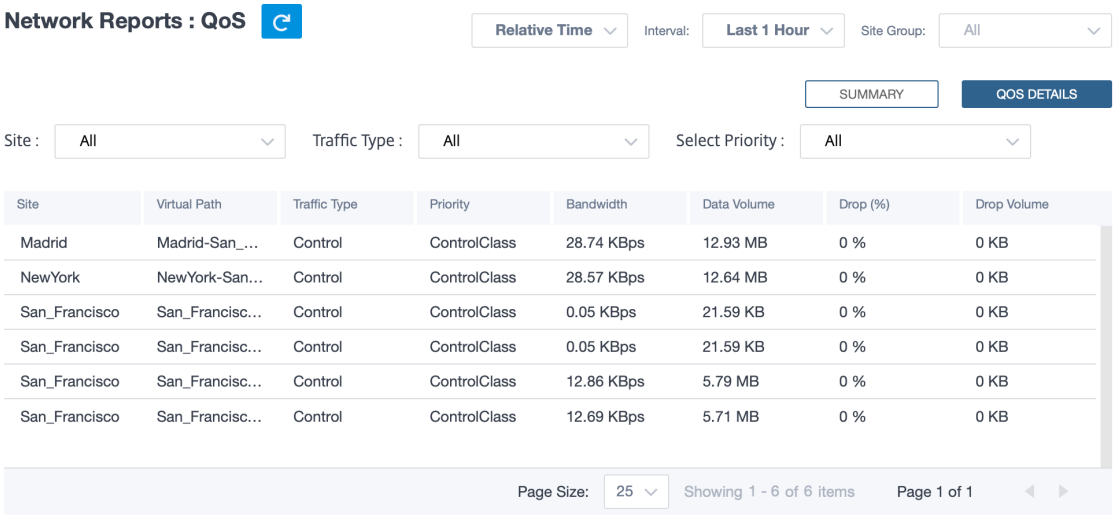
服务质量 (QoS) 管理数据流量，以减少网络上的数据包丢失、延迟和抖动。有关更多信息，请参阅 服务质量。以下是查看服务质量 (QoS) 报告的两种方法：

- 摘要视图：摘要视图概述了所有类型的流量（实时、交互式、批量流量以及网络和每个站点的控制）的带宽消耗。



  - 实时：用于低延迟、低带宽、时间敏感型流量。实时应用程序比较耗时，但实际上不需要高带宽 (例如 IP 语音)。实时应用程序对延迟和抖动敏感，但可以容忍一些损失。
  - 交互式：用于具有低到中等延迟要求和低到中等带宽要求的交互式流量。交互式应用程序以鼠标点击或光标移动的形式涉及人工输入。通常情况下，在客户端与服务器之间进行交互。通信可能不需要高带宽，但对丢失和延迟非常敏感。但是，服务器到客户端确实需要高带宽才能传输图形信息，这可能对丢失不敏感。
  - 批量：用于可以容忍高延迟的高带宽流量。处理文件传输和需要高带宽的应用程序将分类为散装类。这些应用很少涉及人为干扰，主要由系统自己处理。
  - 控制：用于传输包含路由、调度和链路统计信息的控制数据包。

- 详细视图：详细视图捕捉了与叠加虚拟路径相关的每个 QoS 类别的带宽消耗、流量、丢弃的数据包等趋势。



此报告在站点级别提供，用户可以根据两个站点之间的虚拟路径查看 QoS 统计信息。有关更多信息，请参阅 站点报

告。

历史统计

对于每个站点，您可以查看以下网络参数的图表的统计信息：

- 站点
- 虚拟路径
- 路径
- WAN 链接
- 接口
- 班级
- GRE 通道
- IPsec 通道

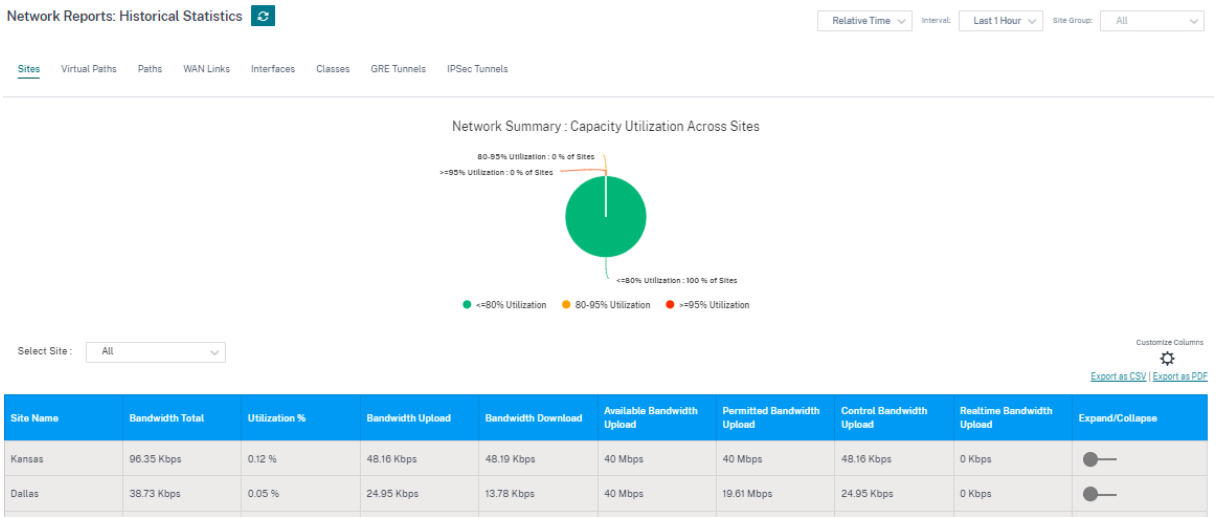
统计数据以图表形式收集。这些图表以时间表与使用情况的关系绘制而成，使您能够了解各种网络对象属性的使用趋势。您可以查看网络范围内应用程序统计信息的图表。

您可以根据需要查看或隐藏图表并自定义列。

站点

要查看站点统计信息，请导航到 报告 **>** 历史统计信息 **>** 站点 选项卡。

从列表中选择站点名称。



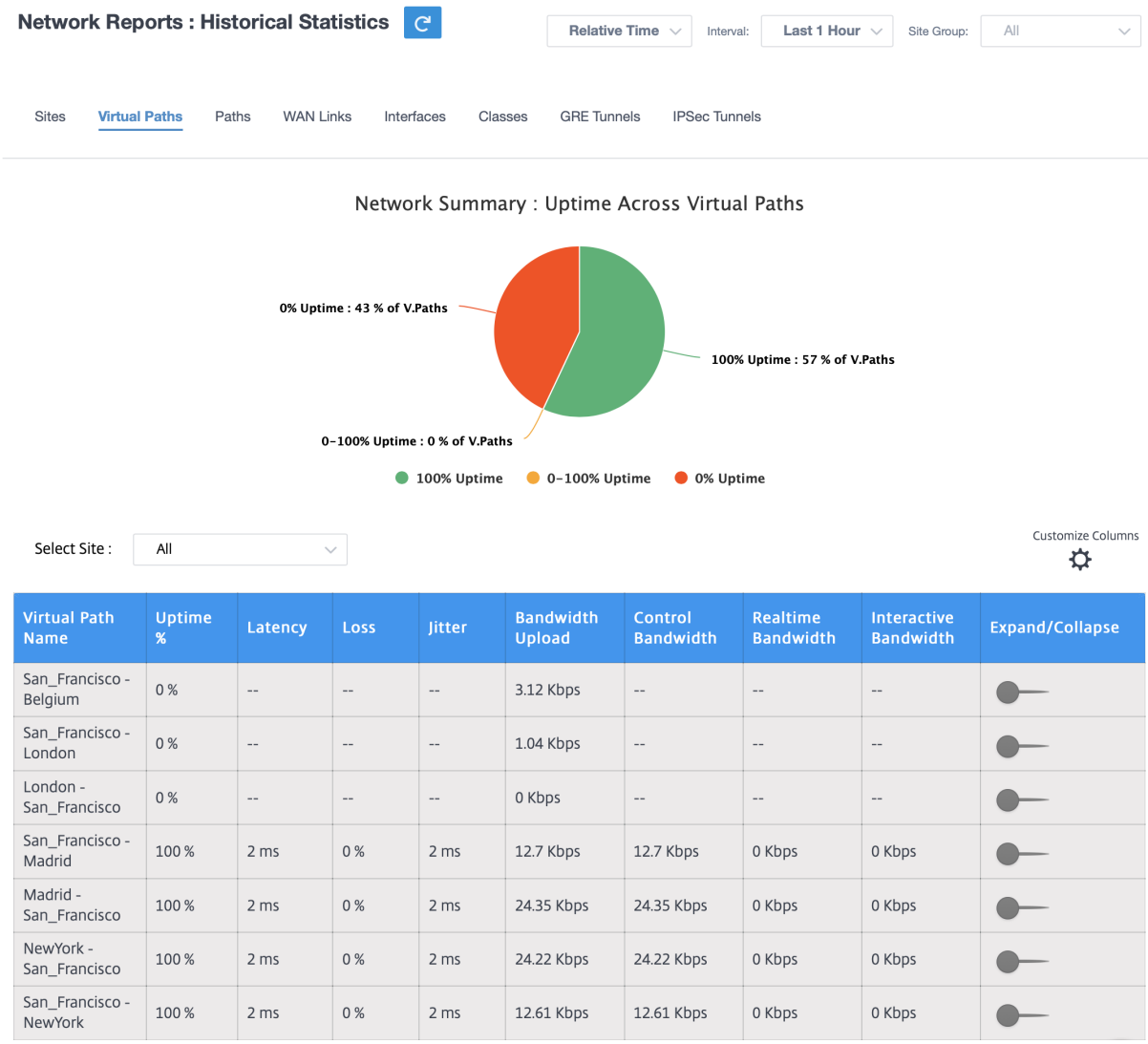
您可以查看以下指标：

- 站点名称：站点名称。
- 总带宽：所有数据包类型消耗的总带宽。带宽 = 控制带宽 + 实时带宽 + 交互带宽 + 批量带宽。

- 利用率：您可以按利用率 (%) 查看站点统计信息。
- 带宽入口：通过 WAN 端口的最大和最小下载速度。
- 输出带宽：通过 WAN 端口的最大和最小上传速度。
- 可用带宽入口：分配给站点的所有 WAN 链接的总带宽。
- 允许的带宽入口：可用于传输信息的带宽。
- 控制带宽入口：用于传输包含路由、调度和链路统计信息的控制数据包的带宽。
- 实时带宽入口：属于 NetScaler SD-WAN 配置中实时类类型的应用程序消耗的带宽。此类应用程序的性能在很大程度上取决于网络延迟。延迟数据包比丢失的数据包（例如 VoIP、Skype for Business）差。
- 展开/折叠：您可以根据需要展开或折叠数据。

虚拟路径

要查看 虚拟路径 统计信息，请导航到 报告 > 统计信息 > 虚拟路径 选项卡。



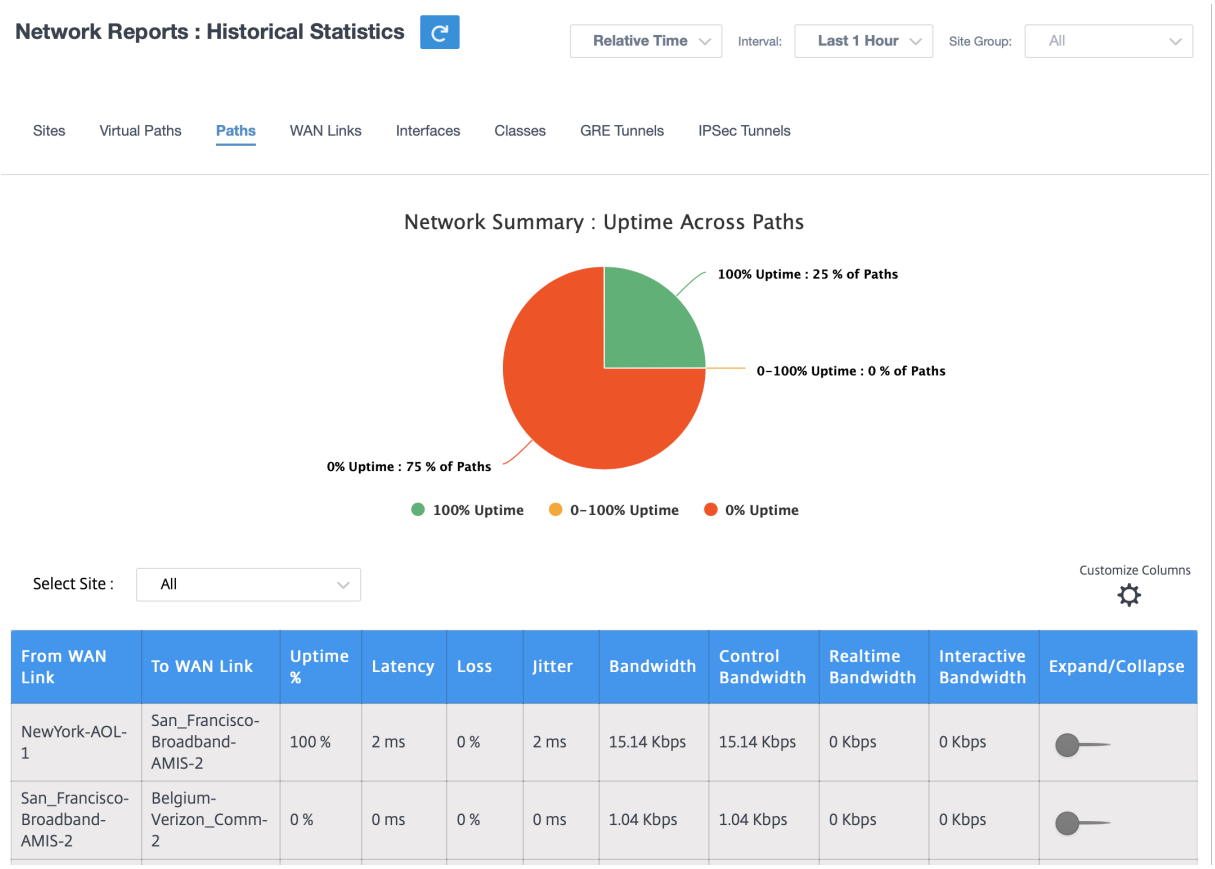
Virtual Path Name	Uptime %	Latency	Loss	Jitter	Bandwidth Upload	Control Bandwidth	Realtime Bandwidth	Interactive Bandwidth	Expand/Collapse
San_Francisco - Belgium	0 %	--	--	--	3.12 Kbps	--	--	--	
San_Francisco - London	0 %	--	--	--	1.04 Kbps	--	--	--	
London - San_Francisco	0 %	--	--	--	0 Kbps	--	--	--	
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	

您可以查看以下指标：

- 虚拟路径名：虚拟路径名。
- 延迟：实时流量的延迟（以毫秒为单位）。
- 丢失：丢失的数据包百分比。
- 抖动：收到的数据包延迟的变化，以毫秒为单位。
- 带宽入口：所选时间段内的入口（局域网到广域网）带宽使用情况。
- 控制带宽：用于传输包含路由、调度和链路统计信息的控制数据包的带宽。
- 实时带宽：属于 SD-WAN 配置中实时类类型的应用程序消耗的带宽。此类应用程序的性能在很大程度上取决于网络延迟。延迟数据包比丢失的数据包（例如 VoIP、Skype for Business）差。
- 交互带宽：属于 SD-WAN 配置中交互类类型的应用程序消耗的带宽。此类应用程序的性能取决于网络延迟以及数据包丢失（例如 XenDesktop、XenApp）的巨大程度。
- 批量带宽：属于 SD-WAN 配置中批量类别类型的应用程序消耗的带宽。这些应用程序很少涉及人为干预，由系统自己处理（例如 FTP、备份操作）。
- 展开/折叠：您可以根据需要展开或折叠数据。

路径

要查看 路径 统计信息，请导航到 报告 **>** 统计信息 **>** 路径 选项卡。

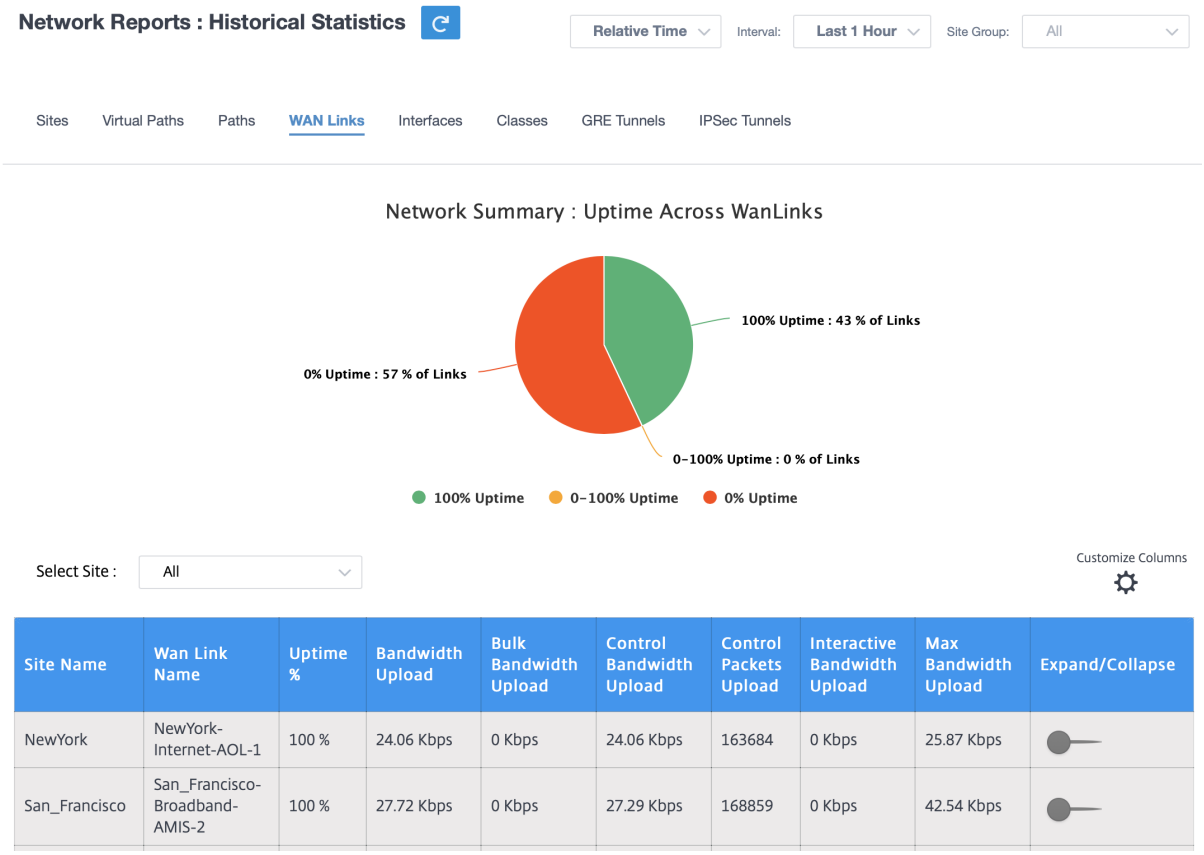


您可以查看以下指标：

- 来自 **WAN** 链接：源 WAN 链接。
- 至 **WAN** 链接：目标 WAN 链接。
- 延迟：实时流量的延迟（以毫秒为单位）。
- 丢失：丢失的数据包百分比。
- 抖动：收到的数据包延迟的变化，以毫秒为单位。
- 带宽：所有数据包类型消耗的总带宽。带宽 = 控制带宽 + 实时带宽 + 交互带宽 + 批量带宽。
- 控制带宽：用于传输包含路由、调度和链路统计信息的控制数据包的带宽。
- 实时带宽：属于 SD-WAN 配置中实时类类型的应用程序消耗的带宽。此类应用程序的性能在很大程度上取决于网络延迟。延迟数据包比丢失的数据包（例如 VoIP、Skype for Business）差。
- 交互带宽：属于 SD-WAN 配置中交互类类型的应用程序消耗的带宽。此类应用程序的性能取决于网络延迟以及数据包丢失（例如 XenDesktop、XenApp）的巨大程度。
- 批量带宽：属于 SD-WAN 配置中批量类别类型的应用程序消耗的带宽。这些应用程序很少涉及人为干预，由系统自己处理（例如 FTP、备份操作）。
- 展开/折叠：您可以根据需要展开或折叠数据。

WAN 链接

要查看 **WAN** 链接 级别的统计信息，请导航到 报告 **>** 统计信息 **> WAN** 链接 选项卡。



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	

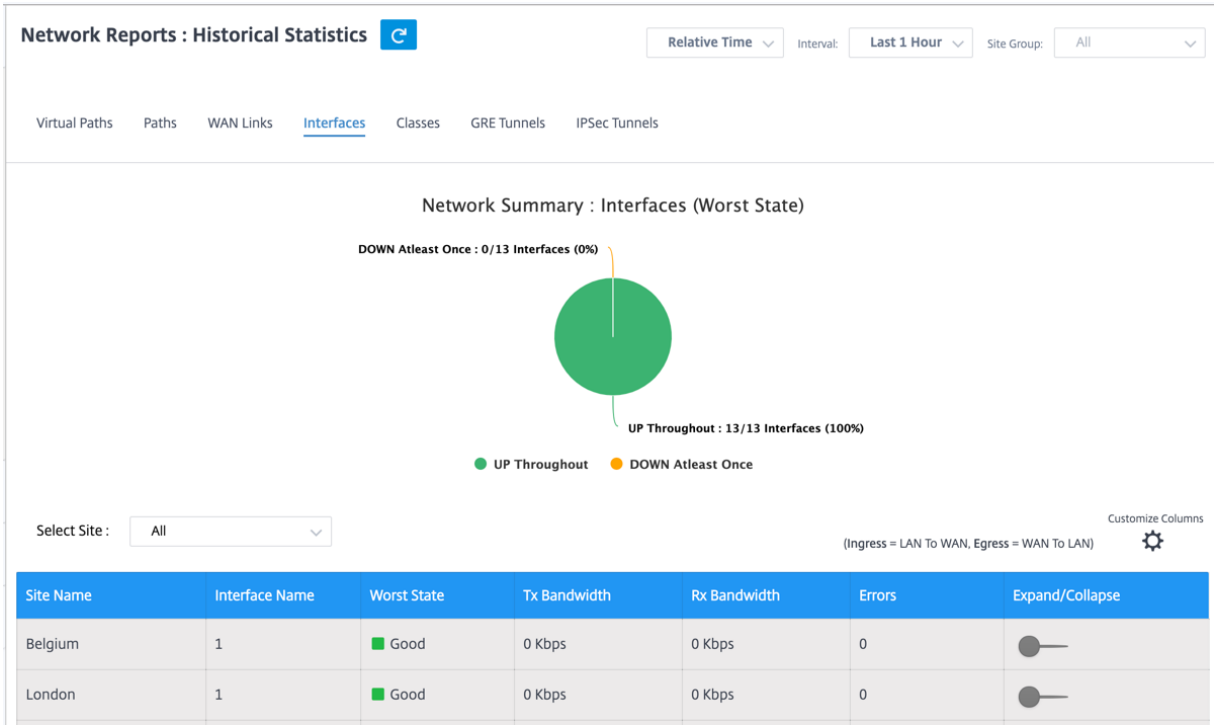
您可以查看以下指标：

- **WAN** 链接名称：路径名。
- 带宽入口：所选时间段内的入口（局域网到广域网）带宽使用情况。
- 批量带宽入口：所选时间段内批量流量使用的入口（局域网到广域网）虚拟路径带宽。
- 控制带宽入口：所选时间段内控制流量使用的入口（局域网到广域网）虚拟路径带宽。
- 控制数据包入口：所选时间段内的入口（局域网到广域网）虚拟路径控制数据包。
- 交互式带宽入口：交互式流量在选定时间段内使用的入口（局域网到广域网）虚拟路径带宽。
- 最大带宽入口：所选时间段内一分钟内使用的最大入口（LAN 到 WAN）带宽。
- 最小带宽入口：所选时间段内一分钟内使用的最小入口（LAN 到 WAN）带宽。
- 展开/折叠：您可以根据需要展开或折叠数据。

接口

接口统计报告可帮助您在故障排除过程中快速查看是否有任何端口关闭。您还可以在每个端口查看传输和接收的带宽或数据包详细信息。您还可以查看在特定时间段内这些接口上发生的错误数。

要查看 接口 统计信息，请导航到 报告 **>** 统计信息 **>** 接口 选项卡。



您可以查看以下指标：

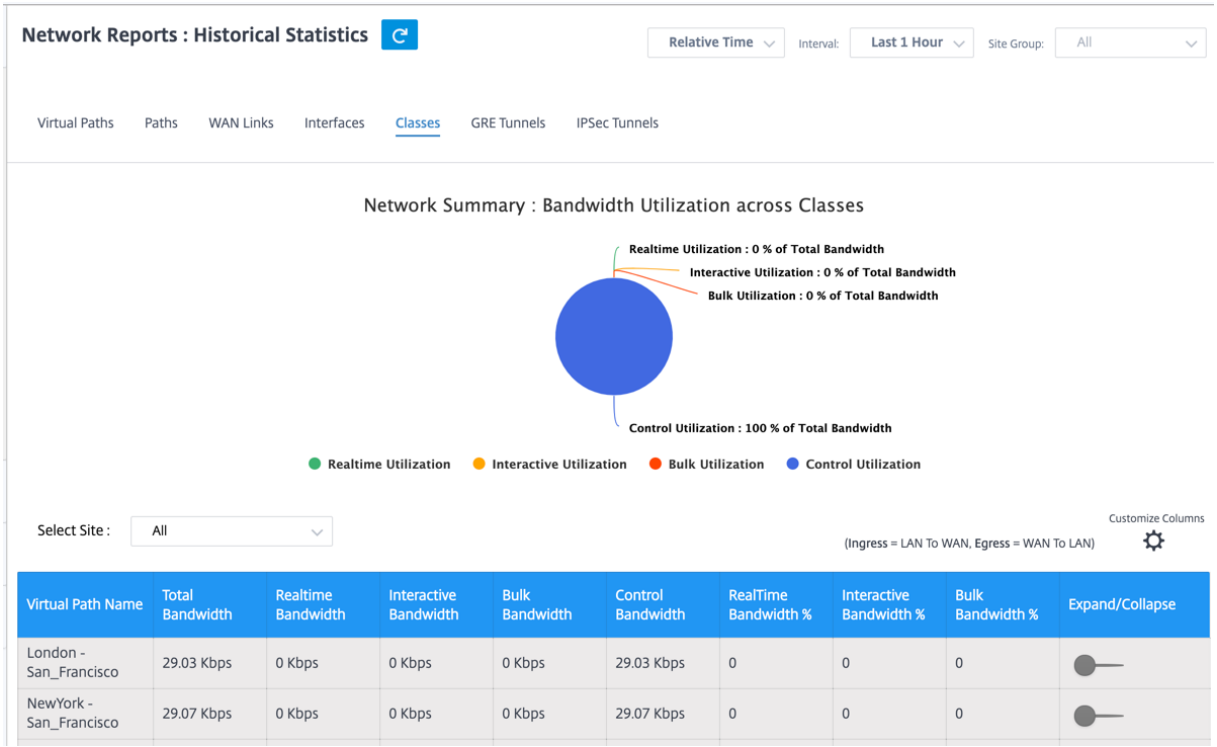
- 接口名称：以太网接口的名称。
- **Tx** 带宽：传输的带宽。
- **Rx** 带宽：接收的带宽。

- 错误：在所选时间段内观察到的错误数。
- 展开/折叠：您可以根据需要展开或折叠数据。

班级

可以将虚拟服务分配给特定的 QoS 类别，不同的带宽限制可以应用于不同的类别。

要查看 类别 统计数据，请导航到 报告 > 统计数据 > 类别 选项卡。



您可以查看以下指标：

- **QoS** 类别：类名。
- 带宽：传输的带宽。
- 数据量：发送的数据，以 Kbps 为单位。
- 丢弃量：丢弃的数据百分比。
- 删除百分比：丢弃的数据百分比。
- 展开/折叠：您可以根据需要展开或折叠数据。

GRE 通道

您可以使用通道机制在另一个协议中传输一个协议的数据包。携带其他协议的协议称为传输协议，而携带的协议称为乘客协议。通用路由封装 (GRE) 是一种通道机制，它使用 IP 作为传输协议，并可以传输许多不同的乘客协议。

通道源地址和目标地址用于标识通道中虚拟点对点链路的两个端点。有关在 Citrix SD-WAN 设备上配置 GRE 隧道的更多信息，请参阅 GRE 隧道。

要查看 **GRE** 隧道 统计信息，请导航到 报告 **>** 统计信息 **> GRE** 隧道 选项卡。

您可以查看以下指标：

- 站点名称：站点名称。
- **Tx** 带宽：传输的带宽。
- **Rx** 带宽：接收的带宽。
- 丢弃的数据包：由于网络拥塞而丢弃的数据包数。
- 已分段的数据包：分段的数据包数。数据包将分段以创建小型数据包，该数据包可以通过传输的 MTU 小于原始数据报。碎片由接收主机重新组装。
- 展开/折叠：您可以根据需要展开或折叠数据。

IPsec 通道

IP 安全 (IPsec) 协议提供安全服务（如加密敏感数据、身份验证、防止重放以及 IP 数据包的数据机密性）。封装安全有效负载 (ESP) 和身份验证头 (AH) 是用于提供这些安全服务的两种 IPSec 安全协议。

在 IPsec 通道模式下，整个原始 IP 数据包受到 IPsec 保护。原始 IP 数据包将打包并加密，并在通过 VPN 通道传输数据包之前添加一个新 IP 报头。
有关在 Citrix SD-WAN 设备上配置 IPsec 隧道的更多信息，请参阅 IPsec 隧道终止。

要查看 **IPsec** 隧道 统计信息，请导航到 报告 **>** 统计信息 **> IPsec** 隧道 选项卡。

您可以查看以下指标：

- 通道名称：通道名称。
- 通道状态：IPsec 通道状态。
- **MTU**：最大传输单位—可通过特定链路传输的最大 IP 数据报的大小。
- 收到的数据包：收到的数据包数。
- 发送的数据包：已发送的数据包数。
- 丢弃的数据包：由于网络拥塞而丢弃的数据包数。
- 丢弃的字节数：丢弃的字节数。
- 展开/折叠：您可以根据需要展开或折叠数据。

实时统计

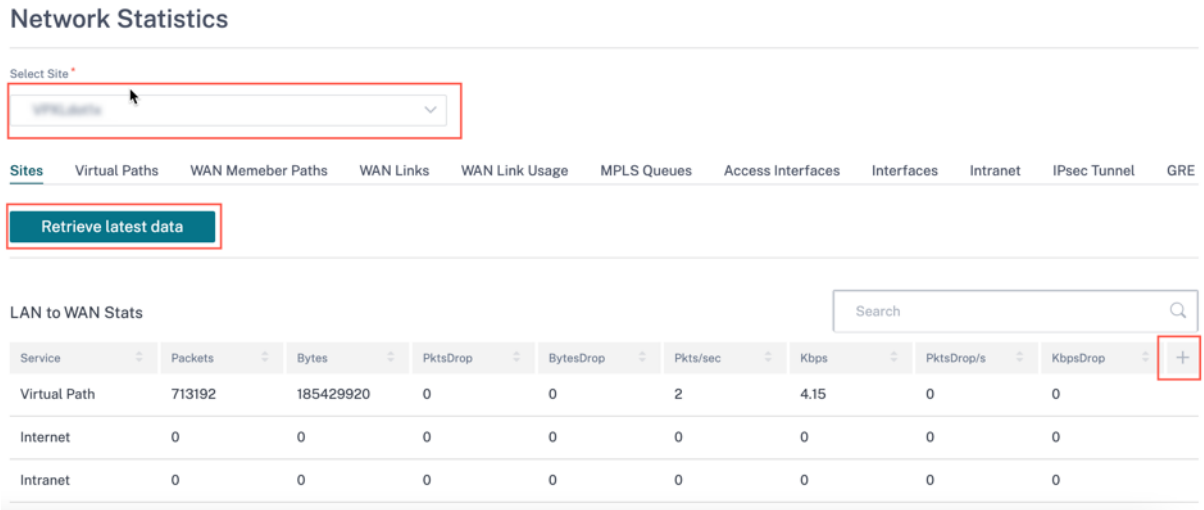
实时统计数据页面显示客户级别的以下统计信息：

网络统计信息

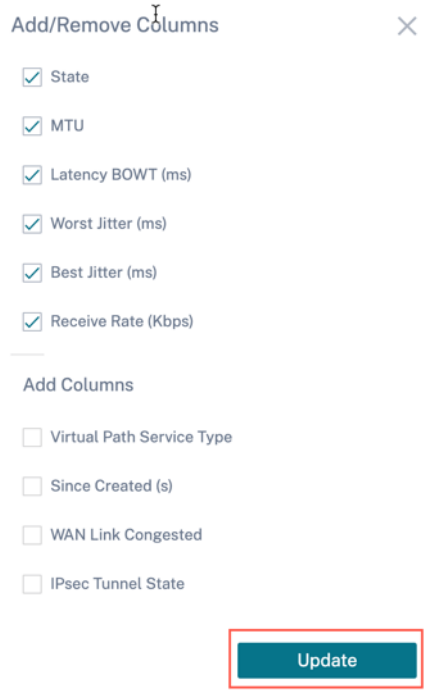
网络统计 页面在“报告”> “实时”> “网络统计”下提供以下实时统计信息：

- 站点
- 虚拟路径
- WAN 成员路径
- WAN 链接
- WAN 链路使用情况
- MPLS 队列
- 访问接口
- 接口
- Intranet
- IPsec 隧道
- GRE

要获取实时统计报告，请转到所需的选项卡（例如站点、虚拟路径、WAN 链接），从下拉列表中选择站点，然后单击“检索最新数据”。



单击加号 (+) 在统计数据表中添加或删除任何列，然后单击 更新。

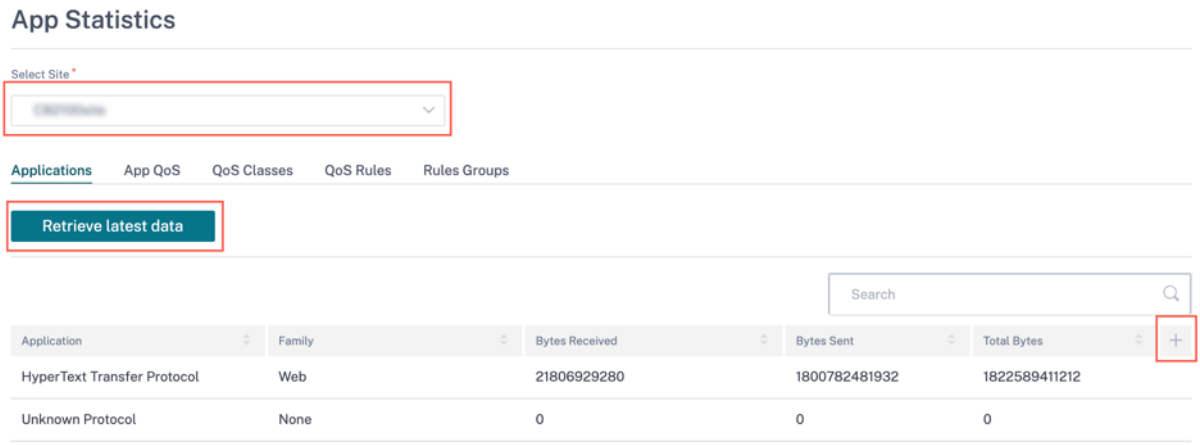


应用程序统计信息

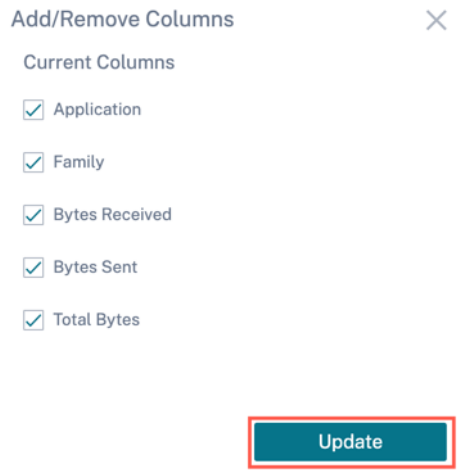
应用程序统计 信息页面在“报告”**>** “实时”**>** “应用程序统计”下提供以下实时统计信息：

- 应用程序
- 应用程序 QoS
- QoS 类别
- QoS 规则
- 规则组

要获取实时统计报告，请转到所需的选项卡（例如应用程序、QoS 规则、QoS 类别），从下拉列表中选择站点，然后单击“检索最新数据”。



如果要在统计表中添加或删除任何列，请单击加号 (+)，然后单击 更新。

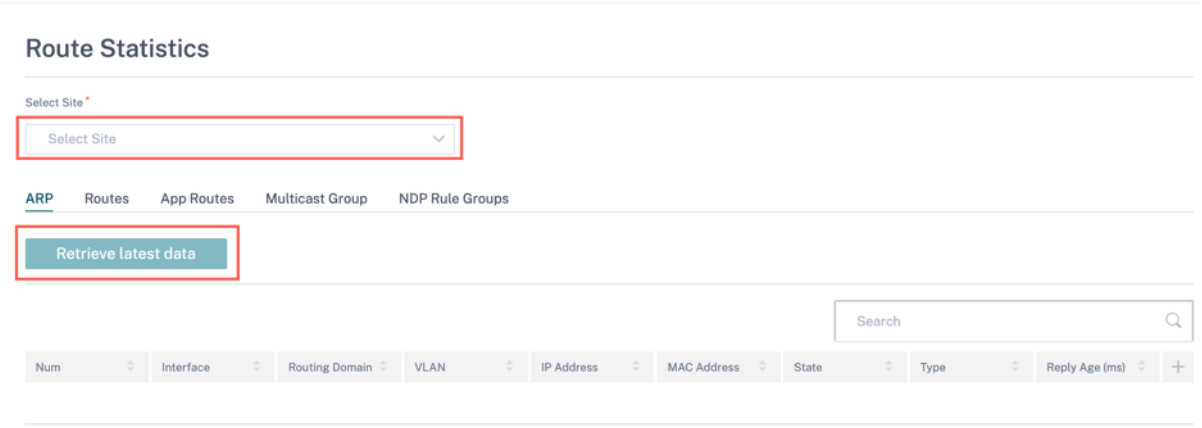


路由统计

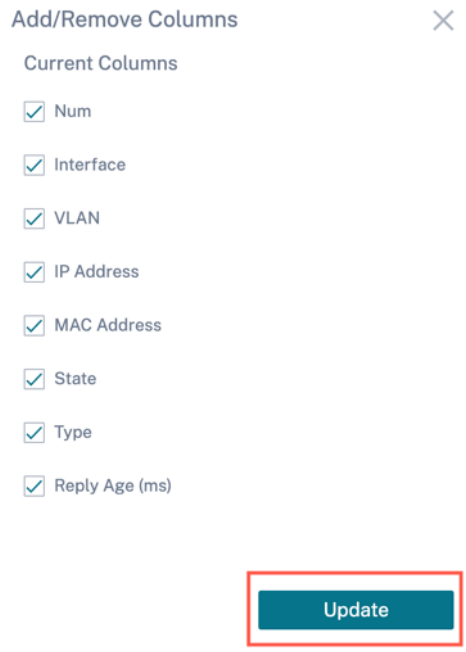
“路由统计”页面在“报告” > “实时” > “路径统计”下提供以下实时统计信息：

- ARP
- 路由
- 应用程序路由
- 观察到的协议
- 多播组
- NDP 规则组

要获取实时统计报告，请转到所需的选项卡（例如 ARP、路由、应用程序路由），从下拉列表中选择站点，然后单击“检索最新数据”。

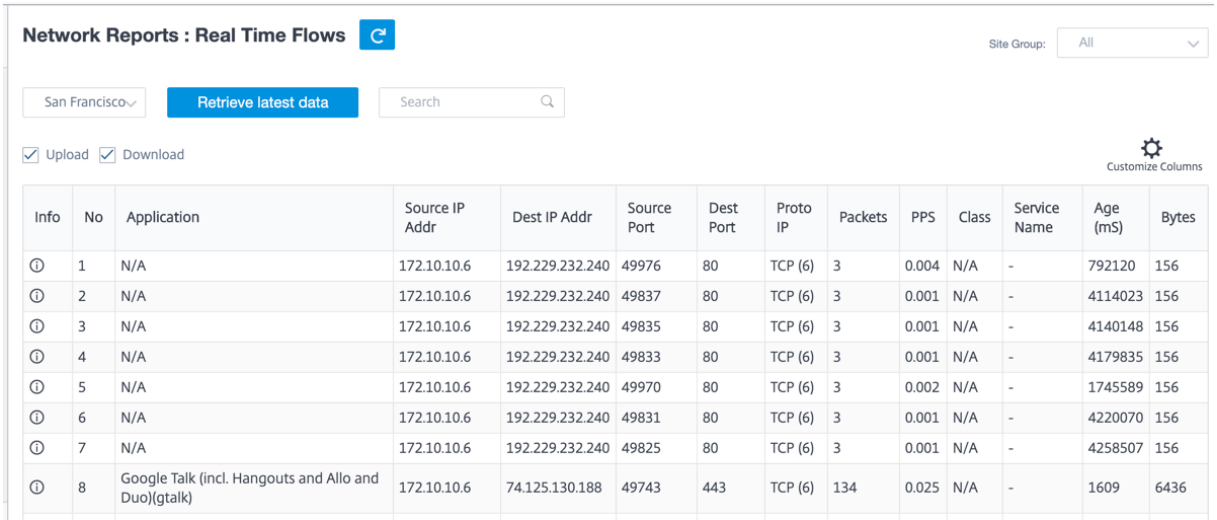


如果要在统计表中添加或删除任何列，请单击加号 (+)，然后单击 更新。



流

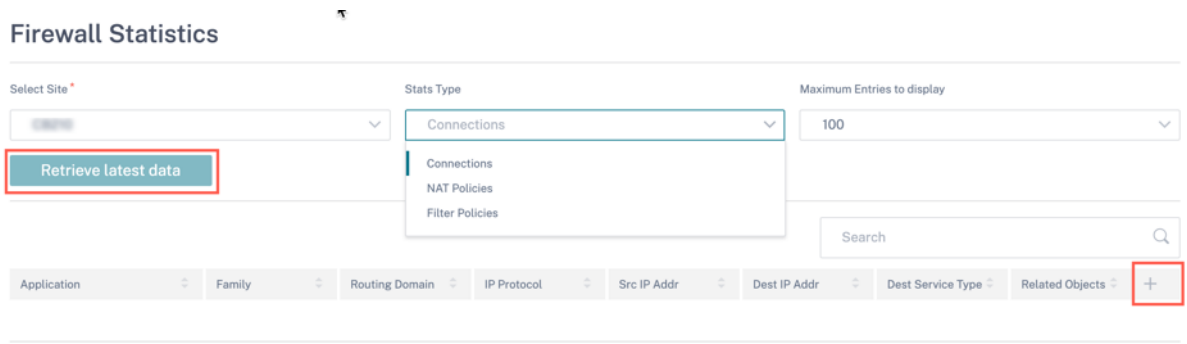
在网络级别，从下拉列表中选择站点，然后才能获取统计信息。流 量功能提供与通过设备的特定会话相关的单向流量信息。这将提供有关流程所属目标服务类型的信息，以及与规则和类型以及传输模式相关的信息。



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

防火墙统计信息

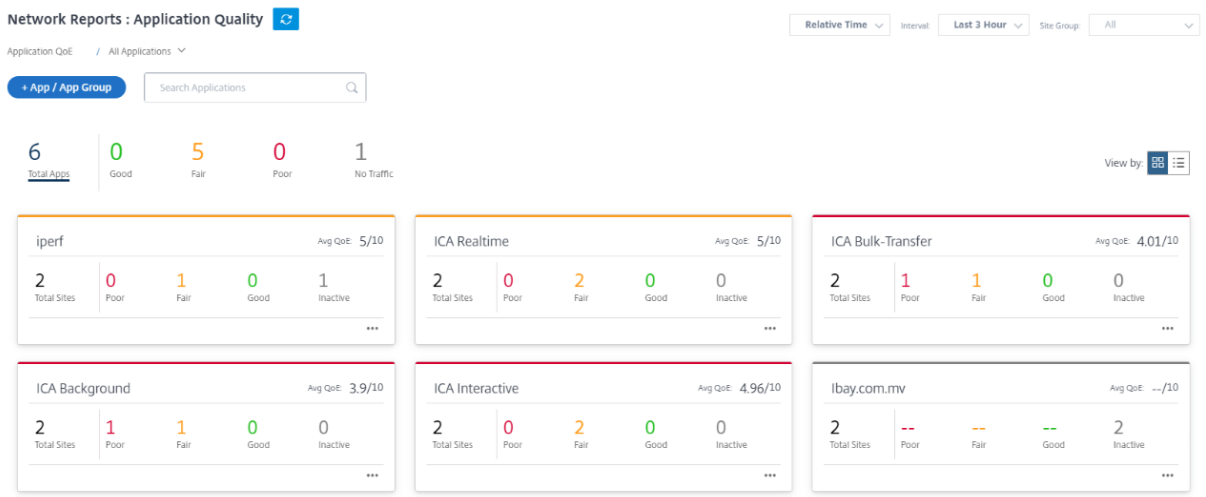
在网络级别，从下拉列表中选择站点，然后才能获取统计信息。防火墙静态 根据配置的防火墙操作提供与特定会话相关的连接状态。防火墙连接还提供有关连接来源和目标的完整详细信息。



