Citrix 远程浏览器隔离

Machine translated content

Disclaimer

Contents

Remote Browser Isolation

July 1, 2024

Citrix Remote Browser Isolation 服务（以前称为 Secure Browser 服务）可隔离 Web 浏览，以保护企业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的 Web 应用程序的一致安全远程访问，无需配置用户设备。管理员可以快速推出远程隔离浏览器，从而即时实现价值。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，而不会影响企业安全性。

用户通过 Citrix Workspace（或 Citrix Receiver）登录，然后可以在配置的 Web 浏览器中打开 Web 应用程序。该网站不会将任何浏览数据直接传输到用户设备或从用户设备传输任何浏览数据，因此体验是安全的。

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

- 共享密码外部 **Web** 应用程序。如果您发布带有共享密码身份验证的浏览器，则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。发布经过身份验证的外部 Web 应用程序并使用 Citrix Workspace 启动应用程序时，Remote Browser Isolation 服务需要一个至少包含一个 Cloud Connector（建议使用两个或更多）的资源位置。有关详细信息，请参阅 Citrix Cloud Connector。对于经过身份验证的应用程序，必须使用 Citrix Cloud 库添加用户。
- 未经身份验证的外部 **Web** 应用程序。发布未经身份验证的外部 Web 应用程序并使用 Citrix Workspace 启动应用程序时，Remote Browser Isolation 服务需要一个至少包含一个 Cloud Connector（建议使用两个或更多）的资源位置。有关详细信息，请参阅 Citrix Cloud Connector。

  尽管通常不建议使用，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。

有关更多信息，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 Workspace 集成
- 将已发布的应用程序与本地 StoreFront 集成
- 简单的 URL 允许列表功能确保安全
- 使用情况监视
- 控制剪贴板使用、打印、展台模式、区域故障转移和客户端驱动器映射

使用 **Citrix Secure Private Access** 的 **Remote Browser Isolation** 服务

您可以使用 Citrix Secure Private Access 控制台启动 Remote Browser Isolation 服务的已发布浏览器来访问企业 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 Remote Browser Isolation 服务的已发布浏览器中打开。

有关通过 Citrix Secure Private Access Private Access 访问隔离的远程浏览器的详细信息，请参阅 Citrix Secure Private Access 文档中的使用多个规则配置访问策略和未经批准的 Web 站点。

参考文章

- Secure Private Access 服务解决方案概述
- Citrix Cloud
- 自助搜索 Remote Browser Isolation (Secure Browser)
- Citrix Enterprise Browser
- 安全性和合规性信息
- 开发人员文档

相关产品中的新增功能

- Secure Private Access
- Citrix Enterprise Browser
- Citrix Analytics for Security

新增功能

October 14, 2022

2022 年 **7** 月

- **Remote Browser Isolation** 支持使用 **Azure Active Directory** 对所有应用程序进行身份验证
  - 用户现在可以使用 Azure Active Directory 凭据从 Citrix Workspace 登录任何 Remote Browser Isolation 应用程序
  - 当 Remote Browser Isolation 用户登录时，他们将使用您为站点配置的 Workspace 登录页面。有关更多信息，请参阅 与 Citrix Workspace 集成。

2021 年 **9** 月

- **Remote Browser Isolation** 支持双向音频。双向音频在 Remote Browser Isolation 中可用。
- 从 **launch.cloud.com** 启动的 **Remote Browser Isolation** 已通过 **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 应用程序时，Citrix Cloud 身份验证会处理他们的证书。这增强了安全性，但不会改变用户体验。

2021 年 3 月

- **Remote Browser Isolation** 支持使用 **Azure Active Directory** 进行身份验证。用户现在可以使用 Azure Active Directory 凭据从 Citrix Workspace 登录 Remote Browser Isolation 应用程序有关更多信息，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。您可以查看有关每个活动会话的基本信息，并在需要时断开会话连接。有关更多信息，请参阅 监视活动会话。

