Citrix Gateway 13.0

Machine translated content

Disclaimer

Contents

Citrix Gateway 发行说明

April 6, 2020

发行说明描述了软件在特定版本中如何更改，以及该版本中已知存在的问题。

发行说明文档包括以下所有或部分部分：

- 新增功能：版本中发布的增强功能和其他更改。
- 已修复的问题：生成中修复的问题。
- 已知问题：生成中存在的问题。
- 注意事项：使用构建时要记住的重要方面。
- 限制：构建中存在的限制。

> 注意
>
> - 问题描述下的 [# XXXXXX] 标签是 Citrix ADC 团队使用的内部跟踪 ID。
> - 这些发行说明不记录与安全相关的修补程序。有关与安全相关的修补程序和通知的列表，请参阅 Citrix 安全公告。

要查看最新的发行说明文档，请参阅发行说明页面。

关于 Citrix Gateway

April 6, 2020

Citrix Gateway 易于部署且易于管理。最典型的部署配置是在 DMZ 中找到 Citrix Gateway 设备。您可以在网络中安装多个 Citrix Gateway 设备以进行更复杂的部署。

首次启动 Citrix Gateway 时，您可以使用串行控制台、配置实用程序中的安装向导或动态主机配置协议 (DHCP) 来执行初始配置。在 MPX 设备上，您可以使用设备前面板上的 LCD 键盘执行初始配置。您可以配置特定于内部网络的基本设置，例如 IP 地址、子网掩码、默认网关 IP 地址和域名系统 (DNS) 地址。配置基本网络设置后，您可以配置特定于 Citrix Gateway 操作的设置，例如身份验证、授权、网络资源、虚拟服务器、会话策略和终端节点策略的选项。

在安装和配置 Citrix Gateway 之前，请查看本节中的主题，了解有关规划部署的信息。部署规划可包括确定设备的安装位置、了解如何在 DMZ 中安装多台设备以及许可要求。您可以在任何网络基础结构中安装 Citrix Gateway，而无需更改安全网络中运行的现有硬件或软件。Citrix Gateway 可与其他网络产品（如服务器负载均衡器、缓存引擎、防火墙、路由器和 IEEE 802.11 无线设备）配合使用。

您可以在配置 Citrix Gateway 之前在安装前清单中写入您的设置。

Citrix Gateway 设备	提供有关 Citrix Gateway 设备和设备安装说明的信息。
安装前清单	提供要查看的规划信息以及在网络中安装 Citrix Gateway 之前要完成的任务列表。
常见部署	提供有关在网络 DMZ、在没有 DMZ 的安全网络中部署 Citrix Gateway 以及使用其他设备支持负载平衡和故障转移的信息。还提供有关使用 Citrix Virtual Apps and Desktops 部署 Citrix Gateway 的信息。
Licensing	提供有关在设备上安装许可证的信息。还提供有关在多个 Citrix Gateway 设备上安装许可证的信息。

Citrix Gateway 体系结构

April 6, 2020

Citrix Gateway 的核心组件是：

- 虚拟服务器。Citrix Gateway 虚拟服务器是代表用户可用的所有已配置服务的内部实体。虚拟服务器也是用户访问这些服务的访问点。您可以在单个设备上配置多个虚拟服务器，从而允许一个 Citrix Gateway 设备为具有不同身份验证和资源访问要求的多个用户社区提供服务。
- 身份验证、授权和会计。您可以配置身份验证、授权和记帐，以允许用户使用 Citrix Gateway 或位于安全网络中的身份验证服务器（例如 LDAP 或 RADIUS）识别的凭据登录 Citrix Gateway。授权策略定义用户权限，确定给定用户有权访问哪些资源。有关身份验证和授权的更多信息，请参阅配置身份验证和授权。会计服务器维护有关 Citrix Gateway 活动的数据，包括用户登录事件、资源访问实例和操作错误。此信息存储在 Citrix Gateway 或外部服务器上。有关会计的详细信息，请参阅在 Citrix Gateway 上配置审核
- 用户连接。用户可以使用以下访问方法登录 Citrix Gateway：
  - 适用于 Windows 的 Citrix Gateway 插件是安装在基于 Windows 的计算机上的软件。用户通过右键单击基于 Windows 的计算机上的通知区域中的图标登录。如果用户正在使用未安装 Citrix Gateway 插件的计算机，则可以使用 Web 浏览器登录下载并安装该插件。如果用户安装了 Citrix Workspace 应用程序，则用户将通过 Citrix Gateway 插件从 Citrix Workspace 应用程序登录。在用户设备上安装 Citrix Workspace 应用程序和 Citrix Gateway 插件时，Citrix Workspace 应用程序会自动添加 Citrix Gateway 插件。
  - 适用于 Mac OS X 的 Citrix Gateway 插件，允许运行 Mac OS X 的用户登录。它具有与适用于 Windows 的 Citrix Gateway 插件相同的功能和功能。您可以通过安装 Citrix ADC 加特威 10.1，构建 120.1316.e，为此插件版本提供端点分析支持。

  - 适用于 Java 的 Citrix Gateway 插件，使 Mac OS X、Linux 和 Windows 用户可以使用 Web 浏览器登录。
  - Citrix Workspace 应用程序，该应用程序允许用户使用 Web Interface 或 Citrix StoreFront 连接到服务器场中的已发布应用程序和虚拟桌面。
  - Citrix Workspace 应用程序、Secure Hub、WorxMail 和 WorxWeb，允许用户访问 Web 和 SaaS 应用程序、iOS 和 Android 移动应用程序以及 Citrix Endpoint Management 中托管的 ShareFile 数据。
  - 用户可以从使用 Citrix Gateway Web 地址的 Android 设备进行连接。当用户启动应用程序时，连接使用 Micro VPN 将网络流量路由到内部网络。如果用户从 Android 设备连接，则必须在 Citrix Gateway 上配置 DNS 设置。有关详细信息，请参阅通过对 Android 设备使用 DNS 后缀支持 DNS 查询。
  - 用户可以从使用 Citrix Gateway Web 地址的 iOS 设备进行连接。您可以在全局或会话配置文件中配置安全浏览。当用户在其 iOS 设备上启动应用程序时，VPN 连接将启动，连接将通过 Citrix Gateway 进行路由。
  - 无客户端访问，为用户提供他们所需的访问权限，而无需在用户设备上安装软件。

    配置 Citrix Gateway 时，您可以创建策略来配置用户登录方式。您还可以通过创建会话和终端节点分析策略来限制用户登录。

- 网络资源。这些服务包括用户通过 Citrix Gateway 访问的所有网络服务，例如文件服务器、应用程序和网站。
- 虚拟适配器。Citrix Gateway 虚拟适配器为需要 IP 欺骗的应用程序提供支持。安装 Citrix Gateway 插件时，虚拟适配器将安装在用户设备上。用户连接到内部网络时，Citrix Gateway 与内部服务器之间的出站连接将使用 Intranet IP 地址作为源 IP 地址。Citrix Gateway 插件作为配置的一部分从服务器接收此 IP 地址。

  如果在 Citrix Gateway 上启用拆分隧道，则所有 Intranet 流量都会通过虚拟适配器路由。拦截 Intranet 绑定的流量时，虚拟适配器会拦截 A 和 AAAA 记录类型的 DNS 查询，同时保持所有其他 DNS 查询不变。未绑定到内部网络的网络流量将通过安装在用户设备上的网络适配器路由。因特网和专用局域网连接保持开放和连接。如果禁用分割隧道，则所有连接都将通过虚拟适配器路由。任何现有连接都会断开连接，用户需要重新建立会话。

  如果配置 Intranet IP 地址，则通过虚拟适配器使用 Intranet IP 地址欺骗到内部网络的流量。

用户连接的工作原理

April 6, 2020

用户可以从远程位置连接到他们的电子邮件、文件共享和其他网络资源。用户可以使用以下软件连接到内部网络资源：

- Citrix Gateway 插件
- Citrix Workspace 应用程序
- WorxMail 和 WorxWeb
- Android 和 iOS 移动设备

使用 **Citrix Gateway** 插件进行连接

Citrix Gateway 插件允许用户通过以下步骤访问内部网络中的资源：

1. 用户通过在 Web 浏览器中键入 Web 地址来首次连接 Citrix Gateway。此时将显示登录页面，并提示用户输入用户名和密码。如果配置了外部身份验证服务器，Citrix Gateway 将联系服务器，身份验证服务器将验证用户的凭据。如果配置了本地身份验证，Citrix Gateway 将执行用户身份验证。
2. 如果配置预身份验证策略，当用户在基于 Windows 的计算机或 Mac OS X 计算机的 Web 浏览器中键入 Citrix Gateway Web 地址时，Citrix Gateway 会在显示登录页之前检查是否已实施任何基于客户端的安全策略。安全检查验证用户设备是否满足与安全相关的条件，例如操作系统更新、防病毒防护和正确配置的防火墙。如果用户设备未通过安全检查，Citrix Gateway 将阻止用户登录。无法登录的用户需要下载必要的更新或软件包并将其安装在用户设备上。当用户设备通过预身份验证策略时，将显示登录页面，用户可以输入其凭据。如果您安装 Citrix Gateway 10.1 Build 120.1316.e，则可以在 Mac OS X 计算机上使用高级端点分析。
3. Citrix Gateway 成功对用户进行身份验证后，Citrix Gateway 将启动 VPN 隧道。Citrix Gateway 提示用户下载并安装适用于 Windows 的 Citrix Gateway 插件或适用于 Mac OS X 的 Citrix Gateway 插件如果您使用的是适用于 Java 的网络网关插件，则还会使用预配置的资源 IP 地址和端口号列表初始化用户设备。
4. 如果配置身份验证后扫描，则 Citrix Gateway 会在用户成功登录后扫描用户设备以获取所需的客户端安全策略。您可以要求与预身份验证策略相同的与安全相关的条件。如果用户设备扫描失败，则不会应用该策略，或者将该用户置于隔离组中，并且用户对网络资源的访问受到限制。
5. 建立会话后，用户将被定向到 Citrix Gateway 主页，用户可以在其中选择要访问的资源。Citrix Gateway 附带的主页称为访问接口。如果用户使用适用于 Windows 的 Citrix Gateway 插件登录，则 Windows 桌面上的通知区域中的图标显示用户设备已连接，并且用户会收到一条消息，指出连接已建立。用户还可以在不使用访问接口（如打开 Microsoft Outlook 和检索电子邮件）的情况下访问网络中的资源。
6. 如果用户请求通过身份验证前和身份验证后的安全检查，Citrix Gateway 随后会联系请求的资源并启动用户设备与该资源之间的安全连接。
7. 用户可以通过右键单击基于 Windows 的计算机上的通知区域中的 Citrix Gateway 图标，然后单击注销来关闭活动会话。会话也可能由于不活动而超时。当会话关闭时，隧道将关闭，并且用户无法再访问内部资源。用户还可以在浏览器中键入 Citrix Gateway Web 地址。当用户按 Enter 时，将显示访问界面，用户可以从中注销。

注意：如果在内部网络中部署 Citrix Endpoint Management，则从内部网络外部连接的用户必须先连接到 Citrix Gateway。用户建立连接后，可以访问 Web 和 SaaS 应用程序、Android 和 iOS 移动应用程序以及 Citrix Endpoint Management 上托管的 ShareFile 数据。用户可以通过无客户端访问或使用 Citrix Workspace 应用程序或 Secure Hub 连接 Citrix Gateway 插件。

与 **Citrix Workspace** 应用程序连接

用户可以连接 Citrix Workspace 应用程序以访问其基于 Windows 的应用程序和虚拟桌面。用户还可以从 Endpoint Management 访问应用程序。要从远程位置进行连接，用户还会在其设备上安装 Citrix Gateway 插件。Citrix Workspace 应用程序会自动将 Citrix Gateway 插件添加到其插件列表中。当用户登录到 Citrix Workspace 应用程序时，他们还可以登录到 Citrix Gateway 插件。您还可以将 Citrix Gateway 配置为在用户登录 Citrix Workspace 应用程序时对 Citrix Gateway 插件执行单点登录。

与 **iOS** 和 **Android** 设备相连接

用户可以通过使用 Secure Hub 从 iOS 或 Android 设备进行连接。用户可以通过使用 Secure Mail 访问其电子邮件，并使用 WorxWeb 连接到网站。

用户从移动设备连接时，连接将通过 Citrix Gateway 路由以访问内部资源。如果用户连接到 iOS，则可以将安全浏览作为会话配置文件的一部分启用。如果用户使用 Android 连接，则连接会自动使用微型 VPN。此外，Secure Mail 和 WorxWeb 使用 Micro VPN 通过 Citrix Gateway 建立连接。您不必在 Citrix Gateway 上配置微型 VPN。

常见部署

April 6, 2020

您可以在组织内部网络（或 Intranet）的外围部署 Citrix Gateway，以便为驻留在内部网络中的服务器、应用程序和其他网络资源提供安全的单点访问。所有远程用户必须先连接到 Citrix Gateway，然后才能访问内部网络中的任何资源。

Citrix Gateway 最常安装在网络中的以下位置：

- 在网络 DMZ 中
- 在没有 DMZ< 的安全网络中

还可以将 Citrix Gateway 与 Citrix Virtual Apps、Citrix Virtual Desktops、StoreFront 和 Citrix Endpoint Management 一起部署给用户，以允许用户访问其 Windows、Web、移动和 SaaS 应用程序。如果您的部署包括 Citrix Virtual Apps、StoreFront 或 Desktops 7，则可以在单跃点或双跃点 DMZ 配置中部署 Citrix Gateway。早期版本的 Citrix Virtual Desktops 或 Citrix Endpoint Management 不支持双跃点部署。

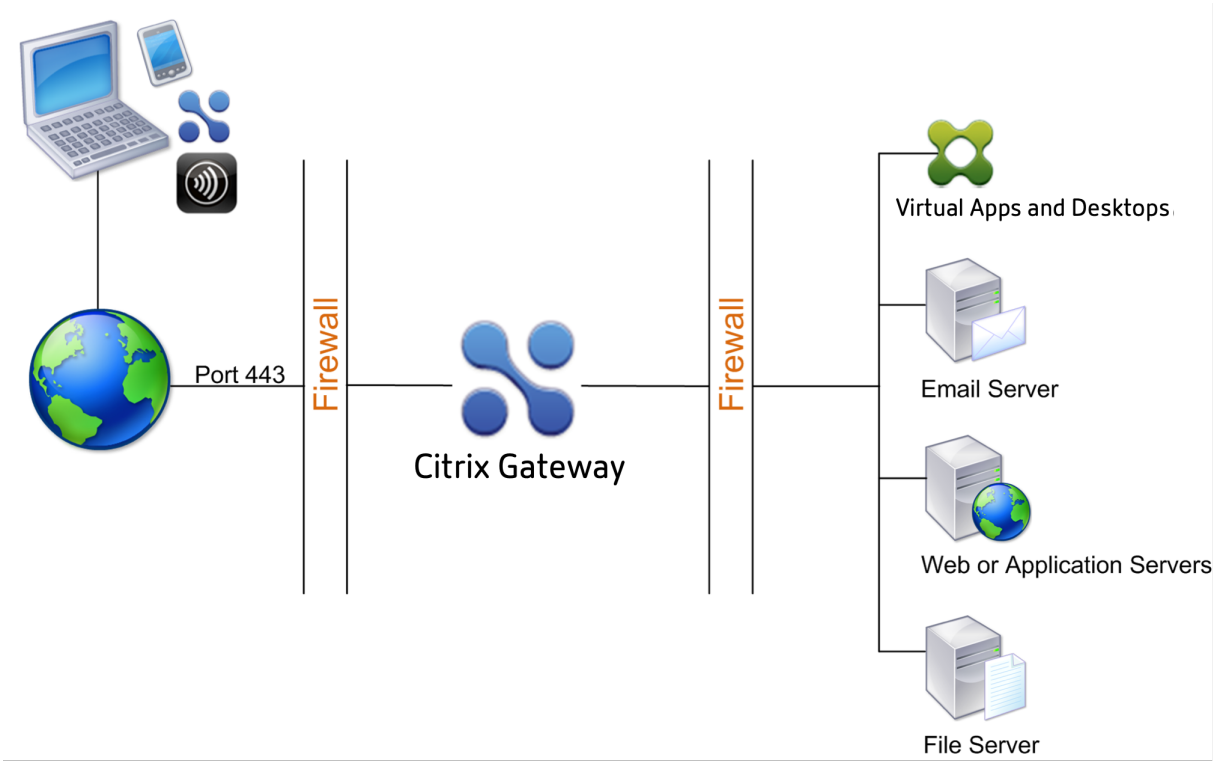
有关使用这些解决方案和其他受支持的 Citrix 解决方案扩展 Citrix Gateway 安装的详细信息，请参阅与 Citrix 产品集成主题。

在 **DMZ** 中部署

April 6, 2020

许多组织使用 DMZ 保护其内部网络。DMZ 是一个子网，位于组织的安全内部网络和 Internet（或任何外部网络）之间。在 DMZ 中部署 Citrix Gateway 时，用户会使用 Citrix Gateway 插件或 Citrix Workspace 应用程序进行连接。

图 1. 在 DMZ 中部署的 Citrix Gateway



在上图所示的配置中，您可以在 DMZ 中安装 Citrix Gateway，并将其配置为连接到 Internet 和内部网络。

DMZ 中的 **Citrix Gateway** 连接

在 DMZ 中部署 Citrix Gateway 时，用户连接必须遍历第一个防火墙才能连接到 Citrix Gateway。默认情况下，用户连接在端口 443 上使用 SSL 来建立此连接。要允许用户连接到内部网络，必须通过第一个防火墙在端口 443 上允许 SSL。

Citrix Gateway 解密来自用户设备的 SSL 连接，并代表用户与第二个防火墙后面的网络资源建立连接。必须通过第二个防火墙打开的端口取决于授权外部用户访问的网络资源。

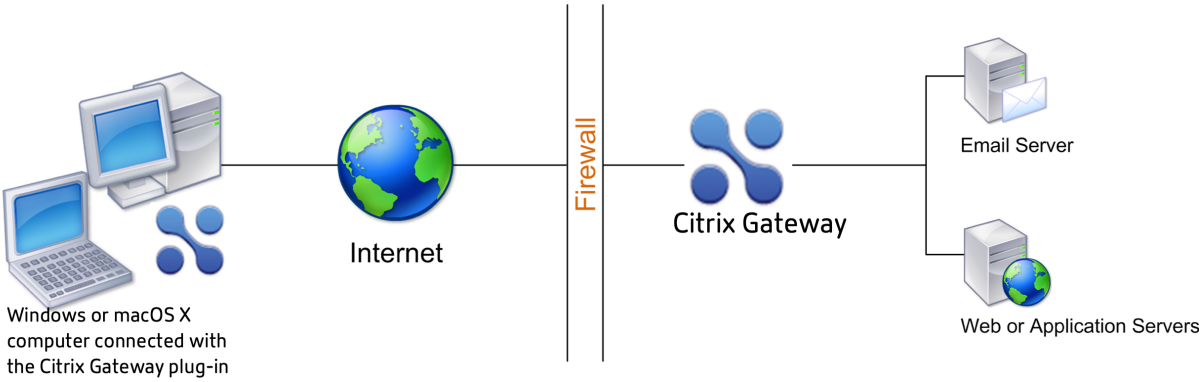
例如，如果授权外部用户访问内部网络中的 Web 服务器，并且此服务器侦听端口 80 上的 HTTP 连接，则必须通过第二个防火墙允许端口 80 上的 HTTP。Citrix Gateway 代表外部用户设备通过第二个防火墙与内部网络上的 HTTP 服务器建立连接。

在安全网络中部署

April 6, 2020

您可以在安全网络中安装 Citrix Gateway。在这种情况下，一个防火墙站在 Internet 和安全网络之间。Citrix Gateway 位于防火墙内，以控制对网络资源的访问。

图 1. 在安全网络中部署的 Citrix Gateway



在安全网络中部署 Citrix Gateway 时，请将 Citrix Gateway 上的一个接口连接到 Internet，将另一个接口连接到安全网络中运行的服务器。将 Citrix Gateway 置于安全网络中可为本地和远程用户提供访问权限。但是，由于此配置只有一个防火墙，因此对于从远程位置连接的用户而言，部署的安全性会降低。尽管 Citrix Gateway 拦截来自 Internet 的流量，但在对用户进行身份验证之前，流量会进入安全网络。在 DMZ 中部署 Citrix Gateway 时，在网络流量到达安全网络之前对用户进行身份验证。

在安全网络中部署 Citrix Gateway 时，Citrix Gateway 插件连接必须通过防火墙才能连接到 Citrix Gateway。默认情况下，用户连接使用端口 443 上的 SSL 协议建立此连接。若要支持此连接，必须在防火墙上打开端口 443。

客户端软件要求

April 6, 2020

本节介绍 Citrix Gateway 客户端软件的系统要求。

Citrix Gateway 通过使用 Citrix Gateway 插件支持用户连接。当用户使用插件登录时，它会建立一个完整的 VPN 隧道。使用 Citrix Gateway 插件，用户可以连接并使用您允许访问的网络资源。

如果在 Citrix Gateway 上配置终端节点策略，则当用户登录时，Citrix Gateway 会自动在用户设备上下载并安装终端节点分析插件。

Citrix Gateway 插件系统要求

April 6, 2020

Citrix Gateway 插件建立了从客户端计算机到 Citrix Gateway 设备的安全连接。

该插件作为适用于 Microsoft Windows、macOS X 和 Linux 操作系统的桌面应用程序分发。使用 Web 浏览器对 Citrix Gateway 设备的安全 URL 进行身份验证后，该插件将自动下载并安装在您的计算机上。

插件作为适用于 Android 和 iOS 设备的移动应用进行配置。

注意：要安装插件，操作系统需要管理员或 root 权限。

以下操作系统和 Web 浏览器支持将 Citrix Gateway 插件作为桌面应用程序。

操作系统	支持的浏览器
macOS 别行政区 X（10.9 及更高版本）	野生动物园 7.1 或更高版本；谷歌浏览器版本 30 或更高版本；火狐版本 30 或更高版本
Windows 10（x86 和 x64）	互联网浏览器 11; 谷歌浏览器版本 30 或更高版本; 火狐浏览器版本 24 或更高版本; 边缘铬
Windows 8.1	互联网浏览器 11; 谷歌浏览器版本 30 或更高版本; 火狐浏览器版本 24 或更高版本; 边缘铬
Windows 8	互联网浏览器 9 和 10; 谷歌浏览器版本 30 或更高版本; 火狐火狐版本 24 或更高版本; 边缘铬
Windows 7	互联网浏览器 9、10 和 11；谷歌浏览器 30 或更高版本；火狐火狐版本 24 或更高版本；边缘铬
Linux；Ubuntu 18.04 LTS、16.04 LTS、14.04 LTS 和 12.04 LTS。支持 32 位和 64 位操作系统。	火狐浏览器 44 及以上版本；谷歌浏览器 50 及以上版本

> 重要提示：由于 Ubuntu 16.04 LTS 中的一个错误（1573408），VPN 插件安装失败。相同的解决方法如下所示。

使用命令行界面键入以下命令：

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

如果缺少所需的依赖项包，则命令会列出它们，并且插件安装失败。这些依赖项包必须手动安装。管理员可以通过使用命令行界面键入以下命令来安装丢失的软件包。

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

以下操作系统支持将 Citrix Gateway 插件作为移动应用程序。

VPN 应用程序	支持的操作系统
Android	Android 4.1 及更高版本
iOS	iOS 8 及更高版本

端点分析要求

April 6, 2020

Citrix Gateway 在用户设备上安装端点分析插件时，插件会扫描用户设备，以了解您在 Citrix Gateway 上配置的端点安全要求。这些要求包括操作系统、防病毒或 Web 浏览器版本等信息。

当 Windows 用户首次使用浏览器连接到 Citrix Gateway 时，门户将请求安装端点分析插件。在后续登录尝试时，插件会检查升级控制配置，以确定是否需要客户端端点分析插件升级。如果有必要，用户将收到下载并安装较新的端点分析插件的提示。Windows 端点分析插件作为 Windows 32 位应用程序安装。安装或使用它不需要特殊权限。

对于 Mac OS X，用户需要安装端点分析插件。Mac OS X 的插件作为 32 位应用程序安装。无需特殊权限即可安装。在后续登录尝试时，如果插件版本不匹配，系统将提示用户下载并安装插件。

要使用端点分析插件，需要在用户设备上使用以下软件：

操作系统	支持的浏览器
–	–
Mac OS X（10.9 及更高版本）	野生动物园 7.1 或更高版本；谷歌浏览器版本 30 或更高版本；火狐版本 30 或更高版本
Windows 10	Internet Explorer 11；Google Chrome 版本 30 或更高版本；Mozilla Firefox 版本 24 或更高版本；Microsoft Edge 不受支持
Windows 8.1	互联网浏览器 11; 谷歌浏览器版本 30 或更高版本; 火狐浏览器版本 24 或更高版本
Windows 8	互联网浏览器 9 和 10; 谷歌浏览器 30 或更高版本; 火狐浏览器版本 24 或更高版本
Windows 7	互联网浏览器 9 和 10，11；谷歌浏览器 30 或更高版本；火狐火狐版本 24 或更高版本
Windows Vista	互联网浏览器 9; 火狐版本 9 和 10
Linux；Ubuntu 12.04 LTS、14.04 LTS 和 16.04 LTS
注意：支持 32 位和 64 位操作系统。	火狐浏览器 44 及以上版本; 谷歌浏览器 50 及以上版本

** 注 1：支持上述操作系统变体的 ** 所有版本。

注 **2**：对于 Windows 版本，必须安装所有服务包和关键更新。

** 注 3：** 对于 IE 浏览器版本，必须启用 Cookie。所需的最低版本为 7.0。

** 注 4：** 对于 Mozilla Firefox 版本，端点分析必须启用插件，所需的最低版本为 3.0。

重要说明：在进行身份验证终端节点分析的情况下，如果用户未在用户设备上安装端点分析插件或选择跳过扫描，则用户无法使用 Citrix Gateway 插件登录。在身份验证后端点分析的情况下，用户可以通过使用无客户端访问或使用 Citrix Workspace 应用程序访问不需要扫描的资源。

与 **Citrix** 产品的兼容性

April 6, 2020

下表提供了 Citrix Gateway 13.0 兼容的 Citrix 产品和版本。

> 注意： Citrix Gateway 功能在 Citrix ADC VPX 上可用。

Citrix 产品和支持的版本

Citrix 产品	发行版本
Citrix SD-WAN	10.2、11.0
Citrix ADC 平台	所有现有 MPX 和 VPX 型号，包括符合 FIPS 标准的设备。
StoreFront	3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14, 3.15
Web Interface	5.4
Citrix Virtual Apps and Desktops	7.6, 7.12, 7.13, 7.14, 7.15, 7.16, 7.17, 7.18
XenMobile	10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12

> 注意：支持 Citrix XenApp 6.5。

Citrix Workspace 应用程序、Citrix 移动生产力应用程序和插件

Citrix Workspace 应用程序或插件	支持的最低版本
适用于 macOS X 的 Citrix Gateway 插件	3.1.8
适用于 Windows 的 Citrix Gateway 插件	12.0
适用于 iOS 的 Citrix Gateway 插件	3.1.4
适用于 Android 的 Citrix Gateway 插件	2.0.14
适用于 Android 的 Citrix Workspace 应用程序	3.11
适用于 iOS 的 Citrix Workspace 应用程序	7.1.3
适用于 Mac 的 Citrix Workspace 应用程序	12.4
适用于 Windows 的 Citrix Workspace 应用程序	4.4
适用于 Linux 的 Citrix Workspace 应用程序	13.4
适用于 HTML5 的 Citrix Workspace 应用程序	2.3
适用于 Chrome 的 Citrix Workspace 应用程序	2.3
Secure Hub for iOS	10.5
Secure Hub for Android	10.5

Citrix Workspace 应用程序或插件	支持的最低版本
Secure Mail for iOS	10.5
Secure Web for iOS	10.5
Secure Mail for Android	10.5
Secure Web for Android	10.5

Windows 网关插件支持的 **Citrix Gateway** 功能

Citrix Gateway 13.0 Build 36.27 及更高版本支持以下功能。

- 设备防护支持
- nFactor 支持
- Opswat v4 支持
- SAML 支助
- AlwaysOn 服务

Licensing

April 6, 2020

必须对设备进行正确授权，然后才能部署 Citrix Gateway 以支持用户连接。

> 重要提示： Citrix 建议您保留收到的所有许可证文件的本地副本。当您保存配置文件的备份副本时，所有上载的许可证文件都包含在备份中。如果您需要重新安装 Citrix Gateway 设备软件，但没有配置备份，则需要原始许可证文件。

在 Citrix Gateway 上安装许可证之前，请设置设备的主机名，然后重新启动 Citrix Gateway。您可以使用安装向导配置主机名。为 Citrix Gateway 生成通用许可证时，主机名将在许可证中使用。

Citrix Gateway 许可证类型

April 6, 2020

Citrix Gateway 需要平台许可证。平台许可证允许使用 ICA 代理连接到 Citrix Virtual Apps、Citrix Virtual Desktops 或 StoreFront。若要允许从 Citrix Gateway 插件、SmartAccess 登录点或 Secure Hub、WorxWeb 或 Secure Mail 连接到网络，还必须添加通用许可证。Citrix Gateway VPX 附带平台许可证。

以下 Citrix Gateway 版本支持平台许可证：

- Citrix Gateway 13.0
- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1
- NetScaler Gateway 11.0
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10
- Citrix ADC VPX

重要提示：Citrix 建议您保留收到的所有许可证文件的本地副本。当您保存配置文件的备份副本时，所有上载的许可证文件都包含在备份中。如果您需要重新安装 Citrix Gateway 设备软件，但没有配置备份，则需要原始许可证文件。

平台许可证

平台许可证允许用户无限制地连接到 Citrix Virtual Apps 中的已发布应用程序或 Citrix Virtual Desktops 中的虚拟桌面。使用 Citrix Workspace 应用程序进行的连接不使用 Citrix Gateway 通用许可证。这些连接只需要平台许可证。所有新 Citrix Gateway 订单（无论是物理订单还是虚拟订单）都以电子方式传递平台许可证。如果您已拥有保修或维护协议所涵盖的设备，则可以从中获取平台许可证Citrix Web 站点。

> 重要提示：基于平台许可证，包括以下数量的通用许可证。
>
> - 标准版-500
> - 高级版 - 1000
> - 高级-无限制

通用授权协议

通用许可证将并发用户会话的数量限制为您购买的许可证数量。

通用许可证支持以下功能：

- 全 VPN 隧道
- Micro VPN
- 端点分析
- 基于策略的 SmartAccess
- 无客户端访问网站和文件共享

如果您购买标准版许可证，您可以随时拥有 500 个并发会话。当用户结束会话时，将为下一个用户释放该许可证。从多台计算机登录到 Citrix Gateway 的用户占用每个会话的许可证。

如果所有许可证都被占用，则在用户结束会话或终止会话之前，无法打开任何其他连接。连接关闭后，许可证将被释放，并可用于新用户。

当您收到 Citrix Gateway 设备时，许可将按以下顺序进行：

- 您在电子邮件中收到许可证授权代码 (LAC)。
- 您可以使用安装向导使用主机名配置 Citrix Gateway。
- 您可以从 Citrix Web 站点分配 Citrix Gateway 许可证。在分配过程中，使用主机名将许可证绑定到设备。
- 您可以在 Citrix Gateway 上安装许可证文件。

有关通用许可证的详细信息，请参阅Citrix Gateway 通用许可证

获取平台或通用许可证文件

April 6, 2020

安装 Citrix Gateway 后，即可从 Citrix 获取平台或通用许可证文件。登录 Citrix 网站以访问可用许可证并生成许可证文件。生成许可证文件后，您将其下载到计算机。当许可证文件位于计算机上时，您将其上传到 Citrix Gateway。有关 Citrix 许可的更多信息，请参阅Citrix Licensing 系统。

在获取许可证文件之前，请确保使用安装向导配置设备的主机名，然后重新启动设备。

重要提示：必须在 Citrix Gateway 上安装许可证。设备不会从 Citrix 许可证服务器获取许可证。

要获取您的许可证，请转到激活、升级和管理 Citrix 许可证网页。在此页面上，您可以获取新许可证并激活、升级和管理 Citrix 许可证。

在 **Citrix Gateway** 上安装许可证的步骤

April 6, 2020

将许可证文件成功下载到计算机后，可以在 Citrix Gateway 上安装许可证。许可证安装在 /nsconfig/license 目录中。

如果使用安装向导配置 Citrix Gateway 上的初始设置，则运行该向导时会安装许可证文件。如果您分配了一部分许可证，然后在稍后的日期分配了一个额外的号码，则可以在不使用安装向导的情况下安装许可证。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“许可证”。
2. 在详细信息窗格中，单击管理许可证。
3. 单击添加新许可证，然后单击浏览，导航到许可证文件，然后单击确定。

   配置实用程序中将显示一条消息，指出您需要重新启动 Citrix Gateway。点击重新启动。

设置最大用户数

在设备上安装许可证后，需要设置允许连接到设备的最大用户数。您可以在全局身份验证策略中设置最大用户计数。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的设置下，单击更改身份验证 AAA 设置。
3. 在“最大用户数”中，键入用户总量，然后单击“确定”。

   此字段中的编号对应于许可证文件中包含的许可证数量。此数量应小于或等于设备上安装的许可证总数。例如，您安装一个包含 100 个用户许可证的许可证和另一个包含 400 个用户许可证的许可证。许可证总数等于 500。可以登录的最大用户数等于或小于 500。如果登录 500 个用户，则在用户注销或终止会话之前，任何尝试登录超出该数量的用户都将被拒绝访问。

验证通用许可证的安装

April 6, 2020

继续操作之前，请验证您的通用许可证是否已正确安装。

使用配置实用程序验证通用许可证的安装

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“许可证”。

   在“许可证”窗格中，您将看到 Citrix Gateway 旁边的绿色复选标记。“允许的最大 Citrix Gateway 用户数量”字段显示设备上许可的并发用户会话数量。

使用命令行验证通用许可证的安装

1. 使用 SSH 客户端（如 PuTTY）打开与设备的安全外壳 (SSH) 连接。
2. 使用管理员凭据登录到设备。
3. 在命令提示符下，键入：显示许可证如果参数 SSL VPN 等于是，最大用户参数等于许可证数，则正确安装许可证。

常见问题解答

April 6, 2020

Licensing

什么是通用许可证 **(CCU)?**

通用许可证是 Citrix ADC 平台许可证之上的附加许可证。这些许可证对于以下情况是必需的：

确保 ICA 会议的安全

1. SmartAccess
2. SmartControl
3. EPA

SSL VPN

1. 适用于所有 SSL VPN 使用案例（Unified Gateway、CVPN、RDP 代理等）
2. 门户

新的许可政策有什么变化**?**

通用许可证的定价如下：

1. 0-2499 个用户-每个用户 100 美元
2. 2500 多个用户-每个用户 50 美元

早期的包装如下：

1. 标准和高级包括 5 个通用许可证
2. 高级许可证包括 100 个通用许可证

更改如下：

1. 标准将包括 500 个许可证
2. 高级将包括 1000 个许可证
3. 高级版没有任何 CCU 要求-这意味着客户不需要使用高级版的 CCU

另一方面，如果用户购买 Premium 11.1 或更高版本，则可以对所有使用案例使用通用许可证。

用户数量	价格
1-10000	$5
10001-20000	$2
20001+	$1.5

新定价何时可供买家使用**?**

新包装将被纳入 2016 年 9 月 26 日发布的 NS 11.1.49.16 版本。新的 SKU 将于 2016 年 9 月 19 日上线。

我们需要什么版本的 **Citrix ADC?**

客户需要 NS 11.1-49.16 或更高版本才能获得带氯化碳的新包装。

现有客户如何得到这个**?**

现有客户需要将其现有 NS 版本升级到 11.1.49.xx 才能获得新的包装。

如果客户不愿意升级并希望使用 NS 进行 SSL VPN，以下是要确保的关键事项：

1. Unified Gateway 仅提供高级版或高级版本
2. 如果他们通过 Citrix Virtual Apps and Desktops（高级版）免费收到 CCU，则需要购买 SSL VPN 的 CCU 或购买运行 11.1.49.xx 的 NS 高级版本
3. 目前正在更新联机 EULA，以反映使用情况。它将张贴在这里：https://www.citrix.com/buy/licensing/product.html
4. 他们可以通过销售例外流程获得相同的定价

如果客户运行标准版，想购买 **5000** 个许可证，他们付多少钱**?**

如果客户正在运行标准版，他们可以免费获得 500 个通用许可证。对于其余部分，他们将按照 1-10000 用户的新定价收取 5 美元的费用。

如果同一个客户回来并购买另外 **6000** 个许可证，他们需要支付多少钱**?**

如果客户回来购买另外 6000 个许可证，他们将被收取 6000 个用户 * 每个用户 5 美元 = 30,000 美元。他们不会得到将该行用于 11,000 个许可证的好处。

此价格也将收取年度维护费。

如果客户运行标准版，想购买 **11000** 许可证，他们付多少钱**?**

如果客户正在运行标准版，他们将免费获得前 500 个许可证。对于其余的，他们将支付 10,500 个用户 * 每个用户 2 美元 = 21,000 美元

其他供应商如何收费**?** 我需要告诉我的客户**?**

所有 SSL VPN 供应商按用户会话许可证收取费用。如果客户购买 Citrix ADC 高级版，Citrix 是唯一不按用户会话许可证收费的公司。

如果我的客户有 **100** 个 **CCU**，他们通过 **Citrix Virtual Apps and Desktops Premium Edition** 收到，并且他们为 **Unified Gateway** 购买了 **100** 个 **CCU**，他们现在是否有 **200** 个 **CCU?**

是。他们确实有 200 个 CCU。但是，他们只能使用 100 个 CCU 作为 SSL VPN 使用案例。但是，他们可以为 Citrix Virtual Apps and Desktops 用例使用 200 个 CCU。

开始前

April 6, 2020

在安装 Citrix Gateway 之前，应评估基础结构并收集信息，以规划满足组织特定需求的访问策略。当您定义访问策略时，您需要考虑安全影响并完成风险分析。您还需要确定允许用户连接到的网络，并决定启用用户连接的策略。

除了规划可供用户使用的资源之外，您还需要规划部署方案。Citrix Gateway 与以下 Citrix 产品配合使用：

- Citrix Endpoint Management
- Citrix Virtual Apps
- Citrix Virtual Desktops
- StoreFront
- Web Interface
- CloudBridge

有关部署 Citrix Gateway 的详细信息，请参阅常见部署和与 Citrix 产品集成

准备访问策略时，请执行以下初步步骤：

- 确定资源。列出要为其提供访问权限的网络资源，例如 Web、SaaS、移动或已发布应用程序、虚拟桌面、服务和您在风险分析中定义的数据。
- 开发访问方案。创建描述用户如何访问网络资源的访问方案。访问方案由用于访问网络、端点分析扫描结果、身份验证类型或其组合的虚拟服务器定义。您还可以定义用户登录到网络的方式。
- 识别客户端软件。您可以使用 Citrix Gateway 插件提供完全 VPN 访问权限，要求用户使用 Citrix Workspace 应用程序、Secure Hub 或使用无客户端访问登录。您还可以限制对 Outlook Web 应用程序或 WorxMail 的电子邮件访问。这些访问方案还决定了用户在获得访问权限时可以执行的操作。例如，您可以指定用户是否可以通过使用已发布的应用程序或连接到文件共享来修改文档。
- 将策略与用户、组或虚拟服务器关联。当单个或一组用户满足指定条件时，您在 Citrix Gateway 上创建的策略将强制执行。您可以根据您创建的访问方案来确定条件。然后，您可以创建策略，通过控制用户可以访问的资源以及用户可以对这些资源执行的操作来扩展网络的安全性。您可以将策略与适当的用户、组、虚拟服务器或全局关联。

本部分包括以下主题，以帮助您规划访问策略：

- 安全规划包括有关身份验证和证书的信息。
- 定义您可能需要的网络硬件和软件的先决条件。
- 您可以在配置 Citrix Gateway 之前记下设置的预安装清单。

安全规划

April 6, 2020

规划 Citrix Gateway 部署时，应了解与证书以及身份验证和授权相关的基本安全问题。

配置安全证书管理

默认情况下，Citrix Gateway 包括一个自签名的安全套接字层 (SSL) 服务器证书，该证书允许设备完成 SSL 握手。自签名证书足以用于测试或示例部署，但 Citrix 不建议将其用于生产环境。在生产环境中部署 Citrix Gateway 之前，Citrix 建议您从已知证书颁发机构 (CA) 请求并接收签名 SSL 服务器证书，然后将其上传到 Citrix Gateway。

如果在 Citrix Gateway 必须作为 SSL 握手中的客户端运行的任何环境中部署 Citrix Gateway（启动与其他服务器的加密连接），则还必须在 Citrix Gateway 上安装受信任的根证书。例如，如果使用 Citrix Virtual Apps 和 the Web Interface 部署 Citrix Gateway，则可以使用 SSL 对从 Citrix Gateway 到 Web Interface 的连接进行加密。在此配置中，必须在 Citrix Gateway 上安装受信任的根证书。

身份验证支持

您可以配置 Citrix Gateway 以对用户进行身份验证，并控制用户对内部网络上网络资源的访问（或授权）级别。

在部署 Citrix Gateway 之前，您的网络环境应具有目录和身份验证服务器，以支持以下身份验证类型之一：

- LDAP
- RADIUS
- TACACS+
- 具有审核和智能卡支持的客户端证书
- 具有 RADIUS 配置的 RSA
- SAML 身份验证

如果您的环境不支持上述列表中的任何身份验证类型，或者远程用户数量较少，则可以在 Citrix Gateway 上创建本地用户列表。然后，您可以配置 Citrix Gateway 以根据此本地列表对用户进行身份验证。使用此配置，您不需要在单独的外部目录中维护用户帐户。

保护您的 **Citrix Gateway** 部署

不同的部署可能需要不同的安全注意事项。Citrix ADC 安全部署指南提供了一般安全指南，帮助您根据特定的安全要求决定适当的安全部署。

有关详细信息，请参阅 Citrix ADC 安全部署指南。

必备条件

April 6, 2020

在 Citrix Gateway 上配置设置之前，请查看以下先决条件：

- Citrix Gateway 已物理安装在您的网络中，并具有对网络的访问权限。Citrix Gateway 部署在 DMZ 或防火墙后面的内部网络中。您还可以在双跃点 DMZ 中配置 Citrix Gateway 并配置到服务器场的连接。Citrix 建议在 DMZ 中部署设备。
- 您可以使用默认网关或内部网络的静态路由配置 Citrix Gateway，以便用户可以访问网络中的资源。Citrix Gateway 默认配置为使用静态路由。
- 用于身份验证和授权的外部服务器已配置并正在运行。有关详细信息，请参阅身份验证和授权。
- 网络具有域名服务器 (DNS) 或 Windows Internet 命名服务 (WINS) 服务器用于名称解析，以提供正确的 Citrix Gateway 用户功能。
- 您从 Citrix 网站下载了用于使用 Citrix Gateway 插件进行连接的通用许可证，并且这些许可证已准备好安装在 Citrix Gateway 上。
- Citrix Gateway 具有由受信任的证书颁发机构 (CA) 签名的证书。有关详细信息，请参阅安装和管理证书。

在安装 Citrix Gateway 之前，请使用预安装清单记下您的设置。

安装前清单

April 6, 2020

清单包括在安装 Citrix Gateway 之前应完成的任务和计划信息列表。

提供空间，以便您可以在完成任务并做笔记时检查每个任务。Citrix 建议您记下在安装过程中和配置 Citrix Gateway 时需要输入的配置值。

有关安装和配置 Citrix Gateway 的步骤，请参阅安装 Citrix Gateway。

用户设备

- 确保用户设备满足Citrix Gateway 插件系统要求
- 识别用户连接的移动设备。注意：如果用户连接到 iOS 设备，则需要在会话配置文件中启用安全浏览。

Citrix Gateway 基础网络连接

Citrix 建议您在开始配置设备之前获取许可证和签名的服务器证书。

- 识别并记下 Citrix Gateway 主机名。注意：这不是完全限定的域名 (FQDN)。FQDN 包含在绑定到虚拟服务器的签名服务器证书中。
- 获取通用许可证，请从Citrix Web 站点
- 生成证书签名请求 (CSR) 并发送到证书颁发机构 (CA)。输入您将 CSR 发送到 CA 的日期。
- 记下系统 IP 地址和子网掩码。
- 记下子网 IP 地址和子网掩码。
- 记下管理员密码。Citrix Gateway 附带的默认密码为 nsroot。

- 记下端口号。这是 Citrix Gateway 侦听安全用户连接的端口。默认值为 TCP 端口 443。此端口必须在不安全的网络（Internet）和 DMZ 之间的防火墙上打开。
- 记下默认网关 IP 地址。
- 记下 DNS 服务器 IP 地址和端口号。默认端口号为 53。此外，如果要直接添加 DNS 服务器，则还必须在设备上配置 ICMP (ping)。
- 记下第一个虚拟服务器 IP 地址和主机名。
- 记下第二个虚拟服务器 IP 地址和主机名（如果适用）。
- 记下 WINS 服务器 IP 地址（如果适用）。

可通过 **Citrix Gateway** 访问的内部网络

- 记下用户可以通过 Citrix Gateway 访问的内部网络。例如：10.10.0.0/24
- 输入用户使用 Citrix Gateway 插件通过 Citrix Gateway 连接时需要访问的所有内部网络和网络段。

高可用性

如果您有两个 Citrix Gateway 设备，则可以在高可用性配置中部署这些设备，其中一个 Citrix Gateway 接受和管理连接，而另一个 Citrix Gateway 则监视第一个设备。如果第一个 Citrix Gateway 出于任何原因停止接受连接，则第二个 Citrix Gateway 将接管并开始主动接受连接。

- 记下 Citrix Gateway 软件版本号。
- 两个 Citrix Gateway 设备上的版本号必须相同。
- 记下管理员密码（nsroot）。两台设备上的密码必须相同。
- 记下主 Citrix Gateway IP 地址和 ID。最大身份证号码为 64。
- 记下辅助 Citrix Gateway IP 地址和 ID。
- 获取并在两台设备上安装通用许可证。
- 必须在两台设备上安装相同的通用许可证。
- 记下 RPC 节点密码。

身份验证和授权

Citrix Gateway 支持多种不同的身份验证和授权类型，这些类型可以用于各种组合。有关身份验证和授权的详细信息，请参阅身份验证和授权。

LDAP 身份验证

如果您的环境包含 LDAP 服务器，则可以使用 LDAP 进行身份验证。

- 记下 LDAP 服务器 IP 地址和端口。

  如果允许与 LDAP 服务器不安全的连接，则默认为端口 389。如果使用 SSL 加密到 LDAP 服务器的连接，则默认为端口 636。

- 记下安全类型。

  您可以使用或不使用加密来配置安全性。

- 记下管理员绑定 DN。

  如果 LDAP 服务器需要身份验证，请输入 Citrix Gateway 在查询 LDAP 目录时应使用的管理员 DN。示例为 cn=administrator,cn=Users,dc=ace, dc=com。

- 记下管理员密码。

  这是与管理员绑定 DN 关联的密码。

- 写下基本 DN。

  用户所在的 DN（或目录级别）；例如，用户 = 用户、dc=ace、dc=com。

- 记下服务器登录名属性。

  输入指定用户登录名的 LDAP 目录人员对象属性。默认值为 “sAMAccountName”。如果您不使用 Active Directory，则此设置的常见值为 cn 或 uid。有
  关 LDAP 目录设置的详细信息，请参阅 配置 LDAP 身份验证

- 记下组属性。
  输入 LDAP 目录人员对象属性，该属性指定用户所属的组。默认值为 “memberOf”。此属性使 Citrix Gateway 能够标识用户所属的目录组。

- 记下子属性名称。

RADIUS 身份验证和授权

如果您的环境包含 RADIUS 服务器，则可以使用 RADIUS 进行身份验证。
RADIUS 身份验证包括 RSA SecurID、SafeWord 和 Gemalto Protiva 产品。

- 记下主 RADIUS 服务器 IP 地址和端口。默认端口是 1812。
- 记下主 RADIUS 服务器密钥（共享密钥）。
- 记下辅助 RADIUS 服务器 IP 地址和端口。默认端口是 1812。
- 记下辅助 RADIUS 服务器密钥（共享密钥）。
- 记下密码编码的类型（PAP、CHAP、MS-CHAP v1、MSCHAP v2）。

SAML 身份验证

安全断言标记语言 (SAML) 是一种基于 XML 的标准，用于在身份提供商 (IdP) 和服务提供商之间交换身份验证和授权。

- 获取并在 Citrix Gateway 上安装安全 IdP 证书。
- 记下重定向 URL。
- 记下用户字段。
- 记下签名证书名称。

- 记下 SAML 颁发者名称。
- 记下默认身份验证组。

通过防火墙打开端口（单跳 **DMZ**）

如果您的组织使用单个 DMZ 保护内部网络，并在 DMZ 中部署 Citrix Gateway，请通过防火墙打开以下端口。如果要在双跃点 DMZ 部署中安装两个 Citrix Gateway 设备，请参阅打开防火墙上的适当端口。

在不安全网络和 **DMZ** 之间的防火墙上

- 在 Internet 和 Citrix Gateway 之间的防火墙上打开 TCP/SSL 端口（默认 443）。用户设备连接到此端口上的 Citrix Gateway。

在安全网络之间的防火墙上

- 在 DMZ 和安全网络之间的防火墙上打开一个或多个适当的端口。Citrix Gateway 连接到一个或多个身份验证服务器或连接到这些端口上的安全网络中运行 Citrix Virtual Apps and Desktops 的计算机。
- 记下身份验证端口。

  仅打开适合您的 Citrix Gateway 配置的端口。

  - 对于 LDAP 连接，默认为 TCP 端口 389。
  - 对于 RADIUS 连接，默认为 UDP 端口 1812。记下 Citrix Virtual Apps and Desktops 端口。
- 如果将 Citrix Gateway 与 Citrix Virtual Apps and Desktops 结合使用，请打开 TCP 端口 1494。如果启用会话可靠性，请打开 TCP 端口 2598 而不是 1494。Citrix 建议将这两个端口保持打开状态。

Citrix Virtual Desktops、Citrix Virtual Apps、Web Interface 或 StoreFront

如果要部署 Citrix Gateway 以通过 Web Interface 或 StoreFront 提供对 Citrix Virtual Apps and Desktops 的访问，请完成以下任务。此部署不需要 Citrix Gateway 插件。用户仅通过使用 Web 浏览器和 Citrix Receiver，通过 Citrix Gateway 访问已发布的应用程序和桌面。

- 记下运行 Web Interface 或 StoreFront 的服务器的 FQDN 或 IP 地址。
- 记下运行安全票证机构 (STA) 的服务器的 FQDN 或 IP 地址（仅适用于 Web Interface ）。

Citrix Endpoint Management

如果在内部网络中部署 Citrix Endpoint Management，请完成以下任务。如果用户从外部网络（如 Internet）连接到 Endpoint Management，则用户必须先连接到 Citrix Gateway，然后才能访问移动、Web 和 SaaS 应用。

- 记下 Endpoint Management 的 FQDN 或 IP 地址。
- 识别用户可以访问的 Web、SaaS 和移动 iOS 或 Android 应用程序。

使用 **Citrix Virtual Apps** 进行双跃点 **DMZ** 部署

如果要在双跃点 DMZ 配置中部署两个 Citrix Gateway 设备，以支持对运行 Citrix Virtual Apps 的服务器的访问，请完成以下任务。

第一个 **DMZ** 中的 **Citrix Gateway**

第一个 DMZ 是位于内部网络最外边缘（最接近 Internet 或不安全的网络）的 DMZ。客户端通过将 Internet 与 DMZ 分开的防火墙连接到第一个 DMZ 中的 Citrix Gateway。在第一个 DMZ 中安装 Citrix Gateway 之前，请收集此信息。

- 完成此 Citrix Gateway 清单的 Citrix Gateway 基本网络连接部分中的项目。

  完成这些项目时，请注意，接口 0 将此 Citrix Gateway 连接到 Internet，接口 1 将此 Citrix Gateway 连接到第二个 DMZ 中的 Citrix Gateway。

- 在主设备上配置第二个 DMZ 设备信息。

  要将 Citrix Gateway 配置为双跃点 DMZ 中的第一个跃点，必须在第一个 DMZ 中的设备上的第二个 DMZ 中指定 Citrix Gateway 的主机名或 IP 地址。指定在第一个跃点中的设备上配置 Citrix Gateway 代理后，请将其全局绑定到 Citrix Gateway 或虚拟服务器。

- 记下设备之间的连接协议和端口。

  要将 Citrix Gateway 配置为双 DMZ 中的第一个跃点，必须指定第二个 DMZ 中 Citrix Gateway 侦听连接的连接协议和端口。连接协议和端口是带 SSL 的 SOCKS（默认端口 443）。协议和端口必须通过分隔第一个 DMZ 和第二个 DMZ 的防火墙打开。

第二个 **DMZ** 中的 **Citrix Gateway**

第二个 DMZ 是最接近内部安全网络的 DMZ。部署在第二个 DMZ 中的 Citrix Gateway 用作 ICA 流量的代理，在外部用户设备和内部网络上的服务器之间遍历第二个 DMZ。

- 完成此 Citrix Gateway 清单的 Citrix Gateway 基本网络连接部分中的任务。

  完成这些项目时，请注意，接口 0 将此 Citrix Gateway 连接到第一个 DMZ 中的 Citrix Gateway。接口 1 将此 Citrix Gateway 连接到安全网络。

升级

April 6, 2020

当新版本可用时，您可以升级驻留在 Citrix Gateway 上的软件。您可以在 Citrix 网站上检查更新。仅当 Citrix Gateway 许可证在发布更新时处于专享升级服务计划下时，才能升级到新版本。您可以随时续订专享升级服务。有关详细信息，请参阅Citrix 支持网站。

有关最新 Citrix Gateway 维护版本的信息，请参阅Citrix 知识中心。

检查软件更新

1. 去Citrix Web 站点。
2. 点击我的帐户并登录。
3. 单击下载。
4. 在“查找下载”下，选择 Citrix Gateway。
5. 在“选择下载类型”中，选择“产品软件”，然后单击“查找”。
   还可以选择虚拟设备以下载 Citrix ADC VPX。选择此选项后，您将收到每个虚拟机管理程序的虚拟机软件列表。
6. 在 Citrix Gateway 页面上，展开 Citrix ADC Gateway 或 Access Gateway。
7. 单击要下载的设备软件版本。
8. 在要下载的版本的设备软件页面上，选择虚拟设备，然后单击“下载”。
9. 按照屏幕上的说明下载软件。

将软件下载到您的计算机时，您可以使用升级向导或命令提示符安装软件。

使用升级向导升级 **Citrix Gateway**

1. 在配置实用程序的 配置选项卡上的导航窗格中，单击系统。
2. 在详细信息窗格中，单击 升级向导。
3. 单击“下一步”，然后按照向导中的说明操作。

使用命令提示符升级 **Citrix Gateway**

1. 要将软件上传到 Citrix Gateway，请使用安全的 FTP 客户端（如 WinSCP）连接到设备。
2. 将软件从计算机复制到设备上的 /var/nsinstall 目录。
3. 使用安全外壳 (SSH) 客户端（如 PuTTY）打开与设备的 SSH 连接。
4. 登录到 Citrix Gateway。
5. 在命令提示窗口中，键入：`shell`
6. 要更改为 nsinstall 目录，请在命令提示符下键入：`cd /var/nsinstall`
7. 要查看目录的内容，请键入：`ls`
8. 要解压软件，请键入：tar –xvzf build_X_XX.tgz

   其中 Build_x_xx.tgz 是要升级到的内部版本的名称。
9. 要开始安装，请在命令提示符下键入：`./installns`
10. 安装完成后，重新启动 Citrix Gateway。

Citrix Gateway 重新启动后，要验证安装成功，请启动配置实用程序。设备上的 Citrix Gateway 版本将显示在右上角。

安装系统

April 6, 2020

当您收到 Citrix Gateway 设备时，您将解压设备并准备站点和机架。确定要安装设备的位置符合环境标准并根据说明安装服务器机架后，即可安装硬件。装载设备后，将其连接到网络、电源和用于初始配置的控制台终端。打开设备后，执行初始配置，并分配管理和网络 IP 地址。请务必遵守安装说明中列出的注意事项和警告。

安装 Citrix ADC VPX 虚拟设备时，必须先获取虚拟设备映像并将其安装在虚拟机管理程序或其他虚拟机监视器上。

Citrix 建议您使用该Citrix Gateway 预安装清单主题，以便在尝试配置 Citrix Gateway 设备之前记录您的设置。清单包括有关安装 Citrix Gateway 以及设备的信息。

配置 **Citrix Gateway**

April 6, 2020

在 Citrix Gateway 上配置基础网络设置后，可以配置详细设置，以便用户可以连接到安全网络中的网络资源。这些设置包括：

- 虚拟服务器。您可以在 Citrix Gateway 上配置多个虚拟服务器，这样可以根据需要实施的用户方案创建不同的策略。每个虚拟服务器都有自己的 IP 地址、证书和策略集。例如，您可以配置虚拟服务器并限制用户使用内部网络中的网络资源，具体取决于用户在组中的成员身份以及绑定到虚拟服务器的策略。您可以使用以下方法创建虚拟服务器：
  - 快速配置向导
  - Citrix Gateway 向导
  - 配置实用程序
- 高可用性。在网络中部署两个 Citrix Gateway 设备时，可以配置高可用性。如果主设备发生故障，辅助设备可以在不影响用户会话的情况下接管。
- 证书。您可以使用证书保护用户与 Citrix Gateway 的连接。创建证书签名请求 (CSR) 时，将完全限定的域名添加到证书。您可以将证书绑定到虚拟服务器。
- 身份验证。Citrix Gateway 支持多种身份验证类型，包括本地 LDAP、RADIUS、SAML、客户端证书和 TACACS+。此外，您还可以配置级联和双重身份验证。
  注意：如果您使用 RSA、Safeword 或 Gemalto Protiva 进行身份验证，则可以使用 RADIUS 配置这些类型。
- 用户连接。您可以使用会话配置文件配置用户连接。在配置文件中，您可以确定用户可以登录的插件以及用户可能需要的任何限制。然后，您可以使用一个配置文件创建策略。您可以将会话策略绑定到用户、组和虚拟服务器。
- 主页。您可以使用默认访问界面作为主页，也可以创建自定义主页。用户成功登录 Citrix Gateway 后，将显示主页。
- 终端分析。您可以在 Citrix Gateway 上配置策略，以便在用户登录时检查用户设备是否有软件、文件、注册表项、进程和操作系统。端点分析允许您通过要求用户设备拥有所需软件来提高网络的安全性。

使用配置实用程序

April 6, 2020

配置实用程序允许您配置大多数 Citrix Gateway 设置。您可以使用 Web 浏览器访问配置实用程序。

登录到配置实用程序

1. 在 Web 浏览器中，键入 Citrix Gateway 的系统 IP 地址，如`http://192.168.100.1`。
   注意：Citrix Gateway 已预配置默认 IP 地址
   192.168.100.1 和子网掩码
   255.255.0.0。
2. 在用户名和密码中，键入 nsroot
3. 在“部署类型”中，选择 Citrix Gateway，然后单击“登录”。

当您首次登录到配置实用程序时，默认情况下，“主页”选项卡上打开仪表板。在“主页”选项卡上，可以使用“快速配置”向导配置虚拟服务器、身份验证、证书和 Citrix Endpoint Management 的设置。您还可以在快速配置向导中配置 StoreFront 或 Web Interface 设置。

有关配置 Citrix Gateway 的详细信息，请参阅：

- 使用安装向导配置初始设置。
- 使用快速配置向导配置设置
- 使用 Citrix Gateway 向导配置设置。

Citrix Gateway 上的策略和配置文件

April 6, 2020

Citrix Gateway 上的策略和配置文件允许您在指定方案或条件下管理和实施配置设置。单个策略声明或定义在满足指定条件集时生效的配置设置。每个策略都有一个唯一的名称，并且可以具有绑定到策略的配置文件。

有关 Citrix Gateway 策略的详细信息，请参阅以下主题：

策略的工作原理

April 6, 2020

策略由布尔条件和称为配置文件的设置集合组成。在运行时评估条件以确定是否应该应用策略。

配置文件是使用特定参数的设置集合。配置文件可以有任何名称，您可以在多个策略中重复使用。您可以在配置文件中配置多个设置，但每个策略只能包含一个配置文件。

您可以使用已配置的条件和配置文件将策略绑定到虚拟服务器、组、用户或全局。策略由它们控制的配置设置类型来引用。例如，在会话策略中，您可以控制用户登录的方式以及用户可以保持登录的时间。

如果将 Citrix Gateway 与 Citrix Virtual Apps 结合使用，Citrix Gateway 名称将作为筛选器发送到 Citrix Virtual Apps。将 Citrix Gateway 配置为使用 Citrix Virtual Apps 和 SmartAccess 时，可以在 Citrix Virtual Apps 中配置以下设置：

- 在设备上配置的虚拟服务器的名称。该名称将作为 Citrix Gateway 场名称发送到 Citrix Virtual Apps。
- 预身份验证或会话策略的名称作为筛选器名称发送。

有关将 Citrix Gateway 配置为与 Citrix Endpoint Management 结合使用的详细信息，请参阅为 Citrix Endpoint Management 环境配置设置。

有关配置 Citrix Gateway 以与 Citrix Virtual Apps and Desktops 结合使用的详细信息，请参阅使用 Web Interface 访问 Citrix Virtual Apps 和 Citrix Virtual Desktops 资源和与 Citrix Endpoint Management 或 StoreFront 集成。

有关预身份验证策略的更多信息，请参阅配置终端策略。

设定政策的优先级

September 26, 2019

策略按策略的约束顺序排列优先级和评估。

以下两种方法确定策略优先级：

- 策略绑定到的级别：全局、虚拟服务器、组或用户。政策级别的排名从最高到最低如下：
  - 用户（最高优先级）
  - 小组
  - 虚拟服务器
  - 全局（最低优先级）
- 无论策略绑定的级别如何，数字优先级都是优先级。如果全局绑定的策略的优先级号为一个，绑定到用户的另一个策略的优先级号为 2，则全局策略优先级为优先级。优先级数越低，策略的优先级越高。

配置条件策略

April 6, 2020

配置策略时，您可以使用任何布尔表达式来表示策略应用时的条件。配置条件策略时，可以使用任何可用的系统表达式，例如：

- 客户端安全字符串
- 网络信息
- HTTP 标头和 Cookie
- 一天中的时间
- 客户端证书值

您还可以创建策略，以便仅在用户设备满足特定条件（如 SmartAccess 的会话策略）时应用。

配置条件策略的另一个示例是改变用户的身份验证策略。例如，您可以要求从内部网络外部（例如从家庭计算机或通过移动设备使用 Micro VPN）连接到 Citrix Gateway 插件的用户进行身份验证，方法是使用 LDAP 和通过广域网 (WAN) 连接的用户进行身份验证。使用 RADIUS。

注意：如果策略规则被配置为会话配置文件中安全设置的一部分，则无法使用基于终端分析结果的策略条件。

在 **Citrix Gateway** 上创建策略

January 10, 2023

您可以使用配置实用程序创建策略。创建策略后，将策略绑定到适当的级别：用户、组、虚拟服务器或全局。将策略绑定到其中一个级别时，如果符合策略条件，用户将收到配置文件中的设置。每个策略和配置文件都有一个唯一的名称。

如果将 Citrix Endpoint Management 或 StoreFront 作为部署的一部分，则可以使用“快速配置”向导配置此部署的设置。有关向导的更多信息，请参阅使用快速配置向导配置设置。

配置系统表达式

April 6, 2020

系统表达式指定强制执行策略的条件。例如，在用户登录时强制执行预身份验证策略中的表达式。会话策略中的表达式将在用户通过身份验证并登录到 Citrix Gateway 后进行评估和强制执行。

Citrix Gateway 上的表达式包括：

- 限制用户在与 Citrix Gateway 建立连接时可以使用的对象的常规表达式
- 用于定义必须在用户设备上安装并运行的软件、文件、进程或注册表值的客户端安全表达式
- 基于网络设置限制访问的基于网络的表达式

Citrix Gateway 也可用作 Citrix ADC 设备。设备上的某些表达式更适用于 Citrix ADC。常规表达式和基于网络的表达式通常与 Citrix ADC 一起使用，通常不与 Citrix Gateway 一起使用。Citrix Gateway 上使用客户端安全表达式来确定在用户设备上安装了正确的项目。

配置客户端安全表达式

表达式是策略的组成部分。表达式表示根据请求或响应评估的单个条件。您可以创建一个简单的表达式安全字符串来检查条件，例如：

- 用户设备操作系统，包括服务包
- 防病毒软件版本和病毒定义
- 文件
- 进程
- 注册表值
- 用户证书

创建简单表达式和复合表达式

April 6, 2020

简单表达式检查单个条件。简单表达式的一个例子是：

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

复合表达式检查多个条件。通过使用逻辑运算符 && 和连接到一个或多个表达式名称来创建复合表达式	。您可以使用符号按求值顺序对表达式进行分组。

复合表达式可分为：

- 命名表达式。作为一个独立的实体，命名表达式可以被其他策略重复使用，并且是策略的一部分。您可以在配置实用程序中的系统级别配置命名表达式。您可以在策略中使用预定义的命名表达式或创建自己的表达式。
- 内联表达式。内联表达式是您在策略特定于策略的策略中构建的表达式。

创建命名表达式

1. 在配置实用程序的配置选项卡上的导航窗格中，展开 AppExpert，然后单击表达式。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“创建策略表达式”对话框的“表达式名称”中，键入表达式的名称。
4. 要创建表达式，请单击“添加”。
5. 执行以下操作之一：
   a) 在“常用表达式”中，从列表中选择一个表达式，单击“确定”，单击“创建”，然后单击“关闭”。
   b) 在“构造表达式”下，选择表达式字符串的参数，单击“确定”，单击“创建”，然后单击“关闭”。

添加自定义表达式

April 6, 2020

如果要创建策略，则可以在配置策略时创建自定义表达式。例如，您正在创建会话配置文件以允许用户使用 Citrix Gateway 插件登录、设置会话的时间限制以及允许使用 Windows 进行单点登录。创建会话配置文件后，可以在“创建会话策略”对话框中创建表达式。以下示例显示了检查进程和防病毒应用程序的表达式：

```
CLIENT.APPLICATION.PROCESS(ccapp.exe)EXISTS -frequent 5 && CLIENT.APPLICATION.AV(Symantec).VERSION==1
-freshness 5 && ns_true
```

在策略表达式中使用运算符和操作数

April 6, 2020

运算符是标识操作一个或多个对象或操作数的运算（例如数学、布尔或关系运算）的符号。本主题的第一部分定义了您可以使用的运算符并提供了定义。第二部分列出了可用于特定限定符（如方法、URL 和查询）的运算符。

运算符和定义

本部分定义了创建策略表达式时可以使用的运算符，并提供了运算符的描述。

- ==,！=、当量、NEQ

这些运算符测试精确匹配。它们区分大小写（“cmd.exe” 不等于 “cMd.exe”）。这些运算符对于创建允许符合确切语法的特定字符串而排除其他字符串的权限非常有用。

- GT

此运算符用于数值比较；它用于 URL 和查询字符串的长度。

- CONTAINS、NOTCONTAINS

这些运算符对指定的限定符执行检查，以确定指定的字符串是否包含在限定符中。这些运算符不区分大小写。

- EXISTS、NOTEXISTS

这些运算符检查是否存在特定限定符。例如，这些运算符可应用于 HTTP 标头，以确定是否存在特定 HTTP 标头或 URL 查询是否存在。

- CONTENTS

此运算符检查限定符是否存在以及它是否具有内容（即，是否存在标头并且具有与它关联的值，无论值如何）。

限定符、运算符、操作数、操作和示例

本部分显示可用于运算符和操作数的参数。每个项目都以限定符开头，然后列出关联的运算符和操作数，描述表达式将执行的操作，并提供一个示例。

- 方法

运算符：EQ、NEQ
操作数：必填项：
- 標準 HTTP 方法
- 支持的方法
- GET、HEAD、POST、PUT、DELETE OPTIONS、TRACE、CONNECT
操作：验证传入请求方法配置的方法。
示例：Method EQ GET

URL

-

运算符：EQ，NEQ
操作数：必填项：URL（格式：/[前缀] [*] [. 后缀]）
操作：使用配置的 URL 验证传入 URL。
示例：
URL EQ / foo*.asp
URL EQ /foo*
URL EQ /*.asp
URL EQ /foo.asp

-

运算符：CONTAINS、NOTCONTAINS
操作数：必需：任何字符串（引号中）
操作：验证传入的 URL 是否存在配置的模式。（包括 URL 和 URL 查询。）
示例：URL CONTAINS ‘ZZZ’

- 网址莱恩

运算符：GT
操作数：必填项：长度（作为整数值）
操作：将传入 URL 长度与配置的长度进行比较。（包括 URL 和 URL 查询。）
示例：URLLEN GT 60

- URL 查询

运算符：CONTAINS、NOTCONTAINS
操作数：必填：任何字符串（引号中）。
可选：长度和偏移量

操作：
验证传入的 URL 查询是否存在配置的模式。
使用类似于内容。
如果未指定选项，则使用模式后的整个 URL 查询。
如果存在选项，则仅使用模式后查询的长度。
偏移量用于指示从哪里开始搜索模式。
示例：URLQUERY CONTAINS ‘ZZZ’

- URL QUERY LEN

运算符：GT
操作数：必需：长度（作为整数值）
操作：将传入 URL 查询长度与配置的长度进行比较。
示例：URLQUERYLN GT 60

- URL 令牌

运算符：EQ，NEQ
操作数：必填：URL 令牌（支持的 URL 令牌 =，+,%,！ ,&,?).
操作：比较传入 URL 是否存在已配置的令牌。必须在问号前面输入反斜杠 ()。
示例：URLTOKENS EQ ‘% , +, &, \?’

- VERSION

运算符：EQ、NEQ
操作数：必填项：标准 HTTP 版本。有效的 HTTP 版本字符串 HTTP/1.0, HTTP/1.1
操作：将传入请求的 HTTP 版本与配置的 HTTP 版本进行比较。
示例：VERSION EQ HTTP/1.1

标题

-

运算符：EXISTS、NOTEXISTS
操作数：无
操作：检查传入请求是否存在 HTTP 头。
示例：Header Cookie EXISTS

-

运算符：CONTAINS、NOTCONTAINS
操作数：必填：任何字符串（引号中）。
可选：长度和偏移量
操作：验证传入请求是否存在特定标头中已配置的模式。使用类似于内容。如果未指定选项，则使用模式后的整个 HTTP 标头值。如果存在选项，则仅使用模式后头的长度。偏移量用于指示从哪里开始搜索模式。
示例：Header Cookie CONTAINS “&sid”

-

运算符：内容
操作数：可选：长度和偏移量
操作：使用 HTTP 标头的内容。如果未指定选项，则使用整个 HTTP 标头值。如果存在选项，则仅使用从偏移量开始的标头长度。
示例：Header User-Agent CONTENTS

- SOURCEIP

运算符：EQ、NEQ
操作数：必填项：IP 地址
可选项：子网掩码
操作：根据配置的 IP 地址验证传入请求中的源 IP 地址。如果指定了可选的子网掩码，则会根据配置的 IP 地址和子网掩码验证传入请求。
示例：Sourceip EQ 192.168.100.0 -netmask 255.255.255.0

- DESTIP

运算符：EQ、NEQ
操作数：必填项：IP 地址
可选项：子网掩码
操作：根据配置的 IP 地址验证传入请求中的目标 IP 地址。如果指定了可选的子网掩码，则会根据配置的 IP 地址和子网掩码验证传入请求。
示例：Sourceip EQ 192.168.100.0 -netmask 255.255.255.0

- SOURCEPORT

运算符：EQ、NEQ
操作数：必需：端口号
可选：端口范围
操作：根据配置的端口号验证传入请求中的源端口号。
示例：SOURCEPORT EQ 10-20

- DESTPORT

运算符：EQ、NEQ
操作数：必需：端口号
可选：端口范围
操作：根据配置的端口号验证传入请求中的目标端口号。
示例：DESTPORT NEQ 80

- CLIENT.SSL.VERSION

运算符：EQ、NEQ
操作数：必填项：SSL 版本

操作：检查安全连接中使用的 SSL 或 TLS 版本的版本。
示例：CLIENT.SSL.VERSION EQ SSLV3

- CLIENT.CIPHER.TYPE

运算符：EQ，NEQ
操作数：必填：客户端密码类型
操作：检查正在使用的密码类型（导出或非导出）。
示例：CLIENT.CIPHER.TYPE EQ EXPORT

- CLIENT.CIPHER.BITS

运算符：EQ、NEQ、GE、LE、GT、LT
操作数：必填项：客户端密码位
操作：检查正在使用的密码的关键强度。
示例：CLIENT.CIPHER.BITS GE 40

- CLIENT.CERT

运算符：EXISTS，NOTEXERS
操作数：无
操作：检查客户端是否在 SSL 握手期间发送了有效证书。
示例：CLIENT.CERT EXISTS

- CLIENT.CERT.VERSION

运算符：EQ、NEQ、GE、LE、GT、LT
操作数：客户端证书版本
操作：检查客户端证书的版本。
示例：CLIENT.CERT.VERSION EQ 2

- CLIENT.CERT.SERIALNUMBER

运算符：EQ、NEQ
操作数：必填项：客户端证书序列号
操作：检查客户端证书的序列号。序列号被视为字符串。
示例：CLIENT.CERT.SER IALNUMBER EQ 2343323

- CLIENT.CERT.SIGALGO

运算符：EQ、NEQ
操作数：必填：客户端证书签名算法。
操作：检查客户端证书中使用的签名算法。
示例：CLIENT.CERT.SIGALGO EQ md5WithRSAEncryption

- CLIENT.CERT.SUBJECT

运算符：CONTAINS、NOTCONTAINS
操作数：必填：客户端证书主题

可选：长度，偏移
操作：检查客户端证书的主题字段。
示例：CLIENT.CERT.SUBJECT CONTAINS CN= Access_Gateway

- CLIENT.CERT.ISSUER

运算符：CONTAINS、NOTCONTAINS
操作数：必需：客户端证书颁发者
可选：长度，偏移
操作：检查客户端证书的颁发者字段。
示例：CLIENT.CERT.ISSUER CONTAINS O=VeriSign

- CLIENT.CERT.VALIDFROM

运算符：EQ、NEQ、GE、LE、GT、LT
操作数：必需：日期
操作：检查客户端证书的有效日期。
有效的日期格式为：
Tue, 05 Nov 1994 08:12:31 GMT
Tuesday, 05-Nov-94 08:12:31 GMT
Tue Nov 14 08:12:31 1994
示例：CLIENT.CERT.VALIDFROM GE ‘Tue Nov 14 08:12:31 1994’

- CLIENT.CERT.VALIDTO

运算符：EQ、NEQ、GE、LE、GT、LT
操作数：必需：日期
操作：检查客户端证书有效的日期。
有效日期格式为：
Tue, 05 Nov 1994 08:12:31 GMT
Tuesday, 05-Nov-94 08:12:31 GMT
Tue Nov 14 08:12:31 1994
示例：CLIENT.CERT.VALIDTO GE ‘Tue Nov 14 08:12:31 1994’

查看 **Citrix Gateway** 配置设置

April 6, 2020

对 Citrix Gateway 进行配置更改时，这些更改将保存在日志文件中。您可以查看多种类型的配置设置：

- 已保存的配置。您可以查看在 Citrix Gateway 上保存的设置。
- 正在运行的配置。您可以查看已配置但尚未保存为 Citrix Gateway 的保存配置的活动设置，例如虚拟服务器或身份验证策略。

- 运行与保存的配置。您可以并排比较 Citrix Gateway 上正在运行和保存的配置。

您还可以清除 Citrix Gateway 上的配置设置。

重要说明：如果选择清除 Citrix Gateway 上的设置，则会删除证书、虚拟服务器和策略。Citrix 建议您不要清除配置。

保存 **Citrix Gateway** 配置

April 6, 2020

您可以将 Citrix Gateway 上的当前配置保存到网络中的计算机，查看当前正在运行的配置，并比较已保存的配置和正在运行的配置。

将配置保存在 **Citrix Gateway** 上的步骤

1. 在配置实用程序的详细信息窗格上方，单击“保存”图标，然后单击“是”。

在 **Citrix Gateway** 上查看并保存配置文件

保存的配置是保存在 Citrix Gateway 上日志文件中的设置，例如虚拟服务器、策略、IP 地址、用户、组和证书的设置。

在 Citrix Gateway 上配置设置时，可以将设置保存到计算机上的文件中。如果您需要重新安装 Citrix Gateway 软件或意外删除了某些设置，则可以使用此文件还原配置。如果需要还原设置，可以将文件复制到 Citrix Gateway，然后使用命令行界面或程序（如 WinSCP）重新启动设备，将文件复制到 Citrix Gateway。

1. 在配置实用程序的配置选项卡上的导航窗格中，展开系统，然后单击诊断。
2. 在详细信息窗格中的“查看配置”下，单击“已保存的配置”。
3. 在保存的配置对话框中，单击将输出文本保存到文件，命名该文件，然后单击保存。
   注意：Citrix 建议使用文件名 ns.conf 保存文件。

查看当前正在运行的配置

对 Citrix Gateway 进行的任何更改如果不努力保存，则称为正在运行的配置。这些设置在 Citrix Gateway 上处于活动状态，但不会保存在设备上。如果配置了其他设置（如策略、虚拟服务器、用户或组），则可以在正在运行的配置中查看这些设置。

1. 在配置实用程序的配置选项卡上的导航窗格中，展开系统，然后单击诊断。
2. 在详细信息窗格中的“查看配置”下，单击“运行配置”。

比较已保存和正在运行的配置

您可以查看哪些设置保存在设备上，并将这些设置与正在运行的配置进行比较。您可以选择保存正在运行的配置或对配置进行更改。

1. 在配置实用程序的配置选项卡上的导航窗格中，展开系统，然后单击诊断。
2. 在详细信息窗格中的查看配置下，单击正在运行的已保存 V/s。

清除 **Citrix Gateway** 配置

April 6, 2020

您可以清除 Citrix Gateway 上的配置设置。您可以从以下三个级别的设置中进行选择以清除：

重要提示：Citrix 建议在清除 Citrix Gateway 配置设置之前保存您的配置。

- Basic)。清除设备上的所有设置，但系统 IP 地址、默认网关、映射 IP 地址、子网 IP 地址、DNS 设置、网络设置、高可用性设置、管理密码以及功能和模式设置除外。
- 延长。清除除系统 IP 地址、映射 IP 地址、子网 IP 地址、DNS 设置和高可用性定义之外的所有设置。
- 满。将配置还原到原始出厂设置，不包括系统 IP (NSIP) 地址和默认路由，这些地址是维持与设备的网络连接所需的。

清除全部或部分配置时，功能设置将设置为出厂默认设置。

清除配置后，不会删除存储在 Citrix Gateway 上的文件（例如证书和许可证）。文件 ns.conf 不会更改。如果要在清除配置之前保存配置，请先将配置保存到您的计算机。如果保存配置，则可以在 Citrix Gateway 上还原 ns.conf 文件。将文件还原到设备并重新启动 Citrix Gateway 后，ns.conf 中的任何配置设置都会恢复。

不会还原对配置文件（如 rc.conf）的修改。

如果您具有高可用性对，则两个 Citrix Gateway 设备都会以相同的方式修改。例如，如果清除一台设备上的基本配置，则更改将传播到第二台设备。

清除 **Citrix Gateway** 配置设置

1. 在配置实用程序的配置选项卡上的导航窗格中，展开系统，然后单击诊断。
2. 在详细信息窗格的 “维护” 下，单击 “清除配置”。
3. 在 “配置级别” 中，选择要清除的级别，然后单击 “运行”。

使用向导配置 **Citrix Gateway**

April 6, 2020

Citrix Gateway 具有以下六个向导，您可以使用这些向导在设备上配置设置：

- 首次登录 Citrix Gateway 设备时，将显示首次安装向导。
- 安装向导可帮助您首次配置基本 Citrix Gateway 设置。

- Citrix Endpoint Management 集成配置可帮助您配置 Citrix Gateway 和 Citrix Endpoint Management 环境。
- “快速配置”向导可帮助您配置与 Citrix Endpoint Management、StoreFront 和 Web Interface 的连接的正确策略、表达式和设置。
- Citrix Gateway 向导可帮助您配置 Citrix Gateway 特定的设置。
- “已发布应用程序”向导可帮助您通过使用 Citrix Workspace 应用程序配置用户连接的设置。

首次安装向导的工作原理

在 Citrix Gateway 设备上完成初始设置的安装和配置后，首次登录配置实用程序时，如果不满足以下条件，将显示首次安装向导：

- 您未在设备上安装许可证。
- 您未配置子网或映射 IP 地址。
- 如果设备的默认 IP 地址是 192.168.100.1。

安装向导的工作原理

您可以使用安装向导在设备上配置以下初始设置：

- 系统 IP 地址和子网掩码
- 映射的 IP 地址和子网掩码
- 主机名
- 默认网关
- 许可证

注意：在运行安装向导之前，请从 Citrix 网站下载您的许可证。有关详细信息，请参阅
许可使用 Citrix Gateway。

集成 **Citrix Endpoint Management** 配置的工作原理

可以使用 Citrix Endpoint Management MDM 部署 Citrix Gateway，该 MDM 提供了扩展应用程序、确保应用程序的高可用性和维护安全性的功能。要使用 Citrix Endpoint Management 配置，需要安装版本 10.1 Build 120.1316.e。

集成 Citrix Endpoint Management 配置将创建以下对象：

- 设备管理器的负载平衡服务器。
- 负载平衡 Microsoft Exchange 服务器与电子邮件筛选。
- ShareFile 的负载平衡服务器。

有关使用集成 Citrix Endpoint Management 配置创建设置的详细信息，请参阅为 Citrix Endpoint Management 环境配置设置

快速配置向导的工作原理

快速配置向导允许您在 Citrix Gateway 上配置多个虚拟服务器。您可以添加、编辑和删除虚拟服务器。

快速配置向导允许对以下部署进行无缝配置：

- 与 Citrix Virtual Apps and Desktops 的 Web Interface 连接，能够配置 Secure Ticket Authority (STA) 的多个实例
- 仅限 Citrix Endpoint Management
- 仅限 StoreFront
- Citrix Endpoint Management 和 StoreFront 结合在一起

快速配置向导允许您在设备上配置以下设置：

- 虚拟服务器名称、IP 地址和端口
- 从不安全端口重定向到安全端口
- LDAP 服务器
- RADIUS 服务器
- 证书
- DNS 服务器
- Citrix Endpoint Management 和 Citrix Virtual Appsand Desktops

Citrix Gateway 支持用户直接连接到 Citrix Endpoint Management，这使用户可以访问其 Web、SaaS 和移动应用程序以及访问 ShareFile。您还可以配置 StoreFront 的设置，从而允许用户访问其基于 Windows 的应用程序和虚拟桌面。

运行“快速配置”向导时，系统会根据 Citrix Endpoint Management、StoreFront 和 Web Interface 设置创建以下策略：

- 会话策略，包括 Receiver、Receiver for Web、Citrix Gateway 插件和程序邻域代理的策略和配置文件
- 无客户端访问
- LDAP 和 RADIUS 身份验证

Citrix Gateway 向导的工作原理

您可以使用 Citrix Gateway 向导在设备上配置以下设置：

- 虚拟服务器
- 证书
- 名称服务提供商
- 身份验证
- 授权
- 端口重定向
- 无客户端访问
- SharePoint 的无客户端访问权限

已发布的应用程序向导的工作原理

可以使用“已发布应用程序”向导将 Citrix Gateway 配置为连接到内部网络中运行 Citrix Virtual Apps and Desktops 的服务器。使用“已发布应用程序”向导，您可以：

- 选择用于连接到服务器场的虚拟服务器。
- 配置 Web Interface 或 StoreFront 的用户连接、单点登录和安全票证颁发机构的设置。
- 创建或选择 SmartAccess 的会话策略。

在向导中，您还可以为用户连接创建会话策略表达式。有关配置 Citrix Gateway 以连接到服务器场的更多信息，请参阅通过 Web Interface 提供对已发布应用程序和虚拟桌面的访问权限。

使用首次安装向导配置 **Citrix Gateway**

April 6, 2020

要首次配置 Citrix Gateway （物理设备或 VPX 虚拟设备），您需要在与该设备相同的网络上配置一台管理计算机。

您必须分配 Citrix Gateway IP (NSIP) 地址作为设备的管理 IP 地址和服务器可连接的子网 IP (SNIP) 地址。您可以分配一个应用于 Citrix Gateway 和 SNIP 地址的子网掩码。您还必须配置时区。如果分配主机名，则可以通过指定设备名称而不是 NSIP 地址来访问设备。

首次安装向导中有两个部分。在第一部分中，您将为 Citrix Gateway 设备配置基本系统设置，包括：

- NSIP 地址、SNIP 地址和子网掩码
- 设备主机名称
- DNS 服务器
- 时区
- 管理员密码

在第二部分中，您将安装许可证。如果指定 DNS 服务器的地址，则可以使用硬件序列号 (HSN) 或许可证激活码 (LAC) 分配许可证，而不是将许可证从本地计算机上传到设备。

注意：Citrix 建议将您的许可证保存到本地计算机。

完成配置这些设置后，Citrix Gateway 会提示您重新启动设备。再次登录到设备时，可以使用其他向导和配置实用程序配置其他设置。

使用快速配置向导配置设置

April 6, 2020

可以使用“快速配置”向导在 Citrix Gateway 中配置设置，以启用与 Citrix Endpoint Management、StoreFront 或 Web Interface 的通信。完成配置后，向导会为 Citrix Gateway、Endpoint Management、StoreFront 或

Web Interface 之间的通信创建正确的策略。这些策略包括身份验证、会话和无客户端访问策略。向导完成后，策略将绑定到虚拟服务器。

完成快速配置向导后，Citrix Gateway 可以与 Endpoint Management 或 StoreFront 进行通信，用户可以访问其基于 Windows 的应用程序和虚拟桌面以及 Web、SaaS 和移动应用程序。然后，用户可以直接连接到 Endpoint Management。

在向导期间，您可以配置以下设置：

- 虚拟服务器名称、IP 地址和端口
- 从不安全端口重定向到安全端口
- 证书
- LDAP 服务器
- RADIUS 服务器
- 用于身份验证的客户端证书（仅适用于双重身份验证）
- Endpoint Management、StoreFront 或 Web Interface

快速配置向导支持 LDAP、RADIUS 和客户端证书身份验证。您可以按照以下准则在向导中配置双重身份验证：

- 如果选择 LDAP 作为主身份验证类型，则可以将 RADIUS 配置为辅助身份验证类型。
- 如果选择 RADIUS 作为主身份验证类型，则可以将 LDAP 配置为辅助身份验证类型。
- 如果选择客户端证书作为主身份验证类型，则可以将 LDAP 或 RADIUS 配置为辅助身份验证类型。

无法使用快速配置向导创建多个 LDAP 身份验证策略。例如，您希望配置一个在服务器登录名称属性字段中使用 sAMAccountName 的策略，并配置另一个 LDAP 策略，该策略使用服务器登录名称属性字段中的用户主体名称 (UPN)。要配置这些单独的策略，请使用 Citrix Gateway 配置实用程序创建身份验证策略。有关详细信息，请参阅配置 LDAP 身份验证。

您可以使用以下方法在快速配置向导中为 Citrix Gateway 配置证书：

- 选择安装在设备上的证书。
- 安装证书和私钥。
- 选择一个测试证书。
  注意：如果您使用测试证书，则必须添加证书中的完全限定域名 (FQDN)。

您可以通过以下两种方式之一打开快速配置向导：

- 当您在 Citrix Gateway 登录页面上并在部署类型中选择 Citrix Gateway 时，将显示“主页”选项卡。如果在“部署类型”中选择任何其他选项，则不会显示“主页”。
- 从 Citrix Gateway 详细信息窗格中的链接创建/监视 Citrix Gateway。如果您安装启用 Citrix ADC 功能的许可证，则会显示该链接。如果仅为 Citrix Gateway 许可设备，则不会显示链接。

最初运行向导后，您可以再次运行向导以创建其他虚拟服务器和设置。

重要说明：如果使用快速配置向导配置其他 Citrix Gateway 虚拟服务器，则必须使用唯一的 IP 地址。不能使用现有虚拟服务器上使用的相同 IP 地址。例如，您的虚拟服务器的 IP 地址为 192.168.10.5，端口号为 80。运行快速配置向导以创建第二个虚拟服务器的 IP 地址 192.168.10.5 端口号 443。当您尝试保存配置时，会出现错误。

使用快速配置向导配置设置

1. 在配置实用程序中，执行以下操作之一：
   a) 如果设备仅为 Citrix Gateway 许可，请单击“主页”选项卡。
   b) 如果设备获得许可以包含 Citrix ADC 功能，则在“配置”选项卡上的导航窗格中，单击 Citrix Gateway，然后在详细信息窗格中的“入门”下，单击“为企业应用商店配置 Citrix Gateway”。
2. 在仪表板中，单击创建新 Citrix Gateway。
3. 在 Citrix Gateway 设置中，配置以下内容：
   a) 在“名称”中，键入虚拟服务器的名称。
   b) 在 IP 地址中，键入虚拟服务器的 IP 地址。
   c) 在端口中，键入端口号。默认端口号为 443。
   d) 选择将请求从端口 80 重定向到安全端口，以允许用户从端口 80 连接到端口 443。
4. 单击继续。
5. 在“证书”页上，执行以下操作之一：
   a) 单击“选择证书”，然后在“证书”中选择证书。
   b) 单击“安装证书”，然后在“选择证书”和“选择密钥”中单击“浏览”以导航到证书和私钥。
   c) 单击使用测试证书，然后在证书 FQDN 中输入测试证书中包含的完全限定域名 (FQDN)。
6. 单击继续。
7. 在身份验证设置中，执行以下操作：
   a) 在主身份验证中，选择 LDAP、RADIUS 或证书。
   b) 选择身份验证服务器或配置您在上一步中选择的身份验证类型的设置。如果选择 Cert，请选择客户端证书或安装新的客户端证书。
   c) 在辅助身份验证中，选择身份验证类型，然后配置身份验证服务器设置。
8. 单击继续。

配置完网络和身份验证设置后，可以配置 Citrix Endpoint Management 或 Citrix Virtual Apps and Desktops（StoreFront 或 Web Interface）设置。

配置企业应用商店设置

Citrix Gateway 仅支持用户通过 Endpoint Management 访问 Web、SaaS 和移动应用程序以及 ShareFile。如果您还部署 StoreFront 或 Web Interface，则用户可以访问基于 Windows 的应用程序和虚拟桌面。您可以为以下选项配置设置：

- 仅限 Endpoint Management
- 仅限 StoreFront
- Endpoint Management 和 StoreFront 结合在一起
- 仅限 Web Interface

单击上述过程中的继续时，您可以配置部署方案的设置。以下过程从 Citrix 集成设置页面开始。

创建虚拟服务器后，在“快速配置”向导中编辑虚拟服务器不允许您更改 Citrix Endpoint Management 或 Citrix Virtual Appsand Desktops 设置。

例如，如果在配置 Citrix 企业应用商店设置之前在任何阶段取消虚拟服务器的配置，则向导会自动选择 Web Interface 而不配置任何设置。出现此情况时，可以编辑用于配置 Web Interface 的虚拟服务器详细信息，但无法切换到 Citrix Endpoint Management。要切换，您必须创建新的虚拟服务器，并且在配置过程中不得随时取消向导。如果您不需要 Web Interface 虚拟服务器，可以使用快速配置向导将其删除。

仅为 **StoreFront** 配置设置

1. 单击 “Citrix Virtual Apps and Desktops”。
2. 在 “部署类型” 中，选择 “StoreFront”。
3. 在 StoreFront FQDN 中，输入 StoreFront 服务器的完全限定域名 (FQDN)。
4. 在 Receiver for Web 路径中，保留默认路径或输入您自己的路径。
5. 选择 HTTPS 进行安全用户连接。
6. 在 “单点登录域” 中，输入 StoreFront 的域。
7. 在 STA URL 中，如果您部署 StoreFront 并提供对 Citrix Virtual Apps 中的已发布应用程序或 Citrix Virtual Desktops 中的虚拟桌面的访问权限，请输入运行 Secure Ticket Authority (STA) 的服务器的完整 IP 地址或 FQDN。
8. 单击完成。

用户通过 Citrix Gateway 连接到 StoreFront 时，用户可以从 Receiver for Web 或 Receiver 启动其应用程序和桌面。

仅配置 **Endpoint Management** 的设置

1. 单击 “Citrix Endpoint Management”。
2. 在 App Controller FQDN 中，输入 Endpoint Management 的 FQDN。
3. 单击完成。

配置 **Web Interface** 设置

1. 在 “快速配置” 向导中，单击 “Citrix Virtual Apps and Desktops”。
2. 在 “部署类型” 中，选择 “Web Interface”，然后配置以下内容：
   a) 在 “Citrix Virtual Apps 站点 URL” 中，键入 Web Interface 的完整 IP 地址或 FQDN。
   b) 在 “Citrix Virtual Apps 服务站点 URL” 中，键入带 PNAgent 路径的 Web Interface 的完整 IP 地址或 FQDN。您可以输入默认路径或输入您自己的路径。
   c) 在单点登录域中，输入要使用的域。
   d) 在 STA URL 中，键入运行 STA 的服务器的完整 IP 地址或 FQDN。
3. 单击完成。

使用 **Citrix Gateway** 向导配置设置

April 6, 2020

运行安装向导后，可以运行 Citrix Gateway 向导以在 Citrix Gateway 上配置其他设置。您可以从配置实用程序运行 Citrix Gateway 向导。

Citrix Gateway 附带测试证书。如果您没有来自证书颁发机构 (CA) 的签名证书，则可以在使用 Citrix Gateway 向导时使用测试证书。收到签名证书后，您可以删除测试证书并安装签名证书。Citrix 建议在将 Citrix Gateway 公开供用户使用之前获取已签名的证书。

注意：您可以在 Citrix Gateway 向导中创建证书签名请求 (CSR)。如果使用 Citrix Gateway 向导创建 CSR，则必须退出向导，然后在收到来自 CA 的签名证书时再次启动向导。有关证书的更多信息，请参阅安装和管理证书。

配置虚拟服务器时，可以在 Citrix Gateway 向导中为 Internet 协议版本 6 (IPv6) 配置用户连接。有关将 IPv6 用于用户连接的更多信息，请参阅为用户连接配置 IPv6。

启动 **Citrix Gateway** 向导

1. 在配置实用程序中，单击配置选项卡，然后在导航窗格中单击 Citrix Gateway。
2. 在详细信息窗格的“入门”下，单击 Citrix Gateway 向导。
3. 单击“下一步”，然后按照向导中的说明操作。

在 **Citrix Gateway** 上配置主机名和 **FQDN**

April 6, 2020

主机名是与许可证文件关联的 Citrix Gateway 设备的名称。主机名对于设备是唯一的，在下载通用许可证时使用。在运行安装向导以首次配置 Citrix Gateway 时定义主机名。

完全限定域名 (FQDN) 包含在绑定到虚拟服务器的签名证书中。您不在 Citrix Gateway 上配置 FQDN。一个设备可以将唯一的 FQDN 分配给使用证书在 Citrix Gateway 上配置的每个虚拟服务器。

您可以通过查看证书的详细信息找到证书的 FQDN。FQDN 位于证书的主题字段中。

查看证书的 **FQDN**

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 SSL，然后单击“证书”。
2. 在详细信息窗格中，选择证书，单击操作，然后单击详细信息。
3. 在“证书详细信息”对话框中，单击“主题”。证书的 FQDN 将显示在列表中。

安装和管理证书

April 6, 2020

在 Citrix Gateway 上，您可以使用证书创建安全连接并对用户进行身份验证。

要建立安全连接，需要在连接的一端提供服务器证书。连接的另一端需要颁发服务器证书的证书颁发机构 (CA) 的根证书。

- 服务器证书。服务器证书证明服务器的身份。Citrix Gateway 需要此类数字证书。
- 根证书。根证书标识为服务器证书签名的 CA。根证书属于 CA。用户设备需要此类数字证书来验证服务器证书。

在用户设备上与 Web 浏览器建立安全连接时，服务器将其证书发送到设备。

当用户设备收到服务器证书时，Web 浏览器（例如 Internet Explorer）会检查哪个 CA 颁发了证书，以及 CA 是否受到用户设备的信任。如果 CA 不受信任，或者如果它是测试证书，则 Web 浏览器会提示用户接受或拒绝证书（有效地接受或拒绝访问站点的能力）。

Citrix Gateway 支持以下三种类型的证书：

- 绑定到虚拟服务器并且也可用于连接到服务器场的测试证书。Citrix Gateway 附带预安装的测试证书。
- PEM 或 DER 格式的证书，由 CA 签名并与私钥配对。
- PKCS #12 格式的证书，用于存储或传输证书和私钥。PKCS#12 证书通常从现有 Windows 证书导出为 PFX 文件，然后安装在 Citrix Gateway 上。

Citrix 建议使用由受信任 CA（如 Thawte 或 VeriSign）签名的证书。

创建证书签名请求

November 7, 2022

要使用 SSL 或 TLS 提供安全通信，Citrix Gateway 上需要服务器证书。您需要生成证书签名请求 (CSR) 和私钥，然后才能将证书上传到 Citrix Gateway。您可以使用 Citrix Gateway 向导中包含的创建证书请求或配置实用程序来创建 CSR。创建证书请求创建一个.csr 文件，该文件将通过电子邮件发送给证书颁发机构 (CA) 进行签名，并创建一个保留在设备上的私钥。CA 对证书进行签名，然后通过您提供的电子邮件地址将其返回给您。收到签名证书后，可以将其安装在 Citrix Gateway 上。当您从 CA 收到证书时，将证书与私钥进行配对。

重要说明：使用 Citrix Gateway 向导创建 CSR 时，必须退出向导并等待 CA 向您发送签名证书。收到证书后，您可以再次运行 Citrix Gateway 向导以创建设置并安装证书。有关 Citrix Gateway 向导的更多信息，请参阅 使用 Citrix Gateway 向导配置设置。

使用 **Citrix Gateway** 向导创建 **CSR**

1. 在配置实用程序中，单击 “配置” 选项卡，然后在导航窗格中单击 Citrix ADC 网关。

2. 在详细信息窗格的“入门”下，单击 Citrix ADC 网关向导。
3. 按照向导中的说明操作，直到进入“指定服务器证书”页。
4. 单击创建证书签名请求并填写字段。
   注意：完全限定的域名 (FQDN) 不需要与 Citrix Gateway 主机名相同。FQDN 用于用户登录。
5. 单击“创建”以将证书保存在您的计算机上，然后单击“关闭”。
6. 退出 Citrix Gateway 向导，而不保存您的设置。

使用 **Citrix ADC GUI** 创建 **CSR**

您也可以使用 Citrix ADC GUI 创建 CSR，而无需运行 Citrix Gateway 向导。

1. 导航到流量管理 > **SSL** > **SSL** 文件，然后选择创建证书签名请求 **(CSR)**。
2. 完成证书的设置，然后单击 创建。

创建证书和私钥后，请将证书电子邮件发送给 CA，例如 Thawte 或 VeriSign。

在 **Citrix Gateway** 上安装签名证书

April 6, 2020

收到来自证书颁发机构 (CA) 的签名证书时，请将其与设备上的私钥配对，然后在 Citrix Gateway 上安装证书。

将签名证书与私钥配对

1. 通过使用安全外壳 (SSH) 程序（如 WinSCP）将证书复制到 Citrix Gateway 到文件夹 nsconfig/ssl。
2. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 SSL，然后单击“证书”。
3. 在详细信息窗格中，单击 Install（安装）。
4. 在证书密钥对名称中，键入证书的名称。
5. 在“证书文件名”中，选择“浏览”中的下拉框，然后单击“设备”。
6. 导航到证书，单击选择，然后单击打开。
7. 在“私有密钥文件名”中，选择“浏览”中的下拉框，然后单击“设备”。私钥的名称与证书签名请求 (CSR) 相同。
   私钥位于 Citrix Gateway 上的目录 \nsconfig\ssl 中。
8. 选择私钥，然后单击打开。
9. 如果证书是 PEM 格式，请在“密码”中键入私钥的密码。
10. 如果要为证书过期时配置通知，请选择“过期时通知”。
11. 在通知期间，键入天数，单击创建，然后单击关闭。

将证书和私钥绑定到虚拟服务器

创建证书和私钥对并链接后，将其绑定到虚拟服务器。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击虚拟服务器，然后单击打开。
3. 在“证书”选项卡上的“可用”下，选择一个证书，单击“添加”，然后单击“确定”。

从虚拟服务器取消绑定测试证书

安装签名证书后，取消绑定到虚拟服务器的所有测试证书。您可以使用配置实用程序取消绑定测试证书。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击虚拟服务器，然后单击打开。
3. 在“证书”选项卡上的“已配置”下，选择测试证书，然后单击“删除”。

配置中间证书

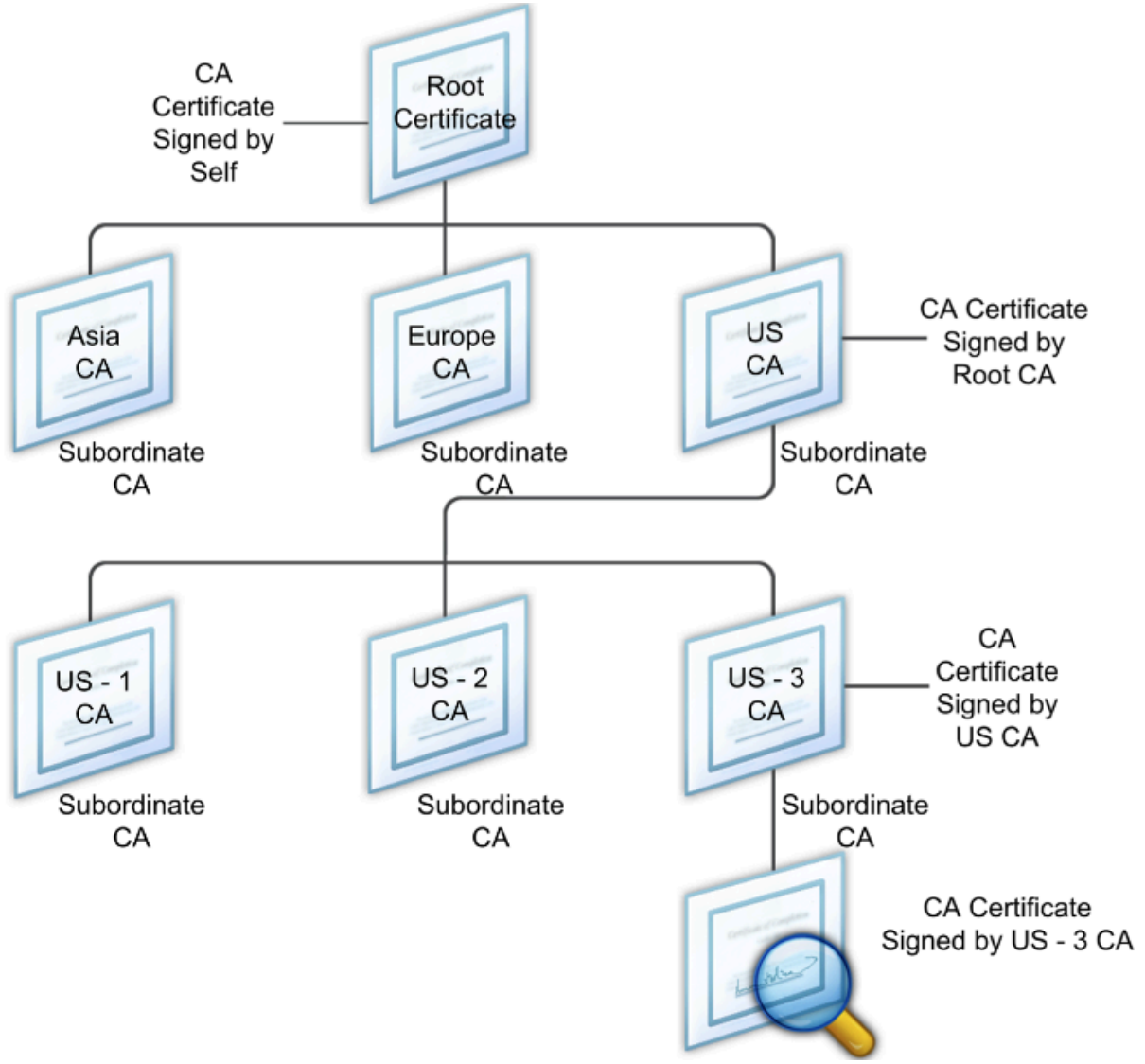
April 6, 2020

中间证书是在 Citrix Gateway（服务器证书）和根证书（通常安装在用户设备上）之间的证书。中间证书是链的一部分。

有些组织将颁发证书的责任下放给组织各单位之间的地域分离问题或将不同的颁发政策适用于组织的不同部门。

可以通过设置从属证书颁发机构 (CA) 来委派颁发证书的责任。CA 可以签署自己的证书（即，它们是自签名的），也可以由其他 CA 签署。X.509 标准包含用于设置 CA 层次结构的模型。在此模型中，如下图所示，根 CA 位于层次结构的顶部，是 CA 的自签名证书。直接从属于根 CA 的 CA 具有由根 CA 签名的 CA 证书。层次结构中从属 CA 下的 CA 证书由从属 CA 签名。

图 1. 显示典型数字证书链分层结构的 X.509 模型



如果服务器证书由具有自签名证书的 CA 签名，则证书链仅由两个证书组成：最终实体证书和根 CA。如果用户或服务器证书由中间 CA 签名，则证书链更长。

下图显示前两个元素是最终实体证书（在本例中为 gwy01.company.com）和中间 CA 的证书，按照该顺序。中间 CA 的证书后跟其 CA 的证书。此列表一直持续到列表中的最后一个证书针对根 CA。链中的每个证书都证明了上一个证书的标识。

图 2. 典型的数字证书链

安装中间证书的步骤

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 SSL，然后单击“证书”。
2. 在详细信息窗格中，单击 Install（安装）。
3. 在证书密钥对名称中，键入证书的名称。
4. 在“详细信息”下的“证书文件名”中，单击“浏览（设备）”，然后在下拉框中选择“本地”或“设备”。
5. 导航到计算机（本地）或 Citrix Gateway （设备）上的证书。
6. 在证书格式中，选择 PEM。
7. 单击安装，然后单击关闭。

在 Citrix Gateway 上安装中间证书时，无需指定私钥或密码。

在设备上安装证书后，证书需要链接到服务器证书。

将中间证书链接到服务器证书

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 SSL，然后单击“证书”。
2. 在详细信息窗格中，选择服务器证书，然后在操作中单击链接。
3. 在 CA 证书名称旁边，从列表中选择中间证书，然后单击确定。

使用设备证书进行身份验证

November 21, 2022

Citrix Gateway 支持设备证书检查，使您能够将设备标识绑定到证书的私钥。设备证书检查可以配置为经典或高级 EPA 策略的一部分。在传统的 EPA 策略中，设备证书只能配置用于预身份验证 EPA。

如果在 Citrix Gateway 上安装了两个或多个设备证书，则用户需要在开始登录 Citrix Gateway 时或在终端分析扫描运行之前选择正确的证书。

创建设备证书时，必须是 X.509 证书。

> 重要提示：默认情况下，Windows 授权访问设备证书的管理员权限。要为非管理员用户添加设备证书检查，必须安装 VPN 插件。VPN 插件版本必须与设备上的 EPA 插件版本相同。

有关创建设备证书的详细信息，请参阅以下内容：

- Microsoft Web 站点上的 Active Directory 证书服务 (AD CS) 中的网络设备注册服务 (NDES)。
- Microsoft System Center Web 站点上的 配置管理器的 PKI 证书的分步部署示例：Windows Server 2008 证书颁发机构。
- Apple 支持网站上的 如何使用 DCE/RPC 和 Active Directory 证书配置文件负载从 Microsoft 证书颁发机构申请证书。
- iPad/iPhone 证书颁发上询问目录服务团队 Microsoft 支持博客。
- 设置网络设备注册服务在 Windows IT Pro 网站上。

在虚拟服务器上启用和绑定经典 **EPA** 策略的设备证书

创建设备证书后，您可以使用的过程在 Citrix Gateway 上安装证书将现有证书导入并安装到 Citrix Gateway。安装证书后，将证书绑定到虚拟服务器。

1. 在配置实用程序中，导航到 **Citrix Gateway** > 虚拟服务器。
2. 在详细信息窗格中，单击虚拟服务器，然后单击 编辑。
3. 在虚拟服务器详细信息窗格中，单击铅笔图标，然后展开更多。
4. 选择 启用设备证书。
5. 在出现的选择对话框中，选择“添加”，然后单击要启用的设备证书。单击所选设备证书旁边的加号图标，然后单击确定。

> 注意：有关在虚拟服务器上启用和绑定设备证书以实现高级 EPA 策略的信息，请参阅nFactor 中的设备证书作为 EPA 组件 。

导入和安装现有证书

April 6, 2020

您可以从运行 Internet 信息服务 (IIS) 的基于 Windows 的计算机或运行安全网关的计算机导入现有证书。

导出证书时，请确保还导出私钥。在某些情况下，无法导出私钥，这意味着无法在 Citrix Gateway 上安装证书。如果发生这种情况，请使用证书签名请求 (CSR) 创建新证书。有关详细信息，请参阅 创建证书签名请求。

当您从 Windows 导出证书和私钥时，计算机将创建一个个人信息交换 (.pfx) 文件。然后将此文件作为 PKCS #12 证书安装在 Citrix Gateway 上。

如果要将安全网关替换为 Citrix Gateway，则可以从安全网关导出证书和私钥。如果要从安全网关到 Citrix Gateway 的就地迁移，则应用程序和设备上的完全限定域名 (FQDN) 必须相同。从安全网关导出证书时，立即停用安全网关，在 Citrix Gateway 上安装证书，然后测试配置。如果安全网关和 Citrix Gateway 具有相同的 FQDN，则无法同时在您的网络上运行。

如果您使用的是 Windows Server 2003 或 Windows Server 2008，则可以使用 Microsoft 管理控制台导出证书。有关详细信息，请参阅 Windows 联机帮助。

保留所有其他选项的默认值，定义密码，然后将.pfx 文件保存到您的计算机。导出证书后，您将其安装在 Citrix Gateway 上。

在 **Citrix Gateway** 上安装证书和私钥

1. 在配置实用程序中，单击配置选项卡，然后在导航窗格中单击 Citrix Gateway。
2. 在详细信息窗格的“入门”下，单击 Citrix Gateway 向导。
3. 单击“下一步”，选择现有虚拟服务器，然后单击“下一步”。

4. 在“证书选项”中，选择“安装 PKCS #12 (.pfx) 文件”。
5. 在 PKCS #12 文件名中，单击浏览，导航到证书，然后单击选择。
6. 在“密码”中，键入私钥的密码。

   这是您在将证书转换为 PEM 格式时使用的密码。
7. 单击“下一步”完成 Citrix Gateway 向导，而不更改任何其他设置。

在 Citrix Gateway 上安装证书后，证书将显示在“SSL”>“证书”节点的配置实用程序中。

创建私有密钥

1. 在配置实用程序中的“配置”选项卡的导航窗格中，单击“SSL”。
2. 在详细信息窗格的 SSL 密钥下，单击创建 RSA 密钥。
3. 在“密钥文件名”中，键入私有密钥的名称，或单击“浏览”以导航到现有文件。
4. 在密钥大小 (位) 中，键入私钥的大小。
5. 在公共指数值中，选择 F4 或 3。

   RSA 密钥的公共指数值。这是密码算法的一部分，是创建 RSA 密钥所必需的。这些值是 F4（十六进制：0x10001）或 3（十六进制：0x3）。默认值为 F4。
6. 在密钥格式中，选择 PEM 或 DER。Citrix 建议证书使用 PEM 格式。
7. 在 PEM 编码算法中，选择 DES 或 DES3。
8. 在 PEM 密码和验证密码中，键入密码，单击创建，然后单击关闭。

   注意：要分配密码，
   密钥格式必须是 PEM，您必须选择编码算法。

要在配置实用程序中创建 DSA 私钥，请单击创建 DSA 密钥。按照上述相同步骤创建 DSA 私钥。

将证书从 **PFX** 格式转换为 **PEM** 格式

April 6, 2020

SSL 证书用于 SSL 负载平衡虚拟服务器和 Citrix Gateway 虚拟服务器。PEM 证书是 Base64 编码的 ASCII 文件。PEM 证书可以在文本编辑器/记事本中打开，您会发现它们包含“—–BEGIN CERTIFICATE—–”和“—–END CERTIFICATE—–”语句。

要获得安全的可信访问，必须在 Citrix Gateway 服务器上安装 SSL 服务器证书。上传的证书文件必须具有以下特征：

- 服务器证书必须由最终用户信任的证书颁发机构 (CA) 颁发。为了获得最佳效果，请使用商业 CA，例如 VeriSign、Thawte 或 GeoTrust。

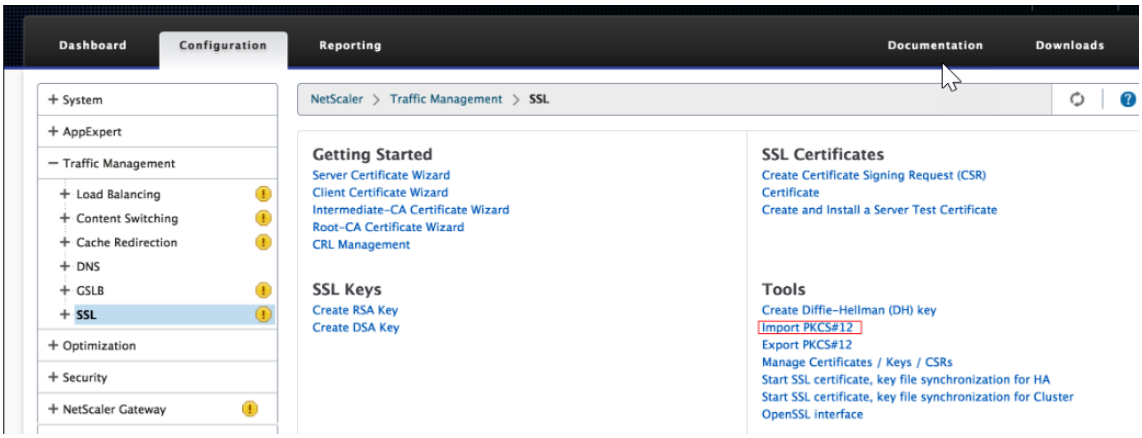
- 证书必须采用隐私增强邮件 (PEM) 格式，这是一种基于文本的格式，是二进制可分辨编码规则 (DER) 格式的 Base64 编码。
- 证书文件必须包含私钥，且私钥不得加密。使用 PEM 文件不需要密码。
- 任何必要的中间证书还必须附加到 PEM 文件的末尾。

完成以下过程之一，将 PFX 证书转换为 PEM 格式以便与 Citrix Gateway 一起使用：

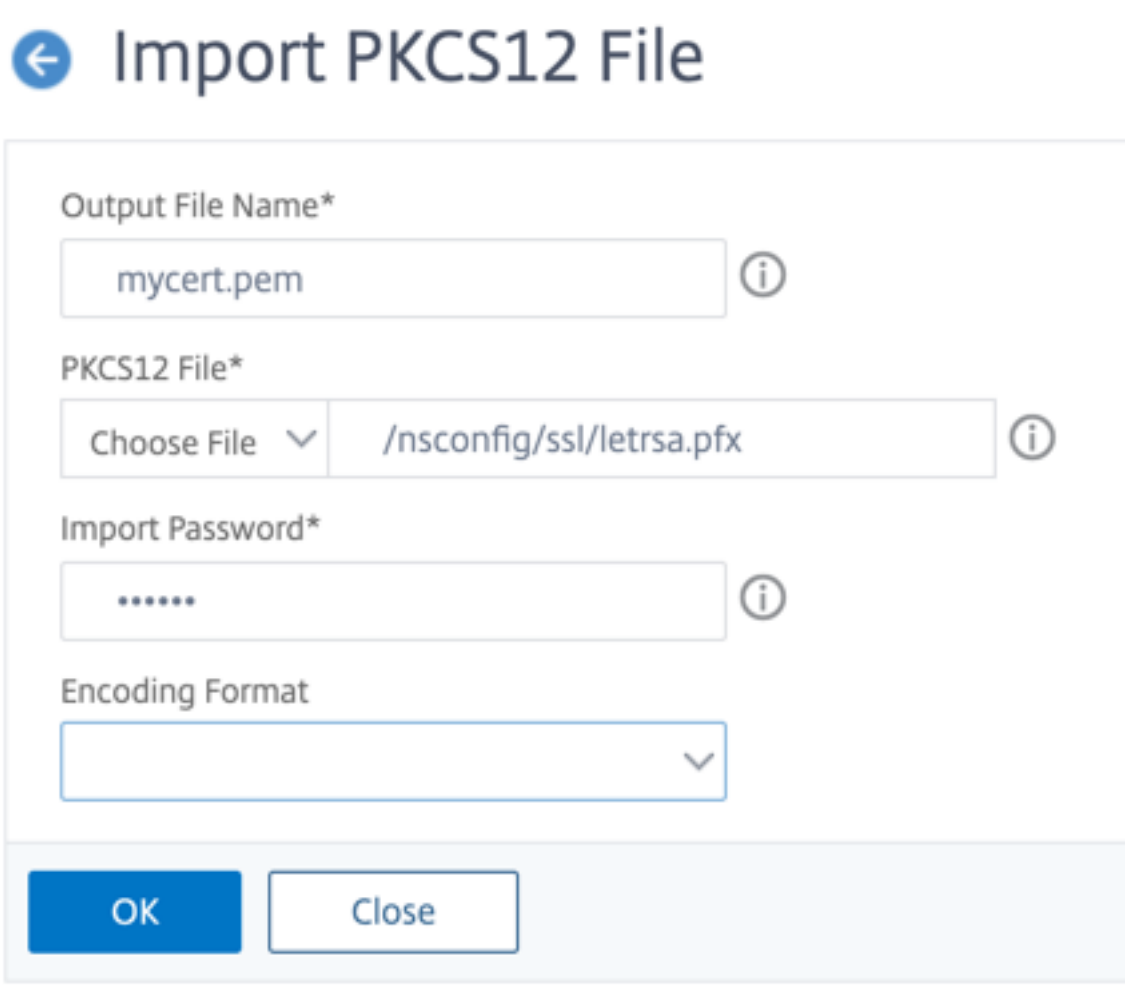
Citrix Gateway 向导

完成以下过程，以使用 Citrix Gateway 向导将 PFX 证书转换为 PEM 格式：

1. 导航到流量管理，选择 SSL 节点。
2. 单击导入 PKCS #12 链接。

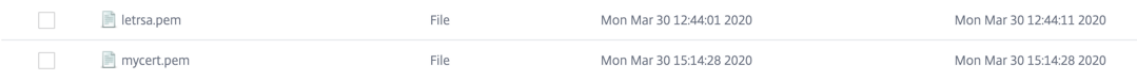


3. 在“输出文件名”字段中为 PEM 证书指定所需的文件名。
4. 单击浏览并选择要转换为 PEM 格式的 PFX 证书。有些用户喜欢将证书上传到 /ncsonfig/SSL 目录并从该目录使用。如果 PFX 证书存储在 Citrix Gateway 上，则选择选项设备，如果它存储在工作站上，则使用本地。



5. 指定导入密码。
6. 单击确定。
7. 如果文件已编码，则选择 DES 或 3DES 作为编码格式：
8. 指定 PEM 密码和验证 PEM 密码。
9. 单击管理证书/密钥/CSR 链接以查看转换后的 PEM 证书文件。

10. 您可以使用转换后的 PEM 文件查看上传的 PFX 文件。



11. 展开 SSL 节点。
12. 选择证书节点。
13. 单击 Install（安装）。
14. 在“安装证书”向导中指定证书密钥对名称。
15. 浏览到 PEM 文件以获取证书文件名和私钥文件名。
16. 指定密码。
17. 单击 Install（安装）。

OpenSSL 实用程序

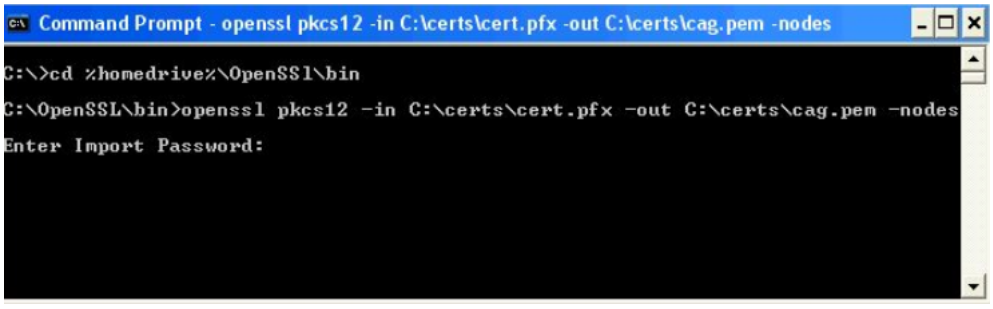
如果您已使用 Internet 信息服务 (IIS) 证书向导请求并将证书安装到 Windows 服务器上，则可以将该证书及其私钥导出到个人信息交换 (PFX) 文件。要将此证书导入 Citrix Gateway，必须将 PFX 文件转换为未加密的 PEM 格式。

您可以使用开源实用程序 OpenSSL 执行从 PFX 到 PEM 的转换。从 Win32 OpenSSL 下载 OpenSSL 的一个 Win32 发行版。

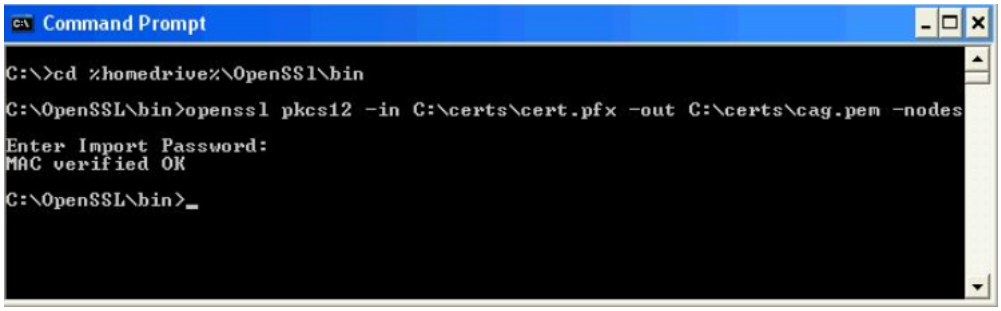
如果您想使用 OpenSSL，您可能还需要 C++ 可再发行文件。从 Microsoft Visual C++ 2008 Redistributable Package (x86) 下载。

要将 PFX 文件转换为 PEM 文件，请在 Windows 计算机上完成以下步骤：

1. 从 Win32 OpenSSL 下载并安装 Win32 OpenSSL 软件包。
2. 创建一个文件夹 c:certs 并将文件复制到 c:certs 文件夹中。
3. 打开命令提示符并更改到 OpenSSL\bin 目录：cd %homedrive%\OpenSSL\bin
4. 运行以下命令将 PFX 文件转换为未加密的 PEM 文件（全部在一行中）：openssl pkcs12 -in c:\certs\yourcert.pfx -out c:\certs\cag.pem –nodes



5. 当提示输入密码时，输入您在将证书导出到 PFX 文件时使用的密码。您应该收到一条消息，显示 MAC 验证确定。



6. 将浏览器指向 Citrix Gateway 管理门户或 HTTPS 端口 9001:https://netscaler-gateway-server:9001。
7. 以 root 身份登录。默认密码是根管理员。
8. 单击页面顶部的维护链接。
9. 单击上传私钥 + 证书 (.pem) 字段旁边的浏览按钮。浏览到 c:certscag.pem 文件，然后单击上传。
10. 重新启动 Citrix Gateway 以便应用新 SSL 证书。

证书吊销列表

April 6, 2020

不时，证书颁发机构 (CA) 颁发证书吊销列表 (CRL)。CRL 包含有关不再受信任的证书的信息。例如，假设安离开 XYZ 公司。公司可以将 Ann 的证书放在 CRL 上，以防止她使用该密钥签名消息。

同样，如果私钥泄露或证书已过期且正在使用新证书，则可以撤销证书。在信任公钥之前，请确保证书不会出现在 CRL 上。

Citrix Gateway 支持以下两种 CRL 类型：

- 列出已吊销或不再有效的证书的 CRL
- 联机证书状态协议 (OCSP)，一种用于获取 X.509 证书吊销状态的 Internet 协议

添加 **CRL**

在 Citrix Gateway 设备上配置 CRL 之前，请确保 CRL 文件本地存储在设备上。在高可用性设置的情况下，CRL 文件必须存在于两个 Citrix Gateway 设备上，并且该文件的目录路径在两个设备上必须相同。

如果需要刷新 CRL，可以使用以下参数：

- CRL 名称：正在 Citrix ADC 上添加的 CRL 的名称。最多 31 个字符。
- CRL 文件：正在 Citrix ADC 上添加的 CRL 文件的名称。Citrix ADC 默认情况下在 /var/netscaler/ssl 目录中查找 CRL 文件。最多 63 个字符。
- URL：最多 127 个字符

- 基本 DN：最多 127 个字符
- 绑定 DN：最多 127 个字符
- 密码：最多 31 个字符
- 天数: 最多 31

1. 在配置实用程序中，在“配置”选项卡上，展开 SSL，然后单击 CRL。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“添加 CRL”对话框中，指定以下值：
    - CRL 名称
    - CRL 文件
    - 格式（可选）
    - CA 证书（可选）
4. 单击 **Create**（创建），然后单击 **Close**（关闭）。在 CRL 详细信息窗格中，选择刚刚配置的 CRL，并验证屏幕底部显示的设置是否正确。

使用配置实用程序中的 **LDAP** 或 **HTTP** 配置 **CRL** 自动刷新

CRL 由 CA 定期生成和发布，在某些情况下，在吊销特定证书后立即生成和发布。Citrix 建议您定期更新 Citrix Gateway 设备上的 CRL，以防止客户端尝试使用无效证书进行连接。

Citrix Gateway 设备可以从 Web 位置或 LDAP 目录刷新 CRL。当您指定刷新参数和 Web 位置或 LDAP 服务器时，在运行命令时，不必在本地硬盘驱动器上存在 CRL。第一次刷新将副本存储在由 CRL File 参数指定的路径中的本地硬盘驱动器上。用于存储 CRL 的默认路径是 /var/netscaler/ssl。

CRL 刷新参数

- **CRL** 名称

在 **Citrix Gateway** 上刷新的 **CRL** 的名称。

```
1  **启 用  CRL  自 动 刷 新**
```

启用或禁用 **CRL** 自动刷新。

```
1  **加 拿 大 证 书**
```

颁发 **CRL** 的 **CA** 证书。必须在设备上安装此 **CA** 证书。**Citrix ADC** 只能从其上安装了证书的 **CA** 更新 **CRL**。

```
1  **方 法**
```


从 **Web** 服务器 **(HTTP)** 或 **LDAP** 服务器获取 **CRL** 刷新的协议。可能的值：**HTTP**、**LDAP**。默认值：**HTTP**。

```
** 作 用 域 **
```

LDAP 服务器上搜索操作的范围。如果指定的作用域为
Base，则搜索与基本 DN 处于同一级别。如果指定的范围为
One，则搜索将扩展到基础 DN 以下的一个级别。

- 服务器 **IP**

从中检索 **CRL** 的 **LDAP** 服务器的 **IP** 地址。选择 **IPv6** 以使用 **IPv6 IP** 地址。

```
** 端 口 **
```

LDAP 或 **HTTP** 服务器通信的端口号。

```
**URL**
```

从中检索 **CRL** 的 **Web** 位置的 **URL**。

```
** 基 本  DN**
```

LDAP 服务器用于搜索 CRL 属性的基本 DN。
注意：Citrix 建议使用基本 DN 属性而不是 CA 证书中的颁发者名称来搜索 LDAP 服务器中的 CRL。发行人名称字段可能不完全匹配 LDAP 目录结构的 DN。

- 绑定 **DN**

用于访问 **LDAP** 存储库中 **CRL** 对象的绑定 **DN** 属性。绑定 **DN** 属性是 **LDAP** 服务器的管理员凭据。配置此参数以限制对 **LDAP** 服务器的未经授权的访问。

```
** 密 码 **
```

用于访问 **LDAP** 存储库中 **CRL** 对象的管理员密码。如果对 **LDAP** 存储库的访问受到限制，即不允许匿名访问，则需要执行此操作。

```
** 时 间 间 隔 **
```


执行 **CRL** 刷新的时间间隔。对于瞬时 **CRL** 刷新，请将间隔指定为 **“NOW”**。可能的值：每月，每日，每周，现在，无。

```
** 天 数 **
```

应执行 **CRL** 刷新的日期。如果间隔设置为每日，则此选项不可用。

```
** 时 间 **
```

应执行 **CRL** 刷新的 **24** 小时格式的确切时间。

```
** 二 进 制 **
```

将基于 LDAP 的 CRL 检索模式设置为二进制。可能的值：是，否。默认值：否。

1. 在导航窗格中，展开 SSL，然后单击 CRL。
2. 选择要更新刷新参数的已配置 CRL，然后单击 “打开”。
3. 选择启用 CRL 自动刷新选项。
4. 在 CRL 自动刷新参数组中，为以下参数指定值：
   注意：星号 (*) 表示必需参数。
   - 方法
   - 二进制
   - 作用域
   - 服务器 IP
   - 端口 *
   - URL
   - 基地 DN*
   - 绑定 DN
   - 密码
   - 时间间隔
   - 天数
   - 时间
5. 单击创建。在 CRL 窗格中，选择刚刚配置的 CRL，并验证屏幕底部显示的设置是否正确。

使用 **OCSP** 监控证书状态

April 6, 2020

联机证书状态协议 (OCSP) 是一种 Internet 协议，用于确定客户端 SSL 证书的状态。Citrix Gateway 支持在 RFC 2560 中定义的 OCSP。OCSP 在及时信息方面比证书吊销列表 (CRL) 具有显著优势。客户证书的最新撤销状态在涉及大笔资金和高价值股票交易的交易中尤其有用。它还使用较少的系统和网络资源。OCSP 的 Citrix Gateway 实现包括请求批处理和响应缓存。

OCSP 的 **Citrix Gateway** 实现

Citrix Gateway 在 SSL 握手期间收到客户端证书时开始对 Citrix Gateway 设备进行 OCSP 验证。要验证证书，Citrix Gateway 创建 OCSP 请求并将其转发给 OCSP 响应程序。为此，Citrix Gateway 可以从客户端证书中提取 OCSP 响应程序的 URL，或使用本地配置的 URL。事务处于挂起状态，直到 Citrix Gateway 评估来自服务器的响应并确定是允许还是拒绝事务。如果来自服务器的响应延迟超过配置的时间，并且未配置其他响应程序，Citrix Gateway 将允许事务或显示错误，具体取决于您将 OCSP 检查设置为可选还是强制。Citrix Gateway 支持 OCSP 请求的批处理和 OCSP 响应的缓存，以减少 OCSP 响应程序的负载并提供更快的响应。

OCSP 请求批处理

Citrix Gateway 每次收到客户端证书时，都会向 OCSP 响应者发送请求。为了帮助避免 OCSP 响应程序过载，Citrix Gateway 可以在同一请求中查询多个客户端证书的状态。为了使请求批处理有效工作，您需要定义超时，以便在等待形成批处理时不会延迟对单个证书的处理。

OCSP 响应缓存

缓存从 OCSP 响应程序收到的响应可以更快地响应用户，并减少 OCSP 响应程序的负载。从 OCSP 响应程序收到客户端证书的吊销状态后，Citrix Gateway 将响应缓存在预定义的时间长度。在 SSL 握手期间收到客户端证书时，Citrix Gateway 首先检查其本地缓存是否有此证书的条目。如果发现仍然有效的条目（在缓存超时限制内），则会对该条目进行评估，并接受或拒绝客户端证书。如果未找到证书，Citrix Gateway 将向 OCSP 响应程序发送请求，并将响应存储在其本地缓存中配置的时间长度。

配置 **OCSP** 证书状态

April 6, 2020

配置联机证书状态协议 (OCSP) 涉及添加 OCSP 响应程序、将 OCSP 响应程序绑定到来自证书颁发机构 (CA) 的签名证书，以及将证书和私钥绑定到安全套接字层 (SSL) 虚拟服务器。如果您需要将不同的证书和私钥绑定到已配置的 OCSP 响应程序，则需要先取消绑定响应程序，然后将响应程序绑定到不同的证书。

配置 **OCSP**

1. 在配置选项卡上的导航窗格中，展开 SSL，然后单击 OCSP 响应程序。

2. 在详细信息窗格中，单击 Add（添加）。
3. 在“名称”中，键入配置文件的名称。
4. 在 URL 中，键入 OCSP 响应程序的 Web 地址。

   此字段为必填字段。Web 地址不能超过 32 个字符。
5. 要缓存 OCSP 响应，请单击“缓存”，然后在“超时”中键入 Citrix Gateway 保存响应的分钟数。
6. 在请求批处理下，单击启用。
7. 在批处理延迟中，指定允许批处理一组 OCSP 请求的时间（以毫秒为单位）。

   这些值可以介于 0 到 10000 之间。默认值为 1。
8. 在“时间偏斜生成”中，键入 Citrix Gateway 在设备需要检查或接受响应时可以使用的时间量。
9. 在响应验证下，如果要禁用 OCSP 响应程序的签名检查，请选择“信任响应”。

   如果启用信任响应，请跳过步骤 8 和步骤 9。
10. 在“证书”中，选择用于签名 OCSP 响应的证书。

    如果未选择证书，则 OCSP 响应程序绑定到的 CA 将用于验证响应。
11. 在“请求超时”中，键入等待 OCSP 响应的毫秒数。

    此时间包括批处理延迟时间。这些值可以介于 0 到 12 万之间。默认值为 2000。
12. 在“签名证书”中，选择用于签名 OCSP 请求的证书和私钥。如果不指定证书和私钥，请求将不签名。
13. 要启用使用一次（任意数）扩展的数字，请选择 Nonce。
14. 若要使用客户端证书，请单击“客户端证书插入”。
15. 单击 Create（创建），然后单击 Close（关闭）。

测试 **Citrix Gateway** 配置

April 6, 2020

在 Citrix Gateway 上配置初始设置后，可以通过连接到设备来测试设置。

要测试 Citrix Gateway 设置，请创建本地用户帐户。然后，使用虚拟服务器 IP 地址或设备的完全限定域名 (FQDN) 打开 Web 浏览器并键入 Web 地址。例如，在地址栏中，键入`https://my.company.com`或`https://192.168.96.183`。

在登录屏幕上，输入您之前创建的用户帐户的用户名和密码。登录后，系统会提示您下载并安装 Citrix Gateway 插件。

安装并成功连接 Citrix Gateway 插件后，将显示访问接口。访问接口是 Citrix Gateway 的默认主页。

使用配置实用程序创建新的用户帐户

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“Citrix Gateway”>“用户管理”，然后单击 AAA 用户。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“用户名”中，键入用户名。
4. 如果使用本地身份验证，请清除“外部身份验证”复选框。使用外部身份验证类型（如 LDAP 或 RADIUS）对用户进行身份验证是默认设置。如果清除此复选框，Citrix Gateway 将对用户进行身份验证。
5. 在“密码”和“确认密码”中，键入用户的密码，单击“创建”，然后单击“关闭”。

使用配置实用程序添加用户时，可以将以下策略绑定到用户：

- 授权
- 流量、会话和审核
- 书签
- 内联网应用程序
- 内联网 IP 地址

如果您在使用测试用户帐户登录时遇到问题，请检查以下内容：

- 如果您收到证书警告，则 Citrix Gateway 上将安装测试证书或无效证书。如果设备上安装了由证书颁发机构 (CA) 签名的证书，请确保用户设备上存在相应的根证书。
- 如果您使用 CA 签名证书，请验证是否通过使用签名证书签名请求 (CSR) 正确生成了站点证书，并且 CSR 中输入的可分辨名称 (DN) 数据是否准确。问题也可能是主机名与签名证书上的 IP 地址不匹配。检查配置的证书的公用名是否对应于已配置的虚拟服务器 IP 地址信息。
- 如果没有出现登录屏幕或者出现任何其他错误消息，请查看安装过程并确认您正确执行了所有步骤并准确地输入了所有参数。

创建虚拟服务器

April 6, 2020

虚拟服务器是用户登录的访问点。每个虚拟服务器都有自己的 IP 地址、证书和策略集。虚拟服务器由 IP 地址、端口和接受传入流量的协议组成。虚拟服务器包含用户登录设备时的连接设置。您可以在虚拟服务器上配置以下设置：

- 证书
- 身份验证
- 策略
- 书签
- 地址池（也称为 IP 池或 Intranet IP）
- 使用 Citrix Gateway 的双跃点 DMZ 部署
- 安全票务管理机构

- SmartAccess ICA 代理会话传输

如果运行 Citrix Gateway 向导，则可以在向导期间创建虚拟服务器。您可以通过以下方式配置其他虚拟服务器：

- 从虚拟服务器节点。此节点位于配置实用程序的导航窗格中。您可以使用配置实用程序添加、编辑和删除虚拟服务器。
- 使用快速配置向导。如果在环境中部署 Citrix Endpoint Management、StoreFront 或 Web Interface，则可以使用“快速配置”向导创建虚拟服务器和部署所需的所有策略。

如果希望用户登录并使用特定身份验证类型（如 RADIUS），则可以配置虚拟服务器并为该服务器分配唯一的 IP 地址。当用户登录时，他们会被定向到虚拟服务器，然后提示他们输入 RADIUS 凭据。

您还可以配置用户登录 Citrix Gateway 的方式。您可以使用会话策略配置用户软件的类型、访问方法和用户登录后看到的主页。

创建其他虚拟服务器

April 6, 2020

您可以使用配置实用程序导航窗格或快速配置向导中的虚拟服务器节点添加、修改、启用或禁用和删除虚拟服务器。有关使用快速配置向导配置虚拟服务器的更多信息，请参阅
使用快速配置向导配置设置。

使用配置实用程序创建虚拟服务器

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 配置所需的设置，单击创建，然后单击关闭。

在虚拟服务器上配置连接类型

April 6, 2020

创建和配置虚拟服务器时，可以配置以下连接选项：

- 与 Citrix Workspace 应用程序的连接仅与 Citrix Virtual Apps and Desktops 没有 SmartAccess、端点分析或网络层隧道功能。
- 与 Citrix Gateway 插件和 SmartAccess 的连接，允许使用 SmartAccess、端点分析和网络层隧道功能。
- 与 Secure Hub 的连接，用于建立从移动设备到 Citrix Gateway 的 Micro VPN 连接。
- 来自多个设备的用户通过 ICA 会话协议建立并行连接。连接将迁移到单个会话，以防止使用多个通用许可证。

如果希望用户在没有用户软件的情况下登录，则可以配置无客户端访问策略并将其绑定到虚拟服务器。

在虚拟服务器上配置基本或 **SmartAccess** 连接

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“名称”中，键入虚拟服务器的名称。
4. 在 IP 地址和端口中，键入虚拟服务器的 IP 地址和端口号。
5. 执行以下操作之一：
   - 若要仅允许 ICA 连接，请单击“基本模式”。
   - 若要允许用户使用 Secure Hub、Citrix Gateway 插件和 SmartAccess 登录，请单击“SmartAccess 模式”。
   - 若要允许 SmartAccess 管理多个用户连接的 ICA 代理会话，请单击 ICA 代理会话迁移。
6. 配置虚拟服务器的其他设置，单击创建，然后单击关闭。

为通配符虚拟服务器配置侦听策略

April 6, 2020

您可以配置 Citrix Gateway 虚拟服务器，以限制虚拟服务器在特定虚拟局域网 (VLAN) 上侦听的能力。您可以使用监听策略创建通配符虚拟服务器，该策略将其限制为处理指定 VLAN 上的流量。

配置参数如下：

参数	说明
名称	虚拟服务器的名称。该名称是必需的，您无法在创建虚拟服务器后更改该名称。名称不能超过 127 个字符，并且第一个字符必须是数字或字母。您还可以使用以下字符：符号 (@)、下划线 (_)、短划线 (-)、句点 (.)、冒号 (:)、英镑符号 (#) 和空格。
IP	虚拟服务器的 IP 地址。对于绑定到 VLAN 的通配符虚拟服务器，值始终为 *。
类型	服务的行为。您的选择是 HTTP，SSL，FTP，TCP，SSL_TCP，UDP，SSL_Bridge，NNTP，DNS，任何，SIP-UDP，DNS-TCP 和 RTSP。
端口	虚拟服务器侦听用户连接的端口。端口号必须介于 0 到 65535 之间。对于绑定到 VLAN 的通配符虚拟服务器，值通常为 *。
聆听优先级	分配给侦听策略的优先级。按相反的顺序评估优先级；数值越低，分配给侦听策略的优先级就越高。

参数	说明
监听策略规则	用于标识虚拟服务器应侦听的 VLAN 的策略规则。规则是：CLIENT.VLAN.ID.EQ (<ipaddressat>) 对于<ipaddressat>，替换分配给 VLAN 的 ID 号码。

使用侦听策略创建通配符虚拟服务器

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“名称”中，键入虚拟服务器的名称。
4. 在协议中，选择协议。
5. 在“IP 地址”中，键入虚拟服务器的 IP 地址。
6. 在端口中，键入虚拟服务器的端口。
7. 在“高级”选项卡上的“侦听策略”下的“侦听优先级”中，键入侦听策略的优先级。
8. 在侦听策略规则旁边，单击配置。
9. 在“创建表达式”对话框中，单击“添加”，配置表达式，然后单击“确定”。
10. 单击 Create（创建），然后单击 Close（关闭）。

在 **Citrix Gateway** 上配置 **IP** 地址

April 6, 2020

您可以将 IP 地址配置为登录到配置实用程序和用户连接。Citrix Gateway 配置的默认 IP 地址为 192.168.100.1，子网掩码为 255.255.0.0，用于管理访问。当用户配置的系统 IP (NSIP) 地址值不存在时，将使用默认 IP 地址。

- NSIP 地址。Citrix Gateway 的管理 IP 地址，用于对设备的所有管理相关访问。Citrix Gateway 还使用 NSIP 地址进行身份验证。
- 默认网关。将流量从安全网络外部转发到 Citrix Gateway 的路由器。
- 子网 **IP (SNIP)** 地址。通过与辅助网络上的服务器通信来表示用户设备的 IP 地址。这与映射的 IP (MIP) 地址类似。

SNIP 地址使用端口 1024 到 64000。

Citrix Gateway 如何使用 **IP** 地址

Citrix Gateway 基于正在发生的功能来自 IP 地址的流量。以下列表描述了几个函数以及 Citrix Gateway 为每个函数使用 IP 地址的方式，作为一般准则：

- 身份验证。Citrix Gateway 使用 SNIP 地址。

- 从主页传输文件。Citrix Gateway 使用 SNIP 地址。
- **DNS** 和 **WINS** 查询。Citrix Gateway 使用 MIP 地址或 SNIP 地址。
- 到安全网络中资源的网络流量。Citrix Gateway 使用 MIP 地址、SNIP 地址或 IP 池，具体取决于 Citrix Gateway 上的配置。
- **ICA** 代理设置。Citrix Gateway 使用 MIP 地址或 SNIP 地址。

更改或删除映射的 **IP** 地址

April 6, 2020

Citrix Gateway 支持一个映射的 IP 地址。如果在设备上配置了一个映射的 IP 地址，则无法更改或删除该地址。如果需要更改映射的 IP 地址，首先创建一个新的映射 IP 地址，然后删除原始映射的 IP 地址。

您可以使用配置实用程序中的安装向导或网络节点配置其他映射的 IP 地址。

创建新的映射 **IP** 地址

1. 在配置实用程序中，在 “配置” 选项卡的导航窗格中，展开 “系统”>“网络”，然后单击 “IP”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在 “创建 IP” 对话框的 “IP 地址” 中，键入 IP 地址。
4. 在网络掩码中，键入子网掩码。
5. 在 “IP 类型” 下，选择 “映射的 IP”，然后单击 “创建”。

删除映射的 **IP** 地址

1. 在配置实用程序中，在 “配置” 选项卡的导航窗格中，展开 “系统”>“网络”，然后单击 “IP”。
2. 在详细信息窗格中，单击映射的地址，然后单击删除。

配置子网 **IP** 地址

April 6, 2020

子网 IP 地址允许用户从驻留在另一个子网的外部主机连接到 Citrix Gateway。添加子网 IP 地址时，会在路由表中创建相应的路由条目。每个子网只创建一个条目。路由条目对应于子网中添加的第一个 IP 地址。

与系统 IP 地址和映射的 IP 地址不同，在 Citrix Gateway 的初始配置期间不必指定子网 IP 地址。

映射的 IP 地址和子网 IP 地址使用端口 1024 到 64000。

添加子网 **IP** 地址

1. 在配置实用程序中，在 “配置” 选项卡的导航窗格中，展开 “系统”>“网络”，然后单击 “IP”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在 “创建 IP” 对话框的 “IP 地址” 中，键入 IP 地址。
4. 在网络掩码中，键入子网掩码。
5. 在 “IP 类型” 下，选择 “子网 IP”，单击 “关闭”，然后单击 “创建”。

为用户连接配置 **IPv6**

April 6, 2020

您可以将 Citrix Gateway 配置为使用 Internet 协议版本 6 (IPv6) 侦听用户连接。配置以下设置之一时，可以选中 IPv6 复选框，然后在对话框中输入 IPv6 地址：

- 全局设置-已发布的应用程序-ICA 代理
- 全局身份验证 - Radius
- 全局身份验证-LDAP
- 全局身份验证-TACACS
- 会话配置文件-已发布的应用程序-ICA 代理
- Citrix Gateway 虚拟服务器
- 创建身份验证服务器 - Radius
- 创建身份验证服务器-LDAP
- 创建身份验证服务器-TACACS
- 创建审核服务器
- 高可用性设置
- 绑定/取消绑定路由监视器以实现高可用性
- 虚拟服务器（负载平衡）

将 Citrix Gateway 虚拟服务器配置为侦听 IPv6 地址时，用户只能使用 Citrix Workspace 应用程序进行连接。IPv6 不支持使用 Citrix Gateway 插件的用户连接。

您可以使用以下准则在 Citrix Gateway 上配置 IPv6：

- Citrix Virtual Apps 和 Web Interface。当您为用户连接配置 IPv6 时，如果存在使用 IPv6 的映射 IP 地址时，Citrix Virtual Apps 和 Web Interface 服务器也可以使用 IPv6。Web Interface 必须安装在 Citrix Gateway 后面。当用户通过 Citrix Gateway 连接时，IPv6 地址将转换为 IPv4。当连接返回时，IPv4 地址将转换为 IPv6。
- 虚拟服务器。运行 Citrix Gateway 向导时，可以为虚拟服务器配置 IPv6。在 “虚拟服务器” 页面上的 Citrix Gateway 向导中，单击 IPv6 并输入 IP 地址。只能使用 Citrix Gateway 向导为虚拟服务器配置 IPv6 地址。
- 其他。要为 ICA 代理、身份验证、审核和高可用性配置 IPv6，请选中对话框中的 IPv6 复选框，然后键入 IP 地址。

解析位于安全网络中的 **DNS** 服务器

April 6, 2020

如果 DNS 服务器位于防火墙后面的安全网络中，且防火墙阻止 ICMP 流量，则无法测试与服务器的连接，因为防火墙阻止了请求。您可以通过执行以下步骤来解决此问题：

- 使用解析为已知完全限定域名 (FQDN) 的自定义 DNS 监视器创建 DNS 服务。
- 在 Citrix Gateway 上创建不可直接寻址的 DNS 虚拟服务器。
- 将服务绑定到虚拟服务器。

注意：

- 仅当 DNS 服务器位于防火墙后面时，配置 DNS 虚拟服务器和 DNS 服务。
- 如果在设备上安装 Citrix ADC 负载平衡许可证，则导航窗格中不会显示“虚拟服务器和服务”节点。您可以通过展开负载平衡，然后单击虚拟服务器来执行此过程。

配置 **DNS** 服务和 **DNS** 监视器的步骤

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“虚拟服务器和服务”，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“名称”中，键入服务的名称。
4. 在协议中，选择 DNS。
5. 在“IP 地址”中，键入 DNS 服务器的 IP 地址。
6. 在端口中，键入端口号。
7. 在服务选项卡上，单击添加。
8. 在“监视器”选项卡上，在“可用”下，选择“dns”，单击“添加”，单击“创建”，然后单击“关闭”。
9. 在创建虚拟服务器（负载平衡）对话框中，单击创建，然后单击关闭。

接下来，通过使用过程创建 DNS 虚拟服务器配置 DNS 虚拟服务器，然后将 DNS 服务绑定到虚拟服务器。

将 **DNS** 服务绑定到 **DNS** 虚拟服务器

1. 在配置虚拟服务（负载平衡）对话框中的服务选项卡上，单击添加，选择 DNS 服务，单击创建，然后单击关闭。

配置 **DNS** 虚拟服务器

April 6, 2020

要配置 DNS 虚拟服务器，请指定名称和 IP 地址。与 Citrix Gateway 虚拟服务器一样，必须为 DNS 虚拟服务器分配 IP 地址。但是，此 IP 地址必须位于目标网络的内部侧，以便用户设备能够解析所有内部地址。您还必须指定 DNS 端口。

注意：如果在设备上安装 Citrix ADC 负载平衡许可证，则导航窗格中不会显示 “
虚拟服务器和服务” 节点。您可以使用负载平衡虚拟服务器配置此功能。有关详细信息，请参阅 Citrix eDocs 中的 Citrix ADC 文档。

配置 **DNS** 虚拟服务器

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “虚拟服务器和服务”，然后单击 “虚拟服务器”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在 “名称” 中，键入虚拟服务器的名称。
4. 在 “IP 地址” 中，键入 DNS 服务器的 IP 地址。
5. 在端口中，键入 DNS 服务器侦听的端口。
6. 在协议中，选择 DNS，然后单击创建。

最后，根据部署的需要，通过以下两种方法之一将 DNS 虚拟服务器与 Citrix Gateway 关联：

- 将服务器全局绑定到 Citrix Gateway。
- 在每个虚拟服务器的基础上绑定 DNS 虚拟服务器。

如果您在全局部署 DNS 虚拟服务器，则所有用户都可以访问该服务器。然后，您可以通过将 DNS 虚拟服务器绑定到虚拟服务器来限制用户。

配置名称服务提供程序

April 6, 2020

Citrix Gateway 使用名称服务提供商将 Web 地址转换为 IP 地址。

运行 Citrix Gateway 向导时，可以配置 DNS 服务器或 WINS 服务器。您也可以使用配置实用程序配置其他 DNS 或 WINS 服务器。

将 **DNS** 服务器添加到 **Citrix Gateway**

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway，然后单击 “全局设置”。
2. 在详细信息窗格的 “设置” 下，单击 “更改全局设置”。
3. 在 “网络配置” 选项卡上，单击 “添加”。
4. 在 “插入名称服务器” 对话框的 “IP 地址” 中，键入 DNS 服务器的 IP 地址，单击 “创建”，然后单击 “关闭”。
5. 在配置实用程序中单击确定。

将 **WINS** 服务器添加到 **Citrix Gateway**

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway，然后单击 “全局设置”。

2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在网络配置选项卡上的 WINS 服务器 IP 中，键入 WINS 服务器的 IP 地址，然后单击确定。

接下来，指定 DNS 虚拟服务器名称和 IP 地址。与 Citrix Gateway 虚拟服务器一样，必须为虚拟服务器分配 IP 地址。但是，此 IP 地址必须位于目标网络的内部侧，以便用户设备正确解析所有内部地址。您还必须指定 DNS 端口。

如果配置 DNS 服务器和 WINS 服务器进行名称解析，则可以使用 Citrix Gateway 向导选择首先执行名称查找的服务器。

指定名称查找优先级

1. 在配置实用程序中，单击配置选项卡，然后在导航窗格中单击 Citrix Gateway。
2. 在详细信息窗格的“入门”下，单击 Citrix Gateway 向导。
3. 单击“下一步”接受当前设置，直到您进入“名称服务提供商”页面。
4. 在“名称查找优先级”中，选择 WINS 或 DNS，然后继续到向导的末尾。

配置服务器启动的连接

April 6, 2020

对于每个登录到 Citrix Gateway 且启用了 IP 地址的用户，DNS 后缀都会附加到用户名中，并将 DNS 地址记录添加到设备的 DNS 缓存中。此技术有助于为用户提供 DNS 名称，而不是用户的 IP 地址。

将 IP 地址分配给用户的会话时，可以从内部网络连接到用户的设备。例如，使用远程桌面或虚拟网络计算 (VNC) 客户端连接的用户可以访问用户设备以诊断问题应用程序。两个具有内部网络 IP 地址且远程登录的 Citrix Gateway 用户也可以通过 Citrix Gateway 相互通信。允许发现设备上已登录用户的内部网络 IP 地址有助于进行此通信。

远程用户可以使用以下 ping 命令发现当时可登录 Citrix Gateway 的用户的内部网络 IP 地址：

平

服务器可以通过以下不同方式启动与用户设备的连接：

- TCP 或 UDP 连接。连接可以来自内部网络中的外部系统，也可以来自登录到 Citrix Gateway 的另一台计算机。分配给登录到 Citrix Gateway 的每个用户设备的内部网络 IP 地址用于这些连接。Citrix Gateway 支持的不同类型的服务器启动连接如下所述。

对于 TCP 或 UDP 服务器启动的连接，服务器先了解用户设备的 IP 地址和端口，并与其建立连接。Citrix Gateway 拦截此连接。

然后，用户设备与服务器建立初始连接，服务器连接到已知或从第一个配置的端口派生的端口上的用户设备。

在这种情况下，用户设备与服务器进行初始连接，然后通过使用嵌入此信息的应用程序特定协议与服务器交换端口和 IP 地址。这使 Citrix Gateway 能够支持应用程序，例如活动 FTP 连接。

- 端口命令.. 这在活动 FTP 和某些 IP 语音协议中使用。
- 插件之间的连接。Citrix Gateway 支持通过使用内部网络 IP 地址在插件之间进行连接。

使用此类连接，使用同一 Citrix Gateway 的两个 Citrix Gateway 用户设备可以启动彼此之间的连接。这种类型的一

个例子是使用即时消息应用程序，如 Office 通信器或雅虎! 信使。
如果用户注销 Citrix Gateway 并且注销请求未到达设备，则用户可以使用任何设备重新登录，并将上一个会话替换为新会话。在为每个用户分配一个 IP 地址的部署中，此功能可能非常有用。
当用户首次登录到 Citrix Gateway 时，将创建会话，并将 IP 地址分配给该用户。如果用户注销但注销请求丢失或用户设备无法执行干净注销，则会话在系统上维护。如果用户尝试从同一设备或另一设备再次登录，则身份验证成功后，将显示传输登录对话框。如果用户选择传输登录，则 Citrix Gateway 上的上一个会话将关闭，并创建一个新会话。登录传输在注销后只有两分钟处于活动状态，如果同时尝试从多个设备登录，则上次登录尝试将替换原始会话。

在 **Citrix Gateway** 上配置路由

April 6, 2020

要提供对内部网络资源的访问权限，Citrix Gateway 必须能够将数据路由到内部安全网络。默认情况下，Citrix Gateway 使用静态路由。

Citrix Gateway 可以将数据路由到的网络取决于您配置 Citrix Gateway 路由表和为 Citrix Gateway 指定的默认网关的方式。

Citrix Gateway 路由表必须包含将数据路由到用户可能需要访问的任何内部网络资源所需的路由。

Citrix Gateway 支持以下路由协议：

- 路由信息协议 (RIP v1 和 v2)
- 开放最短路径优先 (OSPF)
- 边界网关协议 (BGF)

配置静态路由

设置与其他主机或网络的通信时，如果不使用动态路由，则可能需要配置从 Citrix Gateway 到新目标的静态路由。

配置静态路由

1. 在配置实用程序中，在 “配置” 选项卡的导航窗格中，展开 “系统”>“网络”>“高级”，然后单击 “路由”。
2. 在详细信息窗格中的 “基本” 选项卡上，单击 “添加”。
3. 配置路由的设置，然后单击创建。

测试静态路由

1. 在配置实用程序的导航窗格中，展开 “系统”，然后单击 “诊断”。
2. 在详细信息窗格的 “实用程序” 下，单击 “Ping”。
3. 在 “参数” 下的 “主机名” 中，键入设备的名称。

4. 在“高级”的“源 IP 地址”下，键入设备的 IP 地址，然后单击“运行”。

   如果您与其他设备成功通信，则消息表明已传输和接收相同数量的数据包，并且丢失零数据包。

   如果您未与其他设备通信，则状态消息表示接收的数据包为零，并且所有数据包都丢失。要纠正这种缺乏通信的情况，请重复此过程以添加静态路由。

若要停止测试，请在“Ping”对话框中单击“停止”，然后单击“关闭”。

配置自动协商

April 6, 2020

默认情况下，将设备配置为使用自动协商，在这种协商中 Citrix Gateway 同时传输网络流量并确定适当的适配器速度。如果将默认设置保留为“
自动协商”，Citrix Gateway 将使用全双工操作，在这种操作中，网络适配器能够同时向双向发送数据。

如果禁用自动协商，Citrix Gateway 将使用半双工操作，在这种操作中，适配器可以在两个节点之间以两个方向发送数据，但适配器一次只能使用一个方向或另一个方向。

对于首次安装，Citrix 建议您将 Citrix Gateway 配置为对连接到该设备的端口使用自动协商。最初登录并配置 Citrix Gateway 后，您可以禁用自动协商。您不能全局配置自动协商。必须为每个接口启用或禁用设置。

启用或禁用自动协商

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”>“网络”，然后单击“接口”。
2. 在详细信息窗格中，选择界面，然后单击打开。
3. 在“配置接口”对话框中执行以下操作之一：
   - 若要启用自动协商，请单击自动协商旁边的是，然后单击确定。
   - 若要禁用自动协商，请单击自动协商旁边的否，然后单击确定。

身份验证和授权

April 6, 2020

Citrix Gateway 采用灵活的身份验证设计，允许对 Citrix Gateway 进行广泛的用户身份验证进行自定义。您可以使用行业标准身份验证服务器，并将 Citrix Gateway 配置为使用服务器对用户进行身份验证。Citrix Gateway 还支持基于客户端证书中存在的属性进行身份验证。Citrix Gateway 身份验证旨在适应使用单一源进行用户身份验证的简单身份验证过程，以及依赖于多种身份验证类型的更复杂级联身份验证过程。

Citrix Gateway 身份验证包含用于创建本地用户和组的本地身份验证。此设计主要围绕使用策略来控制您配置的身份验证过程。您创建的策略可以在 Citrix Gateway 全局或虚拟服务器级别应用，并可用于根据用户的源网络有条件地设置身份验证服务器参数。

由于策略是全局绑定的，也是绑定到虚拟服务器的，因此您还可以为策略分配优先级，以便在身份验证过程中创建多个身份验证服务器的级联。

Citrix Gateway 包括对以下身份验证类型的支持。

- 本地
- 轻量级目录访问协议 (LDAP)
- RADIUS
- SAML
- TACACS+
- 客户端证书身份验证（包括智能卡身份验证）

Citrix Gateway 还支持 RSA SecurID、Gemalto Protiva 和 SafeWord。您可以使用 RADIUS 服务器配置这些类型的身份验证。

身份验证允许用户登录 Citrix Gateway 并连接到内部网络，但授权将定义用户有权访问的安全网络中的资源。您可以使用 LDAP 和 RADIUS 策略配置授权。

配置默认全局身份验证类型

April 6, 2020

安装 Citrix Gateway 并运行 Citrix Gateway 向导时，您可以在向导中配置身份验证。此身份验证策略将自动绑定到 Citrix Gateway 全局级别。在 Citrix Gateway 向导中配置的身份验证类型是默认身份验证类型。您可以通过再次运行 Citrix Gateway 向导更改默认授权类型，也可以在配置实用程序中修改全局身份验证设置。

如果需要添加其他身份验证类型，可以在 Citrix Gateway 上配置身份验证策略，并使用配置实用程序将策略绑定到 Citrix Gateway。在全局配置身份验证时，您可以定义身份验证类型、配置设置并设置可以进行身份验证的最大用户数。

配置和绑定策略后，您可以设置优先级以定义哪种身份验证类型优先。例如，您配置 LDAP 和 RADIUS 身份验证策略。如果 LDAP 策略的优先级数为 10，RADIUS 策略的优先级数为 15，则无论您在何处绑定每个策略，LDAP 策略都优先级。这称为级联身份验证。

您可以选择从 Citrix Gateway 内存缓存或从 Citrix Gateway 上运行的 HTTP 服务器传递登录页。如果选择从内存缓存传递登录页，则 Citrix Gateway 传递登录页的速度比 HTTP 服务器快得多。选择从内存缓存传递登录页可减少大量用户同时登录时的等待时间。作为全局身份验证策略的一部分，您只能配置从缓存传递登录页。

您还可以配置作为身份验证的特定 IP 地址的网络地址转换 (NAT) IP 地址。此 IP 地址对于身份验证是唯一的，不是 Citrix Gateway 子网、映射或虚拟 IP 地址。这是一个可选设置。

注意：无法使用 Citrix Gateway 向导配置 SAML 身份验证。

您可以使用快速配置向导配置 LDAP、RADIUS 和客户端证书身份验证。运行向导时，可以从 Citrix Gateway 上配置的现有 LDAP 或 RADIUS 服务器中进行选择。您还可以配置 LDAP 或 RADIUS 的设置。如果使用双重身份验证，Citrix 建议使用 LDAP 作为主身份验证类型。

全局配置身份验证

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改身份验证设置”。
3. 在“最大用户数”中，键入可以使用此身份验证类型进行身份验证的用户数。
4. 在 NAT IP 地址中，键入用于身份验证的唯一 IP 地址。
5. 选择“启用静态缓存”以更快地传递登录页面。
6. 选择“启用增强型身份验证反馈”，以便在身份验证失败时向用户提供消息。用户收到的消息包括密码错误、帐户禁用或锁定或找不到用户等。
7. 在“默认身份验证类型”中，选择身份验证类型。
8. 配置身份验证类型的设置，然后单击确定。

配置无授权的身份验证

April 6, 2020

授权定义允许用户通过 Citrix Gateway 连接到的资源。您可以使用表达式配置授权策略，然后将策略设置为允许或拒绝。您可以将 Citrix Gateway 配置为仅使用身份验证，而无需授权。

配置身份验证时，Citrix Gateway 不会执行组授权检查。您为用户或组配置的策略将分配给该用户。

有关配置授权的更多信息，请参阅配置授权。

配置授权

April 6, 2020

授权指定用户登录 Citrix Gateway 时可以访问的网络资源。授权的默认设置是拒绝访问所有网络资源。Citrix 建议使用默认的全局设置，然后创建授权策略来定义用户可以访问的网络资源。

您可以使用授权策略和表达式在 Citrix Gateway 上配置授权。创建授权策略后，可以将其绑定到设备上配置的用户或组。

配置授权策略

April 6, 2020

配置授权策略时，可以将其设置为允许或拒绝访问内部网络中的网络资源。例如，要允许用户访问 10.3.3.0 网络，请使用以下表达式：

REQ.IP.DESTIP==10.3.0.0 -netmask 255.255.0.0

授权策略应用于用户和组。对用户进行身份验证后，Citrix Gateway 通过从 RADIUS、LDAP 或 TACACS+ 服务器获取用户的组信息来执行组授权检查。如果用户可用组信息，Citrix Gateway 将检查该组允许的网络资源。

