远程浏览器隔离

Citrix Remote Browser Isolation™ 服务（前身为 Secure Browser 服务）隔离 Web 浏览，以保护公司网络免受基于浏览器的攻击。Remote Browser Isolation 服务提供对互联网托管 Web 应用程序的一致、安全的远程访问，无需用户设备配置。管理员可以快速部署远程隔离浏览器，从而实现即时价值。通过隔离互联网浏览，IT 管理员可以为最终用户提供安全的互联网访问，而不会损害企业安全性。

用户登录到其应用商店，并在配置的 Web 浏览器中打开 Web 应用程序。网站不会直接将任何浏览数据传输到用户设备或从用户设备传输，因此体验是安全的。

Remote Browser Isolation 服务可以发布远程隔离浏览器，以用于：

- **共享密码外部 Web 应用程序：** 如果您发布了使用共享密码身份验证的浏览器，用户必须输入密码才能启动应用程序。
- **经过身份验证的外部 Web 应用程序：** 当您发布经过身份验证的外部 Web 应用程序并从其应用商店启动这些应用程序时，Remote Browser Isolation 服务需要一个资源位置，其中包含至少一个 Cloud Connector（建议使用两个或更多）。您必须为经过身份验证的应用程序添加用户。有关详细信息，请参阅 Citrix Cloud Connector。
- **未经身份验证的外部 Web 应用程序：** 当您发布未经身份验证的外部 Web 应用程序并从其应用商店启动这些应用程序时，Remote Browser Isolation 服务需要一个资源位置，其中包含至少一个 Cloud Connector（建议使用两个或更多）。有关详细信息，请参阅 Citrix Cloud Connector。

  尽管通常不建议这样做，但未经身份验证的外部 Web 应用程序可用于简单的概念验证。

有关详细信息，请参阅 发布远程隔离浏览器。

该服务还提供：

- 将已发布的应用程序与 Citrix® StoreFront Cloud 集成
- 将已发布的应用程序与本地 StoreFront 集成
- 用于安全性的简单 URL 允许列表功能
- 使用情况监控
- 剪贴板使用、打印、自助服务终端模式、区域故障转移和客户端驱动器映射的控件

与 Citrix Secure Private Access™ 结合的远程浏览器隔离服务

您可以使用 Citrix Secure Private Access 控制台启动远程浏览器隔离服务的已发布浏览器，以访问企业 Web、TCP 和 SaaS 应用程序。您还可以通过 Citrix Secure Private Access 将未经批准的网站重定向到远程浏览器隔离服务的已发布浏览器中打开。

有关通过 Citrix Secure Private Access 访问隔离的远程浏览器的更多信息，请参阅 Citrix Secure Private Access 文档中的配置具有多个规则的访问策略和未经批准的网站。

参考文章

- Secure Private Access 服务解决方案概述
- 思杰云
- 远程浏览器隔离（安全浏览器）的自助服务搜索
- Citrix 企业浏览器(/zh-cn/citrix-enterprise-browser)
- 安全和合规性信息
- 开发人员文档

相关产品中的新增功能

- 安全私有访问(/zh-cn/citrix-secure-private-access/service/whats-new)
- Citrix 企业浏览器(/zh-cn/citrix-enterprise-browser/whats-new)
- Citrix 安全分析(/zh-cn/security-analytics/whats-new)

新增功能

2026 年 8 月

- **NAT 网关内置于目录创建中**：网络地址转换 (NAT) 网关现已内置于目录创建流程中，不再需要单独的开关。

2026 年 7 月

- **粒度复制和粘贴剪贴板策略**：管理员现在可以为已发布的远程浏览器独立配置复制和粘贴策略。以前，“**剪贴板**”策略作为一个单一的开关控制复制和粘贴操作。通过此更新，单一的剪贴板策略被两个粒度控制取代：
  - **复制** — 启用后，允许用户将内容从远程浏览器会话复制到本地剪贴板。
  - **粘贴** — 启用后，允许用户将内容从本地剪贴板粘贴到远程浏览器会话。

  这种分离使管理员能够对远程会话和用户端点之间的数据流进行细粒度控制。有关详细信息，请参阅策略。

2026 年 2 月

- **远程浏览器隔离更新**
  - 您现在可以将 Citrix Remote Browser Isolation™ (RBI) 与 Google Chrome Enterprise Premium (CEP) 集成。使用 Google 令牌注册目录，以在目录级别应用 Chrome 企业策略。管理员可以从 Google 管理控制台集中管理这些策略。有关详细信息，请参阅与 Chrome Enterprise Premium (CEP) 集成。
  - 管理员现在可以在 RBI 会话期间跟踪和审计用户浏览活动。日志捕获访问的网站、访问时间戳、用户标识符和允许列表强制执行状态。所有收集的数据都存储在客户管理的 Azure 存储帐户中，以确保完全的数据所有权和控制。有关详细信息，请参阅用户活动日志记录。

2025 年 6 月

- **远程浏览器隔离 - 自托管工作负载**

- 远程浏览器隔离 (RBI) 自托管工作负载使客户能够在自己的 Azure 订阅中运行远程浏览器工作负载。RBI 自托管工作负载中的数据平面组件（虚拟桌面代理）在客户提供的 Azure 订阅中运行。这允许客户根据需要横向扩展计算机和目录，并预配多个目录以实现更好的工作负载分类。

2022 年 7 月

- **Remote Browser Isolation 支持通过 Microsoft Entra ID 对所有应用进行身份验证**
  - 用户现在可以使用 Microsoft Entra ID 凭据，通过 Citrix Workspace™ 登录任何 Remote Browser Isolation 应用。
  - 当 Remote Browser Isolation 用户登录时，他们会使用您为站点配置的 Workspace 登录页面。有关详细信息，请参阅 与 Citrix Workspace 集成。

2021 年 9 月

- **Remote Browser Isolation 支持双向音频**
  - Remote Browser Isolation 中提供双向音频。
- **从 launch.cloud.com 启动的 Remote Browser Isolation 通过 Citrix Cloud 身份验证进行身份验证**
  - 当用户使用 launch.cloud.com URL 启动 Remote Browser Isolation 应用时，Citrix Cloud 身份验证会处理其凭据。这增强了安全性，但不会改变用户体验。

2021 年 3 月

- **Remote Browser Isolation 支持通过 Microsoft Entra ID 进行身份验证**
  - 用户现在可以使用 Microsoft Entra ID 凭据，通过 Citrix Workspace 登录 Remote Browser Isolation 应用。有关详细信息，请参阅 与 Citrix Workspace 集成。
- **Remote Browser Isolation 允许您监视和注销用户的活动会话**
  - Remote Browser Isolation 提供有关用户活动会话的用户名、会话 ID、客户端 IP、身份验证类型、应用程序名称、会话开始时间和会话持续时间信息。您可以查看每个活动会话的基本信息，并在需要时断开会话。有关详细信息，请参阅 监视活动会话。

2020 年发布

2020年的所有版本都包含有助于提升整体性能和稳定性的增强功能。

远程浏览器隔离入门

远程浏览器隔离 - 自托管工作负载

远程浏览器隔离 (RBI) 自托管工作负载使客户能够在自己的 Azure 订阅中运行远程浏览器工作负载。RBI 自托管工作负载中的数据平面组件（虚拟桌面代理）在客户提供的 Azure 订阅中运行。这允许客户根据需要水平扩展计算机和目录，并预置多个目录以更好地进行工作负载分类。

先决条件：

- Citrix Platform Licenses (CPL) 许可证或 RBI 专用授权，以及 DaaS 高级授权。
- 必须启用 DaaS 服务。

> **注意：**
>
> 仅当客户租户具有必要的授权时，此步骤才可能实现。

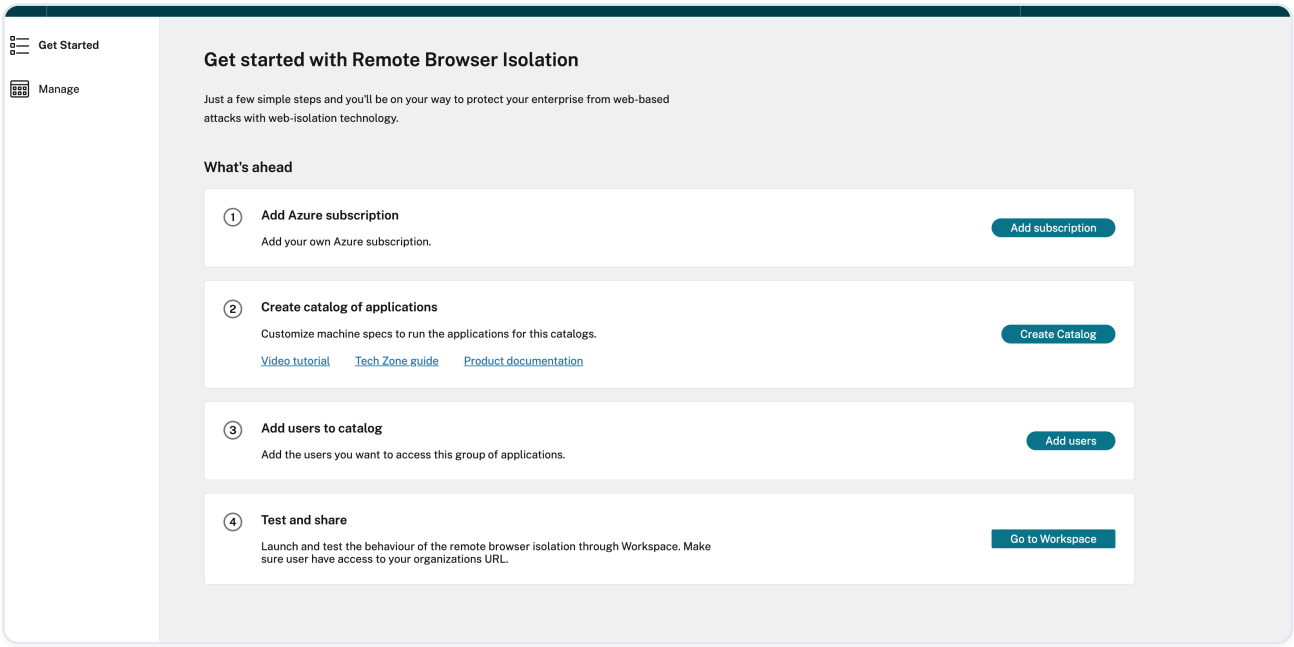
- 在 DaaS 中启用 Rendezvous 协议。

如何启用 DaaS 服务

1. 登录到 Citrix Cloud。
2. 导航到 DaaS 服务。
3. 找到并单击 **Enable DaaS**。 此步骤将为 RBI 自托管工作负载准备必要的 DaaS 基础结构，大约需要 45 分钟。