2020 年发布

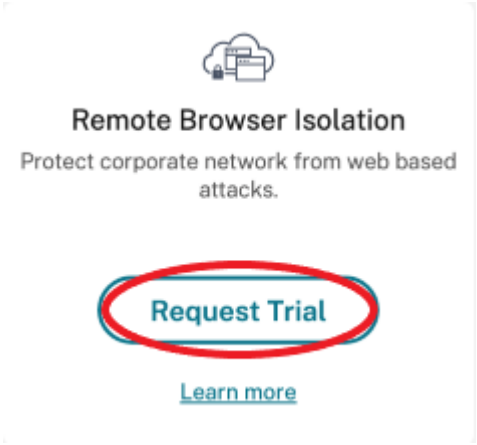
2020 年的所有版本都包含有助于提高整体性能和稳定性的增强功能。

Remote Browser Isolation 入门

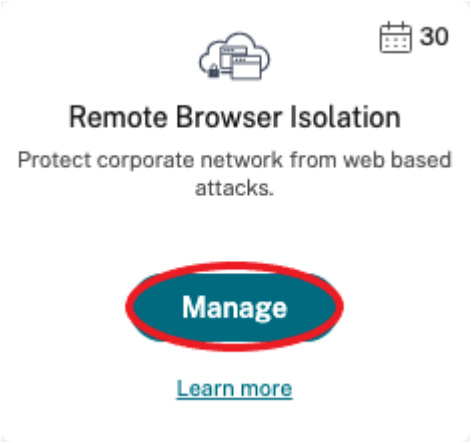
October 14, 2022

以下是关于开始使用 Remote Browser Isolation 服务（以前称为 Secure Browser 服务）的视频。

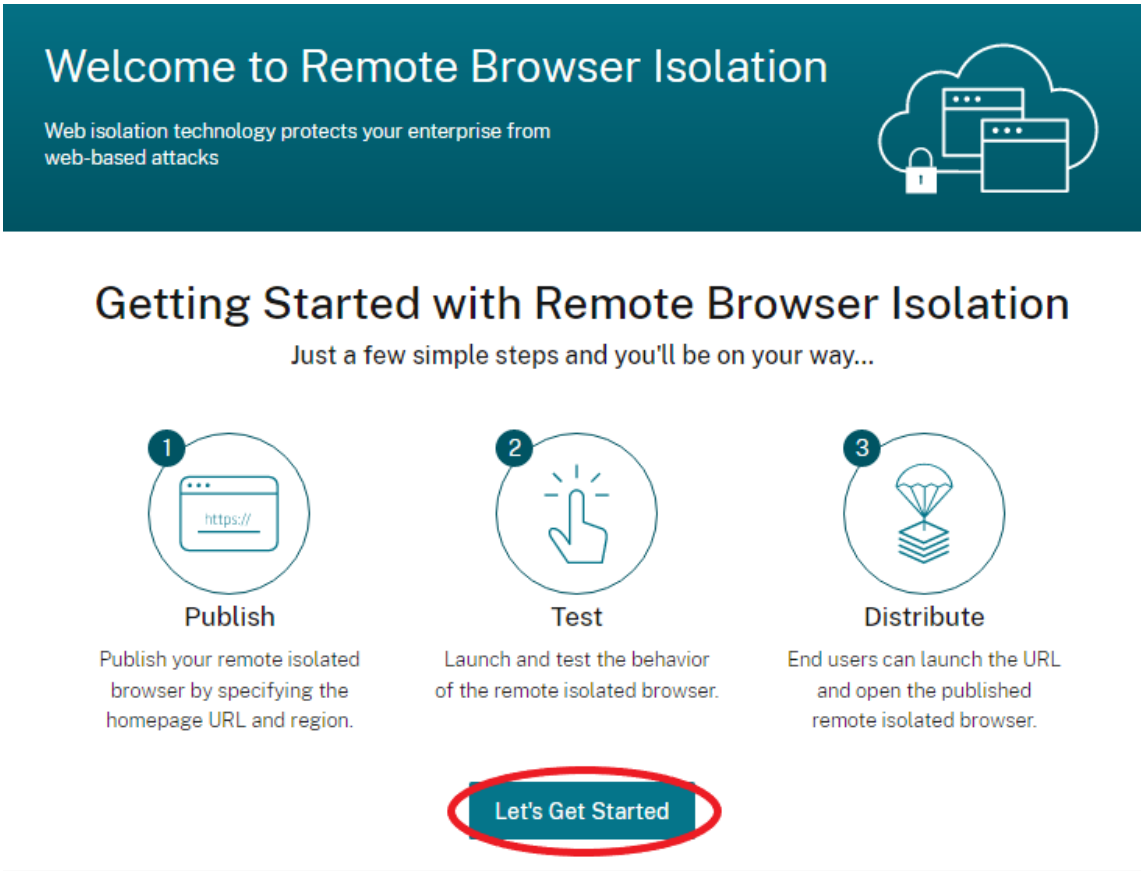
1. 登录 Citrix Cloud。如果您没有帐户，请参阅 注册 Citrix Cloud。您可以申请 Citrix Remote Browser Isolation 的 30 天试用期。
2. 在“**Remote Browser Isolation**”磁贴中，单击“申请试用”。



3. 稍后，您将收到一封电子邮件（与您的 Citrix Cloud 帐户关联的电子邮件）。点击电子邮件中的 登录 链接。
4. 再次进入 Citrix Cloud 后，单击“**Remote Browser Isolation**”磁贴上的“管理”。



5. 在“欢迎使用 **Remote Browser Isolation**”页面上，单击“让我们开始吧”。



6. 选择要发布的远程隔离浏览器的类型：共享密码、已验证或未经身份验证。然后单击继续。

   默认情况下，用户必须使用 launch.cloud.com 启动具有共享密码身份验证的应用程序。Citrix Workspace 和 Citrix Cloud 库不支持具有共享密码的应用程序。

   要使用 Citrix Workspace，您必须发布经过身份验证的应用程序，并在 Citrix Cloud 库中显式分配订阅者（用户）或组。未经身份验证的应用程序可供所有 Workspace 订阅者使用，无需分配用户。

7. 配置以下设置：

- 名称：键入您正在创建的应用程序的名称。
- 起始网址：指定用户启动应用程序时打开的 URL。
- 区域：选择服务器的位置/区域。可用区域包括美国西部、美国东部、东南亚、澳大利亚东部和西欧。

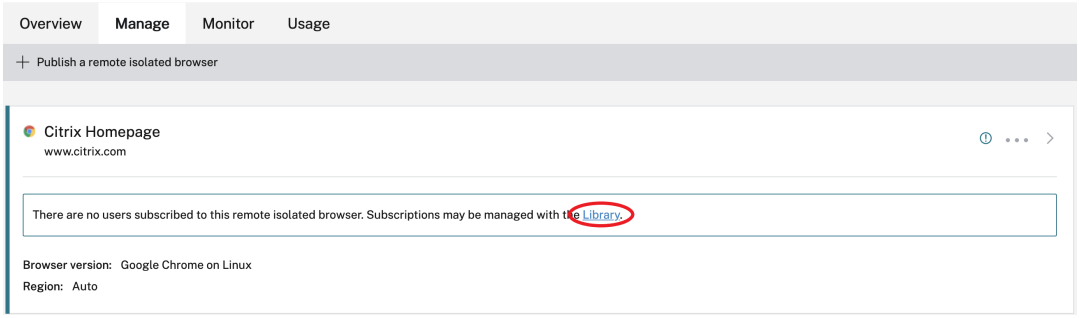
  如果您选择“自动”，则您的隔离浏览器会根据您的地理位置将您连接到最近的区域。
- 密码：如果您选择了采用共享密码身份验证的浏览器，请输入密码以增强对应用程序的安全访问权限。密码长度必须至少为 10 个字符，至少包含 1 个数字和 1 个符号。确保保存密码并与用户共享。用户在使用 launch.cloud.com 启动应用程序时必须输入密码。
- 图标：默认情况下，发布独立浏览器时使用 Google Chrome 可执行文件的图标。现在，您可以选择自己的图标来表示已发布的浏览器。