要控制用户可以访问哪些资源，您必须创建授权策略。如果您不需要创建授权策略，则可以配置默认的全局授权。

如果您在授权策略中创建拒绝访问文件路径的表达式，则只能使用子目录路径而不能使用根目录。例如，使用 fs.path 包含 “\\dir1\\dir2” 而非 fs.path 包含 “\\rootdir\\dir1\\dir2”。如果您在此示例中使用第二个版本，则策略将失败。

配置授权策略后，您将其绑定到用户或组，如以下任务所示。

默认情况下，授权策略首先针对绑定到虚拟服务器的策略进行验证，然后针对全局绑定的策略进行验证。如果您全局绑定策略，并希望全局策略优先于绑定到用户、组或虚拟服务器的策略，则可以更改策略的优先级号。优先级数从零开始。优先级数越低，策略的优先级越高。

例如，如果全局策略的优先级号为 1，用户的优先级为 2，则首先应用全局身份验证策略。

> 重要：
>
> - 传统授权策略仅适用于 TCP 流量。
> - 高级授权策略可应用于所有类型的流量（TCP/UDP/ICMP/DNS）。
>   - 要对 UDP/ICMP/DNS 流量应用策略，策略必须分别绑定为 UDP_REQUEST、ICMP_REQUEST 和 DNS_REQUEST 类型。
>   - 绑定时，如果没有明确提到 “类型” 或 “类型” 设置为 REQUEST，则行为不会从早期版本中改变，即这些策略仅应用于 TCP 流量。

有关高级授权策略的更多详细信息，请参阅文章https://support.citrix.com/article/CTX232237。

使用 **GUI** 配置授权策略

1. 导航到 **Citrix Gateway >** 策略 **>** 授权。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在 “名称” 中，键入策略的名称。
4. 在 “操作” 中，选择 “允许” 或 “拒绝”。
5. 在 “表达式” 中，单击 “表达式编辑器”。
6. 要开始配置表达式，请单击 “选 择” 并选择必要的元素。
7. 表达式 完成后单击 “完成”。

8. 单击创建。

使用 **GUI** 将授权策略绑定到用户

1. 导航到 **Citrix Gateway >** 用户管理。
2. 点击 **AAA** 用户。
3. 在详细信息窗格中，选择一个用户，然后单击 编辑。
4. 在“高级设置”中，单击“授权策略”。
5. 在 策略绑定页面中，选择策略或创建策略。
6. 在“优先级”中，设置优先级号。
7. 在“类型”中，选择请求类型，然后单击“确定”。

使用 **GUI** 将授权策略绑定到组

1. 导航到 **Citrix Gateway >** 用户管理。
2. 点击 **AAA** 组。
3. 在详细信息窗格中，选择一个组，然后单击 编辑。
4. 在“高级设置”中，单击“授权策略”。
5. 在 策略绑定页面中，选择策略或创建策略。
6. 在“优先级”中，设置优先级号。
7. 在“类型”中，选择请求类型，然后单击“确定”。

设置默认全局授权

April 6, 2020

要定义用户在内部网络上可以访问的资源，您可以配置默认的全局授权。您可以通过允许或拒绝访问内部网络上的全局网络资源来配置全局授权。

您创建的任何全局授权操作都将应用于尚未与其关联的授权策略的所有用户，无论是直接还是通过组应用。用户或组授权策略始终覆盖全局授权操作。如果默认授权操作设置为“拒绝”，则必须对所有用户或组应用授权策略，以便使这些用户或组能够访问网络资源。此要求有助于提高安全性。

要设置默认的全局授权：

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“安全”选项卡上的“默认授权操作”旁边，选择“允许”或“拒绝”，然后单击“确定”。

禁用身份验证

April 6, 2020

如果您的部署不需要身份验证，则可以禁用它。您可以为不需要身份验证的每个虚拟服务器禁用身份验证。

重要提示：Citrix 建议谨慎禁用身份验证。如果您未使用外部身份验证服务器，请创建本地用户和组以允许 Citrix Gateway 对用户进行身份验证。禁用身份验证将停止使用用于控制和监视与 Citrix Gateway 连接的身份验证、授权和记帐功能。当用户键入要连接到 Citrix Gateway 的 Web 地址时，不会显示登录页面。

禁用身份验证

1. 在配置实用程序的导航窗格中，展开 Citrix Gateway，然后单击虚拟服务器。
2. 在详细信息窗格中，单击虚拟服务器，然后单击打开。
3. 在“身份验证”选项卡上的“用户身份验证”下，单击以清除“启用身份验证”。

配置特定时间的身份验证

April 6, 2020

您可以配置身份验证策略，以便允许用户在特定时间（例如在正常工作时间）访问内部网络。当用户尝试在不同的时间登录时，登录将被拒绝。

要限制用户登录 Citrix Gateway 的时间，请在身份验证策略中创建一个表达式，然后将其绑定到虚拟服务器或全局。

配置时间、日期或星期中某天的身份验证

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“策略”>“身份验证”。
2. 在“身份验证”下，选择身份验证类型。
3. 在详细信息窗格中，单击策略选项卡，选择身份验证策略，然后单击打开。
4. 在“配置身份验证策略”对话框的“表达式”下，单击“匹配任何表达式”旁边的“添加”。
5. 在“添加表达式”对话框的“表达式类型”中，选择“日期/时间”。
6. 在限定符中，选择以下选项之一：
   - 时间来配置用户无法登录的时间。
   - DATE 配置用户无法登录的日期。
   - DAYOFWEEK 配置用户无法登录的日期。
7. 在“运算符”中，选择值。
8. 在“值”中，单击文本框旁边的日历，然后选择日期、日期或时间。
9. 单击确定两次，单击关闭，然后单击确定。

身份验证策略的工作原理

April 6, 2020

当用户登录到 Citrix Gateway 时，他们将根据您创建的策略进行身份验证。策略定义了身份验证类型。单个身份验证策略可用于简单的身份验证需求，并且通常绑定在全局级别。您还可以使用默认身份验证类型（本地）。如果配置本地身份验证，则还必须在 Citrix Gateway 上配置用户和组。

您可以配置多个身份验证策略并将其绑定以创建详细的身份验证过程和虚拟服务器。例如，您可以通过配置多个策略来配置级联和双重身份验证。您还可以设置身份验证策略的优先级，以确定哪些服务器以及 Citrix Gateway 检查用户凭据的顺序。身份验证策略包括表达式和操作。例如，如果将表达式设置为 True 值，则在用户登录时，操作将用户登录评估为 true，然后用户可以访问网络资源。

创建身份验证策略后，您可以在全局级别或将策略绑定到虚拟服务器。将至少一个身份验证策略绑定到虚拟服务器时，在用户登录到虚拟服务器时，不会使用绑定到全局级别的任何身份验证策略，除非全局身份验证类型的优先级高于绑定到虚拟服务器的策略。

当用户登录到 Citrix Gateway 时，将按以下顺序评估身份验证：

- 将检查虚拟服务器是否存在任何绑定的身份验证策略。
- 如果身份验证策略未绑定到虚拟服务器，Citrix Gateway 会检查全局身份验证策略。
- 如果身份验证策略未绑定到虚拟服务器或全局，则会通过默认身份验证类型对用户进行身份验证。

如果配置 LDAP 和 RADIUS 身份验证策略，并希望为双重身份验证全局绑定策略，则可以在配置实用程序中选择策略，然后选择策略是主身份验证类型还是辅助身份验证类型。您还可以配置组提取策略。

配置身份验证配置文件

April 6, 2020

您可以使用 Citrix Gateway 向导或配置实用程序创建身份验证配置文件。配置文件包含身份验证策略的所有设置。您可以在创建身份验证策略时配置配置文件。

通过 Citrix Gateway 向导，您可以使用所选的身份验证类型来配置身份验证。如果要在运行向导后配置其他身份验证策略，则可以使用配置实用程序。有关 Citrix Gateway 向导的更多信息，请参阅使用 Citrix Gateway 向导配置设置。

使用配置实用程序创建身份验证策略

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“策略”>“身份验证”。
2. 在导航窗格中的身份验证下，选择身份验证类型。
3. 在详细信息窗格的“策略”选项卡上，单击“添加”。
4. 如果您使用的是外部身份验证类型，请单击“服务器”旁边的“新建”。

5. 在“创建身份验证服务器”对话框中，配置身份验证类型的设置，单击“创建”，然后单击“关闭”。
6. 在“创建身份验证策略”对话框的命名表达式旁边，选择“True”值，单击“添加表达式”，单击“创建”，然后单击“关闭”。

   注意：选择身份验证类型并保存身份验证配置文件时，无法更改身份验证类型。要使用其他身份验证类型，您必须创建新策略。

使用配置实用程序修改身份验证策略

您可以修改已配置的身份验证策略和配置文件，例如身份验证服务器的 IP 地址或表达式。

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“策略”>“身份验证”。
2. 在导航窗格中的身份验证下，选择身份验证类型。
3. 在详细信息窗格中的“服务器”选项卡上，选择一个服务器，然后单击“打开”。

删除身份验证策略

如果从网络中更改或删除了身份验证服务器，请从 Citrix Gateway 中删除相应的身份验证策略。

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“策略”>“身份验证”。
2. 在导航窗格中的身份验证下，选择身份验证类型。
3. 在详细信息窗格的“策略”选项卡上，选择一个策略，然后单击“删除”。

绑定身份验证策略

April 6, 2020

配置身份验证策略后，您可以将策略全局绑定或绑定到虚拟服务器。您可以使用配置实用程序绑定身份验证策略。

要使用配置实用程序全局绑定身份验证策略，请执行以下操作：

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“策略”>“身份验证”。
2. 单击身份验证类型。
3. 在详细信息窗格的“策略”选项卡上，单击服务器，然后在“操作”中，单击“全局绑定”。
4. 在“主”或“辅助”选项卡上的“详细信息”下，单击“插入策略”。
5. 在策略名称下，选择策略，然后单击确定。

   注意：选择策略时，Citrix Gateway 会自动将表达式设置为 True 值。

要使用配置实用程序取消绑定全局身份验证策略，请执行以下操作：

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“策略”>“身份验证”。
2. 在“策略”选项卡上的“操作”中，单击“全局绑定”。

3. 在“绑定/取消绑定到全局的身份验证策略”对话框中的“主”或“辅助”选项卡上的“策略名称”中，选择策略，单击“取消绑定策略”，然后单击“确定”。

设置身份验证策略的优先级

April 6, 2020

默认情况下，身份验证策略首先针对绑定到虚拟服务器的策略进行验证，然后针对全局绑定的策略进行验证。如果您全局绑定身份验证策略，并希望全局策略优先于您绑定到虚拟服务器的策略，则可以更改策略的优先级号。优先级数从零开始。优先级数越低，身份验证策略的优先级越高。

例如，如果全局策略的优先级号为 1，虚拟服务器的优先级为 2，则首先应用全局身份验证策略。

设置或更改全局身份验证策略的优先级

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“策略”>“身份验证”。
2. 在“策略”选项卡上的“操作”中，单击“全局绑定”。
3. 在“绑定/取消绑定身份验证全局策略”对话框中的“主”或“辅助”选项卡上的“优先级”下，键入数字，然后单击“确定”。

更改绑定到虚拟服务器的身份验证策略的优先级

您还可以修改绑定到虚拟服务器的身份验证策略。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 选择一个虚拟服务器，然后单击打开。
3. 单击“身份验证”选项卡，然后选择“主”或“辅助”。
4. 选择策略，然后在“优先级”中键入优先级号，然后单击“确定”。

配置本地用户

April 6, 2020

您可以在 Citrix Gateway 上本地创建用户帐户，以补充身份验证服务器上的用户。例如，您可能希望为临时用户（例如顾问或访客）创建本地用户帐户，而无需在身份验证服务器上为这些用户创建条目。

如果使用本地身份验证，请创建用户，然后将其添加到您在 Citrix Gateway 上创建的组中。配置用户和组后，您可以应用授权和会话策略、创建书签、指定应用程序以及指定用户有权访问的文件共享和服务器的 IP 地址。

创建本地用户

1. 在配置实用程序中，单击 “配置” 选项卡，然后在导航窗格中展开 “Citrix Gateway”>“用户管理”，然后单击 “AAA 用户”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在 “用户名” 中，键入用户名。
4. 如果您使用的是本地身份验证，请清除 “外部身份验证”。
   注意：选择
   外部身份验证可让用户对外部身份验证服务器（如 LDAP 或 RADIUS）进行身份验证。清除该复选框可使 Citrix Gateway 对本地用户数据库进行身份验证。
5. 在 “密码” 和 “确认密码” 中，键入用户的密码，单击 “创建”，然后单击 “关闭”。

更改用户密码

创建本地用户后，您可以更改用户的密码或将用户帐户配置为通过外部身份验证服务器进行身份验证。

1. 在配置实用程序中，单击 “配置” 选项卡，然后在导航窗格中展开 “Citrix Gateway”>“用户管理”，然后单击 “AAA 用户”。
2. 在详细信息窗格中，选择一个用户，然后单击打开。
3. 在 “密码” 和 “确认密码” 中，键入用户的新密码，然后单击 “确定”。

更改用户的身份验证方法

如果您的用户配置了本地身份验证，则可以将身份验证更改为外部身份验证服务器。若要执行此操作，请启用外部身份验证。

1. 在配置实用程序中，单击 “配置” 选项卡，然后在导航窗格中展开 “Citrix Gateway”>“用户管理”，然后单击 “AAA 用户”。
2. 在详细信息窗格中，选择一个用户，然后单击打开。
3. 选择外部身份验证，然后单击确定。

删除用户

您还可以从 Citrix Gateway 中删除用户。

1. 在配置实用程序中，单击 “配置” 选项卡，然后在导航窗格中展开 “Citrix Gateway”>“用户管理”，然后单击 “AAA 用户”。
2. 在详细信息窗格中，选择一个用户，然后单击 “删除”。

从 Citrix Gateway 中删除用户时，也会从用户配置文件中删除所有关联的策略。

配置组

April 6, 2020

Citrix Gateway 上可以拥有本地组的组，并且可以使用本地身份验证对用户进行身份验证。如果使用外部服务器进行身份验证，Citrix Gateway 上的组将被配置为匹配在内部网络中的身份验证服务器上配置的组。当用户登录并进行身份验证时，如果组名称与身份验证服务器上的组匹配，则用户将继承 Citrix Gateway 上该组的设置。

配置组后，您可以应用授权和会话策略、创建书签、指定应用程序以及指定用户有权访问的文件共享和服务器的 IP 地址。

如果使用本地身份验证，请创建用户并将其添加到 Citrix Gateway 上配置的组中。然后，用户继承该组的设置。

重要：如果用户是 Active Directory 组的成员，Citrix Gateway 上的组的名称必须与 Active Directory 组相同。

创建新组

1. 在配置实用程序中，单击 “配置” 选项卡，然后在导航窗格中展开 “Citrix Gateway”>“用户管理”，然后单击 “AAA 组”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在 “组名称” 中，键入组的名称，单击 “创建”，然后单击 “关闭”。

删除组

您还可以从 Citrix Gateway 中删除用户组。

1. 在配置实用程序中，单击 “配置” 选项卡，然后在导航窗格中展开 “Citrix Gateway”>“用户管理”，然后单击 “AAA 组”。
2. 在详细信息窗格中，选择组，然后单击 “删除”。

将用户添加到组

April 6, 2020

您可以在组创建过程中或稍后将用户添加到组中。您可以将用户添加到多个组，以便用户可以继承绑定到这些组的策略和设置。

要将用户添加到组：

1. 在配置实用程序中，单击 “配置” 选项卡，然后在导航窗格中展开 “Citrix Gateway”>“用户管理”，然后单击 “AAA 组”。
2. 在详细信息窗格中，选择一个组，然后单击打开。
3. 在 “用户” 选项卡上的 “可用用户” 下，选择用户，单击 “添加”，然后单击 “确定”。

使用组配置策略

April 6, 2020

配置组后，可以使用“组”对话框应用指定用户访问权限的策略和设置。如果使用本地身份验证，则可以创建用户并将其添加到 Citrix Gateway 上配置的组中。然后，用户继承该组的设置。

您可以在“组”对话框中为一组用户配置以下策略或设置：

- 用户
- 授权策略
- 审核策略
- 会话策略
- 流量策略
- 书签
- 内联网应用程序
- 内联网 IP 地址

在配置中，您可能有属于多个组的用户。此外，每个组可能具有一个或多个绑定会话策略，并配置了不同的参数。属于多个组的用户继承分配给该用户所属的所有组的会话策略。要确保哪个会话策略评估优先于另一个，您必须设置会话策略的优先级。

例如，您的 group1 绑定了使用主页 www.homepage1.com 配置的会话策略。Group2 与配置了主页 www.homepage2.com 的会话策略绑定。当这些策略绑定到不具有优先级号或具有相同优先级号的各个组时，属于这两个组的用户显示的主页取决于首先处理哪个策略。通过为主页 www.homepage1.com 的会话策略设置一个较低的优先级编号（这赋予了更高的优先级），您可以确保属于这两个组的用户始终会收到主页 www.homepage1.com。

如果会话策略未分配优先级号或具有相同的优先级号，则按以下顺序评估优先级：

- 用户
- 小组
- 虚拟服务器
- 全局

如果策略绑定到同一级别，没有优先级号，或者如果策略具有相同的优先级号，则评估顺序按策略绑定顺序进行。首先绑定到级别的策略优先于稍后绑定的策略。

配置 **LDAP** 身份验证

April 6, 2020

您可以将 Citrix Gateway 配置为对一个或多个 LDAP 服务器的用户访问进行身份验证。

LDAP 授权要求 Active Directory、LDAP 服务器和 Citrix Gateway 中的组名称相同。字符和大小写也必须匹配。

默认情况下，通过使用安全套接字层 (SSL) 或传输层安全性 (TLS)，LDAP 身份验证是安全的。有两种类型的安全 LDAP 连接。对于一种类型，LDAP 服务器接受与 LDAP 服务器用于接受清除 LDAP 连接的端口分开的 SSL 或 TLS 连接。用户建立 SSL 或 TLS 连接后，可以通过连接发送 LDAP 流量。

LDAP 连接的端口号为：

- 389 用于不安全的 LDAP 连接
- 636 用于安全的 LDAP 连接
- 3268 用于 Microsoft 不安全的 LDAP 连接
- 3269 用于 Microsoft 安全的 LDAP 连接

第二种类型的安全 LDAP 连接使用 StartTLS 命令并使用端口号 389。如果在 Citrix Gateway 上配置端口号 389 或 3268，服务器将尝试使用 StartTLS 建立连接。如果您使用任何其他端口号，服务器将尝试使用 SSL 或 TLS 建立连接。如果服务器无法使用 StartTLS、SSL 或 TLS，则连接将失败。

如果指定 LDAP 服务器的根目录，Citrix Gateway 会搜索所有子目录以查找用户属性。在大型目录中，此方法可能会影响性能。因此，Citrix 建议您使用特定组织单位 (OU)。

下表包含 LDAP 服务器的用户属性字段示例：

LDAP 服务器	用户属性	区分大小写
Microsoft Active Directory 服务器	sAMAccountName	否
Novell eDirectory	ou	是
IBM Directory Server	uid	是
Lotus Domino	CN	是
Sun ONE 目录（前身为 iPlanet）	uid 或 cn	是

此表包含基本 DN 的示例：

LDAP 服务器	基本 DN
Microsoft Active Directory 服务器	DC=citrix,DC=local
Novell eDirectory	ou=users,ou=dev
IBM Directory Server	cn=users
Lotus Domino	OU=City,O=Citrix, C=US
Sun ONE 目录（前身为 iPlanet）	ou=People,dc=citrix,dc=com

下表包含绑定 DN 的示例：

LDAP 服务器	绑定 DN
Microsoft Active Directory 服务器	CN=Administrator, CN=Users, DC=citrix, DC=local
Novell eDirectory	cn=admin, o=citrix
IBM Directory Server	LDAP_dn
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE 目录（前身为 iPlanet）	uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot

注意：有关 LDAP 服务器设置的更多信息，请参阅
确定 LDAP 目录中的属性。

使用配置实用程序配置 **LDAP** 身份验证

April 6, 2020

1. 导航到 **Citrix Gateway** > 策略 > 身份验证。
2. 点击 **LDAP**。
3. 在详细信息窗格的 “策略” 选项卡上，单击 “添加”。
4. 在 “名称” 中，键入策略的名称。
5. 在 服务器旁边，单击 新建。
6. 在 “名称” 中，键入服务器的名称。
7. 在 “服务器” 下的 “**IP** 地址和端口” 中，键入 LDAP 服务器的 IP 地址和端口号。
8. 在 “类型” 中，选择 Active Directory 的 **AD** 或 Novell 目录服务的 **NDS**。
9. 在 “连接设置**”** 下，完成以下操作：
   a) 在 基础 **DN**（用户的位置）中，键入用户所在的基础 DN。基本 DN 搜索位于所选目录（AD 或 NDS）下的用户。

   通过删除用户名并指定用户所在的组，基本 DN 从绑定 DN 派生。基本 DN 的语法示例如下：

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


b) 在 管理员绑定 **DN** 中，键入用于查询到 LDAP 目录的管理员绑定 DN。绑定 DN 语法的示例如下：

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

对于 Active Directory，必须使用指定为 cn=groupname 的组名称。在 Citrix Gateway 中定义的组名和 LDAP 服务器上的组名必须相同。

对于其他 LDAP 目录，组名称不是必需的，或者在必要时指定为 ou= 组名。

Citrix Gateway 使用管理员凭据绑定到 LDAP 服务器，然后搜索用户。查找用户后，Citrix Gateway 将取消绑定管理员凭据并使用用户凭据重新绑定。

c) 在“管理员密码”和“确认管理员密码”中，键入 LDAP 服务器的管理员密码。

10. 要自动检索更多 LDAP 设置，请单击 检索属性。

    单击“检索属性”时，“其他设置”下的字段将自动填充。如果要忽略此步骤，请继续执行步骤 12 和 13。否则，请跳至步骤 14。

11. 在“其他设置”下的“服务器登录名属性”中，键入 Citrix Gateway 应在其下查找要配置的 LDAP 服务器的用户登录名称的属性。默认值为“samAccountName”。

12. 在“搜索筛选器”中，键入要搜索与单个或多个活动目录组关联的用户的值。

    例如，“memberOf=CN=GatewayAccess,OU=Groups,DC=Users,DC=lab”。

    > 注意
    >
    > 您可以使用上述示例将 Citrix Gateway 仅限于特定 AD 组的成员访问。

13. 在组属性中，保留 Active Directory 的默认 memberOf 属性或者将属性更改为您正在使用的 LDAP 服务器类型的属性。此属性使 Citrix Gateway 能够在授权期间获取与用户关联的组。

14. 在“安全类型”中，选择安全类型，然后单击“创建”。

15. 要允许用户更改其 LDAP 密码，请选择“允许更改密码”。

    注意：

    - 如果您选择 **PLAINTEXT** 作为安全类型，则不支持允许用户更改其密码。
    - 如果您选择 **PLAINTEXT** 或 **TLS** 以确保安全性，请使用端口号 389。如果选择 **SSL**，请使用端口号 636。

确定 **LDAP** 目录中的属性

April 6, 2020

如果您需要确定 LDAP 目录属性的帮助，以便在 Citrix Gateway 上配置身份验证设置，则可以使用 Softerra 免费的 LDAP 浏览器轻松查找它们。

您可以从下载 LDAP 浏览器软地 LDAP 管理员网站。安装浏览器后，设置以下属性：

- LDAP 服务器的主机名或 IP 地址。
- LDAP 服务器的端口。默认值为 389。
- 基本 DN 字段，您可以将其留空。LDAP 浏览器提供的信息可帮助您确定在 Citrix Gateway 上配置此设置所需的基本 DN。
- 匿名绑定检查确定 LDAP 服务器是否需要用户凭据才能连接到它。如果 LDAP 服务器需要凭据，请将复选框保持清除状态。

完成设置后，LDAP 浏览器将在左侧窗格中显示配置文件名称并连接到 LDAP 服务器。

配置 **LDAP** 组提取

April 6, 2020

如果您使用的是双重身份验证，则从主身份验证源和辅助身份验证源中提取的组将连接起来。授权策略可应用于从主身份验证服务器或辅助身份验证服务器中提取的组。

将从 LDAP 服务器获取的组名与在 Citrix Gateway 上本地创建的组名进行比较。如果两个组名称匹配，则本地组的属性将应用于从 LDAP 服务器获取的组。

如果用户属于多个 LDAP 组，Citrix Gateway 会从用户所属的所有组中提取用户信息。如果用户是 Citrix Gateway 上的两个组的成员，并且每个组都具有绑定的会话策略，则该用户将继承这两个组的会话策略。要确保用户收到正确的会话策略，请设置会话策略的优先级。

有关将与 Citrix Gateway 授权一起使用的 LDAP 组成员身份属性的详细信息，请参阅以下内容：

- LDAP 组提取如何直接从用户对象中工作
- LDAP 组提取如何从组对象间接工作

LDAP 组提取如何直接从用户对象中工作

April 6, 2020

用于评估来自组对象的组成员身份的 LDAP 服务器使用 Citrix Gateway 授权。

某些 LDAP 服务器允许用户对象包含有关对象所属的组的信息，例如 Active Directory（通过使用 memberOf 属性）或 IBM eDirectory（通过使用 groupMembership 属性）。用户的组成员身份可以是来自用户对象的属性，例如 IBM 目录服务器（通过使用 ibm-allGroups）或 Sun ONE 目录服务器（通过使用 nsRole）。这两种类型的 LDAP 服务器都与 Citrix Gateway 组提取一起工作。

例如，在 IBM 目录服务器中，所有组成员身份（包括静态组、动态组和嵌套组）都可以通过使用 ibm-allGroups 属性返回。在 Sun ONE 中，通过使用 nsRole 属性计算所有角色（包括托管角色、过滤角色和嵌套角色）。

LDAP 组提取如何从组对象间接工作

April 6, 2020

从组对象间接评估组成员身份的 LDAP 服务器不能与 Citrix Gateway 授权一起工作。

某些 LDAP 服务器（如 Lotus Domino）只允许组对象包含有关用户的信息。这些 LDAP 服务器不允许用户对象包含有关组的信息，因此无法使用 Citrix Gateway 组提取。对于这种类型的 LDAP 服务器，通过在组的成员列表中查找用户来执行组成员身份搜索。

LDAP 授权组属性字段

April 6, 2020

下表包含 LDAP 组属性字段的示例：

LDAP 服务器	LDAP 属性
Microsoft Active Directory 服务器	memberOf
Novell eDirectory	groupMembership
IBM Directory Server	ibm-allGroups
Sun ONE 目录（前身为 iPlanet）	nsRole

配置 LDAP 授权

April 6, 2020

您可以通过设置组属性名称和子属性在身份验证策略中配置 LDAP 授权。

1. 在配置实用程序中的 “配置” 选项卡上，展开 “Citrix Gateway”>“策略”>“身份验证”。
2. 在身份验证下，单击身份验证类型。
3. 在详细信息窗格中，单击 Add（添加）。
4. 在 “名称” 中，键入策略的名称。
5. 在服务器旁边，单击新建。

6. 在“名称”中，键入服务器的名称。
7. 在“服务器”下，键入 LDAP 服务器的 IP 地址和端口。
8. 在“组属性”中，键入“memberOf”。
9. 在子属性名称中，键入 CN，然后单击创建。
10. 在“创建身份验证策略”对话框的命名表达式旁边，选择表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置 **LDAP** 嵌套组提取

April 6, 2020

Citrix Gateway 可以查询 LDAP 组，并从您在身份验证服务器上配置的祖先组中提取组和用户信息。例如，您创建了 group1，并在该组中创建了 group2 和 group3。如果用户属于 group3，Citrix Gateway 将从所有嵌套的祖先组（group2、group1）中提取到指定级别的信息。

您可以使用身份验证策略配置 LDAP 嵌套组提取。运行查询时，Citrix Gateway 会搜索这些组，直到它达到最大嵌套级别，或者直到它搜索所有可用的组。

配置 **LDAP** 嵌套组抽取

1. 在配置实用程序的导航窗格中，展开“Citrix Gateway”>“策略”>“身份验证/授权”>“身份验证”» >“身份验证”，然后单击“LDAP”。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在服务器旁边，单击新建。
5. 在“名称”中，键入服务器的名称。
6. 配置 LDAP 服务器的设置。
7. 展开嵌套组提取，然后单击启用。
8. 在“最大嵌套级别”中，键入 Citrix Gateway 检查的级别数。
9. 在组名称标识符中，键入唯一标识 LDAP 服务器上的组名称的 LDAP 属性名称，如 sAMAccountName。
10. 在“组搜索属性”中，键入要在搜索响应中获取的 LDAP 属性名称，以确定任何组（例如 memberOf）的父组。
11. 在“组搜索子属性”中，键入要搜索的 LDAP 子属性名称，作为“组搜索属性”的一部分，以确定任何组的父组。例如，键入 CN。
12. 在“组搜索筛选器”中，键入查询字符串。例如，过滤器可以是 (&(samaccountname=test)(objectClass=*))。
13. 单击 Create（创建），然后单击 Close（关闭）。
14. 在“创建身份验证策略”对话框的命名表达式旁边，选择表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

为多个域配置 **LDAP** 组提取

April 6, 2020

如果您有多个域进行身份验证，并且正在使用 StoreFront 或 Web Interface，则可以将 Citrix Gateway 配置为使用组提取将正确的域名发送到 Web Interface。

在 Active Directory 中，您需要为网络中的每个域创建一个组。创建组后，添加属于该组和指定域的用户。在 Active Directory 中配置组后，您可以在 Citrix Gateway 上为多个域配置 LDAP 组提取。

要为多个域配置 Citrix Gateway 以进行组提取，您需要创建与网络中域数量相同的会话和身份验证策略。例如，您有两个域，名为 Sampa 和子域。每个域接收一个会话策略和一个身份验证策略。

创建策略后，您可以在 Citrix Gateway 上创建组，并将会话策略绑定到该组。然后，将身份验证策略绑定到虚拟服务器。

如果在多个域中部署 StoreFront，则域之间必须存在信任关系。

如果在多个域中部署 Citrix Endpoint Management 或 Web Interface，这些域不需要相互信任。

创建用于组提取的会话策略

April 6, 2020

创建用于组提取的会话策略的第一步是创建两个会话配置文件并设置以下参数：

- 启用 ICA 代理。
- 添加 Web Interface Web 地址。
- 添加 Windows 域。
- 将配置文件添加到会话策略并将表达式设置为 true。

创建用于组提取的会话配置文件

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格中，单击配置文件选项卡，然后单击添加。
3. 在“名称”中，键入配置文件的名称。例如，键入 Sampa。
4. 在“已发布的应用程序”选项卡上，执行以下操作：
    a) 在 ICA 代理旁边，单击覆盖全局，然后选择开。
    b) 在 Web Interface 地址旁边，单击覆盖全局，然后键入 Web Interface 的 Web 地址。
    c) 在单点登录域旁边，单击覆盖全局，键入 Windows 域的名称，然后单击创建。
5. 在“名称”中，清除第一个域的名称，然后键入第二个域的名称，如“子”。
6. 在单点登录域旁边，清除第一个 Windows 域的名称，然后键入第二个域的名称，单击创建，然后单击关闭。

创建会话配置文件后，您将创建两个会话策略。每个会话策略使用其中一个配置文件。

创建会话策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件中，选择第一个域的配置文件。
5. 在命名表达式旁边，单击常规，选择 True 值，单击添加表达式，然后单击创建。
6. 在“名称”中，将名称更改为第二个域。
7. 在“请求配置文件”中，选择第二个域的配置文件，单击“创建”，然后单击“关闭”。

为多个域创建 **LDAP** 身份验证策略

April 6, 2020

在 Citrix Gateway 上创建会话策略后，您将创建几乎相同的 LDAP 身份验证策略。配置身份验证策略时，重要字段是搜索筛选器。在此字段中，您必须键入在 Active Directory 中创建的组的名称。

首先创建身份验证配置文件，然后创建身份验证策略。

为多域组提取创建身份验证配置文件

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“策略”>“身份验证”。
2. 在导航窗格中，单击 LDAP。
3. 在详细信息窗格中，单击“服务器”选项卡，然后单击“添加”。
4. 在“名称”中，键入第一个域的名称，如 Sampa。
5. 配置 LDAP 服务器的设置，然后单击创建。
6. 重复步骤 3、4 和 5 以配置第二个域的身份验证配置文件，然后单击“关闭”。

创建和保存配置文件后，创建身份验证策略。

为多域组提取创建身份验证策略

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“策略”>“身份验证”。
2. 在详细信息窗格中，单击策略选项卡，然后单击添加。
3. 在“名称”中，键入第一个域的名称。
4. 在身份验证类型中，选择 LDAP。
5. 在服务器中，选择第一个域的身份验证配置文件。
6. 在命名表达式旁边，单击常规，选择 True 值，单击添加表达式，然后单击创建。
7. 在“名称”中，键入第二个域的名称。
8. 在服务器中，选择第二个域的身份验证配置文件，单击创建，然后单击关闭。

为多域的 **LDAP** 组提取创建组和绑定策略

April 6, 2020

创建身份验证策略后，您可以在 Citrix Gateway 上创建组。创建组后，将身份验证策略绑定到虚拟服务器。

在 **Citrix Gateway** 上创建组

1. 在配置实用程序中，在 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“用户管理”，然后单击 “AAA 组”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在 “组名称” 中，键入第一个 Active Directory 组的名称。
   重要提示：在 Citrix Gateway 上创建用于从多个域提取的组时，组名称必须与在 Active Directory 中定义的组相同。组名称也区分大小写，大小写必须与您在 Active Directory 中输入的大小写匹配。
4. 在 “策略” 选项卡上，单击 “会话”，然后单击 “插入策略”。
5. 在策略名称下，双击策略，然后单击创建。

将身份验证策略绑定到虚拟服务器

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway，然后单击 “虚拟服务器”。
2. 在配置实用程序的导航窗格中，展开 Citrix Gateway，然后单击虚拟服务器。
3. 在详细信息窗格中，单击虚拟服务器，然后单击打开。
4. 在 “身份验证” 选项卡上，单击 “主要” 的 “策略名称” 下，双击 “插入策略”，然后选择第一个身份验证策略。
5. 在 “策略名称” 下，单击 “插入策略”，双击第二个身份验证策略，然后单击 “确定”。

配置客户端证书身份验证

April 6, 2020

登录到 Citrix Gateway 虚拟服务器的用户也可以根据提供给虚拟服务器的客户端证书的属性进行身份验证。客户端证书身份验证也可以与其他身份验证类型（如 LDAP 或 RADIUS）一起使用，以提供双重身份验证。

要根据客户端证书属性对用户进行身份验证，应在虚拟服务器上启用客户端身份验证，并应请求客户端证书。必须将根证书绑定到 Citrix Gateway 上的虚拟服务器。

当用户登录到 Citrix Gateway 虚拟服务器时，身份验证后，将从证书的指定字段中提取用户名信息。通常，此字段是主题：CN。如果成功提取用户名，则会对用户进行身份验证。如果用户在安全套接字层 (SSL) 握手期间未提供有效证书，或者用户名提取失败，则身份验证将失败。

您可以通过将默认身份验证类型设置为使用客户端证书，基于客户端证书对用户进行身份验证。您还可以创建证书操作，该操作定义基于客户端 SSL 证书的身份验证期间要执行的操作。

将客户端证书配置为默认身份验证类型

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改身份验证设置”。
3. 在“最大用户数”中，键入可以使用客户端证书进行身份验证的用户数。
4. 在“默认身份验证类型”中，选择“证书”。
5. 在“用户名字段”中，选择用于保存用户名的证书字段的类型。
6. 在“组名称字段”中，选择保存组名称的证书字段的类型。
7. 在默认授权组中，键入默认组的名称，然后单击确定。

从客户端证书中提取用户名

如果在 Citrix Gateway 上启用了客户端证书身份验证，则会根据客户端证书的某些属性对用户进行身份验证。身份验证成功完成后，将从证书中提取用户名或用户和组名称，并应用为该用户指定的任何策略。

配置和绑定客户端证书身份验证策略

January 12, 2022

您可以创建客户端证书身份验证策略并将其绑定到虚拟服务器。您可以使用策略限制对特定组或用户的访问。此策略优先于全局策略。

要配置客户端证书身份验证策略：

1. 在配置实用程序中的“配置”选项卡上，展开 **Citrix Gateway >“策略”>“身份验证”**。
2. 在导航窗格的 身份验证下，单击 **CERT**。
3. 在详细信息窗格中，单击 **Add**（添加）。
4. 在 名称字段中，键入策略的名称。
5. 在 服务器旁边，单击 新建。
6. 在“名称”中，键入配置文件的名称。
7. 在“双因子”旁边，选择“关”。
8. 在“用户名”字段和“组名”字段中，选择值，然后单击“创建”。
   注意：如果以前已将客户端证书配置为默认身份验证类型，请使用与策略使用的名称相同。如果您完成了默认身份验证类型的“用
   户名”字段和“
   组名”字段，则对配置文件使用相同的值。
9. 在“创建身份验证策略”对话框的 命名表达式旁边，选择表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

将客户端证书策略绑定到虚拟服务器：

配置客户端证书身份验证策略后，可以将其绑定到虚拟服务器。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** ，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击虚拟服务器，然后单击 打开。
3. 在“配置 **Citrix Gateway** 虚拟服务器”对话框中，单击“身份验证”选项卡。
4. 单击 主要或 辅助。
5. 在 详细信息下，单击 插入策略。
6. 在 策略名称中，选择策略，然后单 击确定。

要配置虚拟服务器以请求客户端证书，请执行以下操作：

要使用客户端证书进行身份验证时，必须配置虚拟服务器，以便在 SSL 握手期间请求客户端证书。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** ，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击 虚拟服务器，然后单击 打开。
3. 在 证书选项卡上，单击 **SSL** 参数。
4. 在“其他”下，单击“客户端身份验证”。
5. 在“客户端证书”中，选 择“可选”或“强制”，然后单击“确定”两次。如果要在同一虚拟服务器上允许其他身份验证类型并且不需要使用客户端证书，请选择“可选”。

> 注意
>
> - 有关回调 URL 的更多信息，请参阅导入 Citrix Gateway。
> - 有关证书的详细信息，请参阅安装、链接和更新证书。

配置双重客户端证书身份验证

April 6, 2020

您可以将客户端证书配置为首先对用户进行身份验证，然后要求用户使用辅助身份验证类型（如 LDAP 或 RADIUS）登录。在这种情况下，客户端证书首先对用户进行身份验证。然后，将显示一个登录页面，用户可以在其中输入用户名和密码。安全套接字层 (SSL) 握手完成后，登录序列可以采用以下两种路径之一：

- 用户名和组都不会从证书中提取。登录页面向用户显示，并提示输入有效的登录凭据。Citrix Gateway 对用户凭据进行正常密码身份验证的情况进行身份验证。
- 从客户端证书中提取用户名和组名。如果仅提取用户名，则登录页面显示登录名所在的用户，并且用户无法修改该名称。只有密码字段为空。

Citrix Gateway 在第二轮身份验证期间提取的组信息会附加到 Citrix Gateway 从证书中提取的组信息（如果有）。

配置智能卡身份验证

September 26, 2022

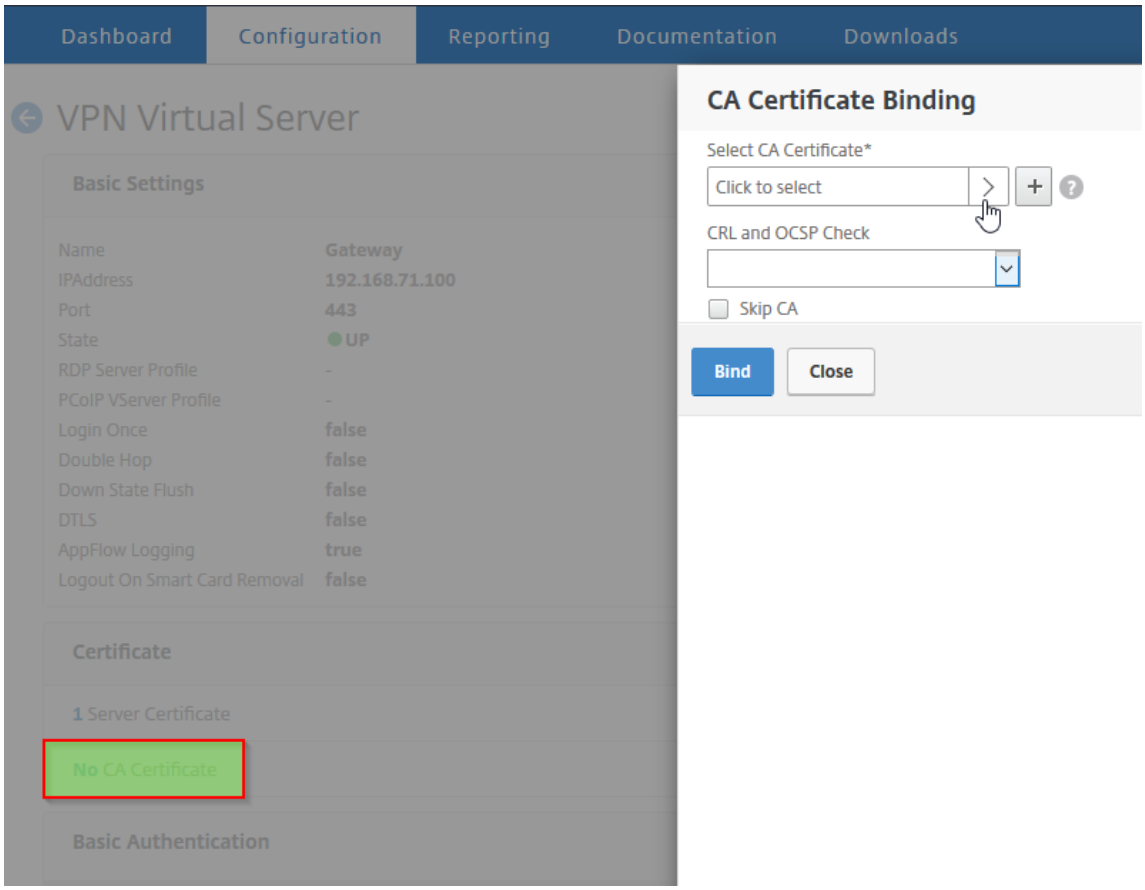
您可以将 Citrix Gateway 配置为使用加密智能卡对用户进行身份验证。

要将智能卡配置为与 Citrix Gateway 一起使用，您需要执行以下操作：

- 创建证书身份验证策略。有关详细信息，请参阅配置客户端证书身份验证。
- 将身份验证策略绑定到虚拟服务器。
- 将颁发客户端证书的证书颁发机构 (CA) 的根证书添加到 Citrix Gateway。有关详细信息，请参阅在 Citrix Gateway 上安装根证书的步骤。

  重要提示：将根证书添加到虚拟服务器进行智能卡身份验证时，必须从 “选择 **CA** 证书” 下拉框中选择证书，如下图所示。

  图 1. 为智能卡身份验证添加根证书



创建客户端证书后，可以将证书（称为闪存）写入智能卡上。完成该步骤后，可以测试智能卡。

如果为智能卡直通身份验证配置 Web Interface，如果存在以下条件之一，则单点登录 Web Interface 将失败：

- 如果您将 “已发布的应用程序” 选项卡上的域设置为 mydomain.com 而不是我的域。
- 如果未在 “已发布的应用程序” 选项卡上设置域名，并且如果运行该命令，则该值设置为 1。在这种情况下，UserPrincipalName 包含域名 “mydomain.com”。

您可以使用智能卡身份验证来简化用户的登录过程，同时提高用户访问基础结构的安全性。对内部企业网络的访问受使用公钥基础结构的基于证书的双重身份验证的保护。私钥受硬件控制保护，离不开智能卡。使用智能卡和 PIN，用户可

以方便地从一系列的企业设备访问其桌面和应用程序。

可以使用智能卡通过 StoreFront 对 Citrix Virtual Apps and Desktops 提供的桌面和应用程序进行用户身份验证。登录 StoreFront 的智能卡用户也可以访问 Citrix Endpoint Management 提供的应用程序。但是，用户必须再次进行身份验证才能访问使用客户端证书身份验证的 Endpoint Management Web 应用程序。

有关更多信息，请参阅 StoreFront 文档中的配置智能卡身份验证。

使用安全 **ICA** 连接配置智能卡身份验证

通过使用在 Citrix Gateway 上配置的具有单点登录功能的智能卡登录并建立安全 ICA 连接的用户可能会在两个不同的时间收到提示输入其个人标识号 (PIN)：登录时和尝试启动已发布资源时。如果 Web 浏览器和 Citrix Workspace 应用程序使用配置为使用客户端证书的同一虚拟服务器，则会出现此情况。Citrix Workspace 应用程序不会与 Web 浏览器共享进程或安全套接字层 (SSL) 连接。因此，当 ICA 连接完成与 Citrix Gateway 的 SSL 握手时，第二次需要客户端证书。

要防止用户接收第二个 PIN 提示，您必须更改两个设置：

- 必须禁用 VPN 虚拟服务器上的客户端身份验证。
- 必须启用 SSL 重新协商。

配置虚拟服务器后，将一个或多个 STA 服务器绑定到虚拟服务器，如中所述在 Web Interface 5.3 中配置 Citrix Gateway 设置。

您可能还需要测试智能卡身份验证。

要禁用客户端身份验证，请执行以下操作：

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 在主详细信息窗格中选择相关虚拟服务器，然后单击编辑。
3. 在“高级选项”窗格中，单击“SSL 参数”。
4. 清除“客户端身份验证”复选框。
5. 单击完成。

要启用 SSL 重新协商，请执行以下操作：

1. 使用配置实用程序，从“配置”选项卡，导航到“流量管理”，然后点击 SSL。
2. 在主面板中，单击更改高级 SSL 设置。
3. 从“拒绝 SSL 重新协商”菜单中，选择“否”。

要测试智能卡身份验证，请执行以下操作：

1. 将智能卡连接到用户设备。
2. 打开 Web 浏览器并登录到 Citrix Gateway。

配置通用访问卡

April 6, 2020

美国国防部使用通用出入卡进行身份识别和身份验证。

要配置通用访问卡，请执行以下操作：

1. 在配置实用程序中的 “配置” 选项卡上，展开 “Citrix Gateway”>“策略”>“身份验证”。
2. 在 “服务器” 选项卡上，单击 “添加”。
3. 在 “名称” 中，键入名称。
4. 在 “身份验证类型” 中，选择 “证书”。
5. 在用户名字段中，键入 SubjectAltName:PrincipalName，然后单击 “创建”。
6. 在 “策略” 选项卡上，创建使用此服务器的策略，然后将策略绑定到虚拟服务器。

配置 **RADIUS** 身份验证

April 6, 2020

您可以将 Citrix Gateway 配置为使用一个或多个 RADIUS 服务器对用户访问进行身份验证。如果您使用的是 RSA SecurID、SafeWord 或 Gemalto Protiva 产品，则通过使用 RADIUS 服务器对其中的每个产品进行配置。

您的配置可能需要使用网络访问服务器 IP 地址 (NAS IP) 或网络访问服务器标识符 (NAS ID)。将 Citrix Gateway 配置为使用 RADIUS 身份验证服务器时，请遵循以下准则：

- 如果启用 NAS IP 的使用，设备将其配置的 IP 地址发送到 RADIUS 服务器，而不是用于建立 RADIUS 连接的源 IP 地址。
- 如果配置 NAS ID，设备会将标识符发送到 RADIUS 服务器。如果未配置 NAS ID，设备将其主机名发送到 RADIUS 服务器。
- 启用 NAS IP 后，设备会忽略使用 NAS IP 配置的与 RADIUS 服务器通信的任何 NAS ID。

配置金雅拓 **Protiva**

Protiva 是金雅拓开发的强大身份验证平台，利用金雅拓智能卡身份验证的优势。使用 Protiva，用户使用 Protiva 设备生成的用户名、密码和一次性密码登录。与 RSA SecurID 类似，身份验证请求将发送到 Protiva 身份验证服务器，服务器验证或拒绝密码。要将金雅拓 Protiva 配置为与 Citrix Gateway 配合使用，请使用以下准则：

- 安装 Protiva 服务器。
- 在 Microsoft IAS RADIUS 服务器上安装 Protiva SAS 代理软件，该软件将扩展 Internet 身份验证服务器 (IAS)。请务必记下 IAS 服务器的 IP 地址和端口号。
- 在 Citrix Gateway 上配置 RADIUS 身份验证配置文件并输入 Protiva 服务器的设置。

配置 **SafeWord**

SafeWord 产品线使用基于令牌的密码提供安全身份验证。用户输入密码后，SafeWord 立即使密码无效，无法再次使用。当您配置 SafeWord 服务器时，您需要以下信息：

- Citrix Gateway 的 IP 地址。这应与您在 RADIUS 服务器客户端配置中配置的 IP 地址相同。Citrix Gateway 使用内部 IP 地址与 RADIUS 服务器进行通信。配置共享机密时，请使用内部 IP 地址。如果配置两个设备以实现高可用性，请使用虚拟内部 IP 地址。
- 一个共享的秘密
- SafeWord 服务器的 IP 地址和端口。默认端口号为 1812。

配置 **RADIUS** 身份验证

April 6, 2020

1. 在配置实用程序中的 “配置” 选项卡上，展开 “Citrix Gateway”>“策略”>“身份验证”。
2. 单击 RADIUS，然后在详细信息窗格中的策略选项卡上，单击添加。
3. 在 “创建身份验证策略” 对话框的 “名称” 中，键入策略的名称。
4. 在 “名称” 中，键入策略的名称。
5. 在服务器旁边，单击新建。
6. 在 “创建身份验证策略” 对话框的 “名称” 中，键入服务器的名称。
7. 在 “服务器” 下的 “IP 地址” 中，键入 RADIUS 服务器的 IP 地址。
8. 在端口中，键入端口。默认值为 1812。
9. 在 “详细信息” 下的 “私有密钥” 和 “确认私有密钥” 中，键入 RADIUS 服务器密钥。
10. 在 NAS ID 中，键入标识符号，然后单击创建。
11. 在 “创建身份验证策略” 对话框的命名表达式旁边，选择表达式，单击 “添加表达式”，单击 “创建”，然后单击 “关闭”。

选择 **RADIUS** 身份验证协议

April 6, 2020

Citrix Gateway 支持已配置为使用多种协议进行用户身份验证的 RADIUS 实现，其中包括：

- 密码身份验证协议 (PAP)
- 质疑握手身份验证协议 (CHAP)
- Microsoft 质询握手身份验证协议（MS-CHAP 版本 1 和版本 2）

如果 Citrix Gateway 的部署配置为使用 RADIUS 身份验证，并且 RADIUS 服务器配置为使用 PAP，则可以通过向 RADIUS 服务器分配强共享密钥来加强用户身份验证。强 RADIUS 共享秘密由大写和小写字母、数字和标点的随机序

列组成，长度至少为 22 个字符。如果可能，请使用随机字符生成程序来确定 RADIUS 共享机密。

要进一步保护 RADIUS 流量，请为每个 Citrix Gateway 设备或虚拟服务器分配不同的共享密钥。在 RADIUS 服务器上定义客户端时，还可以为每个客户端分配单独的共享机密。如果执行此操作，则必须单独配置使用 RADIUS 身份验证的每个 Citrix Gateway 策略。

创建 RADIUS 策略时，您可以在 Citrix Gateway 上配置共享机密，作为策略的一部分。

配置 **IP** 地址提取

April 6, 2020

您可以将 Citrix Gateway 配置为从 RADIUS 服务器中提取 IP 地址。当用户使用 RADIUS 服务器进行身份验证时，服务器将返回分配给用户的框架 IP 地址（在访问请求中也称为 RADIUS 属性 8 帧 IP 地址）。以下是 IP 地址提取的组件：

- 允许远程 RADIUS 服务器为登录到 Citrix Gateway 的用户提供内部网络中的 IP 地址。
- 允许使用 **ipaddress** 类型对任何 RADIUS 属性进行配置，包括供应商编码的属性。

配置 RADIUS 服务器进行 IP 地址提取时，您可以配置供应商标识符和属性类型。供应商 ID 和属性用于建立 RADIUS 客户端和 RADIUS 服务器之间的关联。

- 供应商标识符 (ID) 使 RADIUS 服务器能够从 RADIUS 服务器上配置的 IP 地址池中为客户端分配 IP 地址。供应商 ID 是 RADIUS 响应中提供内部网络 IP 地址的属性。值为零表示属性未经供应商编码
- 属性类型是 RADIUS 响应中的远程 IP 地址属性。最小值为 1，最大值为 255。

一个常见的配置是提取 RADIUS 属性框架 **IP** 地址。供应商 ID 设置为 0 或未指定。属性类型设置为 8。

要从 RADIUS 服务器配置 IP 地址提取，请执行以下操作：

1. 在配置实用程序中的 “配置” 选项卡上，展开 “Citrix Gateway”>“策略”>“身份验证”。
2. 单击 RADIUS，然后在详细信息窗格中的策略选项卡上，选择 RADIUS 策略，然后单击打开。
3. 在 “配置身份验证策略” 对话框中，单击 “服务器” 旁边的 “修改”。
4. 在 “详细信息” 下的 “组供应商标识符” 中，键入值。
5. 在 “组属性类型” 中，键入值，然后单击 “确定” 两次。

配置 **RADIUS** 组提取

April 6, 2020

您可以使用称为组提取的方法来配置 RADIUS 授权。配置组提取允许您管理 RADIUS 服务器上的用户，而不是将其添加到 Citrix Gateway。

您可以通过使用身份验证策略并配置组供应商标识符 (ID)、组属性类型、组前缀和组分隔符来配置 RADIUS 授权。配置策略时，您将添加表达式，然后将策略全局绑定或绑定到虚拟服务器。

在 **Windows Server 2003** 上配置 **RADIUS**

如果在 Windows Server 2003 上使用 Microsoft Internet 身份验证服务 (IAS) 进行 RADIUS 授权，则 Citrix Gateway 的配置期间，您需要提供以下信息：

- 供应商 ID 是您在 IAS 中输入的供应商特定的代码。
- 类型是供应商分配的属性编号。
- 属性名称是您在 IAS 中定义的属性名称的类型。默认名称为 CTXSUserGroups=

如果 RADIUS 服务器上未安装 IAS，您可以从控制面板中的添加或删除程序安装它。有关详细信息，请参阅 Windows 联机帮助。

若要配置 IAS，请使用 Microsoft 管理控制台 (MMC) 并安装 IAS 的管理单元。按照向导操作，确保您选择了以下设置：

- 选择本地计算机。
- 选择远程访问策略并创建自定义策略。
- 为策略选择 Windows 组。
- 选择以下协议之一：
  - Microsoft 质询握手身份验证协议版本 2 (MS-CHAP v2)
  - Microsoft 质询握手身份验证协议 (MS-CHAP)
  - 质疑握手身份验证协议 (CHAP)
  - 未加密身份验证（PAP、SPAP）
- 选择供应商特定属性。

  供应商特定属性需要将您在服务器组中定义的用户与 Citrix Gateway 上的用户进行匹配。为满足此要求，请将供应商特定的属性发送到 Citrix Gateway。请确保选择 RADIUS = 标准。
- RADIUS 默认值为 0。将此编号用于供应商代码。
- 供应商分配的属性编号为 0。

  这是为用户组属性分配的编号。属性采用字符串格式。
- 选择属性格式的字符串。

  属性值需要属性名称和组。

  对于 Access Gateway，属性值为 CTXSUserGroups=groupname。如果定义了两个组（例如销售和财务），属性值为 CTXSUserGroups=sales;finance。用分号分隔每个组。
- 删除“编辑拨入配置文件”对话框中的所有其他条目，保留“特定于供应商”的条目。

在 IAS 中配置远程访问策略后，可以在 Citrix Gateway 上配置 RADIUS 身份验证和授权。

配置 RADIUS 身份验证时，请使用您在 IAS 服务器上配置的设置。

为 **Windows Server 2008** 上的身份验证配置 **RADIUS**

在 Windows Server 2008 上，您可以使用网络策略服务器 (NPS) 来配置 RADIUS 身份验证和授权，该服务器替换 Internet 身份验证服务 (IAS)。您可以使用服务器管理器并添加 NPS 作为安装 NPS 的角色。

安装 NPS 时，请选择网络策略服务。安装后，可以通过在“开始”菜单上从“管理服务”启动 NPS 来配置网络的 RADIUS 设置。打开 NPS 时，将 Citrix Gateway 添加为 RADIUS 客户端，然后配置服务器组。

配置 RADIUS 客户端时，请确保选择以下设置：

- 对于供应商名称，选择 RADIUS 标准。
- 记下共享机密，因为您需要在 Citrix Gateway 上配置相同的共享机密。

对于 RADIUS 组，您需要 RADIUS 服务器的 IP 地址或主机名。请勿更改默认设置。

配置 RADIUS 客户端和组后，您可以在以下两个策略中配置设置：

- 连接请求策略，您可以在其中配置 Citrix Gateway 连接的设置，包括网络服务器的类型、网络策略的条件以及策略的设置。
- 配置可扩展身份验证协议 (EAP) 身份验证和供应商特定属性的网络策略。

配置连接请求策略时，请为网络服务器的类型选择“未指定”。然后，您可以通过选择 NAS 端口类型作为条件，虚拟 (VPN) 作为值来配置您的条件。

配置网络策略时，需要配置以下设置：

- 选择远程访问服务器（VPN 拨号）作为网络访问服务器的类型。
- 为 EAP 选择加密身份验证 (CHAP) 和未加密身份验证 (PAP 和 SPAP)。
- 为供应商特定属性选择 RADIUS 标准。

  默认属性编号为 26。此属性用于 RADIUS 授权。

  Citrix Gateway 需要供应商特定的属性来匹配服务器上组中定义的用户与 Citrix Gateway 上的用户。这可以通过将供应商特定的属性发送到 Citrix Gateway 来完成。

- 选择属性格式的字符串。

  属性值需要属性名称和组。

  对于 Citrix Gateway，属性值为 CTXSUserGroups= groupname。如果定义了两个组（例如销售和财务），属性值为 CTXSUserGroups=sales;finance。用分号分隔每个组。

- 分隔符是您在 NPS 上用来分隔组（例如分号、冒号、空格或句点）的分隔符。

在 IAS 中配置远程访问策略后，可以在 Citrix Gateway 上配置 RADIUS 身份验证和授权。

配置 **RADIUS** 授权

April 6, 2020

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“策略”>“身份验证”。
2. 点击 RADIUS。
3. 在策略选项卡中，单击添加。
4. 在“名称”中，键入策略的名称。
5. 在服务器下方 * 点击 +
6. 在名称中，键入 RADIUS 服务器的名称。
7. 在“服务器”下，键入 RADIUS 服务器的 IP 地址和端口。
8. 在“详细信息”下，输入组供应商标识符和组属性类型的值。
9. 在“密码编码”中，选择身份验证协议，然后单击“创建”。
10. 在“创建身份验证策略”对话框的命名表达式旁边，选择表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置 **RADIUS** 用户核算

April 6, 2020

Citrix Gateway 可以向 RADIUS 记帐服务器发送用户会话启动和停止消息。为每个用户会话发送的消息包括 RFC2866 中定义的属性的子集。表 1 列出了受支持的属性以及发送它们的 RADIUS 记帐消息（RAD_START 和 RAD_STOP）的类型。表 2 列出了可分配给“通知终止-原因”属性的预定义值，以及相应的 Citrix Gateway 事件。

表 1. 支持的 RADIUS 属性

属性	意思是什么意思	RAD_START	RAD_STOP
用户名称	与会话关联的用户名。	X	X
会话编号	NetScaler 会话 ID。	X	X
会话时间	会话持续时间秒。		X
终止原因	账户终止的原因（见下文）。		X

表 2. RADIUS 终止原因

NetScaler 注销方法	RADIUS 终止原因
LOGOUT_SESSN_TIMEDOUT	RAD_TERM_SESSION_TIMEOUT
LOGOUT_SESSN_INITIATEDBYUSER	RAD_TERM_USER_REQUEST
LOGOUT_SESSN_KILLEDBYADMIN	RAD_TERM_ADMIN_RESET
LOGOUT_SESSN_TLOGIN	RAD_TERM_NAS_REQUEST

NetScaler 注销方法	RADIUS 终止原因
LOGOUT_SESSN_MAXLICRCHD	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_CLISECCHK_FAILED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_PREAUTH_CHANGED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_COOKIE_MISMATCH	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_DHT	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_2FACTOR_FAIL	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_ICALIC	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_INTERNALERR	RAD_TERM_NAS_ERROR
其他	RAD_TERM_NAS_ERROR

配置 RADIUS 用户记帐需要创建一对策略。第一个策略是 RADIUS 身份验证策略，指定要向其发送记帐消息的 RADIUS 服务器。第二个是使用 RADIUS 记帐策略作为其操作的会话策略。

要配置 RADIUS 用户记帐，必须：

1. 创建 RADIUS 策略来定义 RADIUS 记帐服务器。会计服务器可以是用于 RADIUS 身份验证的同一服务器。
2. 使用 RADIUS 策略作为指定 RADIUS 用户记帐服务器的操作，创建会话策略。
3. 全局绑定会话策略，以便它应用于所有流量，或应用于 Citrix Gateway 虚拟服务器，以便它仅应用于流经该虚拟服务器的流量。

创建 **RADIUS** 策略

1. 在配置实用程序的导航窗格中，展开 Citrix Gateway 节点，然后展开策略。
2. 展开身份验证并选择 RADIUS。
3. 在详细信息窗格的“策略”选项卡上，单击“添加”。
4. 输入策略的名称。
5. 从服务器菜单中选择一个服务器，或单击 + 图标，然后按照提示添加新 RADIUS 服务器。
6. 在“表达式”窗格中，从“已保存的策略表达式”菜单中，选择 ns_true。
7. 单击创建。

创建会话策略

配置指定 RADIUS 记帐服务器的 RADIUS 策略后，创建在操作中应用此记帐服务器的会话策略，如下所示：

1. 在配置实用程序的导航窗格中，展开 Citrix Gateway 节点，然后展开策略。
2. 选择会话。

3. 在主详细信息窗格中，选择添加。
4. 输入策略的名称。
5. 在 “操作” 菜单中，单击 “+” 图标以添加新的会话操作。
6. 输入会话操作的名称。
7. 单击客户体验选项卡。
8. 在记帐策略菜单中，选择您之前创建的 RADIUS 策略。
9. 单击创建。
10. 在 “表达式” 窗格中，从 “已保存的策略表达式” 菜单中，选择 ns_true。
11. 单击创建。

全局绑定会话策略

1. 在配置实用程序的导航窗格中，展开 Citrix Gateway 节点，然后展开策略。
2. 选择会话。
3. 从主详细信息窗格的 “操作” 菜单中，选择 “全局绑定”。
4. 单击 Bind（绑定）。
5. 在 “策略” 窗格中，选择您之前创建的会话策略，然后单击 “插入”。
6. 在策略列表中，单击会话策略的优先级条目，然后输入介于 0 到 64000 之间的值。
7. 单击确定。

将会话策略绑定到 **Citrix Gateway** 虚拟服务器

1. 在配置实用程序的导航窗格中，展开 Citrix Gateway 节点，然后选择虚拟服务器。
2. 在主详细信息窗格中，选择一个虚拟服务器，然后单击编辑。
3. 在 “策略” 窗格中，单击 “+” 图标以选择策略。
4. 从 “选择策略” 菜单中，选择 “会话”，并确保在 “选择类型” 菜单中选择了 “请求”。
5. 单击继续。
6. 单击 Bind（绑定）。
7. 在 “策略” 窗格中，选择您之前创建的会话策略，然后单击 “插入”。
8. 单击确定。

配置 **SAML** 身份验证

April 6, 2020

安全断言标记语言 (SAML) 是一种基于 XML 的标准，用于在身份提供商 (IdP) 和服务提供商之间交换身份验证和授权。Citrix Gateway 支持 SAML 身份验证。

配置 SAML 身份验证时，您将创建以下设置：

- IdP 证书名称。这是与 IdP 上的私钥对应的公钥。
- 重定向 URL。这是身份验证 IdP 的 URL。未经身份验证的用户将被重定向到此 URL。
- 用户字段。如果 IdP 发送的用户名格式不同于主题标签的 NameIdentifier 标签，则可以使用此字段提取用户名。这是一个可选设置。
- 签名证书名称。这是 Citrix Gateway 服务器的私钥，用于对 IdP 签名身份验证请求。如果未配置证书名称，则发送断言未签名或拒绝身份验证请求。
- SAML 发行者名称。发送身份验证请求时使用此值。发行者字段中必须有一个唯一的名称，以表示发送断言的机构。这是一个可选字段。
- 默认身份验证组。这是身份验证服务器上对用户进行身份验证的组。
- 两个因素。此设置启用或禁用双重身份验证。
- 拒绝未签名的断言。如果启用，Citrix Gateway 将拒绝用户身份验证，如果未配置签名证书名称。

Citrix Gateway 支持 HTTP POST 绑定。在此绑定中，发送方回复用户的 200 OK，其中包含包含所需信息的表单自动发布。具体而言，该默认表单必须包含两个名为 SAMLRequest 和 SAMLResponse 的隐藏字段，具体取决于表单是请求还是响应。该表格还包括 RelayState，即发送方用于发送依赖方未处理的任意信息的状态或信息。依赖方只是将信息发回，以便当发送方与 RelayState 一起获取断言时，发送方知道接下来该怎么做。Citrix 建议您对 RelayState 进行加密或模糊处理。

配置 **Active Directory** 联合身份验证服务 **2.0**

可以在联合服务器角色中使用的任何 Windows Server 2008 或 Windows Server 2012 计算机上配置 Active Directory 联合身份验证服务 (AD FS) 2.0。将 AD FS 服务器配置为使用 Citrix Gateway 时，需要使用 Windows Server 2008 或 Windows 服务器 2012 中的信赖方信任向导配置以下参数。

Windows Server 2008 参数：

- 信赖方信托。您可以提供 Citrix Gateway 元数据文件位置https://vserver.fqdn.com/ns.metadata.xml，例如 vserver.fqdn.com 是 Citrix Gateway 虚拟服务器的完全限定域名 (FQDN)。您可以在绑定到虚拟服务器的服务器证书上找到 FQDN。
- 授权规则。您可以允许或拒绝用户访问信赖方。

Windows Server 2012 参数：

- 信赖方信托。您可以提供 Citrix Gateway 元数据文件位置https://vserver.fqdn.com/ns.metadata.xml，例如 vserver.fqdn.com 是 Citrix Gateway 虚拟服务器的完全限定域名 (FQDN)。您可以在绑定到虚拟服务器的服务器证书上找到 FQDN。
- AD FS 简介。选择 AD FS 配置文件。
- Certificate（证书）。Citrix Gateway 不支持加密。您无需选择证书。
- 启用对 SAML 2.0 WebSSO 协议的支持。这样可以支持 SAML 2.0 SSO。您可以提供 Citrix Gateway 虚拟服务器 URL，例如https:netScaler.virtualServerName.com/cgi/samlauth。

  此 URL 是 Citrix Gateway 设备上的断言使用者服务 URL。这是一个常量参数，Citrix Gateway 需要对此 URL 进行 SAML 响应。

- 依赖方信任标识符。输入名称 Citrix Gateway。这是一个用于识别依赖方的 URL，例如https://netscalerGateway.virtualServerName.com/adfs/services/trust
- 授权规则。您可以允许或拒绝用户访问信赖方。
- 配置声明规则。您可以使用发布转换规则配置 LDAP 属性的值，并使用模板将 LDAP 属性发送为声明。然后，您可以配置 LDAP 设置，其中包括：
  - 电子邮件地址
  - sAMAccountName
  - 用户主体名称 (UPN)
  - memberOf
- 证书签名。您可以通过选择中继方的属性，然后添加证书来指定签名验证证书。

  如果签名证书小于 2048 位，则会显示一条警告消息。您可以忽略警告以继续。如果您正在配置测试部署，请禁用中继方上的证书吊销列表 (CRL)。如果不禁用检查，AD FS 将尝试 CRL 验证证书。

  您可以通过运行以下命令禁用 CRL：Set-ADFWRelayingPartyTrust - SigningCertficateRevocatonCheck None-TargetName NetScaler

配置设置后，请在完成中继方信任向导之前验证信赖方数据。您可以使用终端节点 URL 检查 Citrix Gateway 虚拟服务器证书，例如https://vserver.fqdn.com/cgi/samlauth。

在中继方信任向导中完成设置配置后，选择配置的信任，然后编辑属性。您需要执行以下操作：

- 将安全哈希算法设置为 SHA-1。

  注意：Citrix 仅支持 SHA-1。
- 删除加密证书。不支持加密断言。
- 编辑声明规则，包括以下内容：
  - 选择变换规则
  - 添加声明规则
  - 选择声明规则模板：将 LDAP 属性作为声明发送
  - 给出一个名字
  - 选择属性存储：Active Directory
  - <Active Directory parameters> 选择 LDAP 属性：
  - 选择“正在进行的声明规则”作为“名称 ID”

  注意：不支持属性名称 XML 标签。
- 配置单次注销的注销 URL。声明规则是发送注销 URL。自定义规则应如下：

```
pre codeblock => issue(Type = "logoutURL", Value = "https://<adfs.fqdn
.com>/adfs/ls/", Properties["http://schemas.xmlsoap.org/ws/2005/05/
identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML
:2.0:attrname-format:unspecified"); <!--NeedCopy-->
```


配置 AD FS 设置后，下载 AD FS 签名证书，然后在 Citrix Gateway 上创建证书密钥。然后，您可以使用证书和密钥在 Citrix Gateway 上配置 SAML 身份验证。

配置 **SAML** 双重身份验证

您可以配置 SAML 双重身份验证。使用 LDAP 身份验证配置 SAML 身份验证时，请使用以下准则：

- 如果 SAML 是主身份验证类型，请在 LDAP 策略中禁用身份验证并配置组提取。然后，将 LDAP 策略绑定为辅助身份验证类型。
- SAML 身份验证不使用密码，只使用用户名。此外，SAML 身份验证仅在身份验证成功时通知用户。如果 SAML 身份验证失败，则不会通知用户。由于未发送故障响应，SAML 必须是级联中的最后一个策略或唯一策略。
- Citrix 建议您配置实际用户名而不是不透明字符串。
- SAML 不能绑定为辅助身份验证类型。

配置 **SAML** 身份验证

November 3, 2021

1. 在配置实用程序中的 “配置” 选项卡上，展开 “Citrix Gateway”>“策略”>“身份验证”。
2. 在导航窗格中，单击 SAML。
3. 在详细信息窗格中，单击 Add（添加）。
4. 在 “创建身份验证策略” 对话框的 “名称” 中，键入策略的名称。
5. 在服务器旁边，单击新建。
6. 在 “名称” 中，键入服务器配置文件的名称。
7. 在 IdP 证书名称中，选择证书或单击安装。这是 SAML 或 IDP 服务器上安装的证书。

   如果单击 “安装”，请添加证书和私钥。有关详细信息，请参阅安装和管理证书。
8. 在 “重定向 URL” 中，输入身份验证身份提供程序 (IdP) 的 URL。

   这是用户登录 SAML 服务器的 URL。这是 Citrix Gateway 将初始请求重定向到的服务器。
9. 在 “用户字段” 中，输入要提取的用户名。
10. 在 “签名证书名称” 中，为您在步骤 9 中选择的证书选择私钥。

    这是绑定到 AAA 虚拟 IP 地址的证书。SAML 颁发者名称是用户登录的完全限定域名 (FQDN)，例如 lb.example.com 或 ng.example.com。
11. 在 SAML 颁发者名称中，输入设备向其发送初始身份验证 (GET) 请求的负载平衡或 Citrix Gateway 虚拟 IP 地址的 FQDN。

12. 在默认身份验证组中，输入组名称。
13. 若要启用双因素身份验证，请在“双因素”中单击“开”。
14. 禁用拒绝无符号断言。仅当 SAML 或 IDP 服务器正在对 SAML 响应进行签名时，才启用此设置。
15. 单击 Create（创建），然后单击 Close（关闭）。
16. 在“创建身份验证策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“True 值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

使用 **SAML** 身份验证登录到 **Citrix Gateway**

March 22, 2022

您可以使用 SAML 身份验证使用 Citrix VPN 客户端和 Workspace 应用程序登录到 Citrix Gateway。插件仅通过绑定到身份验证虚拟服务器（即 nfactor 身份验证）的高级 SAML 策略支持 SAML 身份验证。

重要提示：当 SAML 策略直接绑定到 VPN 虚拟服务器（即非 nFactor 身份验证）时，插件不支持 SAML 身份验证。

支持的平台和应用程序

下表列出了支持 SAML 身份验证以登录 Citrix Gateway 的平台和应用程序。

产品	版本
Citrix Gateway	版本 12.0 版本构建 41.16 及更高版本
VPN 客户端	版本 12.1 构建 49.37 和更高版本。支持的平台：Windows 7、Windows 8、Windows 8.1、Windows 10
Workspace 应用程序版本	Windows：1808；Mac：1808

使用高级 **SAML** 策略配置 **SAML** 身份验证

有关使用高级 SAML 策略配置 SAML 身份验证的详细信息，请参阅Citrix ADC 作为 SAML IdP。

SAML 身份验证改进

April 6, 2020

此功能适用于拥有 SAML 知识的用户，并且使用此信息需要基本身份验证能力。读者必须了解 FIPS 才能使用这些信息。

以下 Citrix ADC 功能可用于与 SAML 2.0 规范兼容的第三方应用程序/服务器：

- SAML 服务提供商 (SP)
- SAML 身份提供商 (IdP)

SP 和 IdP 允许云服务之间的单点登录 (SSO)。SAML SP 功能提供了一种解决来自 IdP 的用户声明的方法。IdP 可以是第三方服务或其他 Citrix ADC 设备。SAML IdP 功能用于断言用户登录并提供 SP 使用的声明。

作为 SAML 支持的一部分，IdP 和 SP 模块都对发送到对等方的数据进行数字签名。数字签名包括来自 SP 的身份验证请求、来自 IdP 的断言以及这两个实体之间的注销消息。数字签名验证邮件的真实性。

SAML SP 和 IdP 的当前实现在数据包引擎中执行签名计算。这些模块使用 SSL 证书对数据进行签名。在符合 FIPS 标准的 Citrix ADC 中，SSL 证书的私钥在数据包引擎或用户空间中不可用，因此 SAML 模块当前尚未准备好用于 FIPS 硬件。

本文档介绍了将签名计算卸载到 FIPS 卡的机制。签名验证是在软件中完成的，因为公钥是可用的。

解决方案

SAML 功能集得到增强，以使用 SSL API 进行签名卸载。有关这些受影响的 SAML 子功能的详细信息，请参阅 docs.citrix.com：

1. SAML SP 后绑定 - AuthnRequest 的签名
2. SAML IdP 后绑定-决议/响应的签名
3. SAML SP 单点注销方案 - SP 启动模型中 LogoutRequest 的签名，以及 IdP 启动模型中 LogoutResponse 的签名
4. SAML SP 工件绑定 - ArtifactResolve 请求的签名
5. SAML SP 重定向绑定 - AuthnRequest 的签名
6. SAML IdP 重定向绑定-回应/决定的签名
7. SAML SP 加密支持 — 断言解密

平台

API 只能卸载到 FIPS 平台。

配置

卸载配置在 FIPS 平台上自动执行。

但是，由于 SSL 私钥不适用于 FIPS 硬件中的用户空间，因此在 FIPS 硬件上创建 SSL 证书时会发生轻微的配置更改。

以下是配置信息：

- add ssl fipsKey fips-key

  然后，您需要创建 CSR 并在 CA 服务器上使用它来生成证书。然后，您可以在 /nsconfig/ssl 中复制该证书。让我们假设文件是 fips3cert.cer。

- add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key

  然后，您需要在 SAML SP 模块的 SAML 操作中指定此证书。

- set samlAction <name> -samlSigningCertName fips-cert

  同样，您需要在 SAML IdP 模块的 samlIdpProfile 中使用

- set samlidpprofile fipstest –samlIdpCertName fips-cert

第一次，你不会有上面描述的 fips-key。如果没有 FIPS 密钥，请按如下所述创建一个：https://support.citrix.com/servlet/KbServlet/download/29003-102-665378/NS9000_FIPS_6\[1\]\[1\].1.pdf

- create ssl fipskey <fipsKeyName> -modulus <positive_integer> [-exponent (3 | F4)]
- create certreq <reqFileName> -fipskeyName <string>

配置 **TACACS+** 身份验证

April 6, 2020

您可以配置 TACACS+ 服务器进行身份验证。与 RADIUS 身份验证类似，TACACS+ 使用私有密钥、IP 地址和端口号。默认端口号为 49。

要将 Citrix Gateway 配置为使用 TACACS+ 服务器，请提供服务器 IP 地址和 TACACS+ 密钥。只有当正在使用的服务器端口号不是默认端口号 49 时，才需要指定端口。

要使用用户界面配置 TACACS+ 身份验证，请执行以下步骤。

1. 在配置实用程序中的“配置”选项卡上，展开 **Citrix Gateway >“策略”>“**身份验证”。
2. 单击 **TACACS**。
3. 在详细信息窗格中，单击 **Add**（添加）。
4. 在 名称字段中，键入策略的名称。
5. 在“服务器”字段旁边，单击“添加”以创建新的 TACACS 服务器，或单击“编辑”对现有的 TACACS 服务器进行更改。
6. 在“名称”字段中，键入服务器的名称。
7. 在“**IP** 地址”下，键入 IP 地址。
8. 在“端口”下，使用默认端口号 49。
9. 在 **TACACS** 密钥字段中，键入密钥。在 确认 **TACACS** 密钥字段中，键入要确认的相同密钥。
10. 点击 更多。
11. 在 授权中，选择 开，然后单击 创建。

12. 在 创建身份验证 **TACACS** 策略对话框中，选择表达式，单击创建，然后单击关闭。

若要使用命令行界面配置 TACACS+ 身份验证，请键入以下命令。

```
add authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr
    |*>][-serverPort <port>] [-authTimeout <positive_integer>] {
 -tacacsSecret  }

[-authorization ( ON | OFF )] [-accounting ( ON | OFF )][-
    auditFailedCmds ( ON | OFF )] [-groupAttrName <string>][-
    defaultAuthenticationGroup <string>] [-Attribute1 <string>] [-
    Attribute2 <string>] [-Attribute3 <string>] [-Attribute4 <string>]
[-Attribute5 <string>] [-Attribute6 <string>] [-Attribute7 <string>] [-
    Attribute8 <string>] [-Attribute9 <string>] [-Attribute10 <string>]
[-Attribute11 <string>] [-Attribute12 <string>] [-Attribute13 <string>]
     [-Attribute14 <string>] [-Attribute15 <string>] [-Attribute16 <
    string>]
<!--NeedCopy-->
```

在 Citrix Gateway 中配置 TACACS+ 服务器设置后，绑定策略以使其处于活动状态。您可以在全局或虚拟服务器级别上绑定策略。有关绑定身份验证策略的更多信息，请参阅绑定身份验证策略。

清除配置基本不应清除 **TACACS** 配置

April 6, 2020

概述

此增强的重点是在执行清除配置命令时不清除所有 RBA（基于角色的访问）相关的配置。

当前的清除配置命令在以下三个级别之一执行：

• 基本的

• 延长

• 满

根据所选的级别，NetScaler 配置将被清除并重置为出厂默认值。

使用的命令是：

```
clear ns config \[-force\] \<level\>
```

新命令添加了一个旋钮，以允许/拒绝删除所有与 RBA 相关的配置。

新命令

描述的是 Clear RBAconfig 功能：

1. 是/否带默认旋钮：是。

   管理员决定是否保留 RBA 配置。

2. 只支持清晰配置的基本级别。

3. 未清除以下配置：

   - 添加/绑定系统用户/组。
   - 添加 cmd 策略。
   - TACACS 命令。(添加 TACACS 操作/策略)。
   - 绑定全局系统

   注意：如果策略绑定到全局系统，否则将保留 TACACS 相关的配置（操作/策略），否则将被清除

CLI 配置

使用的命令

```
clear config [ - force] <level> [-RBAconfig]
```

默认情况下，它设置为 YES，并根据指定的级别清除配置。

如果 –RBAconfig 设置为 NO，则保留 RBA 相关的配置。包括以下内容：

- 添加/结合系统用户/组
- 绑定全局系统
- tacacs 相关命令（添加策略动作/策略）
- 添加 cmd 策略

配置多重身份验证

April 6, 2020

您可以在 Citrix Gateway 中配置两种类型的多重身份验证：

- 设置身份验证优先级级别的级联身份验证
- 双重身份验证，要求用户通过使用两种类型的身份验证登录

如果您有多个身份验证服务器，则可以设置身份验证策略的优先级。您设置的优先级级别决定了身份验证服务器验证用户凭据的顺序。优先级数较低的策略优先于数值较高的策略。

您可以让用户对两个不同的身份验证服务器进行身份验证。例如，您可以配置 LDAP 身份验证策略和 RSA 身份验证策略。用户登录时，他们首先使用其用户名和密码进行身份验证。然后，他们使用个人标识号 (PIN) 和来自 RSA 令牌的代码进行身份验证。

配置级联身份验证

April 6, 2020

身份验证允许您使用策略优先级创建多个身份验证服务器的级联。配置级联时，系统将遍历由级联策略定义的每个身份验证服务器，以验证用户的凭据。优先级身份验证策略按升序级联，优先级值可在 1 到 9999 之间。在全局或虚拟服务器级别绑定策略时，您可以定义这些优先级。

在身份验证期间，当用户登录时，首先检查虚拟服务器，然后检查全局身份验证策略。如果用户同时属于虚拟服务器和全局的身份验证策略，则首先应用来自虚拟服务器的策略，然后应用全局身份验证策略。如果希望用户接收全局绑定的身份验证策略，请更改策略的优先级。如果全局身份验证策略的优先级编号为 1，绑定到虚拟服务器的身份验证策略具有优先级编号 2，则全局身份验证策略优先。例如，您可以将三个身份验证策略绑定到虚拟服务器，并且可以设置每个策略的优先级。

如果用户无法针对主级级联中的策略进行身份验证，或者该用户成功地针对主级级联中的策略进行身份验证，但未能针对辅助级联中的策略进行身份验证，则身份验证过程将停止，并将用户重定向到错误页面。

注意：Citrix 建议在将多个策略绑定到虚拟服务器或全局绑定时，为所有身份验证策略定义唯一的优先级。

设置全局身份验证策略的优先级

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“策略”>“身份验证”。
2. 选择全局绑定的策略，然后在“操作”中，单击“全局绑定”。
3. 在“绑定/取消绑定身份验证全局策略”对话框中的“优先级”下，键入数字，然后单击“确定”。

更改绑定到虚拟服务器的身份验证策略的优先级

您还可以修改绑定到虚拟服务器的身份验证策略。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，选择虚拟服务器，然后单击“打开”。
3. 单击“身份验证”选项卡，然后单击“主”或“辅助”。
4. 在身份验证策略旁边的“优先级”下，键入数字，然后单击“确定”。

配置双重身份验证

April 6, 2020

Citrix Gateway 支持双重身份验证。通常，在对用户进行身份验证时，Citrix Gateway 会在通过任何一种配置的身份验证方法成功对用户进行身份验证后立即停止身份验证过程。在某些情况下，您可能需要向一台服务器对用户进行身份验证，但是从另一台服务器中提取组。例如，如果您的网络针对 RADIUS 服务器对用户进行身份验证，但您也使用 RSA SecurID 令牌身份验证并且用户组存储在该服务器上，则可能需要对用户进行身份验证，以便您可以提取这些组。

如果使用两种身份验证类型对用户进行身份验证，并且其中一种类型是客户端证书身份验证，则可以将证书身份验证策略配置为第二种身份验证方法。例如，您使用 LDAP 作为主身份验证类型，并使用客户端证书作为辅助身份验证。当用户使用其用户名和密码登录时，他们可以访问网络资源。

配置双重身份验证时，请选择身份验证类型是主类型还是辅助类型。

配置双重身份验证

1. 在配置实用程序中的 “配置” 选项卡上，展开 “Citrix Gateway”>“策略”>“身份验证”。
2. 在策略选项卡上，单击全局绑定。
3. 在 “绑定/取消绑定到全局的身份验证策略” 对话框中，单击 “主”。
4. 单击插入策略。
5. 在策略名称下，选择身份验证策略。
6. 单击辅助，重复步骤 4 和 5，然后单击确定。

选择单点登录的身份验证类型

April 6, 2020

如果在 Citrix Gateway 上配置了单点登录和双重身份验证，则可以选择用于单点登录的密码。例如，您已将 LDAP 配置为主身份验证类型，RADIUS 配置为辅助身份验证类型。当用户访问需要单点登录的资源时，默认情况下会发送用户名和主密码。您可以设置在会话配置文件中单点登录 Web 应用程序应使用的密码。

配置单点登录的身份验证

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格中，单击配置文件选项卡，然后执行以下操作之一：
    - 要创建新配置文件，请单击添加。
    - 要修改现有配置文件，请单击 “打开”。
3. 在 “客户端体验” 选项卡上，单击 “凭据索引” 旁边的 “覆盖全局”，选择 “主” 或 “辅助”。
4. 如果这是一个新的配置文件，请单击创建，然后单击关闭。

5. 如果要修改现有配置文件，请单击“确定”。

配置客户端证书和 **LDAP** 双重身份验证

April 6, 2020

您可以通过 LDAP 身份验证和授权使用安全客户端证书，例如将智能卡身份验证与 LDAP 结合使用。用户登录，然后从客户端证书中提取用户名。客户端证书是身份验证的主要形式，LDAP 是辅助形式。客户端证书身份验证必须优先于 LDAP 身份验证策略。设置策略的优先级时，为客户端证书身份验证策略分配的数值低于您分配给 LDAP 身份验证策略的数值。

要使用客户端证书，您必须具有在运行 Active Directory 的同一台计算机上运行的企业证书颁发机构 (CA)，例如 Windows Server 2008 中的证书服务。您可以使用 CA 创建客户端证书。

要使用具有 LDAP 身份验证和授权的客户端证书，必须是使用安全套接字层 (SSL) 的安全证书。要对 LDAP 使用安全客户端证书，请在用户设备上安装客户端证书，然后在 Citrix Gateway 上安装相应的根证书。

在配置客户端证书之前，请执行以下操作：

- 创建虚拟服务器。
- 为 LDAP 服务器创建 LDAP 身份验证策略。
- 将 LDAP 策略的表达式设置为 True 值。

使用 **LDAP** 配置客户端证书身份验证

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“策略”>“身份验证”。
2. 在导航窗格的身份验证下，单击 Cert。
3. 在详细信息窗格中，单击 Add（添加）。
4. 在“名称”中，键入策略的名称。
5. 在“身份验证类型”中，选择“证书”。
6. 在服务器旁边，单击新建。
7. 在“名称”中，键入服务器的名称，然后单击“创建”。
8. 在“创建身份验证服务器”对话框的“名称”中，键入服务器的名称。
9. 在“双因子”旁边，选择“开”。
10. 在用户名字段中，选择主题：CN，然后单击创建。
11. 在“创建身份验证策略”对话框的命名表达式旁边，选择“True”值，单击“添加表达式”，单击“创建”，然后单击“关闭”。

创建证书身份验证策略后，将策略绑定到虚拟服务器。绑定证书身份验证策略后，将 LDAP 身份验证策略绑定到虚拟服务器。

重要提示：在将 LDAP 身份验证策略绑定到虚拟服务器之前，必须将证书身份验证策略绑定到虚拟服务器。

在 **Citrix Gateway** 上安装根证书

创建证书身份验证策略后，您可以从 CA 下载并安装 Base64 格式的根证书，并将其保存在计算机上。然后，您可以将根证书上传到 Citrix Gateway。

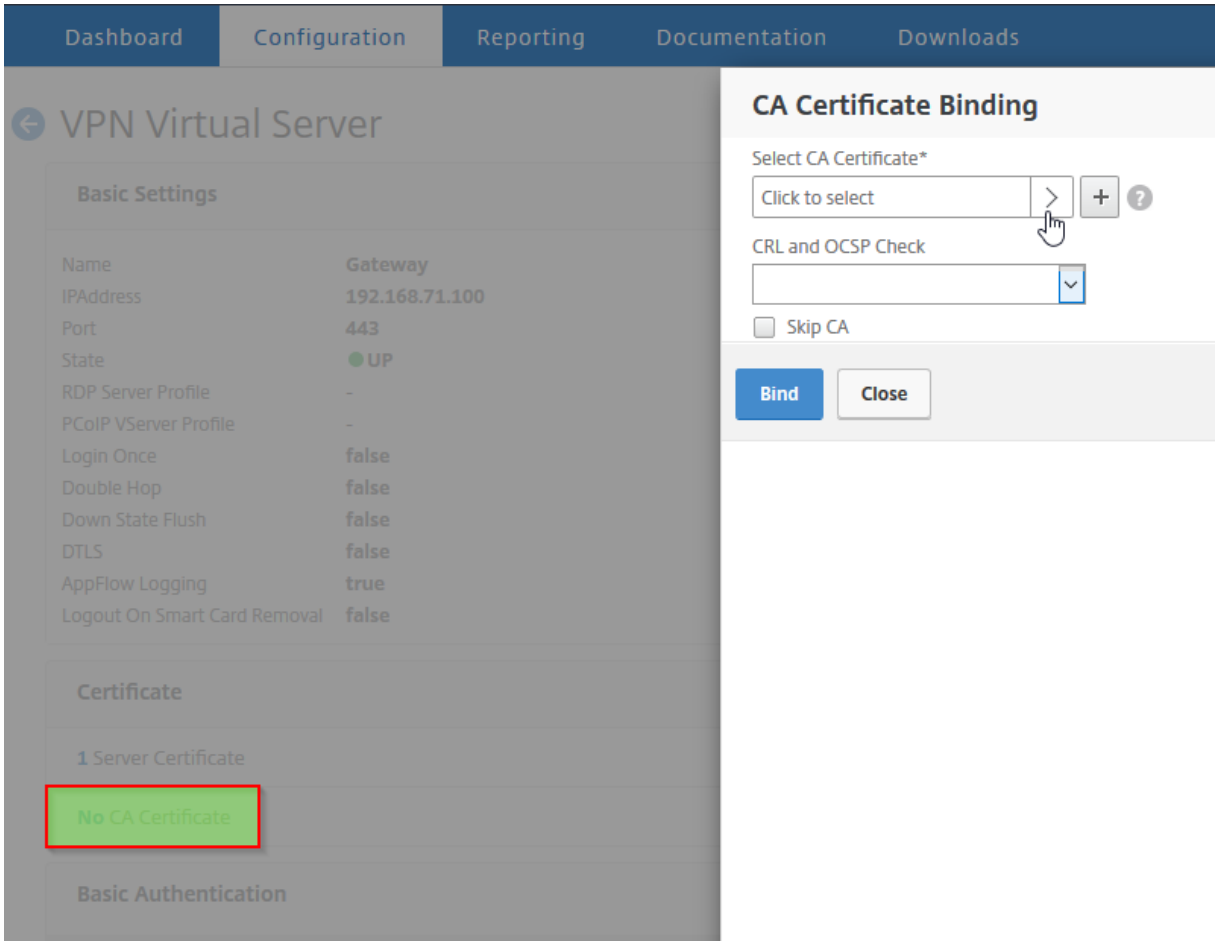
1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 SSL，然后单击“证书”。
2. 在详细信息窗格中，单击 Install（安装）。
3. 在证书-密钥对名称中，键入证书的名称。
4. 在“证书文件名”中，单击“浏览”，然后在下拉框中选择“设备”或“本地”。
5. 导航到根证书，单击打开，然后单击安装。

将根证书添加到虚拟服务器

在 Citrix Gateway 上安装根证书后，将证书添加到虚拟服务器的证书存储区。

重要提示：将根证书添加到虚拟服务器进行智能卡身份验证时，必须从“
选择 **CA** 证书”下拉框中选择证书，如下图所示。

图 1. 将根证书添加为 CA



1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。

2. 在详细信息窗格中，选择虚拟服务器，然后单击“打开”。
3. 在“证书”选项卡上的“可用”下，选择“添加”旁边的证书，在下拉框中单击“作为 CA”，然后单击“确定”。
4. 重复步骤 2。
5. 在证书选项卡上，单击 SSL 参数。
6. 在“其他”下，选择“客户端身份验证”。
7. 在“其他”下，“客户端证书”旁边，选择“可选”，然后单击“确定”两次。
8. 配置客户端证书后，通过使用 Citrix Gateway 插件登录 Citrix Gateway 来测试身份验证。如果您安装了多个证书，您会收到一条提示，要求您选择正确的证书。选择证书后，将显示登录屏幕，其中填充了从证书获取的信息的用户名。键入密码，然后单击登录。

如果在登录屏幕的“用户名”字段中看不到正确的用户名，请检查 LDAP 目录中的用户帐户和组。在 Citrix Gateway 上定义的组必须与 LDAP 目录中的组相同。在 Active Directory 中，在域根级别配置组。如果您创建的 Active Directory 组不在域根级别中，则可能会导致客户端证书的读取错误。

如果用户和组不在域根级别，Citrix Gateway 登录页面将显示在 Active Directory 中配置的用户名。例如，在 Active Directory 中，您有一个名为 Users 的文件夹，并且证书显示 CN=Users。在登录页中的“用户名”中，将显示“用户”一词。

如果不希望将组和用户帐户移动到根域级别，则在 Citrix Gateway 上配置证书身份验证服务器时，请将“用户名字段”和“组名字段”保留为空。

配置单点登录

April 6, 2020

您可以将 Citrix Gateway 配置为支持使用 Windows 进行单点登录、Web 应用程序（如 SharePoint）、文件共享和 Web Interface。单点登录也适用于用户可以通过访问界面中的文件传输实用程序或通知区域中的 Citrix Gateway 图标菜单访问的文件共享。

如果在用户登录时配置单点登录，则用户将自动重新登录，而无需再次输入凭据。

使用 **Windows** 配置单点登录

April 6, 2020

用户通过从桌面启动 Citrix Gateway 插件来打开连接。您可以通过启用单点登录来指定 Citrix Gateway 插件在用户登录到 Windows 时自动启动。配置单点登录时，用户的 Windows 登录凭据将传递到 Citrix Gateway 进行身份验证。为 Citrix Gateway 插件启用单点登录可促进用户设备上的操作，例如安装脚本和自动驱动器映射。

仅当用户设备登录到组织的域时，才启用单点登录。如果启用了单点登录并且用户从不在您的域上的设备进行连接，则系统会提示用户登录。

您可以在全局或使用附加到会话策略的会话配置文件配置与 Windows 配置单点登录。

使用 **Windows** 全局配置单点登录

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户端体验”选项卡上，单击“使用 Windows 单点登录”，然后单击“确定”。

使用会话策略配置 **Windows** 单点登录的步骤

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在“客户端体验”选项卡上，在“使用 Windows 单点登录”旁边，单击“覆盖全局”，单击“使用 Windows 单点登录”，然后单击“确定”。
7. 在“创建会话策略”对话框的命名表达式旁边，选择“常规”，选择“True”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置单点登录到 **Web** 应用程序

April 6, 2020

您可以将 Citrix Gateway 配置为向内部网络中使用基于 Web 的身份验证的服务器提供单点登录。通过单点登录，您可以将用户重定向到自定义主页，例如 SharePoint 站点或 Web Interface。您还可以通过 Citrix Gateway 插件从主页上配置的书签或用户在 Web 浏览器中键入的 Web 地址配置对资源的单点登录。

如果要将主页重定向到 SharePoint 站点或 Web Interface，请提供该站点的网址。当用户通过 Citrix Gateway 或外部身份验证服务器进行身份验证时，用户将被重定向到指定的主页。用户凭据透明地传递到 Web 服务器。如果 Web 服务器接受凭据，则会自动登录用户。如果 Web 服务器拒绝凭据，用户将收到一条身份验证提示，询问其用户名和密码。

您可以在全局范围内或使用会话策略配置 Web 应用程序的单点登录。

在全局范围内配置 **Web** 应用程序的单点登录

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。

3. 在“客户端体验”选项卡上，单击“单点登录到 Web 应用程序”，然后单击“确定”。

使用会话策略配置 **Web** 应用程序的单点登录

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，选择会话策略，然后单击“打开”。
3. 在“配置会话策略”对话框中，单击“请求配置文件”旁边的“修改”。
4. 在“客户端体验”选项卡上，单击“单点登录到 Web 应用程序”旁边，单击“全局覆盖”，单击“单点登录到 Web 应用程序”，然后单击“确定”。

为 **Web** 应用程序单点登录定义 **HTTP** 端口

仅对目标端口被视为 HTTP 端口的网络流量尝试单点登录。要允许对使用端口 80 以外的端口进行 HTTP 流量的应用程序进行单点登录，请在 Citrix Gateway 上添加一个或多个端口号。您可以启用多个端口。端口是全局配置的。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“网络配置”选项卡上，单击“高级设置”。
4. 在 HTTP 端口下，键入端口号，单击添加，然后单击确定两次。

   您可以对要添加的每个端口重复步骤 4。

注意：如果内部网络中的 Web 应用程序使用公有 IP 地址，则单点登录不起作用。要启用单点登录，必须将分割隧道作为全局策略设置的一部分启用，无论是否使用无客户端访问或 Citrix Gateway 插件用于用户设备连接。如果无法在全局级别上启用拆分隧道，请创建使用专用地址范围的虚拟服务器。

使用 **LDAP** 配置单点登录到 **Web** 应用程序

April 6, 2020

当您配置单点登录并使用带
username@domain.com 格式的用户主体名称 (UPN) 登录时，默认情况下，单点登录失败，用户必须进行两次身份验证。如果您需要使用此格式进行用户登录，请修改 LDAP 身份验证策略以接受此形式的用户名。

配置单点登录到 **Web** 应用程序的步骤

1. 在配置实用程序中的“配 置”选项卡上，展开 **Citrix Gateway >“策略”>“身份验证”**。
2. 在详细信息窗格的“策略”选项卡上，选择 LDAP 策略，然后单击“打开”。
3. 在“配置身份验证策略”对话框中，单击“服务器”旁边的“修改”。
4. 在“连接设置**”** 下，在“基本 DN（用户的位置）”中，键入 DC= 域名，DC=com。

5. 在 管理员绑定 **DN** 中，键入 LDAPaccount@domainname.com，其中域名 e.com 是您的域的名称。
6. 在 “管理员密码” 和 “确认管理员密码” 中，键入密码。
7. 在 “其他设置**”** 下的 “服务器登录名称属性” 中，键入 UserPrincipalName。
8. 在 “组属性**”** 中，键入 “memberOf”。
9. 在 子属性名称中，键入 CN。
10. 在 **SSO** 名称属性中，键入用户登录的格式，然后单 击确定两次。此值为 SamAccountName 或 UserPrincipalName。

配置单点登录到域

April 6, 2020

如果用户连接到运行 Citrix Virtual Apps 的服务器并使用 SmartAccess，则可以为连接到服务器场的用户配置单点登录。使用会话策略和配置文件配置对已发布应用程序的访问时，请使用服务器场的域名。

您还可以在网络中配置单点登录到文件共享。

配置域的单点登录

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格的 “策略” 选项卡上，选择会话策略，然后单击 “打开”。
3. 在 “配置会话策略” 对话框中，单击 “请求配置文件” 旁边的 “修改”。
4. 在 “配置会话配置文件” 对话框中的 “已发布的应用程序” 选项卡上的 “单点登录域” 中，单击 “覆盖全局”，键入域名，然后单击 “确定” 两次。

有关使用 Citrix Virtual Apps 配置 Citrix Gateway 的详细信息，请参阅将 Citrix Gateway 与 Citrix Virtual Apps and Desktops 集成。

为 **Microsoft Exchange 2010** 配置单点登录

April 6, 2020

以下部分介绍了 Citrix Gateway 上的 Microsoft Exchange 2010 的单点登录 (SSO) 的配置。在下列情况下，针对 Outlook Web Access (OWA) 2010 的 SSO 不起作用：

- 在 Microsoft Exchange 2010 上使用基于表单的身份验证。
- 通过身份验证、授权和审核流量管理策略进行负载平衡虚拟服务器。

> 注意
>
> 此配置仅适用于使用身份验证、授权和审核流量管理策略进行负载平衡的虚拟服务器。它不适用于 OWA 2010 中的 SSO 与无客户端 VPN。

以下步骤是在 Citrix Gateway 上为 Microsoft Exchange 2010 配置 SSO 之前必须考虑的先决条件。

- 对于 SSO 表单的操作 URL 在 OWA 2010 中是不同的。您必须修改流量管理策略。
- 您需要重写策略才能在 logon.aspx 请求中设置 PBack cookie。在正常情况下，您可以在客户端设置 PBack cookie，然后单击提交。
- 使用 SSO 时，会使用对 logon.aspx 的响应，并且 Citrix Gateway 生成表单请求。表单提交请求中没有附加 Cookie。
- OWA 服务器需要表单提交请求中的 PBack cookie。重写策略需要在表单提交请求中附加 PBack cookie。

使用 **CLI** 执行以下操作

1. 配置身份验证、授权和审核流量管理

```
add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL "/owa/auth.owa
"-userField username -passwdField password -ssoSuccessRule "http.
RES.SET_COOKIE.COOKIE(\"cadata\").VALUE(\"cadata\").LENGTH.GT(70"-
responsesize 15000 -submitMethod POST
```

2. 配置流量管理策略并绑定策略
   - `add tm trafficAction OWA_2010_Prof -appTimeout 1 -SSO ON -formSSO Action OWA_Form_SSO_SSOPro`
   - `add tm trafficPolicy owa2k10_pol "HTTP.REQ.URL.CONTAINS(\"owa/auth/logon.aspx\")"OWA_2010_Prof`
   - `bind tm global -policyName owa2k10_pol -priority 100`

使用 **CLI** 重写配置

在命令提示窗口中，键入：

- `add rewrite action set_pback_cookie insert_after "http.REQ.COOKIE.VALUE(\"OutlookSession\")""\";PBack=0\""-bypassSafetyCheck YES`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")"set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

备用重写配置

在极少数情况下，Microsoft Outlook 可能不会发出 OWA 会话饼干，并且可能也不会插入回忆饼干。执行上述命令以实现重写配置后，可能会出现此问题。

要克服这些情况并作为解决方法，您可以配置以下命令，而不是重写配置。

在命令提示窗口中，键入：

- `add rewrite action set_pback_cookie insert_http_header "Cookie"'"PBack=0"'`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")"set_pback_cookie`
- `set rewrite policy set_pback_cookie -action set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

配置一次性密码使用

April 6, 2020

您可以将 Citrix Gateway 配置为使用一次性密码，例如令牌个人身份识别号 (PIN) 或密码。用户输入密码或 PIN 后，身份验证服务器会立即使一次性密码无效，用户无法再次输入相同的 PIN 或密码。

包括使用一次性密码的商品包括：

- RSA SecurID
- Imprivata OneSign
- SafeWord
- 金雅拓 Protiva
- Nordic SMS PASSCODE

要使用这些产品中的每个产品，请将内部网络中的身份验证服务器配置为使用 RADIUS。有关详细信息，请参阅配置 RADIUS 身份验证。

如果将 Citrix Gateway 上的身份验证配置为使用 RADIUS 的一次性密码（例如，由 RSA SecurID 令牌提供），Citrix Gateway 会尝试使用缓存的密码对用户进行身份验证。如果您对 Citrix Gateway 进行更改，或者 Citrix Gateway 插件与 Citrix Gateway 之间的连接中断然后还原，则会发生此重新身份验证。

如果连接配置为使用 Citrix Workspace 应用程序，并且用户通过 RADIUS 或 LDAP 连接到 Web Interface，也会尝试重新进行身份验证。当用户启动应用程序并使用该应用程序，然后返回 Receiver 以启动另一个应用程序时，Citrix Gateway 会使用缓存信息对用户进行身份验证。

配置 **RSA SecurID** 身份验证

April 6, 2020

为 RSA SecureID 身份验证配置 RSA/ACE 服务器时，您需要完成以下步骤：

使用以下信息配置 RADIUS 客户端：

- 提供 Citrix Gateway 设备的名称。
- 提供描述（非强制性）。
- 提供系统 IP 地址。
- 提供 Citrix Gateway 和 RADIUS 服务器之间的共享机密。
- 将品牌/型号配置为标准 RADIUS。

在代理主机配置中，您需要以下信息：

- 提供 Citrix Gateway 的完全限定域名 (FQDN)（在绑定到虚拟服务器的证书上显示）。提供 FQDN 后，单击 Tab 键，网络地址窗口自行填充。

  输入 FQDN 后，网络地址将自动显示。如果没有，请输入系统 IP 地址。

- 使用通信服务器提供代理类型。
- 配置为导入允许通过 Citrix Gateway 进行身份验证的所有用户或一组用户。

如果尚未配置，请为 RADIUS 服务器创建代理主机条目，包括以下信息：

- 提供 RSA 服务器的 FQDN。

  输入 FQDN 后，网络地址将自动显示。如果没有，请提供 RSA 服务器的 IP 地址。

- 提供代理类型，即 RADIUS 服务器。

有关配置 RSA RADIUS 服务器的详细信息，请参阅制造商的文档。

要配置 RSA SecurID，请创建身份验证配置文件和策略，然后将策略全局绑定或绑定到虚拟服务器。要创建 RADIUS 策略以使用 RSA SecurID，请参阅配置 RADIUS 身份验证。

创建身份验证策略后，将其绑定到虚拟服务器或全局。有关详细信息，请参阅绑定身份验证策略。

使用 **RADIUS** 配置密码返回

April 6, 2020

您可以使用令牌从 RADIUS 服务器生成的一次性密码替换域密码。当用户登录到 Citrix Gateway 时，他们会输入令牌中的个人标识号 (PIN) 和密码。Citrix Gateway 验证其凭据后，RADIUS 服务器将用户的 Windows 密码返回到 Citrix Gateway。Citrix Gateway 接受来自服务器的响应，然后使用返回的密码进行单点登录，而不是使用用户在登录过程中键入的密码。此密码返回与 RADIUS 功能允许您配置单点登录，而不需要用户调用其 Windows 密码。

当用户使用密码返回登录时，他们可以访问内部网络中允许的所有网络资源，包括 Citrix Endpoint Management、StoreFront 和 Web Interface。

要使用返回的密码启用单点登录，可以使用“密码供应商标识符”和“密码属性类型”参数在 Citrix Gateway 上配置 RADIUS 身份验证策略。这两个参数将用户的 Windows 密码返回到 Citrix Gateway。

Citrix Gateway 支持 Imprivata OneSign。所需的最低版本的 Imprivata OneSign 是 4.0 与服务包 3。Imprivata OneSign 的默认密码供应商标识符为 398。Imprivata OneSign 的默认密码属性类型代码为 5。

您可以使用其他 RADIUS 服务器返回密码，例如 RSA、Cisco 或 Microsoft。必须将 RADIUS 服务器配置为在供应商特定的属性值对中返回用户单点登录密码。在 Citrix Gateway 身份验证策略中，必须为这些服务器添加密码供应商标识符和密码属性类型参数。

您可以在上找到供应商标识符的完整列表Internet 编号分配机构 (IANA) Web 站点。例如，RSA 安全性的供应商标识符为 2197，Microsoft 为 311，Cisco Systems 为 9。供应商支持的供应商特定属性必须与供应商确认。例如，Microsoft 在发布了供应商特定属性的列表Microsoft 供应商特定的 RADIUS 属性。

您可以选择任何供应商特定的属性，以便在供应商的 RADIUS 服务器上存储用户的单点登录密码。如果使用用用户密码存储在 RADIUS 服务器上的供应商标识符和属性配置 Citrix Gateway，Citrix Gateway 将请求发送到 RADIUS 服务器的访问请求数据包中的属性值。如果 RADIUS 服务器在访问-接受数据包中使用相应的属性-值对进行响应，则无论使用哪个 RADIUS 服务器，密码都会返回。

要使用返回的密码配置单点登录，请执行以下操作：

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“策略”>“身份验证”。
2. 在导航窗格中，单击 RADIUS。
3. 在详细信息窗格中，单击 Add（添加）。
4. 在“创建身份验证策略”对话框的“名称”中，键入策略的名称。
5. 在服务器旁边，单击新建。
6. 在“名称”中，键入服务器的名称。
7. 配置 RADIUS 服务器的设置。
8. 在“密码供应商标识符”中，键入 RADIUS 服务器返回的供应商标识符。此标识符的最小值必须为 1。
9. 在“密码属性类型”中，键入由 RADIUS 服务器在供应商特定的 AVP 代码中返回的属性类型。该值的范围可以介于 1 到 255 之间。
10. 在“创建身份验证策略”对话框的命名表达式旁边，选择表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置 **SafeWord** 身份验证

April 6, 2020

SafeWord 产品线有助于通过使用基于令牌的密码提供安全身份验证。用户输入密码后，SafeWord 将立即失效，不能再次使用。

如果 Access Gateway 正在替换 Secure Gateway 和 Web Interface 部署中的 Secure Gateway，则可以选择不在 Access Gateway 上配置身份验证，并继续允许 Web Interface 为传入 HTTP 流量提供 SafeWord 身份验证。

Access Gateway 支持以下产品的 SafeWord 身份验证：

- SafeWord 2008
- SafeWord PremierAccess
- SafeWord for Citrix
- SafeWord RemoteAccess

您可以通过以下方式将 Access Gateway 配置为使用 SafeWord 产品进行身份验证：

- 将身份验证配置为使用作为 SafeWord PremierAccess 的一部分安装的 PremierAccess RADIUS 服务器，并允许其处理身份验证。
- 配置身份验证以使用 SafeWord IAS 代理，该代理是 SafeWord RemoteAccess、SafeWord for Citrix 和 SafeWord PremierAccess 4.0 的组件。
- 安装 SafeWord Web Interface 代理以使用 Citrix Web Interface。身份验证不必在 Access Gateway 上配置，并且可以由 Citrix Web Interface 处理。此配置不使用 PremierAccess RADIUS 服务器或 SafeWord IAS 代理。

配置 SafeWord RADIUS 服务器时，您需要以下信息：

- Access Gateway 的 IP 地址。在 RADIUS 服务器上配置客户端设置时，请使用 Access Gateway IP 地址。
- 一个共享的秘密
- SafeWord 服务器的 IP 地址和端口。

配置金雅拓 **Protiva** 身份验证

April 6, 2020

Protiva 是一个强大的身份验证平台，是为了利用金雅拓智能卡身份验证的优势而开发的。使用 Protiva，用户使用 Protiva 设备生成的用户名、密码和一次性密码登录。与 RSA SecurID 类似，身份验证请求将发送到 Protiva 身份验证服务器，并验证或拒绝密码。

要将金雅拓 Protiva 配置为与 Citrix Gateway 一起使用，请使用以下准则：

- 安装 Protiva 服务器。
- 在 Microsoft IAS RADIUS 服务器上安装 Protiva Internet 身份验证服务器 (IAS) 代理插件。请务必记下 IAS 服务器的 IP 地址和端口号。

网关身份验证的 **nFactor**

March 22, 2022

简介

nFactor 身份验证启用了一整套有关身份验证的可能性。使用 nFactor 的管理员在为虚拟服务器配置身份验证因子时享有身份验证、授权和审核的灵活性。

两个策略银行或两个因素不再限制管理员。政策银行的数目可以扩大，以适应不同的需要。根据以前的因素，nFactor 确定身份验证方法。使用 nFactor 可以实现动态登录表单和失败操作。

> 注意： Citrix ADC Standard Edition 不支持 nFactor。Citrix ADC 高级版和 Citrix ADC 高级版支持此功能。

使用案例

nFactor 身份验证启用基于用户配置文件的动态身份验证流。有时，这些流程可以是简单的，对用户来说是直观的。在其他情况下，它们可以与保护活动目录或其他身份验证服务器相结合。以下是特定于网关的一些要求：

1. 动态用户名和密码选择。传统上，Citrix 客户端（包括浏览器和 Receiver）使用 Active Directory (AD) 密码作为第一个密码字段。第二个密码保留给一次性密码 (OTP)。但是，为了保护 AD 服务器的安全，需要先验证 OTP。nFactor 可以在不需要客户端修改的情况下完成此操作。
2. 多租户身份验证终点。某些组织为证书用户和非证书用户使用不同的网关服务器。用户使用自己的设备登录时，用户的访问级别因 Citrix ADC 而异，具体取决于所使用的设备。网关可以满足不同的身份验证需求。
3. 基于组成员身份验证。某些组织从 AD 服务器获取用户属性以确定身份验证要求。对于个人用户，身份验证要求可能会有所不同。
4. 身份验证的辅助因素。有时，会使用不同的身份验证策略对对不同的用户集进行身份验证。提供配对策略可提高有效的身份验证。可以从一个流程中制定相关策略。通过这种方式，独立的一套政策成为其本身的流动，提高效率和降低复杂性。

身份验证响应处理

Citrix Gateway 回调寄存器处理身份验证响应。AAAD（身份验证守护进程）响应和成功/失败/错误/对话代码被馈送到回调句柄。成功/失败/错误/对话代码指示网关采取适当的操作。

客户支持

下表详细介绍了配置详细信息。

客户端	nFactor 支持	身份验证策略绑定点	EPA
浏览器	是	身份验证	是
Citrix Workspace 应用程序	否	VPN	N
网关插件	否	VPN	是

命令行配置

网关虚拟服务器需要一个名为属性的身份验证虚拟服务器。这是此模型所需的唯一配置。

```
add authnProfile <name-of-profile> -authnVsName <name-of-auth-vserver>
<!--NeedCopy-->
```

authnVsName 是身份验证虚拟服务器的名称。此虚拟服务器应配置高级身份验证策略，并用于 nFactor 身份验证。

```
add vpn vserver <name> <serviceType> <IP> <PORT> -authnProfile <name-of
    -profile>
set vpn vserver <name> -authnProfile <name-of-profile>
<!--NeedCopy-->
```

其中 authnProfile 是之前创建的身份验证配置文件。

互操作挑战

除 rfWeb 客户端外，大多数旧网关客户端都是根据网关发送的响应建模的。例如，许多客户端需要对 /vpn/index.html 进行 302 响应。此外，这些客户端依赖于各种网关 cookie，如 “pwcount”，“NSC_CERT”，等等。

端点分析 **(EPA)**

由于身份验证、授权和审核子系统不支持 nFactor 的 EPA；然而，网关虚拟服务器执行 EPA。EPA 之后，登录凭据将使用前面提到的 API 发送到身份验证虚拟服务器。身份验证完成后，Gateway 将继续进行身份验证后过程，并建立用户会话。

配置错误注意事项

网关客户端仅发送一次用户凭据。网关通过登录请求从客户端获取一个或两个凭据。在旧模式下，最多有两个因素。获取的密码用于这些因素。但是，对于 nFactor，可以配置的因子数实际上是无限的。从网关客户端获取的密码将被重复使用（根据配置）用于配置的因子。必须注意不要多次重复使用一次性密码 (OTP)。同样，管理员必须确保在某个因素中重复使用的密码确实适用于该因素。

定义 **Citrix** 客户端

提供配置选项可帮助 Citrix ADC 确定浏览器客户端与厚客户端（如 Receiver）。

提供了一个模式集，即 ns_vpn_client_ 用户代理，供管理员为所有 Citrix 客户端配置模式。

同样，将 “Citrix Receiver” 字符串绑定到上述修补集以忽略用户代理中具有 “Citrix Receiver” 的所有 Citrix 客户端。

限制网关的 **nFactor**

如果存在以下条件，则不会发生网关身份验证的 nFactor。

1. Citrix Gateway 未设置 authnProfile。
2. 高级身份验证策略不绑定到身份验证虚拟服务器，并且在 authnProfile 中提到了相同的身份验证虚拟服务器。
3. HTTP 请求中的用户代理字符串与在修补集 ns_vpn_ 客户代理中配置的用户代理匹配。

如果不满足这些条件，则使用绑定到网关的经典身份验证策略。

如果 User-Agent 或其部分绑定到上述修补集，则来自这些用户代理的请求不会参与 nFactor 流程。例如，下面的命令限制了所有浏览器的配置（假设所有浏览器在用户代理字符串中都包含 “Mozilla”）：

bind patset ns_vpn_client_useragents Mozilla

LoginSchema

LoginSchema 是登录表单的逻辑表示形式。XML 语言定义它。loginSchema 的语法符合 Citrix 的通用表单协议规范。

LoginSchema 定义产品的 “视图”。管理员可以提供表单的自定义描述、辅助文本等。这包括表单本身的标签。客户可以提供成功/失败消息，描述在给定时间点显示的表单。

所需的 **LoginSchema** 和 **nFactor** 知识

预构建的 loginSchema 文件可以在以下 Citrix ADC 位置 /nsconfig/loginschema/LoginSchema/。这些预先构建的 LoginSchema 文件可以满足常见的使用案例，如果需要，可以根据轻微的变化进行修改。

此外，大多数具有少量自定义项的单因素使用案例不需要 loginSchema 配置。

建议管理员检查文档以获取使 Citrix ADC 能够发现这些因素的其他配置选项。用户提交凭据后，管理员可以配置多个因子，以灵活地选择和处理身份验证因子。

在不使用 **LoginSchema** 的情况下配置双重身份验证

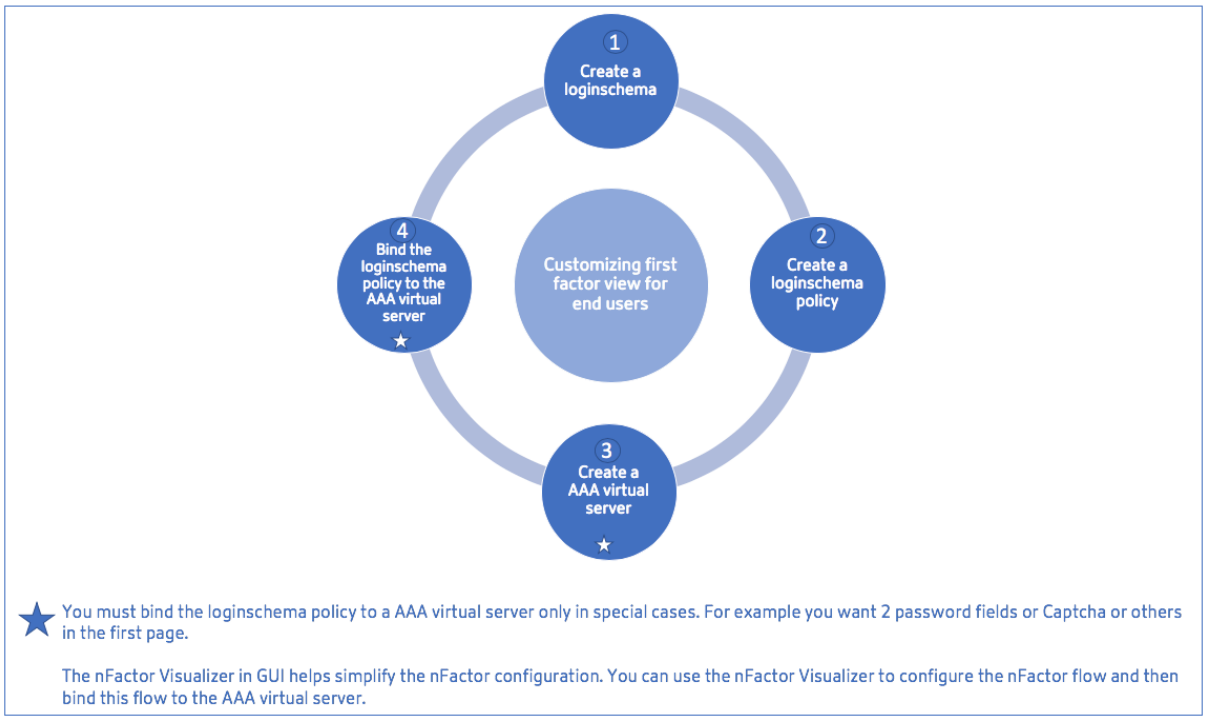
Citrix ADC 基于配置自动确定双因素要求。用户提供这些凭据后，管理员可以在虚拟服务器上配置第一组策略。针对每个策略，可以有一个 “下一个因子” 配置为 “直通”。“直通” 意味着 Citrix ADC 应使用现有凭据集来处理登录，而无需转到用户。通过使用 “直通” 因素，管理员可以以编程方式驱动身份验证流程。建议管理员阅读 nFactor 规范或部署指南以了解更多详细信息。请参阅
多因素 (nFactor) 身份验证。

用户名密码表达式

为了处理登录凭据，管理员必须配置 loginSchema。只有少量 loginSchema 自定义项的单因素或双因素使用案例不需要指定的 XML 定义。LoginSchema 具有其他属性，如使用 userExpression 和 passwdExpression，可用于更改用户提供的用户名/密码。这些是高级策略表达式，也可用于覆盖用户输入。

nFactor 配置中的高级步骤

下图说明 nFactor 配置所涉及的高级步骤。



GUI 配置

本节介绍了以下主题：

- 创建虚拟服务器
- 创建身份验证虚拟服务器
- 创建身份验证 CERT 配置文件
- 创建身份验证策略
- 添加 LDAP 身份验证服务器
- 添加 LDAP 身份验证策略
- 添加 Radius 身份验证服务器

- 添加 Radius 身份验证策略
- 创建身份验证登录架构
- 创建策略标签

创建虚拟服务器

1. 导航到 **Citrix Gateway->** 虚拟服务器。
2. 单击“添加”按钮以创建负载平衡虚拟服务器。
3. 输入以下信息。

参数名称	参数描述
输入虚拟服务器的名称。	Citrix Gateway 虚拟服务器的名称。必须以 ASCII 字母或下划线 (_) 开头，并且必须仅包含 ASCII 字母数字、下划线、井号 (#)、句点 (.)、空格、冒号 (:)、at (@)、equals (=) 和连字符 (-)。可以在创建虚拟服务器后更改。以下要求仅适用于 Citrix ADC CLI：如果名称包含一个或多个空格，请将名称括在双引号或单引号中（例如，“我的服务器”或“我的服务器”）。
输入虚拟服务器的 IP 地址类型	从下拉菜单中选择 IP 地址或不可寻址选项。
输入虚拟服务器的 IP 地址。	互联网协议地址（IP 地址）是一个数字标签，分配给参与使用互联网协议进行通信的计算机网络的每个设备。
输入虚拟服务器的端口号。	输入端口号。
输入身份验证配置文件。	虚拟服务器上的身份验证配置文件实体。此实体可用于将身份验证卸载到身份验证、授权和审核虚拟服务器进行多因素 (nFactor) 身份验证
输入 RDP 服务器配置文件。	与虚拟服务器关联的 RDP 服务器配置文件的名称。
输入最大用户数。	此虚拟服务器上允许的最大并发用户会话数。允许登录此虚拟服务器的实际用户数取决于用户许可证的总数。
输入最大登录尝试次数。	最大登录尝试次数。
输入失败的登录超时。	如果用户超过允许的最大尝试，帐户将被锁定的分钟数。
输入 Windows EPA 插件升级。	选项为 Win 设置插件升级行为。
输入 Linux EPA 插件升级。	选项为 Linux 设置插件升级行为。
进入 MAC EPA 插件升级	选项为 Mac 设置插件升级行为。
登录一次	此选项为此虚拟服务器启用/禁用无缝 SSO。

参数名称	参数描述
仅限 ICA	如果设置为开，则意味着基本模式，用户可以使用 Citrix Workspace 应用程序或浏览器登录，并访问由 Wihome 参数指出的 Citrix Virtual Apps and Desktops 环境中配置的已发布应用程序。不允许用户使用 Citrix Gateway 插件进行连接，并且无法配置终点扫描。在此模式下，可以登录和访问应用程序的用户数不受许可证的限制。- 如果设置为“关”，则意味着用户可以使用 Citrix Workspace 应用程序或浏览器或 Citrix Gateway 插件登录的 SmartAccess 模式。管理员可以配置要在客户端系统上运行的端点扫描，然后使用结果控制对已发布应用程序的访问。在此模式下，客户端可以在其他客户端模式（VPN 和 CVPN）连接到网关。在此模式下，可以登录和访问资源的用户数受 CCU 许可证的限制。
启用身份验证	要求连接到 Citrix Gateway 的用户进行身份验证。
双跃点	在双跃点配置中使用 Citrix Gateway 设备。双跃点部署通过使用三个防火墙将 DMZ 分为两个阶段，为内部网络提供了额外的安全层。此类部署可以在 DMZ 中有一个设备，在安全网络中有一个设备。
向下状态刷新	当虚拟服务器标记为“向下”时关闭现有连接，这意味着服务器可能已超时。断开现有连接可释放资源，并在某些情况下加快重载负载平衡设置的恢复速度。在服务器上启用此设置，当连接被标记为“向下”时可以安全关闭。不要在必须完成其事务的服务器上启用向下状态刷新。
DTLS	此选项启动/停止虚拟服务器上的转弯服务
AppFlow 日志记录	记录包含标准 NetFlow 或 IPFIX 信息的 AppFlow 记录，例如流的开始和结束时间戳、数据包计数和字节计数。还会记录包含应用程序级别信息的记录，例如 HTTP Web 地址、HTTP 请求方法和响应状态代码、服务器响应时间和延迟。
ICA 代理会话迁移	此选项确定用户从其他设备登录时是否传输现有 ICA 代理会话。
状态	虚拟服务器的当前状态，如 UP、关闭、忙等。
启用设备证书	指示作为 EPA 一部分的设备证书检查是打开还是关闭。

4. 选择页面的“无服务器证书”部分。
5. 单击 > 以选择服务器证书。
6. 选择 SSL 证书，然后单击选 择按钮。
7. 单击 **Bind**（绑定）。
8. 如果您看到关于“无可用密码”的警告，请单击“确定”
9. 点击继 续按钮。
10. 在身份验证部分，单击右上角的 **+** 图标。

创建身份验证虚拟服务器

1. 导航到 安全**-> Citrix ADC AAA-**应用程序流量**->** 虚拟服务器。
2. 单击添加按钮。
3. 完成以下基本设置以创建身份验证虚拟服务器。

   注意：必填字段由设置名称右侧的 * 表示。

   a) 输入新的身份验证虚拟服务器的 名称。

   b) 输入 **IP** 地址类型。IP 地址类型可以配置为不可寻址。

   c) 输入 **IP** 地址。IP 地址可以为零。

   d) 输入身份验证虚拟服务器的 协议类型。

   e) 输入虚拟服务器接受连接的 **TCP** 端口。

   f) 输入身份验证虚拟服务器设置的身份验证 cookie 的 域。
4. 单击确定。
5. 单击“无服务器证书”。
6. 从列表中选择所需的服务器证书。
7. 选择所需的 SSL 证书，然后单击选 择按钮。

   注意：身份验证虚拟服务器不需要绑定到它的证书。
8. 配置 服务器证书绑定。
   - 选中 **SNI** 服务器证书框以绑定用于 SNI 处理的证书密钥。
   - 点击 绑定按钮。

创建身份验证 **CERT** 配置文件

1. 导航到 安全**-> Citrix ADC AAA-**应用程序流量**->** 策略**->** 身份验证**->** 基本策略**-> CERT**。
2. 选择配置文件选项卡，然后选择 添加。
3. 完成以下字段以创建身份验证 CERT 配置文件。必填字段由设置名称右侧的 * 表示。
   - **Name** -客户端证书身份验证服务器配置文件的名称（操作）。
   - 两个因素 — 在这种情况下，双重身份验证选项是 NOOP。
   - 用户名字段 — 输入从中提取用户名的客户端证书字段。必须设置为“主题”或“发行人”（包括两组双引号）。
   - 组名称字段 -输入从中提取组的客户端证书字段。必须设置为“主题”或“发行人”（包括两组双引号）。
   - 默认身份验证组 -除提取的组外，当身份验证成功时选择的默认组。
4. 单击创建。

创建身份验证策略

1. 导航到 安全**-> Citrix ADC AAA-**应用程序流量**->** 策略**->** 身份验证**->** 高级策略**->** 策略。
2. 选择 添加按钮
3. 请完成以下信息以创建身份验证策略。必填字段由设置名称右侧的 * 表示。

   a) 名称 — 输入高级身份验证策略的名称。必须以字母、数字或下划线字符 (_) 开头，并且必须仅包含字母、数字和连字符 (-)、句点 (.) (#)、空格 ()、位于 (@)、equals (=)、冒号 (:) 和下划线字符。创建身份验证策略后无法更改。

   以下要求仅适用于 Citrix ADC CLI：如果名称包含一个或多个空格，请使用双引号或单引号将名称括起来（例如，“我的身份验证策略”或“我的身份验证策略”）。

   b) 操作类型 -输入身份验证操作的类型。

   c) 操作-输入策略匹配时要执行的身份验证操作的名称。

   d) 日志操作 - 输入请求与此策略匹配时要使用的消息日志操作的名称。

   e) 表达式 -输入策略用于确定是否尝试使用身份验证服务器对用户进行身份验证的 Citrix ADC 命名规则的名称或默认语法表达式。

   f) 注释 — 输入任何注释以保留有关此政策的信息。
4. 单击创建

添加 **LDAP** 身份验证服务器

1. 导航到 安全**-> Citrix ADC AAA-**应用程序流量**->** 策略**->** 身份验证**->** 基本策略**-> LDAP**。

2. 通过选择“服务器”选项卡并选择“添加”按钮来 添加 LDAP 服务器。

添加 **LDAP** 身份验证策略

1. 转到安全-> Citrix ADC AAA-应用程序流量-> 策略-> 身份验证-> 高级策略-> 策略.
2. 单击 添加以添加身份验证策略。
3. 请完成以下信息以创建身份验证策略。必填字段由设置名称右侧的 * 表示。

   a) 名称 -高级身份验证策略的名称。
   必须以字母、数字或下划线字符 (_) 开头，并且必须仅包含字母、数字和连字符 (-)、句点 (.) (#)、空格 ()、位于 (@)、equals (=)、冒号 (:) 和下划线字符。创建身份验证策略后无法更改。

   以下要求仅适用于 Citrix ADC CLI：如果名称包含一个或多个空格，请使用双引号或单引号将名称括起来（例如，“我的身份验证策略”或“我的身份验证策略”）。

   b) 操作类型 -身份验证操作的类型。

   c) 操作-如果策略匹配，要执行的身份验证操作的名称。

   d) 日志操作 - 请求与此策略匹配时要使用的消息日志操作的名称。

   e) 表达式 -策略用于确定是否尝试使用身份验证服务器对用户进行身份验证的 Citrix ADC 命名规则或默认语法表达式的名称。

   f) 评论 -保留有关此政策的信息的任何评论。
4. 单击创建

添加 **RADIUS** 身份验证服务器

1. 导航到 安全**-> Citrix ADC AAA-**应用程序流量**->** 策略**->** 身份验证**->** 基本策略**-> RADIUS**.
2. 要添加服务器，请选择“服务 器”选项卡并选择“添加”按钮。
3. 输入以下内容以创建身份验证 RADIUS 服务器。必填字段由设置名称右侧的 * 表示。

   a) 输入 RADIUS 操作的 名称。

   b) 输入分配给 RADIUS 服务器的 服务器名称或 服务器 **IP** 地址。

   c) 输入 RADIUS 服务器侦听连接的 端口号。

   d) 在几秒钟内输入 超时值。这是 Citrix ADC 设备等待 RADIUS 服务器响应的值。

   e) 输入 RADIUS 服务器和 Citrix ADC 设备之间共享的私有 密钥。使 Citrix ADC 设备能够与 RADIUS 服务器通信，需要使用私有密钥。

   f) 确认密钥。
4. 单击创建

添加 **RADIUS** 身份验证策略

1. 导航到 安全**-> Citrix ADC AAA-**应用程序流量**->** 策略**->** 身份验证**->** 高级策略**->** 策略。
2. 单击“添加”以创建身份验证策略。
3. 请完成以下信息以创建身份验证策略。必填字段由设置名称右侧的 * 表示。

   a) 名称 -高级身份验证策略的名称。
   必须以字母、数字或下划线字符 (_) 开头，并且必须仅包含字母、数字和连字符 (-)、句点 (.) (#)、空格 ()、位于 (@)、equals (=)、冒号 (:) 和下划线字符。创建身份验证策略后无法更改。

   以下要求仅适用于 Citrix ADC CLI：如果名称包含一个或多个空格，请使用双引号或单引号将名称括起来（例如，“我的身份验证策略”或“我的身份验证策略”）。

   b) 操作类型 -身份验证操作的类型。

   c) 操作-如果策略匹配，要执行的身份验证操作的名称。

   d) 日志操作 - 请求与此策略匹配时要使用的消息日志操作的名称。

   e) 表达式 -策略用于确定是否尝试使用身份验证服务器对用户进行身份验证的 Citrix ADC 命名规则或默认语法表达式的名称。

   f) 评论 -保留有关此政策的信息的任何评论。
4. 单击 **OK**（确定）
5. 验证您的身份验证策略已列出。

创建身份验证登录架构

1. 导航到 安全**-> Citrix ADC AAA-**应用程序流量**->** 登录架构。
2. 选择配置文件选项卡，然后单击 添加按钮。
3. 请完成以下字段以创建身份验证登录架构：

   a) 输入 名称 — 这是新登录架构的名称。

   b）输入 身份验证架构 -这是读取要为登录页面 UI 发送的身份验证架构的文件的名称。此文件应包含根据 Citrix 表单身份验证协议的元素的 xml 定义，以便能够呈现登录表单。如果管理员不希望提示用户输入其他凭据，但继续使用之前获得的凭据，则可以提供“noschema”作为参数。请注意，这仅适用于与用户定义因子一起使用的 loginSchema，而不适用于虚拟服务器因子

   c）输入 用户表达式 -这是登录期间用户名提取的表达式

   d）输入 密码表达式 -这是登录时密码提取的表达式

   e）输入 用户凭据索引 -这是用户输入的用户名应存储在会话中的索引。

   f）输入 密码凭据索引 -这是用户输入的密码应存储在会话中的索引。

   g）输入 身份验证强度 -这是当前身份验证的权重。

4. 单击创建

    a) 验证您的登录架构配置文件已列出。

创建策略标签

策略标签指定特定因子的身份验证策略。每个策略标签对应于一个因素。策略标签指定必须向用户显示的登录表单。策略标签必须绑定为身份验证策略或另一个身份验证策略标签的下一个因素。通常，策略标签包括针对特定身份验证机制的身份验证策略。但是，您也可以具有针对不同身份验证机制的身份验证策略的策略标签。

1. 导航到 安全**-> Citrix ADC AAA-**应用程序流量**->** 策略**->** 身份验证**->** 高级策略**->** 策略标签。
2. 单击添加按钮。
3. 请完成以下字段以创建身份验证策略标签：

    a) 输入新身份验证策略标签的 名称。

    b) 输入与身份验证策略标签关联的 登录架构。

    c) 点击 继续。
4. 从下拉菜单中选择一个策略。
5. 选择所需的 身份验证策略，然后单击 选择按钮。
6. 填写以下字段：

    a) 输入策略绑定的 优先级。

    b) 输入 **Gto** 表达式 **—** 表达式指定下一个策略的优先级，如果当前策略规则的计算结果为 TRUE，则该策略将被评估。
7. 选择所需的身份验证策略，然后单击 选择按钮。
8. 点击 绑定按钮。
9. 单击完成。
10. 查看身份验证策略标签。

nFactor 身份验证的 **reCaptcha** 配置

从 Citrix ADC 发布 12.1 版本 50.x 开始，Citrix Gateway 支持简化 Captcha 配置的新的第一类操作 “captchaAction”。由于验证码是第一类动作，它可以是它自己的一个因素。您可以在 nFactor 流中的任何位置注入验证码。

以前，您必须编写自定义 WebAuth 策略并对 RfWeb UI 进行更改。引入 captchaACtion 后，您不必修改 JavaScript。

> 重要
>
> 如果验证码与架构中的用户名或密码字段一起使用，则提交按钮将被禁用，直到满足验证码。

验证码配置

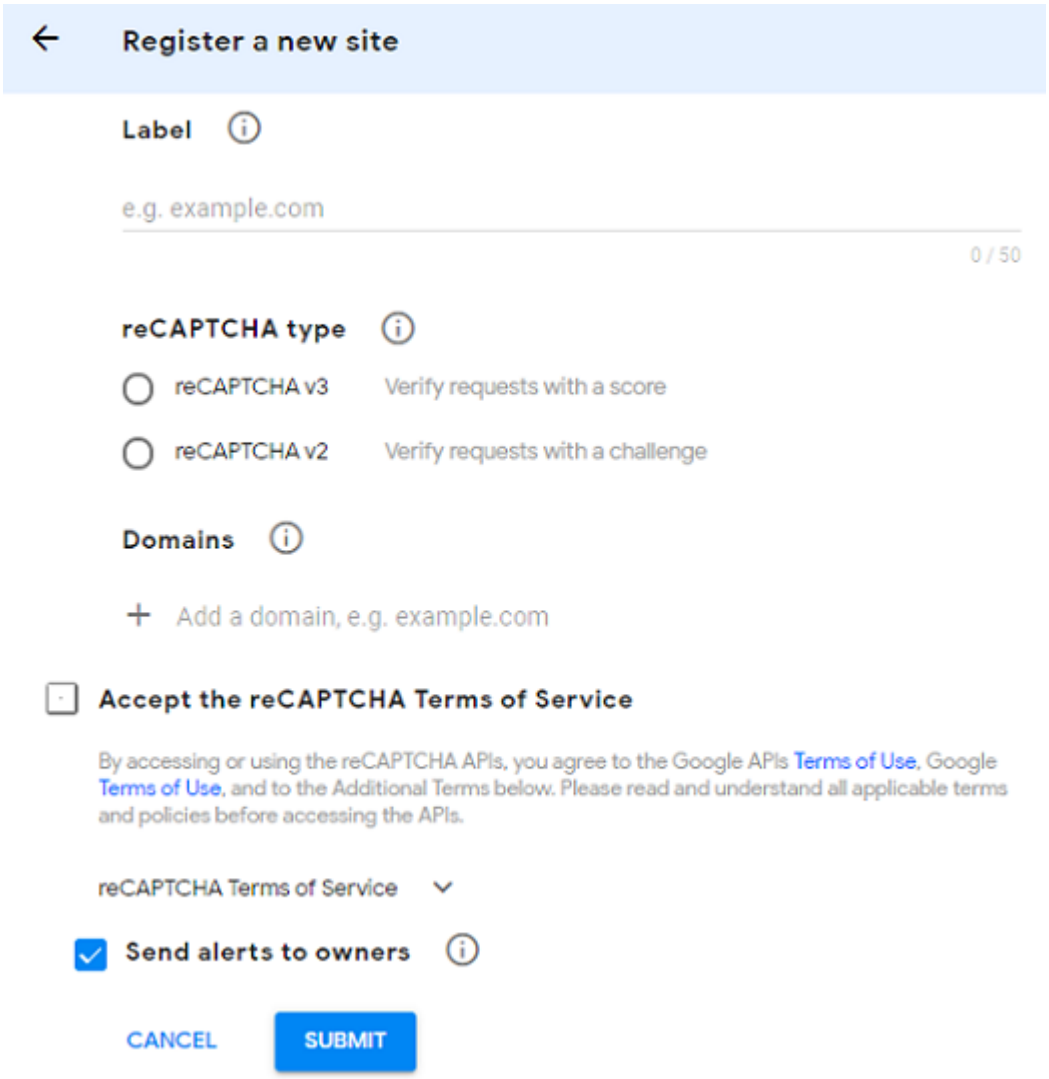
验证码配置涉及两个部分。

1. 配置在谷歌注册验证码。
2. Citrix ADC 设备上的配置以使用验证码作为登录流的一部分。

在谷歌上的验证码配置

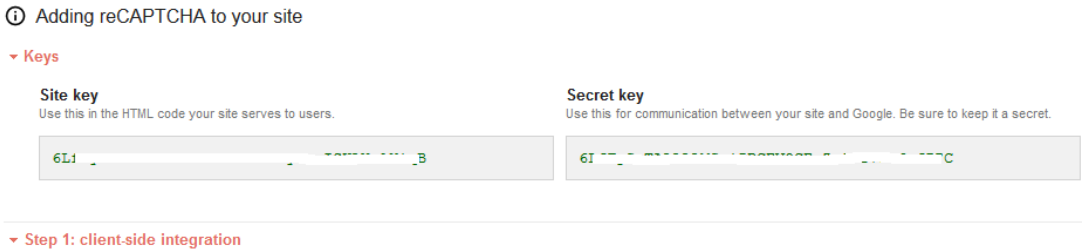
在注册验证码的域名`https://www.google.com/recaptcha/admin##list`。

1. 导航到此页面时，将显示以下屏幕。



> 注意
>
> 仅使用 reCAPTCHA v2。不可见 reCAPTCHA 仍是技术预览版。

2. 域名注册后，显示 “SiteKey” 和 “SecretKey”。



> 注意
>
> 出于安全原因，“SiteKey” 和 “SecretKey” 显示为灰色。“SecretKey” 必须安全保存。

Citrix ADC 设备上的验证码配置

Citrix ADC 设备上的验证码配置可分为三个部分：

- 显示验证码屏幕
- 将验证码响应发布到谷歌服务器
- LDAP 配置是用户登录的第二个因素（可选）

显示验证码屏幕

登录表单自定义是通过 SingleAuthCaptcha.xml loginschema 完成的。此自定义在身份验证虚拟服务器上指定，并发送到 UI 以呈现登录表单。内置登录架构 SingleAuthCaptcha 位于 Citrix ADC 设备上的 /nsconfig/loginSchema/LoginSchema 目录中。

> 重要
>
> - 根据您的用例和不同的架构，您可以修改现有架构。例如，如果您只需要验证码因素（无用户名或密码）或使用验证码进行双重身份验证。
> - 如果执行了任何自定义修改或重命名了文件，Citrix 建议将所有登录模式从 /nsconfig/loginschema/LoginSchema 复制到父目录 /nsconfig/loginschema。

使用 **CLI** 配置验证码的显示

- `add authentication loginSchema singleauthcaptcha -authenticationSchema /nsconfig/loginschema/SingleAuthCaptcha.xml`
- `add authentication loginSchemaPolicy singleauthcaptcha -rule true -action singleauthcaptcha`

- add authentication vserver auth SSL <IP> <Port>
- add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-key-file>
- bind ssl vserver auth -certkey vserver-cert
- bind authentication vserver auth -policy singleauthcaptcha -priority 5 -gotoPriorityExpression END

将验证码响应发布到谷歌服务器

在您配置了必须向用户显示的验证码后，管理员发布将配置添加到 Google 服务器以验证来自浏览器的验证码响应。

验证来自浏览器的验证码响应

- add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-from-google> -secretkey <secretkey-from-google>
- add authentication policy myrecaptcha -rule **true** -action myrecaptcha
- bind authentication vserver auth -policy myrecaptcha -priority 1

如果需要 AD 身份验证，则需要使用以下命令进行配置。否则，您可以忽略此步骤。

- add authentication ldapAction ldap-**new** -serverIP x.x.x.x -serverPort 636 -ldapBase "cn=users,dc=aaatm,dc=com"-ldapBindDn adminuser@aaatm.com -ldapBindDnPassword <password> -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberof -subAttributeName CN -secType SSL -passwdChange ENABLED -defaultAuthenticationGroup ldapGroup
- add authenticationpolicy ldap-**new** -rule **true** -action ldap-**new**

LDAP 配置是用户登录的第二个因素（可选）

LDAP 身份验证后发生，您将其添加到第二个因素。

- add authentication policylabel second-factor
- bind authentication policylabel second-factor -policy ldap-**new** -priority 10
- bind authentication vserver auth -policy myrecaptcha -priority 1 -nextFactor second-factor

管理员需要添加适当的虚拟服务器，具体取决于是使用负载平衡虚拟服务器还是 Citrix Gateway 设备进行访问。如果需要负载平衡虚拟服务器，管理员必须配置以下命令：

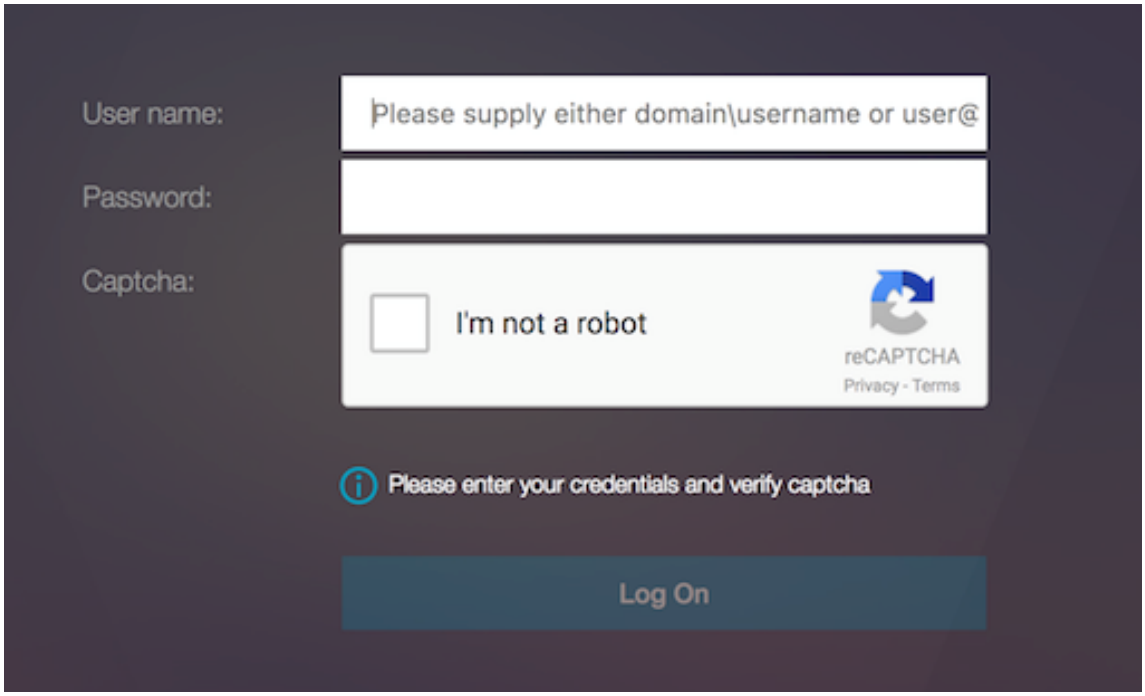
```
1 add lb vserver lbtest HTTP <IP> <Port> -authentication ON -
     authenticationHost nssp.aaatm.com`
```


nssp.aaatm.com — 解析为身份验证虚拟服务器。

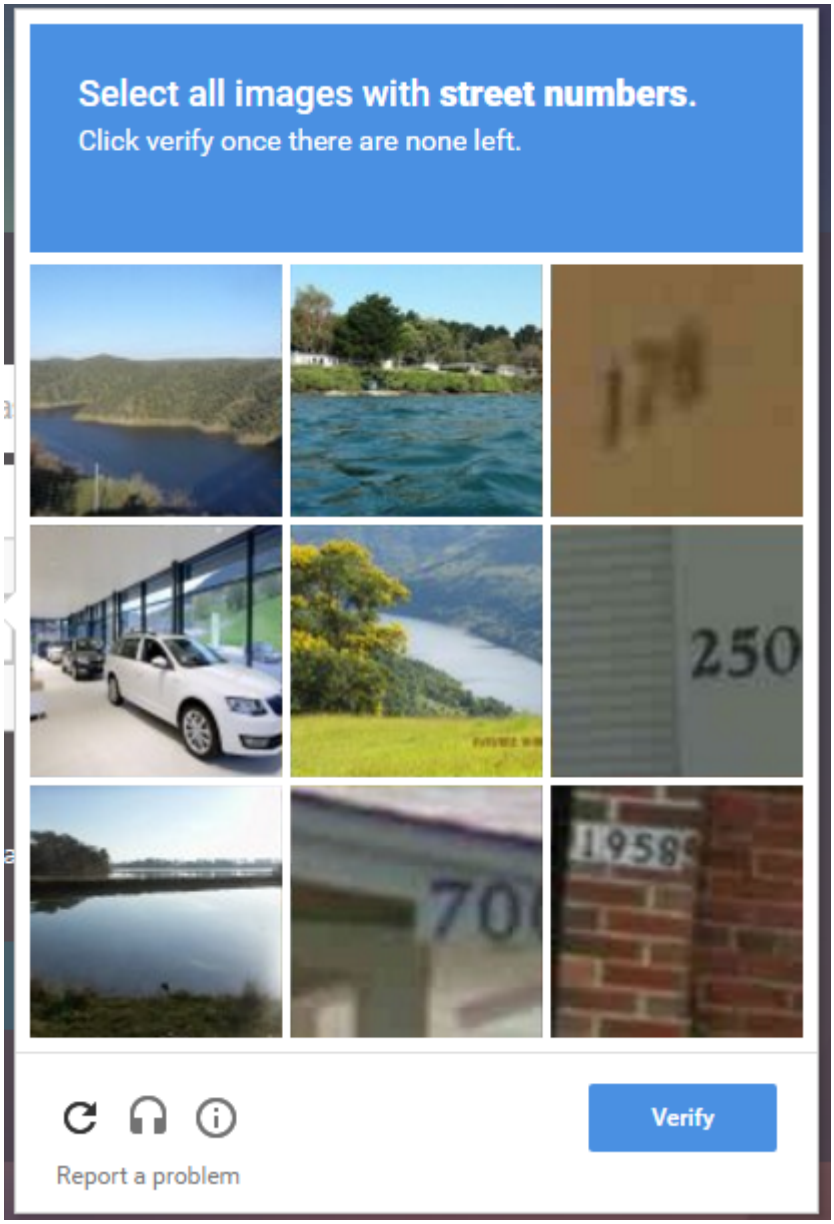
验证码的用户验证

配置了前面部分中提到的所有步骤后，您必须看到下面显示的 UI 屏幕截图。

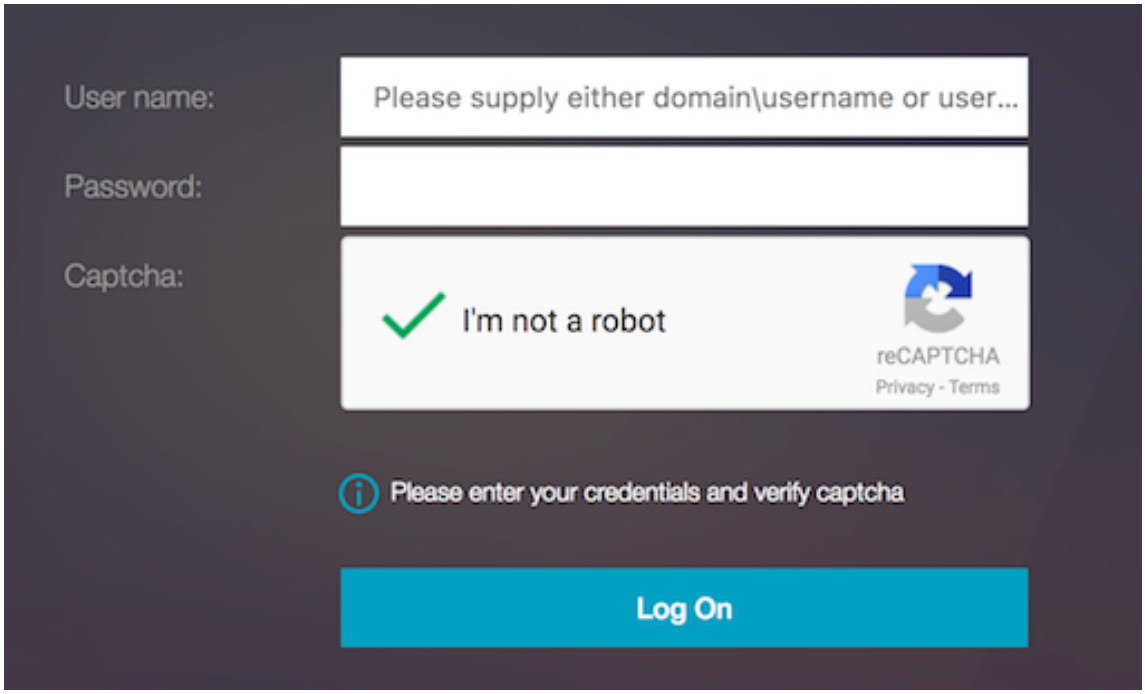
1. 身份验证虚拟服务器加载登录页面后，将显示登录屏幕。登录被禁用，直到验证码完成。



2. 选择我不是一个机器人的选项。将显示验证码小组件。



3. 在显示完成页面之前，您将浏览一系列验证码图像。
4. 输入 AD 凭据，选中“我不是机器人”复选框，然后单击“登录”。如果身份验证成功，您将被重定向到所需资源。



注意

- 如果验证码与 AD 身份验证一起使用，则会禁用凭据的提交按钮，直到验证码完成。
- 验证码发生在其自身的一个因素。因此，像 AD 这样的任何后续验证都必须发生在验证码的“下一个因素”中。

Unified Gateway Visualizer

April 6, 2020

概述

Unified Gateway Visualizer 使用 Unified Gateway 向导提供配置的可视化表示。Unified Gateway Visualizer 用于添加和编辑配置，并诊断后端问题。

Unified Gateway Visualizer 显示以下内容：
配置	配置
—	-
预身份验证策略	身份验证策略
CS 虚拟服务器	VPN 虚拟服务器
LB 虚拟服务器	XA/XD 应用程序
网络应用程序	SaaS 应用程序

Unified Gateway 部署可通过一个 URL 安全远程访问企业或 SaaS 应用程序、无客户端访问应用程序、Citrix Virtual Apps and Desktops 资源。

配置 **Unified Gateway**

1. 从菜单中选择 Unified Gateway。

2. 在下一个屏幕上，验证您是否有以下信息，然后单击“开始”：

```
- Unified Gateway 的公用 IP 地址。
- 带有可选根 CA 证书的 服务器证书链（.PFX 或 .pem）。
- 基于 LDAP/RADIUS/客户端证书的身份验证详细信息。
- 应用程序详细信息（SaaS 应用程序或 Citrix Virtual Apps and Desktops
  服务器详细信息的 URL）。
```

3. 点击继 续按钮。

创建 Unified Gateway 配置虚拟服务器。

1. 输入虚拟服务器的配置 名称。
2. 为 Unified Gateway 部署输入面向公众的 **Unified Gateway IP** 地址。
3. 输入 端口号。端口号的范围是 1-65535。
4. 单击继续。

请完成以下信息以指定服务器证书。

1. 选择“使用现有证书”或“安装证书”单选按钮。
2. 从下拉菜单中选择 服务器证书。
3. 点击继 续按钮。

请完成以下信息以指定身份验证。

1. 从下拉菜单中选择 主身份验证方法。
2. 选择“使用现有服务器”或“添加新服务器”单选按钮。
3. 点击继 续按钮。

1. 从下拉菜单中选择 门户主题。
2. 单击继续。

1. 选择 **Web** 应用程序或 **Citrix Virtual Apps and Desktops** 单选按钮。
2. 单击继续。

请完成以下信息以指定 Web 应用程序。

1. 输入书签链接的名称。

2. 选择 VPN URL 所代表的应用程序类型。可能的值是：

   - 内联网应用程序

- 无客户端访问
- SaaS
- 此 Citrix ADC 上的预配置应用程序

3. 选中此复选框可通过 Unified Gateway URL 访问此应用程序。
4. 输入书签链接的 URL。
5. 从图标 URL 中选择一个文件来获取图标文件。最大长度 = 255
6. 点击继续按钮。

1. 单击完成。

1. 单击继续。

1. 单击完成。

GUI 配置

1. 从菜单中选择 Unified Gateway。

1. 单击 Unified Gateway Visualizer 图标以访问已配置的网关实例。

Unified Gateway Visualizer 如下图所示：

Unified Gateway Visualizer 具有 PreAuth、身份验证和应用程序部分。如果 vpn 虚拟服务器具有预身份验证策略，则只有这样才会在 Unified Gateway Visualizer 中显示预身份验证。

Unified Gateway Visualizer 对负载平衡和 VPN 虚拟服务器使用颜色编码方案来指示它们的状态。

颜色	说明
红色	意味着服务器关闭。
灰色	意味着尚未配置 Web 应用程序/Citrix Virtual Apps。
绿色	意味着虚拟服务器一切都很好。
橙色	意味着负载平衡虚拟服务器服务之一。已关闭，但仍然运行正常。

VPN 虚拟服务器的详细信息

要获取 VPN 虚拟服务器的详细信息，请单击 VPN 虚拟服务器节点。弹出窗口会显示详细信息，如 C/S 规则和所有策略。

1. 通过单击 (+) 图标将策略添加到 VPN 实体。

默认情况下，将绑定以下策略。

1. 单击所需节点，了解已配置策略的详细信息。

对于 VPN 虚拟服务器信息，弹出窗口中的 VPN 标题是一个可点击的实体，进入详细描述 VPN 虚拟服务器的滑块。

VPN 服务器的详细信息显示在此处。

前身份验证区块

如果 VPN 虚拟服务器具有随之分配的预身份验证策略，Unified Gateway Visualizer 将显示一个 PreAuth 块。预身份验证块显示策略，并提供一个选项，用于将预身份验证策略添加到 VPN。

1. 单击 **+** 以添加序言策略。

在没有预身份验证策略被评估的情况下，此块将从视图中隐藏。

身份验证座

身份验证块列出了主策略和辅助策略。身份验证块提供了添加策略的选项。

1. 单击“主”列表中的“**+**”以添加主身份验证绑定，或单击“辅助”列表中的“+”以添加辅助身份验证绑定。

1. 从 主身份验证方法下拉菜单中选择一个选项。这是一个必填字段。
2. 指定它是使用 现有服务器还是通过选择单选按钮 添加新服务器。
3. 从 **LDAP** 策略名称下拉菜单中选择一个选项。这是一个必填字段。
4. 从 辅助身份验证方法下拉菜单中选择一个选项。这是一个必填字段。

1. 指定是要 使用现有服务器还是通过选择单选按钮 添加新服务器。
2. 从 **RADIUS** 下拉菜单中选择一个选项。这是一个必填字段。
3. 单击继续。

添加 **StoreFront**

点击 XA/XD 附近的 **+** ，它将带您添加“XA/XD”应用程序。

您可以选择您的集成点。这些选项是 StoreFront、WI 或 WionNS。单击继续。

1. 请完成以下字段以配置 StoreFront：

| 字段 | 说明 |
|-|—|
|StoreFront FQDN| 输入 *StoreFront* 服务器的 *FQDN*。最大长度：*255* 个字符。⊠ 示例：*//storefront.xendt.net*|
| 站点路径 *| 输入已在 *StoreFront* 上配置的 *Receiver for Web* 站点的路径。|
| 单点登录域 *| 输入用户身份验证的默认域 |
|*StoreFront* 名称 | 输入 STOREFRONT 显示器的名称。
STOREFRONT 是一个定义 StoreFront 服务应用商店名称的参数，用于探测 StoreFront 服务器的运行状况。适用于 STOREFRONT 显示器。最大长度：31|
| 安全票务机构服务器 *| 输入安全票务机构 URL。这通常存在于 Delivery Controller 上。
示例：`http://sta`|

StoreFront 服务器 *	输入 StoreFront 服务器的 IP 地址
协议	输入服务器使用的协议。
端口	输入服务器使用的端口。
负载平衡	输入 StoreFront 服务器的负载平衡配置。
虚拟服务器 *	输入 Unified Gateway 部署的面向公众的 IP 地址。

2. 点击 继续

添加 **SaaS**

1. 点击 **+** 添加 SaaS 应用程序，您将转到 “添加 SaaS” 页面。请完成以下字段以配置 SaaS。需要强制性信息的字段在 * 中注明。

字段	说明
名称 *	输入书签链接的名称。
应用程序类型	输入此 VPN URL 代表的应用程序类型。可能的值为：此 Citrix ADC 上的 Intranet 应用程序/无客户端访问/SaaS/预配置应用程序
输入 URL *	输入内部网应用程序的 URL。
选择文件	输入 URL 以获取显示此资源的图标文件。最大长度 = 255

添加 **Web** 应用程序

1. 点击 **+** 添加 Web 应用程序，它将带您进入 “添加 Web 应用程序” 页面。请完成以下字段以配置 Web 应用程序。需要强制性信息的字段在 * 中注明。

字段	说明
名称 *	输入书签链接的名称。
应用程序类型	输入此 VPN URL 代表的应用程序类型。可能的值为：此 Citrix ADC 上的 Intranet 应用程序/无客户端访问/SaaS/预配置应用程序
输入 URL *	输入内部网应用程序的 URL。
选择文件	输入 URL 以获取显示此资源的图标文件。最大长度 = 255

如果可以通过 Unified Gateway URL 访问应用程序，则可以通过单击应用程序访问负载平衡服务器的详细信息：

可以通过单击 (+) 添加新策略，单击显示策略信息的节点可以查看所有绑定策略。

还会显示绑定到 LB 的服务数量以及整体状态信息。进一步点击将列出所有服务。新服务可以添加到 LB。

有关 LB 的更多详细信息，弹出窗口的标题可以点击，土地到 LB 虚拟服务器详细信息页面。

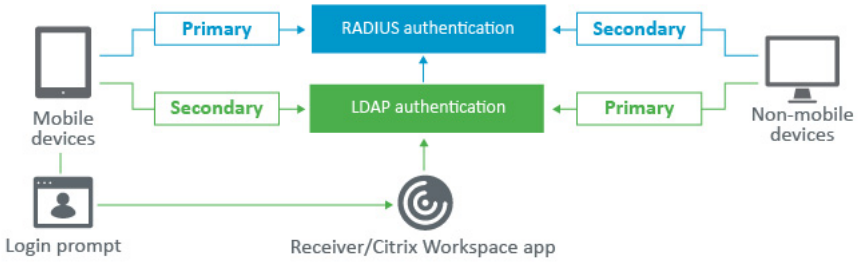
将 **Citrix Gateway** 配置为将 **RADIUS** 和 **LDAP** 身份验证与移动/平板电脑设备配置为使用

April 6, 2020

本节介绍如何将 Citrix Gateway 设备配置为使用 RADIUS 身份验证作为主要使用，并将 LDAP 身份验证用作移动/平板电脑设备的辅助设备。

部分中演示的配置仍然允许所有其他连接首先使用 LDAP 和 RADIUS 秒。

在 Citrix Workspace 应用程序上配置双重身份验证以用于移动/平板电脑设备时，必须添加 RSA SecureID（RADIUS 身份验证）作为主身份验证。但是，当用户收到用户名和密码，Receiver 上的密码提示时，他们将首先将 LDAP 和 RADIUS 作为第二个凭据。从管理员的角度来看，它是一个不同的配置与非移动配置相比。



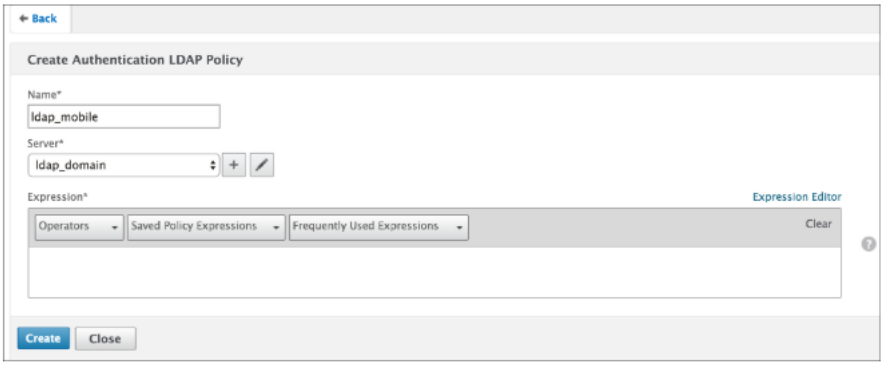
完成以下过程，将 Citrix Gateway 设备配置为使用 RADIUS 身份验证作为主要使用，并将 LDAP 身份验证用作移动/平板电脑设备的辅助设备。