RBI 入门流程

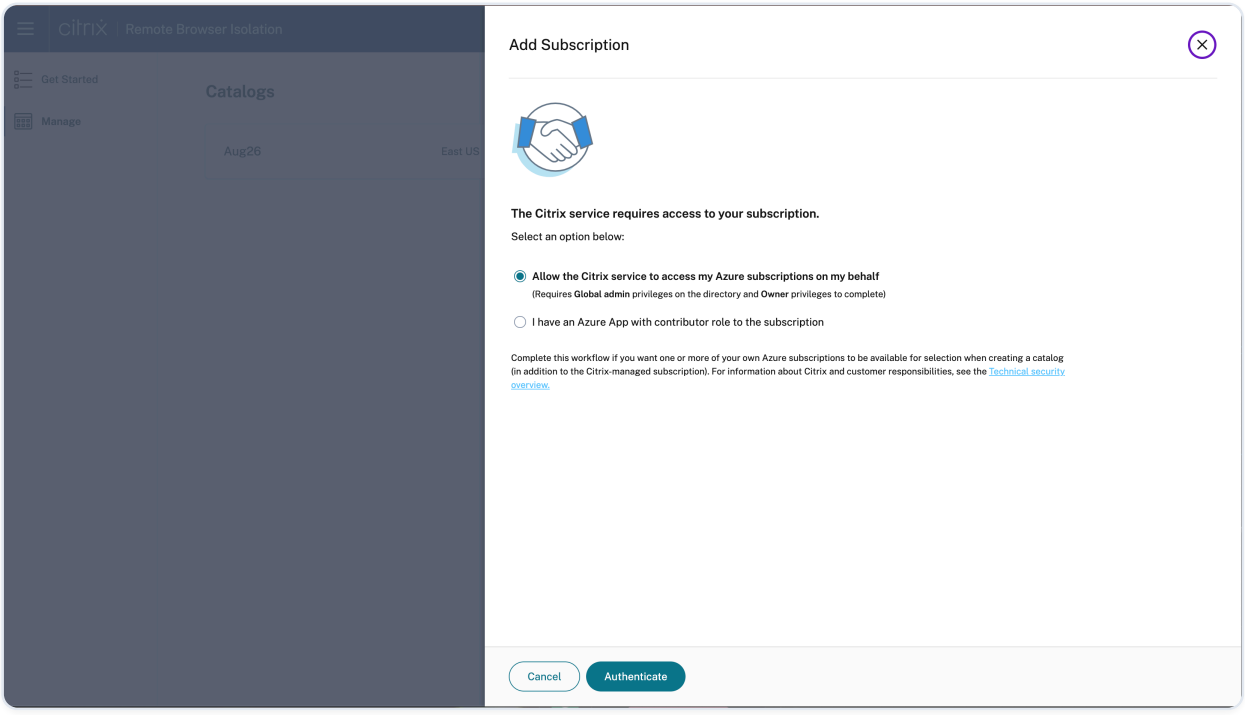
在 Citrix Cloud 页面上，单击 **Manage RBI Service** 以访问 远程浏览器隔离 登录页面。



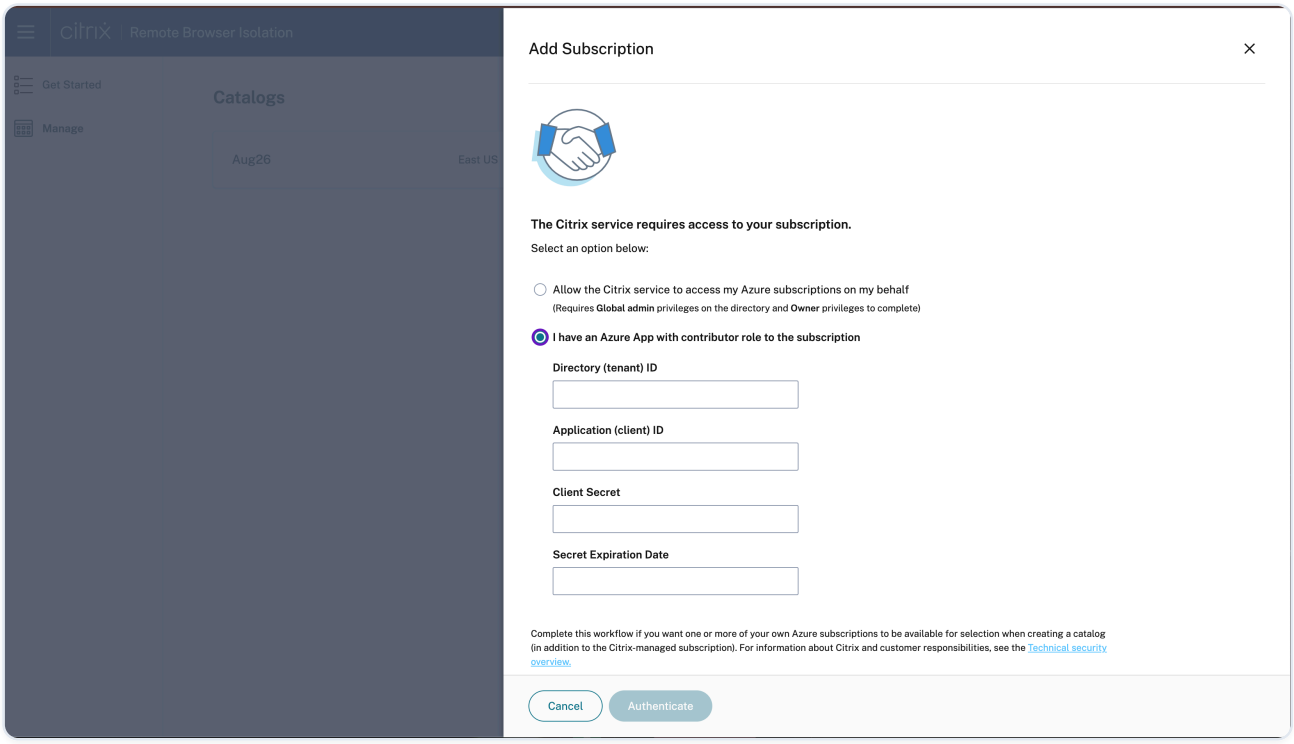
步骤 1：添加 Azure 订阅

1. 在“**远程隔离入门**”页面上，单击“**添加订阅**”。可以通过两种方式将 Azure 订阅添加到 RBI 自托管工作负载：

   - 使用全局管理员凭据：**允许 Citrix 服务代表我访问我的 Azure 订阅**。
   - 使用企业应用注册，并在整个订阅上具有参与者角色。



2. 单击“**我有一个 Azure 应用程序，对订阅具有参与者角色**”。
3. 提供**目录 ID**、**应用程序 ID**、**客户端密钥**和**密钥过期日期**以启用此选项，然后单击“**验证**”。
4. 验证订阅详细信息后，单击“**添加订阅**”。



> **注意：**
>
> 多个 Azure 订阅可以链接到 RBI 自托管工作负载。Azure 订阅可以是新的，也可以是重新利用的。RBI 自托管工作负载会创建一个虚拟网络 (VNet)，并在该边界内部署计算机。

步骤 2：创建应用程序目录

目录是浏览器应用程序的容器。您可以通过为每个组创建不同的目录来组织浏览器应用程序。 目录中的计算机在大小和设置方面是相同的，但不同目录中的计算机在大小和设置方面可能有所不同。此外，目录之间的区域也可能有所不同，这对于优化最终用户启动性能非常有用。

在新链接的订阅中创建目录大约需要 90 分钟。此过程会在 Azure 中部署必要的资源，包括用于管理计算机的资源组。

1. 在 Citrix Cloud™ 页面中，点击 **管理 RBI 服务** > **创建目录**。
2. 在 **创建远程浏览器隔离目录** 页面上，为目录命名，然后点击 **添加远程隔离浏览器**。

> **注意：**
>
> 如果选择创建目录，它将采用默认设置以进行快速部署。

3. 点击 **下一步：计算机设置** 并提供以下详细信息：

   - **订阅**
   - **计算机设置**
   - **区域**

   > **注意：**
   >
   > 默认情况下，设置电源计划是禁用的，但用户可以选择配置此项。

4. 点击 **下一步：摘要** > **创建目录**。
5. 目录创建完成后，点击 **查看详细信息**。

目录配置亮点：

- 目录创建只需单击一下即可设置客户工作负载所需的一切。
- 客户可以为计算机选择自己的电源管理周期，并在目录中发布浏览器。
- 如果客户有多个订阅，他们可以选择部署目录的位置。
- Citrix Catalog Service 管理工作负载。
- 软件补丁和更新会根据客户配置的计算机电源管理设置自动部署。
- 目录中的计算机以无连接器模式（DaaS 的 Rendezvous V2 策略）运行。这意味着客户的资源组中不需要部署连接器。

步骤 2.1：为安全私有访问 (SPA) 应用程序会话分配目录

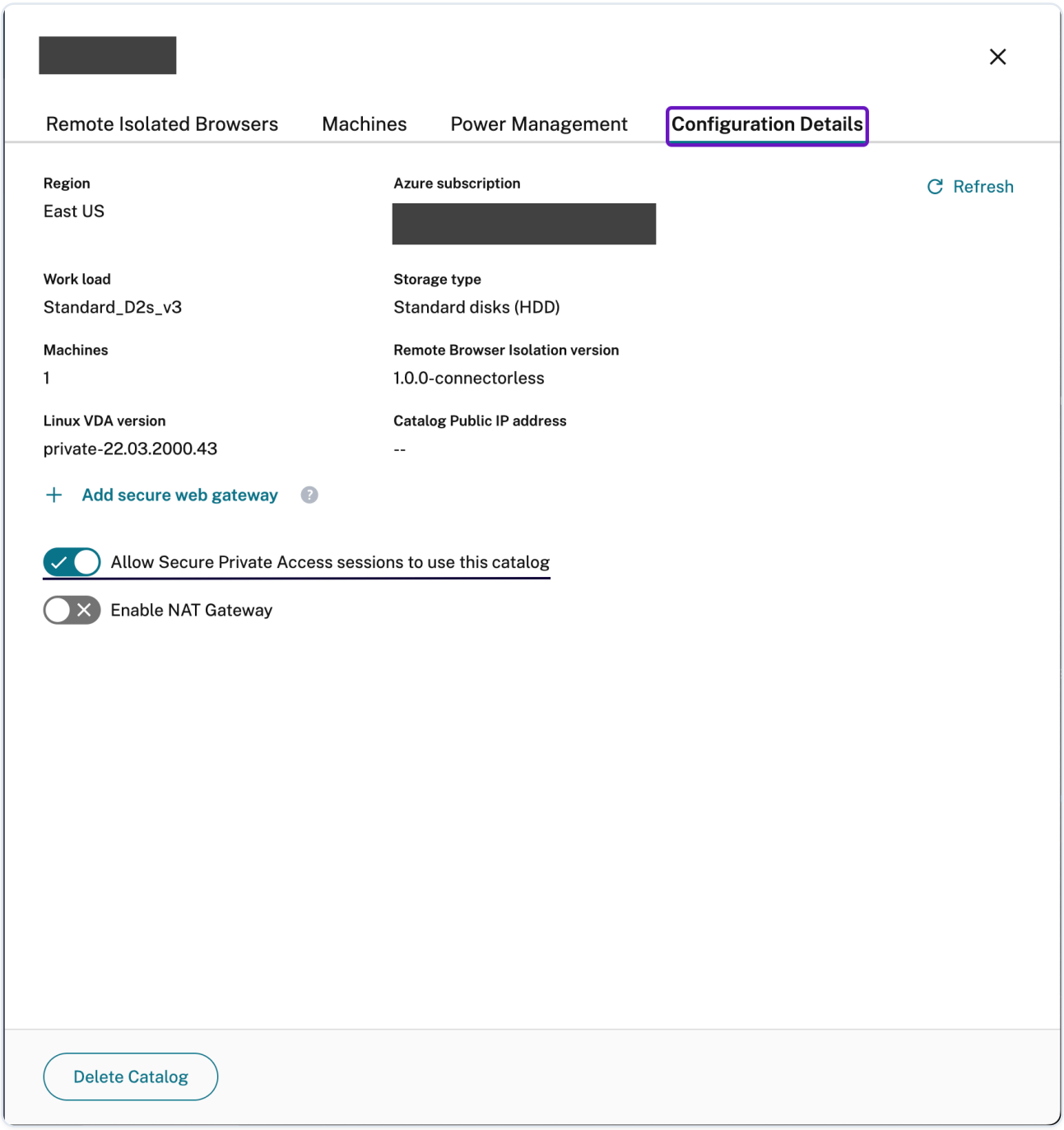
客户管理员可以选择用于 SPA 会话的目录，从而为该目的专门分配一个目录。

先决条件：

必须至少启用一个目录，此选项才能成功启动 SPA RBI 应用程序。

如何启用安全私有访问会话：

1. 在 Citrix Cloud 页面上，单击**管理 RBI 服务**。
2. 单击**管理**，导航到已创建的目录，然后单击**查看详细信息**。
3. 在**配置详细信息**页面上，启用**允许安全私有访问会话使用此目录**的切换选项。



