Citrix Secure Private Access - 旧版

Machine translated content

Disclaimer

Contents

为本地部署配置 **Secure Private Access** 权限 **-** 旧版

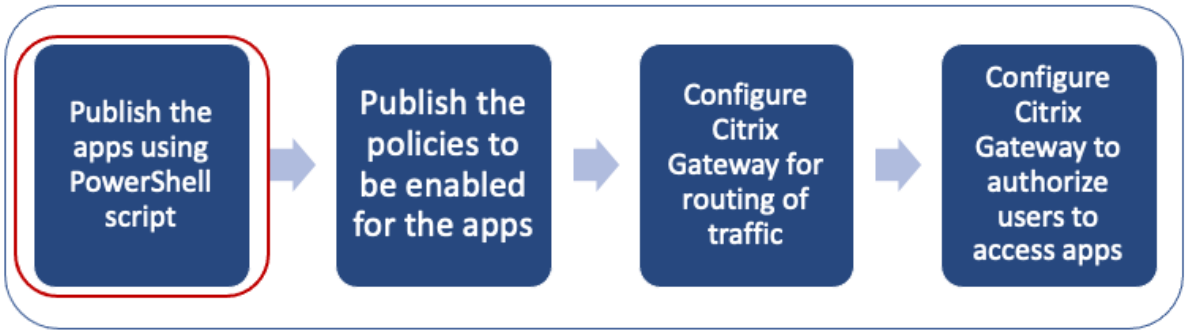
January 9, 2024

本地 Secure Private Access 解决方案配置是一个四步过程。

1. 发布应用程序
2. 发布应用程序的策略
3. 启用通过 NetScaler Gateway 路由流量
4. 配置授权策略

> 重要：
>
> 配置工具可用于快速加载应用程序和应用程序策略，还可以配置 NetScaler Gateway 和 StoreFront 设置。但是，在使用该工具之前，请注意以下几点。
>
> - 阅读发布应用程序和发布应用程序策略部分，确保您完全了解本地解决方案配置的配置要求。
> - 此工具只能用作本主题中记录的现有过程的补充，不能取代必须手动执行的配置。
>
> 有关该工具的完整详细信息，请参阅使用 Secure Private Access 配置工具配置应用程序和策略。

步骤 **1**：发布应用程序



您必须使用 PowerShell 脚本来发布 URL。发布应用程序后，即可使用 Citrix Studio 控制台对其进行管理。

您可以从中下载 PowerShell 脚本 https://www.citrix.com/downloads/workspace-app/powershell-module-for-configuring-secure-private-access-for-storefront/configure-secure-private-access-for-storefront.html。

1. 在包含 PowerShell SDK 的计算机上打开 PowerShell。
2. 请运行以下命令：

```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup  -Name PublishedContentApps
```



```
<!--NeedCopy-->
```

3. 为 Web 应用程序定义变量。

```
$citrixUrl:  “<URL of the app>”
$appName: <app name as it must appear on Workspace>
$DesktopGroupId: 1
$desktopgroupname: <your desktop group name>
$AppIconFilePath:  <path of the image file>
<!--NeedCopy-->
```

> 注意：
>
> 在运行命令之前，请确保更新标有尖括号 (< >) 的占位符。

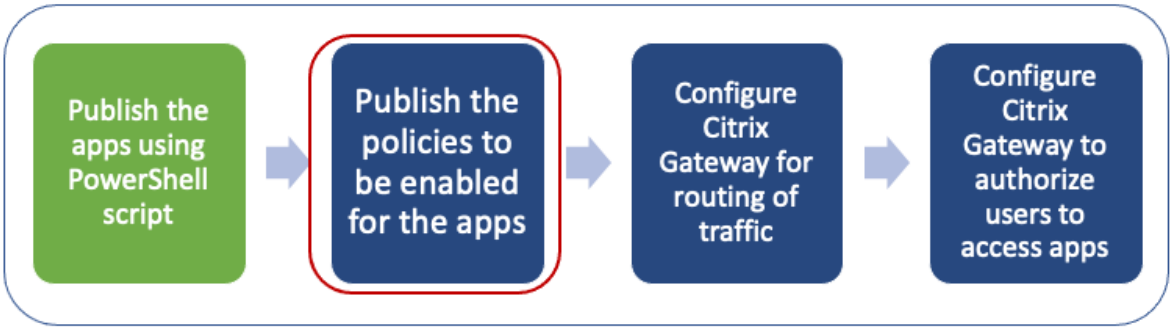
分配位置和应用程序名称后，运行以下命令发布应用程序。

```
New-BrokerApplication -ApplicationType PublishedContent -
    CommandLineExecutable $citrixURL -Name $appName -DesktopGroup $dg.
    Uid
<!--NeedCopy-->
```

已发布的应用程序显示在 **Citrix Studio** 的“应用程序”部分下。现在，您可以从 Citrix Studio 控制台本身修改应用程序详细信息。

有关发布应用程序和更改已发布应用程序的默认图标的更多信息，请参阅 发布内容。

步骤 **2**：发布应用程序的策略



策略文件定义了每个已发布应用程序的路由和安全控制。您必须更新有关 Web 或 SaaS 应用程序的路由方式（通过网关或不通过网关）的策略文件。

要对应用程序强制执行访问策略，必须发布每个 Web 或 SaaS 应用程序的策略。为此，您必须更新策略 JSON 文件和 Web.config 文件。

- 策略 **JSON** 文件：使用应用程序详细信息和应用程序的安全策略更新策略 JSON 文件。然后，必须将策略 JSON 文件放置在 StoreFront 服务器上 `C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser`。

> 注意：
>
> 您必须创建名为 **Resources** 和 **SecureBrowser** 的文件夹，然后在 SecureBrowser 文件夹中添加策略 JSON 文件。
> 有关各种策略操作及其值的更多详细信息，请参阅 应用程序访问策略详细信息。

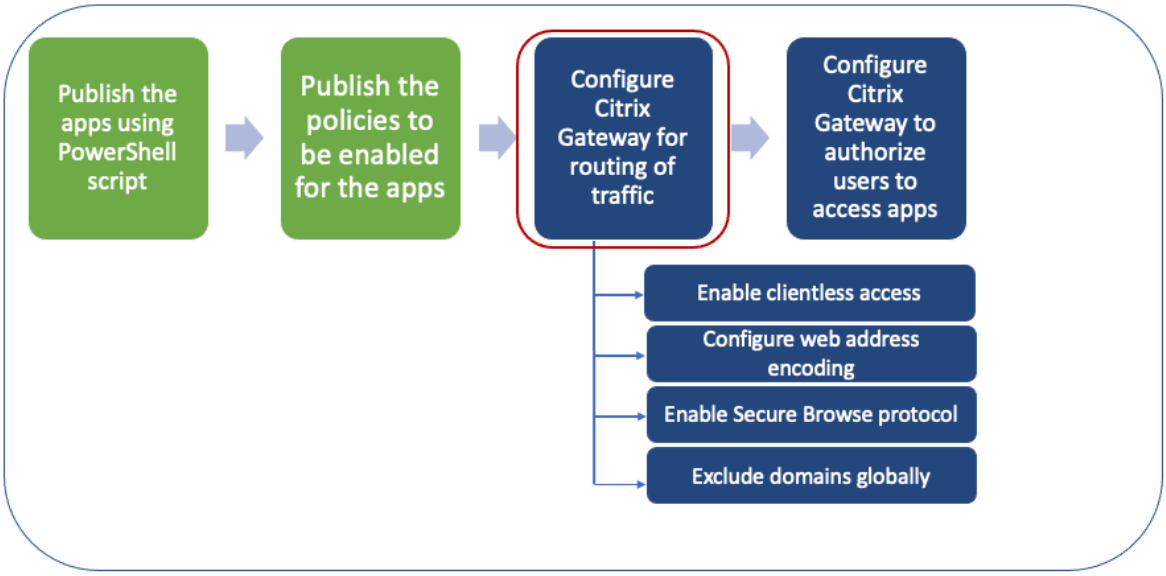
- **Web.config** 文件：要为 Citrix Workspace 应用程序和 Citrix Enterprise Browser 提供新的策略详细信息，必须修改 StoreFront 应用商店目录中的 web.config 文件。必须编辑文件才能添加名为 route 的新 XML 标签。然后必须将 Web.config 文件放在 C:\inetpub\wwwroot\Citrix\Store1. 位置