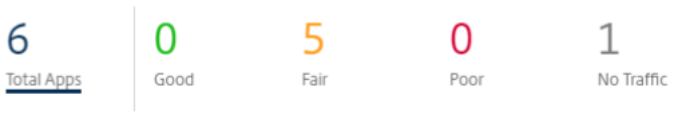
应用质量

应用程序 QoE 是 SD-WAN 网络中应用程序体验质量的度量标准。它测量通过两个 SD-WAN 设备之间的虚拟路径的应用程序的质量。应用程序 QoE 分数是介于 0 到 10 之间的值。它所属的分数范围决定了应用程序的质量。应用程序 QoE 使网络管理员能够审查应用程序的体验质量，并在质量低于可接受阈值时采取主动措施。

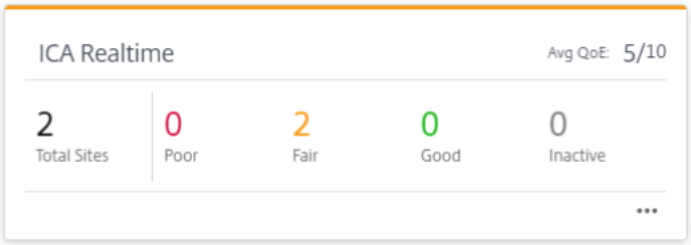
质量	范围	颜色编码
良好	8–10	绿色
一般	4–8	橙色
不佳	0–4	红色



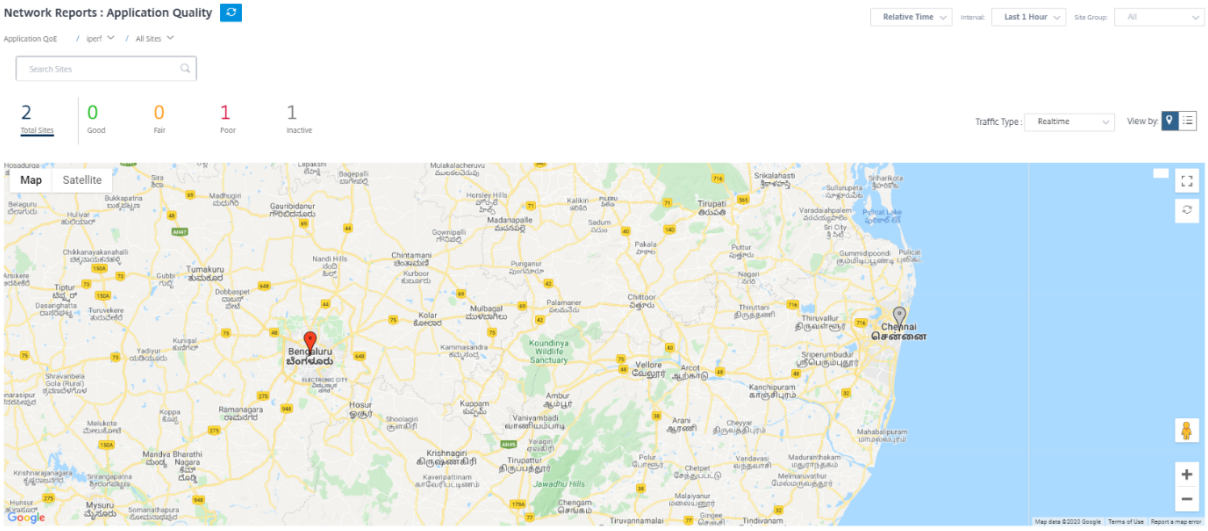
仪表板顶部显示应用程序的总数以及网络中应用程序 QoE 良好、一般或较差的应用程序数量。它还显示没有任何流量的应用程序的数量。



单个应用程序卡显示特定应用程序的应用程序 QoE 差、公平或良好的站点的数量。它还显示未主动使用该应用程序的站点的数量。Avg QoE 是应用程序在网络中所有站点的平均 QoE 分数。

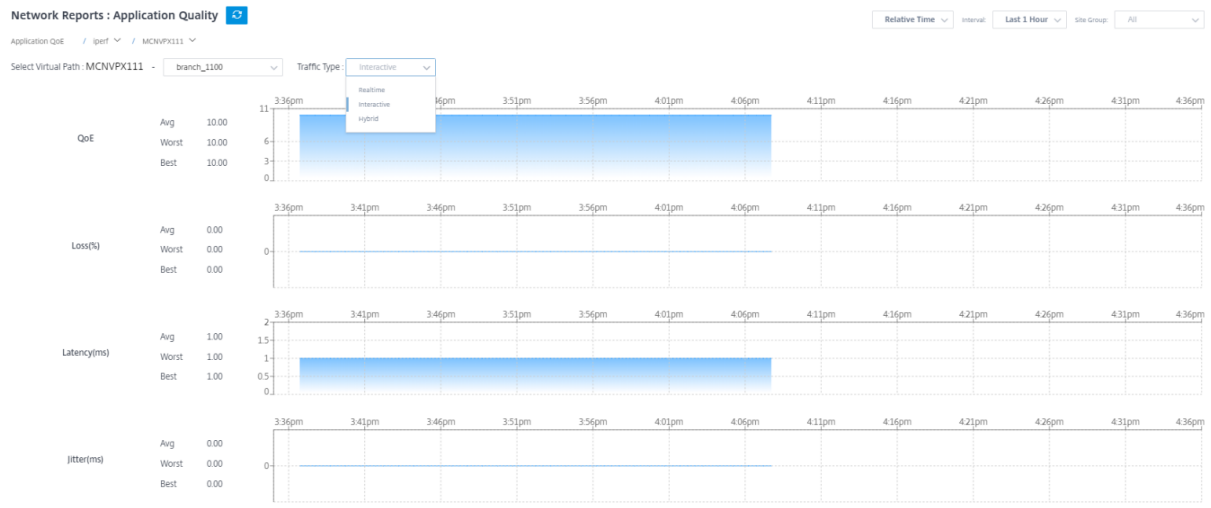


单击单个申请卡可查看有关所选应用程序具有良好、公平或不佳应用程序 QoE 的站点数量的详细信息。将显示运行选定应用程序的所有站点的地图视图。单击地图中的站点以进一步向下钻取并查看站点上各种虚拟路径的应用程序 QoE 统计信息。



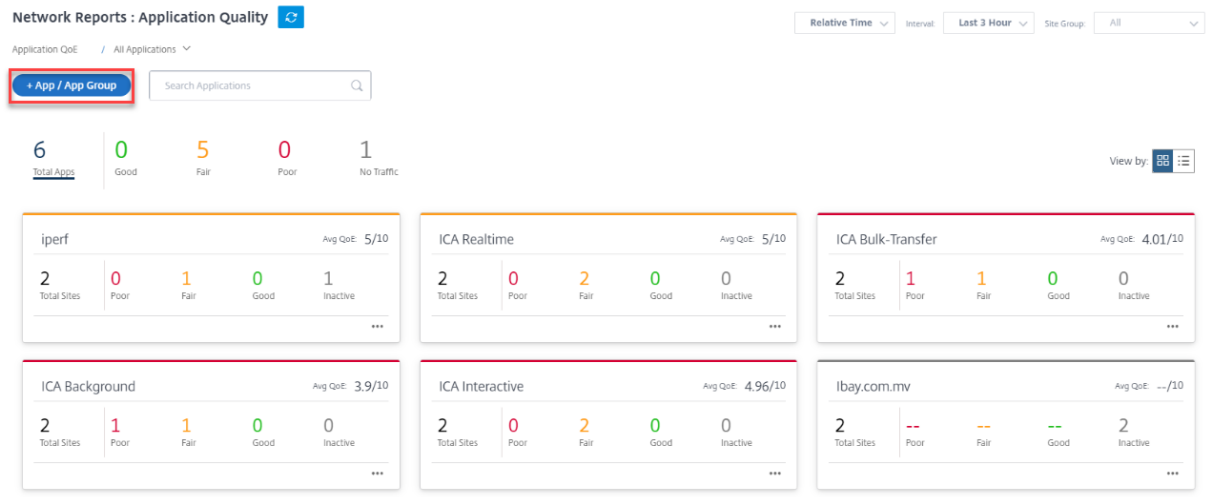
您可以查看所选时间范围内的实时、交互式和混合流量的以下指标：

- **QoE**：流量的 QoE 分数。
- 损失：流量的损失百分比。
- 延迟：流量的延迟（以毫秒为单位）。
- 抖动：观察到的流量抖动（以毫秒为单位）。

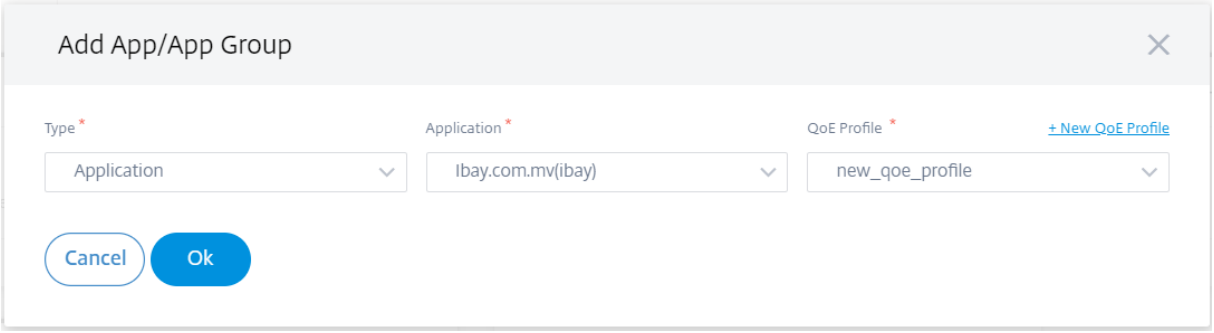


应用程序 **QoE** 配置文件

单击 **+ App/App Gro** up 将应用程序、自定义应用程序或应用程序组映射到默认或自定义 QoE 配置文件。

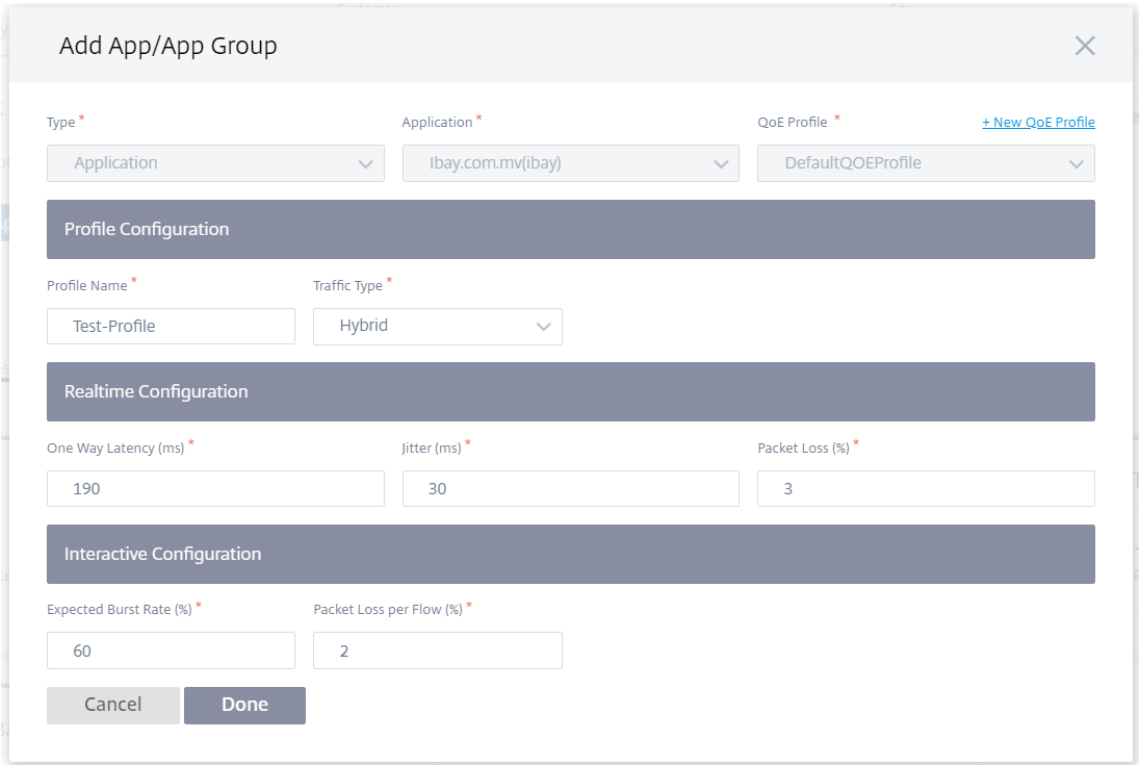


QoE 配置文件定义了实时、交互式和混合流量的阈值。QoE 配置文件中的 QoE 阈值将应用于选定的应用程序或应用程序组。



单击 **+** 新建 **QoE** 配置文件 以创建新的应用程序 QoE 配置文件并输入以下参数的值：

- 配置文件名称：用于标识为实时和交互式流量设置阈值的配置文件的名称。
- 流量类型：选择流量类型：实时、交互或混合。如果流量类型为混合，则可以配置实时和交互式 QoE 配置文件阈值。
- 实时 配置：为选择实时 QoS 策略的流量配置阈值。达到以下延迟、丢失和抖动阈值的实时应用程序流被视为质量良好。
  - 单向延迟：以毫秒为单位的延迟阈值。默认的 QoE 配置文件值为 160 毫秒。
  - 抖动：抖动阈值（以毫秒为单位）。默认的 QoE 配置文件值为 30 毫秒。
  - 数据包丢失：丢包的百分比。默认的 QoE 配置文件值为 2%。
- 交互式配置：为选择交互式 QoS 策略的流量配置阈值。交互式应用程序的流程如果达到以下突发率和数据包丢失阈值，则被认为质量良好。
  - 预期突发速率：预期突发率的百分比。出口突发率必须至少为配置的入口突发率百分比。默认的 QoE 配置文件值为 60%。
  - 每个流量的数据包丢失率：丢包的百分比。默认的 QoE 配置文件值为 1%。



新添加的应用程序显示在“应用程序质量”控制面板中。

您还可以从应用程序和 DNS 设置中定义和配置应用程序 QoE 了解更多信息，请参阅 应用程序质量配置文件 和 应用程序质量配置。

网站报告

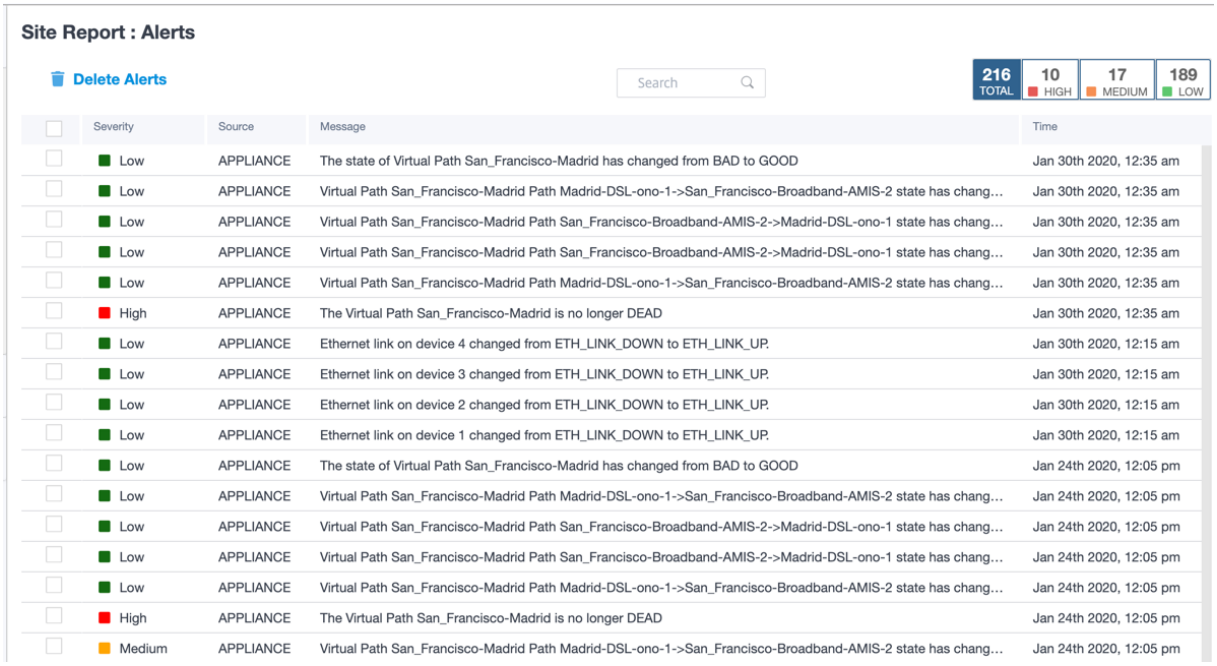
October 21, 2022

站点报告 提供站点级警报、使用趋势、质量、设备信息和防火墙统计信息的可见性。

警报

站点管理员可以查看在站点级别生成的所有事件和警报的详细报告。

它包括严重性、警报产生地点、警报消息、时间和其他详细信息。



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

可以根据需要使用合适的筛选选项，例如：查找站点上的所有高严重性警报或在特定时间段内发生的警报。

您也可以选择和清除警报。

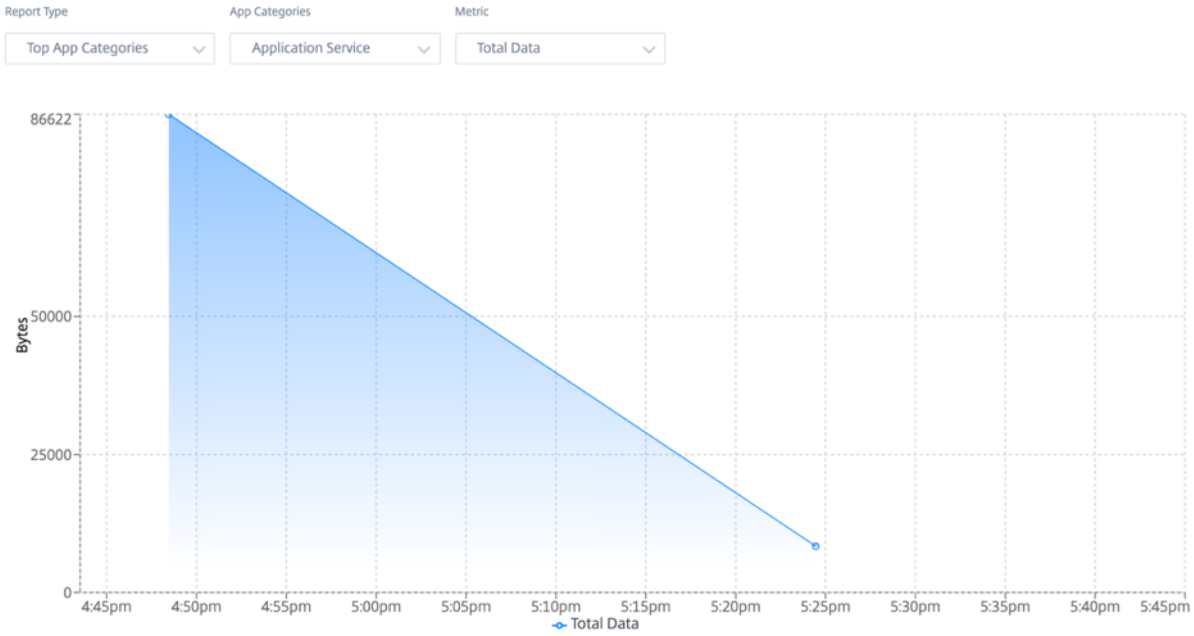
使用情况

站点管理员可以查看特定站点中的使用趋势 ，例如“热门应用程序”、“热门应用程序类别”和“应用程序带宽”。

热门应用程序和应用程序类别

热门应用程序 和 热门应用程序类别 图表显示了站点中广泛使用的顶级应用程序和热门应用程序系列。这允许您分析数据消耗模式，并为站点内的每一类数据重新分配带宽限制。

您还可以查看带宽使用情况统计信息。在所选时间间隔内收集带宽统计信息。您可以根据 报告类型、应用程序或应用程序类别 以及 指标筛选统计报告。

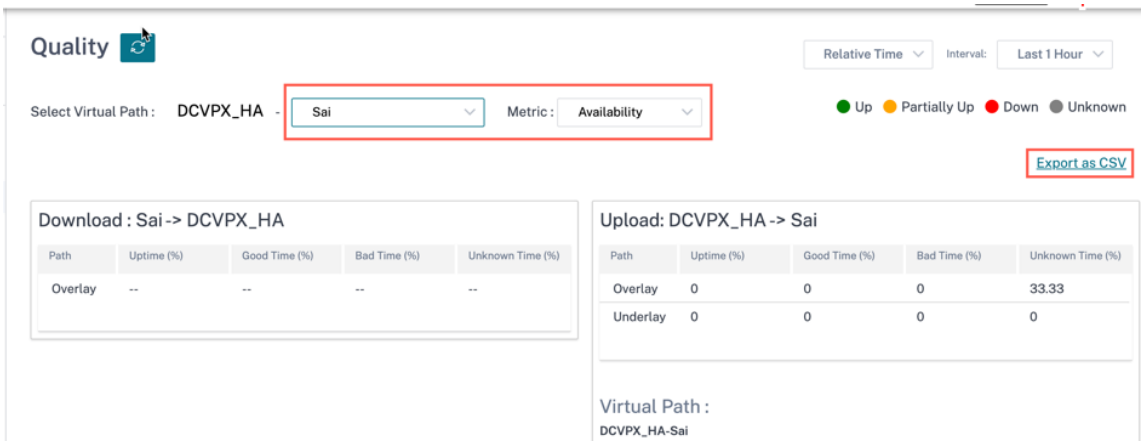


- 报告类型：从列表中选择 热门应用程序或应用程序类别。
- 应用程序/应用程序类别：从列表中选择热门应用程序或类别（例如网络服务）。
- 指标：从列表中选择带宽指标（例如总数据、传入数据、总带宽）。

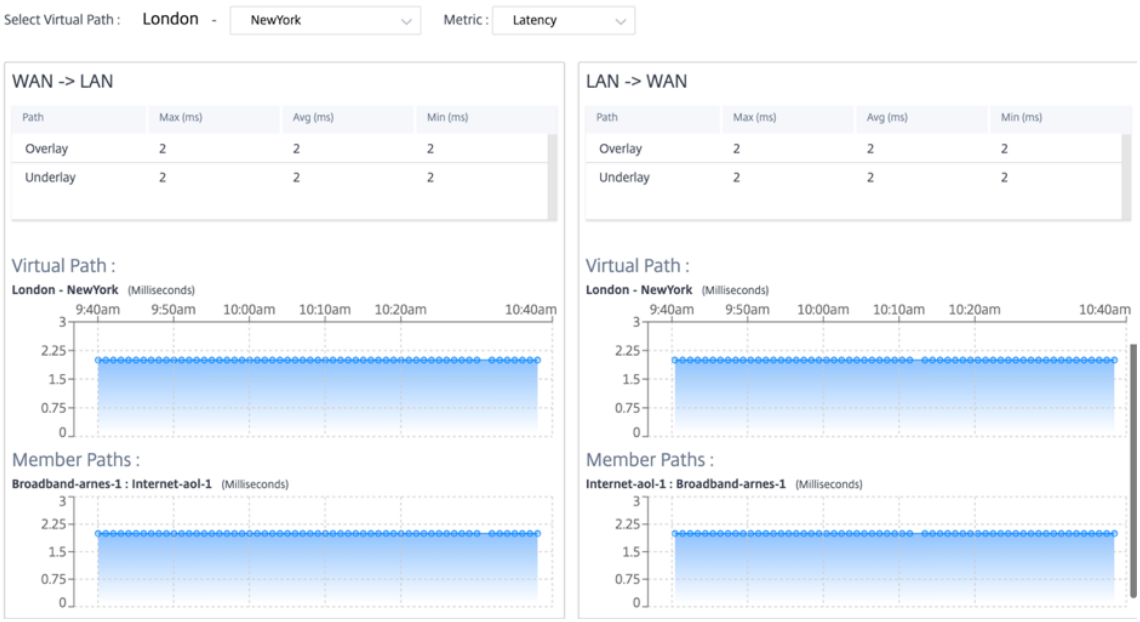
质量

站点管理员可以使用质量报告来分析站点上每个 QoS 指标（例如可用性、丢失、延迟和抖动）的体验质量 (QoE)。显示叠加虚拟路径及其基础成员路径的质量指标。

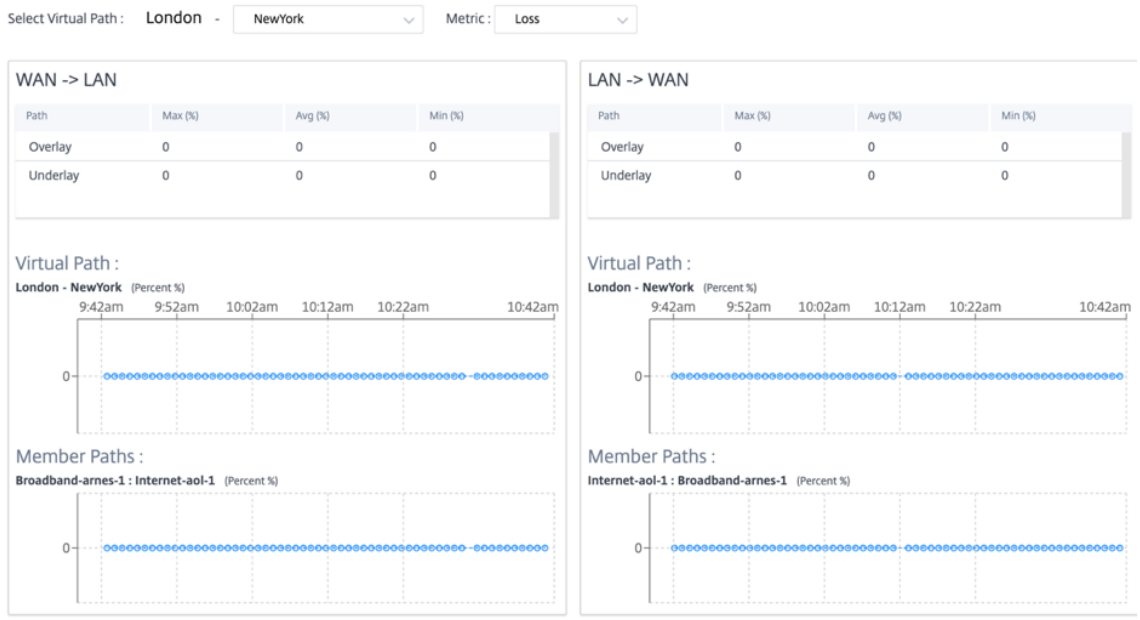
- 可用性



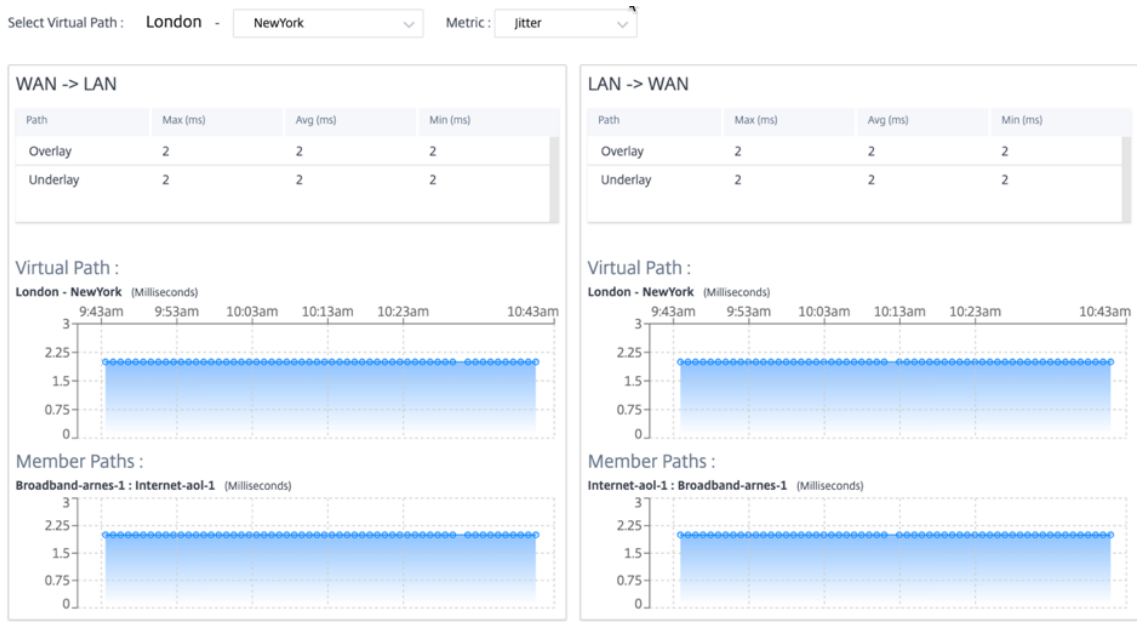
- 延迟



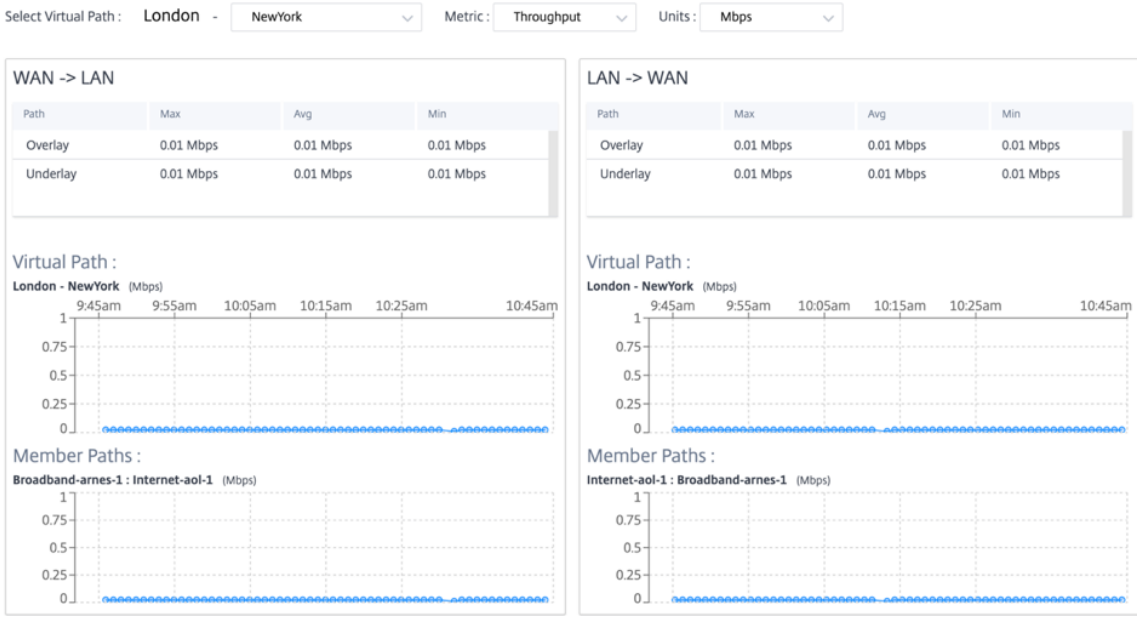
- 损失



- 抖动



- 吞吐量

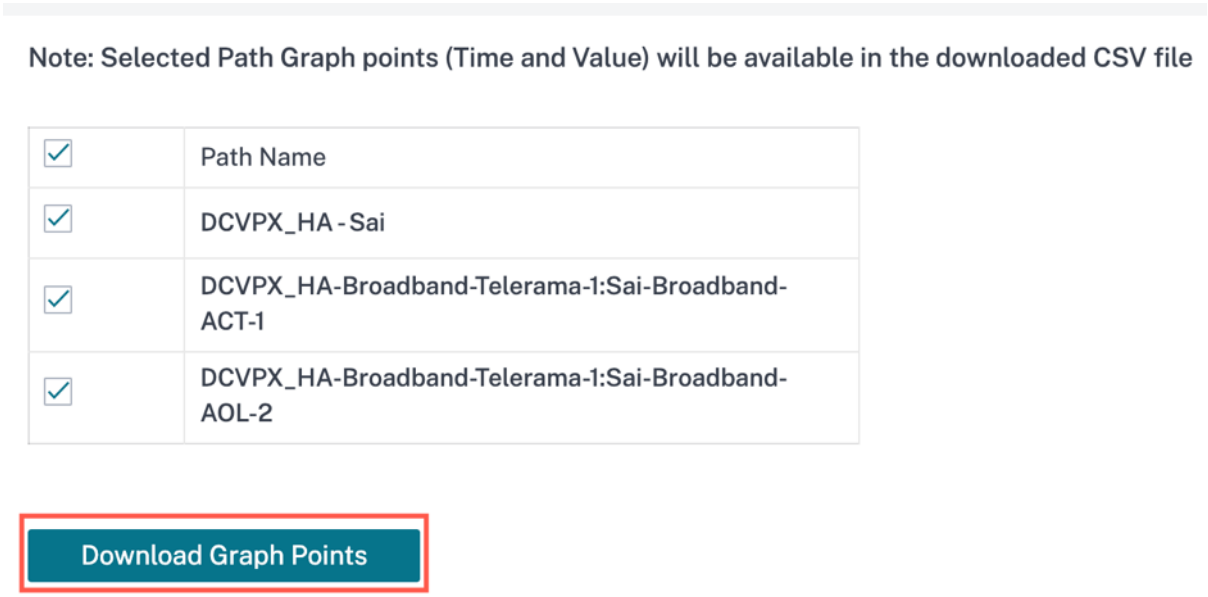


以 **CSV** 格式导出

使用 导出为 **CSV** 功能，您可以将任何时间序列（每小时、每周等）的路径图点（虚拟/成员路径）下载为 excel 逗号分隔值 (CSV) 文件，并能够绘制特定站点报告的所有不同数据点。

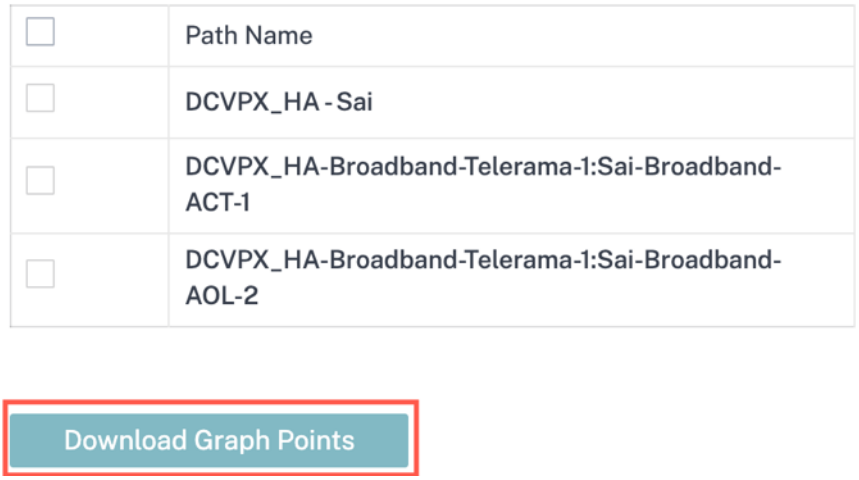
要将路径图下载/导出为 CSV，请导航到 报告 > 站点级别的 质量。从下拉列表中选择站点和指标，然后单击“导出为 **CSV** ”链接。

选择要获取数据的路径，然后单击“下载图点”。

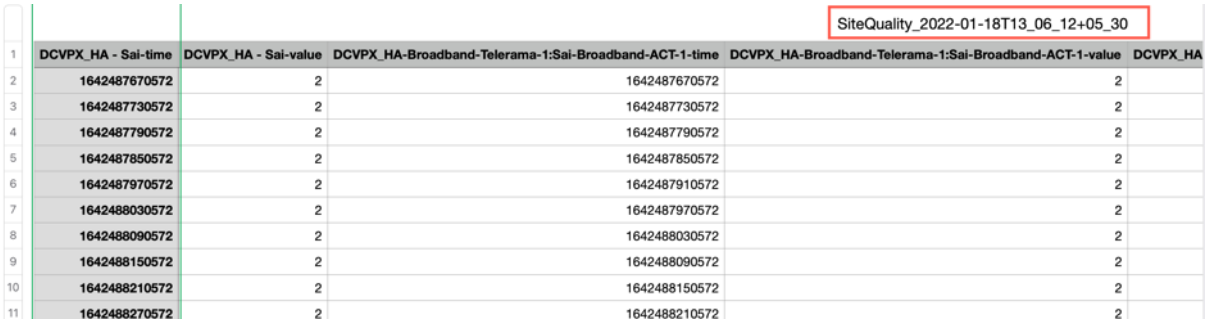


默认情况下，所有路径复选框都是自动选中的。您可以根据需要对其进行修改。

> 注意
>
> 如果未选择任何路径，则 下载图点 按钮将保持禁用状态。



下载的 CSV 文件的命名惯例是 **SiteQ** uality 后跟下载的时间戳。您可以使用一对时间和值以及唯一标识符来查看每条路径。您可以看到以毫秒为单位的时间和以单位表示的值。



			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	

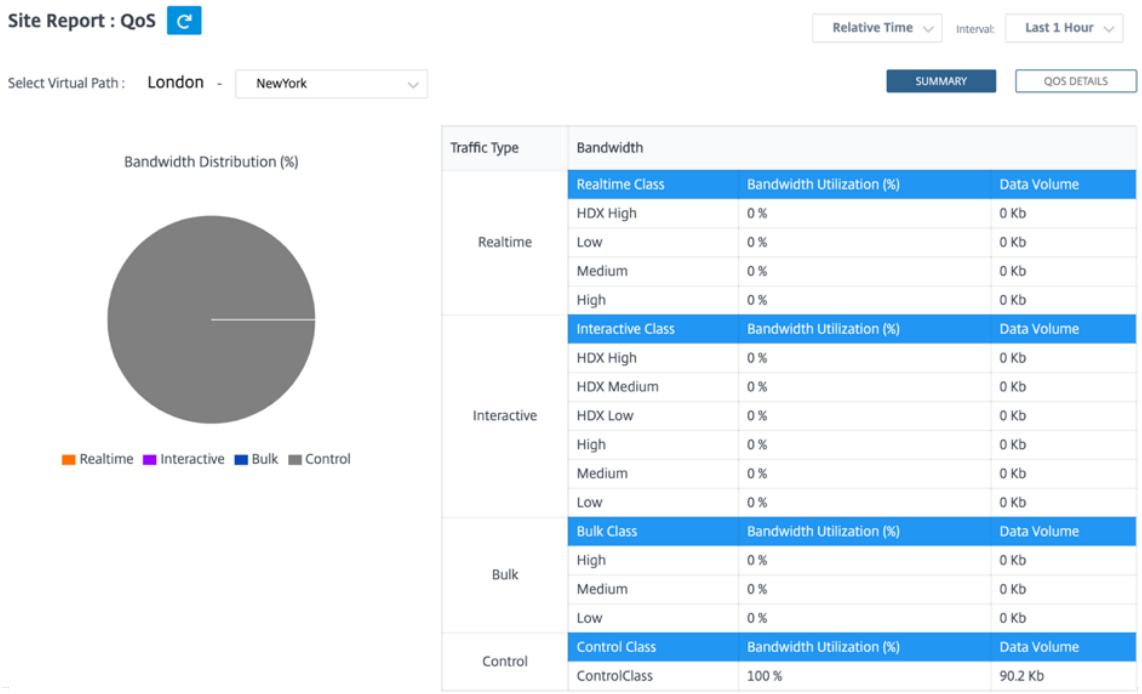
根据以下指标选择，您可以看到 CSV 文件中正在生成不同的值：

- 损失：值以百分比显示。
- 延迟和抖动：该值以毫秒为单位显示。
- 吞吐量：该值以 Kbps 为单位显示。
- 可用性：显示向上、部分向上、向下和未知时间的路径。
  - 如果值为 4，则路径处于 Up 状态。
  - 如果值为 3，则路径部分处于 Up 状态。
  - 如果该值小于 3，则路径处于 Bad/down 状态。

服务质量

服务质量 (QoS) 管理数据流量，以减少网络上的数据包丢失、延迟和抖动。有关更多信息，请参阅 服务质量。以下是查看服务质量 (QoS) 报告的两种方法：

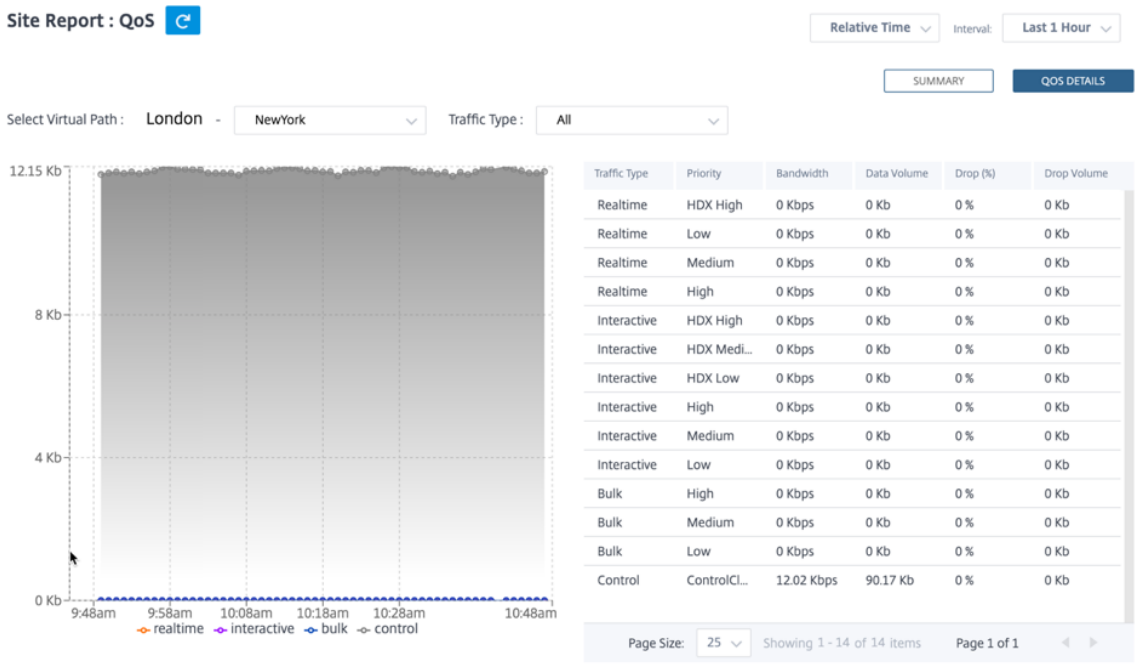
- 摘要视图：摘要视图概述了所有类型的流量（实时、交互式、批量流量以及网络和每个站点的控制）的带宽消耗。



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

  - 实时：用于低延迟、低带宽、时间敏感型流量。实时应用程序对时间很敏感，但实际上并不需要高带宽（例如 IP 语音）。实时应用程序对延迟和抖动敏感，但可以容忍一些损失。
  - 交互式：用于具有低到中等延迟要求和低到中等带宽要求的交互式流量。交互式应用程序以鼠标点击或光标移动的形式涉及人工输入。通常情况下，在客户端与服务器之间进行交互。通信可能不需要高带宽，但对丢失和延迟非常敏感。但是，服务器到客户端确实需要高带宽才能传输图形信息，这可能对丢失不敏感。
  - 批量：用于可以容忍高延迟的高带宽流量。处理文件传输和需要高带宽的应用程序将分类为散装类。这些应用很少涉及人为干扰，主要由系统自己处理。
  - 控制：用于传输包含路由、调度和链路统计信息的控制数据包。

- 详细视图：详细视图记录了与叠加虚拟路径相关的每个 QoS 类别的带宽消耗、流量、丢弃的数据包等趋势。您可以根据两个站点之间的虚拟路径查看 QoS 统计信息。



历史统计

对于每个站点，您可以查看以下网络参数的图表的统计信息：

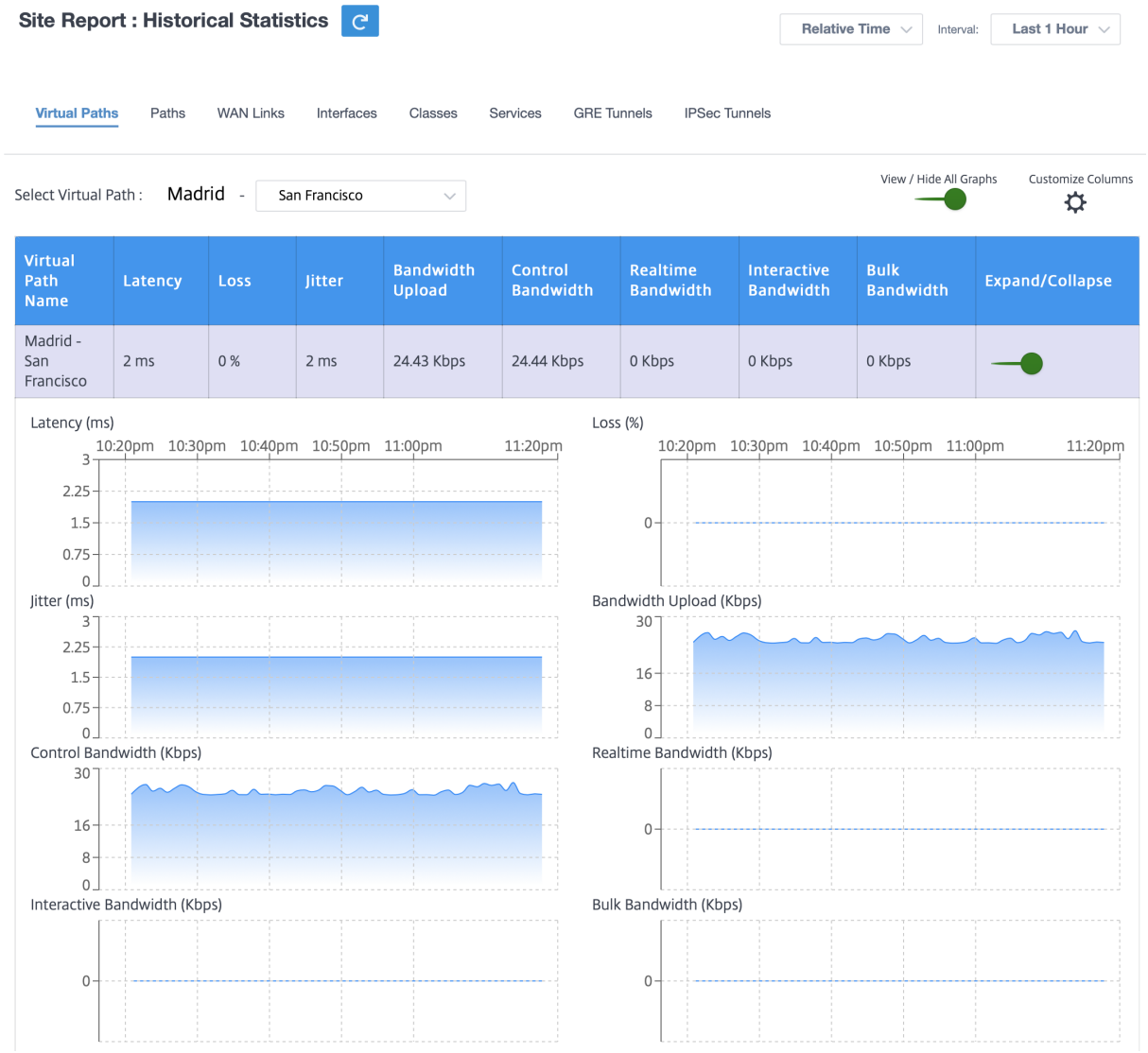
- 虚拟路径
- 路径
- WAN 链接
- 接口
- 班级
- 服务
- GRE 通道
- IPsec 通道