注意：

您可以使用此选项选择多个目录。如果选择了多个目录，SPA 启动将转到距离启动请求发出地最近区域的目录。

步骤 3：发布浏览器应用程序

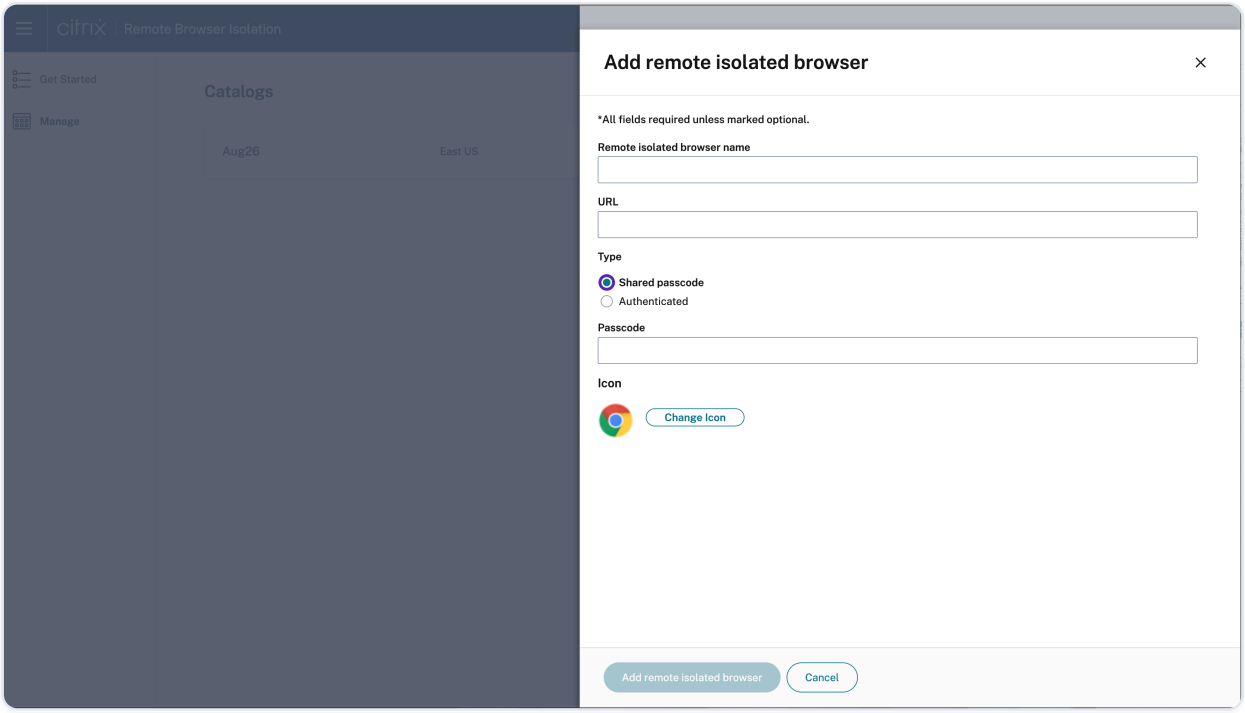
创建浏览器应用程序

按照以下步骤添加远程隔离浏览器：

1. 在 RBI 自托管工作负载控制台的“**管理**”选项卡上单击目录。
2. 单击“**添加远程隔离浏览器**”并提供以下配置详细信息：
   - **浏览器名称：** 输入您喜欢的任何名称。
   - **URL：** 指定目标应用程序 URL。

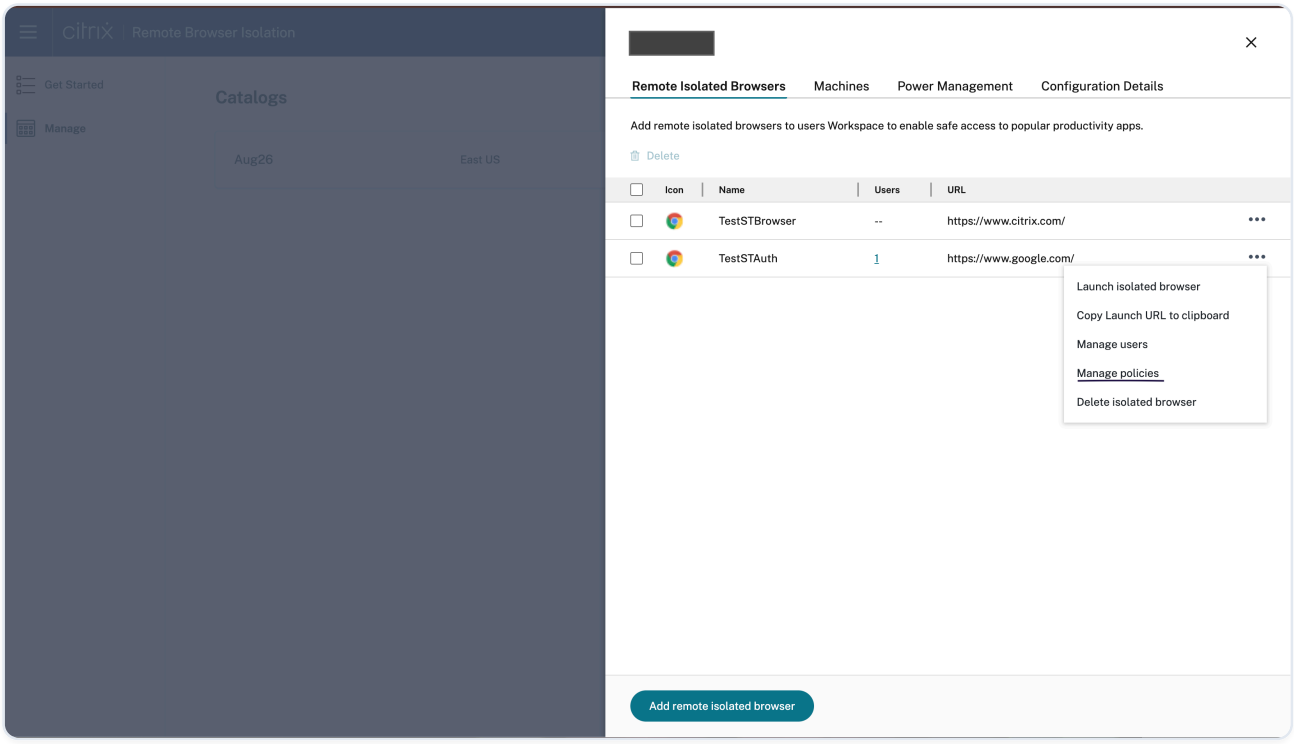
     > **注意：**
     >
     > 远程浏览器托管在安全的隔离环境中。URL 必须可通过互联网访问。

   - **类型：** 选择“**共享密码**”或“**已验证**”，这些对最终用户可见。
   - **密码** 输入密码。
   - **图标：** 上传应用程序图标。
3. 单击“**添加远程隔离浏览器**”。