  有关 示例 XML 文件，请参阅端到端配置 示例。

  > 注意：
  >
  > 在路径中，“store1”是指创建应用商店时为其指定的名称。如果使用不同的应用商店名称，则必须创建相应的文件夹。

  建议您在现有路径的末尾添加一条新路径。如果您在中间添加路线，则必须手动更新所有后续路线的订单号。

步骤 **3**：启用通过 **NetScaler Gateway** 的流量路由



通过 NetScaler Gateway 启用流量路由涉及以下步骤：

- 启用无客户端访问
- 启用 URL 编码
- 启用 Secure Browse
- 排除在无客户端访问模式下重写的域

可以在全局或按会话策略启用无客户端访问、URL 编码和安全浏览。

- 全局启用的设置适用于所有已配置的 NetScaler Gateway 虚拟服务器。
- 每会话策略设置适用于用户、组或 Gateway 虚拟服务器。

启用无客户端访问

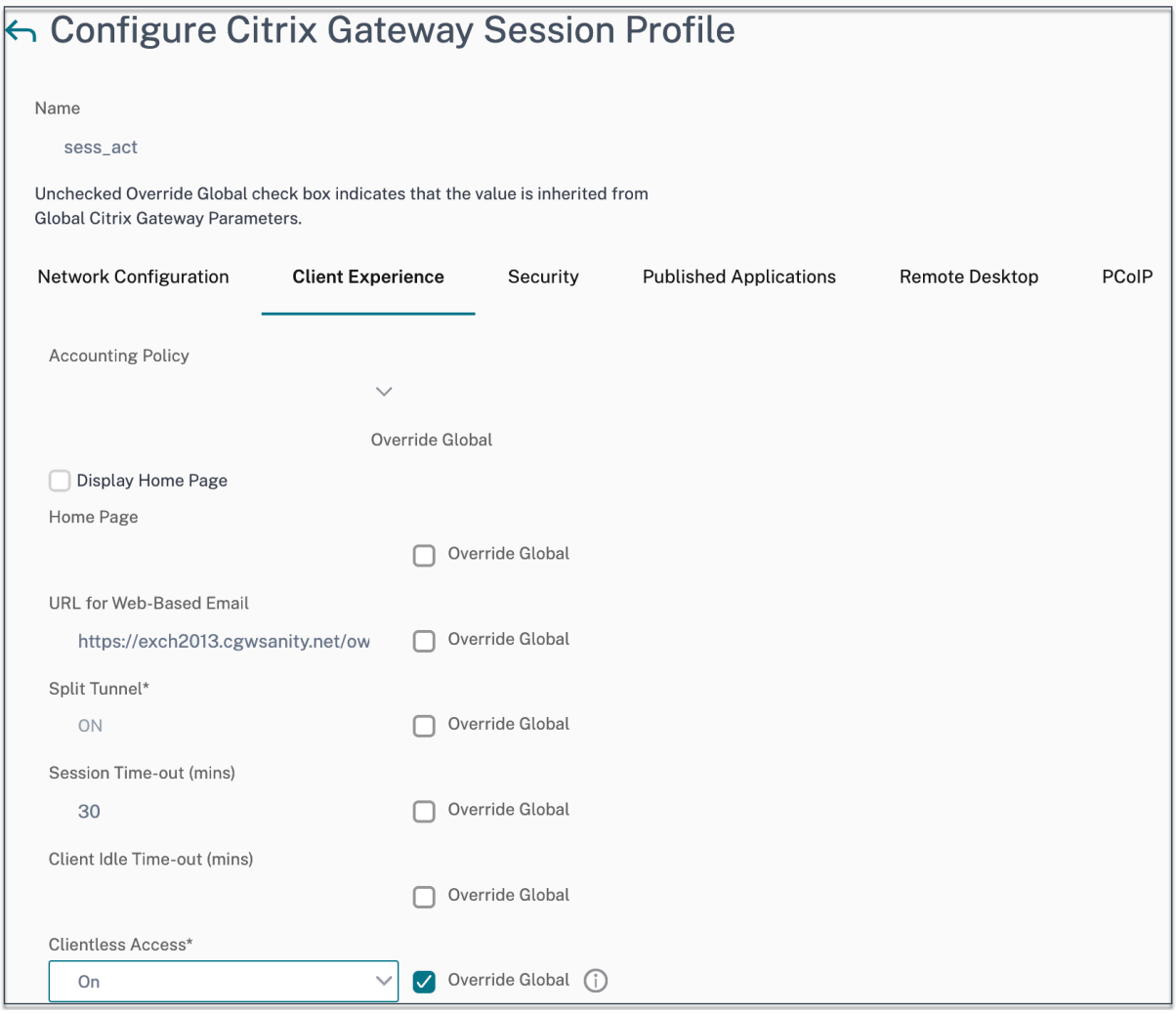
要使用 **NetScaler Gateway GUI** 全局启用无客户端访问，请执行以下操作：

在“配置”选项卡上，展开 **Citrix Gateway**，然后单击“全局设置”。
在“全局设置”页面中，单击更改全局设置。
在“客户端体验”选项卡的“无客户端访问”中，选择“开”，然后单击“确定”。

要使用 **NetScaler Gateway GUI** 使用会话策略启用无客户端访问，请执行以下操作：

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，请在全局范围内禁用或清除无客户端访问。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. 在配置选项卡上，展开 **Citrix Gateway**，然后单击策略 **>** 会话。
2. 单击“会话策略”选项卡，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. 在客户端体验选项卡上，单击“无客户端访问”旁边，单击覆盖全局，选择打开，然后单击创建。
7. 在表达式中，输入 `true`。当您输入值 `true` 时，策略将始终应用到其绑定级别。
8. 单击创建，然后单击关闭。



要使用 **NetScaler Gateway CLI** 实现全局无客户端访问，请执行以下操作：

在命令提示符下，运行以下命令：

```
set vpn parameter -clientlessVpnMode On -icaProxy OFF
<!--NeedCopy-->
```

要使用 **NetScaler Gateway CLI** 启用每次会话的无客户端访问策略，请执行以下操作：

在命令提示符下，运行以下命令：

```
set vpn sessionAction <session-profile-name> -clientlessVpnMode On -
   icaProxy OFF
<!--NeedCopy-->
```