1. 从配置实用程序中，选择 “Citrix Gateway”>“策略”>“身份验证”，然后为移动设备和非移动设备的 LDAP 和 RSA 创建身份验证策略。这是必要的，以避免可能允许用户绕过 RADIUS 身份验证的逻辑条件。
2. 单击 LDAP 的服务器选项卡下的添加选项后，输入 LDAP 服务器详细信息。

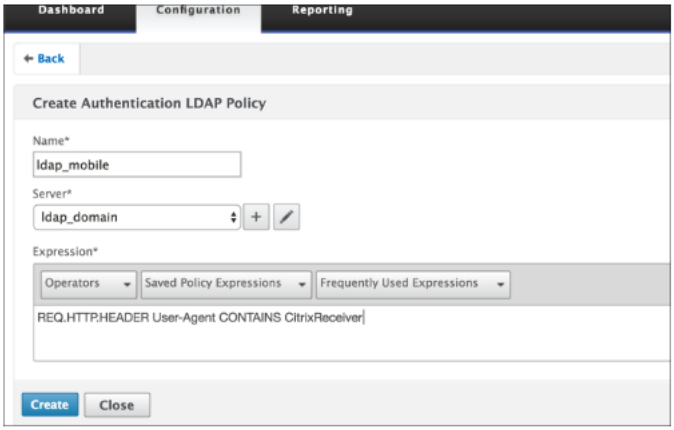
   有关如何配置身份验证服务器的详细信息，请参阅如何在 NetScaler 上配置 LDAP 身份验证的 “创建身份验证服务器” 部分
3. 通过选择所需的 LDAP 服务器，为移动设备创建 LDAP 策略。

   要仅将此策略绑定到移动设备，请使用以下表达式：

   ```
   1 `REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver`
   ```

4. 单击表达式编辑器以创建策略：

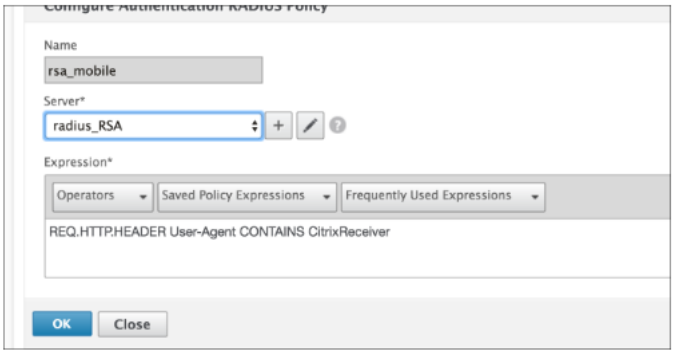


5. 为移动设备创建 RADIUS 策略和 RADIUS 服务器。

   (a) 从 “Citrix Gateway”>“策略”>“身份验证”>“RADIUS” 导航到 “RADIUS” 选项。单击 “服务器” 选项卡下的 “添加”。

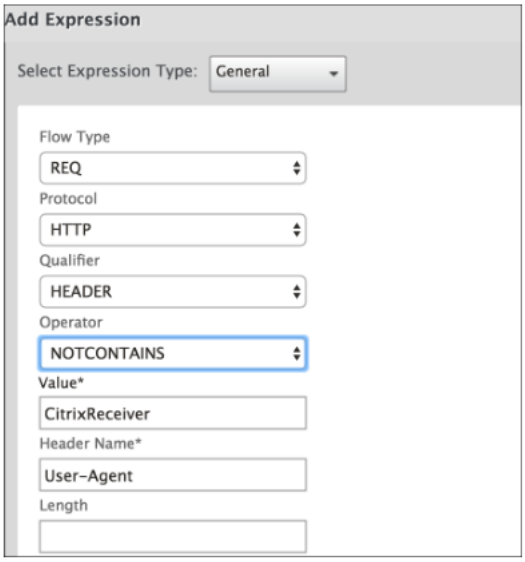
(b) 增加所需的细节。RADIUS 身份验证的默认端口是 1812。

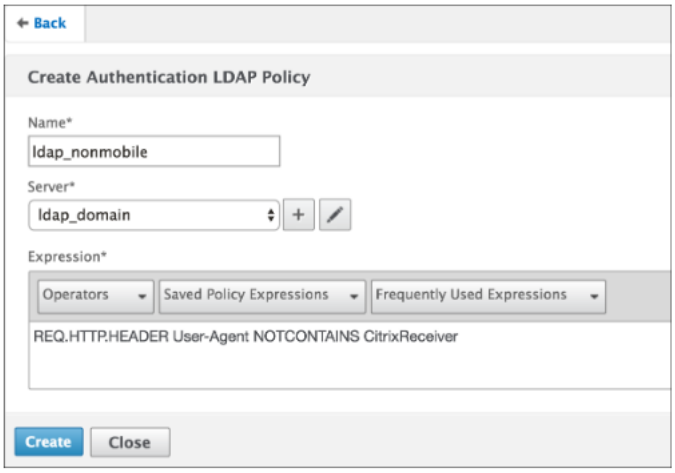
(c) 要仅将此策略绑定到移动设备，请使用以下表达式：



6. 按照相同的步骤为非移动设备创建 LDAP 策略。要仅将此策略绑定到非移动设备，请使用以下表达式：

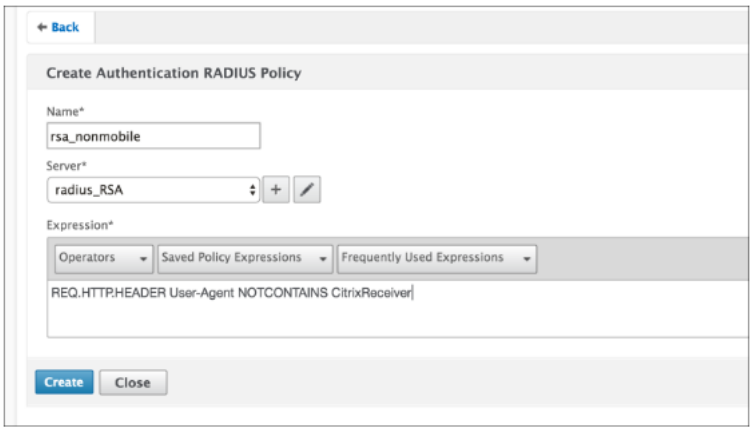
```
1 `REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver`
```

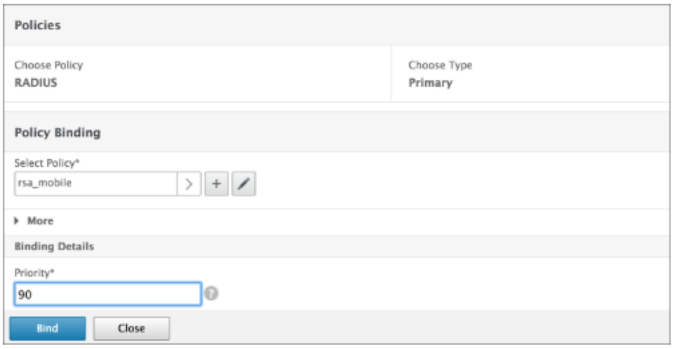


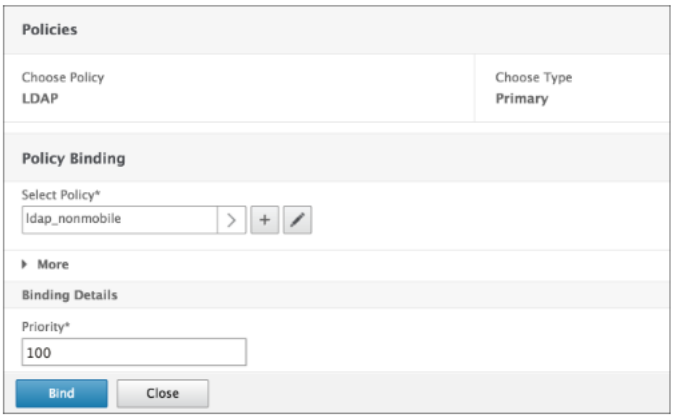
7. 为非移动设备创建 RADIUS 策略。要仅将此策略绑定到非移动设备，请使用以下表达式：

```
`REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver`
```

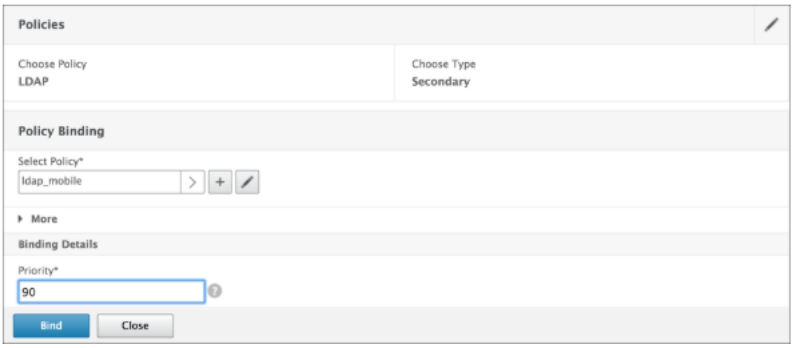


8. 转到 Citrix Gateway 虚拟服务器的属性，然后单击身份验证选项卡。在主身份验证策略上，将 RSA_Mobile 策略添加为最高优先级，并将 LDAP_NonMobile 策略添加为次要优先级：





9. 在辅助身份验证策略上，将 LDAP_Mobile 策略添加为最高优先级，然后将 RSA_NonMobile 策略作为辅助优先级：

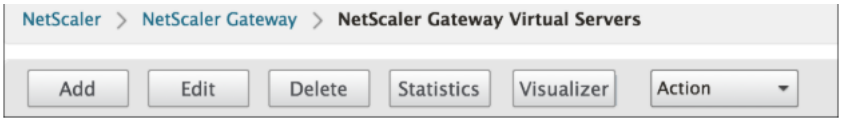


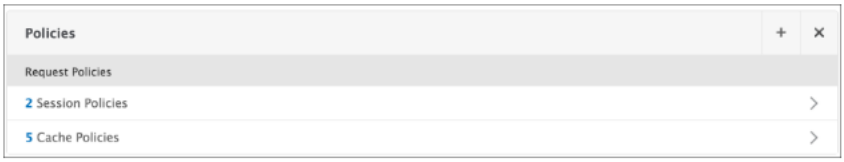
> 会话策略必须具有正确的单点登录凭据索引，也就是说，它必须是 LDAP 凭据。对于移动设备，会话配置文件 > 客户端体验下的凭据索引应设置为辅助，即 LDAP。

因此，您需要两个会话策略，一个用于移动设备，另一个用于非移动设备。

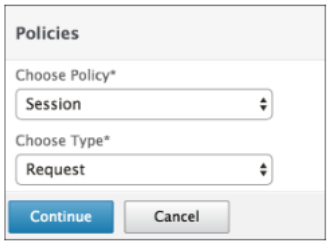
(a) 对于移动设备，会话策略和会话配置文件将如下面的屏幕截图所示。

要创建会话策略，请导航到所需的虚拟服务器，然后单击编辑，转到策略部分，然后单击 + 签名：

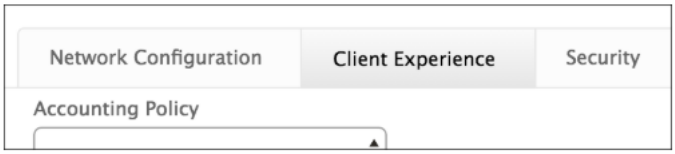


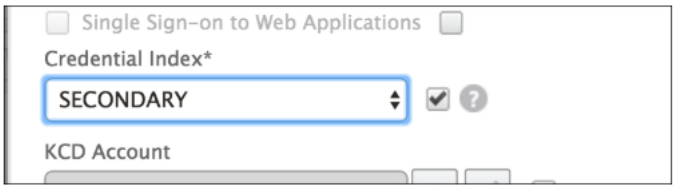


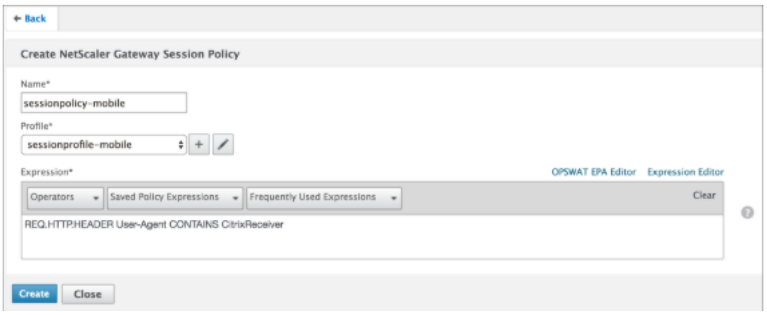
(b) 从下拉菜单中选择会话选项。



(c) 输入所需的会话策略名称，然后单击 + 以创建新的配置文件。对于移动设备，会话配置文件 > 客户端体验下的凭据索引应设置为辅助，即 LDAP。



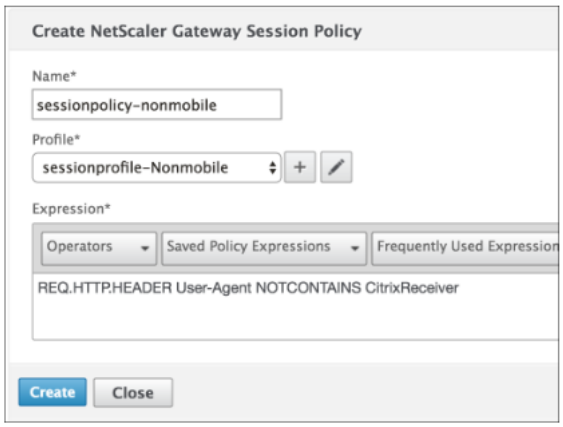




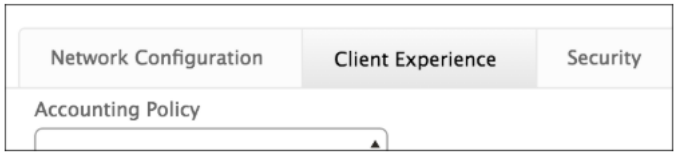
(d) 对于非移动设备，请遵循相同的步骤。会话配置文件 > 客户端体验下的凭据索引应设置为主，即 LDAP。

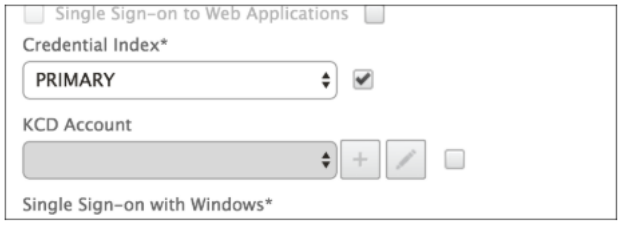
表达式应更改为：

```
1 `REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver`
```

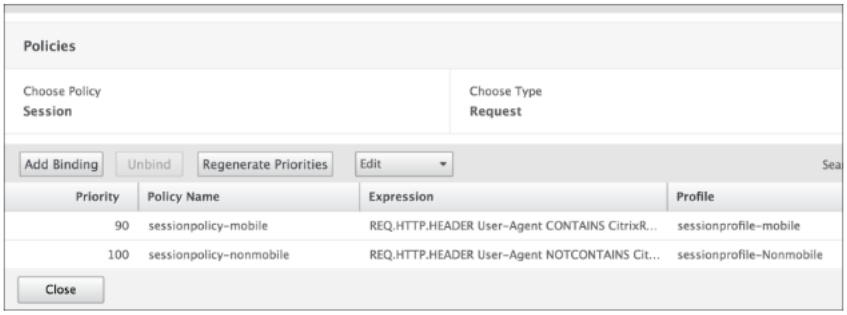



(e) 要为非移动用户创建新的配置文件，请点击 + 签名。

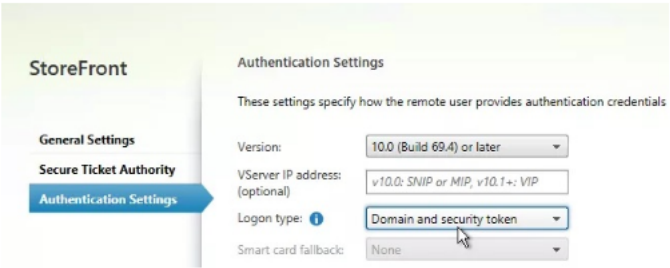


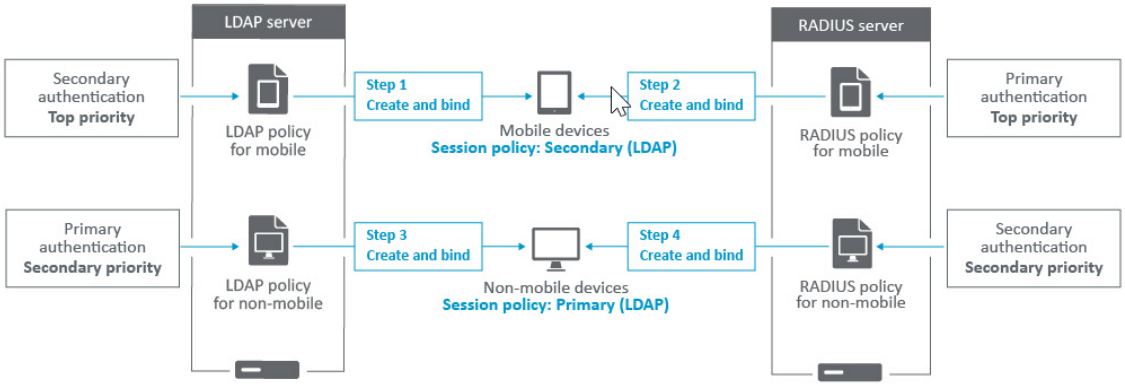


1. 所需虚拟服务器下的策略和配置文件将类似于以下屏幕截图：



2. 此外，在 StoreFront 上，在 Citrix Gateway 配置设置为使用 “登录类型”=“域和安全令牌”





配置 VPN 用户体验

April 6, 2020

用户可以使用以下方法通过 Citrix Gateway 连接到组织的网络资源：

- Citrix Workspace 应用程序，其中包含用户设备上安装的所有 Citrix 插件。
- 适用于 Web 的 Citrix Workspace 应用程序，该应用程序允许用户通过 Web 浏览器连接到应用程序、桌面和 ShareFile。
- Secure Hub，允许用户从其 iOS 和 Android 设备访问 Secure Mail、WorxWeb 和移动应用程序。
- 适用于 Windows、Mac OS X 或 Linux 的 Citrix Gateway 插件。
- 适用于 iOS 和 Android 的 Citrix Gateway 应用程序。
- 适用于 Java 的 Citrix Gateway 插件。
- 无客户端访问，为用户提供他们所需的访问权限，而无需安装用户软件。
- 与 Citrix Repeater 插件的互操作性。

如果用户安装 Citrix Gateway 插件，然后安装适用于 Windows Server 2008 的 Citrix XenApp 6.5 的 Citrix Workspace 应用程序（包括 Feature Pack 和 Feature Pack 2）、Citrix Virtual Desktops 7.0 或更高版本，则 Citrix Workspace 应用程序会自动添加 Citrix Gateway 插件。用户可以通过 Web 浏览器或 Citrix Workspace 应用程序连接 Citrix Gateway 插件。

SmartAccess 根据端点分析扫描的结果自动确定允许用户设备的访问方法。有关 SmartAccess 的详细信息，请参阅配置 SmartAccess主题。

Citrix Gateway 支持适用于 iOS 和 Android 移动设备的 Citrix Endpoint Management Worx 应用程序。Citrix Gateway 包含安全浏览，允许从建立微型 VPN 隧道的 iOS 移动设备连接到 Citrix Gateway。与 Secure Hub 连接的 Android 设备还会自动建立 Micro VPN 隧道，提供对内部网络中资源的 Secure Web 和移动应用程序级访问。如果用户通过 Worx 应用从 Android 设备进行连接，则必须在 Citrix Gateway 上配置 DNS 设置。有关详细信息，请参阅支持使用面向 Android 设备的 DNS 后缀进行 DNS 查询主题。

用户连接如何使用 **Citrix Gateway** 插件

April 6, 2020

Citrix Gateway 的运行方式如下：

- 当用户尝试通过 VPN 隧道访问网络资源时，Citrix Gateway 插件会加密发往组织内部网络的所有网络流量，并将数据包转发到 Citrix Gateway。
- Citrix Gateway 终止 SSL 隧道，接受发往专用网络的任何传入流量，然后将流量转发到专用网络。Citrix Gateway 通过安全隧道将流量发回到远程计算机。

当用户键入 Web 地址时，他们会收到一个登录页面，他们在其中输入凭据并登录。如果凭据正确，Citrix Gateway 将完成与用户设备的握手。

如果用户位于代理服务器后面，则用户可以指定代理服务器和身份验证凭据。有关详细信息，请参阅为用户连接启用代理支持。

Citrix Gateway 插件已安装在用户设备上。第一次连接后，如果用户使用基于 Windows 的计算机登录，他们可以使用通知区域中的图标建立连接。

建立安全隧道

April 6, 2020

当用户连接到 Citrix Gateway 插件、Secure Hub 或 Citrix Workspace 应用程序时，客户端软件会通过端口 443（或 Citrix Gateway 上的任何配置端口）建立安全隧道并发送身份验证信息。建立隧道后，Citrix Gateway 会将配置信息发送到 Citrix Gateway 插件、Secure Hub 或 Citrix Workspace 应用程序，描述要保护的网络，并在启用地址池时包含 IP 地址。

通过安全连接隧道专用网络流量

当 Citrix Gateway 插件启动并对用户进行身份验证时，将捕获发往指定专用网络的所有网络流量，并通过安全隧道重定向到 Citrix Gateway。Citrix Workspace 应用程序必须支持 Citrix Gateway 插件，才能在用户登录时通过安全隧道建立连接。

Secure Hub、Secure Mail 和 WorxWeb 使用 Micro VPN 为 iOS 和 Android 移动设备建立安全通道。

Citrix Gateway 拦截用户设备建立的所有网络连接，并通过安全套接字层 (SSL) 将这些网络连接多路复用到 Citrix Gateway，从而将流量解复用并将连接转发到正确的主机和端口组合。

连接受适用于单个应用程序、应用程序子集或整个 Intranet 的管理安全策略的约束。您可以指定远程用户可以通过 VPN 连接访问的资源（IP 地址/子网对的范围）。

Citrix Gateway 插件拦截并通过已定义的 Intranet 应用程序的以下协议进行隧道：

- TCP（所有端口）
- UDP（所有端口）
- ICMP（类型 8 和 0-回显请求/回复）

来自用户设备上的本地应用程序的连接安全地通道到 Citrix Gateway，后者将重新建立到目标服务器的连接。目标服务器查看来自专用网络上本地 Citrix Gateway 的连接，从而隐藏用户设备。这也称为反向网络地址转换 (NAT)。隐藏 IP 地址可增加源位置的安全性。

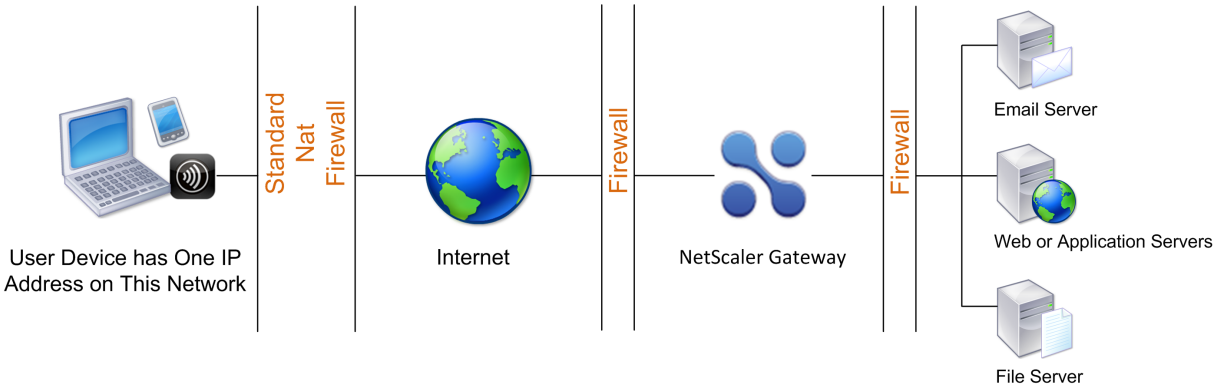
在本地，在用户设备上，所有与连接相关的流量（如 SYN-ACK、PUSH、ACK 和 FIN 数据包）都由 Citrix Gateway 插件重新创建，以便从专用服务器中显示。

通过防火墙和代理操作

April 6, 2020

Citrix Gateway 插件的用户有时位于另一组织的防火墙内，如下图所示：

图 1. 通过两个内部防火墙从用户设备进行连接



NAT 防火墙维护一个表，允许它们将安全数据包从 Citrix Gateway 路由回用户设备。对于面向电路的连接，Citrix Gateway 维护端口映射的反向 NAT 转换表。反向 NAT 转换表使 Citrix Gateway 能够匹配连接，并通过隧道将数据包发回具有正确端口号的用户设备，以便数据包返回到正确的应用程序。

Citrix Gateway 插件升级控制

April 6, 2020

概述

系统管理员控制 Citrix ADC 插件的版本与 Citrix Gateway 修订版本不匹配时的执行方式。新选项控制 Mac、Windows 或操作系统的插件升级行为。

对于 VPN 插件，升级选项可以在 Citrix ADC 用户界面的两个位置设置：

- 在全局设置
- 在会话配置文件级别

插件行为

对于每种客户端类型，Citrix Gateway 允许以下三个选项来控制插件升级行为：

a. 始终如一

当最终用户的插件版本与 Citrix ADC 附带的插件不匹配时，插件始终会升级。这是默认行为。如果您不希望在企业中运行多个插件版本，请选择此选项。

b. 基本 (和安全)

只有在认为必要时才会升级插件。在以下两种情况下认为有必要升级

- 已安装的插件与当前 Citrix ADC 版本不兼容。
- 安装的插件需要更新以便进行必要的安全修复。

如果希望尽量减少插件升级次数，但不希望错过任何插件安全更新，则应选择此选项

c. 从来没有

插件不会升级。

用于控制 **VPN** 插件升级的 **CLI** 参数

Citrix Gateway 支持两种类型的适用于 Windows 和 Mac 操作系统的插件（EPA 和 VPN）。若要在会话级别支持 VPN 插件升级控制，Citrix Gateway 支持两个会话配置文件参数，名为 WindowsinPluginUpgrade 和 MacPluginUpgrade。

这些参数在全局、虚拟服务器、组和用户级别可用。每个参数的值都可以为“始终”、“基本”或“从不”。有关这些参数的说明，请参阅插件行为。

控制 **EPA** 插件升级的 **CLI** 参数

Citrix Gateway 支持适用于 Windows 和 Mac 操作系统的 EPA 插件。为了在虚拟服务器级别支持 EPA 插件升级控制，Citrix Gateway 支持两个名为“窗口插件升级”和“麦当插件升级”的虚拟服务器参数。

这些参数在虚拟服务器级别可用。每个参数的值都可以为“始终”、“基本”或“从不”。有关这些参数的说明，请参阅插件行为

VPN 配置

请按照以下步骤进行 Windows、Linux 和 Mac 插件的 VPN 配置。

1. 转到 “Citrix NetScaler”>“策略”>“会话”。
2. 选择所需的会话策略，然后单击 编辑。
3. 点击 **+** 图标。
4. 选择 客户体验选项卡。
5. 这些对话框选项会影响升级行为。
    - 总是这样
    - 必不可少
    - 从来没有

> 默认值为 “始终”。

1. 选中每个选项右侧的复选框。选择要应用升级行为的频率。

EPA 配置

按照以下步骤为 Windows、Linux 和 Apple 插件配置 EPA。

1. 转到 “Citrix Gateway”>“虚拟服务器”。
2. 选择一个服务器，然后单击 编辑按钮。
3. 点击 铅笔图标。
4. 点击 更多
5. 出现的对话框会影响升级行为。可用的选项包括：

- 总是这样
- 必不可少
- 从来没有

要求

- Windows EPA 和 VPN 插件版本应高于 11.0.0.0
- Mac EPA 插件版本应大于 3.0.0.31
- Mac VPN 插件版本应大于 3.1.4 (357)

> 注意：如果 Citrix ADC 升级到 11.0 版本，则无论升级控制配置如何，以前的所有 VPN（和 EPA）插件都将升级到最新版本。对于后续升级，他们将遵守上述升级控制配置。

在 **Citrix Gateway** 上配置完整的 **VPN** 设置

November 3, 2021

本节介绍如何在 Citrix Gateway 设备上配置完整的 VPN 设置。它包含联网考虑因素和从联网角度解决问题的理想方法。

必备条件

- SSL 证书：应安装此证书并绑定到 VPN 虚拟服务器。
  - CTX109260-如何在 NetScaler 设备上生成和安装公有 SSL 证书
  - CTX122521-如何将 NetScaler 设备的默身份验证书替换为与设备的主机名匹配的受信任 CA 证书
  - Citrix 文档 - 将证书密钥对绑定到基于 SSL 的虚拟服务器
- 身份验证配置文件：应该在 Citrix Gateway 上创建并正常运行。
  - 有关其他信息，请参阅 Citrix 文档-配置外部用户身份验证
  - 有关更多信息，请参阅清单：使用 AD FS 实现和管理单点登录
- 下载 Citrix VPN 客户端
- 会话策略（允许完整的 VPN 连接）

当用户连接到 Citrix Gateway 插件、Secure Hub 或 Citrix Workspace 应用程序时，客户端软件会通过端口 443（或 Citrix Gateway 上的任何配置端口）建立安全隧道并发送身份验证信息。建立隧道后，Citrix Gateway 将配置信息发送到 Citrix Gateway 插件、Citrix Secure Hub 或 Citrix Workspace 应用程序，描述要保护的网络。如果您启用 Intranet IP，则该信息还将包含 IP 地址。

通过定义用户可以在内部网络中访问的资源来配置用户设备连接。配置用户设备连接包括以下内容：

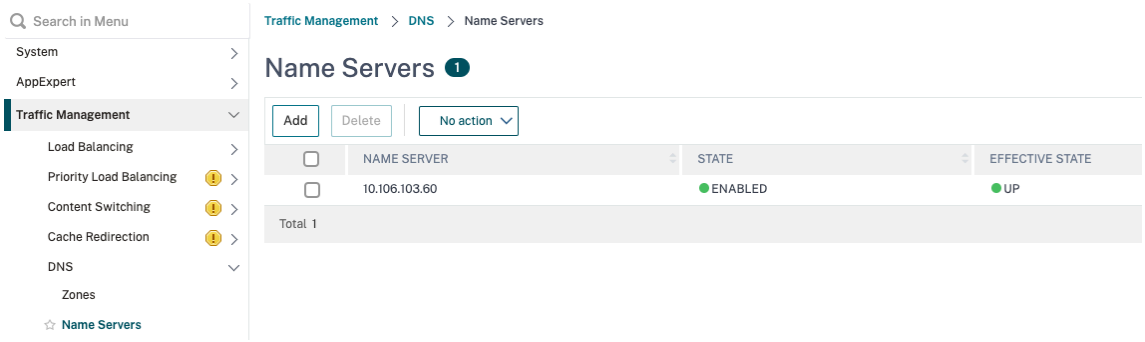
- 分裂式隧道
- 用户的 IP 地址，包括地址池（Intranet IP）
- 通过代理服务器进行连接
- 定义允许用户访问的域
- 超时设置
- 单点登录
- 将通过 Citrix Gateway 连接的用户软件
- 移动设备的访问权限

您可以使用属于会话策略一部分的配置文件配置大多数用户设备连接。您还可以使用每个身份验证、流量和授权策略来定义用户设备连接设置。它们也可以使用 Intranet 应用程序进行配置。

在 **Citrix Gateway** 设备上配置完整的 **VPN** 安装程序

要在 Citrix Gateway 设备上配置 VPN 设置，请完成以下过程：

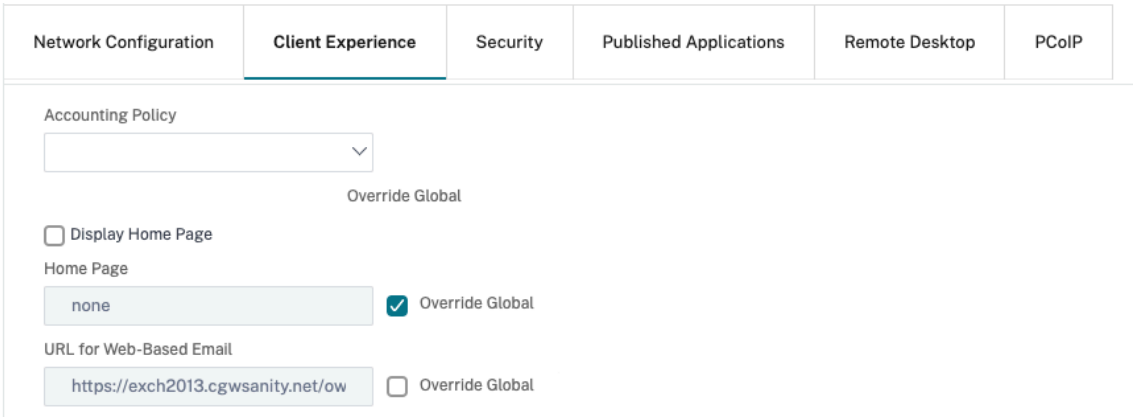
1. 从 NetScaler 配置实用程序，导航到流量管理 > DNS。
2. 选择“名称服务器”节点，如以下屏幕截图所示。确保列出 DNS 名称服务器。如果不可用，请添加 DNS 名称服务器。



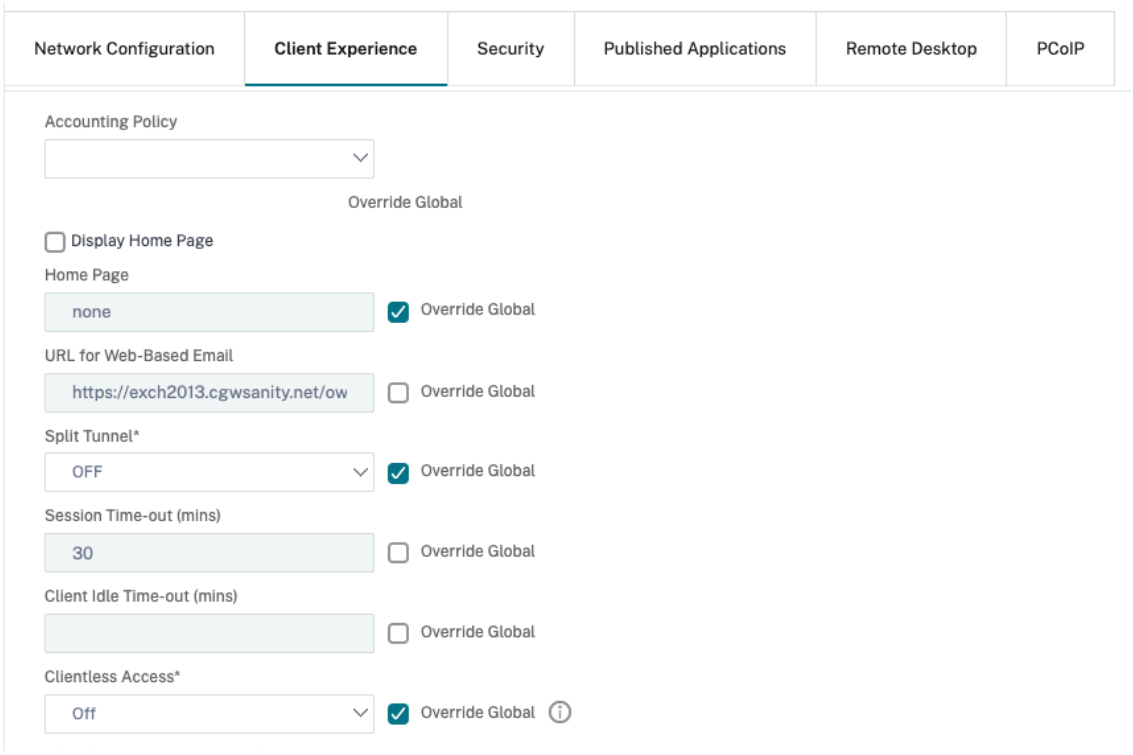
3. 展开“Citrix Gateway”>“策略”。
4. 选择会话节点。
5. 激活 Citrix Gateway 会话策略和配置文件页面的“配置文件”选项卡，然后单击“添加”。

> 对于在“配置 Citrix Gateway 会话配置文件”对话框中配置的每个组件，请确保为相应组件选择“覆盖全局”选项。

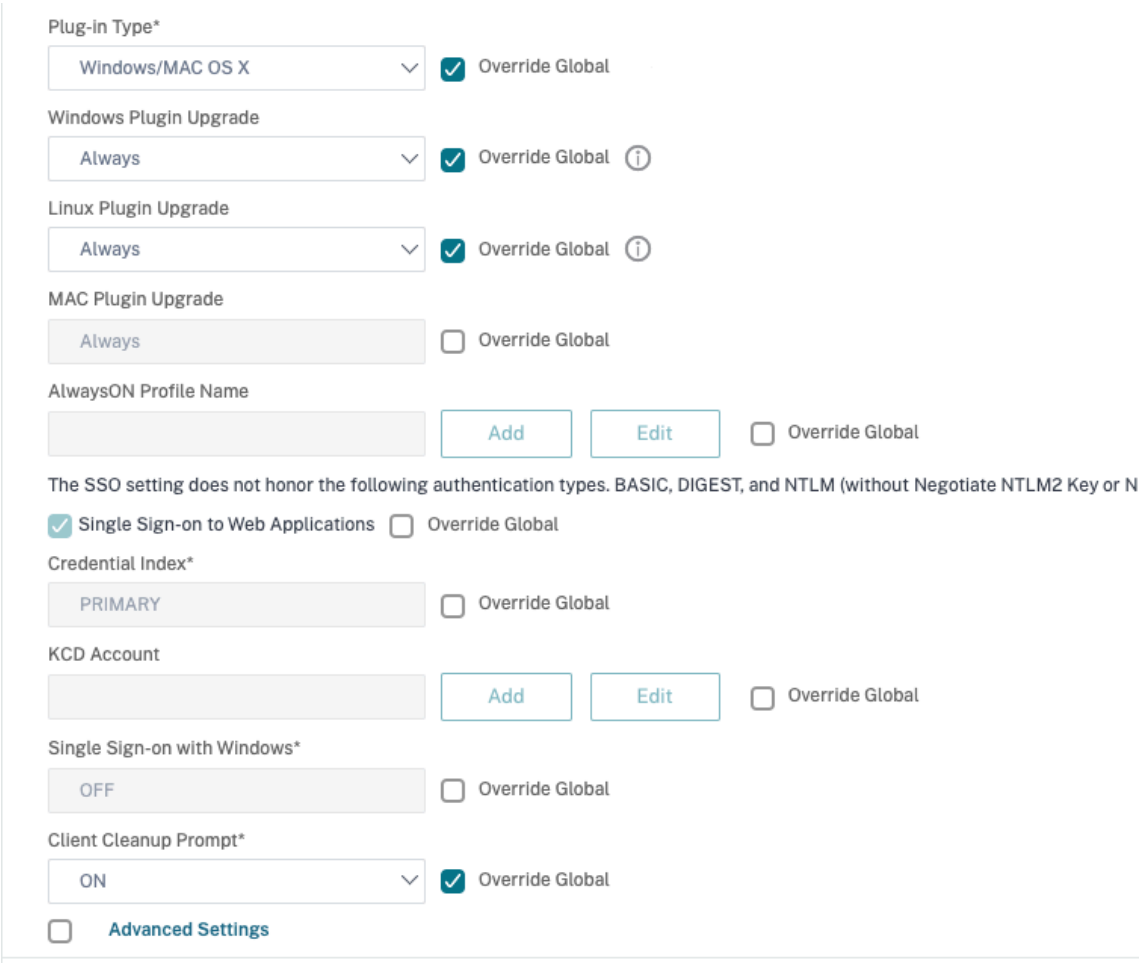
6. 激活“客户体验”选项卡。
7. 如果您希望在用户登录 VPN 时显示任何 URL，请在“主页”字段中键入 Intranet 门户 URL。如果主页参数设置为“nohomepage.html”，则不会显示主页。当插件启动时，浏览器实例会自动启动并被终止。



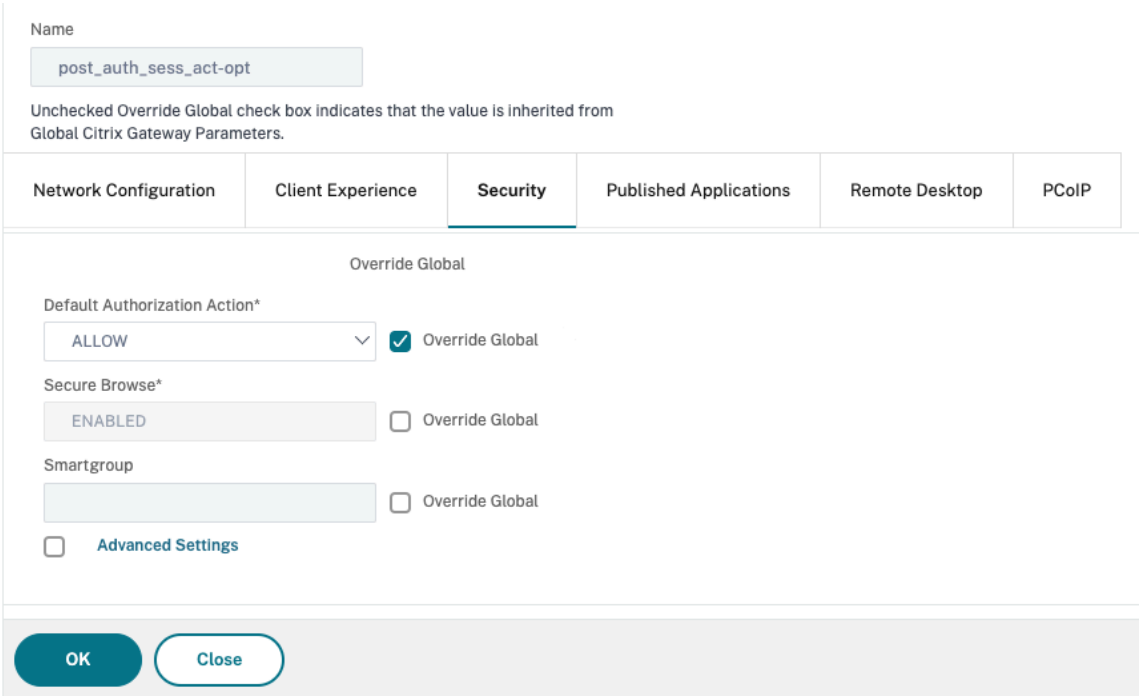
8. 确保从“分割隧道”列表中选择所需的设置（有关此设置的详细信息，请参阅上述）。
9. 如果您需要 FullVPN，请从无客户端访问列表中选择关闭。



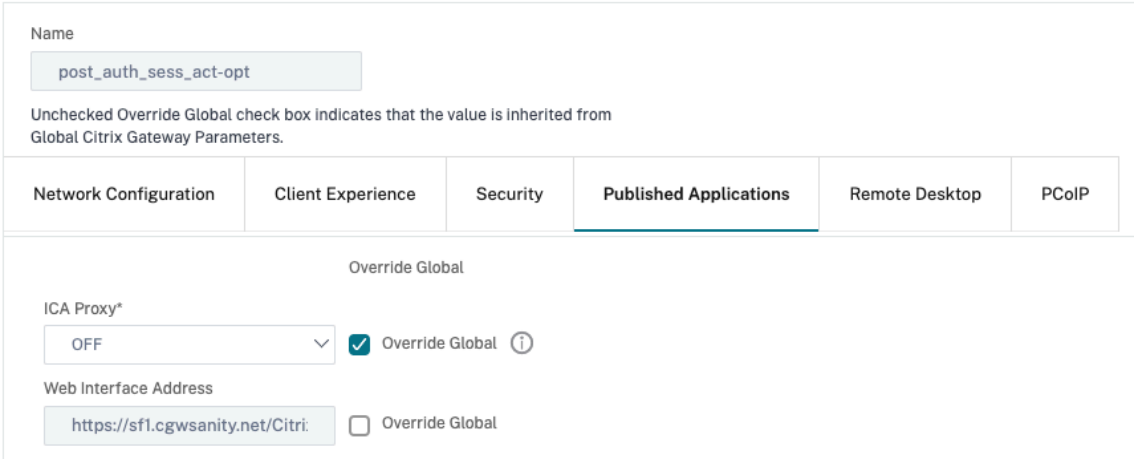
10. 确保从插件类型列表中选择了 Windows/MAC OS X。
11. 如果需要，选择“单点登录到 Web 应用程序”选项。
12. 如果需要，请确保选中“客户端清理提示符”选项，如以下屏幕截图所示：



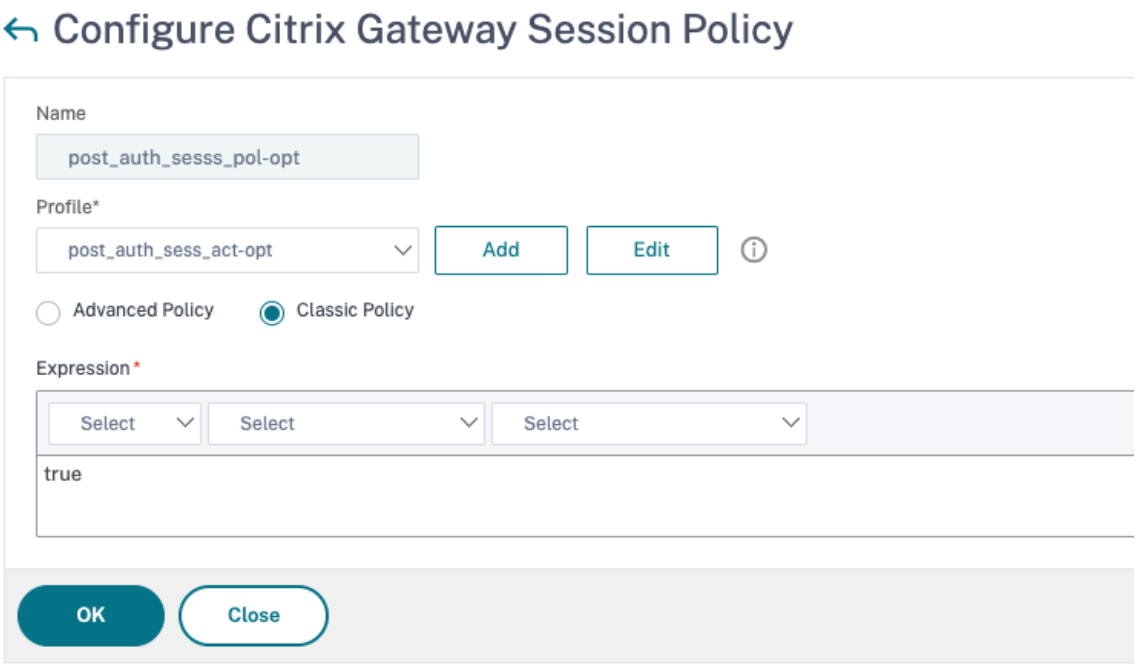
13. 激活“安全”选项卡。
14. 确保从“默认授权操作”列表中选择了“允许”，如以下屏幕截图所示：



15. 激活“已发布的应用程序”选项卡。
16. 确保从“已发布应用程序”选项下的“ICA 代理”列表中选择了 OFF。



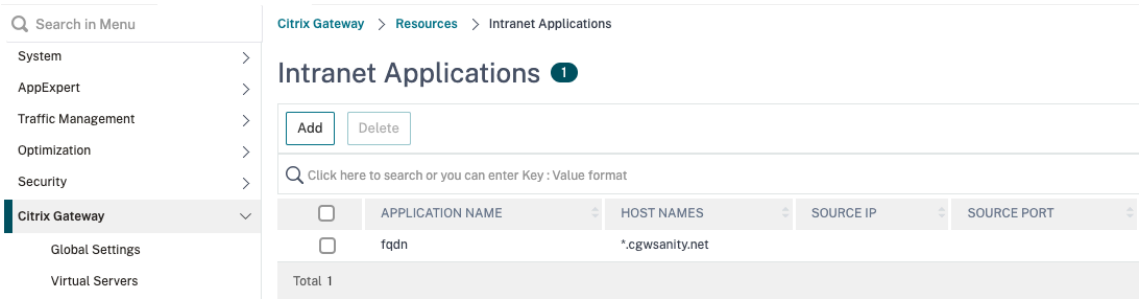
17. 单击创建。
18. 单击关闭。
19. 激活虚拟服务器中 Citrix Gateway 会话策略和配置文件页面的“策略”选项卡，或根据需要在 GROUP/USER 级别激活会话策略。
20. 使用必需的表达式或 ns_true 创建会话策略，如以下屏幕截图所示：



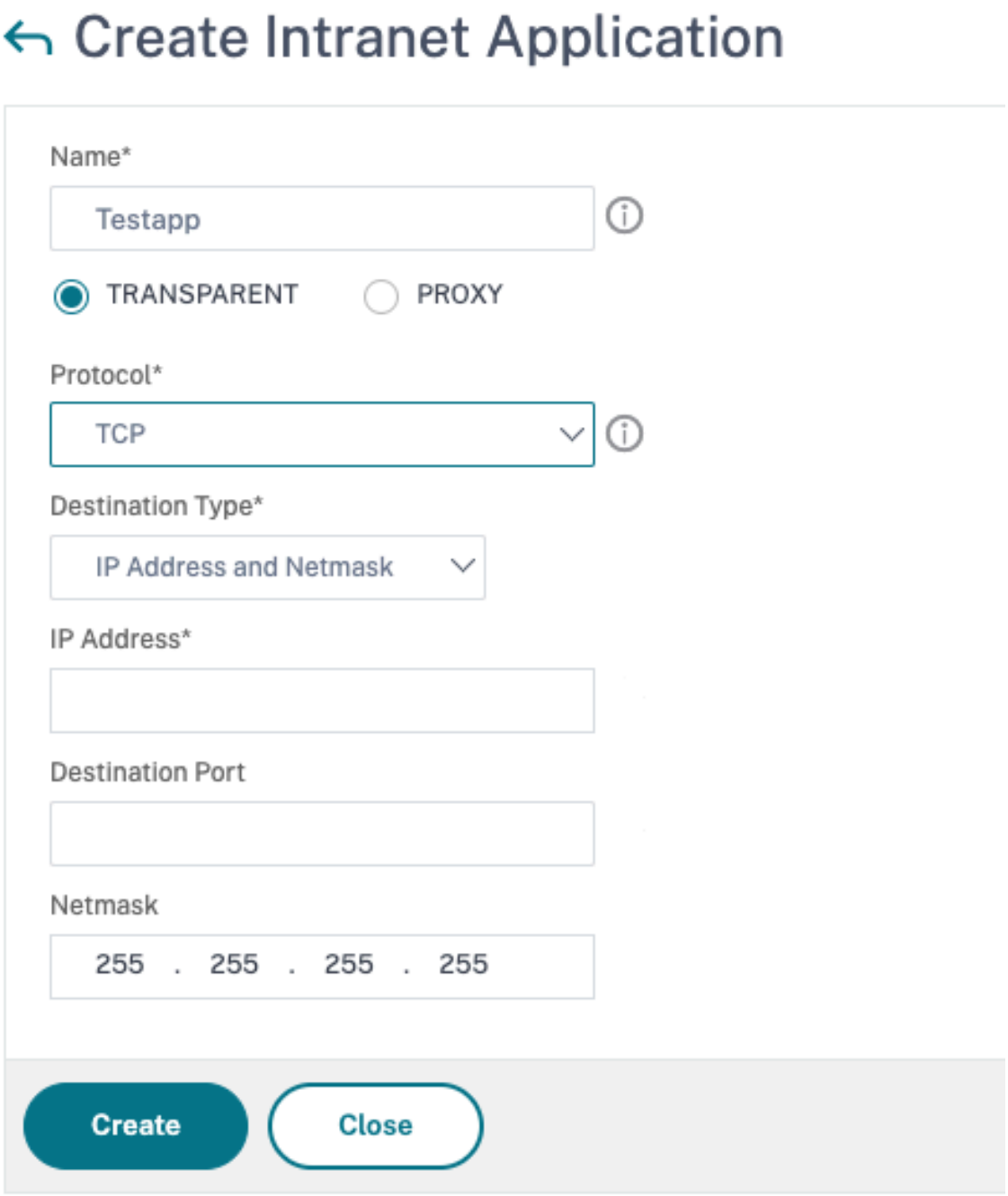
21. 将会话策略绑定到 VPN 虚拟服务器。

    转到 Citrix Gateway 虚拟服务器 > 策略。从下拉列表中选择所需的会话策略（在本示例中为 Session _Policy）。

22. 如果 “拆分隧道” 配置为 “开”，则应配置您希望用户在连接到 VPN 时访问的 Intranet 应用程序。转到 “Citrix Gateway”>“资源”>“Intranet 应用程序”。



23. 创建新的 Intranet 应用程序。为具有 Windows 客户端的完整 VPN 选择透明。选择要允许的协议（TCP、UDP 或任何）、目标类型（IP 地址和掩码、IP 地址范围或主机名）。



24. 使用以下表达式在 iOS 和 Android 上为 Citrix VPN 设置新策略：

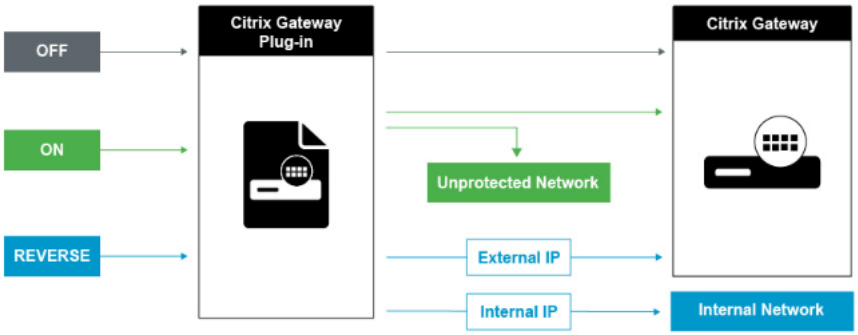
25. 使用以下表达式在 iOS 和 Android 上为 Citrix VPN 设置新策略：
REQ.HTTP.HEADER User-Agent CONTAINS CitrixVPN && (REQ.HTTP.HEADER User-Agent CONTAINS NSGiOSplugin || REQ.HTTP.HEADER User-Agent CONTAINS Android)

26. 根据需要绑定在 USER/GROUP/VSERVER 级别创建的 Intranet 应用程序。

    附加参数

    以下是我们可以配置的一些参数以及每个参数的简要描述：

    分裂隧道



拆分隧道

将分割隧道设置为关闭时，Citrix Gateway 插件会捕获来自用户设备的所有网络流量，并通过 VPN 隧道将流量发送到 Citrix Gateway。换句话说，VPN 客户端建立从客户端 PC 指向 Citrix Gateway VIP 的默认路由，这意味着所有流量都需要通过隧道发送到目标。由于所有流量都将通过隧道发送，因此授权策略必须确定是否允许流量传递到内部网络资源，还是拒绝流量。

当设置为“关闭”时，所有流量都通过隧道，包括到网站的标准 Web 流量。如果目标是监控和控制此 Web 流量，那么我们应该使用 NetScaler 将这些请求转发给外部代理。用户设备也可以通过代理服务器进行连接，以访问内部网络。Citrix Gateway 支持 HTTP、SSL、FTP 和 SOCKS 协议。要为用户连接启用代理支持，必须在 Citrix Gateway 上指定这些设置。您可以指定 Citrix Gateway 上的代理服务器使用的 IP 地址和端口。代理服务器用作所有进一步连接到内部网络的转发代理。

有关更多信息，请查看以下链接：

- 为用户连接启用代理支持
- 拆分隧道关闭

分裂隧道

您可以启用拆分隧道，以防止 Citrix Gateway 插件向 Citrix Gateway 发送不必要的网络流量。如果启用了分割隧道，Citrix Gateway 插件将仅通过 VPN 隧道发送到 Citrix Gateway 保护的网络（Intranet 应用程序）的流量。Citrix Gateway 插件不会将发送到未受保护的网络的网络流量发送到 Citrix Gateway。Citrix Gateway 插件启动时，它将

从 Citrix Gateway 获取 Intranet 应用程序列表，并为客户端 PC 的 Intranet 应用程序选项卡上定义的每个子网建立路由。Citrix Gateway 插件检查从用户设备传输的所有数据包，并将数据包中的地址与 Intranet 应用程序列表（VPN 连接启动时创建的路由表）进行比较。如果数据包中的目标地址位于其中一个 Intranet 应用程序中，Citrix Gateway 插件将数据包通过 VPN 隧道发送到 Citrix Gateway。如果目标地址不在定义的 Intranet 应用程序中，则不会对数据包进行加密，然后用户设备使用客户端 PC 上最初定义的默认路由来正确地路由数据包。“启用分割隧道时，Intranet 应用程序会定义截获并通过隧道发送的网络流量”。

有关更多信息，请查看以下链接：

- 分裂隧道

反分裂隧道

Citrix Gateway 还支持反向分割隧道，该隧道定义 Citrix Gateway 不拦截的网络流量。如果将分割隧道设置为反转，则 Intranet 应用程序会定义 Citrix Gateway 不拦截的网络流量。启用反向分割隧道时，指向内部 IP 地址的所有网络流量都会绕过 VPN 隧道，而其他流量则会通过 Citrix Gateway。反向分割隧道可用于记录所有非本地 LAN 流量。例如，如果用户拥有家庭无线网络并使用 Citrix Gateway 插件登录，则 Citrix Gateway 不会拦截发往打印机或无线网络中其他设备的网络流量。

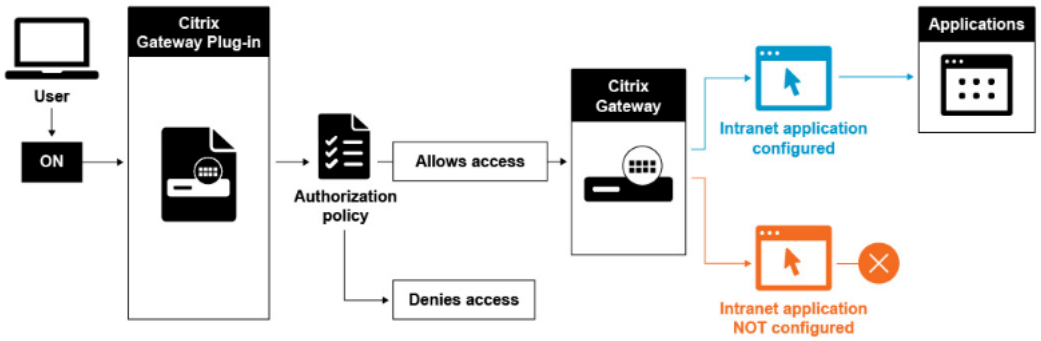
配置分割隧道

1. 从配置实用程序导航到 “配置” 选项卡 >“Citrix Gateway”>“策略”>“会话”。
2. 在详细信息窗格的 “配置文件” 选项卡上，选择一个配置文件，然后单击 “打开”。
3. 在 “客户端体验” 选项卡上，在 “拆分隧道” 旁边，选择 “全局覆盖”，选择一个选项，然后单击 “确定” 两次。

   配置拆分隧道和授权

   在规划 Citrix Gateway 部署时，请务必考虑拆分隧道以及默认授权操作和授权策略。

   例如，您有一个允许访问网络资源的授权策略。您已将隧道拆分设置为开，并且未将 Intranet 应用程序配置为通过 Citrix Gateway 发送网络流量。Citrix Gateway 具有此类配置时，允许访问该资源，但用户无法访问该资源。



如果授权策略拒绝对网络资源的访问，则将隧道拆分设置为 “开”，并且将 Intranet 应用程序配置为通过 Citrix Gateway 路由网络流量，Citrix Gateway 插件将流量发送到 Citrix Gateway，但对资源的访问将被拒绝。

有关授权策略的详细信息，请查看以下内容：

- 配置授权
- 配置授权策略
- 设置默认全局授权

配置对内部网络资源的网络访问

1. 在配置实用程序中，在 “配置” 选项卡 >“Citrix Gateway”>“资源”>“Intranet 应用程序” 上。
2. 在详细信息窗格中，单击 Add（添加）。
3. 完成允许网络访问的参数，单击创建，然后单击关闭。

当我们不为 VPN 用户设置 Intranet IP 时，用户将流量发送到 Citrix Gateway VIP，然后从那里 NetScaler 构建一个新的数据包到位于内部局域网上的 Intranet 应用程序资源。这个新的数据包将从 SNIP 向 Intranet 应用程序提供。从这里，Intranet 应用程序获取数据包，处理它，然后尝试回复该数据包的源（本例中为 SNIP）。SNIP 获取数据包并将答复发送回发送给发出请求的客户端。有
关更多信息，请查看以下链接：

没有内联网 IP

使用 Intranet IP 时，用户将流量发送到 Citrix Gateway VIP，然后从那里 NetScaler 将客户端 IP 映射到池中的一个配置的 Intranet IP 中。请注意，NetScaler 将拥有 Intranet IP 池，因此不应在内部网络中使用这些范围。NetScaler 将为传入 VPN 连接分配 Intranet IP，就像 DHCP 服务器所做的那样。NetScaler 为用户将访问的 LAN 上的 Intranet 应用程序构建一个新的数据包。这个新的数据包将从其中一个 Intranet IP 向 Intranet 应用程序提供。从这里，Intranet 应用程序获取数据包，处理它，然后尝试回复该数据包的源（Intranet IP）。在这种情况下，需要将答复数据包路由回到 NetScaler，其中 Intranet IP 所在地（请记住，NetScaler 拥有 Intranet IP 子网）。要完成此任务，网络管理员应该有一条指向 Intranet IP 的路由，指向其中一个剪切（建议将流量指向 SNIP，该 SNIP 保存数据包第一次离开 NetScaler 的路由，以避免任何非对称流量）。

有关更多信息，请查看以下链接：

内联网 IP

配置名称服务解析

在安装 Citrix Gateway 期间，您可以使用 Citrix Gateway 向导配置其他设置，包括名称服务提供程序。名称服务提供商将完全限定的域名 (FQDN) 转换为 IP 地址。在 Citrix Gateway 向导中，您可以配置 DNS 或 WINS 服务器，设置 DNS 查找的优先级以及重试与服务器连接的次数。

运行 Citrix Gateway 向导时，您可以在此时添加 DNS 服务器。您可以使用会话配置文件向 Citrix Gateway 添加其他 DNS 服务器和 WINS 服务器。然后，可以指示用户和组连接到与最初使用向导配置的名称解析服务器不同的名称解析服务器。

在 Citrix Gateway 上配置其他 DNS 服务器之前，请创建一个充当 DNS 服务器进行名称解析的虚拟服务器。

在会话配置文件中添加 DNS 或 WINS 服务器

1. 在配置实用程序中，依次选择 “配置” 选项卡 >“Citrix Gateway”>“策略”>“会话”。
2. 在详细信息窗格的 “配置文件” 选项卡上，选择一个配置文件，然后单击 “打开”。
3. 在 “网络配置” 选项卡上，执行以下操作之一：
   - 若要配置 DNS 服务器，请单击 “DNS 虚拟服务器” 旁边的 “覆盖全局”，选择该服务器，然后单击 “确定”。
   - 若要配置 WINS 服务器，在 WINS 服务器 IP 旁边，单击覆盖全局，键入 IP 地址，然后单击确定。

选择用户访问方法

April 6, 2020

您可以将 Citrix Gateway 配置为通过以下方案提供用户连接：

- 使用 Citrix Workspace 应用程序进行用户连接。Citrix Workspace 应用程序与 StoreFront 或 Web Interface 配合使用，为用户提供对服务器场中已发布应用程序或虚拟桌面的访问权限。Citrix Workspace 应用程序是使用 ICA 网络协议建立用户连接的软件。用户在用户设备上安装 Citrix Workspace 应用程序。当用户在其基于 Windows 或基于 Mac 的计算机上安装 Citrix Workspace 应用程序时，Citrix Workspace 应用程序会包含所有插件，包括用于用户连接的 Citrix Gateway 插件。Citrix Gateway 还支持从 Citrix Workspace 应用程序的 Android 连接和适用于 iOS 的 Citrix Workspace 应用程序的连接。用户可以通过 Citrix Endpoint Management、StoreFront 或 Web Interface 连接到其虚拟桌面和基于 Windows 的 Web 应用程序、移动应用程序和 SaaS 应用程序。
- 使用 Secure Hub 的用户连接。用户可以连接到在 Endpoint Management 中配置的移动、Web 和 SaaS 应用程序。用户在其移动设备（Android 或 iOS）上安装 Secure Hub。当用户登录到 Secure Hub 时，他们可以安装 WorxMail 和 WorxWeb 以及您在 Endpoint Management 中安装的任何其他移动应用程序。Secure Hub、Secure Mail 和 WorxWeb 使用 Micro VPN 技术通过 Citrix Gateway 建立连接。
- 使用 Citrix Gateway 插件作为独立应用程序进行用户连接。Citrix Gateway 插件是用户可以下载并在用户设备上安装的软件。当用户使用插件登录时，用户可以像在办公室一样访问安全网络中的资源。资源包括电子邮件服务器、文件共享和 Intranet 网站。
- 使用无客户端访问的用户连接。无客户端访问为用户提供所需的访问权限，而无需在用户设备上安装 Citrix Gateway 插件或 Citrix Workspace 应用程序等软件。无客户端访问允许连接到有限的 Web 资源集，例如 Outlook Web Access 或 SharePoint、在 Citrix Virtual Apps 上发布的应用程序、Citrix Virtual Apps and Desktops 中的虚拟桌面以及通过 Access Interface 在安全网络中的文件共享。用户通过在 Web 浏览器中输入 Citrix Gateway Web 地址进行连接，然后从选择页面中选择无客户端访问。
- 如果预身份验证或身份验证后扫描失败，则用户连接。此方案称为访问方案回退。访问方案回退允许用户设备在用户设备未通过初始端点分析扫描时，使用 Citrix Workspace 应用程序从 Citrix 网 Citrix Gateway 插件回退到 StoreFront 或 Web Interface。

  如果用户通过 Citrix Workspace 应用程序登录到 Citrix Gateway，则预身份验证扫描将不起作用。Citrix Gateway 建立 VPN 隧道时，身份验证后扫描会起作用。

用户可以使用以下方法下载和安装 Citrix Gateway 插件：

- 使用 Web 浏览器连接到 Citrix Gateway。
- 连接到配置为接受 Citrix Gateway 连接的 StoreFront。
- 使用组策略对象 (GPO) 安装插件。
- 将 Citrix ADC 插件上传到销售服务器。

为用户访问部署 **Citrix Gateway** 插件

April 6, 2020

Citrix Gateway 附带以下插件供用户访问：

- 适用于 Windows 的 Citrix Gateway 插件
- 适用于 Mac 的 Citrix Gateway 插件
- 适用于 Java 的 Citrix Gateway 插件

当用户首次登录 Citrix Gateway 时，他们会从网页下载并安装 Citrix Gateway 插件。用户通过单击基于 Windows 的计算机上的通知区域中的 Citrix Gateway 图标登录。在 Mac OS X 计算机上，用户可以从 Dock 或应用程序菜单登录。如果将 Citrix Gateway 升级到新软件版本，Citrix Gateway 插件会在用户设备上自动更新。

适用于 Java 的 Citrix Gateway 插件可以在任何支持 Java 的用户设备上使用。适用于 Java 的 Citrix Gateway 插件支持大多数基于 TCP 的应用程序，但仅提供适用于 Windows 的 Citrix Gateway 插件或适用于 Mac OS X 的 Citrix Gateway 插件的某些功能。适用于 Java 的 Citrix Gateway 插件提供对您定义的网络资源的有限访问。有关 Java 插件的详细信息，请参阅使用适用于 Java 的 Citrix Gateway 插件进行连接。

使用 **Citrix Workspace** 应用程序 **Updater** 部署 **Citrix Gateway** 插件

还可以使用 Citrix Workspace 应用程序更新程序部署 Citrix Gateway 插件。当用户安装了 Citrix Workspace 应用程序更新程序时，它会自动将用户设备上安装的所有用户插件添加到 Citrix Workspace 应用程序。用户通过打开 Citrix Workspace 应用程序，然后右键单击 Citrix Gateway 插件并单击登录，使用 Citrix Workspace 应用程序登录到 Citrix Gateway 插件。如果将 Citrix Gateway 设备升级到新版本，Citrix Workspace 应用程序中的 Citrix Gateway 插件将自动升级到新版本。

使用 **MSI** 安装程序包部署 **Citrix Gateway** 插件

可以使用 Microsoft Active Directory 基础结构或标准的第三方 MSI 部署工具（例如 Windows Server Update Services）部署 Citrix Gateway 插件。如果您使用支持 Windows 安装程序包的工具，则可以使用任何支持 MSI 文件的工具部署这些程序包。然后，您可以使用部署工具在相应的用户设备上部署和安装软件。

使用集中式部署工具的优势包括：

- 能够遵守安全要求。例如，您可以在不为非管理用户启用软件安装权限的情况下安装用户软件。

- 控制软件版本。您可以同时将软件的更新版本部署到所有用户。
- 可扩展性。集中式部署策略可轻松扩展以支持其他用户。
- 积极的用户体验。您可以部署、测试和解决与安装相关的问题，而无需使用户参与此过程。

如果首选对用户软件安装进行管理控制，且可随时访问用户设备，Citrix 建议使用此选项。

有关详细信息，请参阅从 Active Directory 部署 Citrix Gateway 插件。

确定要部署哪个软件插件

如果 Citrix Gateway 部署不需要用户设备上的任何软件插件，则您的部署将被视为提供无客户端访问。在这种情况下，用户只需要 Web 浏览器访问网络资源。但是，某些功能需要用户设备上的插件软件。

为用户选择 **Citrix Gateway** 插件

April 6, 2020

配置 Citrix Gateway 时，可以选择用户登录的方式。用户可以使用以下插件之一登录：

- 适用于 Windows 的 Citrix Gateway 插件
- 适用于 Mac OS X 的 Citrix Gateway 插件
- 适用于 Java 的 Citrix Gateway 插件

您可以通过创建会话策略，然后将策略绑定到用户、组或虚拟服务器来完成配置。您还可以通过配置全局设置来启用插件。在全局或会话配置文件中，您可以选择 Windows/MAC OS X 或 Java 作为插件类型。当用户登录时，他们将收到全局定义的插件或在会话配置文件和策略中定义的插件。您必须为插件类型创建单独的配置文件。您只能在会话配置文件中选择 Windows/MAC OS X 或 Java。要为 Java 配置 Citrix Gateway 插件，请参阅使用适用于 Java 的 Citrix Gateway 插件进行连接。

全局配置插件

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户端体验”选项卡上，在“插件类型”旁边，选择“Windows/MAC OS X”，然后单击“确定”。

在会话配置文件中为 **Windows** 或 **Mac OS X** 配置插件类型

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 执行以下操作之一：
   - 如果要创建新的会话策略，请在详细信息窗格中单击“添加”。
   - 如果要更改现有策略，请选择一个策略，然后单击“打开”。

3. 创建新配置文件或修改现有配置文件。为此，请执行以下操作之一：
   - 在请求配置文件旁边，单击新建。
   - 在请求配置文件旁边，单击修改。
4. 在“客户端体验”选项卡上，在“插件类型”旁边，单击“覆盖全局”，然后选择 Windows/MAC OS X。
5. 执行以下操作之一：
   - 如果要创建新配置文件，请单击“创建”，在策略对话框中设置表达式，单击“创建”，然后单击“关闭”。
   - 如果您正在修改现有配置文件，请在进行选择后单击“确定”两次。

为 **Windows** 的 **Citrix Gateway** 插件设置拦截模式

如果要为 Windows 配置 Citrix Gateway 插件，则还需要配置拦截模式并将其设置为透明。

1. 在配置实用程序中，单击“配置”选项卡，展开“Citrix Gateway”>“资源”，然后单击“Intranet 应用程序”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“名称”中，键入策略的名称。
4. 点击透明。
5. 在“协议”中，选择“任何”。
6. 在“目标类型”中，选择“IP 地址和网络掩码”。
7. 在 IP 地址中键入 IP 地址。
8. 在 Netmask 中，键入子网掩码，单击创建，然后单击关闭。

安装适用于 **Windows** 的 **Citrix Gateway** 插件

April 6, 2020

当用户登录到 Citrix Gateway 时，他们将下载并在用户设备上安装 Citrix Gateway 插件。

要安装插件，用户必须是本地管理员或管理员组的成员。此限制仅适用于首次安装。插件升级不需要管理员级别的访问权限。

要使用户能够连接到和使用 Citrix Gateway，您需要向他们提供以下信息：

- Citrix Gateway Web 地址，例如 https://NetScalerGatewayFQDN/
- 如果您配置了终端节点资源和策略，则运行 Citrix Gateway 插件的任何系统要求

根据用户设备的配置，您可能还需要提供以下信息：

- 如果用户在其计算机上运行防火墙，则可能需要更改防火墙设置，以便防火墙不会阻止流入或流出与您授予访问权限的资源相对应的 IP 地址的流量。Citrix Gateway 插件可自动处理 Windows XP 中的 Internet 连接防火墙和 Windows XP Service Pack 2、Windows Vista、Windows 7、Windows 8 或 Windows 8.1 中的 Windows 防火墙。
- 希望通过 Citrix Gateway 连接向 FTP 发送流量的用户必须将其 FTP 应用程序设置为执行被动传输。被动传输意味着远程计算机建立到 FTP 服务器的数据连接，而不是建立 FTP 服务器与远程计算机的数据连接。

- 想要跨连接运行 X 客户端应用程序的用户必须在其计算机上运行 X 服务器（如 XManager）。
- 安装了 Receiver for Windows 或 Receiver for Mac 的用户可以从 Receiver 或使用 Web 浏览器启动 Citrix Gateway 插件。向用户提供有关如何通过 Receiver 或 Web 浏览器使用 Citrix Gateway 插件登录的说明。

由于用户使用文件和应用程序，就像他们是组织网络的本地一样，因此您无需重新培训用户或配置应用程序。

要首次建立安全连接，请使用 Web 登录页登录到 Citrix Gateway。Web 地址的典型格式是https://companyname.com。当用户登录时，他们可以在其计算机上下载并安装 Citrix Gateway 插件。

安装适用于 **Windows** 的 **Citrix Gateway** 插件

1. 在 Web 浏览器中，键入 Citrix Gateway 的 Web 地址。
2. 键入用户名和密码，然后单击登录。
3. 选择“网络访问”，然后单击“下载”。
4. 按照说明安装插件。

下载完成后，Citrix Gateway 插件将连接并在基于 Windows 的计算机上的通知区域中显示一条消息。

如果希望用户在不使用 Web 浏览器的情况下连接 Citrix Gateway 插件，则可以将插件配置为在用户右键单击基于 Windows 的计算机上的通知区域中的 Citrix Gateway 图标或从“开始”菜单启动插件时显示登录对话框。

配置适用于 **Windows** 的 **Citrix Gateway** 插件的登录对话框

要将 Citrix Gateway 插件配置为使用登录对话框，必须登录用户才能完成此过程。

1. 在基于 Windows 的计算机上的通知区域中，右键单击 Citrix Gateway 图标，然后单击配置 Citrix Gateway。
2. 单击配置文件选项卡，然后单击更改配置文件。
3. 在“选项”选项卡上，单击“使用 Citrix Gateway 插件进行登录”。
   注意：如果用户从 Receiver 中打开“
   配置 Citrix Gateway”对话框，则“
   选项”选项卡将不可用。

从 **Active Directory** 部署 **Citrix Gateway** 插件

April 6, 2020

如果用户没有在用户设备上安装 Citrix Gateway 插件的管理权限，则可以从 Active Directory 为用户部署该插件。

使用此方法部署 Citrix Gateway 插件时，可以提取安装程序，然后使用组策略部署该程序。此类部署的常规步骤如下：

- 提取 MSI 软件包。
- 使用组策略分发插件。
- 创建分发点。

- 使用组策略对象分配 Citrix Gateway 插件包。
  注意：仅在 Windows XP、Windows Vista、Windows 7 和 Windows 8 上支持从 Active Directory 中分发 Citrix Gateway 插件。

您可以从配置实用程序或 Citrix 网站下载 MSI 软件包。

从配置实用程序下载 **Citrix Gateway** 插件 **MSI** 包

1. 在配置实用程序中，单击下载。
2. 在 Citrix Gateway 插件下，单击“下载适用于 Windows 的 Citrix Gateway 插件”，然后将文件 nsvpnc_setup.exe 保存到您的 Windows 服务器。

   注意：如果未显示“文件下载”对话框，
   请在单击“下载适用于 Windows 的 Citrix Gateway 插件”链接时
   按 CTRL 键。
3. 在命令提示符下，导航到您将 nsvpnc_setup.exe 保存到的文件夹，然后键入：

   nsvpnc_ 设置/c

   这将提取文件 agee.msi。
4. 将提取的文件保存到 Windows 服务器上的文件夹中。

解压缩文件后，您可以使用 Windows 服务器上的组策略来分发该文件。

在启动分发之前，请在 Windows Server 2003、Windows Server 2008 或 Windows Server 2012 上安装组策略管理控制台。有关详细信息，请参阅 Windows 联机帮助。

注意：当您使用组策略发布 Citrix Gateway 插件时，Citrix 建议将包分配给用户设备。MSI 软件包设计为基于每个设备安装。

在可以分发软件之前，请在发布服务器（如 Microsoft Internet 安全和加速 (ISA) 服务器）上的网络共享上创建分发点。

创建分发点

1. 以管理员身份登录到发布服务器。
2. 创建一个文件夹，并在网络上共享该文件夹，具有对需要访问分发包的所有帐户的读取权限。
3. 在命令提示符下，导航到保存提取的文件的文件夹，然后键入：msiexec-agee.msi
4. 在“网络位置”屏幕上，单击“更改”，然后导航到要在其中创建 Citrix Gateway 插件的管理安装的共享文件夹。
5. 单击确定，然后单击安装。

将提取的程序包放在网络共享上后，将程序包分配给 Windows 中的组策略对象。

将 Citrix Gateway 插件成功配置为托管软件包后，下次用户设备启动时会自动安装该插件。

> 注意：安装程序包分配给计算机时，用户必须重新启动计算机。

安装开始时，用户会收到一条消息，提示正在安装 Citrix Gateway 插件。

使用 **Active Directory** 升级和删除 **Citrix Gateway** 插件

April 6, 2020

Citrix Gateway 插件的每个版本都将打包为完整的产品安装，而不是修补程序。当用户登录并且 Citrix Gateway 插件检测到新版本的插件时，插件会自动升级。还可以使用 Active Directory 部署要升级的 Citrix Gateway 插件。

为此，请为 Citrix Gateway 插件创建新的分发点。创建新的组策略对象并为其分配新版本的插件。然后，在新软件包和现有软件包之间创建链接。创建链接后，Citrix Gateway 插件将更新。

从用户设备中删除 **Citrix Gateway** 插件

要从用户设备中删除 Citrix Gateway 插件，请从组策略对象编辑器中删除分配的软件包。

从用户设备中删除插件时，用户会收到一条消息，提示插件正在卸载。

使用 **Active Directory** 对 **Citrix Gateway** 插件安装进行故障排除

September 26, 2019

如果分配的软件包在用户设备启动时无法安装，您可能会在应用程序事件日志中看到以下警告：

无法将更改应用到软件安装设置。软件安装策略应用程序已延迟到下次登录，因为管理员已启用组策略的登录优化。错误是：组策略框架应该在同步前台策略刷新中调用扩展。

此错误是由 Windows XP 中的快速登录优化引起的，其中允许用户在操作系统初始化所有网络组件（包括组策略对象处理）之前登录。某些策略可能需要多个重新启动才能生效。要解决此问题，请禁用 Active Directory 中的快速登录优化。

要解决托管软件的其他安装问题，Citrix 建议使用组策略启用 Windows 安装程序日志记录。

使用适用于 **Java** 的 **Citrix Gateway** 插件进行连接

April 6, 2020

适用于 Java 的 Citrix Gateway 插件可以在任何支持 Java 的用户设备上使用。

> 注意：以下操作系统和 Web 浏览器需要 Java 运行时环境 (JRE) 版本 1.4.2 直到最新版本的 JRE。

- Mac OS X
- Linux
- Windows XP（所有版本）、Windows Vista、Windows 7 和 Windows 8
- Internet Explorer
- Firefox
- Safari 1.2 到最新版本的网页浏览器

适用于 Java 的 Citrix Gateway 插件支持大多数基于 TCP 的应用程序，但仅提供适用于 Windows 的 Citrix Gateway 插件或适用于 Mac OS X 的 Citrix Gateway 插件的部分功能。

用户不需要用户设备上的管理权限即可使用适用于 Java 的 Citrix Gateway 插件。出于安全原因，您可能需要对特定虚拟服务器、组或用户使用此插件版本，而不管使用哪个用户设备。

要将 Citrix Gateway 配置为在用户设备上安装适用于 Java 的 Citrix Gateway 插件，请配置会话策略，然后将其绑定到虚拟服务器、组或用户。

如果用户从运行 Windows 7 的计算机登录，则不会在 Internet 资源管理器中自动设置代理服务器信息。用户必须在运行 Windows 7 的计算机上手动配置代理服务器。

为 **Java** 配置 **Citrix Gateway** 插件

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格中，单击配置文件选项卡。
3. 选择一个会话配置文件，然后单击打开。
4. 在“客户端体验”选项卡上，在“插件类型”旁边，单击“覆盖全局”，选择 Java，然后单击“确定”。

设置拦截模式

创建会话策略后，创建 Intranet 应用程序，为使用适用于 Java 的 Citrix Gateway 插件登录的用户定义拦截模式。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“Citrix Gateway”>“资源”，然后单击“Intranet 应用程序”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“名称”中，键入名称。
4. 点击代理。
5. 在目标 IP 地址中，键入 IP 地址。
6. 在目标端口中，键入端口号。
7. 在源 IP 地址中，键入 IP 地址。
8. 在源端口中，键入端口号，单击创建，然后单击关闭。

如果未指定源 IP 地址和端口号，Citrix Gateway 将自动使用 127.0.0.1 作为 IP 地址，0 作为端口。

更新基于 **Windows** 的计算机上的主机文件

当用户在运行 Windows Vista、Windows 7 或 Windows 8 的计算机上使用适用于 Java 的 Citrix Gateway 插件登录时，TCP Intranet 应用程序的网络流量不会通道。主机文件不会在运行 Vista 和 Windows 7 的计算机上自动更新。您必须将 Intranet 应用程序手动添加到 HOSTS 文件中。

在基于 Windows 的计算机上，您可以在记事本或其他文本编辑器中编辑 HOSTS 文件。如果在记事本中编辑 HOSTS 文件，则必须以管理员身份运行记事本。为适用于 Java 的 Citrix Gateway 插件添加 Intranet 应用程序的映射条目，然后保存该文件。

将 **Citrix Gateway** 插件与 **Citrix Workspace** 应用程序集成

April 6, 2020

Citrix Gateway 支持 Citrix Workspace 应用程序。协调系统由以下组件组成：

- 适用于 Windows 3.4 或更新版本的 Citrix Workspace 应用程序
- 适用于 Mac 的 Citrix Workspace 应用程序
- 适用于 Android 的 Citrix Workspace 应用程序
- 适用于 iOS 的 Citrix Workspace 应用程序
- StoreFront 2.1 或更新版本
- AppController 2.8 及更新版本或 Citrix Endpoint Management 10
- Citrix 更新服务托管在Citrix Web 站点

有关 Citrix Gateway 与 Citrix 产品兼容性的更多信息，请参阅与 Citrix 产品的兼容性。

您可以配置 Citrix Gateway，以便在用户登录到设备时，Citrix Gateway 插件会打开允许单点登录到 Citrix Workspace 应用程序主页的 Web 浏览器。用户可以从主页下载 Citrix Workspace 应用程序。

用户使用 Citrix Workspace 应用登录时，用户连接可以按照以下方式通过 Citrix Gateway 进行路由：

- 直接发送到 Endpoint Management
- 直接到 StoreFront
- 如果您未在 Endpoint Management 中配置 MDX 移动应用程序，请执行 StoreFront 和 Endpoint Management
- 到 Endpoint Management，然后在 Endpoint Management 中配置 MDX 移动应用程序时进行 StoreFront

注意：仅在 AppController 2.0、AppController 2.5、AppController 2.6、App Controller 2.8 和 App Controller 2.9 中支持直接路由到 Endpoint Management 的连接。如果您的网络中部署了 AppController 1.1，则用户连接必须通过 StoreFront 路由。

用户连接如何与 **Citrix Workspace** 应用程序一起工作

April 6, 2020

用户可以从 Citrix Workspace 应用程序连接到以下应用程序、桌面和数据：

- 在 StoreFront 和 Web Interface 中发布的基于 Windows 的应用程序和虚拟桌面
- 通过 Citrix Endpoint Management 访问的 ShareFile 数据

用户可以使用以下任何 Citrix Workspace 应用程序登录：

- 面向 Web 的 Citrix Workspace 应用程序
- 适用于 Windows 的 Citrix Workspace 应用程序
- 适用于 Mac 的 Citrix Workspace 应用程序
- 适用于 iOS 的 Citrix Workspace 应用程序
- 适用于 Android 的 Citrix Workspace 应用程序

用户可以使用 Web 浏览器或通过用户设备上的 Citrix Workspace 应用程序图标使用适用于 Web 的 Citrix Workspace 应用程序登录。

用户使用任何版本的 Citrix Workspace 应用程序登录时，应用程序、ShareFile 数据和桌面将显示在浏览器或 Citrix Workspace 应用程序窗口中。

将 **Citrix Gateway** 插件添加到 **Citrix Workspace** 应用程序

April 6, 2020

在用户设备上安装 Citrix Workspace 应用程序后，用户可以通过 Citrix Workspace 应用程序使用 Citrix Gateway 插件登录。将 Citrix Gateway 插件上传到 Merchandising Server，然后该服务器将该插件下载并安装到用户设备上的 Citrix Workspace 应用程序。如果用户首次安装 Citrix Workspace 应用程序时安装了 Citrix Gateway 插件，则该插件会自动添加到 Citrix Workspace 应用程序中。

将插件交付到用户设备

要将插件交付到用户设备，您必须在销售服务器上上上传和配置 Citrix Gateway 插件。用户进行选择时，插件会从销售服务器下载并安装。

如果用户安装 Citrix Gateway 插件，然后安装 Citrix Workspace 应用程序，则在 Citrix Workspace 应用程序安装完成后，Citrix Gateway 插件将显示在 Citrix Workspace 应用程序菜单中。

如果用户具有适用于 Windows 的 Citrix Workspace 应用程序，则用户可以安装适用于 Windows 的 Citrix Workspace 应用程序更新程序。这是一个可选组件，用于更新插件并与销售服务器进行通信。Citrix Workspace 应用程序包括所有可供交付的插件，包括 Citrix Gateway 插件。有关适用于 Windows 的 Citrix Workspace 应用程序更新程序的详细信息，请参阅 Citrix eDocs 库中的 “Citrix Workspace 应用程序和插件” 部分。

使用 **Citrix Workspace** 应用程序连接到 **Citrix Gateway**

如果用户使用适用于 Windows 的 Citrix Workspace 应用程序连接，他们可以右键单击通知区域中的 Citrix Workspace 应用程序图标，单击“首选项”，然后单击插件状态。如果用户设备上安装了 Citrix Gateway 插件，则用户右键单击 Citrix Gateway 插件，然后单击登录。身份验证成功后，Citrix Gateway 插件将建立与 Citrix Gateway 的连接并建立完整的 VPN 隧道。

用户也可以使用 Web 浏览器登录。用户输入 Citrix Gateway 的完全限定域名 (FQDN) 并登录。Citrix Gateway 建立连接后，用户可以在 Citrix Workspace 作区应用程序的“首选项”>“插件状态”面板上验证连接。

Citrix Gateway Web 地址是在销售服务器上配置的元数据的一部分，用户无法更改该地址。Citrix Gateway 插件启动对 Citrix Gateway 的登录。如果安装在用户设备上的 Windows Citrix Gateway 插件的版本与 Citrix Gateway 设备上的版本不同，则插件会在用户登录时自动降级或升级。适用于 Mac OS X 的 Citrix Gateway 插件不会自动降级。要在 Mac 计算机上安装早期版本的插件，用户必须先卸载 Citrix Gateway 插件，然后从 Citrix Gateway 下载早期版本。

升级或降级 **Citrix Gateway** 插件

在升级或降级 Citrix Gateway 插件期间，设备会删除、下载并安装正确版本的插件。用户可以通过选中 Citrix Workspace 应用程序的“首选项”>“插件状态”面板上的插件条目来确认新安装。Citrix Gateway 插件的新安装版本可能与 Merchandising Server 上配置的版本不同。

将 **Citrix Gateway** 插件添加到销售服务器

您还可以在销售服务器上配置 Citrix Gateway 插件交付，该服务器提供 Web 配置界面，允许您上传 Citrix Gateway 插件 MSI 安装包。在推销服务器上，您可以：

- 指定 Citrix Gateway 插件的版本和元数据。
- 为 Citrix Gateway 设备配置一个或多个 Web 地址。
- 基于操作系统或其他参数关联特定规则以便交付。

> 用户无法在销售服务器上配置的服务器列表中添加或删除服务器，尽管他们可以从 Citrix Workspace 应用程序的“网络设置”面板中的配置列表中选择不同的服务器。

如果您使用的是访问方案回退或负载平衡，则可以配置一组固定的 Citrix Gateway Web 地址，并将推销服务器指定为默认地址。用户从 Citrix Workspace 应用程序菜单中选择“登录”时连接到默认服务器。用户可以在 Citrix Workspace 应用程序中使用 Citrix Workspace 应用程序的“首选项”>“网络设置”面板从提供的列表中选择不同的地址。

用户可以继续使用 Web 浏览器登录到任何 Citrix Gateway。如果用户使用 Web 浏览器登录，Citrix Gateway 插件会自动升级或降级为 Citrix Gateway 上的版本。

以下是将 Citrix Gateway 插件添加到销售服务器的一般步骤。有关特定配置步骤，请参阅 Citrix eDocs 库的“技术”部分中的“销售服务器”。

- 在销售服务器管理员控制台中的“常规”选项卡上配置设置。
- 将 Citrix Gateway 插件添加到销售服务器。
- 为目标平台选择适当的插件版本。Citrix Gateway 插件必须添加到销售服务器的主页，才能显示在“将插件添加到交付”页面中。
- 配置 Citrix Gateway 插件的传输。
- 对标识 Citrix Gateway Web 地址的位置使用友好名称。此名称显示在 Citrix Workspace 应用程序中。您还可以添加其他 Citrix Gateway 设备。
- 指定身份验证类型并自定义 Citrix Workspace 应用程序登录对话框中显示的特定标签，如用户名、密码或个人标识号 (PIN)。
- 为传递添加规则。
- 如果希望规则显示在“将规则添加到传递”页面中，则必须创建规则。
- 安排配送。

解耦 **Citrix Workspace** 应用程序图标

April 6, 2020

使用与 Citrix Workspace 应用程序集成的 Citrix Gateway 插件配置 Citrix Virtual Apps and Desktops 部署时，连接到 VPN 的用户不可见插件的图标。Citrix Gateway 插件图标通常位于 Windows 系统托盘或 Mac OS X 查找器的菜单栏中。此图标是插件设置和控件的界面。对于 Windows 用户，当 Citrix Workspace 应用程序和 Citrix Gateway 插件集成时，Citrix Workspace 应用程序中的“关于”对话框将显示 Citrix Gateway 插件的控件。对于 Mac OS X 用户，集成后没有 Citrix Gateway 插件可用的控件。

某些集成部署可能需要公开插件控件，同时保留基础功能的集成。为此，请使用以下 CLI 命令或 Citrix ADC 配置实用程序任务切换 VPN 客户端的图标集成。

使用命令行设置图标集成

使用以下命令：

```
set vpn parameter [-iconWithReceiver (ON/OFF)]

<!--NeedCopy-->
```

使用配置实用程序设置图标集成

使用 Citrix ADC 配置实用程序：

1. 在 “配置” 选项卡上，导航到 “Citrix Gateway”>“全局设置”。
2. 单击更改全局设置，然后选择客户端体验选项卡。
3. 点击高级设置
4. 选择使用 Citrix Workspace 应用程序显示 VPN 插件图标。

为 **ICA** 连接配置 **IPv6**

April 6, 2020

Citrix Gateway 支持 ICA 连接的 IPv6 地址。与 Web Interface 或 StoreFront 的 IPv6 连接的工作方式与 IPv4 连接相同。当用户使用 Citrix Gateway Web 地址进行连接时，Citrix Gateway 将代理连接到 Web Interface 或 StoreFront。

您可以为部署在一个 DMZ 中或部署在双跃点 DMZ 中的 Citrix Gateway 配置 IPv6。

您可以使用命令行在 Citrix Gateway 上启用 IPv6。您可以使用以下指南：

- 在设备上启用 IPv6。
- 配置子网 IP 地址。
- 设置 DNS 解析顺序。
- 设置 Web Interface 或 StoreFront 网址。
- 将安全票证颁发机构 (STA) 绑定到 Citrix Gateway。

默认情况下，映射的 IP 地址不支持 IPv6 地址。要将用户通信路由到内部网络，您需要创建子网 IP 地址，然后将 Citrix Gateway 配置为使用子网 IP 地址。

如果您在网络中部署多个 IPv6 子网，请在 Citrix Gateway 上为网络中的每个子网创建多个 IPv6 子网 IP 地址。网络路由使用子网 IP 地址将 IPv6 数据包发送到相应的子网。

为 **ICA** 代理配置 **IPv6**

要为 ICA 代理配置 IPv6，请执行以下操作：

1. 通过使用安全外壳 (SSH) 连接（例如从 PuTTY）登录到 Citrix Gateway。
2. 在命令提示符下，键入 enable ns feature IPv6PT。这将启用 IPv6。
3. 在命令提示符下，键入 enable ns mode USNIP。这样可以使用子网 IP 地址。
4. 在命令提示符下，键入：**set dns parameter –resolutionOrder AAAAThenAQuery AThenAAAA-Query OnlyAAAAQuery OnlyAQuery**
5. 在命令提示符下，键入：**set vpn parameter -wihome `http://XD_domain/Citrix/StoreWeb`**。

其中 <XD_domain> 为 StoreFront 的域名或 IP 地址。

例如，**set vpn parameter -wihome** `http://storefront.domain.com/Citrix/StoreWeb`。

或

set vpn parameter -wihome `http://[1000:2000::3000]/Citrix/StoreWeb`

> 如果您使用 IPv6 地址配置此参数，则 IP 地址必须包含在括号中。

在 **Citrix Gateway** 上配置 **Citrix Workspace** 应用程序主页

April 6, 2020

您可以将 Citrix Workspace 应用程序主页配置为全局配置或作为会话配置文件的一部分配置。如果要配置无法通过 Citrix Gateway 识别 StoreFront 的适用于 Web 的 Citrix Workspace 应用程序版本和更早版本的 Citrix Workspace 应用程序，则需要创建两个单独的会话配置文件。Citrix Workspace 应用程序主页字段需要为每个配置文件提供正确的 Web 地址，以便用户能够成功登录。

对于通过 Citrix Gateway 识别 StoreFront 的 Citrix Workspace 应用程序，您可以让适用于 Web 的 Citrix Workspace 应用程序和 Citrix Workspace 应用程序共享配置文件。但是，Citrix 建议您为适用于 Web 的 Citrix Workspace 应用程序配置会话配置文件，并为所有其他 Citrix Workspace 应用程序配置单独的会话配置文件。

全局配置 **Citrix Workspace** 应用程序主页

要局配置 Citrix Workspace 应用程序主页，请执行以下操作：

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“全局 Citrix Gateway 设置”对话框中，单击“已发布应用程序”选项卡。
4. 在 Citrix Workspace 应用程序主页中，键入 Citrix Workspace 应用程序或适用于 Web 的 Citrix Workspace 应用程序主页的 Web 地址，然后单击“确定”。

在会话配置文件中配 **Citrix Workspace** 应用程序主页

要在会话配置文件中配置 Citrix Workspace 应用程序主页，请执行以下操作：

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway >** 策略，然后单击会话。
2. 在详细信息窗格中的 配置文件选项卡上，单击 添加。
3. 在“创建 **Citrix Gateway** 会话配置文件”对话框中的“已发布应用程序”选项卡上，单击 **Citrix Receiver** 主页旁边的“覆盖全局”。

4. 在 Citrix Workspace 应用程序主页中，键入 Citrix Workspace 应用程序或适用于 Web 的 Citrix Workspace 应用程序主页的 Web 地址，然后单击创建。

将 **Receiver** 主题应用到登录页面

April 6, 2020

您可以使用配置实用程序将 Receiver 主题应用到 Citrix Gateway 的登录页面。您可以在 Receiver 主题、默认主题或您创建的自定义主题之间切换。此功能可用于以下 Citrix Gateway 版本：

- Citrix Gateway 10.1 或更新版本。
- Access Gateway 10 Build 71.6014.e
- Access Gateway 10 Build 73.5002.e

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“全局 Citrix Gateway 设置”对话框中，单击“客户端体验”选项卡。
4. 在 UI 主题旁边，单击绿色气泡，然后单击确定。

   此命令使用 Receiver 主题覆盖原始登录页。注意：应用其他主题后，建议用户清除浏览器缓存以防止缓存页面出现。

为登录页创建自定义主题

April 6, 2020

您可以使用配置实用程序为 Citrix Gateway 的登录页创建自定义主题。您还可以保留默认主题或使用 Citrix Workspace 应用程序主题。选择将自定义主题应用到登录页时，可以使用 Citrix Gateway 命令行创建和部署主题。然后，您可以使用配置实用程序来设置自定义主题页。

您可以使用 Citrix Gateway 全局设置配置自定义主题页。

您可以将此功能与以下版本的 Citrix Gateway 结合使用：

- Citrix Gateway 10.1
- Access Gateway 10 Build 73.5002.e（您必须在构建 71.6104.e 之后安装此版本才能将此功能与 AppController 版本 2.5、2.6 或 2.8 一起使用）
- Access Gateway 10 Build 71.6104.e

使用命令行创建和部署自定义主题

T0 使用命令行创建和部署自定义主题：

1. 登录到 Citrix Gateway 命令行。
2. 在命令提示符下，键入 shell。
3. 在命令提示符下，键入 mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme.tar.g
   ns_gui/*。
4. 使用配置实用程序切换到自定义主题，然后在 /var/ns_gui_ 自定义/ns_gui/VPN 下进行自定义更改。可以执行以下操作：
   - 对 css/ctx. 身份验证.css 文件进行编辑。
   - 将自定义徽标复制到 /var/ns_gui_ 自定义/ns_gui/vpn/媒体文件夹。注意：您可以使用 WinSCP 传输文件。
5. 如果您有多个 Citrix Gateway 设备，请对所有设备重复步骤 3 和 4。

自定义用户门户

January 10, 2023

为 VPN 用户提供门户服务的 Citrix Gateway 安装包括选择门户主题的选项，以便为门户页面创建自定义外观和感觉。您可以从提供的一组主题中进行选择，也可以使用主题作为模板来构建自定义或品牌门户。使用配置实用程序，您可以通过添加新徽标、背景图像、自定义输入框标签和基于 CSS 的门户设计的各种其他属性来修改主题。内置门户主题包括五种语言的内容：英语、法语、西班牙语、德语和日语。不同的用户以不同的语言提供服务，具体取决于其 Web 浏览器报告的区域设置。

您可以选择创建自定义最终用户许可协议 (EULA)，该协议在允许 VPN 用户登录之前提供给他们。EULA 功能支持特定于区域设置的 EULA 版本，这些版本基于 Web 浏览器报告的区域设置提供给用户。

门户主题和 EULA 配置都可以在 VPN 虚拟服务器和 VPN 全局级别独立绑定。

> 重要提示： Citrix 不支持需要修改代码的自定义，也不支持解决除恢复到默认主题之外的问题。

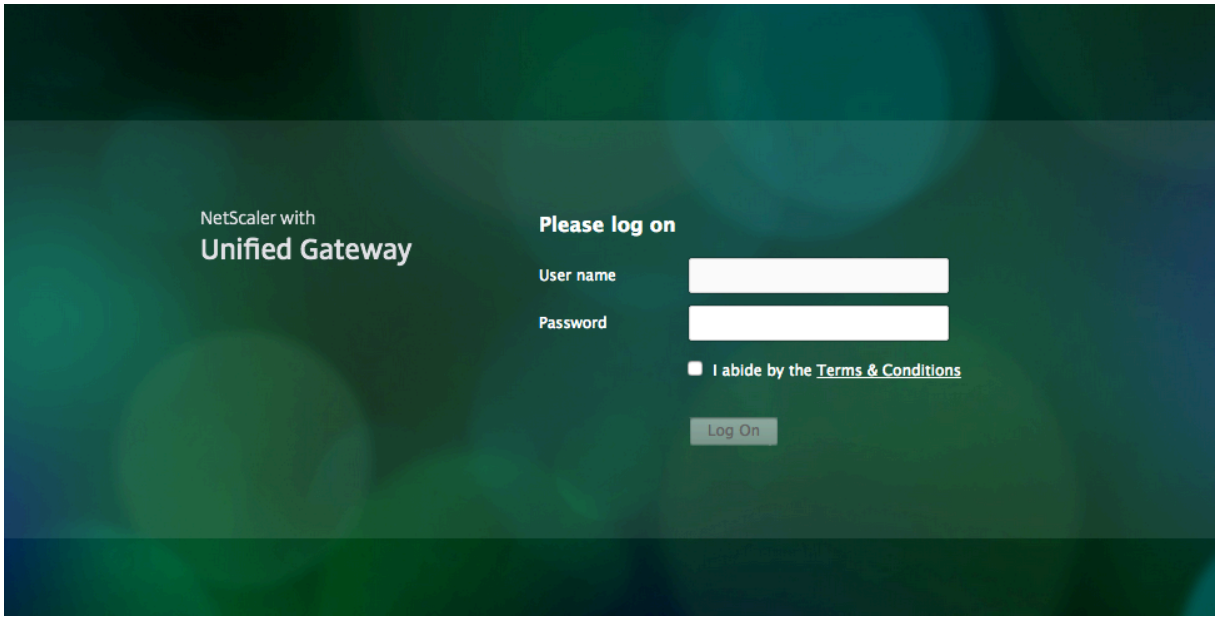
应用门户主题

默认情况下，VPN 门户配置为使用 Caxton 主题。卡克斯顿主题名为默认值。

卡克斯顿主题

Citrix Gateway 包括可应用于门户的两个附加主题：绿色泡沫主题和 X1 主题。

绿泡主题



X1 主题

您可以将提供的任何主题直接应用到 VPN 虚拟服务器或作为全局 VPN 绑定。

将门户主题绑定到 **VPN** 虚拟服务器

您可以在现有虚拟服务器上或创建新虚拟服务器时绑定门户主题。

使用命令行将门户主题绑定到现有 **VPN** 虚拟服务器

在命令提示符下，键入;

```
bind vpn vserver <name> - portaltheme <name>
<!--NeedCopy-->
```

使用配置实用程序将门户主题绑定到现有 **VPN** 虚拟服务器

1. 在配置选项卡上，导航到 **Citrix Gateway**，然后单击虚拟服务器。
2. 选择一个虚拟服务器，然后单击 编辑。
3. 如果门户主题尚未绑定到虚拟服务器，请在详细信息窗格中的“高级设置”下单击“门户主题”。否则，“门户主题”选项已在详细信息窗格中展开。
4. 在详细信息窗格的 门户主题下，单击 无门户主题以展开门户主题绑定窗口。
5. 单击“单击”以选择。
6. 在 门户主题窗口中，单击主题名称，然后单击 选择。
7. 单击 **Bind**（绑定）。
8. 单击完成。

如果您正在创建 VPN 虚拟服务器，则可以在 VPN 虚拟服务器编辑窗格中按照上述步骤从步骤 3 开始绑定门户主题。

将门户主题绑定到 **VPN** 全局

使用命令行将门户主题绑定到 **VPN** 全局范围

在命令提示符下，键入;

```
bind vpn global portaltheme <name>
<!--NeedCopy-->
```

使用配置实用程序将门户主题绑定到 **VPN** 全局范围

1. 在“配置”选项卡上，导航到 **Citrix Gateway**。
2. 在主详细信息窗格中，单击 **Citrix Gateway** 策略管理器。
3. 点击“**+**”图标。
4. 在“绑定点”列表中，选择“资源”。
5. 在“连接类型”列表中，选择“门户主题”。
6. 单击继续。

7. 在“绑定点”屏幕中，单击“添加绑定”。
8. 单击“单击”以选择。
9. 在 门户主题窗口中，单击主题名称，然后单击 选择。
10. 单击 **Bind**（绑定）。
11. 单击关闭。
12. 点击 完成。

> 提示：完成一组更改后，请使用命令行上的“save ns config”命令，或单击配置实用程序中的保存图标，以确保您的更改保存到 Citrix ADC 配置文件中。

创建门户主题

要创建自定义门户设计，请使用提供的门户主题之一作为模板。系统使用您指定的名称创建所选模板主题的副本。

使用股票门户主题作为自定义门户主题的模板

要创建门户主题，可以使用配置实用程序或命令行创建主题实体。但是，详细的自定义控件仅在配置实用程序中可用。

使用命令行创建门户主题

在命令提示符下，键入;

```
add portaltheme <name> basetheme <name>
<!--NeedCopy-->
```

使用配置实用程序创建门户主题

1. 在配置选项卡上，导航到 **Citrix Gateway**，然后单击门户主题。
2. 在主详细信息窗格中，单击 添加。
3. 输入主题的名称，然后从模板列表中选择一个模板，然后单 击确定。
4. 此时，您将看到门户主题编辑窗口的首次视图。点击 确定退出。

您可以继续使用首次视图自定义新门户主题。但是，在继续编辑门户主题之前，您应该阅读以下有关界面的 [门户主题定制 (#portal-theme-customization)] 部分以及界面内自定义门户属性的弹出说明。

创建新主题后，您可以按照 [将门户主题绑定到 VPN 虚拟服务器 (#binding-a-portal-theme-to-a-vpn-virtual-server)] 或中的描述绑定它 [将门户主题绑定到 VPN 全局 (#binding-a-portal-theme-to-vpn-global)]。您可以在创建后或完成自定义项后立即绑定新主题。

门户主题定制

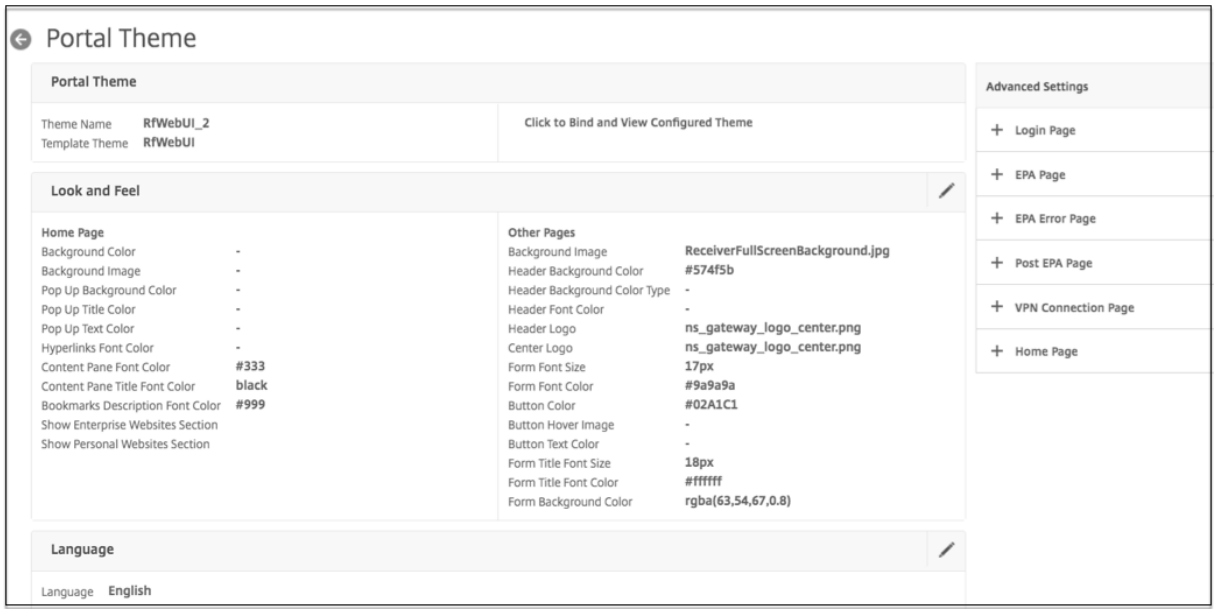
要自定义门户主题，请使用配置实用程序中的门户主题界面。为了获得最佳效果，您应该先了解此界面的各种元素，然后再使用它。

关于门户主题界面

要在 Citrix Gateway 配置实用程序中打开门户主题界面，请在配置选项卡上，导航到 **Citrix Gateway**，然后单击门户主题。您可以按照“创建 门户主题”中的描述创建主题，也可以在主详细信息窗格中选择现有主题，然后单击“编辑”。

门户主题自定义页面包含四个用于修改门户设计的主要组件窗格：“门户主题”窗格、“外观和感觉”窗格、“高级设置”窗格和“语言”窗格。

门户主题界面



页面顶部的“门户主题”窗格报告要加载的主题以及它所基于的模板主题。此处的查看选项允许您查看自定义项，而无需使用用户连接访问 VPN。使用查看选项需要将主题绑定到 VPN 虚拟服务器，并且绑定在查看窗口关闭后仍然有效。

使用页面中心的“查看和感觉”窗格，您可以配置主题的常规属性，例如标题、背景颜色和图像、字体属性和徽标。当此窗格处于编辑模式时，属性图例可用于指导门户页面上使用“外观和感觉”属性的位置。

“高级设置”窗格包含各个门户页面的屏幕内容控件。要加载页面内容以进行编辑，请单击列出的页面之一。然后，页面控件将在其他中心窗格下方打开。只要页面尚未修改，页面会在“高级设置”窗格中跨门户主题编辑内容保持折叠状态。

在“语言”窗格中，可以选择从“高级设置”窗格中选择要编辑的页面时将加载哪些语言。默认情况下会加载英文页面。

可自定义页面属性的类型

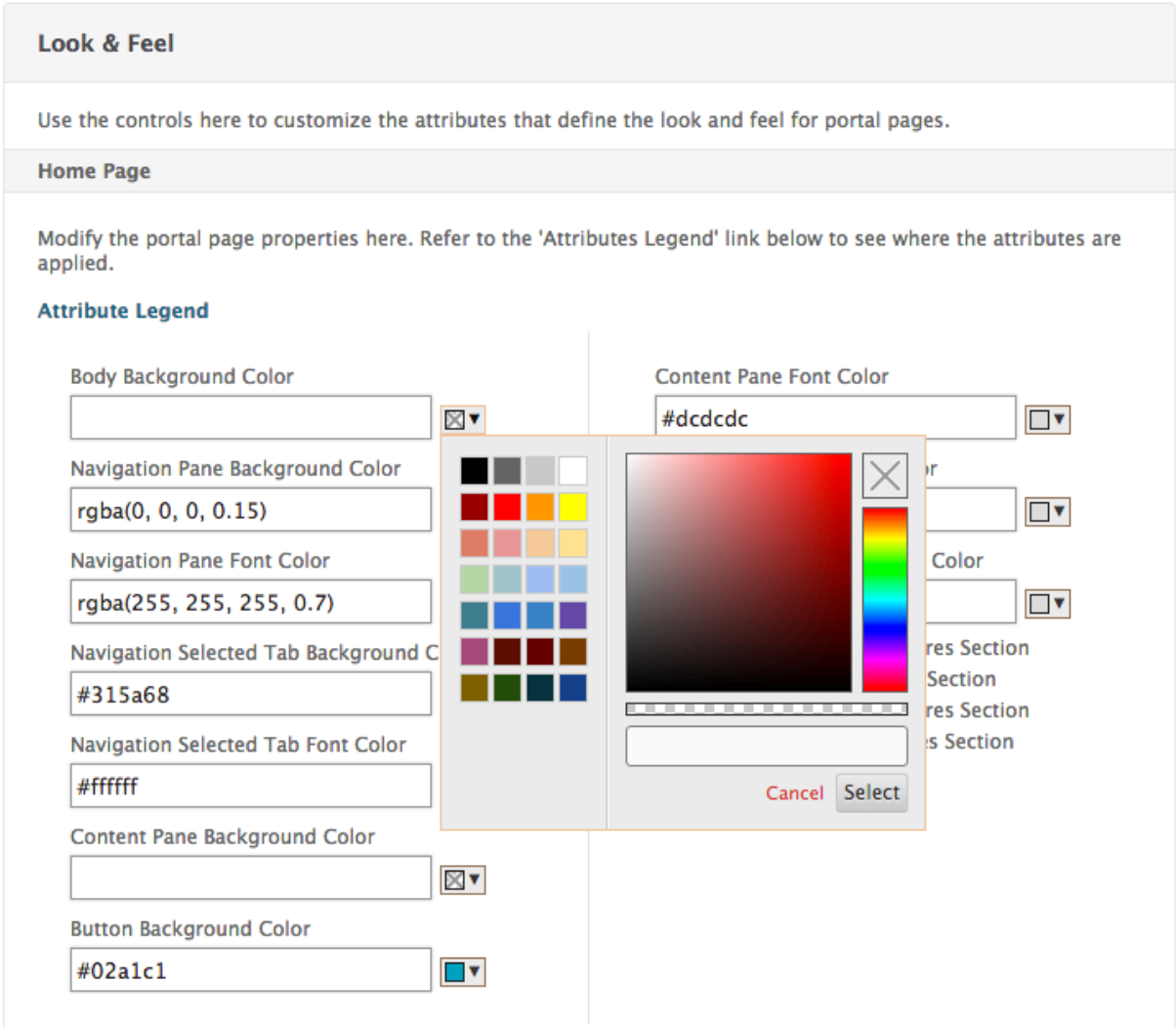
自定义门户主题时，您可以在门户主题界面中修改一系列属性。除了可以编辑的文本和支持的语言外，门户布局的所有图形元素都可以根据您的需求量身定制。每个页面元素类型都有参数或建议，在修改它们之前需要考虑。

颜色

门户设计指定属性的颜色，例如页面背景、高亮、标题和正文内容的文本、按钮控件和悬停响应。要自定义颜色属性，可以直接为选定项目输入颜色值，也可以使用提供的颜色选择器生成颜色值。该界面支持以 RGBA 格式、HTML 十六进

制三重格式和 X11 颜色名称输入有效的 HTML 颜色值。通过单击属性输入字段旁边的颜色框，可以访问任何适用颜色属性的颜色选择器。

拾色器



字体

除了字体颜色外，您还可以修改某些页面属性的字体大小。对于这些属性中的每个属性，菜单提供每个属性的可用大小，具体取决于入口设计。

影像

对于图像，可用于每个控件的弹出描述提供尺寸建议和其他要求。描述根据属性在页面上的位置及其功能而有所不同。您可以使用 PNG 或 JPEG 图像文件格式。您可以选择要上传的图像，方法是选中项目文件名下方的复选框，然后浏览到图像位于本地计算机驱动器上的位置。

标签

在“高级设置”部分，您可以选择要修改的特定门户页面文本。如果您修改页面的默认英文文本，则不会重新翻译其他语言的文本。为方便起见，提供替代语言页面内容，但需要手动更新任何自定义设置。要编辑页面的其他语言版本，请先折叠窗口（如果窗口处于打开状态），方法是单击打开的门户页面的 **X** 图标。然后在“语言”窗格中选择 语言，然后单击“确定”。然后，从“高级设置”窗格打开的所有门户页面都将使用该语言，直到您选择另一个门户页面为止。

> 重要
>
> 在高可用性或群集部署中，门户主题只有分别在主要或配置协调器 Citrix ADC 实体上进行门户主题设置时，才会在共享配置中分发。

关于旧门户自定义的注意事项

对于使用在 11.0 之前的 Citrix Gateway 或 Access Gateway 版本中创建的手动修改的自定义门户设计的安装，Citrix 强烈建议在自定义界面中使用新的门户主题开始。如果你不能这样做，你可以手动应用自定义，但不提供直接支持。

使用手动自定义门户时，必须将自定义门户设置为全局门户配置。但这样做意味着 不能使用 VPN 虚拟服务器级门户主题绑定覆盖应用的全局门户配置。在这种情况下，尝试使用配置实用程序或命令行创建 VPN 虚拟服务器绑定将返回错误。

此外，在高可用性和群集配置的情况下，必须在部署中的每个节点上执行任何手动自定义，因为 Citrix ADC 文件系统上的基础文件不会在自动共享的配置中分发。

手动创建自定义门户配置

要在升级到 Citrix Gateway 11.0 后手动应用较旧的自定义门户配置，您需要修改现有门户页面的副本，将自定义门户文件放入 Citrix ADC 文件系统中，然后选择“自定义”作为 **UIVEM** Y 参数。

您可以使用 WinSCP 或任何其他安全复制程序将文件传输到 Citrix ADC 文件系统。

1. 登录到 Citrix Gateway 命令行。
2. 在命令提示符下，键入 **shell**
3. 在命令提示符下，键入 **mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme ns_gui/***。
4. 在命令提示符下，键入 **cd /var/netscaler/logon/themes/**
   - 如果要自定义绿泡主题，请输入 **cp-r** 绿泡自定义以复制绿泡主题。
   - 如果要自定义默认主题（卡克斯顿），请键入 **cp-r** 默认自定义。
   - 若要自定义 X1 主题，请键入 **cp-r X1** 自定义。
5. 对 **/var/netscaler/logon/themes/Custom** 下的复制的文件进行必要的更改以手动自定义主题。
   - 对 **css/base.css** 进行必要的编辑。
   - 将任何自定义图像复 制到 **/var/ns_gui_** 自定义**/ns_gui/vpn/**媒体目录。
   - 对 资源**/** 目录中存在的文件中的标签进行更改。这些文件对应于门户支持的区域设置。
   - 如果还需要更改 HTML 页面或 JavaScript 文件，您可以使与 **/var/ns_gui_** 定义**/ns_ns_gui/**中的文件相关。

6. 完成所有自定义更改后，在提示符处输入：**tar —cvzf /var/ns_gui_** 定制/自定义**.tar.gz /var/ns_gui_** 定制**/ns_gui/***

> 重要
>
> 在上述步骤中复制主题目录时，复制的文件夹名称必须完全按照“自定义”输入，因为目录名称在 Citrix ADC 外壳界面中区分大小写。如果目录名称未精确输入，则当 **UIVEME** 设置配置为自定义时，无法识别该文件夹。

选择自定义主题作为 **VPN** 全局参数

手动自定义的门户配置完成并复制到 Citrix ADC 文件系统后，需要将其应用于 Citrix Gateway 配置。这可以通过将 UIVEMY 参数设置为自定义来完成，并且可以使用命令行或配置实用程序完成。

要使用命令行，请输入以下命令来设置 **UIVEMY** 参数。

```
1 set vpn parameter UITHEME CUSTOM
2 <!--NeedCopy-->
```

要使用配置实用程序设置 UIVEME 参数，请使用以下过程。

1. 在配置选项卡上，导航到 **Citrix Gateway >** 全局设置。
2. 点击 更改全局设置。
3. 单击 客户体验选项卡。
4. 滚动到屏幕底部，然后从 ****UI** 主题列表菜单中选择自定义 ** 。
5. 单击确定。

您的手动自定义门户现在是向 VPN 用户提供的门户设计。

创建最终用户许可协议

VPN 门户系统提供了将最终用户许可协议 (EULA) 应用于门户配置的选项。一旦 EULA 绑定到 Citrix Gateway 配置（无论是在 VPN 全局范围内还是绑定到相关 VPN 虚拟服务器），VPN 用户必须同意 EULA 作为条款和条件，然后才能允许他们对 VPN 进行身份验证。

与门户主题一样，根据 Web 浏览器报告的区域设置，为用户提供特定语言的 EULA 服务。如果区域设置与任何支持的语言不匹配，则默认提供的语言为英语。对于每个 EULA，您可以使用每种支持的语言输入自定义消息。预翻译的内容不适用于 EULA 配置，因为它是针对门户主题的。如果用户报告的区域设置与未输入 EULA 内容的语言匹配，则当用户单击 VPN 登录页面上的“条款和条件”链接时，将返回一个空白页面。

要创建 EULA，可以在 **Citrix Gateway >** 全局设置 **> EULA** 或 **Citrix Gateway >** 资源 **> EULA** 的配置选项卡上使用配置实用程序中的任一控件。“全局设置”窗格中的控件用于管理 VPN 全局 EULA 绑定，而“资源**”>“EULA**”节点上的控件用于对 EULA 配置进行常规操作。您可以通过在 **Citrix Gateway >** 虚拟服务器上编辑 VPN 虚拟服务器来管理 VPN 虚拟服务器 EULA 绑定。某些命令还可以随命令行一起使用，用于管理 EULA 实体。但是，完整的 EULA 管理控件仅在配置实用程序中可用。

使用命令行创建 **EULA** 实体

在命令提示符下，键入;

```
add vpn eula <name>
<!--NeedCopy-->
```

使用配置实用程序创建 **EULA** 实体

1. 导航到 **Citrix Gateway >** 资源 **> EULA**。
2. 单击“添加”以创建实体。
3. 输入实体的名称。
4. 对于每种语言，粘贴相关选项卡下的内容。您可以使用纯文本或 HTML 标签来设置内容的格式，包括用于添加换行符的标
 签。
5. 单击创建。

创建 EULA 实体后，可以全局绑定到 VPN 配置，也可以绑定到 VPN 虚拟服务器。

使用命令行将 **EULA** 绑定到 **VPN** 全局

在命令提示符下，键入;

```
bind vpn global eula <name>
<!--NeedCopy-->
```

使用配置实用程序进行全局 **EULA VPN** 绑定

1. 在配置选项卡上，导航到 **Citrix Gateway >** 全局设置。
2. 在主详细信息窗格中，单击 配置最终用户许可协议。
3. 单击添加绑定。
4. 单击“单击**”** 以选择。
5. 选择一个 EULA 实体，然后单击 选择。
6. 单击 **Bind**（绑定）。
7. 单击关闭。

使用命令行将 **EULA** 绑定到 **VPN** 虚拟服务器

在命令提示符下，键入;

```
bind vpn vserver <name> eula <name>
<!--NeedCopy-->
```


使用配置实用程序将 **EULA** 绑定到 **VPN** 虚拟服务器

1. 在配置选项卡上，浏览至 **Citrix Gateway >** 虚拟服务器。
2. 在主详细信息窗格中，选择 VPN 虚拟服务器，然后单击 编辑。
3. 从页面右侧的“高级设置”窗格中，单击 **EULA** 。
4. 在新添加的 EULA 窗格中，单击 无 **EULA**。
5. 单击“单击**”** 以选择。
6. 选择一个 EULA 实体，然后单击 选择。
7. 单击 **Bind**（绑定）。
8. 单击完成。

配置无客户端访问

April 6, 2020

无客户端访问允许用户进行所需的访问，而无需安装用户软件（如 Citrix Gateway 插件或 Receiver）。用户可以使用其 Web 浏览器连接到 Web 应用程序，例如 Outlook Web Access。

您可以使用以下步骤配置无客户端访问：

- 全局或使用绑定到用户、组或虚拟服务器的会话策略启用无客户端访问。
- 选择 Web 地址编码方法。

若要仅为特定虚拟服务器启用无客户端访问，请全局禁用无客户端访问，然后创建会话策略以启用该访问。

如果使用 Citrix Gateway 向导配置设备，则可以选择在向导中配置无客户端访问权限。向导中的设置将全局应用。在 Citrix Gateway 向导中，您可以配置以下客户端连接方法：

- Citrix Gateway 插件。仅允许用户使用 Citrix Gateway 插件登录。
- 使用 Citrix Gateway 插件并允许访问方案回退。用户使用 Citrix Gateway 插件登录到 Citrix Gateway。如果用户设备未通过端点分析扫描，则允许用户使用无客户端访问登录。发生这种情况时，用户对网络资源的访问权限有限。
- 允许用户使用 Web 浏览器和无客户端访问登录。用户只能通过使用无客户端访问登录，并接受对网络资源的有限访问。

启用无客户端访问

April 6, 2020

在全局级别上启用无客户端访问时，所有用户都会收到无客户端访问的设置。您可以使用 Citrix Gateway 向导、全局策略或会话策略来启用无客户端访问。

在全局设置或会话配置文件中，无客户端访问具有以下设置：

- 上。启用无客户端访问。如果禁用客户端选择，并且未配置或禁用 StoreFront 或 Web Interface，则用户将使用无客户端访问登录。
- 允许。默认情况下不启用无客户端访问。如果禁用客户端选择，并且未配置或禁用 StoreFront 或 Web Interface，则用户使用 Citrix Gateway 插件登录。如果用户登录时端点分析失败，用户将收到可用无客户端访问的选择页。
- 关闭。关闭无客户端访问。选择此设置时，用户无法使用无客户端访问登录，并且无客户端访问图标不会显示在选择页上。

注意：如果您使用命令行界面配置无客户端访问，则选项为“开”、“关”或“禁用”。

如果未使用 Citrix Gateway 向导启用无客户端访问，则可以使用配置实用程序在全局或在会话策略中启用该向导。

启用全局无客户端访问

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户端体验”选项卡上的“无客户端访问”旁边，选择“开”，然后单击“确定”。

使用会话策略启用无客户端访问的步骤

如果只希望选定的一组用户、组或虚拟服务器使用无客户端访问，请在全局禁用或关闭无客户端访问。然后，使用会话策略启用无客户端访问并将其绑定到用户、组或虚拟服务器。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在“客户端体验”选项卡上，在“无客户端访问”旁边，单击“覆盖全局”，选择“开”，然后单击“创建”。
7. 在“创建会话策略”对话框的命名表达式旁边，选择“常规”，选择“True”，单击“添加表达式”，单击“创建”，然后单击“关闭”。
8. 单击 Create（创建），然后单击 Close（关闭）。

创建启用无客户端访问的会话策略后，将其绑定到用户、组或虚拟服务器。

对网址进行编码

April 6, 2020

启用无客户端访问时，您可以选择对内部 Web 应用程序的地址进行编码，或将地址保留为明文。设置如下：

- 模糊不清这使用标准编码机制来掩盖资源的域和协议部分。
- 清除。Web 地址未编码，对用户可见。
- 加密。域和协议通过使用会话密钥进行加密。对 Web 地址进行加密时，同一 Web 资源的每个用户会话的 URL 会不同。如果用户将编码的 Web 地址添加书签，请将其保存在 Web 浏览器中，然后注销，当用户登录并尝试使用书签再次连接到 Web 地址时，他们将无法连接到 Web 地址。
  注意：如果用户在会话期间将加密的书签保存在 Access 界面中，则每次用户登录时书签都会起作用。

您可以在全局配置此设置，也可以作为会话策略的一部分配置此设置。如果将编码配置为会话策略的一部分，则可以将其绑定到用户、组或虚拟服务器。

全局配置 **Web** 地址编码

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户端体验”选项卡上，在“无客户端访问 URL 编码”旁边，选择编码级别，然后单击“确定”。

通过创建会话策略来配置 **Web** 地址编码

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在“客户端体验”选项卡上，在“无客户端访问 URL 编码”旁边，单击“覆盖全局”，选择编码级别，然后单击“确定”。
7. 在“创建会话策略”对话框的命名表达式旁边，选择“常规”，选择“True”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

无客户端访问策略的工作原理

April 6, 2020

您可以通过创建策略来配置对 Web 应用程序的无客户端访问权限。您可以在配置实用程序中配置无客户端访问策略的设置。无客户端访问策略由规则和配置文件组成。您可以使用 Citrix Gateway 附带的预配置无客户端访问策略。您还可以创建自己的自定义无客户端访问策略。

Citrix Gateway 为以下内容提供了预配置的策略：

- Outlook Web Access 和 Outlook Web App
- SharePoint 2007
- 所有其他 Web 应用程序

请记住预配置的无客户端访问策略的以下特征：

- 它们是自动配置的，无法更改。
- 每个策略都在全球范围内受到约束。
- 除非您在全局或通过创建会话策略启用无客户端访问，否则不会强制执行每个策略。
- 即使您不启用无客户端访问，也无法删除或修改全局绑定。

对其他 Web 应用程序的支持取决于您在 Citrix Gateway 上配置的重写策略级别。Citrix 建议测试您创建的任何自定义策略，以确保应用程序的所有组件都成功重写。

如果您允许从 Receiver for Android、Receiver for iOS 或 WorxHome 进行连接，则必须启用无客户端访问。对于在 iOS 设备上运行的 WorxHome，您还必须在会话配置文件中启用安全浏览。安全浏览和无客户端访问协同工作，以允许从 iOS 设备进行连接。如果用户未连接 iOS 设备，则无需启用安全浏览。

快速配置向导会为移动设备配置正确的无客户端访问策略和设置。Citrix 建议运行 “快速配置” 向导，以配置适用于与 StoreFront 和 Citrix Endpoint Management 的连接的正确策略。

您可以将自定义无客户端访问策略全局绑定或绑定到虚拟服务器。如果要将无客户端访问策略绑定到虚拟服务器，则需要创建新的自定义策略，然后将其绑定。要为全局或虚拟服务器的无客户端访问强制执行不同的策略，请更改自定义策略的优先级号，使其具有低于预配置策略的数量，从而赋予自定义策略更高的优先级。如果没有其他客户端访问策略绑定到虚拟服务器，则预配置的全局策略优先。

注意：您不能更改预配置的无客户端访问策略的优先级号。

创建新的无客户端访问策略

April 6, 2020

如果要使用与默认无客户端访问策略相同的设置，但要将策略绑定到虚拟服务器，则可以复制默认策略，为策略提供新名称。您可以使用配置实用程序复制默认策略。

将新策略绑定到虚拟服务器后，您可以设置策略的优先级，以便在用户登录时首先执行策略。

使用默认设置创建新的无客户端访问策略

1. 在配置实用程序中的导航窗格中，展开 “Citrix Gateway”>“策略”，然后单击 “无客户端访问”。
2. 在详细信息窗格的 “策略” 选项卡上，单击默认策略，然后单击 “添加”。
3. 在 “名称” 中，键入策略的新名称，单击 “创建”，然后单击 “关闭”。

将无客户端访问策略绑定到虚拟服务器

创建新策略后，将其绑定到虚拟服务器。

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway，然后单击 “虚拟服务器”。

2. 在详细信息窗格中，选择虚拟服务器，然后单击“打开”。
3. 在“配置 Citrix Gateway 虚拟服务器”对话框中，单击“策略”选项卡，然后单击“无客户端”。
4. 单击“插入策略”，从列表中选择一个策略，然后单击“确定”。

创建和评估无客户端访问策略表达式

为无客户端访问创建新策略时，您可以为该策略创建自己的表达式。完成表达式创建后，可以评估表达式的准确性。

1. 在配置实用程序中的导航窗格中，展开“Citrix Gateway”>“策略”，然后单击“无客户端访问”。
2. 在详细信息窗格的“策略”选项卡上，单击默认策略，然后单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 配置重写设置，然后单击创建。
7. 在“创建无客户端访问策略”对话框的“表达式”下，单击“添加”。
8. 在“添加表达式”对话框中，创建表达式，然后单击“确定”。
9. 在“创建无客户端访问策略”对话框中，单击“评估”，如果表达式测试为正确，请单击“创建”。

使用 **Citrix Gateway** 进行高级无客户端 **VPN** 访问

April 6, 2020

无客户端 VPN (CVPN) 可以通过 Citrix Gateway 提供对企业内部网络资源的远程访问，而无需在客户端计算机上使用 VPN 客户端应用程序。CVPN 使用客户端的 Web 浏览器提供对企业 Web 应用程序、门户和其他资源的远程访问权限。高级 CVPN 解决方案消除了与 CVPN 有关的以下限制：

- 有时无法识别相对 URL。
- 无法识别动态生成的相对 URL。

高级无客户端 VPN 标识绝对 URL 和主机名称，并以新的唯一方式重写它们，而不是尝试重写 HTTP 响应/网页中存在的相对 URL。SharePoint 不再需要使用默认文件夹来重写 URL，并且支持自定义 SharePoint 访问。

必备条件

以下是配置高级 CVPN 的先决条件。

1. 通配符服务器证书 -VPN 虚拟服务器需要通配符服务器证书。如果服务器托管，`https://vpn.com` 那么服务器证书现在应该有 (`vpn.com` 和 `.vpn.com`) 的条目作为证书 CN 或 SAN 的一部分（其中 CN= 公用名称，SAN = 主题替代名称）。在 Citrix Gateway 上绑定此证书的过程保持不变。

2. 通配符 **DNS** 条目 -s 客户端（Web 浏览器）需要解析高级 CVPN 应用程序的 FQDN。在设置 Citrix Gateway 服务器时，您可以配置要解析的 DNS 条目vpn.com。你需要为 '.' 配置一个子域，以便 '.vpn.com' 现在也解析vpn.com 为。

配置高级无客户端 **VPN** 访问

若要使用命令行界面配置高级无客户端 **VPN** 访问，请在命令提示符下键入：

```
set vpn parameter -clientlessVpnMode ON
set vpn parameter -advancedClientlessVpnMode ENABLED
<!--NeedCopy-->
```

如果会话操作绑定到虚拟服务器，则必须为该会话操作启用 "高级无客户端 VPN 模式" 选项。

示例：

```
set vpn sessionaction SessionActionName -advancedclientlessvpn ENABLED
<!--NeedCopy-->
```

要使用 **Citrix ADC GUI** 配置高级无客户端 **VPN** 访问，请执行以下操作：

1. 在 NetScaler GUI 中，导航到配置 **> Citrix NetScaler >** 全局设置。
2. 在 "全局设置**"** 页上，单击 "更改全局设置"，然后选择 "客户端体验" 选项卡。
3. 在 "客户端体验" 选项卡上的 "无客户端访问" 列表中，单 击 "开"。
4. 在 "客户端体验" 选项卡上的 "高级无客户端 **VPN** 模式" 列表中，单击 "已启用"。

   > 注意：
   >
   > - 如果会话操作绑定到虚拟服务器，则必须为该会话操作启用 "高级无客户端 **VPN** 模式" 选项卡以及 "配置 **Citrix Gateway** 会话配置文件" 页面的 "客户端体验" 选项卡。
   > - 您可以选择 "覆盖全局" 选项来覆盖全局设置。

> 您也可以在会话级别配置高级 CVPN 功能。

注意事项

高级 CVPN 旨在提供对企业 Web 应用程序的访问权限。这些应用程序只有一个 FQDN，用于他们需要的每种资源（JavaScript，CSS，图像等）。由于我们将内部应用程序的完整 FQDN 编码为单八位字节（cvpn），我们失去了子域关系。因此，无论何时使用 CORS 配置企业 Web 应用程序时，有时您可能会在通过高级 CVPN 访问该应用程序时注意到问题。

为用户配置域访问权限

April 6, 2020

如果用户使用无客户端访问进行连接，则可以限制允许用户访问的网络资源、域和网站。您可以使用 Citrix Gateway 向导或全局设置创建包括或排除对域的访问权限的列表。

您可以允许访问所有网络资源、域和网站，然后创建排除列表。排除列表引用了一组不允许用户访问的特定资源。用户无法访问排除列表中的任何域。

您还可以拒绝访问所有网络资源、域和网站，然后创建特定的包含列表。包含列表引用了用户可以访问的资源。用户无法访问列表中未显示的任何域。

注意：如果您为 Citrix Endpoint Management 或 StoreFront 配置了无客户端访问策略，并且用户与 Receiver for Web 连接，则需要允许使用 Receiver for Web 能够访问的域。这是必需的，以便 Citrix Gateway 可以为 StoreFront 和 Endpoint Management 重写网络流量。

使用 **Citrix Gateway** 向导配置域访问

1. 在配置实用程序中，单击配置选项卡，然后在导航窗格中单击 Citrix Gateway。
2. 在详细信息窗格的“入门”下，单击 Citrix Gateway 向导。
3. 单击“下一步”，然后按照向导中的说明操作，直到您到达“配置无客户端访问”页。
4. 单击“为无客户端访问配置域”，然后执行以下操作之一：
    - 要创建排除域的列表，请单击“排除域”。
    - 要创建包含域的列表，请单击“允许域”。
5. 在“域名”下，键入域名，然后单击“添加”。
6. 对要添加到列表中的每个域重复步骤 5，然后在完成后单击确定。
7. 使用 Citrix Gateway 向导继续配置设备。

使用配置实用程序配置域设置

您还可以使用配置实用程序中的全局设置来创建或修改域列表。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格中的“无客户端访问”下，单击“为无客户端访问配置域”。
3. 执行以下操作之一：
    - 要创建排除域的列表，请单击“排除域”。
    - 要创建包含域的列表，请单击“允许域”。
4. 在“域名”下，键入域名，然后单击“添加”。
5. 对要添加到列表中的每个域重复步骤 4，然后在完成后单击确定。

为 **SharePoint 2003**、**SharePoint 2007** 和 **SharePoint 2013** 配置无客户端访问

April 6, 2020

Citrix Gateway 可以重写来自一个或多个 SharePoint 2003 或 SharePoint 2007 或 SharePoint 2013 站点的内容，以便用户可以使用这些内容，而无需使用 Citrix Gateway 插件。要成功完成重写过程，必须使用网络中每个 SharePoint 服务器的主机名配置 Citrix Gateway。

可以使用 Citrix Gateway 向导或配置实用程序配置 SharePoint 站点的主机名。

在 Citrix Gateway 向导中，浏览该向导以配置您的设置。当您访问配置无客户端访问页时，键入 SharePoint 站点的 Web 地址，然后单击添加。

若要在运行 Citrix Gateway 向导后首次添加其他网站或配置 SharePoint，请使用配置实用程序。

使用 **Citrix ADC GUI** 为 **SharePoint** 配置无客户端访问

1. 导航到 **Citrix Gateway** > 全局设置。
2. 在详细信息窗格中的“无客户端访问”下，单击“为 **SharePoint** 配置无客户端访问”。
3. 在 SharePoint 的无客户端访问的 SharePoint 服务器的主机名下，键入 SharePoint 站点的主机名，然后单击添加
4. 对要添加到列表中的每个 SharePoint 站点重复步骤 3，然后在完成后单击确定。

将 **SharePoint** 网站设置为主页

April 6, 2020

如果要将 SharePoint 站点设置为用户的主页，请配置会话配置文件并输入 SharePoint 站点的主机名。

将 **SharePoint** 站点配置为主页

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在客户端体验选项卡上，在主页旁边单击覆盖全局，然后键入 SharePoint 站点的名称。
7. 在无客户端访问旁边，单击覆盖全局，选择打开，然后单击创建。
8. 在“创建会话策略”对话框的命名表达式旁边，选择“常规”，选择“True”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

完成会话策略后，将其绑定到用户、组、虚拟服务器或全局。当用户登录时，他们会看到 SharePoint 网站作为他们的主页。

为 **SharePoint 2007** 服务器启用名称解析

April 6, 2020

SharePoint 2007 服务器将配置的服务器名称作为响应的一部分在各个 URL 中的主机名发送。如果已配置的 SharePoint 服务器名称不是完全限定的域名 (FQDN)，Citrix Gateway 无法使用 SharePoint 服务器名称解析 IP 地址，并且某些用户功能超时并显示错误消息 “-1.1 网关超时”。这些功能可以包括在用户使用无客户端访问登录时检出文件、查看 Workspace 以及上传多个文件。

若要解决此问题，您可以尝试以下操作之一：

- 在 Citrix Gateway 上配置 DNS 后缀，以便 SharePoint 主机名在名称解析之前将其转换为 FQDN。
- 在 Citrix Gateway 上为每个 SharePoint 服务器名称配置本地 DNS 条目。
- 将所有 SharePoint 服务器名称更改为使用 FQDN，例如共享点。内联网域而不是共享点，

配置 **DNS** 后缀

1. 在配置实用程序的配置选项卡上的导航窗格中，展开 DNS，然后单击 DNS 后缀。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在 DNS 后缀中，键入 Intranet 域名作为后缀，单击创建，然后单击关闭。

您可以对要添加的每个域重复步骤 3。

为 **Citrix Gateway** 上的每个 **SharePoint** 服务器名称配置本地 **DNS** 记录

1. 在配置实用程序的导航窗格中，展开 “DNS”>“记录”，然后单击 “地址记录”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在 “主机名” 中，键入 DNS 地址记录的 SharePoint 主机名。
4. 在 IP 地址中，键入 SharePoint 服务器的 IP 地址，单击添加，单击创建，然后单击关闭。

添加 A 记录的主机名不应具有别名记录。此外，设备上不能存在重复的 A 记录。

启用无客户端访问持久性 **Cookie**

April 6, 2020

要访问 SharePoint 的某些功能，例如打开和编辑 SharePoint 服务器上托管的 Microsoft Word、Excel 和 PowerPoint 文档，需要持久 Cookie。

持久性 cookie 保留在用户设备上，并随每个 HTTP 请求一起发送。Citrix Gateway 在将持久 Cookie 发送到用户设备上的插件之前对其进行加密，并在会话存在时定期刷新该 cookie。如果会话结束，cookie 会变得陈旧。

在 Citrix Gateway 向导中，管理员可以在全球范围内启用持久性 Cookie。您还可以创建会话策略以启用每个用户、组或虚拟服务器的持久 Cookie。

以下选项可用于持久性 Cookie：

- 允许启用持久性 cookie，用户可以打开和编辑存储在 SharePoint 中的 Microsoft 文档。
- 拒绝将禁用永久性 Cookie，用户无法打开和编辑存储在 SharePoint 中的 Microsoft 文档。
- 在会话期间，提示用户允许或拒绝持久 Cookie。

如果用户未连接到 SharePoint，则无客户端访问不需要持久 Cookie。

为 **SharePoint** 的无客户端访问配置持久 **Cookie**

April 6, 2020

您可以在全局或作为会话策略的一部分为 SharePoint 的无客户端访问配置持久 Cookie。

在全局配置持久性 **Cookie**

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户端体验”选项卡上，在“无客户端访问永久 Cookie”旁边，选择一个选项，然后单击“确定”。

将持久 **Cookie** 配置为会话策略的一部分

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在“客户端体验”选项卡上，在“无客户端访问永久 Cookie”旁边，单击“覆盖全局”，选择一个选项，然后单击“创建”。
7. 在“创建身份验证策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“True 值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

通过 **Web Interface** 保存无客户端访问的用户设置

April 6, 2020

当用户使用无客户端访问登录并从 Web Interface 注销时，Citrix Gateway 不会转发来自上一个会话的客户端使用的 cookie 集，即使用户多次登录时这些 cookie 是持久性的。您可以使用配置实用程序或命令行将 Cookie 绑定到客户端 Cookie 的模式集，以便在会话之间保留 Web Interface 设置。

使用配置实用程序绑定 **Web Interface** 持久性的 **Cookie**

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“策略”，然后单击“无客户端访问”。
2. 在右窗格的“策略”选项卡上，单击“添加”。
3. 在“创建无客户端访问策略”对话框的“名称”中，键入策略的名称。
4. 在配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在“客户端 Cookie”选项卡上的“客户端 Cookie”中，选择“客户端 Cookie”，然后单击“修改”。
7. 在“配置模式集”对话框的“指定模式”下的“模式”中，输入以下参数：
    - WiUser，然后单击添加。
    - WINGDevice，然后单击添加.
    - WINGSession，然后单击“添加”。
8. 单击确定，然后单击创建。
9. 在“创建无客户端访问策略”对话框中的“表达式”中，键入 true，单击“创建”，然后单击“关闭”。

使用命令行绑定 **Web Interface** 持久性的 **Cookie**

1. 使用安全外壳 (SSH) 连接（如 PuTTY）登录到 Citrix Gateway 命令行。
2. 在命令提示符下，键入 shell。
3. 在命令提示符下，输入以下命令：
    - 绑定策略模式集 ns_cvpn_default_client_cookies WIUser，然后按 ENTER。
    - 绑定策略模式集 ns_cvpn_default_client_cookies WINGDevice，然后按 ENTER。
    - 绑定策略模式集 ns_cvpn_default_client_cookies WINGSession，然后按 ENTER。

配置客户端选择页面

April 6, 2020

您可以将 Citrix Gateway 配置为用户提供多个登录选项。通过配置客户端选择页面，用户可以选择从一个位置登录，具有以下选项：

- 适用于 Windows 的 Citrix Gateway 插件
- 适用于 Mac OS X 的 Citrix Gateway 插件
- 适用于 Java 的 Citrix Gateway 插件
- StoreFront
- Web Interface
- 无客户端访问

用户使用绑定到 Citrix Gateway 或虚拟服务器的证书中的 Web 地址登录到 Citrix Gateway。通过创建会话策略和配置文件，可以确定用户接收的登录选项。根据您配置 Citrix Gateway 的方式，客户端选择页面最多显示三个图标，表示以下登录选项：

- 网络访问。当用户首次使用 Web 浏览器登录 Citrix Gateway，然后选择“网络访问”时，将显示下载页面。当用户单击“下载”时，插件将下载并安装在用户设备上。下载和安装完成后，将显示访问界面。如果您安装了较新版本或还原到较旧版本的 Citrix Gateway，则 Windows 的 Citrix Gateway 插件会静默升级或降级到设备上的版本。如果用户通过使用适用于 Mac 的 Citrix Gateway 插件进行连接，则在用户登录时检测到新设备版本时，该插件将静默升级。此版本的插件不会静默降级。
- Web Interface 或 StoreFront。如果用户选择要登录的 Web Interface，则会显示 Web Interface 页面。然后，用户可以访问其已发布的应用程序或虚拟桌面。如果用户选择 StoreFront 登录，则 Receiver 将打开，用户可以访问应用程序和桌面。
  注意：如果将 StoreFront 配置为客户端选项，则应用程序和桌面不会显示在访问界面的左窗格中。
- 无客户端访问。如果用户选择无客户端访问登录，则会显示访问界面或您的自定义主页。在访问界面中，用户可以导航到文件共享、网站和使用 Outlook Web Access。

如果用户选择适用于 Java 的 Citrix Gateway 插件，则插件将启动，并且用户将登录。不会显示选择页面。

安全浏览允许用户通过 Citrix Gateway 从 iOS 设备进行连接。如果启用安全浏览，则当用户使用 Secure Hub 登录时，安全浏览会禁用客户端选择页。

在登录时显示客户端选择页面

April 6, 2020

启用客户端选择选项后，用户可以在成功对 Citrix Gateway 进行身份验证后使用 Citrix Gateway 插件、Web Interface 、Receiver 或无客户端访问从一个网页登录。登录成功后，用户可以从网页中选择建立连接的方法。您还可以将 Java 的 Citrix Gateway 插件配置为显示在选择页面上。

您可以启用客户端选择，而无需使用终端分析或实施访问方案回退。如果未定义客户端安全表达式，用户将收到 Citrix Gateway 上配置的设置的连接选项。如果用户会话存在客户端安全表达式，并且用户设备无法进行终端分析扫描，则选择页面仅提供使用 Web Interface 的选项（如果已配置）。否则，用户可以使用无客户端访问登录。

您可以通过全局或使用会话配置文件和策略配置客户端选择。

> 重要提示：配置客户端选择时，请勿配置隔离组。未通过端点分析扫描并被隔离的用户设备将被视为通过端点扫描的用户设备。

启用全局客户选择选项

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在客户端体验选项卡上，单击高级设置。
4. 在常规选项卡上，单击客户端选择，然后单击确定。

启用客户端选择作为会话策略的一部分

您还可以将客户端选择配置为会话策略的一部分，然后将其绑定到用户、组和虚拟服务器。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在客户端体验选项卡上，单击高级。
7. 在“常规”选项卡上，在“客户选择”旁边，单击“覆盖全局”，单击“客户选择”，单击“确定”，然后单击“创建”。
8. 在“创建会话策略”对话框的命名表达式旁边，选择“常规”，选择“True”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置客户端选择选项

April 6, 2020

除了通过使用会话配置文件和策略启用客户端选择之外，您还需要为用户软件配置设置。例如，您希望用户使用 Citrix Gateway 插件、StoreFront 或 Web Interface 或无客户端访问登录。您可以创建一个启用所有三个选项和客户端选项的会话配置文件。然后，您创建一个会话策略，表达式设置为 True 值，并附加了配置文件。接下来，将会话策略绑定到虚拟服务器。

在创建会话策略和配置文件之前，您需要为用户创建授权组。

创建授权组

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“Citrix Gateway”>“用户管理”，然后单击“AAA 组”。
2. 在详细信息窗格中，单击 Add（添加）。

3. 在“组名称”中，键入组的名称。
4. 在用户选项卡上，选择用户，单击添加每个用户，单击创建，然后单击关闭。

以下过程是具有 Citrix Gateway 插件、StoreFront 和无客户端访问权限的客户端选择的示例会话配置文件。

为客户端选择创建会话配置文件

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格中，单击配置文件选项卡，然后单击添加。
3. 在“名称”中，键入配置文件的名称。
4. 在“客户端体验”选项卡上，执行以下操作：
   a) 在主页旁边，单击覆盖全局，然后清除显示主页。这将禁用访问接口。
   b) 在无客户端访问旁边，单击覆盖全局，然后选择关。
   c) 在插件类型旁边，单击覆盖全局，然后选择 Windows/MAC OS X。
   d) 单击“高级设置”，然后单击“客户端选择”旁边，单击“覆盖全局”，单击“客户端选择”。
5. 在“安全”选项卡上的“默认授权操作”旁边，单击“覆盖全局”，然后选择“允许”。
6. 在“安全”选项卡上，单击“高级设置”。
7. 在授权组下，单击覆盖全局，单击添加，然后选择组。
8. 在“已发布的应用程序”选项卡上，执行以下操作：
   a) 在 ICA 代理旁边，单击覆盖全局，然后选择关。
   b) 在 Web Interface 地址旁边，单击覆盖全局，然后键入 StoreFront 的 Web 地址，如http://ipAddress/Citrix/。
   c) 在 Web Interface 门户模式旁边，单击覆盖全局，然后选择紧凑。
   d) 在单点登录域旁边，单击覆盖全局，然后键入域的名称。
9. 单击 Create（创建），然后单击 Close（关闭）。

如果要使用适用于 Java 的 Citrix Gateway 插件作为客户端选择，请在“客户端体验”选项卡的“插件类型”中选择 Java。如果选择此选项，则必须配置 Intranet 应用程序并将拦截模式设置为代理。

创建会话配置文件后，创建会话策略。在策略中，选择配置文件，并将表达式设置为 True 值。

要使用 StoreFront 作为客户端选择，还必须在 Citrix Gateway 上配置安全票证颁发机构 (STA)。STA 绑定到虚拟服务器。

> 注意：如果运行 StoreFront 的服务器不可用，则 Citrix Virtual Apps 选项不会显示在选择页面上。

全局配置 **STA** 服务器

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“服务器”下，单击“绑定/取消绑定 STA 服务器”以供安全票证颁发机构使用。
3. 在绑定/取消绑定 STA 服务器对话框中，单击添加。
4. 在配置 STA 服务器对话框的 URL 中，键入 STA 服务器的 Web 地址，然后单击创建。
5. 重复步骤 3 和 4 以添加更多 STA 服务器，然后单击确定。

将 **STA** 绑定到虚拟服务器

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击虚拟服务器，然后单击打开。
3. 在“已发布的应用程序”选项卡上的“安全票证颁发机构”下的“活动”下，选择 STA 服务器，然后单击“确定”

您还可以在“已发布的应用程序”选项卡上添加 STA 服务器。

配置访问方案回退

April 6, 2020

SmartAccess 允许 Citrix Gateway 根据端点分析扫描的结果自动确定允许用户设备的访问方法。访问方案回退通过允许用户设备从 Citrix Gateway 插件回退到 Web Interface 或 StoreFront（如果用 Citrix Workspace 设备未通过初始端点分析扫描），进一步扩展了此功能。

要启用访问方案回退，请配置身份验证后策略，该策略确定用户在登录 Citrix Gateway 时是否收到其他访问方法。此身份验证后策略定义为全局配置或作为会话配置文件的一部分配置的客户端安全表达式。如果配置会话配置文件，则该配置文件将与会话策略相关联，然后将该策略绑定到用户、组或虚拟服务器。启用访问方案回退时，Citrix Gateway 会在用户身份验证后启动终端分析扫描。对于不满足回退身份验证后扫描要求的用户设备，结果如下所示：

- 如果启用了客户端选项，则用户只能使用 Citrix Workspace 应用程序登录到 Web Interface 或 StoreFront。
- 如果禁用了无客户端访问权限和客户端选项，则可将用户隔离到仅提供对 Web Interface 或 StoreFront 的访问权限的组中。
- 如果 Citrix Gateway 上启用了无客户端访问并且 Web Interface 或 StoreFront，并且禁用了 ICA 代理，则用户将回退到无客户端访问。
- 如果未配置 Web Interface 或 StoreFront，并且将无客户端访问设置为允许，则用户将回退到无客户端访问。

禁用无客户端访问时，必须为访问方案回退配置以下设置组合：

- 定义身份验证后退扫描的客户端安全参数。
- 定义 Web Interface 主页。
- 禁用客户端选择。
- 如果用户设备未通过客户端安全检查，则将用户置于隔离组中，该隔离组仅允许访问 Web Interface 或 StoreFront 以及已发布的应用程序。

为访问方案回退创建策略

November 21, 2022

要配置 Citrix Gateway 以进行访问方案回退，您需要通过以下方式创建策略和组：

- 创建一个隔离组，如果终端分析扫描失败，将用户放置在该隔离组中。
- 创建在终端分析扫描失败时使用的全局 Web Interface 或 StoreFront 设置。
- 创建覆盖全局设置的会话策略，然后将会话策略绑定到组。
- 创建在终端分析失败时应用的全局客户端安全策略。

配置访问方案回退时，请使用以下准则：

- 使用客户端选择或访问方案回退需要针对所有用户使用端点分析插件。如果终端分析无法运行，或者用户在扫描期间选择跳过扫描，则将拒绝用户访问。
  注意：在 Citrix Gateway 10.1 Build 120.1316.e 中删除了用于跳过扫描的选项
- 启用客户端选择时，如果用户设备未通过端点分析扫描，则会将用户置于隔离组中。用户可以继续使用 Citrix Gateway 插件或 Citrix Workspace 应用程序登录到 Web Interface 或 StoreFront。
  注意：如果启用客户端选择，Citrix 建议您不要创建隔离组。未通过端点分析扫描并被隔离的用户设备将采用与通过端点扫描的用户设备相同的方式处理。
- 如果终端分析扫描失败，并且用户被置于隔离组中，则仅当没有直接绑定到与绑定到隔离组的策略具有等于或低于绑定到隔离组的策略的用户的策略时，绑定到隔离组的策略才有效。
- 您可以为 Access Interface 和 Web Interface 或 StoreFront 使用不同的 Web 地址。配置主页时，Citrix Gateway 插件的访问接口主页优先，Web Interface 用户优先使用 Web Interface 主页。Citrix Workspace 应用程序主页优先于 StoreFront。

创建隔离组

1. 在配置实用程序中，在 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“用户管理”，然后单击 “AAA 组”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在 “组名称” 中，键入组的名称，单击 “创建”，然后单击 “关闭”。
   重要提示：隔离组的名称不得与用户可能属于的任何域组的名称相匹配。如果隔离组匹配 Active Directory 组名称，即使用户设备通过端点分析安全扫描，也会隔离用户。

创建组后，将 Citrix Gateway 配置为在用户设备无法终端分析扫描时回退到 Web Interface。

将设置配置为隔离用户连接

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway，然后单击 “全局设置”。
2. 在详细信息窗格的 “设置” 下，单击 “更改全局设置”。
3. 在 “全局 Citrix Gateway 设置” 对话框中的 “已发布应用程序” 选项卡上的 ICA 代理旁边，选择 “关”。
4. 在 Web Interface 地址旁边，键入 StoreFront 或 Web Interface 的 Web 地址。
5. 在单点登录域旁边，键入 Active Directory 域的名称，然后单击 “确定”。

配置全局设置后，创建覆盖全局 ICA 代理设置的会话策略，然后将会话策略绑定到隔离组。

创建访问方案回退的会话策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“已发布的应用程序”选项卡上，ICA 代理旁边，单击“覆盖全局”，选择“开”，然后单击“创建”。
6. 在“创建会话策略”对话框的命名表达式旁边，选择“常规”，选择“True”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

创建会话策略后，将策略绑定到隔离组。

将会话策略绑定到隔离组

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“Citrix Gateway”>“用户管理”，然后单击“AAA 组”。
2. 在详细信息窗格中，选择一个组，然后单击打开。
3. 点击会话。
4. 在“策略”选项卡上，选择“会话”，然后单击“插入策略”。
5. 在策略名称下，选择策略，然后单击确定。

在创建启用 Citrix Gateway 上 Web Interface 或 StoreFront 的会话策略和配置文件后，创建全局客户端安全策略。

创建全局客户端安全策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“安全”选项卡上，单击“高级设置”。
4. 在“客户端安全”中，输入表达式。有关配置系统表达式的详细信息，请参阅配置系统表达式和配置复合客户端安全表达式
5. 在隔离组中，选择您在组过程中配置的组，然后单击“确定”两次。

为 **Citrix Gateway** 插件配置连接

April 6, 2020

通过定义用户可以在内部网络中访问的资源来配置用户设备连接。配置用户设备连接包括：

- 定义允许用户访问的域。
- 为用户配置 IP 地址，包括地址池（Intranet IP）。
- 配置超时设置。

- 配置单点登录。
- 配置客户端拦截。
- 配置分割隧道。
- 通过代理服务器配置连接。
- 将用户软件配置为通过 Citrix Gateway 进行连接。
- 配置移动设备的访问权限。

您可以使用属于会话策略一部分的配置文件配置大多数用户设备连接。您还可以使用 Intranet 应用程序、预身份验证和流量策略来定义用户设备连接设置。

注意：Windows VPN 插件和 EPA 插件为其各种操作收集遥测数据。要禁用该功能，请在客户端计算机上执行以下操作。

> 将注册表 “HKLM\Software\Citrix\Secure Access Client\DisableGA” 类型 REG_DWORD 设置为 1。

配置用户会话数

April 6, 2020

您可以配置允许在特定时间点（全局级别或每个虚拟服务器级别）连接到 Citrix Gateway 的最大用户数。当连接到设备的用户数超过您配置的值时，不会在 Citrix Gateway 上创建会话。如果用户数超过允许的数量，用户将收到一条错误消息。

设置全局用户限制

在全局配置用户限制时，该限制将应用于与系统上不同虚拟服务器建立会话的所有用户。当用户会话数达到您设置的值时，无法在 Citrix Gateway 上的任何虚拟服务器上建立新会话。

设置 Citrix Gateway 的默认身份验证类型时，您可以在全局级别设置最大用户数。

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway，然后单击 “全局设置”。
2. 在详细信息窗格的 “设置” 下，单击 “更改身份验证设置”。
3. 在 “全局身份验证设置” 对话框的 “最大用户数” 中，键入用户数，然后单击 “确定”。

设置每个虚拟服务器的用户限制

您还可以将用户限制应用于系统上的每个虚拟服务器。配置每个虚拟服务器的用户限制时，此限制仅适用于与特定虚拟服务器建立会话的用户。与其他虚拟服务器建立会话的用户不受此限制的影响。

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway，然后单击 “虚拟服务器”。
2. 在详细信息窗格中，单击虚拟服务器，然后单击打开。
3. 在 “最大用户” 中，键入用户数，然后单击 “确定”。

配置超时设置

April 6, 2020

您可以将 Citrix Gateway 配置为强制断开连接，如果在指定的分钟数内连接上没有任何活动。在会话超时（断开连接）前一分钟，用户会收到一条警报，指示会话将关闭。如果会话关闭，用户必须重新登录。

有三种超时选项：

- 被迫超时。如果启用此设置，Citrix Gateway 将在超时间隔过后断开会话的连接，而不管用户正在执行什么操作。在超时间隔过后，用户无法采取任何措施来防止断开连接。对于通过 Citrix Gateway 插件、Citrix Workspace 应用程序、Secure Hub 或通过 Web 浏览器连接的用户，强制执行此设置。默认设置为 30 分钟。如果将此值设置为零，则该设置处于禁用状态。
- 会话超时。如果启用此设置，Citrix Gateway 会断开会话，如果在指定的时间间隔内未检测到任何网络活动。对于通过 Citrix Gateway 插件、Citrix Workspace 应用程序、Citrix Secure Hub 或通过 Web 浏览器连接的用户，强制执行此设置。默认超时设置为 30 分钟。如果将此值设置为零，则该设置处于禁用状态。
- 空闲会话超时。如果在指定时间间隔内没有用户活动（例如鼠标、键盘或触摸），Citrix Gateway 插件将终止空闲会话的持续时间。仅对使用 Citrix Gateway 插件连接的用户强制执行此设置。默认设置为 30 分钟。如果将此值设置为零，则该设置处于禁用状态。

> 注意：某些应用程序（如 Microsoft Outlook）会自动将网络流量探测器发送到电子邮件服务器，无需任何用户干预。Citrix 建议您将 “
> 空闲会话超时” 配置为 “
> 会话超时”，以确保用户设备上无人参与的会话在合理的时间内超时。

您可以通过输入介于 1 到 65536 之间的值来为超时间隔指定分钟数来启用上述任何设置。如果启用了多个这些设置，则经过的第一个超时间隔将关闭用户设备连接。

您可以通过配置全局设置或使用会话配置文件来配置超时设置。将配置文件添加到会话策略时，该策略随后绑定到用户、组或虚拟服务器。在全局配置超时设置时，这些设置将应用于所有用户会话。

配置强制超时

April 6, 2020

强制超时会在指定时间后自动断开 Citrix Gateway 插件的连接。您可以在全局或作为会话策略的一部分配置强制超时。

配置全局强制超时

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway，然后单击 “全局设置”。
2. 在详细信息窗格的 “设置” 下，单击 “更改全局设置”。
3. 在 “网络配置” 选项卡上，单击 “高级设置”。

4. 在“强制超时 (min)”中，键入用户可以保持连接的分钟数。
5. 在“强制超时警告 (min)”中，键入用户收到连接将断开连接的警告之前的分钟数，然后单 击“确定”。

在会话策略中配置强制超时

如果要进一步控制谁接收强制超时，请创建会话策略，然后将该策略应用于用户或组。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** > 策略，然后单击“会话”。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在“网络配置”选项卡上，单击“高级”。
7. 在“超时”下，单击“覆盖全局”，并在“强制超时（分钟）”中键入用户可以保持连接的分钟数。
8. 在强制超时警告 (min) 旁边，单击 覆盖全局并键入用户被警告连接将断开连接的分钟数。单击确定两次。
9. 在“创建会话策略”对话框的 命名表达式旁边，选择“常规”，选择“**True**”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置会话或空闲超时