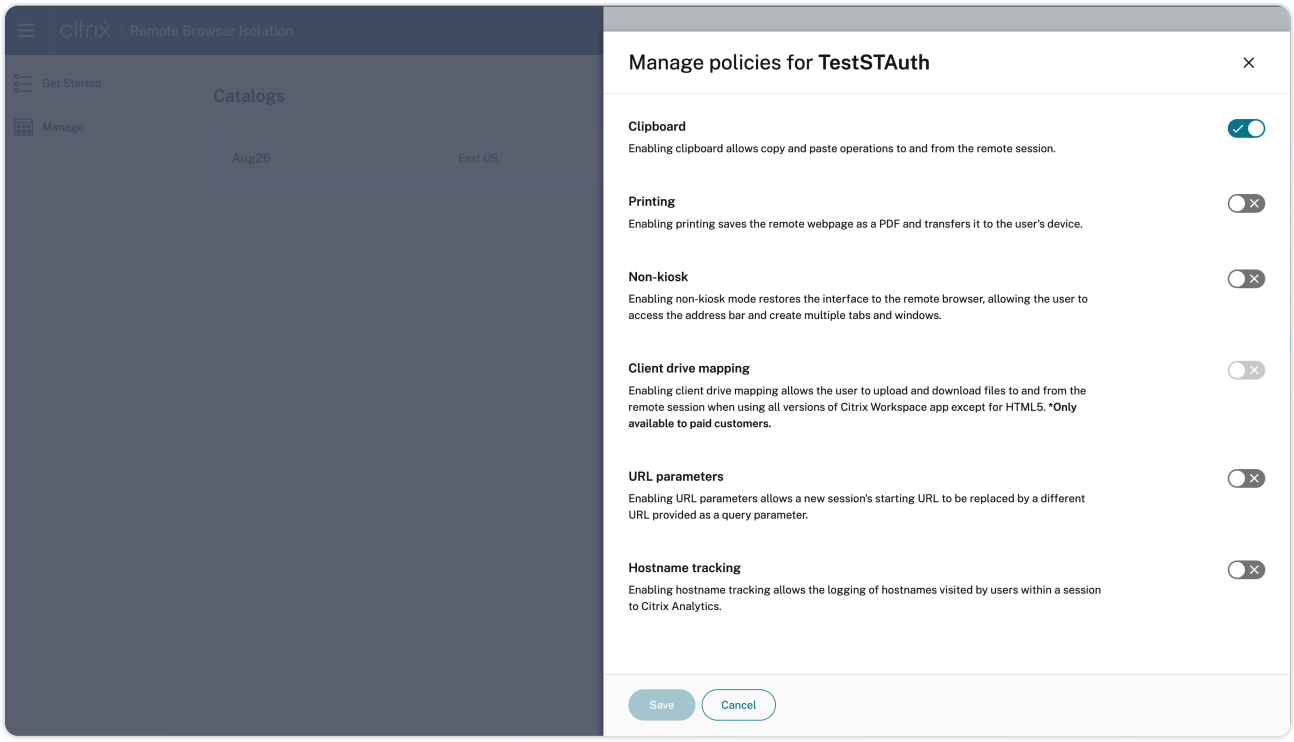


为浏览器应用程序分配策略

创建浏览器后，您可以在浏览器上配置必要的策略。

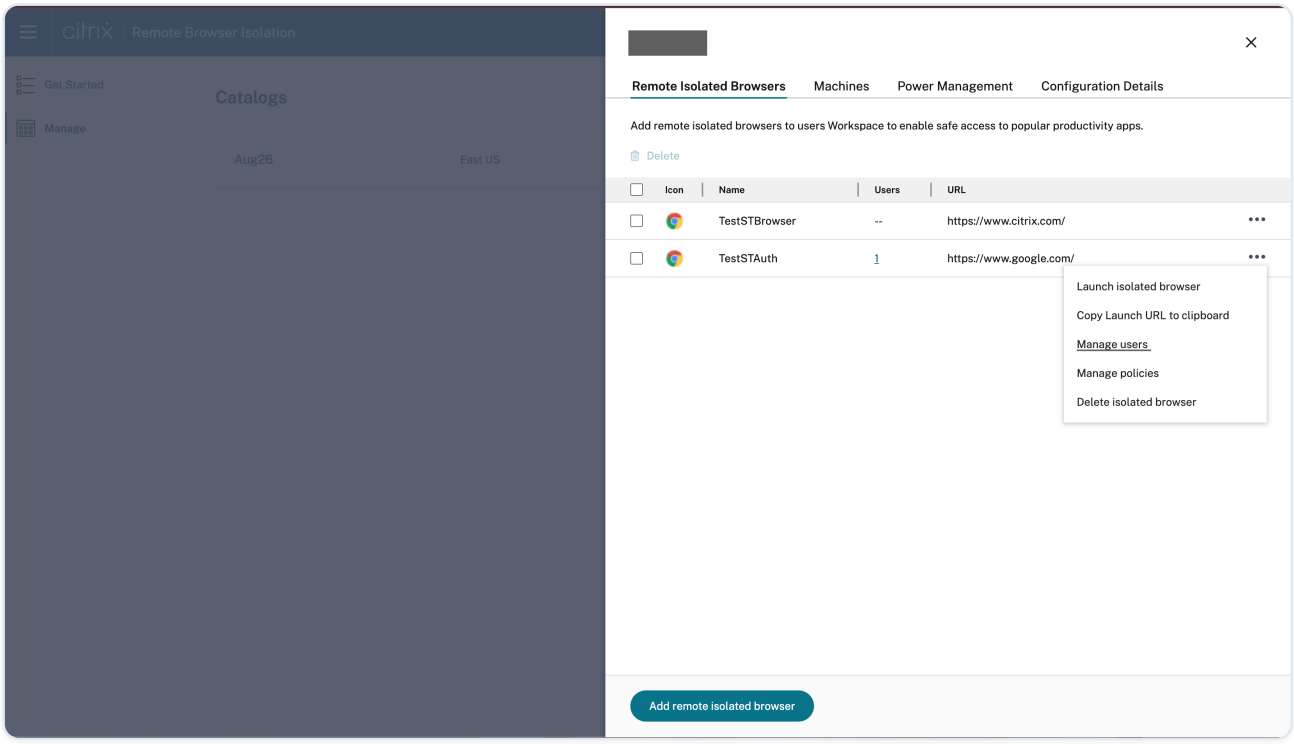


1. 单击省略号，然后单击**管理策略**。
2. 启用所需策略，然后单击**保存**。

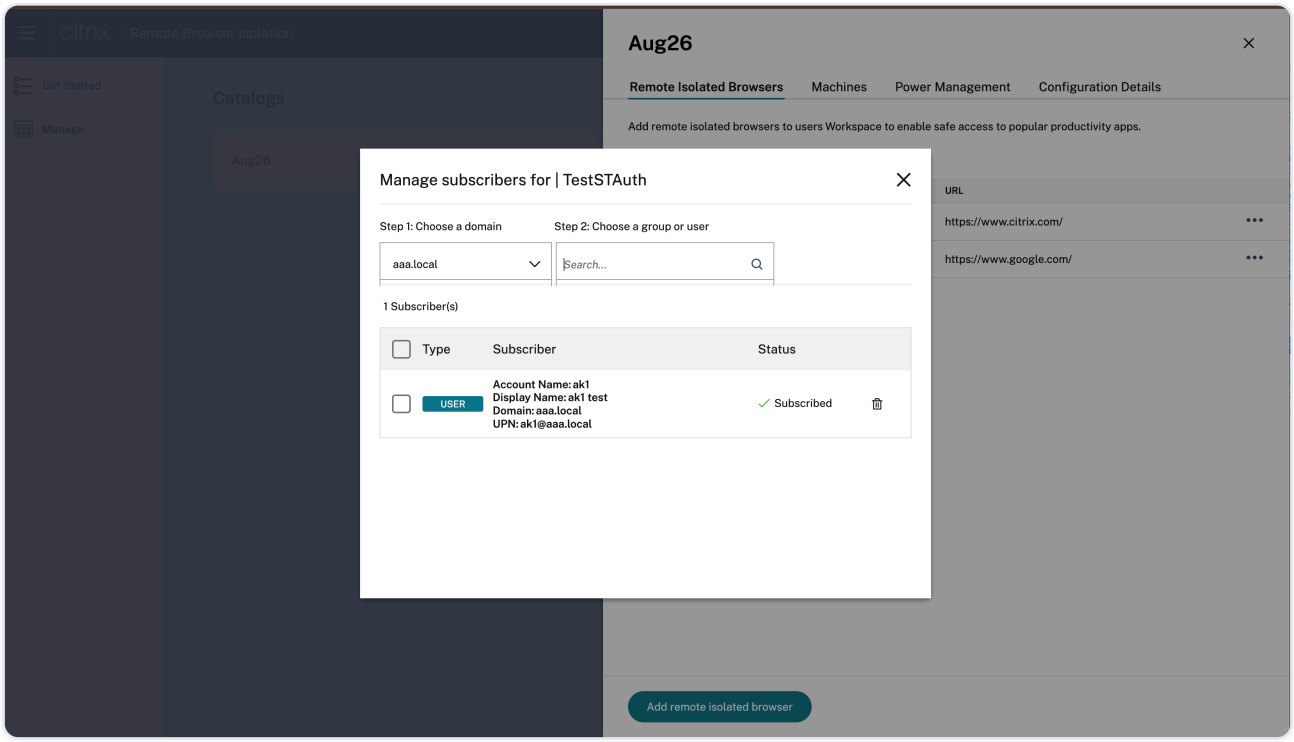


将用户添加到浏览器应用程序

客户需要引入其域和身份提供程序，以便将用户和组分配给目录中已发布的浏览器。



1. 要订阅用户，请单击省略号并选择**管理用户**。
2. 然后，选择域并从下拉菜单中选择一个组或用户。



步骤 4：测试浏览器应用程序并共享

您现在可以通过商店访问已发布的浏览器，或者直接在 Web 浏览器中打开其 URL。 启动请求将定向到您帐户中已分配目录中的计算机。

> **注意：**

> 如果尚未为目录设置计算机的电源管理，并且没有正在运行的计算机，则启动会话会触发计算机的启动，然后计算机等待准备好接受会话。

> **删除浏览器：**

选择要删除的浏览器，然后点击 **删除** 图标。

重新启动或强制重新启动计算机：

在计算机名称旁边，点击省略号，然后点击所需选项。

附加功能

用户活动日志记录

用户活动日志记录功能允许客户跟踪和审计 Citrix 远程浏览器隔离 (RBI) 会话期间的用户浏览活动。此功能捕获访问的主机名、访问时间戳、用户标识符和允许列表强制执行状态。所有收集的数据都存储在客户的 Azure 存储帐户中，这提供了完整的数据所有权和控制权。

> **重要提示：**
>
> 此功能必须在客户级别和应用程序级别同时启用。浏览活动数据每小时上传一次，并非实时。

主要优势

- **合规性和审计：** 满足企业审计要求和法规合规性标准。
- **安全分析：** 识别异常浏览模式和潜在安全威胁。
- **策略优化：** 分析用户行为以优化允许列表配置。
- **数据主权：** 在您的 Azure 环境中将数据置于您的控制之下。