统计数据以图表形式收集。这些图表以时间表与使用情况的关系绘制而成，使您能够了解各种网络对象属性的使用趋势。您可以查看网络范围内应用程序统计信息的图表。

您可以根据需要查看或隐藏图表并自定义列。

虚拟路径

要查看 虚拟路径 统计信息，请导航到 报告 **>** 统计信息 **>** 虚拟路径 选项卡。



您可以查看以下指标：

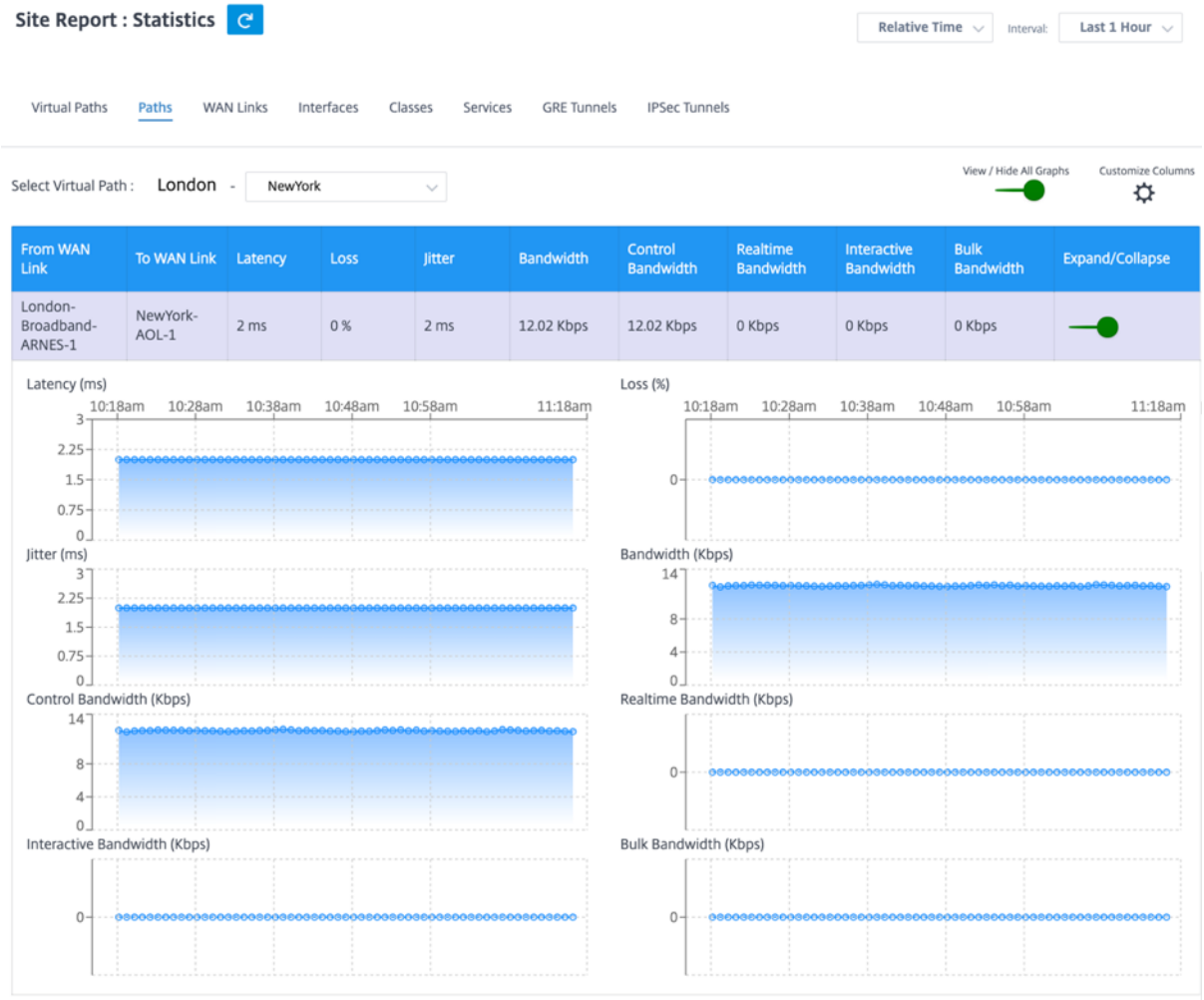
- 虚拟路径名：虚拟路径名。
- 延迟：实时流量的延迟（以毫秒为单位）。
- 丢失：丢失的数据包百分比。
- 抖动：收到的数据包延迟的变化，以毫秒为单位。
- 带宽入口：所选时间段内的 入口（局域网 **>** 广域网）带宽 使用情况。
- 控制带宽：用于传输包含路由、调度和链路统计信息的控制数据包的带宽。
- 实时带宽：属于 SD-WAN 配置中实时类类型的应用程序消耗的带宽。此类应用程序的性能在很大程度上取决于网络延迟。延迟数据包比丢失的数据包（例如 VoIP、Skype for Business）差。
- 交互带宽：属于 SD-WAN 配置中交互类类型的应用程序消耗的带宽。此类应用程序的性能取决于网络延迟以及数据包丢失（例如 XenDesktop、XenApp）的巨大程度。
- 批量带宽：属于 SD-WAN 配置中批量类别类型的应用程序消耗的带宽。这些应用程序几乎不需要人工干预，主

要由系统本身处理（例如 FTP、备份操作）。

- 展开/折叠：您可以根据需要展开或折叠数据。

路径

要查看 路径 统计信息，请导航到 报告 > 统计信息 > 路径 选项卡。



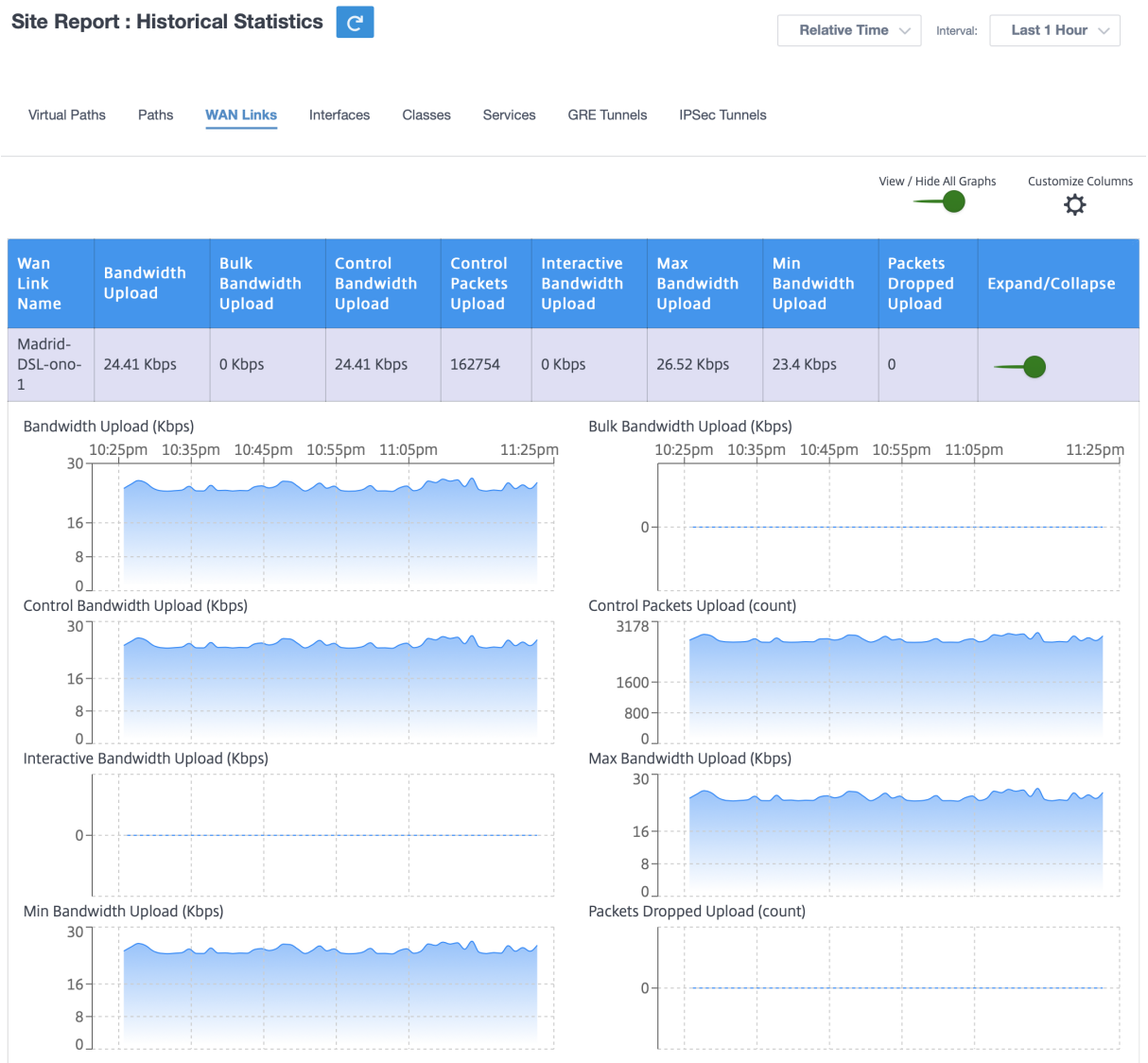
您可以查看以下指标：

- 来自 **WAN** 链接：源 WAN 链接。
- 至 **WAN** 链接：目标 WAN 链接。
- 延迟：实时流量的延迟（以毫秒为单位）。
- 丢失：丢失的数据包百分比。
- 抖动：收到的数据包延迟的变化，以毫秒为单位。
- 带宽：所有数据包类型消耗的总带宽。带宽 = 控制带宽 + 实时带宽 + 交互带宽 + 批量带宽。
- 控制带宽：用于传输包含路由、调度和链路统计信息的控制数据包的带宽。

- 实时带宽：属于 SD-WAN 配置中实时类类型的应用程序消耗的带宽。此类应用程序的性能在很大程度上取决于网络延迟。延迟数据包比丢失的数据包（例如 VoIP、Skype for Business）差。
- 交互带宽：属于 SD-WAN 配置中交互类类型的应用程序消耗的带宽。此类应用程序的性能取决于网络延迟以及数据包丢失（例如 XenDesktop、XenApp）的巨大程度。
- 批量带宽：属于 SD-WAN 配置中批量类别类型的应用程序消耗的带宽。这些应用程序几乎不需要人工干预，主要由系统本身处理（例如 FTP、备份操作）。
- 展开/折叠：您可以根据需要展开或折叠数据。

WAN 链接

要查看 **WAN** 链接 级别的统计信息，请导航到 报告 **>** 统计信息 **> WAN** 链接 选项卡。



您可以查看以下指标：

- **WAN** 链接名称：路径名。
- 带宽入口：所选时间段内的 入口（局域网 **>** 广域网）带宽 使用情况。
- 批量带宽入口：所选时间段内批量流量使用的 入口（**LAN > WAN**）虚拟路径带宽。
- 控制带宽入口：所选时间段内控制流量使用的 入口（**LAN > WAN**）虚拟路径带宽。
- 控制数据包入口：所选时间段内的 入口（局域网 **>** 广域网）虚拟路径控制数据包。
- 交互式带宽入口：交互式流量在选定时间段内使用的 入口（局域网 **>** 广域网）虚拟路径带宽。
- 最大带宽入口：所选时间段内一分钟内使用的最大入口（**LAN > WAN**）带宽。
- 最小 @@ 带宽入口：所选时间段内一分钟内使用 的最小入口（**LAN > WAN**）带宽。
- 展开**/**折叠：您可以根据需要展开或折叠数据。

接口

接口统计报告可帮助您在故障排除期间快速查看是否有任何端口已关闭。您还可以在每个端口查看传输和接收的带宽或数据包详细信息。您还可以查看在特定时间段内这些接口上发生的错误数。

要查看 接口 统计信息，请导航到 报告 **>** 统计信息 **>** 接口 选项卡。

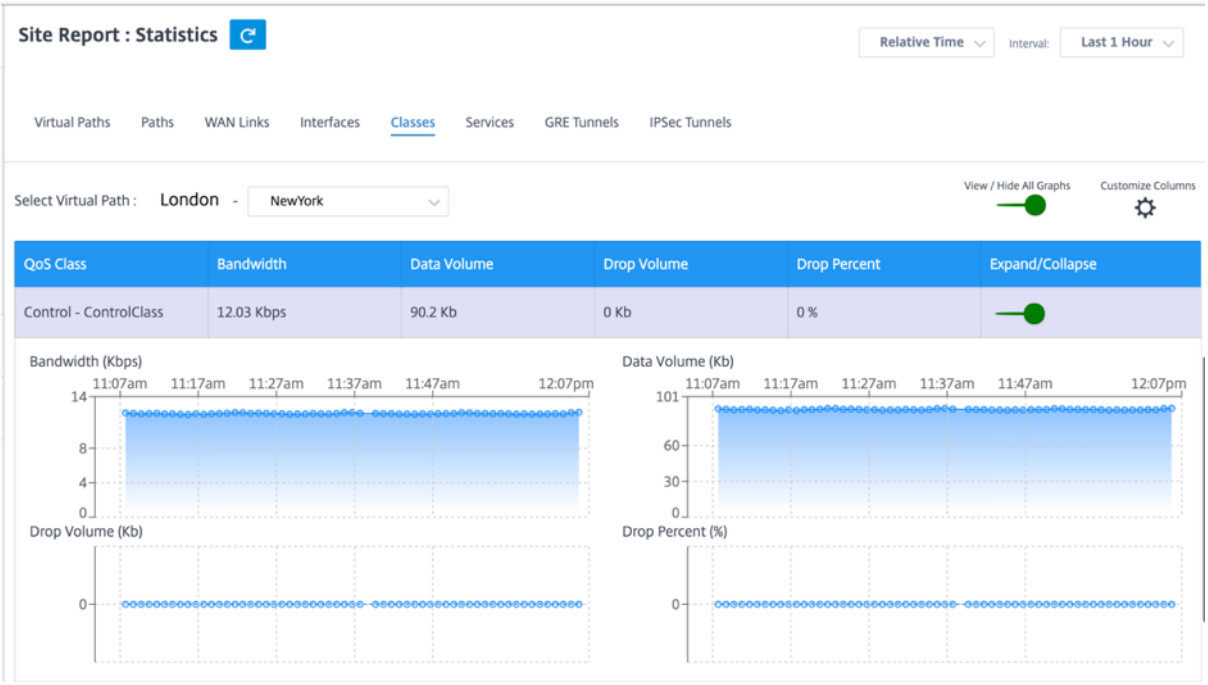
您可以查看以下指标：

- 接口名称：以太网接口的名称。
- **Tx** 带宽：传输的带宽。
- **Rx** 带宽：接收的带宽。
- 错误：在所选时间段内观察到的错误数。
- 展开**/**折叠：您可以根据需要展开或折叠数据。

班级

可以将虚拟服务分配给特定的 QoS 类别，不同的带宽限制可以应用于不同的类别。

要查看 类别 统计数据，请导航到 报告 **>** 统计数据 **>** 类别 选项卡。



您可以查看以下指标：

- **QoS** 类别：类名。
- 带宽：传输的带宽。
- 数据量：发送的数据，以 Kbps 为单位。
- 丢弃量：丢弃的数据百分比。
- 删除百分比：丢弃的数据百分比。
- 展开/折叠：您可以根据需要展开或折叠数据。

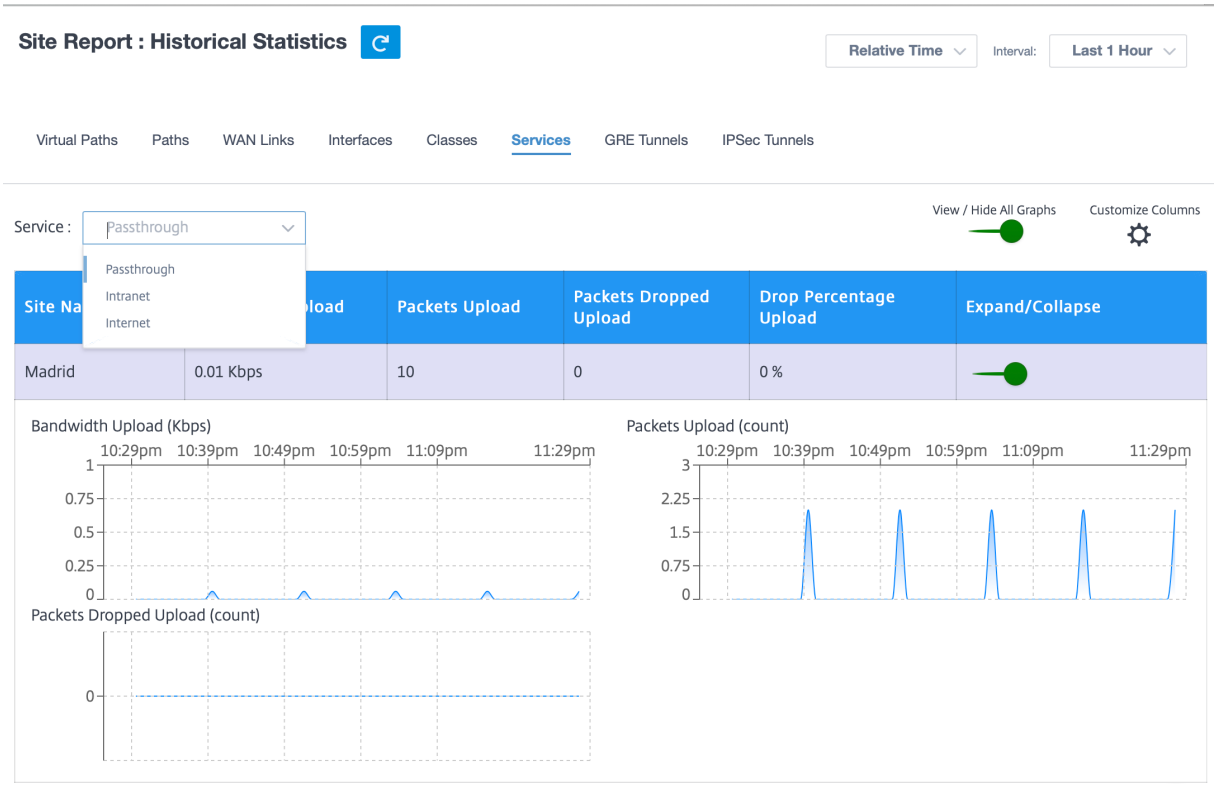
服务

要查看 服务 统计信息，请导航到 报告 **>** 统计 **>** 服务 选项卡。

从列表中选择服务类型。这些选项如下所示：

- 直通—此服务管理未被 SD-WAN 拦截、延迟、调整或更改的流量。定向到直通服务的流量包括广播、ARP 和其他非 IPv4 流量，以及虚拟 WAN 设备本地子网、配置的子网或网络管理员应用的规则上的流量。SD-WAN 不会延迟、形状或更改此流量。因此，必须确保直通流量不会消耗 SD-WAN 设备配置为用于其他服务的 WAN 链接上的大量资源。
- **Intranet** —此服务管理尚未定义为通过虚拟路径进行传输的企业内部网流量。与互联网流量一样，它仍然是未封装的，SD-WAN 通过在拥塞期间限制此流量相对于其他服务类型的速率来管理带宽。在某些情况下，如果为虚拟路径上的 Intranet 回退配置，则通常使用虚拟路径传输的流量可以被视为 Intranet 通信，以保持网络可靠性。

- 互联网—此服务管理企业站点与公共 Internet 上的站点之间的流量。此类型的流量未封装。在拥堵期间，SD-WAN 通过相对于虚拟路径的速率限制互联网流量，主动管理带宽，并根据管理员建立的 SD-WAN 配置管理 Intranet 流量。



您可以查看以下指标：

- 站点名称：站点名称。
- 带宽入口：所选时间段内的 入口（局域网 **>** 广域网）带宽 使用情况。
- 数据包入口：（局域网 **>** 广域网）在所选时间间隔内发送的数据包。
- 展开/折叠：您可以根据需要展开或折叠数据。

GRE 通道

您可以使用通道机制在另一个协议中传输一个协议的数据包。携带其他协议的协议称为传输协议，而携带的协议称为乘客协议。通用路由封装 (GRE) 是一种通道机制，它使用 IP 作为传输协议，并可以传输许多不同的乘客协议。

通道源地址和目标地址用于标识通道中虚拟点对点链路的两个端点。有关在 Citrix SD-WAN 设备上配置 GRE 隧道的更多信息，请参阅 GRE 隧道。

要查看 **GRE** 隧道 统计信息，请导航到 报告 **>** 统计信息 **> GRE** 隧道 选项卡。

您可以查看以下指标：

- 站点名称：站点名称。

- **Tx** 带宽：传输的带宽。
- **Rx** 带宽：接收的带宽。
- 丢弃的数据包：由于网络拥塞而丢弃的数据包数。
- 已分段的数据包：分段的数据包数。数据包将分段以创建小型数据包，该数据包可以通过传输的 MTU 小于原始数据报。碎片由接收主机重新组装。
- 展开/折叠：您可以根据需要展开或折叠数据。

IPsec 通道

IP 安全 (IPsec) 协议提供安全服务（如加密敏感数据、身份验证、防止重放以及 IP 数据包的数据机密性）。封装安全有效负载 (ESP) 和身份验证头 (AH) 是用于提供这些安全服务的两种 IPSec 安全协议。

在 IPsec 通道模式下，整个原始 IP 数据包受到 IPsec 保护。原始 IP 数据包将打包并加密，并在通过 VPN 通道传输数据包之前添加一个新 IP 报头。
有关在 Citrix SD-WAN 设备上配置 IPsec 隧道的更多信息，请参阅 IPsec 隧道终止。

要查看 **IPsec** 隧道 统计信息，请导航到 报告 **>** 统计信息 **> IPsec** 隧道 选项卡。

您可以查看以下指标：

- 通道名称：通道名称。
- 通道状态：IPsec 通道状态。
- **MTU**：最大传输单位—可通过特定链路传输的最大 IP 数据报的大小。
- 收到的数据包：收到的数据包数。
- 发送的数据包：已发送的数据包数。
- 丢弃的数据包：由于网络拥塞而丢弃的数据包数。
- 丢弃的字节数：丢弃的字节数。
- 展开/折叠：您可以根据需要展开或折叠数据。

实时统计

网络统计

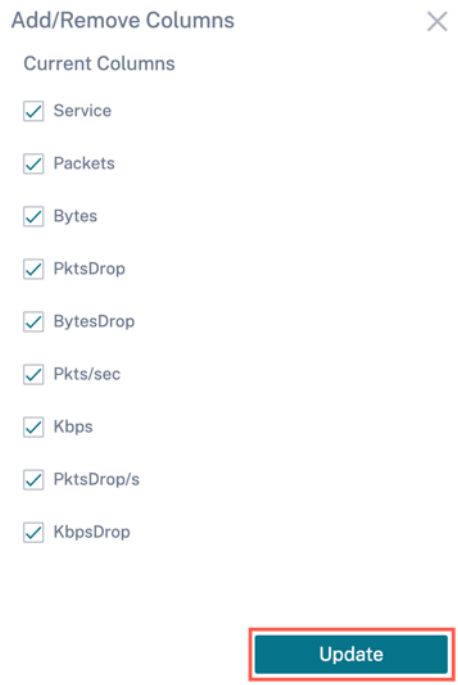
您可以在“报告”**>** “实时”**>** “网络统计”下获得以下实时统计信息：

- 站点
- 虚拟路径
- WAN 成员路径
- WAN 链接
- WAN 链路使用情况
- MPLS 队列
- 访问接口

- 接口
- Intranet
- IPsec 隧道
- GRE

要获取实时统计报告，请转到所需的选项卡（例如站点、虚拟路径、WAN 链接），然后单击“检索最新数据”。

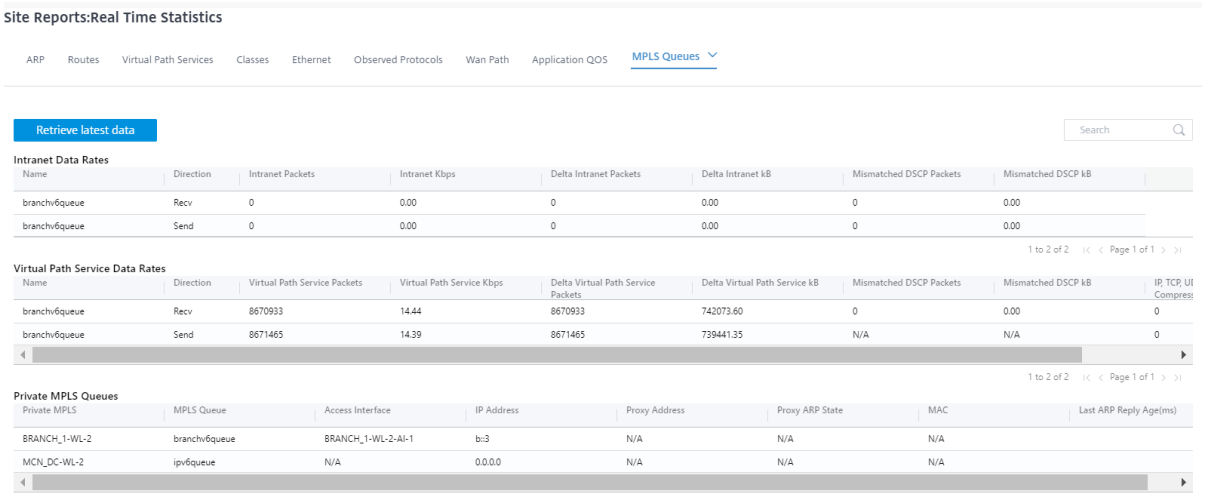
如果要在统计表中添加或删除任何列，请单击加号 (+)，然后单击 更新。



MPLS 队列　MPLS 队列允许您在 MPLS WAN 链接上定义与服务提供商 MPLS 队列对应的队列。有关配置 MPLS 队列的信息，请参阅 MPLS 队列。

要查看 MPLS 队列统计信息，请在站点级别导航到 报告 > 实时 > 网络统计信息。单击 **MPLS** 队列，然后单击“检索最新数据”。最新的 MPLS 队列数据是从设备中检索的，并显示在适用于本地的 Citrix SD-WAN Orchestrator 中。

您可以查看 Intranet 和虚拟路径服务的方向、数据包数量、增量数据包和不匹配的 DSCP 数据包。



对于私有 MPLS 队列，您可以查看以下详细信息：

- 私有 **MPLS**：私有 MPLS 广域网链接。
- **MPLS** 队列：与 MPLS WAN 链接关联的 MPLS 队列。
- 访问接口：与 MPLS 队列关联的访问接口。
- **IP** 地址：与 MPLS 队列关联的 IP 地址。
- 代理地址：与 MPLS 队列关联的代理 IP 地址。
- 代理 **ARP** 状态：代理地址解析协议的状态。已启用、禁用或 N/A
- **MAC**：与 MPLS 队列关联的接口的 MAC 地址。
- 上次 **ARP** 回复时长：收到最后一次 ARP 回复的时间（以毫秒为单位）。

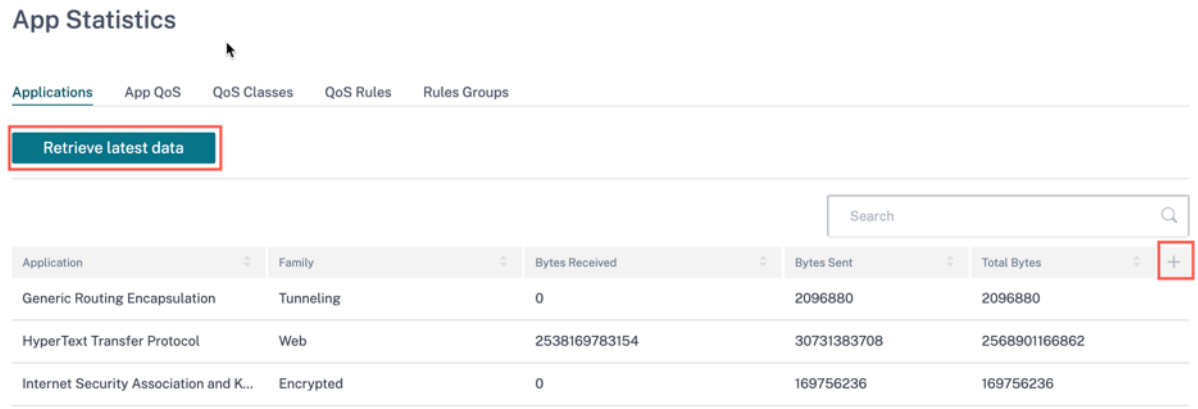
有关故障排除的更多详细信息，请参阅排 除 MPLS 队列故障。

应用程序统计信息

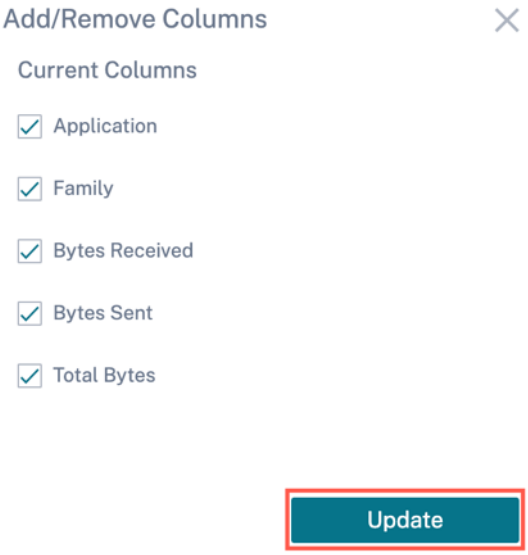
您可以在“报告”**>** “实时”**>** “应用程序统计”下获得以下实时统计信息：

- 应用程序
- 观察到的协议
- 应用程序 QoS
- QoS 类别
- QoS 规则
- 规则组

要获取实时统计报告，请转到所需的选项卡（例如应用程序、应用程序 QoS、QoS 规则），然后单击“检索最新数据”。



如果要在统计表中添加或删除任何列，请单击加号 (+)，然后单击 更新。

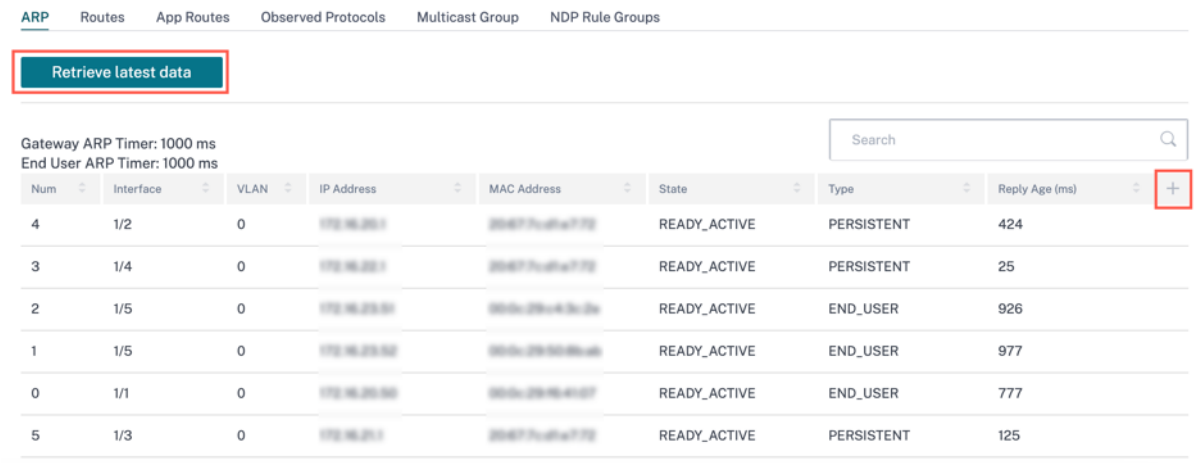


路由统计

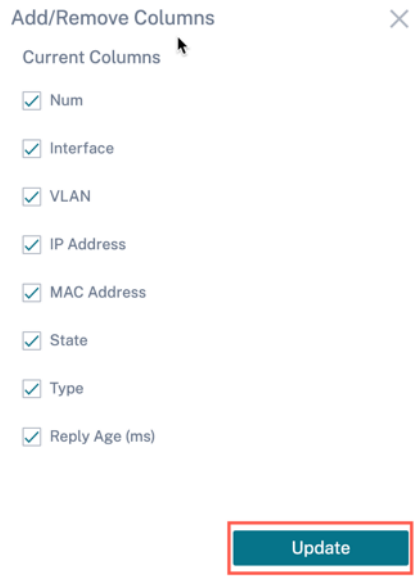
您可以在“报告”**>**“实时”**>**“路径统计”下获得以下实时路径统计信息：

- ARP（地址解析协议）
- 路由
- 应用程序路由
- 观察到的协议
- 多播组
- NDP 规则组

要获取实时统计报告，请转到所需的选项卡（例如 ARP、路由、应用程序路由），然后单击“检索最新数据”。



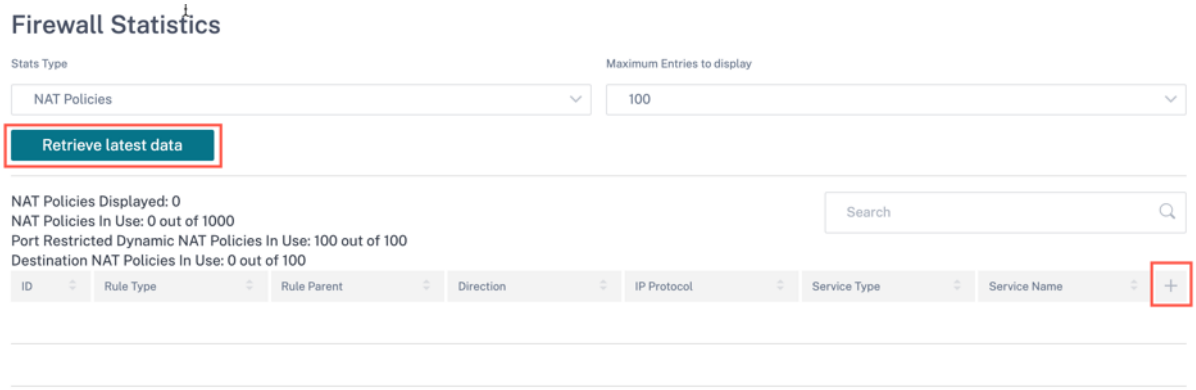
如果要在统计表中添加或删除任何列，请单击加号 (+)，然后单击 更新。



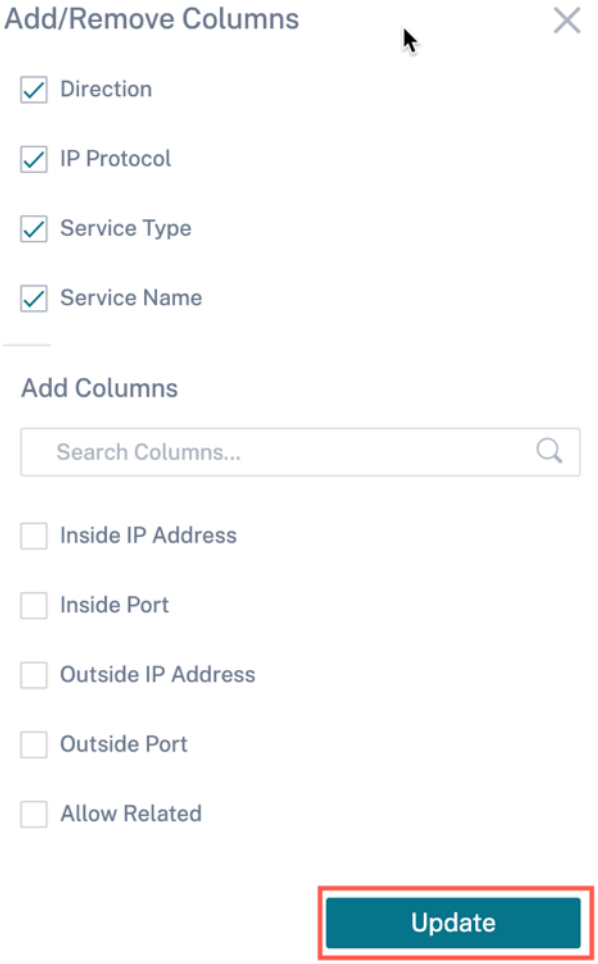
防火墙统计信息

防火墙统计 页面提供连接状态、网络地址协议 (NAT) 策略、基于配置的防火墙操作筛选与特定会话相关的策略。防火墙连接还提供有关连接来源和目标的完整详细信息。

您可以在“报告”**>**“实时”**>**“防火墙统计”下获取实时防火墙统计信息。从下拉列表中选择统计类型（连接、NAT 策略、筛选策略）。选择要显示的最大条目数，然后单击“检索最新数据”。

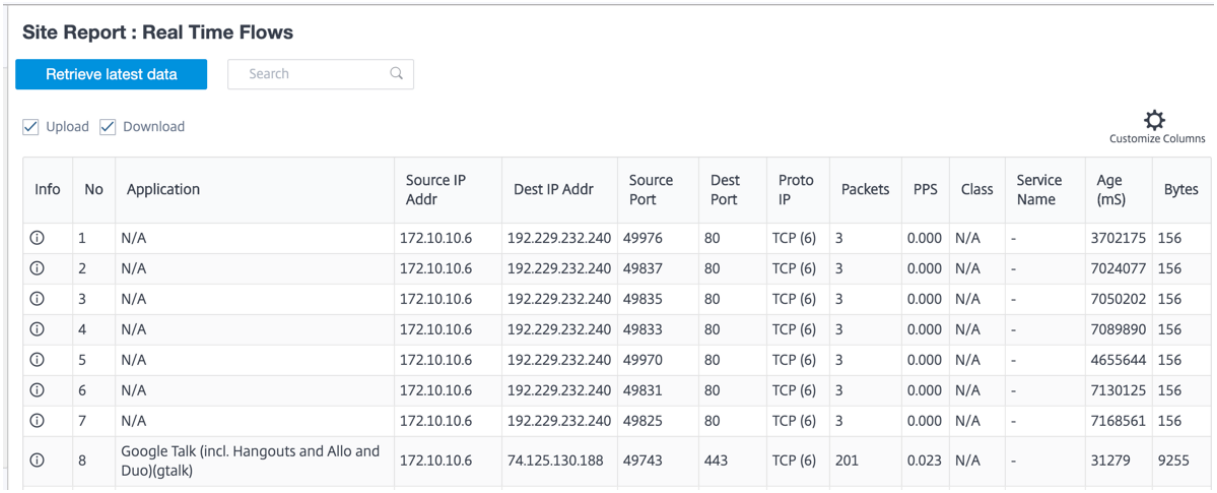


如果要在统计表中添加或删除任何列，请单击加号 (+)，然后单击 更新。



流

流 量功能提供与通过设备的特定会话相关的单向流量信息。这将提供有关流程所属目标服务类型的信息，以及与规则和类型以及传输模式相关的信息。



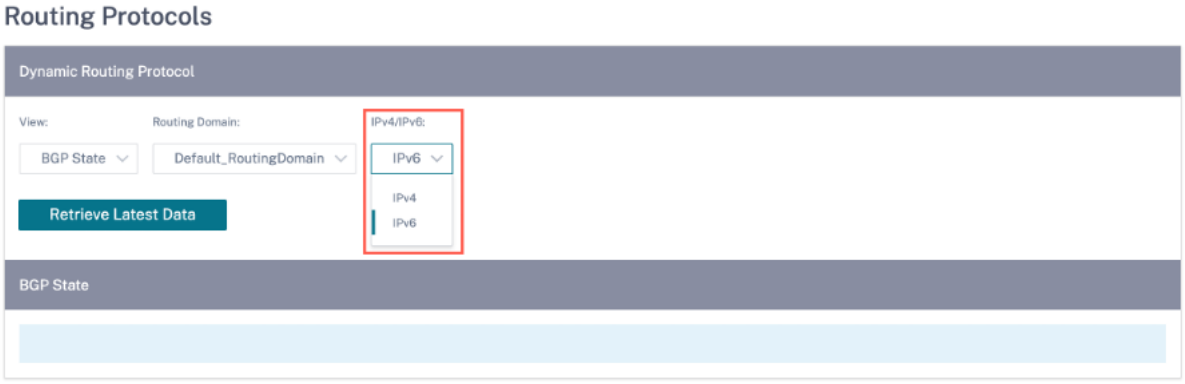
Info	No	Application	Source IP Addr	Dest IP Addr	Source Port	Dest Port	Proto IP	Packets	PPS	Class	Service Name	Age (mS)	Bytes
ⓘ	1	N/A	172.10.10.6	192.229.232.240	49976	80	TCP (6)	3	0.000	N/A	-	3702175	156
ⓘ	2	N/A	172.10.10.6	192.229.232.240	49837	80	TCP (6)	3	0.000	N/A	-	7024077	156
ⓘ	3	N/A	172.10.10.6	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

路由协议

路由协议报告提供与路由协议相关的参数的详细信息。从“查看”下拉列表中选择一个协议，然后从“路由域”下拉列表中选择一个 路由域。单击“检索最新数据”以查看当前数据。