启用 **URL** 编码

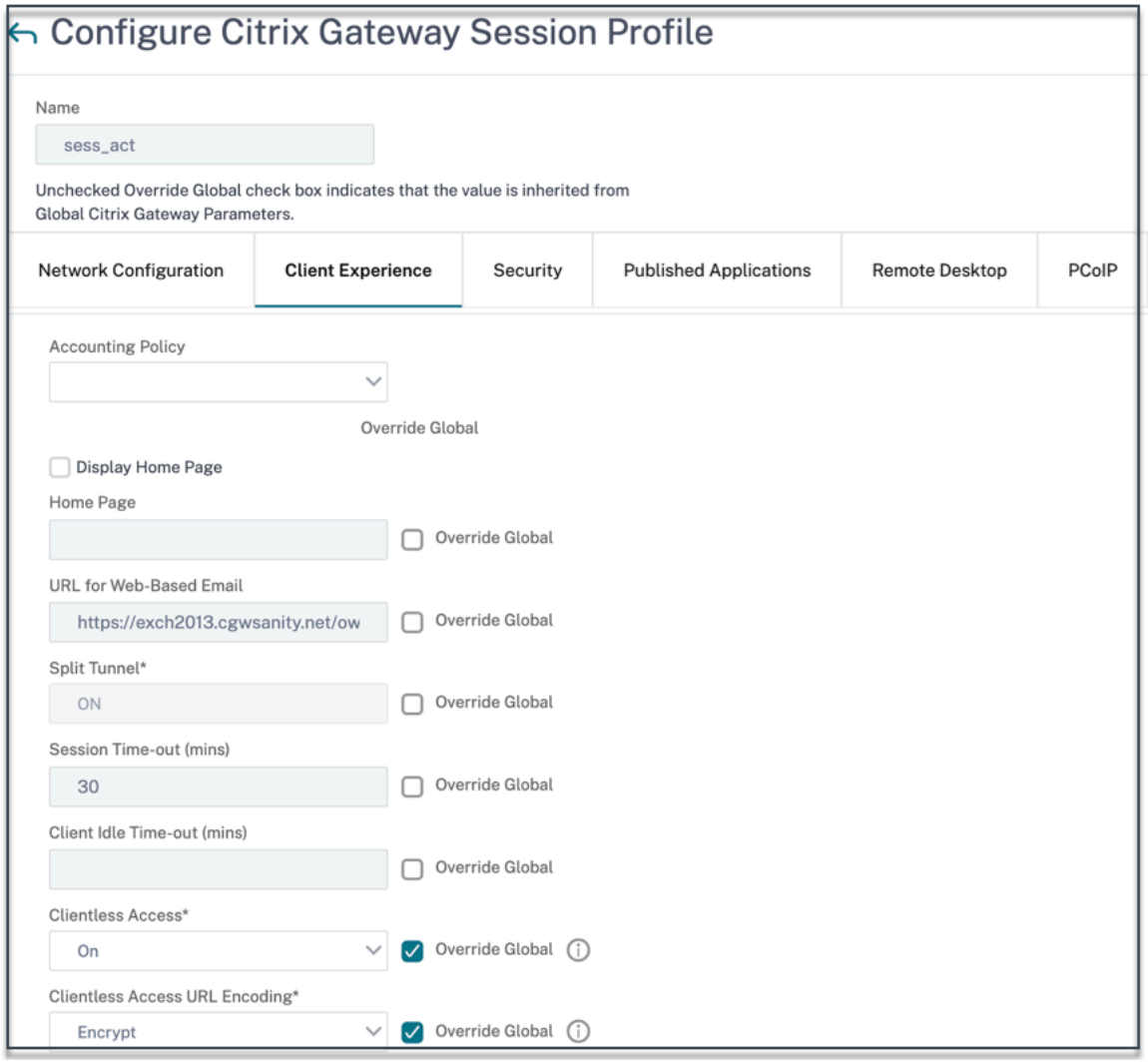
启用无客户端访问时，可以选择对内部 Web 应用程序的地址进行编码或将地址保留为明文。建议您将 Web 地址保留为明文，以便进行无客户端访问。

要使用 **NetScaler Gateway GUI** 全局启用 **URL** 编码，请执行以下操作：

1. 在“配置”选项卡上，展开 **Citrix Gateway**，然后单击“全局设置”。
2. 在“全局设置”页面中，单击“更改全局设置”。
3. 在“客户端体验”选项卡的 无客户端访问 **URL** 编码中，选择用于编码 Web URL 的设置，然后单击“确定”。

要使用 **NetScaler Gateway GUI** 在会话策略级别启用 **URL** 编码，请执行以下操作：

1. 在配置选项卡上，展开 **Citrix Gateway**，然后单击策略 **>** 会话。
2. 单击“会 话策略”选项卡，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. 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. 在表达式中，输入 `true`。当您输入值 `true` 时，策略将始终应用到其绑定级别。



要使用 **NetScaler Gateway CLI** 全局启用 **URL** 编码，请执行以下操作：

在命令提示符下，运行以下命令：

```
1 set vpn parameter -clientlessModeUrlEncoding TRANSPARENT
2 <!--NeedCopy-->
```

要使用 **NetScaler Gateway CLI** 启用每个会话的 **URL** 编码策略，请执行以下操作：

在命令提示符下，运行以下命令：

```
1 set vpn sessionAction <session-profile-name> -clientlessModeUrlEncoding
      TRANSPARENT
2 <!--NeedCopy-->
```


启用 **Secure Browse**

安全浏览和无客户端访问协同工作，允许使用无客户端 VPN 模式进行连接。必须启用安全浏览模式，以便 Citrix Enterprise Browser 可以在没有传统 VPN 的情况下使用安全浏览模式访问应用程序。

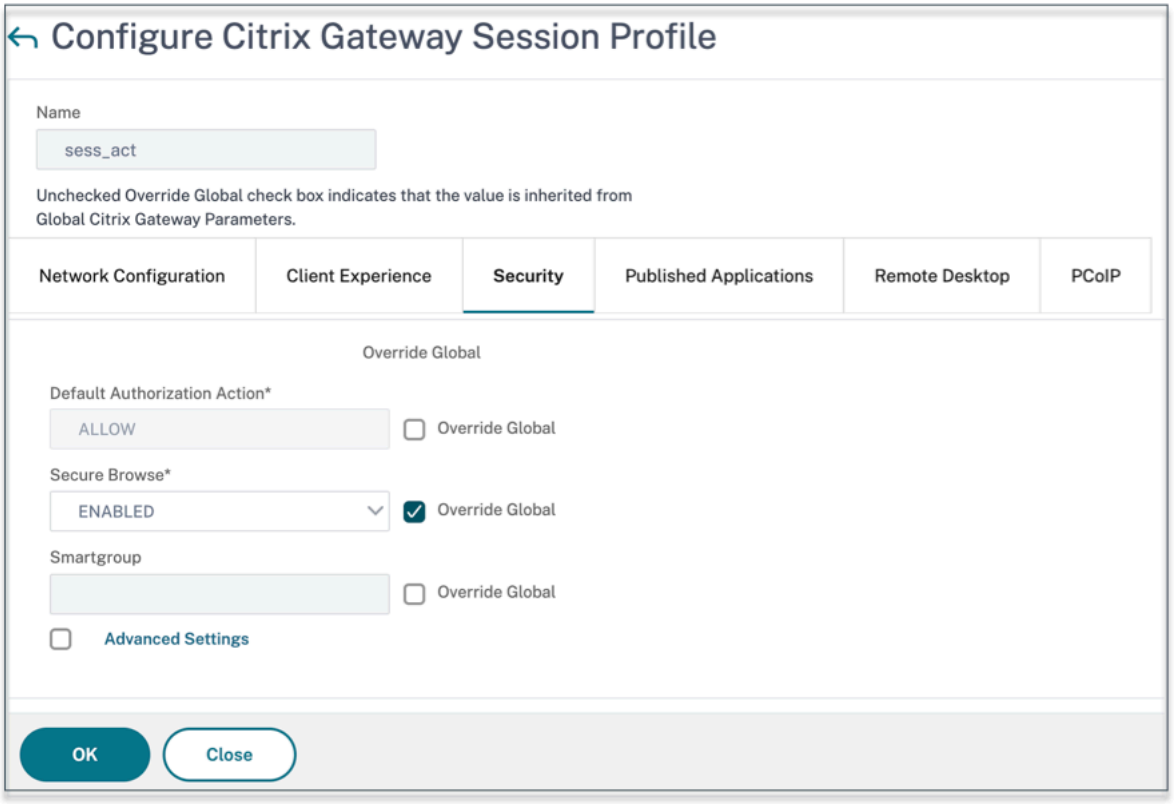
> 注意：
>
> 当最终用户未安装 Citrix Enterprise Browser 时，带有 **SPAEnabled** 标记的已发布 URL 将通过设备的默认浏览器而不是 Citrix Enterprise Browser 打开。在这种情况下，安全策略不适用。该问题仅在 StoreFront 部署中出现。

要使用 **NetScaler Gateway GUI** 全局启用安全浏览模式，请执行以下操作：

1. 在“配置”选项卡上，展开 **Citrix Gateway**，然后单击“全局设置”。
2. 在“全局设置”页面中，单击更改全局设置。
3. 在“安全”选项卡的“Secure Browse”中，选择“已启用”，然后单击“确定”。

要使用 **NetScaler Gateway GUI** 在会话策略级别启用安全浏览模式，请执行以下操作：

1. 在配置选项卡上，展开 **Citrix Gateway**，然后单击策略 **>** 会话。
2. 单击“会话策略”选项卡，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. 在“安全”选项卡上，单击“覆盖全局”，然后将“**Secure Browse**”设置为“已启用”。