先决条件

在配置用户活动日志记录之前，请确保您具备以下条件：

- 有效的 Azure 订阅。
- 用于浏览活动数据的 Azure 存储帐户。
- 在远程浏览器隔离服务下创建的目录。

配置步骤

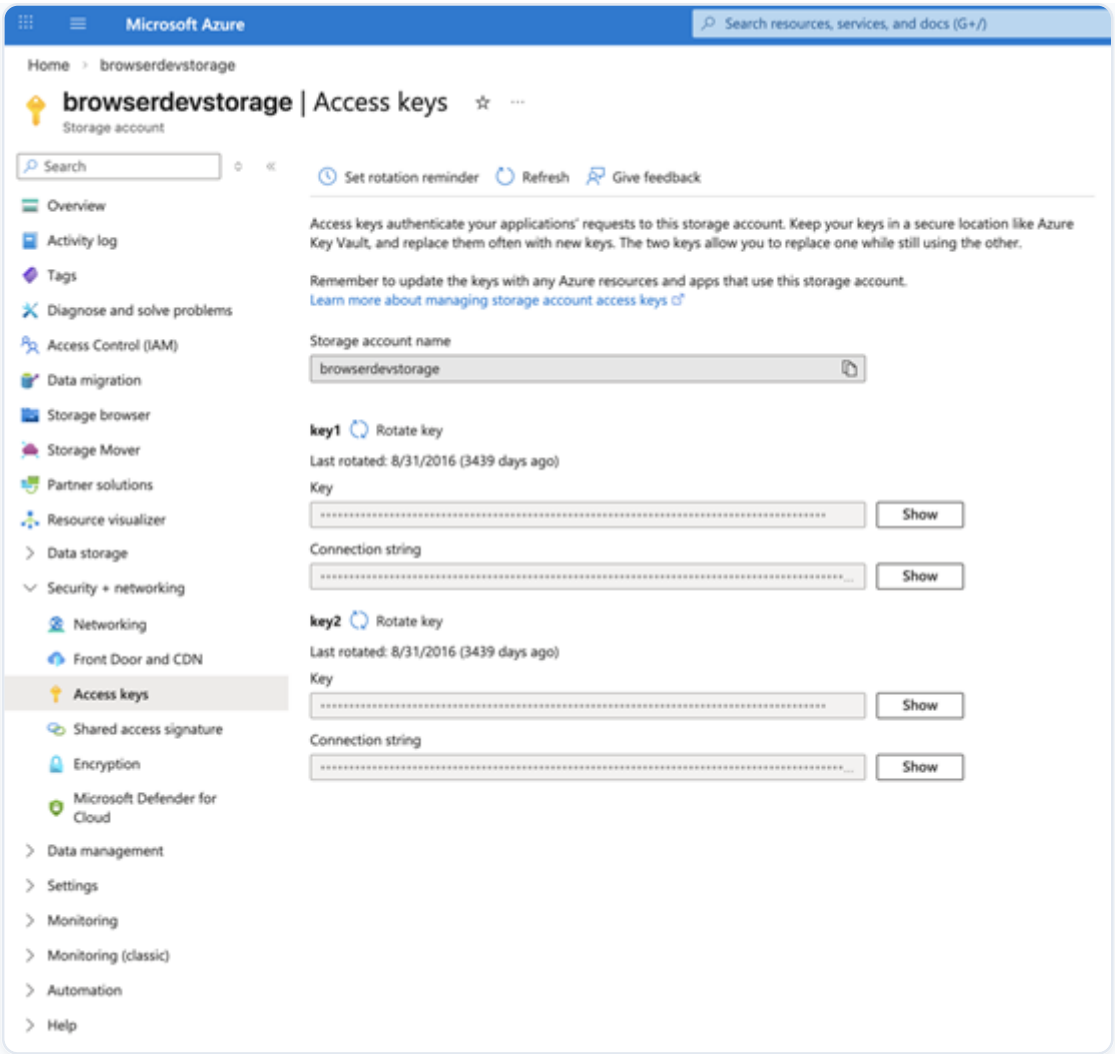
步骤 1：检索 Azure 存储连接字符串

本指南假设已存在 Azure 存储帐户。要创建一个，请参阅 Azure 存储文档。

1. 登录 Azure 门户 并打开存储帐户。
2. 在左侧菜单中，转到“**安全 + 网络**”并选择“**访问密钥**”。

3. 从 key1 或 key2 复制“**连接字符串**”。
4. 安全地存储连接字符串，以供步骤 3（验证功能是否正常工作）中使用。

> **注意：**
>
> 当您保存配置时，Citrix RBI 会自动创建一个名为 `user-activity` 的容器。无需手动创建容器。



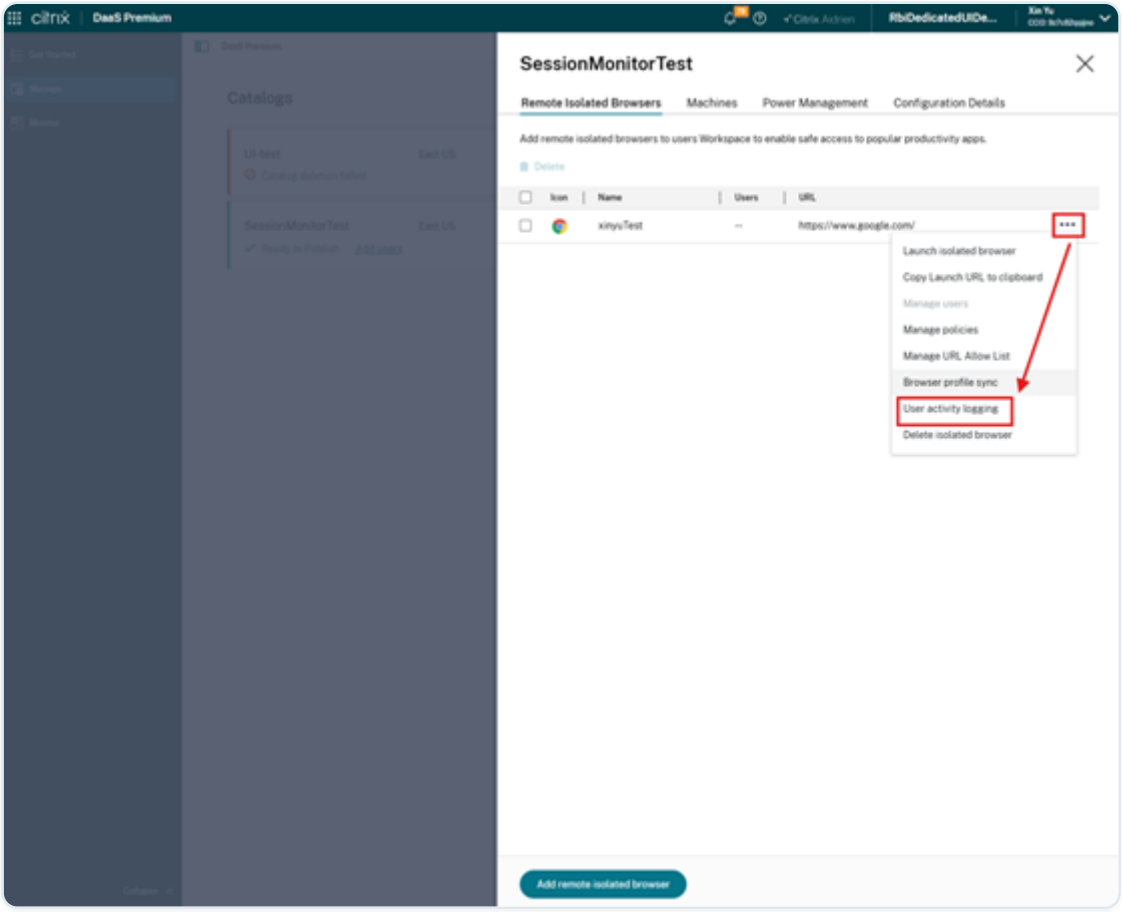
步骤 2：为应用程序配置用户活动日志记录

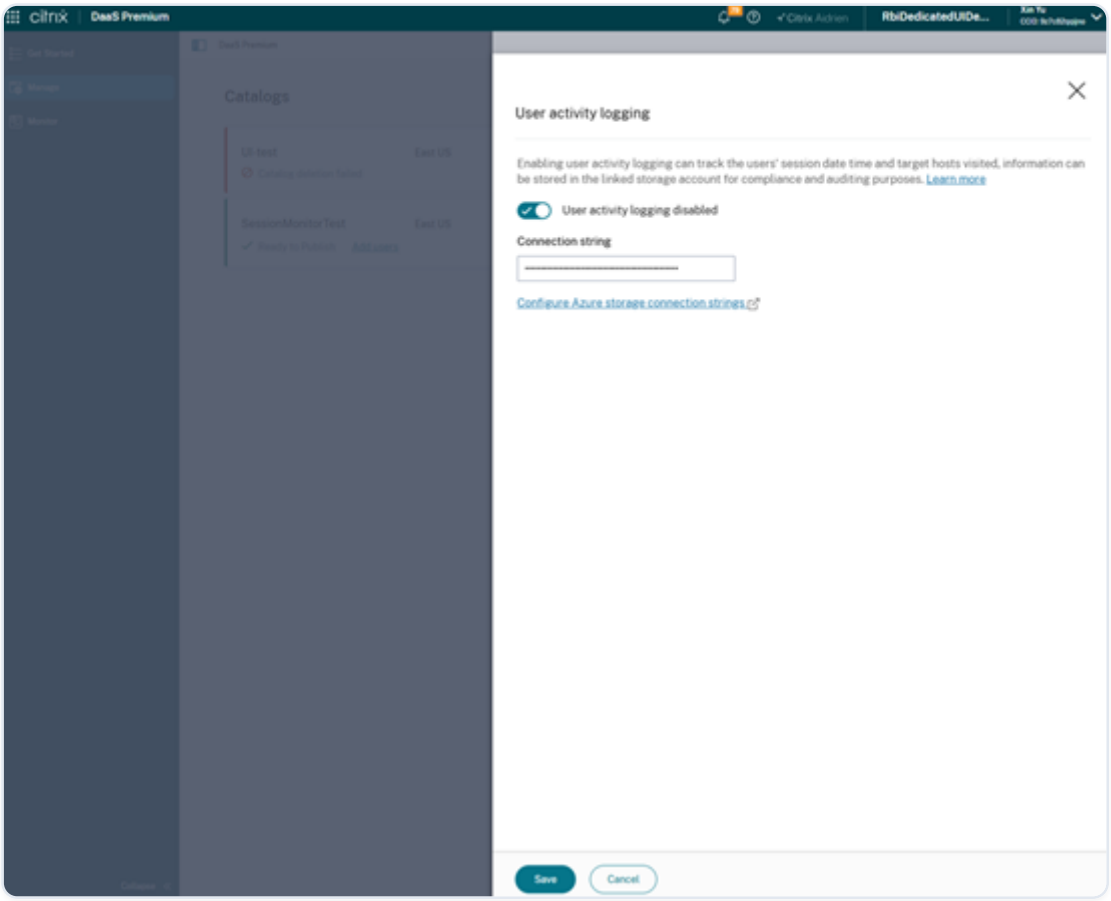
Azure 存储连接可以按应用程序进行配置。

创建或更新配置

1. 在管理控制台中，导航到“**管理**”页面。
2. 选择需要启用用户活动日志记录的目录和应用程序。

3. 找到**用户活动日志记录**设置。
4. 启用**用户活动日志记录**。
5. 粘贴步骤 1 中的 Azure 存储连接字符串。
6. 单击**保存**。





保存配置后，系统将执行以下操作：

- 验证连接字符串。
- 检查与 Azure 存储的连接。
- 如果容器不存在，则创建名为 `user-activity` 的容器。
- 确认连接权限。

删除配置

要停止跟踪特定应用程序的浏览活动，请执行以下操作：

1. 导航到该应用程序的设置页面。
2. 找到**用户活动日志记录**设置。
3. 禁用 **用户活动日志记录**。
4. 单击 **保存**。

删除配置后，新启动的用户会话不再记录浏览活动。已上传到 Azure 存储的历史数据不会被删除。

步骤 3：验证功能是否正常工作

配置完成后，验证该功能：

1. 使用配置了用户活动日志记录的应用程序启动新的浏览器会话。
2. 访问多个网站，例如 `www.google.com` 和 `www.microsoft.com`。
3. 等待上传。浏览活动首先保存在本地，然后每小时上传一次。
4. 对于初始验证，请至少等待 1-2 小时。
5. 在 Azure 门户中，打开存储帐户，然后打开 `user-activity` 容器。
6. 验证是否出现新的 JSON 文件。
7. 下载一个 JSON 文件并确认其中包含所访问网站的主机名。

查看和分析浏览活动

数据存储结构

浏览活动数据在 Azure Blob 存储中按日期和文件名组织：

```
Container: user-activity

|- YYYY-MM-DD/

|  |- {VDAHostname}_{GUID}_{AppName}_{YYYY-MM-DD-HH}.json

|  |- {VDAHostname}_{GUID}_{AppName}_{YYYY-MM-DD-HH}.json

|  `- {VDAHostname}_{GUID}_{AppName}_{YYYY-MM-DD-HH}.json

`- YYYY-MM-DD/

    `- ...
```

文件命名约定

- 文件夹结构：`{YYYY-MM-DD}/`（按日期组织）。
- 文件名模式：`{VDAHostname}_{GUID}_{AppName}_{YYYY-MM-DD-HH}.json`
- `{VDAHostname}`：VDA 计算机的主机名。
- `{GUID}`：每个上传批次的唯一标识符。
- `{AppName}`：安全浏览器应用程序的名称。
- `{YYYY-MM-DD-HH}`：24 小时格式的上传时间戳。

每个活动的 VDA 每小时都会生成新文件。

数据格式说明

每个 JSON 文件都包含 NDJSON 格式（换行符分隔的 JSON）的多个记录。每行代表一个访问事件。


```
{"accessHostEvent":
{"hostName":"www.google.com","acceptHost":true},"accessTime":"2026-01-29T1
4:23:45.123Z","sessionId":"abc123-def456-
ghi789","userName":"user@example.com","appName":"MySecureBrowser"}

{"accessHostEvent":
{"hostName":"www.microsoft.com","acceptHost":true},"accessTime":"2026-01-2
9T14:25:10.456Z","sessionId":"abc123-def456-
ghi789","userName":"user@example.com","appName":"MySecureBrowser"}

{"accessHostEvent":
{"hostName":"malicious.site","acceptHost":false},"accessTime":"2026-01-29T
14:30:22.789Z","sessionId":"abc123-def456-
ghi789","userName":"user@example.com","appName":"MySecureBrowser"}
```


字段说明

字段	说明	示例
`accessHostEvent.hostName`	用户访问的网站主机名。	`www.google.com`
`accessHostEvent.acceptHost`	访问是否由允许列表允许（`true` 表示允许，`false` 表示阻止）。	`true`
`accessTime`	访问时间戳 (UTC)。	`2026-01-29T14:23:45.123Z`
`sessionId`	唯一会话标识符。	`abc123-def456-ghi789`
`userName`	用户标识符。	`user@example.com`
`appName`	应用程序名称。	`MySecureBrowser`

隐私保护： 系统仅记录主机名，例如 `www.example.com`。它不记录完整的 URL 路径、查询参数或用户输入的内容。

查看数据的方法

使用以下方法查看浏览活动记录：

Azure 存储资源管理器

1. 下载并安装 Azure 存储资源管理器。
2. 连接到 **存储帐户**。
3. 浏览 `user-activity` 容器。
4. 下载 `JSON` 文件并查看其内容。

Azure 门户

1. 登录到 **Azure** 门户。
2. 导航到 **存储帐户**。
3. 选择 **容器** > `user-activity`。
4. 下载文件以查看其内容。

提示：为了进行更深入的分析，请将数据导入 Excel、Power BI 或其他分析工具。

主要功能和注意事项

功能亮点

- **自动记录：** 无需手动干预即可捕获网站访问事件。
- **包含被阻止的尝试：** 捕获被阻止的访问尝试 (`acceptHost: false`)，用于允许列表分析。
- **每小时上传：** 每小时批量上传数据以减少网络开销。
- **数据主权：** 将所有数据存储在客户的 Azure 环境中。
- **多应用程序支持：** 支持跨应用程序的独立或共享存储帐户配置。

限制

- **非实时：** 数据可能需要长达一小时才能在 Azure 存储中显示。
- **仅限专用版：** 仅适用于专用版应用程序。
- **固定容器名称：** 容器名称为 `user-activity` 且无法自定义。
- **VDA 重启影响：** 如果 VDA 在上传前重启，尚未上传的数据可能会丢失。

故障排除

问题 1：Azure 存储中没有数据

可能的原因：

- 功能开关未启用。
- 连接字符串不正确或已过期。
- 等待时间不足（至少需要一小时）。
- 应用程序不是专用版。

解决方案：

1. 检查功能开关状态。
2. 重新配置连接字符串并保存。
3. 启动新会话，访问网站，并等待 1-2 小时。
4. 确认应用程序是专用版。
5. 验证 `user-activity` 容器是否已创建。

问题 2：配置连接字符串时验证失败

可能的原因：

- 连接字符串格式不正确。
- 存储帐户网络限制阻止访问。
- 创建容器的权限不足。

解决方案：

1. 从 Azure 门户再次复制完整的连接字符串。
2. 检查存储帐户防火墙设置。为了测试，请暂时允许更广泛的网络访问。
3. 验证连接字符串是否授予了容器创建权限。
4. 确保存储帐户未被锁定或以其他方式受限。

问题 3：数据上传后用户会话中断或变慢

不会，数据上传在后台运行，不会中断正常的浏览器使用。上传使用异步 I/O，资源消耗极少。

问题 4：配置是否立即对活动用户会话生效?