April 6, 2020

您可以使用配置实用程序全局配置会话和客户端超时设置或创建会话策略。创建会话策略和配置文件时，请将表达式设置为
True。

全局配置会话或客户端空闲超时

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户端体验”选项卡上，执行以下一项或两项操作：
   - 在会话超时 (分钟) 中，键入分钟数。
   - 在客户端空闲超时 (分钟) 中，键入分钟数，然后单 击确定。

使用会话策略配置会话或客户端空闲超时设置

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **Citrix Gateway** > 策略，然后单击会话
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在“名称”中，键入策略的名称。

4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在“客户端体验”选项卡上，执行以下一项或两项操作：
   - 在会话超时（分钟）旁边，单击覆盖全局，然后键入分钟数，然后单击 创建。
   - 在客户端空闲超时 (分钟) 旁边，单击 覆盖全局，键入分钟数，然后单击 创建。
7. 在“创建会话策略”对话框的 命名表达式旁边，选择“常 规”，选择“**True**”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

连接到内部网络资源

April 6, 2020

您可以配置 Citrix Gateway 以使用户能够访问内部网络中的资源。如果禁用拆分隧道，则来自用户设备的所有网络流量都会发送到 Citrix Gateway，授权策略将确定是否允许流量通过到内部网络资源。启用拆分隧道时，用户设备只拦截发往内部网络的流量并将其发送到 Citrix Gateway。您可以使用 Intranet 应用程序配置 Citrix Gateway 拦截的 IP 地址。

如果您正在使用适用于 Windows 的 Citrix Gateway 插件，请将拦截模式设置为透明。如果您正在使用适用于 Java 的 Citrix Gateway 插件，请将拦截模式设置为代理。将拦截模式设置为透明时，您可以使用以下方式允许访问网络资源：

- 单个 IP 地址和子网掩码
- 一系列 IP 地址

如果将拦截模式设置为代理，则可以配置目标和源 IP 地址以及端口号。

配置对内部网络资源的网络访问

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，展开“资源”，然后单击“**Intranet 应用程序”**。
2. 在详细信息窗格中，单击 添加。
3. 完成允许网络访问的参数，单击 创建，然后单击 关闭。

配置拆分隧道

April 6, 2020

您可以启用拆分隧道，以防止 Citrix Gateway 插件向 Citrix Gateway 发送不必要的网络流量。

如果不启用拆分隧道，Citrix Gateway 插件将捕获源自用户设备的所有网络流量，并通过 VPN 隧道将流量发送到 Citrix Gateway。

如果启用拆分隧道，Citrix Gateway 插件将仅通过 VPN 隧道发送到 Citrix Gateway 保护的网络的流量。Citrix Gateway 插件不会将发送到未受保护的网络的网络流量发送到 Citrix Gateway。

Citrix Gateway 插件启动时，它将从 Citrix Gateway 获取内部网络应用程序的列表。Citrix Gateway 插件检查从用户设备在网络上传输的所有数据包，并将数据包中的地址与 Intranet 应用程序列表进行比较。如果数据包中的目标地址位于其中一个 Intranet 应用程序中，Citrix Gateway 插件将数据包通过 VPN 隧道发送到 Citrix Gateway。如果目标地址不在已定义的 Intranet 应用程序中，则不会对数据包进行加密，并且用户设备会正确地路由数据包。启用拆分隧道时，Intranet 应用程序会定义被拦截的网络流量。

> 注意：如果用户使用 Citrix Workspace 应用程序连接到服务器场中的已发布应用程序，则无需配置拆分隧道。

Citrix Gateway 还支持反向分割隧道，该隧道定义 Citrix Gateway 不拦截的网络流量。如果将分割隧道设置为反转，则 Intranet 应用程序会定义 Citrix Gateway 不拦截的网络流量。启用反向分割隧道时，指向内部 IP 地址的所有网络流量都会绕过 VPN 隧道，而其他流量则会通过 Citrix Gateway。反向分割隧道可用于记录所有非本地 LAN 流量。例如，如果用户拥有家庭无线网络并使用 Citrix Gateway 插件登录，则 Citrix Gateway 不会拦截发往打印机或无线网络中其他设备的网络流量。

有关 Intranet 应用程序的更多信息，请参阅配置客户端拦截。

配置拆分隧道作为会话策略的一部分。

配置分割隧道

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** 策略，然后单击“会话”。
2. 在详细信息窗格的“配置 文件”选项卡上，选择一个配置文件，然后单击“打开”。
3. 在“客户端体验”选项卡上，在“拆分隧道”旁边，选择“全局覆盖”，选择一个选项，然后单 击“确定”两次。

配置拆分隧道和授权

在规划 Citrix Gateway 部署时，请务必考虑拆分隧道以及默认授权操作和授权策略。

例如，您有一个允许访问网络资源的授权策略。您已将隧道拆分设置为开，并且未将 Intranet 应用程序配置为通过 Citrix Gateway 发送网络流量。Citrix Gateway 具有此类配置时，允许访问该资源，但用户无法访问该资源。

如果授权策略拒绝对网络资源的访问，则将隧道拆分设置为“开”，并且将 Intranet 应用程序配置为通过 Citrix Gateway 路由网络流量，Citrix Gateway 插件将流量发送到 Citrix Gateway，但对资源的访问将被拒绝。

配置客户端拦截

April 6, 2020

您可以使用 Intranet 应用程序为 Citrix Gateway 上的用户连接配置拦截规则。默认情况下，当您在设备上配置系统 IP 地址、映射 IP 地址或子网 IP 地址时，将基于这些 IP 地址创建子网路由。Intranet 应用程序将基于这些路由自动创建，并且可以绑定到虚拟服务器。如果启用拆分隧道，则必须定义 Intranet 应用程序才能发生客户端拦截。

您可以使用配置实用程序配置 Intranet 应用程序。您可以将 Intranet 应用程序绑定到用户、组或虚拟服务器。

如果启用拆分通道并且用户通过 WorxWeb 或 WorxMail 进行连接，则在配置客户端拦截时，必须为 Citrix Endpoint Management 和 Exchange Server 添加 IP 地址。如果不启用拆分隧道，则不需要在 Intranet 应用程序中配置 Endpoint Management 和 Exchange IP 地址。

为 **Citrix Gateway** 插件配置 **Intranet** 应用程序

April 6, 2020

您可以通过定义以下内容来创建用户访问资源的 Intranet 应用程序：

- 一个 IP 地址
- 一系列 IP 地址
- 主机名

在 Citrix Gateway 上定义 Intranet 应用程序时，适用于 Windows 的 Citrix Gateway 插件会拦截发往该资源的用户流量，并通过 Citrix Gateway 发送流量。

配置 Intranet 应用程序时，请考虑以下事项：

- 如果满足以下条件，则无需定义 Intranet 应用程序：
  - 拦截模式设置为透明
  - 用户正在使用适用于 Windows 的 Citrix Gateway 插件连接到 Citrix Gateway
  - 拆分隧道被禁用
- 如果用户使用适用于 Java 的 Citrix Gateway 插件连接到 Citrix Gateway，则必须定义 Intranet 应用程序。适用于 Java 的 Citrix Gateway 插件仅拦截到由 Intranet 应用程序定义的网络资源的流量。如果用户使用此插件连接，请将拦截模式设置为代理。

配置 Intranet 应用程序时，必须选择与用于建立连接的插件软件类型相对应的拦截模式。

注意：您不能为代理和透明拦截配置 Intranet 应用程序。要配置网络资源以供适用于 Windows 的 Citrix Gateway 插件和适用于 Java 的 Citrix Gateway 插件使用，请配置两个 Intranet 应用程序策略并将这些策略绑定到用户、组、虚拟服务器或 Citrix Gateway 全局。

为一个 **IP** 地址创建 **Intranet** 应用程序

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** 资源，然后单击“**Intranet** 应用程序**”**。
2. 在详细信息窗格中，单击 添加。
3. 在“名称”中，键入配置文件的名称。
4. 在“创建 **Intranet** 应用程序”对话框中，选择“透明**”**。
5. 在“目标类型”中，选择“**IP** 地址和 网络掩码**”**。

6. 在“协议”中，选择应用于网络资源的协议。
7. 在 **IP** 地址中，键入 IP 地址。
8. 在 **Netmask** 中，键入子网掩码，单击 创建，然后单击 关闭。

配置 **IP** 地址范围

如果您的网络中有多个服务器（例如 Web、电子邮件和文件共享），则可以配置包含网络资源 IP 范围的网络资源。此设置允许用户访问 IP 地址范围中包含的网络资源。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** 资源，然后单击“**Intranet** 应用程序”。
2. 在详细信息窗格中，单击 添加。
3. 在“名称”中，键入配置文件的名称。
4. 在“协议”中，选择应用于网络资源的协议。
5. 在“创建 Intranet 应用程序”对话框中，选择“透明”。
6. 在“目标类型”中，选择“**IP** 地址范围”。
7. 在“**IP** 开始”中，键入起始 IP 地址，并在“IP 结束”中键入结束 IP 地址，单击“创建”，然后单击“关闭”。

为主机名创建 **Intranet** 应用程序

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** 资源，然后单击“**Intranet** 应用程序”。
2. 在详细信息窗格中，单击 添加。
3. 在“名称”中，键入配置文件的名称。
4. 在“创建 **Intranet** 应用程序”对话框中，选择“透明”。
5. 在 目标类型中，选择 主机名。
6. 在协议中，选择 任何，单击 创建，然后单击 关闭。

注意事项

1. 支持通配符主机名。如果配置了主机名为 *.example.com 的 Intranet 应用程序，则会对 a1.example.com、b2.example.com 等进行通道处理。
2. 基于主机名的 Intranet 应用程序仅在将隧道分割设置为开时才起 作用。
3. 仅 Windows VPN 插件支持基于主机名的内联网应用程序。

为适用于 **Java** 的 **Citrix Gateway** 插件配置内部网络应用程序

April 6, 2020

如果用户使用适用于 Java 的 Citrix Gateway 插件进行连接，则必须配置 Intranet 应用程序并将拦截模式设置为代理。适用于 Java 的 Citrix Gateway 插件使用配置文件中指定的用户设备环回 IP 地址和端口号拦截流量。

如果用户从基于 Windows 的设备进行连接，则适用于 Java 的 Citrix Gateway 插件将尝试通过设置应用程序 HOST 名称来访问配置文件中指定的环回 IP 地址和端口来修改 HOST 文件。用户必须在用户设备上具有主机文件修改的管理权限。

如果用户从非 Windows 设备进行连接，则必须使用 Intranet 应用程序配置文件中指定的源 IP 地址和端口值手动配置应用程序。

为适用于 **Java** 的 **Citrix Gateway** 插件配置 **Intranet** 应用程序

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** 资源，然后单击“**Intranet** 应用程序**”**。
2. 在详细信息窗格中，单击 添加。
3. 在“名称”中，键入配置文件的名称。
4. 点击 代理。
5. 在 目标 **IP** 地址和 目标端口中，键入目标 IP 地址和端口。
6. 在源 **IP** 地址和 源端口下，键入源 IP 地址和端口。

> 注意：您应将源 IP 地址设置为 127.0.0.1 的环回 IP 地址。如果未指定 IP 地址，则使用环回 IP 地址。如果未输入端口值，则使用目标端口值。

配置名称服务解析

April 6, 2020

在安装 Citrix Gateway 期间，您可以使用 Citrix Gateway 向导配置其他设置，包括名称服务提供程序。名称服务提供商将完全限定的域名 (FQDN) 转换为 IP 地址。在 Citrix Gateway 向导中，您可以配置 DNS 或 WINS 服务器，设置 DNS 查找的优先级以及重试与服务器连接的次数。

运行 Citrix Gateway 向导时，您可以在此时添加 DNS 服务器。您可以使用会话配置文件向 Citrix Gateway 添加其他 DNS 服务器和 WINS 服务器。然后，可以指示用户和组连接到与最初使用向导配置的名称解析服务器不同的名称解析服务器。

在 Citrix Gateway 上配置其他 DNS 服务器之前，请创建一个充当 DNS 服务器进行名称解析的虚拟服务器。

在会话配置文件中添加 **DNS** 或 **WINS** 服务器

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** 策略，然后单击“会话**”**。

2. 在详细信息窗格的“配置文件”选项卡上，选择一个配置文件，然后单击“打开”。
3. 在“网络配置”选项卡上，执行以下操作之一：
   - 若要配置 DNS 服务器，请单击“DNS 虚拟服务器”旁边的“覆盖全局”，选择该服务器，然后单 击**“**确定**”**。
   - 若要配置 WINS 服务器，在 WINS 服务器 IP 旁边，单击 覆盖全局，键入 IP 地址，然后单 击确定。

为用户连接启用代理支持

April 6, 2020

用户设备可以通过代理服务器进行连接，以访问内部网络。Citrix Gateway 支持 HTTP、SSL、FTP 和 SOCKS 协议。要为用户连接启用代理支持，请在 Citrix Gateway 上指定设置。您可以指定 Citrix Gateway 上的代理服务器使用的 IP 地址和端口。代理服务器用作所有进一步连接到内部网络的转发代理。

配置用户连接的代理支持

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** ，然后单击“全局设置**”**。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在客户端体验选项卡上，单击高级设置。
4. 在“代理**”** 选项卡上的“代理设置”下，选择“开**”**。
5. 对于协议，键入 IP 地址和端口号，然后单 击确定。

> 注意：如果选择“设备”，则可以配置仅支持安全和不安全的 HTTP 连接的代理服务器。

在 Citrix Gateway 上启用代理支持后，您可以在用户设备上为与协议相对应的代理服务器指定配置详细信息。

启用代理支持后，Citrix Gateway 会将代理服务器详细信息发送到客户端 Web 浏览器，并更改浏览器上的代理配置。用户设备连接到 Citrix Gateway 后，用户设备可以直接与代理服务器通信以连接到用户的网络。

将一个代理服务器配置为使用 **Citrix Gateway** 的所有协议

您可以配置一个代理服务器以支持 Citrix Gateway 使用的所有协议。此设置为所有协议提供一个 IP 地址和端口组合。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** ，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在 客户端体验选项卡上，单击 高级设置。
4. 在“代理”选项卡上的“代理设置”下，选择“开**”**。
5. 对于协议，键入 IP 地址和端口号。
6. 单击对所有协议使用同一代理服务器，然后单 击确定。

禁用拆分隧道并将所有代理设置设置为“开”时，代理设置将传播到用户设备。如果代理设置设置为“设备”，则这些设置不会传播到用户设备。

Citrix Gateway 代表用户设备与代理服务器建立连接。代理设置不会传播到用户的浏览器，因此用户设备和代理服务器之间不可能直接通信。

将 **Citrix Gateway** 配置为代理服务器的步骤

将 Citrix Gateway 配置为代理服务器时，不安全且安全的 HTTP 是唯一受支持的协议。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** ，然后单击“全局设置**”**。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在 客户端体验选项卡上，单击 高级设置。
4. 在“代理”选项卡上的“代理设置”下，选择“设备”。
5. 对于协议，键入 IP 地址和端口号，然后单 击确定。

配置地址池

April 6, 2020

在某些情况下，使用 Citrix Gateway 插件连接的用户需要 Citrix Gateway 的唯一 IP 地址。例如，在 Samba 环境中，连接到映射网络驱动器的每个用户都需要看起来来自不同的 IP 地址。为组启用地址池（也称为 IP 池）时，Citrix Gateway 可以为每个用户分配唯一的 IP 地址别名。

您可以使用 Intranet IP 地址配置地址池。以下类型的应用程序可能需要使用从 IP 池中配置的唯一 IP 地址：

- IP 语音
- 活动 FTP
- 即时通讯
- 安全外壳 (SSH)
- 虚拟网络计算 (VNC) 连接到计算机桌面
- 远程桌面 (RDP) 连接到客户端桌面

您可以将 Citrix Gateway 配置为将内部 IP 地址分配给连接到 Citrix Gateway 的用户。静态 IP 地址可以分配给用户，也可以将一系列 IP 地址分配给组、虚拟服务器或全局系统。

Citrix Gateway 允许您将内部网络中的 IP 地址分配给远程用户。远程用户可以通过内部网络上的 IP 地址寻址。如果您选择使用一系列 IP 地址，系统会根据需要将该范围内的 IP 地址动态分配给远程用户。

配置地址池时，请注意以下事项：

- 分配的 IP 地址需要正确路由。要确保正确的路由，请考虑以下事项：
  - 如果不启用拆分隧道，请确保 IP 地址可以通过网络地址转换 (NAT) 设备路由。
  - 通过具有 Intranet IP 地址的用户连接访问的任何服务器都必须配置适当的网关来访问这些网络。
  - 在 Citrix Gateway 上配置网关或静态路由，以便将来自用户软件的网络流量路由到内部网络。

- 分配 IP 地址范围时，只能使用连续子网掩码。范围的子集可以分配给较低级别的实体。例如，如果 IP 地址范围绑定到虚拟服务器，则将范围的子集绑定到组。
- IP 地址范围不能绑定到绑定级别内的多个实体。例如，绑定到组的地址范围的子集不能绑定到第二个组。
- Citrix Gateway 不允许您在用户会话主动使用的 IP 地址时删除或取消绑定。
- 内部网络 IP 地址通过使用以下层次结构分配给用户：
  - 用户的直接绑定
  - 组分配的地址池
  - 虚拟服务器分配的地址池
  - 全球地址范围
- 在分配地址范围时，只能使用连续子网掩码。但是，分配范围的子集可能会进一步分配给较低级别的实体。绑定的全局地址范围可以具有绑定到以下内容的范围：
  - 虚拟服务器
  - 小组
  - 用户
- 绑定的虚拟服务器地址范围可以具有绑定到以下内容的子集：
  - 小组
  - 用户

绑定组地址范围可以绑定到用户的子集。

将 IP 地址分配给用户时，该地址将保留用于用户下次登录，直到地址池范围已耗尽。地址用尽后，Citrix Gateway 会从从 Citrix Gateway 注销时间最长的用户处回收 IP 地址。

如果无法回收地址并且所有地址正在使用，Citrix Gateway 将不允许用户登录。当所有其他 IP 地址都不可用时，您可以允许 Citrix Gateway 使用映射的 IP 地址作为 Intranet IP 地址来防止这种情况。

内联网 **IP** 域名注册

如果将 Intranet IP 分配给客户端计算机，并在 VIP 隧道建立后，VPN 插件会检查该客户端计算机是否已加入域。如果客户端计算机是已加入域的计算机，则 VPN 插件将启动 DNS 注册过程，以将计算机的主机名 Intranet 与分配的 Intranet IP 地址联系起来。该登记将在隧道拆除前恢复。

要成功注册 DSN，请确保设置了以下 nsapimgr 旋钮。还请确保将权威 DNS 服务器设置为允许 “非安全”DNS 更新。

- **nsapimgr -ys enable_vpn_dns_override=1**：此标志与其他配置参数一起发送到 NetScaler Gateway VPN 客户端。如果此标志未设置，并且 VPN 客户端拦截 DNS/WINS 请求时，它会通过隧道向 NetScaler Gateway 虚拟服务器发送相应的 “GET /DNS”http 请求以获取已解析的 IP 地址。但是，如果设置了 “enable_vpn_dnstruncate_fix” 标志，VPN 客户端将 DNS/WINS 请求透明地转发到 NetScaler Gateway 虚拟服务器。在这种情况下，DNS 数据包按原样通过 VPN 隧道发送到 NetScaler Gateway 虚拟服务器。当从 NetScaler Gateway 中配置的名称服务器返回的 DNS 记录很大并且不适合 UPD 响应数据包时，这将有所帮助。在这种情况下，当客户端回退到使用 TCP-DNS 时，此 TCP-DNS 数据包按原样到达 NetScaler Gateway 服务器，因此 NetScaler Gateway 服务器对 DNS 服务器进行 TCP-DNS 查询。

- **nsapimgr -ys enable_vpn_dnstruncate_fix=1**：此标志由 NetScaler Gateway 服务器本身使用。如果设置此标志，NetScaler 网关会覆盖“DNS 端口上的 TCP 连接”的目标到 NetScaler Gateway 上配置的 DNS 服务器（而不是尝试将它们发送到最初存在于传入 TCP-DNS 数据包中的 DNS 服务器 IP）。对于 UDP DNS 请求，默认情况下使用配置的 DNS 服务器进行 DNS 解析。

有关设置这些旋钮的更多信息，请参阅https://support.citrix.com/article/CTX200243。

配置地址池

April 6, 2020

您可以使用配置实用程序在要绑定策略的级别配置地址池。例如，如果要为虚拟服务器创建地址池，请在该节点上配置 Intranet IP 地址。配置地址池后，策略将绑定到配置它的实体。您还可以创建地址池并在 Citrix Gateway 上全局绑定该地址池。

为用户、组或虚拟服务器配置地址池

1. 在配置实用程序的导航窗格中，展开 **Citrix Gateway**，执行以下操作之一：
   - 展开 Citrix Gateway 用户管理，然后单击 **AAA** 用户。
   - 展开 **Citrix Gateway** > 用户管理，然后单击 **AAA** 组。
   - 展开 **Citrix Gateway** ，然后单击 虚拟服务器。
2. 在详细信息窗格中，单击用户、组或虚拟服务器，然后单击 打开。
3. 在 **Intranet IP** 选项卡上的 IP 地址和网络掩码中，键入 IP 地址和子网掩码，然后单击 添加。
4. 对要添加到池的每个 IP 地址重复步骤 3，然后单击“确定”。

全局配置地址池

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** ，然后单击“全局设置”。
2. 在详细信息窗格中的 **Intranet IP** 下，单击要分配唯一的静态 IP 地址或 IP 地址池供所有客户端 Citrix Gateway 会话使用，请配置 Intranet IP。
3. 在 绑定 **Intranet IP** 对话框中，单击 操作，然后单击 插入。
4. 在“IP 地址和网络掩码”中，键入 IP 地址和子网掩码，然后单击“添加”。
5. 对要添加到池的每个 IP 地址重复步骤 3 和 4，然后单 击确定。

定义地址池选项

April 6, 2020

您可以使用会话策略或全局 Citrix Gateway 设置来控制是否在用户会话期间分配 Intranet IP 地址。通过定义地址池选项，您可以将 Intranet IP 地址分配给 Citrix Gateway，同时禁用特定用户组的 Intranet IP 地址。

您可以通过以下三种方式之一使用会话策略来配置地址池：

- 非溢出 - 当您为 Intranet IP 地址配置地址池时，您将获得具有池中可用 IP 的会话。对于已使用所有可用的 Intranet IP 地址的用户，将显示“转移登录”页面。
- 溢出 - 当您配置地址池并将映射的 IP 用作 Intranet IP 地址时，映射的 IP 地址将用于已使用所有可用的 Intranet IP 地址的用户。
- 关闭-未配置地址池。

> 注意：如果未配置映射的 IP 地址，则使用 SNIP。

配置地址池

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** > 策略，然后单击“会话”。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在“网络配置”选项卡上，单击“高级”。
7. 在 Intranet IP 旁边，单击 覆盖全局，然后选择一个选项。
8. 如果在步骤 9 中选择溢出，则在映射的 IP 旁边，单击“覆盖全局”，选择设备的主机名，单击“确定”，然后单击“创建”。
9. 在“创建会话策略”对话框中，创建一个表达式，单击“创建”，然后单击“关闭”。

配置传输登录页面

如果用户没有可用的 Intranet IP 地址，然后尝试使用 Citrix Gateway 建立另一个会话，则会显示“转移登录”页面。“转移登录”页面允许用户将其现有 Citrix Gateway 会话替换为新会话。

如果注销请求丢失或用户未执行干净注销，也可以使用“转移登录”页面。例如：

- 为用户分配了静态 Intranet IP 地址，并具有现有 Citrix Gateway 会话。如果用户尝试从其他设备建立第二个会话，则会显示“转移登录”页面，用户可以将会话传输到新设备。
- 为用户分配了五个 Intranet IP 地址，并通过 Citrix Gateway 拥有五个会话。如果用户尝试建立第六个会话，则会显示“转移登录”页面，用户可以选择将现有会话替换为新会话。

> 注意：如果用户没有可用的 > 分配的 IP 地址，并且无法通过使用 > 转移登录页面建立新的 > 会话，用户将收到 > 错误消息。

仅当您配置地址池并禁用溢出时，才会显示“转移登录”页面。

配置 **DNS** 后缀

当用户登录到 Citrix Gateway 并被分配一个 IP 地址时，用户名和 IP 地址组合的 DNS 记录将添加到 Citrix Gateway DNS 缓存中。您可以配置 DNS 后缀，以便在将 DNS 记录添加到缓存中时追加到用户名。这样可以通过 DNS 名称引用用户，而 DNS 名称比 IP 地址更容易记住。当用户从 Citrix Gateway 注销时，该记录将从 DNS 缓存中删除。

配置 **DNS** 后缀

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** > 策略，然后单击“会话”。
2. 在详细信息窗格的“策略”选项卡上，选择会话策略，然后单击“打开”。
3. 在请求配置文件旁边，单击修改。
4. 在“网络配置”选项卡上，单击“高级”。
5. 在 Intranet IP DNS 后缀旁边，单击 覆盖全局，键入 DNS 后缀，然后单 击确定三次。

支持 **VoIP** 电话

April 6, 2020

将 Citrix Gateway 作为独立设备安装并且用户使用 Citrix Gateway 插件进行连接时，Citrix Gateway 支持与 IP 语音 (VoIP) 软电话进行双向通信。

实时应用程序，如语音和视频，通过用户数据报协议 (UDP) 实现。传输控制协议 (TCP) 不适用于实时流量，因为确认和重新传输丢失的数据包引起了延迟。实时交付数据包比确保交付所有数据包更重要。但是，使用任何通过 TCP 进行隧道技术，无法实现这种实时性能。

Citrix Gateway 支持以下 VoIP 软件电话。

- 思科软通话
- 阿瓦亚 IP 软件电话

IP PBX 和用户设备上运行的软件电话软件之间支持安全隧道。要使 VoIP 流量能够遍历安全隧道，必须在同一用户设备上安装 Citrix Gateway 插件和其中一个受支持的软件电话。当通过安全隧道发送 VoIP 流量时，支持以下软件电话功能：

- 从 IP 软电话发出的传出呼叫
- 被放置到 IP 软电话的传入呼叫
- 双向语音通信

对 VoIP 软件电话的支持通过使用内部网 IP 地址进行配置。您必须为每个用户配置 Intranet IP 地址。如果您使用的是思科 Softphone 通信，则在配置 Intranet IP 地址并将其绑定到用户之后，不需要其他配置。有关配置 Intranet IP 地址的更多信息，请参阅配置地址池。

如果您启用拆分隧道，请创建 Intranet 应用程序并指定 Avaya Softphone 应用程序。此外，您必须启用透明拦截。

为适用于 **Java** 的 **Citrix Gateway** 插件配置应用程序访问

April 6, 2020

您可以配置访问级别，并允许用户在安全网络中访问的应用程序。如果用户使用适用于 Java 的 Citrix Gateway 插件登录，则在“安全访问远程会话”对话框中，用户可以单击“应用程序”。此时将出现 Intranet 应用程序对话框，其中列出了用户有权访问的所有应用程序。

当用户连接到适用于 Java 的 Citrix Gateway 插件时，您可以配置允许用户访问应用程序的两种方法之一。

- HOSTS 文件修改方法
- SourceIP 和 SourcePort 方法

使用 **HOSTS** 文件修改方法访问应用程序

使用 HOSTS 文件修改方法时，适用于 Java 的 Citrix Gateway 插件会添加一个条目，该条目与您在 HOSTS 文件中配置的应用程序相对应。若要在基于 Windows 的设备上修改此文件，您必须以管理员身份登录或具有管理员权限。如果您未使用管理员权限登录，请手动编辑 HOSTS 文件并添加相应的条目。

注意：在基于 Windows 的计算机上，主机文件位于以下目录路径中：%systemroot%\system32\drivers\etc 。在 Macintosh 或 Linux 计算机上，主机文件位于 /etc/hosts。

例如，您希望使用 Telnet 连接到安全网络中的计算机。您可以使用远程计算机在安全网络和远程（例如，在家中）工作。IP 地址应该是本地主机 IP 地址 127.0.0.1。在 HOSTS 文件中，添加 IP 地址和应用程序名称，例如：

127.0.0.1 telnet1

编辑 HOSTS 文件并保存在用户设备上时，您可以测试您的连接。您可以通过打开命令提示符并使用 Telnet 进行连接来测试连接。如果用户使用的用户设备不在安全网络内，请在启动 Telnet 之前登录到 Citrix Gateway。

要连接到安全网络中的计算机，请执行以下操作：

1. 使用计算机的可用软件启动 Telnet 会话。
2. 从命令提示符中键入：打开 telnet

   将显示远程计算机的登录提示。

使用 **SourceIP** 和 **SourcePort** 方法访问应用程序

如果用户需要访问安全网络中的应用程序并且对用户设备没有管理权限，请使用位于 Intranet 应用程序对话框中的源 IP 地址和端口号配置 HOSTS 文件。

打开 Intranet 应用程序对话框并找到 IP 地址和端口号

1. 用户使用插件登录时，在“安全远程访问”对话框中，单击“应用程序”。

2. 在列表中找到应用程序，并记下源地址和源端口号。

当您具有 IP 地址和端口号时，启动 Telnet 会话以连接到远程网络中的计算机。

配置访问接口

April 6, 2020

Citrix Gateway 包含一个默认主页，该主页是用户登录后显示的网页。默认主页称为访问界面。您可以使用访问界面作为主页，或将 Web Interface 配置为主页或自定义主页。

访问接口包含三个面板。如果您的部署中有 Web Interface，则用户可以在访问界面左侧面板中登录 Receiver。如果您的部署中有 StoreFront，则用户无法从左侧面板登录 Receiver。

访问界面用于提供指向内部和外部网站的链接，以及指向内部网络中文件共享的链接。您可以通过以下方式自定义访问界面：

- 更改访问接口。
- 创建访问界面链接。

用户可以通过添加自己的链接到网站和文件共享来自定义访问界面。用户还可以使用主页将文件从内部网络传输到其设备。

> 注意：当用户登录并尝试从访问接口打开文件共享时，文件共享不会打开，用户会收到错误消息“无法与服务器建立 TCP 连接。”若要解决此问题，请将防火墙配置为允许从 Citrix Gateway 系统 IP 地址到 TCP 端口 445 和 139 上的文件服务器 IP 地址的流量。

将访问界面替换为自定义主页

April 6, 2020

您可以使用全局设置或会话策略和配置文件配置自定义主页以替换默认主页（访问界面）。配置策略后，您可以将策略绑定到用户、组、虚拟服务器或全局。配置自定义主页时，用户登录时不会显示访问接口。

全局配置自定义主页

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** ，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户体验”选项卡上的“主页”中，单击“显示主页”，然后输入自定义主页的 Web 地址。
4. 单击 确定，然后单击 关闭。

在会话配置文件中配置自定义主页

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** 策略，然后单击“会话”。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在“客户端体验”选项卡上，在“主页”旁边，单击“覆盖全局”，单击“显示主页”，然后键入主页的 Web 地址。
7. 在“创建会话策略”对话框的 命名表达式旁边，选择“常 规”，选择“True”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

更改访问接口

April 6, 2020

您可能希望将用户引导到自定义主页，而不是依赖访问界面。若要执行此操作，请在 Citrix Gateway 上安装主页，然后将会话策略配置为使用新主页。

安装自定义主页

1. 在配置实用程序中，单击 配置选项卡，然后在导航窗格中单击 **Citrix Gateway**。
2. 在详细信息窗格中的“自定义访问界面”下，单击“上传访问界面”。
3. 若要从网络中的计算机上的文件安装主页，请在“本地文件”中单击“浏览”，导航到该文件，然后单击“选择”。
4. 要使用 Citrix Gateway 上安装的主页，请在“远程路径”中单击“浏览”，选择该文件，然后单击“选择”。
5. 单击“上传”，然后单击“关闭”。

创建和应用 **Web** 和文件共享链接

November 7, 2022

您可以将访问接口配置为显示用户可用的一组指向内部资源的链接。创建这些链接需要首先将链接定义为资源。然后，您将它们绑定到用户、组、虚拟服务器或全局，以使它们在访问接口中处于活动状态。您创建的链接将显示在企业网站和企业文件共享下的网站和文件共享窗格中。如果用户添加自己的链接，这些链接将显示在“
个人网站”和“个人文件共享”下。

在会话策略中创建访问接口链接

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** 资源，然后单击“门户书签”。

2. 在详细信息窗格中，单击 添加。
3. 在 “名称” 中，键入书签的名称。
4. 在要显示的 文本中，键入链接的描述。该描述将显示在 访问界面中。
5. 在 书签中，键入 Web 地址，单击 创建，然后单击 关闭。

如果启用无客户端访问，则可以确保对 Web 站点的请求通过 Citrix Gateway。例如，您添加了书签Google。在 “创建书签” 对话框中，选中 “将 Citrix Gateway 用作反向代理” 复选框。选中此复选框后，网站请求将从用户设备发送到 Citrix Gateway，然后发送到网站。清除该复选框后，请求将从用户设备发送到网站。仅当您启用无客户端访问时，此复选框才可用。

全局绑定书签

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 **Citrix Gateway** ，然后单击 “全局设置”。
2. 在详细信息窗格的 “书签” 下，单击 “创建指向要在 **Citrix Gateway** 门户页面上访问的 HTTP 和 Windows 文件共享应用程序的链接”。
3. 在 配置 **VPN** 全局绑定 * 对话框中，单击 添加。
4. 在 “可用” 下，选择一个或多个书签，单击右箭头以移动已配置下的书签，然后单击 “确定”。

绑定访问接口链接

您可以将访问接口链接绑定到以下位置：

- 用户
- 组
- 虚拟服务器

保存配置后，用户可以在 “主页” 选项卡上的 “访问界面” 中使用这些链接，该选项卡是用户在成功登录后看到的第一页。这些链接根据类型、网站链接或文件共享链接在页面上进行组织。

1. 在配置实用程序的导航窗格中，执行以下操作之一：
   - 展开 **Citrix Gateway** 用户管理，然后单击 **AAA** 用户。
   - 展开 **Citrix Gateway** 用户管理，然后单击 **AAA** 抓取。
   - 展开 **Citrix Gateway** ，然后单击 虚拟服务器。
2. 在详细信息窗格中，执行以下操作之一：
   - 选择一个用户，然后单击打开。
   - 选择一个组，然后单击打开。
   - 选择一个虚拟服务器，然后单击打开。
3. 在对话框中，单击书 签选项卡。
4. 在 “可用书签” 下，选择一个或多个书签，单击右箭头以移动已配置书签下的书签，然后单击 “确定”。

在书签中配置用户名令牌

April 6, 2020

您可以使用特殊令牌%username% 配置书签和文件共享 URL。用户登录时，令牌将替换为每个用户的登录名。例如，您为名为 Jack 的员工创建书签，作为 \\EmployeeServer\%username%\ 文件夹。当 Jack 登录时，文件共享 URL 将映射到 \\EmployeeServer\Jack\。在书签中配置用户名令牌时，请记住以下情况：

- 如果您使用的是一种身份验证类型，则用户名将替换令牌%username%。
- 如果您使用的是双重身份验证，则主身份验证类型中的用户名将用于替换%username% 令牌。
- 如果您使用的是客户端证书身份验证，则使用客户端证书身份验证配置文件中的用户名字段替换%username% 令牌。

流量策略的工作原理

April 6, 2020

流量策略允许您为用户连接配置以下设置：

- 对从不受信任的网络访问的敏感应用程序实施更短的超时。
- 将网络流量切换为某些应用程序使用 TCP。如果选择 TCP，则需要为某些应用程序启用或禁用单点登录。
- 识别要将其他 HTTP 功能用于 Citrix Gateway 插件流量的情况。
- 定义与文件类型关联一起使用的文件扩展名。

创建流量策略

April 6, 2020

要配置流量策略，您需要创建配置文件并配置以下参数：

- 协议 (HTTP 或 TCP)
- 申请超时
- 单点登录到 Web 应用程序
- 形成单点登录
- 文件类型关联
- 中继器插件
- Kerberos 约束委派 (KCD) 账户

创建流量策略后，您可以将策略绑定到虚拟服务器、用户、组或全局。

例如，您有 Web 应用程序 PeopleSoft 人力资源安装在内部网络中的服务器上。您可以为此应用程序创建定义目标 IP 地址、目标端口的流量策略，还可以设置用户可以保持登录到应用程序的时间（如 15 分钟）。

如果要配置其他功能（如 HTTP 压缩到应用程序），则可以使用流量策略配置设置。创建策略时，请使用 HTTP 参数执行操作。在表达式中，为运行应用程序的服务器创建目标地址。

配置流量策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“Citrix Gateway”>“策略”，然后单击“流量”。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“创建流量策略”对话框的“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在协议中，选择 HTTP 或 TCP。

   > 注意：如果选择 TCP 作为协议，则无法配置单点登录，并且在配置文件对话框中禁用该设置。

7. 在 AppTimeout（分钟）中，键入分钟数。此设置限制了用户可以保持登录 Web 应用程序的时间。
8. 要启用对 Web 应用程序的单点登录，请在单点登录中选择开。

   注意：如果要使用基于表单的单点登录，可以在流量配置文件中配置设置。有关更多信息，请参阅配置基于表单的单点登录。

9. 要指定文件类型关联，请在“文件类型关联”中选择“开”。
10. 若要使用中继器插件优化网络流量，请在“分支中继器”中选择“开”，单击“创建”，然后单击“关闭”。
11. 如果您在设备上配置 KCD，请在 KCD 帐户中选择该帐户。

    有关在设备上配置 KCD 的更多信息，请参阅在 NetScaler 设备上配置 Kerberos 约束委派。

12. 在“创建流量策略”对话框中，创建或添加表达式，单击“创建”，然后单击“关闭”。

配置基于表单的单点登录

April 6, 2020

基于表单的单点登录允许用户一次性登录到网络中的所有受保护的应用程序。在 Citrix Gateway 中配置基于表单的单点登录时，用户可以访问需要基于 HTML 表单的登录的 Web 应用程序，而无需再次键入密码。如果没有单点登录，用户需要单独登录才能访问每个应用程序。

创建表单单点登录配置文件后，您可以创建包含表单单点登录配置文件的流量配置文件和策略。有关详细信息，请参阅创建流量策略。

配置基于表单的单点登录

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”，然后单击 “流量”。
2. 在详细信息窗格中，单击表单 SSO 配置文件选项卡，然后单击添加。
3. 在 “名称” 中，键入配置文件的名称。
4. 在操作 URL 中，键入已完成表单提交到的 URL。

   > 注意： URL 是根相对 URL。

5. 在 “用户名字段” 中，键入用户名字段的属性名称。
6. 在 “密码字段” 中，键入密码字段的属性名称。
7. 在 SSO 成功规则中，创建一个表达式，用于描述策略调用此配置文件时执行的操作。您还可以使用此字段下的 “前缀”、“添加” 和 “运算符” 按钮来创建表达式。

   此规则检查单点登录是否成功。

8. 在 “名称值对” 中，键入用户名字段值，后跟和符号 (&)，然后键入密码字段值。

   值名称由 & 符号 (&) 分隔，例如 name1=value1&name2=value2。

9. 在响应大小中，键入数字字节以允许完整响应大小。键入要解析的响应中的字节数以提取表单。
10. 在 “提取” 中，选择名称/值对是静态还是动态。默认设置为动态。
11. 在 “提交方法” 中，选择单点登录表单用于将登录凭据发送到登录服务器的 HTTP 方法。默认值为 Get。
12. 单击 Create（创建），然后单击 Close（关闭）。

配置 **SAML** 单点登录

April 6, 2020

您可以为单点登录 (SSO) 创建 SAML 1.1 或 SAML 2.0 配置文件。用户可以连接到支持单点登录 SAML 协议的 Web 应用程序。Citrix Gateway 支持 SAML Web 应用程序的身份提供商 (IdP) 单点登录。

配置 **SAML** 单点登录

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”，然后单击 “流量”。
2. 在详细信息窗格中，单击 SAML SSO 配置文件选项卡。
3. 在详细信息窗格中，单击 Add（添加）。
4. 在 “名称” 中，键入配置文件的名称。
5. 在签名证书名称中，输入 X.509 证书的名称。
6. 在 ACS URL 中，输入身份提供商或服务提供商的断言使用者服务。AssertionConsumerServiceURL (ACS URL) 为用户提供 SSO 功能。

7. 在中继状态规则中，从保存的策略表达式和常用表达式为策略构建表达式。从“运算符”列表中选择以定义表达式的评估方式。若要测试表达式，请单击“评估”。
8. 在“发送密码”中，选择“开”或“关”。
9. 在颁发者名称中输入 SAML 应用程序的标识。
10. 单击 Create（创建），然后单击 Close（关闭）。

绑定流量策略

April 6, 2020

您可以将流量策略绑定到虚拟服务器、组、用户和 Citrix Gateway 全局。您可以使用配置实用程序绑定流量策略。

使用配置实用程序全局绑定流量策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“Citrix Gateway”>“策略”，然后单击“流量”。
2. 在详细信息窗格中，选择一个策略，然后在操作中单击全局绑定。
3. 在“绑定/取消绑定流量策略”对话框的“详细信息”下，单击“插入策略”。
4. 在策略名称下，选择策略，然后单击确定。

删除流量策略

April 6, 2020

您可以使用配置实用程序从 Citrix Gateway 中删除流量策略。如果使用配置实用程序删除流量策略，并且策略绑定到用户、组或虚拟服务器级别，则必须先取消绑定策略。然后，您可以删除策略。

使用配置实用程序取消绑定流量策略

1. 在配置实用程序的导航窗格中，执行以下操作之一：
   - 展开 Citrix Gateway，然后单击虚拟服务器。
   - 展开“Citrix Gateway”>“用户管理”，然后单击“AAA 组”。
   - 展开“Citrix Gateway”>“用户管理”，然后单击“AAA 用户”。
2. 在详细信息窗格中，选择虚拟服务器、组或用户，然后单击“打开”。
3. 在配置 Citrix Gateway 虚拟服务器、配置 AAA 组或配置 AAA 用户对话框中，单击策略选项卡。
4. 单击“流量”，选择策略，然后单击“取消绑定策略”。
5. 单击确定，然后单击关闭。

解除流量策略绑定后，您可以删除该策略。

使用配置实用程序删除流量策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“Citrix Gateway”>“策略”，然后单击“流量”。
2. 在详细信息窗格的“策略”选项卡上，选择流量策略，然后单击“删除”。

配置会话策略

April 6, 2020

会话策略是应用于用户、组、虚拟服务器和全局的表达式和设置的集合。

您可以使用会话策略配置用户连接的设置。您可以定义用于配置软件用户登录使用的设置，例如适用于 Windows 的 Citrix Gateway 插件或适用于 Mac 的 Citrix Gateway 插件。您还可以配置设置以要求用户使用 Citrix Workspace 应用程序或 Secure Hub 登录。对用户进行身份验证后，会对会话策略进行评估和应用。

根据以下规则应用会话策略：

- 会话策略始终覆盖配置中的全局设置。
- 未使用会话策略设置的任何属性或参数都会在为虚拟服务器建立的策略上进行设置。
- 任何未由会话策略或虚拟服务器设置的其他属性均由全局配置进行设置。

> 重要提示：以下说明是创建会话策略的一般指南。有关为不同配置（例如无客户端访问权限或访问已发布应用程序）配置会话策略的具体说明。说明可能包含配置特定设置的说明；但是，该设置可以是会话配置文件和策略中包含的许多设置之一。这些说明指导您在会话配置文件中创建设置，然后将该配置文件应用于会话策略。您可以更改配置文件和策略中的设置，而无需创建新的会话策略。此外，您可以在全局级别上创建所有设置，然后创建会话策略以覆盖全局设置。

如果您在网络中部署 Citrix Endpoint Management 或 StoreFront，Citrix 建议您使用“快速配置”向导配置会话策略和配置文件。运行向导时，您可以定义部署的设置。然后 Citrix Gateway 创建所需的身份验证、会话和无客户端访问策略。

创建会话策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 完成会话配置文件的设置，然后单击创建。
7. 在“创建会话配置文件”对话框中，为策略添加表达式，单击“创建”，然后单击“关闭”。
   注意：在表达式中，选择
   True 值，以便始终将策略应用于其绑定到的级别。

创建会话配置文件

April 6, 2020

会话配置文件包含用户连接的设置。

会话配置文件指定在用户设备满足策略表达式条件时应用于用户会话的操作。配置文件与会话策略一起使用。您可以使用配置实用程序独立于会话策略创建会话配置文件，然后将该配置文件用于多个策略。您只能将一个配置文件与策略结合使用。

为会话配置文件中的用户连接配置网络设置

您可以使用会话配置文件中的“网络配置”选项卡为用户连接配置以下网络设置：

- DNS 服务器
- WINS 服务器 IP 地址
- 可用作 Intranet IP 地址的映射 IP 地址
- 地址池的溢出设置（Intranet IP 地址）
- 内联网 IP DNS 后缀
- HTTP 端口
- 强制超时设置

在会话配置文件中配置连接设置

您可以使用会话配置文件中的“客户端体验”选项卡配置以下连接设置：

- 访问界面或自定义主页
- 基于 Web 的电子邮件的 Web 地址，例如 Outlook Web Access
- 插件类型（适用于 Windows 的 Citrix Gateway 插件、适用于 Mac OS X 的 Citrix Gateway 插件或适用于 Java 的 Citrix Gateway 插件）
- 分裂式隧道
- 会话和空闲超时设置
- 无客户端访问
- 无客户端访问 URL 编码
- 插件类型（Windows、Mac 或 Java）
- 单点登录到 Web 应用程序
- 用于身份验证的凭据索引
- 使用 Windows 进行单点登录
- 客户端清理行为
- 登录脚本
- 客户端调试设置
- 拆分 DNS

- 访问专用网络 IP 地址和本地局域网访问
- 客户选择
- 代理设置

有关配置用户连接设置的更多信息，请参阅为 Citrix Gateway 插件配置连接。

在会话配置文件中配置安全设置

您可以使用会话配置文件中的“安全”选项卡配置以下安全设置：

- 默认授权操作（允许或拒绝）
- 安全浏览来自 iOS 设备的连接
- 隔离组
- 授权组

有关在 Citrix Gateway 上配置授权的更多信息，请参阅配置授权。

在会话配置文件中配置 **Citrix Virtual Apps and Desktops** 设置

可以使用会话配置文件中的“已发布应用程序”选项卡为与运行 Citrix Virtual Apps and Desktops 的服务器的连接配置以下设置：

- ICA 代理，这是使用 Citrix Workspace 应用程序的客户端连接
- Web Interface 地址
- Web Interface 门户模式
- 单点登录到服务器场域
- Citrix Workspace 应用程序主页
- 账户服务地址

有关配置连接到服务器场中已发布应用程序的设置的更多信息，请参阅通过 Web Interface 提供对已发布应用程序和虚拟桌面的访问权限。

您可以独立于会话策略创建会话配置文件。创建策略时，您可以选择要附加到策略的配置文件。

使用配置实用程序创建会话配置文件

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格中，单击配置文件选项卡，然后单击添加。
3. 配置配置文件的设置，单击创建，然后单击关闭。

创建配置文件后，您可以将其包含在会话策略中。

使用配置实用程序将配置文件添加到会话策略

1. 在配置实用程序的导航窗格中，展开“Access Gateway”>“策略”，然后单击“会话”。

2. 在“策略”选项卡上，执行以下操作之一：
   - 单击“添加”以创建新的会话策略。
   - 选择一个策略，然后单击打开。
3. 在请求配置文件中，从列表中选择一个配置文件。
4. 完成配置会话策略，然后执行以下操作之一：
   a) 单击创建，然后单击关闭以创建策略。
   b) 单击确定，然后单击关闭以修改策略。

绑定会话策略

April 6, 2020

创建会话策略后，将其绑定到用户、组、虚拟服务器或全局。会话策略按以下顺序作为层次结构应用：

- 用户
- 组
- 虚拟服务器
- 全球范围

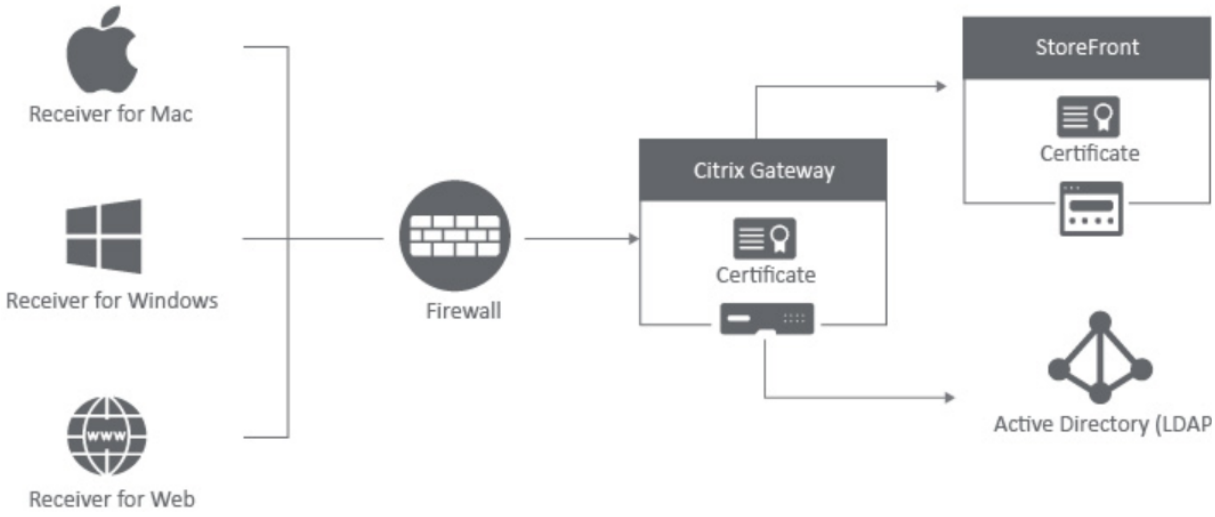
使用配置实用程序绑定会话策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后执行以下操作之一：
   a) 单击虚拟服务器。
   b) 展开用户管理，然后单击 AAA 组。
   c) 展开用户管理，然后单击 AAA 用户。
2. 根据您在步骤 1 中的选择，单击以下对话框之一中的“策略”选项卡：
   - 创建 Citrix Gateway 虚拟服务器
   - 配置 AAA 组
   - 配置 AAA 用户
3. 单击“会话”以添加会话策略。
4. 单击插入策略，选择会话策略，然后单击确定。

为 **StoreFront** 配置 **Citrix Gateway** 会话策略

November 3, 2021

本文介绍如何使用 Citrix Workspace 应用程序或 Web 浏览器的用户使用 StoreFront 配置 Citrix Gateway 域仅身份验证。

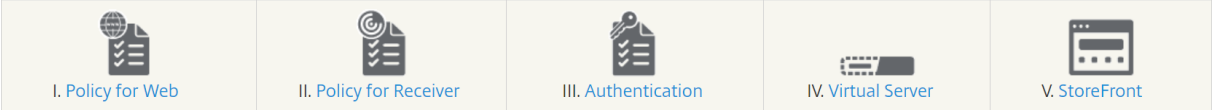


最低要求

- Citrix StoreFront 2.x 或 3.0
- Citrix ADC 10.5 及更高版本
- 适用于 Windows 4.x 的 Citrix Workspace 应用程序
- Citrix Workspace 应用程序的 Mac 11.8
- Web 浏览器（面向 Web 的 Citrix Workspace 应用程序）
- 如 CTX108876 所述，在 Citrix ADC 设备上配置身份验证-如何在 Citrix ADC 设备上配置 LDAP 身份验证
- 为 StoreFront 服务器和 Citrix Gateway 配置的 SSL 证书。有关以下主题的详细信息，请参阅StoreFront 文档。

  - 安装和设置 StoreFront 2.6
    - Windows 2012 服务器证书
    - 向站点添加 SSL 绑定
    - 安装和管理 Citrix ADC 设备 10.5 的证书

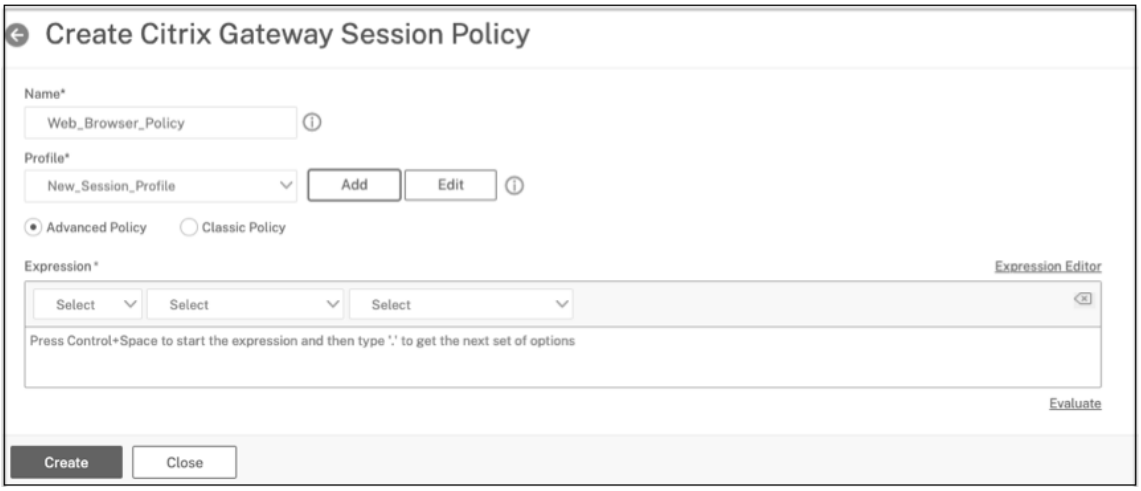
使用 **StoreFront** 配置 **Citrix Gateway**



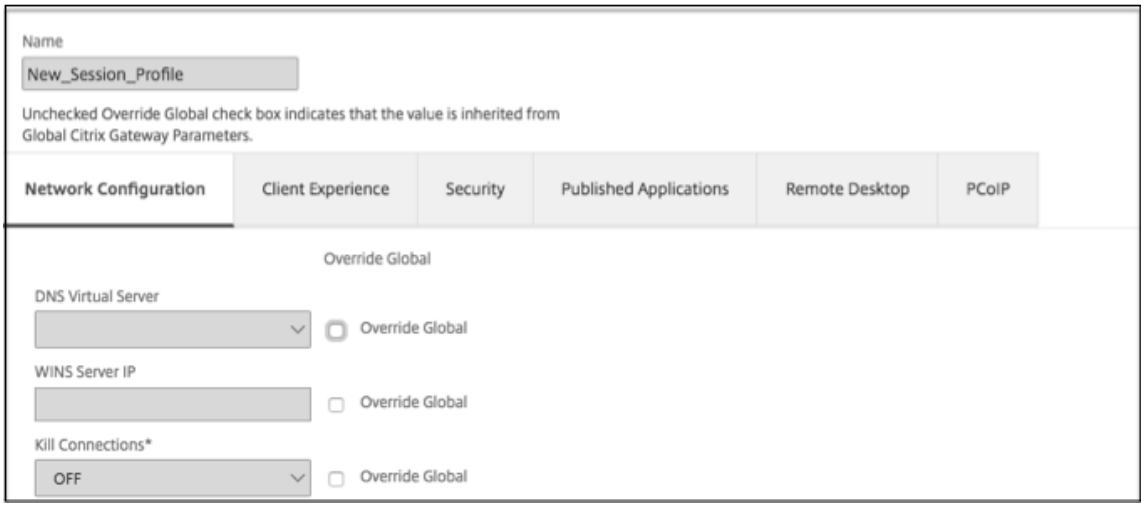
为基于 **Web** 浏览器的访问创建会话策略

1. 要创建会话策略，请导航到 **Citrix Gateway >** 策略 **>** 会话。

2. 在会 话策略字段中，单击 添加。
3. 在名 称字段中，键入会话策略的名称。例如，Web 浏览器策略。
4. 单击带有 + 符号的框。

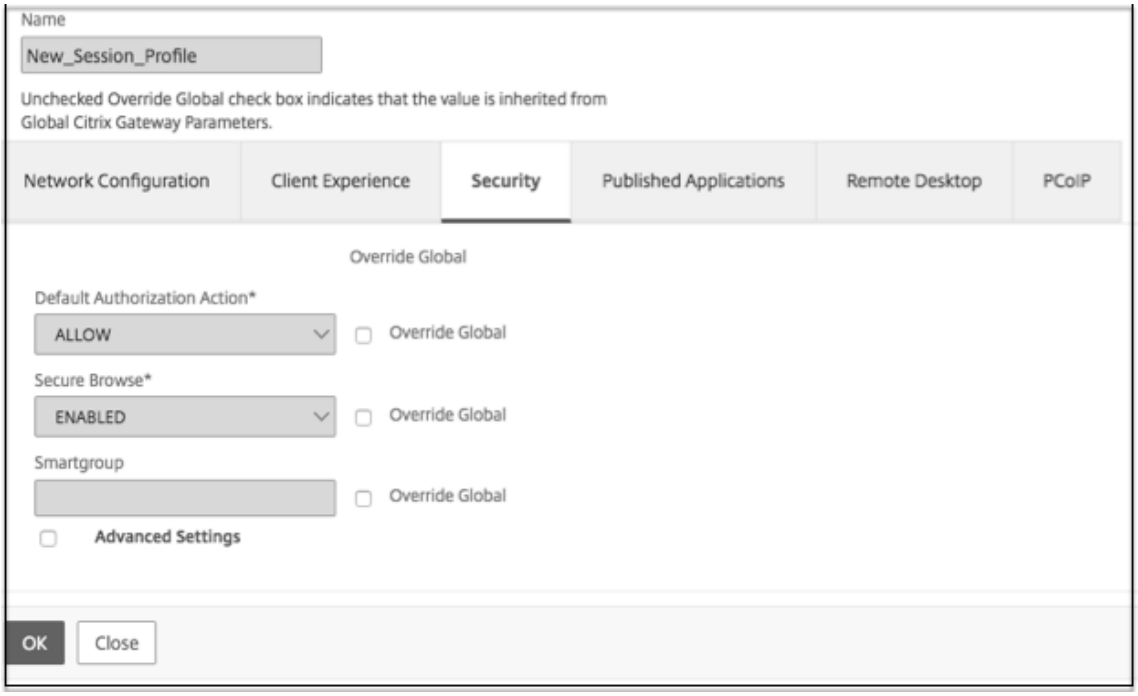


5. 在 配置 **Citrix Gateway** 会话配置文件窗口中键入新会话配置文件的名称。



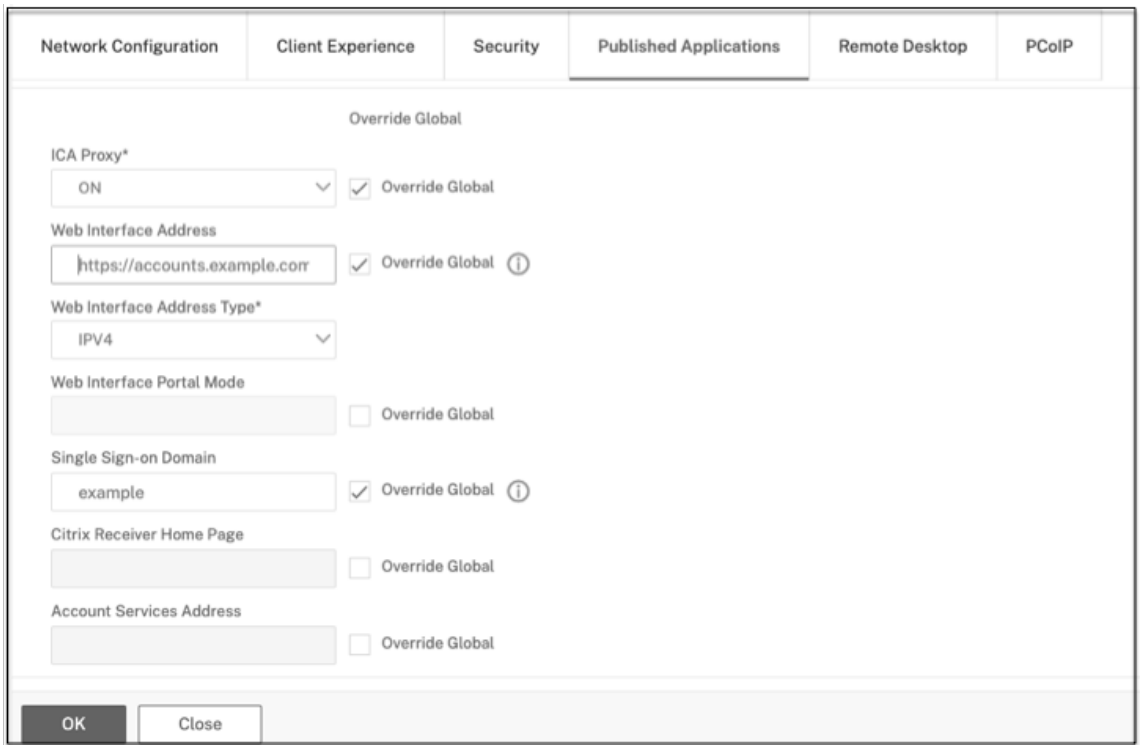
6. 在“客户端体验”选项卡中，启用以下设置：
   - 无客户端访问：设置为“开”
   - 单点登录到 **Web** 应用程序：选中复选框
   - 插件类型：设置为 **Windows/MAC OS X**

7. 在“安全”选项卡中，启用 默认授权操作并将其设置为“允许”。



8. 在“已发布的应用程序”选项卡中，启用以下设置：

   - **ICA** 代理：设置为开。
   - **Web Interface** 地址：StoreFront 服务器的 FQDN 后跟到 Web 应用商店的路径
   - 单点登录域**-**域的 NetBIOS 名称



9. 单击创建。
10. 如果您使用的是“经典策略”表达式，请在“表 达式”字段中添加以下信息，然后单击“创建”。

```
1 REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

11. 如果使用高级策略表达式，请在“表 达式”字段中添加以下信息，然后单击“创建”。

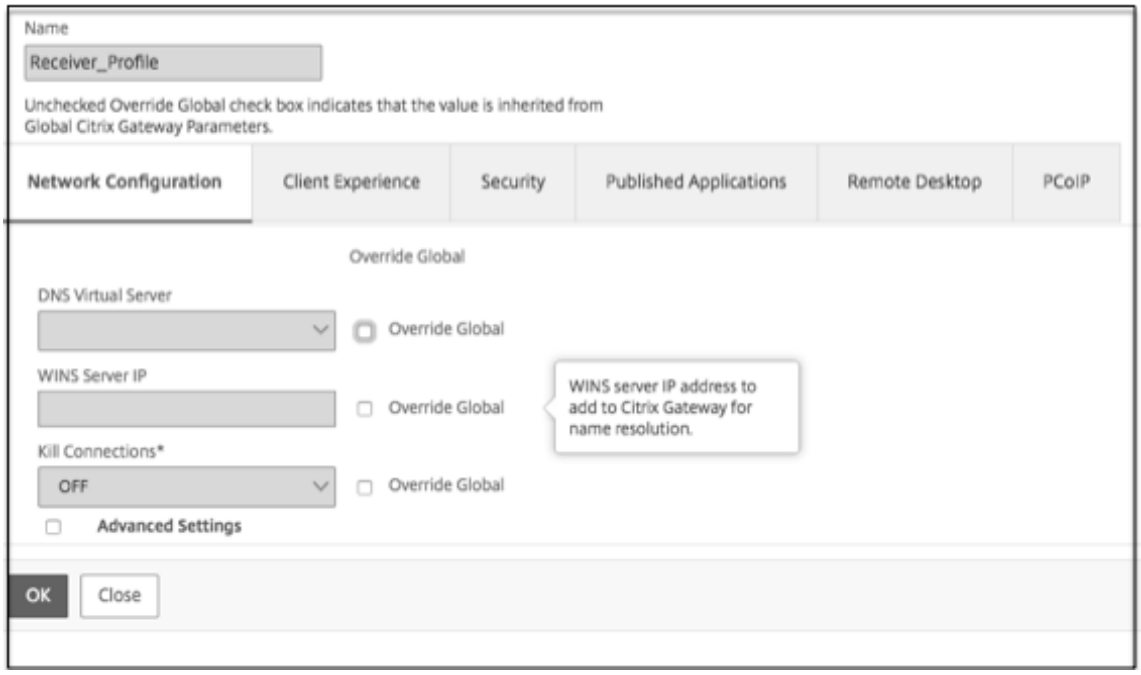
```
1 HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

Citrix ADC 需要使用此策略来区分基于 Web 浏览器的连接和基于 Citrix Workspace 应用程序的连接。此策略适用于基于 Web 浏览器的连接。

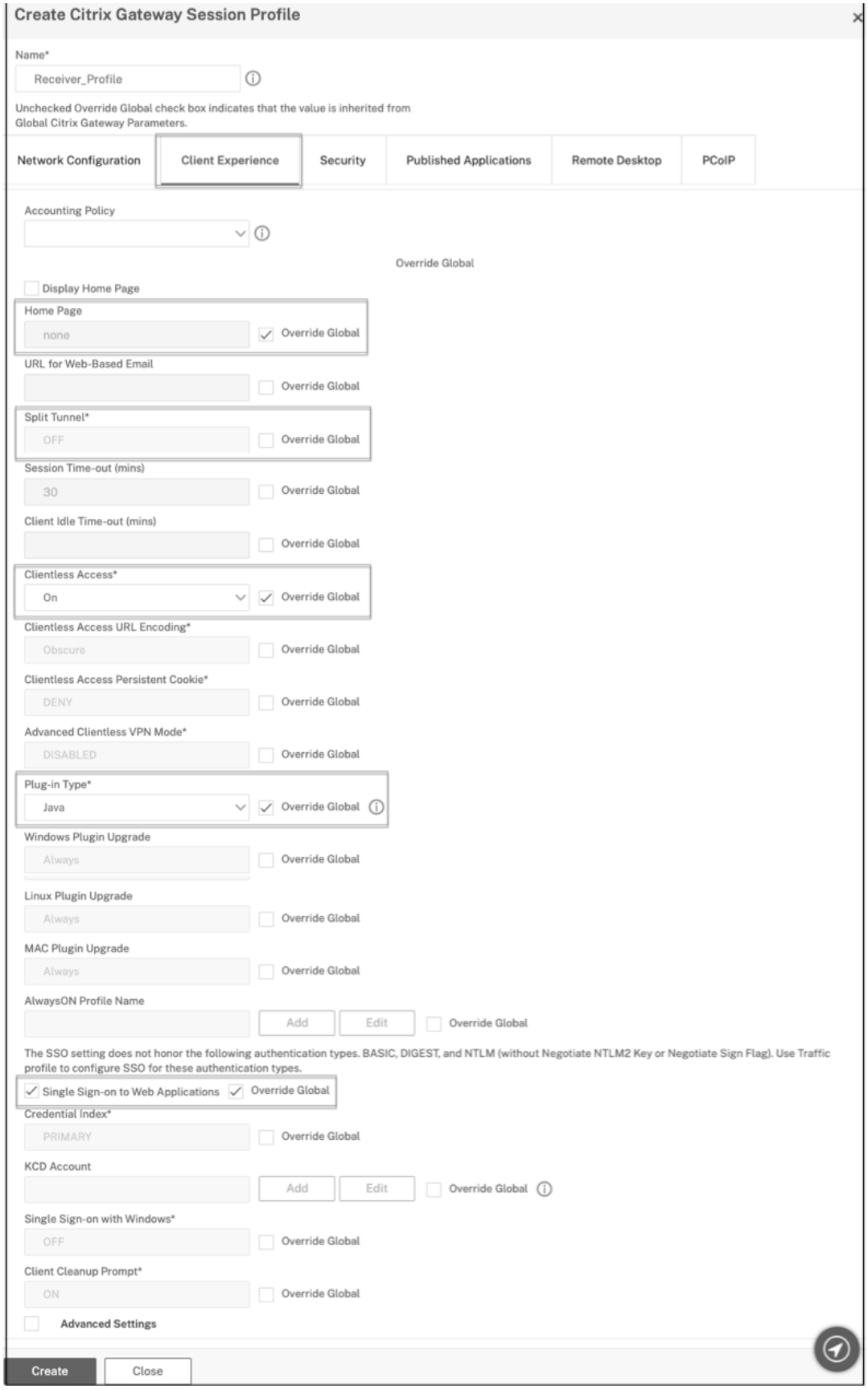
为适用于 **Windows** 或 **Mac** 的 **Citrix Workspace** 应用程序以及 **Citrix Gateway** 上的移动设备创建会话策略

1. 导航到 **Citrix Gateway >** 策略 **>** 会话。
2. 在会 话策略字段中，单击 添加。
3. 在“名称”字段中，键入会话策略的名称。例如，接收者策略
4. 单击带有 + 符号的框。

5. 在“配置 **Citrix Gateway** 会话配置文件”窗口中键入新会话配置文件的名称。

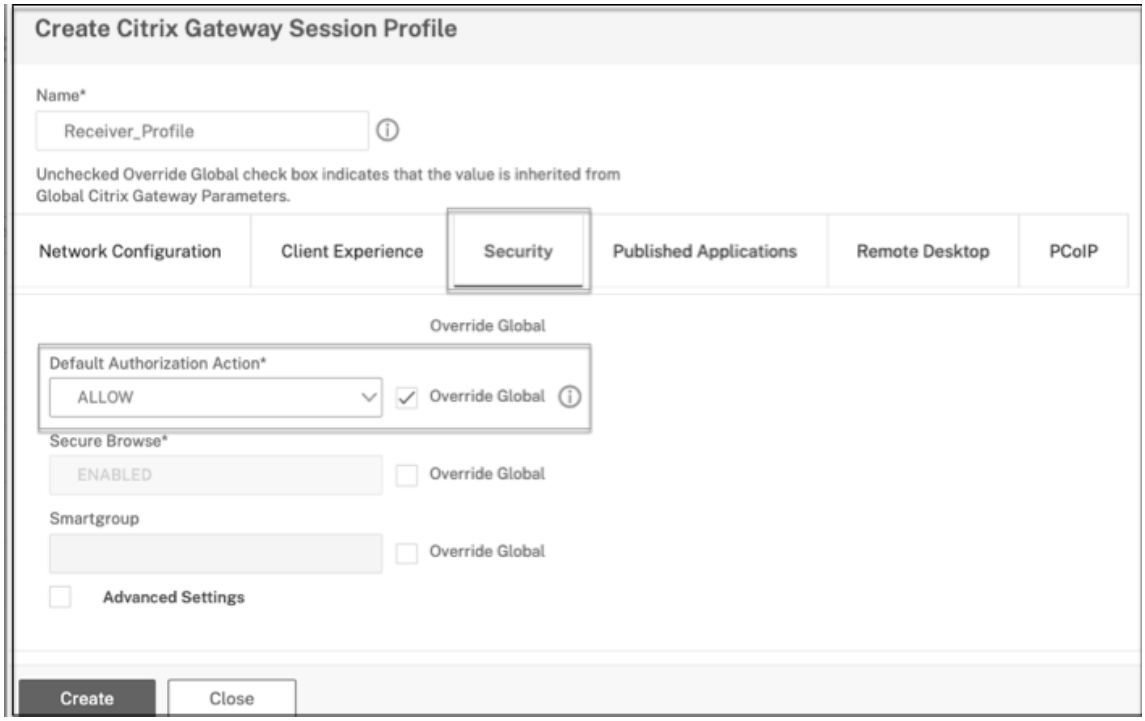


6. 在“客户端体验”选项卡中，启用以下设置：



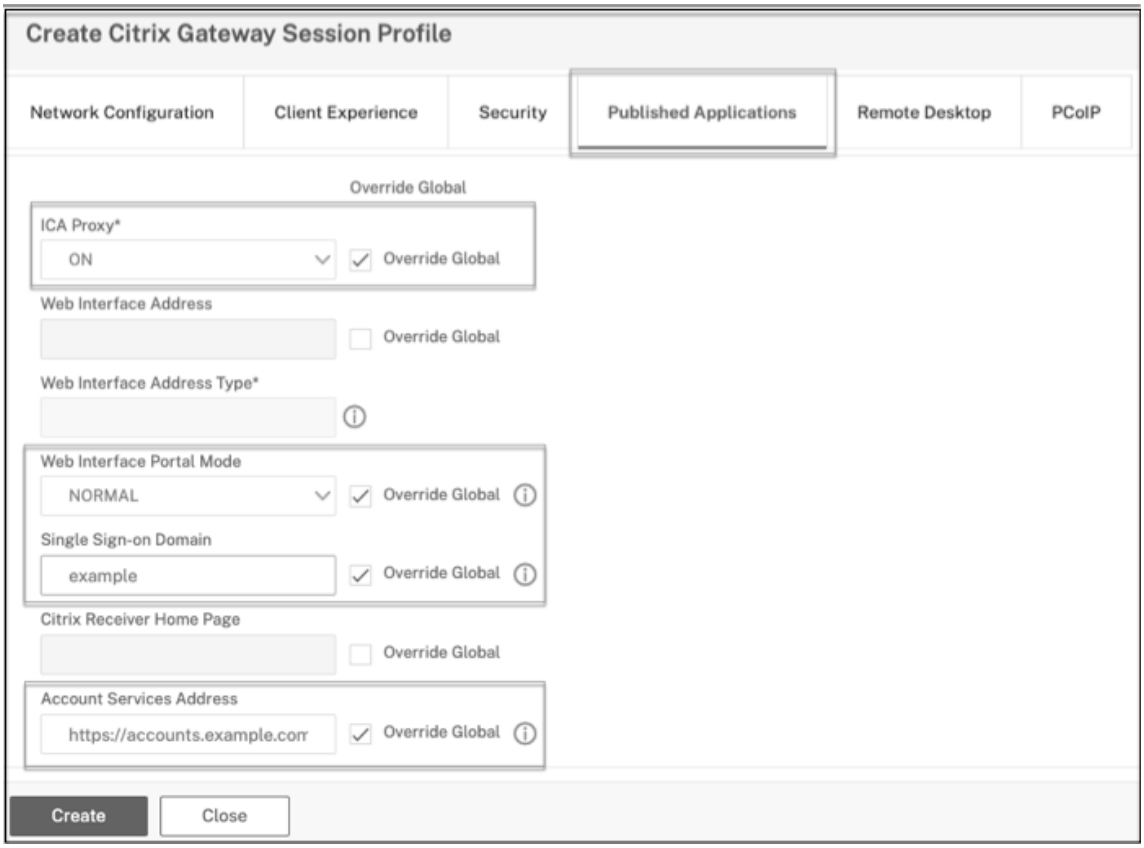
- 主页：设置为 无
- 分割隧道：设置为 **OFF**
- 无客户端访问：设置为 “开”
- 单点登录到 **Web** 应用程序：选中复选框
- 插件类型：设置为 **Java**

7. 在 “安全” 选项卡中，将 默认授权操作设置为 “允许”。



8. 在 “已发布的应用程序” 选项卡中，启用以下设置：

- **ICA** 代理：设置为开。
- **Web Interface** 地址： StoreFront 服务器的 FQDN 后跟到商店的路径
- 单点登录域：域的 NetBIOS 名称
- 账户服务地址：输入账户服务地址。最后一个反斜杠很重要。



9. 单击创建。
10. 如果使用“经典策略”表达式，请在“表达式”字段中添加以下信息，然后单击“创建”。

```
1 REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
```

11. 如果使用高级策略表达式，请在“表 达式”字段中添加以下列出的信息，然后单击“创建”。

```
1 HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
```


Citrix ADC 需要使用此策略来区分基于 Web 浏览器的连接和基于 Citrix Workspace 应用程序的连接。此策略适用于基于 Citrix Workspace 应用程序的连接。

在 **Citrix ADC** 设备上配置身份验证

有关在 Citrix ADC 设备上配置 LDAP 身份验证的信息，请参阅配置 LDAP 身份验证。

创建 **Citrix Gateway** 虚拟服务器并绑定会话策略

1. 导航到 **Citrix Gateway >** 虚拟服务器，然后单击 添加以添加新的虚拟服务器。
2. 创建虚拟服务器后，根据贵公司的要求将特定会话策略绑定到虚拟服务器。

配置 **StoreFront** 的身份验证

1. 从 StoreFront 上的 Citrix Gateway 启用直通身份验证。有关详细信息，请参阅配置身份验证服务。

   StoreFront 必须为身份验证回调服务信任 Citrix Gateway 虚拟服务器绑定证书（根证书和/或中间证书）的颁发者。

2. 将 Citrix Gateway 添加到 StoreFront。有关详细信息，请参阅添加 Citrix Gateway 连接。

   网关 URL 必须与用户在 Web 浏览器地址栏中输入的内容完全匹配。

3. 在 StoreFront 商店中启用远程访问。有关详细信息，请参阅管理通过 Citrix Gateway 对应用商店的远程访问。

企业书签的高级策略支持

April 6, 2020

企业书签 (VPN URL) 现在可以配置为高级策略。

将 **VPN URL** 配置为高级策略

要将 VPN URL 配置为高级策略，需要执行以下任务。

- 创建 VPN URL 操作
- 创建 VPN URL 策略）
- 将策略绑定到绑定点

创建 **VPN URL** 操作

在命令提示窗口中，键入以下内容：

```
add vpn urlAction <name> -linkName <string> -actualURL <string> [-
    vServerName <string>] [-clientlessAccess ( ON | OFF )] [-comment <
    string>] [-iconURL <URL>] [-ssotype <ssotype>] [-applicationtype <
    applicationtype>] [-samlSSOProfile <string>]
```

创建 **VPN URL** 操作

在命令提示窗口中，键入以下内容：

```
add vpn urlAction <name> -linkName <string> -actualURL <string> [-
    vServerName <string>] [-clientlessAccess ( ON | OFF )] [-comment <
    string>] [-iconURL <URL>] [-ssotype <ssotype>] [-applicationtype <
    applicationtype>] [-samlSSOProfile <string>]
```

创建 **VPN URL** 操作

在命令提示窗口中，键入以下内容：

```
add vpn urlAction <name> -linkName <string> -actualURL <string> [-
    vServerName <string>] [-clientlessAccess ( ON | OFF )] [-comment <
    string>] [-iconURL <URL>] [-ssotype <ssotype>] [-applicationtype <
    applicationtype>] [-samlSSOProfile <string>]
```

支持 **VPN URL** 操作的以下操作

- **add**

```
add vpn urlAction <name> -linkName <string> -actualURL <string> [-
    vServerName <string>] [-clientlessAccess ( ON | OFF )] [-
    comment <string>] [-iconURL <URL>] [-ssotype <ssotype>] [-
    applicationtype <applicationtype>] [-samlSSOProfile <string>]
```


- **set**

```
set vpn urlAction <name> [-vServerName <string>] [-
    clientlessAccess ( ON | OFF )] [-comment <string>] [-iconURL <
    URL>] [-ssotype <ssotype>] [-applicationtype <applicationtype>]
     [-samlSSOProfile <string>]
```

- **unset**

```
unset vpn urlAction <name> [-vServerName] [-clientlessAccess] [-
    comment] [-iconURL] [-ssotype] [-applicationtype] [-
    samlSSOProfile]
```

- **show**

```
show vpn urlAction [<name>]
```

- **remove**

```
remove vpn urlAction <name>
```

- **rename**

```
rename vpn urlAction <name>@ <newName>@
```

支持 **VPN URL** 策略的以下操作

- **add**

```
add vpn urlPolicy <name> -rule <expression> -action <string> [-
    comment <string>] [-logAction <string>]
```

- **set**

```
set vpn urlPolicy <name> [-rule <expression>] [-action <string>]
    [-comment <string>] [-logAction <string>]
```

- **unset**

```
unset vpn urlPolicy <name> [-comment] [-logAction]
```

- **show**


```
show vpn urlPolicy [<name>]
```

- **remove**

```
remove vpn urlPolicy <name>
```

- **rename**

```
rename vpn urlpolicy <name>@ <newName>@
```

- **stat**

```
stat vpn urlpolicy [<name>] [-detail] [-fullValues] [-ntimes <
    positive_integer>] [-logFile <input_filename>] [-clearstats (
    basic | full )]
```

- **bind**

```
bind vpn vserver <vserver name> -policy <string> -priority <
    positive_integer> [-gotoPriorityExpression <expression>]
bind vpn global -policyName <string> -priority <positive_integer>
    [-gotoPriorityExpression <expression>]
bind aaa user <userName> -policy <string> [-priority <
    positive_integer>] [-type <type>] [-gotoPriorityExpression <
    expression>]
bind aaa group <groupName> -policy <string> [-priority <
    positive_integer>] [-type <type>] [-gotoPriorityExpression <
    expression>]
```

- **unbind**

```
unbind vpn vserver <name> -policy <string>
unbind vpn global -policyName <string>
unbind aaa user <name> -policy <string>
unbind aaa group <name> -policy <string>
```

注意：绑定点是安全用户，安全用户，vpnvserver 和 vpnglobal。

配置终端策略

September 26, 2019

端点分析是一种扫描用户设备并检测信息的过程，例如操作系统以及防病毒软件、防火墙或 Web 浏览器软件的存在和版本级别。您可以使用端点分析来验证用户设备是否符合您的要求，然后允许其连接到您的网络或在用户登录后保持连接。您可以在用户会话期间监视用户设备上的文件、进程和注册表项，以确保设备继续满足要求。

终端节点策略的工作原理

April 6, 2020

您可以将 Citrix Gateway 配置为在用户登录之前检查用户设备是否满足某些安全要求。这称为预身份验证策略。您可以将 Citrix Gateway 配置为检查用户设备是否存在防病毒、防火墙、反垃圾邮件、进程、文件、注册表项、Internet 安全或您在策略中指定的操作系统。如果用户设备未能进行身份验证预扫描，则不允许用户登录。

如果需要配置未在预身份验证策略中使用的其他安全要求，请配置会话策略并将其绑定到用户或组。此类策略称为身份验证后策略，该策略在用户会话期间运行，以确保所需项目（如防病毒软件或进程）仍然为真。

配置预身份验证或身份验证后策略时，Citrix Gateway 会下载端点分析插件，然后运行扫描。每次用户登录时，端点分析插件都会自动运行。

您可以使用以下三种类型的策略配置终端节点策略：

- 使用是或否参数的预身份验证策略。扫描将确定用户设备是否满足指定的要求。如果扫描失败，用户将无法在登录页面上输入凭据。
- 具有条件且可用于 SmartAccess 的会话策略。
- 会话策略中的客户端安全表达式。如果用户设备未能满足客户端安全表达式的要求，则可以将用户配置为放入隔离组。如果用户设备通过扫描，则可将用户置于另一个可能需要进行额外检查的组中。

您可以将检测到的信息合并到策略中，从而使您能够根据用户设备授予不同级别的访问权限。例如，您可以为从具有当前防病毒和防火墙软件要求的用户设备远程连接的用户提供具有下载权限的完全访问权限。对于从不受信任的计算机连接的用户，您可以提供更受限制的访问级别，允许用户在远程服务器上编辑文档而无需下载文档。

端点分析执行以下基本步骤：

- 检查有关用户设备的初始信息集，以确定应用哪些扫描。
- 运行所有适用的扫描。当用户尝试连接时，端点分析插件会检查用户设备是否符合预身份验证或会话策略中指定的要求。如果用户设备通过扫描，则允许用户登录。如果用户设备扫描失败，则不允许用户登录。
  注意：端点分析扫描在用户会话使用许可证之前完成。
- 将在用户设备上检测到的属性值与配置扫描中列出的所需属性值进行比较。
- 生成一个输出，验证是否找到所需的属性值。

> 注意：有关创建终端分析策略的说明是一般准则。一个会话策略中可以有多个设置。配置会话策略的具体说明可能包含配置特定设置的说明；但是，该设置可以是会话配置文件和策略中包含的许多设置之一。

评估用户登录选项

April 6, 2020

用户登录时，他们可以选择跳过端点分析扫描。如果用户跳过扫描，Citrix Gateway 将此操作作为失败的终端分析进行处理。当用户扫描失败时，他们只能访问 Web Interface 或通过无客户端访问。

例如，您希望使用 Citrix Gateway 插件为用户提供访问权限。要使用该插件登录 Citrix Gateway，用户必须运行防病毒应用程序，如诺顿防病毒软件。如果用户设备未运行应用程序，则用户只能使用 Receiver 登录并使用已发布的应用程序。您还可以配置无客户端访问，这将限制对指定应用程序（例如 Outlook Web Access）的访问。

要将 Citrix Gateway 配置为实现此登录方案，请将限制性会话策略分配为默认策略。然后，您可以配置设置，以便在用户设备通过端点分析扫描时将用户升级到特权会话策略。此时，用户具有网络层访问权限，并可以使用 Citrix Gateway 插件登录。

要将 Citrix Gateway 配置为首先强制执行限制性会话策略，请执行以下步骤：

- 如果指定的应用程序未在用户设备上运行，则配置启用 ICA 代理的全局设置和所有其他必要设置。
- 创建启用 Citrix Gateway 插件的会话策略和配置文件。
- 在会话策略的规则部分中创建一个表达式以指定应用程序，例如：

  （client.application.process(symantec.exe) 存在）

用户登录时，首先应用会话策略。如果终端分析失败或用户跳过扫描，Citrix Gateway 将忽略会话策略中的设置（会话策略中的表达式视为 false）。因此，用户可以使用 Web Interface 或无客户端访问限制访问权限。如果通过端点分析，Citrix Gateway 将应用会话策略，用户对 Citrix Gateway 插件具有完全访问权限。

设置预身份验证策略的优先级

April 6, 2020

您可以拥有绑定到不同级别的多个预身份验证策略。例如，您有一个策略，用于检查绑定到 AAA Global 的特定防病毒应用程序和绑定到虚拟服务器的防火墙策略。用户登录时，首先应用绑定到虚拟服务器的策略。在 AAA 全局绑定的策略将第二次应用。

您可以更改预身份验证扫描的顺序。要使 Citrix Gateway 首先应用全局策略，请更改绑定到虚拟服务器的策略的优先级号，使其具有高于全局绑定策略的优先级号。例如，将全局策略的优先级号设置为 1，将虚拟服务器策略设置为 2。用户登录时，Citrix Gateway 首先运行全局策略扫描，然后运行虚拟服务器策略扫描。

更改预身份验证策略的优先级

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。

2. 在详细信息窗格中，选择虚拟服务器，然后单击“打开”。
3. 在“策略”选项卡上，单击“预身份验证”。
4. 在“优先级”下，键入策略的优先级号，然后单击“确定”。

配置预身份验证策略和配置文件

January 10, 2023

> 警告
>
> 从 NetScaler 12.0 版本 56.20 版本开始，AAA 预身份验证策略已弃用，作为替代方案，Citrix 建议您使用 nFactor 身份验证。有关更多信息，请参阅多因素 (nFactor) 身份验证主题。

您可以将 Citrix Gateway 配置为在用户进行身份验证之前检查客户端安全性。此方法可确保与 Citrix Gateway 建立会话的用户设备符合您的安全要求。您可以通过使用特定于虚拟服务器或全局的预身份验证策略来配置客户端安全检查，如以下两个过程所述。

预身份验证策略由配置文件和表达式组成。配置配置文件以使用操作允许或拒绝在用户设备上执行进程。例如，文本文件，clienttext.txt，正在用户设备上运行。当用户登录到 Citrix Gateway 时，如果文本文件正在运行，则可以允许或拒绝访问。如果您不希望允许用户登录，如果进程正在运行，请配置配置文件，以便在用户登录之前停止进程。

您可以为预身份验证策略配置以下设置：

- 表达式。包括以下设置以帮助您创建表达式：
  - 表达式。显示所有创建的表达式。
  - 匹配任何表达式。配置策略以匹配所选表达式列表中存在的任何表达式。
  - 匹配所有表达式。配置策略以匹配所选表达式列表中存在的所有表达式。
  - 表格表达式。使用 OR (||) 或 AND (&&) 运算符创建具有现有表达式的复合表达式。
  - 高级自由形状。使用表达式名称以及 OR (||) 和 AND (&&) 运算符创建自定义复合表达式。仅选择需要的表达式，并从选定表达式列表中省略其他表达式。
  - 添加。创建新表达式。
  - 修改。修改现有表达式。
  - 删除。从复合表达式列表中删除选定的表达式。
  - 命名表达式。选择已配置的命名表达式。您可以从 Citrix Gateway 上已存在的表达式下拉列表中选择命名表达式。
  - 添加表达式。将选定的命名表达式添加到策略中。
  - 替换表达式。将选定的命名表达式替换为策略。
  - 预览表达式。显示选择命名表达式时将在 Citrix Gateway 上配置的详细客户端安全字符串。

使用配置实用程序全局配置预身份验证配置文件

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。

2. 在详细信息窗格的“设置”下，单击“更改预身份验证设置”。
3. 在“全局预身份验证设置”对话框中，配置设置：
   a) 在“操作”中，选择“允许”或“拒绝”。
      在端点分析发生后拒绝或允许用户登录。
   b) 在要取消的进程中，输入流程。
      这将指定要由端点分析插件停止的进程。
   c) 在要删除的文件中，输入文件名。
      这将指定要由端点分析插件删除的文件。
4. 在表达式中，您可以保留表达式 ns_true 或为特定应用程序（如防病毒软件或安全软件）构建表达式，然后单击“确定”。

使用配置实用程序配置预身份验证配置文件

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“Citrix Gateway”>“策略”>“身份验证/授权”，然后单击“预身份验证 EPA”。
2. 在详细信息窗格中的配置文件选项卡上，单击添加。
3. 在“名称”中，键入要检查的应用程序的名称。
4. 在“操作”中，选择“允许”或“拒绝”。
5. 在要取消的进程中，键入要停止的进程的名称。
6. 在要删除的文件中，键入要删除的文件的名称，如 c:clientext.txt，单击创建，然后单击关闭。

> 注意：如果要删除文件或进程停止，用户会收到一条消息，要求确认。步骤 5 和 6 是可选参数。

如果您使用配置实用程序配置预身份验证配置文件，则通过单击“策略”选项卡上的“添加”来创建预身份验证策略。在“创建预身份验证策略”对话框中，从“请求配置文件”下拉列表中选择配置文件。

配置端点分析表达式

April 6, 2020

预身份验证和客户端安全会话策略包括配置文件和表达式。策略可以有一个配置文件和多个表达式。要扫描用户设备中的应用程序、文件、进程或注册表项，请在策略中创建表达式或复合表达式。

表达式类型

表达式由表达式类型和表达式的参数组成。表达式类型包括：

- 常规
- 客户安全
- 基于网络的

将预配置的表达式添加到预身份验证策略

Citrix Gateway 附带预配置的表达式，称为命名表达式。配置策略时，您可以为策略使用命名表达式。例如，您希望预身份验证策略检查 Symantec AntiVirus 10 是否具有更新的病毒定义。创建预身份验证策略并添加表达式，如以下过程中所述。

创建预身份验证或会话策略时，可以在创建策略时创建表达式。然后，您可以使用表达式将策略应用于虚拟服务器或全局。

以下过程介绍如何使用配置实用程序将预配置的防病毒表达式添加到策略中。

将命名表达式添加到预身份验证策略

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”>“身份验证/授权”，然后单击 “预身份验证 EPA”。
2. 在详细信息窗格中，选择一个策略，然后单击打开。
3. 在命名表达式旁边，选择防病毒，从列表中选择防病毒产品，单击添加表达式，单击创建，然后单击关闭。

配置自定义表达式

April 6, 2020

自定义表达式是您在策略中创建的表达式。创建表达式时，可以配置表达式的参数。

您还可以创建自定义客户端安全表达式来引用常用的客户端安全字符串。这简化了配置预身份验证策略的过程以及维护已配置的表达式的过程。

例如，您希望为 Symantec AntiVirus 10 创建自定义客户端安全表达式，并确保病毒定义不超过三天。创建新策略，然后配置表达式以指定病毒定义。

以下过程显示如何在预身份验证策略中创建客户端安全策略。您可以在会话策略中使用相同的步骤。

创建预身份验证策略和自定义客户端安全表达式

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”>“身份验证/授权”，然后单击 “预身份验证 EPA”。
2. 在详细信息窗格中，单击 Add（添加）。此时将打开 “创建预身份验证策略” 对话框。
3. 在 “名称” 中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在 “创建身份验证配置文件” 对话框的 “名称” 中，键入配置文件的名称，然后在 “操作” 中，选择 “允许”，然后单击 “创建”。
6. 在 “创建预身份验证策略” 对话框中，在 “匹配任何表达式” 旁边，单击 “添加”。
7. 在 “表达式类型” 中，选择 “客户端安全”。

8. 配置以下内容：
   a) 在组件中，选择防病毒。
   b) 在“名称”中，键入应用程序的名称。
   c) 在限定符中，选择版本。
   d) 在“运算符”中，选择 = =。
   e) 在“值”中，键入值。
   f) 在“新鲜度”中，键入 3，然后单击“确定”。
9. 在“创建预身份验证策略”对话框中，单击“创建”，然后单击“关闭”。

配置自定义表达式时，会将其添加到策略对话框中的“表达式”框中。

配置复合表达式

April 6, 2020

预身份验证策略可以有一个配置文件和多个表达式。如果配置复合表达式，则可以使用运算符指定表达式的条件。例如，您可以配置复合表达式以要求用户设备运行以下防病毒应用程序之一：

- Symantec Antivirus 10
- McAfee Antivirus 11
- Sophos Antivirus 4

使用 OR 运算符配置表达式以检查前三个应用程序。如果 Citrix Gateway 检测到用户设备上任何应用程序的正确版本，则允许用户登录。策略对话框中的表达式显示如下：

av_5_Symantec_1	av_5_McAfeevirus	av_5_sophos_4

有关复合表达式的更多信息，请参阅配置复合表达式。

绑定预身份验证策略

April 6, 2020

创建预身份验证或客户端安全会话策略后，将策略绑定到应用该策略的级别。您可以将预身份验证策略绑定到虚拟服务器或全局。

全局创建和绑定预身份验证策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。

2. 在详细信息窗格中，单击更改预身份验证设置。
3. 在“全局预身份验证设置”对话框的“操作”中，选择“允许”或“拒绝”。
4. 在“名称”中，键入策略的名称。
5. 在“全局身份验证前 settigns”对话框中，在命名表达式旁边，选择“常规”，选择“真值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

将预身份验证策略绑定到虚拟服务器

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，选择虚拟服务器，然后单击“打开”。
3. 在“配置 Citrix Gateway 虚拟服务器”对话框中，单击“策略”选项卡，然后单击“预身份验证”。
4. 在“详细信息”下，单击“插入策略”，然后在“策略名称”下，选择预身份验证策略。
5. 单击确定。

解除绑定和删除预身份验证策略

April 6, 2020

如有必要，您可以从 Citrix Gateway 中删除预身份验证策略。删除预身份验证策略之前，请从虚拟服务器或全局取消绑定。

取消绑定全局预身份验证策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“Citrix Gateway”>“策略”>“身份验证/授权”，然后单击“预身份验证 EPA”。
2. 在详细信息窗格中，选择一个策略，然后在操作中单击全局绑定。
3. 在“绑定/解除绑定到全局的身份验证前策略”对话框中，选择一个策略，单击“取消绑定策略”，然后单击“确定”。

从虚拟服务器取消绑定预身份验证策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 在“配置 Citrix Gateway 虚拟服务器”对话框中，单击“策略”选项卡，然后单击“预身份验证”。
3. 选择策略，然后单击取消绑定策略。

取消绑定预身份验证策略后，您可以从 Citrix Gateway 中删除该策略。

删除预身份验证策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“Citrix Gateway”>“策略”>“身份验证/授权”，然后单击“预身份验证 EPA”。
2. 在详细信息窗格中，选择一个策略，然后单击“删除”。

配置身份验证后策略

April 6, 2020

身份验证后策略是用户设备必须满足的一组通用规则，才能保持会话处于活动状态。如果策略失败，与 Citrix Gateway 的连接将结束。配置身份验证后策略时，您可以配置任何可以成为条件的用户连接的设置。

> 注意：此功能仅适用于 Citrix Gateway 插件。如果用户使用 Citrix Workspace 应用程序登录，则终端分析扫描仅在登录时运行。

您可以使用会话策略配置身份验证后策略。首先，创建策略应用到的用户。然后，您将用户添加到组。接下来，将会话、流量策略和 Intranet 应用程序绑定到该组。

您还可以指定组作为授权组。此类型的组允许您根据会话策略中的客户端安全表达式将用户分配给组。

如果用户设备不符合策略的要求，您还可以配置身份验证后策略以将用户置于隔离组中。简单的策略包括客户端安全表达式和客户端安全消息。当用户位于隔离组中时，用户可以登录到 Citrix Gateway；但是，他们获得对网络资源的有限访问权限。

无法使用相同的会话配置文件和策略创建授权组和隔离组。创建身份验证后策略的步骤相同。创建会话策略时，您可以选择授权组或隔离组。您可以创建两个会话策略并将每个策略绑定到组。

身份验证后策略也与 SmartAccess 一起使用。有关 SmartAccess 的更多信息，请参阅在 Citrix Gateway 上配置 SmartAccess。

配置身份验证后策略

April 6, 2020

您可以使用会话策略配置身份验证后策略。简单的策略包括客户端安全表达式和客户端安全消息。

配置身份验证后策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway >** 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。

4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在“安全”选项卡上，单击“高级设置”。
7. 在“客户端安全”下，单击“覆盖全局”，然后单击“新建”。
8. 配置客户端安全表达式，然后单击创建。
9. 在“客户端安全”下的“隔离组”中，选择一个组。
10. 在错误消息中，键入您希望用户在身份验证后扫描失败时收到的消息。
11. 在授权组下，单击覆盖全局，选择一个组，单击添加，单击确定，然后单击创建。
12. 在“创建会话策略”对话框的命名表达式旁边，选择“常规”，选择“True”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置身份验证后扫描的频率

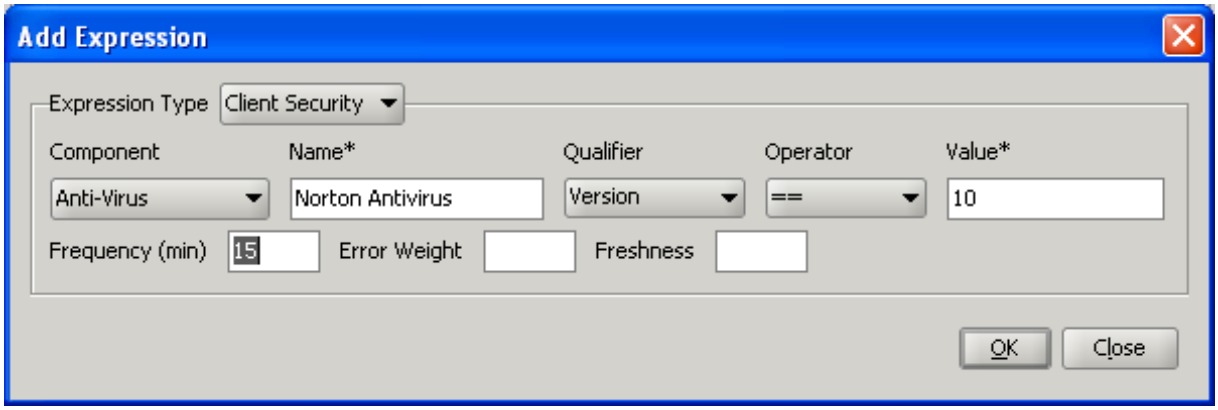
April 6, 2020

您可以将 Citrix Gateway 配置为按指定间隔运行身份验证后策略。例如，您配置了客户端安全策略，并希望该策略每 10 分钟在用户设备上运行一次。您可以通过在策略中创建自定义表达式来配置此频率。

> 注意：身份验证后策略的频率检查功能仅适用于 Citrix Gateway 插件。如果用户使用 Citrix Workspace 应用程序登录，则终端分析扫描仅在登录时运行。

您可以按照步骤在配置客户端安全策略时设置频率（以分钟为单位）配置身份验证后策略。下图显示了可以在“添加表达式”对话框中输入频率值的位置。

图 1. 用于配置身份验证后扫描频率的对话框



配置隔离和授权组

April 6, 2020

当用户登录到 Citrix Gateway 时，您将其分配给您在 Citrix Gateway 或安全网络中的身份验证服务器上配置的组。如果用户未能进行身份验证后扫描，则可以将该用户分配到被限制的组（称为隔离组），该组限制对网络资源的访问。

您还可以使用授权组限制用户对网络资源的访问。例如，您可能有一组合同人员只能访问您的电子邮件服务器和文件共享。当用户设备通过您在 Citrix Gateway 上定义的安全要求时，用户可以动态地成为组的成员。

您可以使用全局设置或会话策略来配置绑定到用户、组或虚拟服务器的隔离和授权组。您可以根据会话策略中的客户端安全表达式将用户分配到组。当用户是组的成员时，Citrix Gateway 会根据组成员身份应用会话策略。

配置隔离组

April 6, 2020

配置隔离组时，可以使用会话配置文件中的“安全设置-高级设置”对话框配置客户端安全表达式。

配置隔离组的客户端安全表达式

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在“安全”选项卡上，单击“高级设置”。
7. 在“客户端安全”下，单击“覆盖全局”，然后单击“新建”。
8. 在“客户端表达式”对话框中，配置客户端安全表达式，然后单击“创建”。
9. 在隔离组中，选择组。
10. 在错误消息中，键入描述用户问题的消息，然后单击创建。
11. 在“创建会话策略”对话框的命名表达式旁边，选择“常规”，选择“True”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

创建会话策略后，将其绑定到用户、组或虚拟服务器。

> 注意
>
> 如果终端分析扫描失败，并且用户被置于隔离组中，则仅当没有直接绑定到与绑定到隔离组的策略具有等于或低于绑定到隔离组的策略的用户的策略时，绑定到隔离组的策略才有效。

配置全局隔离组

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“安全”选项卡上，单击“高级设置”。

4. 在“客户端安全”中，配置客户端安全表达式。
5. 在隔离组中，选择组。
6. 在错误消息中，键入描述用户问题的消息，然后单击确定。

配置授权组

April 6, 2020

配置端点分析扫描时，可以在用户设备通过扫描时动态将用户添加到授权组。例如，您创建检查用户设备域成员身份的终端分析扫描。在 Citrix Gateway 上，创建名为“加入域的计算机”的本地组，并将其添加为通过扫描的任何人的授权组。当用户加入组时，用户将继承与组关联的策略。

您不能将授权策略全局绑定或绑定到虚拟服务器。当用户未配置为 Citrix Gateway 上的另一个组的成员时，可以使用授权组提供一组默认授权策略。

使用会话策略配置授权组

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在“安全”选项卡上，单击“高级设置”。
7. 在授权组下，单击覆盖全局，从下拉列表中选择一个组，单击添加，单击确定，然后单击创建。
8. 在“创建会话策略”对话框的命名表达式旁边，选择“常规”，选择“True”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

创建会话策略后，您可以将其绑定到用户、组或虚拟服务器。

配置全局授权组

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“安全”选项卡上，单击“高级设置”。
4. 在授权组下，从下拉列表中选择一个组，单击添加，然后单击确定两次。

如果要全局或从会话策略中删除授权组，请在“安全设置-高级”对话框中，从列表中选择授权组，然后单击“删除”。

为用户设备配置安全预身份验证表达式

April 6, 2020

Citrix Gateway 在用户登录期间或在会话期间的其他配置时间提供各种终端安全检查，以帮助提高安全性。只有通过这些安全检查的用户设备才能建立 Citrix Gateway 会话。

以下是可以在 Citrix Gateway 上配置的用户设备上的安全检查类型：

- 反垃圾邮件
- 防病毒
- 文件策略
- 網路安全
- 操作系统
- 个人防火墙
- 流程政策
- 登记处政策
- 服务策略

如果用户设备上的安全检查失败，则在后续检查通过之前不会建立新连接（如果是定期检查）；但是，流过现有连接的流量将继续通过 Citrix Gateway 进行隧道。

您可以使用配置实用程序在会话策略中配置预身份验证策略或安全表达式，这些策略旨在对用户设备执行安全检查。

配置防病毒、防火墙、**Internet** 安全或反垃圾邮件表达式

April 6, 2020

您可以在“添加表达式”对话框中配置防病毒、防火墙、Internet 安全和反垃圾邮件策略的设置。每个策略的设置相同：差异是您选择的值。例如，如果要检查用户设备是否有 Norton AntiVirus Version 10 和 ZoneAlarm Pro，则可以在会话或预身份验证策略中创建两个表达式，用于指定每个应用程序的名称和版本号。

选择“客户端安全”作为表达式类型时，可以配置以下内容：

- 组件：客户端安全的类型，例如防病毒、防火墙或注册表项。
- 名称：应用程序、进程、文件、注册表项或操作系统的名称。
- 限定符：表达式检查的组件的版本或值。
- 运算符：检查值是否存在或等于值。
- 值：用户设备上的防病毒、防火墙、Internet 安全或反垃圾邮件软件的应用程序版本。
- 频率：运行身份验证后扫描的频率（以分钟为单位）。
- 错误权重：当多个表达式具有不同的错误字符串时，为嵌套表达式中包含的每条错误消息分配的权重。权重决定显示哪个错误消息。
- 新鲜度：定义病毒定义的年龄。例如，您可以配置表达式，使病毒定义不超过三天。

将客户端安全策略添加到预身份验证或会话策略

1. 在配置实用程序的导航窗格中，执行以下操作之一：
   a) 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
   b) 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”>“身份验证/授权”，然后单击 “预身份验证 EPA”。
2. 在详细信息窗格的 “策略” 选项卡上，单击 “添加”。
3. 在 “名称” 中，键入策略的名称。
4. 在 “匹配任意表达式” 旁边，单击 “添加”。
5. 在 “添加表达式” 对话框的 “表达式类型” 中，选择 “客户端安全”。
6. 配置以下设置：
   a) 在 “组件” 中，选择要扫描的项目。
   b) 在 “名称” 中，键入应用程序的名称。
   c) 在限定符中，选择版本。
   d) 在 “运算符” 中，选择值。
   e) 在 “值” 中，键入客户端安全字符串，单击 “确定”，单击 “创建”，然后单击 “关闭”。

配置服务策略

April 6, 2020

服务是在用户设备上静默运行的程序。创建会话或预身份验证策略时，可以创建一个表达式，以确保在建立会话时用户设备正在运行特定服务。

配置服务策略

1. 在配置实用程序的导航窗格中，执行以下操作之一：
   a) 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
   b) 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”>“身份验证/授权”，然后单击 “预身份验证 EPA”。
2. 在详细信息窗格的 “策略” 选项卡上，单击 “添加”。
3. 在 “名称” 中，键入策略的名称。
4. 在 “匹配任意表达式” 旁边，单击 “添加”。
5. 在 “添加表达式” 对话框的 “表达式类型” 中，选择 “客户端安全”。
6. 配置以下设置：
   a) 在组件中，选择服务。
   b) 在 “名称” 中，键入服务的名称。
   c) 在限定符中，留空或选择版本。
   d) 根据您在限定符中的选择，执行以下操作之一：

- 如果留空，请在运算符中选择 == 或! =
- 如果您选择了版本，则在运算符的值中键入值，单击确定，然后单击关闭。

您可以在以下位置检查基于 Windows 的计算机上的所有可用服务的列表以及每个服务的状态：

控制面板 > 管理工具 > 服务

> 注意：每个服务的服务名称与其列出的名称不同。通过查看 “
> 属性” 对话框来检查服务的名称。

配置流程策略

April 6, 2020

创建会话或预身份验证策略时，您可以定义要求所有用户设备在用户登录时运行特定进程的规则。该过程可以是任何应用程序，并可以包括定制的应用程序。

注意：Windows 任务管理器的 “进程” 选项卡上显示在基于 Windows 的计算机上运行的所有
进程的列表。

配置进程策略

1. 在配置实用程序的导航窗格中，执行以下操作之一：
   a) 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
   b) 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”>“身份验证/授权”，然后单击 “预身份验证 EPA”。
2. 在详细信息窗格的 “策略” 选项卡上，单击 “添加”。
3. 在 “名称” 中，键入策略的名称。
4. 在 “匹配任意表达式” 旁边，单击 “添加”。
5. 在 “添加表达式” 对话框的 “表达式类型” 中，选择 “客户端安全”。
6. 配置以下设置：
   a) 在 “组件” 中，选择 “处理”。
   b) 在 “名称” 中，键入应用程序的名称。
   c) 在 “运算符” 中，选择 EXISTS 或 NOTEXISTS，单击 “确定”，然后单击 “关闭”。

配置端点分析策略（身份验证前或身份验证后）以检查进程时，可以配置 MD5 校验和。

为策略创建表达式时，您可以将 MD5 校验和添加到要检查的进程。例如，如果您正在检查 notepad.exe 是否正在用户设备上运行，则表达式为：
CLIENT.APPLICATION.PROCESS(notepad.exe_md5_388b8fbc36a8558587afc90fb23a3b00) EXISTS

配置操作系统策略

April 6, 2020

创建会话或预身份验证策略时，可以配置客户端安全字符串，以确定用户设备是否在用户登录时运行特定操作系统。您还可以配置表达式以检查特定的 Service Pack 或修补程序。

Windows 和 Macintosh 的值为：

操作系统	值
Mac OS X	macOS
Windows 8.1	win8.1
Windows 8	win8
Windows 7	win7
Windows Vista	远景
Windows XP	温克普
Windows Server 2008	win2008
Windows Server 2003	win2003
Windows 2000 Server	win2000
Windows 64 位平台	win64

配置操作系统策略

1. 在配置实用程序的导航窗格中，执行以下操作之一：
   a) 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
   b) 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”>“身份验证/授权”，然后单击 “预身份验证 EPA”。
2. 在详细信息窗格的 “策略” 选项卡上，单击 “添加”。
3. 在 “名称” 中，键入策略的名称。
4. 在 “匹配任意表达式” 旁边，单击 “添加”。
5. 在 “添加表达式” 对话框的 “表达式类型” 中，选择 “客户端安全”。
6. 配置以下设置：
   a) 在组件中，选择操作系统。
   b) 在 “名称” 中，键入操作系统的名称。
   c) 在限定符中，执行以下操作之一：
      - 留空。

- 选择服务包。
- 选择修补程序。
- 选择仅适用于 Mac OS X 的版本。

d) 根据您在步骤 C 中的选择，在运算符中执行以下操作之一：

- 如果限定符为空，请在运算符中选择 EQUAL (= =)、NOTEQUAL (!=)、EXISTS 或 NOTEXISTS。
- 如果您选择了 Service Pack 或修补程序，请选择运算符，然后在值中键入值。

7. 单击 Create（创建），然后单击 Close（关闭）。

如果要配置服务包，如 client.os (winxp) .sp，如果数字不在值字段中，Citrix Gateway 将返回错误消息，因为表达式无效。

如果操作系统具有服务包存在，例如补丁 3 和补丁 4，您可以配置只针对补丁 4 的检查，因为补丁 4 的存在会自动指示以前的服务包存在。

配置注册表策略

April 6, 2020

创建会话或预身份验证策略时，可以检查用户设备上是否存在注册表项和值。仅当特定条目存在或具有已配置或更高值时，才会建立会话。

配置注册表达式时，请使用以下准则：

- 四个反斜杠用于分隔关键帧和子项，例如

  HKEY_LOCAL_MACHINE\\\\SOFTWARE

- 下划线用于分隔子项和关联值名称，例如

  HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\VirusSoftware_Version

- 反斜杠 () 用于表示空格，例如以下两个示例：

  HKEY_LOCAL_MACHINE\\\\SOFTWARE\\Citrix\\\\Secure\ Access\ Client_ProductVersion

  CLIENT.REG(HKEY_LOCAL_MACHINE\\\\Software\\\\Symantec\\Norton\ AntiVirus_Version).VALUE == 12.8.0.4 -frequency 5

以下是用户登录时查找 Citrix Gateway 插件注册表项的注册表达式：

CLIENT.REG(secureaccess).VALUE==HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\CITRIX\\\\Secure\Access\Client_Pro

> 注意：如果您正在扫描注册
> 表项和值，并在表达式对话框中选择
> 高级自由格式，则表达式必须以
> CLIENT.REG 开头

以下最常见的五种类型支持注册表检查：

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

要检查的注册表值使用以下类型：

- 字符串

  对于字符串值类型，检查区分大小写。

- DWORD

  对于 DWORD 类型，该值进行比较，并且必须相等。

- 扩展的字符串

  不支持其他类型，如二进制和多字符串。

- 只支持 '==' 比较运算符。
- 不支持其他比较运算符，如 <、> 和区分大小写的比较。
- 总注册表字符串长度应小于 256 字节。

您可以向表达式添加值。该值可以是软件版本、Service Pack 版本或任何其他值出现在注册表中。如果注册表中的数据值与您测试的值不匹配，用户将被拒绝登录。

> 注意：您无法扫描子项中的值。扫描必须与命名值和关联的数据值匹配。

配置注册表策略

1. 在配置实用程序的导航窗格中，执行以下操作之一：
   a) 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
   b) 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”>“身份验证/授权”，然后单击 “预身份验证 EPA”。
2. 在详细信息窗格的 “策略” 选项卡上，单击 “添加”。
3. 在 “名称” 中，键入策略的名称。
4. 在 “匹配任意表达式” 旁边，单击 “添加”。
5. 在 “添加表达式” 对话框的 “表达式类型” 中，选择 “客户端安全”。
6. 配置以下设置：
   a) 在组件中，选择注册表。
   b) 在 “名称” 中，键入注册表项的名称。
   c) 在限定符中，留空或选择 “值”。
   d) 在运算符中，执行以下操作之一：
      - 如果限定符留空，请选择 EXISTS 或 NOTEXISTS

- 如果您选择了限定符中的值，请选择 == 或! ==

e) 在“值”中，键入在注册表编辑器中显示的值，单击“确定”，然后单击“关闭”。

配置复合客户端安全表达式

November 7, 2022

您可以组合客户端安全字符串以形成复合客户端安全表达式。

Citrix Gateway 中支持的布尔运算符有：

- 和 (&)
- 或者 (||)
- 不是 (!)

为了获得更高的精度，您可以使用括号将字符串分组在一起。

> 注意：如果您使用命令行配置表达式，请在构成复合表达式时使用括号将安全表达式分组在一起。使用括号可改善客户端表达式的理解和调试。

使用 **AND (&&)** 运算符配置策略

AND (&&) 运算符通过组合两个客户端安全字符串来工作，以便复合检查仅在两个检查都为真时通过。表达式从左到右求值，如果第一次检查失败，则不执行第二次检查。

您可以使用关键字 ‘AND’ 或符号 ‘&’ 来配置 AND (&&) 运算符。

示例：

以下是客户端安全检查，用于确定用户设备是否已安装并运行 Sophos AntiVirus 7.0 版本。它还检查 netlogon 服务是否在同一台计算机上运行。

CLIENT.APPLICATION.AV(sophos).version==7.0 AND CLIENT.SVC(netlogon) EXISTS

此字符串也可以配置为：

CLIENT.APPLICATION.AV(sophos).version==7.0 && CLIENT.SVC(netlogon) EXISTS

使用 **OR (||)** 运算符配置策略

OR (	）运算符通过组合两个安全字符串来工作。复合校验在任一校验为真时通过。表达式从左到右求值，如果第一次检查通过，则不执行第二次检查。如果第一次检查没有通过，则进行第二次检查。

您可以配置或（	) 运算符使用关键字 ‘OR’ 或符号 ‘	’.

示例:

以下是一个客户端安全检查，用于确定用户设备上是否具有文件 c: file.txt 还是在其上运行 putty.exe 进程。

client.file(c:\\\\file.txt) EXISTS) OR (client.proc(putty.exe) EXISTS

此字符串也可以配置为

client.file(c:\\\\file.txt) EXISTS)	(client.proc(putty.exe) EXISTS

使用不配置策略 **(!)** 运算符

不是（!）或否定运算符否定客户端安全字符串。

示例:

如果文件 c: sophos_virus_defs.dat 文件不超过两天，则会通过以下客户端安全检查：

!(client.file(c:\\\\sophos_virus_defs.dat).timestamp==2dy)

高级端点分析扫描

April 6, 2020

高级终端点分析 (EPA) 用于扫描用户设备以了解 Citrix Gateway 设备上配置的终端安全要求。如果用户设备尝试访问 Citrix Gateway 设备，则在管理员授予对 Citrix Gateway 设备的访问权限之前，会扫描设备以获取操作系统、防病毒、Web 浏览器版本等安全信息。

高级 EPA 扫描是一种基于策略的扫描，您可以在 Citrix Gateway 设备上为身份验证前和身份验证后会话配置该扫描。该策略在用户设备上执行注册表检查，根据评估，该策略允许或拒绝访问 Citrix ADC 网络。

您可以执行两种类型的 EPA 扫描：OPSWAT 扫描和系统扫描。以下部分介绍扫描类型及其详细信息。

OPSWAT 扫描。扫描机制在不同级别提供安全性，例如：

- 商品特定扫描
- 供应商特定扫描
- 通用扫描

产品特定扫描：您可以为特定产品配置扫描标准（例如 **Avast!** 免费杀毒软件）由特定供应商（例如 **AVAST** 软件 **a.s**.）针对某一类别（例如防病毒软件）提供。访问权限仅授予满足指定条件的计算机。 **

供应商特定的扫描：您可以为某个类别的特定供应商（例如 **AVAST** 软件 **A.s**.）配置扫描条件（例如：杀毒软件）。配置的扫描检查供应商提供的所有产品的指定条件。访问权限仅授予满足指定条件的计算机。

通用扫描：您可以为特定类别配置扫描条件（例如，杀毒软件）。配置的扫描检查所有供应商和供应商提供的产品的指定条件。访问权限仅授予满足指定条件的计算机。

系统扫描。系统扫描为系统级别属性（如 MAC 地址）提供安全性。您可以为系统属性（例如 **MAC** 地址）配置扫描条件。访问权限仅授予满足指定条件的计算机。

配置高级端点分析扫描

January 10, 2023

您可以配置两种类型的 EPA 扫描：OPSWAT 扫描和系统扫描。

配置 **OPSWAT** 扫描

在 Citrix Gateway 设备上配置了以下 OPSWAT 扫描。

- 商品特定扫描
- 供应商特定扫描
- 通用扫描

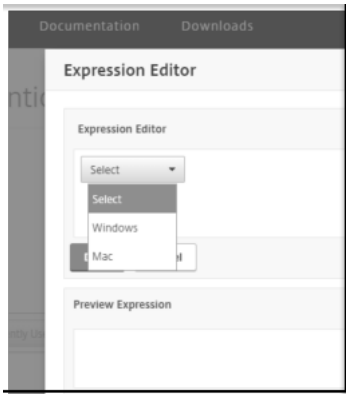
注意：特定产品支持的扫描将显示在 GUI 中。此外，以下 OPSWAT 扫描配置将预身份验证 EPA 作为示例。OPSWAT 扫描也可以配置为身份验证后 EPA。

配置产品特定的 **OPSWAT** 扫描

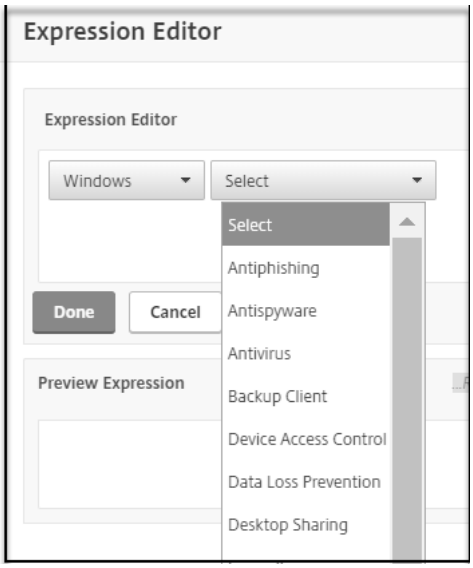
要使用 NetScaler GUI 配置产品特定的 OPSWAT 扫描，请执行以下操作：

1. 导航到配置 **> Citrix NetScaler >** 全局设置。

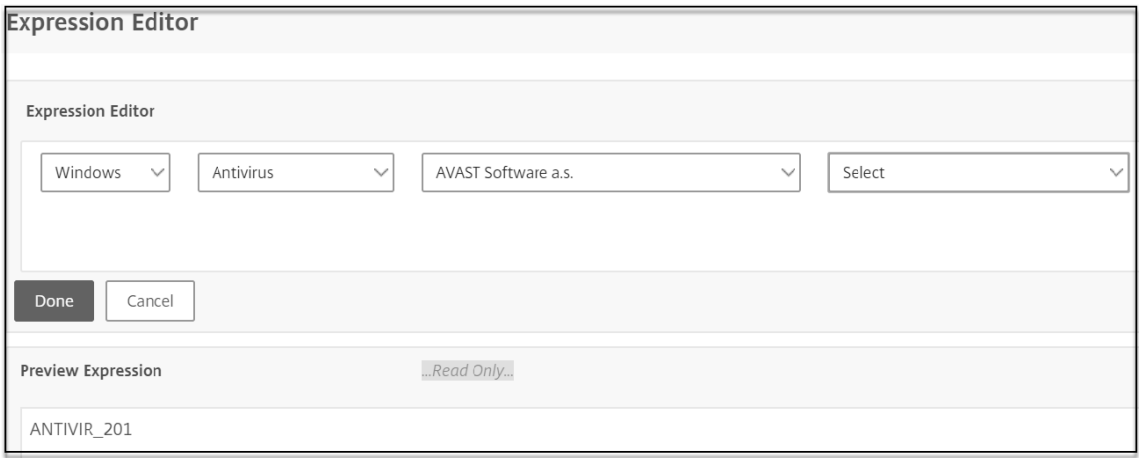
2. 在“全局设置”页上，单击“更改预身份验证设置”链接。
3. 在配置 **AAA** 预身份验证参数页面上，单击 **OPSWAT EPA** 编辑器链接。
4. 在“表达式编辑器”区域下，选择操作系统。



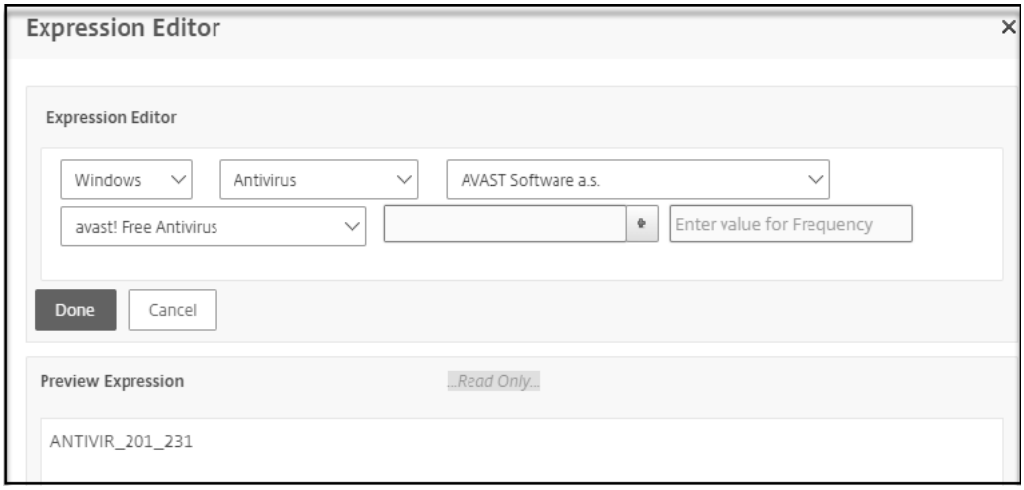
5. 选择类别，例如 防病毒软件。



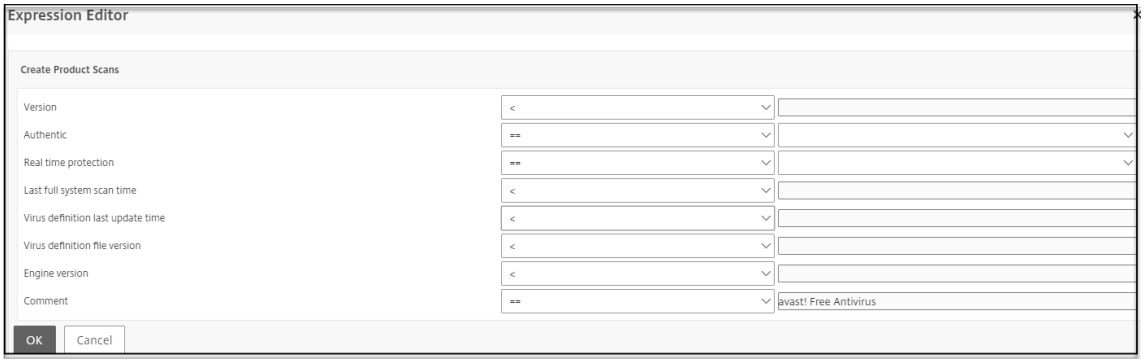
6. 选择供应商，例如 **AVAST** 软件。



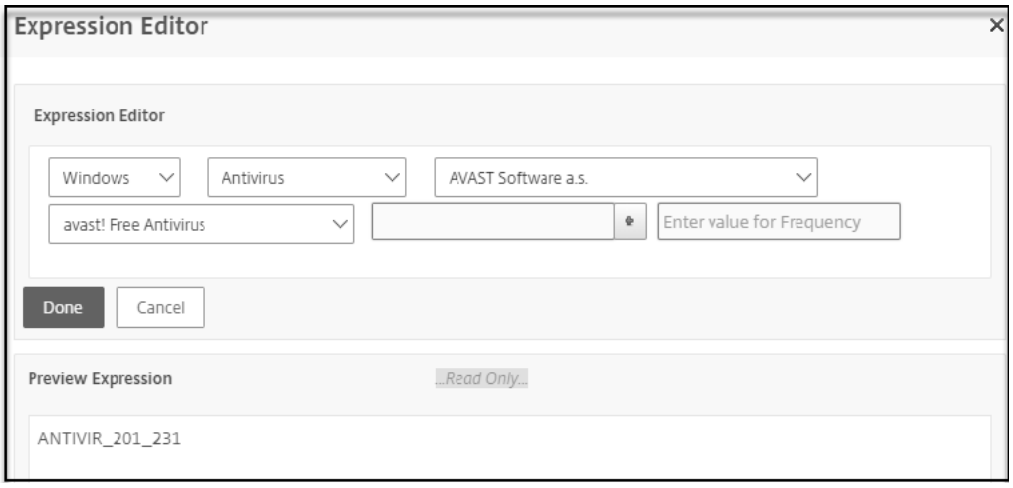
7. 选择产品，例如 **Avast**！免费杀毒软件。



8. 单击产品下拉菜单旁边的 **+** 以配置产品扫描。



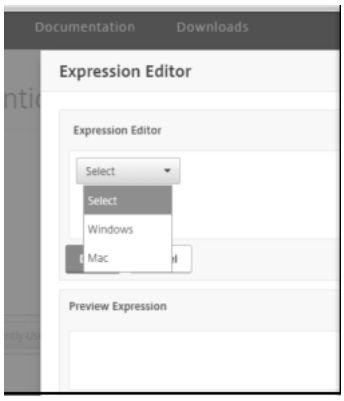
9. 如果需要定期扫描，则可选择输入扫描频率值。



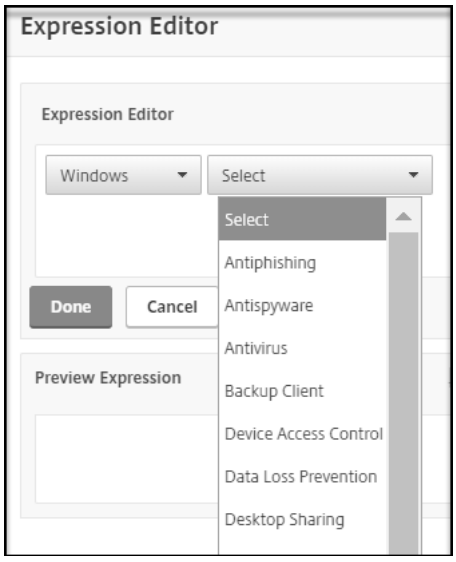
配置供应商特定的 **OPSWAT** 扫描

要使用 NetScaler GUI 配置供应商特定的 OPSWAT 扫描，请执行以下操作：

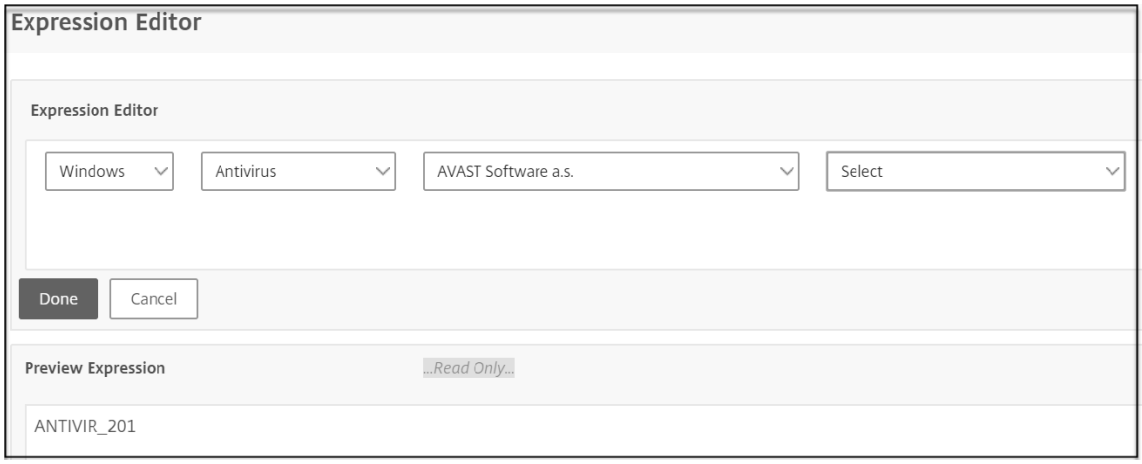
1. 导航到配置 **> Citrix NetScaler >** 全局设置。
2. 在“全局设置”页上，单击“更改预身份验证设置”链接。
3. 在配置 **AAA** 预身份验证参数页面上，单击 **OPSWAT EPA** 编辑器链接。
4. 在“表达式编辑器”区域下，选择操作系统。



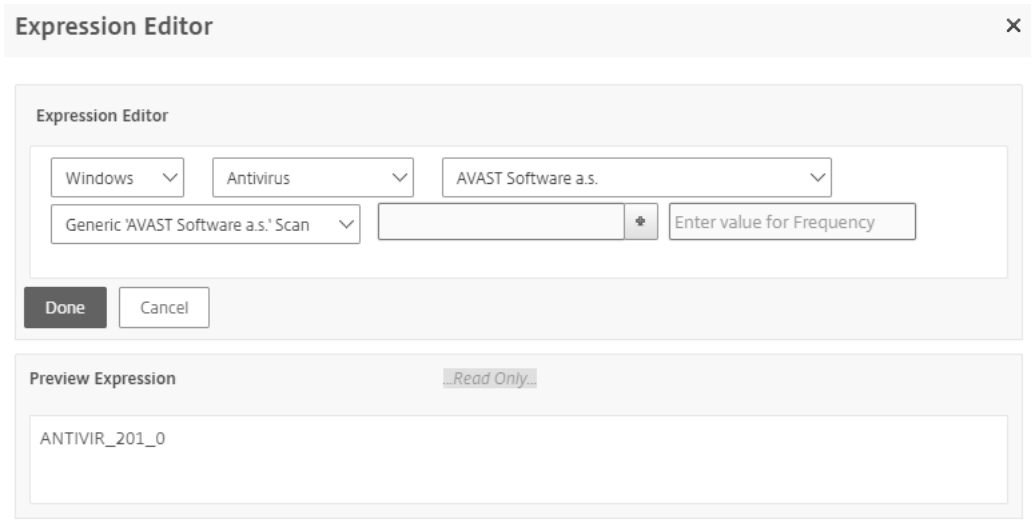
5. 选择类别，例如 防病毒软件。



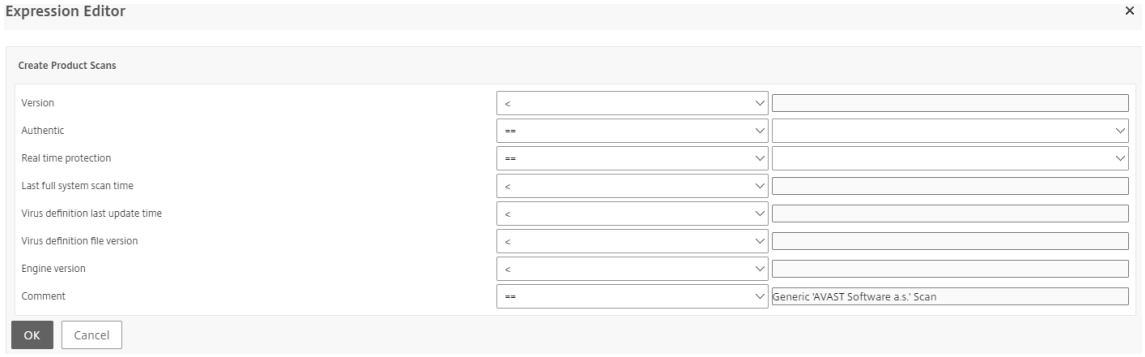
6. 选择供应商，例如 **AVAST** 软件。



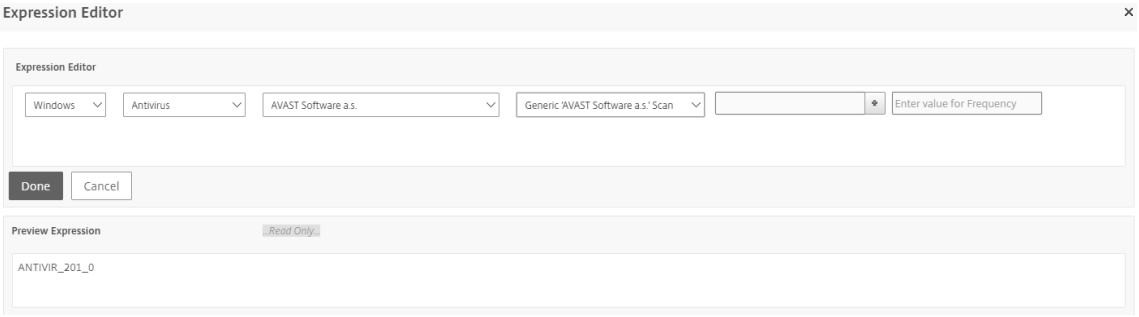
7. 选择 通用 **'AVAST** 软件**.'** 扫描供应商特定扫描。



8. 单击产品下拉菜单旁边的 **+** 以配置扫描。



9. 如果需要定期扫描，则可选择输入扫描频率值。

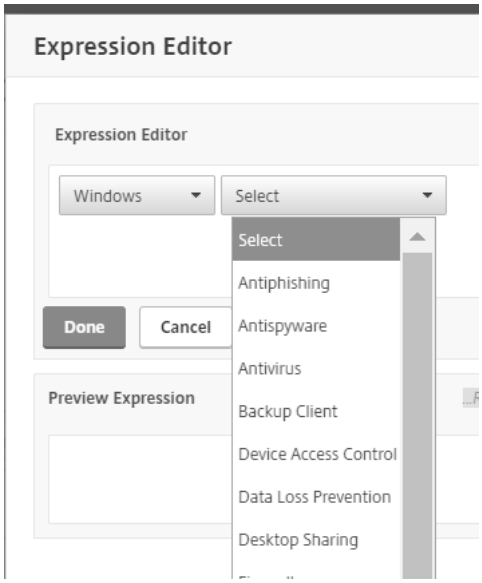


配置通用 **OPSWAT** 扫描

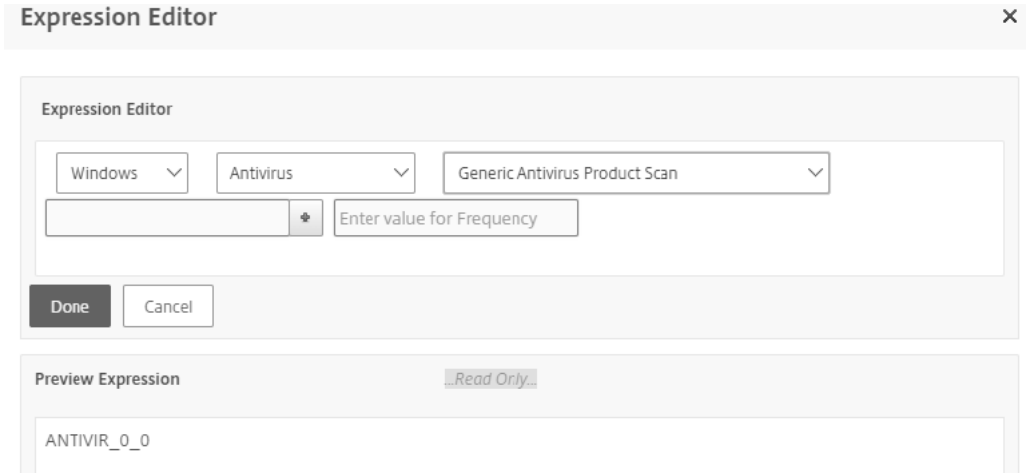
要使用 NetScaler GUI 配置通用 OPSWAT 扫描，请执行以下操作：

1. 导航到配置 **> Citrix NetScaler >** 全局设置。
2. 在“全局设置”页上，单击“更改预身份验证设置”链接。
3. 在配置 AAA 预身份验证参数页上，单击 **OPSWAT EPA** 编辑器链接。
4. 在“表达式编辑器”区域下，选择操作系统。

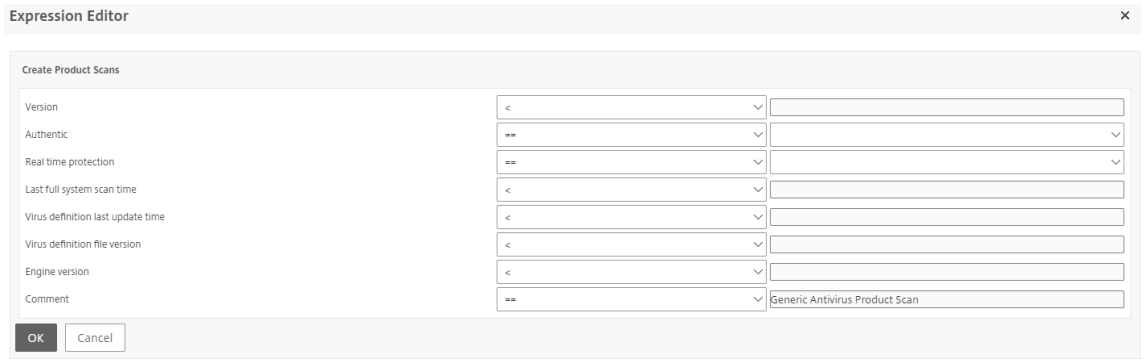
5. 选择类别，例如 防病毒软件。



6. 选择“通用”类别特定的扫描，例如 通用防病毒产品扫描。



7. 单击产品下拉菜单旁边的 **+** 以配置扫描。



8. 如果需要定期扫描，则可选择输入扫描频率的值。

配置系统扫描

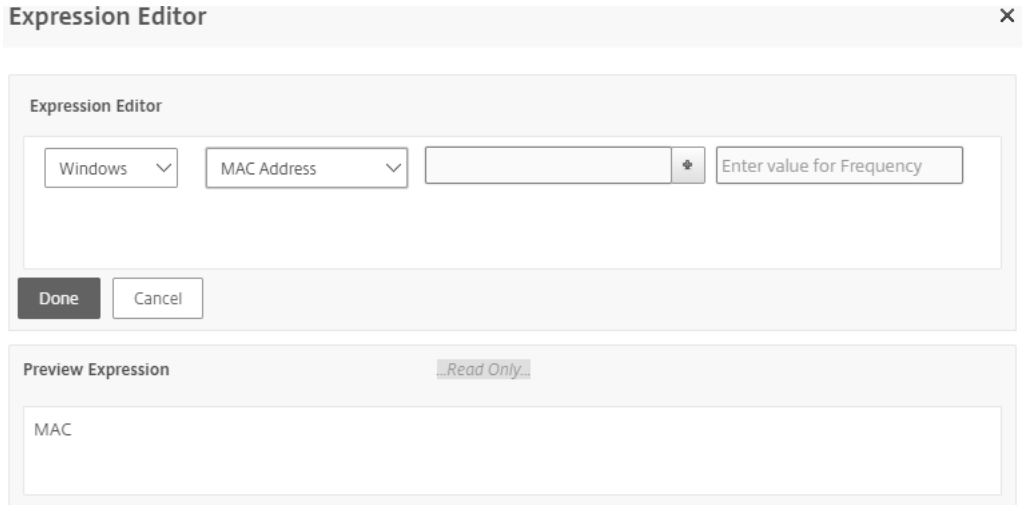
在 Citrix Gateway 设备上配置了以下系统扫描。

- MAC 地址
- 域名检查
- 数字注册表
- 非数字注册表
- Windows Update

若要使用 NetScaler GUI 配置 OPSWAT 系统扫描，请执行以下操作：

1. 导航到配置 **> Citrix NetScaler >** 全局设置。
2. 在“全局设置”页上，单击“更改预身份验证设置”链接。
3. 在配置 **AAA** 预身份验证参数页面上，单击 **OPSWAT EPA** 编辑器链接。
4. 在“表达式编辑器”区域下，选择操作系统。

5. 从下拉菜单中选择所需的系统扫描。例如，**MAC** 地址。



6. 单击产品下拉菜单旁边的 **+** 以配置您的扫描。

7. 如果需要定期扫描，则可选择输入扫描频率的值。

升级 **EPA** 库

要使用 NetScaler GUI 升级 EPA 库，请执行以下操作：

1. 导航到配置 **> Citrix NetScaler >** 更新客户端组件。
2. 在更新客户端组件下，单击升级 **EPA** 库链接。
3. 选择所需文件，然后单击 升级。

有关由 OPSWAT 支持的用于 Citrix ADC 扫描的 Windows 和 MAC 应用程序的列表，请单击https://support.citrix.com/article/C

使用高级端点分析表达式配置预身份验证配置文件

1. 在配置实用程序的导航窗格中，展开 Citrix Gateway 节点，然后展开策略子节点。
2. 选择预身份验证。
3. 在详细信息窗格中的配置文件选项卡上，单击添加。
4. 输入配置文件的名称。
5. 选择一个操作。
6. 或者，在客户端端点系统上输入要停止的任何进程或要删除的文件的名称。
7. 单击创建。

您的配置文件现在可用于预身份验证策略中，作为请求操作

使用高级端点分析表达式配置预身份验证策略

1. 在配置实用程序的导航窗格中，展开 Citrix Gateway 节点，然后展开策略子节点。
2. 选择预身份验证。
3. 在详细信息窗格的“策略”选项卡上，单击“添加”。
4. 输入策略的名称。
5. 从“请求操作”菜单中，选择所需的配置文件。
6. 在表达式窗格中，选择 OPSWAT EPA 编辑器。
7. 在第一个下拉菜单中，选择客户端操作系统。
8. 在出现的第二个下拉菜单中，选择扫描类型。
9. 完成策略构建后，单击创建。

您必须绑定高级端点分析预身份验证策略才能启用该策略。

绑定预身份验证策略

1. 在配置实用程序的导航窗格中，展开 Citrix Gateway 节点，然后展开策略子节点。
2. 选择预身份验证。
3. 在详细信息窗格的“策略”选项卡上，单击“添加”。
4. 从“操作”菜单中，选择“全局绑定”。
5. 单击 Bind（绑定）。
6. 在出现的“策略”详细信息窗格中，选中所需策略旁边的复选框。
7. 点击插入。
8. 策略会自动分配优先级（权重）。单击优先级条目以根据需要进行编辑。
9. 单击“确定”以绑定策略。

为特定会话配置高级端点分析策略

1. 在配置实用程序的导航窗格中，展开 Citrix Gateway 节点，然后展开策略子节点。
2. 选择会话。

3. 在详细信息窗格的“策略”选项卡上，单击“添加”。
4. 输入策略的名称。
5. 在“操作”菜单中，执行以下操作之一：
   - a. 选择现有操作。
   - b. 单击加号图标以显示可由会话策略设置的配置参数。单击配置选项右侧的覆盖全局复选框以激活它。选择创建。
6. 在表达式窗格中，选择 OPSWAT EPA 编辑器。
7. 在第一个下拉菜单中，选择客户端操作系统。
8. 在出现的第二个下拉菜单中，选择扫描类型。
9. 完成策略构建后，单击创建。

您必须绑定高级端点分析会话策略才能启用该策略。

绑定会话策略

1. 在配置实用程序的导航窗格中，展开 Citrix Gateway 节点，然后展开策略子节点。
2. 选择会话。
3. 在详细信息窗格的“策略”选项卡上，单击“添加”。
4. 从“操作”菜单中，选择“全局绑定”。
5. 单击 Bind（绑定）。
6. 在出现的“策略”详细信息窗格中，选中所需策略旁边的复选框。
7. 点击插入。
8. 策略会自动分配优先级（权重）。单击优先级条目以根据需要进行编辑。
9. 单击“确定”以绑定策略。

高级端点分析策略表达式参考

April 6, 2020

本参考介绍了高级端点分析表达式的格式和构造。此处包含的表达式元素由 Citrix Gateway 配置实用程序自动构建，不需要手动配置。

表达式格式

高级端点分析表达式具有以下格式：

```
CLIENT.APPLICATION (SCAN-type_ Product-id_ Method-name _ Method-comparator_
 Method-param _…)
```

其中，

扫描类型是正在分析的应用程序类型。

产品编号是分析应用的产品标识。

方法名称是正在分析的产品或系统属性。

方法比较器是用于分析的选择比较器。

方法参数是正在分析的一个或多个属性值。

例如：

client.application(ANTIVIR_2600*RTP*==_TRUE)

> 注意：对于非应用程序扫描类型，表达式前缀是 CLIENT.SYSTEM instead of CLIENT.APPLICATION。

表达式字符串

高级端点分析中的每种受支持的扫描类型都在表达式中使用唯一标识符。下表列举了每种扫描类型的字符串。

扫描类型	扫描类型表达式字符串
反钓鱼	ANTIPHI
反间谍软件	ANTISPY
防病毒	ANTIVIR
备份客户端	BACKUP
设备访问控制	DEV-CONT
数据丢失防护	DATA-PREV
桌面共享	DESK-SHARE
防火墙	FIREWALL
运行状况代理	HEALTH
硬盘加密	HD-ENC
即时通讯	IM
Web 浏览器	BROWSER
P2P	P2P
修补程序管理	PATCH
URL 过滤	URL-FILT
MAC 地址	MAC

扫描类型	扫描类型表达式字符串
域名检查	DOMAIN
数字注册表扫描	REG-NUM
非数字注册表扫描	REG-NON-NUM

> 注意：对于 Mac OS X 特定扫描，表达式在方法类型之前包含前缀 MAC-。因此，对于防病毒和防网络钓鱼扫描，方法分别为 MAC-ANTIVIR 和 MAC-ANTIPHI。例如：pre codeblock client.application(MAC-ANTIVIR_2600*RTP*==_TRUE)

应用程序扫描方法

在配置高级端点分析表达式时，使用方法定义端点扫描的参数。这些方法包括方法名称、比较器和值。下表列举了可在表达式中使用的所有方法。

常见扫描方法：

以下方法用于多种类型的应用程序扫描。

方法	说明	比较器	可能的值
VERSION*	指定应用程序的版本。	<, <=, >, >=, !=, ==	版本字符串
AUTHENTIC**	检查给定的应用程序是否真实。	==	TRUE
ENABLED	检查应用程序是否已启用。	==	TRUE
RUNNING	检查应用程序是否正在运行。	==	TRUE
COMMENT	注释字段（扫描忽略）。在表达式内由 [] 界定。	==	任何文本

* 版本字符串可以指定最多四个值的十进制字符串，例如 1.2.3.4。

** 一个真实的检查验证应用程序的二进制文件的真实性。

> 注意：您可以为应用程序扫描类型选择通用版本。选择通用扫描后，商品编码将为 0。

网关提供了一个选项，用于为每种类型的软件配置通用扫描。使用通用扫描，管理员可以扫描客户端计算机，而不会将扫描检查限制到任何特定产品。

对于通用扫描，只有在用户系统上安装的产品支持该扫描方法时，扫描方法才能起作用。要了解哪些产品支持特定扫描方法，请联系 Citrix 支持部门。

唯一扫描方法：

以下方法对于指定类型的扫描是唯一的。

方法	说明	比较器	可能的值
ENABLED-FOR	检查是否为所选应用程序启用了防网络钓鱼软件。	allof、anyof、noneof	对于 **Windows**：Internet Explorer、Mozilla Firefox、Google Chrome、Opera、Safari。对于 **Mac**：野生动物园，火狐火狐，谷歌，浏览器，歌剧

表 2. 反间谍软件和防病毒

方法	说明	比较器	可能的值
RTP	检查是否打开实时保护。	==	TRUE
SCAN-TIME	执行完整系统扫描后多少分钟。	<, <=, >, >=, !=, ==	任何正数
VIRDEF-FILE-TIME	自病毒定义文件更新以来的分钟数（即病毒定义文件戳和当前时间戳之间的分钟数）。	<, <=, >, >=, !=, ==	任何正数
VIRDEF-FILE-VERSION	定义文件的版本。	<, <=, >, >=, !=, ==	版本字符串
ENGINE-VERSION	引擎版本。	<, <=, >, >=, !=, ==	版本字符串

表 3. 备份客户端

方法	说明	比较器	可能的值
最后一次 B-活动	自上次备份活动完成后多少 分钟。	<, <=, >, >=, !=, ==	任何正数

表 4. 数据丢失预防

方法	说明	比较器	可能的值
ENABLED	检查应用程序是否启用，并且时间保护是否启用。	==	TRUE

表 5. 运行状况检查代理

方法	说明	比较器	可能的值
SYSTEM-COMPL	检查系统是否符合要求。	==	TRUE

表 6. 硬盘加密

方法	说明	比较器	可能的值
ENC-PATH	用于检查加密状态的 PATH。	无运算符	任何文本
电子类型	检查是否为指定路径加密类型。	allof、anyof、noneof	包含以下选项的列表：UNENCRYPTED、PARTIAL、ENCRYPTED、VIRTUAL、SUSPENDED、PENDING

表 7. 网页浏览器

方法	说明	比较器	可能的值
DEFAULT	检查是否设置为默认浏览器。	==	TRUE

表 8. 修补程序管理 </caption>

方法	说明	比较器	可能的值
SCAN-TIME	自上次扫描修补程序后执行多少分钟。	<, <=, >, >=, !=, ==	任何正数

方法	说明	比较器	可能的值
MISSED-PATCH	客户端系统不会丢失这些类型的补丁。	anyof、noneof	任何预先选择的（在补丁管理器服务器上预先选择的补丁）
NON			

方法	说明	比较器	可能的值
ADDR	检查客户端计算机 MAC 地址是否在给定列表中。	anyof、noneof	可编辑列表

表 10. 域成员资格 </caption>

方法	说明	比较器	可能的值
SUFFIX	检查给定列表中是否存在客户端计算机。	anyof、noneof	可编辑列表

方法	说明	比较器	可能的值
PATH	注册表检查的路径。格式为：HKEY_LOCAL_MACHINE Access Client\EnableAutoUpda 不需要转义特殊字符。所有注册表根项：HKEY_LOCAL_MACHINE HKEY_CURRENT_USER HKEY_USERS、HKEY_CLASSES_ROOT、HKEY_CURRENT_CONF	无运算符	任何文本

方法	说明	比较器	可能的值
REDIR-64	遵循 64 位重定向。如果设置为 TRUE，将遵循 WOW 重定向（即将在 32 位系统上检查注册表路径，但将检查 64 位系统的 WOW 重定向路径）。如果未设置，则不会遵循 WOW 重定向（即 32 位和 64 位系统将检查相同的注册表路径）。对于未重定向的注册表项，此设置将不起作用。有关在 64 位系统上重定向的注册表项列表，请参阅以下文章：http://msdn.microsoft.com/en-us/library/aa384253%28v=vs.85%29.aspx	==	TRUE
值	上述路径的预期值。此扫描仅适用于注册表类型的 REG_DWORD 和 REG_QWORD。	<, <=, >, >=, !=, ==	任何数字

方法	说明	比较器	可能的值
PATH	注册表检查的路径。		
检查注册表扫描数字类型。	NO 运算符	任何文本	
REDIR-64	遵循 64 位重定向		
检查注册表扫描数字类型。	==	TRUE	

方法	说明	比较器	可能的值
值	上述路径的预期值。对于字符串类型的注册表项，直接将注册表值与预期值进行比较。对于 REG_BINARY 注册表项类型，注册表值转换为大写的十六进制字符串，并将此字符串与预期值进行比较。	==,! =	任何文本

高级端点分析扫描故障排除

April 6, 2020

为了帮助对高级端点分析扫描进行故障排除，客户端插件会将日志记录信息写入客户端点系统上的文件。这些日志文件可以在以下目录中找到，具体取决于用户的操作系统。

Windows Vista、**Windows 7**、**Windows 8**、**Windows 8.1** 和 **Windows 10**：

C:\Users\<username>\AppData\Local\Citrix\AGEE\nsepa.txt

Windows XP：

C:\Documents and Settings\All Users\Application Data\Citrix\AGEE\nsepa.txt

Mac OS X 系统：

~/Library/Application Support/Citrix/EPAPlugin/epaplugin.log

（其中 ~ 符号表示相关 Mac OS X 用户的主目录路径。）

管理用户会话

April 6, 2020

您可以在“活动用户会话”对话框中的配置实用程序中管理用户会话。此对话框显示 Citrix Gateway 上活动用户会话的列表。

您可以使用用户名、组名称或 IP 地址在此对话框中的最终用户或组会话。

您还可以在此对话框中查看活动会话。会话信息包括：

- 用户名
- 用户设备的 IP 地址
- 用户设备的端口号
- 虚拟服务器的 IP 地址
- 虚拟服务器的端口号
- 分配给用户的内联网 IP 地址

查看用户会话

1. 在配置实用程序中，单击配置选项卡，然后在导航窗格中单击 Citrix Gateway。
2. 在详细信息窗格的监视器连接下，单击活动用户会话。
3. 查看会话下的会话列表。

刷新会话列表

您可以检索有关 Citrix Gateway 的会话的更新信息。

1. 在配置实用程序中，单击配置选项卡，然后在导航窗格中单击 Citrix Gateway。
2. 在详细信息窗格的监视器连接下，单击活动用户会话。
3. 单击刷新。

最终用户或组会话

您可以终止用户和组会话。您还可以结束具有特定 Intranet IP 地址和子网掩码的会话。

1. 在配置实用程序中，单击配置选项卡，然后在导航窗格中单击 Citrix Gateway。
2. 在详细信息窗格的监视器连接下，单击活动用户会话。
3. 在“会话”下，选择一个用户或组，然后单击“终止”。

使用 **Intranet IP** 地址结束会话

1. 在配置实用程序中，单击配置选项卡，然后在导航窗格中单击 Citrix Gateway。
2. 在详细信息窗格的监视器连接下，单击活动用户会话。
3. 选择内联网 IP
4. 在 Intranet IP 中，键入 IP 地址。
5. 在网络掩码中，键入子网掩码，然后单击终止。

AlwaysON

April 6, 2020

Citrix Gateway 的 AlwaysOn 功能可确保用户始终连接到企业网络。这种持久的 VPN 连接是通过自动建立 VPN 隧道来实现的。

> 注意
>
> AlwaysON 功能支持面向 Citrix ADC 12.0 Build 51.24 及更高版本的强制网络门户。

何时使用 **AlwaysOn**

如果您需要根据用户位置提供无缝 VPN 连接，并且必须防止未连接到 VPN 的用户进行网络访问，请使用 AlwaysOn。

下面的情况说明了使用 AlwaysOn。

- 员工在企业网络外启动笔记本电脑，需要帮助来建立 VPN 连接。
  解决方案：当笔记本电脑在企业网络之外启动时，AlwaysOn 无缝建立隧道并提供 VPN 连接。
- 使用 VPN 连接的员工进入企业网络。员工切换到企业网络，但仍然连接到 VPN 隧道，这不是理想的状态。
  解决方案：当员工进入企业网络时，AlwaysOn 会破解 VPN 隧道，将员工无缝切换到企业网络。
- 员工移动到企业网络之外并关闭笔记本电脑（不关闭）。员工需要帮助，以便在笔记本电脑上恢复工作时建立 VPN 连接。
  解决方案：当员工移动到企业网络之外时，AlwaysOn 无缝建立隧道并提供 VPN 连接。
- 企业希望在其用户未连接到 VPN 隧道时对其提供的网络访问进行规范。
  解决方案：根据配置，AlwaysOn 限制访问，允许用户仅访问网关网络。

了解 **AlwaysOn** 框架

AlwaysOn 会自动将用户连接到客户端先前建立的 VPN 隧道。用户首次需要 VPN 隧道时，用户必须连接到 Citrix Gateway URL 并建立隧道。将 AlwaysOn 配置下载到客户端后，此配置将推动隧道的后续建立。

Citrix Gateway 客户端可执行文件始终在客户端计算机上运行。当用户登录或网络更改时，Citrix Gateway 客户端将确定用户笔记本电脑是否位于企业网络上。根据位置和配置，Citrix Gateway 客户端可以建立隧道或拆除现有隧道。

只有在用户登录到计算机后才启动隧道建立。Citrix Gateway 客户端使用客户端计算机的凭据对网关服务器进行身份验证，并尝试建立隧道。

自动重建隧道

当 Citrix Gateway 拆除 VPN 通道时，将触发自动重建通道。

> 注意
>
> 在终端点分析失败时，Citrix Gateway 客户端不会重新尝试建立隧道，但会显示错误消息。如果身份验证失败，Citrix Gateway 客户端会提示用户输入凭据。

支持的无缝隧道建立用户身份验证方法

支持的用户身份验证方法如下：

- 用户名 + AD 密码：如果 Windows 用户名和密码用于身份验证，Citrix Gateway 客户端将使用这些凭据无缝建立隧道。
- 用户证书：如果用户证书进行身份验证，且计算机上只有一个证书，Citrix Gateway 客户端将使用此证书无缝建立隧道。如果安装了多个客户端证书，则在用户选择首选证书后建立隧道。Citrix Gateway 客户端将此首选项用于以后建立的隧道。
- 用户证书和用户名 + AD 密码：此身份验证方法是之前描述的身份验证方法的组合。

> 注意
>
> 支持所有其他身份验证机制，但隧道建立不适用于任何其他身份验证方法。所有其他身份验证方法都需要用户干预。

AlwaysOn 的配置要求

企业管理员必须对托管设备强制执行以下操作：

- 用户不能为特定配置结束进程/服务
- 用户必须无法卸载软件包进行特定配置
- 用户必须无法更改特定的注册表项

> 注意
>
> 如果用户具有管理权限（如非托管设备的情况），该功能可能无法按预期工作。

启用 **AlwaysOn** 功能时的注意事项

在启用 AlwaysOn 功能之前，请查看以下部分。

主网络访问：隧道建立后，根据分段隧道配置确定企业网络的流量。不提供其他配置来覆盖此行为。

客户端计算机的代理设置：连接到网关服务器时忽略客户端计算机的代理设置。

> 注意
>
> Citrix ADC 设备的代理配置不会被忽略。仅忽略客户端计算机的代理设置。在其系统上配置了代理的用户会收到通知，该 VPN 插件已忽略其代理设置。

当配置值设置为“拒绝”时，以下更改将适用：

- 客户端 UI-禁用插件上下文菜单和插件 UI 中的注销和退出选项。不允许用户更改网关 URL。
- 浏览器登录-不允许浏览器登录到其他 Gateway。客户端控件已禁用。

配置 **AlwaysOn**

要配置 AlwaysOn，请在 Citrix Gateway 设备上创建 AlwaysOn 配置文件并应用该配置文件。

要创建一个 AlwaysOn 配置文件，请执行以下操作：

1. 在 Citrix ADC GUI 中，导航到配置 **> Citrix Gateway >** 策略 **> AlwaysON**。
2. 在 “AlwaysOn 配置文件” 页上，单击 “添加”。
3. 在 “创建 AlwaysOn 配置文件” 页面上，输入以下详细信息：
   - 名称 — 您的配置文件的名称。
   - 基于位置的 **VPN** — 选择以下设置之一：
     - 远程使客户端能够检测它是否在企业网络中，如果不在企业网络中，则建立隧道。此为默认设置。
     - 无论客户端位置如何，都可以让客户端跳过位置检测并建立隧道
   - 客户端控制 — 选择以下设置之一：
     - 拒绝以阻止用户注销并连接到另一个网关。此为默认设置。
     - 允许用户注销并连接到另一个网关。
   - **VPN** 故障上的网络访问 — 选择以下设置之一：
     - 当未建立隧道时，允许网络流量流入客户端和流出客户端的完全访问权限。此为默认设置。
     - 仅限到网关，以防止网络流量流入或流出客户端时未建立隧道。但是，允许流入或流出网关 IP 地址的流量。
4. 单击 创建完成您的个人资料的创建。

要应用 AlwaysOn 配置文件，请执行以下操作：

1. 在 Citrix ADC 接口中，选择配置 **> Citrix Gateway >** 全局设置。
2. 在 “全局设置” 页上，单击 “更改全局设置” 链接，然后选择 “客户端体验” 选项卡。
3. 从 **AlwaysOn** 配置文件名称下拉菜单中，选择新创建的配置文件，然后单击确定。

> 注意
>
> 可以在会话配置文件中进行类似的配置，以便在组级别、服务器杠杆或用户级别应用策略。

管理员用户和非管理员用户不同配置的行为摘要

下表总结了不同配置的行为。它还详细介绍了某些用户操作的可能性，这可能会影响 AlwaysOn 功能。

networkAccessONVPNFailure	客户端控制	非管理员用户	管理员用户
全面接触	允许	隧道自动建立。用户可以注销并停留网络。用户还可以指向另一个 Citrix Gateway。	隧道自动建立。用户可以注销并停留在企业网络之外。用户还可以指向另一个 Citrix Gateway。

networkAccessONVPNFailure	客户端控制	非管理员用户	管理员用户
全面接触	拒绝	隧道自动建立。用户无法注销或指向另一个 Citrix Gateway。	隧道自动建立。用户可以卸载 Citrix Gateway 客户端或移动到另一个 Citrix Gateway。
onlyToGateway	允许	隧道自动建立。用户可以注销（无网络访问）。用户还可以指向另一个 Citrix Gateway，在这种情况下，访问权限仅给予新指向的 Citrix Gateway。	隧道自动建立。用户可以卸载 Citrix Gateway 客户端或移动到另一个 Citrix Gateway。
onlyToGateway	拒绝	隧道自动建立。用户无法注销或指向另一个 Citrix Gateway。	隧道自动建立。用户可以卸载 Citrix Gateway 客户端或移动到另一个 Citrix Gateway。

AlwaysOn 关闭时，将 **URL** 列入白名单

用户可以访问一些网站，即使 AlwaysOn 关闭并且网络被锁定。管理员可以使用 **AlwaysOnWhitelist** 注册表添加您希望在 AlwaysOn 关闭时启用访问权限的网站。