  单击 更改图标 **>** 选择图标 以上传您选择的图标，或选择 使用默认图标以使用 现有的 Google Chrome 浏览器图标。

单击“发布”。

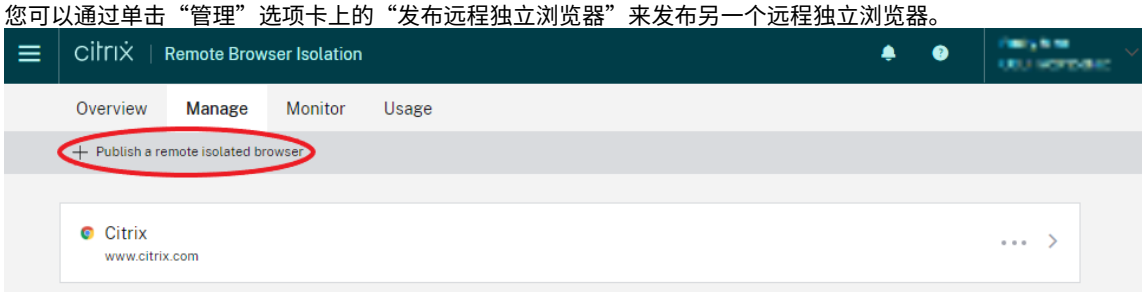
8. 管理 选项卡列出了您发布的浏览器。要启动您刚刚创建的浏览器，请单击包含隔离浏览器的图块上的省略号，然后单击“启动已发布浏览器”。

   - 如果您发布了经过身份验证的隔离浏览器，则必须使用 Citrix Cloud Library 来添加用户或群组。单击该行末尾的向右箭头，展开包含指向库的链接的详细信息窗格。

     当您单击提供的链接时，系统会引导您进入包含远程隔离浏览器的图书馆显示屏。单击包含隔离浏览器的图块上的省略号，然后单击“管理订阅者”。有关添加订阅者的信息，请参阅 使用库将用户和组分配到服务方案。

您可以通过单击“管理”选项卡上的“发布远程独立浏览器”来发布另一个远程独立浏览器。



有关购买 Citrix Remote Browser Isolation 服务（以前称为 Citrix Secure Browser 服务）的信息，请访问 https://www.citrix.com/products/citrix-remote-browser-isolation/。

与 **Citrix Workspace** 集成

Remote Browser Isolation 可以与 Citrix Workspace 集成。要确保其集成，请执行以下操作：

1. 登录 Citrix Cloud。
2. 在左上角的菜单中，选择 **Workspace** 配置。
3. 选择“服务集成”选项卡。
4. 确认“Remote Browser Isolation”服务条目显示“已启用”。如果没有，请单击省略号菜单，然后选择 启用。

如果尚未执行此操作，请按照配置工作区身份验证中所述 配置 Workspace URL、外部连接和工作区身份验证。

Remote Browser Isolation 支持使用 Active Directory 和 Azure Active Directory 进行身份验证。默认情况下，使用 Active Directory 进行身份验证。有关使用 Azure Active Directory 配置身份验证的信息，请参阅 将 Azure Active Directory 连接到 Citrix Cloud。

如果您使用 Azure Active Directory 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）云连接器

与您的本地 **StoreFront** 集成

拥有本地 StoreFront 的 Citrix Virtual Apps and Desktops 客户可以轻松地与 Remote Browser Isolation 服务集成，从而提供以下好处：

- 将已发布的远程隔离浏览器与现有的 Citrix Virtual Apps and Desktops 应用程序聚合在一起，以获得统一的商店体验。
- 使用本机 Citrix Receiver 增强最终用户体验。
- 使用与 StoreFront 集成的现有多因素身份验证解决方案，增强 Remote Browser Isolation 启动的安全性。