不会，用户必须关闭当前会话并启动新会话才能应用更新的设置。活动会话将继续使用启动时存在的配置。

问题 5：多个应用程序可以使用同一个存储帐户吗?

是的，多个应用程序可以共享同一个存储帐户和 `user-activity` 容器。文件命名和 `appName` 字段有助于区分应用程序之间的数据。

与 Chrome 企业高级版 (CEP) 集成

本主题介绍了 Citrix Remote Browser Isolation (RBI) 与适用于 Linux VDA 的 Google Chrome Enterprise Premium (CEP) 之间的集成。它解释了此功能的作用、工作原理以及管理员在启用之前必须了解的内容。

简介

Google Chrome Enterprise Premium (CEP) 为企业环境提供高级安全性、浏览器管理和策略实施。借助此功能，Citrix RBI 浏览器可以使用 Google 注册令牌注册到 Chrome Enterprise 策略中。管理员随后可以从 Google Admin console 集中管理组织和部门的安全浏览器策略。

此集成提供了一种可扩展的云管理方法，可在无需 EDR 代理的情况下，对不受信任的端点设备强制执行安全性和合规性。

此功能的作用

借助 CEP 集成：

管理员可以：

- 将 Chrome Enterprise 策略应用于同一目录中的所有 Citrix RBI 浏览器用户。
- 通过 Google Admin console 集中管理这些策略。

用户可以：

- 使用在注册后成为托管浏览器的 RBI 浏览器。
- 接收一致的企业策略，例如复制和粘贴控制以及 URL 阻止列表。
- 从 Google Cloud 接收自动策略更新。

如何使用

准备工作

在启用 CEP 集成之前：

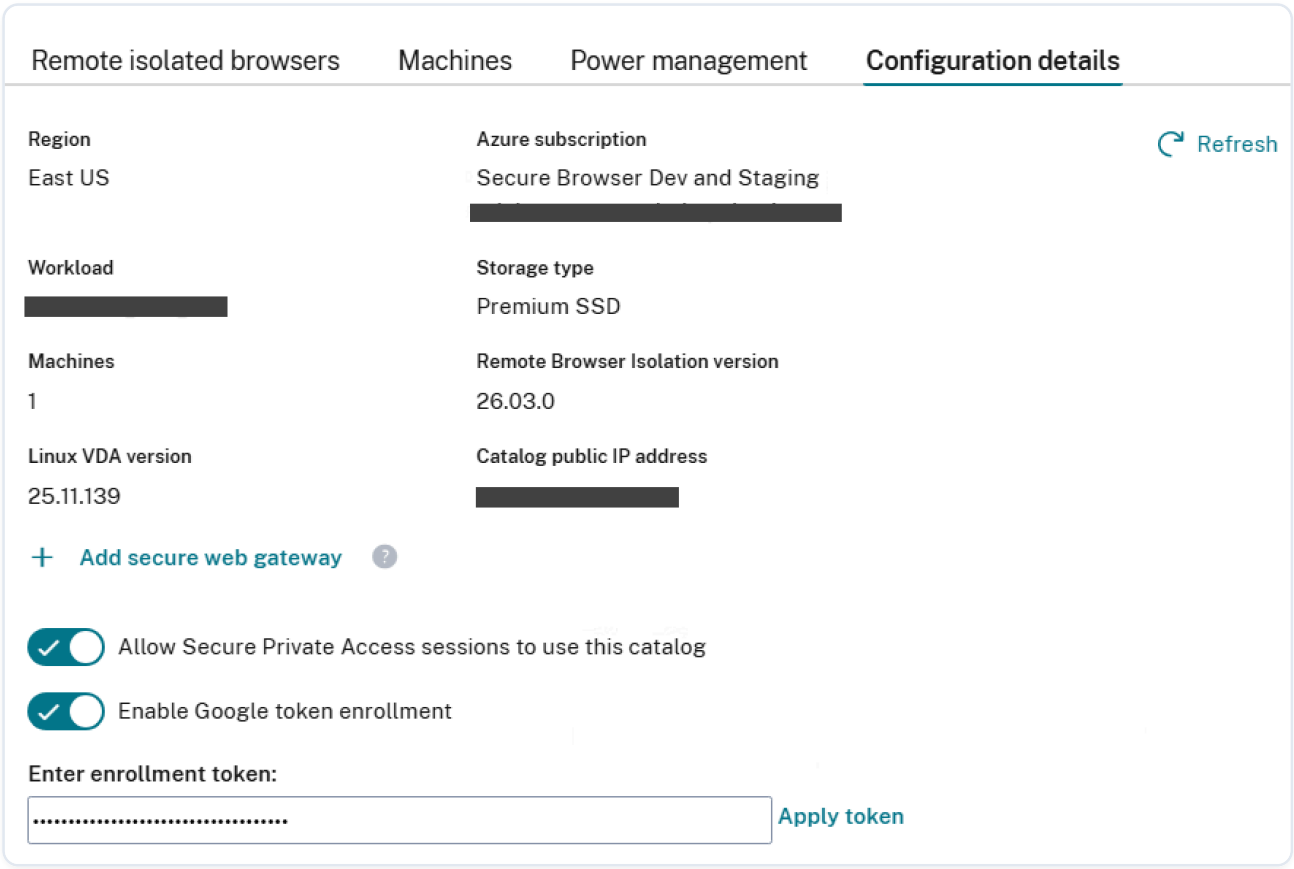
1. 确认 Google 工作区 支持 Chrome 企业高级版。
2. 确保至少存在一个 Citrix RBI 目录。如果不存在，请创建一个。
3. 确定哪些 RBI 目录必须受 Chrome 策略管理。
4. 如有需要，在 Google 管理控制台中为每个组织单位 (OU) 生成一个注册令牌。

Citrix Cloud 门户上的配置

CEP 要求每个目录都有一个注册令牌。Citrix 会自动将令牌分发给从该目录启动的用户会话。

注册流程

1. 从 Google 管理控制台获取注册令牌。
2. 登录 Citrix Cloud 并导航到“远程浏览器隔离”。
3. 在左侧菜单中选择 **管理**。
4. 选择目标目录，然后打开 **配置详细信息**。
5. 启用 **启用 Google 令牌注册** 并输入注册令牌。
6. 选择 **应用令牌**。



当用户在该目录中启动安全浏览器应用程序时，令牌注册会自动发生，并且浏览会在已注册 CEP 的浏览器中继续。

管理员任务

- 禁用或重新启用 **启用 Google 令牌注册**，或更新注册令牌。
- 使用 `chrome://policy` 监控 Chrome 策略执行。
- 定期查看 Google 管理员设备列表并删除过时记录。

限制和已知行为

不支持用户配置文件同步

Chrome 用户配置文件云同步在 CEP 令牌注册的 RBI 浏览器中不起作用。

每次配置更改都需要重新启动

由于 RBI 使用临时文件系统，如果管理员启用或禁用 CEP 集成，或更新 CEP 令牌，则需要重新启动。

允许列表策略行为

如果目录下的 RBI 浏览器应用程序配置的允许列表从默认的 `*:*` 修改，请包含 `*.google.com:*` 以完成 CEP 注册。CEP 启动后，RBI 允许列表策略将不被遵守。

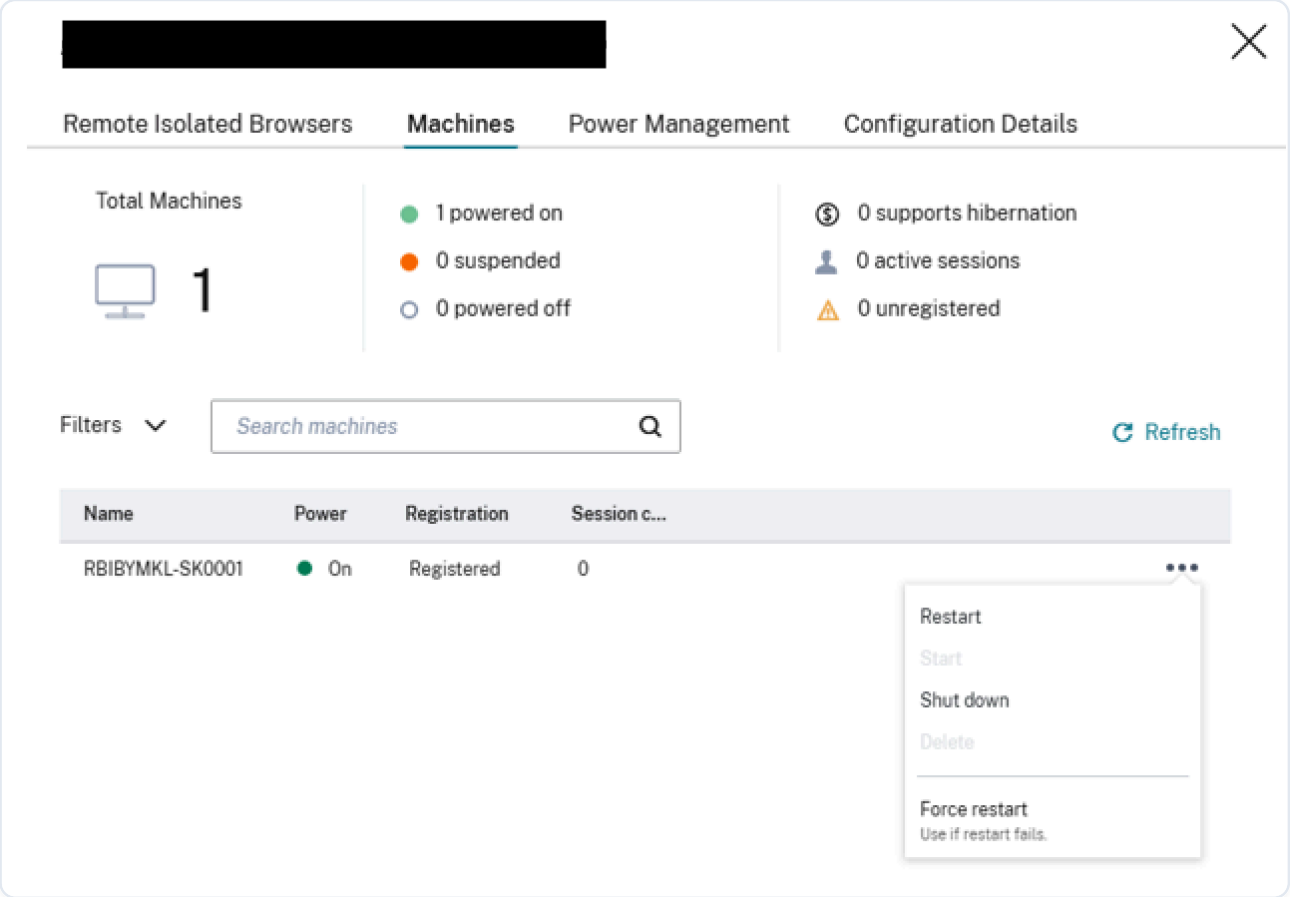
Google 管理员可能会显示重复设备

映像升级后，计算机可能会收到新的 ID。这可能会在 Google 管理控制台中创建额外的设备记录。

重新启动目录中的计算机

对于目录中列出的每台计算机：

1. 选择右侧的菜单。
2. 选择 **重新启动**。



配置用于客户管理的 RBI 目录虚拟网络的 Azure 防火墙

Azure 防火墙使您能够筛选远程浏览器隔离服务中目录计算机的传出 Web 请求。通过在现有 Azure 虚拟网络中部署 Azure 防火墙，您可以控制和监视出站流量。这有助于您增强网络安全性并管理工作负载的出站连接。