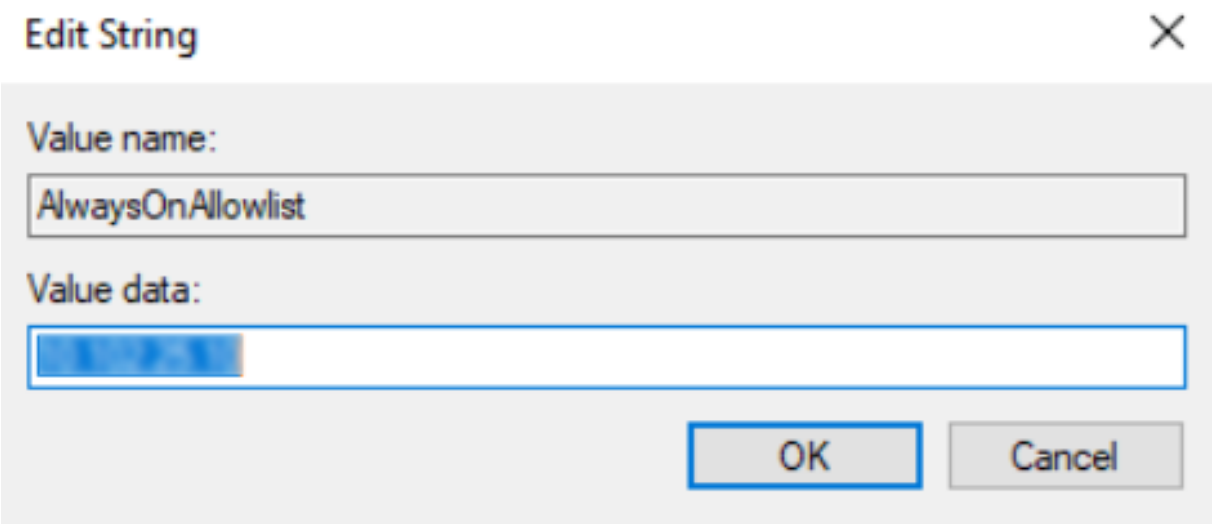
> 注意：
>
> - 版本 13.0 版本 47.x 及更高版本支持 **AlwaysOnWhitelist** 注册表。
> - **AlwaysOnWhitelist** 注册表位置为 Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client。
> - **AlwaysOnWhitelist** 注册表不支持通配符 URL /FQDN。

设置 **AlwaysOnWhitelist** 注册表

使用分号分隔的 FQDN、IP 地址范围或您希望允许访问的 IP 地址列表来设置 **AlwaysOnWhitelist** 注册表。

示例： mycompany.com-mycdn.com-10.120.67.0-10.120.67.255,67.67.67.67

下图显示了一个示例 **AlwaysOnWhitelist** 注册表。



Windows 登录之前的 AlwaysOn VPN（官方名称为 AlwaysOn 服务）

November 3, 2021

Windows 登录之前的 **AlwaysOn VPN** 功能允许用户在用户登录到 Windows 系统之前建立计算机级 VPN 隧道。隧道保持活动状态，直到机器关闭。用户登录后，设备级 VPN 隧道由用户级 VPN 隧道接管。用户注销后，用户级隧道会被撕裂，并建立设备级隧道。只能通过使用高级策略来配置 Windows 登录之前的 AlwaysOn VPN。有关详细信息，请参阅在 Windows 登录之前配置 AlwaysOn VPN。

在 Windows 登录之前，AlwaysOn VPN 包含以下内容：

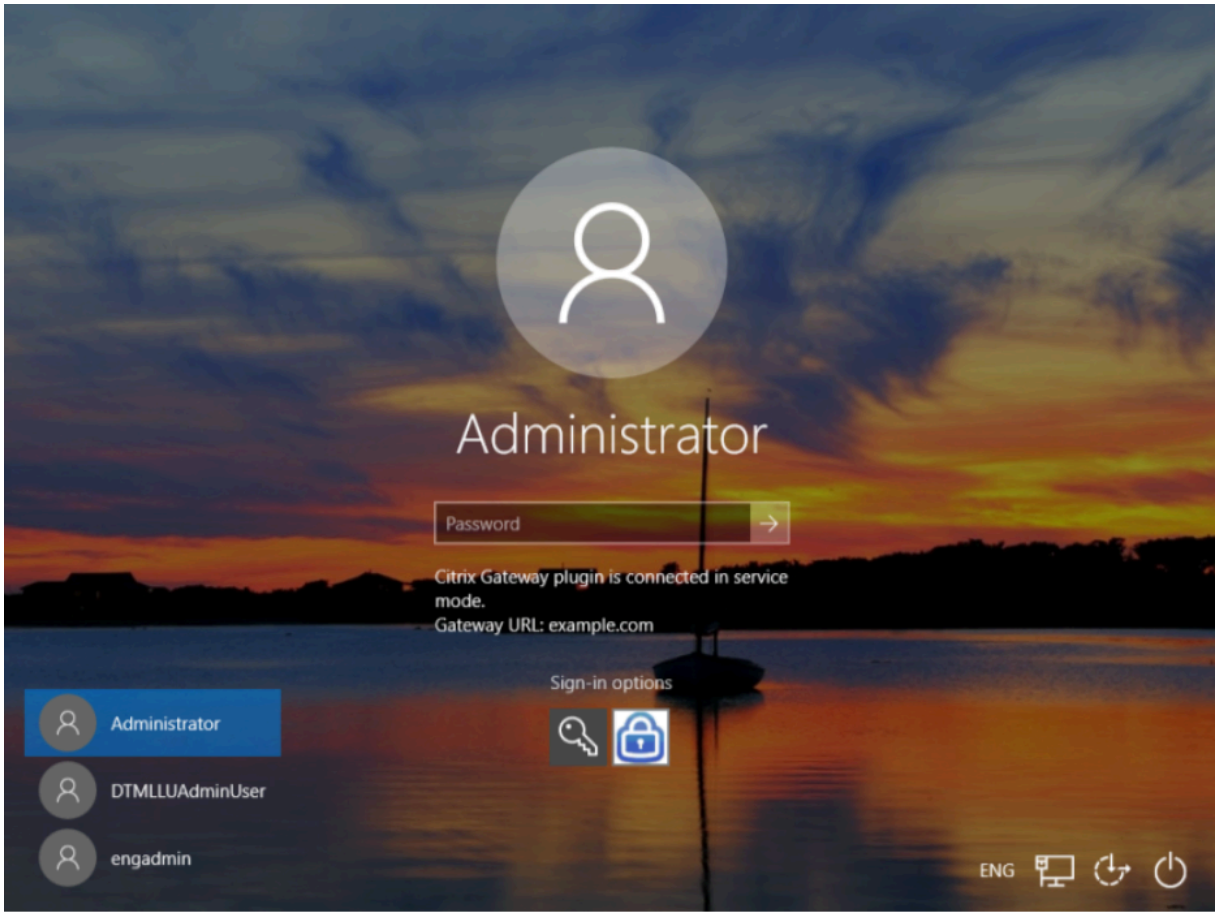
- Windows 计算机可以使用公司活动目录 (AD) 验证用户的登录凭据，并且计算机上的 Windows 凭据不会缓存。此外，将启用新的公司 AD 用户无缝登录到计算机。
- 甚至在用户登录之前，Windows 计算机就会成为企业内部网络的一部分，从而允许 IT 管理员从企业网络访问客户端计算机以进行调试。
- 即使不同用户登录或注销计算机，Windows 计算机的 VPN 隧道仍保持连接状态。

注意事项：

- Citrix Gateway 和 VPN 插件必须是版本 13.0.41.20 及更高版本。
- 如果客户端计算机没有互联网连接，则在 Windows 登录之前，AlwaysOn VPN 等待互联网连接变为可用，然后再建立 VPN 隧道。
- 如果客户端计算机连接到专用门户网络，则在 Windows 登录之前 AlwaysOn VPN 等待用户对专用门户进行身份验证。用户登录并启用互联网访问后，Windows 登录之前 AlwaysOn VPN 建立 VPN 隧道。
- 在 Windows 登录之前，AlwaysOn VPN 支持 Citrix ADC 的专用门户。
- 如果未为 Windows 启用缓存登录凭据选项，则用户无法登录以下情况：
  - 机器没有互联网连接
  - 计算机连接到专属门户网络

Windows 登录配置之前，AlwaysOn VPN 之后的 Windows 凭据管理器屏幕

在配置 Windows 登录之前的 AlwaysOn VPN 功能后，Windows 凭据管理器屏幕将按如下方式进行修改。



在登录屏幕上单击登录 选项时，将显示以下信息：

- Citrix Gateway 图标表明计算机是否连接到 Citrix Gateway。
- 根据用户配置模式，登录屏幕上会显示以下语句之一。
  - Citrix Gateway 以服务模式连接
  - Citrix Gateway 以用户模式连接

在 Windows 登录之前配置 AlwaysOn VPN

November 7, 2022

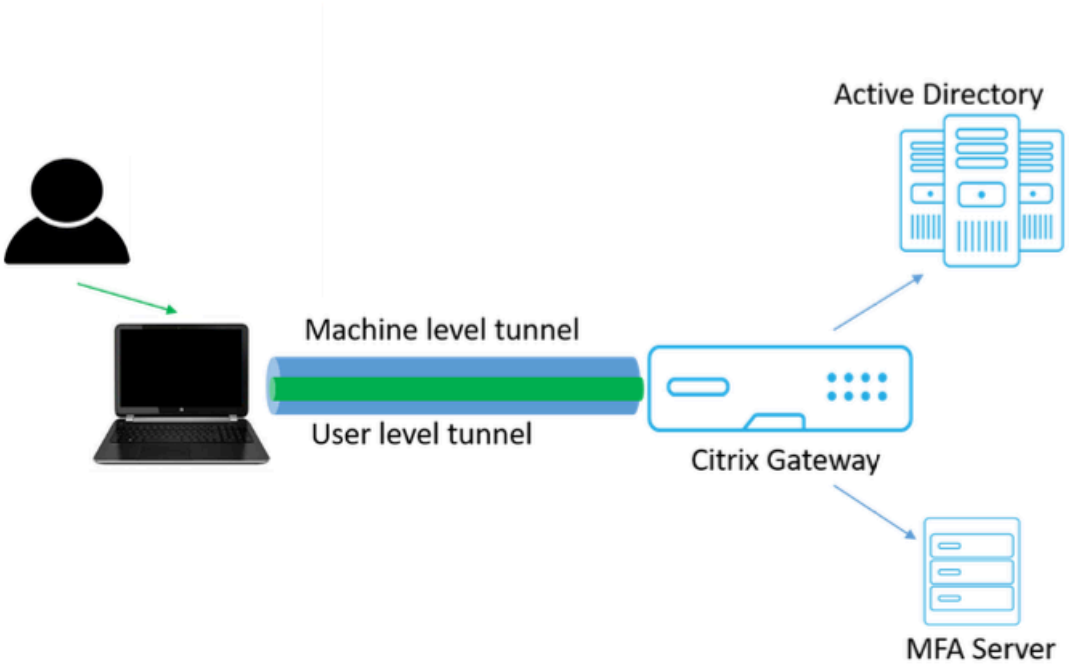
Windows 登录之前 AlwaysOn VPN 提供以下功能。

- 管理员为首次远程工作的用户提供一次性密码，使用该密码，用户可以连接到域 Controller 以更改其密码。
- 即使在用户登录之前，管理员也可远程管理/强制执行 AD 策略。

- 在用户登录后，管理员根据用户组为用户提供精细级别的控制。例如，使用用户级隧道，限制或提供对特定用户组的资源的访问权限是可能的。
- 可根据用户要求为 MFA 配置用户隧道。
- 同一台机器可以被多个用户使用，根据用户配置文件提供对选择性资源的访问。例如，在自助亭中，一台机器可以被多个用户毫不费力地使用。
- 远程工作的用户连接到域 Controller 以更改其密码。

了解 **Windows** 登录之前的 **AlwaysOn VPN**

以下是 Windows 登录功能之前的 AlwaysOn 的事件流程。



- 用户打开笔记本电脑后，使用设备证书作为标识，针对 Citrix Gateway 建立计算机级隧道。
- 用户使用 AD 凭据登录到笔记本电脑。
- 登录后，用户将面临 MFA 的挑战。
- 身份验证成功后，计算机级隧道将替换为用户级隧道。
- 用户注销后，用户级隧道将替换为机器级隧道。

通过使用 **GUI** 在 **Windows** 登录之前配置 **AlwaysOn VPN**

必备条件

- Citrix Gateway 和 VPN 插件必须是版本 13.0.41.20 及更高版本。
- Citrix ADC 高级版及更高版本才能使解决方案工作。
- 您只能使用高级策略配置功能。

配置涉及以下高级别步骤：

- 创建身份验证配置文件
- 创建身份验证虚拟服务器
- 创建身份验证策略
- 将策略绑定到身份验证配置文件

使用 **GUI** 配置功能

基于客户端证书的身份验证

1. 在“配置”选项卡上，导航到 **Citrix Gateway >** 虚拟服务器。
2. 在 Citrix Gateway 虚拟服务器页面上，选择现有虚拟服务器，然后单击 编辑。
3. 在 VPN 虚拟服务器页面上，单击编辑图标。
4. 单击“设备证书 **CA”** 部分旁的“添加”，然后单击“确定”。

   注意：请勿选中“启用设备证书”复选框。
5. 要将 CA 证书绑定到虚拟服务器，请单击“证书**”** 部分下的 **CA** 证书。单击 **SSL** 虚拟服务器 **CA** 证书绑定页面下的 ****** 添加绑定 ** 。
6. 单击文本，单击以选择选择所需的证书。
7. 选择所需的 CA 证书。
8. 单击 **Bind**（绑定）。
9. 在 VPN 虚拟服务器页上的身份验证配置文件部分下，单击 添加。
10. 在“创建身份验证配置文件”页上，提供身份验证配置文件的名称，然后单击“添加”。
11. 在“身份验证虚拟服务器”页上，提供身份验证虚拟服务器的名称，选择“IP 地址类型”为 不可寻址，然后单 击 **“**确定”。
12. 在“高级身份验证策略”下，单击“身份验证策略”内部。
13. 在策略绑定页面上，单击 选择策略旁边的 添加。
14. 在“创建身份验证策略”页面上；

    a) 输入高级身份验证策略的名称。
    b) 从操作类型列表中选择 **EPA**。
    c) 点击 操作旁边的 添加。
15. 在“创建身份验证 EPA 操作”页面上；

a) 输入要创建的 EPA 操作的名称。
b) 在“表达式”字段 中输入系统服务器（**“设备-证书 _0_0”**）。
c) 单击创建。

16. 在“创建身份验证策略”页面上；

a) 输入身份验证策略的名称。
b) 在“表达式**”** 字段中输入 **“**服务”。
c) 单击创建。

17. 在策略绑定页面上，输入 **100** 优先级，然后单击绑定。

> 注意：机器级隧道配置现已完成。如果您不希望 Windows 登录后使用用户级隧道，则可以跳过步骤 18-25 并继续进行客户端配置。

要在 **Windows** 登录后将计算机级隧道替换为用户级隧道，请继续执行以下配置。

18. 将 **“**转到**”** 表达式更改为“下一步”而不是“结束”步骤 17 中绑定的策略。
19. 在“身份验证虚拟服务器”页面上，单击“身份验证策略”内部。
20. 在“身份验证策略”页上，单击“添加绑定”选项卡。
21. 在“策略绑定”页面上，单击“选择策略”旁边的“添加”。
22. 在“创建身份验证策略”页面上；

a) 输入要创建的“无身份验证”策略的名称。
b) 选择操作类型作为 **NO_Authn**。
c) 在“表达式**”** 字段中输入 **“**不是”。
d) 单击创建。

> 注意：表达 式不适用于 Citrix Gateway 13.0 版本 41.20 及更高版本。

23. 在策略绑定页面上，在“优先级”中输入 **110** ，单击“选择下一个因素**”** 旁边的“添加”。
24. 在身份验证策略标签页上，创建 LDAP 身份验证策略。请参阅以下文章以创建 LDAP 身份验证策略。欲了解更多详情，请参阅使用配置实用程序配置 LDAP 身份验证。
25. 单击策略 绑定页面上的绑定。

客户端配置

AlwaysOn、locationDetection 和 suffixList 注册表是可选的，仅当需要位置检测功能时才需要。

注册表项	注册表类型	价值和说明
AlwaysOnService	REG_DWORD	1 => 在没有用户角色的情况下启用 AlwaysOn 服务; 2 => 对用户角色启用 AlwaysOn 服务
AlwaysOnURL	REG SZ	Citrix Gateway 虚拟服务器用户要连接的 URL。示例：`https://xyz.companyDomain.com`
AlwaysOn	REG_DWORD	1 => 在 VPN 故障时允许网络访问; 2=> 在 VPN 故障时阻止网络访问
locationDetection	REG_DWORD	1 => 启用位置检测; 0 => 禁用位置检测
suffixList	REG SZ	以逗号分隔的内联网域列表。启用位置检测时使用。

有关这些注册表项的更多信息，请参阅AlwaysOn。

若要在 Windows 登录之前使用经典策略配置 AlwaysOn VPN，请参阅使用经典策略在 Windows 登录之前配置始终在 VPN 上

配置 Citrix Gateway

April 6, 2020

Citrix ADC 与 Citrix Gateway：一个 URL

Citrix ADC 与 Citrix Gateway 使桌面和移动用户可通过单个 URL 简化对任何应用程序的安全访问。在这个单一 URL 后面，管理员有一个单一的点来配置、安全和控制应用程序的远程访问。远程用户通过无缝单点登录到他们需要的所有应用程序以及登录/注销，一旦易于使用，就可以获得更好的体验。

为此，具有网关的 Citrix ADC 以及 Citrix ADC 的内容交换能力和广泛的身份验证基础设施，可通过此单个 URL 访问组织站点和应用程序。此外，远程用户还可以使用 iOS 或 Android 移动设备以及 Linux、PC 或 Mac 系统与 Citrix Gateway 客户端插件一起使用，以便对 Citrix Gateway URL 进行统一访问，无论它们位于何处。

Citrix Gateway 部署允许对以下类别的应用程序进行单个 URL 访问：

- 内联网应用程序.
- 无客户端应用程序
- 软件即服务应用程序

- Citrix ADC 提供的预配置应用程序
- Citrix Virtual Apps and Desktops 发布的应用程序

Intranet 应用程序可能是驻留在安全企业网络内的任何基于 Web 的应用程序。这些是内部资源，例如组织内部网站、错误跟踪应用程序或 wiki。

Citrix Gateway 通常也位于安全企业网络内，无客户端应用程序 Citrix Gateway 提供对 Outlook Web Access 和 SharePoint 的单个 URL 访问。这些应用程序提供对 Exchange 电子邮件和团队资源的访问，而无需专用客户端软件，这些软件需要向远程用户提供。

SaaS 应用程序（通常也称为云应用程序）是组织依赖的外部基于云的应用程序，例如 Sharefile、SalesForce 或 NetSuite。提供 SAML 的 SaaS 应用程序支持基于 SAML 的单点登录。

某些组织可能已经 预配置了部署在 **Citrix ADC** 负载平衡配置中的 **Citrix ADC** 服务的应用程序；这通常也称为“反向代理”应用程序。当部署的虚拟服务器驻留在同一 Citrix ADC Citrix Gateway 实例或设备上时，Citrix Gateway 支持这些应用程序。这些应用程序可能具有自己的身份验证配置，该配置独立于 Citrix Gateway 配置的身份验证配置。

任何已发布的 **Citrix Virtual Apps and Desktops** 发布的应用程序都可以通过 Citrix Gateway URL 获得。SmartAccess 和智能控制策略可以选择性地应用于精细策略和对这些资源的访问控制。

Citrix Gateway 配置向导

使用 Citrix Gateway 部署配置 Citrix ADC 的推荐方法是使用 Citrix Gateway 配置向导。该向导将引导您完成配置，并创建所有必要的虚拟服务器、策略和表达式，并根据提供的详细信息应用设置。初始设置后，该向导可用于管理您的部署并监视其操作。

> 注
> 意 Citrix Gateway 配置向导不执行初始系统配置。在配置 Citrix Gateway 之前，您的 Citrix Gateway 设备或 VPX 实例必须完成基本安装。请参阅安装说明使用首次安装向导配置 Citrix Gateway以完成基本配置。

由向导配置的 Citrix Gateway 元素包括：

- Citrix Gateway 主虚拟服务器
- Citrix Gateway 虚拟服务器的 SSL 服务器证书
- 主身份验证和任何可选的辅助身份验证配置
- 门户主题选择和可选自定义
- 要通过 Citrix Gateway 门户访问的用户应用程序

对于这些元素中的每个元素，您需要提供配置信息。对于基本 Citrix Gateway 部署，需要以下信息。

- 对于主 Citrix Gateway 虚拟服务器，部署的公有 IP 地址和 IP 端口号。这将是 DNS 中解析为 Citrix Gateway URL 主机名的 IP 地址。例如，如果 Citrix Gateway 部署的 URL 为`https://mycompany.com/`，则必须将 IP 地址解析为 mycompany.com。
- 部署的签名 SSL 服务器证书。Citrix Gateway 支持 PEM 或 PFX 格式的证书。

- 主身份验证服务器信息。此身份验证配置支持的身份验证系统基于 LDAP /Active Directory、RADIUS 和证书。还可以创建辅助 LDAP 或 RADIUS 身份验证配置。身份验证服务器 IP 地址必须与任何相关的管理员凭据或目录属性一起提供。对于证书身份验证，必须提供设备证书属性和 CA 证书。
- 可以选择门户主题。如果需要自定义或品牌门户设计，则可以使用向导将自定义图形上传到系统。
- 对于基于 Web 的用户应用程序，必须指定各个应用程序的 URL。对于要使用 SAML 单点登录身份验证的 Web 应用程序，该实用程序将收集断言使用者服务 URL 以及其他可选 SAML 参数。事先收集使用 SAML 身份验证系统的应用程序的配置详细信息。
- 要通过 Citrix Gateway 部署提供 Citrix Virtual Apps and Desktops 发布的资源，您需要指定集成点（StoreFront、Web Interface 或 Citrix ADC 上的 Web Interface）。该实用程序需要集成点的完全限定域名、站点路径、单点登录域、安全票证颁发机构 (STA) 服务器 URL 以及其他具体取决于集成点类型的 URL。

其他配置管理

对于 Citrix Gateway 配置实用程序中不可用的站点特定设置（例如备用 SSL 设置或会话策略），您可以在 Citrix Gateway 配置实用程序中管理所需的设置。在 Citrix Gateway 配置实用程序创建内容交换或 VPN 虚拟服务器上的这些设置后，您可以修改这些设置。

内容交换虚拟服务器

这是部署的主 IP 地址和 URL 后面的 Citrix ADC 配置实体。SSL 服务器证书和参数在此虚拟服务器上进行管理。由于此虚拟服务器是部署的响应网络主机，因此如有必要，可以在此虚拟服务器上修改 ICMP 服务器响应和 RHI 状态。内容交换虚拟服务器可以在 “流量管理**”>“**内容交换”>“虚拟服务器” 的 “配置” 选项卡下找到。

VPN 虚拟服务器

Citrix Gateway 配置的所有其他 VPN 参数、配置文件和策略绑定都在此虚拟服务器上进行管理，包括主身份验证配置。此实体在 “Citrix Gateway”>“虚拟服务器” 的 “配置” 选项卡下进行管理。相关 VPN 虚拟服务器的名称将包括在初始 Citrix Gateway 配置期间给内容交换虚拟服务器的名称。

> 注意
> 为 Citrix Gateway 部署创建的 VPN 虚拟服务器不可寻址，并且分配了 0.0.0.0 IP 地址。

Unified Gateway 常见问题解答

April 6, 2020

什么是 Unified Gateway?
**

Unified Gateway 是 Citrix ADC 11.0 版本中的一项新功能，能够在单个虚拟服务器（称为 Unified Gateway 虚拟服务器）上接收流量，然后根据情况在内部将该流量引导到绑定到 Unified Gateway 虚拟服务器的虚拟服务器。

Unified Gateway 功能允许最终用户使用单个 IP 地址或 URL（与 Unified Gateway 虚拟服务器关联）访问多个服务。管理员可以释放 IP 地址并简化 Citrix Gateway 部署的配置。

作为编队的一部分，每个 Unified Gateway 虚拟服务器都可以前端一个 Citrix Gateway 虚拟服务器以及零个或多个负载平衡虚拟服务器。Unified Gateway 通过利用 Citrix ADC 设备的内容交换功能来工作。

Unified Gateway 部署的一些示例：

- Unified Gateway 虚拟服务器 -> [一台 Citrix Gateway 虚拟服务器]
- Unified Gateway 虚拟服务器 -> [一台 Citrix Gateway 虚拟服务器、一台负载平衡虚拟服务器]
- Unified Gateway 虚拟服务器 -> [一台 Citrix Gateway 虚拟服务器、两台负载平衡虚拟服务器]
- Unified Gateway 虚拟服务器 -> [一台 Citrix Gateway 虚拟服务器、三台负载平衡虚拟服务器]

每个负载平衡虚拟服务器都可以是承载后端服务（如 Microsoft Exchange 或 Citrix ShareFile）的任何标准负载平衡服务器。

为什么使用 Unified Gateway?
**

Unified Gateway 功能使最终用户能够使用单个 IP 地址或 URL（与 Unified Gateway 虚拟服务器关联）访问多个服务。对于管理员来说，其优点是他们可以释放 IP 地址并简化 Citrix Gateway 部署的配置。

是否可以有多个 Unified Gateway 虚拟服务器?
**

是。根据需要，可以有尽可能多的 Unified Gateway 虚拟服务器。

为什么 Unified Gateway 需要内容交换?
**

内容交换功能是必需的，因为内容交换虚拟服务器是接收流量并在内部将其定向到相应的虚拟服务器的服务器。内容交换虚拟服务器是 Unified Gateway 功能的主要组成部分。

在 11.0 之前的版本中，内容切换可用于接收多个虚拟服务器的流量。这种用途也称为 Unified Gateway 吗?
**

早于 11.0 的版本支持使用内容交换虚拟服务器接收多个虚拟服务器的流量。但是，内容交换无法将流量引导到 Citrix Gateway 虚拟服务器。

11.0 中的增强功能使内容交换虚拟服务器能够将流量引导到任何虚拟服务器（包括 Citrix Gateway 虚拟服务器）。

Unified Gateway 中的内容交换策略发生了什么变化?
**

1. 为内容切换操作添加了一个新的命令行参数 “-targetVserver”。新参数用于指定目标 Citrix Gateway 虚拟服务器。示例：


```
add cs action UG_CSACT_MyUG -targetVserver UG_VPN_MyUG
```

在 Citrix Gateway 配置实用程序中，内容交换操作具有一个新选项，即“目标虚拟服务器”，该选项可引用 Citrix Gateway 虚拟服务器。

2. 新的高级策略表达式 is_vpn_url 可用于匹配 Citrix Gateway 和特定于身份验证的请求。

Unified Gateway 当前不支持哪些 Citrix Gateway 功能?
**

Unified Gateway 支持所有功能。但是，通过 VPN 插件本机登录报告了一个小问题（问题 ID 544325）。在这种情况下，无缝单点登录 (SSO) 不起作用。

使用 Unified Gateway，EPA 扫描的行为是什么?
**

使用 Unified Gateway 时，仅针对 Citrix Gateway 访问方法触发终端分析，而不针对 AAAA-TM 访问触发。如果用户尝试访问 AAAA-TM 虚拟服务器，即使在 Citrix Gateway 虚拟服务器上完成了身份验证，则不会触发 EPA 扫描。但是，如果用户试图获得无客户端 VPN/ 完全 VPN 访问权限，则触发配置的 EPA 扫描。在这种情况下，将完成身份验证或无缝 SSO。

设置

Unified Gateway 的许可证要求是什么?
**

仅高级和高级许可证支持 Unified Gateway。它不适用于 Citrix Gateway 或标准许可证版本。

与 Unified Gateway 一起使用的 Citrix Gateway 虚拟服务器是否需要 IP/端口/SSL 配置?
**

对于与 Unified Gateway 虚拟服务器一起使用的 Citrix Gateway 虚拟服务器，Citrix Gateway 虚拟服务器上不需要 IP/port /SSL 配置。但是，对于 RDP 代理功能，您可以将相同的 SSL/TLS 服务器证书绑定到 Citrix Gateway 虚拟服务器。

是否需要重新配置 Citrix Gateway 虚拟服务器上的 SSL/TLS 证书以便与 Unified Gateway 虚拟服务器配合使用?
**

您无需重新设置当前绑定到 Citrix Gateway 虚拟服务器的证书。您可以自由地重复使用任何现有 SSL 证书，并将这些证书绑定到 Unified Gateway 虚拟服务器。

单个 URL 和多主机部署有什么区别? 我需要哪一个?
**

单个 URL 是指 Unified Gateway 虚拟服务器能够处理一个完全限定域名 (FQDN) 的流量。当 Unified Gateway 使用使用 FQDN 填充证书主体的 SSL/TLS 服务器证书时，存在此限制。例如：ug.citrix.com

但是，如果 Unified Gateway 使用通配符服务器证书，它可以处理多个子域的流量。例如：

另一个选项是带有服务器名称指示器 (SNI) 功能的 SSL/TLS 配置，以允许绑定多个 SSL/TLS 服务器证书。示例：身份验证、身份验证、身份验证、身份验证、身份验证、身份验证、身份验证

单个主机与多个主机类似于网站通常托管在 Web 服务器上的方式（例如 Apache HTTP 服务器或 Microsoft Internet 信息服务 (IIS)）。如果有单个主机，您可以使用站点路径切换流量，就像在 Apache 中使用别名或“虚拟目录”的方式一样。如果有多个主机，则可以使用主机头来切换流量，类似于在 Apache 中使用虚拟主机的方式。

身份验证

Unified Gateway 可以使用哪些身份验证机制?
**

与 Citrix Gateway 一起使用的所有现有身份验证机制都与 Unified Gateway 一起工作。

这些包括 LDAP、RADIUS、SAML、Kerberos、基于证书的身份验证等。

当 Citrix Gateway 虚拟服务器置于 Unified Gateway 虚拟服务器后面时，将自动使用升级前在 Citrix Gateway 虚拟服务器上配置的任何身份验证机制。除了向 Citrix Gateway 虚拟服务器分配不可寻址的 IP 地址 (0.0.0.0) 之外，不涉及其他配置步骤。

什么是“自我身份验证”身份验证?
**

自我身份验证本身并不是一种身份验证类型。自我身份验证描述如何创建 URL。新的命令行参数 ssotype 可用于 VPN URL 配置。示例:

```
\> add vpn url RGB RGB "http://blue.citrix.lab/"-vServerName Blue -ssotype
selfauth
```

自我身份验证是 ssotype 参数的值之一。此类型的 URL 可用于访问与 Unified Gateway 虚拟服务器不在同一域中的资源。配置书签时，可以在配置实用程序中看到该设置。

什么是“递升式”身份验证?
**

当访问 AAAA-TM 资源需要额外的更安全级别的身份验证时，您可以使用递升式身份验证。在命令行上，使用 authnProfile 命令来设置 authenticationLevel 参数。示例:

> add authentication authnProfile AuthProfile -authnVsName AAATMVserver -AuthenticationHost auth.citrix.lab -AuthenticationDomain citrix.lab -AuthenticationLevel 100

此身份验证配置文件绑定到负载平衡虚拟服务器。

AAA-TM 虚拟服务器是否支持递升式身份验证?
**

是的，它是支持的。

什么是登录一次/注销一次?
**

登录一次：VPN 用户登录一次 AAAA-TM 或 Citrix Gateway 虚拟服务器。从那时起，VPN 用户可以无缝访问所有企业/云/Web 应用程序。用户无需重新进行身份验证。但是，对特殊情况（如 AAA-TM 递升式）进行重新身份验证。

注销一次：创建第一个 AAAA-TM 或 Citrix Gateway 会话后，它将用于为该用户创建后续的 AAAA-TM 或 Citrix Gateway 会话。如果这些会话中的任何一个已注销，Citrix ADC 设备也会注销用户的其他应用程序或会话。

是否可以在 Unified Gateway 级别指定常用身份验证策略，并在负载平衡虚拟服务器级别指定 AAAA-TM 负载平衡虚拟服务器特定身份验证绑定？支持此用例的配置步骤是什么？
**

如果需要为 Unified Gateway 后面的 AAAA-TM 虚拟服务器指定单独的身份验证策略，则需要有一个单独的、可独立寻址的身份验证虚拟服务器（类似于普通的 AAAA-TM 配置）。负载平衡虚拟服务器上的身份验证主机设置必须指向此身份验证虚拟服务器。

如何配置 Unified Gateway，以便绑定的 AAAA-TM 虚拟服务器具有自己的身份验证策略？
**

在这种情况下，负载平衡服务器必须将身份验证 FQDN 选项设置为指向 AAA-TM 虚拟服务器。AAAA-TM 虚拟服务器必须具有独立的 IP 地址，并且可以从 Citrix ADC 和客户端访问。

对通过 Unified Gateway 虚拟服务器对用户进行身份验证是否需要 AAAA-TM 身份验证虚拟服务器？
**

否。Citrix Gateway 虚拟服务器甚至会对 AAA-TM 用户进行身份验证。

在哪里指定 Citrix Gateway 身份验证策略 - 在 Unified Gateway 虚拟服务器或 Citrix Gateway 虚拟服务器上？
**

身份验证策略将绑定到 Citrix Gateway 虚拟服务器。

如何在 Unified Gateway 内容交换虚拟服务器后面的 AAAA-TM 虚拟服务器上启用身份验证？
**

在 AAAA-TM 上启用身份验证，并将身份验证主机指向 Unified Gateway 内容交换 FQDN。

AAA 交通管理

如何在内容切换（单 URL 与多主机）后面添加 TM 虚拟服务器？
**

为单个 URL 添加 AAAA-TM 虚拟服务器与为多个主机添加该虚拟服务器之间没有区别。在任何一种情况下，虚拟服务器都会在内容切换操作中作为目标添加。单 URL 与多主机之间的区别由内容切换策略规则实现。

如果将虚拟服务器移到 Unified Gateway 虚拟服务器后面，绑定到 AAAA-TM 负载平衡虚拟服务器的身份验证策略会发生什么情况？
**

身份验证策略绑定到身份验证虚拟服务器，身份验证虚拟服务器绑定到负载平衡虚拟服务器。对于 Unified Gateway 虚拟服务器，Citrix 建议将 Citrix Gateway 虚拟服务器作为单一身份验证点，这样就不需要在身份验证虚拟服务器上

执行身份验证（甚至不需要特定身份验证虚拟服务器）。将身份验证主机指向 Unified Gateway 虚拟服务器 FQDN 可确保由 Citrix Gateway 虚拟服务器完成身份验证。如果将身份验证主机指向 Unified Gateway 的内容切换，并且仍具有身份验证虚拟服务器绑定，绑定到身份验证虚拟服务器的身份验证策略将被忽略。但是，如果将身份验证主机指向独立的可寻址身份验证虚拟服务器，绑定的身份验证策略将生效。

如何为 AAA-TM 会话配置会话策略?
**

如果在 Unified Gateway 中，未为 AAAA-TM 虚拟服务器指定身份验证虚拟服务器，则 AAA-TM 会话将继承 Citrix Gateway 会话策略。如果指定了身份验证虚拟服务器，则应用绑定到该虚拟服务器的 AAA-TM 会话策略。

门户定制

Citrix ADC 11.0 中的 Citrix Gateway 门户有哪些更改?
**

在 Citrix ADC 早于 11.0 的版本中，可以在全局级别设置单个门户自定义。给定 Citrix ADC 设备中的每个网关虚拟服务器都使用全局门户自定义。

在 Citrix ADC 11.0 中，通过门户主题功能，您可以设置多个门户主题。主题可以全局绑定，也可以绑定到特定的虚拟服务器。

Citrix ADC 11.0 是否支持 Citrix Gateway 门户自定义?
**

使用配置实用程序，您可以使用新的门户主题功能完全自定义和创建新的门户主题。您可以上传不同的图片，设置配色方案，更改文本标签等。

可以自定义的门户页面包括：

- 登录页面
- 端点分析页面
- 端点分析错误页面
- 后端点分析页面
- VPN 连接页面
- 门户网站主页

在此版本中，您可以使用独特的门户设计自定义 Citrix Gateway 虚拟服务器。

Citrix ADC 高可用性或群集部署中是否支持门户主题?
**

是。Citrix ADC 高可用性和群集部署支持门户主题。

我的自定义项是否会作为 Citrix ADC 11.0 升级过程的一部分进行迁移?
**

否。升级到 Citrix ADC 11.0 时，不会自动迁移通过 rc.conf/rc.netScaler 文件修改或使用 10.1/10.5 中的自定义主题功能调用的 Citrix Gateway 门户页面的现有自定义项。

是否有任何升级前步骤可以为 Citrix ADC 11.0 中的门户主题做好准备?
**

必须从 rc.conf 或 rc.netScaler 文件中删除任何现有的自定义项。

另一种选择是，如果使用了自定义主题，则必须为它们分配默认设置：

导航到配置 **> Citrix Gateway >** 全局设置

点击 更改全局设置。单击 客户端体验，然后从 **UI** 主题下拉列表中选择 默认值。

我有自定义项存储在 Citrix ADC 实例上，由 rc.conf 或 rc.netScaler 调用。如何移动到门户主题?
**

Citrix 知识中心文章 CTX126206 详细介绍了针对 Citrix ADC 9.3 和 10.0 发行版的此类配置（最高至 10.0 Build 73.5001.e）。自 Citrix ADC 10.0 构建 10.0 73.5002.e（包括 10.1 和 10.5）以来，UIVE 自定义参数可帮助客户在重新启动过程中保留其自定义设置。如果自定义项存储在 Citrix ADC 硬盘驱动器上，并且您希望继续使用这些自定义项，请备份 11.0 GUI 文件并将其插入到现有的自定义主题文件中。如果要移动到门户主题，必须首先在“全局设置”或“会话”配置文件中的“客户端体验”下取消设置 UIVEME 参数。或者，您可以将其设置为默认值或绿色泡沫。然后，您可以开始创建和绑定门户主题。

如何在升级到 Citrix ADC 11.0 之前导出当前的自定义设置并保存它们? 是否可以将导出的文件移动到其他 Citrix ADC 设备?
**

上传到 ns_gui_custom 文件夹的自定义文件位于磁盘上，并在升级过程中保留。但是，这些文件可能不完全兼容新的 Citrix ADC 11.0 内核和作为内核一部分的其他 GUI 文件。因此，Citrix 建议备份 11.0 GUI 文件并自定义备份。

此外，配置实用程序中没有将 ns_custom_gui 文件夹导出到另一个 Citrix ADC 设备的实用程序。您必须使用 SSH 或文件传输实用程序（如 WinSCP）才能从 Citrix ADC 实例中取出文件。

AAAA-TM 虚拟服务器是否支持门户主题?
**

是。AAA-TM 虚拟服务器支持门户主题。

RDP 代理

Citrix Gateway 11.0 的 RDP 代理中发生了什么变化?
**

自 Citrix ADC 10.5.e 增强版本以来，已对 RDP 代理进行了许多增强。在 Citrix ADC 11.0 中，该功能可从第一个发布的版本中获得。

许可变更

Citrix ADC 11.0 中的 RDP 代理功能只能用于高级版和高级版本。必须为每个用户获得 Citrix 并发用户 (CCU) 许可证。

启用命令

在 Citrix ADC 10.5.e 中，没有用于启用 RDP 代理的命令。在 Citrix ADC 11.0 中，已添加启用命令：

> 启用功能 rdpproxy

该功能必须获得许可才能运行此命令。

其他 **RDP** 代理更改

服务器配置文件上的预共享密钥 (PSK) 属性已成为必填项。

要将 RDP 代理的现有 Citrix ADC 10.5.e 配置迁移到 Citrix ADC 11.0，应理解并解决以下详细信息。

如果管理员想要将现有 RDP 代理配置添加到选定的 Unified Gateway 部署中：

- 必须编辑 Citrix Gateway 虚拟服务器的 IP 地址并将其设置为不可寻址的 IP 地址 (0.0.0.0)。
- 任何 SSL/TLS 服务器证书，身份验证策略都必须绑定到 Citrix Gateway 虚拟服务器，该虚拟服务器是所选 Unified Gateway 组成部分。

如何将基于 Citrix ADC 10.5.e 的远程桌面协议 (RDP) 代理配置迁移到 Citrix ADC 11.0?
**

选项 1：使用高级许可证或高级许可证保留具有 RDP 代理配置的现有 Citrix Gateway 虚拟服务器。

选项 2：移动具有 RDP 代理配置的现有 Citrix Gateway 虚拟服务器，将其置于 Unified Gateway 虚拟服务器后面。

选项 3：将具有 RDP 代理配置的独立 Citrix Gateway 虚拟服务器添加到现有标准版设备。

如何使用 Citrix ADC 11.0 发行版为 RDP 代理配置设置 Citrix Gateway?
**

有两个选项可用于使用 NS 11.0 版本部署 RDP 代理：

1) 使用面向外部的 Citrix Gateway 虚拟服务器。这需要 Citrix Gateway 虚拟服务器一个外部可见的 IP 地址 /FQDN。此选项是 Citrix ADC 10.5.e 中可用的选项。

2) 使用 Unified Gateway 虚拟服务器前端 Citrix Gateway 虚拟服务器。

使用选项 2，Citrix Gateway 虚拟服务器不需要自己的 IP 地址 /FQDN，因为它使用不可寻址的 IP 地址 (0.0.0.0)。

与其他 **Citrix** 软件集成

HDX Insight 能否与 Unified Gateway 一起工作?
**

使用 Unified Gateway 部署 Citrix Gateway 时，Citrix Gateway 虚拟服务器必须具有绑定到该网关的有效 SSL 证书，并且该证书必须处于 UP 状态，才能为 Citrix ADC Insight Center 生成 AppFlow 记录，以便进行 HDX Insight 报告。

如何迁移现有 HDX Insight 配置?
**

不需要移徙。如果 Citrix Gateway 虚拟服务器置于 Unified Gateway 虚拟服务器后面，绑定到 Citrix Gateway 虚拟服务器的 AppFlow 策略将继承该策略。

对于 Citrix Gateway 虚拟服务器的 Citrix ADC Insight Center 中的现有数据，有两种可能性：

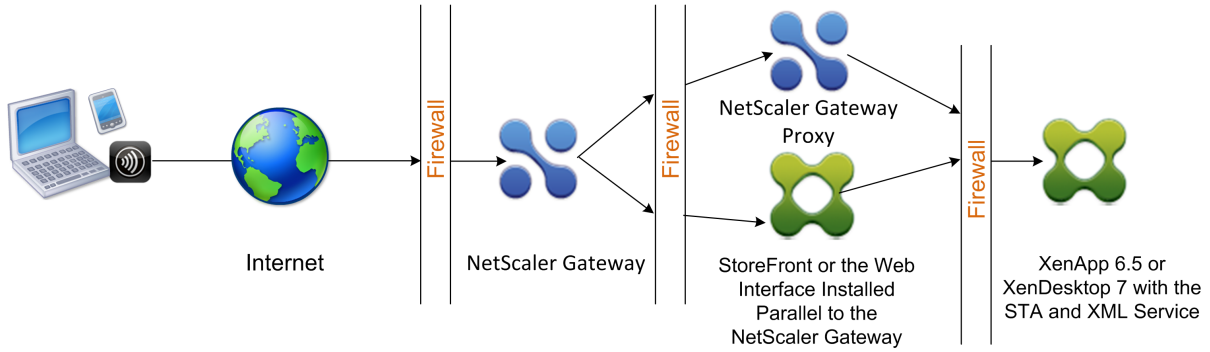
- 如果 Citrix Gateway 虚拟服务器的 IP 地址作为迁移到 Unified Gateway 的一部分分配给 Unified Gateway 虚拟服务器，则数据将保持链接到 Citrix Gateway 虚拟服务器
- 如果为 Unified Gateway 虚拟服务器分配了一个单独的 IP 地址，则 Citrix Gateway 虚拟服务器的 AppFlow 数据将链接到新 IP 地址。因此，现有数据不会成为新数据的一部分。

在双跃点 **DMZ** 中部署

April 6, 2020

一些组织使用三个防火墙来保护其内部网络。三个防火墙将 DMZ 分为两个阶段，为内部网络提供额外的安全层。此网络配置称为双跃点 DMZ。

图 1. 部署在双跃点 DMZ 中的 Citrix Gateway 设备



> 注意：出于说明目的，上述示例介绍了使用具有 StoreFront、Web Interface 和 Citrix Virtual Apps 的三个防火墙的双跃点配置，但您也可以使用 DMZ 中的一个设备和安全网络中的一个设备的双跃点 DMZ。如果使用 DMZ 中的一个设备和安全网络中的一个设备配置双跃点配置，则可以忽略在第三个防火墙上打开端口的说明。

您可以配置双跃点 DMZ 以使用 Citrix StoreFront 或与 Citrix Gateway 代理并行安装的 Web Interface。用户通过使用 Citrix Workspace 应用进行连接。

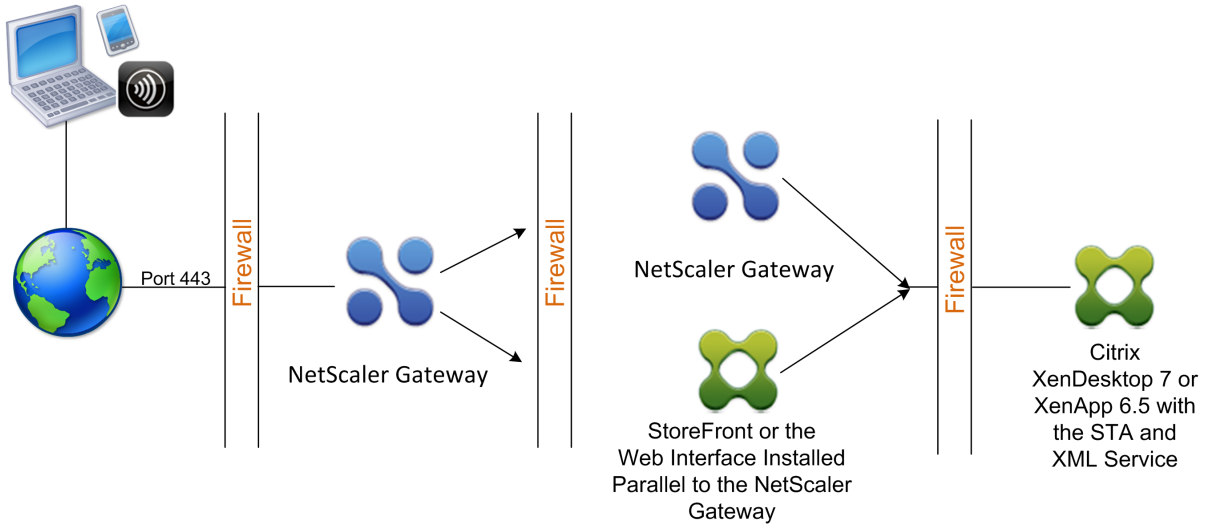
> 注意：如果在具有 StoreFront 的双跳 DMZ 中部署 Citrix Gateway，则 Citrix Workspace 应用程序的基于电子邮件的自动发现将不起作用。

在双跃点 DMZ 中部署 Citrix Gateway

April 6, 2020

一些组织使用三个防火墙来保护其内部网络。三个防火墙将 DMZ 分为两个阶段，为内部网络提供额外的安全层。此网络配置称为双跃点 DMZ。可以使用 Citrix Virtual Apps 和 StoreFront 在双跃点 DMZ 中部署 Citrix Gateway。

图 1. 部署在双跃点 DMZ 中的 Citrix Gateway 设备



注意：为了说明，上述示例介绍了使用三个防火墙和 Web Interface 的双跃点配置，但您也可以使用 DMZ 中的一个设备和安全网络中的一个设备的双跃点 DMZ。如果使用 DMZ 中的一个设备和安全网络中的一个设备配置双跃点配置，则可以忽略在第三个防火墙上打开端口的说明。

您可以配置双跃点 DMZ 以使用 Citrix StoreFront 或 Web Interface。用户通过使用 Citrix Workspace 应用进行连接。

> 注意
>
> 如果在具有 StoreFront 的双跳 DMZ 中部署 Citrix Gateway，则 Citrix Workspace 应用程序的基于电子邮件的自动发现将不起作用。

双跃点部署的工作原理

April 6, 2020

可以在双跃点 DMZ 中部署 Citrix Gateway 设备，以控制对运行 Citrix Virtual Apps 的服务器的访问。双跃点部署中的连接发生如下所示：

- 用户通过使用 Web 浏览器并使用 Citrix Workspace 应用程序选择已发布的应用程序连接到第一个 DMZ 中的 Citrix Gateway。

- Citrix Workspace 应用程序在用户设备上启动。用户连接到 Citrix Gateway 以访问在安全网络中服务器场中运行的已发布应用程序。

  注意：双跃点 DMZ 部署不支持 Secure Hub 和 Citrix Gateway 插件。仅 Citrix Workspace 应用程序用于用户连接。

- 第一个 DMZ 中的 Citrix Gateway 处理用户连接并执行 SSL VPN 的安全功能。此 Citrix Gateway 对用户连接进行加密，确定如何对用户进行身份验证，并控制对内部网络中服务器的访问。
- 第二个 DMZ 中的 Citrix Gateway 用作 Citrix Gateway 代理设备。此 Citrix Gateway 使 ICA 流量能够遍历第二个 DMZ，以完成与服务器场的用户连接。第一个 DMZ 中的 Citrix Gateway 与内部网络中的安全票证颁发机构 (STA) 之间的通信也可通过第二个 DMZ 中的 Citrix Gateway 进行代理。

Citrix Gateway 支持 IPv4 和 IPv6 连接。您可以使用配置实用程序配置 IPv6 地址。

下表建议了对各种 ICA 功能的双跳部署支持：

ICA 功能	双跳支持
SmartAccess	是
SmartControl	是
Enlightened Data Transport (EDT)	是
HDX Insight	是
ICA 会话可靠性（端口 2598）	是
ICA 会话迁移	是
ICA 会话超时	是
多流 ICA	是
Framehawk	否
UDP 音频	否

双跃点 **DMZ** 部署中的通信流

April 6, 2020

要了解双跃点 DMZ 部署中涉及的配置问题，您应基本了解双跃点 DMZ 部署中的各种 Citrix Gateway 和 Citrix Virtual Apps 组件如何通信以支持用户连接。StoreFront 和 Web Interface 的连接过程是相同的。

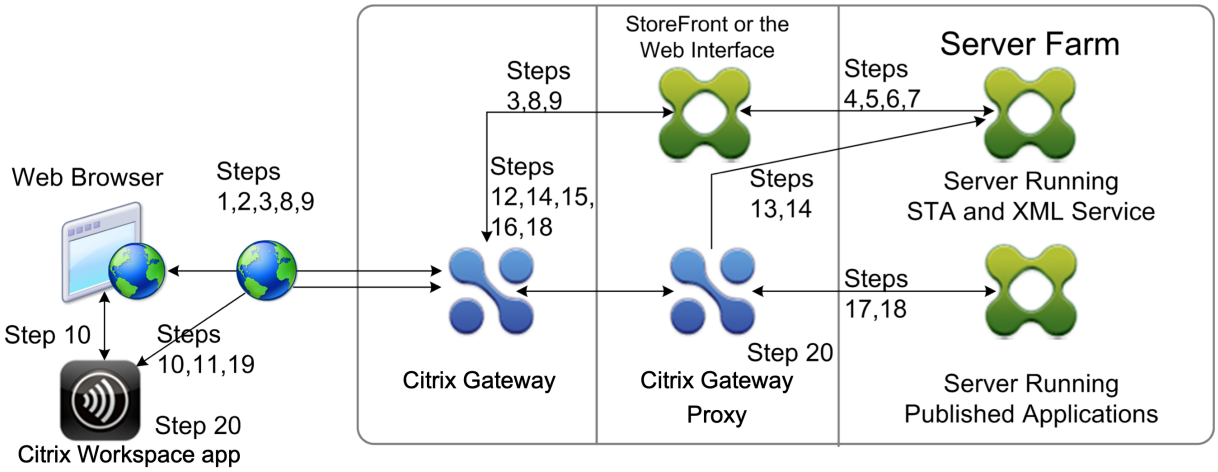
尽管用户连接过程发生在一个连续流程中，但以下四个主题中详细介绍了这些步骤：

- 对用户进行身份验证

- 创建会话票证
- 启动 Citrix Workspace 应用程序
- 完成连接

下图显示了用户连接到 StoreFront 或 Web Interface 的过程中出现的步骤。在安全网络中，运行 Citrix Virtual Apps 的计算机还运行 Secure Ticket Authority (STA)、XML Service 和已发布的应用程序。

图 1. 双跃点 DMZ 用户连接过程

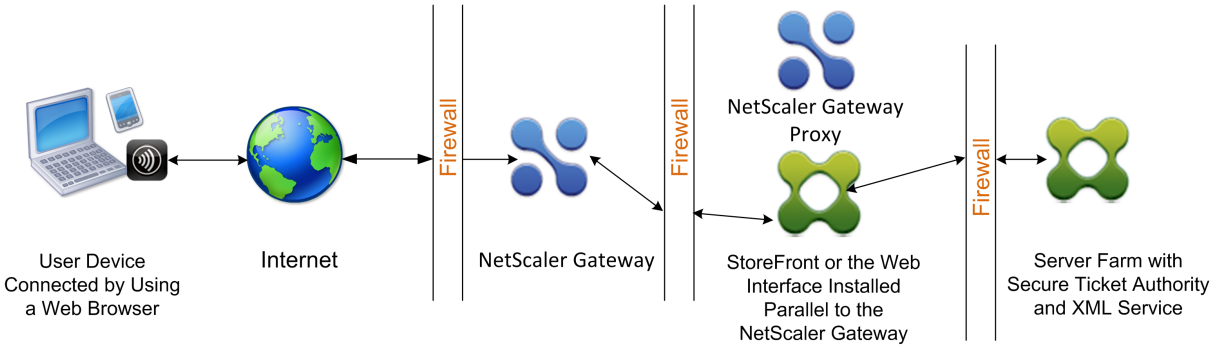


对用户进行身份验证

April 6, 2020

对用户进行身份验证是双跃点 DMZ 部署中用户连接过程的第一步。下图显示了此部署中的用户连接过程。

图 1. 双跃点 DMZ 中用户身份验证的通信流



在用户身份验证阶段，将发生以下基本过程：

1. 用户键入 Citrix Gateway 的地址，例如https://www.ng.wxyco.com 在 Web 浏览器中以连接到第一个 DMZ 中的 Citrix Gateway。如果在 Citrix Gateway 上启用了登录页身份验证，Citrix Gateway 将对用户进行身份验证。

2. 第一个 DMZ 中的 Citrix Gateway 接收请求。
3. Citrix Gateway 将 Web 浏览器连接重定向到 Web Interface。
4. Web Interface 将用户凭据发送到内部网络中服务器场中运行的 Citrix XML 服务。
5. Citrix XML 服务对用户进行身份验证。
6. XML 服务创建用户有权访问的已发布应用程序的列表，并将此列表发送到 Web Interface。

如果在 Citrix Gateway 上启用身份验证，设备将向用户发送 Citrix Gateway 登录页。用户在登录页面上输入身份验证凭据，设备将对用户进行身份验证。然后 Citrix Gateway 将用户凭据返回到 Web Interface。

如果未启用身份验证，Citrix Gateway 将不执行身份验证。设备连接到 Web Interface，检索 Web Interface 登录页，并将 Web Interface 登录页发送给用户。用户在 Web Interface 登录页面上输入身份验证凭据，Citrix Gateway 将用户凭据传回 Web Interface。

创建会话票证

April 6, 2020

创建会话票证是双跃点 DMZ 部署中用户连接过程的第二阶段。

在会话工单创建阶段，会发生以下基本过程：

1. Web Interface 与内部网络中的 XML 服务和安全票证颁发机构 (STA) 进行通信，以便为用户有权访问的每个已发布应用程序生成会话票证。会话票证包含运行托管已发布应用程序的 Citrix Virtual Apps 的计算机的别名地址。
2. STA 保存承载已发布应用程序的服务器的 IP 地址。然后 STA 将请求的会话票证发送到 Web Interface。每个会话票证都包含一个别名，该别名代表承载已发布应用程序的服务器的 IP 地址，但不代表实际的 IP 地址。
3. Web Interface 为每个已发布的应用程序生成 ICA 文件。ICA 文件包含 STA 签发的票据。然后，Web Interface 创建并填充一个网页，其中包含指向已发布应用程序的链接列表，并将此网页发送到用户设备上的 Web 浏览器。

启动 **Citrix Workspace** 应用程序

April 6, 2020

启动 Citrix Workspace 应用程序是双跳 DMZ 部署中用户连接过程的第三阶段。基本过程如下：

1. 用户在 Web Interface 中单击指向已发布应用程序的链接。Web Interface 将该已发布应用程序的 ICA 文件发送到用户设备的浏览器。

   ICA 文件包含指示 Web 浏览器启动 Receiver 的数据。

   ICA 文件还包含第一个 DMZ 中 Citrix Gateway 的完全限定域名 (FQDN) 或域名系统 (DNS) 名称。

2. Web 浏览器启动 Receiver，用户通过使用 ICA 文件中的 Citrix Gateway 名称连接到第一个 DMZ 中的 Citrix Gateway。初始 SSL/TLS 握手是为了建立运行 Citrix Gateway 的服务器的标识。

完成连接

April 6, 2020

完成连接是双跃点 DMZ 部署中用户连接过程的第四个也是最后一个阶段。

在连接完成阶段，会发生以下基本过程：

- 用户在 Web Interface 中单击指向已发布应用程序的链接。
- Web 浏览器接收由 Web Interface 生成的 ICA 文件，并启动 Citrix Workspace 应用程序。
  注意：ICA 文件包含指示 Web 浏览器启动 Citrix Workspace 应用程序的代码。
- Citrix Workspace 应用程序在第一个 DMZ 中启动与 Citrix Gateway 的 ICA 连接。
- 第一个 DMZ 中的 Citrix Gateway 与内部网络中的 Secure Ticket Authority (STA) 通信，以便将会话票证中的别名地址解析为运行 Citrix Virtual Apps 或 StoreFront 的计算机的真实 IP 地址。此通信由 Citrix Gateway 代理通过第二个 DMZ 进行代理。
- 第一个 DMZ 中的 Citrix Gateway 完成了与 Citrix Workspace 应用程序的 ICA 连接。
- Citrix Workspace 应用程序现在可以通过两个 Citrix Gateway 设备与内部网络上运行 Citrix Virtual Apps 程序的计算机进行通信。

完成用户连接过程的详细步骤如下：

1. Citrix Workspace 应用程序将已发布应用程序的 STA 票证发送到第一个 DMZ 中的 Citrix Gateway。
2. 第一个 DMZ 中的 Citrix Gateway 与内部网络中的 STA 联系以进行票证验证。若要与 STA 联系，Citrix Gateway 会在第二个 DMZ 中建立一个 SOCKS 或 SOCKS 与 Citrix Gateway 代理的 SSL 连接。
3. 第二个 DMZ 中的 Citrix Gateway 代理将票证验证请求传递给内部网络中的 STA。STA 验证票证并将其映射到运行托管已发布应用程序的 Citrix Virtual Apps 的计算机。
4. STA 向第二个 DMZ 中的 Citrix Gateway 代理发送响应，该响应将传递给第一个 DMZ 中的 Citrix Gateway。此响应完成票证验证，并包括承载已发布应用程序的计算机的 IP 地址。
5. 第一个 DMZ 中的 Citrix Gateway 将 Citrix Virtual Apps 服务器的地址合并到用户连接数据包中，并将此数据包发送到第二个 DMZ 中的 Citrix Gateway 代理。
6. 第二个 DMZ 中的 Citrix Gateway 代理向连接数据包中指定的服务器发出连接请求。
7. 服务器响应第二个 DMZ 中的 Citrix Gateway 代理。第二个 DMZ 中的 Citrix Gateway 代理将此响应传递给第一个 DMZ 中的 Citrix Gateway，以完成第一个 DMZ 中的服务器与 Citrix Gateway 之间的连接。
8. 第一个 DMZ 中的 Citrix Gateway 通过将最终连接数据包传递给用户设备来完成 SSL/TLS 握手。建立从用户设备到服务器的连接。
9. ICA 流量通过第一个 DMZ 中的 Citrix Gateway 和第二个 DMZ 中的 Citrix Gateway 代理在用户设备和服务器之间流动。

准备双跃点 **DMZ** 部署

April 6, 2020

要在配置双跃点 DMZ 部署时进行适当准备并避免不必要的问题，您应回答以下问题：。

- 我是否要支持负载平衡?
- 我需要在防火墙上打开哪些端口?
- 我需要多少个 SSL 证书?
- 在开始部署之前，我需要哪些组件?

本节中的主题包含有助于您根据环境回答这些问题的信息。

开始部署所需的组件

在开始双跃点 DMZ 部署之前，请确保您具有以下组件：

- 至少必须有两个 Citrix Gateway 设备可用（每个 DMZ 一个）。
- 运行 Citrix Virtual Apps 的服务器必须在内部网络中安装并运行。
- Web Interface 或 StoreFront 必须安装在第二个 DMZ 中，并配置为与内部网络中的服务器场一起运行。
- 至少必须在第一个 DMZ 的 Citrix Gateway 上安装一个 SSL 服务器证书。此证书可确保 Web 浏览器和与 Citrix Gateway 的用户连接进行加密。

  如果要对双跃点 DMZ 部署中其他组件之间发生的连接进行加密，则需要其他证书。

在双跃点 **DMZ** 中安装和配置 **Citrix Gateway**

January 10, 2023

您需要完成几个步骤才能在双跃点 DMZ 中部署 Citrix Gateway。这些步骤包括在两个 DMZ 中安装设备以及为用户设备连接配置设备。

在第一个 **DMZ** 中安装 **Citrix Gateway**

要在第一个 DMZ 中安装 Citrix Gateway，请按照中的说明操作安装 MPX 5500 型设备。

如果要在第一个 DMZ 中安装多个 Citrix Gateway 设备，则可以在负载均衡器后面部署这些设备。

在第一个 **DMZ** 中配置 **Citrix Gateway**

在双跃点 DMZ 部署中，必须配置第一个 DMZ 中的每个 Citrix Gateway 以将连接重定向到第二个 DMZ 中的 StoreFront 或 Web Interface。

重定向到 StoreFront 或 Web Interface 将在 Citrix Gateway 全局或虚拟服务器级别执行。要通过 Citrix Gateway 连接到 Web Interface，用户必须与已启用 Web Interface 重定向的 Citrix Gateway 用户组关联。

在第二个 **DMZ** 中安装 **Citrix Gateway**

第二个 DMZ 中的 Citrix Gateway 设备称为 Citrix Gateway 代理，因为它代理跨第二个 DMZ 的 ICA 和安全票证颁发机构 (STA) 流量。

按照中的说明安装 MPX 5500 型设备在第二个 DMZ 中安装每个 Citrix Gateway 设备。

您可以使用此安装过程在第二个 DMZ 中安装其他设备。

在第二个 DMZ 中安装 Citrix Gateway 设备后，您可以配置以下设置：

- 在 Citrix Gateway 代理上配置虚拟服务器。
- 将第一个和第二个 DMZ 中的 Citrix Gateway 设备配置为相互通信。
- 将第二个 DMZ 中的 Citrix Gateway 全局绑定或绑定到虚拟服务器。
- 在第一个 DMZ 中的设备上配置 STA。
- 在分隔 DMZ 的防火墙中打开端口。
- 在设备上安装证书。

在 **Citrix Gateway** 代理上的虚拟服务器上配置设置

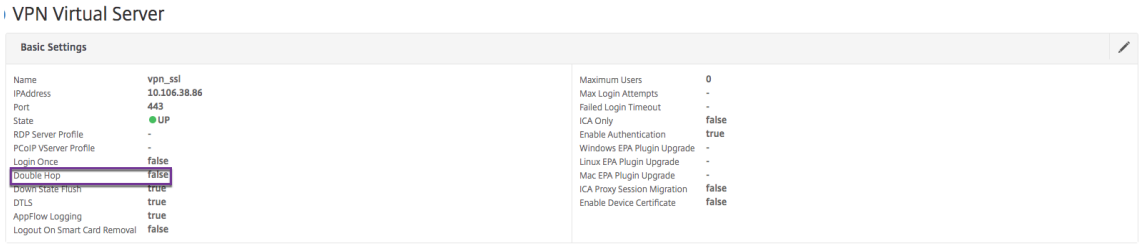
April 6, 2020

要允许在 Citrix Gateway 设备之间传递连接，请在 Citrix Gateway 代理上的虚拟服务器中启用双跃点。

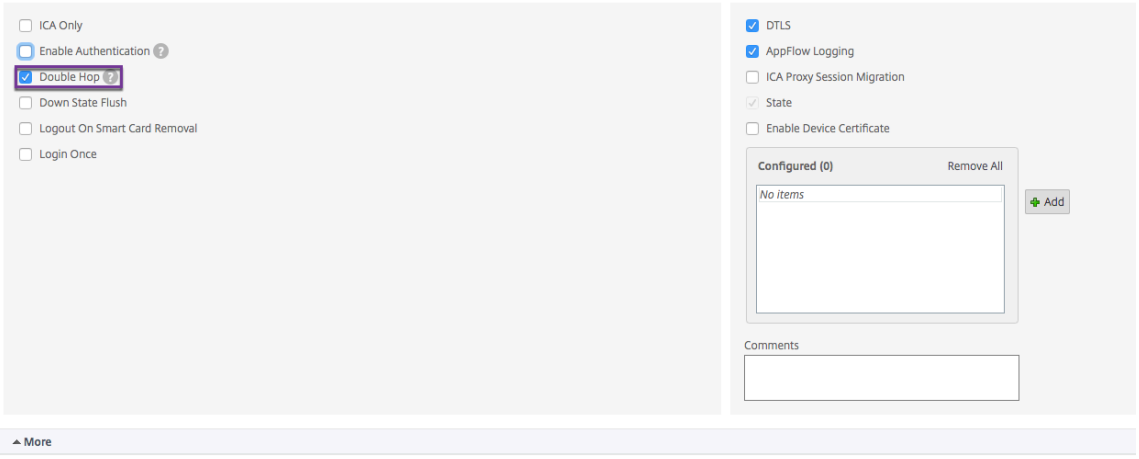
用户连接时，Citrix Gateway 设备会对用户进行身份验证，然后将连接代理到代理设备。在第一个 DMZ 中的 Citrix Gateway 上，将虚拟服务器配置为与第二个 DMZ 中的 Citrix Gateway 通信。请勿在 Citrix Gateway 代理上配置身份验证或策略。Citrix 建议在虚拟服务器上禁用身份验证。

使用 **GUI** 在 **Citrix Gateway** 代理上的虚拟服务器上启用双跃点

1. 导航到 配置 **> Citrix Gateway >** 虚拟服务器。
2. 选择一个虚拟服务器，然后单击 编辑。
3. 在 基本设置部分，单击编辑图标，然后单击 更多。



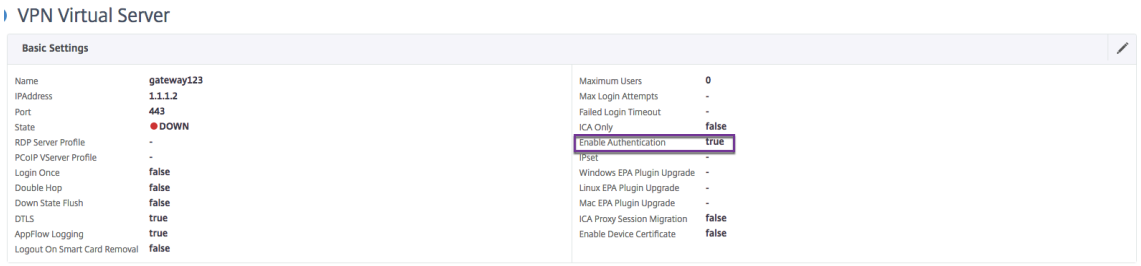
4. 选择 双跳。



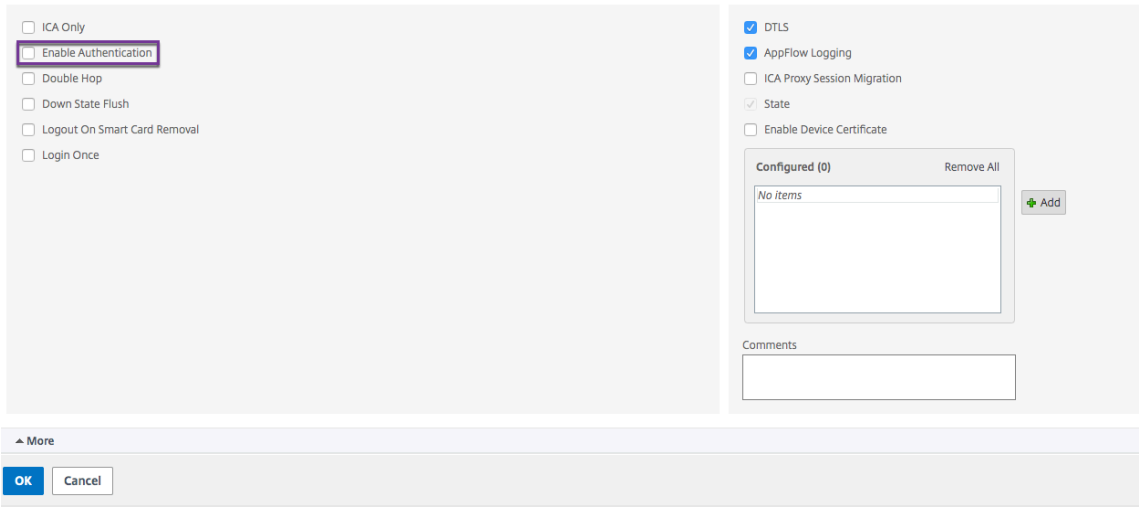
5. 单击确定。

使用 **GUI** 在 **Citrix Gateway** 代理上的虚拟服务器上禁用身份验证的步骤

1. 导航到 配置 **> Citrix Gateway >** 虚拟服务器。
2. 选择一个虚拟服务器，然后单击 编辑。
3. 在 基本设置部分，单击编辑图标，然后单击 更多。



4. 清除 启用身份验证复选框。



5. 单击确定。

将设备配置为与设备代理通信

April 6, 2020

在双跃点 DMZ 中部署 Citrix Gateway 时，必须在第一个 DMZ 中配置 Citrix Gateway，以便与第二个 DMZ 中的 Citrix Gateway 代理进行通信。

如果在第二个 DMZ 中部署多个设备，则可以将第一个 DMZ 中的每个设备配置为与第二个 DMZ 中的每个代理设备进行通信。

注意：如果要使用 IPv6，请使用配置实用程序配置下一跃点服务器。为此，请展开
“Citrix Gateway”>“资源”，然后单击
“下一跃点服务器”。按照以下过程中的步骤操作，然后选中
IPv6 复选框。

将 **Citrix Gateway** 配置为与 **Citrix Gateway** 代理通信的步骤

1. 在配置实用程序中的 “配置” 选项卡上，展开 “Citrix Gateway”>“资源”，然后单击 “下一跃服务器”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在 “名称” 中，键入第一个 Citrix Gateway 的名称。
4. 在 IP 地址中，键入第二个 DMZ 中 Citrix Gateway 代理的虚拟服务器 IP 地址。
5. 在端口中，键入端口号，单击创建，然后单击关闭。如果您使用的是安全端口，例如 443，请选择安全。

必须将安装在第一个 DMZ 中的每个 Citrix Gateway 配置为与第二个 DMZ 中安装的所有 Citrix Gateway 代理设备进行通信。

配置 Citrix Gateway 代理的设置后，将策略绑定到 Citrix Gateway 全局中的下一跃服务器或虚拟服务器。

全局绑定 **Citrix Gateway** 下一跃点服务器

1. 在配置实用程序中的“配置”选项卡上，展开“Citrix Gateway”>“资源”，然后单击“下一跃服务器”。
2. 在详细信息窗格中，选择下一个跃点服务器，然后在“操作”中，选择“全局绑定”。
3. 在“配置下一个合并服务器全局绑定”对话框的“下一个合并服务器名称”中，选择代理设备，然后单击“确定”。

将 **Citrix Gateway** 下一跃点服务器绑定到虚拟服务器

1. 在配置实用程序中的“配置”选项卡上，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，选择虚拟服务器，然后单击“打开”。
3. 在“已发布的应用程序”选项卡上的“下一跃服务器”下，单击项目，然后单击“确定”。

您还可以从“已发布应用程序”选项卡添加下一个跃点服务器。

配置 **Citrix Gateway** 以处理 **STA** 和 **ICA** 流量

April 6, 2020

在双跃点 DMZ 中部署 Citrix Gateway 时，必须在第一个 DMZ 中配置 Citrix Gateway，以适当地处理与安全票证颁发机构 (STA) 和 ICA 流量的通信。运行 STA 的服务器可以绑定到全局或虚拟服务器。

配置 STA 后，您可以将 STA 绑定到全局或虚拟服务器。

要全局配置和绑定 STA，请执行以下操作：

1. 在配置实用程序中的“配置”选项卡上，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“服务器”下，单击“绑定/取消绑定 STA 服务器”以供安全票证颁发机构使用。
3. 在绑定/取消绑定 STA 服务器对话框中，单击添加。
4. 在“配置 STA 服务器”对话框的 URL 中，键入运行 STA 的服务器的路径，如http://mycompany.com 或http://ipAddress ，然后单击“创建”。

要配置 STA 并将其绑定到虚拟服务器，请执行以下操作：

1. 在配置实用程序中的“配置”选项卡上，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，选择虚拟服务器，然后单击“打开”。
3. 在“已发布的应用程序”选项卡上的“安全票证颁发机构”下，单击“添加”。
4. 在“配置 STA 服务器”对话框的 URL 中，键入运行 STA 的服务器的路径，如http://mycompany.com 或http://ipAddress ，然后单击“创建”。

打开防火墙上的适当端口

April 6, 2020

您必须确保在防火墙上打开相应的端口，以支持双跃点 DMZ 部署中涉及的各个组件之间发生的不同连接。有关连接过程的更多信息，请参阅双跃点 DMZ 部署中的通信流。

下图显示了可在双跃点 DMZ 部署中使用的常用端口。

下表显示了通过第一个防火墙发生的连接以及必须打开才能支持连接的端口。

通过第一个防火墙进行连接	使用的端口
来自互联网的 Web 浏览器连接到第一个 DMZ 中的 Citrix Gateway。注意： Citrix Gateway 包含一个用于将端口 80 上建立的连接重定向到安全端口的选项。如果在 Citrix Gateway 上启用此选项，则可以通过第一个防火墙打开端口 80。当用户与端口 80 上的 Citrix Gateway 建立未加密连接时，Citrix Gateway 会自动将连接重定向到安全端口。	通过第一个防火墙打开 TCP 端口 443。
来自互联网的 Citrix Workspace 应用程序连接到第一个 DMZ 中的 Citrix Gateway。	通过第一个防火墙打开 TCP 端口 443。

下表显示了通过第二个防火墙发生的连接以及必须打开才能支持连接的端口。

通过第二个防火墙进行连接	使用的端口
第一个 DMZ 中的 Citrix Gateway 连接到第二个 DMZ 中的 Web Interface。	为不安全的连接打开 TCP 端口 80，或通过第二个防火墙建立安全连接的 TCP 端口 443。
第一个 DMZ 中的 Citrix Gateway 连接到第二个 DMZ 中的 Citrix Gateway。	打开 TCP 端口 443 通过第二个防火墙进行安全的 SOCKS 连接。
如果在第一个 DMZ 中启用 Citrix Gateway 上的身份验证，则此设备可能需要连接到内部网络中的身份验证服务器。	打开身份验证服务器侦听连接的 TCP 端口。示例包括端口 1812 用于 RADIUS 和端口 389 用于 LDAP。

下表显示了通过第三个防火墙发生的连接以及必须打开才能支持连接的端口。

通过第三个防火墙进行连接	使用的端口
StoreFront 或第二个 DMZ 中的 Web Interface 连接到内部网络中服务器上托管的 XML 服务。	为不安全的连接打开端口 80 或通过第三个防火墙建立安全连接的端口 443。
StoreFront 或第二个 DMZ 中的 Web Interface 连接到内部网络中服务器上托管的安全票证机构 (STA)。	为不安全的连接打开端口 80 或通过第三个防火墙建立安全连接的端口 443。

通过第三个防火墙进行连接	使用的端口
第二个 DMZ 中的 Citrix Gateway 连接到驻留在安全网络中的 STA。	为不安全的连接打开端口 80 或通过第三个防火墙建立安全连接的端口 443。
第二个 DMZ 中的 Citrix Gateway 与内部网络中的服务器上的已发布应用程序或虚拟桌面建立 ICA 连接。	打开 TCP 端口 1494 以通过第三个防火墙支持 ICA 连接。如果在 Citrix Virtual Apps 上启用了会话可靠性，请打开 TCP 端口 2598 而非 1494。
如果在第一个 DMZ 中启用 Citrix Gateway 上的身份验证，则此设备可能需要连接到内部网络中的身份验证服务器。	打开身份验证服务器侦听连接的 TCP 端口。示例包括端口 1812 用于 RADIUS 和端口 389 用于 LDAP。

在双跃点 **DMZ** 部署中管理 **SSL** 证书

April 6, 2020

必须安装加密双跃点 DMZ 部署中组件之间的连接所需的 SSL 证书。

在双跃点 DMZ 部署中，部署中涉及的各个组件之间存在多种不同类型的连接。这些连接没有端到端 SSL 加密。但是，每个连接都可以单独加密。

加密连接需要您在连接中涉及的组件上安装适当的 SSL 证书（可信的根证书或服务器证书）。

下表显示了通过第一个防火墙发生的连接以及对其中每个连接进行加密所需的 SSL 证书。必须通过第一个防火墙对连接进行加密，以确保通过 Internet 发送的流量的安全。

通过第一个防火墙进行连接	加密所需的证书
来自互联网的 Web 浏览器连接到第一个 DMZ 中的 Citrix Gateway。	第一个 DMZ 中的 Citrix Gateway 必须安装 SSL 服务器证书。Web 浏览器必须安装与 Citrix Gateway 上的服务器证书相同的证书颁发机构 (CA) 签名的根证书证书。
来自互联网的 Citrix Workspace 应用程序连接到第一个 DMZ 中的 Citrix Gateway。	此连接的证书管理与 Web 浏览器到 Citrix Gateway 连接相同。如果您安装了证书来加密 Web 浏览器连接，则此连接也会使用这些证书加密。

下表显示了通过第二个防火墙发生的连接以及对其中每个连接进行加密所需的 SSL 证书。对这些连接进行加密可增强安全性，但不是强制性的。

通过第二个防火墙进行连接	加密所需的证书
第一个 DMZ 中的 Citrix Gateway 连接到第二个 DMZ 中的 Web Interface。	StoreFront 或 Web Interface 必须安装 SSL 服务器证书。第一个 DMZ 中的 Citrix Gateway 必须安装与 Web Interface 上的服务器证书相同的 CA 签名的根证书。
第一个 DMZ 中的 Citrix Gateway 连接到第二个 DMZ 中的 Citrix Gateway。	第二个 DMZ 中的 Citrix Gateway 必须安装 SSL 服务器证书。第一个 DMZ 中的 Citrix Gateway 必须安装与第二个 DMZ 中 Citrix Gateway 上的服务器证书相同的 CA 签名的根证书。

下表显示了通过第三个防火墙发生的连接以及对其中每个连接进行加密所需的 SSL 证书。对这些连接进行加密可增强安全性，但不是强制性的。

通过第三个防火墙进行连接	加密所需的证书
StoreFront 或第二个 DMZ 中的 Web Interface 连接到内部网络中服务器上托管的 XML 服务。	如果 XML Service 在 Citrix Virtual Apps 服务器上的 Microsoft Internet Information Services (IIS) 服务器上运行，则必须在 IIS 服务器上安装 SSL 服务器证书。如果 XML Service 是标准 Windows 服务（不驻留在 IIS 中），则必须在服务器上的 SSL Relay 内安装 SSL 服务器证书。StoreFront 或 Web Interface 必须安装与 Microsoft IIS 服务器或 SSL Relay 上安装的服务器证书相同的 CA 签名的根证书。
StoreFront 或第二个 DMZ 中的 Web Interface 连接到内部网络中服务器上托管的 STA。	此连接的证书管理与 Web Interface 到 XML 服务连接相同。您可以使用相同的证书来加密此连接。（服务器证书必须驻留在 Microsoft IIS 服务器或 SSL Relay 上。必须在 Web Interface 上安装相应的根证书。）
第二个 DMZ 中的 Citrix Gateway 连接到内部网络中服务器上托管的 STA。	此连接中 STA 的 SSL 服务器证书管理与此表中讨论的前两个连接所描述的相同。（服务器证书必须驻留在 Microsoft IIS 服务器或 SSL Relay 上。）第二个 DMZ 中的 Citrix Gateway 必须安装与 STA 和 XML Service 使用的服务器证书相同的 CA 签名的根证书。
第二个 DMZ 中的 Citrix Gateway 与内部网络中的服务器上的已发布应用程序建立 ICA 连接。	SSL 服务器证书必须安装在托管已发布应用程序的服务器上的 SSL Relay 中继中。第二个 DMZ 中的 Citrix Gateway 代理必须安装与 SSL Relay 中安装的服务器证书相同的 CA 签名的根证书。

使用高可用性

April 6, 2020

两个 Citrix Gateway 设备的高可用性部署可以在任何事务中提供不间断的操作。将一个设备配置为主节点，另一个配置为辅助节点时，主节点接受连接并管理服务器，而辅助节点监视主节点。如果由于任何原因，主节点无法接受连接，则辅助节点将接管。

辅助节点通过发送定期消息（通常称为检测信号消息或运行状况检查）来监视主节点，以确定主节点是否接受连接。如果运行状况检查失败，辅助节点将在指定时间段内重试连接，之后确定主节点无法正常工作。然后，辅助节点接管主节点（称为故障转移的进程）。

故障转移后，所有客户端都必须重新建立与托管服务器的连接，但会话持久性规则保持在故障转移之前的状态。

启用 Web 服务器日志记录持久性时，不会因故障转移而丢失日志数据。要启用日志记录持久性，日志服务器配置必须在 log.conf 文件中包含两个系统的条目。

下图显示了具有高可用性对的网络配置。

图 1. 高可用性配置中的 Citrix Gateway 设备

配置高可用性的基本步骤如下：

1. 创建一个基本设置，其中两个节点都位于同一子网中。
2. 自定义节点传递运行状况检查信息的间隔。
3. 自定义节点保持同步的过程。
4. 自定义命令从主命令到辅助命令的传播。
5. 或者，配置故障安全模式，以防止出现两个节点都不是主节点的情况。
6. 如果您的环境包含不接受 Citrix Gateway 无偿 ARP 消息的设备，请配置虚拟 MAC 地址。

当您准备好进行更复杂的配置时，您可以在不同的子网中配置高可用性节点。

为了提高高可用性设置的可靠性，您可以配置路由监视器并创建冗余链接。在某些情况下，例如故障排除或执行维护任务时，您可能希望强制节点故障转移（将主状态分配给另一个节点），或者强制辅助节点保持辅助节点或强制主节点保持主节点保持主节点。

高可用性的工作原理

April 6, 2020

在高可用性对中配置 Citrix Gateway 时，辅助 Citrix Gateway 会通过发送定期消息（也称为检测信号消息或运行状况检查）来监视第一个设备，以确定第一个设备是否接受连接。如果运行状况检查失败，辅助 Citrix Gateway 将在指定的时间内再次尝试连接，直到确定主设备无法工作。如果辅助设备确认运行状况检查失败，则辅助 Citrix Gateway 接管主 Citrix Gateway。这称为故障转移。

以下端口用于在 Citrix Gateway 设备之间交换与高可用性相关的信息：

- UDP 端口 3003 用于交换 hello 数据包，用于通信时间间隔的状态。
- TCP 端口 3010 用于高可用性配置同步。
- TCP 端口 3011 用于同步配置设置。

配置高可用性的指南

在配置高可用性对之前，您应查看以下准则：

- 每个 Citrix Gateway 设备都必须运行相同版本的 Citrix Gateway 软件。您可以在配置实用程序中找到页面顶部的版本号。
- Citrix Gateway 不会在两台设备之间自动同步密码。您可以选择使用对中其他设备的用户名和密码配置每个 Citrix Gateway。
- 主 Citrix Gateway 和辅助 Citrix Gateway 上的配置文件 ns.conf 中的条目必须匹配，但以下例外情况除外：
  - 主 Citrix Gateway 设备和辅助设备必须使用各自的唯一系统 IP 地址进行配置。使用安装向导配置或修改 Citrix Gateway 上的系统 IP 地址。
  - 在高可用性对中，Citrix Gateway ID 和关联的 IP 地址必须指向另一个 Citrix Gateway。
    例如，如果您有两台设备（名为 AG1 和 AG2），则必须使用唯一的 Citrix Gateway ID 和 AG2 的 IP 地址配置 AG1。必须使用唯一的 Citrix Gateway ID 和 AG1 的 IP 地址配置 AG2。
    注意：每个 Citrix Gateway 设备始终标识为节点 0。使用唯一的节点 ID 配置每个设备。
- 高可用性对中的每个设备必须具有相同的许可证。有关许可的更多信息，请参阅Licensing。
- 如果使用不直接通过配置实用程序或命令行界面的方法在任一节点上创建配置文件（例如，导入 SSL 证书或更改为启动脚本），则必须将配置文件复制到另一节点或创建相同的文件在该节点上。
- 配置高可用性对时，请确保主设备和辅助设备的映射 IP 地址和默认网关地址相同。如有必要，您可以随时通过运行安装向导更改映射的 IP 地址。

您可以使用安装前检查表查看高可用性部署中需要配置的特定设置列表。有关详细信息，请参阅安装前清单。

配置高可用性设置

April 6, 2020

要设置高可用性配置，需要创建两个节点，每个节点都将另一个 Citrix Gateway IP 地址定义为远程节点。您可以先登录要配置高可用性的两个 Citrix ADC 设备之一，然后添加节点。将其他设备的 Citrix Gateway IP 地址指定为新节点的地址。然后，登录到另一台设备，并添加一个节点，该节点具有第一台设备的 Citrix Gateway IP 地址。算法确定哪个节点变为主节点，哪个节点变为辅助节点。

在配置设备之前，请添加高可用性节点。此节点表示高可用性对中的第一个或第二个 Citrix Gateway。要配置高可用性，首先创建节点，然后配置高可用性设置。

添加高可用性节点

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中的节点选项卡上，单击添加。
3. 在“高可用性设置”对话框的“HA 设置”对话框的“远程节点 IP 地址”文本框中，键入要添加为远程节点的 Citrix ADC 的 NSIP 地址。如果 Citrix Gateway IP 地址是 IPv6 地址，请在输入地址之前选中 IPv6 复选框。
4. 如果要将本地节点自动添加到远程节点，请选择“配置远程系统以参与高可用性设置”。如果未选择此选项，则必须登录到由远程节点表示的设备并添加当前正在配置的节点。
5. 单击以启用关闭接口/通道上的 HA 监视器。
6. 如果远程设备具有不同的用户名和密码，请在“远程系统登录凭据”中单击“远程系统登录凭据”与“自我节点”不同。
7. 在“用户名”中，键入远程设备的用户名。
8. 在“密码”中，键入远程设备的密码。
9. 单击确定。

启用或禁用辅助节点

您只能禁用或启用辅助节点。禁用辅助节点时，它会停止向主节点发送检测信号消息，因此主节点无法再检查辅助节点的状态。启用节点时，节点将参与高可用性配置。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中的“节点”选项卡上，选择本地节点，然后单击“打开”。
3. 在“HA 配置节点”对话框中的“高可用性状态”中，选择“已启用”（不参与 HA）。
4. 单击确定。状态栏中将显示一条消息，指出节点已成功配置。

配置高可用性设置

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中的“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在“HA 配置节点”对话框的“ID”中，键入节点标识符的编号。ID 指定其他设备的唯一节点编号。
4. 在“IP 地址”中，键入系统 IP 地址，然后单击“确定”。IP 地址指定其他设备的 IP 地址。

注意：高可用性对中节点的最大 ID 为 64。

更改 **RPC** 节点密码

April 6, 2020

要与其他 Citrix Gateway 设备通信，每个设备都需要了解其他设备，包括如何在 Citrix Gateway 上进行身份验证。RPC 节点是内部系统实体，用于系统与系统之间的配置和会话信息通信。每个 Citrix Gateway 上都存在一个 RPC 节

点，用于存储信息，例如其他 Citrix Gateway 设备的 IP 地址和用于身份验证的密码。与其他 Citrix Gateway 进行联系的 Citrix Gateway 将检查 RPC 节点中的密码。

Citrix Gateway 要求在高可用性对中的两台设备上使用 RPC 节点密码。最初，每个 Citrix Gateway 都配置了相同的 RPC 节点密码。为了增强安全性，必须更改默认的 RPC 节点密码。您可以使用配置实用程序配置和更改 RPC 节点。

在添加节点或添加全局服务器负载平衡 (GSLB) 站点时隐式创建 RPC 节点。无法手动创建或删除 RPC 节点。

重要提示：您还必须保护设备之间的网络连接。在配置 RPC 节点密码时，可以通过选中“安全”复选框来配置 安全性。

更改 **RPC** 节点密码并启用安全连接

1. 导航到 系统 **>** 网络 **> RPC**。
2. 在详细信息窗格中，选择节点，然后单击 编辑。
3. 在“密码”和“确认密码”中，键入新密码。
4. 在 源 **IP** 地址中，键入其他 Citrix Gateway 设备的系统 IP 地址。
5. 单击 安全，然后单击 确定。

> 注意：启用“安全”选项后，设备会加密从节点发送到其他 RPC 节点的所有通信，从而保护 RPC 通信。

使用 **CLI** 更改 **RPC** 节点密码

在命令提示窗口中，键入：

```
set ns rpcNode <IPAddress> {
 -password }
  [-secure ( YES | NO )]

show ns rpcNode
<!--NeedCopy-->
```

示例：

```
> set ns rpcNode 192.0.2.4 -password mypassword -secure YES
 Done
> show rpcNode
.
.
.
 IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
     SrcIP:  *           Secure:  ON
Done
>
<!--NeedCopy-->
```


配置主设备和辅助设备以实现高可用性

April 6, 2020

更改 RPC 节点密码并启用安全通信后，请使用配置实用程序配置主要和辅助 Citrix Gateway 高可用性节点。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中的“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在“高可用性状态”下，单击“已启用（积极参与 HA）”，然后单击“确定”。

配置通信间隔

April 6, 2020

将 Citrix Gateway 配置为高可用性对时，可以将辅助 Citrix Gateway 配置为以特定间隔（以毫秒为单位）进行侦听。这些间隔称为 Hello 间隔和死区间隔。

hello 间隔是将检测信号消息发送到对等节点的间隔。死区间是一个时间间隔，如果没有收到检测信号数据包，则对等节点标记为“向下”的时间间隔。检测信号消息是发送到高可用性对中其他节点的端口 3003 的 UDP 数据包。

配置您好间隔时，您可以使用值 200 到 1000。默认值为 200。死区间值为 3 到 60。默认值为 3。

> 注意
>
> 死区间必须设置为 hello 间隔的倍数。

配置辅助 **Citrix Gateway** 的通信间隔

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中的“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在“间隔”下，执行以下一项或两项操作：
   - 在 Hello 间隔 (msec) 中，键入值，然后单击确定。默认值为 200 毫秒。
   - 在死间隔 (秒) 中，键入值，然后单击确定。默认设置为三秒。

同步 **Citrix Gateway** 设备

April 6, 2020

默认情况下，处于启用高可用性对中的 Citrix Gateway 设备的自动同步状态。通过自动同步，您可以对一个设备进行更改，并启用更改自动传播到第二个设备。同步使用端口 3010。

发生以下情况时，同步开始：

- 辅助节点重新启动。
- 故障转移后，主节点变为辅助节点。

您可以禁用同步，这会阻止辅助 Citrix Gateway 在主设备上发生更改时将其配置与主 Citrix Gateway 同步。您也可以强制同步。

在对中的辅助节点上启用或禁用高可用性同步。

启用或禁用高可用性同步

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中的“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在“配置节点”对话框的“HA 同步”下，执行以下操作之一：
    - 要禁用同步，请清除“辅助节点将从主节点获取配置”复选框。
    - 要启用同步，请选中“辅助节点将从主节点获取配置”复选框。
4. 单击确定。状态栏中将显示一条消息，指出节点配置成功。

强制设备之间的同步

除了自动同步之外，Citrix Gateway 还支持高可用性对中的两个节点之间的强制同步。

您可以在主 Citrix Gateway 设备和辅助设备上强制同步。但是，如果同步已在进行中，则命令将失败，并且 Citrix Gateway 显示警告。在以下情况下，强制同步也会失败：

- 在独立系统上强制同步。
- 辅助节点处于禁用状态。
- 禁用辅助节点上的高可用性同步。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在节点选项卡上，单击强制同步。

在高可用性设置中同步配置文件

April 6, 2020

在高可用性设置中，您可以将主节点的各种配置文件同步到辅助节点。

用于在高可用性设置中同步文件的参数

- 模式

要执行的同步类型。以下描述在括号中包括指定选项的命令行参数。
- 除了许可证和 **rc.conf** （全部）以外的一切。同步与系统配置、Citrix Gateway 书签、SSL 证书、SSL CRL 列表、

HTML 注入脚本和应用程序防火墙 XML 对象相关的文件。
- 书签（书签）。同步所有 Citrix Gateway 书签。
- **SSL** 证书和密钥 (ssl)。同步 SSL 功能的所有证书、密钥和 CRL。
- 许可证和 **Rc.conf** （杂项）。同步所有许可证文件和 rc.conf 文件。
- 所有内容包括许可证和 **rc.conf** （all_plus_misc）。同步与系统配置、Citrix Gateway 书签、SSL 证书、SSL CRL 列表、HTML 注入脚本、应用程序防火墙 XML 对象、许可证和 rc.conf 文件相关的文件。

注意：如果在设备上安装 Citrix ADC 许可证，则有更多可用选项。

使用配置实用程序同步高可用性设置中的文件

1. 在导航窗格中，展开系统，然后单击诊断。
2. 在详细信息窗格的“实用工具”下，单击“启动 HA 文件同步”。
3. 在“开始文件同步”对话框的“模式”下拉列表中，选择适当的同步类型（例如，除许可证和 rc.conf 之外的所有内容），然后单击“确定”。

配置命令传播

April 6, 2020

在高可用性设置中，在主节点上发出的任何命令都会自动传播到辅助节点上并在辅助节点上运行，然后再在该节点上运行该命令。如果命令传播失败，或者如果辅助节点上的命令执行失败，则主节点将执行命令并记录错误。命令传播使用端口 3011。

在高可用性对配置中，默认情况下，在主节点和辅助节点上启用命令传播。您可以在高可用性对中的任一节点上启用或禁用命令传播。如果禁用主节点上的命令传播，则命令不会传播到辅助节点。如果禁用辅助节点上的命令传播，则不会在辅助节点上执行从主节点传播的命令。

注意：重新启用传播后，请记住强制同步。

注意：如果在禁用传播时发生同步，则在禁用传播生效之前所做的任何与配置相关的更改都将与辅助节点同步。同步过程中禁用传播的情况也是如此。

启用或禁用主节点上的传播

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中的“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在 HA 传播下，执行以下操作之一：
    - 要禁用高可用性传播，请清除“主节点将配置传播到辅助”复选框。
    - 要启用高可用性传播，请选中“主节点将配置传播到辅助”复选框。
4. 单击确定。

命令传播故障排除

April 6, 2020

下面的列表描述了命令传播可能失败的原因，以及恢复设置的解决方案：

- 网络连接不处于活动状态。如果命令传播失败，请检查主 Citrix Gateway 设备和辅助设备之间的网络连接。
- 辅助 Citrix Gateway 上缺少资源。如果命令在主 Citrix Gateway 上成功执行，但无法传播到辅助 Citrix Gateway，请直接在辅助 Citrix Gateway 上运行命令以查看错误消息。发生此错误可能是因为命令所需的资源存在于主 Citrix Gateway 上，而辅助 Citrix Gateway 上不可用。此外，请确认每个设备上的许可证文件是否匹配。

  例如，验证每个 Citrix Gateway 上都存在所有安全套接字层 (SSL) 证书。验证这两个 Citrix Gateway 设备上是否存在任何初始化脚本自定义。
- 身份验证失败。如果收到身份验证失败错误消息，请验证每台设备上的 RPC 节点设置。

配置故障安全模式

April 6, 2020

在高可用性配置中，故障安全模式可确保当两个节点均未通过运行状况检查时，一个节点始终处于主节点。故障安全模式可确保当节点仅部分可用时，备份方法可以激活并处理流量。

您可以在每个节点上独立配置高可用性故障安全模式。

下表显示了一些故障安全案例。NOT_UP 状态表示节点未通过运行状况检查，但节点部分可用。UP 状态表示节点通过了运行状况检查。

表 1. 故障安全模式案例

节点 A（主）运行状况	节点 B（辅助）运行状况	默认高可用性行为	启用故障安全的高可用性行为	说明
未向上（最后一次失败）	NOT_UP（首先失败）	A（辅助）、B（辅助）	A（主）、B（辅助）	如果两个节点都发生故障，则作为最后一个主节点的节点仍然是主节点。
NOT_UP（首先失败）	未向上（最后一次失败）	A（辅助）、B（辅助）	A (中学), B (小学)	如果两个节点都发生故障，则作为最后一个主节点的节点仍然是主节点。

节点 A（主）运行状况	节点 B（辅助）运行状况	默认高可用性行为	启用故障安全的高可用性行为	说明
UP	UP	A（主）、B（辅助）	A（主）、B（辅助）	如果两个节点都通过运行状况检查，则在启用故障安全的情况下不会改变行为。
UP	NOT_UP	A (小学), B (中学)	A（主）、B（辅助）	如果只有辅助节点出现故障，则启用故障安全的行为不会更改。
NOT_UP	UP	A (中学), B (小学)	A (中学), B (小学)	如果只有主服务器失败，则启用了故障保护功能的行为不会更改。
NOT_UP	UP (STAYSEC-ONDARY)	A（辅助）、B（辅助）	A（主）、B（辅助）	如果辅助设备配置为 STAYSUBIT，则主设备即使失败，也会保持主设备。

配置故障安全模式

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中的“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在“配置节点”对话框的“故障安全模式”下，选择“即使两个节点运行状况不佳的情况下仍然保持一个主节点”，然后单击“确定”。

配置虚拟 **MAC** 地址

April 6, 2020

虚拟 MAC 地址由主要和辅助 Citrix Gateway 设备在高可用性设置中共享。

在高可用性设置中，主 Citrix Gateway 拥有所有浮动 IP 地址，例如映射的 IP 地址或虚拟 IP 地址。它使用自己的 MAC 地址响应这些 IP 地址的地址解析协议 (ARP) 请求。因此，将使用浮动 IP 地址和 Citrix Gateway MAC 地址更新外部设备（如路由器）的 ARP 表。发生故障转移时，辅助 Citrix Gateway 将接管为新的主 Citrix Gateway。然后，它使用无偿地址解析协议 (GARP) 公布从主设备获取的浮动 IP 地址。新主设备公布的 MAC 地址是其自身界面的地址。

某些设备不接受 Citrix Gateway 生成的 GARP 消息。因此，一些外部设备保留旧主 Citrix Gateway 公布的旧 IP 到 Mac 映射。这种情况可能会导致网站变得不可用。要解决此问题，请在高可用性对的两个 Citrix Gateway 设备上配置虚拟 MAC 地址。此配置意味着两个 Citrix Gateway 设备具有相同的 MAC 地址。因此，发生故障转移时，辅助 Citrix Gateway 的 MAC 地址保持不变，并且无需更新外部设备上的 ARP 表。

要创建虚拟 MAC 地址，请创建虚拟路由器标识符 (ID) 并将其绑定到接口。在高可用性设置中，用户需要将 ID 绑定到两个设备上的接口。

当虚拟路由器 ID 绑定到接口时，系统会生成一个虚拟 MAC 地址，其中虚拟路由器 ID 为最后八位字节。通用虚拟 MAC 地址的一个示例是 00:00:5e:00:01:<VRID>。例如，如果您创建了值 60 的虚拟路由器 ID 并将其绑定到接口，则生成的虚拟 MAC 地址为 00:00:5e:00:01:3c，其中 3c 是虚拟路由器 ID 的十六进制表示形式。您可以创建 255 个虚拟路由器 ID，范围从 1 到 254。

您可以为 IPv4 和 IPv6 配置虚拟 MAC 地址。

配置 **IPv4** 虚拟 **MAC** 地址

April 6, 2020

创建 IPv4 虚拟 MAC 地址并将其绑定到接口时，从接口发送的任何 IPv4 数据包都使用绑定到接口的虚拟 MAC 地址。如果没有绑定到接口的 IPv4 虚拟 MAC 地址，则使用接口的物理 MAC 地址。

通用虚拟 MAC 地址的格式为 00:00:5e:00:01:<VRID>。例如，如果您创建值为 60 的 VRID 并将其绑定到接口，则生成的虚拟 MAC 地址为 00:00:5e:00:01:3c，其中 3c 是 VRID 的十六进制表示。您可以创建 255 个 VRID，其值介于 1 到 255 之间。

创建或修改 **IPv4** 虚拟 **MAC** 地址

April 6, 2020

您可以通过为 IPv4 虚拟 MAC 地址分配一个虚拟路由器 ID 来创建 IPv4 虚拟 MAC 地址。然后，您可以将虚拟 MAC 地址绑定到接口。不能将多个虚拟路由器 ID 绑定到同一个接口。要验证虚拟 MAC 地址配置，应显示并检查虚拟 MAC 地址以及绑定到虚拟 MAC 地址的接口。

配置虚拟 **MAC** 地址的参数

- VRID

识别虚拟 **MAC** 地址的虚拟路由器 **ID**。可能的值：**1** 至 **255**。


```
ifnum
```

要绑定到虚拟 MAC 地址的接口号（插槽/端口符号）。

配置虚拟 **MAC** 地址

1. 在配置实用程序中的 “配置” 选项卡上，展开 “系统”>“网络”，然后单击 “VMAC”。
2. 在详细信息窗格中的 VMAC 选项卡上，单击添加。
3. 在 “创建 VMAC” 对话框中的 “虚拟路由器 ID” 中，键入值。
4. 在 “关联接口” 下，在 “可用接口” 中，选择一个网络接口，单击 “添加”，单击 “创建”，然后单击 “关闭”。

创建虚拟 MAC 地址后，该地址将显示在配置实用程序中。如果选择了网络接口，则虚拟路由器 ID 绑定到该接口。

删除虚拟 **MAC** 地址

要删除虚拟 MAC 地址，您需要删除相应的虚拟路由器 ID。

1. 在配置实用程序中的 “配置” 选项卡上，展开 “系统”>“网络”，然后单击 “VMAC”。
2. 在详细信息窗格中，选择一个项目，然后单击删除。

绑定和取消绑定虚拟 **MAC** 地址

创建虚拟路由器 ID 时，您在 Citrix Gateway 上选择了一个网络接口，然后将虚拟路由器 ID 绑定到网络接口。您也可以从网络接口取消绑定虚拟 MAC 地址，但保留在 Citrix Gateway 上配置的 MAC 地址。

1. 在配置实用程序中的 “配置” 选项卡上，展开 “系统”>“网络”，然后单击 “VMAC”。
2. 在详细信息窗格中，选择一个项目，然后单击打开。
3. 在 “已配置接口” 下，选择一个网络接口，单击 “删除”，单击 “确定”，然后单击 “关闭”。

配置 **IPv6** 虚拟 **MAC** 地址

April 6, 2020

Citrix Gateway 支持 IPv6 数据包的虚拟 MAC 地址。您可以将任何接口绑定到 IPv6 的虚拟 MAC 地址，即使 IPv4 虚拟 MAC 地址已绑定到该接口。从接口发送的任何 IPv6 数据包都使用绑定到该接口的虚拟 MAC 地址。如果没有绑定到接口的虚拟 MAC 地址，IPv6 数据包将使用物理 MAC。

创建或修改 **IPv6** 的虚拟 **MAC** 地址

April 6, 2020

您可以通过为其分配 IPv6 虚拟路由器 ID 来创建 IPv6 虚拟 MAC 地址。然后，您可以将虚拟 MAC 地址绑定到接口。您不能将多个 IPv6 虚拟路由器 ID 绑定到接口。要验证虚拟 MAC 地址配置，应显示并检查虚拟 MAC 地址以及绑定到虚拟 MAC 地址的接口。

配置 **IPv6** 虚拟 **MAC** 地址的参数

- 虚拟路由器 ID

识别虚拟 **MAC** 地址的虚拟路由器 **ID**。可能的值：**1** 至 **255**。

```
1 ifnum
```

要绑定到虚拟 MAC 地址的接口号（插槽/端口符号）。

为 **IPv6** 配置虚拟 **MAC** 地址

1. 在配置实用程序中的 “配置” 选项卡上，展开 “系统”>“网络”，然后单击 “VMAC”。
2. 在详细信息窗格中的 VMAC6 选项卡上，执行以下操作之一：
   - 要创建新的虚拟 MAC 地址，请单击 “添加”。
   - 要修改现有虚拟 MAC 地址，请单击 “打开”。
3. 在 “创建 VMAC6” 或 “配置 VMAC6” 对话框中的 “虚拟路由器 ID” 中，输入值，如 vrID6。
4. 在关联界面中，单击添加，单击创建，然后单击关闭。状态栏中将显示一条消息，指出虚拟 MAC 地址已配置。

删除 **IPv6** 的虚拟 **MAC** 地址

1. 在配置实用程序中的 “配置” 选项卡上，展开 “系统”>“网络”，然后单击 “VMAC”。
2. 在详细信息窗格中的 VMAC6 选项卡上，选择要删除的虚拟路由器 ID，然后单击删除。状态栏中将显示一条消息，指出虚拟 MAC 地址已删除。

在不同的子网中配置高可用性对

April 6, 2020

典型的高可用性部署是当高可用性对中的两个设备驻留在同一子网上时。高可用性部署还可以由两个 Citrix Gateway 设备组成，其中每个设备位于不同的网络中。本主题介绍后一种配置，包括示例配置以及一个网络内和跨网络的高可用性配置之间的差异列表。

您还可以配置链路冗余和路由监视器。这些 Citrix Gateway 功能在跨网络高可用性配置中非常有用。这些功能还涵盖每个 Citrix Gateway 使用的运行状况检查过程，以确保合作伙伴设备处于活动状态。

独立网络配置的工作原理

Citrix Gateway 设备连接到两个不同网络上的不同路由器（称为 R3 和 R4）。设备通过这些路由器交换检测信号数据包。检测信号包是一种定期发生的信号，以确保连接仍处于活动状态。您可以扩展此配置以适应涉及任意数量的接口的部署。

注意：如果您在网络上使用静态路由，则必须在所有系统之间添加静态路由，以确保成功发送和接收检测信号数据包。（如果您在系统上使用动态路由，则不需要静态路由。）

当高可用性对中的设备驻留在两个不同的网络上时，辅助 Citrix Gateway 必须具有独立的网络配置。这意味着不同网络上的 Citrix Gateway 设备无法共享映射的 IP 地址、虚拟 LAN 或网络路由。这种类型的配置称为独立网络配置或对称网络配置，其中高可用性对中的 Citrix Gateway 设备具有不同的可配置参数。

下表汇总了独立网络配置的可配置参数，并显示必须如何在每个 Citrix Gateway 上设置这些参数：

可配置参数	行为
IP 地址	Citrix Gateway 特有。仅在该设备上处于活动状态。
虚拟 IP 地址	浮动。
虚拟局域网	Citrix Gateway 特有。仅在该设备上处于活动状态。
路由	Citrix Gateway 特有。仅在该设备上处于活动状态。链路负载平衡 (LLB) 路由处于浮动状态。
访问控制列表 (ACL)	浮动（常见）。在两台设备上均处于活动状态。
动态路由	Citrix Gateway 特有。仅在该设备上处于活动状态。辅助 Citrix Gateway 还应运行路由协议并与上游路由器对等。
L2 模式	浮动（常见）。在两台设备上均处于活动状态。
L3 模式	浮动（常见）。在两台设备上均处于活动状态。
反向网络地址转换 (NAT)	Citrix Gateway 特有。使用虚拟 IP 地址反向 NAT，因为 NAT IP 地址处于浮动状态。

添加远程节点

April 6, 2020

当高可用性对的两个节点驻留在不同的子网上时，每个节点必须具有不同的网络配置。因此，要将两个独立的系统配置为作为高可用性对运行，必须在配置过程中指定独立的网络计算模式。

添加高可用性节点时，必须为未连接或未用于流量的每个接口禁用高可用性监视器。

为独立网络计算模式添加远程节点

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中，单击节点选项卡，然后单击添加。
3. 在“高可用性设置”对话框的“远程节点 IP 地址”文本框中，键入作为远程节点的设备的 Citrix Gateway IP 地址。

   要使用 IPv6 地址，请在输入 IP 地址之前单击 IPv6 复选框。
4. 如果要将本地节点自动添加到远程节点，请选择“配置远程系统以参与高可用性设置”。如果未选择此选项，则需要登录到由远程节点表示的设备并添加当前正在配置的节点。
5. 单击以启用关闭接口/通道上的 HA 监视器。
6. 单击以启用在自模式上打开 INC（独立网络配置）模式。
7. 单击确定。节点页面显示高可用性配置中的本地节点和远程节点。

删除远程节点

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中，单击节点选项卡。
3. 选择要删除的节点，单击删除，然后单击是。

配置路由监视器

April 6, 2020

无论表是否包含任何动态学习路由还是静态路由，都可以使用路由监视器使高可用性状态依赖于内部路由表。在高可用性配置中，每个节点上的路由监视器检查内部路由表，以确保始终存在用于到达特定网络的路由条目。如果路径条目不存在，则路径监视器的状态将更改为“向下”。

如果 Citrix Gateway 设备只具有用于访问网络的静态路由，并且您想要为网络创建路由监视器，则必须为静态路由启用受监视的静态路由。受监视的静态路由从内部路由表中删除无法访问的静态路由。如果在静态路由上禁用受监视的静态路由，则无法访问的静态路由可能会保留在内部路由表中，从而无法实现路由监视器的目的。

启用或禁用的“独立网络配置”设置支持路由监视器。下表显示了在高可用性设置中的路由监视器以及启用或禁用了独立网络配置的情况。

在禁用的独立网络配置模式下的高可用性路由监视器	在启用的独立网络配置模式下的高可用性路由监视器
路由监视器由节点传播并在同步过程中交换。	路由监视器既不会由节点传播，也不会在同步过程中交换。
路由监视器仅在当前主节点中处于活动状态。	路由监视器在主节点和辅助节点上都处于活动状态。
Citrix Gateway 设备始终将路由监视器的状态显示为 UP，无论路由条目是否存在于内部路由表中。	如果内部路由表中不存在相应的路由条目，Citrix Gateway 设备将路由监视器的状态显示为“向下”。
路由监视器在以下情况下开始监视其路由，以便 Citrix Gateway 能够了解动态路由（可能需要 180 秒）：重新启动、故障转移、为 v6 路由设置 route6 命令、为 v4 路由设置 route msr enable/disable 命令、添加新的路由监视器	不适用。

如果禁用独立网络配置模式，并且希望主节点中的网关无法访问，则路由监视器非常有用。

例如，在双臂拓扑中使用路由器 R1 和交换机 SW1、SW2 和 SW3 在同一子网中具有 Citrix Gateway 设备 NS1 和 NS2 的双臂拓扑中禁用独立网络配置，如下图所示。由于 R1 是此设置中的唯一路由器，因此您希望无法从当前主节点访问 R1 时，高可用性设置进行故障转移。您可以在每个节点上配置路由监视器（例如 RM1 和 RM2），以监视 R1 从该节点的可达性。

将 NS1 作为当前主节点，网络流如下所示：

1. NS1 上的路由监视器 RM1 监视 NS1 的内部路由表是否存在路由器 R1 的路由条目。NS1 和 NS2 定期通过交换机 SW1 或 SW3 交换检测信号消息。
2. 如果交换机 SW1 失败，NS1 上的路由协议会检测到 R1 无法访问，因此从内部路由表中删除 R1 的路由条目。NS1 和 NS2 定期通过交换机 SW3 交换检测信号消息。
3. 检测 R1 的路由条目不存在于内部路由表中，RM1 将启动故障转移。如果从 NS1 和 NS2 中断到 R1 的路由，则每 180 秒进行一次故障转移，直到其中一台设备能够达到 R1 并恢复连接。

添加或移除路由监视器

April 6, 2020

当高可用性对的设备驻留在不同的网络上时，Citrix Gateway 的高可用性状态取决于是否可以访问设备。在跨网络高可用性配置中，每个 Citrix Gateway 上的路由监视器都会扫描内部路由表，以确保始终存在其他 Citrix Gateway 的条目。

添加路径监视器

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在“绑定/取消绑定路由监视器”对话框中的“路由监视器”选项卡上，单击“操作”，然后单击“配置”。
3. 在“指定路由监视器”下，键入其他 Citrix Gateway 设备的网络 IP 地址。

   若要配置 IPv6 地址，请单击 IPv6，然后键入 IP 地址。
4. 在 Netmask 中，键入其他网络的子网掩码，单击添加，然后单击确定。

完成此过程后，路由监视器将绑定到 Citrix Gateway。

注意：如果路由监视器未绑定到 Citrix Gateway，则任一设备的高可用性状态由接口的状态决定。

移除路由监视器

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在路由监视器选项卡上，单击操作，然后单击配置。
3. 在“配置的路由监视器”下，选择监视器，单击“删除”，然后单击“确定”。

配置链路冗余

April 6, 2020

链接冗余将网络接口分组在一起，以防止因具有其他正常运行接口的 Citrix Gateway 的一个网络接口出现故障而导致故障转移。主 Citrix Gateway 上的第一个接口出现故障将触发故障转移，尽管第一个接口仍可以使用其第二个链接来提供用户请求。配置链路冗余时，您可以将这两个接口分组到故障转移接口集中，以防止单个链路故障导致故障转移到辅助 Citrix Gateway，除非主 Citrix Gateway 上的所有接口都不起作用。

故障转移接口集中的每个接口都维护独立的桥接条目。未绑定到故障接口集的 Citrix Gateway 上启用的监视器接口和高可用性称为关键接口，因为如果这些接口中的任何一个出现故障，则会触发故障转移。

配置链路冗余

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在“故障转移接口集”选项卡上，单击“添加”。
3. 在“名称”中，键入集的名称。

4. 在接口中，单击添加。
5. 在“可用接口”下，选择一个接口，然后单击箭头将接口移动到“已配置”。
6. 对第二个界面重复步骤 4 和 5，然后单击创建。

您可以根据需要在接口之间进行故障转移时添加任意数量的接口。

从故障转移接口集中删除接口

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在“故障转移接口集”选项卡上，选择一个集，然后单击“删除”。

删除故障转移接口集

如果您不再需要故障转移接口集，则可以将其从 Citrix Gateway 中移除。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在“故障转移接口集”选项卡上，选择一个集，然后单击“删除”。

了解故障转移的原因

April 6, 2020

以下事件可能会导致高可用性配置中的故障转移：

1. 如果辅助节点在一段时间内未从主节点接收检测信号数据包，超过在辅助节点上设置的死区间。有关设置死区间的更多信息，请参阅配置通信间隔。节点未从对等节点接收检测信号数据包的可能原因包括：
   - 网络配置问题阻止检测信号遍历高可用性节点之间的网络。
   - 对等节点遇到硬件或软件故障，导致其冻结（挂起）、重新启动或停止处理和转发检测信号数据包。
2. 主节点的 SSL 卡出现硬件故障。
3. 主节点在三秒钟内不会在其网络接口上接收任何检测信号数据包。
4. 在主节点上，不属于故障转移接口集 (FIS) 或链路聚合 (LA) 通道的一部分并且已启用高可用性监视器 (HAMON) 的网络接口将失败。接口已启用，但进入“关闭”状态。
5. 在主节点上，FIS 中的所有接口都失败。接口已启用，但进入“关闭”状态。
6. 在主节点上，启用了 HAMON 的 LA 通道将失败。接口已启用，但进入“关闭”状态。
7. 在主节点上，所有接口都会失败。在这种情况下，无论 HAMON 配置如何，都会发生故障转移。
8. 在主节点上，手动禁用所有接口。在这种情况下，无论 HAMON 配置如何，都会发生故障转移。
9. 通过在任一节点上发出强制故障转移命令，强制故障转移。
10. 绑定到主节点的路由监视器变为“关闭”。

从节点强制故障转移

September 26, 2019

例如，如果需要替换或升级主节点，则可能需要强制进行故障转移。您可以强制从主节点或辅助节点进行故障转移。强制故障转移不会传播或同步。要查看强制故障转移后的同步状态，可以查看节点的状态。

在以下任何情况下，强制故障转移将失败：

- 在独立系统上强制故障转移。
- 辅助节点处于禁用状态。
- 辅助节点配置为保持辅助节点。

如果在运行强制故障转移命令时检测到潜在问题，Citrix Gateway 设备会显示一条警告消息。该消息包含触发警告并请求在继续操作之前进行确认的信息。

在主节点或辅助节点上强制故障转移

April 6, 2020

如果在主节点上强制故障转移，主节点将成为辅助节点，辅助节点将成为主节点。只有当主节点可以确定辅助节点为 UP 时，才可能强制故障转移。

如果辅助节点为 DRON，强制故障转移命令返回以下错误消息：”操作不可能由于无效的对等状态。纠正并重试。“

如果辅助系统处于声明状态或非活动状态，则该命令返回以下错误消息：“现在不可能操作。请等待系统稳定后再重试。”

如果从辅助节点运行强制故障转移命令，则辅助节点变为主节点，主节点变为辅助节点。只有当辅助节点的运行状况良好且节点未配置为保持辅助节点时，才会发生强制故障转移。

如果辅助节点不能成为主节点，或者如果辅助节点被配置为保持辅助节点（使用 STAYSECONDARY 选项），则节点显示以下错误消息：”操作不可能，因为我的状态无效。查看节点了解更多信息。”

在主节点或辅助节点上强制故障转移

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中的“节点”选项卡上，选择主节点，然后在“操作”中，单击“强制故障转移”。
3. 在警告对话框中，单击是。

强制主节点保持主节点

April 6, 2020

在高可用性配置中，即使在设备故障转移后，您也可以强制主 Citrix Gateway 保持主网关保持主网关。您只能在独立的 Citrix Gateway 设备和作为高可用性对中主设备的 Citrix Gateway 上配置此设置。

强制主节点保持主节点

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中的“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在“高可用性状态”下，单击“保持主”，然后单击“确定”。

您只能使用以下命令清除此配置：

```
clear configuration full
```

以下命令不会更改 Citrix Gateway 高可用性配置：

```
clear configuration basic
```

```
clear configuration extended
```

强制辅助节点保持辅助节点

April 6, 2020

在高可用性设置中，您可以强制辅助 Citrix Gateway 保持辅助状态，与主 Citrix Gateway 的状态无关。将 Citrix Gateway 配置为保持辅助功能时，即使主 Citrix Gateway 发生故障，也会保持辅助功能。

例如，在现有的高可用性设置中，假设您需要升级主 Citrix Gateway，并且此过程需要指定的时间。在升级过程中，主 Citrix Gateway 可能变得不可用，但您不希望辅助 Citrix Gateway 接管。即使在主 Citrix Gateway 中检测到故障，您希望它仍然是辅助 Citrix Gateway。

如果高可用性对中 Citrix Gateway 的状态配置为保持辅助状态，则该状态不会参与高可用性状态计算机转换。您可以在“节点”选项卡上的配置实用程序中检查 Citrix Gateway 的状态。

此设置适用于独立和辅助 Citrix Gateway。

设置高可用性节点时，不会传播或同步该节点，只会影响配置此设置的 Citrix Gateway。

强制辅助节点保持辅助节点

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中的“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在“高可用性状态”下，单击“保持辅助”（保持监听模式），然后单击“确定”。

将 **Citrix Gateway** 作为活动的高可用性设备恢复服务

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中的“节点”选项卡上，选择要保留主节点的设备，然后单击“打开”。
3. 在“高可用性状态”下，单击“已启用（积极参与 HA）”，然后单击“确定”。

使用群集

April 6, 2020

Citrix Gateway 可以部署在群集配置中，以便为 VPN 客户端流量提供高完整性、高可用性和可扩展性。在群集中，一组 Citrix Gateway 设备或虚拟机作为单个系统映像运行，以协调用户会话并管理到网络资源的流量。Citrix Gateway 群集可以使用至少两个和最多 32 个 Citrix Gateway 设备或配置为群集节点的虚拟机构建

开始配置 Citrix Gateway 群集之前，应先阅读
Citrix ADC 群集文档。请特别注意该文档中的以下主题。

- 请参阅硬件和软件要求以验证您计划使用的系统是否满足要求。
- 有关聚类概念的说明，请集群的工作原理参阅。
- 请参设置节点间通信阅规划部署并确定可能与您的环境相关的任何警告。

Citrix Gateway 群集作为发现 VIP 配置类型 Citrix ADC 群集运行。

配置群集

April 6, 2020

设置 Citrix Gateway 群集的主要任务是：

1. 决定哪个 Citrix Gateway 设备或 VM 将作为配置协调器，并在该系统上创建群集实例（如果尚未存在群集实例）。
2. 将 Citrix Gateway 系统作为节点加入群集。
3. 在集群实例上创建一个节点组，并设置了“粘性”选项。
4. 将单个群集节点绑定到群集节点组。
5. 在配置协调器上配置 Citrix Gateway 虚拟服务器，并将其绑定到群集节点组。

有多种方法可用于配置 Citrix ADC 群集。以下一组任务使用配置实用程序中可用的最直接方法。

使用配置实用程序创建 **Citrix Gateway** 群集实例

按顺序排列了所有部署详细信息后，开始在将担任配置协调器的 Citrix Gateway 上进行配置。

警告：创建集群实例会清除配置。如果您需要保存现有系统配置以供参考，请在继续集群配置之前存档副本。在群集建立后，可以在配置协调器上重新应用要在群集中使用的任何现有设置。

1. 登录到 NSIP 地址的 Citrix ADC 配置实用程序。
2. 展开系统节点，然后展开群集子节点。
3. 在详细信息窗格中，单击管理群集。
4. 在“群集配置”对话框中，设置创建群集所需的参数。
    a) 输入集群实例 ID。这是集群实例的数字标识符。默认值为 1，但您可以将其设置为 1 到 16 之间的任意数字。
    b) 输入群集 IP 地址。这是群集的配置协调器 IP 地址，它是群集的管理 IP 地址。
    c) 选择首选背板界面。这是 Citrix Gateway 接口，用于在群集节点之间进行通信。
5. 单击创建。
6. 在提示确认系统重新启动时，单击是。
7. 节点启动并成功同步后，从群集 IP 地址更改节点和群集 IP 地址的 RPC 凭据。有关更改 RPC 节点密码的更多信息，请参阅更改 RPC 节点密码。
8. 等待系统重新启动。一旦可用，请登录到步骤 4 (2) 中配置的群集 IP 地址的配置实用程序。

注意：在系统信息详细信息窗格中，NSIP 地址的本地节点报告为配置协调器。这确认了基础集群实例现在正在运行。

配置协调器的本地节点将自动添加到群集中。可以在以下任务中添加更多节点。

向 **Citrix Gateway** 群集添加节点

集群实例建立后，您可以开始向集群添加其他 Citrix Gateway 节点。

要向群集添加更多 Citrix Gateway 系统，可以使用配置实用程序远程发出群集节点创建和加入群集设置。

注意：应在配置 Citrix Gateway 设置之前完成向群集添加节点。这样，如果群集配置出现问题，并且您想要删除群集并重新开始，则不必重复 Citrix Gateway 配置。

1. 登录到群集 IP 地址的 Citrix ADC 配置实用程序。
2. 展开系统节点，然后展开群集子节点。
3. 在详细信息窗格中，单击管理群集。
4. 在群集节点详细信息窗格中，单击添加。
5. 在“创建群集节点”窗格中，输入此节点的唯一节点 ID。
6. 输入要添加为群集节点的系统的 Citrix ADC IP 地址。
7. 在群集节点凭据窗格中，输入远程 Citrix Gateway 系统的 Citrix Gateway 用户名和密码。
8. 在配置协调器凭据窗格中，输入本地授权用户的密码。
9. 单击创建。
10. 出现提示时，单击 YES 以允许保存系统配置并对远程 Citrix Gateway 执行热重启。
11. 节点启动并成功同步后，从群集 IP 地址更改节点和群集 IP 地址的 RPC 凭据。有关更改 RPC 节点密码的更多信息，请参阅更改 RPC 节点密码。

对要配置为群集节点的每个其他远程 Citrix Gateway 系统重复步骤 4 到 11。

验证群集节点是否包含在群集节点详细信息窗格中的活动节点列表中。如果缺少任何节点，请重复步骤 4 到 10，直到列出所有必要的节点。

创建群集节点组

添加群集节点后，可以创建群集节点组。

1. 登录到群集 IP 地址的 Citrix ADC 配置实用程序。
2. 展开系统节点，然后展开群集子节点。
3. 单击节点组。
4. 在详细信息窗格中，单击 Add（添加）。
5. 输入群集节点组的名称。
6. 选择粘性选项。这是支持 Citrix Gateway 虚拟服务器类型所必需的。
7. 单击继续。

现在已建立群集节点组。在离开配置实用程序的此区域之前，您可以将本地 Citrix Gateway 节点绑定到新的群集节点组。这是绑定到群集组的唯一节点。

将本地群集节点绑定到群集节点组

由于 Citrix Gateway 群集配置是斑点类型，因此只能将一个节点绑定到该节点组。以下过程将配置协调器上的本地节点绑定到节点组，但群集中的任何节点都可用于此绑定。

1. 在高级窗格中，展开群集节点。
2. 在中间的群集节点窗格中，选择 “无群集节点”。
3. 在群集节点配置屏幕上，单击绑定。
4. 为此 Citrix Gateway 系统选择由 NSIP 地址表示的本地节点。
5. 点击插入。
6. 单击确定。
7. 单击完成。

现在已填充群集并准备共享由以下任务配置的 Citrix Gateway 虚拟服务器。

将 **Citrix Gateway** 虚拟服务器绑定到群集节点组

建立群集后，您可以继续构建群集部署要提供的 Citrix Gateway 配置。要将配置与群集绑定，您需要创建 Citrix Gateway 虚拟服务器并将其绑定到设置为键入 Sticky 的群集节点组。将虚拟服务器绑定到群集节点组后，您可以继续配置 Citrix Gateway。

如果配置了多个 Citrix Gateway 虚拟服务器，则这些服务器也必须绑定到群集节点组。

注意：如果尚未配置 Citrix Gateway 虚拟服务器，则可能必须首先在 “
系统”>“设置”>“配置基本功能” 下启用 Citrix Gateway 和身份验证、授权和审核功能。

1. 登录到群集 IP 地址的 Citrix ADC 配置实用程序。
2. 展开系统节点，然后展开群集子节点。
3. 单击节点组。
4. 在“节点组”窗格中，选择所需的节点组名称，然后单击“编辑”。
5. 在右侧的“高级”窗格中，展开“虚拟服务器”选项，然后单击“+”图标以添加虚拟服务器。
6. 选择 VPN 虚拟服务器类型，然后单击继续。
7. 单击 Bind（绑定）。
8. 如果列出了所需的虚拟服务器，请选择它，然后单击“插入”，然后单击“确定”。
9. 如果您必须创建新的虚拟服务器，请单击“添加”。继续完成 Citrix ADC 虚拟服务器配置。最低限度地说，所需要的只是创建虚拟服务器，以便它可以绑定到群集节点组。
10. 虚拟服务器在 Citrix Gateway 虚拟服务器列表中可用后，将其选中，然后单击“插入”。
11. 单击确定。
12. 单击完成。

注意：如果配置了多个 Citrix Gateway 虚拟服务器，则必须使用相同的方法将这些服务器绑定到群集节点组。

维护和监控系统

April 6, 2020

完成 Citrix Gateway 的配置后，您需要维护和监控设备。您可以通过以下方式执行此操作：

- 您可以将 Citrix Gateway 升级到最新版本的软件。登录到 Citrix 网站时，可以导航到 Citrix Gateway 下载站点和下载软件。您可以在 Citrix 知识中心中找到维护版本的自述文件。
- 您可以将 Citrix Gateway 配置和管理任务分配给组中的不同成员。通过委派管理，您可以将访问级别分配给个人，从而限制他们在 Citrix Gateway 上执行特定任务。
- 您可以将 Citrix Gateway 配置保存到设备或计算机上的文件中。您可以比较当前正在运行的配置和保存的配置。您还可以从 Citrix Gateway 清除配置。
- 您可以在 Citrix Gateway 配置实用程序中查看、刷新和最终用户会话。
- 您可以在 Citrix Gateway 上配置日志记录。日志提供了有关设备的重要信息，并且在遇到问题时非常有用。

配置委派管理员

April 6, 2020

Citrix Gateway 具有默认的管理员用户名和密码。默认用户名和密码是 nsroot。首次运行安装向导时，您可以更改管理员密码。

您可以创建其他管理员帐户，并为每个帐户分配具有不同级别的 Citrix Gateway 访问权限。这些附加帐户称为委派管理员。例如，您有一个人被分配监控 Citrix Gateway 连接和日志，另一个人负责在 Citrix Gateway 上配置特定设置。

第一个管理员具有只读访问权限，第二个管理员对设备的访问权限有限。

要配置委派管理员，请使用命令策略和系统用户和组。

配置委派管理员时，配置过程为：

- 添加系统用户。系统用户是具有指定权限的管理员。所有管理员都会继承其所属组的策略。
- 添加系统组。系统组包含具有特定权限的系统用户。系统组的成员继承他们所属的一个或多个组的策略。
- 创建命令策略。命令策略允许您定义允许用户或组访问和修改 Citrix Gateway 配置的哪些部分。您还可以调节允许管理员和组配置哪些命令（例如命令组、虚拟服务器以及其他元素）。
- 通过设置优先级将命令策略绑定到用户或组。配置委派管理时，请将优先级分配给管理员或组，以便 Citrix Gateway 确定优先级的策略。

Citrix Gateway 具有默认拒绝系统命令策略。命令策略不能全局绑定。必须将策略直接绑定到系统管理员（用户）或组。如果用户和组没有关联的命令策略，则会应用默认拒绝策略，用户无法执行任何命令或配置 Citrix Gateway。

您可以配置自定义命令策略，以便为用户权限分配定义更高级别的详细信息。例如，您可以授予一个人向 Citrix Gateway 添加会话策略的能力，但不允许用户执行任何其他配置。

为委派管理员配置命令策略

April 6, 2020

Citrix Gateway 具有四个内置命令策略，可用于委派管理：

- 只读。允许只读访问以显示除系统命令组和 ns.conf show 命令之外的所有命令。
- 运算符。允许只读访问，并允许访问以启用和禁用服务上的命令。此策略还允许将服务和服务器设置为“关闭访问”。
- 网络。允许几乎完全的系统访问，不包括系统命令和 shell 命令。
- 超级用户。授予完全系统权限，例如授予默认管理员 nsroot 的权限。

命令策略包含内置表达式。您可以使用配置实用程序创建系统用户、系统组、命令策略，并定义权限。

在 **Citrix Gateway** 上创建管理用户

1. 在配置实用程序的导航窗格中的 配置选项卡上，展开“系统”>“用户管理”，然后单击“系统用户”。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在“用户名**”** 中，键入用户名。
4. 在“密码”和“确认密码”字段中，键入密码。
5. 要将用户添加到组，请在“的成员”中，单击“添加”。
6. 在“可用”中，选择一个组，然后单击向右箭头。
7. 在命令策略的操作中，单击插入。
8. 在“插入命令策略”对话框中，选择命令，单击“确定”，单击“创建”，然后单击“关闭”。

创建管理组

管理组包含在 Citrix Gateway 上具有管理权限的用户。您可以在配置实用程序中创建管理组。

使用配置实用程序配置管理组

1. 在配置实用程序的导航窗格中的 配置选项卡上，展开 “系统”>“用户管理”，然后单击 “系统组”。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在 “组名称” 中，键入组的名称。
4. 要将现有用户添加到组，请在 “成员” 中单击 “添加”。
5. 在 “可用” 下，选择一个用户，然后单击向右箭头。
6. 在 “命令策略” 下的 “操作” 中，单击 “插入”，选择一个或多个策略，单击 “确定”，单击 “创建”，然后单击 “关闭”。

为委派管理员配置自定义命令策略

April 6, 2020

配置自定义命令策略时，请提供策略名称，然后配置策略组件以创建命令规范。使用命令规范，您可以限制允许管理员使用的命令。例如，您希望拒绝管理员使用 remove 命令的能力。配置策略时，请将操作设置为拒绝，然后配置参数。

您可以配置简单或高级命令策略。如果配置简单策略，则可以在设备上配置组件，例如 Citrix Gateway 和身份验证。如果配置高级策略，则选择称为实体组的组件，然后选择允许管理员在组中执行的命令。

创建简单的自定义命令策略

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “系统”>“用户管理”，然后单击 “命令策略**”**。
2. 在详细信息窗格中，单击 添加。
3. 在 策略名称中，键入策略的名称。
4. 在 “操作” 中，选择 “允许” 或 “拒绝”。
5. 在 命令规范下，单击 添加。
6. 在 “添加命令” 对话框的 “简单” 选项卡的 “操作” 中，选择委派管理员可以执行的操作。
7. 在 “实体组” 下，选择一个或多个组。

   您可以按 CTRL 键选择多个组。
8. 单击 **Create**（创建），然后单击 **Close**（关闭）。

创建高级自定义命令策略

1. 在配置实用程序的导航窗格中的 配置选项卡上，展开 “系统”>“用户管理”，然后单击 “命令策略”。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在 策略名称中，键入策略的名称。
4. 在 “操作” 中，选择 “允许” 或 “拒绝”。
5. 在 命令规范下，单击 添加。
6. 在 “添加命令” 对话框中，单击 “高级” 选项卡。
7. 在 实体组中，选择命令所属的组，例如身份验证或高可用性。
8. 在 “实体” 下，选择策略。

   您可以按 CTRL 键在列表中选择多个项目。
9. 在 操作中，选择命令，单击 创建，然后单击 关闭。

   您可以按 CTRL 键在列表中选择多个项目。
10. 单击 **Create**（创建），然后单击 **Close**（关闭）。
11. 在 创建命令策略对话框中，单击 创建，然后单击 关闭。

单击 “创建” 时，表达式将显示在 “创建命令策略” 对话框中的 “命令规范” 下。

创建自定义命令策略后，您可以将其绑定到用户或组。

> 注意：您只能将自定义命令策略绑定到您创建的用户或组。您不能将自定义命令策略绑定到用户 nsroot。

将自定义命令策略绑定到用户或组

1. 在配置实用程序中，在 “配置” 选项卡的导航窗格中，展开 “系统”>“用户管理”，然后单击 “系统用户” 或单击 “系统组”。
2. 在详细信息窗格中，从列表中选择一个用户或组，然后单击 “打开”。
3. 在 “命令策略” 下，选择策略，然后单击 “确定”。

在 **Citrix Gateway** 上配置审核

April 6, 2020

Citrix Gateway 允许您记录设备收集的状态和状态信息。您可以使用审核日志按时间顺序查看事件历史记录。日志中的消息包含有关生成消息的事件、时间戳、消息类型以及预定义的日志级别和消息信息的信息。您可以配置设置来确定记录的信息和存储消息的位置。

Citrix Gateway 目前支持两种日志格式：用于本地日志的专有日志格式和用于 syslog 服务器的系统日志格式。您可以配置审核日志以提供以下信息：

等级	说明
紧急情况	仅记录主要错误。日志中的条目表明 Citrix Gateway 遇到导致其无法使用的严重问题。
警报	记录可能导致 Citrix Gateway 无法正常运行但对其操作不至关重要的问题。应尽快采取纠正措施，以防止 Citrix Gateway 遇到严重问题。
严重	记录不限制 Citrix Gateway 操作但可能升级为更大问题的关键条件。
错误	记录 Citrix Gateway 上操作失败导致的条目。
警告	记录可能导致错误或严重错误的潜在问题。
通知	记录比信息级别日志更深入的问题，但用途与通知相同。
信息	记录 Citrix Gateway 执行的操作。此级别对于故障排除问题非常有用。

如果您配置 TCP 压缩，Citrix Gateway 审核日志还会存储 Citrix Gateway 的压缩统计信息。针对不同数据实现的压缩比存储在每个用户会话的日志文件中。

Citrix Gateway 使用日志签名会话 ID。这允许您跟踪每个会话而不是每个用户的日志。作为会话一部分生成的日志具有相同的会话 ID。如果用户从具有相同 IP 地址的同一用户设备建立两个会话，则每个会话都具有唯一的 Sesession ID。

> 重要提示：如果您编写了自定义日志解析脚本，则需要在自定义解析脚本中进行此签名更改。

在 **Citrix Gateway** 上配置日志

April 6, 2020

在 Citrix Gateway 上配置日志记录时，可以选择将审核日志存储在 Citrix Gateway 上或将其发送到系统日志服务器。您可以使用配置实用程序创建审核策略并配置设置以存储审核日志。

创建审核策略

1. 在配置实用程序中的“配置”选项卡上，展开 **Citrix Gateway** > 策略 > 审核。
2. 在“名称”中，键入策略的名称。

3. 选择以下选项之一：
   - 系统日志（如果要将日志发送到 Syslog 服务器）。
   - Nslog 将日志存储在 Citrix Gateway 上。

     注意：如果选择此选项，日志将存储在设备上的 /var/log 文件夹中。
4. 在详细信息窗格中，单击 **Add**（添加）。
5. 为存储日志的服务器信息键入以下信息：
   - 在“名称”中，键入服务器的名称。
   - 在“服务器”下，键入日志服务器的名称或 IP 地址。
6. 单击 Create（创建），然后单击 Close（关闭）。

创建审核策略后，您可以将策略绑定到以下任意组合：

- 全球范围
- 虚拟服务器
- 组
- 用户

全局绑定审核策略

1. 在配置实用程序中的“配置”选项卡上，展开 **Citrix Gateway** > 策略 > 审核。
2. 选择 系统日志或 **Nslog** 。
3. 在详细信息窗格中，单击 操作，然后单击 全局绑定。
4. 在“绑定 **/**取消绑定审核策略到 全局”对话框中的“详细信息”下，单击“插入策略”。
5. 在“策略名称”下，选择一个策略，然后单击“确定”。

修改审核策略

您可以修改现有审核策略以更改日志发送到的服务器。

1. 在配置实用程序中的配置选项卡上，展开 **Citrix Gateway** > 策略 > 审核”
2. 选择 系统日志或 **Nslog** 。
3. 在详细信息窗格中，单击策略，然后单击 打开。
4. 在服务器中，选择新的服务器，然后单 击确定。

删除审核策略

您可以从 Citrix Gateway 中删除审核策略。删除审核策略时，该策略将自动取消绑定。

1. 在配置实用程序中的“配置”选项卡上，展开 **Citrix Gateway** > 策略 > 审核。
2. 选择 系统日志或 **Nslog** 。
3. 在详细信息窗格中，单击策略，然后单击 删除。

配置 **ACL** 日志记录

April 6, 2020

您可以将 Citrix Gateway 配置为记录与扩展访问控制列表 (ACL) 匹配的数据包的详细信息。除了 ACL 名称之外，记录的详细信息还包括特定于数据包的信息，例如源和目标 IP 地址。信息存储在 syslog 或 nslog 文件中，具体取决于您启用的日志记录类型（syslog 或 nslog）。

您可以在全局级别和 ACL 级别启用日志记录。但是，要在 ACL 级别启用日志记录，您还必须在全局级别启用它。全局设置优先。

为了优化日志记录，当来自同一个 ACL 的多个数据包匹配时，仅记录第一个数据包的详细信息。对于属于同一流的每个其他数据包，计数器都会递增。流定义为具有以下参数相同值的一组数据包：

- 源 IP
- 目标 IP
- 源端口
- 目的端口
- 协议 (TCP 或 UDP)

如果数据包不是来自同一流，或者如果时间持续时间超出了平均时间，则会创建一个新的流。平均时间是相同流的数据包不会生成额外消息的时间（尽管计数器递增）。

> 注意：在任何给定时间可以记录的不同流量的总数限制为 10,000。

下表描述了可以在规则级别为扩展 ACL 配置 ACL 日志记录的参数。

参数名称	说明
日志状态	ACL 的日志记录功能的状态。可能的值：已启用和已禁用。默认值：已禁用。
利率限制	特定 ACL 可以生成的日志消息数。默认值：100。

使用配置实用程序配置 **ACL** 日志记录

您可以为 ACL 配置日志记录并指定规则可生成的日志消息数。

1. 在配置实用程序的导航窗格中，展开 “系统”>“网络”，然后单击 ACL。
2. 在详细信息窗格中，单击 扩展 **ACL** 选项卡，然后单击添加。
3. 在 “创建扩展 **ACL**” 对话框的 “名称” 中，键入策略的名称。
4. 选中日 志状态复选框。
5. 在 “日 志速率限制” 文本框中，键入要为规则指定的速率限制，然后单击 “创建”。

配置 ACL 日志记录后，可以在 Citrix Gateway 上启用它。创建审核策略，然后将其绑定到用户、组、虚拟服务器或全

局。

在 **Citrix Gateway** 上启用 **ACL** 或 **TCP** 日志记录

1. 在配置实用程序的导航窗格中，展开 **Citrix Gateway** > 策略 > 审核。
2. 选择系统日志或 nslog。
3. 在“服务器”选项卡上，单击“添加”。
4. 在“创建审核服务器”对话框的“名称”中，键入服务器的名称，然后配置服务器设置。
5. 单击 **ACL** 日志记录或 **TCP** 日志记录，然后单击 创建。

启用 **Citrix Gateway** 插件日志记录

April 6, 2020

可以将 Citrix Gateway 插件配置为将所有错误记录到存储在用户设备上的文本文件中。用户可以配置 Citrix Gateway 插件以设置用户设备上的日志记录级别，以记录特定用户活动。用户配置日志记录时，插件会在用户设备上创建以下两个文件：

- 挂钩日志 <num> .txt，它记录 Citrix Gateway 插件生成的拦截消息。
- nssslvpn.txt，其中列出了插件的错误。

> 注意： Hooklog.txt 文件不会自动删除。Citrix 建议定期删除这些文件。

用户日志位于用户设备上的 Windows 中的以下目录中：

- Windows XP（所有用户）：%SystemDrive%:\Documents and Settings\All Users\Application Data\Citrix\AGEE
- Windows XP（特定于用户）：%SystemDrive%:\Documents and Settings\%username%\Local Settings\Application Data\Citrix\AGEE
- Windows Vista（所有用户）：%SystemDrive%:\ProgramData\Citrix\AGEE
- Windows Vista(特定于用户的):%SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 7（所有用户）：%SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 7（特定于用户）：%SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 8（所有用户）：%SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 8（特定于用户）：%SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE

您可以使用这些日志文件对 Citrix Gateway 插件进行故障排除。用户可以通过电子邮件将日志文件发送给技术支持。

在“配置”对话框中，用户可以设置 Citrix Gateway 插件的日志记录级别。日志记录级别为：

- 记录错误消息
- 记录事件消息
- 记录 Citrix Gateway 插件统计信息

- 记录所有错误、事件消息和统计信息

启用日志记录

1. 在用户设备上，右键单击通知区域中的 Citrix Gateway 图标，然后单击配置 Citrix Gateway。
2. 单击“跟踪”选项卡，选择日志级别，然后单击“确定”。

> 注意：用户必须使用 Citrix Gateway 插件登录才能打开“
> 配置”对话框。

监视 **ICA** 连接

April 6, 2020

可以使用“
ICA 连接”对话框监视服务器场上的活动用户会话。此对话框提供以下信息：

- 连接到服务器场的人员的用户名
- 服务器场的域名
- 用户设备的 IP 地址
- 用户设备的端口号
- 运行 Citrix Virtual Apps and Desktops 的服务器的 IP 地址
- 运行 Citrix Virtual Apps and Desktops 的服务器的端口号

1. 在配置实用程序的导航窗格中，单击 Citrix ADC 网关。
2. 在详细信息窗格的监视器连接下，单击 ICA 连接以查看监视对话框。

与 **Citrix** 产品集成

July 19, 2022

如果您是负责安装和配置 Citrix Gateway 的系统管理员，则可以将设备配置为使用 Citrix Endpoint Management、StoreFront 和 Web Interface。

用户可以从内部网络或远程位置直接连接到 Endpoint Management。用户连接后，他们可以访问他们的 Web、SaaS 和移动应用程序。他们还可以从任何设备处理位于 ShareFile 中的文档。

要允许用户通过 Citrix Gateway 连接到服务器场，请在 StoreFront 或 Web Interface 以及 Citrix Gateway 上配置设置。用户连接时，他们可以访问已发布的应用程序和虚拟桌面。

将 Citrix Gateway 与 Endpoint Management、StoreFront 和 Web Interface 集成的配置步骤假定如下：

- Citrix Gateway 位于 DMZ 中，并连接到现有网络。
- Citrix Gateway 作为独立设备进行部署，远程用户直接连接到 Citrix Gateway。
- StoreFront、Endpoint Management、Citrix Virtual Apps, Citrix Virtual Desktops, and the Web Interface 驻留在安全网络中。
- 在 Endpoint Management 中配置了 ShareFile。有关 ShareFile 的详细信息，请参阅ShareFile主题和为用户访问配置 ShareFile主题。

部署 StoreFront 和 Endpoint Management 的方式取决于您向移动设备提供的应用程序。如果用户有权访问使用 MDX Toolkit 包装的 MDX 应用程序，则 Endpoint Management 位于安全网络中 StoreFront 的前面。如果您不提供对 MDX 应用的访问权限，StoreFront 将位于安全网络中的 Endpoint Management 的前面。

用户如何连接到应用程序、桌面和 **ShareFile**

April 6, 2020

如果您的部署中有 Citrix Endpoint Management，则用户可以通过以下方式进行连接：

- Citrix Gateway 插件，用于为内部网络中的资源建立完整的 VPN 隧道。创建会话配置文件以选择适用于 Windows 的 Citrix Gateway 插件或适用于 Mac 的 Citrix Gateway 插件。当用户使用插件登录时，端点分析扫描可以在用户设备上运行。

> 注意：要允许在 Mac 计算机上运行端点分析扫描，必须安装 Citrix Gateway 10.1 Build 120.1316.e 或更新版本。

- Citrix Workspace 应用程序通过 Endpoint Management 连接到 ShareFile 中的 Web、SaaS 和企业应用程序、Web 链接和文档。当用户使用 Citrix Workspace 应用登录时，Citrix Gateway 将连接路由到 Endpoint Management。Citrix Workspace 应用程序建立连接时，用户的应用程序和文档将显示在 Citrix Workspace 应用程序中。如果用户使用 Citrix Workspace 应用登录并直接连接到 Endpoint Management，则必须在 Citrix Gateway 中启用无客户端访问。此部署不需要 StoreFront。
- Citrix Workspace 应用程序通过 StoreFront 或 Web Interface 连接到已发布的应用程序和虚拟桌面。当用户使用 Citrix Workspace 应用登录时，Citrix Gateway 会将连接路由到 StoreFront 或 Web Interface。Citrix Workspace 应用程序建立连接时，用户应用程序和桌面将显示在 Citrix Workspace 应用程序中。
- Secure Hub 可通过 Endpoint Management 从移动设备连接到 iOS 和 Android 应用程序，包括 WorxMail 和 WorxWeb。当用户登录到 Secure Hub 时，他们可以访问您在 Endpoint Management 中配置的移动应用程序，当 Citrix Gateway 建立微型 VPN 连接时，用户移动应用程序将显示在 Secure Hub 窗口中。用户可以从 Secure Hub 启动应用程序。某些应用程序要求用户在移动设备上下载并安装该应用程序。

在上述任何方案中，如果用户想要通过 Citrix Gateway 进行连接，则会执行以下操作：

- 用户通过使用 Citrix Gateway 插件或 Citrix Workspace 应用程序登录。要首次登录，用户可打开 Web 浏览器并键入 Citrix Gateway 或 Citrix Workspace 应用程序的完全限定域名 (FQDN)。使用移动设备的用户使用 Secure Hub 登录。
- 在登录页面上，用户输入其凭据并进行身份验证。

- 身份验证后，用户会话将重定向到 StoreFront 或 Endpoint Management，具体取决于您的部署。
- 如果同时部署 StoreFront 和 Endpoint Management，Citrix Gateway 将联系部署中的第一台服务器。例如，如果在 Endpoint Management 中配置 MDX 移动应用程序，则在 Endpoint Management 后面部署 StoreFront。如果您不提供对 MDX 移动应用的访问权限，则可以在 StoreFront 后面部署 Endpoint Management。
- 所有用户的桌面、文档以及基于 Web、SaaS 和 Windows 的应用程序都显示在 Citrix Workspace 应用程序或 Secure Hub 中。

如果用户需要访问内部网络中的其他资源（如 Exchange、文件共享或内部网站），他们也可以使用 Citrix Gateway 插件登录。例如，如果用户想要连接到网络中的 Microsoft Exchange Server，他们将在其计算机上启动 Microsoft Outlook。安全连接使用连接到 Citrix Gateway 的 Citrix Gateway 插件进行。SSL VPN 隧道创建到 Exchange Server，用户可以访问他们的电子邮件。

> 重要提示：Citrix 建议在 Citrix Gateway 虚拟服务器上配置身份验证。在 Citrix Gateway 中禁用身份验证时，未经身份验证的 HTTP 请求将直接发送到运行内部网络中 Web Interface、StoreFront 或 Endpoint Management 的服务器。

使用 **Citrix Endpoint Management**、**Citrix Virtual Apps and Desktops** 进行部署

November 3, 2021

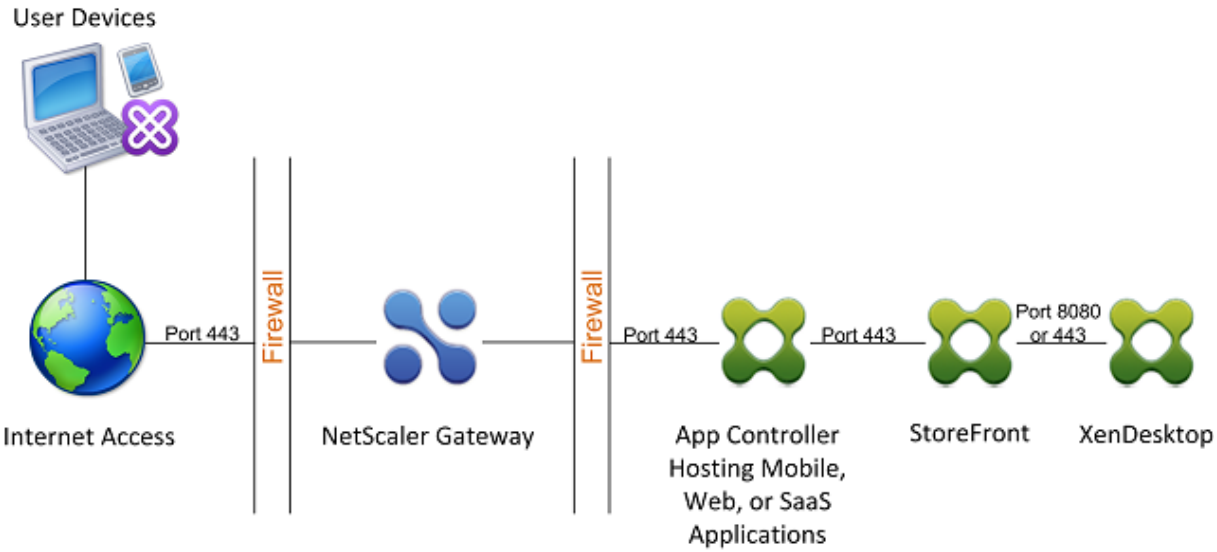
您可以让用户连接到网络中托管的 Windows、Web、SaaS 和移动应用程序以及虚拟桌面。可以使用 Citrix Gateway、Citrix Endpoint Management 以及 Citrix Virtual Apps and Desktops，为远程和内部用户提供对应用程序和桌面的访问权限。Citrix Gateway 对用户进行身份验证，然后允许用户使用 Citrix Workspace 应用程序或 Secure Hub 访问其应用程序。

用户通过使用 Citrix Workspace 应用程序和 StoreFront 连接到在 Citrix Virtual Apps 中发布的基于 Windows 的应用程序以及在 Citrix Virtual Desktops 中发布的虚拟桌面。

Citrix Endpoint Management 包含 Citrix Endpoint Management，允许用户连接到 Web、SaaS 和 MDX 应用程序。通过 Endpoint Management，您可以管理 Web、SaaS 和 MDX 应用程序，用于单点登录 (SSO) 以及 ShareFile 文档。在内部网络中安装 Endpoint Management。远程用户通过 Citrix Gateway 连接到 Endpoint Management 以访问其应用程序和 ShareFile 数据。远程用户可以使用 Citrix Gateway 插件、Citrix Workspace 应用程序或 Secure Hub 进行连接，以访问应用程序和 ShareFile。内部网络中的用户可以使用 Citrix Workspace 应用直接连接到 Endpoint Management。下图显示了使用 Endpoint Management 和 StoreFront 部署的 Citrix Gateway。

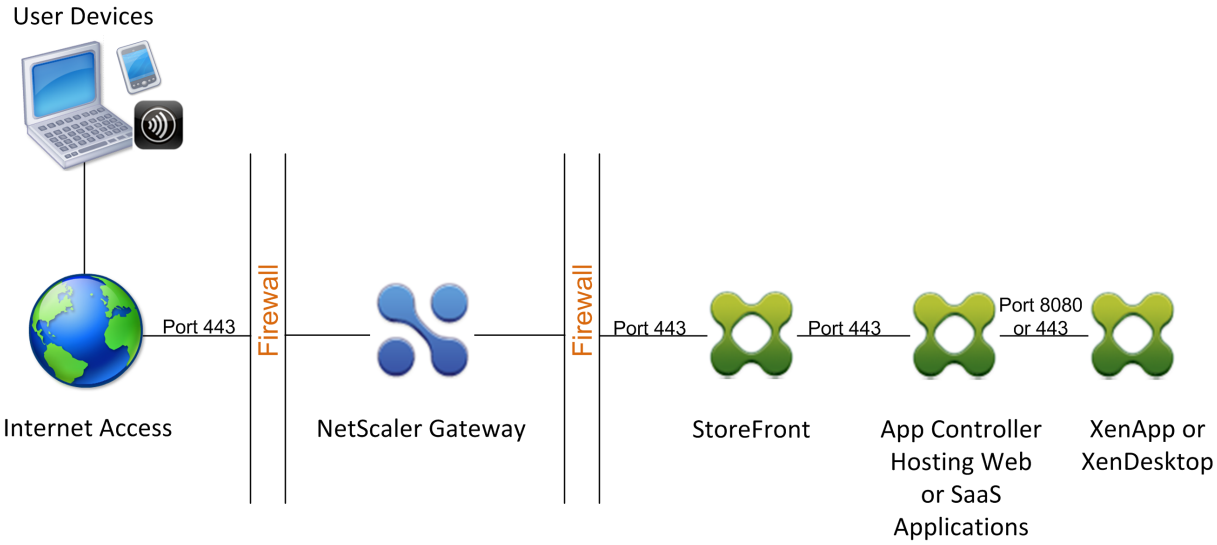
如果您的部署提供了从 Endpoint Management 访问 MDX 应用程序的权限，并从 StoreFront 访问基于 Windows 的应用程序，则可以在 StoreFront 前部署 Endpoint Management，如下图所示：

图 1. 在 StoreFront 前面使用 Endpoint Management 部署 Citrix Gateway



如果您的部署不提供对 MDX 应用程序的访问权限，StoreFront 将位于 Endpoint Management 的前面，如下图所示：

图 2. 在 Endpoint Management 前面使用 StoreFront 部署 Citrix Gateway



对于每个部署，StoreFront 和 Endpoint Management 必须驻留在内部网络中，Citrix Gateway 必须位于 DMZ 中。有关部署 Endpoint Management 的更多信息，请参阅安装 Endpoint Management主题。有关部署 StoreFront 的更多信息，请参阅StoreFront主题。

使用 **Web Interface** 访问 **Citrix Virtual Apps and Desktops** 资源

April 6, 2020

运行 Citrix Virtual Apps and Desktops 的一台或多台计算机创建服务器场。如果您的企业网络包含服务器场，则可以使用 Web Interface 部署 Citrix Gateway，以便为已发布的应用程序或虚拟桌面提供安全的 Internet 访问。

在此类部署中，Citrix Gateway 与 Web Interface 和 Secure Ticket Authority (STA) 配合使用，为运行 Citrix Virtual Apps 的计算机上托管的已发布应用程序或 Citrix Virtual Desktops 提供的虚拟桌面提供身份验证、授权和重定向。

通过将 Citrix Gateway 与 Web Interface、Citrix Virtual Apps and Desktops 集成来实现此功能。此集成为 Web Interface 的高级身份验证和访问控制选项。有关 Web Interface 的详细信息，请参阅 Citrix 文档库中的 Web Interface 文档。

远程连接到服务器场不需要 Citrix Gateway 插件。要访问已发布的应用程序或桌面，用户可以使用 Citrix Workspace 应用进行连接。

将 **Citrix Gateway** 与 **Citrix Virtual Apps and Desktops** 集成

April 6, 2020

为用户连接配置 Citrix Gateway 时，可以包含到 Citrix Virtual Apps、Citrix Virtual Desktops 或两者的网络流量的设置。为此，请将 Citrix Gateway 和 Web Interface 配置为相互通信。

集成这些产品的任务包括：

- 在 Citrix Virtual Apps and Desktops 场中创建 Web Interface 站点。
- 在 Web Interface 中配置设置以通过 Citrix Gateway 路由用户连接。
- 将 Citrix Gateway 配置为与 Web Interface 和安全票证颁发机构 (STA) 进行通信。

您还可以通过在双跃点 DMZ 中部署 Citrix Gateway，将 Citrix Gateway 配置为与 Citrix Virtual Apps 服务器场进行通信。有关详细信息，请参阅在双跃点 DMZ 中部署 Citrix Gateway。

Citrix Gateway 和 Web Interface 使用 STA 和 Citrix XML 服务建立用户连接。STA 和 XML Service 可以在 Citrix Virtual Apps and Desktops 服务器上运行。

建立到服务器场的安全连接

April 6, 2020

以下示例演示了部署在 DMZ 中的 Citrix Gateway 如何与 Web Interface 配合使用，以便为安全企业网络中可用的已发布资源提供安全的单点访问。

在此示例中，存在以下所有条件：

- Internet 中的用户设备通过使用 Citrix Workspace 应用程序连接到 Citrix Gateway。

- Web Interface 位于安全网络中的 Citrix Gateway 后面。用户设备与 Citrix Gateway 建立初始连接，并将连接传递到 Web Interface。
- 安全网络包含服务器场。此服务器场中的一台服务器运行安全票证颁发机构 (STA) 和 Citrix XML 服务。STA 和 XML Service 可以在 Citrix Virtual Apps and Desktops 上运行。

进程概述：用户访问服务器场中的已发布资源

1. 远程用户键入 Citrix Gateway 的地址；例如https://www.ag.wxyco.com，在 Web 浏览器的地址字段中。用户设备在端口 443 上尝试此 SSL 连接，必须通过防火墙打开该端口才能成功连接。
2. Citrix Gateway 接收连接请求，系统会要求用户提供其凭据。凭据将通过 Citrix Gateway 传回，对用户进行身份验证，并将连接传递到 Web Interface。
3. Web Interface 将用户凭据发送到服务器场中运行的 Citrix XML 服务。
4. XML 服务对用户凭据进行身份验证，并向 Web Interface 发送一个已发布的应用程序或用户有权访问的桌面列表。
5. Web Interface 使用用用户有权访问的已发布资源（应用程序或桌面）的列表填充网页，并将此网页发送到用户设备。
6. 用户单击已发布的应用程序或桌面链接。HTTP 请求会发送到 Web Interface，指示用户单击的已发布资源。
7. Web Interface 与 XML 服务交互，并收到一个票证，指示运行已发布资源的服务器。
8. Web Interface 向 STA 发送会话工单请求。此请求指定运行已发布资源的服务器的 IP 地址。STA 保存此 IP 地址并将请求的会话票证发送到 Web Interface。
9. Web Interface 生成一个 ICA 文件，其中包含 STA 发出的票证，并将其发送到用户设备上的 Web 浏览器。Web Interface 生成的 ICA 文件包含 Citrix Gateway 的完全限定域名 (FQDN) 或域名系统 (DNS) 名称。请注意，运行请求资源的服务器的 IP 地址永远不会向用户显示。
10. ICA 文件包含指示 Web 浏览器启动 Citrix Workspace 应用程序的数据。用户设备通过使用 ICA 文件中的 Citrix Gateway FQDN 或 DNS 名称连接到 Citrix Gateway。进行初始 SSL/TLS 握手以建立 Citrix Gateway 的标识。
11. 用户设备将会话票证发送到 Citrix Gateway，然后 Citrix Gateway 联系 STA 进行票证验证。
12. STA 将请求的应用程序驻留在其上的服务器的 IP 地址返回到 Citrix Gateway。
13. Citrix Gateway 建立到服务器的 TCP 连接。
14. Citrix Gateway 完成与用户设备的连接握手，并向用户设备指示已与服务器建立连接。用户设备和服务器之间的所有其他流量都通过 Citrix Gateway 进行代理。用户设备与 Citrix Gateway 之间的流量已加密。Citrix Gateway 和服务器之间的流量可以单独加密，但默认情况下不加密。

使用 **Web Interface** 进行部署

April 6, 2020

当您部署 Citrix Gateway 以提供对 Citrix Virtual Apps and Desktops 的安全远程访问时，Citrix Gateway 与 Web Interface 和 Secure Ticket Authority (STA) 结合使用，以提供对服务器场中托管的已发布应用程序和桌面的

访问权限。

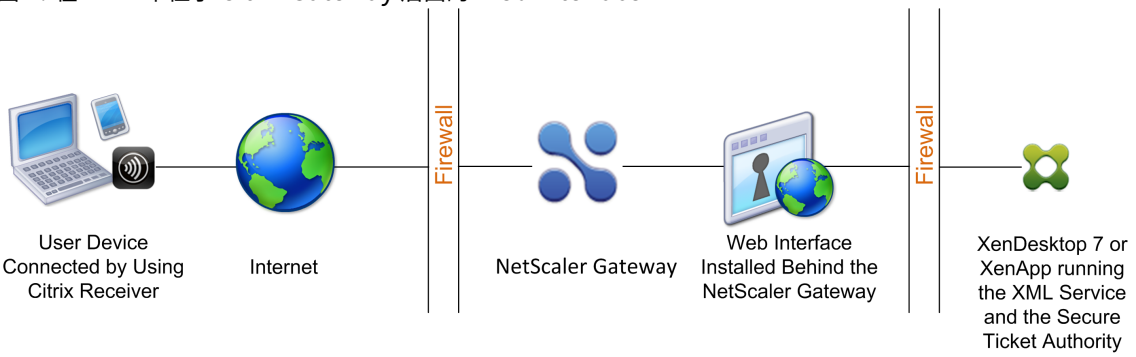
在 DMZ 中部署 Citrix Gateway 是使用服务器场运行时最常见的配置。在此配置中，Citrix Gateway 为通过 Web Interface 访问已发布资源的 Web 浏览器和 Citrix Workspace 应用程序提供安全的单一访问点。本节介绍有关此部署选项的基本方面。

组织网络的配置决定了使用服务器场运行时 Citrix Gateway 的部署位置。您有以下两个选项：

- 如果您的组织使用单个 DMZ 保护内部网络，请在 DMZ 中部署 Citrix Gateway。
- 如果您的组织使用两个 DMZ 保护内部网络，请在双跃点 DMZ 配置的两个网段中的每个网段中部署一个 Citrix Gateway。有关详细信息，请参阅在双跃点 DMZ 中部署 Citrix Gateway。
  注意：您还可以使用安全网络中的第二个 Citrix Gateway 设备配置双跃点 DMZ。