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

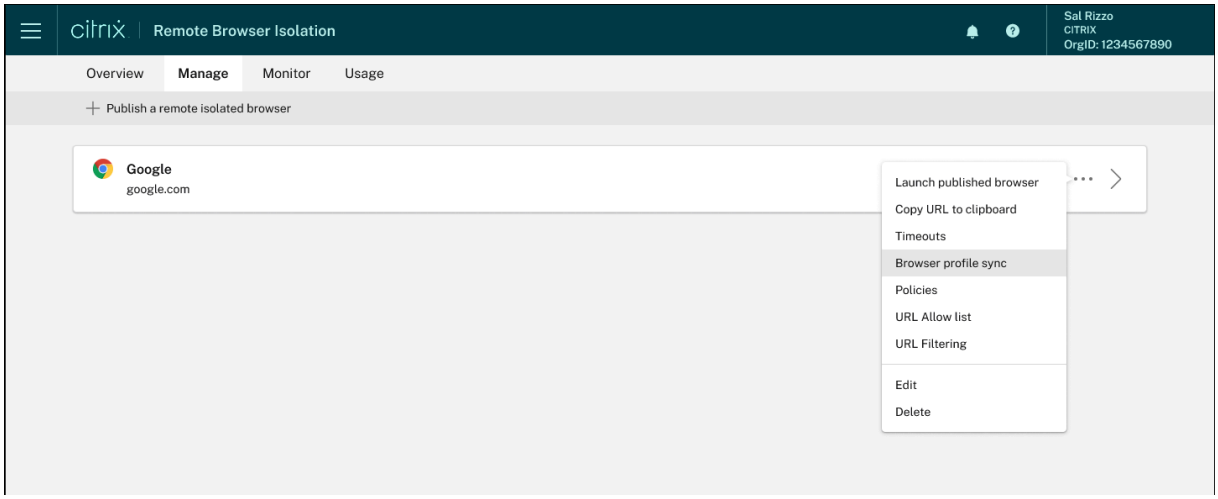
管理和监视远程隔离浏览器

April 5, 2024

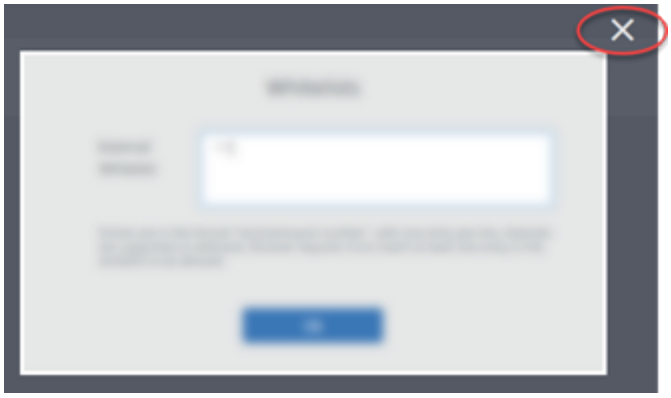
现在，您可以在 Remote Browser Isolation 中管理、监视和检查已发布浏览器的使用情况。

管理

管理选项卡列出了已发布的浏览器。要访问管理任务，请单击已发布浏览器右端的省略号，然后选择所需的任务。



如果选择了某个菜单项，然后决定不进行任何更改，请通过单击对话框外的 **X** 来取消选择。

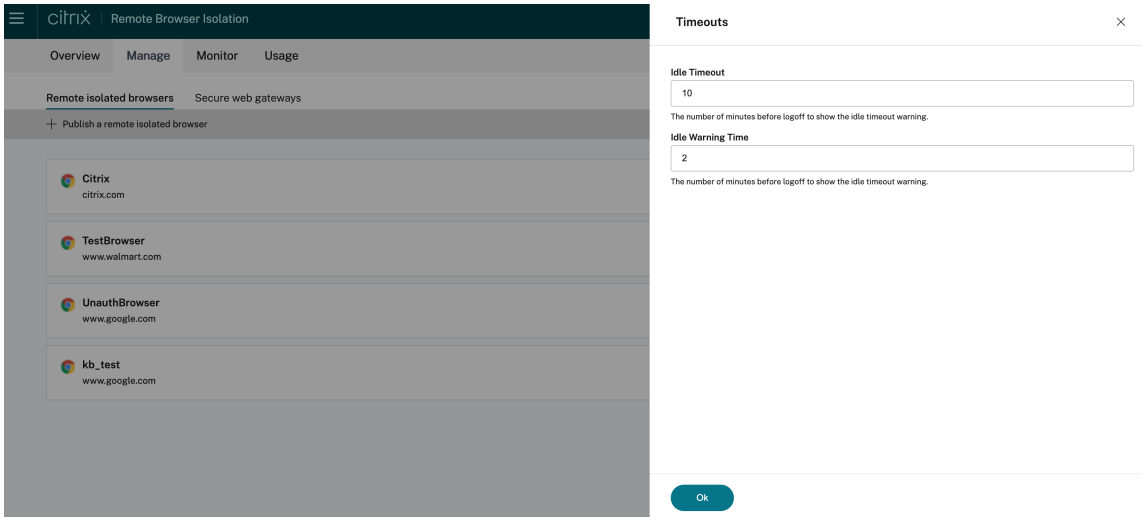


您可以使用以下任务管理已发布的隔离浏览器：

- 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。
- 超时：您可以通过选择超时任务来设置空闲超时和空闲警告时间。
  - 空闲超时：会话在因不活动而结束之前可以保持空闲状态的分钟数。
  - 空闲警告时间：在结束会话之前向用户发送警告消息的分钟数。

  例如，如果您将“空闲超时”设置为 20，“空闲警告时间”设置为 5，则如果会话中在 15 分钟内没有活动，系统将显示一条警告消息。如果用户没有响应，会话将在五分钟后结束。