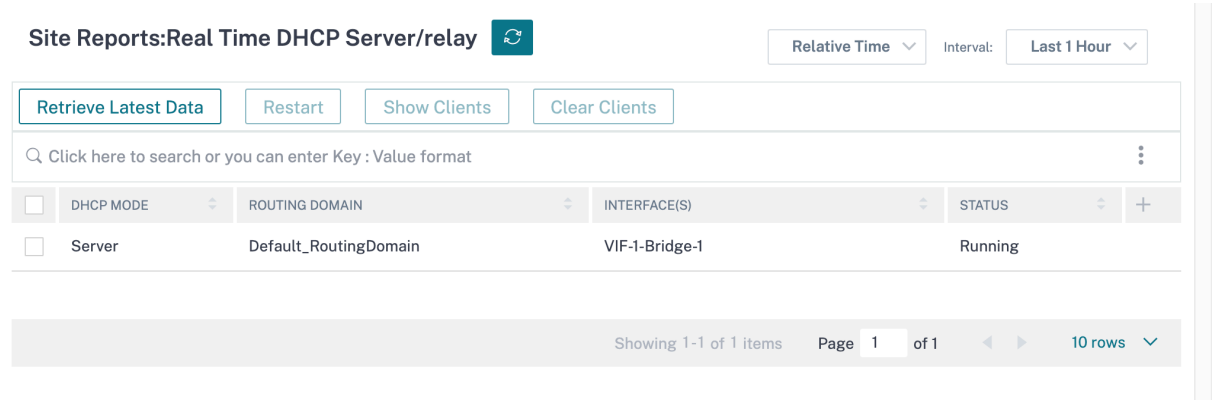
您可以查看与以下内容相关的参数详细信息：

- BGP 状态
- OSPF 状态
- OSPF 拓扑
- OSPF 接口
- OSPF LSADB
- OSPF 邻居
- 路由表

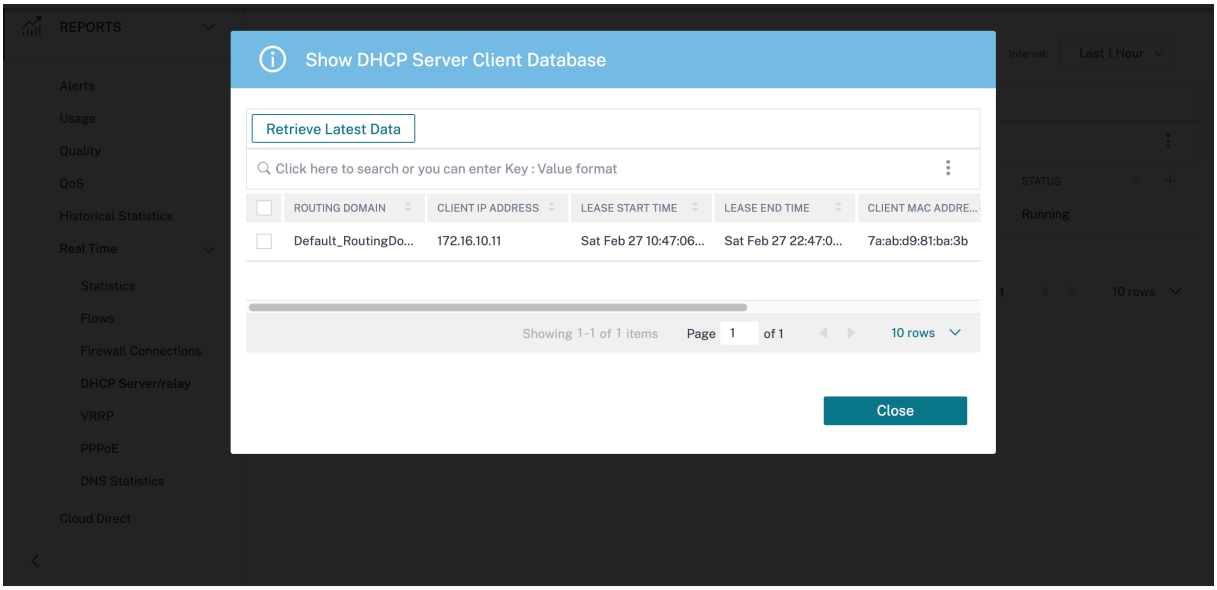


DHCP 服务器和中继

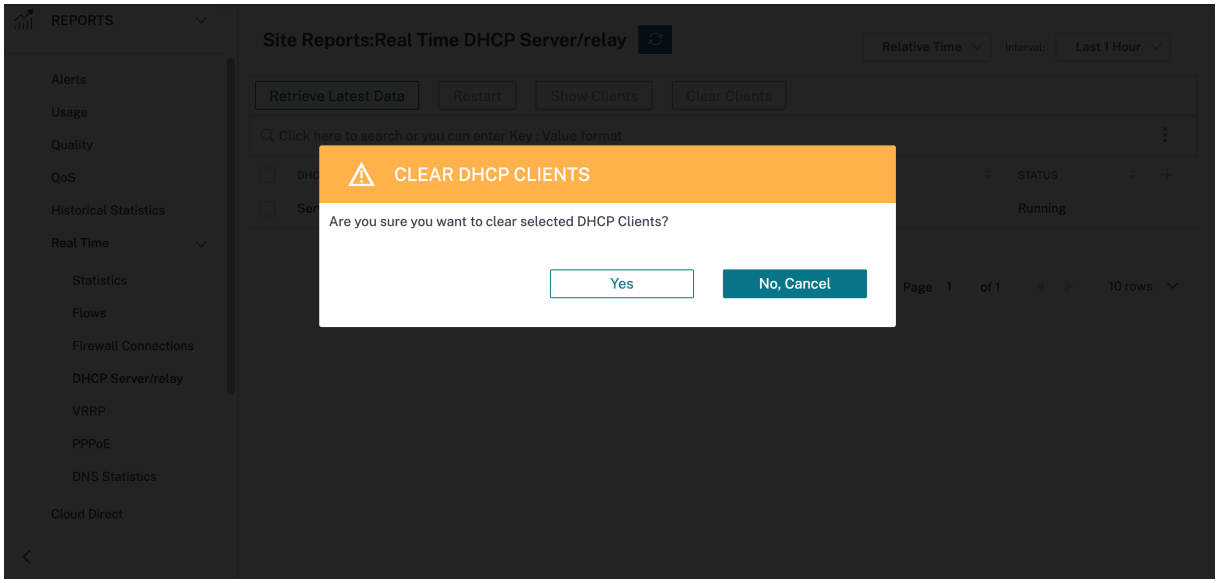
DHCP 服务器/中继 报告提供有关配置为 DHCP 服务器或中继的接口及其关联的路由域和状态的信息。您可以使用 Ke **y: Valu** e 格式搜索所需的 DHCP 服务器或中继信息。



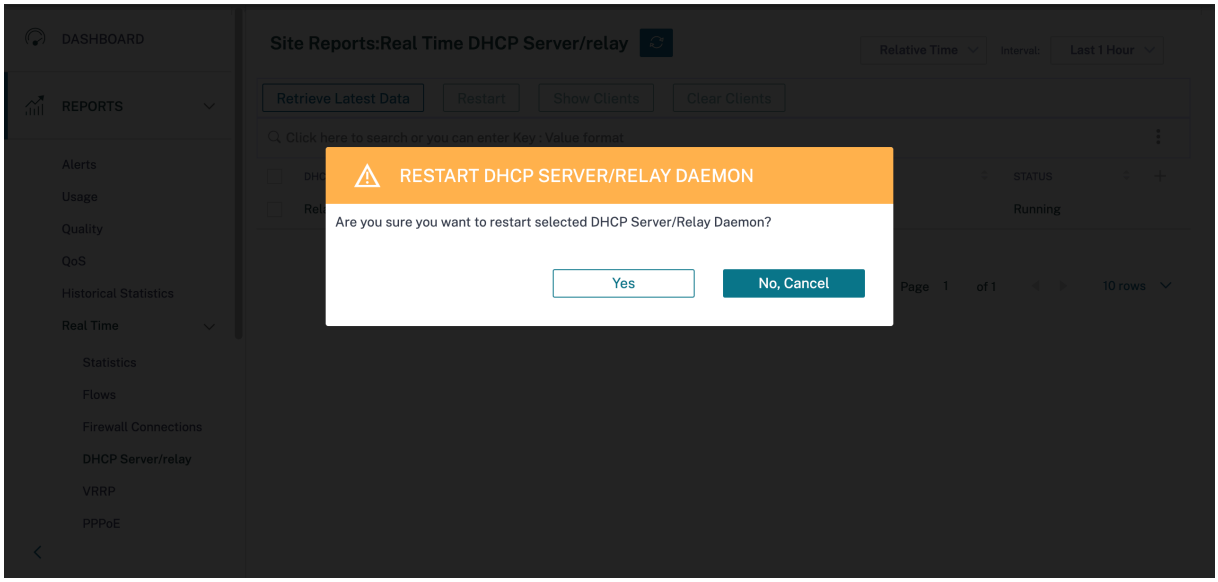
如果模式为“服务器”，则可以单击“显示客户端”并查看与 DHCP 服务器关联的 DHCP 客户机列表。



单击“清除客户机”以删除当前与 DHCP 服务器关联的 DHCP 客户机。



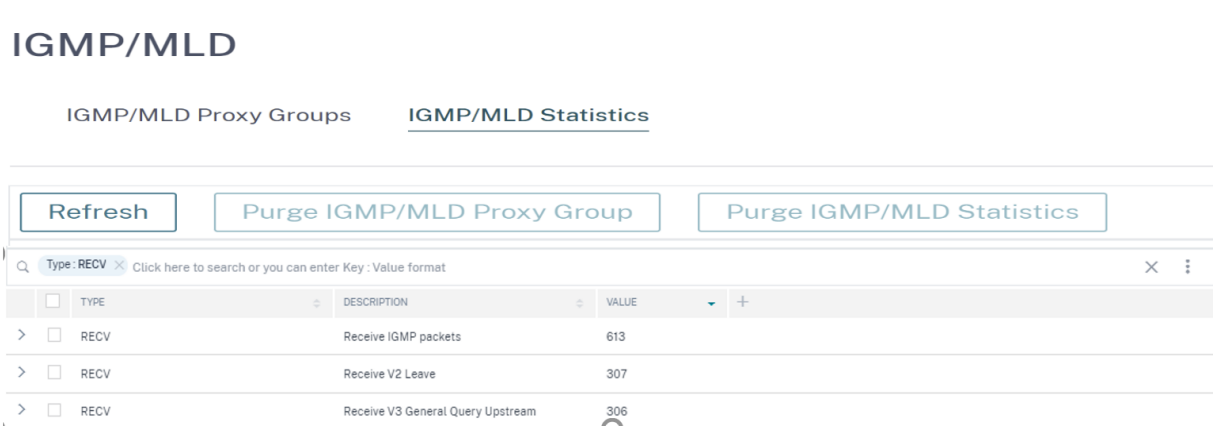
单击“重新启动”以重新启动 DHCP 服务器或中继。



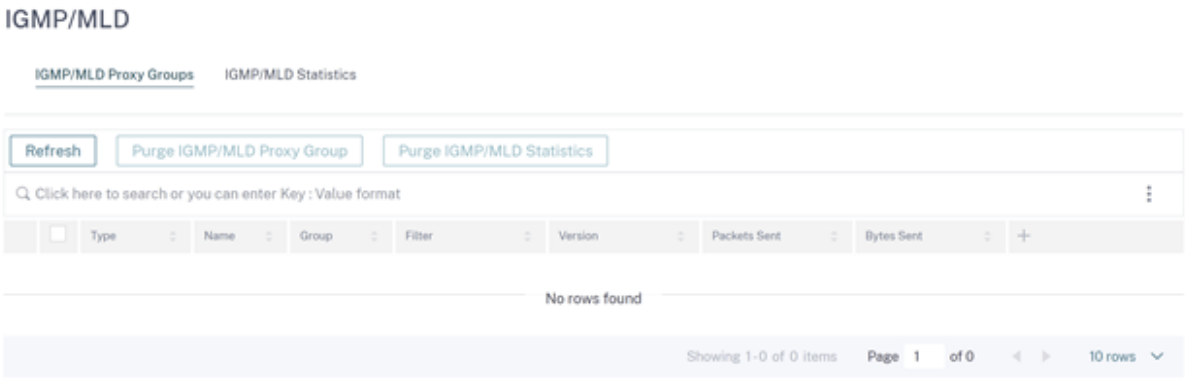
IGMP/MLD

当多播接收方发起加入组请求时，您可以在 报告 > 实时 > IGMP/MLD > **IGMP/MLD** 统计信息下查看接收方详细信息。您可以在源和目标处看到此信息。单击刷新 以获取当前数据。

下图显示接收的 IGMP 数据包和过滤器类型 RECV 用于包括 IGMP 接收数据包。



要查看 IGMP 代理组的详细信息，请导航到 报告 > 实时 > **IGMP/MLD** > **IGMP/MLD** 代理组。单击 刷新 以获取当前数据。



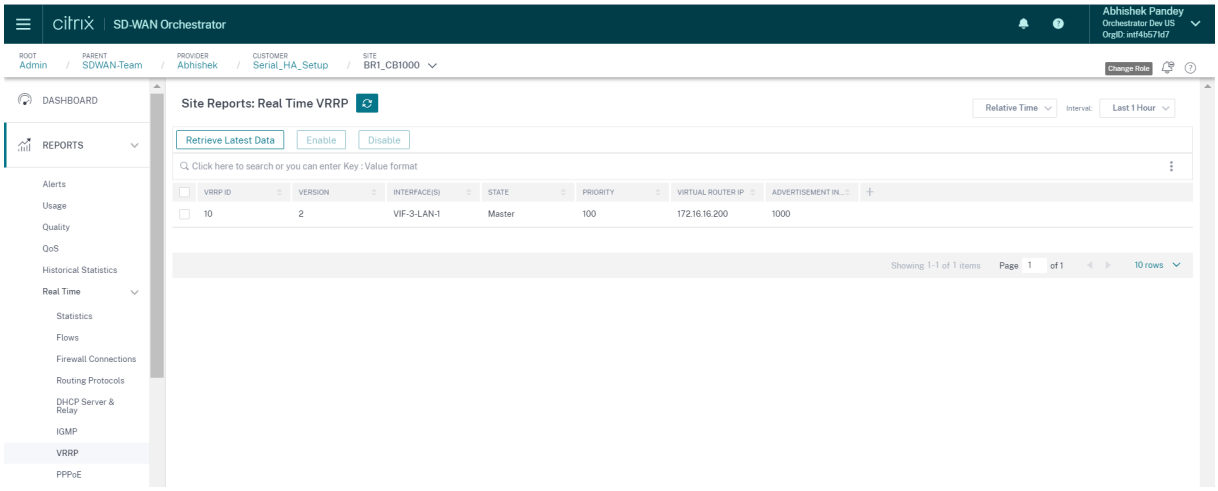
选择 清除 **IGMP/MLD** 统计 数据可从 IGMP 统计表中删除 IGMP 统计数据。

选择“清除 **IGMP/MLD** 组”，从 IGMP 组表中删除 IGMP 组数据。

VRRP

VRRP 实时报告提供有关已配置 VRRP 组的详细信息。

要查看虚拟路由器冗余协议 (VRRP) 报告，请导航到 报告 > 实时 > **VRRP**。单击“检索最新数据”以获取当前数据。



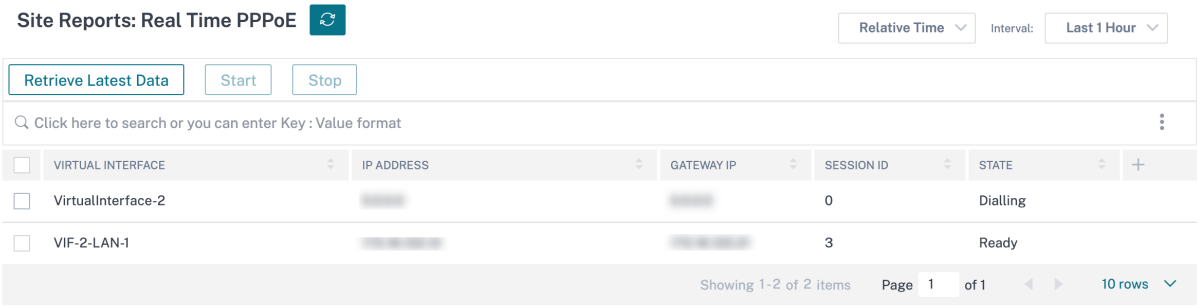
ppPoE

PPPoE 报告提供采用 PPPoE 静态或动态客户端模式的已配置虚拟接口的状态信息。它允许您手动启动或停止会话以进行故障排除。

- 虚拟接口：与 PPPoE 关联的虚拟接口。
- **IP** 地址：与虚拟接口关联的 IP 地址。如果虚拟接口已启动并准备就绪，则显示最近收到的值。如果虚拟接口已停止或处于故障状态，则显示上次收到的值。
- 网关 **IP**：与网关关联的 IP 地址。如果虚拟接口已启动并准备就绪，则显示最近收到的值。如果虚拟接口已停止或处于故障状态，则显示上次收到的值。
- 会话 **ID**：与 PPPoE 会话相关的唯一标识符。
- 状态：状态 列显示 PPPoE 会话的状态。下表描述了状态和描述。

PPPoE 会话类型	说明
已配置	VNI 配置了 PPPoE。这是一个初始状态。
正在拨号	配置 VNI 后，PPPoE 会话状态通过启动 PPPoE 发现移动到拨号状态。数据包信息被捕获。
会话	VNI 从发现状态移至会话状态，等待接收 IP（如果是动态的），或者等待服务器确认通告的 IP（静态）。
已就绪	接收 IP 数据包，VNI 和关联的 WAN 链接已准备就绪可供使用。
失败	PPP/PPPoE 会话终止。失败的原因可能是配置无效或致命错误。会话将在 30 秒后尝试重新连接。
已停止	PPP/PPPoE 会话手动停止。
终止	由于某种原因而终止的中间状态。此状态在一定持续时间后自动启动（正常错误为 5 秒，致命错误为 30 秒）。

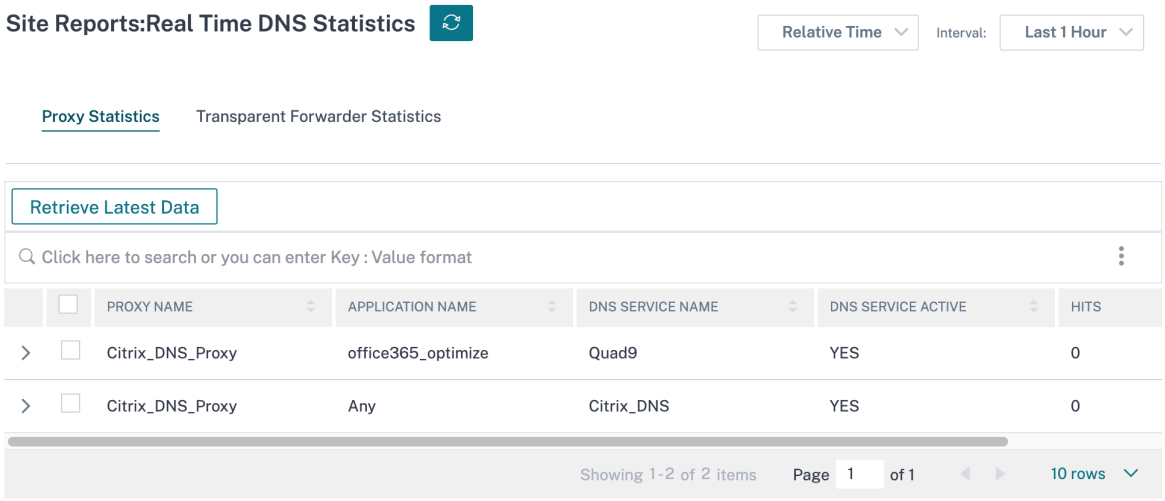
PPPoE 会话类型	说明
已禁用	SD-WAN 服务处于禁用状态。



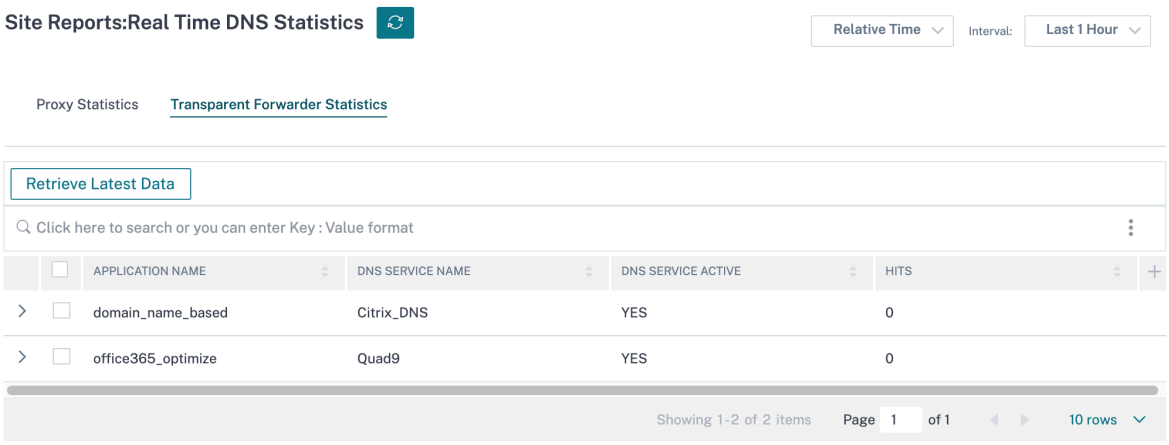
DNS 统计信息

DNS 统计数据 提供有关应用程序名称、DNS 服务名称、DNS 服务状态以及 DNS 服务数量 `hits` 的信息。DNS 代理和 DNS 透明转发器的信息显示在两个不同的选项卡上。

代理统计



透明的转发器统计



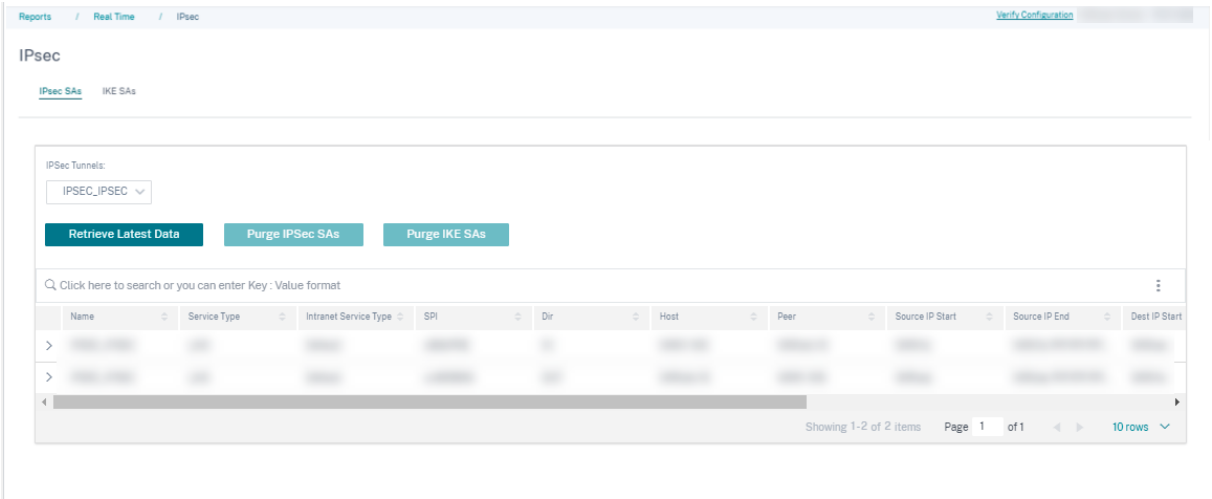
IPsec 的

IPsec 实时报告提供有关网络上 IPsec 隧道设置的详细信息。

要查看 IPsec 安全关联 (IPsec SA) 的详细信息，请导航到 报告 > 实时 > **IPsec** > **IPsec SA**。单击“检索最新数据”以获取当前数据。

要查看互联网密钥交换安全关联 (IKE SA) 的详细信息，请导航到 报告 > 实时 > **IPsec** > **IKE SA**。单击“检索最新数据”以获取当前数据。

您还可以通过分别选择“清除 IPsec 组”和“清除 **IKE** 统计信息”来清除 IPsec 组数据和统计数据。

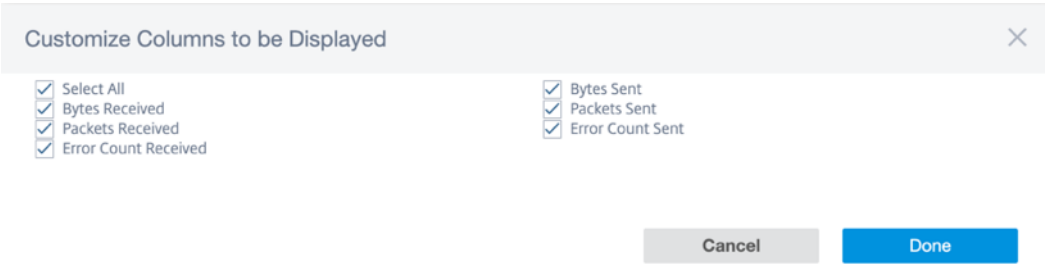


设备报告（预览版）

设备报告提供网络流量和系统使用情况报告。使用此数据，您可以对网络问题进行故障排除或分析 Citrix SD-WAN 设备的行为。您可以在“设备报告”页面下看到以下选项卡：

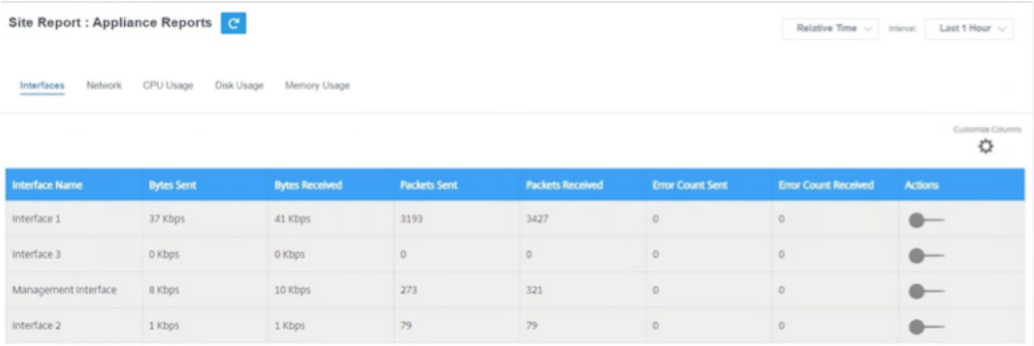
- 接口
- 网络
- CPU 使用率
- 磁盘使用情况
- 内存使用率

单击每个选项卡可按小时、日、每周和每月查看或监视设备图表。您可以根据需要在绝对时间和相对时间之间切换。表格列是可自定义的。单击表格右上角的“自定义”列，然后选择/取消选择要在表格中显示或隐藏的选项。



接口

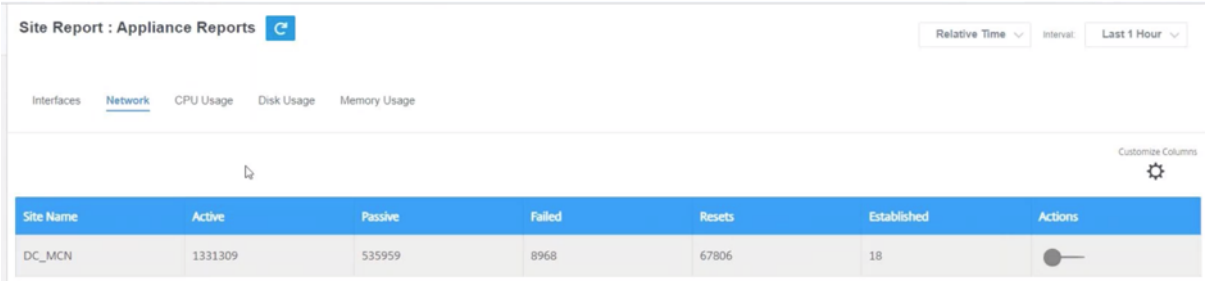
接口 页面显示管理接口错误/流量。所有网络分为不同的接口，例如管理界面、接口 1/2/3。



- 接口名称 -显示接口名称。
- 发送的字节—在所选时长内发送的平均字节数（以 Kbps 为单位）。
- 接收的字节—在所选时长内接收的平均字节数（以 Kbps 为单位）。
- 发送的数据包 -在所选时长内发送的数据包的平均数量。
- 收到的数据包 -在所选持续时间内收到的平均数据包数。
- 发送的错误数 -在选定持续时间内发送的错误数。
- 收到的错误数 -在选定持续时间内收到的错误数。
- 操作 -您可以打开操作按钮来查看网络图。

网络

网络 页面显示每个已配置站点的 TCP 连接数。



- 站点名称 -显示站点名称。
- 活动 -选定持续时间内活动 TCP 连接的平均次数。
- 被动 -所选持续时间内被动 TCP 连接的平均次数。
- 失败 -选定持续时间内失败的 TCP 连接的平均次数。
- 重 @@ 置 -所选持续时间内重置 TCP 连接的平均次数。
- 已建立 -在选定持续时间内建立的 TCP 连接的平均数量。
- 操作 -您可以打开操作按钮来查看网络图。

CPU 使用率

CPU 使用 率页面以百分比形式显示 SD-WAN 设备的 CPU 利用率。CPU 图显示了所选时间内常规时间间隔的平均 CPU 消耗量。

- 站点名称 -显示站点名称。
- 系统 -CPU 处理系统空间程序所花费的总时间百分比。
- 用户—CPU 处理用户空间程序所花费的总时间的百分比。
- 不错—当 CPU 正在运行优先级低于正常的用户任务时，效果很好。
- 空闲—CPU 处于空闲模式的总时间百分比。
- **Io Wait** —**CPU** 等待 I/O 操作所花费的总时间的百分比。
- **Irq** —内核提供的中断请求 (IRQ) 值。
- 窃取 -在虚拟化环境中运行时，虚拟机管理程序可能会出于各种原因窃取专用于您的 CPU 的周期，然后将其交给另一个 CPU。这次被称为偷。
- 操作 -您可以打开操作按钮来查看网络图。

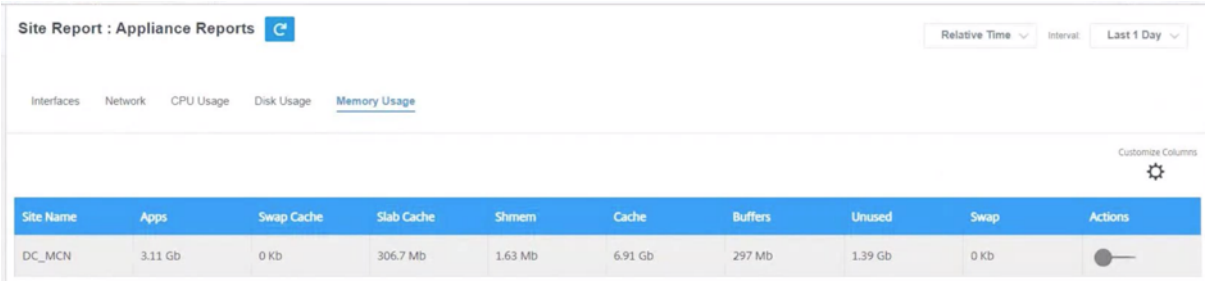
磁盘使用情况

“磁盘使用 量”页面以每秒 I/O (IOPS) 值显示操作系统和数据分区使用的硬盘空间量。

- 站点名称 -显示站点名称。
- 磁盘名称 -显示硬盘名称。
- 读取 **IOPS** —显示选定时间范围内每秒读取 IOPS 的平均数。
- 写入 **IOPS** —显示选定时间范围内每秒写入 IOPS 的平均数。
- 延迟 -显示选定时间范围内来自选定卷工作负载的成功读取和写入请求的延迟值。建议将延迟值低于 10 毫秒最适合 I/O 性能。
- 读取吞吐量 -显示选定时间内磁盘读取操作的平均磁盘吞吐量值，以 Kbps 为单位。
- 写入吞吐量 -显示选定时间内磁盘写入操作的平均磁盘吞吐量值，以 Kbps 为单位。
- 磁盘利用率 -显示所选时间范围内的平均磁盘利用率值（以百分比表示）。
- 操作 -您可以打开操作按钮来查看网络图。

内存使用率

内存使用情况 页面显示已用内存量的报告。

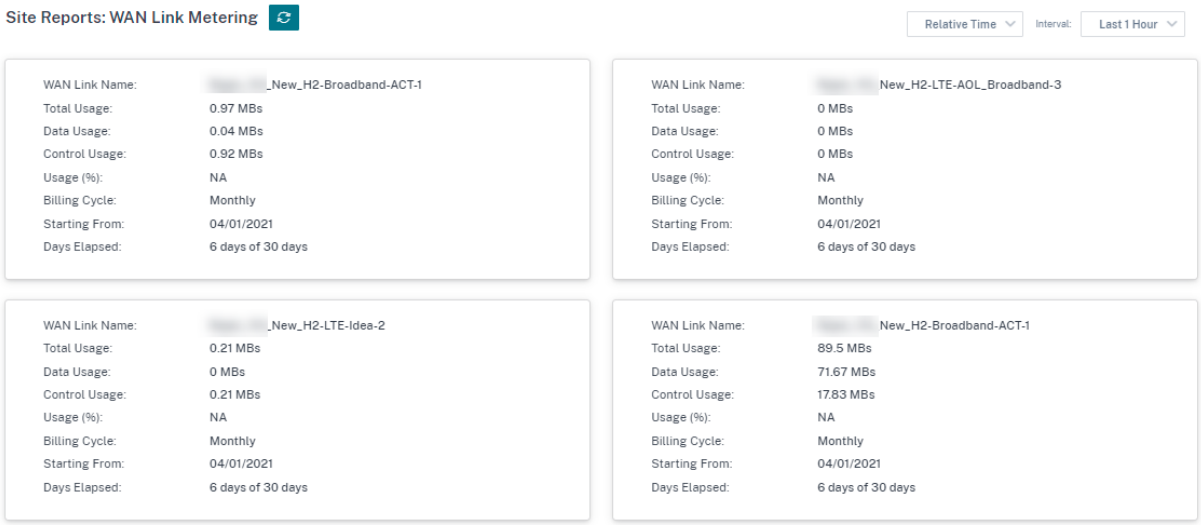


- 站点名称 -显示站点名称。
- 应用程序 -以 Gb 为单位显示已使用的应用程序值。
- 交换缓存 -以 Mb 为单位显示交换缓存编号。交换缓存是页表条目的列表，每个物理页面有一个条目。
- **Slab Cache** —显示预分配的内存块的数量。在 Mb
- **Shmem** —以 Mb 为单位显示已用共享内存的总值。
- 缓存 -显示使用的缓存内存数量（以 Gb 为单位）。
- 缓冲区 -显示缓冲区缓存使用的物理内存的数量。

- 未使用 -显示用于缓存的未使用内存的数量。
- 交换 -显示交换空间的数量。如果物理内存需要一些空间扩展，则会使用交换空间。
- 操作 -您可以打开操作按钮来查看网络图。

WAN 链路计量

WAN 链路计量报告提供有关计量的 WAN 链路使用情况的详细信息。您可以查看报告，深入了解按流量计费的 WAN 链接的数据消耗情况。要查看 WAN 链接计量报告，请导航到 报告 **> WAN** 链接计量。



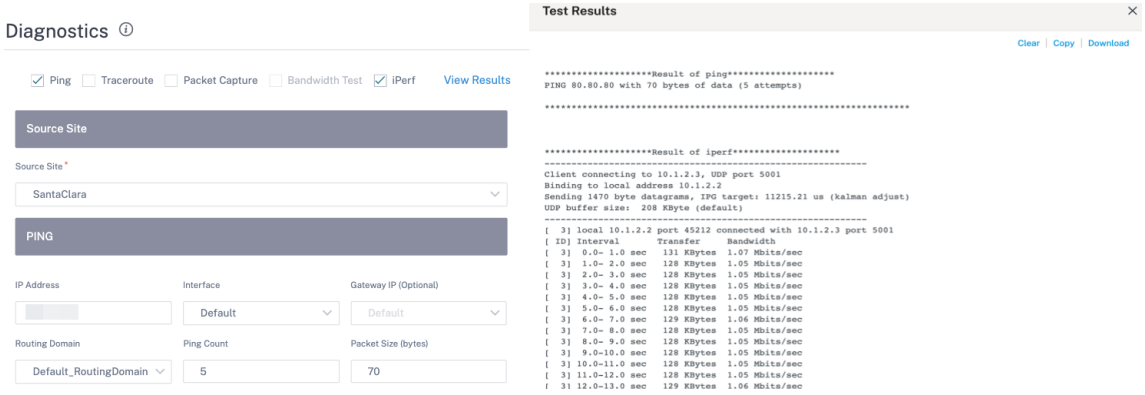
诊断

October 21, 2022

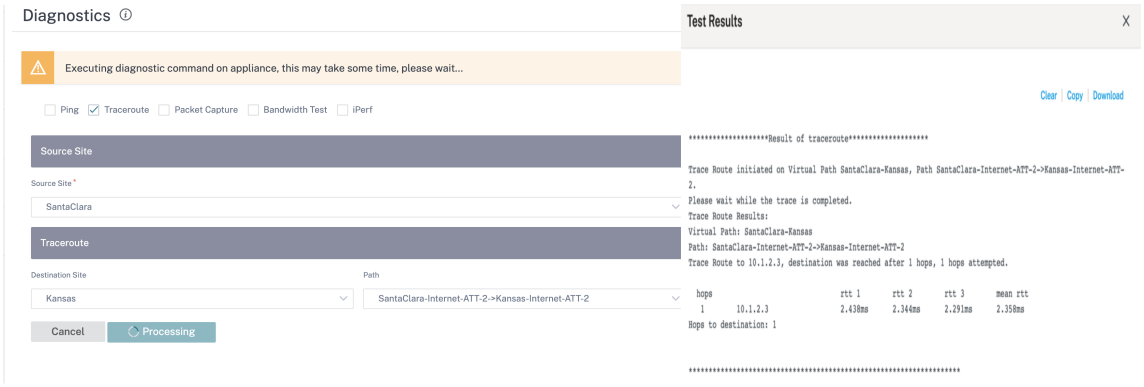
您可以使用 Ping、Traceroute、数据包捕获、带宽测试和 iPerf 诊断实用程序来测试和调查 SD-WAN 网络上的网络连接问题。要查看“诊断”页面，请导航到“故障排除”> “诊断”。

要查看诊断结果，请单击“诊断”页面右上角的“查看结果”。您可以根据需要 下载、复制和 清除 报告结果。

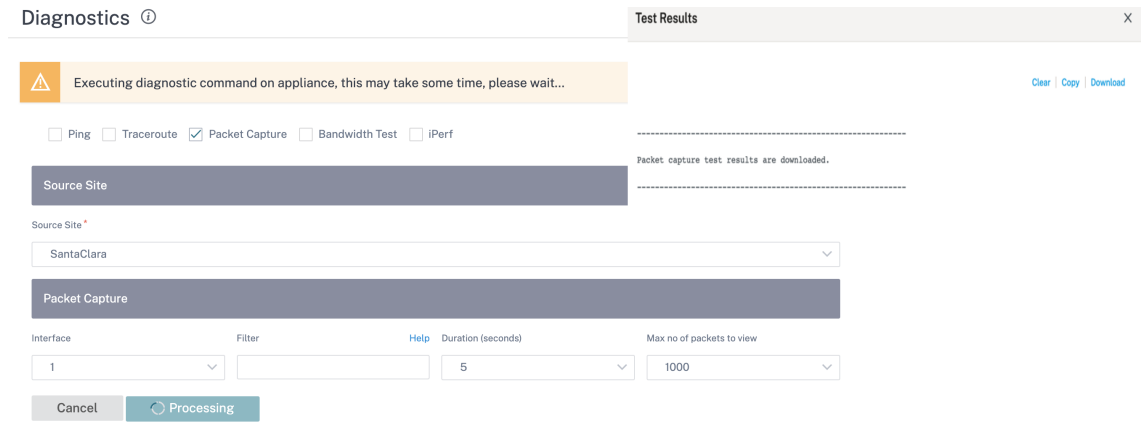
- P@@**ing** —您可以通过 ping 远程主机或站点来检查网络连接。输入目标详细信息，指定发送 ping 请求的次数和数据字节数。提供目标 **IP** 地址，然后单击“运行”。



- **Traceroute** -您可以跟踪路线和站点之间的跳数。选择源站点和目标站点以及要跟踪的路径，然后单击“运行”。

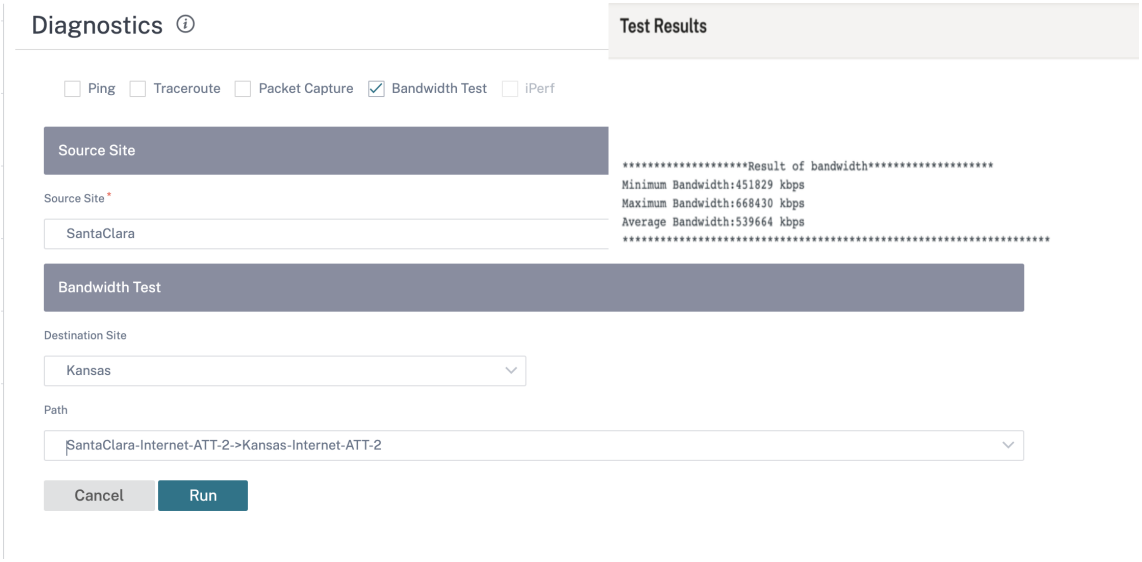


- 数据包捕获 -您可以拦截通过所选站点中存在的选定活动接口传输的数据包。您可以查看源和目的地的详细信息。



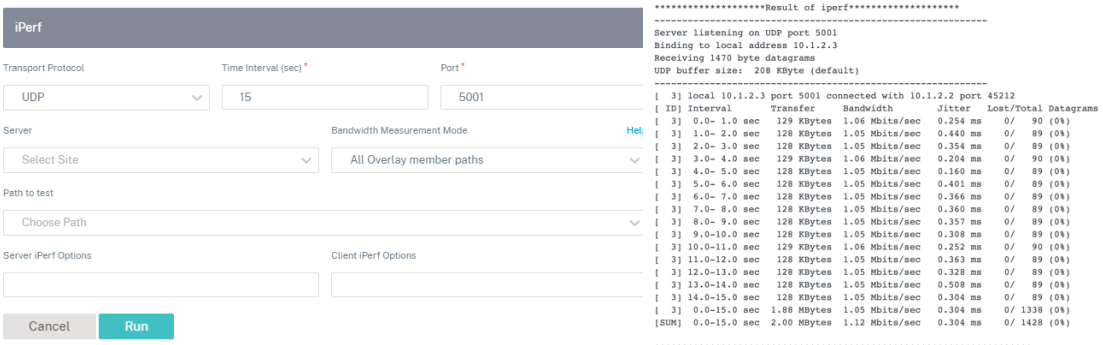
帮助 选项提供了有关 筛选选项的更多详细信息。

- 带宽测试 -您可以在站点的特定路径上运行带宽测试，以查看最大、最小和平均带宽使用情况。输入源站点、目标站点，然后选择路径。单击运行。



- **iPerf** —您可以在站点的特定路径上运行 iPerf 测试。iPerf 诊断工具用于生成测试流量，允许您解决可能导致以下情况的网络问题：
  - 路径状态经常从“好”更改为“不好”
  - 应用程序性能差
  - 更高的数据包丢失

  要运行 iPerf 诊断测试，请从客户级别导航到 故障排除 > 诊断，然后选中 **iPerf** 复选框。输入传输协议、时间间隔、端口号、服务器、带宽测量模式、测试路径、服务器 iPerf 选项，然后单击“运行”。



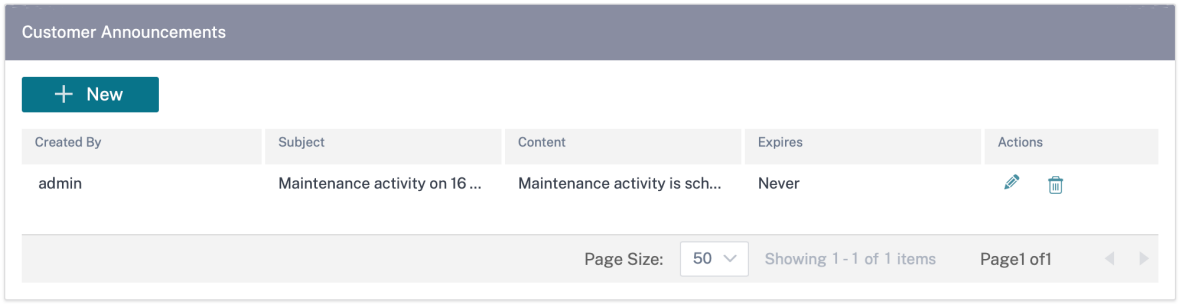
公告

October 21, 2022

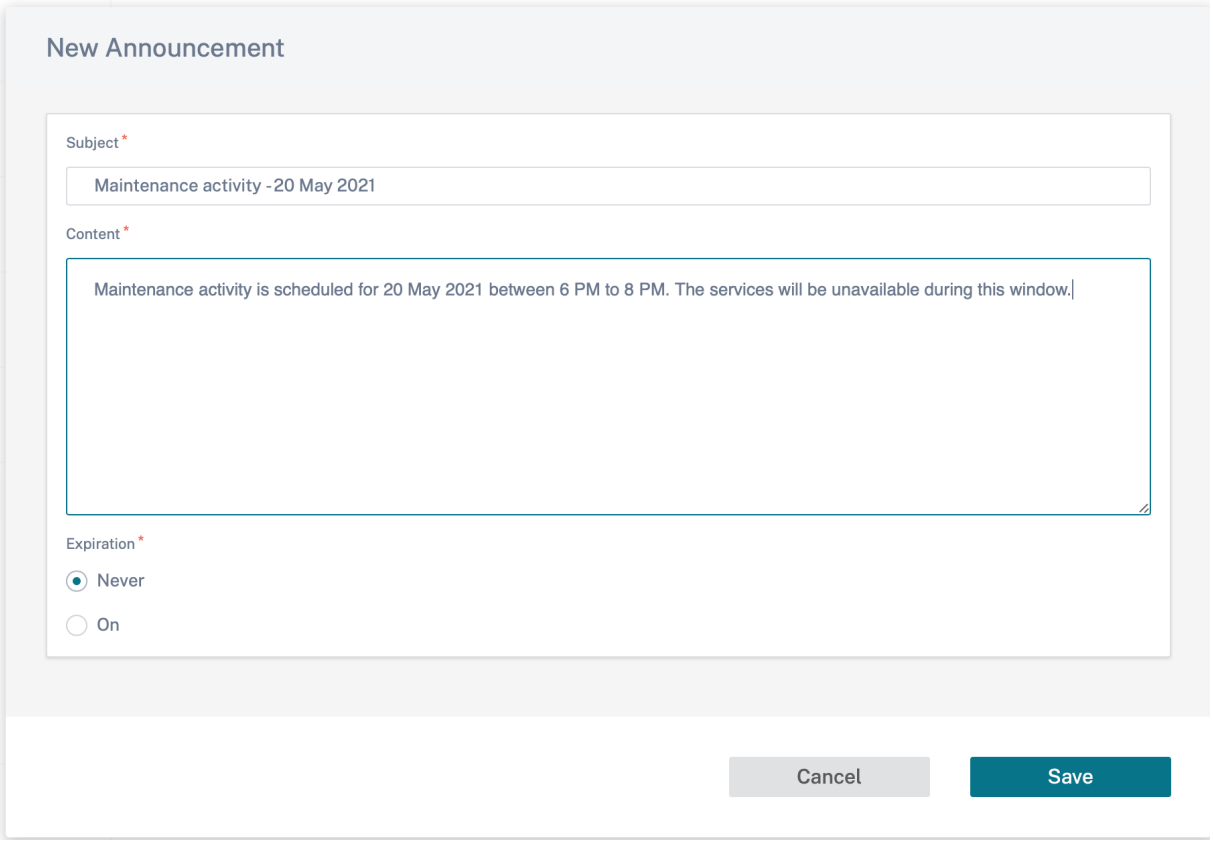
提供商可以使用公 告 选项向其客户发送公告或通知。

您可以导航到“管理” **>** “公告”，然后单击“+ 新建”选项来创建提供商公 告。

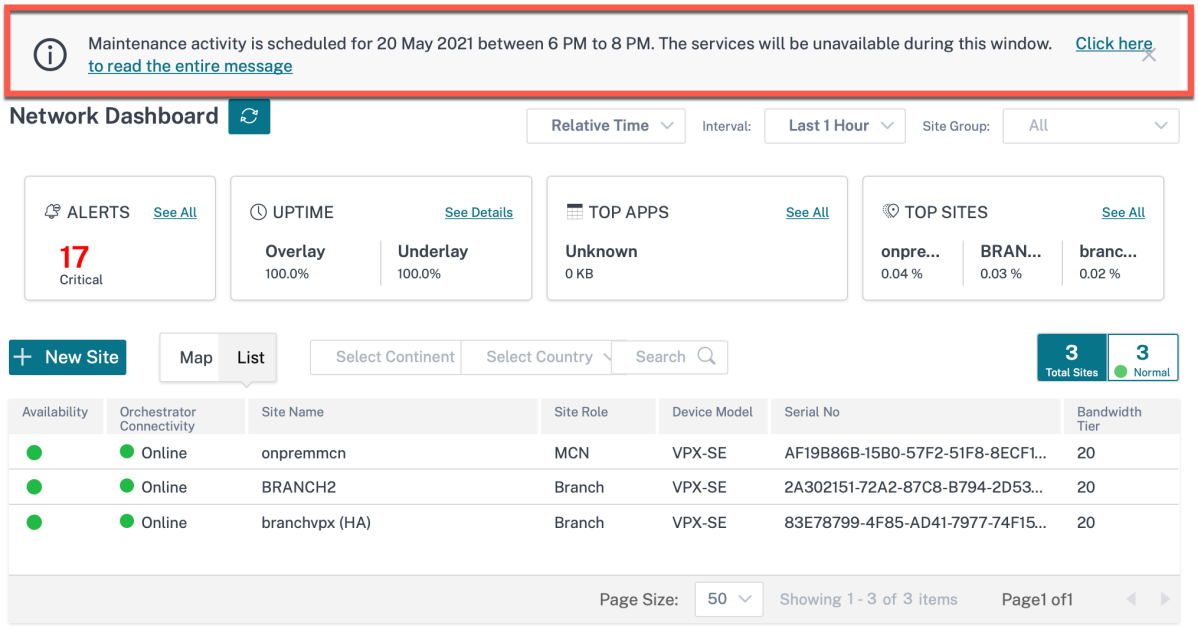
Provider Administration: Announcements



提供主题行并以 HTML 或纯文本格式输入内容。您还可以设置公告到期。



保存的公告将显示给所有客户。



用户管理

October 2, 2024

适用于本地的 Citrix SD-WAN Orchestrator 支持基于角色的访问控制 (RBAC)。RBAC 根据分配给单个用户的角色来管理对 SD-WAN Orchestrator 资源的访问权限。RBAC 允许用户仅访问其角色需要的数据，并限制任何其他数据。