在 DMZ 中部署 Citrix Gateway 以提供对服务器场的远程访问时，可以实现以下三个部署选项之一：

- 在 DMZ 中的 Citrix Gateway 后面部署 Web Interface。在此配置中，如下图所示，Citrix Gateway 和 Web Interface 都部署在 DMZ 中。初始用户连接转到 Citrix Gateway，然后重定向到 Web Interface。
  图 1. 在 DMZ 中位于 Citrix Gateway 后面的 Web Interface



- 部署与 DMZ 中的 Web Interface 并行的 Citrix Gateway。在此配置中，Citrix Gateway 和 Web Interface 都部署在 DMZ 中，但初始用户连接将转到 Web Interface 而不是 Citrix Gateway。
- 在 DMZ 中部署 Citrix Gateway 并在内部网络中部署 Web Interface。在此配置中，Citrix Gateway 会在将请求中继到安全网络中的 Web Interface 之前对用户请求进行身份验证。Web Interface 不执行身份验证，但与 STA 交互并生成 ICA 文件，以确保 ICA 流量通过 Citrix Gateway 路由到服务器场。

部署 Web Interface 的位置取决于许多因素，包括：

- 身份验证。用户登录时，Citrix Gateway 或 Web Interface 都可以对用户凭据进行身份验证。在网络中放置 Web Interface 的位置是部分决定用户身份验证的一个因素。
- 用户软件。用户可以使用 Citrix Gateway 插件或 Citrix Workspace 应用程序连接到 Web Interface。可以仅使用 Citrix Workspace 应用程序限制用户可以访问的资源，或者使用 Citrix Gateway 插件为用户提供更大的网络访问权限。用户连接方式以及允许用户连接的资源有助于确定在网络中部署 Web Interface 的位置。

在安全网络中部署 **Web Interface**

April 6, 2020

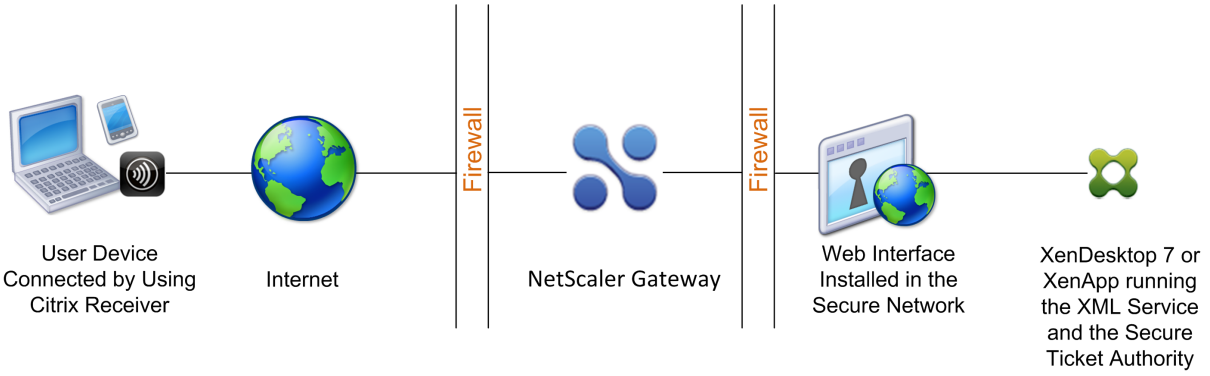
在此部署中，Web Interface 驻留在安全的内部网络中。Citrix Gateway 位于 DMZ 中。Citrix Gateway 在将请求发送到 Web Interface 之前对用户请求进行身份验证。

在安全网络中部署 Web Interface 时，必须在 Citrix Gateway 上配置身份验证。

如果使用 Citrix Virtual Apps and Desktops 部署 Web Interface，则在安全网络中部署 Web Interface 是默认部署方案。安装 Desktop Delivery Controller 时，也会安装 Web Interface 的自定义版本。

> 重要提示：
> 当 Web Interface 位于安全网络中时，应在 Citrix Gateway 上启用身份验证。用户连接到 Citrix Gateway，键入其凭据，然后连接到 Web Interface。禁用身份验证时，未经身份验证的 HTTP 请求将直接发送到运行 Web Interface 的服务器。仅当 Web Interface 位于 DMZ 中且用户直接连接到 Web Interface 时，才建议禁用 Citrix Gateway 上的身份验证。

图 1. 位于安全网络内的 Web Interface



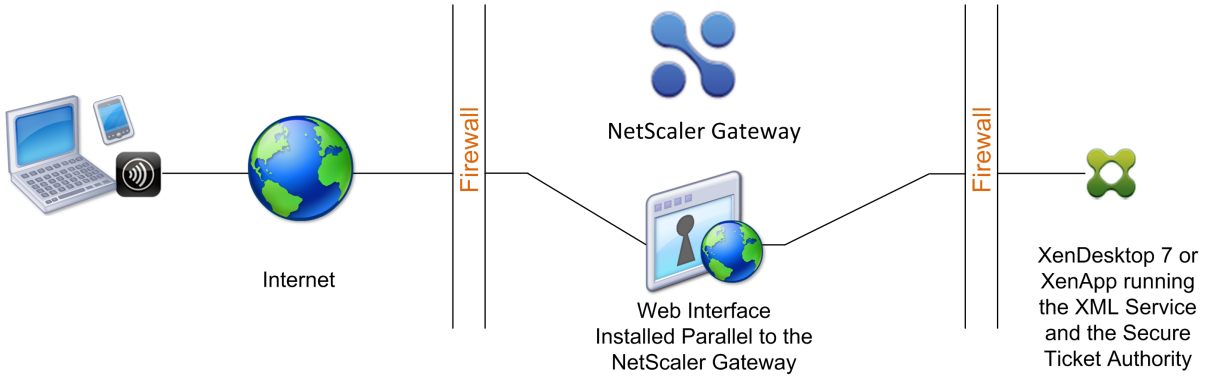
在 **DMZ** 中部署与 **Citrix Gateway** 并行的 **Web Interface**

April 6, 2020

在此部署中，Web Interface 和 Citrix Gateway 都位于 DMZ 中。用户通过使用 Web 浏览器或 Citrix Workspace 应用直接连接到 Web Interface。用户连接首先发送到 Web Interface 进行身份验证。身份验证后，连接将通过 Citrix Gateway 进行路由。用户成功登录 Web Interface 后，可以访问服务器场中的已发布应用程序或桌面。当用户启动应用程序或桌面时，Web Interface 会发送一个 ICA 文件，其中包含通过 Citrix Gateway 路由 ICA 流量的说明，就好像它是运行安全网关的服务器一样。Web Interface 提供的 ICA 文件包括由安全票证机构 (STA) 生成的会话票证。

当 Citrix Workspace 应用程序连接到 Citrix Gateway 时，系统会显示票证。Citrix Gateway 联系 STA 以验证会话票证。如果票证仍然有效，则用户的 ICA 流量将中继到服务器场中的服务器。下图显示了此部署。

图 1. 与 Citrix Gateway 并行安装的 Web Interface



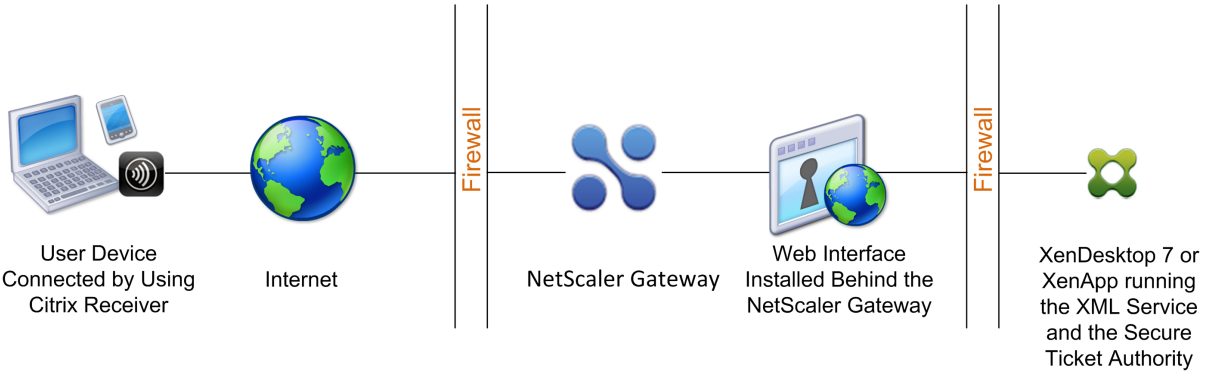
当 Web Interface 与 DMZ 中的 Citrix Gateway 并行运行时，您无需在 Citrix Gateway 上配置身份验证。Web Interface 对用户进行身份验证。

在 **DMZ** 中部署 **Citrix Gateway** 后面的 **Web Interface**

April 6, 2020

在此配置中，Citrix Gateway 和 Web Interface 都部署在 DMZ 中。当用户使用 Citrix Workspace 应用登录时，初始用户连接将转到 Citrix Gateway，然后重定向到 Web Interface。要通过单个外部端口路由所有 HTTPS 和 ICA 流量并要求使用单个 SSL 证书，Citrix Gateway 可充当 Web Interface 的反向 Web 代理。

图 1. 位于 Citrix Gateway 后面的 Web Interface



当 Web Interface 部署在 DMZ 的 Citrix Gateway 后面时，您可以在设备上配置身份验证，但不是必需的。您可以让 Citrix Gateway 或 Web Interface 对用户进行身份验证，因为两者都位于 DMZ 中。

设置 **Web Interface** 站点以工作

April 6, 2020

通过 Web Interface，用户可以访问 Citrix Virtual Apps 和内容以及 Citrix Virtual Desktops 虚拟桌面。用户通过标准 Web 浏览器或 Citrix Workspace 应用访问其已发布的应用程序和桌面。

您可以使用访问管理控制台配置 Web Interface 5.1 站点，并使用 Web Interface 管理控制台来创建版本 5.2、5.3 和 5.4 的 Web Interface 站点。您只能在基于 Windows 的平台上安装控制台。

要将 Web Interface 配置为与 Citrix Gateway 一起使用，您需要：

- 为您正在使用的版本创建 Web Interface 站点。
- 在 Web Interface 中配置设置。
- 在 Citrix Gateway 上配置 Web Interface 设置。

Web Interface 功能

April 6, 2020

在配置 Web Interface 以使用 Citrix Gateway 之前，您需要了解 Citrix Virtual Apps Web 站点与 Citrix Virtual Apps Services 站点之间的区别。

- **Citrix Virtual Apps Web** 站点。Web Interface 提供了创建和管理 Citrix Virtual Apps Web 站点的功能。用户使用 Web 浏览器和插件远程访问已发布的资源和流应用程序。
- **Citrix Virtual Apps Services** 站点。Citrix Virtual Apps 是专为灵活性和易于配置而设计的插件。通过将 Citrix Virtual Apps 与 Web Interface 上的 Citrix Virtual Apps Services 站点结合使用，您可以将已发布的资源与用户桌面集成。用户可通过单击桌面或“开始”菜单上的图标，或通过单击计算机桌面的通知区域访问远程和流应用程序以及远程桌面和内容。您可以确定用户可以访问和修改的配置选项，例如音频、显示和登录设置。

  > 注意：如果选择此选项，则不支持对虚拟桌面的访问。

有关详细信息，请参阅 Citrix eDocs 库中“技术”节点中的 Web Interface 文档。

设置 Web Interface 站点

April 6, 2020

如果在安全网络中部署 Web Interface 并在 Citrix Gateway 上配置身份验证，则当用户连接到 Citrix Gateway 时，设备会对用户进行身份验证。

> 重要提示：在配置 Citrix Gateway 之前安装和配置 Web Interface。有关详细信息，请参阅 Citrix eDocs 库中“
> 技术”节点中的 Web Interface 文档。

创建 Web Interface 站点的步骤包括：

- 选择用户登录的方式。这可以通过 Web 浏览器、Citrix Gateway 插件或 Citrix Workspace 应用程序进行。有关信息，请参阅 Web Interface 功能。
- 确定用户身份验证的位置。Citrix Gateway 或 Web Interface。

> 注意：当 Web Interface 位于安全网络中时，您可以在 Citrix Gateway 上的虚拟服务器上启用身份验证。禁用身份验证时，未经身份验证的 HTTP 请求将直接发送到运行 Web Interface 的服务器。仅当 Web Interface 位于 DMZ 中且用户直接连接到 Web Interface 时，才建议禁用 Citrix Gateway 上的身份验证。

确保您在 Citrix Gateway 上安装了有效的服务器证书。有关使用证书的更多信息，请参阅安装和管理证书。

> 重要：要使 Web Interface 与 Citrix Gateway 10.1 正常工作，运行 Web Interface 的服务器必须信任 Citrix Gateway 证书，并能够将虚拟服务器完全限定域名 (FQDN) 解析为正确的 IP 地址。

创建 **Web Interface 5.4** 站点

April 6, 2020

Citrix Web Interface Management 控制台是 Microsoft 管理控制台 (MMC) 3.0 管理单元，可用于创建和配置 Microsoft Internet Information Services (IIS) 上托管的 Citrix Virtual Apps Web 和 Citrix Virtual Apps Services 站点。Web Interface 站点类型显示在左窗格中。中央结果窗格显示左窗格中选定的站点类型容器中的可用站点。

Citrix Web Interface 管理控制台使您能够快速轻松地执行日常管理任务。“操作” 窗格列出了当前可用的任务。与左窗格中所选项目相关的任务显示在顶部，结果窗格中所选项目可用的操作如下所示。

使用控制台时，您的配置在您使用控制台提交更改时生效。因此，如果某些 Web Interface 设置的值与当前配置不相关，并且相应的设置在 Webinterface.conf 中重置为默认值，则可能会禁用某些 Web Interface 设置。Citrix 建议您为您的站点创建 WebInterface.conf 和 config.xml 文件的定期备份。

安装 Microsoft Internet 信息服务的 Web Interface 时，将自动安装 Citrix Web Interface 管理控制台。通过单击“开始”>“所有程序”>“Citrix”>“管理控制台”>“Citrix Web Interface 管理” 来运行控制台。

> 注意：
> 必须确保在安装 Web Interface 的服务器上存在 MMC 3.0，因为这是安装 Citrix Web Interface 管理控制台的先决条件。默认情况下，MMC 3.0 在支持托管 Web Interface 的所有 Windows 平台上都可用。

使用配置文件

您可以编辑以下配置文件来配置 Web Interface 站点：

- Web Interface 配置文件。Web Interface 配置文件 WebInterface.conf 允许您更改许多 Web Interface 属性；它可以在 Microsoft Internet 信息服务 (IIS) 和 Java 应用程序服务器上使用。您可以使用此文件执行日常管理任务并自定义更多设置。编辑 WebInterface.conf 中的值并保存更新后的文件以应用更改。有关

使用 WebInterface.conf 配置 Web Interface 的详细信息，请参阅 Citrix eDocs 中“技术”节点中的 Web Interface 文档。

- Citrix 在线插件配置文件。您可以使用 Web Interface 服务器上的 config.xml 文件配置 Citrix 联机插件。

使用 **Citrix Web Interface** 管理控制台配置站点

April 6, 2020

Citrix Web Interface Management 控制台是 Microsoft 管理控制台 (MMC) 3.0 管理单元，可用于创建和配置 Microsoft Internet Information Services (IIS) 上托管的 Citrix Virtual Apps Web 和 Citrix Virtual Apps Services 站点。Web Interface 站点类型显示在左窗格中。中央结果窗格显示左窗格中选定的站点类型容器中的可用站点。

Citrix Web Interface 管理控制台使您能够快速轻松地执行日常管理任务。“操作”窗格列出了当前可用的任务。与左窗格中所选项目相关的任务显示在顶部，结果窗格中所选项目可用的操作如下所示。

使用控制台时，您的配置在您使用控制台提交更改时生效。因此，如果某些 Web Interface 设置的值与当前配置不相关，并且相应的设置在 Webinterface.conf 中重置为默认值，则可能会禁用某些 Web Interface 设置。Citrix 建议您为您的站点创建网络接口.Conf 和配置.xml 文件的定期备份。

当您安装适用于 Microsoft IIS 的 Web Interface 时，将自动安装 Citrix Web Interface 管理控制台。通过单击“开始”>“所有程序”>“Citrix”>“管理控制台”>“Citrix Web Interface 管理”来运行控制台。

注意：必须确保在安装 Web Interface 的服务器上存在 MMC 3.0，因为这是安装 Citrix Web Interface 管理控制台的先决条件。默认情况下，MMC 3.0 在支持托管 Web Interface 的所有 Windows 平台上都可用。

在 **Web Interface 5.4** 中配置 **Citrix Gateway** 设置

April 6, 2020

要在部署中使用 Citrix Gateway，必须配置 Web Interface 支持该设备。若要执行此操作，请使用 Citrix Web Interface 管理控制台中的“安全访问”任务。

在 **Web Interface** 中配置 **Citrix Gateway** 设置

1. 在 Windows“开始”菜单上，单击“所有程序”>“Citrix”>“管理控制台”>“Citrix Web Interface Management”。

2. 在 Citrix Web Interface Management 控制台的左窗格中，单击“Citrix Virtual Apps Web 站点”或“Citrix Virtual Apps Services 站点”，然后在结果窗格中选择您的站点。

3. 在操作窗格中，单击安全访问。

4. 在“指定访问方法”页上，执行以下操作之一：

- 单击“添加”以添加新的访问路由。
- 从列表中选择现有路线，然后单击“编辑”。

5. 从“访问方法”列表中，选择以下选项之一：

- 如果要将 Citrix 服务器的实际地址发送到 Citrix Gateway，请选择网关直接。
- 如果要将 Citrix Virtual Apps 服务器的备用地址发送到 Citrix Gateway，请选择备用网关。

  注意：如果使用备用地址，则无法访问 Citrix Virtual Desktops 虚拟机。
- 如果希望提供给 Citrix Gateway 的地址由 Web Interface 中设置的地址转换映射确定，请选择已转换的网关。

6. 输入用于标识客户端网络的网络地址和子网掩码。使用“上移”和“下移”按钮在“用户设备地址”表中按优先级顺序放置访问路由，然后单击“下一步”。

7. 如果您不使用网关地址转换，请继续执行步骤 10。如果使用网关地址转换，请在“指定地址转换”页面上执行以下操作之一：

- 单击添加添加新的地址翻译。
- 从列表中选择现有地址转换，然后单击编辑。

8. 在“访问类型”区域中，选择以下选项之一：

- 如果希望 Citrix Gateway 使用转换的地址连接到 Citrix 服务器，请选择网关路由转换。
- 如果您在“用户设备地址”表中配置了客户端转换的路由，并希望 Citrix 客户端和 Citrix Gateway 使用已转换的地址连接到 Citrix 服务器，请选择“用户设备和网关路由转换”。

9. 输入 Citrix 服务器的内部和外部（已转换）端口和地址，单击“确定”，然后单击“下一步”。
Citrix Gateway 连接到 Citrix 服务器时，它将使用外部端口号和地址。确保您创建的映射与服务器场正在使用的寻址类型相匹配。

10. 在“指定网关设置”页面上，指定客户端必须使用的 Citrix Gateway 设备的完全限定域名 (FQDN) 和端口号。FQDN 必须与网关上安装的证书上的内容匹配。

11. 如果希望 Citrix 服务器在客户端尝试自动重新连接时保持断开连接的会话打开状态，请选择“启用会话可靠性”。

12. 如果您启用了会话可靠性并希望使用来自两个安全票证颁发机构 (STA) 服务器的同时票证，请选择从两个 STA 请求票证（如果可用）。启用此选项时，Web Interface 会从两个不同的 STA 获取票证，以便如果一个 STA 在会话过程中变得不可用，则不会中断用户会话。如果 Web Interface 由于任何原因无法联系两个 STA，则会回退为使用单个 STA。单击下一步。

13. 在“指定安全票证颁发机构设置”页上，执行以下操作之一：

- 单击“添加”以指定 Web Interface 可以使用的 STA 的 URL。
- 从列表中选择一个条目，然后单击编辑。

使用“上移”和“下移”按钮按优先级顺序放置 STA。
STA 包含在 Citrix XML 服务中；例如，`http\[s\]://servername.domain.com/scripts/ctxsta.dll`。

您可以为容错指定多个 STA；但是，Citrix 建议您不要为此目的使用外部负载均衡器。

14. 选择“用于负载均衡”以选择是否启用 STA 之间的负载均衡。

启用负载平衡可让您在服务器之间均匀分配连接，以免任何一台服务器变得过载。

15. 选择“绕过失败的服务器”以指定绕过无法访问的 STA 的时间长度。

Web Interface 提供 STA URL 列表上的服务器之间的容错能力，以便如果发生通信错误，则在指定的时间段内绕过失败的服务器。

创建 **Web Interface 5.3** 站点

April 6, 2020

创建 Web Interface 5.3 站点时，可以要求用户使用 Web 浏览器、Citrix Workspace 应用程序或 Citrix Desktop Citrix Workspace 应用程序登录。可以使用 Citrix Web Interface Management 控制台创建多个 Web Interface 站点。

您只能使用智能卡启用单点登录到带 Web Interface 5.3 的 Web Interface。此版本的 Web Interface 可以在 Citrix Virtual Apps 4.5、5.0 和 6.0 上运行。

Web Interface 5.3 在以下操作系统上运行：

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

> 注意：
> Citrix Virtual Apps 6.0 仅在 Windows Server 2008 R2 上运行。

创建 **Web Interface 5.3** 站点

1. 单击开始 > 所有程序 > Citrix > 管理控制台 > Citrix Web Interface 管理。
2. 在左窗格中，选择 Citrix Virtual Apps Web 站点。用户使用 Web 浏览器登录到 Web Interface。
3. 在操作菜单上，单击创建站点。
4. 保留默认的 Internet 信息服务 (IIS) 站点和路径，然后单击下一步。

   默认站点路径为 /Citrix/Citrix Virtual Apps，或者您可以指定路径。

   > 注意：
   > 如果有任何预先存在的 Citrix Virtual Apps Web 站点使用默认路径，则会添加适当的增量来区分新站点。

5. 在“指定进行用户身份验证的位置”中，选择以下选项之一：

- 在 Web Interface，让用户使用 Web Interface 进行身份验证。

  如果 Web Interface 部署为并行于非军事区 (DMZ) 中 Citrix Gateway 的独立服务器，请选择此选项。

- 在 Access Gateway，让用户使用 Citrix Gateway 设备进行身份验证。

  如果选择此选项，Citrix Gateway 将对用户进行身份验证，并启动 Web Interface 的单点登录（如果在设备上配置了 Web Interface）。

> 注意：
> 如果在 Citrix Gateway 上配置了 SmartAccess，则此设置将在 Citrix Virtual Apps and Desktops 中启用 SmartAccess。

6. 单击下一步。
7. 在步骤 5 中，在“身份验证服务 URL”中，键入 Citrix Gateway 身份验证服务 URL 的 Web 地址，例如 `https://access.company.com/CitrixAuthService/AuthService.asmx`，然后单击“下一步”。
8. 在“身份验证选项”下，选择用户登录的方式。
   - 明确的。用户通过使用 Web 浏览器登录。
   - 智能卡用户通过使用智能卡登录。
9. 单击下一步。
10. 如果您在步骤 8 中选择了智能卡，请选择以下选项之一：

```
- 提示用户输入 PIN。用户在启动已发布的应用程序或桌面时输入个人标识号 (PIN)。
- 用户在启动已发布的应用程序或桌面时不必输入 PIN。
```

您将收到一个显示您的设置的摘要屏幕。单击“
下一步”以创建 Web Interface 网站。成功创建站点后，系统会提示您配置 Web Interface 中的其余设置。按照向导中的说明完成配置。

在 **Web Interface 5.3** 中配置 **Citrix Gateway** 设置

April 6, 2020

创建 Web Interface 5.3 站点后，可以使用 Citrix Web Interface 管理配置 Citrix Gateway 的设置。

为 **Citrix Gateway** 配置 **Web Interface 5.3** 设置的步骤

1. 单击开始 > 所有程序 > Citrix > 管理控制台 > Citrix Web Interface 管理。
2. 在 Citrix Web Interface Management 的左窗格中，单击“Citrix Virtual Apps Web 站点”。

3. 在操作窗格中，单击安全访问。
4. 在“编辑安全访问设置”对话框中，单击“添加”。
5. 在“添加访问路由”对话框中，键入用户设备地址、子网掩码，然后在“访问方法”中，选择“网关直接”，单击“确定”，然后单击“下一步”。如果未指定用户设备地址和子网掩码，则网关直接选项将应用于所有用户设备。网关直接选项适用于从内部网络外部连接的用户设备，而 Direct 选项适用于从内部网络内连接的用户设备。
6. 在地址 (FQDN) 中，键入 Citrix Gateway 完全限定域名 (FQDN)。这必须与 Citrix Gateway 证书上使用的 FQDN 相同。
7. 在端口中，键入端口号。默认值为 443。
8. 若要启用会话可靠性，请单击“启用会话可靠性”，然后单击“下一步”。
9. 在安全票证机构 URL 下，单击添加。
10. 在“Secure Ticket Authority URL”中，键入在 Citrix Virtual Apps 上运行 XML Service 的主服务器的名称，单击“确定”，然后单击“完成”。例如，键入`http://Citrix Virtual Appssrv01/Scripts/CtxSta.dll`。

在 Web Interface 中配置设置后，可以在 Citrix Gateway 上配置设置。

将 **Citrix Virtual Apps and Desktops** 添加到单个站点

April 6, 2020

如果您正在运行 Citrix Virtual Apps and Desktops，则可以将两个应用程序添加到一个 Web Interface 站点。此配置允许您使用 Citrix Virtual Apps and Desktops 中的相同 Secure Ticket Authority (STA) 服务器。

> 注意：
> Citrix Virtual Desktops 支持 Web Interface。Web Interface 所需的最低版本为 5.0。

如果您使用的是 Web Interface 5.3 或 5.4，则可以使用 Web Interface Management 控制台将 Citrix Virtual Apps and Desktops 站点组合起来。

> 注意：
> 如果服务器场位于不同的域中，则必须在域之间建立双向信任。

使用 **Web Interface 5.3** 或 **5.4** 将 **Citrix Virtual Apps and Desktops** 添加到单个站点

1. 单击开始 > 所有程序 > **Citrix** > 管理控制台 > **Citrix Web Interface** 管理。
2. 在左窗格中，选择 **Citrix Virtual Apps Web** 站点。
3. 在“操作”窗格中，右键单击站点，然后单击“服务器场”。
4. 在“管理服务器场”对话框中，单击“添加”。
5. 完成服务器场的设置，然后单击“确定”两次。

要获得使用 Citrix Virtual Desktops 时的最佳体验，请将 WebInterface.conf 配置文件中的 UserInterfaceBranding 设置更改为 Desktops。

通过 **Citrix Gateway** 路由用户连接

November 3, 2021

在 Citrix Virtual Apps and Desktops 中，可以将服务器配置为仅接受通过 Citrix Gateway 路由的连接。在 Citrix XenApp 6.5 中，您可以在 Citrix AppCenter 中配置策略，以便通过 Citrix Gateway 路由连接。在 Citrix Virtual Desktops 7.1 中，您可以使用 Citrix Studio 配置设置。

将 **Citrix XenApp 6.5** 服务器属性配置为仅接受通过 **Citrix Gateway** 路由的连接

1. 单击 “开始”>“管理工具”>“Citrix”>“管理控制台”>“Citrix AppCenter”。
2. 展开 “NetScaler 资源”>“Citrix Virtual Apps”>“farmName”，其中 farmName 为服务器场的名称。
3. 点击策略。
4. 在中心窗格中，单击计算机或用户，然后单击新建。
5. 在 “新建策略” 向导的 “名称” 中，键入策略的名称，然后单击 “下一步”。
6. 在 “类别” 下，单击 “服务器设置”。
7. 在 “设置” 下，单击 “连接访问控制” 旁边的 “添加”。
8. 在添加设置 **-** 连接访问控制对话框中的值中，选择 **“**仅 **Citrix Access Gateway** 连接**”**，然后单击确定。
9. 单击 下一步两次，然后单击 创建。Citrix Virtual Apps 创建策略。

将 **Citrix Virtual Desktops** 服务器属性配置为仅接受通过 **Citrix Gateway** 路由的连接

您可以限制对交付组计算机的访问。您可以使用可筛选通过 Citrix Gateway 建立的用户连接的 SmartAccess 来限制用户的访问权限。您可以在 Studio 的 “策略” 节点中执行此任务，也可以通过中所述的策略设置执行此任务快速参考表。

1. 在 Studio 中的交付组下，选择要限制的交付组。
2. 单击编辑交付组，然后单击访问策略。
3. 在 “访问策略” 页面上，选择 “通过 Citrix Gateway 连接”。仅允许通过 Citrix Gateway 进行连接。
4. 要选择这些连接的子集，请选择满足以下任何筛选器的连接：
   a) 定义 Citrix Gateway 站点。
   b) 添加、编辑或删除用于定义交付组允许的用户访问方案的 SmartAccess 字符串。有关配置 SmartAccess 的更多信息，请参阅在 Citrix Gateway 上配置 SmartAccess。

配置与 **Web Interface** 的通信

April 6, 2020

可以将 Citrix Gateway 配置为与 Citrix Virtual Apps and Desktops 上运行的 Web Interface 进行通信。为此，请在 Citrix Gateway 上配置虚拟服务器。接下来，将签名服务器证书和身份验证、会话、预身份验证和身份验证后策略绑定到虚拟服务器。Citrix Gateway 使用虚拟服务器 IP 地址将用户连接路由到 Web Interface。

“已发布应用程序向导” 允许您配置 Citrix Gateway 以将用户连接路由到 Web Interface。Citrix Gateway 使用安全票证机构 (STA) 进行用户连接。

为已发布的应用程序和桌面配置策略

April 6, 2020

要与 Citrix Virtual Apps and Desktops 服务器建立通信，需要配置 Citrix Gateway 以识别这些服务器。您可以全局配置设置，也可以使用绑定到用户、组或虚拟服务器的策略。

在 **Citrix Gateway** 上全局配置 **Web Interface**

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway，然后单击 “全局设置”。
2. 在详细信息窗格的 “设置” 下，单击 “更改全局设置”。
3. 在 “全局 Citrix Gateway 设置” 对话框的 “客户端体验” 选项卡上，执行以下操作：
   a) 在插件类型中，选择 Java。
   b) 在无客户端访问中，选择允许。

   > 注意：执行步骤 3 以支持具有 VPN 功能的 Citrix Workspace 应用程序，例如适用于 iOS 的 Citrix Workspace 应用程序或适用于 Android 的 Citrix Workspace 应用程序。要支持移动 Citrix Workspace 应用程序，您必须至少安装访问网关 10、构建 69.6 或访问网关 10，构建 71.6014.e。如果您正在运行 Access Gateway 9.3，则无需执行此步骤。
4. 在 “已发布的应用程序” 选项卡上，ICA 代理旁边，选择 “开”。
5. 在 Web Interface 地址旁边，键入 Web Interface 的 Web 地址，然后单 击确定。

为 **Web Interface** 配置会话策略

您可以配置会话策略并将其绑定到虚拟服务器以限制对 Web Interface 的访问。

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway 策略，然后单击 “会话”。
2. 在详细信息窗格的 “策略” 选项卡上，单击 “添加”。
3. 在 “创建会话策略” 对话框的 “名称” 中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在 “创建会话配置文件” 对话框的 “名称” 中，键入配置文件的名称。
6. 在 “客户端体验” 选项卡上，执行以下操作：
   a) 在插件类型旁边，选择覆盖全局，然后选择 Java。
   b) 在无客户端访问旁边，选择覆盖全局，然后选择允许。
7. 在 ICA 代理旁边，单击覆盖全局并选择开。
8. 在 Web Interface 地址旁边，单击覆盖全局，键入 Web Interface 的 Web 地址，然后单击创建。
9. 在 “创建会话策略” 对话框的命名表达式旁边，选择 “常规”，选择 “True”，单击 “添加表达式”，单击 “创建”，然后单击 “关闭”。

创建会话策略后，将策略绑定到虚拟服务器。

将会话策略绑定到虚拟服务器

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，选择虚拟服务器，然后单击“打开”。
3. 在“策略”选项卡上，单击“会话”，然后单击“插入策略”。
4. 从列表中选择会话策略，输入优先级号（可选），然后单击“确定”

使用已发布的应用程序向导配置设置

April 6, 2020

要使用 Web Interface 配置 Citrix Gateway，您需要以下信息：

- 运行 Citrix Virtual Apps and Desktops 的服务器的 IP 地址。
- 运行 Web Interface 的服务器的完全限定域名 (FQDN)。
- 在 Citrix Gateway 上配置的虚拟服务器。
- 为 SmartAccess 配置的会话策略。
- 如果要配置 Web Interface 故障转移，则运行 Web Interface 的其他服务器的 IP 地址。

使用 **“**已发布的应用程序**”** 向导配置 **Web Interface** 设置

1. 在配置实用程序中，单击配置选项卡，然后在导航窗格中单击 Citrix Gateway。
2. 在详细信息窗格的“入门”下，单击“已发布应用程序”向导。
3. 单击“下一步”，然后按照向导中的说明操作。

您可以在“已发布应用程序”向导中配置和激活安全票证颁发机构 (STA)。完成“已发布应用程序”向导后，设置将全局绑定。

在 **Citrix Gateway** 上配置安全票证颁发机构

April 6, 2020

Secure Ticket Authority (STA) 负责签发会话票证，以响应 Citrix Virtual Apps 上的已发布应用程序和 Citrix Virtual Desktops 上的已发布桌面的连接请求。这些会话票证构成了访问已发布资源的身份验证和授权的基础。

您可以将 STA 全局绑定或绑定到虚拟服务器。配置虚拟服务器时，还可以添加运行 STA 的多个服务器。

如果要保护 Citrix Gateway 和 STA 之间的通信，请确保在运行 STA 的服务器上安装了服务器证书。

有关 STA 的详细信息，请参阅文章NetScaler Gateway 安全票证机构。

全局绑定 **STA**

1. 导航到 **Citrix Gateway >** 全局设置。
2. 在详细信息窗格的“服务器”下，单击“绑定/取消绑定 **STA** 服务器”以供安全票证颁发机构使用。
3. 在绑定 /取消绑定 **STA** 服务器对话框中，单击 添加。
4. 在 配置 **STA** 服务器对话框中，输入 STA 服务器的 URL，单击 创建，然后单 击确定。
5. 在“**STA** 服务器”对话框的“URL”中，键入运行 STA 的服务器的 IP 地址或完全限定域名 (FQDN)，然后单击“创建”。

   > 注意：
   > 您可以将运行 STA 的多台服务器添加到列表中。Web Interface 中列出的 STA 必须与 Citrix Gateway 上配置的 STA 匹配。如果要配置多个 STA，请勿在 Citrix Gateway 和运行 STA 的服务器之间使用负载平衡。

将 **STA** 绑定到虚拟服务器

1. 导航到 **Citrix Gateway >** 虚拟服务器。
2. 在详细信息窗格中，选择一个虚拟服务器，然后单击 编辑。
3. 在“已发布的应用程序”选项卡上的“安全票证颁发机构”下，单击“添加”。
4. 在“配置 **STA** 服务器”对话框中，输入 STA 服务器的 URL，然后单击“创建”。
5. 重复步骤 4 添加其他 STA 服务器，然后单 击确定。

在 **Citrix Gateway** 上配置其他 **Web Interface** 设置

April 6, 2020

如果在 Web Interface 环境中部署 Citrix Gateway，则可以完成以下可选任务：

- 配置 Web Interface 故障转移将 Citrix Gateway 配置为故障转移到运行 Web Interface 的辅助服务器。
- 使用 Web Interface 配置智能卡访问 通过使用 Citrix Workspace 应用程序和智能卡身份验证，将用户会话配置为直接登录到 Web Interface。

配置 **Web Interface** 故障转移

April 6, 2020

可以使用已发布的应用程序向导将 Citrix Gateway 配置为故障转移到运行 Web Interface 的辅助服务器。

Web Interface 故障转移允许用户连接在主 Web Interface 发生故障时保持活动状态。配置故障转移时，除了系统 IP 地址、映射 IP 地址或虚拟服务器 IP 地址之外，还需要定义新的 IP 地址。新 IP 地址必须与系统或映射 IP 地址位于同一子网上。

在 Citrix Gateway 上配置 Web Interface 故障转移时，发送到新 IP 地址的任何网络流量都将中继到主 Web Interface。您在“已发布的应用程序”向导中选择的虚拟服务器用作网络地址转换 (NAT) IP 地址。真正的 IP 地址是 Web Interface 的地址。如果主 Web Interface 失败，网络流量将发送到辅助 Web Interface。

配置 **Web Interface** 故障转移

1. 在配置实用程序中，单击配置选项卡，然后在导航窗格中单击 Citrix Gateway。
2. 在详细信息窗格的“入门”下，单击“已发布应用程序”向导。
3. 单击“下一步”，选择一个虚拟服务器，然后单击“下一步”。
4. 在“配置客户端连接”页上，单击“配置 Web Interface 故障转移”。
5. 在“主 Web Interface”下的“Web Interface 服务器”中，键入主 Web Interface 的 IP 地址。
6. 在 Web Interface 服务器端口中，键入主 Web Interface 的端口号。
7. 在虚拟服务器 IP 中，键入用于故障转移的新 IP 地址。
8. 在虚拟服务器端口中，输入虚拟服务器的端口号。
9. 在“备份 Web Interface”下的“Web Interface 服务器”中，键入运行 Web Interface 的服务器的 IP 地址，或从列表中选择一个服务器。
10. 在 Web Interface 服务器端口中，键入 Web Interface 的端口号，然后单击确定。
11. 单击“下一步”，然后按照说明完成向导。

使用 **Web Interface** 配置智能卡访问

April 6, 2020

将 Web Interface 配置为使用智能卡身份验证时，可以配置以下部署方案以集成 Citrix Gateway，具体取决于用户登录方式：

- 如果用户通过使用 Citrix Workspace 应用程序和智能卡身份验证直接登录到 Web Interface，则 Web Interface 必须与 DMZ 中的 Citrix Gateway 并行。运行 Web Interface 的服务器也必须是域成员。

  在这种情况下，Citrix Gateway 和 Web Interface 都执行 SSL 终止。Web Interface 终止安全的 HTTP 流量，包括用户身份验证、显示已发布的应用程序和启动已发布的应用程序。Citrix Gateway 终止传入 ICA 连接的 SSL。

- 如果用户使用 Citrix Gateway 插件登录，Citrix Gateway 将执行初始身份验证。Citrix Gateway 建立 VPN 隧道时，用户可以使用智能卡登录 Web Interface。在这种情况下，您可以在 DMZ 或安全网络中安装 Citrix Gateway 后面的 Web Interface。

> 注意：
> Citrix Gateway 还可以使用客户端证书使用智能卡进行身份验证。

有关详细信息，请参阅
配置智能卡身份验证。

在 **Web Interface** 中配置对应用程序和虚拟桌面的访问

April 6, 2020

您可以将 Citrix Gateway 配置为使用 Citrix Gateway 插件（而不是 Receiver）授予用户访问已发布的应用程序和虚拟桌面的权限。要配置对应用程序和桌面的访问，可以将 Citrix Gateway 上的配置从仅使用 Receiver 连接到 Citrix Gateway，更改为使用 Citrix Gateway 插件启用连接并单点登录 Web Interface 的配置。例如，您可以配置 Citrix Gateway，以便所有用户使用 Citrix Gateway 插件进行连接，并将 Web Interface 用作主页。此方案支持单点登录到 Web Interface。

除了访问应用程序和桌面之外，用户还可以运行安装在用户设备上的应用程序，通过 VPN 隧道建立网络连接。

要启动配置，请使用以下准则：

- 创建 Web Interface 网站。
- 配置高级访问控制设置。
- 配置 SmartAccess。
- 在 Citrix Gateway 上配置端点分析。
- 在 Citrix Virtual Apps and Desktops 上配置策略和过滤器。
- 配置 Citrix Gateway，以便用户通过使用 Citrix Gateway 插件访问已发布的应用程序和虚拟桌面进行登录。

有关详细信息，请参阅 Citrix eDocs 中的以下主题：

- 设置 Web Interface 站点。
- SmartAccess 如何适用于 Citrix Virtual Apps and Desktops
- 配置终端策略
- 配置 Citrix Virtual Apps 策略和过滤器
- 在 Citrix Virtual Desktops 5 中配置策略和筛选器
- 将 Citrix Gateway 配置为与 Web Interface 通信

配置用户登录到 Citrix Virtual Apps and Desktops 时，首先要创建会话配置文件以选择适用于 Windows 的 Citrix Gateway 插件。然后，创建用于访问 Citrix Virtual Apps、Citrix Virtual Desktops 和 Web Interface 的内部网应用程序的配置文件。

为 **Citrix Gateway** 插件配置全局设置以访问应用程序和桌面

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。

2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“已发布的应用程序”选项卡上，ICA 代理旁边，选择“关”。
4. 在 Web Interface 地址中，键入 Web Interface 站点的 URL。这将成为用户的主页。
5. 在单点登录域中，键入 Active Directory 域名。
6. 在“客户端体验”选项卡上，在“插件类型”旁边，选择“Windows/MAC OS X”，然后单击“确定”。

配置 **Intranet** 应用程序

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“Citrix Gateway”>“资源”，然后单击“Intranet 应用程序”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“名称”中，键入应用程序的名称。
4. 点击透明。
5. 在协议中，选择 TCP、UDP 或任意。
6. 在“目标类型”中，选择“IP 地址和网络掩码”。例如，键入 172.16.100.0，子网掩码 255.255.255.0 以表示 172.16.100.x 子网上的所有服务器。Web Interface、Citrix Virtual Apps 和用户连接的所有其他服务器的 IP 地址必须位于定义为 Intranet 应用程序的子网之一中。

   创建 Intranet 应用程序后，您可以将其全局绑定或绑定到虚拟服务器。
7. 在“IP 地址和 NetMask”中，键入代表内部网络的 IP 地址和子网掩码，单击“创建”，然后单击“关闭”。

   创建 Intranet 应用程序后，您可以将其全局绑定或绑定到虚拟服务器。

全局绑定 **Intranet** 应用程序

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“全局设置”。
2. 在详细信息窗格中的 Intranet 应用程序下，单击针对适用于 Java 的 Citrix Gateway 插件的安全网络中的 TCP 应用程序创建映射。
3. 在配置 VPN Intranet 应用程序对话框中，单击添加。
4. 在“可用”下，选择一个或多个 Intranet 应用程序，单击箭头将 Intranet 应用程序移动到已配置，然后单击“确定”。

将 **Intranet** 应用程序绑定到虚拟服务器

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，选择虚拟服务器，然后单击“打开”。
3. 在配置 Citrix Gateway 虚拟服务器对话框中，单击 Intranet 应用程序选项卡。
4. 在“可用应用程序名称”下，选择 Intranet 应用程序，单击“添加”，然后单击“确定”。

用户使用 Citrix Gateway 插件登录时，将建立 VPN 隧道，并将 Receiver 或 Web Interface 用作主页。

配置 SmartAccess

April 6, 2020

可以将 SmartAccess 与 Citrix Virtual Apps and Desktops 结合使用，以智能方式向用户交付已发布的应用程序和虚拟桌面。

SmartAccess 允许您通过使用 Citrix Gateway 会话策略控制对服务器上已发布应用程序和桌面的访问。您可以使用预身份验证和身份验证后检查以及其他条件来访问已发布资源。其他条件包括可以使用 Citrix Virtual Apps and Desktops 策略控制的任何内容，例如打印机带宽限制、用户设备驱动器映射、剪贴板、音频和打印机映射。可以根据用户是否通过 Citrix Gateway 检查来应用 Citrix Virtual Apps and Desktops 策略。

Citrix Gateway 可以使用与 Web Interface 、ICA 代理访问、无客户端访问和 Citrix Gateway 访问相同的选项来交付 Citrix Virtual Desktops。

通过将 Citrix Gateway 组件与 Web Interface、Citrix Virtual Apps and Desktops 集成来实现此功能。此集成为 Web Interface 提供了高级身份验证和访问控制选项。有关详细信息，请参阅 Citrix eDocs 库中“技术”节点中的 Web Interface 文档。

远程连接到服务器场不需要 Citrix Gateway 插件。用户可以使用 Citrix Workspace 应用程序进行连接。用户可以使用 Citrix Gateway 插件登录并通过访问界面（Citrix Gateway 的默认主页）接收已发布的应用程序和虚拟桌面。

SmartAccess 如何适用于 Citrix Virtual Apps and Desktops

April 6, 2020

要配置 SmartAccess，您需要在 Web Interface 上配置 Citrix Gateway 设置，并在 Citrix Gateway 上配置会话策略。运行已发布应用程序向导时，可以选择为 SmartAccess 创建的会话策略。

配置 SmartAccess 后，该功能的工作原理如下：

1. 当用户在 Web 浏览器中键入虚拟服务器的 Web 地址时，您配置的任何预身份验证策略都会下载到用户设备。
2. Citrix Gateway 将预身份验证和会话策略名称作为筛选器发送到 Web Interface。如果策略条件设置为 true，则始终以筛选器名称发送策略。如果未满足策略条件，则不会发送筛选器名称。这样，您就可以根据端点分析的结果区分已发布的应用程序和桌面列表以及运行 Citrix Virtual Apps and Desktops 的计算机上的有效策略。
3. Web Interface 与 Citrix Virtual Apps and Desktops 服务器联系，并将已发布的资源列表返回给用户。除非满足筛选条件，否则应用过滤器的任何资源都不会显示在用户列表中。

您可以在 Citrix Gateway 上配置 SmartAccess 端点分析。要配置终端分析，请创建启用 ICA 代理设置的会话策略，然后配置客户端安全字符串。

当用户登录时，终端分析策略会使用您在 Citrix Gateway 上配置的客户端安全字符串对用户设备进行安全检查。

例如，您要检查 Sophos 防病毒软件的特定版本。在表达式编辑器中，客户端安全字符串显示为：


```
client.application.av(sophos).version == 10.0.2
<!--NeedCopy-->
```

配置会话策略后，将其绑定到用户、组或虚拟服务器。当用户登录时，SmartAccess 策略检查将启动并验证用户设备是否安装了 10.0.2 版或更高版本的 Sophos 防病毒软件。

当 SmartAccess 端点分析检查成功时，Web Interface 门户将显示在无客户端会话的情况下；否则，将显示访问接口。

当您为 SmartAccess 创建会话策略时，会话配置文件没有配置任何设置，这将创建一个空配置文件。在这种情况下，Citrix Gateway 使用为 SmartAccess 全局配置的 Web Interface URL。

配置 **Citrix Virtual Apps** 策略和过滤器

April 6, 2020

在 Citrix Gateway 上创建会话策略后，您可以在运行 Citrix Virtual Apps 的计算机上配置根据端点分析配置应用于用户的策略和过滤器。

配置 **Citrix XenApp 6.5** 策略和筛选器的步骤

1. 在运行 Citrix Virtual Apps 的服务器上，单击 “开始”>“管理工具”>“Citrix Virtual Apps”。如果出现提示，请配置并运行发现。
2. 在左侧窗格中，展开 “Citrix ADC 资源”>“Citrix Virtual Apps”>“farmName”，其中 farmName 为服务器场的名称。
3. 点击应用程序。
4. 在中心窗格中，右键单击应用程序，然后单击应用程序属性。
5. 在导航窗格的 “属性” 下，单击 “高级”>“访问控制”。
6. 在右窗格中，单击符合以下任何筛选器的任何连接，然后单击添加。
7. 在 Access Gateway 场中，键入 Citrix Gateway 虚拟服务器的名称。
8. 在 Access Gateway 筛选器中，键入端点会话策略的名称，然后单击 “确定”。
9. 在 “应用程序属性” 对话框中，清除 “允许所有其他连接”，然后单击 “确定”。

为 **SmartAccess** 配置会话策略的步骤

April 6, 2020

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格的 “策略” 选项卡上，单击 “添加”。
3. 在 “创建会话策略” 对话框的 “名称” 中，键入策略的名称，如 ValidEndpoint。

4. 在“请求配置文件”中，单击“新建”，并在“名称”中键入配置文件的名称，如“空”，然后单击“创建”。
5. 在“创建会话策略”对话框中，创建客户端安全表达式，单击“创建”，然后单击“关闭”。

客户端安全表达式用于区分有效和无效终端。您可以根据终端分析的结果提供对已发布应用程序或桌面的不同级别的访问权限。

创建会话策略后，请将其全局绑定或绑定到虚拟服务器。

在 **Citrix Virtual Apps** 上配置用户设备映射

April 6, 2020

可以使用应用于运行 Citrix Virtual Apps 的计算机上的策略的 Citrix Gateway 过滤器。过滤器允许用户访问 Citrix Virtual Apps 功能，例如基于端点分析结果的用户设备驱动器映射、打印机映射或剪贴板映射。

Citrix Workspace 应用程序支持在用户设备上映射设备，以便用户可以访问用户会话中的外部设备。用户设备映射提供：

- 访问本地驱动器和端口
- 用户会话和本地剪贴板之间的剪切和粘贴数据传输
- 从用户会话播放音频（系统声音和.wav 文件）

在登录期间，用户设备将可用的用户驱动器和 COM 端口通知服务器。在 Citrix XenApp 6.5 中，用户驱动器映射到服务器并使用用户设备驱动器号。这些映射仅在当前会话期间对当前用户可用。当用户注销时，映射将被删除，并在用户下次登录时重新创建。

启用 XML 服务后，您需要为用户设备映射配置策略。

若要强制基于 SmartAccess 筛选器的用户设备映射策略，请在服务器上创建以下两个策略：

- 禁用用户设备映射并应用于所有 Citrix Gateway 用户的限制性 ICA 策略。
- 启用用户设备映射并仅适用于满足终端分析会话策略的用户的完整 ICA 策略
  注意：筛选的非限制性 ICA 策略的优先级必须高于限制性 ICA 策略，以便在应用于用户时，非限制性策略将覆盖禁用用户设备映射的策略。

您可以使用 Citrix AppCenter 在 Citrix XenApp 6.5 上配置限制性和非限制性策略。

在 **Citrix XenApp 6.5** 上配置限制性策略

April 6, 2020

1. 单击“开始”>“管理工具”>“管理控制台”>“Citrix AppCenter”。
2. 在左窗格中，展开 Citrix Virtual Apps，展开服务器，然后单击“策略”。
3. 在策略窗格中，单击用户选项卡，然后单击新建。

4. 在“名称”中，键入策略的名称，然后单击“下一步”。
5. 在“类别”下，单击“所有设置”。
6. 在“设置”下的“自动连接客户端驱动器”中，单击“添加”。
7. 在添加设置对话框中，单击禁用，单击确定，然后单击下一步。
8. 在“类别”下，单击“所有筛选器”。
9. 在“筛选器”下的“访问控制”中，单击“添加”。
10. 在“新建筛选器”对话框中，单击“添加”。
11. 在模式下，单击拒绝。
12. 在“连接类型”中，选择“使用 Access Gateway”。
13. 在 AG 场中，键入虚拟服务器名称。
14. 在“访问条件”中，键入或选择在 Citrix Gateway 上配置的会话策略名称，单击“确定”两次，单击“下一步”，然后单击“创建”以完成向导。

在 **Citrix XenApp 6.5** 上配置非限制性策略

April 6, 2020

1. 单击“开始”>“管理工具”>“管理控制台”>“Citrix AppCenter”。
2. 在左窗格中，展开 Citrix Virtual Apps，展开服务器，然后单击“策略”。
3. 在策略窗格中，单击用户选项卡，然后单击新建。
4. 在“名称”中，键入策略的名称，然后单击“下一步”。
5. 在“类别”下，单击“所有设置”。
6. 在“设置”下的“自动连接客户端驱动器”中，单击“添加”。
7. 单击已启用，单击确定，然后单击下一步。
8. 在“类别”下，单击“所有筛选器”。
9. 在“筛选器”下的“访问控制”中，单击“添加”。
10. 在“新建筛选器”对话框中，单击“添加”。
11. 在模式下，单击允许。
12. 在“连接类型”中，选择“使用 Access Gateway”。
13. 在 AG 场中，键入虚拟服务器名称。
14. 在“访问条件”中，键入或选择在 Citrix Gateway 上配置的会话策略名称，单击“确定”两次，单击“下一步”，然后单击“创建”以完成向导。

将 **Citrix Virtual Apps** 作为隔离访问方法启用

April 6, 2020

如果您在 Citrix Gateway 上配置了终端分析，则通过终端节点扫描的用户可以访问您在 Citrix Gateway 上配置的所

有资源。您可以将终端节点扫描失败的用户放在隔离组中。这些用户只能从 Citrix Virtual Apps 访问已发布的应用程序。终端分析扫描的成功或失败决定了用户可用的访问方法。

例如，创建端点分析扫描以检查用户登录时是否在用户设备上运行记事本。如果记事本正在运行，用户可以使用 Citrix Gateway 插件登录。如果记事本未运行，则用户将仅收到已发布应用程序的列表。

要配置受限用户访问，请在 Citrix Gateway 上创建隔离组。在会话配置文件中创建隔离组，然后将配置文件添加到会话策略。

为隔离组创建会话策略和终端分析扫描

April 6, 2020

要将 Citrix Virtual Apps 作为隔离访问方法启用，请在 Citrix Gateway 上创建一个用作隔离组的组。然后，创建一个会话策略，您可以在其中选择该组。

创建会话策略后，将策略绑定到隔离组。配置策略并将其绑定到组后，测试结果。例如，要使用户成功登录，记事本必须在用户设备上运行。如果记事本正在运行，用户可以使用 Citrix Gateway 插件登录。如果记事本未运行，用户可以使用 Citrix Workspace 应用登录。

有关配置终端分析策略的更多信息，请参阅配置终端策略。

创建终端分析扫描并添加隔离组

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“创建会话策略”对话框的“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“创建会话配置文件”对话框的“名称”中，键入配置文件的名称。
6. 在“安全”选项卡上，单击“高级”。
7. 在“安全设置-高级”对话框的“客户端安全”下，单击“覆盖全局”，然后单击“新建”。
8. 在“创建表达式”对话框中，在“匹配任何表达式”旁边，单击“添加”。
9. 在“表达式类型”中，选择“客户端安全”。
10. 在“组件”中，选择“处理”。
11. 在名称中键入记事本.exe，单击确定，然后单击创建。
12. 在“安全设置-高级”对话框的“隔离组”中，选择隔离组，单击“创建”，单击“确定”，然后单击“创建”。
13. 在“创建会话策略”对话框的命名表达式旁边，选择“True”值，单击“添加表达式”，单击“创建”，然后单击“关闭”。

为 **SmartAccess** 配置 **Citrix Virtual Desktops**

April 6, 2020

Citrix Gateway 使 Citrix Virtual Desktops 能够向远程用户交付安全桌面。Citrix Virtual Desktops 可以使用 Citrix Gateway 的 SmartAccess 功能智能交付桌面。使用 Citrix Virtual Desktops 中的交付服务控制台创建桌面组时，您可以配置用于访问控制的策略和筛选器。

要将 Citrix Gateway 配置为交付已发布的桌面，请使用与 Web Interface 、ICA 代理访问、无客户端访问和 Citrix Gateway 访问相同的选项。

在“已发布应用程序”选项卡上创建会话策略并配置设置时，请使用 Citrix Virtual Desktops Web Interface 站点的 Web 地址。创建策略后，将其绑定到虚拟服务器。然后，创建一个空会话配置文件，您不在其中配置设置。Web Interface 配置是从全局设置继承的。

使用 **Citrix Virtual Desktops** 配置 **SmartAccess** 的会话策略

April 6, 2020

通过创建绑定到虚拟服务器的会话策略，可以在 Citrix Gateway 上配置 SmartAccess 以访问 Citrix Virtual Desktops。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway > 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“创建会话策略”对话框的“名称”中，键入策略的名称，如 Citrix Virtual Desktops 策略。
4. 在请求配置文件中，单击新建。
5. 在“创建会话配置文件”对话框的“名称”中，键入配置文件的名称，如 Citrix Virtual Desktops 配置文件。
6. 在“已发布的应用程序”选项卡上，ICA 代理旁边，单击“覆盖全局”，然后选择“开”。
7. 在 Web Interface 地址中，单击“覆盖全局”，然后键入 Citrix Virtual Desktops Web Interface 站点的 URL。
8. 在单点登录域中，单击覆盖全局，键入域名，然后单击创建。
9. 在“创建会话策略”对话框的命名表达式旁边，选择“真正值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

您还需要创建绑定到虚拟服务器的空会话策略。会话配置文件不包含任何配置，使其成为空配置文件。在会话策略中，添加 True Value 表达式，然后保存策略。

创建两个会话策略后，将两个策略绑定到虚拟服务器。

在 **Citrix Virtual Desktops 5** 中配置策略和筛选器

April 6, 2020

您可以使用桌面 Studio 或组策略编辑器在 Citrix Virtual Desktops 5 中配置设置。在 Citrix Virtual Desktops 中配置 Citrix Gateway 设置时，请使用 Citrix Gateway 虚拟服务器名称和会话策略名称。然后，配置访问控制以允许连接满足定义的筛选条件。您也可以使用 SmartAccess 策略。

1. 在 Citrix Virtual Desktops 服务器上，单击 “开始”>“所有程序”>“Citrix”>“Desktop Studio”。
2. 在左窗格中，单击以展开 HDX 策略，然后单击中间窗格中的用户选项卡。
3. 在 “用户” 下，单击 “新建”。
4. 在 “新建策略” 对话框中，在 “标识您的策略” 下，然后在 “名称” 中键入名称。
5. 点击下一步两次。
6. 在 “新建策略” 对话框中的 “筛选器” 选项卡上的 “筛选器” 下，单击 “访问控制”，然后单击 “添加”。
7. 在 “新建筛选器” 对话框中，单击 “添加”。
8. 在 “新建筛选器元素” 对话框的 “连接类型” 中，选择 “使用 Access Gateway”。

   要将策略应用于通过 Citrix Gateway 建立的连接而不考虑 Citrix Gateway 策略，请将默认条目保留在 AG 服务器场名称和 Access 条件中。
9. 如果要将策略应用于基于现有 Citrix Gateway 策略通过 Citrix Gateway 建立的连接，请执行以下操作：
   a) 在 AG 场名称中，键入虚拟服务器名称。
   b) 在 “访问条件” 中，键入终端分析策略或会话策略的名称。

   > 重要：Citrix Virtual Desktops 不验证 Citrix Gateway 虚拟服务器、终端分析策略或会话策略名称。确保信息正确无误。
10. 单击确定两次，单击下一步，然后单击创建。

将 **Desktop Delivery Controller** 添加为 **STA**

April 6, 2020

要与 Citrix Virtual Desktops 建立 ICA 连接，请将 Desktop Delivery Controller 的 IP 地址作为 Secure Ticket Authority (STA) 添加到虚拟服务器。

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway，然后单击 “虚拟服务器”。
2. 在详细信息窗格中，选择虚拟服务器，然后单击 “打开”。
3. 在 “已发布的应用程序” 选项卡上的 “安全票证颁发机构” 下，单击 “添加”。

4. 在配置 STA 服务器对话框中，输入 STA 服务器的 URL，然后单击创建。
5. 重复步骤 4 添加其他 STA 服务器，然后单击“确定”在“配置 Citrix Gateway 虚拟服务器”对话框中。

配置 **SmartControl**

January 10, 2023

智能控制允许管理员定义精细策略，以配置和强制执行 Citrix Gateway 上的 Citrix Virtual Apps and Desktops 的用户环境属性。智能控制允许管理员从单个位置管理这些策略，而不是在这些服务器类型的每个实例管理这些策略。

智能控制是通过 Citrix Gateway 上的 ICA 策略实现的。每个 ICA 策略都是表达式和访问配置文件组合，可应用于用户、组、虚拟服务器和全局。ICA 策略在用户在会话建立时进行身份验证后进行评估。

下表列出了智能控制可以强制执行的用户环境属性：

| | |
| ——————————————————————————— | ——————————————————————————— |
| ConnectClientDrives | 指定用户登录时与客户端驱动器的默认连接。
|ConnectClientLPTPorts| 指定用户登录时从客户端自动连接 LPT 端口。LPT 端口是本地打印机端口。|
|ClientAudioRedirection| 指定服务器上托管的应用程序，以便通过客户端计算机上安装的声音设备传输音频。|
|ClientClipboardRedirection| 在客户端设备上指定并配置剪贴板访问，并在服务器上映射剪贴板。|
|ClientCOMPortRedirection| 指定到客户端和从客户端的 COM 端口重定向。COM 端口是通信端口。这些是串行端口。|
|ClientDriveRedirection| 指定到客户端和从客户端的驱动器重定向。|
| 多流 | 指定指定用户的多流功能。|
|ClientUSBDeviceRedirection| 指定 USB 设备与客户端之间的重定向（仅限工作站主机）。|
| 本地远程数据 | 指定 Citrix Workspace 应用程序的 HTML5 文件上传下载功能。|
|ClientPrinterRedirection| 指定用户登录到会话时要映射到服务器的客户端打印机。|
| 策略 | 操作 | 访问配置文件 |
| 添加 | 编辑 | 删除 | |
显示绑定 | 策略管理器 | 操作 |

策略

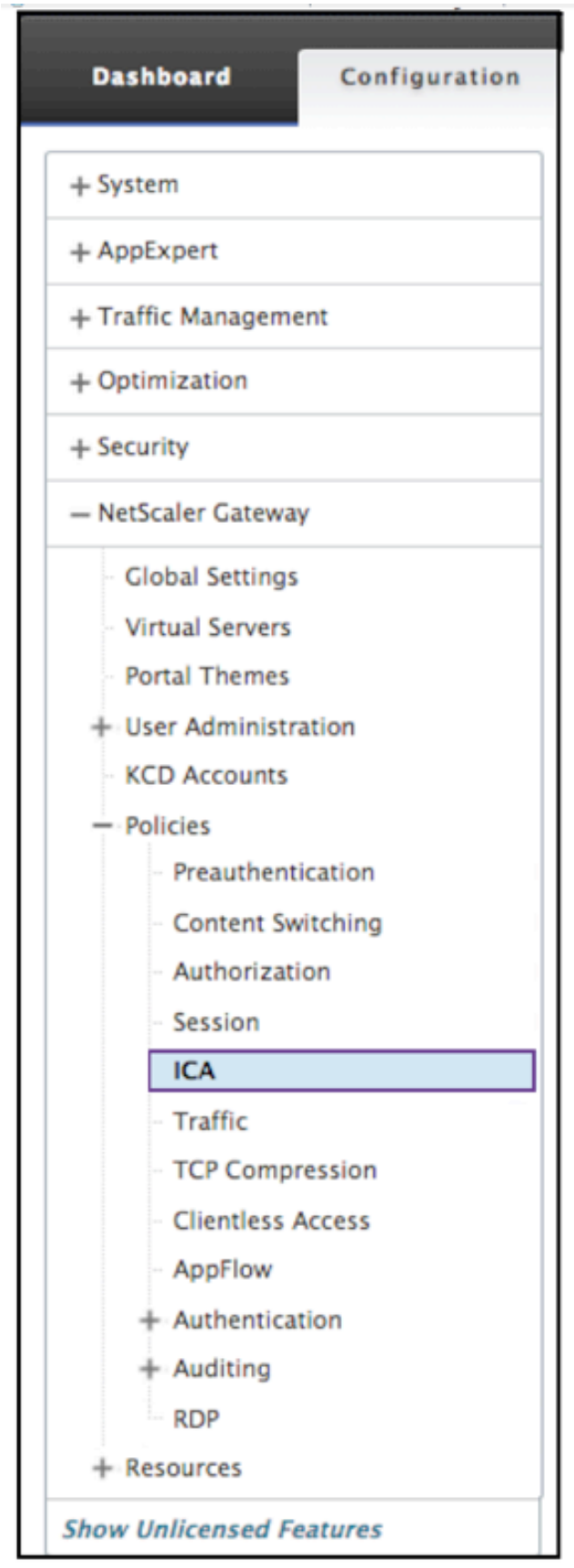
ICA 策略指定操作、访问配置文件、表达式以及可选的日志操作。以下命令可从“策略”选项卡中获得：

- 添加
- 编辑
- 删除
- 显示绑定

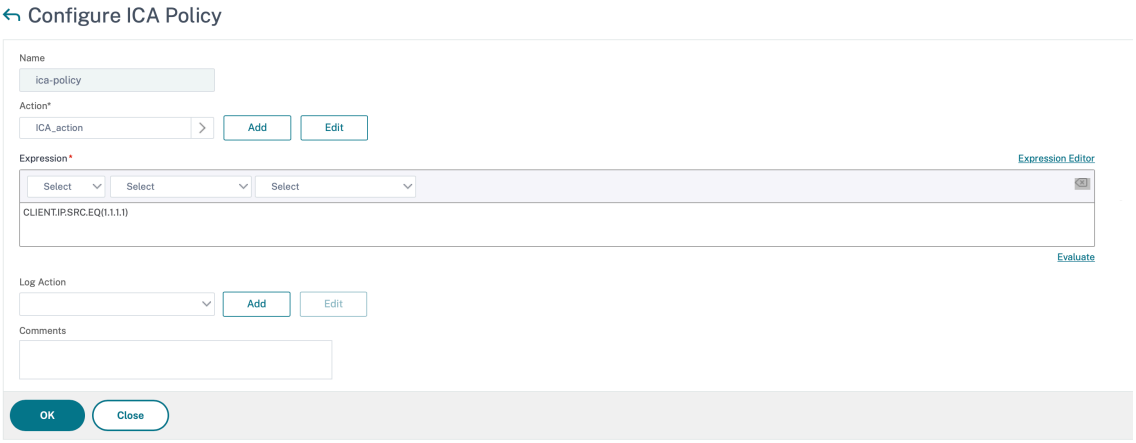
- 策略管理器
- 操作

添加

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”，然后单击 “ICA”。



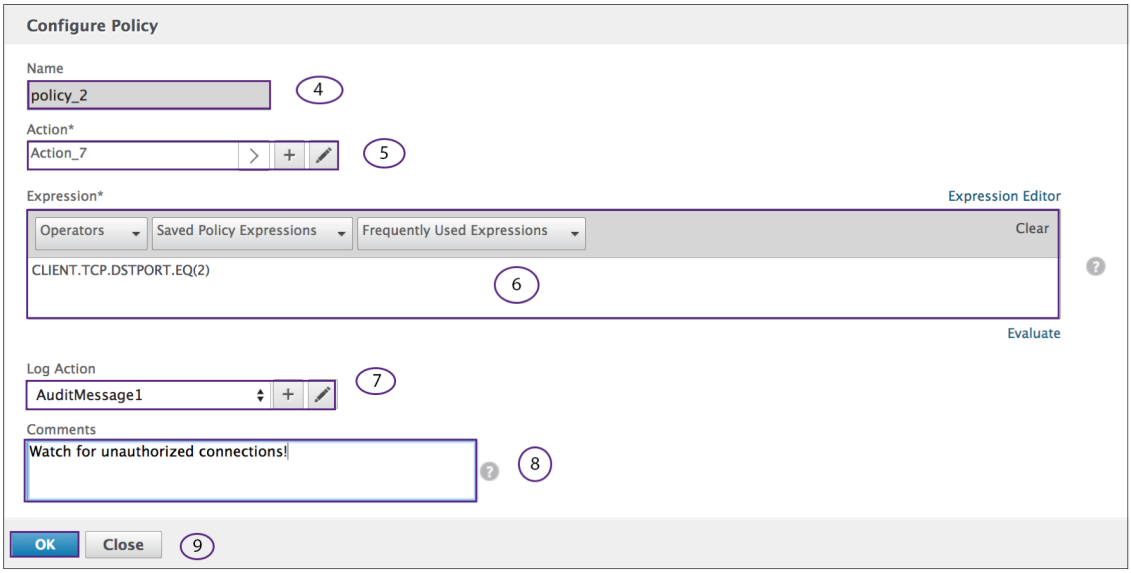
2. 在详细信息窗格的 “策略” 选项卡上，单击 “添加”。
3. 此时将显示以下屏幕。在 “名 称” 对话框中，键入策略的名称。这是必填字段。所有必填字段均以星号表示。



4. 在操作旁边执行以下操作之一：
   - 单击 **>** 图标以选择现有操作。有关详细信息，请参阅 [选择一个操作] 下 (#common-进程)。
   - 单击 **+** 图标以创建新动作。有关详细信息，请参阅 [创建新操作] 下 (#common-进程)。
   - 铅笔图标处于禁用状态。
5. 创建表达式。
6. 创建 日志操作。欲了解更多详情，请参阅创建日志操作。
7. 在注释框中输入一条消息。注释写入消息日志。此字段是可选的。
8. 单击创建。

编辑

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”，然后单击 “ICA”。
2. 从列表中选择 ICA 策略。
3. 在详细信息窗格的 “策略” 选项卡上，单击 “编辑”。
4. 验证策略名称。



5. 要修订该 行动，请执行以下操作之一：
   - 单击 **>** 图标以修改现有 操作。有关详细信息，请参阅 [选择一个操作] 下 (#common-进程)。
   - 单击 **+** 以创建新 动作图标。有关详细信息，请参阅 [创建新操作] 下 (#common-进程)。
   - 单击 铅笔图标以修改 [访问配置文件] 。
6. 根据需要修改 表达式。有关详细信息，请参阅 [表达式] 下 (#common-进程)。
7. 要修改 日志操作，请执行以下操作之一：
   - 单击 + 以创建新的 日志操作。
   - 单击 铅笔图标以配置审核消息。
8. 根据需要修改评论。
9. 单击确定。

删除

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”，然后单击 “ICA”。
2. 从列表中选择所需的 ICA 策略。
3. 在详细信息窗格的 “策略” 选项卡上，单击 “删除”。
4. 单击 “是”，确认您要删除策略。

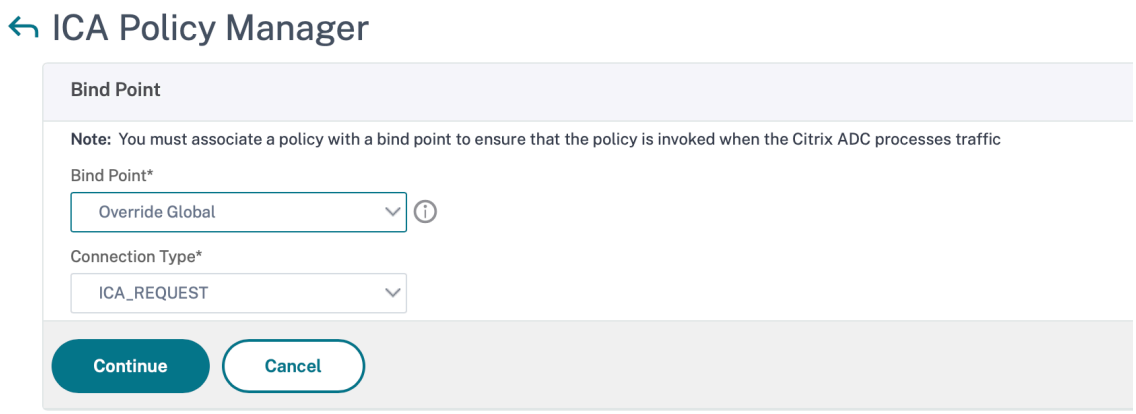
显示绑定

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”，然后单击 “ICA”。
2. 从列表中选择 ICA 策略。

3. 在详细信息窗格的“策略”选项卡上，单击“显示绑定”。

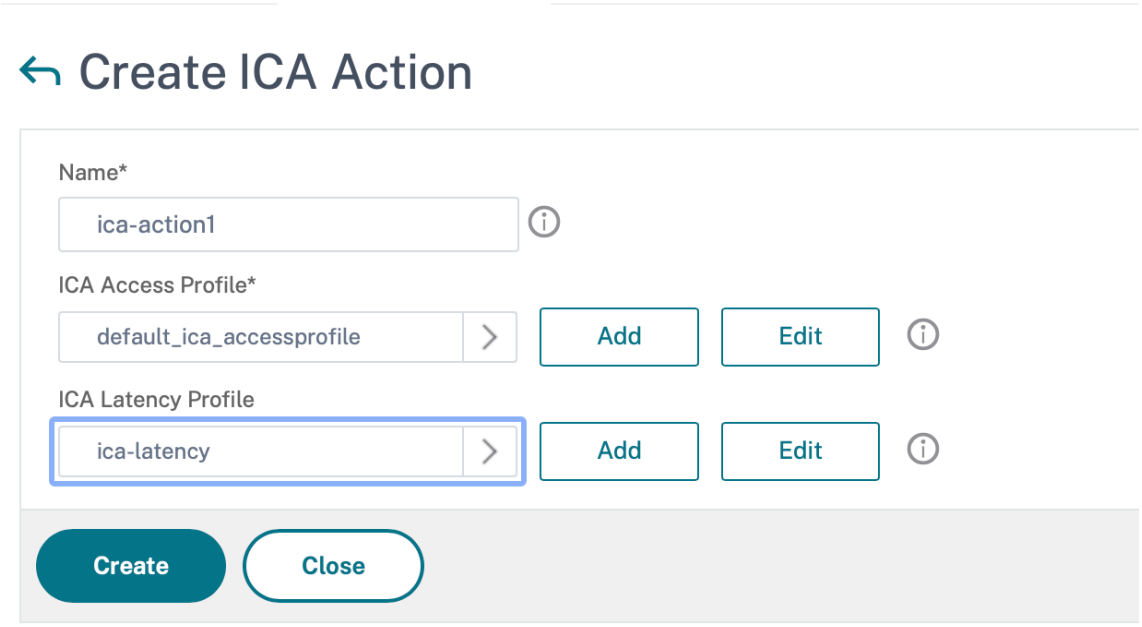
策略管理器

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“Citrix Gateway”>“策略”，然后单击“ICA”。
2. 从列表中选择所需的 ICA 策略。
3. 在详细信息窗格的“策略”选项卡上，单击“策略管理器”
4. 从“绑定点”对话框中，从下拉菜单中选择一个策略。以下是以下选项：
   - 覆盖全局
   - VPN 虚拟服务器
   - 缓存重定向虚拟服务器
   - 默认全局
5. 从“连接类型”对话框中，从下拉菜单中选择绑定策略。
6. 如果选择 VPN 虚拟服务器或缓存重定向虚拟服务器，则使用下拉框连接到服务器。
7. 单击 继续。



添加装订

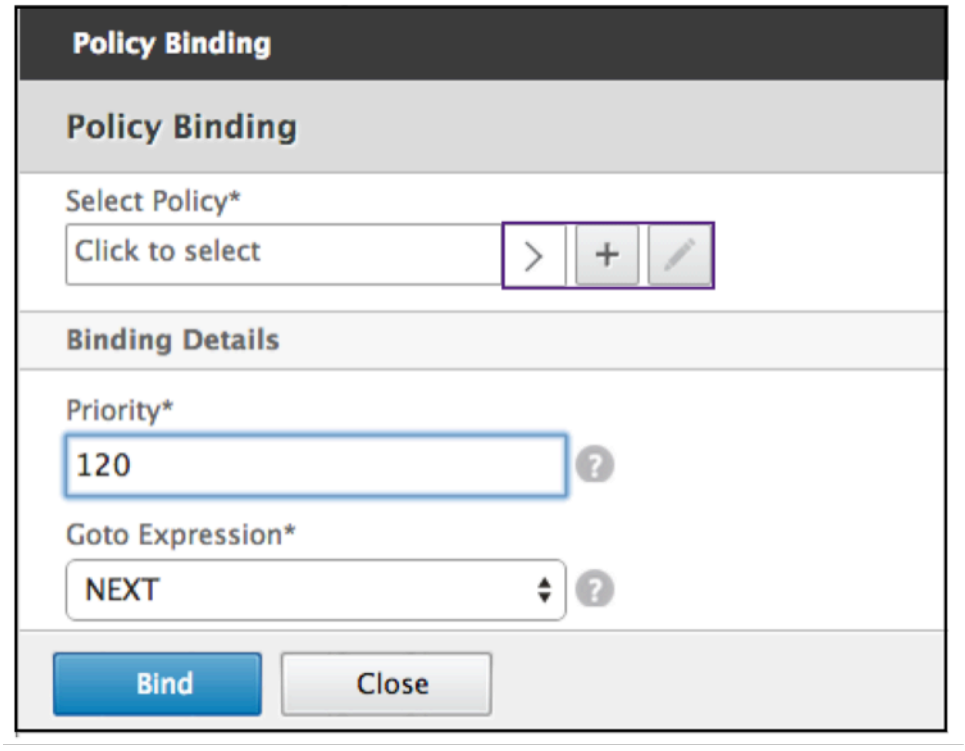
1. 选择“继续”后，将显示此屏幕。
2. 选择要附加绑定的策略。
3. 选择添加装订。



策略绑定

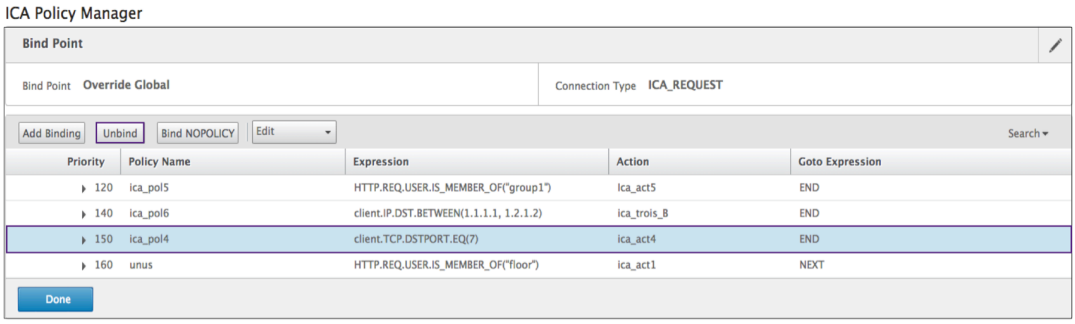
1. 选择完成后，将显示此屏幕。

- 单击 **>** 图标以选择现有策略。详情请参阅选择现有策略。
- 单击 **+** con 以创建新策略。详情请参阅创建新策略。



取消绑定策略

1. 选择要取消绑定的策略，然后单击“取消绑定”按钮。



2. 点击 完成
3. 单击弹出屏幕上的“是”按钮以确认您希望取消绑定所选实体。

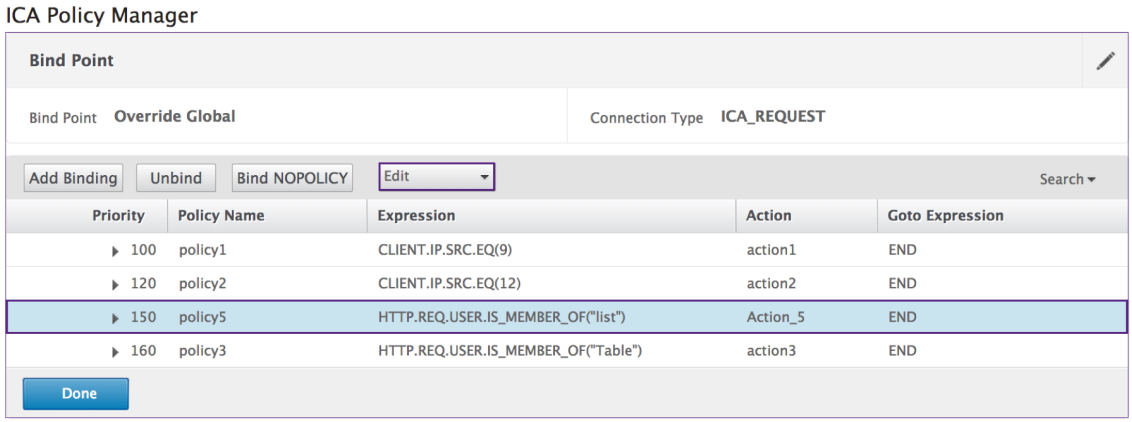
绑定国家保护机制

1. 选择需要 NOPICS 的策略，然后单击 绑定 **NOPICS** 按钮。
2. 点击 完成

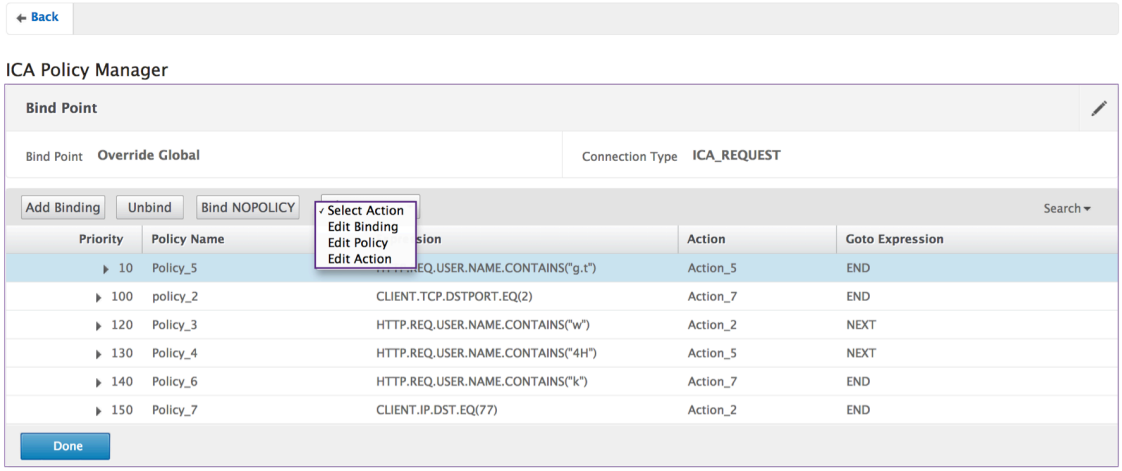
编辑

您可以从 ICA 策略管理器进行编辑。

1. 选择要编辑的策略，然后选择 编辑。



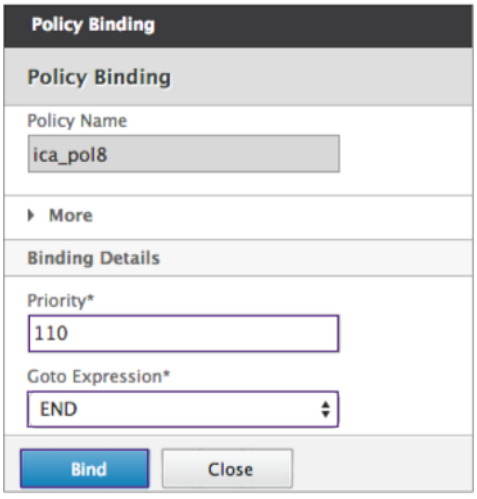
2. 您可以选择进行以下编辑：** 编辑绑定 **，编辑策略 **[[]]**、编辑操作 **[]**。



有关更多信息 **[编辑绑定]，请参阅 []、[]。**

编辑绑定

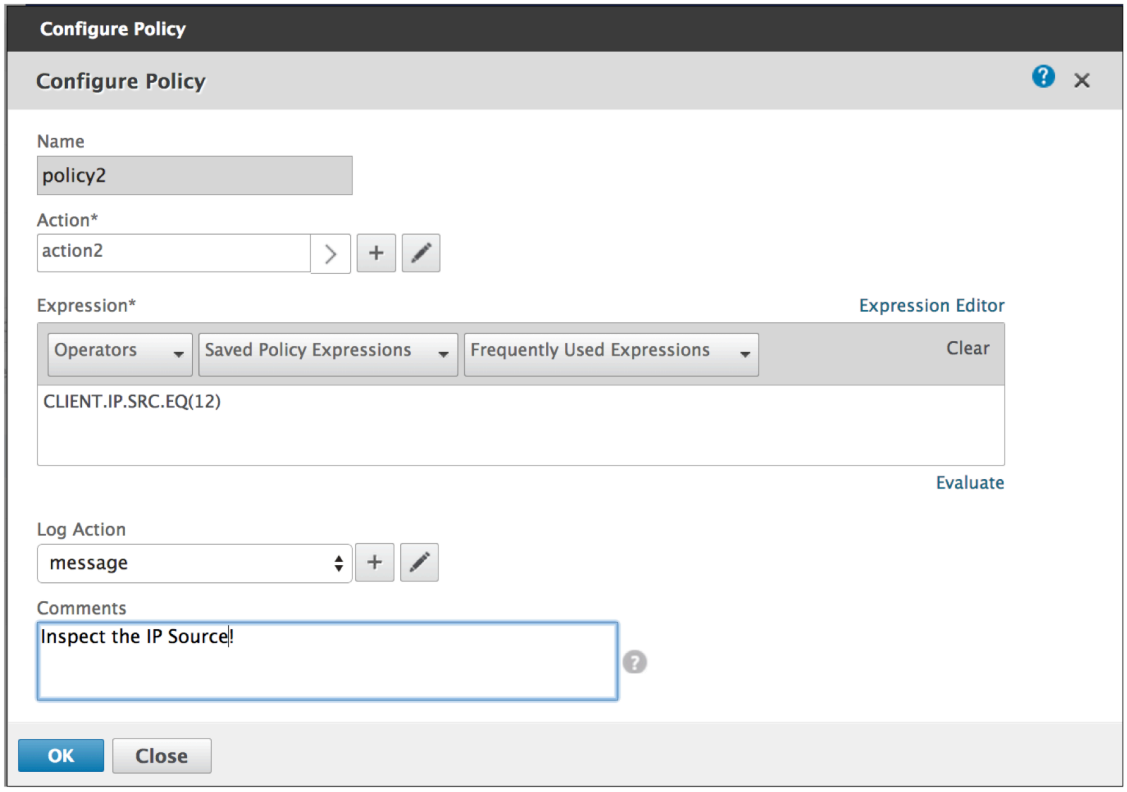
1. 选择策略后，单击 编辑绑定。
2. 验证您正在编辑所需的策略。此策略名称不可编辑。



3. 根据需要设置优先级。
4. 根据需要设置转到表达式。
5. 点击 绑定按钮。

编辑策略

1. 选择策略后，单击 编辑策略。
2. 验证策略名称以确保您正在编辑所需的策略。此字段不可编辑。



3. 要修改“操作”策略，请执行以下操作之一：

   - 单击 **>** 图标以选择现有操作。有关详细信息，请参阅 [选择一个操作] 下 (#common-进程)。
   - 单击 **+** 图标以创建动作。有关详细信息，请参阅 [创建新操作] 下 (#common-进程)。
   - 单击 铅笔图标以修改访问配置文件。有关详细信息，请参阅 [选择现有访问配置文件] 下 (#common-进程)。

4. 根据需要修改表达式。有关更多详细信息，请参阅 [表达式] 下 (#common-进程)。
5. 从下拉菜单中选择所需的消息类型。要创建日志操作，请执行以下操作之一：

   - 单击 **+** 图标以创建动作。详情请参阅创建日志操作。
   - 单击 铅笔图标以修改配置审核消息操作。详情请参阅配置审核消息操作。

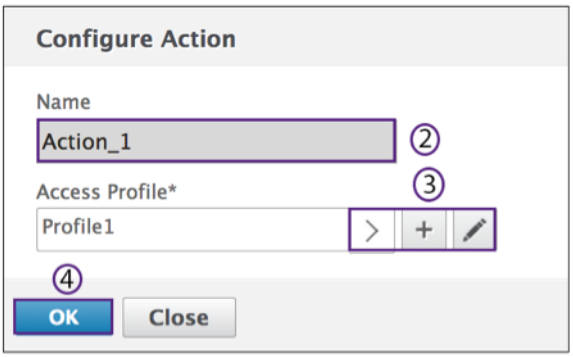
6. 输入有关 ICA 策略的注释。
7. 编辑完成后，单击 **“确定”**。

编辑操作

1. 选择策略后，单击 编辑操作。
2. 验证操作名称以确认您正在编辑所需操作。此字段不可编辑。
3. 在访问配置文件旁边执行以下操作之一：

- 单击 **>** 图标以选择其他访问配置文件。详情请参阅配置操作。
- 单击 **+** 图标以选择新的频道配置文件。创建访问配置文件 #creating-an-access-profile-with-the-configuration-utility[()]。
- 单击 铅笔图标以修改访问配置文件。有关详细信息，请参阅 [选择现有访问配置文件] 下 (#common-进程)。

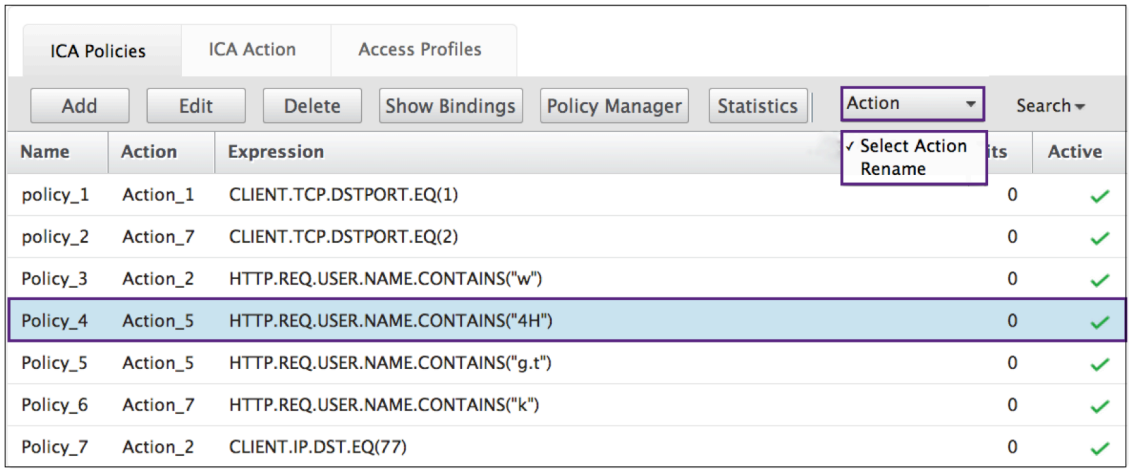
4. 单击确定。



操作

策略 > 操作命令用于重命名操作。

1. 从列表中选择所需的 ICA 操作。
2. 在 ICA 策略选项卡上，单击操作。从下拉菜单中选择重命名。



3. 重命名操作。
4. 单击 **OK**（确定）

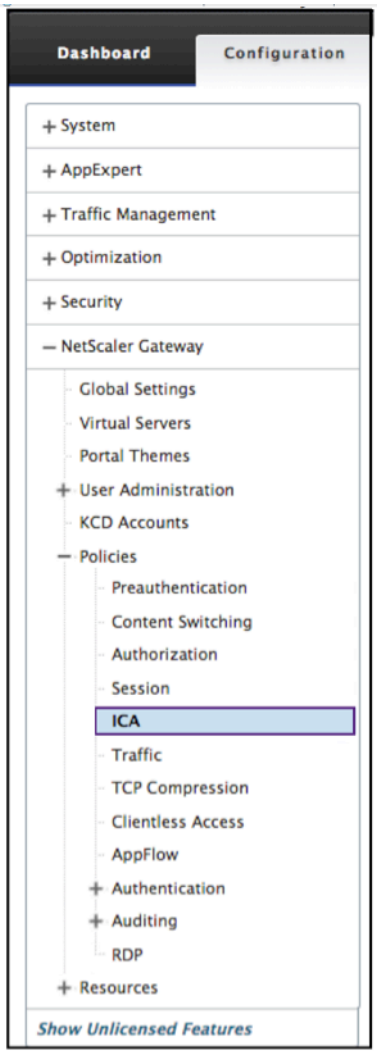
操作

操作将策略与访问配置文件相连接。以下命令可从“策略”选项卡中获得：

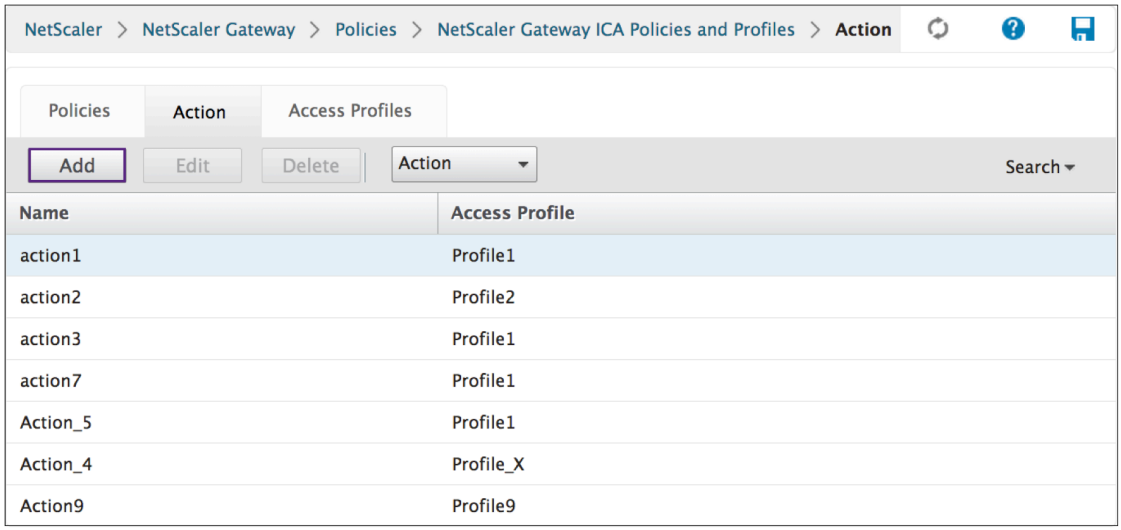
- 添加
- 编辑
- 删除
- 操作

添加

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“Citrix Gateway”>“策略”，然后单击“ICA”。

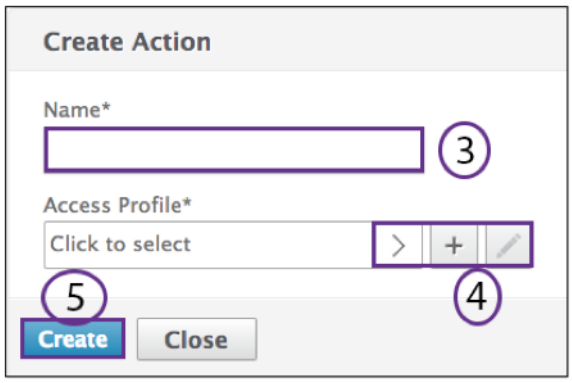


2. 在详细信息窗格中的“操作”选项卡上，单击“添加”。



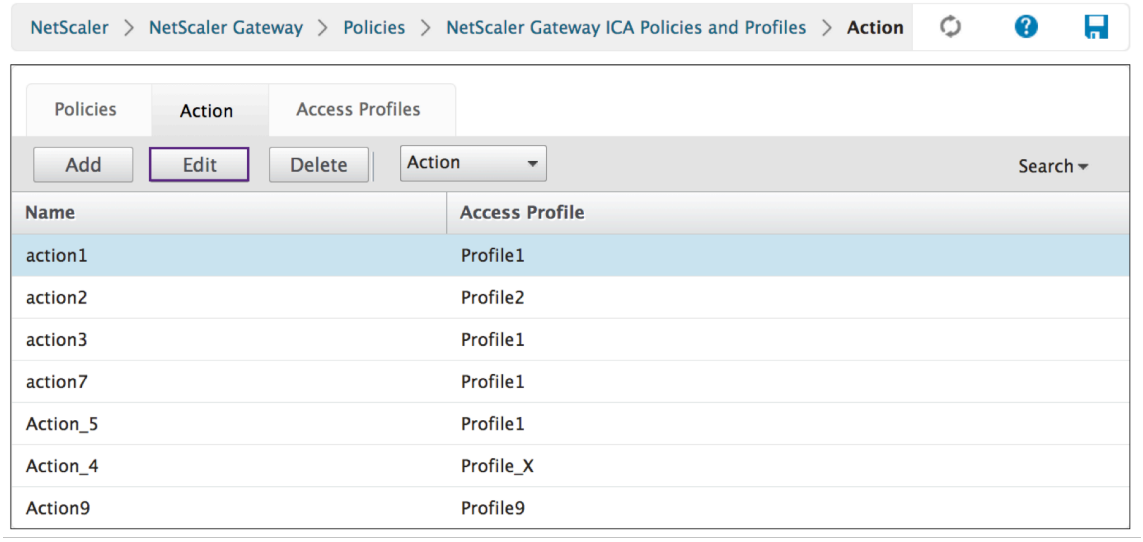
- 单击 **>** 图标以选择现有的访问配置文件。有关详细信息，请参阅 [选择现有访问配置文件] 下 (#common-进程)。
- 单击 **+** 图标以创建新的访问配置文件。详情请参阅创建访问配置文件。。
- 此屏幕禁用 铅笔图标。

3. 单击创建。



编辑

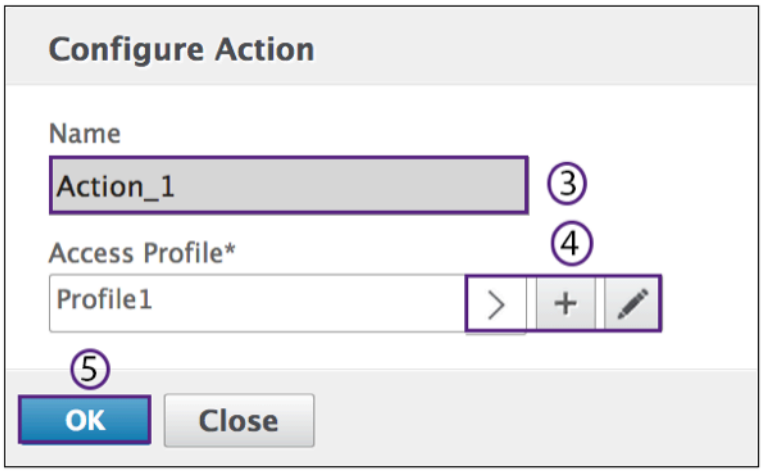
1. 从列表中选择所需的 ICA 策略。



2. 在详细信息窗格中的“操作”选项卡上，单击“编辑”。

配置操作

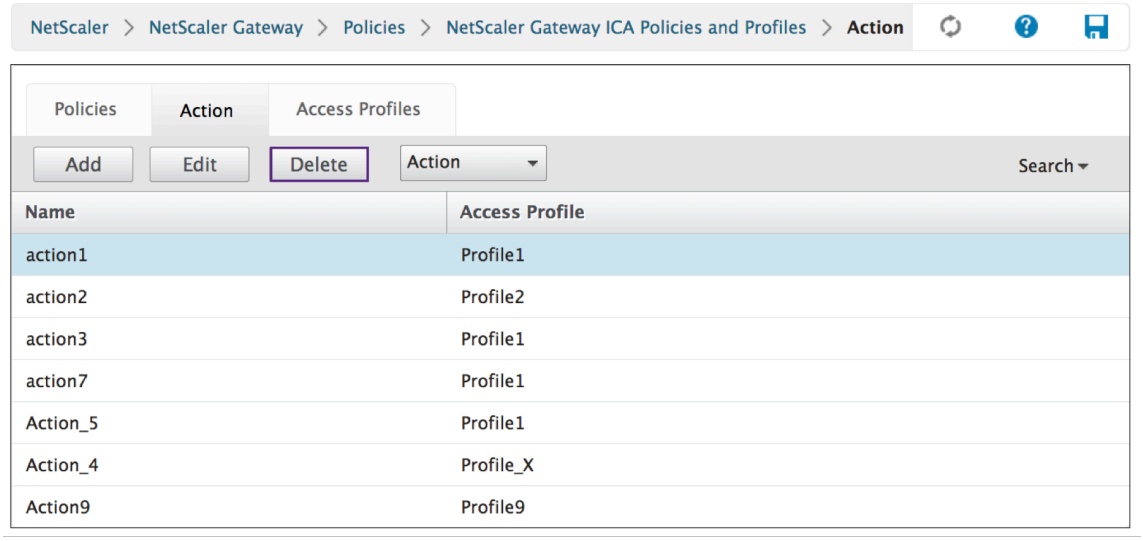
1. 验证操作名称以确认您正在编辑所需操作。此字段不可编辑。
2. 在访问配置文件旁边执行以下操作之一：
   - 单击 **>** 以选择现有访问配置文件。有关详细信息，请参阅 [选择现有访问配置文件] 下 (#common-进程)。
   - 单击 **+** 以创建新的访问配置文件。详情请参阅创建访问配置文件。
   - 单击 铅笔图标以配置访问配置文件 。
3. 单击确定。



删除

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“Citrix Gateway”>“操作”，然后单击“ICA”。

2. 从列表中选择所需的 ICA 操作。
3. 在详细信息窗格中的 “操作” 选项卡上，单击 “删除”。

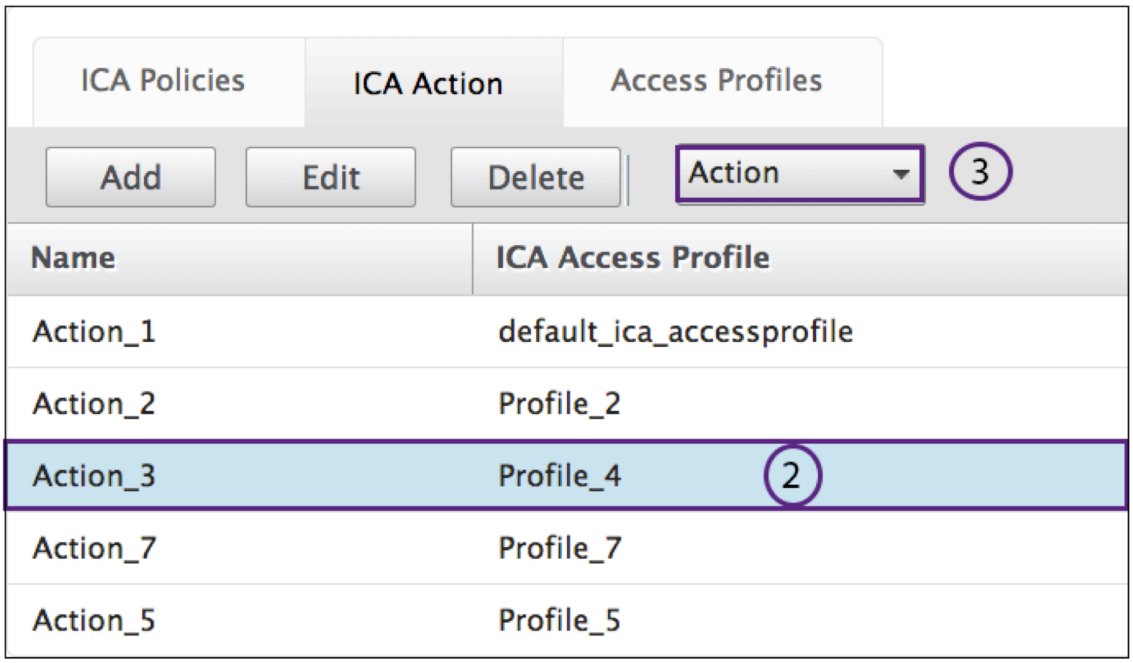


4. 单击 “是”，确认要删除策略的操作。

操作

ICA 操作 > 操作命令用于重命名操作。

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“操作”，然后单击 “ICA”。
2. 从列表中选择所需的 ICA 操作。
3. 在详细信息窗格中的 “操作” 选项卡上，单击 “操作”。



4. 从下拉菜单中选择 “操作”>“重命名”。
5. 重命名操作。
6. 单击 **OK**（确定）

访问配置文件

ICA 配置文件定义用户连接的设置。

访问配置文件指定在用户设备满足策略表达式条件时应用于用户的 Citrix Virtual Apps and Desktops 环境 ICA 的操作。您可以使用配置实用程序独立于 ICA 策略创建 ICA 配置文件，然后将该配置文件用于多个策略。您只能将一个配置文件与策略结合使用。

您可以独立于 ICA 策略创建访问配置文件。创建策略时，您可以选择要附加到策略的 Access 配置文件。访问配置文件指定用户可用的资源。以下命令可从 “策略” 选项卡中获得：

- 添加
- 编辑
- 删除

使用配置实用程序创建访问配置文件

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”，然后单击 “ICA”。
2. 在详细信息窗格中，单击访问配置文件选项卡，然后单击添加。
3. 配置配置文件的设置，单击创建，然后单击关闭。创建配置文件后，您可以将其包含在 ICA 策略中。

使用配置实用程序将访问配置文件添加到策略

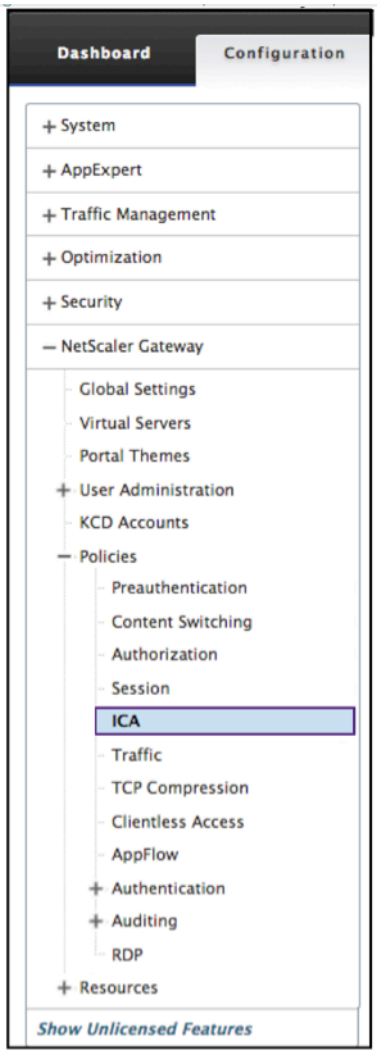
1. 在配置实用程序中的导航窗格中，展开 “Citrix Gateway”>“策略”，然后单击 “ICA”。
2. 在 “策略” 选项卡上，执行以下操作之一：
   - 单击添加以创建新的 ICA 策略。
   - 选择一个策略，然后单击打开。
3. 在 “操作” 菜单中，从列表中选择访问配置文件。
4. 完成 ICA 策略的配置，然后执行以下操作之一：

   a. 单击创建，然后单击关闭以创建策略。

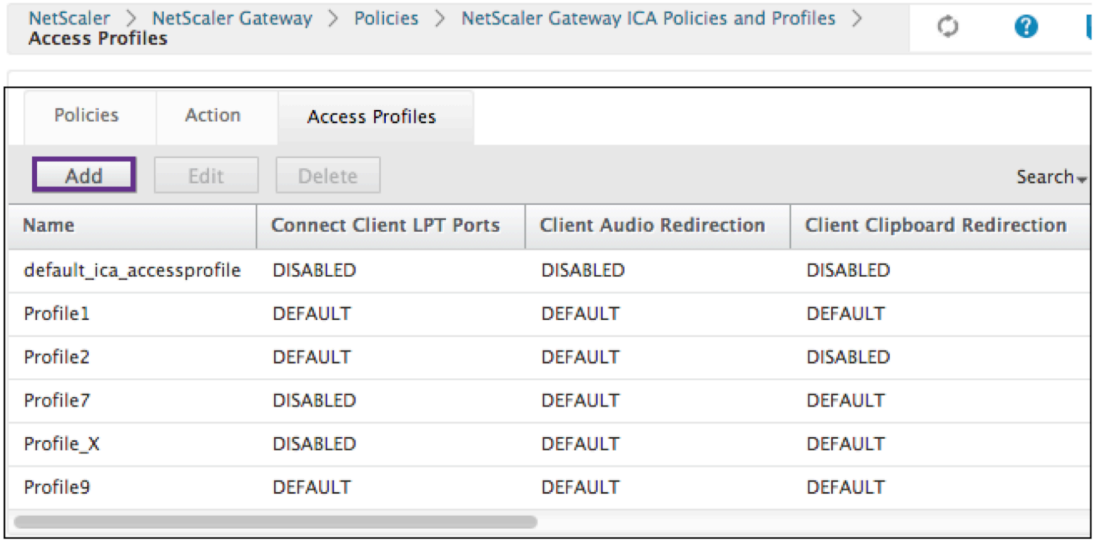
   b. 单击确定，然后单击关闭以修改策略。

添加

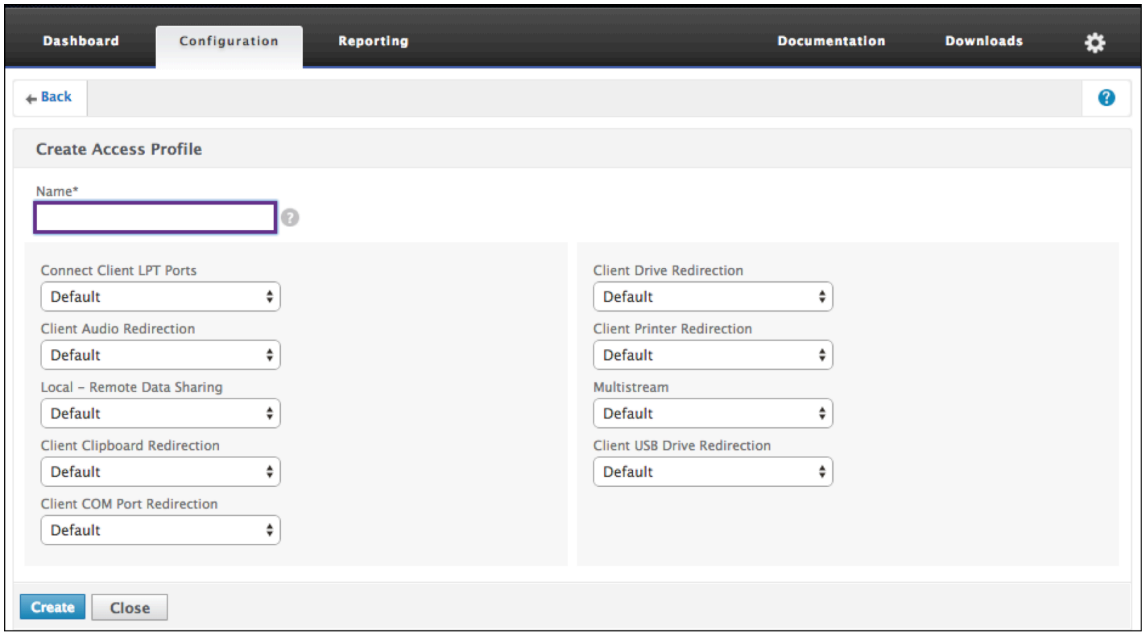
1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“策略”，然后单击 “ICA”。



2. 在详细信息窗格中的访问配置文件选项卡上，单击 添加。**



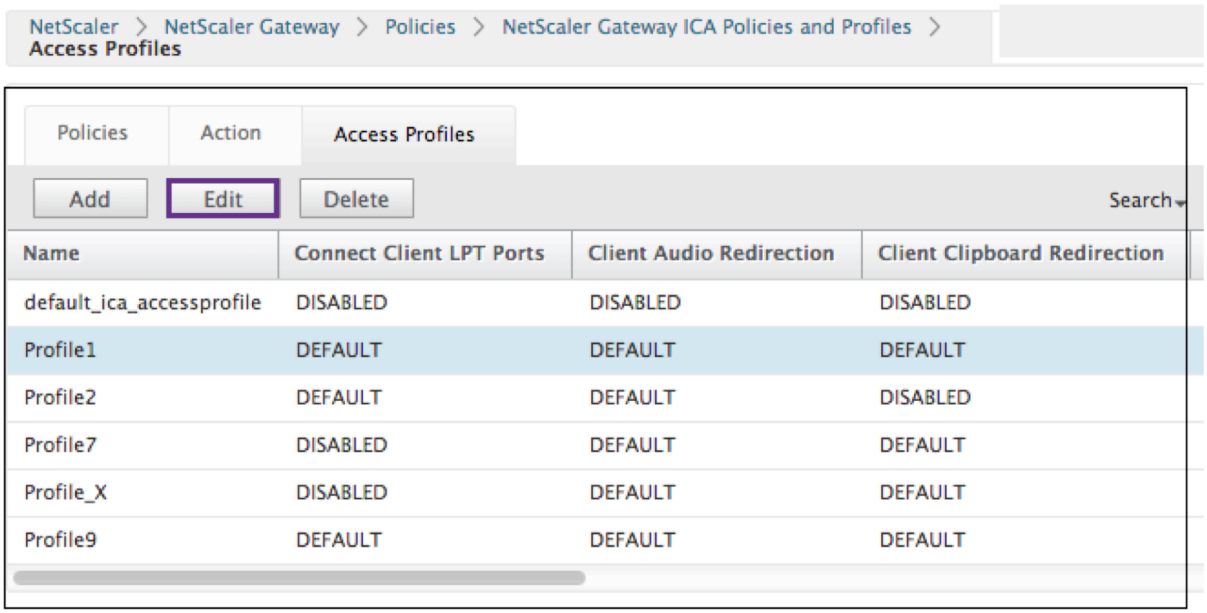
3. 在“名称”中，键入访问配置文件的名称。这是必填字段 **。**



4. 从显示的下拉菜单中选择“默认”或“禁用”以创建访问配置文件。
5. 单击创建。

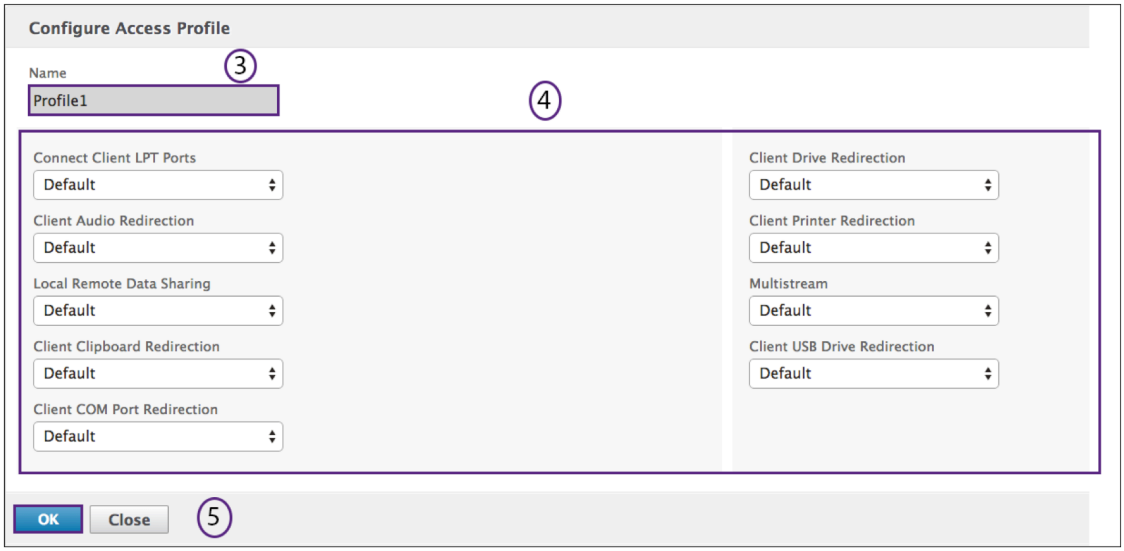
编辑

1. 选择要编辑的访问配置文件。
2. 在详细信息窗格中的访问配置文件选项卡上，单击 编辑。



配置访问配置文件

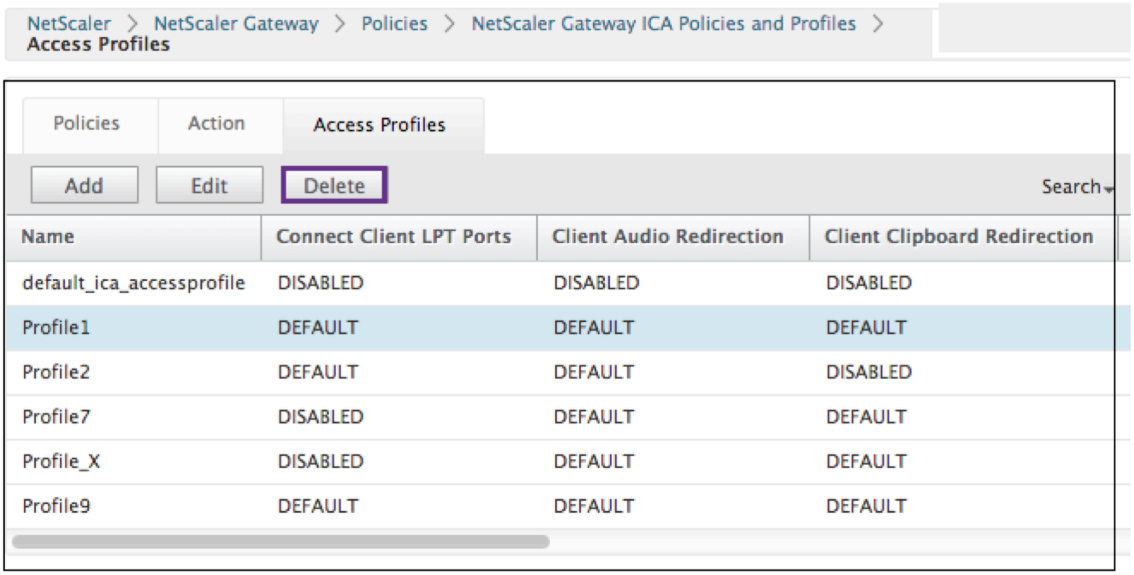
1. 验证名 称是您想要修改的名称。



2. 从下拉菜单中选择 “默认” 或 “禁用” 以根据需要进行配置。
3. 单击确定。

删除

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 “Citrix Gateway”>“操作”，然后单击 “ICA”。
2. 从列表中选择所需的 ICA 操作。
3. 在详细信息窗格中的 “操作” 选项卡上，单击 “删除”。

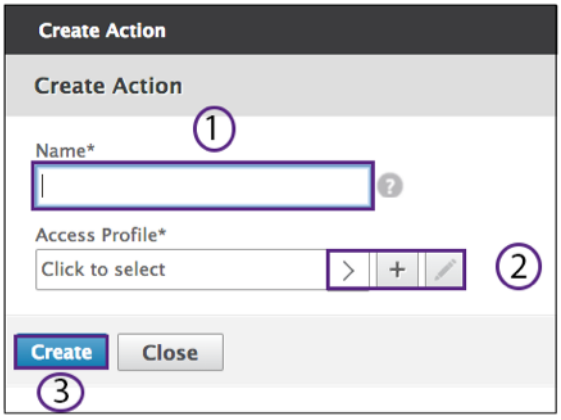


4. 单击“是”，确认要删除的访问配置文件。

共同程序

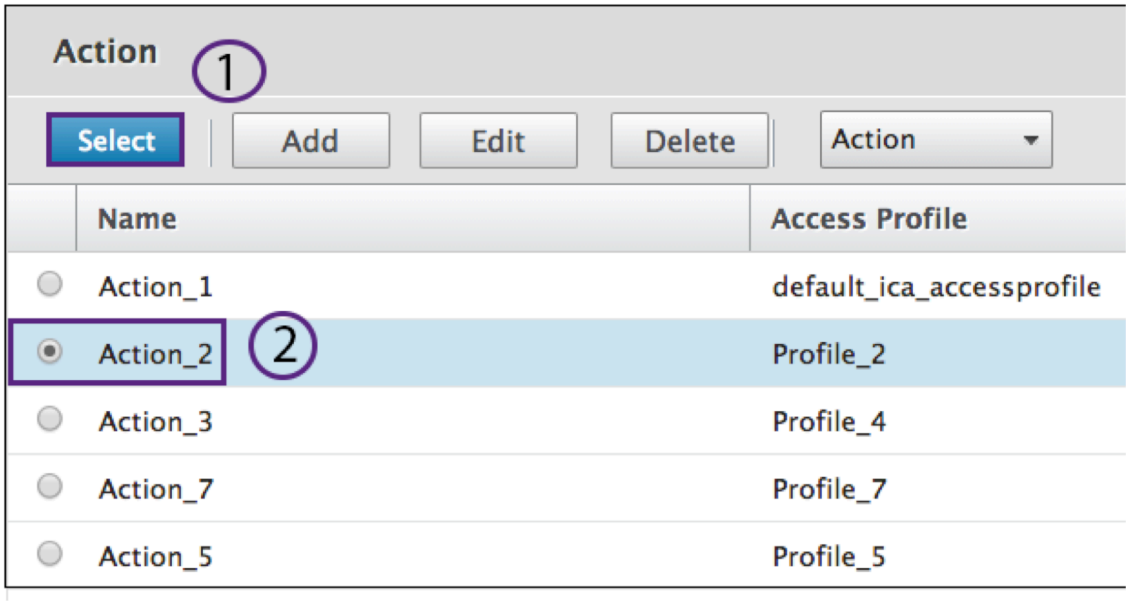
创建新操作

1. 键入操作的名称。
2. 选择以下选项之一以提供访问配置文件：
   - 单击 **>** 以选择现有访问配置文件。请参阅 #common-进程 下的详细信息。
   - 单击 **+** 以创建新的访问配置文件。详情请参阅创建访问配置文件。
   - 铅笔图标处于禁用状态。
3. 单击创建。



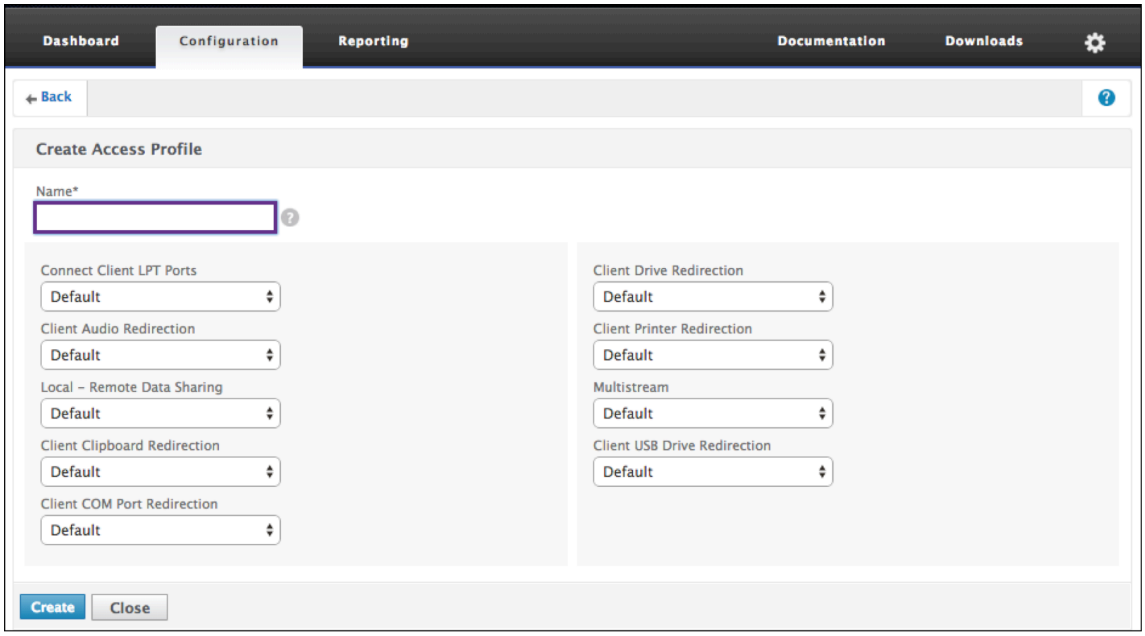
选择一个操作

1. 通过单击左侧的单选按钮来选择一个操作。关联的访问配置文件指定允许的用户功能。
2. 点击选 择按钮。



创建访问配置文件

1. 命名访问配置文件。



2. 您可以选择从此菜单中配置访问配置文件。
3. 单击创建。

选择现有访问配置文件

1. 通过点击访问配置文件来选择它。

2. 单击编辑。
3. 配置访问配置文件。详情请参阅配置访问配置文件。

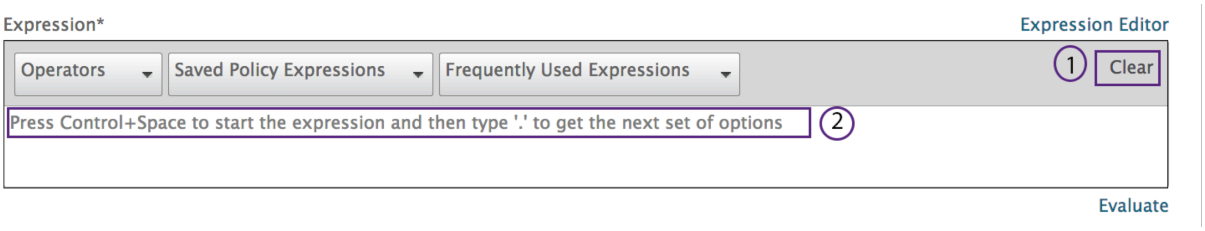
表达式

1. 要创建或修改现有表达式，请选择 “清除”。

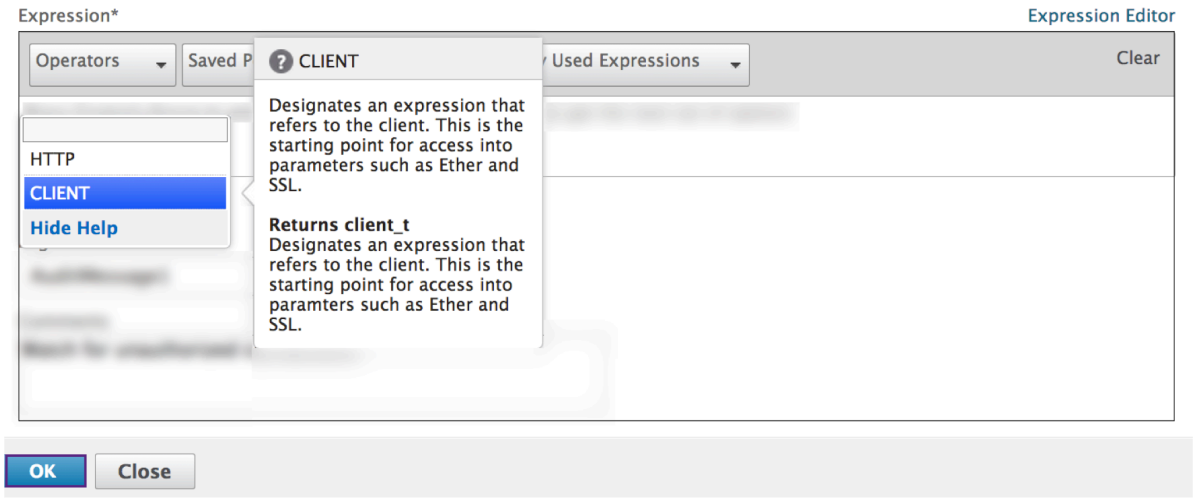
这些是典型的 ICA 表达式。对于 HTTP 表达式，输入带有 “” 的名称并删除 ()。

ICA.SERVER.PORT	此表达式检查指定的端口是否与用户尝试连接的 Citrix Virtual Apps and Desktops 上的端口号匹配。
ICA.SERVER.IP	此表达式检查指定的 IP 是否与用户尝试连接的 Citrix Virtual Apps and Desktops 上的 IP 地址匹配。
HTTP.REQ.USER.IS_MEMBER_OF(“”).NOT	此表达式检查当前连接是否由非指定组名成员的用户访问。
HTTP.REQ.USER.IS_MEMBER_OF(“groupname”)	此表达式检查访问当前连接的用户是否是指定组的成员。
HTTP.REQ.USERNAME.CONTAINS(“”).NOT	此表达式检查访问当前连接的用户是否不是指定组的成员。
HTTP.REQ.USERNAME.CONTAINS(“enter username”) 指定用于用户名的资源。	此表达式检查当前连接是否按指定名称进行访问。
CLIENT.IP.DST.EQ(enter ip address here).NOT	此表达式检查当前流量的目标 IP 不等于指定的 IP 地址。
CLIENT.IP.DST.EQ(enter ip address here)	此表达式检查当前流量的目标 IP 是否等于指定的 IP 地址。
CLIENT.TCP.DSTPORT.EQ (enter port number).NOT	此表达式检查目标端口是否等于指定的端口号。
CLIENT.TCP.DSTPORT.EQ (enter port number)	此表达式检查目标端口是否等于指定的端口号。

2. 同时，选择 “控制” 和 “空格键”，然后您的选项可见。



3. 键入周期。进行选择，然后按 空格键。
4. 在上表中表达式的每个句点，键入句点。进行选择，然后按空格键。
5. 单击确定。

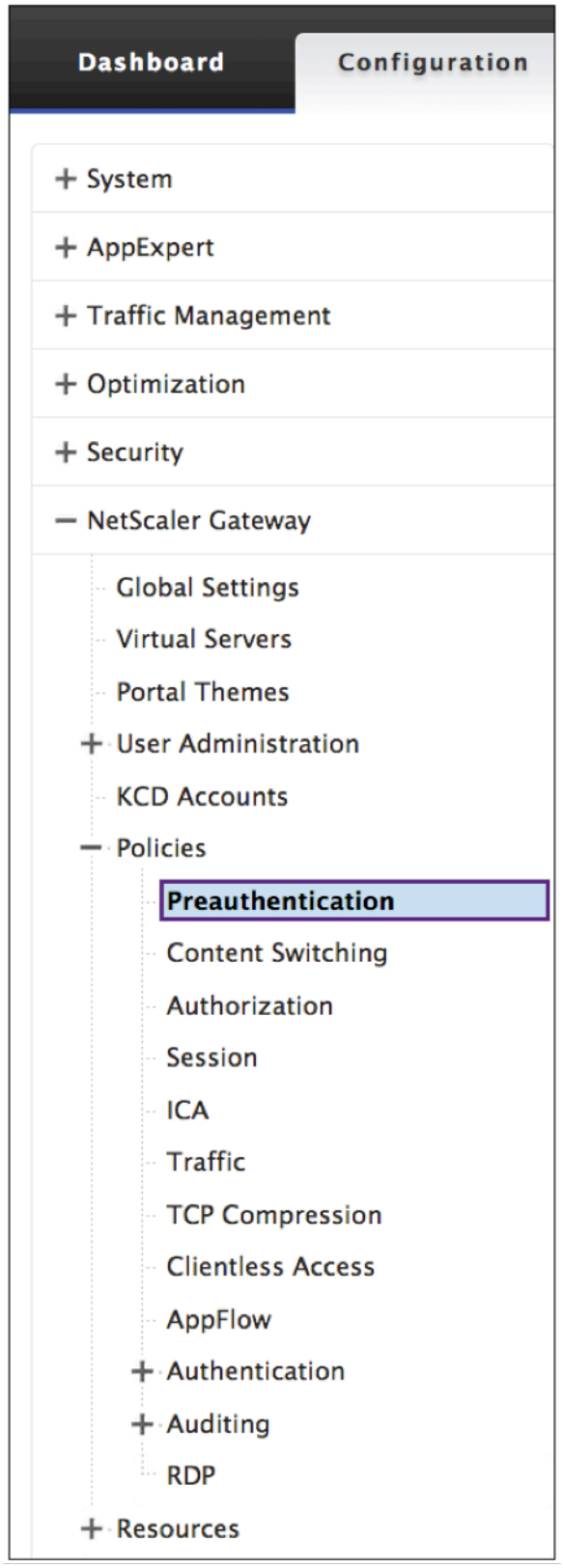


群体识别

带有组名变量的表达式由预真实函数或会话函数定义。

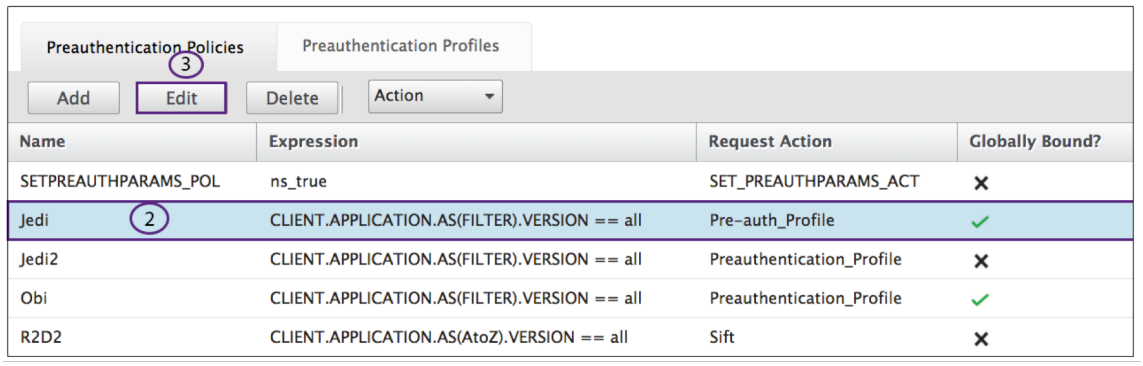
预验证

1. 从配置窗格中选择预身份验证。

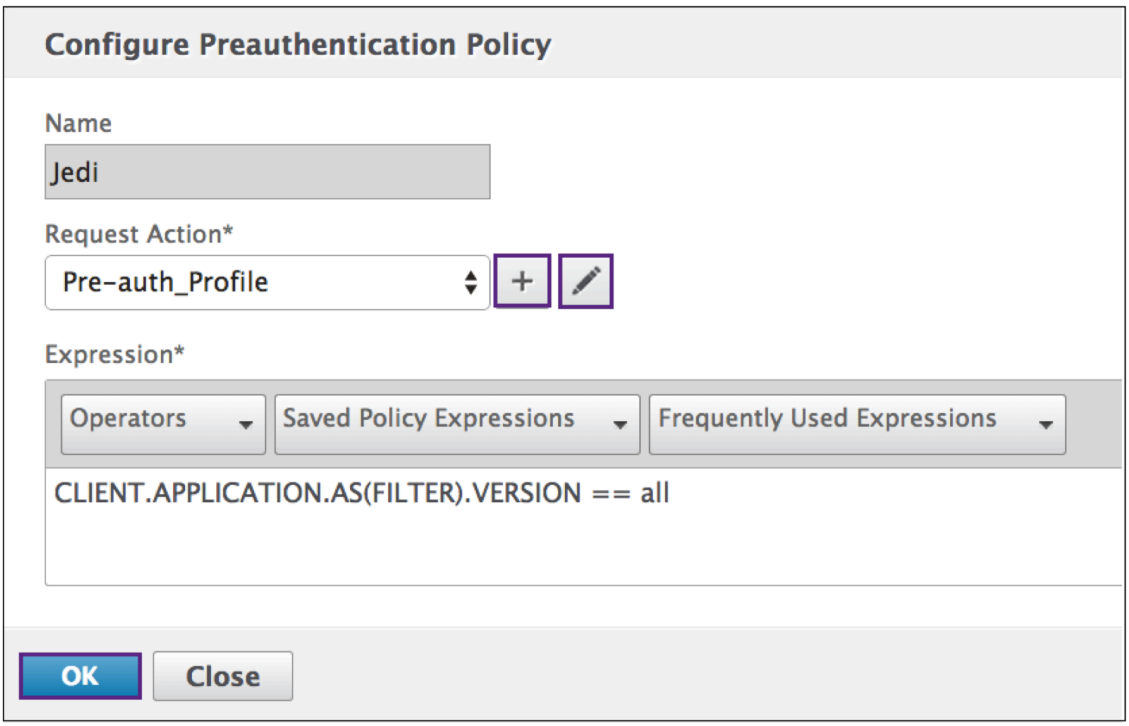


1. 从预身份验证策略中选择一个名称。

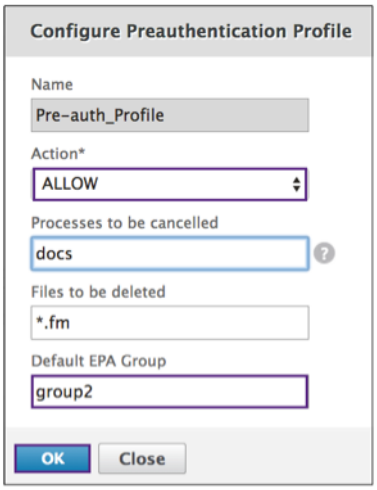
2. 从“预身份验证策略”选项卡中选择“编辑”。



3. 选择“请求操作”对话框旁边的 铅笔图标或 **+** 。

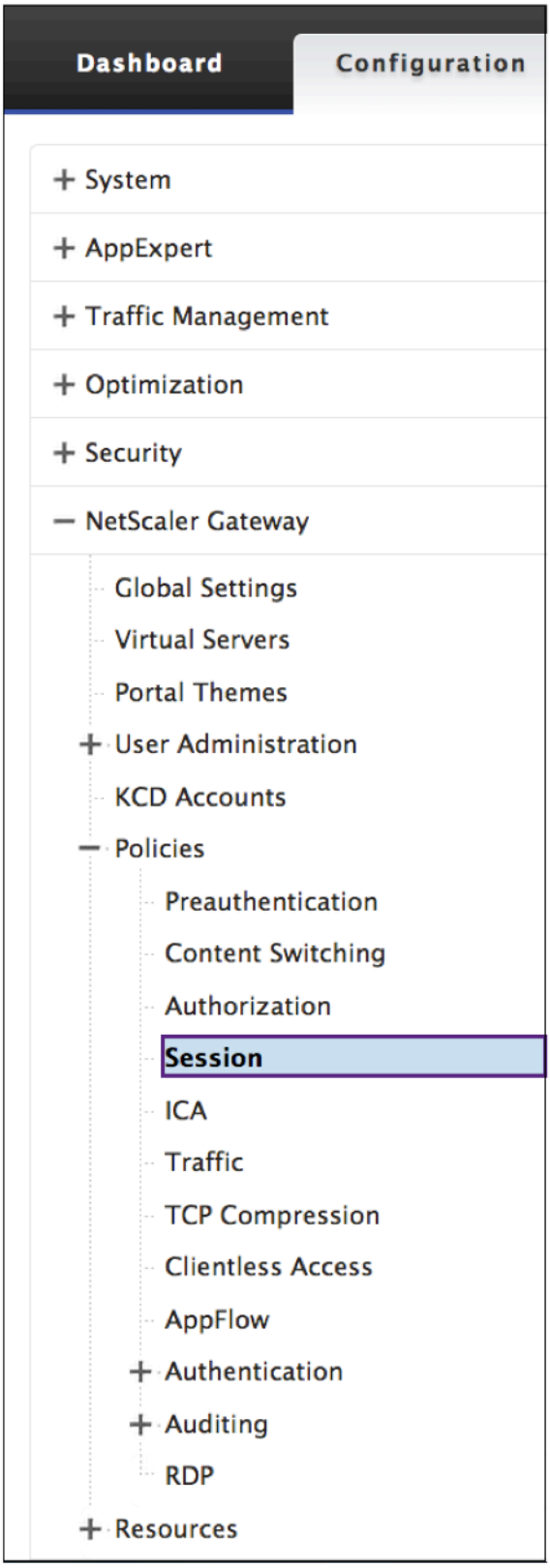


4. 在 <groupname> 默认 EPA 组对话框中定义 (“”)。



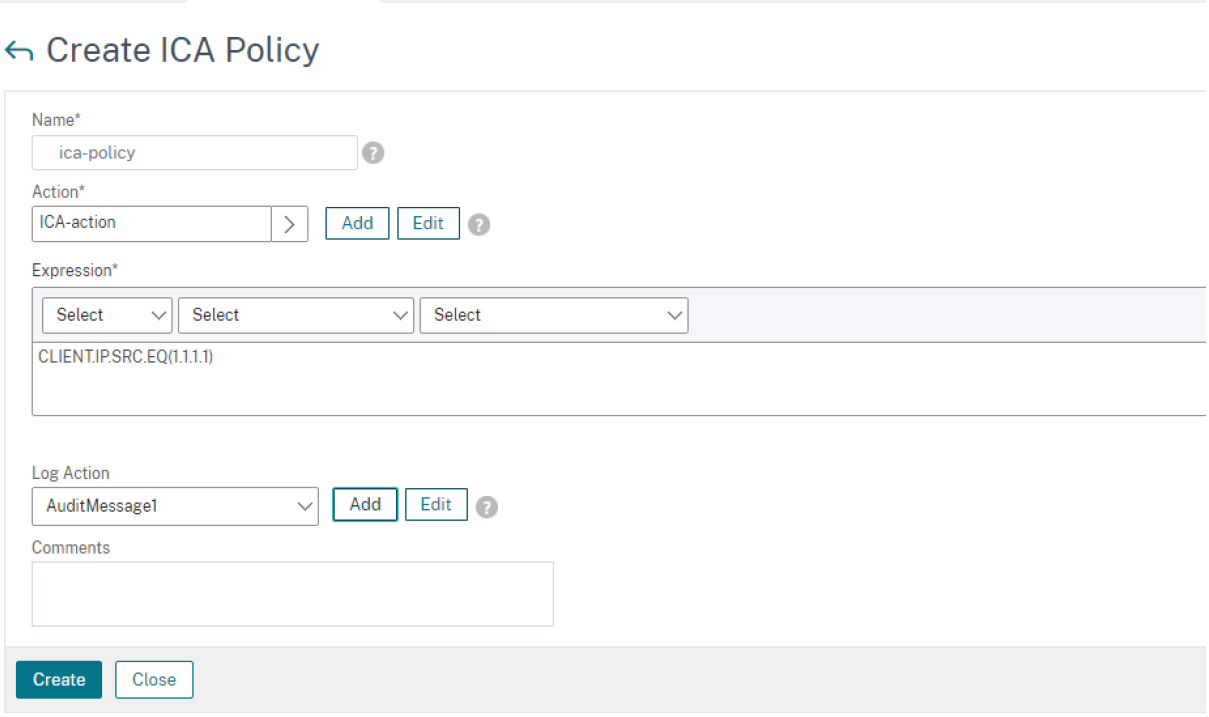
会议

1. 从配置窗格中选择会话。



创建日志操作

1. 在“配置策略”屏幕中，“日志操作”对话框旁边，选择“+”图标



创建审核消息操作

2. 此时将显示“创建审核消息操作”屏幕。命名审核消息。审核消息仅接受数字、字母或下划线字符。

3. 从下拉菜单中指定审核日志级别。

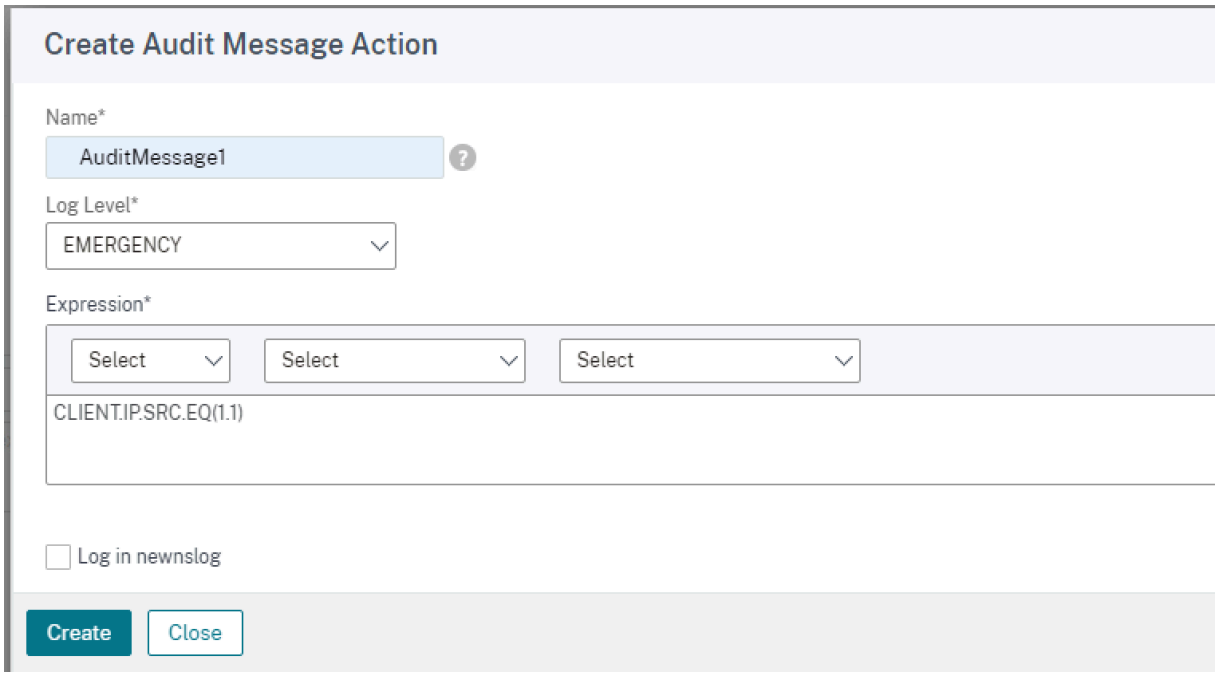
紧急情况	指示服务器上立即发生危机的事件。
警报	可能需要操作的事件。
严重	表明服务器危机迫在眉睫的事件。
错误	指示某种类型错误的事件。
警告	需要在不久的将来采取行动的事件。
注意事项	管理员应了解的事件。
参考信息	除低级别事件外，所有事件。
调试	所有的事件，在极端的细节。

4. 输入表达式。表达式定义日志的格式和内容。

5. 复选框。

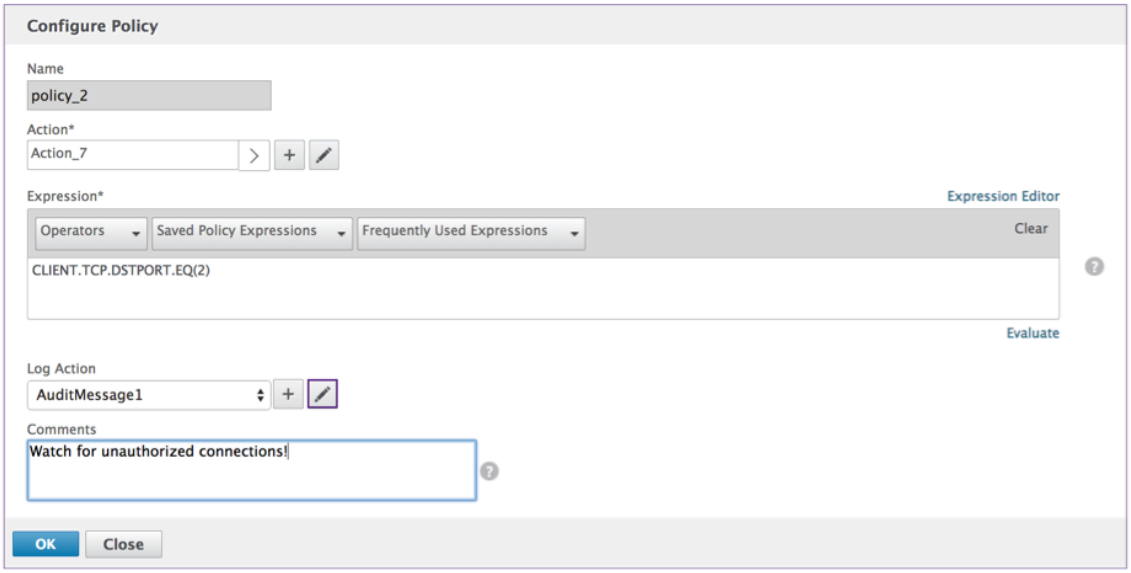
   - 检查在 newnslog 中登录以将消息发送到新的 ns 日志。
   - 检查旁路安全检查以绕过安全检查。这允许不安全的表达式。

6. 单击创建。



修改日志操作

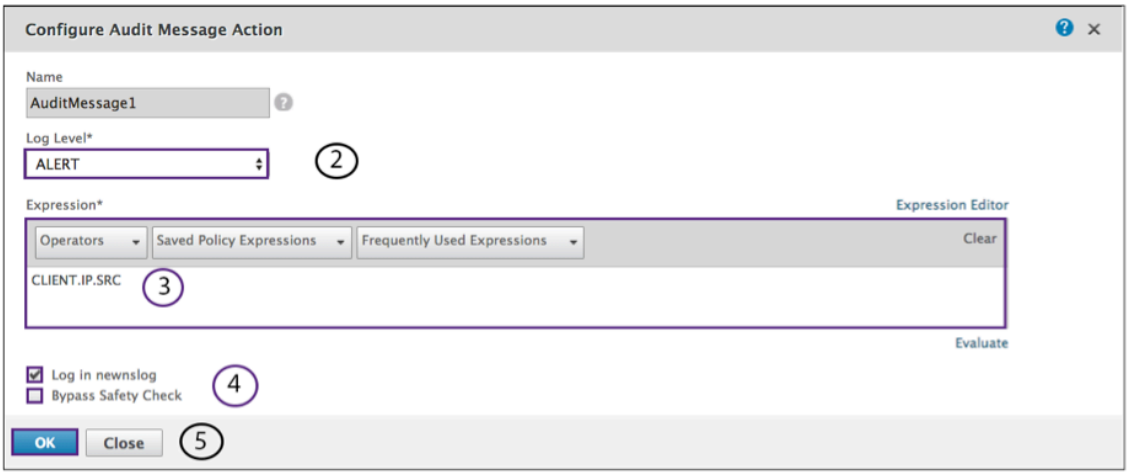
1. 在“配置策略”屏幕中，单击“日志操作”对话框旁边的图标。



配置审核消息操作

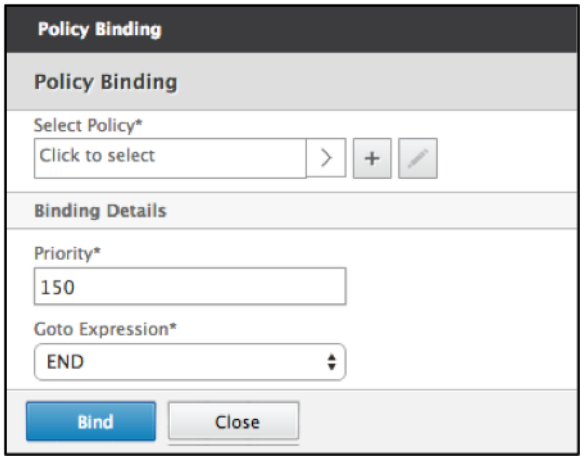
以下是可编辑字段：

1. 从下拉菜单中指定审核日志级别。
2. 输入表达式。表达式定义日志的格式和内容。
3. 复选框：
   - 检查在 newnslog 中登录以将消息发送到新的 ns 日志。
   - 检查旁路安全检查以绕过安全检查。这允许不安全的表达式。
4. 单击确定。

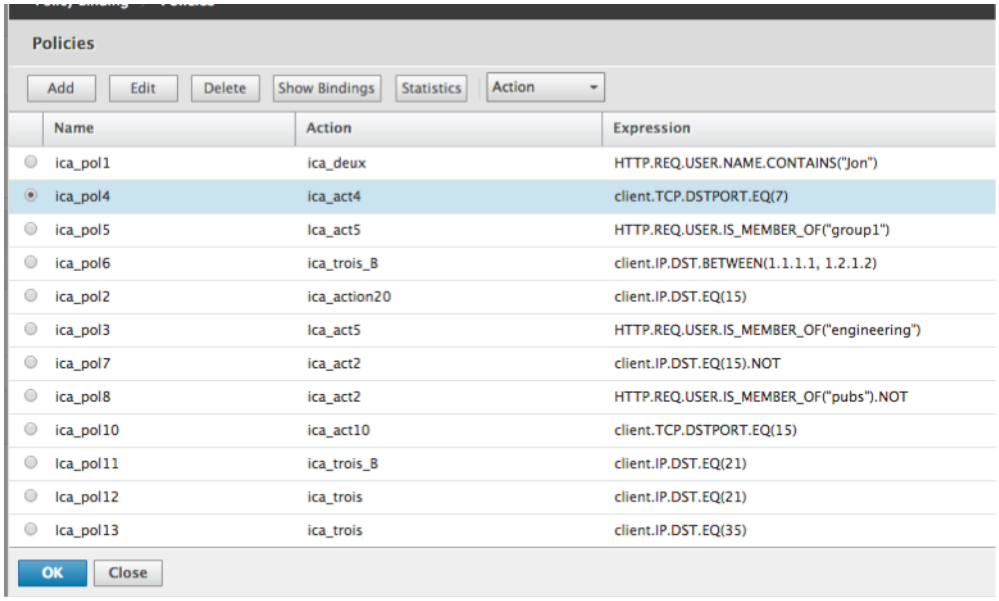


选择现有策略

1. 单击 **>** 图标以选择现有策略。

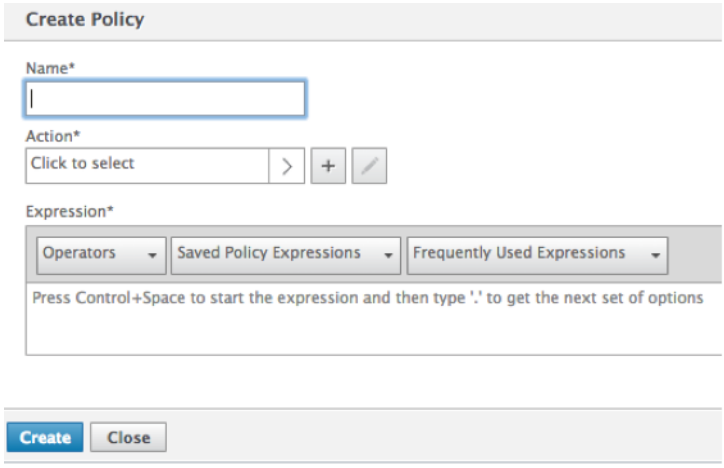


2. 选择所需策略的单选按钮。

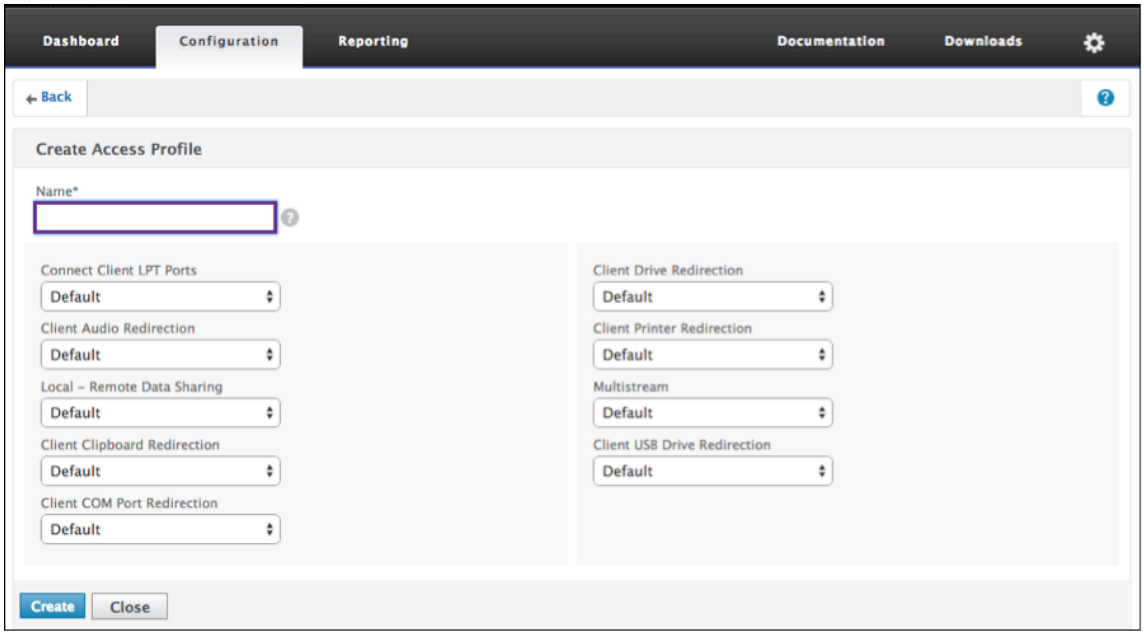


创建新策略

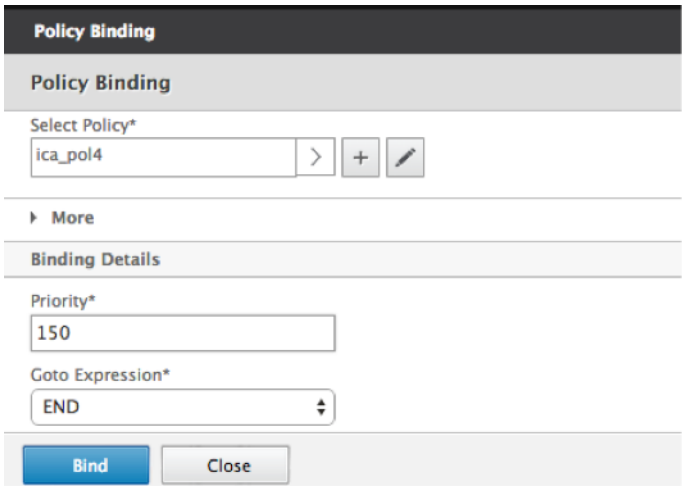
1. 在“名称”中，键入策略的名称。这是必填字段。
2. 单击 **+** 以创建新策略。



3. 创建操作。有关详细信息，请参阅 创建新操作。
4. 命名访问配置文件。



5. 从此菜单中配置访问配置文件。
6. 单击创建。
7. 单击 **Bind**（绑定）。



配置身份验证前和身份验证后端点分析

本节介绍如何配置身份验证后和身份验证前端分析 (EPA)。

要使用智能控制配置身份验证后 EPA，请使用 VPN 会话操作中的智能组参数。EPA 表达式在 VPN 会话策略上配置。

您可以为智能组参数指定组名。此组名可以是任何字符串。groupname 不需要是 Active Directory 中的现有组。

使用表达式 HTTP.REQ.IS_MEMBER_OF (“groupname”) 配置 ICA 策略。使用先前为智能组指定的组名。

要使用智能控制配置预身份验证 EPA，请使用预身份验证配置文件中的默认 EPA 组参数。EPA 表达式在预身份验证策略上进行配置。

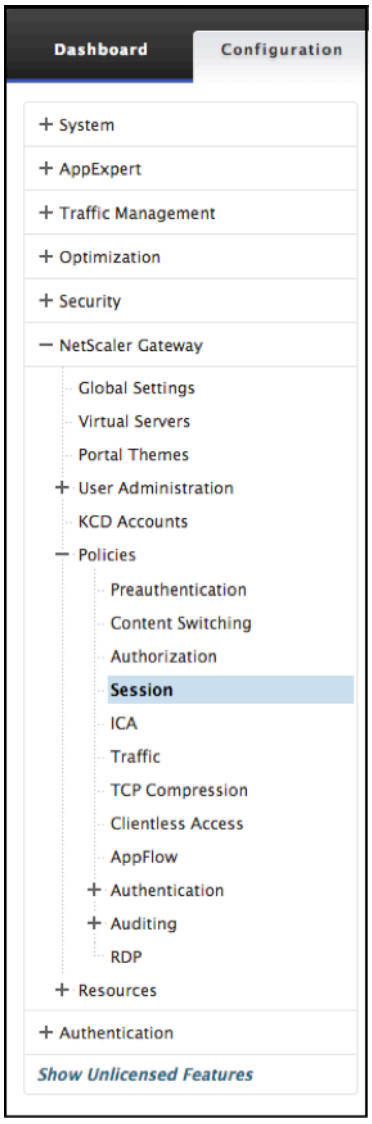
您可以为默认 EPA 组参数指定组名。此组名可以是任何字符串。groupname 不需要是 Active Directory 中的现有组。

使用表达式 HTTP.REQ.IS_MEMBER_OF (“groupname”) 配置 ICA 策略，使用之前为默认 EPA 组指定的组名。

身份验证后配置

使用以下过程为身份验证后配置设置智能组。

1. 转到 “Citrix NetScaler”>“策略”> 会话。



2. 转到会话配置文件 > 添加。

创建 **Citrix Gateway** 会话配置文件

1. 选择“安 全”选项卡。
2. 输入 Citrix Gateway 配置文件的 名称（操作）。
3. 选中下拉菜单右侧的框，然后选择所需的 默认授权操作。

   指定用户登录到内部网络时有权访问的网络资源。授权的默认设置是拒绝访问所有网络资源。Citrix 建议使用默认的全局设置，然后创建授权策略来定义用户可以访问的网络资源。如果将默认授权策略设置为“拒绝”，则必须明确授权对任何网络资源的访问，从而提高了安全性。
4. 选中下拉菜单右侧的框，然后选择所需的 安全浏览。

   允许用户通过 Citrix Gateway 从安装了 Citrix Workspace 应用程序的 iOS 和 Android 移动设备连接到网络资源。用户无需建立完整的 VPN 通道即可访问安全网络中的资源。
5. 选中下拉菜单右侧的框并输入 智能组名称。

   这是当与此会话操作关联的会话策略成功时，用户所在的组。VPN 会话策略将执行身份验证 EPA 后检查，如果检查成功，用户将被放置在 Smartgroup 指定的组中。然后，表达式 is_member_of (http.req.user.is_member_of) 可以与策略一起使用，以检查 EPA 是否已传递给属于此智能组的用户。
6. 单击创建。
7. 转到“Citrix NetScaler”>“策略”> 会话。
8. 转到会话策略 > 添加。
9. 在此 字段中输入名称。

   这是用户登录 Citrix Gateway 后应用的新会话策略的名称。
10. 使用下拉菜单选择 配置文件操作。

    如果满足规则条件，则新会话策略应用的操作。

    > 如果需要创建所需的配置文件，请选择 +。有关更多详细信息，请参阅 创建 **Citrix Gateway** 会话配置文件。
11. 在此字段中输入 表达式。

    此字段定义指定与策略匹配的流量的命名表达式。表达式可以使用默认语法或经典语法编写。表达式的文字字符串的最大长度为 255 个字符。较长的字符串可拆分为较小的字符串，每个字符串最多 255 个字符，而较小的字符串与 + 运算符串连接。例如，您可以创建一个 500 个字符的字符串，如下所示：’“”+“”’

    > 以下要求仅适用于 Citrix ADC CLI：

    * 如果表达式包含一个或多个空格，则将整个表达式用双引号括起来。如果表达式本身包含双引号，请使用字符转义引号。或者，您可以使用单引号将规则括起来，在这种情况下，不必转义双引号。
12. 单击创建。
13. 转到 会话策略。

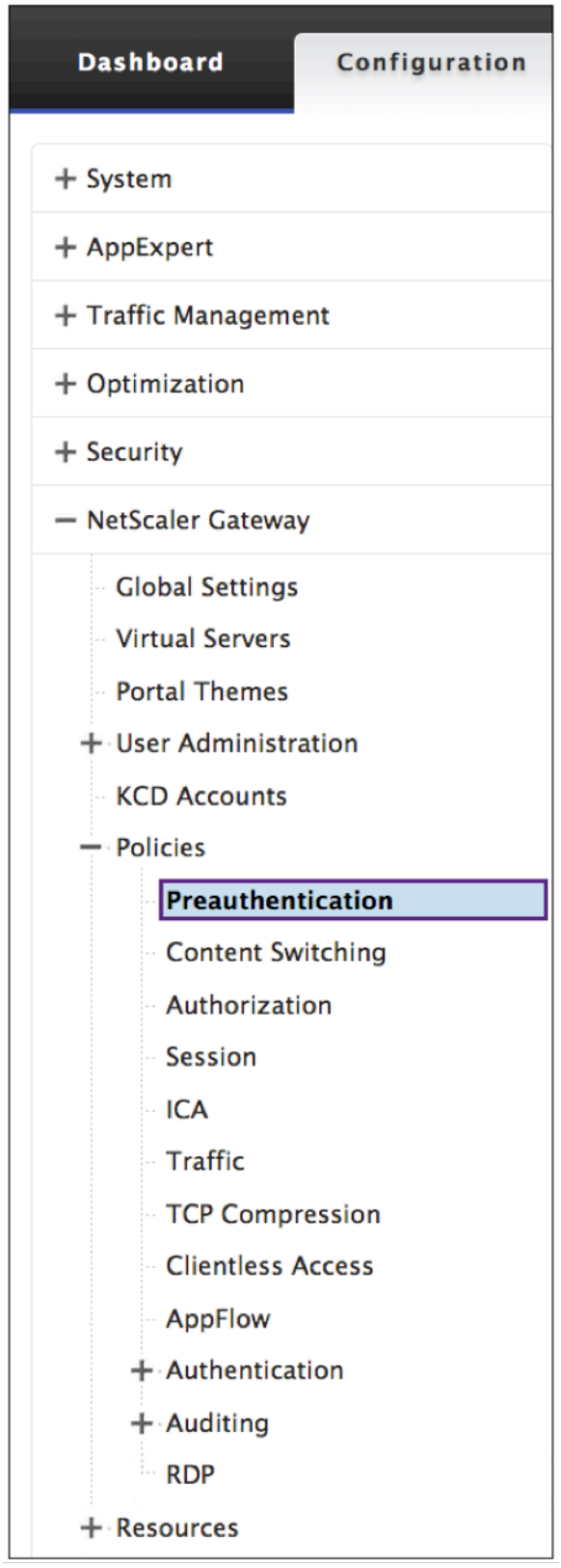
14. 选择会话策略的 名称。
15. 从“操作”下拉菜单中选择“全局绑定”。
16. 选择 添加装订。
17. 选择 **>** 以选择现有策略。