要使用 **NetScaler Gateway CLI** 实现全球安全浏览，请执行以下操作：

在命令提示符下，运行以下命令：

```
set vpn parameter -secureBrowse ENABLED
<!--NeedCopy-->
```

要使用 **NetScaler Gateway CLI** 启用安全按会话浏览策略，请执行以下操作：

在命令提示符下，运行以下命令：

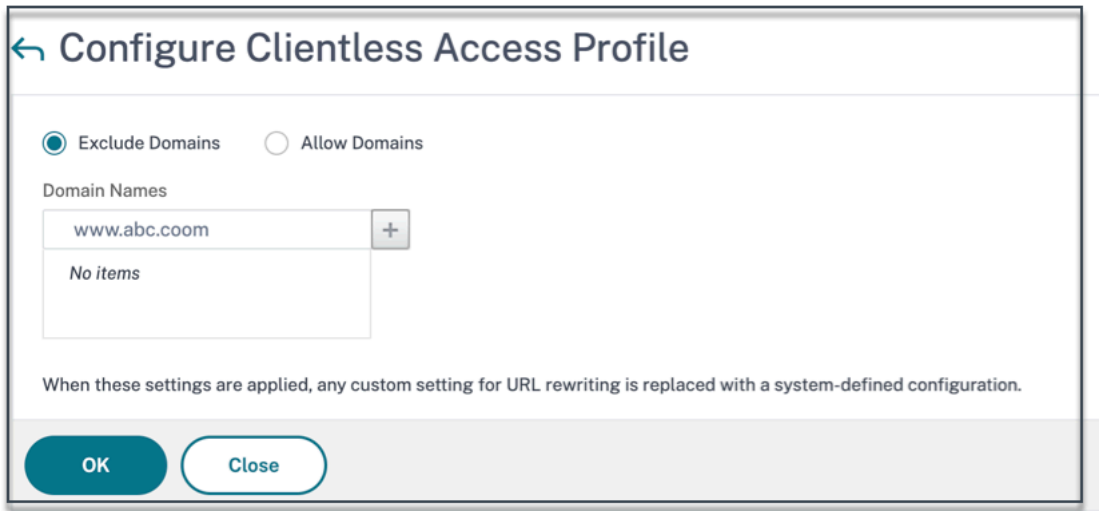
```
set vpn sessionAction <session-profile-name> -secureBrowse ENABLED
<!--NeedCopy-->
```

排除在无客户端访问模式下重写的域

您必须指定域以防止 StoreFront 在无客户端访问模式下重写 URL。不包括 StoreFront 服务器 FQDN 或 StoreFront 负载平衡器 FQDN 和 citrix.com。此设置只能全局应用。

1. 导航到 **Citrix Gateway >** 全局设置。
2. 在 无客户端访问中，单击“为无客户端访问 配置域”。
3. 选择“排除域”。
4. 在 域名中，输入域名（StoreFront 服务器 FQDN 或 StoreFront 负载平衡器 FQDN）。
5. 单击 **+** 符号并输入 `citrix.com`。

6. 单击确定。

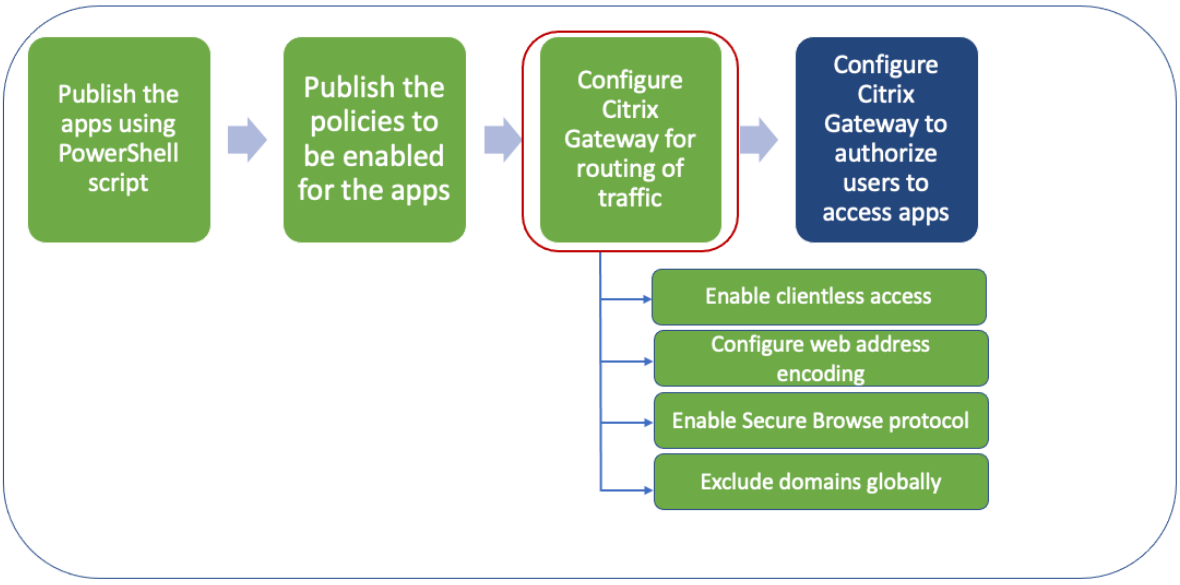


要使用 **NetScaler Gateway CLI** 排除域，请执行以下操作：

在命令提示符下，运行以下命令：

```
1 bind policy patset ns_cvpn_default_bypass_domains <StoreFront-FQDN>
2 bind policy patset ns_cvpn_default_bypass_domains citrix.com
3 <!--NeedCopy-->
```

步骤 **4**：配置授权策略



授权指定了用户在登录 NetScaler Gateway 时有权访问的网络资源。授权的默认设置为拒绝对所有网络资源的访问。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 NetScaler Gateway 上配置授权。创建授权策略后，可以将其绑定到您在设备上配置的用户或组。用户策略的优先级高于组绑定策略。

默认授权策略：必须创建两个授权策略以允许访问 StoreFront 服务器并拒绝访问所有已发布的 Web 应用程序。

- Allow_StoreFront
- Deny_ALL

Web 应用程序授权策略：创建默认授权策略后，必须为每个已发布的 Web 应用程序创建授权策略。

- Allow_<app1>
- Allow_<app2>

要使用 **NetScaler Gateway GUI** 配置授权策略，请执行以下操作：

1. 导航到 **Citrix Gateway >** 策略 **>** 授权。
2. 在详细信息窗格中，单击“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. 要配置表达式，请单击“选择”并选择必要的元素。
7. 单击 **Done**（完成）。
8. 单击 **Create**（创建）。

要使用 **NetScaler Gateway CLI** 配置授权策略，请执行以下操作：

在命令提示符下，运行以下命令：

```
1 add authorization policy <policy-name> "HTTP.REQ.HOSTNAME.CONTAINS("<
     StoreFront-FQDN>")" ALLOW
2 <!--NeedCopy-->
```

要使用 **NetScaler Gateway GUI** 将授权策略绑定到用户/组，请执行以下操作：

1. 导航到 **Citrix Gateway >** 用户管理。
2. 单击 **AAA** 用户 或 **AAA** 组。
3. 在详细信息窗格中，选择一个用户/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，设置优先级编号。
7. 在 类型中，选择请求类型，然后单击 确定。

要使用 **NetScaler Gateway CLI** 绑定授权策略，请执行以下操作：

在命令提示符下，运行以下命令：

```
1 bind aaa group <group-name> -policy <policy-name> -priority <priority>
     -gotoPriorityExpression END
```



```
<!--NeedCopy-->
```

端到端配置示例

在此示例中，一个名为“文档”且具有 URL 的应用程序 https://docs.citrix.com 被发布到 Citrix Workspace。

1. 在包含 PowerShell SDK 的计算机上打开 PowerShell。
2. 运行以下命令。

```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup -Name PublishedContentApps
<!--NeedCopy-->
```