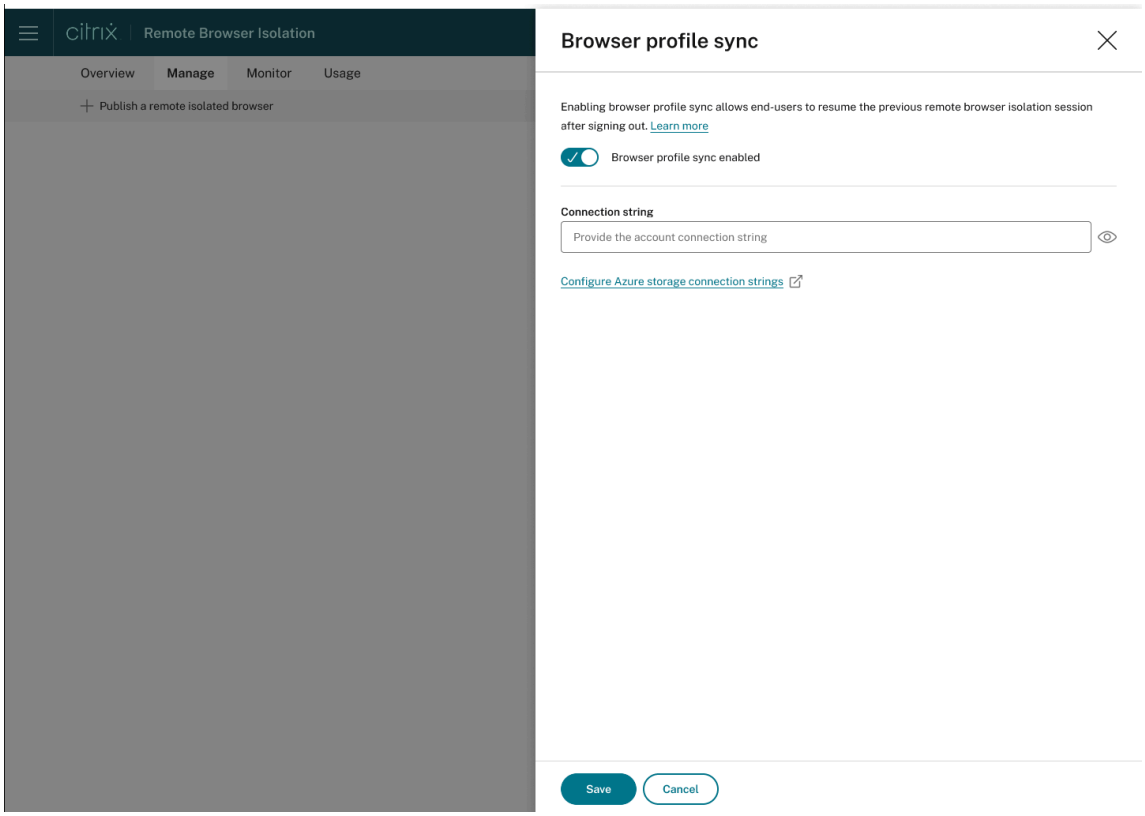
  要设置已发布的独立浏览器的空闲超时和空闲警告时间，请选择超时任务，然后在超时对话框中设置空闲超时和空闲警告时间。然后，单击“确定”保存更改。



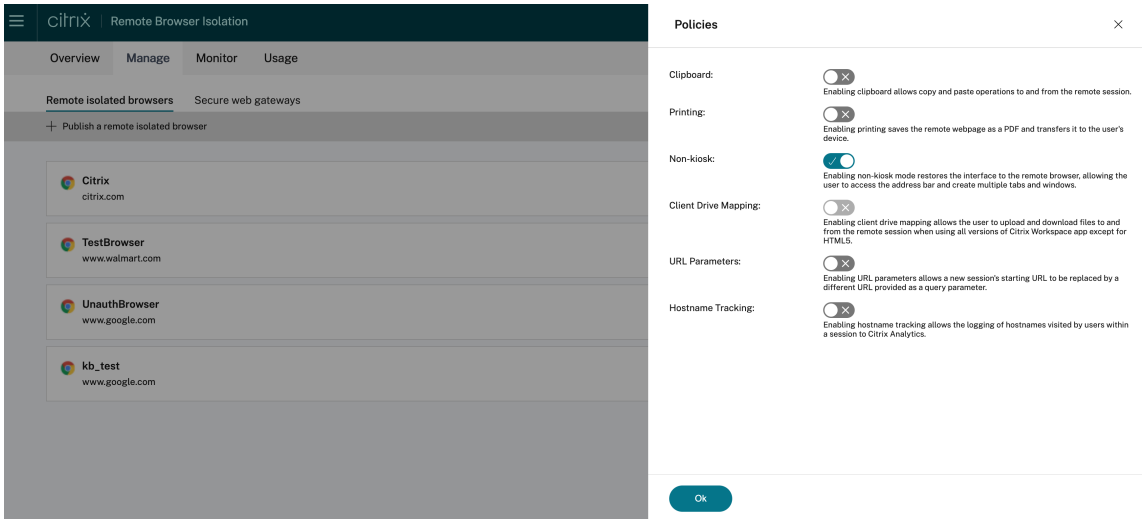
- 浏览器配置文件同步：允许最终用户在注销后恢复之前的浏览器会话。管理员可以为其 Azure 存储指定连接字符串，以启用浏览器配置文件的存储。当用户使用相同的配置文件打开另一个浏览器会话时，它会从用户中断的地方恢复之前的浏览器会话。如果用户登录了任何网站，则这些网站负责身份验证。尽管此功能可以保存会话、Cookie 和其他信息，但网站可能要求用户重新登录。目前，此功能仅支持选项卡恢复。

  要启用浏览器配置文件同步功能，请执行以下步骤：

  1. 为所需的已发布浏览器选择浏览器配置文件同步任务。
  2. 在浏览器配置文件同步对话框中，启用浏览器配置文件同步并输入连接字符串。有关配置连接字符串的详细信息，请参阅 Azure Blob 存储文档中的配置 Azure 存储连接字符串。
  3. 单击保存。