    注意：选择 **+** 以创建新策略。有关更多详细信息，请参阅 创建 **Citrix Gateway** 会话配置文件。
18. 从列表中选择一个名称，然后按 **“选择”** 按钮。
19. 输入 优先级并单击 绑定。
20. 点击 完成
21. 该检查显示您的选择是全局绑定的。

预身份验证配置

使用以下过程设置预身份验证配置。

1. 转到“Citrix NetScaler”>“策略”> 预身份验证。



2. 选择“预身份验证配置文件”选项卡，然后选择“添加”。

3. 输入名 称

   这是预身份验证操作的名称。名称必须以字母、数字或下划线字符 (_) 开头，并且只能由字母、数字和连字符 (-)、句点 (.) (#)、空格 ()、在 (@)、equals (=)、冒号 (:) 和下划线字符组成。创建预身份验证操作后无法更改。

   > 注意：以下要求仅适用于 Citrix ADC CLI：
   > 如果名称包含一个或多个空格，请使用双引号或单引号将名称括起来。

4. 从下拉菜单中选择 请求操作。这是策略在连接匹配策略时要调用的操作。

   > 注意：如果要或创建预身份验证配置文件，请选择 +。有关更多信息，请参阅创建预身份验证配置文件

5. 输入表 达式

   这是 Citrix ADC 命名规则的名称，或者用于定义与策略匹配的连接的默认语法表达式。

6. 单击创建。

7. 转到“预身份验证策略”选项卡并选择所需的策略。

8. 从“操作”下拉菜单中选择“全局绑定”。

9. 选择 添加绑定。

10. 选择 **>** 以选择现有策略。

    > 选择 **+** 以创建新策略。有关更多详细信息，请参阅“创建 Citrix Gateway 会话配置文件”。

11. 选择策略。

12. 输入 优先级并单击 绑定。

13. 单击完成。

14. 检查显示 预身份验证策略是 全局绑定的。

创建预身份验证配置文件

1. 输入 名称。

   这是预身份验证操作的 名称。名称必须以字母、数字或下划线字符 (_) 开头，并且只能由字母、数字和连字符 (-)、句点 (.) (#)、空格 ()、在 (@)、equals (=)、冒号 (:) 和下划线字符组成。创建预身份验证操作后无法更改。

   > 以下要求仅适用于 Citrix ADC CLI：
   > 如果名称包含一个或多个空格，请使用双引号或单引号将名称括起来。

2. 从下拉菜单中输入 操作。

   此选项将在终端分析 (EPA) 结果后允许或拒绝登录。

3. 要取消的流程

   此选项标识要由端点分析 (EPA) 工具终止的一串流程。

4. 要删除的文件

   此选项标识一个字符串，指定要由端点分析 (EPA) 工具删除的文件的路径和名称。

5. 默认 **EPA** 组

   这是 EPA 检查成功时选择的默认组。

6. 单击创建。

配置单点登录到 **Web Interface**

April 6, 2020

您可以将 Citrix Gateway 配置为向内部网络中使用基于 Web 的身份验证的服务器提供单点登录。通过单点登录，您可以将用户重定向到自定义主页，例如 SharePoint 站点或 Web Interface。您还可以通过 Citrix Gateway 插件从访问界面中配置的书签或用户在 Web 浏览器中键入的 Web 地址配置对资源的单点登录。

如果要将访问界面重定向到 SharePoint 站点或 Web Interface，请提供该站点的 Web 地址。当用户通过 Citrix Gateway 或外部身份验证服务器进行身份验证时，用户将被重定向到指定的主页并自动登录。用户凭据透明地传递到 Web 服务器。如果 Web 服务器接受凭据，则会自动登录用户。如果 Web 服务器拒绝凭据，用户将收到一条身份验证提示，询问其用户名和密码。

您可以在全局范围内或使用会话策略配置 Web 应用程序的单点登录。

您还可以使用智能卡配置 Web Interface 的单点登录。有关详细信息，请参阅 使用智能卡配置单点登录到 Web Interface。

Citrix Gateway 与以下版本的 Web Interface 配合使用：

- Web Interface 4.5
- Web Interface 5.0
- Web Interface 5.1
- Web Interface 5.2
- Web Interface 5.3
- Web Interface 5.4

在配置单点登录之前，请确保 Web Interface 已配置并使用 Citrix Gateway。

在全局范围内配置 **Web** 应用程序的单点登录

April 6, 2020

全局应用单点登录将允许 Web 服务对所有 Web 应用程序会话进行身份验证，而不是在 Citrix Gateway 上对这些会话进行身份验证。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** ，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“全局 **Citrix Gateway** 设置”对话框的“客户端体验”选项卡上，单击 **“**单点登录到 Web 应用程序”，然后单 击“确定”。

使用会话策略配置 **Web** 应用程序的单点登录

April 6, 2020

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** > 策略，然后单击“会话”。
2. 在详细信息窗格的“配置文件”选项卡上，选择一个策略，然后单击“添加”。
3. 在“配置会话策略”对话框中，单击“请求配置文件”旁边的“修改”。
4. 在“配置会话配置文件”对话框的“客户端体验”选项卡上的“单点登录到 Web 应用程序”旁边，单击“全局覆盖”，单击 **“**单点登录到 **Web** 应用程序”，然后单 击“确定”。

为 **Web** 应用程序单点登录定义 **HTTP** 端口

April 6, 2020

仅对目标端口被视为 HTTP 端口的网络流量尝试单点登录。要允许对使用端口 80 以外的端口进行 HTTP 流量的应用程序进行单点登录，请在 Citrix Gateway 上添加一个或多个端口号。您可以启用多个端口。您可以在全局配置端口。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** ，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“网络配置”选项卡上，单击“高级设置”。
4. 在 HTTP 端口中，键入端口号，单击 添加，然后单 击确定。

> 注意：如果内部网络中的 Web 应用程序使用不同的端口号，请键入端口号，然后单击“添加”。您必须定义 HTTP 端口号，以允许单点登录 Web 应用程序，包括 Web Interface。

其他配置指南

April 6, 2020

为单点登录配置 Web Interface 时，请使用以下准则：

- 身份验证服务 URL 必须以 https 开头。

- 运行 Web Interface 的服务器必须信任 Citrix Gateway 证书，并且能够将证书完全限定域名 (FQDN) 解析为虚拟服务器 IP 地址。
- Web Interface 必须能够打开与 Citrix Gateway 虚拟服务器的连接。任何 Citrix Gateway 虚拟服务器都可用于此目的；它不一定是用户登录的虚拟服务器。
- 如果 Web Interface 和 Citrix Gateway 之间存在防火墙，则防火墙规则可能会阻止用户访问，从而禁用对 Web Interface 的单点登录。要变通解决此问题，请放松防火墙规则或在 Citrix Gateway 上创建另一个虚拟服务器，Web Interface 可以连接到该虚拟服务器。虚拟服务器必须具有内部网络中的 IP 地址。连接到 Web Interface 时，请使用安全端口 443 作为目标端口。
- 如果对虚拟服务器使用来自私有证书颁发机构 (CA) 的证书，则在 Microsoft 管理控制台 (MMC) 中，使用证书管理单元在运行 Web Interface 的服务器上的本地计算机证书存储中安装 CA 根证书。
- 当用户登录并收到拒绝访问的错误消息时，请检查 Web Interface 事件查看器以获取更多信息。
- 要成功连接到已发布的应用程序或桌面，您在 Citrix Gateway 上配置的安全票证机构 (STA) 必须与您在 Web Interface 上配置的 STA 匹配。

测试与 **Web Interface** 的单点登录连接

April 6, 2020

为 Web Interface 配置单点登录后，从客户端设备打开 Web 浏览器并测试连接是否成功。

1. 在 Web 浏览器中，键入`https://NetScalerGatewayFQDN`，其中 NetScalerGatewayFQDN 是绑定到虚拟服务器的证书中的完全限定域名 (FQDN)。
2. 登录到 Active Directory 中的域用户帐户。登录时，您将被重定向到 Web Interface。

应用程序自动显示，无需额外身份验证。当用户启动已发布的应用程序时，Citrix Workspace 应用程序将通过 Citrix Gateway 设备的流量定向到场中的服务器。

使用智能卡配置单点登录到 **Web Interface**

January 10, 2023

如果使用智能卡进行用户登录，则可以配置单点登录到 Web Interface。在 Citrix Gateway 上配置设置，然后将 Web Interface 配置为接受使用智能卡的单点登录。单点登录也称为直通身份验证。

Web Interface 5.3 和 5.4 版支持使用智能卡单点登录 Web Interface。如果启用 NetScaler 版本 10 中提供的 Citrix ADC 上的 Web Interface 功能，也可以使用智能卡的单点登录。有关配置此功能的更多信息，请参阅通过 Citrix Gateway 对 Web Interface 使用智能卡身份验证。

只要证书操作中的用户名提取为 “SubjectAltName:PrincipalName”，用户就可以在 Active Directory 中的多个 CN 组中进行单点登录工作。如果您使用参数主题：CN，则用户不能成为多个 CN 组的一部分。

要使用智能卡将 Citrix Gateway 配置为单点登录到 Web Interface，您需要执行以下操作：

- 从证书颁发机构 (CA) 安装签名的服务器证书。有关详细信息，请参阅在 Citrix Gateway 上安装签名证书。
- 在 Citrix Gateway 和用户设备上安装根证书。
- 创建虚拟服务器作为 Web Interface 的登录点。配置虚拟服务器时，必须将客户端证书 SSL 参数设置为可选。有关配置虚拟服务器的更多信息，请参阅创建虚拟服务器。
- 创建在 SSL 参数中禁用客户端身份验证的辅助虚拟服务器。此配置可防止用户收到个人标识号 (PIN) 的辅助请求。
- 创建客户端证书身份验证策略。在“用户名”字段中，使用参数 SubjectAltName:PrincipalName 从多个组中提取用户。将组名称字段留空。
- 在 Citrix Gateway 上创建会话策略和配置文件。在会话配置文件中，您可以启用 ICA 代理并指定用于单点登录的 Web Interface 和域。

您可以使用以下过程创建用于使用智能卡单点登录的会话配置文件。

使用智能卡为单点登录创建会话配置文件

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway 策略，然后单击“会话”。
2. 在详细信息窗格中，单击配置文件选项卡，然后单击添加。

3. 在“客户体验”选项卡上，在主页旁边，单击“覆盖全局”，然后清除“显示主页”。

1. 在单点登录到 Web 应用程序旁边，单击覆盖全局，然后单击单点登录到 Web 应用程序。
2. 单击 Published Applications（已发布的应用程序）选项卡。
3. 在 ICA 代理旁边，单击覆盖全局，然后选择开。
4. 在 Web Interface 地址中，单击覆盖全局，然后键入完全限定的域名 (FQDN) 或 Web Interface。
5. 在单点登录域中，单击覆盖全局，然后键入域名。

   > 注意：您必须使用格式域，而不是格式域。

6. 单击 **Create**（创建），然后单击 **Close**（关闭）。

完成会话配置文件后，请配置会话策略并将该配置文件用作策略的一部分。然后，您可以将会话策略绑定到虚拟服务器。

使用智能卡配置单点登录的客户端证书

April 6, 2020

如果使用智能卡配置 Web Interface 的单点登录，则必须在虚拟服务器对话框中选择“
证书上的
客户端身份验证”，然后将客户端证书配置为“

可选”。如果选择 “
强制”，则单点登录 Web Interface 将失败。

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 Citrix Gateway，然后单击 “虚拟服务器”。
2. 在详细信息窗格中，单击虚拟服务器，然后单击打开。
3. 在 “配置 Citrix Gateway 虚拟服务器” 对话框中的 “证书” 选项卡上，单击 “SSL 参数”。
4. 在 “配置 SSL 参数” 对话框的 “其他” 下，单击 “客户端身份验证”。
5. 在客户端证书中，选择可选，然后单击确定两次。

为 **Citrix Virtual Apps** 和文件共享配置单点登录

April 6, 2020

如果用户连接到运行 Citrix Virtual Apps 的服务器并使用 SmartAccess，则可以为连接到服务器场的用户配置单点登录。使用会话策略和配置文件配置对已发布应用程序的访问时，请使用服务器场的域名。

您还可以在网络中配置单点登录到文件共享。

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 **Citrix Gateway** > 策略，然后单击 “会话”。
2. 在详细信息窗格的 “策略” 选项卡上，选择会话策略，然后单击 “打开”。
3. 在 “配置会话策略” 对话框中，单击 “请求配置文件” 旁边的 “修改”。
4. 在 “配置会话配置文件” 对话框中的 “已发布的应用程序” 选项卡上的 “单点登录域” 中，单击 “覆盖全局”，键入域名，然后单 击 “确定” 两次。

允许文件类型关联

April 6, 2020

文件类型关联允许用户在通过 Citrix Virtual Apps 或 Citrix Virtual Desktops 7 发布的应用程序中打开文档。您可以使用此权限允许用户在受信任环境中的服务器上打开和编辑文档，并避免将文档发送到用户设备。只有在 Citrix Gateway 上正确配置虚拟服务器属性时，才能对与已发布应用程序关联的文档类型使用文件类型关联。

提供文件类型关联作为编辑资源文档的唯一方法有助于提高安全性，因为它需要在服务器上进行编辑，而不是在用户设备上进行编辑。例如，您可以选择为员工发布正在进行的项目会议报告的文件共享授予文件类型关联，而无需提供下载或上载功能。

提供文件类型关联要求：

- 用户在用户设备上运行 Citrix Workspace 应用程序。
- 用户通过具有绑定流量策略并为 Citrix Virtual Apps 配置策略的虚拟服务器进行连接。
- 用户将被分配到 Citrix Virtual Apps and Desktops 7 中的所需应用程序。
- 管理员配置 Citrix Virtual Apps 以使用 Citrix Gateway。

创建文件类型关联的步骤包括：

- 创建 Web Interface 站点。
- 使用 Citrix Gateway 上的流量策略配置文件类型关联。
- 在 Citrix Virtual Apps and Desktops 7 中定义文件扩展名。

创建 **Web Interface** 站点

April 6, 2020

若要将 Web Interface 配置为使用文件类型关联，请首先创建 Web Interface 站点。Web Interface 站点可以是直接或高级访问控制。将以下目录复制到您的 Web Interface 站点：

- 应用程序数据
- 身份验证
- 站点

将这些目录复制到 Web Interface 站点时，现有目录将被覆盖。

如果您使用的是 Web Interface 4.6 或 5.0，请在 Web Interface 站点目录中打开 web.config 文件并添加以下代码。您可以从 Citrix 支持站点上下载此代码http://support.citrix.com/article/ctx116253。

```
pre codeblock
<location path="site/contentLaunch.ica">
<system.web>
<httpHandlers>
<add verb="\*" path="\*.ica" type="System.Web.UI.PageHandlerFactory"/>
</httpHandlers>
</system.web>
</location>
<location path="site/contentLaunch.rad">
<system.web>
<httpHandlers>
<add verb="\*" path="\*.rad" type="System.Web.UI.PageHandlerFactory"/>
</httpHandlers>
</system.web>
</location>
<!--NeedCopy-->
```

此代码必须在 web.config 文件中的以下部分之后添加：

```
pre codeblock
<location path="site/launch.rad">
        <system.web>
```



```
            <httpHandlers>
                <add verb="\*" path="\*.rad" type="System.Web.UI.
                   PageHandlerFactory"/>
            </httpHandlers>
        </system.web>
    </location>
<!--NeedCopy-->
```

为文件类型关联配置 **Citrix Gateway**

November 3, 2021

在 Citrix Gateway 上配置文件类型关联之前，请将 Web Interface 站点配置为使用文件类型关联。创建和配置 Web Interface 后，需要在 Citrix Gateway 上创建设置。这些步骤包括：

- 创建新的虚拟服务器或使用现有的虚拟服务器。有关创建虚拟服务器的更多信息，请参阅创建虚拟服务器。
- 创建配置了 Web Interface 的新会话策略和配置文件。
- 将会话策略绑定到虚拟服务器。
- 创建流量策略。

创建会话策略并将其绑定到虚拟服务器之后，请创建流量策略并将其绑定到虚拟服务器。

为文件类型关联配置流量策略时，您可以创建一个表达式来定义文件扩展名。例如，您要启用文件类型关联的 Microsoft Word 和 Microsoft Excel。一个示例表达式是：

俄罗斯`EQ.HTTP.URL == /\*.doc || REQ.HTTP.URL == /\*.xls`

为文件类型关联创建会话策略和配置文件

1. 在配置实用程序中，单击配置选项卡，然后在导航窗格中展开 **Citrix Gateway** > 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在“已发布的应用程序”选项卡上，配置以下设置：
   a) 在 Web Interface 地址旁边，单击覆盖全局，然后键入 Web Interface 的 Web 地址。
   b) 在 Web Interface 门户模式旁边，单击“覆盖全局”，然后选择“正常”或“压缩”。
   c) 在单点登录域旁边，单击“覆盖全局”，键入用户帐户所在域的名称，然后单击“创建”。
7. 在“创建会话策略”对话框中，在“命名表达式”旁边，选择“**True**”值，单击“添加表达式”，单击“创建”，然后单击“关闭”。

为文件类型关联创建流量配置文件

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway 策略，然后单击“流量”。
2. 在详细信息窗格中，单击配置文件选项卡，然后单击添加。
3. 在“名称”中，键入配置文件的名称。
4. 在文件类型关联中，选择开，单击创建，然后单击关闭。

在流量策略中配置文件类型关联

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway 策略，然后单击“流量”。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在请求配置文件中，选择一个配置文件。
5. 在“创建流量策略”对话框的“表达式”下，选择“高级自由格式”，然后单击“添加”。
6. 在“添加表达式”对话框中，执行以下操作：
   a) 在“表达式类型”中，单击“常规”。
   b) 在流量类型中，选择 REQ。
   c) 在协议中，选择 HTTP。
   d) 在限定符中，选择 URL。
   e) 在“运算符”中，选择 = =。
   f) 在“值”中，键入 /*.FileExtensionType，其中.FileExtensionType 为文件类型，例如.doc 或.xls，然后单击确定。
7. 在“创建流量策略”对话框的“表达式”下，单击“高级自由格式”旁边的“或”。
8. 对要包括的每个文件扩展名重复步骤 4、5 和 6，单击“创建”，然后单击“关闭”。

将 Citrix Gateway 与 Citrix Virtual Apps and Desktops 集成

April 6, 2020

部署和配置 StoreFront 服务器以管理对已发布资源和数据的访问。为了进行远程访问，建议在 StoreFront 前面添加 Citrix Gateway。

> 注意
>
> 有关如何将 Citrix Virtual Apps and Desktops 与 Citrix Gateway 集成的详细配置步骤，请参阅StoreFront 文档。

下图说明了包含 Citrix Gateway 的简化 Citrix 部署示例。Citrix Gateway 与 StoreFront 通信来保护 Citrix Virtual Apps and Desktops 提供的应用程序和数据。用户设备运行 Citrix Workspace 应用程序来创建安全连接以及访问其应用程序、桌面和文件。

用户使用 Citrix Gateway 登录并进行身份验证。Citrix Gateway 部署在 DMZ 中并受到保护。配置了双重身份验证。用户会根据用户凭据获得相关的资源和应用程序。应用程序和数据位于相应的服务器上（图中未显示）。安全性敏感应用程序和数据使用单独的服务器。

将 **Citrix Gateway** 与 **StoreFront** 集成

April 6, 2020

Citrix Virtual Apps and Desktops 向导用于将 StoreFront 与 Citrix Gateway 集成。该集成有助于通过 Citrix Gateway 访问托管虚拟桌面 (XenDesktop) 和托管 Windows 虚拟应用程序 (XenApp)。

为了与 Storefront 无缝集成 Citrix Gateway，Citrix Virtual Apps and Desktops 向导工作流现在通过以下功能增强。

- 检索在受支持的 **StoreFront** 上配置的应用商店：只需单击即可检索在受支持的 StoreFront 上配置的应用商店。这有助于避免手动干预，从而避免人为错误（错误）。
- 对 **StoreFront** 配置文件的导出支持：可以在 Citrix Gateway 上导出 StoreFront 配置文件。然后，可以在受支持的 StoreFront 服务器上下载并最终导入此文件。导入文件后，StoreFront 将完成 NetScaler 集成。
- **StoreFront** 作为身份验证服务器：通过引入高级 身份验证操作，将 StoreFront 用作身份验证服务的身份验证服务器，可以简化身份验证。

> 注意
> 身份验证服务器也可用于非 Citrix Virtual Apps and Desktops 部署。

如何配置 **Citrix Gateway** 以便与 **StoreFront** 一起使用

必备条件

您必须具备以下信息才能将 NetScaler 与 StoreFront 集成：

- Citrix Gateway 虚拟服务器的 IP 地址
- StoreFront 服务器的完全限定域名 (FQDN)
- Citrix Gateway 的服务器证书
- 身份验证服务器详细信息

还要确保以下内容：

- Citrix Gateway 和 StoreFront 之间的防火墙端口处于打开状态
- StoreFront 具有局域网访问权限

要使用 **Citrix Gateway GUI** 将 **StoreFront** 与 **Citrix Gateway** 集成，请执行以下操作：

1. 导航到配置 > **Citrix Virtual Apps and Desktops**。
2. 点击 开始。

3. 选择 **StoreFront** 并单击继续。
4. 在 Citrix Gateway 区域中输入以下字段的值，然后单击 继续。
    - 网关 **FQDN** - Citrix Gateway 的 FQDN
    - 网关 **IP** 地址 - Citrix Gateway 的 IP 地址
    - 端口 - Citrix Gateway 的端口
5. 在“服务器证书”区域中导入以下文件，然后单击“继续”。证书文件 -Citrix Gateway 的服务器证书。
6. 在 **StoreFront** 区域中提供以下信息，然后单击继续。
    - **StoreFront URL** — StoreFront 服务器的 URL
    - **Receiver for Web** 路径 - 已在 StoreFront 上配置的 Receiver for Web 的路径
    - 默认 **Active Directory** 域 - 用于内部网络中的单点登录应用程序的单点登录域
    - 安全票证授权 **URL** — 安全票证授权 URL。这通常存在于 Delivery Controller 上。

    > 注意：在选择“
    > 检索应用商店 Citrix Gateway 联系 StoreFront，并返回 StoreFront 上配置的所有应用商店信息。然后，您可以从下拉菜单中选择首选应用商店。
    > 检索应用商店选项仅适用于最新的 StoreFront 服务器。
7. 使用新的身份验证设置，用户可以创建新的身份验证策略，也可以使用现有的身份验证策略。

    要创建新的基于域的身份验证策略，请在中输入以下字段的值，然后单击 继续。
8. 选择身份验证类型**-** 从下拉菜单中选择域
9. 选择 添加新服务器或根据您的要求 使用现有服务器
    - **IP** 地址 — 域服务器的 IP 地址
    - 端口 — 域服务器的端口
    - 基本 **DN** -用户所在的基本 DN
    - 服务帐户 - 用于查询 Active Directory 的帐户
    - 密码 -登录域服务器所需的密码
    - 超时**-**查找域目录的时间持续时间
    - 服务器登录名属性 - NetScaler 设备用于查询外部域服务器或 Active Directory 的名称属性。

    您可以选择单击 测试连接以确保服务器可访问并提供有效凭据。

    > 注意：要使用现有身份验证策略，请从“选择 身份验证类型”下拉列表中 选择所需的身份验证类型，并提供上面列出的信息。
10. 在 Citrix Gateway 设置页面上，单击 完成。
11. 点击 下载文件。

以下是 **StoreFront GUI** 中所需的配置步骤：

1. 将 StoreFront 配置.zip 文件复制到 StoreFront。

2. 点击 商店。
3. 选择 管理 **Citrix Gateway**，然后单击管理 **Citrix Gateway** 窗口中的从文件导入链接。
4. 在导入 **NetScaler** 配置窗口中的选择文件区域下，单击下一步。
5. 在“选择登录类型”区域下，可选地为 StoreFront 提供 回调 **URL** 以联系 Citrix Gateway，然后单击“下一步”。
6. 在安全票据管理机构下单击下一步。
7. 在“查看更改”下，单击 **“**下一步”。
8. 单击完成。

为 **Citrix Endpoint Management** 环境配置设置

April 6, 2020

适用于 Citrix Endpoint Management 的 Citrix ADC 向导将指导您完成适用于 Citrix Endpoint Management 部署的 Citrix ADC 功能的配置。您可以使用向导执行以下操作：

- 设置一个微型 **VPN**。在这种情况下，远程用户可以访问内部网络中的应用程序和桌面。
  - 对于 Citrix Endpoint Management 模式，必须使用 Citrix Gateway 进行身份验证。
  - 对于 MDM 部署，Citrix 推荐用于移动设备 VPN 的 Citrix Gateway。
  - 对于 ENT 部署，如果用户选择退出 MDM 注册，则设备将在旧版 MAM 模式下运行，并使用 Citrix Gateway FQDN 进行注册。
- 配置基于证书的身份验证。Citrix Endpoint Management 的默认配置为用户名和密码身份验证。要为 Citrix Endpoint Management 环境中的注册和访问再增加一个安全层，请考虑使用基于证书的身份验证。
- 对 **Citrix Endpoint Management** 服务器进行负载平衡。如果您有多个 Citrix Endpoint Management 服务器，或者 Citrix Endpoint Management 位于 DMZ 或内部网络中（因此流量从设备流向 Citrix ADC，再流向 Citrix Endpoint Management），则所有 Citrix Endpoint Management 设备模式都需要 Citrix ADC 负载平衡。在这种情况下，Citrix ADC 设备位于用户设备与 Citrix Endpoint Management 服务器之间的 DMZ 中，以便对从移动设备发送到 Citrix Endpoint Management 服务器的加密数据进行负载平衡。
- 通过电子邮件筛选功能对 **Microsoft Exchange Server** 进行负载平衡。在这种情况下，Citrix ADC 设备位于用户设备与 Citrix Endpoint Management Citrix ADC Connector (XNC) 之间，以及用户设备与 Microsoft Exchange CAS 服务器之间。来自用户设备的所有请求都会转到 Citrix Gateway 设备，然后该设备与 XNC 通信以检索有关设备的信息。根据来自 XNC 的响应，Citrix ADC 设备将请求从列入白名单的设备转发到内部网络中的服务器，或从列入黑名单的设备中断连接。
- 根据请求的内容类型对 **ShareFile StorageZones Connector** 进行负载平衡。此方案提示您输入有关 StorageZones Controller 环境的基本信息，然后生成执行以下操作的配置：
  - 在 StorageZones Controller 对流量进行负载平衡。

- 为存储区域连接器提供用户身份验证。
- 验证 ShareFile 上载和下载的 URI 签名。
- 终止 Citrix ADC 设备上的 SSL 连接。

有关配置 ShareFile 的更多信息，请参阅为 StorageZones Controller 配置 Citrix ADC。

> 重要
>
> 在使用 Citrix Endpoint Management 向导之前，请务必参阅以下 Citrix Endpoint Management 部署文章，了解设计和部署信息及建议：
>
> Citrix Endpoint Management 集成
>
> 将 Citrix Gateway 与 Citrix ADC 相集成
>
> MDX 应用程序的 SSO 和代理注意事项
>
> 身份验证
>
> 只能使用适用于 Citrix Endpoint Management 的 Citrix ADC 向导一次。如果需要多个 Citrix Endpoint Management 实例（例如，用于测试、开发和生产环境），必须手动为其他环境配置 Citrix ADC。以下支持文章列出了向导运行的命令，并提供了运行这些命令以创建新 Citrix ADC 实例的说明：
>
> Citrix ADC 上的 Citrix Endpoint Management 向导生成的命令 - SSL 桥接
>
> Citrix ADC 上的 Citrix Endpoint Management 向导生成的命令 - SSL 卸载

Citrix ADC 功能的许可证要求

您必须安装许可证才能启用以下 Citrix ADC 功能：

- Citrix Endpoint Management MDM 负载平衡需要 Citrix ADC 标准许可证。
- 使用 StorageZones 进行 ShareFile 负载平衡需要 Citrix ADC 标准许可证。
- Exchange 负载平衡需要 Citrix ADC 许可证或高级许可证，并添加了集成缓存许可证。

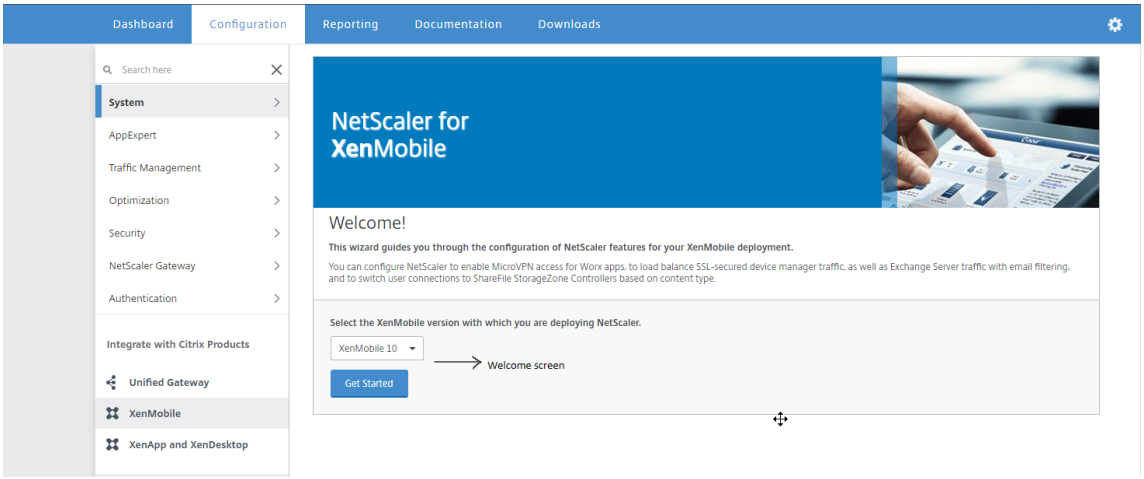
适用于 Citrix Endpoint Management 的 Citrix ADC 向导

本部分提供了使用适用于 Citrix Endpoint Management 的 Citrix ADC 向导的示例：

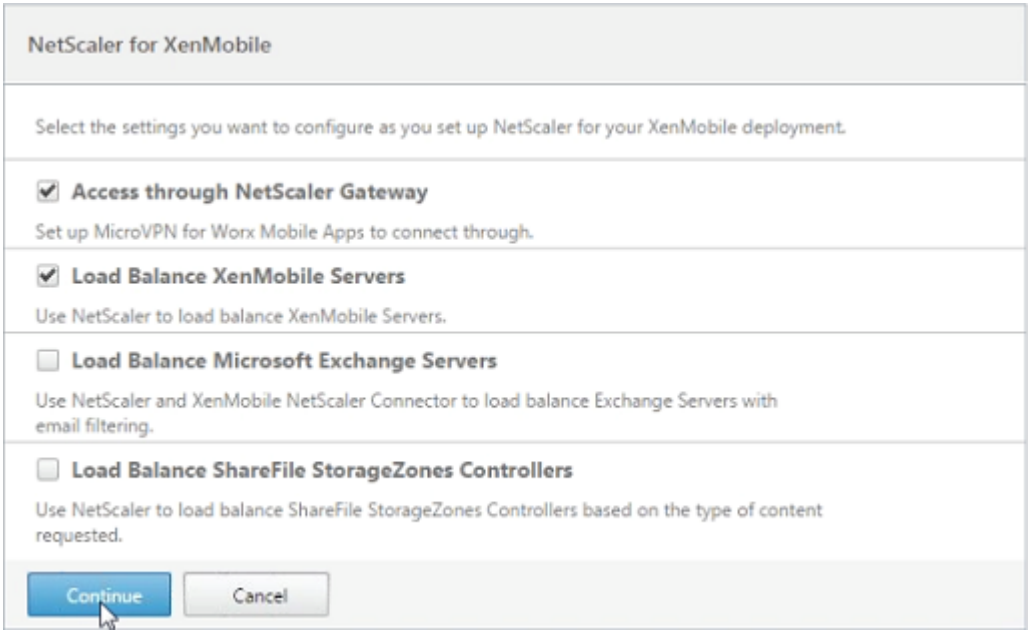
- 为远程用户与您的内部网络中的 Citrix Endpoint Management 托管的资源设置 Micro VPN 访问权限
- 配置基于证书的身份验证。有关获取和安装公用 SSL 证书的信息，请参阅安装和管理证书。
- 为 Citrix Endpoint Management 服务器配置负载平衡。

要使用向导，请执行以下操作：

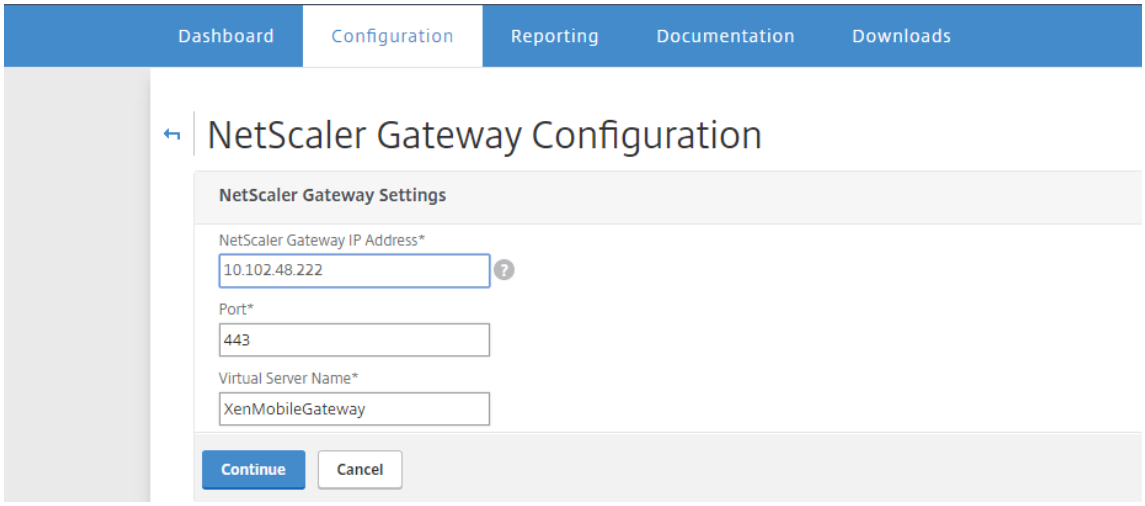
1. 在配置实用程序中，单击配置选项卡，然后单击 **Citrix Endpoint Management**。



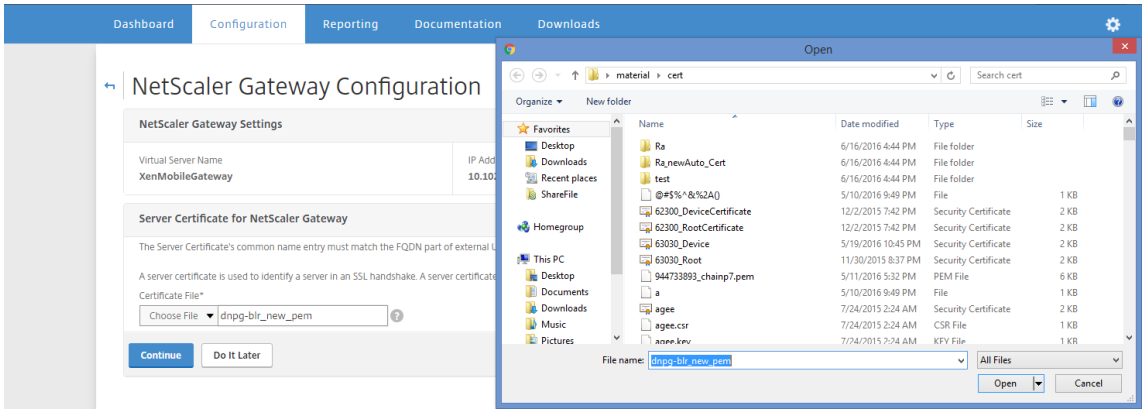
2. 选择 Citrix Endpoint Management 版本，然后单击开始。
3. 选中要配置的功能的复选框。请记住，您只能使用一次此向导，因此您需要手动执行后续配置。这些说明假定您选择了以下设置：通过 **Citrix Gateway** 访问（适用于在 ENT 或 MAM 模式下运行的 Citrix Endpoint Management）
   对 **Citrix Endpoint Management** 服务器进行负载平衡



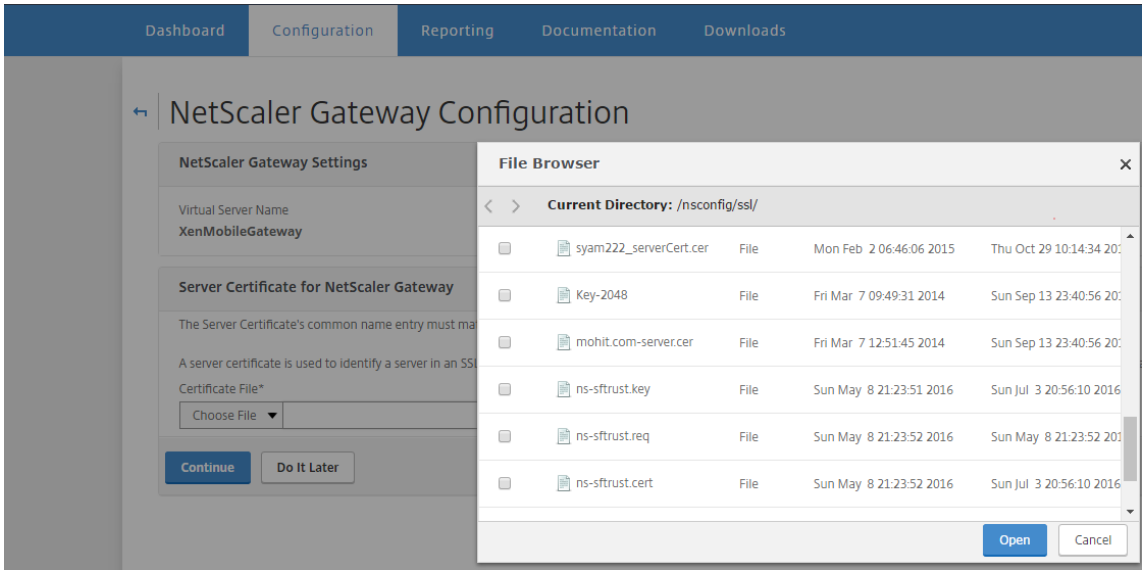
4. 在 **Citrix Gateway** 设置页面上，输入面向外部的 **Citrix Gateway IP** 地址、端口和虚拟服务器名称的值。



5. 在 **Citrix Gateway** 的服务器证书页上，从“证书文件”下拉菜单中，从“本地”或“设备”中选择证书文件。如果您的证书位于本地计算机上：



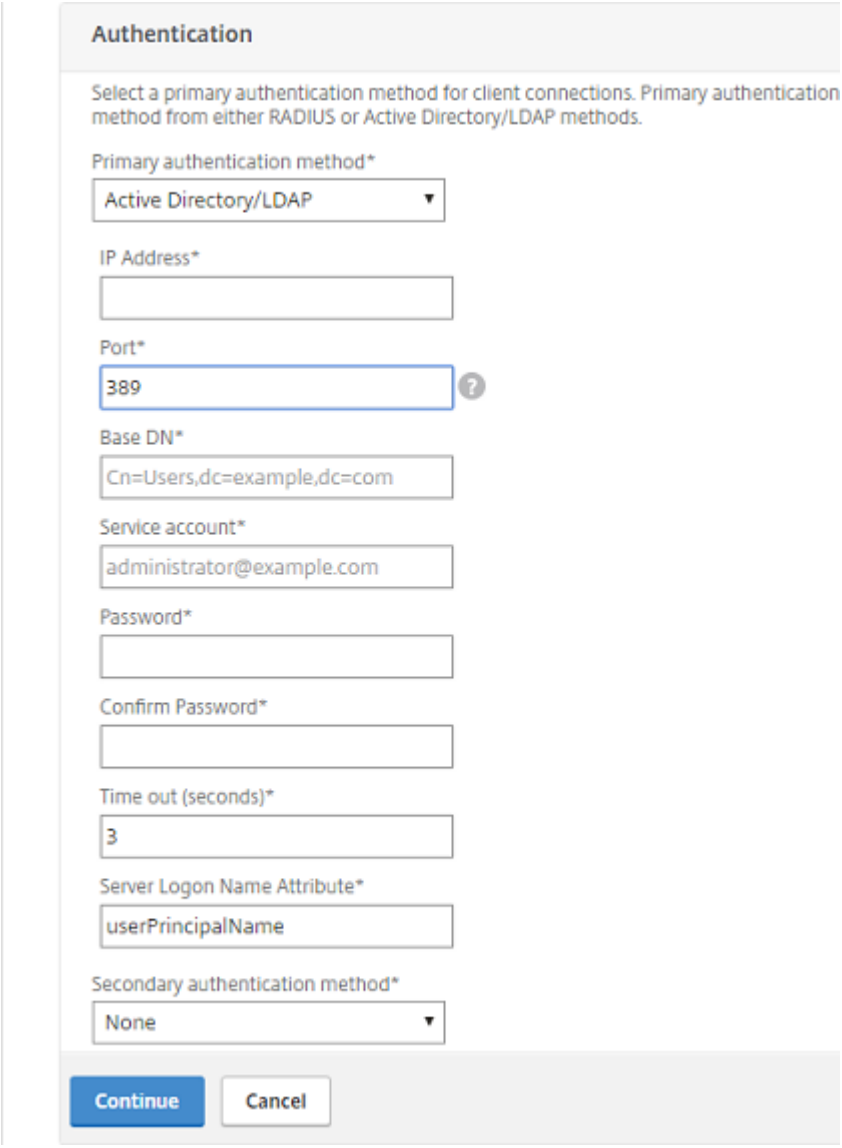
如果您的证书位于设备上：



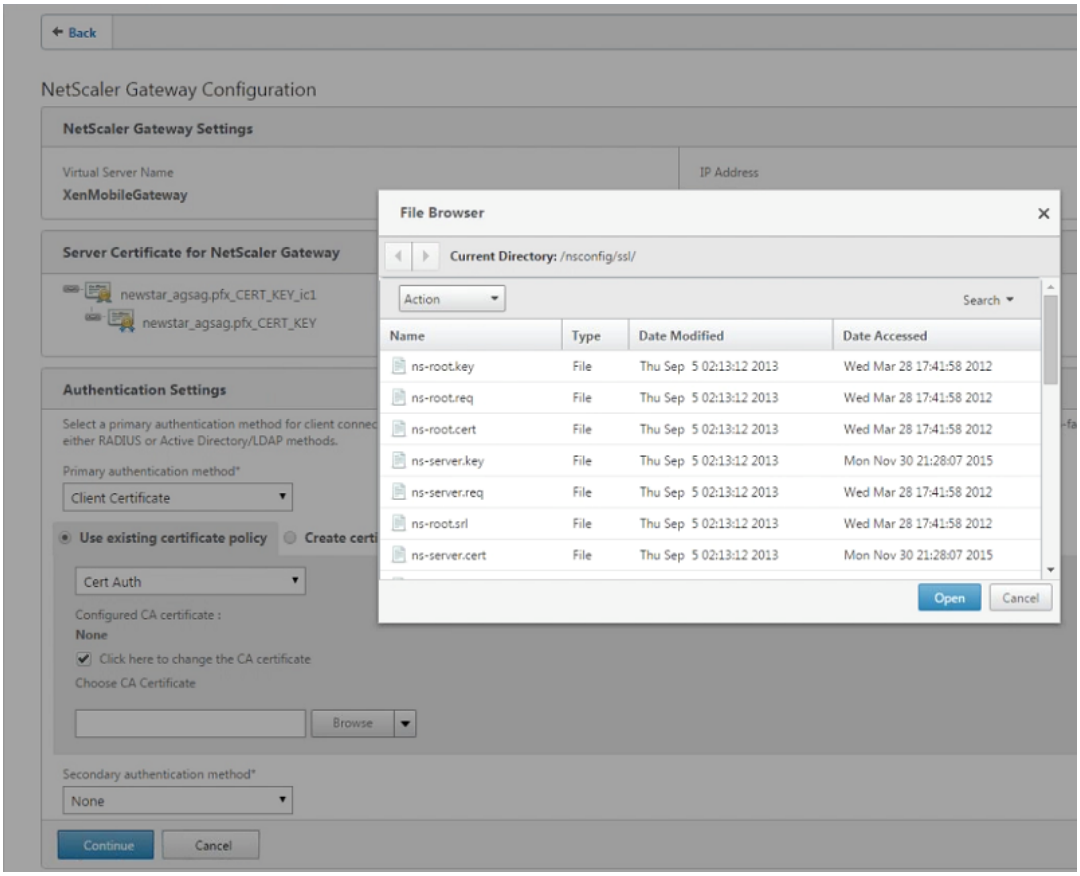
6. 在“身份验证设置”页的“主身份验证方法”字段中，选择“客户端证书”。

这将在接下来的两个字段中自动选择“使用现有证书策略”和“证书 身份验证”。以下步骤假定您已经有证书策略。

如果需要创建证书策略，请单击“创建证书策略”并完成设置。在 **Citrix Endpoint Management** 证书屏幕上，选择现有服务器证书或安装新证书。如果您正在运行多个 Citrix Endpoint Management 服务器，则将为每个服务器添加一个证书。对于服务器登录名称属性，请根据您的要求指定 **userPrincipalName** 或 **samAccountName**。



- a. 选择“单击此处”以更改 **CA** 证书，然后在“浏览”列表中导航到所需的 CA 证书。



- b. 将客户端证书作为主身份验证类型，您可以选择将 LDPA（或 RADIUS）配置为辅助身份验证类型。

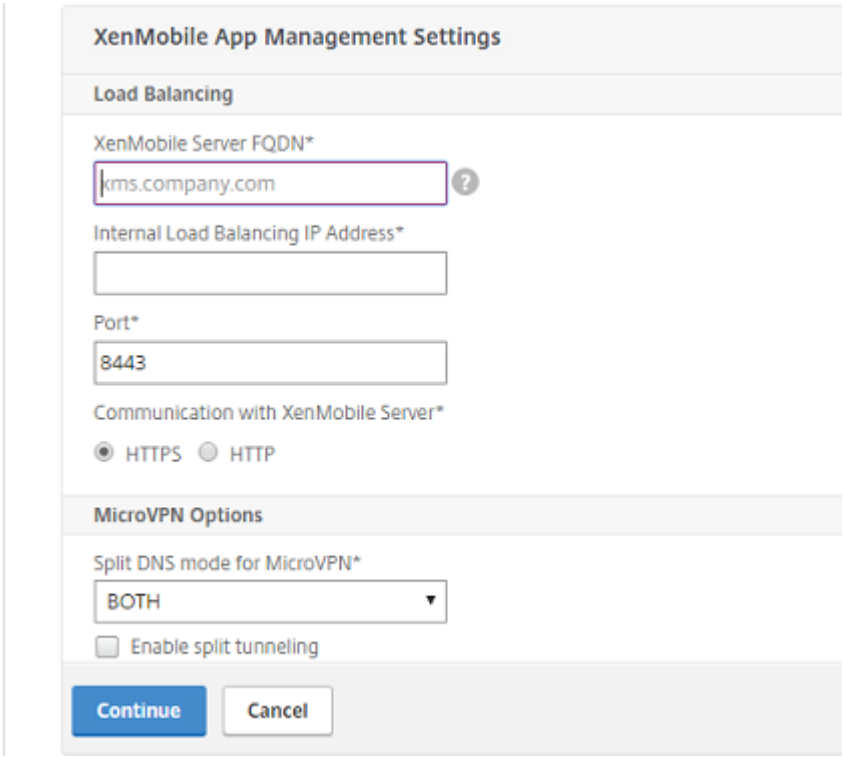
  若要仅使用客户端证书身份验证，请将 第二个身份验证方法保留为 无，然后单击 继续。

  要使用客户端证书 + 域 (LDAP) 身份验证，请将 第二个身份验证方法更改为 **LDAP** 并配置身份验证服务器设置。

- c. 在设备证书屏幕上，如果尚未安装证书，则必须从 Citrix Endpoint Management 控制台导出此证书：在控制台中，单击右上角的齿轮图标以打开设置屏幕。
- d. 单击 证书，然后从列表中选择 CA 证书。
- e. 单击导出。
- f. 返回到 Citrix ADC 向导，然后选择导出（下载）的证书以进行安装。
- g. 单击继续。

此时将显示您配置的 Citrix Endpoint Management IP 地址。

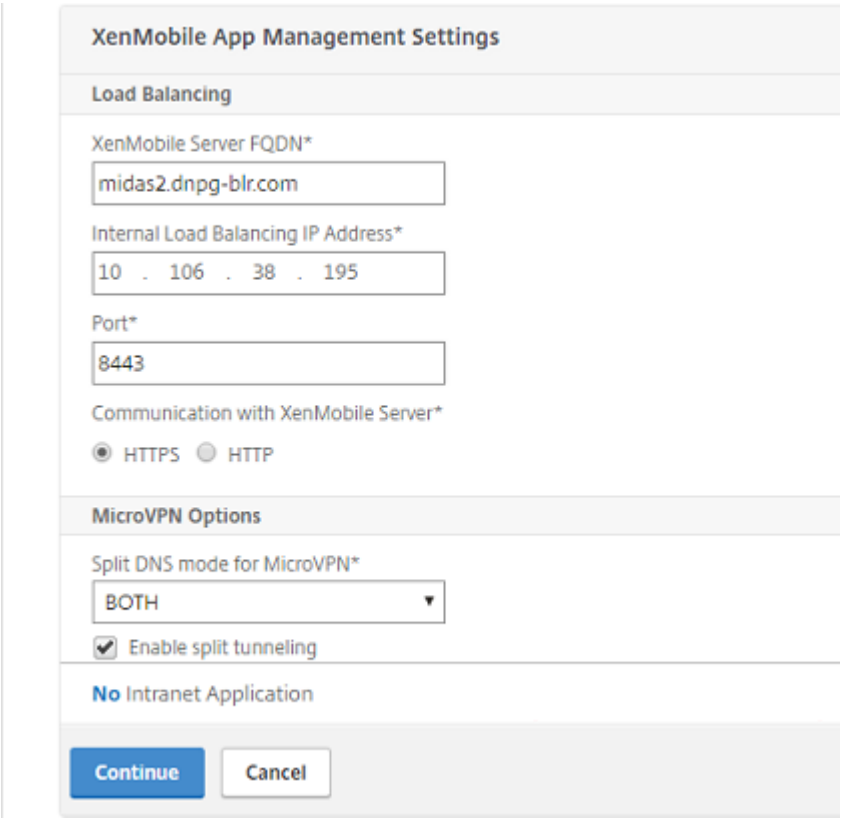
7. 配置 **Citrix Endpoint Management** 应用程序管理设置。



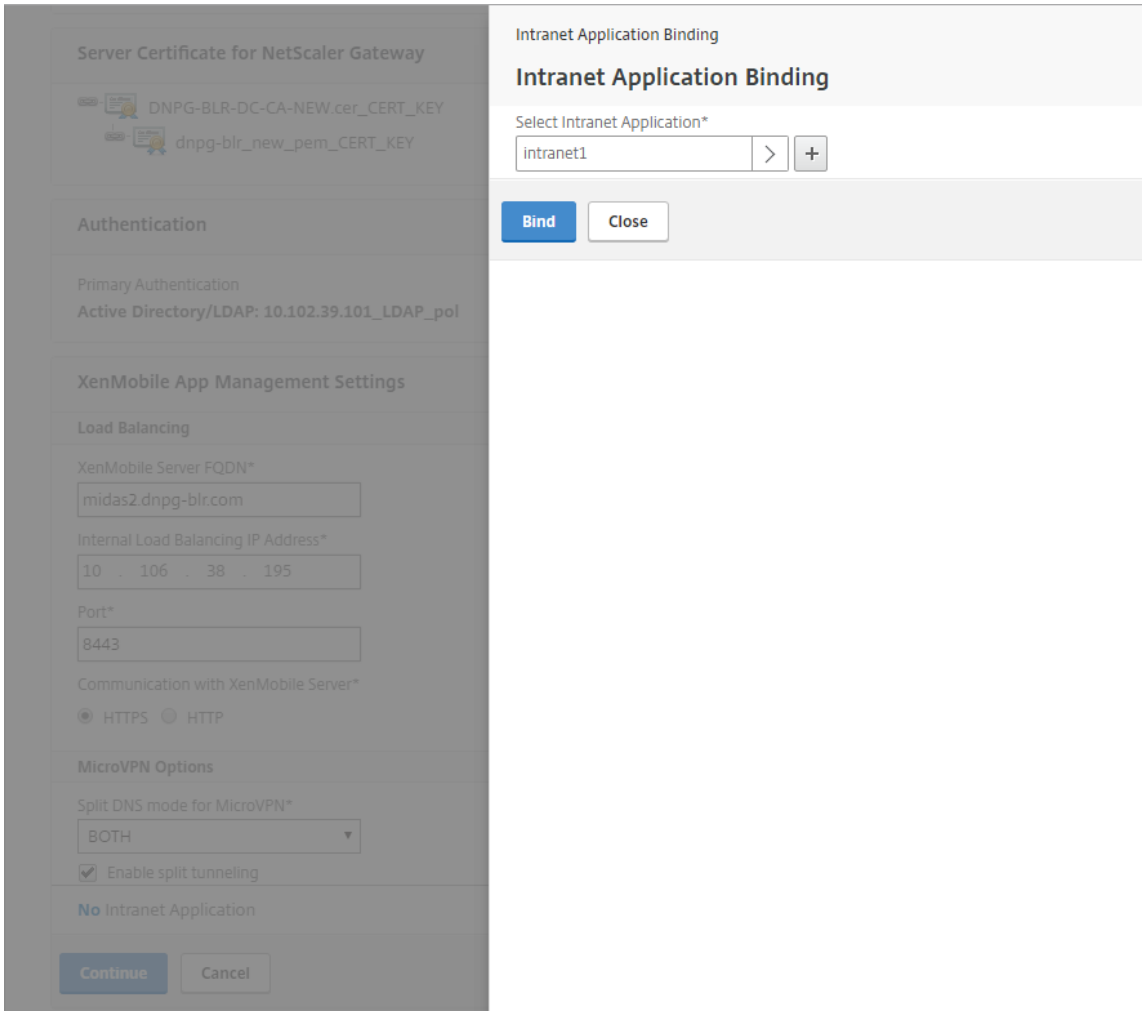
- 输入 **Citrix Endpoint Management FQDN**。这是适用于 MAM 的负载平衡 FQDN。
- 为对 Citrix Endpoint Management 服务器进行负载平衡的虚拟服务器输入仅 MAM 内部负载平衡 **IP** 地址。Citrix Gateway 通过此 MAM 负载平衡虚拟 IP 与 Citrix Endpoint Management 进行通信。
- 这是 SSL 卸载部署，因此，请在与 **Citrix Endpoint Management** 的通信中选择 **HTTP**。
- **MicroVPN** 字段的拆分 **DNS** 模式自动设置为 两者。

如果您的部署需要拆分隧道，请选择“启用拆分隧道”。接下来，如果启用拆分隧道，则必须配置 Intranet 应用程序绑定。

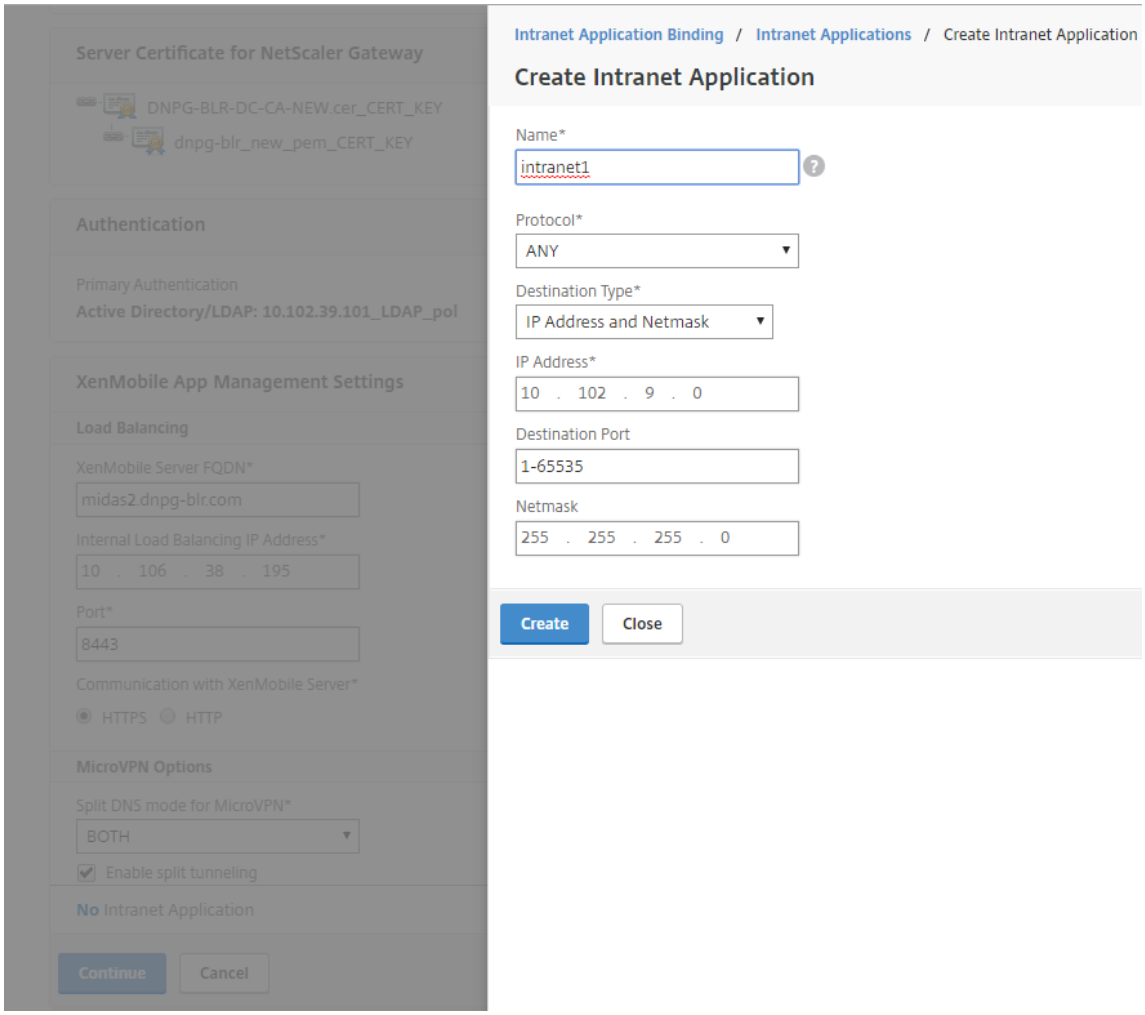
默认情况下，Secure Web 访问通道到内部网络，这意味着 Secure Web 使用每个应用程序的 VPN 通道返回到内部网络进行所有网络访问，Citrix ADC 设备使用拆分通道设置。



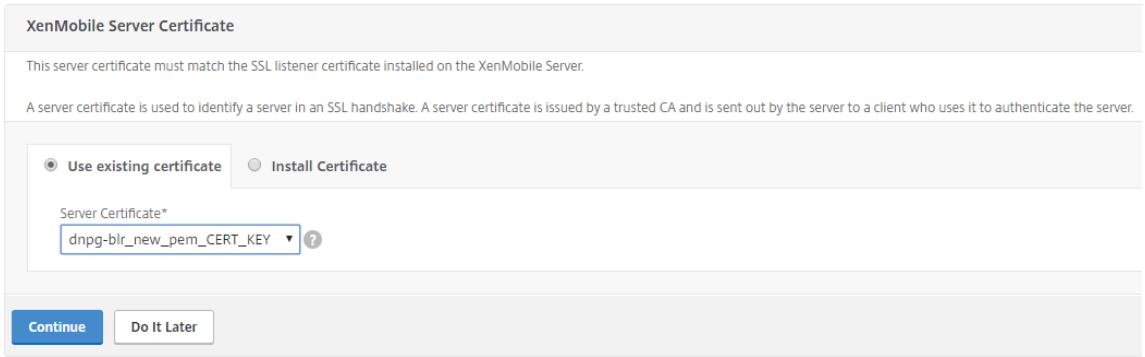
8. 要为 Citrix Gateway 上的用户连接配置拦截规则，必须配置 **Intranet** 应用程序绑定。单击 **+** 以添加绑定。



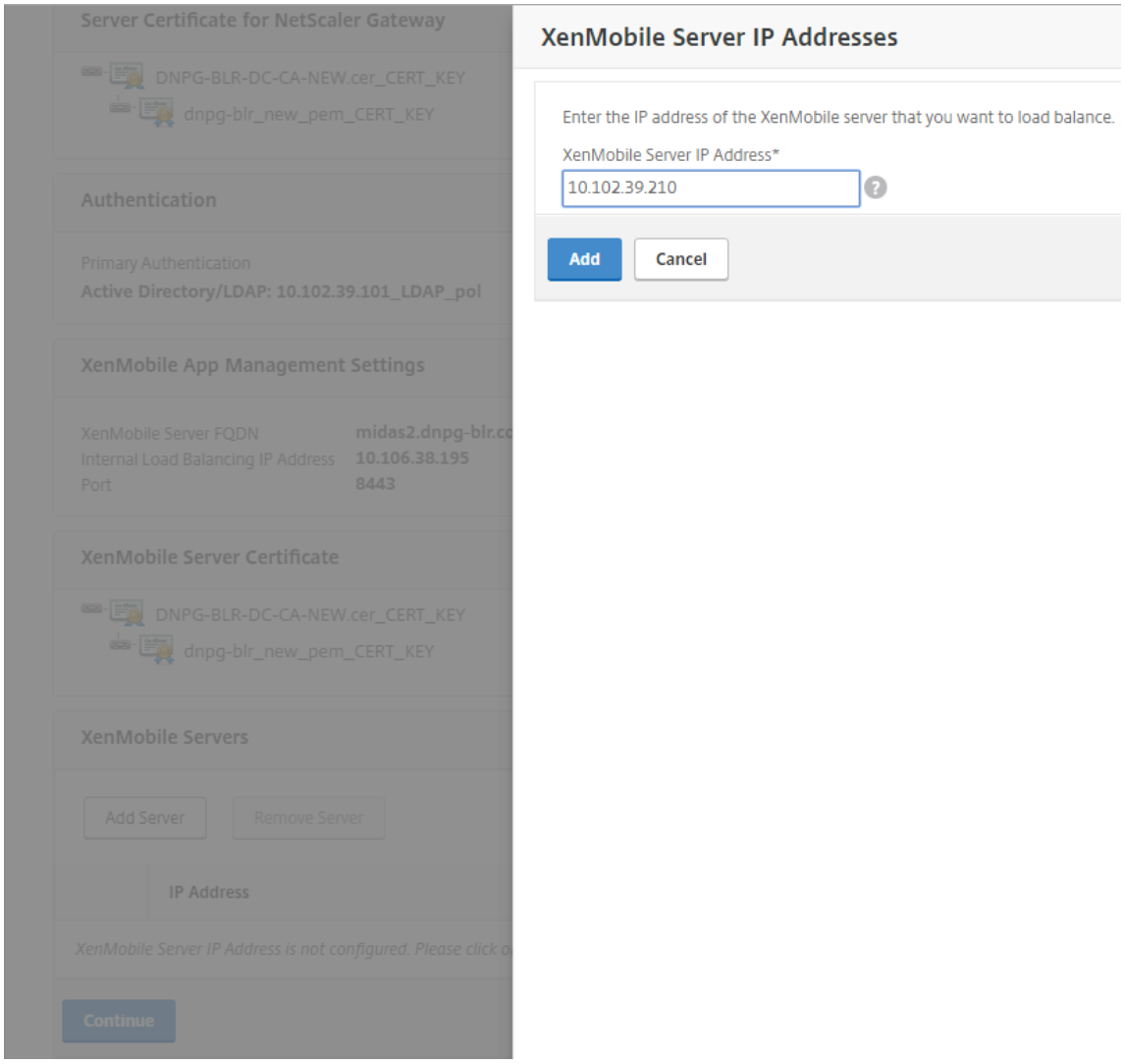
9. 完成允许网络访问的参数，然后单击 创建。



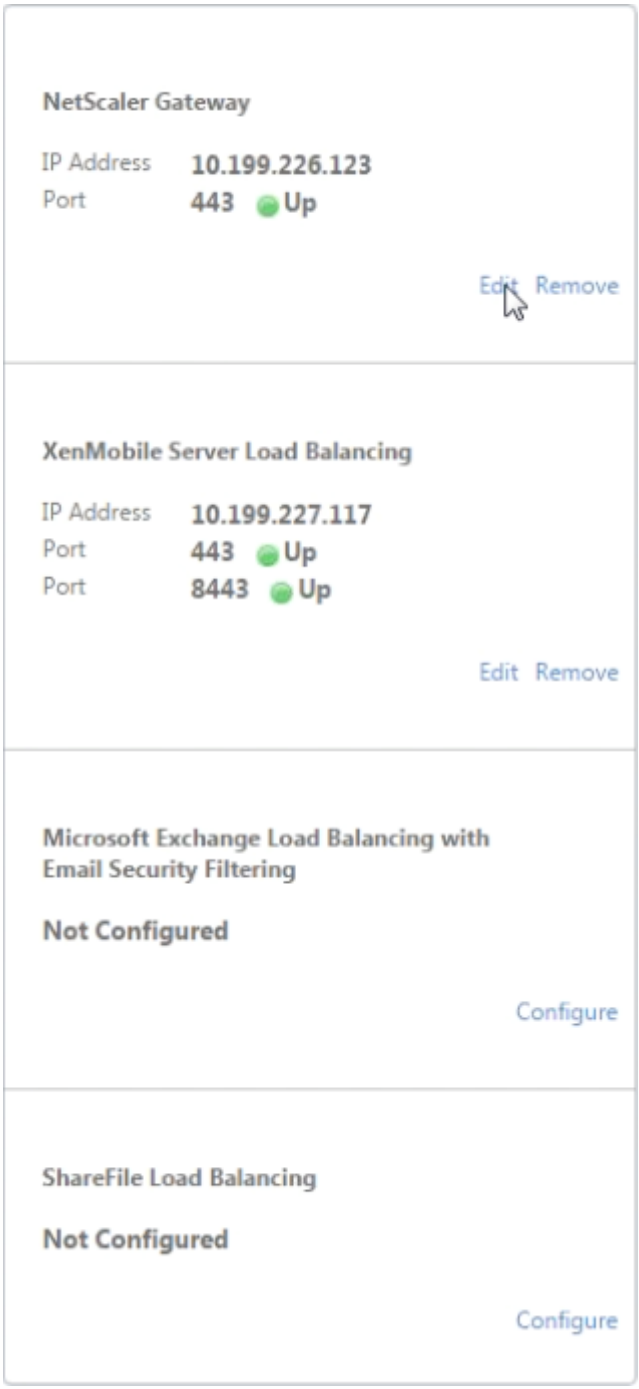
10. 添加 Citrix Endpoint Management 证书。这将用于 MAM 负载平衡虚拟服务器。



11. 在 **Citrix Endpoint Management** 服务器下，单击添加服务器以添加 **Citrix Endpoint Management IP** 地址以绑定到负载平衡虚拟 IP。



12. 在 Citrix ADC 控制板上，确认 Citrix Gateway 和 Citrix Endpoint Management 是否按如下所示进行配置。



如果您将使用用户证书中的 sAMAccount 属性作为用户主体名称 (UPN) 的替代品，请按照中所述配置证书配置文件手动配置 Citrix Gateway 以进行客户端证书身份验证。

为 Citrix Endpoint Management 或 Citrix XenMobile Server 配置负载平衡服务器

April 6, 2020

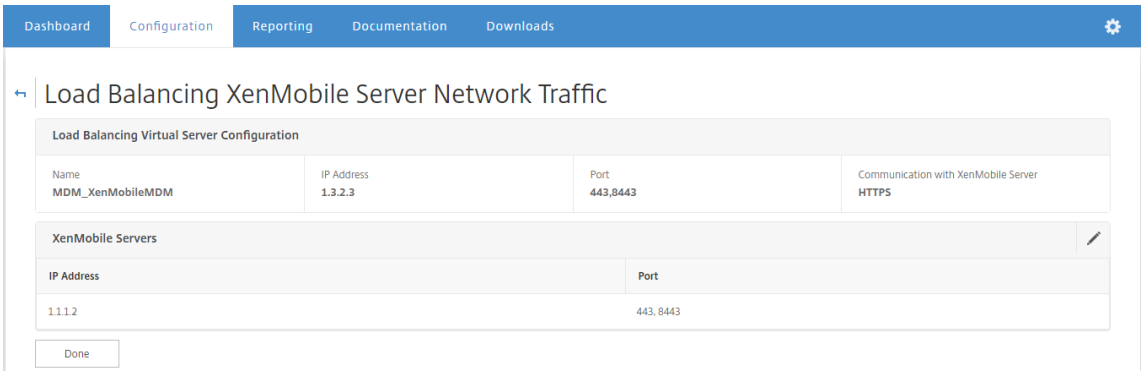
使用适用于 **Citrix Endpoint Management** 的 **Citrix ADC** 向导进行初始设置后，使用 Citrix Gateway 配置实用程序配置负载平衡，如本部分中所述。对于 Citrix Endpoint Management，请使用 SSL 卸载。对于 Citrix Endpoint Management 服务器，请务必参阅将 Citrix Gateway 与 Citrix ADC 相集成中的“部署摘要”下的负载平衡模式建议。

对 Citrix ADC VIP 使用 SSL 桥接模式

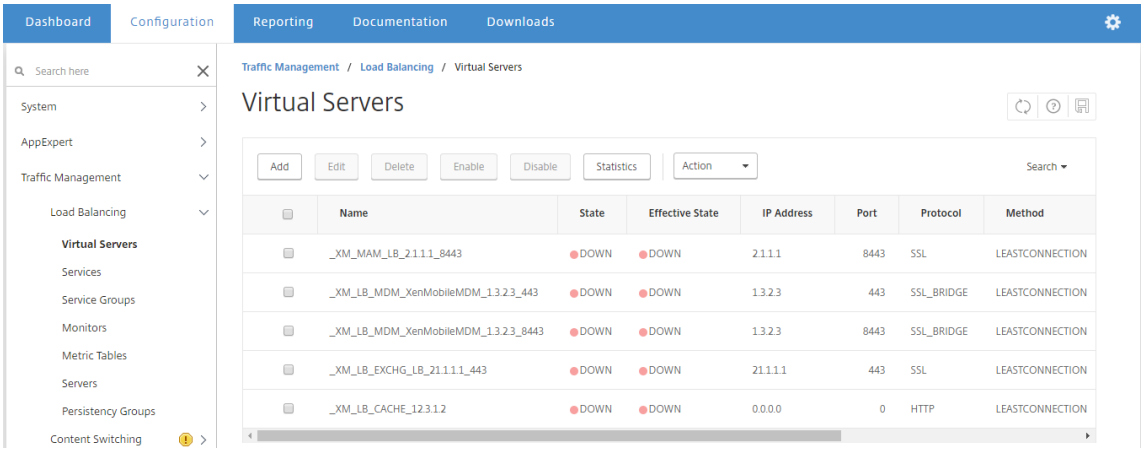
如果 Citrix Endpoint Management 位于 DMZ 中，请使用 SSL 桥接模式。在 SSL 桥接模式下，当 Citrix Endpoint Management 与 Citrix ADC VIP 进行负载平衡时，Internet 流量直接流入 Citrix Endpoint Management 服务器，连接终止。SSL 桥模式是设置和故障排除的最简单模式。

1. 在配置 SSL 桥接模式之前，请转到 **Citrix Endpoint Management** 应用程序管理设置，并验证与 **Citrix Endpoint Management** 服务器的通信是否为 **HTTPS**。

2. 登录到配置实用程序后，在 主页选项卡上的 **MDM** 服务器 **LB** 中，单击 配置。
3. 在“用于设备管理的 **LB** 虚拟服务器”下，在“名称”中键入服务器的名称。
4. 在“**IP** 地址”中，键入虚拟服务器的 IP 地址，然后单击“继续”。
5. 在对 **Citrix Endpoint Management MDM** 服务器进行负载平衡页面上，重复执行步骤 3 和步骤 4，然后单击创建。
6. 验证设置是否正确，然后单击“完成”。



7. 要验证负载平衡配置，请转到 流量管理 > 虚拟服务器。

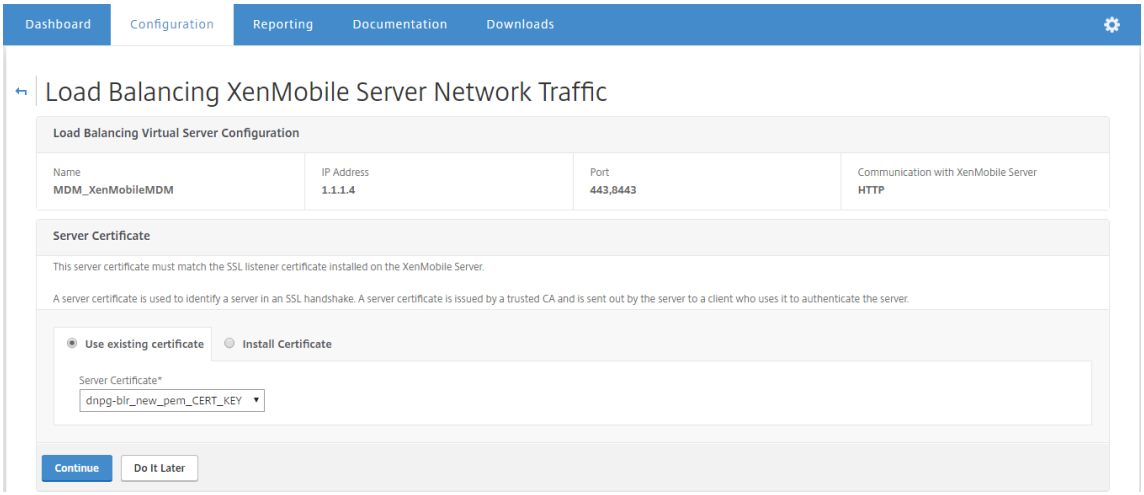


对 **Citrix ADC** 贵宾使用 **SSL** 卸载模式

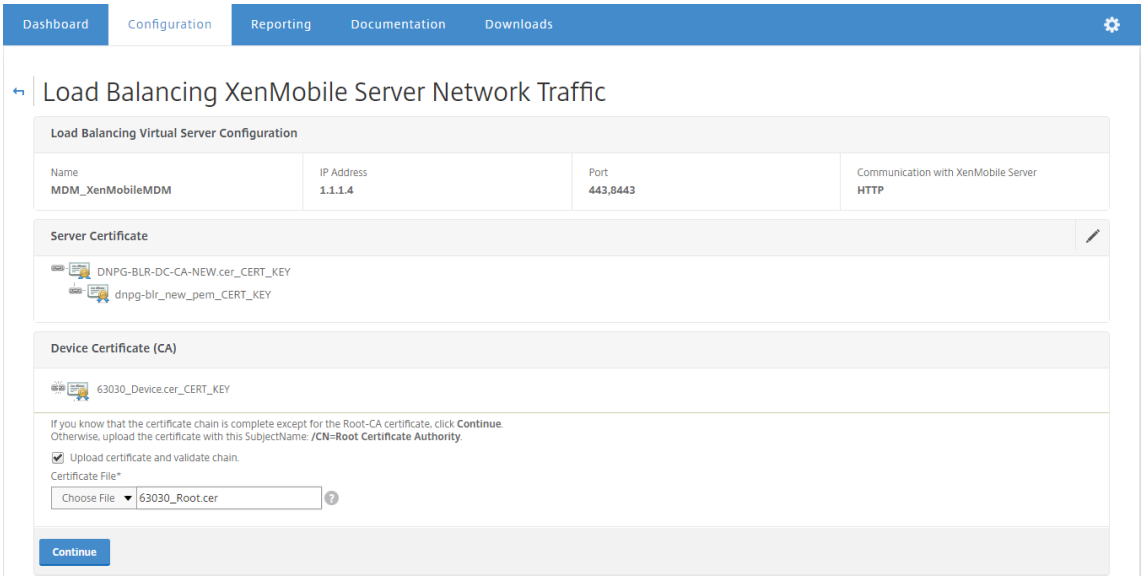
对 Citrix Endpoint Management 使用 SSL 卸载。当本地 Citrix Endpoint Management 位于内部网络中时，如果需要，也可以使用 SSL 卸载（以满足安全标准）。在 SSL 卸载模式下，当 Citrix Endpoint Management 与 Citrix ADC VIP 进行负载平衡时，Internet 流量直接流入 Citrix ADC 设备，连接终止。然后，Citrix Gateway 建立从设备到 Citrix Endpoint Management 的新会话。SSL 卸载模式在安装和故障排除过程中涉及额外的复杂性。

1. 在配置 SSL 卸载模式之前，请转到 **Citrix Endpoint Management** 应用程序管理设置，并验证与 **Citrix Endpoint Management** 服务器的通信是否为 **HTTP**。

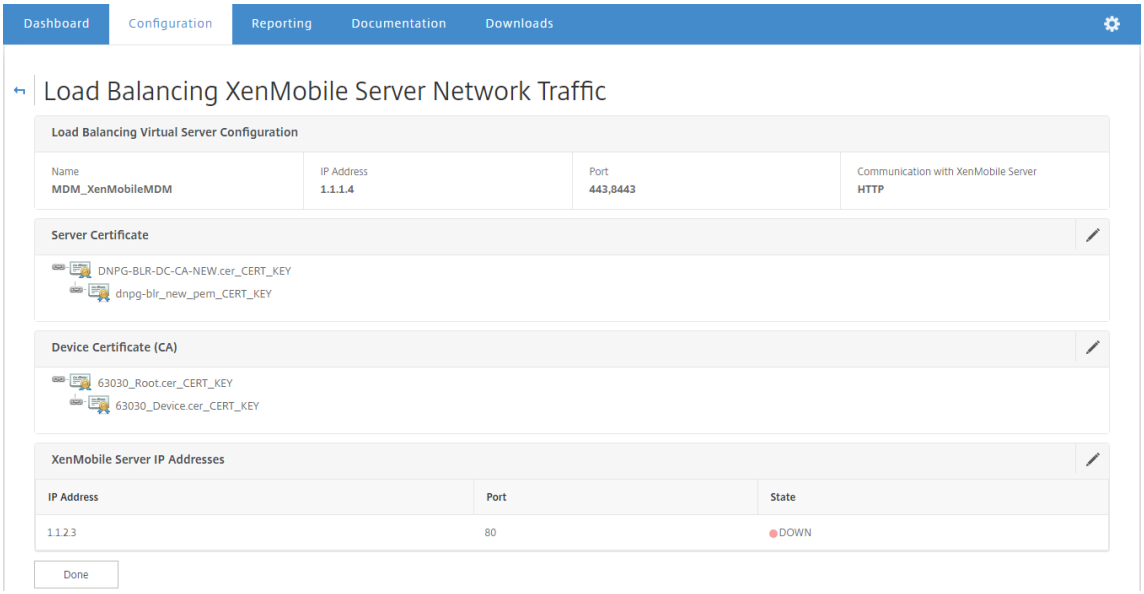
2. 登录到配置实用程序。在主 页选项卡上的 **MDM** 服务器 **LB** 中，单击 配置。
3. 在“用于设备管理的 **LB** 虚拟服务器”下，在“名称”中键入服务器的名称。
4. 在“**IP** 地址”中，键入虚拟服务器的 IP 地址，然后单击“继续”。
5. 在对 **Citrix Endpoint Management MDM** 服务器进行负载平衡页面上，重复执行步骤 3 和步骤 4，然后单击创建。
6. 验证设置，然后单击“完成”。
7. 当提示添加服务器证书时，选择服务器证书，然后单击 继续。



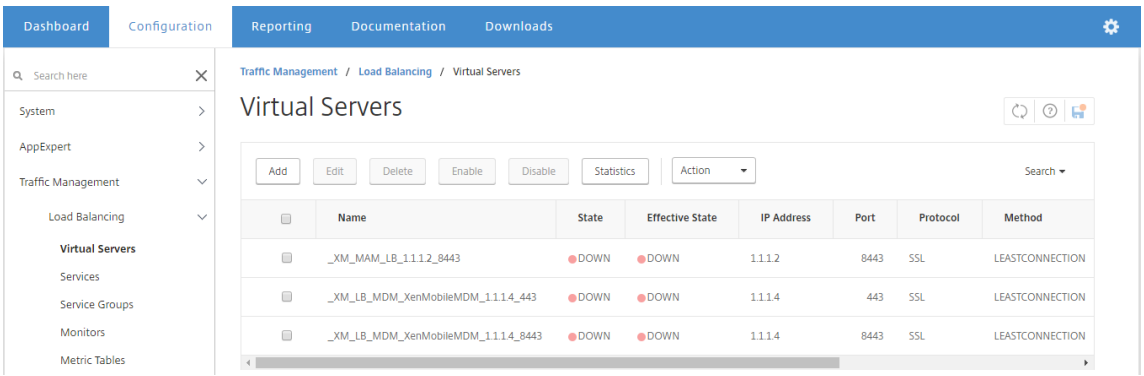
8. 指定 CA 证书，然后单击 继续。



9. 保留相同的 Citrix Endpoint Management IP 地址。单击完成。



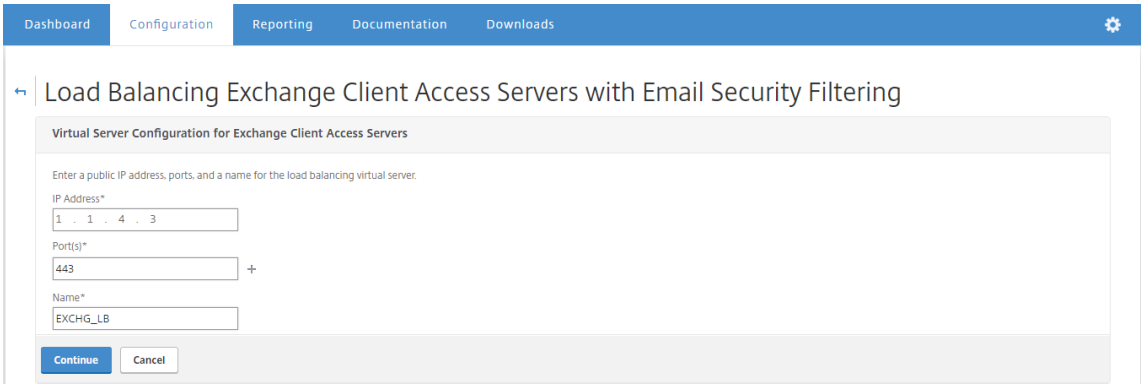
10. 要验证负载平衡配置，请转到 流量管理 **>** 虚拟服务器。



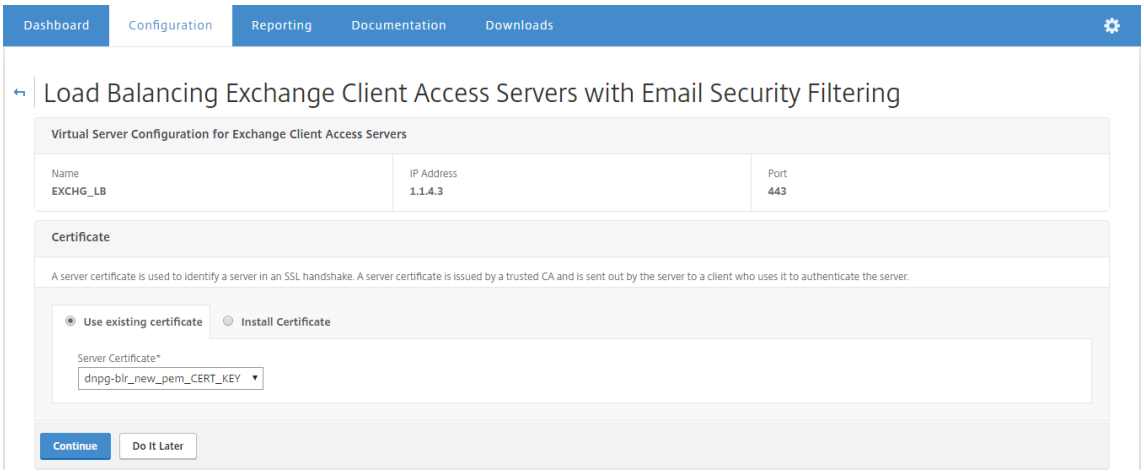
通过电子邮件安全筛选为 **Microsoft Exchange** 配置负载平衡服务器

April 6, 2020

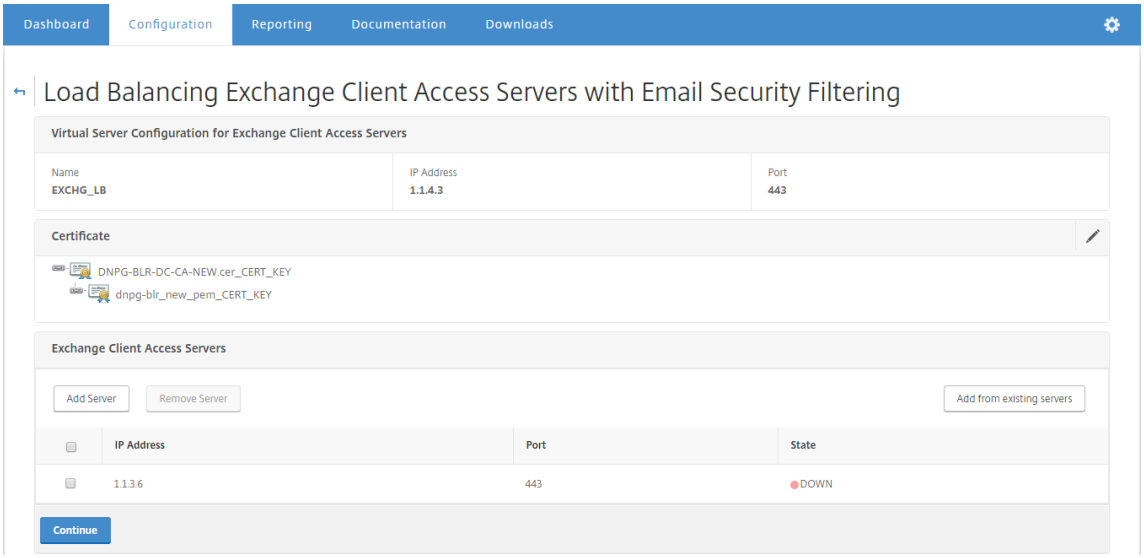
1. 在主 页选项卡上的 **MDM** 服务器 **LB** 中，单击 配置。
2. 在 **Exchange CAS** 的 **LB** 虚拟服务器下，在 名称中键入服务器的名称。
3. 在 “**IP** 地址” 中，键入虚拟服务器的 IP 地址。
4. 在 端口中，键入端口号。要添加更多端口，请单击加号 (**+**)，然后键入端口号。
5. 单击继续。



6. 在“证书”下，选择现有证书或安装计算机（本地）或 Citrix ADC 设备（设备）上的证书。
7. 单击继续。



8. 在 **Exchange CAS** 服务实例下，键入虚拟服务器的名称、IP 地址和端口号。然后，单击 添加并 继续。



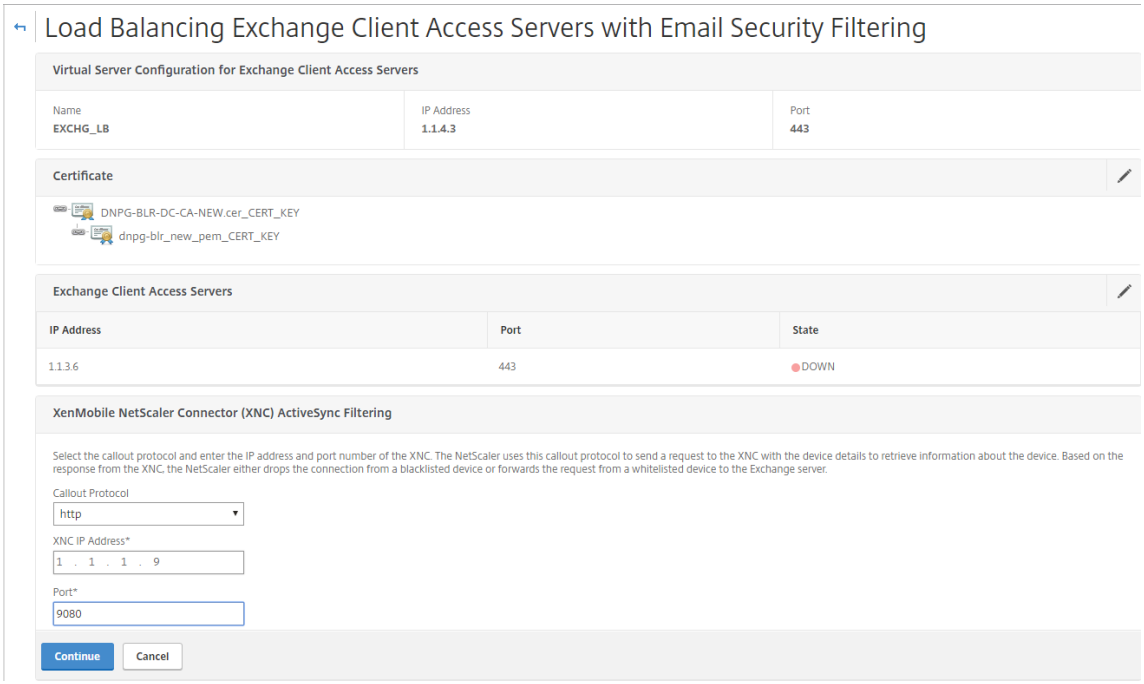
单击完成时，将显示用于配置 Citrix Endpoint Management Citrix ADC Connector (XNC) ActiveSync 过滤的字段。

配置 Citrix Endpoint Management Citrix ADC Connector (XNC) ActiveSync 过滤

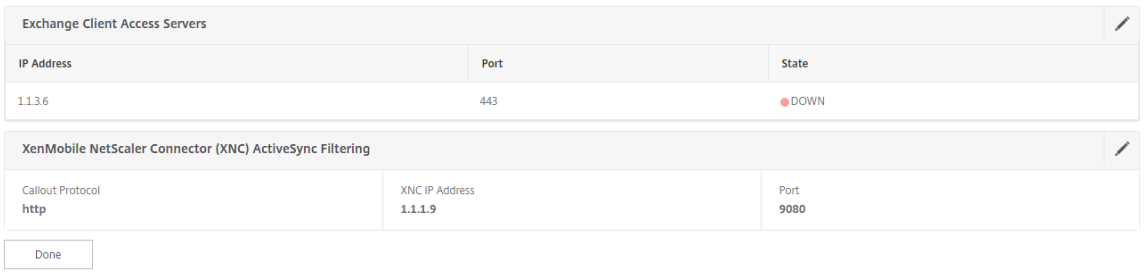
April 6, 2020

Citrix Endpoint Management Citrix ADC Connector (XNC) 向 Citrix ADC 提供 ActiveSync 客户端的设备级别授权服务，而 Citrix ADC 用作 Exchange ActiveSync 协议的反向代理。授权由在 Citrix Endpoint Management 中定义的策略组合以及 XNC 在本地定义的规则控制。

1. 在 **Citrix Endpoint Management Citrix ADC Connector (XNC) ActiveSync** 过滤下，对于标注协议，请选择 **http** 或 **https**。
2. 在 **XNC IP** 地址中，键入 Citrix Endpoint Management Citrix ADC Connector 的 IP 地址。
3. 在 端口中，为 HTTP 网络流量键入 **9080** 或为 HTTPS 网络流量键入 **9443**，然后单击 继续。



将显示您的配置。



通过 **Citrix** 移动生产力应用，允许从移动设备访问

November 3, 2021

适用于 XenMobile 的 Citrix ADC 向导配置了允许用户通过 Citrix Gateway 从受支持的设备连接到内部网络中的移动应用程序和资源所需的设置。用户通过使用 Secure Hub（以前称为 Worx Home）进行连接，该中心建立了一个 Micro VPN 通道。用户连接后，VPN 隧道将打开至 Citrix Gateway，然后将传递给内部网络中的 XenMobile。然后，用户可以从 XenMobile 访问其 Web、移动应用和 SaaS 应用程序。

要确保用户在使用多个设备同时连接到 Citrix Gateway 时使用单个通用许可证，可以在虚拟服务器上启用会话传输。有关详细信息，请参阅 在虚拟服务器上配置连接类型。

如果在使用适用于 XenMobile 的 Citrix ADC 向导后需要更改配置，请使用本文中的部分获取指导。在更改设置之前，请确保您了解更改的含义。有关更多信息，请参阅文XenMobile 部署章。

在 **Citrix Gateway** 中配置安全浏览

您可以更改安全浏览作为全局设置的一部分或作为会话配置文件的一部分。您可以将会话策略绑定到用户、组或虚拟服务器。配置安全浏览时，还必须启用无客户端访问。但是，无客户端访问不需要启用安全浏览。配置无客户端访问时，请将 无客户端访问 **URL** 编码设置为 “清除”。

要在全局配置安全浏览，请执行以下操作：

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 **Citrix Gateway** ，然后单击 “全局设置”。
2. 在详细信息窗格的 “设置” 下，单击 “更改全局设置”。
3. 在 “全局 **Citrix Gateway** 设置” 对话框的 “安全” 选项卡上，单击 “安全 浏览”，然后单 击 “确定”。

要在会话策略和配置文件中配置安全浏览，请执行以下操作：

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 **Citrix Gateway >** 策略，然后单击 “会话”。
2. 在详细信息窗格中，执行以下操作之一：
   - 如果要创建新的会话策略，请单击 “添加”。
   - 如果要更改现有策略，请选择一个策略，然后单击 “打开”。
3. 在策略中，创建新配置文件或修改现有配置文件。为此，请执行以下操作之一：
   - 在请求配置文件旁边，单击新建。
   - 在请求配置文件旁边，单击修改。
4. 在 “安全” 选项卡上的 “安全浏览” 旁边，单击 “覆盖全局”，然后选择 “安全浏览”。
5. 执行以下操作之一：
   - 如果要创建新配置文件，请单击 “创建”，在策略对话框中设置表达式，单击 “创建”，然后单击 “关闭”。
   - 如果您正在修改现有配置文件，请在进行选择后单击 “确定” 两次。

要在安全浏览模式下为 Secure Web 配置流量策略，请执行以下操作：

使用以下步骤配置流量策略，以便在安全浏览模式下通过代理服务器路由 Secure Web 流量。

1. 在配置实用程序中的配置选项卡上，展开 **Citrix Gateway >** 策略，然后单击流量。
2. 在右窗格中，单击“流量配置文件”选项卡，然后单击“添加”。
3. 在“名称”中，输入配置文件的名称，选择 **TCP** 作为协议，并保持其余设置原样。
4. 单击创建。
5. 单击 流量配置文件选项卡，然后单击 添加。
6. 在“名称”中，输入配置文件的名称，然后选择 **HTTP** 作为 协议。
   此流量配置文件适用于 HTTP 和 SSL。根据设计，CVPN 流量是 HTTP 流量，无论目标端口或服务类型如何。因此，您可以在流量配置文件中将 SSL 和 **HTTP** 流量指定为 HTTP。
7. 在 代理中，输入代理服务器的 IP 地址。在 端口中，输入代理服务器的端口号。
8. 单击创建。
9. 单击 流量配置文件选项卡，然后单击 添加。
10. 输入流量策略的名称，对于请求配置文件，选择您在步骤 3 中创建的流量配置文件。输入以下 表达式，然后单击创建：

REQ.HTT HOST 包含 Ac- tiveSync Server	REQ.HTT User- Agent CON- TAINS Worx- Mail	REQ.HTT User- Agent CON- TAINS com.zen	REQ.HTT User- Agent CON- TAINS Worx- Home	REQ.HTT CON- TAINS AGSer- vices	REQ.HTTP.URL CON- TAINS StoreWeb

该规则根据主机标头执行检查。要绕过来自代理的 Activesync 流量，请将 **ActiveSyncServer** 替换为适当的 ActiveSync 服务器名称。

11. 单击 流量配置文件选项卡，然后单击 添加。输入流量策略的名称，对于请求配置文件，选择在步骤 6 中创建的流量配置文件。输入以下 表达式，然后单击 创建：

(REQ.HTTP.HEADE User-Agent CONTAINS Mozilla	REQ.HTTP.HEADEI User-Agent CONTAINS com.citrix.browsei	REQ.HTTP.HEADER User-Agent CONTAINS WorxWeb) && REQ.TCP.DESTPORT == 80

12. 单击 流量配置文件选项卡，然后单击 添加。输入流量策略的名称，对于请求配置文件，选择在步骤 6 中创建的流

量配置文件。输入以下 表达式，然后单击 创建：

(REQ.HTTP.HEADE User-Agent CONTAINS Mozilla	REQ.HTTP.HEADEF User-Agent CONTAINS com.citrix.browse	REQ.HTTP.HEADER User-Agent CONTAINS WorxWeb) && REQ.TCP.DESTPORT == 443

13. 导航到 **Citrix Gateway >** 虚拟服务器，在右窗格中选择虚拟服务器，然后单击编辑。
14. 在 策略行上，单击 **+** 。
15. 从 “选择策略” 菜单中，选择 “流量”。
16. 单击继续。
17. 在 策略绑定下，从 选择策略对面单击 **>**。
18. 选择您在步骤 10 中创建的策略，然后单 击确定。
19. 单击 **Bind**（绑定）。
20. 在 策略下，单击 流量策略。
21. 在 **VPN** 虚拟服务器流量策略绑定下，单击 添加绑定。
22. 在 策略绑定下，在 “选择策略” 菜单旁边，单击 **>** 以查看策略列表。
23. 选择您在步骤 17 中创建的策略，然后单 击确定。
24. 单击 **Bind**（绑定）。
25. 在 策略下，单击 流量策略。
26. 在 **VPN** 虚拟服务器流量策略绑定下，单击 添加绑定。
27. 在 策略绑定下，在 “选择策略” 菜单旁边，单击 **>** 以查看策略列表。
28. 选择您在步骤 18 中创建的策略，然后单 击确定。
29. 单击 **Bind**（绑定）。
30. 单击关闭。
31. 单击完成。

请务必在 XenMobile 控制台中配置 Secure Web (WorxWeb) 应用程序。转到配置 **>** 应用程序，选择 Secure Web 应用程序，单击编辑，然后进行以下更改：

- 在 “应用程序信息” 页面上，将 “初始 **VPN** 模式” 更改为 “安全浏览”。
- 在 **iOS** 页面上，将 初始 **VPN** 模式更改为 安全浏览。
- 在 **Android** 页面上，将 首选 **VPN** 模式更改为 安全浏览。

配置应用程序和 **MDX** 令牌超时

当用户从 iOS 或 Android 设备登录时，会发出应用程序令牌或 MDX 令牌。令牌类似于安全票证机构 (STA)。

您可以设置令牌处于活动状态的秒数或分钟数。如果令牌过期，用户将无法访问请求的资源，例如应用程序或网页。

令牌超时是全局设置。配置设置时，该设置将应用于登录到 Citrix Gateway 的所有用户。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **Citrix Gateway** ，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“全局 **Citrix Gateway** 设置”对话框的“客户端体验”选项卡上，单击“高级设置”。
4. 在“常 规”选项卡上的“应用程序令牌超时 **(**秒**)**”中，输入令牌到期前的秒数。默认值为 **100** 秒。
5. 在 **MDX** 令牌超时（分钟）中，输入令牌到期前的分钟数，然后单 击确定。默认值为 **10** 分钟。

禁用移动设备的端点分析

如果配置终端分析，则需要配置策略表达式，以便终端分析扫描不会在 Android 或 iOS 移动设备上运行。移动设备不支持端点分析扫描。

如果将终端分析策略绑定到虚拟服务器，则必须为移动设备创建辅助虚拟服务器。请勿将身份验证前或身份验证后策略绑定到移动设备虚拟服务器。

在预身份验证策略中配置策略表达式时，您可以添加用户代理字符串以排除 Android 或 iOS。当用户从其中一个设备登录并排除设备类型时，端点分析不会运行。

例如，您创建以下策略表达式来检查用户代理是否包含 Android，如果应用程序病毒.exe 不存在，并结束进程 keylogger.exe（如果它正在使用预身份验证配置文件运行）。策略表达式可能如下所示：

REQ.HTTP.HEADER User-Agent NOTCONTAINS Android && CLIENT.APPLICATION.PROCESS contains	CLIENT.APPLICATION.PROCESS (virus.exe) 包含

创建预身份验证策略和配置文件后，将策略绑定到虚拟服务器。当用户从 Android 或 iOS 设备登录时，扫描不会运行。如果用户从基于 Windows 的设备登录，则扫描将运行。

有关配置预身份验证策略的更多信息，请参阅配置终端策略。

通过对 **Android** 设备使用 **DNS** 后缀支持 **DNS** 查询

当用户从 Android 设备建立微型 VPN 连接时，Citrix Gateway 会向用户设备发送拆分 DNS 设置。Citrix Gateway 支持基于您配置的拆分 DNS 设置的拆分 DNS 查询。Citrix Gateway 还可以支持基于您在设备上配置的 DNS 后缀的拆分 DNS 查询。如果用户从 Android 设备连接，则必须在 Citrix Gateway 上配置 DNS 设置。

拆分 DNS 的工作方式如下：

- 如果将拆分 DNS 设置为本地，Android 设备将所有 DNS 请求发送到本地 DNS 服务器。
- 如果将拆分 DNS 设置为远程，则所有 DNS 请求都会发送到 Citrix Gateway （远程 DNS 服务器）上配置的 DNS 服务器以进行解析。
- 如果将拆分 DNS 设置为两者，Android 设备将检查 DNS 请求类型。
  - 如果 DNS 请求类型不是 “A”，它将 DNS 请求数据包发送到本地和远程 DNS 服务器。
  - 如果 DNS 请求类型为 “A”，则 Android 插件将提取查询 FQDN 并将该 FQDN 与 Citrix ADC 上配置的 DNS 后缀列表匹配。如果 DNS 请求的 FQDN 匹配，则 DNS 请求将发送到远程 DNS 服务器。如果 FQDN 不匹配，则 DNS 请求将发送到本地 DNS 服务器。

下表总结了基于类型 A 记录和后缀列表的拆分 DNS 工作。

拆分 DNS 设置	这是 A 型记录吗？	它是否在后缀列表上？	DNS 请求的发送位置
本地	“是” 或 “否”	“是” 或 “否”	本地
远程	“是” 或 “否”	“是” 或 “否”	远程
都	否	不适用	都
都	是	是	远程
都	是	否	本地

要配置 DNS 后缀，请执行以下操作：

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 **Citrix Gateway >** 策略，然后单击 “会话”。
2. 在详细信息窗格的 “策略” 选项卡上，选择会话策略，然后单击 “打开”。
3. 在请求配置文件旁边，单击修改。
4. 在 “网络配置” 选项卡上，单击 “高级”。
5. 在 **Intranet IP DNS** 后缀旁边，单击 覆盖全局，键入 DNS 后缀，然后单 击确定三次。

要在 Citrix Gateway 上全局配置拆分 DNS：

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 **Citrix Gateway** ，然后单击 “全局设置”。
2. 在详细信息窗格的 “设置” 下，单击 “更改全局设置”。
3. 在 客户端体验选项卡上，单击 高级设置。
4. 在 “常规” 选 项卡上的 “拆分 **DNS**” 中，选择 “同时”、“远程” 或 “本地”，然后单 击 “确定”。

要在 Citrix Gateway 上的会话策略中配置拆分 DNS，请执行以下操作：

1. 在配置实用程序中的 “配置” 选项卡的导航窗格中，展开 **Citrix Gateway >** 策略，然后单击 “会话”。
2. 在详细信息窗格的 “策略” 选项卡上，单击 “添加”。
3. 在 “名称” 中，键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在 “名称” 中，键入配置文件的名称。

6. 在 客户端体验选项卡上，单击 高级设置。
7. 在 “常规” 选 项卡上，在 “拆分 **DNS**” 旁边，单击 “覆盖全局”，选择 “同时”、“远程” 或 “本地”，然后单 击 “确定”。
8. 在 “创建会话策略” 对话框的 命名表达式旁边，选择 “常 规”，选择 “**True**”，单击 “添加表达式”，单击 “创建”，然后单击 “关闭”。

为 **Citrix Endpoint Management** 配置域和安全令牌身份验证

April 6, 2020

可以将 Citrix Endpoint Management 配置为要求用户通过 RADIUS 协议使用其 LDAP 凭据以及一次性密码进行身份验证。本节介绍该双重身份验证类型所需的 Citrix Gateway 配置。

必备条件

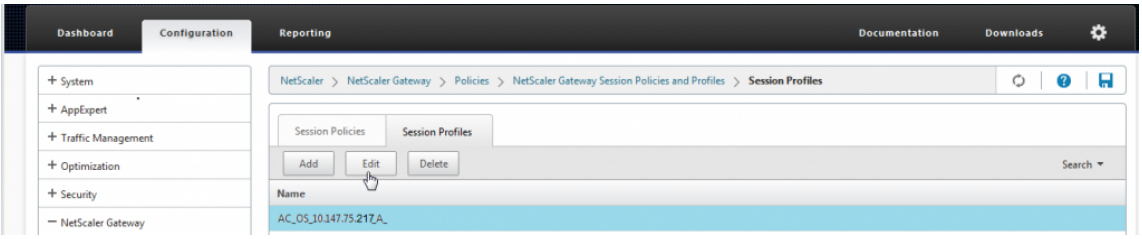
如果尚未运行适用于 Citrix Endpoint Management 的 Citrix ADC 向导，请参阅为 Citrix Endpoint Management 环境配置设置中的适用于 *Citrix Endpoint Management* 的 *Citrix ADC* 向导部分。确保 Citrix ADC 配置包含以下内容：

- **LDAP** 端口号 = **636** （这是安全 LDAP 连接的默认端口）
- 服务器登录名属性 = **samAccountName** 或 **userPrincipalName**，具体取决于您的要求

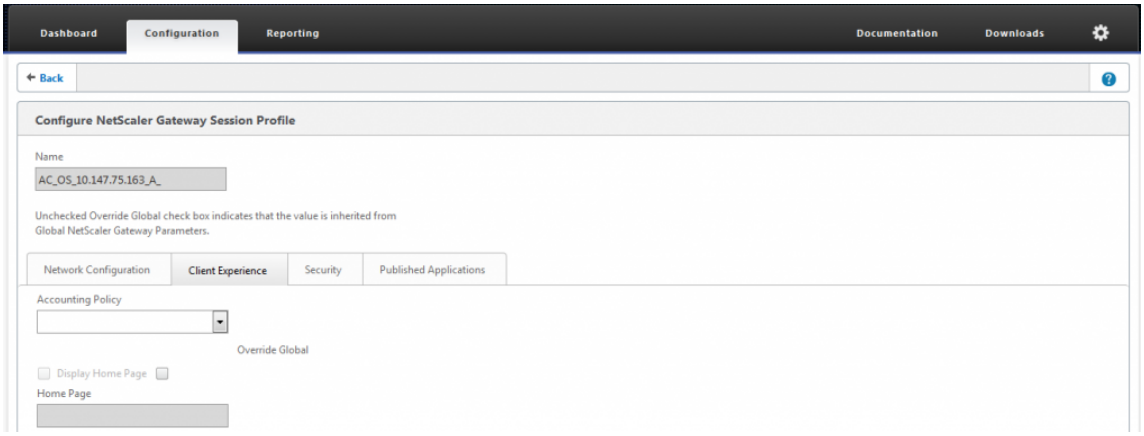
配置域和安全令牌身份验证

1. 转到 **Citrix Gateway >** 虚拟服务器。选择虚拟服务器，然后单击 编辑。
2. 点击 无 **CA** 证书。
3. 从 “选 择 **CA** 证书” 中，选择一个证书，单 击 **“**确定”，单击 “绑定”，然后单击 “完成”。

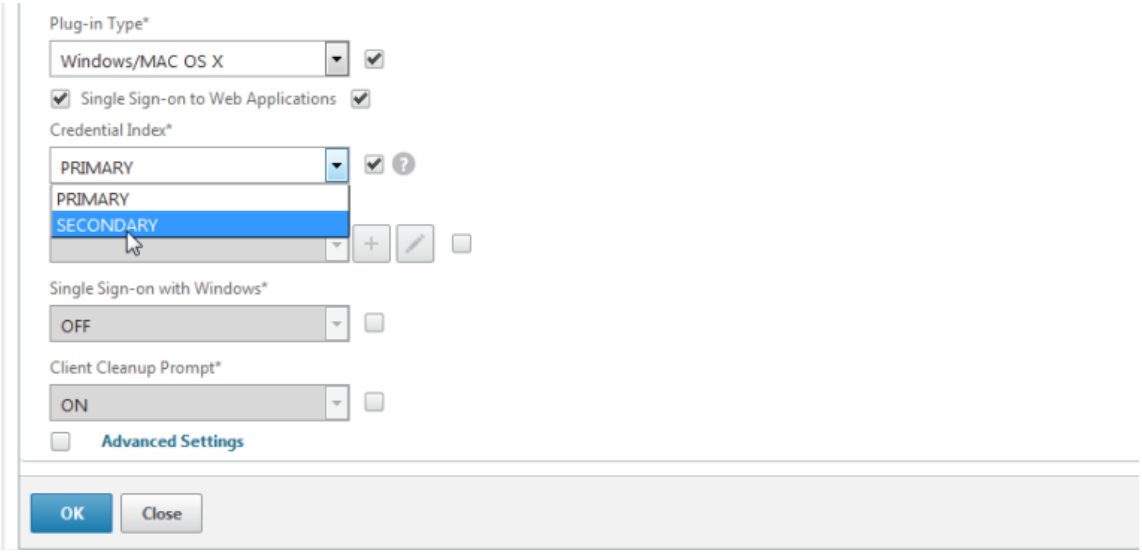
4. 转到“策略”>“会话”>“会话配置文件”，选择以 **AC_OS** 开头的配置文件，然后单击“编辑”。



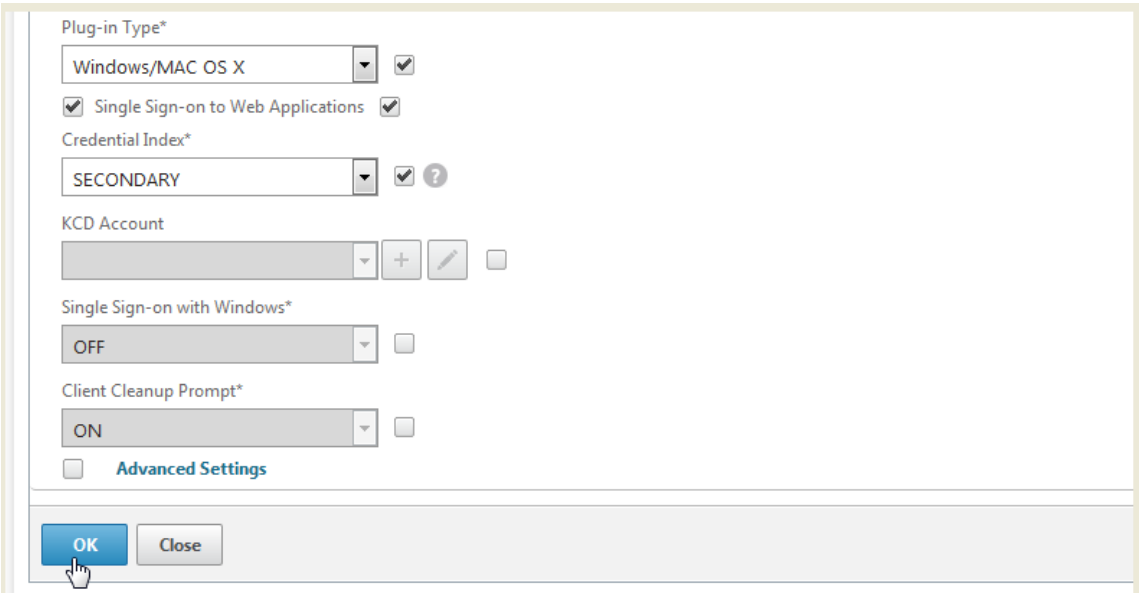
5. 单击 客户体验选项卡，然后转到页面底部。



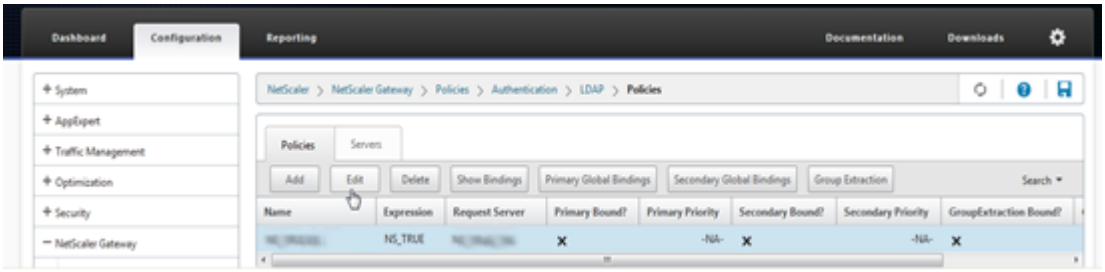
6. 从 凭据索引中，选择“辅助”。



7. 单击确定。

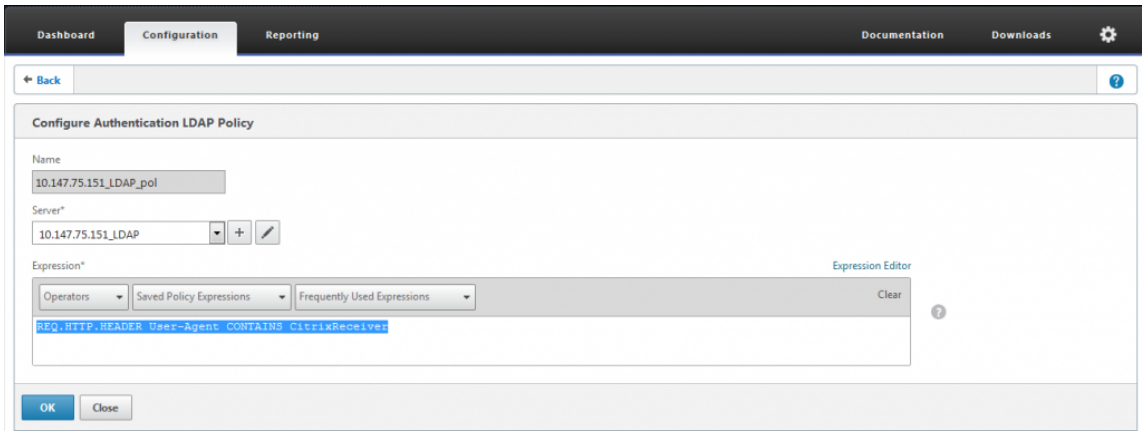


8. 转到“策略”>“身份验证”>“**LDAP** 策略”选项卡，然后单击“编辑”。

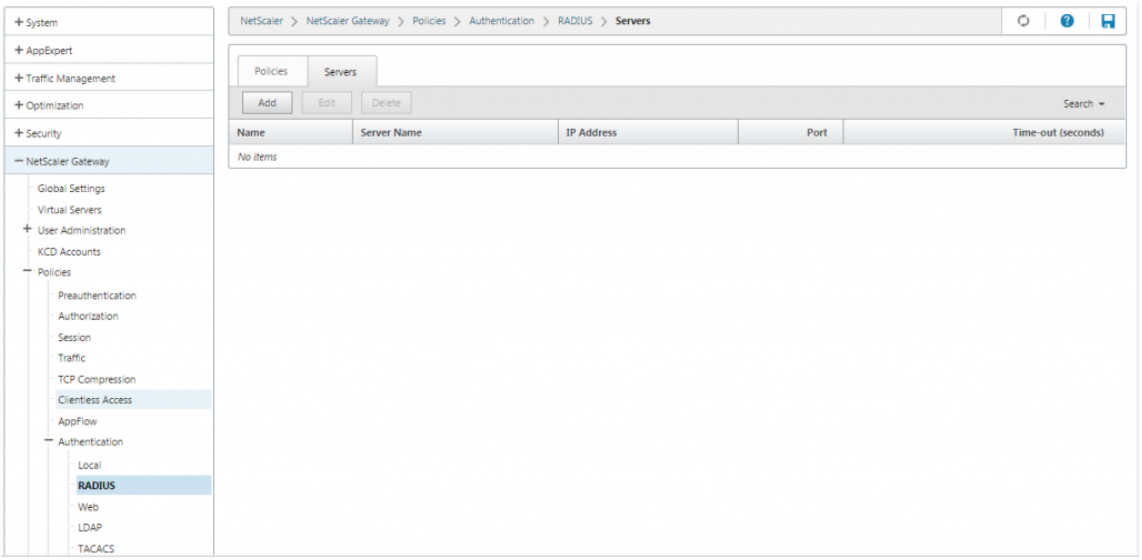


9. 要对 Citrix Endpoint Management 和 Citrix Virtual Apps and Desktops 使用单独的 Citrix Gateway VIP，请在表达式中将 **NS_TRUE** 替换为以下内容：

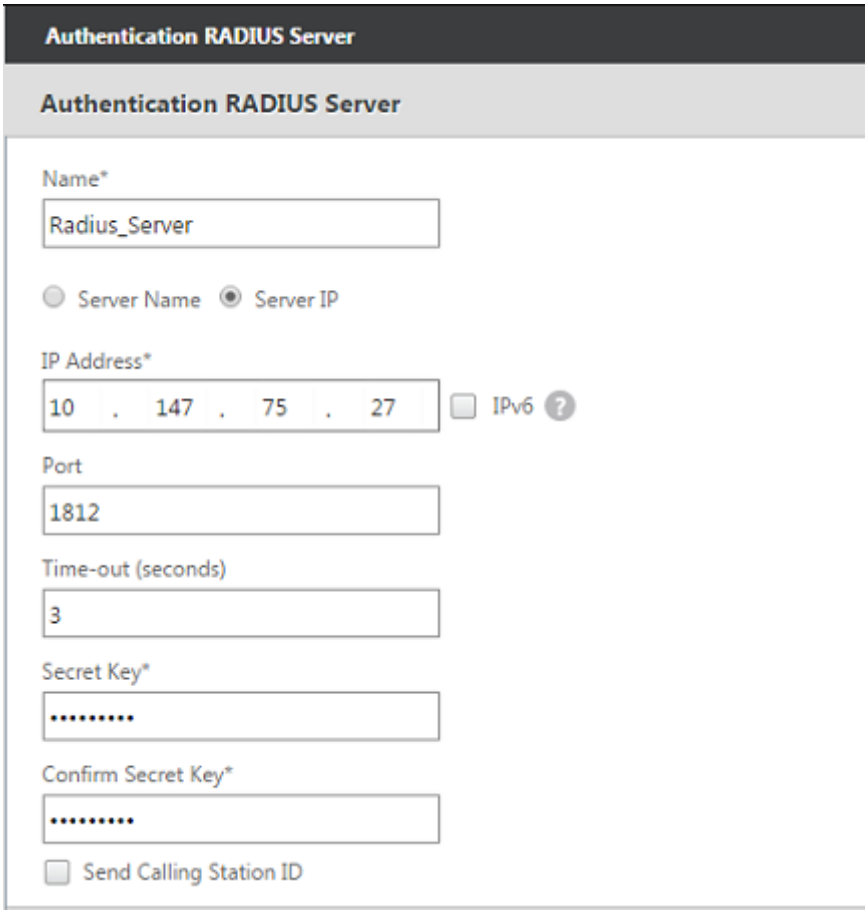
REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver



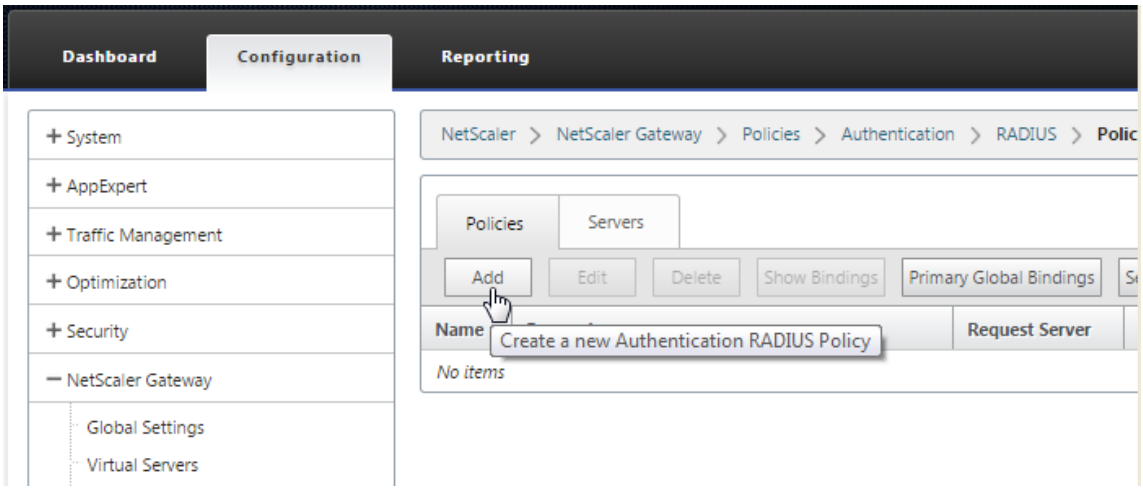
10. 转到 “策略”>“身份验证”>“**RADIUS**”，然后单击 “服务器” 选项卡。



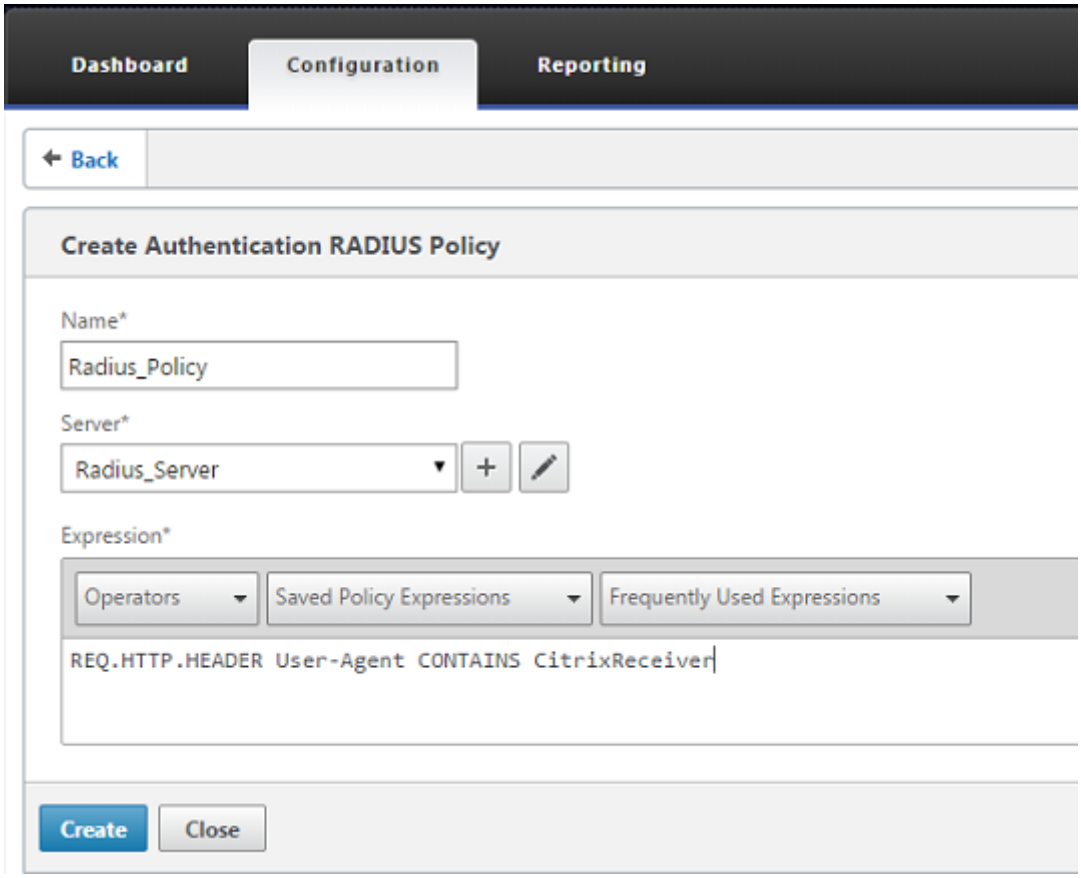
11. 单击 添加，输入 Radius 服务器详细信息，然后单击 创建。



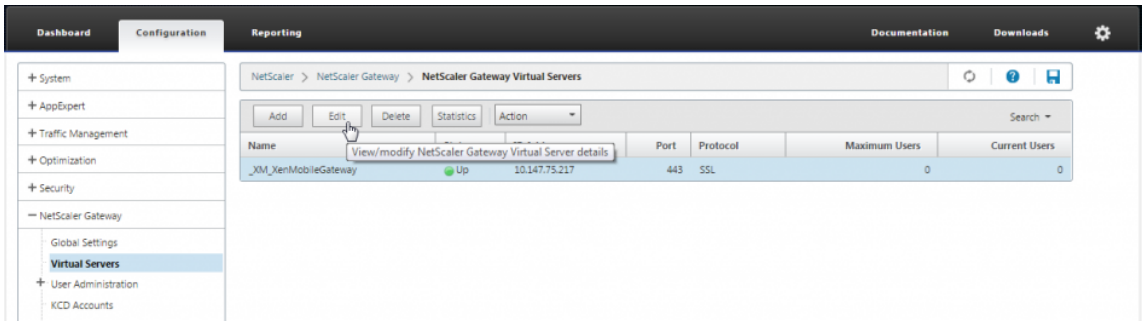
12. 转到 策略，然后单击 添加。



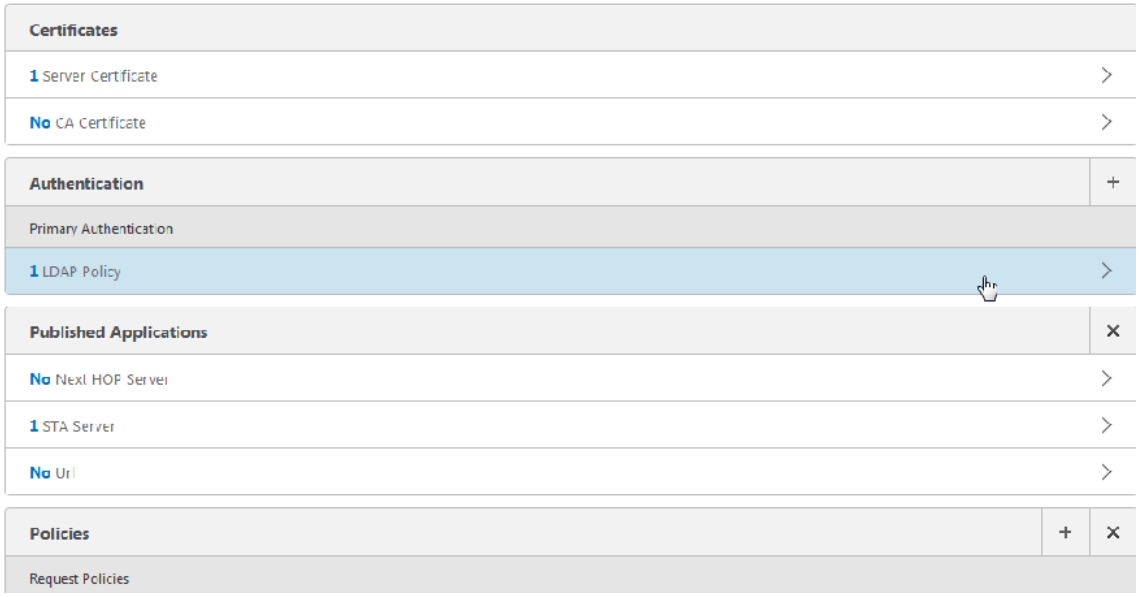
13. 输入策略的 名称。从服务器下拉菜单中，选择 Radius 服务器名称（在我们的示例中为 **Radius_Server**）。
14. 对于表达式，输入 **REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver**，然后单击创建。



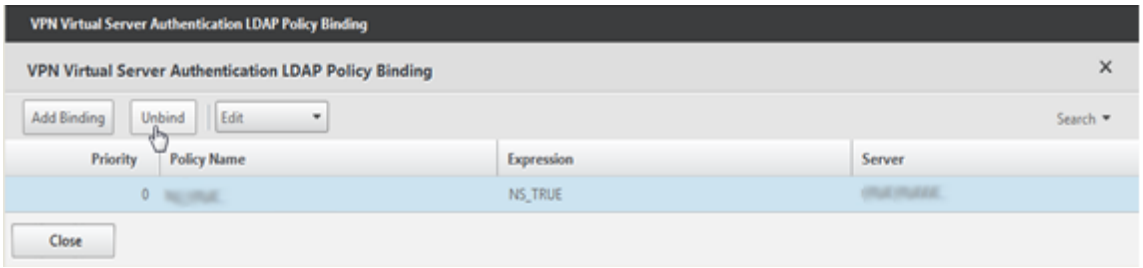
15. 选择虚拟服务器，然后单击 编辑。



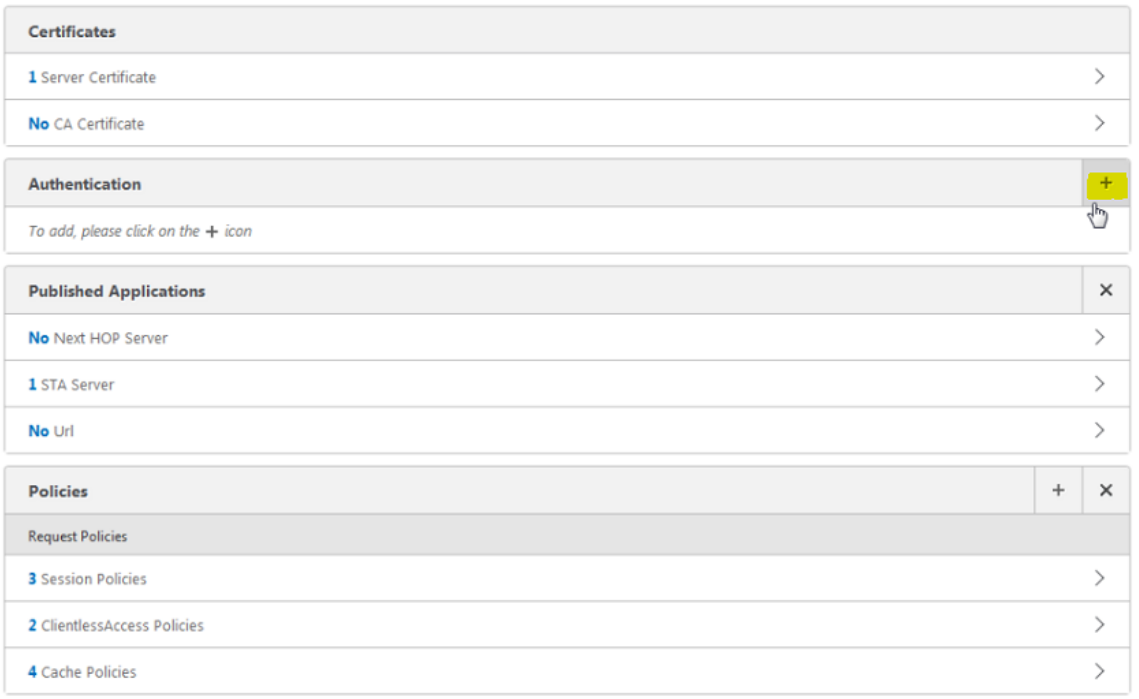
16. 在 主身份验证下，单击 **LDAP** 策略。



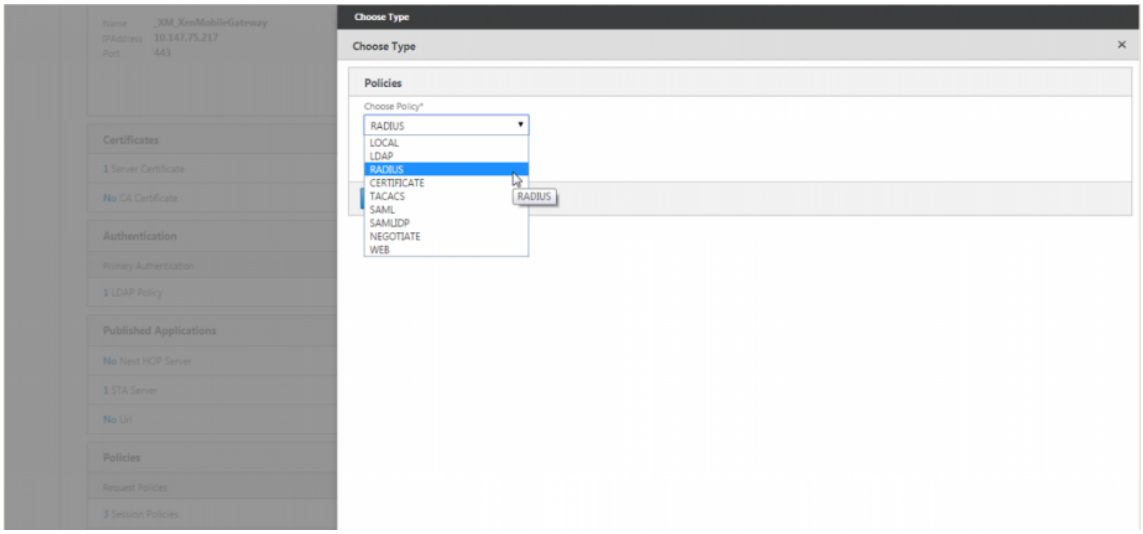
17. 选择策略，单击 取消绑定，然后单击 关闭。



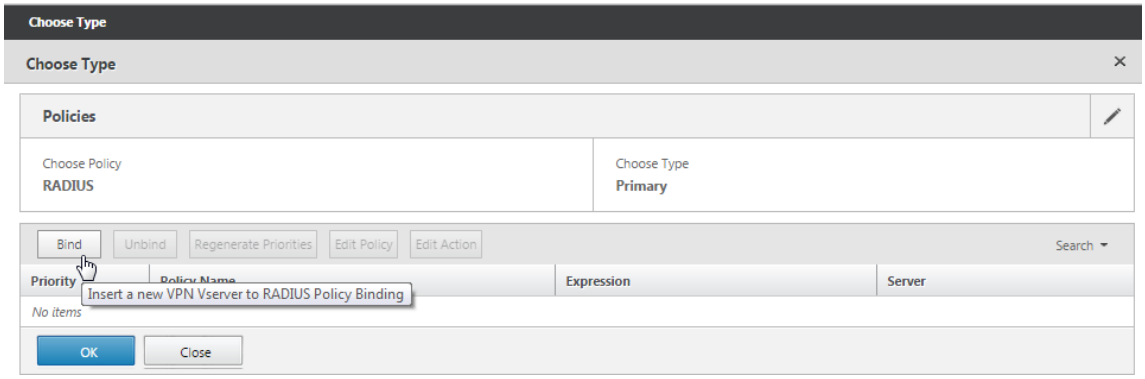
18. 在 身份验证行上，单击 **+** 以添加 Radius 身份验证。



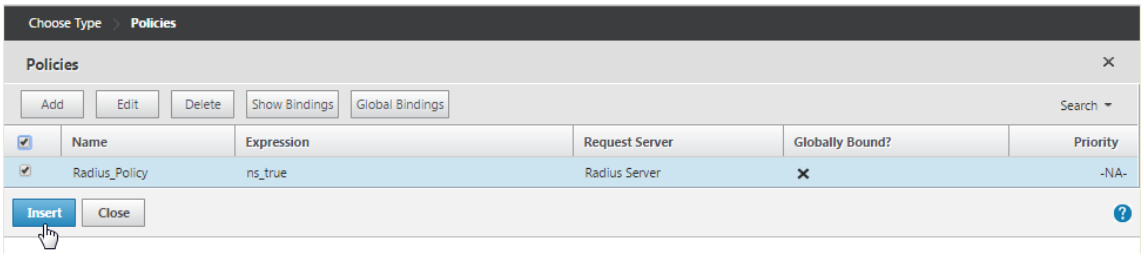
19. 在“选择类型”下，从“选择策略”中选择“**RADIUS**”。



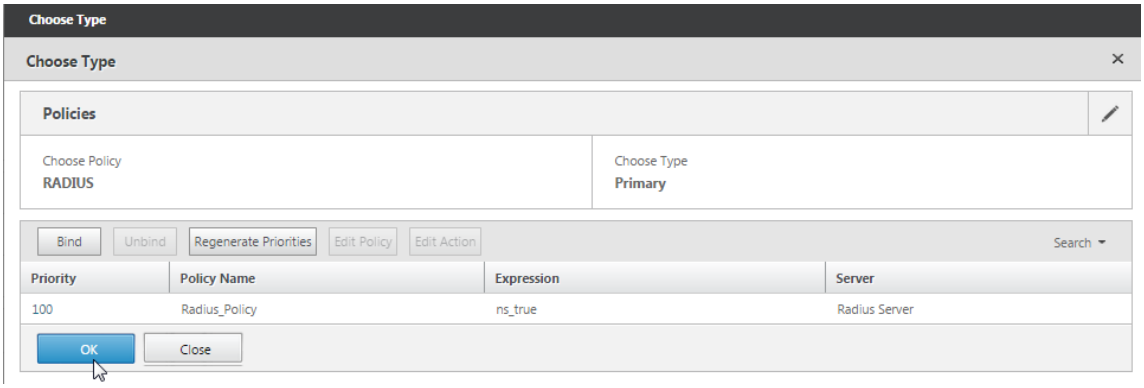
20. 单击 **Bind**（绑定）。



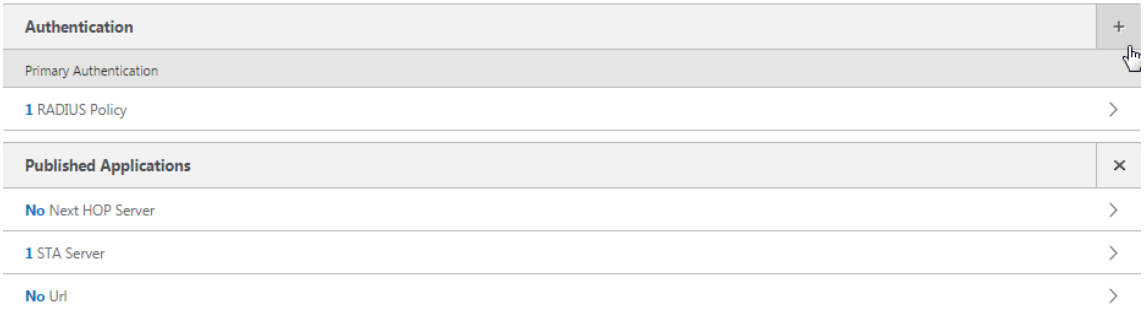
21. 选择您之前创建的 Radius 身份验证策略，然后单击 插入。



22. 单击确定。



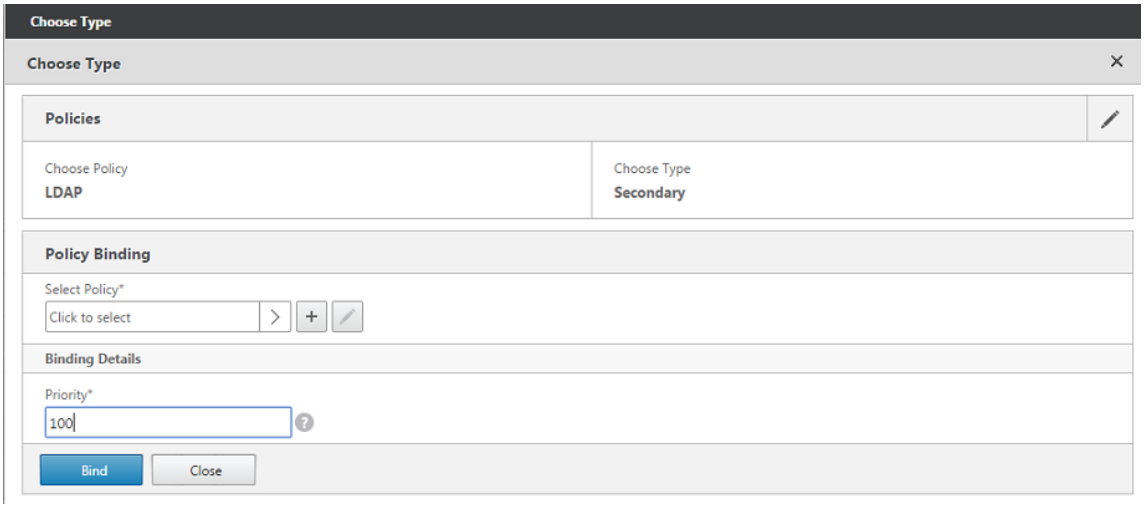
23. 要将 LDAP 添加为辅助身份验证策略：在“身份验证”行上，单击“**+**”。



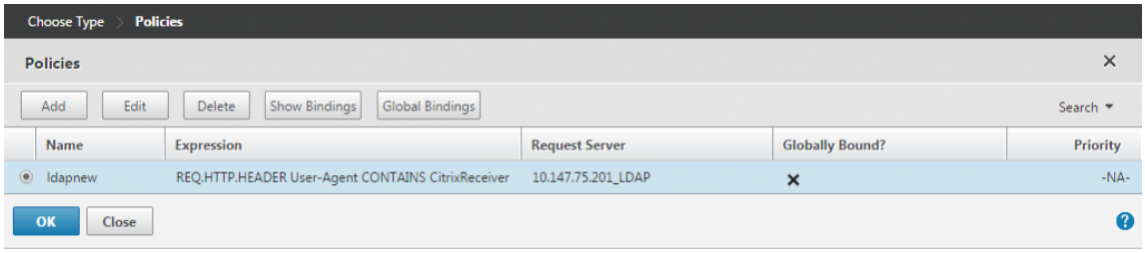
24. 从“选择策略”中，选择 **LDAP**。

25. 从“选择类型”中，选择“辅助”。

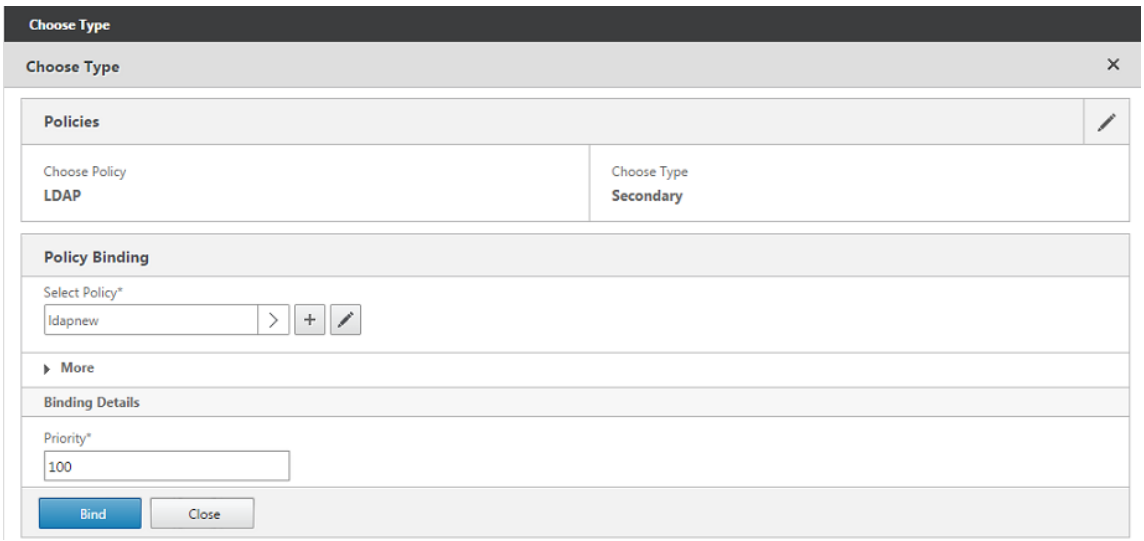
26. 从“选择策略”中，选择 LDAP 策略。



27. 选择策略，然后单击 确定。



28. 单击 **Bind**（绑定）。



29. 单击完成。

30. 验证您创建的策略具有最高优先级。这可确保即使为非移动用户添加了其他策略，它们也具有最高优先级。有关详细信息，请参阅设置身份验证策略的优先级。

配置客户端证书或客户端证书和域身份验证

January 10, 2023

使用 Citrix ADC 仅证书身份验证或证书加域身份验证时，可以使用适用于 Citrix Endpoint Management Citrix ADC 向导设置 Citrix Endpoint Management 所需的配置。只能运行适用于 Citrix Endpoint Management 的 Citrix ADC 向导一次。有关使用向导的信息，请参阅为 Citrix Endpoint Management 环境配置设置。

如果您已使用该向导，请按照本文中的说明进行客户端证书身份验证或客户端证书加域身份验证所需的附加配置。

若要确保处于“纯 MAMA”模式的设备用户无法使用设备上的现有证书进行身份验证，请参阅本文后面的“Citrix ADC 证书吊销列表 (CRL)”。

手动配置 **Citrix Gateway** 以进行客户端证书身份验证

1. 在“流量管理”>“负载平衡”>“虚拟服务器”下，转到每个虚拟服务器（443 和 8443），更新 **SSL** 参数，并将“启用会话重用”设置为“禁用”。

2. 在 Citrix Gateway 虚拟服务器上，在“启用客户端身份验证”->“客户端证书”上，选择“客户端身份验证”，对于“客户端证书”，选择“必需”。
3. 创建身份验证证书策略，以便 Citrix Endpoint Management 可以从 Secure Hub 提供的客 户端证书中提取用户主体名称或 **sAMAccount** 到 Citrix Gateway。有关详细信息，请参阅 适用于 XenMobile 向导的 Citrix ADC。
4. 为证书配置文件设置以下参数：

   身份验证类型：**CERT**

   两个因素：**OFF** （仅用于证书身份验证）

   用户名字段：主题：**CN**

   组名字段：**SubjectAltName:PrincipalName**
5. 仅将证书身份验证策略绑定为 Citrix Gateway 虚拟服务器中的 主身份验证。
6. 绑定根 CA 证书以验证呈现给 Citrix Gateway 的客户端证书的信任。

为客户端证书和域身份验证手动配置 Citrix Gateway

1. 在“流量管理”>“负载平衡”>“虚拟服务器”下，转到每个虚拟服务器（443 和 8443），更新 **SSL** 参数，并将“启用会话重用”设置为“禁用”。
2. 转到“策略”>“身份验证”>“证书”，选择“服务器”选项卡，然后单击“添加”。
3. 输入配置文件的名称，将两个因子设置为开，然后从用户名字段中选择 **SubjectAltNamePrincipalName**。
4. 转到“策略”并单击“添加”。
5. 输入策略的 名称，从 服务器中选择证书配置文件，将表 达式设置为 **ns_true**，然后单击 创建。
6. 转到 虚拟服务器，选择虚拟服务器，然后单击 编辑。
7. 在 身份验证旁边，单击 **+** 以添加证书身份验证。
8. 要选择身份验证方法：从“选择策略”中，选择“证书”。
9. 从“选择类型”中，选择“主”。这将证书身份验证绑定为主身份验证，其优先级与 LDAP 身份验证类型相同。
10. 在 策略绑定下，单击 单击以选择以选择之前创建的证书策略。
11. 选择之前创建的证书策略，然后单击“确定”。
12. 将 优先级设置为 **100** ，然后单击 绑定。在后续步骤中配置 LDAP 身份验证策略时，请使用相同的优先级编号。
13. 在 **LDAP** 策略的行上，单击 **>**。
14. 选择策略，然后从“编辑”下拉菜单中单击“编辑绑定”。
15. 输入您为证书策略指定的相同 优先级值。单击 **Bind**（绑定）。

16. 单击关闭。
17. 在“高级”下，单击 **SSL** 参数。
18. 选中“客户端身份验证”复选框，从“客户端证书”中选择“强制”，然后单 击 **“**确定”。
19. 单击完成。

Citrix ADC 证书吊销列表 **(CRL)**

Citrix Endpoint Management 仅支持对第三方证书颁发机构使用证书吊销列表 (CRL)。如果您配置了 Microsoft CA，Citrix Endpoint Management 将使用 Citrix ADC 来管理吊销。配置基于客户端证书的身份验证时，请考虑是否需要配置 Citrix ADC 证书吊销列表 (CRL) 设置“启用 **CRL** 自动刷新**”**。此步骤可确保处于仅 MAM 模式的设备的用户无法使用设备上的现有证书进行身份验证。Citrix Endpoint Management 会重新颁发新证书，因为如果吊销用户证书，则不会限制用户生成用户证书。此设置提高了 CRL 检查过期的 PKI 实体时 PKI 实体的安全性。

使用 **CloudBridge** 优化网络流量

April 6, 2020

当用户使用 Citrix Gateway 插件登录时，可以使用 CloudBridge 插件优化连接，该插件安装在用户设备上的 CloudBridge 插件。当通过使用 CloudBridge 插件优化连接时，网络流量将通过 Citrix Gateway 进行压缩和加速。为连接启用 CloudBridge 时，Citrix Gateway 上的 TCP 压缩策略将被禁用。

将部署 CloudBridge 插件并与 Citrix Gateway 插件配合使用。

Citrix Gateway 支持中继器插件的 5.5 和 6.1 版本以及 CloudBridge 插件的 6.2 和 7.0 版本。

CloudBridge 优化和流控制优先于需要动态内容修改的 Citrix Gateway 优化功能。如果为 HTTP 流量启用了 CloudBridge 优化，则以下 Citrix Gateway 功能将不可用：

- 单点登录到 Web 应用程序
- 文件类型关联
- HTTP 授权

要允许单点登录 Web 应用程序，您可以禁用 HTTP 上的加速。为此，请使用命令行。登录到 Citrix Gateway 串行控制台，然后在命令提示符下键入：

```
add vpn trafficAction ssoact http -SSO ON
```

针对 Citrix Gateway 上已配置 HTTP 端口的网络流量将自动排除在 CloudBridge 优化之外。此为默认设置。如果您在 HTTP 端口上为 CloudBridge 优化配置流量策略，则支持流量策略，并由 CloudBridge 优化网络流量。但是，对于受该策略影响的所有流量，将禁用 Citrix Gateway 优化功能。CloudBridge 可以加速发往非 HTTP 端口的网络流量，而不会影响其他 Citrix Gateway 功能。

您可以使用流量策略配置用户连接以使用 CloudBridge 插件。然后，您可以将策略绑定到用户、组、虚拟服务器或全局。策略的优先级取决于您绑定策略的位置或您给策略的优先级号。

创建流量策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 Citrix Gateway 策略，然后单击“流量”。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在“名称”中键入策略的名称。
4. 在请求配置文件旁边，单击新建。
5. 在“名称”中，键入配置文件的名称。
6. 在 分支中继器中，选择 开，然后单击 创建。
7. 在“创建流量策略”对话框中，在“添加表达式”旁边，选择或输入表示要启用 CloudBridge 加速的流量类型的表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

添加表达式时，请选择网络表达式以使用与 CloudBridge 配置为加速的相同的 IP 地址和端口范围。要发生 CloudBridge 加速，Citrix Gateway 上配置的流量类型必须与在 CloudBridge 上配置的服务类策略相匹配。

所有 TCP 流量都受益于 CloudBridge 加速。如果您计划使用单点登录，请不要加速 HTTP 流量，因为加速会禁用单点登录。

关于网关用户体验配置的 **RfWebUI** 角色

November 7, 2022

RfWebUI 角色是一个主题，为通过 Citrix Gateway 登录的 Citrix Gateway 用户提供了新的登录和门户页面。门户向接收器、店铺和 Citrix Endpoint Management 用户提供的 GUI 与直接访问其中一个产品时相同。

何时使用 **RfWebUI** 角色

当您需要由不同的 Citrix 产品（例如 Web 和软件即服务 (SaaS) 应用程序、虚拟 Windows 应用程序和桌面）提供的所有应用程序的单窗格视图时，请使用 Citrix Gateway 中的 RfWebUI 角色。

以下场景说明了 RfWebUI 角色的使用。

- 用户使用 Gateway 访问店面，并找到与他们在访问没有网关的产品时看到的图形用户界面不同的图形用户界面。
  解决方案：当用户使用网关访问店面时，RfWebUI 主题提供了类似于他们在不使用网关的情况下访问产品时看到的用户界面。
- 用户使用网关访问 Citrix Workspace 应用程序、店铺和 Citrix Endpoint Management 应用程序，并且很难找到所需的应用程序，因为这些应用程序未按逻辑方式进行分组。
  解决方案：RfWebUI 角色通过创建由不同产品（例如 Receiver、StoreFront、Citrix Endpoint Management 等）提供的应用程序的逻辑捆绑来提供单窗格视图用户体验。

RfWebUI 角色提供的功能

新的 RfWebUI 提供以下功能：

- 走吧
- 应用程序的汇总
- 用户配置的 RDP 代理链接
- 最喜欢的应用程序

走吧

GO： Go 功能可以通过无临床 VPN（CVPN）访问网页。用户只需在 书签选项卡的 URL 部分中键入 URL，然后点击 **GO** 。

目前，**GO** 功能仅支持 Outlook Web 应用程序 (OWA) 和 SharePoint URL。

> 注意
> **GO** 选项卡只有当会话策略中的 *clientlessAccessVPNMode* 参数处于 **Enabled** 状态时才可见。

应用程序的汇总

应用程序聚合： RfWebUI 主题通过将不同产品提供的应用程序捆绑在描述性横幅下，提供单窗格视图。例如，Citrix ADC 管理员配置的所有 VPN URL 都位于名为 **Web** 和 **SaaS** 应用程序的捆绑中，用户特定的 Web 书签位于“个人书签”下。如果在 StoreFront 中配置了 Citrix Virtual Apps and Desktops 应用程序捆绑包，Citrix Gateway 中的单窗格视图也会列出这些捆绑包。

用户配置的 **RDP** 代理链接

用户可以将远程桌面协议 (RDP) 代理链接添加为个人书签。个人书签显示在“桌面”选项卡下。

支持以下 RDP 模式：

- 单一网关
- 无状态（双）网关

> 注意
> 用户只能添加 RDP 代理链接，如果配置了 *RDPP* 客户端配置文件。有关 RDP 配置的详细信息，请参阅 *RDP* 代理文档。

最喜欢的应用程序

用户可以通过单击应用程序名称旁边的添加到收藏夹链接来添加 **Web** 和 **SaaS** 应用程序和个人书签到收藏夹选项卡下列出的所需应用程序。添加后的应用程序可以在“收藏夹”选项卡下看到。同样也可以通过单击“收藏夹”选项卡内的应用程序旁边的“删除”链接从收藏夹选项卡中删除。

启用 **RfWebUI** 角色时的注意事项

RfWebUI 角色不完全支持以下内容：

文件服务功能用于访问 SMB 文件共享的文件服务功能不受支持。
电子邮件主页：电子邮件主页 VPN 参数不可用作 Citrix Gateway 门户的嵌入式视图。它可以作为应用程序在 RfWebUI 的应用程序选项卡下的 **Web** 和 **SaaS** 应用程序包中进行访问。
Java 客户端：用于建立 SSL 隧道的基于浏览器的 Java 客户端在此主题中不可用。

配置 **RfWebUI** 角色

要应用 **RfWebUI** 角色，请执行以下操作：

1. 在 Citrix ADC 界面中，导航到 配置 **> Citrix Gateway** 门户主题。
2. 在门户主题页面上，选择 **RfWebUI** 复选框。
3. 单 击门户主题页面右上角的保存图标。
4. 在 保存确认对话框中，单击 是。

RDP 代理

April 6, 2020

通过 **Citrix Gateway** 的 **RDP** 代理概述和增强功能

以下 RDP 代理功能可通过 Citrix Gateway 访问远程桌面场：

- 通过 CVPN 或 ICA 代理模式（无完整隧道）保护 RDP 流量。
- 通过 Citrix Gateway 登录到 RDP 服务器的单次登录 (SSO)。如果需要，还提供了一个禁用 SSO 的选项)。
- 强制 (SmartAccess) 功能，其中 Citrix ADC 管理员可以通过 Citrix Gateway 配置禁用某些 RDP 功能。
- 满足所有需求的单/无状态（双）网关解决方案 (VPN/ICA/RDP/Citrix Endpoint Management)。
- 与本机 Windows MSTSC 客户端的 RDP 兼容性，而无需任何自定义客户端。
- 在 macOSX、iOS 和 Android 上使用 Microsoft 提供的现有 RDP 客户端。

部署概述

下图描述了部署的概述：

RDP 代理功能作为 Citrix Gateway 的一部分提供。在典型部署中，RDP 客户端在远程用户的计算机上运行。Citrix Gateway 设备部署在 DMZ 内，RDP 服务器场位于内部企业网络中。远程用户连接到 Citrix Gateway 公有 IP 地址，建立 SSL VPN 连接，并对自己进行身份验证，之后该用户可以通过 Citrix Gateway 设备访问远程桌面。

在 CVPN 和 ICA 代理模式下支持 RDP 代理功能。

> 注意： Citrix Gateway 不支持远程桌面会话主机 (RDSH)/远程应用程序 /RDS 多用户 RDP 会话。

通过 **CVPN** 进行部署

在此模式下，RDP 链接将以书签形式在网关主页或门户网站上发布，通过 “add vpn url” 配置或通过外部门户网站。用户可以单击这些链接以访问远程桌面。

通过 **ICA** 代理进行部署

在此模式下，通过使用 wihome 参数在网关 VIP 上配置自定义主页。可以使用允许用户访问的远程桌面资源列表自定义此主页。此自定义页面可以托管在 Citrix ADC 上，如果是外部页面，则可以是现有网关门户页面中的 iFrame。

在任何一种模式下，用户单击已置备的 RDP 链接或图标后，相应资源的 HTTPS 请求到达 Citrix Gateway。网关为请求的连接生成 RDP 文件内容并将其推送到客户端。调用本机 RDP 客户端，并连接到网关上的 RDP 侦听器。网关通过支持强制 (SmartAccess) 对 RDP 服务器执行 SSO，其中 Gateway 根据 Citrix ADC 配置阻止客户端对某些 RDP 功能的访问，然后代理 RDP 客户端和服务器之间的 RDP 流量。

执行详细信息

Citrix ADC 管理员可以通过 Citrix Gateway 配置配置某些 RDP 功能。Citrix Gateway 为重要的 RDP 参数提供了 “RDP 强制执行” 功能。Citrix ADC 确保客户端无法启用阻止的参数。如果已启用阻止的参数，则 RDP 强制功能将取代启用客户端的参数，并且不支持这些参数。

支持强制执行的 **RDP** 参数

支持强制执行以下重定向参数。这些可作为 RDP 客户端配置文件的一部分进行配置。

- 剪贴板的重定向
- 打印机的重定向
- 磁盘驱动器的重定向
- COM 端口的重定向
- pnp 设备的重定向

连接流程

连接流程可分为两个步骤：

- RDP 资源枚举和 RDP 文件下载。
- RDP 连接启动。

基于上述连接流程，有两种部署解决方案：

- 无状态（双）网关解决方案-RDP 资源枚举和 RDP 文件下载通过身份验证器网关进行，但 RDP 连接启动通过 RDP 侦听器网关进行。
- 单个网关解决方案-通过同一网关进行 RDP 资源枚举、RDP 文件下载和 RDP 连接启动。

无状态（双）网关兼容性

下图描述了部署情况：

- 用户连接到身份验证器网关 VIP 并提供凭据。
- 成功登录到网关后，用户将被重定向到主页或外部门户，该门户将枚举用户可以访问的远程桌面资源。
- 用户选择 RDP 资源后，身份验证器网关 VIP 将接收请求，格式为 `https://vserver-vip/rdpproxy/rdptarget/listener`，指示用户单击的已发布资源。此请求包含有关用户选择的 RDP 服务器的 IP 地址和端口的信息。
- /rdpproxy/ 请求由身份验证器网关处理。由于用户已经通过身份验证，因此此请求附带有效的网关 cookie。
- RDPTarget 和 RDP 用户信息存储在 STA 服务器上，并生成 STA 票证。通过使用配置的预共享密钥对存储在 STA 服务器上的信息进行加密。身份验证器网关使用网关虚拟服务器上配置的 STA 服务器之一。
- 在 /rdpproxy/ 请求中获得的 “侦听器” 信息作为 “fulladdress” 放入.rdp 文件中，STA 票证（预先使用 STA AuthID）作为 “loadbalanceinfo” 放入.rdp 文件中。
- .rdp 文件被发送回客户端端点。
- 本机 RDP 客户端启动并连接到 RDPListener 网关。它在初始数据包中发送 STA 票证。

  RDPListener 网关验证 STA 票证并获取 RDPs 目标和 RDPs 用户信息。要使用的 STA 服务器通过使用负载均衡信息中存在的 “AuthID” 来检索。

单网关兼容性

下图描述了部署情况：

在单个网关部署的情况下，不需要 STA 服务器。身份验证器 Gateway 对 RDPTarget 和 Citrix ADC AAA 会话 cookie 进行安全编码，并将它们作为.rdp 文件中的负载均衡信息发送。当 RDP 客户端在初始数据包中发送此令牌时，身份验证器网关将解码 RDPTarget 信息，查找会话并连接到 RDPTarget。

RDP 代理的许可证要求

高级版，高级版

> 注意：只拥有网关平台许可证或仅拥有标准版的客户不可用 RDP 代理功能。

RDP 代理功能必须启用 RDP 代理才能工作。


```
enable feature rdpProxy
<!--NeedCopy-->
```

配置步骤

高级配置步骤如下所示：

1. 启用此功能
2. 在网关门户上创建书签或使用枚举 RDP 资源的自定义网关门户
3. 配置 RDP 客户端配置文件
4. 配置 RDP 服务器配置文件

启用所需的功能和模式

- enable ns feature ssl
- enable ns feature sslvpn
- enable ns feature rdpproxy
- 启用模式 usnip

创建书签

1. 在门户页面上创建书签以访问 RDP 资源：（actualURL 以 rdp:// 开头）。
2. Add vpn url <urlName> <linkName> <actualURL>
   - URL 必须采用以下格式：rdp://<TargetIP:Port>。
   - 对于无状态 RDP 代理模式，URL 必须采用以下格式：rdp://<TargetIP:Port>/<ListenerIP:Port>
   - 该 URL 以下列格式在门户上发布：
     https://<VPN-VIP>/rdpproxy/<TargetIP:Port>
     https://<VPN-VIP>/rdpproxy/<TargetIP:Port>/<ListenerIP:Port>
3. 将书签绑定到用户、组、VPN 虚拟服务器或 VPN 全局。