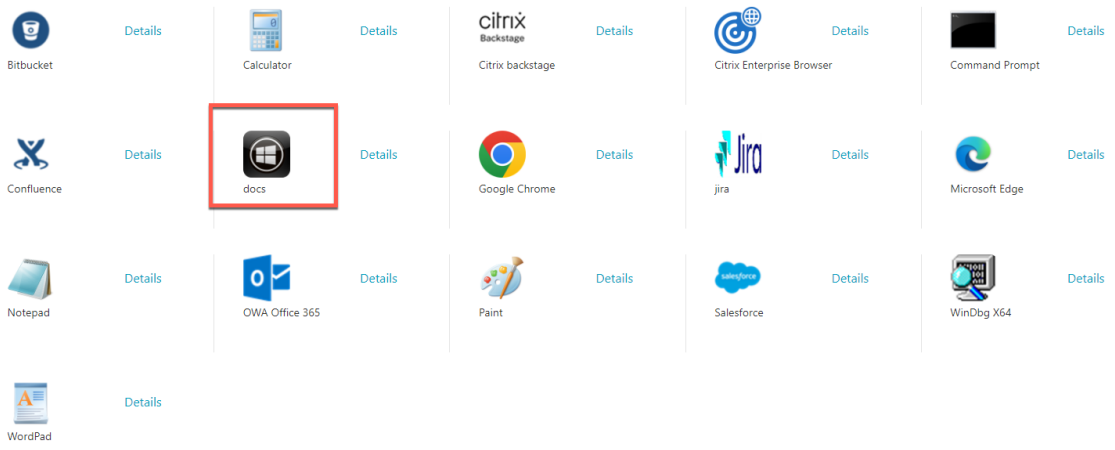
3. 将以下详细信息添加到 cmdlet 中。

```
$citrixUrl: “https://docs.citrix.com”
$appName: docs
$DesktopGroupId: 1
$desktopgroupname: <mydesktop23>
<!--NeedCopy-->
```

4. 运行以下命令。

```
New-BrokerApplication -ApplicationType PublishedContent -
    CommandLineExecutable $citrixURL -Name $appName -DesktopGroup
     $dg.Uid
<!--NeedCopy-->
```

该应用程序现已在 Citrix Workspace 上发布。



5. 使用应用程序（“文档”）详细信息更新策略 JSON 文件。请务必满足以下各项条件：

   - `proxytraffic_v1` 值始终设置为 `secureBrowse`。此设置可确保 Citrix Enterprise Browser 使用安全浏览协议通过 NetScaler Gateway 将流量通过通道传输到网页。

- `browser_v1` 值始终设置为 `embeddedBrowser`。仅当 Citrix Enterprise Browser (CEB) 配置为工作浏览器时，此设置才适用。如果设置为 `embeddedBrowser`，则与已配置的 Secure Private Access 域相关的链接将在 CEB 中打开。
- `secureBrowseAddress` 值是您的 NetScaler Gateway URL。

```
{
  "policies": [
    {
      "name": "Docs",
      "patterns": ["*.docs.netscaler.com/*"],
      "policy": {
        "watermark_v1": "enabled",
        "clipboard_v1": "disabled",
        "printing_v1": "disabled",
        "download_v1": "disabled",
        "upload_v1": "disabled",
        "keylogging_v1": "disabled",
        "screencapture_v1": "enabled",
        "proxytraffic_v1": "secureBrowse",
        "browser_v1" : "embeddedBrowser"
      }

    }],
  "system": {
    "secureBrowseAddress": "https://yournetscalergateway.com"
  }
}
```

6. 将策略 JSON 文件放在 C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser.
7. 修改 Web.config 文件以指向您更新的策略文件。

```
<route name="webSecurePolicy" order="22" url="Resources/SecureBrowser/policy.json">
        <defaults>
          <add param="controller" value="BrowserPolicy" />
          <add param="action" value="BrowserResources" />
        </defaults>
        <data>
          <add name="endpointId" value="WebSecurePolicy" />
          <add name="endpointCapabilities" value="webSecurePolicy" />
          <add name="CommonData" factory="Citrix.DeliveryServices.Configuration.ObjectCollectionFactory, Citrix.DeliveryServices.Configuration, Version=3.23.0.0, Culture=neutral,
PublicKeyToken=e8b77d454fa2a856" path="citrix.deliveryservices/dazzleResources" property="commonData" />
        </data>
      </route>
```

8. 在您的 NetScaler Gateway 本地设备上，执行以下操作：
   - 启用对应用程序的无客户端访问。您可以在全局或会话级别启用无客户端访问。

- 启用 Web 地址编码
- 启用 Secure Browse 模式
- 排除在无客户端访问模式下重写的域

有关详细信息，请参阅步骤 3：使用本地 NetScaler Gateway 启用身份验证和授权。

最终用户流程

- 以可以访问 PublishedContentApps 交付组中应用程序的用户身份登录 StoreFront。
- 登录后，必须看到带有默认图标的新应用程序。您可以根据需要自定义图标。有关详细信息，请参阅 https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/。
- 当您单击该应用程序时，该应用程序将在 Citrix Enterprise Browser 中打开。

应用程序访问策略详情

下表列出了可用的访问策略选项及其值。

注册表项名称	策略说明	值
–	–	–
screencapture_v1	启用或禁用网页的反屏幕捕获功能	已启用或已禁用
键盘记录 _v1	启用或禁用网页的反键盘记录	已启用或已禁用
watermark_v1	在网页上显示或不显示水印	已启用或已禁用
upload_v1	启用或禁用上载网页	已启用或已禁用
printing_v1	启用或禁用网页打印	已启用或已禁用
download_v1	启用或禁用从网页下载	已启用或已禁用
clipboard_v1	在网页上启用或禁用剪贴板	已启用或已禁用
proxytraffic_v1	确定 Citrix Enterprise Browser 是使用安全浏览通过 NetScaler Gateway 将流量通过通道传输到网页，还是启用直接访问	direct 或 secureBrowse
browser_v1	仅当 Citrix Enterprise Browser 配置为工作浏览器时才适用。设置为 embeddedBrowser 时，与已配置的 Secure Private Access 域相关的链接将在 Citrix Enterprise Browser 中打开	systemBrowser 或 embeddedBrowser
Name|Web 或 SaaS 应用程序的名称已发布	建议您使用与发布应用程序模式时输入的相同名称	逗号分隔的与此应用程序相关的域名列表。您也可以使用通配符。Citrix Enterprise 浏览器使用这些域名对应用程序应用策略。| 示例：”*.office.com/*”，“*.office.net/*”，“*.microsoft.com/* “.sharepoint.com/*”

> 注意：
>
> 防键盘记录和防屏幕捕获需要安装 Citrix Workspace 应用程序自带的 App Protection 功能。

使用 **Secure Private Access** 配置工具配置应用程序和策略 **-** 旧版

February 20, 2024

您可以在 Citrix Virtual Apps and Desktops Delivery Controller 上使用 Secure Private Access 配置工具来快速创建 SaaS 或 Web 应用程序。此外，您可以使用此工具设置应用程序限制、流量路由和创建 NetScaler Gateway。该工具生成脚本文件作为输出，可以在相应的计算机上运行以部署配置。

支持的产品版本

确保您的产品符合最低版本要求。

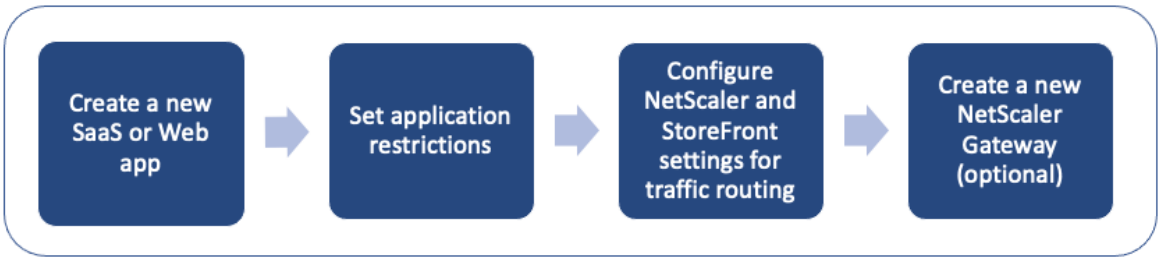
- Citrix Workspace 应用程序
  - Windows —2303 及更高版本
  - macOS —2304 及更高版本
- Citrix Virtual Apps and Desktops - 支持的 LTSR 和当前版本
- StoreFront —LTSR 2203 或非 LTSR 2212 及更高版本
- NetScaler —12.1 及更高版本

使用配置工具的先决条件

- 可以从“下载”页面下载配置工具。
- 在 Citrix Virtual Apps and Desktops 控制器上运行配置工具的管理员权限。
- Delivery Controller 上至少存在一个交付组。