- 策略：您可以为已发布的浏览器设置策略。

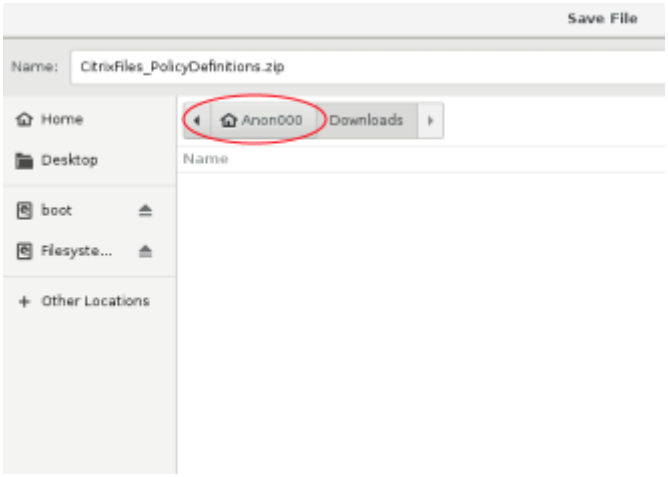


策略页面上的设置控制以下内容：

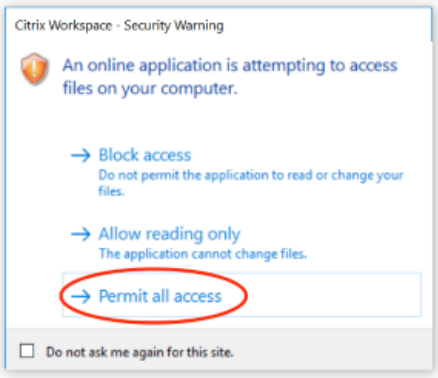
- 剪贴板：启用剪贴板策略允许在远程会话之间进行复制和粘贴操作。（禁用剪贴板策略会从 Citrix Workspace 应用程序工具栏中删除“剪贴板”按钮。）默认情况下，此设置处于禁用状态。
- 打印：启用打印功能会将远程网页另存为 PDF 并将其传输到用户的设备。然后，用户可以按 Ctrl-P 并选择 Citrix PDF 打印机。默认情况下，禁用此设置。
- 非 **Kiosk**：启用非 Kiosk 模式可将界面恢复到远程浏览器。然后，用户可以访问地址栏并创建多个选项

卡和窗口。（禁用非展台模式会删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（非展台模式处于开启状态）。

- 区域故障转移：如果您当前的区域报告了问题，则区域故障转移策略会自动将您发布的浏览器转移到其他区域。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，则您的隔离浏览器将保持注册状态。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向远程会话上载和下载文件。此功能仅适用于使用 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。
  * 用户只能将下载的文件保存在 **Anonxxx** 目录中的 **ctxmnt** 磁盘上。为此，用户必须导航到存储文件的所需位置。例如，**Anonxxx > ctxmnt > C >** 用户 **>** 用户名 **>** 文档。



  * 该对话框可能会提示用户接受“允许所有访问”或“读写”权限才能访问 **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 Remote Browser Isolation。默认情况下，禁用此设置。有关更多信息，请参阅概念证明指南：在 Azure 中使用 Citrix ADC 将 URL 重定向到 Remote Browser Isolation。
- 主机名跟踪：使用主机名跟踪启用 Remote Browser Isolation，以便在用户会话期间记录主机名。默认情况下禁用此策略。此信息将与 Citrix Analytics 共享。有关更多信息，请参阅 Citrix Analytics。

完成后，单击确定。

- **URL** 允许列表：使用白名单任务限制用户在其发布的 Remote Browser Isolation 会话中仅访问允许的 URL。此功能适用于外部经过身份验证的 Web 应用程序。

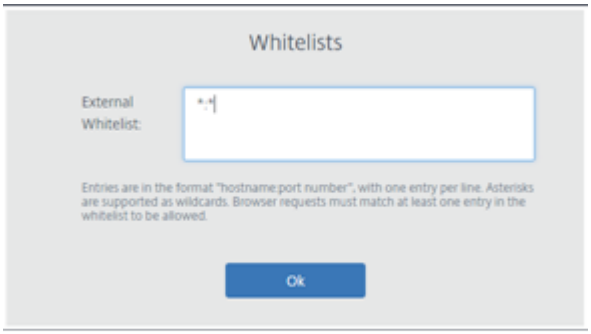
  在表单中输入允许列表条目 `hostname:port number`。在新行中指定每个条目。星号支持作为通配符。浏览器请求必须与允许列表中的至少一个条目匹配。

  例如，要设置 `https://example.com` 为允许的 URL，请执行以下操作：

  - `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任何指向其他 URL 和端口的链接访问此 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的集成，可以获得高级 Web 筛选功能。如需了解详情，请参阅使用案例：选择性访问应用程序。