配置客户端配置文件

在身份验证器网关上配置客户端配置文件。以下是一个示例配置：


```
add rdpClient profile <name> [-addUserNameInRdpFile ( YES | NO )] [-
    audioCaptureMode ( ENABLE | DISABLE )] [-keyboardHook <keyboardHook
    >] [-multiMonitorSupport ( ENABLE | DISABLE )] [-psk <string>] [-
    rdpCookieValidity <positive_integer>] [-rdpCustomParams <string>] [-
    rdpFileName <string>] [-rdpHost <optional FQDN that will be put in
    the RDP file as 'fulladdress>] [-rdpUrlOverride ( ENABLE | DISABLE
    )] [-redirectClipboard ( ENABLE | DISABLE )] [-redirectComPorts (
    ENABLE | DISABLE )] [-redirectDrives ( ENABLE | DISABLE )] [-
    redirectPnpDevices ( ENABLE | DISABLE )] [-redirectPrinters ( ENABLE
     | DISABLE )] [-videoPlaybackMode ( ENABLE | DISABLE )]
<!--NeedCopy-->
```

将 RDP 客户端配置文件与 VPN 虚拟服务器关联。

这可以通过配置 sessionAction+sessionPolicy 或通过设置全局 vpn 参数来完成。

示例:

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <prioritynumber>
```

或

```
set vpn parameter -rdpClientprofile <name>
```

配置服务器配置文件

在侦听器网关上配置服务器配置文件。

- `add rdpServer Profile <profilename> -rdpIP <IPV4 address of the RDP listener> -rdpPort <port for terminating RDP client connections> -psk <key to decrypt RDPTarget/RDPUser information, needed while using STA>`

rdpServer 配置文件必须在 “VPN 虚拟服务器” 上进行配置。

- `add vpn vserver v1 SSL <publicIP> <portforterminatingvpnconnections> -rdpServerProfile <rdpServer Profile>`

示例配置

- 启用所需的功能和模式
  - enable ns feature ssl
  - enable ns feature sslvpn

  - enable ns feature rdpproxy
  - 启用模式 usnip

- 为具有目标信息的用户添加 VPN URL

```
add aaa user Administrator  -password freebsd123$%^

add vpn url rdp RdpLink rdp://rdpserverinfo

add dns addrec rdpserverinfo 10.102.147.132

bind aaa user Administrator   -urlName rdp
<!--NeedCopy-->
```

- 为 VPN 连接配置 RDP 客户端和服务器配置文件

```
add rdp clientprofile p1  -psk citrix -redirectClipboard ENABLE

add rdp serverprofile p1 -rdpIP 10.102.147.134 -psk citrix

add vpn vserver mygateway SSL  10.102.147.134 443  -
   rdpserverprofile p1

set vpn parameter -clientlessVpnMode ON -
   defaultAuthorizationAction ALLOW -rdpClientProfileName p1

add ssl certKey gatewaykey -cert rdp_rootcert.pem  -key
   rdp_rootkey

bind ssl vserver mygateway -certkeyName gatewaykey
<!--NeedCopy-->
```

- 添加 SNIP 以便从 Citrix ADC 连接到目标

```
add ns ip 10.102.147.135  255.255.255.0  -type SNIP
<!--NeedCopy-->
```

禁用 **SSO** 的选项

可以通过配置 Citrix ADC 流量策略来禁用具有 RDP 代理的 SSO（单点登录）功能，以便始终提示用户输入凭据。当 SSO 被禁用时，RDP 强制（SmartAccess）不起作用。

示例配置：

```
add vpn trafficaction <TrafficActionName> HTTP -SSO OFF
```



```
<!--NeedCopy-->
```

流量策略可以根据要求进行配置，以下是两个示例：

• 要为所有流量禁用 SSO，请执行以下操作：

```
add vpn trafficpolicy <TrafficPolicyName>  "url contains rdpproxy" <
    TrafficActionName>
<!--NeedCopy-->
```

• 基于源/目标 IP/FQDN 禁用 SSO

```
add vpn trafficPolicy <TrafficPolicyName>  "REQ.HTTP.URL CONTAINS
    rdpproxy && REQ.IP.SOURCEIP == <IP/FQDN>" <TrafficActionName> bind
    vpnvserver rdp -policy <TrafficActionName>
<!--NeedCopy-->
```

支持单个监听器

- 用于 RDP 和 SSL 流量的单个侦听器。
- RDP 文件下载和 RDP 流量可以通过 Citrix ADC 上的相同 2 元组（即 IP 和端口）进行处理。

书签

通过门户网站生成 **RDP** 链接。无需为用户配置 RDP 链接或通过外部门户发布 RDP 链接，您可以通过提供 targerIP:Port 为用户提供生成自己的 URL 的选项。对于无状态 RDP 代理部署，管理员可以在 FQDN：端口格式中包含 RDP 侦听器信息，作为 RDP 客户端配置文件的一部分。这是在 rdpListener 选项下完成的。此配置用于在双网关模式下通过门户生成 RDP 链接。

RDP 代理配置

执行以下操作来配置 RDP 代理：

1. 展开 **Citrix Gateway**，展开 策略，右键单击 RDP，然后单击 启用功能。
2. 点击左侧的 RDP。在右侧，切换到 客户端配置文件选项卡，然后单击 添加。
3. 为客户端配置文件指定一个名称，并根据需要对其进行配置。向下滚动
4. 在 RDP 主机字段中，输入解析为 RDP 代理侦听器的 FQDN，该侦听器通常与 Citrix Gateway 设备的 FQN 相同。
5. 底部附近是一个预共享密钥。输入密码，然后单击 确定。你稍后需要这个。
6. 为服务器配置文件指定一个名称。

7. 输入要绑定的网关虚拟服务器的 IP 地址。
8. 输入您为 RDP 客户端配置文件配置的相同预共享密钥。单击创建。
9. 如果要将 RDP 书签放在“无客户端访问”门户页面上，请在左侧展开 **Citrix Gateway**，展开“资源”，然后单击“书签”。
10. 点击右侧的“添加”。
11. 为书签指定一个名称。
12. 对于 URL，请使用 IP 或 DNS 输入 rdp://MyRDPServer。
13. 选中使用 Citrix Gateway 作为反向代理旁边的复选框，然后单击创建。
14. 根据需要创建更多书签。
15. 创建或编辑会话配置文件或策略。
16. 在“安全”选项卡上，将“默认授权操作”设置为“允许”。或者，您可以使用授权策略来控制访问。
17. 在“远程桌面”选项卡上，选择您之前创建的 RDP 客户端配置文件。
18. 如果要使用书签，请在“客户端体验”选项卡上，将 无客户端访问设置为“开”。
19. 在“已发布的应用程序”选项卡上，确保 **ICA** 代理处于 关闭状态。
20. 修改或创建网关虚拟服务器。
21. 在 基本设置部分，单击 更多。
22. 使用 RDP 服务器配置文件列表选择之前创建的 RDP 服务器配置文件。
23. 向下滚动。确保未选中“仅 **ICA**”。
24. 绑定证书。
25. 绑定身份验证策略。
26. 绑定配置了 RDP 客户端配置文件的会话策略/配置文件。
27. 您可以将书签绑定到 Citrix Gateway 虚拟服务器或 Citrix ADC AAA 组。要绑定到 Citrix Gateway 虚拟服务器，请在右侧的“高级设置”部分中单击“已发布的应用程序”。
28. 在左侧的“已发布的应用程序”部分，单击 **No Url** 。
29. 绑定您的书签。
30. 由于未为此 Citrix Gateway 虚拟服务器指定“仅 ICA”，因此请确保正确配置了 Citrix Gateway 通用许可证。在左侧，展开 **Citrix Gateway**，然后单击全局设置。
31. 单击右侧的 更改身份验证 **AAA** 设置。
32. 将 最大用户数更改为您的许可限制。
33. 如果要使用 DNS 连接到 RDP 服务器，请确保在设备上配置了 DNS 服务器（流量管理 **> DNS >** 名称服务器）。

34. 如果要使用短名称而不是 FQDN，请添加 D**NS** 后缀（流量管理 **> DNS > DNS** 后缀）。
35. 连接到您的网关并登录。
36. 如果配置了 书签，请单击书 签。
37. 您可以将地址栏更改为 **/rdpproxy/MyRDPServer**。您可以输入一个 IP 地址（例如，一个 IP 地址 /192.168.1.50）或 DNS 名称（/rdpprox/ 我的服务器）。
38. 打开下载的.rdp 文件。
39. 您可以转到 **Citrix Gateway** 策略 **> RDP** 查看当前已连接的用户。右侧是“连接”选项卡。

无状态 **RDP** 代理

April 6, 2020

无状态 RDP 代理访问 RDP 主机。当用户在单独的 Citrix Gateway 身份验证器上进行身份验证时，将通过 Citrix Gateway 上的 RDPListener 授予访问权限。Citrix Gateway 的 RDPListener 所需的信息安全地存储在 STA 服务器上。

此处介绍了为此功能创建的流程和新旋钮。

必备条件

- 用户在 Citrix Gateway 身份验证器上进行身份验证。
- 初始 /rdpproxy URL 和 RDP 客户端连接到不同的 RDPListener Citrix Gateway。
- 验证器网关使用 STA 服务器安全地传递 RDPListener 网关信息。

配置

- 添加新的 *rdpServer* 配置文件。在 RDPListener 网关上配置了服务器配置文件。

```
1  add rdpServer Profile [profilename] -rdpIP [IPV4 address of the
       RDP listener] -rdpPort [port for terminating RDP client
       connections] -psk [key to decrypt RDPTarget/RDPUser
       information, needed while using STA].
2  <!--NeedCopy-->
```

  对于无状态 RDP 代理，STA 服务器验证由 RDP 客户端发送的 STA 票证，以获取 RDP 目标 /RDP 用户信息。

  使用以下命令在 vpn 虚拟服务器上配置 rdpServer 配置文件：


```
add vpn vserver v1 SSL [publicIP] [
    portforterminatingvpnconnections] -rdpServerProfile [rdpServer
     Profile]
<!--NeedCopy-->
```

> 警告
>
> 一旦在 VPN 虚拟服务器上配置了 rdpServerProfile 配置文件，无法修改。此外，同一个服务器配置文件不能在另一个 VPN 虚拟服务器上重复使用。

rdp 配置文件命令已重命名为 **RDPClient** 配置文件并具有新参数。添加了 multiMonitorSupport 命令。此外，还添加了一个选项来配置自定义参数，该参数不支持作为 RDP 客户端配置文件的一部分。clientSSL 参数已被删除，因为连接始终是安全的。在身份验证器网关上配置客户端配置文件。

```
add rdpClient profile <name> -rdpHost <optional FQDN that will be put
    in the RDP file as 'fulladdress' > [-rdpUrlOverride ( ENABLE |
    DISABLE )] [-redirectClipboard ( ENABLE | DISABLE )] [-
    redirectDrives ( ENABLE | DISABLE )]

[-redirectPrinters ( ENABLE | DISABLE )] [-keyboardHook <keyboardHook>]
     [-audioCaptureMode ( ENABLE | DISABLE )] [-videoPlaybackMode (
    ENABLE | DISABLE )]

[-rdpCookieValidity <positive_integer>][-multiMonitorSupport ( ENABLE |
     DISABLE )] [-rdpCustomParams <string>] 在单个网关部署中使用 -
    rdpHost 配置。
```

- 将 RDP 配置文件与 VPN 虚拟服务器关联。

这可以通过配置 sessionAction+sessionPolicy 或通过设置全局 vpn 参数来完成。

示例

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <
    prioritynumber>

或

set vpn parameter -rdpClientprofile <name>
```


连接计数器

添加了一个新的连接计数器 n_rdp_totr_curr_active_conn，该计数器保留正在使用的活动连接数的记录。它可以被视为 NetScaler 外壳上 nsconmsg 命令的一部分。稍后，我们将提供一个新的 CLI 命令来查看此计数器。

连接流程

RDP 代理流中涉及两个连接。第一个连接是用户与 Citrix Gateway VIP 的 SSL VPN 连接，以及 RDP 资源的枚举。

第二个连接是与 Citrix Gateway 上 RDP 侦听器的本机 RDP 客户端连接（使用 rdpIP 和 rdpPort 进行配置），以及随后将 RDP 客户端安全地代理到服务器数据包。

1. 用户连接到身份验证器网关 VIP 并提供其凭据。
2. 成功登录到网关后，用户将被重定向到主页/外部门户，该门户枚举用户可以访问的远程桌面资源。
3. 用户选择 RDP 资源后，身份验证器网关 VIP 将接收请求，格式为 `https://AGVIP/rdpproxy/ip:port/rdptargetproxy`，指示用户单击的已发布资源。此请求包含有关用户选择的 RDP 服务器的 IP 和端口的信息。
4. /rdpproxy/ 请求由身份验证器网关处理。由于用户已经通过身份验证，因此此请求附带有效的网关 cookie。
5. RDPTarget 和 RDP 用户信息存储在 STA 服务器上，并生成 STA 票证。信息存储为 XML Blob，可选择使用配置的预共享密钥加密。如果加密，则 Blob 将被 base64 编码和存储。身份验证器网关将使用网关虚拟服务器上配置的 STA 服务器之一。
6. XML Blob 将采用以下格式

   <Value name=”IPAddress”>ipaddr</Value>\n<Value name=”Port”>port</Value>\n

   <Value name=”Username”>username</Value>\n<Value name=”Password”>pwd</Value>
7. 在 /rdpproxy/ 请求中获得的 “rdptargetproxy” 被放置为 “完整地址”，STA 票证（预先使用 STA AuthID）被放置为.rdp 文件中的 “负载均衡信息”。
8. .rdp 文件被发送回客户端端点。
9. 本机 RDP 客户端启动并连接到 RDPListener 网关。它在初始 x.224 数据包中发送 STA 票证。
10. RDPListener 网关验证 STA 票证并获取 RDPs 目标和 RDPs 用户信息。使用负载均衡信息中存在的 “AuthID” 检索要使用的 STA 服务器。
11. 创建网关会话用于存储授权/审核策略。如果用户已经存在会话，则会重新使用该会话。
12. RDPListener 网关连接到使用 CREDSSP 的 RDPTarget 和单个标志。

单网关兼容性

如果 RDP 文件是使用 /rdpproxy/rdp 目标/rdp 目标代理 URL 生成的，我们将生成 STA 票证，否则将使用当前指向会话的 “负载平衡信息” 方法。

在单个网关部署的情况下，/rdpproxy URL 进入身份验证器网关本身。STA 服务器不是必需的。身份验证器网关对 RDPTarget 和 AAA 会话 cookie 进行安全编码，并将其作为.rdp 文件中的 “负载均衡信息” 发送。当 RDP 客户端在 x.224 数据包中发送此令牌时，身份验证器网关将解码 RDPTarget 信息，查找会话并连接到 RDPTarget。

升级说明

较早的配置不适用于此新版本，因为之前在 vpn 虚拟服务器上配置的参数 rdpIP 和 rdpPort 已更新为 rdpServerProfile 的一部分，并且 “rdp Profile” 已重命名为 “rdp ClientProfile”，旧参数 clientSSL 已被删除。

创建 **RDP** 服务器配置文件

1. 转到 “Citrix Gateway”>“策略”>“RDP”。
2. 转到服务器配置文件选项卡，然后单击 添加。
3. 输入以下信息以创建 RDP 服务器配置文件。

配置 **RDP** 客户端配置文件

1. 转到 “Citrix Gateway”>“策略”>“RDP”
2. 转到客户配置文件选项卡，然后单击 添加。
3. 输入以下信息以配置 RDP 服务器配置文件。

设置虚拟服务器

1. 转到 “Citrix Gateway”>“虚拟服务器”。
2. 单击 添加以创建新的 RDP 服务器。
3. 完成此基本设置页面上的数据，然后单 击确定。
4. 单击 铅笔以编辑页面。

RDP 连接重定向

April 6, 2020

Citrix Gateway 设备现在支持在连接代理或会话目录存在的情况下进行 RDP 连接重定向。RDP 代理通信不再需要从客户端到服务器的每个连接的独占 URL。相反，代理使用单个 URL 连接到 RDP 服务器场，从而减少了管理员的维护和配置开销。

注意事项：

- 只有在启用 SSO 时，才支持 RDP 连接重定向，并且在单网关和无状态模式或双网关模式下以及强制 (Smart Access) 都支持该重定向。
- 仅支持基于令牌的重定向支持 IP Cookie 的 RDP 代理功能。禁用 “使用 IP 地址重定向” 功能时，基于 IP 的路由令牌 “msts=” 由 Windows 会话代理或连接代理交回。
- 可以配置 RDP 代理连接的专用重定向器。

在连接代理存在的情况下部署 **RDPProxy**

在连接代理存在的情况下，可以通过以下两种方式部署 RDPProxy。

- RD 会话主机服务器参与 RD 连接代理负载平衡。
- 存在 RDP 负载平衡功能。

RD 会话主机服务器参与 **RD** 连接代理负载平衡：

在这种情况下，可以将 RDP URL 链接配置为指向其中一个 RDP 服务器作为目标服务器，该服务器充当重定向器。此外，可以将场中的一个 RDP 服务器作为目标服务器（在这种情况下，服务器不接受任何 RDP 会话）。有关更多信息，请参阅远程桌面协议 (RDP) 服务器的负载平衡。

在具有 **RDP** 负载平衡功能的情况下：

当未启用连接代理负载平衡时，我们可以在 Citrix ADC 上提供 RDP 负载平衡功能，以便在连接代理存在的情况下对 RDP 会话执行所需的负载平衡。在这种情况下，必须将 RDP URL 链接配置为将 RDP 负载均衡器作为目标服务器。RDP 负载均衡器可与 RDP 代理位于同一 Citrix Gateway 设备上。有关更多信息，请参阅加载平衡 rdp 服务器。

> 注意：
> 要在连接代理的情况下支持 RDPProxy，应在 Citrix Gateway 上启用 RDP 连接重定向。

在连接代理存在的情况下配置 **RDPProxy**

要使用命令行界面配置 **RDP** 连接重定向，请在命令提示符处键入：

```
1     add rdpserverprofile <Name> -psk <string> -rdpRedirection ( ENABLE
          | DISABLE )
2
3     add rdpserverprofile serverProfileName -psk  “secretString”  -
          rdpRedirection ENABLE
4  <!--NeedCopy-->
```

使用 Citrix ADC GUI 配置 RDP 连接重定向：

1. 导航到 **Citrix Gateway >** 策略 **> RDP**。
2. 右键单击 **RDP** 以 启用或禁用 RDP 重定向功能。

基于 LDAP 属性填充 RDP URL

April 6, 2020

您可以将 Citrix Gateway 设备配置为从 LDAP 服务器属性检索 RDP 服务器 (IP/FQDN) 列表。根据检索到的列表，设备显示特定用户要访问的服务器的 RDP URL。

根据 LDAP 属性功能配置填充 RDP URL

要使用命令行界面填充基于 **LDAP** 属性的 **RDP URL**，请在命令提示符下键入：

```
1     add rdpclientprofile <Name>  - rdpUrlLinkAttribute <string>
2
3 <!--NeedCopy-->
```

```
1     add rdpclientprofile clientProfileName  - rdpUrlLinkAttribute
         rdpServerAttribute
2
3 <!--NeedCopy-->
```

在上面的示例中，rdpServerAttribute 对应于 LDAP 服务器上给定用户的 rdp 服务器详细信息。

注意：若要从 LDAP 服务器获取 LDAP 属性详细信息，LDAP 操作应配置为使用 pUrlLinkAttribute 配置的相同字符串，如下所示。

```
1     add authentication ldapAction dnpg_ldap -serverIP <IP address>-
         ldapBase <"domain name"> -ldapBindDn <username> -ldapLoginName
         sAMAccountName -ldapbindDnpassword <password>
2
3 <!--NeedCopy-->
```

```
1 add authentication ldapAction dnpg_ldap -serverIP 10.102.39.101 -
     ldapBase "dc=dnpg-blr,dc=com" -ldapBindDn sqladmin@dnpg-blr.com -
     ldapLoginName sAMAccountName -ldapbindDnpassword xxxx
```

```
1     add authentication ldapPolicy dnpg_ldap_pol ns_true dnpg_ldap
2
3 <!--NeedCopy-->
```

```
1 bind vpn vs vserver<name> -pol dnpg_ldap_pol
2
3 set ldapaction dnpg_ldap -attributes "rdpServerAttribute"
4
```



```
set rdpclientprofile ldap -rdpLinkAttribute rdpServerAttribute
<!--NeedCopy-->
```

在 LDAP 服务器上，执行以下步骤：

1. 导航至特定 用户。
2. 在 **AD** 用户和计算机中，单击 “查看”，然后单击 “详细信息”。
3. 右键单击 用户名，然后单击 属性编辑器。
4. 更改所需属性 (displayName) 值，然后单击确定。

要使用 GUI 填充基于 LDAP 属性的 RDP URL：

1. 导航到 **Citrix Gateway >** 策略 **> RDP**。
2. 在 “**RDP** 配置文件和连接” 页上，单击 “客户端配置文件” 选项卡，然后选择要在其中配置 RDP 文件名的客户端配置文件。
3. 在 “配置 **RDP** 客户端配置文件” 页上，在 “**RDP** 文件名” 字段中输入文件名。

使用 **RDP** 代理随机化 **RDP** 文件名

April 6, 2020

当您点击一个 RDP URL 时，将下载一个 RDP 文件。再次单击 RDP URL 后，会下载具有相同名称的新 RDP 文件，从而弹出一个用现有文件替换新文件的弹出窗口。为了避免这种情况，管理员可以选择随机化 rdp 文件名。文件名现在通过以 <rdpFileName>_<outputof time()>.rdp 格式附加 time () 函数的输出来随机化。通过执行此操作，设备会在每次下载文件时生成唯一的 RDP 文件名。

配置对使用 **RDP** 代理随机化 **RDP** 文件名的支持

要通过在命令提示符下使用命令行界面配置对使用 **RDP** 代理随机化 **RDP** 文件名的支持，请键入：

```
    add rdpclientprofile <profileName> -rdpfileName <filename> -
       randomizeRDPFilename <YES/NO>

    add rdpclientprofile clientProfileName -rdpfileName testRDP -
       randomizeRDPFilename YES
<!--NeedCopy-->
```

使用 **Citrix ADC GUI** 配置对使用 **RDP** 代理随机化 **RDP** 文件名的支持：

1. 导航到 **Citrix Gateway** > 策略 > **RDP**。
2. 在 “**RDP** 配置文件和连接” 页上，单击 “客户端配置文件” 选项卡，然后选择要在其中配置随机化 RDP 文件名功能的客户端配置文件。
3. 在 “配置 **RDP** 客户端配置文件” 页上，在 “**** 随机化 **RDP** 文件名” 字段旁边的下拉列表中选择 YES** 。

配置 **RDP** 应用程序的文件名

April 6, 2020

下载 RDP 应用程序后，可以使用配置的文件名将应用程序存储在本地。

配置 **RDP** 应用程序的文件名

要使用 **CLI** 配置 **RDP** 应用程序的文件名，请在命令提示符下键入：

```
set rdpclientprofile <Name> -rdpfilename <filename>.rdp
<!--NeedCopy-->
```

使用 **GUI** 配置 **RDP** 应用程序的文件名：

1. 导航到 **Citrix Gateway** > 策略 > **RDP**。
2. 在 **RDP** 配置文件和连接页上，单击 客户端配置文件选项卡。选择要在其中配置随机化 RDP 文件名功能的客户端配置文件。
3. 在“配置 **RDP** 客户端配置文件”页上，在 RDP 文件名字段中输入 **rdp** 配置文件的名称。文件的名称必须采用以下格式:。该名称最多允许 31 个字符。

对 **VMware Horizon View** 启用了 **Citrix Gateway** 的 **PCoIP** 代理支持

April 6, 2020

Citrix Gateway 12.0 支持 PC (PCoIP) 协议，该协议是多种非 Citrix VDI 解决方案（包括 VMware Horizon View）的远程显示协议。PCoIP 类似于 Citrix HDX/ICA 协议和 Microsoft RDP 协议。PCoIP 使用 UDP 端口 4172。

通过 Citrix Gateway 代理 PCoIP 时，Citrix Gateway 可以替换传统的 PCoIP 远程访问解决方案，如 View 安全管理服务器或 VMware 接入点。

以下方案说明了使用 **Citrix Gateway** 启用 **VMware Horizon View** 解决方案的情况。

- VMware Horizon PCoIP 用户需要通过 Citrix Gateway 远程访问 VMware Horizon View 桌面池和应用程序池，而无需部署 Horizon View Security Server 或 VMware Access Point。
- PCoIP 用户通过 Citrix Gateway 远程访问其他基于 PCoIP 的虚拟桌面解决方案。

> 注意
>
> Citrix Gateway 作为远程访问解决方案进行部署。

为 **VMware Horizon View** 配置启用了 **Citrix Gateway** 的 **PCoIP** 代理

November 7, 2022

必备条件

版本 - Citrix ADC 12.0 或更高版本

通用许可证 -PCoIP 代理使用 Citrix Gateway 的无客户端访问功能，这意味着每个 Citrix Gateway 连接都必须获得 Citrix Gateway 通用许可证。在 Citrix Gateway 虚拟服务器上，确保未选中 “仅 **ICA**”。

Horizon View 基础结构 - 功能齐全的内部 Horizon View 基础结构。确保您能够在没有 Citrix Gateway 的情况下内部连接到 Horizon View 客户端。确保 Citrix ADC 将代理连接到的视图连接服务器上未启用 Horizon View **HTTP (S)** 安全隧道和 **PCoIP** 安全网关。
支持以下版本的 VMware Horizon View。

- 连接服务器：7.0.1 及更高版本
- Horizon Client：4.2.0 及更高版本（Windows 和 Mac）

防火墙端口：

确保以下内容：

- UDP 4172 和 TCP 443 必须从 Horizon View 客户端打开到 Citrix Gateway VIP。
- UDP 4172 必须从 Citrix ADC SNIP 打开到所有内部 Horizon View 代理。
- 在 NAT 后面部署的 Citrix ADC 上支持 PCoIP 代理。以下是需要考虑的要点：
  - 支持基于 VPN 虚拟服务器 FQDN 参数设置
  - 仅支持可公开访问的 FQDN，不支持 IP
  - 仅支持 443 和 4172 个端口
  - 必须是静态 NAT

证书 — Citrix Gateway 虚拟服务器的有效证书。

身份验证 — 使用经典语法的 LDAP 身份验证策略/服务器。

Unified Gateway（可选） - 如果是 Unified Gateway，则在添加 PCoIP 功能之前创建 Unified Gateway。

RfWebUI 门户主题 — 对于 Web 浏览器访问 Horizon View，Citrix Gateway 虚拟服务器必须使用 RfWebUI 主题进行配置。

Horizon View 客户端 — 即使使用 Citrix ADC RfWebUI 门户访问 Horizon 发布的图标，也必须在客户端设备上安装地 Horizon View 客户端。

要将 **Citrix Gateway** 配置为支持 **VMware Horizon View** 的 **PCoIP** 代理，请执行以下操作：

1. 在 Citrix ADC 管理 GUI 中，导航到 配置 > **Citrix Gateway** > 策略 > **PCoIP**。
2. 在 “PCoIP 配置文件和 连接” 页面上创建虚拟服务器配置文件和 **PCoIP** 配置文件。

3. 要创建虚拟服务器配置文件，请在虚拟服务器配置文件选项卡上单击添加。

a. 输入虚拟服务器配置文件的名称。

b. 输入将用于单点登录以查看连接服务器的 Active Directory 域名，然后单击创建。

注意： 每个 Citrix Gateway 虚拟服务器仅支持一个 Active Directory 域。此外，此处指定的域名将显示在 Horizon View 客户端中。

c. 点击 登录。

4. 若要创建 PCoIP 配置文件，请在配置 文件选项卡上单击 添加。

a. 输入 PCoIP 配置文件的名称。

b. 输入内部 VMware Horizon View 连接服务器的连接 URL，然后单击 创建。

5. 导航到 配置 > **Citrix Gateway** > 策略 > 会话。

6. 在右侧，选择“会话配置文件”选项卡。

7. 在 **Citrix Gateway** 会话策略和配置文件页面上，创建或编辑 Citrix Gateway 会话配置文件。

a. 要创建 Citrix Gateway 会话配置文件，请单击“添加”，然后提供名称。

b. 要编辑 Citrix Gateway 会话配置文件，请选择该配置文件，然后单击 编辑。

8. 在“客户端体验”选项卡上，确保“无客户端访问”值设置为“开”。

9. 在“安全”选项卡上，确保“默认授权操作”值设置为“允许”。

10. 在 **PCoIP** 选项卡上，选择所需的 PCoIP 配置文件，然后单击 创建。您还可以通过此选项卡创建或编辑 PCoIP 配置文件。

11. 单击“创建”或“确定”以完成创建或编辑会话配置文件。

12. 如果创建了新的会话配置文件，则还必须创建相应的会话策略。

a. 导航到 配置 > **Citrix Gateway** > 策略 > 会话。

b. 在右侧，选择“会话策略”选项卡。

c. 单击“添加”，为会话策略提供名称，然后从“配置文件”下拉列表中选择所需的会话 配置文件名称。

d. 如果您希望使用默认语法创建会话策略，请在表达式区域输入“true”（不带引号），然后单击 创建。注意：Unified Gateway 默认为经典语法。

e. 如果您希望使用经典语法创建会话策略，请先点击 切换到经典语法。然后在表达式区域中，键入“ns_true”（不带引号），然后单击 创建。

13. 将创建的 PCoIP 虚拟服务器配置文件和会话策略绑定到 Citrix Gateway 虚拟服务器。

a. 转到 **Citrix Gateway >** 虚拟服务器。

b. 在右侧，添加新的 Citrix Gateway 虚拟服务器或 编辑现有 Citrix Gateway 虚拟服务器。

c. 如果要编辑现有 Citrix Gateway 虚拟服务器，请在“基本设置”部分中单击铅笔图标。

d. 对于添加和编辑，请在“基本设置”部分单击“更多”。

e. 使用 **PCoIP** 虚拟服务器配置文件下拉菜单选择所需的 PCoIP 虚拟服务器配置文件。

f. 向下滚动并确保仅 ICA 处于未选中状态。然后单 击确定关闭 基本设置部分。

g. 如果要创建新的 Citrix Gateway 虚拟服务器，请绑定 证书并绑定 LDAP 身份验证策略。

h. 向下滚动到 策略部分，然后单击加号图标。

一. 选择类型页面默认为会话和请求。单击继续。

j. 在 策略绑定部分，单击 单击以选择。

k. 选择配置了 PCoIP 配置文件的所需会话策略，然后单击 选择。

l. 在 策略绑定页面中，单击 绑定。

米。如果要使用 Web 浏览器连接到 VMware Horizon View，请在右侧的“高级设置**”** 下添加“门户主题”部分。如果仅使用 Horizon View 客户端连接到 Citrix Gateway，则无需执行此步骤。

n. 使用门户主题下拉菜单选择 **RfWebUI**，然后单击确定。

o. Horizon View 已发布图标将添加到 RfWebUI 门户。

启用 **USB** 重定向的步骤

可以从虚拟桌面和应用程序访问连接到客户端计算机的 USB 设备。以下是启用 USB 重定向的步骤：

1. 登录到 VMware Horizon 管理员控制台。
2. 导航到 清单 -> 查看 配置 -> 服务器。
3. 选择“连接服务器”选项卡。
4. 选择列出的连接服务器，然后单击 编辑。
5. 在“常规”选项卡下，选择“**HTTP (S)** 安全隧道”下的“使用安全隧道连接到计算机”选项。在“外部 **URL**”字段中提供 NSG 外部 URL。

更新 **Unified Gateway** 的内容交换表达式

如果 Citrix Gateway 虚拟服务器位于 Unified Gateway（内容交换虚拟服务器）后面，则必须更新内容交换表达式以包含 PCoIP URL 路径。

1. 在 Citrix ADC GUI 中，导航到 配置 > 流量管理 **>** 内容交换 **>** 策略。
2. 在“表达式”区域下追加以下 表达式，然后单击“确定”。

http.req.url	http.req.url	http.req.url client")	http.req.url.path.contai tunnel")

使用 **PCoIP** 网关

1. 要进行连接，您必须在客户端设备上安装了 Horizon View 客户端。安装后，您可以使用 Horizon View 客户端的用户界面连接到 Citrix Gateway，也可以使用 Citrix Gateway RfWebUI 门户页面查看从 Horizon 发布的图标。

2. 要查看活动的 PCoIP 连接，请转到 **Citrix Gateway > PCoIP**。

3. 在右侧，切换到 "连接" 选项卡。活动会话将显示以下数据：用户名、Horizon View 客户端 IP 和 Horizon View 代理目标 IP。

4. 要终止连接，请右键单击 "连接" 选项卡，然后单击 "终止连接"。或者单击 "终止所有连接" 以终止所有 PCoIP 连接。

配置 VMware Horizon View Connection Server

April 6, 2020

要通过 Citrix Gateway 支持 PCoIP 代理，请执行以下操作：

1. 登录到 **VMware Horizon** 管理员控制台。

2. 导航到我 **nventory** -> 查看配置 -> 服务器。

3. 选择 "连接服务器" 选项卡。

4. 选择列出的连接服务器，然后单击 编辑。

5. 在 "常 规" 选项卡下，取消选择 "HTTP (S) 安全隧道**"** 下的 **"**使用安全隧道连接到计算机" 选项。

6. 单击 "确定" 关闭 "编 辑连接服务器设置" 窗口。

7. 在所有列出的连接服务器上运行步骤 4 到 6。

HDX 开明的数据传输支持

April 6, 2020

对 Citrix Gateway 的 Enlightened Data Transport (EDT) 支持可确保运行 Citrix Workspace 应用程序的用户获得高清晰度的虚拟桌面的会话中用户体验。

此外，使用 DTLS 1.0 进行端到端加密，以便在 Citrix Workspace 应用程序和 VDA 之间进行 EDT 终止。有关 DTLS 配置的更多信息，请单击支持 DTLSv1.0 协议。

启用 EDT 的 Citrix Gateway 可在 LAN 和 WAN 条件下提供良好的用户体验，从一个漫游到另一个时，无需任何管理或用户配置。这种优势在具有中度数据包丢失的高延迟网络中最为明显，在这些网络中，用户体验通常会与替代方案滞后。

支持 **DTLS 1.2** 协议

从版本 13.0 版本 47.x 中，Citrix ADC VPX 设备支持 DTLS 1.2 协议。可以使用 VPN 虚拟服务器 VPX 设备上的 **enable_dtls12_vpn_vserver** nsapimgr knob 启用或禁用 DTLS 1.2。

默认情况下，DTLS 1.2 处于禁用状态，并且 **enable_dtls12_vpn_vserver** knob 设置为 0。

要启用 DTLS 1.2，请将 **enable_dtls12_vpn_vserver** knob 设置为 1。更改旋钮值后，请关闭 DTLS 并使用`set vpn vserver <vservername> dtls <ON/OFF>` 命令重新打开旋钮以使旋钮生效。

> 重要提示：升级到 13.0 版本 47.x 或更高版本后，如果您已启用 DTLS 并且在早期版本中仅使用 TLSv1.2 密码，建议使用 nsapimgr 命令启用 DTLS 1.2。

何时使用 **Enlightened Data Transport** 支持

April 6, 2020

以下方案说明了启用 EDT 的 Citrix Gateway 的使用情况。

- 在远程访问业务资源的同时，用户希望获得与 LAN 环境一样的体验。
- 用户希望在 Wi-Fi 和蜂窝网络上获得丰富的虚拟应用程序和桌面用户体验，这些网络质量由于拥塞、数据包丢失和高延迟而导致网络质量较差。

使用 EDT 时要注意以下几点。

- 默认情况下，虚拟服务器级别的 DTLS 旋钮处于启用状态。
- 不支持使用 DTLS 的 SNI。
- 不支持使用 DTLS 的 IPv6。
- 如果启用了 DTLS，智能控制策略和 ICA 策略将不起作用。
- 此外，设备现在可以配置为 Receiver 和 VDA 之间的 EDT 流量的双跃点功能。有关更多信息，请单击在双跃点 DMZ 中部署。

> 注意：版本 12.1 版本 49.xx 及更高版本中的 MPX FIPS 平台支持 EDT。在基于英特尔科莱托 SSL 芯片的 MPX 设备上，EDT 从 12.1 版本 51.16 及更高版本支持。

配置 Citrix Gateway 以支持 Enlightened Data Transport 和 HDX Insight

April 6, 2020

通过网关的 EDT 流量现在具有端到端的可视性。Citrix ADM 具有实时和历史可见性数据，能够支持各种各样的使用案例。

支持以下方案：

情景	EDT 支持
Citrix Gateway	是
具有高可用性 (HA) 的 Citrix Gateway	是
具有高可用性 (HA) 优化的 Citrix Gateway	是
使用 Unified Gateway 的 Citrix ADC	是
带 GSLB 的 Citrix Gateway	是
带群集的 Citrix Gateway	是
Citrix Workspace 应用程序到 Citrix Gateway DTLS 加密	是
Citrix Gateway 上的双安全票务机构 (STA)	是
Citrix Gateway ICA 会话超时	是
Citrix Gateway 多流 ICA	是
Citrix Gateway 会话可靠性（端口 2598）	是
Citrix Gateway 双跃点	是
Citrix ADC 到 VDA DTLS 加密	是
HDX Insight	是
IPv6 模式下的 Citrix Gateway	否
Citrix Gateway SOCKS（端口 1494）	否
Citrix ADC 纯 LAN 代理	否

配置 Citrix Gateway 以支持 Enlightened Data Transport

如果使用 Enlightened Data Transport (EDT)，则必须启用数据报传输层安全性 (DTLS) 才能加密 EDT 使用的 UDP 连接。必须在网关 VPN 虚拟服务器级别启用 DTLS 参数。此外，必须正确升级和配置 Citrix Virtual Apps and Desktops 组件，以实现网关 VPN 虚拟服务器与用户设备之间的加密流量。

> 注意：为 Citrix Gateway 前端虚拟服务器配置的 UDP 端口（例如端口 443）必须在 DMZ 中打开虚拟服务器才能接收 DTLS 连接。DTLS 和 CGP 是 EDT 与 Citrix Gateway 一起工作的先决条件。

使用 **GUI** 将 **Citrix Gateway** 配置为支持 **EDT**

1. 部署和配置 Citrix Gateway 以便与 StoreFront 进行通信，并对 Citrix Virtual Apps and Desktops 进行身份验证。
2. 在 Citrix ADC GUI 的“配置”选项卡上，展开 **Citrix Gateway** 并选择虚拟服务器。
3. 单击 编辑显示 VPN 虚拟服务器的基本设置，然后验证 DTLS 设置的状态。
4. 单击“更多”以显示其他配置选项。
5. 选择 **DTLS** 为数据报协议提供通信安全性。单击确定。VPN 虚拟服务器的 基本设置区域显示 DTLS 标志设置为 T **rue** 。

使用 **CLI** 配置 **Citrix Gateway** 以获得 **EDT** 支持

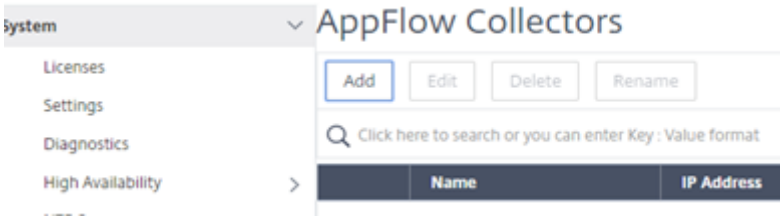
```
set vpn vserver vs1 -DTLS ON
```

配置 **Citrix Gateway** 以支持 **HDX Insight**

HDX Insight 为通过 Citrix ADC 传递到虚拟应用程序和桌面的 HDX 流量提供端到端可见性。它还使管理员能够查看实时客户端和网络延迟指标、历史报告、端到端性能数据，并对性能问题进行故障排除。

使用 **GUI** 配置 **Citrix Gateway** 以支持 **HDX Insight** 能分析

1. 在配置选项卡上，导航到系统 **> AppFlow > Collector**，然后单击添加。



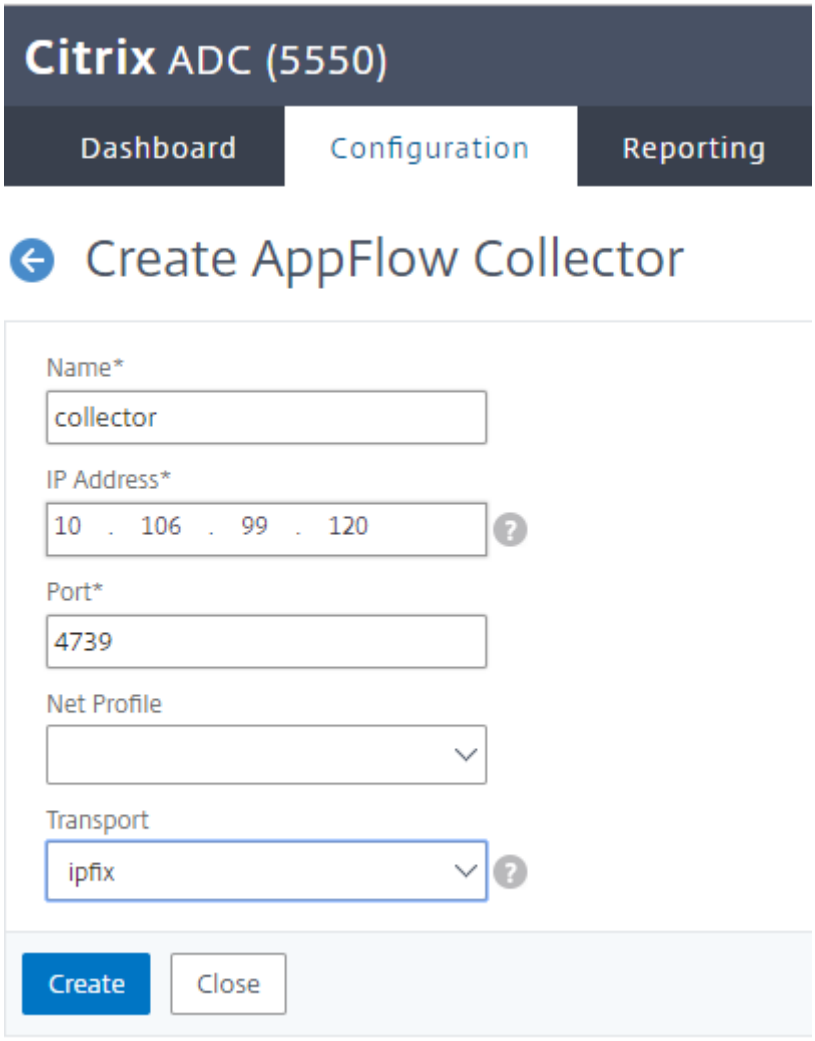
2. 在创建 **AppFlow Collector** 页面上，填充以下字段，然后单击“创建”。
   名称 — 收集器的名称

   IP 地址 — 收集器的 IPv4 地址

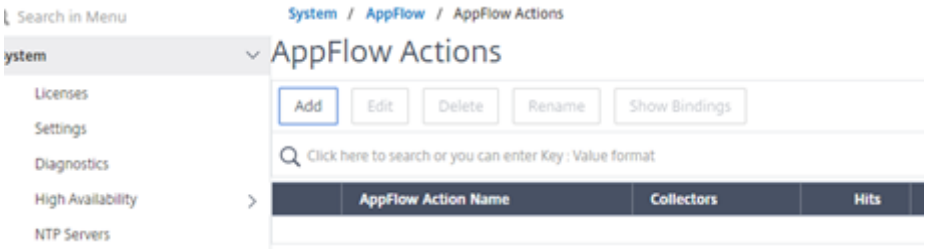
   端口 — 收集器侦听的端口

   网络配置文件-要与收集器关联的网络配置文件。在配置文件中定义的 IP 地址用作此收集器的 AppFlow 流量的源 IP 地址。如果未设置此参数，则将使用 Citrix ADC IP (NSIP) 地址作为源 IP 地址。

运输 — 收集器的运输类型。



3. 导航到系统 **> AppFlow >** 操作，单击添加。



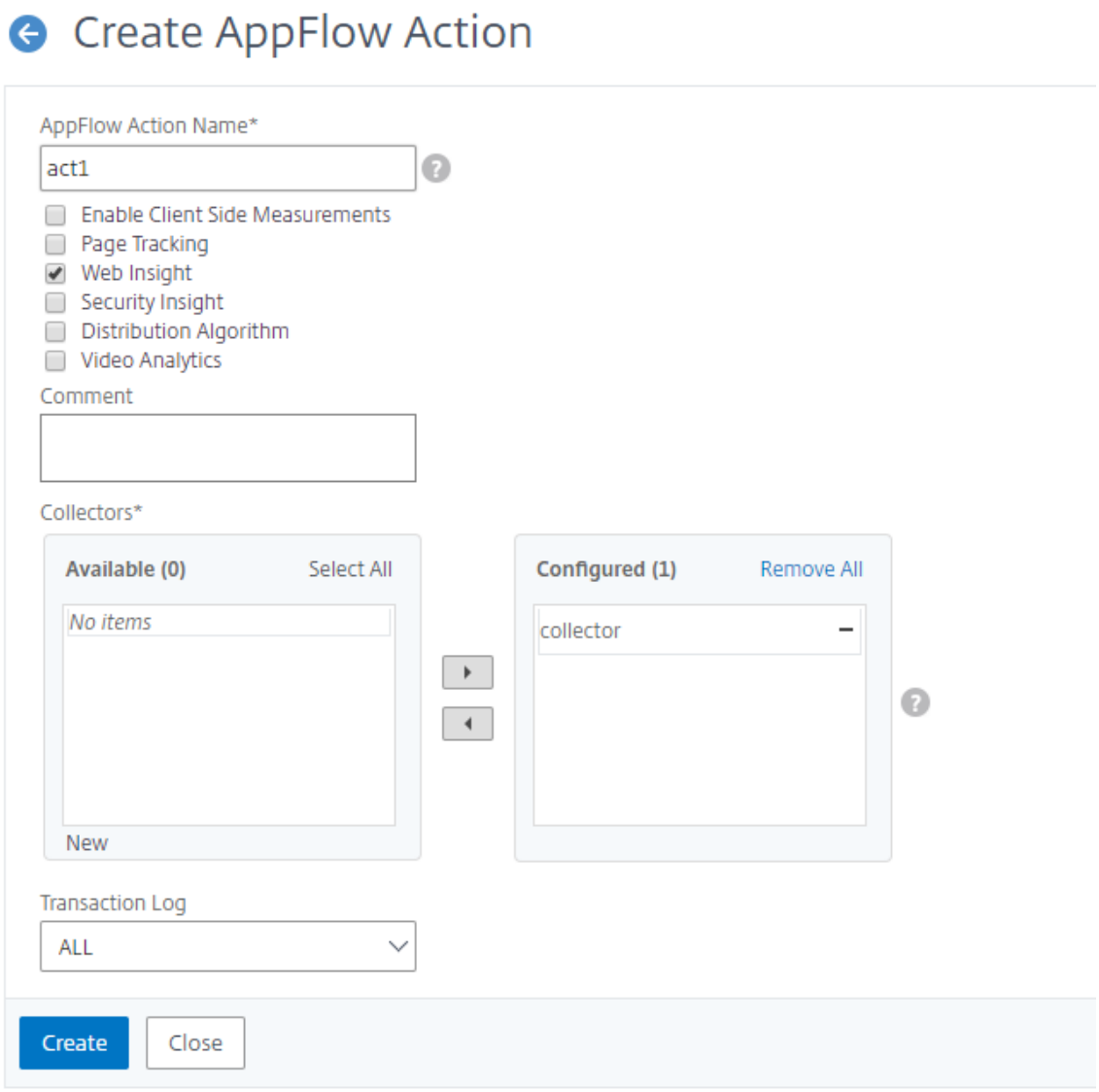
4. 在“创建 **AppFlow** 操作”页上，填充以下字段，然后单击“创建”。

   AppFlow 操作名称 - 操作的名称

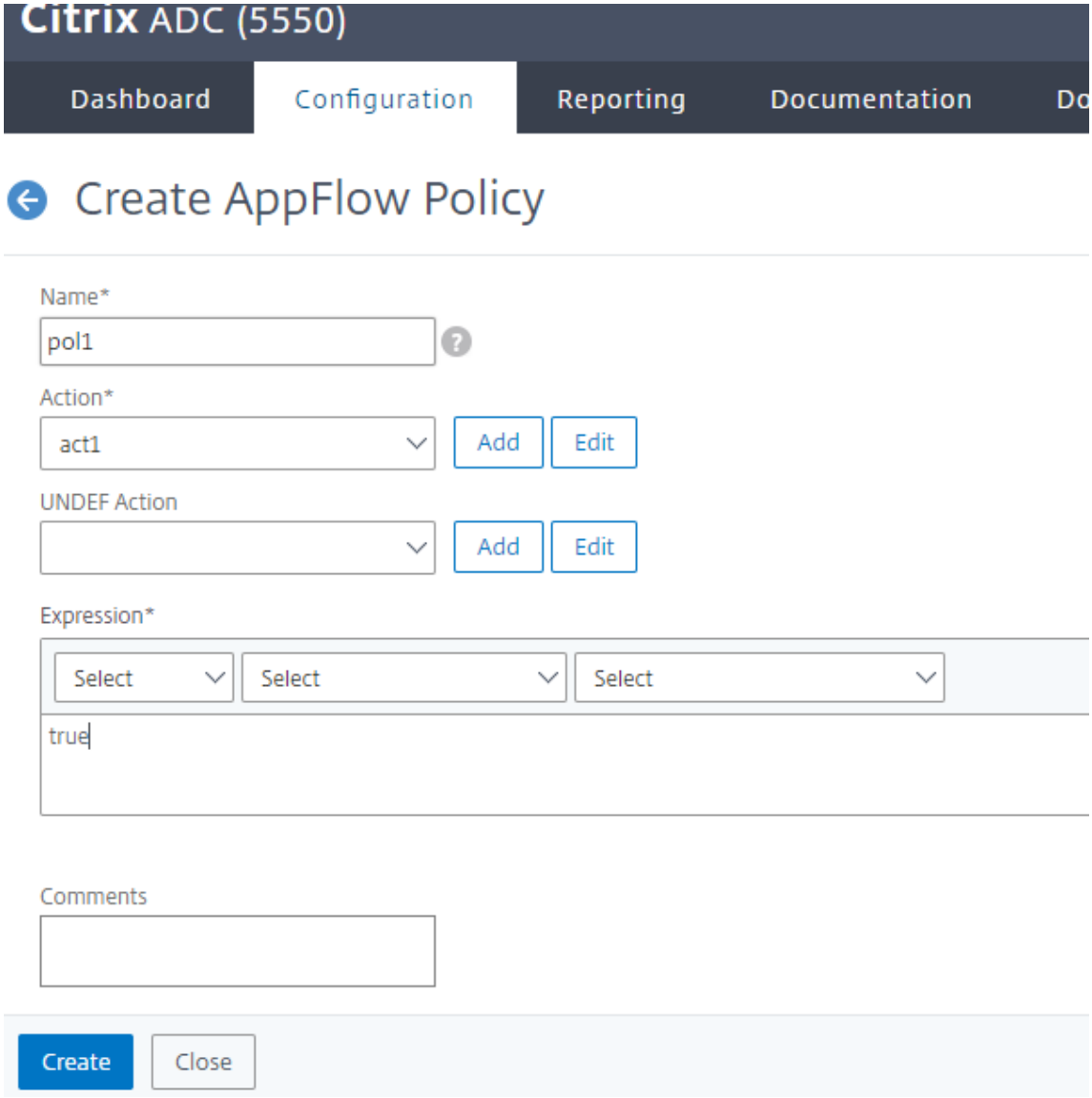
   评论 — 关于操作的任何评论

   Collector - 选择要与 AppFlow 操作关联的 Collector 的名称。

事务日志 — 要记录的事务类型。



5. 导航到系统 **> AppFlow >** 策略，单击添加。



6. 在创建 **AppFlow** 策略页面上，填充以下字段，然后单击创建。

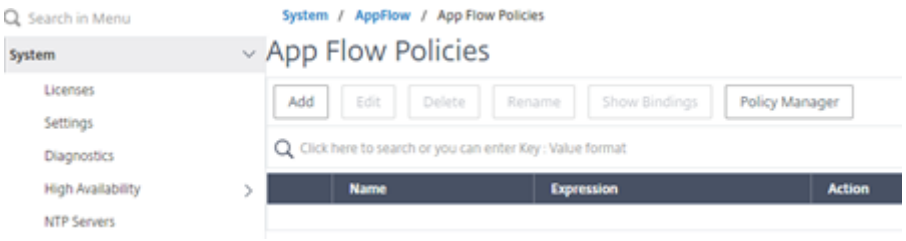
   名称 — 策略的名称。

   操作 — 要与策略关联的操作的名称。

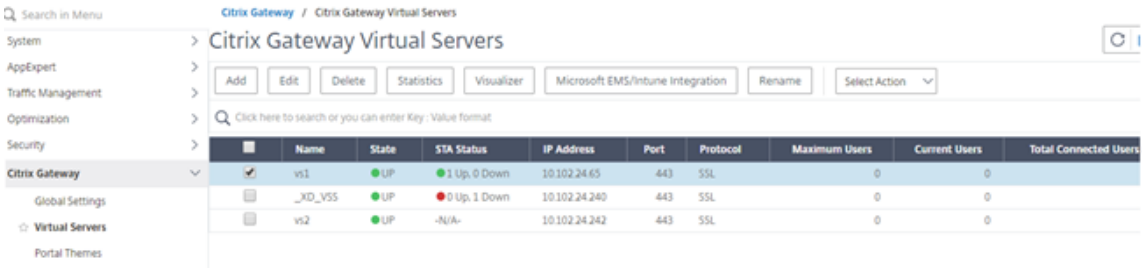
   UNDEF - 在发生未定义的事件时与此策略关联的 AppFlow 操作的名称。

   表达式-评估流量所依据的表达式或其他值。必须是布尔表达式。

   注释 — 关于此政策的任何注释。

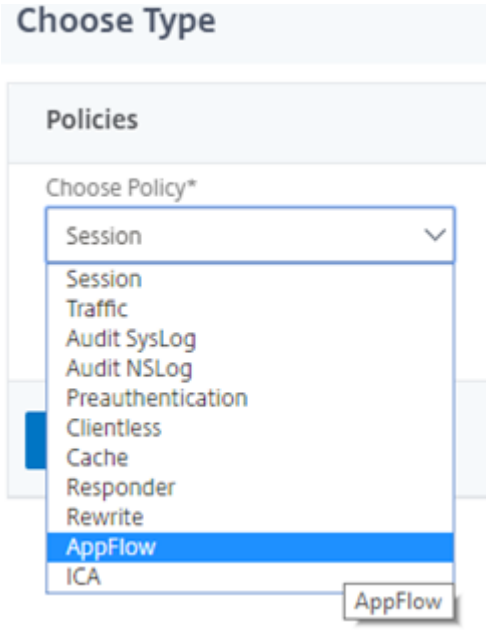


7. 导航到 **Citrix Gateway >** 虚拟服务器，选择“虚拟服务器”，然后单击编辑。

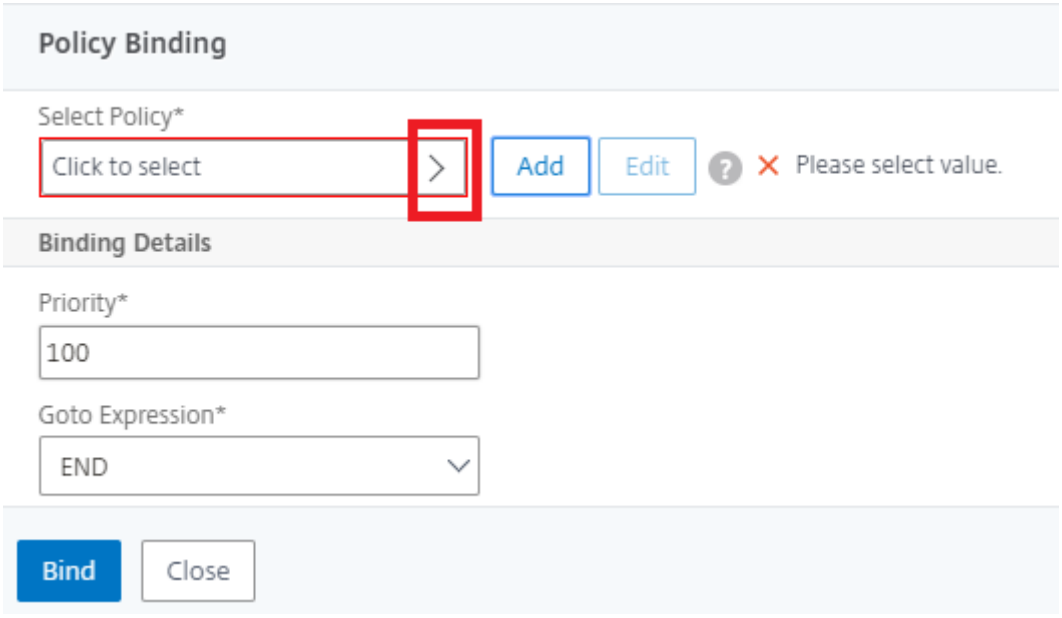


8. 向下滚动 **VPN** 虚拟服务器页面，然后在 策略部分下单击 **+** 。

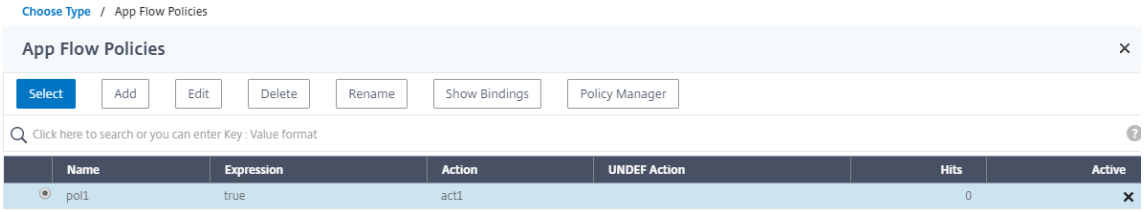
9. 在选择类型屏幕上的选择策略下拉菜单中，选择 **AppFlow**。在“选择类型”下拉菜单中，选择“请求”或“**ICA** 请求”，然后单击“继续”。



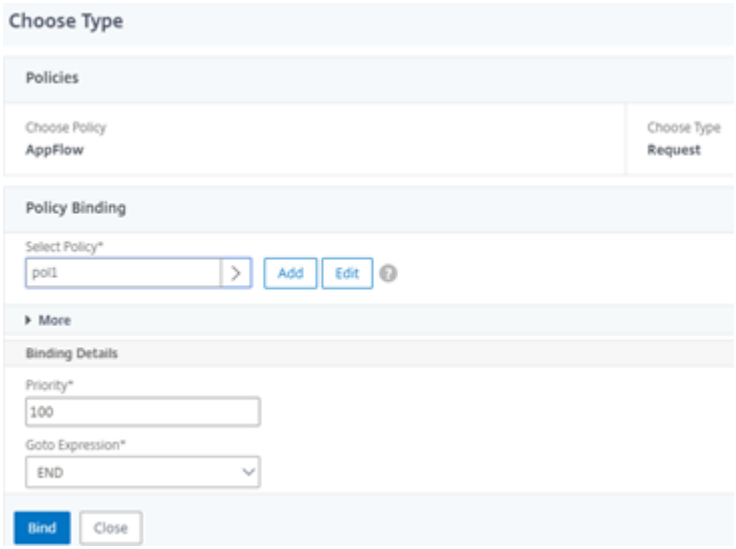
10. 单击 选择策略下突出显示的箭头。



11. 选择 **AppFlow** 策略，然后单击选择。



12. 最后点击 绑定。



要使用 **CLI** 配置 **Citrix Gateway** 以获得 **HDX Insight** 支持，请键入以下命令

```
1 add appflow collector col3 -IPAddress<ip_mas>
```



```
2 add appflow action act1 <action_name>
3 add appflow policy <policy_name> true <action_name>
4 bind vpn Vserver <vserver_name>  -pol <policy_name> - priority101 END -
     type <ICA_Request>
```

禁用非 **NSAP HDX** 会话的 **HDX Insight**

在 Citrix ADC 设备中，您现在可以为非 NSAP HDX 会话禁用 HDX Insight。

在命令提示窗口中，键入：

```
1 set ica parameter
2 DisableHDXInsightNonNSAP(YES | NO )
```

默认情况下，启用非 NSAP 会话的 HDX Insight。

L7 延迟阈值

April 6, 2020

HDX Insight 中的 L7 延迟阈值功能在应用程序级别主动检测端到端网络延迟问题，并采取主动措施。L7 延迟阈值功能执行实时延迟监控以检测峰值，并在延迟超过观测到的最小延迟时向 Insight Center 发送通知。

以前，平均客户端和服务器端 L7 延迟值每 60 秒发送一次到 Insight Center。在此区间内看到的任何峰值均会被平均化，因此仍未被发现。此外，没有实时延迟监控来检测这些峰值。

L7 延迟与 **L4** 延迟有何不同

网络延迟也会捕获并显示在 L4 级别。这些延迟是从 TCP 层计算的，不需要解析 ICA 流量。因此，它们相对容易获得，CPU 密集程度较低。但是，L4 延迟的主要缺点是了解端到端延迟。如果路径中存在 TCP 代理，则 L4 延迟仅捕获从 Citrix ADC 到 TCP 代理的延迟。这可能会导致信息不完整，从而导致在调试问题时遇到困难。

L7 延迟是通过解析 ICA 流量计算的。L7 延迟计算在 ICA 层完成，因此中间代理不会导致不完整的延迟值。因此，提供端到端延迟检测。

下图显示了带和不带 TCP 代理的部署类型。

Fig 2. Deployment with TCP Proxies

ICA RTT 和 **L7** 延迟计算之间的差异

ICA RTT 表示从 Citrix Workspace 应用程序到 Virtual Desktop Agent (VDA) 的总往返时间。L7 延迟提供了有关客户端以及服务器端延迟的详细信息。L7 客户端延迟是 Citrix Workspace 应用程序到 Citrix Gateway 之间的延迟。L7 服务器延迟是 Citrix Gateway 到 VDA 之间的延迟。

> 注意：仅 Citrix Virtual Apps and Desktops 版本 7.13 及更高版本支持服务器端的服务器 L7 延迟计算。

使用 **CLI** 配置 **L7** 延迟阈值

1. 添加 ICA 延迟配置文件。

```
add ica latencyprofile <name> [-l7LatencyMonitoring ( ENABLED |
    DISABLED )] [-l7LatencyThresholdFactor <positive_integer>] [-
    l7LatencyWaitTime <positive_integer>] [-l7LatencyNotifyInterval <
    positive_integer>] [-l7LatencyMaxNotifyCount <positive_integer>]
<!--NeedCopy-->
```

2. 添加 ICA 操作。

```
add ica action <name> [-latencyprofileName <string>]
<!--NeedCopy-->
```

3. 添加 ICA 策略。

```
add ica policy <name> -rule <expression> -action <string> [-comment<
    string>] [-logAction <string>
<!--NeedCopy-->
```

4. 将 ICA 策略绑定到 VPN 服务器或 ICA 全局绑定点。

```
bind ica global -policyName <string> -priority <positive_integer> [-
    gotoPriorityExpression <expression>] [-type ( ICA_REQ_OVERRIDE |
    ICA_REQ_DEFAULT )]
<!--NeedCopy-->
```


或者

```
bind vpn vserver <name> -policy <string>  [-priority <positive_integer
    >]
<!--NeedCopy-->
```

或者

```
bind cr vserver <name> -policy <string> [-priority <positive _integer>]
<!--NeedCopy-->
```

参数

- 延迟监控：用于启用或禁用 L7 阈值监控的参数。启用此参数后，当满足设置的条件时，通知将发送到 Insight Center。

  默认值：已禁用

- **LatencyThresholdFactor**：活动延迟必须大于观测到的最小延迟才能得出超过阈值并因此必须向 Insight Center 发送通知的因子。

  默认值：4

  最小值：2

  最大值：65535

- **LatencyWaitTime**：设备等待超过延迟阈值以向 Insight Center 发送通知的时间（以秒为单位）。

  默认值：20

  最小值：1

  最大值：65535

- **LatencyNotifyInterval**：设备在等待时间过后向 Insight Center 发送后续通知的时间间隔（以秒为单位）。

  默认值：20

  最小值：1

  最大值：65535

- **LatencyMaxNotifyCount**：在延迟超过阈值的时间间隔内可以发送到 Insight Center 的最大通知数。

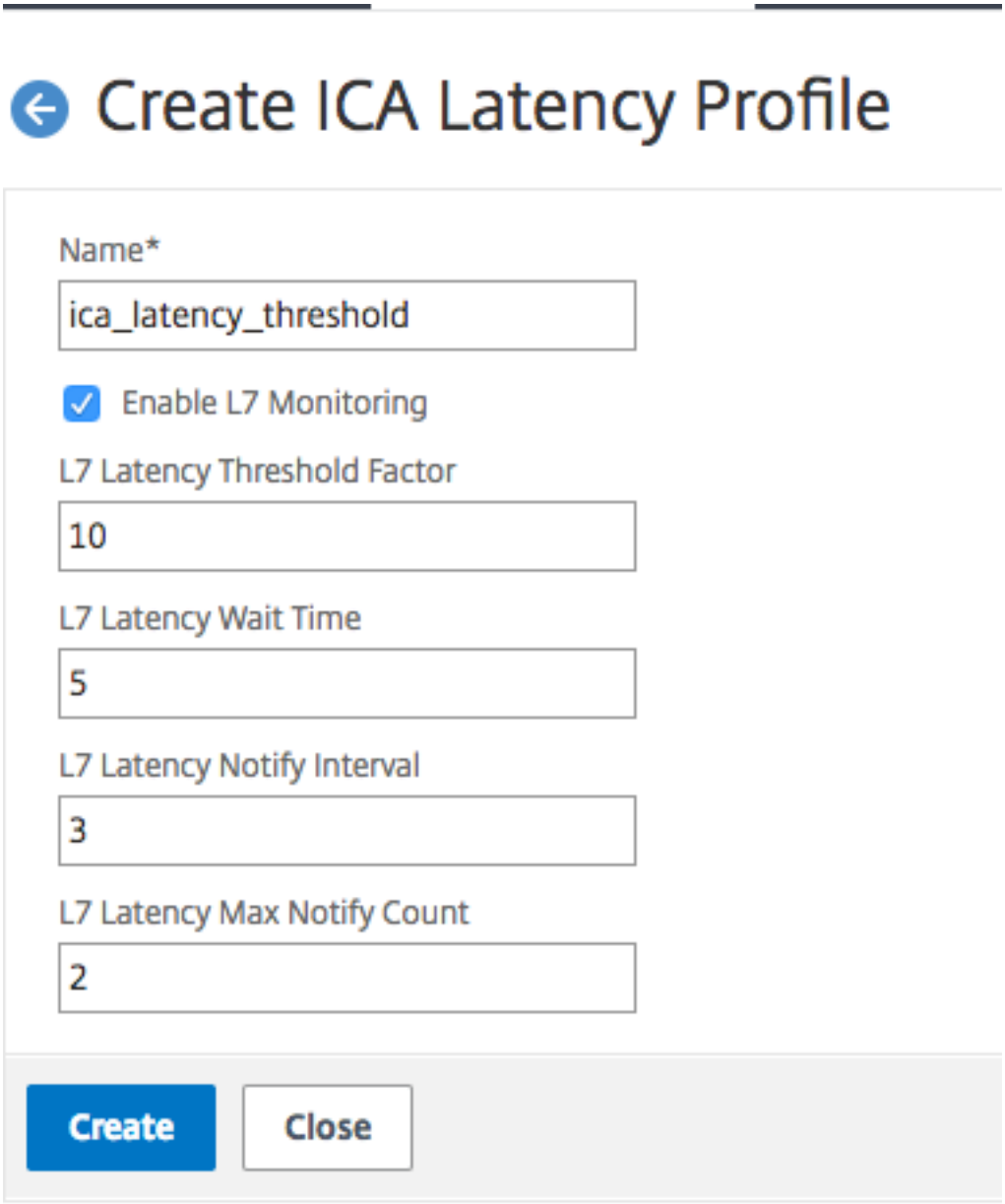
  默认值：5

使用 **GUI** 配置 **L7** 延迟阈值

1. 导航到配置 > **NetScaler Gateway** > 策略 > **ICA**。

2. 选择 **ICA** 延迟配置文件选项卡，然后单击 添加。

3. 在“创建 **ICA** 延迟配置文件”页面中，执行以下操作。



- 选择 **L7** 延迟监控以启用 L7 阈值监控。
- 在 **L7** 阈值因子中，输入活动延迟应超过观测到的最小延迟的值，以便向 Insight Center 发送通知。
- 在 **L7** 延迟等待时间中，输入设备在超过阈值以向 Insight Center 发送通知后等待的时间（以秒为单位）。
- 在 **L7** 延迟通知间隔中，输入设备在等待时间过后向 Insight Center 发送后续通知的时间（以秒为单位）。
- 在 **L7** 延迟最大通知计数中，输入延迟超过阈值的时间间隔内可以发送到 Insight Center 的最大通知数。

> 注意：一旦超过阈值，L7 最大延迟通知计数将适用，当活动延迟低于阈值时重置。这些通知的周期由通知间隔决定。

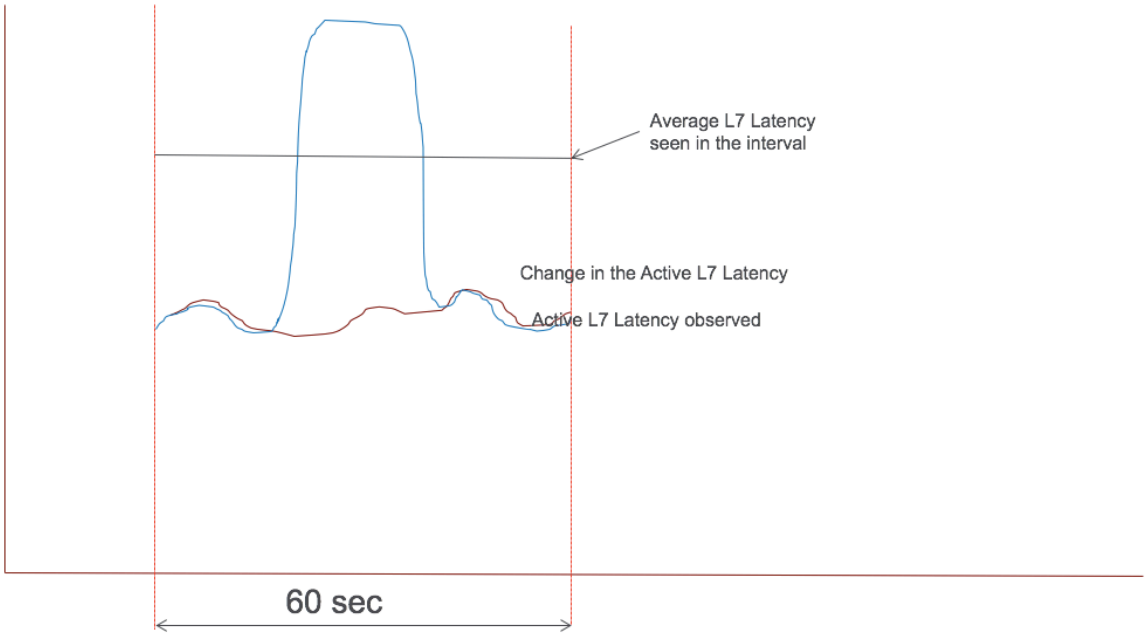
4. 单击创建。

L7 延迟测量模型与 L7 延迟阈值报告模型

L7 延迟测量模型

在 L7 延迟测量模块中，平均客户端和服务器端 L7 延迟值每 60 秒发送到 Insight Center。因此，在此区间内看到的峰值会被平均化，因此不会被检测到。此外，L7 延迟测量模块没有实时延迟监控功能。

下图说明了示例 L7 延迟测量模型。

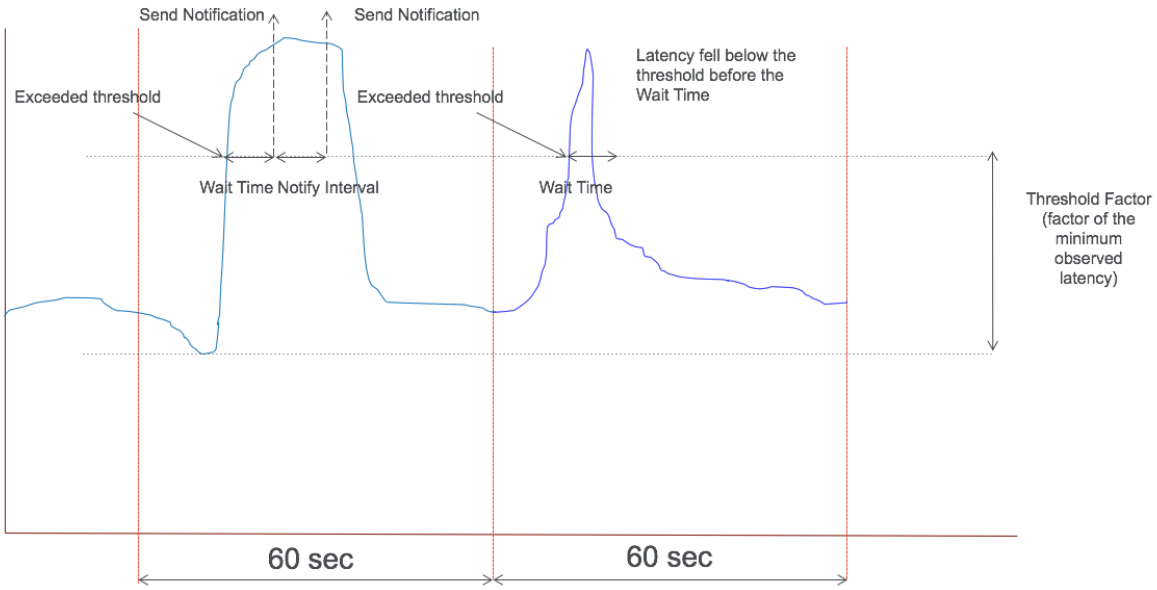


L7 延迟阈值报告模型

L7 延迟阈值报告模型具有实时延迟监控功能来检测峰值。如果延迟超过观测到的最小延迟，则会向 Insight Center 发送通知。

每当超过阈值因子时，都会检测到延迟增加。配置的阈值等待时间过期后，系统会向 Insight Center 发送通知。等待时间过期并且仍超过阈值因子后，将向 Insight Center 发送后续通知。
如果延迟值在等待时间到期之前低于阈值因子，则不会向 Insight Center 发送任何通知。

下图说明了示例 L7 延迟阈值报告模型。



可以在运行时配置以下参数：

- 阈值监控（开/关）
- 阈值因子
- 阈值等待时间
- 通知间隔
- 最大通知计数

Microsoft Intune 集成

November 3, 2021

Microsoft Intune 与 Citrix Gateway 的集成提供了由 Citrix Gateway 和 Intune 提供的最佳应用程序访问和数据保护解决方案。

您可以获得最完整的安全生产力应用套件，包括电子邮件、日历、联系人、笔记、文档编辑和远程访问，所有这些都可以跨不同平台集中管理。Intune 和 Citrix Gateway 集成提供了世界级的移动设备管理 (MDM) 功能，而 Citrix Gateway 客户端技术使这些 Intune 开明的应用程序能够通过 Citrix Gateway 安全访问公司数据和应用程序。

通过集成，Citrix Gateway 可以从 Intune 中提取合规性数据，从而启用条件访问策略。有条件访问策略使 Citrix Gateway 能够更精细地控制基于设备功能等的访问。例如，管理员可以创建一个策略，其中只有禁用 “Camera” 的设备才被授予访问权限。

在配置 Citrix Gateway 虚拟服务器后，Citrix Gateway 支持 Azure Active Directory Libraries (ADAL) 令牌身份验证。配置后，使用 Citrix 仅网络包装器或 SDK 包装的移动应用程序使用 ADAL 令牌访问 Citrix Gateway，该应用程序可以直接从 AAD 中获取该令牌。

Citrix Micro VPN 与 Microsoft Endpoint Manager 集成

Citrix Gateway 客户可以对 Microsoft Endpoint Manager (Intune) 使用 Micro VPN。Citrix Micro VPN 与 Microsoft Endpoint Management 集成使您的应用程序能够访问本地资源。

Citrix 微型 VPN 技术提供了一种按需 VPN，可降低数据传输成本并简化安全性，因为 VPN 隧道并非始终处于活动状态。相反，它仅在需要时处于活动状态，从而降低了风险并优化了设备的性能，从而获得更好的用户体验。这也有助于延长移动电池寿命。Citrix 的微型 VPN 技术为移动用户提供了对内部业务资源的安全访问，同时为他们提供最佳用户体验。

微型 VPN 仅支持以下使用案例：

- 仅 Intune 移动应用程序管理 (MAM)
- Intune 移动设备管理 (MDM) 和移动应用程序管理 (MAM)

> 重要：
>
> - Citrix Gateway 客户有权在 2021 年 1 月之前将 Micro VPN 与 Microsoft Endpoint Manager 结合使用，无需额外费用。
> - 微型 VPN 需要 Citrix Gateway 高级版或高级版（VPX 3000 或更高版本）才能使 SSL VPN 功能。

有关设置 Citrix Micro VPN 与 Microsoft Endpoint Manager 集成的详细信息，请参阅设置 Citrix Gateway 以便对 Microsoft Endpoint Manager 使用 Micro VPN。

何时使用集成的 Intune MDM 解决方案

April 6, 2020

以下场景说明了集成 Intune MDM 解决方案的使用：

- 新客户决定在 Intune 上使用预置 Citrix Gateway 部署
- 现有 Citrix Gateway 用户想要使用 Intune 添加移动设备管理
- 现有 Intune 用户希望允许移动设备和/或应用程序访问位于公司 DMZ 中的 Citrix Gateway 物理或虚拟设备的公司网络内的数据

> 注意
>
> 仅支持 iOS 和 Android 客户端。

了解 Citrix Gateway-Intune MDM 集成

April 6, 2020

以下是典型 Citrix Gateway-Intune MDM 集成中事件流的示例：

1. 使用 Intune 注册移动设备。
2. 公司批准的应用程序和设备策略将推送到设备。
3. 从设备浏览 SharePoint（本地应用程序）。
4. 浏览器请求转到 Citrix Gateway。
5. Citrix Gateway 设备使用 Intune 检查设备的注册状态。
6. 如果成功注册了符合规定的设备，则将授予 SharePoint 访问权限。

当设备未满足条件访问 (CA) 策略时，Citrix Gateway VPN 客户端会向用户显示一条错误消息，其中包含指向 Intune 托管的页面的链接，以注册或修复设备合规性状态。

注意：管理员在将证书推送到 Intune 时必须确保满足以下条件，以便用户能够区分其设备上的各种证书。

- 证书必须具有主题摘要。
- 不同证书的主题摘要必须是不同的。

为 **Citrix Gateway** 虚拟服务器配置网络访问控制设备检查以实现单因素登录

January 10, 2023

> 重要
>
> 以下部分列出了使用 Citrix Gateway 配置 Intune 的步骤。有关在 Azure 门户上配置 Citrix Gateway 应用程序以获取 客户端 **ID**、客户端密钥和 租户 **ID** 的信息，请参阅 Azure 产品文档。
>
> 以下功能需要 **Citrix ADC** 高级版许可证。

为网关部署添加具有 **nFactor** 的 **Citrix Gateway** 虚拟服务器

1. 导航到 Citrix Gateway 树节点下的虚拟服务器。
2. 单击添加。
3. 在“基本设置”区域中提供所需信息，然后单击“确定”。
4. 选择 服务器证书。
5. 选择所需的服务器证书，然后单击“绑定”。
6. 单击继续。
7. 单击继续。
8. 单击继续。
9. 单击策略旁边的加号图标 **[+]**，然后从选择策略列表中选择会话，然后从选择类型列表中选择请求，然后单击继续。
10. 单击选 择策略 **+**[+]** 旁边的加号图标。

11. 在“创建 **NetScaler Gateway** 会话策略”页面上，提供会话策略的名称。
12. 单击配置文件旁边的加号图标 [+]，并在创建 **NetScaler Gateway** 会话配置文件页面上，提供会话配置文件的名称。
13. 在“客户端体验”选项卡上，单击“无客户端访问”旁边的复选框，然后从列表中选择“关闭”。
14. 单击插件类型旁边的复选框，然后从列表中选择 Windows/MAC OS X。
15. 单击“高级设置”，然后选中“客户端选择”旁边的复选框，并将其值设置为“开”。
16. 在“安全”选项卡上，单击“默认授权操作”旁边的复选框，然后从列表中选择“允许”。
17. 在“已发布的应用程序”选项卡上，单击 **ICA** 代理旁边的复选框，然后 从列表中选择关。
18. 单击创建。
19. 在“创建 **NetScaler Gateway** 会话策略”页上的“表达式”区域下输入 **NS_TRUE** 。
20. 单击创建。
21. 单击 **Bind**（绑定）。
22. 在 高级设置中选择 身份验证配置文件。
23. 单击加号图标 **[+]** 并提供身份验证配置文件的名称。
24. 单击加号图标 **[+]** 以创建身份验证虚拟服务器。
25. 在“基本设置”区域下指定身份验证虚拟服务器的名称和 IP 地址类型，然后单 击 **“**确定”。IP 地址类型也可以是不可寻址的。
26. 单击 身份验证策略。
27. 在策略绑定视图下，单击加号图标 **[+]** 以创建身份验证策略。
28. 选择 **OAUTH** 作为 操作类型，然后单击加号图标 **[+]** 为 NAC 创建 OAuth 操作。
29. 使用 客户端 **ID**、客户端密钥和 租户 **ID** 创建 OAuth 操作。

    在 Azure 门户上配置 **Citrix Gateway** 应用程序后，将生成客户端 **ID**、客户端密钥和租户 ID。

    确保您的设备上配置了适当的 DNS 名称服务器以解析和访问https://login.microsoftonline.com/https://graph.windows.net/、和 *.manage.microsoft.com。
30. 为 **OAuth** 操作创建身份验证策略。

规则： http.req.header(“User-Agent”).contains(“NAC/1.0”)&& ((http.req.header(“User-Agent”).contains(“iOS”) && http.req.header(“User-Agent”).contains(“NSGiOSplugi	(http.req.header(“User-Agent”).contains(“Android”) && http.req.header(“User-Agent”).contains(“CitrixVPN”)))

31. 单击加号图标 **[+]** 以创建 “下一因子” 策略标签。
32. 单击加号图标 **[+]** 以创建登录架构。
33. 选择 **noschema** 作为身份验证架构，然后单击 “创建”。
34. 选择创建的登录架构后，单击 继续。
35. 在 “选择策略” 中，选择用户登录的现有身份验证策略，或单击加号图标 **+** 以创建身份验证策略。有关创建身份验证策略
    的详细信息，请参阅配置高级身份验证策略。
36. 单击 **Bind**（绑定）。
37. 单击完成。
38. 单击 **Bind**（绑定）。
39. 单击继续。
40. 单击完成。
41. 单击创建。
42. 单击确定。
43. 单击完成。

将身份验证登录架构绑定到身份验证虚拟服务器，以指示 VPN 插件作为 /cgi/login 请求的一部分发送设备 ID

1. 导航到 安全 > **AAA-**应用程序流量 > 虚拟服务器。
2. 选择先前选择的虚拟服务器，然后单击 编辑。
3. 单击 “高级设置” 下的 登录架构。
4. 单击 登录架构进行绑定。
5. 单击 **[>]** 以在登录架构策略中选择和绑定 NAC 设备检查的现有内部版本。

6. 选择适合您的身份验证部署的所需登录架构策略，然后单击“选择”。

   在上述部署中，使用单因素身份验证 (LDAP) 以及 NAC OAuth 操作策略，因此已选择 **lschema_** 单因厂 **_** 设备 **eid** 。

7. 单击 **Bind**（绑定）。

8. 单击完成。

了解 **Azure ADAL** 令牌身份验证

April 6, 2020

以下是典型的 Citrix Gateway-Microsoft ADAL 令牌身份验证中的事件流程：

1. 在 iOS 或 Android 中启动应用程序时，该应用程序将联系 Azure。系统会提示用户使用用户凭据登录。成功登录后，应用程序将获得 ADAL 令牌。

2. 此 ADAL 令牌将呈现给 Citrix Gateway，该网关已配置为验证 ADAL 令牌。

3. Citrix Gateway 使用来自 Microsoft 的相应证书验证 ADAL 令牌的签名。

4. 验证成功后，Citrix Gateway 会提取用户的主体名称 (UPN)，并授予应用程序 VPN 访问内部资源。

为 **Microsoft ADAL** 令牌身份验证配置 **Citrix Gateway** 虚拟服务器

November 7, 2022

若要配置 Citrix Gateway 虚拟服务器以监视 Microsoft ADAL 令牌身份验证，您需要以下信息：

- certEndpoint：包含用于 ADAL 令牌验证的 Json Web 密钥 (JWK) 端点的 URL。
- 受众：应用程序向其发送 ADAL 令牌的 Citrix ADC 虚拟服务器的 FQDN。
- 颁发者：AAD 颁发者的名称。默认情况下获取填充。
- TenantID：Azure ADAL 注册的租户 ID。
- ClientID：作为 ADAL 注册的一部分，给网关应用程序的唯一 ID。
- ClientSecret：作为 ADAL 注册的一部分，给网关应用程序的秘密密钥。

1. 创建一个 OAuthAction：

   add authentication OAuthAction <oauth_action_name>
   -OAuthType INTUNE –clientid <client_id> -
   clientsecret <client_secret>
   -audience <audience>
   -tenantid <tenantID>

-issuer <issuer_name> -
userNameField upn-certEndpoint <certEndpoint_name>

示例:

add authentication OAuthAction tmp_action -OAuthType INTUNE -clientid id 1204 -clientsecret a -audience “
http://hello” -tenantid xxxx -issuer “
https://hello” -userNameField upn -certEndpoint
https://login.microsoftonline.com/common/discovery/v2.0/keys

2. 创建身份验证策略以与新创建的 OAuth 关联:

   add
   authentication Policy <policy_name>
   -rule true -action <oauth intune action>

   示例:

   add authentication Policy oauth_intune_pol -rule true -action tmp_action

3. 将新创建的 OAuth 绑定到 AuthVS:

   bind authentication vserver <auth_vserver>
   -policy <oauth_intune_policy>
   -priority 2 -gotoPriorityExpression END

   示例:

   bind authentication vserver auth_vs_for_gw1_intune -policy oauth_pol -priority 2 -gotoPriorityExpression END

4. 创建 LoginSchema:

   add authentication loginSchema <loginSchemaName>
   -authenticationSchema <authenticationSchema”location”>

   add authentication loginSchemaPolicy <loginSchemaPolicyName>
   -rule true -action <loginSchemaName>

   示例:

   add authentication loginSchema oauth_loginschema -authenticationSchema “/nsconfig/login-schema/LoginSchema/OnlyOAuthToken.xml”

   add authentication loginSchemaPolicy oauth_loginschema_pol -rule true -action oauth_loginschema

5. 使用 LoginSchema 绑定 AuthVS:

   bind authentication vserver <auth_vs> **-policy** <oauth_pol> **-priority 2 -gotoPriorityExpression END**

示例:

bind authentication vserver auth_vs_for_gw1_intune -policy oauth_loginschema_pol -priority 2 -gotoPriorityExpression END

6. 添加 authnprofile 并将其分配给 VPN 虚拟服务器:

   add authnprofile <nfactor_profile_name>**-authnvsName** <authvserver>

   set vpn vserver <vserverName>**-authnprofile** <nfactor_profile_name>

   示例:

   add authnprofile nfactor_prof_intune -authnvsName auth_vs_for_gw1_intune

   set vpn vserver gw1_intune-authnprofile nfactor_prof_intune

设置 Citrix Gateway 以便对 Microsoft Endpoint Manager 使用 Micro VPN

April 6, 2020

Citrix Micro VPN 与 Microsoft Endpoint Management 集成使您的应用程序能够访问本地资源。有关详细信息，请参阅Citrix Micro VPN 与 Microsoft Endpoint Manager 集成。

系统要求

- Citrix Gateway 版本 12.0.59.x 或 12.1.50.x 或更高版本。

  可以从 Citrix Gateway 下载页面下载最新版本的 Citrix Gateway。
- 运行 Windows 7 或更高版本的 Windows 桌面（仅适用于 Android 应用程序打包）
- Microsoft
  - Azure AD 访问权限（具有租户管理权限）
  - 启用了 Intune 的租户
- 防火墙规则
  - 启用防火墙规则以允许 SSL 流量从 Citrix Gateway 子网 IP 传输到 `*.manage.microsoft.com`、`https://login.microsoftonline.com` 和 `https://graph.windows.net`（端口 443）
  - Citrix Gateway 必须能够在外部解析上述 URL。

必备条件

- **Intune** 环境：如果您没有 Intune 环境，请设置一个。有关说明，请参阅Microsoft 文档。

- **Edge** 浏览器应用程序： Micro VPN SDK 集成在适用于 iOS 和 Android 的 Microsoft Edge 应用程序和 Intune Managed Browser 应用程序中。有关 Managed Browser 的详细信息，请参阅 Microsoft Managed Browser 页面。

授予 **Azure Active Directory (AAD)** 应用程序权限

1. 同意 Citrix 多租户 AAD 应用程序，以允许 Citrix Gateway 使用 AAD 域进行身份验证。Azure 全局管理员必须访问以下 URL 并获得同意：

   https://login.windows.net/common/adminconsent?client_id=b6a53a76-5d50-499e-beb3-c8dbdad5c40b&redirect_uri=https://www.citrix.com&state=consent。

2. 同意 Citrix 多租户 AAD 应用程序，以允许移动应用程序使用 Citrix Gateway 微型 VPN 进行身份验证。只有当 Azure 全局管理员已将用户可以注册应用程序的默认值从是更改为否时，才需要此链接。
   此设置可以在 Azure 门户中的 Azure **Active Directory >** 用户 **>** 用户设置下找到。
   Azure 全局管理员必须访问以下 URL 并同意（添加
   租 户 ID）https://login.microsoftonline.com/%5Btenant_id%5D/adminconsent?client_id=9215b80e-186b43a1-8aed-9902264a5af7。

为微型 **VPN** 配置 **Citrix Gateway**

要将 Micro VPN 与 Intune 结合使用，必须将 Citrix Gateway 配置为对 Azure AD 进行身份验证。现有 Citrix Gateway 虚拟服务器不适用于此用例。
首先，将 Azure AD 配置为与本地 Active Directory 同步。此步骤对于确保 Intune 与 Citrix Gateway 之间正确进行身份验证是必要的。

下载脚本： .zip 文件包含一个自述文件，其中包含实施脚本的说明。您需要手动输入脚本所需的信息，并在 Citrix Gateway 上运行脚本以配置服务。您可以从下载脚本文件Citrix 下载页面。

> 重要提示：完成 Citrix Gateway 配置后，如果看到 “完成” 以外的 OAuth 状态，请参阅 “疑难解答” 部分。

配置 **Microsoft Edge** 浏览器

1. 登录到 https://portal.azure.com/，然后导航到 **Intune >** 移动应用程序。
2. 正常发布 Edge 应用程序，然后添加应用程序配置策略。
3. 在管理下，单击应用程序配置策略。
4. 单击添加，然后为要创建的策略输入名称。对于 “设备注册类型”，请选择 “托管应用”。
5. 点击一个分离的应用程序。
6. 选择要应用策略的应用程序（Microsoft Edge 或 Intune 托管浏览器），然后单 击确定。
7. 单击配置设置。
8. 在 “名称” 字段中，输入下表中列出的其中一个策略的名称。
9. 在值字段中，输入要为该策略应用的值。单击该字段以将策略添加到列表中。可以添加多个策略。

10. 单击确定，然后单击添加。

该策略将添加到您的策略列表中。

名称 (iOS/Android)	值	说明
MvpnGatewayAddress	`https://external.companyname.com`	Citrix Gateway 关的外部 URL
MvpnNetworkAccess	MvpnNetworkAccessTunneledWebSSO 不受限制	MvpnNetworkAccessTunneledWebSSO 为通道的默认设置
MvpnExcludeDomains	要排除的域名列表以逗号分隔	可选。默认值 = 空白

> 注意： Web SSO 是设置中 Secure Browse 的名称。该行为是相同的。

- **MvpnNetworkAccess** - MvpnNetworkAccessTunneledWebSSO 通过 Citrix Gateway（也称为 “通道 - Web SSO）启用 HTTP/HTTPS 重定向。Gateway 关在内联响应 HTTP 身份验证挑战，提供单点登录 (SSO) 体验。要使用 Web SSO，请将此策略设置为 **MvpnNetworkAccessTunneledWebSSO**。目前不支持完全隧道重定向。使用 “不受限制” 保持微型 VPN 隧道关闭状态。
- **MvpnExcludeDomains** - 要排除的通过 Citrix Gateway 反向 Web 代理路由的主机或域名的逗号分隔列表。即使 Citrix Gateway 配置的拆分 DNS 设置可能会选择域或主机，也会排除主机或域名。

  > 注意：此策略仅适用于 **MvpnNetworkAccessTunneledWebSSO** 连接。如果 MvpnNetworkAccess 设置为不受限制，则忽略此策略。

故障排除

常规问题

问题	解决方案
打开应用程序时显示 “需要添加策略” 消息	在 Microsoft Graph API 中添加策略
存在政策冲突	每个应用只允许使用单个策略
包装应用程序时会显示 “无法打包应用程序” 消息。有关完整消息，请参阅下面的	该应用程序与 Intune SDK 集成。您不需要使用 Intune 包装应用程序
您的应用无法连接到内部资源	确保正确的防火墙端口处于打开状态，正确的租户 ID 等

无法打包应用程序错误消息：

Failed to package app. com.microsoft.intune.mam.apppackager.utils.AppPackagerException: This app already has the MAM

SDK integrated.(无法打包应用程序。*com.microsoft.intune.mam.apppackager.utils.AppPackagerException:* 此应用程序已集成 *MAM SDK*。)
com.microsoft.intune.mam.apppackager.AppPackager.packageApp(AppPackager.java:113)
com.microsoft.intune.mam.apppackager.PackagerMain.mainInternal(PackagerMain.java:198)
com.microsoft.intune.mam.apppackager.PackagerMain.main(PackagerMain.java:56)
The application cannot be wrapped.

Citrix Gateway 问题

问题	解决方案
为 Azure 上的 Gateway 应用配置所需的权限不可用。	检查是否有适当的 Intune 许可证可用。尝试使用manage.windowsazure.com门户查看是否可以添加权限。如果问题仍然存在，请与 Microsoft 支持部门联系。
Citrix Gateway 无法访问login.microsoftonline.comandgraph.windows.net。	从 NS 壳，检查你是否能够访问以下 Microsoft 网站：curl-v-khttps://login.microsoftonline.com。然后，检查是否在 Citrix Gateway 上配置了 DNS。同时检查防火墙设置是否正确（如果 DNS 请求是防火墙）。
配置 OAuthAction 后，ns.log 中会出现错误。	检查 Intune 许可是否已启用，以及 Azure 网关应用程序是否设置了适当的权限。
Sh OAuthAction 命令不会显示 OAuth 状态为完成。	检查 Azure Gateway 应用程序的 DNS 设置和配置权限。
Android 或 iOS 设备不显示双重身份验证提示。	检查双重设备 ID 登录架构是否绑定到身份验证虚拟服务器。

Citrix Gateway OAuth 状态和错误条件

状态	错误状况
AADFORGRAPH	密钥无效、URL 未解析、连接超时
MDMINFO	*manage.microsoft.com已关闭或无法访问
GRAPH	图形端点已关闭，无法访问

状态	错误状况
CERTFETCH	由于 DNS 错误无法与令牌端点 https://login.microsoftonline.com 通信。要验证此配置，请转到 shell 并键入 curlhttps://login.microsoftonline.com。此命令必须验证。

注意：当 OAuth 状态成功时，状态将显示为 “完成”。

UDP 流量的服务支持类型

April 6, 2020

对 UDP 的服务类型 (ToS) 支持可确保一旦发件人为 UDP 数据包配置了 ToS 值，Citrix Gateway 将保留该值，直到数据包到达其目标。根据配置的值和目标网络的配置，目标网络将 UDP 数据包放置在优先级出站队列中。

> 注意
> 使用 ToS 信息，您可以为每个 IP 数据包分配优先级，并请求特定处理，如高吞吐量、高可靠性、低延迟等。

Citrix Gateway 的出站代理支持的代理自动配置

November 7, 2022

将 Citrix Gateway 设备配置为支持代理自动配置 (PAC) 时，PAC 文件的 URL 将推送到客户端浏览器。然后，根据 PAC 文件中定义的条件，来自客户端的流量将被重定向到相应的代理。

以下是出站代理 PAC 的一些常见用例：

- 配置多个处理客户端流量的代理服务器。
- 跨子网负载平衡代理流量。

使用命令行界面配置 Citrix Gateway 全局参数以支持出站代理的 PAC

在命令提示窗口中，键入：

```
1 ```
2 set vpn parameter -proxy BROWSER -autoProxyUrl <URL>
3 <!--NeedCopy--> ```
```

将 Citrix Gateway 配置为在会话配置文件中支持 PAC 的步骤

在命令提示窗口中，键入：

```
1 ```
2 add vpn sessionAction <name> -proxy BROWSER -autoProxyUrl <URL>
3 <!--NeedCopy--> ```
```

值

- URL — 代理服务器的 URL
- 名称 — VPN 会话操作的名称

使用 Citrix ADC GUI 配置 Citrix Gateway 全局参数以支持出站代理的 PAC

1. 导航到 配置 > **Citrix Gateway** > 全局设置。
2. 在 “全局设置” 页上，单击 “更改全局设置”，然后选择 “客户端体验” 选项卡。
3. 在 “客户端体验” 选项卡上，选择 “高级设置”，然后选择 “代理” 选项卡。
4. 在 “代理” 选项卡上，选择 “浏览器”，然后选择 “使用自动配置”。
5. 在 “到 自动代理配置文件的 URL” 字段中，键入所需 PAC 文件的 URL。
6. 点击 创建。

使用 Citrix ADC GUI 将 Citrix Gateway 配置为在会话配置文件上支持 PAC 的步骤

1. 导航到 配置 > **Citrix Gateway** > 策略 > 会话。
2. 在 Citrix Gateway 会话策略和配置文件页面上，创建 Citrix Gateway 会话配置文件。

要创建 Citrix Gateway 会话配置文件，请选择 “会 话配置文件” 选项卡，单击 “添加”，然后输入名称。

1. 在 “客户端体验” 选项卡上，选择 “高级设置”，然后选择 “代理” 选项卡。
2. 在 “代理” 选项卡上，选择 “浏览器”，然后选择 “使用自动配置”。
3. 在 “到 自动代理配置文件的 URL” 字段中，键入所需 PAC 文件的 URL。
4. 点击 创建。

出站 **ICA** 代理支持

April 6, 2020

对 Citrix Gateway 的出站 ICA 代理支持使网络管理员能够使用 SmartControl 功能，即使 Receiver 和 Citrix Gateway 部署在不同的组织中也是如此。

以下方案说明了出站 ICA 代理解决方案的使用：

当 Receiver 和 Citrix Gateway 部署在不同的组织中时，网络管理员需要控制 ICA 会话相关的功能。

了解出站 **ICA** 代理支持：

为了将 SmartControl 功能带到具有接收机的企业组织 A 公司，我们需要添加用作 LAN 代理的 Citrix ADC 设备。Citrix ADC LAN 代理强制执行智能控制，并将流量代理到公司 B 的 Citrix Gateway 在此部署方案中，Receiver 将流量转发到 Citrix ADC LAN 代理，从而允许 A 公司的网络管理员强制执行智能控制。部署情况如下图所示。

在这种情况下，LAN 代理和 Citrix Gateway 之间的流量通过 SSL。

> 注意不得在 Citrix Gateway 上启用基于
> 客户端证书的身份验证。

配置出站 **ICA** 代理

April 6, 2020

要使用 CLI 配置出站 ICA 代理，请按照下列步骤操作：

1. 添加缓存重定向虚拟服务器：

   add cr vserver <name> <serviceType> <IPAddress> <port> -**cacheType** <cacheType>

   服务必须是 HDX

   CacheType 必须为 FORWARD

   示例：

   add cr vserver CR_LAN_Proxy HDX 10.217.208.197 8080 -cacheType FORWARD

2. 添加 ICA 智能控制配置文件：

   add ica accessprofile <name> -**ConnectClientLPTPorts** (DEFAULT | DISABLED) **ClientAudioRedirection** (DEFAULT | DISABLED) -**LocalRemoteDataSharing** (DEFAULT | DISABLED) -**ClientClipboardRedirection** (DEFAULT | DISABLED) -**ClientCOMPortRedirection** (DEFAULT |DISABLED) -**ClientDriveRedirection** (DEFAULT | DISABLED) -**ClientPrinterRedirection** (DEFAULT |DISABLED) -**Multistream** (DEFAULT | DISABLED) -**ClientUSBDriveRedirection** (DEFAULT | DISABLED)

   示例：

   ```
   1 add ica accessprofile disableCDM -ConnectClientLPTPorts DEFAULT -
       ClientAudioRedirection DEFAULT  - LocalRemoteDataSharing DEFAULT
        -ClientClipboardRedirection DEFAULT -ClientCOMPortRedirection
       DEFAULT  - ClientPrinterRedirection DEFAULT -Multistream DEFAULT
        -ClientUSBDriveRedirection DEFAULT
   ```

3. 添加 ICA 操作：

   add ica action <name> **-accessProfileName** <string>

   示例：


```
add ica action disableCDM\_action -accessProfileName disableCDM
```

4. 添加 ICA 策略：

   add ica policy <name> **-rule** <expression> **-action** <string> **-comment** <string> **-logAction** <string>

5. 将 ICA 策略绑定到虚拟服务器或全局：

   a. 绑定到虚拟服务器

```
**bind cr vserver** \<name\> **-policyName** \<string\> **-
   priority** \<positive\_integer\>
```

   示例：

```
bind cr vserver CR\_LAN\_Proxy  - policyname disableCDM\_pol  -
   priority 10
```

   b. 绑定到全局

```
**bind ica global -policyName** \<string\> -**priority** \<
   positive\_integer\>
```

   示例：

```
bind ica global  - policyName disableCDM\_pol  - priority 10
```

> 注意
>
> 设置安全 ICA 端口：此值是 LAN 代理与其建立出站连接的 Citrix Gateway 上的端口号。默认情况下，它被设置为 443。使用以下命令更改端口。
>
> **set ns param -secureicaPorts**<port>
>
> 示例：
>
> set ns param -secureicaPorts 8443

将 Citrix Gateway 与 Citrix Virtual Apps and Desktops 集成

April 6, 2020

部署和配置 StoreFront 服务器以管理对已发布资源和数据的访问。为了进行远程访问，建议在 StoreFront 前面添加 Citrix Gateway。

> 注意：
> 有关如何将 Citrix Virtual Apps and Desktops 与 Citrix Gateway 集成的详细配置步骤，请参阅StoreFront 文档。

下图说明了包含 Citrix Gateway 的简化 Citrix 部署示例。Citrix Gateway 与 StoreFront 通信来保护 Citrix Virtual Apps and Desktops 提供的应用程序和数据。用户设备运行 Citrix Workspace 应用程序来创建安全连接以及访问其应用程序、桌面和文件。

本机 **OTP** 支持身份验证

November 7, 2022

Citrix Gateway 支持一次性密码 (OTP)，而无需使用第三方服务器。一次性密码是一种高度安全的选项，用于对服务器进行身份验证，因为生成的号码或密码是随机的。以前，OTP 由专业公司提供，例如 RSA 提供具有生成随机数的特定设备的 RSA。此系统必须与客户端保持持续通信，才能生成服务器预期的数字。

除了降低资本和运营开支外，此功能还通过将整个配置保留在 Citrix ADC 设备上，增强了管理员的控制能力。

> 注意
>
> 由于不再需要第三方服务器，Citrix ADC 管理员必须配置接口来管理和验证用户设备。

必须向 Citrix Gateway 虚拟服务器注册用户才能使用 OTP 解决方案。每个唯一设备只需要注册一次，并且可以限制在某些环境中。配置和验证注册用户类似于配置额外的身份验证策略。

拥有本地 **OTP** 支持的优势

- 除 Active Directory 之外，无需在身份验证服务器上拥有额外的基础结构，从而降低运营成本。
- 仅将配置整合到 Citrix ADC 设备，从而为管理员提供极好的控制权。
- 消除了客户端依赖额外的身份验证服务器来生成客户端预期的数字。

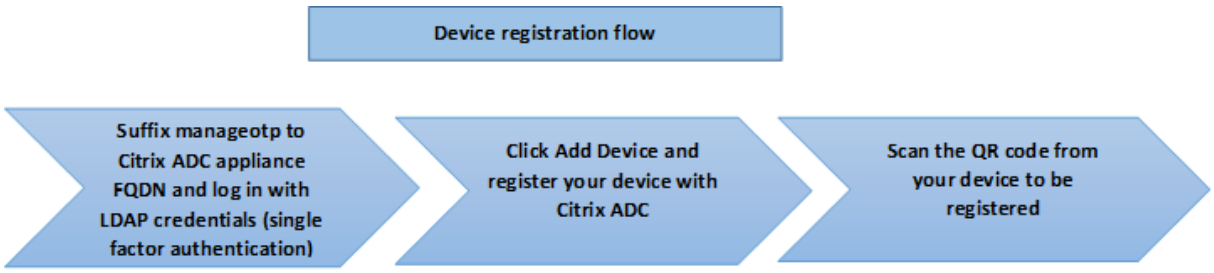
本地 **OTP** 工作流程

本机 OTP 解决方案是一个双重过程，工作流程分类如下：

- 设备注册
- 最终用户登录

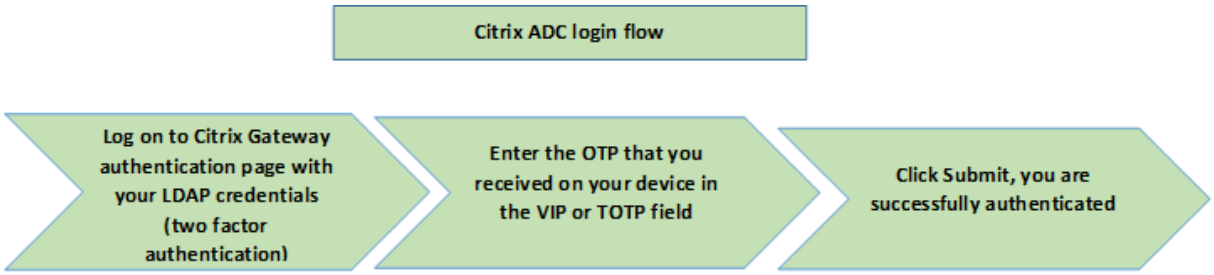
> 重要
>
> 如果您正在使用第三方解决方案或管理 Citrix ADC 设备以外的其他设备，则可以跳过注册过程。添加的最后一个字符串必须采用 Citrix ADC 指定的格式。

下图描述了注册新设备以接收 OTP 的设备注册流程。



> 注意
>
> 设备注册可以使用任意数量的因素来完成。单一因素（如上图所述）用作解释设备注册过程的示例。

下图描述了通过注册设备验证 OTP 的情况。



必备条件

要使用本机 OTP 功能，请确保满足以下必备条件。

- Citrix ADC 功能的发行版为 12.0 Build 51.24 及更高版本。
- Citrix Gateway 上安装了高级版或高级版许可证。
- Citrix Gateway 配置了管理 IP，并且可以使用浏览器和命令行访问管理控制台。
- Citrix ADC 配置了身份验证、授权和审核虚拟服务器，以对用户进行身份验证。
- Citrix ADC 设备配置了 Unified Gateway，并将身份验证、授权和审核配置文件分配给网关虚拟服务器。
- 本机 OTP 解决方案仅限于 nFactor 身份验证流。配置解决方案需要高级策略。有关更多详细信息，请参阅文章 CTX222713。

还要确保 Active Directory 的以下内容：

- 最小属性长度为 256 个字符。
- 属性类型必须是 “DirectoryString”，如 UserParameters。这些属性可以包含字符串值。
- 如果设备名称为非英文字符，则属性字符串类型必须为 Unicode。
- Citrix ADC LDAP 管理员必须具有对所选 AD 属性的写入权限。
- Citrix ADC 设备和客户端计算机必须同步到公共网络时间服务器。

使用 **GUI** 配置本机 **OTP**

本机 OTP 注册不仅仅是单一因素身份验证。以下部分帮助您配置单因素和第二因素身份验证。

为第一因素创建登录架构

1. 导航到安全 **AAA >** 应用程序流量 **>** 登录架构。
2. 转到配置文件，然后单击添加。
3. 在创建身份验证登录架构页上，在名称字段下输入 *lschema_first_factor*，然后单击 **noschema** 旁边的编辑。
4. 单击 **LoginSchema** 文件夹。
5. 向下滚动以选择 **SingleAuth.xml**，然后单击选择。
6. 单击创建。
7. 单击策略，然后单击添加。
8. 在“创建身份验证登录架构策略”屏幕上，输入以下值。

   名称： lschema_first_factor
   配置文件：从列表中选择 schema_first_factor。
   规则： HTTP.REQ.COOKIE.VALUE(“NSC_TASS”).EQ(“manageotp”)

配置身份验证、授权和审核虚拟服务器

1. 导航到安全 **> AAA-**应用程序流量 **>** 身份验证虚拟服务器。单击以编辑现有虚拟服务器。
2. 单击右侧窗格的“高级设置”下登录架构旁边的 **+** 图标。
3. 选择无登录架构。
4. 单击箭头并选择 **lschema_** 第一因子策略。
5. 选择“优先因子**”** 策略，然后单击“选择”。
6. 点击 绑定。
7. 向上滚动并在 高级身份验证策略下选择 **1** 个身份验证策略。
8. 右键单击 **nFactor** 策略，然后选择编辑绑定。
9. 单击“选择下一个因子**”** 下的 **“+”** 图标，创建下一个因子，然后单击“绑定”。
10. 在“创建身份验证策略标签”屏幕上，输入以下内容，然后单击“继续”：

    名称：OTP 管理因素

    登录架构：Lschema_Int

11. 在身份验证策略标签屏幕上，单击 **+** 图标以创建策略。
12. 在“创建身份验证策略”屏幕上，输入以下内容：

    名称。otp_manage_ldap

13. 使用“操作类型”列表选择操作类型。

14. 在操作字段中，单击 **+** 图标以创建操作。
15. 在“创建身份验证 **LDAP** 服务器”页面中，选择“服务器 **IP**”单选按钮，取消选中“身份验证”旁边的复选框，输入以下值，然后选择“测试连接”。

    名称：LDAP_no_auth

    IP 地址：192.168.10.11

    基础 **DN**：DC=training, DC=lab

    管理员：Administrator@training.lab

    密码：xxxxx
16. 向下滚动到其他设置部分。使用下拉菜单选择以下选项。

    服务器登录名称属性为新建并键入 **userprincipalname**。
17. 使用下拉菜单选择 **SSO** 名称属性为新建并键入 **userprincipalname**。
18. 在 **OTP** 密码字段中输入“UserParameters”，然后单击更多。
19. 输入以下属性。

    属性 **1** = mail
    属性 **2** = objectGUID
    属性 **3** = immutableID
20. 单击确定。
21. 在“创建身份验证策略”页上，将表达式设置为 **true** ，然后单击“创建”。
22. 在“创建身份验证策略标签”页上，单击“绑定”，然后单击“完成**”**。
23. 在策略绑定页面上，单击绑定。
24. 在“身份验证策略”页上，单击“关闭”，然后单击“完成”。

> 注意
>
> 身份验证虚拟服务器必须绑定到 RFWebUI 门户主题。将服务器证书绑定到服务器。服务器 IP ‘1.2.3.5’ 必须具有相应的 FQDN，即 Otpauth.server.com，供以后使用。

为第二因素 **OTP** 创建登录架构

1. 导航到“安全**”>“AAA-**应用程序流量**”>“**虚拟服务器”。选择要编辑的虚拟服务器。
2. 向下滚动并选择 **1** 个登录架构。
3. 单击添加绑定。
4. 在策略绑定部分下，单击 **+** 图标以添加策略。
5. 在“创建身份验证登录架构策略”页上，输入名称为 OTP，然后单击 **+** 图标创建配置文件。

6. 在“创建身份验证登录架构”页上，输入名称为 OTP，然后单击 noschema 旁边的图标。
7. 单击 **LoginSchema** 文件夹，选择 **DualAuth.xml**，然后单击选择。
8. 单击创建。
9. 在“规则”部分中，输入“**True**”。单击创建。
10. 单击 **Bind**（绑定）。
11. 注意身份验证的两个因素。单击关闭并单击完成。

配置用于管理 **OTP** 的内容交换策略

如果您使用的是 Unified Gateway，则需要以下配置。

1. 导航到 流量管理 **>** 内容切换 **>** 策略。选择内容切换策略，右键单击，然后选择“编辑”。
2. 编辑表达式以评估以下或语句，然后单击“确定”：

is_vpn_url	HTTP.REQ.URL.CONTAINS(“manageotp”)

使用 **CLI** 配置本机 **OTP**

您必须具有以下信息才能配置 OTP 设备管理页面：

- 分配给身份验证虚拟服务器的 IP
- 与分配的 IP 对应的 FQDN
- 身份验证虚拟服务器的服务器证书

> 注意
>
> 本机 OTP 仅是基于 Web 的解决方案。

配置 **OTP** 设备注册和管理页面

创建身份验证虚拟服务器

```
1 > add authentication vserver authvs SSL 1.2.3.5 443
2 > bind authentication vserver authvs -portaltheme RFWebUI
3 > bind ssl vserver authvs -certkeyname otpauthcert
```

> 注意
>
> 身份验证虚拟服务器必须绑定到 RFWebUI 门户主题。必须将服务器证书绑定到服务器。服务器 IP ‘1.2.3.5’ 必须具有相应的 FQDN，即 Otpauth.server.com，供以后使用。

创建 **LDAP** 登录操作

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP
> - serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
ldapBindDnPassword <PASSWO> -ldapLoginName <USER FORMAT>
```

示例：

```
1 add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4 -
    serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
    administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
    ldapLoginName userprincipalname
```

添加 **LDAP** 登录的身份验证策略

```
1 add authentication Policy auth_pol_ldap_logon -rule true -action
    ldap_logon_action
```

通过 **LoginSchema** 显示 **UI**

在登录时向用户显示用户名字段和密码字段

```
1 add authentication loginSchema lschema_single_auth_manage_otp -
    authenticationSchema "/nsconfig/loginschema/LoginSchema/
    SingleAuthManageOTP.xml"
```

显示设备注册和管理页面

Citrix 推荐两种显示设备注册和管理屏幕的方法：URL 或主机名。

- 使用网址

  当 URL 包含 “/manageotp”

  - add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_url -rule "http.req.cookie.value("NSC_TASS").contains("manageotp")"-action lschema_single_auth_manage_otp
  - bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_url -priority 10 -gotoPriorityExpression END

- 使用主机名

  当主机名为 “alt.server.com” 时。


```
- add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_host
   -rule "http.req.header("host").eq("alt.server.com")"-action
  lschema_single_auth_manage_otp
- bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_hos
   -priority 20 -gotoPriorityExpression END
```

使用 **CLI** 配置用户登录页面

您必须具有以下信息才能配置“用户登录”页：

- 负载平衡虚拟服务器的 IP
- 负载平衡虚拟服务器的相应 FQDN
- 负载平衡虚拟服务器的服务器证书

> 注意
>
> 重用现有身份验证虚拟服务器 (authvs) 进行双重身份验证。

创建负载平衡虚拟服务器

```
1 > add lb vserver lbvs_https SSL 1.2.3.162 443 -persistenceType NONE -
     cltTimeout 180 -  AuthenticationHost otpauth.server.com -
     Authentication ON -authnVsName authvs
2 > bind ssl vserver lbvs_https -certkeyname lbvs_server_cert
```

负载平衡中的后端服务表示如下：

```
1 > add service iis_backendsso_server_com 1.2.3.210 HTTP 80
2 > bind lb vserver lbvs_https iis_backendsso_server_com
```

创建 **OTP** 密码验证操作

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP> -
serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -ldapBindDnPassword
 <PASSWORD> -ldapLoginName <USER FORMAT> -authentication DISABLED -OTPSecret
 <LDAP ATTRIBUTE>
```

示例：

```
1 add authentication ldapAction ldap_otp_action -serverIP 1.2.3.4 -
     serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
     administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
     ldapLoginName userprincipalname -authentication DISABLED -OTPSecret
     userParameters
```


> 重要
>
> LDAP 登录和 OTP 操作之间的区别在于需要禁用身份验证并引入一个新的参数 “OTPSecret”。不得使用 AD 属性值。

添加 **OTP** 密码验证的身份验证策略

```
> add authentication Policy auth_pol_otp_validation -rule true -action
    ldap_otp_action
```

通过 **LoginSchema** 呈现双重身份验证

添加用于双重身份验证的 UI。

```
> add authentication loginSchema lscheme_dual_factor -
    authenticationSchema "/nsconfig/loginschema/LoginSchema/DualAuth.xml
    "

> add authentication loginSchemaPolicy lpol_dual_factor -rule true -
    action lscheme_dual_factor
```

通过策略标签创建密码验证系数

为下一个因素创建管理 OTP 流策略标签（第一个因素是 LDAP 登录）

```
> add authentication loginSchema lschema_noschema -authenticationSchema
     noschema

> add authentication policylabel manage_otp_flow_label -loginSchema
    lschema_noschema`
```

将 **OTP** 策略绑定到策略标签

```
bind authentication policylabel manage_otp_flow_label -policyName
    auth_pol_otp_validation -priority 10 -gotoPriorityExpression NEXT
```

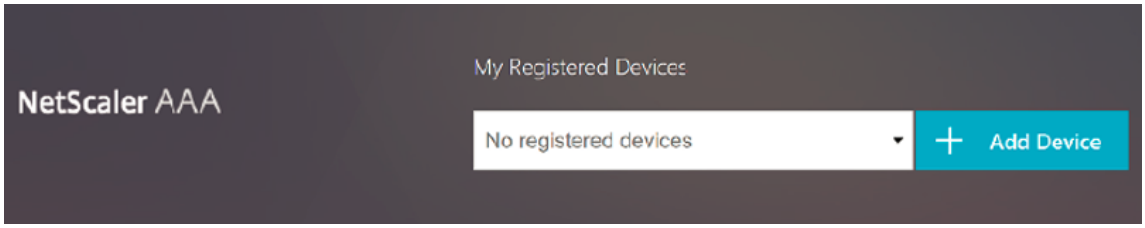
绑定 **UI** 流

绑定 LDAP 登录，然后使用身份验证虚拟服务器进行 OTP 验证。

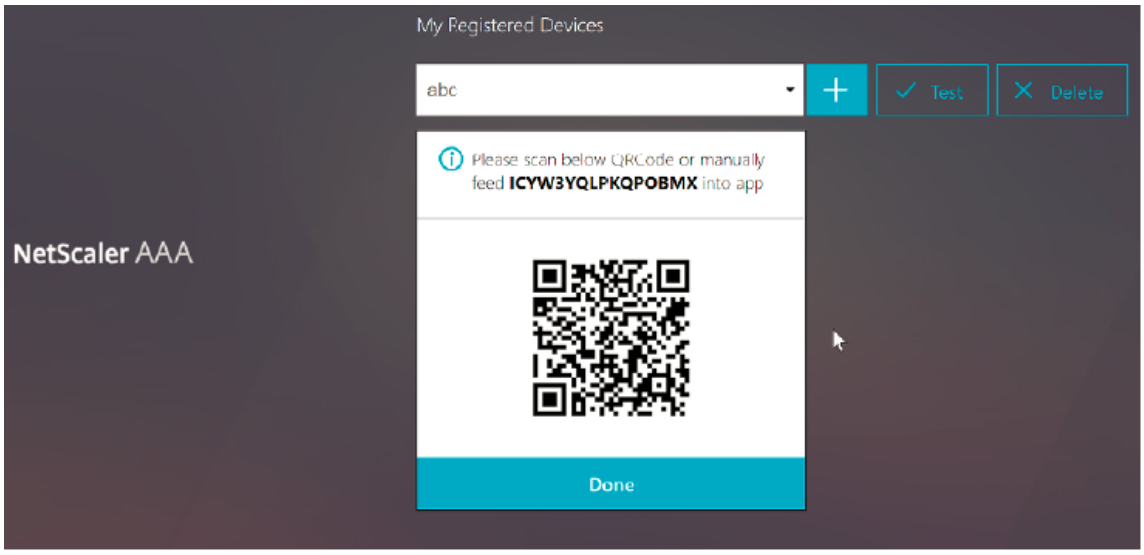

```
> bind authentication vserver authvs -policy auth_pol_ldap_logon -
    priority 10 -nextFactor  manage_otp_flow_label -
    gotoPriorityExpression NEXT

> bind authentication vserver authvs -policy lpol_dual_factor -priority
     30 -gotoPriorityExpression END
```

将您的设备注册到 **Citrix ADC**

1. 导航到您的 Citrix ADC FQDN（第一个面向公众的 IP），并带有 /管理 otp 后缀。例如，使用用户凭据登录 https://otpauth.server.com/manageotp。
2. 单击 **+** 图标以添加设备。

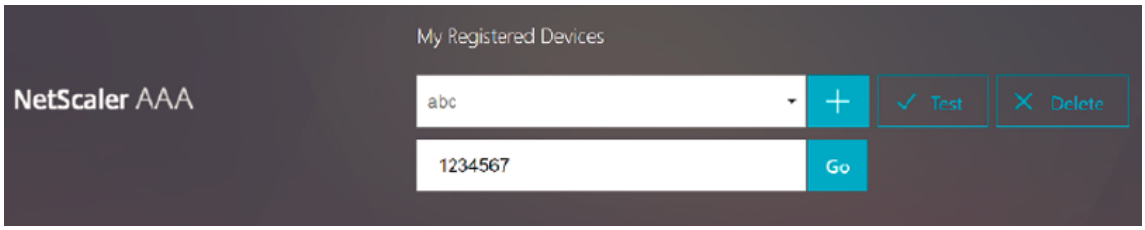


3. 输入设备名称，然后按转到。屏幕上显示条形码。
4. 单击开始设置，然后单击扫描条形码。
5. 将设备相机悬停在 QR 码上。您可以选择输入 16 位代码。



> 注意
>
> 显示的 QR 码有效期为 3 分钟。

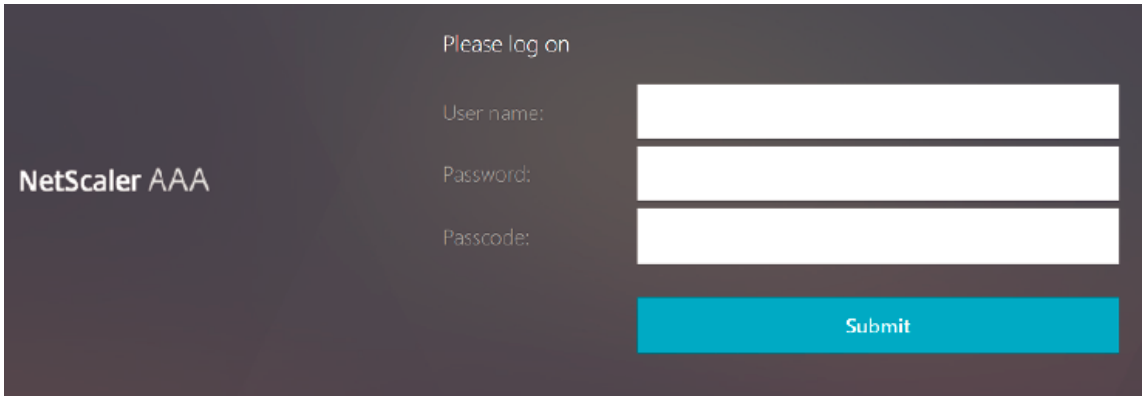
6. 扫描成功后，您会看到一个可用于登录的 6 位数时间敏感的代码。



7. 要进行测试，请单击 QR 屏幕上的“完成”，然后单击右侧的绿色复选标记。
8. 从下拉菜单中选择您的设备，然后输入 Google Authenticator 中的代码（必须为蓝色，不是红色），然后单击转到。
9. 请确保使用页面右上角的下拉菜单注销。

使用 **OTP** 登录到 **Citrix ADC**

1. 导航到您的第一个面向公众的 URL，然后从 Google Authenticator 输入您的 OTP 进行登录。
2. 对 Citrix ADC 启动页面进行身份验证。



OTP 的推送通知

April 6, 2020

Citrix Gateway 支持 OTP 的推送通知。用户无需手动输入其注册设备上收到的 OTP 即可登录 Citrix Gateway。管理员可以配置 Citrix Gateway，以便使用推送通知服务将登录通知发送到用户注册的设备。当用户收到通知时，他们只需单击通知上的允许以登录 Citrix Gateway。当网关收到来自用户的确认时，它会识别请求的来源，并向该浏览器连接发送响应。

如果在超时期限（30 秒）内未收到通知响应，则用户将被重定向到 Citrix Gateway 登录页面。然后，用户可以手动输入 OTP，或单击重新发送通知，在注册的设备上再次接收通知。

管理员可以使用为推送通知创建的 LoginSchema，将推送通知身份验证作为默认身份验证。

> 重要：推送通知功能可用于 Citrix ADC 高级版许可证。

推送通知的优势

- 推送通知提供了更安全的多重身份验证机制。在用户批准登录尝试之前，对 Citrix Gateway 的身份验证不会成功。
- 推送通知易于管理和使用。用户必须下载并安装不需要任何管理员协助的 Citrix SSO 移动应用程序。
- 用户无需复制或记住代码。他们必须简单地单击设备才能获得身份验证。
- 用户可以注册多个设备。

推送通知的工作原理

推送通知工作流程可分为两类：

- 设备注册
- 最终用户登录

使用推送通知的必备条件

- 完成 Citrix Cloud 登录过程。
  1. 创建 Citrix Cloud 公司帐户或加入现有帐户。有关详细过程和如何继续的说明，请参阅 “注册加入 Citrix Cloud”。
  2. 登录 https://citrix.cloud.com，然后选择客户。
  3. 从菜单中，选择 “身份和访问管理”，然后导航到 “API 访问” 选项卡，为客户创建客户端。
  4. 复制 ID、密码和客户 ID。将 Citrix ADC 中的推送服务分别配置为 “ClientID” 和 “ClientSecret” 时，需要 ID 和密钥。

> 重要：
>
> - 相同的 API 凭据可用于多个数据中心。
> - 本地 Citrix ADC 设备必须能够解析服务器地址 mfa.cloud.com 和 trust.citrixworkspacesapi.net，并且可以从设备访问。这是为了确保这些服务器通过端口 443 没有防火墙或 IP 地址块。

- 分别从适用于 iOS 设备和 Android 设备的 App Store 和 Play 应用商店下载 Citrix SSO 移动应用程序。Push notification is supported on iOS from build 1.1.13 on Android from 2.3.5.
- 确保 Active Directory 的以下内容。
  - 最小属性长度必须至少为 256 个字符。
  - 属性类型必须是 “DirectoryString”，如 UserParameters。这些属性可以包含字符串值。
  - 如果设备名称为非英文字符，则属性字符串类型必须为 Unicode。
  - Citrix ADC LDAP 管理员必须具有对所选 AD 属性的写入权限。
  - Citrix ADC 和客户端计算机必须同步到通用的网络时间服务器。

推送通知配置

下面是使用推送通知功能必须完成的高级步骤。

- Citrix Gateway 管理员必须配置界面以管理和验证用户。
  1. 配置推送服务。
  2. 为 OTP 管理和最终用户登录配置 Citrix Gateway。

     用户必须将其设备注册到网关才能登录到 Citrix Gateway。
  3. 使用 Citrix Gateway 注册您的设备。
  4. 登录到 Citrix Gateway。

创建推送服务

1. 导航到 “安全”>“**AAA-**应用程序流量”>“策略”>“身份验证”>“高级策略”>“操作”>“推送服务”，然后单击 “添加”。
2. 在 “名称” 中，输入推送服务的名称。
3. 在客户端 **ID** 中，输入用于与云中 Citrix Push 服务器通信的信赖方的唯一标识。
4. 在 “客户端密钥” 中，输入与云中 Citrix Push 服务器通信的信赖方的唯一密钥。
5. 在客户 **ID** 中，输入用于创建客户 ID 和客户密钥对的云中帐户的客户 ID 或名称。

为 **OTP** 管理和最终用户登录配置 **Citrix Gateway**

完成 OTP 管理和最终用户登录的以下步骤。

- 创建 OTP 管理的登录架构
- 配置身份验证、授权和审核虚拟服务器
- 配置 VPN 或负载平衡虚拟服务器
- 配置策略标签
- 为最终用户登录创建登录架构

有关配置的详细信息，请参阅本地 OTP 支持。

重要：对于推送通知，管理员必须明确配置以下内容：

- 创建推送服务。
- 为 OTP 管理创建登录架构时，请根据需要选择单个 SingleAuthManageOTP.xml 登录架构或等效。
- 在为最终用户登录创建登录模式时，请根据需要选择 DualAuthOrPush.xml 登录模式或等效模式。

将您的设备注册到 **Citrix Gateway**

用户必须将其设备注册到 Citrix Gateway 才能使用推送通知功能。

1. 在 Web 浏览器中，浏览到 Citrix Gateway FQDN，并将后缀 **/manageotp** 附加到 FQDN。

   这将加载身份验证页面。
   示例：https://gateway.company.com/manageotp

2. 根据需要，使用 LDAP 凭据或适当的双重身份验证机制登录。
3. 单击添加设备。
4. 输入设备的名称，然后单击“转到”。

   QR 码将显示在 Citrix Gateway 浏览器页面上。

5. 使用 Citrix SSO 应用程序从要注册的设备扫描此二维码。

   Citrix SSO 验证 QR 码，然后向网关注册推送通知。如果注册过程中没有错误，则该令牌将成功添加到密码令牌页面。

6. 如果没有其他设备可以添加/管理注销，请使用页面右上角的列表。

测试一次性密码身份验证

1. 要测试 OTP，请从列表中单击您的设备，然后单击 测试。
2. 输入您在设备上收到的 OTP，然后单击“转到”。

   将显示 OTP 验证成功消息。

3. 使用页面右上角的列表注销。

注意：您可以随时使用 OTP 管理门户测试身份验证、删除已注册的设备或注册更多设备。

登录到 **Citrix Gateway**

将其设备注册到 Citrix Gateway 后，用户可以使用推送通知功能进行身份验证。

1. 导航到 Citrix Gateway 身份验证页面（例如：https://gateway.company.com)

   系统会提示您仅输入 LDAP 凭据，具体取决于 LoginSchema 配置。

2. 输入您的 LDAP 用户名和密码，然后选择“提交”。

   将向您注册的设备发送通知。

   注意：如果要手动输入 OTP，则必须选择单击手动输入 OTP，然后在 **TOTP** 字段中输入 OTP。

3. 打开已注册设备上的 Citrix SSO 应用，然后单击允许。

注意：

- 身份验证服务器等待推送服务器通知响应，直到配置的超时期限过期。超时后，Citrix Gateway 将显示登录页面。然后，用户可以手动输入 OTP，或单击重新发送通知，在注册的设备上再次接收通知。根据您选择的选项，网关将验证您已输入的 OTP，或在注册的设备上重新发送通知。
- 不会向您注册的设备发送有关登录失败的通知。

失效条件

- 在以下情况下，设备注册可能会失败。
  - 服务器证书可能不受最终用户设备的信任。
  - 用于注册 OTP 的 Citrix Gateway 无法由客户端访问。
- 在以下情况下，通知可能会失败。
  - 用户设备未连接到 Internet
  - 用户设备上的通知被阻止
  - 用户不批准设备上的通知

在这些情况下，身份验证服务器将等待，直到配置的超时期限过期。超时后，Citrix Gateway 会显示一个登录页面，其中包含手动输入 OTP 或在注册设备上重新发送通知的选项。根据所选选项，进一步验证。

iOS 上的 **Citrix SSO** 应用程序行为 **-** 要注意的事项

通知快捷方式

Citrix SSO iOS 应用程序包括对可操作通知的支持，以增强用户体验。在 iOS 设备上收到通知后，如果设备已锁定或 Citrix SSO 应用程序未位于前台，则用户可以使用通知中内置的快捷方式批准或拒绝登录请求。

要访问通知快捷方式，用户需要强制触摸（3D 触摸）或长按通知，具体取决于设备的硬件。选择“允许快捷方式”操作将向 Citrix ADC 发送登录请求。根据身份验证、授权和审核虚拟服务器上配置身份验证策略的方式；

- 登录请求可能会在后台发送，而无需将应用程序启动到前台或解锁设备。
- 应用程序可能会提示输入触摸 ID/面部 ID/密码作为额外的因素，在这种情况下，应用程序将启动到前台。

从 **Citrix SSO** 中删除密码令牌

1. 要删除 Citrix SSO 应用程序中注册用于推送的密码令牌，用户必须执行以下步骤：
2. 取消注册（删除）网关上的 iOS/Android 设备。显示用于从设备中删除注册的 QR 码。
3. 打开 Citrix SSO 应用程序，然后单击要删除的密码令牌的信息按钮。
4. 单击删除令牌并扫描二维码。

注意：

- 如果 QR 码有效，则该令牌将从 Citrix SSO 应用程序中成功删除。
- 如果设备已从网关中删除，用户可以单击“强制删除”即可删除密码令牌，而无需扫描二维码。如果设备尚未从 Citrix Gateway 中删除，则强制删除可能会导致设备继续接收通知。

配置服务器名称指示扩展名

April 6, 2020

现在可以将 Citrix Gateway 设备配置为在发送到后端服务器的 SSL“客户端 hello” 数据包中包含服务器名称指示 (SNI) 扩展。SNI 扩展可帮助后端服务器识别 SSL 握手期间请求的 FQDN，并使用相应的证书进行响应。

> 注意
>
> 当多个 SSL 域托管在同一服务器上时，启用 SNI 支持。

若要使用 **GUI** 将 **Citrix Gateway** 配置为支持 **SNI**，请执行以下操作：

1. 在 NetScaler GUI 中，导航到配置 **> Citrix NetScaler >** 全局设置。
2. 单击 更改全局设置链接，然后从 后端服务器 **SNI** 下拉菜单中选择 已启用。

要使用命令行界面配置 **Citrix Gateway** 以支持 **SNI**，请在命令提示符处键入：

```
1 set vpn parameter backendServerSni <ENABLED><DISABLED>
```

在 **SSL** 握手期间验证服务器证书

April 6, 2020

现在可以将 Citrix Gateway 设备配置为验证 SSL 握手期间后端服务器提供的服务器证书。

使用配置实用程序配置 Citrix Gateway 全局参数以支持出站代理的 PAC

绑定 CA 证书

1. 导航到配置 > **Citrix Gateway** > **Citrix Gateway** 策略管理器 > 证书绑定。**
2. 在 证书绑定屏幕上，单击 **+** 图标。
3. 在 “**CA** 证书绑定**”** 屏幕上，单击 **“**添加绑定”，然后单击 “安装”。
4. 在 “证书文件名” 字段中选择 证书文件名，然后单击 “安装”。
5. 在 “**CA** 证书绑定” 屏幕上，选择证书，然后单击 “绑定”。
6. 单击完成。

启用证书验证：

1. 导航到 **Citrix Gateway >** 全局设置。
2. 点击 更改全局设置。**
3. 从 后端服务器证书验证下拉菜单中选择 已启用，然后单 击确定。

使用命令行配置 Citrix Gateway 全局参数以支持服务器证书

在命令提示符下，键入以下命令：


```
    bind vpn global cacert DNPGCA1

    set vpn parameter backendcertValidation ENABLED
<!--NeedCopy-->
```

使用高级策略创建 **VPN** 策略

April 6, 2020

经典策略引擎 (PE) 和高级策略基础结构 (PI) 是 Citrix ADC 当前支持的两种不同的策略配置和评估框架。

高级策略基础结构由非常强大的表达式语言组成。表达式语言可用于定义策略中的规则、定义操作的各个部分以及支持的其他实体。表达式语言可以分析请求或响应的任何部分，还可以让您深入查看标头和有效负载。相同的表达式语言在 Citrix ADC 支持的每个逻辑模块中扩展和工作。

> 注意：建议
> 您使用高级策略创建策略。

为什么从传统策略迁移到高级策略**?**

高级策略具有丰富的表达式集，并提供比传统策略更大的灵活性。Citrix ADC 可扩展并满足各种客户端的需求，因此必须支持远远超过高级策略的表达式。有关详细信息，请参阅策略和表达式。

以下是高级策略的添加功能。

- 能够访问消息的正文。
- 支持许多附加协议。
- 访问系统的许多附加功能。
- 具有更多的基本函数、运算符和数据类型。
- 满足 HTML，JSON 和 XML 文件的解析。
- 促进快速并行多字符串匹配（Patsets 等）。

现在，可以使用高级策略配置以下 VPN 策略。

- 会话策略
- 授权策略
- 流量策略
- 隧道策略
- 审计政策

此外，端点分析 (EPA) 可配置为验证功能的 nFactor。EPA 用作试图连接网关设备的端点设备的门卫。在终端设备上显示网关登录页之前，根据网关管理员配置的资格条件，检查设备是否有最低硬件和软件要求。根据执行的检查结果授

予对网关的访问权限。以前，EPA 被配置为会话策略的一部分。现在可以将其链接到 nFactor，提供更大的灵活性，以及可以执行的时间。有关 EPA 的更多信息，请参阅终端节点策略的工作原理主题。有关 nFactor 的更多信息，请参阅nFactor 身份验证主题。

使用案例：

使用高级 **EPA** 预身份验证 **EPA**

预身份验证 EPA 扫描会在用户提供登录凭据之前进行。有关使用预身份验证 EPA 扫描为身份验证因素之一配置 Citrix Gateway 以进行 nFactor 身份验证的信息，请参阅CTX224268主题。

使用高级 **EPA** 的身份验证后 **EPA**

验证后 EPA 扫描会在验证用户凭据后进行。在传统策略基础结构下，身份验证后 EPA 被配置为会话策略或会话操作的一部分。在高级策略基础设施下，EPA 扫描将被配置为 n 因素身份验证中的 EPA 因子。有关使用身份验证后 EPA 扫描为身份验证因素之一配置 Citrix Gateway 以进行 n 因素身份验证的信息，请参阅CTX224303主题。

使用高级策略进行身份验证前和身份验证后 **EPA**

EPA 可以在身份验证前和身份验证后执行。有关使用身份验证前和身份验证后 EPA 扫描配置 Citrix Gateway 以进行 nFactor 身份验证的信息，请参阅CTX231362主题。

定期 **EPA** 扫描作为 **nFactor** 身份验证的一个因素

在传统策略基础结构下，定期 EPA 扫描被配置为会话策略操作的一部分。在高级策略基础设施下，它可以被配置为 n 因素身份验证中 EPA 因子的一部分。

有关将定期 EPA 扫描配置为 nFactor 身份验证中的一个因素的更多信息，请单击CTX231361主题。

故障排除：

故障排除需要记住以下几点。

- 同一类型的经典和高级策略（例如，会话策略）不能绑定到同一实体/绑定点。
- 对于所有 PI 策略，优先级都是强制性的。
- VPN 的高级策略可以绑定到所有绑定点。
- 具有相同优先级的高级策略可以绑定到单个绑定点。
- 如果没有任何配置的授权策略被命中，则应用 VPN 参数中配置的全局授权操作。
- 在授权策略中，如果授权规则失败，则不撤销授权操作。

经典策略的常用高级策略等效表达式：

经典策略表达式	高级政策表达方式
ns_true	true
ns_false	false
REQ.HTTP	HTTP.REQ
RES.HTTP	HTTP.RES
HEADER “foo”	HEADER(“foo”)
CONTAINS ”bar”	.CONTAINS(“bar”) [注意使用 “.”。]
REQ.IP	CLIENT.IP
RES.IP	SERVER.IP
SOURCEIP	SRC
DESTIP	DST
REQ.TCP	CLIENT.TCP
RES.TCP	SERVER.TCP
SOURCEPORT	SRCPORT
DESTPORT	DSTPORT
STATUSCODE	STATUS
REQ.SSL.CLIENT.CERT	CLIENT.SSL.CLIENT_CERT

使用模板简化 **SaaS** 应用配置

April 6, 2020

通过为流行的 SaaS 应用配置模板下拉菜单，简化了在 Citrix Gateway 上使用单点登录的 SaaS 应用配置。可以从菜单中选择要配置的 SaaS 应用程序。模板预填充了配置应用程序所需的大部分信息。但是, 还必须提供客户特定的信息。

注意：以下部分介绍了要在 **Citrix Gateway** 上执行的使用模板配置和发布应用程序的步骤。后续部分将介绍在 **app server** 上执行的配置步骤。

使用模板配置和发布应用程序**-Citrix Gateway** 特定配置

以下配置将 **AWS** 控制台应用程序作为使用模板配置和发布应用程序的示例。

在开始之前，您需要以下内容：

- AWS 控制台的管理员账户

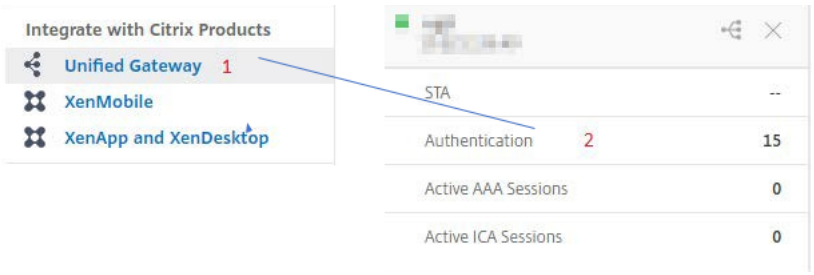
- Citrix Gateway 的管理员帐户

AWS 控制台配置步骤如下所示：

1. 使用应用程序目录配置 AWS 控制台。
2. 从 Citrix ADC 导出 AWS 控制台 IdP 元数据。
3. 在 AWS 控制台中配置 IdP。

步骤 **1**：使用应用程序目录配置 AWS 控制台

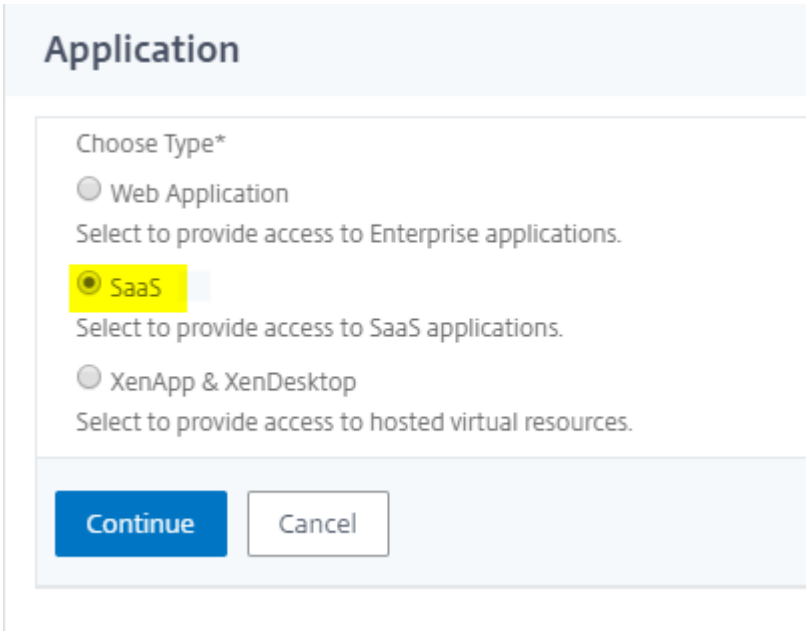
1. 单击 **Unified Gateway >** 身份验证。



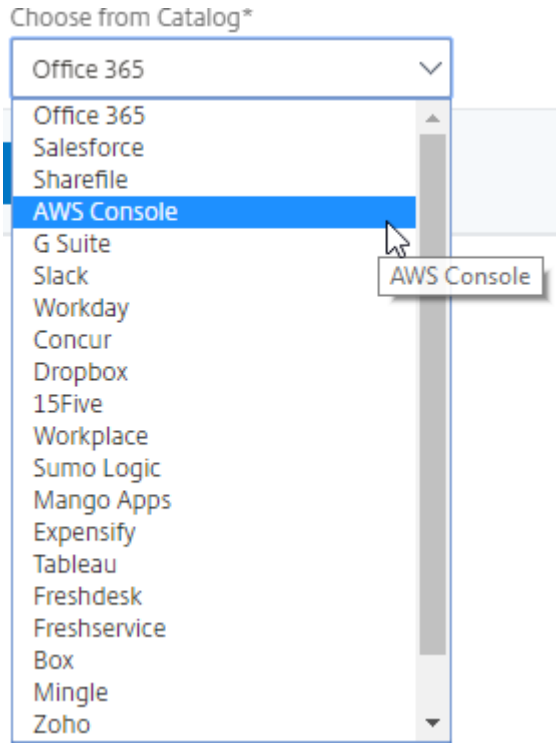
   此时将显示 Unified Gateway 配置屏幕。

2. 在 应用程序部分，点击编辑图标。现在，点击加号图标。此时将显示应用程序窗口。

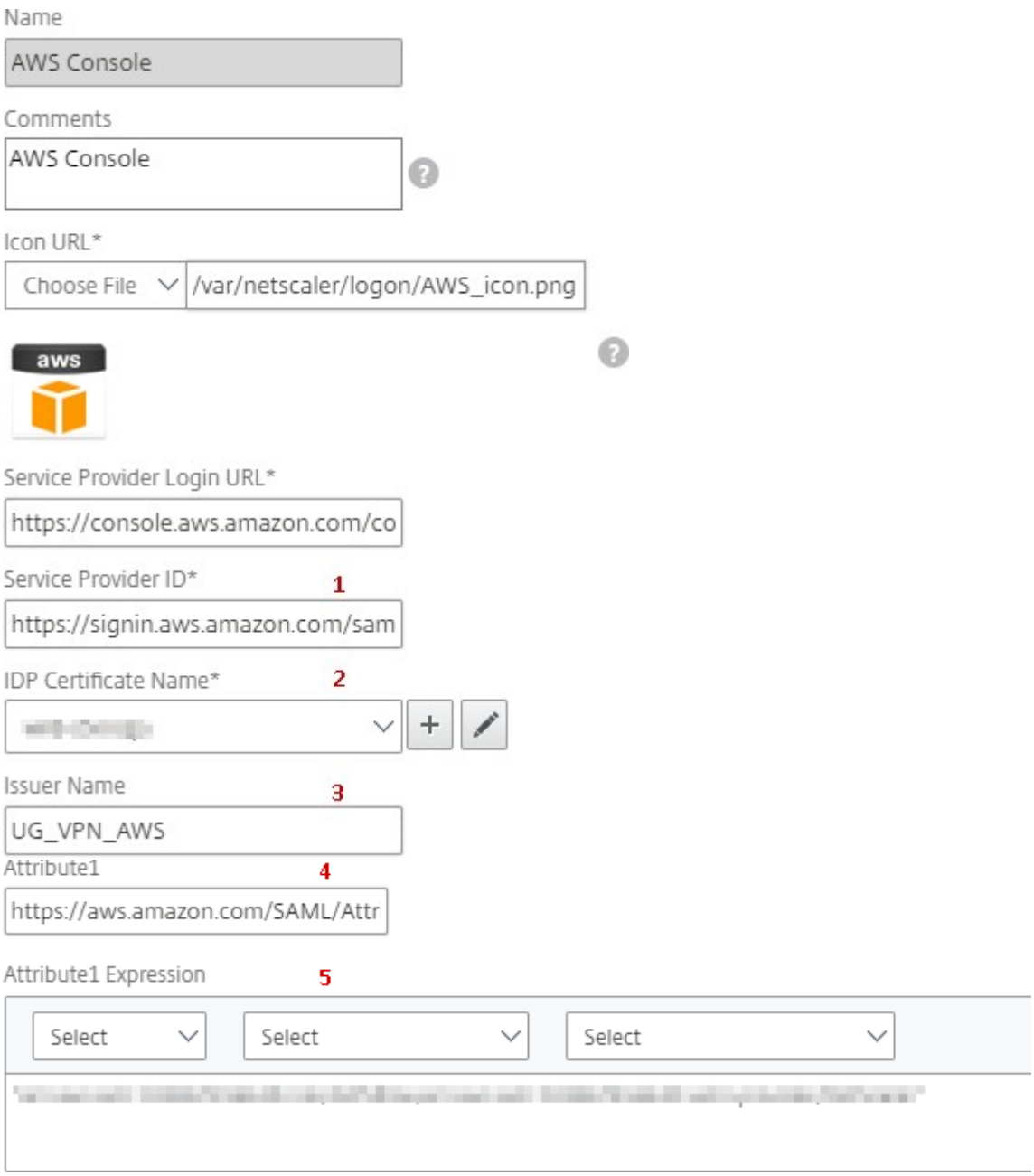
3. 从应用程序类型中选择 **SaaS** 。



4. 从下拉列表中选择 **AWS** 控制台。



5. 使用适当的值填写应用程序模板。



6. 输入以下 SAML 配置详细信息，然后单击 继续。

   服务提供商 **ID** —https://signin.aws.amazon.com/saml

   签名证书名称 — 需要选择 IdP 证书

   发行人名称 — 发行人名称可根据您的选择填写

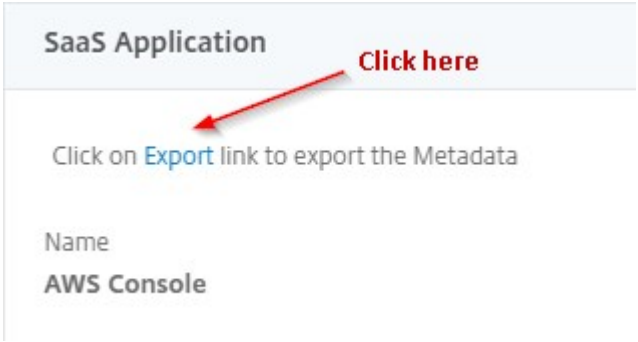
   Attribute1 – `https://aws.amazon.com/SAML/Attributes/Role`

   属性 **1** 表达式 — 角色 ARN、IdP ARN，如步骤 3 所示

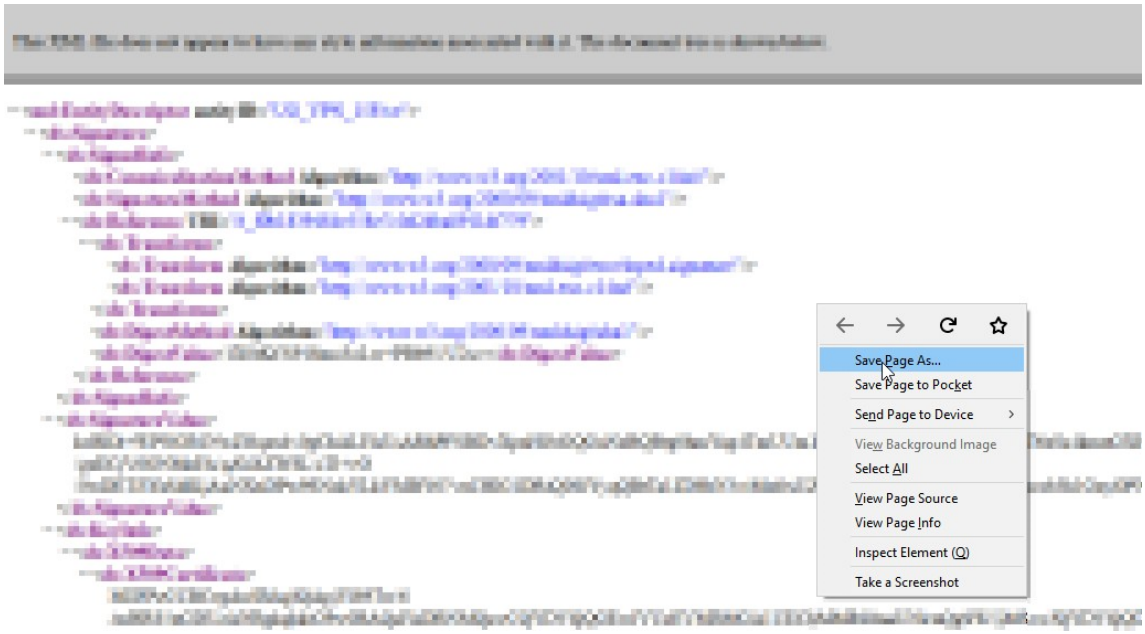
7. 单击完成。

步骤 **2**：从 Citrix Gateway 导出 AWS 控制台 IdP 元数据。

1. 单击 **Unified Gateway >** 身份验证。
2. 向下滚动并单击 **AWS** 控制台模板。此时将显示 SaaS 应用程序窗口。点击 导出链接。



3. 元数据将在不同窗口中打开。保存 **IdP** 元数据文件



步骤 **3**： 将 IdP 配置到 AWS 控制台 。

使用模板**-App server** 特定配置配置和发布应用程序

下面是 pdf 链接, 这些链接针对应用程序服务器特定配置的指导, 以使用模板配置和发布热门 SaaS 应用程序。

- 15Five
- Absorb
- Accompa
- Adobe Captivate Prime

- Adobe 创意云端
- Aha
- Alertops
- Allocadia
- 阿里巴
- Assembla
- AWS 控制台
- BambooHR
- Base CRM
- BitaBIZ
- Bluejeans
- Blissbook
- Bonusly
- Box
- Bugsnag
- Buildkite
- CakeHR
- Cardboard
- 塞德西斯
- Celoxis
- 思科美拉基
- ClearSlide
- CloudCheckr
- ConceptShare
- Concur
- 汇合
- Contactzilla
- Convo
- 克里奥诺斯

- Dashlane
- 数据日志
- 台式电脑
- Deputy
- DigiCert
- Docusign
- 多莫
- Dropbox
- Duo
- 冒犯
- Ekarda
- Envoy
- ERP
- Expensify
- EZOfficeInventory
- EZRentOut
- Favro
- Federated Directory
- Feedly
- Fivetran
- Flatter Files
- 花坞
- Freshdesk
- 前面
- G-Suite
- GitHub
- GlassFrog
- GotoMeeting
- Happyfox

- Helpjuice
- Help Scout
- Hoshinplan
- Humanity
- Igloo
- Illumio
- Image Relay
- iMeet Central
- InteractGo
- iQualify One
- Jira
- Kanban Tool
- Keeper Security
- Kentik
- Kentik
- Kissflow
- KnowBe4
- KnowledgeOwl
- Kudos
- LaunchDarkly
- Lifesize
- Litmos
- LiquidPlanner
- LogDNA
- Mango
- Manuscript
- Marketo
- Mingle
- Mixpanel

- MuleSoft
- MyWebTimesheets
- New Relic
- Nmbrs
- Nuclino
- Office365
- OneDesk
- OpsGenie
- Orginio
- Pagerduty
- Panorama9
- ParkMyCloud
- Peakon
- People HR
- Pingboard
- Pipedrive
- PlanMyLeave
- PlayVox
- Podio
- ProdPad
- Proto.io
- Proxyclick
- PurelyHR
- Quandora
- Rackspace
- RealtimeBoard
- Remedyforce
- Robin
- Rollbar

- Salesforce
- Samanage
- Samepage
- Sentry
- ServiceDesk Plus
- ServiceNow
- Shufflrr
- Skeddly
- Skills Base
- Slack
- Slemma
- Sli.do
- Smartsheet
- Spoke
- Spotinst
- SproutVideo
- StatusCast
- Status Hero
- Statushub
- Statuspage
- Sumologic
- Supermood
- Syncplicity
- Tableau
- Targetprocess
- Teamphoria
- Testable
- TestFairy
- TextExpander

- TextMagic
- ThousandEyes
- Thycotic Secret server
- Tinfoil Security
- Trisotech
- Trumba
- TwentyThree
- Unifi
- UserEcho
- UserVoice
- Velpic
- VictorOps
- Vidizmo
- Visual Paradigm
- Weekdone
- Wepow
- When I Work
- Workday
- Workpath
- Workplace
- Workstars
- Workteam
- XaitPorter
- Ximble
- XMatters
- Yodeck
- Zendesk
- Zivver
- 佐霍一号

- Zivver
- Zoom

nFactor 中的设备证书作为 EPA 组件

January 10, 2023

设备证书可以在 nFactor 中配置为 EPA 组件。设备证书可以作为 EPA 的一部分显示为任何因素。

以下是在 nFactor 中配置设备证书作为 EPA 组件的好处。

- 设备证书验证失败不会导致登录失败。根据配置，登录可以继续，用户可以被放置在具有有限访问权限的组中。
- 由于设备证书检查是策略驱动的，因此您可以根据设备证书身份验证选择性地允许或阻止对企业 Intranet 资源的访问。例如，设备证书身份验证可用于仅在企业托管的笔记本电脑上提供对 Office 365 应用程序的条件访问。

设备证书验证不能作为定期 EPA 扫描的一部分。

> 重要提示：默认情况下，Windows 授权访问设备证书的管理员权限。要为非管理员用户添加设备证书检查，您必须在设备上安装与 EPA 插件版本相同的 VPN 插件。

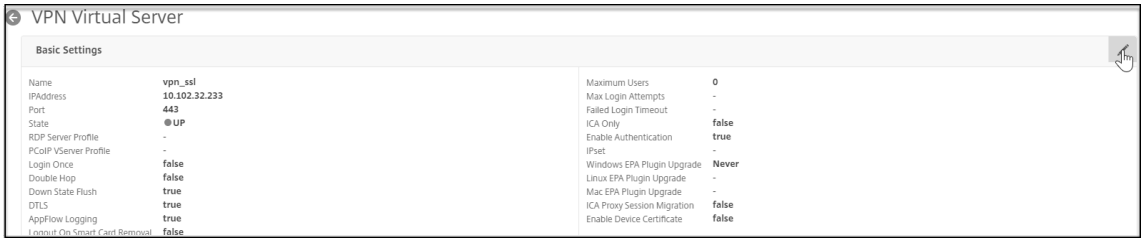
在 nFactor 中配置设备证书作为 EPA 组件

要使用命令行界面将 **nFactor** 中的设备证书配置为 **EPA** 组件，请在命令提示符处键入：

```
1 add authentication epaAction epa-act -csecexpr sys.client_expr("device-
      cert_0_0") -defaultgroup epa_pass -quarantine_group epa_fail
2
3 <!--NeedCopy-->
```

若要使用 **Citrix ADC GUI** 将 **nFactor** 中的设备证书配置为 **VPN** 虚拟服务器的 **EPA** 组件，请执行以下操作：

1. 在 NetScaler GUI 中，导航到配置 **> Citrix Gateway >** 虚拟服务器。
2. 在 **Citrix Gateway** 虚拟服务器页面上，选择要修改的虚拟服务器，然后单击 编辑。
3. 在 **VPN** 虚拟服务器页面上，单击编辑图标。

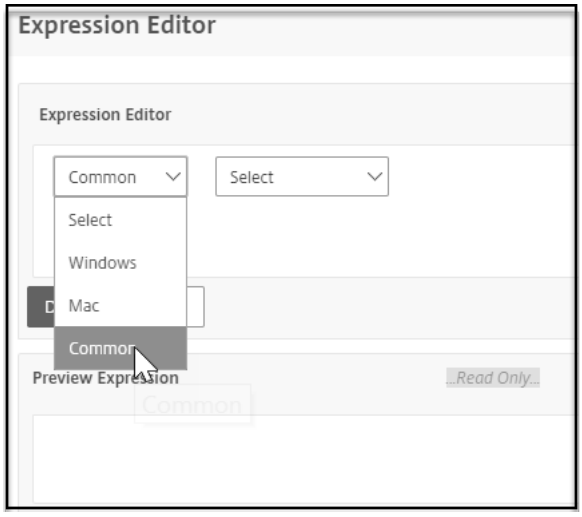


4. 点击 更多。

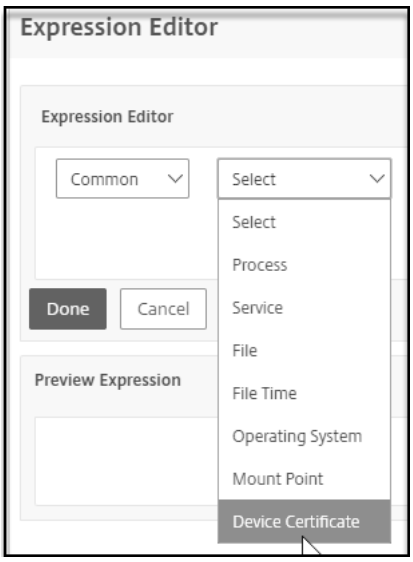
5. 单击“设备证书 CA”部分旁的“添加”，然后单击“确定”。

> 不要选中“启用设备证书”复选框。启用它可以在经典 EPA 中进行设备证书验证。

6. 在 NetScaler GUI 中，导航到配置 **>** 安全 **> AAA-**应用程序流量 **>** 策略 **>** 身份验证 **>** 高级策略 **>** 操作 **> EPA>**
7. 在身份验证 **EPA** 操作页上，单击添加。您可以单击编辑以编辑现有 EPA 操作。
8. 在“创建身份验证 **EPA** 操作”页面上，提供创建身份验证 EPA 操作所需字段的值，然后单击 **EPA** 编辑器链接。
9. 从“表达式编辑器**”** 列表中选择“公 用”。



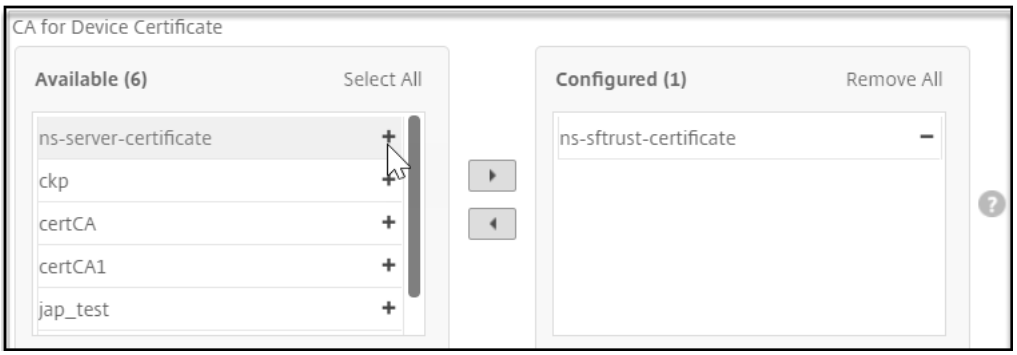
10. 从显示的后续列表中选择“设备证书”，然后单击“完成”以完成配置。



要使用 **Citrix ADC GUI** 将 **nFactor** 中的设备证书配置为 **AAA** 虚拟服务器的 **EPA** 组件，请执行以下操作：

1. 在 Citrix DC GUI 中，导航到 安全 **> AAA** 应用程序流量 **>** 虚拟服务器。
2. 在 **Citrix Gateway** 虚拟服务器页面上，选择要修改的虚拟服务器，然后单击编辑。
3. 在“身份验证虚拟服务器”页上，单击“编辑”图标。
4. 点击 更多。
5. 单击 “**** 设备证书 CA” 部分旁边的 ****“添加”。

6. 选择要添加的证书，然后单 击 **“**确定” 完成配置。



7. 重复上 一节中列出的步骤 **6** 到步骤 **10** 以完成配置。

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States