开始使用配置工具

您可以使用配置工具执行以下任务。

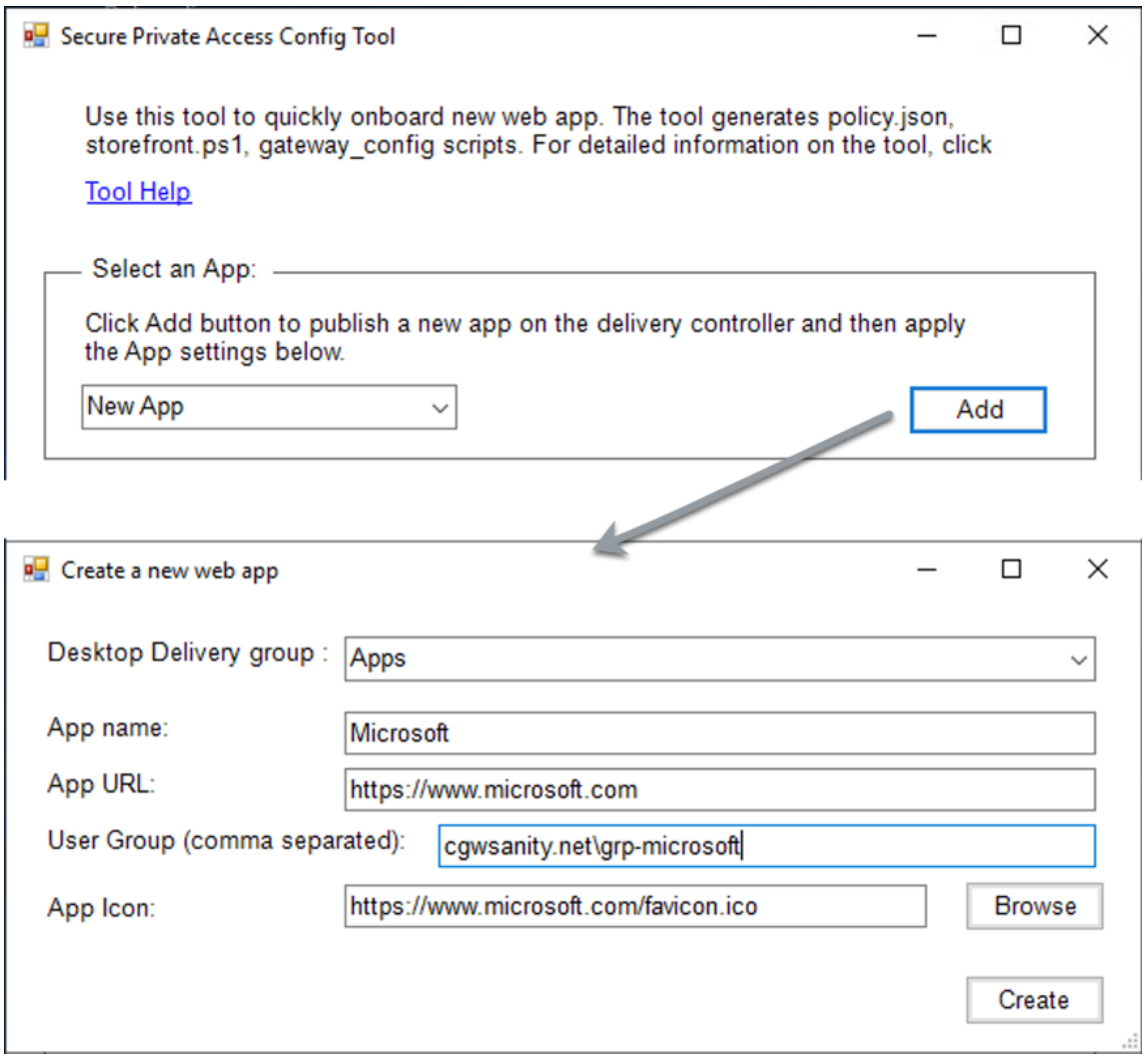


- 发布新应用程序
- 设置应用程序限制

- 配置 StoreFront 和 NetScaler Gateway 设置
- 配置新的 NetScaler Gateway

发布新应用程序

1. 运行配置工具。
2. 在“选择应用程序”部分中，在下拉列表中选择“新建应用程序”，然后单击“添加”。



3. 完成应用程序配置。
   - 桌面交付组：选择必须允许该应用程序访问的交付组。
     桌面交付组中列举了所有现有的交付组。
   - 应用程序名称：输入应用程序名称。
   - 应用程序 **URL**：指定应用程序的 URL。

- 用户组：以“域\ 组”格式输入域名和组名。用户组可以包含空格。例如，“cgwsanity.net\grp-microsoft”、“cgwsanity.net\grp microsoft”。
  这些组必须已经存在于 Active Directory 中。

  > **Note:**
  >
  > - Built-in domain security groups such as “Domain Users” or “Domain Admins” are not supported. Only the manually created user groups must be used.
  > - The user group is only used in NetScaler Gateway authorization policies and not for app assignments in Citrix Virtual Apps and Desktops. Hence, the user group that you enter here is not visible in Studio.

- 应用程序图标：如果检测到该工具，则使用 URL 的 favicon.ico。如有必要，管理员还可以自定义图标。
  如果管理员未提供任何图标，则将默认图标分配给应用程序。