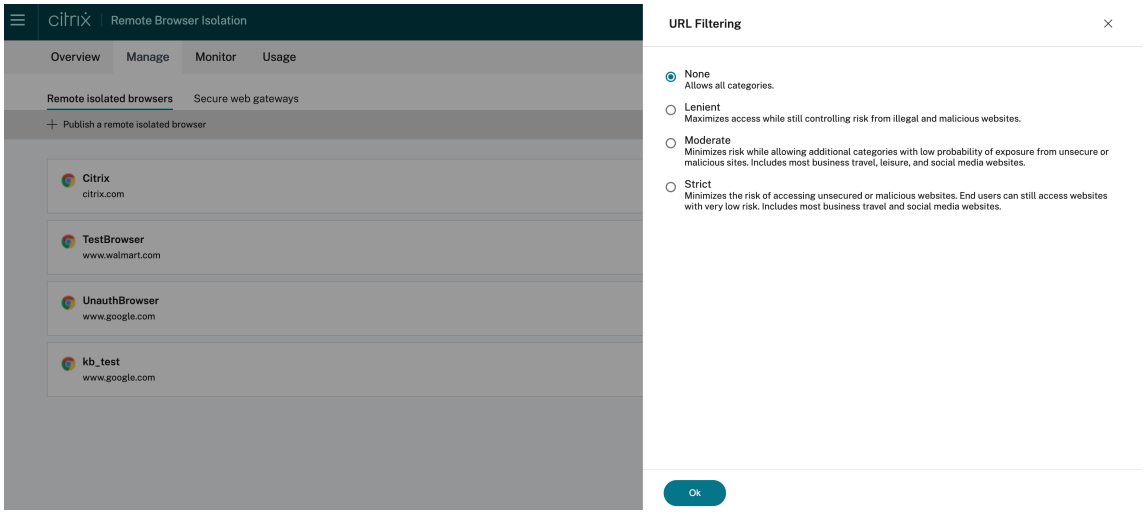
- **URL** 过滤：您可以配置 URL 过滤，以根据与风险模型相关的预定义类别来控制访问方法。URL 过滤选项包括：
  - 无 -允许所有类别。
  - 宽容 -最大限度地提高访问权限，同时仍然控制来自非法和恶意网站的风险。包括以下类别：
    - 成人**:** 怪诞, 性教育, A 片, 裸露, 性服务, 成人搜索和链接, 泳衣和内衣, 成人杂志和新闻, 性表达 (文本), 恋物癖, 和约会.
    - 计算和互联网：远程代理、私有 IP 地址、点对点文件共享和种子。
    - 赌博：抽奖、奖品、彩票和一般赌博。
    - 非法和有害：恐怖主义、极端主义、仇恨、诽谤、武器、暴力、自杀、非法毒品、药物、非法活动、大麻和一般宣传。
    - 恶意软件和垃圾邮件：黑客，恶意软件，垃圾邮件，间谍软件，僵尸网络，受感染的站点，网络钓鱼网站，键盘记录器，移动恶意软件，电话机器人，恶意和危险的网站。
  - 中等**-**最大限度 地降低风险，同时允许更多类别从不安全或恶意网站曝光的可能性较小。包括以下类别：
    - 成人**:** 怪诞, 性教育, A 片, 裸露, 性服务, 成人搜索和链接, 泳衣和内衣, 成人杂志和新闻, 性表达 (文本), 恋物癖, 和约会.

  - 商业和工业：拍卖。
  - 计算和互联网：广告、横幅、远程代理、私有 IP 地址、点对点文件共享和种子。
  - 下载：移动应用商店、存储服务、下载和程序下载。
  - 电子邮件：基于 Web 的邮件和电子邮件订阅。
  - 金融：加密货币。
  - 赌博：抽奖、奖品、彩票和一般赌博。
  - 恶意软件和垃圾邮件：黑客，恶意软件，垃圾邮件，间谍软件，僵尸网络，受感染的站点，网络钓鱼网站，键盘记录器，移动恶意软件，电话机器人，恶意和危险的网站。
  - 消息、聊天和电话：即时消息和基于 Web 的聊天。
  - 新闻、娱乐和社会： WordPress（帖子和上载）、不支持的网址、神秘的、无内容、杂项、星座运势、占星术、算命、饮酒、宗教、个人网页、博客和在线游戏。
  - 社交网络：照片搜索和共享站点、IT 公告板和公告板。

- 严格 -将访问不安全或恶意网站的风险降至最低。最终用户仍然可以低风险访问网站。包括以下类别：

  - 成人**:** 怪诞, 性教育, A 片, 裸露, 性服务, 成人搜索和链接, 泳衣和内衣, 成人杂志和新闻, 性表达 (文本), 恋物癖, 和约会.
  - 商业和工业：拍卖。
  - 计算和互联网：广告、横幅、动态 DNS、移动应用程序、发布商、托管域、远程代理、私有 IP 地址、点对点文件共享和种子。
  - 下载：移动应用商店、存储服务、下载和程序下载。
  - 电子邮件：基于 Web 的邮件和电子邮件订阅。
  - 金融：加密货币和金融产品。
  - 赌博：抽奖、奖品、彩票和一般赌博。
  - 非法和有害：恐怖主义、极端主义、仇恨、诽谤、武器、暴力、自杀、非法毒品、药物、非法活动、大麻和一般宣传。
  - 职位和简历：就业、职业发展和 LinkedIn（更新、邮件、联系和工作）。
  - 恶意软件和垃圾邮件：黑客，恶意软件，垃圾邮件，间谍软件，僵尸网络，受感染的站点，网络钓鱼网站，键盘记录器，移动恶意软件，电话机器人，恶意和危险的网站。
  - 消息、聊天和电话：即时消息和基于 Web 的聊天。
  - 新闻、娱乐和社会： WordPress（帖子和上载）、住宿、旅行和旅游、不支持的网址、政治、时尚和美容、艺术和文化活动、参考、娱乐和爱好、当地社区、其他、饮酒、热门话题、特别活动、新闻、社会还有文化、在线杂志、在线游戏、生活事件、神秘学、无内容、星座、占星术、算命、名人、流媒体、娱乐、场所、活动、个人网页和博客以及宗教。
  - 社交网络：一般社交网络、YikYak（帖子）、Twitter（帖子、邮件和关注）、Vine（上载、评论和消息）、Google+（照片和视频上载、帖子、视频聊天和评论）、Instagram（上载和评论）、YouTube（分享和评论）、Facebook（组、游戏、问题、视频上载、照片上载、活动、聊天、应用程序、帖子、评论和朋友）、Tumblr（帖子、评论、照片和视频上载）、Pinterest（图钉和评论）、IT 公告板和公告板。