先决条件：

- 在您的 Azure 订阅中，在远程浏览器隔离服务下创建的目录。
- 创建和管理 Azure 资源的足够权限。

查找 Azure 虚拟网络

1. 在 **Citrix Cloud DaaS** 控制台中，识别您要保护的计算机目录。
2. 从目录中选择一台计算机，并复制其名称的第一部分（例如，RBI3BLR6-O80001）。
3. 在 Azure 门户中，使用此名称搜索 VM。
4. 在 VM 的概述中，选择**链接的虚拟网络**。

创建 Azure 防火墙

1. 在虚拟网络的菜单中，在 **设置** 下选择 **子网**。
2. 添加新子网，并将用途设置为 **Azure 防火墙**（使用默认设置）。
3. 返回虚拟网络概述，然后在**功能**下选择 **Azure Firewall**。
4. 单击**添加新防火墙**。
5. 填写以下字段：
   - **订阅**和**资源组**：根据需要选择。
   - **名称**：输入防火墙的名称。
   - **区域**：与虚拟网络的区域匹配。
   - **防火墙层**：选择**标准**。
   - **虚拟网络**：选择步骤 1 中确定的网络。
   - **防火墙策略**：选择**使用防火墙策略管理此防火墙**。
   - **策略名称**：单击**添加新项**并输入名称（例如，Test-policy）。
   - **防火墙管理 NIC**：禁用此设置。
6. 检查您的设置并创建防火墙。

配置路由

1. 部署后，打开 Azure 防火墙资源并记下其私有 IP 地址。
2. 在 Azure 门户中，导航到您的虚拟网络并选择**子网**。
3. 识别目录 VM 所在的子网（通常命名为 default）。
4. 创建新的路由表，或选择与此子网关联的现有路由表。
5. 添加新路由：
   - **目标**：`0.0.0.0/0`
   - **下一跳类型**：`Virtual appliance`

- **下一跳地址**：输入 Azure 防火墙的私有 IP 地址。

6. 保存路由。

配置防火墙规则

1. 在 Azure 门户中，转到“**防火墙管理器 > Azure 防火墙策略**”。
2. 选择您创建的策略（例如，Test-policy）。
3. 转到 **Rules**。
4. 添加新的**应用程序规则集合**（建议用于 Web 筛选）。
5. 定义规则以允许或拒绝特定的 FQDN 或 URL 类别。例如，要拒绝访问 `www.example.com`：
   - **名称**：`DenyExampleWebsite`
   - **源 IP 地址**：目录 VM 的子网范围。
   - **目标 FQDN**：`www.example.com`
   - **协议**：`http:80`、`https`
   - **操作**：`Deny`
6. 保存规则集合。
7. 根据需要添加额外的允许或拒绝规则，并相应调整优先级。（可选）

测试配置

1. 从配置的目录中的计算机启动浏览器会话。
2. 尝试访问允许和阻止的网站，以确认访问控制正常工作。
3. 验证防火墙是否根据定义的规则正确过滤网络流量。

故障排除

如果遇到问题，请参阅 Azure 防火墙文档。

限制

同一目录中的所有浏览器都使用相同的防火墙、策略和规则。

软件升级和补丁管理

Citrix 创建并管理计算机映像和目录，包括软件管理。当新版本的目录可用时，Citrix 会将这些升级推送到客户目录，确保客户的计算机在下次重新启动时收到最新的修复和补丁。RBI 使用 DaaS 目录服务来促进客户订阅中的这些升级。

与 Citrix® StoreFront Cloud 集成

远程浏览器隔离可以与 StoreFront Cloud 集成。为确保其已集成：

1. 登录到 Citrix Cloud。
2. 在左上角菜单中，选择 **StoreFront Cloud**。
3. 选择 **服务集成** 选项卡。
4. 确认远程浏览器隔离服务条目显示为 **已启用**。如果未显示，请单击省略号菜单并选择 **启用**。

如果尚未配置，请按照 配置对商店的身份验证 中的说明，为您的商店配置商店 URL、外部连接和商店身份验证。

远程浏览器隔离支持使用 Active Directory 和 Microsoft Entra ID 进行身份验证。默认情况下，已配置使用 Active Directory 进行身份验证。有关使用 Microsoft Entra ID 配置身份验证的信息，请参阅 将 Microsoft Entra ID 连接到 Citrix Cloud。

如果使用 Microsoft Entra ID 配置身份验证，则包含 Active Directory 域控制器的本地域必须包含一个（最好是两个）Cloud Connector。

与您的本地 StoreFront 集成

拥有本地 StoreFront 的 Citrix Virtual Apps and Desktops™ 客户可以轻松与远程浏览器隔离服务集成，以提供以下优势：

- 将您发布的远程隔离浏览器与现有 Citrix Virtual Apps™ 和 Desktops 应用程序聚合，以获得统一的商店体验。
- 使用本机 Citrix Receiver 增强最终用户体验。
- 通过使用与 StoreFront 集成的现有多重身份验证解决方案，加强远程浏览器隔离启动的安全性。

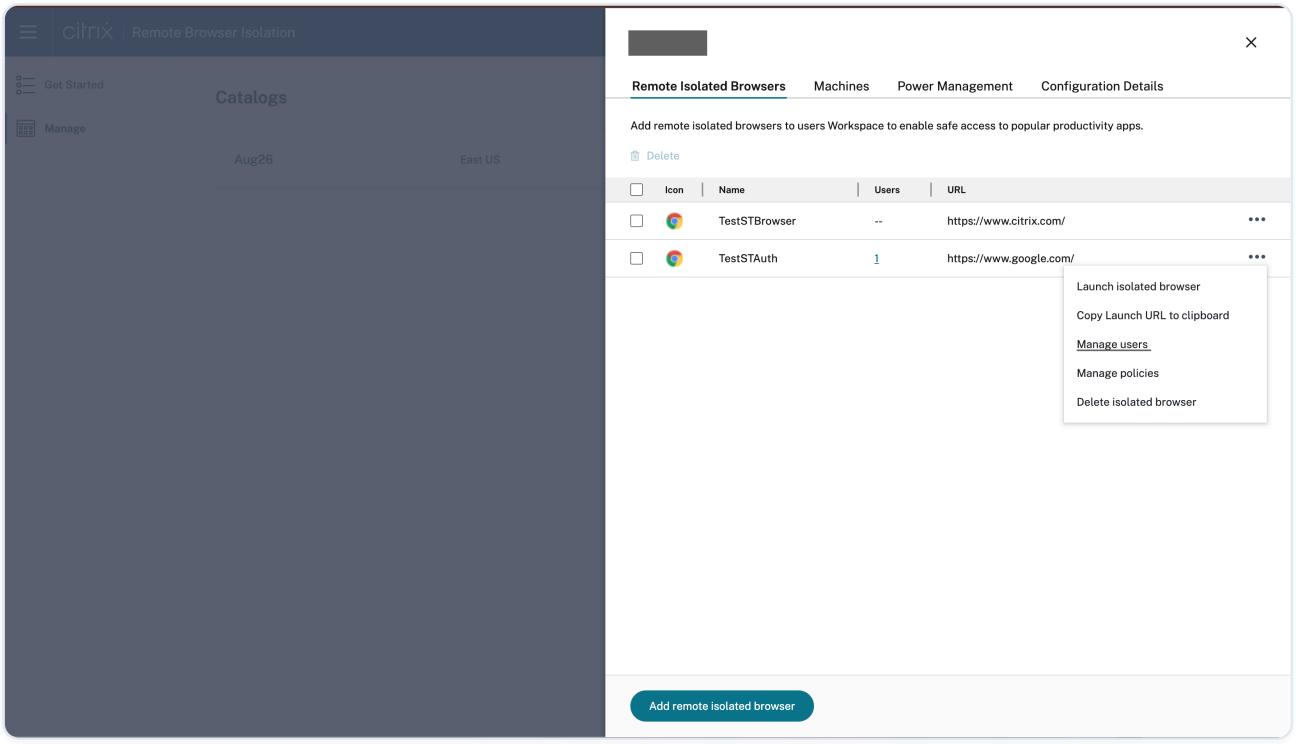
有关详细信息，请参阅 CTX230272 和 StoreFront 配置文档。

管理和监控远程隔离浏览器

您可以管理已发布的浏览器的策略和其他配置，并监控远程浏览器隔离中的活动用户会话。

管理

“**管理**”选项卡列出了现有的远程浏览器隔离 (RBI) 目录。您可以选择现有目录来更新已发布浏览器的配置。单击已发布浏览器右侧的**省略号**，然后选择所需任务。

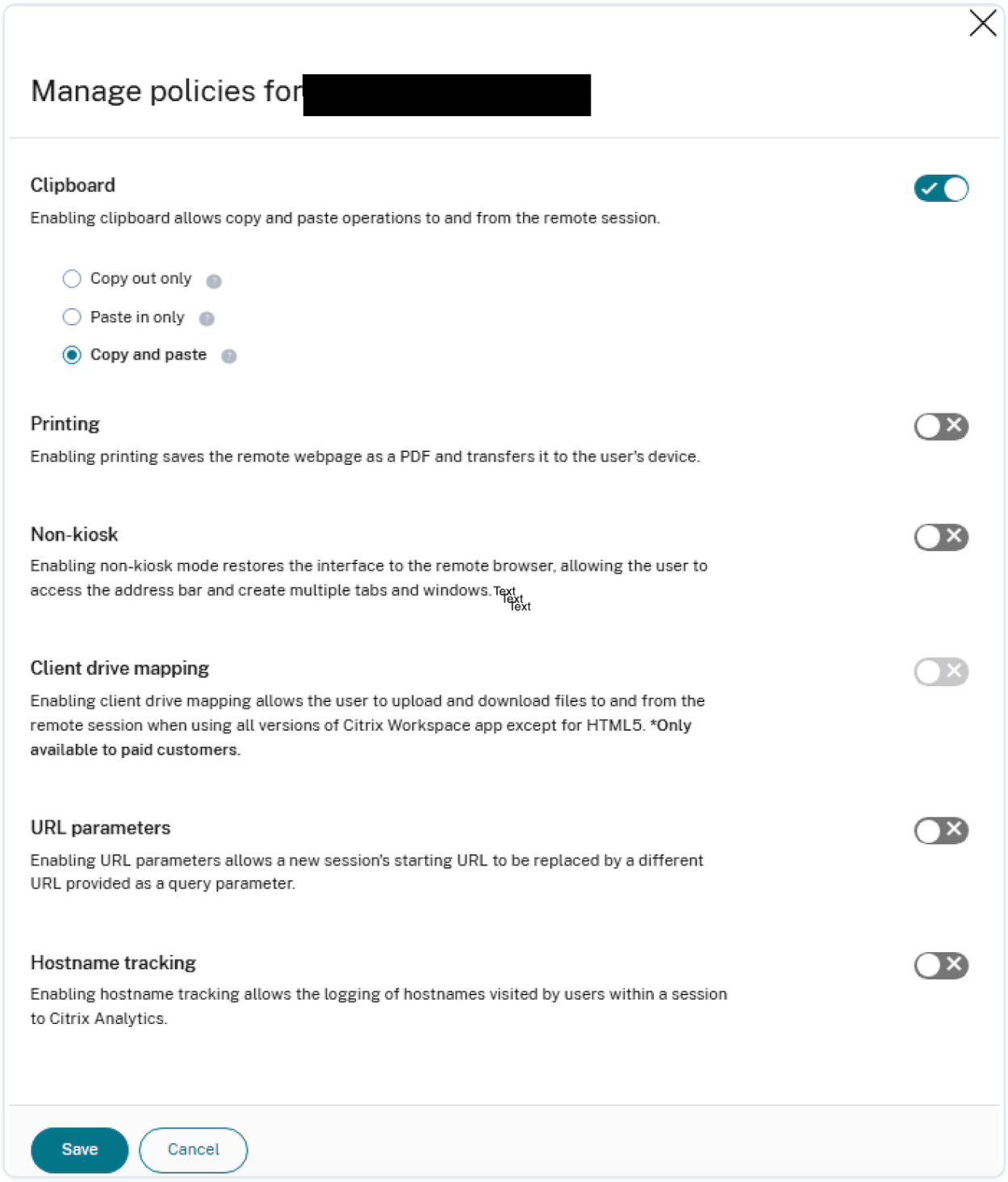


如果您选择了一个菜单项，然后决定不进行任何更改，请单击对话框外部的 **X** 取消选择。



您可以使用以下任务管理已发布的隔离浏览器：

- **启动已发布的浏览器：** 打开已发布的浏览器会话。发布浏览器后，您可以选择此任务来验证已发布的浏览器会话的启动。
- **将 URL 复制到剪贴板：** 复制已发布的浏览器的 URL。您可以与最终用户共享此 URL 以访问已发布的浏览器。
- **策略：** 您可以为已发布的浏览器设置策略。