角色定义了在适用于本地的 Citrix SD-WAN Orchestrator 上查看和执行各种活动的权限。您可以从预定义角色列表中为用户分配角色。

默认情况下，在 Citrix SD-WAN Orchestrator for Inclouse 上创建一个用户帐户，用户名 管理员 和密码设置为 密码。在初次登录期间，要求用户更改默认密码。

您可以添加可以在本地和远程进行身份验证的用户。通过远程身份验证的用户通过 RADIUS 或 TACACS+ 身份验证服务器进行身份验证。

提供商角色

下表列出了预定义的提供程序角色。

提供者角色	说明
Provider-Master-Admin-All	可以管理提供商及其所有客户信息的管理员

提供者角色	说明
Provider-Master-Admin-Tenant	可以管理提供商及其客户信息子集的管理员
Provider-master-read-all	只能查看提供商和客户信息的管理员
提供商网络管理员（预览版）	只能查看和编辑网络相关信息的管理员
提供商安全管理员（预览版）	只能查看和编辑安全相关信息的管理员

Provider-Master-Admin-All 角色可以执行以下操作：

- 为提供商和客户网络中的用户分配角色
- 管理所有其他管理员角色对客户的访问
- 编辑或删除分配的角色

客户角色

下表列出了预定义的客户角色：

角色	说明
Customer-Master-Admin	可以查看和编辑客户信息的客户管理员
Customer-Master-ReadOnly-Admin	只能查看客户信息的客户管理员
客户网络管理员（预览版）	只能查看和编辑网络相关信息的客户管理员
客户安全管理员（预览版）	只能查看和编辑安全相关信息的客户管理员

具有 客户主管理员角色的 用户可以执行以下操作：

- 添加用户和分配客户角色
- 编辑或删除分配的角色

> 注意：
>
> 将关键角色（主管理员、安全管理员和网络管理员）专门分配给受信任的用户非常重要。

支持角色

出于故障排除的目的，客户可以分配支持角色并允许支持团队成员查看和编辑其信息。支持角色的有效期是在分配角色时定义的。有效期到期后，支持用户将失去对客户信息的访问权限。但是，支持用户详细信息继续显示在“管理”**>**“用户管理”下。根据需要，客户管理员可以删除或延长支持角色的有效期。

角色	说明
Customer-Support-ReadWrite	可以查看和编辑客户信息的支持团队成员
Customer-Support-ReadOnly	只能查看客户信息的支持团队成员

身份验证类型

适用于本地的 Citrix SD-WAN Orchestrator 支持以下类型的身份验证：

- 单因素身份验证：单因素身份验证提供了一种身份验证方法，可让用户访问本地版 Citrix SD-WAN Orchestrator。
- 双因素身份验证 **(TFA)**：双因素身份验证提供了两种身份验证方法，可让用户访问适用于本地的 Citrix SD-WAN Orchestrator。它在登录序列中引入了额外的安全层。

单因素和双因素身份验证支持以下身份验证方法：

- 本地：选中后，用户必须使用在 Citrix SD-WAN Orchestrator 上为本地配置的密码才能获得访问权限。
- **RADIUS**：选择后，用户必须使用 RADIUS 服务器密码才能获得访问权限。
- **TACACS+**：选择后，用户必须使用 TACACS+ 服务器密码才能获得访问权限。

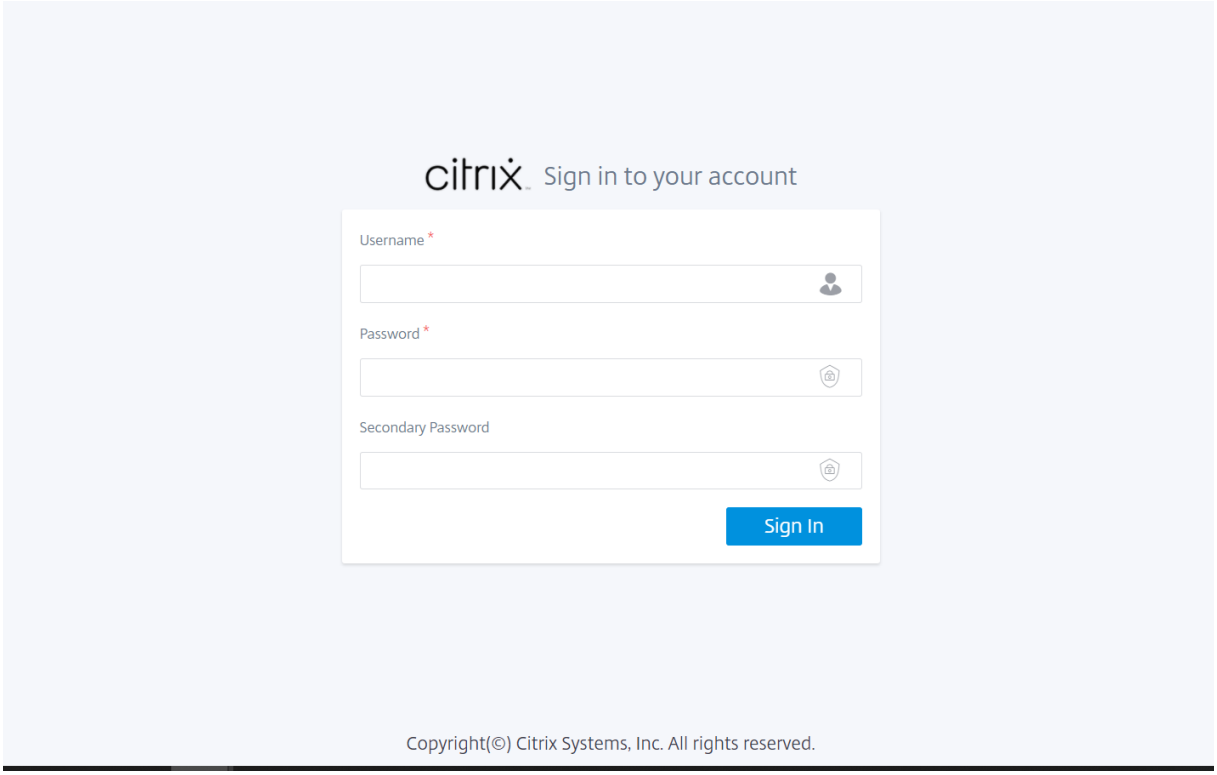
下表列出了在本地进行身份验证的用户支持的主要和辅助身份验证方法：

	主要身份验证类型	辅助身份验证类型
单因素身份验证	本地	-
双重身份验证	本地	RADIUS 或 TACACS+

下表列出了远程身份验证的用户支持的主要和辅助身份验证方法：

	主要身份验证类型	辅助身份验证类型
单因素身份验证	本地、RADIUS 或 TACACS+	-
双重身份验证	本地、RADIUS 或 TACACS+	RADIUS 或 TACACS+

如果启用了 双因素身份验证 并将 RADIUS/TACACS+ 服务器配置为辅助身份验证类型，则登录页面上会显示 辅助密码字段。



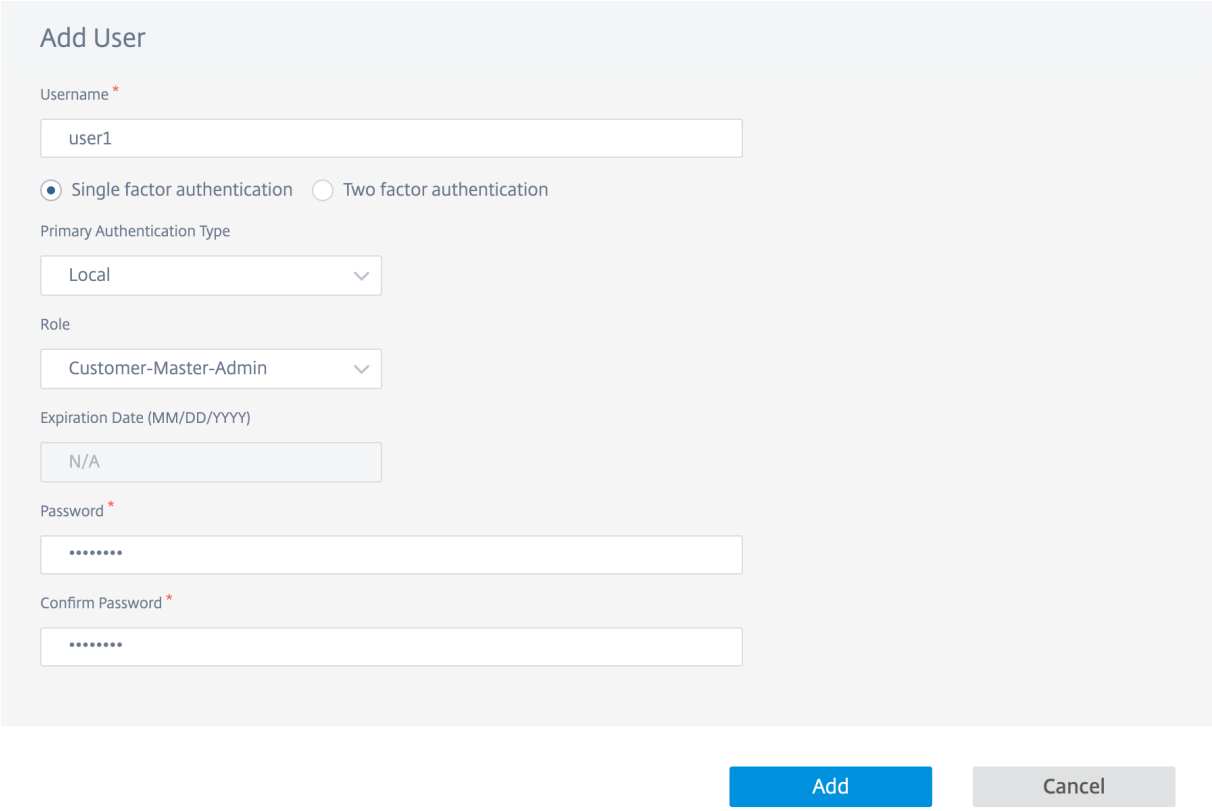
添加用户

导航到 管理 > 用户管理 > 单击 **+** 新建 > 输入以下详细信息 > 单击“添加”。

- 输入用户名。
- 单因素身份验证：仅启用登录用户的主身份验证。
- 双因素身份验证：为用户登录启用主身份验证和辅助身份验证。有关更多信息，请参阅 远程身份验证服务器。
- 主身份验证类型：选择本地或远程身份验证服务器的 IP 地址。
- 辅助身份验证类型：选择远程身份验证服务器的 IP 地址。

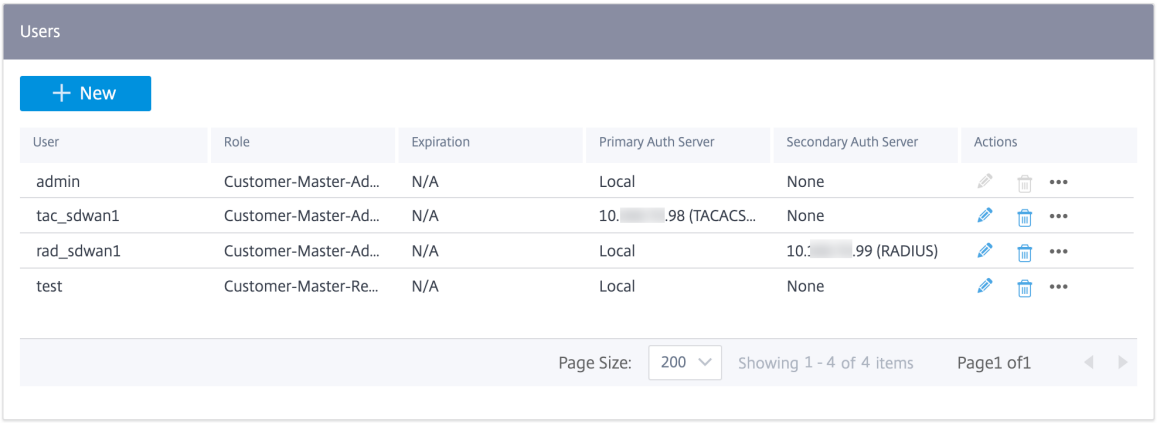
  > 笔记
  >
  > 如果选择单因素 身份验证，则辅助身份验证类型 字段将显示为灰色。

- 角色：从可用角色列表中选择一个角色。
- 拒绝客户访问：（仅在提供商级别可用）。在添加用户时，提供商可以拒绝特定客户的访问。
- 到期日期 **(MM/DD/YYYY)**：支持用户有权访问客户信息的截止日期。默认有效期为自分配角色之日起的两周。
- 输入您的密码。密码长度必须介于 8 到 128 个字符之间。



使用“操作”列，您可以更改用户角色、更新密码和编辑身份验证类型。如有必要，您也可以删除该用户。

Network Administration: User Administration



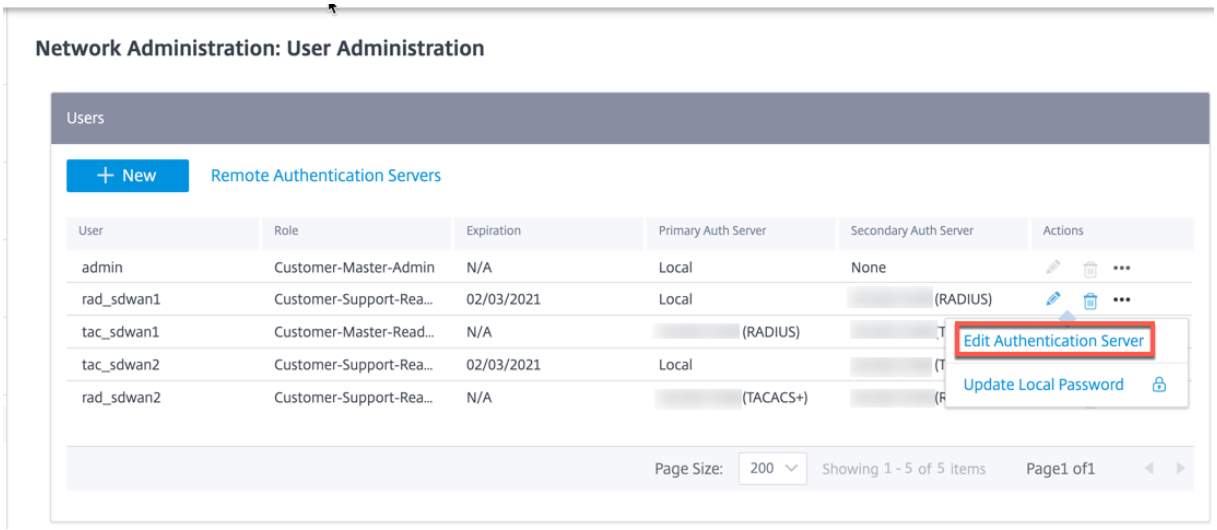
限制

适用于本地的 Citrix SD-WAN Orchestrator 不支持在同一提供商下为其他客户复制用户名。执行此操作时，您会看到错误消息“创建帐户时出错”。

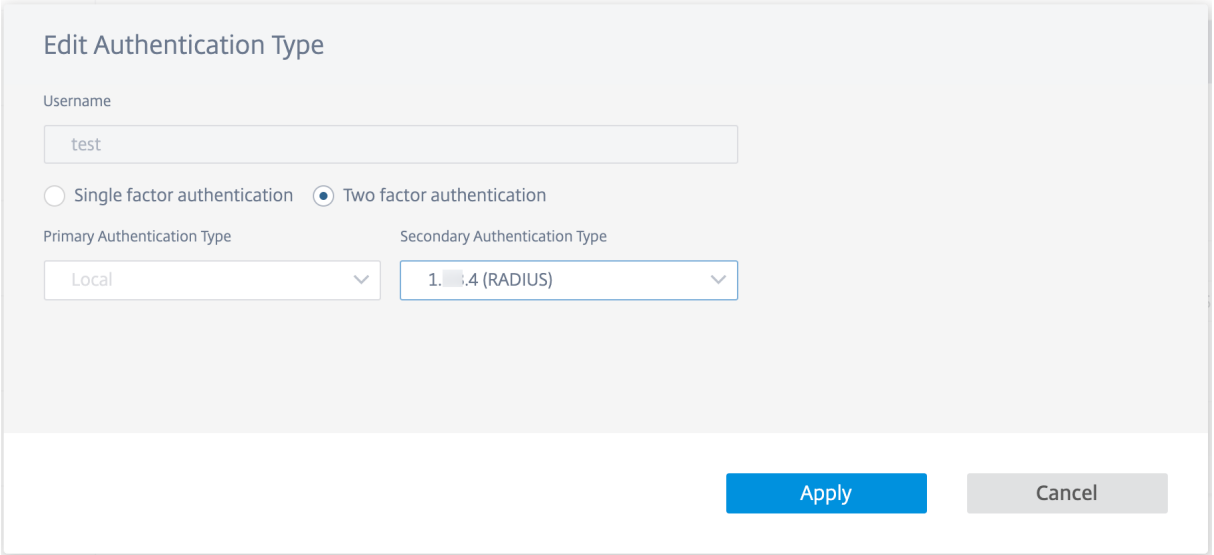
更改身份验证类型

您可以将用户的身份验证类型从单因素身份验证更改为双因素身份验证，反之亦然。

要更改用户的身份验证类型，请在“操作”列中单击 …，然后单击“编辑身份验证服务器”。



如果您当前选择了 单因素身份验证，则可以切换到双因素身份验证。单击“双因素身份验证”，然后从“辅助身份验证类型”下拉列表中选择远程服务器。单击应用。



如果您当前选择了双因素身份验证，则可以选择仅更改辅助身份验证类型或切换到单因素身份验证。

要切换到单因素身份验证，请单击 单因素身份验证。辅助身份验证类型 下拉列表被禁用，仅启用 主身份验证类型 下拉列表。

主身份验证类型 只能在创建用户时设置，以后无法编辑。

更改密码

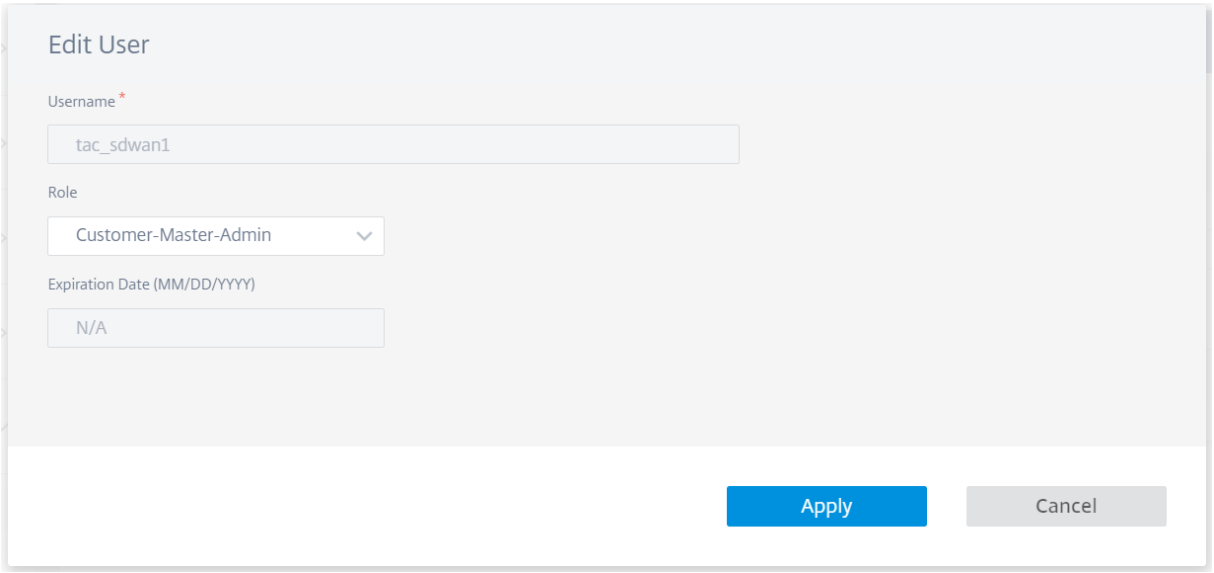
您可以更改本地用户的密码。要更改用户的密码，请在“操作”列中单击“…”并单击“更新本地密码”。

> 笔记
>
> 您只能修改本地用户的密码。对于通过远程身份验证的用户，必须更新外部服务器上的密码。

更改用户角色

要更改用户角色，请单击“操作”列中的 “编辑”图标。选择一个 角色，然后单击“应用”。

> 笔记
>
> 您无法编辑默认管理员用户的角色。



域名

October 21, 2022

域名是地址栏中使用的虚假网址，用于访问本地的 Citrix SD-WAN Orchestrator。使用域名可以更容易记住，还可以让您使用公司的品牌名称。

要使用域名，请确保您的本地 DNS 服务器配置了一条 DNS 记录，该记录将域名链接到 Citrix SD-WAN Orchestrator 用于本地管理 IP 地址。确保在早期配置期间配置了域名。设置域名后，用于本地的 Citrix SD-WAN Orchestrator 会自动重新启动并重新生成证书。必须在各个设备上配置相同的域名。有关更多详细信息，请参阅 SD -WAN 设备上的本地 SD-WAN Orchestrator 配置。

配置域名不是强制性的。如果您没有域名但仍想使用 DNS 服务器进行 IP 地址解析，请为以下三个 FQDN 配置指向本地 IP 的 Citrix SD-WAN Orchestrator 的 DNS 记录：

- sdwanzt.citrixnetworkapi.net
- 下载.citrixnetworkapi.net
- sdwan-home.citrixnetworkapi.net

例如，如果本地域的 Citrix SD-WAN Orchestrator 配置为 c **itrix.com**，则必须在 DNS 服务器中为以下 FQDN 创建 DNS 记录，为本地 IP 地址创建 Citrix SD-WAN Orchestrator：

- download.citrix.com
- sdwanzt.citrix.com
- sdwan-home.citrix.com

在高级配置中：

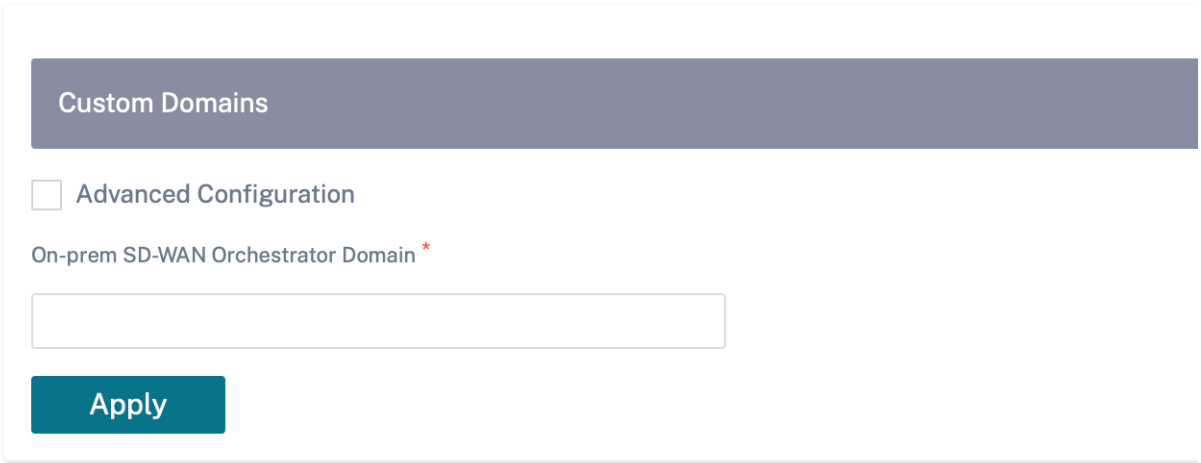
例如：如果本地域的 Citrix SD-WAN Orchestrator 配置为 c **itrix.com**，则下载管理服务域 配置为 **download.citrix.com**，统计管理服务域 配置为 统计信息。**citrix.com**，那么你必须在 DNS 服务器中为以下 FQDN 和相应的 IP 地址创建 DNS 记录：

- download.citrix.com
- sdwanzt.citrix.com
- statistics.citrix.com

为现有配置配置配置或更改域名会影响用于本地和设备连接的 Citrix SD-WAN Orchestrator。您必须手动执行 证书身份验证 过程或使用 站点零接触部署设置 选项。

> 注意
>
> 在提供商托管设置中，只有提供商管理员有权编辑与域名相关的信息。

要配置域名，请在网络级别导航到“管理”**>**“域名”，然后为本地域名 提供 Citrix SD-WAN Orchestrator。



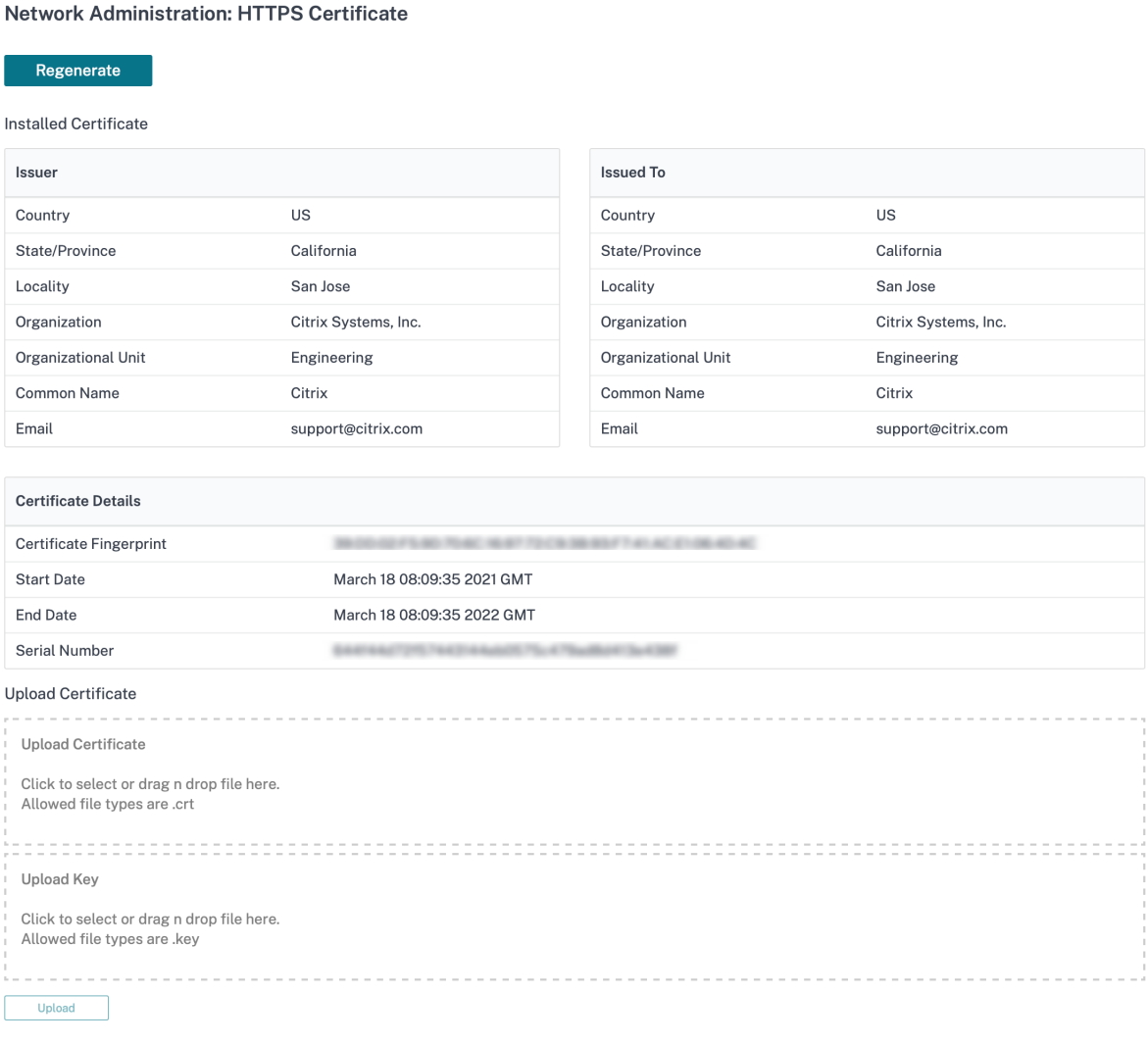
HTTPS 证书

October 21, 2022

建立与本地版 Citrix SD-WAN Orchestrator 的安全管理 HTTPS 连接需要 HTTPS 证书。您可以使用适用于本地 GUI 的 Citrix SD-WAN Orchestrator 上提供的默认 HTTPS 证书，也可以上传从任何其他框架（例如 OpenSSL）或可信机构生成的自定义 HTTPS 证书。自定义 HTTPS 证书允许您控制安全性以及与证书相关的其他主题参数。

要查看默认证书，请导航到 管理 **> HTTPS** 证书。

> 注意
>
> 在提供商托管设置中，只有提供商管理员有权重新生成和上传 HTTPS 证书。



“已安装的证书”部分提供了设备上安装的证书的摘要。设备使用此证书在网络中标识自身。

颁发给 部分提供了有关向谁颁发证书的详细信息。证书中的公 用名 称与设备名称匹配，因为证书绑定到设备名称。颁 发者部分提供了对证书签名的证书签名颁发机构的详细信息。证书详细信息包括证书的指纹、序列号和证书的有效期。

要重新生成证书，请导航到“管理”**>** “**HTTPS** 证书”，然后单击“重新生成”。

> 注意
>
> 重新生成证书会断开所有现有连接的 HTTPS 会话并重新启动 HTTPS 服务器。成功重新生成证书后，GUI 会自动刷新。

您可以从任何其他框架（例如 OpenSSL）或可信机构生成 HTTPS 证书，然后将其上传到本地的 Citrix SD-WAN Orchestrator 上。支持的证书格式为.crt，支持的密钥格式为.key。

要上传自定义 HTTPS 证书，请在“上传 证书”和“上传密钥”框中分别单击“上传”或拖动证书 和 密钥 文件。成功上传后，GUI 会自动刷新。

磁盘空间管理

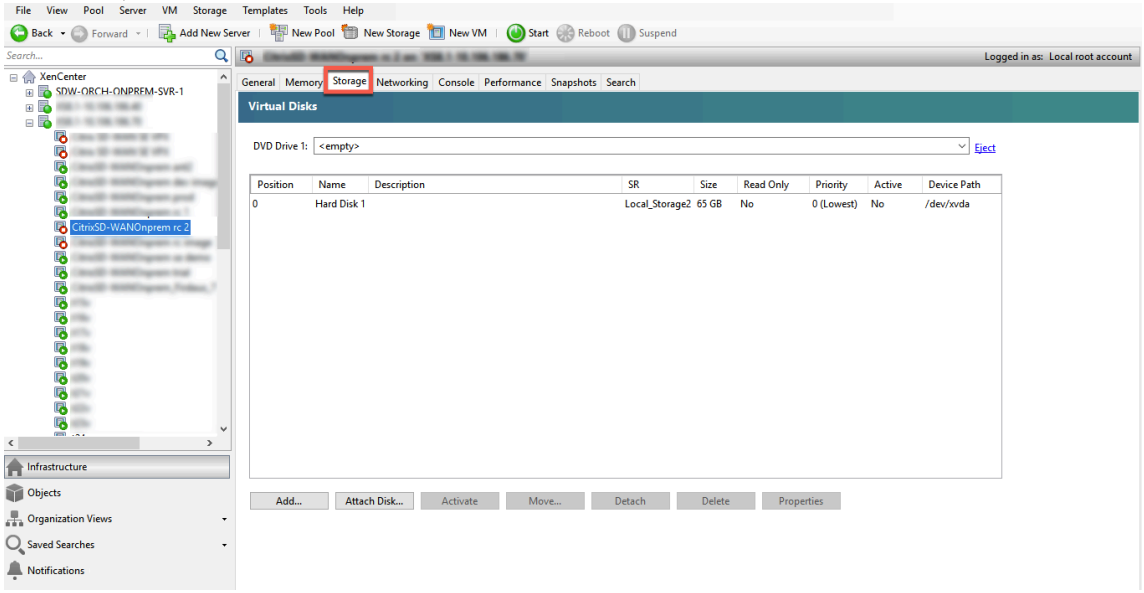
October 21, 2022

您可以增加为本地的 Citrix SD-WAN Orchestrator 分配的磁盘空间。

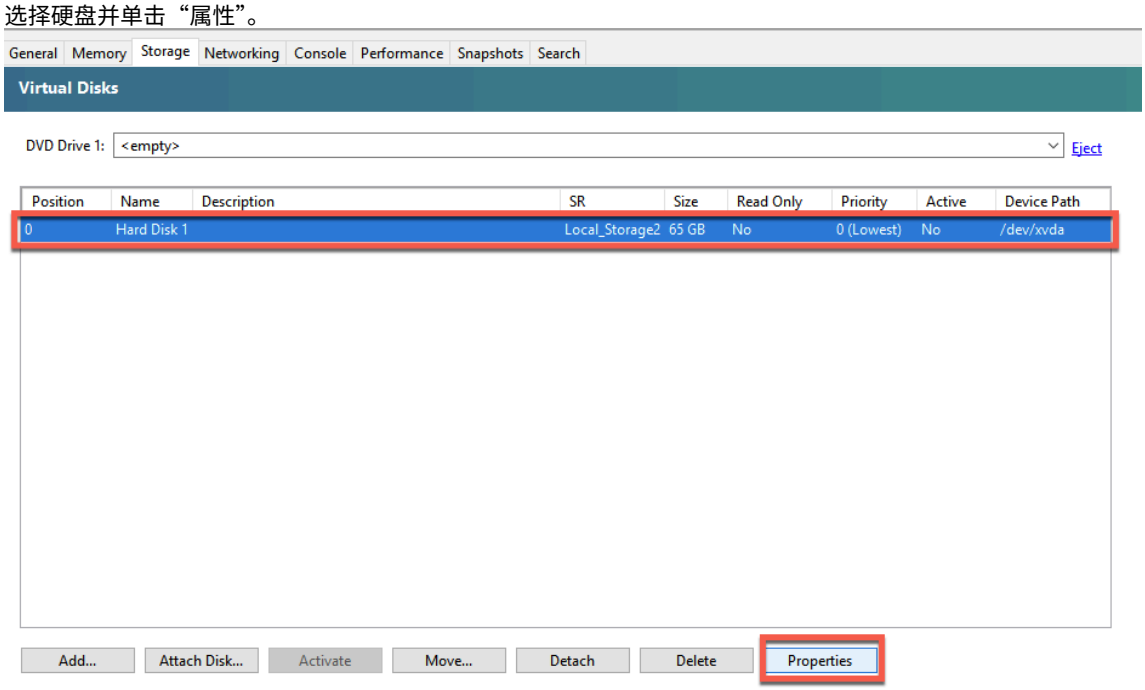
增加 **Citrix Hypervisor** 上的磁盘空间

增加 Citrix Hypervisor 上的磁盘空间。

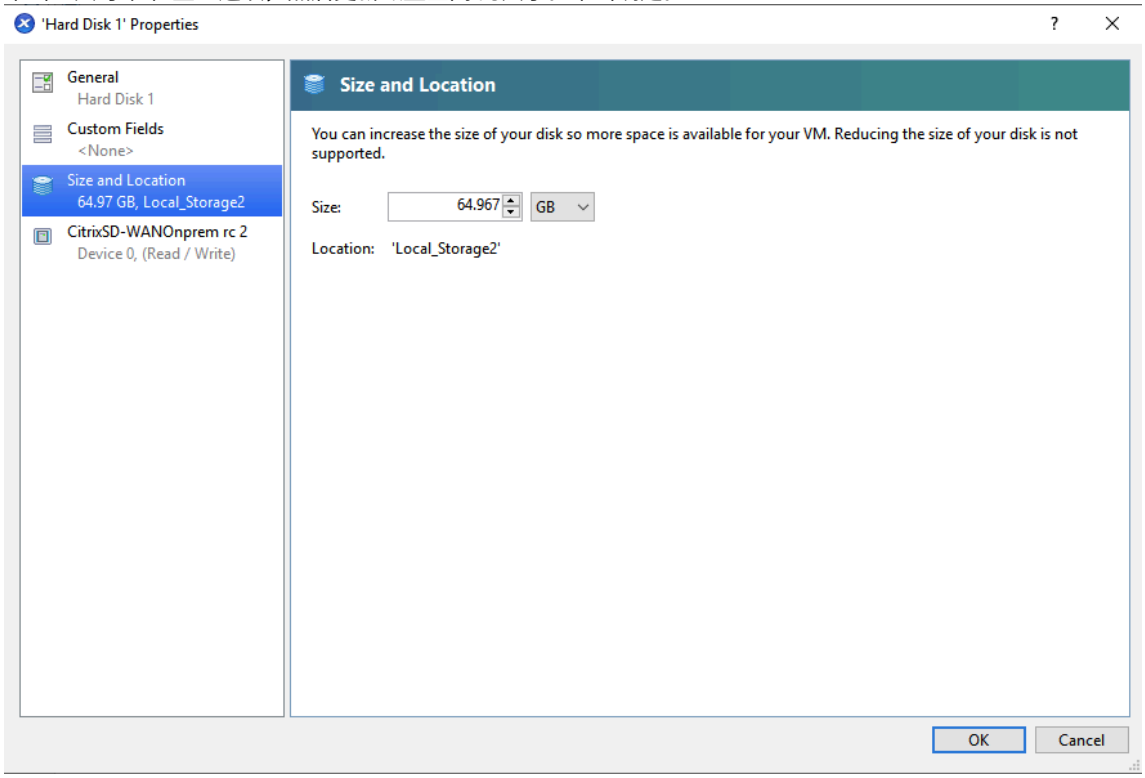
1. 从虚拟机管理程序关闭虚拟机 (VM)。
2. 选择虚拟机，然后单击“存储”选项卡。