完成后，单击确定。



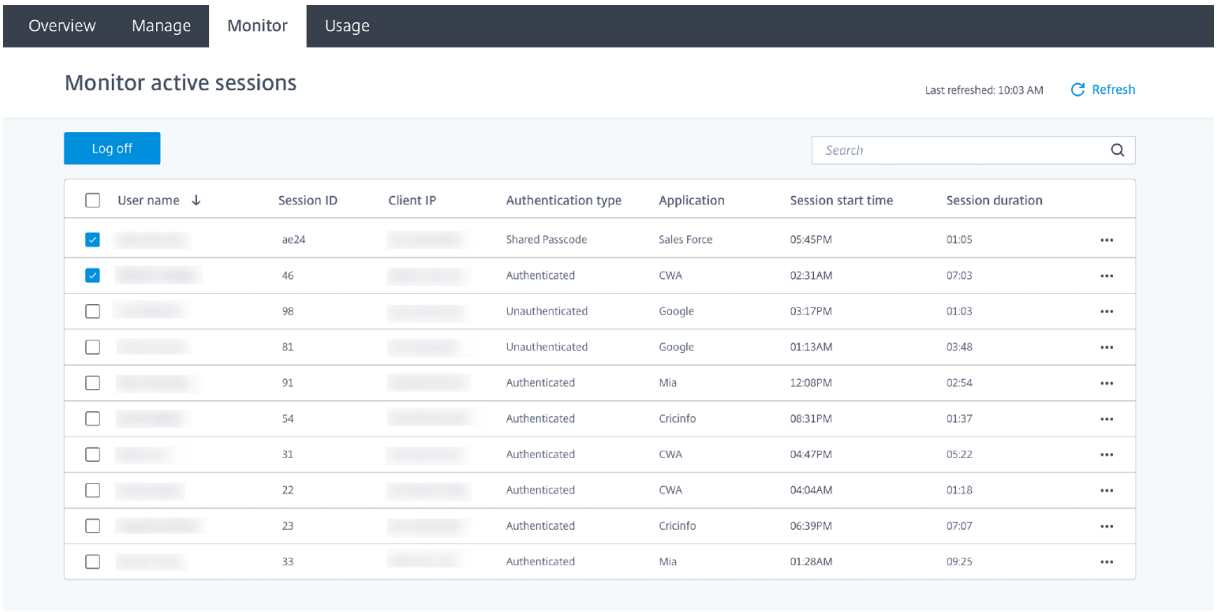
- 编辑：您可以使用编辑任务更改已发布浏览器的名称、起始 URL、区域或通行码。完成后，单击“发布”。
- 删除：您可以使用删除任务删除已发布的隔离浏览器。选择此任务时，系统会提示您确认删除。

Monitor

“监视”选项卡提供有关用户实时会话的信息。您可以监视一个或多个活动会话并断开连接。

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。

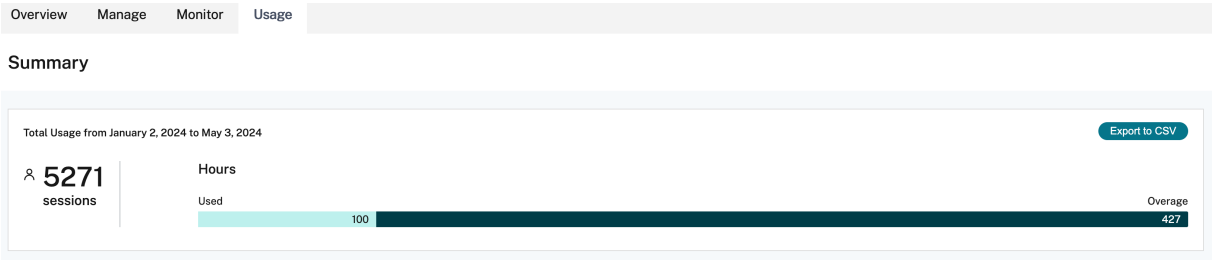
要断开多个会话的连接，请在列表中选择活动会话，然后单击页面顶部的 注销 按钮。确认更改后，Remote Browser Isolation 会立即断开所有选定会话的连接。



使用情况

“使用情况”选项卡显示已启动的会话数量和使用的小时数。

要创建包含使用情况详细信息的电子表格，请单击 导出为 **CSV** 并选择时间范围。



Remote Browser Isolation 技术安全概述

October 14, 2022

Remote Browser Isolation（以前称为 Secure Browser 服务）是由 Citrix 管理和运营的 SaaS 产品。它允许通过云中托管的中间 Web 浏览器访问 Web 应用程序。

云端服务

Citrix Remote Browser Isolation 服务由在 Virtual Delivery Agent (VDA) 上运行的 Web 浏览器以及用于管理用户和将用户连接到这些 VDA 的管理控制台组成。Citrix Cloud 管理这些组件的操作，包括操作系统、Web 浏览器和 Citrix 组件的安全和修补。

在使用 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。

使用兼容 HTML5 的 Web 浏览器访问 Remote Browser Isolation 服务。该服务不提供任何可下载的客户端。正在使用的浏览器和云服务之间的所有流量均使用行业标准的 TLS 加密进行加密。Remote Browser Isolation 仅支持 TLS 1.2。

Remote Browser Isolation 的出口流量使用特定的 IP 地址来保护内部网络。有关接受的 IP 地址的列表，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，包括修补 Web 服务器和应用程序以防漏洞。

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。为了在流经互联网时保护这些流量，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 安全网站：https://www.citrix.com/security
- Citrix Cloud 文档：Citrix Cloud 平台安全部署指南