策略页面上的设置控制以下内容：

- **剪贴板：** 启用剪贴板策略允许复制和粘贴操作有三个选项：

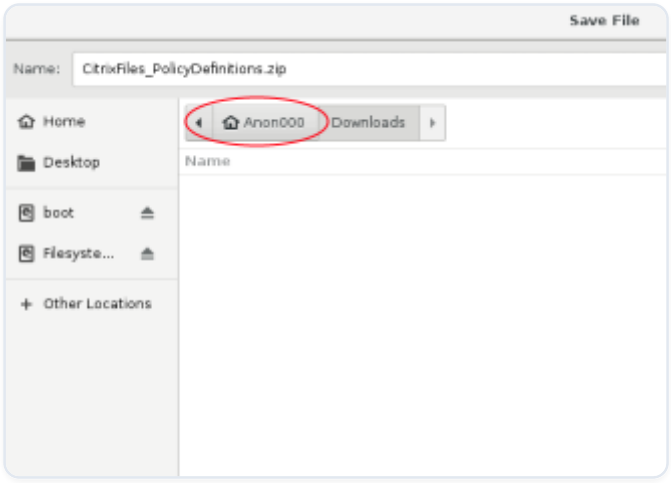
- **仅复制出：** 用户可以将内容从 RBI 会话复制到本地设备，但禁止粘贴到 RBI 中。
- **仅粘贴：** 用户可以将内容粘贴到 RBI 会话中，但禁止复制出内容。
- **复制和粘贴：** 完全双向剪贴板访问。

禁用剪贴板策略开关会从 Citrix Workspace™ 应用程序工具栏中移除剪贴板按钮。

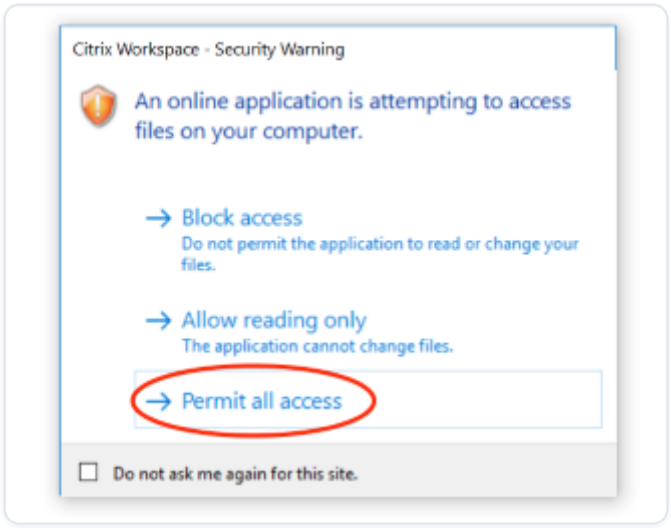
这些精细的策略选项使管理员能够对远程会话和用户端点之间的数据流进行细粒度控制。例如，组织可以允许用户从远程浏览器复制文本以供参考，同时阻止粘贴操作到会话中，以降低数据注入的风险。

> **注意：**
>
> 对于已启用剪贴板策略的现有已发布浏览器，在迁移过程中会自动启用复制和粘贴功能，以保留之前的行为。无需管理员操作。

- **打印：** 启用打印功能会将远程网页保存为 PDF 并传输到用户的设备。然后用户可以按 Ctrl-P 并选择 Citrix PDF 打印机。默认情况下，此设置处于禁用状态。
- **非信息亭模式：** 启用非信息亭模式会将界面恢复到远程浏览器。然后用户可以访问地址栏并创建多个选项卡和窗口。（禁用非信息亭模式会移除远程浏览器的导航控件和地址栏。）默认情况下，此设置处于启用状态（非信息亭模式已开启）。
- **区域故障转移：** 如果您当前区域报告问题，区域故障转移策略会自动将您发布的浏览器转移到不同的区域。要选择退出，请禁用区域故障转移策略。如果您使用“**自动**”区域选择发布了浏览器，则您的隔离浏览器仍将受此策略约束。默认情况下，此设置处于启用状态。
- **客户端驱动器映射：** 启用客户端驱动器映射策略允许用户在远程会话中上传和下载文件。此功能仅适用于通过 Citrix Workspace 应用程序启动的会话。默认情况下，此设置处于禁用状态。
  - 用户必须将下载的文件仅保存到 `Anonxxx` 目录中的 `ctxmnt` 磁盘上。为此，用户必须导航到所需的存储文件位置。例如，**Anonxxx > ctxmnt > C > Users > User Name > Documents**。



◦ 对话框可能会提示用户接受“**允许所有访问**”或“**读取和写入**”权限以访问 `ctxmnt` 文件夹。



◦ **URL 参数：** 启用 URL 参数允许您在用户启动应用程序时更改新会话的起始 URL。要使此策略生效，请配置本地代理服务器以识别可疑网站并将其重定向到远程浏览器隔离。默认情况下，此设置处于禁用状态。有关详细信息，请参阅 概念验证指南：使用 Azure 中的 Citrix ADC 将 URL 重定向到远程浏览器隔离。

◦ **主机名跟踪：** 使用主机名跟踪功能，使远程浏览器隔离在用户会话期间记录主机名。此策略默认禁用。此信息与 Citrix Analytics 共享。有关详细信息，请参阅 Citrix Analytics。

完成后，单击 **确定**。

- **URL 允许列表：** 使用 **白名单** 任务，将用户限制为仅在其发布的远程浏览器隔离会话中访问允许的 URL。此功能适用于外部经过身份验证的 Web 应用程序。

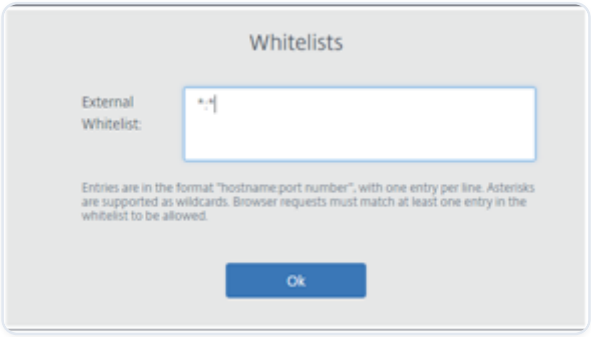
  以 `hostname:port number` 形式输入允许列表条目。每行指定一个条目。支持星号作为通配符。浏览器请求必须与允许列表中的至少一个条目匹配。

  例如，要将 `https://example.com` 设置为允许的 URL：

- `example.com:*` 允许从任何端口连接到此 URL。
- `example.com:80` 仅允许从端口 80 连接到此 URL。
- `*:*` 允许从任何端口以及从指向其他 URL 和端口的任何链接访问此 URL。`*.*` 格式允许从已发布的应用程序访问所有外部 Web 应用程序。此格式是 Web 应用程序 **外部白名单** 字段的默认设置。

完成后，单击 **确定**。

通过与访问控制服务集成，可以使用高级 Web 筛选功能。有关详细信息，请参阅 用例：选择性访问应用程序。



监视

监视 选项卡提供有关用户实时会话的信息。您可以监视和断开一个或多个活动会话。

要停止单个会话，请选择该会话，然后单击条目行末尾的省略号菜单。单击 **注销会话** 并确认您的更改。

要断开多个会话，请选择列表中的活动会话，然后单击页面顶部的 **注销** 按钮。确认更改后，远程浏览器隔离会立即断开所有选定会话。

Remote Browser Isolation 技术安全概述

Remote Browser Isolation（以前称为 Secure Browser 服务）是一种由 Citrix 管理和运营的 SaaS 产品。它允许通过托管在云中的中间 Web 浏览器访问 Web 应用程序。

云服务

Citrix Remote Browser Isolation™ 服务由在虚拟投递代理 (VDA) 上运行的 Web 浏览器以及用于管理和连接用户到这些 VDA 的管理控制台组成。Citrix Cloud 管理这些组件的运行，包括操作系统、Web 浏览器和 Citrix 组件的安全和修补。

使用 Remote Browser Isolation 服务时，托管的 Web 浏览器会跟踪用户的浏览历史记录并执行 HTTP 请求的缓存。Citrix 使用强制配置文件，并确保在浏览会话结束时删除此数据。

Remote Browser Isolation 服务可通过兼容 HTML5 的 Web 浏览器访问。该服务不提供任何可下载的客户端。使用中的浏览器与云服务之间的所有流量均使用行业标准 TLS 加密进行加密。Remote Browser Isolation 仅支持 TLS 1.2。

Remote Browser Isolation 的出站流量使用特定的 IP 地址来保护内部网络。有关接受的 IP 地址列表，请参阅知识中心文章 CTX286379。

Web 应用程序

Citrix Remote Browser Isolation 用于交付由客户或第三方拥有的 Web 应用程序。Web 应用程序的所有者负责其安全性，包括修补 Web 服务器和应用程序以防范漏洞。

Remote Browser Isolation 与 Web 应用程序之间的流量安全性取决于 Web 服务器的加密设置。为了在流量流经 Internet 时保护它，管理员会发布 HTTPS URL。

更多信息

有关更多安全信息，请参阅以下资源：

- Citrix 安全站点：https://www.citrix.com/security
- Citrix Cloud 文档：Citrix Cloud 平台安全部署指南

Citrix 远程浏览器隔离文档历史记录

以下表格描述了 Citrix 远程浏览器隔离服务（原 Secure Browser 服务）产品文档的重要变更。要接收这些更新的通知，请订阅 RSS 源。

有关 2022 年 7 月之前远程浏览器隔离服务文档的变更，请参阅 Citrix Cloud 文档历史记录。

日期	变更	描述
30 Jun 2025	软件升级和补丁管理。	Citrix 创建并管理计算机映像和目录，包括软件管理。当新版本的目录可用时，Citrix 会将这些升级推送到客户目录，确保客户的计算机在下次重新启动时接收最新的修复和补丁。有关详细信息，请参阅软件升级和补丁管理。
30 Jun 2025	启用网络地址转换 (NAT) (Secure Web) 网关。	在"配置详细信息"页面上，您可以选择为特定目录添加 Secure Web Gateway。有关详细信息，请参阅 启用网络地址转换 (NAT) (Secure Web) 网关。
30 Jun 2025	为客户管理的 RBI 目录虚拟网络配置 Azure 防火墙。	Azure 防火墙使您能够筛选远程浏览器隔离服务中目录计算机的传出 Web 请求。通过在现有 Azure 虚拟网络中部署 Azure 防火墙，您可以控制和监视出站流量。有关详细信息，请参阅 为客户管理的 RBI 目录虚拟网络配置 Azure 防火墙。
30 Jun 2025	远程浏览器隔离自托管工作负载。	远程浏览器隔离自托管工作负载使客户能够在自己的 Azure 订阅中运行远程浏览器工作负载。有关详细信息，请参阅

日期	变更	描述
		远程浏览器隔离 - 自托管工作负载。
05 Oct 2022	Secure Browser 更名为 Remote Browser Isolation。	Secure Browser 更名为 Remote Browser Isolation。
27 Jul 2022	远程浏览器隔离支持使用 Azure Active Directory 对所有应用程序进行身份验证。	远程浏览器隔离支持使用 Azure Active Directory 对所有应用程序进行身份验证，并允许用户在 Citrix Workspace 登录页面上登录。有关详细信息，请参阅 新增功能。