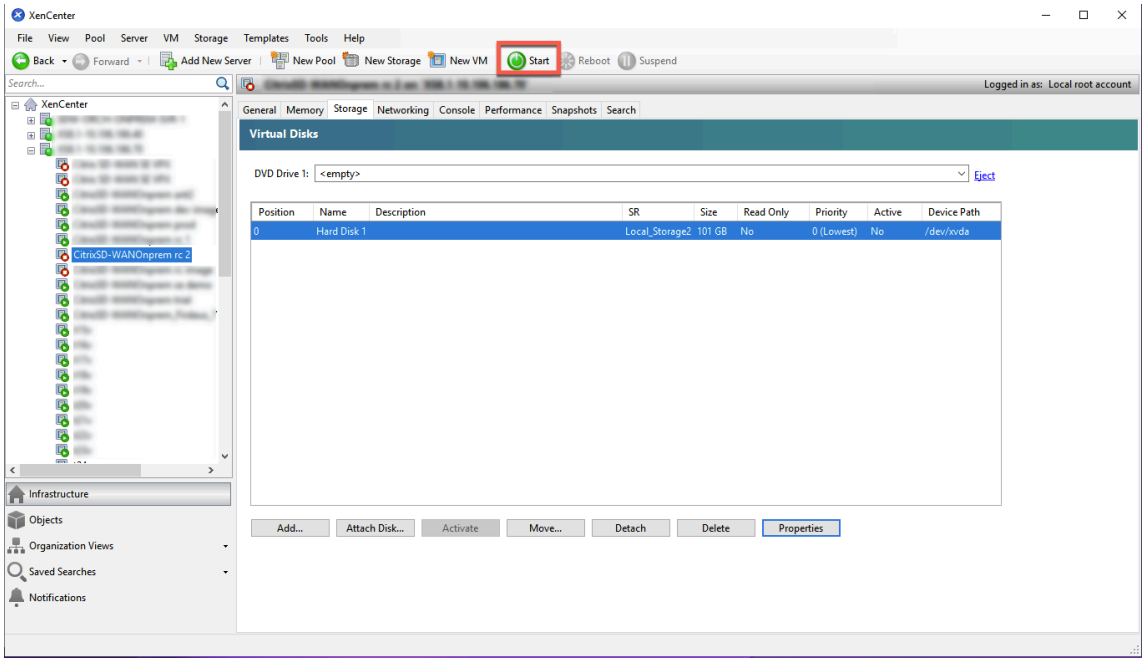
3. 选择硬盘并单击“属性”。



4. 单击“大 小和位置”选项，然后更新磁盘空间 的大小。单击确定。



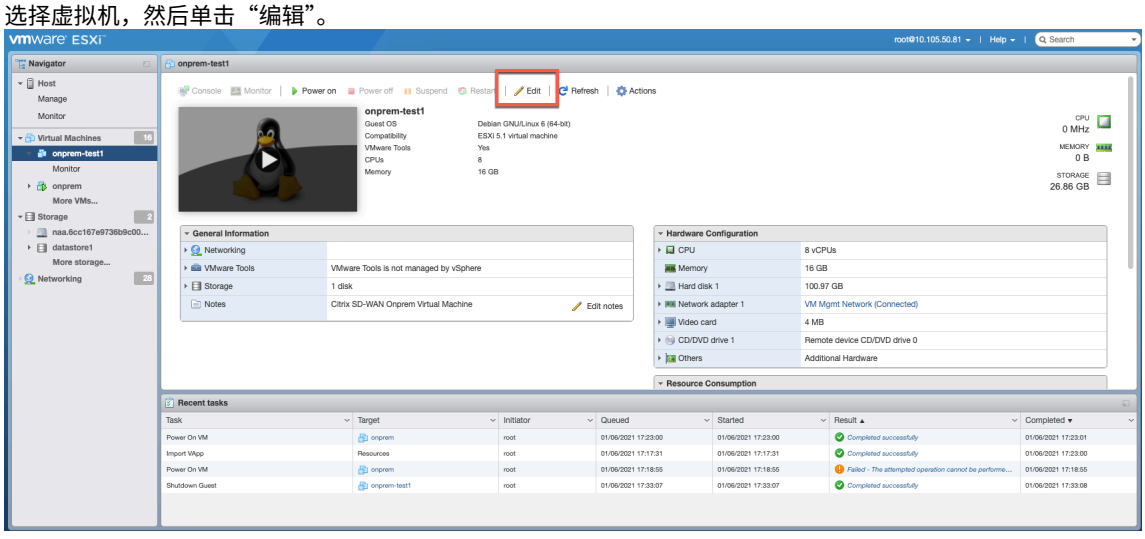
5. 单击 **Start**（开始）。



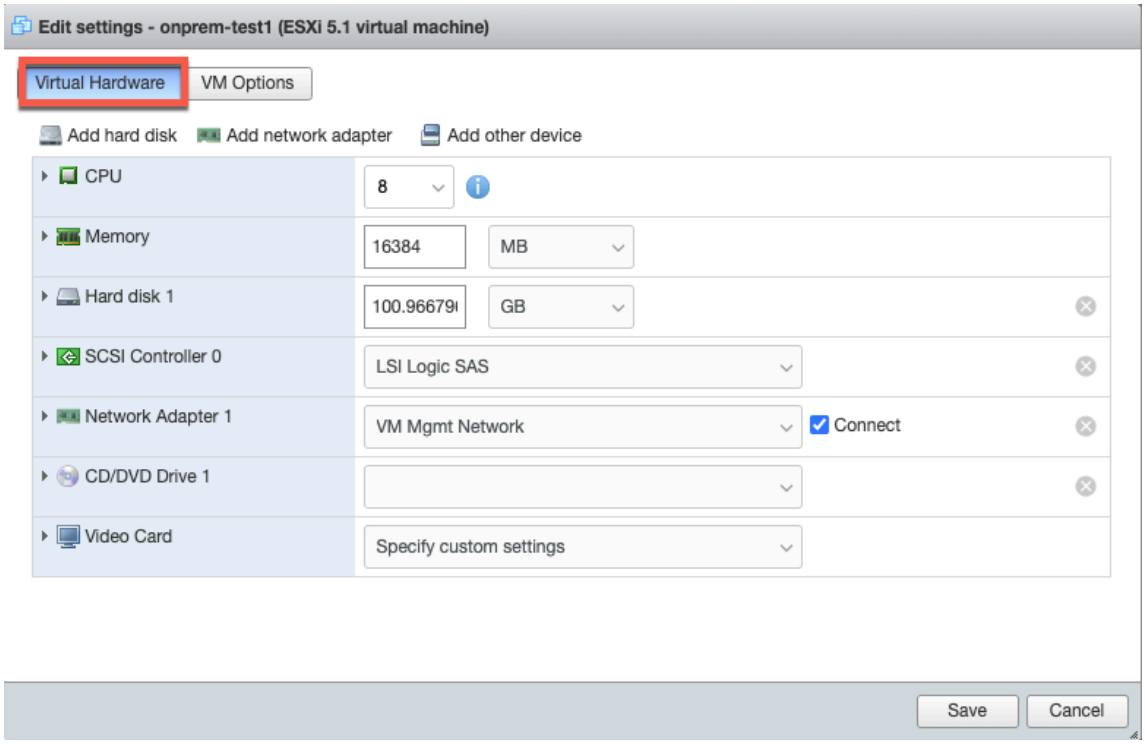
增加 **ESXi** 服务器上的磁盘空间

增加 ESXi 服务器上的磁盘空间。

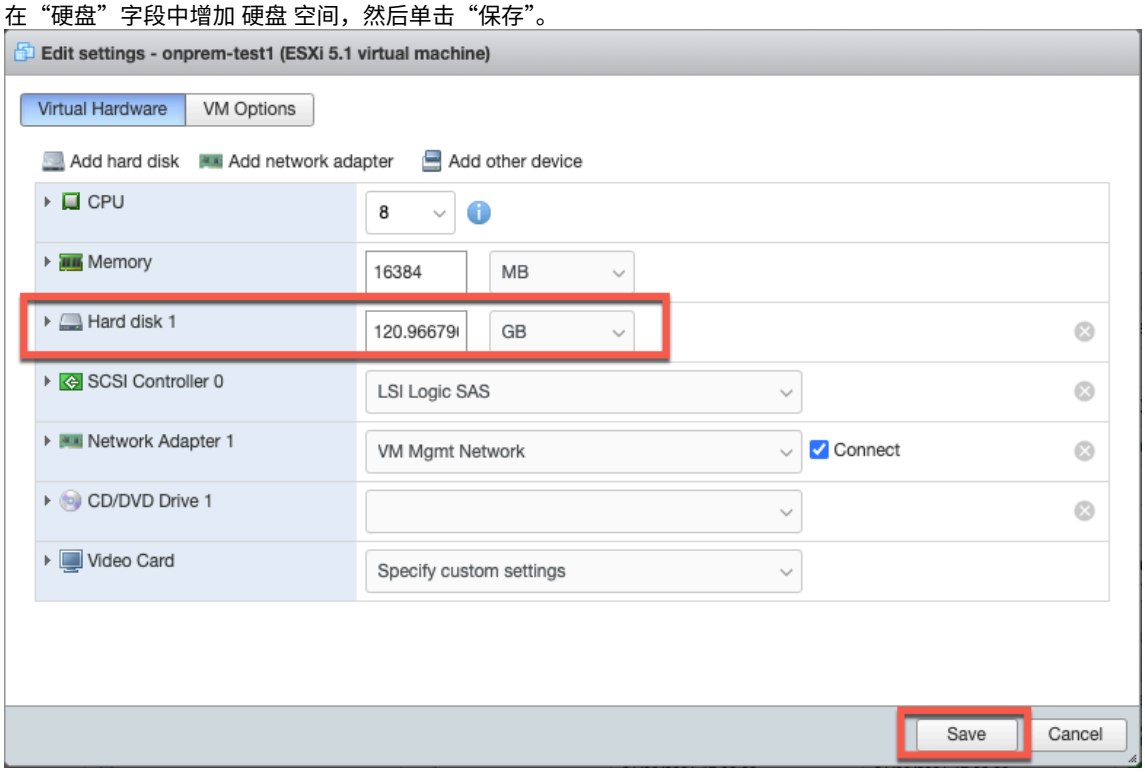
1. 从虚拟机管理程序关闭虚拟机 (VM)。
2. 选择虚拟机，然后单击“编辑”。



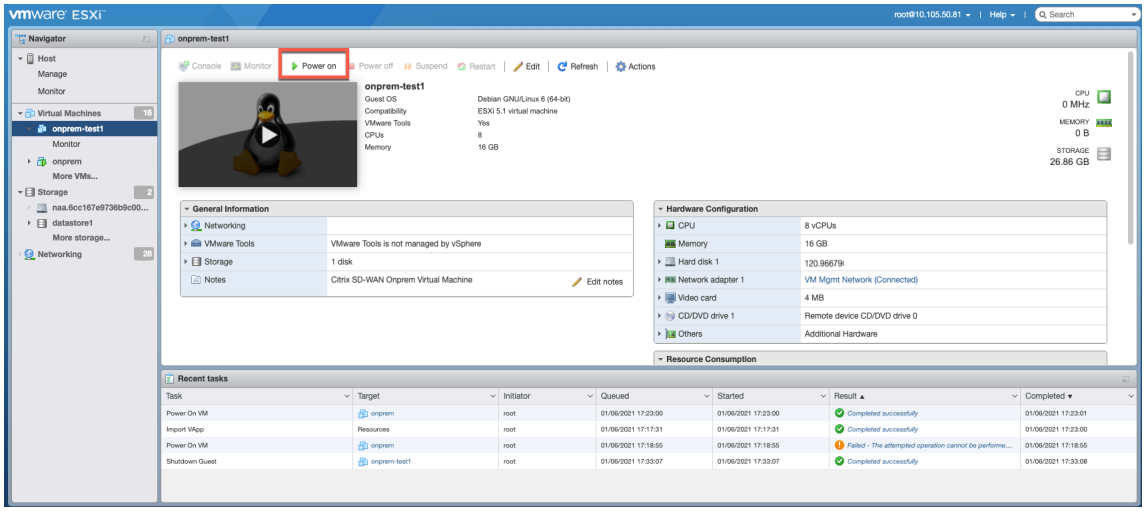
3. 选择“虚拟硬件”选项卡。



4. 在“硬盘”字段中增加 硬盘 空间，然后单击“保存”。



5. 单击“开机”。



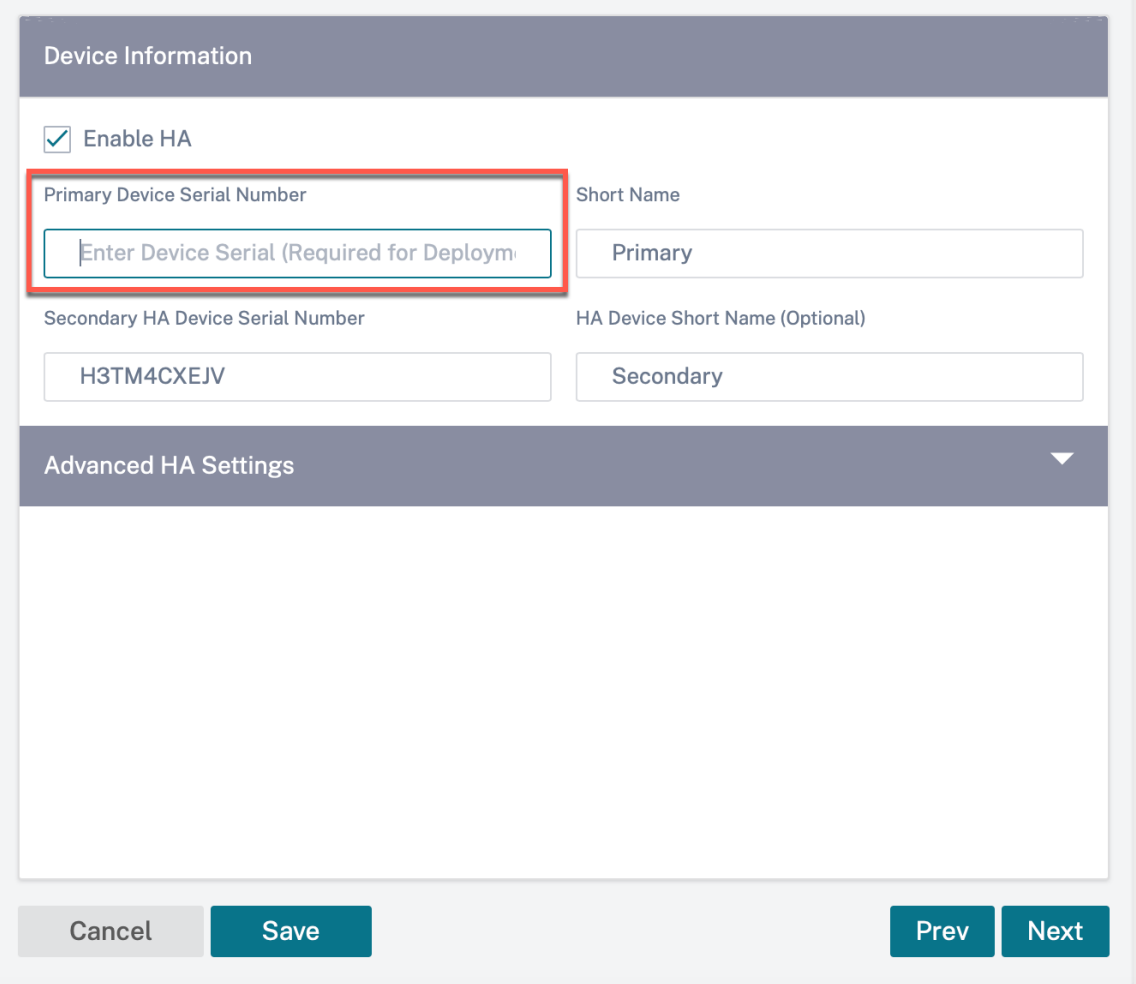
更换受影响的 **Citrix SD-WAN** 设备

October 21, 2022

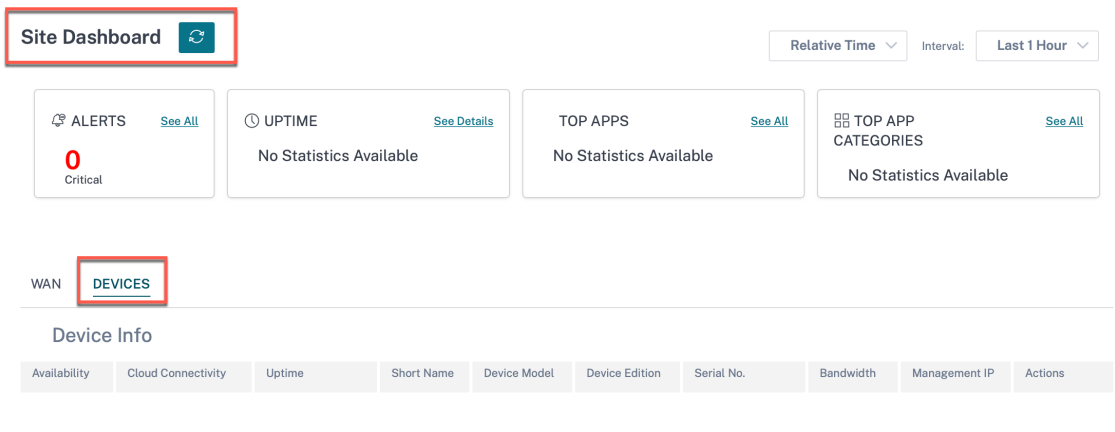
要在 Citrix SD-WAN Orchestrator 本地部署中更换受影响的设备，请执行以下操作：

1. 登录本地版 Citrix SD-WAN Orchestrator 并选择受影响的站点。在站点级别，导航到 **配置 > 站点配置 > 设备信息**，然后从“主设备序列号”字段中删除序列号。单击保存。

   > 注意
   >
   > 如果仍然可以通过本地的 Citrix SD-WAN Orchestrator 访问该设备，则该设备处于“恢复出厂设置”状态。

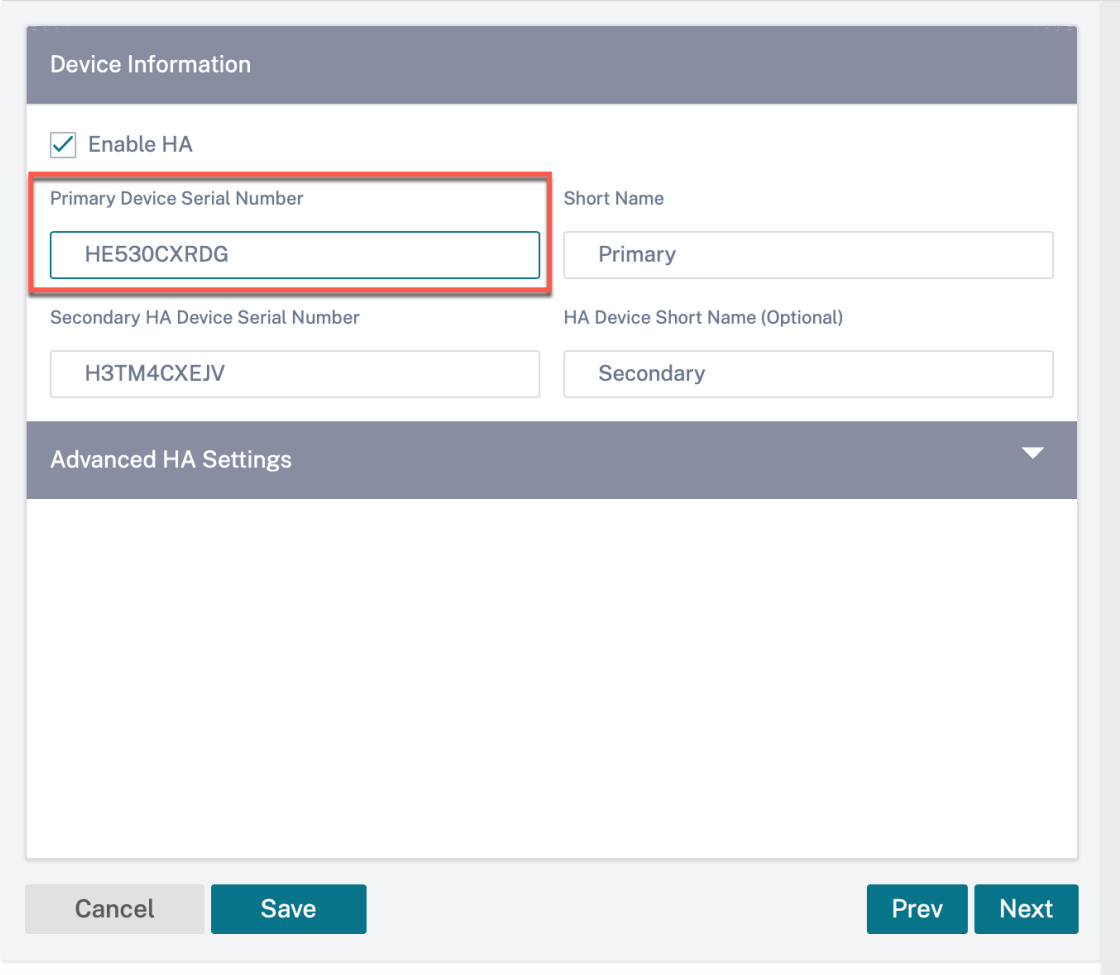


2. 导航到 控制面板 > 设备，并确保将受影响的设备从列表中删除。



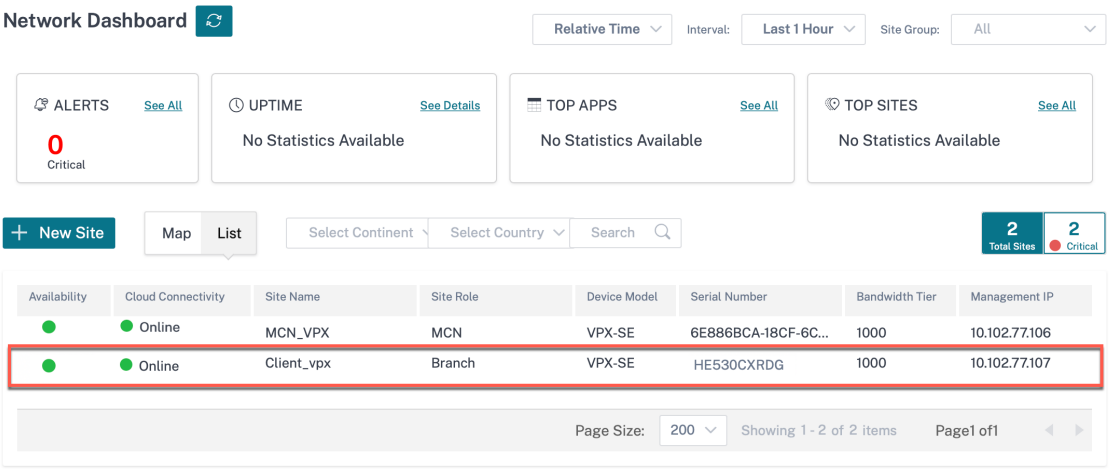
3. 记下受影响设备的电源和布线设置，然后从机架上拆下该设备。
4. 将新设备安装在机架上，然后像对待受影响设备一样重做电源和布线。
5. 在适用于本地用户界面的 Citrix SD-WAN Orchestrator 中，在站点级别导航到 配置 > 站点配置 > 设备详细信

息。在“主设备序列号”字段中添加新装置的序列号。单击保存。



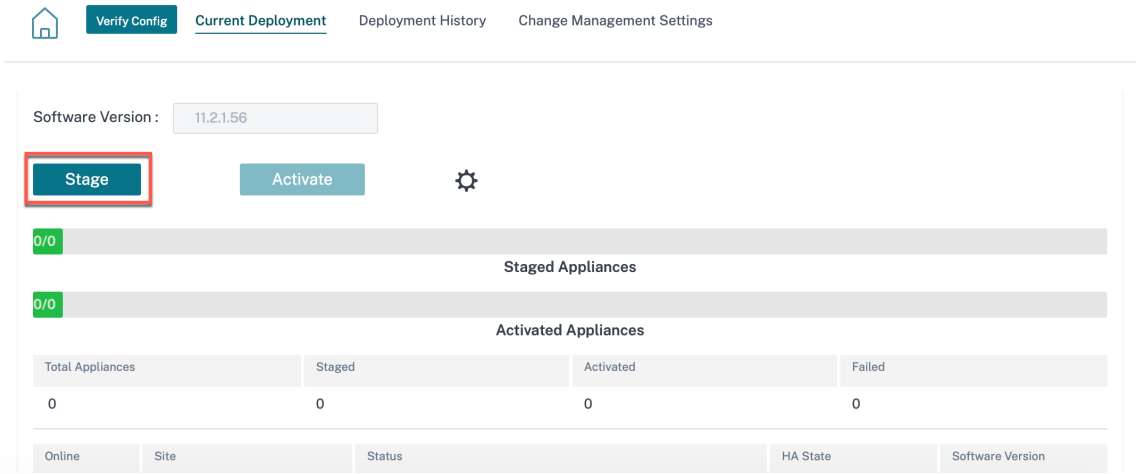
6. 配置零接触部署。有关更多信息，请参阅 零接触部署。

7. 等待几分钟，让设备更新站点仪表板上的云连接。



8. 在网络级别，导航到“配置” > “网络配置主页”，然后单击“部署配置/软件”。

9. 单击“舞台”。



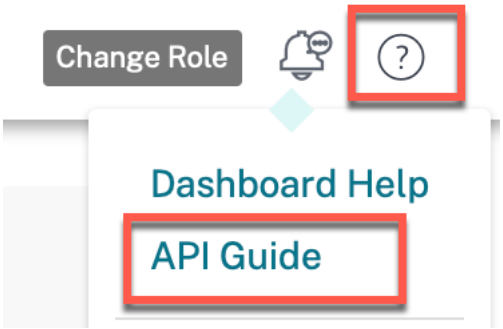
10. 部署完成后，单击“激活”。
11. 导航到站点仪表板并验证设备是否成功激活。

适用于本地 **Citrix SD-WAN Orchestrator** 的 **API** 指南

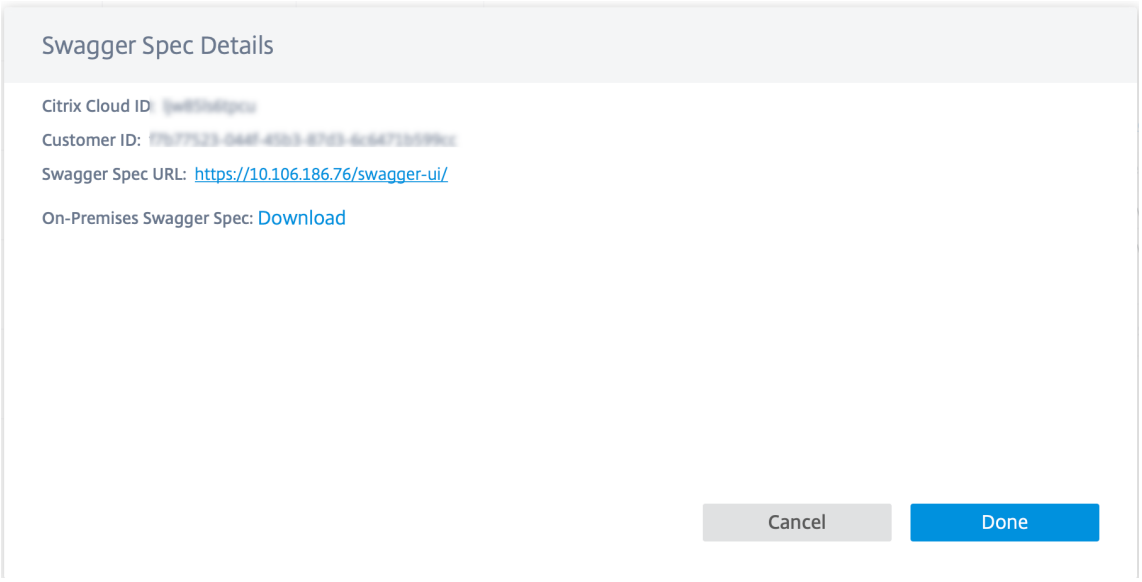
October 21, 2022

要在 Swagger 用户界面上访问 Citrix SD-WAN Orchestrator 本地部署 API 指南，请执行以下操作：

1. 登录本地的 Citrix SD-WAN Orchestrator 然后单击？ 在 UI 的右上角，然后单击 **API** 指南。



此时将显示 Swagger 规格详细信息。



2. 单击 Swagger 规范 URL 以访问 API 指南。

Citrix SD-WAN Orchestrator 通过 curl 提供本地 API

必备条件

- 云端登录
- 本地登录

执行以下步骤，通过 curl 使用 Citrix 本地编排器 API：

1. 云登录：如果是全新的 XVA，则必须先登录到云端。

```
curl -k -X POST -H "Content-Type: application/json "https://<
   onprem-orchestrator-ip>/policy/v1/onprem/cloudLogon  - data '{
 "clientId":"<clientId>","clientSecret":"<clientSecret> ","ccId":"
    <ccid>", "pop": "<popName>" }
 '
```

`clientIdclientSecret`、和 `ccId` 可以从 IAM 页面获取。

> 注意在尝试云登录之前，请
>
> 确保客户帐户已在云中创建。

2. 本地登录：然后进行本地登录以获取身份验证令牌。

```
curl -k -X POST -H "Content-Type: application/json" https://<
   onprem-orchestrator-ip>/onpm/v1/logon --data '{
 "username":"admin","password":"<passwordField>" }
 '
```


这会返回 代币 和 客户 **ID** 作为响应。CustomerID 保持不变，在其他 API 调用中需要它。保存 客户 **ID** 以备日后使用。该令牌的有效期为一小时。之后，你必须重新登录。

示例：使用身份 验证令牌和 **CustomerID** 启动 其他 Citrix 本地 API。

```
curl -k -X GET -H "authorization:CWSAuth bearer= <token> " -H "
    Content-Type: application/json"https://<onprem-orchestrator-ip
    >/onpm/v1/scope/<customerId>/globalSettings/ntpSettings
```

管弦乐器管理

October 21, 2022

本节为您提供有关可以在适用于本地的 Citrix SD-WAN Orchestrator 平台上执行的管理活动的信息。

软件

您可以下载网络中所有设备所需的 Citrix SD-WAN 设备软件版本，并存储在本地的 Citrix SD-WAN Orchestrator 中。使用存储的软件将适用于本地的 Citrix SD-WAN Orchestrator 软件升级到最新版本。

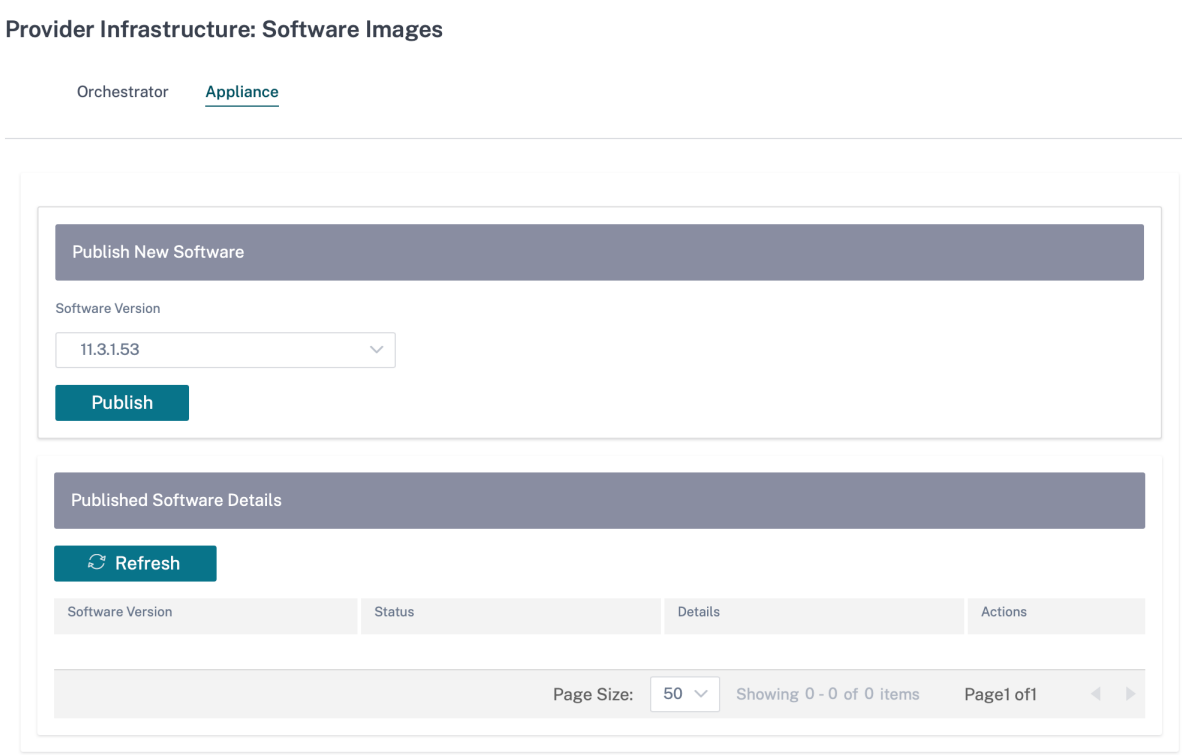
> 注意
>
> 提供商托管安装是从适用于本地 10.3 版本的 Citrix SD-WAN Orchestrator 中引入的。不支持降级到低于本地 10.3 版本的 Citrix SD-WAN Orchestrator 版本的软件版本。

发布软件

在提供商托管设置中，适用于本地的 Citrix SD-WAN Orchestrator 允许提供商管理员下载网络中所有设备所需的 Citrix SD-WAN 设备软件版本。提供商管理员可以发布下载的软件版本。已发布的软件已下载并存储在适用于本地的 Citrix SD-WAN Orchestrator 中。客户管理员可以将已发布的软件部署到由 Citrix SD-WAN Orchestrator 管理的所有本地设备上。

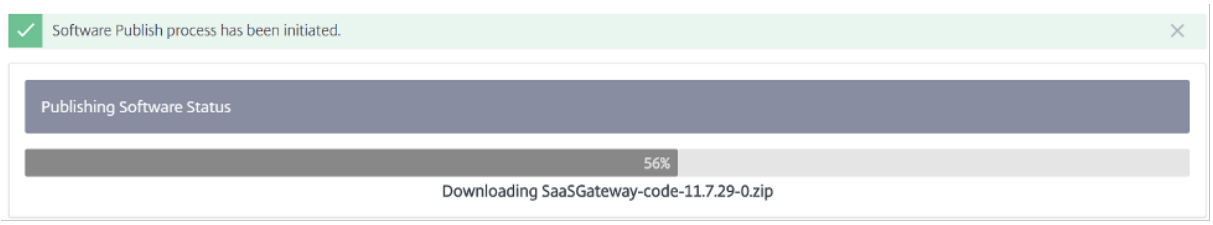
在客户托管设置中，客户管理员可以下载网络中所有设备所需的 Citrix SD-WAN 设备软件版本。他们可以在适用于本地的 Citrix SD-WAN Orchestrator 中发布该软件，并将该软件部署到所有设备。

要发布软件，请导航到 基础架构 **> Orchestrator** 管理 **>** 软件映像 **>** 设备。

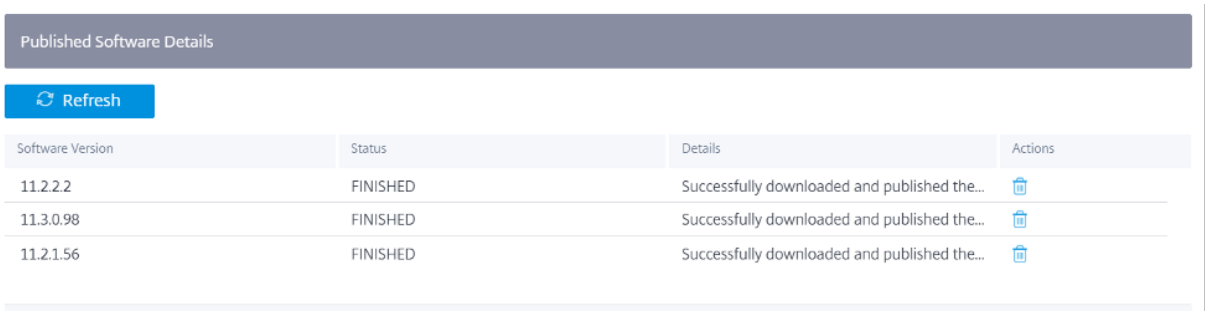


您可以从当前 Citrix SD-WAN Orchestrator 支持本地部署的 Citrix SD-WAN Orchestrator 的预建软件版本列表中选择要发布的软件版本。对于列表中未提供的较新软件版本，请升级到支持新软件版本的最新 Citrix SD-WAN Orchestrator for Inclouse 版本。有关升级适用于本地的 Citrix SD-WAN Orchestrator 的信息，请参阅 软件升级。

适用于本地的 Citrix SD-WAN Orchestrator 下载适用于所有平台的选定版本的 Citrix SD-WAN 软件。进度条表示发布过程的进度。



已发布的软件版本显示在“已发布的软件详细信息”下。在任何给定时刻，适用于本地的 Citrix SD-WAN Orchestrator 最多可以存储三个已发布的软件版本。如果您打算发布其他软件版本，请在开始发布过程之前删除三个可用版本中的一个。



发布成功后，您可以从“网络 配置”页面将软件部署、暂存和激活到网络 上的所有设备。有关更多信息，请参阅 网络配置。要成功部署，请确保所有设备都连接到适用于本地的 Citrix SD-WAN Orchestrator。有关更多详细信息，请参阅 与 Citrix SD-WAN 设备的连接。

软件升级

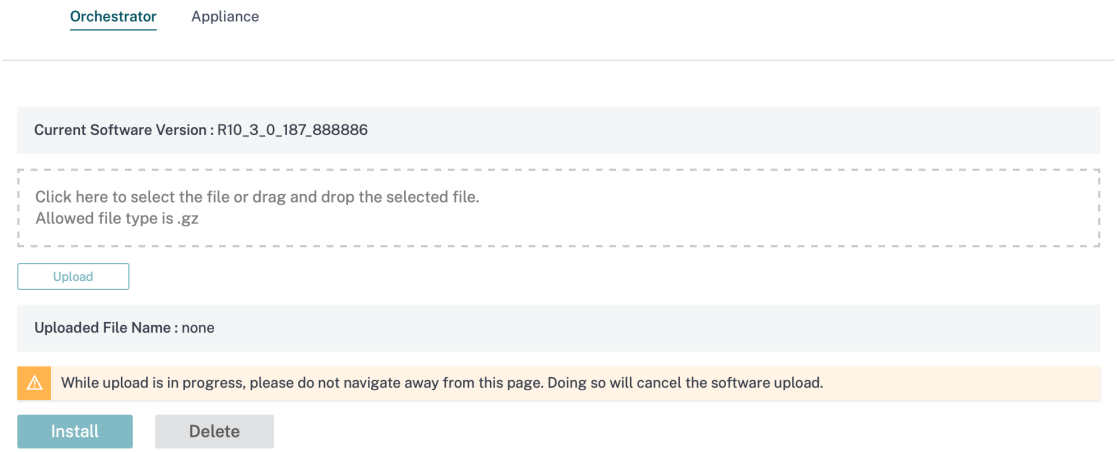
在提供商托管设置中，只有提供商管理员才能将适用于本地的 Citrix SD-WAN Orchestrator 软件升级到最新版本。

在客户托管设置中，客户管理员可以将适用于本地的 Citrix SD-WAN Orchestrator 软件升级到最新版本。

> 注意
>
> - 将相应的 Citrix SD-WAN Orchestrator for Inclouse 软件包下载到您的本地计算机。您可以从下载页面下载 此软件包。
> - Citrix 建议在虚拟机管理程序中拍摄虚拟机的快照。此外，SD-WAN 配置是在升级之前下载的。
> - Citrix 还建议定期拍摄虚拟机和 SD-WAN 配置的快照。

执行以下步骤来上传和安装适用于本地的 Citrix SD-WAN Orchestrator 软件的新版本：

1. 在适用于本地用户界面的 Citrix SD-WAN Orchestrator 中，导航到 基础架构 **> Orchestrator** 管理 **>** 软件映像 **> Orchestrator**。
2. 在框内单击，然后选择您已下载并保存在本地系统上的 ctx-onprem-1（最新日期）.tar.gz 二进制文件。



3. 单击“上传”将选定的软件包上传到当前适用于本地虚拟机的 Citrix SD-WAN Orchestrator。
4. 上传完成后，单击“安装”。
5. 当系统提示确认时，单击“安装”。

管理设置

> 注意
>
> 在提供商托管设置中，只有提供商管理员有权编辑 基础架构 **> Orchestrator** 管理 **>** 管理设置下的配置。

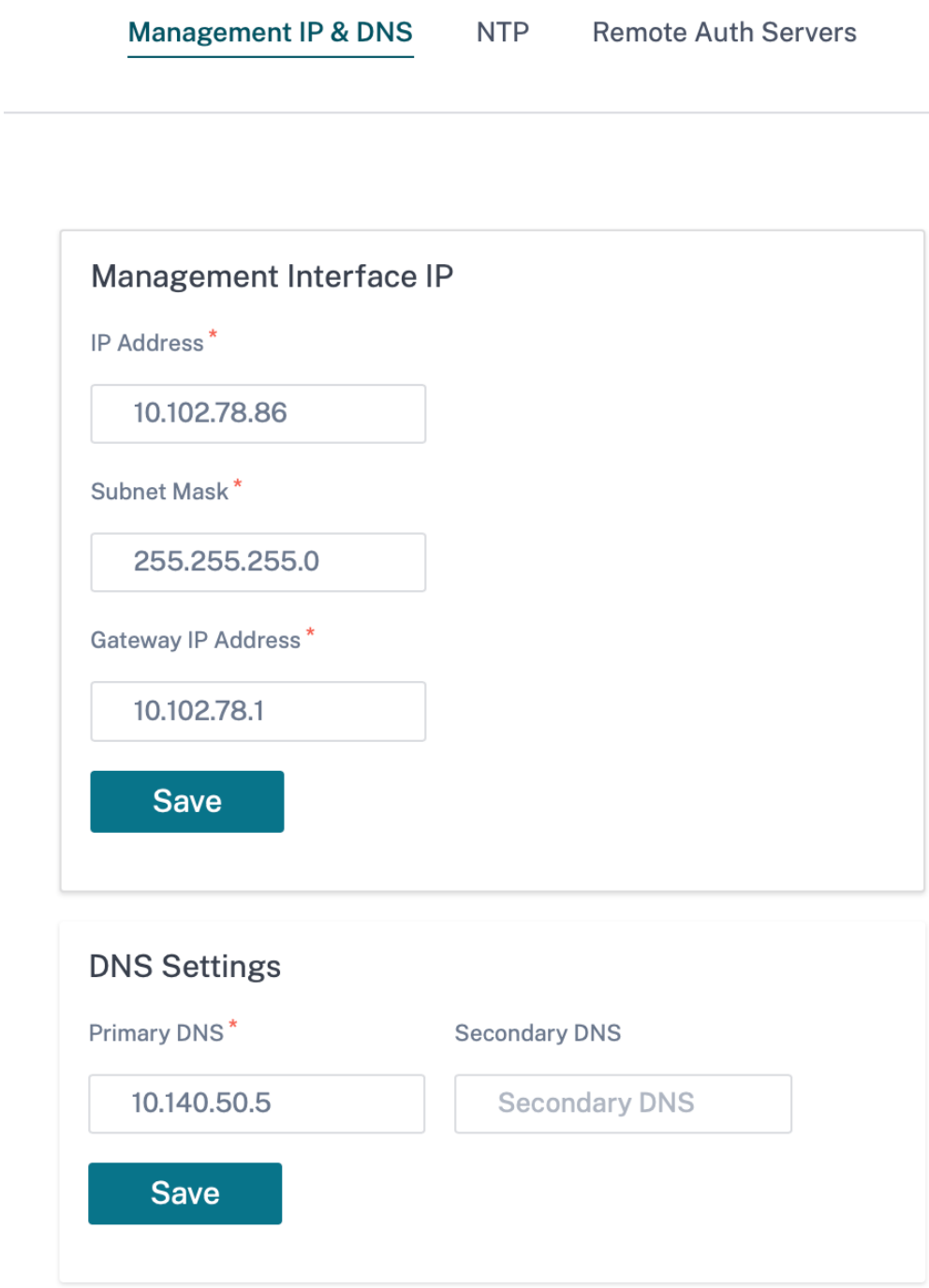
管理 **IP** 和 **DNS**

部署适用于本地虚拟机 (VM) 的 Citrix SD-WAN Orchestrator 并手动或通过 DHCP 配置管理 IP 后，您可以通过适用于本地 GUI 的 Citrix SD-WAN Orchestrator 更改 管理 **IP** 和 **DNS** 设置。适用于本地堆栈的 Citrix SD-WAN Orchestrator 大约需要 3 分钟才能重新启动。更改管理 IP 地址后，SSH 连接将重新建立。

要配置/更改管理 IP 和 DNS 设置，请在网络级别导航到 基础架构 **> Orchestrator** 管理 **>** 管理设置 **>** 管理 **IP** 和 **DNS**。

提供以下详细信息：

- **IP** 地址：适用于本地虚拟机的 Citrix SD-WAN Orchestrator 的 IP 地址。
- 网关 **IP** 地址：适用于本地的 Citrix SD-WAN Orchestrator 用于与外部网络通信的网关 IP 地址。
- 子网掩码：用于定义本地版 Citrix SD-WAN Orchestrator 可用的网络的子网掩码。
- 主 **DNS**：来自本地的 Citrix SD-WAN Orchestrator 的所有 DNS 请求都将转发到的主 DNS 服务器的 IP 地址。
- 辅助 **DNS**：在主 DNS 服务器不可用时用于解析 DNS 请求的辅助 DNS 服务器的 IP 地址。

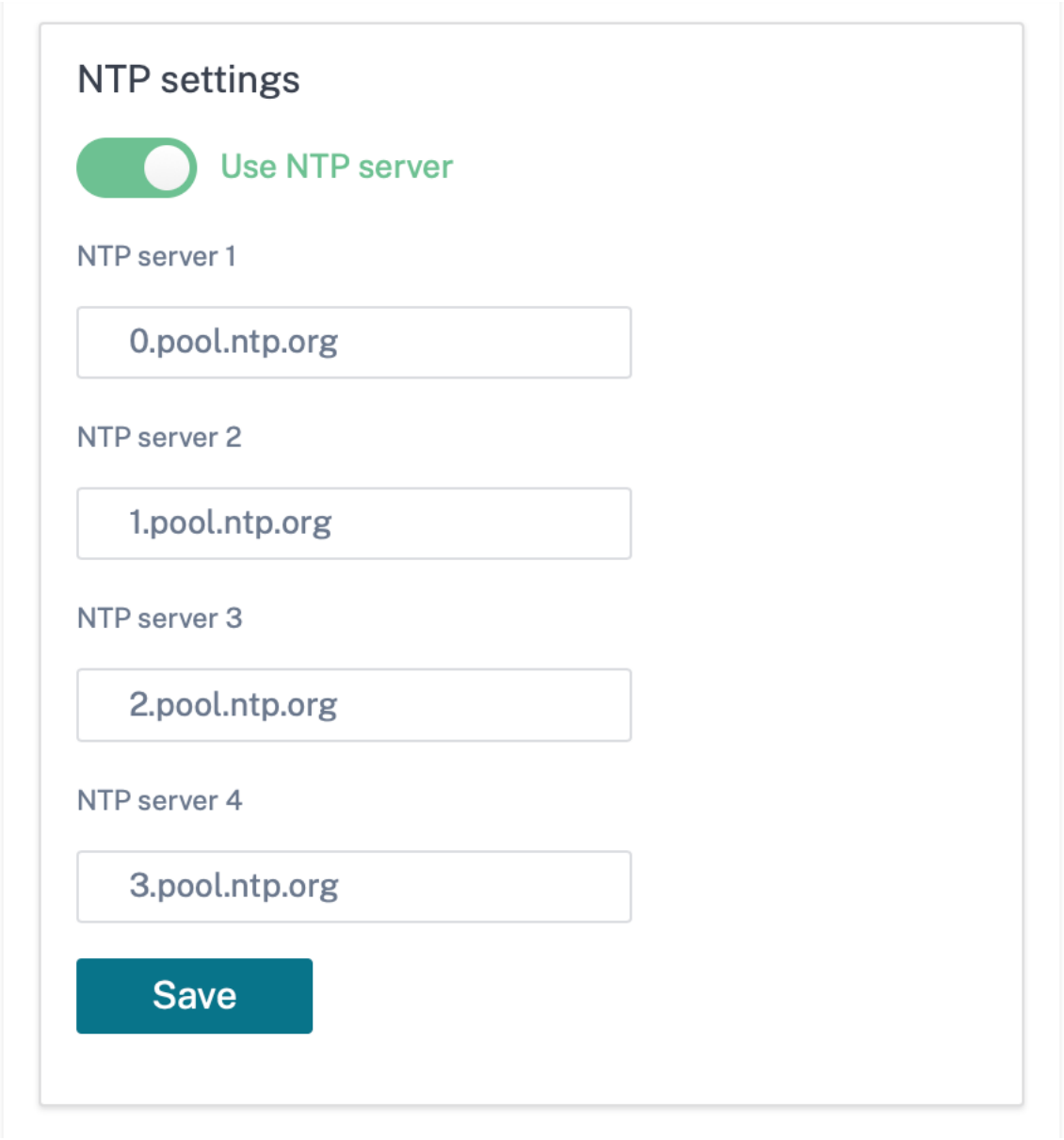


NTP 设置

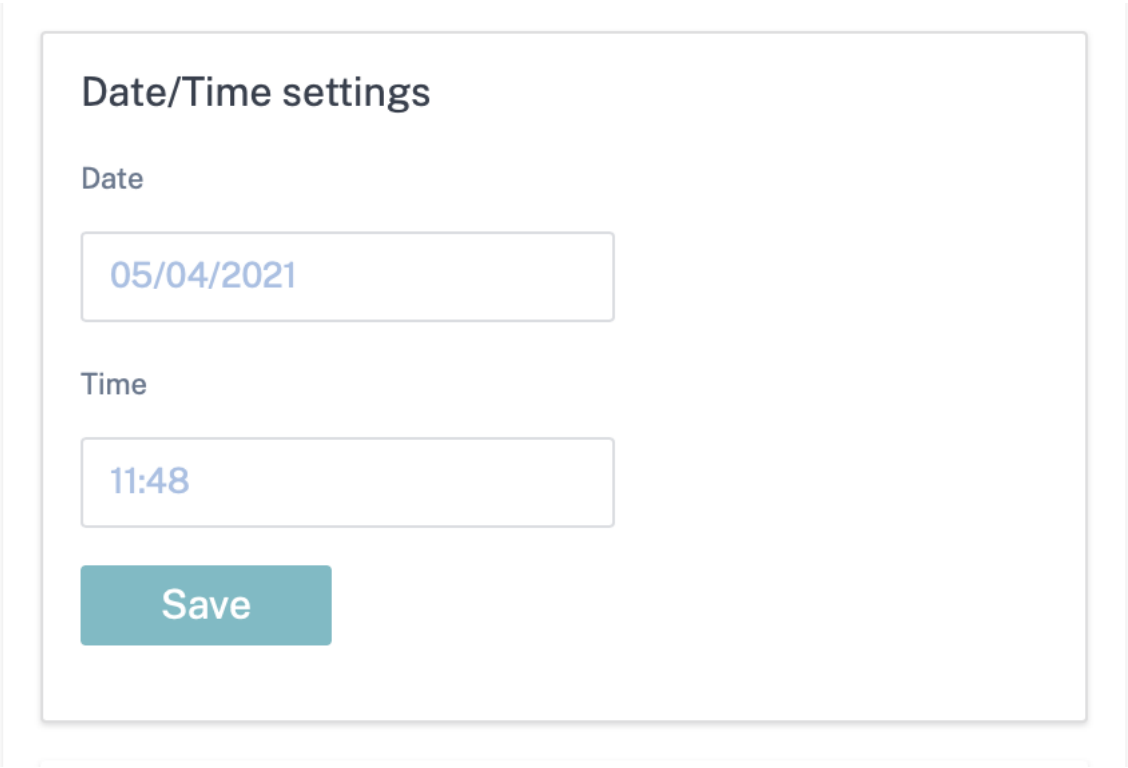
您可以手动设置日期和时间，也可以使用网络时间协议 (NTP) 服务器将 Citrix SD-WAN Orchestrator 的本地时钟时间与协调世界时 (UTC) 同步。