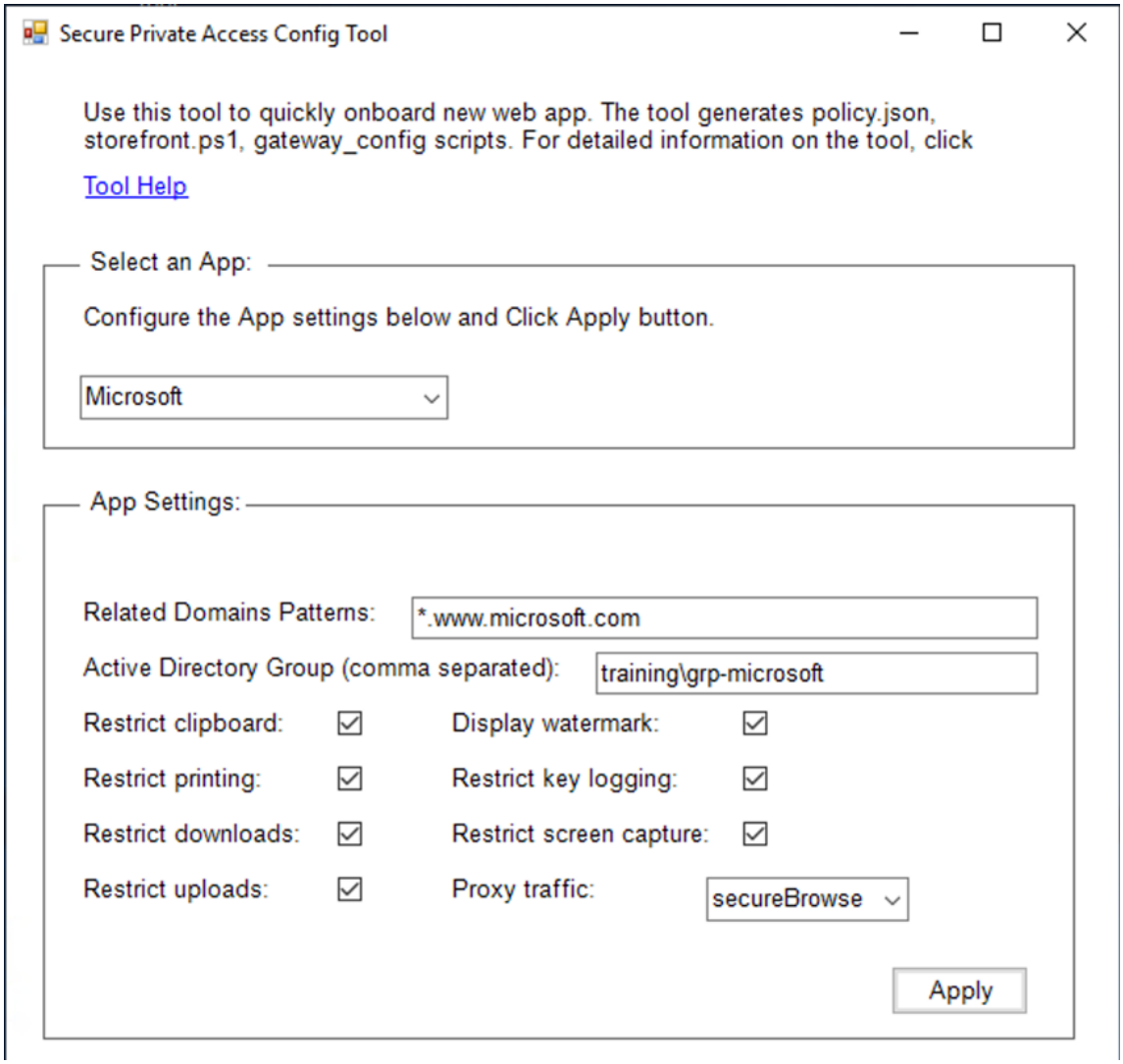
4. 单击 **Create**（创建）。

该应用程序在 Delivery Controller 上发布，可供 StoreFront 用户组中的用户使用。

设置应用程序限制

发布新应用程序后，您可以启用或禁用该应用程序的限制。

1. 在 选择应用程序 部分中，从下拉列表中选择要对其强制执行设置的应用程序。



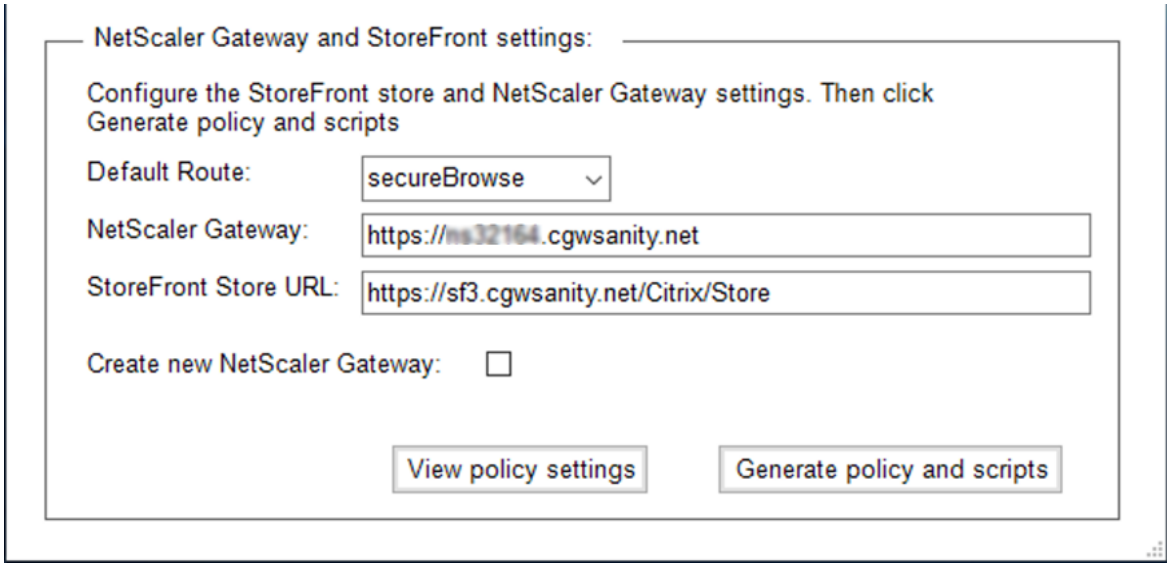
2. 在“应用程序设置”部分中配置 应用程序设置。

   - 相关域名模式：相关域 URL 根据应用程序 URL 自动填充。管理员可以添加其他用逗号分隔的域名。
   - **Active Directory** 组：输入必须可以访问此应用程序的组。此字段为必填字段。
     您可以输入用逗号分隔的多个组。这些组必须与 Active Directory 中的可用组相匹配。未对您在此处输入的组名进行验证。因此，请务必注意输入与 Active Directory 中的组名相匹配的组名。
   - 应用程序设置：默认情况下，所有应用程序设置均受限制（选中）。您可以为用户组选择或清除所需的相应设置。
   - 代理流量：选择 secureBrowse。此设置允许 Citrix Enterprise Browser 通过 NetScaler Gateway 将流量通过通道传送到网页。

3. 单击应用。

配置 **StoreFront** 和 **NetScaler Gateway** 设置

您可以配置通过 NetScaler Gateway 路由流量的设置。您可以在 **Gateway** 和 **StoreFront** 设置部分配置现有的 NetScaler Gateway 或创建新的 NetScaler Gateway。



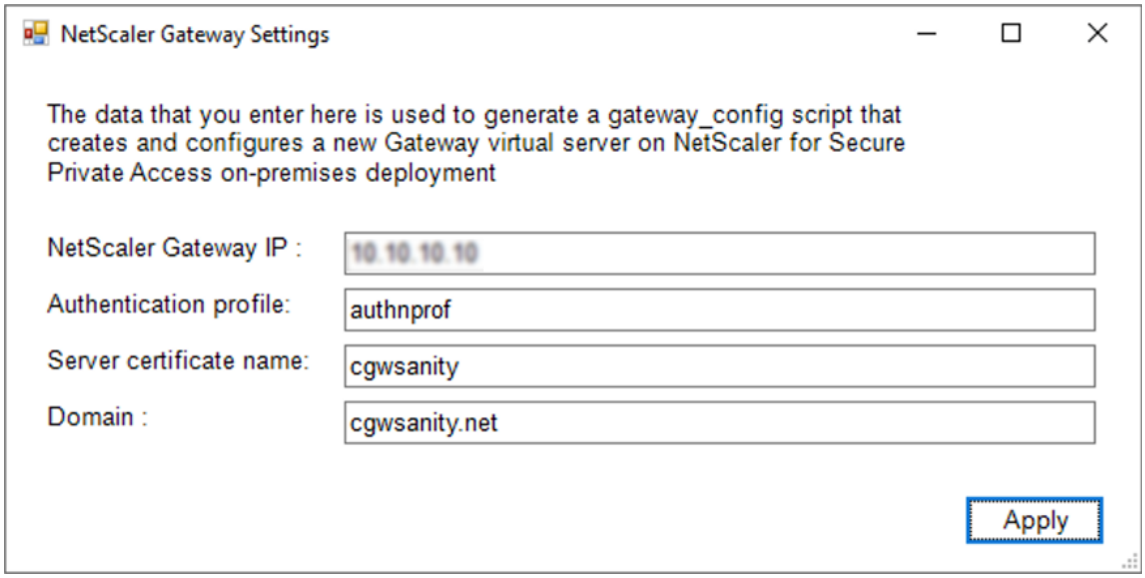
- 默认路由：如果未为应用程序定义策略，则将默认路由应用于应用程序。
  - **secureBrowse**：Citrix Enterprise Browser 通过 NetScaler Gateway 将流量传送到网页。
  - 直接：Citrix Enterprise Browser 允许直接访问应用程序。
- **NetScaler Gateway**：输入 NetScaler Gateway URL。
- **StoreFront** 应用商店 **URL**：输入完整的 StoreFront 应用商店 URL。例如，`http://<directory path>/Citrix/<StoreName>`。您可以从 StoreFront 控制台获取 URL。
- （可选）创建新网关：选中复选框以创建新的 NetScaler Gateway，然后单击“创建”。

创建新的 **NetScaler Gateway**（可选）

如果您不想更改现有网关设置，则可以创建新的 NetScaler Gateway。

如果您已经有 NetScaler Gateway，则可以使用配置工具为应用程序配置授权策略和绑定。

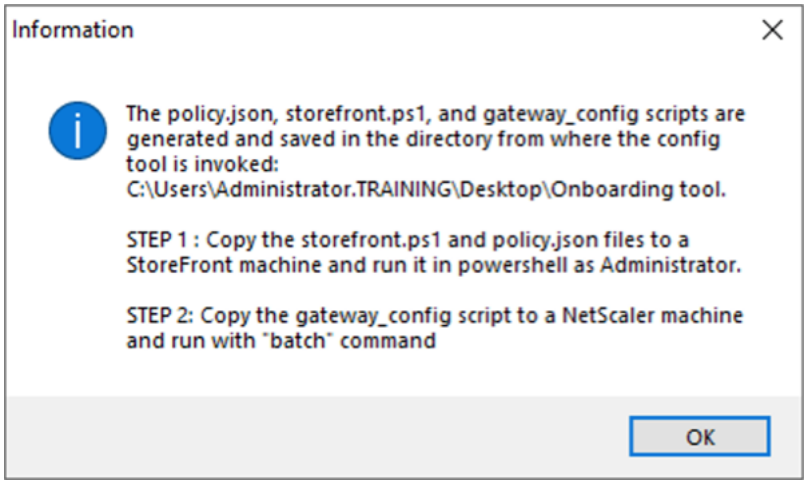
1. 您必须为新的 NetScaler Gateway 输入以下详细信息。该工具不会对您在创建新网关时输入的值进行验证。因此，务必注意输入准确的值。