要配置 NTP 服务器，请在网络级别导航到 基础架构 **> Orchestrator** 管理 **>** 管理设置 **> NTP** ，然后启用“使用 **NTP** 服务器”。

提供 NTP 服务器 IP 地址或域名。您最多可以提供四台 NTP 服务器，但请确保至少配置了一台。如果一台 NTP 服务器出现故障，Citrix SD-WAN Orchestrator for Inclouse 会自动与另一台 NTP 服务器同步。如果为 NTP 服务器指定域名，请确保将外部 DNS 服务器配置为将域名指向 IP 地址。

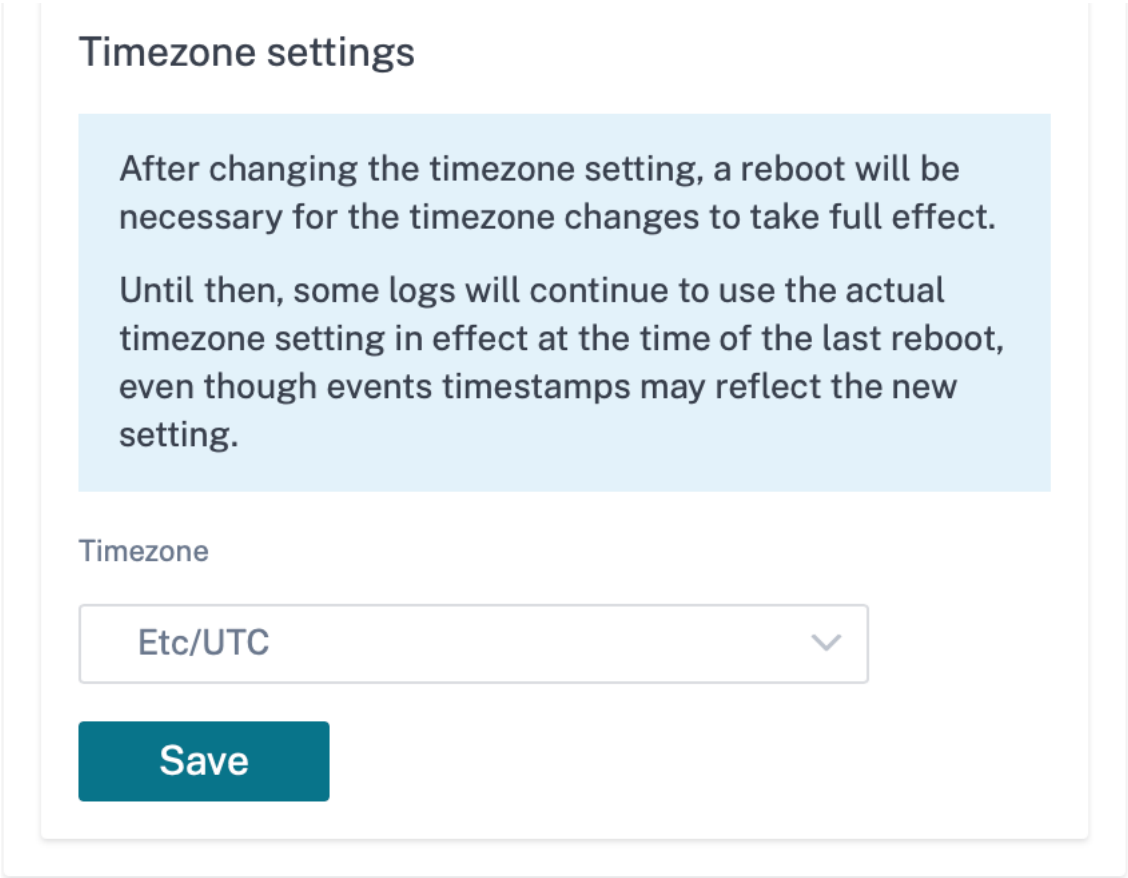


要手动配置日期和时间，请禁用“使用 **NTP** 服务器”选项，然后手动选择日期和时间。



根据您的国家/城市选择时区。

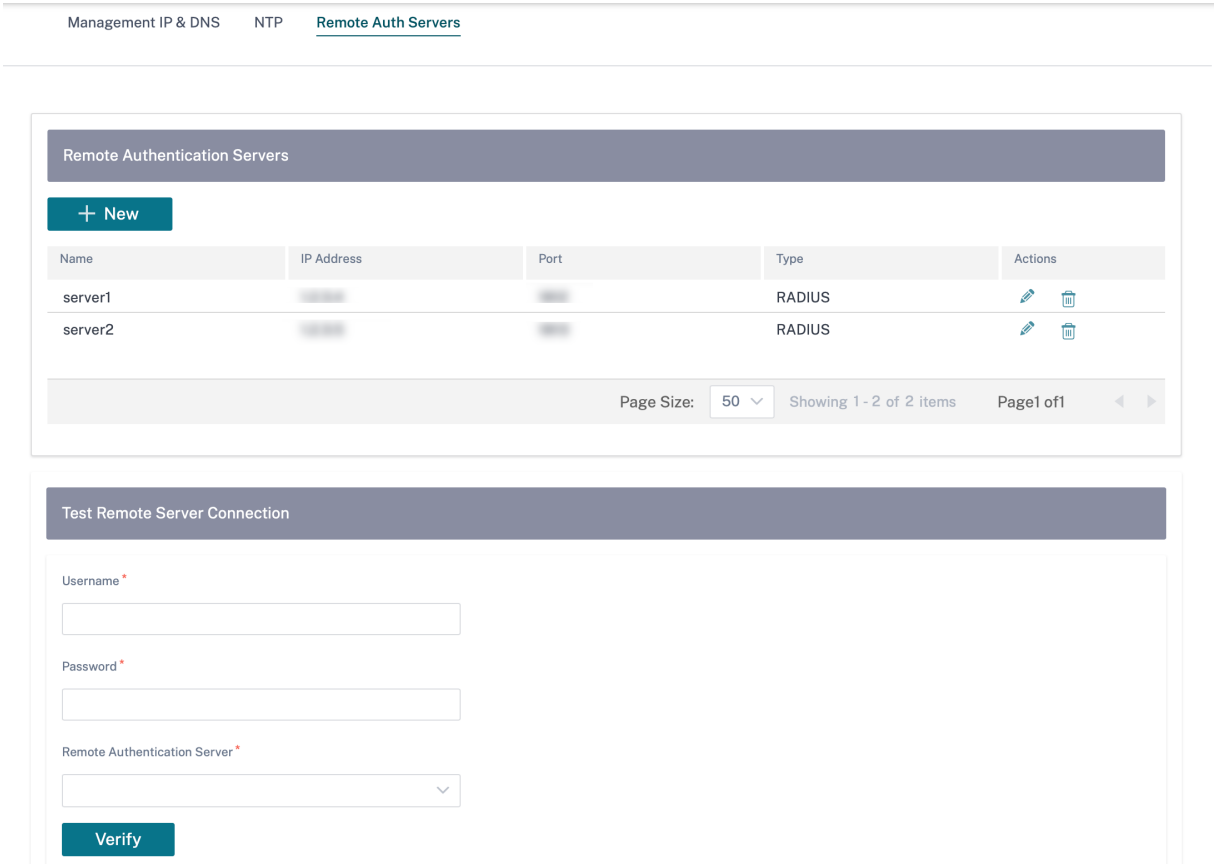
> 注意
>
> 更改时区后重新启动 Orchestrator 虚拟机。有些日志会继续使用以前的时区，直到重新启动完成。有关说明，请参阅 重启 Orchestrator 虚拟机。



远程认证服务器

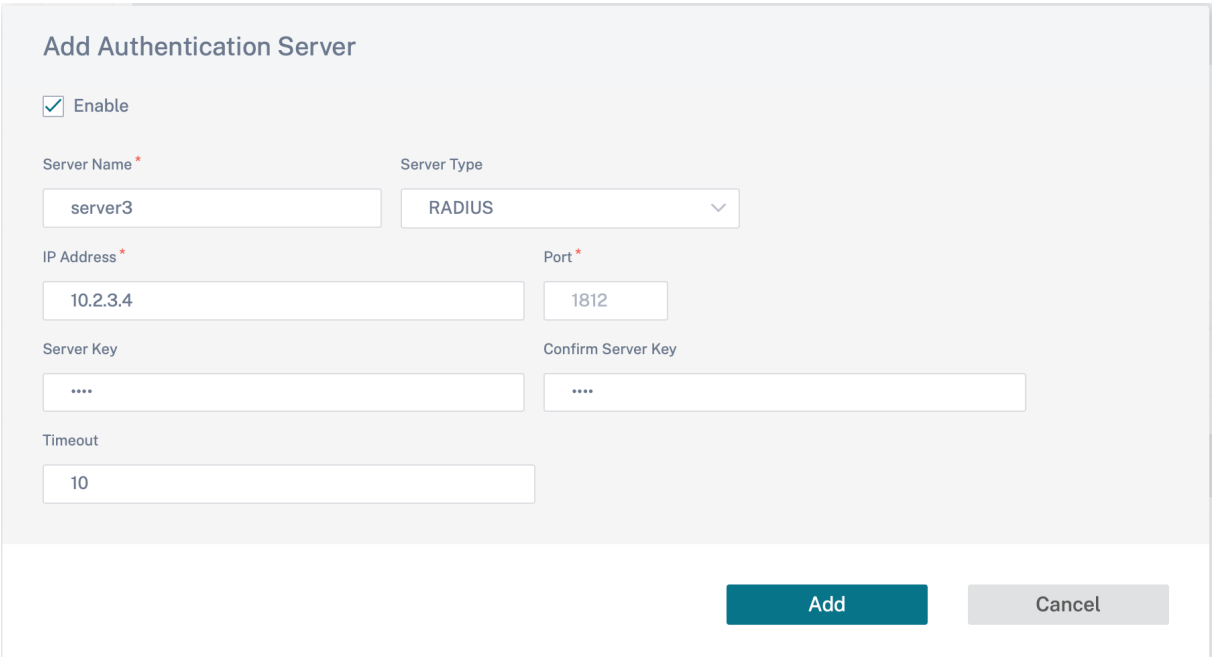
在提供商托管设置中，只有提供商管理员才能为经过远程身份验证的用户配置 RADIUS 或 TACACS+ 服务器。客户管理员可以使用提供商管理员配置的远程身份验证服务器。在客户管理的设置中，客户管理员可以配置 RADIUS 或 TACACS+ 服务器。

> 注意
>
> 确保在 RADIUS 或 TACACS+ 身份验证服务器上创建所需的用户帐户。



要配置远程身份验证，请导航到 基础架构 **>** **Orchestrator** 管理 **>** 管理设置 **>** 远程身份验证服务器。单击 **+** 新建。输入以下详细信息：

- 启用：启用远程身份验证服务器配置。
- 服务器名称：远程身份验证服务器的名称。
- 服务器类型：远程身份验证服务器的类型-RADIUS 或 TACACS+。
- **IP** 地址：远程身份验证服务器的主机 IP 地址。
- 端口：远程身份验证服务器的端口号。RADIUS 服务器的默认端口为 1812，TACACS+ 服务器的默认端口为 49。
- 服务器密钥 和 确认服务器密钥：连接到远程身份验证服务器时使用的密钥。
- 身份验证类型：（仅适用于 TACACS+ 服务器）选择用于将用户名和密码发送到 TACACS+ 服务器的加密方法。
  - **PAP**：使用密码身份验证协议 (PAP) 通过为 TACACS+ 服务器分配强共享密钥来加强用户身份验证。
  - **ASCII**：使用 ASCII 字符集通过为 TACACS+ 服务器分配强共享密钥来加强用户身份验证。
- 超时：等待来自远程身份验证服务器的身份验证响应的时间间隔（以秒为单位）。



您也可以测试远程服务器连接。在“测试远程服务器连接”下，提供您的 用户名 和 密码。选择远程身份验证服务器，然后单击“验证”。

数据库管理

您可以为在 Citrix SD-WAN Orchestrator 上运行的当前数据库创建备份，然后使用备份的文件恢复相同的数据库状态。

> 注意
>
> - 在提供商托管设置中，只有提供商管理员有权创建和恢复数据库备份。
> - 您无法在客户管理的设置上恢复在提供商管理的设置中创建的数据库备份。同样，您无法在提供商管理的设置上恢复在客户管理的设置中创建的数据库备份。

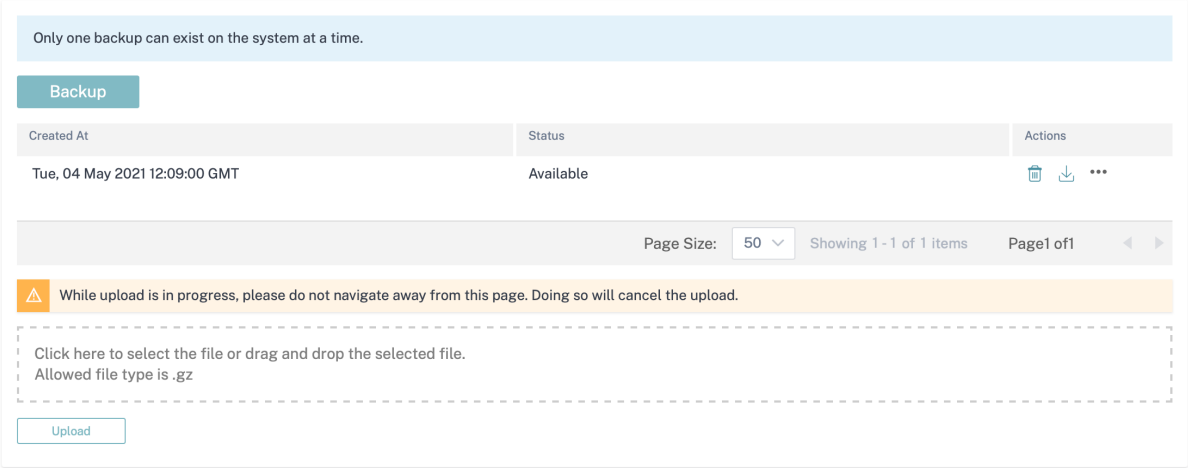
要创建数据库备份，请导航到 基础架构 > **Orchestrator** 管理 > 数据库管理。单击备份。

在“操作”列下单击“下载”，下载已备份的数据库。

单击“上传”浏览并上传下载的文件。您也可以将下载的文件拖放到屏幕上。

要恢复，请单击“操作”列下的“恢复”。

> 注意
>
> - 一次只能保存一个数据库备份。要用最新备份替换现有备份，请删除现有备份，然后单击“备份”。
> - 数据库的还原必须与进行数据备份的本地版 Citrix SD-WAN Orchestrator 的版本相同。
> - 数据库备份仅对配置和统计数据进行备份。它不备份与平台相关的数据。



存储管理

适用于本地的 Citrix SD-WAN Orchestrator 支持将客户配置、统计信息、本地数据库和已发布的 Citrix SD-WAN 发行版本从现有磁盘迁移到新磁盘。

在提供商托管设置中，只有提供程序管理员才能执行磁盘迁移。提供商托管设置中的客户管理员没有执行磁盘迁移的权限。在客户管理的设置中，客户管理员可以执行磁盘迁移。

您可以执行磁盘迁移以增加磁盘空间或用于灾难恢复。

- 添加新磁盘：您可以添加一个新磁盘，其存储大小至少是本地的 Citrix SD-WAN Orchestrator 消耗的当前数据的两倍。通过适用于本地用户界面的 Citrix SD-WAN Orchestrator，您可以激活新磁盘并迁移现有的客户配置、统计信息、本地数据库和已发布的 Citrix SD-WAN 发行版本。激活新添加的磁盘后，适用于本地的 Citrix SD-WAN Orchestrator 将重新启动。
- 灾难恢复：发生灾难时，您可以将包含数据的磁盘连接到适用于本地虚拟机的 Citrix SD-WAN Orchestrator 的新实例，该实例与 Citrix SD-WAN Orchestrator 的本地版本相同。在适用于本地用户界面的 Citrix SD-WAN Orchestrator 中，无需选择“迁移数据”选项即可激活磁盘。激活磁盘后，适用于本地的 Citrix SD-WAN Orchestrator 将重新启动。

> 注意
>
> - 当磁盘迁移正在进行时，请勿关闭电源或手动重启 Citrix SD-WAN Orchestrator for Indeliad。关闭电源或手动重启可能会导致数据丢失。
> - 将磁盘从之前添加的磁盘分区迁移到新创建的磁盘分区时，迁移后，旧磁盘中的数据不会被删除。要删除旧磁盘中的数据，请将其连接到另一个操作系统并安全地删除数据。

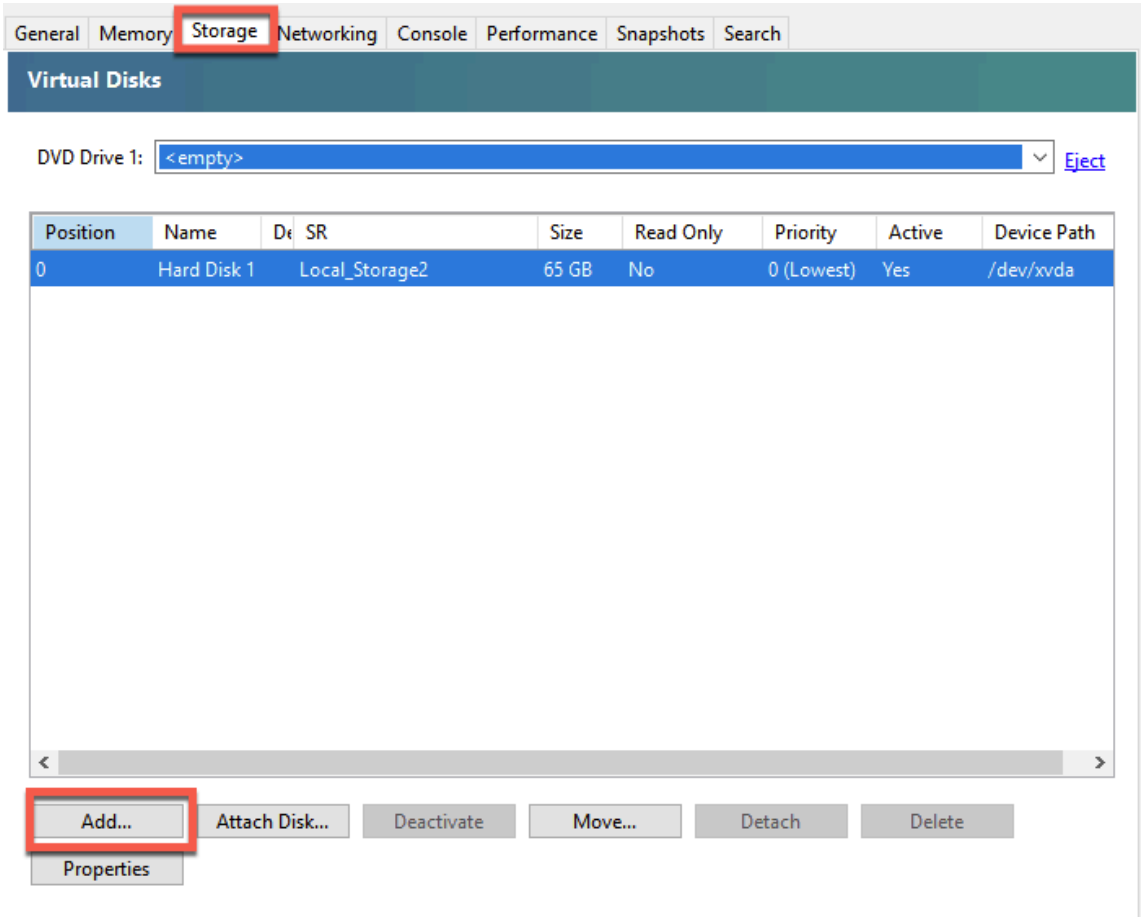
限制

以下是磁盘迁移过程的限制：

- 旧版本中的用户不会迁移到新版本。迁移后，删除用户并重新创建。
- 在用于本地虚拟机的旧 Citrix SD-WAN Orchestrator 上创建的 STS 不会迁移。但是，迁移后，用户界面会列出在适用于本地虚拟机的旧 Citrix SD-WAN Orchestrator 上生成的 STS。手动删除 STS。
- 在旧的 Citrix SD-WAN Orchestrator 中创建的本地数据库备份不会迁移。迁移后，如果已列出，请手动将其删除。
- 默认情况下，假设磁盘迁移到的新 Citrix SD-WAN Orchestrator for Inclouse 可以连接到所有双因素身份验证服务器。如果管理员帐户使用双因素身份验证服务器，并且与双因素身份验证服务器的连接不可用，则即使管理员也无法登录。在这种情况下，请联系 Citrix 支持人员。
- 迁移到新磁盘后，您无法增加为本地的 Citrix SD-WAN Orchestrator 分配的磁盘空间。
- 在灾难恢复场景中，您必须在激活磁盘后重新配置自定义域。
- 在灾难恢复场景中，激活磁盘后，您必须执行非云零接触部署或云代理零接触部署，才能在站点上的 Citrix SD-WAN 设备与 Citrix SD-WAN Orchestrator for Incloude 之间建立连接。

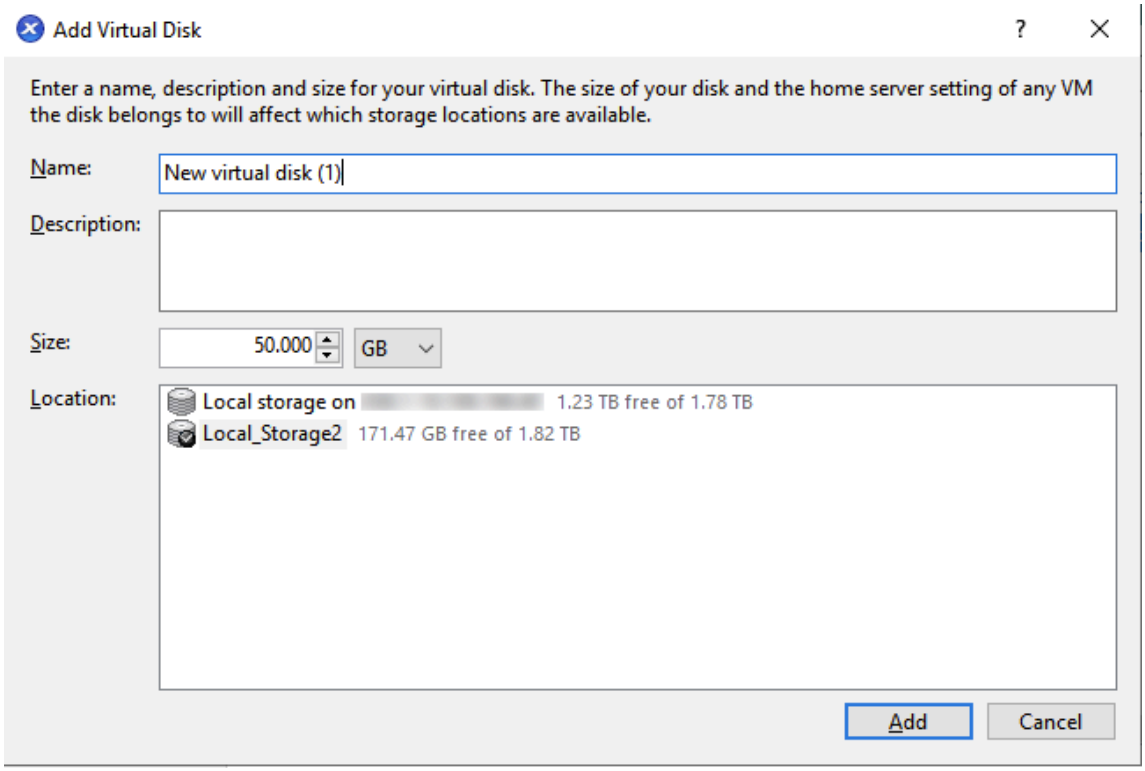
在 **Citrix Hypervisor** 上添加新磁盘

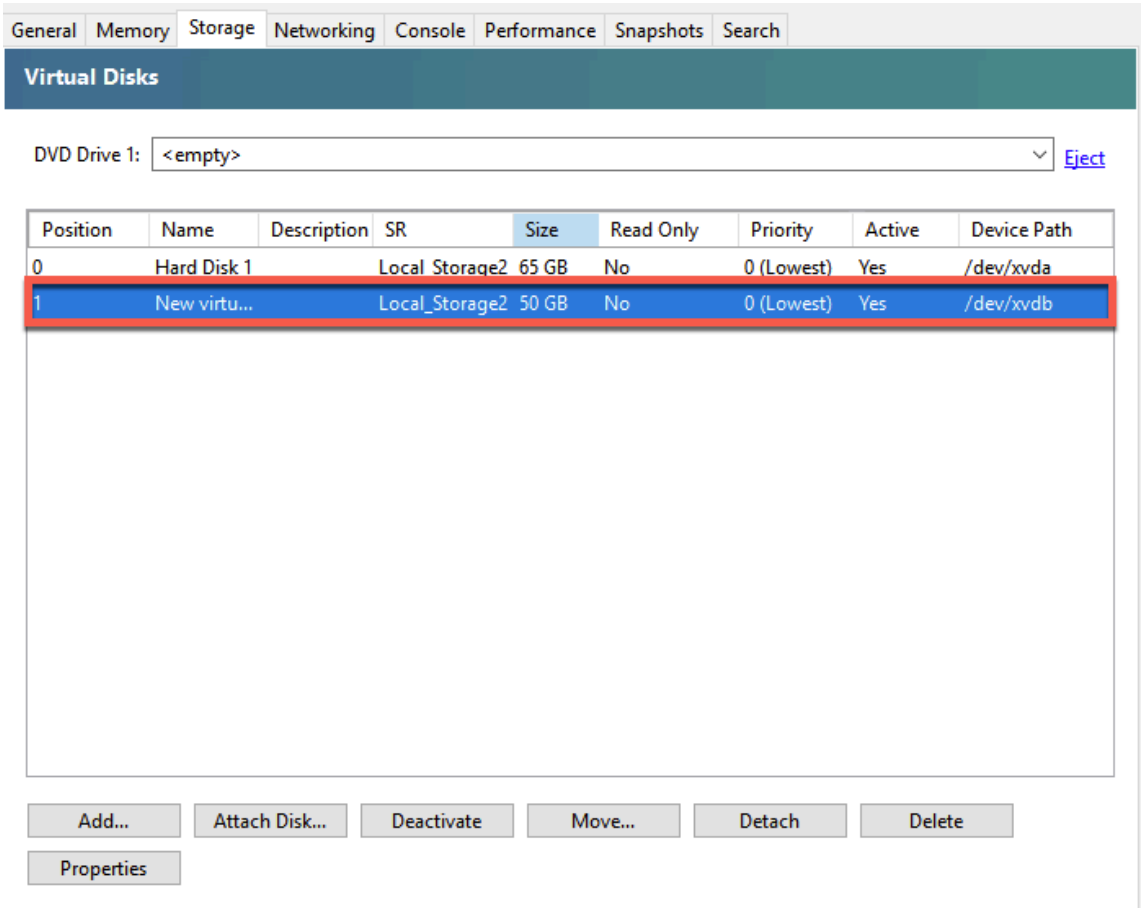
1. 从虚拟机管理程序中选择虚拟机 (VM)。选择“存储”选项卡，然后单击“添加”。



2. 提供详细信息，例如新磁盘的名称、描述、大小和位置。单击添加。新添加的磁盘将列在“存储”选项卡下。

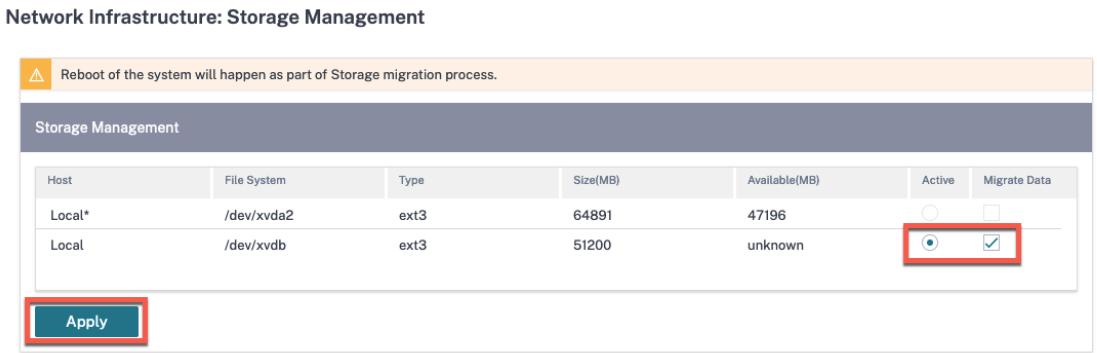
> 注意
>
> 磁盘大小必须至少是本地的 Citrix SD-WAN Orchestrator 消耗的当前数据的两倍。



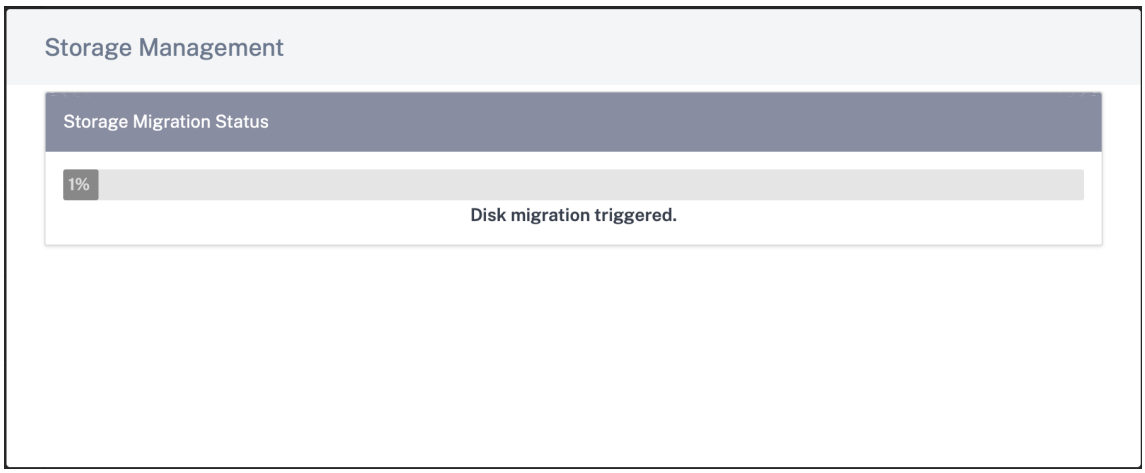


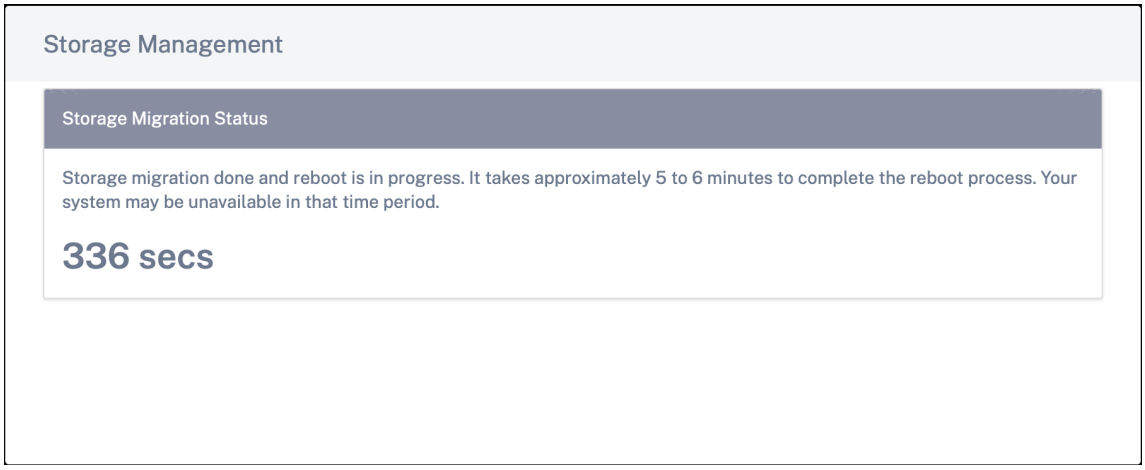
3. 登录本地用户界面的 Citrix SD-WAN Orchestrator，然后导航到 基础架构 **> Orchestrator** 管理 **>** 存储管理。新连接的磁盘会自动列在“存储管理”下。

4. 选择“活动”单选按钮，然后选中“迁移数据”复选框。单击应用。



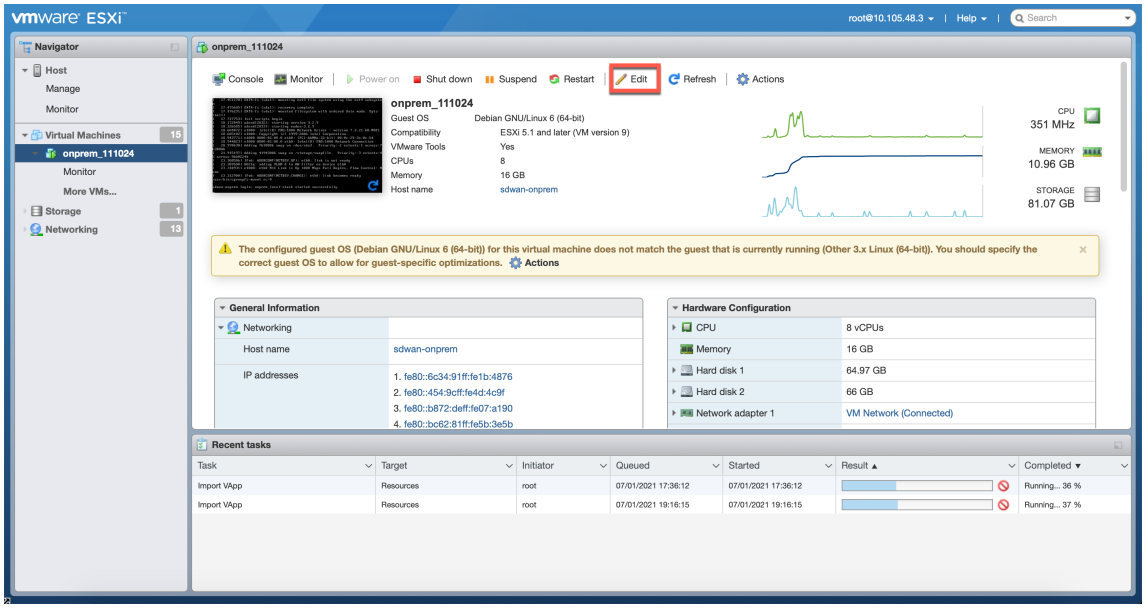
5. 磁盘迁移过程被触发。现有磁盘上的客户配置、统计信息、本地数据库和 Citrix SD-WAN 发行版本将迁移到新磁盘。迁移完成后，适用于本地的 Citrix SD-WAN Orchestrator 将重新启动。



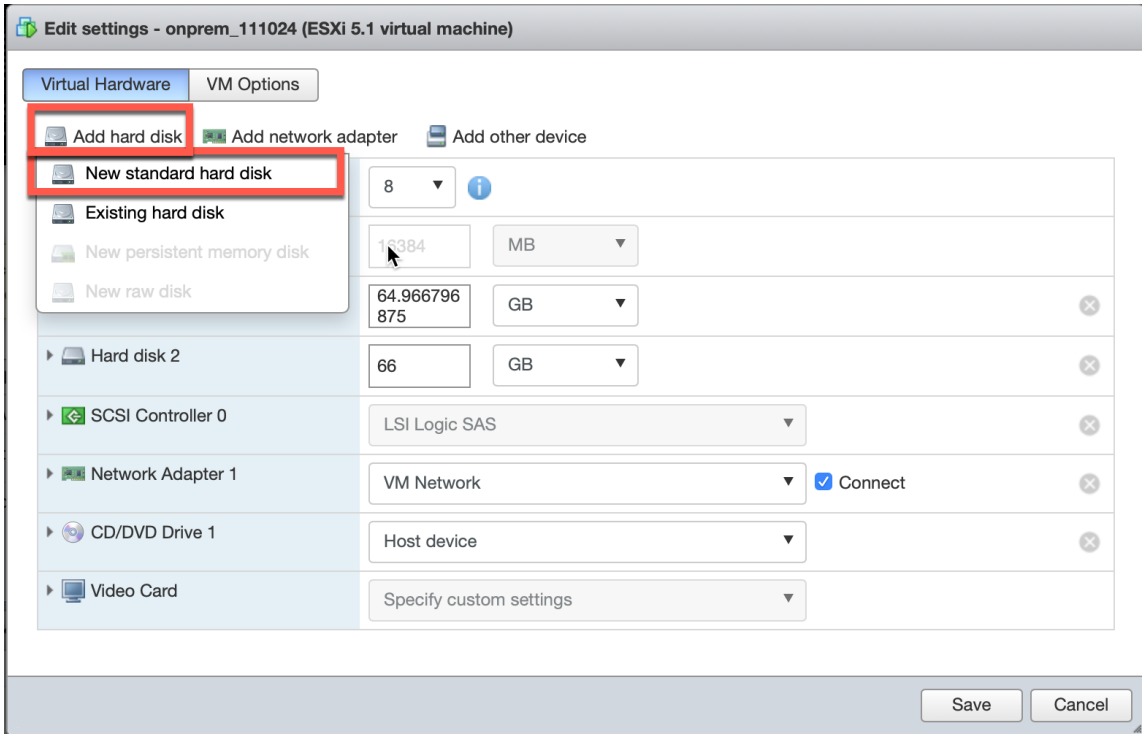


在 **ESXi** 服务器上添加新磁盘

1. 登录到您的 ESXi 服务器并选择虚拟机。单击编辑。

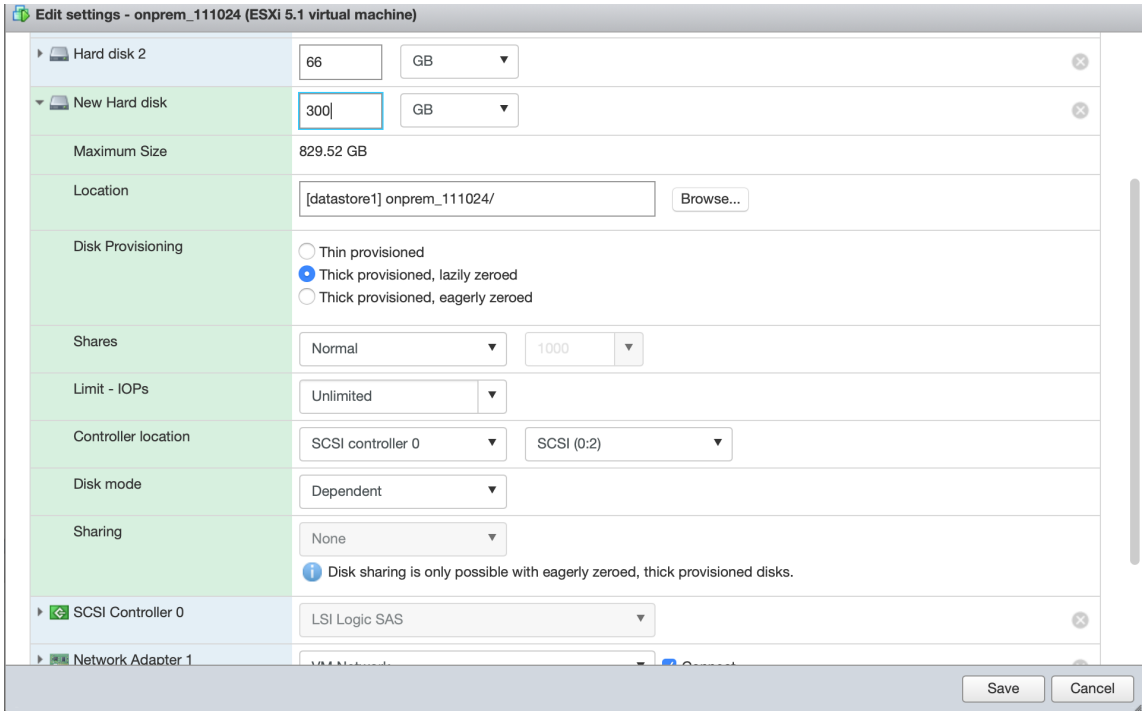


2. 单击“添加硬盘”**>**“新建标准硬盘”。

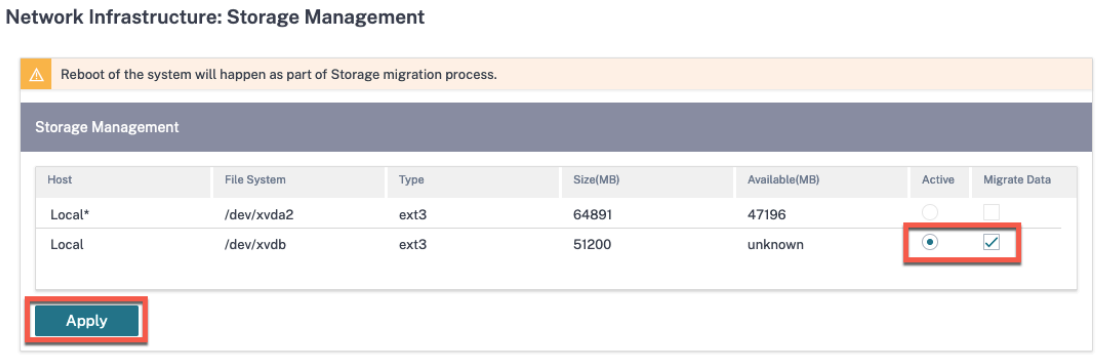


3. 根据您的喜好输入磁盘存储空间和其他设置。单击保存。

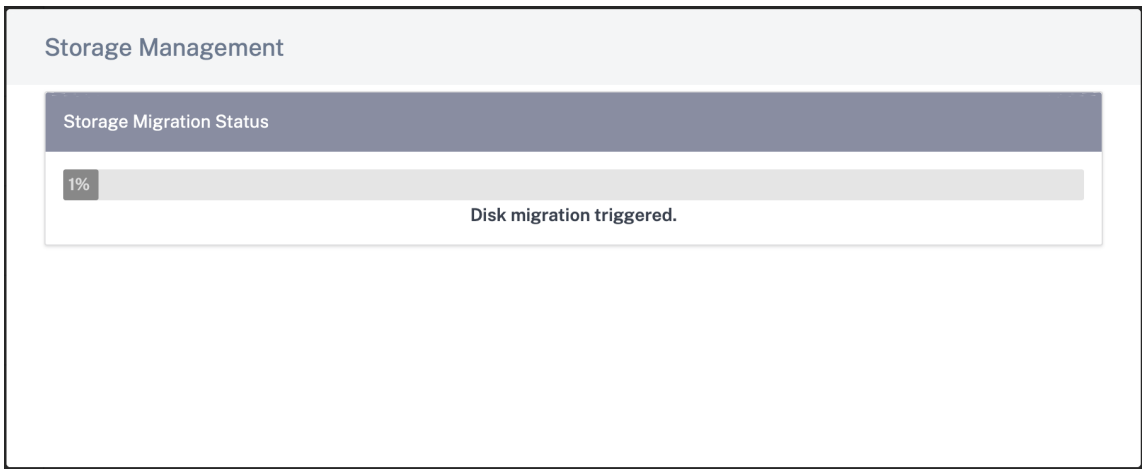
> 注意
>
> 磁盘大小必须至少是本地的 Citrix SD-WAN Orchestrator 消耗的当前数据的两倍。

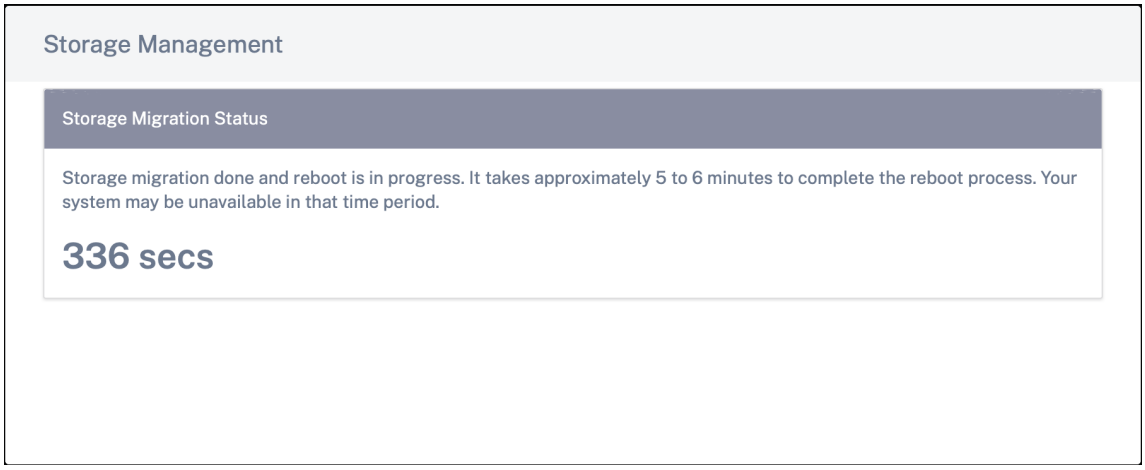


4. 登录本地的 Citrix SD-WAN Orchestrator，然后导航到 基础架构 **> Orchestrator** 管理 **>** 存储管理。此处列出了新连接的磁盘。
5. 选择“活动”单选按钮，然后选中“迁移数据”复选框。单击应用。



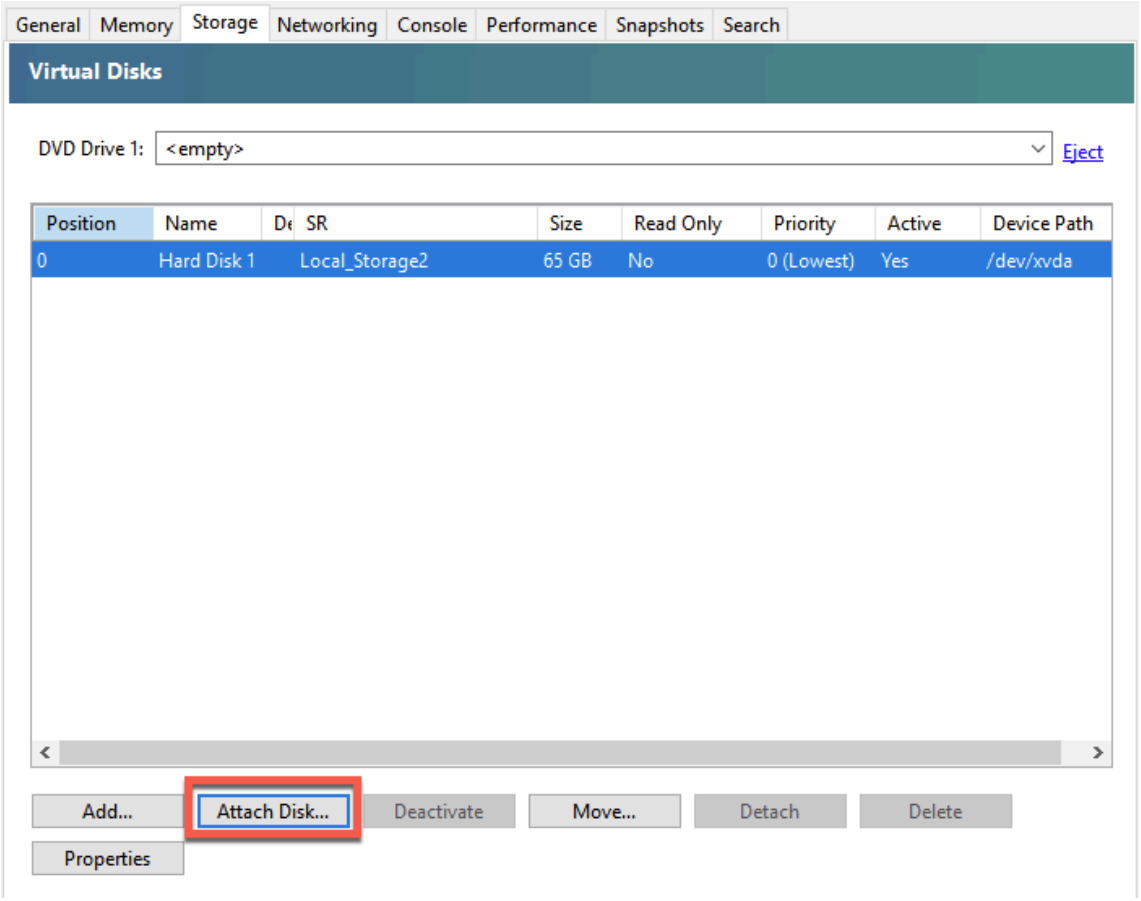
6. 磁盘迁移过程被触发。现有磁盘上的客户配置、本地数据库、Citrix SD-WAN 发行版本和数据库统计信息将迁移到新磁盘。迁移完成后，适用于本地的 Citrix SD-WAN Orchestrator 将重新启动。





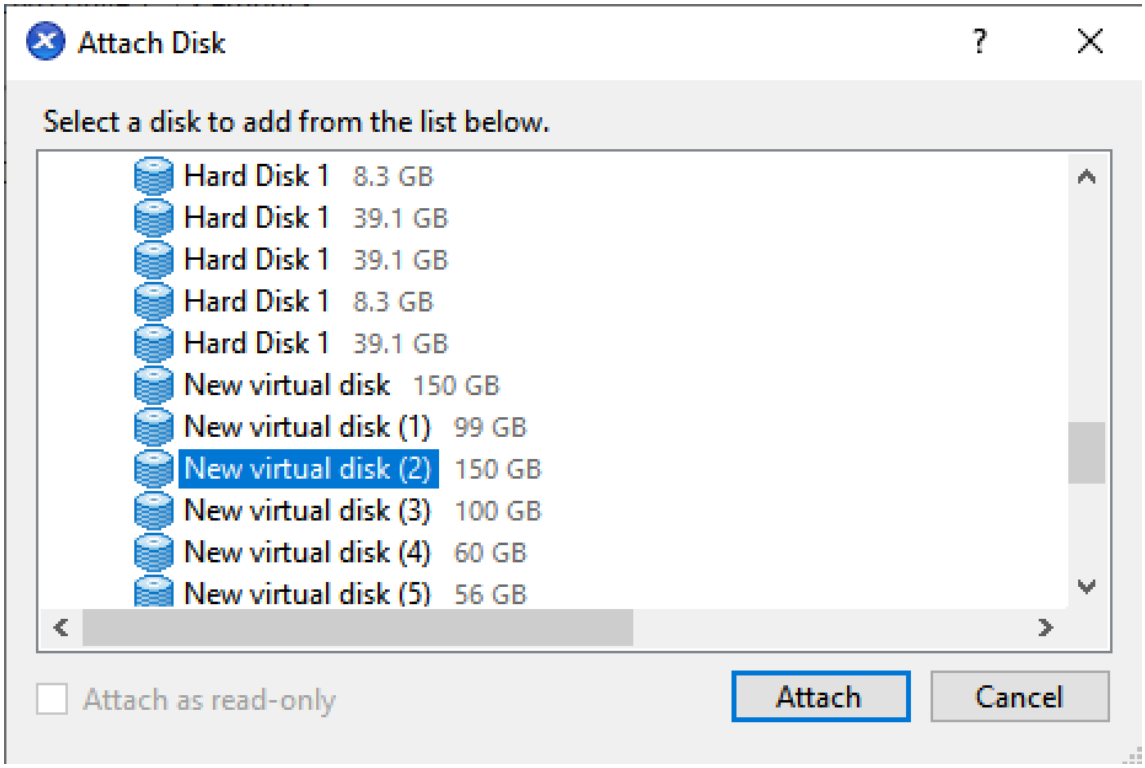
Citrix Hypervisor 上的灾难恢复

1. 从虚拟机管理程序中选择虚拟机 (VM)。选择“存储”选项卡，然后单击“连接磁盘”。



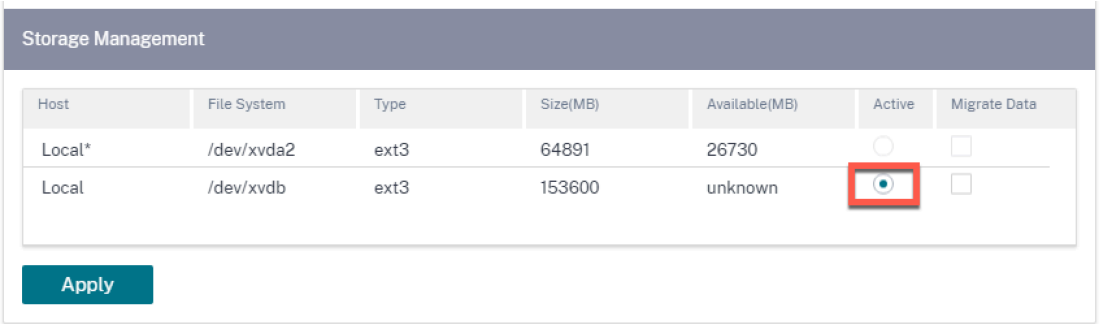
2. 选择连接到 Citrix SD-WAN Orchestrator for Inclouse 的、发生灾难的磁盘，然后单击“附加”。

   如果磁盘未列出，请确保连接到 Citrix SD-WAN Orchestrator for Inclouse 但发生灾难的磁盘已分离，并且本地的 Citrix SD-WAN Orchestrator 处于关闭状态。

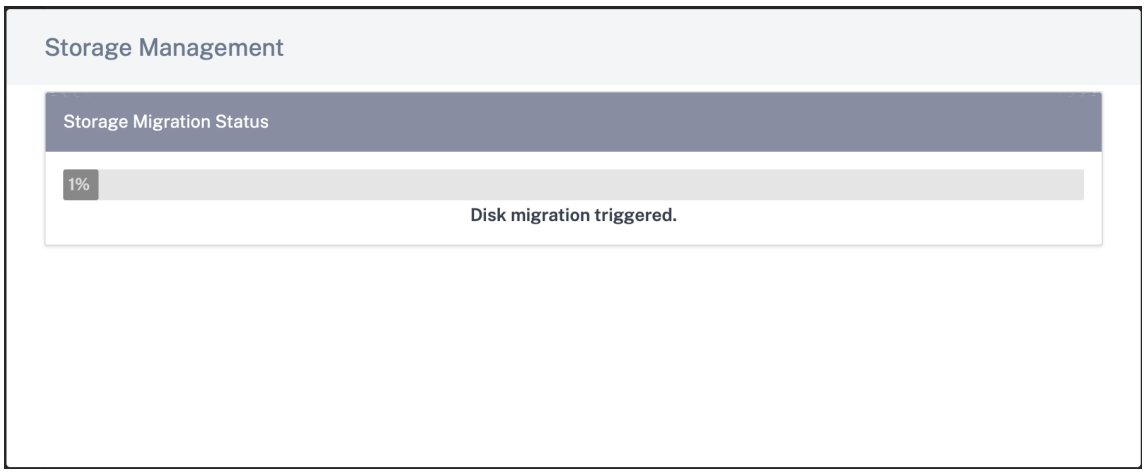


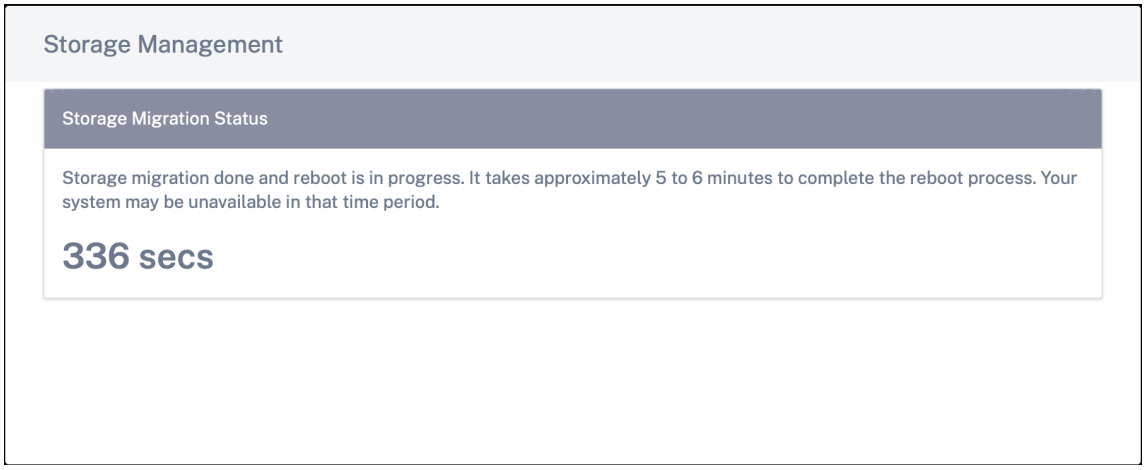
3. 登录本地用户界面的 Citrix SD-WAN Orchestrator，然后导航到 基础架构 **> Orchestrator** 管理 **>** 存储管理。此处列出了新连接的磁盘。
4. 仅选择“活动”单选按钮（如果选中，则清除“迁移数据”复选框），然后单击“应用”。

> 注意
>
> 不要选中“迁移数据”复选框。适用于本地的 Citrix SD-WAN Orchestrator 会在后端触发迁移，并在迁移完成后自行重启。



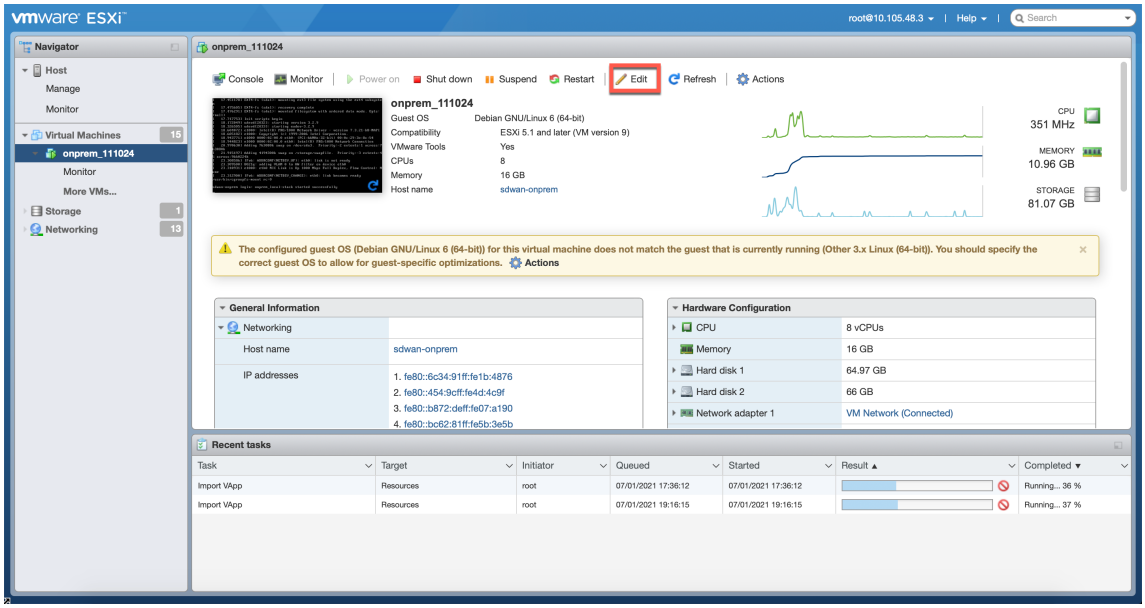
5. 迁移完成后，适用于本地的 Citrix SD-WAN Orchestrator 将重新启动。



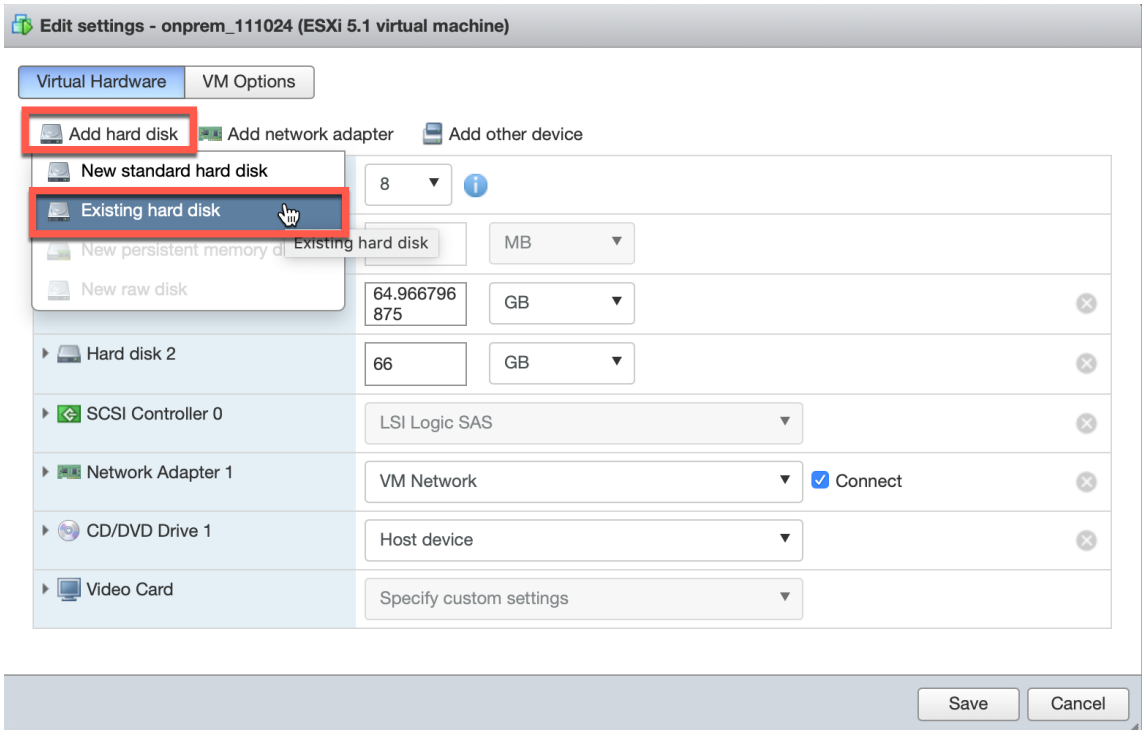


ESXi 服务器上的灾难恢复

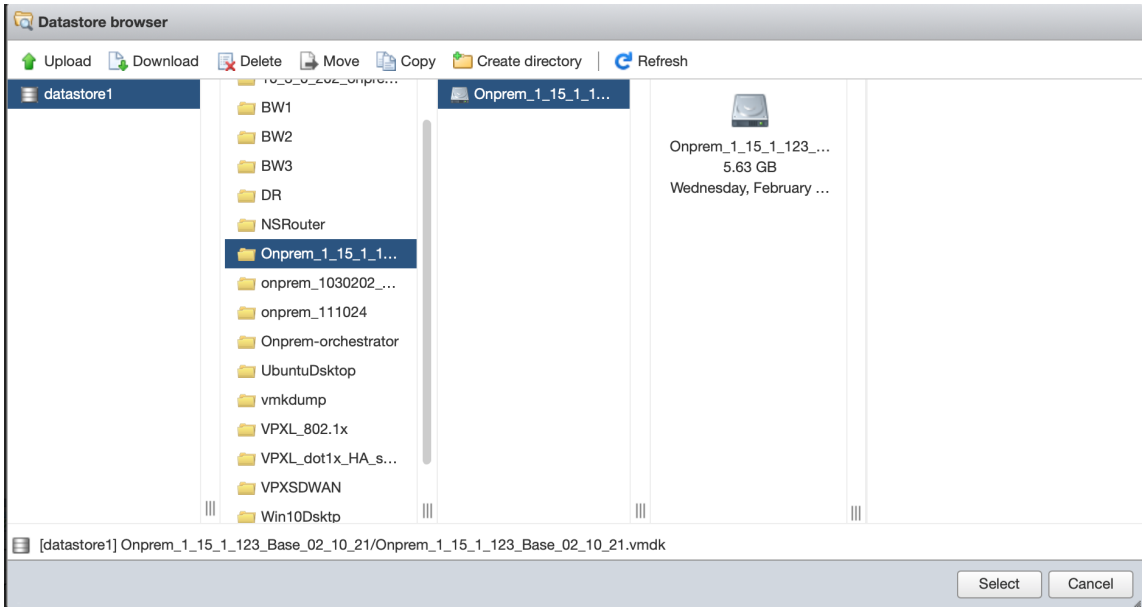
1. 登录 ESXi 服务器并选择虚拟机。单击编辑。



2. 单击“添加硬盘”**>** “现有硬盘”。

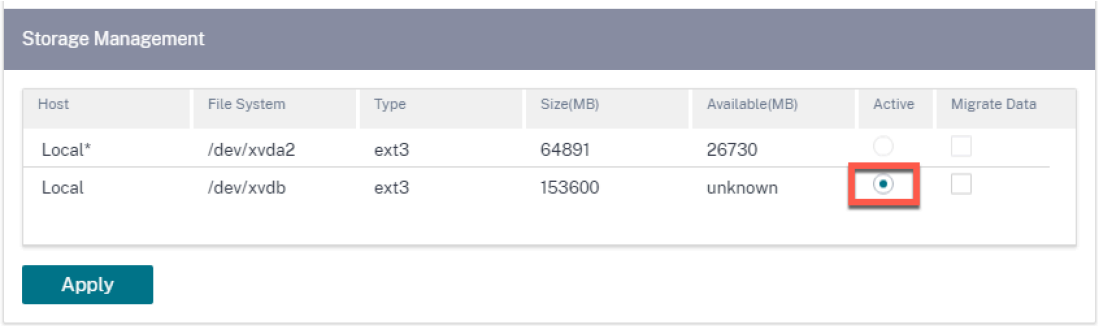


3. 浏览连接到 Citrix SD-WAN Orchestrator for Inclouse 的、发生灾难的磁盘，然后单击“选择”。

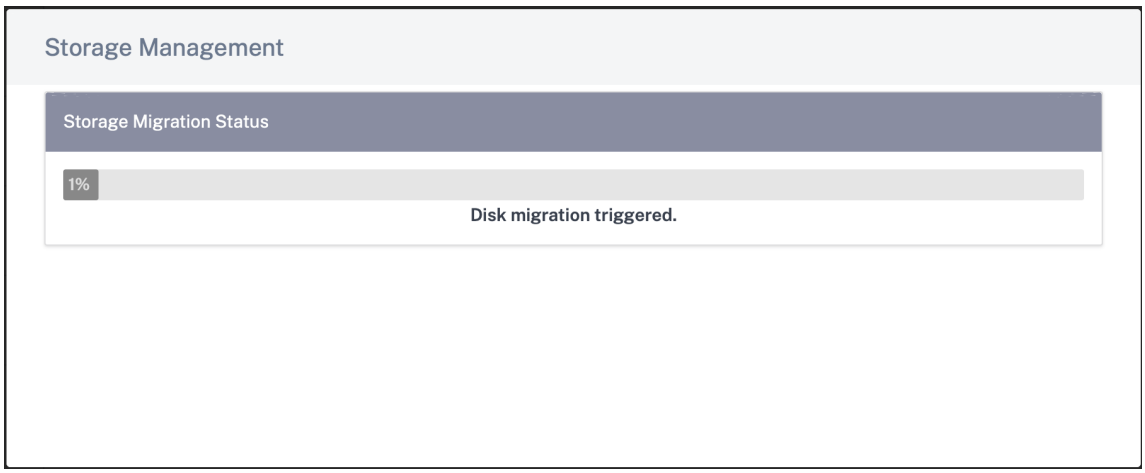


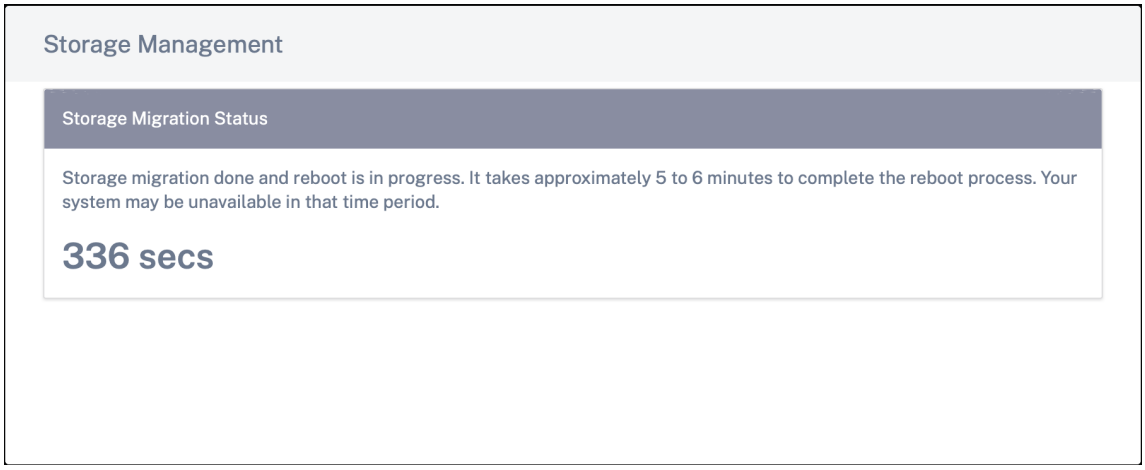
4. 登录本地用户界面的 Citrix SD-WAN Orchestrator，然后导航到 基础架构 **> Orchestrator** 管理 **>** 存储管理。此处列出了新连接的磁盘。
5. 仅选择“活动”单选按钮（如果选中，则清除“迁移数据”复选框），然后单击“应用”。

> 注意
>
> 不要选中“迁移数据”复选框。适用于本地的 Citrix SD-WAN Orchestrator 会在后端触发迁移，并在迁移完成后自行重启。



6. 迁移完成后，适用于本地的 Citrix SD-WAN Orchestrator 将重新启动。





HTTP 代理

适用于本地的 Citrix SD-WAN Orchestrator 需要互联网连接才能获得许可、云登录、云代理 ZTD、Cloud direct 和发布软件。如果 Citrix SD-WAN Orchestrator for Inclouse 通过 HTTP 代理服务器连接到互联网，则可以在 Citrix SD-WAN Orchestrator 上为本地虚拟机配置 HTTP 代理服务器设置。

HTTP 代理设置集中管理向 Citrix Cloud 发出的所有传出请求。管理员可以通过 HTTP 代理服务器将来自本地的 Citrix SD-WAN Orchestrator 的传出请求路由到 Citrix Cloud。

开始之前的准备工作

要首次使用 HTTP 代理进行云登录，必须通过 Citrix SD-WAN Orchestrator 的 CLI 控制台配置 HTTP 代理设置。

在适用于本地虚拟机的新 Citrix SD-WAN Orchestrator 的云登录页面上，如果您想将 HTTP 代理用于从本地部署的 Citrix SD-WAN Orchestrator 到 Citrix SD-WAN Orchestrator 服务的所有出站连接，则必须使用 CLI 配置 HTTP 代理详细信息。Cloud 登录完成并访问配置页面后，即可在 UI 上配置 HTTP 代理服务器的详细信息。

在 **CLI** 上配置 **HTTP** 代理服务器设置

通过运行 `set_http_proxy` 命令配置 HTTP 代理设置。您可以使用下面提供的任一选项配置 HTTP 代理：

- 在代理服务器上启用身份验证时：

  ```
  set <ip address> <port> <user name> <password>
  ```

- 在代理服务器上未启用身份验证时：

  ```
  set <ip address> <port>
  ```

显示 **HTTP** 代理服务器设置

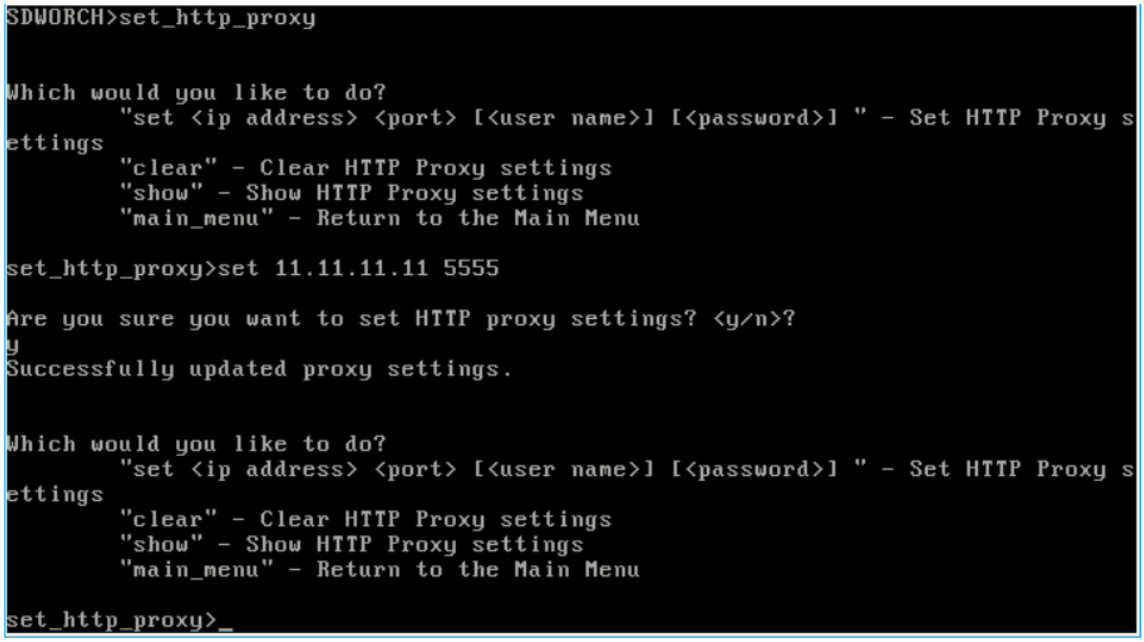
- `show`：此命令在 CLI 上显示代理设置。输出不显示密码。

清除 **HTTP** 代理设置

- `clear`：此命令删除 HTTP 代理设置。

返回主菜单

- `main_menu`：此命令将你重定向到本地版 Citrix SD-WAN Orchestrator 的 CLI 控制台。



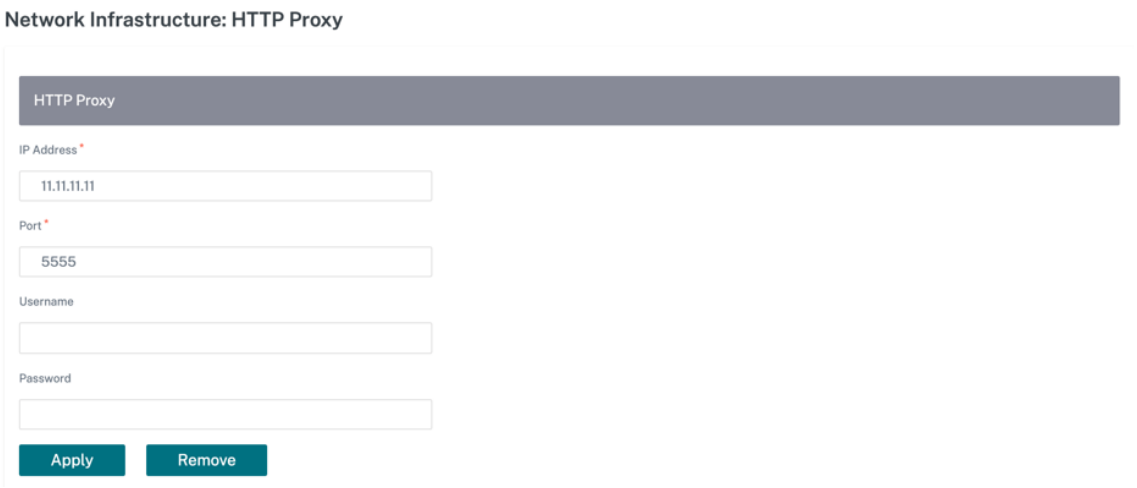
在 **UI** 上配置 **HTTP** 代理服务器设置

1. 登录本地用户界面的 Citrix SD-WAN Orchestrator，然后导航到 基础架构 > **Orchestrator** 管理 > **HTTP** 代理。

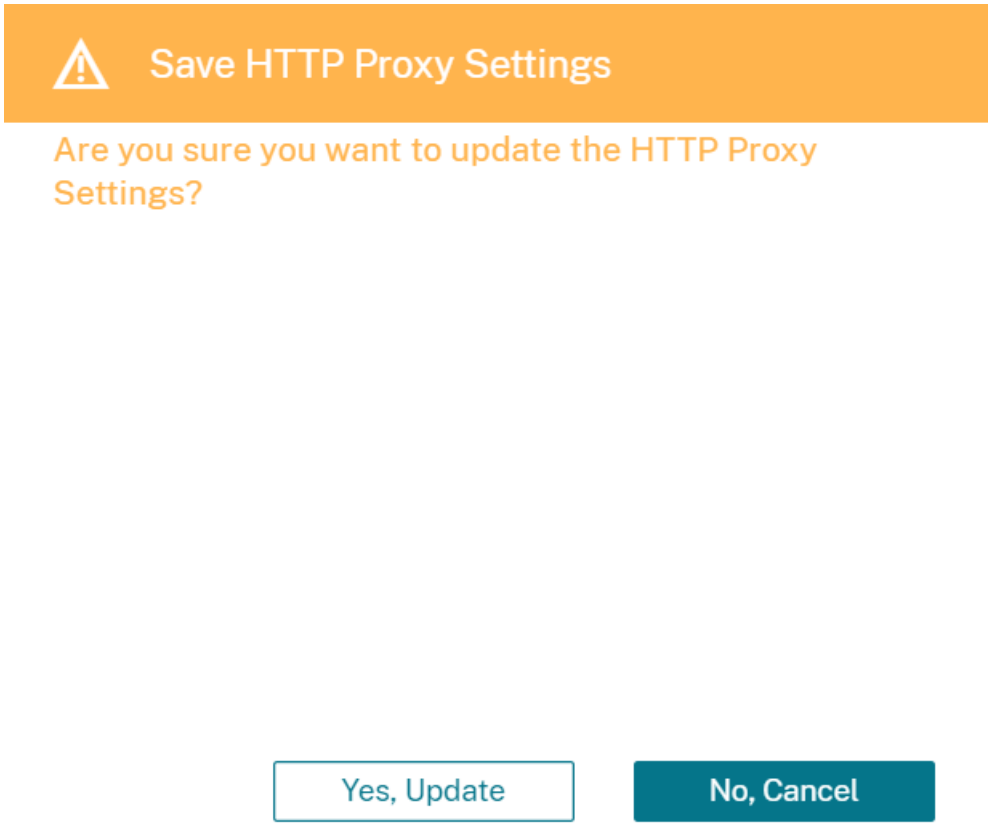
2. 在“网络基础架构：**HTTP** 代理”部分中，输入以下字段的值：

   - **IP** 地址：代理服务器的 IP 地址。
   - 端口：代理服务器接受连接的网络端口号。
   - 用户名：代理服务器的用户名。
   - 密码：代理服务器的密码。

   > 注意
   >
   > 如果代理服务器上未配置身份验证，则可以将用户名和密码字段留空。



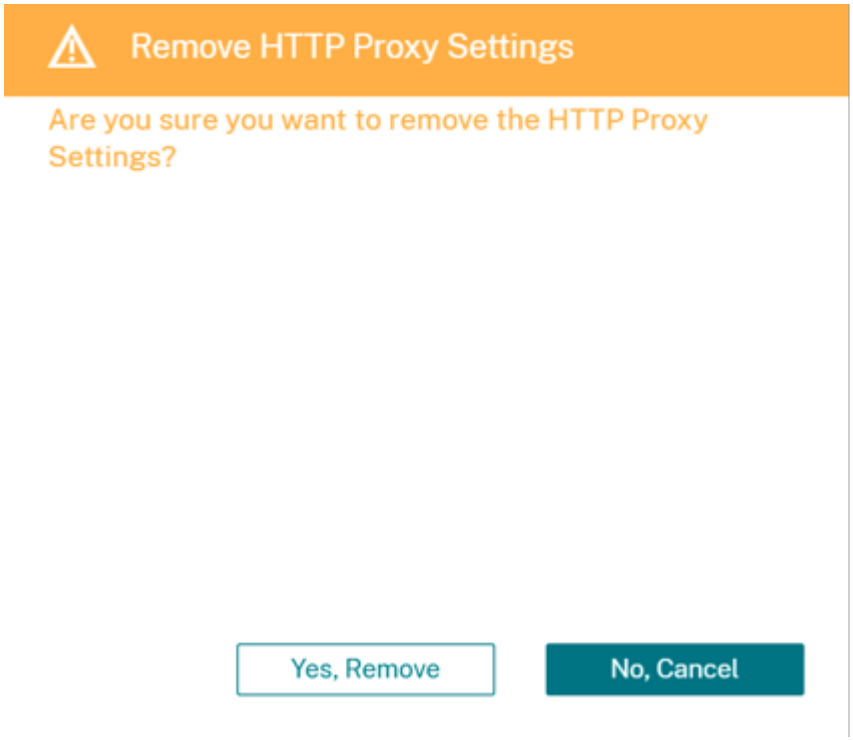
3. 单击应用。此时将显示确认对话框。
4. 单击 是，更新。



> 备注
>
> - 要使用 HTTP 代理服务器处理从本地的 Citrix SD-WAN Orchestrator 到 Citrix Cloud 的出站流量，必须将代理服务器配置为透明 SSL HTTP 代理或 SSL 绕过 HTTP 代理服务器。服务器不得欺骗 Citrix SD-WAN Orchestrator 服务的 SSL 证书。
> - 如果 Citrix SD-WAN Orchestrator for Inclouse 直接连接到互联网，则可以完全删除代理服务器设置。如有必要，您还可以删除代理服务器设置并配置其他代理服务器。

移除 **UI** 上的代理服务器设置

1. 在适用于本地用户界面的 Citrix SD-WAN Orchestrator 中，导航到 基础架构 > **Orchestrator** 管理 > **HTTP** 代理。
2. 在“网络基础架构：**HTTP** 代理”部分中，单击“删除”。此时将显示确认对话框。
3. 单击“是，删除”。



清除设置

您可以清除所选时间间隔内的历史统计数据/数据。早于设定日期的统计数据/数据将被清除。数据一经清除，便不再可用。默认情况下，适用于本地的 Citrix SD-WAN Orchestrator 会清除 30 天之前的历史统计数据/数据。

在网络级别，导航到 基础架构 > **Orchestrator** 管理 > 清除设置，选择时间间隔，然后单击“应用”。例如，如果要清除 180 天之前的历史统计数据/数据，请从“清除统计间隔（天）”下拉列表中选择 180，然后单击“应用”。清除过程在每天凌晨 12:48 左右在 SD-WAN 设备上设置的时区进行。

管弦乐器诊断

October 21, 2022

本节提供有关可以在适用于本地基础架构的 Citrix SD-WAN Orchestrator 上执行的诊断活动的信息。

> 注意
>
> 在提供商托管设置中，提供商管理员可以访问所有 GUI 页面 基础架构 **> Orchestrator** 诊断。客户管理员只能查看 平台事件和日志以及平台运行状况 GUI 页面。

平台事件和日志

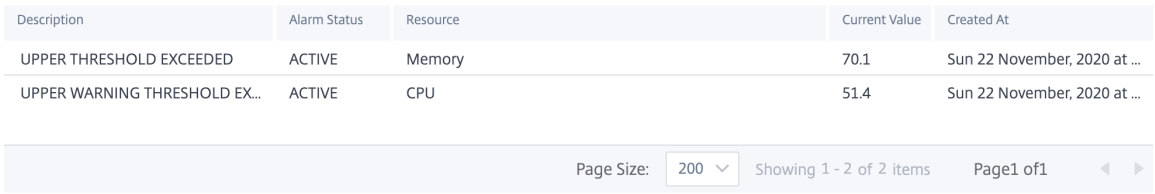
平台级属性（例如系统中的 CPU、内存或存储）的任何更改都将记录为事件并显示在 Citrix SD-WAN Orchestrator for Inclouse for Inclouse 上。

例如，如果 CPU 使用率超过设定的限制，则会记录平台事件并触发警报。警报出现在通知栏中。如果 CPU 使用率降低，则通知将被清除。平台事件和日志 页面维护已触发的所有平台相关警报的历史记录。如果 CPU 使用率降低，则警报状态变为“非活动”。如果仍高于限制，则警报状态将保持活动状态。

要查看平台事件，请导航到 基础架构 > **Orchestrator** 诊断 > 平台事件和日志。

显示了记录的平台事件的以下详细信息：

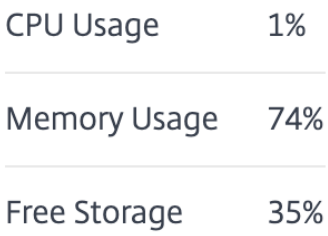
- 描述：平台事件的描述。
- 警报状态：警报的状态。如果平台属性超过设置的限制，则状态为 ACTIVE。如果平台级别属性降至设定限制内的某个值，则警报状态为 INACTIVE。
- 资源：平台级别的属性—CPU、内存或存储。
- 当前值：记录的平台属性的最新值。
- 创建时间：平台事件发生的时间。



平台运行状况

您可以查看适用于本地平台的 Citrix SD-WAN Orchestrator 的运行状况。运行状况信息包括 CPU 使用率、内存使用率和可用存储空间的实时值（百分比）。

要查看平台运行状况，请导航到 基础架构 **> Orchestrator** 诊断 **>** 平台运行状况。

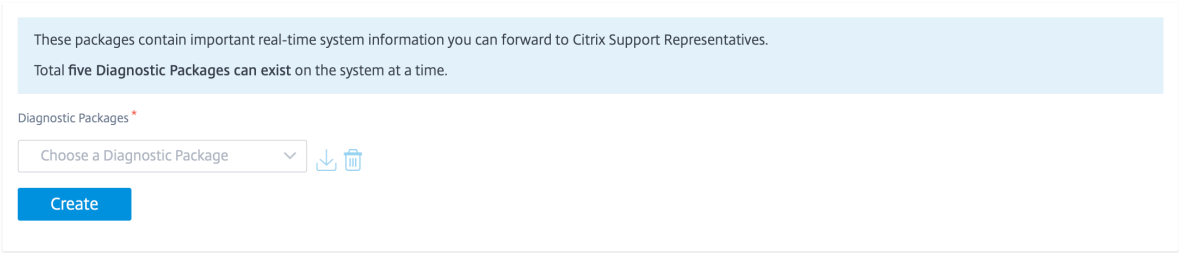


诊断信息

诊断包由系统日志文件、系统信息和其他必要细节组成，可帮助支持团队诊断和解决系统问题。

要创建诊断包，请导航到 基础架构 > **Orchestrator** 诊断 > 诊断信息。单击创建。创建软件包后，您可以将其下载到您的计算机上，然后与支持团队共享。

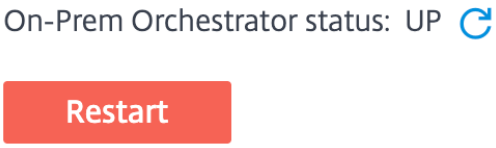
> 注意：
>
> 适用于本地的 Citrix SD-WAN Orchestrator 一次最多可以存储五个诊断包。



重启适用于本地应用程序的 **Citrix SD-WAN Orchestrator**

无需重新启动操作系统 (OS)，您只能重新启动 Citrix SD-WAN Orchestrator for 本地应用程序。在重启期间，适用于本地的 Citrix SD-WAN Orchestrator 应用程序脱机，所有服务都变得不可用。重启大约需要 6 分钟才能完成。重启后，将显示适用于本地的 Citrix SD-WAN Orchestrator 登录页面。

要重启适用于本地的 Citrix SD-WAN Orchestrator 应用程序，请导航到 基础架构 **> Orchestrator** 诊断 **>** 重启 **Orchestrator** 应用程序单击“重新启动”和“是，重新启动”进行确认。

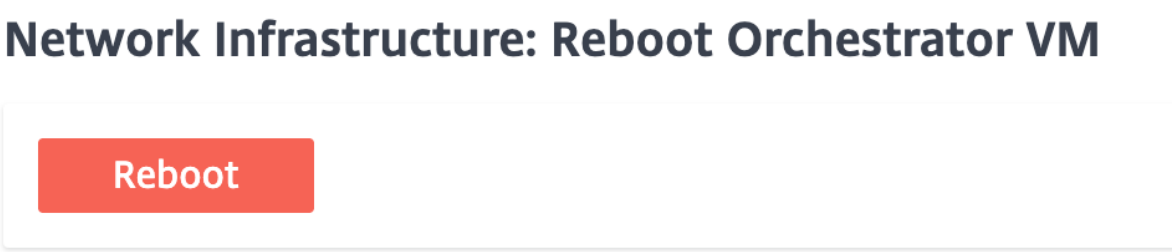


为本地虚拟机重启 **Citrix SD-WAN Orchestrator**

重启过程会重新启动 Citrix SD-WAN Orchestrator 的本地操作系统 (OS)。在重启期间，适用于本地的 Citrix SD-WAN Orchestrator 脱机，所有服务都变得不可用。重启大约需要 6 到 8 分钟才能完成。重启后，将显示适用于本地的 Citrix SD-WAN Orchestrator 登录页面。

作为故障排除活动的一部分或在维护活动期间，您可以重新启动适用于本地的 Citrix SD-WAN Orchestrator。

要重启，请导航到 基础架构 **> Orchestrator** 诊断 **>** 重启 **Orchestrator** 虚拟机。单击“重新启动”和“是，重新启动”进行确认。



警报

October 21, 2022

您可以查看与 Citrix SD-WAN Orchestrator 本地部署相关的平台特定警报和服务特定警报。平台特定警报显示与平台相关的警报，例如存储问题、RAM、CPU。服务警报显示本地版 Citrix SD-WAN Orchestrator 中运行的微服务的状态。

要 查看警报，请单击 Citrix SD-WAN Orchestrator 本地用户界面右上角的钟形图标，然后根据需要选择 平台警报或服务警报。