- 网关 **IP**：NetScaler Gateway 的 IP 地址。
- 身份验证配置文件：输入已在 NetScaler 上配置的身份验证配置文件名称。有关详细信息，请参阅 验证配置
- 服务器证书名称：输入已在 NetScaler 上配置的 SSL 证书名称。有关详细信息，请参阅 SSL 证书。
- 域：用于对内部网络中的应用程序进行 SSO。有关详细信息，请参阅 VPN 会话操作。

2. 单击应用。
3. 单击“生成策略和脚本”。

   policy.json、storefront.ps1 和 gateway_config 文件是生成并存储在您运行配置工具的位置。



在支持的应用程序中打开 gateway_config 文件时，可以查看输出文件中的两个部分。

- 与 NetScaler Gateway 配置相关的部分（仅适用于创建新网关时）
- 与授权策略、用户组和用户组绑定策略相关的部分。

下图显示了新的 NetScaler Gateway 配置的 gateway_config 文件。

```
#############################################################################################################
#1. Upload file to NetScaler (e.g. to /var/tmp)
#2. Run batch command (e.g. batch -fileName /var/tmp/gateway_config -outfile /var/tmp/gateway_config_output)
#3. Analyze output (e.g. cat /var/tmp/gateway_config_output)
#############################################################################################################

# Enable NS features
enable ns feature SSL SSLVPN AAA

# Add Gateway
add vpn vserver _XD_SPAGateway_443 SSL [redacted] -Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile
-deploymentType ICA_STOREFRONT -vserverFqdn gwalextest.spaopdev.local -authnProfile spaopdev_auth_prof -icaOnly OFF

# Add excluded domains
bind policy patset ns_cvpn_default_bypass_domains corealextest.spaopdev.local
bind policy patset ns_cvpn_default_bypass_domains citrix.com

# Add session actions
add vpn sessionAction AC_OS_SPAGateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF
-wihome "http://corealextest.spaopdev.local/Citrix/StoreWeb" -ClientChoices OFF -ntDomain spaopdev.local -clientlessVpnMode ON
-clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -storefronturl "http://corealextest.spaopdev.local" -sfGatewayAuthType domain

add vpn sessionAction AC_WB_SPAGateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF
-wihome "http://corealextest.spaopdev.local/Citrix/StoreWeb" -ClientChoices OFF -ntDomain spaopdev.local -clientlessVpnMode ON
-clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -storefronturl "http://corealextest.spaopdev.local" -sfGatewayAuthType domain

# Add session policies
add vpn sessionPolicy PL_OS_SPAGateway "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")" AC_OS_SPAGateway
add vpn sessionPolicy PL_WB_SPAGateway "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT" AC_WB_SPAGateway

# Bind policies to vserver
bind vpn vserver _XD_SPAGateway_443 -policy PL_OS_SPAGateway -priority 100 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver _XD_SPAGateway_443 -policy PL_WB_SPAGateway -priority 110 -gotoPriorityExpression NEXT -type REQUEST

# Bind SSL cert to GW
bind ssl vserver _XD_SPAGateway_443 -certkeyName spaopdev

# Add default authorization policies
add authorization policy ALLOW_STOREFRONT "HTTP.REQ.HOSTNAME.CONTAINS(\"corealextest.spaopdev.local\")" ALLOW
add authorization policy DENY_ALL true DENY

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "SPAOP users"
bind aaa group "SPAOP users" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "SPAOP users" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.google.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.google.com\")" ALLOW

unbind aaa group "SPAOP users" -policy www.google.com
bind aaa group "SPAOP users" -policy www.google.com -priority 100 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupab"
bind aaa group "groupab" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupab" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

unbind aaa group "groupab" -policy www.google.com
bind aaa group "groupab" -policy www.google.com -priority 110 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupxy"
bind aaa group "groupxy" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupxy" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.microsoft.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.microsoft.com\")" ALLOW

unbind aaa group "groupxy" -policy www.microsoft.com
bind aaa group "groupxy" -policy www.microsoft.com -priority 120 -gotoPriorityExpression END

# Save
save ns config
```

下图显示了更新后的 NetScaler Gateway 配置的 gateway_config 文件。


```
#############################################################################################################
#1. Upload file to NetScaler (e.g. to /tmp)
#2. Run batch command (e.g. batch -fileName /tmp/Gateway_config -outfile /tmp/Gateway_config_output)
#3. Analyze output (e.g. cat /tmp/Gateway_config_output)
#############################################################################################################

# Add default authorization policies
add  policy ALLOW_STOREFRONT "HTTP.REQ.HOSTNAME.CONTAINS(\"corealextest.spaopdev.local\")" ALLOW
add  policy DENY_ALL true DENY

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "SPAOP users"
bind aaa group "SPAOP users" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "SPAOP users" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.google.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.google.com\")" ALLOW

unbind aaa group "SPAOP users" -policy www.google.com
bind aaa group "SPAOP users" -policy www.google.com -priority 100 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupab"
bind aaa group "groupab" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupab" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

unbind aaa group "groupab" -policy www.google.com
bind aaa group "groupab" -policy www.google.com -priority 110 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupxy"
bind aaa group "groupxy" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupxy" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.microsoft.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.microsoft.com\")" ALLOW

unbind aaa group "groupxy" -policy www.microsoft.com
bind aaa group "groupxy" -policy www.microsoft.com -priority 120 -gotoPriorityExpression END

# Save
save ns config
```

使用新的 **NetScaler Gateway** 配置 **StoreFront**

- 要在工具中配置 StoreFront 和 NetScaler Gateway 设置，您需要以下内容：
  - NetScaler Gateway FQDN
  - StoreFront 应用商店 URL
- StoreFront 配置要求：
  - NetScaler Gateway：远程访问已启用。
  - 来自 NetScaler Gateway 的直通身份验证已启用。
  - 活动目录：管理员访问权限，用于添加或更新用户或组，以及在 NetScaler 上配置身份验证配置文件或策略。

有关更多详细信息，请参阅 将 NetScaler Gateway 与 StoreFront 集成。

使用配置工具输出文件部署应用程序和策略配置

配置工具生成以下文件。这些文件保存在上载和运行该工具的位置/目录中。

- policy.json
- storefront.ps1
- gateway_config

1. 将 storefront.ps1 文件复制到 StoreFront。
2. 以管理员身份在 PowerShell 上运行 storefront.ps1 脚本。

   如果 Resources\SecureBrowser 文件夹在存储路径中尚不可用，则脚本会创建该文件夹。

   该脚本还更新了 policy.json 文件路由的 web.config 文件。
3. 将 policy.json 文件复制到 storefront.ps1 在应用商店下创建的 Resources\SecureBrowser 文件夹。
4. 将 gateway_config 复制到 NetScaler，然后在 NetScaler CLI 上使用以下批处理命令运行脚本。

   ```
   batch -fileName /var/tmp/gateway_config -outfile /var/tmp/gateway_config_o
   ```

> 注意：
>
> - 在工具中进行任何配置更改时，必须重新生成脚本和策略。您必须再次将 policy.json 文件复制到 StoreFront 计算机上的 Resources\SecureBrowser 文件夹，然后必须在 NetScaler 上再次运行 gateway_config 脚本。
> - 如果应用商店名称/URL 未更改，则不必再次运行 storefront.ps1。

其他参考资料

有关更多详细信息，请参阅以下文档。

- 本地 Secure Private Access
- 部署指南：本地 Secure Private Access